



Deploying Avaya Aura[®] System Manager on System Platform

Release 6.3
October 2013

Notice

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

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya 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](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	7
Purpose	7
Intended audience	7
Document changes since last issue	7
Related resources	8
Documentation	8
Training	9
Viewing Avaya Mentor videos	9
Support	10
Warranty	10
Chapter 2: System Manager - installation requirements	11
Introduction	11
Server requirements	11
Browser support	12
Chapter 3: Checklists and Worksheets	13
System Manager installation checklist	13
System Manager information worksheet	14
Installation worksheet for System Platform	15
Prerequisites for servers on System Platform in the Geographic Redundancy setup	25
Chapter 4: Installing System Platform	27
Preinstallation tasks for System Platform	27
Preinstallation checklist for System Platform	27
Registering the system	28
Registering for PLDS	29
Downloading software from PLDS	30
Verifying the downloaded ISO image	30
Writing the downloaded software to DVD	31
Installing System Platform	32
Installation methods	32
Server requirements	33
Installation checklist for System Platform	33
Connecting your laptop to the server	37
Starting the installation	38
Selecting the type of keyboard	40
Verifying the System Platform server hardware	41
Verifying the System Platform image on the DVD	42
Configuring network settings for System Domain	42
Configuring network settings for Console Domain	45
Installing the Services virtual machine	47

Configuring the time zone for the System Platform server.....	49
Configuring the date and time for the System Platform server.....	49
Configuring System Platform passwords.....	50
Verifying installation of System Platform.....	53
Accessing System Platform.....	54
Configuring SAL Gateway on System Platform.....	58
SAL Gateway.....	58
Configuration prerequisites.....	60
Changing the Product ID for System Platform.....	60
System and browser requirements.....	61
Starting the SAL Gateway user interface.....	61
Configuring the SAL Gateway.....	62
Configuring a proxy server.....	64
Configuring SAL Gateway communication with a Concentrator Core Server.....	66
Configuring SAL Gateway communication with a Concentrator Remote Server.....	67
Configuring NMS.....	68
Managing service control and status.....	69
Applying configuration changes.....	70
Managed element worksheet for SAL Gateway.....	70
Adding a managed element.....	71
Using a stand-alone SAL Gateway.....	73
Installing a solution template.....	74
Search Local and Remote Template field descriptions.....	77
Configuring a proxy.....	78
Configuring System Platform High Availability.....	79
About System Platform High Availability.....	79
Template administration during High Availability operation.....	79
Prerequisites for High Availability configuration.....	80
Configuring System Platform High Availability.....	82
High Availability start/stop.....	86
Manually switching High Availability server roles.....	88
Removing the High Availability configuration.....	89
Chapter 5: Installing System Manager.....	90
Downloading System Manager from the Avaya Support website.....	90
Downloading System Manager from PLDS.....	90
Checking the RAID Controller Battery state.....	91
Installation methods.....	92
Installing the System Manager Release 6.3 template using ISO.....	92
Installing System Manager using a DVD.....	97
Installing the System Manager Release 6.3.13 bin file.....	101
Default credentials.....	101
Installing and committing the patches.....	102
Downloading patches.....	102

Installing patches.....	103
Configuring a proxy.....	103
Committing patches.....	104
Rolling back patches.....	105
Chapter 6: Postinstallation verification.....	106
Verifying the installation of System Manager.....	106
Chapter 7: Configuring System Manager.....	107
System Manager configuration.....	107
Backup Definition field descriptions.....	107
Network Management Systems Destinations.....	108
Chapter 8: Removing the System Manager template	110
Removing the System Manager template.....	110

Chapter 1: Introduction

Purpose

This document provides procedures for installing and configuring Avaya Aura® System Manager on System Platform. The document includes installation checklist, installation, basic configuration, and installation verification procedures.

Intended audience

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

This document does not include optional or customized aspects of a configuration.

Document changes since last issue

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

- Added procedure for installing the System Manager Release 6.3.13 bin file.
- Added procedure for installing the System Platform 6.3.4.08007.0 patch.
- Added support for the following browsers:
 - Internet Explorer 8.x, 9.x, and 10.x
 - Firefox on 27, 28, and 29

Related resources

Documentation

The following table lists the documents related to System Manager. Download the documents from the Avaya Support website at <http://support.avaya.com>.

Title	Description	Audience
Design		
<i>Avaya Aura® System Manager Overview and Specification</i>	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		
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 Avaya Aura® System Platform	Describes the procedures to install and troubleshoot System Platform.	Implementation Engineers and Support personnel
Administration		
<i>Administering Avaya Aura® System Manager</i>	Describes the procedures to configure System Manager and the managed elements that System Manager supports.	Implementation Engineers and Support personnel
Maintenance and Troubleshooting		
<i>Upgrading Avaya Aura® System Manager on System Platform</i>	Describes the procedures to upgrade System Manager from the previous releases. Also, provides the procedures to migrate the System Manager data to Release 6.3.13 by using the data migration utility.	Implementation Engineers and Support personnel
<i>Troubleshooting Avaya Aura® System Manager</i>	Describes the procedures to troubleshoot the problems during the installation and administration of System Manager and the managed elements that System Manager supports.	Implementation Engineers and Support personnel

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: System Manager - installation requirements

Introduction

Use this document to install Avaya Aura® System Manager Release 6.3.13 on System Platform.

Installing the System Manager virtual appliance includes:

1. Installation of System Platform Release 6.3.0.0.18002 on the supported server.

For information, see [Installing System Platform](#) on page 40.

2. Installation of the System Platform 6.3.4.08007.0 patch.

For information, see [Installing patches](#) on page 103.

3. Installation of System Manager Release 6.3 on System Platform.

For information, see [Installing System Manager](#) on page 92.

4. Installation of the `System_Manager_6.3.13_r5003336.bin` file.

For information, see [Installing the System Manager patch](#) on page 101.

Avaya Aura® provides System Manager Geographic Redundancy, a resiliency feature that handles scenarios where the primary System Manager server fails or the data network partially loses connectivity. In such scenarios, the system manages and administers products such as Avaya Aura® Session Manager and Avaya Aura® Communication Manager across the customer enterprise using the secondary System Manager server.

The installation process does not enable Geographic Redundancy (GR). You must manually configure GR on the standalone server. For Geographic Redundancy-related procedures, see Geographic Redundancy in *Administering Avaya Aura® System Manager*.

For procedures to deploy System Manager on VMware, see *Deploying Avaya Aura® System Manager on VMware® in Virtualized Environment*.

Server requirements

You must install System Platform on the server before you install System Manager.

For the existing System Manager servers, Avaya supports System Manager installations on the following servers:

- S8800
- Dell™ PowerEdge™ R610
- HP ProLiant DL360 G7
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R620

 Note:

For new purchases, Avaya provides the HP ProLiant DL360p G8 server with System Manager. However, the customer can also request for the Dell™ PowerEdge™ R620 server.

Browser support

System Manager Release 6.3.13 supports the following browsers:

Browser	Supported release
Internet Explorer	8.x, 9.x, and 10.x
Firefox	27, 28, and 29

 Note:

Release 6.3.13 does not support the earlier releases of the browsers.

Chapter 3: Checklists and Worksheets

System Manager installation 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.	! Important: If the RAID Controller battery depletes, the Disk Cache policy is set to WriteThrough. As a result, the overall system operations slow down and the duration of the upgrade process increases. For additional information, see the S8800 or HP ProLiant DL360p G8 server RAID on the Avaya Support website at http://support.avaya.com/ .	
2	Download the following software from the Avaya Support website at http://support.avaya.com/ : • The System Platform Release 6.3.0.0.18002 software • The System Platform 6.3.4.08007.0 patch file • The System_Manager_06_03_Version_II.iso file • The System_Manager_6.3.13_r5003336.bin file	Verify that the md5sum for the downloaded ISO image matches the number on the support website.	
3	Set up a DVD or a USB flash drive to install System Platform from a DVD or USB flash drive.	-	
4	Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.	See <i>Administering Avaya Aura® System Manager</i>	

Table continues...

Serial Number	Action	Notes	✓
5	Install System Platform.	See the Installing System Platform section.	
6	Install the System Platform 6.3.4.08007.0 patch.	Installing patches on page 103	
7	Install the System_Manager_06_03_Version_II.iso file.	Installing System Manager on page 92	
8	Install the System_Manager_6.3.13_r5003336.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 patch on page 101	
9	Verify that the System Manager installation is successful.	Verifying the installation of System Manager on page 106	

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.

Table continues...

Field	Value	Notes
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:		

Table continues...

Name	Value	Description
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 the WebLM application. Default value = <code><cdom_IP_address></code> .
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

Table continues...

Name	Value	Description
		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 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/next/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 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 <i>search</i> 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, <code>SPCdom.mydomainname.com</code> . 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, <code>SPDom0.mydomainname.com</code> . 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).

Table continues...

Name	Value	Description
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. 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

Table continues...

Name	Value	Description
		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.
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 • 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

Table continues...

Name	Value	Description
		For more information about bonding modes, see http://www.linuxhorizon.ro/bonding.html . * 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 subnetmask 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

Table continues...

Name	Value	Description
		1001119999 is set. You must change this default ID to the unique Product ID that Avaya provides. * 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 <code>public</code> .
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.
Idap Password		The password for the Idap 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

Table continues...

Name	Value	Description
		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.

Table continues...

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

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 System Platform 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.

Chapter 4: 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 28.	 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 15.		
3	Register for PLDS unless you have already registered. See Registering for PLDS on page 29.		
4	Download the System Platform installer ISO image file from PLDS. See Downloading software from PLDS on page 30.		
5	Download the appropriate solution template and licenses from PLDS. See Downloading software from PLDS on page 30.		

Table continues...

No.	Task	Notes	✓
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 30 and Verifying the ISO image on a Windows-based computer on page 31.		
7	Write the ISO images to separate DVDs. See Writing the ISO image to DVD or CD on page 32.	 Note: If the software files you are writing on media are less than 680 Mb in size, you can use a CD instead of a DVD.	

Registering the system

About this task

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

Avaya assigns a Solution Element ID (SE ID) and Product ID to each SAL Gateway and managed device that is registered. In 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

Avaya uses 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 60

[SAL Gateway](#) on page 58

[Gateway Configuration field descriptions](#) on page 63

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 pradmin@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 37.

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 **BROKEN LINK:** [Feature Pack installation](#).

! 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 37. • Disable use of proxy servers in the Web browser on the laptop.		

Table continues...

No.	Task	Notes	✓
	See Disabling proxy servers in Microsoft Internet Explorer on page 37 or Disabling proxy servers in Mozilla Firefox on page 38 .		
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 38 or Starting the installation from the server console on page 40 depending on your selection of installation method.		
6	If using the server console to install System Platform, enter the <code>vspmediacheck</code> command and press Enter. The <code>vspmediacheck</code> command verifies that the image on the System Platform DVD is not corrupt. See Starting the installation from the server console on page 40.		
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 38.		
8	Select the required keyboard type. See Selecting the type of keyboard on page 40.		
9	Verify the System Platform server hardware. See Verifying the System Platform server hardware on page 41.		

Table continues...

No.	Task	Notes	✓
10	Verify that the image on the System Platform DVD is not corrupt. See Verifying the System Platform image on the DVD on page 42.		
11	Configure the network settings for the System Domain (Domain-0). See Configuring network settings for System Domain on page 42.		
12	Configure the network settings for the Console Domain. See Configuring network settings for Console Domain on page 45.		
13	Install the Services Virtual Machine (services_vm). See Installing the Services virtual machine on page 47.	! Important: When the Services VM Network Configuration window displays at the beginning of the System Platform installation <i>for the standby server</i> in a System Platform High Availability configuration, clear the Enable Services VM check box to ensure that you install the Services VM in a disabled state. If a failover occurs later during HA system operation, the failover subsystem activates the Services VM on the former standby (now active) server, propagates the current Services VM configuration to that server, and deactivates the Services VM on the former active (now standby) server.	
14	Configure the time zone for the System Platform server. See Configuring the time zone for the System Platform server on page 49.		
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 49		
16	Configure the System Platform passwords.		

Table continues...

No.	Task	Notes	✓
	See Configuring System Platform passwords on page 50.		
17	Verify that System Platform installed correctly. See Verifying installation of on page 53.		
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 103 and BROKEN LINK: Feature Pack installation .		
19	If your NMS uses SNMP v2c, change the SNMP version that is supported on the Services virtual machine. See BROKEN LINK: Configuring SNMP version support on the Services VM .	The Services VM supports SNMP v3.	
20	Configure the SAL gateway for remote access and alarming. See SAL Gateway on page 58.		
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 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 82.		

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 40.

Related Links

[Connecting to the server through the services port](#) on page 54

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 40.

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 42.

- 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 42.

Next steps

- Verify that the System Platform image copied correctly to the DVD. See [Verifying the System Platform image on the DVD](#) on page 42.
- OR
- Configure the network settings for System Domain (Domain-0). See [Configuring network settings for System Domain \(Domain-0\)](#) on page 42

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 40

About this task

After [Selecting the type of keyboard](#) on page 40, 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 42. 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 42

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 42.

Related Links

[Writing the ISO image to DVD or CD](#) on page 32

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 44.

Welcome to Avaya Aura (TM) System Platform

System Domain Network Configuration

Hostname: _____

Primary DNS: _____

Secondary DNS: _____

Physical Devices: eth8

Static IP: _____

Subnet mask: 255.255.255.0

Default gateway IP: _____

☐ IPv6 Enabled:

IPv6 Address: _____

IPv6 Prefix: _____

IPv6 Gateway: _____

☒ Enable IP Forwarding

OK Back

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

2. Perform the following steps to configure the interface that is connected to the customer network:
 - a. Use the `Tab` key to highlight the **Physical Devices** field.
 - b. Complete the **Static IP** field.
 - c. Modify the subnet mask if necessary. The server displays a default value of 255.255.255.0.
3. Complete the **Default gateway IP** field.
4. Use the `Tab` key to highlight the **IPv6 Enabled** field. Press the `Spacebar` to either enable or disable entering IP addresses in IPv6 format.
5. If you have enabled IPv6, fill in the following fields:
 - **IPv6 Address**
 - **IPv6 Prefix**
 - **IPv6 Gateway**

- 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).

- Use the **Tab** key to highlight **OK** and press **Enter** to accept the configuration.
- 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 45.

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, <code>SPDom0.mydomainname.com</code> . Otherwise, just enter the IP address for System Domain, or enter the hostname for System Domain in non-FQDN format. When using a Domain Name System (DNS) server in your network, the System Domain hostname must be FQDN format.
Primary DNS	The primary Domain Name System (DNS) server address.
Secondary DNS	(Optional) The secondary DNS server address.
Physical Devices	This field displays the physical Ethernet interface (NIC) that connects to the customer 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.

Table continues...

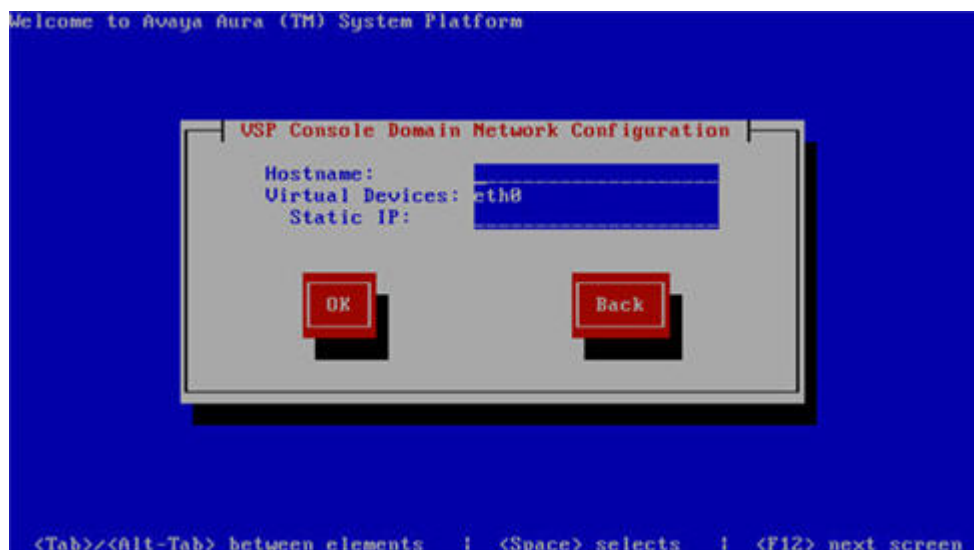
Name	Description
IPv6 Enabled	The indicator to show whether the IP addresses required by System Platform must be IPv6-compliant.
IPv6 Address	The IPv6-compliant IP address of System Domain.
IPv6 Prefix	The IPv6 prefix for IPv6 Address .
IPv6 Gateway	The IP address of the default gateway for IPv6 traffic.
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

- 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 47.

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, <code>SPCdom.mydomainname.com</code> . 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

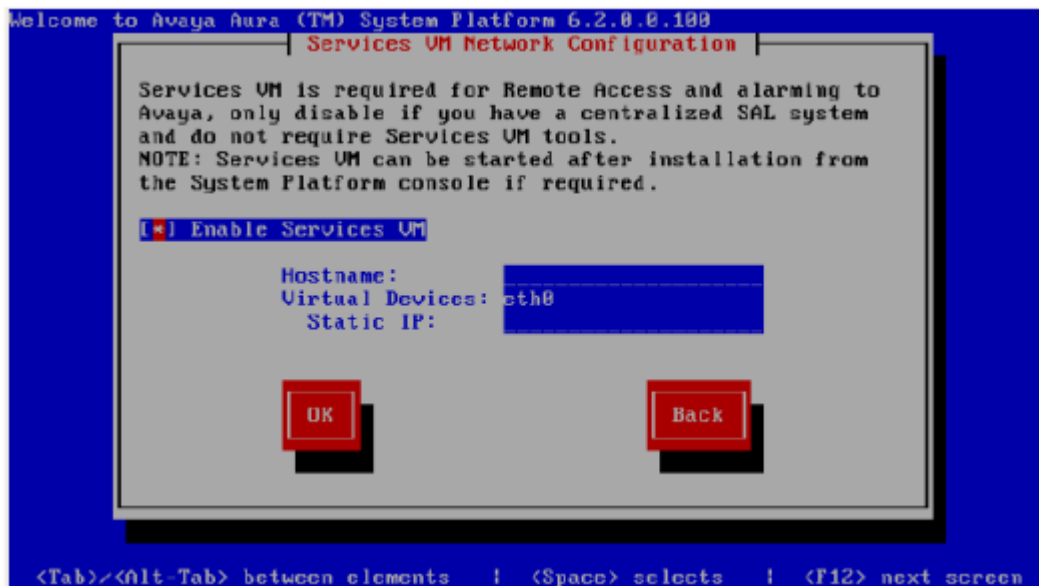
- You have completed the task, “Configuring network settings for Console Domain.”
- If you plan to deploy a standalone SAL Gateway on a server elsewhere in your network, you must download, install, and configure the SAL 2.2 software on that server. For instructions, see the SAL Gateway installation section 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 48.
- 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 49

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 47

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 56.

Next steps

Verify System Platform installation. See [Verifying installation of](#) on page 53.

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.

Table continues...

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

Verifying installation of System Platform

Before you begin

To 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 55.

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 57

[Accessing the System Platform Web Console](#) on page 56

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 37

[Disabling proxy servers in Mozilla Firefox](#) on page 38

[Disabling proxy servers in Microsoft Internet Explorer](#) on page 37

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 Platform Web 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 55.

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 55

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 Platform includes 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 73. 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 74.

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.

Avaya assigns 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 60

[Registering the system](#) on page 28

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 28

[SAL Gateway](#) on page 58

[Registering the system](#) on page 28

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 63.

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 63

[Applying configuration changes](#) on page 70

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 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 <i>Secure Access Link Gateway 1.8 Implementation Guide</i>. 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 62

[Registering the system](#) on page 28

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 64

[Applying configuration changes](#) on page 70

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 64

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 66

[Applying configuration changes](#) on page 70

Core Server field descriptions

Name	Description
Passphrase	Default passphrase is <code>Enterprise-production</code> . 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

Table continues...

Name	Description
	SAL Gateway and the Secure Access Concentrator Core Server.
Primary Core Server	IP Address or the host name of the primary Secure Access Concentrator Core Server. The default value is <code>secure.alarming.avaya.com</code> .
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 66

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 68

[Applying configuration changes](#) on page 70

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 <code>sl1.sal.avaya.com</code> .
Port	The port number of the primary Secure Access Concentrator Remote Server. The default value is <code>443</code> .
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 67

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 69

[Applying configuration changes](#) on page 70

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 <code>public</code> as the Community , as SAL agents support only public as community at present.

Related Links

[Configuring NMS](#) on page 68

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 Gateway 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	

Related Links

[Adding a managed element](#) on page 71

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 72

[Applying configuration changes](#) on page 70

[Managed element worksheet for SAL Gateway](#) on page 70

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 <i>Secure Access Link Gateway 1.8 Implementation Guide</i> . This document is available at http://support.avaya.com .

Table continues...

Name	Description
Inventory collection schedule	Interval in hours at which the SAL Gateway collects inventory information about the managed device.
Monitor health for this device	Check box to enable health monitoring of the managed device by SAL Gateway. SAL Gateway uses heartbeats to monitor health. Heartbeats must be configured on the device.
Generate Health Status missed alarm every	Interval in minutes at which SAL Gateway generates an alarm if it does not receive a heartbeat from the managed device. You must restart the SAL Gateway for the configuration changes to take effect. SAL Gateway starts monitoring heartbeats from the device after the restart and generates alarms if it does not receive a heartbeat within the configured interval.
Suspend health monitoring for this device	Check box to suspend health monitoring for the managed device.
Suspend for	Number of minutes to suspend health monitoring for the managed device. SAL Gateway resumes monitoring the device after the configured time elapses.

Related Links

[Adding a managed element](#) on page 71

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 78.

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 <code>/vsp-template</code> file system in the Console Domain of the System Platform server. SP CD/DVD

Table continues...

Name	Description
	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.
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 System Platform 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 virtual machine: Fast Reboot (FRHA) If Machine Preserving High Availability (MPHA) is selected for

Table continues...

VM Name	VM Description	Protection Mode
		the solution template, the protection mode for all other virtual machines automatically changes to Live Migration.
<code><solution_template_vm></code>	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.

Table continues...

Name	Description
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 87

[Stopping System Platform High Availability](#) on page 88

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 86

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 86

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.

Chapter 5: Installing System Manager

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_6.3.13_r5003336.bin` file.

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_Version_II.tar`
 - `System_Manager_06_03_Post_Deploy.tar`
 - `SystemManager.mf`
 - `SystemManager.ovf`
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**.

You can also download these files individually from the PLDS website.

- The `System_Manager_6.3.13_r5003336.bin` file

When the installation is complete, the web page on PLDS displays the downloads with a check mark.

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.

Installation methods

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

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

Related Links

[Installing the System Manager Release 6.3 template using ISO](#) on page 92

[Installing System Manager using a DVD](#) on page 97

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.



The screenshot shows the 'VFQDN' configuration page. On the left is a sidebar with a 'Configuration' menu and an 'Installation' section containing links for Network Settings, VFQDN, Logins, SNMP, Backup, Summary, and Finish. The main content area is titled 'VFQDN' and contains a table with two columns: 'Virtual Hostname' and 'Virtual Domain'. The 'Virtual Hostname' field is labeled 'System Manager VFQDN' and contains the value 'grsmgr'. The 'Virtual Domain' field contains the value 'platform.avaya.com'. At the bottom of the page are two buttons: 'Previous Step' and 'Next Step'.

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

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



The screenshot shows the 'Logins' configuration page. The sidebar is identical to the previous page. The main content area is titled 'Logins' and has a subtitle 'Non root user for System Manager'. It contains a single text input field labeled 'Non-root User:' with the value 'admin'. At the bottom of the page are two buttons: 'Previous Step' and 'Next Step'.

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.

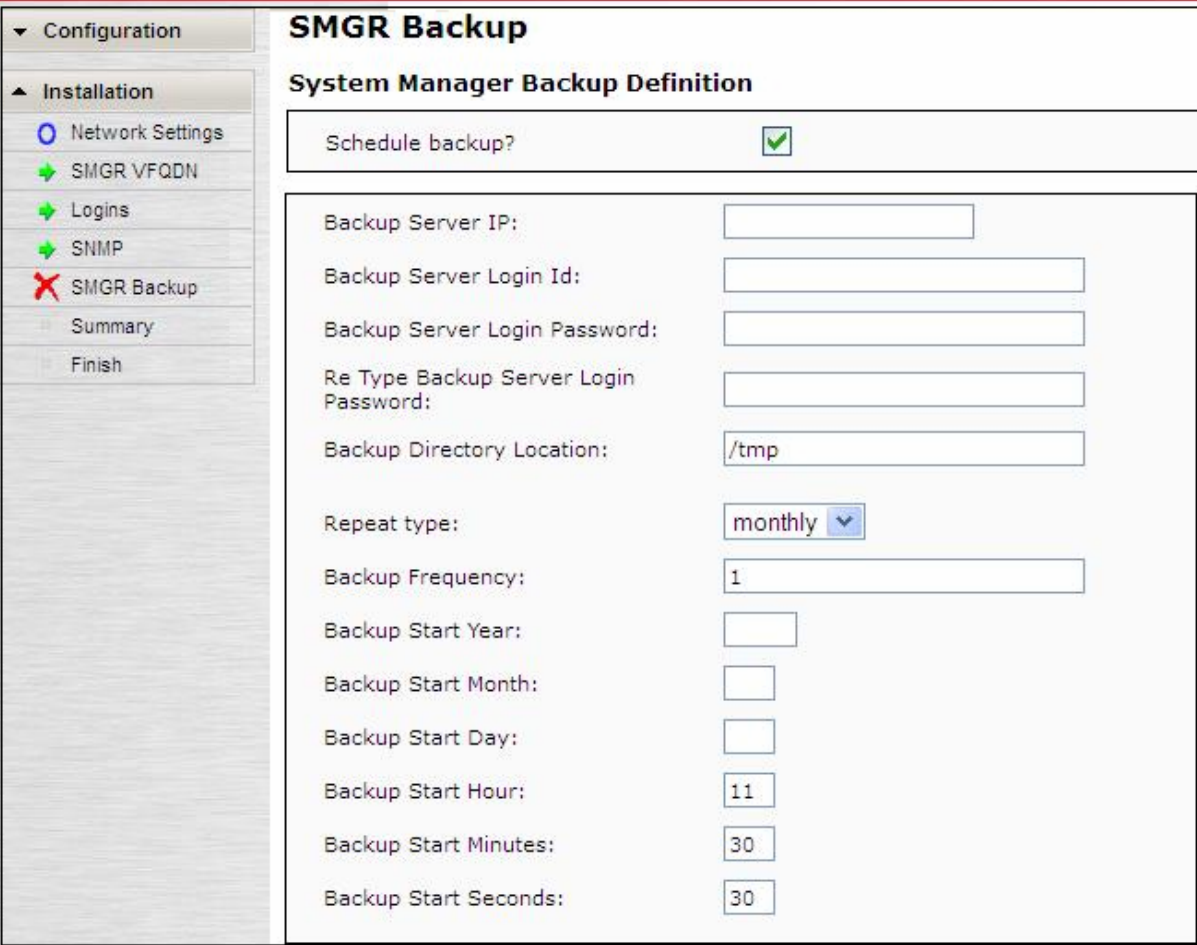
The screenshot shows the 'SNMPv3 Parameters' configuration page. On the left is a navigation pane with a tree structure. Under 'Configuration', 'Installation' is expanded, showing 'Network Settings' (selected with a blue circle), 'SMGR VFQDN' (green plus), 'Logins' (green plus), 'SNMP' (red X), 'SMGR Backup' (red X), 'Summary' (grey square), and 'Finish' (grey square). The main content area is titled 'SNMP' and 'SNMPv3 Parameters'. It contains five input fields: 'User Name Prefix' with the value 'global', 'Authentication Protocol Password' (masked with 10 dots), 'Re-type Authentication Protocol Password' (masked with 10 dots), 'Privacy Protocol Password' (masked with 10 dots), and 'Re-type Privacy Protocol Password' (masked with 10 dots). At the bottom, there are two buttons: 'Previous Step' with a left-pointing red arrow and 'Next Step' with a right-pointing red arrow.

SNMPv3 Parameters	
User Name Prefix	global
Authentication Protocol Password	
Re-type Authentication Protocol Password	
Privacy Protocol Password	
Re-type Privacy Protocol Password	

[Previous Step](#) [Next Step](#)

16. Click **Next Step**.

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



Configuration

- Installation
 - Network Settings
 - SMGR VFQDN
 - Logins
 - SNMP
 - SMGR Backup**
 - Summary
 - Finish

SMGR Backup

System Manager Backup Definition

Schedule backup? ☒

Backup Server IP:

Backup Server Login Id:

Backup Server Login Password:

Re Type Backup Server Login Password:

Backup Directory Location:

Repeat type:

Backup Frequency:

Backup Start Year:

Backup Start Month:

Backup Start Day:

Backup Start Hour:

Backup Start Minutes:

Backup Start Seconds:

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*.

Related Links

[Backup Definition field descriptions](#) on page 107

Installing System Manager using a DVD

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.

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. Select **SP CD/DVD**.
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 **Install**.
9. 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.

10. In the **Domain** field, enter the domain name of the virtual machine.
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.

The screenshot shows the 'VFQDN' configuration page. On the left is a navigation menu with 'Configuration' expanded and 'Installation' selected. Under 'Installation', 'Network Settings' is active, and 'VFQDN' is highlighted with a green plus icon. Other options like 'Logins', 'SNMP', 'Backup', 'Summary', and 'Finish' are listed. The main content area is titled 'VFQDN' and contains a table with two columns: 'Virtual Hostname' and 'Virtual Domain'. The 'System Manager VFQDN' row shows 'grsmgr' in the hostname field and 'platform.avaya.com' in the domain field. At the bottom, there are 'Previous Step' and 'Next Step' navigation links.

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

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

The screenshot shows the 'Logins' configuration page. The left navigation menu is the same as in the previous screenshot, but 'Logins' is now highlighted with a green plus icon. The main content area is titled 'Logins' and 'Non root user for System Manager'. It features a 'Non-root User' field with the value 'admin' entered. At the bottom, there are 'Previous Step' and 'Next Step' navigation links.

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

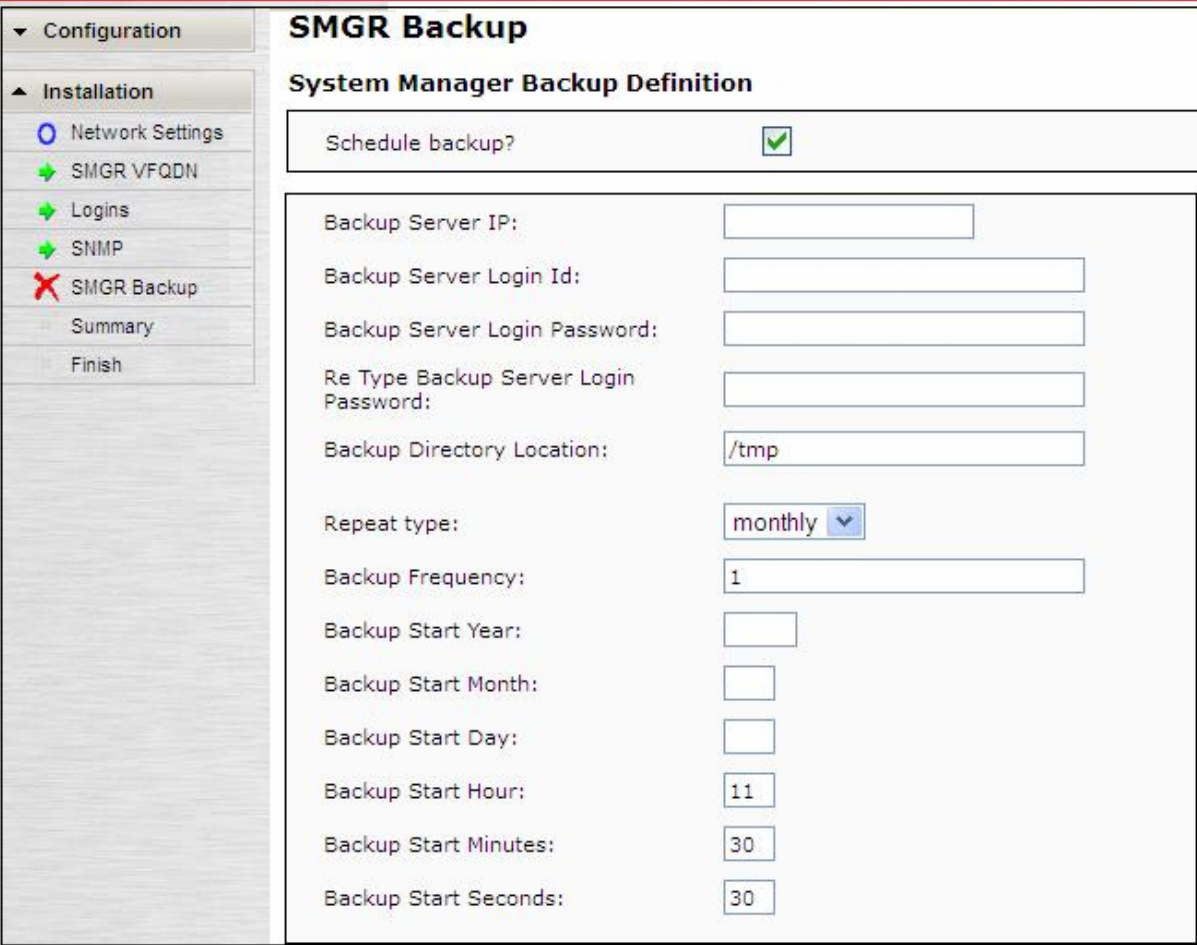
The screenshot shows the 'SNMPv3 Parameters' configuration page. On the left is a navigation pane with a tree structure. Under 'Configuration', 'Installation' is expanded, showing 'Network Settings' (selected with a blue circle), 'SMGR VFQDN' (green plus), 'Logins' (green plus), 'SNMP' (red X), 'SMGR Backup' (red X), 'Summary' (grey square), and 'Finish' (grey square). The main content area is titled 'SNMP' and 'SNMPv3 Parameters'. It contains five input fields: 'User Name Prefix' with the text 'global', 'Authentication Protocol Password' (masked with dots), 'Re-type Authentication Protocol Password' (masked with dots), 'Privacy Protocol Password' (masked with dots), and 'Re-type Privacy Protocol Password' (masked with dots). At the bottom, there are two buttons: 'Previous Step' with a left-pointing red arrow and 'Next Step' with a right-pointing red arrow.

SNMPv3 Parameters	
User Name Prefix	global
Authentication Protocol Password	
Re-type Authentication Protocol Password	
Privacy Protocol Password	
Re-type Privacy Protocol Password	

[Previous Step](#) [Next Step](#)

14. Click **Next Step**.

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



Configuration

- Installation
 - Network Settings
 - SMGR VFQDN
 - Logins
 - SNMP
 - SMGR Backup**
 - Summary
 - Finish

SMGR Backup

System Manager Backup Definition

Schedule backup? ☒

Backup Server IP:

Backup Server Login Id:

Backup Server Login Password:

Re Type Backup Server Login Password:

Backup Directory Location:

Repeat type:

Backup Frequency:

Backup Start Year:

Backup Start Month:

Backup Start Day:

Backup Start Hour:

Backup Start Minutes:

Backup Start Seconds:

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 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.

Related Links

[Backup Definition field descriptions](#) on page 107

Installing the System Manager Release 6.3.13 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.13_r5003336.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_6.3.13_r5003336.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

[Downloading patches](#) on page 102

[Installing patches](#) on page 103

Default credentials

Accessing the System Manager command line interface

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

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

Accessing the System Manager common Web console

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

Using the System Manager Trap Listener service

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

Note:

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

After you change the Trap Listener settings, as an administrator, create a new SNMP Target profile for System Manager IP address, and a new SNMPv3 user profile for System Manager. The values in the profiles must match the values in the Trap Listener settings. You must also attach the SMGR SNMPv3 user profile to the SMGR Target profile, and then attach the target profile to all the Serviceability Agents. For information on creating SNMP User and Target profiles and attaching the Target profiles to Serviceability Agents, see “Managing Serviceability Agents” in *Administering Avaya Aura® System Manager*.

Installing and committing the patches

Downloading patches

Procedure

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

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.

Configuring a proxy

About this task

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

Procedure

1. Click **Server Management > Patch Management**.
2. Click **Upload/Download**.

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

Committing patches

Before you begin

You have completed the following tasks using the Web Console:

- [Downloading patches](#) on page 102 (finding and downloading the particular patch you must install)
- [Configuring a proxy](#) on page 103 (if the patches are located in a different server)
- [Installing patches](#) on page 103 (for the particular patch you must install)

About this task

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

Note:

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

Procedure

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

The Server Management Patch List page displays.

3. Click the patch that you must commit.

The Web Console displays the Server Management Patch Detail page.

4. Click **Commit**.

The Server Management Patch Detail page displays an in-progress message, for example: Patch <patch_id> is being committed. Please wait.... The Patch Detail page then displays a completion message, for example: Patch <patch_id> has been successfully committed, or, Failed to commit patch.

Rolling back patches

About this task

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

 Note:

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

Procedure

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

The Server Management Patch List page displays.

3. Click the patch that you want to roll back.

The Web Console displays the Server Management Patch Detail page.

4. Click **Rollback**.

The Server Management Patch Detail page displays an in-progress message, for example: Patch <patch_id> is being rolled back. Please wait.... The Patch Detail page then displays a completion message, for example: Patch <patch_id> has been successfully rolled back, **or**, Failed to roll back patch.

Chapter 6: Postinstallation verification

Verifying the installation of System Manager

You must perform the following verification procedure after you install System Manager Release 6.3.13 and configure System Manager.

Before you begin

Log on to the System Manager web console by using admin credentials.

Procedure

1. On the web browser, type `https:// <fully qualified domain name of System Manager>`.

The system must display the System Manager web console.

2. On the upper-right corner, click  and **About**.

The system displays the About SMGR window with the build details.

3. Verify the version number of System Manager.

Chapter 7: 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.

Backup Definition field descriptions

Use the Backup Definition page to schedule remote backup during the System Manager installation.

 Note:

You can skip the configuration of the backup definition parameters to schedule the backup jobs later.

If you set the **Backup Start Month** field to 5, **Backup Start Day** field to 24, and **Repeat Type** field to Weekly, the system executes the backup job every Friday if May 24th is a Friday.

Name	Description
Schedule Backup?	Use to skip the backup definition if you do not want the system to schedule backup jobs.
Backup Server IP	The IP address of the backup server.
Backup Server Login Id	The login ID of the backup server through CLI.
Backup Server Login Password	The password to log in to the backup server through CLI.
Re Type Backup Server Login Password	The password that you re-enter to log in to the backup server through CLI.

Table continues...

Name	Description
Backup Directory Location	The location of the backup server.
Repeat Type	The type of the backup. The possible values are: • Hourly • Daily • Weekly • Monthly
Backup Frequency	The frequency of the backup taken for the selected backup type.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be six hours greater than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

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*.

Chapter 8: Removing the System Manager template

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.

Index

A

active server	
manually changing to standby	88
admin password	52

B

Backup Definition field descriptions	107
bin file	
System Manager	101
browser	
System Platform support	56
Browser support	12

C

checking RAID Controller Battery state	91
checklist	
installation	33
preinstallation	27
checklist, installation, ...	13
command line	
accessing Console Domain	58
accessing System Domain	57
configuration	
System Manager	107
Configure HA	
field descriptions	84
console domain	
configuring network settings	45
Console Domain	
accessing command line	58
Console Domain Network Configuration screen	
configuring	45
courses	9
craft password	52
cust password	52

D

date	
configuring	49
Date/Time and NTP setup screen	
configuring	49
default credentials	101
Deploy System Manager	11
documentation	8
downloading software	30
downloading System Manager from Avaya Support website	
.....	90
downloading System Manager from PLDS	90

DVD

requirements	31
writing ISO image	32

F

field descriptions	
Backup Definition	107
Managed Element page	72
Proxy Server page	64
Firefox	12
disabling proxy servers	38
System Platform support	56

G

Gateway Configuration	
field descriptions	63
Geographic Redundancy	
prerequisites	25

H

hardware and software prerequisites on the primary and	
secondary servers	25
hardware requirements	11
High Availability	
and template configuration	79
common prerequisites	80
configuring local	82
FRHA/LMHA/MPHA prerequisites	81
manually interchanging node roles	88
prerequisites	80
removing configuration	89
start/stop	86
starting	87
stopping	88
High Availability;	
System Platform	79

I

install	
System Manager	92
installation	
checklist	33
using laptop	38
using server console	40
worksheet	15
installation checklist	13
installation methods	92
installing System Manager; DVD	97

installing System Manager template	92	P	
installing System Manager through DVD	97	passwords	
install System Manager bin file	101	configuring in System Platform	50
Internet Explorer	12	default	50
disabling proxy servers	37	Passwords screen	
System Platform support	56	configuring	50
IP forwarding		field descriptions	52
disabling	55	patches	
enabling	55	committing	104
IP settings		downloading	102
configuring on laptop	37	installing	103
ISO image		rolling back	105
verifying on DVD	42	perform the System Manager tests	106
verifying on Linux-based computer	30	PLDS	29
verifying on Windows-based computer	31	downloading software	30
writing to DVD or CD	32	post install configuration	107
K		preinstallation checklist	27
keyboard		prerequisites	25
selecting type	40	Product ID	
Keyboard Type screen	40	changing for System Platform	60
L		product registration	60
laptop		proxy	
configuring to connect to server	37	configuring	103
connecting to server	54	configuring for System Platform	78
using to install System Platform	38	proxy server	
ldap password	52	configuring for SAL Gateway	64
legal notice		Proxy Server page	
M		field descriptions	64
managed element		proxy servers	
adding in SAL Gateway	71	disabling in Firefox	38
worksheet for SAL Gateway	70	disabling in Internet Explorer	37
Managed Element page		R	
field descriptions	72	RAID Controller Battery state	91
N		registering	29
Network Management Systems Destinations	108	registration	
Network Management Systems page		of system	28
field descriptions	69	related documentation	8
network settings		remote server	
configuring for console domain	45	configuring	67
configuring for system domain (domain-0)	42	field descriptions	68
NMS		Remote Server	
configuring for SAL Gateway	68	field descriptions	68
field descriptions	69	remove System Manager template	110
NMS destinations	108	Removing the HA configuration	89
NTP server		requirements	
configuring in System Platform	49	hardware	11
		server	11
		root password	52
		S	
		SAL Core Server	
		configuring	66
		field descriptions	66

SAL Gateway	58	install	11
adding a managed element	71	System manager from Avaya Support website	
applying configuration changes	70	download	90
browser requirements	61	System manager from PLDS	
configuring	62	download	90
configuring a proxy server	64	System Manager information worksheet	14
configuring Concentrator Core Server	66	System Manager install	11
configuring network management system	68	System Manager installation	
configuring NMS servers	69	verify	106
configuring remote server	67, 68	System Manager patch	101
configuring SAL Core Server	66	System Manager template	
disabling	74	install	92
managing service control and status	69	remove	110
prerequisites for configuration	60	System Platform	
registering	28	High Availability	
starting user interface	61	field descriptions	84
worksheet for managed elements	70	High Availability field descriptions	84
Search Local and Remote Template page		registering	28
field descriptions	77	System Platform Web Console	
Secure Access Gateway Server	58	accessing	56
server			
connecting laptop	54	T	
hardware requirements	33	Telnet	
manually interchanging node roles	88	opening session from laptop to System Platform server	
Server			38
hardware checks	41	template	
server console		and High Availability Failover	79
using to install System Platform	40	installing	74
server requirements	11	remove	110
services port		time	
accessing System Platform through	55	configuring	49
Services virtual machine (VM)		time zone	
installing	47	configuring	49
Services VM		Time Zone Selection screen	
network configuration		configuring	49
field descriptions	49	training	9
SNMP trap receivers		V	
adding	73	verify	
SNMP traps	108	System Manager installation	106
solution template		verifying	
and High Availability Failover	79	RAID Controller Battery state	91
installing	74	version	
registering applications	28	Firefox	12
Status		Internet Explorer	12
SAL Gateway service	69	videos	9
support	10	Virtual Machine Management page	
browser	12	field descriptions	77
System Domain		VSP Console Domain Network Configuration screen	
accessing command line	57	configuring	45
system domain (domain-0)		field descriptions	46
configuring network settings	42	vspmediacheck	42
System Domain Network Configuration screen			
field descriptions	44		
System Manager			
administrative task	107		
configuration	107		
deploy	11		

W

warranty	10
Web browser	
System Platform support	56
Web Console	
accessing	56
worksheet	
installation	15
SAL Gateway managed elements	70
worksheet, System Manager information	14