Deploying standalone Avaya WebLM in Virtualized Environment

Release 10.1.x
Issue 9
February 2026

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

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 media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

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, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for deploying the Avaya WebLM virtual application on a customer-provided Virtualized Environment, Avaya Solutions Platform 130 (Dell PowerEdge R640) in a Avaya-Supplied VMware ESXi 7.0. 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 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.

Prerequisites

Before deploying the Avaya WebLM OVA, ensure that you have the following knowledge, skills, and tools.

Knowledge

- **For VMware:** VMware® vSphere™ virtualized environment.
- Linux® Operating System.
- WebLM.

Skills

To administer VMware® vSphere™ virtualized environment.

Tools

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

Change history

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

Issue	Date	Summary of changes
9	February 2026	Updated the following section: • Supported servers for Avaya Aura applications on page 14
8	September 2025	Updated the following section: • Supported footprints of WebLM on VMware on page 16
7	June 2025	Updated the following section: • Supported ESXi version on page 12
6	February 2025	Updated Supported ESXi version on page 12
5	December 2024	Added the sections: • Deployment options on page 29 • Checklist for deploying WebLM on KVM using scripts on page 30 • Deploying Avaya WebLM on ASP R6.0.x (KVM on RHEL 8.10) using Script on page 35 • Supported footprint of WebLM on KVM on page 16 Updated the sections: • Checklist for deploying WebLM on KVM using Cockpit on page 29 • Creating a staging directory on page 31 • Extracting the OVA on page 31 • Converting from thin provisioning to thick provisioning on page 32 • Copying the files to the images directory on page 32 • Changing permissions on page 33
4	December 2024	Added the sections: • Virtualized Environment component for ASP R6.0.x (KVM on RHEL 8.10) on page 11 • Supported hardware for ASP R6.0.x (KVM on RHEL 8.10) on page 12 • Supported KVM version on page 12 • Checklist for deploying WebLM on KVM using Cockpit on page 29 • Creating a staging directory on page 31 • Extracting the OVA on page 31 • Converting from thin provisioning to thick provisioning on page 32 • Copying the files to the images directory on page 32 • Changing permissions on page 33 • Deploying WebLM using KVM Cockpit on page 33 • Updating the CPU resources for KVM Cockpit on page 40

Table continues…

Issue	Date	Summary of changes
3	March 2024	Spelling correction in multiple topics.
2	January 2024	Updated the section: Supported ESXi version on page 12
1	February 2023	Release 10.1.2 document.

Chapter 2: Virtualized Environment overview

You can deploy the Avaya Aura® Release 10.1.x applications in one of the following Virtualized Environment:

- Avaya Solutions Platform 130 Release 5.x (Dell PowerEdge R640) is a single host server with preinstalled ESXi 7.0 Standard VMware License.
- VMware in customer-provided Virtualized Environment.

Note:

With Release 10.1.x and later, Avaya Aura® will no longer have the KVM OVA. Deployment on KVM virtualized environment is supported through the Software-Only offer.

For more information about deploying application, see the product-specific Software-Only and Infrastructure as a Service guide.

Supported applications in Virtualized Environment

- Avaya Aura® System Manager Release 10.2.x
- Avaya WebLM Release 10.1.3.x
- Avaya Aura® Session Manager Release 10.2.x
- Avaya Aura® Communication Manager Release 10.2.x
- Avaya Aura® Application Enablement Services Release 10.2.x
- Avaya Aura® Media Server Release 10.2.x

For the latest and most accurate information about other Avaya product compatibility information, go to **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

Virtualized Environment components for VMware

Virtualized component	Description
Open Virtualization Appliance (OVA)	The virtualized OS and application packaged in a single file that is used to deploy a virtual machine.
Customer-provided VMware or Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0)	
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.
ESXi Embedded Host Client	The ESXi Embedded Host Client is a native HTML and JavaScript application and is served directly from the ESXi host.
vSphere Client (HTML5)	Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.
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. This is not applicable for Avaya Solutions Platform 130.

Note:

With VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported.

Virtualized Environment component for ASP R6.0.x (KVM on RHEL 8.10)

Virtualized component	Description
Avaya Solutions Platform 130 (Avaya-Supplied KVM on RHEL R8.10) or Avaya Solutions Platform S8300 (Avaya-Supplied KVM on RHEL R8.10)	
KVM Cockpit	Cockpit is a system administration tool that provides a user interface for monitoring and administering servers through a web browser. Cockpit administrators can create and manage KVM-based virtual machines on the host system

Chapter 3: Planning and configuration

Hardware support

Supported hardware for VMware

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

Supported hardware for ASP R6.0.x (KVM on RHEL 8.10)

The only supported hardware for the KVM images is Avaya Solutions Platform 130 Release 6.0.x and Avaya Solutions Platform S8300 Release 6.0.x.

Supported KVM version

The following table lists the supported KVM versions of Avaya Aura® applications:

Avaya Solutions Platform (KVM on RHEL 8.10 version)	Avaya Aura® Release	
	8.1.x	10.1.x
KVM Release 8.10	Y	Y

Note:

- Please check the release notes for the availability of 8.1 and 10.1.

Supported ESXi version

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

ESXi version	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
ESXi 5.0	N	N	N	N	N
ESXi 5.1	N	N	N	N	N
ESXi 5.5	Y	N	N	N	N
ESXi 6.0	Y	Y	Y	N	N
ESXi 6.5	Y	Y	Y	N	N
ESXi 6.7	N	Y	Y	Y	N
ESXi 7.0	N	N	Starting from Release 8.1.3: Y	Y	Y
ESXi 8.0	N	N	N	N	Y

Note:

- Avaya Solutions Platform 130 Appliance and Avaya Solutions Platform S8300 R6.0 supports Avaya-supplied KVM on RHEL 8.10. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell or RHEL website, this results in an unsupported configuration.
- Avaya Aura® Release 10.2.x supports VMware 8.0, VMware 8.0 Update 2, and VMware 8.0 Update 3.

  Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the Broadcom website (formerly VMware).
- As of October 15, 2022, VMware has ended support for VMware vSphere 6.x. Therefore, it is recommended to upgrade to supported vSphere versions.

  For customer-provided environments and how to upgrade to supported vSphere version, see the VMware website.
- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL website, this results in an unsupported configuration.
- From VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is supported.
- Avaya Aura® applications support the particular ESXi version and its subsequent update. For example, the subsequent update of VMware ESXi 7.0 can be VMware ESXi 7.0 Update 3.
- WebLM Release 10.1.2 OVA and higher are certified with ESXi 8.0, ESXi 8.0 Update 2 (U2) deployments, and ESXi 8.0 Update 3 (U3) deployments.

Supported servers for Avaya Aura® applications

The following table lists the Avaya sourced supported servers for the Avaya Aura® applications:

Supported servers	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
S8300D	Y	N	N	N	N
S8300E[1]	Y	Y	Y	Y	Y
HP ProLiant DL360 G7 (CSR1)	Y	N	N	N	N
HP ProLiant DL360p G8 (CSR2)	Y	Y	Y	N	N
HP ProLiant DL360 G9 (CSR3)	Y	Y	Y	N	N
Dell™ PowerEdge™ R610 (CSR1)	Y	N	N	N	N
Dell™ PowerEdge™ R620 (CSR2)	Y	Y	Y	N	N
Dell™ PowerEdge™ R630 (CSR3)	Y	Y	Y	N	N
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 [2]	N	Y	Y	N	N
Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 and R660xs [3]	N	Y	Y Avaya Solutions Platform 130 Release 5.x/6.x	Y Avaya Solutions Platform 130 Release 5.x/6.x	Y Avaya Solutions Platform 130 Release 5.1/6.x
Avaya Solutions Platform S8300 [4]	N	N	N	Y Release 5.1	Y Release 5.1/6.x

[1] You can migrate the S8300E server to Avaya Solutions Platform S8300 Release 6.x. For information, see *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300* on the Avaya Support website.

[2] Avaya Solutions Platform 120 Appliance uses Appliance Virtualization Platform to support virtualization.

[3] You can migrate the Avaya Solutions Platform 120 Appliance to Avaya Solutions Platform 130 Appliance Release 6.x. For information, see *Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130* on the Avaya Support website.

Avaya Solutions Platform 130 Appliance 5.1.x uses VMware vSphere ESXi software to support virtualization. Avaya Solutions Platform 130 Appliance 6.x uses KVM on RHEL software to support virtualization.

[4] Avaya Solutions Platform S8300 5.1.x supports virtualization using VMware vSphere ESXi foundation license for Communication Manager and Branch Session Manager. Avaya Solutions Platform S8300 6.x supports virtualization using KVM on RHEL 8.10 software.

Avaya Solutions Platform 130 Appliance R4/5 uses VMware vSphere ESXi Standard License to support virtualization

Note:

- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL website, this results in an unsupported configuration.
- From Avaya Aura® Release 10.1 and later, Avaya-provided HP ProLiant DL360p G8, HP ProLiant DL360 G9, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, and Avaya Solutions Platform 120 servers are not supported.

  However, in Release 10.2.x, Avaya Solutions Platform 120 can be upgraded to Avaya Solutions Platform 130 Release 6.0.
- From Avaya Aura® Release 8.0 and later, S8300D, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers are not supported.

With the introduction of Avaya Solutions Platform R6.0.x (KVM on RHEL 8.10), you no longer need a specific license key as was the case with Avaya Solutions Platform 5.1.x and earlier versions running on ESXi. However, it is imperative that customers have a record in PLDS for each and every instance of the server hypervisor as customers and Avaya will be subject to audits to ensure right to use royalties have been paid.

Configuration tools and utilities

You must have the following tools and utilities for deploying and configuring standalone Avaya WebLM open virtual application (OVA) on customer-provided Virtualized Environment on VMware and KVM:

- A remote computer running the VMware vSphere Client.
- A browser for accessing the Avaya WebLM web interface.
- An SFTP client for Windows, for example WinSCP.
- An SSH client, for example, PuTTY and PuTTYgen.

Note:

Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

Supported footprints of WebLM on VMware

These footprints are common for VMware and Avaya Solutions Platform 130 Release 5.x.

Note:

- WebLM supports VMware hosts with Hyperthreading enabled at the BIOS level.
- Reservations are not permitted for Avaya Solutions Platform 4200 series solutions (formerly known as CPOD/PodFx) deployment. For reservationless deployment of Avaya Aura® applications, see the recommendations given in *Application Notes on Best Practices for Reservationless deployment of Avaya Aura® software release 10.1 on VMware*.

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

  If you use the WebLM server to acquire licenses for more than 5000 clients, use Profile 2. If products such as Avaya Agent for Desktop, Workplace, or Avaya Vantage™ are sending more than 300 requests simultaneously, use Profile 2.

Resource	Profile 1	Profile 2
vCPU	1	1
CPU reservation	**Avaya Solutions Platform 130 and VMware:** 2185 MHz	**Avaya Solutions Platform 130 and VMware:** 2185 MHz
Memory reservation	1GiB	2GiB
Storage reservation	40GiB	40GiB
Shared NICs	1	1

Note:

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

Supported footprints of WebLM on KVM

These footprints are common for KVM and Avaya Solutions Platform 130 Release 5.x.

Note:

- Reservations are not permitted for Avaya Solutions Platform 4200 series solutions (formerly known as CPOD/PodFx) deployment. For reservationless deployment of Avaya Aura® applications, see the recommendations given in *Application Notes on Best*

Practices for Reservationless deployment of Avaya Aura® software release 10.1 on VMware.

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

Resource	Profile 1	Profile 2
vCPU	1	1
CPU reservation	**Avaya Solutions Platform 130 and KVM:** 2185 MHz	**Avaya Solutions Platform 130 and KVM:** 2185 MHz
Memory reservation	1GiB	2GiB
Storage reservation	40GiB	40GiB
Shared NICs	1	1

Note:

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

Software details of WebLM

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

Downloading software from PLDS

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

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

Note:

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

Procedure

1. On your web browser, type https://plds.avaya.com to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS Home page, select **Assets**.

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

   Note:

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

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

Customer configuration data for WebLM

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

Required data	Description	Example value for the system	✔
IP address	The IP address of the WebLM interface.	For IPv4: 10.10.x.x For IPv6: 2001:0db8::a	
Netmask	The network address mask.	255.255.0.0	
Default Gateway	The default network traffic gateway.	For IPv4: 10.16.x.x For IPv6: 2001:0db8::1	

Table continues…

Required data	Description	Example value for the system	✔
DNS IP Address	The IP address of the primary DNS server.	For IPv4: 10.x.x For IPv6: 2001:0db8::5	
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. The application supports only the NTP server. It does not support the NTP pool.	For IPv4: 10.16.x.x For IPv6: 2001:0db8::b	
Time Zone	The time zone you want to choose.	America/Denver	
CLI User details	The command-line interface user details.	abcd	
Admin UI password	The admin UI password.		
EASG	Enhanced Access Security Gateway		
Customer root account details	The customer root account details.		

Deployment guidelines

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

SAL Gateway

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

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

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

Chapter 4: Deploying WebLM on VMware

Checklist for deploying WebLM on VMware®

No.	Task	Links/Notes	✔
1.	Download the WebLM OVA file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com/	Downloading software from PLDS on page 17	
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 18	
4.	Deploy the WebLM OVA file.	Deploying the WebLM OVA by using vSphere Client (HTML5) on page 21	
5.	Start the WebLM virtual machine.	Starting the WebLM server virtual machine on page 28	
6.	Verify the installation of the WebLM virtual machine.		
7.	Install the WebLM feature pack file.	Installing a WebLM patch, feature pack, or service pack on page 27	
8.	Restart the WebLM virtual machine from CLI to get the updated kernel running in memory.		

Deploying the WebLM OVA by using vSphere Client (HTML5)

Procedure

1. To access the vCenter Server, do the following:
   a. On the web browser, type the vCenter FQDN or IP Address.
   b. Select vSphere Client (HTML5) and type the vCenter Server credentials.

2. Select the Cluster or ESXi host, right-click, and then click **Deploy OVF Template**.

   The system displays the Deploy OVF Template dialog box.

3. On the Select template page, perform one of the following steps:
   - To download the WebLM OVA from a web location, select **URL**, and provide the complete path of the OVA file.
   - To access the WebLM OVA from the local computer, select **Locate file**, click **Browse**, and navigate to the OVA file.
4. Click **Next**.
5. On the Select a name and folder page, do the following:
   a. In **Virtual machine name**, type a name for the virtual machine.
   b. In **Select a location for the virtual machine**, select a location for the virtual machine.
6. Click **Next**.
7. On the Select a compute resource page, select a host, and click **Next**.
8. On the Review details page, verify the OVA details, and click **Next**.
9. To accept the End User License Agreement, on the License agreements page, click **I accept all license agreements**.
10. Click **Next**.
11. On the Select configuration page, from **Configuration**, select the WebLM profile.
12. Click **Next**.
13. On the Select storage page, in **Select virtual disk format**, click the required disk format.
14. Click **Next**.
15. On the Select networks page, select the destination network for each source network.
16. Click **Next**.
17. On the Customize template page, enter the configuration and network parameters.

    For information about the configuration and network parameters, see Configuring the network parameters fields and descriptions on page 51.

    Note:
    - If you do not provide the details in the mandatory fields, you cannot power on the virtual machine even if the deployment is successful.
    - During the startup, the system validates the inputs that you provide. If the inputs are invalid, the system prompts you to provide the inputs again on the console of the virtual machine.
18. Click **Next**.

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

    Wait until the system deploys the OVA file successfully.

20. To start the WebLM virtual machine, if WebLM is not already powered on perform one of the following steps:

    - Click VM radio button, and click **Actions** > **Power** > **Power On**.
    - Right-click the virtual machine, and click **Power** > **Power On**.
    - On the **Inventory** menu, click **VirtualMachine** > **Power** > **Power On**.

    The system starts the WebLM virtual machine.

21. Click the **Console** tab and verify that the system startup is successful.

Next steps

Note:

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

Related links

Deploying the application OVA by accessing the ESXi host directly on page 23
Application Deployment field descriptions on page 51

Deploying the application OVA by accessing the ESXi host directly

About this task

Use this procedure to deploy the application OVA on Avaya Solutions Platform 130 and equivalent server.

Before you begin

When you deploy or upgrade Avaya Aura® applications on Avaya Solutions Platform 130 ensure to:

- Update the Dell R640 BIOS and firmware to the latest release.
- Enable the iDRAC and connect it to an ethernet switch.

Note:

After deploying OVA directly from host, you must check that HDD size matches your profile.

Procedure

1. To access the ESXi host, do the following:

   a. On the web browser, type the ESXi host FQDN or IP address.

b. In **User name**, type the username of the ESXi host.
c. In **Password**, type the password of the ESXi host.
d. Click **Log in**.

2. Right-click an ESXi host and select **Create/Register VM**.

   The system displays the New virtual machine dialog box.

3. On the Select creation type page, select **Deploy a virtual machine from an OVF or OVA file**.
4. Click **Next**.
5. On the Select OVF and VMDK file page, do the following:
   a. Type a name for the virtual machine.
   b. Click to select files or drag and drop the OVA file from your local computer.
6. Click **Next**.
7. On the Select storage page, select a datastore, and click **Next**.
8. Click **Next**.
9. On the Deployment options page, perform the following:
   a. From **Network mappings**, select the required network.
   b. From **Disk provisioning**, select **Thick provision lazy zeroed**.
   c. From **Deployment type**, select profile.
   d. Clear **Power on automatically**.
10. Click **Next**.
11. On the Additional settings page, click **Next**.
12. On the Ready to complete page, review the settings, and click **Finish**.

    Wait until the system deploys the OVA file successfully.
13. To edit the virtual machine settings, click the VM radio option and perform the following:
    - Click **Actions** > **Edit Settings** to edit the required parameters.

      Note:
    - Click **Save** to save the reservation changes.

    Note:

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

Note:

If you do not enable autostart, manually start the virtual machine after the hypervisor reboot. Autostart must be enabled on the Host for the virtual machine autostart to function.

15. To start the virtual machine, if application is not already powered on, perform one of the following steps:
    - Click the VM radio option and click **Actions** > **Power** > **Power On**.
    - Right-click the virtual machine and click **Power** > **Power On**.
    - Navigate to **Host** > **Virtual Machines**, select the virtual machine and click **Actions** > **Power** > **Power On**.

    The system starts the application virtual machine. When the system starts for the first time, configure the parameters for the application.
16. Click **Actions** > **Console**, select the open console type, verify that the system startup is successful, then input the application configuration parameters.

Related links

Deploying the WebLM OVA by using vSphere Client (HTML5) on page 21
Application Deployment field descriptions on page 51

Deploying WebLM by using Solution Deployment Manager

Before you begin

- Install the Solution Deployment Manager client if System Manager is unavailable.
- Add a location.
- Add a required host to the location.
- Ensure that the certificate is valid on the host or vCenter managed hosts.
- Download the required OVA file to System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a platform.
3. On the **Applications** tab, in the Applications for Selected Location <location name> section, click **New**.

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

b. In **Select Platform**, select a platform.

Solution Deployment Manager displays the host name in the **Platform FQDN** field.

5. In **Data Store**, select a data store, if not displayed upon host selection.

   The Capacity Details section displays the capacity details.

6. Click **Next**.
7. To get the OVA file, select the **OVA** tab, and click one of the following:
   - **URL**, in **OVA File**, type the absolute path to the application OVA file, and click **Submit**.
   - **S/W Library**, in **File Name**, select the application OVA file.
   - **Browse**, select the required application OVA file from a location on the computer, and click **Submit File**.

   If the OVA file does not contain a valid Avaya certificate, then the system does not parse the OVA and displays the following message: `Invalid file content. Avaya Certificate not found or invalid`
8. In **Flexi Footprint**, select the footprint size that the application supports.
9. In the Network Parameters and Configuration Parameters sections, complete the required fields.

   For information about the fields, see “Application Deployment field descriptions”.

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

    In the Platforms for Selected Location <location name> section, Solution Deployment Manager displays the deployment status in the **Current Action Status** column.

    Solution Deployment Manager displays the virtual machine on the Applications for Selected Location <location name> page.

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

Next steps

- After completing the OVA deployment, install the patch file.
- From the WebLM web console, verify that the About page displays the correct version and build details.
- Restart WebLM to get the updated kernel running in memory.

Cloned and copied OVAs are not supported

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. At this time, Avaya only supports the deployment of new OVAs.

Installing a WebLM patch, feature pack, or service pack

Before you begin

- Create backup of WebLM.
- Check the installed WebLM software version. For more information, see “Verifying the WebLM software version”.
- Copy the patch file, feature pack file, or the service pack file to the WebLM server in the `/var/WebLMPatch` folder.

Note:

If you have older WebLM 10.1.2 OVA (`WebLM-10.1.2.0.0-39162-e70-64.ova`) deployed, then it is recommended to re-deploy WebLM using the new re-spun OVA (`WebLM-10.1.2.0.0-39457-e70-72.ova`). For more details about the WebLM 10.1.2 re-spun OVA, see PSN006085u.

If you copy the WebLM patch file in a folder other than `/var/WebLMPatch` and initiate the patch installation, WebLM stops the patch execution and displays the following message:

```
Verifying the patch binary.....
The patch bin file needs to be copied under /var/WebLMPatch/
folder.
```

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Verify the MD5 checksum of the patch file.
3. Type `WebLMPatchdeploy <absolute path to the WebLM feature pack file>`.

   For example, `WebLMPatchdeploy /var/WebLMPatch/VEWebLM_10.1.x.x_xxx.bin`.

   WebLM installs the patch file.
4. To accept the license terms, read the End User License Agreement carefully and type `Y`.

   The patch installation takes about 10–15 minutes to complete. You can view to monitor the WebLM patch progress status from the `/var/log/Avaya/WebLM_Patch.log` file.

   If the installation is successful, the system displays a warning message on the dashboard and on the command line interface to restart WebLM if kernel is updated.
5. After patch installation is successful, relogin to CLI to check if the updated kernel is running.
6. Restart the standalone WebLM.

Next steps

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

Note:

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

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.

Chapter 5: Deploying WebLM on KVM

Deployment options

There are two options. You can deploy KVM using Cockpit or Command Line Interface (CLI) scripts.

- Checklist for deploying WebLM on KVM using Cockpit on page 29
- Checklist for deploying WebLM on KVM using scripts on page 30

Checklist for deploying WebLM on KVM using Cockpit

No.	Task	Links/Notes	✔
1.	Install ASP R6.0.x (KVM on RHEL 8.10).	For more information, see *Installing the Avaya Solutions Platform 130 Series* at https://support.avaya.com/css/public/documents/101091802.	
2.	Download the WebLM OVA file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com/	Downloading software from PLDS on page 17	
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 18	
5.	Create a staging directory.	Creating a staging directory on page 31	
6.	Extract the OVA.	Extracting the OVA on page 31	
7.	Convert the file from thin provisioning to thick provisioning	Converting from thin provisioning to thick provisioning on page 32	
8.	Copy the files to the images directory.	Copying the files to the images directory on page 32	

Table continues…

No.	Task	Links/Notes	✔
9.	Change permissions.	Changing permissions on page 33	
10.	Deploy the WebLM OVA file using Cockpit.	Deploying WebLM using KVM Cockpit on page 33	
11.	Start the WebLM virtual machine.	Starting the WebLM server virtual machine on page 28	
12.	Verify the installation of the WebLM virtual machine.		
13.	Install the WebLM feature pack file.	Installing a WebLM patch, feature pack, or service pack on page 27	
14.	Restart the WebLM virtual machine from CLI to get the updated kernel running in memory.		

Checklist for deploying WebLM on KVM using scripts

No.	Task	Links/Notes	✔
1.	Install ASP R6.0.x (KVM on RHEL 8.10).	For more information, see *Installing the Avaya Solutions Platform 130 Series* at https://support.avaya.com/css/public/documents/101091802.	
2.	Download the WebLM OVA file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com/	Downloading software from PLDS on page 17	
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 18	
5.	Deploy the WebLM OVA file using scripts.	Deploying Avaya WebLM on ASP R6.0.x (KVM on RHEL 8.10) using Script on page 35	
6.	Start the WebLM virtual machine.	Starting the WebLM server virtual machine on page 28	
7.	Verify the installation of the WebLM virtual machine.		
8.	Install the WebLM feature pack file.	Installing a WebLM patch, feature pack, or service pack on page 27	

Table continues…

No.	Task	Links/Notes	✔
9.	Restart the WebLM virtual machine from CLI to get the updated kernel running in memory.		

Creating a staging directory

Procedure

1. Download the WebLM KVM image from PLDS to your computer.
2. Log in to the ASP R6.0.x CLI with **custadm** credentials.
3. Run the following command to ensure that the staging folder exists: `/var/lib/libvirt/staging`.

   ```
   sudo ls -ld /var/lib/libvirt/staging
   ```
4. Remove older images from the staging folder.
5. Ensure sufficient space is available in the staging folder to copy the KVM image.
6. **(Optional)** If the staging folder does not exist, create it using the following commands:
   - `sudo mkdir /var/lib/libvirt/staging`
   - `sudo chown custadm:wheel /var/lib/libvirt/staging`

   The **chown** command now allows **custadm** to write into the `staging` directory with **sudo**. The permissions should look as follows:

   ```
   drwxr-x---. 2 custadm wheel 6 Oct 23 14:32 /var/lib/libvirt/staging
   ```

Extracting the OVA

Procedure

1. Copy the WebLM KVM image to the ASP R6.0.x host in `/var/lib/libvirt/staging` using the Winscp tool and **custadm** credentials.
2. Ensure you are logged into the CLI. If not, log in to the ASP R6.0.x CLI with **custadm** credentials.
3. Ensure that the network bridge is configured during the KVM deployment.
4. Run the following command to verify the WebLM KVM image available in the staging folder: **sudo ls -lr /var/lib/libvirt/staging**
5. Go to `/var/lib/libvirt/staging` folder, and run the following command to extract the ova file: **sudo tar -xvf WebLM-**<*version number*>**-KVM-4E.ova**.

KVM OVA file extracts the following files:

- `WebLM-*.ovf`
- `WebLM-*.mf`
- `WebLM-*.cert`
- `install_vm.py`
- `ovf.py`
- `WebLM-*.qcow2`

Converting from thin provisioning to thick provisioning

About this task

The WebLM-<*version number*>-KVM-4E-disk1.qcow2 images are in thin provision format. You must convert the qcow2 images to thick provision. When running the commands to convert to thick provision, add a unique identifier to the new qcow2 image, such as WebLM-<*version number*>-KVM-4E-THICKdisk1.qcow2.

Procedure

1. Go to the `/var/lib/libvirt/staging` folder, and run the following command to convert the thin qcow image to a thick qcow image:

   sudo qemu-img convert -O qcow2 -o preallocation=full WebLM-<*version number*>-KVM-4E-disk1.qcow2 WebLM-<*version number*>-KVM-4E-THICKdisk1.qcow2

2. Run the following command to verify the disk size and that the conversion is successful:

   sudo qemu-img info WebLM-<*version number*>-KVM-4E-THICKdisk1.qcow2

   The disk size must display as 40 GB.

Copying the files to the images directory

Procedure

1. Go to the `/var/lib/libvirt/staging` folder.
2. Run the following command to copy the `WebLM-<version number>-KVM-4E-THICKdisk1.qcow2` file to the `/var/lib/libvirt/images` directory:

   sudo cp WebLM-<*version number*>-KVM-4E-THICKdisk1.qcow2 /var/lib/libvirt/images

3. Go to `/var/lib/libvirt/staging` directory and run the following command to verify the qcow2 image is present:

   `cd /var/lib/libvirt/staging`

   `sudo ls -lrt`

Changing permissions

Procedure

1. From the `/var/lib/libvirt/images` directory, run the following command to change the owner and permissions to 640 on the files:

   `sudo chown qemu:qemu sudo cp WebLM-`<*version number*>**`-KVM-4E-THICKdisk1.qcow2`**

   `sudo chmod 640 sudo cp WebLM-`<*version number*>**`-KVM-4E-THICKdisk1.qcow2`**

2. Go to `/var/lib/libvirt/staging` directory and remove all the extracted images and converted images. This is important to ensure that there is sufficient space for future deployments of KVM images. Do not remove files from the images directory.

   `cd /var/lib/libvirt/staging`

   `sudo ls -lrt`

   `sudo rm WebLM-*`

   `sudo rm README*`

Deploying WebLM using KVM Cockpit

Procedure

1. Log in to the KVM Cockpit web console as **`custadm`** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

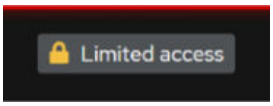


Figure 1: Limited access button

Note:

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **custadm**.

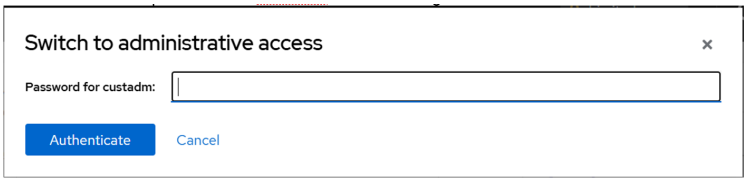


Figure 2: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

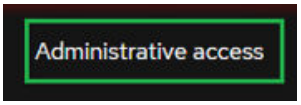


Figure 3: Administrative access button

4. Navigate to **System** > **Virtual Machines** > **Import VM**.
5. In the Import a virtual machine window, do the following:
   a. In the **Name** field, enter a name for the WebLM virtual machine.
   b. In the **Disk Image** field, select the `WebLM-10.1.2.0.0-39690-KVM-4E-THICKdisk1.qcow2` image of the Communication Manager on the KVM Cockpit host under `/var/lib/libvirt/images/` directory.
   c. In the **Operating System** field, select **RHEL 8.6 (Oopta)** version.
   d. In the **Memory** field, select the required memory in MiB format.

      Note:

      Based on the required footprint, enter a value in the **Memory** field.

      For more information on footprints, see *Upgrading standalone Avaya WebLM*.

   e. Click **Import and edit**.

      Virtual Machine details page appears.

      Under the Disks section, verify the `WebLM-10.1.2.0.0-39690-KVM-4E-THICKdisk1.qcow2` disk image size is correctly displayed in the **Capacity** field.

      By default, **virtio** is selected under the **Bus** field, and this needs to be modified.
6. Under the Disks section, click **Edit**.

7. In the Edit <attributes name> window, do the following:
   a. In the **Bus** field, select **scsi**.
   b. In the **Cache** field, select **directsync**.
   c. Click **Save**.

      In the Disks section, ensure that **scsi** appears under the **Bus** field and **directsync** appears under the **Additional Cache** field.
8. In the Overview section, in the **Firmware** field, select **UEFI** and click **Save**.
9. In the Overview section, in the **CPU** field, click **edit**.

   CPU Details window opens.
10. In the CPU details window, based on the required footprint, enter a value in the **vCPU Maximum** and **vCPU Count** fields.
11. In the **Mode** field, keep the default **host-model**.
12. Click **Apply**.
13. In the Network interfaces section, click **Edit** and select the Network Bridge, and click **Save**.
14. On the virtual machine, click **Run** to start the System Manager virtual machine.

Next steps

On first boot of the System Manager virtual machine, log in to the virtual console using the `craft`/`craft01` and provide the configuration and networking parameters.

Deploying Avaya WebLM on ASP R6.0.x (KVM on RHEL 8.10) using Script

About this task

Use this procedure to run a Command Line Interface (CLI) script to create a virtual machine. Verify that you successfully created the virtual machine by logging in to KVM Cockpit to view the list of virtual machines.

Avaya WebLM provides a KVM OVA that contains one `qcow2` file:

`WebLM-*.qcow2`

Note:

- Always follow A1SC output for deployment of applications on the host(s). There should never be more than one instance of a specific application on the same host.
- Deployment of applications *MUST* be performed one at a time and delete the artifacts prior to deploying the next application.

Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

Before you begin

- Install ASP R6.0.x (KVM on RHEL 8.10).

  For more information, see *Installing the Avaya Solutions Platform 130 Series* at https://support.avaya.com/css/public/documents/101091802.
- Download the Avaya WebLM KVM image from PLDS to your computer.
- Login to the ASP R6.0.x CLI with **custadm** credentials.
- Ensure that the staging folder exists:

  sudo ls -ld /var/lib/libvirt/staging
- Ensure to remove the older images from the staging folder.
- Ensure sufficient space is available in the staging folder to copy the KVM image.
- If the staging folder does not exist, create it using the following commands:

  - **sudo mkdir /var/lib/libvirt/staging**

  - **sudo chown custadm:wheel /var/lib/libvirt/staging**
- The chown command now allows **custadm** to write into the staging directory with **sudo**. For example, the permissions should look as follows:

```
drwxr-x---. 2 custadm wheel 6 Oct 23 14:32 /var/lib/libvirt/staging
```

- Copy the Avaya WebLM KVM image to the ASP R6.0.x host in `/var/lib/libvirt/staging` using winscp and **custadm** credentials.
- Ensure you are logged into the ASP R6.0.x CLI. If not, login to the ASP R6.0.x CLI with **custadm** credentials.

  Note:

  All the commands *listed in the below points must* be prefaced with **sudo**:
- Run the following command to verify the Avaya WebLM KVM image is available in the staging folder:

  sudo ls -lr /var/lib/libvirt/staging
- Go to `/var/lib/libvirt/staging` folder, and run the following command to extract the ova file: **sudo tar -xvf WebLM-*.ova**

  KVM OVA file extracts the following files:

  - `WebLM-*.ovf`

  - `WebLM-*.mf`

  - `WebLM-*.cert`

  - `install_vm.py`

  - `ovf.py`

- `WebLM-*.qcow2`

Procedure

1. Log in to the ASP R6.0.x CLI and go to the staging folder:

   `sudo cd /var/lib/libvirt/staging`

2. Run the following script to deploy Avaya WebLM:

   `sudo python3 install_vm.py`

3. Press **`ENTER`** to read the **`EULA`**.
4. Press **`Y`** to accept the **`EULA`**.
5. Enter a name for the Avaya WebLM virtual machine. For example, `WebLM_Main`.
6. Select the required Avaya WebLM profile.

   For more information, see Supported footprint of WebLM on KVM on page 16

7. Select the network interfaces.

   ASP 6.0.x CLI displays the currently available network interface bridges and select the required bridge for Avaya WebLM.

   ASP 6.0.x CLI displays the currently available disk space and the required disk space to deploy Avaya WebLM.

8. To configure the VM properties, enter **`Y`** in the **Would you like to configure the VM properties? [y/n]:** field, and continue providing the property details:
   a. **Please enter the IPv4 Address to assign to the VM**. For example, x.x.x.x
   b. **Please enter the Netmask to assign to the VM**. For example, m.m.m.m
   c. **Please enter the IPv4 Address of your default gateway**. For example, x.x.x.x
   d. **Please enter the IP Address of your DNS server**. For example, x.x.x.x

      You can type multiple IP's seperated by a comma.

   e. **Please enter the Short Hostname to assign to the VM**. For example, xyz
   f. **(Optional) IPv6 Address. Please enter IPv6 address**
   g. **(Optional) IPv6 Network Prefix. Please enter IPv6 Network Prefix**
   h. **(Optional) IPv6 Gateway. Please enter IPv6 Gateway**
   i. **Please enter the Domain Name to assign to the VM**, enter valid domain name for the virtual machine.
   j. **(Optional) Please enter the default Search List**, enter the valid search list.
   k. **Please provide NTP Server IP/FQDN**, enter the valid NTP server IP or FQDN.

      You can type multiple IP or FQDN seperated by a comma.

   l. **Please enter the WebLM command line user name**, enter valid user name for the Avaya WebLM. For example: cust.

Do not use user names such as admin, csadmin.

Do not use: initial, admin, csadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, chrony, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, nortel.

a. In the **Please enter the WebLM command line user password** field, enter the password for Avaya WebLM command line user.

b. In the **Confirm Please enter the WebLM command line user password** field, re-enter the password

c. In the **Please enter the WebLM UI admin user password** field, enter the password for Avaya WebLM UI admin.

d. In the **Confirm Please enter the WebLM UI admin user password** field, re-enter the password.

9. Enable or disable Enhanced Avaya Security Gateway (EASG).

Important:

Avaya recommends to enable **EASG**.

Note:

Enable: (Recommended)

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

In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

Disable:

By disabling EASG, you are denying Avaya access to the system. This setting is not recommended as it can impact Avaya's ability to provide support for the product. Unless the customer can manage the product, Avaya Services Logins should not be disabled.

- Enter `1` to enable EASG.
- Enter `2` to disable EASG.

10. In the **`Do you want to set a root password?(yes/no)`** field, enter the required value.
11. In the **Root Password** field, enter the root password. If this field is left blank, default password will be used. Reenter the root password in the **Confirm Root Password** field.

12. In the **`Power on VM automatically after deploy?: [y/n]`** field, enter one of the following:
    - **`y`**: Indicates Avaya WebLM virtual machine is automatically powered-on after deployment.
    - **`n`**: Indicates user has to manually power on the Avaya WebLM virtual machine on KVM cockpit.
13. In the **`Proceed?[y/n]`** field, enter one of the following:
    - **`y`**: Avaya WebLM deployment begins.
    - **`n`**: Avaya WebLM deployment cancels.

    Note:

    Once the Avaya WebLM virtual machine is successfully deployed, ASP R6.0.x displays the following message: `Domain creation completed`. Otherwise, repeat step 2 on page 35 onwards.
14. Log in to the KVM Cockpit web console as **`custadm`** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
15. If Web console is in **Limited access** mode, click on **Turn on administrative access** button.

    Note:

    VMs are not visible when in **Limited access** mode.
16. For administration actions, on the top-right of the window, click on the **Limited access** or **Turn on administrative access** button.
17. Navigate to **System** > **Virtual Machines**.

    The Avaya WebLM is deployed.
18. If the **Power on VM automatically after deploy?: [y/n]** field is set to n, then click **Run** to power on the virtual machine.

    If the **Power on VM automatically after deploy?: [y/n]** field is set to y, the virtual machine starts automatically.
19. Login to Avaya WebLM virtual machine using cust user credentials.

    During the first login, change the cust user password.
20. **(Optional)** In the Overview section, enable **AutoStart** to automatically start the virtual machine whenever the host reboots.

Updating the CPU resources for KVM Cockpit

Procedure

1. Log in to the KVM Cockpit web console as **`custadm`** in the following format: https://<*IP address or FQDN of KVM host*>:9090.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

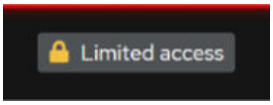


Figure 4: Limited access button

Note:

You require administrator access in order to view virtual machines. Administrator access is like root access. Ensure that you take care making updates.

3. In the Switch to administrative access window, enter the password for **`custadm`**.

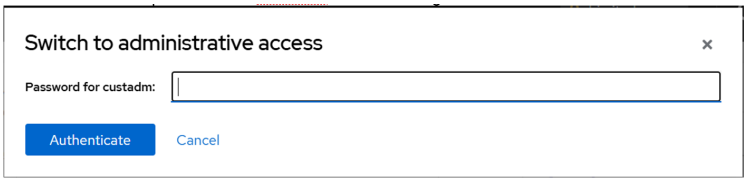


Figure 5: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

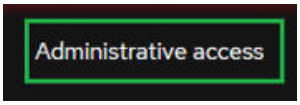


Figure 6: Administrative access button

4. Navigate to **System** > **Virtual Machines**.
5. If the virtual machine is running, right-click on the virtual machine to update and select **Shut Down**.
6. Right-click on the virtual machine and choose **Open/Edit**, and go to Overivew section.

   KVM Cockpit displays the CPU details window.
7. Update the CPU reservation details such as vCPU maximum, vCPU count, Sockets, Core per socket, and Threads per core.
8. Click **Apply**.
9. Click **Run** to start the virtual machine.

Chapter 6: Managing the ESXi host by using SDM

Adding a location

About this task

You can define the physical location of the host and configure the location-specific information. You can update the information later.

Procedure

1. On the **Locations** tab, in the Locations section, click **New**.
2. In the New Location section, do the following:
   a. In Required Location Information, type the location information.
   b. In Optional Location Information, type the network parameters for the virtual machine.
3. Click **Save**.

   System Manager displays the new location in the **Application Management Tree** section.

Adding an Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 host

About this task

Use this procedure to add an Appliance Virtualization Platform Release 8.x or earlier, ESXi, or Avaya Solutions Platform 130 Release 5.0 host. You can associate an ESXi host with an existing location.

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

Note:

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

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

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

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

You can add Avaya Solutions Platform 130 Release 5.0 (Avaya Supplied ESXi) similar to VMware ESXi host.

Note:

- To add an Appliance Virtualization Platform host, ensure that you accept the AVP EULA before you add the host to the SDM inventory.
- To add an ESXi host in Solution Deployment Manager, set the vmk0 interface as the IP Address of the ESXi host. Otherwise, Solution Deployment Manager does not support adding the ESXi host in Solution Deployment Manager.
- To add an Avaya Solutions Platform host, ensure that you use the FQDN. Do not use the IP address to add an Avaya Solutions Platform host.

Before you begin

Add a location.

Procedure

1. In **Application Management Tree**, select a location.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
3. In the New Platform section, do the following:
   a. Provide details such as the platform name, platform FQDN or IP address, username, and password.

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

   b. In **Platform Type**, select **AVP/ESXi**.
   c. Set the Platform IP address of Appliance Virtualization Platform to 192.168.13.6, if you are connected through the services port.
4. Click **Save**.
5. In the Certificate dialog box, click **Accept Certificate**.

   System Manager generates the certificate and adds the Appliance Virtualization Platform host. For the ESXi host, you can accept the certificate. If the certificate is invalid, Solution

Deployment Manager displays the error. To generate the certificate, see the VMware documentation.

In the Application Management Tree section, System Manager displays the new host in the specified location and discovers applications.

Next steps

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

Adding an Avaya Solutions Platform 130 Release 5.1 host

About this task

Use this procedure to add an Avaya Solutions Platform 130 Release 5.1 host. You can associate an Avaya Solutions Platform 130 Release 5.1 host with an existing location.

Before you begin

- If you are connected to the Avaya Solutions Platform 130 host through the services port using the SDM client, perform the following:
  1. Edit the `C:\Windows\System32\Drivers\etc\hosts` file in your laptop to add the IP Address and FQDN of the host.
  2. Add the host in the format 192.11.13.6 <*changed FQDNname*>

     For example: `192.11.13.6 esxihost6.hostdomain.com`
- If Appliance Virtualization Platform that was migrated to Avaya Solutions Platform 130 Release 5.1 is available in Solution Deployment Manager on the **Platforms** tab, remove that Appliance Virtualization Platform and then add the Avaya Solutions Platform 130 Release 5.1 host.
- Regenerate the self-signed certificate using the FQDN.

  See "Regenerating Avaya Solutions Platform 130 self-signed certificate with FQDN using the command line interface".
- Add Avaya Solutions Platform 130 host to an existing location or associate it with a new location.
- Install a valid license file on the Avaya Solutions Platform 130 Release 5.1 host.

Procedure

1. To add an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, choose one of the following:
   - For System Manager SDM, on the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.

- For SDM client, on the **SDM Client** web console, click **Application Management**.

2. In **Application Management Tree**, select an existing location or add a new location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
   a. Provide details of Platform name, Platform FQDN, username, and password.

      For Avaya Solutions Platform 130 deployment, you can also provide the root username.

   b. In **Platform Type**, select **ASP 130/S8300**.
5. Click **Save**.

   The Avaya Solutions Platform 130 certificate is updated based on the platform FQDN.

After adding an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, perform the following:

6. Deploy the required virtual machines.
7. In the Certificate dialog box, click **Accept Certificate**.

   System Manager generates the certificate and adds the Avaya Solutions Platform 130 host.

   In the **Application Management Tree**, System Manager displays the new host in the specified location and discovers applications.

Next steps

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

Managing vCenter

Creating a role for a user

About this task

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

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

Procedure

1. Log in to vCenter Server.

2. On the Home page, click **Administration** > **Roles**.

   The system displays the Create Role dialog box.
3. In **Role name**, type a role name for the user.
4. To provide complete administrative-level privileges, select the **All Privileges** check box.
5. **(Optional)** To provide minimum mandatory privileges, do the following.
   a. In All Privileges, select the following check boxes:
      - **Datastore**
      - **Datastore cluster**
      - **Distributed switch**
      - **Folder**
      - **Host profile**
      - **Network**
      - **Resource**
      - **Tasks**
      - **Virtual machine**
      - **vApp**

      Note:

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

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

      Note:

      You must select all the subprivileges under **Configuration**.
6. Click **OK** to save the privileges.

Next steps

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

Adding a vCenter to Solution Deployment Manager

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 6.0, 6.5, 6.7, 7.0, and 8.0. When you add vCenter, System Manager discovers the ESXi hosts that this vCenter manages, adds them to the repository, and displays in the Managed Hosts section.

Also, System Manager discovers virtual machines running on the ESXi host and adds to the repository.

System Manager displays vCenter, ESXi host, and virtual machines on the Manage Elements page.

Before you begin

Ensure that you have the required permissions.

Procedure

1. In the lower pane, click **Map vCenter**.
2. On the Map vCenter page, click **Add**.
3. In the New vCenter section, provide the following vCenter information:
   a. In **vCenter FQDN**, type FQDN of vCenter.
      - For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.
      - The FQDN value must match the value of the **SAN** field of the vCenter certificate. The FQDN value is case-sensitive.

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

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

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

      PSC must have a valid certificate.

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

   f. **(Optional)** In **PSC IP or FQDN**, type the IP or FQDN of PSC.
4. Click **Save**.
5. On the certificate dialog box, click **Accept Certificate**.

   The system generates the certificate and adds vCenter.

   In the Managed Hosts section, the system displays the ESXi hosts that this vCenter manages.

   Note:

   - System Manager does not support vCenter with Cluster level.

- If there is a large data center with multiple hosts in a vCenter, there can be a delay in discovering all the VMs of those hosts when mapping that vCenter in the Solution Deployment Manager. If you select a smaller number of hosts rather than all hosts, this process can be faster.

Related links

Editing vCenter on page 47
Map vCenter field descriptions on page 48
New vCenter and Edit vCenter field descriptions on page 48

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. In the lower pane, click **Map vCenter**.
2. On the Map vCenter page, select a vCenter server and click **Edit**.
3. In the Edit vCenter section, change the vCenter information as appropriate.
4. If vCenter is migrated from an earlier release, on the Certificate page, click **Save**, and then click **Accept Certificate**.
5. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:
   - Select an ESXi host and click the edit icon ( ).
   - Select one or more ESXi hosts, select the location, click **Bulk Update** > **Update**.
6. Click **Commit** to get an updated list of managed and unmanaged hosts.

   If you do not click **Commit** after you move the host from Managed Hosts to Unmanaged Hosts or vice versa, and you refresh the table, the page displays the same host in both the tables.

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

1. In the lower pane, click **Map vCenter**.
2. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
3. Click **Yes** to confirm the deletion of servers.

   The system deletes the vCenter from the inventory.

Map vCenter field descriptions

Name	Description
Name	The name of the vCenter server.
IP	The IP address of the vCenter server.
FQDN	The FQDN of the vCenter server. **Note:** Use FQDN to successfully map and log in to vCenter from Solution Deployment Manager. With IP address, the system displays an error message about the incorrect certificate and denies connection.
License	The license type of the vCenter server.
Status	The license status of the vCenter server.
Certificate Status	The certificate status of the vCenter server. The options are: • : The certificate is correct. • : The certificate is not accepted or invalid.

Button	Description
View	Displays the certificate status details of the vCenter server.
Generate/Accept Certificate	Displays the certificate dialog box where you can generate and accept a certificate for vCenter. For vCenter, you can only accept a certificate. You cannot generate a certificate.

Button	Description
Add	Displays the New vCenter page where you can add a new ESXi host.
Edit	Displays the Edit vCenter page where you can update the details and location of ESXi hosts.
Delete	Deletes the ESXi host.
Refresh	Updates the list of ESXi hosts in the Map vCenter section.

New vCenter and Edit vCenter field descriptions

Name	Description
vCenter FQDN	The FQDN of vCenter.
User Name	The user name to log in to vCenter.
Password	The password that you use to log in to vCenter.

Table continues…

Name	Description
Authentication Type	The authentication type that defines how Solution Deployment Manager performs user authentication. The options are: • **SSO**: Global username used to log in to vCenter to authenticate to an external Active Directory authentication server. • **LOCAL**: User created in vCenter If you select the authentication type as **SSO**, Solution Deployment Manager displays the **Is SSO managed by Platform Service Controller (PSC)** field.
Is SSO managed by Platform Service Controller (PSC)	The check box to specify if PSC manages SSO service. When you select the check box, the system enables **PSC IP or FQDN**.
PSC IP or FQDN	The IP or FQDN of PSC.

Button	Description
Save	Saves any changes you make to FQDN, username, and authentication type of vCenter.
Refresh	Refreshes the vCenter details.

Managed Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
Host Name	The IP address of the ESXi host.
Location	The physical location of the ESXi host.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

Button	Description
Edit	The option to edit the location and host.
Bulk Update	Provides an option to change the location of more than one ESXi hosts. **Note:** You must select a location before you click **Bulk Update**.
Update	Saves the changes that you make to the location or hostname of the ESXi host.
Commit	Commits the changes that you make to the ESXi host with location that is managed by vCenter.

Unmanaged Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
ESXi Version	Displays the versions of the ESXi host linked to **vCenter FQDN**. **Note:** • For Release 8.1 and later, do not select the 5.0 and 5.1 versions. • For Release 10.1 and later, do not select the 6.0 and 6.5 versions.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

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

Chapter 7: Configuration

Application Deployment field descriptions

Configuration Parameters

Note:

The master WebLM server and the local WebLM server must be in the same IP mode either IPv4 or IPv6.

Name	Description
IPv4 Address	The IPv4 address of the WebLM virtual machine.
Netmask	The IPv4 subnetwork mask to assign to the WebLM virtual machine.
IPv4 Default Gateway	The gateway IPv4 address to assign to the WebLM virtual machine.
IP Address of DNS Server	The DNS IPv4 address to assign to the WebLM virtual machine. Separate the IP addresses with commas (,).
Short Hostname	The short hostname to assign to the WebLM virtual machine.
IPv6 Address	The IPv6 address of the WebLM virtual machine.
IPv6 Network Prefix	The IPv6 subnetwork mask to assign to the WebLM virtual machine.
IPv6 Gateway	The gateway IPv6 address to assign to the WebLM virtual machine.
Domain Name	The domain name of the WebLM virtual machine.
Default Search List	The short hostname to assign to the WebLM virtual machine.
NTP Server IP/FQDN	The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).
Timezone	The timezone where the WebLM virtual machine is located. A list is available where you select the name of the continent and the name of the country.

WebLM CLI USER

Name	Description
WebLM command line user name	Specifies the WebLM command line user name. **Note:** Do not provide the common user names, such as admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel. Do not use the user names, such as, admin and csadmin.
WebLM command line user password	Specifies the WebLM command line user password.
Confirm Password	Re-type the WebLM command line user password.

WebLM UI Password for User - admin

Name	Description
WebLM UI admin user Password	Specifies the WebLM admin user password. **Note:** Do not use the default password for admin.
Confirm Password	Re-type the WebLM admin user password.

Enhanced Access Security Gateway (EASG) - EASG User Access

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

Networking Parameters

When you deploy the application on VMware, the system displays the Select a Network Mapping for VM Network Interfaces section.

Name	Description
Public	The port number that is mapped to public port group. You must configure Public network configuration parameter only.

Button	Description
Deploy	Displays the EULA acceptance screen. To accept EULA and start the deployment process, click **Accept**.

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 Web 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.

Chapter 8: Post-deployment verifications

Logging on to the WebLM web console

About this task

The WebLM web console is the main interface of Avaya WebLM. You must log on to the WebLM web console to perform any task. The WebLM home page displays the navigation menu that provides access to shared services to perform operations that WebLM supports.

Before you begin

Get a user account to log on to the WebLM web console. To create a new account, go to the Avaya Support website at https://support.avaya.com.

Procedure

1. On a web browser, type the WebLM URL: `https://<IP Address or Fully Qualified Domain Name>/WebLM` or `https://<IP Address or Fully Qualified Domain Name>/`.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Click **Log On**.

   WebLM validates the credentials with the WebLM user account and displays the home page with the WebLM *<version_number>*. If the credentials fail, WebLM displays an error message and prompts you to reenter the credentials.

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 about installing a license file, see *Administering standalone Avaya WebLM*.

Verifying the WebLM software version

About this task

To verify the WebLM version, perform the following procedure after you deploy or upgrade WebLM.

- On the WebLM console, do the following:
  1. Log on to the WebLM web console with administrator privilege credentials.
  2. On the home page, click **About**.

     WebLM displays the About WebLM window with the build details.
  3. Verify the software version of WebLM.
- On the WebLM command line interface, do the following:
  1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
  2. Do one of the following:

  - Type **swversion**.

    WebLM displays the following message:

```
**********************************************
StandAlone WebLM Software Information

**********************************************
Standalone WebLM on VMware 10.1.0.0 Build Number 10.1.0.0.0.xxxxx
Patch 10.1.0.0 Build Number 10.1.2.0.0.xxxxx

**********************************************
Operating System Information

**********************************************
Red Hat Enterprise Linux release 8.6 (Ootpa)
Linux weblm50.avaya.com 4.18.0-372.19.1.el8_6.x86_64 #1 SMP Mon
Jul 18 11:14:02 EDT 2022 x86_64 x86_64 x86_64 GNU/Linux

**********************************************
JAVA Version

openjdk version "1.8.0_342"
OpenJDK Runtime Environment (build 1.8.0_342-b07)

OpenJDK 64-Bit Server VM (build 25.342-b07, mixed mode)
```

- Type **swversion -s**.

Note:

The output varies based on the application deployment and the virtualization environment.

- Following is an example of VMware deployment using profile1:

```
Application Name: WebLM
Application Version: 10.1.2.0.0.xxxxx
Application Deployment: Virtual Machine
Virtualization Environment: VMware
Current application size: profile1
```

- Following is an example of *Software-Only* deployment using profile2:

```
Application Name: WebLM
Application Version: 10.1.2.0.0.xxxxx
Application Deployment: Software Only
Virtualization Environment: AWS
Current application size: profile2
```

Enhanced Access Security Gateway

Enhanced Access Security Gateway (EASG) overview

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

Managing EASG from CLI

About this task

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

Before you begin

Log in to the application CLI interface.

Procedure

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

   The system displays the status of EASG.

2. To enable EASG, do the following:
   a. Run the command: **`EASGManage --enableEASG`**.

      The system displays the following message:

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

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

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

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

3. To disable EASG, do the following:
   a. Run the command: **`EASGManage --disableEASG`**.

      The system displays the following message:

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

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

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

Viewing the EASG certificate information

Procedure

Log in to the application CLI interface.

EASG site certificate

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

Managing site certificates

Before you begin

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

Procedure

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

Chapter 9: Maintenance

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

Note:

The existing license files become invalid when you:

- change the WebLM IP address
- perform a WebLM update
- clone a virtual machine

When you redeploy the WebLM, then you must reinstall a new license file to match the new Host ID generated in the WebLM server.

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

Before you begin

Log in to the WebLM command line interface with administrator privilege CLI user credentials.

Important:

Ensure that WebLM maintenance is not in progress.

Procedure

1. Type `changeIPFQDN –IP <IP Address> –FQDN <FQDN> –GATEWAY <Gateway address> –NETMASK <Netmask address> –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 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.

2. To add more than one IP address for the DNS server, type `changeIPFQDN –dns primary_DNS_IPaddress, secondary_DNS_IPaddress, DNS_N_IPaddress....” to “changeIPFQDN –dns primary_DNS_IPaddress, secondary_DNS_IPaddress, ..., DNS_N_IPaddress.`

   You must separate each DNS IP address by a comma (,). For example, `changeIPFQDN –dns 10.14.16.2,14.17.13.5.`

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

   Note:

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

Related links

Rehosting license files on page 55
WebLM CLI operations on page 65

Configuring multiple DNS IP addresses

Before you begin

- Deploy the WebLM application.
- Start the WebLM virtual machine.

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

Note:

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

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.

   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, type `changeIPFQDN –dns primary_DNS_IPaddress, secondary_DNS_IPaddress, DNS_N_IPaddress....” to “changeIPFQDN –dns primary_DNS_IPaddress, secondary_DNS_IPaddress, ..., DNS_N_IPaddress`.

   You must separate each DNS IP address by a comma (,). For example, `changeIPFQDN -dns 10.14.16.2,14.17.13.5`.

   The system takes a few seconds to apply the DNS changes to the network.
4. Log on to the WebLM web console with administrator privilege credentials.
5. Ensure that the system displays the multiple DNS IP addresses.

Related links

WebLM CLI operations on page 65

Configuring the time zone

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Type `configureTimeZone`.
3. Select the time zone from the list.

   For example, America/Denver.

Related links

WebLM CLI operations on page 65

Configuring the NTP server

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Type `configureNTP <IP address of the NTP server>`.

   The system configures the NTP server.

Related links

WebLM CLI operations on page 65

Resetting the WebLM password through CLI

About this task

Any CLI user who is part of the gcliuser and admin groups created during deployment can run the command to reset the WebLM password through CLI.

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Type the **`weblm_password`** command and press `Enter`.
3. In **Enter new WebLM UI Admin Password**, type a new password.

   The password must be 6-14 characters long.
4. In **Re-enter new WebLM UI Admin Password**, type the new password again.

   WebLM successfully resets the password. You can log in to the WebLM UI with user 'admin' and the new password.

Performing WebLM backup

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Type **`WebLMBackup <backup_location>`**.

   Where: <backup_location> is the absolute path of the backup file.

   You can copy the backup files to a remote computer or to an external storage device.

Performing WebLM restore

About this task

WebLM restores user, data, and license information from the backup based on the data available in the backup file.

Procedure

1. Log in to the WebLM command-line interface with administrator privilege CLI user credentials.
2. Type **`WebLMRestore <Full path where the Backup files have been saved>`**.

Where, **<Full path where the Backup files have been saved>** is the absolute path of the backup file.

WebLM restores required details from the specified backup file location.

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 vSphere Web 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 vSphere Web 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**.

WebLM CLI operations

Note:

Any CLI user who is part of the gcliuser, and admin groups created at the time of deployment can execute the following commands:

#	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 names of the NTP servers with commas (,).

Table continues…

#	Command	Parameters	Description	Usage
3.	**configureTimeZone**	< Time zone that you want to select >	Configures the time zone with the value that you select.	Select a time zone. For example, America/Denver
4.	**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/`.
5.	**weblm_password**		Resets the WebLM password through CLI. Any CLI user who is part of the gcliuser and admin groups, created at the time of deployment can execute the command.	
6.	**configureTLS**	• -ENABLE_TLS_VERSIONS TLSv1.3 • -ENABLE_TLS_VERSIONS TLSv1.2 • -ENABLE_TLS_VERSIONS TLSv1.1 • -ENABLE_TLS_VERSIONS TLSv1.0	Configures the TLS version.	Type one of the following options: • **configureTLS -ENABLE_TLS_VERSIONS TLSv1.3** • **configureTLS -ENABLE_TLS_VERSIONS TLSv1.2** • **configureTLS -ENABLE_TLS_VERSIONS TLSv1.1** • **configureTLS -ENABLE_TLS_VERSIONS TLSv1.0**
7.	**collectLogs**		Collects the WebLM logs in the `/tmp/WebLM_Logs_DDMonYY_XXXXXXXXXXXXXXX.zip` file.	
8.	**swversion**		Verifies the WebLM software version.	

Table continues…

#	Command	Parameters	Description	Usage
9.	**swversion -s**		Verifies the WebLM software version and also displays information about the application name, profile, and deployment type.	**swversion -s** **Note:** The output varies based on the application deployment and the virtualization environment.
10.	**WebLMBackup**	<backup_location>	Performs the WebLM backup.	**WebLMBackup <backup_location>** **Note:** You can copy the backup files to a remote computer or to an external storage device.
11.	**WebLMRestore**	<Full path where the Backup files have been saved>	WebLM restores user, data, and license information from the backup based on the data available in the backup file.	**WebLMRestore <Full path where the Backup files have been saved>**
12.	**configureCiphersList**	• 1: To view the configured cipher suites. • 2: To configure relaxed cipher suites. • 3: To configure strict cipher suites.	You can toggle between the Relaxed cipher suites or Strict cipher suites.	
13.	**weblmStart**		Starts the WebLM Application server.	**weblmStart**
14.	**weblmStatus**		Checks the status of the WebLM Application server.	**weblmStatus**
15.	**weblmStop**		Stops the WebLM Application server.	**weblmStop**
16.	**weblmRestart**		Restarts the WebLM Application server.	**weblmRestart**

Table continues…

#	Command	Parameters	Description	Usage
17.	**manageWebLMCertificate**	• -display • -replace • -generateSelfSigned	Allows you to view a WebLM certificate, replace a WebLM certificate with a third-party certificate, and generate a self-signed WebLM certificate.	Type one of the following options: • **manageWebLMCertificate -display** • **manageWebLMCertificate -replace -certpath <file> -password <password>** • **manageWebLMCertificate -generateSelfSigned**
18.	**manageCACertificates**	• -list • -add • -remove	Allows you to view, add, and delete CA imported certificates in the WebLM server truststore.	Type one of the following options: • **manageCACertificates -list** • **manageCACertificates -add -certpath <file> -alias <alias>** • **manageCACertificates -remove -alias <alias>**

Table continues…

#	Command	Parameters	Description	Usage
19.	**setWebLMClientAuth**	• 1: Displays existing WebLM client certificate authentication configuration. • 2: Enables WebLM client certificate authentication. • 3: Disables WebLM client certificate authentication.	Allows you to manage the client certificate authentication for WebLM port 52233. **Note:** From 10.1.3.3 onwards, the WebLM client certificate authentication configuration is ON by default and you need to setup WebLM client certificate for communication with WebLM server for licensing to work. You must disable client certificate authentication if you do not require it (WebLM client certificate for communication). You can re-enable it once the WebLM client certificate for communication is configured.	

Table continues…

#	Command	Parameters	Description	Usage

20	**toggleOldWebLMClientCommunication**	Run this utility as the following:
		• Type `1` to check the old WebLM client communication status
		• Type `2` to enable the old WebLM client communication status
		• Type `3` to disable the old WebLM client communication status
		Note:
		The user can enter the values specified above based on their usage.
			This utility is used to check, enable, and disable the old WebLM client communication status with releases 10.1.3.1 and later. For the older WebLM client communication, the default status is ENABLED.	• Type `1` to check the old WebLM client communication status.
				• Type `2` to enable the old WebLM client communication status.
				• Type `3` to disable the old WebLM client communication status.
				If your input is 1 and the current status is enabled, the message
				`Old WebLM client communication status is ENABLED`
				is displayed.
				If the current status is disabled, the message
				`Old WebLM client communication status is DISABLED`
				is displayed.
				If your input is 2, the message
				`Old WebLM client communication is now ENABLED`
				is displayed.
				If your input is 3, the message
				`Old WebLM client communication is now DISABLED`
				is displayed.

Viewing the job history of virtual machine operations

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the desktop, click the SDM icon (), and then click **Application Management**.
3. In the lower pane, click **Job History**.
4. On the Job History page, in **Operation**, select one or more operations.
5. Click **Submit**.

   The page displays the details of jobs that you selected.

Job History field descriptions

Name/Button	Description
Operation	The operation that is performed on a virtual machine. You can select one or more operations that are performed on a virtual machine, such as host restart, virtual machine deployment, and patch installation.
Submit	Provides details of jobs that you selected.

History

Name	Description
Job ID	The unique name of the virtual machine management job.
IP/FQDN	The IP address or host name of the virtual machine or the host where the operation is performed.
Operation	The operation performed on the virtual machine or host. For example, host refresh, virtual machine deployment, and patch installation.
Status	The status of the job.
Start Time	The start time of the job.
End Time	The end time of the job.

Monitoring a host and virtual machine

Monitoring a platform

Procedure

1. Click **Monitor Platforms**.

2. On the Monitor Hosts page, do the following:
   a. In **Hosts**, click a host.
   b. Click **Generate Graph**.

   The system displays the graph regarding the CPU/memory usage of the host that you selected.

Monitoring an application

Procedure

1. Click **Monitor Applications**.
2. In the Monitor VMs page, do the following:
   a. In **Hosts**, click a host.
   b. In **Virtual machines**, click a virtual machine on the host that you selected.
3. Click **Generate Graph**.

   The system displays the graph regarding the CPU/memory usage of the virtual machine that you selected.

Chapter 10: Resources

Avaya WebLM documentation

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

Title	Description	Audience
Implementing		
Deploying standalone Avaya WebLM in Virtualized Environment	Deploy the application in virtualized environment.	Implementation personnel
Deploying standalone Avaya WebLM in Software-Only and Infrastructure as a Service Environment	Deploy the application on software-only environment and cloud services.	Implementation personnel
Upgrading standalone Avaya WebLM	Upgrade the application.	Implementation personnel
Administering		
Administering standalone Avaya WebLM	Perform administration tasks	System administrators

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.

8. Click to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.

- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available at http://www.avaya-learning.com/. To search for the course, enter the course code in the **Search** field and click **Go**.

Course code	Course title
71201V	Integrating Avaya Aura® Core Components

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

Using the Avaya InSite Knowledge Base

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

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.

- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

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

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

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Appendix A: Best practices for VM performance and features

BIOS

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

For information about how to use BIOS settings to improve the environment for latency-sensitive workloads for an application, see the technical white paper, “Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs” at https://www.vmware.com/.

The following sections describe the recommended BIOS settings for:

- Intel Virtualization Technology
- Dell PowerEdge Servers

Related links

Intel Virtualization Technology on page 78
Dell PowerEdge Server on page 79

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 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 78

Dell PowerEdge Server

The following are the BIOS recommendations for Dell PowerEdge Servers supported by Avaya SBC:

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 78

VMware Tools

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

VMware tools provide:

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

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

Important:

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

Timekeeping

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

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

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

In certain situations, the ESXi hypervisor pushes an updated view of its clock into a virtual machine. These situations include starting the virtual machine and resuming a suspended virtual machine, If this view differs more than 1000 seconds from the view that is received over the network, the NTP service might shutdown. In this situation, the guest OS administrator must manually set the guest clock to be the same or as close as possible to the network time source clock. To keep the NTP service active, the clock on the ESXi host must also use an accurate clock source, such as the same network time source that is used by the guest operating system.

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

After you administer the NTP service in the application, run the **`chronyc sources -v`** command from a command window. The results from this command:

- 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 **chronyd**. 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.

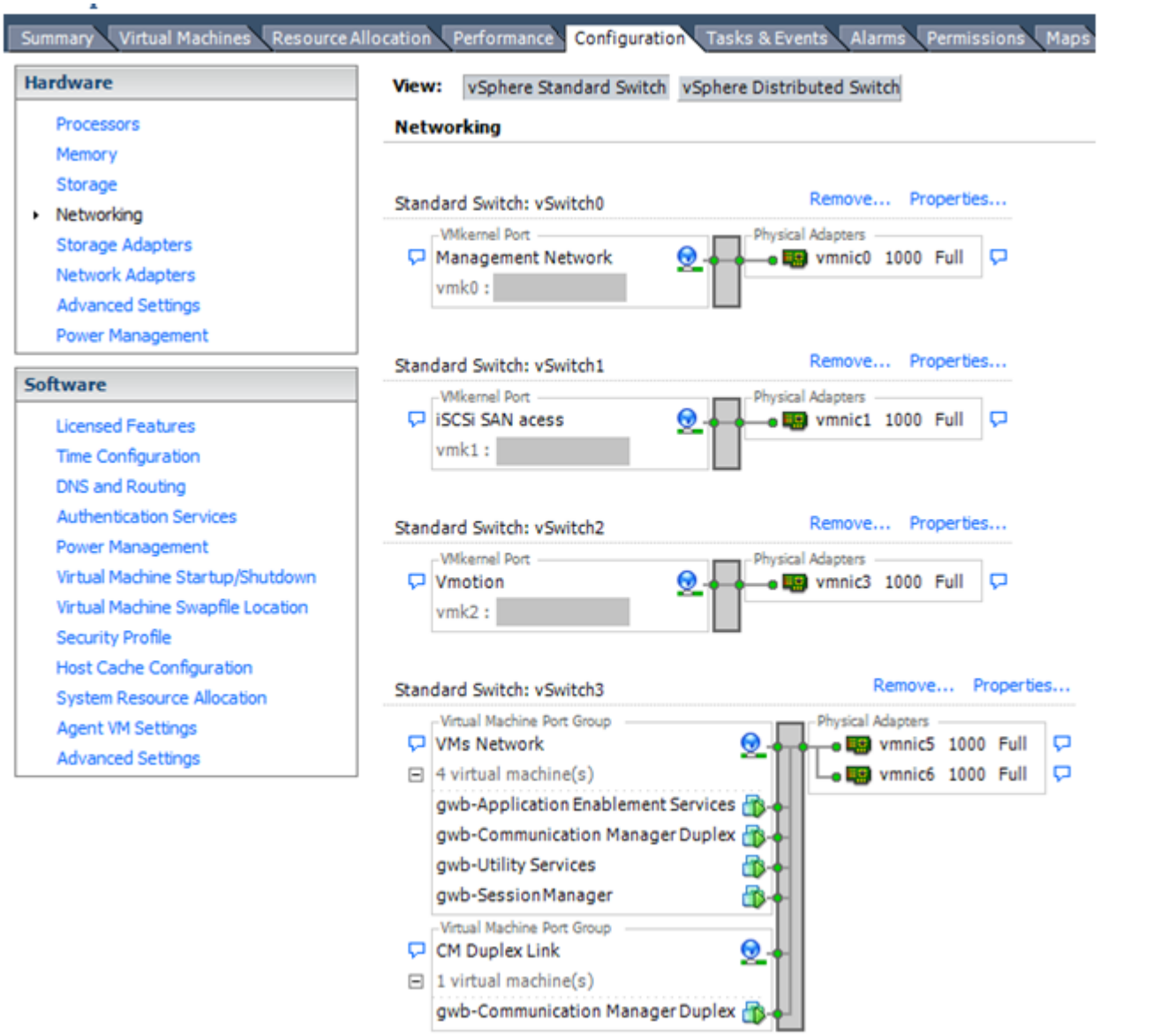
This section is not a substitute for the VMware documentation. Review the VMware networking best practices before deploying any applications on an ESXi host.

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).

Disclaimer: The images in this section represent older ESXi versions and may vary for the latest ESXi versions.

Networking Avaya applications on VMware ESXi – Example 1

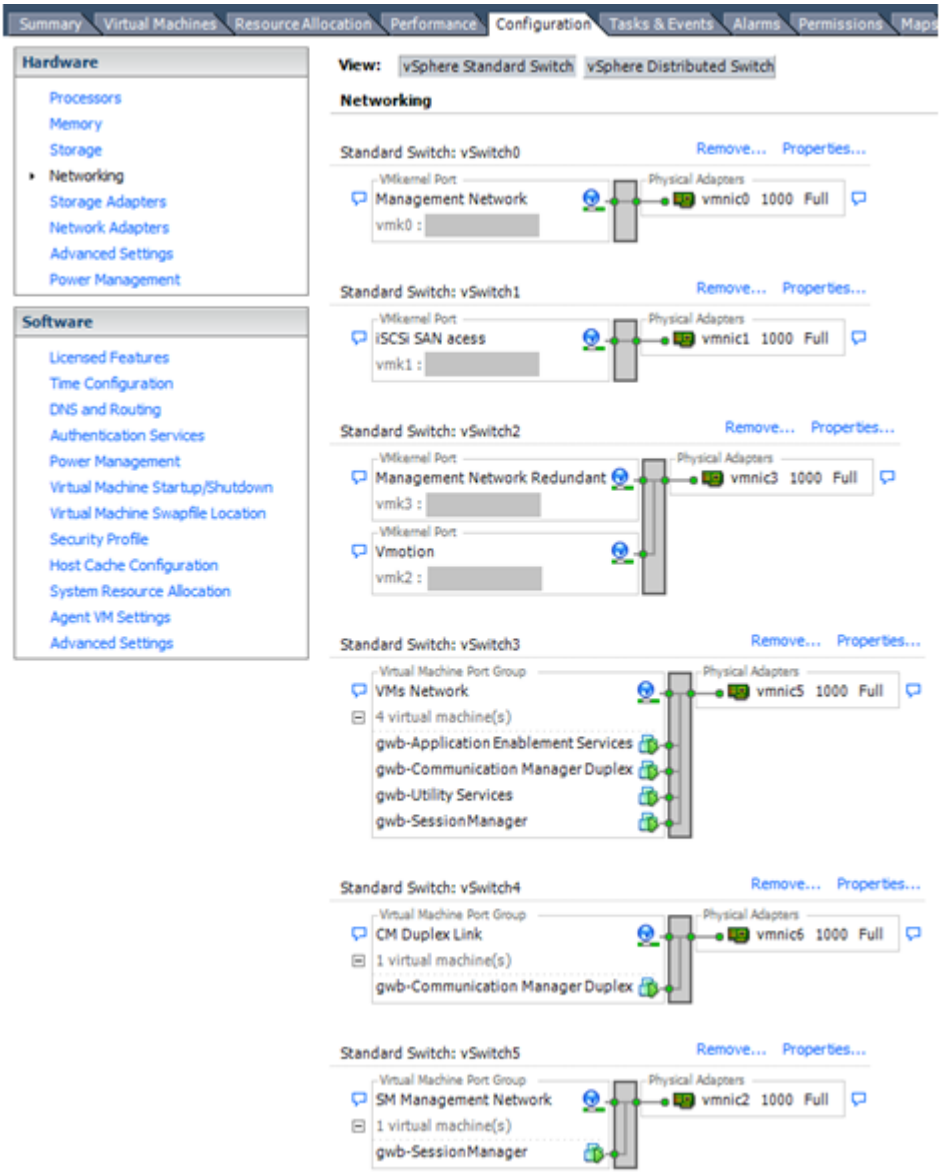


This configuration describes a simple version of networking Avaya applications within the same ESXi host. Highlights to note:

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

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

Networking Avaya applications on VMware ESXi – Example 2



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

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

References

Title	Link
Product Support Notice PSN003556u	Go to https://support.avaya.com and search for PSN003556u.
VMware vSphere 8.0 Documentation	Go to https://www.vmware.com/support/pubs/ and search for *VMware vSphere 8.0 Documentation*.
VMware vSphere 7.0 Documentation	Go to https://www.vmware.com/support/pubs/ and search for *VMware vSphere 7.0 Documentation*.
VMware Documentation Sets	https://www.vmware.com/support/pubs/

Storage

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

Thin vs. thick deployments

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

- Thin-provisioned disks can grow to the full size as specified at the time of virtual disk creation, but they cannot shrink. Once you allocate the blocks, you cannot deallocate them.
- Thin-provisioned disks run the risk of overallocating storage. If storage is over-allocated, thin virtual disks can grow to fill an entire datastore if left unchecked.
- If a guest operating system needs to make use of a virtual disk, the guest operating system must first partition and format the disk to a file system it can recognize. Depending on the type of format selected within the guest operating system, the formatting process may cause the thin-provisioned disk to grow to full size. For example, if you present a thin-provisioned disk to a Microsoft Windows operating system and format the disk, unless you explicitly select the Quick Format option, the format tool in Microsoft Windows writes information to all sectors on the disk, which in turn inflates the thin-provisioned disk to full size.

VMware snapshots

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

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

Caution:

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

Only take snapshots during a maintenance window.

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.

  If your virtual machine contains snapshots that are more than 72 hours old, system performance might be impacted. When you no longer need a snapshot, remember to delete it.
- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.
- When taking a snapshot, do not save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear

to be active or in progress and can cause confusion to the user. To create a clean snapshot image from which to boot, do the following when you create a snapshot:

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

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

Note:

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

Related resources

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

VMware vMotion

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

With vMotion, you can:

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

Before using vMotion, you must:

- Ensure that each host that migrates virtual machines to or from the host uses a licensed vMotion application and the vMotion is enabled.

- Ensure that you have identical vSwitches. You must enable vMotion on these vSwitches.
- Ensure that the Port Groups are identical for vMotion.
- Use a dedicated NIC to ensure the best performance.

Note:

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

VMware cloning

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

Note:

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

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

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

VMware high availability

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

Note:

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

VMware features supported by Avaya Aura®

This section does not cover Avaya Solutions Platform (ASP) 130 and ASP S83000. Avaya does not support advanced VMware features on its ASP 130 and ASP S8300 hardware. It supports the basic VMware features as listed in the following table. For more information about support and limitations on ASP 130 and ASP S8300, see https://download.avaya.com/css/public/documents/101062774.

Note:

For more information about Avaya Aura® Media Server, see *Deploying and Updating Avaya Aura® Media Server Appliance*.

The following table lists the VMware features supported on customer-provided Virtualized Environment for various Avaya Aura® Release10.2 components.

Product or feature	Communication Manager	Session Manager	System Manager	Application Enablement Services	Avaya SBC	Avaya Aura® Device Services
ESXi 7.0	Yes	Yes	Yes	Yes	Yes	Yes
ESXi 8.0	Yes	Yes	Yes	Yes	Yes	Yes
vCenter See foot note[1]	Yes	Yes	Yes	Yes	Yes	Yes
vSphere WebClient (HTML5)	Yes	Yes	Yes	Yes	Yes	Yes
VMFS 6	Yes	Yes	Yes	Yes	Yes	Yes
VMware vMotion See foot note[2]	Yes	Yes	Yes	Yes	Yes	Yes
Storage vMotion	Yes	Yes	Yes	Yes	Yes	Yes
VMware Snapshot See foot note[3]	Yes	Yes	Yes	Yes	Yes	Yes
VMware Live Snapshot	Not supported	Not supported	Not supported	Not supported	Not supported	No
VMware High Availability	Yes	Yes	Yes	Yes	Yes	Yes

Table continues…

[1] Limited to deployment, managing VMs, basic monitoring, and making VMs part of a vCenter cluster.
[2] Ensure that vMotion occurs when an Avaya Aura® application virtual machine is in maintenance mode.

Product or feature	Communication Manager	Session Manager	System Manager	Application Enablement Services	Avaya SBC	Avaya Aura® Device Services
Proactive High Availability	Best effort basis support (Not tested)	Best effort basis support (Not tested)	Best effort basis support (Not tested)	Best effort basis support (Not tested)	Best effort basis support (Not tested)	Best effort basis support (Not tested)
Storage DRS	Yes	Yes	Yes	Yes	Yes	Yes
Hyperthreading	Yes	Yes	Yes	Yes	Yes	Yes
Hyperthreading ratio for Virtual CPUs and Physical CPU	2:1	2:1	2:1	2:1	2:1	2:1
VMware DRS (Compute and Memory) See foot note[4]	Yes	Yes	Yes	Yes See foot note[5]	Yes	Yes
Secure boot for virtual machine	Yes	Yes	Yes	Yes	Yes	Yes
Content Library	Yes	Yes	Yes	Yes	Yes	Yes
VMware Fault Tolerance (FT)	Not supported	Not supported	Not supported	Yes See foot note[6]	Not supported	Yes
vSphere Standard Switch	Yes	Yes	Yes	Yes	Yes	Yes
vSphere Distributed Switch	Yes	Yes	Yes	Yes	Yes	Yes
Hot Pluggable Virtual Hardware	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported

Table continues…

[3] Snapshots should be used when patching the products. As per the backup mechanism provided in the product-specific documentation, you should perform daily backups instead of using snapshots of the products. Applicable for Communication Manager, Session Manager, System Manager, and Application Enablement Services.

[4] With two conservative modes - Applicable for Communication Manager, Session Manager, System Manager, and Application Enablement Services.

[5] DRS supports In-cluster migration - Applicable for Avaya SBC for Enterprise.

[6] For more information about the Fault Tolerance for Application Enablement Services, see *Avaya Aura Application Enablement (AE) Services 7.x, 8.x, and 10.x High Availability (HA) White Paper.*

Product or feature	Communication Manager	Session Manager	System Manager	Application Enablement Services	Avaya SBC	Avaya Aura® Device Services
Reservation Required see foot note[7]	Yes	Yes	Yes	Yes	Yes	Yes
vSAN support See foot note[8]	Yes	Yes	Yes	Yes	Yes	Yes
Thin Provisioning	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported

[7] Avaya Aura® does not support reservationless deployments on ASP 130. Avaya recommends always making reservations when choosing a reservationless deployment. It is crucial to strictly adhere to the guidelines outlined in the Application Notes. For more information on reservationless deployment, see the *"Application Notes on Best Practices for Reservationless deployment of Avaya Aura® software release 10.1 on VMware"* at https://support.avaya.com .

[8] If you are using vSAN, use Thick Provisioning. Even though VMware supports vSAN with Thin Provisioning, Avaya Aura® does not support it.

Appendix B: PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) for any software update. For example, a PCN must accompany a service pack or an update that must be applied universally. Avaya issues a product-support notice (PSN) to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a work around for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at https://support.avaya.com and log in.
2. On the top of the page, in **Search Product**, type the product name.

   The Avaya Support website displays the product name.
3. Select the required product name.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. On the product page, click **Product Documents**.
6. In the Latest Support, Service and Product Correction Notices section, click **View All Notices**.
7. Select the appropriate filters as per your search requirement.

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

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

Signing up for PCNs and PSNs

About this task

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

To sign up for notifications:

Procedure

1. Go to https://support.avaya.com and search for “Guide to Managing Your Avaya Access Profile for Customers and Partners”.

   Under the Search Results section, click Guide to Managing Your Avaya Access Profile for Customers and Partners.

2. Set up e-notifications.

   For detailed information, see the **Subscribe to E-Notifications** procedure.

Glossary

Application	A software solution development by Avaya that includes a guest operating system.
Blade	A blade server is a stripped-down server computer with a modular design optimized to minimize the use of physical space and energy. Although many components are removed from blade servers to save space, minimize power consumption and other considerations, the blade still has all of the functional components to be considered a computer.
EASG	Enhanced Access Security Gateway. The Avaya Services Logins to access your system remotely. The product must be registered using the Avaya Global Registration Tool for enabling the system for Avaya Remote Connectivity.
ESXi	A virtualization layer that runs directly on the server hardware. Also known as a *bare-metal hypervisor.* Provides processor, memory, storage, and networking resources on multiple virtual machines.
Hypervisor	A hypervisor is also known as a Virtual Machine Manager (VMM). A hypervisor is a hardware virtualization technique which runs multiple operating systems on the same shared physical server.
MAC	Media Access Control address. A unique identifier assigned to network interfaces for communication on the physical network segment.
OVA	Open Virtualization Appliance. An OVA contains the virtual machine description, disk images, and a manifest zipped into a single file. The OVA follows the Distributed Management Task Force (DMTF) specification.
PLDS	Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.
Reservation	A reservation specifies the guaranteed minimum required amounts of CPU or memory for a virtual machine.
SAN	Storage Area Network. A SAN is a dedicated network that provides access to consolidated data storage. SANs are primarily used to make

	storage devices, such as disk arrays, accessible to servers so that the devices appear as locally attached devices to the operating system.
Snapshot	The state of a virtual appliance configuration at a particular point in time. Creating a snapshot can affect service. Some Avaya virtual appliances have limitations and others have specific instructions for creating snapshots.
Storage vMotion	A VMware feature that migrates virtual machine disk files from one data storage location to another with limited impact to end users.
vCenter Server	An administrative interface from VMware for the entire virtual infrastructure or data center, including VMs, ESXi hosts, deployment profiles, distributed virtual networking, and hardware monitoring.
virtual appliance	A virtual appliance is a single software application bundled with an operating system.
VM	Virtual Machine. Replica of a physical server from an operational perspective. A VM is a software implementation of a machine (for example, a computer) that executes programs similar to a physical machine.
vMotion	A VMware feature that migrates a running virtual machine from one physical server to another with minimal downtime or impact to end users. vMotion cannot be used to move virtual machines from one data center to another.
VMware HA	VMware High Availability. A VMware feature for supporting virtual application failover by migrating the application from one ESXi host to another. Since the entire host fails over, several applications or virtual machines can be involved. The failover is a reboot recovery level which can take several minutes.
vSphere Web Client	The vSphere Web Client is an interface for administering vCenter Server and ESXi. Downloadable versions are VMware 5.5 and 6.0. A browser-based Web client version is VMware 6.5 and later.

Index

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W