Installing and Configuring Avaya Aura® System Platform

Release 6.3
Issue 5
June 2015

Notices

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, 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 types

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.

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

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

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.

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 products, 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 Aura is a registered trademark of Avaya.

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

PuTTY is copyright 1997-2009 Simon Tatham.

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: System Platform installation overview

Introduction

This book covers installation of the latest ISO release of System Platform software, and, when appropriate, any Feature Pack (FP) software for that release.

To upgrade an existing version of System Platform to the latest version, see the platform upgrade topics in your Avaya Aura® solution documentation.

System Platform 6.3.7 is an ISO image.

Related Links

Feature packs on page 46

Installation process overview

Installation of System Platform consists of the following tasks:

Procedure

1. Install the server hardware.
2. Connect the server to the customer network.

   This step is for best practice, although it is possible to install the System Platform software without an initial connection to the customer network.
3. Connect the two servers if using a System Platform High Availability option.

   Note:

   Cable interconnection requirements depend typically on the configured System Platform HA mode, Ethernet specifications, restrictions on the use of layer-2 switches to extend maximum cable distance, and in a small percentage of site-specific scenarios, ambient electrical and signal noise (RFI) affecting the choice of Ethernet cable types (for example, CAT5E, CAT5A, CAT6A). For more details, see topics associated with System Platform HA cable requirements in your Avaya Solution documentation.

4. Install the System Platform software, service packs, and any required Feature Pack on the server.If using the High Availability Failover option, also install the System Platform software, service packs, and any required Feature pack on the standby server.
5. Configure the Secure Access Link (SAL) Gateway for remote support and alarming. You can use the SAL Gateway that is included with System Platform or installed on a standalone SAL Gateway.

   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.
6. Install the solution template.

   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.
7. Configure High Availability if using that option.

Related Links

SAL Gateway on page 60

Chapter 2: Installation requirements for System Platform

What Avaya provides

Avaya provides the following items for installing System Platform:

- One or two servers. One is for a standard configuration, and two are for High Availability Failover configuration.
- Slide rails to mount the servers in a standard 19-inch, 4-post rack that have square holes.
- System Platform installation software.
- Other hardware as ordered, such as an uninterruptible power supply (UPS). UPS is a required component.
- Product registration form. The form is available on http://support.avaya.com. Click **More Resources** > **Avaya Equipment Registration**. Under **Non-Regional (Product) Specific Documentation**, click **Universal Install/SAL Product Registration Request Form**. For more information, see Registering the system on page 13.

Note:

Avaya provides the System Platform installation software. The customer must either buy the System Platform DVD or download the ISO image and write that image to a DVD.

What customer provides

The customer must provide the following items for installing System Platform.

- Standard equipment rack correctly installed and solidly secured.
- USB keyboard, USB mouse, and VGA monitor or laptop with an Ethernet crossover cable.

  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.

The supported keyboard types are sg-latin1, sk-qwerty, slovene, sv-latin1, trq, uautf, uk, and us.

- Gigabit-certified Ethernet cable for High Availability Failover.
- DVDs written with the software for installing.
- A computer that can route to the System Platform server and has a supported version of Internet Explorer or Firefox installed. Internet Explorer versions 7 through 9 are supported. Firefox versions 3.6 through 19 are supported.
- Filled-out worksheets with the system and network information needed for installation and configuration.
- (Optional) Electronic preinstallation worksheet (EPW) and Avaya Bulk Import Tool (ABIT) files.
- Access to the customer network.
- (Optional) VPN Gateway for providing remote access to Avaya Partners.

Note:

Avaya Partners must arrange for their own IP-based connectivity (for example, B2B VPN) to provide remote services. Modem connectivity is unsupported.

Note:

Secure Access Link (SAL) Gateway is required for remote service and alarming. System Platformincludes an embedded SALGateway, or you can use a standalone SAL Gateway.

Chapter 3: Preinstallation tasks

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 13.	❗ **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 112.		
3	Register for PLDS unless you have already registered. See Registering for PLDS on page 14.		
4	Download the System Platform installer ISO image file from PLDS. See Downloading software from PLDS on page 15.		
5	Download the appropriate solution template and licenses from PLDS. See Downloading software from PLDS on page 15.		

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 15 and Verifying the ISO image on a Windows-based computer on page 16.		
7	Write the ISO images to separate DVDs. See Writing the ISO image to DVD or CD on page 16.	**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

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

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

Note:

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

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

Procedure

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

2. Complete the Universal Install Product Registration page and submit it at least three weeks before the planned installation date.

   Provide the following:

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

   Avayauses this information to register your system. When processing of the registration request is complete, Avaya sends you an email with an ART install script attached. This script includes instructions for installation and the SE IDs and Product IDs that you must enter in SAL Gateway to add managed devices.

3. Complete and submit the Universal Install Alarm Registration page after the installation is complete.

Related Links

Configuration prerequisites on page 61
SAL Gateway on page 60
Gateway Configuration field descriptions on page 64

Registering for PLDS

Procedure

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

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

2. Log in to SSO with your SSO ID and password.

   The PLDS registration page is displayed.

3. If you are registering:

   - as an Avaya Partner, enter the Partner Link ID. If you do not know your Partner Link ID, send an email to prmadmin@avaya.com.
   - as a customer, enter one of the following:
     - Company Sold-To
     - Ship-To number
     - License authorization code (LAC)

4. Click **Submit**.

   Avaya will send you the PLDS access confirmation within one business day.

Downloading software from PLDS

✱ **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

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

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

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.

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.

Electronic preinstallation worksheet

An EPW file

An Electronic Pre-installation Worksheet (EPW) file plays an important role in installing an Avaya Aura® solution template on System Platform. Creating an EPW file helps you set up and save those parameters required during the template installation ahead of time. When installing the template, you upload the EPW file and let the installation happen with minimal intervention. For example, get the required IP addresses before the installation and enter those IP addresses when you create the EPW file. Then when you upload the EPW file at the customer site, the IP addresses are automatically populated in the installation wizard.

To reinstall a template, reuse the original EPW with the correct specifications.

To create the EPW file, use a standalone version of the installation wizard that you install on a Windows-based computer. The standalone installation wizard displays the same configuration pages that appear in the installation wizard. The configuration pages displayed by the standalone installation wizard depend on which template you install.

Creating an electronic preinstallation worksheet

You must have the zip file for the standalone installation wizard downloaded from PLDS and installed on your computer.

To create an electronic preinstallation worksheet (EPW), you use a standalone installation wizard. The standalone installation wizard is the same as the installation wizard that launches as part of the template installation. By downloading, installing, and filling out the fields in the standalone installation wizard file ahead of time, you save time during the template installation. The standalone installation wizard installs only on a Windows-based computer.

Procedure

1. Unzip the standalone installation wizard file, and extract the file to a location on your computer.

2. Find the setup_wizard.exe file and click it to begin the setup.
3. Click through the Setup screens to complete the installation.

   The installation creates a shortcut link within the **Start** > **Programs** menu.
4. To begin the standalone installation wizard, select **Start** > **Programs** > ***PreinstallWizardname*** > `Run` ***PreinstallWizardname***, where *PreinstallWizardname* is the name of the standalone installation wizard for the template, for example, SP Pre-installation Wizard.

   The standalone installation wizard opens in your default browser.
5. On the Load Files page, select the appropriate template, and then click **Next Step**.
6. Complete the fields on the rest of the screens. Click **Next Step** to move from screen to screen.
7. On the Save page, read the warning text, and then click **Accept**.
8. Click **Save EPW file**, and save the file to a location on your computer.

   Give the file a unique name that identifies the template.

Chapter 4: 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 23.

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 6.3.7, the Services Virtual Machine (VM), and SAL Gateway registration and configuration.

Important:

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

No.	Task	Notes	✔
1	If you are installing System Platform from a laptop, perform the following tasks: • Ensure that a Telnet and Secure Shell application are installed on the laptop. Avaya supports use of the open source Telnet/SSH client application PuTTy. • Configure the IP settings of the laptop for direct connection to the server. See Configuring the laptop for direct connection to the server on page 23. • Disable use of proxy servers in the Web browser on the laptop. See Disabling proxy servers in Microsoft Internet Explorer on page 24 or Disabling proxy servers in Mozilla Firefox on page 24 .		
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.		

Table continues…

No.	Task	Notes	✔
	See Starting the installation from your laptop on page 25 or Starting the installation from the server console on page 26 depending on your selection of installation method.		
6	If using the server console to install System Platform, enter the `vspmediacheck` command and press **Enter**. The `vspmediacheck` command verifies that the image on the System Platform DVD is not corrupt. See Starting the installation from the server console on page 26.		
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 25.		
8	Select the required keyboard type. See Selecting the type of keyboard on page 27.		
9	Verify the System Platform server hardware. See Verifying the System Platform server hardware on page 27.		
10	Verify that the image on the System Platform DVD is not corrupt. See Verifying the System Platform image on the DVD on page 28.		
11	Configure the network settings for the System Domain (Domain-0). See Configuring network settings for System Domain on page 29.		
12	Configure the network settings for the Console Domain. See Configuring network settings for Console Domain on page 32.		
13	Install the Services Virtual Machine (services_vm). See Installing the Services virtual machine on page 33.	**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	

Table continues…

No.	Task	Notes	✔
		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 36.		
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 36		
16	Configure the System Platform passwords. See Configuring System Platform passwords on page 37.		
17	Verify that System Platform installed correctly. See Verifying installation of on page 40.		
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 50 and Feature Pack installation on page 47.		
19	If your NMS uses SNMP v2c, change the SNMP version that is supported on the Services virtual machine. See Configuring SNMP version support on the Services VM on page 58.	The Services VM supports SNMP v3.	
20	Configure the SAL gateway for remote access and alarming. See SAL Gateway on page 60.		

Table continues…

No.	Task	Notes	✔
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 99.		

Connecting your laptop to the server

Configuring the laptop for direct connection to the server

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

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

- 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.

Select the required keyboard type. See Selecting the type of keyboard on page 27.

Related Links

Connecting to the server through the services port on page 41

Starting the installation from the server console

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.

Select the required keyboard type. See Selecting the type of keyboard on page 27.

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 28.

   - 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 29.

- Verify that the System Platform image copied correctly to the DVD. See Verifying the System Platform image on the DVD on page 28.

  OR

- Configure the network settings for System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 29

Verifying the System Platform server hardware

- You are performing a new installation of the System Platform software.

- You have completed the task, Selecting the type of keyboard on page 27

After Selecting the type of keyboard on page 27, 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 28. 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.

If the server hardware check passed, continue with Verifying the System Platform image on the DVD on page 28

Verifying the System Platform image on the DVD

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.

Configure the network settings for System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 29.

Related Links

Writing the ISO image to DVD or CD on page 16

Configuring network settings for System Domain

Procedure

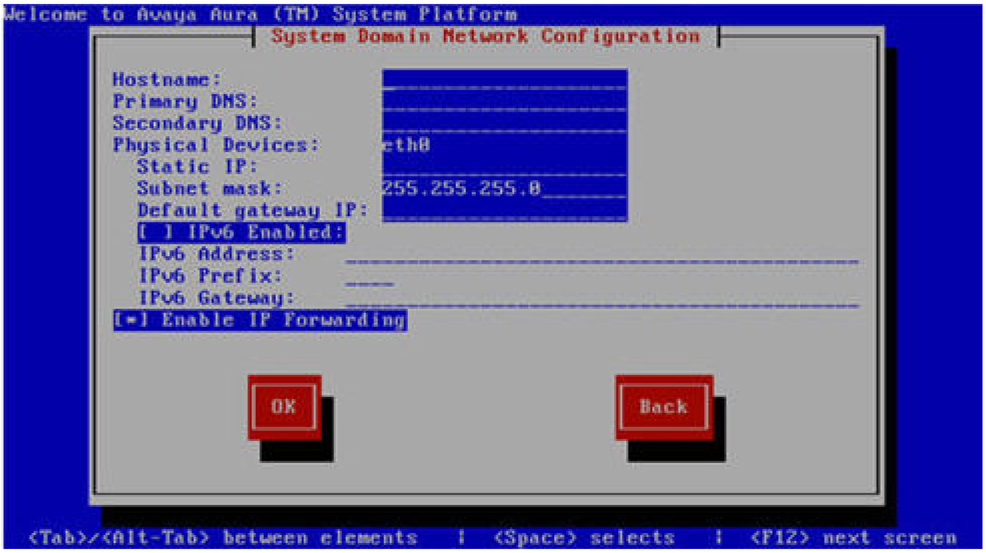
1. On the System Domain Network Configuration screen, complete the following fields:

   - **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 31.



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

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

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

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

    Note:

    IP forwarding is enabled by default and is denoted by an asterisk (* character).
7. Use the `Tab` key to highlight **OK** and press **Enter** to accept the configuration.
8. If IP forwarding is enabled, a confirmation message displays. Use the `Tab` key to highlight **OK** and press **Enter**.

    The system displays the System Platform Console Domain Network Configuration screen.

Configure network settings for Console Domain. See Configuring network settings for Console Domain on page 32.

System Domain Network Configuration field descriptions

Name	Description
Hostname	Depending on requirements of your solution template, you might need to enter the host name for System Domain as a fully qualified domain name (FQDN), for example, `SPDom0.mydomainname.com`. Otherwise, just enter the IP address for System Domain, or enter the hostname for System Domain in non-FQDN format. When using a Domain Name System (DNS) server in your network, the System Domain hostname must be FQDN format.
Primary DNS	The primary Domain Name System (DNS) server address.
Secondary DNS	(Optional) The secondary DNS server address.
Physical Devices	This field displays the physical Ethernet interface (NIC) that connects to the customer network. You must configure this interface for IP. The specific Ethernet interface number depends on the server model being used.
Static IP	The static IP address for the Ethernet interface that connects to the customer network.
Subnet Mask	The subnet mask for the Ethernet interface that connects to the customer network.
Default gateway IP	The default gateway IP address. This default gateway IP address will be used for all the virtual machines if you do not specify gateway IP addresses for them.
IPv6 Enabled	The indicator to show whether the IP addresses required by System Platform must be IPv6-compliant.
IPv6 Address	The IPv6-compliant IP address of System Domain.
IPv6 Prefix	The IPv6 prefix for **IPv6 Address**.
IPv6 Gateway	The IP address of the default gateway for IPv6 traffic.
Enable IP Forwarding	The indicator to show whether IP forwarding is enabled. An asterisk on the left of the field denotes that IP forwarding is enabled.

Table continues…

Name	Description
	IP forwarding enables access through the services port to virtual machines on System Platform, including System Domain and Console Domain. IP forwarding must be enabled for both SSH and Web Console access.

Configuring network settings for Console Domain

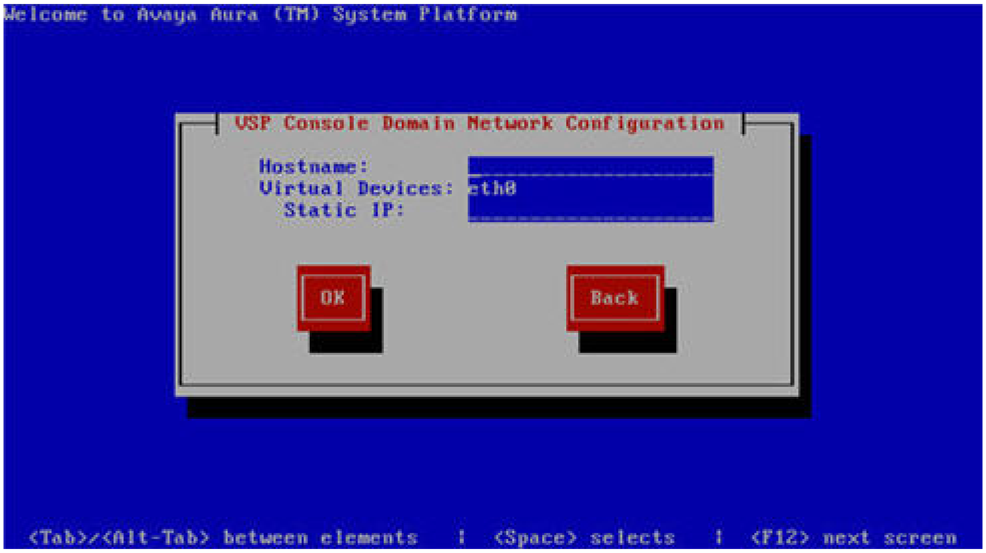
Procedure

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

   - **Hostname**.

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

   - **Static IP**



```
Welcome to Avaya Aura (TM) System Platform

VSP Console Domain Network Configuration

Hostname:
Virtual Devices: eth0
  Static IP:
```

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

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

Install and configure the Services Virtual Machine. See Installing the Services virtual machine on page 33.

System Platform Console Domain Network Configuration field descriptions

Name	Description
Hostname	Depending on requirements of your solution template, you may need to enter the host name for Console Domain as a fully qualified domain name (FQDN), for example, `SPCdom.mydomainname.com`. Otherwise, just enter the IP address for Console Domain or enter the hostname for Console Domain in non-FQDN format.
Static IP	The IP address for the Console Domain. **Note:** The Console Domain does not have a physical interface. It has a virtual interface that uses the physical interface in System Domain (Domain-0). Because System Domain acts like a bridge, the IP address that you enter here must be a valid IP address. Further, the Console Domain must be on the same network as System Domain (Domain-0).
Virtual Devices	The virtual device (port) assigned to the Console Domain (Cdom) virtual machine. Default value (eth0) automatically assigned. No user input necessary.

Installing the Services virtual machine

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

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

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

Important:

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

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

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

- 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.

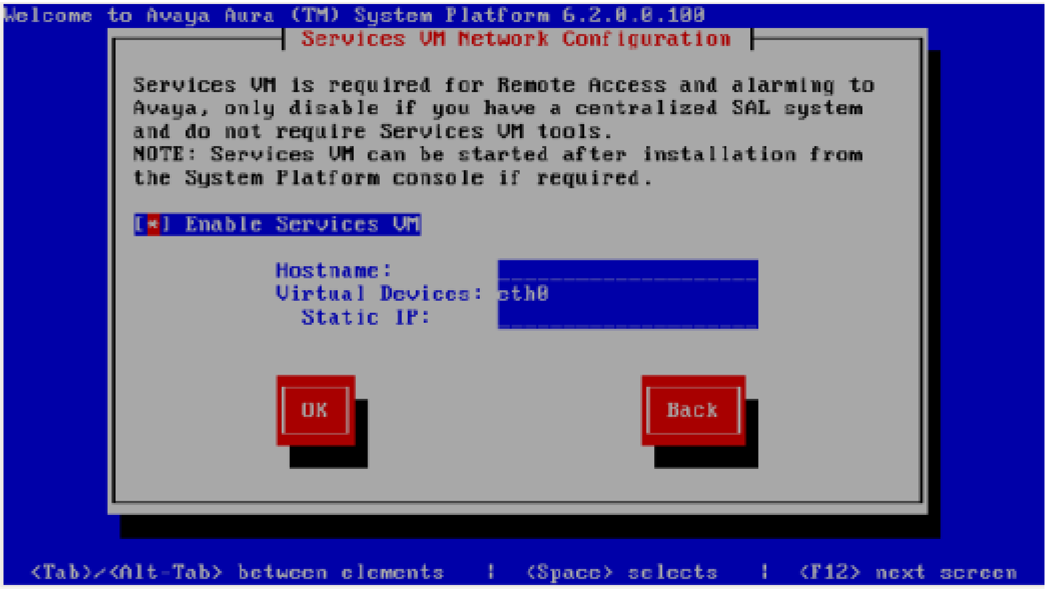
Use this procedure to install the Services VM in an enabled or disabled state, when the Services VM Network Configuration window displays during System Platform installation .

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 35.

   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.



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

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

   [*] Enable Services VM

              Hostname:
              Virtual Devices: eth0
                Static IP:

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

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

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

4. Click **OK**.

   The Time Zone Selection screen is displayed.

Configure the time zone for the server.

Related Links

Services VM Network Configuration field descriptions on page 35

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.

Table continues…

Name	Description
	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 33

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.

Configure date and time for the server.

Configuring the date and time for the System Platform server

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.

Configure System Platform passwords.

Configuring System Platform passwords

Configure the date and time for the System Platform server.

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

Table continues…

Login	Default password	Capability
		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.

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 43.

Verify System Platform installation. See Verifying installation of on page 40.

Passwords field descriptions

Note:

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

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

Name	Description
root Password	The password for the root login.
admin Password	The password for the admin login.
cust Password	The password for the cust login. The cust login is for audit purposes. It has read-only access to the Web Console, except for changes to its password, and no command line access.
ldap Password	The password for the ldap login. System Platform uses a local LDAP directory to store login and password details. Use this login and 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

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 42.

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 43
[Accessing the System Platform Web Console](#) on page 43

Accessing System Platform

Connecting to the server through the services port

- 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 23
Disabling proxy servers in Mozilla Firefox on page 24
Disabling proxy servers in Microsoft Internet Explorer on page 24

Enabling IP forwarding to access System Platform through the services port

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

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

Note:

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

Procedure

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

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

Browser support for System Platform Web Console

The System PlatformWeb Console supports the following Web browsers:

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

Accessing the System Platform Web Console

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 42.

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 42

Accessing the command line for System Domain

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

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.

Chapter 5: Installing Feature Pack software on System Platform

Feature packs

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

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

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

Guidelines for RPM-based feature packs

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

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

Guidelines for ISO-based feature packs

For any ISO-based System Platformfeature pack, only the following guideline applies:

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

Feature Pack installation process

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

1. Upgrade System Platform from version 6.0 to version 6.2.1.
2. Install RPM-based Feature Pack 1 for System Platform 6.2.1. This step brings System Platform to version 6.2.2.
3. Upgrade Communication Manager from version 6.0 to version 6.2.

4. Install Service Pack 4 for Communication Manager 6.2.

High availability configurations

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

Feature Pack installation

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

RPM-based feature packs

For RPM-based feature packs (for example, Feature Pack 3, System Platform 6.3.4), see Patch management on page 47.

ISO-based feature packs

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

Managing patches

Patch management

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

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

Patch commit and rollback

System Platform **Patch Management** features make it possible for you to install, commit, roll back (undo), or remove patches. The manual rollback feature allows you to test a patch before committing it to the system. The automatic rollback feature makes it possible for the system to autonomously recover from problems resulting from patch installation, or from an administrative lockout after installing a patch remotely over the Secure Access Link.

On the Server Management Patch Detail page, a field labeled **rollbackable** with values of `Yes` or `No` indicates whether you can roll back an installed patch. (You can also **Remove** the patch.)

You can also install, commit, or remove RPM (*.rpm) patches on either the System Platform or an installed Avaya Aura® solution template.

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.

Patch commit and rollback on System Platform

Patch rollback on System Platform applies only to CentOS kernel updates. These are patches applied to the CentOS kernel for System Platform.

Important:

Install kernel updates only during a planned downtime for system maintenance.

The following conditions apply to System Platform patch Commit and Rollback operations:

- If you install a CentOS kernel patch on the System Platform, the platform restarts, also logging you out of the Web Console. If you log on to the Web Console within 4 hours, the system automatically commits the kernel patch at that time. If you installed the patch with communication over the Secure Access Link (SAL), but cannot log on to the Web Console, the system automatically rolls back the kernel patch after 4 hours, so that you can get to the Web Console. After automatic rollback of a kernel patch, System Platform restarts from the kernel version that was installed before you installed the latest patch.
- If you perform one or more operations before committing or rolling back a patch, those operations are implemented and visible on the system. If you roll back a patch, any operations performed before the rollback are not implemented or visible on the system.

  If you perform operations locally during a patch installation, but neither **Commit** nor **Rollback** the patch within 4 hours, then System Platform automatically rolls back and restarts using the previous most recent System Platform version.

  If you perform one or more operations related to template functionality and must undo those operations after committing or rolling back the patch, use the Web Console to manually roll back the template-related changes. Rolling back a patch does not automatically roll back your template-related changes. Changes that you made before committing a patch are not implemented or visible on the system.
- If you install and commit a CentOS kernel patch on the System Platform, but the Domain-0 virtual machine fails to open because of a kernel panic or other condition of similar severity, then System Platform rolls back automatically to the patch level installed before you installed the new patch.
- If you install any other type of patch on System Platform, you can effectively roll back (undo) effects of the patch by using the Web Console to remove it from the system. (See Removing patches on page 53.)

Patch commit and rollback on a Solution Template VM

You can only roll back a solution template patch if it has a **rollbackable** value of `Yes` on the Patch Detail page.

Important:

> Installing or rolling back a patch on the solution template VM will cause the VM to restart. Install or roll back a patch to the template VM only during planned downtime for system maintenance. Patch rollback usually requires several minutes of system downtime. *Committing* a patch does not cause the template VM to restart.

When you finish installing a rollbackable patch on the solution template Virtual Machine (VM), the Web Console displays the Server Management Patch Detail page, where you can click either **Commit** or **Rollback**, as appropriate.

Rollbackable solution template patches do not have a timer for automatic rollback. You can perform the rollback manually or remove the patch.

You can only install or remove solution template VM patches that have a rollbackable value of `No` on the Patch Detail page.

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.

Related Links

Search Local and Remote Patch field descriptions on page 53

Configuring a proxy

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.

Related Links

Search Local and Remote Patch field descriptions on page 53
Downloading patches on page 49

Installing patches

- 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.

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**.

Commit the patch.

Related Links

Patch List field descriptions on page 55
Patch Detail field descriptions on page 56
Downloading patches on page 49

Installing System Platform patches on High Availability systems

Before downloading any patch, be sure to check its description in the Release Notes. When indicated by the patch description, you must install patches on both the primary and secondary servers independently. The primary server does not automatically replicate patches to the secondary/standby server.

See the separate procedures for stopping, removing, and starting System Platform High Availability as needed during this procedure.

Procedure

1. Log in to the Web Console of the server chosen to be the preferred node.
2. Click **Server Management** > **High Availability**.
3. Click **Stop HA** and confirm the displayed warning.
4. If the server restarts after stopping HA, log on to the Web Console of the preferred node and **Remove HA**.
5. Apply patches in the required sequence to the preferred node.
6. Log on to the Web Console of the standby node.
7. Apply the same patches that were applied to the preferred node.

Related Links

Starting System Platform High Availability on page 104
Stopping System Platform High Availability on page 105
Removing the High Availability configuration on page 106

Committing patches

You have completed the following tasks using the Web Console:

- Downloading patches on page 49 (finding and downloading the particular patch you must install)
- Configuring a proxy on page 50 (if the patches are located in a different server)
- Installing patches on page 50 (for the particular patch you must install)

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

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`.

Removing patches

Use this procedure to uninstall a patch from either System Platform or the template. This procedure uninstalls, but does not delete, the patch file from the system. The patch is available for reinstallation.

When you remove a patch, the system reverts to a completely unpatched state, and you must reinstall previous patches as required.

Remove any uninstalled patches using the remove button, unless you want to reinstall the patch in the future. Removing patches that are no longer required will speed the patch management page display time. A patch can be redownloaded to the system.

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 that you must remove.
4. On the Patch Detail page, click **Remove** if you are removing a template patch.

   ⊕ **Tip:**

   You can clean up the hard disk of your system by removing a patch installation file that is not installed.

Related Links

Patch List field descriptions on page 55
Patch Detail field descriptions on page 56

Search Local and Remote Patch field descriptions

Use the Search Local and Remote Patch page to search for available patches and to upload or download a patch.

Name	Description
Supported Patch File Extensions	The patch that you are installing must match one of the extensions in this list: *.tar.gz,*.tar.bz,*.gz,*.bz,*.zip,*.tar,*.jar,*.rpm,*.patch.
Choose Media	Displays the available location options for searching a patch. Options are: • **Avaya Downloads (PLDS)**: The template files are in the Avaya Product Licensing and Delivery System (PLDS) website. You must enter an Avaya SSO login and password. The list contains all your company's entitled 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**: A different server stores the files. You must specify the Patch URL for the server. • **SP Server**: Files are located in the vsp-template file system in the System Platform server. You must specify the Patch URL for the server. **Tip:** To move files from your laptop to the System Platform Server, some errors can occur because System Domain (Domain-0) and Console Domain support only SCP, but most laptops do not come with SCP support. You can download the following two programs to enable SCP (Search the Internet for detailed procedures to download them): - Pscp.exe - WinSCP • **SP CD/DVD**: Files are located in a System Platform CD or DVD. • **SP USB Device**: Files are located in a USB flash drive. This option is: - supported for RPM patch upgrades not exceeding the storage capacity of the flash drive. - not supported for full-platform (ISO) upgrades to System Platform 6.2 or later. • **Local File System**: Files are located in a local computer.

Table continues…

Name	Description
Patch URL	Active only when you select **HTTP** or **SP Server** as the media location. URL of the server where the patch files are located.

Button descriptions

Button	Description
Search	Searches for the available patches in the media location you specify.
Configure Proxy	Active only when you select **HTTP** as the media location option. Opens the System Configuration page and lets you configure a proxy based on your specifications. If the patches are located in a different server, and depending on your network setup, configure a proxy address and port.
Add	Displays when **Local File System** is selected and adds a patch file to the local file system.
Upload	Displays when **Local File System** is selected and uploads a patch file from the local file system.
Download	Downloads a patch file.

Related Links

Downloading patches on page 49

Patch List field descriptions

The Patch List page displays:

- Patches you can install or remove on the System Platform server.
- In three separate panels, the fields associated with System Platform patches, services_vm patches, and Solution Template patches.

Components with patches

Name	Description
System Platform	List of patches available for System Platform.
services_vm	List of patches available for the Services Virtual Machine.
Templates	List of patches available for a specific solution template.

Fields per patch

Name	Description
Patch ID	File name of a patch. Click the name to view more details about the patch.
Description	Information about the patch, for example, if the patch is available for System Platform, the description is shown as `SP patch`.
Status	Status of a patch. Possible values of **Status** are **Installed**, **Not Installed**, **Active**, and **Not Activated**.
Service Affecting	Shows if installing the patch causes the associated virtual machine to restart.

Button descriptions

Button	Description
Refresh	Refreshes the patch list.

Related Links

Removing patches on page 53

Installing patches on page 50

Patch Detail field descriptions

The Patch Detail page provides detailed information about a patch. Use this page to view details of a patch or to install, commit, roll back, or remove a patch.

Name	Description
ID	File name of the patch file.
Version	Version of the patch file.
Product ID	Name of the virtual machine.
Description	Virtual machine name for which the patch is applicable.
Detail	Virtual machine name for which the patch is applicable. For example, Console Domain (cdom patch).
Dependency	Shows if the patch file has any dependency on any other file.
Applicable for	Shows the software load for which the patch is applicable.

Table continues…

Name	Description
Service affecting when	Shows the action (if any) that causes the selected patch to restart the System Platform Web Console.
Restart this console when	Shows the conditions or circumstances when the System Platform Web Console must be restarted.
Disable sanity when	Shows at what stage the sanity is set to disable.
Status	Shows if the patch is available for installing or already installed.
Patch File	Shows the URL for the patch file.
Publication Date	Shows the publication date of the patch file.
License Required	This field is applicable only for products that support Service Pack Guardian. Communication Manageris the only product that supports this feature.
Rollbackable	Shows whether you can roll back the patch after installation.

Button descriptions

Button	Description
Refresh	Refreshes the Patch Details page.
Patch List	Opens the Patch List page, that displays the list of patches.
Install	Installs the respective patch.
Rollback	Rolls back the installed patch if the **Rollbackable** field value is `Yes`.
Remove	Uninstalls the respective patch. This button uninstalls, but does not delete, the patch file from the system. The patch is available for reinstallation. When you remove a patch, the system reverts to a completely unpatched state, and you must reinstall previous patches as required.
Remove Patch File	Deletes the respective patch file from the system. After the patch file is deleted, it is unavailable for reinstallation. To reinstall the patch, you must download the patch again.

Related Links

Removing patches on page 53

Installing patches on page 50

Chapter 6: Configuring SNMP on the Services virtual machine

SNMP configuration overview

Services-VM can support either SNMP v2c or v3 for SAL Gateway. In case of a fresh installation of Services-VM, Services-VM supports SNMP v3 by default. You can change the configuration to support the required SNMP version.

After you upgrade Services-VM from 1.0 to 2.0, Services-VM supports the SNMP version that was configured on Services-VM 1.0.

Services-VM contains two files, `snmpv2c.conf` and `snmpv3.conf`, for SNMP v2c configuration and SNMP v3 configuration respectively. Based on the SNMP version you want to support, you must use one of the two files for SNMP configuration. The files contain the following default values that you must modify with actual values after a consultation with your network administrator.

File	Parameter	Default value
`snmpv2c.conf`	Community string	avaya123
`snmpv3.conf`	User name	initial
	Authentication protocol	MD5
	Authentication password	avaya123
	Privacy protocol	Data Encryption Standard (DES)
	Privacy password	avaya123

Configuring SNMP version support on the Services VM

You must have:

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

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

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

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

Procedure

1. Open an SSH session to log on to the Services VM as **root**.
2. Change the current directory to /etc/snmp.
3. Find the **snmpd.conf** file.
4. Check the version of **snmp<v2c| v3>.conf** linked to the file **snmpd.conf** .

   For example:

   ```
   # ls -l
   ```

   ```
   lrwxrwxrwx 1 root root 11 Jul 19 20:35 snmpd.conf -> snmpv3.conf
   -rw-r--r-- 1 root root 77 Jun 28 11:54 snmpv2c.conf
   -rw-r--r-- 1 root root 72 Jun 28 11:54 snmpv3.conf
   ```
5. If the **snmpd** service is active, run the following command to stop the service:

   ```
   /sbin/service snmpd stop
   ```
6. Run the following command to back up the file **snmpd.conf** :

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

   ```
   rm —f snmpd.conf
   ```
8. Run one of the following commands to create a soft link to the SNMP version you want to support:

   To configure the Master Agent for SNMP v3:

   ```
   ln -s snmpv3.conf snmpd.conf
   ```

   To configure the Master Agent for SNMP v2c:

   ```
   ln -s snmpv2c.conf snmpd.conf
   ```
9. Run the following command to start the **snmpd** service:

   ```
   /sbin/service snmpd start
   ```

Chapter 7: Configuring SAL Gateway on System Platform

SAL Gateway

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

Remote Serviceability

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

Note:

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

Standalone SAL Gateway

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

If you use a standalone SAL Gateway, you must add it as an SNMP trap receiver for System Platform. See Adding an SNMP trap receiver on page 75. 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 75.

SAL Gateway configuration

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

To configure SAL, perform these high-level steps:

1. Register the system.

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

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

2. Configure the SAL Gateway.

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

Note:

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

Related Links

Installation process overview on page 8

Configuration prerequisites on page 61

Registering the system on page 13

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 13

SAL Gateway on page 60

Registering the system on page 13

Changing the Product ID for System Platform

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.

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

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 64.
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.

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 64

Applying configuration changes on page 71

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.

Table continues…

Name	Description
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 *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com
Inventory collection schedule	Interval in hours at which the SAL Gateway collects inventory data.

Related Links

Configuring the SAL Gateway on page 63

Registering the system on page 13

Configuring a proxy server

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.

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 66

Applying configuration changes on page 71

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.

Table continues…

Name	Description
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 65

Configuring SAL Gateway communication with a Concentrator Core Server

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.

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 68

Applying configuration changes on page 71

Core Server field descriptions

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

Related Links

Configuring SAL Gateway communication with a Concentrator Core Server on page 67

Configuring SAL Gateway communication with a Concentrator Remote Server

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.

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 69

Applying configuration changes on page 71

Remote Server field descriptions

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

Related Links

Configuring SAL Gateway communication with a Concentrator Remote Server on page 68

Configuring NMS

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.

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 70

Applying configuration changes on page 71

Network Management Systems field descriptions

Name	Description
NMS Host Name/ IP Address	The IP address or host name of the NMS server.
Trap port	The port number of the NMS server.
Community	The community string of the NMS server. Use `public` as the **Community**, as SAL agents support only public as community at present.

Related Links

Configuring NMS on page 70

Managing service control and status

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

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Service Control & Status**.

   The system displays the Gateway Service Control page. The page displays several Gatew:ay Services such as:

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

   The Gateway Service Control page also displays the status of each service as:

   - **Stopped**
   - **Running**

2. Click one of the following buttons:

   - **Stop** to stop a service.
   - **Start** to start a service that is stopped.
   - **Test** to send a test alarm to the Secure Access Concentrator Core Server.

   Important:

   Use caution if you stop the Remote Access service. Stopping the Remote Access service blocks you from accessing SAL Gateway remotely.

Applying configuration changes

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Apply Configuration Changes**.

   The system displays the Apply Configuration Changes page.

2. Click the **Apply** next to **Configuration Changes**.

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

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

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

Managed element worksheet for SAL Gateway

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

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

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

Important:

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

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

Related Links

Adding a managed element on page 73

Adding a managed element

Complete the Managed Element Worksheet for SAL Gateway.

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.

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 73
Applying configuration changes on page 71
Managed element worksheet for SAL Gateway on page 72

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.

Table continues…

Name	Description
Product ID	The Product ID (also called Alarm ID). The Product ID is in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm.
Provide Remote Access to this device	Check box to allow remote connectivity to the managed device.
Transport alarms from this device	(Optional) Check box to enable alarms from this device to be sent to the Secure Access Concentrator Core Server.
Collect Inventory for this device	Check box to enable inventory collection for the managed device. When this check box is selected, SAL Gateway collects inventory information about the managed device and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel working on tickets and must review the configuration of managed devices. For more information on this feature, see the *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com.
Inventory collection schedule	Interval in hours at which the SAL Gateway collects inventory information about the managed device.
Monitor health for this device	Check box to enable health monitoring of the managed device by SAL Gateway. SAL Gateway uses heartbeats to monitor health. Heartbeats must be configured on the device.
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 73

Using a stand-alone SAL Gateway

Adding an SNMP trap receiver

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.

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**.

Chapter 8: Installing and deleting a solution template

Template installation

After installing System Platform, install the solution templates.

After installing the templates, manage the templates from the System Platform Web Console.

Note:

The procedures for configuring a solution template differ depending on the template. See the documentation for the specific solution template for the configuration steps.

Prerequisites for installing a solution template

- Stop High Availability if it is running and remove the High Availability configuration. You cannot install a solution template if High Availability is running.
- Verify the IP addresses for the *avprivate* bridge do not conflict with any other IP addresses in your network.

  Go to the Network Configuration page on the System Platform Web Console (**Server Management** > **Network Configuration**) to view the addresses that are allocated to avprivate. The range of IP addresses starts with the Domain-0 interface on avprivate. Console Domain automatically receives the consecutive IP address. Resolve any conflicts by assigning an IP address for Domain-0 on a subnet that you know is not used in your network. Also keep in mind that some templates require additional addresses on the private bridge.

  The avprivate bridge is an internal, private bridge that allows virtual machines to communicate with each other. This private bridge has no connection to your LAN. During installation, System Platform runs an algorithm to find a set of IP addresses that do not conflict with the addresses configured on the System Domain Network Configuration page. However, it is still possible that the addresses selected conflict with other addresses in your network. Since this private bridge is isolated from your LAN, this address conflict could result in the failure of System Platform or an installed template to route packets correctly.
- Optional. Create an EPW file to load configuration data into the template. See Creating an EPW file on page 17.
- Optional. Create an Avaya Bulk Input Tool (ABIT) file to upload station data, including user name, station type, and port, into the system.

For more information about creating and using ABIT files, see those topics in your Avaya Aura® solution documentation.

Related Links

Stopping System Platform High Availability on page 105

Removing the High Availability configuration on page 106

Configuring a proxy

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.

Installing a solution template

- 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.

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.

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.

Related Links

Prerequisites for installing a solution template on page 77
Search Local and Remote Template field descriptions on page 81
An EPW file on page 17

Search Local and Remote Template field descriptions

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

Name	Description
Install Template From	Locations from which you can select a template and install it on System Platform. Available options are as follows: **Avaya Downloads (PLDS)** The template files are located in the Avaya Product Licensing and Delivery System (PLDS) website. You must enter an Avaya SSO login and password. The list contains your company's templates. Each line in the list begins with the “sold-to” number to allow you to select the appropriate template for the site where you are installing. Hold the mouse pointer over the selection to view more information about the “sold-to” number. **HTTP** The template files are located on an HTTP server. You must enter the template URL information. **SP Server** The template files are located in the `/vsp-template` file system in the Console Domain of the System Platform server. **SP CD/DVD** The template files are located on a CD or DVD in the CD/DVD drive on the server. **SP USB Disk** The template files are located on a USB flash drive connected to the server.
SSO Login	Active only when you select the **Avaya Downloads (PLDS)** option to search for a template. Login id for logging on to Single Sign On.
SSO Password	Active only when you select the **Avaya Downloads (PLDS)** option to search for a template. Password for Single Sign On.

Search Local and Remote Template button descriptions

Name	Description
Install	Installs the solution template. This button only displays if there is not an installed System Platform template.
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.

Deleting a solution template

This procedure deletes all applications (virtual machines) in the solution template that is installed.

Procedure

1. Click **Virtual Machine Management** > **Templates**.
2. On the Search Local and Remote Template page, click **Delete**.
3. Click **Ok** to confirm deletion or **Cancel** to cancel deletion.

Chapter 9: Installing license files and authentication files

Installing license files

License files

Use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files for the template that is installed. PLDS is an online, Web-based tool for managing license entitlements and electronic delivery of software and related license files.

After you get the license file, use WebLM to install it.WebLM is a Web-based application for managing licenses and is installed as part of System Platform in the Console Domain.

The license file is an Extensible Markup Language (XML) file. It contains information about the product, major release, license features, and capacities.

A 30-day grace period applies to new installations or upgrades of the template that is installed. You have 30 days from the day of installation to install a license file.

PLDS Overview

The Avaya Product Licensing and Delivery System (PLDS) provides customers, Avaya Partners, distributors, and Avaya Associates with tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads.

Installation software packages for Avaya products are available as ISO files on PLDS. Users can download the ISO images to a computer, and choose to either burn a DVD or transfer the ISO file to the target server for installation.

You can check PLDS to determine if a later service pack or software release is available. If updates do exist, see the appropriate upgrade procedures, contact Avaya, or contact the Avaya Partner Service representative.

When you place an order for a PLDS-licensed software product such as , the license entitlements on the order are automatically created in PLDS. When these license entitlements are created, you receive an email notification from PLDS. This email notification includes a license activation code (LAC). Using the LAC, you can quickly find and activate the newly purchased license entitlements in PLDS. You can then download the license file.

Important:

You must provide the WebLM host ID to activate the license file in PLDS. The primary WebLM host ID is the MAC address of a physical network interface card (NIC) on the server.

See Obtaining the WebLM host ID on page 84 for how to get the WebLM host ID.

Examples of license management tasks that you can perform in PLDS include:

- Adding more license entitlements to an existing activation
- Upgrading a license file to a new major release
- Moving license entitlement activations between license hosts
- Regenerating a license file with an new host ID

Accessing WebLM from the System Platform Web Console

Procedure

1. Start the System Platform Web Console and log in.
2. In the navigation pane, click **Server Management** > **License Management**.
3. On the License Management page, click **Launch WebLM License Manager** .
4. When WebLM displays its Logon page, enter the user name and password for WebLM. For initial login to WebLM, the user name is `admin`, and the password is `weblmadmin`. However, you must change the password the first time that you log in to WebLM.

Getting the WebLM host ID

You must provide the WebLM host ID to activate the license file in PLDS. The primary WebLM host ID is the MAC address of a physical network interface card (NIC) on the server.

Procedure

1. Start the WebLM Web interface and log in.
2. In the left navigation pane, click **Server Properties**.
3. Make a note of the MAC address that displays in the **Primary Host ID** field.

Activating license entitlements in PLDS

Obtain the Host ID of WebLM if you are activating license entitlements on a new License Host.

Use License Activation Code (LAC) to activate one or more license entitlements. You can activate all of the licenses, or you can specify a number of licenses to activate from the quantity available. Upon successful activation of the license entitlements, PLDS creates an Activation Record and sends an Activation Notification email message to the customer who is registered with the entitlements. The Activation Record and Activation Notification provide details on the number of activated licenses and the License Host. The license file can be accessed on the License/Keys tab of the Activation Record in PLDS and is also an attachment to the Activation Notification email message. You must install the license file on WebLM to use the licenses.

For more information about PLDS, see *Getting Started with Avaya PLDS* at http://support.avaya.com.

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. In the **LAC(s)** field of the Quick Activation section, enter the LAC that you received in an email message.

   ✱ **Note:**

   If you do not have an email message with your LAC, you can search for your entitlements and find the LAC. See “Searching for entitlements” in *Getting Started with Avaya PLDS*.

   ✱ **Note:**

   The Quick Activation automatically activates all license entitlements on the LAC. However, you can remove line items or specify a number of licenses to activate from the quantity available.
4. Enter the License Host information.

   You can either create a new license host or use an existing license host.
5. Click **Next** to validate the registration detail.
6. Enter the License Host Information.
   - The Host ID of the WebLM server. The Host ID is obtained from the Server Properties page of the WebLM server where the license file is installed.
   - If you are using Centralized Licensing, enter the Centralized Licensing ID of the WebLM server where the license file is installed. Obtain the Centralized Licensing ID from the Server Properties page of the System Manager WebLM server.
7. Enter the number of licenses to activate.
8. Review the Avaya License Agreement and accept the agreement if you agree.
9. Perform the following steps to send an activation notification email message:
   a. In the **E-mail to** field, enter the email addresses of the additional activation notification recipients.
   b. Enter the comments or special instructions in the **Comments** field.
   c. Click **Finish**.
10. Click **View Activation Record**.
    - The **Overview** tab displays a summary of the license activation information.

- The **Ownership** tab displays the registration information.
- The **License/Key** tab displays the license files resulting from the license activation. On the **License/Key** tab, you can view and download the license files. Each license file must be installed on the WebLM server that is associated with the License Host.

Installing a license file in WebLM

Get the license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

Procedure

1. Start the WebLM Web interface and log in.
2. In the left navigation pane, click **Install license**.
3. On the Install license page, enter the license file path. You can also click **Browse** to select the license file.
4. Click **Install** to install the license file.

   WebLM displays a message on successful installation of the license file. The installation of the license file can fail for various reasons, such as:

   - When WebLM finds an invalid digital signature on the license file. If you get such an error, request PLDS to redeliver the license file.
   - The current capacity use exceeds the capacity in the installed license.

Installing authentication files

Authentication files

The authentication file contains Access Security Gateway (ASG) keys and the server certificate for the template that is installed. ASG keys make it possible for Avaya Services to securely access the customer’s system.

System Platformand the template that is installed share the same authentication file. A default authentication file is installed with System Platform. The default authentication file has an authentication file ID (AFID) of 7100000000. However, the default file must be replaced with a unique file. Unique authentication files are created by Authentication File System (AFS) at http://rfa.avaya.com. After you create and download the authentication file, you install it from the System Platform Web Console of the server. When you install the authentication file in System Platform, the file is automatically installed on all virtual machines on the server.

Every time you upgrade the template to a new major release you must generate and install an authentication file for the upgrade. (Ex, from 5.2 to 6.1, or from 6.2 to 7.0) The updated authentication file has the same AFID as the previous file, but contains new ASG keys.

About the authentication file

AFS authentication files have a plain text XML header with encrypted authentication data and an encrypted server certificate.

Each authentication file contains an authentication file ID (AFID) that identifies it. Use this AFID to create a new authentication file for an upgrade or to replace the current authentication file on the server.

Starting the AFS application

AFS is available only to Avaya service personnel and Avaya Partners. If you are a customer in need of an authentication file, contact Avaya or your authorized Avaya Partner.

You must have a login ID and password to open the AFS application. You can sign up for a login at http://rfa.avaya.com.

Procedure

1. Type `http://rfa.avaya.com` in your Web browser.
2. Enter your login information and click **Submit**.
3. Click **Start the AFS Application**.

   A security message displays.
4. Click **I agree**.

   The AFS application starts.

Creating an authentication file

Creating an authentication file for a new system

You can choose to download the authentication file directly from AFS to your computer, or you can have the authentication file sent in an e-mail message.

Procedure

1. Start and log in to AFS. See Starting the AFS application on page 87.
2. In the **Product** field, select **SP System Platform**.
3. In the **Release** field, select the release number of the software, and then click **Next**.
4. Select **New System**, and then click **Next**.
5. Enter the fully qualified domain name (FQDN) of the host system where the template is installed.

6. To download the authentication file directly from AFS to your computer:
    a. Click **Download file to my PC**.
    b. Click **Save** in the File Download dialog box.
    c. Select the location where you want to save the authentication file, and then click **Save**.
    d. Click **Close** in the Download complete dialog box to complete the download.

    After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
7. To have the authentication file sent in an e-mail message:
    a. Enter the e-mail address in the **Email Address** field.
    b. Click **Download file via email**.

        AFS sends the e-mail message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.
    c. Save the authentication file to a location on the e-mail recipient's computer.

    After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
8. To view the header information in the authentication file, go to the location where the file is saved and use WordPad to open the file.

    The header includes the AFID, product name and release number, and the date and time that the authentication file was generated.

Creating an authentication file for a file replacement

You must have the AFID of the authentication file that you are replacing. See Obtaining the AFID from Web Console on page 89.

You can choose to download the authentication file directly from AFS to your computer, or you can have the authentication file sent in an e-mail message.

Procedure

1. Start and log in to AFS. See Starting the AFS application on page 87.
2. In the **Product** field, select **SP System Platform**.
3. In the **Release** field, select the release number of the software, and then click **Next**.
4. Select **Upgrade or Re-deliver for Existing System**.
5. In the **Authentication File ID** field, enter the AFID for the authentication file that is currently installed on the system, and then click **Next**.
6. Select one of the following options:
    - If you use an Avaya Services login to access the template application, read the product access instructions. After reading the instructions, select **I read and understand the Product Access Instructions**.

- If you do not use an Avaya Services login to access the template application, select **I do not use Avaya Services logins**.

7. To download the authentication file directly from AFS to your computer:

    a. Click **Download file to my PC**.

    b. Click **Save** in the File Download dialog box.

    c. Select the location where you want to save the authentication file, and then click **Save**.

    d. Click **Close** in the Download complete dialog box to complete the download.

    After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).

8. To have the authentication file sent in an e-mail message:

    a. Enter the e-mail address in the **Email Address** field.

    b. Click **Download file via email**.

        AFS sends the e-mail message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.

    c. Save the authentication file to a location on the e-mail recipient's computer.

    After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).

9. To view the header information in the authentication file, go to the location where the file is saved and use WordPad to open the file.

    The header includes the AFID, product name and release number, and the date and time that the authentication file was generated.

Obtaining the AFID from System Platform Web Console

To replace an authentication file, you must have the AFID of the installed authentication file.

Procedure

1. Start the System Platform Web Console and log in.
2. In the navigation pane, click **User Administration** > **Authentication File**.

Related Links

Creating an authentication file for a file replacement on page 88

Installing an authentication file

You must create and download the authentication file from AFS.

System Platform and the template applications share the same authentication file. When you install the authentication file in System Platform, the file is automatically installed on all virtual machines on the server.

Procedure

1. Start the System Platform Web Console and log in.
2. Select **User Administration** > **Authentication File**.
3. Click **Upload**.
4. In the Choose File to Upload dialog box:
   a. Find and select the authentication file.
   b. Click **Open**.

      ✱ **Note:**

      To override validation of the AFID and date and time, select **Force load of new file** on the Authentication File page. Select this option if you:

      - must install an authentication file that has a different unique AFID than the file that is currently installed, or
      - have already installed a new authentication file but must reinstall the original file

      Do *not* select this option if you are replacing the default authentication file with a unique authentication file.
5. Click **Install**.

   The system uploads the selected authentication file and validates the file. The system installs the authentication file if it is valid.

Chapter 10: Managing Certificates

Certificate management

A user who has the correct administrative privileges can use the certificate management feature to replace the default System Platform Web Console certificate and private key. The user can also upload and replace the Enterprise LDAP certificate if the Transport Layer Security (TLS) option was selected on the Enterprise LDAP page.

The user can replace the default System Platform Web Console certificate and private key by selecting and uploading a new certificate file and a new private key from the local computer. When System Platform is installed, the default System Platform Web Console certificate is generated with the CN value set to the same value as the Console Domain hostname. During a platform upgrade, the certificate is first backed up and then restored after the upgrade completes.

Similarly, a user can upload and replace the Enterprise LDAP certificate by selecting a new certificate file on the local computer and uploading the file.

The following restrictions apply:

- The only acceptable extension of a new certificate file is `.crt`.
- The only acceptable extension of a new private key file is `.key`.
- The option to select and upload the key is only for the System Platform Web Console certificate.
- An uploaded certificate is valid if its start date is not set to a date later than the current date and its end date is not set to a date earlier than the current date. An uploaded private key is valid if it matches the uploaded certificate.

Generating a CSR

This procedure is for advanced users who are familiar with the Linux command line and file transfer utilities.

Use this procedure to generate a certificate signing request (CSR). You must have root permission to the command line for Console Domain.

Procedure

1. Start an SSH session to Console Domain.

> ✚ **Tip:**
>
> The IP address of Console Domain (cdom) is the same as the IP address of the System Platform Web Console.

2. Log in to the Console Domain command line and become the root user:
    1. When prompted, log in as `admin`.
    2. Once logged in, type the following command to log in as the root user: `su — root`
    3. Enter the password for the *root* user.
3. Enter the following command: **`openssl req -new -newkey rsa:1024 -keyout Avaya.key.new -out Avaya_cdom.csr`**
4. When prompted enter the following information:
    - PEM pass phrase
    - Country code, 2 letters, for example GB or US
    - State or province name
    - Locality name, for example, city
    - Organization name, for example, company name
    - Organizational unit name, for example, company division or section
    - Common name, for example, your name or server host name
    - Email address
    - Challenge password, optional
    - Company name, optional
5. Use the **`scp`** command or a similar tool to copy the `Avaya_cdom.csr` file from the server to your local computer.

    The file is saved in your current working directory on the server.

Send the CSR to a certificate authority (CA) to request your certificate.

Generating a self-signed certificate

This procedure is for advanced users who are familiar with the Linux command line and file transfer utilities.

Use this procedure to generate a self-signed certificate. You must have root permission to the command line for Console Domain.

Procedure

1. Start an SSH session to Console Domain.

Tip:

The IP address of Console Domain (cdom) is the same as the IP address of the System Platform Web Console.

2. Log in to the Console Domain command line and become the root user:
    a. When prompted, log in as `admin`.
    b. Once logged in, type the following command to log in as the root user: `su — root`
    c. Enter the password for the *root* user.
3. Enter the following command: **`openssl x509 -req -days 3650 -in Avaya_cdom.csr -signkey Avaya.key.new -out Avaya.crt`**
4. When prompted, enter a pass phrase for the new key.
5. Use the **`scp`** command or a similar tool to copy the `Avaya.crt` and `Avaya.key.new` files from the server to your local computer.

    The file is saved in your current working directory on the server.

Install the self-signed certificate on the Certificate Management page.

Installing a new System Platform certificate

Procedure

1. Select **Server Management** > **Certificate Management**.
2. Click **Provide New Certificate**the **System Platform Certificate** area.
3. Click **Select New Certificate**.
4. Select the new certificate file you want to upload from your local machine to System Platform.
5. Click **Select Private Key File**.
6. Select the private key file you want to upload from your local machine to System Platform.
7. **(Optional)** Enter a **Private Key Passphrase**.
8. If you entered a private key passphrase, reenter the value in the **Confirm Passphrase** field.
9. **(Optional)** Click **Provide New Certificate** the **Upload Chain Certificate File** section.
10. Click **Save**.

Installing an enterprise LDAP certificate

Use this procedure only if **TLS** was selected on the Enterprise LDAP page.

Procedure

1. Select **Server Management** > **Certificate Management**.
2. Click **Provide New Certificate** the Enterprise LDAP Certificate area.
3. Click **Select New Certificate File**.
4. Select the new certificate file you want to upload from your local machine to System Platform.
5. (Optional). Click **Provide New Certificate** the **Upload Chain Certificate File** section of the Enterprise LDAP panel.
6. Click **Save**.

Certificate Management field descriptions

Use the Certificate Management page to get a new certificate from your certification authority for System Platform Web Console or Enterprise LDAP. For System Platform Web Console, you can also get the private key.

Field descriptions

Name	Description
Type	The type of the certificate issued.
Version	The version number of the certificate.
Start Date	The first date on which the certificate is valid.
Expiry Date	The last date (inclusive) on which the certificate is valid.
Issuer	The issuing agency of the certificate.
Subject	The entity requiring authentication using this certificate.
Serial Number	The unique serial number assigned to a new certificate by the certificate authority.
SHA-1 Thumbprint	The unique sequence of bytes authenticating the certificate to a remote entity (node or application).
Private Key Passphrase	The private key passphrase for the System Platform Web Console certificate.
Confirm Passphrase	The **Private Key Passphrase** (reentered for confirmation).

Button descriptions

Use **Provide New Certificate** to select a new System Platform Web Console certificate and private key or Enterprise LDAP certificate, depending on the page where the button is located.

Upload New Certificate File (Required)	
Select New Certificate File	Select a new System Platform Web Console certificate and private key or Enterprise LDAP certificate, depending on the area where the button is located.
Upload New Private Key File (Required)	
Select Private Key File	Select a new private key file to upload from your local machine to use with the new System Platform certificate.
Upload Chain Certificate File (Optional)	
Provide New Certificate	You can optionally select a new chain certificate to upload from your local machine for use with the new primary System Platform certificate.
Other	
Save	Save the new certificate file, private key file, and chain certificate you selected for your System Platform server.

Chapter 11: 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 System PlatformHigh 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 System Platform High Availability

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)
- 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

Table continues…

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

Local and remote server Cdom and Dom0 network interface configuration

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

Table continues…

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

Ping targets configuration

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

Buttons

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

High Availability start/stop

High Availability start

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

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

High Availability stop

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

> ❗ **Important:**
>
> Stopping High Availability operations during disk synchronization might corrupt the file system of the standby console domain. Check the status of virtual machine disk synchronization on the High Availability page of the web console.

When High Availability operations halt:

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

Related Links

Starting System Platform High Availability on page 104

Stopping System Platform High Availability on page 105

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.

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 104

Stopping System Platform High Availability

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.

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 104

Manually switching High Availability server roles

- 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.

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.

- You have stopped System Platform High Availability.

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 12: Troubleshooting the installation

Template DVD does not mount

The template DVD does not mount automatically.

Troubleshooting steps

Procedure

1. Log in to the Console Domain as admin.
2. Enter `su -`
3. Enter the root password.
4. Run the following commands:

```
> ssh dom0.vsp /opt/avaya/vsp/template/scripts/udomAttachCd
> mount /dev/xvde /cdrom/
```

Cannot ping Console Domain or get to the Web Console

Use this procedure to determine if the state of the Console Domain virtual machine is the reason why you cannot get to the System PlatformWeb Console.

Troubleshooting steps

The Web Console runs on the Console Domain virtual machine, so if output of the **`xm list`** command described in this procedure shows that the Console Domain virtual machine is in either a normal or abnormal shutdown state, then the administrator is likely to lose access to the Web Console.

Important:

If you encounter these symptoms after completing the following procedure, go to the Avaya Support website at http://support.avaya.com. Take no further action to troubleshoot the issue locally.

Procedure

1. Log in to the System Domain (Domain-0) as `admin`.
2. Enter **`su -`** to log in as root.
3. At the prompt, type **`xm list`**.

   The **`xm list`** command shows information about the running virtual machines in a Linux screen.

   Two virtual machines are running now: System Domain (shown as `Domain-0`) and Console Domain (shown as `udom` in **`xm list`**).

   A state of `r` indicates that the virtual machine is running. A state of `b` indicates that the virtual machine blocked.

   Note:

   The blocked state does not mean that there is a problem with the virtual machine. The blocked state only means that the virtual machine is not using any CPU time.

   Other possible virtual machine states are:

   - p: paused
   - s: shutdown
   - c: crashed

   For more information about the information displayed, see the Linux manual page for the **`xm`** command.
4. On the Linux screen, type **`exit`** to log off as root. Type `exit` again to log off from System Domain (Domain-0).

Example

`xm list` output:

```
Name                                       ID   Mem VCPUs      State   Time(s)
Domain-0                                    0   512     2     r-----   60227.8
aes                                        15  1024     1     -b----   12674.4
cm                                         17  1024     1     -b----   14898.2
cobar                                      14   512     1     -b----    8492.7
ses                                        19  1024     1     -b----    4775.0
udom                                       16  1024     1     -b----    9071.6
utility_server                             18   512     1     -b----    1909.0
```

If High Availability Failover is enabled, the output of the **`xm list`** command differs for the active server and the standby server. The output for the active server is similar to that shown above.

`xm list` output for the standby server:

If High Availability Failover is enabled, the output for the standby is similar to the following:

```
Name                                        ID   Mem VCPUs      State   Time(s)
Domain-0                                     0   512     2     r-----  21730.2
aes                                             1024     1              2786.0
cm                                              1024     1              3023.7
cobar                                            512     1              1745.1
ses                                             1024     1              1021.7
udom                                            1024     1              2714.1
utility_server                                   512     1               400.0
```

SAL does not work

SAL will not work until product registration is complete.

Complete product registration before proceeding with the troubleshooting steps.

Troubleshooting steps

If the Secure Access Link (SAL) in your Avaya Aura solution is not operating normally, Avaya Support does not receive alarms and other important messages originating from the various components and applications in your system. Neither will Avaya Support be able to connect to your system for remote diagnosis.

If you do not see results similar to those shown in the **ping** and **wget** examples following these troubleshooting steps, contact your corporate IT organization.

Procedure

1. Ping the DNS server in the customer network.
2. Ping the proxy server in the customer network.
3. Ping support.avaya.com to check DNS is working.
4. Enter the command **`wget`** using the proxy from the command line to check if the proxy is working correctly.

Example

Ping for server DNS or proxy server reachability:

```
ping 135.9.69.123
```

```
Pinging 135.9.69.123 with 32 bytes of data:
Reply from 135.9.69.123: bytes=32 time=111ms TTL=54
Reply from 135.9.69.123: bytes=32 time=101ms TTL=54
Reply from 135.9.69.123: bytes=32 time=100ms TTL=54
Reply from 135.9.69.123: bytes=32 time=100ms TTL=54
Ping statistics for 135.9.69.123:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 100ms, Maximum = 111ms, Average = 103ms
```

Ping for Avaya support server reachability

```
ping support.avaya.com
```

Pinging support.avaya.com [198.152.212.23] with 32 bytes of data:

```
Reply from 198.152.212.23: bytes=32 time=101ms TTL=244
Reply from 198.152.212.23: bytes=32 time=101ms TTL=244
Reply from 198.152.212.23: bytes=32 time=101ms TTL=244
Reply from 198.152.212.23: bytes=32 time=102ms TTL=244
Ping statistics for 198.152.212.23:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 101ms, Maximum = 102ms, Average = 101ms
```

WGET for HTTP response from Avaya support

```
wget http://support.avaya.com
HTTP request sent, awaiting response... 200 OK
```

Multiple reinstallations can result in an out of memory error

If you use an installation wizard to install a template and you reinstall the template by deleting and installing it multiple times, an out of permanent generation memory space (PermGen) error can occur.

Troubleshooting steps

Perform the following steps to ensure that a PermGen error does not occur.

Procedure

1. Delete the template.
2. Restart Tomcat by performing the following steps:
    a. Log in to Console Domain as admin.
    b. Enter `su`
    c. Enter `/sbin/service tomcat restart`
3. Start the preinstallation Web application.
4. Install the template.

Appendix A: Installation worksheet for System Platform

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

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

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

System Configuration

Name	Value	Description
	Proxy Configuration:	
Status		Specifies whether an http proxy should be used to access the Internet, for example, when installing templates, upgrading patches, or upgrading platform.
Address		The address for the proxy server.
Port		The port address for the proxy server.
	Cdom Session Timeout	
Session Timeout Status		Specifies whether Cdom session timeout is enabled or disabled.
Session Timeout (minutes)		The maximum time in minutes that a Cdom session remains open after the last user transaction with the System Platform Web Console or Cdom CLI.
	WebLM Configuration:	
SSL		Specifies whether the Secure Sockets Layer (SSL) protocol will

Table continues…

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

Table continues…

Name	Value	Description
		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/getnext/getbulk: entPhysicalTable – One table entry for the Dom0 physical interface. entLogicalTable – One table entry for the Cdom virtual machine, and one table entry for each virtual machine associated with the installed solution template. Each entry contains the virtual machine name, type, software version, and IP address. If you disable this option, SNMP manager systems will be unable to automatically discover this System Platform server.

Enable IPv6 Configuration

Name	Value	Description
Turn On IPv6		Enables IPv6.

General Network Settings Configuration

Name	Value	Description
Default Gateway		The default gateway IP address.
Primary DNS		The primary Domain Name System (DNS) server address.
Secondary DNS		(Optional) The secondary DNS server address.
Domain Search List		The search list, which is normally determined from the local domain name. By default, it contains only the local domain name. You can change this by listing the domain search path that you want following the *search* keyword, with spaces or tabs separating the names.
Cdom Hostname		Depending on requirements of your solution template, you may need to enter the host name for Console Domain as a fully qualified domain name (FQDN), for example, `SPCdom.mydomainname.com`. Otherwise, just enter the IP address for Console Domain or enter the hostname for Console Domain in non-FQDN format.
Dom0 Hostname		Depending on requirements of your solution template, you might need to enter the host name for System Domain as a fully qualified domain name (FQDN), for example, `SPDom0.mydomainname.com`. Otherwise, just enter the IP address for System Domain, or enter the hostname for System Domain in non-FQDN format. When using a Domain Name System (DNS) server in your network, the System Domain hostname must be FQDN format.
Physical Network Interface		The physical network interface details for eth0 and eth1 (and eth2 if High Availability Failover is enabled).

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 or S8300E 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 subnetwork mask for the destination network.
Gateway		The address of a next-hop gateway that can route System Platform traffic to or from a remote services host on the destination network.

SNMP Trap Receiver Configuration

Name	Value	Description
Product Id		Product ID for System Platform Console Domain. When you install System Platform, a default Product ID of

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 `public`.
Device Type		Default setting is **INADS**. Do not change this settings.
Notify Type		Default setting is **TRAP**. Do not change this setting.
Protocol Version		Default setting is **V2c**. Do not change this setting.

Password Configuration

Note:

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

Name	Value	Description
root Password		The password for the root login.
admin Password		The password for the admin login.
cust Password		The password for the cust login. The cust login is for audit purposes. It has read-only access to the Web Console, except for changes to its password, and no command line access.
ldap Password		The password for the ldap login. System Platform uses a local LDAP directory to store login and password details. Use this login and password to log in to the local LDAP directory. This login does not have permissions to access

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.

Index