Installing and Upgrading Avaya Aura™ System Manager

Beta Release 5.2
November 2009

Notice

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

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

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

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site: http://www.avaya.com/support

Licenses

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

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/ThirdPartyLicense/

Preventing toll fraud

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

Avaya fraud intervention

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

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

Trademarks

Avaya, the Avaya logo, Avaya Aura™ System Manager are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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

Contact Avaya Support

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

Contents

Chapter 1: System Manager - installation requirements

Introduction

The System Manager Template is packaged and delivered in a gunzip file. This template contains Red Hat Enterprise Linux 5.3 and System Manager installed on RHEL 5.3. Installing the System Manager virtual appliance requires you to perform the following steps

1. Install System Platform
2. Install the System Manager virtual appliance on System Platform.

Hardware requirements

System Manager is to be installed on either an Avaya S8510 server or an Avaya S8800 server, depending on what was ordered. These servers arrive at the customer's site with all the required components and memory. Prior to installing System Manager on the server you have to install System Platform product on the hardware.

Chapter 2: Checklists and worksheets

System Manager installation checklist

#	Action	Notes	✔
1	Download the System Platform Installer ISO image & applicable patch from the Avaya PLDS Web site.	Verify that the md5sum for the downloaded ISO matches the number mentioned on the PLDS site.	
2	Download the System Manager template present in the form of a zipped file from PLDS & the supporting ovf and backup plugin.	Verify that the md5sum for the downloaded template matches the number mentioned on the PLDS site.	
3	Set up a DVD or USB flash drive to perform the System Platform installation from a DVD or USB flash drive.	See *Installing System Platform* guide to deploy the System Platform product on the hardware.	
4	Deploy the System Manager template on the System Platform by following the installation procedure mentioned in this doc.		

System Manager information worksheet

The System Manager template deployment using the System Platform Console requires you to fill in several fields. Having the information available at the time of installation expedite the System Manager deployment and ensures accuracy. Print out the following tables and work with your network administrator to fill in the appropriate value for each field displayed in the tables.

For the System Manager Virtual Appliance

Field	Value	Notes
IP address		Enter the IP address that is to be assigned to the System Manager virtual appliance on System Platform.
Short Hostname		Enter the short host name for the System Manager.
Non-root User		This is an optional field. A non-root user ID to be entered if you want to do the install using a non-root ID.

For the Network Configurations

Field	Value	Notes
Domain Name		Enter the domain name for your setup. For example: production.mydomain.com
Gateway Address		Enter the IP address of the server that has been set up as the gateway in your enterprise environment.
Network Mask		Enter the network mask value
DNS		Enter the IP address of the Domain Name Server.

Chapter 3: Installing System Manager Template

Downloading System Manager from PLDS

1. Type `http://plds.avaya.com` in your web browser to open the Product Licensing and Delivery System Web site.
2. Click **Log in with my password**.
3. Enter your login and password details
   Your login id is your e-mail address.
4. Click **Log In**.
5. On the Home page, expand Asset Mgmt and click **View Downloads**.
6. On the Downloads page, enter your company's name in the **%Company** field.
7. In the **Application drop down** menu, choose “System Manager”.
8. Click **Search Downloads**.
9. From the Software Downloads list, locate the following files: `System Manager 5.2 BETA template (gzip file)`, `System Manager 5.2 BETA backup script file (sh file)`, and `System Manager 5.2 BETA template descriptor (ovf file)` and download them.
10. On the About the Download Manager page, click **Click to download your file now**.
11. If you receive an error message, click on the message, install Active X, and continue with the download.
12. When the security warning displays, click **Install**.
    When the install is complete, Product Licensing and Delivery System (PLDS) displays the downloads again with a checkmark next to the download which is successfully completed.

Installing the System Manager Template

When you install System Manager on a virtual machine using the System Manager Template, the System Manager Template installs Linux Operating System and System Manager.

Prerequisites

Use the System Platform ISO file `System Platform 1.1 build 8 ISO installer for Avaya Aura™ System Manager 5.2` and patch file `System Platform 1.1 build 8 ISO Patch RPM` for installing System Platform.

Note:

See the *Installing System Platform* guide on the Avaya Support Web site for information on the installation of System Platform.

1. Enter the `https://<IPAddress>/webconsole` URL in the web browser to log in to the C-dom web console, where <IPAddress> is the IP address of C-dom.
2. Log in to the C-dom web console with the administrator credentials made available at the time of the System Platform installation.
3. On the System Platform console, click **Virtual Machine Management** > **Solution Template** in the left navigation pane.
4. On the Search Local and Remote Template page, select an appropriate installation mode.

   Note:

   The files downloaded from the PLDS Web site can be stored on different locations. The selection of a location depends on the mode using which you want to deploy the System Manager template. See the Selecting a template to install section in Chapter 8 of the *Installing System Platform* guide.

5. Click **Search** to find the installation OVF file.
6. From the **Select Template** drop-down field, click the appropriate installation OVF file and click **Select**.
7. On the Templates Details page, click **Install**.
8. Click **Save**.
9. On the Templates Details page, in the **IP address of the SMGR** field enter the IP address of the virtual machine on which you are installing System Manager.

   This IP address should be different from the IP address of the C-dom and Dom–0 virtual machines.

10. In the **SMGR short hostname** field, enter the short host name of the virtual machine.
11. In the **SMGR domain** field, enter an appropriate domain name based on your enterprise environment.

    For example you can enter a domain name in the form of mydomain.com.
12. In the **Gateway address** field, enter the IP address of the computer configured as gateway in your enterprise environment.
13. In the **Network mask** field, enter the network mask value.
14. In the **DNS** field, enter an the IP address of the domain name server.
15. In the **Non-root User** field, enter the non root user name. This is an optional field.
16. Click **Install**.

    Enter the `https://<IPAddress>/SMGR` URL in the web browser to access the System Manager, where<IPAddress> is the IP address of the System Manager virtual appliance.

Related topics:

Default Credentials on page 11

Default Credentials

Accessing System Manager Virtual Appliance

To login on the command prompt of the System Manager virtual appliance, you need to ssh to the IP address of the virtual appliance. Use root as the login ID and root01 as password. It is advisable to change the password on the initial login.

Accessing System Manager Common Console

To access System Manager Common Console, enter the `https://<IPAddress>/SMGR` URL in the web browser where <IPAddress> is the IP address of the System Manager virtual appliance. The default user name and password for accessing the System Manager common console is admin and admin123. You must change the default password on the initial login.

Chapter 4: System Manager Upgrades

Upgrade the System Manager Template

The upgrade for System Manager is available from previous load to the current load of System Manager Release 5.2 and as release to release upgrade from System Manager Release 1.0 to System Manger Release 5.2.

Related topics:

[Performing load to load upgrade](#) on page 13
[Performing release to release upgrade](#) on page 14

Performing load to load upgrade

1. Download the latest System Manager Template files from the PLDS Web site.
2. Enter the `https://<IPAddress>/webconsole` URL in the web browser to log in to the C-dom web console, where <IPAddress> is the IP address of C-dom.
3. Log in to the C-dom web console with the administrator credentials made available at the time of the System Platform installation.
4. On the System Platform console, click **Virtual Machine Management** > **Solution Template** in the left navigation pane.
5. On the Search Local and Remote Template page, select an appropriate installation mode.

   Note:
   The files downloaded from the PLDS Web site can be stored on different locations. The selection of a location depends on the mode using which you want to deploy the System Manager template. See the Selecting a template to install section in Chapter 8 of the *Installing System Platform* guide.

6. Click **Upgrade**.
7. On the Select Template page, click the appropriate upgrade OVF file and click **Select**.
8. Click **Upgrade**.

9. On the Template Network Configuration page, verify network configuration and click **Save**.
10. Enter the non root user information in the **Non-root user** field for performing the non root configuration. This field is an optional field.
11. Click **Upgrade**.

Performing release to release upgrade

Prerequisites

Before you perform the upgrade procedure, you must keep a backup of the installed System Manager Template.

Note:

Upgrades from System Manager R1.0 to System Manager Release 5.2 will not be supported until January 2010.

1. Download the latest System Manager Template files from the PLDS Web site.
2. Go to the `/opt/vsp` directory from the command prompt.
3. Type the `sh BackupSMGR.sh` command at the command prompt to run the BackupSMGR.sh script file on your release 1.0 system.
4. Copy the `/tmp/MgmtBackup_1.0.*.zip` file to some external machine if upgrading on the same machine.
5. Install System Platform.

   See the *installing System Platform* guide on the Avaya Support Web site for information on the installation of System Platform.
6. Install System Manager Template.

   See the Installing System Manager section in this guide for more information on the installation of System Manager Template.

   Note:

   Since this is an upgrade, you are required to use same Hostname and IPAddress for System Manager Template machine. If you are using different machine for SP installation, switch off the R1.0 machine.

7. Copy the backed up `MgmtBackup_1.0.*.zip` file in Step 6 to `/tmp/` directory in the Release 5.2 template.
8. Run the `RestoreSMGR.sh` script file present at `/opt/vsp` directory from the command prompt using the `sh RestoreSMGR.sh` command.

Chapter 5: Switching to Cold Standby Server

Cold Standby server as the failover server for System Manager

A cold standby System Manager server acts as a failover server when the main server running System Manager fails. This section covers the Cold Standby failover process for the System Manager application deployed on System Platform. This section explains the process with an example of having 2 nodes, one being active and the other being the cold standby node. The section refers to Node A as the primary server that is active. Node B is the cold standby server. The cold standby procedure is to be executed in the scenario of Node A going down and the application is to be switched to Node B.

Setting up a Cold Standby server

Prerequisites

1. Primary (Node A) and Cold Standby (Node B) servers must have the same IP address and hostname. It is assumed that when the primary server is running, the Standby server is turned off.
2. The System Manager 5.2 template is deployed on the Primary and Standby server using the install procedure mentioned in the Avaya Aura™ System Manager Installation Guide.
3. The system date must be identical on both the servers.
4. Using the Remote backup facility of System Manager Element Manager you must take regular backup of System Manager database of the Primary Server. Taking Regular backup of System Manager database ensures the availability of latest data that you need for a cold standby procedure in case the Primary sever fails. Create the backup of the database on a remote computer or on an external storage device (for example, Tape drive, DVD, and so on). When the Primary server fails, use the backup to restore the database on the Standby server. The section “Scheduling a Data Backup” mentions the steps for scheduling a backup on the System Manager Node.

1. Confirm that the Primary server (Node A) is turned off.
2. Turn on the Standby server (Node B).
3. Restore the last database backup that you took from the Primary sever on Standby server using the backup & restore utility of System Manager Element Manager provided with System Manger. The section “Restoring a Backup” mentions the steps for performing a restore of the backup on the System Manager Node.

   After restoration, System Manager on the Standby server (Node B) becomes available for operations.

Related topics:

Restoring a backup on page 18
Creating backup of application data on page 19

Restoring a backup

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Backup and Restore** .
3. Click **Restore**.
4. On the Restore page, perform one of the following steps:
   - To restore data from a local backup
     i. Click **Local** option.
     ii. Enter the back up file name in the **File name** field.
   - To restore data from a remote backup
     i. Click **Remote** option.
     ii. Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
5. Click **Restore**.

After the successful restore operation, the user who initiated the restore is logged out of the System Manager console.

Creating backup of application data

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Backup and Restore** .
3. Click **Backup**.
4. On the Backup page, perform one of the following steps:
   - To back up data to a local drive, do the following:
     i. Click **Local** option.
     ii. In the **File name** field, enter the name of the backup file field that you want to create.
   - To back up data to a remote location, do the following:
     i. Click **Remote** option.
     ii. Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
5. Click **Now**.

If the backup is successful, the Backup and Restore page displays a message Backup created successfully!!.

Chapter 6: Removing the System Manager Template

1. Enter the `https://<IPAddress>/webconsole` URL in the web browser to log in to the C-dom web console, where <IPAddress> is the IP address of C-dom.
2. Log in to the C-dom web console with the administrator credentials made available at the time of the System Platform installation.
3. On the System Platform console, click **Virtual Machine Management** > **Solution Template** in the left navigation pane.
4. Click **Delete Installed Template** to delete the System Manager Template.

Index