Deploying Avaya Aura® System Manager in Virtualized Environment

Release 8.1.x
Issue 9
February 2023

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” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

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 as set forth below in the Designated System(s) License (DS) section as applicable. 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 set of Designated Processors that hosts (physically or virtually) 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: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. 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. Unless otherwise stated, 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 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 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.

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for deploying the Avaya Aura® System Manager virtual application on VMware® in a customer-provided Virtualized Environment and Kernel-based Virtual Machine (KVM). It includes installation, configuration, installation verification, troubleshooting, and basic maintenance checklists and procedures.

The primary audience for this document is anyone who is involved with installing, configuring, and verifying System Manager at a customer site. For example, implementation engineers, field technicians, business partners, solution providers, and customers.

This document does not include optional or customized aspects of a configuration.

Prerequisites

Before deploying the System Manager OVA, ensure that you have the following knowledge, skills and tools.

Knowledge

- **For KVM:** KVM hypervisor installation and set up
- **For VMware:** VMware® vSphere™ virtualized environment
- Linux® Operating System
- System Manager

Skills

To administer:

- VMware® vSphere™ virtualized environment
- KVM hypervisor

Tools

For information about tools and utilities, see “Configuration tools and utilities”.

Change history

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

Issue	Date	Summary of changes
9	February 2023	Updated the following sections: • Supported footprints for System Manager on VMware on page 23 • Supported footprints for System Manager on KVM on page 24
8	June 2022	Updated the section: Downloading software from PLDS on page 17
7	November 2020	Updated the section: Capability and scalability specification on page 66
6	October 2020	For Release 8.1.3, updated the following sections: • VMware software requirements on page 19 • Supported ESXi version on page 19 • Deploying the System Manager OVA file by using the Solution Deployment Manager client on page 32 • Adding a vCenter to Solution Deployment Manager on page 55 • New vCenter and Edit vCenter field descriptions on page 58
5	May 2020	Updated the section: Storage on page 138
4	March 2020	For Release 8.1.2, updated the following sections: • Customer configuration data for System Manager on page 21 • Installing the mandatory System Manager Release 8.1.3 patch on page 34 • Configuring the network parameters from console on page 86 • Network and configuration field descriptions on page 89 • Creating a data backup on a remote server on page 102 • Creating a data backup on a local server on page 103 • Restoring a backup from a remote server on page 104 • Restoring data backup from a local server on page 105
3	October 2019	For Release 8.1.1, updated the following sections: • Software details of System Manager on page 25 • Deployment checklist on page 26 • Installing the mandatory System Manager Release 8.1.3 patch on page 34 • Deploying the System Manager OVA file by using the Solution Deployment Manager client on page 32

Table continues…

Issue	Date	Summary of changes
2	July 2019	Updated the following sections: • Deploying the System Manager OVA by using vSphere Web Client on page 27 • Deploying the System Manager OVA using vSphere Web Client by accessing the host directly on page 30
1	June 2019	Release 8.1 document.

Chapter 2: Virtualized Environment overview

You can deploy the Avaya Aura® applications in one of the following Virtualized Environment:

- VMware in customer-provided Virtualized Environment

  Avaya Solutions Platform 130 Appliance (Dell PowerEdge R640) is a single host server with ESXi 6.5 preinstalled.

- Kernel-based Virtual Machine Virtualized Environment

Avaya Aura® Virtualized Environment overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® and Kernel-based Virtual Machine (KVM).

Kernel-based Virtual Machine overview

Kernel-based Virtual Machine (KVM) is a virtualization infrastructure for the Linux kernel that turns the Linux kernel into a hypervisor. You can remotely access the hypervisor to deploy applications on the KVM host.

Supported applications in Virtualized Environment

Application	Release	VMware	KVM
Avaya Aura® System Manager	Release 8.1.3	Y	Y
Avaya WebLM	Release 8.1.3	Y	Y
Avaya Aura® Session Manager	Release 8.1.3	Y	Y
Avaya Aura® Communication Manager	Release 8.1.3	Y	Y

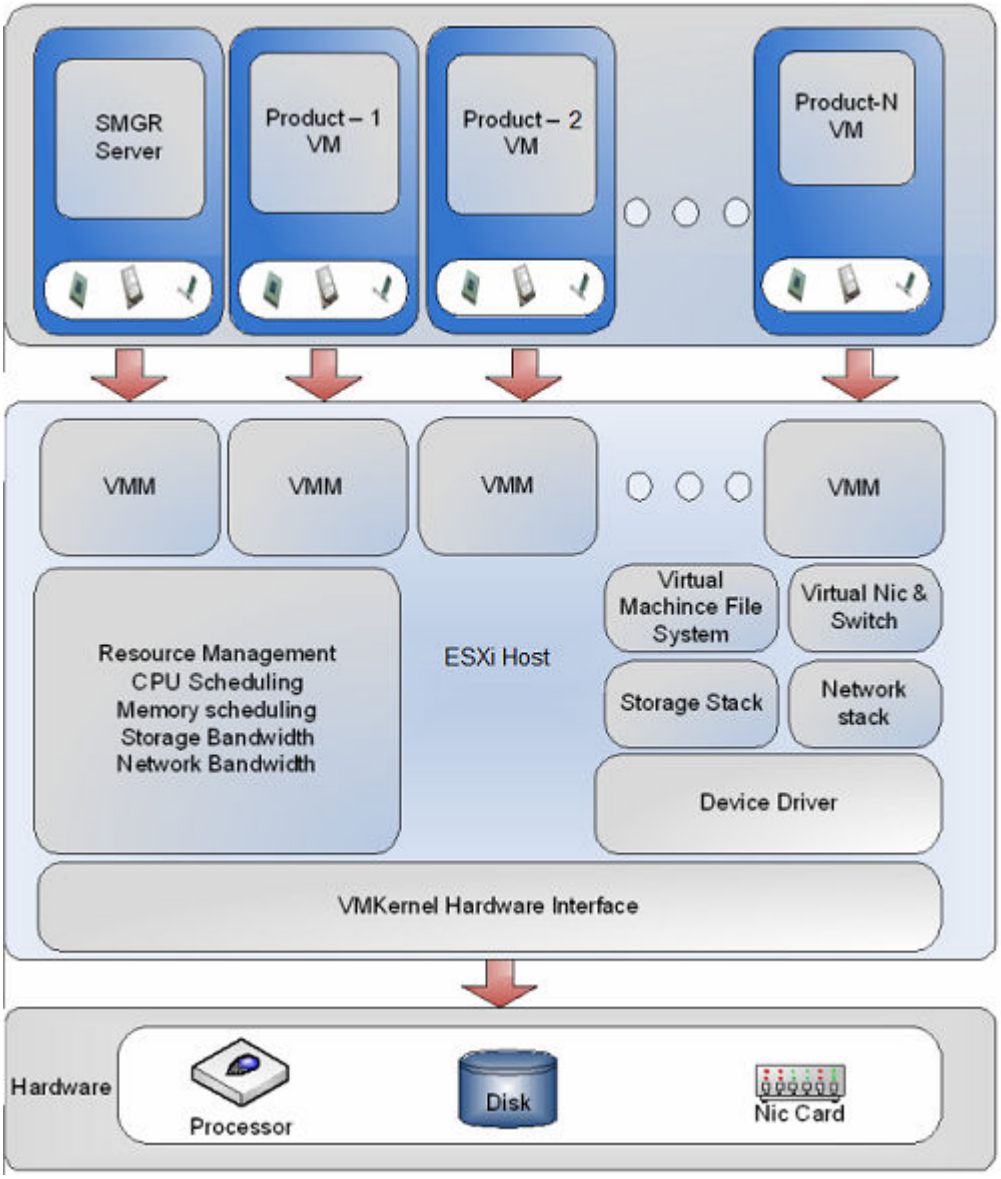
Table continues…

Application	Release	VMware	KVM
Avaya Aura® AVP Utilities	Release 8.1.3	—	—
Avaya Aura® Application Enablement Services	Release 8.1.3	Y	Y
Avaya Aura® Media Server (Software only)	Release 8.0	Y	Y

For information about other Avaya product compatibility information, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Topology

The following is an example of a deployment infrastructure for System Manager on VMware.



Virtualized Environment components

Virtualized component	Description
Open Virtualization Appliance (OVA)	The virtualized OS and application packaged in a single file that is used to deploy a virtual machine.
VMware	
ESXi Host	The physical machine running the ESXi Hypervisor software.

Table continues…

Virtualized component	Description
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.
vSphere Web Client	Using a Web browser, vSphere Web Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.
vSphere Client (HTML5)	vSphere Client (HTML5) is available from vSphere 6.5 and later. Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. This is the only vSphere client administration tool after the next vSphere release.
vCenter Server	vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion.
KVM	
KVM hypervisor	A platform that runs multiple operating systems on a host computer at the same time.

Chapter 3: Planning and preconfiguration

Planning Checklist

Planning checklist for deploying System Manager on VMware

Complete the following tasks before deploying System Manager on VMware:

No.	Task	Link/Notes	✔
1.	Download the required software and patches.	Downloading software from PLDS on page 17 Latest software updates and patch information on page 18	
2.	Obtain the required licenses.	—	
3.	Register for PLDS, and activate license entitlements.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
4.	Verify the software compatibility.	VMware software requirements on page 19	
5.	Keep the following information handy to create a backup on the remote server: • IP address • Directory • User Name • Password	Customer configuration data for System Manager on page 21	

Planning checklist for deploying System Manager on KVM

Ensure that you complete the following before deploying System Manager on KVM:

No.	Task	Link/Notes	✔
1.	Download the required software.	Downloading software from PLDS on page 17 Latest software updates and patch information on page 18	
2.	Purchase and obtain the required licenses.	—	
3.	Register for PLDS and activate license entitlements.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
4.	Prepare the site.	Supported hardware and software for KVM on page 19 Site preparation checklist for KVM on page 21	

Downloading software from PLDS

When you place an order for an Avaya Product Licensing and Delivery System (PLDS)-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements.

In addition to PLDS, you can download the product software from http://support.avaya.com using the **Downloads and Documents** tab at the top of the page.

Note:

Only the latest service pack for each release is posted on the support site. Previous service packs are available only through PLDS.

Procedure

1. On your web browser, type http://plds.avaya.com to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS Home page, select **Assets**.
4. Click **View Downloads**.
5. Click the search icon for Company Name.

6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. In the **Download Manager** box, click the appropriate **Download** link.

   Note:

   The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.
10. If you use the Download Manager, click **Details** to view the download progress.
11. Select a location where you want to save the file, and click **Save**.
12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Latest software updates and patch information

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest release notes, Product Support Notices (PSNs), and Product Correction Notices (PCNs) for the product or solution on the Avaya Support web site at https://support.avaya.com/.

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you need to download and install any updates or patches.

VMware software requirements

Customer-provided Virtualized Environment offer supports the following software versions:

- VMware® vSphere ESXi 6.0, 6.5, 6.7, or 7.0
- VMware® vCenter Server 6.0, 6.5, 6.7, or 7.0

Note:

- Avaya Aura® Release 8.0.1 and later does not support vSphere ESXi 5.0 and 5.5.
- With VMware® vSphere ESXi 6.5, vSphere Web Client replaces the VMware® vSphere Client for ESXi and vCenter administration.

Supported hardware 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 https://www.vmware.com/guides.html.

Supported hardware and software for KVM

To deploy the Avaya Aura® application KVM OVA on a customer-provided server, the server must be on the Red Hat supported server list for Red Hat Enterprise Linux 7.6.

Supported ESXi version

The following table lists the supported ESXi versions of Avaya Aura® applications.

ESXi version	Avaya Aura® Release			
	7.0.x	7.1.x	8.0.x	8.1.x
ESXi 5.0	Y			
ESXi 5.1	Y			
ESXi 5.5	Y	Y		
ESXi 6.0		Y	Y	Y
ESXi 6.5		Y	Y	Y
ESXi 6.7			Y	Y

Table continues…

ESXi version	Avaya Aura® Release			
	7.0.x	7.1.x	8.0.x	8.1.x
ESXi 7.0				Y

Note:

- With VMware® vSphere ESXi 6.5, vSphere Web Client replaces the VMware vSphere Client for ESXi and vCenter administration.
- Avaya Aura® applications support the ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 6.7 can be VMware ESXi 6.7 Update 3.
- Only the Encrypted Core Session Manager (8.1E OVA) is supported on VMware ESXi 7.0.
- Application Enablement Services Release 8.1.1 OVA is supported on VMware ESXi 7.0.

Supported servers for Avaya Aura® applications

The following table lists the supported servers of Avaya Aura® applications.

Supported servers	Avaya Aura® Release			
	7.0.x	7.1.x	8.0.x	8.1.x
S8300D	Y	Y		
S8300E	Y	Y	Y	Y
HP ProLiant DL360 G7	Y	Y		
HP ProLiant DL360p G8	Y	Y	Y	Y
HP ProLiant DL360 G9	Y	Y	Y	Y
Dell™ PowerEdge™ R610	Y	Y		
Dell™ PowerEdge™ R620	Y	Y	Y	Y
Dell™ PowerEdge™ R630	Y	Y	Y	Y
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 *			Y	Y
Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 **			Y	Y

*Avaya Solutions Platform 120 Appliance supports virtualization using Appliance Virtualization Platform.

**Avaya Solutions Platform 130 Appliance supports virtualization using VMware vSphere ESXi Standard License.

Note:

From Avaya Aura® Release 8.0 and later, S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers are not supported.

Site preparation checklist for KVM

Use the following checklist to know the set up required to deploy the KVM OVA.

No.	Task	Description	✔
1	Install the KVM hypervisor.		
2	Install the MobaXterm and Xming softwares on your laptop/computer.	To remotely access the KVM hypervisor, the Virt Manager GUI, and Virsh command line interface.	

Customer configuration data for System Manager

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

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.

Important:

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

Required data	Description	Example Value for the system	✔
IP address	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	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.	

Table continues…

Required data	Description	Example Value for the system	✔
Domain name	not enabled, Public network configuration is optional.	mydomain.com	
Default search list		mydomain.com	
NTP server		172.16.1.100	
Time zone		America/Denver	
VFQDN short hostname	VFQDN	grsmgr	
VFQDN domain name		dev.com	
User Name Prefix	SNMP Parameters	org	
Authentication Protocol Password		orgpassword	
Privacy Protocol Password		orgpassword	
Backup Definition parameters	See Backup Definition Parameters	-	
EASG status	EASG	Enable or Disable	
Data Encryption	Data Encryption	Enable or Disable	

Configuration tools and utilities

You must have the following tools and utilities for deploying and configuring System Manager application:

- Solution Deployment Manager client running on your computer
- If you are running a VMware server then a remote computer running the VMware vSphere Client
- A browser for accessing the System Manager and the Solution Deployment Manager Client web interface
- An SFTP client for Windows, for example WinSCP
- An SSH client, for example, PuTTY and PuTTYgen

Supported footprints

Supported footprints for System Manager on VMware

The following table describes the resource requirements to support different profiles for System Manager on VMware customer-provided Virtualized Environment.

Note:

- Avaya Aura® System Manager supports VMware hosts with Hyper-threading enabled at the BIOS level.
- Reservations are not permitted for Avaya Solutions Platform 4200 series solutions (formerly known as CPOD/PodFx) deployment. For reservationless deployment of Avaya Aura® applications, see the recommendations given in *Application Notes on Best Practices for Reservationless deployment of Avaya Aura® software release 8.1 on VMware*.

  Ensure to consider reservations for deploying Avaya Aura® applications on Appliance Virtualization Platform, Avaya Solutions Platform 130, and Avaya Solutions Platform S8300.

Resource	Profile 2	Profile 3	Profile 4
vCPU Reserved	6	8	18
Minimum vCPU Speed	2185 MHz	2185 MHz	2185 MHz
CPU reservation	13110 MHz	17480 MHz	39330 MHz
Virtual RAM	12 GB	18 GB	36 GB
Memory reservation	12288 MB	18432 MB	36864 MB
Virtual Hard Disk	105 GB	250 GB	850 GB
Shared NICs	1	1	1
IOPS	44	44	44
Number of users	>35000 to 250000 users with up to 250 Branch Session Manager and 12 Session Manager	>35000 to 250000 users with up to 500 Branch Session Manager and 28 Session Manager	>35000 to 300000 users with up to 5000 Branch Session Manager and 28 Session Manager

Note:

From Release 8.0 and later, System Manager Profile 1 is not supported. If System Manager is on a pre Release 8.0 and using the Profile 1, ensure that the server has the required resources to configure Profile 2 on Release 8.0 and later.

Related links

Adjusting the System Manager virtual machine properties on page 24

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.

Related links

Supported footprints for System Manager on VMware on page 23

Supported footprints for System Manager on KVM

Note:

Avaya Aura® System Manager supports VMware hosts with Hyper-threading enabled at the BIOS level.

Footprint	Profile 2	Profile 3	Profile 4
Number of vCPUs	6	8	18

Table continues…

Footprint	Profile 2	Profile 3	Profile 4
RAM (GB)	12	18	36
HDD (GB)	105	250	850
NICs	1	1	1
Number of users	250000	250000	300000

Note:

From Release 8.0 and later, System Manager Profile 1 is not supported. If System Manager is on a pre Release 8.0 and using the Profile 1, ensure that the server has the required resources to configure Profile 2 on Release 8.0 and later.

Software details of System Manager

For Avaya Aura® application software build details, see Avaya Aura® Release Notes on the Avaya Support website at http://support.avaya.com/.

Supported tools for deploying the KVM OVA

You need one of the following tools to deploy KVM OVA:

- Virt Manager GUI
- Virsh command line interface

Deployment guidelines

- Deploy maximum number of virtualized environments on the same host.
- Deploy the virtualized environment on the same cluster if the cluster goes beyond the host boundary.
- Segment redundant elements on a different cluster, or ensure that the redundant elements are not on the same host.
- Plan for rainy day scenarios or conditions. Do not configure resources only for traffic or performance on an average day.
- Do not oversubscribe resources. Oversubscribing affects performance.
- Monitor the server, host, and virtualized environment performance.

Chapter 4: Deploying System Manager on VMware

Deployment checklist

Use the following checklist to deploy the System Manager Release 8.1.3 OVA by using vSphere Web Client.

Note:

- Deployment of the System Manager OVA by using the vApps option is not supported.
- Deployment of the System Manager OVA by using vSphere Client is not supported.
- Deployment of the System Manager OVA using vSphere Web Client by accessing the ESXi host 6.7 directly might fail. Therefore, to deploy the System Manager OVA, use vCenter 6.7 (HTML5) or Solution Deployment Manager Client.

#	Action	Link/Notes	✔
1	From the Avaya Support website at http://support.avaya.com, download the System Manager OVAs and System Manager Release 8.1.3 bin files.	For information about the software build details, see *Avaya Aura® Release Notes* on the Avaya Support website.	
2	Gain access to vCenter and vSphere Web Client.	Download from the VMware website. **Note:** With VMware® vSphere ESXi 6.5, vSphere Web Client replaces the VMware vSphere Client for ESXi and vCenter administration. **Note:** In vSphere 6.0 and later, the vSphere Web Client is installed as part of the vCenter Server on Windows or the vCenter Server Appliance deployment.	

Table continues…

#	Action	Link/Notes	✔
3	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. Ensure that the license file copies are accessible.	-	
4	Ensure that the following information is handy: • FQDN/IP address, netmask, and gateway • Out of Band Management configuration details.	Customer configuration data for System Manager on page 21 "Out of Band Management configuration"	
5	Deploy the System Manager OVA file.	-	
6	You can perform one of the following to start the virtual machine. • Configure the System Manager virtual machine to start automatically after the deployment. • Start the System Manager virtual machine.	-	
7	Verify network parameters.	-	
8	Verify the deployment of the System Manager virtual machine.	-	
9	In the settings icon (☰), click **About** to verify that the System Manager version is Release 8.1.3.	-	
10	(Optional) Reconfigure the hardware resources for flexible footprint.	-	
11	Install the System Manager Release 8.1.3 bin file. The patch installation takes about 45 minutes to complete.	-	

Deploying the System Manager OVA by using vSphere Web Client

Before you begin

- Access vCenter Server by using vSphere Web Client.
- Download the Client Integration Plug-in.

Procedure

1. On the web browser, type the following URL: `https://<vCenter FQDN or IP Address>/vsphere-client/`.
2. To log in to vCenter Server, do the following:
   a. In **User name**, type the user name of vCenter Server.
   b. In **Password**, type the password of vCenter Server.
3. Right-click the ESXi host and select **Deploy OVF Template**.

   The system displays the Deploy OVF Template dialog box.
4. On the Select template page, do one of the following:
   - To download the System Manager OVA from a web location, select **URL**, and provide the complete path of the OVA file.
   - To access the System Manager OVA from the local computer, select **Locate file**, click **Browse**, and navigate to the OVA file.
5. Click **Next**.
6. On the Select name and location page, do the following:
   a. In **Name**, type a name for the virtual machine.
   b. In **Browse**, select a datacenter.
7. Click **Next**.
8. On the Select a resource page, select a host, and click **Next**.
9. On the Review details page, verify the OVA details, and click **Next**.
10. To accept the End User License Agreement, on the Accept license agreements page, click **Accept**.
11. Click **Next**.
12. On the Select configuration page, in **Configuration**, select the required profile.
13. Click **Next**.
14. On the Select storage page, in **Select virtual disk format**, click the required disk format.
15. Click **Next**.
16. On the Select networks page, select the destination network for each source network.
17. Click **Next**.
18. On the Customize template page, enter the configuration and network parameters.

    For more information about the configuration and network parameters, see Network and configuration field descriptions on page 89.

Note:

- If you do not provide the details in the mandatory fields, you cannot turn 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.

19. Click **Next**.
20. On the Ready to complete page, review the settings, and click **Finish**.

    Wait until the system deploys the OVA file successfully.
21. To start the System Manager virtual machine, if System Manager is not already powered on perform one of the following steps:
    - Click VM radio button, and click **Actions** > **Power** > **Power On**.
    - 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.
22. Click the **Console** tab and verify that the system startup is successful.

Next steps

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. Once the configuration is complete, the log file displays the message: `exit status of eject command is 0`.

To verify that the System Manager installation is complete and the system is ready for patch deployment, do one of the following:

- On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, and ensure that the system displays the System Manager Log on page.

  The system displays the message: Installation of latest System Manager patch is mandatory.
- On the Command Line Interface, log on to the System Manager console, and verify that the system does not display the message: `Maintenance: SMGR Post installation configuration is In-Progress`.

  It should only display the message: `Installation of latest System Manager patch is mandatory`.

Note:

Modifying the network or management configuration is not recommended before the patch deployment.

Deploying the System Manager OVA using vSphere Web Client by accessing the host directly

Before you begin

- Access vCenter Server by using vSphere Web Client.
- Download the Client Integration Plug-in.
- This procedure is applicable for ESXi 6.5 u2 onwards.

Procedure

1. On the Web browser, type the host URL: `https://<Host FQDN or IP Address>/ui`.
2. Enter login and password.
3. Right-click an ESXi host and select **Create/Register VM**.

   The system displays the New virtual machine dialog box.
4. On the Select creation type page, select **Deploy a virtual machine from an OVF or OVA file**.
5. Click **Next**.
6. On the Select OVF and VMDK file page, do the following:
   a. Type a name for the virtual machine.
   b. Click to select files or drag and drop the OVA file from your local computer.
7. Click **Next**.
8. On the Select storage page, select a datastore, and click **Next**.
9. To accept the End User License Agreement, on the License agreements page, click **I Agree**.
10. Click **Next**.
11. On the Deployment options page, perform the following:
    a. From **Network mappings**, select the required network.
    b. From **Disk provisioning**, select the required disk format.
    c. From **Deployment type**, select profile.
    d. Uncheck **Power on automatically**.
12. Click **Next**.
13. On the Additional settings page, click **Next**.
14. On the Ready to complete page, review the settings, and click **Finish**.

    Wait until the system deploys the OVA file successfully.

15. To edit the virtual machine settings, click VM radio option and perform the following:
    - Click **Actions** > **Edit Settings** to edit the required parameters.

      Note:
    - Click **Save**.

    Note:

    Ensure that the virtual machine is powered down to edit the settings.
16. To ensure that the virtual machine automatically starts after a hypervisor reboot, click VM radio option, and click **Actions** > **Autostart** > **Enable**.

    Note:

    If you do not enable autostart, you must manually start the virtual machine after the hypervisor reboot. Autostart must be enabled on the Host for the virtual machine autostart to function.
17. To start the System Manager virtual machine, if System Manager is not already powered on perform one of the following steps:
    - Click VM radio option, and click **Actions** > **Power** > **Power On**.
    - 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.

    When the system starts for the first time, configure the parameters for System Manager. For more information about the configuration and network parameters, see Network and configuration field descriptions on page 89.
18. Click **Actions** > **Console**, select the open console type, verify that the system startup is successful, then input the System Manager configuration parameters.

Next steps

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. Once the configuration is complete, the log file displays the message: `exit status of eject command is 0`.

To verify that the System Manager installation is complete and the system is ready for patch deployment, do one of the following:

- On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, and ensure that the system displays the System Manager Log on page.

  The system displays the message: Installation of latest System Manager patch is mandatory.
- On the Command Line Interface, log on to the System Manager console, and verify that the system does not display the message: `Maintenance: SMGR Post installation configuration is In-Progress`.

It should only display the message: `Installation of latest System Manager patch is mandatory`.

Note:

Modifying the network or management configuration is not recommended before the patch deployment.

Deploying the System Manager OVA file by using the Solution Deployment Manager client

About this task

Use the procedure to deploy System Manager by using the Solution Deployment Manager client.

Before you begin

- Install the Solution Deployment Manager client on your computer.
- Add a location.

  For information, see Adding a location on page 51.
- Add the ESXi, vCenter, or Appliance Virtualization Platform host.

  For information about adding the Appliance Virtualization Platform or ESXi host, see Adding an Appliance Virtualization Platform or ESXi host on page 51.

  For information about adding vCenter, see Adding a vCenter to Solution Deployment Manager on page 55.
- Ensure to establish the trust with AVP Utilities.

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 **Application Management Tree**, select a platform.
3. On the **Applications** tab, in the Applications for Selected Host <host name> section, click **New**.

   System Manager displays the Applications Deployment window.
4. In the Select Location and Platform section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Platform**, select a platform.

      The system displays the host name in the **Platform FQDN** field.
5. In **Data Store**, select a data store, if not displayed upon host selection.

   The page displays the capacity details.

6. Click **Next**.
7. On the **OVA** tab, click one of the following:
   - **URL**, in the **OVA File** field, type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the System Manager OVA file, and click **Submit**.
   - **S/W Library**, in the **File Name** field, select the System Manager OVA file from the drop-down list.

     To use the **S/W Library** option, the OVA file must be present in the local software library directory that is defined during the Solution Deployment Manager client installation. The system displays the directory name when the **S/W Library** option is selected.
   - **Browse**, select the required OVA file from your local computer, and click **Submit File**.

   When you select the OVA, the system:
   - Displays the CPU, memory, and other parameters in the Capacity Details section.
   - Disables the **Flexi Footprint** field.
8. **(Optional)** To install the System Manager bin file, click **Service or Feature Pack**, and enter the appropriate parameters.
   - **URL**, and type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the latest service or feature pack.
   - **S/W Library**, and select the latest service or feature pack from the drop-down list.
   - **Browse**, and select the latest service or feature pack from your local computer, and click **Submit File**.

   You can install the System Manager Release 8.1.3 bin file now or after completing the System Manager OVA deployment.

   If you do not provide the System Manager Release 8.1.3 bin file at the time of deploying the System Manager OVA, the system displays the following message:

   ```
   Installation of the latest System Manager patch is mandatory. Are
   you sure you want to skip the patch installation?
   If Yes, ensure to manually install the System Manager patch later.
   ```
9. Click **Next**.

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

    For more information, see “Application Deployment field descriptions”.
11. In the Network Parameters section:
    - For Appliance Virtualization Platform, the system auto populates the following fields and these fields are read only:
      - **Public**

- **Out of Band Management**

• For the ESXi host, select the required port groups.

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

    In the Platforms 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 Applications for Selected Location <location name> page.
14. To view details, click the **Status Details** link.

Next steps

To configure System Manager, log on to the System Manager web console. At your first log in, change the System Manager web console credentials.

Update the user password for the system to synchronize the data from applications.

When System Manager is operational, you can use Solution Deployment Manager from System Manager to deploy all other Avaya Aura® applications or continue to use the Solution Deployment Manager client.

Deployment of cloned and copied OVAs

To redeploy a virtual machine, do *not* create a copy of the virtual machine or clone the virtual machine. These processes have subtle technical details that require a thorough understanding of the effects of these approaches. To avoid any complexities and unexpected behavior, deploy a new OVA on the virtual machine. At this time, Avaya only supports the deployment of new OVAs.

Installing the mandatory System Manager Release 8.1.3 patch

About this task

Note:

After enabling data encryption and installing the System Manager 8.1.2 and later patch, if the local or remote key store is not enabled, the Data Encrypted server prompts for the encryption passphrase. Once you enter the encryption passphrase, the system automatically reboots. This happens only after first reboot and prompts you to add the encryption passphrase one more time.

Before you begin

- Ensure that System Manager is running on Release 8.1.
- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the  icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.
- Download the `System_Manager_R8.1.x_xxxx_manadatoryPatch.bin` file from the Avaya Support website at http://support.avaya.com/ and copy the file to the `/swlibrary` location on System Manager.

Procedure

1. Create the snapshot of the System Manager application.

   This activity might impact the service.

2. At the CLI 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 45 minutes to complete.

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

4. Perform one of the following:
   - 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.

     To collect logs, you can run the **`collectLogs`** command. The system creates a `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file at `/swlibrary` directory. Copy the `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file to remote server and share the file with Avaya Support Team.

Next steps

Note:

Modifying the network or management configuration is not recommended before the patch deployment.

Log on to the System Manager web console. At your first log in, change the System Manager web console credentials.

Starting the System Manager virtual machine

About this task

The system packages System Manager and other products for VMware in the .OVA package format. You can install the OVA file using vSphere Web Client.

Before you begin

Deploy the System Manager OVA.

Procedure

On vSphere Web Client, start the System Manager virtual machine by doing one of the following:

- Click VM radio option, and click **Actions** > **Power** > **Power On**.
- 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.

Chapter 5: Deploying System Manager on Kernel-based Virtual Machine

Extracting KVM OVA

Procedure

1. Create a folder on the KVM host and copy the application KVM OVA in the created folder.
2. Type the command **`tar -xvf`** *<application_KVM.ova>*.

   The system extracts the files from the application KVM OVA.

Deploying System Manager KVM OVA by using Virt Manager

Before you begin

- Access the KVM host remotely using mobaXterm or equivalent application.
- Create a folder on the KVM host and copy the System Manager KVM OVA in the created folder.
- Extract the System Manager KVM OVA files.

Procedure

1. On the KVM host, run the command: `virt-manager`.
2. On the Virtual Machine Manager window, click **File** > **New Virtual Machine**, and select **Import existing disk image** option.
3. On the Create a new virtual machine Step 1 of 4 window, select **Import existing disk image**.
4. Click **Forward**.
5. On the Create a new virtual machine Step 2 of 4 window, perform the following:
   a. In **Provide the existing storage path**, click **Browse**, and select the qcow2 image of System Manager on the KVM host.
   b. In **OS type**, select **Linux**.

c. In **Version**, select **Red Hat Linux Enterprise 7.6**.

d. Click **Forward**.

6. On the Create a new virtual machine Step 3 of 4 window, perform the following:

a. In **Memory (RAM)**, enter the required memory. For more information, see “Supported footprints for System Manager on KVM”.

b. In **CPU**, enter the number of CPUs for the virtual machine based on the application profile.

c. Click **Forward**.

7. On the Create a new virtual machine Step 4 of 4 window, perform the following:

a. In **Name**, type the name of the virtual machine.

b. Select the **Customize Configuration before Install** check box.

c. Check **Network selection** and verify the required network interface.

d. Click **Finish**.

8. In the left navigation pane, click **Disk 1**. In the **Advanced options** section, perform the following:

a. In **Disk bus**, select **IDE**.

b. In **Storage format**, type `qcow2`.

c. Click **Apply**.

9. In the left navigation pane, click **Boot Options** and perform the following:

a. In **Boot device order**, click **Hard Disk**.

b. Click **Apply**.

10. Click **Begin Installation**.

The system creates a new System Manager virtual machine.

Next steps

On first boot of the virtual machine, provide the System Manager configuration and networking parameters.

Deploying System Manager KVM from CLI by using virsh

Before you begin

- Access the KVM host remotely using mobaXterm or equivalent application.
- Create a folder on the KVM host and copy the System Manager KVM OVA in the created folder.
- Extract the System Manager KVM OVA files.

Procedure

On the KVM host CLI, perform the following:

a. Navigate to the System Manager KVM OVA directory.

b. Run the System Manager installation utility, type the command: `sh SMGR-installer.sh <System Manager KVM OVF file>`.

c. When the system prompts, select the required System Manager profile.

d. In **VM name**, type a name of the virtual machine.

e. In **Drive storage location**, type storage location of the virtual machine.

f. In **Out of Band Management network**, select the network.

g. In **Public network**, select the public network.

The system displays the command to deploy the image.

h. To continue, type `Y`.

The system displays the message: `Deploying image`.

i. Access the System Manager virtual machine that was deployed using mobaXterm or equivalent application.

Next steps

On first boot of the virtual machine, provide the System Manager configuration and networking parameters.

For more information about the configuration and network parameters, see Network and configuration field descriptions on page 89.

Deploying System Manager KVM OVA by using OpenStack

Connecting to OpenStack Dashboard

Before you begin

- Create an OpenStack account.
- Acquire adequate permission to upload and deploy the KVM ova.

Procedure

1. In your web browser, type the OpenStack URL.

   For example, http://<openstack.xyz.com>/horizon.

2. In **Domain**, type the domain name.

3. In **User Name**, type the user name.

4. Click **Connect**.

   The system displays the Instance Overview - OpenStack Dashboard page.

Uploading the qcow2 image

Procedure

1. Connect to OpenStack Dashboard.
2. In the left navigation pane, click **Project** > **Compute** > **Images**.
3. On the Images page, click **Create Image**.

   The system displays the Create An Image dialog box.
4. In **Name**, type the name of the image.
5. In **Description**, type the description of the image.
6. In **Image Source**, click **Image Location** or **Image File**, and perform one of the following:
   - In **Image Location**, type the exact URL of the qcow2 image.
   - In **Image File**, click **Browse**. In the Choose File to Upload dialog box, select the qcow2 image from your local system, and click **Open**.
7. In **Format**, click **QCOW2 - QEMU Emulator**.
8. Click **Create Image**.

   The system displays the created image on the Images page.

Flavors

Flavors are footprints of an application. The administrator must create flavors for each application.

For information about the footprints, see the profiles and footprints information for the application.

Creating a security group

About this task

Security groups are sets of IP filter rules. Each user must create security groups to specify the network settings for the application.

Procedure

1. Connect to OpenStack Dashboard.
2. In the left navigation pane, click **Project** > **Compute** > **Access & Security**.
3. On the Access & Security page, click **Create Security Group**.

   The system displays the Create Security Group dialog box.
4. In **Name**, type the name of the security group.
5. In **Description**, type the description of the security group.

6. Click **Create Security Group**.

   The system displays the created security group on the Access & Security page.

Next steps

Add rules to security group.

Related links

Adding rules to a security group on page 41

Adding rules to a security group

Before you begin

Create a security group.

Procedure

1. On the Access & Security page, click **Manage Rules** that is corresponding to the created security group.
2. On the Access & Security / Manage Security Group Rules page, click **Add Rule**.

   The system displays the Add Rule dialog box.
3. In **Rule**, click a rule

   The system displays the fields that are associated with the selected rule.
4. Enter the appropriate values in the fields.
5. Click **Add**.

   The system displays the created rule on the Access & Security / Manage Security Group Rules page.

Related links

Creating a security group on page 40

Deploying application by using OpenStack

Before you begin

- Create flavors.
- Create a security group.

Procedure

1. Connect to OpenStack Dashboard.
2. In the left navigation pane, click **Project** > **Compute** > **Instances**.
3. On the Instance page, click **Launch Instance**.

   The system displays the Launch Instance dialog box.

4. In **Details**, perform the following:
    a. In **Instance Name**, type a name of the instance.
    b. In **Availability zone**, select the availability zone of the instance.
    c. Click **Next**.
5. In **Source**, perform the following:
    a. In the **Available** section, select a check box corresponding to an instance image.

       The system displays the selected image in the **Allocated** section.
    b. Click **Next**.
6. In **Flavors**, perform the following:
    a. In the **Available** section, select a check box corresponding to a flavor name.

       The system displays the selected flavor in the **Allocated** section.
    b. Click **Next**.
7. In **Networks**, perform the following:
    a. In the **Available** section, select a check box corresponding to a network name.

       The system displays the selected network in the **Allocated** section.
    b. Click **Next**.
8. In **Network Ports**, leave the default settings, and click **Next**.
9. In **Security Groups**, perform the following:
    a. In the **Available** section, select a check box corresponding to a security group name.

       The system displays the selected security group in the **Allocated** section.
    b. Click **Next**.
10. In **Key Pair**, leave the default settings, and click **Next**.
11. In **Configuration**, leave the default settings, and click **Next**.
12. In **Metadata**, leave the default settings.
13. Click **Launch Instance**.

    The system displays the created instance on the Instances page. The **Status** column displays: `Spawning`. When the system creates the application instance, the **Status** column displays: `Active`.

    The system displays the static IP Address of the application in the **IP Address** column.

Next steps

Configure the application instance. Use the static IP Address to configure the application instance.

Configuring application instance

Procedure

1. On the Instances page, in the **INSTANCE NAME** column, click the application instance name.
2. On the Instances / <Instance Name> page, click **Console**.
3. On the Instance Console page, go to console, and follow the prompt to configure the application instance.

Deploying System Manager KVM OVA by using Nutanix

Logging on to the Nutanix Web console

Procedure

1. To log on to the Nutanix Web console, in your web browser, type the PRISM URL.

   For example, http://<PRISM_IPAddress>/.
2. In **username**, type the user name.
3. In **password**, type the password.
4. Press **Enter**.

   The system displays the Home page.

Transferring the files by using the WinSCP utility

About this task

Use the following procedure to transfer the files from a remote system to a Nutanix container by using the WinSCP utility.

Procedure

1. Use WinSCP or a similar file transfer utility to connect to the Nutanix container.
2. In **File protocol**, click **SCP**.
3. Enter the credentials to gain access to SCP.
4. Click **Login**.
5. Click **OK** or **Continue** as necessary in the warning dialog boxes.
6. In the WinSCP destination machine pane, browse to `/home/<Container_Name>` as the destination location for the file transfer.
7. Click and drag the `qcow2` image from the WinSCP source window to `/home/<Container_Name>` in the WinSCP destination window.

8. Click the WinSCP **Copy** button to transfer the file.
9. When the copy completes, close the WinSCP window (**x** icon) and click **OK**.

Uploading the qcow2 image

Procedure

1. Log on to the Nutanix Web console.
2. Click **Settings icon ( )** > **Image Configuration**.

   The system displays the Image Configuration dialog box.
3. Click **+ Upload Image**.

   The system displays the Create Image dialog box.
4. In **NAME**, type the name of the image.
5. In **ANNOTATION**, type the description of the image.
6. In **IMAGE TYPE**, click **DISK**.
7. In **STORAGE CONTAINER**, click the storage container of the image.
8. In **IMAGE SOURCE**, perform one of the following:
   - Select **From URL**, type the exact URL of the qcow2 image. For example: `nfs://<127.0.0.1>/<Storage Container Name>/<Image Name>`
   - Select **Upload a file**, click **Browse**. In the Choose File to Upload dialog box, select the qcow2 image from your local system, and click **Open**.
9. Click **Save**.

   The system displays the created image on Image Configuration.

Creating the virtual machine by using Nutanix

Before you begin

- Upload the `qcow2` image.
- Configure the network.

Procedure

1. Log on to the Nutanix Web console.
2. Click **Home** > **VM**.
3. Click **+ Create VM**.

   The system displays the Create VM dialog box.
4. In the General Configuration section, perform the following:
   a. In **NAME**, type the name of the virtual machine.

b. In **DESCRIPTION**, type the description of the virtual machine.

5. In the Compute Details section, perform the following:
   a. In **VCPU(S)**, type the number of virtual CPUs required for the virtual machine.
   b. In **NUMBER OF CORES PER VCPU**, type the number of core virtual CPUs required for the virtual machine.
   c. In **Memory**, type the memory required for the virtual machine.

      The value must be in GiB.

   You must select the CPU and Memory according to the application footprint profile.
6. In the Disk section, perform the following:
   a. Click **+ Add New Disk**.

      The system displays the Add Disk dialog box.
   b. In **TYPE**, click **DISK**.
   c. In **OPERATION**, click **Clone from Image Service**.
   d. In **IMAGE**, click the application image.
   e. In **BUS TYPE**, click **IDE**.
   f. Click **Add**.

      The system displays the added disk in the **Disk** section.
7. In the Disk section, select a boot device.
8. In the Network Adopters (NIC) section, perform the following:
   a. Click **Add New NIC**.

      The system displays the Create NIC dialog box.
   b. In **VLAN NAME**, click the appropriate NIC.

      The system displays **VLAN ID**, **VLAN UUID**, and **NETWORK ADDRESS / PREFIX** for the selected NIC.
   c. Click **Add**.

      The system displays the added NIC in the Network Adopters (NIC) section.

   You must select the number of NIC according to the application footprint profile.

   If you are configuring Out of Band Management, select one more NIC.
9. In the VM Host Affinity section, perform the following:
   a. Click **Set Affinity**.

      The system displays the Set VM Host Affinity dialog box.
   b. Select one or more host to deploy the virtual machine.
   c. Click **Save**.

The system displays the added hosts in the VM Host Affinity section.

10. Click **Save**.

    The system displays the message: `Received operation to create VM <name of the VM>`.

    After the operation is successful, the system displays the created virtual machine on the VM page.

Next steps

Start the virtual machine.

Starting a virtual machine

Before you begin

Create the virtual machine.

Procedure

1. Click **Home** > **VM**.
2. On the VM page, click **Table**.
3. Select the virtual machine.
4. At the bottom of the table, click **Power On**.

   The system starts the virtual machine.

Next steps

Launch the console. On the first boot of the virtual machine, provide the configuration and networking parameters.

Configuring the virtual machine

Procedure

1. Click **Home** > **VM**.
2. On the VM page, click **Table**.
3. Select the virtual machine.
4. At the bottom of the table, click **Launch Console**.
5. Follow the prompt to configure the virtual machine.

Deploying application by using Red Hat Virtualization Manager

Logging on to the Red Hat Virtualization Manager Web console

Procedure

1. In your web browser, type the Red Hat Virtualization Manager URL.

   For example, https://<RedHatVirtualizationManager_IPAddress>/ovirt-engine/.

2. To log in, click **Not Logged In** > **Login**.

   The system displays the Red Hat Virtualization Manager Log In page.

3. In **Username**, type the user name.
4. In **Password**, type the password.
5. In **Profile**, click the appropriate profile.
6. Click **Log In**.

   The system displays the Red Hat Virtualization Manager Web Administration page.

Uploading the disk

Before you begin

You must import the `ovirt-engine` certificate into your browser by accessing the `http://<engine_url>/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA` link to get the certificate. Establish the trust for the new Certificate Authority (CA) with the website.

Procedure

1. Log on to the Red Hat Virtualization Manager Web console.
2. In the left navigation pane, click **System**.
3. On the **Disks** tab, click **Upload** > **Start**.

   The system displays the Upload Image dialog box.

4. Click **Browse**.
5. In the Choose File to Upload dialog box, select the qcow2 disk image from your local system, and click **Open**.
6. In **Size(GB)**, type the size of the disk.
7. In **Alias**, type the name of the disk.
8. In **Description**, type the description of the disk.
9. In **Data Center**, click the data center to store the disk.

10. In **Storage Domain**, click the storage domain of the disk.
11. In **Disk Profile**, click disk profile.
12. In **Use Host**, click the host of the disk.
13. Click **OK**.

    The system displays the uploaded image on the **Disks** tab. Once the disk image is successfully uploaded, the **Status** column displays `OK`.

Creating the virtual machine by using Red Hat Virtualization Manager

Before you begin

- Upload the `qcow2` disk image.
- Create an instance type.
- Configure the network.

Procedure

1. Log on to the Red Hat Virtualization Manager Web console.
2. In the left navigation pane, click **System**.
3. On the **Virtual Machines** tab, click **New VM**.

   The system displays the New Virtual Machine dialog box.
4. In **Operating System**, click **Linux**.
5. In **Instance Type**, click an instance type.

   You must select the instance type according to the application footprint profile.
6. In **Optimized for**, click **Server**.
7. In **Name**, type the name of the virtual machine.
8. In **Description**, type the description of the virtual machine.
9. In the Instance Images section, perform the following:
   a. Click **Attach**.

      The system displays the Attach Virtual Disks dialog box.
   b. In **Interface**, click **IDE**.
   c. Click **OK**.

      The system displays the added disk in the Instance Images section.
10. In **nic1**, click a vNIC profile.

    If you are configuring Out of Band Management, select one more NIC.
11. Click **OK**.

After the operation is successful, the system displays the created virtual machine on the **Virtual Machines** tab.

Next steps

Start the virtual machine.

Starting a virtual machine

Before you begin

Create the virtual machine.

Procedure

Right-click the virtual machine and click **Run**.

When the system starts the virtual machine, the system displays a green upward arrow key (▲) corresponding to the virtual machine name.

Next steps

Launch the console. On the first boot of the virtual machine, provide the configuration and networking parameters

Configuring the virtual machine

Before you begin

- Start the virtual machine.
- Install the `virt-viewer` installer to access console.

Procedure

1. Right-click the virtual machine and click **Console**.
2. Follow the prompt to configure the virtual machine.

Installing the System Manager patch from CLI

About this task

From System Manager Release 7.1 and later, you must install the patch after the ova deployment is complete.

Before you begin

Download the latest System Manager patch file and save the patch file to the `/swlibrary` location of System Manager.

Procedure

1. Log in to the System Manager command line interface.

2. Run the command: **SMGRPatchdeploy** /swlibrary/<System_Manager_R8.1.x.x_xxxxxxxxx.bin>.

Next steps

Note:

Modifying the network or management configuration is not recommended before the patch deployment.

Log on to the System Manager web console. At your first log in, change the System Manager web console credentials.

Click **About** and check the software version.

Chapter 6: Managing the ESXi host by using SDM

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** > **Application Management**.
2. On the **Locations** 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 **Application Management Tree** section.

Adding an Appliance Virtualization Platform or 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.

If you are adding a standalone ESXi host to System Manager Solution Deployment Manager or to the Solution Deployment Manager client, add the standalone ESXi host using its FQDN only.

Note:

You can add a VMware ESXi host in Solution Deployment Manager only if Standard or Enterprise VMware license is applied on the VMware ESXi host.

If VMware vSphere Hypervisor Free License is applied on the VMware ESXi host or VMware ESXi host is in evaluation period, you cannot add that VMware ESXi host in Solution Deployment Manager.

Solution Deployment Manager only supports the Avaya Aura® Appliance Virtualization Platform and VMware ESXi hosts. If you try to add another host, the system displays the following error message:

```
Retrieving host certificate info is failed: Unable to communicate with
host. Connection timed out: connect. Solution Deployment Manager only
supports host management of VMware-based hosts and Avaya Appliance
Virtualization Platform (AVP).
```

Before you begin

Add a location.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click **Application Management**.
3. In **Application Management Tree**, select a location.
4. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
5. In the New Platform section, do the following:
   a. Provide details of Platform name, Platform FQDN or IP address, user name, and password.

      For Appliance Virtualization Platform and VMware ESXi deployment, you can also provide the root user name.

   b. In **Platform Type**, select **AVP/ESXi**.

   c. If you are connected through the services port, set the Platform IP address of Appliance Virtualization Platform to 192.168.13.6.
6. Click **Save**.
7. In 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, Solution Deployment Manager displays the error. To generate certificate, see VMware documentation.

   In the Application Management Tree section, the system displays the new host in the specified location. The system also discovers applications.

8. To view the discovered application details, such as name and version, establish trust between the application and System Manager doing the following:
   a. On the **Applications** tab, in the Applications for Selected Location <location name> section, select the required application.
   b. Click **More Actions** > **Re-establish connection**.

      For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
   c. Click **More Actions** > **Refresh App**.

   Important:

   When you change the IP address or FQDN of the Appliance Virtualization Platform host from the local inventory, you require AVP Utilities. To get the AVP Utilities application name during the IP address or FQDN change, refresh AVP Utilities to ensure that AVP Utilities is available.
9. On the **Platforms** tab, select the required platform and click **Refresh**.

Next steps

After adding a new host under Application Management Tree, the **Refresh Platform** operation might fail to add the virtual machine entry under **Manage Element** > **Inventory**. This is due to the absence of **Application Name** and **Application Version** for the virtual machines discovered as part of the host addition. After adding the host, do the following:

1. In Application Management Tree, establish trust for all the virtual machines that are deployed on the host.
2. Ensure that the system populates the **Application Name** and **Application Version** for each virtual machine.

Adding a software-only platform

About this task

Use this procedure to add an operating system on Solution Deployment Manager. In Release 8.1.3, the system supports the Red Hat Enterprise Linux Release 7.6 64-bit operating system.

Before you begin

Add a location.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Platforms** tab, click **Add**.
3. In **Platform Name**, type the name of the platform.

4. In **Platform FQDN or IP**, type the FQDN or IP address of the base operating system.
5. In **User Name**, type the user name of the base operating system.

   For a software-only deployment, the user name must be a direct access admin user. If the software-only application is already deployed, provide the application cli user credentials.
6. In **Password**, type the password of the base operating system.
7. In **Platform Type**, select **OS**.
8. Click **Save**.

   If the platform has some applications running, the system automatically discovers those applications and displays the applications in the **Applications** tab.

   - If Solution Deployment Manager is unable to establish trust, the system displays the application as Unknown.
   - If you are adding OS, only **Add** and **Remove** operations are available on the **Platforms** tab. You cannot perform any other operations. On the **Applications** tab, the system enables the **New** option. If the application is System Manager, the system enables **Update App** on Solution Deployment Manager Client

   The system displays the added base operating system on the **Platforms** tab.

Managing vCenter

Creating a role for a user

About this task

To manage a vCenter or ESXi in Solution Deployment Manager, you must provide complete administrative-level privileges to the user.

Use the following procedure to create a role with administrative-level privileges for the user.

Procedure

1. Log in to vCenter Server.
2. On the Home page, click **Administration** > **Roles**.

   The system displays the Create Role dialog box.
3. In **Role name**, type a role name for the user.
4. To provide complete administrative-level privileges, select the **All Privileges** check box.
5. **(Optional)** To provide minimum mandatory privileges, do the following.
   a. In All Privileges, select the following check boxes:
      - **Datastore**

- **Datastore cluster**
- **Distributed switch**
- **Folder**
- **Host profile**
- **Network**
- **Resource**
- **Tasks**
- **Virtual machine**
- **vApp**

Note:

You must select all the subprivileges under the list of main set of privileges. For example, when you select the **Distributed switch** check box, ensure that you select all the related subprivileges. This is applicable for all the main privileges mentioned above. If you do not select all the subprivileges, the system might not work properly.

b. In All Privileges, expand **Host**, and select the **Configuration** check box.

Note:

You must select all the subprivileges under **Configuration**.

6. Click **OK** to save the privileges.

Next steps

Assign this role to the user for mapping vCenter in Solution Deployment Manager. To assign the role to the user, see the VMware documentation.

Adding a vCenter to Solution Deployment Manager

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 6.0, 6.5, 6.7, and 7.0. 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** > **Application 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:
   a. In **vCenter FQDN**, type FQDN of vCenter.
      - 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.
      - The FQDN value must match with the value of the **SAN** field of the vCenter certificate. The FQDN value is case sensitive.

   b. In **User Name**, type the user name to log in to vCenter.
   c. In **Password**, type the password to log in to vCenter.
   d. In **Authentication Type**, select **SSO** or **LOCAL** as the authentication type.

      If you select the authentication type as **SSO**, the system displays the **Is SSO managed by Platform Service Controller (PSC)** field.

   e. **(Optional)** If PSC is configured to facilitate the SSO service, select **Is SSO managed by Platform Service Controller (PSC)**.

      PSC must have a valid certificate.

      The system enables **PSC IP or FQDN** and you must provide the IP or FQDN of PSC.

   f. **(Optional)** In **PSC IP or FQDN**, type the IP or FQDN of PSC.
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 56
Map vCenter field descriptions on page 57
New vCenter and Edit vCenter field descriptions on page 58

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** > **Application 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 an earlier release, on the Certificate page, click **Save**, and then click **Accept Certificate**.
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, click **Bulk Update** > **Update**.
7. Click **Commit** to get an updated list of managed and unmanaged hosts.

   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.

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** > **Application 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.

Table continues…

Name	Description
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 options 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 a certificate for vCenter. For vCenter, you can only accept a certificate. You cannot generate a 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 vCenter and Edit vCenter field descriptions

Name	Description
vCenter FQDN	The 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 If you select the authentication type as **SSO**, the system displays the **Is SSO managed by Platform Service Controller (PSC)** field.

Table continues…

Name	Description
Is SSO managed by Platform Service Controller (PSC)	The check box to specify if PSC manages SSO service. When you select the check box, the system enables **PSC IP or FQDN**.
PSC IP or FQDN	The IP or FQDN of PSC.

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.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

Button	Description
Edit	The option to edit the location and host.
Bulk Update	Provides an option to change the location of more than one ESXi hosts. **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	Displays the versions of the ESXi host linked to **vCenter FQDN**. **Note:** For Release 8.1 and later, do not select the 5.0 and 5.1 versions.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

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

Chapter 7: Configuration

Configuring Out of Band Management on System Manager

About this task

If you do not configure Out of Band Management during the deployment of System Manager OVA from Solution Deployment Manager on an Avaya-provided server, you can use the **configureOOBM** command to configure Out of Band Management anytime after the deployment.

Before you begin

- Enable Out of Band Management on Appliance Virtualization Platform.
- Install System Manager on the Appliance Virtualization Platform host on which Out of Band Management is installed.
- Ensure that IP address or hostname of Public network and Management network are different.

  If both are in the same network, Out of Band Management configuration might not function as expected.
- Log in to System Manager by using an SSH client utility.

  When you enable Out of Band Management configuration, you might lose the connection as the system does a network restart. You can login to System Manager from the Console of VMware vSphere Web Client. that is configured to connect to the Appliance Virtualization Platform host server.

Procedure

1. To enable Out of Band Management, type `configureOOBM -EnableOOBM`.

   The system enables Out of Band Management on the System Manager virtual machine. With **EnableOOBM**, the system configures the additional Ethernet interface, updates network configuration, and sets the firewall rules.
2. To disable Out of Band Management, type `configureOOBM -DisableOOBM`.

   The system disables Out of Band Management on the System Manager virtual machine. With **DisableOOBM**, the system disables the additional Ethernet interface that you configured earlier and sets the firewall rules to default.

Configuring Out of Band Management on System Manager in the Geographic Redundancy setup

About this task

Note:

You cannot enable Out of Band Management on secondary System Manager server when Out of Band Management on primary System Manager server is disabled.

Before you begin

Identify one of the following:

- Enable Out of Band Management on both the primary and secondary System Manager server.
- Enable Out of Band Management on the primary System Manager server and not enable Out of Band Management on the secondary System Manager server.
- Disable Out of Band Management on secondary System Manager server.
- Disable Out of Band Management on both the primary and secondary System Manager server.

Procedure

1. To enable Out of Band Management on both primary and secondary System Manager server, perform the following:
   a. Disable Geographic Redundancy replication on primary System Manager server.
   b. Convert primary System Manager server to standalone System Manager server and activate the secondary System Manager server.
   c. Enable Out of Band Management on both primary and secondary System Manager server.
   d. Reconfigure the Geographic Redundancy on the secondary System Manager server.
   e. Enable Geographic Redundancy replication on primary System Manager server.
2. To enable Out of Band Management on the primary System Manager server and not enable Out of Band Management on secondary System Manager server, perform the following:
   a. Disable Geographic Redundancy replication on primary System Manager server.
   b. Convert primary System Manager server to standalone System Manager server.
   c. Enable Out of Band Management on primary System Manager server.
   d. Once Out of Band Management on primary System Manager server is enabled, reconfigure Geographic Redundancy on secondary System Manager server.
   e. Enable Geographic Redundancy replication on primary System Manager server.

3. To disable Out of Band Management on secondary server, perform the following:
    a. Disable Geographic Redundancy replication on primary System Manager server.
    b. Convert primary System Manager server to standalone System Manager server.
    c. Activate secondary System Manager server and disable Out of Band Management.
    d. Reconfigure primary System Manager server from the web console of the secondary System Manager server.
    e. Enable Geographic Redundancy replication on primary System Manager server.
4. To disable Out of Band Management on both servers, perform the following:
    a. Disable Geographic Redundancy replication on primary System Manager server.
    b. Convert primary System Manager server to standalone System Manager server and disable Out of Band Management.
    c. Activate secondary System Manager server and disable Out of Band Management.
    d. Reconfigure Geographic Redundancy on secondary System Manager server with old primary System Manager server which is now standalone.
    e. Enable Geographic Redundancy replication on primary System Manager server.

Enabling Multi Tenancy on Out of Band Management-enabled System Manager

About this task

By default, the Multi Tenancy feature is disabled on System Manager when Out of Band Management is enabled. You must enable Multi Tenancy on Out of Band Management-enabled System Manager for the Tenant Management administrator to manage tenant users.

Before you begin

Start an SSH session.

Procedure

1. Log in to System Manager by using the command line utility.
2. Type `opt/vsp/OOBM/ enableMultitenancyInPublicInterface.sh`.

Configuring Out of Band Management using the configureOOBM command

After the deployment of System Manager, use **`configureOOBM`** to configure Out of Band Management. You can enable or disable Out of Band Management.

Syntax

```
configureOOBM [-EnableOOBM|-DisableOOBM]
```

Option	Description
EnableOOBM	Enables Out of Band Management on System Manager virtual machine. With **EnableOOBM**, the additional Ethernet interface is configured, network configuration is updated, and firewall rules are set.
DisableOOBM	Disables Out of Band Management on System Manager virtual machine. With **DisableOOBM**, the system disables the additional Ethernet interface that you configured earlier and sets the firewall rules to default.

Configuring the virtual machine automatic startup settings on VMware

About this task

When a vSphere ESXi host restarts after a power failure, the virtual machines that are deployed on the host do not start automatically. You must configure the virtual machines to start automatically.

In high availability (HA) clusters, the VMware HA software does not use the startup selections.

Before you begin

Verify with the ESXi system administrator that you have the permissions to configure the automatic startup settings.

Procedure

1. In the web browser, type the vSphere vCenter host URL.
2. Click one of the following icons: **Hosts and Clusters** or **VMs and Templates** icon.
3. In the navigation pane, click the host where the virtual machine is located.
4. Click **Manage**.
5. In Virtual Machines, click **VM Startup/Shutdown**, and then click **Edit**.

   The software displays the Edit VM Startup and Shutdown window.
6. Click **Automatically start and stop the virtual machines with the system**.
7. Click **OK**.

SAL Gateway

You require a Secure Access Link (SAL) Gateway for remote access and alarming.

Through SAL, support personnel or tools can gain remote access to managed devices to troubleshoot and debug problems.

A SAL Gateway:

1. Receives alarms from Avaya products in the customer network.
2. Reformats the alarms.
3. Forwards the alarms to the Avaya support center or a customer-managed Network Management System.

For more information about SAL Gateway and its deployment, see the Secure Access Link documentation on the Avaya Support website at http://support.avaya.com.

Configuring hardware resources to support VE footprint flexibility

Virtualized Environment footprint flexibility

Virtualized applications provide a fixed profile based on maximum capacity requirements. However, many customers require only a fraction of the maximum capacity.

Certain virtualized applications offer a flexible footprint profile based on the number of users that are supported. The customer can configure VMware CPU and RAM of a virtual machine according to a particular capacity line size requirement.

The applications that currently support Virtualized Environment footprint flexibility are:

- Avaya Aura® System Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® Application Enablement Services

Related links

Capability and scalability specification on page 66

Reconfiguring hardware resources for flexible footprint

About this task

Reconfigure the CPU and RAM resources for the System Manager virtual machine.

Procedure

1. Connect to the host or cluster by using the VMware vSphere Web client.
2. Log in by using the admin login name and password.
3. To power off the virtual machine, perform the following:
   a. Right-click on the virtual machine name.
   b. Select **Power** > **Shut Down Guest**.
   c. Click **Yes** in the Shutdown Confirmation dialog box.
4. On the virtual machine name, right-click and select **Edit Settings**.
5. Click the Hardware tab.
6. Click **Memory** and change the **Memory Size** to the appropriate limit.

   For more information, see System Manager Virtualized Environment footprint hardware resource matrix.
7. Click on the Resources tab.
8. Select **Memory** and verify the **Reservation** is set correctly.
9. Clear the **unlimited** check box and verify the **Limit** slide is set to the same value as the **Reservation**.
10. Click the Hardware tab.
11. Select **CPUs** and change the **Number of sockets** according to the limit requirement.

    For more information, see System Manager Virtualized Environment footprint hardware resource matrix.
12. Click the Resources tab.
13. Select **CPUs** and verify that the **Reservation** is set correctly.
14. Clear the **unlimited** check box and verify that the **Limit** slide is set to the same value as the **Reservation** field.
15. Click **OK** and wait until the virtual machine completes the reconfiguration process.
16. Power on the virtual machine.

Related links

Capability and scalability specification on page 66

Capability and scalability specification

The table provides the maximum capacities supported for each element type.

Note:

Only one System Manager is available with each Avaya Aura® deployment. Therefore, the solution number is not the sum of all supported elements listed in the table.

Capacity	Maximum limit	Notes
Administrator logins	250	
Simultaneous logins	50	
Total administered endpoints of all types	250,000	To see the total number of endpoints, go to the **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints** page on the System Manager web console.
Total administered users defined in the System Manager database	250,000	The total number of administered users with an Identity is configured in System Manager and might not have a communication profile defined. To see the defined users, go to the **Users** > **User Management** > **Manage Users** page on the System Manager web console.
Messaging mailboxes	250,000	
Contacts per user	250	
Public contacts	1000	
Personal contact lists per user	1	
Members in a personal contact list	250	
Groups	300	
Members in a group	400	
Elements	25,000	
Communication Manager or CS 1000 or both	500	Specifies the capacity counts against the total number of elements.
Session Managers	28	
Branch Session Manager	5,000	
SIP Users	300,000	Total number of SIP users.
Total SIP devices	1,000,000	Total number of SIP devices.
IP Office	3500	To support central licensing of 3500 IP Office 9.x and later, local WebLM licensing servers that are slaved to System Manager licensing are required. For more information, see the IP Office 9.x and later product offer.
IP Office Unified Communication Module or Application servers as part of Branch deployments	3500	
Roles	200	
Roles per user	20	
Licensing clients	1000	
Concurrent License requests per WebLM	300	

Table continues…

Capacity	Maximum limit	Notes
License requests during any 9 minute window per WebLM	50,000	
Local WebLM	22	
Trust management clients	2500	
Tenants (System Manager Multi Tenant)	250	

Geographic Redundancy configuration

Prerequisites for the Geographic Redundancy setup

In a Geographic Redundancy setup, the two standalone System Manager servers that you designate as primary and secondary servers must meet the following requirements:

- Contain the same version of the software that includes software packs.
- Contain the same profile for primary and secondary System Manager Geographic Redundancy virtual machines. For example, if the primary System Manager contains Profile 2, the secondary System Manager must also contain Profile 2.
- Contain the same version of the System Manager software that includes service pack and software patches.
- Contain the same parent domain names for two System Manager systems. For example, smgr.abc.com and smgr.xyz.com are invalid domain names because the parent domain names abc and xyz are different.
- Communicate with each other over the network by using the IP address and FQDN.
- In the Geographic Redundancy setup, the primary and secondary System Manager must use the same VFQDN.
- Have a synchronized network time.
- Use DNS to ensure that the name resolution is automatic. Otherwise, you must resolve the IP address and the host name in the `/etc/hosts` file on the primary and secondary System Manager servers.
- Have open required ports to support the Geographic Redundancy feature. For port usage information, see *Avaya Port Matrix: Avaya Aura® System Manager* on the Avaya Support website at http://support.avaya.com/.
- Have T1 as the minimum data pipe between the primary and the secondary System Manager server. T1 provides 1.544 Mbps.
- Have network latency that is less than 500 ms.

- In the Geographic Redundancy setup, if you need to configure the outbound firewall rules, then you need to add the peer IP addresses on the primary and secondary System Manager servers.

Prerequisites for System Manager on VMware in the Geographic Redundancy setup

In a Geographic Redundancy-enabled system running on VMware, ensure that System Manager that you designate as primary and secondary systems meet the following requirements:

- Contain the same profile for primary and secondary System Manager Geographic Redundancy virtual machines. For example, if the primary System Manager contains Profile 2, the secondary System Manager must also contain Profile 2.
- Contain the same version of the System Manager software that includes service pack and software patches.
- Contain the same parent domain names for two System Manager systems. For example, smgr.abc.com and smgr.xyz.com are invalid domain names because the parent domain names abc and xyz are different.
- Communicate with each other over the network by using the IP address and FQDN.
- Have a synchronized network time.
- Use DNS to ensure that the name resolution is automatic. Otherwise, you must resolve the IP address and the host name in the `/etc/hosts` file on the primary and secondary System Manager servers.
- Have open required ports to support the Geographic Redundancy feature. For port usage information, see *Avaya Port Matrix: Avaya Aura® System Manager* on the Avaya Support website at http://support.avaya.com/.
- Have network latency that is less than 500 ms.
- Have T1 as the minimum data pipe between the primary and the secondary System Manager server. T1 provides 1.544 Mbps.

Key tasks for Geographic Redundancy

Prerequisites

Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.

Key tasks

Only the system administrator can perform Geographic Redundancy-related operations.

- Configure Geographic Redundancy.

  Configure Geographic Redundancy to handle the situation when the primary System Manager server fails or when the managed element loses connectivity to the primary System Manager server.

Important:

During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

- Enable the Geographic Redundancy replication between the two servers.

  Enable the replication in the following scenarios:

  - After you configure the two standalone System Manager servers for Geographic Redundancy, you must enable the Geographic Redundancy replication between the two servers to ensure that the secondary System Manager server contains the latest copy of the data from the primary System Manager server.
  - During the system maintenance or upgrades, Geographic Redundancy replication must be disabled. After maintenance activity is complete, you must enable Geographic Redundancy replication if it was manually or automatically disabled due to the maintenance activity.

    Note:

    If the heartbeat between the two System Manager servers in which the Geographic Redundancy replication is enabled stops due to network connectivity failure or the server failure, the system automatically disables the Geographic Redundancy replication within a preconfigured time. The default is 5 minutes. If the primary and secondary System Manager servers are running and if the network connectivity between the two servers fails, the system triggers auto-disable on both servers. If one of the two servers becomes nonoperational, the system triggers auto-disable on the server that is operational.

  - After the primary System Manager server recovers from failure.

  Important:

  During the bulk activities such as import, export, and full synchronization of Communication Manager, the system might disable the Geographic Redundancy replication for reasons, such as the size of the data involved in the bulk activity and the bandwidth between the primary and the secondary System Manager server. After you complete the bulk activity, enable the Geographic Redundancy replication if the replication is disabled.

- Disable the Geographic Redundancy replication between the two servers.

  Disable the Geographic Redundancy replication before you start the maintenance activities such as upgrades, installation of software patches or hot fixes. If the primary and the secondary System Manager servers disconnect from each other for more than the threshold period, the system automatically disables the Geographic Redundancy replication. The default threshold period is 5 minutes.

- Activate the secondary System Manager server.

  Activate the secondary System Manager server in the following scenarios:

  - The primary System Manager becomes nonoperational.
  - The enterprise network splits.

- Deactivate the secondary System Manager server.

  Deactivate the secondary System Manager server in the following situations:

  - The primary System Manager server becomes available.
  - The element network restores from the split.

- Restore the primary System Manager server.

  After you activate the secondary System Manager server, to return to the active-standby mode, you must restore the primary System Manager server. You can choose to restore from the primary System Manager or the secondary System Manager server.

  Note:

  The system does not merge the data from the primary and secondary server.

- Reconfigure Geographic Redundancy.

  You can reconfigure Geographic Redundancy when the secondary System Manager is in the standby mode or active mode. The reconfiguration process copies the data from the primary System Manager server to the secondary System Manager server.

- Convert the primary System Manager server to the standalone server.

  Perform this procedure to convert the primary System Manager server in the Geographic Redundancy-enabled system to a standalone server or if you have to configure a new secondary server.

For detailed instructions to complete each task, see the appropriate section in this document.

Prerequisites before configuring Geographic Redundancy

Geographic Redundancy prerequisites overview

Before enabling and configuring Geographic Redundancy, do the following:

1. Configure CRL download on the secondary System Manager server.

   Note:

   By default, CRL is valid only for 7 days. Therefore, you must configure Geographic Redundancy before the expiry date of CRL.

2. Add the trusted certificate of primary server to the secondary System Manager server.
3. If certificate is replaced on Primary Server by third-party signed certificate then same certificate type must be replaced on Secondary Server by same third-party CA.

   For example: If *Management Container TLS Service* is replaced by third-party CA signed certificate on Primary Server then same type certificate must be replaced on Secondary Server by same third-party CA.

4. Install third-party certificate on both servers prior to Geographic Redundancy configuration and post Geographic Redundancy configuration.

   For more information, see “Managing certificates”.

5. Ensure that third-party CA certificate is added into trust store of both System Manager.
6. Replaced certificate must have full chain (id certificate ->inter CA (if present) certificate -> root CA certificate) and also must contain correct FQDN/VFQDN in required places.
7. Configure CRL download is mandatory for Geographic Redundancy.
8. If CRL URL for third-party is not accessible from System Manager, then set **Certificate Revocation Validation** from **BEST_EFFORT** to **NONE** on the **Security** > **Configuration** > **Security Configuration** > **Revocation Configuration** page.

   JBoss service automatically restarts after 10 minutes.

Related links

Configuring CRL download on the secondary System Manager server on page 73
Adding the trusted certificate of primary server to the secondary System Manager server on page 74

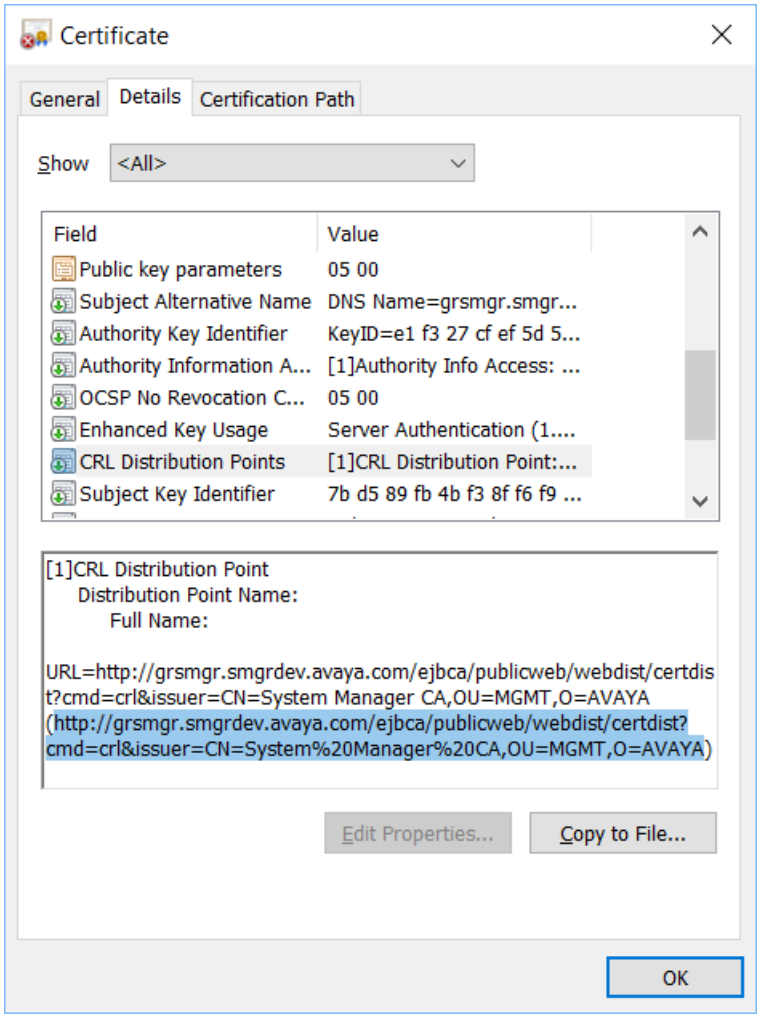
Copying the CRL URL

Procedure

1. On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, the System Manager URL.
2. On the address bar, click the Lock icon.
3. Click **View certificates**.
4. On the Certificate dialog box, do the following:
   a. Click on the **Details** tab.
   b. Scroll down and click the **CRL Distribution Points** field.

      The system displays the CRL URL in the text box.

      For example: http://<vFQDN>/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA



c. Press **Ctrl+C** and copy the URL in Notepad for configuring CRL download in the Geographic Redundancy set up.

d. Click **OK**.

Configuring CRL download on the secondary System Manager server

Procedure

1. Access the login page of the primary System Manager server.
2. Copy the CRL of the browser certificate.

   For information about copying the CRL URL, see “Copying the CRL URL.”
3. Replace the vFQDN in the CRL with the IP address of the primary System Manager server.

   For example, the CRL in the certificate is:

```
http://<vFQDN>/ejbca/publicweb/webdist/certdist?
cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
```

The new CRL for the certificate will be:

```
http://<ip-address>/ejbca/publicweb/webdist/certdist?
cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
```

Where, *<vFQDN>* and *<ip-address>* are the respective vFQDN and IP address.

Note:

If you installed a third-party certificate on System Manager servers, this step is not required. If third-party certificate, then configure CRL URL of the third-party certificate for CRL download.

4. Log on to the secondary System Manager web console.
5. On the System Manager web console, click **Services** > **Security**.
6. In the navigation pane, click **Configuration** > **CRL Download**.
7. On the CRL Download Configuration page, click **Add**.

   The system displays the Schedule CRL Download page.
8. In **Job Name**, type the job name.
9. In **Job Frequency**, set the frequency and recurrence to schedule the job within a few minutes after the CRL addition.

   For more information, see Schedule CRL Download field descriptions.
10. Copy the new CRL URL from Notepad and paste the URL in the **Configure CRL Distribution Point** field.

    For information about copying the CRL URL, see “Copying the CRL URL.”

    CRL URL example:

    ```
    http://<ip-address>/ejbca/publicweb/webdist/certdist?
    cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
    ```
11. Click **Add**, and then click **Commit**.

    Ensure that the job is completed successfully.

Next steps

Add the trusted certificate of primary server to the secondary System Manager server.

Adding the trusted certificate of primary server to the secondary System Manager server

Procedure

1. Log in to the primary System Manager web console.
2. On the System Manager web console, click **Services** > **Security**.
3. In the navigation pane, click **Certificates** > **Authority**.
4. Click **CA Functions** > **CA Structure & CRLs**.

5. Click **Download PEM file**.
6. Log in to the secondary System Manager web console.
7. On the System Manager web console, click **Services** > **Inventory**.
8. In the navigation pane, click **Manage Elements**.
9. On the Manage Elements page, select the System Manager certificate and click **More Actions** > **Manage Trusted Certificates**.
10. On the Manage Trusted Certificates page, click **Add**.
11. Click **Choose File** and select the previously downloaded PEM file.
12. Click **Retrieve Certificate**, and then click **Commit**.

Configuring Geographic Redundancy

Before you begin

- For the new installation of System Manager, ensure that you change the default password for the system administrator user.
- Ensure that you change CLI passwords on primary and secondary System Manager servers.

  60 days after the System Manager CLI password expires, Geographic Redundancy becomes nonoperational. You must set a new password on primary and secondary System Manager servers for Geographic Redundancy to become operational again.
- Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.

About this task

For resiliency, from the pair of standalone System Manager servers, you can configure Geographic Redundancy.

Important:

- During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.
- After the Geographic Redundancy configuration is complete, the credentials used for logging in to the secondary System Manager becomes identical to the login credentials of the primary System Manager.

Procedure

1. Log on to the System Manager web console of the standalone server that you require to designate as the secondary server and perform the following:
   a. On the System Manager web console, click **Services** > **Geographic Redundancy**.
   b. Click **Configure**.

c. In the dialog box, provide the details of the primary System Manager server in the following fields:

- **Primary Server Username**

  Enter the system administrator user name that you use to log on to the primary System Manager server.

- **Primary Server Password**

  Enter the system administrator password that you use to log on to the primary System Manager server.

- **Primary Server IP**
- **Primary Server FQDN**

d. Click **OK**.

The configuration process takes about 30 minutes. However, the duration might vary depending on the size of the data on the primary System Manager server.

Note:

Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

The server that you configured becomes the secondary server and the other standalone server becomes the primary System Manager server.

2. To view the status of the Geographic Redundancy configuration during the restart of the two application servers, perform one of the following:

- Log on to the web console of the primary System Manager server and perform the following:

  a. On the System Manager web console, click **Services** > **Geographic Redundancy**.

  b. Refresh the GR Health page.

  If **Enable** is available, the configuration is complete.

  Note:

  Log off and log on to the primary System Manager server to view the updated status of Geographic Redundancy health.

- Log in to the secondary System Manager server as system administrator by using the command line interface and perform the following:

  a. Type `tail -f /home/ucmdeploy/quantum/autoReconfig.log`.

  The system displays the progress during the restart of the two application servers. When the second application server restart completes, the system displays the following messages:

  ```
  SMGR :: operationStatus=success
  ```

```
                SMGR  ::  Quantum has been successfully
        configured as a secondary.
```

Next steps

On the web console of the primary System Manager server, enable the Geographic Redundancy replication.

Related links

Converting the primary System Manager server to the standalone server on page 82
Prerequisites for System Manager on VMware in the Geographic Redundancy setup on page 69

Enabling the Geographic Redundancy replication

Enable the Geographic Redundancy replication between the two servers to ensure that the data gets continuously replicated between the primary and secondary System Manager servers.

Before you begin

- Log on to the System Manager web console of the primary server.
- Ensure that CLI passwords on primary and secondary System Manager servers do not expire.

  60 days after the System Manager CLI password expires, Geographic Redundancy becomes nonoperational. You must set a new password on primary and secondary System Manager servers for Geographic Redundancy to become operational again.

About this task

Important:

During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Enable Replication**.

   The system displays the progress information in the **Enable GR Status** section.

   Note:

   Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

   If the enabling process is successful, the system displays the Geographic Redundancy replication status as `Enabled`. If the process fails, the system displays an error message with the replication status as `Failed` on the primary the System Manager web console. The primary server remains in the failed state while the secondary server rolls back to the previous state. Verify if the system has raised an alarm for a temporary network

connectivity failure. Retry when the network connectivity is restored. If the problem persists, contact Avaya service personnel.

Related links

Disabling the Geographic Redundancy replication on page 78
Geographic Redundancy field descriptions on page 83

Disabling the Geographic Redundancy replication

Before you begin

Log on to the System Manager web console of the primary server.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Disable Replication**.
3. In the dialog box, click **Yes**.

   The system displays the progress information in the **Disable GR Status** section.

   If the disabling process is successful, the system displays the Geographic Redundancy replication status as `Disabled`. The system stops replicating the data from the primary and secondary System Manager server. If the disabling process fails, the system displays an error message on the web console of the primary System Manager.

Related links

Enabling the Geographic Redundancy replication on page 77
Geographic Redundancy field descriptions on page 83

Activating the secondary System Manager server

About this task

- When you activate the secondary System Manager server, the system stops replicating the data from the primary System Manager server to the secondary System Manager server. During activation, you cannot gain access to the web console of the secondary System Manager server for some time.
- In the same browser instance, do not open the primary and secondary System Manager server in different tabs. The system might display an unknown error after the activation, deactivation, or recovery is complete. You can ignore this error message.

Before you begin

Log on to the System Manager web console of the secondary server.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy** > **GR Health**.
2. Click **Activate Secondary Server**.

The system displays the Geographic Redundancy (GR) Health Current status dialog box.

3. In the Select the reason for activation, choose one of the following options:
   - **Primary Down**: When the primary System Manager server becomes nonoperational, the server hardware is faulty and unusable, or the application server fails to recover.
   - **Network Split**: When the enterprise network splits and servers fail to communicate with each other.
   - **Maintenance**: When the maintenance activities such as backup, restore, upgrade, and shutdown are in progress.
   - **Other**: Any other reason where the primary System Manager server becomes unusable and needs the secondary System Manager server to become operational.
4. Click **Yes**.

   The system displays the initialization of the activation process.
5. Click **Yes**.

   The activation process takes about 15–20 minutes to complete.

   If the activation process fails, the system displays an error message on the secondary System Manager web console and rolls back to the previous state. If the activation process is successful, the secondary System Manager server changes to the active mode and provides complete System Manager functionality.

   Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

Related links

Deactivating the secondary System Manager server on page 79
Geographic Redundancy field descriptions on page 83

Deactivating the secondary System Manager server

Before you begin

Log on to the System Manager web console of the secondary server.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy** > **GR Health**.
2. Click **Deactivate Secondary Server**.

   The system displays the Deactivate Secondary Server dialog box and the progress while performing the deactivation process.
3. Click **OK**.

   If the deactivation process is complete, the secondary System Manager server goes to the standby mode. If the deactivation process fails, the system displays an error message on the secondary System Manager web console and the server remains in the active mode.

Next steps

Restore primary System Manager. For information, see “Restoring the primary System Manager server”.

Related links

Activating the secondary System Manager server on page 78
Geographic Redundancy field descriptions on page 83

Restoring the primary System Manager server

Before you begin

Log on to the System Manager web console of the primary server.

About this task

You can restore the data when the secondary System Manager server is active or in the standby mode. However, for minimum system nonfunctional time during data restoration or an emergency or both, you can restore the data when the secondary System Manager server is active.

Important:

After you restore the system with the secondary System Manager data, if you want to revert to the primary System Manager data, you can restore to the primary System Manager data using the procedure in Step 4. However, you must restore to the primary System Manager data, before you enable the Geographic Redundancy replication. After you enable the Geographic Redundancy replication, you cannot restore to the primary System Manager server data.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Restore Data**.
3. On the Restore GR dialog box, select a server whose data you want to retain:
   - **Primary Server**

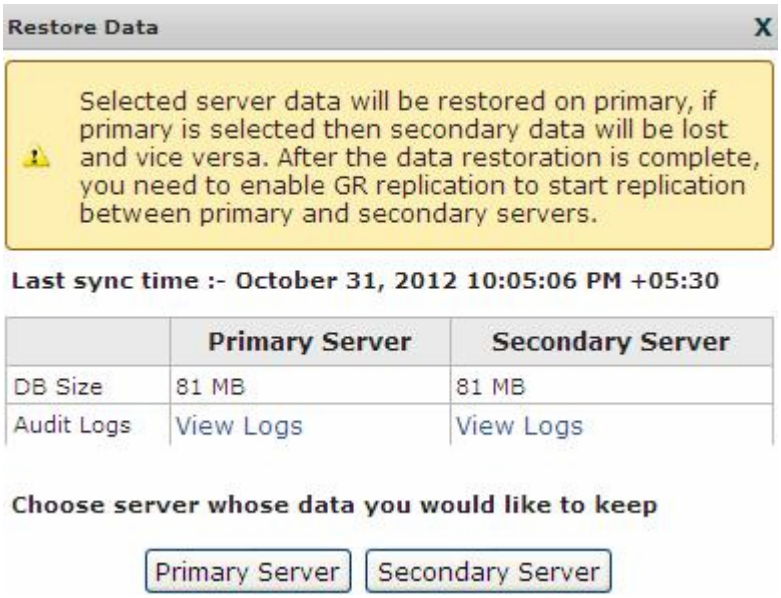
     The system keeps the primary System Manager server data. The data on the secondary System Manager server is lost.

     Select the secondary System Manager server if the secondary System Manager server data changes significantly during the interval between activation and deactivation and the administrator wants to retain those changes even after restoring the data using **Restore Data**.
   - **Secondary Server**

     The system restores the data from the secondary server on the primary System Manager server. the System Manager web console is unavailable for some time. The time that the system takes to restore depends on the network speed and the size of the data that the system must restore.

     After the system recovery, select the secondary System Manager server if the secondary System Manager server data changes significantly during the interval between the system recovery and the deactivation and if you want to retain the changes

from the secondary System Manager server after restoring the data by using **Restore Data**.



The system displays the Restore Status dialog box.

The system displays the restore operation status and the status of the primary and the secondary System Manager server.

Important:

After you restore the data, all changes that you make on the secondary System Manager server that is active will not be available on the primary System Manager server.

4. If you later decide to revert to the database of the primary System Manager server, perform the following steps after the restore is complete:
   a. Using the command line interface, log in to System Manager of the primary server with administrator privilege CLI user credentials.
   b. Change to the `$MGMT_HOME/geo/bin` directory.
   c. Type `sh backupandrestore.sh recovery secondaryIP secondaryFQDN`.

      When the script completes, System Manager restarts and contains the data from the primary System Manager server that was available before you restored with the secondary System Manager data.

      Note:

      - To restore with the secondary System Manager server data again, activate and deactivate the secondary System Manager server.

- Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

Next steps

Verify the data and deactivate the secondary System Manager server if the server is active during the restoration process.

Enable the Geographic Redundancy replication to synchronize the primary and secondary System Manager servers.

Related links

Enabling the Geographic Redundancy replication on page 77
Deactivating the secondary System Manager server on page 79
Geographic Redundancy field descriptions on page 83

Converting the primary System Manager server to the standalone server

Before you begin

- Log on to the System Manager web console of the primary server.
- Disable the Geographic Redundancy replication if you have not already disabled.

Note:

You can also reconfigure secondary System Manager to the standalone server by performing the same steps.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Select the primary System Manager server, and click **Convert To Standalone**.

   The system displays a dialog box.
3. Click **OK**.

   If the conversion is successful, the system displays `Converted to Standalone successfully` and converts the primary System Manager server to a standalone server.

   The system displays the status of the server as `Unconfigured` on the Manage Elements page. The administrator can configure the server when required.

Related links

Configuring Geographic Redundancy on page 75
Enabling the Geographic Redundancy replication on page 77
Geographic Redundancy field descriptions on page 83

Geographic Redundancy field descriptions

The Geographic Redundancy and the GR Health pages remain blank on a standalone server or until you configure a secondary System Manager.

Primary Server Details

The system displays the IP address and the FQDN of the primary System Manager server.

Name	Description
Convert to Standalone	Converts to a standalone server. The system displays the **Convert to Standalone** button only when the replication is disabled.
Configure	Configures Geographic Redundancy. The system displays the **Configure** button only on the standalone System Manager server.
Reconfigure	Configures Geographic Redundancy. The system displays the **Reconfigure** button only on the secondary System Manager server.

Secondary Server Configured

You can use the **Enable Replication**, **Disable Replication**, and **Restore Data** buttons only from the primary System Manager server.

Button	Description
Enable Replication	Continuously replicates the data between the primary and the secondary System Manager server. The system displays the **Enable Replication** button after the following events: • State of Geographic Redundancy is Disable. • Geographic Redundancy configuration. • Restoration of the primary Geographic Redundancy server is complete.
Disable Replication	Stops replicating the data between the primary and the secondary System Manager server. The system displays the **Disable Replication** button when the state of Geographic Redundancy is Enable.
Restore Data	Recovers the server after the failback. The system displays the **Restore Data** button when the secondary System Manager server is deactivated.

Field name	Description
IP	Displays the IP address of the secondary System Manager server.
FQDN	Displays FQDN of the secondary System Manager server.
Replication Status	Displays the status of replication. The values are Disabled and Enabled.
Last Action	Displays the last action that you performed on the secondary System Manager server.
Last Action Status	Displays the status of the last action that you performed on the secondary System Manager server.

GR Health field descriptions

The information available on the GR Health page is read-only.

The Geographic Redundancy and the GR Health pages remain blank on a standalone server or until you configure a secondary System Manager.

GR Health

Name	Description
GR Health Status	Displays the health status of the monitored services. The page displays: • ■, if the monitored service stops. • ✔, if the monitored service is running. • ✘, if the monitored service fails to run.
Activate Secondary Server	Click to make the secondary server provide full System Manager functionality when the primary System Manager server fails, or the data network splits. **Note:** • The system displays **Activate Secondary Server** only on the secondary System Manager server. • The system displays the **Activate Secondary Server** or the **Deactivate Secondary Server** button on the page.

Table continues…

Name	Description
Deactivate Secondary Server	Click to make the primary System Manager resume operation. You use this option when the primary System Manager server restores operation or recovers from a network failure. **Note:** The system displays **Deactivate Secondary Server** only on the secondary System Manager server.
Service Name	Displays the name of the service for which the system provides the status of the health.
View Detail	Click **View Graph**. • For database and directory replication, the system displays the graph for default interval. If no graph is present for the default interval, using the calendar, you can set the period for which you require to check the health status, and click **Generate** to view health details in a graph. For database replication, the system displays graphs for time lag and the size lag. For directory replication, the system displays graph for time lag only. • For file replication, the system displays the last replication time and the size of the lag.

HeartBeat status

Click **View Heartbeat Status** to view the details. The system displays the GR Heartbeat page.

Name	Description
Service Name	The name of the monitored service. The services are: • **System Health**: The heartbeat status indicates if the primary or the secondary System Manager server can communicate with the peer System Manager server over the network. • **Database Replication**: The heartbeat status indicates if the data stored in the System Manager database is getting replicated between the primary and the secondary System Manager server. • **Application System Health**: The heartbeat status indicates if the application server of primary or secondary System Manager can query the application server of the peer System Manager. • **File Replication**: The heartbeat status indicates if the configuration files are getting replicated between the primary and the secondary System Manager server. • **Directory Replication**: The heartbeat status indicates if the data stored in the internal LDAP server is getting replicated in the respective System Manager server.
Last Successful Heartbeat Time	The last time the heartbeat was successful for the monitored service.
Last Missed Heartbeat Time	The last time when the monitored service missed the heartbeat.
View Details	The **View Graph** link to view the health status of the monitored service over a period of time. To configure the time period, click **Edit Dates**. The graph displays the status in 0 and 1. • 0 indicates that the monitored service is either stopped or failed at that point of time • 1 indicates that the monitored service is running at that point of time.

Configuring the network parameters from console

About this task

When first started, the System Manager virtual machine collects the network parameters. When the system prompts, enter the network parameters.

Before you begin

Deploy System Manager.

Procedure

1. To provide configuration input, type `y`.

   At this prompt, if you type n thrice, the system displays the following message and also displays the prompt for configuration input.

   ```
   WARNING - Number of re-attempts exceeded the allowed limit.
   ```

   - To enter the configuration details, type `y`.
   - To shut down the application, type `n`.

2. Read the End User License Agreement (EULA).
3. To accept the EULA, in **Do you accept the Avaya Software License Terms? (Y)es/(N)o**, type `Y`.
4. At the prompt, enter the management network parameters, public network parameters, virtual FQDN parameters, SMGR CLI User parameters, and SNMPv3 parameters of the System Manager virtual machine.
5. To schedule the remote backup during the System Manager installation, in **Schedule SMGR Backup**, type the backup definition parameters for the System Manager virtual machine.
6. At the Data Encryption prompt, perform one of the following:
   - To enable data encryption, type `1`.
   - To disable data encryption, type `2`.
7. At the **Enhanced Access Security Gateway (EASG)** prompt, read the following messages, and type one of the following:

   Enable: (Recommended)

   ```
   By enabling Avaya Logins you are granting Avaya access to your
   system.
   This is necessary to maximize the performance and value of your
   Avaya support entitlements, allowing Avaya to resolve product
   issues in a timely manner.
   In addition to enabling the Avaya Logins, this product should
   be registered with Avaya and technically onboarded for remote
   connectivity and alarming. Please see the Avaya support site
   (support.avaya.com/registration) for additional information for
   registering products and establishing remote access and alarming.
   ```

   Disable:

   ```
   By disabling Avaya Logins you are preventing Avaya access to your
   system.
   This is not recommended, as it impacts Avaya’s ability to provide
   support for the product. Unless the customer is well versed
   ```

`in managing the product themselves, Avaya Logins should not be disabled.`

a. 1: To enable EASG.

   Avaya recommends to enable EASG.

   You can also enable EASG after deploying or upgrading the application by using the command: **`EASGManage --enableEASG`**.

b. 2: To disable EASG.

8. To confirm the network parameters, type `Y`.

   The system starts the configuration of the network parameters.

   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. Once the configuration is complete, the log file displays the message: `exit status of eject command is 0`.

Next steps

Once the first boot configuration is complete, it is mandatory to deploy the latest patch.

To verify that the System Manager installation is complete and the system is ready for patch deployment, do one of the following:

- On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, and ensure that the system displays the System Manager Log on page.

  The system displays the message: Installation of latest System Manager patch is mandatory.

- On the Command Line Interface, log on to the System Manager console, and verify that the system does not display the message: `Maintenance: SMGR Post installation configuration is In-Progress`.

  It should only display the message: `Installation of latest System Manager patch is mandatory`.

Note:

Modifying the network or management configuration is not recommended before the patch deployment.

Related links

Network and configuration field descriptions on page 89

Network and configuration field descriptions

Name	Description
Management IPv4 Address (or Out of Band Management IPv4 Address)	The IPv4 address of the System Manager application 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 application.
Management Gateway	The gateway IPv4 address to assign to the System Manager application.
IP Address of DNS Server	The DNS IP addresses to assign to the primary, secondary, and other System Manager applications. Separate the IP addresses with commas (,).
Management FQDN	The FQDN to assign to the System Manager application. **Note:** System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.
IPv6 Address	The IPv6 address of the System Manager application for out of band management. The field is optional.
IPv6 Network prefix	The IPv6 subnetwork mask to assign to the System Manager application. The field is optional.
IPv6 Gateway	The gateway IPv6 address to assign to the System Manager application. The field is optional.
Default Search List	The search list of domain names. The field is optional.
NTP Server IP/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 application is located. A list is available where you select the name of the continent and the name of the country.

Note:

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

Name	Description
Public IP Address	The IPv4 address to enable public access to different interfaces. The field is optional.
Public Netmask	The IPv4 subnetwork mask to assign to System Manager application. The field is optional.
Public Gateway	The gateway IPv4 address to assign to the System Manager application. The field is optional.

Table continues…

Name	Description
Public FQDN	The FQDN to assign to the System Manager application. The field is optional.
Public IPv6 Address	The IPv6 address to enable public access to different interfaces. The field is optional.
Public IPv6 Network Prefix	The IPv6 subnetwork mask to assign to System Manager application. The field is optional.
Public IPv6 Gateway	The gateway IPv6 address to assign to the System Manager application. The field is optional.

Name	Description
Virtual Hostname	The virtual hostname of the System Manager application. **Note:** • The VFQDN value must be unique and different from the FQDN value of System Manager and the elements. • VFQDN is a mandatory field. • By default, VFQDN entry gets added in the `/etc/hosts` file during installation. Do not remove VFQDN entry from the `/etc/hosts` file. • VFQDN entry will be below FQDN entry and mapped with IP address of system. Do not manually change the order and value. • You must keep VFQDN domain value same as of FQDN domain value. • If required, VFQDN value can be added in DNS configuration, ensure that the value can be resolved. • Secondary Server (Standby mode) IP address value is mapped with VFQDN value in hosts file of Primary server IP address. After Secondary Server is activated, then the IP address gets updated with Secondary Server IP address. • 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: 1. Log in to System Manager with administrator privilege credentials. 2. Run the **`changeVFQDN`** command. **Important:** When you run the **`changeVFQDN`** command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.
Virtual Domain	The virtual domain name of the System Manager application.

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.

Name	Description
SMGR command line user name	The user name of the System Manager CLI user. **Note:** Do not provide the common user names, such as, admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel.
SMGR command line user password	The password for the System Manager CLI user.
Confirm Password	The password that you retype to confirm the System Manager CLI user authentication.

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. The system generates an alarm if you do not schedule a System Manager backup every seven days.
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 six 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.

Name	Description
Public	The port number that is mapped to public port group. You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.
Out of Band Management	The port number that you must assign to the Out of Band Management port group. The field is mandatory.

Enhanced Access Security Gateway (EASG) - EASG User Access

Name	Description
Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG	Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks. The options are: • 1: To enable EASG. • 2: To disable EASG. Avaya recommends to enable EASG. You can also enable EASG after deploying or upgrading the application by using the command: **`EASGManage --enableEASG`**.

Customer Root Account

Note:

The **Customer Root Account** field is applicable only in case of deploying application OVA on Appliance Virtualization Platform and VMware by using Solution Deployment Manager. The system does not display the **Customer Root Account** field, when you deploy an application:

- OVA on VMware by using VMware vSphere Web Client.
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

Name	Description
Enable Customer Root Account for this Application	Enables or disables the customer root account for the application. Displays the ROOT ACCESS ACCEPTANCE STATEMENT screen. To accept the root access, click **Accept**. When you accept the root access statement, the system displays the **Customer Root Password** and **Re-enter Customer Root Password** fields.
Customer Root Password	The root password for the application
Re-enter Customer Root Password	The root password for the application

Data Encryption

Note:

- From Release 8.1.2 and later, Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized Environment.
- For data encryption, you must use a new encryption capable variant of Release 8.1E OVA.

For more information, see the application-specific Data Privacy Guidelines on the Avaya Support website.

Name	Description
Data Encryption	Enables or disables the data encryption. The options are: • **1**: To enable the data encryption. • **2**: To disable the data encryption. **Important:** • An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa. • While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to vCenter limitation. Therefore, ensure that you enter the encryption passphrase, if data encryption is enabled. • **On Solution Deployment Manager:** When the **Data Encryption** field is set to 1, the system enables the **Encryption Pass-Phrase** and **Re-enter Encryption Pass-Phrase** fields to enter the encryption passphrase. • **On vCenter or ESXi:** When the **Data Encryption** field is set to 1, enter the encryption passphrase in the **Password** and **Confirm Password** fields.
Encryption Pass-Phrase	This field is applicable when data encryption is enabled. The passphrase for data encryption. When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules. When you deploy the application by using vCenter or ESXi, the system does not apply the passphrase complexity rules.
Re-enter Encryption Pass-Phrase	The passphrase for data encryption.

Table continues…

Name	Description
Require Encryption Pass-Phrase at Boot-Time	If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default, the **Require Encryption Pass-Phrase at Boot-Time** check box is selected. **Important:** You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA. If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure. You can also set up the remote key server by using the **`encryptionRemoteKey`** command after the deployment of the application.

Related links

Configuring the network parameters from console on page 86

Chapter 8: Post-installation verification

Post-installation steps

Procedure

Recreate all licenses with the new host ID format, and install the new license files.

System Manager uses a new host ID format for Avaya WebLM server. Therefore, all previously installed licenses become invalid. For instructions to install the license file, see Managing licenses in *Administering Avaya Aura® System Manager*.

Verifying the installation of System Manager

About this task

Perform the following verification procedure after you install System Manager Release 8.1.3 and configure System Manager.

Procedure

1. On the web browser, type `https:// <fully qualified domain name of System Manager>`, and ensure that the system displays the System Manager web console.
2. On the upper-right corner, click  and click **About**.

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

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.

Note:

After installing the language pack, you cannot uninstall the language pack.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Type `locate LocalizationScript.sh`, and press `Enter`.

   System Manager displays the path of the localization script.

   For example: `/opt/Avaya/Mgmt/8.1.x/CommonConsole/script/LocalizationScript.sh`
3. Type `locate FrenchResourceBundle.zip`, and press `Enter`.

   The System Manager displays the path of the `FrenchResourceBundle.zip` script.

   For example: `/opt/Avaya/Mgmt/8.1.x/CommonConsole/localization/common_console/FrenchResourceBundle.zip`

   This is just an example of the path; the path might vary based on actual path that you get.
4. Type `cd $MGMT_HOME/CommonConsole/script/` to go to the localization script folder.
5. To run the localization script, type `sudo ./LocalizationScript.sh $MGMT_HOME/CommonConsole/localization/common_console/FrenchResourceBundle.zip`.
6. If you are running the data migration through SSH connection, then do not close the SSH session or terminate the connection.

   If you close the SSH session or terminate the connection, System Manager kills the process and the installation fails.

   Note:

   During this activity, System Manager 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 after secondary server is active.
7. Change the browser language setting to French.

Enhanced Access Security Gateway (EASG) overview

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

Managing EASG from CLI

About this task

After deploying or upgrading an Avaya Aura® application, you can enable, disable, remove, restore or view the status of EASG.

Before you begin

Log in to the application CLI interface.

Procedure

1. To view the status of EASG, run the command: **`EASGStatus`**.

   The system displays the status of EASG.

2. To enable EASG, do the following:

   a. Run the command: **`EASGManage --enableEASG`**.

      The system displays the following message.

      ```
      By enabling Avaya Services Logins you are granting Avaya access
      to your system. This is required to maximize the performance
      and value of your Avaya support entitlements, allowing Avaya to
      resolve product issues in a timely manner.

      The product must be registered using the Avaya Global
      Registration Tool (GRT, see https://grt.avaya.com) to be
      eligible for Avaya remote connectivity. Please see the
      Avaya support site (https://support.avaya.com/ registration)
      for additional information for registering products and
      establishing remote access and alarming.
      ```

   b. When the system prompts, type `yes`.

      The system displays the message: `EASG Access is enabled`.

3. To disable EASG, do the following:

   a. Run the command: **`EASGManage --disableEASG`**.

      The system displays the following message.

      ```
      By disabling Avaya Services Logins you are denying Avaya access
      to your system. This is not recommended, as it can impact
      Avaya's ability to provide support for the product. Unless the
      customer is well versed in managing the product themselves,
      Avaya Services Logins should not be disabled.
      ```

   b. When the system prompts, type `yes`.

      The system displays the message: `EASG Access is disabled`.

Viewing the EASG certificate information

Procedure

1. Log in to the application CLI interface.
2. Run the command: **`EASGProductCert --certInfo`**.

   The system displays the EASG certificate details, such as, product name, serial number, and certificate expiration date.

EASG product certificate expiration

The Avaya Aura® application raises an alarm if the EASG product certificate has expired or is about to expire in 365 days, 180 days, or 30 days. To resolve this alarm, the customer must apply the patch for a new certificate or upgrade to the latest release. Else, the customer loses the ability for Avaya to provide remote access support.

If the EASG product certificate expires, EASG access is still possible through the installation of EASG site certificate.

EASG site certificate

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge/response.

Managing site certificates

Before you begin

1. Obtain the site certificate from the Avaya support technician.
2. You must load this site certificate on each server that the technician needs to access. Use a file transfer tool, such as WinSCP to copy the site certificate to /home/*cust* directory, where *cust* is the login ID. The directory might vary depending on the file transfer tool used.
3. Note the location of this certificate and use in place of *installed_pkcs7_name* in the commands.
4. You must have the following before loading the site certificate:
   - Login ID and password
   - Secure file transfer tool, such as WinSCP
   - Site Authentication Factor

Procedure

1. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.
2. To view information about a particular certificate: run the following command:
   - `sudo EASGSiteCertManage --list`: To list all the site certificates that are currently installed on the system.
   - `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.
3. To delete the site certificate, run the following command:
   - `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.
   - `sudo EASGSiteCertManage --delete all`: To delete all the site certificates that are currently installed on the system.

Chapter 9: Maintenance

Backup and restore

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.

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. **(Optional)** To create encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the following fields:

      - **Backup Encryption Password**
      - **Confirm Backup Encryption Password**

   b. In **Backup Encryption Password**, type the encryption password.
   c. In **Confirm Backup Encryption Password**, retype the encryption password.

      You must remember the password to restore the backup.
6. 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

About this task

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

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 **File name**, type the backup file that you want to create.
5. **(Optional)** To create encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the following fields:

      - **Backup Encryption Password**
      - **Confirm Backup Encryption Password**

   b. In **Backup Encryption Password**, type the encryption password.
   c. In **Confirm Backup Encryption Password**, retype the encryption password.

      You must remember the password to restore the backup.
6. 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 Release 8.1 with Release 8.1.1 software patch installed, System Manager on which you restore the backup must run Release 8.1 that has Release 8.1.1 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. **(Optional)** To restore encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the **Backup Encryption Password** field.

   b. In **Backup Encryption Password**, type the encryption password.
5. 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:

     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**.

6. 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.
   ```

7. 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

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

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:

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

5. **(Optional)** To restore encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

System Manager displays the **Backup Encryption Password** field.

b. In **Backup Encryption Password**, type the encryption password.

6. 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.
   ```

7. 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. • 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.

Table continues…

Name	Description
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 back up the System Manager data.
Restore	Opens the Restore page from where you can restore the data to System Manager.

Monitoring a host and virtual machine

Monitoring a platform

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click **Monitor Platforms**.
3. On 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 an application

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click **Monitor Applications**.
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.

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.

Note:

On the System Manager Release 7.1 and later system, if you change the IP Address of System Manager by using the **changeIPFQDN** command, the system changes the host ID of System Manager and invalidate the existing installed license file. Therefore, you must reinstall the license file on System Manager after changing the IP Address of System Manager.

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 < >-IPV6 < >
-IPV6GW < >-IPV6PREFIX < >
```

#	Option	Description	Usage
1	IP	The new Management IPv4 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 IPv4 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 can 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**
7	IPV6	The new Management IPv6 address of System Manager.	**changeIPFQDN -IPV6 2001:b00d:dead:1111:1111:1111:1234:8080**
8	IPV6GW	The new Management Gateway IPv6 address of System Manager.	**changeIPFQDN -IPV6GW 2001:b00d::1**

Table continues…

#	Option	Description	Usage
9	IPV6PREFIX	The new Management netmask prefix of System Manager. The default value is 64.	**changeIPFQDN -IPV6PREFIX 64**

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
```

```
changeIPFQDN -IPV6 2001:b00d:dead:1111:1111:1111:1234:8080 -IPV6GW 2001:b00d::1
-IPV6PREFIX 64
```

changePublicIPFQDN command

Use the **changePublicIPFQDN** command to change the Public IP address when Out of Band Management is enabled. With this command, you can change the IP address, FQDN, Gateway, and Netmask address for Public network configuration of System Manager.

To change the Management IP address when Out of Band Management is enabled, use the **changeIPFQDN** command.

Syntax

changePublicIPFQDN -publicIP < > -publicFQDN < > -publicGATEWAY < > -publicNETMASK < >

#	Option	Description	Usage
1	publicIP	The new Public IPv4 address of System Manager.	**changePublicIPFQDN -IP 10.11.12.13**
2	IPV6	The new public IPv6 address of System Manager.	**changePublicIPFQDN -IPV6 2001:b00d:dead:1111:1111:1111:1234:8080**
3	IPV6GW	The new public IPv6 Gateway address of System Manager.	**changePublicIPFQDN -IPV6GW 2001:b00d::1**
4	IPV6PREFIX	The new public IPv6 Prefix address of System Manager.	**changePublicIPFQDN -IPV6PREFIX 64**
5	publicFQDN	The new Public FQDN of System Manager.	**changePublicIPFQDN -FQDN a.mydomain.smgr.com**
6	publicGATEWAY	The new Public Gateway IPv4 address of System Manager.	**changePublicIPFQDN -GATEWAY 10.11.1.1**
7	publicNETMASK	The new Public netmask address of System Manager.	**changePublicIPFQDN -NETMASK 255.255.203.0**

Example

You can provide options in any combination that the system supports:

```
changePublicIPFQDN -publicIP 10.11.y.z -publicFQDN a.domain.weblm.com -publicGATEWAY
10.11.1.1 -publicNETMASK 255.255.255.0
```

```
changePublicIPFQDN -publicFQDN a.domain.weblm.com -publicGATEWAY 10.11.1.1
```

```
changePublicIPFQDN -publicIP 10.11.y.z
```

Changing the IP address, FQDN, DNS, Gateway, or Netmask address of System Manager 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 Web 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.

Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the  icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.
- 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 <IPv4 address> -FQDN <FQDN> -GATEWAY <Gateway IPv4 address> -NETMASK <Netmask address> -DNS <DNS address> -SEARCH <search list of domain names> -IPV6 <IPv6 address> -IPV6GW <IPv6 Gateway address> -IPV6PREFIX <IPv6 prefix>`.

   For information, see **`changeIPFQDN`**.

2. To configure Public network parameters, type `changePublicIPFQDN -IP <IP address> -PublicFQDN <FQDN> -PublicGATEWAY <Gateway IP address> -PublicNETMASK <Netmask address>`.

For information, see **changePublicIPFQDN**.

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*.

Configuring the NTP server

Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the  icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.

Procedure

Type `configureNTP <IP address of NTP server>`.

Configuring the time zone

About this task

When you run the **configureTimeZone** command, it restarts the database connection.

Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the  icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.

Procedure

1. Type `configureTimeZone` on the System Manager command line interface.
2. Select the time zone from the list.

   For example, America/Denver.

3. Reboot the system to reflect the time zone changes.

System Manager command line interface operations

#	Command	Parameters	Description	Usage
1	**changeIPFQDN**	• **-IP <new Management interface or Out of Band Management IP address for System Manager>** • **-FQDN <new Management or Out of Band Management fully qualified domain name for System Manager>** • **-GATEWAY <new Management interface or Out of Band Management Gateway address for System Manager>** • **-NETMASK <new Management interface or Out of Band 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 Band Management IP address, FQDN, Gateway, Netmask, DNS, and the search list with the new value. **Note:** On the System Manager Release 7.1 and later system, if you change the IP Address of System Manager by using the **changeIPFQDN** command, the system changes the host ID of System Manager and invalidate the existing installed license file. Therefore, you must reinstall the license file on System Manager after changing the IP Address of System Manager.	• **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>**

Table continues…

#	Command	Parameters	Description	Usage
2	**changePublicIPFQDN**	• **-publicIP <new IP address for System Manager>** • **-publicFQDN <new fully qualified domain name for System Manager>** • **-publicGATEWAY <new Gateway address for System Manager>** • **-publicNETMASK <new netmask address for System Manage>**	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 Public IP address> -publicGATEWAY <new Public Gateway address for System Manager>**
3	**upgradeSMGR**	**<absolute path to the dmutility.bin> -m –v**	Upgrades System Manager using the data migration utility.	**upgradeSMGR dmutility *.bin -m –v**
4	**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 SMGRservicepackName>** **Note:** Copy the System Manager service pack or patches that you must install to `/swlibrary`.
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**

Table continues…

#	Command	Parameters	Description	Usage
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)
8	**configureOOBM**		Enables or disables the Out of Band Management configuration.	• To enable Out of Band Management: **configureOOBM –EnableOOBM** • To disable Out of Band Management: **configureOOBM -DisableOOBM**
9	**enableOOBMMultiTenancy**		If Out of Band Management and MultiTenancy are enabled on system, use this command to provision tenant administrators to available on public interface.	
10	**setSecurityProfile**		Enabling the commercial and military grade hardening.	• Enabling commercial grade hardening: **setSecurityProfile --enable-commercial-grade** • Enabling military grade hardening: **setSecurityProfile --enable-military-grade**

Table continues…

#	Command	Parameters	Description	Usage
11	**EASGManage**		Enables or disables EASG.	• **EASGManage --enableEASG** • **EASGManage --disableEASG**
12	**EASGStatus**		Displays the status of EASG.	
13	**EASGProductCert**		Displays the EASG certificate details.	**EASGProductCert --certInfo**
14	**EASGSiteCertManage**		To manage EASG Certificates.	
15	**editHosts**		To modify the `/etc/hosts` file.	
16	• **swversion** • **swversion -s**		• swversion: Displays the System Manager software information. • swversion -s: Displays the System Manager software version and also displays information about the application name, profile, and deployment type. • **Note:** The output varies based on the application deployment and the virtualization environment.	

Table continues…

#	Command	Parameters	Description	Usage
17	**changeVFQDN**		To change the System Manager Virtual FQDN.	**changeVFQDN** Type the System Manager Virtual FQDN. **Note:** When you run the **changeVFQDN** command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.

Table continues…

#	Command	Parameters	Description	Usage
18	**pairIPFQDN**		Changing the IP address and FQDN on the secondary System Manager server when the secondary is in the standby or active mode.	• If you changed both the IP address and FQDN of primary server, type the following on the secondary server: `#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the primary server> -NEWIP <New IP of the primary server> -OLDFQDN <Old FQDN of the primary server> -NEWFQDN <New FQDN of the primary server>` • If you changed the IP address of primary server, type the following on secondary server: `#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the primary server> -NEWIP <New IP of the primary server>` • If you changed FQDN of primary server, type the following on secondary server: `#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDFQDN <Old FQDN of`

Table continues…

#	Command	Parameters	Description	Usage
				the primary server> -NEWFQDN <New FQDN of the primary server>
19	**smgr**		Starts, stops, and checks the status of Jboss service.	**smgr** start/stop/status
20	**smgr-db**		Starts, stops, and checks the status of postgresql.service.	**smgr-db** start/stop/status
21	**toggleWeblmOldcert**		Replaces identity certificate with old certificate.	**toggleWeblmOldcert**
22	**getUserAuthCert**		Generates a user specific certificate for System Manager to facilitate certificate-based authentication.	
23	**changeCipherSuiteList**		Configures cipher suite mode for System Manager	• To configure strict cipher suite list, type the following command. This would disable CBC ciphers: **changeCipherSuiteList LIST2** • To configure relax cipher suite list, type the following command. This would enable CBC ciphers: **changeCipherSuiteList LIST1**
24	**collectLogs**		Collects the required logs.	• To collect all the logs: **collectLogs** • To collect all the logs along with backup: **collectLogs -Db** • To collect all the logs along with CND data: **collectLogs -CND**

Table continues…

#	Command	Parameters	Description	Usage
25	**rebootVM**		Reboots the System Manager virtual machine.	Type `y` or `n` to reboot the System Manager virtual machine.
26	**powerOffVM**		Power off the System Manager virtual machine.	Type `y` or `n` to power off the System Manager virtual machine.
27	sudo /bin/ systemctl (parameter) snmpd	start/stop/restart/status	To start or stop, and to check status of the SNMP service.	
28	sudo /bin/ systemctl (parameter) spiritAgent	start/stop/restart/status	To start or stop, and to check status of the Spirit Agent service.	
29	sudo /bin/ systemctl (parameter) cnd	start/stop/restart/status	To start or stop, and to check status of the CND service.	
30	encryptionPassphrase	[add | change | remove | list]	To add, change, remove, and display the encryption passphrase.	• **encryptionPassphrase add**: To add encryption passphrase. • **encryptionPassphrase change**: To change existing encryption passphrase. • **encryptionPassphrase remove**: To remove encryption passphrase. • **encryptionPassphrase list**: To display the encryption passphrase and slot assignment.

Table continues…

#	Command	Parameters	Description	Usage
31	encryptionRemoteKey	[add | remove | list]	To add, remove, and display the remote key server.	• **encryptionRemoteKey add**: To add remote key server. • **encryptionRemoteKey remove**: To remove remote key server. • **encryptionRemoteKey list**: To display the remote key server and slot assignment.
32	encryptionLocalKey	[enable | disable]	To enable and disable the local key store.	• **encryptionLocalKey enable**: To enable local key store. • **encryptionLocalKey disable**: To disable local key store.
33	encryptionStatus		Displays information about encryption on the system.	**encryptionStatus** displays information about encryption on the system.
34	**updateLogRetention.sh**	[-p] [-v] [maxRetentionTime]	Manages the log retention time.	
35	**pruneAllLogs.sh**	[-b] [-t] [-v] [-h] [maxRetentionTime]	Manages the deletion of log files.	

Table continues…

#	Command	Parameters	Description	Usage
36	**manageEntityClassWhitelist**	[-h] [addAll *-e* <ENTITY_CLASS_NAME> *-f* <INPUT_FILE> *-u* <USERNAME> *-p* <PASSWORD>] [add *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-u* <USERNAME> *-p* <PASSWORD>] [list *-e* <ENTITY_CLASS_NAME> *-f* <OUTPUT_FILE> *-u* <USERNAME> *-p* <PASSWORD> *-pn* <PAGENUMBER> *-ps* <PAGESIZE>] [view *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-f* <OUTPUT_FILE> *-u* <USERNAME> *-p* <PASSWORD>] [subjectCheck *-e* <ENTITY_CLASS_NAME> *-u* <USERNAME> *-p* <PASSWORD>] [deleteAll *-e* <ENTITY_CLASS_NAME> *-u* <USERNAME> *-p* <PASSWORD>] [delete *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-u* <USERNAME> *-p* <PASSWORD>]	You can add, list, view, and delete the subject names for the provided entity class. You can add and delete the bulk entries of subject names and check the status of the subject name validation for the entity class.	
37	**outboundConnectionLogging**	[enable] [disable]	If you enable this, you can capture the logs in the `/var/log/Avaya/connections` file for every new outgoing connections initiated from System Manager.	
38	**configureOutboundFirewall**	[add {*-s*} {*-f*}] [list] [status] [remove {*-e*} {*-f*}] [disable] [overwrite {*-s*} {*-f*}] [enable-logging] [disable-logging] [logging-status]	If you enable this, you can configure System Manager outbound firewall.	

Table continues…

#	Command	Parameters	Description	Usage
39	**setSecurityPolicy**	[--status] [--display-only] [--restore-standard] [--refresh-custom]	You can modify the default password policy settings of System Manager by using the **setSecurityPolicy** command. This command is only applicable for changing or setting up the password for the CLI user or root user that gets created at the time of deployment.	

Generating test alarms

Test alarms

You can generate a test alarm and a clear event corresponding to the generated test alarm. The severity level of the test alarm is minor. The clear event generated has no definite severity level. The clear event updates the status of the test alarms from Raised to Cleared. If Secure Access Link (SAL) Enterprise is configured to forward alarms to Avaya Data Center (ADC), the system also forwards the test alarm and the clear event for the test alarm to the ADC.

Test Alarm Event

Test Alarm property	Value
Alarm.Message	Test alarm
Alarm.Severity	Minor
Alarm.Status	Raised
Alarm.Log.ProcessName	TESTALARM
Alarm.Log.EventCode	TEST_ALARM_GEN_0001

Test Clear Event

Test Clear Event property	Value
Alarm.Message	Clear event for test alarm
Alarm.Severity	Indeterminate
Alarm.Status	Cleared
Alarm.Log.ProcessName	TESTALARM
Alarm.Log.EventCode	TEST_ALARM_CLR_0000

Related links

Generating the test alarm from the web console on page 123

Generating the test alarm from CLI on page 123

Generating the test alarm from the web console

About this task

You can generate test alarms from the System Manager web console for agents, hosts, or elements that are installed with Serviceability Agents running version 6.3.2.4-6706-SDK-1.0 or later.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In the **Agent List** section, select one or more agents for which you want to generate alarms.
4. Click **Generate Test Alarm**.

   The system generates the alarm.
5. To view the alarm, click **Events** > **Alarms**.

   To view the details of the alarm, wait until the system displays the alarms on the Alarming page.

Generating the test alarm from CLI

Procedure

1. Log in to the computer on which you installed System Manager.
2. At the command prompt, perform the following:
   a. To check the status of SAL Agent, type `service spiritAgent status` and press `Enter`.

      The system displays `SPIRIT Agent is running`.

      Note:

      If the system displays `SPIRIT Agent is not running`, then start SAL Agent.

   b. To start SAL Agent, type `service spiritAgent start` and press `Enter`.

      The `utils` directory contains SAL Agent command line utilities.
3. To navigate to the `utils` directory, at the prompt, type `cd $SPIRIT_HOME/scripts/utils/`and press `Enter`.

4. Perform one of the following:
   - To generate the test alarm for System Manager, type `sh generateTestAlarm.sh`, and press `Enter`.
   - To generate the clear alarm for System Manager, type `sh generateTestAlarm.sh -c`, and press `Enter`.
5. Perform one of the following:
   - To generate the test alarm for a different product, type `sh generateTestAlarm.sh -l LOG_LOCATION -p PRODUCT_TYPE`, and press `Enter`.
   - To generate the clear alarm for a different product, type `sh generateTestAlarm.sh -c -l LOG_LOCATION -p PRODUCT_TYPE`, and press `Enter`.

     Here, *LOG_LOCATION* is one of the log files that the SAL agent tails for this product, and `PRODUCT_TYPE` is the log product type that you configured for this product in the SAL agent.

Network Management Systems Destinations

The Session Manager serviceability agent can send SNMPv2c/v3 traps or informs for alarms to multiple destinations such as:

- SAL Gateway, mandatory trap destination
- System Manager trap listener
- Third-party NMS
- Avaya SIG server

SAL Gateway is a mandatory trap destination for traps sent to Avaya Services for system maintenance. SAL Gateway converts the traps to alarms and forwards the alarms to the Avaya Data Centre for ticketing purposes. Therefore, after you install or upgrade from release earlier than 6.2 to Session Manager Release 6.2 or later, you must configure the serviceability agent with SAL Gateway as a trap destination. You can configure the serviceability agent by using the System Manager web console. You must also configure Session Manager as a managed device on SAL Gateway.

Optionally, you can configure any third-party Network Management Systems (NMS) as a trap destination. Based on customer requirements, Avaya technicians can also configure the Avaya SIG server as another trap destination.

For upgrades from Release 6.2 or later, the configuration of the serviceability agent persists through the Session Manager upgrade.

You can add an NMS destination using the System Manager web console. To add an NMS destination, you must create a target profile for the NMS destination and then attach the target profile to a serviceability agent. For more information on activating agents and attaching target profiles, see Managing Serviceability Agents in *Administering Avaya Aura® System Manager*.

Adding Network Management Systems Destination

You can add an NMS destination using the System Manager web console. To add an NMS destination, you must create a target profile for the NMS destination and then attach the target profile to a serviceability agent. For more information on activating agents and attaching target profiles, see “Managing Serviceability Agents” in *Administering Avaya Aura® System Manager*.

Deleting the virtual machine snapshot

Deleting the virtual machine snapshot from the Appliance Virtualization Platform host

Procedure

1. In the Web browser, type the following URL: `https://<AVP IP Address or FQDN>/ui`
2. To log in to the Appliance Virtualization Platform host, provide the credentials.
3. In the left navigation pane, click **Virtual Machines**.
4. Select the virtual machine, click **Actions** > **Snapshots** > **Manage snapshots**.

   The system displays the Manage snapshots - <Virtual machine name> dialog box.
5. Select the snapshot and click **Delete snapshot**.

   The system deletes the selected snapshot.

Deleting the virtual machine snapshot from the vCenter managed host or standalone host

Procedure

1. Log in to the vSphere Web client for the vCenter managed host or the standalone host.
2. Depending on the host, perform one of the following
   a. On the vCenter managed host, select the host, and then select the virtual machine.
   b. On the Standalone host, select the virtual machine.
3. Right-click the selected virtual machine, click **Snapshot** > **Snapshot Manager**.

   The system displays the Snapshot for the <Virtual machine name> dialog box.
4. Select the snapshot and click **Delete**.

   The system deletes the selected snapshot.

Chapter 10: Resources

System Manager documentation

The following table lists the documents related to System Manager. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		
Avaya Aura® System Manager Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Administering Avaya Aura® System Manager	Administering System Manager applications and install patches on System Manager applications.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Certificate Management	Understand certificate management.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Data Privacy Guidelines	Describes how to administer System Manager to fulfill Data Privacy requirements.	System administrators and IT personnel
Using		
Using the Solution Deployment Manager client	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Avaya Aura® System Manager Solution Deployment Manager Job-Aid	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Implementation		
Upgrading Avaya Aura® System Manager	Upgrade the Avaya Aura® System Manager application to Release 8.1.x.	Implementation personnel
Deploying Avaya Aura® System Manager in Virtual Appliance	Deploy System Manager applications in Virtual Appliance.	Implementation personnel
Deploying Avaya Aura® System Manager in Virtualized Environment	Deploy System Manager applications in Virtualized Environment.	Implementation personnel

Table continues…

Title	Description	Audience
Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment	Deploy System Manager applications in Infrastructure as a Service Environment.	Implementation personnel
Deploying Avaya Aura® System Manager in Software-Only Environment	Deploy System Manager applications in Software-Only Environment.	Implementation personnel
Maintenance and Troubleshooting		
Avaya Aura® System Manager Fault Management and monitoring using SNMP	Monitor System Manager using SNMP.	System administrators and IT personnel
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

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support by Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.

5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
7. Click **Enter**.

Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
  - Click **Filters** to select a product and then type key words in **Search**.
  - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** ( ).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:
  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After you login to the website, enter the course code or the title in the **Search** field and click **Go** to search for the course.

Course code	Course title
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
20970W	Introducing Avaya Device Adapter
20980W	What's New with Avaya Aura® Release 8.1
71200V	Integrating Avaya Aura® Core Components
72200V	Supporting Avaya Aura® Core Components
20130V	Administering Avaya Aura® System Manager Release 8.1
21450V	Administering Avaya Aura® Communication Manager Release 8.1

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.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://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.

Related links

Using the Avaya InSite Knowledge Base on page 130

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.

3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Support on page 130

Appendix A: Best practices for VM performance and features

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, “Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs” at https://www.vmware.com/.

The following sections describe the recommended BIOS settings for:

- Intel Virtualization Technology
- Dell PowerEdge Servers
- HP ProLiant Servers

Related links

Intel Virtualization Technology on page 132
Dell PowerEdge Server on page 133
HP ProLiant G8 and G9 Servers on page 133

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 132

Dell PowerEdge Server

Following are the BIOS recommendations for Dell PowerEdge Servers supported by Avaya SBCE:

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 132

HP ProLiant G8 and G9 Servers

The following are the recommended BIOS settings for the HP ProLiant G8 and G9 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 132

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.

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.

VMware networking best practices

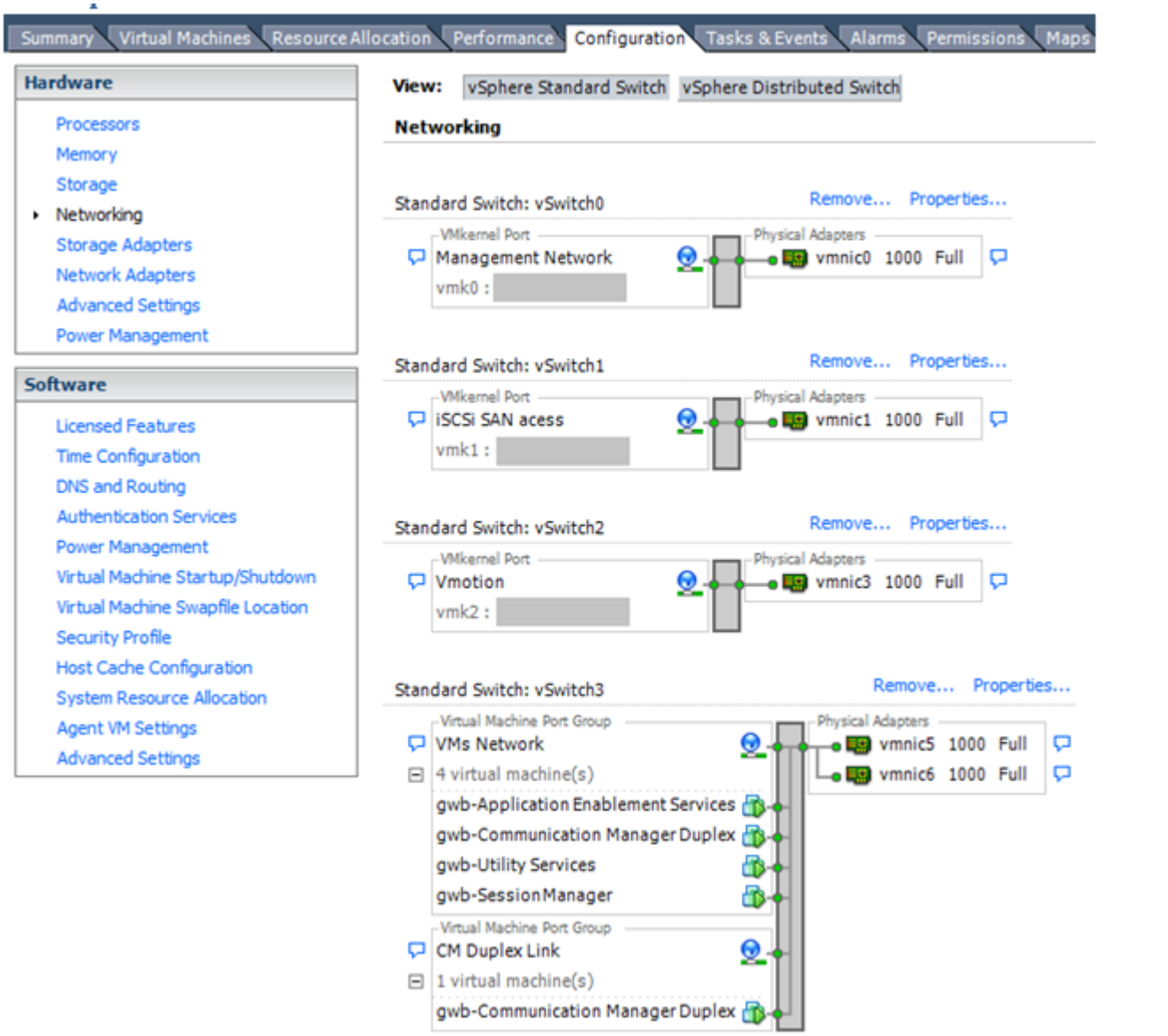
You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

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

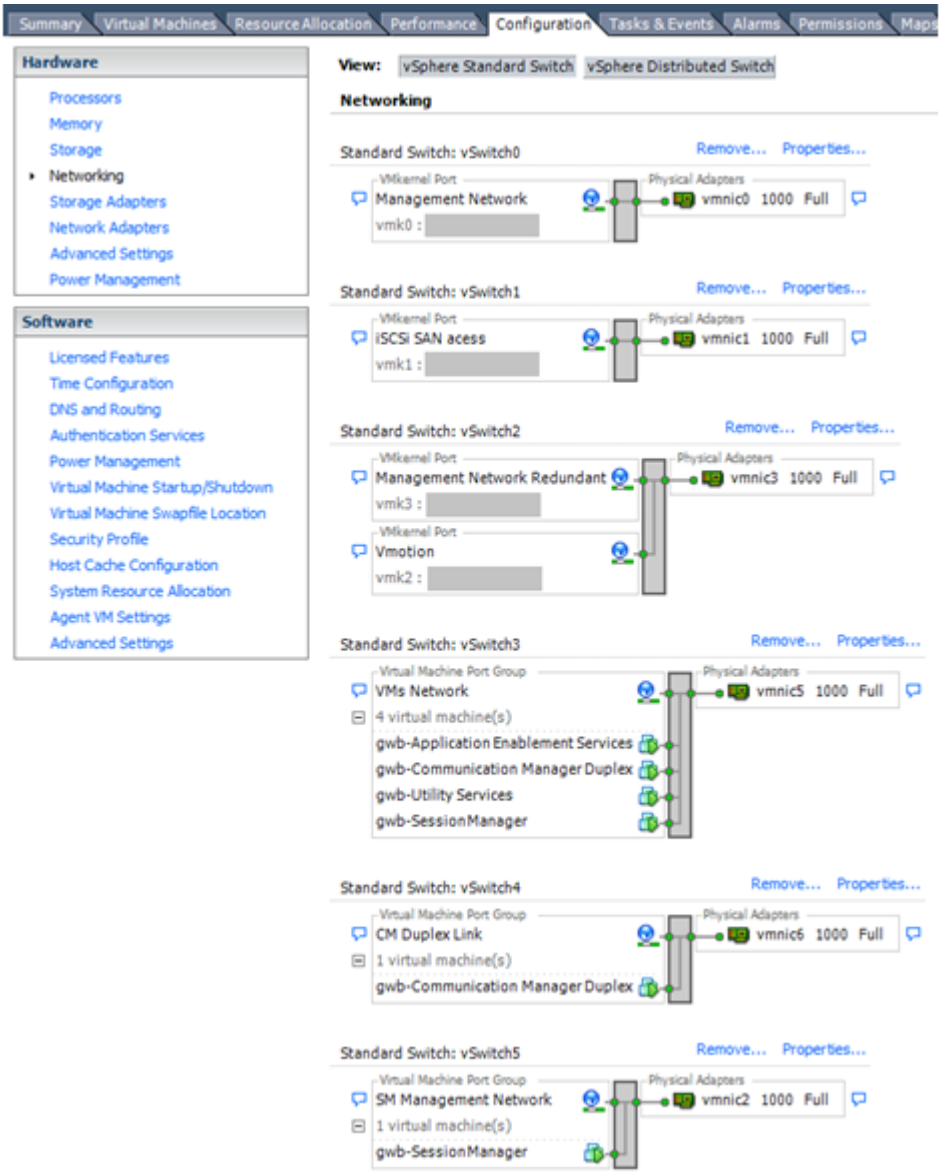


This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

- 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.
- 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	Go to http://support.avaya.com and search for PSN003556u.
Performance Best Practices for VMware vSphere® 6.0	Go to https://www.vmware.com/support/pubs/ and search for *Performance Best Practices for VMware vSphere® 6.0*.
VMware vSphere 7.0 Documentation	Go to https://www.vmware.com/support/pubs/ and search for *VMware vSphere 7.0 Documentation*.
VMware vSphere 6.5 Documentation	Go to https://www.vmware.com/support/pubs/ and search for *VMware vSphere 6.5 Documentation*.
VMware vSphere 6.0 Documentation	Go to https://www.vmware.com/support/pubs/ and search for *VMware vSphere 6.0 Documentation*.
VMware Documentation Sets	https://www.vmware.com/support/pubs/

Storage

For best performance, use System Manager on disks local to the ESXi Host, Storage Area Network (SAN) storage devices, or Network File System (NFS) shares. Network storage system performance (IOPS and latency) must not impact the ability of the System Manager virtual machine to perform I/O operations in a timely fashion. CPU I/O wait times of the virtual machine should be zero or very close to zero. Slow network I/O performance can cause serious stability issues with the OS and the System Manager application.

Thin vs. thick deployments

VMware ESXi uses a thick virtual disk by default when it creates a virtual disk file.. The thick disk preallocates the entire amount of space specified during the creation of the disk. For example, if you create a 10 megabyte disk, all 10 megabytes are preallocated for that virtual disk.

- Thin-provisioned disks can grow to the full size as specified at the time of virtual disk creation, but they cannot shrink. Once you allocate the blocks, you cannot deallocate them.

- Thin-provisioned disks run the risk of overallocating 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 formatting process 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 format tool in Microsoft Windows writes information to all sectors on the disk, which in turn inflates the thin-provisioned disk to full size.

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

VMware vMotion

VMware uses the vMotion technology to migrate a running virtual machine from one physical server to another physical server without incurring down time. 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 WebLM is being used either as a master WebLM server or a local WebLM server in an enterprise licensing deployment for a product, after migration of virtual machine to another physical server using vMotion, validate connectivity from the master WebLM server for all the added local WebLM servers to ensure that the master WebLM server can communicate with the local WebLM servers.

VMware cloning

WebLM supports VMware cloning. However, WebLM does not support the Guest Customization feature. Therefore, do not use the Guest Customization wizard in the VMware cloning wizard while cloning WebLM.

Note:

Do not perform WebLM cloning. If a clone of a WebLM VMware is created, all existing licenses become invalid. You must rehost all the licenses.

If WebLM is the master server in an enterprise licensing deployment for a product, after cloning the master WebLM server, the enterprise license file is invalidated on the clone. You must then rehost the enterprise license file on the cloned WebLM server and redo the enterprise configurations. The administrator must add the local WebLM server again and change allocations for each WebLM server to use the cloned master WebLM server with the existing local WebLM servers.

If WebLM is the local WebLM server in an enterprise licensing deployment for a product, after cloning the local WebLM server, the allocation license file on the local WebLM server is invalidated due to the changed host ID. The administrator must validate the connectivity for the local WebLM server from the master WebLM server and change allocations to push a new allocation license file to the local WebLM server with a valid host ID.

VMware high availability

In a virtualized environment, you must use the VMware High Availability (HA) method to recover WebLM in the event of an ESXi Host failure. For more information, see “High Availability documentation for VMware”.

Note:

High Availability will not result in HostID change and all the installed licenses are valid.

Appendix B: PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) for any software update. For example, a PCN must accompany a service pack or an update that must be applied universally. Avaya issues a product-support notice (PSN) when there is no update, service pack, or release fix, but the business unit or Avaya Services need to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a work around for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at https://support.avaya.com.

   If the Avaya Support website displays the login page, enter your SSO login credentials.
2. On the top of the page, click **DOCUMENTS**.
3. On the Documents page, in the **Enter Your Product Here** field, type the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. Select the appropriate filters as per your search requirement.

   For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

   You can apply multiple filters to search for the required documents.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new services packs are available. The Avaya Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to http://support.avaya.com and search for “Avaya Support Web Tips and Troubleshooting: E-Notifications Management”.

   Under the Results section, click Avaya Support Web Tips and Troubleshooting: E-Notifications Management.

2. Set up e-notifications.

   For detailed information, see the **How to set up your E-Notifications** procedure.

Glossary

Application	A software solution development by Avaya that includes a guest operating system.
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.
EASG	Enhanced Access Security Gateway. The Avaya Services Logins to access your system remotely. The product must be registered using the Avaya Global Registration Tool for enabling the system for Avaya Remote Connectivity.
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.
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 Web Client	The vSphere Web Client is an interface for administering vCenter Server and ESXi. Downloadable versions are VMware 5.5 and 6.0. A browser-based Web client version is VMware 6.5 and later.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W