Upgrading Avaya Aura® System Manager to Release 6.3.15 on VMware® in Virtualized Environment

Release 6.3
Issue 3
November 2015

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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: http://support.avaya.com 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.

Licenses

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

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

License types

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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

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

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

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, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Aura® System Manager from earlier releases to Release 6.3.15 running on VMware in Virtualized Environment. This document includes upgrading checklists and procedures.

Document changes since last issue

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

- Added support for the deployment on VMware Release ESXi 5.5 in Virtualized Environment.
- Added support for the data migration utility wrapper.
- Added support for running the data migration utility as the background process.
- Added support for EULA prompt during the installation of System Manager bin file on VMware.
- Added the message that the system displays while accessing System Manager command line interface if a kernel update requires a restart of the virtual machine.

Intended audience

The primary audience for this document is anyone who is involved with installing, configuring, upgrading, and verifying System Manager on VMware® vSphere™ 5.0, 5.1, or 5.5 Virtualized Environment. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

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

Related resources

Documentation

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

Title	Description	Audience
Design		
Avaya Aura® Virtualized Environment Solution Description	Describes the Virtualized Environment solution from a functional view. Includes a high-level description of the solution, topology diagrams, customer requirements, and design considerations.	Sales engineers
Avaya Aura® System Manager Overview and Specification	Describes product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Sales engineers, Solution architects, Implementation engineers, and Support personnel
Implementation		
Deploying Avaya Aura® System Manager on VMware in Virtualized Environment	Describes the procedures for deploying the Avaya Aura® System Manager virtual application in Virtualized Environment. The document includes procedures for installation, configuration, initial administration, troubleshooting, and basic maintenance.	Implementation engineers, Support personnel
Administration		
Administering Avaya Aura® System Manager	Describes the procedures to configure System Manager and the managed elements that System Manager supports.	Implementation engineers, Support personnel
Maintenance and Troubleshooting		
Troubleshooting Avaya Aura® System Manager	Describes the procedures to troubleshoot the problems during the installation and administration of System Manager and the managed elements that System Manager supports.	Implementation Engineers and Support personnel

Training

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

Course code	Course title	Type
1A00234E	Avaya Aura® Fundamental Technology	AvayaLive™ Engage Theory
1A00236E	Knowledge Access: Avaya Aura® Session Manager and System Manager Fundamentals	AvayaLive™ Engage Theory
5U00106W	Avaya Aura® System Manager Overview	WBT Level 1
4U00040E	Knowledge Access: Avaya Aura®Session Manager and System Manager Implementation	ALE License
5U00050E	Knowledge Access: Avaya Aura®Session Manager and System Manager Support	ALE License
5U00095V	Avaya Aura® System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 1
5U00097I	Avaya Aura®Session Manager and System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 2
3102	Avaya Aura® Session Manager and System Manager Implementation and Maintenance Exam	Exam (Questions)
5U00103W	Avaya Aura® System Manager 6.2 Delta Overview	WBT Level 1

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

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

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

Upgrade overview

The document provides the procedures for upgrading Avaya Aura® System Manager from earlier releases to System Manager Release 6.3.15 on VMware® vSphere™ 5.0, 5.1, or 5.5 in Virtualized Environment.

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

- Network Routing Policy (NRP) export and import utility: To upgrade System Manager from Release 5.2.x, on the 5.2.x system, export the routing data using the NRP export utility and then import the routing data using the NRP import utility to the Release 6.3.15 system.
- Data migration utility: To upgrade System Manager from Release 6.x to Release 6.3.15, use the data migration utility from the command line interface (CLI).

  To upgrade the System Manager virtual application on VMware in Avaya Aura® Virtualized Environment to Release 6.3.15, the data migration utility is the only method.

Important:

The target release mentioned in this document is Release 6.3.15. However, to upgrade to the latest release available for System Manager, use the appropriate System Manager bin file. For more information, see the latest System Manager 6.3.x release notes on the Avaya Support website at http://support.avaya.com/.

For procedures to upgrade System Manager from earlier releases to Release 6.3.15 on System Platform, see *Upgrading Avaya Aura® System Manager on System Platform* on the Avaya Support website at http://support.avaya.com/.

Upgrade paths supported on VMware

The document provides the upgrade procedures for the following paths to upgrade System Manager from releases earlier than Release 6.3.15 to System Manager virtual application Release 6.3.15 on VMware:

From System Manager release	To System Manager Release 6.3.15 on VMware	
	Checklist	**Procedure**
5.2.x on System Platform	Checklist for upgrade from System Manager 5.2.x on page 26	Importing the data to System Manager Release 6.3.15 on page 31
6.0.x, 6.1.x, or 6.2.x on System Platform	Checklist for upgrade from System Manager 6.x on page 16	Upgrading System Manager from Release 6.0, 6.1, and 6.2 to Release 6.3.15 on VMware on page 20
6.2.x on VMware	Checklist for upgrade from System Manager 6.x on page 16	Upgrading System Manager from Release 6.0, 6.1, and 6.2 to Release 6.3.15 on VMware on page 20
6.3.0 through 6.3.15 on System Platform with or without Geographic Redundancy	-	Upgrading System Manager from Release 6.3.x on System Platform to Release 6.3.15 on VMware on page 22
6.3.2 through 6.3.15 on VMware with or without Geographic Redundancy	Checklist for upgrade from System Manager 6.3.2 through 6.3.15 on page 23	Upgrading System Manager from Release 6.3.x on VMware to Release 6.3.15 on VMware on page 24

Chapter 2: Planning and configuration

Server hardware and resources

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

Configuration tools and utilities

System Manager OVA includes the VMware tools. The tools are a suite of utilities that enhance the performance of the guest operating system and improve the management of the virtual machine.

Customer configuration data

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

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

Important:

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

	Required data	Value for the system	Example Value
Network Configuration	IP address		172.16.1.10
	Default netmask		255.255.0.0
	Default 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.

Table continues…

	Required data	Value for the system	Example Value
			Note: System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.
	Domain name		mydomain.com
	Default search list		mydomain.com
	NTP server		172.16.1.100
	Time zone		America/Denver
VFQDN **Note:** The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.	VFQDN short hostname		grsmgr
	VFQDN domain name		dev.com
SNMP Parameters	User Name Prefix		org
	Authentication Protocol Password		orgpassword
	Privacy Protocol Password		orgpassword
Backup Definition Parameters	See Backup Definition parameters		-

System Manager virtual machine resource requirements

The Avaya Aura® System Manager virtual machine requires the following set of resources to be available on the ESXi host before deployment:

VMware resource	Minimum value
CPU core	4
CPU reservation	9600 MHz
Minimum CPU speed based on Xeon E5620 or equivalent processor	2.4 GHz

Table continues…

VMware resource	Minimum value
Memory	9 GB
Memory reservation	9 GB
Storage reservation	72 GB
Shared NIC(s)	1

If the host does not have the minimum resources to allocate to the virtual machine, the system does not start the System Manager virtual machine.

Related links

Adjusting the System Manager virtual machine properties on page 13

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.

VMware software requirements

The following VMware software versions are supported:

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

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

Note:

System Manager does not support ESXi releases earlier than 5.0.

Chapter 3: Upgrading from System Manager 6.x

Overview

Use this section to migrate the data from the following System Manager releases to System Manager Release 6.3.15:

- 6.0, 6.0 SP1, or SP2
- 6.1, 6.1 SP1.1, SP2, SP3, SP4, SP5, SP6, SP7, or SP8
- 6.2, 6.2 SP1, SP2, SP3, or SP4

  For information about upgrading from 6.0.x, 6.1.x, or 6.2.x, see Upgrading System Manager from Release 6.0, 6.1, and 6.2 to Release 6.3.15 on VMware on page 20.
- 6.3, 6.3 SP1, 6.3.2, or later

  For information about upgrading from 6.3.x, see Upgrading System Manager from Release 6.3.x on VMware to Release 6.3.15 on VMware on page 24.

Upgrade worksheet

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

Serial Number	Field	Value	Notes
1	**IP address of external device for remote backup**		On the remote backup page of System Manager Web Console, enter the IP address of the remote server on which you saved the backup file.
2	**User Name and Password of the remote server**		To gain access to the backup file that is located on a remote server, enter the

Table continues…

Serial Number	Field	Value	Notes
			user name and the password for the account on System Manager Web Console.
3	**System Manager command line interface credential**		Open an SSH session and enter `admin` as the user name and password.
4	**Root password of System Manager**		On the CLI, to change to root, type the **`su -`** command.
5	**Path and the file name of the backup file on the remote server**		Enter the path and the file name of the backup file.

Checklist for upgrade from System Manager 6.x

Use the following checklist for upgrading System Manager vAppliance from Release 6.x to Release 6.3.15.

#	Action	Link/Notes	✔
1	Download the `DMUtility_6.3.8_r24.bin` file, the `System_Manager_6.3.15_r5203972.bin` file, and required service packs from the Avaya Support website at http://support.avaya.com.	For the latest service packs and software patches, see System Manager release notes on the Avaya Support website at http://support.avaya.com.	
2	Record the number of users and number of roles. You require this information later to verify that the upgrade is successful.	For information, see Managing users and Managing roles in *Administering Avaya Aura® System Manager*.	

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

4	Keep a copy of the license files for the Avaya Aura® products so you can	-	

Table continues…

#	Action	Link/Notes	✔
	replicate with the new Host ID after the OVA file installation. Ensure that the license file copies are accessible.		
5	Ensure that the server is compatible with System Manager Release 6.3.15.	Server hardware and resources on page 11	
6	Create the snapshot of the System Manager virtual machine.	Creating a data backup on a remote server on page 33	
7	Turn off the System Manager virtual machine.	-	
8	On the ESXi server, install the `SMGR-6.3.0.8.5682-e50-68.ova` file. Use the same IP address or FQDN as that of the existing System Manager. **Note:** System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.	Deploying the System Manager OVA file by using vSphere on page 40	
9	Copy `DMUtility_6.3.8_r24.bin`, `System_Manager_6.3.8_r4502376.bin`, `System_Manager_6.3.15_r5203972.bin`, and the backup file to the `/home/admin` location.	You can use the tools such as SCP, WinSCP, and FileZilla to copy the files.	
10	Create the snapshot of the System Manager virtual machine.	Creating the System Manager virtual machine snapshot on page 19	
11	Install the `System_Manager_6.3.8_r4502376.bin` file.	Installing the System Manager Release 6.3.15 bin file on page 30	
12	In the settings icon (🔧), click **About** to verify that the System Manager version is 6.3.8.	-	
13	Verify the System Manager functionality.	Verifying the functionality of System Manager on page 32	
14	Create the snapshot of the System Manager virtual machine.	Creating the System Manager virtual machine snapshot on page 19	
15	On System Manager Release 6.3.8, run the `DMUtility_6.3.8_r24.bin` file. The upgrade takes about 80–90 minutes. However, the duration depends on the	Upgrading System Manager from Release 6.0, 6.1, and 6.2 to Release 6.3.15 on VMware on page 20	

Table continues…

#	Action	Link/Notes	✔
	factors such as the number of users, backup size, hardware used, and the number of resources shared during the upgrade.		
16	Install the `System_Manager_6.3.15_r5203972.bin` file. The patch installation takes about 60–65 minutes to complete.	Installing the System Manager Release 6.3.15 bin file on page 30	
17	From the **About** link in the settings icon (🔧), verify that the System Manager version is Release 6.3.15.		

You can set up Geographic Redundancy after you upgrade the system to Release 6.3.15. For information, see Geographic Redundancy in *Administering Avaya Aura® System Manager*.

To upgrade from System Manager Release 6.3.2 or later running on VMware, see Upgrading System Manager from 6.3.0, or 6.3.2, through 6.3.15 on VMware to System Manager Release 6.3.15.

Verifying the current software version

About this task

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

Procedure

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

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

Creating a data backup on a remote server

Procedure

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

   - For System Manager 6.0, on System Manager Web Console, click **System Manager Data** > **Backup and Restore**.

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

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

Installing the System Manager OVA file

Procedure

Install the `SMGR-6.3.0.8.5682-e50-68.ova` file.

Related links

Deploying the System Manager OVA file by using vSphere on page 40

Deploying the System Manager OVA file using vCenter on page 46

Creating the System Manager virtual machine snapshot

About this task

❗ **Important:**

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

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

Procedure

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

4. In the Recent Tasks window, perform the following:
    a. Verify the **Status** of the **Create virtual machine snapshot** task.
    b. Wait until the system displays `Completed`.

Upgrading System Manager from Release 6.0, 6.1, and 6.2 to Release 6.3.15 on VMware

Before you begin

- Ensure that System Manager is running.
- Download `DMUtility_6.3.8_r24.bin`, `System_Manager_6.3.8_r4502376.bin`, and `System_Manager_6.3.15_r5203972.bin` files from the Avaya Support website at http://support.avaya.com.

About this task

Use this procedure to upgrade System Manager from Release 6.0, 6.1, and 6.2 to Release 6.3.15 on VMware. The data migration utility runs in the background.

Procedure

1. Log on to the System Manager web console.
2. Record the software version of System Manager from the **About** link.
3. Create the System Manager data backup using System Manager or the System Platform web console and copy the backup to the remote server.
4. Log in to the System Manager command line interface of the existing system as admin.
5. Shut down the System Manager virtual machine using one of the following:
    - On System Platform, click **Shutdown Server** on the Server Reboot/Shutdown page.
        a. Click **Virtual Machine Management** > **Manage**.
        b. Click the System Manager virtual machine and click **Stop**.
    - On VMware, click **Power** > **Power Off**.
6. On the ESXi server, install the `SMGR-6.3.0.8.5682-e50-68.ova` file.

    Important:

    Use the same IP address or FQDN and system parameters that you recorded earlier.
7. Ensure that System Manager is running.
8. Create a snapshot of the System Manager virtual machine.
9. On vSphere Client, select the System Manager virtual machine and click the **Console** tab.
10. To log in to the System Manager virtual machine.

11. Copy `DMUtility_6.3.8_r24.bin`, System Manager backup file, `System_Manager_6.3.8_r4502376.bin`, and `System_Manager_6.3.15_r5203972.bin` files to the `/home/admin` location on System Manager.
12. At the prompt, run the following command to install the System Manager Release 6.3.15 bin file:

    ```
    SMGRPatchdeploy <absolute path to the System Manager 6.3.8 bin file>
    ```

13. On System Manager Release 6.3.8, at the prompt, perform the following:

    a. To remove any older data migration utility-related files, type `rm -fr /opt/Avaya/data_migration`.

    b. Type `upgradeSMGR`.

    c. Type the following absolute path to the data migration utility:

    ```
    /home/admin/<DMUtility name>.bin -m -v
    ```

    d. Type the absolute path to the backup file:

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

    The system displays the following message:

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

14. To continue with the upgrade, type `Y`.

    The system displays the following warning message:

    ```
    The system is now going down for a halt and will be inaccessible for some time.
    Remote broadcast message (Sun Feb 22 21:06:27 2015):
    Data Migration executes in background process. For details, see System Manager
    Data Migration logs in the /var/log/Avaya/datamigration/data_migration.log
    ```

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

15. Log on to System Manager and verify that the upgrade is successful.
16. At the prompt, run the following command to install the Release 6.3.15 bin file:

    ```
    SMGRPatchdeploy <absolute path to the System_Manager_6.3.15_r5203972.bin file>
    ```

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

17. To verify that the bin file installation is successful, on the System Manager web console, click the settings icon (🔧) and click **About**.

Related links

Installing the System Manager Release 6.3.15 bin file on page 30

Creating a data backup on a remote server on page 33

Verifying the functionality of System Manager on page 32

Upgrading System Manager from Release 6.3.x on System Platform to Release 6.3.15 on VMware

About this task

Use this procedure to upgrade System Manager Release 6.3.x running on System Platform to Release 6.3.15 on VMware.

Before you begin

Ensure that System Manager is running.

Procedure

1. Log on to the System Manager web console.
2. Record the software version of System Manager from the **About** link.
3. If Geographic Redundancy is configured on this system, convert the primary System Manager server to a standalone server.

   For more information, see Geographic Redundancy in *Administering Avaya Aura® System Manager*.
4. Create the System Manager data backup from System Platform web console, and copy the backup to the remote server.
5. Shutdown the System Platform server that hosts System Manager.
6. On the ESXi server, install the `SMGR-6.3.0.8.5682-e50-68.ova` file.

   Important:

   Use the same IP address or FQDN and system parameters that you recorded earlier.
7. Upgrade System Manager to the same 6.3.x version, and install the software patches on which System Platform-based System Manager was running earlier.
8. Ensure that System Manager is running.
9. Create a snapshot of the System Manager virtual machine.
10. Using System Manager Backup and Restore page, restore the data from the backup that is taken in Step 4 on page 22.
11. Confirm that System Manager is operational, delete the old snapshot, and create a new snapshot.

    Note:

    Do not keep more than one snapshot at any given point in time. Keeping more than one snapshot might affect the virtual machine performance.

12. On System Manager 6.3.x that is running on VMware, install the System Manager Release 6.3.15 bin file.
13. Verify that the upgrade is successful and then delete the snapshot.
14. To set up Geographic Redundancy, configure Geographic Redundancy.

    For more information, see Geographic Redundancy in *Administering Avaya Aura® System Manager*.

Checklist for upgrade from System Manager 6.3.2 through 6.3.15

Use the following checklist for upgrading System Manager from Release 6.3.2 through 6.3.15 to Release 6.3.15 on VMware.

#	Field	Notes	✔
1	Download the `System_Manager_6.3.15_r5203972.bin` file from the Avaya Support website at http://support.avaya.com.	-	
2	Verify the software version of the current System Manager.		
3	Disable the Geographic Redundancy replication if already enabled on the system.	Perform only in the Geographic Redundancy setup.	
4	Create the snapshot of the System Manager virtual machine.	Creating the System Manager virtual machine snapshot on page 19	
5	Install the `System_Manager_6.3.15_r5203972.bin` file. In the Geographic Redundancy setup, complete the installation on the primary System Manager first and then perform on the secondary Geographic Redundancy.	Installing the System Manager Release 6.3.15 bin file on page 30 **Note:** The upgrade process on the primary System Manager takes about 60–65 minutes and about 70–75 minutes on the secondary System Manager. Wait until the upgrade process is complete, and continue with the next step.	
6	Enable the Geographic Redundancy replication if you disabled on the system.	Perform only in the Geographic Redundancy setup.	
7	Verify that the version of System Manager in the **About** link is Release 6.3.15.	-	

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

Upgrading System Manager from Release 6.3.x on VMware to Release 6.3.15 on VMware

Before you begin

- Ensure that System Manager is running.
- To reach the System Manager CLI, use one of the following methods:
  - Open vSphere Client and click on the **Console** tab or the 🖥 icon.
  - Start an SSH on System Manager.
- Download the `System_Manager_6.3.15_r5203972.bin` file from the Avaya Support website at http://support.avaya.com/ and copy the file to the `/home/admin` location on System Manager.

About this task

Use this procedure to upgrade System Manager from Release 6.3.x on VMware to System Manager Release 6.3.15 on VMware.

Procedure

1. Log on to the System Manager web console.
2. Record the software version of System Manager from the **About** link.
3. Disable the Geographic Redundancy replication if already enabled on the system.

   Note:

   Perform the step only in the Geographic Redundancy setup.

   For information, see Geographic Redundancy in *Administering Avaya Aura® System Manager*.
4. Create a snapshot of the System Manager virtual machine.
5. At the prompt, run the following command to install the bin file:

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

   In the Geographic Redundancy setup, install the bin file on the primary System Manager first and then install on the secondary System Manager.

   The upgrade process on the primary System Manager takes about 60–65 minutes and about 70–75 minutes on the secondary System Manager.

   Wait until the upgrade process is complete, and continue with the next step.
6. Verify that the bin file installation is successful.
7. Enable the Geographic Redundancy replication if you disabled on the system.

   Note:

   Perform the step only in the Geographic Redundancy setup.

For more information, see Geographic Redundancy in *Administering Avaya Aura® System Manager*.

Related links

Installing the System Manager Release 6.3.15 bin file on page 30
Creating a data backup on a remote server on page 33
Verifying the functionality of System Manager on page 32

Chapter 4: Upgrading from System Manager 5.2.x

Overview

Use this section to upgrade System Manager Release 5.2, 5.2 SP1, or 5.2 SP2 to Release 6.3.15 running on VMware.

During the upgrade from System Manager Release 5.2.x to Release 6.3.15, the system only retains the routing data. You must manually add the remaining System Manager data to the Release 6.3.15 system.

Checklist for upgrade from System Manager 5.2.x

Use the following checklist for upgrading System Manager from Release 5.2, 5.2 SP1, or 5.2 SP2 to Release 6.3.15 on VMware.

#	Field	Notes	✔
1	Download the .OVA file, service packs, and patches from the Avaya Support website at http://support.avaya.com.	For the latest service packs and software patches, see System Manager release notes on the Avaya Support website at http://support.avaya.com.	
2	Verify the software version of the current System Manager.	Verifying the current software version on System Manager 5.2.x or earlier on page 28	
3	Record the number of users and number of roles. You require this information later to verify that the upgrade is successful.	For information, see Managing users and Managing roles in *Administering Avaya Aura® System Manager*.	
4	Record the IP address or FQDN and the system parameters.	In the command line interface, type the following commands for the details: `# ifconfig eth0 | grep inet` The system displays `inet addr:xxx.xxx.xxx.xxx`	

Table continues…

#	Field	Notes	✔

		`Bcast:xxx.xxx.xxx.xxx`
		`Mask:xxx.xxx.xxx.xxx.`
		`#admin >hostname`	

5	Create a backup of System Manager and copy to the remote server.	Creating a data backup on a remote server on page 28	
6	Export the routing data from System Manager Release 5.2.x.	Exporting the routing data from System Manager 5.2.x on page 28	
7	Ensure that the server is compatible with System Manager Release 6.3.15.	Server hardware and resources on page 11	
8	On the ESXi server, install the `SMGR-6.3.0.8.5682-e50-68.ova` file. Use the same IP address or FQDN as that of the existing System Manager. System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.	Deploying the System Manager OVA file by using vSphere on page 40	
9	Copy the `System_Manager_6.3.15_r5203972.bin` file to the `/home/admin` location on System Manager.		
10	Install the `System_Manager_6.3.15_r5203972.bin` file. The patch installation takes about 60–65 minutes to complete.	Installing the System Manager Release 6.3.15 bin file on page 30	
11	From the **About** link in the settings icon (🔧), verify that the System Manager version is Release 6.3.15.	-	
12	Verify the System Manager functionality.	Verifying the functionality of System Manager on page 32	
13	Create the snapshot of the System Manager virtual machine.	Creating the System Manager virtual machine snapshot on page 19	
14	Import the routing data to System Manager Release 6.3.15.	Importing the data to System Manager Release 6.3.15 on page 31	

You can set up Geographic Redundancy after you upgrade the system to Release 6.3.15. For information, see Geographic Redundancy in *Administering Avaya Aura® System Manager*.

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

Procedure

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

Creating a data backup on a remote server

Before you begin

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

Procedure

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

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

Exporting the routing data from System Manager 5.2.x

Before you begin

- Create a backup of System Manager 5.2.x and copy to the remote server.
- Record the NRP records on System Manager 5.2.x. To view the records, on the web console of System Manager 5.2, click **Routing** > **Policies**. After you import the data, you require these records to verify if the system has successfully imported the data on System Manager Release 6.3.15.
- Record the data related to users, custom roles, and configuration. After importing the NRP data, you must manually add the data to System Manager Release 6.3.15.

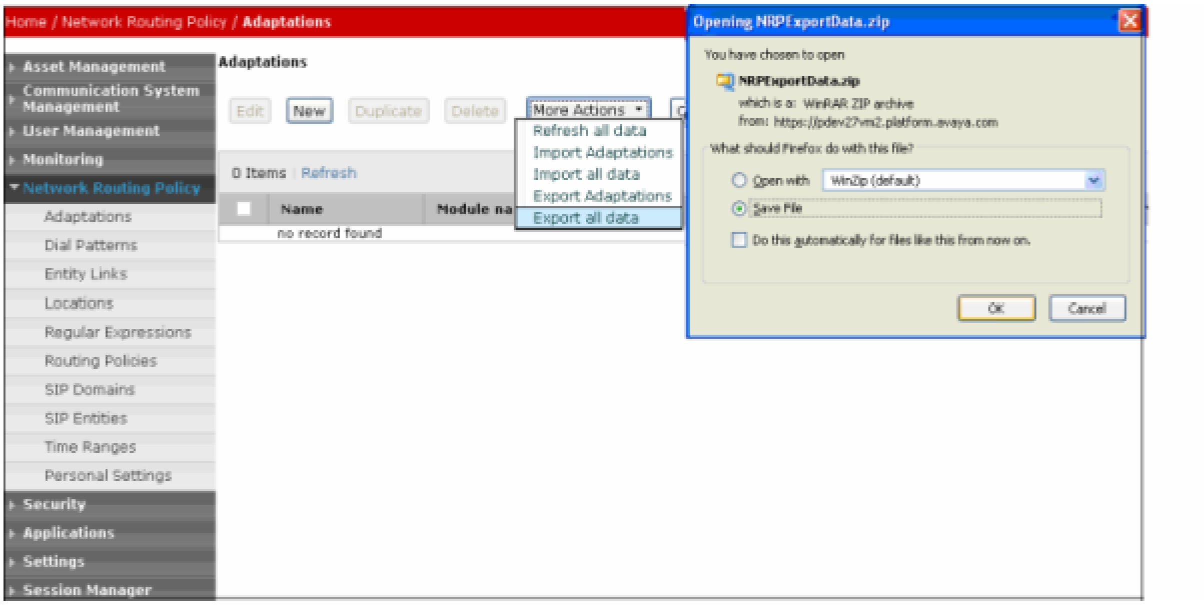
- Record the network parameters on System Manager 5.2.x.

About this task

Use this procedure to export the System Manager routing data from Release 5.2, 5.2 SP1, or 5.2 SP2 to System Manager Release 6.3.15.

Procedure

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



Opening NRPExportData.zip

You have chosen to open

NRPExportData.zip

which is a: WinRAR ZIP archive

from: https://pdev27vm2.platform.avaya.com

What should Firefox do with this file?

○ Open with WinZip (default)

● Save File

□ Do this automatically for files like this from now on.

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

Installing the System Manager OVA file

Procedure

Install the `SMGR-6.3.0.8.5682-e50-68.ova` file.

Related links

[Deploying the System Manager OVA file by using vSphere](#) on page 40

[Deploying the System Manager OVA file using vCenter](#) on page 46

Installing the System Manager Release 6.3.15 bin file

Before you begin

- Ensure that System Manager is running on Release 6.3.
- To reach the System Manager CLI, use one of the following methods:
    - Open vSphere Client and click on the **Console** tab or the 🖥 icon.
    - Start an SSH on System Manager.
- Log in to the System Manager virtual machine as admin.
- Download the `System_Manager_6.3.15_r5203972.bin` file from the Avaya Support website at http://support.avaya.com/ and copy the file to the `/home/admin` location on System Manager.

About this task

If you fail to install the Release 6.3.15 bin file for System Manager, the Virtualized Environment-specific functionality might be unavailable in System Manager.

Procedure

1. Create the System Manager virtual machine snapshot.

   Note:

   This activity might impact the service.

2. At the prompt, run the following command:

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

   The system displays the license information.

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

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

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

Next steps

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

      Note:

      Snapshots occupy the system memory and degrades the performance of the virtual application. Therefore, delete the snapshot after you verify the patch installation or the system upgrade.

    - If the patch installation fails, use the snapshot to restore the system to the original state.
2. Shut down the System Manager virtual machine.
3. Turn on the System Manager virtual machine.

System Manager takes about 15 minutes to start.

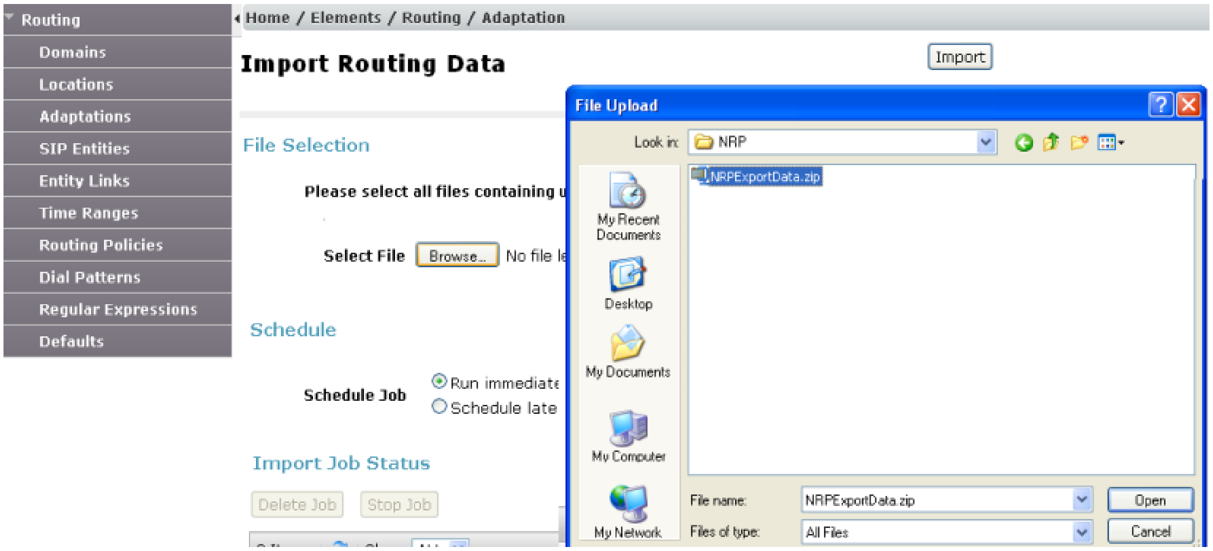
Importing the data to System Manager Release 6.3.15

Perform this procedure on System Manager 5.2.x to import the System Manager data from Release 5.2, 5.2 SP1, or 5.2 SP2 to System Manager Release 6.3.15.

Procedure

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

   The system displays the Import Routing Data page.
5. In the File Selection section, click Browse to open the `NRPExportData.zip` file.



6. To import the NRP data, click **Import**.
7. Verify that the NRP data is successfully imported to System Manager Release 6.3.15.
8. Create users, custom roles, and configuration information that you recorded from the System Manager web console of Release 5.2.x.

Chapter 5: Postupgrade verification

Verifying the functionality of System Manager

About this task

Note:

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

When you upgrade to System Manager Release 6.3.15 from release:

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

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

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

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

Procedure

1. Type `https://<fully qualified domain name of System Manager>/SMGR` on the web browser to log on to the System Manager web console of the upgraded system.
2. Click the settings icon (🔧), click **About**, and verify that the system displays the version number of System Manager with the highest build number for the release.
3. To verify if the system has generated any new call processing alarms during the System Manager upgrade, perform the following:

   a. Click **Services** > **Events**.

   b. In the left navigation pane, click **Events** > **Alarms**.

   c. On the Alarms page, in the **Alarms List** section, note alarms that the system generated.

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

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

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

Creating a data backup on a remote server

Procedure

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

     Important:

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

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

Creating a Snapshot restore

About this task

Important:

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

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

Procedure

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

SSO login to remote machine fails

For System Manager deployments that involve remote machines such as CS 1000 Servers and solutions based on the System Manager Single Sign On (SSO) client, the Web-based Single Sign On between System Manager and the remote machine fails.

During the data migration or IP-FQDN change, the system does not import the LDAP attribute that contains the SSO cookie domain value back to the directory. Therefore, the System Manager SSO login to the remote machine fails. Enable SSO after the data migration or the IP-FQDN change.

Related links

Reimporting the SSO cookie domain value on page 34

Reimporting the SSO cookie domain value

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.

2. In the left navigation pane, click **Security** > **Policies**.
3. In the section **Single Sign-on Cookie Domain** section, click **Edit**.
4. In the **Single Sign-on Cookie Domain** field, select an appropriate domain based on the FQDN of the servers that you deployed.
5. Click **Save**.

Chapter 6: Maintenance

Backup and restore System Manager data

Creating a data backup on a remote server

Procedure

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

     ❗ **Important:**

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

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

Creating a data backup on a local server

Procedure

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

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

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

Restoring a backup from a remote server

About this task

Note:

- Do not restore the backup data from VMware on System Platform.
- 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 **Remote**.
4. In the **Parameterized Restore** tab, perform one of the following:
   - Provide the name of the file that you must restore, the file transfer protocol, the remote server IP, remote server port, user name, and the password to access the remote computer in the respective fields.

     Note:

     The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.
   - 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. In the Backup List, view the list of the remote backups that are created by using the SFTP and SCP protocols.

If the location of a backup file is modified, in the **Parameterized Restore** tab, specify the correct location of the backup file in the **File Name** field. You can select only one file at a time.

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

Note:

- Do not restore the backup data from VMware on System Platform.
- 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 complete path of the file that you must restore.

   Note:

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

5. Click **Restore**. On the Restore Confirmation page, the system displays the following message:

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

6. Click **Continue**.

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

Result

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

Backup and Restore field descriptions

Use this page to view the details of backup files or the files you require to restore.

Name	Description
Operation	Specifies the type of operation. The values are: • Backup • Restore
File Name	• For the backup operation, specifies the name of the backup file. • For the restore operation, specifies the name of the file you want to restore.
Path	• For the backup operation, specifies the path of the backup file. • For the restore operation, specifies the path of the file you want to restore.
Status	Indicates the status of the backup or restore operation. The values are: • SUCCESS • FAILED • PLANNED • RUNNING
Status Description	Displays the error details of the backup or restore operation that has failed.
Operation Time	Specifies the time of the backup or restore operation.

Table continues…

Name	Description
Operation Type	Defines whether the backup or restore operation is local or remote.
User	Displays the user who performed the operation.

Button	Description
Backup	Opens the Backup page. Use this page to back up data on a specified local or remote location.
Restore	Opens the Restore page. Use this page to restore data to a specified local or remote location.

Common upgrade procedures

Deploying the System Manager OVA file by using vSphere

Before you begin

Install vSphere Client.

Procedure

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

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

The system displays the data store that you selected and the available space.

12. On the Network Mapping page, for each network that you specified in the OVA Template Details page, in the **Destination Network** column, select a host network from the list.

    For example, click VM Network 2.

13. Click **Next**.
14. Review the settings and click **Finish**.

    Wait until the system deploys the OVA file successfully.

15. To start the System Manager virtual machine, perform one of the following steps:

    - Right-click the virtual machine, and click **Power** > **Power On**.
    - On the **Inventory** menu, click **Virtual Machine** > **Power** > **Power On**.

    The system starts the System Manager virtual machine.

Next steps

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

  From the time you power on the system, the deployment process takes about 30–40 minutes to complete. Do not reboot the system until the configuration is complete. You can monitor the post deployment configuration from the `/var/log/Avaya/PostDeployLogs/post_install_sp.log` file.
- Verify the deployment of the System Manager OVA file.
- Install the `System_Manager_6.3.15_r5203972.bin` file.

Related links

[Deploying the System Manager OVA file using vCenter](#) on page 46

Configuring the network parameters from the vSphere console

Before you begin

- Deploy the System Manager virtual machine OVA file.
- Start the System Manager virtual machine.
- To reach the System Manager CLI, open vSphere Client and click the **Console** tab or the 🖥 icon.

About this task

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

Procedure

1. At the prompt, enter the following network parameters:

    - **IP**. The IP address of the System Manager virtual machine.

- **Netmask**. The subnetwork mask of the System Manager virtual machine.
- **Short Hostname**. The host name of the System Manager virtual machine. For example, smgrdev.

  Note:

  System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.
- **Domain name**. The domain name of the System Manager virtual machine. For example, platform.mydomain.com.
- **Default Gateway**. The IP address of the System Manager virtual machine gateway For example, 172.16.1.1.
- **DNS IP**. Enter one of the following:
  - DNS IP address of the primary System Manager virtual machine. For example, 172.16.1.2.
  - DNS IP addresses of primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,). For example, 172.16.1.2, 172.16.1.4.
- **Default Search List**. The search list of domain names. The field is optional.
- **NTP Server IP or FQDN**. The IP address or FQDN of the NTP server. This is an optional field. Separate the IP addresses with commas (,).
- **Time Zone**. From the lists that the system displays, select the name of the continent and the name of the country.

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

       Note:

       - The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.
       - VFQDN is a mandatory field.
       - Do not add VFQDN entries in the DNS configuration.
       - Do not add VFQDN in the `/etc/hosts` file on System Manager. Adding VFQDN in the `/etc/hosts` file might cause failures.

- In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.
- After the System Manager installation, you cannot change the VFQDN unless you reinstall System Manager.

4. Type the backup definition parameters for the System Manager virtual machine to schedule the remote backup during the System Manager installation. For information, see Backup Definition parameters.
5. To confirm the network parameters, type `Y`.

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

   From the time you power on the system, the deployment process takes about 30–40 minutes to complete. Do not reboot the system until the configuration is complete. You can monitor the post deployment configuration from the `/var/log/Avaya/PostDeployLogs/post_install_sp.log` file.
6. On the web browser, enter `https://FQDN/SMGR` to gain access to the System Manager web console.

   The system displays the System Manager web console.

Backup Definition parameters

Use the backup definition to schedule remote backup during the System Manager installation.

Note:

You can skip the configuration of the backup definition parameters to schedule the backup jobs later.

The backup time must be 6 hours later than the System Manager installation time.

If you set the **Backup Start Month** field to 5, **Backup Start Day** field to 24, and **Repeat Type** field to Weekly, the system executes the backup job every Friday if May 24th is a Friday.

Name	Description
Schedule Backup?	• Yes: To schedule the backup jobs during the System Manager installation. • No: To schedule the backup jobs later. **Note:** If you select No, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server.

Table continues…

Name	Description
	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 CLI.
Backup Server Login Password	The password to log in to the backup server through CLI.
Re-Type Backup Server Login Password	The password that you re-enter to log in to the backup server through CLI.
Backup Directory Location	The location on the remote backup server.
Repeat Type	The type of the backup. The possible values are: • `Hourly` • `Daily` • `Weekly` • `Monthly`
Backup Frequency	The frequency of the backup taken for the selected backup type.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be 6 hours later than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

Installing the System Manager Release 6.3.15 bin file

Before you begin

- Ensure that System Manager is running on Release 6.3.
- To reach the System Manager CLI, use one of the following methods:
    - Open vSphere Client and click on the **Console** tab or the 🖥 icon.
    - Start an SSH on System Manager.
- Log in to the System Manager virtual machine as admin.
- Download the `System_Manager_6.3.15_r5203972.bin` file from the Avaya Support website at http://support.avaya.com/ and copy the file to the `/home/admin` location on System Manager.

About this task

If you fail to install the Release 6.3.15 bin file for System Manager, the Virtualized Environment-specific functionality might be unavailable in System Manager.

Procedure

1. Create the System Manager virtual machine snapshot.

    Note:

    This activity might impact the service.

2. At the prompt, run the following command:

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

    The system displays the license information.

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

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

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

Next steps

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

        Note:

        Snapshots occupy the system memory and degrades the performance of the virtual application. Therefore, delete the snapshot after you verify the patch installation or the system upgrade.

    - If the patch installation fails, use the snapshot to restore the system to the original state.
2. Shut down the System Manager virtual machine.
3. Turn on the System Manager virtual machine.

System Manager takes about 15 minutes to start.

Deploying the System Manager OVA file using vCenter

Before you begin

- Install vSphere client.
- Install vCenter server and connect vSphere Client to vCenter.

Procedure

1. Start vSphere Client.
2. Enter the IP address and the user credentials for the vCenter server.

   Ignore any security warning that the system displays.
3. On vSphere Client, click **File** > **Deploy OVF Template**.
4. In the Deploy OVF Template dialog box, perform one of the following steps:
   - In the **Deploy from a file or URL** field, enter the path to the `.ova` file.
   - Click **Browse** and navigate to the `.ova` file from the local computer, network share, CD-ROM, or DVD.
5. On the OVF Template Details page, verify the details, and click **Next**.
6. On the End User License Agreement page, click **Accept**.
7. Click **Next**.
8. **(Optional)** On the Name and Location page, in the **Name** field, change the name for the virtual machine.
9. In the **Inventory Location** area, select the datacenter and click **Next**.
10. If the cluster exists, select the cluster and click **Next**.
11. Select the specific host within the cluster and click **Next**.
12. On the Storage page, select the required data store and click **Next**.
13. On the Disk Format page, click **Thick Provision Lazy Zeroed**.

    The system displays the data store that you selected and the available space.
14. On the Network Mapping page, for each network that you specified in the OVA Template Details page, in the **Destination Network** column, select a host network from the list.

    For example, click VM Network 2.
15. On the Properties page:
    a. Configure the following network parameters:
       - **IP**. The IP address of the System Manager virtual machine.
       - **Netmask**. The Subnet mask of the System Manager virtual machine.

- **Default Gateway**. The IP address of your default gateway.
- **DNS IP**. The IP address of your DNS server. Separate IP addresses with commas (,).
- **Short Hostname**. The hostname of the System Manager virtual machine. For example, smgrdev.

  Note:

  System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.

- **Domain Name**. The domain name of the System Manager virtual machine. For example, platform.mydomain.com.
- **Default Search List**. The search list of domain names. Separate IP addresses with commas (,).
- **NTP Server IP or FQDN**. The IP address or FQDN of the NTP server. Separate IP addresses or FQDNs with commas (,).
- **Time Zone**. The time zone. Select a time zone from the list.
- **Virtual FQDN** for the System Manager virtual machine.
  - Virtual short hostname. For example, grsmgr.
  - Virtual domain. For example, dev.com.
    - The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.
    - VFQDN is a mandatory field.
    - Do not add VFQDN entries in the DNS configuration.
    - Do not add VFQDN in the `/etc/hosts` file on System Manager. Adding VFQDN in the `/etc/hosts` file might cause failures.
    - In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.
    - After the System Manager installation, you cannot change the VFQDN unless you reinstall System Manager.

b. Configure the following SNMPv3 parameters:

- **User Name Prefix**. For example, global.
- **User Authentication Protocol Password**. For example, globalpass.
- **User Privacy Protocol Password**. For example, globalpass.

c. **(Optional)** Select the **Schedule SMGR backup** check box to schedule the System Manager backup and configure the backup definition input parameters. For information, see Backup Definition parameters.

> **Note:**
>
> - If you do not provide the details in the mandatory fields, you cannot power on the virtual machine even if the deployment is successful.
> - During the startup, the system validates the inputs that you provide. If the inputs are invalid, the system prompts you to provide the inputs again on the console of the virtual machine.
> - The system does not validate the backup definition data that you provide. If the data is invalid, the system does not schedule the backup.

16. Click **Next**.
17. Review the settings and click **Finish**.

    Wait until the system deploys the OVA file successfully.

    From the time you power on the system, the deployment process takes about 30–40 minutes to complete. Do not reboot the system until the configuration is complete. You can monitor the post deployment configuration from the `/var/log/Avaya/PostDeployLogs/post_install_sp.log` file.
18. To start the System Manager virtual machine, perform one of the following steps:
    - Right-click the virtual machine, and click **Power** > **Power On**.
    - On the **Inventory** menu, click **Virtual Machine** > **Power** > **Power On**.

    The system starts the System Manager virtual machine.
19. Click the **Console** tab and verify that the system startup is successful.

Next steps

- Verify the deployment of the System Manager OVA file.
- Install the `System_Manager_6.3.15_r5203972.bin` file.

Related links

Deploying the System Manager OVA file by using vSphere on page 40

Changing the IP address, FQDN, DNS, Gateway, or Netmask address from CLI

Before you begin

- To reach the System Manager CLI, use one of the following methods:
  - Open vSphere Client and click on the **Console** tab or the 🖥 icon.
  - Start an SSH on System Manager.
- Log in to the System Manager virtual machine as admin.
- Create the System Manager virtual machine snapshot.

Note:

Delete the snapshot after the System Manager operation is complete.

About this task

Important:

- After the System Manager installation, you cannot change the VFQDN unless you reinstall System Manager.
- Do not change the network settings from vSphere Client when the virtual machine is in the power off mode.
- The FQDN value must be unique and different from the virtual FQDN value of System Manager.

Procedure

Type `changeIPFQDN -IP <IP address> -FQDN <FQDN> -GATEWAY <Gateway address> -NETMASK <Netmask address> -DNS <DNS address> -SEARCH <search list of domain names>`.

For information, see changeIPFQDN command.

Next steps

Get new licenses from PLDS containing the new host ID and install the new licenses.

After you change the IP address of System Manager, the system generates a new host ID for WebLM server that System Manager hosts. Therefore, all previously installed licenses become invalid.

For instructions to install a license file, see Managing Licenses in *Administering Avaya Aura® System Manager*.

Related links

changeIPFQDN command on page 49
System Manager command line interface operations on page 51

changeIPFQDN command

Use the **changeIPFQDN** command to change the IP address, FQDN, DNS address, Gateway, Netmask address for System Manager, and the search list for the DNS address.

Syntax

```
changeIPFQDN -IP < >  -FQDN < > -GATEWAY < >-NETMASK < > -DNS < > -SEARCH < >
```

#	Option	Description	Usage
1	IP	The new IP address of System Manager.	**changeIPFQDN -IP 10.11.12.13**
2	FQDN	The new FQDN of System Manager.	**changeIPFQDN -FQDN a.mydomain.smgr.com**

Table continues…

#	Option	Description	Usage
3	GATEWAY	The new Gateway address of System Manager.	**`changeIPFQDN -GATEWAY 10.11.1.1`**
4	NETMASK	The new netmask address of System Manager.	**`changeIPFQDN -NETMASK 255.255.203.0`**

5	DNS	The new DNS address of System Manager.
		You an provide multiple DNS addresses. Separate each address by a comma.
			`changeIPFQDN -DNS 10.11.1.2`
			`changeIPFQDN -DNS 10.11.12.5,10.11.12.3`

6	SEARCH	The new search list of domain names.	**`changeIPFQDN -SEARCH smgr.com`**

Example

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

```
changeIPFQDN -IP 10.11.y.z -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1 -NETMASK
255.255.255.0 -DNS 10.11.1.2 -SEARCH platform.avaya.com
```

```
changeIPFQDN -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1
```

```
changeIPFQDN -IP 10.11.y.z
```

Installing the System Manager service pack or patch from CLI

Before you begin

- To reach the System Manager CLI, use one of the following methods:
  - Open vSphere Client and click on the **Console** tab or the 🖥 icon.
  - Start an SSH on System Manager.
- Log in to the System Manager virtual machine as admin.

Procedure

Enter `SMGRPatchdeploy <absolute path to the service pack or patch for System Manager>`.

If you do not enter the name of the patch or the service pack, the console displays menu items. Provide the absolute path to the patch or the service pack that you want to install for System Manager.

Related links

System Manager command line interface operations on page 51

System Manager command line interface operations

#	Command	Parameters	Description	Usage
1	`changeIPFQDN`	• `-IP <new IP address for System Manager>` • `-FQDN <new fully qualified domain name for System Manager>` • `-GATEWAY <new Gateway address for System Manager>` • `-NETMASK <new netmask address for System Manage>` • `-DNS <new DNS address for System Manager>` • `-SEARCH <new search list for DNS address>`	Updates the existing IP address, FQDN, Gateway, Netmask, DNS, and the search list with the new value.	• `changeIPFQDN -IP <new IP address>` • `changeIPFQDN -FQDN <new fully qualified domain name>` • `changeIPFQDN -IP <new IP address> -GATEWAY <new Gateway address for System Manager> -SEARCH <new search list for DNS address>`
2	`upgradeSMGR`	`<absolute path to the dmutility.bin> -m -v -V -H`	Upgrades System Manager using the data migration utility.	`upgradeSMGR dmutility *.bin -m -v -V -H`
3	`SMGRPatchdeploy`	`<absolute path to the System Manager service pack or the software patch>`	Installs the software patch or the service pack for System Manager.	`SMGRPatchdeploy <absolute path to /home/admin/<SMGRservicepackName>` **Note:** Copy the System Manager service pack or patches that you must install to `/home/admin/`.
4	`updateASG`	`<absolute path to the ASG XML file>`	Updates the ASG XML file.	`updateASG <absolute path to the ASG XML file>`

5	`configureTimeZone`	`Time zone that you select`	Configures the time zone with the value that you select.	`configureTimeZone`
				`Select a time zone. For example, America/Denver`

Table continues…

#	Command	Parameters	Description	Usage
5	**`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 (,).

Appendix A: Best Practices for VMware 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 at http://www.vmware.com/files/pdf/techpaper/VMW-Tuning-Latency-Sensitive-Workloads.pdf.

The following sections describe the recommended BIOS settings for:

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

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.

- 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.

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.

Dell PowerEdge Server

When the Dell server starts, press F2 to display the system setup options.

- Set the Power Management Mode to **Maximum Performance**.
- Set the CPU Power and Performance Management Mode to **Maximum Performance**.
- In Processor Settings, set:
  - **Turbo Mode** to **enable**.
  - **C States** to **disabled**.

HP ProLiant Servers

The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to **Static High Mode**.
- Disable **Processor C-State Support**.
- Disable **Processor C1E Support**.
- Disable **QPI Power Management**.
- Enable **Intel Turbo Boost**.

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.

For more information, see *Timekeeping best practices for Linux guests* at http://kb.vmware.com/kb/1006427. The article presents best practices for Linux timekeeping to achieve best timekeeping results. The article includes:

- specifics on the particular kernel command line options to use for the Linux operating system of interest.
- recommended settings and usage for NTP time sync, configuration of VMware Tools time synchronization, and Virtual Hardware Clock configuration.

Configuring the NTP time

Procedure

1. Select the ESXi server and click the **Configuration** tab.
2. In the left navigation pane, click **Software** > **Time Configuration**.
3. At the upper-right side of the Time Configuration page, click **Properties...**.
4. On the Time Configuration dialog box, in the NTP Configuration area, perform the following:
    a. Select the **NTP Client Enabled** check box.
    b. Click **Options**.
5. On the NTP Daemon (ntpd) Options dialog box, perform the following:
    a. In the left navigation pane, click **NTP Settings**.
    b. Click **Add**.
    c. On the Add NTP Server dialog box, in the **NTP Server** area, enter the IP address of the NTP server.
    d. Click **OK**.

The date and time of the System Manager virtual machine synchronizes with the NTP server.

6. Select the **Restart NTP service to apply changes** check box.
7. Click **OK**.

   The Time Configuration page displays the date and time, NTP Servers, and the status of the NTP client.

VMware networking best practices

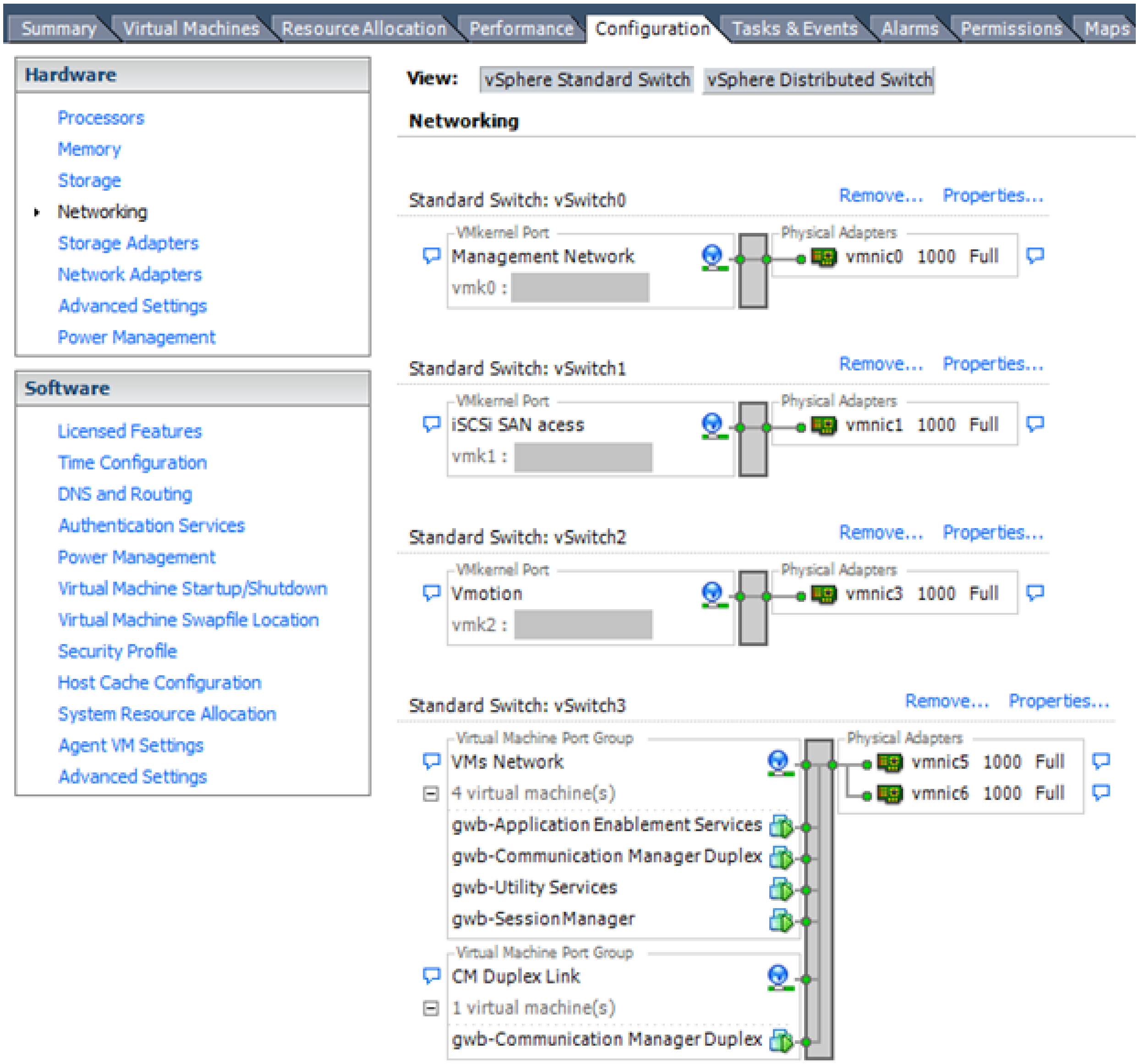
You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

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 VMkernal vNICs to be the same IP Maximum Transmission Unit (MTU).

Networking Avaya applications on VMware ESXi – Example 1



Standard Switch: vSwitch0

VMkernel Port: Management Network, vmk0 : [redacted]
Physical Adapters: vmnic0 1000 Full

Standard Switch: vSwitch1

VMkernel Port: iSCSi SAN acess, vmk1 : [redacted]
Physical Adapters: vmnic1 1000 Full

Standard Switch: vSwitch2

VMkernel Port: Vmotion, vmk2 : [redacted]
Physical Adapters: vmnic3 1000 Full

Standard Switch: vSwitch3

Virtual Machine Port Group: VMs Network
4 virtual machine(s)
gwb-Application Enablement Services
gwb-Communication Manager Duplex
gwb-Utility Services
gwb-SessionManager

Physical Adapters:
vmnic5 1000 Full
vmnic6 1000 Full

Virtual Machine Port Group: CM Duplex Link
1 virtual machine(s)
gwb-Communication Manager Duplex

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

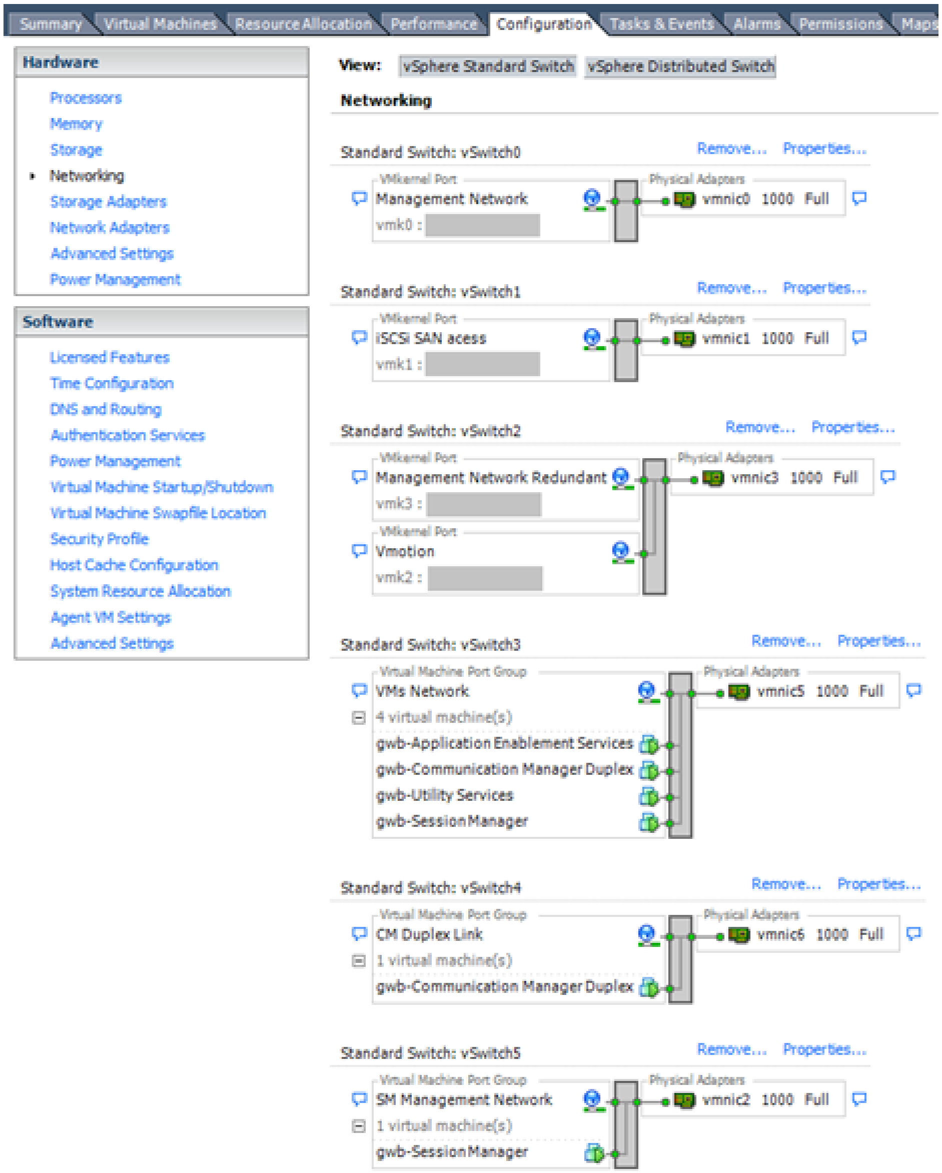
- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides additional bandwidth for the Virtual Machines Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.
- Communication Manager Duplex link: Communication Manager software duplication must be separated from all other network traffic. Example 1 displays one method of separating Communication Manager Duplex with a port group combined with a VLAN. The

Communication Manager software duplication link must meet specific network requirements. for more information, see Avaya PSN003556u at PSN003556u. The following are the minimum requirements of the Communication Manager software duplex connectivity:

- The total capacity must be 1 Gbps or greater. Reserve 50 Mbps of bandwidth for duplication data.
- The round-trip delay must be 8 ms or less.
- The round-trip packet loss must be 0.1% or less.
- Both servers duplication ports must be on the same IP subnet.
- You must disable duplication link encryption for busy-hour call rates that result in greater than 40% CPU occupancy. You can view the CPU occupancy using the `list measurements occupancy` command and looking at the results under the **Static + CPU occupancy** heading.
- The system must maintain CPU occupancy on the active server (Static + CPU) at less than 65% to provide memory refresh from the active to standby server.

- Session Manager vNIC mapping: Session Manager OVA defines four separate virtual NICs within the VM. However, Example 1 shows all interfaces networked through a single virtual machine network, which is supported. If the Session Manager Management and Session Manager Asset networks are separated by subnets, you can create a VLAN for the appropriate network.
- Virtual networking: The network connectivity between virtual machines that connect to the same vSwitch is entirely virtual. In Example 2, the virtual machine network of vSwitch3 can communicate without entering the physical network. Virtual networks benefit from faster communication speeds and lower management overhead.

Networking Avaya applications on VMware ESXi – Example 2



Networking

Standard Switch: vSwitch0
VMkernel Port: Management Network, vmk0 : [redacted]
Physical Adapters: vmnic0 1000 Full

Standard Switch: vSwitch1
VMkernel Port: iSCSI SAN acess, vmk1 : [redacted]
Physical Adapters: vmnic1 1000 Full

Standard Switch: vSwitch2
VMkernel Port: Management Network Redundant, vmk3 : [redacted]
VMkernel Port: Vmotion, vmk2 : [redacted]
Physical Adapters: vmnic3 1000 Full

Standard Switch: vSwitch3
Virtual Machine Port Group: VMs Network
4 virtual machine(s)
gwb-Application Enablement Services
gwb-Communication Manager Duplex
gwb-Utility Services
gwb-Session Manager
Physical Adapters: vmnic5 1000 Full

Standard Switch: vSwitch4
Virtual Machine Port Group: CM Duplex Link
1 virtual machine(s)
gwb-Communication Manager Duplex
Physical Adapters: vmnic6 1000 Full

Standard Switch: vSwitch5
Virtual Machine Port Group: SM Management Network
1 virtual machine(s)
gwb-Session Manager
Physical Adapters: vmnic2 1000 Full

This configuration shows a complex situation using multiple physical network interface cards. The key differences between Example 1 and Example 2 are:

- VMware Management Network redundancy: Example 2 includes a second VMkernel Port at vSwitch2 to handle VMware Management Network traffic. In the event of a failure of vmnic0, VMware Management Network operations can continue on this redundant management network.
- Removal of Teaming for Virtual Machines Network: Example 2 removes the teamed physical NICs on vSwitch3. vSwitch3 was providing more bandwidth and tolerance of a single NIC failure instead of reallocating this NIC to other workloads.
- Communication Manager Duplex Link: vSwitch4 is dedicated to Communication Manager Software Duplication. The physical NIC given to vSwitch4 is on a separate physical network that follows the requirements described in PSN003556u at PSN003556u.

- Session Manager Management Network: Example 2 shows the Session Manager Management network separated onto its own vSwitch. The vSwitch has a dedicated physical NIC that physically segregates the Session Manager Management network from other network traffic.

References

Title	Link
Product Support Notice PSN003556u	https://downloads.avaya.com/css/P8/documents/100154621
Performance Best Practices for VMware vSphere™ 5.0	Performance Best Practices for VMware vSphere™ 5.0
Performance Best Practices for VMware vSphere™ 5.5	http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf
VMware vSphere 5.0 Basics	VMware vSphere Basics - ESXi 5.0
VMware vSphere 5.5 Documentation	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html
VMware Documentation Sets	https://www.vmware.com/support/pubs/

Storage

When you deploy Avaya Aura® System Manager in Virtualized Environment, observe the following set of storage recommendations:

- Always deploy System Manager with a thickly provisioned disk.
- For best performance, use System Manager only on disks local to the ESXi Host, or Storage Area Network (SAN) storage devices. Do not store System Manager on an NFS storage system.

Thin vs. thick deployments

When creating a virtual disk file, VMware ESXi uses a thick type of virtual disk by default. The thick disk pre-allocates all of the space specified during the creation of the disk. For example, if you create a 10 megabyte disk, all 10 megabytes are pre-allocated for that virtual disk.

In contrast, a thin virtual disk does not pre-allocate all of the space. Blocks in the VMDK file are not allocated and backed by physical storage until they are written during the normal course of operation. A read to an unallocated block returns zeroes, but the block is not backed with physical storage until it is written. Consider the following when implementing thin provisioning in your VMware environment:

- Thin provisioned disks can grow to the full size specified at the time of virtual disk creation, but do not shrink. Once the blocks have been allocated, they cannot be un-allocated.

- By implementing thin provisioned disks, you are able to over-allocate storage. If storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked.
- If a guest operating system needs to make use of a virtual disk, the guest operating system must first partition and format the disk to a file system it can recognize. Depending on the type of format selected within the guest operating system, the format may cause the thin provisioned disk to grow to full size. For example, if you present a thin provisioned disk to a Microsoft Windows operating system and format the disk, unless you explicitly select the Quick Format option, the Microsoft Windows format tool writes information to all of the sectors on the disk, which in turn inflates the thin provisioned disk to full size.

Thin provisioned disks can over-allocate storage. If the storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked. You can use thin provisioned disks, but you must use strict control and monitoring to maintain adequate performance and ensure that storage is not completely consumed. If operational procedures are in place to mitigate the risk of performance and storage depletion, then thin disks are a viable option.

Best Practices for VMware features

VMware Snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. You can create a snapshot before upgrading or installing a patch.

The best time to take a snapshot is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

⚠ **Caution:**

Snapshot operations can adversely affect service. Before performing a snapshot operation, you must stop the application that is running on the virtual machine or place the application out-of-service. When the snapshot operation is complete, start or bring the application back into service.

Snapshots can:

- Consume large amounts of data resources.
- Increase CPU loads on the host.
- Affect performance.
- Affect service.

To prevent adverse behaviors, consider the following recommendations when using the Snapshot feature:

- *Do not* rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- *Do not run a virtual machine off of 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, a warning is displayed in the UI.

Related resources

Title	Link
Best practices for virtual machine snapshots in the VMware environment	Best Practices for virtual machine snapshots in the VMware environment
Understanding virtual machine snapshots in VMware ESXi and ESX	Understanding virtual machine snapshots in VMware ESXi and ESX
Working with snapshots	Working with snapshots
Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots	Send alarms when virtual machines are running from snapshots
Consolidating snapshots in vSphere 5.x	Consolidating snapshots in vSphere 5.x

VMware Cloning

System Manager does not support VMware Cloning.

VMware High Availability

InVirtualized Environment, use the VMware High Availability (HA) method to recover System Manager in the event of ESXi Host failure. For more information, see the High Availability documentation for VMware.

When you use VMware HA with System Manager, the communication between System Manager and Avaya Aura® Communication Manager fails. The virtual machine then starts again on a standby server, and the system starts running.

VMware vMotion

VMware uses the vMotion technology to migrate a running virtual machine from one physical server to another physical server without incurring downtime. The migration process, also known as a hot migration, migrates running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

With vMotion, you can:

- Schedule migration to occur at predetermined times and without the presence of an administrator.
- Perform hardware maintenance without scheduled downtime.
- Migrate virtual machines away from failing or underperforming servers.

Before using vMotion, you must:

- Ensure that each host that migrates virtual machines to or from the host uses a licensed vMotion application and the vMotion is enabled.
- Ensure that you have identical vSwitches. You must enable vMotion on these vSwitches.
- Ensure that the Port Groups are identical for vMotion.
- Use a dedicated NIC to ensure the best performance.

Note:

If System Manager WebLM is being used as a master WebLM server in an enterprise licensing deployment for a product, after migration of virtual machine to another physical server by using vMotion, validate connectivity with added local WebLM servers. This is to ensure that the master WebLM server can communicate with local WebLM servers.

Glossary

AFS Authentication File System. AFS is an Avaya Web system that allows you to create Authentication Files for secure Avaya Global Services logins for supported non-Communication Manager Systems.

Application A software solution development by Avaya that includes a guest operating system.

Avaya Appliance A physical server sold by Avaya running a VMware hypervisor that has several virtual machines, each with its virtualized applications. The servers can be staged with the operating system and application software already installed. Some of the servers are sold as just the server with DVD or software downloads.

Blade A blade server is a stripped-down server computer with a modular design optimized to minimize the use of physical space and energy. Although many components are removed from blade servers to save space, minimize power consumption and other considerations, the blade still has all of the functional components to be considered a computer.

ESXi A virtualization layer that runs directly on the server hardware. Also known as a *bare-metal hypervisor.* Provides processor, memory, storage, and networking resources on multiple virtual machines.

Hypervisor A hypervisor is also known as a Virtual Machine Manager (VMM). A hypervisor is a hardware virtualization technique which runs multiple operating systems on the same shared physical server.

MAC Media Access Control address. A unique identifier assigned to network interfaces for communication on the physical network segment.

OVA Open Virtualization Appliance. An OVA contains the virtual machine description, disk images, and a manifest zipped into a single file. The OVA follows the Distributed Management Task Force (DMTF) specification.

PLDS Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.

Reservation A reservation specifies the guaranteed minimum required amounts of CPU or memory for a virtual machine.

RFA

Remote Feature Activation. RFA is an Avaya Web system that you use to create Avaya License Files. These files are used to activate software including features, capacities, releases, and offer categories. RFA also creates Authentication Files for secure Avaya Global Services logins for Communication Manager Systems.

SAN

Storage Area Network. A SAN is a dedicated network that provides access to consolidated data storage. SANs are primarily used to make storage devices, such as disk arrays, accessible to servers so that the devices appear as locally attached devices to the operating system.

Snapshot

The state of a virtual appliance configuration at a particular point in time. Creating a snapshot can affect service. Some Avaya virtual appliances have limitations and others have specific instructions for creating snapshots.

Storage vMotion

A VMware feature that migrates virtual machine disk files from one data storage location to another with limited impact to end users.

vCenter Server

An administrative interface from VMware for the entire virtual infrastructure or data center, including VMs, ESXi hosts, deployment profiles, distributed virtual networking, and hardware monitoring.

virtual appliance

A virtual appliance is a single software application bundled with an operating system.

VM

Virtual Machine. Replica of a physical server from an operational perspective. A VM is a software implementation of a machine (for example, a computer) that executes programs similar to a physical machine.

vMotion

A VMware feature that migrates a running virtual machine from one physical server to another with minimal downtime or impact to end users. vMotion cannot be used to move virtual machines from one data center to another.

VMware HA

VMware High Availability. A VMware feature for supporting virtual application failover by migrating the application from one ESXi host to another. Since the entire host fails over, several applications or virtual machines can be involved. The failover is a reboot recovery level which can take several minutes.

vSphere Client

The vSphere Client is a downloadable interface for administering vCenter Server and ESXi.

Index