Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment

Release 6.3.1
165879
Issue 1
July 2014

Contents

Chapter 1: Introduction 4
- Purpose 4
- Intended audience 4
- Related resources 4
  - Documentation 4
  - Training 6
  - Viewing Avaya Mentor videos 6
- Support 7

Chapter 2: Avaya Aura® Virtualized Environment overview 8
- Topology 9
- Components 10
  - Avaya components 10
  - VMware components 11
  - Third-party components 12

Chapter 3: Deployment process 13

Chapter 4: Planning and preconfiguration 14
- Planning checklist 14
  - Software requirements 14
  - Key customer configuration information 15
  - Configuration tools and utilities 15
- Downloading the Messaging OVA 16
  - Registering for PLDS 16
  - Downloading software from PLDS 16

Chapter 5: Initial setup and connectivity 18
- Deployment guidelines 18
- Hardware requirements 18
  - Server hardware and resources 18
  - Messaging virtual machine resource requirements 19
- Software installation checklist 20
  - Deploying the Messaging OVA 21
  - Editing the virtual machine resources 22
  - Starting the Messaging virtual machine 23
  - Administering network parameters 23
- WebLM 24

Chapter 6: Configuration 25
- Configuration checklist 25
- Configuring the virtual machine automatic startup settings 25
- Configuring the network settings 26
- Network Configuration field descriptions 26

Setting the time zone 27
Setting up the network time protocol 27
Service pack installation 28
Messaging service packs 28
Downloading service packs 28
Installing a service pack 29
Removing a service pack 31
Chapter 7: Initial administration 34
Initial administration checklist 34
Account management 34
Authentication file management 36
License management 39
Routine maintenance 40
Application backup and restore 40
Stopping Messaging 43
Starting Messaging 44
Shutting down the server 44
Transferring files using WinSCP 45
Chapter 8: Optimization and scalability 46
BIOS 46
Intel Virtualization Technology 46
Dell PowerEdge Server 47
HP ProLiant Servers 47
VMware Tools 47
Timekeeping 48
VMware networking best practices 49
Thin vs. thick deployments 52
Appendix A: Upgrading Messaging 53
Appendix B: Migration 54
Overview 54
Migration roadmap and limitations 54
Migrating Messaging to Virtualized Environment 55
Backing up data from the old system 55
Restoring data on the new system 56
Glossary 58

Chapter 1: Introduction

Purpose

This document provides procedures for deploying the Avaya Aura® Messaging virtual application in the Avaya Aura® Virtualized Environment.

The procedures relate to installation, configuration, initial administration, troubleshooting, and basic maintenance of the application.

Intended audience

This document is intended for people who install and configure a verified reference configuration at a customer site.

Related resources

Documentation

You can download the documents you need from the Avaya Support website at http://support.avaya.com. In addition to the documentation listed here, you can download a zip file that is a compilation of the Avaya Aura® Messaging documentation library. You can install this library on a computer or on your corporate network.

The Avaya Support website also includes the latest information about product compatibility, ports, and Avaya Aura® Messaging releases.

Security

Title	Description	Audience
Avaya Aura® Messaging Security Design	Discusses security issues to consider when designing a corporate security strategy. Topics include network security, toll fraud,	Solution architects, deployment engineers, and administrators

Title	Description	Audience
	and recommendations for maintaining a secure system.	

VMware configurations

Title	Description	Audience
Avaya Aura® Messaging VMware® in the Virtualized Environment Reference Configuration	Describes the design, capacities, interoperability, and limitations of systems configured for a virtualized environment.	Sales and deployment engineers, solution architects, and support personnel
Avaya Aura® Virtualized Environment Solution Description	Describes this market solution focusing on the functional view of the solution architecture.	Sales and deployment engineers, solution architects, and support personnel

Administration

Title	Description	Audience
Administering Avaya Aura® Messaging	Explains how to use the System Management Interface (SMI) to configure your system, use reports and diagnostic tools, manage software and users, and perform routine maintenance tasks. The content is available in two formats: HTML and PDF.	Administrators
Job aid for Administering Avaya Aura® Messaging	Includes routine administration tasks. This job aid is a subset of the administration guide.	Administrators
Avaya Aura® Messaging Alarms and Events	Describes system alarms, events, and repair procedures.	Administrators and support personnel

User functions

Title	Description	Audience
Using Avaya Aura® Messaging	Explains how to set up and use User Preferences and the Messaging toolbar in your email client. The content is available in two formats: HTML and PDF.	Users
Using Avaya Aura® Messaging Job Aid	Includes the most common user tasks. This job aid is a subset of the user guide.	Users and support personnel
Avaya Aura® Messaging Quick Reference (Aria)	Describes how to use the Aria telephone user interface.	Users

Title	Description	Audience
Avaya Aura® Messaging Quick Reference (Audix®)	Describes how to use the Audix® telephone user interface.	Users
Avaya Aura® Messaging Quick Reference (CallPilot®)	Describes how to use the CallPilot telephone user interface.	Users

Training

You can get the following Messaging courses at https://www.avaya-learning.com. Enter the course code in the **Search** field and click **Go** to search for the course.

The course titles might differ from the titles shown.

Course code	Course title
2U00230W	Avaya UC Messaging — Overview
2U00231W	Avaya UC Messaging — Heritage
2U00232W	Avaya UC Messaging — Avaya Aura® Messaging
2U00233O	Selling Avaya UC Messaging Learning Bytes
3U00141W	Designing UC Messaging — Avaya Aura® Messaging
5U00140E	Avaya Aura® Messaging Implementation and Support
5U00141E	Avaya Aura® Messaging Administration
ATI01674VEN	Avaya Aura® Messaging — Caller Applications

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.

Chapter 2: Avaya Aura® Virtualized Environment overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with the virtualized server architecture of VMware. Virtualized Environment provides the following benefits:

- Simplifies IT management using common software administration and maintenance.
- Requires fewer servers and racks, which reduces the footprint.
- Lowers cooling requirements, which reduces power consumption.
- Enables cost savings on capital equipment.
- Lowers operational expenses.
- Uses standard operating procedures for both Avaya and non-Avaya products.
- Enables deployment of Avaya products in a virtualized environment on customer-specified servers and hardware.
- Accommodates business scalability and rapid response to changing business needs.

For customers who have a VMware IT infrastructure, Avaya Aura® Virtualized Environment provides an opportunity to deploy Messaging using their own VMware infrastructure.

The Virtualized Environment capability is only for VMware and is not intended to include any other industry hypervisor.

Note:

The following terms are often used interchangeably in the document:

- Server and host
- Reservations and configuration values

Customer deployment

vCenter Server and vSphere Client manage the deployment into the blade, cluster, and server.

The customer must provide the servers and the VMware infrastructure including the VMware licenses.

Software delivery

The software is delivered as prepackaged Open Virtualization Appliance (OVA) files with the following components:

- The application software and operating system

- Preinstalled VMware tools
- Preset configuration details for:
  - RAM and CPU reservations and storage requirements
  - Network Interface Card (NIC)

Patches and updates

A minimum patch level is required for each supported application. For more information, see the compatibility matrix tool at http://support.avaya.com/CompatibilityMatrix/Index.aspx.

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.

Performance and capacities

The OVA file is built with configuration values that optimize performance and follow recommended best practices. You must change the preconfigured settings in the OVA.

For more information about supported resource requirements, see Messaging virtual machine resource requirements on page 19.

Best Practices for VMware performance and features

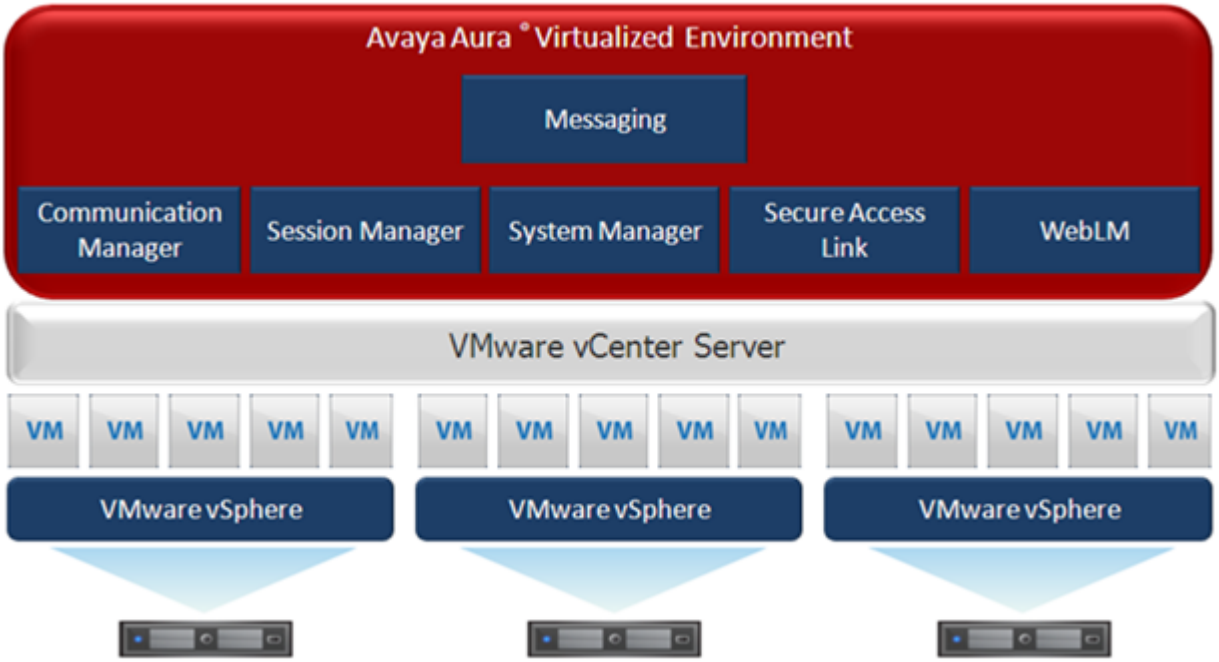
For more information about Avaya Aura® Virtualized Environment, see *Avaya Aura® Virtualized Environment Solution Description*.

Important:

Do not use VMware Snapshots because Snapshot operations can adversely affect Messaging service.

Topology

The following diagram shows the high-level topology for deploying Messaging in Virtualized Environment.



The VMware virtualization platform, VMware vSphere, supports the virtual machines. Each Avaya Aura® application, including Messaging, is installed as a separate virtual machine. You can install Messaging in one or more virtual machines depending on capacity requirement. The VMware vCenter Server management system manages the applications as virtual machines and provides management and implementation features in addition to the standard System Manager features.

Components

Avaya components

Component	Version	Platform	Description
Avaya Aura® components			
Avaya Aura® Communication Manager	6.3 6.3.2	Virtualized Environment	The IP telephony foundation on which Avaya delivers intelligent communications to large and small enterprises.
Avaya Aura® Messaging	6.3.1	Virtualized Environment	A part of the Avaya Aura® architecture, but Messaging can also be used in other environments
Avaya Aura® Session Manager	6.3.2 6.3.4	Virtualized Environment	A SIP routing and integration tool that integrates SIP entities across the enterprise network. You can view and manage each location, branch, and application in totality, not as separate units within the enterprise.

Component	Version	Platform	Description
Avaya Aura® System Manager	6.3.2 6.3.4 6.3.8	Virtualized Environment	A product that takes a solution-level approach to network administration. System Manager centralizes provisioning, maintenance, and troubleshooting to simplify and reduce management complexity and solution servicing. System Manager provides a common management framework that reduces the complexity of operations for distributed multisite networks with multiple control points inherent in SIP.
Other Avaya components			
Avaya Voice Message Form	6.3	Microsoft Exchange Server	A component that provides a toolbar for Microsoft Office Outlook and Exchange Server. The tool supports playback of voice messages on your telephone through the computer.
Avaya WebLM	-	Virtualized Environment	A web-based license manager that manages licenses of one or more Avaya software products.
Message Networking	5.2	Avaya server with Red Hat Enterprise Linux	A component that supports interoperability with legacy voice mail products.
one-X Speech	5.2 6.3	Windows Server 2003 for one-X Speech Release 5.2 Windows Server 2012 for one-X Speech Release 6.3	A component that supports speech-based commands and text-to-speech functions for voice mail, email, calendar, and telephony functions.
Avaya service components			
Secure Access Link	2.1	-	A component that remotely manages Messaging and sends alarms to Avaya Services.

For more information about interoperability between these products, see *Avaya Aura® Messaging Overview and Specification* at the Avaya Support website: http://support.avaya.com.

VMware components

Component	Version	Description
ESXi Host	5.1	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	5.1	A platform that runs multiple operating systems on a host computer at the same time.
vSphere Client	5.1	vSphere Client is an application that installs and manages virtual machines. vSphere Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. The application is

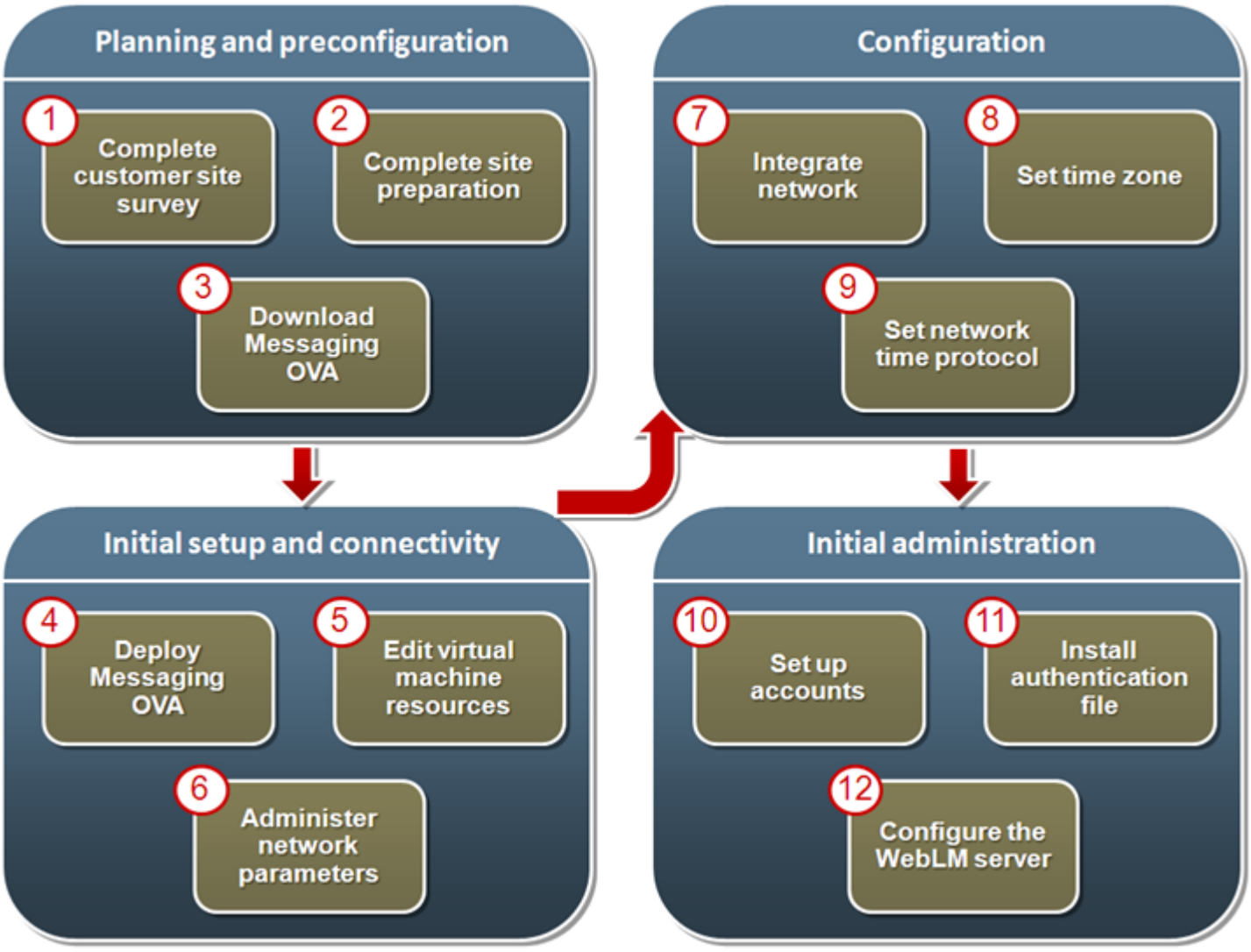
Component	Version	Description
		installed on a personal computer or accessible through a web interface. **Note:** You must access the ESXi host or the vCenter server by using the vSphere client from a computer running Windows Vista or a later version.
vCenter Server	5.1	vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion.

Third-party components

Component	Description
AudioCodes SIP gateway	Messaging uses SIP for integration with mixed telephony server environments. With the AudioCodes Mediant 1000 and 1000B gateways, Messaging connects to third-party telephony servers that Session Manager does not support.
Nuance Loquendo Text to Speech	This component supports conversion of text to speech.
EVM Plus giSTT	This component is a unified messaging application that provides speech-to-text functions for voice mail. Using this application, you can read, listen, and control your voice mail.
Storage Area Network	SAN is a high-speed network of storage devices that also connects those storage devices with servers.

Chapter 3: Deployment process

The following image shows the high-level tasks for deploying Messaging in a Virtualized Environment configuration.



Chapter 4: Planning and preconfiguration

Planning checklist

No.	Task	References	Notes	✔
1	Download the required documentation.	See Documentation on page 4.	—	
2	Identify the hypervisor and verify that the capacity meets the OVA requirements.	See Server hardware and resources on page 18.	—	
3	Plan the staging and verification activities and assign the resources.	See Messaging virtual machine resource requirements on page 19.	—	
4	Download Messaging OVA.	See Downloading software from PLDS on page 16.	—	

Software requirements

The following table lists the required software and the supported versions for Messaging in the Virtualized Environment:

Table 1: VMware software requirement

Equipment	Software versions
VMware vSphere ESXi	5.1
VMware vCenter Server	5.1

Table 2: Messaging software requirement

Software	Software versions
Messaging	6.3.1

Table 3: Service pack requirement

Software	Software versions
VMware tools	See *Avaya Aura® Messaging Release Notes*.

Software	Software versions
Kernel	See *Avaya Aura® Messaging Release Notes*.
Security	See *Avaya Aura® Messaging Release Notes*.
Communication Manager	See *Avaya Aura® Messaging Release Notes*.
Messaging	See *Avaya Aura® Messaging Release Notes*.

Key customer configuration information

The following table identifies the customer configuration information that you must enter during the deployment and configuration processes:

Required data	Value for the system
IPv4 IP address	
IPv4 subnet mask	
IPv4 Default Gateway address	

Configuration tools and utilities

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

- A remote computer running the VMware vSphere Client
- A browser for accessing the Messaging System Management Interface pages
- An sftp client for Windows, for example WinSCP
- An ssh client, for example, PuTTy

SAL Gateway

A Secure Access Link (SAL) Gateway is required for remote access and alarming.

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

A SAL Gateway:

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

You can deploy the SAL Gateway OVA using vCenter through a vSphere client. You can also deploy the SAL Gateway OVA directly to the ESXi server through a vSphere client.

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

Downloading the Messaging OVA

Registering for PLDS

Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

   The PLDS website redirects you to the Avaya single sign-on (SSO) webpage.

2. Log in to SSO with your SSO ID and password.

   The PLDS registration page is displayed.

3. If you are registering:
   - as an Avaya Partner, enter the Partner Link ID. If you do not know your Partner Link ID, send an email to prmadmin@avaya.com.
   - as a customer, enter one of the following:
     - Company Sold-To
     - Ship-To number
     - License authorization code (LAC)
4. Click **Submit**.

   Avaya will send you the PLDS access confirmation within one business day.

Downloading software from PLDS

About this task

Note:

You can download product software from http://support.avaya.com also.

Procedure

1. Type http://plds.avaya.com in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS website.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Search for the available downloads using one of the following methods:
   - By download name
   - By selecting an application type from the drop-down list

- By download type

  After entering the search criteria, click **Search Downloads**.

6. Click the download icon from the appropriate download.
7. When the system displays the confirmation box, select **Click to download your file now**.
8. If you receive an error message, click the message, install Active X, and continue with the download.
9. When the system displays the security warning, click **Install**.

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

Chapter 5: Initial setup and connectivity

Deployment guidelines

The high-level deployment steps are:

1. Deploy the OVA or OVAs.
2. Configure the application.
3. Verify the installation.

The deployment guidelines for the virtual appliances are:

- Deploy as many virtual appliances on the same host as possible.
- Deploy the virtual appliances on the same cluster if the cluster goes beyond the host boundary.
- Segment redundant elements on a different cluster, or ensure that the redundant elements are not on the same host.
- Plan for rainy day scenarios or conditions. Do not configure resources only for traffic or performance on an average day.
- Do not oversubscribe resources. Oversubscribing affects performance.
- Monitor the server, host, and virtual appliance performance.

Important:

The values for performance, occupancy, and usage can vary greatly. The blade server might run at 5% occupancy, but a virtual machine might run at 50% occupancy. Note that a virtual machine behaves differently when the CPU usage is higher.

Hardware requirements

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.

Messaging virtual machine resource requirements

The Messaging OVA is built with configuration values that optimize performance and follow recommended best practices. After installing the OVA, adjust resource settings as needed to meet the guidelines set forth in the following table.

The following set of resources must be available on the ESXi host for deploying the Messaging virtual machines:

Resource requirements	Combined application and storage virtual machine	Two application virtual machines and one storage virtual machine	Three application virtual machines and one storage virtual machine
	Heavy traffic[1]	**Medium traffic[2]**	**Heavy traffic[3]**
Mailboxes	6000	10000	20000
Ports	100	150	300
Virtual Machines	1	3	4
Virtual CPUs	4	4	4
Minimum CPU speed based on Xeon E5620 or equivalent processor	2 GHz	2 GHz	2 GHz
Virtual CPU reservations	8 GHz	8 GHz	8 GHz
Virtual memory	6 GB	Application: 6 GB Storage: 8 GB	Application: 6 GB Storage: 8 GB
Virtual memory reservations	6 GB	Application: 6 GB Storage: 8 GB	Application: 6 GB Storage: 8 GB
Virtual storage	260 GB	260 GB	260 GB
Average I/OPS	208	Application: 35 Storage: 204	Application: 106 Storage: 382
Shared Network Interface Cards	One @ 1000 Mbps	One @ 1000 Mbps	One @ 1000 Mbps
Average network usage	25 Mbps	25 Mbps per virtual machine	25 Mbps per virtual machine

For Messaging to run at full capacity, ensure that the recommended resource requirements are met.

- Values recommended in the table are for each virtual machine.

[1] Messaging is expecting to serve two calls per second. On average, each user receives nine voice messages every 24 hours.

[2] Messaging is expecting to serve a new call every 1 to 6 seconds. On average, each user receives three to six voice messages every 24 hours.

[3] Messaging is expecting to serve two calls per second. On average, each user receives nine voice messages every 24 hours.

- The default value for the Messaging OVA is 4 vCPU and 8 GB memory without any reservation.
- Use the recommended CPU and memory reservations to meet the acceptable performance level. You can check the CPU requirements in the **Summary** tab of the virtual machine.
- Messaging might not perform adequately if the cumulative CPU or memory resources of the virtual machines co-located on the same physical ESXi host as the Messaging virtual machine exceeds 70% of the physical hardware of server. The customer assumes all risk if this threshold is exceeded.
- The recommended resource requirements are based on the following hardware configurations:
  - iSCSI SAN storage: One Dell Equallogic PS6100XV array of 24 terabytes.
  - ESXi 5.1 hosts: Six Dell R720 servers. Each server with two quad-core Xeon 2620 CPU and 2 GHz, HyperThreaded. Each host server with 32 logical vCPUand each vCPU core provides 2 GHz.
  - VCenter server and Dell SAN Headquarter: One Dell R320 server running Windows 2008R2, with a single quad-core Xeon CPU and 500 GB RAID-1 hard disk drive array.
  - LAN: A stacked pair of Avaya ERS4850GTS, dedicated and configured for each Dell Equallogic SAN requirements. Each ESXi host server has four connections to the SAN switch to take advantage of the Dell Equallogic Multi-I/O for max storage I/O performance. A fifth SAN connection is dedicated for vMotion traffic.

Note:

- Avaya does not provide support for performance issues due to variance in the recommended settings.
- If a problem occurs with the virtual machine, Avaya Global Support Services (GSS) might not be able to assist in resolving the problem. Reset the values to the required values before starting to investigate the problem.

Software installation checklist

No.	Task	References	Notes	✔
1	Deploy the Messaging OVA.	See Deploying the Messaging OVA on page 21.	—	
2	Edit the virtual machine resources.	See Editing the virtual machine resources on page 22.	—	
3	Administer network parameters.	See Administering network parameters on page 23.	—	

Deploying the Messaging OVA

About this task

Use this procedure to deploy the Messaging OVA to the ESXi server through a vSphere client.

Procedure

1. Log in to the vCenter or the ESXi server using the vSphere Client.
2. Select **File** > **Deploy OVF Template**.
3. In the Deploy OVF Template window, perform one of the following to select the OVA file:
   - If the OVA file is downloaded to a location accessible from your computer, click **Browse** to select the location.
   - If the OVA file is located on an http server, enter the full URL in the **Deploy from a file or URL** field.
4. Click **Next**.
5. In the OVF Template Details window, verify the details of the Messaging OVA template and click **Next**.
6. In the End User License Agreement window, read the license agreement, click **Accept**, and click **Next**.
7. In the Name and Location window, in the **Name** field, type a unique name for the new virtual machine, and select the inventory location to deploy the virtual machine and click **Next**.
8. Select the host or cluster and click **Next**.

   If you did not select a host before deploying the template, the wizard prompts you to select now. If you selected a host or cluster while deploying the OVF template, the wizard processes the request to install the virtual machine on that host.
9. In the Storage window, select the data store location to store the virtual machine files, and click **Next**.

   The data store can be local to the host or a mounted shared storage, such as SAN. The virtual machine configuration file and virtual disk files are stored on the data store. Select a data store large enough to accommodate the virtual machine and all its virtual disk files.
10. In the Disk Format window, accept the default disk format, **Thick Provision Lazy Zeroed**, and click **Next**.

    The default disk format allocates the required 260-GB disk space for the Messaging virtual machine.

    For more information about the virtual disk, see Thin vs. thick deployments on page 52.

11. If there are multiple virtual machine networks configured on the host where you are deploying the Messaging OVA, the wizard prompts you to associate networks specified in the OVA with networks available on the host.
    - For a single **source network**, choose a host network by clicking the **Destination Network** column. Click the entry in the drop-down menu, for example, VM Network 2. Click **Next**.
    - If there is only a single virtual machine network on the host you are deploying the Messaging OVA, the wizard will not prompt you.
12. In the Ready to Complete window, verify the deployment settings, and click **Finish**.

    The progress of the tasks displays in a **vSphere Client Status** panel.

    The deployment process takes about 10 to 12 minutes to complete. If the OVA file location is an http server, the deployment process might take more time.

Next steps

Edit the virtual machine resources.

Editing the virtual machine resources

About this task

The OVA file is built with configuration values that optimize performance and follow recommended best practices.

After installing the OVA, use this procedure to adjust the virtual machine resources as needed to meet the guidelines set forth in Messaging virtual machine resource requirements on page 19.

Important:

For optimal performance, configure memory reservation so that VMware uses the physical memory of the server, not the swap space on the data store's hard disk.

Procedure

1. Right-click the virtual machine, and click **Edit Settings**.
2. On the Virtual Machine Properties window, click the **Hardware** tab.
    a. CPU: In the left pane, click **CPUs**. Select a value from the **Number of virtual sockets** and the **Number of cores per socket** fields.

       To determine the total number of cores, multiply the number of cores per socket by the number of virtual sockets. The resulting total number of cores is a number equal to or less than the number of logical CPUs on the host.

    b. Memory: In the left pane, click **Memory**. Adjust the memory configuration slider to an appropriate number. Alternatively, in the **Memory Size** field, enter the exact number.

3. On the Virtual Machine Properties window, click the **Resources** tab.
    a. CPU limitations: In the left pane, click **CPU**. Adjust the CPU reservation to an appropriate number. Alternatively, in the **Reservations** field, enter the exact CPU reservation number.
    b. Memory: In the left pane, click **Memory**. Adjust the memory reservation to an appropriate number. Alternatively, in the **Reservations** field, enter the exact memory reservation number.
4. Click **OK**.

Next steps

If you did not select the option to start the virtual machine automatically, start the virtual machine manually.

Start the Messaging virtual machine console, and configure the Messaging parameters.

Starting the Messaging virtual machine

Procedure

1. In the vSphere client, right-click the Messaging virtual machine, and click **Power** > **Power On**.
2. In the Recent Tasks window, wait until the status of the **Power on virtual machine** shows **Completed**.
3. Right-click the Messaging virtual machine, and select **Open Console**.

   The console displays the system startup messages. The system starts the system services and the Messaging services. After the startup process is complete, the system displays a message to log in to the virtual machine.

Next steps

Administer network parameters.

Administering network parameters

Procedure

1. In the vSphere client console window, log in as `craft`.

   Note:

   If you need any assistance for log in to the system, go to the Avaya Support website at http://support.avaya.com to open a service request.
2. Provide information in the following fields:
    a. **IPv4 IP address** : Enter the IP address.
    b. **IPv4 subnet mask**: Enter the network mask IP address.

c. **IPv4 Default Gateway address**: Enter the default gateway IP address.

3. In the **Are these correct** field, verify the IP address details and enter `y` to confirm.

Important:

You might have to reenter the data in the following conditions:

- The initial network prompt for entering the IP address, Subnet mask, and Default gateway address is interrupted.
- Incorrect data is specified.

To reenter data, run the following on the command line:

```
/opt/ecs/bin/serverInitialNetworkConfig
```

4. Configure additional network settings.

For more information, see Configuring the network settings on page 26.

WebLM

Avaya provides a web-based license manager (WebLM) to manage licenses of one or more Avaya software products.

To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

The license file is in XML format and contains information about the product such as the licensed capacities of each feature that you purchase. You activate the license file in PLDS and install the license file on the WebLM server.

You must run WebLM as a separate VMware virtual machine or use the WebLM running on System Manager. For more information about WebLM administration, see *Administering Avaya Aura® System Manager*.

Chapter 6: Configuration

Configuration checklist

No.	Tasks	References	Notes	✔
1	Configure the virtual machine automatic startup settings.	See Configuring the virtual machine automatic startup settings on page 25.	—	
2	Configure the network settings.	See Configuring the network settings on page 26.	—	
3	Set the time zone.	See Setting the time zone on page 27.	—	
4	Set up the network time protocol.	See Setting up the network time protocol on page 27.	—	
5	Install service packs.	See Messaging service packs on page 28.	—	

Configuring the virtual machine automatic startup settings

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

In high availability (HA) clusters, the VMware HA software ignores the startup selections.

Before you begin

Verify with the system administrator that you have the proper level of permissions to configure the automatic startup settings.

Procedure

1. In the vSphere Client inventory, select the host where the virtual machine is located.
2. Click the **Configuration** tab.
3. In the **Software** section, click **Virtual Machine Startup/Shutdown**.
4. Click **Properties** in the upper-right corner of the screen.

5. In the **System Settings** section, select **Allow virtual machines to start and stop automatically with the system**.
6. In the **Manual Startup** section, select the virtual machine.
7. Use the **Move up** button to move the virtual machine to the **Automatic Startup** section.
8. Click **OK**.

Configuring the network settings

Use the Network Configuration Web page to configure or view the settings for the host name, DNS domain name, DNS search list, DNS IP addresses, server ID, and default gateway.

Procedure

1. Log on to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Network Configuration**.
3. Click **Continue** at the warning.
4. Enter the appropriate information in the fields.

   For more information, see Network Configuration field descriptions on page 26.
5. Click **Change**.

Network Configuration field descriptions

Name	Description
Host Name	The Messaging system host name. The host name must be unique.
DNS Domain	The DNS domain name of the server. For example, company.com.
Search Domain List	The DNS search list. If there is more than one entry, use a comma (,) to separate each entry.
Primary DNS	The Primary DNS IP address.
Secondary DNS	The Secondary DNS IP address.
Tertiary DNS	The Tertiary DNS IP address.
Server ID	The unique server ID (SVID) of the server.

Name	Description
Default Gateway IPV4	The default gateway address of IP version 4. If the server supports IPv6 network, in the IPv6 area, enter or view the default gateway address of IP version 6.
IP Configuration	The IPv4 address and mask that are part of the IP configuration.
Mask	The number for the mask. If you are assigning an IPv4 address, you must set this field to the subnet mask that is required for this network setup. The system supports short version and long version of the mask. If you are using the short version, enter a numeric number from 1 to 32.
Functional Assignment	This field is not used.

Setting the time zone

Procedure

1. Log on to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Time Zone Configuration**.
3. On the Time Zone Configuration page, select the time zone and click **Apply**.

Note:

After changing the time zone settings, some features of the system use the new time zone only after you reboot the virtual machine. However, you can defer the reboot until you install the service packs.

Setting up the network time protocol

Procedure

1. Log on to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **NTP Configuration**.
3. Enable or disable the NTP mode.
4. In NTP Servers, enter the primary server, secondary server (Optional), and tertiary Server (Optional) details.

5. Click **Apply**.

Service pack installation

Messaging service packs

A service pack provides product updates and bug fixes. When a service pack is available on the Avaya Support website, the supporting information clearly states the issues addressed in the service pack. Even if the system does not have problems, install the service packs to keep the systems up-to-date and minimize the likelihood of future issues.

You must install, download, and manage the service packs from Messaging System Management Interface.

For each type of service pack, when the latest version is available, you must install the service packs in the following order:

- VMware Tools
- Kernel
- Security
- Communication Manager
- Messaging

For Messaging kernel service packs, additional caution is required:

- To install a kernel service pack, unpack, activate, and commit the service pack.
- To remove a kernel service pack, deactivate, commit, and remove the service pack.

Important:

- To install the latest version of any service pack, you must remove the earlier installed version.
- You cannot install or remove a service pack if any other service pack is being installed or removed.

For each applicable service pack, repeat the procedures in Downloading service packs on page 28 and Installing service pack on page 29.

Downloading service packs

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Miscellaneous** > **Download Files**.

2. To download files from your system to the Avaya server, select **File(s) to download from the machine I'm using to connect to the server** and then:
   a. Click **Choose File** or enter the path to the file that resides on your system. You can specify up to four files to download.
   b. Click **Open**.
3. To download files from a Web server to the Avaya server, select **File(s) to download from the LAN using URL** and then:
   a. Specify the complete URL of up to four files.
   b. If you require a proxy server for an external Web server that is not on the corporate network, you must enter the details in the `server:port` format.
      - Enter the name of the proxy server such as network.proxy or IP address.
      - If the proxy server requires a port number, add a colon (:).
   c. Click **Download**.

Installing a service pack

Procedure

1. Log on to Messaging System Management Interface.
2. Click **Server (Maintenance)** > **Server Upgrades** > **Manage Updates**.

   The Manage Updates page displays the list of uploaded service packs.
3. Select a service pack from the list.
   a. Click **Unpack**.
   b. Click **Continue** to return to the Manage Updates page.

   The status of the selected service pack changes to **unpacked**.
4. Select the same service pack from the list.
   a. Click **Activate**.

      If the service pack installation process affects the availability of the Messaging service, the system prompts you to confirm the action.
   b. **(Optional)** Click **Yes** to confirm the action.
   c. Click **Continue** to return to the Manage Updates page.

   The status of the selected service pack changes to **activated**. If the selected service pack is a kernel service pack, the status stays in the **activating** state until about one minute after the system reboots. Then the status changes to **pending_commit**.

Note:

The service pack installation process takes approximately 10 minutes for a kernel or security service pack.

5. Click **Messaging** > **Server Information** > **System Status** to verify that the Messaging system is functional.

   The System Status webpage displays the status of the various processes and modules depending on the server role.

Server role	Status of the processes and modules	Examples
Application only	All entries in the list of processes must have a status of `Running` or `Online`.	• Voice Messaging Application - Last known AxC status • Voice Browser - Text-To-Speech • Application Distributed Cache Server • Storage Synchronizer • Web Access - Java Servlet Container (Tomcat) - HTTP Server (Apache) - Flash Policy Server
Storage only	All entries in the list of modules must have a status of `IN SERVICE` or `UP`.	• Message Store • Other enabled software modules such as: - Enhanced-List Administration - Internet Messaging - LDAP processes - Corporate LAN LDAP Access - Voice System
Application and storage	All entries related to the lists of processes and modules must have the respective status.	Both of the above.

Tip:

Click the **Refresh** button of your browser until all entries show the relevant status.

Note:

The system reboots for a kernel or security service pack installation. During the system reboot, the System Status webpage remains inaccessible.

6. Verify that the status of the installed service pack shows **activated** on the Manage Updates page.

   If the status shows **pending_commit**, proceed to Step 7.

7. **(Optional)** Select the service pack from the list if the update that you want to activate shows **pending_commit** in the **Status** column.

   a. Click **Commit**.

   b. Click **Yes** to confirm the action.

   c. Click **Continue** to return to the Manage Updates page.

Removing a service pack

Procedure

1. Log on to Messaging System Management Interface.
2. Click **Server (Maintenance)** > **Server Upgrades** > **Manage Updates**.

   The Manage Updates page displays the list of uploaded service packs.

3. Select a service pack from the list.

   a. Click **Deactivate**.

      If the service pack installation process affects the availability of the Messaging service, the system prompts you to confirm the action.

   b. Click **Yes** to confirm the action.

   c. Click **Continue** to return to the Manage Updates page.

   The status of the selected service pack changes to **unpacked**. If the selected service pack is a kernel service pack, the status stays in **deactivating** state until about one minute after the system reboot and then changes to **pending_deactivate**.

   Note:

   The service pack deactivation process takes approximately 10 minutes for a kernel or security service pack.

4. Click **Messaging** > **Server Information** > **System Status** to verify that the Messaging system is functional.

   The System Status webpage displays the status of the various processes and modules depending on the server role.

Server role	Status of the processes and modules	Examples
Application only	All entries in the list of processes must have a status of `Running` or `Online`.	• Voice Messaging Application - Last known AxC status

Server role	Status of the processes and modules	Examples
		• Voice Browser - Text-To-Speech • Application Distributed Cache Server • Storage Synchronizer • Web Access - Java Servlet Container (Tomcat) - HTTP Server (Apache) - Flash Policy Server
Storage only	All entries in the list of modules must have a status of `IN SERVICE` or `UP`.	• Message Store • Other enabled software modules such as: - Enhanced-List Administration - Internet Messaging - LDAP processes - Corporate LAN LDAP Access - Voice System
Application and storage	All entries related to the lists of processes and modules must have the respective status.	Both of the above.

Tip:

Click the **Refresh** button of your browser until all entries show the relevant status.

Note:

The system reboots for a kernel or security service pack installation. During the system reboot, the System Status webpage remains inaccessible.

5. Verify that the status of the installed service pack shows **deactivated** on the Manage Updates page.

   If the status shows **pending_deactivate**, proceed to Step 6.

6. **(Optional)** Select the same service pack from the list if the update that you want to deactivate shows **pending_deactivate** in the **Status** column.

   a. Click **Commit**.

   b. Click **Yes** to confirm the action.

   c. Click **Continue** to return to the Manage Updates page.

   The status of the selected service pack changes to **deactivated**.

7. **(Optional)** Select the same service pack from the list to remove the deactivated service packs and reclaim the server space.
   a. Click **Remove**.
   b. Click **Yes** to confirm the action.
   c. Click **Continue** to return to Manage Updates page.

   The status of the selected service pack changes to **packed**.
8. **(Optional)** Select the same service pack from the list to clean up the hard disk drive by deleting the installation file of an uninstalled service pack.
   a. Click **Remove**.
   b. Click **Yes** to confirm the action.
   c. Click **Continue** to return to Manage Updates page.

   The list does not display the removed service pack. Repeat Step 8 if the service pack continues to display in the list.

Chapter 7: Initial administration

Initial administration checklist

No.	Tasks	References	Notes	✔
1	Add the privileged administrator login.	See Adding a privileged administrator login on page 34.	—	
2	Download and install the authentication file.	See Authentication file installation on page 36.	—	
3	Install the license file.	See License file for Messaging on page 39.	—	
4	Reboot the server.	See Shutting down the server on page 44.	—	

Account management

Adding a privileged administrator login

About this task

You must add a privileged administrator login that is a member of the SUSERS group. This login provides the highest level of access with the maximum permissions. A user with the privileged administrator login can gain access to all the System management Interface pages and Command Line Interface after you install the authentication file.

Procedure

1. Log on to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Administrator Accounts**.
3. In the **Select Action** area, select **Add Login**.
4. Select **Business Partner Login (dadmin)**.

   This login provides the highest level of access with the maximum permissions to a user. A user can gain access to all the SMI pages and CLI. You can add this login only once.
5. Click **Submit**.

The system displays the Administrator Accounts -- Add Login: Privileged Administrator Web page.

6. Enter information in the following fields:
   - **Date after which account is disabled-blank to ignore (YYYY-MM-DD)**: Clear this field
   - **Enter password or key**
   - **Re-enter password or key**
7. Click **Submit**.
8. Click **Continue** to go back to the Administrator Accounts Web page.

Administrator Accounts field descriptions

Field	Description
Select Action	
Add Login	Select this option and select the type of login to add. The options are: • **Privileged Administrator**: Provides the highest level of access with the maximum permissions. A user can gain access to all the SMI pages and CLI. • **Unprivileged Administrator**: Provides restricted access. A user can gain access to the SMI pages that are for querying the Messaging status and backing up data and CLI. • **Web Access Only**: Provides access only to the SMI pages. A user can administer the SMI pages that the user can gain access to in the **Web Access Mask** settings of the profile of the user. • **CDR Access Only**: Not applicable. • **Business Partner Login (dadmin)**: Provides the highest level of access with the maximum permissions to a user and is similar to **Privileged Administrator**. A user can gain access to all the SMI pages and CLI. You can add this login only once. • **Business Partner Craft Login**: Provides the highest level of access with the maximum permissions and is similar to **Business Partner Login (dadmin)**. A user can gain access to all the SMI pages and CLI. With this login, the user can suppress alarms from the server when logging in to SMI. • **Custom Login**: Provides customized access. You can select the level of access to the user.

Field	Description
Change Login	Select this option and select a login from the drop-down list.
Remove Login	Select this option and select a login from the drop-down list.
Lock/Unlock Login	Select this option and select a login from the drop-down list.
Add Group	Select this option to add a group.
Remove Group	Select this option and select a group from the drop-down list.

Authentication file management

Authentication file installation

To grant Avaya service personnel and Avaya partners access to the customer system, you need a new authentication file with Access Security Gateway (ASG) keys and the server certificate for Messaging. Authentication file ensures system security and prevents unauthorized access to your Messaging system.

Authentication files have a plain text XML header with encrypted authentication data and an encrypted server certificate. To change the authentication information, replace the entire file. If the authentication file is missing or corrupted, the system denies all logins to the Avaya server. The Messaging system continues to run, but the system blocks further administration until you install a new authentication file.

Note:

If the authentication file is not installed, the system displays an error message that the system cannot display the authentication file information.

Starting the AFS application

Before you begin

Authentication File System (AFS) is available only to Avaya service personnel and Avaya partners. If you are a customer and need an authentication file, contact Avaya or your authorized Avaya Partner.

To start the AFS application, you must have a login ID and password. Sign up for a login ID at http://rfa.avaya.com.

Procedure

1. Type http://rfa.avaya.com in your web browser.
2. Enter your login information and click **Submit**.
3. Click **Start the AFS Application**.

The system displays a security message.

4. Click **I agree**.

   The system starts the AFS application.

Next steps

Create an authentication file.

Creating an authentication file for a new system

Procedure

1. Log in to the AFS application.
2. In the **Product** field, click **SP System Platform/VE VMware**.
3. In the **Release** field, click the release number of the software, and then click **Next**.
4. On the Authentication File Delivery page, select **New System**, and then click **Next**.
5. In the **Communication Manager 6.x** field, type the fully qualified domain name (FQDN) of the host system where Messaging is installed.
6. To download the authentication file directly from AFS to your computer:
   a. Click **Download file to my PC**.
   b. In the File Download dialog box, click **Save**.
   c. Select the location to save the authentication file, and then click **Save**.
   d. In the Download complete dialog box, click **Close**.

   AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
7. To send the authentication file in an email message:
   a. In the **Email Address** field, enter the email address.
   b. Click **Download file via email**.

   AFS sends the email message that contains:

   - The system AFID, system type, and system release in the message text.
   - The authentication file as an attachment.
8. To view the header information in the authentication file, open the file in WordPad.

   The header includes the following information:

   - AFID
   - Product name
   - Release number
   - Date and time

Next steps

Install the authentication file.

Installing the authentication file

Procedure

1. Log on to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Load Authentication File**.
3. In the **Select the Authentication File** field, click **Browse**.
4. In the **Choose File to Upload** dialog box, click the authentication file, and then click **Open**.

   Note:

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

   - Must install an authentication file with a different AFID than the installed file.
   - Must reinstall the original file after installing a new authentication file.

   Do not select this option to replace the default authentication file, AFID 7100000000, with a unique authentication file.

   Caution:

   Use caution when selecting the **Force load of new file** option. If you install the wrong authentication file, you might encounter certificate errors and login issues.
5. Click **Install**.

   The system uploads the selected authentication file and validates the file before installing it.

Obtaining the AFID

If you want to redeploy the authentication file, use this procedure to obtain the AFID.

Procedure

1. Log on to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Authentication File**.

   The system displays the AFID in the AFID field.

License management

License file for Messaging

The license file is an Extensible Markup Language (XML) file with information about the product, the major release, and the license features and capacities. Avaya provides a web-based license manager (WebLM) to easily manage licenses of one or more Avaya software products.

You must run WebLM as a separate VMware virtual machine or use the WebLM running on System Manager. For more information about WebLM administration. see *Administering Avaya Aura® System Manager*.

You can use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files for Messaging. The Avaya PLDS provides customers, Avaya Partners, distributors, and Avaya Associates with easy-to-use tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads.

When you place an order for a PLDS-licensed software product such as Messaging, the license entitlements on the order are automatically created in PLDS. After these license entitlements are created, you receive an email notification from PLDS with a license activation code (LAC). Using the LAC, you can quickly find and activate the newly purchased license entitlements in PLDS. You can then download the license file.

Configuring the WebLM server

Procedure

1. Log in to Messaging System Management Interface.
2. On the **Administration** menu, click **Licensing**.
3. In the left navigation pane, click **WebLM Configuration**.

   The system displays the WebLM Configuration page.
4. In the **WebLM Server Address** field, type the WebLM server IP address to fetch the license file.

   Note:

   You can specify the IP address of the WebLM server within System Manager or of the standalone WebLM virtual appliance.
5. Click **Submit**.

Routine maintenance

Application backup and restore

Backing up the system

About this task

Messaging uses LAN to back up the Messaging data to an external server. The Messaging application data and the server data can be backed up simultaneously or independently. During a system failure, Messaging uses the information stored on the external server to restore the system.

Messaging supports the following backup methods:

- FTP
- SFTP
- SCP

Procedure

1. Log on to Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging** > **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The system delays the shutdown for three minutes after which the system ends all active calls.

   The Stop Messaging Software webpage refreshes periodically during the shutdown routine. After the Messaging software stops, the system displays the `Stop of Messaging completed` message.
4. Click **OK**.
5. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/Restore** > **Backup Now**.
6. On the Backup Now webpage, in the **Data Sets** area, click **Specify Data Sets**. Click the following fields:
   a. **Server and System Files**
   b. **Security File**
   c. **Messaging**
7. In the **Messaging** area, click **Messaging Application, Translations, Names, and Messages**.
8. In the **Backup Method** area, click **Network Device** and then complete the following fields:
   a. **Method**
   b. **User Name**

c. **Password**

d. **Host Name**

e. **Directory**

9. If you want to encrypt the backup data, select **Encrypt backup using pass phrase** and enter a pass phrase using an arbitrary string of 15 to 256 characters.
10. Click **Start Backup**.

    For more information, see Backup Now field descriptions on page 41.
11. On the **Administration** menu, click **Messaging** > **Utilities** > **Start Messaging**.

    The Start Messaging Software webpage refreshes periodically during the startup process and displays a status message after displaying the **Start Messaging information** message.

    After the Messaging software starts successfully, the system displays the `Start of Messaging completed` message.
12. Click **OK**.

Backup Now field descriptions

Settings	Description
Specify Data Sets	The data sets that you want to back up. The available options are: • **Server and System Files**: Back up the variable information to configure the server for a particular installation. • **Security File**: Back up the variable information to maintain security of the server. • **Messaging**: Back up one of the following Messaging options: - **Messaging Application, Translations and Messages** - **Messaging Application, Translations, Names, and Messages** - **Messaging Application, Translations and Names** - **Messaging Application and Translations** - **Messaging Application**
Full Backup	A full backup includes security data sets and files that configure both the Linux operating system and the applications. A **Full Backup** does not include any of the Messaging data sets.

Settings	Description
Backup Method	
Method	The following methods are available for backup: • **SCP**: A means of securely transferring computer files between a local and a remote host, or between two remote hosts, using the Secure Shell (SSH) protocol. • **FTP**: When you choose this option, you must enter the user name, the password, the host name or the IP address, and the directory. The default directory for backup data on the FTP server is `/var/home/ftp`. If you want to use the default directory, enter a forward slash (/) in the directory field. You must start the FTP server before backing up data. • **SFTP**: A network protocol that provides file transfers over data streams. The system adds the SFTP client to all Linux platforms.
User Name	The user name for storing the backup.
Password	The password for storing the backup.
Host Name	The host name of the backup server.
Directory	The backup is stored on this network directory.
Encryption	
Encrypt backup using pass phrase	Defines if you want to encrypt the backup data. The pass phrase can be an arbitrary string of 15 to 256 characters. The pass phrase can contain any characters except the following: single quote ('), ampersand (&), back slash (\), single back quote (`), quote ("), and percent sign (%).

Restoring data

Before you begin

Stop Messaging.

About this task

The time required to restore the database depends on the amount of data in the backup and the LAN speed. Perform the following procedure for attended and unattended backups.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **View/Restore Data**.

   The system displays the View/Restore Data webpage.

2. In the **View current backup contents in** area, select **Network Device** or **Local Directory**.

3. If you select **Network Device**, in the following fields, enter the same information that you used when you backed up the data:
   - **Method**
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   In **Host Name**, enter the IP address of the backup server.
4. If you select **Local Directory**, enter the path of the directory.
5. Click **View**.

   If you do not select a backup image, the system displays an error message. To clear the error message, click **Back** on the browser and then select a backup image.
6. On the View/Restore Data Results webpage, select a backup image stored in the location that you specified.

   The system lists the most recent backups at the bottom of the list.
7. To select the backup image you want to view or restore, click the corresponding option.
8. Click **Preview** if you are unsure that you selected the correct backup image.

   The system displays a brief description of the data associated with the backup image.

   Messaging data has one of the following names attached to the backup file name:
   - os-* for server and system files
   - security-* for security files
   - audix-ap-tr-msg-* for translations and messages
   - audix-ap-tr-name-msg-* for translations, names, and messages
   - audix-ap-tr-name-* for translations and names
   - audix-ap-tr-* for translations only
9. Click **Restore** on the second screen to begin the restore process.

   If the server name does not match, click **Force Restore if server name mismatch**.

   When you click **Restore**, the system displays the View/Restore Data Results webpage with the status of the restore process.

Stopping Messaging

Use the Stop Messaging Software Web page to stop the Messaging software.

Procedure

1. Log on to Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging** > **Utilities** > **Stop Messaging**.

   The system displays the Stop Messaging Software Web page.
3. To initiate a shutdown, click **Stop**.

   The system delays the shutdown process until all calls are completed. However, after three minutes the system ends all calls that remain active.

   The Stop Messaging Software Web page refreshes periodically during the shutdown process and displays a status message following the **Stop Messaging info** text.

   After the Messaging software stops completely, the system displays the *Stop of Messaging completed* message.
4. Click **OK**.

Starting Messaging

Use the Start Messaging Software Web page to start the Messaging software.

Procedure

1. Log on to Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging** > **Utilities** > **Start Messaging**.

   The system displays the Start Messaging Software Web page.

   The Start Messaging Software Web page refreshes periodically during the startup process and displays a status message following the **Start Messaging information** text.

   After the Messaging software starts successfully, the system displays the *Start of Messaging completed* message.
3. Click **OK**.

Shutting down the server

Procedure

1. Log on to Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Shutdown Server**.
3. On the Shutdown Server Web page, select from the following options:
   - **Delayed Shutdown**
   - **Immediate Shutdown**

4. (Optional) Select the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The system displays the confirmation screen.
6. Click **Ok** to continue.

Transferring files using WinSCP

Use the WinSCP utility to securely transfer files from a remote system to the virtual machine. WinSCP uses Secure Shell (SSH) and supports Secure FTP and legacy SCP protocols.

Before you begin

Ensure you have WinSCP on your computer. If not, download WinSCP from the Internet.

Procedure

1. Use WinSCP to connect to the virtual machine
2. Enter the credentials for SCP access.
3. In the warning dialogue boxes, click **OK** or **Continue** as necessary.
4. Change the file transfer protocol from SFTP to SCP.
5. Click **Browse** to locate and select the file.
6. In the WinSCP destination machine window, browse to **/home/**.
7. Select **/home/<customerloginname>** as the destination location for the file transfer. This is likely to be the first destination when WinSCP opens.
8. Click and drag the file from the WinSCP source window to **/home/<customerloginname>** in the WinSCP destination window.
9. Click the WinSCP **Copy** button to start the file transfer.
10. When the transfer is complete, close the WinSCP window and click **OK**.

Chapter 8: Optimization and scalability

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.

If you use the names of the time servers instead of the IP address, you must configure the Domain Name Service in the guest OS before you administer the NTP service. Otherwise, the NTP service cannot locate the time servers. If you administer the NTP service first, you must restart the NTP service after administering the DNS service.

After you administer the NTP service in the application, run the `ntpstat` or `/usr/sbin/ntpq -p` command from a command window. The results from these commands:

- Verify if the NTP service is getting time from a network time source.
- Indicate which network time source is in use.
- Display how closely the guest OS matches the network time.
- Display how often the guest OS checks the time.

The guest OS polls the time source every 65 to 1024 seconds. Larger time intervals indicate that the guest clock is tracking the network time source closely. If the time source is **local**, then the NTP service is not using a network time source and a problem exists.

If the clock value is consistently wrong, look through the system log for entries regarding **ntpd**. The NTP service writes the activities it performs to the log, including when the NTP service loses synchronization with a network time source.

VMware networking best practices

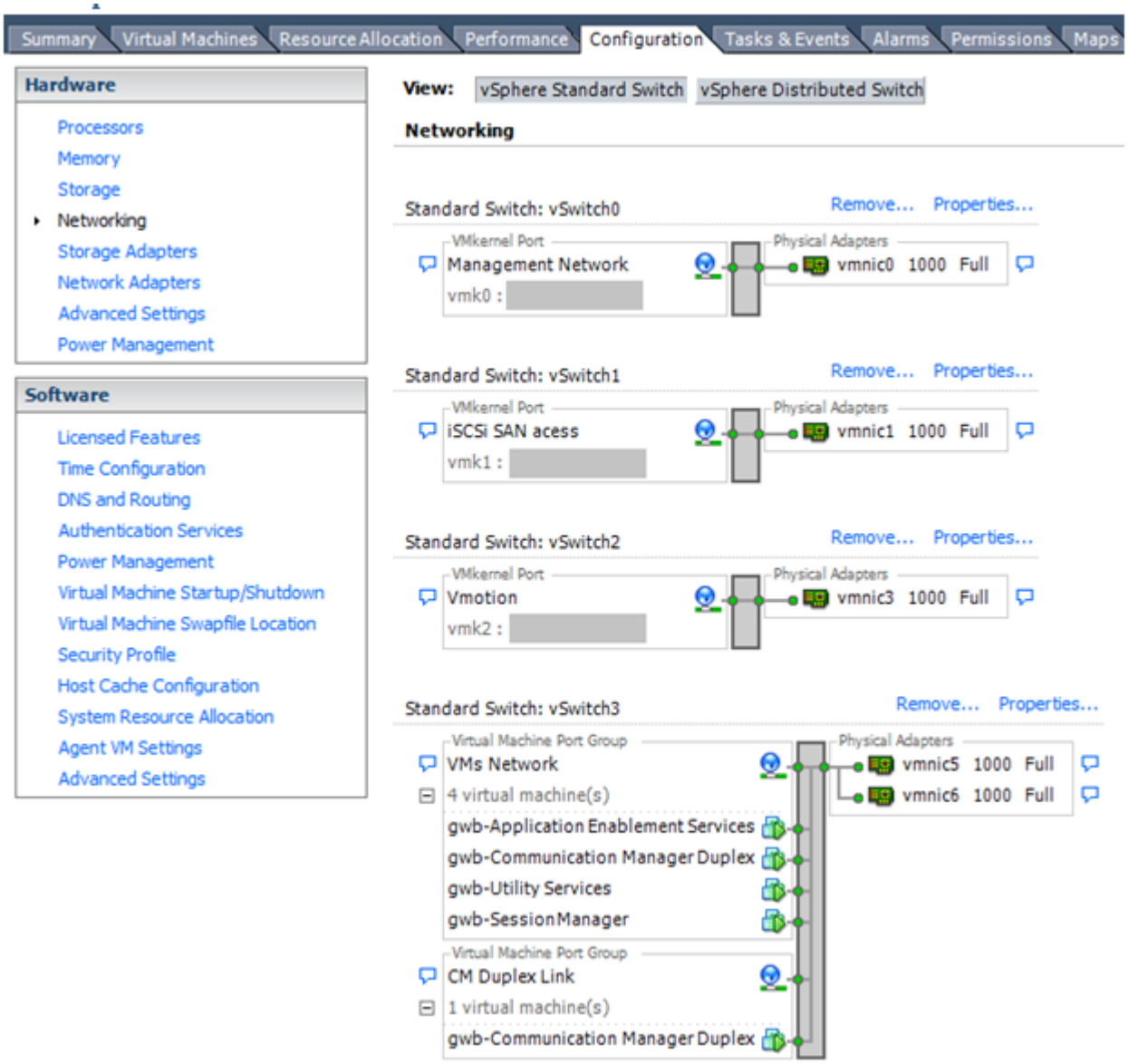
You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

This section is not a substitute for the VMware documentation. Review the VMware networking best practices before deploying any applications on an ESXi host.

The following are the suggested best practices for configuring a network that supports deployed applications on VMware Hosts:

- Separate the network services to achieve greater security and performance by creating a vSphere standard or distributed switch with dedicated NICs for each service. If you cannot use separate switches, use port groups with different VLAN IDs.
- Configure the vMotion connection on a separate network devoted to vMotion.
- For protection, deploy firewalls in the virtual machines that route between virtual networks that have uplinks to physical networks and pure virtual networks without uplinks.
- Specify virtual machine NIC hardware type **vmxnet3** for best performance.
- Connect all physical NICs that are connected to the same vSphere standard switch to the same physical network.
- Connect all physical NICs that are connected to the same distributed switch to the same physical network.
- Configure all VMkernal vNICs to be the same IP Maximum Transmission Unit (MTU).

Networking Avaya applications on VMware ESXi – Example 1

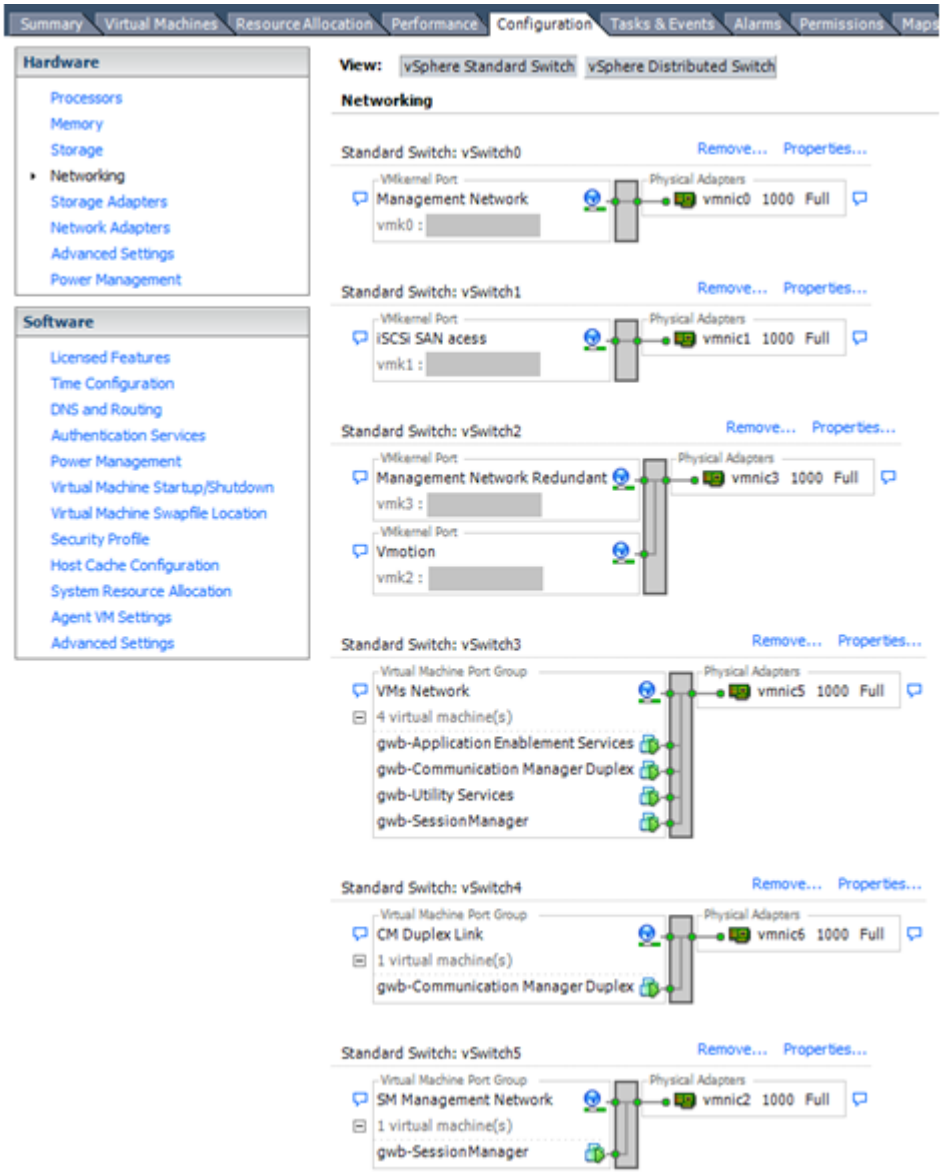


This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and virtual machine networks are segregated to separate physical NICs.
- Teamed network interfaces: vSwitch 3 in Example 1 displays use of a load-balanced NIC team for the Virtual Machines Network. Load balancing provides additional bandwidth for the Virtual Machines Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.
- Virtual networking: The network connectivity between virtual machines that connect to the same vSwitch is entirely virtual. In Example 2, the virtual machine network of vSwitch3 can

communicate without entering the physical network. Virtual networks benefit from faster communication speeds and lower management overhead.

Networking Avaya applications on VMware ESXi – Example 2



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

- VMware Management Network redundancy: Example 2 includes a second VMkernel Port at vSwitch2 to handle VMware Management Network traffic. In the event of a failure of vmnic0, VMware Management Network operations can continue on this redundant management network.
- Removal of Teaming for Virtual Machines Network: Example 2 removes the teamed physical NICs on vSwitch3. vSwitch3 was providing more bandwidth and tolerance of a single NIC failure instead of reallocating this NIC to other workloads.

- Communication Manager Duplex Link: vSwitch4 is dedicated to Communication Manager Software Duplication. The physical NIC given to vSwitch4 is on a separate physical network that follows the requirements described in PSN003556u at PSN003556u.
- Session Manager Management Network: Example 2 shows the Session Manager Management network separated onto its own vSwitch. The vSwitch has a dedicated physical NIC that physically segregates the Session Manager Management network from other network traffic.

References

Title	Link
Product Support Notice PSN003556u	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/

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.

Messaging only supports thick provisioning.

Appendix A: Upgrading Messaging

About this task

Use the following procedure to upgrade to a new release of a Messaging on VMware by taking a backup on an existing Messaging Virtual Machine and restoring the backup on a new Virtual Machine containing the new release of Messaging.

Procedure

1. Perform Full Backup and Messaging data backup. For more information, see Backing up the system on page 40.

   Note:

   Do not start Messaging after backup.

2. Shutdown Messaging. Clear the **Restart server after shutdown** check box. For more information, see Shutting down the server on page 44.
3. Deploy the Messaging OVA.

   For more information, see Deploying the Messaging OVA on page 21.
4. Administer network parameters. Perform only steps 1 to 3 of Administering network parameters on page 23.
5. Restore Full Backup. For more information, see Restoring data on page 42.

   Note:

   - Do not stop Messaging before restore.
   - In the **Host Name** field, enter the IP address of the backup server. Do not enter FQDN of the backup server.
   - Select the **Force Restore if server name mismatch** check box.
6. Reboot Messaging. Select the **Restart server after shutdown** check box. For more information, see Shutting down the server on page 44.
7. Restore the Messaging data backed up in step 1. Restore the backup files prefixed with audix. For more information, see Restoring data on page 42.
8. Start Messaging.

   For more information, see Starting Messaging on page 44.

Appendix B: Migration

Overview

You can migrate the Messaging system running on System Platform to a Virtualized Environment using VMware®.

The migration process consists of two phases:

1. Backing up data from the old system on page 55.
2. Restoring data on the new system on page 56.

Supported migration paths are based on the Communication Manager platform on which Messaging is installed.

If the installed Messaging system does not match the minimal software release and patches required on System Platform to start the migration, first upgrade your Messaging system. For more information, see Migration roadmap and limitations on page 54.

Migration roadmap and limitations

Roadmap

The minimal software required to migrate from Messaging running on System Platform to Virtualized Environment is:

System Platform	VMware
Messaging 6.2 with Communication Manager Service Pack 7.01 and Messaging Service Pack 4.	Messaging 6.3.1 with Communication Manager Service Pack 6.3.3.0 and Messaging Service Pack 0.
Messaging 6.3 with Communication Manager Service Pack 6.3.1 and Messaging Service Pack 0.	Messaging 6.3.1 with Communication Manager Service Pack 6.3.3.0 and Messaging Service Pack 0.

Supported data types

The system migrates the following types of data:

- Users, passwords, and profiles for System Management Interface and ssh access to Messaging virtual machine
- System password policies

- Backup schedules configured on System Management Interface
- Alarming and SNMP configuration
- System configuration, users, names, greetings, and messages

Limitations

The system does not migrate the following types of data. You must reconfigure the following data on VMware:

- Network configuration
- Time zone
- Network time protocol
- Authentication file
- Licensing configuration

Migrating Messaging to Virtualized Environment

Backing up data from the old system

Procedure

1. Upgrade the Messaging system to the minimal required software version. For more information about minimal required software, see Migration roadmap and limitations on page 54.
2. Stop Messaging.

   For more information, see Stopping Messaging on page 43.
3. Back up the following data from the command line:
   a. Migration data on the Messaging virtual machine by running the `sudo /opt/ecs/sbin/backup -b -d ftp|scp|sftp://<user>:<passwd>@<hostname></full-path-directory> --verbose -- migration-60` command. Where:

`ftp|scp|sftp`	Enter one of the backup method.
user	Enter the user name for storing the backup.
passwd	Enter the password for storing the backup.
hostname	Enter the host name of the backup server.
/full-path-directory	Enter the directory path where you want to store the backup.

b. Messaging application data by running the `sudo /opt/ecs/sbin/backup -b -d ftp|scp|sftp://<user>:<passwd>@<hostname></full-path-directory> --verbose -- audix-ap-tr-name-msg` command. Where:

`ftp|scp|sftp`	Enter one of the backup method.
user	Enter the user name for storing the backup.
passwd	Enter the password for storing the backup.
hostname	Enter the host name of the backup server.
/full-path-directory	Enter the directory path where you want to store the backup.

Note:

Only privileged users, dadmin, craft, init, and sroot can perform the migration backup. Administrative users admin and cust cannot perform migration backups.

4. Shutdown Messaging. Clear the **Restart server after shutdown** check box. For more information, see Shutting down the server on page 44.

Next steps

Restore data on the new system.

Restoring data on the new system

Procedure

1. Deploy the Messaging OVA.

   For more information, see Deploying the Messaging OVA on page 21.

2. Administer network parameters. For more information, see Administering network parameters on page 23.

3. Configure the network settings.

   For more information, see Configuring the network settings on page 26.

4. Set the time zone. For more information, see Setting the time zone on page 27.

5. Set up the network time protocol. For more information, see Setting up the network time protocol on page 27.

6. Install the minimal required Messaging service packs.

   For more information, see Messaging service packs on page 28.

7. Stop Messaging.

   For more information, see Stopping Messaging on page 43.

8. Restore the following data using the *craft* user login:
   a. Migration data
   b. Messaging application data

   For more information, see Performing a restore on page 42.
9. Download and install the authentication file. For more information, see Authentication file installation on page 36.
10. Install the license file.

    For more information, see License file for Messaging on page 39.
11. Reconfigure the password for the scheduled backup.

    For more information, see *Administering Avaya Aura® Messaging*.
12. Reboot Messaging. Select the **Restart server after shutdown** check box. For more information, see Shutting down the server on page 44.

    If you assigned a new virtual machine IP address that is different from the IP address for the virtual machine on System Platform, proceed to Step 13 and 14.
13. **(Optional)** Reconfigure the server IP addresses on the following Messaging System Management Interface pages:
    a. **Messaging** > **Messaging System (Storage)** > **Topology**
    b. **Messaging** > **Server Settings** > **Server Role / AxC Address**
14. **(Optional)** Reconfigure the telephony parameters on the switch.

    For more information, see switch configuration notes.

    Note:

    If you are migrating from Messaging Release 6.2, you must perform additional tasks. For more information about these tasks, see *Upgrading Avaya Aura® Messaging for Single Server Systems*.

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

A

adding
privileged administrator login 34
administering
network parameters 23
AFID
obtaining 38
AFS
starting 36
attended backup 40
authentication file
creating for new system 37
installing 38
automatic restart
virtual machine 25

B

backing up
system 40
backup screen
field descriptions 41
best practices
VMware networking 49
BIOS 46
BIOS for HP servers 47
BIOS settings
for Dell servers 47

C

checklist
configuration 25
initial administration 34
planning 14
software installation 20
components
Avaya 10
third party 12
VMware 11
configuration data
customer 15
configuration tools 15
configuring
network settings 26
virtual machine automatic restart 25
WebLM Server 39
customer configuration information 15

D

data
restoring 42
deploying
OVA 21
deployment
thick 52
thin 52
deployment guidelines 18
deployment process 13
documentation 4
administration 5
overview 4
security 4
user functions 5
VMware systems 5
downloading
service packs 28
downloading software 16

E

editing
virtual machine resources 22

F

field descriptions
Administrator Accounts 35
backup screen 41
network configuration 26

G

guidelines
deployment 18

I

installing
authentication file 38
service packs 29
Intel Virtualization Technology 46

L

license manager 24
licensing 39

M

managing
licenses 24
Messaging
migration roadmap 54
migrating
Messaging 55
virtualized environment 56
VMware 56
migration 54
roadmap 54
migration roadmap 54

N

network configuration 26
field descriptions 26
network settings
configuring 26
network time protocol
setting 27
NTP time source 48

O

obtaining
AFID 38
overview 8

P

planning
checklist 14
PLDS 16
downloading software 16
privileged administrator login
adding 34
purpose 4

R

registering 16
removing
service packs 31
requirements
software 14
virtual machine resources 19
resource requirements 19
resources
server 18
restoring
data 42

S

SAL Gateway 15
server hardware and resources 18
service pack 28
service packs
installing 29
removing 31
setting
network time protocol 27
time zone 27
shutting down
server 44
software installation
checklist 20
software requirements 14
starting
virtual machine 23
start Messaging 44
stop Messaging 43
support 7
system
backing up files 40
start 44
stop 43

T

thick deployment 52
thin deployment 52
third party
components
product 12
timekeeping 48
time zone
setting 27
topology 9
training courses 6

U

upgrading
virtualized environment 53
VMware 53
utilities 15

V

videos 6
virtual machine
automatic restart configuration 25
starting 23
virtual machine resource requirements 19
virtual machine resources
editing 22
VMware

VMware *(continued)*
components 11
VMware networking
best practices 49
VMware Tools 47
VT support 46

W

WebLM 24
WinSCP
using 45