



Administering Avaya Aura™ System Platform

Release 6.0
June 2010

Notices

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

Documentation disclaimer

Avaya shall not be 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. 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 End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on 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 to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be

accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

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

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

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

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

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

Shrinkwrap License (SR). 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, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

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

Preventing toll fraud

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

Avaya 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 Aura is a registered trademark of Avaya.

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

PuTTY is copyright 1997-2009 Simon Tatham.

Downloading documents

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

Contact Avaya Support

Avaya 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: System Platform administration overview.....	11
Administration overview.....	11
System Platform Web Console overview.....	11
Enabling IP forwarding to access System Platform through the services port.....	12
Accessing the System Platform Web Console.....	13
Chapter 2: Managing System Platform virtual machines.....	15
Virtual Machine Management.....	15
Solution template.....	15
Viewing virtual machines.....	15
Rebooting a virtual machine.....	16
Shutting down a virtual machine.....	16
Virtual Machine List field descriptions.....	17
Virtual Machine Configuration Parameters field descriptions.....	18
Deleting a solution template.....	21
Chapter 3: Server management.....	23
Server Management overview.....	23
Managing patches.....	23
Patch management.....	23
Downloading patches.....	23
Configuring a proxy.....	24
Installing patches.....	25
Removing patches.....	25
Search Local and Remote Patch field descriptions.....	26
Patch List field descriptions.....	27
Patch Detail field descriptions.....	28
Viewing System Platform logs.....	29
Log viewer.....	29
Viewing log files.....	30
Log Viewer field descriptions.....	30
Configuring date and time.....	31
Configuring System Platform to synchronize with an NTP server.....	31
Configuring date and time.....	32
NTP daemon.....	33
Removing a time server.....	34
Date Time Configuration field descriptions.....	34
Configuring Logging.....	35
Log severity levels.....	35
Log retention.....	36
Configuring log levels and retention parameters.....	36
Logging Configuration field descriptions.....	36
Configuring the system.....	37
Configuring system settings for System Platform.....	37
System configuration field descriptions.....	38
Configuring network settings.....	38
Configuring System Platform network settings.....	38
Network Configuration field descriptions.....	39

Adding a bonding interface.....	42
Deleting a bonding interface.....	42
Configuring static routes.....	42
Adding a static route.....	42
Deleting a static route.....	43
Modifying a static route.....	43
Static route configuration field descriptions.....	44
Configuring Ethernet settings.....	44
Configuring Ethernet interface settings.....	44
Ethernet configuration field descriptions.....	45
Configuring alarms.....	45
Alarm descriptions.....	45
Configuring alarm settings.....	46
Alarm configuration field descriptions.....	47
Managing Certificates.....	48
Certificate management.....	48
Selecting System Platform certificate.....	48
Selecting enterprise LDAP certificate.....	49
Certificate Management field descriptions.....	49
Managing System Platform licenses.....	50
License management.....	50
Launching WebLM.....	50
License Management field descriptions.....	50
Configuring the SAL Gateway.....	51
SAL.....	51
Launching the SAL Gateway management portal.....	52
Configuring the SAL Gateway.....	52
SAL Gateway Management field descriptions.....	53
Viewing System Platform statistics.....	53
Performance statistics.....	53
Viewing performance statistics.....	54
Exporting collected data.....	55
Performance statistics field descriptions.....	55
Ejecting the CD or DVD.....	56
Deleting old, unused files.....	56
Configuring security.....	57
Security configuration.....	57
Configuring security.....	57
Security Configuration field descriptions.....	58
Backing up System Platform.....	59
System Platform backup.....	59
Backing up the system by using the System Platform Web Console.....	60
Scheduling a backup.....	61
Transferring the Backup Archives to a remote destination.....	62
Viewing backup history.....	62
Backup field descriptions.....	62
Restoring System Platform.....	64
Restoring backed up configuration information.....	64
Restore field descriptions.....	65
Viewing restore history.....	65
Rebooting or shutting down the System Platform server.....	66

Rebooting the System Platform Server.....	66
Rebooting the whole High Availability Failover system.....	66
Shutting down the System Platform Server.....	67
Shutting down the whole High Availability Failover system.....	67
Server Reboot Shutdown field descriptions.....	68
Chapter 4: User Administration.....	71
User Administration overview.....	71
User roles.....	71
Managing System Platform users.....	72
Creating users.....	74
Modifying users.....	75
Deleting users.....	76
Local Management field descriptions.....	76
Authenticating System Platform users against an enterprise LDAP.....	77
Authentication against an enterprise LDAP.....	77
Configuring authentication against an enterprise LDAP.....	78
Enterprise LDAP field descriptions.....	78
Changing the System Platform LDAP password.....	79
Changing your System Platform password.....	80
Managing the authentication file.....	80
Authentication file for ASG.....	80
Installing an authentication file.....	81
Chapter 5: Configuring High Availability Failover.....	83
High Availability Failover overview.....	83
How High Availability Failover works.....	84
Ping targets.....	84
Initial data synchronization.....	85
Online propagation of data changes.....	86
Data changes during disconnection.....	87
Automatic split-brain resolution.....	88
Automatic failover.....	89
High Availability Failover and template configuration.....	89
Requirements for High Availability Failover.....	89
Prerequisites for configuring High Availability Failover.....	90
Configuring High Availability Failover.....	90
Configure Failover field descriptions.....	91
Start and stop of High Availability Failover.....	92
Starting High Availability Failover.....	93
Stopping High Availability Failover.....	93
Removing the High Availability Failover configuration.....	94
Switching from an active server to a standby server manually.....	94
Chapter 6: System Platform security.....	97
Command line login to System Domain and Console Domain.....	97
Firewall settings for IPv4.....	97
Stopping firewall rules.....	97
Starting firewall rules.....	98
Displaying currently set firewall rules.....	98
Logging IP packets blocked by firewall.....	98
Stopping logging of IP packets blocked by firewall.....	99

Firewall settings for IPv6.....	99
Stopping firewall rules.....	99
Starting firewall rules.....	99
Displaying currently set firewall rules.....	100
Logging IP packets blocked by firewall.....	100
Stopping logging of IP packets blocked by firewall.....	101
Linuxshield installation and configuration.....	101
LinuxShield virus scan.....	101
Installing and configuring Linuxshield on System Domain.....	102
Installing and configuring Linuxshield on Console Domain.....	102
Files requiring the SUID and SGID bits set.....	103
Files requiring SUID and SGID bits set on System Domain.....	103
Files requiring SUID and SGID bits set on Console Domain.....	104
Disabling booting from removable media.....	105
BIOS changes to disable booting from removable media.....	105
Disabling booting from removable media on S8510.....	106
Disabling booting from removable media on S8800.....	106
Disabling booting from removable media on S8300D.....	107
Avaya port matrix.....	108
Port summary.....	108
Security port matrix for Virtual Server Platform on Domain 0.....	109
Security port matrix for Virtual Server Platform on CDom.....	109
Chapter 7: Log harvest utility.....	113
Using the log harvest utility.....	114
Chapter 8: Troubleshooting.....	115
Template DVD does not mount.....	115
Troubleshooting steps.....	115
Checking RAID status.....	115
raid_status command.....	115
Virtual machine has no connectivity outside after assigning dedicated NIC support.....	116
Troubleshooting steps through System Domain (Dom-0).....	116
Troubleshooting steps through System Platform Web Console.....	117
General issues with the system and contacting support.....	117
Troubleshooting steps.....	117
Issues when configuring High Availability Failover.....	118
Cannot establish communication through crossover network interface.....	118
Local IP address provided.....	118
Standby first-boot sequence is not yet finished.....	118
Cluster nodes are not equal.....	119
A template is installed on remote node.....	119
NICs are not active on both sides.....	120
Cannot establish High Availability network interface.....	120
Issues when starting High Availability Failover.....	120
Different platform versions on cluster nodes.....	120
A template is installed on remote node.....	121
Resources are not started on any node and cannot access the Web Console.....	121
Cannot access the Web Console after starting High Availability Failover.....	122
Active server fails.....	122
Data switch fails.....	122
Heartbeat link fails.....	123

High Availability Failover does not work.....	123
Start LDAP service on System Domain (Dom-0).....	124
Troubleshooting steps.....	124
System Platform Web Console not accessible.....	124
Troubleshooting steps.....	124
Restarting High Availability Failover after one node has failed.....	125
Troubleshooting steps.....	125
Re-enabling failed standby node to High Availability Failover.....	126
Troubleshooting steps.....	126
Re-enabling failed preferred node to High Availability Failover.....	127
Troubleshooting steps.....	127
Multiple reinstallations can result in an out of memory error.....	127
Troubleshooting steps.....	128
Chapter 9: Fault detection and alarming.....	129
Hardware fault detection and alarming.....	129
Fault types.....	130
For S8510.....	130
For HP DL360 G6.....	132
For S8800.....	136
For S8300D.....	137
General software faults.....	137
Lifecycle manager faults.....	138
Performance faults.....	139
High Availability Failover faults.....	141
Appendix A: Changing VLAN ID.....	143
Appendix B: Errors encountered while downloading files from PLDS.....	145
Index.....	147

Chapter 1: System Platform administration overview

Administration overview

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

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

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

 **Important:**

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

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

System Platform Web Console overview

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

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

In the navigation pane, the system lists the administrative options under three categories: Virtual Machine Management, Server Management, and User Administration.

Virtual Machine Management

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

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

Server Management

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

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

User Administration

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

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

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Dom-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. If you disable IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

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

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding.

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

-
1. Open a compatible Internet browser on your computer.
Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
 2. Type the URL: `https://ipaddress`, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

 **Note:**

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

3. Enter a valid User ID.

 **Note:**

If you use an Avaya services login that is Access Security Gateway (ASG)-protected, you must have an ASG tool to generate a response for the challenge that is generated by the login page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools

must be able to reach the ASG manager servers behind the Avaya firewall. An Avaya Services representative will use Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative will use those keys to generate the response for the challenge generated by the login page.

4. Click **Continue**.
5. Enter a valid Password.
6. Click **Log On**.
The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end user license agreement.
The system displays the Virtual Machine List page in the System Platform Web Console.

AVAYA Avaya Aura™ System Platform
 admin
 Previous successful login: Fri Jun 04 18:31:56 MDT 2010
 Failed login attempts since: 0
 Failover status: **Not configured**

Home About Help | Log Out

Virtual Machine Management
 Virtual Machine List

System Domain Uptime: 27 days, 22 hours, 8 minutes, 44 seconds

Current template installed: CM_Simplex 6.0.0.0.1800 (cm 00.0.345.0, utility_server 6.0.0.0.9)

Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
Domain-0	6.0.0.0.11	172.21.20.130	512.0 MB	8	1d 20h 1m 5s	Running	N/A
sm	00.0.345.0	172.21.20.138	5.0 GB	1	1d 2h 55m 20s	Running	Running
cdom	6.0.0.0.11	172.21.20.131	1024.0 MB	1	13h 56m 1s	Running	N/A
utility_server	6.0.0.0.9	172.21.20.132	500.0 MB	1	1h 26m 7s	Running	Running

Chapter 2: Managing System Platform virtual machines

Virtual Machine Management

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

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

Solution template

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

Viewing virtual machines

-
1. Click **Home** or click **Virtual Machine Management > Manage**.
The Virtual Machine List page displays a list of all the virtual machines that are currently running on the system.
 2. To view details of a specific virtual machine, click the virtual machine name.

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

Related topics:

[Virtual Machine List field descriptions](#) on page 17

[Virtual Machine Configuration Parameters field descriptions](#) on page 18

Rebooting a virtual machine

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

Related topics:

[Virtual Machine List field descriptions](#) on page 17

[Virtual Machine Configuration Parameters field descriptions](#) on page 18

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 name 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 entire server including all of the virtual machines, perform one of the following steps:

- On the Virtual Machine List page, click **Domain-0** in the **Name** column.
On the Virtual Machine Configuration Parameters page, click **Shutdown Server**.
- Click **Server Management > Server Reboot / Shutdown**.
On the Server Reboot/Shutdown page, click **Shutdown Server**.

Related topics:

[Virtual Machine List field descriptions](#) on page 17

[Virtual Machine Configuration Parameters field descriptions](#) on page 18

Virtual Machine List field descriptions

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

Name	Description
Name	Name of the virtual machines running on System Platform.
Version	Version number of the respective virtual machine.
IP Address	IP address of the virtual machine.
Maximum Memory	This is a display only field. The value is set by Avaya, and cannot be configured by the users. The amount of physical memory from the total server memory the virtual machine has allocated in the template file.
Maximum Virtual CPUs	This is a display only field. CPU allocation for the virtual machine from the template file.
CPU Time	The amount of CPU time the virtual machine has had since boot. This is not the same as uptime.
State	Current status of the virtual machine. Possible values are as follows: <ul style="list-style-type: none"> • 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.

Name	Description
	<ul style="list-style-type: none"> • No State: The virtual machine is not running or the application watchdog is not being used. • N/A: The normal state applicable for System Domain and Console Domain virtual machines.
Application State	<p>Current status of the application (respective virtual machine). Possible values are as follows:</p> <ul style="list-style-type: none"> • 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.

Button descriptions

Name	Description
Refresh	Refreshes the list of virtual machines.


Related topics:

- [Viewing virtual machines](#) on page 15
- [Rebooting a virtual machine](#) on page 16
- [Shutting down a virtual machine](#) on page 16


Virtual Machine Configuration Parameters field descriptions

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

Name	Description
Name	Name of the virtual machines running on System Platform.
MAC Address	Machine address of the virtual machine.
IP Address	IP address of the virtual machine.
OS Type	Operating system of the virtual machine, for example, Linux or Windows.
State	<p>Current status of the virtual machine. Possible values are as follows:</p> <ul style="list-style-type: none"> • 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.
Application State	<p>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:</p> <ul style="list-style-type: none"> • Starting: Virtual machine is currently booting and should enter a running state when complete. • Running: Virtual machine is running normally. • Stopped: Virtual machine has been shutdown. • Stopping: Virtual machine is in the process of shutting down and should enter stopped state when complete. • Partial : Some elements of the virtual machine are running, but not all elements. • Timeout: Virtual machine has missed a heartbeat, 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	The amount of physical memory from the total server memory the virtual machine has allocated in the template file.

Name	Description
	This is a display only field.
CPU Time	The amount of CPU time the virtual machine has had since boot. This is not the same as uptime.
Virtual CPUs	The maximum number of virtual CPUs used by the respective virtual machine.
Domain UUID	Unique ID of the virtual machine.
Auto Start	<p>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).</p> <p> Note: This value should be changed only for troubleshooting purposes.</p>

Button descriptions

Button	Description
Reboot	<p>Reboots the respective virtual machine. In the case of System Domain (Domain-0), this reboot operation is the same as the reboot operation available in the left navigation pane. When you reboot the System Platform server using the reboot option in the left navigation pane, the system shuts down the System Platform server and all the virtual machines running on it.</p> <p> Important: When you reboot System Domain (Domain-0), the system reboots the System Platform server and all the virtual machines running on it, causing potential service disruption. When you reboot Console Domain, the system loses connection with the System Platform Web Console. You can log in again after Console Domain finishes the reboot operation.</p>
Shutdown Server	Appears only if Domain-0 is selected and shuts down the server and all virtual machines running on it.
Stop	Appears if a virtual machine other than System Domain (Domain-0) or Console Domain is selected and stops the selected virtual machine.
Start	Appears if a virtual machine other than System Domain (Domain-0) or Console Domain is selected and starts the selected virtual machine.

Related topics:

[Viewing virtual machines](#) on page 15

[Rebooting a virtual machine](#) on page 16

[Shutting down a virtual machine](#) on page 16

Deleting a solution template

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

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

Chapter 3: Server management

Server Management overview

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

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

Managing patches

Patch management

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

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

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. Options are:
 - **Avaya Downloads (PLDS)**
 - **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 specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Related topics:

[Configuring a proxy](#) on page 24

[Search Local and Remote Patch field descriptions](#) on page 26

[Errors encountered while downloading files from PLDS](#) on page 145

Configuring a proxy

If the patches are located in a different server (for example, Avaya PLDS or HTTP), you may be required to configure a proxy depending on your network.

-
1. Click **Server Management > Patch Management** .
 2. Click **Upload/Download**.
 3. On the Search Local and Remote Patch page, click **Configure Proxy**.
 4. On the System Configuration page, click **Enabled** for the **Proxy Status** field.
 5. Specify the proxy address.
 6. Specify the proxy port.
 7. Select the keyboard layout as required.

8. Select the required option for statistics collection.
9. Click **Save** to save the settings and configure proxy.

Related topics:

[Search Local and Remote Patch field descriptions](#) on page 26

[System configuration field descriptions](#) on page 38

Installing patches

Use this task to install all patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

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

Related topics:

[Patch List field descriptions](#) on page 27

[Patch Detail field descriptions](#) on page 28

Removing patches

-
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**, if you are removing a template patch.
 5. Click **Remove**.



Tip:

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**.


Related topics:

[Patch List field descriptions](#) on page 27

[Patch Detail field descriptions](#) on page 28

Search Local and Remote Patch field descriptions

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

Name	Description
Supported Patch File Extensions	The patch that you are installing should match the extensions in this list. For example, *.tar.gz, *.tar.bz, *.gz, *.bz, *.zip, *.tar, *.jar, *.rpm, *.patch.
Choose Media	<p>Displays the available location options for searching a patch. Options are:</p> <ul style="list-style-type: none"> • Avaya Downloads (PLDS): The template files are located in the Avaya Product Licensing and Delivery System (PLDS) Web site. You must enter an Avaya SSO login and password. The list will contain all the templates to which your company is entitled. Each line in the list begins with the “sold-to” number to allow you to select the appropriate template for the site where you are installing. You may hold the mouse pointer over the selection to view more information about the “sold-to” number. • HTTP: Files are located in a different server. You must specify the Patch URL for the server. • SP Server: Files are located in the vsp-template file system in the System Platform server. You must specify the Patch URL for the server. <p> Tip:</p> <p>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 for detailed procedures to download them):</p> <ul style="list-style-type: none"> - Pscp.exe - WinSCP <ul style="list-style-type: none"> • SP CD/DVD: Files are located in a System Platform CD or DVD.

Name	Description
	<ul style="list-style-type: none"> • 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.

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, you may be required to configure a proxy depending on your network.
Add	Appears when Local File System is selected and adds a patch file to the local file system.
Upload	Appears when Local File System is selected and uploads a patch file from the local file system.
Download	Downloads a patch file.

Related topics:

[Downloading patches](#) on page 23

[Configuring a proxy](#) on page 24

[Errors encountered while downloading files from PLDS](#) on page 145

Patch List field descriptions

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

Name	Description
System Platform	Lists the patches available for System Platform under this heading.
Solution Template	Lists the patches available for the respective solution templates under respective solution template headings.
Patch ID	File name of a patch.
Description	Information of a patch, for example, if the patch is available for System Platform the description is shown as SP patch.
Status	Shows the status of a patch.

Name	Description
	Possible values of Status are Installed , Not Installed , Active , and Not Activated .
Service Effecting	Shows if installing the patch causes the respective virtual machine to reboot.

Button descriptions

Button	Description
Refresh	Refreshes the patch list.

Related topics:

[Installing patches](#) on page 25

[Removing patches](#) on page 25

Patch Detail field descriptions

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

Name	Description
ID	File name of the patch file.
Version	Version of the patch file.
Product ID	Name of the virtual machine.
Description	Virtual machine name for which the patch is applicable.
Detail	Virtual machine name for which the patch is applicable. For example, Console Domain (cdom patch).
Dependency	Shows if the patch file has any dependency on any other file.
Applicable for	Shows the software load for which the patch is applicable.
Service effecting when	Shows the action (if any) that causes the selected patch to restart the System Platform Web Console.
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.

Button descriptions

Button	Description
Refresh	Refreshes the Patch Details page.
Patch List	Opens the Patch List page, that displays the list of patches.
Install	Installs the respective patch.
Activate	Activates the installed patch of a solution template.
Deactivate	Deactivates the installed patch of a solution template.
Remove	Removes the respective patch.
Remove Patch File	Removes the respective patch file. The button appears only if the patch file is still present in the system. On removing the patch file, the button does not appear.

Related topics:

[Installing patches](#) on page 25

[Removing patches](#) on page 25

Viewing System Platform logs

Log viewer

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

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

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

- Select one of the following logs to view:
 - System logs
 - Event logs

- Audit logs

- Select one of the log levels relevant to the selected logs. The log level denotes the type of incident that might have occurred such as an alert, an error condition, a warning, or a notice.
- Specify a time duration within which an incident of the selected log level might have occurred.
- Enter some text that you want to search in the selected logs. This is optional.

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**.

Related topics:

[Log Viewer field descriptions](#) on page 30

Log Viewer field descriptions

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

Name	Description
Messages	Select the type of log messages that you want to view. Options are: <ul style="list-style-type: none">• System Logs are log messages generated by the System Platform operating system (syslog).• Event Logs are log messages generated by the System Platform software. These logs are related to processes and commands that have run on System Platform.• Audit Logs are a history of commands that users have run on the platform.

Name	Description
Log Levels	Select the severity of log messages that you want to view: Options are: <ul style="list-style-type: none"> • Alert • Critical/Fatal • Error • Warning • Notice • Informational • Debug/Fine If you select Audit Logs for Messages , you have only Informational as an option.
Timestamp From	The timestamp of the last message in the type of log messages selected. This timestamp is greater than or equal to the value entered for Timestamp From .
To	The timestamp of the first message in the type of log messages selected. This timestamp is less than or equal to the value entered for To .
Find	Lets you search for particular log messages or log levels.

Button descriptions

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

Related topics:

[Viewing log files](#) on page 30

[Log severity levels](#) on page 35

Configuring date and time

Configuring System Platform to synchronize with an NTP server

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 Network Time Protocol (NTP) 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 the System Platform.

Related topics:

[NTP daemon](#) on page 33

[Date Time Configuration field descriptions](#) on page 34

Configuring date and time

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

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 **Save Date and Time** button.
The system displays the Set Date and Time page.

**Note:**

If the **Save Date and Time** button is not enabled, you must stop the NTP server that is currently being used.

3. Select a date in the calendar to change the default date and set the required date.
4. Do the following to set the time:
 - a. Click the time field at the bottom of the calendar.
The system displays a box showing time information.
 - b. Use the up and down arrow keys beside the hour to change the hour, and up and down arrows beside the minutes field to set the minutes.
 - c. Click **OK** to accept your time changes.
5. Click **Apply** to save your changes.
6. Click **Save Date and Time**.
The system displays a warning message stating that this action will cause a full system reboot.
7. Click **OK** to accept the message and set the updated date and time in the system.

Related topics:

[Date Time Configuration field descriptions](#) on page 34

NTP daemon

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

Reference time sources are specified using IP addresses, or host names which can be resolved by a name server. NTP uses the pseudo IP address `127.127.1.0` to access its own system clock, also known as the local clock. You must not mix this IP address with `127.0.0.1`, which is the IP address of the local host, that is the computer's loopback interface. The local clock will be used as a fallback resource if no other time source is available. That is why the system does not allow you to remove the local clock.

Related topics:

[Configuring System Platform to synchronize with an NTP server](#) on page 31

[Date Time Configuration field descriptions](#) on page 34

Removing a time server

1. Click **Server Management > Date/Time Configuration**.
The system displays the Date/Time Configuration page.
2. Select a time server from the list of added servers and click **Remove Time Server** to remove the selected time server.

**Note:**

The changes will be effective after you restart NTP.

Related topics:

[Date Time Configuration field descriptions](#) on page 34

Date Time Configuration field descriptions

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

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

Button descriptions

Button	Description
Start ntpd	Starts the Network Time Protocol (NTP) daemon on System Platform to synchronize the server time with an NTP server. If the NTP daemon (ntpd) is started, this button changes to Stop ntpd . Click this button to stop the NTP daemon.
Set Date and Time	Edits the date and time that are configured for System Platform. The button is disabled if ntpd is running.

Button	Description
Set Time Zone	Edits the time zone that is configured for System Platform . System Platform updates the time zone on System Domain (Domain-0), Console Domain, and the virtual machines running on System Platform.
Ping	Checks whether the specified time server, that is, the specified host, is reachable across the network.
Add	Adds the time server that you specify to the list of time servers with which System Platform can synchronize.
Remove Time Server	Removes the selected time server.
Query State	Checks the status of the NTP daemon on System Platform.

Related topics:

[Configuring System Platform to synchronize with an NTP server](#) on page 31

[Configuring date and time](#) on page 32

[NTP daemon](#) on page 33

[Removing a time server](#) on page 34

Configuring Logging

Log severity levels

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

- Fine
- Informational
- Warning
- Error
- Fatal

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

Log retention

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

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

Configuring log levels and retention parameters

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

Related topics:

[Log severity levels](#) on page 35

[Log retention](#) on page 36

[Logging Configuration field descriptions](#) on page 36

Logging Configuration field descriptions

Use the Logging Configuration page to configure the severity of log messages that you want logged, a maximum size for log files, and the number of backup files that you want retained.

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.

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

Related topics:

[Log severity levels](#) on page 35

[Log retention](#) on page 36

[Configuring log levels and retention parameters](#) on page 36

Configuring the system

Configuring system settings for System Platform


-
1. Click **Server Management > System Configuration**.
 2. Fill in all the fields on the System Configuration page to configure the System Platform settings.
 3. Click **Save**.
-

Related topics:

[System configuration field descriptions](#) on page 38

System configuration field descriptions

Use the System Configuration page to configure proxy settings, change the current keyboard layout, or enable or disable statistics collection.

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.
Statistics Collection	<p>If you disable this option, the system stops collecting the statistics data.</p> <p> Note: If you stop collecting statistics, the system-generated alarms will be disabled automatically.</p>

Related topics:

[Configuring system settings for System Platform](#) on page 37

Configuring network settings

Configuring System Platform network settings

Important:

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

Make sure that the IP address for the *avprivate* bridge do not conflict with any other IP addresses in your network.

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

The avprivate bridge is an internal, private bridge that allows virtual machines to communicate with each other. This private bridge 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 page. 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.

 **Important:**

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

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

Related topics:

[Network Configuration field descriptions](#) on page 39

Network Configuration field descriptions

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

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

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

Enable IPv6 field description



Name	Description
Turn On IPv6	Enables IPv6.

General Network Settings field descriptions

Name	Description
Default Gateway	The default gateway.

Name	Description
Primary DNS	The primary DNS server address.
Secondary DNS	(Optional) The secondary DNS server address.
Domain Search List	The search list, which is normally determined from the local domain name. By default, it contains only the local domain name. This may be changed by listing the desired domain search path following the <i>search</i> keyword with spaces or tabs separating the names.
Udom hostname	The host name for the Console Domain. This must be a fully qualified domain name (FQDN), for example, SPCdom.mydomainname.com.
Dom0 hostname	The host name for System Domain (Dom-0). This must be a fully qualified domain name (FQDN), for example, SPDom0.mydomainname.com.
Physical Network Interface	The physical network interface details for eth0 and eth1 (and eth2 in case of High Availability Failover is enabled).
Domain Dedicated NIC	Applications with high network traffic 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: <ul style="list-style-type: none"> • avprivate: This is called a private bridge because it does not use any Ethernet interface, so it is strictly internal to the server. The System Platform installer attempts to assign IP addresses that are not in use. • avpublic: This bridge uses the Ethernet interface associated with the default route, which is usually eth0, but can vary based on the type of the server. This bridge generally provides access to the LAN for System Platform elements (System Domain (Dom-0) and Console Domain) and for any guest domains that are created when installing a template. The IP addresses specified during System Platform installation are assigned to the interfaces that System Domain (Dom-0) and Console Domain have on this bridge. • template bridge: These bridges are created during the template installation and are specific to the virtual machines installed.
Domain Network Interface	The domain network interface details for System Domain (Dom-0) or Console Domain that are grouped by domain based on your selection.
Global Template Network Configuration	The set of IP addresses and host names of the applications hosted on System Platform. Also includes the gateway address and network mask.

Bonding Interface field descriptions

Name	Description
Name	Is a valid bond name. It should match regular expression in the form of "bond[0-9]+".
Mode	<p>Is a list of available bonding modes that are supported by Linux. The available modes are:</p> <ul style="list-style-type: none"> • Round Robin • Active/Backup • XOR Policy • Broadcast • IEEE 802.3ad • Adaptive Transmit Load Balancing • Adaptive Load Balance <p>For more information about bonding modes, refer to http://www.linuxhorizon.ro/bonding.html.</p> <p> Note: The default mode of new bonding interface is Active/Backup.</p> <p> Important: System Platform doesn't allow to configure any advance parameters not listed in this page. If you want to configure an advanced feature, log in to System Platform Web Console and make the required changes.</p>
Slave 1/ Primary	Is the first NIC to be enslaved by the bonding interface. If the mode is Active/Backup, this will be the primary NIC.
Slave 2/ Secondary	Is the second NIC to be enslaved by the bonding interface. If the mode is Active/Backup, this will be the secondary NIC.

Bonding Interface link descriptions

Name	Description
Add Bond	Adds new bonding interface.
Delete	Deletes a bonding interface.

Related topics:

[Configuring System Platform network settings](#) on page 38

Adding a bonding interface

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

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

Deleting a bonding interface

It is assumed here that all the bonding interface entries will show at once. The user will click the **Delete** link against the bonding interface the user wants to delete.

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

-
1. Scroll down to make the Bonding Interface frame visible.
 2. Click **Delete** link against the bonding interface you want to delete.
-

Configuring static routes

Adding a static route

Use this procedure to add a static route to System Platform. Static routes can be used to route packets through a VPN to an Avaya Partner that is providing remote service.

-
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**.
-

Related topics:

[Static route configuration field descriptions](#) on page 44

Deleting a static route

-
1. Click **Server Management > Static Route Configuration**.
 2. Click **Delete** next to the static route that you want to delete.
-

Related topics:

[Static route configuration field descriptions](#) on page 44

Modifying a static route

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

Related topics:

[Static route configuration field descriptions](#) on page 44

Static route configuration field descriptions

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

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

Related topics:

[Adding a static route](#) on page 42

[Deleting a static route](#) on page 43

[Modifying a static route](#) on page 43

Configuring Ethernet settings

Configuring Ethernet interface settings

-
1. Click **Server Management > Ethernet Configuration**.
The Ethernet Configuration page displays the values for all Ethernet interfaces on the server, for example, eth0, eth1, eth2, and so on.
 2. Modify the values for eth0 and eth1 as appropriate.
 3. Click **Save** to save your settings.
-

Related topics:

[Ethernet configuration field descriptions](#) on page 45

Ethernet configuration field descriptions

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

Name	Description
Speed	Sets the speed in MB per second for the interface. Options are: <ul style="list-style-type: none"> • 10 Mb/s half duplex • 10 Mb/s full duplex • 100 Mb/s half duplex • 100 Mb/s full duplex • 1000 Mb/s full duplex Auto-Negotiation must be disabled to configure this field.
Port	Lists the available Ethernet ports. Auto-Negotiation must be disabled to configure this field.
Auto-Negotiation	Enables or disables auto-negotiation. By default it is enabled, but might cause some problems with some network devices. In such cases you can disable this option.

Button descriptions

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

Related topics:

[Configuring Ethernet interface settings](#) on page 44

Configuring alarms

Alarm descriptions

System Platform generates the following alarms:

Alarm	Description
High CPU	Average CPU Usage of VM
Disk Usage (Logical Volume)	Percentage of logical volume used (/ , / template-env, /dev/shm, /vspdata, vsp-template)
Disk (Volume Group)	Percentage of volume group used (VolGroup00)
Disk reads	Disk read rate (sda)
Disk Writes	Disk write rate (sda)
Load Average	Load average on each virtual machine
Network I/O received	Network receive rate for all guests (excluding dedicated NICs)
Network I/O Transmit	Network transmit rate for all guests (excluding dedicated NICs)
Webconsole heap	Percentage of webconsole (tomcat) heap memory in use
Webconsole open files	Number of file descriptors that webconsole has open
Webconsole permgen	Percentage of webconsole (tomcat) permgen heap used
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

 **Note:**

A virtual machine other than System Domain and Console Domain may support configuring alarms relevant to its operations. Please check the administration document of the virtual machine to know whether any alarms are present for the virtual machine and how to configure them.

Configuring alarm settings

1. Click **Server Management > Alarm Configuration**.
2. On the Alarm Configuration page, modify the settings as appropriate.

3. Select **Enabled** to enable an alarm.
4. In the **Limit Value** field, enter the threshold value for the alarm.
5. Specify the number of consecutive samples that must exceed the threshold value for the system to generate an alarm.
6. Specify the **Suppression Period** for an alarm after the system generates the previous alarm.
7. Click **Save** to save the settings.

Related topics:

[Alarm descriptions](#) on page 45

[Alarm configuration field descriptions](#) on page 47

Alarm configuration field descriptions

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

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

Related topics:

[Alarm descriptions](#) on page 45

[Configuring alarm settings](#) on page 46

Managing Certificates

Certificate management

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

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

Similarly, the user can upload and replace the enterprise LDAP certificate by selecting new certificate file on the local machine, and uploading it. The Certificate Management page shows the following data for the current System Platform Web Console and Enterprise LDAP certificate:

- Type
- Version
- Expiry date
- Issuer

Here are the things to note relating to a certificate:

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

Related topics:

[Enterprise LDAP field descriptions](#) on page 78

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.
-

Related topics:

[Configuring authentication against an enterprise LDAP](#) on page 78

Certificate Management field descriptions

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

Field descriptions

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

Button descriptions

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

Managing System Platform licenses

License management

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

Launching WebLM

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

1. Click **Server Management > License Management**.
2. On the License Management page, click **Launch WebLM License Manager**.
3. When WebLM displays its Logon page, enter the user name and password for WebLM. For initial login to WebLM, the user name is `admin`, and the password is `weblmadmin`. However, you must change the password the first time that you log in to WebLM.
4. Manage the licenses as appropriate.

For more information on managing licenses in Avaya WebLM, see *Installing and Configuring Avaya WebLM Server* at <http://www.avaya.com/css/P8/documents/100069577>.

Related topics:

[License management](#) on page 50

[License Management field descriptions](#) on page 50

License Management field descriptions

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

Button descriptions

Name	Description
Launch WebLM License Manager	Launches the WebLM application.

Related topics:

[License management](#) on page 50

[Launching WebLM](#) on page 50

Configuring the SAL Gateway

SAL

System Platform includes Avaya's Secure Access Link (SAL) Gateway to manage service delivery (alarming and remote access). SAL Gateway is a software application that:

- Facilitates remote access to support personnel and tools that are needed to access supported devices
- Collects and sends alarm information to a Secure Access Concentrator Core Server, on behalf of the managed devices
- Provides a user interface to configure its interfaces to managed devices, Concentrator Remote and Core Servers, and other settings

SAL requires an upload bandwidth (customer to Avaya) of at least 90 kB/s (720 kb/s) with latency no greater than 150 ms (round trip.)

During the installation of System Platform, you must register the system (System Platform, solution templates, and SAL Gateway) and configure SAL for the customer's network.

Important:

For Avaya to provide support, Avaya Partners or their customers must ensure that SAL is registered and configured properly. Avaya support will be delayed or not possible if SAL is not properly implemented.

Avaya Partners must provide their own B2B VPN connection (or other IP-based connectivity) to deliver remote services. SAL does not support modem connections.

You can launch the SAL Gateway management portal from within System Platform.

Launching the SAL Gateway management portal

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

-
1. Click **Server Management > SAL Gateway Management**.
 2. On the SAL Gateway Management page, click **Launch SAL Gateway Management Portal**.
 3. When the portal displays its Log On page, enter your user name and password for Console Domain.
 4. Configure the SAL Gateway as appropriate.

Related topics:

[SAL](#) on page 51

[Configuring the SAL Gateway](#) on page 52

[SAL Gateway Management field descriptions](#) on page 53

Configuring the SAL Gateway

To configure the SAL Gateway for the customer's network and System Platform, follow the instructions that are provided in *Administering SAL on Avaya Aura™ System Platform*. This document is available on <http://support.avaya.com/css/P8/documents/100069101>.



Note:

For an understanding of how to administer the customer's network to support SAL, follow the instructions provided in *Secure Access Link 1.8 SAL Gateway Implementation Guide*. This document is available on <http://www.avaya.com/support>.

SAL Gateway Management field descriptions

Button	Description
Launch SAL Gateway Management Portal	Launches the SAL Gateway management portal in a new Web browser window. You must provide valid certificate details to access the portal.

Related topics:

[SAL](#) on page 51

[Launching the SAL Gateway management portal](#) on page 52

[Configuring the SAL Gateway](#) on page 52

Viewing System Platform statistics

Performance statistics

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

Data retention and consolidation

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

Monitored parameters

System Platform collects data on the following parameters every minute:

Variable	Domain	Description	Source
CPU usage	All domains	Average CPU usage. Is calculated from cpuSeconds	<code>xm list -long</code>
System Platform Web Console memory	cdom	Free and used heap and permgen memory.	JVM

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

Graphs

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

Alarms

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

Related topics:

[Log severity levels](#) on page 35

[Exporting collected data](#) on page 55

[Performance statistics field descriptions](#) on page 55

Viewing performance statistics

1. Click **Server Management > Performance Statistics**.
2. On the Server Management page, perform one of the following steps:
 - Select **All Statistics** to generate a graph for all recorded statistics.

- Clear **All Statistics**, and select the type of graph from the **Type** drop down menu. Then select the required domain from the list in the **Domains** box.
3. Specify the date and time for the period that you want the report to cover.
 4. Click **Generate** to generate the performance graph for the system.

Related topics:

[Exporting collected data](#) on page 55

[Performance statistics field descriptions](#) on page 55

Exporting collected data

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

-
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 export.
 4. Click **Save** and specify the location to download the data.

Related topics:

[Log severity levels](#) on page 35

[Performance statistics](#) on page 53

[Performance statistics field descriptions](#) on page 55

Performance statistics field descriptions

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

Field Names	Descriptions
All Statistics	If you select this option, the system displays a graph for all the recorded statistics.
Type	Appears only if the All Statistics check box is cleared. Lets you specify the type of statistics you want to display from a list of options.

Field Names	Descriptions
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.

Related topics:

[Viewing performance statistics](#) on page 54

[Exporting collected data](#) on page 55

Ejecting the CD or DVD

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

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

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

Deleting old, unused files

Use the File Management page to delete old versions of the solution template files and platform upgrade images. However, you cannot delete the files for the currently installed solution templates. System Platform stores solution template files and platform upgrade images in a folder on the system.

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

Configuring security

Security configuration

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

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

 **Important:**

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

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

 **Important:**

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





Configuring security





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

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

Security Configuration field descriptions

Field descriptions

Name	Description
Remove network debugging tools (wireshark)	<p>Indicates whether or not to remove the network debugging tools.</p> <p> Important: Removing the network debugging tools is irreversible. The tools are removed from System Platform Web Console and the Console Domain. A platform upgrade makes the tools available again and the Remove network debugging tools (wireshark) check box is also enabled.</p>
Enable Audit	<p>Indicates whether or not the audit is to be enabled.</p> <p> Important: Enabling audit is irreversible.</p>
Reset Grub Password	Is the new System Platform Web Console Grub password.
Retype Grub Password	Is the new System Platform Web Console Grub password being retyped for verification.
Verify Dom0 Reset Password	Is the System Platform Web Console root password to reset the System Platform Web Console Grub password.
Cdom Hosts Allow List	<p>Is the list of hosts that can access the Console Domain.</p> <p> Note: The list of hosts is maintained in the <code>hosts.allow</code> file at <code>/etc</code> on the Console Domain.</p>
Cdom Hosts Deny List	<p>Is the list of hosts that cannot access the Console Domain.</p> <p> Note: The list of hosts is maintained in the <code>hosts.deny</code> file at <code>/etc</code> on the Console Domain.</p>

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

Button descriptions

Name	Description
Save	Saves the security configuration.

Backing up System Platform

System Platform backup

You can back up configuration information for System Platform and the solution template (all 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 Failover node back to High Availability Failover configuration. Follow the instructions in this document on how to re-enable failed High Availability Failover node back to High Availability Failover configuration.

Related topics:

[Re-enabling failed standby node to High Availability Failover](#) on page 126

[Re-enabling failed preferred node to High Availability Failover](#) on page 127

Backing up the system by using the System Platform Web Console

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

-
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 free space at the location where you are storing the backup archive.

4. Select where to store or send the backup files:
 - **Local:** Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
 - **SFTP:** Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.

- **Email:** Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

**Note:**

Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.

5. Enter other information as appropriate.
6. Click **Backup Now**.

Related topics:

[Backup field descriptions](#) on page 62

Scheduling a backup

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

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

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

5. Click **Schedule Backup**.

Related topics:

[Backup field descriptions](#) on page 62

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

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

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

Backup field descriptions

Use the Backup page to back up configuration information for System Platform and the solution template (all virtual machines).

Backup Now fields

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

Field Names	Descriptions
Backup Method	<p>Select a location to send the backup file:</p> <ul style="list-style-type: none"> • Local: Stores the backup archive file on System Platform in the /vspdata/backup/archive directory. • SFTP: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server. Enter the hostname, directory, user name, and password for the SFTP server. • Email: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server. Enter the e-mail address and the server address of the recipient.
Backup Now	Starts the backup operation.

Schedule Backup fields

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

Field Names	Descriptions
Frequency	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Daily • Weekly • Monthly
Start Time	The start time for the backup.
Archives kept on the server	The number of backup archives to store on the System Platform server. The default is 10.
Backup Method	<p>Select a location to send the backup file:</p> <ul style="list-style-type: none"> • Local: Stores the backup archive file on System Platform in the /vspdata/backup/archive directory. • SFTP: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server. Enter the hostname, directory, user name, and password for the SFTP server. • Email: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server. Enter the e-mail address and the server address of the recipient.
Schedule Backup	Schedules the backup process.
Cancel Schedule	Cancels an existing backup schedule.

Related topics:

[Backing up the system by using the System Platform Web Console](#) on page 60

[Scheduling a backup](#) on page 61

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 Failover configuration from the backup file. It is not the aim of the restore feature to re-enable the failed High Availability Failover node back to High Availability Failover configuration. Follow the instructions given in this document on how to re-enable the failed High Availability Failover node back to High Availability Failover configuration. Avaya recommends that you restore the backup configuration before configuring and starting High Availability Failover.

-
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 Web Console to restart, so you must log in again when the restore operation is completed.

Related topics:

[System Platform backup](#) on page 59

[Restore field descriptions](#) on page 65

Restore field descriptions

Field Names	Descriptions
Restore from	Select the location of the backup archive file from which you want to restore configuration information. <ul style="list-style-type: none"> • Local: Restores from a file on System Platform. If you select this option, the Restore page displays a list of previously backed up archives on the System Platform system. • SFTP: Restores from a file on a remote server. If you select this option, enter the hostname or IP address of the remote server, directory where the archive file is located, and user name and password for the SFTP server. • Upload: Restores from a file on your computer.
Archive Filename	Filenames of the backup archive files at the location you specify.
Archive Date	Date that the file was created.
Selection	Select this check box to restore from the archive file.
Restore History	Displays the restore history for the last ten restores. If an error occurred during the last restore, the system directs you to this page after login and continues to display an error message until a restore is successful.

Button descriptions

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

Related topics:

[Restoring backed up configuration information](#) on page 64

Viewing restore history

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

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

Rebooting or shutting down the System Platform server

Rebooting the System Platform Server

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. When this happens, a service disruption may occur.

 **Note:**

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

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

Related topics:

[Server Reboot Shutdown field descriptions](#) on page 68

Rebooting the whole High Availability Failover system

When you reboot the whole High Availability Failover system, the system shuts down all the virtual machines running on the primary server, reboots the standby server, and reboots primary server to prevent failover. When this happens, a service disruption may occur.

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

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



Note:

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

Shutting down the System Platform Server

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. When this happens, a service disruption may occur.



Note:

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

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

Related topics:

[Server Reboot Shutdown field descriptions](#) on page 68

Shutting down the whole High Availability Failover system

When you shut down the whole High Availability Failover system, the system shuts down all the virtual machines running on the primary server, shuts down the secondary server, and shuts down the primary server to prevent failover. When this happens, a service disruption may occur.

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

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



Note:

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

Server Reboot Shutdown field descriptions

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

Name	Description
Name	Name of the application being shutdown. This is always System Domain (Domain-0).
MAC Address	Machine address of the virtual machine.
IP Address	IP address of the System Platform server.
OS Type	Operating system of the System Platform server, for example, Linux.
State	<p>Current status of the virtual machine. Possible values are as follows:</p> <ul style="list-style-type: none"> • 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.
Application State	<p>Current status of the application (respective virtual machine). Possible values are as follows:</p> <ul style="list-style-type: none"> • 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.

Name	Description
	<ul style="list-style-type: none"> • 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. This is not the same as uptime.
Virtual CPUs	The maximum number of virtual CPUs that can run on System Platform server.
Domain UUID	Unique ID of the virtual machine.
Auto Start	Status of auto start - shows if the System Platform server starts automatically after a shut down operation. Available status are True (if auto start is set), and False (if auto start is not set).

Button descriptions

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

Related topics:

[Rebooting the System Platform Server](#) on page 66

[Shutting down the System Platform Server](#) on page 67

Chapter 4: User Administration

User Administration overview

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

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

User roles

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

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

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

Related topics:

[Creating users](#) on page 74

[Modifying users](#) on page 75

Managing System Platform users

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

- Administrator
- Advanced Administrator

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

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

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

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

A user with Administrator role can only change own password.

Access restrictions for Administrator role

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

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

Menu	Option	Web page control	Access restriction
			SyncSpeed, Pause/Unpause Sync buttons.
	Performance Statistics		Granted
	Eject CD / DVD		Granted
	File Manager		Granted
	Security Configuration		Denied
	Backup / Restore > Backup		Granted
	Backup / Restore > Restore		Denied
	Server Reboot / Shutdown		Denied
User Administration	Local Management		Denied
	Change LDAP Password		Denied
	Enterprise LDAP		Denied
	Change Password		Denied
	Authentication File		Denied

 **Note:**

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

Creating users

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

-
1. Click **User Administration > Local Management**.
 2. On the Local Management page, click **Create User**. The Local Management page changes to accept the details of new user.
 3. In the **User Id** field, enter a unique user ID.
 4. In the **User Password** field, enter a password.

 **Note:**

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

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 create the user with the details you have specified.

Related topics:

[Local Management field descriptions](#) on page 76

Modifying users

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

 **Note:**

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

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

 **Note:**

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

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.

Related topics:

[Local Management field descriptions](#) on page 76

Deleting users

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

 **Note:**

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

-
1. Click **User Administration > Local Management**.
 2. On the Local Management page, select the user that you want to delete:
 3. Click **Delete User**.
 4. In the dialog box that appears to confirm deleting the user, click **OK**.
-

Related topics:

[Local Management field descriptions](#) on page 76

Local Management field descriptions


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

Manage Users

Name	Description
User Id	User name for the user.
User Role	Role of the user. Options are: <ul style="list-style-type: none"> • Advanced Administrator • Administrator

Create User and Edit User

Name	Description
User Id	User name for the user.
User Password	Password for the respective user.

Name	Description
	 Note: Passwords must be at least six characters long. Avaya recommends using only alphanumeric characters.
Confirm Password	Reenter the password for the user.
User Role	Role of the user. Options are: <ul style="list-style-type: none"> • Advanced Administrator • Administrator

Related topics:

[Creating users](#) on page 74

[Modifying users](#) on page 75

[Deleting users](#) on page 76

Authenticating System Platform users against an enterprise LDAP

Authentication against an enterprise LDAP

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

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

 **Note:**

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

Related topics:

[Configuring authentication against an enterprise LDAP](#) on page 78

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.

Related topics:

[Selecting enterprise LDAP certificate](#) on page 49

[Authentication against an enterprise LDAP](#) on page 77

[Enterprise LDAP field descriptions](#) on page 78

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 .

Name	Description
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 LDAP user.
Attribute Map	Specifies LDAP filters for the advanced administrator and administrator roles. A simple filter can be <i>memberOf=admin_Group</i> . A complex filter can contain multiple criteria such as: <i>(&(memberOf=vsp-craft)(userstatus=ACTIVE))</i> .
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 <i>(&(memberOf=vsp-craft)(userstatus=ACTIVE))</i> 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 <i>(&(memberOf=vsp-admin)(userstatus=ACTIVE))</i> will filter the active users who are the members of vsp-admin.

Related topics:

[Configuring authentication against an enterprise LDAP](#) on page 78

Changing the System Platform LDAP password

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

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



Note:

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

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

Changing your System Platform password

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

-
1. Click **User Administration > Change Password**.
 2. In the **Old Password** field, enter your current password.
 3. In the **New Password** field, enter a new password.



Note:

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

4. In the **Confirm Password** field, reenter the new password.
 5. Click **Change Password** to change the current password.
-

Managing the authentication file

Authentication file for ASG

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

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

Installing an authentication file

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

 **Note:**

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

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

You do not need to select this option if you are replacing the default authentication file with a unique authentication file.

 **Caution:**

Use caution when selecting the **Force load of new file** option. If you install the wrong authentication file, certificate errors and login issues may occur.

4. Click **Install**.
The system uploads the selected authentication file and validates the file. The system installs the authentication file if it is valid.

 **Note:**

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

Chapter 5: Configuring High Availability Failover

High Availability Failover overview

The System Platform High Availability Failover is an optional feature aimed at providing service continuity. However, it does not support critical reliability. Moreover, certain solution templates (Communication Manager is one such template) do not support this feature.

 **Note:**

System Platform High Availability Failover does not support IPv6 and cannot be configured with IPv6 addresses.

The System Platform High Availability Failover feature offers the following capabilities:

Node scores

High Availability Failover uses node scores to compute the ability of each machine to run the resources and determine which node runs the resources. If the system has no issues, and resources could run on either node, both machines have the same score. Thus System Platform uses the term “preferred node” for the machine that should run the resources when the system has no issues. The preferred node has a small score benefit. So if both machines are booted at the same time, the preferred node will run resources. The node from which you configure High Availability Failover is designated the preferred node. If you stop High Availability Failover, the currently active node becomes the preferred node.

No auto-failback

High Availability Failover does not use auto-failback to migrate resources back to the preferred node when the resources are running on the standby node and the preferred node becomes available again. Switching servers disrupts service, and if both servers are healthy, then running on the preferred node offers no increased benefit. If you want to migrate resources back to the preferred node after a failover or a switchover, you can do so by using the **Manual Switchover** option in the Failover menu at the most suitable time.

Expected failover/switchover times

High Availability Failover uses 30 seconds as a timeout interval after which the standby node will declare the active node dead and start resources (even though the active node may be not accessible, not running or blocked). Note that System Platform does not provide any Web interface to modify this interval.

For manual switchover or when the system initiates a preemptive failover, the total time between the start of the command and activating the standby node includes a graceful shutdown and restart of all resources:

- Stop of resources—Up to 5 minutes.
- Start of resources—Up to 5 minutes.
- Resulting longest switchover time—Up to 10 minutes.

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

- Detect active node failure—30 seconds.
- Start of resources—Up to 5 minutes.
- Resulting longest switchover time—Up to 5.5 minutes.

*** Note:**

The switchover time is approximate and varies depending on the hardware running System Platform with no templates. The switchover is further delayed by the following factors:

- The system runs complex templates.
- The system shutdown was not proper. Therefore, the system performs an FSCK (File System Check) as it boots up and starts the virtual machines.

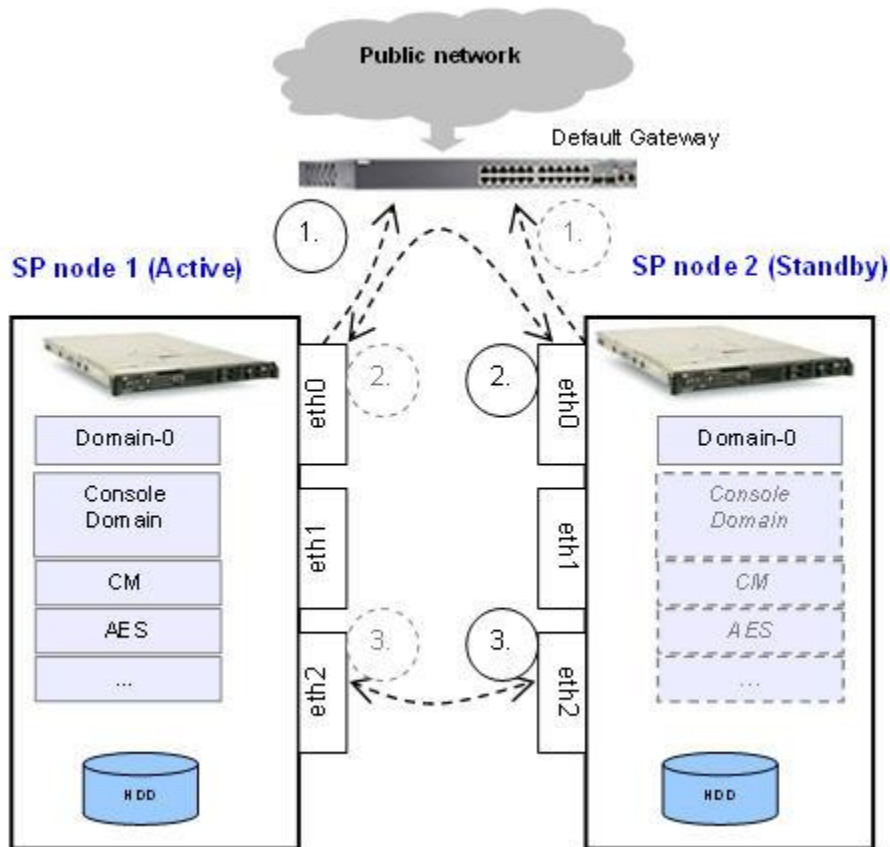
How High Availability Failover works

Ping targets

High Availability Failover uses node scoring to compute the ability of each machine to run the resources and determine which node runs the resources. Each node uses the following three ping targets:

- The default network gateway as a public ping target.
- The eth0 network interface of the peer.
- The crossover interface of the peer (eth2 by default).

Each successful ping result adds points to the node's score. The node that has the higher score becomes the active node. Therefore, if both machines can reach all three ping targets, they both have the same score, and resources run on the preferred node. The following image shows the two System Platform servers with their three ping targets.



Ping requests to these targets fail in three scenarios. These scenarios and their results are as follows:

- If the crossover link is interrupted on any node, no action occurs because both machines have the same score.
- If the public link is interrupted on the standby node, no action occurs because the active node still has the full score while the standby node has lost two ping sources.
- If the public link is interrupted on the active node, failover occurs because the active node has lost two ping sources while the standby has the full score.

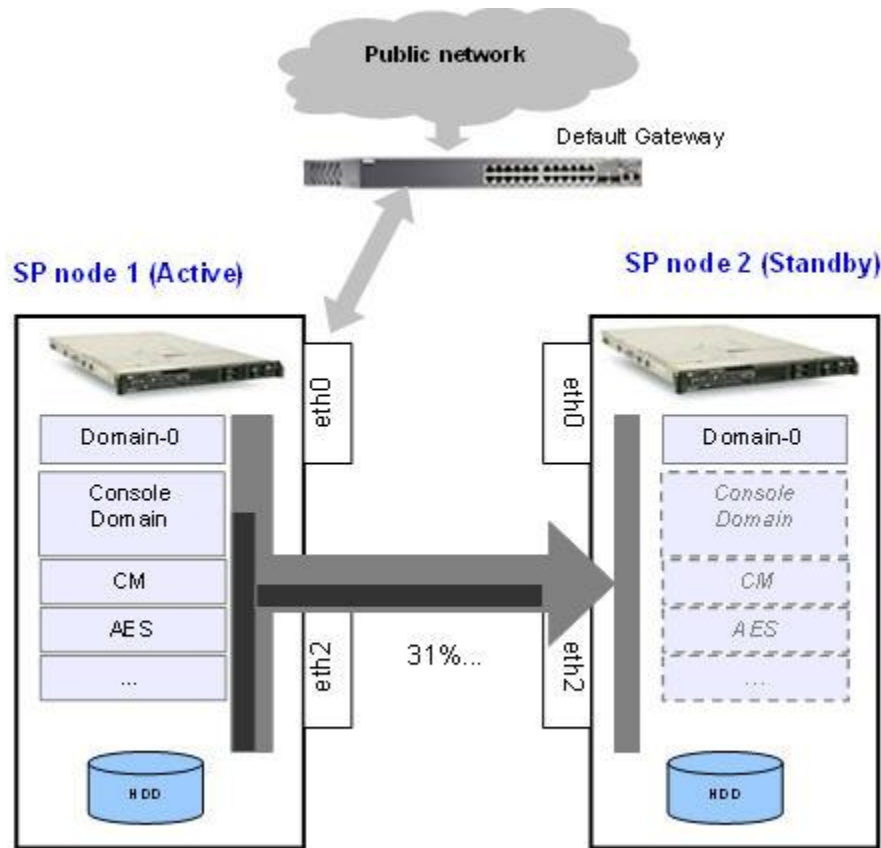
! Important:

The default gateway is the ping target and cannot be configured. Ensure that your gateway replies to ICMP pings that come from the System Platform nodes.

Initial data synchronization

High Availability Failover uses the Distributed Replicated Block Device (DRBD) software component to propagate online changes that are made on the active node. Each logical volume propagated by DRBD uses a separate DRBD resource. You can view the synchronization status on the System Platform Failover page. However, before the initial synchronization of

the DRBD resources is complete, the standby node does not have sufficient data to start the virtual machines. The following image shows the initial data synchronization from the active node to the standby node:



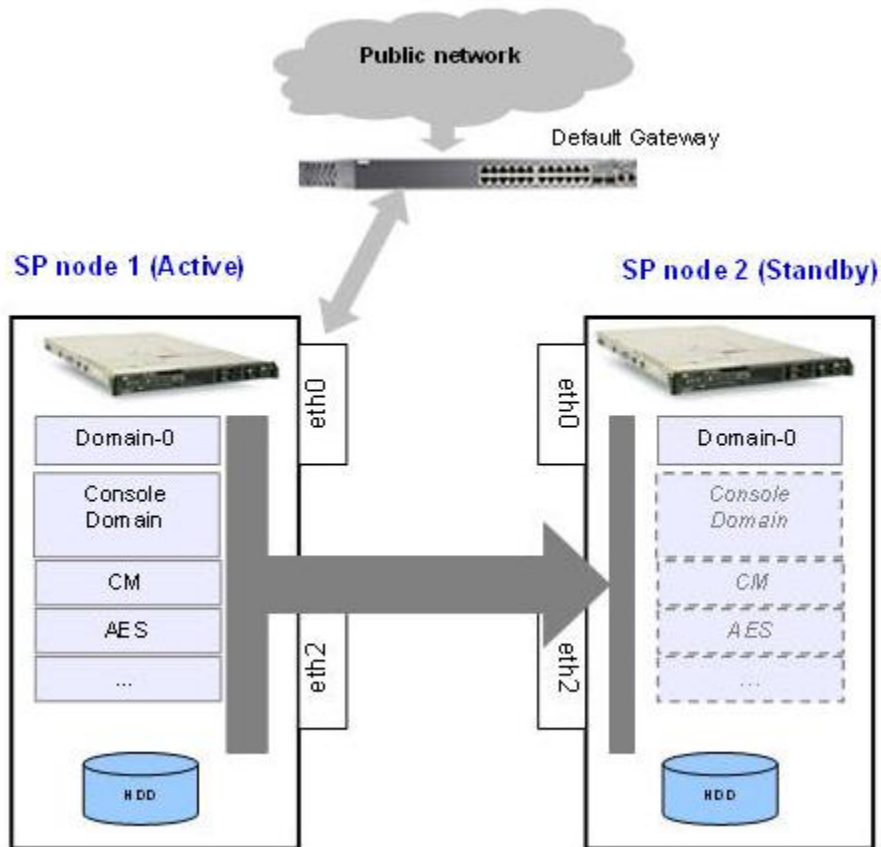
*** Note:**

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 30 MB/s. You can modify this value from the Failover page in case the system is not overloaded.

For more information on the DRBD component, see <http://www.drbd.org>.

Online propagation of data changes

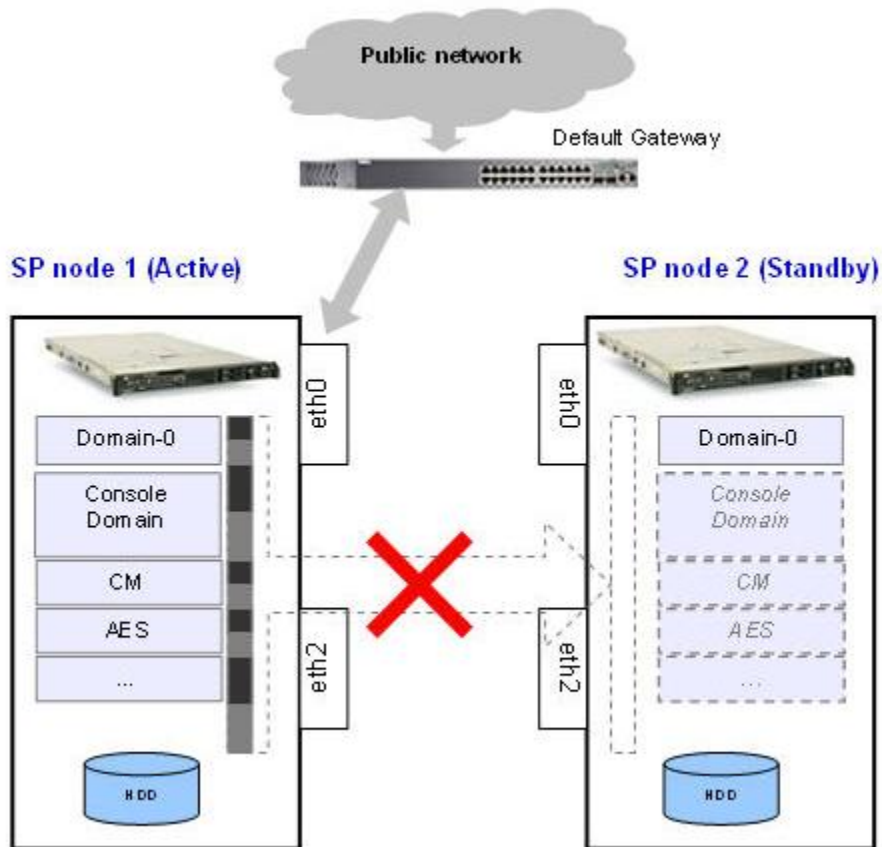
High Availability Failover uses the Distributed Replicated Block Device (DRBD) software component to propagate online changes that are made on the active node. DRBD's protocol C ensures that when changes are made on the active node, those changes are not reported as complete until they are made and confirmed on the standby node. This ensures that the machines are kept in a consistent state, and the standby node can take over when required. The following image shows data propagation from the active node to the standby node.



If a failover or switchover occurs and 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.

Data changes during disconnection

If the replication link is interrupted, DRBD uses metadata to keep the history of modified data blocks since the connection was interrupted. 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 shows the data change history that is marked in the DRBD metadata during an interruption of the replication link.



Automatic split-brain resolution

If all network links between the two nodes fail and the nodes are unable to communicate, both nodes may become active at the same time. This situation is called Split-Brain. After both nodes are on the network again, data changes must be discarded from one of the nodes. High Availability Failover uses a DRBD feature to recognize which node was the node that became active as the first node (active at the time of disconnection). This node is rebooted immediately and its data changes are discarded. After successful reboot, it will synchronize the changes that occurred on the node that activated after disconnection.

Automatic failover

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

The system performs the following steps:

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

High Availability Failover and template configuration

System Platform does not support installation, upgrade, or deletion of templates while High Availability Failover is running. A warning message is displayed on template pages, and you cannot perform these actions. To install, upgrade, or delete a template, you must first stop High Availability Failover. When you stop High Availability Failover, System Platform removes any installed templates from the standby node. Any template operations that you perform must be performed on the preferred node. Once you have finished with template configuration, you can restart High Availability Failover.

Important:

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

Related topics:

[Starting High Availability Failover](#) on page 93

[Stopping High Availability Failover](#) on page 93

Requirements for High Availability Failover

The requirements for High Availability Failover are as follows:

- Two servers with exactly the same hardware configuration. The standby server cannot have less memory, number of processors, total disk space or free disk space than the primary server.
- The hardware must be supported by System Platform.
- The servers must have a spare Gigabit network interface to be dedicated exclusively to High Availability Failover services. The servers must be connected on the same ports on both machines.
- Both the servers must be in the same subnet.
- Both servers must be in close proximity so that they can be connected with the crossover cable. The Ethernet specification limit for this distance is 100 meters.
- The same version of System Platform must be installed on the active and standby nodes.
- Do not install a template on the standby node. If you do so, you will not be able to start High Availability Failover. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability Failover.

Prerequisites for configuring High Availability Failover

The prerequisites for configuring High Availability Failover are as follows:

- Connect both the servers with a Gigabit-certified Ethernet cable on the same ports on both machines.
- Ensure that your network gateway replies to ICMP requests from the System Platform nodes. The default network gateway is the ping target of the High Availability Failover heartbeat. This target cannot be configured differently.

Configuring High Availability Failover

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

1. Log in to the Web Console of the server that you want to be the preferred node.
2. Click **Server Management > Failover** to display the Failover page.
The Failover page displays the current status of High Availability Failover.
3. Click **Configure Failover**.
4. On the Configure failover page, enter the appropriate information to configure High Availability Failover.

5. Click **Create**.
6. After the system completes creation of the High Availability Failover configuration, click **Start Failover Mode** and confirm the warning that is displayed.
System Platform Web Console redirects to the Reboot page and after a few minutes redirects to the Login page.
7. Log in to the System Platform Web Console.
8. Click **Server Management > Failover**.
You can check the status of the failover components on the Failover page and ensure that Distributed Replicated Block Device (DRBD) is synchronizing the hard disks of the two servers.

**Tip:**

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

Related topics:

[Configure Failover field descriptions](#) on page 91

Configure Failover field descriptions

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

Related topics:

[Configuring High Availability Failover](#) on page 90

[Troubleshooting steps](#) on page 125

Start and stop of High Availability Failover

Starting High Availability Failover

System Platform can be changed from a standard configuration to a High Availability Failover configuration during system installation or anytime later. Once you have installed a new server that has the same configuration, such as the number of processors and disk space, and installed the same version of System Platform, you are ready to proceed.

 **Important:**

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

When you start High Availability Failover, the console domain and all template virtual machines are restarted. When this happens, System Platform Web Console redirects to the Reboot page and after a few minutes redirects to the Login page.

Stopping High Availability Failover

If you want to stop High Availability Failover, you should do so as soon as no disk synchronization is in progress or the disk synchronization is not paused. If you stop High Availability Failover during disk synchronization, the file system of the standby console domain could be corrupted.

When you stop High Availability Failover, the console domain and all template virtual machines are restarted. When this happens, System Platform Web Console redirects to the Reboot page and after a few minutes redirects to the Login page.

When High Availability Failover is stopped, the system does not propagate changes from the preferred node to the standby node.

When High Availability Failover is stopped, you can access the Web Console on the standby server by using its IP address (provided during configuration of High Availability Failover).

Removing the High Availability Failover configuration

If you want to permanently remove the High Availability Failover configuration, you can do so.

Related topics:

[Starting High Availability Failover](#) on page 93

[Stopping High Availability Failover](#) on page 93

Starting High Availability Failover

Prerequisites

High Availability Failover is configured on the system.

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

This procedure restarts the console domain and all template virtual machines.

-
1. Click **Server Management > Failover**.
 2. Click **Start Failover Mode** and confirm the warning that is displayed.
System Platform Web Console redirects to the Reboot page and after a few minutes redirects to the Login page.
 3. Log in to the System Platform Web Console.
 4. Click **Server Management > Failover** and check the disc synchronization progress.

Related topics:

[Start and stop of High Availability Failover](#) on page 92

Stopping High Availability Failover

This procedure stops High Availability Failover but does not remove the High Availability Failover configuration. You can restart it at any time.

This procedure restarts the console domain and all template virtual machines.

-
1. Click **Server Management > Failover**.
 2. Click **Stop Failover Mode** and confirm the warning that is displayed.
System Platform Web Console redirects to the Reboot page and after a few minutes redirects to the Login page.

3. Log in to the System Platform Web Console.
4. Click **Server Management > Failover** and check the status of the High Availability Failover.

Related topics:

[Start and stop of High Availability Failover](#) on page 92

Removing the High Availability Failover configuration

Use this procedure to permanently remove the High Availability Failover configuration.

-
1. Click **Server Management > Failover**.
 2. Click **Remove Failover** and confirm the warning that is displayed.
-

Switching from an active server to a standby server manually

-
1. Click **Switch Over** on Configure Failover page.
 2. Click **OK** to confirm the warning message.
The system performs the following tasks:
 - a. Shuts down the virtual machines on the active node.
 - b. Sets the DRBD devices as secondary on the active node.
 - c. Assigns the secondary node as a new primary node, and sets the primary node as a secondary node.
 - d. Sets the DRBD devices as primary on the new active node.
 - e. Boots the virtual machines on the new active node.

 **Note:**

When you perform a manual switchover, the system shuts down all template virtual machines and the Console Domain on the active node. System Platform Web Console redirects to the Reboot page until the Console Domain is up on the

new active server (previously standby server). After that it redirects to the Login page.



Chapter 6: System Platform security

Command line login to System Domain and Console Domain

The `admin` and `cust` user IDs can be used to access the system through the command line interface. The user can open an SSH session or directly connect a keyboard and monitor to the System Platform server to log in. An Avaya technical support person can log in to the system using the `craft` user ID and the ASG challenge/response mechanism.

 **Note:**

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

Firewall settings for IPv4

System Platform firewall rules on System Domain and on Console Domain are on by default. You need to log in using the `root` user ID to perform this task.

Stopping firewall rules

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

Starting firewall rules

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

Displaying currently set firewall rules

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

Logging IP packets blocked by firewall

 **Note:**

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

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

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

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

Stopping logging of IP packets blocked by firewall

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

Firewall settings for IPv6

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

You need to log in using the `root` user ID to perform this task.

Stopping firewall rules

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

Starting firewall rules

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

Displaying currently set firewall rules

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

Logging IP packets blocked by firewall

 **Note:**

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

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

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

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

Stopping logging of IP packets blocked by firewall

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

Linuxshield installation and configuration

LinuxShield virus scan

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

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

 **Note:**

System Platform runs a hardened Linux-based operating system and it is unlikely that any viruses or other types of malicious code will be able to penetrate the system. LinuxShield provides an additional layer of protection to an already secure system for the enterprises that have very high security requirements. Most systems will not need to install LinuxShield.

Avaya recommends that LinuxShield is installed and configured only by people who have knowledge of working on Linux servers. Further, LinuxShield virus scan may affect the system performance.

Installing and configuring Linuxshield on System Domain

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



Note:

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

Installing and configuring Linuxshield on Console Domain

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



Note:

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

Files requiring the SUID and SGID bits set

Files requiring SUID and SGID bits set on System Domain

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

Permissions	Location	File name	Ownership
-rwsr-xr-x	/bin	umount	
-rwsr-xr-x	/bin	ping6	
-rwsr-x---	/bin	fusermount	
-rwsr-xr-x	/bin	ping	
-rwsr-xr-x	/bin	su	
-rwsr-sr-x	/opt/dell/srvadmin/oma/ bin	omcliproxy	
-rwxr-sr-x	/usr/bin	ssh-agent	
---s--x--x	/usr/bin	sudo	
-rwsr-xr-x	/usr/bin	chage	
-rwsr-sr-x	/usr/bin	crontab	
-rws--x--x	/usr/bin	Xorg	
-rwsr-xr-x	/usr/bin	newgrp	
---s--x--x	/usr/bin	sudoedit	
-rws--x--x	/usr/bin	chsh	
-rwxr-sr-x	/usr/bin	write	
-rwsr-xr-x	/usr/bin	passwd	
-rws--x--x	/usr/bin	chfn	
-rwxr-sr-x	/usr/bin	cl_status	
-r-xr-sr-x	/usr/bin	wall	
-rwsr-xr-x	/usr/bin	gpasswd	
-rwsr-xr-x	/usr/libexec	libvirt_proxy	
-rwx--s--x	/usr/libexec/utempter	utempter	

Permissions	Location	File name	Ownership
-rwsr-xr-x	/usr/libexec/openssh	ssh-keysign	
-rws--x--x	/usr/sbin	userhelper	
-rwsr-xr-x	/usr/sbin	usernetctl	
-rwsr-x---	/lib64/dbus-1	dbus-daemon-launch-helper	
-rwsr-x---	/sbin	mount.ecryptfs_private	
-rwsr-xr-x	/sbin	unix_chkpwd	
-rwsr-xr--	/sbin	drbdsetup	
-rwsr-xr--	/sbin	drbdmeta	
-rwsr-xr-x	/sbin	umount.nfs	
-rwsr-xr-x	/sbin	mount.nfs4	
-rwxr-sr-x	/sbin	netreport	
-rwsr-xr-x	/sbin	pam_timestamp_check	
-rwsr-xr-x	/sbin	mount.nfs	
-rwsr-xr-x	/sbin	umount.nfs4	

Files requiring SUID and SGID bits set on Console Domain

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

Permissions	Location	File name	Ownership
-rwsr-xr-x	/bin	su	
-rwsr-xr-x	/bin	mount	
-rwsr-xr-x	/bin	ping6	
-rwsr-xr-x	/bin	ping	
-rwsr-x---	/bin	fusermount	
-rwsr-xr-x	/bin	umount	
-rwsr-xr-x	/usr/libexec	libvirt_proxy	
-rwsr-xr-x	/usr/libexec/openssh	ssh-keysign	
-rwxr-sr-x	/usr/bin	ssh-agent	

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

Disabling booting from removable media

BIOS changes to disable booting from removable media

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

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

Disabling booting from removable media on S8510

-
1. Upon booting, press the **F2** key to start the BIOS setup utility.
You may need to enter the setup password.
 2. From the menu, click **Boot Sequence**.
A list of bootable devices will be displayed..
 3. Select **Hard Drive** from the boot sequence list and press the **+** key to move it to the first position in the list.
 4. Press the **Spacebar** to clear selection of all other devices such as CD-ROM and embedded NIC in the boot sequence list.
 5. If a BIOS password has not been enabled, click **System Security** from the main menu and enter a password.
 6. Press **Escape** to exit from the boot sequence list.
 7. Click **Save changes**.
-

Disabling booting from removable media on S8800

-
1. Upon booting, press the **F1** to start UEFI.
You may need to enter the setup password.
 2. From the menu, click **Boot Manager**.
 3. In the **Boot Manager** screen, click **Change Boot Order**.
 4. Select **Hard Drive** from the boot sequence list and press the **+** key to move it to the first position in the list.
 5. Exit **Change Boot Order**.

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

Disabling booting from removable media on S8300D

1. Enter the BIOS setup by performing the following steps:
 - a. Power down the server.
 - b. Take out the S8300D board.
You will require special cables to connect a keyboard and a VGA monitor.
 - c. Connect keyboard to the location labelled 'KBD'.
 - d. Connect monitor to the location labeled 'VGA'.
 - e. Power up the server.
 - f. Press the **F2** key to enter the BIOS setup.
2. Change the boot device by performing the following steps:
 - a. Press the **Right Arrow** key until **Boot** is selected at the top.
 - b. Press the **Down Arrow** until **Hard drive** is selected.
 - c. Press the **+** key until **Hard drive** is at the top of the list.
 - d. Press the **F10** key to save the changes and exit the BIOS setup.
3. Enter a password by performing the following steps:
 - a. Press the **Right Arrow** key until **Security** is selected at the top.
 - b. Press the **Down Arrow** key to select **Set Supervisor Password**.
 - c. Press the **Enter** key.
 - d. Type the password.
 - e. Type the same password to confirm.

- f. Press the **F10** key to save the changes.
The server will reboot.
-

Avaya port matrix

Port summary

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

Security port matrix for Virtual Server Platform on Domain 0

	Ports	Network/ Application Protocol	Optionally Enabled/ Disabled?	Default Port State	Column Descriptions
Ingress					Ingress -- data flows coming into the product. Egress -- data flows leaving the product. Port(s) – Logical number(s) at OSI layer-4. Valid values are in the range 0 – 65535. Network / Application Protocol – Top layer protocol, that is, RTP, HTTP, etc. Optionally Enabled/Disabled – indicates whether customers can enable or disable a layer-4 port changing its default port setting. Valid value is 'Yes' or 'No'. Default Port State: Valid Values include: Open, Closed, Filtered or N/A
1	1	ICMP	No	Open	
2	22	UDP/SSH	No	Open	
3	22	TCP/SSH	No	Open	
4	80	UDP/HTTP	No	Open	
5	80	TCP/HTTP	No	Open	
6	389	UDP/LDAP	No	Open	
7	389	TCP/LDAP	No	Open	
8	636	UDP/LDAPS	No	Open	
9	636	TCP/LDAPS	No	Open	
10	6659	TCP	No	Open	
11	6660	TCP	No	Open	
Egress					
1	All		No	Open	

 **Note:**

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

Security port matrix for Virtual Server Platform on CDom

	Ports	Network/ Application Protocol	Optionally Enabled/ Disabled?	Default Port State	Column Descriptions
Ingress					Ingress -- data flows coming into the product.
1	1	ICMP	No	Open	

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



Note:

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

Chapter 7: Log harvest utility

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

Note:

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

Using the log harvest utility

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

Note:

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

Compressed file structure

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

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

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

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

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

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

Related topics:

[Using the log harvest utility](#) on page 114

Using the log harvest utility

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

 **Note:**

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

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

Chapter 8: Troubleshooting

Template DVD does not mount

The template DVD does not mount automatically.

Troubleshooting steps

-
1. Log in to the Console Domain as admin.
 2. Type `su -`
 3. Enter the root password.
 4. Run the following commands:
 - > `ssh dom0.vsp /opt/avaya/vsp/template/scripts/udomAttachCd`
 - > `mount /dev/xvde /cdrom/`
-

Checking RAID status

`raid_status` command

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

- s: Shows short RAID status information; is the default output form
- p: Displays physical disk drive data; can be used with -v and -s
- r: Returns 0 if server supports RAID

Example

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

Note:

In case of physical disk information, -s -p is the default form of output. Specifying -v -s options together will result in an invalid command.

Virtual machine has no connectivity outside after assigning dedicated NIC support

Troubleshooting steps through System Domain (Dom-0)

-
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 Web 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 Web Console.
-

General issues with the system and contacting 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 High Availability Failover

Cannot establish communication through crossover network interface

Troubleshooting steps

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

Local IP address provided

Troubleshooting steps

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

Standby first-boot sequence is not yet finished

Troubleshooting steps

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

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



Note:

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

Cluster nodes are not equal

Troubleshooting steps

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

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



Note:

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

A template is installed on remote node

Troubleshooting steps

A solution template is installed on the standby node.



Note:

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

Either delete the solution template from the standby node or reinstall System Platform on the standby node and retry configuration of High Availability Failover.

NICs are not active on both sides

Troubleshooting steps

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 High Availability 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 High Availability Failover

Different platform versions on cluster nodes

Troubleshooting steps

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

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

A template is installed on remote node

Troubleshooting steps

A solution template is installed on the standby node.



Note:

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

Delete the solution template from the standby node.

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

Troubleshooting steps

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

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

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

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

Related topics:

[High Availability Failover overview](#) on page 83

[Ping targets](#) on page 84

[Prerequisites for configuring High Availability Failover](#) on page 90

Cannot access the Web Console after starting High Availability 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 correct port for High Availability Failover.
-

Start LDAP service on System Domain (Dom-0)

Troubleshooting steps

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

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

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

System Platform Web Console not accessible

Troubleshooting steps

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

Restarting High Availability Failover after one node has failed

Troubleshooting steps

 **Note:**

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

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

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

-
1. Log in to the System Platform Web Console on the active node.
 2. Click **Server Management** > **Failover**.
 3. Click **Stop Failover Mode** and confirm the warning that is displayed.
System Platform Web Console redirects to the Reboot page and after a few minutes redirects to the Login page.
 4. Log in again to the System Platform Web Console on the active node.
 5. Click **Server Management** > **Failover**.
 6. Click **Remove Failover** and confirm the warning that is displayed.
 7. Click **Configure Failover**.
 8. On the Configure failover page, enter the appropriate information to configure High Availability Failover.
 9. Click **Create**.
 10. After the system completes creation of the High Availability Failover configuration, click **Start Failover Mode** and confirm the warning that is displayed.
System Platform Web Console redirects to the Reboot page and after a few minutes redirects to the Login page.
 11. Log in to the System Platform Web Console.
 12. Click **Server Management** > **Failover**.

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



Tip:

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

Related topics:

[Configure Failover field descriptions](#) on page 91

Re-enabling failed standby node to High Availability Failover

Related topics:

[System Platform backup](#) on page 59

[Re-enabling failed preferred node to High Availability Failover](#) on page 127

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 with System 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

Related topics:

[System Platform backup](#) on page 59

[Re-enabling failed standby node to High Availability Failover](#) on page 126

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.

Multiple reinstallations can result in an out of memory error

If a pre-installation Web application is used to install a template and the template is reinstalled by deleting and installing it multiple times, an out of permanent generation memory space (PermGen) error can occur.

Troubleshooting steps

Perform the troubleshooting steps given here to ensure that a PermGen error does not occur.

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

Chapter 9: Fault detection and alarming

Hardware fault detection and alarming

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

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

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

```
[root@mesaverdel 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
Storage Service EventID: 2299	Bad PHY or physical connection
Storage Service EventID: 2307	Bad block table is full. Unable to log block

Message	Note
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 HP DL360 G6

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

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

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

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

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

Message	Note
Physical drive failed: <location> of <controller>	<location> <ul style="list-style-type: none"> • Port [Number] • Port [Type][Number] Box [Number], where Type = I for internal, E for external <controller> <ul style="list-style-type: none"> • Embedded Array Controller • Array Controller in slot [Number] • Array Controller in slot [unknown] For example: Physical drive failed: Port 1I Box 1 Bay 3 of Embedded Array Controller
Physical Drive Status Change: <location> of <controller>. Status is now <status>	<location> <ul style="list-style-type: none"> • Port [Number] • Slot [Number] Port [Type][Number] Box [Number], where Type = I for internal, E for external <controller> <ul style="list-style-type: none"> • Embedded Array Controller • Array Controller in slot [Number] • Array Controller in slot [unknown] <status> <ul style="list-style-type: none"> • OK • Failed • Unconfigured • Interim Recovery • Ready For Rebuild • Rebuilding • Wrong Physical Drive Replaced

Message	Note
	<ul style="list-style-type: none"> • Physical Drive Not Properly Connected • Hardware Overheating • Hardware Overheated • Expanding • Not Available • Queued For Expansion • Unknown <p>For example: Physical Drive Status Change: Slot 0 Port 1I Box 1 Bay 3. Status is now Failed</p>
<p>Logical drive [Number] of <controller>, has changed from <old status> to <new status></p>	<p><controller></p> <ul style="list-style-type: none"> • Embedded Array Controller • Array Controller in slot [Number] • Array Controller in slot [unknown] <p><status></p> <ul style="list-style-type: none"> • OK • Failed • Unconfigured • Interim Recovery • Ready For Rebuild • Rebuilding • Wrong Physical Drive Replaced • Physical Drive Not Properly Connected • Hardware Overheating • Hardware Overheated • Expanding • Not Available • Queued For Expansion • Unknown <p>For example: Logical drive 1 of Embedded Array Controller, has changed from status Interim Recovery to Failed</p>

Message	Note
<p>Logical drive [Number] of <controller>, is in a FAILED state but has one or more drive replacements and is ready to go to OK. However, this will not happen until an Accepted Media Exchange command is issued to the logical drive.</p>	<p><controller></p> <ul style="list-style-type: none"> • Embedded Array Controller • Array Controller in slot [Number] • Array Controller in slot [unknown] <p>For example: Logical drive 1 of Embedded Array Controller, is in a FAILED state but has one or more drive replacements and is ready to go to OK. However, this will not happen until an Accepted Media Exchange command is issued to the logical drive.</p>
<p>Logical drive [Number] of <controller>:I/O request fatal error.</p>	<p><controller></p> <ul style="list-style-type: none"> • Embedded Array Controller • Array Controller in slot [Number] • Array Controller in slot [unknown] <p>For example: Logical drive 1 of Embedded Array Controller: I/O request fatal error.</p>
<p>Logical Drive Status Change: Slot [Number], Drive [Number]. Status is now <status></p>	<p><status></p> <ul style="list-style-type: none"> • OK • Failed • Unconfigured • Interim Recovery • Ready For Rebuild • Rebuilding • Wrong Physical Drive Replaced • Physical Drive Not Properly Connected • Hardware Overheating • Hardware Overheated • Expanding • Not Available • Queued For Expansion • Unknown <p>For example: Logical Drive Status Change: Slot 0, Drive: 1. Status is now Interim Recovery.</p>

Refer to the HP ProLiant Servers Troubleshooting Guide at <http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c00300504/c00300504.pdf> for more information on troubleshooting and fault resolution.

For 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.

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

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

For S8300D

System Platform does not monitor hardware on the S8300D server.

General software faults

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

Alarm text	Problem/Action
Backup archive <archive> could not be sent on server <server>	Verify that SFTP is enabled on the server <server>. Log in to the System Platform Management Console. Click Server Management > Backup/Restore . Click Backup . Select SFTP from the Backup Method list. Verify that the SFTP Directory and SFTP Username are valid on <server>. Re-enter the SFTP Password. Check the details in /var/log/vsp/vsp-all.log.
Backup archive <archive> could not be sent on mail <email>	Verify that <email> is a valid email address that is currently able to accept email. Check the details in /var/log/vsp/vsp-all.log.
Restore of archive file <archive> failed.	Check the details in /vspdata/backup/backup.log log file.

In the “Alarm text” and “Problem/Action” columns:

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

Lifecycle manager faults

System Platform has a lifecycle manager that monitors the health of any virtual machines that were installed as part of a product template. An application in the virtual machine is expected to provide a periodic heartbeat. If this heartbeat is missed for a number of periods, the lifecycle manager will reboot the virtual machine. If the lifecycle manager does not see heartbeats after a reboot for a number of consecutive reboots, the lifecycle manager 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.

Alarm text	Problem/Action
VSP Virtual system <vm> shutdown as the result of sanity heartbeat failures	Check the virtual system log to see why sanity heartbeat failed.

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

Performance faults

Alarm text	Problem/Action
VSP High CPU Usage detected for <vm>	Check <vm> 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> 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 .

Alarm text	Problem/Action
	<p> Note: If unable to log in to System Platform Management Console, use the <code>xm reboot</code> command while logged in to dom0.</p>
VSP High Webconsole open files	<p>Log in to the System Platform Management Console. Click Virtual Machine Management > Manage. Click the cdom link. Click Reboot.</p> <p> Note: If unable to log in to System Platform Management Console, use the <code>xm reboot</code> command while logged in to dom0.</p>
VSP High SAL Agent heap usage	<p>Log in to the System Platform Management Console. Click Virtual Machine Management > Manage. Click the cdom link. Click Reboot.</p> <p> Note: If unable to log in to System Platform Management Console, use the <code>xm reboot</code> command while logged in to dom0.</p>
VSP High SAL Agent permgen usage	<p>Log in to the System Platform Management Console. Click Virtual Machine Management > Manage. Click the cdom link. Click Reboot.</p> <p> Note: If unable to log in to System Platform Management Console, use the <code>xm reboot</code> command while logged in to dom0.</p>
High Memory Usage in Domain-0	Check Memory Usage in Domain-0.
High Memory Usage in cdom	Check Memory Usage in cdom.

In the “Alarm text” and “Problem/Action” columns:

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

High Availability Failover faults

Alarm text	Problem/Action
VSP Webconsole encountered problem while retrieving status of failover.	Check the details in <code>/var/log/vsp/vspha.log</code> log file in dom0.
VSP Webconsole encountered problem while synchronising services to secondary node.	Check the details in <code>/var/log/vsp/vspha.log</code> log file in dom0.
VSP Webconsole encountered problem while removing template virtual machines from failover.	Check the details in <code>/var/log/vsp/vspha.log</code> log file in dom0.
VSP Webconsole encountered problem while adding template virtual machines into failover.	Check the details in <code>/var/log/vsp/vspha.log</code> log file in dom0.
VSP Webconsole encountered problem while upgrading console virtual machine.	Check the details in <code>/var/log/vsp/vspha.log</code> log file in dom0.
Not able to read machine hardware state; error executing IPMI command: <command> (raised on <hostname>)	Check the details in <code>/var/log/vsp/vspha.log</code> 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 <code>/var/log/vsp/vspha.log</code> and <code>/var/log/vsp/ha-log</code> for possible causes
Start HA failed: <details> (raised on <hostname>)	See <code>/var/log/vsp/vspha.log</code> and <code>/var/log/vsp/ha-log</code> for possible causes
Stop HA failed: <details> (raised on <hostname>)	See <code>/var/log/vsp/vspha.log</code> and <code>/var/log/vsp/ha-log</code> for possible causes
HA Failover failed: <details> (raised on <hostname>)	See <code>/var/log/vsp/vspha.log</code> and <code>/var/log/vsp/ha-log</code> for possible causes
Crossover connection between the machines is broken (raised on <hostname>)	Check the crossover network connection between the machines

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

In the “Alarm text” column:

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

Appendix A: Changing VLAN ID

-
1. Log in to System Platform System Domain as advanced administrator.
 2. Type `change vlan new_vlan_number`
-

Example

`change vlan -?` shows the available options as explained below:

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

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

```
change vlan -l
```

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

```
change vlan new_vlan_id
```

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

Appendix B: Errors encountered while downloading files from PLDS

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

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

To resolve these errors, check or initialize the proxy settings, if the errors suggest to do so. You may also contact Avaya Partners for support.

Errors encountered while downloading files from PLDS

Index

A

active server	
manually changing to standby	94
administrator user role	71
advanced administrator user role	71
Alarm Configuration page	
field descriptions	47
alarms	
configuring	46
System Platform	45
ASG	80
authenticating System Platform users	77
authentication file	80 , 81
installing	81
uploading	81

B

backing up	
System Platform and solution template	60
backup	
about	59
scheduling	61
viewing history	62
backup method	62
Backup page	
field descriptions	62
bonding interface	
adding	42
deleting	42

C

CD	
ejecting from System Platform server	56
certificate management	48
Certificate Management page	
field descriptions	49
changing VLAN ID	143
command line login	
Console Domain	97
System Domain	97
configuration	
restoring for System Platform	64
Configure Failover page	

field descriptions	91
configuring security	57
Console Domain	
command line login	97
create users	72

D

date	
configuring	32
Date/Time Configuration page	
field descriptions	34
delete users	72
disable booting from removable media	
BIOS changes	106
on S8300D	107
on S8510	106
on S8800	106
displaying currently set firewall rules on IPv4	98
displaying currently set firewall rules on IPv6	100
DVD	
does not mount automatically	115
ejecting from System Platform server	56

E

edit users	72
Eject CD/DVD page	56
email	62
enterprise LDAP	
authenticating System Platform users	77
configuring in System Platform	78
Enterprise LDAP page	
field descriptions	78
Ethernet Configuration page	
field descriptions	45
Ethernet interface settings	
configuring for System Platform	44

F

failover	
configuring	90
removing configuration	94
fault detection and alarming	

hardware fault	129
fault types	130 , 132 , 136 , 137
for HP DL360 G6	132
for S8300D	137
for S8510	130
for S8800	136
File Management page	56
files requiring SGID bits set on Console Domain	104
files requiring SGID bits set on System Domain	103
files requiring SUID bits set on Console Domain	104
files requiring SUID bits set on System Domain	103
firewall settings for IPv4	97
firewall settings for IPv6	99
folder	
deleting	56

G

general software faults	137
-------------------------------	---------------------

H

High Availability Failover	
and template configuration	89
configuring	90
data changes during disconnection	87
DRBD	85
faults	141
initial data synchronization	85
manually changing active server to standby	94
overview	83
ping targets	84
prerequisites for configuring	90
propagation of data changes	86
rebooting the system	66
removing configuration	94
requirements	89
shutting down the system	67
split-brain resolution	88
starting	93
stop and start of	92
stopping	93

I

installing Linuxshield on Console Domain	102
installing Linuxshield on System Domain	102
IP forwarding	
disabling	12
enabling	12

L

LDAP password	
changing	79
legal notices	2
License Management page	
field descriptions	50
licenses	
managing	50
LinuxShield virus scan	101
Local Management page	
field descriptions	76
log files	
viewing	30
log harvest utility	113
log retention	
about	36
configuring parameters	36
log severity levels	
about	35
configuring	36
log viewer	29
Log Viewer page	
field descriptions	30
Logging Configuration page	
field descriptions	36
logging IP packets blocked by firewall on IPv4 ...	98 , 100

M

managing System Platform users	72
--------------------------------------	--------------------

N

Network Configuration page	
field descriptions	39
network settings	
configuring for System Platform	38
notices, legal	2
NTP server	
removing	34
synchronizing with	31

P

password	
changing	80
Patch Detail page	
field descriptions	28
Patch List page	

field descriptions	27	selecting System Platform certificate	49
patches		server	
downloading	23	manually changing active to standby	94
installing	25	Server Reboot/Shutdown page	
removing	25	field descriptions	68
performance statistics	53–55	services port	
exporting	55	accessing System Platform through	12
viewing	54	SFTP	62
Performance Statistics page		shutting down	
field descriptions	55	System Platform server	67
PLDS		shutting down whole High Availability Failover system ...	67
errors encountered while downloading files	145	software fault detection and alarming	
port summary	108	lifecycle manager faults	138
proxy		performance faults	139
configuring	24	solution template	15, 21, 89
		and High Availability Failover	89
R		deleting	21
re-enabling failed preferred node to HA	127	starting firewall rules on IPv4	98
Re-enabling failed standby node to HA	126	starting firewall rules on IPv6	100
rebooting		static route	
System Platform server	66	adding	42
virtual machine	16	deleting	43
rebooting whole High Availability Failover system	66	modifying	43
requirements		Static Route Configuration page	
for High Availability Failover	89	field descriptions	44
restore		statistics	
viewing history	65	exporting	55
Restore page		viewing	54
field descriptions	65	stopping firewall rules on IPv4	97
restoring System Platform configuration information	64	stopping firewall rules on IPv6	99
RRDtool	53	stopping logging of IP packets blocked by firewall on IPv4	99
		99
S		stopping logging of IP packets blocked by firewall on IPv6	101
SAL Gateway		system	
about	51	configuring	37
configuring	52	System Configuration page	
launching management portal	52	configuring	37
SAL Gateway Management page		field descriptions	38
button descriptions	53	System Domain	
Search Local and Remote Patch page		command line login	97
field descriptions	26	System Platform Web Console	
security configuration	57	accessing	13
Security Configuration page		overview	11
field descriptions	58		
security port matrix		T	
for Virtual Server Platform on CDom	109	template	
for Virtual Server Platform on Domain 0	109	and High Availability Failover	89
selecting enterprise LDAP certificate	49	time	

configuring	32
time server	
removing	34
troubleshooting	
a template is installed on remote node	119 , 121
active server fails	122
cannot access System Platform Web Console after starting High Availability Failover	122
cannot establish communication through crossover network interface	118
cannot establish High Availability network interface	120
checking RAID status	115
cluster nodes are not equal	119
data switch fails	122
different platform versions on cluster nodes	120
DVD does not mount	115
general issues with the system and contacting support	117
heartbeat link fails	123
High Availability Failover does not work	123
local IP address provided	118
multiple reinstallations can result in an out of memory error	127
NICs are not active on both sides	120
re-enabling failed preferred node to HA	127
Re-enabling failed standby node to HA	126
resources not started on either node and cannot access System Platform Web Console	121
restarting High Availability Failover after one node has failed	125
standby first-boot sequence is not yet finished	118
Start LDAP service on System Domain (Dom-0)	124

System Platform Web Console not accessible	124
virtual machine has no connectivity	116

U

user administration	
overview	71
users	
creating in System Platform	74
deleting in System Platform	76
modifying in System Platform	75
roles	71
using the log harvest utility	114

V

Virtual Machine Configuration Parameters page	
field descriptions	18
Virtual Machine List page	
field descriptions	17
virtual machines	
shutting down	16
viewing	15

W

Web Console	
accessing	13
Web License Manager	
about	50
launching	50
WebLM	
about	50
launching	50