Deploying standalone Avaya WebLM

Release 7.0.1
Issue 3
March 2017

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

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

Licence 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.

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 virtual appliance has its own ordering code. Note that each instance of a virtual appliance must be ordered separately. If the enduser customer or Business Partner wants to install two of the same type of virtual appliances, then two virtual appliances of that type must be ordered.

Third Party Components

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

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL

PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for deploying the Avaya WebLM virtual application in the Avaya Appliance Virtualization Platform and customer Virtualized Environment. The document includes installation, configuration, installation verification, troubleshooting, and basic maintenance checklists and procedures.

The primary audience for this document is anyone who is involved with installing, configuring, and verifying WebLM in a VMware® vSphere™ virtualization environment at a customer site. 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.

Change history

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

Issue	Date	Summary of changes
3.0	March 2017	• Updated the “Appliance Virtualization Platform overview” section. • Updated the “WebLM vAppliance minimum resource requirements” section.
2.0	May 2016	• Added procedure for installing WebLM Release 7.0.1 feature pack. • Added procedure for upgrading WebLM to Release 7.0.1. • Added support for deployment on standalone WebLM OVA on VMware ESXi 6.0.

Warranty

Avaya provides a 90-day limited warranty on the Appliance Virtualization Platform software. For detailed terms and conditions, see the sales agreement or other applicable documentation. Also, 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 more information, see “Help & Policies > Policies & Legal > License Terms”.

Chapter 2: Architecture overview

Appliance Virtualization Platform overview

From Release 7.0, Avaya uses the VMware®-based Avaya Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya Aura® Virtualized Appliance offer.

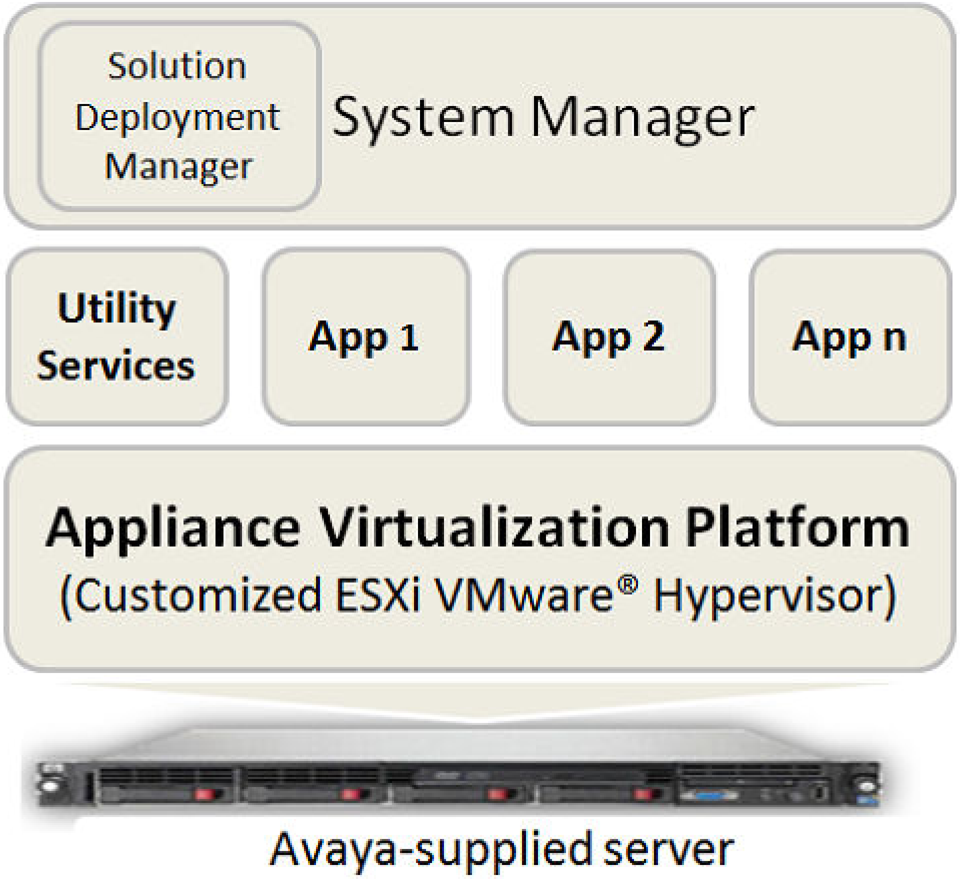
Avaya Aura® Virtualized Appliance offer includes:

- Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360 G7, HP ProLiant DL360p G8, and HP ProLiant DL360 G9
- S8300D and S8300E

  Note:

  With WebLM Release 7.x, you cannot deploy WebLM on S8300D Server or S8300E Server running on Appliance Virtualization Platform.

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements.


Solution Deployment Manager
System Manager
Utility Services
App 1
App 2
App n
Appliance Virtualization Platform
(Customized ESXi VMware® Hypervisor)
Avaya-supplied server

From Release 7.0, Appliance Virtualization Platform replaces System Platform.

Avaya Aura® Release 7.0.1 supports the following applications on Appliance Virtualization Platform:

- Utility Services 7.0.1
- System Manager 7.0.1
- Session Manager 7.0.1
- Branch Session Manager 7.0.1
- Communication Manager 7.0.1
- Application Enablement Services 7.0.1
- WebLM 7.0.1
- Avaya Breeze™ 3.1.1
- SAL 2.5
- Communication Manager Messaging 7.0
- Avaya Aura® Media Server 7.7.0.292 (SP3)
- Avaya Scopia® 8.3.5
- Avaya Proactive Contact 5.1.2

For more information about installing Avaya Proactive Contact and administering Appliance Virtualization Platform with Avaya Proactive Contact, see the Avaya Proactive Contact documentation.

Avaya Aura® Virtualized Environment overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® virtualized server architecture.

Using Avaya Aura® Virtualized Environment, customers with a VMware IT infrastructure can upgrade to the next release level of collaboration using their own VMware infrastructure. For customers who need to add more capacity or application interfaces, Avaya Aura® applications on VMware offer flexible solutions for expansion. For customers who want to migrate to the latest collaboration solutions, Avaya Aura® Virtualized Environment provides a hardware-efficient simplified solution for upgrading to the latest Avaya Aura® release and adding the latest Avaya Aura® capabilities.

The Virtualized Environment project applies only for Avaya Appliance Virtualization Platform and customer VMware®, and does not include any other industry hypervisor.

Note:

This document uses the following terms, and at times, uses the terms interchangeably.

- server and host
- reservations and configuration values

Deployment considerations

The following manage the deployment to the blade, cluster, and server:

- Avaya Appliance Virtualization Platform from System Manager Solution Deployment Manager or the Solution Deployment Manager client
- VMware® vCenter and VMware® vSphere

Virtualized components

Software component	Description
ESXi Host	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.
vSphere Client	vSphere Client is an application that installs and manages virtual machines. vSphere Client connects to a vCenter server or directly to an

Table continues…

Software component	Description
	ESXi host if a vCenter Server is not used. The application is installed on a personal computer or accessible through a web interface.
vCenter Server	vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion.
Appliance Virtualization Platform	Avaya-provided virtualization turnkey solution that includes the hardware and all the software including the VMware hypervisor.
Solution Deployment Manager	Centralized software management solution of Avaya that provides deployment, upgrade, migration, and update capabilities for the Avaya Aura® virtual applications.
Open Virtualization Appliance (OVA)	The virtualized OS and application packaged in a single file that is used to deploy a virtual machine.

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.

Chapter 3: Planning and configuration

Server hardware and resources for VMware

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

Customer configuration data

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

Required data	Value for the system	Example value
IP address	The IP address of the WebLM interface.	192.168.x.x
Netmask	The network address mask.	255.255.0.0
Default Gateway	The default network traffic gateway.	172.16.x.x
DNS IP Address	The IP address of the primary DNS server.	172.16.x.x
Domain Name	The domain name which must be a fully qualified domain name.	abc.mydomain.com
Short HostName		weblm
Default Search List	The domain name string that is used for default search.	abc.mydomain.com
NTP Server	The IP address of the NTP server.	172.16.x.x
Time Zone	The time zone you want to choose.	America/Denver

WebLM vAppliance minimum resource requirements

The following tables describe the minimum resource requirement to deploy WebLM through VMware.

WebLM Server vAppliance minimum resource requirements

VMware resource	Profile 1	Profile 2
vCPU	1	1
CPU reservation	2290 MHz	2290 MHz
Memory	1GB	2GB
Memory reservation	1GB	2GB
Storage reservation	30GB	30GB
Shared NICs	1	1

Note:

If you use WebLM Server to acquire licenses for more than 5000 clients, use Profile 2.

Software versions

Application	Version
VMware vCenter Server	6.0, 5.5, 5.1, and 5.0.0
VMware vSphere Client	6.0, 5.5, 5.1, and 5.0.0
VMware ESXi Host	6.0, 5.5, 5.1, and 5.0.0
WebLM Server	7.0.1
Cent OS	6.5, 64-bit

SAL Gateway

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

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

A SAL Gateway:

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

You can deploy SALGateway OVA:

- On Avaya Aura® Virtualized Appliance by using Solution Deployment Manager
- In the Avaya Aura® Virtualized Environment by using vCenter, vSphere or Solution Deployment Manager

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

Chapter 4: Deploying WebLM OVA from Solution Deployment Manager

Methods of WebLM OVA file deployment

You can deploy WebLM 7.0 by using one of the following methods:

- WebLM OVA file:
    - Deploying WebLM using System Manager Solution Deployment Manager or the Solution Deployment Manager client.
    - Deploying WebLM on customer Virtualized Environment:
        - By using vSphere. For more information, see Deploying the WebLM server through vSphere on page 20
        - By using vCenter. For more information, see Deploying the WebLM server through vCenter on page 20
- WebLM war file: Installing the WebLM war file on Windows and Linux.

Checklist for deploying WebLM from Solution Deployment Manager

No.	Task	Links/Notes	✔
1.	Download the OVA file and the feature packs for WebLM from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com/	Downloading software from PLDS on page 19	
2.	Keep a copy of license files of Avaya Aura® products handy so you can replicate with the new Host ID after the OVA file installation.		
3.	Keep the network configuration data handy.	Customer configuration data on page 12	

Table continues…

No.	Task	Links/Notes	✔
4.	Add a location.		
5	Add the Appliance Virtualization Platform host.		
6.	Deploy the WebLM OVA file.	Deploying WebLM from Solution Deployment Manager on page 15	
7.	Start the WebLM virtual machine.	Starting a virtual machine from Solution Deployment Manager on page 17	
8.	Verify the installation of the WebLM virtual machine.		
9.	Install the WebLM 7.0.1 feature pack file.	Installing a WebLM patch, feature pack, or service pack on page 38	
10.	Restart the WebLM virtual machine from CLI to get the updated kernel running in memory.		

Deploying WebLM from Solution Deployment Manager

Before you begin

- Install the Solution Deployment Manager client if System Manager is unavailable.
- Add a location.
- Add Appliance Virtualization Platform or an ESXi host to the location.
- Download the required OVA file to System Manager.

Procedure

1. Deploy the WebLM OVA file.

   For instructions, see Deploying an OVA file for an Avaya Aura® application. For more information, see *Deploying Avaya Aura® applications from System Manager*.

2. Install the WebLM Release 7.0.1 feature pack.
3. From the WebLM web console, verify that the About page displays the Release 7.0.1 version and build details.
4. Restart WebLM to get the updated kernel running in memory.

Related links

Deploying an OVA file for an Avaya Aura application on page 16

Deploying an OVA file for an Avaya Aura® application

About this task

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

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

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

Before you begin

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

Procedure

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

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

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

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

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

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

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

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

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

    For each application that you deploy, fill the appropriate fields. For more information, see “VM Deployment field descriptions”.

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

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

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

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

Next steps

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

Starting a virtual machine from Solution Deployment Manager

Procedure

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

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

Chapter 5: Deploying the WebLM OVA

Deployment of cloned and copied OVAs

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

Checklist for deploying WebLM

No.	Task	Links/Notes	✔
1.	Download the OVA file for WebLM from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com/	Downloading software from PLDS on page 19	
2.	Install the vSphere client 5.0, 5.1, 5.5, or 6.0.		
3.	Keep a copy of license files of Avaya Aura® products handy so you can replicate with the new Host ID after the OVA file installation.		
4.	Keep the network configuration data handy.	Customer configuration data on page 12	
5.	Deploy the WebLM OVA file.	Deploying the WebLM server through vSphere on page 20 Deploying the WebLM server through vCenter on page 20	
6.	Start the WebLM virtual machine.	Starting the WebLM server virtual machine on page 21	
7.	Verify the installation of the WebLM virtual machine.		
8.	Install the WebLM 7.0.1 feature pack file.	Installing a WebLM patch, feature pack, or service pack on page 38	
9.	Restart the WebLM virtual machine from CLI to get the updated kernel running in memory.		

Downloading software from PLDS

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

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

Note:

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

Procedure

1. Enter http://plds.avaya.com in your Web browser to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS home page, select **Assets**.
4. Click **View Downloads**.
5. Click on the search icon (magnifying glass) for **Company Name**.
6. In the **%Name** field, enter **Avaya** or the Partner company name.
7. Click **Search Companies**.
8. Locate the correct entry and click the **Select** link.
9. Enter the Download Pub ID.
10. Click **Search Downloads**.
11. Scroll down to the entry for the download file and click the **Download** link.
12. In the **Download Manager** box, click the appropriate download link.

    Note:

    The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.
13. If you use Internet Explorer and get an error message, click the **install ActiveX** message at the top of the page and continue with the download.
14. Select a location where you want to save the file and click **Save**.
15. If you used the Download Manager, click **Details** to view the download progress.

Deploying the WebLM server through vSphere

Before you begin

Download the vSphere client.

Procedure

1. Log in to the ESXi host.
2. Click **File**.
3. Click **Browse** to navigate to the OVA file from the local computer, network share, CD-ROM, or DVD, and click **Open**.

   If the OVA file is available in the Web, enter the URL.
4. Click **Next**.
5. Read through the End User License Agreement page, and click **Accept**.
6. Confirm the OVF Template Details, and click **Next**.
7. Choose a **Name and Location** for the WebLM virtual machine, and click **Next**.
8. Select **a destination storage for the virtual machine files:**, and click **Next**.
9. Select **Thick Provision Lazy Zeroed**, and click **Next**.
10. Map the networks used in the OVF template to the networks in your inventory.
11. Review the deployment settings, and click **Finish**.
12. Start the virtual machine.
13. At the system prompt, type the network parameters.
14. Confirm the network parameters. Press `n` to reenter the values.

    The WebLM boot up sequence continues and WebLM configuration starts. This process takes about 2 to 3 minutes.

Next steps

Install the WebLM 7.0.1 feature pack file.

Deploying the WebLM server through vCenter

Before you begin

Download and install the vSphere client.

Procedure

1. Start the vSphere client.
2. Log in to the vCenter host.

Ignore any security warning the system displays.

3. Select the target Host ESX host server.
4. On the vCenter client, click **File** > **Deploy OVF template**.
5. In the Deploy OVF Template dialog box, perform one of the following actions:
    - In the **Deploy from a file or URL** field, enter the path to the OVA file.
    - Click **Browse**, navigate to the OVA file saved on the local computer, network share, CD-ROM, or DVD, and click **Open**.
6. On the OVF Template Details page, verify the details and click **Next**.
7. Read through the End User License Agreement page, click **Accept** > **Next**.
8. In the **Name** field, enter the name of the virtual machine, and click **Next**.
9. On the Disk Format page, click **Thick Provisioned Lazy Zeroed**.

    The system displays the data store that you selected and the available space.
10. Click **Next**.
11. On the Network Mapping page, map the networks used in the OVF template to the networks in your inventory.
12. Click **Next**.
13. On the Properties page, enter the network parameters, and click **Next**.
14. Review the settings, and click **Finish**.

    If you want to start the WebLM server immediately after installation, select **Power on after deployment**.

Next steps

Install the WebLM 7.0.1 feature pack file.

Starting the WebLM server virtual machine

Procedure

1. From the list of virtual machines for the target host, select the WebLM server machine that you have deployed.
2. Click **Power On**.
3. If you have deployed WebLM through vSphere, at the system prompt, enter the network parameters.
4. Confirm the network parameters. Press `n` to reenter the values.

    The WebLM boot-up sequence continues and WebLM configuration starts.
5. Right-click the deployed WebLM server virtual machine, and select **Open Console**.

The WebLM server virtual machine starts.

Note:

You must re-host all the required licenses after upgrading WebLM. For a fresh installation, you need not re-host the licenses.

Related links

Rehosting license files on page 22

Rehosting license files

Procedure

1. On the WebLM console, click **Server Properties**.
2. On the Server Properties page, note the WebLM server host ID.
3. Go to the PLDS website regenerate the license file for your product using the same host ID.
4. Install the license file that you generated on the WebLM server.

   For more information on installing a license file, see “Installing the license file” in *Administering Avaya WebLM*.

Chapter 6: Configuration

Configuring the virtual machine automatic startup settings

About this task

This procedure does not apply for deployments and upgrades of applications running on Appliance Virtualization Platform.

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**.

WebLM configuration

The `weblmserver.properties` file defines WebLM server configuration. This file is located in the `<$CATALINA_HOME>/webapps/WebLM/data` folder. If you make any changes to this file, you must restart Tomcat for the changes take effect.

The following table specifies important properties defined in the `weblmserver.properties` file.

Property Name	Description	Default Value
WebLM.LicenseAllocation.Backup.FileSize	The size of the license allocation backup file size in MB. You must enter an integer value for this property. For example, 1, 10. A decimal value like 1.5 is invalid.	10MB
WebLM.Usages.MaxUsageCount	The maximum usage query results that WebLM maintains. You must enter an integer value for this property. A decimal value like 1.5 is invalid.	5
WebLM.Usages.UsageCount	The number of usage query results that WebLM maintains. You must enter an integer value for this property within a range of 1 to whatever is the value of property in WebLM.Usages.MaxUsageCount. A decimal value like 1.5 is invalid. You can also configure this property using the WebLM UI.	1

The `log4j.properties` file defines WebLM server logging configuration. This file is located in the `<$CATALINA_HOME>/webapps/WebLM/WEB-INF/classes` folder. If you make any changes to this file, you must restart Tomcat for the changes take effect.

The following table specifies important properties defined in the `log4j.properties` file:

Property Name	Logger Type	Default Value	Description
log4j.appender.weblmDebugAppender.File	Deubug	$CATALINA_HOME/webapps/WebLM/data/log/weblmserverdebug.log	Use this property to specify the location where you want to save the log files. Enter the path followed by the file name. For example, `/var/log/weblm/weblmserver.log`.
log4j.appender.weblmOperationalAppender.File	Operational	$CATALINA_HOME/webapps/WebLM/data/log/weblmserveroperational.log	Use this property to specify the location where you want to save the log files. Enter the path followed by the file name. For example, `/var/log/weblm/weblmserver.log`.
log4j.appender.weblmAuditAppender.File	Audit	$CATALINA_HOME/webapps/WebLM/data/log/weblmserveraudit.log	Use this property to specify the location where you want to save the log files. Enter the path followed by the file name. For example, `/var/log/weblm/weblmserver.log`.

Table continues…

Property Name	Logger Type	Default Value	Description
log4j.appender.weblmSecurityAppender.File	Security	$CATALINA_HOME/webapps/WebLM/data/log/weblmserversecurity.log	Use this property to specify the location where you want to save the log files. Enter the path followed by the file name. For example, `/var/log/weblm/weblmserver.log`.
log4j.appender.weblmDebugAppender.threshold	Debug	ERROR	Use this property to specify the log level. The log files contain log messages with levels you have specified in this property. The following are the log levels that you can assign in the increasing order of granularity: FATAL, ERROR, WARN, INFO, DEBUG. To change the log levels, the value of this property as well as the log level mentioned at the respective logger level must be changed.
log4j.appender.weblmOperationalAppender.threshold	Operational	ERROR	Use this property to specify the log level. The log files contain log messages with levels you have specified in this property. The following are the log levels that you can assign in the increasing order of granularity: FATAL, ERROR, WARN, INFO, DEBUG. To change the log levels, the value of this property as well as the log level mentioned at the respective logger level must be changed.
log4j.appender.weblmAuditAppender.threshold	Audit	INFO	Use this property to specify the log level. The log files contain log messages with levels you have specified in this property. The following are the log levels that you can assign in the increasing order of granularity: FATAL, ERROR, WARN, INFO, DEBUG.

Table continues…

Property Name	Logger Type	Default Value	Description
			To change the log levels, the value of this property as well as the log level mentioned at the respective logger level must be changed.
log4j.appender.weblmSecurityAppender.threshold	Security	WARN	Use this property to specify the log level. The log files contain log messages with levels you have specified in this property. The following are the log levels that you can assign in the increasing order of granularity: FATAL, ERROR, WARN, INFO, DEBUG. To change the log levels, the value of this property as well as the log level mentioned at the respective logger level must be changed.
log4j.appender.weblmDebugAppender.MaxFileSize	Debug	10 MB	Use this property to specify the maximum log file size before it is rolled over.
log4j.appender.weblmOperationalAppender.MaxFileSize	Operational	10 MB	Use this property to specify the maximum log file size before it is rolled over.
log4j.appender.weblmAuditAppender.MaxFileSize	Audit	10 MB	Use this property to specify the maximum log file size before it is rolled over.
log4j.appender.weblmSecurityAppender.MaxFileSize	Security	10 MB	Use this property to specify the maximum log file size before it is rolled over.
log4j.appender.weblmDebugAppender.MaxBackupIndex	Debug	5	Use this property to specify the number of log files to be backed up once it reaches the maximum size as specified in property: log4j.appender.<MaxFileSize>
log4j.appender.weblmOperationalAppender.MaxBackupIndex	Operational	3	Use this property to specify the number of log files to be backed up once it reaches the maximum size as specified in property: log4j.appender.<MaxFileSize>

Table continues…

Property Name	Logger Type	Default Value	Description
log4j.appender.weblmAuditAppender.MaxBackupIndex	Audit	3	Use this property to specify the number of log files to be backed up once it reaches the maximum size as specified in property: log4j.appender.<MaxFileSize>
log4j.appender.weblmSecurityAppender.MaxBackupIndex	Security	3	Use this property to specify the number of log files to be backed up once it reaches the maximum size as specified in property: log4j.appender.<MaxFileSize>

Updating the WebLM server memory

About this task

To handle more than five thousand license requests at a time, WebLM requires large memory. Perform the following procedure to update the memory settings of WebLM on VMware.

Procedure

1. Log in to the VMware vSphere client, and shut down the WebLM virtual machine.
2. Select the WebLM virtual machine, and right-click.

   If you cannot view the WebLM virtual machine, click **Home** > **Inventory** > **Hosts and Clusters**
3. Click **Edit Settings**.
4. In the Edit Settings or Virtual Machine Properties dialog box, select the **Hardware** tab and edit the **Memory Size** from 1 GB to 2 GB.
5. In the **Resources** tab, type `2048` in the text field.
6. Select **MB** from the drop-down list, and click **OK**.
7. In the left navigation pane, right-click the WebLM virtual machine.
8. In the context menu, click **Power On**.

Updating network parameters for cloned WebLM

About this task

If a WebLM virtual machine is cloned or exported to another host by using OVF tool, you cannot change the IP address of the cloned WebLM virtual machine instance by using the **`changeIPFQDN`** command immediately after cloning because the network interface is unavailable. Use the following procedure to update network parameters for cloned WebLM.

Before you begin

Deploy WebLM OVA on ESXi.

Procedure

1. Log on to the WebLM web interface and CLI, and ensure that the login is successful.
2. Power off the WebLM that you deployed.
3. Clone WebLM by using the following:
    a. Select the WebLM virtual machine.
    b. Right-click and select **Clone**.
    c. Ensure that the cloning is successful.
4. Power on the cloned WebLM virtual machine.
5. Perform the following to check the MAC address:
    a. Right-click the cloned WebLM virtual machine.
    b. Click **Edit Settings** > **Network Adapter 1** > **MAC Address**, and note the MAC address.
6. On the Console tab of VMware client, perform the following steps:
    a. Type the MAC address that you noted in the earlier step in the `/etc/sysconfig/network-scripts/ifcfg-eth0`.
    b. Update the required network parameters.
7. Power off the WebLM virtual machine.

    On the WebLM virtual machine, the eth0 turns on with the old IP address from the cloned WebLM virtual machine.
8. Restart the network services by using `/etc/init.d/network restart` utility.
9. Log on to the WebLM web interface, and ensure that the system displays the host ID.

Related links

VMware cloning on page 53

Chapter 7: Post Installation Verification

Verifying successful installation

Before you begin

Log on to the WebLM web console as an administrator.

About this task

You must perform the following verification procedure after you install the WebLM OVA file and configure WebLM.

Procedure

1. On the web browser, type `https://<FQDN or IP address of WebLM>:<port>/WebLM`.

   The system displays the WebLM web console.

   Note:

   WebLM uses the default port 52233.

2. Log on to the web console.

   If you log in as user admin, weblmadmin is the default password. Change the default password after the first login.

3. On the home page, click **About**.

   The system displays the About WebLM window with the build details.

4. Verify the version number of WebLM.

5. Click **Server Properties**.

6. Verify whether the new WebLM host ID is generated.

   The WebLM host ID has 12 alphanumeric characters. The host ID starts with the letter V.

Chapter 8: Maintenance

Maintenance

The maintenance chapter describes the procedures to change the WebLM IP address, FQDN, and other parameters from Command Line Interface (CLI). This chapter also provides information on performing backup, restore, snapshot backup and snapshot restore of WebLM.

Note:

The existing license files become invalid when you:

- change the WebLM IP address
- perform a WebLM upgrade
- clone a virtual machine
- install WebLM using a new OVA template

You require a new license file to match the new Host ID generated in the WebLM server.

Downloading the authentication file

About this task

To gain access to the Avaya RFA home page, in the Web browser, enter http://rfa.avaya.com

Procedure

1. Log in to the RFA home page.
2. Click **Start the AFS Application**.
3. On the license page, click **I Agree**.
4. In the **Product** field, select **SP System Platform/VE VMware**.
5. In the **Release** field, click **6.x**.
6. Click **Next**.
7. Click **New System - Product:SP System Platform Release: 6.x**.
8. Click **Next**.

9. In the **Enter the fully qualified domain name** field, retain the default value myhost.mydomain.com or leave the field blank.
10. Click **Download file to my PC** to download the authentication file to your computer.

    You can also click **Download file via email** to receive the file through email.

Related links

Installing the authentication file in WebLM on page 31

Installing the authentication file in WebLM

Before you begin

Download the authentication file from http://rfa.avaya.com.

Log in to the WebLM virtual machine as craft, init, inads, or admin to update the ASG file.

About this task

An Avaya Business partner or an Avaya representative provides the authentication file to the customer and the customer must install the authentication file during the deployment of the OVA file. Therefore, the Avaya Business partner or the Avaya APS representative must obtain and install the authentication file.

Procedure

1. Using WinSCP, copy the authentication file to the `/tmp` directory in the server.

   Note the exact name of the authentication file. For example, the file name can be AF-7000438702-121024-172934.xml.
2. Log in to WebLM as an administrator, and change the login user to superuser.
3. To reach the `tmp` directory, type `cd /tmp`.
4. Type `ls`.

   The system lists the authentication file, if present.
5. To load the authentication file, type **`loadauth -l <auth_file_path> —f`**.

   The **`loadauth`** command removes the password for the root user. After running this utility, you can access the root-only level as an ASG-enabled sroot user.

   `auth_file_path` is the complete path for the authentication file that you downloaded from RFA.

Related links

Downloading the authentication file on page 30

Changing the IP, FQDN, DNS, Gateway, or Netmask addresses

Before you begin

To reach the WebLM CLI, use one of the following methods:

- Open vSphere client and click the **Console** tab.
- Start an SSH session on the WebLM server.

Log in to the WebLM virtual machine using the login `admin`.

Procedure

Enter `changeIPFQDN —IP <IP Address> —FQDN <FQDN> —GATEWAY <Gateway address> —NETMASK <Netmask address> —DNS <DNS address> —SEARCH <search list for DNS> —NTP <NTP> —TIME ZONE <Time Zone>`.

Warning:

Do not change the IP address settings from VMware tools when WebLM is in the Power Off state.

Note:

After a WebLM IP/FQDN change, the licenses become invalid. You must re-host the licenses. The license data varies based on the installed license as part of the license re-host.

Related links

Rehosting license files on page 22
WebLM CLI operations on page 34
Updating network parameters for cloned WebLM on page 28
VMware cloning on page 53

Configuring multiple DNS IP addresses

Before you begin

- Deploy the WebLM OVA file.
- Start the WebLM virtual machine.

  When you turn on WebLM for the first time after you deploy the OVA file, the system applies the network configurations that you provided during the deployment of the WebLM OVA file.

Note:

The command to configure multiple DNS IP addresses overrides all the previous DNS IP address entries.

Procedure

1. Log in to the WebLM CLI as an administrator using the login admin.

   Important:

   Ensure that WebLM maintenance is not in progress.

2. Check the existing DNS IP address of WebLM.
3. To add more than one IP address for the DNS server, enter `changeIPFQDN -DNS primary_DNS_IPaddress, secondary_DNS_IPaddress, DNS_N_IPadress....” to “changeIPFQDN -DNS primary_DNS_IPaddress, secondary_DNS_IPaddress, ..., DNS_N_IPadress`.

   You must separate each DNS IP address by a comma (,). For example, `changeIPFQDN -DNS 148.147.162.2,148.147.163.5`.

   The system takes a few seconds to apply the DNS changes to the network.

4. Log in to the WebLM console as an administrator.
5. Ensure that the system displays the multiple DNS IP addresses.

Related links

WebLM CLI operations on page 34

Configuring the time zone

Before you begin

To gain access to the WebLM CLI, use one of the following methods:

- Open the vSphere client, and click the **Console** tab.
- Start an SSH session on the WebLM server.

Log in to the WebLM virtual machine using the login `admin`.

Procedure

1. Type `configureTimeZone`.
2. Select the time zone from the list.

   For example, America/Denver.

Related links

WebLM CLI operations on page 34

Configuring the NTP server

Before you begin

To gain access to the WebLM CLI, use one of the following methods:

- Open the vSphere client, and click the **Console** tab.
- Start an SSH session on the WebLM server.

Log in to the WebLM virtual machine as `admin`.

Procedure

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

The system configures the NTP server.

Related links

WebLM CLI operations on page 34

WebLM CLI operations

#	Command	Parameters	Description	Usage
1.	**`changeIPFQDN`**	• IP < new IP address for WebLM > • FQDN < new fully qualified domain name of WebLM > • GATEWAY < new gateway address for WebLM > • NETMASK < new netmask address for WebLM > • DNS < new DNS address for WebLM > • SEARCH < new search list for DNS addresses >	Updates the 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 WebLM > -SEARCH < new search list for DNS addresses >
2.	**`configureNTP`**	< IP address of the NTP server >	Configures the NTP server details.	configureNTP < IP address of the NTP server > Separate the IP addresses or the host

Table continues…

#	Command	Parameters	Description	Usage
				names of the NTP servers with commas (,).
3.	**`configureTimeZone`**	< Time zone that you want to select >	Configures the time zone with the value that you select.	configureTimezone Select a time zone. For example, America/ Denver
4.	**`loadauth`**	<absolute path to the ASG XML file>	Updates the ASG XML file.	updateASG < absolute path to the ASG XML file >
5.	**`WebLMPatchdeploy`**	< absolute path to the WebLM service pack, feature pack, or the software patch >	Installs the software patch, the service pack, or the feature pack for WebLM.	WebLMPatchdeploy <absolute path to `home/ admin/< WebLM FeaturepackName >` **Note:** Copy the WebLM feature pack or patches that you install to `/home/ admin/`.
6.	**`weblm_password`**	<reset> <restore>	Reset option backs up the existing user configuration and applies the predefined password. Restore option restores the backed-up user configuration. The utility also supports the non-root user, such as admin.	weblm_password `reset` weblm_password `restore`

Resetting the WebLM password through CLI

Before you begin

To reach the WebLM CLI, use one of the following methods:

- Open vSphere client, and click the **Console** tab.
- Start an SSH session on the WebLM server.

Log in to the WebLM virtual machine as an administrator.

Procedure

Enter the **`weblm_password <reset|restore>`** command.

Using password reset you can back up the existing user configuration and apply the predefined password. By resetting the password, you can restore the backed up configuration.

Performing WebLM backup

Procedure

1. Log in to the WebLM CLI as an administrator.
2. Perform one of the following actions:
   - Enter **`WebLMBackup <backup_location>`** and provide the backup location as a parameter. In this case, the WebLM backup is stored at the location you specify as a parameter.
   - Enter **`WebLMBackup`**. In this case, the backup location is not provided, and the WebLM backup is stored at the default location. You can edit the default location using the conf.properties file.

   Copy the backup files to a remote computer or to an external storage device.

   You can also use a simple SFTP client to perform a remote backup.

Performing WebLM restore

Procedure

1. Log in to the WebLM CLI as an administrator.
2. Perform one of the following depending on your restore requirement:
   - Enter **`WebLMRestore full <backup_location>`** to restore all the WebLM files by picking up the backup file at the specified location.
   - Enter **`WebLMRestore full`** to restore all the WebLM files by picking up the backup file at the default location specified in conf.properties.
   - Enter **`WebLMRestore selective <backup_location>`** to restore a set of files necessary for the functionality of the WebLM server from the specified backup location.
   - Enter **`WebLMRestore selective`** to restore a set of files necessary for the functionality of the WebLM server from the default location specified in conf.properties.

     Note:

     The conf.properties file is located at `/opt/vsp/conf.properties`. You can modify the default location of the backup files through the conf.properties file.

Creating a snapshot backup

About this task

Important:

Do not perform any activity on WebLM until the snapshot backup is complete.

To create the snapshot backup, use the vCenter client or the vSphere client.

Procedure

1. From the list of virtual machines, right-click the required WebLM virtual machine, and select **Snapshot**.
2. Click **Take Snapshot**.
3. In the **Name** and **Description** fields, enter a name and the description for the snapshot.
4. Set the following Snapshot options:
   a. Enable **Snapshot the virtual machine's memory**.
   b. Enable **Quiesce guest file system (Needs VMware Tools installed)**.

      Note:

      Quiescing indicates pausing or altering the state of running processes, particularly the processes that might modify the information stored on disk during a backup. Quiescing ensures a consistent and usable backup.
5. Click **OK**.
6. In the Recent Tasks window, ensure that the status of the **Create virtual machine snapshot** task is **Completed**.

Creating a snapshot restore

About this task

Important:

Do not perform any activity on WebLM until the snapshot restore is complete.

Performing the VMware snapshot restore is not the same as application specific restore.

To restore the snapshot backup, use the vCenter client or the vSphere client.

Procedure

1. From the list of virtual machines, select the deployed WebLM virtual machine, and right-click and select **Snapshot**.
2. Open **Snapshot Manager**.

3. Select the snapshot version that you want to restore.
4. Click **Go to**.
5. In the Recent Tasks window, verify whether the **Status** of the **Revert snapshot** task is **Completed**.

Installing a WebLM patch, feature pack, or service pack

Before you begin

- Ensure that you have configured `/etc/hosts` with the WebLM IP address.
- Create a snapshot backup for WebLM.
- Copy the patch file, feature pack file, or the service pack file to the WebLM virtual machine.
- Do one of the following to go to the WebLM CLI:
  - Open the vSphere client, and click the Console tab.
  - Start an SSH session on the WebLM server.
- To check the installed WebLM version, type `swversion`.

  The system displays the version details. For example:

  ```
  ************************************************
  StandAlone WebLM Software Information
  ************************************************
  Standalone WebLM on VMware 7.0.0 Build Number 7.0.4.6790 Patch 7.0.1
  Build Number 7.0.1.1.21002
  ```

Procedure

1. Log in to the WebLM virtual machine as an administrator.
2. Perform a WebLM backup.
3. Verify that the MD5 checksum of the patch that you install is MD5Sum - bf940aa02d1e641c2117cf173a8be1a1.
4. Type `WebLMPatchdeploy <absolute path to the WebLM feature pack file>`.

   For example, `<absolute path to the WebLMFeaturePack VEWebLM_7.0.1.0_xxx.bin>`.

   The system installs the patch file.
5. Restart the standalone WebLM.
6. Perform a WebLM restore.

   If the patch or service pack installation fails, perform a snapshot restore to go to the previous version of WebLM.

Upgrading WebLM to Release 7.0.1

About this task

WebLM supports the following upgrade paths:

- Release 6.2.x, VE 1.0, to Release 7.0.1
- Release 6.3.x, VE 2.0, to Release 7.0.1

Though upgrade is supported, you must regenerate the license files because the host ID changes.

Procedure

1. Log in to the WebLM virtual machine as administrator.
2. Create a backup of WebLM.
3. Ensure that you copy the backup to a remote computer or to an external storage device, such as DVD.
4. Turn off the power on the existing WebLM virtual machine.
5. Deploy the WebLM Release 7.0 OVA.
6. Perform a restore of WebLM.
7. Verify that the upgrade is successful, and WebLM is operational.
8. Install the WebLM Release 7.0.1 feature pack.
9. Delete the previous version of the WebLM virtual machine.

Next steps

Rehost the license file only after you perform the WebLM restore.

When you rehost licenses, the system resets the license data, such as license usage data.

Chapter 9: 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	Use this document to:	Audience
Overview		
Avaya Aura® Virtualized Environment Solution Description	Understand the high-level solution features and functionality	Customers and sales, services, and support personnel
Implementing		
Deploying Avaya Aura® applications	Deploy the Avaya Aura® applications with Solution Deployment Manager	Implementation personnel
Administering		
Administering Avaya Aura® standalone WebLM	Perform administration tasks	System administrators
Using		
Using the Solution Deployment Manager client	Deploy Avaya Aura® applications and install patches on Avaya Aura® applications.	System administrators

Related links

Finding documents on the Avaya Support website on page 40

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.

5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Related links

Documentation on page 40

Training

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

Course code	Course title	Type
2007V/W	What is New in Avaya Aura® Release 7.0.1	AvayaLive™ Engage Theory
2008V/W	What is New in Avaya Aura® Application Enablement Services 7.0	AvayaLive™ Engage Theory
2009V/W	What is New in Avaya Aura® Communication Manager 7.0	AvayaLive™ Engage Theory
2010V/W	What is New in Avaya Aura® Presence Services 7.0	AvayaLive™ Engage Theory
2011/V/W	What is New in Avaya Aura® Session Manager Release 7.0.1 and Avaya Aura® System Manager Release 7.0.1	AvayaLive™ Engage Theory
2012V	Migrating and Upgrading to Avaya Aura® Platform 7.0	AvayaLive™ Engage Theory
2013V	Avaya Aura® Release 7.0.1 Solution Management	AvayaLive™ Engage Theory
1A00234E	Avaya Aura® Fundamental Technology	AvayaLive™ Engage Theory
1A00236E	Knowledge Access: Avaya Aura® Session Manager and Avaya Aura® System Manager Fundamentals	AvayaLive™ Engage Theory
5U00106W	Avaya Aura® System Manager Overview	WBT Level 1

Table continues…

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

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

    Note:

    Videos are not available for all products.

Support

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

Appendix A: Best practices for VM performance and features

BIOS

For optimal performance, turn off power saving server options. See the technical data provided by the manufacturer for your particular server regarding power saving options.

For information about how to use BIOS settings to improve the environment for latency-sensitive workloads for an application, see the technical white paper at http://www.vmware.com/files/pdf/techpaper/VMW-Tuning-Latency-Sensitive-Workloads.pdf.

The following sections describe the recommended BIOS settings for:

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

Related links

Intel Virtualization Technology on page 44
Dell PowerEdge Server on page 45
HP ProLiant Servers on page 45

Intel Virtualization Technology

Intel CPUs require EM64T and Virtualization Technology (VT) support in the chip and in the BIOS to run 64–bit virtual machines.

All Intel Xeon processors include:

- Intel Virtualization Technology
- Intel Extended Memory 64 Technology
- Execute Disable Bit

Ensure that VT is enabled in the host system BIOS. The feature is also known as VT, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions.

Note:

The VT setting is locked as either **On** or **Off** when the server starts. After enabling VT in the system BIOS, save your changes to the BIOS settings and exit. The BIOS changes take effect after the host server reboots.

Other suggested BIOS settings

Servers with Intel Nehalem class and newer Intel Xeon CPUs offer two more power management options: C-states and Intel Turbo Boost. These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell and HP servers are described in the following sections. Other server models might use other terminology for the same BIOS controls.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to a fully active state.
- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power. The default for this option is **enabled**. Do not change the default.

Related links

BIOS on page 44

Dell PowerEdge Server

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

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

Related links

BIOS on page 44

HP ProLiant Servers

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

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

Related links

BIOS on page 44

VMware Tools

The VMware Tools utility suite is built into the application OVA. The tools enhance the performance of the guest operating system on the virtual machine and improve the management of the virtual machine.

VMware tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing

For more information about VMware tools, see *Overview of VMware Tools* at http://kb.vmware.com/kb/340.

Important:

Do not upgrade the VMware tools software that is packaged with each OVA unless instructed to do so by Avaya. The supplied version is the supported release and has been thoroughly tested.

Timekeeping

For accurate timekeeping, use the Network Time Protocol (NTP) as a time source instead of the ESXi hypervisor.

The NTP servers can be local or over the Internet. If the NTP servers are on the Internet, the corporate firewall must open UDP port 123 so that the NTP service can communicate with the external NTP servers.

The VMware tools time synchronization method is disabled at application deployment time to avoid dueling clock masters. You must configure the NTP service first because the applications are not receiving clock updates from the hypervisor. To verify that VMware Tools Timesync is disabled, run the command `/usr/bin/vmware-toolbox-cmd timesync status`.

In certain situations, the ESXi hypervisor pushes an updated view of its clock into a virtual machine. These situations include starting the virtual machine and resuming a suspended virtual machine, If this view differs more than 1000 seconds from the view that is received over the network, the NTP service might shutdown. In this situation, the guest OS administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest operating system. The VMware recommendation is to add **tinker panic 0** to the first line of the **ntp.conf** file so that the NTP can adjust to the network time even with large differences.

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

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

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

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

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

VMware networking best practices

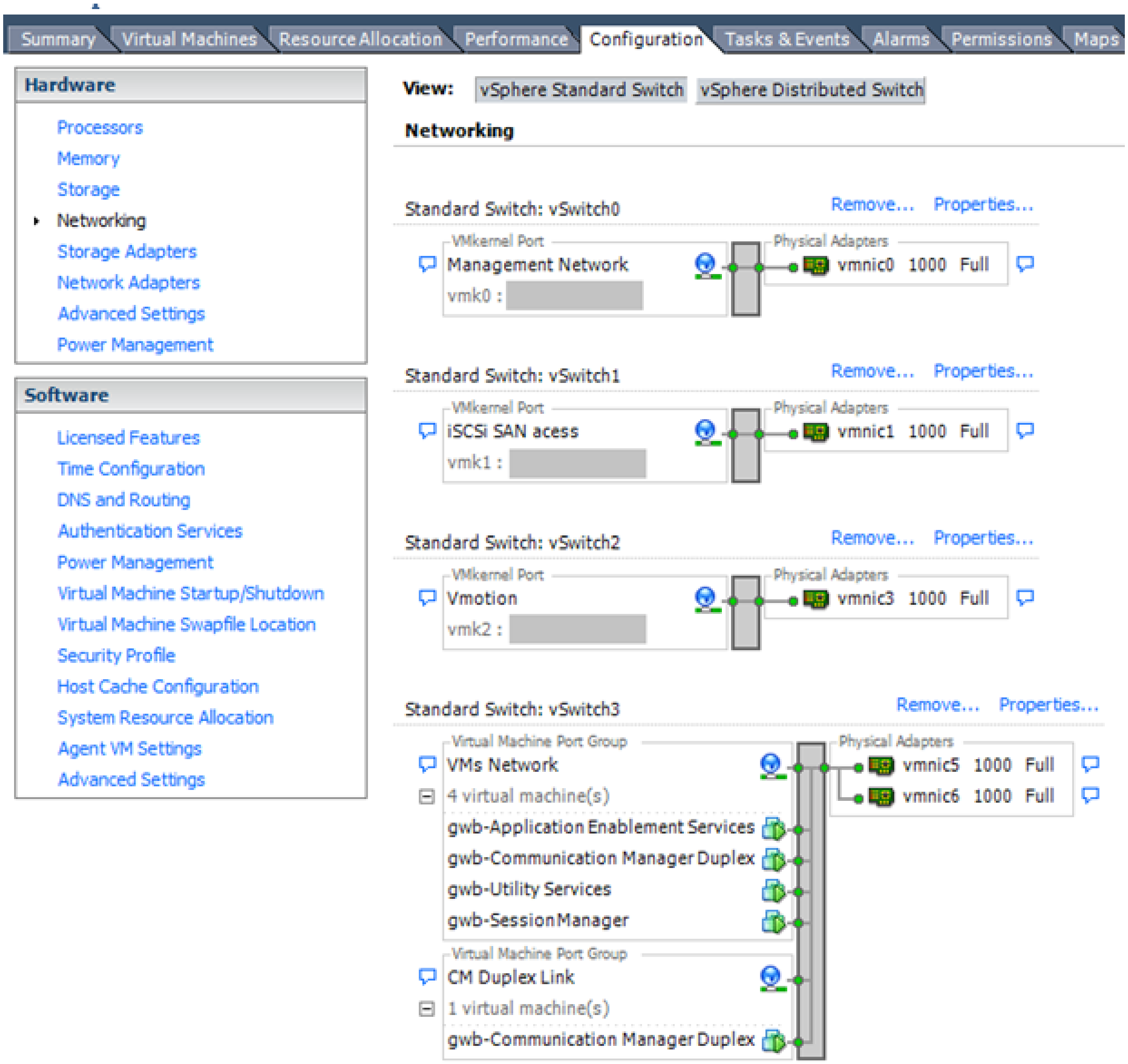
You can administer networking in a VMware environment for many different configurations. The examples in this section describe some of the VMware networking possibilities.

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

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

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

Networking Avaya applications on VMware ESXi – Example 1



Standard Switch: vSwitch0

VMkernel Port: Management Network, vmk0 :

Physical Adapters: vmnic0 1000 Full

Standard Switch: vSwitch1

VMkernel Port: iSCSi SAN acess, vmk1 :

Physical Adapters: vmnic1 1000 Full

Standard Switch: vSwitch2

VMkernel Port: Vmotion, vmk2 :

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

Virtual Machine Port Group: CM Duplex Link

1 virtual machine(s)

gwb-Communication Manager Duplex

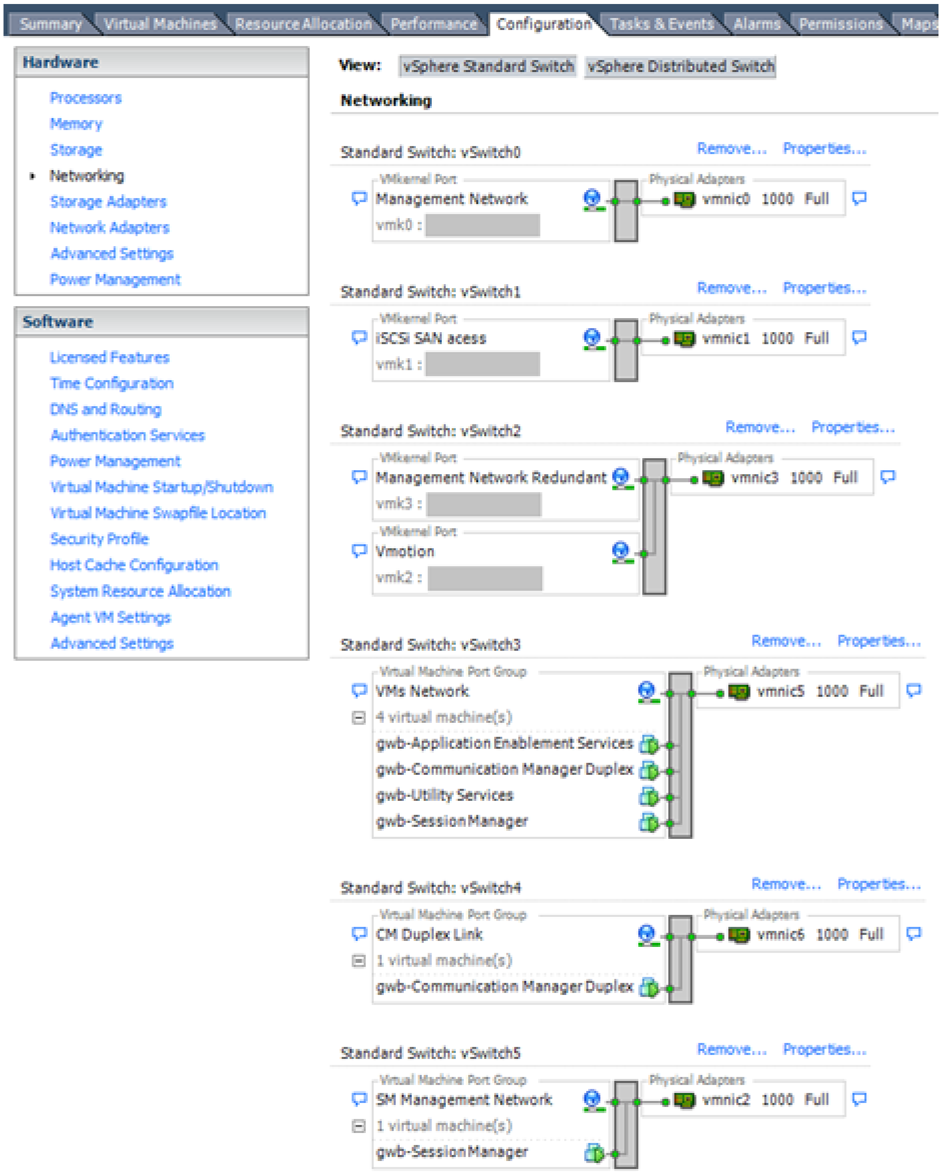
Physical Adapters: vmnic5 1000 Full; vmnic6 1000 Full

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



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® 5.5	http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf
Performance Best Practices for VMware vSphere® 6.0	http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf
VMware vSphere 5.5 Documentation	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html
VMware vSphere 6.0 Documentation	https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html
VMware Documentation Sets	https://www.vmware.com/support/pubs/

Storage

When you deploy WebLM in a virtualized environment, observe the following set of storage recommendations:

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

- Thin provisioned disks can grow to the full size specified at the time of virtual disk creation, but do not shrink. Once the blocks have been allocated, they cannot be un-allocated.
- By implementing thin provisioned disks, you are able to over-allocate storage. If storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked.

- If a guest operating system needs to make use of a virtual disk, the guest operating system must first partition and format the disk to a file system it can recognize. Depending on the type of format selected within the guest operating system, the format may cause the thin provisioned disk to grow to full size. For example, if you present a thin provisioned disk to a Microsoft Windows operating system and format the disk, unless you explicitly select the Quick Format option, the Microsoft Windows format tool writes information to all sectors on the disk, which in turn inflates the thin provisioned disk to full size.

VMware Snapshots

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

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

⚠ **Caution:**

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

Snapshots can:

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

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

- Do not rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- Do not run a virtual machine from a snapshot. Do not use a single snapshot for more than 24 to 72 hours.
- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.
- When taking a snapshot, do not save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual

machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user. To create a clean snapshot image from which to boot, do the following when you create a snapshot:

  - In the **Take Virtual Machine Snapshot** window, clear the **Snapshot the virtual machine's memory** check box.
  - Select the **Quiesce guest file system (Needs VMware Tools installed)** check box to ensure that all write instructions to the disks are complete. You have a better chance of creating a clean snapshot image from which to boot.

- If you are going to use snapshots for a long time, you must consolidate the snapshot files regularly to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

  Note:

  If a consolidation failure occurs, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, the system displays a warning on the user interface.

Related resources

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

VMware vMotion

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

With vMotion, you can:

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

Before using vMotion, you must:

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

Note:

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

VMware cloning

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

Note:

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

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

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

Related links

Updating network parameters for cloned WebLM on page 28

VMware high availability

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

Note:

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

Glossary

AFS

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

Appliance Virtualization Platform

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements.

Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware® tools, such as vCenter and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.

Application

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

Avaya Appliance

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

Blade

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

ESXi

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

Hypervisor

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

MAC

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

OVA

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

PLDS

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

Reservation

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

RFA

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

SAN

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

Snapshot

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

Storage vMotion

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

vCenter Server

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

virtual appliance

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

VM

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

vMotion

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

VMware HA

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

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

Index