Administering 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 administration overview

Administration overview

After installing Avaya Aura® System Platform and solution templates, you can perform administrative activities for System Platform and solution templates by accessing the System Platform Web Console. Some of the activities that you can perform include:

- Viewing the log information
- Monitoring the health of the system
- Updating and managing patches
- Managing users and passwords
- Rebooting or shutting down the server

Your administrative operations for System Platform can affect the performance of the solution templates running on System Platform. For example, if you reboot or shut down the System Platform server, the system also reboots or shuts down the solution templates running on System Platform. However, some solution templates have their independent administrative procedures that you can perform by accessing the respective solution template.

Important:

System Platform does not tag Quality of Service (QOS) bits for any packets (known as Layer 2 802.1p tagging). However, System Platform supports tagging of packets for QOS at the Layer 2 switch.

System Platform allows configuring VLAN (from 1 to 4092) only on the S8300D/E server, which is housed in a routing media gateway. To fulfill the VLAN requirements, the S8300D/E will pass traffic to the media gateway based on the configured VLAN. Other server such as S8510 or S8800 will exist as a host on the enterprise network and the VLAN configuration will not have an impact.

System Platform Web Console overview

The System Platform Web interface is called System Platform Web Console. After installing System Platform, you can log on to the System Platform Web Console to view details of System Platform

virtual machines (namely, System Domain (Dom-0) and Console Domain), install the required solution template, and perform various administrative activities by accessing options from the navigation pane.

In the navigation pane, there are three categories of administrative options: Virtual Machine Management, Server Management, and User Administration.

Virtual Machine Management

Use the options under Virtual Machine Management to view details and manage the virtual machines on System Platform. Some of the management activities that you can perform include rebooting or shutting down a virtual machine.

The System Domain (Dom-0), Console Domain, and components of the solution templates running on the System Platform are known as virtual machines. The System Domain (Dom-0) runs the virtualization engine and has no direct management access. Console Domain (cdom) provides management access to the system from the System Platform Web Console.

Server Management

Use the options under Server Management to perform various administrative activities for the System Platform server. Some of the administrative activities that you can perform include:

- Configuring various settings for the server
- Viewing log files
- Upgrading to a latest release of the software
- Backing up and restoring current version of the software

User Administration

Use the options under User Administration to manage user accounts for System Platform. Some of the management activities that you can perform include:

- Viewing existing user accounts for System Platform
- Creating new user accounts
- Modifying existing user accounts
- Changing passwords for existing user accounts

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 12.

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 (cdom).

Note:

You can connect using `http`, but you will be immediately redirected to https. Either of two https formats are acceptable for accessing Web Console administration pages.

- - https://*<IP_Address>*
- https://*<FQDN>*

  Use the FQDN of the server if the network configuration provides Domain Name Services (DNS).

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 Virtual Machine List page in the System Platform Web Console.

Chapter 2: Managing System Platform virtual machines

Virtual Machine Management

Use the options under Virtual Machine Management to view details and manage the virtual machines on System Platform. Some of the management activities that you can perform include rebooting or shutting down a virtual machine.

The System Domain (Dom-0), Console Domain, and components of the solution templates running on the System Platform are known as virtual machines. The System Domain (Dom-0) runs the virtualization engine and has no direct management access. Console Domain (cdom) provides management access to the system from the System Platform Web Console.

Solution Templates

Solution template

After installing System Platform, you can install various solutions templates to run on System Platform. After installing the templates, you can manage the templates from the System Platform Web Console.

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.

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 16.
- 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 150
Removing the High Availability configuration on page 151

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 17.

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 17
Search Local and Remote Template field descriptions on page 20
An EPW file on page 15

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.

Table continues…

Name	Description
	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.

Viewing the template Install/Upgrade Log

View Install/Upgrade Log

The System Platform Web Console provides a high–level workflow view of the last template installation or upgrade, at the following location:

Virtual Machine Management > **View Install/Upgrade Log** > **Log of Last Template Installation/ Upgrade**

Use the log to view major template installation/upgrade tasks such as file downloads, template checks, pre-installation events, software component installations, software component starts and restarts, and finalization of the overall template installation/upgrade process. The log provides a view of the following parameters for every task:

- **Start Time**
- **Task Description**
- **State** (In-progress or Complete)
- **% Complete**
- **Actual** (time to complete)

View Install/Upgrade Log field descriptions

The Install/Upgrade log provides a high-level workflow view of the most recent template installation or upgrade event. The log describes each task within the event in terms of the following parameters:

Name	Description
Start Time	Start time of the task.
Task Description	Brief description of the task.
State	State of the task (`In-progress` or `Completed`)
% Complete	Percentage of the task completed.
Actual	Actual time of the task in-progress or the task completed, in minutes and seconds.

Button	Description
Delete Log	Delete the log currently displayed.

Viewing virtual machines

Procedure

1. Click **Home** or click **Virtual Machine Management** > **Manage**.

The Virtual Machine List page displays a list of all the virtual machines that are currently running on the system.

2. To view details of a specific virtual machine, click the virtual machine name.

   The Virtual Machine Detail page displays configuration details for the virtual machine, including its MAC address, IP address, and operating system.

Related Links

Virtual Machine List field descriptions on page 24
Virtual Machine Detail field descriptions on page 25

Rebooting a virtual machine

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. On the Virtual Machine List page, click the name of the virtual machine.
3. On the Virtual Machine Detail page, click **Reboot**.

Related Links

Virtual Machine List field descriptions on page 24

Shutting down a virtual machine

Procedure

1. Click **Virtual Machine Management** > **Manage**.
2. To stop a virtual machine, click the name of the virtual machine on the Virtual Machine List page.

   On the Virtual Machine Configuration Parameters page, click **Stop**.

   Note:

   The Console Domain can only be restarted and not stopped. If the Console Domain is stopped, administration of the system will no longer be possible.

3. To shut down the entire server including all of the virtual machines, perform one of the following steps:

   - On the Virtual Machine List page, click **Domain-0** in the **Name** column.

     On the Virtual Machine Configuration Parameters page, click **Shutdown Server**.

   - Click **Server Management** > **Server Reboot / Shutdown**.

     On the Server Reboot/Shutdown page, click **Shutdown Server**.

Related Links

Virtual Machine List field descriptions on page 24
Virtual Machine Detail field descriptions on page 25

Virtual Machine List field descriptions

The Virtual Machine List page displays a list of all the virtual machines currently running in the system.

Name	Description
Name	Name of the virtual machines running on System Platform.
Version	Version number of the respective virtual machine.
IP Address	IP address of the virtual machine.
Max Memory	This is a display only field. The value is set by Avaya, and cannot be configured by the users. The amount of physical memory from the total server memory the virtual machine has allocated in the template file.
Virtual CPUs	This is a display only field. CPU allocation for the virtual machine from the template file.
CPU Time	The amount of CPU time the virtual machine has had since boot. This is not the same as uptime.
State	Current status of the virtual machine. Possible values are as follows: • **Running**: Virtual machine is running normally. • **Starting**: Virtual machine is currently booting and should enter a running state when complete. • **Stopping**: Virtual machine is in the process of being shutdown and should enter stopped state when complete. • **Stopped**: Virtual machine has been shutdown. • **Rebooting**: Virtual machine is rebooting and should return to the Running state upon completion. • **No State**: Virtual machine is not running or the application watchdog is not being used.

Table continues…

Name	Description
	• **N/A**: The normal state applicable for System Domain and Console Domain virtual machines.
Application State	Current status of the application (respective virtual machine). Possible values are as follows: • **Starting**: Application is currently booting and should enter a running state when complete. • **Running**: Application is running normally. • **Stopped**: Application has been shutdown. • **Stopping**: Application is in the process of being shutdown and should enter stopped state when complete. • **Partial**: Some elements of the application are running, but not all elements. • **Timeout**: Application has missed a heartbeat, and the Console Domain will reboot the virtual machine associated with the application if necessary to clear the problem. • **Error**: Application sanity mechanism provided some kind of error message. • **Unknown**: Application sanity mechanism failed.

Button descriptions

Name	Description
Refresh	Refreshes the list of virtual machines.

Related Links

Viewing virtual machines on page 22
Shutting down a virtual machine on page 23
Rebooting a virtual machine on page 23

Virtual Machine Detail field descriptions

Use the Virtual Machine Detail page to view runtime details for a virtual machine or to reboot or shut down a virtual machine.

Name	Description
Name	Name of the virtual machine.

Table continues…

Name	Description
MAC Address	Machine address of the virtual machine.
IP Address	IP address of the virtual machine.
OS Type	Operating system of the virtual machine, for example, Linux.
State	Current status of the virtual machine. Possible values are as follows: • **Running**: Virtual machine is running normally. • **Starting**: Virtual machine is currently booting and should enter a running state when complete. • **Stopping**: Virtual machine is in the process of being shutdown and should enter stopped state when complete. • **Stopped**: Virtual machine has been shutdown. • **Rebooting**: Virtual machine is rebooting and should return to the Running state upon completion. • **No State**: Virtual machine is not running or the application watchdog is not being used.
Application State	State of virtual machine as communicated by the watchdog. A virtual machine that includes an application watchdog communicates application health back to the Console Domain. Current status of the application associated with the watchdog. Possible values are as follows: • **Starting**: Virtual machine is currently booting and should enter a running state when complete. • **Running**: Virtual machine is running normally. • **Stopped**: Virtual machine has been shutdown. • **Stopping**: Virtual machine is in the process of shutting down and should enter stopped state when complete. • **Partial** : Some elements of the virtual machine are running, but not all elements. • **Timeout**: Virtual machine has missed a heartbeat, and the Console Domain will reboot the virtual machine if necessary to clear the problem.

Table continues…

Name	Description
	• **Error**: Virtual machine sanity mechanism provided some kind of error message. • **Unknown**: Virtual machine sanity mechanism failed.
Max Memory	The amount of physical memory from the total server memory the virtual machine has allocated in the template file. This is a display only field.
CPU Time	The amount of CPU time the virtual machine has had since boot. This is not the same as uptime.
Virtual CPUs	The maximum number of virtual CPUs used by the virtual machine.
Domain UUID	Unique ID of the virtual machine.
Auto Start	Status of auto start for the virtual machine. Auto start automatically starts the virtual machine after a shut down. Available status are **True** (auto start is enabled), or **False** (auto start is disabled). **Note:** This value should be changed only for troubleshooting purposes.

Button descriptions

Button	Description
Reboot	Reboots the virtual machine. In the case of System Domain (Domain-0), this reboot is the same as the reboot that is available in the navigation pane. When you reboot the System Platform server using the reboot option in the navigation pane, the system shuts down the System Platform server and all the virtual machines that are running on it. **Important:** When you reboot System Domain (Domain-0), the system reboots the System Platform server and all the virtual machines running on it, causing potential service disruption. When you reboot Console Domain, the system loses connection with the System Platform Web Console. You can log in again after Console Domain finishes the reboot operation.

Table continues…

Button	Description
Shutdown Server	Shuts down the server and all virtual machines running on it. Appears only if **Domain-0** is selected.
Stop	Stops the selected virtual machine. Appears only for virtual machines other than Domain-0, cdom, or services_vm.
Start	Starts the selected virtual machine. Appears only for virtual machines other than Domain-0, cdom, or services_vm.

Related Links

Viewing virtual machines on page 22
Shutting down a virtual machine on page 23
Rebooting a virtual machine on page 23

Chapter 3: Server management

Server Management overview

Use the options under Server Management to perform various administrative activities for the System Platform server. Some of the administrative activities that you can perform include:

- Configuring various settings for the server
- Viewing log files
- Upgrading to a latest release of the software
- Backing up and restoring current version of the software

Viewing system information

System server information

You can use the System Platform Web Console to view and print system information for the following server hardware and virtualization parameters:

- Number of cores (CPUs)
- Hardware Virtual Machine (HVM) support
- Total memory
- Available memory
- Total disk space
- Available disk space
- Virtualization architecture support
- Ethernet cards
- Ethernet port aggregation (bonding)

Avaya customers can send this information to Avaya support personnel for server evaluation before attempting to install an Avaya Aura® solution template.

Related Links

Viewing system hardware and virtualization information on page 30
System Information field descriptions on page 30

Viewing system hardware and virtualization information

Procedure

1. Click **Server Management** > **System Information**.
2. Click the **Refresh** button to retrieve the latest set of data for the System Information page.
3. Click the **Print** button to print the contents of the System Information page.
4. Use a screen capture application to save the contents of the System Information page for transmission to Avaya support.

Related Links

System server information on page 29
System Information field descriptions on page 30

System Information field descriptions

Category	Name	Description
Processors	**Number of cores**	Number of CPUs (logical processors)
	Support HVM	Hardware Virtual Machine support is enabled or disabled
Memory	**Total**	Total physical memory in the system
	Available	Available memory not allocated to Xen or any other domains
Disk space	**Total**	Total disk space in the system
	Available	Available disk space not allocated to any domains
Virtualization	**Supported architectures**	Xen version and architectures supported on the system: • x86_32 • x86_32p [Physical Address Extension (PAE) is enabled] • x86_64, ia64
Ethernet cards	**Name**	Name assigned to a PCI card, for example: eth0, eth1, eth2
	Device	Manufacturer's nomenclature for the device, for example: `Broadcom Corporation Nextreme BCM 5709 Gigabit Ethernet (rev 20)`

Table continues…

Category	Name	Description
Bonds	**Name**	Name assigned to an aggregated (bonded) pair of Ethernet ports
	Slave1/Primary	Name of the primary port in a bonded pair of Ethernet ports
	Slave2/Secondary	Name of the secondary port in a bonded pair of Ethernet ports

Related Links

[Viewing system hardware and virtualization information](#) on page 30
[System server information](#) on page 29

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.

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 37.)

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 38

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 38
Downloading patches on page 34

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 40
Patch Detail field descriptions on page 40
Downloading patches on page 34

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 149
Stopping System Platform High Availability on page 150
Removing the High Availability configuration on page 151

Committing patches

You have completed the following tasks using the Web Console:

- Downloading patches on page 34 (finding and downloading the particular patch you must install)
- Configuring a proxy on page 34 (if the patches are located in a different server)
- Installing patches on page 35 (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 40
Patch Detail field descriptions on page 40

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

Table continues…

Name	Description
	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.
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 34

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 37
Installing patches on page 35

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.
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.

Table continues…

Button	Description
	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 37
Installing patches on page 35

Viewing System Platform logs

Log viewer

You can use the Log Viewer page to view the following log files that System Platform generates:

- System logs: These logs contain the messages that the System Platform operating system generates.
- Event logs: These logs contain the messages that the System Platform generates.
- Audit logs: These logs contain the messages that the System Platform generates as a record of user interaction such as the action performed, the time when the action was performed, the user who performed the action, and so on.

To view a log, you should provide the following specifications:

- Select one of the following logs to view:
  - System logs
  - Event logs
  - Audit logs
- Select one of the log levels relevant to the selected logs. The log level denotes the type of incident that might have occurred such as an alert, an error condition, a warning, or a notice.
- Specify a time duration within which an incident of the selected log level might have occurred.
- Optionally search the selected logs by entering some text in the **Find** field and then click **Search**.

Viewing log files

Procedure

1. Click **Server Management** > **Log Viewer**.
2. On the Log Viewer page, do one of the following to view log files:
   - Select a message area and a log level area from the list of options.
   - Enter text to find a log.
3. Click **Search**.

Related Links

Log Viewer field descriptions on page 43

Log Viewer field descriptions

Use the Log Viewer page to view various log messages that the system has generated.

Name	Description
Messages	Select the type of log messages to view. Options are: • **System Logs** are log messages generated by the System Platform operating system (syslog). • **Event Logs** are log messages generated by the System Platform software. These logs are related to processes and commands that have run on System Platform. • **Audit Logs** are a history of commands that users have run on the platform.
Log Levels	Select the severity of log messages to view: Options are: • **Alert** • **Critical/Fatal** • **Error** • **Warning** • **Notice** • **Informational** • **Debug/Fine**

Table continues…

Name	Description
	If you select **Audit Logs** for **Messages**, you have only **Informational** as an option.
Timestamp From	The timestamp of the last message in the type of log messages selected. This timestamp is greater than or equal to the value entered for **Timestamp From**.
To	The timestamp of the first message in the type of log messages selected. This timestamp is less than or equal to the value entered for **To**.
Find	Lets you search for particular log messages or log levels.

Button descriptions

Button	Description
Search	Searches for the log messages based on your selection of message category and log levels.

Related Links

Viewing log files on page 43
Log severity levels on page 51

Configuring date and time

Configuring System Platform time to synchronize with an NTP 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. Click **Server Management** > **Date/Time Configuration**.

   The system displays the Date/Time Configuration page with default configuration settings.

2. In the Select Time Zone panel, select a time zone and click **Save** at the bottom of the page.

The system sets the selected time zone on the System Platform virtual machines (System Domain (Dom-0) and Console Domain). The system also updates the time zone on the other virtual machines.

3. Click **Use NTP for date and time**.

   The Set Time and Date panel changes and displays fields and buttons for configuring, pinging, querying, and removing NTP servers.

4. Click **Ping** to check whether System Platform can reach the specified time server (NTP host) in your network.
5. Specify the IP address or hostname of a time server in your network and click **Add** in the Set Time and Date panel.

   The new time server is added to the configuration file for the local NTP daemon, and the new server should appear in the **Added Servers** list.

6. Click **Save** to synchronize the System Platform time with the NTP server.

   System Platform restarts for the NTP synchronization to take effect.

7. Log in again to the System Platform Web Console.
8. Click **Server Management** > **Date/Time Configuration**.

   The system displays the Date/Time Configuration page with default configuration settings.

9. Click **Query State** to check the NTP (Network Time Protocol) status.

   The system displays the status of the NTP daemon (NTPd) on System Platform. The various time sources in the NTPd status table appear in order of use. The primary (active) NTP server is listed first in the table, followed by one or more entries for fallback (backup) NTP servers in a preferred order.

Related Links

NTP daemon on page 46
Date Time Configuration field descriptions on page 48

Removing a time server

Use this procedure only if your System Platform server has been configured to synchronize with an NTP server, and, for example, the NTP server is no longer available in your network.

Procedure

1. Click **Server Management** > **Date/Time Configuration**.

   The system displays the Date/Time Configuration page.

2. Select a time server from the list of added servers and click **Remove Time Server** in the Set Time and Date panel.
3. Click **Save**.

Note:

The changes take effect after the NTP daemon restarts.

Related Links

Date Time Configuration field descriptions on page 48

NTP daemon

The NTP daemon on System Platform reads its configuration from a file named ntp.conf. The file contains a list of reference time sources (NTP servers). Each source can be another computer on the network or a clock connected to the local system. You specify reference time sources using IP addresses or host names that can be resolved by a domain name server.

NTP uses the pseudo IP address 127.127.1.0 to access its own system clock, also known as the local clock. Do not confuse NTP's pseudo IP address with 127.0.0.1, which is the IP address of the loopback interface for the local host.

The local clock is not directly accessible to administrators and cannot be removed using the Web Console. The local clock will be used by default as a fallback resource if no other time source is available.

Related Links

Configuring System Platform time to synchronize with an NTP server on page 44
Date Time Configuration field descriptions on page 48

Configuring the time zone for the System Platform server

If you need to configure System Platform date and time settings manually instead of configuring the system to synchronize with a Network Time Protocol (NTP) server, you will first need to manually set the time zone in which the System Platform server resides.

Procedure

1. Click **Server Management** > **Date/Time Configuration**.

   The system displays the Date/Time Configuration page with default configuration settings.

2. Within the Select Time Zone panel, select a time zone and click **Save** at the bottom of the page.

   The system sets the selected time zone on the System Platform virtual machines (System Domain and Console Domain). The system also updates the time zone for other virtual machines running on the platform.

   Note:

   Clicking **Save** to make any change to the date or time configuration take effect will cause System Platform to reboot.

Configure the date and time manually.

Related Links

Configuring date and time manually on page 47

Configuring date and time manually

Configure the time zone for the System Platform server.

Use this procedure to configure the date and time if you are not synchronizing the System Platform server with an NTP server.

Procedure

1. Click **Server Management** > **Date/Time Configuration**.

   The system displays the Date/Time Configuration page with default or last-configured settings.

2. If the current configuration uses an NTP server, click **Manually set date and time**.

   The panel changes and displays fields, nested calendar/time icons, and buttons for manually setting a local time to which the System Platform server can resynchronize all operations.

3. Click the calendar button .

4. Select a date in the calendar to change the default date and set the required date.

5. Do the following to set the time:

   a. Click the time field at the bottom of the calendar.

      The system displays a box showing time information.

   b. Use the up and down arrow keys beside the hour to change the hour, and up and down arrows beside the minutes field to set the minutes.

   c. Click **OK** to accept your changes.

6. Click **Apply** to save your changes.

7. Click **Save and Stop Ntpd**.

   The system displays a warning message stating that this action will cause a full system reboot.

8. Click **OK** to accept the message and set the updated date and time in the system.

Related Links

Date Time Configuration field descriptions on page 48

Configuring the time zone for the System Platform server on page 46

Date Time Configuration field descriptions

Use the Date/Time Configuration page to view, change, or manually configure the current time source that System Platform uses.

Caution:

Making changes to the time zone, date, and time configuration will cause a temporary disruption of System Platform services.

Date/Time Configuration

Name	Description
Local Time	Local time at the server location.
UTC Time	Coordinated Universal Time (UTC) at the server location, relative to UTC-0 (Zulu Time zone).
NTPD	Status of the NTP daemon on the System Platform server. Status values are: • NTPD is stopped • NTPD is running

Select Time Zone

Name	Description
Time zone	Menu for selecting the time zone for the city and country where the System Platform server is located.

Set Time and Date

Name	Description
Manually set date and time	Makes it possible for the System Platform administrator to manually set a local time for the server. This is an alternative to the preferred method of specifying NTP servers from which System Platform can select a single reference time source. Selecting **Manually set date and time** causes the Set Time and Date panel to display a field and a calendar button for manually setting a time reference for System Platform.
Use NTP for date and time	Makes it possible for the System Platform administrator to add one or more NTP servers for System Platform to select as its preferred time source. This is also the preferred method for designating a time source for System Platform. The NTP server declared by System Platform as the preferred time source typically has the highest (most

Table continues…

Name	Description
	accurate, lowest numbered) clock stratum level, relative to the Stratum-1 atomic clock standard. Selecting **Use NTP for date and time** causes the Set Time and Date panel to display fields and buttons appropriate for adding or removing NTP servers
[Server local time (UTC/GMT)]	The calendar-based month, day, year and UTC/GMT time where the System Platform server is located. This field is displayed when **Manually set date and time** is selected.
Time Server	Host name or IP address of an NTP server time source that you want to add to the System Platform configuration. This field is displayed when **Use NTP for date and time** is selected.
Added Servers	List of NTP time servers that is available to the local System Platform server. The NTP server declared by System Platform as the preferred time source typically has the highest (most accurate, lowest numbered) clock stratum level, relative to the Stratum-1 atomic clock standard. If you click **Query State**, the currently active NTP server appears with an asterisk preceding its host name. This field is displayed when **Use NTP for date and time** is selected.

Button descriptions

Button	Description
Save	Saves the time and date reference configuration and starts the Network Time Protocol (NTP) daemon. The NTP daemon synchronizes local server time with the reference time from an NTP server. **Note:** Clicking **Save** to make permanent any change to the date and time configuration is service-disrupting and causes a full System Platform reboot. This button is displayed when **Use NTP for date and time** is selected.
Add	Adds a time server that you specify to the list of time servers available to System Platform as a time reference. The NTP server declared by System

Table continues…

Button	Description
	Platform as the preferred time source typically has the highest (most accurate, lowest numbered) clock stratum level, relative to the Stratum-1 atomic clock standard. This button is displayed when **Use NTP for date and time** is selected.
Ping	Checks whether the specified time server, that is, the NTP host that you want to add, can be reached across the network. This button is displayed when **Use NTP for date and time** is selected.
Query State	Checks the status of the NTP daemon on System Platform. This button is displayed when **Use NTP for date and time** is selected.
Remove Time Server	Removes the selected time server. Use this button only if your System Platform server has been configured to synchronize with an NTP server, and, for example, that NTP server is no longer available in your network.
Save and Stop NTPD	Saves the time and date that you manually configured and stops the Network Time Protocol (NTP) daemon if it is running. **Note:** Clicking **Save and Stop NTPD** to make permanent any change to the date and time configuration is service-disrupting and causes a full System Platform reboot. This button is displayed when **Manually set date and time** is selected.

Related Links

Configuring System Platform time to synchronize with an NTP server on page 44
NTP daemon on page 46
Configuring date and time manually on page 47
Removing a time server on page 45

Configuring Logging

Log severity levels

Different log messages in System Platform have different severity levels. The severity levels are:

- Fine
- Informational
- Warning
- Error
- Fatal

You can select how detailed the log output of System Platform will be. Log messages of the severity you select and of all higher severities are logged. For example, if you select Information, log messages of severity levels Information, Warning, Error, and Fatal are logged. Log messages of severity level Fine are not logged.

Log retention

To control the size and number of historical log files that System Platform retains, you configure a maximum size for log files and a maximum number of log files.

When a log file reaches the maximum size, it rolls over. When rollover occurs, .1 is appended to the file name of the current log file and a new, empty log file is created with the original name. For example, `vsp-all.log` is renamed `vsp-all.log.1`, and a new, empty `vsp-all.log` file is created. The number that is appended to older log files is increased by one. For example, the previous `vsp-all.log.1` is renamed `vsp-all.log.2`, `vsp-all.log.2` is renamed `vsp-all.log.3`, and so on. When the maximum number of backup (old) log files is reached, the oldest log file is deleted.

Configuring log levels and retention parameters

Procedure

1. Click **Server Management** > **Logging Configuration**.
2. Edit the default values, if required.
3. Click **Save** to save the settings.

Related Links

Log retention on page 51
Log severity levels on page 51
Logging Configuration field descriptions on page 52

Logging Configuration field descriptions

Use the Logging Configuration page to configure the severity of messages to log, a maximum size for log files, and the number of backup files to retain.

Caution:

Change the default values only for troubleshooting purposes. If you change the logger level to **FINE**, the system writes many log files. There are chances of potential performance issues when using this logging level. Switch to **FINE** only to debug a serious issue.

Name	Description
SP Logger	SP Logger is used for the System Platform Web Console logs, which are generated by the System Platform code base (for example, com.avaya.vsp).
3rd Party Logger	Third Party Logger is the root logger, which can include logs from other third party components included in the System Platform Web Console (for example, com.* or com.apache.*).
vsp-all.log	Contains all logs generated bySystem Platform Web Console, regardless of whether they include event codes.
vsp-event.log	Contains all event logs generated by System Platform Web Console. The logs in vsp-event are available in Avaya common logging format.
vsp-rsyslog.log	Contains syslog messages.
Max Backups	Maximum number of historical files to keep for the specified log file.
Max FileSize	Maximum file size (for example, for a file vsp-all.log. Once the maximum file size is reached it, the log file will roll over (be renamed) to vsp-all.log.1.

Related Links

Configuring log levels and retention parameters on page 51
Log retention on page 51
Log severity levels on page 51

Configuring the system

Introduction

Use the System Configuration page to:

- Configure proxy server settings for Internet access
- Configure the cdom session timeout value for Web Console access to the local System Platform server.
- Configure Web LM server access
- Configure the language associated with your keyboard layout
- Enable or disable statistics collection by System Platform on the local server.
- Enable or disable SNMPv2-based auto-discovery of the local System Platform server and its configuration
- View the Syslog server address
- Configure system elements or components associated with a specific Avaya Aura® solution template.

Configuring system settings for System Platform

Procedure

1. Click **Server Management** > **System Configuration**.
2. On the System Configuration page, modify the fields as appropriate. If the default settings are satisfactory, no changes are necessary.
3. Click **Save**.

Related Links

System configuration field descriptions on page 53

System configuration field descriptions

Use the System Configuration page to configure Internet proxy server settings, change the current keyboard language setting, configure WebLM server information, disable or reenable collection of System Platform statistics, disable or reenable autodiscovery of System Platform servers, and configure various elements of the installed solution template.

Note:

If an administrator modifies WebLM parameters in the System Configuration page, for example, to configure an alternate WebLM Server, then the Web console halts the local instance of WebLM. If the administrator clicks the License Manager menu option, the web console goes to the alternate instance of WebLM. If the administrator blanks out WebLM host and port values, the Web console recovers WebLM default values, resaves them, and then restarts the local instance of WebLM.

Refer to the Release Notes for more information about any known issues relating to WebLM behavior.

Proxy Configuration

Name	Description
Status	Specifies whether an http proxy should be used to access the Internet, for example, when installing templates, upgrading patches, or upgrading platform.
Host	The address for the proxy server.
Port	The port address for the proxy server.

Cdom Session Timeout

Name	Description
Session Timeout Status	Specifies whether Cdom session timeout is enabled or disabled.
Session Timeout (minutes)	The maximum amount of time in minutes that a Cdom session remains open since the last user transaction with the System Platform Web Console or the Cdom CLI.

WebLM Configuration

Name	Description
SSL	Specifies whether the Secure Sockets Layer (SSL) protocol will be used to invoke the WebLM server. Select **Yes** if the alternate WebLM application has an HTTPS web address. Otherwise, select **No** if the alternate WebLM application has an HTTP web address. Default value = **Yes**.
Host	The IP address or hostname 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

Name	Description
Keyboard Layout	Determines the specified keyboard layout for the keyboard attached to the System Platform server.

Table continues…

Name	Description
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 the 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 enterprise solutions at a glance. This feature eliminates the tedious and error-prone task of manually adding a large number of System Platform servers to an SNMP management system, where that system typically requires three or more IP addresses for each System Platform server instance. SNMP management systems can also query any recognized System Platform server for its logical 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.
Syslog IP Address	IP address of the Syslog server, which collects log messages generated by the System Platform operating system.

Related Links

Configuring system settings for System Platform on page 53
Configuring an alternate WebLM server on page 74

Configuring network settings

Configuring System Platform network settings

Important:

The System Platform network settings are independent of the network settings for the virtual machines running on it. This means that the System Platform network settings will not affect the network settings of the virtual machines.

Verify the IP addresses for the *avprivate* bridge do not conflict with any other IP addresses in your network.

The Network Configuration page displays the addresses that are allocated to avprivate. The range of IP addresses starts with System Domain's (Dom-0) interface on avprivate. If any conflicts exist, resolve them. Keep in mind any additional addresses that the template you install will also require 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.

Important:

Change all IP addresses (whenever required) in a single network configuration session to minimize the service disruption.

Procedure

1. Click **Server Management** > **Network Configuration**.
2. On the Network Configuration page enter values to configure the network settings.
3. Click **Save**.

Related Links

Network Configuration field descriptions on page 56

Network Configuration field descriptions

Use the **Network Configuration** page to configure network settings for System Platform. The first time that you view this page, it displays the network settings that you configured during installation of System Platform.

After you install a template, the Network Configuration page displays additional fields based on the specific template installed. Examples of template-specific fields include bridges, dedicated NICs, or IP configuration for each of the guest domains created for the template.

The bonding interface fields explained below are applicable only to certain templates such as Duplex Survivable Core.

Enable IPv6 field description

Name	Description
Turn On IPv6	Enables IPv6. **Important:** When you enable IPv6, the system reboots and you cannot later disable IPv6.

General Network Settings field descriptions

Name	Description
Default Gateway	The default gateway.
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. To change this, list the desired domain search path 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.

Table continues…

Name	Description
Physical Network Interface	The physical network interface details for eth0 and eth1 (and eth2 in case of High Availability Failover is enabled).
Domain Dedicated NIC	The NIC dedicated to a specific domain used by applications with high network traffic or time-sensitive traffic. This means the virtual machine connects directly to the customer network by way of a dedicated Ethernet port and interconnecting Ethernet cable. 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 generally provides access to the LAN for System Platform elements (System Domain (Dom-0) and Console Domain) and for any guest domains that are created when installing a template. The IP addresses specified during System Platform installation are assigned to the interfaces that System Domain (Dom-0) and Console Domain have on this bridge. • **template bridge**: These bridges are created during the template installation and are specific to the virtual machines installed.
Domain Network Interface	The domain network interface details for System Domain (Dom-0) or Console Domain that are grouped by domain based on your selection.
Global Template Network Configuration	The set of IP addresses and host names of the applications hosted on System Platform. Also includes the gateway address and network mask.

Bonding Interface field descriptions

Name	Description
Name	Is a valid bond name. It should match regular expression in the form of “bond[0-9]+”.

Table continues…

Name	Description
Mode	Is the Linux bonding mode supported by System Platform. The supported default mode is **Active/Backup**. For more information about bonding modes and best practices, see http://www.cyberciti.biz/howto/question/static/linux-ethernet-bonding-driver-howto.php.
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.

Bonding Interface link descriptions

Name	Description
Add Bond	Adds new bonding interface. **Note:** • The new bonding interface does not take effect until you **Save** the new settings in the Network Configuration page. • If your solution uses System Platform High Availability, and then you **Start HA**, the **Add Bond** link becomes unavailable. • The **Add Bond** link is unavailable if your System Platform server has an insufficient number of available ports.
Delete	Deletes a bonding interface. **Note:** The bonding interface is not removed until you **Save** the new settings in the Network Configuration page.

Related Links

Configuring System Platform network settings on page 56

Adding a bonding interface

NIC bonding configuration enables two network ports to function as a single, higher-bandwidth port. The two ports are typically of the same type, for example, 1GB or 10GB, although this is not a requirement.

Use this procedure to add a bonding interface while configuring the Network Configuration page of the Web Console.

Procedure

1. Scroll down to make the Bonding Interface frame visible.
2. Click **Add Bond** link.
3. Enter the following fields:
    a. **Name**
    b. **Mode**
    c. **Slave 1/Primary**
    d. **Slave 2/Primary**
4. Click **Save**.

Deleting a bonding interface

While you are configuring network settings in the Network Configuration page, use this procedure to delete a bonding interface.

Procedure

1. Scroll down to make the Bonding Interface frame visible.
2. Click **Delete** corresponding to the bonding interface you must delete.
3. Click **Save**.

Configuring Services Virtual Machine network settings

If you installed the Services Virtual Machine during System Platform installation, you did so to allow installation and configuration of an on-board (local) SAL gateway to support SNMP trap and alarm forwarding to a Network Management System (NMS). Use this procedure to later assign a different hostname and/or IP address to the Services VM for any reason.

The Enable Services VM checkbox is selected.

Use this procedure to reconfigure hostname and IP address settings for the local Services VM, for example, when network address allocations and assignments will be changing in your network.

Procedure

1. In the Navigation pane of the System Platform web console, click **Server Management** > **Network Configuration**.

   The Server Management Network Configuration page appears.

2. Scroll down to the **Template - Services VM** area of the Server Management Network Configuration page.
3. Enter new Services VM hostname and address values to accommodate your new network configuration.
4. Click **Save**.

Related Links

Enabling the Service Virtual Machine on page 61
Disabling the Services Virtual Machine on page 62
Configuring Services VM field descriptions on page 63

Enabling the Service Virtual Machine

- You installed the Services Virtual Machine during System Platform installation.
- You earlier performed the administrative task, Disabling the Services Virtual Machine on page 62.

Use this procedure to reenable the Services Virtual Machine previously disabled (shut down) on the local solution server for one or more of the following reasons:

- You must disable your local SAL gateway to troubleshoot or maintain your solution server.
- You have decided not to deploy the SAL gateway on another server, but instead must redeploy the SAL gateway locally on your solution server.

The procedure attempts to restart the Services VM. The success or failure of each attempt depends on disk and memory resources currently available on the solution server.

Procedure

1. In the Navigation pane of the System Platform web console, click **Server Management** > **Network Configuration**.

   The Network Configuration page appears.

2. In the **Templates – Services VM** area of the Network Configuration page, select **Enable Services VM**.
3. Enter values for the **Services VM Hostname** and **Services VM IPv4 address**.

   If you have enabled IPv6, enter a value for the **Services VM IPv6 address**.

4. At the bottom of the Network Configuration page, click **Save**.

If your attempt to restart the local Services VM succeeds, see **Next steps** following this procedure.

If your attempt to restart the Services VM fails, it is likely because the server does not currently have sufficient disk and memory space to allow restarting the Services VM. You should see an

`Insufficient resources` error message describing the issue. To get assistance from this point, contact Avaya Support at http://support.avaya.com.

- Go to the web console SNMP Trap Receiver Configuration page to reset the SNMP trap receiver destination address for the local SAL gateway. (See SAL Gateway on page 79.)
- Verify the configuration of the local SAL gateway. (See Launching the SAL Gateway management portal on page 80.)
- Restart the local SAL gateway. (See Enabling SAL Gateway on page 83.)

Related Links

Configuring Services Virtual Machine network settings on page 60

Disabling the Services Virtual Machine

You installed the Services virtual machine during System Platform installation.

Use this procedure to change your network configuration from using the local SAL Gateway to using a stand-alone SAL Gateway running on an independent server in your network. To use a stand-alone SAL Gateway, you must disable the on-board SAL Gateway (by disabling its Services VM host) to ensure that during normal operation, Avaya receives the heartbeat message of only the stand-alone SAL Gateway.

Note:

Disabling the Services virtual machine:

- Shuts it down but does not remove it from the node configuration. Reactivation of the Services virtual machine at a later time is possible. For example, you can reactivate the Services virtual machine to use its on-board SAL Gateway, instead of continuing to deploy a SAL Gateway on a separate stand-alone server.
- Shuts down the local SAL Gateway running on the local Services VM
- Reclaims, if necessary, System Platform disk and memory resources formerly used by the local Services VM. This could lead to a shortage of disk and memory resources required to reenable (restart) the local Services VM.

Since this action also disables the local SAL Gateway, you must complete the actions described in **Next steps** following this procedure.

Procedure

1. In the Navigation pane of the System Platform Web console, click **Server Management** > **Network Configuration**.

   The Network Configuration page appears.

2. In the Templates – Services VM area of the Network Configuration page, clear **Enable Services VM**.
3. At the bottom of the Network Configuration page, click **Save**.

- Install and configure a new SAL Gateway on a stand-alone server to receive SNMP traps/alarms from your solution server. (See the latest version of the *Secure Access Link 2.2 SAL Gateway Implementation Guide*, available from the Avaya Support portal at http://support.avaya.com/.

- Go to the Web console SNMP Trap Receiver Configuration page to set the SNMP trap receiver destination address of the new gateway.

Related Links

Configuring Services Virtual Machine network settings on page 60

Configuring Services VM field descriptions

You can access the current Services VM configuration to accommodate any changes to hostname and/or IP address allocations and assignments planned for your network. Services VM configuration fields are accessible from the left Navigation pane of theSystem Platform Web console, under **Server Management** > **Network Configuration**. (Scroll down to **Templates – Services VM**.)

Note:

The Services Virtual Machine detects any change in its current hostname and/or IP address and automatically reconfigures the local SAL gateway for normal operation. For this reason, modifying and saving the Services VM hostname/IP configuration does not require any administrative actions related to SAL reconfiguration.

You can also disable the Services VM from this page. However, disabling the Services VM shuts down the local SAL gateway, as well. For this reason, disable the Services VM only if you are installing and configuring a new SAL gateway on a separate, dedicated server in your network, or you are temporarily troubleshooting or maintaining your solution server and must disable the Services VM for that purpose.

Name	Description
Enable Services VM	Indicates the current state of the Services VM: • Services VM enabled (checkbox selected) • Services VM disabled and stopped (checkbox deselected) **Enable Services VM** also allows you to change the current state of the Services VM. If you deselect **Enable Services VM**, System Platform displays a confirmation box: `The Services VM will be shut down when saving network configuration. Are you sure you want to disable Services VM?` For more information about the effects of disabling or reenabling the Services VM, see also: • Enabling the Service Virtual Machine on page 61 • Disabling the Services Virtual Machine on page 62
Preferred IP Address Type	Indicates the preferred type of IP address for applications running on the Services VM. • **IPv4** • **IPv6**

Table continues…

Name	Description
	If you deselected the **Enable Services VM** checkbox, the web console does not display the **Preferred IP Address Type**.
Services VM IPv4 Address	The IPv4 address required for the Services VM, if you are running the solution server on an IPv4 network. If you deselected the **Enable Services VM** checkbox, the web console does not display the **Services VM IPv4 Address**.
Services VM IPv6 Address	The IPv6 address required for the Services VM, if you a running the solution server on an IPv6 network. If you deselected the **Enable Services VM** checkbox, the web console does not display the **Services VM IPv6 Address**.
Services VM Hostname	Required name for the Services VM. The hostname must be unique and valid within your network, and entered in the correct format: `<Hostname>.<Domain>` **Example:** `admin4.dr.acme.com` If you deselected the **Enable Services VM** checkbox, the web console does not display the **Services VM Hostname**.

Button	Description
Save	Saves any new entries or changes made to the **Server Management** > Network Configuration page (including Services VM configuration).

Related Links

Configuring Services Virtual Machine network settings on page 60

Configuring static routes

Adding a static route

Use this procedure to add a static route to System Platform. You can add a static route, for example, to route packets through a VPN to an Avaya Partner that is providing remote service.

Procedure

1. Click **Server Management** > **Static Route Configuration**.
2. On the Static Route Configuration page, select the **avpublic** interface.
3. Enter the network address.
4. Enter the network mask value.
5. Enter the gateway address.
6. Click **Add Route**.

Related Links

Static route configuration field descriptions on page 65

Deleting a static route

Procedure

1. Click **Server Management** > **Static Route Configuration**.
2. Click **Delete** next to the static route that you must delete, or click **Delete All Routes** to remove all configured static routes.

   The web console displays a message after you click **Delete** or **Delete All Routes**.
3. Click **OK** when the confirmation message appears.

Related Links

Static route configuration field descriptions on page 65

Modifying a static route

Procedure

1. Click **Server Management** > **Static Route Configuration**.
2. Click **Edit** next to the static route you must modify.
3. Modify the settings as appropriate.
4. Click **Modify Route** to save the settings.

Related Links

Static route configuration field descriptions on page 65

Static route configuration field descriptions

Use the Static Route Configuration page to add static routes to System Domain (Dom-0), view details of existing static routes, or modify or delete existing static routes.

Field Names	Descriptions
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.

Related Links

Adding a static route on page 64
Deleting a static route on page 65
Modifying a static route on page 65

Configuring Ethernet settings

Configuring Ethernet interface settings

Procedure

1. Click **Server Management** > **Ethernet Configuration**.

   The Ethernet Configuration page displays the values for all Ethernet interfaces on the server, for example, eth0, eth1, eth2, and so on.

2. Modify the values for eth0 and eth1 as appropriate.
3. Click **Save** to save your settings.

Related Links

Ethernet configuration field descriptions on page 66

Ethernet configuration field descriptions

Use the Ethernet Configuration page to configure settings for the Ethernet interfaces on System Platform.

Name	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 auto-negotiation. By default it is enabled, but might cause some problems with some network devices. In such cases you can disable this option.

Button descriptions

Button	Description
Apply	Saves and applies the settings for the Ethernet device.
Refresh	Refreshes the Ethernet Configuration page.

Related Links

Configuring Ethernet interface settings on page 66

Configuring alarms

Alarm descriptions

System Platform generates the following alarms:

Alarm	Description
High CPU	Average CPU Usage of VM
Disk Usage (Logical Volume)	Percentage of logical volume used (/, /template-env, /dev/shm, /vspdata, vsp-template)

Table continues…

Alarm	Description
Disk reads	Disk read rate (sda)
Disk Writes	Disk write rate (sda)
Load Average	Load average on each virtual machine
Network I/O received	Network receive rate for all guests (excluding dedicated NICs)
Network I/O Transmit	Network transmit rate for all guests (excluding dedicated NICs)
Webconsole heap	Percentage of webconsole (tomcat) heap memory in use
Webconsole open files	Number of file descriptors that webconsole has open
Webconsole permgen	Percentage of webconsole (tomcat) permgen heap used
Webconsole Virtual Memory	Memory for Web Console
Domain-0 Memory (Committed_AS)	Memory for System Domain (Dom-0)
udom Memory (Committed_AS)	Memory for Console Domain

Note:

Virtual machines other than System Domain and Console Domain typically support alarms relevant to their operations. For more information, refer to alarms configuration topics in your Avaya Solution documentation.

Configuring alarm settings

Procedure

1. Click **Server Management** > **Alarm Configuration**.
2. On the Alarm Configuration page, modify the settings as appropriate.
3. Select **Enabled** to enable an alarm, or clear the **Enabled** check box to disable an alarm.

   By default, all alarms are enabled.
4. In the **Limit Value** field, enter the threshold value for the alarm.
5. Specify the number of consecutive samples that must exceed the threshold value for the system to generate an alarm.
6. Specify the **Suppression Period** for an alarm after the system generates the previous alarm.
7. Click **Save** to save the settings.

Related Links

Alarm descriptions on page 67
Alarm configuration field descriptions on page 69

Alarm configuration field descriptions

Use the **Alarm Configuration** page to configure alarms generated from the data collected by the Performance Statistics feature.

Field Names	Descriptions
Alarm	Name of the alarm.
Limit Values	The threshold value above which the value is potentially in an alarming state.
For	The period for which the value must be above the threshold to generate an alarm.
Suppression Period	The period for which the same alarm is not repeated after generating the alarm for the first time.
Enable	Enables the selected alarm.

Related Links

Configuring alarm settings on page 68
Alarm descriptions on page 67

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.

Related Links

Enterprise LDAP field descriptions on page 125

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:
   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 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**.

Related Links

[Configuring authentication against an enterprise LDAP](#) on page 124

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.

Table continues…

Name	Description
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.

Managing System Platform licenses

License management

System Platform includes Avaya's Web License Manager (WebLM) to manage its licenses. WebLM is a Web-based software application that facilitates easy tracking of licenses. You can launch the WebLM application from within System Platform.

Launching WebLM

You are using one of the following Internet browsers:

- Microsoft Internet Explorer, versions 7.*x* and 8.*x*
- Mozilla Firefox, versions 3.5 and 3.6

System Platform uses Web License Manager (WebLM) to manage its licenses. Use this procedure to launch WebLM from System Platform.

Procedure

1. Click **Server Management** > **License Management**.
2. On the License Management page, click **Launch WebLM License Manager** .
3. 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.
4. Manage the licenses as appropriate.

   For more information on managing licenses in Avaya WebLM, see *Installing and Configuring Avaya WebLM Server* at http://support.avaya.com.

Related Links

License management on page 74
License Management launch page field descriptions on page 78

Configuring an alternate WebLM server

- Obtain the Web address of the alternate WebLM application. It should be in either HTTP or HTTPS format, including either the hostname or host IP, plus a logical port number, for example, any of the following:
  - **http://111.125.34.56:4533/WebLM/LicenseServer**
  - **http://avayahost-a:4533/WebLM/LicenseServer**
  - **https://111.125.34.56:4533/WebLM/LicenseServer**

- **https://avayahost-a:4533/WebLM/LicenseServer**

  Extract information from the web address to enter as WebLM configuration values during the following procedure.

Perform this task to designate an alternate server to host a different (non-default) instance of the WebLM application.

Procedure

1. Click **Server Management** > **System Configuration**.
2. On the System Configuration page, modify the following fields according to information obtained through the prerequisites:
   - **SSL** – 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.
   - **Address** – Enter the hostname (for example, `avayahost-a`) or host IP address extracted from the web address of the alternate WebLM application.
   - **Port** – Enter the logical port number (for example, `4533`) extracted from the web address of the alternate WebLM application
3. Click **Save**.

Related Links

System configuration field descriptions on page 53

WebLM password reset and restore

WebLM password reset and restore overview

Use the CLI-based WebLM password reset and restore utilities to recover from, or work around, circumstances such as the following:

- You must reset your WebLM password to its factory default value.
- Your WebLM password or local WebLM administrator is temporarily unavailable. Use the WebLM factory default password to make immediate licensing changes on your WebLM server, and then restore your WebLM administrator's private password after finishing the licensing updates.
- Your WebLM password has been lost or forgotten. Use the WebLM factory default password to make immediate licensing changes on your WebLM server, and then set a new WebLM administrator's private password.

Each WebLM password use or recovery scenario requires you to follow a different sequence of procedures to achieve a successful result. For more information, see WebLM password reset and restore procedures on page 76.

Note:

WebLM password files contain only encoded data, not the actual passwords.

WebLM password reset and restore procedures

This topic provides a high-level workflow for each password reset or restore scenario described in the WebLM password reset and restore overview on page 75.

Resetting an Avaya WebLM password to factory default

See Resetting a WebLM password to factory default on page 76.

Making license changes when the Avaya WebLM password is temporarily unavailable

Follow the sequence outlined in the following table:

Item	Procedure
1.	See Resetting a WebLM password to factory default on page 76.
2.	Complete any licensing updates on the Avaya WebLM server. (For more information, see “Getting started with WebLM” in *Installing and Configuring Avaya WebLM server* at http://support.avaya.com.)
3.	See Restoring a WebLM private password on page 77.

Making license changes when the Avaya WebLM password has been lost

Follow the sequence outlined in the following table:

Item	Procedure
1.	See Resetting a WebLM password to factory default on page 76.
2.	Complete any licensing updates on the Avaya WebLM server. (For more information, see “Getting started with WebLM” in *Installing and Configuring Avaya WebLM server* at http://support.avaya.com.)
3.	Set a new Avaya WebLM private password. (For more information, see *Installing and Configuring Avaya WebLM server* at http://support.avaya.com.

Resetting a WebLM password to factory default

Use this procedure to reset a Avaya WebLM private password to its original factory default value (`weblmadmin`).

You have root level user access to the Linux command line on your System Platform server. (This is for System Platform Advanced Administrators, Avaya Support personnel, and Avaya Partners.)

The `weblm_password reset` command:

- Copies your existing (customized) WebLM password file (`Users.xml`) to a duplicate file named `Users.xml.cust`. This preserves your private WebLM password value in `Users.xml.cust`.
- Copies the WebLM default password file (`Users.xml.default`) to a duplicate file named `Users.xml`. This effectively overwrites the contents of your existing `Users.xml` file, thereby resetting the active Avaya WebLM password to its original factory default value.

Procedure

1. Log on to the Linux CLI as root user on your System Platform server, either by means of a direct local (physical) connection to the server, or by means of remote access (SSH) session.
2. Log on to the System Platform Console Domain (Cdom) CLI with username `admin` (advanced administrator) or `craft` (reserved for Avaya personnel only), plus the password currently associated with the username you entered.
3. At the Cdom command prompt, enter **`weblm_password reset`**.

   Your input and the server's response should be similar to the following example:

   ```
   [root@s83-vsp-sdom bin]# weblm_password reset
   Copied /opt/avaya/vsp/tomcat/webapps/WebLM/admin/Users.xml to
   /opt/avaya/vsp/tomcat/webapps/WebLM/admin/Users.xml.cust
   Copied /opt/avaya/vsp/bin/.weblm/ Users.xml.default to
   /opt/avaya/vsp/tomcat/webapps/WebLM/admin/Users.xml
   Password now set to weblmadmin.
   ```

- You can use the factory default password to access the WebLM server and complete any required licensing updates. (See "Getting started with WebLM" in *Installing and Configuring Avaya WebLM Server*, available at http://support.avaya.com.)
- If you completed this procedure because your WebLM password was temporarily unavailable, you must complete the procedure, Restoring a WebLM private password on page 77.
- If you completed this procedure because you lost or forgot your original WebLM private password, do not run the **`weblm_password restore`** command at this time. If you attempt to restore a lost or forgotten password:
  - You will be unable to see the password because of how it is stored in the system.
  - You will have to run the **`weblm_password reset`** command again, prior to every subsequent attempt to launch the WebLM interface from the System Platform Web Console.
- You can set a new WebLM private password. (See *Installing and Configuring Avaya WebLM Server*, available at http://support.avaya.com.)

Restoring a WebLM private password

Use this procedure to restore a WebLM private password to its former value after gaining temporary WebLM access to perform licensing updates.

- You have root level user access to the Linux command line on your System Platform server. (This is for System Platform Advanced Administrators, Avaya Support personnel, and Avaya Partners.)
- You have completed the procedure, Resetting a WebLM password to factory default on page 76.

The **`weblm_password restore`** command copies the temporary duplicate WebLM password file `Users.xml.cust` (created by Resetting a WebLM password to factory default on page 76) to a new file named `Users.xml`. This effectively overwrites the contents of your existing `Users.xml` file, thereby restoring the WebLM administrator's private password.

Procedure

1. Log on to the Linux CLI as root user on your System Platform server, either by means of a direct local (physical) connection to the server, or by means of remote access (SSH) session.
2. Log on to the System Platform Console Domain (Cdom) CLI with username `admin` (advanced administrator) or `craft` (reserved for Avaya personnel only), plus the password currently associated with the username you entered.
3. At the Cdom command prompt, enter **`weblm_password restore`**.

   Your input and the server's response should be similar to the following example:

   ```
   [root@s83-vsp-sdom bin]# weblm_password restore
   Restored customer WebLM password file.
   ```

   Note:

   If you accidentally run the **`weblm_password restore`** command a second time after your first attempt to restore the WebLM administrator's private password, or if you did not complete the prerequisite procedure, Resetting a WebLM password to factory default on page 76, the temporary duplicate WebLM password file `Users.xml.cust` will not exist, yielding the following error message:

   ```
   [root@s83-vsp-sdom bin]# weblm_password restore
   Customer password backup file does not exist.
   No file to restore.
   ```

- You can access the WebLM server to complete any required licensing updates. (See "Getting started with WebLM" in *Installing and Configuring Avaya WebLM Server*, available at http://support.avaya.com)
- You can set a new WebLM private password. (See *Installing and Configuring Avaya WebLM Server*, available at http://support.avaya.com.)

License Management launch page field descriptions

Use the **License Management** page to launch the Web License Manager (WebLM) application and manage System Platform licenses.

Button descriptions

Name	Description
Launch WebLM License Manager	Launches the WebLM application.

Related Links

Launching WebLM on page 74
License management on page 74

Configuring the SAL Gateway

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 111. 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 83.

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.

Launching the SAL Gateway management portal

Use this procedure to launch the SAL Gateway management portal from within System Platform.

Procedure

1. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
2. On the **Server Management: SAL Gateway Management** page, click **Enable SAL Gateway**.
3. On the SAL Gateway Management page, click **Launch SAL Gateway Management Portal**.
4. When the portal displays its Log On page, enter your user name and password for Console Domain.
5. Configure the SAL Gateway as appropriate.

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 82.
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.

Gateway Configuration field descriptions

Name	Description
Hostname	A host name for the SAL Gateway. **Warning:** Do not edit this field as the SAL Gateway inherits the same hostname as the CentOS operating system that hosts both the System Platform Web Console and the SAL Gateway.
IP Address	The IP address of the SAL Gateway. This IP address must be different from the unique IP addresses assigned to either the Cdom or Dom0 virtual machines.
Solution Element ID	The Solution Element ID that uniquely identifies the SAL Gateway. Format is `(000)123-4567`. If you have not obtained Solution Element IDs for the system, start the registration process. The system uses the SAL Gateway Solution Element ID to authenticate the SAL Gateway and its devices with the Secure Access Concentrator Remote Server.
Alarm ID	The Product ID (also called Alarm ID) for the SAL Gateway. This ID should start with a 5 and include ten digits. The system uses the value in the this field to uniquely identify the source of Gateway alarms in the Secure Access Concentrator Core Server.
Alarm Enabled	Enables the alarming component of the SAL Gateway. This check box must be selected for the SAL Gateway to send alarms.
Inventory Collection	Enables inventory collection for the SAL Gateway. When this check box is selected, SAL Gateway collects inventory information about the supported managed devices and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel working on tickets and must review the configuration of managed devices. For more information on this feature, see the *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com

Table continues…

Name	Description
Inventory collection schedule	Interval in hours at which the SAL Gateway collects inventory data.

Related Links

Configuring the SAL Gateway on page 81

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**.

Enabling SAL Gateway

Use this procedure to enable the SAL Gateway that is embedded in System Platform. The embedded SAL Gateway is enabled by default and only needs to be enabled if you have previously disabled it.

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 **Enable SAL Gateway**.

Related Links

SAL Gateway Management field descriptions on page 84

SAL Gateway Management field descriptions

Button	Description
Launch SAL Gateway Management Portal	Launches the SAL Gateway management portal in a new Web browser window. You must provide valid certificate details to access the portal.
Disable SAL Gateway	Disables the SAL Gateway that is embedded in System Platform. If you are sending alarms to a stand-alone SAL Gateway, disable the embedded SAL Gateway.
Enable SAL Gateway	Enables the SAL Gateway that is embedded in System Platform.

Related Links

Enabling SAL Gateway on page 83

Viewing System Platform statistics

Performance statistics

System Platform collects data on operational parameters such as CPU usage, free and used heap and permgen memory, number of open files on System Platform Web Console, and disk input and output operations to name a few. System Platform collects this data at one minute interval and stores it in an RDD database. System Platform presents this data as graphs using an open source data logging and graphing tool called RRDtool. The following sections should help you understand the System Platform performance statistics capability:

Data retention and consolidation

System Platform stores data for 24 hours and then consolidates it into one hour average and maximum, which is kept for a week. After a week, System Platform consolidates the one hour average and maximum data into 4 hour average and maximum, and stores it for six months.

Monitored parameters

System Platform collects data on the following parameters every minute:

Variable	Domain	Description	Source
CPU usage	All domains	Average CPU usage. Is calculated from cpuSeconds	`xm list -long`
System Platform Web Console memory	cdom	Free and used heap and permgen memory.	JVM
System Platform Web Console open files	cdom	Number of open file handles.	`proc <pid>/fd`
Memory usage	Domain-0, cdom	Committed_AS and kernel.	`/proc/meminfo`
Disk space (logical info)	Domain-0, cdom	Mounted at: /, /template-env, /dev/shm, /vspdata, vsp-template	`df`
Disk space (volume group)	Domain-0	VolGroup00	`vgs`
Disk I/O	Domain-0	Disk read and write rate for sda.	`iostat`
Network I/O	All domains	Network receive/transmit rate for all guests (excluding dedicated NICs.)	`xentop`
Load average	Domain-0, cdom	average load.	`/proc/loadavg`

Graphs

Click **Server Management** > **Performance Statistics** to generate graphs for all or selected parameters and for a specified duration. You can also obtain the comma separated value (CSV) file of the graphed data.

Alarms

System Platform can raise alarms for parameters whose values and frequencies exceed the configured threshold limits.

Related Links

Log severity levels on page 51
Exporting collected data on page 86
Performance statistics field descriptions on page 86

Viewing performance statistics

Procedure

1. Click **Server Management** > **Performance Statistics**.
2. On the Server Management page, perform one of the following steps:
   - Select **All Statistics** to generate a graph for all recorded statistics.
   - Clear **All Statistics**, and select the type of graph from the **Type** drop down menu. Then select the required domain from the list in the **Domains** box.
3. Specify the date and time for the period for the report to cover.
4. Click **Generate** to generate the performance graph for the system.

Related Links

Exporting collected data on page 86
Performance statistics field descriptions on page 86

Exporting collected data

Use this procedure to export to a CSV file the data points that were used to generate a graph.

Procedure

1. Click **Server Management** > **Performance Statistics**.
2. On the Performance Statistics page, select the required details and generate a graph.
3. Click the **Download CSV File** link associated with the data being exported.
4. Click **Save** and specify the location to download the data.

Related Links

Log severity levels on page 51
Performance statistics on page 84
Performance statistics field descriptions on page 86

Performance statistics field descriptions

Use the **Performance Statistics** page to view the health and usage of the system. The Performance Statistics page displays the performance statistics for System Platform and the hosted virtual machines.

Field Names	Descriptions
All Statistics	If you select this option, the system displays a graph for all the recorded statistics.
Type	Appears only if the **All Statistics** check box is cleared. Lets you specify the type of statistics available to display from a list of options.
Domains	Appears only if the **All Statistics** check box is cleared. Lets you select the virtual machines for which System Platform will generate statistics, for example, System Domain (Dom-0) and Console Domain.
Date and Time	Lets you specify the date and time for generating performance statistics from three options as follows: **Predefined Values**: Lets you specify the range of days. **Last**: Lets you specify the day or time. **Between**: Lets you specify the date range.
Generate	Generates the performance statistics of the system based on your specifications.

Related Links

Viewing performance statistics on page 86
Exporting collected data on page 86

Eject CD/DVD

Ejecting the CD or DVD

Use the Eject CD/DVD page to force open the DVD drive of the System Platform server. The CD or DVD used for installing System Platform and virtual machines ejects automatically after successfully completing the installation or an upgrade . However, if any problem occurs during installation or upgrade, the CD or DVD remains locked in the drive. You can use the **Eject CD/DVD** page to force open the drive and remove the CD or DVD.

The data on the CD or DVD receives no damage because of force opening the drive.

Procedure

1. Click **Server Management** > **Eject CD/DVD**.
2. Click **Eject** on the Eject CD/DVD page to eject the CD or DVD.

Eject CD/DVD field descriptions

Button	Description
Eject	Eject the CD or DVD from the System Platform server.
Cancel	Cancel this operation.

Managing Files

File Management overview

With the File Manager in the System Platform Web GUI, an administrator can:

- Copy files from CD or DVD into the **/vsp-template** directory in the Console Domain. This feature helps to facilitate more efficient installation of templates contained on multiple CDs or DVDs.
- Delete directories and files under the **/vsp-template** directory in the Console Domain. This feature helps to free local disk space on the System Platform server when a template installed earlier has no further use, is not a candidate for upgrade, and the administrator needs to install a new solution template.

Note:

File Manager does not allow you to delete the current/active template directory.

Copying files from CD or DVD

An administrator can copy files from CD or DVD to the **/vsp-template** of Console Domain (cdom). This feature facilitates more efficient installation of templates that are contained on multiple CDs or DVDs.

Procedure

1. In the navigation pane, click **Server Management** > **File Manager**.
2. Insert a CD or DVD into the server.
3. In the **Copy from server DVD/CD** panel of the File Management window, click **View CD/DVD** to display the contents of the disk.

   File Manager selects all files in the CD/DVD by default.

4. Clear the check box associated with any file that you must not copy to the **/vsp-template** directory.

   File Manager does not automatically clear the check box for child objects contained in a directory that you cleared. File Manager copies all files that have not been cleared.

5. In the **Copy from server DVD/CD** panel of the File Management window, click **Copy Files**.

   File Manager copies all selected contents of the disk into the **/vsp-template** directory. A new **Copied files from disks** area appears in the File Management window and displays the labels of any disks from which you copied files.

   File Manager overwrites any files in the **/vsp-templates** directory that have the same name as files copied from disk.

6. Repeat all prior steps until you finish copying all of the CDs or DVDs that contain template files for a specific solution.

   While the CD/DVDs load into the **/vsp-templates** directory, File Manager collects and populates the names of all ***.ovf** files from disk into the drop down box at the right side of the **Copy from server DVD/CD** area.

7. Make a selection or enter a new final destination directory name in the drop-down box.

   The text in the drop-down box becomes the final subdirectory where the copied files reside. If the final destination directory you selected or entered already exists, File Manager overwrites any files in the destination directory with any file having the same name in the temporary **cdrom** subdirectory. (File Manager replaces the **/cdrom** subdirectory with the name of the final destination subdirectory.)

   Note:

   If you leave the drop-down box blank, File Manager copies directories and files directly into the **/vsp-template/** directory by default.

Related Links

File Management field descriptions on page 90

Deleting directories and files

An administrator can delete directories and files in the **/vsp-template** directory of Console Domain (cdom). Deleting a directory also deletes all of its subdirectories and files. The administrator can also delete multiple template directories simultaneously. This feature helps to free local disk space on the System Platform server when a template installed earlier has no further use, is not a candidate for upgrade, and a new template must be installed.

Note:

You cannot delete the **/vsp-template** directory. You also cannot delete the directory containing the files used originally as the source for installing the active solution template. To delete the latter directory, you must first uninstall the active solution template from the server. For more information, see Deleting a solution template on page 21.

Procedure

1. In the navigation pane, click **Server Management** > **File Manager**.
2. In the **File Manager** area of the File Management window, select the box to the right of any directory or file that you must delete.
3. Click **Delete**.

   The File Manager area refreshes with the deleted directories or files no longer shown in the hierarchy of the **/vsp-template** directory.

Related Links

File Management field descriptions on page 90

File Management field descriptions

Use the File Management page to:

- copy directories and files from CD or DVD to the **/vsp-template** directory.
- delete directories and files under the **/vsp-template** directory.

Fields

Name	Description
/vsp-template/ ...	This drop-down box specifies the final destination subdirectory in which files (copied originally from CD or DVD to subdirectory `/cdrom`) will reside. While the CDs or DVDs load into the System Platform server, File Manager collects the names of all `ovf` (template installer initialization) files found on the disks and populates them into the drop down box. Following the initial copy from CD/DVD operation, you can either make a selection from values automatically populated into the box, or manually enter a new directory name into the box. If the destination directory you selected or entered already exists, File Manager merges the contents of the temporary `/cdrom` subdirectory with the current contents of the final destination directory. During the merge, File Manager overwrites any files in the destination directory with any file having the same name in the `/cdrom` subdirectory. If you leave the drop-down box blank, File Manager copies the files directly into the `/vsp-template` by default.

Buttons

Button	Description
View DVD/CD	Displays the contents of the CD or DVD inserted into the System Platform server.
Copy files	Copies all selected (file and directory) contents of the disk into the `/vsp-template` directory. A new **Copied files from disks** panel displays the labels of any disks from which the administrator copies files into the `/vsp-template` directory. File Manager overwrites any files in the `/vsp-templates` directory with the contents of any files having the same name on the source disk(s).
Finalize copy	Moves the contents of the temporary subdirectory `/vsp-template/cdrom/` to the subdirectory specified in the drop-down box. (File Manager actually replaces the temporary `/cdrom` subdirectory with the name of the selected or manually entered final target subdirectory for template files not yet installed on the System Platform.)
Delete	Deletes any directories (and their contents) and individual files you have selected (by checkbox) from the directory `/vsp-template.` .

Icons

Icon	Description
	The directory (`/vsp-template`) and temporary subdirectory (`/cdrom`) into which the File Manager copies directories and files from CDs or DVDs. File Manager replaces the temporary `/cdrom` subdirectory with the name of the selected or manually entered final target subdirectory for template files not yet installed on the System Platform.

Related Links

Copying files from CD or DVD on page 88
Deleting directories and files on page 89

Configuring security

Security configuration

Most JITC features are built into the System Platform image and are available after installing System Platform. However, there are some features requiring more user input, and these can be configured from the Security Configuration page. This page allows an advanced administrator user to do the following tasks:

- Remove network debugging tools, namely wireshark from System Platform
- Enable JITC Audit
- Set certain security parameters on the system

Important:

Removing the network debugging tools is irreversible. The tools are removed from System Platform Web Console and the Console Domain.

The **Remove network debugging tools (wireshark)** check box is not enabled once the tools are removed from the system. However, a platform upgrade makes the tools available again and the **Remove network debugging tools (wireshark)** check box is also enabled.

Important:

Enabling audit is also irreversible. The **Enable Audit** check box is not available again after you save the changed security configuration.

Configuring security

Use this procedure to change one or more security features such as enabling audit, resetting the Grub password, changing host access list, and so on.

Procedure

1. Click **Server Management** > **Security Configuration**.
2. Enter one or more required fields in the Security Configuration page.
3. Click **Save**.

Configuring Host Allow and Deny Lists in System Platform HA deployments

Use this procedure to configure the Host Allow and the Host Deny lists for both servers in a System Platform High Availability (SPHA) configuration.

The Cdom and Dom0 virtual machines on both servers in a System Platform High Availability configuration must be able to execute remote SSH commands to each other for HA to function. If you configure security in any way preventing the Cdom or Dom0 virtual machines on either HA node from executing SSH commands to its companion node, HA will not function.

Procedure

1. Log on to the Web Console of the primary HA node.
2. Click **Stop HA** and confirm the displayed warning.
3. Click **Server Management** > **Security Configuration**.
4. Verify that the value `All:All` does not exist in the **Cdom Hosts Deny List** or the **Dom0 Hosts Deny List**.
5. Click **Server Management** > **High Availability**.
6. Configure System Platform High Availability if you have not already done so.
7. Using an SSH session, log on to Dom0 as **admin** .
8. While logged on to the Dom0 domain, run this command and write down resulting output values:

   ```
   sudo /opt/avaya/ha/scripts/vspha status
   ```

   The command collects all three IP addresses used by the primary HA node, including the host address, crossover address, and the udom address.
9. Log off the primary HA node.
10. Log on to the Web Console of the secondary (standby) HA node.
11. Click **Server Management** > **Security Configuration**.
12. Verify that the value `All:All` does not exist in the **Cdom Hosts Deny List** or the **Dom0 Hosts Deny List** of the secondary (standby) HA node.
13. Using an SSH session, log on to Dom0 as **admin** .
14. While logged on to the Dom0 domain, run this command and write down the resulting output values:

    ```
    sudo /opt/avaya/ha/scripts/vspha status
    ```

    The command collects all three IP addresses used by the secondary HA node, including the host address, crossover address, and the udom address.
15. From the Security Configuration page of the secondary (standby) node, add the following entries into the **Cdom Hosts Allow List**
    - `ALL:<primary_HA_node_host_IP>`
    - `ALL:<primary_HA_node_crossover_IP>`
    - `ALL:<primary_HA_node_udom_IP>`
    - `ALL.localhost`
16. Add the following entry into the **Cdom Hosts Deny List** and the **Dom0 Hosts Deny List**:

```
All:All
```

17. **Save** the Security Configuration.
18. Log off the secondary (standby) HA node.
19. Log on to the Web Console of the primary HA node.
20. Click **Server Management** > **Security Configuration**.
21. Add the following entries into the **Cdom Hosts Allow List**
    - `ALL:<secondary_HA_node_host_IP>`
    - `ALL:<secondary_HA_node_crossover_IP>`
    - `ALL:<secondary_HA_node_udom_IP>`
    - `ALL.localhost`
22. Add the following entry into the **Cdom Hosts Deny List** and the **Dom0 Hosts Deny List**:

    ```
    All:All
    ```
23. **Save** the security configuration.
24. Click **Server Management** > **High Availability**.
25. Click **Start HA**.

Security Configuration field descriptions

Field descriptions

Name	Description
Remove network debugging tools (wireshark)	Indicates whether or not to remove the network debugging tools. **Important:** Removing the network debugging tools is irreversible. The tools are removed from System Platform Web Console and the Console Domain. A platform upgrade makes the tools available again and the **Remove network debugging tools (wireshark)** check box is also enabled.
Enable Audit	Indicates whether or not the audit is to be enabled. **Important:** Enabling audit is irreversible.

Table continues…

Name	Description
Restrict Access to System Platform LDAP	Indicates whether access to System Platform LDAP is restricted to applications that are running on this instance of System Platform. If this check box is selected, access is restricted, and attempts by any external sources to access System Platform LDAP are blocked. Default is not restricted. Restricting access to System Platform LDAP prevents sources external to the server from being able to access the System Platform LDAP. Restricting this access provides an additional layer of security. **Note:** Enabling this feature does not block access to System Platform LDAP by the standby server in a High Availability system. The standby server must have access to System Platform LDAP on the primary server to maintain a synchronized state. **Important:** Restricting access to System Platform LDAP does not affect Avaya Aura® application logins or user IDs.
Grub Password	New System Platform Web Console Grub password. **Note:** If your solution is deployed in a System Platform High Availability configuration, you must stop High Availability before attempting to reset the grub password. After you reset the grub password on either the primary or secondary node (or both nodes), start High Availability on the primary/preferred node. The grub password on the secondary/ standby node does not have to be identical to the grub password on the primary/preferred node.
Retype Grub Password	Is the new System Platform Web Console Grub password being retyped for verification.
Verify Dom0 Root Password	Is the System Platform Web Console root password to reset the System Platform Web Console Grub password.
Cdom Hosts Allow List	Is the list of hosts that can access the Console Domain.

Table continues…

Name	Description
	Note: The list of hosts is maintained in the `hosts.allow` file at `/etc` on the Console Domain.
Cdom Hosts Deny List	Is the list of hosts that cannot access the Console Domain. **Note:** The list of hosts is maintained in the `hosts.deny` file at `/etc` on the Console Domain. **Important:** When JITC is enabled, all that `hosts.deny` has is the entry `ALL:ALL`.
Dom0 Hosts Allow List	Is the list of hosts that can access the System Platform Web Console. **Note:** The list of hosts is maintained in the `hosts.allow` file at `/etc` on the System Platform Web Console.
Dom0 Hosts Deny List	Is the list of hosts that cannot access the System Platform Web Console. **Note:** The list of hosts is maintained in the `hosts.deny` file at `/etc` on the System Platform Web Console. **Important:** When JITC is enabled, all that `hosts.deny` has is the entry `ALL:ALL`.
Login Banner Header	Is the header shown for the login banner.
Login Banner Text	Is the text shown for the login banner.

Button descriptions

Name	Description
Save	Saves the security configuration.

Backing up System Platform

System Platform backup

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

Note:

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

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

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

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

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

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

Important:

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

Backups and restores across different versions of System Platform

You cannot restore an older version of System Platform from a backup created on a newer version of System Platform. For example, you cannot restore a System Platform 6.3 backup to System

Platform 6.0. However, you can (for example), restore a System Platform 6.0 backup to System Platform 6.3, although not all templates support this ability. Confirm in your solution documentation whether or not the solution template supports restoring an older version of System Platform backup to the current version.

Backups and System Platform High Availability

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

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

Utility Services settings and size of System Platform backups

Note:

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

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

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

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

Related Links

Re-enabling failed standby node to High Availability Failover on page 178
Re-enabling failed preferred node to High Availability Failover on page 178

Backup progress window

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

Backup progress monitoring

The backup progress window shows:

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

make a more informed decision about whether a problem occurred requiring a system recovery.

Backup progress monitoring runs automatically for the following operations:

- Manual backup
- Template upgrade backup

Backup progress warning and error messages

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

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

Note:

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

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

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

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all template virtual machines). Use the System Platform Web Console to back up the files.

For information about limitations of the backup feature, see System Platform backup on page 97.

Important:

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

Important:

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

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

significantly larger and take longer to generate when they include firmware. For more information see, *Accessing and Managing Avaya Aura® Utility Services*.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

   Note:

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

   - You need to repeatedly terminate a backup operation manually.
   - System Platform automatically terminates a backup operation because of system errors.

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

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

Related Links

Backup field descriptions on page 102

Scheduling a backup

Use this procedure to back up System Platform and the solution template on a regular basis. Backups are not scheduled by default on System Platform.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select **Schedule Backup**.
4. Specify the following:
   - **Frequency**
   - **Start Time**
   - **Archives kept on server**.
   - **Backup Method**

     Use this field to copy the backup archive file to a remote server or to send the file to an e-mail address. The file is also stored on the on the System Platform server.
5. Click **Schedule Backup**.

Related Links

Backup field descriptions on page 102

Transferring the Backup Archives to a remote destination

You can send the backup archive to a mail address or to a remote server by SFTP with using the **Backup Method** option.

Procedure

1. To send the archive by email:
   a. Select the **Email** option as the **Backup Method**.
   b. Specify the **Email Address** and the **Mail Server**.
2. To send the archive to a remote server by SFTP:
   a. Select **SFTP** option as the **Backup Method**.
   b. Specify the **SFTP Hostname** (or IP Address), Directory to which the archive will be sent and the username and password to log in the server.

Viewing backup history

Use this procedure to view the last 10 backups executed and their status. If the last backup failed, the system automatically redirects you to the Backup page after login and displays the following message: `Last Backup Failed`. The system continues to display the message until a backup is successful.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select **Backup History**.

   The system displays the last 10 backups executed with their dates and the status.

Backup field descriptions

Use the Backup page to back up configuration information for System Platform and the solution template.

Backup Now fields

The following table describes the fields that are displayed if you select **Backup Now** at the top of the Backup page.

Field Names	Descriptions
Backup Method	Select a location to send the backup file: • **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory. • **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server. Enter the hostname, directory, user name, and password for the SFTP server. • **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server. Enter the e-mail address and the server address of the recipient.
Backup Now	Starts the backup operation.

Schedule Backup fields

The following table describes the fields that are displayed if you select **Schedule Backup** at the top of the Backup page.

Field Names	Descriptions
Frequency	Select one of the following options: • **Daily** – Backup daily at the specified **Start Time** . • **Weekly** – Backup each week on the chosen **Day** and specified **Start Time**. • **Monthly** – Backup every month on a chosen **Day** (1–28). The numbered list of days does not allow for backup operations on day numbers 29, 30, or 31 occurring only periodically.
Start Time	The start time for the backup.
Archives kept on the server	The number of backup archives to store on the System Platform server. The default is 10.
Backup Method	Select a location to send the backup file: • **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory. • **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server. Enter the hostname, directory, user name, and password for the SFTP server. • **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server. Enter the e-mail address and the server address of the recipient.
Schedule Backup	Schedules the backup process.
Cancel Schedule	Cancels an existing backup schedule.

Related Links

Backing up the system on page 99
Scheduling a backup on page 101

Restoring System Platform

System Platform restore

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

Note:

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

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

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

You can restore data from a backup archive stored in any of the following locations:

- Your System Platform Server
- Another server with SFTP access
- Your local system (for example, your PC)

Note:

A System Platform restore disrupts normal server operations. For this reason, plan to restore during periods of minimum system use, and notify all users of the start and end times for completing the operation. When the restore finishes, you must log on again to the Web Console.

Restore progress window

Restore operations for some machines can be lengthy, depending on the amount of data to restore on the system. As an administrative aid, System Platform displays a window to report progress information during an active restore operation.

Restore progress monitoring

The restore progress window shows:

- Time-stamped progress messages for restoration of System Platform and application data sets, including messages filtered directly from the restore logs, for example, data set restore start, pause, end, or failure.
- A restore process countdown timer. The timer counts down until the operation ends successfully, halts abruptly due to system errors, or the estimated timer value expires. The

countdown timer supplements progress message content, enabling you to make a more informed decision about whether a problem occurred requiring a system recovery.

Restore progress monitoring runs automatically for the following operations:

- Manual restore
- Template upgrade restore

Restore progress warning and error messages

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

- Non-fatal warning messages, such as:
  - A message reporting a normal event requiring no remedial action.
  - A series of error messages associated with a particular template virtual machine. This scenario suggests that restoration of the data set in progress appears to have a problem.
- Fatal warning messages – In the event of any critical restore error, the operation in progress immediately terminates with a message describing the failure. In this case, contact Avaya Support at http://support.avaya.com/.

To aid in troubleshooting a failed system restore, you can also retrieve from the Web Console Restore page any progress messages captured from the last restore attempt.

Restoring backed up configuration information

To restore the backed up configuration information for System Platform and the Solution Template (all virtual machines), use this procedure.

Note:

Do not use the restore functionality to make networking changes. Perform networking changes only from the Network Configuration page of the web console.

Note:

You cannot restore an older version of System Platform from a backup set created on a newer version of System Platform. For example, you cannot restore a System Platform 6.2 backup to System Platform 6.0. However, you can (for example), restore a System Platform 6.0 backup to System Platform 6.2, although not all templates support this capability. Confirm in your solution documentation whether the solution template supports restoring an older version of System Platform backup to the current version.

Note:

The restore operation does not restore the High Availability configuration from the backup file. The restore feature does not re-enable a failed High Availability node to normal operation. See troubleshooting topics for instructions on how to re-enable a failed High Availability node to its latest configuration and normal operation. Restore the backup configuration before separately attempting to re-enable a failed HA node.

Procedure

1. Click **Server Management** > **Backup/Restore**.

2. Click **Restore**.

   The Restore page displays a list of previously backed up archives on the System Platform system.

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

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

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

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

Related Links

System Platform backup on page 97
Restore field descriptions on page 106

Restore field descriptions

Field Names	Descriptions
Restore from	Select the location of the backup archive file from which you must restore configuration information. • **Local**: Restores from a file on System Platform. If you select this option, the Restore page displays a list of previously backed up archives on the System Platform system. • **SFTP**: Restores from a file on a remote server. If you select this option, enter the hostname or IP address of the remote server, directory where the archive file is located, and user name and password for the SFTP server. • **Upload**: Restores from a file on your computer.
Archive Filename	Filenames of the backup archive files at the location you specify.
Archive Date	Date that the file was created.
Selection	Select this check box to restore from the archive file.

Table continues…

Field Names	Descriptions
Restore History	Displays the restore history for the last ten restores. If an error occurred during the last restore, the system directs you to this page after login and continues to display an error message until a restore is successful.

Button descriptions

Button	Description
Search	Displayed if you select **SFTP**. Searches for archive files in the specified directory of the remote server.
Clear Search Result	Clears the list of archive files found on a remote server after an SFTP search.

Related Links

Restoring backed up configuration information on page 105

Viewing restore history

Use this procedure to view the last 10 restores executed and their status. If the last restore failed, the system automatically redirects you to the Restore page after login and displays the following message: `Last Restore Failed`. The system continues to display the message until a restore is successful

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.
3. On the Restore page, select the **Restore History** option.

Rebooting or shutting down the System Platform server

Rebooting the System Platform Server

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

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

If the SAL agent shuts down due to a system reboot, the system automatically creates a backlog of system log files if necessary to process alarms. To circumvent a processing overload under this

condition, the system temporarily throttles the processing of system log files. This has the effect of delaying the forwarding of alarm conditions that occur directly after a system reboot.

Procedure

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

Related Links

Virtual Machine Detail or Server Reboot/Shutdown field descriptions on page 108

Shutting down the System Platform Server

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

Note:

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

Procedure

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

Related Links

Virtual Machine Detail or Server Reboot/Shutdown field descriptions on page 108

Virtual Machine Detail or Server Reboot/Shutdown field descriptions

The Server Reboot/Shutdown page and Virtual Machine Detail: Domain-0 page are identical. They both:

- display runtime values for the Domain-0, System Domain, virtual machine.
- provide buttons for rebooting, starting, and shutting down the server.

Name	Description
Name	Domain-0, which is System Domain.
MAC Address	Machine address of the Domain-0 virtual machine.
IP Address	IP address of the Domain-0 virtual machine.
OS Type	Operating system of Domain-0, for example, Linux.
State	Current status of Domain-0.

Table continues…

Name	Description
	Possible values are as follows: • **Running**: Virtual machine is running normally. • **Starting**: Virtual machine is currently booting and should enter a running state when complete. • **Stopping**: Virtual machine is in the process of being shutdown and should enter stopped state when complete. • **Stopped**: Virtual machine has been shutdown. • **Rebooting**: Virtual machine is rebooting and should return to the Running state upon completion. • **No State**: Virtual machine is not running or the application watchdog is not being used.
Application State	State of the virtual machine as communicated by the watchdog. A virtual machine that includes an application watchdog communicates application health to the Console Domain. Possible values are as follows: • **Starting**: Virtual machine is currently booting and should enter a running state when complete. • **Running**: Virtual machine is running normally. • **Stopped**: Virtual machine has been shutdown. • **Stopping**: Virtual machine is in the process of shutting down and should enter stopped state when complete. • **Partial** : Some elements of the virtual machine are running, but not all elements. • **Timeout**: Virtual machine has missed a heartbeat, and the Console Domain will reboot the virtual machine if necessary to clear the problem. • **Error**: Virtual machine sanity mechanism provided some kind of error message. • **Unknown**: Virtual machine sanity mechanism failed.
Maximum Memory	Amount of physical memory from the total server memory that Domain-0 has allocated in the template file. This is a display only field.

Table continues…

Name	Description
CPU Time	The amount of CPU time the virtual machine has had since boot. This is not the same as uptime.
Virtual CPUs	The maximum number of virtual CPUs used by the Domain-0 virtual machine.
Domain UUID	Unique ID of Domain-0.
Auto Start	Status of auto start for Domain-0. Auto start automatically starts the virtual machine after a shut down. Available status are **True** (auto start is enabled), or **False** (auto start is disabled). **Note:** This value should be changed only for troubleshooting purposes.

Button descriptions

Button	Description
Reboot	Reboots the virtual machine. In the case of System Domain (Domain-0), this reboot is the same as the reboot that is available in the navigation pane. When you reboot the System Platform server using the reboot option in the navigation pane, the system shuts down the System Platform server and all the virtual machines that are running on it. **Important:** When you reboot System Domain (Domain-0), the system reboots the System Platform server and all the virtual machines running on it, causing potential service disruption. When you reboot Console Domain, the system loses connection with the System Platform Web Console. You can log in again after Console Domain finishes the reboot operation.
Shutdown Server	Shuts down the server and all virtual machines running on it.

Related Links

[Rebooting the System Platform Server](#) on page 107
[Shutting down the System Platform Server](#) on page 108

Configuring SNMP trap receivers

SNMP trap receiver configuration

System Platform can send SNMP v2 alarms to up to five trap receivers, including a stand-alone SAL Gateway if appropriate. By sending traps to a stand-alone SAL Gateway, you can consolidate alarms from multiple SAL Gateways instead of having multiple SAL Gateways communicate independently with Avaya.

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**.

Related Links

SNMP Trap Receiver Configuration field descriptions on page 112

Modifying an SNMP trap receiver

Procedure

1. In the navigation pane of the System Platform Web Console, click **Server Management** > **SNMP Trap Receiver Configuration**.
2. In the **SNMP Trap Receivers** area of the SNMP Trap Receiver Configuration page, click **Edit** in the row for the trap receiver you must modify.
3. Modify the settings as appropriate.
4. Click **Apply** to save the settings or **Cancel** to discard your changes.

Related Links

SNMP Trap Receiver Configuration field descriptions on page 112

Deleting an SNMP trap receiver

Procedure

1. In the navigation pane of the System Platform Web Console, click **Server Management** > **SNMP Trap Receiver Configuration**.
2. In the **SNMP Trap Receivers** area of the SNMP Trap Receiver Configuration page, click **Delete** in the row for the trap receiver you must delete.
3. When the confirmation message is displayed, click **OK**.

Related Links

SNMP Trap Receiver Configuration field descriptions on page 112

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**.

Related Links

SNMP Trap Receiver Configuration field descriptions on page 112

SNMP Trap Receiver Configuration field descriptions

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

Table continues…

Name	Description
	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. **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.

Related Links

Adding an SNMP trap receiver on page 111
Deleting an SNMP trap receiver on page 112
Changing the Product ID for System Platform on page 112
Modifying an SNMP trap receiver on page 111

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 4: User Administration

User Administration overview

Use the options under User Administration to manage user accounts for System Platform. Some of the management activities that you can perform include:

- Viewing existing user accounts for System Platform
- Creating new user accounts
- Modifying existing user accounts
- Changing passwords for existing user accounts

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.

User roles

System Platform users must be assigned a user role. Two user roles are available:

- Administrator
- Advanced Administrator

Advanced Administrators have full access to the system by means of both the Web Console and command line. They can make configuration changes to the system in both interfaces. The `admin` login that is created when you install System Platform has a role of Advanced Administrator.

The Administrator role is for audit purposes only. It has read-only access to the Web Console, except for changes to its own password, and no access to the command line. The `cust` login that is created when you install System Platform has a role of Administrator.

Related Links

Creating users on page 117
Editing users on page 118

System Platform users on page 116

Password hashing

Beginning in System Platform 6.3.1, SHA2 is used for hashing of user passwords instead of MD5. When the upgrade to System Platform 6.3 is complete, users must change their existing passwords for SHA2 hashing to take effect. MD5 hashes are retained until users change their passwords. If the 6.3 patch is removed, previous users and passwords are restored, and any new users that were created in 6.3 are removed.

Services Virtual Machine users

Users with root access to the Linux command line can log on directly to the Services VM to perform services-only tasks, such as configuring SNMP version support.

The default password for root is the same as the System Platform default password. However, the Services VM root account is independent of the System Platform root account. Customers must log on the Services VM as root, and are responsible for changing the Services VM default password as soon as possible after upgrading Services VM according to ongoing security policies of the customer organization.

See *Implementing and Administering Services-VM on Avaya Aura® System Platform*, available from the Avaya Support website (http://support.avaya.com), for information regarding how to upgrade the Services VM.

Managing System Platform users

System Platform users

By default, System Platform is shipped with a local LDAP server, known as an OpenLDAP Directory Server, that is installed in System Domain.

System Platform installation creates two users, `admin` and `cust`, in the local LDAP server. The `admin` user has a role of Advanced Administrator. The `admin` user has full access to the system by means of both the Web Console and command line and can make configuration changes to the system in both interfaces. The `cust` user has a role of Administrator and has read-only access to the Web Console, except for changes to its own password. The `cust` user has no access to the command line.

Only an Advanced Administrator can access the **Local Management** option and can perform the following functions:

- View existing users
- Create new users
- Modify existing users
- Change passwords for existing users
- Delete existing users
- Change the LDAP Manager password

Note:

When you use the **User Administration** menu in System Platform Web Console to create a user, the user information is stored in the local LDAP server and does not appear in the `/etc/shadow` file.

Related Links

User roles on page 115

Creating users

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

Procedure

1. Click **User Administration** > **Local Management**.
2. On the Local Management page, click **Create User**.
3. In the **User Id** field, enter a unique user ID.
4. In the **User Password** field, enter a password.

   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.
5. In the **Confirm Password**, enter the same password.
6. In the **User Role** field, click the user role most appropriate for the user.
7. Click **Save User** to the create the user with the details you have specified.

Related Links

Local Management field descriptions on page 119

Editing users

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

Note:

The `cust` and `admin` user IDs cannot be modified or deleted.

Procedure

1. Click **User Administration** > **Local Management**.
2. On the Local Management page, select the user whose details you must modify.
3. Click **Edit User**. The Local Management page displays details for the user.
4. In the **New Password** field, enter a new password.

   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.
5. In the **Confirm Password**, enter the same password.
6. In the **User Role** field, click the user role most appropriate for the user.
7. Click **Save** to save the modified user details.

Related Links

Local Management field descriptions on page 119

Deleting users

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

Note:

You can delete the default `cust` and `admin` users using this procedure. You must first create a user with the user role of Advanced Administrator and log in to System Platform Web Console using the login credentials of the new user.

Procedure

1. Click **User Administration** > **Local Management**.
2. On the Local Management page, select the user that you wish to delete.
3. Click **Delete User**.
4. In the dialog box, click **OK** to confirm the deletion of the user.

Related Links

Local Management field descriptions on page 119

Local Management field descriptions

Use the Local Management page to view, create, modify, or delete user accounts for System Platform.

Name	Description
User Id	Displays the login name of the user.
User Role	Displays the role of the user that defines access permissions. The options are: • Advanced Administrator • Administrator

Button	Description
Create User	Displays the Create User page under **User Administration** > **Local Management**.
Edit User	Displays the Edit User page under **User Administration** > **Local Management**.
Delete User	Allows an Advanced Administrator to remove System Platform access privileges associated with an existing user. The **Delete User** button is active only when you click the checkbox adjacent to the user ID in the initial Local Management summary page.

Related Links

Creating users on page 117
Editing users on page 118
Deleting users on page 118

Create User and Edit User field descriptions

Name	Description
User Id	Username for login access to the system. Conforms to the rules displayed when you click **Username Rules**.
User Password	The password of the user. Required for access to System Platform. Conforms to the rules displayed when you click **Password Rules**.
Confirm Password	The **User Password** value, reentered for confirmation of the initial password value.
User Role	Role of the user. Options are: • **Advanced Administrator** (read/write access to System Platform) • **Administrator** (read-only access to System Platform)

Button	Description
Save User	Saves the **User ID**, **User Password**, and **User Role** values entered when you create a new user or edit those values for an existing user.
Edit User	Allows an Advanced Administrator to modify the **User ID**, **User Password**, and **User Role** values of an existing user. The **Edit User** button is active only when you click the checkbox adjacent to the user entry in the initial Local Management summary page.
Delete User	Allows an Advanced Administrator to remove System Platform access privileges associated with an existing user. The **Delete User** button is active only when you click the checkbox adjacent to the user ID in the initial Local Management summary page.
Password Rules	Displays the minimum acceptable rules for creating a user password. **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.

Table continues…

Button	Description
	• Cannot include the user ID as part of the password. • Cannot be changed more than once a day.
Username Rules	Displays the minimum acceptable rules for creating a new User ID or for modifying an existing User ID.

Viewing administrators and super administrators

Use the **getusers** command to view System Platform administrators and super administrators. Only super administrators have permission to use this command.

Procedure

1. Access the System Domain or Console Domain command line.
2. Enter the **getusers** command with appropriate options and parameters.

Related Links

getusers command syntax on page 121

getusers command syntax

Syntax

```
getusers [-h] [-c] [-f <table | csv>] [-l] [-q] [-r <roles>] [-u <users>]
```

-h	Help.
-c	Clean up all generated query reports.
-f <table | csv>	Specify a report format. The default format is table. Alternatively, you can specify csv for a comma separated file.
-l	List all available roles. The roles are defined as **User Role** in the User Administration pages of the System Platform Web Console.
-q	Run in quiet mode. In quiet mode, command results are saved in the `/temp/getusers/data/` directory but are not displayed.
-r	List users and their groups for the specified roles. Use a comma as the delimiter. Replace any black space in the role name with an underscore character (_).
-u	List roles and groups for the specified user IDs. Use a comma as the delimiter. Replace any blank space in the user ID with an underscore character (_).

Description

The **getusers** command lists System Platform users who have a role of administrator or super administrator. Super administrators can enter this command from either the System Domain or Console Domain command line.

The results are also saved to a file for downloading or browsing. If **getusers** is used repeatedly, use the **getusers** `-c` command to prevent the excess build up of files on the system. Alternatively, the system will delete the files after 90 days. If the you need to save the files for longer than 90 days, copy them from the system before the 90-day limit is reached.

Example

getusers

```
QUERY REPORT:

=============



ROLE                                    GROUP
USER

-----------------------------------     -----------------------------------
-----------------------------------

Administrator                           vsp-admin
cust

Administrator                           vsp-admin
example_user2

Advanced_Administrator                  vsp-craft
admin

Advanced_Administrator                  vsp-craft
example_user1



* query results have been saved in /tmp/getusers/data/getusers_CDom_2013_01_03_13_37_25/
```

`getusers –f csv` displays results in a comma separated file.

`getusers -r Advanced_Administrator` displays users who have the Advanced Administrator role and the group to which they are assigned.

`getusers -r Administrator,Advanced_Administrator` displays users who have a role of Administrator or Advanced Administrator and the group to which each user is assigned.

`getusers -u cust` displays the role and group that is assigned to user ID cust.

`getusers -u admin,cust` displays the role and group that is assigned to user IDs admin and cust.

Considerations

- Only super administrators have permission to use this command.

- If **getusers** is used repeatedly, use the **getusers** `-c` command to prevent the excess build up of files on the system.

Files

Results of the getusers command are saved in the following files for downloading or browsing. The system will delete the files after 90 days if you do not delete them manually.

`temp/getusers/data/getusers_CDOM_<date and time>`, where <*date and time*> is in the format of year_month_day_hour_minute_second.

Related Links

Viewing administrators and super administrators on page 121

Changing your System Platform password

The Change Password option is available only for local users. Enterprise LDAP users cannot change their passwords from the System Platform Web Console.

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.

Procedure

1. Click **User Administration** > **Change Password**.
2. In the **Old Password** field, enter your current password.
3. In the **New Password** field, enter a new password.
4. In the **Confirm Password** field, reenter the new password.
5. Click **Change Password** to change the current password.

LDAP management

Authenticating System Platform users against an enterprise LDAP

Authentication against an enterprise LDAP

You can configure System Platform to authenticate System Platform users against an enterprise LDAP in addition to authenticating against the local System Platform LDAP. If you do so, users can enter either their enterprise user name and password or System Platform user name and password to log in to the System Platform Web Console.

If the Access Security Gateway (ASG) is present, System Platform attempts to authenticate a user against the Access Security Gateway (ASG). If the ASG is not present or if the login information does not match the ASG, System Platform attempts to authenticate the user against the local LDAP. If the login information does not match the local LDAP, System Platform attempts to authenticate the user against the enterprise LDAP.

Note:

You must have a user role of Advanced Administrator to enable or configure user authentication against an enterprise LDAP.

Related Links

Configuring authentication against an enterprise LDAP on page 124

Configuring authentication against an enterprise LDAP

Use this procedure to enable and configure authentication of System Platform users against your enterprise LDAP.

Procedure

1. Select **User Administration** > **Enterprise LDAP**.
2. Select **Enable Enterprise LDAP**.
3. Enter the appropriate information.
4. Click **Save Configuration**.
5. If the **TLS** checkbox is selected:
   a. Click **Upload Certificate** to replace the existing enterprise LDAP certificate.
   b. Click **Test Connection** to verify that you are able to connect to the Enterprise LDAP server.

   Note:

   The enterprise LDAP certificate was uploaded successfully if you can connect to the enterprise LDAP server.

Related Links

Enterprise LDAP field descriptions on page 125
Installing an enterprise LDAP certificate on page 72
Authentication against an enterprise LDAP on page 124

Enterprise LDAP field descriptions

The following table describes the fields on the Enterprise LDAP page. Use the Enterprise LDAP page to enable and configure authentication of System Platform users against your enterprise LDAP.

Enterprise LDAP

Name	Description
Enable Enterprise LDAP	Select this checkbox to enable external LDAP authentication. If you save the page without selecting this checkbox, the system saves the configuration without activating the Enterprise LDAP authentication.
TLS	Select this checkbox to use Transport Layer Security (TLS).
LDAP Server	Displays the Host name or IP address of the LDAP server.
User Attribute	Displays the LDAP attribute for the user. This is usually **cn** or **uid**.
Port	Displays the port number for the LDAP connection. • For TLS-based LDAP connection, the default port number is 636. • For non-TLS-based LDAP connection, the default port number is 389.
Base DN	Displays the Distinguished Name of the path where the user search will run. This value is used for connection authentication to the LDAP server. For example, `cn=admin,ou=sv,dc=avaya,dc=com`. This parameter is used to login to the LDAP server.
User DN	Displays the distinguished name of the LDAP user.
User Password	Displays the password of the LDAPuser.
Enable different group search base	Selecting this checkbox allows you to configure a different search base for searching and retrieving user Group information in a different part of the tree structure, relative to the User sub-tree. If the checkbox is selected, the system searches under the subtree specified by the **Group search**

Table continues…

Name	Description
	base DN instead of searching under the authenticating User's DN. If the checkbox is not selected: • The system searches user group information under the immediate subtree of the authenticating user's DN. • The system disables (grays out) fields in the panel, **Enable different group search base**.
Group search base DN	Displays the distinguished name of the different search base the system will use to search for the user's group information.
User substitution criteria	Criteria for substituting a value defined for the *%LDAP_USER%* variable, if an administrator has defined the value. There are two mutually exclusive settings for this parameter: • **Username Only** – Select this option to search for the user's group information by username alone. **Example** – if the Advanced Administrator filter is: `(&(cn=vsp-craft)(uniquemember=%LDAP_USER%))` and you select **Username Only**, the system substitutes the value of the Username or User ID of the authenticating user (0123456789) for the *%LDAP_USER%* variable before including the filter in the search for Group Information, shown as: (&(cn=vsp-craft)(uniquemember=0123456789)) • **Full User DN** – Select this option to cause the system to search for the user's group information by substituting the entire user DN for the variable *%LDAP_USER%* . (An Advanced Administrator must define this variable in an administrative filter.) **Example** – If the administrative filter is: `(&(cn=vsp-craft)(uniquemember=%LDAP_USER%))` and you select **Full User DN**, then the system substitutes the value of the DN of the authenticating user `(sid=0123456789,ou=internal,o=avaya,c=us)` for the `%LDAP_USER%` variable before including the filter in the search for Group Information, shown as:

Table continues…

Name	Description
	`(&(cn=vsp-craft) (uniquemember=sid=0123456789,ou=internal,o=avaya,c=us))`
Ldap Search scope	Select the LDAP scope to use when searching for a user's group information under the specified **Group search base DN**: • **Object_Scope**: Search only the entry at the specified **Group search base DN**. • **Onelevel_Scope**: Search all entries one level under the specified **Group search base DN**.
Attribute Map	Displays LDAP filters for the advanced administrator and administrator roles. A simple filter can be `memberOf=admin_Group`. A complex filter can contain multiple criteria such as: `(&(memberOf=vsp-craft) (userstatus=ACTIVE))`.
Advanced Administrator Filter	Displays the LDAP filter on a user to check if the user has System Platform advanced administrator role. For example, the LDAP filter `(&(memberOf=vsp-craft)(userstatus=ACTIVE))` will filter the active users who are the members of `vsp-craft`.
Administrator Filter	Displays the LDAP filter on a user to check if the user has System Platform administrator role. For example, the LDAP filter `(&(memberOf=vsp-admin)(userstatus=ACTIVE))` will filter the active users who are the members of vsp-admin.

Button	Description
Save Configuration	Save the Enterprise LDAP configuration.
Upload Certificate	Upload a Certificate for authentication with the LDAP server.
Test Connection	Test the connection to the LDAP server.

Related Links

Configuring authentication against an enterprise LDAP on page 124

Changing the System Platform LDAP password

The local LDAP directory stores login and password details for System Platform users. Use the LDAP login and password to log in to the local LDAP directory. This login does not have permissions to access the System Platform Web Console.

Procedure

1. Select **User Administration** > **Change LDAP Password**.
2. Enter the new password.

   Note:

   LDAP passwords must adhere to the following rules:

   - Include a minimum of 15 characters.
   - Include one or more characters from each category:
     - Numbers
     - Lowercase letters
     - Uppercase letters
     - Special characters
   - Include no more than five repeating characters.
   - Cannot include the user ID as part of the password.
   - Cannot be changed more than once a day.
3. Confirm the new password.
4. Click **Save** to save the new password.

Change LDAP Password field descriptions

Name	Description
New Password	A new password for the LDAP **manager**. The password must conform to the rules displayed when you click **Password Rules**.
Confirm Password	The new LDAP **manager** password, entered a second time for verification of the **New Password** value when you click **Change Password**.

Button	Description
Change Password	Changes the LDAP **manager** password to the value you entered on the Change LDAP Password page. For the change to succeed, the new and confirmed passwords must be identical and must conform to the rules displayed when you click **Password Rules**.
Password Rules	Displays the minimum acceptable rules for any new or modified LDAP **manager** password.

Managing the authentication file

Authentication file for ASG

The Access Security Gateway (ASG) ensures that Avaya Business Partners can access a customer enterprise communication solution in a secure manner. The Avaya Business Partners use a predetermined user ID while providing service at the customer site. This user ID is challenged by ASG and requires a proper response to login successfully. Only the Avaya Business Partners can respond to the ASG challenge. The passwords can only be used once.

ASG creates a set of customer-specific ASG keys that are stored in an authentication file. Customers must download and install the authentic files specially prepared for their sites to allow Avaya Business Partners to access their system.

Installing an authentication file

Caution:

Use caution when selecting the **Force load of new file** option. Certificate errors and login issues typically follow if you install the wrong authentication file.

Procedure

1. Select **User Administration** > **Authentication File**.
2. Click **Upload**.
3. 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.
4. Click **Install**.

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

Note:

If System Platform is configured for High Availability Failover, the authentication file propagates to the backup server.

Authentication File field descriptions

This page displays mainly read-only fields relevant to the Authentication file currently in use, and a button to upload a new replacement authentication file.

Name	Description
Force load of new file	Selecting this checkbox overrides validation of the AFID and date and time. 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. **Caution:** Use caution when selecting the **Force load of new file** option. Certificate errors and login issues typically follow if you install the wrong authentication file.

Button	Description
Upload	Uploads a new authentication file that you choose from your local system.

Chapter 5: Configuring High Availability

High Availability Introduction

About 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.

High availability operation incorporates a primary (preferred) server and a secondary (standby) server. Using the Web Console, an administrator can log on to the primary node to configure, start, stop, or remove High Availability operations on both nodes. While running on both nodes, the High Availability software continuously replicates data from the primary (active) node to the standby node. Should a switchover or failover event occur, the standby node becomes the new active node and provides continuity of Avaya Aura® solution services.

Note:

Avaya Aura System Platform High Availability does not support:

- IPv6 and cannot be configured with IPv6 addresses.
- Customer provided servers.

Template-driven High Availability:

The Avaya Aura® solution template you install determines the High Availability modes supported on your System Platform server. To determine exact High Availability mode support, see relevant topics in your solution documentation.

Related Links

Configuring locally redundant System Platform High Availability on page 144
Configure HA field descriptions on page 146

Node classification

Each server is a node in the High Availability configuration, as follows:

- *Active node* — The primary node, actively providing Avaya Aura® services in your network. The active node also replicates data to a standby node.
- *Standby node* — The secondary node, providing High Availability backup protection to the active node. The standby node becomes the active node in the event of a High Availability switchover or failover event.
- *Preferred node* — The node where you initially configure and start System Platform High Availability operations..

High Availability events

High Availability events vary in terms of type and characterization, as follows:

- **Planned (manual) switchover** — An administrator can perform a planned switchover when the active and standby nodes become synchronized and therefore contain the same data. The administrator performs this action typically to complete maintenance on the active server, causing it to become the new standby node during the maintenance action. This action triggers a *graceful shutdown* of node resources, where the system sequentially and safely shuts down key processes on the active node just prior to the actual switchover. No loss of data should occur during a planned switchover.
- **Preemptive (automatic) failover** — An automatic and graceful failover of the two nodes, typically triggered by ongoing detection of an intermittent hardware failure or transient shortages of node resources (for example, insufficient disk or memory space). Like the planned switchover, a preemptive failover requires full disk data synchronization across the active and standby servers. The preemptive failover triggers a graceful shutdown of resources on the active node, and a transition of all node resources to the standby node while incurring no loss of data during the failover interval.

  Note:

  System Platform does not support preemptive failover on customer provided hardware.
- **Unplanned (spontaneous) failover** — A non-graceful but instantaneous failover of nodes, commonly triggered by a loss of power, a sudden and severe hardware failure, or a sudden loss of connectivity. (The latter condition can cause *split-brain* operation. See Network link failure and recovery on page 136 for more information.)

Regardless of the High Availability event type, you can view the reason for failover on the High Availability page of the web console.

Locally Redundant High Availability

With System Platform Locally Redundant High Availablity (LRHA), primary and secondary servers are in close proximity, sufficient for replication of configuration and services data over a high-speed, point-to-point, Ethernet crossover cable. LRHA offers several modes of operation:

- Fast Reboot High Availability (FRHA mode)
- Machine Preserving High Availability (MPHA mode), working together with Live Migration High Availability (LMHA mode)

Note:

A solution administrator configures each virtual machine to run with a specific type (or mode) of High Availability protection, according to Avaya Aura solution template requirements. (Refer to the feature support information for your specific solution template.)

Some High Availability configurations enable the administrator to apply High Availability protection to a single virtual machine, while other configurations automatically impose the same mode of High Availability protection to multiple template (application) virtual machines, concurrently.

Fast Reboot High Availability (FRHA)

FRHA is the default High Availability protection mode for template (application) virtual machines running on an Avaya Aura® solution server. Once initialized, the High Availability software on the active node propagates this configuration to virtual machines on the standby node. FRHA continuously captures and propagates disk data from the active node to the standby node to allow for recovery from any future switchover/failover events. As implied by the name of this High Availability mode, any planned, preemptive, or unplanned switchover/failover event causes the standby node to become the new active node, and its virtual machines boot up to continue providing solution services in your network. There is a brief pause in operations associated with a node switchover/failover event, plus the time it takes for all virtual machines to boot on the new active server.

Machine Preserving High Availability with Live Migration

Currently designed for solution templates that have exactly one virtual machine, MPHA mode can provide failover protection for that VM. MPHA continuously captures and propagates both disk and memory data from the Active server to the Standby server. MPHA uses a memory checkpointing protocol for fast error detection, and consequently provides switchover/failover times much faster than those achieved using either FRHA.

MPHA works in conjunction with Live Migration High Availability (LMHA). If you configure a template virtual machine with MPHA protection, the system automatically applies LMHA protection to all standard System Platform virtual machines (Cdom and Services_vm). With basic behavior similar to FRHA, LMHA additionally provides live migration of Cdom and Services virtual machine operations from the active node to the standby node, with no boot delays on the standby node. LMHA continuously captures and propagates both disk and memory data from the Active server to the Standby server. LMHA switchover/failover times are generally faster than those achieved with FRHA protection.

Note:

- You must have an Avaya license to configure and use MPHA/LMHA.
- System Platform does not support MPHA mode on customer provided server hardware.

Locally Redundant High Availability mode comparisons

The following table summarizes and compares characteristics and behaviors of the four High Availability modes. Application and full solution template recovery behaviors depend on additional factors not discussed here. for more information.)

High Availability characteristic or behavior	Fast Reboot High Availability (FRHA)	Machine Preserving High Availability (MPHA)	Live Migration High Availability (LMHA)
Virtual Machine applicability	• All solution template virtual machines (except where a specific template disallows FRHA operation) • Services virtual machine (runs SAL gateway)	• Solution templates using a single virtual machine • Some solution templates disallow MPHA protection. • With MPHA applied to one template virtual machine, server standard virtual machines (Cdom and Services_vm) automatically acquire LMHA protection. • Only one template virtual machine per server can use MPHA protection. • System Platform does not support MPHA mode on customer provided server hardware.	• template virtual machine (user applications domain) • services_vm virtual machine (runs SAL gateway)
Data replication	Disk	Disk and memory	Disk and memory
Physical connection for data replication	CAT5A crossover cable from primary to secondary server	CAT6A crossover cable from primary to secondary server	CAT6A crossover cable from primary to secondary server. (LMHA operates exclusively with MPHA.)

Table continues…

High Availability characteristic or behavior		Fast Reboot High Availability (FRHA)	Machine Preserving High Availability (MPHA)	Live Migration High Availability (LMHA)
Network interface for data replication		1 Gb/sec.	10 Gb/sec.	10 Gb/sec.
Server resource cost		Nominal	High	Nominal
Recovery type (See High Availability events on page 132.)	**Planned switchover:**	Graceful	Continuous, uninterrupted execution of virtual machines	Graceful, with live migration of Cdom and Services virtual machines
	Preemptive failover:	Graceful	Continuous, uninterrupted execution of virtual machines	Graceful, with live migration of Cdom and Services virtual machines
	Spontaneous failover:	Non-graceful	Non-graceful, virtual machine execution continues from last machine state captured at the time of failover.	Non-graceful; LMHA reverts to FRHA behaviors
Failure detection interval		30 seconds	450 milliseconds	450 milliseconds
Split-Brain resolution		Embedded	Embedded	Embedded
Switchover/ failover times	**Planned switchover:**	5–6 minutes	200 milliseconds	2–4 seconds
	Preemptive failover:	5–6 minutes	200 milliseconds	2–4 seconds
	Spontaneous failover:	5–10 minutes	600 milliseconds to 1 minute, nominal	5–10 minutes. (LMHA reverts to FRHA behavior.)
Data loss	**Planned switchover:**	None	None	None
	Preemptive failover:	None	None	None
	Spontaneous failover	Some disk and/or memory losses possible during failover	Minimal disk and/or memory losses during failover	Limited disk and/or memory losses possible during failover. (LMHA reverts to FRHA behavior.)
End-user services loss	**Planned switchover**	5–6 minutes	500 milliseconds or less	450 milliseconds
	Preemptive failover:	5–6 minutes	500 milliseconds or less	450 milliseconds
	Spontaneous failover:	5–10 minutes	500 milliseconds or less	5–10 minutes. (LMHA reverts to FRHA behavior.)

Data capture and replication

With the System Platform High Availability feature, the active node:

- continuously captures individual snapshots of Virtual Machine disk and memory data (type of capture depends on the High Availability mode).
- continuously replicates (propagates) every snapshot of data to the standby node.

The two nodes become synchronized and ready for High Availability operation when they both contain exactly the same data. You can check the current state of node synchronization by viewing the High Availability page in the web console.

During initial synchronization, the disk data replication software propagates to the standby node any differences in disk data that existed just prior to establishment of connectivity between the two servers, plus any new changes ongoing since initial synchronization began. The replication software requires the standby server to commit and confirm all changes propagated by the active server. This process helps to ensure that both servers are running in a consistent (synchronized) state, which in turn enables the standby node to:

- assume the role of active server in the event of a High Availability switchover or failover event
- begin providing Avaya Aura® solution services to end-users.

Disk data propagation speed

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.

Data propagation during switchover or failover events

During any switchover or failover event, the two nodes reverse roles. Likewise, the direction of data propagation reverses, now replicating data from the new active node to the new standby node.

Replication link failure and recovery

If an interruption occurs in the data replication link, DRBD keeps track of disk changes that occurred up to the point of interruption. When the replication link recovers, DRBD propagates and synchronizes disk changes that occurred up to the time the link went down, in parallel with any new disk changes occurring in realtime following link recovery.

Network link failure and recovery

If all links between the two nodes fail and the nodes are unable to communicate, both nodes can become active at the same time. This unacceptable condition is called *split-brain*. Once both nodes are on the network again, another HA mechanism chooses one server to be the active node and the other server to be the standby node based on node health and other node arbitration factors.

Memory data replication

The system uses a memory checkpoint protocol to continuously capture, propagate, commit, and synchronize memory data snapshots (pages of memory) across the active and standby nodes. (Applies to MPHA mode only.)

High Availability recovery sequence

Node arbitration software on the standby node continuously monitors connectivity with the active node and other node and network behaviors. If system operating conditions become sufficiently adverse (diminished node and/or network health), the software triggers a node switchover (failover) event. The standby node now becomes the active node, where virtual machines, applications, and overall solution services recover in stages:

- Virtual machines restart first, depending mainly on data replicated from the active node, which in turn depends on each virtual machine's High Availability mode and current operational state.
- Applications (one per virtual machine) restart next, depending mainly on recovery of the underlying virtual machine and internal efficiencies of the application itself, for example, when a large and complex application recovers with slight delays after its host virtual machine has already recovered.
- The Avaya Aura® solution template recovers last, depending mainly on recovery of its underlying applications. For example, a solution template with only one or two efficient applications recovers more quickly than a template that includes larger and more complex or interdependent applications.

The full recovery time of an Avaya Aura® solution after a switchover/failover event depends on the collective recovery times of the underlying virtual machines, the applications they support, and the overall solution template itself.

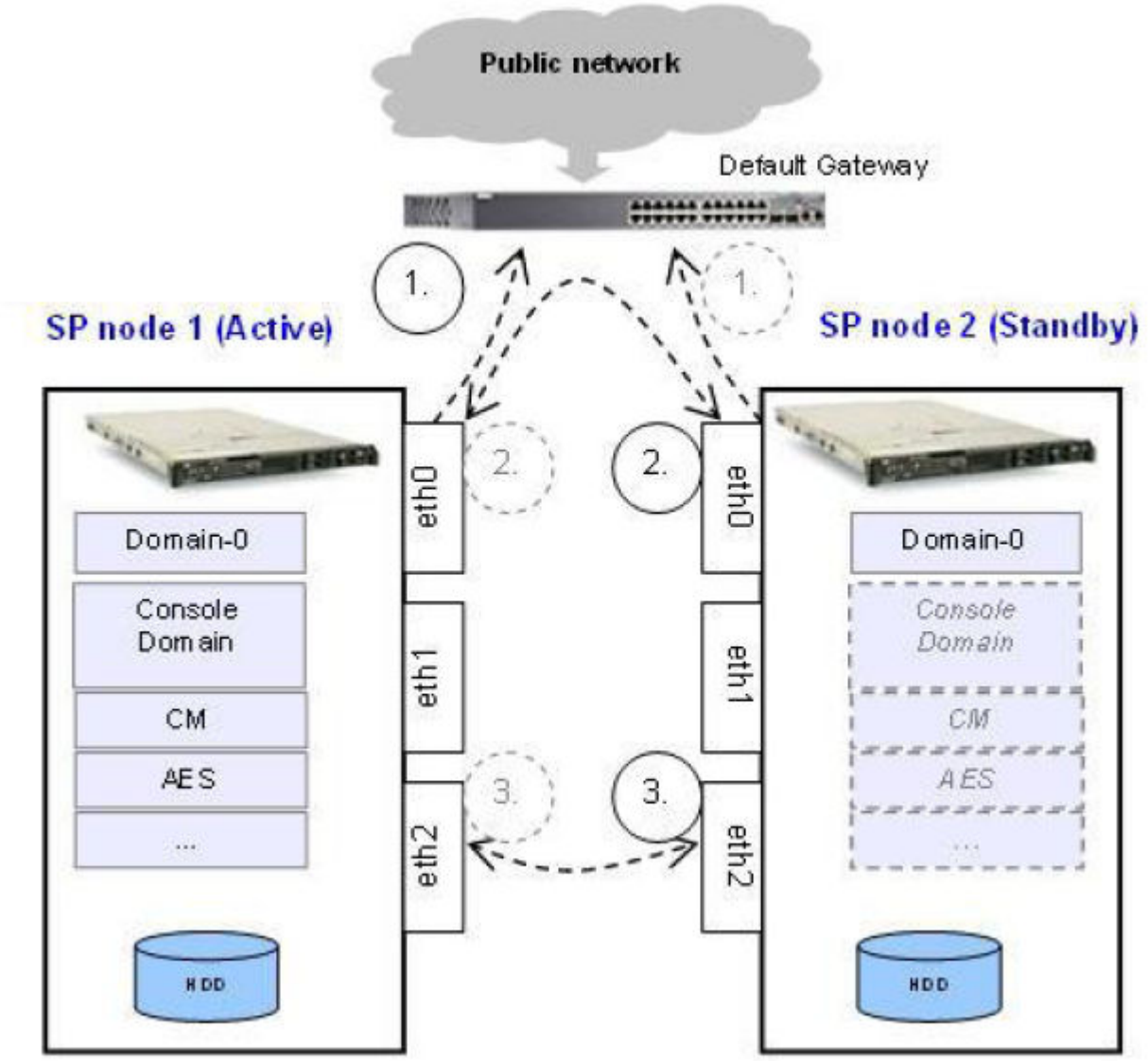
High Availability node arbitration

Node arbitration is a mechanism of the High Availability software to monitor node health and decide which of two nodes in a High Availability configuration should be the active node at any given time. All System Platform High Availability modes support automatic split-brain resolution as part of node arbitration. The node arbitration mechanism continually evaluates three main sources of information:

- ICMP Ping requests and responses between the each node and its local default gateway
- Heartbeat messaging and acknowledgements between the two nodes
- Hardware health information monitored on the two nodes

From these inputs, the software calculates an overall evaluation for each node, which in turn helps determine which of the two nodes is the preferred node. That node becomes the active node providing Avaya Aura® solution services to end-users.

The following figure illustrates the communication paths for node arbitration:



Key:

1. Public link: Ping
2. Public link: Heartbeat messaging
3. Disk data replication and Heartbeat messaging

ICMP Ping

Each node sends Ping requests periodically to its local default gateway device (and if needed, various solution servers), according to the requirements of your Avaya Aura® solution template and/or networking context. Each successful ping reply received by a node raises or maintains a node's evaluation. Each unsuccessful (or significantly delayed) ping reply lowers the node's evaluation. This mechanism helps to verify ongoing connectivity to the IP network, and helps to detect a Split Brain condition in your High Availability system.

Heartbeat messaging

Each node sends periodic heartbeat messages to the other node and expects valid acknowledgement messages.

The concurrent paths for heartbeat messaging are typically:

- *Public link:* eth0, node 1 to eth 0, node 2 by way of the IP default gateway (required). This is the public or “avpublic” link.
- *Crossover link:* eth2, node 1 to eth2, node 2 by way of the direct high-speed crossover cable connection. (If eth2 is unavailable, you can use any other Ethernet port of the required speed. You must use the same port on both nodes..)

Ping and heartbeat messaging can fail or have neutral effect on node evaluation and arbitration in various scenarios, such as those described in the table below:

Failure scenario	Outcomes
Either node detects a connectivity fault on the high-speed crossover link between the active and standby nodes.	Disk data replication over the crossover link has been interrupted, but each server is still aware of its counterpart as they communicate over the **avpublic** link. For this reason, the standby server is aware that the active server is still alive. No failover occurs because the node arbitration software determines that both nodes have been affected in the same way by the conditions in this scenario.
Either node detects a connectivity fault on the high-speed crossover link between the active and standby nodes. In addition, the active node detects a connectivity fault on its public link.	• The data replication path between the active and standby nodes has been interrupted. • The heartbeat messaging paths between the active and standby nodes have been interrupted. • The active node has lost one or more of its ping targets. • The standby node cannot ping the active node, but has not necessarily lost all of its ping targets. • The two servers cannot communicate. The active node cannot tell if the standby node is impaired, so the active node remains in its current state. Meanwhile, the standby node also cannot tell if the active node is impaired, and so assumes that the active node has failed. The standby node switches to active status. At this point, both nodes have active status. When the active node's public link is restored, the active and standby nodes communicate to determine if they are in a “split brain” condition. The “split brain resolver” software then determines which node will be the active node and, by default, the other node becomes the standby. High Availability data replication and node

Table continues…

Failure scenario	Outcomes
	synchronization resumes when the high-speed crossover link is restored.
The active node detects a connectivity fault over its public link.	• The active and standby nodes still have a data replication path between them by way of the high-speed crossover link. • The active and standby nodes continue to receive heartbeat messaging from each other by way of the high-speed crossover link. • The active node has lost one of more of its ping targets. • If three consecutive pings fail from the active node to its ping target (usually the default gateway), health of the active node has declined. If at the same time the standby node succeeds with its pings to that same ping target, the health of this node remains unchanged. These conditions trigger a failover because the node arbitration software detects impairment of the active node. After failover, the former active node (now the standby node) retains its last (diminished) evaluation by the node arbitration software until the connectivity fault over its public link recovers.
The standby node detects a connectivity fault over its public link.	• The active and standby nodes still have a data replication path between them by way of the high-speed crossover link. • The active and standby nodes continue to receive heartbeat messaging from each other by way of the high-speed crossover link. • The active node can still reach its ping targets. • The standby node has lost one or more of its ping targets. • Health of the standby node has declined, but no failover occurs. The active node retains its current operational status.

Server hardware health

Each node monitors and reports to the node arbitration software the relative health of its own hardware, for example, server internal operating temperature, available disk and memory resources, and other key indicators of server health.

No Automatic Failback

High Availability modes do not automatically migrate resources to the preferred node when system resources are running on the standby node when the preferred node becomes available again. If both servers are healthy, then running system resources on the preferred node offers no increased benefit.

Note:

To migrate resources back to the preferred node after a switchover or failover event, use the **Manual Interchange** (manual switchover) option on the High Availability page at a time least disruptive to solution users.

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.

Related Links

About High Availability on page 131

Configure HA field descriptions on page 146

High Availability field descriptions

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

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

Configure HA field descriptions

The following tables describe:

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

Virtual Machine Protection Mode configuration

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

Table continues…

VM Name	VM Description	Protection Mode
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.
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.

Related Links

Configuring locally redundant System Platform High Availability on page 144
About High Availability on page 131
Troubleshooting steps on page 177

High Availability start/stop

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 149
Stopping System Platform High Availability on page 150

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 149

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.

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 6: System Platform security

Command line login to System Domain and Console Domain

The `admin` user ID can access the system through the command line interface. The user can open an SSH session or directly connect a keyboard and monitor to the System Platform server to log in. The `cust` user ID cannot log in to the command line interface. An Avaya technical support person can log in to the system using the `craft` user ID and the ASG challenge/response mechanism.

Note:

It is not possible to directly access the system using the `root` and `sroot` user IDs. If it is required to log in using one of these user IDs, log in as an unprivileged user and run the `su` command to switch to either the `root` or `sroot` user ID. If you use the `root` user ID, you will enter the `root` password. In the case of the `sroot` user ID, you will use the correct response to the ASG challenge.

Firewall settings for IPv4

System Platform firewall rules on System Domain and on Console Domain are on by default.

Log in using the `root` user ID to perform this task.

Stopping firewall rules

Procedure

1. Log in to System Domain or Console Domain where you must stop the firewall rules.
2. Type `service firewall stop`
3. Log out of the system.

Starting firewall rules

Procedure

1. Log in to System Domain or Console Domain where you must start the firewall rules.
2. Type `service firewall start`
3. Log out of the system.

Displaying currently set firewall rules

Procedure

1. Log in to System Domain or Console Domain where you must display the firewall rules.
2. Type `service firewall status`
3. Log out of the system.

Logging IP packets blocked by firewall

Note:

All blocked IP packets are logged in the file `/var/log/vsp/vsp-rsyslog` on Console Domain. You can view these IP packets by using the command `dmesg` on Console Domain command line.

All IP packets blocked on System Domain are logged in the file `/var/log/messages` on the System Domain. You can view these IP packets by using the command `dmesg` on the System Domain command line.

Avaya advises logging of blocked IP packets only on rare occasions and for short time periods to prevent flooding of log files.

Procedure

1. Log in to System Domain or Console Domain where you must start the logging of IP packets blocked by the firewall.
2. Type `service firewall logging`
3. Log out of the system.

Stopping logging of IP packets blocked by firewall

Procedure

1. Log in to System Domain or Console Domain where you must stop the logging of IP packets blocked by the firewall.
2. Type `service firewall restart`
3. Log out of the system.

Firewall settings for IPv6

System Platform firewall rules on System Domain and on Console Domain are on by default.

Log in using the `root` user ID to perform this task.

Stopping firewall rules

Procedure

1. Log in to System Domain or Console Domain where you must stop the firewall rules.
2. Type `service firewallIPv6 stop`
3. Log out of the system.

Starting firewall rules

Procedure

1. Log in to System Domain or Console Domain where you must start the firewall rules.
2. Type `service firewallIPv6 start`
3. Log out of the system.

Displaying currently set firewall rules

Procedure

1. Log in to System Domain or Console Domain where you must display the firewall rules.
2. Type `service firewallIPv6 status`
3. Log out of the system.

Logging IP packets blocked by firewall

Note:

All blocked IP packets are logged in the file `/var/log/vsp/vsp-rsyslog` on Console Domain. You can view these IP packets by using the command `dmesg` on Console Domain command line.

All IP packets blocked on System Domain are logged in the file `/var/log/messages` on the System Domain. You can view these IP packets by using the command `dmesg` on the System Domain command line.

Avaya advises logging of blocked IP packets only on rare occasions and for short time periods to prevent flooding of log files.

Procedure

1. Log in to System Domain or Console Domain where you must start the logging of IP packets blocked by the firewall.
2. Type `service firewallIPv6 logging`
3. Log out of the system.

Stopping logging of IP packets blocked by firewall

Procedure

1. Log in to System Domain or Console Domain where you must stop the logging of IP packets blocked by the firewall.
2. Type `service firewallIPv6 restart`
3. Log out of the system.

Linuxshield installation and configuration

LinuxShield virus scan

LinuxShield is a virus scan utility that protects a Linux server from attacks by worms, viruses, and malicious code. The utility offers real-time, on-access virus scanning for Linux servers. Additional features of LinuxShield include:

- Behavior-based scanning: LinuxShield detects attack based on behavior rules. As a result, LinuxShield does not download signatures to identify and block malware (worms, virus, and malicious code) variants.
- Ability to detect malware hidden in archived files: LinuxShield can detect malware that is hidden in archived files.
- Cross-platform protection: LinuxShield protects enterprise systems comprising heterogeneous severs such as Windows and Linux servers.

Note:

System Platform runs a hardened Linux-based operating system and it is unlikely that any viruses or other types of malicious code will be able to penetrate the system. LinuxShield provides an additional layer of protection to an already secure system for the enterprises that have very high security requirements. Most systems will not install LinuxShield. Further, LinuxShield virus scan can affect system performance. Only administrators who have Linux server knowledge and experience should attempt install and configure LinuxShield when required.

Installing and configuring Linuxshield on System Domain

Procedure

1. Log in to System Domain through SSH.
2. Type `su - root`, and then type the password for the root user ID.
3. Type `cd /tmp`
4. Download the 64–bit version of McAfee Linuxshield™ software.
5. Install and configure McAfee Linuxshield™ as per the accompanying documentation.

   Note:

   During installation, set the YOUR_IP_ADDRESS field to the IP address of System Domain. Set the scanning schedule to daily during the configuration of McAfee Linuxshield™.

Installing and configuring Linuxshield on Console Domain

Procedure

1. Log in to Console Domain through SSH.
2. Type `su - root`, and then type the password for the root user ID.
3. Type `cd /tmp`
4. Download the 64–bit version of McAfee Linuxshield™ software.
5. Install and configure McAfee Linuxshield™ as per the accompanying documentation.

Note:

During installation, set the YOUR_IP_ADDRESS field to the IP address of Console Domain. Set the scanning schedule to daily during the configuration of McAfee Linuxshield™.

Files requiring the SUID and SGID bits set

Files requiring SUID and SGID bits set on System Domain

The following table lists the files that require the SUID or SGID bits set. The permissions, location, and ownership of these files must be documented with the IAO.

Permissions	Location	File name	Ownership
-rwsr-xr-x	/bin	umount	
-rwsr-xr-x	/bin	ping6	
-rwsr-x---	/bin	fusermount	
-rwsr-xr-x	/bin	ping	
-rwsr-xr-x	/bin	su	
-rwsr-sr-x	/opt/dell/srvadmin/oma/bin	omcliproxy	
-rwxr-sr-x	/usr/bin	ssh-agent	
---s--x--x	/usr/bin	sudo	
-rwsr-xr-x	/usr/bin	chage	
-rwsr-sr-x	/usr/bin	crontab	
-rws--x--x	/usr/bin	Xorg	
-rwsr-xr-x	/usr/bin	newgrp	

Table continues…

Permissions	Location	File name	Ownership
---s--x--x	/usr/bin	sudoedit	
-rws--x--x	/usr/bin	chsh	
-rwxr-sr-x	/usr/bin	write	
-rwsr-xr-x	/usr/bin	passwd	
-rws--x--x	/usr/bin	chfn	
-rwxr-sr-x	/usr/bin	cl_status	
-r-xr-sr-x	/usr/bin	wall	
-rwsr-xr-x	/usr/bin	gpasswd	
-rwsr-xr-x	/usr/libexec	libvirt_proxy	
-rwx--s--x	/usr/libexec/utempter	utempter	
-rwsr-xr-x	/usr/libexec/openssh	ssh-keysign	
-rws--x--x	/usr/sbin	userhelper	
-rwsr-xr-x	/usr/sbin	usernetctl	
-rwsr-x---	/lib64/dbus-1	dbus-daemon-launch-helper	
-rwsr-x---	/sbin	mount.ecryptfs_private	
-rwsr-xr-x	/sbin	unix_chkpwd	
-rwsr-xr--	/sbin	drbdsetup	
-rwsr-xr--	/sbin	drbdmeta	
-rwsr-xr-x	/sbin	umount.nfs	
-rwsr-xr-x	/sbin	mount.nfs4	
-rwxr-sr-x	/sbin	netreport	
-rwsr-xr-x	/sbin	pam_timestamp_check	
-rwsr-xr-x	/sbin	mount.nfs	
-rwsr-xr-x	/sbin	umount.nfs4	

Files requiring SUID and SGID bits set on Console Domain

The following table lists the files that require the SUID or SGID bits set. The permissions, location, and ownership of these files must be documented with the IAO.

Permissions	Location	File name	Ownership
-rwsr-xr-x	/bin	su	
-rwsr-xr-x	/bin	mount	
-rwsr-xr-x	/bin	ping6	

Table continues…

Permissions	Location	File name	Ownership
-rwsr-xr-x	/bin	ping	
-rwsr-x---	/bin	fusermount	
-rwsr-xr-x	/bin	umount	
-rwsr-xr-x	/usr/libexec	libvirt_proxy	
-rwsr-xr-x	/usr/libexec/openssh	ssh-keysign	
-rwxr-sr-x	/usr/bin	ssh-agent	
---s--x--x	/usr/bin	sudo	
-rwsr-xr-x	/usr/bin	chage	
-rwsr-sr-x	/usr/bin	crontab	
-rwsr-xr-x	/usr/bin	newgrp	
---s--x--x	/usr/bin	sudoedit	
-rws--x--x	/usr/bin	chsh	
-rwxr-sr-x	/usr/bin	write	
-rwsr-xr-x	/usr/bin	passwd	
-rws--x--x	/usr/bin	chfn	
-r-xr-sr-x	/usr/bin	wall	
-rwsr-xr-x	/usr/bin	gpasswd	
-rws--x--x	/usr/sbin	userhelper	
-rwsr-xr-x	/usr/sbin	usernetctl	
-rwsr-x---	/lib64/dbus-1	dbus-daemon-launch-helper	
-rwsr-xr-x	/sbin	umount.nfs4	
-rwxr-sr-x	/sbin	netreport	
-rwsr-xr-x	/sbin	mount.nfs4	
-rwsr-xr-x	/sbin	pam_timestamp_check	
-rwsr-xr-x	/sbin	umount.nfs	
-rwsr-xr-x	/sbin	mount.nfs	
-rwsr-xr-x	/sbin	unix_chkpwd	

Disabling booting from removable media

BIOS changes to disable booting from removable media

BIOS changes are required for each of the following server types to disable booting from removable media:

- S8510 (also known as Dell Poweredge 1950)
- S8800 (also known as IBM x3550 M2)
- S8300D

Disabling booting from removable media on S8510

Procedure

1. Upon booting, press the **F2** key to start the BIOS setup utility.

   Enter the setup password if needed.

2. From the menu, click **Boot Sequence**.

   A list of bootable devices will be displayed..

3. Select **Hard Drive** from the boot sequence list and press the **+** key to move it to the first position in the list.
4. Press the **Spacebar** to clear selection of all other devices such as CD-ROM and embedded NIC in the boot sequence list.
5. If a BIOS password has not been enabled, click **System Security** from the main menu and enter a password.
6. Press **Escape** to exit from the boot sequence list.
7. Click **Save changes**.

Disabling booting from removable media on S8800

Procedure

1. Upon booting, press the **F1** to start UEFI.

   Enter the setup password if needed.

2. From the menu, click **Boot Manager**.
3. In the **Boot Manager** screen, click **Change Boot Order**.
4. Select **Hard Drive** from the boot sequence list and press the **+** key to move it to the first position in the list.

5. Exit **Change Boot Order**.
6. Click **Delete Boot Option**.
7. Delete all boot options except **Hard Drive**.
8. Exit **Delete Boot Option**.
9. If a UEFI password has not been enabled, click **User Security** from the main menu and enter the admin password.
10. Press **Escape** to exit.
11. Click **Save Settings** to save your changes.
12. Press **Escape** to exit UEFI.
13. Boot the server.

Disabling booting from removable media on S8300D

Procedure

1. Enter the BIOS setup by performing the following steps:
   a. Power down the server.
   b. Take out the S8300D board.
   c. Connect 10-pin side of the serial console cable to the 10-pin header labeled “COM1” on the S8300D.
   d. Connect the DB-9 side of the serial console cable to the serial port of the services laptop
   e. Open a console terminal on the services laptop (speed: 115200, type: ANSI, Data bits: 8, Parity: none, Flow control: none)
   f. Insert the S8300D into the gateway to power up.
   g. When prompted on the serial console press the **Delete** key to enter the BIOS setup menu.
2. Enter a password by performing the following steps:
   a. Press the **Right Arrow** key until **Security** is selected at the top.
   b. Press the **Down Arrow** key to select **Change Supervisor Password**.
   c. Press the **Enter** key.
   d. Type the password.
   e. Type the same password to confirm.
   f. Press the **Escape** key.
   g. Press the **Right Arrow** to the Exit menu.
   h. Select **Save Changes and Exit**.

i. Press **OK** to confirm.

   The server will reboot.

3. Change the boot device by performing the following steps:
   a. Press the **Right Arrow** key until **Advanced** is selected at the top.
   b. Press the **Down Arrow** until **USB Configuration** is selected.
   c. Press the **Down Arrow** until **Legacy USB Support** is selected.
   d. Select **Disabled**.
   e. Press the **Escape** key.
   f. Press the **Right Arrow** to the Exit menu.
   g. Select **Save Changes and Exit**.
   h. Press **OK** to confirm.

      The server will reboot.

Disabling booting from removable media on S8300E

Procedure

1. Enter the BIOS setup by performing the following steps:
   a. Shut down the S8300E server by pressing the **Shut down** button on the faceplate.
   b. Take out the S8300E board when the OK-to-shutdown LED is on solid.
   c. Connect 10-pin side of the serial console cable to the 10-pin header labeled “COM PORT” on the S8300E. Ensure that pin one on the cable matches pin one on the board.
   d. Connect the DB-9 side of the serial console cable to the serial port of a laptop/PC.
   e. Open a console terminal on the services laptop (speed: 115200, type: VT100, Data bits: 8, Parity: none, Flow control: none)
   f. Insert the S8300E into the gateway to power up.
   g. When prompted on the serial console, press the **Delete** key to enter the BIOS setup menu.
2. Enter a password by performing the following steps at the BIOS menu:
   a. Press the **Right Arrow** key until **Security** is selected at the top.
   b. Press the **Down Arrow** key to select **Administrator Password**.
   c. Press the **Enter** key.
   d. Type the password.
   e. Type the same password to confirm.
   f. Press the **Right Arrow** to the Save & Exit menu.

g. Select **Save Changes and Reset**.
h. Press **Yes** to confirm.

   The server will reboot.

3. Change the boot device by performing the following steps at the BIOS menu:
   a. Press the **Right Arrow** key until the **Boot** menu is selected at the top.
   b. Press the **Down Arrow** until **USB Configuration** is selected.
   c. Press the **Down Arrow** until **USB Boot Support** is selected.
   d. Press the **Enter** key to select.
   e. Use the **Down Arrow** to select **Disabled**.
   f. Press the **Enter** key.
   g. Press the **Right Arrow** to the Save & Exit menu.
   h. Select **Save Changes and Reset**.
   i. Press **Yes** to confirm.

      The server will reboot.

Avaya port matrix

Port summary

- Ingress: This indicates data flowing into the product defined in the matrix.
- Egress: This indicates data flowing away from the product defined in the matrix.
- Port(s): This is the layer-4 port number. Valid values are in the range of 0 – 65535. All ports listed are the destination ports.
- Network/Application Protocol: This is the name associated with the layer-4 protocol and layers-5-7 application.
- Optionally Enabled / Disabled: This field indicates whether customers can enable or disable a layer-4 port changing its default port setting. Valid values are 'Yes' and 'No'.
  - No means the default port state cannot be changed (that is, enabled or disabled).
  - Yes means the default port state can be changed and that the port can either be enabled or disabled.
- Default Port State: A port is either open, closed, filtered, or N/A.
  - Open ports will respond to queries.

- Closed ports do not always respond to queries and are only listed when they can be optionally enabled.
- Filtered ports can be open or closed. Filtered UDP ports will not respond to queries. Filtered TCP will respond to queries, but will not allow connectivity.
- N/A is used for the egress default port state since these are not listening ports on the product.

Security port matrix for Virtual Server Platform on Domain 0

	Ports	Network/ Application Protocol	Optionally Enabled/ Disabled?	Default Port State	Notes	Column Descriptions
Ingress						Ingress -- data flows coming into the product. Egress -- data flows leaving the product. Port(s) – Logical number(s) at OSI layer-4. Valid values are in the range 0 – 65535. Network / Application Protocol – Top layer protocol, that is, RTP, HTTP, etc. Optionally Enabled/ Disabled – indicates whether customers can enable or disable a layer-4 port changing its default port setting. Valid value is 'Yes' or 'No'. Default Port State: Valid Values include: Open, Closed, Filtered or N/A
1	1	ICMP	No	Open		
2	22	UDP/SSH	No	Open		
3	22	TCP/SSH	No	Open		
4	80	UDP/HTTP	No	Open	Redirects to CDom from service port.	
5	80	TCP/HTTP	No	Open	Redirects to CDom from service port.	
6	389	UDP/LDAP	No	Open		
7	389	TCP/LDAP	No	Open		
8	636	UDP/LDAPS	No	Open		
9	636	TCP/LDAPS	No	Open		
10	6659	TCP/ COLLECTD	No	Open		
Egress						
1	All		No	Open		
2	6660	TCP/ COLLECTD	No	Open		
3	22	TCP/SSH	No	Open		
4	53	TCP/DNS				
Other						
1	123	NTP	Yes	Open		

Note:

The port numbers are assigned by IANA (Internet Assigned Numbers Authority) and can be found at http://www.iana.org/assignments/port-numbers.

Security port matrix for Virtual Server Platform on CDom

	Ports	Network/ Application Protocol	Optionally Enabled/ Disabled?	Default Port State	Notes	Column Descriptions
Ingress						Ingress -- data flows coming into the product. Egress -- data flows leaving the product. Port(s) – Logical number(s) at OSI layer-4. Valid values are in the range 0 – 65535. Network / Application Protocol – Top layer protocol, that is, RTP, HTTP, etc. Optionally Enabled/ Disabled – indicates whether customers can enable or disable a layer-4 port changing its default port setting. Valid value is 'Yes' or 'No'. Default Port State: Valid Values include: Open, Closed, Filtered or N/A
1	1	ICMP	No	Open		
2	22	UDP/SSH	No	Open		
3	22	TCP/SSH	No	Open		
4	80	UDP/HTTP	No	Open		
5	80	TCP/HTTP	No	Open		
6	161	SNMP DISCOVERY				
7	162	UDP/SNMPTRAP	No	Open		
8	443	UDP/HTTPS	No	Open		
9	443	TCP/HTTPS	No	Open		
10	514	UDP/SYSLOG	No	Open		
11	7443	TCP	No	Open		
12	8080	UDP/HTTP-ALT	No	Open		
13	8080	TCP/HTTP-ALT	No	Open		
14	8162	UDP	No	Open		
15	8443	UDP/PCSYNC-HTTPS	No	Open		
16	8443	TCP/PCSYNC-HTTPS	No	Open		
17	9443	TCP/HTTPS	No	Open		
18	9443	UDP/HTTPS	No	Open		
19	52233	UDP/”WEBLM”	No	Open		
20	52233	TCP/”WEBLM”	No	Open		
21	25826	UDP/COLLECTD	No	Open		
Egress						
1	All		No	Open		
2	53	DNS	No	Open		

Note:

The port numbers are assigned by IANA (Internet Assigned Numbers Authority) and can be found at http://www.iana.org/assignments/port-numbers.

Chapter 7: Log harvest utility

Avaya provides the log harvest utility that collects logs and command line outputs and prepares a compressed file. You can send this compressed file to an Avaya Partner to investigate the System Platform performance in your enterprise.

Note:

The log harvest utility is installed on System Domain and Console Domain at `/opt/avaya/vsp/bin` during the System Platform installation.

Using the log harvest utility

To use the log harvest utility, log in to either System Domain or Console Domain using SSH. The log harvest utility collects logs and command line outputs and prepares a compressed file with the filename as `vsp_logs_`*`hostname`*`_YYMMDDHHMM.zip`. In the filename, *`hostname`* is the short hostname of either System Domain or Console Domain from where the log harvest utility was run and *`YYMMDDHHMM`* is the timestamp when the compressed file created.

Note:

Use the log harvest utility from Console Domain. When run from Console Domain, the log harvest utility collects logs and command line outputs from both System Domain and Console Domain. When run from System Domain, the log harvest utility collects logs and command line outputs only from System Domain.

Compressed file structure

The compressed file has `files` and `cmds` categories in which respectively the logs and the command line outputs are collected. The structure of the compressed file is as follows:

```
vsp_logs_hostname_YYMMDDHHMM
      /files
      /cmds
      /dom0.vsp
         /files
         /cmds
      /dom0-standby.vsp
         /files
         /cmds
```

In the above structure, if the log harvest utility is run from Console Domain, the logs and command line outputs will be collected under the `/files` and `/cmds` directories immediately following the filename. The logs and command line outputs for System Domain will be collected under the subdirectories under the `/dom0.vsp` directory. The `dom0-standby.vsp` directory will be present if High Availability Failover is configured and will have the logs and command line outputs for System Domain of the secondary server.

If the log harvest utility is run from System Domain, the logs and command line outputs will be collected under the `/files` and `/cmds` directories immediately following the filename and the `/dom0-standby.vsp` directory will be present only if High Availability Failover is configured. There will not be log and command line outputs collected for Console Domain.

The log harvest utility retains the location information of the log files under the `files` directories. For example, the `/var/log` directory from Console Domain will show up as `…/files/var/log` and that from System Domain will show up as `…/dom0.vsp/files/var/log`.

The `cmds` directories contain files that are named after the commands used to produce the output. Each output file has the command at its beginning.

Related Links

Using the log harvest utility on page 168

Using the log harvest utility

Procedure

1. Log in to System Domain or Console Domain from where you must run the log harvest utility.

   Note:

   Use the log harvest utility from Console Domain. When run from Console Domain, the log harvest utility collects logs and command line outputs from both System Domain and Console Domain. When run from System Domain, the log harvest utility collects logs and command line outputs only from System Domain.

2. Type `su - root`, and then type the password for the root user ID.
3. Type the password of the `root` user ID.
4. Type `getlogs`
5. Log out of the system.

Related Links

Log harvest utility on page 167

Chapter 8: Troubleshooting

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/
```

Checking RAID status

raid_status command

Use **`raid_status`** to display the server RAID (Redundant Array of Independent Disks) controller status.

Procedure

1. Log in to Domain-0 as root.
2. Enter `raid_status` with one or more of the following parameters:

   `-h`: Displays the help message (usage statement)

   `-v`: Verbose output, displays all RAID Controller data

`-s`: (default) Short output, displays one-line status

`-p`: Displays physical disk drive data, use with `-v` or `-s`

`-p -s`: (default) Displays physical disk drive data, short output form

`-p -v`: Displays physical disk drive data, verbose output form

`-r`: Returns 0 if the server supports RAID

Example

```
raid_status -h
raid_status [-s|-v]
raid_status [-s|-v] -p
raid_status -r
```

Note:

You cannot specify the `-v -s` options together.

Virtual machine has no connectivity outside after assigning dedicated NIC support

Troubleshooting steps through System Domain (Dom-0)

Procedure

1. Verify the pci ID entry is in the `/etc/rc.local and /etc/modprobe.conf` files.
2. Verify the pci ID is bound properly to the pciback driver.
3. Verify the directory `/sys/bus/pci/drivers/pciback` exists.
4. Check if the eth0 on the virtual machine is available and the IP Address is assigned using the command `ifconfig –a`.
5. Check if the MAC Address that is assigned to the virtual machine eth0 is a physical MAC Address using the command `ifconfig –a`.
6. Verify there are no error messages displayed when you enter the command **`modinfo`** *bnx2* (where *bnx2* is a driver name).

Troubleshooting steps through System Platform Web Console

Procedure

1. Verify the Ethernet cable is connected on the correct Ethernet port, for example, eth3.
2. Shutdown the virtual machine and restart it from System Platform Web Console.

General issues with the system and contacting support

Troubleshooting steps

System Platform provides a script (`getlogs`) that combines configuration files, log files, and system status information into a compressed file (`vsp_logs_<hostname>_<date_time>.tbz`). If you run the `getlogs`command from an SSH session with the console domain, `getlogs` also obtains this information from Domain-0. If System Platform High Availability has been configured, you can run `getlogs` from Domain-0 of the primary and secondary nodes to create the compressed file for each node. You can then provide the file for one node (or for the primary and secondary HA nodes) to your support technician for help with troubleshooting various server or solution issues.

Procedure

1. To create the compressed file, log on to the console domain and run the **`getlogs`** command.

   This action creates `vsp_logs_<hostname>_<date_time>.tbz` in the current directory.

2. If console domain is inaccessible, log on to Domain-0 and run the **`getlogs`** command. If System Platform High Availability has been configured, run the command from Domain-0 of the primary and secondary HA nodes.

Provide the file to your support technician.

Issues when configuring High Availability Failover

Cannot establish communication through crossover network interface

Troubleshooting steps

Procedure

1. Ensure that the crossover cable is properly connected to the same interface on both machines.
2. Verify that you selected the correct interface for configuring the High Availability Failover.

Local IP address provided

Troubleshooting steps

Procedure

Verify that you specify the remote console domain IP address when configuring High Availability Failover.

Standby first-boot sequence is not yet finished

Troubleshooting steps

You provided the IP address of the remote console domain when the initial start-up procedure was not yet completed.

Procedure

Wait for the start-up process to complete and try configuring High Availability Failover again later.

Note:

The process can take up to 5 minutes to finish from the time you log in into System Domain (Dom-0).

Cluster nodes are not equal

Troubleshooting steps

When you set up High Availability Failover, you added the weaker server and then the preferred server to the system.

Procedure

Do one of the following:

- Use another server that has the same or better configuration parameters.
- Swap the servers so that the weaker server becomes preferred node.

Note:

The standby server cannot have less memory, fewer number of processors, or less total or free disk space than the active server.

A template is installed on remote node

Troubleshooting steps

A solution template is installed on the standby node.

Note:

System Platform prevents setup of High Availability Failover when a template is installed on the standby node.

Procedure

Do one of the following:

- Delete the solution template from the standby node, or
- Reinstall System Platform on the standby node and retry configuration of High Availability Failover.

NICs are not active on both sides

Troubleshooting steps

The public or crossover network interface is not available on one of the nodes. Both public and crossover network interfaces must be available and properly working on both nodes.

Procedure

Ensure you have enough network interfaces on the system.

Cannot establish High Availability network interface

Troubleshooting steps

The crossover network interface cannot be setup on one of the nodes. The crossover network interface must be available and working properly on both nodes.

Procedure

Ensure that the network interface is not enslaved to the network bridge on the system.

Issues when starting High Availability Failover

Different platform versions on cluster nodes

Troubleshooting steps

The System Platform versions are not the same on both cluster nodes. System Platform prevents the start of High Availability Failover if the versions are not the same on both cluster nodes.

Procedure

Both machines must be installed with the same version of System Platform. If you install a patch, ensure that it is installed on both machines.

A template is installed on remote node

Troubleshooting steps

Note:

System Platform prevents the start of High Availability Failover when a template is installed on the standby node.

Procedure

Delete the solution template from the standby node.

Resources are not started on any node and cannot access the Web Console

Troubleshooting steps

High Availability Failover uses the default network gateway as a ping target to:

- check the ability of each machine to communicate with the network
- compute the score of each machine for running resources

If the gateway is not replying to the ping requests, System Platform cannot designate either node as the active node because the score of both nodes is equal. As a result, no resources are activated on either node.

Procedure

Verify that your default network gateway is able to receive and reply to ICMP echo requests from both System Platform nodes.

Cannot access the Web Console after starting High Availability Failover

Troubleshooting steps

Procedure

1. Check `/var/log/vsp/vspha.log` log file for details.
2. Run the **`getlogs`** command on the preferred node.
3. Provide the resulting `vsp_logs_<hostname>_<date_time>.zip` compressed file to your support technician.

Active server fails

Troubleshooting steps

Procedure

1. Verify that the crossover connection is working properly.
2. Disconnect the main network cable from the active server.
3. Verify that the standby server becomes active.

Data switch fails

Troubleshooting steps

Note:

This procedure does not apply to High Availability configurations that do not use a local crossover connection.

Procedure

1. Ensure that the crossover connection is working properly.
2. Disconnect the main network cable from both the active and standby server.

3. Reconnect the cables after few minutes. The previously active server should remain as active.

High Availability does not work

Troubleshooting steps

Procedure

1. Remove the SAMP board from the S8510 server before installing System Platform.
2. Ensure that the Dual NIC card is connected to the correct port for High Availability operation.

Start LDAP service on System Domain (Dom-0)

Troubleshooting steps

If the system reboots without first performing the shutdown procedure (for example, a power outage), the LDAP might not start on the next boot-up sequence. In that case, all users that are stored in LDAP database will not be able to log in.

Procedure

1. Log in to the system console as a user that is not using LDAP credentials.
2. Run the following commands:

```
# su -
# cd /var/lib/ldap
# slapd_db_recover -v
# service ldap restart
```

System Platform Web Console not accessible

Troubleshooting steps

Procedure

1. Check the internet connection.
2. Ensure that the Web address is correct.

3. Check proxy settings in your browser.

Restarting High Availability Failover after one node has failed

Troubleshooting steps

Note:

This procedure is service-disruptive. You must plan your activities accordingly.

All services are still running on the preferred node. Use this procedure to restart High Availability Failover after the standby node is reinstalled with the same version of System Platform as the currently active node.

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

Procedure

1. Log in to the System Platform Web Console on the active node.
2. Click **Server Management** > **High Availability**.
3. Click **Stop HA** and confirm the displayed warning.
4. Click **Server Management** > **High Availability**.
5. Click **Remove HA** and confirm the displayed warning.
6. Click **Configure HA**.
7. On the Configure HA page, enter the appropriate information to configure High Availability operation for all template virtual machines.
8. Click **Create**.
9. After the system finishes creating the High Availability configuration, click **Start HA** and confirm the displayed warning.
10. Click **Server Management** > **High Availability**.

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

Related Links

Configure HA field descriptions on page 146

Re-enabling failed standby node to High Availability Failover

Related Links

Re-enabling failed preferred node to High Availability Failover on page 178
System Platform backup on page 97

Troubleshooting steps

Note:

This procedure is service-disruptive. You must plan your activities accordingly.

All of the services are still running on the preferred node. To re-enable the standby node after it was reinstalled with System Platform of the same version as the currently active node, perform the following steps:

Procedure

1. Log in as admin user to the Web Console of the active node.
2. Select **Server Management** > **High Availability**.
3. Click **Stop HA** and confirm the displayed warning.
4. Select **Server Management** > **High Availability**.
5. Click **Remove HA** and confirm the displayed warning.
6. Click **Configure HA**, and enter the appropriate information about the reinstalled standby node.
7. After the system finishes creating the High Availability configuration, click **Start HA** and confirm the displayed warning.

Re-enabling failed preferred node to High Availability Failover

Related Links

Re-enabling failed standby node to High Availability Failover on page 178
System Platform backup on page 97

Troubleshooting steps

All of the services are running on the standby node. The resolution could differ in the following cases:

- a new server must be re-enabled into the HA system, or
- the previous preferred machine with a new primary network card (the card with eth0 and eth1 NICs) must be re-enabled

If you plan to re-enable the machine into the HA system, the process is exactly the same as re-enabling the failed standby node. Refer to the Re-enabling failed standby node to High Availability Failover section for more information.

To re-enable the previously used preferred node with the same primary network card, additional steps are required that are not available on the System Platform Web Console. Contact Avaya Support to assist you with resolving this condition.

Important:

Do not try to reinstall the failed node with System Platform on the same network as the currently active node. The installation will fail. If you already reinstalled the machine, you will have to reinstall it again with assistance from Avaya Support.

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.

Chapter 9: Fault detection and alarming

Hardware fault detection and alarming

System Platform uses a combination of Intelligent Platform Management Interface (IPMI) and RAID tools to monitor server hardware operation. System Platform periodically uses IPMI to query sensor data, and generates an alarm for each sensor that is in the critical range. The set of sensors varies by server type. System Platform also monitors chassis status. If an alarm is generated, the text provided in the alarm provides a description of the sensor found to be in the critical range or of the chassis fault. The following table illustrates typical alarm texts that are generated for sensor and chassis-type alarms.

Alarm type	Alarm text
Sensor	Detected non-ok component in Sensor Data Repository (SDR): component=<component>, id=<id>, type=<type>, sensor reading=<reading>, status=<status> <component> is unique by server type (refer to information on monitored sensors for each server type). Example: Detected non-ok component in Sensor Data Repository (SDR): component=Planar 3.3V (0x16), id=7.1 (System Board), type=Voltage, sensor reading=3.294 (+/- 0) Volts, status=Lower Critical
Chassis	Detected chassis status fault = <fault>, state=<state> <fault>is listed under “Monitored chassis status" for each server type. Example: Detected chassis status fault = Cooling/Fan Fault, state = true

For a sensor alarm type, the information provided in the alarm string is essentially the same information provided by IPMI. Using the example above, **`ipmitool`** can display full detail as shown below:

```
[root@mesaverde1 log]# ipmitool sensor get "Planar 3.3V"
Locating sensor record...
Sensor ID              : Planar 3.3V (0x16)
Entity ID             : 7.1
Sensor Type (Analog)  : Voltage
Sensor Reading        : 3.294 (+/- 0) Volts
Status                : Lower Critical
Lower Non-Recoverable : na
```

```
Lower Critical        : 3.294
Lower Non-Critical    : na
Upper Non-Critical    : na
Upper Critical        : 3.564
Upper Non-Recoverable : na
Assertion Events      : lcr-
Assertions Enabled    : lcr- ucr+
Deassertions Enabled  : lcr- ucr+
```

The sensor ID in this example (`Planar 3.3V` in the output example above) is the *component* in the alarm string.

RAID tools constantly monitor RAID operation and will create an alarm when a problem is detected. The RAID monitoring tools differ by server type. Therefore, server-specific alarms are described separately.

Fault types

IPMI can detect two generalized fault types, namely, sensor-related and chassis status-related faults for various server types. This section presents information on the fault types for S8510 and S8800 servers. The information provided here should not be considered exhaustive, as server hardware and sensors vary over time. Further, a firmware update can update the list of monitored sensor-related faults at any time.

Check your vendor's documentation to understand the implementation of monitored sensor-related faults.

For HP DL360 G6

The monitored sensor-related faults for HP DL360 G6 server are as follows:

- VRM 1
- VRM 2
- UID Light
- Int. Health LED
- Ext. Health LED
- Power Supply x (where x is 1 or 2, depending on the number of power supplies)
- Fan Block y (where y is 1, 2, 3, 4)
- Fans
- Temp n (where n is 1 – 28)
- Power Meter
- Memory
- RAID backup battery

The monitored chassis-related faults for HP DL360 G6 server are as follows:

- Power Overload
- Main Power Fault
- Power Control Fault
- Drive Fault
- Cooling/Fan Fault

Currently, HP DL360 G6 does not support the RAID alarms.

Message	Note
Physical drive failed: <location> of <controller>	<location> • Port [Number] • Port [Type][Number] Box [Number], where Type = I for internal, E for external <controller> • Embedded Array Controller • Array Controller in slot [Number] • Array Controller in slot [unknown] For example: Physical drive failed: Port 1I Box 1 Bay 3 of Embedded Array Controller
Physical Drive Status Change: <location> of <controller>. Status is now <status>	<location> • Port [Number] • Slot [Number] Port [Type][Number] Box [Number], where Type = I for internal, E for external <controller> • Embedded Array Controller • Array Controller in slot [Number] • Array Controller in slot [unknown] <status> • OK • Failed • Unconfigured • Interim Recovery • Ready For Rebuild • Rebuilding • Wrong Physical Drive Replaced

Table continues…

Message	Note
	• Physical Drive Not Properly Connected • Hardware Overheating • Hardware Overheated • Expanding • Not Available • Queued For Expansion • Unknown For example: Physical Drive Status Change: Slot 0 Port 1I Box 1 Bay 3. Status is now Failed
Logical drive [Number] of <controller>, has changed from <old status> to <new status>	<controller> • Embedded Array Controller • Array Controller in slot [Number] • Array Controller in slot [unknown] <status> • OK • Failed • Unconfigured • Interim Recovery • Ready For Rebuild • Rebuilding • Wrong Physical Drive Replaced • Physical Drive Not Properly Connected • Hardware Overheating • Hardware Overheated • Expanding • Not Available • Queued For Expansion • Unknown For example: Logical drive 1 of Embedded Array Controller, has changed from status Interim Recovery to Failed

Table continues…

Message	Note
Logical drive [Number] of <controller>, is in a FAILED state but has one or more drive replacements and is ready to go to OK. However, this will not happen until an Accepted Media Exchange command is issued to the logical drive.	<controller> • Embedded Array Controller • Array Controller in slot [Number] • Array Controller in slot [unknown] For example: Logical drive 1 of Embedded Array Controller, is in a FAILED state but has one or more drive replacements and is ready to go to OK. However, this will not happen until an Accepted Media Exchange command is issued to the logical drive.
Logical drive [Number] of <controller>:I/O request fatal error.	<controller> • Embedded Array Controller • Array Controller in slot [Number] • Array Controller in slot [unknown] For example: Logical drive 1 of Embedded Array Controller: I/O request fatal error.
Logical Drive Status Change: Slot [Number], Drive [Number]. Status is now <status>	<status> • OK • Failed • Unconfigured • Interim Recovery • Ready For Rebuild • Rebuilding • Wrong Physical Drive Replaced • Physical Drive Not Properly Connected • Hardware Overheating • Hardware Overheated • Expanding • Not Available • Queued For Expansion • Unknown For example: Logical Drive Status Change: Slot 0, Drive: 1. Status is now Interim Recovery.

See the HP ProLiant Servers Troubleshooting Guide at http://www.hp.com/ for more information on troubleshooting and fault resolution.

For Dell R610

The monitored sensor-related faults for the Dell R610 server are as follows:

- Temp (processor 1, processor 2, power supply 1, power supply 2)
- Ambient Temp
- FAN MOD xx RPM (where xx is 1A, 1B, 2A, 2B, etc.)
- Current 1, 2 (sensor for each power supply)
- Voltage 1, 2 (sensor for each power supply)
- System Level
- RAID backup battery

The monitored chassis-related faults for the Dell R610 server are as follows:

- Power Overload
- Main Power Fault
- Power Control Fault
- Drive Fault
- Cooling/Fan Fault

The RAID alarms for the Dell R610 server are as summarized below:

Storage Service EventID:	Note
2048	Device failed
2049	Physical disk removed
2056	Virtual disk failed / Virtual disk consistency check failed
2057	Virtual disk degraded
2076	Virtual disk failed / Virtual disk consistency check failed
2080	Physical disk Initialization or rebuild fail
2083	Physical disk Initialization or rebuild fail
2102	Temperature exceeded the maximum failure threshold
2103	Temperature dropped below the minimum failure threshold
2163	HDD rebuild completed with error(s)
2169	Controller battery must be replaced
2268	Storage Management has lost communication with the controller
270	Physical disk Initialization or rebuild fail
2272	Patrol Read found an uncorrectable media error
2273	A block on the physical disk has been punctured by the controller

Table continues…

Storage Service EventID:	Note
2282	Hot spare SMART polling failed
2289	Multi-bit ECC error on controller DIMM
2299	Bad PHY or physical connection
2307	Bad block table is full. Unable to log block
2320	Single bit ECC error. The DIMM is critically degraded
2321	Controller DIMM is critically degraded
2340	The background initialization (BGI) completed with uncorrectable errors
2347	Rebuild failed due to errors on the source or target physical disk
348	Rebuild failed due to errors on the source or target physical disk
2349	A bad disk block could not be reassigned during a write operation
2350	Unrecoverable disk media error during the rebuild or recovery

For S8510

The monitored sensor-related faults for the S8510 server are as follows:

- Temp (processor 1, processor 2, power supply 1, power supply 2)
- Ambient Temp
- FAN MOD xx RPM (where xx is 1A, 1B, 2A, 2B, etc.)
- Current 1, 2 (sensor for each power supply)
- Voltage 1, 2 (sensor for each power supply)
- System Level
- RAID backup battery

The monitored chassis-related faults for the S8510 server are as follows:

- Power Overload
- Main Power Fault
- Power Control Fault
- Drive Fault
- Cooling/Fan Fault

The following table contains the RAID alarms for the S8510 server.

Storage Service EventID:	Note
2048	Device failed
2049	Physical disk removed

Table continues…

Storage Service EventID:	Note
2056	Virtual disk failed / Virtual disk consistency check failed
2057	Virtual disk degraded
2076	Virtual disk failed / Virtual disk consistency check failed
2080	Physical disk Initialization or rebuild fail
2083	Physical disk Initialization or rebuild fail
2102	Temperature exceeded the maximum failure threshold
2103	Temperature dropped below the minimum failure threshold
2163	HDD rebuild completed with error(s)
2169	Controller battery must be replaced
2268	Storage Management has lost communication with the controller
2270	Physical disk Initialization or rebuild fail
2272	Patrol Read found an uncorrectable media error
2273	A block on the physical disk has been punctured by the controller
2282	Hot spare SMART polling failed
2289	Multi-bit ECC error on controller DIMM
2299	Bad PHY or physical connection
2307	Bad block table is full. Unable to log block
2320	Single bit ECC error. The DIMM is critically degraded
2321	Controller DIMM is critically degraded
2340	The background initialization (BGI) completed with uncorrectable errors
2347	Rebuild failed due to errors on the source or target physical disk
2348	Rebuild failed due to errors on the source or target physical disk
2349	A bad disk block could not be reassigned during a write operation
2350	Unrecoverable disk media error during the rebuild or recovery

See the Systems Hardware Owner's manual at http://support.dell.com/support/edocs/systems/pe1950/ or the Message Reference Guide at http://support.dell.com/support/edocs/software/svradmin/5.3/index.htm for more information on troubleshooting and fault resolution.

For S8800

The monitored sensor-related faults for S8800 server are as follows:

- Ambient Temp
- Altitude
- Avg Power
- Planar 3.3V
- Planar 5V

- Planar 12V
- Planar VBAT
- Fan xx Tach (where xx is 1A, 1B, 2A, 2B, and so on)
- RAID backup battery

The monitored chassis-related faults for S8800 server are as follows:

- Power Overload
- Main Power Fault
- Power Control Fault
- Drive Fault
- Cooling/Fan Fault

The following table contains the RAID alarms for S8800 server.

Message	Note
Drive Slot sensor Drive [0–9]+ [^\-]*- Drive Presented Deasserted	A drive has been removed. No alarm message is generated when the drive is inserted.
Drive Slot sensor Drive [0–9]+ [^\-]*- Drive Predictive Failure Asserted	A predictive failure was detected. The drive must be replaced.
Drive Slot sensor Drive [0–9]+ [^\-]*- In Critical Array Asserted	A critical failure was detected. The drive must be replaced.
Drive Slot sensor Drive [0–9]+ [^\-]*- In Failed Array Asserted	The device has failed. The drive must be replaced.
Drive Slot sensor Drive [0–9]+ [^\-]*- In Rebuild Abort Asserted	The rebuild has failed.

See the Problem Determination and Service Guide at http://www.ibm.com/ for more information on troubleshooting and fault resolution.

For S8300D and S8300E

System Platform does not monitor hardware on the S8300D/E server.

General software faults

Alarm text	Problem/Action
VSP WebConsole cannot start due to `libvirt_jni` cannot be found.	Ensure `/usr/local/lib/libvirt_jni.so` exists on cdom; if it is a symbolic link, ensure the link points to a valid shared library.
VSP WebConsole cannot start due to missing configuration file (vsp.properties).	Ensure `/opt/avaya/vsp/tomcat/lib/vsp.properties` exists on cdom.
VSP Webconsole encountered problem running `/opt/avaya/vsp/bin/vsp_rsyslog_rotate.sh`	Ensure `/etc/logrotate.d/vsp_rsyslog` exists and verify the permissions (should be 644 and owned by root/root) on cdom.
VSP Webconsole encountered problem with `log4j.xml` file.	Ensure `/opt/avaya/vsp/tomcat/webapps/webconsole/WEB-INF/classes/log4j.xml` exists on cdom.
CDom Webconsole tomcat died.	Check the tomcat log files in `/opt/avaya/vsp/tomcat/logs/catalina.out` on cdom.
VSP Backup failed.	Check the details in the `/vspdata/backup/backup.log` log file.
Backup archive <archive> could not be sent on server <server>	Verify that SFTP is enabled on the server <server>. Log in to the System Platform Management Console. Select **Server Management** > **Backup/Restore**. Click **Backup**. Select SFTP from the **Backup Method** list. Verify that the SFTP Directory and SFTP Username are valid on <server>. Re-enter the SFTP Password. Check the details in `/var/log/vsp/vsp-all.log`.
Backup archive <archive> could not be sent on mail <email>	Verify that <email> is a valid email address and that it is able to accept email. Check the details in `/var/log/vsp/vsp-all.log`.
Restore of archive file <archive> failed.	Check the details in the `/vspdata/backup/backup.log` log file.

In the **Alarm text** and **Problem/Action** columns:

- <archive> is the name of a backup archive file.
- <server> is the name or IP address of a server where SFTP is enabled so that a backup archive file can be sent to the server.
- <email> is a valid email address.

Lifecycle manager faults

System Platform has a lifecycle manager that monitors the operation of any virtual machine that was installed as part of a product template. An application in the virtual machine is expected to provide a periodic heartbeat. If this heartbeat is missed for a number of periods, the lifecycle manager will reboot the virtual machine. If the lifecycle manager does not see heartbeats after a reboot for a number of consecutive reboots, the lifecycle manager can shut down the virtual machine. Each product template defines its own values for the frequency of the heartbeat, the number of consecutive missed heartbeats before rebooting, and the number of consecutive reboots before shutting down.

Alarm text	Problem/Action
VSP Virtual system <vm> sanity heartbeat failure	Check the virtual system log to see why sanity heartbeat failed.
VSP Virtual system <vm> reboot as the result of sanity heartbeat failures	Check the virtual system log to see why sanity heartbeat failed.
VSP Virtual system sanity reboot failed.	Check the details in `/var/log/vsp/vsp-all.log` on cdom.
VSP Virtual system <vm> shutdown as the result of sanity heartbeat failures	Check the virtual system log to see why sanity heartbeat failed.

In the **Alarm text** column, <vm> is the name of the virtual machine as it appears in the System Platform Management Console under the Virtual Machine Management page.

Performance faults

Alarm text	Problem/Action
VSP High CPU Usage detected for <vm>	Check <vm> Troubleshoot the virtual machine.
VSP High Webconsole heap usage	Verify the Webconsole is OK.
VSP High Network I/O (Tx) from for <vm>	Check <vm> Troubleshoot the virtual machine.
VSP High Network I/O (Rx) from for <vm>	Check <vm> Troubleshoot the virtual machine.
VSP High Load Average <vm>	Check <vm> Troubleshoot the virtual machine.
VSP Low logical volume free space <lv>	Volume <lv> is running out of space. Free some space on logical volume <lv> Troubleshoot the virtual machine.

Table continues…

Alarm text	Problem/Action
VSP Low volume group free space (VolGroup00)	Free some space on volume group VolGroup00 in dom0. Troubleshoot the virtual machine.
VSP High disk read rate on disk (sda)	From dom0, check the device sda.
VSP High disk write rate on disk (sda)	From dom0, check the device sda.
VSP High Webconsole permgen usage	Log in to the System Platform Management Console. Select **Virtual Machine Management** > **Manage**. Click the **cdom** link. Click **Reboot**. **Note:** If you are unable to log in to System Platform Management Console, use the `xm reboot` command while logged in to dom0.
VSP High Webconsole open files	Log in to the System Platform Management Console. Select **Virtual Machine Management** > **Manage**. Click the **cdom** link. Click **Reboot**. **Note:** If you are unable to log in to System Platform Management Console, use the `xm reboot` command while logged in to dom0.
VSP High SAL Agent heap usage	Log in to the System Platform Management Console. Select **Virtual Machine Management** > **Manage**. Click the **cdom** link. Click **Reboot**. **Note:** If you are unable to log in to System Platform Management Console, use the `xm reboot` command while logged in to dom0.
VSP High SAL Agent permgen usage	Log in to the System Platform Management Console. Select **Virtual Machine Management** > **Manage**. Click the **cdom** link. Click **Reboot**.

Table continues…

Alarm text	Problem/Action
	Note: If you are unable to log in to System Platform Management Console, use the `xm reboot` command while logged in to dom0.
High Memory Usage in Domain-0	Check Memory Usage in Domain-0.
High Memory Usage in cdom	Check Memory Usage in cdom.

In the **Alarm text** and **Problem/Action** columns:

- <vm> is the name of the virtual machine as it appears in the System Platform Management Console under the Virtual Machine Management page.
- <lv> is the name of a logical volume used as a virtual disk within a virtual machine.

High Availability Failover faults

Alarm text	Problem/Action
VSP Webconsole encountered problem while retrieving status of failover.	Check the details in `/var/log/vsp/vspha.log` log file in dom0.
VSP Webconsole encountered problem while synchronising services to secondary node.	Check the details in `/var/log/vsp/vspha.log` log file in dom0.
Not able to read machine hardware state; error executing IPMI command: <command> (raised on <hostname>)	Check the details in `/var/log/vsp/vspha.log` log file in dom0.
Migrating resources to other node; a critical condition has existed for longer than xx minutes (raised on <hostname>)	Seek appropriate service for the critical condition
Failed migrating resources to other node: <hostname> (raised on <hostname>)	See `/var/log/vsp/vspha.log` and `/var/log/vsp/ha-log` for possible causes
Start HA failed: <details> (raised on <hostname>)	See `/var/log/vsp/vspha.log` and `/var/log/vsp/ha-log` for possible causes
Stop HA failed: <details> (raised on <hostname>)	See `/var/log/vsp/vspha.log` and `/var/log/vsp/ha-log` for possible causes
HA Failover failed: <details> (raised on <hostname>)	See `/var/log/vsp/vspha.log` and `/var/log/vsp/ha-log` for possible causes

Table continues…

Alarm text	Problem/Action
Crossover connection between the machines is broken (raised on <hostname>)	Check the crossover network connection between the machines
Failover occurred, activating this node (raised on <hostname>)	Check the `/var/log/vsp/ha-log` and `/var/log/messages` for the cause of failover
Failover has failed because directory <dir> for environment ISO image does not exist (raised on <hostname>)	Ensure that the directory <dir> exists in dom0 and is accessible

In the “Alarm text” column:

- <hostname> is the short hostname (not the fully qualified domain name).
- <details> is a more detailed error string.
- <dir> is a Linux-style directory name.

Appendix A: Changing VLAN ID

You can change the VLAN ID that was set up during the installation of System Platform on an S8300D/E server by executing a script at the System Platform System Domain command line.

Procedure

1. Log in to System Platform System Domain as advanced administrator.
2. Type `change_vlan` *`new_vlan_number`*

Example

`change_vlan -?` shows the available options as explained below:

- `-n` Don't restart network
- `-y` Restart network without prompting
- `-l` List existing VLANs
- `-f num` Specify which VLAN ID to change

You can view the currently configured VLAN IDs by typing the command:

```
change_vlan -l
```

You can change the current VLAN ID to new VLAN ID by typing the commands:

`change_vlan` *`new_vlan_id`*

In the above command, the script prompts you to know whether the network should be restarted immediately or not. You can suppress those prompts by appending `-n` or `-y` to the command.

Appendix B: Errors encountered while downloading files from PLDS

While downloading files from PLDS, one can encounter one of the following errors:

Error message
The SSO user id and/or password are not valid.
Error establishing SSO session. Check the log for additional information.
The provided SSO credentials are not authorized to access PLDS Web Services.
PLDS Web Services error. Check the log for additional information.
Error accessing SSO URL.
Error accessing PLDS Web Service URL.
Error accessing SSO URL. Verify that the proxy settings are correct.
Error accessing SSO URL due to an SSL problem.
Error accessing PLDS Web Service URL. Verify proxy settings are correct.
Error accessing PLDS Web Service URL due to an SSL problem.
Error downloading from Akamai. Verify that proxy settings are correct.
Error accessing Akamai URL.
Error accessing Akamai URL. Troubleshoot the virtual machine. Verify proxy settings are correct.
Error accessing Akamai URL due to an SSL problem.
No File Found in Avaya Downloads (PLDS) for this credential.

To resolve these errors, check or initialize the proxy settings, if the errors suggest to do so. Contact Avaya or Avaya Partners Support for additional help.

Index

F

G

H

I

L

M

N

P

R

S

T

U

V

W