Upgrading Avaya Aura® System Manager to Release 7.0.1

Release 7.0.1
Issue 2
August 2016

Notice

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

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Aura® System Manager from earlier releases to Release 7.0.1 on Avaya-provided server in the Avaya Aura® Virtualized Appliance offer and customer Virtualized Environment. This document includes upgrading checklists and procedures.

This document is intended for people who perform System Manager upgrades.

Change history

The following changes have been made to this document since the last issue:

Issue	Date	Summary of changes
2.0	May 2016	• Added procedures for installing the Release 7.0.1 feature pack on Release 7.0. • Added procedures for the following in VM Management: - Enabling and disabling SSH on Appliance Virtualization Platform. - Changing network settings that includes, changing VLAN ID, NIC speed, and NIC team and unteaming for an Appliance Virtualization Platform host. - Restarting the Appliance Virtualization Platform host. - Shutting down the Appliance Virtualization Platform host. - Viewing the job history of all operations that are performed on VM Management. - Updating the license status of hosts and virtual machines state. - Removing the Appliance Virtualization Platform patch. - Changing the IP address and default gateway of the host. - Validating the certificates. • Cleaning up the current pending or pause state of applications during upgrade.

Issue	Date	Summary of changes
		• Added procedure to upgrade System Manager directly to Release 7.0.1 by using the System Manager upgrade manager on the Solution Deployment Manager client. • Added support for Dell™ PowerEdge™ R630 and HP ProLiant DL360 G9 common servers.

Warranty

Avaya provides a 90-day limited warranty on the System Manager software. For detailed terms and conditions, see the sales agreement or other applicable documentation. Additionally, for the standard warranty description of Avaya and the details of support, see **Help & Policies** > **Policies & Legal** > **Maintenance and Warranty Information** on the Avaya Support website at http://support.avaya.com. For additional information, see **Help & Policies** > **Policies & Legal** > **License Terms**.

For more details on the hardware maintenance for supported products, see http://portal.avaya.com/ptlWeb/services/SV0452.

Chapter 2: Upgrade overview and considerations

Upgrade overview

The document provides the procedures for upgrading Avaya Aura® System Manager from earlier releases to System Manager Release 7.0.1 on the following:

- VMware 5.5 in Avaya-provided appliance
- VMware 5.0, 5.1, 5.5, or 6.0 in customer-provided Virtualized Environment

Depending on the System Manager release, use one of the following methods to upgrade System Manager:

- Network Routing Policy (NRP) export and import utility: To upgrade System Manager from Release 5.2.x, on the 5.2.x system, export the routing data by using the NRP export utility and then import the routing data using the NRP import utility to the Release 7.0.1 system.
- Data migration utility: Use the data migration utility to migrate the System Manager data from Release 6.x to 7.x:
  - On VMware in customer-provided Virtualized Environment by using vSphere client.
  - From System Platform to Release 7.0.1 running on Appliance Virtualization Platform on Avaya-provided server by using the Solution Deployment Manager client.

Note:

Install the service pack or feature pack only after you run the data migration utility on System Manager Release 7.0.

Upgrades

You must perform the upgrade operation when System Manager Release 6.x is running on customer-provided VMware ESXi 5.5 in Virtualized Environment.

Migration

You must perform the migration process in the following scenarios:

- All System Manager releases earlier than Release 7.0 running on System Platform.
- Change to System Manager Release 7.0.1 supported servers.

  For the list of Release 7.0.1 supported servers, see Supported servers.
- Change to the VMware ESXi 5.5 or 6.0 host.

- Change the operating system to CentOS 6.5.

Overview

You can migrate the data from the following System Manager releases to System Manager Release 7.0.1:

- 6.0, 6.0 SP1, or SP2
- 6.1, 6.1 SP1.1, SP2, SP3, SP4, SP5, SP6, SP7, or SP8
- 6.2, 6.2 SP1, SP2, SP3, or SP4
- 6.3.x
- For information about migrating the backup data from System Manager Release 6.x running on System Platform, see Upgrading to System Manager on Avaya-provided server.
- For information about migrating the backup data from System Manager Release 6.x by using the Solution Deployment Manager client, see Upgrading System Manager by using the Solution Deployment Manager client.
- For information about upgrading System Manager from 6.3.x on VMware in Virtualized Environment, see Upgrading System Manager from VMware in Virtualized Environment.

Supported upgrade paths

The document provides upgrade procedures for the following paths to upgrade System Manager from releases earlier than Release 7.0 to System Manager Release 7.0.1 in Avaya-provided appliance environment and customer-provided Virtualized Environment:

From System Manager release	To System Manager Release 7.0.1 on VMware	
	Checklist	**Procedure**
5.2.x	Checklist for upgrades from System Manager Release 5.2.x on Avaya-provided server on page 61	Importing the data to System Manager Release 7.0.1 on page 69
6.0.x, 6.1.x, 6.2.x, or 6.3.x on System Platform	Checklist for upgrading from System Manager 6.x on page 39	Upgrading to System Manager Release 7.0.1 running on an Avaya-provided server on page 45
6.2.x on VMware	Checklist for upgrade from System Manager 6.x on page 49	Upgrading System Manager from Release 6.0, 6.1, 6.2, and 6.3 to

Table continues…

From System Manager release	To System Manager Release 7.0.1 on VMware	
	Checklist	**Procedure**
		Release 7.0.1 on VMware on page 53
6.3.2, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.3.8, 6.3.9. 6.3.10, 6.3.11, 6.3.12, 6.3.13, 6.3.14, or later on VMware with Geographic Redundancy	Checklist for upgrading System Manager Release 6.3.x in the Geographic Redundancy setup to Release 7.0.1 on page 55	Upgrading System Manager from Release 6.3.x in the Geographic Redundancy setup to Release 7.0.1 on page 57

Chapter 3: Planning and preconfiguration

Prerequisites

Serial Number	Prerequisite	Notes
1	Download the following software from the Avaya Support website at http://support.avaya.com: • The System Manager Release 7.0.1 OVA, `SMGR-7.0.0.0.16266-e55-43-29-II.ova` • The `Data_Migration_Utility_7.0.1.0_r96.bin` file • System Manager Release 7.0.1 bin file	
2	Verify that the existing server is compatible with System Manager Release 7.0.1. If the existing server is incompatible, change the server as instructed in the workflow described in this chapter.	Release 7.0.1 supports the following servers: • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7 • Dell™ PowerEdge™ R620 • HP ProLiant DL360p G8 • Dell™ PowerEdge™ R630 • HP ProLiant DL360 G9
3	Keep the following checklists: • The System Manager Release 7.0.1 installation checklist • Upgrade checklist	
4	Keep the following information handy to create a backup on the remote server: • IP address • Directory • User Name • Password	

Table continues…

Serial Number	Prerequisite	Notes
5	Record the number of users and custom roles in the current release of System Manager. After the upgrade, you require this data to verify if the system has successfully imported the users and roles from the earlier release to System Manager Release 7.0.1.	For more information, see Managing users and Managing roles in *Administering Avaya Aura® System Manager for Release 7.0.1*.

Upgrade worksheet

Use the following worksheet to record the data that you will need during the upgrade.

Serial Number	Field	Value	Notes
1	**IP address of external device for remote backup**		On the remote backup page of System Manager Web Console, enter the IP address of the remote server on which you saved the backup file.
2	**User Name and Password of the remote server**		To gain access to the backup file that is located on a remote server, enter the user name and the password for the account on the System Manager web console.
3	**System Manager command line interface credential**		Open an SSH session and enter `admin` as the user name and password.
4	**Root password of System Manager**		On CLI, to change to root, type the **`su -`** command.
5	**Path and the file name of the backup file on the remote server**		Enter the path and the file name of the backup file.

Supported servers

In the Avaya Aura® Virtualized Appliance model, Solution Deployment Manager supports the following servers for deployments and upgrades to Release 7.0.1:

- Dell™ PowerEdge™ R610
- HP ProLiant DL360 G7
- Dell™ PowerEdge™ R620
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G9

If you must change the server, use Dell™ PowerEdge™ R630 or HP ProLiant DL360 G9 to install Appliance Virtualization Platform and System Manager Release 7.0.1.

Server hardware and resources for VMware

VMware offers compatibility guides that list servers, system, I/O, storage, and backup compatibility with VMware infrastructure. For more information about VMware-certified compatibility guides and product interoperability matrices, see http://www.vmware.com/resources/guides.html.

Configuration tools and utilities

You must have the following tools and utilities for deploying and configuring System Manager open virtual application (OVA):

- Solution Deployment Manager client running on your computer
- A remote computer running the VMware vSphere Client
- A browser for accessing the System Manager web interface
- An SFTP client for Windows, for example WinSCP
- An SSH client, for example, PuTTy

Customer configuration data

Keep a copy of the license files for the Avaya Aura® products so you can replicate with the new Host ID after the OVA file installation.

The following table identifies the key customer configuration information that you must provide throughout the deployment and configuration process.

Important:

Password must be 8 to 256 alphanumeric characters and without white spaces.

	Required data	Value for the system	Example Value
Management (Out of Band Management) and Public network configuration Configure Public network details only when Out of Band Management is enabled. If Out of Band Management is not enabled, Public network configuration is optional.	IP address		172.16.1.10
	Netmask		255.255.0.0
	Gateway		172.16.1.1
	DNS Server IP address		172.16.1.2
	Short hostname		myhost. The host name must be a valid short name. **Note:** System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.
	Domain name		mydomain.com
	Default search list		mydomain.com
	NTP server		172.16.1.100
	Time zone		America/Denver
VFQDN **Note:** The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.	VFQDN short hostname		grsmgr
	VFQDN domain name		dev.com
SNMP Parameters	User Name Prefix		org
	Authentication Protocol Password		orgpassword
	Privacy Protocol Password		orgpassword
Backup Definition Parameters	See Backup Definition parameters		-

System Manager footprint hardware resource matrix

The following table describes the resource requirements to support different profiles for System Manager in Avaya-Appliance offer and customer Virtualized Environment.

Table 1: Avaya Appliance Virtualization Platform

VMware resource	Profile-1	Profile-2	Profile-3
vCPU Reserved	4	6	8
Minimum vCPU Speed	2290 MHz	2290 MHz	2290 MHz
Virtual RAM	9 GB	12 GB	18 GB
Virtual Hard Disk	105 GB	105 GB	250 GB
Number of users	Up to 35000 with up to 35 Branch Session Manager and 12 Session Manager	>35000 to 250000 with up to 250 Branch Session Manager and 12 Session Manager	>35000 to 250000 with up to 500 Branch Session Manager and 28 Session Manager
Common Server R1 support	Yes	No	No
Common Server R2 and R3 support	Yes	Yes	Yes

Table 2: Customer Virtualized Environment

VMware resource	Profile-1	Profile-2	Profile-3
vCPU Reserved	4	6	8
Minimum vCPU Speed	2290 MHz	2290 MHz	2290 MHz
CPU reservation	9160 MHz	13740 MHz	18320 MHz
Virtual RAM	9 GB	12 GB	18 GB
Memory reservation	9126 MB	12288 MB	18432 MB
Virtual Hard Disk	105 GB	105 GB	250 GB
Shared NICs	1	1	1
Number of users	Up to 35000 with up to 35 Branch Session Manager and 12 Session Manager	>35000 to 250000 with up to 250 Branch Session Manager and 12 Session Manager	>35000 to 250000 with up to 500 Branch Session Manager and 28 Session Manager

Related links

Adjusting the System Manager virtual machine properties on page 17

Adjusting the System Manager virtual machine properties

About this task

If the system encounters CPU resource limitations, the system displays a message similar to `Insufficient capacity on each physical CPU`. To correct the CPU limitation, you require to adjust the virtual machine properties.

If the CPU adjustments you make does not correct the virtual machine start up conditions, you must further reduce the CPU speed. Use the same procedure to reduce the values for other virtual machine resources.

Do not modify the resource settings, for example, remove the resources altogether. Modifying the allocated resources can have a direct impact on the performance, capacity, and stability of the System Manager virtual machine. To run the System Manager virtual machine at full capacity, the resource size requirements must be met; removing or greatly downsizing reservations could put the resource size requirement at risk.

Important:

Any deviation from the requirement is at your own risk.

Procedure

1. Right click on the virtual machine and select **Edit Settings…**.

   The system displays the Virtual Machine Properties dialog box.

2. Click the **Resources** tab.

   In the left pane, the system displays the details for CPU, memory, disk advanced CPU, and advanced memory.

3. Select CPU.

4. In the **Resource Allocation** area, in the **Reservation** field, perform one of the following to start the virtual machine:

   - Adjust the slider to the appropriate position.
   - Enter the exact value.

Software requirements

Avaya Aura® supports the following software versions:

- Avaya Aura® Virtualized Appliance offer: Appliance Virtualization Platform 7.0.x on a customized version of VMware® ESXi 5.5
- Customer-provided Virtualized Environment offer: Supports the following software versions:
  - VMware® vSphere ESXi 5.0
  - VMware® vSphere ESXi 5.1
  - VMware®vSphere ESXi 5.5

- VMware® vSphere ESXi 6.0
- VMware® vCenter Server 5.0
- VMware® vCenter Server 5.1
- VMware® vCenter Server 5.5
- VMware® vCenter Server 6.0

To view compatibility with other solution releases, see VMware Product Interoperability Matrix at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php.

Note:

Avaya Aura® Release 7.0 and later does not support ESXi releases earlier than 5.0.

Installing the Solution Deployment Manager client on your computer

About this task

In Avaya Aura® Virtualized Appliance offer, when the centralized Solution Deployment Manager on System Manager is unavailable, use the Solution Deployment Manager client to deploy the Avaya Aura® applications.

You can use the Solution Deployment Manager client to install software patches and hypervisor patches.

Use the Solution Deployment Manager client to deploy, upgrade, and update System Manager.

Note:

Click **Next** only once, and wait for the installer to load the next screen.

Before you begin

1. If an earlier version of the Solution Deployment Manager client is running on the computer, remove the older version from **Control Panel** > **Programs** > **Programs and Features**.

   If you are unable to uninstall, see *Uninstalling the Solution Deployment Manager client*.

2. Ensure that Windows 7, Windows 8.1 64-bit, or Windows 10 64-bit operating system is installed on the computer.

   Tip:

   On **Computer**, right-click properties, and ensure that Windows edition section displays the version of Windows operating system.

3. Ensure that at least 5 GB of disk space is available at the location where you want to install the client.

Tip:

Using the Windows file explorer, click **Computer**, and verify that the Hard Disk Drives section displays the available disk space available.

4. To avoid port conflict, stop any application server that is running on your computer.

   Tip:

   From the system tray, open the application service monitor, select the application server that you want to stop, and click **Stop**.

5. Ensure that the firewall allows the ports that are required to install the Solution Deployment Manager client installation and use the Solution Deployment Manager functionality.
6. Ensure that ports support Avaya Aura® 7.0.1 supported browsers.
7. Close all applications that are running on your computer.
8. Do not set CATALINA_HOME as environment variable on the computer where you install the Solution Deployment Manager client.

   Tip:

   On **Computer**, right-click properties, and perform the following:

   a. In the left navigation pane, click **Advanced system settings**.
   b. On the System Properties dialog box, click Advanced tab, and click **Environment Variables**.
   c. Verify the system variables.

9. Ensure that the computer on which the Solution Deployment Manager client is running is connected to the network.

   Operations that you perform might fail if the computer is not connected to the network.

Procedure

1. Download the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.zip` file from the Avaya PLDS website at https://plds.avaya.com/.

   On the Avaya PLDS website, at https://plds.avaya.com/, click **Support by Products** > **Downloads**, and provide the product **System Manager**, and version as **7.0.x**.

2. Copy the zip file, and extract to a location on your computer by using the WinZip application.

   You can also copy the zip file to your software library directory, for example, `c:/tmp/Aura`.

3. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.

4. On the Welcome page, click **Next**.
5. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.

6. On the Install Location page, perform one of the following:
   - To install the Solution Deployment Manager client in the system-defined folder, click **Restore Default Folder**.
   - To specify a different location for installation, click **Choose** and browse to an empty folder.
7. Click **Next**.
8. On the Preinstallation Summary page, review the information, and click **Next**.
9. On the User Input page, perform the following:
   a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.
   b. To change the default directory, in Select Location of Software Library Directory, click **Choose** and select a directory.

      The system saves the artifacts in the specified directory. During deployments, you can select the OVA file from the directory.
   c. In **Data Port No**, select the appropriate port from the range 1527 through 1627.
   d. In **Application Port No**, select the appropriate port from the range 443 through 543.
   e. **(Optional)** Click **Reset All to Default**.
10. On the Summary and Validation page, verify the product information and the system requirements.

    The system performs the feasibility checks, such as disk space and memory. If the requirements are not met, the system displays an error message. To continue with the installation, make the disk space, memory, and the ports available.
11. Click **Install**.
12. To exit the installer, on the Install Complete page, click **Done**.

    The installer creates a shortcut on the desktop.
13. To start the client, click the Solution Deployment Manager client icon,  .

Next steps

- Configure the laptop to get connected to the services port if you are using the services port to install.
- Connect the Solution Deployment Manager client to Appliance Virtualization Platform through the customer network or services port.

  For more information, see “Methods to connect Solution Deployment Manager client to Appliance Virtualization Platform”.

Accessing the Solution Deployment Manager client dashboard

About this task

Note:

If you perform deploy, upgrade, and update operations from the Solution Deployment Manager client, ignore the steps that instruct you to access System Manager Solution Deployment Manager and the related navigation links.

Procedure

To start the Solution Deployment Manager client, perform one of the following:

- Click **Start** > **All Programs** > **Avaya**, and click **SDM Client** > **Avaya SDM Client**.
- Click  .

Accessing Solution Deployment Manager

About this task

You require to start Solution Deployment Manager to deploy and upgrade virtual machines, and install service packs or patches.

Procedure

Perform one of the following:

- If System Manager is not already deployed, double-click the Solution Deployment Manager client.
- If System Manager is available, on the web console, click **Services** > **Solution Deployment Manager**.

Deploying the Utility Services OVA file

About this task

Use the procedure to create a virtual machine on the ESXi host, and deploy Utility Services OVA on the Avaya-provided server.

To deploy Utility Services, you can use Solution Deployment Manager from System Manager or the Solution Deployment Manager client, when System Manager is unavailable. Deploy Utility Services first, install the Release 7.0.1 feature pack, and then deploy all other applications one at a time.

Before you begin

- Complete the deployment checklist.

For information about the deployment checklist, see *Deploying Avaya Aura® applications from System Manager*.

- Add a location.
- Add Appliance Virtualization Platform or an ESXi host to the location.
- Download the required OVA file to System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click **New**.

   The system displays the VM Deployment section.
4. In the Select Location and Host section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Host**, select a host.
   c. In **Host FQDN**, type the virtual machine name.
5. In **Data Store**, select a data store.

   The page displays the capacity details.
6. Click **Next**.
7. In the Deploy OVA section, perform the following:
   a. In **Select Software Library**, select the local or remote library where the OVA file is available.

      If you are deploying the OVA from the Solution Deployment Manager client, you can use the default software library that is set during the client installation.
   b. In **Select OVAs**, select the OVA file that you want to deploy.
   c. In **Flexi Footprint**, select the footprint size that the application supports.
      - **S8300D**: Due to the limited resources available on S8300D, the only footprint option is minimal
      - **Default**: For all other server platforms.
8. Click **Next**.

   In Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to the application that you deploy.
9. In the Network Parameters section, ensure that the following fields are preconfigured:
   - **Public**
   - **Services**: Only for Utility Services

- **Out of Band Management**: Only if Out of Band Management is enabled

For more information, see “VM Deployment field descriptions”.

10. In the Configuration Parameters section, complete the fields.

    For more information about Configuration Parameters, see Network Parameters and Configuration Parameters field descriptions.

11. Click **Deploy**.
12. Click **Accept the license terms**.

    In the Hosts for Selected Location <location name> section, the system displays the deployment status in the **Current Action Status** column.

    The system displays the virtual machine on the VMs for Selected Location <location name> page.

13. To view details, click the **Status Details** link.

    For information about VM Management field descriptions, see *Deploying Avaya Aura® applications from System Manager*.

14. Install the Release 7.0.1 feature pack.
15. Reboot the Utility Services virtual machine.

Next steps

1. Deploy System Manager and install the Release 7.0.1 feature pack.
2. To activate the serviceability agent registration, reset the Utility Services virtual machine.
3. Deploy all other Avaya Aura® applications one at a time.

Related links

VM Deployment field descriptions on page 115
Network Parameters and Configuration Parameters field descriptions

Installing software patches

About this task

Use the procedure to install software patches, service packs, and feature packs that are entitled for an Avaya Aura® application, and commit the patches that you installed.

Before you begin

- Perform the preupgrade check.
- If you upgrade an application that was not deployed from Solution Deployment Manager:
  1. Select the virtual machine.
  2. To establish trust, click **More Actions** > **Re-establish Connection**.
  3. Click **Refresh VM**.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.

   Note:

   If an application is unreachable, the auto commit operation might fail and the Update Patch Status window displays a warning message. You must wait for some time, select the same patch in the Installed Patches section, and perform the commit operation again.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. Click **Save**.
11. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

    If the field displays , review the information on the Edit Upgrade Configuration page.
12. Click **Upgrade**.
13. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
14. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display .
15. To view the update status, click .

    The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.

    When the update is complete, the **Update status** and **Last Action Status** fields displays .
16. Click **Upgrade Actions** > **Installed Patches**.
17. On the Installed Patches page, in the Patch Operation section, click **Commit**.

The page displays all software patches that you can commit.

You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.

18. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

    You can schedule to commit the patch at a later time by using the **Schedule later** option.

19. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.

20. Ensure that **Update status** and **Last Action Status** fields display .

Chapter 4: Upgrading System Manager using the Solution Deployment Manager client

Upgrade overview

You can use the Solution Deployment Manager client to upgrade System Manager running releases earlier than 7.0. To upgrade System Manager 7.0 to 7.0.1, you can install the System Manager 7.0.1 bin file from the Solution Deployment Manager client.

Upgrading System Manager on a different server by using Solution Deployment Manager client

About this task

You can upgrade System Manager on the same server or a different server.

The procedure describes the steps to upgrade System Platform-based System Manager on a different server.

Before you begin

- Add a location.
- Install the Appliance Virtualization Platform host.
- Add the Appliance Virtualization Platform host from the VM Management page.
- Install the Solution Deployment Manager client.
- Obtain the following System Manager software:
  - OVA file, `SMGR-7.0.0.0.16266-e55-43-29-II.ova`
  - Data migration utility, `Data_Migration_Utility_7.0.1.0_r96.bin`
  - Release 7.0.1 bin file, `System_Manager_7.0.1.0_r701064859.bin`
- Create the System Manager backup and copy the file to the same computer where Solution Deployment Manager client is installed.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **VM Management**.
3. The system displays the Upgrade Elements page
4. **(Optional)** If System Manager element is not present, do the following:
   a. Click **Add Elements**, add the System Manager element and console domain information.
   b. Click **Save**.
5. If System Manager element is present, select the required element.
6. Click **Upgrade**.
7. **(Optional)** In , select the host.

   On the SMGR Upgrade dialog box, the system might preselect and disable .
8. Select the datastore on the host.

   The system populates the network parameters and configuration parameters from the System Platform-based virtual machine.
9. Click **Next**.
10. Select the tab.
11. To get the OVA file from , do the following:
    a. Click .
    b. In , enter the absolute path to the System Manager OVA file, and click .
12. To get the OVA file from , do the following:
    a. Click .
    b. In , select the System Manager OVA file.
13. To get the OVA file from a location on the computer, do the following:
    a. Click and select the required OVA file.
    b. Click .
14. Select , if required.
15. Select the flexi footprint.
16. Click the tab, do one of the following:
    - For the URL option, click , and provide the absolute path to the latest data migration utility file.
    - For SW Library, click , and select the latest data migration utility file.
    - For Browse, click , and select the latest data migration utility file.

17. Click the tab and do one of the following:
    - For URL, click , and provide the absolute path to the latest service or feature pack.
    - For SW Library, click , and select the latest service or feature pack.
    - For Browse, click , and select the latest service or feature pack.

    For upgrades from System Manager 6.3.14 or earlier, the bin patch file is optional.
18. Click **Next**.
19. In the section, provide FQDN, Timezone, and SNMP passwords.

    Note:

    Use the same IP address and FQDN as that on the old System Manager.
20. In the Network Parameters section, provide the Public and Out of Band Management details.

    Note:

    Use the same IP address and FQDN as that on the old System Manager.
21. Click **Upgrade** and accept the license terms.

    The existing virtual machine shuts down, deploys OVA, and restores the data on the new virtual machine.
22. To view the status, in the **Upgrade Status** column, click **Status Details**.

    The complete process takes about 3 hours depending on the data on System Manager.

Related links

Upgrade Management field descriptions on page 31
Upgrade Management field descriptions on page 33

Upgrading System Manager on the same server by using Solution Deployment Manager client

About this task

You can upgrade System Manager on the same server or a different server.

The procedure describes the steps to upgrade System Platform-based System Manager on the same server.

Before you begin

- Add a location.
- Install the Solution Deployment Manager client.
- Obtain the following System Manager software:
  - OVA file, `SMGR-7.0.0.0.16266-e55-43-29-II.ova`

- Data migration utility, `Data_Migration_Utility_7.0.1.0_r96.bin`
- Release 7.0.1 bin file, `System_Manager_7.0.1.0_r701064859.bin`

- Create the System Manager backup and copy the file to the same computer where Solution Deployment Manager client is installed.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **VM Management**.
3. In the lower pane, click **Upgrade Management**.
4. Click **Save**.
5. If System Manager element is present, select the required element.
6. Click **Upgrade**.
7. On the Upgrade Management page, select the **Install on Same ESXi** check box.
8. Click **Continue**.

   The system shuts down the virtual machine and reaches the paused state.

   You must add the Appliance Virtualization Platform host from VM Management.
9. Install the Appliance Virtualization Platform host on the server on which System Platform was running.
10. To resume the upgrade operation, click **Upgrade Elements** > **Resume from Upgrade elements** list.
11. **(Optional)** In , select the host.

    On the SMGR Upgrade dialog box, the system might preselect and disable .
12. Select the datastore on the host.

    The system populates the network parameters and configuration parameters from the System Platform-based virtual machine.
13. Select the tab.
14. In the section, provide FQDN, Timezone, and SNMP passwords.

    Note:

    Use the same IP address and FQDN as that on the old System Manager.
15. In the Network Parameters section, provide the Public and Out of Band Management details.

    Note:

    Use the same IP address and FQDN as that on the old System Manager.
16. Click **Upgrade** and accept the license terms.

The existing virtual machine shuts down, deploys OVA, and restores the data on the new virtual machine.

17. To view the status, in the **Upgrade Status** column, click **Status Details**.

    The complete process takes about 3 hours depending on the data on System Manager.

Related links

Upgrade Management field descriptions on page 31
Upgrade Management field descriptions on page 33

Installing service packs and software patches on System Manager by using the Solution Deployment Manager client

About this task

Use the procedure to install service packs, feature packs, or software patches on System Manager by using Solution Deployment Manager client.

Before you begin

Install the Solution Deployment Manager client.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **VM Management**.
3. In VM Management Tree, select a location.
4. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select System Manager on which you want to install the patch.
5. **(Optional)** If updating from a different client, perform the following:
   a. Click **More Actions** > **Re-establish connection**.
   b. Click on **Refresh VM**.
   c. To view the status, in the **Current Action** column, click **Status Details**.
   d. Proceed with the next step.
6. Click **More Actions** > **Update VM**.

   The system displays the System Manager Update dialog box.
7. In **Select bin file from Local SDM Client**, provide the absolute path to the software patch or service pack.

Note:

The absolute path is the path on the computer on which the Solution Deployment Manager client is running. The patch is uploaded to System Manager.

8. **(Optional)** Click the **Auto commit the patch** check box.
9. Click **Install**.

   In the VMs for Selected Location <location name> section, the system displays the status.
10. To view the details, in the **Current Action** column, click **Status Details**.

    SMGR Patching Status window displays the details. The system displays the Installed Patches page. The patch installation takes some time.
11. On the Installed Patches page, perform the following:
    a. In **Action to be performed**, click **Commit**.

       The system installs the patch, service pack or feature pack that you selected.
    b. Click **Get Info**.
    c. Select the patch, service pack or feature pack, and click **Commit**.

Upgrade Management field descriptions

Upgrade Elements

Name	Description
IP/FQDN	The IP address or the FQDN of System Manager virtual machine.
SMGR Name	System Manager name.
Upgrade Status	The status of the upgrade process. The status can be **Upgrading**, **Completed**, or **Failed**. The **Status Details** link provides more information about the System Manager upgrade.
Last Action	The last upgrade action.

Button	Description
Add Elements	Displays the Add Element page where you add System Manager.
Upgrade	Displays the Upgrade Management page where you upgrade the System Manager virtual machine.

Table continues…

Button	Description
Edit	Displays the Edit Element page where you can change the details of System Manager that you added.
Delete	Deletes the System Manager virtual machine.

Add Element field descriptions

Required Element information

Name	Description
SMGR IP	The IP address of System Manager
SMGR NAME	The name of the System Manager virtual machine
SMGR SSH User Name	The SSH user name of System Manager
SMGR SSH Password	The SSH password of System Manager

Required C-DOM information

Name	Description
C-DOM IP/FQDN	The C-DOM IP/FQDN
C-DOM SSH User Name	The C-DOM SSH user name
C-DOM SSH Password	The C-DOM SSH password
C-DOM Root User Name	The C-DOM root user name
C-DOM Root password	The C-DOM root password

Button	Description
Save	Saves the element that you added

Edit Elements field descriptions

Required Element information

Name	Description
SMGR IP	The IP address of System Manager
SMGR NAME	The name of System Manager virtual machine.
SMGR SSH User Name	The SSH user name of System Manager
SMGR SSH Password	The SSH password of System Manager

Required C-DOM information

Name	Description
C-DOM IP/FQDN	The C-DOM IP/FQDN
C-DOM SSH User Name	The C-DOM SSH user name
C-DOM SSH Password	The C-DOM SSH password
C-DOM Root User Name	The C-DOm root user name
C-DOM Root password	The C-DOM root password

Button	Description
Update	Updates the changes to the element.

Upgrade Management field descriptions

Name	Description
Install on Same ESXi	The option to select the same or a different server. The options are: • Select: To upgrade on the same server. • Clear: To upgrade to a different server. If you do not select the check box, you must add a new server or select a server from the list to which you want to update.
Host FQDN	The Host FQDN to which you want to update. The system displays the CPU and memory details of the host in the Capacity Details section.
VM Name	The virtual machine name displayed on the Add Element page.

Deploy OVA

Name	Description
Select the OVA	The option to select a `.ova` file of the virtual machine that is available on System Manager.
OVA file	The absolute path to the `.ova` file of the virtual machine. The field is available only when you click **Select the OVA from Local SMGR**.
Submit File	Selects the `.ova` file of the virtual machine that you want to deploy.

Table continues…

Name	Description
	The field is available only when you click **Select the OVA from Local SMGR**. The system displays the network configuration details in the Network Parameters section based on the System Manager virtual machine.
Flexi Footprint	The footprint size supported for the selected server. The system validates for the CPU, memory, and other parameters in the Capacity Details section. You must ensure that the status is .
SMGR Datamigration Utility file	The absolute path to the System Manager data migration utility file. **Note:** Provide the latest datamigration bin that is available for the System Manager release.
Backup file	The absolute path to the backup of System Manager virtual machine.
Service Pack or Feature Pack	The absolute path to the service pack or feature pack. For the latest service pack or feature pack, see the latest System Manager release notes.

Note:

- For upgrades from System Manager Release 6.3.15 or later, the bin file is mandatory.
- For upgrades from System Manager 6.3.14 or earlier, the bin patch file is optional.

  If you provide the service pack or feature pack, the datamigration utility automatically deploys the service pack or feature pack on System Manager Release 7.0.0.0 after data migration.

Configuration Parameters

The system populates most of the fields depending on the OVA file. You must provide information, such as password, FQDN, and timezone.

Name	Description
Management IP Address (Out of Band Management IP Address)	The IP address of the System Manager virtual machine for Out of Band Management. The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network.
Management Netmask	The Out of Band Management subnetwork mask to assign to the System Manager virtual machine.

Table continues…

Name	Description
Management Gateway	The gateway IP address to assign to the System Manager virtual machine. For example, 172.16.1.1.
IP Address of DNS Server	The DNS IP addresses to assign to the primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,). For example, 172.16.1.2, 172.16.1.4.
Management Hostname	The hostname to assign to the System Manager virtual machine. For example, bouldervm2.
Default Search List	The search list of domain names. The field is optional.
NTP Server IP or FQDN	The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).
Time Zone	The timezone where the System Manager virtual machine is located. A list is available where you can select the continent and the country.

Public Network Settings

Name	Description
Public IP Address	The IP address to enable public access to different interfaces.
Public Netmask	The subnetwork mask to assign to System Manager virtual machine.
Public Gateway	The gateway IP address to assign to the System Manager virtual machine. For example, 172.16.1.1.
Public Hostname	The hostname to assign to the System Manager virtual machine. For example, bouldervm2.

Virtual FQDN

Name	Description
Virtual Hostname	The virtual hostname of the System Manager virtual machine. For example, grsmgr.
Virtual Domain	The virtual domain name of the System Manager virtual machine. For example, dev.com.

SNMPv3 Parameters

Name	Description
SNMPv3 User Name Prefix	The prefix for SNMPv3 user.
SNMPv3 User Authentication Protocol Password	The password for SNMPv3 user authentication.

Table continues…

Name	Description
Confirm Password	The password that you retype to confirm the SNMPv3 user authentication protocol.
SNMPv3 User Privacy Protocol Password	The password for SNMPv3 user privacy.
Confirm Password	The password that you must provide to confirm the SNMPv3 user privacy protocol.

Backup Definition

Name	Description
Schedule Backup?	• **Yes**: To schedule the backup jobs during the System Manager installation. • **No**: To schedule the backup jobs later. **Note:** If you select No, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server. **Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id	The login ID of the backup server to log in through the command line interface.
Backup Server Login Password	The SSH login password to log in to the backup server from System Manager through the command line interface.
Confirm Password	The password that you reenter to log in to the backup server through the command line interface.
Backup Directory Location	The location on the remote backup server.
File Transfer Protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.
Repeat Type	The type of the backup. The possible values are: • `Hourly` • `Daily` • `Weekly` • `Monthly`

Table continues…

Name	Description
Backup Frequency	The frequency of the backup taken for the selected backup type.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be 6 hours later than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

Network Parameters

Name	Description
Out of Band Management IP Address	The port number that you must assign to the Out of Band Management port group. The field is mandatory.
Public	The port number that you must assign to public port group. The field is optional.

Button	Description
Upgrade	Displays the EULA acceptance screen where you must click **Accept** to start the upgrade.

Install on Same ESXi field descriptions

Name	Description
Install on Same ESXi	The option to select the same or a different server during the upgrade. The options are: • Select: To upgrade on same server. • Clear: To upgrade on a different server.

Table continues…

Name	Description
HOST FQDN	The fully qualified domain name. For example, platform.mydomain.com.

Chapter 5: Upgrading System Manager 6.x on the Avaya-provided server

Data migration utility

Use the data migration utility to migrate the backup data of System Manager 6.x to System Manager Release 7.0.1 on an Avaya-provided server with Appliance Virtualization Platform. In the data migration utility process, you do not have to perform the intermediate steps for upgrading System Manager to Release 7.0.1.

Use the data migration utility process to:

- Migrate the data when you replace the existing server.
- Upgrade across multiple releases. For example, upgrades from Release 6.0 to Release 7.0.1.

In the data migration utility method, the system does not:

- Support the rollback operation.

  To recover data, perform the cold standby procedure for software-only upgrades and start the existing server for hardware upgrades.
- Import System Platform data and the Services VM data.

Checklist for upgrading from System Manager 6.x

Data migration from System Manager Release 6.0.x, 6.1.x, 6.2.x, or 6.3.x running on System Platform to Release 7.0.1 on Appliance Virtualization Platform involves the following tasks:

Serial Number	Task	Notes	✔
1	Download the `Data_Migration_Utility_7.0.1.0_r96.bin` file, `System Manager 7.0.1 bin` file, and `SMGR-7.0.0.0.16266-`		

Table continues…

Serial Number	Task	Notes	✔
	`e55-43-29-II.ova` from the PLDS website at http://plds.avaya.com.		
2	Download the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.zip` file from the Avaya Support website at http://support.avaya.com.		
3	Verify the software version of the current System Manager.	Verifying the current software version on System Manager 5.2.x or earlier on page 65	
4	Create a backup of System Manager and copy to the remote server.	r on page 44	
5	Record the System Platform configuration data such as SAL Gateway configuration, static routes, High Availability (HA) configuration data, and users.	Use data to reconfigure the new System Manager installation.	

6	Record the IP address or FQDN and the system parameters.	For the details, in the command line interface, type the following:
		`# ifconfig eth0 | grep inet`
		The system displays `inet addr:xxx.xxx.xxx.xxx Bcast:xxx.xxx.xxx.xxx Mask:xxx.xxx.xxx.xxx.`
		`#admin >hostname`	

7	Before you turn off the system, copy the Avaya Breeze™ snap-in svar files that you might need in the future to the `/var/avaya/svars` location on the local computer. When you upgrade System Manager from Release 6.x to Release 7.0.1, System Manager always contains a new virtual machine. Therefore, all data from the old file system is lost.	-	
8	If the existing server is not compatible with System Manager Release 7.0.1, change the server to one of the following: • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7 • Dell™ PowerEdge™ R620 • HP ProLiant DL360p G8	For more information, see *Installing the HP ProLiant DL360p G8 Server* or *Installing the Dell™ PowerEdge™ R620 Server*.	

Table continues…

Serial Number	Task	Notes	✔
	• Dell™ PowerEdge™ R630 • HP ProLiant DL360 G9 Release 7.0 and later does not support S8510 and S8800 servers.		
9	Install the `Avaya_SDMClient_win64_7.0.1.0.062031 9_44.exe` file.	Installing the Solution Deployment Manager client on your computer on page 18	
10	For hardware upgrades, install Appliance Virtualization Platform on the supported server.	-	
11	Add a location.	Adding a location on page 80	
12	Add the Appliance Virtualization Platform host.	Adding an ESXi host on page 87	
13	Add the virtual machine.	Deploying an OVA file for an Avaya Aura application on page 107	
14	Deploy the System Manager Release 7.0 ova file.	Deploying an OVA file for an Avaya Aura application on page 107	
15	Copy the data migration utility and the Release 7.0 bin file to the `/home/admin` location, and the backup file to the `/swlibrary` location on System Manager Release 7.0.	-	
16	On System Manager Release 7.0 command line interface, run **`upgradeSMGR`** with `Data_Migration_Utility_7.0.1.0_r96.bin` and the service pack or feature pack as inputs.	Upgrading to System Manager Release 7.0.1 running on an Avaya-provided server on page 45	
17	Verify that System Manager is functional.	Verifying the functionality of System Manager on page 46	
18	Install the System Manager Release 7.0.1 bin file.	**Note:** Install the service pack or feature pack only after you run the data migration utility on System Manager Release 7.0.	
19	To get the updated kernel that is running in the memory, reboot System Manager.	-	
20	Reconfigure System Manager with the data that you recorded in Step 5.	-	

Table continues…

Serial Number	Task	Notes	✔
21	Copy the Avaya Breeze™ snap-in svar files that you saved earlier to the Release 7.0.1 system.	-	
22	Create a backup of System Manager and copy to the remote server.	Creating a data backup on a remote server on page 47	
23	Regenerate licenses from PLDS after migration.	-	

You can set up Geographic Redundancy on the system after you upgrade the system to Release 7.0.1. For information, see Geographic Redundancy in *Administering Avaya Aura® System Manager for Release 7.0.1*.

Checklist for upgrade from System Manager configured with Geographic Redundancy on System Platform

The data migration from System Manager running on System Platform in the Geographic Redundancy setup to Release 7.0.1 on Appliance Virtualization Platform includes the following tasks:

S No	Field	Notes	✔
1	Download the `Data_Migration_Utility_7.0.1.0_r96.bin` file, `System Manager 7.0.1 bin` file, and `SMGR-7.0.0.0.16266-e55-43-29-II.ova` from the PLDS website at http://plds.avaya.com.	For the latest service packs and software patches, see System Manager release notes on the Avaya Support website at http://support.avaya.com.	
2	Download the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.zip` file from the Avaya Support website at http://support.avaya.com.	-	
3	Verify the software version of the current System Manager.	Verifying the current software version on page 65	
4	Create a backup of System Manager and copy to the remote server.	Creating a data backup on a remote server on page 44	
5	Keep a copy of the license files for the Avaya Aura® products so you can replicate with the new Host ID after the OVA file installation.	-	

Table continues…

S No	Field	Notes	✔
6	Disable the Geographic Redundancy replication.	See *Administering Avaya Aura® System Manager for Release 7.0.1*.	
7	Install the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.exe` file.	Installing the Solution Deployment Manager client on your computer on page 18	
8	If the existing server is not compatible with System Manager Release 7.0.1, change the server to one of the following: • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7 • Dell™ PowerEdge™ R620 • HP ProLiant DL360p G8 • Dell™ PowerEdge™ R630 • HP ProLiant DL360 G9 Release 7.0 and later does not support S8510 and S8800 servers.	For more information, see *Installing the HP ProLiant DL360p G8 Server* or *Installing the Dell™ PowerEdge™ R620 Server*.	
9	Add a location.	Adding a location on page 80	
10	Add the Appliance Virtualization Platform host.	Adding an ESXi host on page 87	
11	Add the virtual machine.	Deploying an OVA file for an Avaya Aura application on page 107	
12	Deploy the System Manager Release 7.0 ova file. In the Geographic Redundancy setup, complete the installation on the primary System Manager first and then perform on the secondary Geographic Redundancy.	Deploying an OVA file for an Avaya Aura application on page 107	
13	Copy the data migration utility and the Release 7.0 bin file to the `/home/admin` location, and the backup file to the `/swlibrary` location on System Manager Release 7.0.	-	
14	On System Manager Release 7.0 command line interface, run **`upgradeSMGR`** with `Data_Migration_Utility_7.0.1.0_r96.bin` and the service pack or feature pack as inputs.	Upgrading to System Manager Release 7.0.1 running on an Avaya-provided server on page 45 **Note:** The upgrade process on the primary System Manager takes about 65–70 minutes and about 75–80 minutes on the secondary System Manager.	

Table continues…

S No	Field	Notes	✔
		Wait until the upgrade process is complete, and continue with the next step.	
15	Verify that System Manager is functional.	-	
16	Install the System Manager Release 7.0.1 bin file.	**Note:** Install the service pack or feature pack only after you run the data migration utility on System Manager Release 7.0.	
16	On the primary System Manager server, enable the Geographic Redundancy replication.	See *Administering Avaya Aura® System Manager for Release 7.0.1*.	

For Geographic Redundancy-related procedures, see *Administering Avaya Aura® System Manager for Release 7.0.1*.

Verifying the current software version

About this task

Use this procedure to verify the current software version for System Manager 6.x.

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   The system displays the About SMGR window with the build details.
3. Verify the version number of System Manager with the highest build number for the release.

Creating a data backup on a remote server

Procedure

1. Perform one of the following:
   - For System Manager 6.1 and later, on System Manager Web Console, click **Services** > **Backup and Restore**.
   - For System Manager 6.0, on System Manager Web Console, click **System Manager Data** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.

3. On the Backup page, click **Remote**.
4. Specify the remote server IP, remote server port, user name, password, and name and path of the backup file that you create.
5. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

Upgrading to System Manager Release 7.0.1 running on an Avaya-provided server

About this task

Use the procedure to upgrade System Manager to Release 7.0.1 running on an Avaya-provided server with Appliance Virtualization Platform.

Before you begin

- Ensure that System Manager is running.
- Download the `Data_Migration_Utility_7.0.1.0_r96.bin` file, `System Manager 7.0.1 bin` file, and the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file from the Avaya Support website at http://support.avaya.com.

Procedure

1. Log on to the System Manager web console.
2. Record the software version of System Manager from the **About** link.
3. Create the System Manager data backup by using System Manager and copy the backup to the `/swlibrary` folder of the server.

   For upgrades by using data migration utility, use only the backup that you created from the System Manager web console.
4. Log in to the System Manager command line interface of the existing system.
5. Shut down System Manager.
6. Deploy the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` on the System Manager.

   Important:

   Use the same network parameters and system parameters that you recorded on the existing system.
7. Copy `Data_Migration_Utility_7.0.1.0_r96.bin` to the `/home/admin` location, and the Release 7.0.1 bin file and System Manager backup file to the `/swlibrary` location on System Manager.
8. To log in to the System Manager virtual machine as the root user, type `su - root`.

9. On System Manager Release 7.0.1, at the prompt, perform the following:
   a. To remove any older data migration utility-related files, type `rm -fr /opt/Avaya/data_migration`.
   b. Type `sh /home/admin/<dm utility filename.bin> -m -v`.
   c. Type the absolute path to the backup file:

      ```
      /home/admin/<backupfile name.*>
      ```

      The system displays the following message:

      ```
      Verified that the file /home/admin/<backupfile name>.zip exists.
      You are about to run the System Manager Data Migration utility.
      The System Manager will be inaccessible for approx. 90 mins,
      depending on the resources available on the system.
      ```

Verifying the functionality of System Manager

To ensure that System Manager is working correctly after the data migration is complete, verify that the current installation of System Manager is successful.

About this task

Note:

When you migrate to System Manager Release 6.3 from:

- 6.0.x or 6.1.x. If you have users with roles other than *admin*, the system resets the user passwords to the login name of the users.

  For example, the system sets the password of a user with the login name dsmith@avaya.com and a role other than end user to dsmith@avaya.com after the migration.

  The end user passwords in System Manager Release 6.3 or 6.2 remain the same as in 6.1.
- 6.0.x. The system resets the admin password.
- 6.1.x or 6.2.x. The admin password remains the same.

When you promote an end user to an administrator, the system resets the password for the end user to the login name of the user.

Procedure

1. To log on to the System Manager web console, in the web browser, type `https://<FQDN>/SMGR`, where *FQDN* is the fully qualified domain name of System Manager.
2. On the upgraded system, verify that the following data matches the number of users and roles that you recorded before the upgrade.
   - The number of users

- The number of roles

For more information, see Managing users and Managing roles in *Administering Avaya Aura® System Manager for Release 7.0.1*.

3. Verify if the following function correctly:
   - Creation and deletion of a user
   - Creation of a role
   - Creation of a job
   - Creation of the remote data backup
   - Replication of the data using Data Replication Service (DRS)

   For more information on completing each verification task, see *Administering Avaya Aura® System Manager for Release 7.0.1*.

Creating a data backup on a remote server

Before you begin

Ensure that the backup server supports the required algorithms for the System Manager remote backup. For more information, see Supported ciphers, key exchange algorithms, and mac algorithms.

System Manager requires password authentication to enable the remote backup servers for successful backup.

Note:

System Manager does not support authentication mechanisms, such as Keyboard-Interactive and public key-based support.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - Perform the following:
     a. In the **File transfer protocol** field, click `SCP` or `SFTP`.
     b. Enter the remote server IP, remote server port, user name, password, and name and the path of the backup file that you create.
   - Select the **Use Default** check box.

Important:

To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

5. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

Chapter 6: Upgrading from System Manager 6.x to Release 7.0.1 on VMware in customer-provided Virtualized Environment

Checklist for upgrade from System Manager 6.x

Use the following checklist for upgrading System Manager vAppliance from Release 6.x to Release 7.0.1.

#	Action	Link/Notes	✔
1	Download the `Data_Migration_Utility_7.0.1.0_r96.bin` file, `System Manager 7.0.1 bin` file, and `SMGR-7.0.0.0.16266-e55-43-29-II.ova` from the PLDS website at http://plds.avaya.com.	For the latest service packs and software patches, see System Manager release notes on the Avaya Support website at http://support.avaya.com.	
2	Record the number of users and number of roles. You require this information later to verify that the upgrade is successful	For more information, see Managing users and Managing roles in *Administering Avaya Aura® System Manager for Release 7.0.1*.	

3	Record the IP address or FQDN and the system parameters.	In the command line interface, type the following commands for the details:
		`# ifconfig eth0 | grep inet`
		The system displays `inet addr:xxx.xxx.xxx.xxx Bcast:xxx.xxx.xxx.xxx Mask:xxx.xxx.xxx.xxx.`
		`#admin >hostname`	

4	Keep a copy of the license files for the Avaya Aura® products so you can replicate with the new Host ID after the OVA file installation.	-	

Table continues…

#	Action	Link/Notes	✔
5	Before you turn off the system, copy the Avaya Breeze™ snap-in svar files that you might need in the future to the `/var/avaya/svars` location on the local computer. When you upgrade System Manager from Release 6.x to Release 7.0.1, System Manager always contains a new virtual machine. Therefore, all data from the old file system is lost.	-	
6	Ensure that the server is compatible with System Manager Release 7.0.1.	Server hardware and resources on page 14	
7	Create a backup of System Manager.	Creating a data backup on a remote server on page 47	
8	Turn off the System Manager virtual machine.	-	
9	On the ESXi server, install the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file. Use the same IP address or FQDN as that of the existing System Manager. **Note:** System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.	Deploying the System Manager OVA file by using vSphere on page 129	
10	Copy the data migration utility and the Release 7.0 bin file to the `/home/admin` location, and the backup file to the `/swlibrary` location on System Manager Release 7.0.	You can use the tools such as SCP, WinSCP, and FileZilla to copy the files.	
11	Create the snapshot of the System Manager virtual machine.	Creating the System Manager virtual machine snapshot on page 52	
12	In the settings icon ( ), click **About** to check the System Manager version.	-	
13	Verify that System Manager is functional.	Verifying the functionality of System Manager on page 71	
14	Create the snapshot of the System Manager virtual machine.	Creating the System Manager virtual machine snapshot on page 52	

Table continues…

#	Action	Link/Notes	✔
15	On System Manager Release 7.0 command line interface, run **upgradeSMGR** with `Data_Migration_Utility_7.0.1.0_r96.bin` and the service pack or feature pack as inputs. The upgrade takes about 80–90 minutes. However, the duration depends on the factors such as the number of users, backup size, hardware used, and the number of resources shared during the upgrade.	Upgrading System Manager from Release 6.0, 6.1, 6.2, and 6.3 to Release 7.0.1 on VMware on page 53	
16	Copy the Avaya Breeze™ snap-in svar files that you saved earlier to the Release 7.0.1 system.	-	

You can set up Geographic Redundancy after you upgrade the system to Release 7.0.1. For more information, see Geographic Redundancy in *Administering Avaya Aura® System Manager for Release 7.0.1*.

To upgrade from System Manager Release 6.3.2 or later running on VMware, see Upgrading System Manager from 6.3.x on VMware to System Manager Release 7.0.1.

Verifying the current software version

About this task

Use this procedure to verify the current software version for System Manager 6.x.

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   The system displays the About SMGR window with the build details.
3. Verify the version number of System Manager with the highest build number for the release.

Creating a data backup on a remote server

Procedure

1. Perform one of the following:
   - For System Manager 6.1 and later, on System Manager Web Console, click **Services** > **Backup and Restore**.
   - For System Manager 6.0, on System Manager Web Console, click **System Manager Data** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Specify the remote server IP, remote server port, user name, password, and name and path of the backup file that you create.
5. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

Installing the System Manager OVA file

Procedure

Deploy the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file on one of the following:

- Avaya-provided server
- Customer-provided Virtualized Environment

Related links

Deploying the System Manager OVA file by using vSphere on page 129
Deploying the System Manager OVA file using vCenter on page 134
Deploying an OVA file for an Avaya Aura application on page 107

Creating the System Manager virtual machine snapshot

About this task

Important:

Do not perform any activity on System Manager until the snapshot is created.

You can create the snapshot of the System Manager virtual machine using vSphere Client.

Procedure

1. From the list of virtual machines, right-click the required System Manager virtual machine, and click **Snapshot**.
2. On the **Take Virtual Machine Snapshot** dialog box, perform the following:
   a. In the **Name** and **Description** fields, enter a name and the description for the snapshot.
   b. Ensure that the following check boxes are cleared:
      - Snapshot the virtual machine's memory
      - Quiesce guest file system (Needs VMware Tools installed)
3. Click **OK**.
4. In the Recent Tasks window, perform the following:
   a. Verify the **Status** of the **Create virtual machine snapshot** task.
   b. Wait until the system displays `Completed`.

Upgrading System Manager from Release 6.0, 6.1, 6.2, and 6.3 to Release 7.0.1 on VMware

Before you begin

- Ensure that System Manager is running.
- Download the `Data_Migration_Utility_7.0.1.0_r96.bin` file, `System Manager 7.0.1 bin` file, and the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file from the Avaya Support website at http://support.avaya.com.
- Install the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.exe` file.

About this task

Use this procedure to upgrade System Manager from Release 6.0, 6.1, 6.2, and 6.3.x to Release 7.0.1 on VMware. The data migration utility runs in the background.

Procedure

1. Log on to the System Manager web console.
2. Record the software version of System Manager from the **About** link.
3. Create the System Manager data backup by using System Manager and copy the backup to the `/swlibrary` folder of the server.

   For upgrades by using data migration utility, use only the backup that you created from the System Manager web console.
4. Log in to the System Manager command line interface of the existing system as admin.

5. To shut down the System Manager virtual machine, perform one of the following:
   - On System Platform, click **Shutdown Server** on the Server Reboot/Shutdown page.
     a. Click **Virtual Machine Management** > **Manage**.
     b. Click the System Manager virtual machine and click **Stop**.
   - On VMware, click **Power** > **Power Off**.
6. On the SDM Client Dashboard, click **VM Management**.
7. On the ESXi server, install the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file.

   For more information, see Deploying an OVA file for Avaya Aura® application.

   Important:

   Use the same IP address or FQDN and system parameters that you recorded earlier.
8. Ensure that System Manager is running.
9. Create a snapshot of the System Manager virtual machine.
10. On vSphere Client, select the System Manager virtual machine and click the Console tab.
11. Log in to the System Manager virtual machine.
12. Copy `Data_Migration_Utility_7.0.1.0_r96.bin` to the `/home/admin` location, and the Release 7.0.1 bin file and System Manager backup file to the `/swlibrary` location on System Manager.
13. At the prompt, do the following:
    a. To remove any older data migration utility-related files, type `rm -fr /opt/Avaya/data_migration`.
    b. To run the data migration utility, type the following command:

       ```
       upgradeSMGR /home/admin/<DMUtility_bin file name>.bin -m -v
       ```

       You must provide the absolute path to the data migration utility.
    c. Type the absolute path to the backup file:

       ```
       /home/admin/<backupfile name.*>
       ```

       The system displays the following message:

       ```
       Verified that the file /home/admin/<backupfile name>.zip exists.
       You are about to run the System Manager Data Migration utility.
       The System Manager will be inaccessible for approx. 90 mins,
       depending on the resources available on the system.
       ```
    d. At the prompt, type `Y`.
    e. At the prompt, type the absolute path to the service pack or feature pack file.

       For example, `swlibrary/System_Manager_R7.0.1xxx.bin`.

Note:

For upgrades from System Manager 6.3.14 or earlier, install the service pack or feature pack by using the **SMGRPatchdeploy** command or from Solution Deployment Manager.

The system displays the following warning message:

```
The system is now going down for a halt and will be inaccessible for some time.
Remote broadcast message (Thu July 30 21:06:27 2015):
Data Migration executes in background process. For details, see System Manager
Data Migration logs in the /var/log/Avaya/datamigration/data_migration.log
```

The system upgrades the System Manager data in the verbose mode. The upgrade process takes about 70–80 minutes to complete. Wait until the upgrade process is complete, and continue with the next step.

14. Log on to System Manager and verify that the upgrade is successful.

Related links

Creating a data backup on a remote server on page 47
Verifying the functionality of System Manager on page 71

Checklist for upgrading System Manager Release 6.3.x in the Geographic Redundancy setup to Release 7.0.1

Perform the following tasks to upgrade System Manager Release 6.3.x in the Geographic Redundancy setup to Release 7.0.1.

Table 3: Prerequisites

No.	Task	Notes	✔
1	Download the `Data_Migration_Utility_7.0.1.0_r96.bin` file, `System Manager 7.0.1 bin` file, and `SMGR-7.0.0.0.16266-e55-43-29-II.ova` from the PLDS website at http://plds.avaya.com.		
2	Get a valid license file.		

Table 4: Tasks on the primary System Manager server

No.	Task	Notes	✔
1	Disable the Geographic Redundancy replication.		
2	Create a remote backup of the System Manager data.		
3	Turn off or remove the System Manager virtual machine.		
4	Install the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file. **Note:** After you install the Release 7.0.1 `.ova` file and before you perform operations such as configuring Geographic Redundancy and changing the IP or FQDN, you must run the data migration utility.		
5	Verify that the System Manager installation is successful.		
6	Copy the data migration utility and the Release 7.0 bin file to the `/home/admin` location, and the backup file to the `/swlibrary` location on System Manager Release 7.0.		
7	Create the snapshot of the System Manager virtual machine.		
8	Run the data migration utility and provide the backup file and the Release 7.0.1 bin file.	Upgrading System Manager from Release 6.3.x in the Geographic Redundancy setup to Release 7.0.1 on page 57	
9	For Release 6.3.14 or earlier: Install the System Manager Release 7.0.1 bin file. The patch installation takes about 60–65 minutes to complete.		
10	Verify that the data is successfully migrated to Release 7.0.1.		
11	Convert the primary System Manager server to the standalone server.		

Table 5: Tasks on the secondary System Manager server

No.	Task	Notes	✔
1	Turn off or remove the System Manager virtual machine.		
2	Install the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file.		
3	Verify that the System Manager installation is successful.		
4	Create the snapshot of the System Manager virtual machine.		
5	Install the System Manager Release 7.0.1 bin file. The patch installation takes about 60–65 minutes to complete.	**Note:** Install the service pack or feature pack only after you run the data migration utility on System Manager Release 7.0.	
6	Configure Geographic Redundancy with the details of the primary server that you converted to standalone.		
7	Enable the Geographic Redundancy replication from the primary server.		

Upgrading System Manager from Release 6.3.x in the Geographic Redundancy setup to Release 7.0.1

About this task

Use this procedure to upgrade System Manager from Release 6.3.x in the Geographic Redundancy setup to Release 7.0.1.

Perform the procedure on the primary System Manager server.

Before you begin

- Ensure that the primary and secondary System Manager servers are running.
- Download the `SMGR-7.0.0.0.16266-e55-43-29-II.ova`, `System_Manager_7.0.1.0_r701064859.bin` file, and `Data_Migration_Utility_7.0.1.0_r96.bin` files from the Avaya Support website at http://support.avaya.com.
- Install the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.exe` file.

Procedure

1. Log on to the web console of the primary System Manager server.
2. Disable the Geographic Redundancy replication if replication is enabled.

   For more information, see Disabling the Geographic Redundancy replication.
3. Record the software version of System Manager from the **About** link.
4. Create the System Manager data backup, and copy the backup to the remote server.
5. Shut down the System Manager virtual machine by using one of the following:
   - On System Platform:
     a. Click **Virtual Machine Management** > **Manage**.
     b. Click the System Manager virtual machine, and click **Stop**.
   - On VMware, click **Power** > **Power Off**.
6. On the ESXi host, install the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file.

   For more information, see *Deploying Avaya Aura® System Manager*.

   Important:

   - Use the same IP address or FQDN, and system parameters of the primary server that you want to upgrade.
   - After you install the Release 7.0.1 `.ova` file and before you perform operations such as configuring Geographic Redundancy and changing the IP or FQDN, you must run the data migration utility.
7. Ensure that System Manager is running and the installation is successful.

   Important:

   Do not run the data migration utility from the command line interface after you successfully log on to the System Manager console.

   The migration process might fail and the system data gets corrupted if you log on to the web console. To repair the system, you must deploy the OVA file again.
8. Copy the `Data_Migration_Utility_7.0.1.0_r96.bin` file to the `/home/admin` location, and Release 7.0.1 bin file and System Manager backup file to the `/swlibrary` location on the primary System Manager server.
9. Create a snapshot of the primary System Manager virtual machine.
10. At the prompt, do the following:
    a. To remove any older data migration utility-related files, type `rm -fr /opt/Avaya/data_migration`.
    b. To run the data migration utility, type the following command:

       ```
       upgradeSMGR /home/admin/<DMUtility_bin file name>.bin -m -v
       ```

       You must provide the absolute path to the data migration utility.

c. Type the absolute path to the backup file:

```
/home/admin/<backupfile name.*>
```

The system displays the following message:

```
Verified that the file /home/admin/<backupfile name>.zip exists.
You are about to run the System Manager Data Migration utility.
The System Manager will be inaccessible for approx. 90 mins,
depending on the resources available on the system.
```

d. At the prompt, type `Y`.

e. At the prompt, type the absolute path to the service pack or feature pack file.

For example, `swlibrary/System_Manager_R7.0.1xxx.bin`.

Note:

For upgrades from System Manager 6.3.14 or earlier, install the service pack or feature pack by using the **`SMGRPatchdeploy`** command or from Solution Deployment Manager.

The system displays the following warning message:

```
The system is now going down for a halt and will be inaccessible for some time.
Remote broadcast message (Thu July 30 21:06:27 2015):
Data Migration executes in background process. For details, see System Manager
Data Migration logs in the /var/log/Avaya/datamigration/data_migration.log
```

The system upgrades the System Manager data in the verbose mode. The upgrade process takes about 70–80 minutes to complete. Wait until the upgrade process is complete, and continue with the next step.

11. Log on to the System Manager web console, and verify that the data is migrated to the new system.

    At this point, System Manager becomes the primary server with Geographic Redundancy configured on it.

12. Convert the primary System Manager to a standalone System Manager.

    For more information, see Converting the primary System Manager server to the standalone server.

    The system takes about 10 minutes to convert the primary System Manager server to the standalone server.

Next steps

- Upgrade the secondary System Manager server.
- Reinstall the license files because after the data migration, the existing license files become invalid.

Upgrading the secondary System Manager server

About this task

Perform the procedure on the secondary System Manager server.

Before you begin

- On the primary System Manager server, ensure the following:
  - Install the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file.
  - Run `Data_Migration_Utility_7.0.1.0_r96.bin`.
  - Install the System Manager Release 7.0.1 bin file.
  - Convert the primary System Manager server to the standalone server.
- Ensure that the secondary System Manager server is running.
- Download the `SMGR-7.0.0.0.16266-e55-43-29-II.ova`, `System_Manager_7.0.1.0_r701064859.bin` file, and `Data_Migration_Utility_7.0.1.0_r96.bin` files from the Avaya Support website at http://support.avaya.com.

Procedure

1. Log on to the web console of the secondary System Manager server, and remove the System Manager virtual machine.
2. On the ESXi host, install the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file.

   Important:

   Use the same IP address or FQDN, and system parameters of the secondary server that you removed.
3. Verify that the installation is successful.
4. Install the `System Manager 7.0.1 bin` file.

   The patch installation takes about 60–65 minutes to complete.
5. Create a snapshot of the System Manager virtual machine.
6. Configure Geographic Redundancy, and provide the details of the standalone System Manager server.

   The system takes about 30 minutes to configure Geographic Redundancy.
7. Enable the Geographic Redundancy replication from the primary server.

Result

The process upgrades the primary and secondary System Manager servers in the Geographic Redundancy setup to Release 7.0.1.

Chapter 7: Upgrading from System Manager 5.2.x

Overview

Use this section to upgrade System Manager Release 5.2, 5.2 SP1, or 5.2 SP2 to Release 7.0.1 running on Avaya-provided server or customer-provided Virtualized Environment.

During the upgrade from System Manager Release 5.2.x to Release 7.0.1, the system only retains the routing data. You must manually add the remaining System Manager data to the Release 7.0.1 system.

NRP import and export utility

Use the NRP import and export utility to import and export only the routing data from System Manager 5.2.x to System Manager Release 7.0.1. You cannot migrate the data related to other System Manager options.

Checklist for upgrades from System Manager Release 5.2.x on Avaya-provided server

The upgrades from System Manager Release 5.2, 5.2 SP1, or 5.2 SP2 to Release 7.0.1 on Avaya-provided server consists the following high-level tasks. Perform the tasks sequentially.

#	Field	Notes	✔
1	Download `SMGR-7.0.0.0.16266-e55-43-29-II.ova` and the `System Manager 7.0.1 bin` file from the PLDS website at http://plds.avaya.com.	For the latest service packs and software patches, see System Manager release notes on the Avaya Support website at http://support.avaya.com.	

Table continues…

#	Field	Notes	✔
2	Download the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.zip` file from the Avaya Support website at http://support.avaya.com.	-	
3	Create a backup of System Manager and copy to the remote server.	Creating a data backup on a remote server on page 65	
4	Export the routing data from System Manager Release 5.2.x.	-	
5	Record the System Platform configuration data such as SAL Gateway configuration, static routes, High Availability (HA) configuration data, and users.	Use data to reconfigure the new System Manager installation.	

6	Record the IP address or FQDN and the system parameters.	In the command line interface, type the following commands for the details:
		`# ifconfig eth0 | grep inet`
		The system displays `inet addr:xxx.xxx.xxx.xxx Bcast:xxx.xxx.xxx.xxx Mask:xxx.xxx.xxx.xxx.`
		`#admin >hostname`	

7	If the existing server is not compatible with System Manager Release 7.0.1, change the server to one of the following: • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7 • Dell™ PowerEdge™ R620 • HP ProLiant DL360p G8 • Dell™ PowerEdge™ R630 • HP ProLiant DL360 G9 Release 7.0 and later does not support S8510 and S8800 servers.	For more information, see *Installing the HP ProLiant DL360p G8 Server* or *Installing the Dell™ PowerEdge™ R620 Server*.	
8	For hardware upgrades, install Appliance Virtualization Platform on the supported server.		
9	Install the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.exe` file.	Installing the Solution Deployment Manager client on your computer on page 18	
10	Add a location.	Adding a location on page 80	
11	Add the Appliance Virtualization Platform host.	Adding an ESXi host on page 87	

Table continues…

#	Field	Notes	✔
12	Add the virtual machine.	Deploying an OVA file for an Avaya Aura application on page 107	
13	Deploy the System Manager Release 7.0 ova file.	Deploying the OVA on the virtual machine on page 107	
14	Copy the backup file on System Manager Release 7.0.	-	
15	Install the System Manager Release 7.0.1 bin file. The patch installation takes about 60–65 minutes to complete.		
16	Import the data to System Manager Release 7.0.1.	Importing the data to System Manager Release 7.0.1 on page 69	
17	Verify that System Manager is functional.	Verifying the functionality of System Manager on page 46	
18	Reconfigure System Manager with the data that you recorded in Step 5.	-	
19	Create a backup of System Manager and copy to the remote server.	Creating a data backup on a remote server on page 47	

Checklist for upgrade from System Manager 5.2.x

The following contains the key tasks for upgrading System Manager from Release 5.2, 5.2 SP1, or 5.2 SP2 to Release 7.0.1 on VMware in Virtualized Environment.

#	Task	Notes	✔
1	Download `SMGR-7.0.0.0.16266-e55-43-29-II.ova` and the `System Manager 7.0.1 bin` file from the PLDS website at http://plds.avaya.com.	For the latest service packs and software patches, see System Manager release notes on the Avaya Support website at http://support.avaya.com.	
2	Download the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.zip` file from the Avaya Support website at http://support.avaya.com.		
3	Verify the software version of the current System Manager.	Verifying the current software version on System Manager 5.2.x or earlier on page 65	

Table continues…

#	Task	Notes	✔
4	Record the number of users and number of roles. You require this information later to verify that the upgrade is successful	For more information, see Managing users and Managing roles in *Administering Avaya Aura® System Manager for Release 7.0.1*.	

5	Record the IP address or FQDN and the system parameters.	In the command line interface, type the following commands for the details:
		`# ifconfig eth0 | grep inet`
		The system displays `inet addr:xxx.xxx.xxx.xxx Bcast:xxx.xxx.xxx.xxx Mask:xxx.xxx.xxx.xxx.`
		`#admin >hostname`	

6	Copy the backup file on System Manager Release 7.0.1.	Creating a data backup on a remote server on page 65	
7	Export the routing data from System Manager Release 5.2.x.	Exporting the routing data from System Manager 5.2.x on page 65	
8	Ensure that the server is compatible with System Manager Release 7.0.1.	Server hardware and resources for VMware on page 14	
9	Install the `Avaya_SDMClient_win64_7.0.1.0.0620319_44.exe` file.	Installing the Solution Deployment Manager client on your computer on page 18	
10	On the ESXi server, install the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file. Use the same IP address or FQDN as that of the existing System Manager. System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.	Deploying the System Manager OVA file by using vSphere on page 129	
11	In the settings icon (), click **About** to check the System Manager version.	-	
12	Verify that System Manager is functional.	Verifying the functionality of System Manager on page 71	
13	Create the snapshot of the System Manager virtual machine.	Creating the System Manager virtual machine snapshot on page 52	
14	Install the System Manager Release 7.0.1 bin file. The patch installation takes about 60–65 minutes to complete.		
15	Import the routing data to System Manager Release 7.0.1.	Importing the data to System Manager Release 7.0.1 on page 69	

You can set up Geographic Redundancy after you upgrade the system to Release 7.0.1. For more information, see Geographic Redundancy in *Administering Avaya Aura® System Manager for Release 7.0.1*.

Verifying the current software version on System Manager 5.2.x or earlier

Procedure

1. Log in to System Manager from the command line interface (CLI).
2. At the prompt, enter `vi /opt/Avaya/installdata/inventory.xml`.
3. In the `inventory.xml` file, search for the term System Manager and note the version ID.
4. Verify the version number of System Manager with the highest build number for the release.

Creating a data backup on a remote server

Before you begin

Log on to System Manager Web Console as `admin`.

Procedure

1. Click **Settings** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. To back up the data to a remote location, on the Backup page:
   a. Click **Remote**.
   b. Enter the details in the **SCP server IP**, **SCP server port**, **User name**, **Password**, and the file name in the respective fields.
4. Click **Now**.

   If the backup is successful, the Backup and Restore page displays `Backup created successfully!!`

Exporting the routing data from System Manager 5.2.x

Before you begin

- Create a backup of System Manager 5.2.x and copy to the remote server.

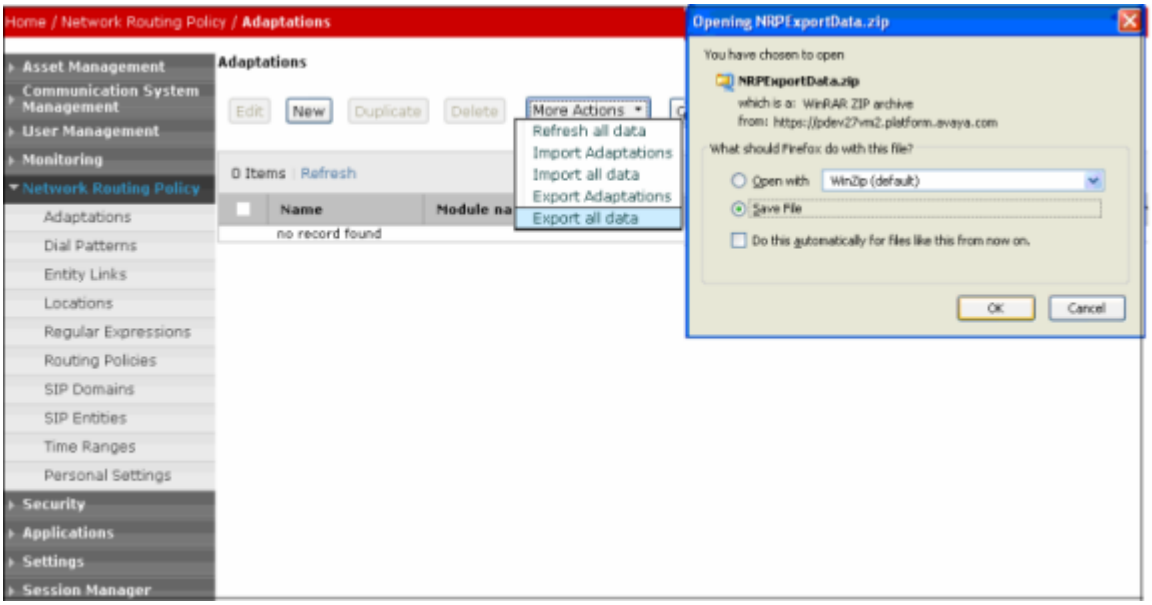
- Record the NRP records on System Manager 5.2.x. To view the records, on the web console of System Manager 5.2, click **Routing** > **Policies**. After you import the data, you require these records to verify if the system has successfully imported the data on System Manager Release 7.0.1.
- Record the data related to users, custom roles, and configuration. After importing the NRP data, you must manually add the data to System Manager Release 7.0.1.
- Record the network parameters on System Manager 5.2.x.

About this task

Use this procedure to export the System Manager routing data from Release 5.2, 5.2 SP1, or 5.2 SP2 to System Manager Release 7.0.1.

Procedure

1. On the Web browser, type `https://<IPAddress of System Manager>/SMGR` to log on to System Manager Web Console.
2. Log on to System Manager Web Console using the administrator credentials made available at the time of the System Manager installation.
3. Click **Network Routing Policy** > **Adaptations**.
4. On the Adaptations page, click **More Actions** > **Export All Data**.



5. Save the `NRPExportData.zip` file to a location that you can easily access.
6. Shut down the server on which System Manager is running.

Installing the System Manager OVA file

Procedure

Deploy the `SMGR-7.0.0.0.16266-e55-43-29-II.ova` file on one of the following:

- Avaya-provided server
- Customer-provided Virtualized Environment

Related links

Deploying the System Manager OVA file by using vSphere on page 129
Deploying the System Manager OVA file using vCenter on page 134
Deploying an OVA file for an Avaya Aura application on page 107

Installing service packs and software patches on System Manager by using the Solution Deployment Manager client

About this task

Use the procedure to install service packs, feature packs, or software patches on System Manager by using Solution Deployment Manager client.

Before you begin

Install the Solution Deployment Manager client.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon () on the desktop.
2. Click **VM Management**.
3. In VM Management Tree, select a location.
4. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select System Manager on which you want to install the patch.
5. **(Optional)** If updating from a different client, perform the following:
   a. Click **More Actions** > **Re-establish connection**.
   b. Click on **Refresh VM**.
   c. To view the status, in the **Current Action** column, click **Status Details**.
   d. Proceed with the next step.
6. Click **More Actions** > **Update VM**.

   The system displays the System Manager Update dialog box.

7. In **Select bin file from Local SDM Client**, provide the absolute path to the software patch or service pack.

   Note:

   The absolute path is the path on the computer on which the Solution Deployment Manager client is running. The patch is uploaded to System Manager.

8. **(Optional)** Click the **Auto commit the patch** check box.
9. Click **Install**.

   In the VMs for Selected Location <location name> section, the system displays the status.

10. To view the details, in the **Current Action** column, click **Status Details**.

    SMGR Patching Status window displays the details. The system displays the Installed Patches page. The patch installation takes some time.

11. On the Installed Patches page, perform the following:
    a. In **Action to be performed**, click **Commit**.

       The system installs the patch, service pack or feature pack that you selected.

    b. Click **Get Info**.
    c. Select the patch, service pack or feature pack, and click **Commit**.

Installing the System Manager Release 7.0.1 bin file

Before you begin

- Ensure that System Manager is running on Release 7.0.1.
- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Client and click on the **Console** tab or the  icon.
  - Start an SSH on System Manager.
- Log in to the System Manager virtual machine as admin.
- Download the `System_Manager_7.0.1.0_r701064859.bin` file from the Avaya Support website at http://support.avaya.com/ and copy the file to the `/home/admin` location on System Manager.

About this task

If you fail to install the Release 7.0.1 bin file for System Manager, the Virtualized Environment-specific functionality might be unavailable in System Manager.

Procedure

1. Create the System Manager virtual machine snapshot.

Note:

This activity might impact the service.

2. At the prompt, run the following command:

```
SMGRPatchdeploy <absolute path to the bin file>
```

The system displays the license information.

3. Read the End User License Agreement carefully, and to accept the license terms, type `Y`.

The patch installation takes about 60–65 minutes to complete.

If the installation is successful, the system displays a warning message on the web console and on the command line interface to restart System Manager if kernel is updated.

Next steps

1. Verify the patch installation.
   - If the patch installation is successful, log off from the system, and remove the snapshot.

     Note:

     Snapshots occupy the system memory and degrades the performance of the virtual application. Therefore, delete the snapshot after you verify the patch installation or the system upgrade.
   - If the patch installation fails, use the snapshot to restore the system to the original state.
2. Shut down the System Manager virtual machine.
3. Turn on the System Manager virtual machine.

   System Manager takes about 15 minutes to start.

Importing the data to System Manager Release 7.0.1

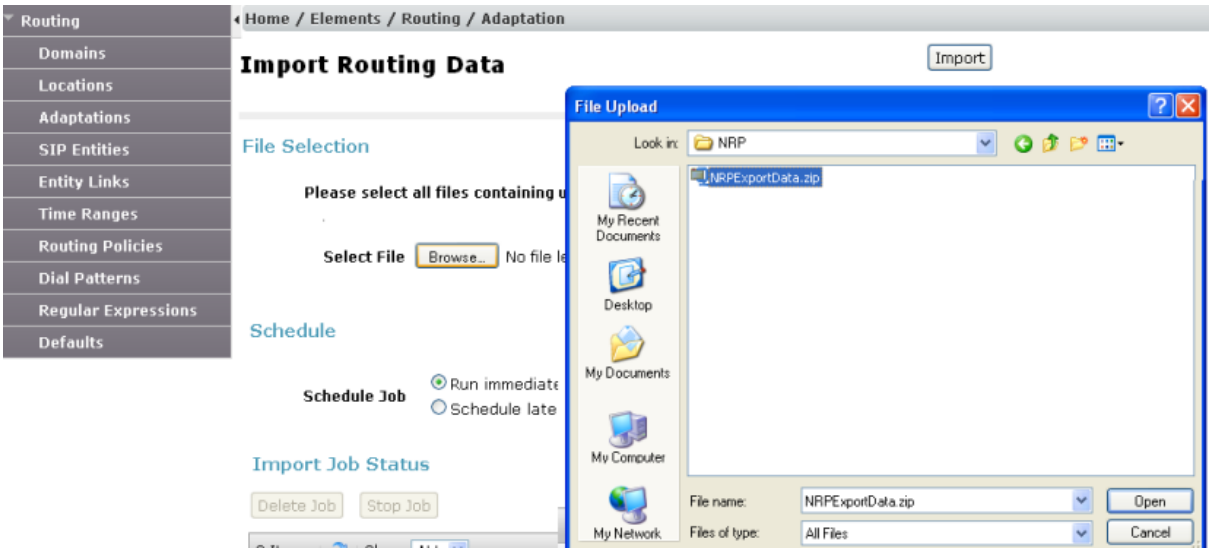
Perform this procedure on System Manager 5.2.x to import the System Manager data from Release 5.2, 5.2 SP1, or 5.2 SP2 to System Manager Release 7.0.1.

Procedure

1. On the Web browser, type `https://<fully qualified domain name of System Manager>/SMGR`.
2. Log on to System Manager Web Console using the administrator credentials made available at the time of the System Manager installation.
3. Click **Elements** > **Routing** > **Adaptations**.
4. On the Adaptations page, click **More Actions** > **Import**.

   The system displays the Import Routing Data page.

5. In the File Selection section, click Browse to open the `NRPExportData.zip` file.



6. To import the NRP data, click **Import**.
7. Verify that the NRP data is successfully imported to System Manager Release 7.0.1.
8. Create users, custom roles, and configuration information that you recorded from the System Manager web console of Release 5.2.x.

Chapter 8: Postupgrade Verification

Verifying the functionality of System Manager

About this task

Note:

To ensure that System Manager is operational after the upgrade, verify that the installation of System Manager is successful.

When you upgrade to System Manager Release 7.0 or later from release:

- 6.0.x or 6.1.x: For users with roles other than admin, the system resets the user passwords to the login name of the users.

  For example, after the migration, the system sets the password of a user with the login name dsmith@avaya.com and a role other than End-User to dsmith@avaya.com.

  The end user passwords in System Manager Release 6.2 and later remain the same as in Release 6.1.
- 6.0.x: The system resets the admin password.
- 6.1.x or later: The admin password remains unchanged.

When you promote an end user to an administrator, the system resets the password to the login name of the user.

Procedure

1. Type `https://<fully qualified domain name of System Manager>/SMGR` on the web browser to log on to the System Manager web console of the upgraded system.
2. Click the settings icon ( ), click **About**, and verify that the system displays the version number of System Manager with the highest build number for the release.
3. To verify if the system has generated any new call processing alarms during the System Manager upgrade, perform the following:
   a. Click **Services** > **Events**.
   b. In the left navigation pane, click **Events** > **Alarms**.
   c. On the Alarms page, in the **Alarms List** section, note the alarms that the system generated.

4. On the upgraded system, verify that the following data matches the number of users and roles that you recorded before the upgrade:
   - The number of users
   - The number of roles

   For information about managing users and managing roles, see *Administering Avaya Aura® System Manager for Release 7.0.1*.
5. Verify that the following function correctly:
   - Creation and deletion of a user
   - Creation of a role
   - Creation of a job
   - Creation of the remote data backup
   - Replication of the data by using Data Replication Service (DRS)

   For instructions to complete each verification task, see *Administering Avaya Aura® System Manager for Release 7.0.1*.

Creating a data backup on a remote server

Before you begin

Ensure that the backup server supports the required algorithms for the System Manager remote backup. For more information, see Supported ciphers, key exchange algorithms, and mac algorithms.

System Manager requires password authentication to enable the remote backup servers for successful backup.

Note:

System Manager does not support authentication mechanisms, such as Keyboard-Interactive and public key-based support.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - Perform the following:
     a. In the **File transfer protocol** field, click `SCP` or `SFTP`.
     b. Enter the remote server IP, remote server port, user name, password, and name and the path of the backup file that you create.

- Select the **Use Default** check box.

  Important:

  To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

5. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

Creating a Snapshot restore

About this task

Important:

Do not perform any activity on the System Manager virtual machine until the Snapshot restoration is complete.

You can restore the Snapshot backup using the vCenter or vSphere Client.

Procedure

1. Select the deployed System Manager virtual machine from the list of VMs, right-click and select **Snapshot**.
2. Open **Snapshot Manager**.
3. Select the Snapshot version that you want to restore.
4. Click **Goto**.
5. In the **Recent Tasks** window, verify the **Status** of the **Revert snapshot** task and wait until the system displays `Completed`.

Third-party certificate for upgrades

You must regenerate and reimport the third- party certificate for an upgrade from System Manager Release 6.2 or earlier to System Manager Release 7.0.1. This applies if System Manager uses third- party identity certificates before the upgrade. For System Manager and Session Manager replication, System Manager identity certificate must have the virtual fully qualified domain name (VFQDN) of System Manager in the Subject Alternative Name. If you upgrade System Manager to Release 7.0.1, the system retains the identity certificate that was used before the upgrade, but the

certificate does not have the VFQDN as the Subject Alternative Name. Therefore, replication to Session Manager stops when Session Manager systems in the environment are upgraded to Release 7.0.1.

Installing language pack on System Manager

About this task

After you install, upgrade, or apply a service or a feature pack, run the language pack to get the localization support for the French language.

Procedure

1. Log in to the System Manager command line interface as admin.
2. Run the command: **`#service jboss stop`**.
3. Once the system stops the JBoss service, run the command: **`sh $MGMT_HOME/CommonConsole/script/LocalizationScript.sh $MGMT_HOME/CommonConsole/localization/common_console/FrenchResourceBundle.zip`**.
4. If you are running the data migration through SSH connection, then do not close the SSH session or terminate the connection, otherwise the process gets killed and the installation fails.

   Note:

   During this activity, the system restarts the JBoss service, therefore, the System Manager Web console will not be accessible. If System Manager is in the Geographic Redundancy mode then apply these steps on the Secondary System Manager server also.

Chapter 9: Maintenance

Backup and restore the System Manager data

Creating a data backup on a remote server

Before you begin

Ensure that the backup server supports the required algorithms for the System Manager remote backup. For more information, see Supported ciphers, key exchange algorithms, and mac algorithms.

System Manager requires password authentication to enable the remote backup servers for successful backup.

Note:

System Manager does not support authentication mechanisms, such as Keyboard-Interactive and public key-based support.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - Perform the following:
     a. In the **File transfer protocol** field, click `SCP` or `SFTP`.
     b. Enter the remote server IP, remote server port, user name, password, and name and the path of the backup file that you create.
   - Select the **Use Default** check box.

     Important:

     To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click

Services > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

5. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

Creating a data backup on a local server

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local**.
4. In the **File name** field, enter the backup file that you want to create.
5. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

Restoring a backup from a remote server

About this task

Note:

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

To restore the original system at any point of time, you must restore the backup on the same release and the same software patch of that of the original System Manager. For example, if you have created a backup of System Manager xyz with 1234 software patch installed, System Manager on which you restore the backup must run xyz that has 1234 software patch installed.

If the System Manager release on which you restore the backup does not match, the restore operation fails.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Remote**.
4. To specify the file name for the restore operation, perform one of the following:
   - Click the Backup List tab, and select a file name.

Use this method if the path of the backup file on the remote server is valid, and the credentials used while creating the backup file is unaltered.

- Click the Parameterized Restore tab, enter a valid file name, the file transfer protocol, the remote server IP address, remote server port, user name, and the password to access the remote computer in the respective fields.

  Note:

  The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

- Click the Parameterized Restore tab, select the **Use Default** check box.

  Important:

  To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

5. Click **Restore**.

   On the Restore Confirmation page, the system displays the following message:

   ```
   The Restore operation will terminate all sessions and no services
   will be available until the operation completes. So, the System
   Manager console will not be available for approximately 45 minutes
   but this time may vary based on Database size. Click on Continue to
   go ahead with the Restore operation or click on Cancel to abort the
   operation.
   ```

6. Click **Continue**.

   The system logs you out of the System Manager web console and then shuts down.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Restoring data backup from a local server

About this task

Note:

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.

2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Local**.
4. In the **File name** field, type the file name that you must restore.

   If the file name does not appear in the list, specify the absolute path to the backup file and the file name that you must restore.

   Note:

   The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

5. Click **Restore**.

   On the Restore Confirmation page, the system displays the following message:

   ```
   The Restore operation will terminate all sessions and no services
   will be available until the operation completes. So, the System
   Manager console will not be available for approximately 45 minutes
   but this time may vary based on Database size. Click on Continue to
   go ahead with the Restore operation or click on Cancel to abort the
   operation.
   ```

6. Click **Continue**.

   The system logs you out of the System Manager web console and then shuts down.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Backup and Restore field descriptions

Name	Description
Operation	The type of operation. The values are: • Backup • Restore
File Name	• For the backup operation, the name of the backup file. • For the restore operation, the name of the backup file that was used for the restore.
Path	• For the backup operation, the path of the backup file.

Table continues…

Name	Description
	• For the restore operation, the path of the backup file that was used for the restore.
Status	The status of the backup or restore operation. The values are: • SUCCESS • FAILED • PLANNED • RUNNING
Status Description	The error details of the backup or restore operation that has failed.
Operation Time	The time of the backup or restore operation.
Operation Type	Defines whether the backup or restore operation is local or remote.
User	The user who performed the operation.

Button	Description
Backup	Opens the Backup page from where you can backup the System Manager data.
Restore	Opens the Restore page from where you can restore the data to System Manager.

Common upgrade procedures

Methods of System Manager OVA file deployment

You can deploy the System Manager OVA file by using one of the following:

- For Avaya-appliance deployments, the Solution Deployment Manager client

  For more information, see Deploying the System Manager OVA file by using the Solution Deployment Manager client.

- For customer Virtualized Environment, vSphere or vCentre

  For more information, see Deploying System Manager by using vSphere or Deploying System Manager by using vCenter.

Related links

Deploying an OVA file for an Avaya Aura application on page 107
Deploying the System Manager OVA file by using vSphere on page 129

Deploying the System Manager OVA file using vCenter on page 134

Virtual machine management

Virtual machine management

The VM Management link from Solution Deployment Manager provides the virtual machine management.

VM Management provides the following capabilities:

- Defines the physical location, Appliance Virtualization Platform or ESXi host, and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Supports password change, patch installation, restart, shutdown, and certificate validation of host. Also, enables and disables SSH on the host.
- Manages lifecycle of the OVA applications that are deployed on the ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.
- Deploys Avaya Aura® application OVAs on customer-provided Virtualized Environment and Avaya Aura® Virtualized Appliance environments.
- Removes the Avaya Aura® application OVAs that are deployed on a virtual machine.
- Configures application and networking parameters required for application deployments.
- Supports flexible footprint definition based on capacity required for the deployment of the Avaya Aura® application OVA.

You can deploy the OVA file on the virtual machine by using the System Manager Solution Deployment Manager and the Solution Deployment Manager client.

Related links

Certification validation on page 100

Managing the location

Viewing a location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. Click the Locations tab.

   The Locations section lists all locations.

Adding a location

About this task

You can define the physical location of the host and configure the location specific information. You can update the information later.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the Location tab, in the Locations section, click **New**.
3. In the New Location section, perform the following:
   a. In the Required Location Information section, type the location information.
   b. In the Optional Location Information section, type the network parameters for the virtual machine.
4. Click **Save**.

   The system displays the new location in the VM Management Tree section.

Related links

New and Edit location field descriptions on page 86

Editing the location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the Location tab, in the Locations section, select a location that you want to edit.
3. Click **Edit**.
4. In the Edit Location section, make the required changes.
5. Click **Save**.

Related links

New and Edit location field descriptions on page 86

Deleting a location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the Location tab, in the Locations section, select one or more locations that you want to delete.
3. Click **Delete**.
4. On the Delete confirmation dialog box, click **Yes**.

   The system does not delete the virtual machines that are running on the host, and moves the host to **Unknown location host mapping** > **Unknown location**.

VM Management field descriptions

Name	Description
Auto-Reload VM Management Tree	The option to automatically reload the VM Management Tree after the completion of operations such as refreshing virtual machines.

Locations

Name	Description
Location Name	The location name.
City	The city where the host is located.
Country	The country where the host is located.

Button	Description
New	Displays the New Location section where you can provide the details of the location that you want to add.
Edit	Displays the Edit Location section where you can change the details of an existing location.
Delete	Deletes the locations that you select. The system moves the hosts associated with the deleted locations to unknown location.

Hosts

Name	Description
Host Name	The name of the ESXi host.
Host IP	The IP address of the ESXi host.
Host FQDN	FQDN of the ESXi host.
vCenter IP/FQDN	The IP address or FQDN of vCentre.
Current Action	The operation that is currently being performed on the ESXi host.
Last Action	The last completed operation on the ESXi host.
License Status	The status of the license.
Host Version	The ESXi host version. The options are 5.5, 5.1, and 5.0. 6.0 only for VMware ESXi host.
Offer Type	The ESXi host type. The options are: • **AVP**: Appliance Virtualization Platform host • **Customer VE**: customer-provided VMware ESXi host

Table continues…

Name	Description
SSH Status	The SSH service status. The values are: • **enabled** • **disabled**
Host Certificate	The certificate status of the Appliance Virtualization Platform host. The values are: • ✔: The certificate is added in Solution Deployment Manager and correct. • ⊗: The certificate is not accepted or invalid. You can click **View** for details of the certificate status.
vCenter Certificate	The certificate status of the ESXi host. The values are: • ✔: The certificate is correct. The system enables all the options in **More Actions** that apply to VMware ESXi host. • ⊗: The certificate is not accepted or invalid. You can click **View** for details of the certificate status.

Note:

Depending on the Appliance Virtualization Platform host and vCenter certificate status, the system enables the options in **More Actions**.

Button	Description
Auto Refresh	The option to automatically refresh the page with the latest changes. For example, the page updates: • The VM state when a virtual machine changes • The license status or certificate status of host when host changes The system refreshes the data every minute.
Add	Displays the New Host section where you can provide the details of the host that you want to add.
Edit	Displays the Host Information section where you can change the details of an existing host.
Remove	Removes the hosts that you select. The system moves the hosts associated with the deleted locations to unknown location.

Table continues…

Button	Description
Change Network Params > **Change Host IP Settings**	Displays the Host Network/IP Settings section where you can change the host IP settings for the Appliance Virtualization Platform host.
Change Network Params > **Change Network Settings**	Displays the Host Network Setting section where you can change the network settings for the Appliance Virtualization Platform host.
Refresh	Refreshes the status of the hosts.
More Actions > **Change Password**	Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host.
More Actions > **Update**	Displays the Update host page where you can select the file for updating the Appliance Virtualization Platform host.
More Actions > **Enable SSH**	Enables SSH for the Appliance Virtualization Platform host. When SSH for the Appliance Virtualization Platform host is enabled, the system displays `SSH enabled successfully`.
More Actions > **Disable SSH**	Disables SSH on the Appliance Virtualization Platform host. When SSH for Appliance Virtualization Platform is disabled, the system displays `Disabling SSH for AVP host with <IP address> <FQDN>, <username>`.
More Actions > **Host Restart**	Restarts the host and virtual machines that are running on the Appliance Virtualization Platform host.
More Actions > **Host Shutdown**	Shuts down the host and virtual machines that are running on the Appliance Virtualization Platform host.
More Actions > **Generate/Accept Certificate**	Displays the Certificate dialog box where you can manage certificates for the host. Depending on the host type, the options are: • **Generate Certificate**: To generate certificate for Appliance Virtualization Platform host only. • **Accept Certificate**: To accept a valid certificate for the host or vCenter. • **Decline Certificate**: To decline the certificate for Appliance Virtualization Platform host only. You must regenerate the certificate and accept if you decline a host certificate.

Virtual Machines

Name	Description
VM Name	The name of the virtual machine.
VM IP	The IP address of the virtual machine.
VM FQDN	FQDN of the virtual machine.
VM App Name	The name of the application virtual machine . For example, Session Manager.
VM App Version	The version of the application virtual machine. For example, 7.0.0.0.
VM State	The state of the virtual machine. The states are **Started** and **Stopped**.
Current Action Status	The status of the current operation. The statuses are: • **Deploying** • **Starting** • **Stopping** The **Status Details** link provides the details of the operation in progress.
Last Action	The last action performed on the virtual machine.
Host Name	The hostname of the VMware host or Appliance Virtualization Platform host
Trust Status	The status of the connection between System Manager and the virtual machine. The status can be **Success** or **Failed**. When the connection between System Manager and the virtual machine establishes, **Trust Status** changes to **Success**. Only when the trust status is **Success**, you can perform other operations.
Data Store	The data store with the available size.

Button	Description
New	Displays the VM Deployment section where you can provide the host and deploy an application.
Edit	Displays the VM Deployment section where you can change the details of a virtual machine.
Delete	Turns off the virtual machines and deletes the selected virtual machines.
Start	Starts the selected virtual machines.

Table continues…

Button	Description
Stop	Stops the selected virtual machines.
Show Selected	Displays only the selected virtual machines.
More Actions > **Restart**	Starts the selected virtual machines that were stopped earlier.
More Actions > **Refresh VM**	Updates the status of the virtual machines.
More Actions > **Reestablish Connection**	Establishes the connection between System Manager and the virtual machine. When the connection between System Manager and the virtual machine establishes, the **Trust Status** changes to **Success**.
More Actions > **Update Static Routing**	Displays the VM Update Static Routing section where you can update the IP address of Utility Services for static routing.

New and Edit location field descriptions

Required Location Information

Name	Description
Name	The location name.
Avaya Sold-To #	The customer contact number. Administrators use the field to check entitlements.
Address	The address where the host is located.
City	The city where the host is located.
State/Province/Region	The state, province, or region where the host is located.
Zip/Postal Code	The zip code of the host location.
Country	The country where the host is located.

Optional Location Information

Name	Description
Default Gateway	The IP address of the virtual machine gateway. For example, 172.16.1.1.
DNS Search List	The search list of domain names.
DNS Server 1	The DNS IP address of the primary virtual machine. For example, 172.16.1.2.
DNS Server 2	The DNS IP address of the secondary virtual machine. For example, 172.16.1.4.
NetMask	The subnetwork mask of the virtual machine.
NTP Server	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).

Button	Description
Save	Saves the location information and returns to the Locations section.
Edit	Updates the location information and returns to the Locations section.
Delete	Deletes the location information, and moves the host to the Unknown location section.
Cancel	Cancels the add or edit operation, and returns to the Locations section.

Managing the host

Adding an ESXi host

About this task

Use the procedure to add an Appliance Virtualization Platform or ESXi host. You can associate an ESXi host with an existing location.

Before you begin

A location must be available.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Hosts for Selected Location <location name> section, click **New**.
4. In the New Host section, provide the following:

   Host name, IP address, user name, and password.
5. Click **Save**.
6. On the Certificate dialog box, click **Accept Certificate**.

   The system generates the certificate and adds the Appliance Virtualization Platform host. For the ESXi host, you can only accept the certificate. If the certificate is invalid, to generate certificate, see the VMware documentation.

   In the VM Management Tree section, the system displays the new host in the specified location. The system also discovers applications.
7. To view the discovered application details, such as name and version, establish trust between the application and System Manager using the following:
   a. Click **More Actions** > **Re-establish connection**.
   b. Click **Refresh VM**.

Important:

When you change the IP address or FQDN of the Appliance Virtualization Platform host from the local inventory, you require Utility Services. To get the Utility Services application name during the IP address or FQDN change, refresh Utility Services to ensure that Utility Services is available.

Related links

New and Edit host field descriptions on page 97
Generating and accepting certificates on page 101

Editing an ESXi host

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Hosts for Selected Location <location name> section, select an ESXi host that you want to update.
4. Change the ESXi host information.
5. Click **Save**.

   The system updates the ESXi host information.

Related links

New and Edit host field descriptions on page 97

Installing the Appliance Virtualization Platform patch from Solution Deployment Manager

About this task

Install the Release 7.0.1 feature pack on the existing Appliance Virtualization Platform Release 7.0 by using the Solution Deployment Manager client or System Manager Solution Deployment Manager.

Note:

From System Manager Solution Deployment Manager, you cannot update an Appliance Virtualization Platform that hosts this System Manager.

Do not use this procedure for installing the Appliance Virtualization Platform patch on an S8300D server.

Before you begin

1. Add a location.
2. Add a host.
3. Enable the SSH service on the Appliance Virtualization Platform host.
4. Stop all virtual machines that are running on the Appliance Virtualization Platform host.

Note:

Install only Avaya-approved service packs or software patches on Appliance Virtualization Platform. Do not install the software patches that are downloaded directly from VMware®.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the **Host** tab, in the Hosts for Selected Location <location name> section, select the Appliance Virtualization Platform host, and click **More Actions** > **Update**.
4. On the Update Host page, click **Select patch from local SDM client machine**.
5. In **Select patch file**, provide the absolute path to the patch file of the host, and click **Update Host**.

   For example, the absolute path on your computer can be `/tmp/avp/avaya-avp-7.0.0.1.0.5.zip`.

   In the Hosts for Selected Location <location name> section, the system displays the update status in the **Current Action** column.
6. To view the details, in the **Current Action** column, click **Patching**.

   Host Patching Status window displays the details. The patch installation takes some time. When the patch installation is complete, the **Current Action** column displays the status.

Next steps

If virtual machines that were running on the Appliance Virtualization Platform host does not automatically start, manually start the machines.

Related links

Update field descriptions on page 100

Changing the network parameters for an Appliance Virtualization Platform host

About this task

Use this procedure to change the network parameters of Appliance Virtualization Platform after deployment. You can change network parameters only for the Appliance Virtualization Platform host.

Note:

If you are connecting to Appliance Virtualization Platform through the public management interface, you might lose connection during the process. Therefore, after the IP address changes, close Solution Deployment Manager, and restart Solution Deployment Manager by using the new IP address to reconnect.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.

2. In VM Management Tree, select a location.
3. On the Host tab, in the Hosts for Selected Location <location name> section, select an ESXi host and click **Change Network Params** > **Change Host IP Settings**.
4. In the Host Network/ IP Settings section, change the IP address, subnetmask, and other parameters as appropriate.

   Note:

   An Appliance Virtualization Platform host and all virtual machines running on the host must be on the same subnet mask.

   If Out of Band Management is configured in an Appliance Virtualization Platform deployment, you need two subnet masks, one for each of the following:

   - Public or signaling traffic, Appliance Virtualization Platform, and all virtual machines public traffic.
   - Management, Appliance Virtualization Platform, and all virtual machine management ports.

5. To change the gateway IP address, perform the following:
   a. Click **Change Gateway**.

      The **Gateway** field becomes available for providing the IP address.

   b. In **Gateway**, change the IP address.
   c. Click **Save Gateway**.
6. Click **Save**.

   The system updates the Appliance Virtualization Platform host information.

Related links

Change Network Parameters field descriptions on page 98

Changing the network settings for an Appliance Virtualization Platform host from Solution Deployment Manager

About this task

With Appliance Virtualization Platform, you can team NICs together to provide a backup connection when the server NIC or the Ethernet switch fails. You can also perform NIC teaming from the command line on Appliance Virtualization Platform.

Appliance Virtualization Platform supports Active-Standby and Active-Active modes of NIC teaming. For more information, see “NIC teaming modes”.

Note:

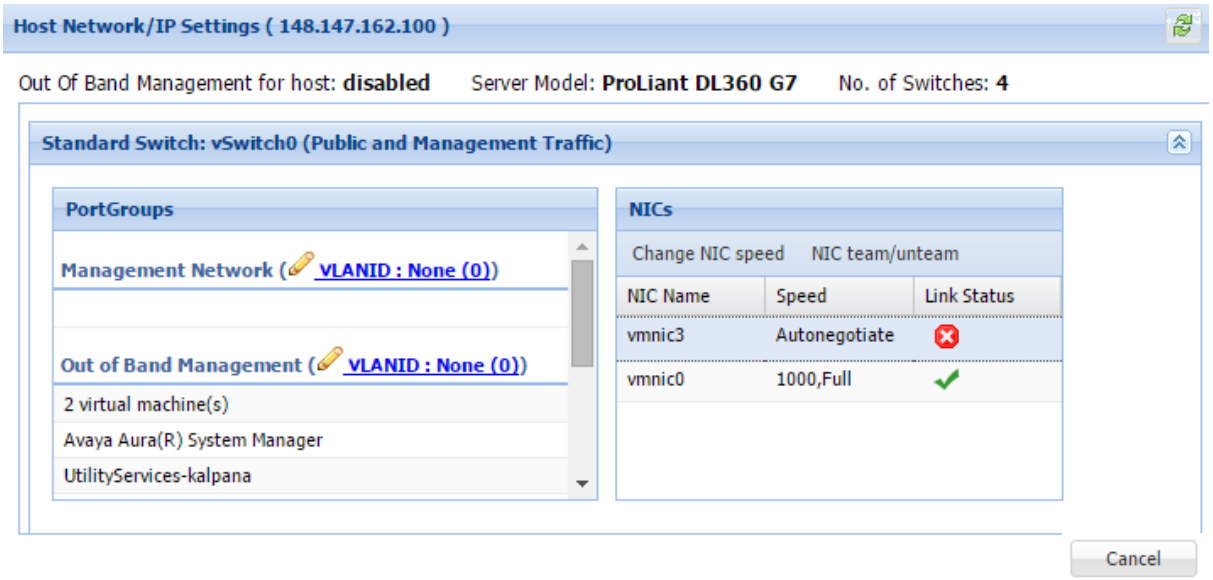
- If you add a host with service port IP address in Solution Deployment Manager and change the IP address of the host to the public IP address by using Host Network/ IP Settings, the system updates the public IP address in the database. Any further operations that you perform on the host fails because public IP address cannot be reached with the service port. To avoid this error, edit the host with the service port IP address again.

- If FQDN of the Appliance Virtualization Platform host is updated by using Host Network/IP setting for domain name, refresh the host to get the FQDN changes reflect in Solution Deployment Manager.

Use this procedure to change network settings, such as changing VLAN ID, NIC speed, and NIC team and unteaming for an Appliance Virtualization Platform host.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Host for Selected Location <location name>, select an Appliance Virtualization Platform host.
4. Click **Change Network params** > **Change Network Settings**.



The Host Network/ IP Settings page displays the number of switches as 4.

You can configure port groups for the following switches:

- **vSwitch0**, reserved for the Public and Management traffic.
- **vSwitch1**, reserved for services port. You cannot change the values.
- **vSwitch2**, reserved for Out of Band Management.
- **vSwitch3**. No reservations.

5. To change VLAN ID, perform the following:
   a. To expand the Standard Switch: vSwitch<n> section, click .

      The section displays the vSwitch details.

   b. Click on the VLANID link or the edit icon ( ).

The system displays the Port Group Properties page where you can edit the VLAN ID port group property.

c. In **VLAN ID**, select an ID from the available values.

For more information about the value, see NIC teaming.

d. Click **OK**.

The system displays the new VLAN ID.

Note:

You can change the services port VLAN ID for S8300D servers only through Solution Deployment Manager.

6. To change the NIC speed, perform the following:
   a. Ensure that the system displays a vmnic in the **NIC Name** column.
   b. Click **Change NIC speed**.

      The system displays the selected vmnic dialog box.
   c. In **Configured speed, Duplex**, click a value.
   d. Click **OK**.

      For more information, see VLAN ID assignment.

   The system displays the updated NIC speed in the **Speed** column.

   If the NIC is connected, the system displays ✔ in **Link Status**.

   Note:

   You can change the speed only for common servers. You cannot change the speed for S8300D and S8300E servers.

7. To change the NIC teaming, perform the following:
   a. Select a vmnic.
   b. Click **NIC team/unteam**.

      The system displays the Out of Band Management Properties page.
   c. To perform NIC teaming or unteaming, select the vmnic and click **Move Up** or **Move Down** to move the vmnic from **Active Adapters**, **Standby Adapters**, or **Unused Adapters**.

      For more information, see NIC teaming modes.
   d. Click **OK**.

      The vmnic teams or unteams with **Active Adapters**, **Standby Adapters**, or **Unused Adapters** as required.
   e. To check the status of the vmnic, click **NIC team/ unteam**.
8. To get the latest data on host network IP settings, click **Refresh**.

The system displays the current status of the vmnic.

Note:

You cannot perform NIC teaming for S8300D and S8300E servers.

Related links

Host Network / IP Settings field descriptions on page 99

Changing the password for an Appliance Virtualization Platform host

About this task

You can change the password only for the Appliance Virtualization Platform host. This is the password for the user that you provide when adding the Appliance Virtualization Platform host.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Hosts for Selected Location <location name> section, select an ESXi host and click **More Actions** > **Change Password**.
4. In the Change Password section, enter the current password and the new password.

   For more information about password rules, see “Password policy”.
5. Click **Change Password**.

   The system updates the password of the Appliance Virtualization Platform host.

Related links

Password policy on page 93
Change Password field descriptions on page 100

Password policy

The password must meet the following requirements:

- Must contain at least eight characters.
- Must contain at least one of each: an uppercase letter, a lowercase letter, a numerical, and a special character.
- Must not contain an uppercase letter at the beginning and a digit or a special character at the end.

Examples of invalid passwords:

- Password1: Invalid. Uppercase in the beginning and a digit at the end.
- Password1!: Uppercase in the beginning and a special character at the end.

Example of a valid password: myPassword!1ok

If the password does not meet the requirements, the system prompts you to enter a new password. Enter the existing password and the new password in the correct fields.

Ensure that you keep the root password safe. You need the password while adding the host to Solution Deployment Manager and for troubleshooting.

Related links

Changing the password for an Appliance Virtualization Platform host on page 93

Enabling and disabling SSH on Appliance Virtualization Platform from Solution Deployment Manager

About this task

For security purpose, SSH access to Appliance Virtualization Platform shuts down in the normal operation. You must enable the SSH service on Appliance Virtualization Platform from Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. Select an Appliance Virtualization Platform host.
4. To enable SSH, click **More Actions** > **Enable SSH**.

   The system displays `enabled` in the **SSH status** column.
5. To disable SSH, click **More Actions** > **Disable SSH**.

   The system displays `disabled` in the **SSH status** column.

Enabling and disabling SSH on Appliance Virtualization Platform from System Manager CLI

About this task

For security purpose, SSH access to Appliance Virtualization Platform shuts down in the normal operation. You must enable the SSH service on Appliance Virtualization Platform.

You can enable SSH, disable SSH, and check the SSH status on the Appliance Virtualization Platform host.

Before you begin

Start an SSH session.

Procedure

1. Log in to the System Manager command line interface as root.
2. Navigate to the `$MGMT_HOME/infra/bin/avpSSHUtility` location.
3. Type `./enableDisableSSHOnAVP.sh`.

   The system displays the following options:

   - Enable SSH on the Appliance Virtualization Platform host.
   - Disable SSH on the Appliance Virtualization Platform host.

- Check the SSH status on the Appliance Virtualization Platform host.

4. To enable SSH, perform the following:
   a. At the prompt, type `1` and press `Enter`.
   b. Type the IP address of the Appliance Virtualization Platform host.
   c. Type the time in minutes.

      The time is the duration after which the system blocks any new SSH connections. The valid range 10 to 120 minutes.

      The system displays the message and enables SSH on Appliance Virtualization Platform host.

   For example, if you set the time to 50 minutes, after 50 minutes, the system blocks any new SSH connections. If you reenable SSH before completion of 50 minutes, the system adds 50 minutes to the initial 50 minutes to reenable connections.
5. To disable SSH, perform the following:
   a. At the prompt, type `2` and press `Enter`.
   b. Type the IP address of the Appliance Virtualization Platform host.

   If SSH is already disabled, the system displays `False` and the message `SSH is already disabled. No operation performed. Exiting`.
6. **(Optional)** To view the status of SSH, perform the following:
   a. At the prompt, type `3` and press `Enter`.
   b. Type the IP address of the Appliance Virtualization Platform host.

   If SSH is enabled, the system displays `Is SSH enable – false`.

   If SSH is disabled, the system displays `Is SSH disable – true`.

Changing the IP address and default gateway of the host

About this task

When you change the default gateway and IP address from the vSphere, the change might be unsuccessful.

You cannot remotely change the IP address of the Appliance Virtualization Platform host to a different network. You can change the IP address remotely only within the same network.

To change the Appliance Virtualization Platform host to a different network, perform Step 2 or Step 3.

Before you begin

Connect the computer to the services port.

Procedure

1. Using an SSH client, log in to the Appliance Virtualization Platform host.

2. Connect the Solution Deployment Manager client to services port on the Appliance Virtualization Platform host, and do the following:

   a. To change the IP address, at the command prompt of the host, type the following:

   ```
   esxcli network ip interface ipv4 set -i vmk0 -I <old IP address of the host> -
   N <new IP address of the host> -t static
   ```

   For example:

   ```
   esxcli network ip interface ipv4 set -i vmk0 -I 135.27.162.121 -N 255.255.25
   5.0 -t static
   ```

   b. To change the default gateway, type `esxcfg-route <new gateway IP address>`.

   For example:

   ```
   esxcfg-route 135.27.162.1
   ```

3. Enable SSH on the Appliance Virtualization Platform host and run the **`./serverInitialNetworkConfig`** command.

   For more information, see Configuring servers preinstalled with Appliance Virtualization Platform.

Shutting down the Appliance Virtualization Platform host

About this task

You can perform the shutdown operation on one Appliance Virtualization Platform host at a time. You cannot schedule the operation.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Host for Selected Location <location name>, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Host Shutdown**.

   The Appliance Virtualization Platform host and virtual machines shut down.

Restarting the Appliance Virtualization Platform host

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Host for Selected Location <location name>, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Host Restart**.

   The system restarts the Appliance Virtualization Platform host and virtual machines.

Deleting an ESXi host

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the Host tab, in the Hosts for Selected Location <location name> section, select one or more hosts that you want to delete.
3. Click **Delete**.
4. On the Delete confirmation page, click **Yes**.

Mapping the ESXi host to an unknown location

About this task

When you delete a location, the system does not delete the virtual machines running on the host, and moves the host to **Unknown location host mapping** > **Unknown location**. You can configure the location of an ESXi host again.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In the left navigation pane, click the **Unknown location host mapping** link.
3. In the Host Location Mapping section, select an ESXi host and click **Edit**.

   The system displays the Host Information page.
4. Select a location to which you want to map the ESXi host.
5. Click **Submit**.

   The system displays the ESXi host in the selected location.

New and Edit host field descriptions

Name	Description
Location	The location where the host is availabe. The field is read only.
Host Name	The hostname of Appliance Virtualization Platform or the ESXi host. For example, smgrdev.
Host FQDN or IP	The IP address or FQDN of Appliance Virtualization Platform or the ESXi host.
User Name	The user name to log in to Appliance Virtualization Platform or the ESXi host.

Table continues…

Name	Description
	Note: For Appliance Virtualization Platform, provide the root login and password that you configured in the spreadsheet.
Password	The password to log in to Appliance Virtualization Platform or the ESXi host.

Button	Description
Save	Saves the host information and returns to the Hosts for Selected Location <location name> section.

Change Network Parameters field descriptions

Network Parameters

Name	Description
Name	The name of the Appliance Virtualization Platform host. The field is display-only.
IP	The IP address of the Appliance Virtualization Platform host
Subnet Mask	The subnet mask the Appliance Virtualization Platform host
Host Name	The host name the Appliance Virtualization Platform host
Domain Name	The domain name the Appliance Virtualization Platform host
Preferred DNS Server	The preferred DNS server
Alternate DNS Server	The alternate DNS server
Gateway	The gateway IP address. The field is available only when you click **Change Gateway**.

Button	Description
Change Gateway	Makes the **Gateway** field available, and displays **Save Gateway** and **Cancel Gateway Change** buttons.
Save Gateway	Saves the gateway IP address value that you provide.
Cancel Gateway Change	Cancels the changes made to the gateway.

Button	Description
Save	Saves the changes that you made to network parameters.

Host Network / IP Settings field descriptions

Port Groups

Standard Switch vSwitch <n> displays the Port Groups and NICs sections.

Name	Description
or **VLAN ID** link	Displays the Port Group Properties page where you configure VLAN ID.
VLAN ID	Displays the VLAN ID. The options are: • **None (0)** • **1 to 4093** The field displays only unused IDs.
OK	Saves the changes.

NIC speed

Button	Description
Change NIC speed	Displays the vmnic<n> dialog box.

Name	Description
Configured speed, Duplex	Displays the NIC speed. The options are: • **Autonegotiate** • **10,Half** • **10,Full** • **100,Half** • **100,Full** • **1000,Full**
OK	Saves the changes.

NIC teaming

Button	Description
NIC team/unteam	Displays the Out of Band Management Properties vSwitch<n> dialog box.

Button	Description
Move Up	Moves the VMNIC from unused adapters to standby or active adapters or from standby to active adapter.
Move Down	Moves the VMNIC from active to standby adapter or from standby to unused adapter.
Refresh	Refreshes the page.
OK	Saves the changes.

Change Password field descriptions

Name	Description
Current Password	The password for the user you input when adding the host.
New Password	The new password
Confirm New Password	The new password

Button	Description
Change Password	Saves the new password.

Update field descriptions

Name	Description
Patch location	The location where the Appliance Virtualization Platform patch is available. The options are: • **Select Patch from Local SMGR**: To use the Appliance Virtualization Platform patch that is available on the local System Manager. • **Select Patch from software library**: To use the Appliance Virtualization Platform patch that is available in the software library.
Select patch file	The absolute path to the Appliance Virtualization Platform patch file.

Button	Description
Update Host	Installs the patch on the Appliance Virtualization Platform host.

Certificate validation

Certification validation

With System Manager Solution Deployment Manager and Solution Deployment Manager client, you can enable a certificate-based TLS connection between the Solution Deployment Manager service and a host that is running Avaya Aura® 7.x applications. This enables to establish secure communications between System Manager Solution Deployment Manager or the Solution Deployment Manager client and Appliance Virtualization Platform or ESXi hosts.

The certificate-based sessions apply to the Avaya Aura® Virtualized Appliance offer using host self-signed certificates and the customer-provided Virtualization Environment using host self-signed or third party certificates.

You can check the following with certificate based TLS sessions:

- Certificate valid dates
- Origin of Certificate Authority
- Chain of Trust

- CRL or OCSP state
- Log Certificate Validation Events

Solution Deployment Manager checks the certificate status of hosts. If the certificate is incorrect, Solution Deployment Manager does not connect to the host.

For the correct certificate:

- The fully qualified domain or IP address of the host to which you are connecting must match the value in the certificate and the certificate must be in date.
- Appliance Virtualization Platform and VMware ESXi hosts do not automatically regenerate their certificates when host details such as IP address or hostname and domain changes. The certificate might become incorrect for the host.

If the certificate is incorrect:

- For the Appliance Virtualization Platform host, Solution Deployment Manager regenerates the certificate on the host and then uses the corrected certificate for the connection.
- For the VMware ESXi host or vCenter, the system denies connection. The customer must update or correct the certificate on the host or vCenter.

  For more information about updating the certificate, see “Updating the certificate on the ESXi host from VMware”.

Note:

Solution Deployment Manager:

- Validates certificate of vCenter
- Does not validate certificates for hosts that vCenter manages

With Solution Deployment Manager, you can only accept certificate while adding vCenter. If a certificate changes, the system gives a warning that the certificate does not match the certificate in the trust store on Solution Deployment Manager. You must get a new certificate, accept the certificate as valid, and save the certificate on the system.

To validate certificates, you can directly log on to the host and confirm that the details in the `/etc/vmware/ssl/rui.crt` file match the details displayed on the screen.

Generating and accepting certificates

About this task

With Solution Deployment Manager, you can generate certificates only for Appliance Virtualization Platform hosts.

For the VMware ESXi hosts, if the certificate is invalid:

- Get a correct certificate for the host and add the certificate.
- Regenerate a self-signed certificate on the host.

  For more information, see “Generating new self-signed certificates for the ESXi host”.

Before you begin

Require permissions to add a host to generate certificates.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Host for Selected Location <location name>, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Generate/Accept Certificate**.
5. On the Certificate window, do the following:
   a. Click **Generate Certificate**.

      Note:

      You can generate certificate only for the Appliance Virtualization Platform host.

   b. Click **Accept Certificate**.

   In the Hosts for Selected Location <location name> section, the **Host Certificate** column must display ✔.

Next steps

If the system displays an SSL verification error when you gain access to the Appliance Virtualization Platform host from the vSphere client, restart the Appliance Virtualization Platform host.

Related links

Adding an ESXi host on page 87
Generating new self-signed certificates for the ESXi host on page 104

Updating the certificate on the ESXi host from VMware

About this task

Use the procedure to update the ESXi host certificate.

For information about updating vCenter certificates, see the VMware documentation.

Before you begin

Start an SSH session on the ESXi host.

Procedure

1. Start vSphere client, and log in to the ESXi host as admin or root user.
2. Ensure that the domain name and the hostname of the ESXi host is set correctly and matches the FQDN that is present on the DNS servers, correct the entries to match if required.

   For security reason, the common name in the certificate must match the hostname to which you connect.
3. To generate new certificates, type `/sbin/generate-certificates`.

The system generates and installs the certificate.

4. Restart the ESXi host.
5. **(Optional)** Do the following:
   a. Move the ESXi host to the maintenance mode.
   b. Install the new certificate.
   c. From the Direct Console User Interface (DCUI), restart management agents.

Note:

The host certificate must now match the fully qualified domain name of the host.

VMware places only FQDN in certificates that are generated on the host. Therefore, use a fully qualified domain name to connect to ESXi hosts and vCenter from Solution Deployment Manager.

Appliance Virtualization Platform places an IP address and FQDN in generated certificates. Therefore, from Solution Deployment Manager, you can connect to Appliance Virtualization Platform hosts through IP address or FQDN.

The connection from Solution Deployment Manager 7.0.1 to a vCenter or ESXi host by using an IP address fails because the IP address is absent in the certificate and the connection is not sufficiently secure.

Related links

Generating new self-signed certificates for the ESXi host on page 104

Managing certificates for existing hosts

About this task

By default, the certificate status of the host or vCenter that is migrated from earlier release is invalid. To perform any operation on the host from Solution Deployment Manager, you require a valid certificate. Therefore, you must get the valid certificate and accept the certificate.

Depending on the host type and the validity of the certificate, use appropriate steps to generate the certificate, and then accept the certificate.

Before you begin

Require permissions to add a host to generate certificates.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Host for Selected Location <location name>, select a host.
4. **(Optional)** On an Appliance Virtualization Platform host, click **More Actions** > **Generate/ Accept Certificate**, and on the Certificate dialog box, do one of the following:
   - If the certificate is valid, click **Accept Certificate**.

- If the certificate is invalid, click **Generate Certificate**, and then click **Accept Certificate**.

5. For the ESXi host, do one of the following:
   - If the certificate is valid, on the Certificate dialog box, click **More Actions** > **Generate/ Accept Certificate**, and click **Accept Certificate**.
   - If the certificate is invalid, log in to the ESXi host, validate the certificate, and then from Solution Deployment Manager, accept the certificate.

     For more information, see “Generating new self-signed certificates for the ESXi host”.
6. For vCenter, do the following:
   a. Click **Map vCenter**, select the vCenter server, and click **Edit**.
   b. In the Certificate dialog box, accept certificate, and click **Save**.

Related links

Generating new self-signed certificates for the ESXi host on page 104
Generating and accepting certificates on page 101

Generating new self-signed certificates for the ESXi host

About this task

Generate new certificates only if you change the host name or accidentally delete the certificate. Under certain circumstances, you must force the host to generate new certificates.

To receive the full benefit of certificate checking, particularly if you want to use encrypted remote connections externally, do not use a self-signed certificate. Instead, install new certificates that are signed by a valid internal certificate authority or purchase a certificate from a trusted security authority.

Before you begin

Start an SSH session on the ESXi host.

Procedure

1. Log in to the ESXi host as an admin user.
2. To create a backup of any existing certificates, in the `/etc/vmware/ssl` directory, rename the certificates by using the following commands:

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

   Note:

   Do not perform the step if you are regenerating certificates because you deleted the certificates.
3. To generate new certificates, type `/sbin/generate-certificates`.
4. Restart the ESXi host.

   The generation process places the certificates places in the correct location.

5. **(Optional)** Do the following:
   a. Move the ESXi host to the maintenance mode.
   b. Install the new certificate.
   c. Restart management agents from Direct Console User Interface (DCUI).
6. Do the following to confirm that the host successfully generated new certificates:
   a. Type `ls -la`.
   b. Compare the time stamps of the new certificate files with `orig.rui.crt` and `orig.rui.key`.

Next steps

Replace the self-signed certificate and the key with a trusted certificate and key.

Managing the virtual machine

Deploying the Utility Services OVA file

About this task

Use the procedure to create a virtual machine on the ESXi host, and deploy Utility Services OVA on the Avaya-provided server.

To deploy Utility Services, you can use Solution Deployment Manager from System Manager or the Solution Deployment Manager client, when System Manager is unavailable. Deploy Utility Services first, install the Release 7.0.1 feature pack, and then deploy all other applications one at a time.

Before you begin

- Complete the deployment checklist.

  For information about the deployment checklist, see *Deploying Avaya Aura® applications from System Manager*.
- Add a location.
- Add Appliance Virtualization Platform or an ESXi host to the location.
- Download the required OVA file to System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click **New**.

   The system displays the VM Deployment section.
4. In the Select Location and Host section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Host**, select a host.

c. In **Host FQDN**, type the virtual machine name.

5. In **Data Store**, select a data store.

   The page displays the capacity details.

6. Click **Next**.

7. In the Deploy OVA section, perform the following:

   a. In **Select Software Library**, select the local or remote library where the OVA file is available.

      If you are deploying the OVA from the Solution Deployment Manager client, you can use the default software library that is set during the client installation.

   b. In **Select OVAs**, select the OVA file that you want to deploy.

   c. In **Flexi Footprint**, select the footprint size that the application supports.

      - **S8300D**: Due to the limited resources available on S8300D, the only footprint option is minimal
      - **Default**: For all other server platforms.

8. Click **Next**.

   In Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to the application that you deploy.

9. In the Network Parameters section, ensure that the following fields are preconfigured:

   - **Public**
   - **Services**: Only for Utility Services
   - **Out of Band Management**: Only if Out of Band Management is enabled

   For more information, see “VM Deployment field descriptions”.

10. In the Configuration Parameters section, complete the fields.

    For more information about Configuration Parameters, see Network Parameters and Configuration Parameters field descriptions.

11. Click **Deploy**.

12. Click **Accept the license terms**.

    In the Hosts for Selected Location <location name> section, the system displays the deployment status in the **Current Action Status** column.

    The system displays the virtual machine on the VMs for Selected Location <location name> page.

13. To view details, click the **Status Details** link.

    For information about VM Management field descriptions, see *Deploying Avaya Aura®* *applications from System Manager*.

14. Install the Release 7.0.1 feature pack.

15. Reboot the Utility Services virtual machine.

Next steps

1. Deploy System Manager and install the Release 7.0.1 feature pack.
2. To activate the serviceability agent registration, reset the Utility Services virtual machine.
3. Deploy all other Avaya Aura® applications one at a time.

Related links

VM Deployment field descriptions on page 115
Network Parameters and Configuration Parameters field descriptions

Deploying an OVA file for an Avaya Aura® application

About this task

Use the procedure to create a virtual machine on the ESXi host, and deploy OVA for an Avaya Aura® application on the virtual machine.

To deploy an Avaya Aura® application, you can use Solution Deployment Manager from System Manager or the Solution Deployment Manager client if System Manager is unavailable.

Deploy Utility Services first, and then deploy all other applications one at a time.

Before you begin

- Add a location.
- Add Appliance Virtualization Platform or an ESXi host to the location.
- Ensure that the certificate is valid on the Appliance Virtualization Platform host or vCentre if used.
- Download the required OVA file to System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click **New**.

   The system displays the VM Deployment section.
4. In the Select Location and Host section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Host**, select a host.
   c. In **Host FQDN**, type the virtual machine name.
5. In **Data Store**, select a data store.

   The page displays the capacity details.
6. Click **Next**.

7. In the Deploy OVA section, do the following:
   a. In **Select Software Library**, select the local or remote library where the OVA file is available.

      To deploy the OVA by using the Solution Deployment Manager client, you can use the default software library that is set during the client installation.
   b. In **Select OVAs**, select the OVA file that you want to deploy.
   c. In **Flexi Footprint**, select the footprint size that the application supports.
8. Click **Next**.

   In Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to the application that you deploy.
9. In the Network Parameters section, ensure that the following fields are preconfigured:
   - **Public**
   - **Services**: Only for Utility Services
   - **Out of Band Management**: Only if Out of Band Management is enabled

   For more information, see “VM Deployment field descriptions”.
10. In the Configuration Parameters section, complete the fields.

    For each application that you deploy, fill the appropriate fields. For more information, see “VM Deployment field descriptions”.
11. Click **Deploy**.
12. Click **Accept the license terms**.

    In the Hosts for Selected Location <location name> section, the system displays the deployment status in the **Current Action Status** column.

    The system displays the virtual machine on the VMs for Selected Location <location name> page.
13. To view details, click **Status Details**.

Next steps

Install the Release 7.0.1 patch file for the Avaya Aura® application.

Related links

Installing software patches on page 23
VM Deployment field descriptions on page 115

Installing software patches

About this task

Use the procedure to install software patches, service packs, and feature packs that are entitled for an Avaya Aura® application, and commit the patches that you installed.

Before you begin

- Perform the preupgrade check.
- If you upgrade an application that was not deployed from Solution Deployment Manager:
  1. Select the virtual machine.
  2. To establish trust, click **More Actions** > **Re-establish Connection**.
  3. Click **Refresh VM**.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.

   Note:

   If an application is unreachable, the auto commit operation might fail and the Update Patch Status window displays a warning message. You must wait for some time, select the same patch in the Installed Patches section, and perform the commit operation again.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. Click **Save**.
11. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

    If the field displays , review the information on the Edit Upgrade Configuration page.
12. Click **Upgrade**.
13. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
14. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display .
15. To view the update status, click .

The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.

When the update is complete, the **Update status** and **Last Action Status** fields displays .

16. Click **Upgrade Actions** > **Installed Patches**.
17. On the Installed Patches page, in the Patch Operation section, click **Commit**.

    The page displays all software patches that you can commit.

    You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.
18. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

    You can schedule to commit the patch at a later time by using the **Schedule later** option.
19. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.
20. Ensure that **Update status** and **Last Action Status** fields display .

Editing a virtual machine

Before you begin

- Install the Solution Deployment Manager client.
- An ESXi host must be available.
- When you change the IP address or FQDN:
  - Utility Services must be available and must be discovered.
  - If Utility Services is discovered, the system must display Utility Services in the **VM App Name** column. If the application name in **VM App Name** is empty, perform the following to establish trust between the application and System Manager:
    - Click **More Actions** > **Re-establish connection**.
    - Click **More Actions** > **Refresh VM**.

Procedure

1. To start the Solution Deployment Manager client, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client** or the SDM icon ( ) on the desktop.
2. In VM Management Tree, select a location.
3. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select a virtual machine, and click **Edit**.

   The system displays the Edit VMs section.
4. **(Optional)** Click **Change Flexi Footprint** and do the following:
   a. Click **Change flexi foot print value**.
   b. In **Flexi Footprint**, select a foot print that the application supports.

Important:

Each application must ensure that only the supported flexible footprint is selected.

5. To update the IP address and FQDN of the virtual machine, perform the following:
   a. Click **More Actions** > **Re-establish connection**.

      Note:

      To update IP address or FQDN for Utility Services, establish trust on all virtual machines that are running on the host on which Utility Services resides.

   b. Click **More Actions** > **Refresh VM**.

      Note:

      To update IP address or FQDN for Utility Services, refresh all virtual machines that are running on the host on which Utility Services resides.

   c. Click **Update IP/FQDN in Local Inventory**.
   d. Click **Update VM IP/FQDN**.
   e. Provide the IP address and FQDN of the virtual machine.

      Update IPFQDN in Local Inventory updates the IP address or FQDN only in the local database in System Manager. The actual IP address or FQDN of the host does not change. Use **Update Network Params** in the Host tab to update the IP address or FQDN of the host.

6. Click **Save**.

Deleting a virtual machine

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the right navigation pane, click **Virtual Machines**.
4. On the Virtual Machines page, select one or more virtual machines.
5. On the Delete page, click **Delete**, and click **Yes** to confirm the deletion.

   The system turns off the virtual machines, and deletes the selected virtual machines from the host.

Changing the network parameters of Appliance Virtualization Platform and Avaya Aura® applications

About this task

Change the network parameters for Appliance Virtualization Platform and each Avaya Aura® application from the application, and then change the IP address and FQDN of Avaya Aura® applications and Appliance Virtualization Platform from Solution Deployment Manager.

Before you begin

- Connect the system on which Solution Deployment Manager is running to the new network for changing network parameters.
- When many Avaya Aura® applications are running on an Appliance Virtualization Platform host, ensure that you change the network parameter in the following order:
  1. Appliance Virtualization Platform
  2. Avaya Aura® applications that are running on the host except Utility Services.
  3. Utility Services

Note:

If you fail to follow the order, Utility Services network parameter update might fail.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Hosts for Selected Location <location name> section, select an ESXi host and click **Change Network Params** > **Change Host IP Settings**.
4. In the Network Parameters section, change the following as appropriate, and click **Save**:
   - IP address, subnetmask, and other parameters
   - Gateway IP address

   For more information, see “Change Network Parameters field descriptions”.
5. Change the network parameters first for each Avaya Aura® application on the host, and then for Utility Services.

   For more information, see *Administering Avaya Aura® application* available for each application. Also, see “Network Parameters for Avaya Aura® applications”.
6. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, do the following first for all Avaya Aura® applications except Utility Services, and then for Utility Services:
   a. In the Edit VMs section, select a virtual machine and click **Edit**.
   b. Click **Update IP/FQDN in Local Inventory**.
   c. Click **Update VM IP/FQDN**.
   d. Provide the IP address and FQDN of the virtual machine.

      Update IPFQDN in Local Inventory updates the IP address or FQDN only in the local database in System Manager. The actual IP address or FQDN of the host does not change. Use **Update Network Params** in the Host tab to update the IP address or FQDN of the host.
7. Click **Save**.

8. Do the following first for all Avaya Aura® applications except Utility Services, and then for Utility Services:
   a. Click **More Actions** > **Re-establish connection**.

      Note:

      To update IP address or FQDN for Utility Services, establish trust on all virtual machines that are running on the host on which Utility Services resides.

   b. Click **More Actions** > **Refresh VM**.

      Note:

      To update IP address or FQDN for Utility Services, refresh all virtual machines that are running on the host where Utility Services resides.

   When you update the IP address and FQDN for Utility Services, the system also updates the Services Port static route for each application.

Related links

Change Network Parameters field descriptions on page 98
Changing the network parameters for an Appliance Virtualization Platform host on page 89
Network parameter update for Avaya Aura applications on page 123

Updating Services Port Static Routing on an Avaya Aura® application

About this task

You might have to change the static routing if the Avaya Aura® application that is running on the Appliance Virtualization Platform host is:

- Deployed by using the vSphere client and does not have the route.
- Non-operational or unreachable when you start the Avaya Aura® application update.

Before you begin

- Update network parameters of Utility Services if applicable.
- Ensure that the Avaya Aura® application resides on the same subnetwork as Utility Services.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, select an Avaya Aura® application.
3. Click **More Actions** > **Update Static Routing**.

   The VM Update Static Routing page displays the details of Avaya Aura® application and Utility Services. The fields are read-only.
4. Click **Update**.
5. On the Success dialog box, click **OK**.

The system updates the Avaya Aura® application with the new IP address of Utility Services for Services Port static routing.

Related links

Update Static Routing field descriptions on page 121

Starting a virtual machine from Solution Deployment Manager

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. From the virtual management tree, select a host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to start.
4. Click **Start**.

   In **VM State**, the system displays `Started`.

Stopping a virtual machine from Solution Deployment Manager

About this task

System Manager is operational and ESXi or vCenter is added to the VM Management page to deploy Avaya Aura® Application OVA on ESXi virtual machines.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. From the virtual management tree, select a ESXi or vCentre host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to stop.
4. Click **Stop**.

   In **VM State**, the system displays `Stopped`.

Restarting a virtual machine from Solution Deployment Manager

Before you begin

- System Manager is operational, and ESXi or vCenter is added to the VM Management page to deploy Avaya Aura® Application OVA on ESXi virtual machines.
- Virtual machines must be in the running state.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. From the virtual management tree, select a host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to restart.
4. Click **Restart**.

In **VM State**, the system displays `Stopped` and then `Started`.

VM Deployment field descriptions

Select Location and Host

Name	Description
Select Location	The location name. The field is display-only.
Select Host	The hostname of the ESXi host. For example, smgrdev. The field is display-only.
Host FQDN	FQDN of the ESXi host.
Data Store	The data store with the available size. The page populates the Capacity Details section.
Next	Displays the Deploy OVA section in the Location & Host Details screen where you provide the details required for deployment.

Capacity Details

The system displays the CPU and memory details of the host. The fields are read-only.

Note:

If the host is in a cluster, the system does not display the capacity details of CPU and memory. Ensure that the host resource requirements are met before you deploy the virtual machine.

Name	Description
Name	The name
Full Capacity	The maximum capacity
Free Capacity	The available capacity
Reserved Capacity	The reserved capacity
Status	The configuration status

Deploy OVA on System Manager Solution Deployment Manager

Name	Description
Select Software Library	The software library where the `.ova` file is available.
Select OVAs	The `.ova` file that you want to deploy.
Flexi Footprint	The footprint size supported for the selected host. **Important:** • Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory.

Table continues…

Name	Description
	• Ensure that the application contains the footprint size values that are supported.
Next	Displays the Configuration Parameters tab in the OVA Details screen where you provide the OVA details.

Deploy OVA on the Solution Deployment Manager client

Name	Description
Provide OVA path	The option to select a `.ova` file of the virtual machine that is available on the system that hosts the Solution Deployment Manager client.
OVA File	The absolute path to the `.ova` file on the system that hosts the Solution Deployment Manager client. The field is available only when you click **Select the OVA from Local SMGR**.
Submit File	Selects the `.ova` file of System Manager that you want to deploy.
Flexi Footprint	The footprint size supported for the selected host. **Important:** Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory.
Next	Displays the Configuration Parameters tab in the OVA Details screen where you provide the OVA details.

Configuration Parameters

The system populates most of the fields depending on the OVA file.

Note:

For configuration parameter fields, for Communication Manager Messaging and Utility Services, see VM Deployment Configuration and Network Parameters field descriptions on page 118.

Name	Description
VM Name	The name of the virtual machine.
Product	The name of the Avaya Aura® application that is being deployed. The field is read-only.

Table continues…

Name	Description
Version	Release number of the Avaya Aura® application that is being deployed. The field is read-only.
ME Deployment	The option to perform the Midsize Enterprise deployment. The option is available only while deploying Communication Manager simplex OVA.

Table 6: Configuration Parameters for Communication Manager simplex OVA deployment

Name	Description
CM IPv4 Address	The IP address of the Communication Manager virtual machine.
CM IPv4 Netmask	The network mask of the Communication Manager virtual machine.
CM IPv4 Gateway	The default gateway of the Communication Manager virtual machine.
Out of Band Management IPv4 Address	The IP address of the Communication Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management Netmask	The subnetwork mask of the Communication Manager virtual machine for out of band management.
CM Hostname	The hostname of the Communication Manager virtual machine.
NTP Servers	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).
DNS Servers	The DNS IP address of the Communication Manager virtual machine.
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
WebLM Server IPv4 Address	The IP address of WebLM. The field is mandatory.
CM Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time.
CM Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time.
Confirm Password	The password required to be confirmed.

Network Parameters

Name	Description
Public	The port number that is mapped to public port group.

Table continues…

Name	Description
	You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.
Services	The port number that is mapped to the services port group when Utility Services is deployed in the solution. Utility Services provides routing from the services port to the virtual machines and additional functions, such as alarm conversion.
Duplication Link	The connection for server duplication. The field is available only when you deploy duplex Communication Manager.
Out of Band Management	The port number that is mapped to the out of band management port group.

Button	Description
Deploy	Displays the EULA acceptance screen where you must click **Accept** to start the deployment process.

Related links

VM Deployment Configuration and Network Parameters field descriptions on page 118

VM Deployment Configuration and Network Parameters field descriptions

Table 7: Configuration Parameters for Communication Manager Messaging deployment

Name	Description
Messaging IPv4 address	The IP address of the Communication Manager Messaging virtual machine.
Messaging IPv4 Netmask	The network mask of the Communication Manager Messaging virtual machine.
Messaging IPv4 Gateway	The default gateway of the Communication Manager Messaging virtual machine. For example, 172.16.1.1.
Out of Band Management IPv4 Address	The IP address of the Communication Manager Messaging virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network.
Out of Band Management IPv4 Netmask	The subnetwork mask of the Communication Manager Messaging virtual machine for out of band management.

Table continues…

Name	Description
Messaging Hostname	The hostname of the Communication Manager Messaging virtual machine.
NTP Servers	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,). The field is optional.
DNS Server(s)	The DNS IP address of the Communication Manager Messaging virtual machine. Separate the IP addresses with commas(,). The field is optional.
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
WebLM Server IPv4 Address	The IP address of WebLM. The field is mandatory.
Messaging Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time.
Messaging Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time.
Confirm Password	The password required to be confirmed.

Configuration and Network Parameters for Utility Services deployment

Name	Description
Configuration Parameters	
Communication Manager IP	IP address of Communication Manager. **Note:** A unique Communication Manager IP address is required for each Utility Services. If you are not associated with a Communication Manager server, specify a static IP that is in your network range.
Hostname	Linux hostname or fully qualified domain name for Utility Services virtual machine.
TImezone setting	The selected timezone setting for the Utility Services virtual machine.
NTP Server IP	IP address of a server running Network Time Protocol that Communication Manager can use for time synchronization.
Out of Band Management Mode	The Out of Band Management mode in which you want to deploy. The options are as follows: • **OOBM_Enabled**: To enable Out of Band Management. • **OOBM_Disabled**: To disable Out of Band Management.

Table continues…

Name	Description
	Note: **OOBM_Disabled** is the default setting. If the mode is set to **OOBM_Disabled**, then you do not need to configure Out of Band Management.
Utility Services Mode	The mode in which you want to deploy Utility Services. The options are: • **Services Port Only**: Deploys Services Port only. Use when the customer already has Utility Services running on another virtual machine and providing the services. With the services port feature, through a laptop connected to the services port of Appliance Virtualization Platform, you can gain access to Avaya virtual machines and the hypervisor that are deployed. • **Utility Servers Only**: Use to disable routing. Set this mode only for Virtualized Environment. If you set this mode for an Avaya appliance, the services port becomes non-operational. • **Full Functionality**: Utility Services and services port enabled. The default mode for Appliance Virtualization Platform. You can set the mode only during the deployment. You cannot change the mode after the virtual machine is deployed. **Note:** For the Solution Deployment Manager client to connect to the services port features of Utility Services, change the IP address to 192.11.13.5 on the computer of the technician Utility Services can gain access to the hypervisor and all virtual machines. Utility Services provides application routing between the physical port and virtual applications.
Primary System Manager IP address for application registration	The IP address of System Manager that is required for application registration.
Enrollment Password	The enrollment password.
Confirmation password	The confirmation password.
Network Parameters	
Default Gateway	The IP address of the default gateway. Required field unless you use DHCP.
DNS	The IP address of domain name servers for the Utility Services virtual machine. Separate each IP address by a comma. Required field unless you use DHCP.
Public IP address	The IP address for this interface.

Table continues…

Name	Description
	Required field unless you use DHCP.
Public Netmask	The netmask for this interface. Required field unless you use DHCP.
Out of Band Management IP Address	The IP address for this interface.
Out of Band Management Netmask	The netmask for this interface.

Update Static Routing field descriptions

Name	Description
VM Name	The virtual machine name
VM IP/FQDN	The IP address or FQDN of the virtual machine
Utility Services IP	The IP address of Utility Services

Button	Description
Update	Updates the static IP address for routing.

Installed Patches field descriptions

Button	Description
Action to be performed	The operation that you want to perform on the software patch, service pack, or feature pack that you installed. The options are: • **All**: Displays all the software patches. • **Commit**: Displays the software patches that you can commit. • **Rollback**: Displays the software patches that you can rollback.
Get Info	Displays software patches, service packs, and feature packs that you installed.
Commit	Commits the selected software patch.
Rollback	Rolls back the selected software patch.

Name	Description
VM Name	The name of the System Manager virtual machine on which you want to install the patch.
VM IP	The IP address of System Manager on which you want to install the patch.
Patch Name	The software patch name that you want to install.

Table continues…

Name	Description
Patch Type	The patch type. The options are service pack and software patch.
Patch Version	The software patch version.
Patch State	The software patch state. The states are: • Activated • Deactivated • Removed • Installed
Patch Status	The software patch status.

Update VM field descriptions

Name	Description
VM Name	The System Manager virtual machine name
VM IP	The IP address of System Manager
VM FQDN	FQDN of System Manager
Host Name	The host name
Select bin file from Local SMGR	The option to select the software patch or service pack for System Manager. The absolute path is the path on the computer on which the Solution Deployment Manager client is running. The patch is uploaded to System Manager. This option is available only on the Solution Deployment Manager client.
Auto commit the patch	The option to commit the software patch or service pack automatically. If the check box is clear, you must commit the patch from **More Actions** > **Installed Patches**.

Button	Description
Install	Installs the software patch or service pack on System Manager.

Reestablish Connection field descriptions

Name	Description
VM Name	The virtual machine name
VM IP/FQDN	The IP address or FQDN of the virtual machine
User Name	The user name
Password	The password

Button	Description
Reestablish Connection	Establishes connection between System Manager and the virtual machine.

Network parameter update for Avaya Aura® applications

You can change the network parameters for Avaya Aura® applications that run on an Appliance Virtualization Platform server.

The commands listed might change. Therefore, from the Avaya Support website at https://support.avaya.com, get the latest command update for an Avaya Aura® application from the appropriate document.

Tip:

On the Avaya Support website navigate to **Support by Product** > **Documents** > **<Avaya Aura application>**, type the release number, click **Installation, Upgrades & Config**, click **Enter**, and search for the updates.

Avaya Aura® application	Command	Interface where you perform the task
Appliance Virtualization Platform	`serverInitialNetworkConfig`	CLI
System Manager	`changeIPFQDN -IP <IP address> –FQDN <FQDN> -GATEWAY <Gateway address> -NETMASK <Netmask address> -DNS <DNS address> -SEARCH <search list of domain names>`	CLI or vSphere client
Communication Manager	-	The Network Configuration page from **Administration** > **server(Maintenance)** > **ServerConfiguration** on Communication Manager SMI.
Session Manager	`SMnetSetup`	vSphere client
Avaya Breeze™ and all installed snap-ins	-	vSphere client
Utility Services	`VMware_conf.sh`	CLI
Avaya Aura® Media Server	-	See the Avaya support website.
SAL Gateway	-	Currently, you cannot change Network Parameters for SAL Gateway

Monitoring a host and virtual machine

Monitoring a host

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. Click the Monitor Hosts tab.
3. In the Monitor Hosts page, do the following:
   a. In **Hosts**, click a host.
   b. Click **Generate Graph**.

   The system displays the graph regarding the CPU/memory usage of the host that you selected.

Monitoring a virtual machine

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. Click the Monitor VMs tab.
3. In the Monitor VMs page, do the following:
   a. In **Hosts**, click a host.
   b. In **Virtual machines**, click a virtual machine on the host that you selected.
4. Click **Generate Graph**.

   The system displays the graph regarding the CPU/memory usage of the virtual machine that you selected.

Managing vCenter

Adding a vCenter to Solution Deployment Manager

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 5.0, 5.1, 5.5, and 6.0. When you add vCenter, System Manager discovers the ESXi hosts that this vCenter manages, adds to the repository, and displays in the Managed Hosts section. Also, System Manager discovers virtual machines running on the ESXi host and adds to the repository.

System Manager displays vCenter, ESXi host, and virtual machines on the Manage Elements page.

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.

2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **Add**.
4. In the New vCenter section, provide the following vCenter information:
   - **vCenter FQDN**

     For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.
   - **User Name**
   - **Password**
   - **Authentication Type**
5. Click **Save**.
6. On the certificate dialog box, click **Accept Certificate**.

   The system generates the certificate and adds vCenter.

   In the Managed Hosts section, the system displays the ESXi hosts that this vCenter manages.

Related links

Editing vCenter on page 125
Map vCenter field descriptions on page 126
New vCentre and Edit vCentre field descriptions on page 127

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select a vCenter server and click **Edit**.
4. In the Edit vCenter section, change the vCenter information as appropriate.
5. If vCenter is migrated from earlier release, on the Certificate page, click **Accept Certificate**, and click **Save**.
6. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:
   - Select an ESXi host and click the edit icon ( ).
   - Select one or more ESXi hosts, select the location, and click **Bulk Update** and click **Update**.

If you do not click **Commit** after you move the host from Managed Hosts to Unmanaged Hosts or vice versa, and you refresh the table, the page displays the same host in both the tables. Click **Commit** to get an updated list of managed and unmanaged hosts.

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
4. Click **Yes** to confirm the deletion of servers.

   The system deletes the vCenter from the inventory.

Map vCenter field descriptions

Name	Description
Name	The name of the vCenter server.
IP	The IP address of the vCenter server.
FQDN	The FQDN of the vCenter server. **Note:** Use FQDN to successfully map and log in to vCenter from Solution Deployment Manager. With IP address, the system displays an error message about the incorrect certificate and denies connection.
License	The license type of the vCenter server.
Status	The license status of the vCenter server.
Certificate Status	The certificate status of the vCenter server. The values are: • : The certificate is correct. • : The certificate is not accepted or invalid.

Button	Description
View	Displays the certificate status details of the vCenter server.
Generate/Accept Certificate	Displays the certificate dialog box where you can generate and accept certificate for vCenter.

Table continues…

Button	Description
	For vCenter, you can only accept certificate. You cannot generate certificate.

Button	Description
Add	Displays the New vCenter page, where you can add a new ESXi host.
Edit	Displays the Edit vCenter page, where you can update the details and location of ESXi hosts.
Delete	Deletes the ESXi host.
Refresh	Updates the list of ESXi hosts in the Map vCenter section.

New vCentre and Edit vCentre field descriptions

Name	Description
vCenter FQDN	FQDN of vCenter.
User Name	The user name to log in to vCenter.
Password	The password that you use to log in to vCenter.
Authentication Type	The authentication type that defines how Solution Deployment Manager performs user authentication. The options are: • **SSO**: Global username used to log in to vCenter to authenticate to an external Active Directory authentication server. • **LOCAL**: User created in vCenter

Button	Description
Save	Saves any changes you make to FQDN, username, and authentication type of vCenter.
Refresh	Refreshes the vCenter details.

Managed Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
Host Name	The IP address of the ESXi host.
Location	The physical location of the ESXi host.
Edit	The option to edit the location and host.
Bulk Update	Provides an option to change the location of more than one ESXi hosts.

Table continues…

Name	Description
	Note: You must select a location before you click **Bulk Update**.
Update	Saves the changes that you make to the location or hostname of the ESXi host.
Commit	Commits the changes that you make to the ESXi host with location that is managed by vCenter.

Unmanaged Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
ESXi Version	The version of the ESXi host. The options are: 5.0, 5.1, 5.5, and 6.0.

Button	Description
Commit	Saves all changes that you made to vCenter on the Map vCenter page.

Viewing the job history of virtual machine operations

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
2. In the lower pane, click **Job History**.
3. On the Job History page, in **Operation**, select one or more operations.
4. Click **Submit**.

   The page displays the details of jobs that you selected.

Related links

Job History field descriptions on page 128

Job History field descriptions

Name/Button	Description
Operation	The operation that is performed on a virtual machine. You can select one or more operations that are performed on a virtual machine, such as host restart, virtual machine deployment, and patch installation.
Submit	Provides details of jobs that you selected.

History

Button	Description
Job ID	The unique name of the virtual machine management job.
IP/FQDN	The IP address or host name of the virtual machine or the host where the operation is performed.
Operation	The operation performed on the virtual machine or host. For example, host refresh, virtual machine deployment, and patch installation.
Status	The status of the job.
Start Time	The start time of the job.
End Time	The end time of the job.

Deploying System Manager in Virtualized Environment

Deploying the System Manager OVA file by using vSphere

Before you begin

Install vSphere Client.

Procedure

1. Start vSphere Client.
2. Enter the IP address and the user credentials for the ESXi host.

   Ignore any security warning that the system displays.
3. On vSphere Client, click **File** > **Deploy OVF Template**.
4. In the Deploy OVF Template dialog box, perform one of the following steps:
   - In the **Deploy from a file or URL** field, enter the path to the `.ova` file.
   - Click **Browse** and navigate to the `.ova` file from the local computer, network share, CD-ROM, or DVD.
5. On the OVF Template Details page, verify the details, and click **Next**.
6. On the End User License Agreement page, click **Accept**.
7. Click **Next**.
8. **(Optional)** On the Name and Location page, in the **Name** field, change the name for the virtual machine.
9. Click **Next**.

10. On the Deployment Configuration page, in the **Configuration** field, click one of the following:
    - **SMGR Profile 2 Max User 250K**: To support 250000 users. This configuration requires 6 vCPUs and 12 GB memory.
    - **SMGR Profile 1 Max User 35K**: To support 35000 users. This configuration requires 4 vCPUs and 9 GB memory.
11. Click **Next**.
12. On the Storage page, select the required data store and then click **Next**.
13. On the Disk Format page, click **Thick Provision Lazy Zeroed**.

    The system displays the data store that you selected and the available space.
14. On the Network Mapping page, for each network that you specified in the OVA Template Details page, in the **Destination Network** column, select a host network for the Out of Band Management interface and Public interface.
15. Click **Next**.
16. Review the settings and click **Finish**.

    Wait until the system deploys the OVA file successfully.
17. To start the System Manager virtual machine, if System Manager is not already powered on perform one of the following steps:
    - Right-click the virtual machine, and click **Power** > **Power On**.
    - On the **Inventory** menu, click **Virtual Machine** > **Power** > **Power On**.

    The system starts the System Manager virtual machine.

Next steps

- When the system starts for the first time, configure the parameters for System Manager. For instructions, see Configuring the network parameters from the vSphere console.

  From the time you power on the system, the deployment process takes about 30–40 minutes to complete. Do not reboot the system until the configuration is complete. You can monitor the post deployment configuration from the `/var/log/Avaya/PostDeployLogs/post_install_sp.log` file.
- Verify the deployment of the System Manager OVA file.

Related links

Deploying an OVA file for an Avaya Aura application on page 107
Deploying the System Manager OVA file using vCenter on page 134

Configuring the network parameters from the vSphere console

Before you begin

- Deploy the System Manager virtual machine OVA file.
- Start the System Manager virtual machine.

If the **Power on after deployment** check box is clear during deployment, you must manually start the virtual machine.

- To reach the System Manager command line interface, start vSphere Client and click the **Console** tab or the  icon.

About this task

When first started, System Manager virtual machine collects the network parameters. Enter the network parameters at the system prompt when first started.

Procedure

1. At the prompt, enter the following management network parameters:
   - **Management IP Address (or Out of Band Management IP address)**: The Management or Out of Band Management IP address to assign to the System Manager virtual machine.
   - **Management Netmask**: The subnetwork mask to assign to the Management interface of the System Manager virtual machine.
   - **Management Gateway**: The gateway IP address to assign to the Management interface of the System Manager virtual machine. For example, 172.16.1.1.
   - **IP Address of DNS Server**: The DNS IP addresses to assign to the primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,). For example, 172.16.1.2, 172.16.1.4.
   - **Management Short Hostname**: The hostname to assign to the System Manager virtual machine. For example, bouldervm2.

     Note:

     System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.
   - **Management Domain Name**: The domain name to assign to the System Manager virtual machine. For example, smgrdev.com.
   - **Default Search List**: The search list of domain names. The field is optional.
   - **NTP Server IP or FQDN**: The IP address or FQDN of the NTP server. This is an optional field. Separate the IP addresses or FQDNs with commas (,).
   - **Time Zone**: The timezone where the System Manager virtual machine is located. A list is available where you select the name of the continent and the name of the country.
2. At the prompt, enter the following public network parameters:
   - **Public IP Address**: The IP address for the Public interface of the System Manager virtual machine.
   - **Public Netmask**: The subnetwork mask to assign to the Public interface of the System Manager virtual machine.
   - **Public Gateway**: The gateway IP address to assign to the Public interface of the System Manager virtual machine. For example, 172.16.1.1.

- **Public Hostname**: The hostname to assign to the System Manager virtual machine. For example, bouldervm2.
- **Public Domain Name**: The domain name to assign to the System Manager virtual machine. For example, smgrdev.dev.

Note:

You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.

3. Enter the following SNMPv3 parameters:
   - **User Name Prefix**: For example, global.
   - **Authentication Protocol Password**: For example, globalpass.
   - **Privacy Protocol Password**: For example, globalpass.
4. Enter the following virtual FQDN details of the System Manager virtual machine:
   - Virtual host name. For example, grsmgr.
   - Virtual domain name. For example, dev.com.

   Note:

   - The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.
   - VFQDN is a mandatory field.
   - Do not add VFQDN entries in the DNS configuration.
   - Do not add VFQDN in the `/etc/hosts` file on System Manager. Adding VFQDN in the `/etc/hosts` file might cause failures.
   - In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.
   - After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:

     a. Log in to the System Manager virtual machine as root user.

     b. Run the following command, `#sh /opt/Avaya/vsp/SMGRVirtualFqdnUtility.sh`.
5. Type the backup definition parameters for the System Manager virtual machine to schedule the remote backup during the System Manager installation. For information, see Backup Definition parameters.
6. To confirm the network parameters, type `Y`.

   The system starts the configuration of the network parameters. The deployment process takes about 30–40 minutes to complete.

   From the time you power on the system, the deployment process takes about 30–40 minutes to complete. Do not reboot the system until the configuration is complete. You can monitor

the post deployment configuration from the `/var/log/Avaya/PostDeployLogs/post_install_sp.log` file.

7. On the web browser, enter `https://FQDN/SMGR` to gain access to the System Manager web console.

   The system displays the System Manager web console.

Backup Definition parameters

Use the backup definition to schedule remote backup during the System Manager installation.

Note:

You can skip the configuration of the backup definition parameters to schedule the backup jobs later.

The backup time must be 6 hours later than the System Manager installation time.

If you set the **Backup Start Month** field to 5, **Backup Start Day** field to 24, and **Repeat Type** field to Weekly, the system executes the backup job every Friday if May 24th is a Friday.

Name	Description
Schedule Backup?	• **Yes**: To schedule the backup jobs during the System Manager installation. • **No**: To schedule the backup jobs later. **Note:** If you select No, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server. **Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id	The login ID of the backup server to log in through the command line interface.
Backup Server Login Password	The SSH login password to log in to the backup server from System Manager through the command line interface.
Confirm Password	The password that you reenter to log in to the backup server through the command line interface.
Backup Directory Location	The location on the remote backup server.
File Transfer Protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.

Table continues…

Name	Description
Repeat Type	The type of the backup. The possible values are: • `Hourly` • `Daily` • `Weekly` • `Monthly`
Backup Frequency	The frequency of the backup taken for the selected backup type.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be 6 hours later than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

Deploying the System Manager OVA file using vCenter

Before you begin

- Install vSphere client.
- Install vCenter server and connect vSphere Client to vCenter.

Procedure

1. Start vSphere Client.
2. Enter the IP address and the user credentials for the vCenter server.

   Ignore any security warning that the system displays.
3. On vSphere Client, click **File** > **Deploy OVF Template**.
4. In the Deploy OVF Template dialog box, perform one of the following steps:
   - In the **Deploy from a file or URL** field, enter the path to the `.ova` file.
   - Click **Browse** and navigate to the `.ova` file from the local computer, network share, CD-ROM, or DVD.

5. On the OVF Template Details page, verify the details, and click **Next**.
6. On the End User License Agreement page, click **Accept**.
7. Click **Next**.
8. **(Optional)** On the Name and Location page, in the **Name** field, change the name for the virtual machine.
9. On the Deployment Configuration page, in the **Configuration** field, click one of the following:
   - **SMGR Profile 2 Max User 250K**: To support 250000 users. This configuration requires 6 vCPUs and 12 GB memory.
   - **SMGR Profile 1 Max User 35K**: To support 35000 users. This configuration requires 4 vCPUs and 9 GB memory.
10. Click **Next**.
11. In the **Inventory Location** area, select the datacenter and click **Next**.
12. If the cluster exists, select the cluster and click **Next**.
13. Select the specific host within the cluster and click **Next**.
14. On the Storage page, select the required data store and click **Next**.
15. On the Disk Format page, click **Thick Provision Lazy Zeroed**.

    The system displays the data store that you selected and the available space.
16. On the Network Mapping page, for each network that you specified in the OVA Template Details page, in the **Destination Network** column, select a host network for the Out of Band Management interface and Public interface.
17. On the Properties page:
    a. At the prompt, enter the following management network parameters:
       - **Management IP Address (or Out of Band Management IP address)**: The Management or Out of Band Management IP address to assign to the System Manager virtual machine.
       - **Management Netmask**: The subnetwork mask to assign to the Management interface of the System Manager virtual machine.
       - **Management Gateway**: The gateway IP address to assign to the Management interface of the System Manager virtual machine. For example, 172.16.1.1.
       - **IP Address of DNS Server**: The DNS IP addresses to assign to the primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,). For example, 172.16.1.2, 172.16.1.4.
       - **Management Hostname**. The fully qualified domain name to assign to the Management interface of the System Manager virtual machine. For example, bouldervm1.smgrpub.com.
       - **Default Search List**: The search list of domain names. The field is optional.

- **Time Zone**: The timezone where the System Manager virtual machine is located. A list is available where you select the name of the continent and the name of the country.

b. At the prompt, enter the following public network parameters:

- **Public IP Address**: The IP address for the Public interface of the System Manager virtual machine.
- **Public Netmask**: The subnetwork mask to assign to the Public interface of the System Manager virtual machine.
- **Public Gateway**: The gateway IP address to assign to the Public interface of the System Manager virtual machine. For example, 172.16.1.1.
- **Public Hostname**: The fully qualified domain name to assign to the Public interface of the System Manager virtual machine. For example, bouldervm2.smgrdev.com.
- **Virtual FQDN** for the System Manager virtual machine.
  - Virtual short hostname. For example, grsmgr.
  - Virtual domain. For example, dev.com.
    - The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.
    - VFQDN is a mandatory field.
    - Do not add VFQDN entries in the DNS configuration.
    - Do not add VFQDN in the `/etc/hosts` file on System Manager. Adding VFQDN in the `/etc/hosts` file might cause failures.
    - In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.
    - After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:
      a. Log in to the System Manager virtual machine as root user.
      b. Run the following command, `#sh /opt/Avaya/vsp/SMGRVirtualFqdnUtility.sh`.

Note:

You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.

c. Configure the following SNMPv3 parameters:

- **User Name Prefix**: For example, global.
- **Authentication Protocol Password**: For example, globalpass.
- **Privacy Protocol Password**: For example, globalpass.

d. **(Optional)** Select the **Schedule SMGR backup** check box to schedule the System Manager backup and configure the backup definition input parameters. For information, see Backup Definition parameters.

Note:

- If you do not provide the details in the mandatory fields, you cannot power on the virtual machine even if the deployment is successful.
- During the startup, the system validates the inputs that you provide. If the inputs are invalid, the system prompts you to provide the inputs again on the console of the virtual machine.
- The system does not validate the backup definition data that you provide. If the data is invalid, the system does not schedule the backup.

18. Click **Next**.
19. Review the settings and click **Finish**.

    Wait until the system deploys the OVA file successfully.

    From the time you power on the system, the deployment process takes about 30–40 minutes to complete. Do not reboot the system until the configuration is complete. You can monitor the post deployment configuration from the `/var/log/Avaya/PostDeployLogs/post_install_sp.log` file.
20. To start the System Manager virtual machine, if System Manager is not already powered on perform one of the following steps:
    - Right-click the virtual machine, and click **Power** > **Power On**.
    - On the **Inventory** menu, click **Virtual Machine** > **Power** > **Power On**.

    The system starts the System Manager virtual machine.
21. Click the Console tab and verify that the system startup is successful.

Next steps

Verify the deployment of the System Manager OVA file.

Changing the IP address, FQDN, DNS, Gateway, or Netmask address from CLI

About this task

Use this procedure to change the network configuration parameters for Public interface and Management interface when OOBM is enabled.

Important:

- Do not change the network settings from vSphere Client when the virtual machine is in the power off state.
- FQDN value must be unique and different from the virtual FQDN value of System Manager.

- After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:
  1. Log in to the System Manager virtual machine as root user.
  2. Run the following command, `#sh /opt/Avaya/vsp/SMGRVirtualFqdnUtility.sh`.

Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Client and click on the **Console** tab or the  icon.
  - Start an SSH on System Manager.
- Log in to the System Manager virtual machine as admin.
- Create the System Manager virtual machine snapshot.

Note:

Delete the snapshot after the System Manager operation is complete.

Procedure

1. To configure Management network parameters, type `changeIPFQDN -IP <IP address> –FQDN <FQDN> -GATEWAY <Gateway address> -NETMASK <Netmask address> -DNS <DNS address> -SEARCH <search list of domain names>`.

   For information, see changeIPFQDN command.

2. To configure Public network parameters, type `changePublicIPFQDN -IP <IP address> –PublicFQDN <FQDN> -PublicGATEWAY <Gateway address> -PublicNETMASK <Netmask address>`.

   For information, see changePublicIPFQDN command.

Next steps

Get new licenses from PLDS containing the new host ID and install the new licenses.

After you change the IP address of System Manager, the system generates a new host ID for WebLM server that System Manager hosts. Therefore, all previously installed licenses become invalid.

For instructions to install a license file, see Managing Licenses in *Administering Avaya Aura® System Manager*.

Related links

changeIPFQDN command on page 138

System Manager command line interface operations on page 140

changeIPFQDN command

Use the **changeIPFQDN** command to change the Management IP address when Out of Band Management is enabled. With this command you can change the IP address, FQDN, DNS address, Gateway, Netmask address for Management network configuration of System Manager, and the search list for the DNS address.

To change the Public IP address when Out of Band Management is enabled, use the **changePublicIPFQDN** command

Syntax

```
changeIPFQDN -IP < >  -FQDN < > -GATEWAY < >-NETMASK < > -DNS < > -SEARCH < >
```

#	Option	Description	Usage
1	IP	The new Management IP address of System Manager.	**changeIPFQDN -IP 10.11.12.13**
2	FQDN	The new Management FQDN of System Manager.	**changeIPFQDN -FQDN a.mydomain.smgr.com**
3	GATEWAY	The new Management Gateway address of System Manager.	**changeIPFQDN -GATEWAY 10.11.1.1**
4	NETMASK	The new Management netmask address of System Manager.	**changeIPFQDN -NETMASK 255.255.203.0**
5	DNS	The new Management DNS address of System Manager. You an provide multiple DNS addresses. Separate each address by a comma.	**changeIPFQDN -DNS 10.11.1.2** **changeIPFQDN -DNS 10.11.12.5,10.11.12.3**
6	SEARCH	The new search list of domain names.	**changeIPFQDN -SEARCH smgr.com**

Example

You can provide options in any combination that the system supports:

```
changeIPFQDN -IP 10.11.y.z -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1 -NETMASK
255.255.255.0 -DNS 10.11.1.2 -SEARCH platform.avaya.com
```

```
changeIPFQDN -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1
```

```
changeIPFQDN -IP 10.11.y.z
```

Installing the System Manager service pack or patch from CLI

Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Client and click on the **Console** tab or the  icon.
  - Start an SSH on System Manager.
- Log in to the System Manager virtual machine as admin.
- Take a snapshot of the System Manager virtual machine.

Procedure

Type `SMGRPatchdeploy <absolute path to the service pack or patch for System Manager>`.

If you do not provide the name of the patch or service pack, the console displays menu items. Provide the absolute path to the patch or service pack that you want to install for System Manager.

Next steps

Delete the snapshot after you verify the System Manager functionality.

Related links

System Manager command line interface operations on page 140

System Manager command line interface operations

#	Command	Parameters	Description	Usage
1	`changeIPFQDN`	• `-IP <new Management interface or Out of Bound Management IP address for System Manager>` • `-FQDN <new Management or Out of Bound Management fully qualified domain name for System Manager>` • `-GATEWAY <new Management interface or Out of Bound Management Gateway address for System Manager>` • `-NETMASK <new Management interface or Out of Bound Management netmask address for System Manager>` • `-DNS <new DNS address for System Manager>` • `-SEARCH <new search list for DNS address>`	Updates the existing Management interface or Out of Bound Management IP address, FQDN, Gateway, Netmask, DNS, and the search list with the new value.	• `changeIPFQDN -IP <new IP address>` • `changeIPFQDN -FQDN <new fully qualified domain name>` • `changeIPFQDN -IP <new IP address> -GATEWAY <new Gateway address for System Manager> -SEARCH <new search list for DNS address>`
1	`changePublicIPFQDN`	• `-publicIP <new IP address for System Manager>` • `-publicFQDN <new fully qualified domain name for System Manager>` • `-publicGATEWAY <new Gateway address for System Manager>`	Updates the existing Public IP address, FQDN, Gateway, and Netmask with the new value.	• `changePublicIPFQDN -publicIP <new Public IP address>` • `changePublicIPFQDN -publicFQDN <new fully qualified domain name for public interface>` • `changePublicIPFQDN -publicIP <new`

Table continues…

#	Command	Parameters	Description	Usage
		• **-publicNETMASK <new netmask address for System Manage>**		**Public IP address> -publicGATEWAY <new Public Gateway address for System Manager>**
2	**upgradeSMGR**	**<absolute path to the dmutility.bin> -m -v -V -H**	Upgrades System Manager using the data migration utility.	**upgradeSMGR dmutility *.bin -m -v -V -H**
3	**SMGRPatchdeploy**	**<absolute path to the System Manager service pack or the software patch>**	Installs the software patch or the service pack for System Manager.	**SMGRPatchdeploy <absolute path to /home/admin/ <SMGRservicepackName>** **Note:** Copy the System Manager service pack or patches that you must install to `/home/admin/`.
4	**updateASG**	**<absolute path to the ASG XML file>**	Updates the ASG XML file.	**updateASG <absolute path to the ASG XML file>**
5	**configureTimeZone**	**Time zone that you select**	Configures the time zone with the value that you select.	**configureTimeZone** **Select a time zone. For example, America/Denver**
6	**configureNTP**	**<IP address of NTP server>**	Configures the NTP server details.	**configureNTP <IP address of NTP server>** Separate IP addresses or hostnames of NTP servers with commas (,).
7	**createCA**		Creates a new Certificate Authority by using SHA2 signing algorithm and 2048 key size. For more information, see, Creating a new Certificate Authority by using SHA2 signing algorithm and 2048 key size.	**createCA** You must provide the desired Common Name (CN)

Chapter 10: Resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Overview		
Avaya Aura® Virtualized Environment Solution Description	Understand high-level solution and functionality.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Implementation		
Deploying Avaya Aura® System Manager	Deploy the Avaya Aura® System Manager virtual machine.	Implementation personnel
Administration		
Administering Avaya Aura® System Manager for Release 7.0.1	Perform administration tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators
Using		
Using the Solution Deployment Manager client	Deploy Avaya Aura® applications and install patches on Avaya Aura® applications.	System administrators
Maintenance and Troubleshooting		
Troubleshooting Avaya Aura® System Manager	Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators and IT personnel

Related links

Finding documents on the Avaya Support website on page 143

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Related links

Documentation on page 142

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After you log into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title	Type
2007V/W	What is New in Avaya Aura® Release 7.0.1	AvayaLive™ Engage Theory
2008V/W	What is New in Avaya Aura® Application Enablement Services 7.0	AvayaLive™ Engage Theory
2009V/W	What is New in Avaya Aura® Communication Manager 7.0	AvayaLive™ Engage Theory

Table continues…

Course code	Course title	Type
2010V/W	What is New in Avaya Aura® Presence Services 7.0	AvayaLive™ Engage Theory
2011/V/W	What is New in Avaya Aura® Session Manager Release 7.0.1 and Avaya Aura® System Manager Release 7.0.1	AvayaLive™ Engage Theory
2012V	Migrating and Upgrading to Avaya Aura® Platform 7.0	AvayaLive™ Engage Theory
2013V	Avaya Aura® Release 7.0.1 Solution Management	AvayaLive™ Engage Theory
1A00234E	Avaya Aura® Fundamental Technology	AvayaLive™ Engage Theory
1A00236E	Knowledge Access: Avaya Aura® Session Manager and Avaya Aura® System Manager Fundamentals	AvayaLive™ Engage Theory
5U00106W	Avaya Aura® System Manager Overview	WBT Level 1
4U00040E	Knowledge Access: Avaya Aura® Session Manager and System Manager Implementation	ALE License
5U00050E	Knowledge Access: Avaya Aura® Session Manager and System Manager Support	ALE License
5U00095V	Avaya Aura® System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 1
5U00097I	Avaya Aura® Session Manager and System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 2
3102	Avaya Aura® Session Manager and System Manager Implementation and Maintenance Exam	Exam (Questions)
5U00103W	Avaya Aura® System Manager 6.2 Delta Overview	WBT Level 1

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.

- In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Appendix A: Best Practices for VMware performance and features

The following sections describe the best practices for VMware performance and features.

Related links

BIOS on page 146
VMware Tools on page 148
Timekeeping on page 148
Configuring the NTP time on page 150
VMware networking best practices on page 150
Storage on page 154
Thin vs. thick deployments on page 154

BIOS

For optimal performance, turn off power saving server options. See the technical data provided by the manufacturer for your particular server regarding power saving options.

For information about how to use BIOS settings to improve the environment for latency-sensitive workloads for an application, see the technical white paper at http://www.vmware.com/files/pdf/techpaper/VMW-Tuning-Latency-Sensitive-Workloads.pdf.

The following sections describe the recommended BIOS settings for:

- Intel Virtualization Technology
- Dell PowerEdge Servers
- HP ProLiant Servers

Related links

Best Practices for VMware performance and features on page 146
Intel Virtualization Technology on page 147
Dell PowerEdge Server on page 147
HP ProLiant Servers on page 148

Intel Virtualization Technology

Intel CPUs require EM64T and Virtualization Technology (VT) support in the chip and in the BIOS to run 64–bit virtual machines.

All Intel Xeon processors include:

- Intel Virtualization Technology
- Intel Extended Memory 64 Technology
- Execute Disable Bit

Ensure that VT is enabled in the host system BIOS. The feature is also known as VT, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions.

Note:

The VT setting is locked as either **On** or **Off** when the server starts. After enabling VT in the system BIOS, save your changes to the BIOS settings and exit. The BIOS changes take effect after the host server reboots.

Other suggested BIOS settings

Servers with Intel Nehalem class and newer Intel Xeon CPUs offer two more power management options: C-states and Intel Turbo Boost. These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell and HP servers are described in the following sections. Other server models might use other terminology for the same BIOS controls.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to a fully active state.
- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power. The default for this option is **enabled**. Do not change the default.

Related links

BIOS on page 146

Dell PowerEdge Server

When the Dell server starts, press F2 to display the system setup options.

- Set the Power Management Mode to **Maximum Performance**.
- Set the CPU Power and Performance Management Mode to **Maximum Performance**.
- In Processor Settings, set:
  - **Turbo Mode** to **enable**.
  - **C States** to **disabled**.

Related links

BIOS on page 146

HP ProLiant Servers

The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to **Static High Mode**.
- Disable **Processor C-State Support**.
- Disable **Processor C1E Support**.
- Disable **QPI Power Management**.
- Enable **Intel Turbo Boost**.

Related links

BIOS on page 146

VMware Tools

The VMware Tools utility suite is built into the application OVA. The tools enhance the performance of the guest operating system on the virtual machine and improve the management of the virtual machine.

VMware tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing

For more information about VMware tools, see *Overview of VMware Tools* at http://kb.vmware.com/kb/340.

Important:

Do not upgrade the VMware tools software that is packaged with each OVA unless instructed to do so by Avaya. The supplied version is the supported release and has been thoroughly tested.

Related links

Best Practices for VMware performance and features on page 146

Timekeeping

For accurate timekeeping, use the Network Time Protocol (NTP) as a time source instead of the ESXi hypervisor.

The NTP servers can be local or over the Internet. If the NTP servers are on the Internet, the corporate firewall must open UDP port 123 so that the NTP service can communicate with the external NTP servers.

The VMware tools time synchronization method is disabled at application deployment time to avoid dueling clock masters. You must configure the NTP service first because the applications are not receiving clock updates from the hypervisor. To verify that VMware Tools Timesync is disabled, run the command `/usr/bin/vmware-toolbox-cmd timesync status`.

In certain situations, the ESXi hypervisor pushes an updated view of its clock into a virtual machine. These situations include starting the virtual machine and resuming a suspended virtual machine, If this view differs more than 1000 seconds from the view that is received over the network, the NTP service might shutdown. In this situation, the guest OS administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest operating system. The VMware recommendation is to add **tinker panic 0** to the first line of the **ntp.conf** file so that the NTP can adjust to the network time even with large differences.

If you use the names of the time servers instead of the IP address, you must configure the Domain Name Service in the guest OS before you administer the NTP service. Otherwise, the NTP service cannot locate the time servers. If you administer the NTP service first, you must restart the NTP service after administering the DNS service.

After you administer the NTP service in the application, run the `ntpstat` or `/usr/sbin/ntpq -p` command from a command window. The results from these commands:

- Verify if the NTP service is getting time from a network time source.
- Indicate which network time source is in use.
- Display how closely the guest OS matches the network time.
- Display how often the guest OS checks the time.

The guest OS polls the time source every 65 to 1024 seconds. Larger time intervals indicate that the guest clock is tracking the network time source closely. If the time source is **local**, then the NTP service is not using a network time source and a problem exists.

If the clock value is consistently wrong, look through the system log for entries regarding **ntpd**. The NTP service writes the activities it performs to the log, including when the NTP service loses synchronization with a network time source.

For more information, see *Timekeeping best practices for Linux guests* at http://kb.vmware.com/kb/1006427. The article presents best practices for Linux timekeeping to achieve best timekeeping results. The article includes:

- specifics on the particular kernel command line options to use for the Linux operating system of interest.
- recommended settings and usage for NTP time sync, configuration of VMware Tools time synchronization, and Virtual Hardware Clock configuration.

Related links

Best Practices for VMware performance and features on page 146

Configuring the NTP time

Procedure

1. Select the ESXi server and click the **Configuration** tab.
2. In the left navigation pane, click **Software** > **Time Configuration**.
3. At the upper-right side of the Time Configuration page, click **Properties...**.
4. On the Time Configuration dialog box, in the NTP Configuration area, perform the following:
   a. Select the **NTP Client Enabled** check box.
   b. Click **Options**.
5. On the NTP Daemon (ntpd) Options dialog box, perform the following:
   a. In the left navigation pane, click **NTP Settings**.
   b. Click **Add**.
   c. On the Add NTP Server dialog box, in the **NTP Server** area, enter the IP address of the NTP server.
   d. Click **OK**.

   The date and time of the System Manager virtual machine synchronizes with the NTP server.
6. Select the **Restart NTP service to apply changes** check box.
7. Click **OK**.

   The Time Configuration page displays the date and time, NTP Servers, and the status of the NTP client.

Related links

Best Practices for VMware performance and features on page 146

VMware networking best practices

You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

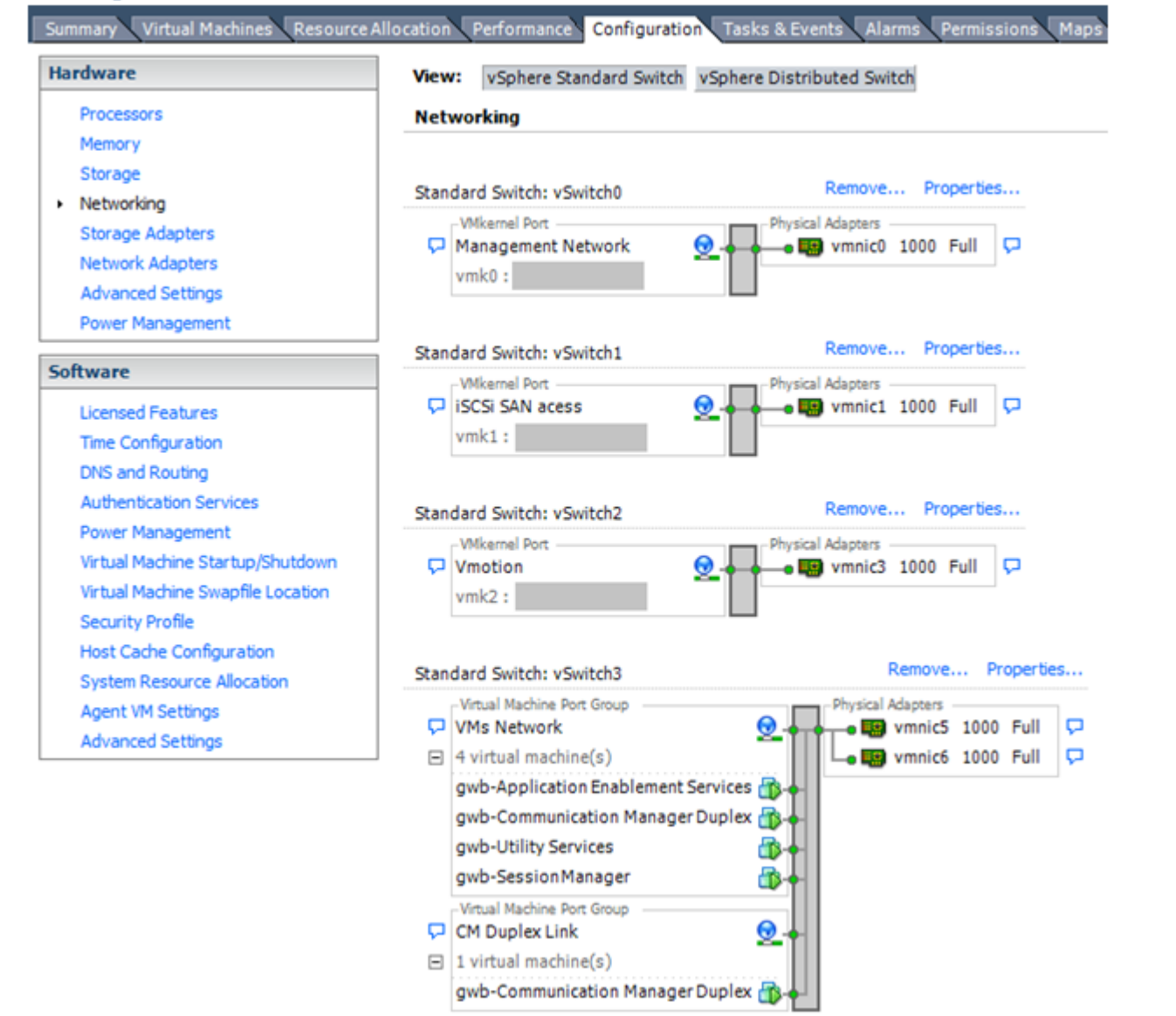
This section is not a substitute for the VMware documentation. Review the VMware networking best practices before deploying any applications on an ESXi host.

The following are the suggested best practices for configuring a network that supports deployed applications on VMware Hosts:

- Separate the network services to achieve greater security and performance by creating a vSphere standard or distributed switch with dedicated NICs for each service. If you cannot use separate switches, use port groups with different VLAN IDs.
- Configure the vMotion connection on a separate network devoted to vMotion.

- For protection, deploy firewalls in the virtual machines that route between virtual networks that have uplinks to physical networks and pure virtual networks without uplinks.
- Specify virtual machine NIC hardware type **vmxnet3** for best performance.
- Connect all physical NICs that are connected to the same vSphere standard switch to the same physical network.
- Connect all physical NICs that are connected to the same distributed switch to the same physical network.
- Configure all VMkernel vNICs to be the same IP Maximum Transmission Unit (MTU).

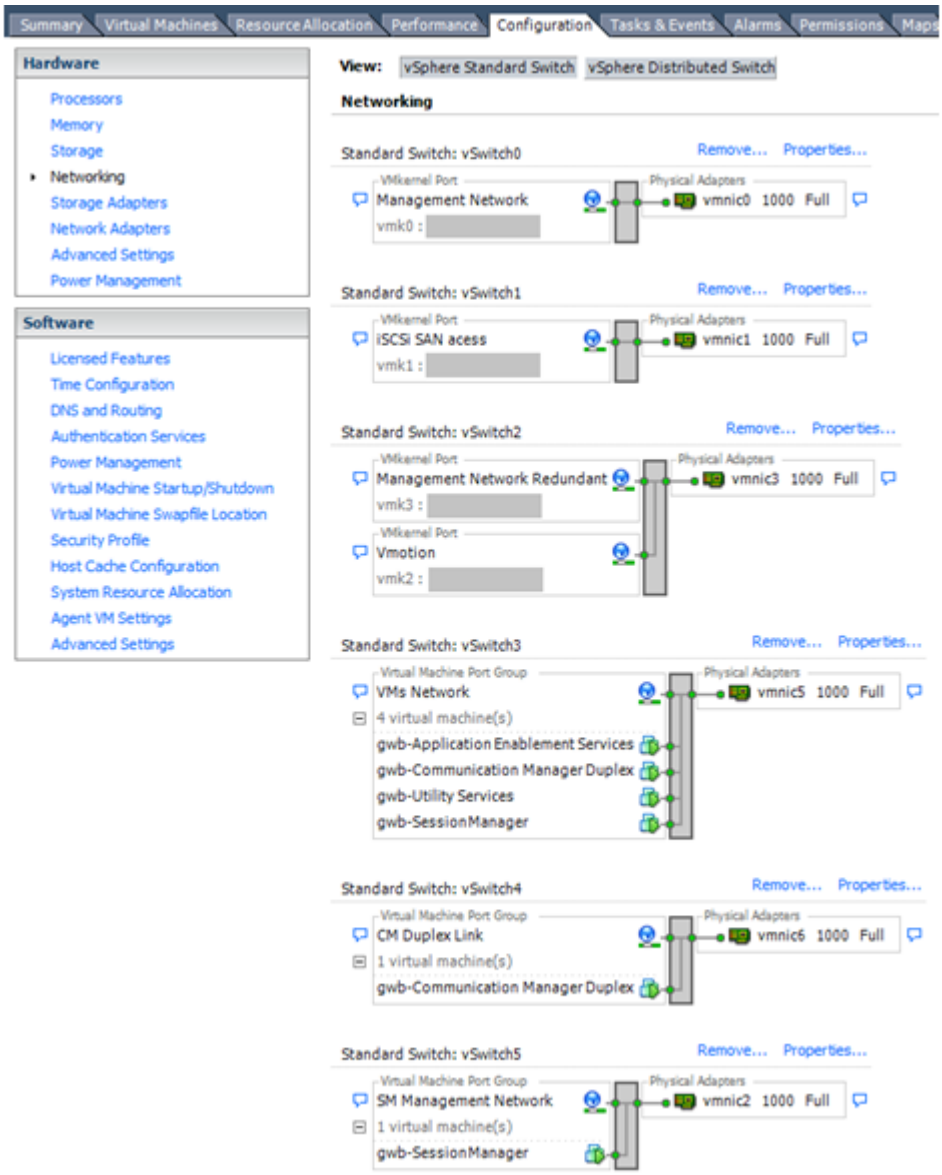
Networking Avaya applications on VMware ESXi – Example 1



This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides additional bandwidth for the Virtual Machines Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.
- Communication Manager Duplex link: Communication Manager software duplication must be separated from all other network traffic. Example 1 displays one method of separating Communication Manager Duplex with a port group combined with a VLAN. The Communication Manager software duplication link must meet specific network requirements. For more information, see Avaya PSN003556u at PSN003556u. The following are the minimum requirements of the Communication Manager software duplex connectivity:
  - The total capacity must be 1 Gbps or greater. Reserve 50 Mbps of bandwidth for duplication data.
  - The round-trip delay must be 8 ms or less.
  - The round-trip packet loss must be 0.1% or less.
  - Both servers duplication ports must be on the same IP subnet.
  - You must disable duplication link encryption for busy-hour call rates that result in greater than 40% CPU occupancy. You can view the CPU occupancy using the `list measurements occupancy` command and looking at the results under the **Static + CPU occupancy** heading.
  - The system must maintain CPU occupancy on the active server (Static + CPU) at less than 65% to provide memory refresh from the active to standby server.
- Session Manager vNIC mapping: Session Manager OVA defines four separate virtual NICs within the VM. However, example 1 shows all interfaces networked through a single virtual machine network, which is supported. If the Session Manager Management and Session Manager Asset networks are separated by subnets, you can create a VLAN for the appropriate network.
- Virtual networking: The network connectivity between virtual machines that connect to the same vSwitch is entirely virtual. In example 2, the virtual machine network of vSwitch3 can communicate without entering the physical network. Virtual networks benefit from faster communication speeds and lower management overhead.

Networking Avaya applications on VMware ESXi – Example 2



This configuration shows a complex situation using multiple physical network interface cards. The key differences between example 1 and example 2 are:

- VMware Management Network redundancy: Example 2 includes a second VMkernel Port at vSwitch2 to handle VMware Management Network traffic. In the event of a failure of vmnic0, VMware Management Network operations can continue on this redundant management network.
- Removal of Teaming for Virtual Machines Network: Example 2 removes the teamed physical NICs on vSwitch3. vSwitch3 was providing more bandwidth and tolerance of a single NIC failure instead of reallocating this NIC to other workloads.
- Communication Manager Duplex Link: vSwitch4 is dedicated to Communication Manager Software Duplication. The physical NIC given to vSwitch4 is on a separate physical network that follows the requirements described in PSN003556u at PSN003556u.

- Session Manager Management Network: Example 2 shows the Session Manager Management network separated onto its own vSwitch. The vSwitch has a dedicated physical NIC that physically segregates the Session Manager Management network from other network traffic.

References

Title	Link
Product Support Notice PSN003556u	https://downloads.avaya.com/css/P8/documents/100154621
Performance Best Practices for VMware vSphere® 5.5	http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf
Performance Best Practices for VMware vSphere® 6.0	http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf
VMware vSphere 5.5 Documentation	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html
VMware vSphere 6.0 Documentation	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html
VMware Documentation Sets	https://www.vmware.com/support/pubs/

Related links

Best Practices for VMware performance and features on page 146

Storage

When you deploy Avaya Aura® System Manager in Virtualized Environment, observe the following set of storage recommendations:

- Always deploy System Manager with a thickly provisioned disk.
- For best performance, use System Manager only on disks local to the ESXi Host, or Storage Area Network (SAN) storage devices. Do not store System Manager on an NFS storage system.

Related links

Best Practices for VMware performance and features on page 146

Thin vs. thick deployments

When creating a virtual disk file, VMware ESXi uses a thick type of virtual disk by default. The thick disk pre-allocates the space specified during the creation of the disk. For example, if you create a 10 megabyte disk, all 10 megabytes are pre-allocated for that virtual disk.

In contrast, a thin virtual disk does not pre-allocate nspace. Blocks in the VMDK file are not allocated and backed by physical storage until they are written during the normal course of

operation. A read to an unallocated block returns zeroes, but the block is not backed with physical storage until it is written. Consider the following when implementing thin provisioning in your VMware environment:

- Thin provisioned disks can grow to the full size specified at the time of virtual disk creation, but do not shrink. Once the blocks have been allocated, they cannot be un-allocated.
- By implementing thin provisioned disks, you are able to over-allocate storage. If storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked.
- If a guest operating system needs to make use of a virtual disk, the guest operating system must first partition and format the disk to a file system it can recognize. Depending on the type of format selected within the guest operating system, the format may cause the thin provisioned disk to grow to full size. For example, if you present a thin provisioned disk to a Microsoft Windows operating system and format the disk, unless you explicitly select the Quick Format option, the Microsoft Windows format tool writes information to all sectors on the disk, which in turn inflates the thin provisioned disk to full size.

Thin provisioned disks can over-allocate storage. If the storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked. You can use thin provisioned disks, but you must use strict control and monitoring to maintain adequate performance and ensure that storage is not completely consumed. If operational procedures are in place to mitigate the risk of performance and storage depletion, then thin disks are a viable option.

Related links

Best Practices for VMware performance and features on page 146

Best Practices for VMware features

VMware Snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. You can create a snapshot before upgrading or installing a patch.

The best time to take a snapshot is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

Caution:

Snapshot operations can adversely affect service. Before performing a snapshot operation, you must stop the application that is running on the virtual machine or place

the application out-of-service. When the snapshot operation is complete, start or bring the application back into service.

Snapshots can:

- Consume large amounts of data resources.
- Increase CPU loads on the host.
- Affect performance.
- Affect service.

To prevent adverse behaviors, consider the following recommendations when using the Snapshot feature:

- Do not rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- Do not run a virtual machine from a snapshot. Do not use a single snapshot for more than 24 to 72 hours.
- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.
- When taking a snapshot, do not save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user. To create a clean snapshot image from which to boot, do the following when you create a snapshot:
  - In the **Take Virtual Machine Snapshot** window, clear the **Snapshot the virtual machine's memory** check box.
  - Select the **Quiesce guest file system (Needs VMware Tools installed)** check box to ensure that all write instructions to the disks are complete. You have a better chance of creating a clean snapshot image from which to boot.
- If you are going to use snapshots for a long time, you must consolidate the snapshot files regularly to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

  Note:

  If a consolidation failure occurs, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, the system displays a warning on the user interface.

Related resources

Title	Link
Best practices for virtual machine snapshots in the VMware environment	Best Practices for virtual machine snapshots in the VMware environment
Understanding virtual machine snapshots in VMware ESXi and ESX	Understanding virtual machine snapshots in VMware ESXi and ESX
Working with snapshots	Working with snapshots
Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots	Send alarms when virtual machines are running from snapshots
Consolidating snapshots in vSphere 5.x	Consolidating snapshots in vSphere 5.x

Related links

Best Practices for VMware performance and features on page 146

VMware Cloning

System Manager does not support VMware Cloning.

Related links

Best Practices for VMware performance and features on page 146

VMware High Availability

InVirtualized Environment, use the VMware High Availability (HA) method to recover System Manager in the event of ESXi Host failure. For more information, see the High Availability documentation for VMware.

When you use VMware HA with System Manager, the communication between System Manager and Avaya Aura® Communication Manager fails. The virtual machine then starts again on a standby server, and the system starts running.

Related links

Best Practices for VMware performance and features on page 146

VMware vMotion

VMware uses the vMotion technology to migrate a running virtual machine from one physical server to another physical server without incurring downtime. The migration process, also known as a hot migration, migrates running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

With vMotion, you can:

- Schedule migration to occur at predetermined times and without the presence of an administrator.
- Perform hardware maintenance without scheduled downtime.
- Migrate virtual machines away from failing or underperforming servers.

Before using vMotion, you must:

- Ensure that each host that migrates virtual machines to or from the host uses a licensed vMotion application and the vMotion is enabled.
- Ensure that you have identical vSwitches. You must enable vMotion on these vSwitches.
- Ensure that the Port Groups are identical for vMotion.
- Use a dedicated NIC to ensure the best performance.

Note:

If System Manager WebLM is being used as a master WebLM server in an enterprise licensing deployment for a product, after migration of virtual machine to another physical server by using vMotion, validate connectivity with added local WebLM servers. This is to ensure that the master WebLM server can communicate with local WebLM servers.

Related links

Best Practices for VMware performance and features on page 146

Glossary

AFS	Authentication File System. AFS is an Avaya Web system that allows you to create Authentication Files for secure Avaya Global Services logins for supported non-Communication Manager Systems.
Appliance Virtualization Platform	Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements. Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware® tools, such as vCenter and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.
Application	A software solution development by Avaya that includes a guest operating system.
Avaya Appliance	A physical server sold by Avaya running a VMware hypervisor that has several virtual machines, each with its virtualized applications. The servers can be staged with the operating system and application software already installed. Some of the servers are sold as just the server with DVD or software downloads.
Blade	A blade server is a stripped-down server computer with a modular design optimized to minimize the use of physical space and energy. Although many components are removed from blade servers to save space, minimize power consumption and other considerations, the blade still has all of the functional components to be considered a computer.
ESXi	A virtualization layer that runs directly on the server hardware. Also known as a *bare-metal hypervisor.* Provides processor, memory, storage, and networking resources on multiple virtual machines.
Hypervisor	A hypervisor is also known as a Virtual Machine Manager (VMM). A hypervisor is a hardware virtualization technique which runs multiple operating systems on the same shared physical server.

MAC	Media Access Control address. A unique identifier assigned to network interfaces for communication on the physical network segment.
OVA	Open Virtualization Appliance. An OVA contains the virtual machine description, disk images, and a manifest zipped into a single file. The OVA follows the Distributed Management Task Force (DMTF) specification.
PLDS	Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.
Reservation	A reservation specifies the guaranteed minimum required amounts of CPU or memory for a virtual machine.
RFA	Remote Feature Activation. RFA is an Avaya Web system that you use to create Avaya License Files. These files are used to activate software including features, capacities, releases, and offer categories. RFA also creates Authentication Files for secure Avaya Global Services logins for Communication Manager Systems.
SAN	Storage Area Network. A SAN is a dedicated network that provides access to consolidated data storage. SANs are primarily used to make storage devices, such as disk arrays, accessible to servers so that the devices appear as locally attached devices to the operating system.
Snapshot	The state of a virtual appliance configuration at a particular point in time. Creating a snapshot can affect service. Some Avaya virtual appliances have limitations and others have specific instructions for creating snapshots.
Storage vMotion	A VMware feature that migrates virtual machine disk files from one data storage location to another with limited impact to end users.
vCenter Server	An administrative interface from VMware for the entire virtual infrastructure or data center, including VMs, ESXi hosts, deployment profiles, distributed virtual networking, and hardware monitoring.
virtual appliance	A virtual appliance is a single software application bundled with an operating system.
VM	Virtual Machine. Replica of a physical server from an operational perspective. A VM is a software implementation of a machine (for example, a computer) that executes programs similar to a physical machine.
vMotion	A VMware feature that migrates a running virtual machine from one physical server to another with minimal downtime or impact to end users. vMotion cannot be used to move virtual machines from one data center to another.
VMware HA	VMware High Availability. A VMware feature for supporting virtual application failover by migrating the application from one ESXi host to

another. Since the entire host fails over, several applications or virtual machines can be involved. The failover is a reboot recovery level which can take several minutes.

vSphere Client

The vSphere Client is a downloadable interface for administering vCenter Server and ESXi.

Index

Special Characters

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W