Administering Avaya Aura™ System Platform

Release 1.1.1
April 2010

Notices

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site: http://www.avaya.com/support

Licenses

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://www.avaya.com/support/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

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 Products, 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 Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). Customer 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). Customer 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 Product that permits one user to interface with the Product.

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use 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 identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/ThirdPartyLicense/

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 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://www.avaya.com/support/

Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya and Avaya Aura are registered trademarks of Avaya.

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

PuTTY is copyright 1997-2009 Simon Tatham.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya Inc. provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: Administering System Platform

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 Management 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 solutions 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 2 802.1 p tagging). However, System Platform supports tagging of packets for QOS at the Layer 2 switch.

System Platform Management Console overview

The System Platform Web interface is called System Platform Management Console. After installing System Platform, you can log on to the System Platform Management Console to view details of System Platform virtual machines (namely, System Domain (Dom-0) and Console Domain) and install the required solution templates, such as Midsize Business Template and perform various administrative activities by accessing options from the navigation pane.

The system displays the administrative options under three categories as follows:

- **Virtual Machine Management**

  Components of System Platform and of the solution templates installed on the System Platform server are known as virtual machines. You can view details and manage the various virtual machines by using the options displayed under **Virtual Machine Management**.

- **Server Management**

  You can perform various administrative activities for the System Platform server such as configuring various settings for the server, viewing log files, upgrading to a latest release of the software, and backing up and restoring current version of the software by using the options displayed under **Server Management**.

- **User Administration**

  You can view existing user profiles for System Platform Server, create new user profiles, edit existing user profiles, and change existing passwords by using the options displayed under **User Administration**.

Note:

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 or udom) provides management access to the system through System Platform Management Console.

Accessing System Platform Management Console

You can view the System Platform information by accessing the System Platform Management Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. On a Web browser, type the following URL: https://*ipaddress*/webconsole, where ipaddress is the IP address for the Console Domain that you configure during the System Platform installation.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

2. Enter a valid User ID.

   Important:

   The standard login/passwords are root/ root01, admin/ admin01, and cust/ cust01. The root and admin logins have advanced administrator capabilities,

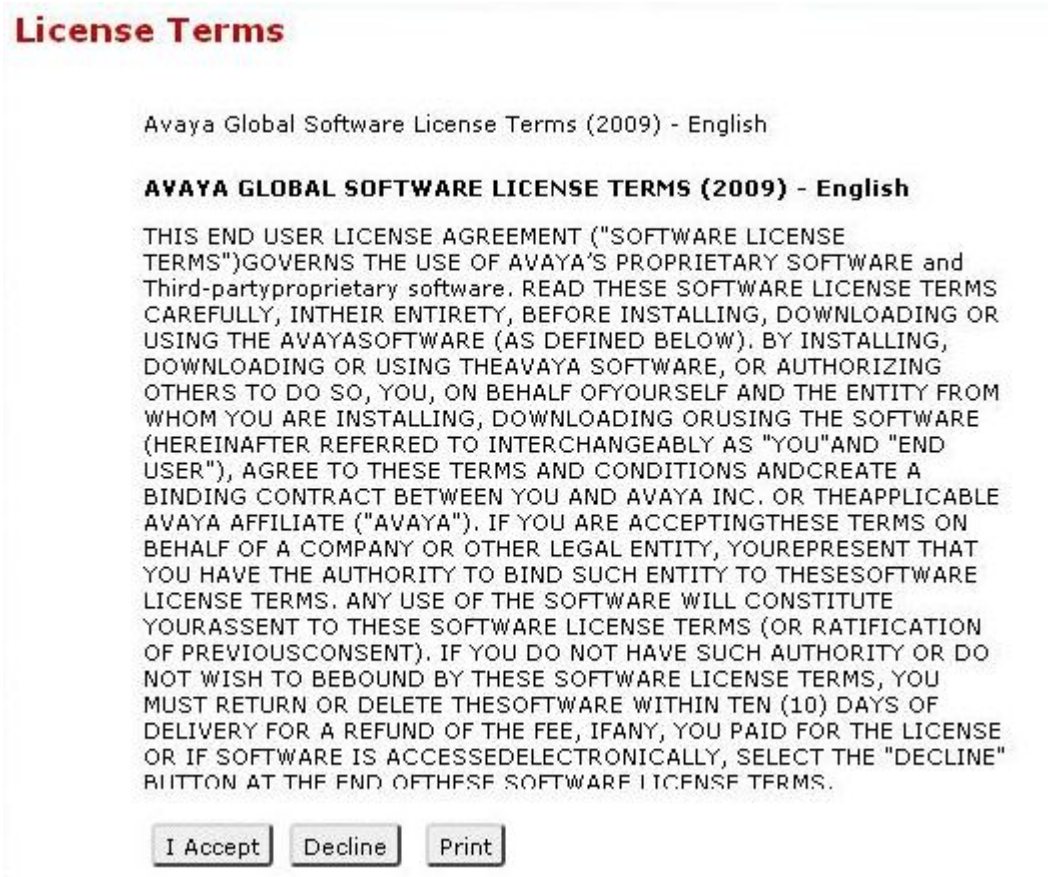
while the cust login has normal administrator capabilities. The root login is not allowed for general login.

Avaya recommends that you change these default passwords after your first login. Passwords must be at least six characters long. Avaya recommends using only alphanumeric characters.

The craft login uses ASG feature. If you are using craft login, you must have the ASG tool on your desktop to generate a response based on the request generated by the login page.

3. Click **Continue**.
4. Enter a valid Password.
5. Click **LogOn**.

   The system displays the License Terms page when you log in for the first time.



6. Click **I Accept** to accept the end user license agreement.

   The system displays the Virtual Machine List page in the System Platform Management Console. The various administrative options are located in the left navigation menu.

Accessing System Platform through services port

You must enable IP forwarding on System Domain (Dom-0) to access System Platform through services port. You can set IP forwarding status as enabled or disabled during System Platform installation. If you set the status as disabled during installation, and want to change the status later, perform the following steps:

1. To enable IP forwarding:
   a. Log on to System Domain (Dom-0) as admin.
   b. In the command line, type **`ip_forwarding enable`** and press `Enter`.
2. For security reasons, you should always disable IP forwarding after finishing your task. Perform the following tasks to disable IP forwarding:
   a. Log on to System Domain (Dom-0) as admin.
   b. In the command line, type **`ip_forwarding disable`** and press `Enter`.

Virtual Machine Management

The System Domain (Dom-0) and Console Domain components of System Platform and the components of various templates installed on the System Platform server are called virtual machines. You can view details and manage the virtual machines available in the system, including rebooting or shutting down a virtual machine. The Virtual Machine List page displays

a list of all the virtual machines currently running in the system. When you click on a respective virtual machine name, the system displays all the details of the virtual machine, for example, MAC address, IP address, Operating System and so on.

Access the Virtual Machine List page either by clicking **Home** or by clicking **Virtual Machine Management** > **Manage**. The system displays the Virtual Machine List page when you log on to the System Platform Management Console for the first time.

Virtual Machine Management field descriptions

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 virutal 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 and is not the same as up time.
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 in the process of a reboot and should return to running when complete. • **No State** The virtual machine is not running or the application watchdog is not being used.

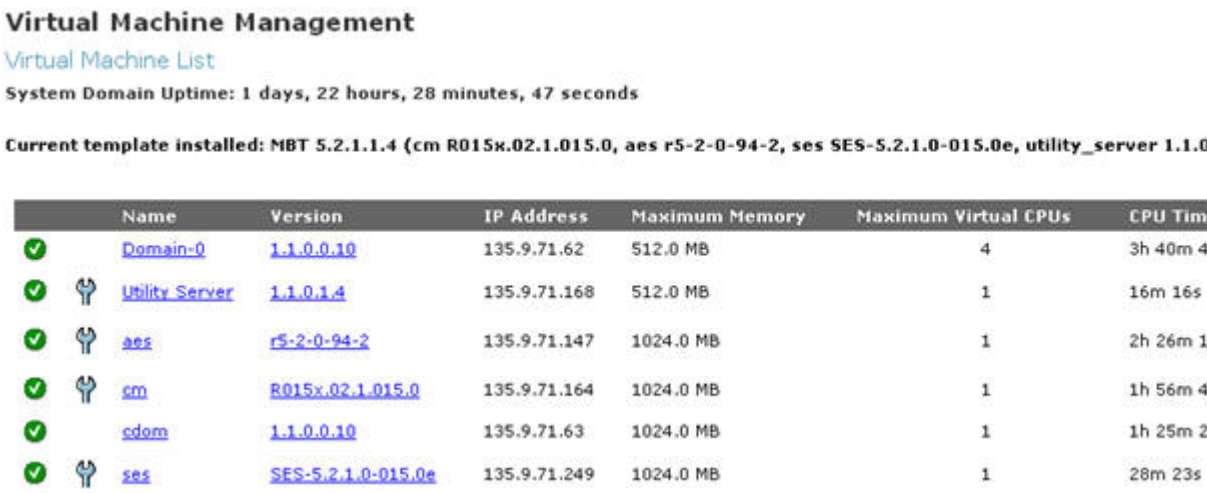
Name	Description
Application State	Current status of the application (respective virtual machine). Possible values are as follows: • **Starting** Application is currently booting and should enter a running state when complete. • **Running** Application is running normally. • **Stopped** Application has 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, signifying a problem and may result in the Console Domain rebooting the virtual machine to clear the problem. • **Error** Application's sanity mechanism provided some kind of error message. • **Unknown** Application's sanity mechanism failed.

Virtual Machine Management button descriptions

Name	Description
Refresh	Refreshes the lists the virtual machines.

Viewing details of a virtual machine

1. Click **Virtual Machine Management** > **Manage**.
   The system displays a list of virtual machine currently running on the server.



2. On the Virtual Machine List page, click the virtual machine for which you want to see the details.
   The Virtual Machine Configuration Parameters page displays the configuration details for the virtual machine.

Rebooting a virtual machine

1. Click **Virtual Machine Management** > **Manage**.
2. On the Virtual Machine List page, click the virtual machine which you want to reboot.
3. On the Virtual Machine Configuration Parameters page, click **Reboot**.

Shutting down a virtual machine

1. Click **Virtual Machine Management** > **Manage**.
2. If you want to stop a virtual machine, then click the entry corresponding to 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. If you want to shutdown the server, do one of the following steps:

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

     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**.

Virtual Machine Configuration Parameters field descriptions

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 in the process of a reboot and should return to running when complete. • **No State** The virtual machine is not running or the application watchdog is not being used.

Name	Description
Application State	State of virtual machine as communicated by the watchdog. A virtual machine may include an application watchdog. This 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 being shutdown 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, signifying a problem and may result in the Console Domain rebooting the virtual machine to clear the problem. • **Error** Virtual machine's sanity mechanism provided some kind of error message. • **Unknown** Virtual machine's sanity mechanism failed.
Used Memory	The amount of memory currently used by the virtual machine.
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 and is not the same as up time.
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.

Virtual Machine Configuration Parameters button descriptions

Button	Description
Reboot	Reboots the respective virtual machine. In the case of System Domain (Dom-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 (Dom-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 Management 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 the virtual machines running on it.

Solution template

After installing System Platform you can install various solutions templates to run on System Platform. These templates can be Midsize Business Template, Modular Messaging and so on. After installing the templates on System Platform, you can manage the templates from the System Platform Management Console.

See *Installing a solution template* section in *Installing and Configuring Avaya Aura™ System Platform* for more information.

Server management

Server Management overview

You can perform various administrative activities for the System Platform server such as configuring various settings for the server, viewing log files, upgrading to a latest release of the software, and backing up and restoring current version of the software by using the options displayed under Server Management.

Patch Management

Search local and remote patch

Use the Search Local and Remote Patch page to search for the available patches in the following media locations. These media store the various patches so that you can download, upload, or install them later on System Platform:

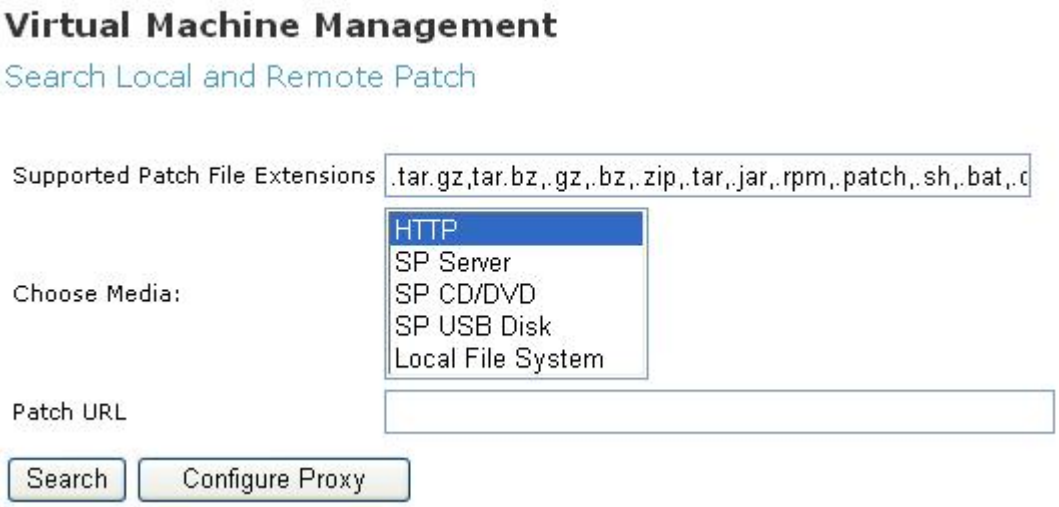
- HTTP
- SP Server
- SP CD/DVD
- SP USB Disk
- Local File System

Visit the Avaya support site (http://support.avaya.com) and refer to the latest Release Notes to find out the latest patches, and access the regular updates and patches for System Platform and the various templates provided by Avaya. You can also install or download the patches from the Avaya Product Licensing and Delivery System (PLDS) Web site (http://avaya.plds.com).

Downloading patches

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

3. On the Search Local and Remote Patch page, choose a location to search for a patch from the following options:
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Disk**
   - **Local File System**



4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to create a proxy server using the specified URL. Refer to System configuration on page 36.
6. If you selected **Local File System**, click **Browser** 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**.

Installing patches

Important:

If you plan to install a patch on a High Availability system, see Installing System Platform patches on High Availability systems on page 21 for details before you install the patch.

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:

Installing System Platform patches on High Availability systems on page 21

Installing System Platform patches on High Availability systems

Unless the Release Notes for the patch state otherwise, if the patch includes a System Domain (Dom-0) patch, you must install the patch on both the active and standby nodes. You must stop High Availability before installing such patch and then install the patch on both the primary and secondary node.

Note:

If you install the patch before stopping High Availability, you must remove the patch, stop High Availability, and then reinstall the patch. Otherwise, you will not be able to install the patch on the standby node. The standby node will inaccurately report that the patch is already installed and prevent you from installing it.

1. Log in to System Platform Management Console.
2. Click **Server Management** > **Failover**.

3. Click **Stop Failover Mode** and confirm the warning that is displayed.
   System Platform Management Console redirects to the Reboot page and after a few minutes redirects to the Login page.
4. Log in to System Platform Management Console of the active node again and install the patch.
5. Log in to System Platform Management Console of the standby node and install the patch.
6. On System Platform Management Console of the active node, click **Server Management** > **Failover**.
7. Click **Start Failover Mode** and confirm the warning that is displayed.

   System Platform Management Console redirects to the Reboot page and after a few minutes redirects to the Login page.

Related topics:

Installing patches on page 20

Removing patches

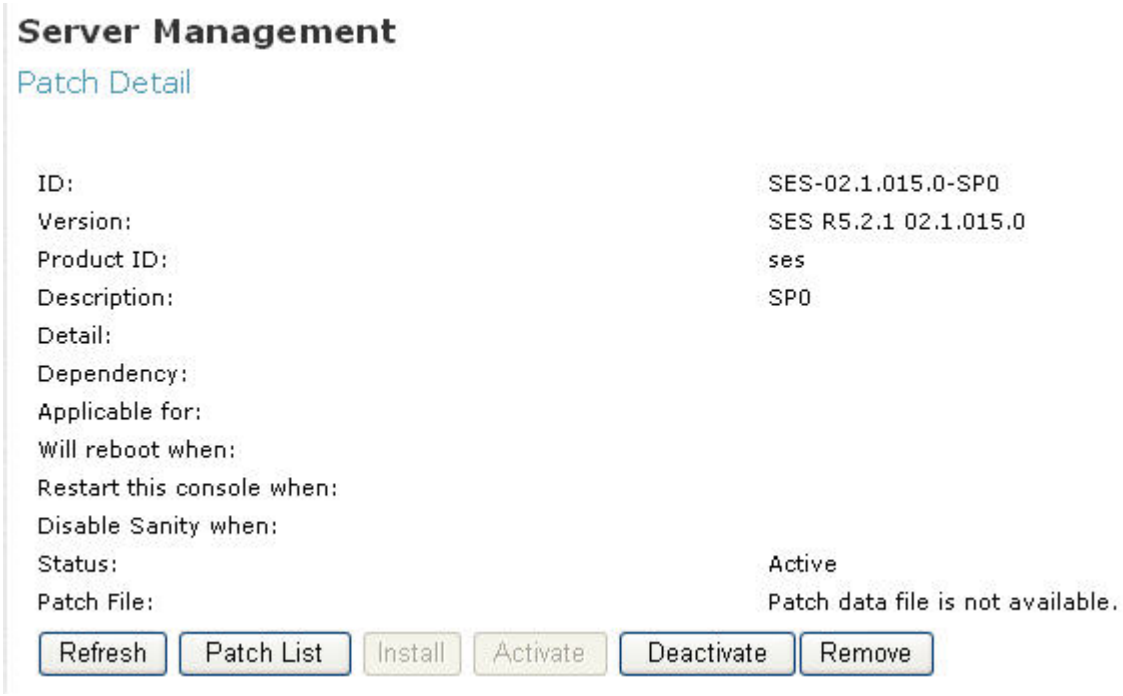
Unless the Release Notes for the patch state otherwise, if the patch includes a System Domain (Dom-0) patch, you must remove the patch from both the active and standby nodes. You must stop High Availability before removing such patch and then remove the patch on both the primary and secondary node.

Note:

If you removed the patch before stopping High Availability, you must install the patch again, stop High Availability, and then remove the patch from both machines. Otherwise, you will not be able to remove the patch from the standby node. The standby node will inaccurately report that the patch is already removed and prevent you from removing it.

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 want to remove.

4. On the Patch Detail page, click **Deactivate**.
5. Click **Remove**.



Note:

You can clean up the hard disk of your system by removing a patch installation file that is not installed. To do so, in the last step, click **Remove Patch File**.

Search Local and Remote Patch field descriptions

Name	Description
Supported Patch File Extensions	The patch 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. The available options are as follows: **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.

Name	Description
	Tip: When you want to move files from your laptop to the System Platform Server, you may encounter some errors, as System Domain (Dom–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 on the Internet about the 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. **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.

Search Local and Remote Patch button descriptions

Button	Description
Search	Searches for the available patches in the media location you specify.
Configure Proxy	Active only when you select **HTTP** as the media location option. Opens the System Configuration page and lets you configure a proxy based on your specifications. If the patches are located in a different server (for example, HTTP), you may be required to configure a proxy depending on your network.
Upload	Uploads a patch file when **Local File System** is selected.
Download	Downloads a patch file.

Patch list

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.

Server Management field descriptions

Name	Description
System Platform	Lists the patches available for System Platform under this heading.

Name	Description
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**.
Cause Reboot	Shows if installing the patch causes the respective virtual machine to reboot.

Patch detail

The Patch Detail page provides information for a patch. The information includes patch ID or patch file name, the version, the virtual machine to which the patch belongs, and the status.

Patch Detail field descriptions

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.
Will reboot when	Shows the action (if any) that causes the selected patch to restart the virtual machine when the patch is applied.
Restart this console when	Shows the action (if any) that causes the selected patch to restart the System Platform Management Console.
Disable sanity when	Shows at what stage the sanity is set to disable.
Status	Shows if the patch is available for installing or already installed.
Patch File	Shows the URL for the patch file.

Patch Detail button descriptions

Button	Description
Refresh	Refreshes the Patch Details page.

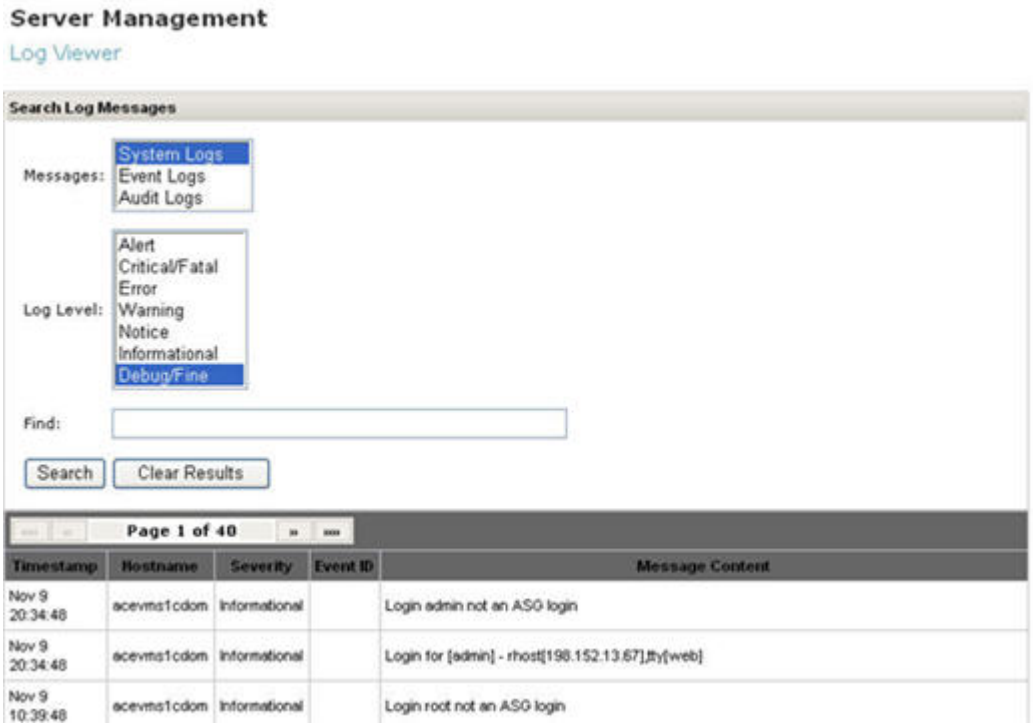
Button	Description
Patch List	Opens the Patch List page, that displays the list of patches.
Install	Installs the respective patch.
Remove	Removes the respective patch.
Remove Patch File	Removes the respective patch file.

Log viewer

Use the **Log Viewer** option to view various log messages sent by the system to the log files, after specifying the message category and the severity level of the logs.

Viewing log files

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**.

Log Viewer field descriptions

Field Names	Descriptions
Messages	Provides three types of log messages, namely **System Logs**, **Event Logs**, and **Audit Logs** sent to log files by the system. The **System Logs** are log messages generated by the System Platform operating system (syslog). The **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. The **Audit Logs** are history of commands that users have run on the History of commands that users have run on the platform.
Log Levels	The various log levels indicate the severity level of the logs for each category of log messages.
Find	Lets you search for particular log messages or log levels.
Search	Searches for the log messages based on your selection of message category and log levels.

Date and time configuration

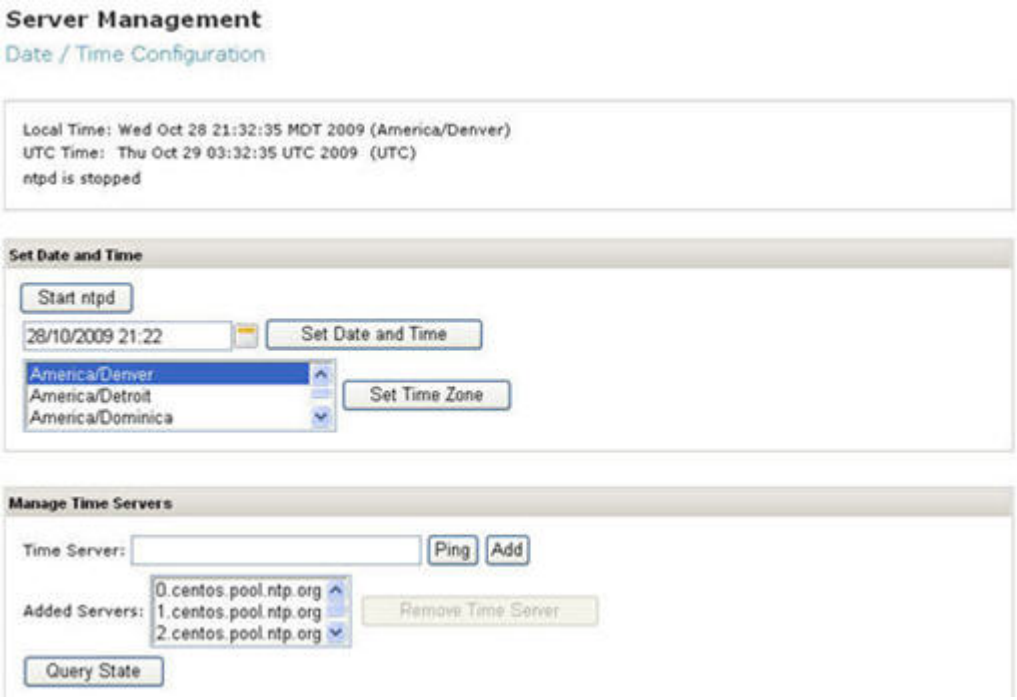
The Date/Time Configuration page displays the current settings, current time, current time zone, status of ntpd and so on. You can modify the date and time in the System Platform server, after the date and time was set during the System Platform installation. You can also turn on ntpd and change the current time zone.

Configuring date and time

Configuring the date and time are optional and you can skip these steps. However, you must set up the correct time zone for System Platform.

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

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



2. Specify a time server and click **Add** to add the time server to the configuration file.
3. Click **Ping** to check whether the specified time server, that is, the specified host, is reachable across the network.
4. Click **Start ntpd** to synchronize the System Platform time with the NTP (Network Time Protocol) server.

If you want to stop the synchronization, click the same button, which the system now displays as **Stop ntpd**.

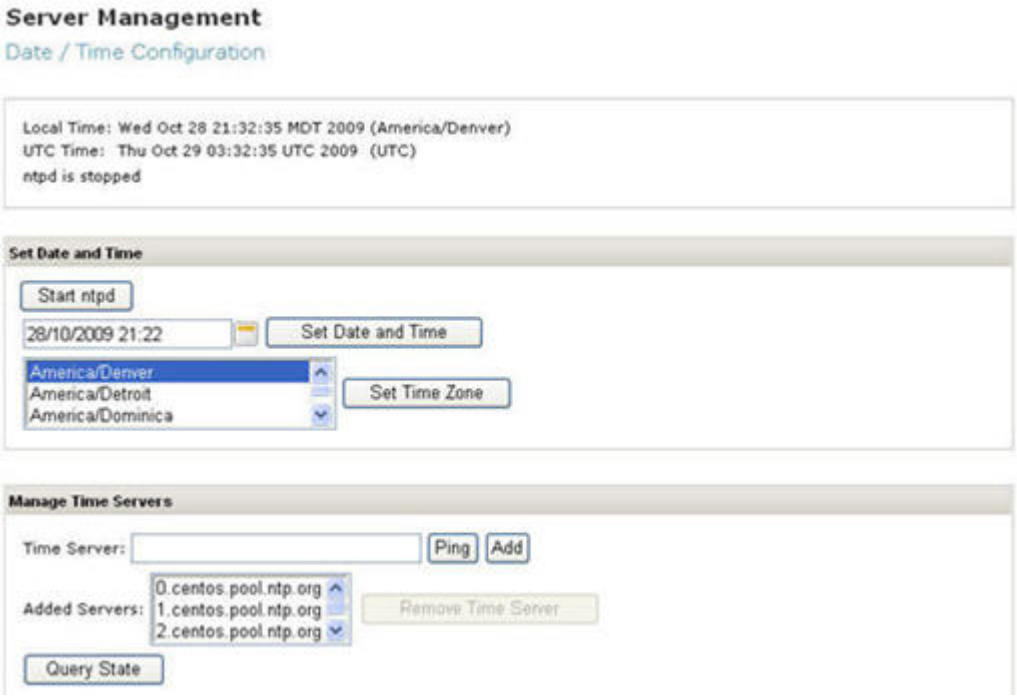
5. Select a time zone and click **Set Time Zone** to set the time zone in System Platform. The system sets the selected time zone on the System Platform virtual machines (System Domain (Dom-0) and Console Domain). The system also updates the time zone on the other virtual machines.
6. Click **Query State** to check the NTP (Network Time Protocol) status. The system displays the status of the NTP daemon on page 31 on the System Platform.

Configuring date and time using calendar option

Configuring the date and time are optional and you can skip these steps. However, you must set up the correct time zone for System Platform.

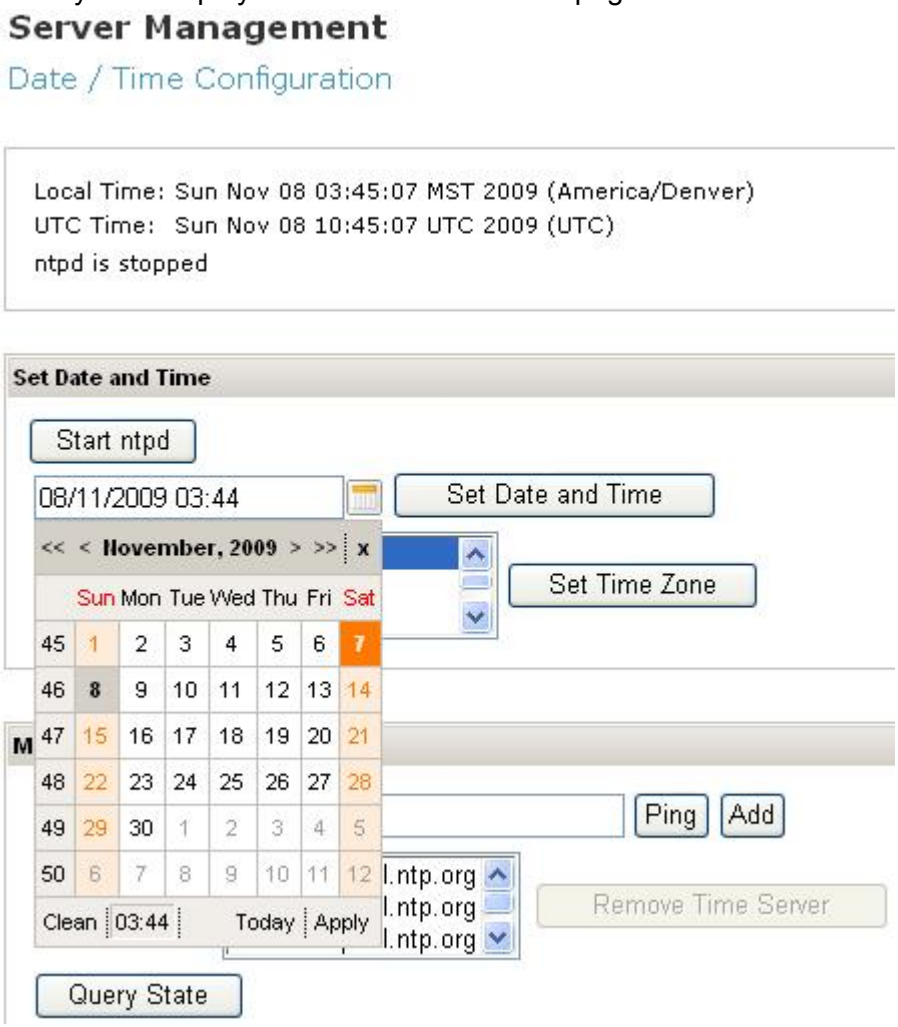
1. Click **Server Management** > **Date/Time Configuration**.

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

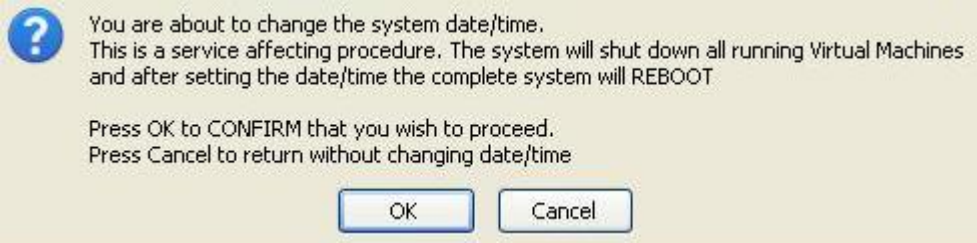


2. Click the calendar icon located next to the **Set Date and Time** button.

The system displays the Set Date and Time page.



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 pop-up screen 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 **Set 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.

NTP daemon

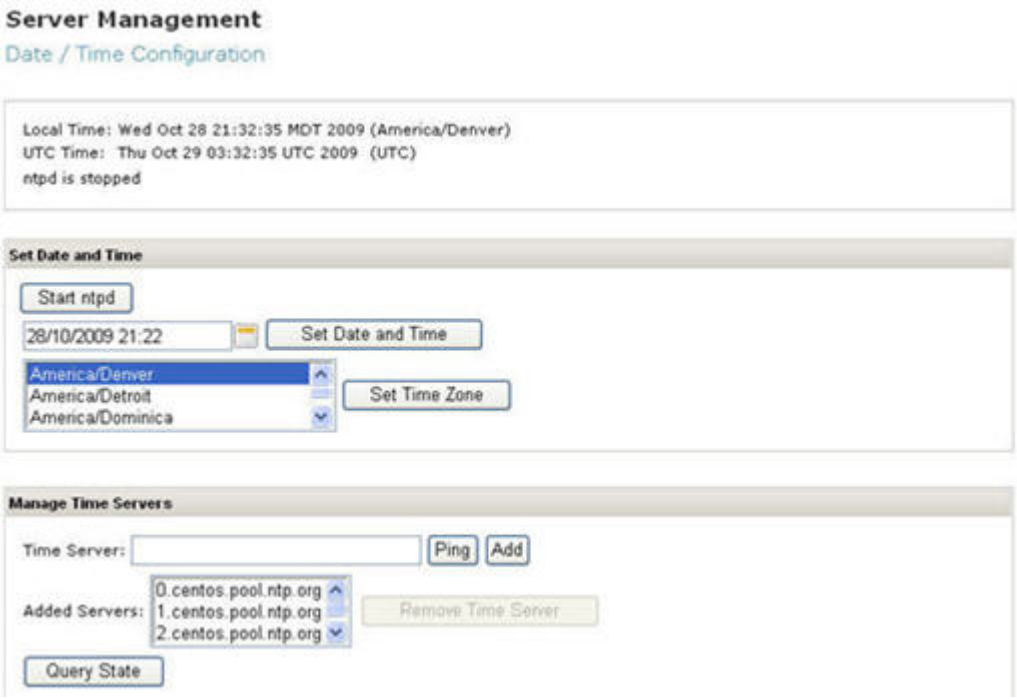
The NTP daemon reads its configuration from a file named ntp.conf. The ntp.conf file contains at least one or more lines starting with the keyword *server*. Each of those lines specify one reference time source, that is, time server, which can be either another computer on the network, or a clock connected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

Removing a time server

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

   The system displays the Server Management page with default configuration settings.



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 on restarting ntp.

Date Time Configuration field descriptions

Name	Description
Date/Time Configuration	Shows the local time and the UTC time. Also shows the status of ntpd, if it is started or stopped.
Set 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.

Date / Time Configuration button descriptions

Button	Description
Start ntpd	Starts ntpd to synchronize System Platform time with NTP (Network Time Protocol) server. If ntpd is started, the system now shows the button as Stop ntpd. You can stop ntpd by using this button.
Set Date and Time	Edits the date and time set while installing System Platform and sets the new date and time. The button will not be enabled if ntpd is running.
Set Time Zone	Edits the time zone that you set during System Platform installation. 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.
Add	Adds a time server to the EPW (Electronic Pre-installation Worksheet) file based on your specifications.
Remove Time Server	Removes the selected time server.
Query State	Check the NTP (Network Time Protocol) status.

Logging configuration

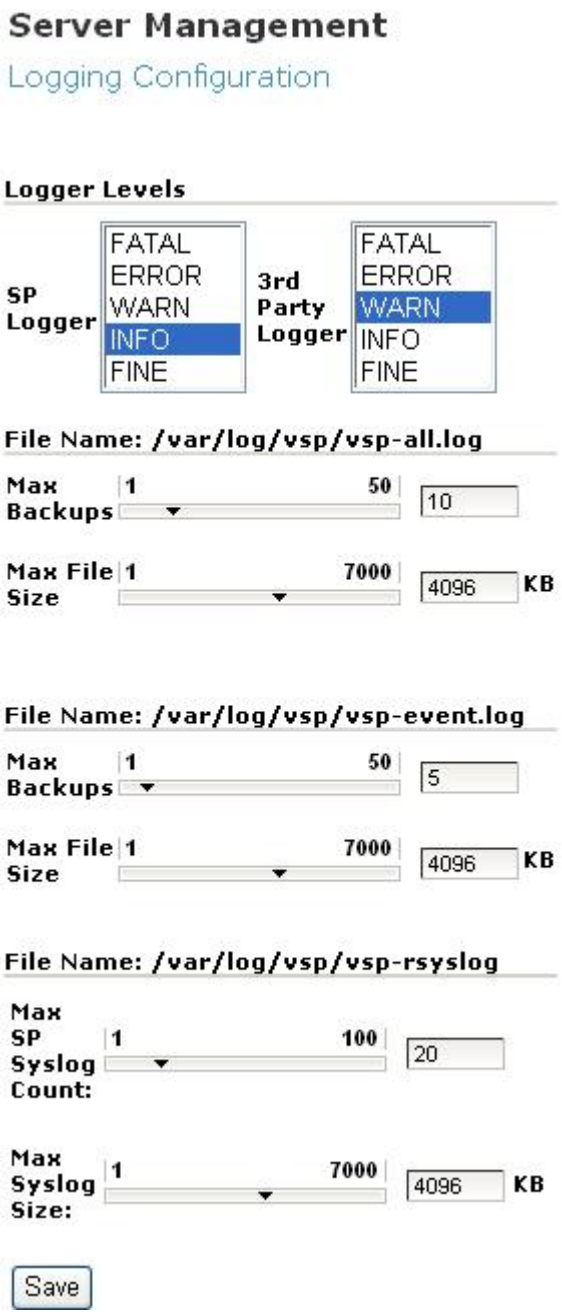
The **Logging Configuration** option lets you configure the log levels (what the log should contain) for the logs written by the system to the log files. The different log levels indicate the severity of the logs that the system writes to the log files, that is, whether you want to write INFO or high severity logs, for example, ERROR, FATAL, and so on. See Logging Configuration field descriptions on page 36 for more information.

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. So, Avaya recommends you to switch to **FINE** only to debug a serious issue.

Configuring log levels and retention parameters

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



2. Edit the default values, if required.
3. Click **Save** to save the settings.

Logging Configuration field descriptions

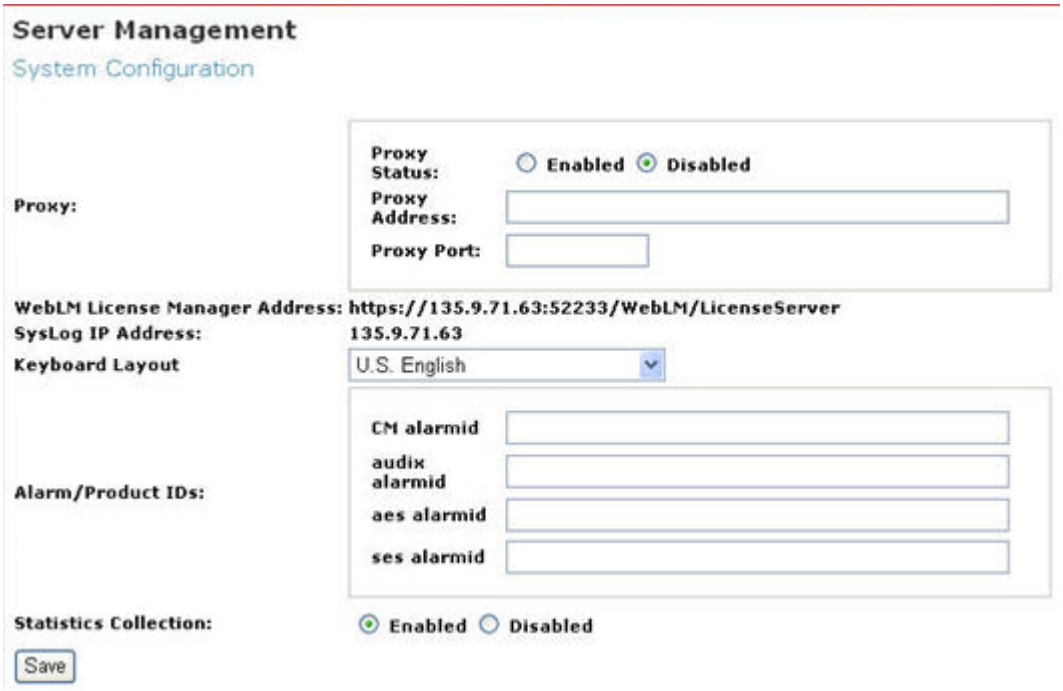
Name	Description
SP Logger	SP Logger is used for the System Platform Management Console logs which are generated by the System Platform codebase (for example, com.avaya.vsp).
3rd Party Logger	Third Party Logger is the root logger which can include logs from other 3rd-party components included in the System Platform Management Console (for example, com.* or com.apache.*).
vsp-all.log	Contains all the logs generated bySystem Platform Management Console, irrespective of whether they have eventcodes in it.
vsp-event.log	Contains all the event logs generated by System Platform Management Console. The logs in sp-event are available in Avaya common logging format.
vsp-rsyslog.log	Contains syslog messages.
Max Backups	Maximum number of backups or rotations to keep for the specified file.
Max FileSize	Maximum file size (for example, for a file vsp-all.log, once max file size is reached it will be rotated/renamed to vsp-all.log.1

System configuration

Use the System Configuration page to configure proxy settings, change the current keyboard layout, enable or disable statistics collection. See Configuring System Platform system configuration parameters on page 36 for more information.

Configuring System Platform system configuration parameters

1. Click **Server Management** > **System Configuration**.
2. Fill in the fields on the System Configuration page to configure the System Platform parameters. See System configuration field descriptions on page 37.



System configuration field descriptions

Name	Description
Proxy Status	Specifies whether an http proxy should be used to access the Internet, for example, when installing templates, upgrading patches, or upgrading platform.
Proxy Address	The address for the proxy server.
Proxy Port	The port address for the proxy server.
Keyboard Layout	Determines the specified keyboard layout for the keyboard attached to the System Platform server.
CM alarmid	Specifies alarm ID for Communication Manager.
audix alarmid	Specifies alarm ID for Communication Manager Messaging.
aes alarmid	Specifies alarm ID for AES.
ses alarmid	Specifies alarm ID for SES.
Statistics Collection	If you disable this option, the system stops collecting the statistics data.

Name	Description
	Note: If you stop collecting statistics, the system-generated alarms will be disabled automatically.

Network configuration

Note:

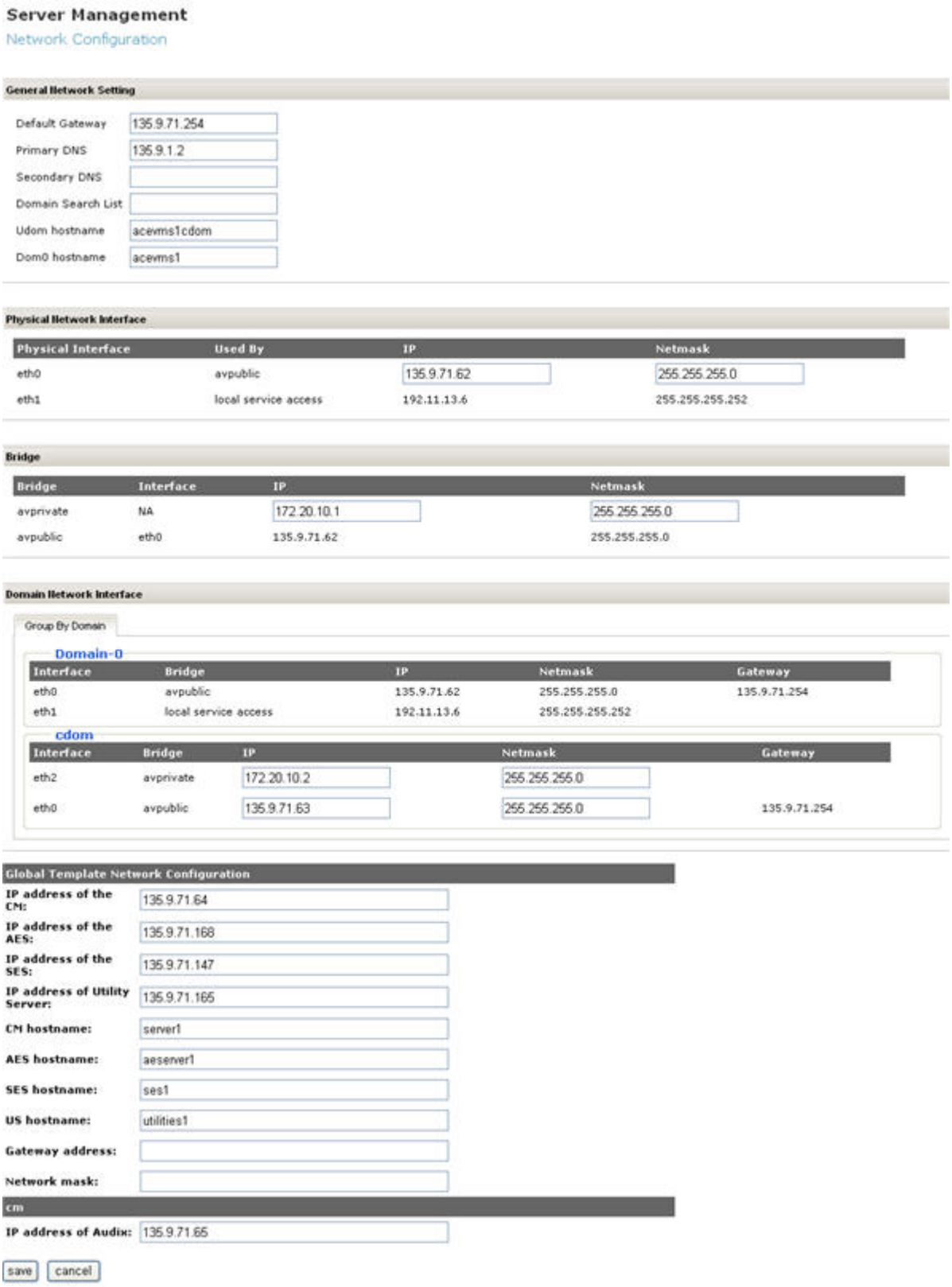
This operation is not supported while the system running in High Availability Failover Mode. To proceed to install, you will have to stop the High Availability Failover Mode. Refer to Switch between simplex and high availability failover modes on page 54 for details.

After configuring the network settings during System Platform installation, you can view and modify these settings from the **Network Configuration** option in System Platform Management Console.

When you log on to the System Platform Management Console after installing System Platform, the Network Configuration page displays the settings that you configured during the installation. When you install a template, the Network Configuration page displays additional fields based on the resources requested during template installation, such as bridges, dedicated NICs, or IP configuration for each of the guest domains created for the template.

Configuring and editing System Platform network settings

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


Server Management
Network Configuration
General Network Setting
Default Gateway 135.9.71.254
Primary DNS 135.9.1.2
Secondary DNS
Domain Search List
Udom hostname acevms1cdom
Dom0 hostname acevms1
Physical Network Interface
Physical Interface Used By IP Netmask
eth0 avpublic 135.9.71.62 255.255.255.0
eth1 local service access 192.11.13.6 255.255.255.252
Bridge
Bridge Interface IP Netmask
avprivate NA 172.20.10.1 255.255.255.0
avpublic eth0 135.9.71.62 255.255.255.0
Domain Network Interface
Group By Domain
Domain-0
Interface Bridge IP Netmask Gateway
eth0 avpublic 135.9.71.62 255.255.255.0 135.9.71.254
eth1 local service access 192.11.13.6 255.255.255.252
cdom
Interface Bridge IP Netmask Gateway
eth2 avprivate 172.20.10.2 255.255.255.0
eth0 avpublic 135.9.71.63 255.255.255.0 135.9.71.254
Global Template Network Configuration
IP address of the CM: 135.9.71.64
IP address of the AES: 135.9.71.168
IP address of the SES: 135.9.71.147
IP address of Utility Server: 135.9.71.165
CM hostname: server1
AES hostname: aeserver1
SES hostname: ses1
US hostname: utilities1
Gateway address:
Network mask:
cm
IP address of Audix: 135.9.71.65
save
cancel

3. Click **Save**.

Important:

Avaya recommends you to change all the IP addresses (wherever required) in a single instance to minimize the service disruption.

System Platform creates an internal, private bridge that allows virtual machines to communicate with each other. This private bridge does not have any 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 screen. However, it is still possible that the addresses selected conflict with other addresses in your network. Since this private bridge is not connected to your LAN, this address conflict could result in the failure of System Platform or an installed template to route packets correctly.

After the System Platform installation, check the Network Configuration page to see if the IP addresses on the private bridge conflict with addresses in the corporate network, and if there is a conflict, change the IP addresses on this page. Keep in mind that the template you install may take additional addresses on the private bridge. The range of addresses start with System Domain's (Dom-0) interface on “avprivate”.

Network Configuration field descriptions

Name	Description
Default Gateway	The default gateway.
Primary DNS	The primary DNS server address.
Secondary DNS	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. This may be changed by listing the desired domain search path following the *search* keyword with spaces or tabs separating the names.
Udom hostname	The host name of the Console Domain.
Dom0 hostname	The host name of the System Domain (Dom-0).
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	Applications with high network or time sensitive traffic may be allocated a dedicated nic. This means the virtual machine connects directly to a physical ethernet port and may require a separate cable connection to the customer network. See respective template installation topics for more information.
Bridge	The bridge details for the following:

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

Static route configuration

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

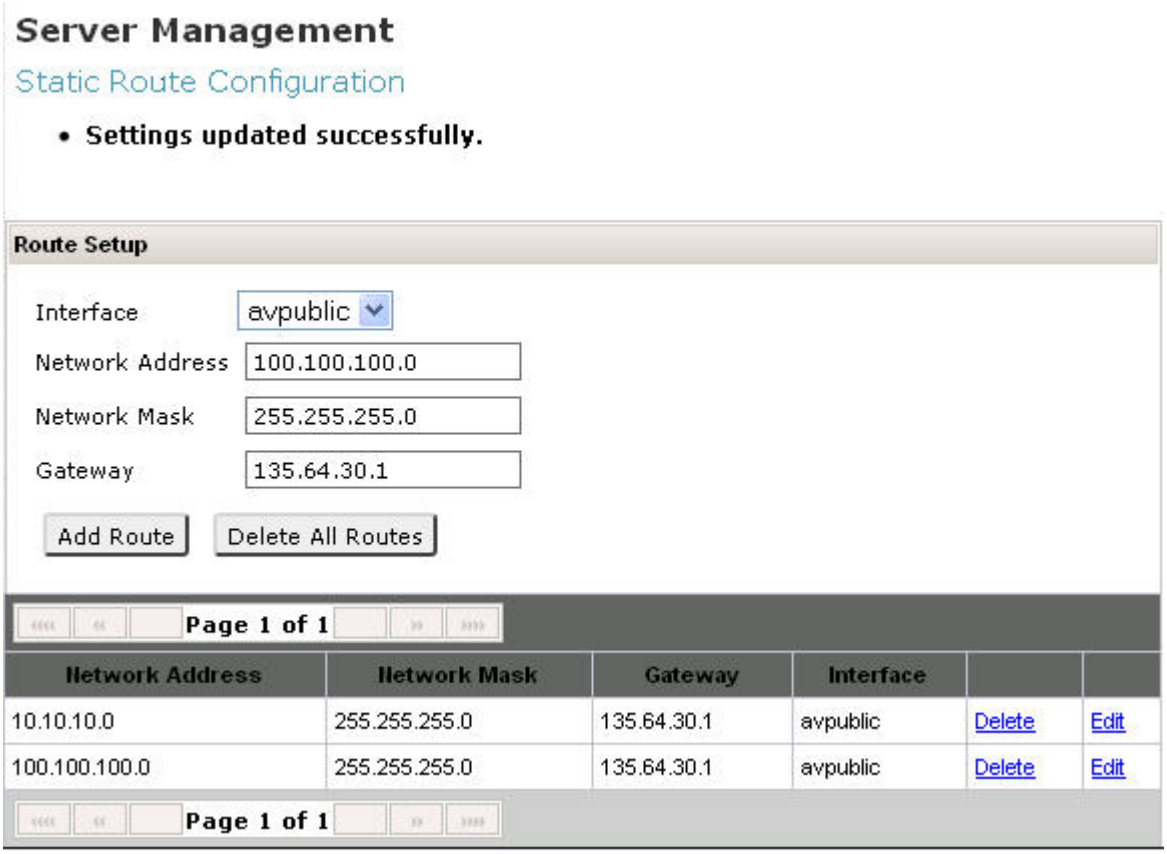
Adding a static route

1. Click **Server Management** > **Static Route Configuration**.
2. On the Static Route Configuration page, select the required interface.

3. Enter the network address.
4. Enter the network mask address.
5. Enter the gateway address.
6. Click **Add Route** add the static route with the present settings.

Deleting a static route

1. Click **Server Management** > **Static Route Configuration**.
2. Click **Delete** against a corresponding static route on the page.



Editing a static route

1. Click **Server Management** > **Static Route Configuration**.
2. Clear the **Auto-Negotiation** check box against an Ethernet interface to change.
3. Select the new Ethernet configuration from the drop-down lists.
4. Click **Apply** to save the settings.

Static route configuration field descriptions

Field Names	Descriptions
Interface	The bridge through which the route is enabled.
Network Address	The destination network for which the static route is configured.
Network Mask	The network mask for the destination network for which the static route is configured.
Gateway	The gateway or the router through which the route functions.

Ethernet configuration

Use the Ethernet Configuration page for configuring the settings of an Ethernet device and modifying the existing settings.

Editing ethernet configuration

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

   The Ethernet Configuration page displays the values for all the ethernet interfaces of the server, for example, eth0, eth1, eth2, and so on.
2. Edit the default values for etho and eth1.
3. Click **Save** to save your settings.

Ethernet configuration field descriptions

Name	Description
Speed	You can set the speed in MB, if Auto-Negotiation is disabled. The drop down menu shows the supported device speeds.
Port	Lists the available device ports, if Auto-Negotiation is disabled.
Auto-Negotiation	Specifies if speed auto negotiation is enabled. By default it is enabled, but might cause some problems with some network devices. In such cases you can disable this option.

Ethernet Configuration button descriptions

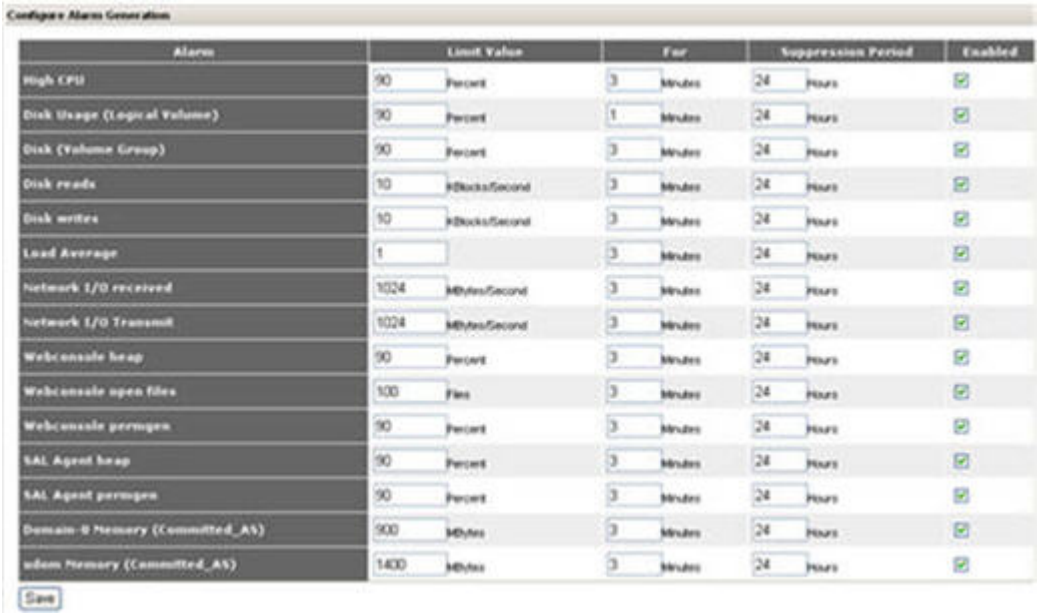
Button	Description
Apply	Saves and applies the settings for the Ethernet device.
Refresh	Refreshes the Ethernet Configuration page.

Alarm configuration

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

Configuring alarms

1. Click **Server Management** > **Alarm Configuration**.
2. On the Alarm Configuration page, edit the default values, if required.
   You can edit the parameters for the following alarms:
   - **High CPU**
   - **Disk Usage (Logical Volume)**
   - **Disk (Volume Group)**
   - **Disk reads**
   - **Disk writes**
   - **Load Average**
   - **Network I/O received**
   - **Network I/O Transmit**
   - **Webconsole heap**
   - **Webconsole open files**
   - **Webconsole permgen**
   - **SAL Agent heap**
   - **SAL Agent permgen**



3. Select the **Enabled** option to enable an alarm.
4. Enter the **Limit Value** for an alarm. This is the threshold value.
5. Specify the number of consecutive samples that must exceed the threshold value before the system generates an alarm.
6. Specify the **Suppression Period** for an alarm after the system generates the previous alarm.
7. Click **Save** to save the settings.

Alarm configuration field descriptions

Field Names	Descriptions
Alarm	Name of the alarm. The alarms are as follows: • **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)

Field Names	Descriptions
	• **Disk Writes** Disk write rate (sda) • **Load Average** Load average on each virtual machine • **Network I/O received** Network receive rate for all guests (excluding dedicated NICs) • **Network I/O Transmit** Network receive rate for all guests (excluding dedicated NICs) • **Webconsole heap** Percentage of webconsole (tomcat) heap memory in use • **Webconsole open files** Number of file descriptors webconsole has open • **Webconsole permgen** Percentage of webconsole (tomcat) permgen heap used • **SAL Agent heap SAL Agent permgen** Percentage of SAL heap memory in use • **SAL Agent permgen** Percentage of SAL permgen heap used • **Domain-0 Memory (Committed_AS)** Memory for System Domain (Dom-0) • **udom Memory (Committed_AS)** Memory for Console Domain
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 before generating an alarm.
Suppression Period	The period for which the same alarm is not repeated after sending the alarm for the first time.
Enable	Enables the selected alarm.

Managing Certificates

Certificate management

The certificate management feature allows a user with the right administrative privileges to replace the default System Platform Management 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 Management 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 Management 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 Management 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 Management 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:

Enterprise LDAP field descriptions on page 80

Selecting System Platform certificate

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

Selecting enterprise LDAP certificate

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

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

Certificate Management field descriptions

Use the Certificate Management page to receive new certificate for System Platform Management Console or Enterprise LDAP. In the case of System Platform Management 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 Management Console certificate and private key or Enterprise LDAP certificate depending on the area where the button is located.

License management

Use the **License Management** option to launch the WebLM License Manager page and manage the existing System Platform licenses.

Managing licenses

1. Click **Server Management** > **License Management** to manage licenses for the solution.

2. Click **Launch WebLM License Manager** to launch the WebLM License Manager page.
3. On the WebLM License Manager page, follow the instructions to manage licenses.

   For more information on managing licenses through Avaya WebLM, see *WebLM Administration Guide 4.5* available in the Avaya Support Site: http://www.avaya.com/support.

SAL gateway management

SAL stands for secure access link. SAL provides remote access and alarming for serviceability of templates on System Platform to Avaya service technicians and/or Avaya Business Partners. You can modify the alarm settings by logging into the SAL gateway application. See *Administering SAL on Avaya Aura™ System Platform* for details on administering the SAL gateway for System Platform.

Managing SAL settings

1. Click **Server Management** > **SAL Gateway Management**.
2. On the SAL Gateway Management page, click on the **Launch SAL Gateway Management Portal** link.
3. On the SAL Gateway page, enter your Console Domain user name and password to log in.
4. Edit the settings as required, and then click **Save**.

SAL Gateway Management button descriptions

Button	Description
Launch SAL Gateway Management Portal	Opens the SAL Gateway Management portal in a different web browser. You must provide a valid certificate details to access the portal.

System Platform Failover

System Platform High Availability Failover overview

The System Platform High Availability Failover is an optional feature. This feature offers the following capabilities:

Node scores

System Platform High Availability Failover uses node score to compute the ability of every machine to run the resources and decide on which node resources should be running for each particular situation. In the case there is no issue with the system and resources could be running on any node, both machines have the same score. Thus System Platform uses a term of “preferred node” – machine that is supposed to run the resources in the case there is no issue with the system. This preferred node has a small score benefit. So if both machines are booted up at the same time, this node will run resources.

No auto-failback

System Platform High Availability Failover does not use a feature called auto-failback that migrates resources back to the preferred node in case it reappears again and resources are currently running on the standby node. This is because there is a service impact to switching servers and if both servers are healthy then running on the preferred node offers no increased benefit. If the user wants to migrate resources back to the preferred node after a failover or a switchover, the user can do so using the **Manual Switchover** option in Failover menu during the best suitable time.

Note:

Remote reboot (also called STONITH) is disabled by default and not supported in the current version of System Platform High Availability. Remote reboot should not be configured when using High Availability.

Expected failover/switchover times

System Platform High Availability Failover uses 30 seconds as a timeout interval of lost ping replies upon which standby node will declare active node as dead (although it can be not accessible, not running or blocked). When that period expires, the standby node executes a

takeover (that is, starts resources). Note that System Platform does not provide any web interface to modify this interval.

In case of manual switchover or in case there is some state of the system that initiates preemptive failover, the total time between start of the command and time when all resources are running on the standby node includes graceful shutdown of all resources and start of all the resources:

- stop of resources - up to 5 minutes
- start of resources - up to 5 minutes
- resulting longest switchover time - up to 10 minutes

In case of failover due to total failure of the active node, the total time between the start of the outage and time when all resources are running on the standby node includes detection interval timeout and start of all the resources:

- detect active node failure - 30 seconds
- start of resources - up to 5 minutes
- resulting longest switchover time - up to 5.5 minutes

Note:

Switchover time will vary depending on hardware in use and the specific template installed on the system. Templates with more virtual machines will take slightly longer to switch over due to multiple virtual machines booting simultaneously.

See *How System Platform High Availability Failover works* for more information.

Prerequisites

The prerequisites for configuring System Platform High Availability Failover are as follows:

- Two servers with exactly the same configuration.
- Hardware supported by System Platform.
- The servers must have a spare Gigabit network interface to be used as a crossover connection dedicated exclusively to High Availability Failover services (heartbeat health checks and DRBD (Distributed Replicated Block Device) sync propagation)
- Both the servers must be in the same subnet.
- Both the servers in close proximity, approximately 10 meters.
- The same version of System Platform installed on both the active and standby nodes.
- Both the servers must be connected with a gigabit-crossover cable on the ports detected as eth2 on operating system.
- If you want to install a template on a preferred node, you must do it before starting HA.
- The standby server cannot have less memory, number of processors, and total or free disk space than the primary server.

- The standby server cannot have installed template. If present, the failover configuration will fail with an error. If you are using the bundled System Platform installation (with solution template), disable template installation on the standby server.
- Default network gateway is the System Platform High Availability Failover heartbeat's ping target and it is not a configurable parameter. Ensure that your network gateway replies to ICMP requests coming from the System Platform nodes. Heartbeat sets payload with node-identifying data and checks that the data in replied packet payload is correct. The size of these ICMP ping packets is in the range of 132-256 Bytes. If you apply firewall rules against the ping service (at the gateway), specifically packet size restriction, you must allow for packet sizes up to 256 bytes.

Configuring System Platform High Availability Failover

1. Log on to System Platform Management Console on the active server as an advanced administrator.
2. Click **Server Management** > **Failover** to display the Failover page.

   The Failover page displays the current status of failover.
3. Complete the fields on the page. See Configure Failover field descriptions on page 54 for more information.

4. Click **Create** to configure failover.
5. Click **Start Failover** only after the system completes the failover creation operation.

   The Start Failover operation blocks all the connections to the System Platform Management Console and the system redirects you to a page that informs you about the restart of Console Domain. When the System Platform Management Console is accessible again, the system redirects you to the login page automatically. You must log in again at this stage.
6. Log on to System Platform Management Console
7. Click **Server Management** > **Failover**.

You can check the status of the failover components in the Failover page and ensure that DRDB (Distributed Replicated Block Device) is synchronizing the hard disks of the two servers.

Tip:

During the disk synchronization process, you can increase or decrease the speed of the sync with a slider bar provided on the console. The default value of this rate is 30 MB. If you set the value too high, it may affect the performance of the virtual machines running on the active server.

Configure Failover field descriptions

Name	Description
Remote cdom IP address	The secondary Console Domain IP address.
Remote cdom user name	User name for Console Domain.
Remote cdom password	The password for Console Domain.
Primary network interface	The required Ethernet NIC.
Crossover network interface	The required Ethernet NIC.

Automatic switching from the active server to the standby server

When the System Platform server encounters missing heartbeat checks, the standby System Platform server becomes the active System Platform server. The system shuts down the original active server, and reboots all the virtual applications on this new active server.

The system performs the following:

- Detects problems of the active (primary) node by missing heartbeat checks during a specified period of time.
- Assigns the secondary node as a new primary node.
- Sets the Distributed Replicated Block Device (DRBD) devices as primary on the new active node.
- Boots the virtual machines on the new active node.

Switch between simplex and high availability failover modes

Switching to high availability failover mode

System Platform can be extended from simplex mode to high availability failover mode during system installation or anytime later. Once you have installed a new machine with System Platform of the same version without a template and the machine has at least the same (or

better) configuration such as the number of processors and disk space, you are ready to proceed.

Switching to simplex mode

There are two variants to switching from high availability failover mode:

Stopping high availability failover mode: If you want to stop the high availability failover and switch to the simplex mode, you can do so as soon as there is no disk synchronization in progress or the disc synchronization is not paused. The stoppage of high availability failover could lead to corruption of the file system of the standby console domain, if the condition just mentioned is not satisfied.

Removing failover configuration: If you want to remove the failover configuration permanently, you will use this variant.

Switching to simplex mode for template configuration

System Platform does not support template install, upgrade or delete operations while it runs in the high availability failover mode. You will see a warning message on template pages and not be able to execute any of these operations. To proceed with template install, upgrade or delete, you have to stop the high availability failover mode first.

Switching to high availability mode after template configuration

Once you have finished with template operation, you can start the high availability failover mode from the Failover page.

Switching to high availability failover mode

Prerequisites

The system is configured with high availability failover. Refer to Configuring System Platform High Availability Failover on page 53.

1. Click **Server Management > Failover**.
2. Click **Start Failover**.

   System Platform Management Console will redirect to the reboot page. After a couple of minutes, System Platform Management Console will redirect to the login page.
3. Log in to the System Platform Management Console.
4. Click **Server Management > Failover** and check the disc synchronization progress.

   This operation will synchronize all the required configuration settings from preferred node to the standby node so that it will be ready for takeover of resources when required. Please note that this operation will restart console domain and all template virtual machines.

Stopping high availability failover mode

1. Click **Server Management > Failover**.
2. Click **Stop Failover**.

   System Platform Management Console will redirect to reboot page. After a couple of minutes, System Platform Management Console should redirect into the login page.
3. Log in to System Platform Management Console.
4. Click **Server Management > Failover** and check the status of the high availability failover.

   Now the system is not propagating changes from the preferred node to the standby node. However the high availability failover mode is still configured so that you can start it anytime later. The template on the standby node is removed during this operation. You can now access standby System Platform Management Console using its IP address (that was provided during the configuration of high availability failover). Please note that this operation will restart the console domain and all template virtual machines. You can completely remove the node from the high availability failover. Refer to Removing failover configuration on page 56 on how to proceed.

Removing failover configuration

1. Click **Server Management > Failover**.
2. Click **Remove Failover**.

   Note:

   This operation leaves the standby console domain in inconsistent state and this node cannot be again used to configure high availability failover without reinstalling it.

Switching to simplex mode for template configuration

Note:

If you stop the high availability failover mode, System Platform removes the template (if installed) from the standby node. Every template operation can only be executed on the

preferred node. You should not try to install a template on the standby node as this prevents starting the high availability failover mode afterwards.

1. Click **Server Management > Failover**.
2. Click **Stop Failover**.

   System Platform Management Console will redirect to reboot page. After a couple of minutes, System Platform Management Console should redirect to the login page.
3. Log in to System Platform Management Console.
4. Click **Template Install/Upgrade** and proceed with template operation.

Next steps

Start the high availability failover mode from the Failover page. Refer to Switching to high availability failover mode after template configuration on page 57 for details.

Switching to high availability failover mode after template configuration

Refer to Switching to high availability failover mode on page 55 for details on how to proceed.

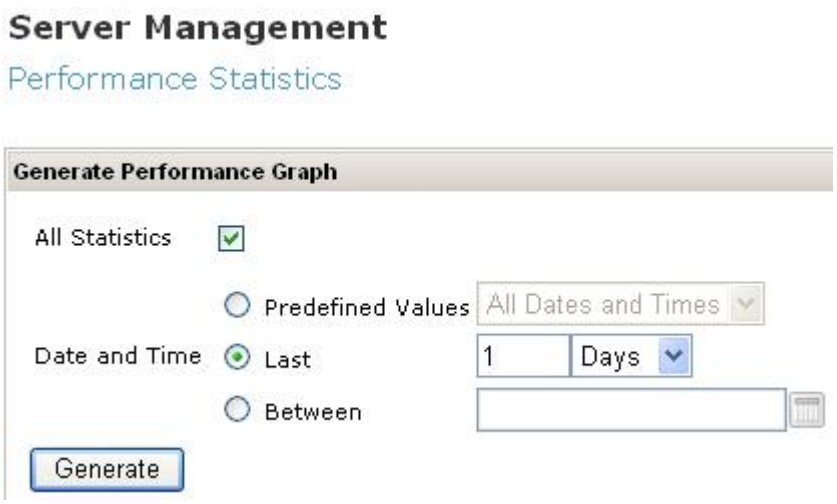
Performance statistics

Use the **Performance Statistics** option to view the status of the health and usage of the system. The Performance Statistics page lets you view the performance statistics System Platform and the hosted virtual machines.

Viewing performance statistics

The **Performance Statistics** page provides you a status of the health and usage of the system. Use this page to view the System Platform performance statistics and the hosted virtual machines.

1. Click **Server Management** > **Performance Statistics**.



2. On the Server Management page, click the **All Statistics** check box to generate a graph for all recorded statistics.
3. Clear the **All Statistics** check box, and select the type of graph from the **Type** drop down menu. Then select the required domain from the list in the **Domains** box.
4. Specify the date and time for the period you want to view the reports from.
5. Click **Generate** to generate the performance graph for the system.

Generating a graph

1. Click **Server Management** > **Performance Statistics**.
2. On the Performance Statistics page, select the required details.
3. Click **Generate**.

Exporting collected data

1. Click **Server Management** > **Performance Statistics**.
2. On the Performance Statistics page, select the required details and generate a graph.

3. Click **Download CSV File** for the data you want to download.
4. Click **Save** and specify the location to download the data.

Performance statistics field descriptions

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 you want 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 you want to generate the 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.

Eject CD or DVD

The CD or DVD used for installing System Platform and virtual machines ejects automatically after successfully completing the installation or an upgrade . However, if there is any problem during installation or upgrade, the CD or DVD remains locked in the drive. You can use the **Eject CD/DVD** option to force open the drive and take out the CD or DVD.

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

Ejecting the CD or DVD

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

File Manager

System Platform stores the solution template files and platform upgrade images in a directory in the system. The File Manager option enables you to clean up the older versions of the solution template files and platform upgrade images. However, you cannot delete the files for the currently installed solution templates.

Deleting a folder

1. Click **Server Management** > **File Manager**.
2. Select the folder file that you want to delete.
3. Click **Delete**.

Backing up System Platform

System Platform backup

You can back up configuration information for System Platform and the solution template (all virtual machines). Sets of data are backed up and combined into a larger backup archive. Backup sets are related data items that need to be backed up. When you perform a back up, the system executes all the backup sets. All the backup sets must succeed to produce a backup archive. If any of the backup sets fail, then the system removes the backup archive. The amount of data backed up is dependent 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, so that you can restore the data, 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. You can also send the backup data to an external e-mail address if the file size is not larger than 10 MB.

If a backup fails, 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.

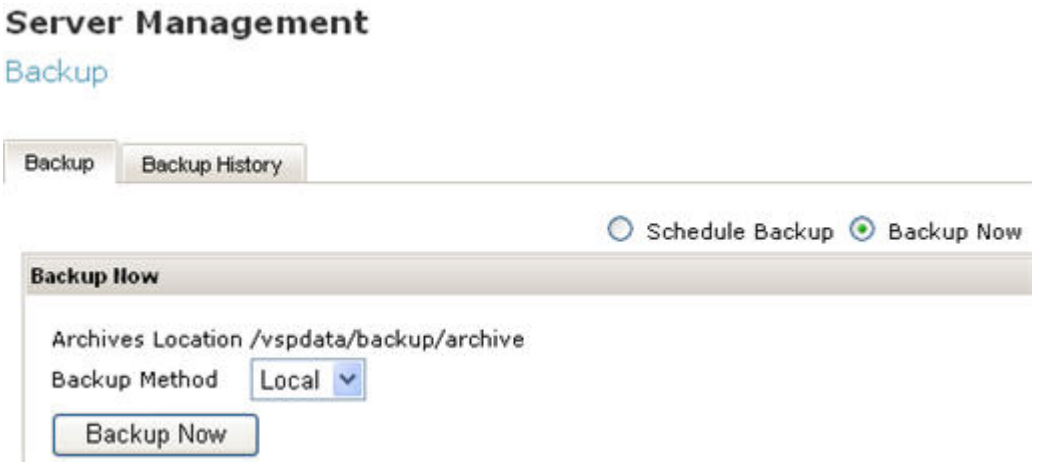
Note:
It is not the aim of the backup feature to provide a mechanism to re-enable a failed High Availability node back to High Availability configuration. Follow the instructions given in this

document on how to re-enable failed High Availability node back to High Availability configuration.

Restoring using System Platform Management Console a backup archive produced with High Availability active results in a failure. To work around this issue, take backup with High Availability disabled.

Backing up data

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.



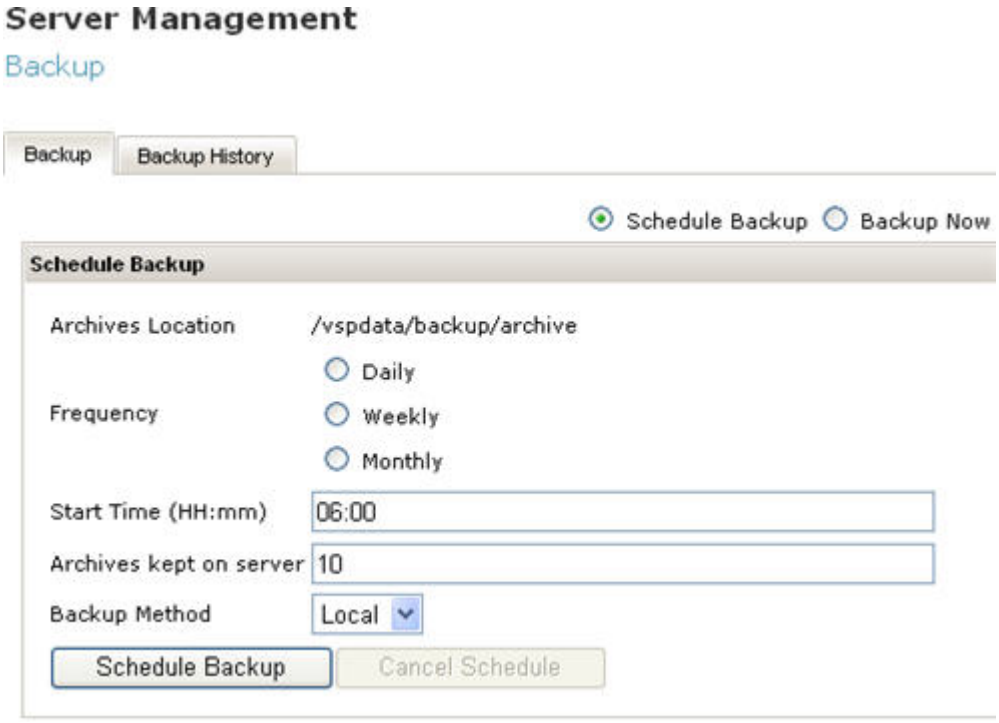
Important:
The backup file size can reach 3 GB. Ensure that you have that much of free space on the location you are keeping your backup archive.

4. Specify where to send the backup files from the following backup method options.
   - **Local**
   - **SFTP**
   - **Email**

   You can specify a remote destination to which the archive will be sent by changing the backup method. See Transferring the Backup Archives to a remote destination on page 63 for more information.
5. Click **Backup Now**.

Scheduling a backup

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Schedule Backup** option to schedule the backup operation later.



4. Specify the following:
   - **Frequency**
   - **Start Time**
   - **Archives kept on server**.
   - **Backup Method**

     You can specify a remote destination to which the archive will be sent by changing the backup method. See Transferring the Backup Archives to a remote destination on page 63 for more information.
5. Click **Schedule Backup**.

Backup field descriptions

Field Names	Descriptions
Backup Method	Lets you specify a location to send the backup files from the following options: **Local** The files are stored on System Platform under **/vspdata/backup/archive** directory. **SFTP** A copy of the file is stored in the designated SFTP host server. In the SFTP box, enter the following information: Hostname, directory, user name, and password. **Email** A copy of the backup archive is sent by an e-mail to a recipient. In the e-mail box, enter the e-mail address and the server address of the recipient.
Backup Now	Launches the backup operation.

Schedule Backup field descriptions

Field Names	Descriptions
Daily	You can schedules the backups to run daily.
Weekly	You can select the day of the week to run backups.
Monthly	You can specify a day in the month to run backups.
Start Time	The start time for the backup.
Archives kept on the server	The number of backup archives to store on System Platform. The default is 10.
Backup Method	You can specify a location to send the backup files from the available options.
Schedule Backup	You can use this option to schedule the backup process.
Cancel Schedule	You can use this option to cancel an existing backup schedule.

Transferring the Backup Archives to a remote destination

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

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

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup History** option.
   The system displays the last 10 backups executed with their dates and the status.

Restoring System Platform

Restoring backed up configuration information

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

Note:
The restore operation does not restore the High Availability configuration from the backup file. It is not the aim of the restore feature to re-enable the failed High Availability node back to High Availability configuration. Follow the instructions given in this document on how to re-enable the failed High Availability node back to High Availability configuration. Avaya recommends restoring backup before configuring and starting the High Availability mode.

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.

   Restoring an archive requires the System Platform Management Console to restart, so you must log in again when the restore operation is completed.

Restore field descriptions

Field Names	Descriptions
Restore Archive	Lists the locations from where you can select to restore the backed up data. Also displays details of the archived data including the file name and creation date. **Local** The list of archive located in the SP Server (Default location). **SFTP** Restore archive located in a remote server. You must specify the following: • **SFTP Hostname** Hostname or IP address of the remote server • **SFTP Directory** Path where the archive is located on the remote server. • **SFTP Username** Username for the remote server. • **SFTP Password** Password for the remote server • **Search** Button to search the list of archives present in the specified directory of the remote server . • **Clear Search Result** Button to clear the list of archives found on a remote server after a SFTP search. **Upload** Restore archive located in your computer.
Restore History	Displays the restore history for 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 till a successful restore action.

Viewing restore history

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

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

Shutdown or reboot the System Platform server

Use the **Server Reboot/ Shutdown** option to reboot or shutdown the System Platform server. When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform, causing potential service disruption.

Note:

If you have enabled System Platform High Availability and you have to shut down or reboot the system, check the section *Shut down the system running in High Availability mode* for details.

Related topics:

Shut down the system running in High Availability mode on page 69

Rebooting the System Platform Server

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

   Note:

   Only an Advanced Administrator user can reboot the server.
2. On the Server Reboot/Shutdown page, click **Reboot**.

Shutting down the System Platform Server

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

   Note:
   Only an Advanced Administrator user can shutdown the server.

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

Server Reboot Shutdown field descriptions

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. • **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 running when complete. • **No State** The virtual machine is not running or the application watchdog is not being used.

Name	Description
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, signifying a problem and may result in the Console Domain rebooting the virtual machine to clear the problem. • **Error** Application's sanity mechanism provided some kind of error message. • **Unknown** Application's sanity mechanism failed.
Used Memory	The amount of memory currently used by the virtual machine.
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 and is not the same as up time.
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).

Server Reboot / Shutdown button descriptions

Button	Description
Reboot	Reboots the System Platform server and all the virtual machines running on it.
Shutdown Server	Shuts down the System Platform server and all the virtual machines running on it.

Shut down the system running in High Availability mode

You can shut down the system running in High Availability mode by one of the following methods:

- Stopping High Availability and shutting down both of nodes separately
- Shutting down both nodes using CLI
- Shutting down active server followed by standby server using System Platform Management Console

Stopping High Availability and shutting down both servers separately

This is the preferred method of preparing the system for shutdown to ensure that the system is split into two independent servers. There is no chance of data loss and the timing of the operations is not that critical as using other methods.

Use this method unless there is real need to shut down the system very fast.

1. Log in to System Platform Management Console.
2. Check that the system is ready to be shutdown correctly. See Checking correct system state using System Platform Management Console on page 70.
3. Stop High Availability. See Stopping high availability failover mode.
4. Log in to System Platform Management Console on the standby server.
5. Shut down the standby server using System Platform Management Console. See Shutting down a server using System Platform Management Console on page 70.

6. Log in to System Platform Management Console on active server.
7. Shut down the active server using System Platform Management Console. See Shutting down a server using System Platform Management Console on page 70.

Checking correct system state using System Platform Management Console

Use the Failover page to identify the possible issue of the system.

1. Log in to System Platform Management Console as admin.
2. Click **Server Management** > **Failover**.
3. Check that the **Manual Switchover** button is enabled to click.

Note:

If the **Manual Switchover** button is not enabled to click, check the detailed table on the Failover page to identify the issue that is preventing manual switch over and fix it.

Important:

Do not proceed to shut down without fixing the issue.

Shutting down a server using System Platform Management Console

1. Log in to System Platform Management Console as admin.
2. Click **Server Management** > **Server Reboot / Shutdown**.
3. Click **Shutdown Server**.
4. In the warning that appears to confirm shutdown, click **OK**.
   The Shutdown page appears.

Shutting down both servers using CLI

1. Log in to currently active System Platform Management Console as admin
2. Check that the system is ready to shut down correctly. See Checking system is in correct state using CLI on page 71.

3. Stop the CRM on the standby node by typing `vspha stop-standby-crm`
4. Stop the CRM on the active node by typing `sudo service heartbeat stop`
5. Log in to System Platform Management Console on the standby server as admin.
6. Type `su`
7. Type `shutdown now`
8. Log in to System Platform Management Console on the active server as admin.
9. Type `su`
10. Type `shutdown now`

Checking system is in correct state using CLI

Use the System Platform High Availability status command to identify the possible issue of the system.

1. Log in to the currently active System Platform Management Console as admin.
2. Ensure that the system you are currently logged in is active by typing:
   `vspha status | grep 'Active node'`
   The output may appear as shown next:
   ```
   Active node : Local
   ```
3. Type `vspha status -s`
   The output may appear as shown next:
   ```
   $ vspha status -s
   Status of High Availability on the VSP
   Summary
   -------
   System status : Started
   Local CRM running : Yes
   Remote CRM running : Yes
   Remote public link : up
   Remote crossover link : up
   ```
4. In the output of step 3, check that both local and remote CRM processes are running.
   Here are the lines you must check:
   `Local CRM running : Yes`

```
Remote CRM running : Yes
```

5. In the output of step 3, check that both remote network interfaces are up.
   Here are the lines you must check:

   ```
   Remote public link : up
   Remote crossover link : up
   ```

6. Ensure that all DRBD resources are connected and fully synchronized by typing `vspha status`
   The output may appear as shown next:

   ```
   DRBD Disk Syncing
   -----------------
   0:Domain00 Connected Primary/Secondary UpToDate/UpToDate C
   1:udom0 Connected Primary/Secondary UpToDate/UpToDate C
   2:udom1 Connected Primary/Secondary UpToDate/UpToDate C
   3:udom2 Connected Primary/Secondary UpToDate/UpToDate C
   ```

   Important:
   Do not proceed to shut down without fixing the issue.

Shutting down both servers using System Platform Management Console

It is possible to shut down a server using System Platform Management Console. However, if the server is running in High Availability, you can only shut down the currently active server. Use this procedure to shut down the High Availability system.

1. On the active server, log in to System Platform Management Console as admin.
2. Check that the system is ready to be shutdown correctly. See Checking correct system state using System Platform Management Console on page 70.
3. Shut down the active server. See Shutting down a server using System Platform Management Console on page 70.
4. Wait until the standby server takes over.

   Note:
   Ensure that the standby server has taken over successfully, by checking the availability of System Platform Management Console on the standby server. For that, use the URL of System Platform Management Console regularly.

5. On the standby server, log in to System Platform Management Console as admin.
6. Shut down the standby server. See Shutting down a server using System Platform Management Console on page 70.

User Administration

User Administration overview

You can view existing user profiles for System Platform Server, create new user profiles, edit existing user profiles, and change existing passwords by using the options displayed under User Administration.

Local management

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 Management 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 Management Console. However, a user with Administrator role has access restrictions in using System Platform Management 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
	License Management		Granted

Menu	Option	Web page control	Access restriction
	SAL Gateway Management		Granted
	Failover		Denied for the **Configure**, **Delete**, **Start**, **Stop**, **Switchover**, **Update SyncSpeed**, **Pause/ Unpause Sync** buttons.
	Performance Statistics		Granted
	Eject CD / DVD		Granted
	File Manager		Granted
	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 Management Console is stored in the local LDAP server and will not appear in the `/etc/shadow` file.

Creating users

1. Click **User Administration** > **Local Management**. The Local Management page appears:

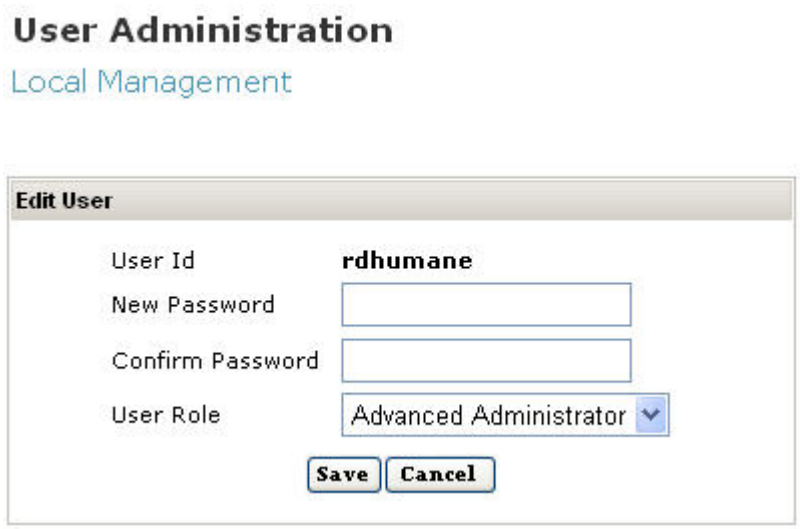
2. On the Local Management page, click **Create User**. The Local Management page changes to accept the details of new user:

3. In the **User Id** field, enter a unique user ID.
4. In the **User Password** field, enter a password.
5. In the **Confirm Password**, enter the same password.
6. In the **User Role** field, click the user role you want to assign to the user.
7. Click **Save User** to the create the user with the details you have specified.

Editing users

1. Click **User Administration** > **Local Management**.
2. On the Local Management page, click the check box against the user whose details you want to edit.

3. Click **Edit User**. The Local Management page changes to enable editing the details of new user:



4. In the **New Password** field, enter new password.
5. In the **Confirm Password**, enter the same password.
6. In the **User Role** field, click the user role you want to assign to the user.
7. Click **Save** to save the edited user details.

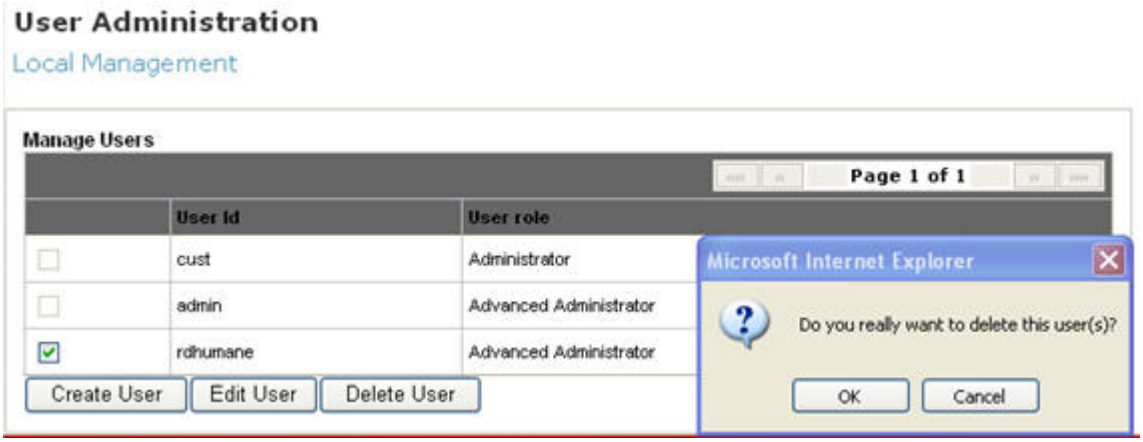
Note:

The `cust` and `admin` user IDs are non-editable.

Deleting users

1. Click **User Administration** > **Local Management**.
2. On the Local Management page, click the check box against the user whose details you want to delete:

3. Click **Delete User**.
4. In the dialog box that appears to confirm deleting the user, click **OK**.



Note:

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

Local Management field descriptions

Name	Description
User Id	User name for a user.
User Password	Password for a respective user.
User Role	Role of a user. Provides information whether a user has the rights of an administrator or advanced administrator. You can change the user roles by using the Edit User option.

Local Management button descriptions

Button	Description
Create User	Opens the Create User page and lets you create a user profile.
Save User	Saves the user profile and creates the user with these specifications.
Edit User	Opens the Edit User page and lets you edit an existing user profile.
Delete User	Active only when you select an existing user from the Local Management page. Deletes the selected user.

Enterprise LDAP

Use the Enterprise LDAP page to configure and enable enterprise LDAP authentication through the System Platform Management Console so that the system will authenticate logins with an external LDAP server.

Use this page to configure enterprise LDAP server parameters, so that the enterprise users can use the enterprise logins and passwords to log on to the System Platform Management Console.

Note:

Only a user under the Advanced Administrator role can access the **Enterprise LDAP** option.

Configuring authentication against an enterprise LDAP

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

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.

Enterprise LDAP field descriptions

Use the Enterprise LDAP page to enable and configure authentication of System Platform users against your 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 be executed. This is used for connection authentication to the LDAP server. For example, cn=admin,ou=sv,dc=avaya,dc=com. This parameter is used to login to the LDAP server.
User DN	Is the distinguished name of the LDAP user.
User Password	Is the password of the LDAPuser.

Name	Description
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))*.
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

Use the **Change LDAP Password** page for changing the System Platform LDAP password.

The LDAP password is associated with the System Platform LDAP, which provides the LDAP authentication. Thus, the LDAP password is different from the System Platform user password that lets you access the System Platform Management Console.

Note:

Passwords must be at least six characters long. Avaya recommends using only alphanumeric characters.

Changing LDAP password

You can change the LDAP password set during the System Platform installation.

1. Click **User Administration** > **Change LDAP Password**.
2. Enter the new password.
3. Confirm the new password.
4. Click **Save** to save the new password.

Change System Platform password

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

Use the Change Password page to change the user password that lets you access the System Platform Management Console.

Note:

Passwords must be at least six characters long. Avaya recommends using only alphanumeric characters.

Changing System Platform user passwords

1. Click **User Administration** > **Change Password**.
2. Fill up the following fields on the Change Password page.
   - Old Password
   - New Password
   - Confirm Password

3. Click **Change Password** to change the current password.

Chapter 2: Troubleshooting

DVD does not mount

The DVD does not mount automatically.

Troubleshooting steps

1. Log on to 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/udom
AttachCd > mount /dev/xvde /cdrom/
```

Virtual machine has no connectivity outside after assigning dedicated NIC support

Troubleshooting steps-through System Domain (Dom-0)

1. Check if the pci ID entry is in the `/etc/rc.local and /etc/modprobe.conf`.
2. Check if the pci ID is binded properly to `/sys/bus/pci/drivers/pciback/` .

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 Management Console

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 Management Console.

General issues with the system and wants to contact support

Troubleshooting steps

System Platform provides scripts that gather all the required configuration files, log files, and system status commands, and collect them into a zip file. If this script is executed from console domain SSH session, it also gathers this information from Domain-0 (if High Availability Failover is not configured) or from both Domain-0s (if High Availability Failover is configured).

1. To create such zip file execute **getlogs** command from console domain.

It will create `vsp_logs_<hostname>_<date_time>.zip` compressed file in the current directory.

2. If console domain is not accessible, execute **`getlogs`** command on Domain-0 (if High Availability Failover is not configured) or on both Domain-0s (if High Availability Failover is configured).

Result

This file can be then used to your support technician.

Issues when configuring System Platform High Availability Failover

Cannot establish communication through crossover network interface

Troubleshooting steps

Ensure that the crossover cable is properly connected to eth2 interface on both machines.

Local IP address provided

Troubleshooting steps

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

Cannot establish SSL communication

Troubleshooting steps

You have provided IP address remote console domain IP address that was already part of System Platform High Availability Failover but was later removed as a standby node.

Note:
Such console domain cannot become a member of System Platform High Availability Failover.

Reinstall the standby machine with the System Platform and retry the Configure Failover method.

Standby first-boot sequence is not yet finished

Troubleshooting steps

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

Provide enough time to complete this start-up process and try configuring the System Platform 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

You attempted to set up System Platform High Availability Failover adding the weaker machine then the preferred one to the system.

Either use another machine that has the same or better configuration parameters or swap the machines so that the weaker one becomes preferred node.

Note:

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

A template is installed on remote node

Troubleshooting steps

There is a template (Solution Template) installed on the standby node.

Note:

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

Either delete Solution Template from the standby node or reinstall it with System Platform and retry configuration of the System Platform High Availability Failover.

NICs are not active on both sides

Troubleshooting steps

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.

Ensure you have enough network interfaces on the system.

Cannot establish HA network interface

Troubleshooting steps

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

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

Issues when starting System Platform High Availability Failover

Different platform versions against cluster nodes

Troubleshooting steps

Versions of System Platform are not equal on both cluster nodes. Systems checks if the System Platform versions are equal on both cluster nodes and forbids to start System Platform High Availability Failover if they are not.

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

A template is installed on remote node

Troubleshooting steps

There is a template (Solution Template) installed on the standby node. System Platform forbids to start System Platform High Availability Failover when there is a template installed on the standby node.

Delete Solution Template from the standby node.

Resources are not started on any node and cannot access System Platform Management Console

Troubleshooting steps

System Platform High Availability Failover uses default network gateway as a ping target. It is used to check machine's ability to communicate to network and compute computer's score to run resources. If the gateway is not replying to those ping requests, System Platform High Availability Failover is not able to assign any node as active node, because their score is equal and as a result no resources are activated on any node.

Check that your default network gateway is able to receive and reply to ICMP echo requests from both System Platform nodes. If there are firewall rules filtering the ICMP requests by packet size, ensure that packet sizes up to 256 bytes are allowed by these rules. See the Prerequisites section in *Installing and Configuring Avaya Aura™ System Platform* for more information.

Cannot access System Platform Management Console after Start Failover

Troubleshooting steps

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

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

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.

Heartbeat link fails

Troubleshooting steps

1. Disconnect crossover cable between the two servers.
2. Reconnect the crossover cable after few minutes.

Result

Active server remains as active. Active server will resync the data to standby server.

Note:
The crossover connection interruption should not initiate any failover action.

High Availability Failover does not work

Troubleshooting steps

1. Remove the SAMP board from the S8510 server before installing System Platform.
2. Ensure that the Dual NIC card is connected to the eth2 port.

Start LDAP service on System Domain (Dom-0)

Troubleshooting steps

If the system crashed or was reset for any other reason, 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.

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 Management Console not accessible

Troubleshooting steps

1. Check the internet connection.
2. Ensure that the Web address is correct.
3. Check proxy settings in your browser.

Re-enabling failed standby node to High Availability Failover

Troubleshooting steps

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:

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

Troubleshooting steps

In this case all the services are running on the standby node. However, the resolution could differ in the following cases:

- completely new machine is to be re-enabled into the HA system, or
- previous preferred machine with new primary network card (the card with eth0 and eth1 NICs) is to 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. Please 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 that are not available on the webconsole are required. Please contact Avaya support to assist you with resolving of this state.

Important:

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

Troubleshooting virtual machine with dedicated NIC may fail after System Platform upgrade

Troubleshooting steps

Dedicated NIC settings are lost upon the next server reboot once the `/etc/rc.local` symbolic link is changed to a file. The virtual machine using the dedicated NIC will fail to boot.

1. Log in to System Platform Management Console as admin
2. Type `su`
3. Type `ll /etc/rc.local`
   The system displays the following information:

   ```
   /etc/rc.local -> rc.d/rc.local
   ```

4. In case the symbolic link doesn't exist, perform the following steps:
   a. Move the `/etc/rc.local` file to `/etc/rc.d/rc.local` by typing the command `mv -f /etc/rc.local /etc/rc.d/rc.local`
   b. Create a symbolic link to the file `/etc/rc.d/rc.local` by typing the command `ln -s /etc/rc.d/rc.local /etc/rc.local`
   c. Reboot the server either from System Platform Management Console or the command line.

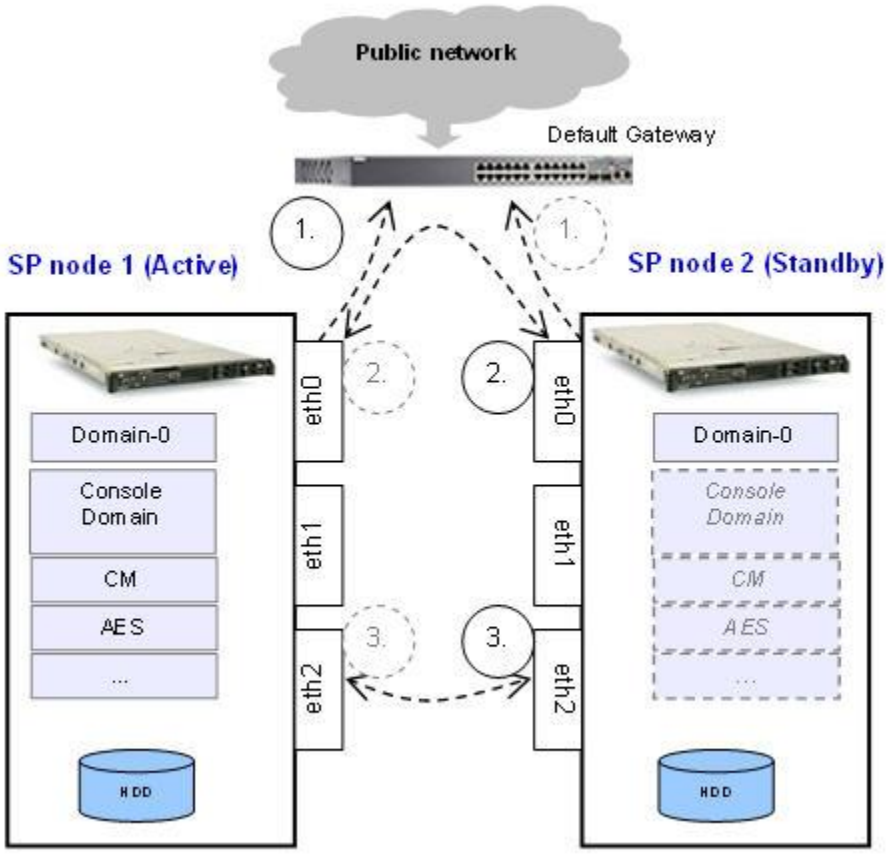
Appendix A: How System Platform High Availability Failover works

Ping targets

System Platform High Availability Failover uses a node scoring to decide which node resources should run in each particular situation. Every node uses the following 3 ping targets:

1. Default network gateway as a public ping target.
2. eth0 network interface of the peer.
3. eth2 network interface of the peer.

Every successful ping result gives a machine the same score amount for every ping target. Therefore, if both machines can reach all the 3 ping targets, they both have the same score and resources run on the preferred node. The following image depicts the overview of the machines with their 3 ping targets:



As a consequence of ping targets, one of the following things may happen:

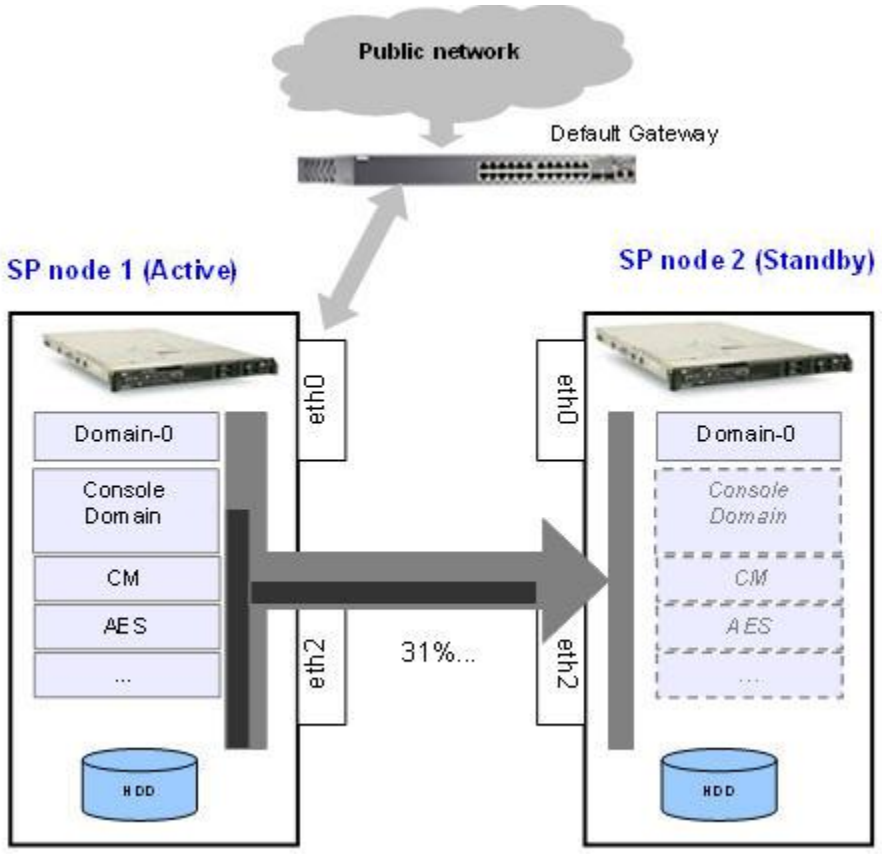
1. If the crossover link is interrupted on any node, no action will result because both machines have the same score.
2. If the public link is interrupted on the standby node, no action will result because the active node still has the full score while the standby node has lost 2 ping sources.
3. If the public link is interrupted on the active node, heartbeat will initiate failover because active node has lost 2 ping sources while the standby has the full score.

Note:

The default gateway is the ping target and it is not a configurable parameter. Ensure that your gateway replies to ICMP pings which have payloads larger that the defaults and come from the System Platform nodes.

DRBD initial data synchronization

System Platform High Availability Failover uses the Distributed Replicated Block Device (DRBD) component to propagate online changes that are made on the active node. Each Logical Volume that is propagated by DRBD uses separate DRBD resource. List of these DRBD resources and their states can be checked on the System Platform Failover page. However, before the initial synchronization of the DRBD resources is completed, the standby node does not have the reliable data that could be used to start the virtual machines. The time interval during initial data block synchronization is called initial data synchronization. The following image depicts the initial data synchronization from the active node to the standby node:

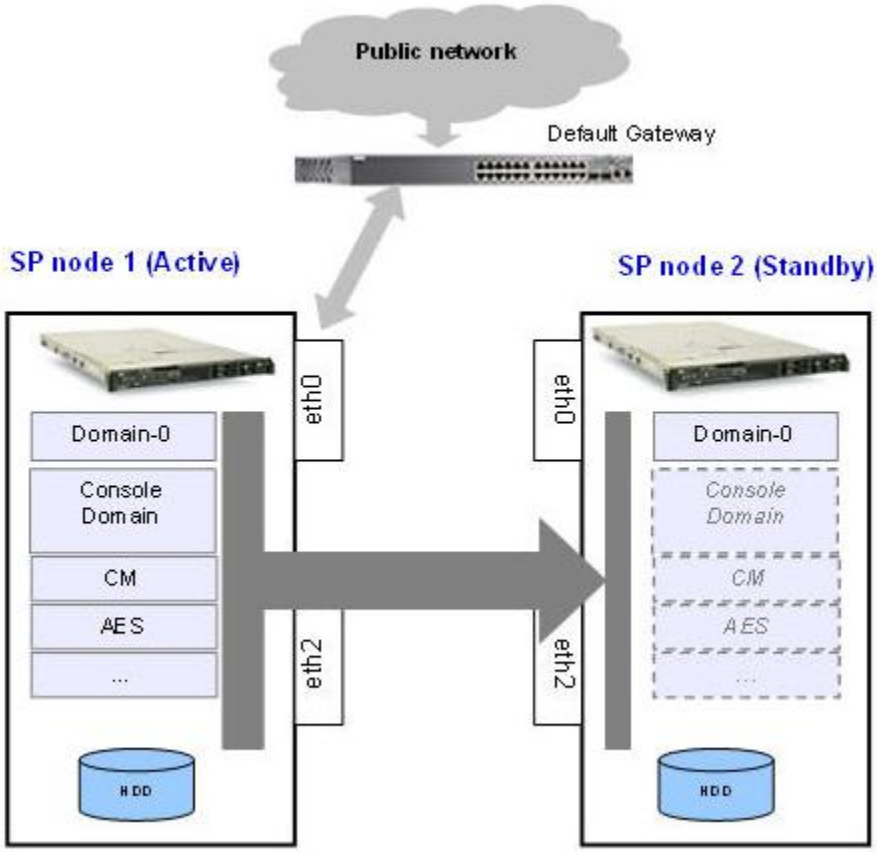


Note:

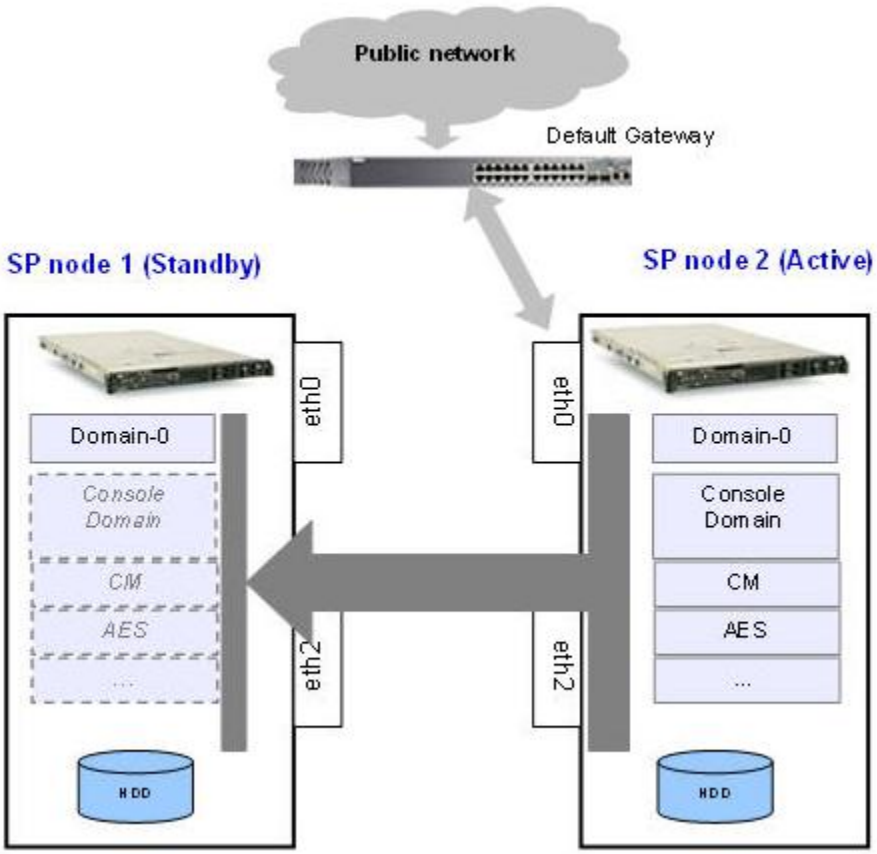
During the initial synchronization, the online changes are also propagated. It is essential to provide enough network throughput for the successful completion of the online changes. Thus the System Platform sets the DRBD initial synchronization rate to 30MB/s. You can modify this value from the Failover page in case system is not overloaded.

DRBD online propagation of data changes

System Platform High Availability Failover uses the Distributed Replicated Block Device component to propagate online changes that are made on the active node. It uses its protocol “C” which ensures that writing to the local hard disk is only confirmed when the same write is acknowledged on the remote node. This ensures that the machines are kept in consistent state to enable the standby node to takeover when required. The following image depicts the data propagation from active node to the standby node:

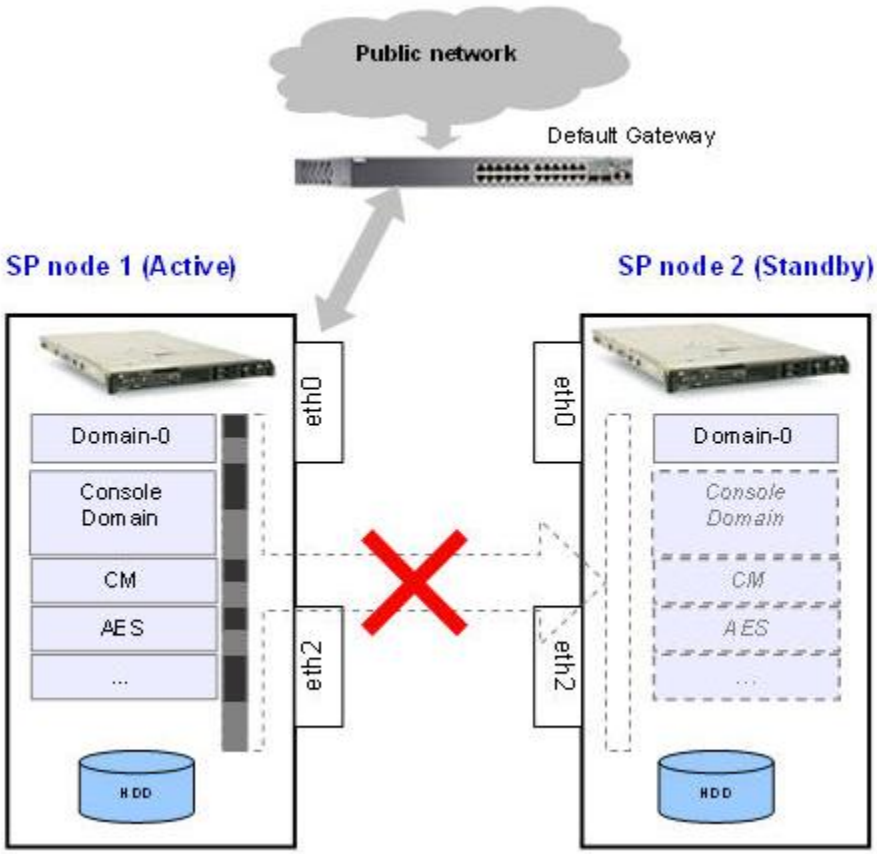


In the event of failover or switchover when the node roles are changed (that is, the active node becomes the standby node and vice versa), the propagation direction swaps to ensure that the changes on the active node are propagated to the current standby node. The following image depicts data propagation after a failover/switchover:



Data changes during disconnection

In case of the replication link interruption, DRBD uses its own metadata to keep the history of modified data blocks since the connection break up. Later when the connection is reestablished, the missing data blocks are synchronized on the standby node in parallel with the online changes propagation. The following image depicts the data changes history marked in the DRBD metadata during the propagation link disconnection:



Automatic Split-Brain resolution

In case there is no communication path between the nodes, Cluster Resource Manager can activate resources on both nodes at the same time. This situation is called Split-Brain. After both nodes appear on the network again, the data changes that occurred on the nodes must be discarded on one of them. System Platform High Availability Failover uses a DRBD feature to recognize which node became active as the last one. This node is rebooted immediately and its data changes are discarded. After successful reboot, it will synchronize the changes that occurred on the survival node since the disconnection before split-brain.

Appendix B: Administering SAL on System Platform

SAL Gateway configuration

The SAL (Secure Access Link) Gateway includes a Web-based Gateway user interface that provides status information, logging information, and configuration interfaces. Use the procedures in this section to configure the gateway and other devices for alarming and remote access. The devices include System Platform's System Domain (dom 0), Console Domain (cdom), and other product virtual machines (Communication Manager, Communication Manager Messaging, SIP Enablement Services, Application Enablement Services, Utility Server and Media Services) in System Platform.

Related topics:

Launching SAL Gateway UI on page 101
Configuring SAL Gateway on page 102
Configuring SAL Enterprise on page 103
Configuring Remote Access Server on page 104
Configuring NMS on page 105
Managing service control on page 105
Applying configuration changes on page 106
Configuring a managed element on page 106
Products and models on page 107

Launching SAL Gateway UI

The SAL (Secure Access Link) Gateway includes a Web-based Gateway user interface that provides status information, logging information, and configuration interfaces. Use the procedures in this section to configure the gateway and other devices for alarming and remote access. The devices include System Platform's System Domain (dom 0), Console Domain (cdom), and other product virtual machines (Communication Manager, Communication Manager Messaging, SIP Enablement Services, Application Enablement Services, Utility Server and Media Services) in System Platform.

1. Go to Avaya Aura System Platform's Web console and log on.
2. Go to **Server Management**> **SAL Gateway Management**.
3. On the SAL Gateway Management page, click **Launch SAL Gateway Management Portal** to launch the SAL Gateway UI (user interface) .
4. On the SAL Gateway page, log on to the SAL Gateway using the same login credentials that you used for the System Platform Web console.
5. On the Gateway home page navigation pane, click **Administration**.
   The system displays the following options under **Administration**:
   - **Gateway Configuration**
   - **LDAP**
   - **Proxy**
   - **SAL Enterprise**
   - **Remote Access**
   - **Policy Server**
   - **NMS**
   - **Service Control**
   - **Apply Configuration Changes**

Configuring SAL Gateway

1. On the Gateway home page, click **Administration** > **Gateway Configuration**.
2. On the Gateway Configuration page, click **Edit**.
   The system displays the **Gateway Configuration** (edit) panel.
3. In the **Gateway Hostname** field, enter a distinguishing host name for the SAL Gateway.
4. In the **Gateway IP Address** field, enter the IP address of the SAL Gateway.
5. In the **Solution Element ID** field, enter the Solution Element ID that uniquely identifies the SAL Gateway.
   The system uses the SAL Gateway Solution Element ID to register the SAL Gateway with the Secure Access Concentrator Remote Server.
6. In the **Gateway Alarm ID** field, enter the Alarm ID of the SAL Gateway.

The system uses the value in the **Gateway Alarm ID** field to uniquely identify the source of Gateway alarms in the Secure Access Concentrator Core Server.

7. Click **Apply**.
   The system changes the configuration and the configuration changes take effect immediately.
8. Click **Undo Edit** to undo the changes.
   The system returns to the configuration before you clicked the **Edit** button.

   See the *Secure Access Link 1.5 Gateway Implementation Guide* for more information.

Configuring SAL Enterprise

1. On the Gateway home page, click **Administration** > **SAL Enterprise**.
   The system displays the SAL Enterprise page.
2. In the **Primary Enterprise** field, enter the IP Address or host name of the primary SAL Enterprise.
3. In the **Port** field, enter the Port number of the primary SAL Enterprise.
4. In the **Secondary Enterprise** field, enter the IP Address or the host name of the secondary SAL Enterprise.
5. In the **Port** field, enter the Port number of the secondary SAL enterprise.
6. Click **Apply**.
   The system displays the following buttons in the page:
   - **Edit**: to change the configuration.
   - **Apply**: to apply the changes made to the configuration.
   - **Test**: to run the diagnostic tests for connectivity.

   Important:
   You must restart the SAL Gateway for the configuration to take effect. Till you restart the SAL Gateway, the system does not connect to the new SAL Enterprise.

   When you restart the SAL Gateway, the system might miss some SNMP traps.
7. (Optional) If you want to use the Avaya production enterprise server, perform the following tasks:
   a. In the **Primary Enterprise** field, enter `alarming.esp.avaya.com`.

b. In the **Port** field, enter `8002`.

c. Use the Avaya proxy when connecting from Avaya internal network.

See the *Secure Access Link 1.5 Gateway Implementation Guide* for more information.

Configuring Remote Access Server

1. On the Gateway home page, click **Administration** > **Remote Access**.
   The system displays the Remote Access page
2. In the **Primary Enterprise** field, enter the IP Address or host name of the primary Remote Access Server.
3. In the **Port** field, enter the port number of the primary Remote Access Server.
4. (Optional) In the **Secondary Enterprise** field, enter the IP Address or Host name of the secondary Remote Access Server.
5. (Optional) In the **Port** field, enter the port number of the secondary Remote Access Server
6. Click **Apply**.
   The system displays the following buttons in the page:
   - **Edit**: to change the configuration.
   - **Apply**: to apply the changes made to the configuration.
   - **Test**: to run the diagnostic tests for connectivity.

   Important:
   You must restart the SAL Gateway for the configuration to take effect. Until you restart the SAL Gateway, the system does not connect to the new Secure Access Concentrator Remote Servers.

   When you restart the SAL Gateway, the system terminates all active connections.

   See the *Secure Access Link 1.5 Gateway Implementation Guide* for more information.

Configuring NMS

1. On the Gateway home page, click **Administration** > **NMS**.
   The system displays the Network Management Systems page.
2. In the **NMS Host Name/ IP Address** field, enter the IP Address or host name of the NMS server.
3. In the **Trap port** field, enter the port of the NMS server.
4. In the **Community** field, enter the community string of the NMS server.
   Enter `public` as the **Community**, as SAL agents support only public as community at present.
5. Click **Apply**.
6. (Optional) Use the **Add** button to add multiple NMS(s).
   See the *Secure Access Link 1.5 Gateway Implementation Guide* for more information.

Managing service control

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

1. On the Gateway home page, click **Administration** > **Service Control**.
   The system displays the Gateway Service Control page. The page lists the following services:
   - **Inventory** (disabled in the current release)
   - **Alarming**
   - **Remote Access**

   The Gateway Service Control page also displays the status of each service as:
   - **Stopped**
   - **Running**

See the *Secure Access Link 1.5 Gateway Implementation Guide* for more information.

2. Click **Stop** to stop a service.
3. Click **Test** to test a service.

Applying configuration changes

1. On the Gateway home page, click **Administration** > **Apply Configuration**. The system displays the Apply Configuration Changes page.
2. Click the **Apply** button next to **Configuration Changes**.

   See the *Secure Access Link 1.5 Gateway Implementation Guide* for more information.

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

Configuring a managed element

1. On the Gateway home page, click **Administration** > **Managed Element**. The system displays the Managed Element page.
2. Click **Add new**.
3. In the **Host Name** field, enter a host name for the managed device.
4. In the **IP Address** field, enter the IP address of the managed device.
5. Select the **NIU** check box if you want to use a Network Interface Unit port for remote access and select a value from the list box.

   The range of values allowed is one through nine. Some older managed devices can only be reached on a network though an NIU interface. The NIU emulates a modem to convert a managed device from modem support to network accessibility. To make a remote connection to the NIU-supported devices, you must know which NIU port number to connect to.
6. In the **Solution Element ID** field, enter the Solution Element ID of the device.

7. In the **Product ID** field, enter the Product ID or Alarm ID.
8. In the **Model** field, enter the model that is applicable for the managed device.
9. (Optional) Select the **Provide Remote Access to this device** check box, if you want to allow remote connectivity to the managed device.
10. (Optional) Select the **Transport alarms from this device** check box, if you want alarms from this device to be sent to the Secure Access Concentrator Core Server.
11. (Optional) Select the **Collect Inventory for this device** check box, if you want an inventory schedule at the managed device level.

    This selection manages Inventory Collection and sends the inventory to Avaya. The selection also decides the Inventory Collection Schedule interval. This feature is not supported yet.
12. Click **Add**.
13. Click **Apply** to apply the changes.
14. Click **Edit** to change the configuration.
15. Click **Delete** to delete the configurations.

Important:

After you select **Apply** or **Delete**, you must restart the SAL Gateway services for the configuration to take effect.

Products and models

This section presents the relationship between the product devices managed by the SAL Gateway and the models the managed devices must use.

Are we supposed to change the product names/model names from VSP to System Platform? Please verify all the product names and domain names.

Products	Models
System Platform System Domain (Dom 0)	VSP_1.0
System Platform Console Domain (cdom and udom)	VSPU_1.0
SAL Gateway	SAL_Gateway_1.0
Communication Manager	CM_Media_server_1.0
Communication Manager Messaging	CM_Media_server_1.0 (temporary solution)
Application Enablement Services	AES_1.0

Products	Models
SIP Enablement Services	SIP_Server_1.0
Utility Server	VUS_1.0
Media Services	Cobar_1.0

You can create a cheat sheet as follows:

System Platform domain	IP Address	SEID	Product ID	Models	Notes
System Domain (Dom 0)	10.0.0.66	(076)934-2000	7000135491	VSP_1.0	
Console Domain (cdom and udom)	10.0.0.67	(076)934-2001	5023427441	VSPU_1.0	
Dom1-Communication Manager	10.0.0.71	(076)934-2002	1000237197	CM_Media_server_1.0	
Dom -Communication Manager Messaging	10.0.0.72	(076)934-2003	2000041897	CM_Media_server_1.0	Use Communication Manager model as a temporary solution
Dom2-SIP Enablement Services	10.0.0.73	(076)934-2004	1000237198	SIP_Server_1.0	
Dom3-Application Enablement Services	10.0.0.74	(076)934-2005	4000006620	AES_1.0	
Dom4-Utility Server	10.0.0.75	(076)934-2006		VUS_1.0	
Dom5-Media Services	10.0.0.76	(076)934-2007		Cobar_1.0	

Note:

There is no alarm mechanism in Utility Server and Media Services. You are not required to enable alarming for the managed elements used by Utility Server and Media Services.

System Domain (Dom 0) (VSP) does not have alarming enabled, but Cdom (VSPU) has alarming enabled. System Domain (Dom 0) sends all syslog (system logs) to Cdom (Console

Domain) and Cdom triggers alarms on behalf of System Domain (Dom 0). But System Domain (Dom 0) has its own AlarmID (ProductID).

In System Platform HA (High Availability) mode, you require two different solution element IDs (SEID) for System Domain (Dom 0): one is for active System Domain (Dom 0) and the other is for standby System Domain (Dom 0). You must administer both SEIDs through the SAL Gateway UI (user interface).

Making SAL Gateway communicate with SAL Enterprise

Use this procedure to make SAL 1.5 Gateway in System Platform communicate with the SAL Enterprise in Session Manager.

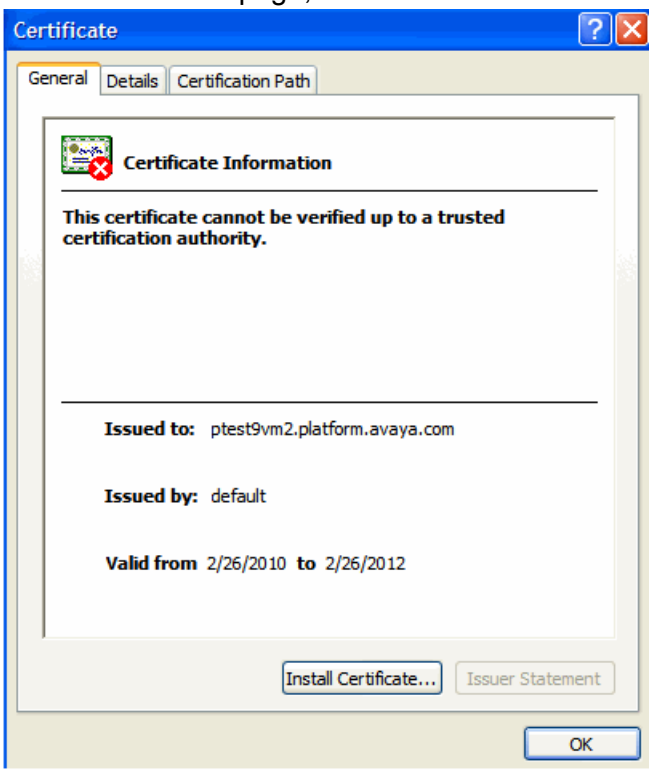
Use Step 1 through Step 8 to export the Self-Signed Certificate of Session Manager. If you already know how to export a certificate, or if Session Manager is using a certificated signed by trusted agencies, for example Verisign, go to Step 9.

Note:

This procedure uses *ptest9vm2.platform.avaya.com* for Session Manager and *ptest9vm1.platform.avaya.com* for Console Domain (cdom and udom) in System Platform, where SAL 1.5 Gateway is located.

1. On a Web browser, type the following URL: `https://ptest9vm2.platform.avaya.com/`
2. On the HTTP Status 404 page, double-click the lock icon (**SSL Secured**) located at the bottom.

3. On the Certificate page, click **Details**.



4. Click **Copy to File**.
5. On the Certificate Export Wizard page, click **Next**.
6. Check that the **DER encoded binary X.509 (.CER)** option is selected by default, then click **Next**.
7. On the Save As page, select a location to save the certificate and click **Save**.
8. On the Certificate Export Wizard page, click **Finish**.
   The system saves the Self-Signed Certificate named **ptest9vm2.platform.avaya.com.cer** in your specified location.
9. Open an SSH session to *ptest9vm2.platform.avaya.com*.
10. Type `vi /opt/Avaya/Mgmt/3.0.5/SpiritEnterprise/config/DataTransportConfig.xml`
11. Make a note of the value in bold letters to be used in later steps:

    <!— A name that uniquely identifies an Agent or Enterprise deployed within an organization. —

    <string name=”SpiritPlatformQualifier” displaykey=”SpiritPlatformQualifier”

    value=”**Enterprise-ptest9vm2.platform.avaya.com**”isadministrable=”true”/>
12. On a Web browser, type the following URL: `https://ptest9vm1.platform.avaya.com:7443/salgateway` and log on to SAL 1.5 Gateway.

13. Make a note of the gateway configuration details from the Gateway Configuration page.
14. Add SAL Gateway as a managed device using the details from the Gateway Configuration page.

    See *Configuring a managed element* topic for more information.
15. On the Managed Element Configuration page, check the Transport alarms from this device option.

    Do not restart the SAL and Axeda agents.
16. Edit the SAL Enterprise as follows:
    a. On the SAL Enterprise page, make sure that the **Primary Enterprise** and **Secondary Enterprise** fields contain `ptest9vm2.platform.avaya.com`.
    b. Click the **Test** button to check the connection.
    c. Click Apply.

       Do not restart the SAL and Axeda agents.
17. Open an SSH session to *ptest9vm1.platform.avaya.com*.
18. Locate the file `SPIRITAgent_1_0_DataTransportConfig_xxxxxxxx_xxxxxx_xxx.xml` with the most recent timestamp in the filename.
19. Change the following entry: `<entry key="Connection.AvayaBase.PlatformQualifie”>Enterprise-production</entry>` to `<entry key="Connection.AvayaBase.PlatformQualifie”>Enterprise-ptest9vm2.platform.avaya.com</entry>`
20. Locate the file `SPIRITAgent_1_0_SpiritComponentConfig _xxxxxxxx_xxxxxx_xxx.xml` with the most recent timestamp in the filename.
21. Replace all the occurrences of *Enterprise-production* to *Enterprise-ltest9vm2.platform.avaya.com*.

    If Session Manager uses a certificate that is signed by a trusted agency, then you can directly go to Step 25 (restarting Spirit and Axeda). If Session Manager uses a Self-Signed Certificate and you have followed Step 1 through Step 8 earlier, then continue with the following steps.
22. Copy the Self-Signed Certificate *ptest9vm2.platform.avaya.com.cer* you created earlier to `/opt/avaya/SAL/gateway/SpiritAgent/security`.
23. Type the following command to import the certificate to Spirit Agent’s trust store:

    `cd /opt/avaya/SAL/gateway/SSL/`

    `keytool –import –alias ptest9vm2.platform.avaya.com –keystore spirit-trust.jks –file`

/opt/avaya/SAL/gateway/SpiritAgent/security/ptest9vm2.platform.avaya.com.cer

24. Enter avaya123 when the system prompts you for password.
25. Type the following commands to restart the Spirit and Axeda Agents:
    service spiritAgent restart

    service axedaAgent restart
26. On a Web browser, type the following URL: `https://ptest9vm1.platform.avaya.com:7443/` and log on to SAL 1.5 Gateway.
27. Go to **Administration** > **Service Control**.
28. Click the **Test** button.
    The system displays the **Test alarm sent** message.
29. On a Web browser, type the following URL: `https://ptest9vm2.platform.avaya.com/SMGR` and log on to Session Manager.
30. Go to **Alarms**.
    The system displays the following:

Appendix C: Hardware 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. Please note that the information provided here should not be considered exhaustive as the server hardware and sensors may vary over time. Further, a firmware update may also change the list of monitored sensor-related faults.

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

For S8510

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

- Power Overload
- Main Power Fault
- Power Control Fault

- Drive Fault
- Cooling/Fan Fault

The RAID alarms for 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
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 needs to 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

Message	Note
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 will likely need to be replaced.
Drive Slot sensor Drive [0–9]+[^\-]*- In Critical Array Asserted	A critical failure was detected. The drive will likely need to be replaced.
Drive Slot sensor Drive [0–9]+[^\-]*- In Failed Array Asserted	The device has failed. The drive will likely need to be replaced.
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.

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.

Alarm text	Problem/Action
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.
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 may 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.
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> This may require troubleshooting within the virtual machine.
VSP High Webconsole heap usage	Check Webconsole is OK.
VSP High Network I/O (Tx) from for <vm>	Check <vm> This may require troubleshooting within the virtual machine.
VSP High Network I/O (Rx) from for <vm>	Check <vm>

Alarm text	Problem/Action
	This may require troubleshooting within the virtual machine.
VSP High Load Average <vm>	Check <vm> This may require troubleshooting within the virtual machine.
VSP Low logical volume free space <lv>	Free some space on logical volume <lv> This may require troubleshooting within the virtual machine.
VSP Low volume group free space (VolGroup00)	Free some space on volume group VolGroup00 in dom0. This may require troubleshooting within 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.
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**.

Alarm text	Problem/Action
	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 faults

Prior to SP 1.1.1.7.2

Alarm text	Problem/Action
VSP Webconsole encountered problem while changing full resync speed.	Check the details in `/var/log/vsp/vspha.log` log file.
VSP Webconsole encountered problem while pausing full resynchronisation.	Check the details in `/var/log/vsp/vspha.log` log file.
VSP Webconsole encountered problem while resuming full resynchronisation.	Check the details in `/var/log/vsp/vspha.log` log file.
VSP Webconsole encountered problem while creating failover configuration.	Check the details in `/var/log/vsp/vspha.log` log file.
VSP Webconsole encountered problem while removing failover configuration	Check the details in `/var/log/vsp/vspha.log` log file.
VSP Webconsole encountered problem while switching over the machines.	Check the details in `/var/log/vsp/vspha.log` log file.

Alarm text	Problem/Action
VSP Webconsole encountered problem while starting failover.	Check the details in `/var/log/vsp/vspha.log` log file.
VSP Webconsole encountered problem while stopping failover.	Check the details in `/var/log/vsp/vspha.log` log file.
VSP Webconsole encountered problem while saving ipmi parameters.	Check the details in `/var/log/vsp/vspha.log` log file.
VSP Webconsole encountered problem while deleting ipmi parameters.	Check the details in `/var/log/vsp/vspha.log` log file.
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>	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	Seek appropriate service for the critical condition.
Failed migrating resources to other node: <hostname>	Check `/var/log/vsp/vspha.log` and `/var/log/vsp/ha-log` for possible causes.

In the “Alarm text” column, <hostname> is the fully qualified domain name.

SP 1.1.1.7.2 and later

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
Failover occurred, activating this node (raised on <hostname>)	Check the `/var/log/vsp/ha-log` and `/var/log/messages` for the cause of failover

Alarm text	Problem/Action
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.

Index

F

G

H

I

L

M

N

P

R

S

T

U

V

W