Avaya WebLM using VMware® in the Virtualized Environment Deployment Guide

Release 6.2
Issue 1
November 2012

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its 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 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 its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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. “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.

Licence types

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, 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, or hardware provided by Avaya. All content on this site, the documentation 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 that 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”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, 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 Aura® Virtualized Environment. The document includes installation, configuration, installation verification, troubleshooting, and basic maintenance checklists and procedures.

Intended audience

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.

Related resources

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Visit the Avaya Mentor Videos website at Avaya Mentor Videos and enter **virtual appliance** in the **Search channel** field to view the list of available videos.

You can also enter the application product name to view videos that are available for a particular product.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. On the Avaya Support website at http://support.avaya.com, search for notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to get answers to questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

Chapter 2: Architecture overview

Avaya Aura® Virtualized Environment overview

Traditionally, Avaya Aura® has been sold and installed as an individual appliance within customer networks to offer collaboration capabilities and business advantages. Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® virtualized server architecture. Virtualized Environment provides the following benefits:

- simplifies IT management by providing common software administration and maintenance.
- requires fewer servers and racks which reduces the footprint.
- lowers power consumption and cooling requirements.
- enables capital equipment cost savings.
- lowers operational expenses.
- uses standard operating procedures for both Avaya and non-Avaya products.
- satisfies customer demand for Avaya products in a virtualized environment on customer-specified servers and hardware.
- enables business to scale rapidly to accommodate growth and to respond to changing business requirements.

For existing customers who have a VMware IT infrastructure, Avaya Aura® Virtualized Environment provides an opportunity to 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 to 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 is only for VMware and is not intended to include any other industry hypervisor. Virtualized Environment is inclusive of the Avaya Aura® portfolio.

Note:

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

- server and host
- reservations and configuration values

Virtualized Environment applications

The Virtualized Environment supports the following Avaya products:

- Avaya Aura® Communication Manager Release 6.2 (Simplex & Duplex)
- Avaya Agile Communication Environment™ Release 6.2 (ACE)
- Avaya Aura® Application Enablement Services Release 6.2 (AES)
- WebLM Standalone Release 6.2 (WebLM)
- Secure Access Link Release 2.2 (SAL)
- Avaya Aura® System Manager Release 6.2 (SMGR)
- Avaya Aura® Presence Services Release 6.1 (PS)
- Avaya Aura® Session Manager Release 6.2 (SM)
- Avaya Aura® Utility Services Release 6.2 (US)

Customer deployment

Deployment into the blade, cluster, and server is managed by vCenter or vSphere.

The customer provides the servers, the virtual appliances, the hardware, and the VMware infrastructure including the VMware licenses.

Software delivery

The software is delivered as a pre-packaged Open Virtualization Application (OVA) file posted on the Avaya Product Licensing and Download System (PLDS). The OVA contains the following components:

- the application software and operating system.
- pre-installed VMware tools for deployment on VMware ESXi 5.0.
- preset configuration details for
  - RAM and CPU reservations and storage requirements
  - Network Interface Card (NIC)
  - other settings

Patches and upgrades

A minimum patch level can be required for each supported application. See the Compatibility Matrix at Compatibility Matrix for more information regarding the application patch requirements.

Important:

Do not update the VMware tools software which 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 template is built with configuration values which optimize performance and follow recommended Best Practices.

Caution:

Modifying these values can have a direct impact on the performance, capacity, and stability of the virtual machine. It is the responsibility of the customer to understand the aforementioned impacts when changing configuration values. Avaya Global Support Services (GSS) may not be able to assist in fully resolving a problem if the resource allocation has been changed for a virtual application. Avaya GSS could require the customer to reset the values to the optimized values before starting to investigate the issue.

VMware components

VMware 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	The client application that is installed on a personal computer or accessible through a Web interface. It connects to a vCenter server or directly to an ESXi server in the case where vCenter is not used. Enables the installation and management of virtual machines.
vCenter	vCenter provides centralized control and visibility at every level of the virtual infrastructure. Virtual machines are managed through vSphere client software which provides alarming and performance monitoring of ESXi hosts and virtual machines.

Deployment guidelines

The high-level deployment steps are:

1. Deploy the OVA.
2. Configure the application/system.
3. Verify the installation.

The following are deployment guidelines for the virtual appliances:

- Deploy the virtual appliances on the same host as possible, depending on host size and VMs.
- Deploy the virtual appliances on the same cluster if it goes beyond the host boundary.
- Segment redundant elements on a different cluster. For example, Communication Manager duplication pair.
- Create a tiered or segmented cluster infrastructure that isolates critical applications, such Avaya Aura®, from other VMs.
- Ensure that you have enough resources for rainy day scenarios or conditions. Resources may only be configured for traffic or performance on an average day.
- Do not over-subscribe resources. Over-subscribing affects performance.
- Monitor the blade, host, and virtual appliance performance.

Important:

The values for performance, occupancy, and use can vary greatly. The blade may be running a 5% occupancy, but a VM may be running at 50%. Note that some VMs will behave differently at a higher CPU usage.

Chapter 3: Planning and configuration

Server hardware and resources

The server must be listed in the VMware Hardware Compatibility Guide. Go to http://www.vmware.com/resources/guides.html to see the list of certified servers.

Virtualized Environment requires VMware-certified servers to be running ESXi 5.0 and its updates. Releases prior to 5.0 are not supported and 5.1 is not supported.

Customer configuration data

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

Important:

Currently, the system does not support special characters such as - in passwords. Password characters are restricted to uppercase letters, lowercase letters, and numbers only.

Required data	Value for the system	Example value
IP address	IP address for the management interface	172.16.100.239
Hostname	The linux hostname. The hostname must be a fully qualified domain name	abc.mydomain.com
Netmask	The network address mask	255.255.255.0
Default Gateway	The default network traffic gateway	172.16.100.1
DNS IP Address	The IP address of the primary DNS server	172.16.100.100
Default Search List		myorg

WebLM vAppliance minimum resource requirements

The following tables give the minimum resource requirement you require for deploying WebLM through VMware.

WebLM server vAppliance minimum resource requirements

VMWare resource	Value
vCPU	1
CPU reservation	2400 MHz
CPU speed	2.4 GHz
Memory reservation	1GB
Storage reservation	30GB
Shared NIC(s)	1

Software versions

Application	Version
VMware vCenter Server	5.0.0, 455964
VMware vSphere Client	5.0.0, 469512
VMware ESXi Host	5.0.0, 469512
WebLM	6.2 GA version
OS	CentOS - hardened and packaged as part of the ova file.

Chapter 4: Deploying the WebLM OVA

Methods of WebLM OVA file deployment

- Deploying WebLM using vSphere. For more information, see Deploying the WebLM server using vSphere on page 16
- Deploying WebLM using vCenter. For more information, see Deploying the WebLM server using vCenter on page 16

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/		
2.	Install the vSphere 5.0 client.		
3.	Keep the network configuration data handy.	Customer configuration data on page 13	
4.	Deploy the WebLM OVA file.	Deploying the WebLM server using vSphere on page 16 Deploying the WebLM server using vCenter on page 16	
5.	Start the WebLM virtual machine.	Starting the WebLM server virtual machine on page 17	
6.	Verify the installation of the WebLM virtual machine.		

Deploying the WebLM server through vSphere

Before you begin

Download the vSphere client.

Procedure

1. Log in to the ESXi host.
2. Select the target Host ESX server.
3. From the **Client** menu, select **File**.
4. 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.
5. Click **Next**.
6. Read through the End User License Agreement page, and click **Accept**.
7. Confirm the OVF Template Details, and click **Next**.
8. Choose a **Name and Location** for the WebLM virtual machine, and click **Next**.
9. Select **a destination storage for the virtual machine files:**, and click **Next**.
10. Select **Thick Provision Lazy Zeroed**, and click **Next**.
11. Review the deployment settings, and click **Finish**.
12. Start the virtual machine.
13. At the system prompt enter the network parameters.
14. Confirm the network parameters. Press `n` to reenter the values.

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

Deploying the WebLM server using 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. On the client, select **File** > **Deploy OVF template**.
4. 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** and navigate to the OVA file from the local computer, network share, CD-ROM, or DVD. Click **Open**.
5. On the OVF Template Details page, verify the details and click **Next**.
6. Read through the End User License Agreement page, click **Accept** > **Next**.
7. In the **Name** field, enter the name of the virtual machine, and click **Next**.
8. On the Disk Format page, click **Thick Provisioned Lazy Zeroed**.
   The system displays the data store you selected and the available space.
9. Click **Next**.
10. On the Properties page, enter the network parameters, and click **Next**.
11. Review the settings, and click **Finish**.
    If you want to boot the WebLM server immediately after installation, select **Power on after deployment**.

Starting the WebLM server virtual machine

Procedure

1. Select the WebLM server virtual machine you have deployed from the list of virtual machines for the target host.
2. Click **Power On**.
3. If you deploy WebLM through vSphere, enter the network parameters at the system prompt.
4. Confirm the network parameters. Press `n` to reenter the values.
   The WebLM boot up sequence continues and configuration starts.
5. With the deployed WebLM server virtual machine in the selected state, right click and select **Open Console**.

The WebLM server virtual machine starts.

Note:

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

Chapter 5: VMware Best Practices for performance

The following sections describe the Best Practices for VMware performance and features.

BIOS

For details on BIOS settings to improve the environment for latency-sensitive workloads for an application, see the *Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs* technical white paper at http://www.vmware.com/files/pdf/techpaper/VMW-Tuning-Latency-Sensitive-Workloads.pdf.

The following are examples of the best performance BIOS settings for a few specific servers. Similar changes are needed to the BIOS settings of your server to enhance performance. Please consult the manufacturer technical data for your particular server.

Intel Virtualization Technology support

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 feature:

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

Ensure that VT is enabled in the host system BIOS. The feature may be called VT, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions.

Note:

The VT setting is locked (either on or off) at boot time. After enabling VT in the system BIOS, save your changes to the BIOS settings and exit. The host server will reboot, and the BIOS changes will take effect.

Other suggested BIOS settings

Servers with Intel Nehalem class and newer Intel Xeon CPUs also offer two power management options: C-states and Intel Turbo Boost.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to full power on.
- 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 make and models may have other terminology but equivalent BIOS controls.

Dell PowerEdge Servers — BIOS settings

When the Dell server starts, you select F2 to display the system setup options. The following are the recommended BIOS settings for the Dell PowerEdge servers:

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

HP ProLiant Servers — BIOS settings

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

VMware Tools are included as part of the application OVA. The tools are a suite of utilities that enhances the performance of the guest operating system on the virtual machine and improves the management of the virtual machine.

The tools provide:

- VMware Network acceleration
- Host to Guest time synchronization
- Disk sizing
- Startup/Shutdown

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

Important:

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

Time keeping

Linux guests should use the Network Time Protocol (NTP) as a time source, rather than the ESXi hypervisor, for accurate time keeping.

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

VMware tools time synchronization 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 VMware Tools Timesync is **Disabled**, run the command **/usr/bin/vmware-toolbox-cmd timesync status**.

In special situations, such as powering up the virtual machine, after vMotion, and after resuming a suspended virtual machine, the ESXi hypervisor will push an updated view of its clock into a virtual machine. If this view is very different from that received over the network (over 1000 seconds), the NTP service might not adjust to the network time and shutdown. In this situation, the guest 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. 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 in setting the NTP configuration, you must configure the Domain Name Service in the guest before administering the NTP service. Otherwise, the NTP service will not be able to locate the time servers. If the NTP service is administered 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 to verify the NTP service is getting time from a network

time source. The results indicate which network time source is being used, how close the guest is to the network time, and how often the guest checks the time. The guest polls the time source between every 65 and 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 seems to be consistently wrong, look through the system log for entries regarding **ntpd**. The NTP service writes the activities it performs to the log, including when it loses synchronization with a network time source.

For more information, see *Timekeeping best practices for Linux guests* at http://kb.vmware.com/kb/1006427. The article presents best practices for Linux timekeeping. These recommendations include specifics on the particular kernel command line options to use for the Linux operating system of interest. There is also a description of the recommended settings and usage for NTP time sync, configuration of VMware Tools time synchronization, and Virtual Hardware Clock configuration to achieve best timekeeping results.

VMware networking best practices

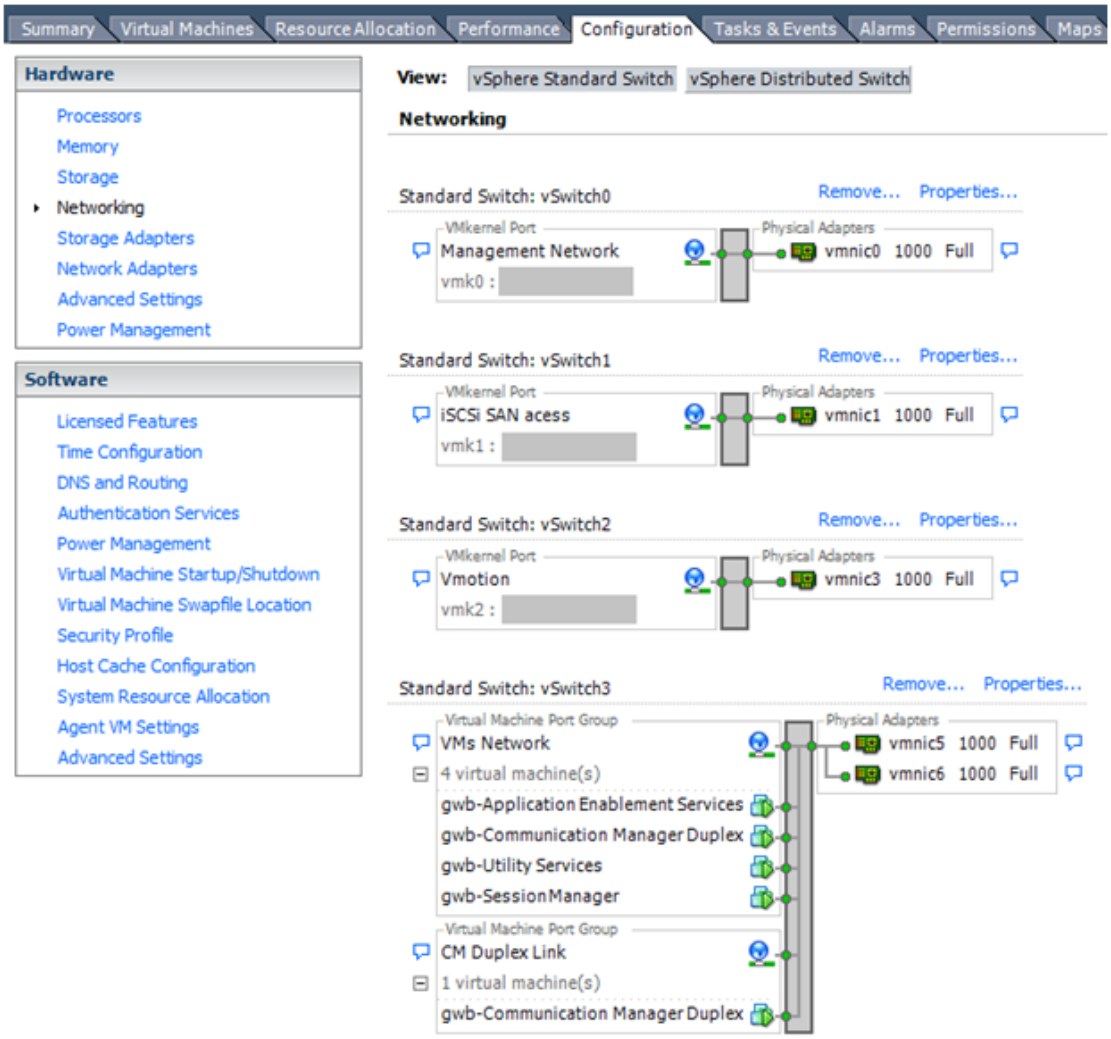
You can administer networking in a VMware environment for many different configurations. The information in this section provides a few of the examples of the VMware networking possibilities. These examples are not the only supported networking configurations, and implement several best practices and recommendations from Avaya's perspective.

This section is not a substitute for the actual VMware documentation. If you do not have experience networking with VMware, you must 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 supporting applications deployed on VMware Hosts:

- Separate network services to achieve greater security and performance. Create a vSphere standard or distributed switch with dedicated NICs for each service. If separate switches are not possible, consider port groups with different VLAN IDs.
- The vMotion connection must be located on a separate network devoted to vMotion.
- To protect sensitive VMs, deploy firewalls in the VM that route between virtual networks with uplinks to physical networks and pure virtual networks with no uplinks to physical networks.
- Specify VM NIC hardware type **vmxnet3** for best performance. Avaya OVA files are built using **vmxnet3** by default.
- All physical NICs that are connected to the same vSphere standard or distributed switch must be connected to the same physical network.
- Configure all VMkernal vNICs to the same MTU (IP Maximum Transmission Unit).

Networking Avaya applications on VMware ESXi — Example 1



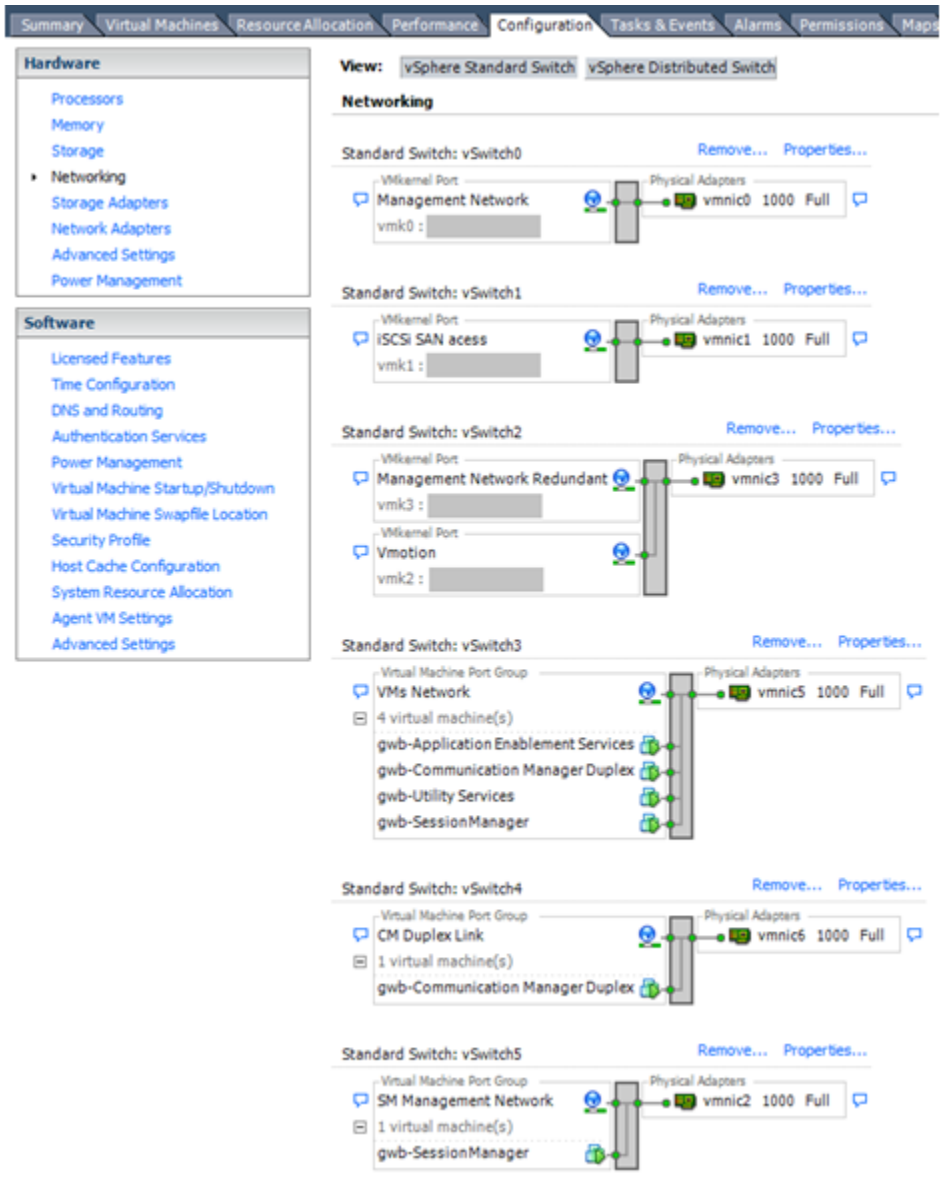
This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

- Separation of networks: VMware Management, VMware vMotion, iSCSI (SAN traffic), and VM 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 VMs Network. Load balancing provides additional bandwidth for the VMs Network, while also providing network connectivity for the virtual machines in the case of a single NIC failure.
- Communication Manager Duplex link: Communication Manager software duplication must be separated from all other network traffic. There are several methods of doing this, but Example 1 displays separating Communication Manager Duplex with a port group combined with a VLAN. The Communication Manager software duplication link must meet specific network requirements, detailed in Avaya PSN003556u at PSN003556u. Communication Manager software duplex connectivity minimum requirements are defined as:

  - 1 Gbps total capacity, or greater, with 50 Mbps of reserved bandwidth for duplication data.
  - 8 ms round-trip delay, or less.
  - 0.1% round-trip packet loss, or less.
  - Both servers duplication ports are on the same IP subnet.
  - Duplication link encryption must be disabled for busy-hour call rates that result in 9 greater than 40% CPU occupancy (`list measurements occupancy`, Static + CPU occupancy).
  - CPU occupancy on the active server (Static + CPU) must be maintained at less than 65% to provide memory refresh from the active to standby server.

- Session Manager vNIC mapping: The Session Manager OVA defines four separate virtual NICs within the VM. However, this example shows all of those interfaces networked 15 through a single virtual machine network, which is supported. If the Session Manager Management and Session Manager Asset networks are separated by subnets, it is possible to create a VLAN for the appropriate network.
- Virtual networking: Virtual machines which connect to the same vSwitch, as is the case in VMs Network of vSwitch 3, can communicate without ever entering the physical network. In other words, the network connectivity between these VMs is purely virtual. Virtual networks benefit from faster communication speeds and lower management overhead.

Networking Avaya applications on VMware ESXi — Example 2



This configuration shows a more complicated situation of using more available physical network interface cards. Highlights which differ from Example 1 include:

- VMware Management Network redundancy: In this example, a second VMkernel Port has been added to 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 VMs Network: This example removes the teamed physical NICs on vSwitch3, which was providing more bandwidth and tolerance of a single NIC failure in favor of reallocating this NIC to other workloads.
- Communication Manager Duplex Link: vSwitch4 has been dedicated to Communication Manager Software Duplication. The physical NIC given to vSwitch4 is on a separate

physical network, which still follows the requirements described in PSN003556u at PSN003556u.

- Session Manager Management Network: This example also shows the Session Manager Management network separated onto its own vSwitch, including a dedicated physical NIC which physically segregates the Session Manager Management network from other network traffic.

References

Title	Link
Product Support Notice — PSN003556u	PSN003556u
Performance Best Practices for VMware vSphere™ 5.0	Performance Best Practices for VMware vSphere™ 5.0
VMware vSphere 5.0 Basics	VMware vSphere Basics - ESXi 5.0

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

The general recommendation is to deploy thick disks which are *lazy-zeroed*. A lazy-zeroed thick disk has all of the space allocated at the time of creation, but each block is zeroed only on the first write. The result is a shorter creation time but reduced performance the first time a block is written.

Some configurations require *eager-zeroed* thick disks. An eager-zeroed thick disk

- has all space allocated and zeroed out at the time of creation.
- increases the time it takes to create the disk.
- results in the best performance, even on the first write to each block.

Thin provisioned disks:

- can grow to the full size specified at the time of the virtual disk creation but do not shrink. The blocks cannot be unallocated after the blocks have been allocated.
- can over-allocate storage. If the storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked.

You can use thin provisioned disks, but you must use strict control and monitoring to maintain adequate performance and ensure that storage is not completely consumed. If operational procedures are in place to mitigate the risk of performance and storage depletion, thin disks are a viable option. Otherwise, the general recommendation is to deploy thick disks.

Best Practices for VMware features

VMware Snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. The snapshots are useful for short-term point-in-time copies of the running system before major upgrades or before patching the system.

Snapshots can:

- consume large amounts of data resources.
- cause increased CPU loads on the host.
- affect performance.
- affect service.

Due to these adverse behaviors, consider the following recommendations when using the Snapshot feature.

- Snapshot operations can adversely affect service. The application that is running on the VM should be stopped or set to out-of-service before you perform a snapshot operation. When the snapshot operation has completed, the application can then be restarted or brought back into service.
- Do no rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- **Do not run a virtual machine off of a snapshot.** Do not use a single snapshot for more than 24-72 hours. The recommended actions are to take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot as soon as the proper working state of the virtual machine is verified. Following the recommended actions prevents 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 length of time the host takes to write the memory onto the disk is relative to the amount of memory

the virtual machine is configured to use and can add several minutes to the time it takes to complete the operation. If the snapshot is activated, saving memory will make calls appear to be active or in progress and can cause confusion to the user. When creating a snapshot, make sure that you:

- uncheck the **Snapshot the virtual machine's memory** check box in the **Take Virtual Machine Snapshot** window.
- select the **Quiesce guest file system (Needs VMware Tools installed)** check box to make sure all writes to the disks have completed. It gives a better chance of creating a clean snapshot image from which to boot.

- If you are going to use snapshots over a long period of time, you must consolidate the snapshot files on a regular basis 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:

In the event of a consolidate failure, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, a warning is displayed in the UI.

Related resources

Title	Web page
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	Understanding virtual machine snapshots in VMware ESXi and ESX
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 ESX host from one ESX host to another without incurring downtime. The migration process, also known as a **hot-migration**, enables the live migration of running virtual machines with zero downtime, continuous service availability, and complete transaction integrity.

When you use vMotion, note the following:

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

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:

If a clone of a WebLM VMware is created, all the existing licenses become invalid. You must rehost all the licenses.

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 the High Availability documentation for VMware.

Note:

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

Chapter 6: Configuration

Configuring the virtual machine automatic startup settings

Configure the virtual machine to automatically start after a power failure or restart of the hypervisor. The default is set to **no**.

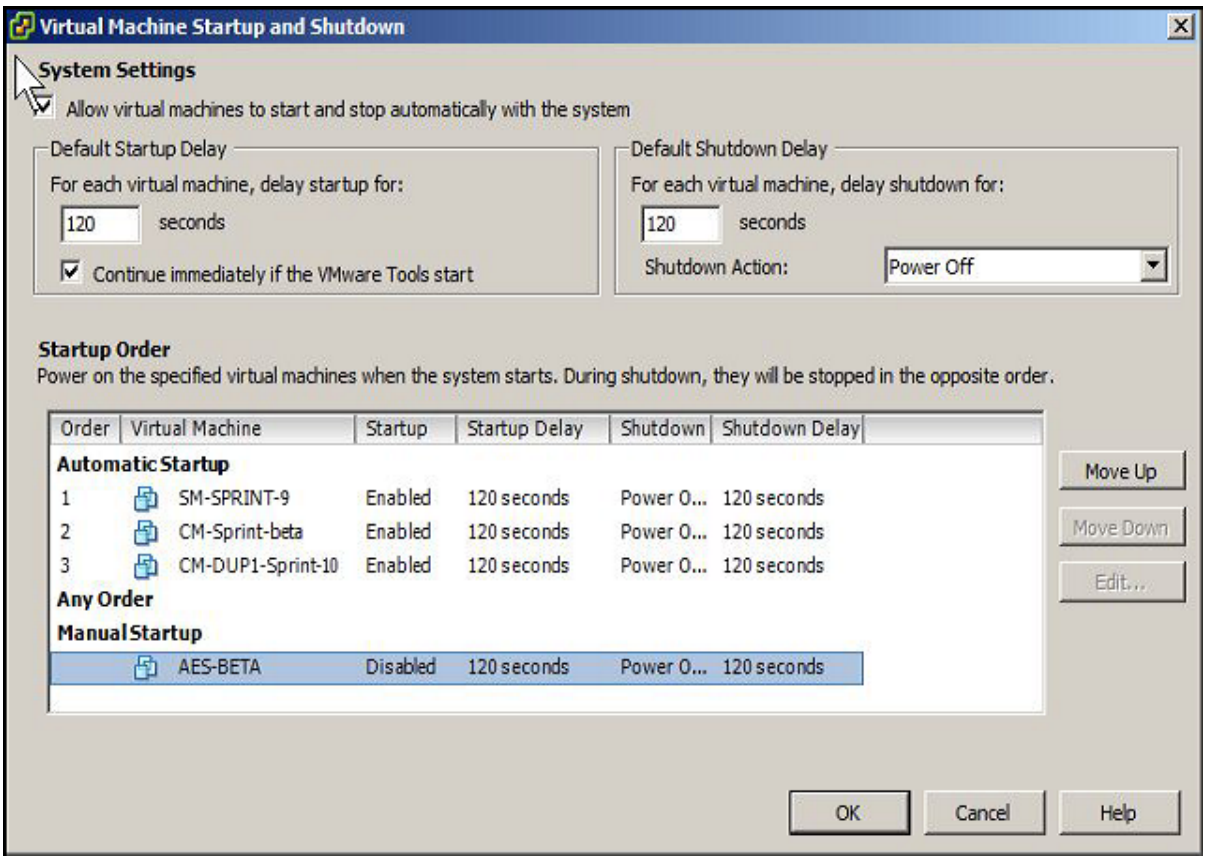
In high availability (HA) clusters, the VMware HA software ignores the startup selections.

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 under **Automatic Startup**.
8. Click **OK**.

Example

The following is an example of the **Virtual Machine Startup/Shutdown** screen.



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.

Procedure

1. Log in to the WebLM CLI using the user name `admin` and password `admin`.

   Important:

   Ensure that the 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.

   Note:

   This command overrides all the previous DNS IP address entries.

4. Log in to the WebLM console as admin.
5. Verify that the system displays the multiple DNS IP addresses.

Configuring the time zone in the WebLM server

Procedure

1. Log in to the WebLM virtual machine using root credentials.
2. Check the current time zone by executing the **date** command on the linux prompt. For example, `# date Mon Sep 17 22:59:24 IST 2010`
3. To change the directory to `/etc`, enter **`# cd /etc`**.
4. To delete the current local time file in the `/etc/` directory , enter **`# rm –f localtime`**.
5. To view the region for the time zone that you want to change, enter **`# ls /usr/share/zoneinfo/*`**.

   The `/usr/share/zoneinfo/*` directory contains the time zones of all the regions.
6. Link the time zone file from the `/usr/share/zoneinfo/` directory to the `/etc/localtime` directory.

   For example, to link the UTC time zone to the local time, enter the following command:

   `# cd /etc`

   `# ln -s /usr/share/zoneinfo/UTC /etc/localtime`
7. For the system to reflect the time zone details, in the `/etc/sysconfig/clock configuration` file, enter **`# ZONE="UTC”`**.

8. To verify the change in the time zone on the Linux system, enter **`# date`**. For example, if you change the time zone to UTC, the system displays the date as *Mon Sep 17 22:59:24 UTC 2010*.
9. Restart the Tomcat service using the **`service tomcat restart`** command.

Configuring the NTP time

Before you begin

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

- Open vSphere Client and click the **Console** tab or the icon.
- Start an SSH on the WebLM server.

Log in to the WebLMvirtual machine as admin.

Procedure

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

   The date and time of the WebLM virtual machine synchronizes with the NTP server.
6. Select the **Restart NTP service to apply changes** check box.
7. Click **OK**.

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

Chapter 7: Verifying successful installation

Before you begin

Log in to the WebLM Web console using admin credentials.

About this task

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

Procedure

1. In the Web browser, enter https:// <FQDN or IP address>:<port>/ WebLM. FQDN is the fully qualified domain name of WebLM.

   The system displays the WebLM Web console.

   Note:

   WebLM uses the default port 52233.

2. Log in to the Web console.

   If you log in as 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**. Verify if 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 a few other parameters from CLI. The maintenance chapter also gives information on performing a WebLM backup, restore and performing a snapshot backup and restore.

Note:

The existing license files become invalid when you:

- copy a WebLM virtual machine
- 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 in accordance with 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 send the file through email.

Related topics:

Installing the authentication file in WebLM on page 38

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. Copy the authentication file to the `/tmp` directory in the server using an application like WinSCP.

   Note the exact name of the authentication file. For example, the file name can be AF-7000438702-121024-172934.xml.
2. Using SSH log in to WebLM as admin, and change the login user to root.
3. Type `cd /tmp` to reach the `tmp` directory.
4. Type `ls`.
   The system lists the authentication file, if present.
5. Type **`loadauth -l <auth_file_path> –f`** to load the authentication file.

   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` mentioned in the command is the authentication file you downloaded from RFA.

The system displays the following message: *Loading file /tmp/ AF-7000438702-121024-172934.xml Skipping certificate installation on System Platform.*

You can ignore the line skipping certificate installation on System Platform.

Related topics:

Downloading the authentication file on page 37

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

Before you begin

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

- Open vSphere Client and click the **Console** tab or the icon.
- Start an SSH on the WebLM server.

Log in to the WebLM virtual machine as admin.

Procedure

Enter `ChangeIPFQDN –IP <IP Address> –FQDN <FQDN> –GATEWAY <Gateway dddress> –NETMASK <Netmask dddress> –DNS <DNS address> –SEARCH <search list for DNS>`.

Warning:

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

Note:

After you perform a WebLM upgrade, or an IP/FQDN change, when you do a restore operation, the licenses become invalid. You must re-host the licenses for a successful restore. The license data varies based on the installed license as part of the license re-host.

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 or the icon.
- Start an SSH on the WebLM server.

Log in to the WebLM virtual machine as admin.

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 admin.
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 such as DVD.

Performing WebLM restore

Procedure

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

Note:

The conf.properties file is located at `/opt/vsp/conf.properties`.

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 or vSphere Client.

Procedure

1. From the list of virtual machines, right-click the required WebLM virtual machine, and click **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, verify the **Status** of the **Create virtual machine snapshot** task, and wait until the system displays *Completed*.

Creating a snapshot restore

About this task

Important:

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

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

Procedure

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

Installing a patch or a 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 or the service pack file to the WebLM virtual machine.

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

- Open vSphere Client and click the **Console** tab or the icon.
- Start an SSH on the WebLM server.

Procedure

1. Log in to the WebLM virtual machine as admin.
2. Perform a WebLM backup.
3. Enter the **WebLMPatchDeploy** command.
4. Provide the location of the patch file.
5. Once the patch is installed successfully, perform a WebLM restore.

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

Glossary

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.
Avaya Services VM	A virtual machine that supports Avaya services applications. Currently the services virtual machine is part of System Platform which uses a non-VMWare hypervisor.
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.
DRS	Distributed Resource Scheduler. A VMware feature that intelligently places workloads based on available virtual resources.
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.
HA	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.
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 Application. An OVA is 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 is the amount of physical RAM, CPU cycles, or memory that are reserved for a virtual machine.
SAN	Storage Area Network. A SAN is a dedicated network that provides access to consolidated data storage. SANs are primarily used to make storage devices, such as disk arrays, accessible to servers so that the devices appear as locally attached devices to the operating system.
Snapshot	Capture a virtual appliance configuration 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	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.
vSphere	< < v vSphere is VMware’s computer cloud virtualization operating system.

Index

P

R

S

T

V

W