Administering Avaya Aura® System Platform

Release 6.2.1
July 2012

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 generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Avaya grants End User a license within the scope of the license types described below. 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 End User. “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. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

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

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.

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

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya 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). End User 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). Customer 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”). (see “Third-party Components” for more information).

Copyright

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

the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Preventing Toll Fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. 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 Web site: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support Web site: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support Web site: http://support.avaya.com, 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 server, which is housed in a routing media gateway. To fulfill the VLAN requirements, the S8300D 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

About this task

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

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

Note:

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

Procedure

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

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

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 12.

About this task

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

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7, and Firefox 3.6 and later.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain.

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 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.

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 Configuration Parameters page displays configuration details for the virtual machine, including its MAC address, IP address, and operating system.

Related topics:

Virtual Machine List field descriptions on page 17
Virtual Machine Configuration Parameters field descriptions on page 19

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 Configuration Parameters page, click **Reboot**.

Related topics:

Virtual Machine List field descriptions on page 17
Virtual Machine Configuration Parameters field descriptions on page 19

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 topics:

Virtual Machine List field descriptions on page 17
Virtual Machine Configuration Parameters field descriptions on page 19

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.
Maximum 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.
Maximum 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.

Name	Description
	• **Stopped**: Virtual machine has been shutdown. • **Rebooting**: Virtual machine is rebooting and should return to the Running state upon completion. • **No State**: The virtual machine is not running or the application watchdog is not being used. • **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's sanity mechanism provided some kind of error message. • **Unknown**: Application's sanity mechanism failed.

Button descriptions

Name	Description
Refresh	Refreshes the list of virtual machines.

Related topics:

Viewing virtual machines on page 15
Rebooting a virtual machine on page 16
Shutting down a virtual machine on page 16

Virtual Machine Configuration Parameters field descriptions

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

Name	Description
Name	Name of the virtual machines running on System Platform.
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 or Windows.
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**: The virtual machine is not running or the application watchdog is not being used.
Application State	State of virtual machine as communicated by the watchdog.

Name	Description
	A virtual machine that includes an application watchdog communicates application health back to the Console Domain. Current status of the application (respective virtual machine). 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's sanity mechanism provided some kind of error message. • **Unknown**: Virtual machine's sanity mechanism failed.
Maximum 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 respective virtual machine.
Domain UUID	Unique ID of the virtual machine.
Auto Start	Status of auto start of a virtual machine: if the virtual machine starts automatically after a shut down operation. Available status are **True** (if auto start is set), and **False** (if auto start is not set).

Name	Description
	Note: This value should be changed only for troubleshooting purposes.

Button descriptions

Button	Description
Reboot	Reboots the respective virtual machine. In the case of System Domain (Domain-0), this reboot operation is the same as the reboot operation available in the left navigation pane. When you reboot the System Platform server using the reboot option in the left navigation pane, the system shuts down the System Platform server and all the virtual machines 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	Appears only if **Domain-0** is selected and shuts down the server and all virtual machines running on it.
Stop	Appears if a virtual machine other than System Domain (Domain-0) or Console Domain is selected and stops the selected virtual machine.
Start	Appears if a virtual machine other than System Domain (Domain-0) or Console Domain is selected and starts the selected virtual machine.

Related topics:

Viewing virtual machines on page 15
Rebooting a virtual machine on page 16
Shutting down a virtual machine on page 16

Deleting a solution template

About this task

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

Procedure

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

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 topics:

Viewing system hardware and virtualization information on page 24
System Information page field descriptions on page 24

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 topics:

System server information on page 23
System Information page field descriptions on page 24

System Information page 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

Category	Name	Description
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)`
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 topics:

System server information on page 23
Viewing system hardware and virtualization information on page 24

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) Web site at http://plds.avaya.com.

System Platform patches and service packs

When required, you upgrade System Platform with software patches and service packs. Patches typically provide software bug fixes. Service Packs often include new functionality, such as a new or improved feature.

System Platform patches

Avaya distributes **.rpm* patches for you to apply to your existing version of System Platform. Each patch contains bug fixes, some of which are temporary pending the release of a subsequent service pack. You must apply these patches in the sequence prescribed in the *Release Notes for System Platform 6.2*.

Note:

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

Important:

Before installing any patches on either server, **Stop HA** and **Remove HA** on the primary server.

System Platform service packs

Avaya distributes *ISO* and *.rpm* service packs for you to apply to your existing version of System Platform. Each service pack represents a full System Platform image, including any patches issued since the prior service pack or major/minor release of System Platform.

Patch commit and rollback

Using **Patch Management** features of the Web Console, you can install, commit, roll back (undo), or remove kernel patches. (These are patches applied to the CentOS kernel for System Platform.) The manual rollback feature allows you to test a patch before committing it to the system. The automatic rollback feature enables 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` indicate whether you can roll back an installed patch. (You can alternatively **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.

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 reboots, also logging you out of the Web Console. If you log on to the Web Console within four hours, the system automatically commits the kernel patch at that time. If you installed the patch by means of communication over the Secure Access Link (SAL) but cannot log back on to the Web Console, the system automatically rolls back the kernel patch after 4 hours, enabling you to regain access to the Web Console. Following automatic rollback of a kernel patch, System Platform reboots off the kernel version established before applying the latest patch.

  The following additional caveats apply to patch commit and rollback on System Platform:

  Note:

  - If you perform one or more operations before committing or rolling back a platform upgrade, those operations will be implemented and visible on the system. If you **Commit** a Platform Upgrade, any operations performed prior to the **Commit** will not be implemented or visible on the system.
  - If you perform operations locally during a Platform Upgrade but neither **Commit** nor **Rollback** the upgrade within 4 hours, then System Platform automatically rolls back to reboot off the System Platform version established prior to the upgrade attempt.
  - If you perform one or more operations related to Template functionality and must undo those operations after committing or rolling back the System Platform upgrade, a Platform Upgrade rollback will not automatically roll back your Template-related changes. Instead, use the Web Console to manually roll back the Template-related changes. Changes you made prior to a Platform Upgrade **Commit** will not be implemented or visible on the system.
- If you install any other type of patch on the System Platform, you can effectively roll back (undo) its effects by simply removing it from the system. (See Removing patches on page 32.)

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 reboot. Install or roll back a patch to the template VM only during planned downtime for system maintenance. Patch rollback typically requires several minutes of system downtime. *Committing* a patch does not cause the template VM to reboot.

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 just 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 patch URL.

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

Related topics:

Configuring a proxy on page 29
Search Local and Remote Patch field descriptions on page 32
Errors encountered while downloading files from PLDS on page 193

Configuring a proxy

About this task

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

Procedure

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

Related topics:

Search Local and Remote Patch field descriptions on page 32

Installing patches

Before you begin

To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.

About this task

Perform the following tasks to install all service packs and other patches (that is, System Platform and solution template patches) through the System Platform Web Console.

Note:

Do not use the patch installers provided by your solution templates.

Procedure

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Related topics:

Patch List field descriptions on page 34
Patch Detail field descriptions on page 35

Committing patches

See Patch commit and rollback on System Platform on page 27 for information about committing patches installed on the Avaya Aura® System Platform.

See the prerequisites and procedure below for information about how to commit patches to the Avaya Aura® solution template Virtual Machine (VM).

Before you begin

You have completed the following tasks using the Web Console:

- Downloading patches on page 28 (finding and downloading the particular patch you must install)
- Configuring a proxy on page 29 (if the patches are located in a different server)
- Installing patches on page 29 (for the particular patch you must install)

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.

About this task

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Management**.
   The Server Management Patch List page appears.
3. Click the patch that you must commit.
   The Web Console displays the Server Management Patch Detail page.

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

Rolling back patches

See Patch commit and rollback on System Platform on page 27 for information about rolling back patches installed on the Avaya Aura® System Platform.

See the prerequisites and procedure below for information about how to roll back patches to the Avaya Aura® solution template Virtual Machine (VM).

Before you begin

You have completed the following tasks using the Web Console:

- Downloading patches on page 28 (finding and downloading the particular patch you must install)
- Configuring a proxy on page 29 (if the patches are located in a different server)
- Installing patches on page 29 (for the particular patch you must install)

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.

About this task

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Management**.
   The Server Management Patch List page appears.
3. Click the patch that you must commit.
   The Web Console displays the Server Management Patch Detail page.
4. Click **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

Procedure

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch 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 topics:

Patch List field descriptions on page 34
Patch Detail field descriptions on page 35

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 should match the extensions in this list. For example, *.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 located in the Avaya Product Licensing and Delivery System (PLDS) Web site. You must enter an Avaya SSO login and password. The list will contain all the templates to which your company is entitled. Each line in the list begins with the “sold-to” number to allow you to select the

Name	Description
	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**: Files are located in a different server. You must specify the Patch URL for the server. • **SP Server**: Files are located in the vsp-template file system in the System Platform server. You must specify the Patch URL for the server. **Tip:** To move files from your laptop to the System Platform Server, some errors can occur because System Domain (Domain-0) and Console Domain support only SCP, but most laptops do not come with SCP support. You can download the following two programs to enable SCP (Search the Internet for detailed procedures to download them): - Pscp.exe - WinSCP • **SP CD/DVD**: Files are located in a System Platform CD or DVD. • **SP USB Disk**: Files are located in a USB flash drive. (Option not supported for upgrades to System Platform 6.2 and 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.

Button	Description
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 if necessary.
Add	Appears when **Local File System** is selected and adds a patch file to the local file system.
Upload	Appears when **Local File System** is selected and uploads a patch file from the local file system.
Download	Downloads a patch file.

Related topics:

Downloading patches on page 28
Configuring a proxy on page 29
Errors encountered while downloading files from PLDS on page 193

Patch List field descriptions

The Patch List page displays the patches on the System Platform server for installing or removing. Use this page to view the details of patch file by clicking on the file name.

Name	Description
System Platform	Lists the patches available for System Platform under this heading.
Solution Template	Lists the patches available for the respective solution templates under respective solution template headings.
Patch ID	File name of a patch.
Description	Information of a patch, for example, if the patch is available for System Platform the description is shown as SP patch.
Status	Shows the status of a patch. Possible values of **Status** are **Installed**, **Not Installed**, **Active**, and **Not Activated**.

Name	Description
Service Affecting	Shows if installing the patch causes the respective virtual machine to reboot.

Button descriptions

Button	Description
Refresh	Refreshes the patch list.

Related topics:

[Installing patches](#) on page 29
[Removing patches](#) on page 32

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 effecting 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.

Name	Description
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	Shows whether installation and use of the patch file requires the Avaya Aura® customer to obtain a software license from the Avaya corporation.
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.
Commit	Commits the installed patch.
Activate	Activates the installed patch of a solution template.
Deactivate	Deactivates the installed patch of a solution template.
Rollback	Rolls back the installed patch if the **Rollbackable** field value is Yes.
Remove	Removes the respective patch.
Remove Patch File	Removes the respective patch file. The button appears only if the patch file is still present in the system. On removing the patch file, the button does not appear.

Related topics:

Installing patches on page 29
Removing patches on page 32

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 topics:

Log Viewer field descriptions on page 38

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** 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.

Name	Description
	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 topics:

Viewing log files on page 37
Log severity levels on page 43

Configuring date and time

Configuring System Platform to synchronize with an NTP server

About this task

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

Procedure

1. Click **Server Management** > **Date/Time Configuration**.
   The system displays the Date/Time Configuration page with default configuration settings.
2. Select a time zone and click **Set Time Zone** to set the time zone in System Platform.
   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. Specify a time server and click **Add** to add the time server to the configuration file.

4. Click **Ping** to check whether the specified time server, that is, the specified host, is reachable across the network.
5. Click **Start ntpd** to synchronize the System Platform time with the Network Time Protocol (NTP) server.
   System Platform restarts for the NTP synchronization to take effect.
6. Log in again to the System Platform Web Console.
7. Click **Server Management** > **Date/Time Configuration**.
   The system displays the Date/Time Configuration page with default configuration settings.
8. Click **Query State** to check the NTP (Network Time Protocol) status.
   The system displays the status of the NTP daemon on System Platform.

Related topics:

NTP daemon on page 41
Date Time Configuration field descriptions on page 42

Configuring date and time

About this task

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 configuration settings.
2. Click the calendar icon located next to the **Save Date and Time** button.
   The system displays the Set Date and Time page.

   Note:

   If the **Save Date and Time** button is not enabled, you must stop the NTP server that is currently being used.
3. Select a date in the calendar to change the default date and set the required date.
4. 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 time changes.

5. Click **Apply** to save your changes.
6. Click **Save Date and Time**.
   The system displays a warning message stating that this action will cause a full system reboot.
7. Click **OK** to accept the message and set the updated date and time in the system.

Related topics:

Date Time Configuration field descriptions on page 42

Removing a time server

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** to remove the selected time server.

Note:

The changes will be effective after you restart NTP.

Related topics:

Date Time Configuration field descriptions on page 42

NTP daemon

The NTP daemon reads its configuration from a file named `ntp.conf`. The `ntp.conf` file contains at least one or more lines starting with the keyword *server*. Each of those lines specify one reference time source, that is, time server, which can be either another computer on the network, or a clock connected to the local computer.

Reference time sources are specified using IP addresses, or host names which can be resolved by a name server. NTP uses the pseudo IP address 127.127.1.0 to access its own system clock, also known as the local clock. You must not mix this IP address with 127.0.0.1, which is the IP address of the local host, that is the computer's loopback interface. The local

clock will be used as a fallback resource if no other time source is available. That is why the system does not allow you to remove the local clock.

Related topics:

Configuring System Platform to synchronize with an NTP server on page 39
Date Time Configuration field descriptions on page 42

Date Time Configuration field descriptions

Use the Date/Time Configuration page to view or change the current date, time, time zone, or the status of NTP daemon on the System Platform server.

Name	Description
Date/Time Configuration	Shows the local time and the UTC time. Also shows the status of the NTP daemon, if it is started or stopped.
Save Date and Time	Lets you edit the date and time set during System Platform installation.
Manage Time Servers	Lets you ping a time server and see its status and manage the existing time servers.

Button descriptions

Button	Description
Start ntpd	Starts the Network Time Protocol (NTP) daemon on System Platform to synchronize the server time with an NTP server. If the NTP daemon (ntpd) is started, this button changes to **Stop ntpd**. Click this button to stop the NTP daemon.
Set Date and Time	Edits the date and time that are configured for System Platform. The button is disabled if ntpd is running.
Set Time Zone	Edits the time zone that is configured for System Platform . System Platform updates the time zone on System Domain (Domain-0), Console Domain, and the virtual machines running on System Platform.
Ping	Checks whether the specified time server, that is, the specified host, is reachable across the network.

Button	Description
Add	Adds the time server that you specify to the list of time servers with which System Platform can synchronize.
Remove Time Server	Removes the selected time server.
Query State	Checks the status of the NTP daemon on System Platform.

Related topics:

Configuring System Platform to synchronize with an NTP server on page 39
Configuring date and time on page 40
Removing a time server on page 41
NTP daemon on page 41

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 topics:

Log severity levels on page 43
Log retention on page 43
Logging Configuration field descriptions on page 44

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.*).

Name	Description
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 topics:

Log severity levels on page 43
Log retention on page 43
Configuring log levels and retention parameters on page 44

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

- Configure 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 topics:

System configuration field descriptions on page 46

System configuration field descriptions

Use the System Configuration page to configure Internet proxy server settings, change the current keyboard language setting, configure Web LM 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 – 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 behaviour.

Name	Description
Proxy Configuration Area:	
Status	Specifies whether an http proxy should be used to access the Internet, for example, when installing templates, upgrading patches, or upgrading platform.
Address	The address for the proxy server.

Name	Description
Port	The port address for the proxy server.
	WebLM Configuration Area:
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 Area:
Syslog IP Address	IP address of the Syslog server, which collects log messages generated by the System Platform operating system.
Keyboard Layout	Determines the specified keyboard layout for the keyboard attached to the System Platform server.
Statistics Collection	If you disable this option, the system stops collecting the statistics data. **Note:** If you stop collecting statistics, the system-generated alarms will be disabled automatically.
SNMP Discovery	By default, this feature enables SNMPv2 management systems to automatically discover any System Platform server in an Avaya Aura®-based network, including retrieval of server status and vital statistics. This is useful, for example, when using System Manager to view the entire inventory of System Platform servers across multiple Avaya Aura® enterprise solutions at a glance. This feature eliminates the tedious and error-prone task of manually adding 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.

Name	Description
	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.

Related topics:

Configuring system settings for System Platform on page 46
Configuring an alternate WebLM server on page 66

Configuring network settings

Configuring System Platform network settings

About this task

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.

Make sure that 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 topics:

Network Configuration field descriptions on page 49

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.

Name	Description
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	The host name for the Console Domain. When using a Domain Name System (DNS) server in your network, the Cdom hostname must be a Fully Qualified Domain Name (FQDN), for example, `SPCdom.mydomainname.com`.
Dom0 Hostname	The host name for System Domain (Dom0). When using a Domain Name System (DNS) server in your network, the Dom0 hostname must be a Fully Qualified Domain Name (FQDN), for example, `SPCdom.mydomainname.com`.
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

Name	Description
	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]+”.
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 topics:

Configuring System Platform network settings on page 48

Adding a bonding interface

About this task

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**

Deleting a bonding interface

About this task

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.

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.

Before you begin

The Enable Services VM checkbox is selected.

About this task

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 **Solution 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 topics:

Enabling the Service Virtual Machine on page 54
Disabling the Services Virtual Machine on page 55
Configuring Services VM field descriptions on page 56

Enabling the Service Virtual Machine

Before you begin

- You installed the Services Virtual Machine during System Platform installation. (See Installing the Services Virtual Machine.)
- You earlier performed the administrative task, Disabling the Services Virtual Machine on page 55.

About this task

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 **Solution Template – 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**.

Result

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.

Next steps

- 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 71.)
- Verify the configuration of the local SAL gateway. (See Starting the SAL Gateway user interface.)
- Restart the local SAL gateway. (See Enabling SAL Gateway on page 75.)

Disabling the Services Virtual Machine

Before you begin

You installed the Services Virtual Machine during System Platform installation. (See Installing the Services Virtual Machine.)

About this task

Use this procedure when changing your network configuration, from using the local SAL gateway to using a stand-alone SAL gateway running on an independent server elsewhere in your network. In this circumstance, you must disable the on-board SAL (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. Services Virtual Machine reactivation at a later time is possible, for example, if reverting to use of the SAL Gateway formerly configured to run on the Services Virtual Machine, instead of continuing to deploy the 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 re-enable (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.

See also Enabling the Service Virtual Machine on page 54

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 **Solution Template – Services VM** area of the Network Configuration page, deselect **Enable Services VM**.
3. At the bottom of the Network Configuration page, click **Save**.

Next steps

- 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 2.1 SAL Gateway Implementation Guide*, available from the Avaya Support portal (http://support.avaya.com/ > **View all documents** > **S** > **Secure Access Link**.
- Go to the web console SNMP Trap Receiver Configuration page to set the SNMP trap receiver destination address of the new gateway.

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 **Solution Template – 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**,

Name	Description
	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 54 • Disabling the Services Virtual Machine on page 55
Preferred IP Address Type	Indicates the preferred type of IP address for applications running on the Services VM. • **IPv4** • **IPv6** 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).

Configuring static routes

Adding a static route

About this task

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 topics:

Static route configuration field descriptions on page 59

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 topics:

Static route configuration field descriptions on page 59

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 topics:

Static route configuration field descriptions on page 59

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 topics:

Adding a static route on page 58
Deleting a static route on page 58
Modifying a static route on page 59

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 topics:

Ethernet configuration field descriptions on page 60

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

Name	Description
	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 topics:

Configuring Ethernet interface settings on page 60

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)
Disk (Volume Group)	Percentage of volume group used (VolGroup00)
Disk reads	Disk read rate (sda)
Disk Writes	Disk write rate (sda)
Load Average	Load average on each virtual machine

Alarm	Description
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.
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 topics:

Alarm descriptions on page 61
Alarm configuration field descriptions on page 63

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 topics:

Alarm descriptions on page 61
Configuring alarm settings on page 62

Managing Certificates

Certificate management

The certificate management feature allows a user with the right administrative privileges to replace the default System Platform Web Console certificate and private key. It also allows the user to upload and replace the enterprise LDAP certificate, if the option of transport layer security (TLS) was enabled in the Enterprise LDAP page.

The user can replace the default System Platform Web Console certificate and private key by selecting a new certificate file and a new private key on the local machine and uploading them. The default System Platform Web Console certificate is generated during System Platform installation with the CN value same as the Console Domain hostname. During platform upgrade, the certificate is first backed up and then restored after the upgrade completes.

Similarly, the user can upload and replace the enterprise LDAP certificate by selecting new certificate file on the local machine, and uploading it. The Certificate Management page shows

the following data for the current System Platform Web Console and Enterprise LDAP certificate:

- Type
- Version
- Expiry date
- Issuer

Here are the things to note relating to a certificate:

- 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 upload the key is only for the System Platform Web Console certificate.
- An uploaded certificate is valid if its start date is not after the current date and its end date is not before the current date. An uploaded private key is valid if it matches the uploaded certificate.

Related topics:

LDAP field descriptions on page 114

Selecting System Platform certificate

Procedure

1. Click **Server Management** > **Certificate Management**.
2. Click **Select New Certificate** in the System Platform Certificate area.

Selecting enterprise LDAP certificate

About this task

This task is enabled only if **TLS** was clicked in the Enterprise LDAP page.

Procedure

1. Click **Server Management** > **Certificate Management**.
2. Click **Select New Certificate** in the Enterprise LDAP Certificate area.

Related topics:

Configuring authentication against an enterprise LDAP on page 113

Certificate Management field descriptions

Use the Certificate Management page to get new certificate issued from your certification authority for System Platform Web Console or Enterprise LDAP. In the case of System Platform Web Console, you also get the private key.

Field descriptions

Name	Description
Type	Is the type of the certificate issued.
Version	Is the version number of the certificate.
Expiry Date	Is the expiry date of the certificate.
Issuer	Is the issuing agency of the certificate.

Button descriptions

Name	Description
Select New Certificate	Selects new System Platform Web Console certificate and private key or Enterprise LDAP certificate depending on the area where the button is located.

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

Before you begin

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

About this task

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 topics:

License management on page 65
License Management launch page field descriptions on page 71

Configuring an alternate WebLM server

Before you begin

- 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.

About this task

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 topics:

System configuration field descriptions on page 46

WebLM password reset and restore

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

Each Avaya 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 68.

Note:

Avaya 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 Avaya WebLM password reset and restore overview on page 67.

Resetting an Avaya WebLM password to factory default

See Resetting an Avaya WebLM password to factory default on page 68.

Making license changes when the Avaya WebLM password is temporarily unavailable

Follow the sequence outlined in the following table:

Item	Procedure
1.	See Resetting an Avaya WebLM password to factory default on page 68.
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 an Avaya WebLM private password on page 70.

Making license changes when the Avaya WebLM password has been lost

Follow the sequence outlined in the following table:

Item	Procedure
1.	See Resetting an Avaya WebLM password to factory default on page 68.
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 an Avaya WebLM password to factory default

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

Before you begin

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.)

About this task

The `weblm_password reset` command:

- Copies your existing (customized) Avaya WebLM password file (`Users.xml`) to a duplicate file named `Users.xml.cust`. This preserves your private Avaya WebLM password value in `Users.xml.cust`.
- Copies the Avaya 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.
   ```

Next steps

- You can use the factory default password to access the Avaya 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 Avaya WebLM password was temporarily unavailable, you must complete the procedure, Restoring an Avaya WebLM private password on page 70.
- 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 an Avaya WebLM private password

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

Before you begin

- 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 an Avaya WebLM password to factory default on page 68.

About this task

The `weblm_password restore` command copies the temporary duplicate Avaya WebLM password file `Users.xml.cust` (created by Resetting an Avaya WebLM password to factory default on page 68) to a new file named `Users.xml`. This effectively overwrites the contents of your existing `Users.xml` file, thereby restoring the Avaya 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 Avaya WebLM administrator's private password, or if you did not complete the prerequisite procedure, Resetting an Avaya WebLM password to factory default on page 68, 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.
```

Next steps

- 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 topics:

License management on page 65
Launching WebLM on page 66

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

Remote Serviceability

System Platform utilizes SAL as Avaya’s exclusive method for remote delivery of services. System Platform can be serviced remotely, possibly eliminating a service technician visit to the

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

Note:

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

Stand-alone SAL Gateway

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

If you use a stand-alone SAL Gateway, you must add it as an SNMP trap receiver for System Platform. See Adding an SNMP trap receiver on page 102. You can also disable the SAL Gateway that is embedded in System Platform so that it does not send duplicate heart beat messages to Avaya. See Disabling SAL Gateway on page 75.

SAL Gateway configuration

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

To configure SAL, perform these high-level steps:

1. Register the system.

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

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

2. Configure the SAL Gateway.

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

Note:

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

Related topics:

Configuring the SAL Gateway

Launching the SAL Gateway management portal on page 73

SAL Gateway Management field descriptions on page 76

Launching the SAL Gateway management portal

About this task

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.

Related topics:

Configuring the SAL Gateway

SAL Gateway on page 71

SAL Gateway Management field descriptions on page 76

Configuring the SAL Gateway

About this task

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

Procedure

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

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

   Note:

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

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

   See the *Secure Access Link Gateway 2.1 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

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

Disabling SAL Gateway

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

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

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

About this task

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

Note:

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

Procedure

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

Enabling SAL Gateway

About this task

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**.

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 topics:

Configuring the SAL Gateway

SAL Gateway on page 71

Launching the SAL Gateway management portal on page 73

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 topics:

Log severity levels on page 43

Exporting collected data on page 78

Performance statistics field descriptions on page 79

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 topics:

Exporting collected data on page 78
Performance statistics field descriptions on page 79

Exporting collected data

About this task

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 topics:

Log severity levels on page 43
Performance statistics on page 76
Performance statistics field descriptions on page 79

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 topics:

Viewing performance statistics on page 78
Exporting collected data on page 78

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/DVD

About this task

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 topics:

File Management field descriptions on page 82

Ejecting the CD or DVD

About this task

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.

Deleting directories and files

About this task

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 22.

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 topics:

File Management field descriptions on page 82

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

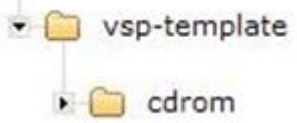
Name	Description
/vsp-template/ ...	This drop-down box specifies the final destination subdirectory in which files (copied originally from CD or DVD to subdirectory `/cdrom`) will reside. While the CDs or DVDs load into the System Platform server, File Manager collects the names of all `ovf` (template 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/`

Button	Description
	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 topics:

Copying files from CD/DVD on page 80
Deleting directories and files on page 82

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

About this task

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.

About this task

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.

Name	Description
	Important: Enabling audit is irreversible.
Reset Grub Password	Is the new System Platform Web Console Grub password.
Retype Grub Password	Is the new System Platform Web Console Grub password being retyped for verification.
Verify Dom0 Reset 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. **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.

Name	Description
	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

You can back up configuration information for System Platform and the solution template (all template virtual machines).

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.

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 hostname, Console Domain IP and hostname, 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.

Note:

You cannot restore an older version of System Platform from a backup set created on a newer version of System Platform.

Important:

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

Related topics:

Re-enabling failed standby node to High Availability Failover on page 172
Re-enabling failed preferred node to High Availability Failover on page 173

Backing up the system

About this task

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 89.

Important:

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

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
4. 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**.

Related topics:

Backup field descriptions on page 93

Scheduling a backup

About this task

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 topics:

Backup field descriptions on page 93

Transferring the Backup Archives to a remote destination

About this task

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

About this task

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 topics:

Backing up the system on page 90
Scheduling a backup on page 91

Restoring System Platform

Restoring backed up configuration information

About this task

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

Note:

Do not attempt to use 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.

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. Select an archive file from the list, and then click **Restore** to restore from the selected archive.

   To restore an archive, restart the System Platform Web Console. Log in again after the restore operation is complete.

Related topics:

System Platform backup on page 89
Restore field descriptions on page 96

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.
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 topics:

Restoring backed up configuration information on page 95

Viewing restore history

About this task

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

Before you begin

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

About this task

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

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 topics:

Server Reboot Shutdown field descriptions on page 99

Rebooting the whole High Availability Failover system

Before you begin

Only the users of Advanced Administrator role can perform this task.

About this task

When you reboot the entire High Availability system, the system shuts down all the virtual machines running on the primary server, reboots the standby server, and reboots the primary server to prevent failover. A service disruption follows this operation if needed.

Procedure

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

Note:

The **Reboot HA System** button is enabled only if the High Availability Failover system is settled and stable to perform this operation.

Shutting down the System Platform Server

About this task

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

Note:

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

Procedure

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

Related topics:

Server Reboot Shutdown field descriptions on page 99

Shutting down the whole High Availability Failover system

Before you begin

Only the users of Advanced Administrator role can perform this task.

About this task

When you shut down the whole High Availability Failover system, the system shuts down all the virtual machines running on the primary server, shuts down the secondary server, and shuts down the primary server to prevent failover. These actions sometimes result in a disruption of services..

Procedure

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

Note:

The **Shutdown HA System** button is enabled only if the High Availability Failover system is settled and stable to perform this operation.

Server Reboot Shutdown field descriptions

Use the Server Reboot/Shutdown page to reboot or shutdown the System Platform server and all the virtual machines running on it.

Name	Description
Name	Name of the application being shutdown. This is always System Domain (Domain-0).
MAC Address	Machine address of the virtual machine.
IP Address	IP address of the System Platform server.
OS Type	Operating system of the System Platform server, 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.

Name	Description
	• **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 in the process of a reboot and should return to the Running state when complete. • **No State**: The virtual machine is not running or the application watchdog is not being used.
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. The Console Domain reboots the virtual machine if necessary to clear the problem. • **Error**: Application's sanity mechanism provided some kind of error message. • **Unknown**: Application's sanity mechanism failed.
Maximum Memory	This is a display only field. The amount of physical memory from the total server memory the virtual machine has allocated in the template file.
CPU Time	The amount of CPU time the virtual machine has had since boot. This is not the same as uptime.

Name	Description
Virtual CPUs	The maximum number of virtual CPUs that can run on System Platform server.
Domain UUID	Unique ID of the virtual machine.
Auto Start	Status of auto start - shows if the System Platform server starts automatically after a shut down operation. Available status are **True** (if auto start is set), and **False** (if auto start is not set).

Button descriptions

Button	Description
Reboot	Reboots the System Platform server and all the virtual machines running on it.
Reboot HA System	Reboots the whole High Availability Failover system that includes the primary and the secondary servers and all the virtual machines running on the primary server.
Shutdown Server	Shuts down the System Platform server and all the virtual machines running on it.
Shutdown HA System	Shuts down the whole High Availability Failover system that includes the primary and the secondary servers and all the virtual machines running on the primary server.

Related topics:

Rebooting the System Platform Server on page 97
Shutting down the System Platform Server on page 98

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

About this task

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

Procedure

1. In the navigation pane of the System Platform Web Console, click **Server Management** > **SNMP Trap Receiver Configuration**.
2. On the SNMP Trap Receiver Configuration page, complete the following fields:
   - **IP Address**
   - **Port**
   - **Community**
3. Click **Add SNMP Trap Receiver**.

Related topics:

SNMP Trap Receiver Configuration field descriptions on page 104

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 topics:

SNMP Trap Receiver Configuration field descriptions on page 104

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 topics:

SNMP Trap Receiver Configuration field descriptions on page 104

Changing the Product ID for System Platform

Before you begin

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

About this task

When you install System Platform, a default Product ID of 100111999 is set. You must change this default ID to the unique Product ID that Avaya provides.

Procedure

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

   Note:

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

Related topics:

SNMP Trap Receiver Configuration field descriptions on page 104

SNMP Trap Receiver Configuration field descriptions

Name	Description
Product Id	Product ID for System Platform Console Domain. When you install System Platform, a default Product ID of 100111999 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 topics:

Adding an SNMP trap receiver on page 102
Modifying an SNMP trap receiver on page 102
Deleting an SNMP trap receiver on page 103
Changing the Product ID for System Platform on page 103

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

User roles

System Platform users must be assigned a user role. Two user roles are available: Administrator and Advanced Administrator. The following table shows which administrative activities each role can perform.

Administrative activity	Administrator	Advanced Administrator
View list of virtual machines.	Yes	Yes
Reboot or shut down virtual machines.	No	Yes
Install solution template.	No	Yes
Upgrade System Platform.	No	Yes
Perform other administrative activities that are available under **Server Management** in the Web Console. Some of these activities include configuring network settings, viewing log files, and backing up the System Platform configuration.	Yes	Yes
Change own password.	Yes	Yes
Create, modify, or delete System Platform users.	No	Yes

Administrative activity	Administrator	Advanced Administrator
Change the password for the System Platform local LDAP.	No	Yes
Configure authentication of System Platform users against an enterprise LDAP.	No	Yes

Related topics:

Creating users on page 108
Modifying users on page 109

Managing System Platform users

By default, System Platform comes with a local LDAP server which is an OpenLDAP Directory Server installed in System Domain. A System Platform user has one of the following two roles that are defined in the local LDAP server:

- Administrator
- Advanced Administrator

System Platform installation creates two users, namely, `admin` and `cust` in the local LDAP server. These users can login to System Platform Web Console. They can also use the command line login to log in to System Domain and Console Domain. The `admin` user has the role of Advanced Administrator and the `cust` user has the role of Administrator.

You can create new System Platform users in the local LDAP server by using the **Local Management** option in the **User Administration** menu.

You can access the **Local Management** option only with an Advanced Administrator role and can perform the following functions:

- Viewing existing users
- Creating new users
- Modifying existing users
- Changing passwords for existing users
- Deleting existing users
- Changing LDAP Manager password

A user with Administrator role can only change own password.

Access restrictions for Administrator role

A user with Advanced Administrator role has no access restrictions when using System Platform Web Console. However, a user with Administrator role has access restrictions in using System Platform Web Console. The following table summarizes those access restrictions:

Menu	Option	Web page control	Access restriction
Virtual Machine Management	**Solution Template**		Denied
	Manage		Granted
	Manage	**Domain-0** link	Denied clicking the **Reboot** and **Shutdown** buttons
	Manage	**cdom** link	Denied clicking the **Reboot** button
	Manage	***VM*** links	Denied clicking the **Reboot**, **Start**, and **Stop** buttons
	View Install/ Upgrade Log		Denied
Server Management	**Patch Management** > **Download/Upload**		Denied
	Platform Upgrade		Denied
	Log Viewer		Granted
	Date / Time Configuration		Granted
	Loggin Configuration		Denied
	System Configuration		Granted
	Network Configuration		Granted
	Static Route Configuration		Granted
	Ethernet Configuration		Granted
	Alarm Configuration		Granted
	Certificate Management		Granted

Menu	Option	Web page control	Access restriction
	License Management		Granted
	SAL Gateway Management		Granted
	Failover		Denied for the **Configure**, **Delete**, **Start**, **Stop**, and **Switchover** buttons.
	Performance Statistics		Granted
	Eject CD / DVD		Granted
	File Manager		Granted
	Security Configuration		Denied
	Backup / Restore > **Backup**		Granted
	Backup / Restore > **Restore**		Denied
	Server Reboot / Shutdown		Denied
User Administration	**Local Management**		Denied
	Change LDAP Password		Denied
	Enterprise LDAP		Denied
	Change Password		Denied
	Authentication File		Denied

Note:

A user created using the **User Administration** menu in System Platform Web Console is stored in the local LDAP server and will not appear in the `/etc/shadow` file.

Creating users

About this task

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**. The Local Management page changes to accept the details of new 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 conform to all of the following content and usage rules. That is, Passwords:

   - Must contain a minimum of 8 characters.
   - Must contain one or more lowercase characters.
   - Must contain one or more uppercase characters.
   - Must contain one or more digits.
   - Must contain one or more special characters.
   - Must not be identical to any of the last 10 passwords.
   - Must not be similar to the prior password. Passwords are similar when they share a sufficiently long common substring, where removal of that substring results in a weak new password.
   - Must be changed within 90 days. At the end of this authorization interval, every user must change their password upon login to the Cdom (or Web Console) domain.
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 topics:

Local Management field descriptions on page 111

Modifying users

About this task

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 conform to all of the following content and usage rules. That is, Passwords:

   - Must contain a minimum of 8 characters.
   - Must contain one or more lowercase characters.
   - Must contain one or more uppercase characters.
   - Must contain one or more digits.
   - Must contain one or more special characters.
   - Must not be identical to any of the last 10 passwords.
   - Must not be similar to the prior password. Passwords are similar when they share a sufficiently long common substring, where removal of that substring results in a weak new password.
   - Must be changed within 90 days. At the end of this authorization interval, every user must change their password upon login to the Cdom (or Web Console) domain.
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 edited user details.

Related topics:

Local Management field descriptions on page 111

Deleting users

About this task

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

Note:

You can delete the default `cust` and `admin` users by means of 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 must delete:
3. Click **Delete User**.
4. In the dialog box that appears to confirm deleting the user, click **OK**.

Related topics:

Local Management field descriptions on page 111

Local Management field descriptions

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

Manage Users

Name	Description
User Id	User name for the user.
User Role	Role of the user. Options are: • Advanced Administrator • Administrator

Create User and Edit User

Name	Description
User Id	User name for the user.
User Password	Password for the respective user. **Note:** Passwords for all users, including `root`, must conform to all of the following content and usage rules. That is, Passwords:

Name	Description
	• Must contain a minimum of 8 characters. • Must contain one or more lowercase characters. • Must contain one or more uppercase characters. • Must contain one or more digits. • Must contain one or more special characters. • Must not be identical to any of the last 10 passwords. • Must not be similar to the prior password. Passwords are similar when they share a sufficiently long common substring, where removal of that substring results in a weak new password. • Must be changed within 90 days. At the end of this authorization interval, every user must change their password upon login to the Cdom (or Web Console) domain.
Confirm Password	Reenter the password for the user.
User Role	Role of the user. Options are: • Advanced Administrator • Administrator

Related topics:

Creating users on page 108
Modifying users on page 109
Deleting users on page 110

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.

System Platform first attempts to authenticate a user against the Access Security Gateway (ASG), if present. 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 finally 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 topics:

Configuring authentication against an enterprise LDAP on page 113

Configuring authentication against an enterprise LDAP

About this task

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

Procedure

1. Click **User Administration** > **Enterprise LDAP**.
2. Select **Enable Enterprise LDAP**.
3. Enter the appropriate information.
4. Click **Save Configuration**.
5. If the **TLS** check box was selected, click **Upload Certificate** to replace the existing enterprise LDAP certificate.

6. Click **Test Connection** to check that you are able to connect to the Enterprise LDAP server.

Note:

If you selected the **TLS** check box and could successfully connect to the enterprise LDAP server, it means that you could successfully upload the enterprise LDAP certificate.

Related topics:

Selecting enterprise LDAP certificate on page 64
Authentication against an enterprise LDAP on page 113
LDAP field descriptions on page 114

LDAP field descriptions

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	This check box enables external LDAP authentication. If you save the page without selecting this check box, the system saves the configuration without activating the enterprise LDAP authentication.
TLS	This check box enables to use Transport Layer Security (TLS).
LDAP Server	Is the Host name or IP address of the LDAP server.
User Attribute	Is the LDAP attribute for the user. This is usually **cn** or **uid**.
Port	Is 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	Is the distinguished name of the path where the user search will run. This is used for connection authentication to the LDAP server.

Name	Description
	For example, `cn=admin,ou=sv,dc=avaya,dc=com`. This parameter is used to login to the LDAP server.
User DN	Is the distinguished name of the LDAP user.
User Password	Is the password of the LDAPuser.
Enable different group search base	This check box 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 this checkbox contains a checkmark, then instead of searching under the authenticating User's DN, the system searches under the subtree specified by the **Group search base DN** . If the checkbox does not contain a checkmark, then: • 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	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 for the *%LDAP_USER%* variable, if an administrator has defined one. There are two mutually exclusive settings for this parameter: • **Username Only** – Select 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 for the *%LDAP_USER%* variable the value of the Username or

Name	Description
	User ID of the authenticating user (0123456789) before including the filter in the search for Group Information, all shown together here as follows: (&(cn=vsp-craft) (uniquemember=0123456789)) • **Full User DN** – Select to have the system search for the user's group information by substituting the authenticating user's entire 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 for the %LDAP_USER% variable the value of the DN of the authenticating user `(sid=0123456789,ou=internal ,o=avaya,c=us)` before including the filter in the search for Group Information, all shown together here as follows: `(&(cn=vsp-craft) (uniquemember=sid=0123456789 ,ou=internal,o=avaya,c=us))`
Ldap Search scope	The LDAP scope to use when searching for a user's group information under the specified **Group search base DN**, as follows: • **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	Specifies 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))`.

Name	Description
Advanced Administrator Filter	Specifies 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	Specifies 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.

Change LDAP Password

Name	Description
New Password	The LDAP administrator password, conforming to the rules displayed by clicking the **Password Rules** button.
Confirm Password	The LDAP administrator password, entered a second time for verification of the **New Password** value when you click the **Change Password** button.

Related topics:

Configuring authentication against an enterprise LDAP on page 113

Changing the System Platform LDAP password

About this task

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. Click **User Administration** > **Change LDAP Password**.

2. Enter the new password.

   Note:

   Passwords must be at least six characters long. Use only alphanumeric characters.

3. Confirm the new password.
4. Click **Save** to save the new password.

Changing your System Platform password

About this task

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

Important:

Passwords for all users, including `root`, must conform to all of the following content and usage rules. That is, Passwords:

- Must contain a minimum of 8 characters.
- Must contain one or more lowercase characters.
- Must contain one or more uppercase characters.
- Must contain one or more digits.
- Must contain one or more special characters.
- Must not be identical to any of the last 10 passwords.
- Must not be similar to the prior password. Passwords are similar when they share a sufficiently long common substring, where removal of that substring results in a weak new password.
- Must be changed within 90 days. At the end of this authorization interval, every user must change their password upon login to the Cdom (or Web Console) domain.

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.

Managing the authentication file

Authentication file for ASG

ASG stands for access security gateway. This gateway ensures that Avaya Partners access the customers' enterprise communication solutions in a secure manner. The Avaya Partners use a predetermined user ID while providing service at the customer site. This user ID is challenged by ASG and requires proper response to make the login successful. Only the Avaya Partners are able to respond to the ASG challenge and that their passwords have single-use life.

An important component of this security mechanism is the customer-specific ASG keys that ASG sets. These keys are stored in an authentication file. To enable Avaya Partners to access their system, customers have to download and install the authentic files specially prepared for their sites.

Installing an authentication file

Procedure

1. Click **User Administration** > **Authentication File**.
2. Click **Upload**.
3. In the Choose File to Upload dialog box, find and select the authentication file, and then 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.

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.

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.

Chapter 5: Configuring High Availability operation

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 topics:

Configuring locally redundant High Availability on page 135
Configuring locally redundant High Availability field descriptions on page 137

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 127 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

High Availability characteristic or behavior		Fast Reboot High Availability (FRHA)	Machine Preserving High Availability (MPHA)	Live Migration High Availability (LMHA)
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.)
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 122.)	**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

High Availability characteristic or behavior		Fast Reboot High Availability (FRHA)	Machine Preserving High Availability (MPHA)	Live Migration High Availability (LMHA)
	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.

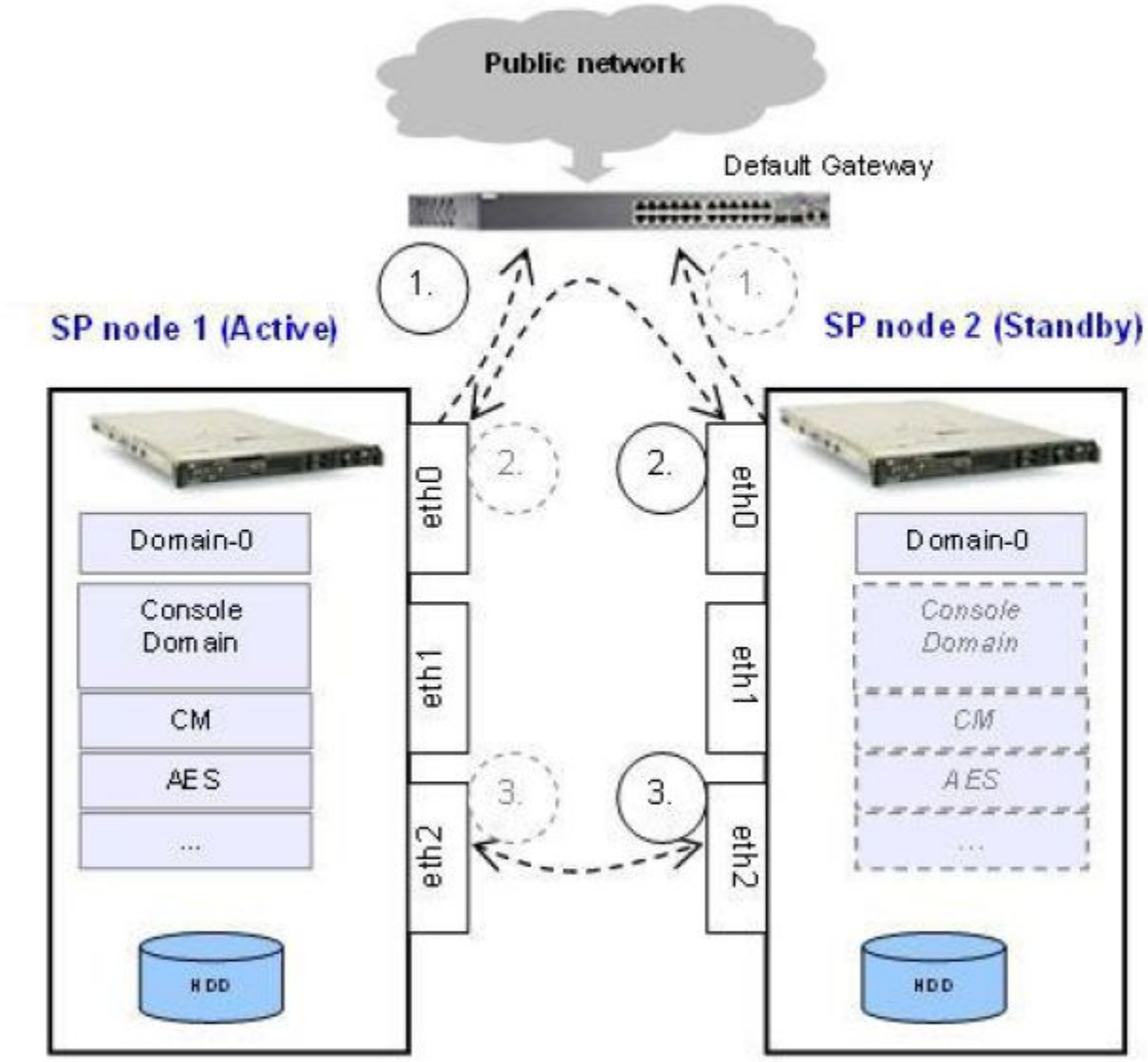
High Availability node arbitration

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
Locally Redundant High Availability Configurations	
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

Failure scenario	Outcomes
Locally Redundant High Availability Configurations	
	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 synchronization resumes when the high-speed crossover link is restored.
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 operation. Next, System Platform removes any installed templates from the standby node.

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

Important:

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:

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

System Platform supports Locally Redundant High Availability configurations

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

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

Common prerequisites for all High Availability modes

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

Servers

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

Cabling

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

Software

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

  Note:

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

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

Prerequisites for locally redundant High Availability

If your Avaya Aura® solution template will be using System Platform FRHA, and/or MPHA with LMHA High Availability modes, you must satisfy all of the common prerequisites for all HA

modes, plus the prerequisites specifically for Locally Redundant High Availability described in this topic.

Network Interface Cards (NICs)

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

Cabling

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

  Note:

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

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

Networking for locally redundant High Availability

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

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

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

  `ping <default_gateway_IP_address>`.

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

Configuring System Platform High Availability

Configuring locally redundant High Availability

Before you begin

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

You must complete:

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

About this task

- Perform this task only on the System Platform server chosen to be the Preferred (primary) Node in the High Availability pair.
- The primary server propagates its configuration to the secondary (standby) server when you start High Availability operation.
- This procedure synchronizes all required configuration settings from the preferred node to the standby node so that the standby node can assume the role of active node if required.
- 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 `Ready for Interchange` 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 topics:

About High Availability on page 121
Configuring locally redundant High Availability field descriptions on page 137

Configuring locally redundant High Availability field descriptions

Enter required values for these fields when deploying your primary and secondary System Platform servers in a locally redundant High Availability configuration.

Name	Description
Remote cdom IP address	IP Address of Console Domain on the standby node.
Remote cdom user name	User name for Console Domain on the standby node.
Remote cdom password	Password for Console Domain on the standby node.
Crossover network interface	Network interface connected to the standby server.

Related topics:

About High Availability on page 121
Configuring locally redundant High Availability on page 135
Troubleshooting steps on page 171

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:

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

High Availability stop

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

Important:

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

Once High Availability operations halt:

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

Related topics:

Starting System Platform High Availability on page 138
Stopping System Platform High Availability on page 139

Starting System Platform High Availability

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

About this task

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

Important:

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

Note:

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

High Availability start/stop on page 137

Stopping System Platform High Availability

Before you begin

Important:

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

About this task

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

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

Procedure

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

2. Click **Stop HA** and confirm the displayed warning.
   Verify the status of virtual machine replication on the High Availability page.

Manually switching High Availability server roles

Before you begin

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

About this task

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

Procedure

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

Removing the High Availability configuration

Use this procedure to permanently remove the High Availability configuration.

Before you begin

- You have stopped System Platform High Availability.

About this task

Use this procedure, for example:

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

Procedure

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

Chapter 6: System Platform security

Command line login to System Domain and Console Domain

The `admin` and `cust` user IDs can be used to 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. 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

About this task

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

About this task

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 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`
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`
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	
---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	

Permissions	Location	File name	Ownership
-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	
-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	

Permissions	Location	File name	Ownership
---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 Powerledge 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.
      You will require special cables to connect a keyboard and a VGA monitor.
   c. Connect keyboard to the location labelled 'KBD'.
   d. Connect monitor to the location labeled 'VGA'.
   e. Power up the server.
   f. Press the **F2** key to enter the BIOS setup.
2. Change the boot device by performing the following steps:
   a. Press the **Right Arrow** key until **Boot** is selected at the top.
   b. Press the **Down Arrow** until **Hard drive** is selected.
   c. Press the **+** key until **Hard drive** is at the top of the list.
   d. Press the **F10** key to save the changes and exit the BIOS setup.
3. 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 **Set Supervisor Password**.
c. Press the **Enter** key.
d. Type the password.
e. Type the same password to confirm.
f. Press the **F10** key to save the changes.

   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		

	Ports	Network/ Application Protocol	Optionally Enabled/ Disabled?	Default Port State	Notes	Column Descriptions
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.

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`
3. Type the password of the `root` user ID.
4. Type `getlogs`
5. Log out of the system.

Chapter 8: Troubleshooting

Template DVD does not mount

The template DVD does not mount automatically.

Troubleshooting steps

About this task

Procedure

1. Log in to the Console Domain as admin.
2. Type `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

Procedure

1. Log in to System Domain (Domain-0) as root.
2. Type `raid_status` with one or more of the following parameters:
   `-h`: Shows help on how to use the command

`-v`: Shows detailed RAID status information

`-s`: Shows short RAID status information; is the default output form

`-p`: Displays physical disk drive data; can be used with `-v` and `-s`

`-r`: Returns 0 if server supports RAID

Example

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

Note:

In case of physical disk information, `-s -p` is the default form of output.

Specifying `-v -s` options together will result in an invalid command.

Virtual machine has no connectivity outside after assigning dedicated NIC support

Troubleshooting steps through System Domain (Dom-0)

Procedure

1. Check if the pci ID entry is in the `/etc/rc.local and /etc/modprobe.conf`.
2. Check if the pci ID is bound properly to the pciback driver.
   If it is, a directory named `/sys/bus/pci/drivers/pciback/` should exist.
3. Check if the eth0 on virtual machine is available and IP Address is assigned (type: ifconfig -a).
4. Check if the MAC Address that is assigned to virtual machine eth0 is a physical MAC Address (type: ifconfig -a).
5. Also check if there are no error messages displayed when you type **`modinfo`** *bnx2* (where *bnx2* is a driver name).

Troubleshooting steps through System Platform Web Console

Procedure

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

General issues with the system and contacting support

Troubleshooting steps

About this task

System Platform provides a script (`getlogs`) that gathers configuration files, log files, and system status information into a compressed file (`vsp_logs_<hostname>_<date_time>.tbz`). If you run `getlogs` from an SSH session with the console domain, `getlogs` also gathers 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 reference in 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.

Result

Provide the file to your support technician.

Issues when configuring High Availability Failover

Cannot establish communication through crossover network interface

Troubleshooting steps

Procedure

Ensure that the crossover cable is properly connected to the same interface on both machines and that you selected correct interface when configuring the High Availability Failover.

Local IP address provided

Troubleshooting steps

Procedure

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

Standby first-boot sequence is not yet finished

Troubleshooting steps

About this task

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

Procedure

Provide enough time to complete this start-up process and try configuring High Availability Failover again later.

Note:

The machine can take up to 5 minutes until this process is finished from the moment you can log in into System Domain (Dom-0).

Cluster nodes are not equal

Troubleshooting steps

About this task

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

Procedure

Either use another server that has the same or better configuration parameters or swap the servers so that the weaker server becomes preferred node.

Note:

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

A template is installed on remote node

Troubleshooting steps

About this task

A solution template is installed on the standby node.

Note:

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

Procedure

Either 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

About this task

Either public and 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

About this task

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

Procedure

Ensure that this 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

About this task

Versions of System Platform are not the same on both cluster nodes. System Platform forbids 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

About this task

A solution template is installed on the standby node.

Note:

System Platform forbids 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

About this task

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

- check each machine's ability to communicate with the network
- compute each machine's score to run resources

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

Procedure

Check 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. Execute `# getlogs` command on preferred node.
3. Provide the resulting `vsp_logs_<hostname>_<date_time>.zip` compressed file to your support technician.

Active server fails

Troubleshooting steps

About this task

Procedure

Disconnect the main network cable only from the active server.

Result

The standby server become active.

Note:

Ensure that the crossover connection is working fine before the test.

Data switch fails

Troubleshooting steps

About this task

Procedure

1. Disconnect the main network cable from both active and standby server.
2. Reconnect the cables after few minutes.

Result

Previous active server remains as active.

Note:

Ensure that the crossover connection is working fine before the test.

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

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

About this task

If from any reason (for example, in case of power outage) system rebooted without initiating shutdown procedure, the LDAP can prevent to start on next boot up sequence. In that case all users that are stored in LDAP database will not be able to log in.

Procedure

Log in to the system console as user that is not using LDAP credentials and execute 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

About this task

Note:

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

In this case all services are still running on the preferred node. Use this procedure to restart High Availability Failover after the standby node is reinstalled with System Platform of the same version 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**.

    You can 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 topics:

Configuring locally redundant High Availability field descriptions on page 137

Re-enabling failed standby node to High Availability Failover

Related topics:

System Platform backup on page 89
Re-enabling failed preferred node to High Availability Failover on page 173

Troubleshooting steps

About this task

Note:

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

In this case all the services are still running on the preferred node. To re-enable standby node after it was reinstalled withSystem Platform of the same version as currently active node, perform the following steps:

Procedure

1. Log on to active node webconsole as admin user and navigate to **Server Management** > **Failover**.
2. Execute the “Stop Failover Mode” operation from the active node webconsole.
3. After the webconsole is accessible again, log on to active node webconsole as admin user and navigate to **Server Management** > **Failover**.
4. Execute the “Remove Failover” operation.
5. Execute the “Configure Failover” operation with newly reinstalled standby node.

6. Execute the “Start Failover Mode” from the active node webconsole.

Re-enabling failed preferred node to High Availability Failover

Related topics:

System Platform backup on page 89
Re-enabling failed standby node to High Availability Failover on page 172

Troubleshooting steps

About this task

In this case all the services are running on the standby node. However, 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 new primary network card (the card with eth0 and eth1 NICs) must be re-enabled

If you plan to re-enable into HA system the machine that fits to any of the above conditions, 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 previously used preferred node with the same primary network card, some additional steps are required that are not available on the Web Console. Contact Avaya Support to assist you with resolving this condition.

Important:

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

Multiple reinstallations can result in an out of memory error

If an installation wizard is used 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

About this task

Perform the troubleshooting steps given here 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. Type `su`
   c. Type `/sbin/service tomcat restart`
3. Start the pre-installation Web application.
4. Install the template.

Chapter 9: Fault detection and alarming

Hardware fault detection and alarming

System Platform uses a combination of IPMI (Intelligent Platform Management Interface) and RAID tools to monitor server hardware health. System Platform periodically uses IPMI to query sensor data, and generates an alarm for each sensor that is in 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 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 `ipmitool` command (“Planar 3.3V” from the example in the table above) is the *component* in the alarm string.

RAID tools constantly monitor RAID health and 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

The monitored chassis-related faults for S8800 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

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

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.

Refer to the HP ProLiant Servers Troubleshooting Guide at http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c00300504/c00300504.pdf 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

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:

Message	Note
Storage Service EventID: 2048	Device failed
Storage Service EventID: 2049	Physical disk removed
Storage Service EventID: 2056	Virtual disk failed / Virtual disk consistency check failed
Storage Service EventID: 2057	Virtual disk degraded
Storage Service EventID: 2076	Virtual disk failed / Virtual disk consistency check failed
Storage Service EventID: 2080	Physical disk Initialization or rebuild fail
Storage Service EventID: 2083	Physical disk Initialization or rebuild fail

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

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 RAID alarms for the S8510 server are as summarized below:

Message	Note
Storage Service EventID: 2048	Device failed
Storage Service EventID: 2049	Physical disk removed
Storage Service EventID: 2056	Virtual disk failed / Virtual disk consistency check failed
Storage Service EventID: 2057	Virtual disk degraded
Storage Service EventID: 2076	Virtual disk failed / Virtual disk consistency check failed
Storage Service EventID: 2080	Physical disk Initialization or rebuild fail
Storage Service EventID: 2083	Physical disk Initialization or rebuild fail
Storage Service EventID: 2102	Temperature exceeded the maximum failure threshold

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

Refer to the Systems Hardware Owner's manual found at http://support.dell.com/support/edocs/systems/pe1950/ or to 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)

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 RAID alarms for S8800 server are as summarized below:

Message	Note
Drive Slot sensor Drive [0–9]+[^\-]*- Drive Presented Deasserted	This message indicates that 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.

Message	Note
Drive Slot sensor Drive [0–9]+[^\-]*- In Rebuild Abort Asserted	The rebuild has failed.

Refer to the Problem Determination and Service Guide at ftp://ftp.software.ibm.com/systems/support/system_x_pdf/59y6780.pdf for more information on troubleshooting and fault resolution.

For S8300D

System Platform does not monitor hardware on the S8300D server.

General software faults

Alarm text	Problem/Action
VSP WebConsole cannot start due to `libvirt_jni` cannot be found.	Check the existence of `/usr/local/lib/libvirt_jni.so` on cdom; if it is a symbolic, ensure it points to a valid shared lib.
VSP WebConsole cannot start due to missing configuration file (vsp.properties).	Check the existence of `/opt/avaya/vsp/tomcat/lib/vsp.properties` on cdom.
VSP Webconsole encountered problem while starting, restarting or stopping of NTP Service.	Check the logs of the system by enabling FINE in the `/opt/avaya/vsp/tomcat/webapps/webconsole/WEB-INF/classes/log4j.xml` file on cdom, or check that the NTP service exists.
VSP Webconsole encountered problem running `/opt/avaya/vsp/bin/vsp_rsyslog_rotate.sh`	Check existence of `/etc/logrotate.d/vsp_rsyslog` and permissions (should be 644 and owned by root/root) on cdom.
VSP Webconsole encountered problem with `log4j.xml` file.	Check the existence of `/opt/avaya/vsp/tomcat/webapps/webconsole/WEB-INF/classes/log4j.xml` on cdom.
CDom Webconsole tomcat died.	Check tomcat log files in `/opt/avaya/vsp/tomcat/logs/catalina.out` on cdom.
VSP Backup failed.	Check the details in `/vspdata/backup/backup.log` log file.

Alarm text	Problem/Action
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. Click **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 that is currently able to accept email. Check the details in `/var/log/vsp/vsp-all.log`.
Restore of archive file <archive> failed.	Check the details in `/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 health of any virtual machines that were 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 contract for the frequency of the heartbeat (how often to expect 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.

Alarm text	Problem/Action
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 virtual machine's name 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	Check 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>	Free some space on logical volume <lv> Troubleshoot the virtual machine.
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. Click **Virtual Machine Management** > **Manage**. Click the **cdom** link. Click **Reboot**. **Note:** If unable to log in to System Platform Management Console, use the `xm reboot` command while logged in to dom0.

Alarm text	Problem/Action
VSP High Webconsole open files	Log in to the System Platform Management Console. Click **Virtual Machine Management** > **Manage**. Click the **cdom** link. Click **Reboot**. **Note:** If 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. Click **Virtual Machine Management** > **Manage**. Click the **cdom** link. Click **Reboot**. **Note:** If 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. Click **Virtual Machine Management** > **Manage**. Click the **cdom** link. Click **Reboot**. **Note:** If 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.
VSP Webconsole encountered problem while removing template virtual machines from failover.	Check the details in `/var/log/vsp/vspha.log` log file in dom0.
VSP Webconsole encountered problem while adding template virtual machines into failover.	Check the details in `/var/log/vsp/vspha.log` log file in dom0.
VSP Webconsole encountered problem while upgrading console virtual machine.	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
Crossover connection between the machines is broken (raised on <hostname>)	Check the crossover network connection between the machines

Alarm text	Problem/Action
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

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

G

H

I

L

M

N

P

R

S

T

U

V

W