Deploying Avaya Aura® Experience Portal in an Avaya Customer Experience Virtualized Environment

Release 6.0.2
Issue 2
June 2013

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each vAppliance will have its own ordering code. Note that each instance of a vAppliance must be separately ordered. If the end user customer or Business Partner would like to install two of the same type of vAppliances, then two vAppliances of that type must be ordered.

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

Avaya, the Avaya logo, Avaya Aura® Experience Portal, Avaya Aura® Communication Manager, and Avaya Aura® Orchestration Designer are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Document changes since last issue

The following change has been made to this document since the last issue:

- Updated the resource requirements in Experience Portal Virtual Machine resource requirements on page 16.

Purpose

This document provides procedures for deploying the Avaya Aura® Experience Portal virtual application in the Avaya Customer Experience Virtualized Environment. This document includes installation, configuration, initial administration, troubleshooting, and basic maintenance checklists and procedures.

Intended audience

The primary audience for this document is anyone who is involved with installing, configuring, and verifying Avaya Aura® Experience Portal in a VMware® vSphere™ 5.0 or 5.1 virtualization environment at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

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

Related resources

Documentation

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

Title	Description	Audience
Avaya Customer Experience Virtualized Environment Solution Description	Describes the Avaya Customer Experience Virtualized Environment market solution from a holistic perspective focusing on the functional view of the solution architecture.	Sales engineers Solution architects Implementation engineers Support personnel
Application Notes for Avaya Aura® Experience Portal 6.0 on VMware vSphere	Describes the best practices and guidelines for Avaya Aura® Experience Portal configuration in a virtual environment that uses VMware vSphere. The data and recommendations in this document are a result of a joint effort between Avaya and VMware to validate Avaya Aura® Experience Portal configuration on VMware vSphere.	Sales engineers Design engineers Implementation engineers Implementation engineers
Avaya WebLM using VMware® in the Virtualized Environment Deployment Guide	Provides procedures for deploying the Avaya WebLM OVA in a virtualized environment.	Implementation engineers
Administering Avaya Aura® Experience Portal	Provides procedures for administering and configuring Avaya Aura® Experience Portal with a Web-based interface.	Implementation engineers System administrators

Title	Description	Audience
Avaya Aura® Experience Portal 6.0 Service Pack 2 Release Note	This document contains Avaya Aura® Experience Portal 6.0 Service Pack 2 product information that is not included in the product documentation. This document highlights known issues about Avaya Aura® Experience Portal along with workarounds that are available.	Implementation engineers System administrators

Training

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

Course code	Course title
4C00100V 4C00100I	Avaya Aura® Experience Portal Implementation
5C00090V 5C00090I	Avaya Aura® Experience Portal, Avaya Aura® Orchestration Designer, and Proactive Outreach Manager Maintenance and Troubleshooting
3C00093O	Avaya Aura® Contact Center Experience Portal Technical Sales Knowledge Session
V: Virtual course I: Instructor led course	

Avaya Mentor videos

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

Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

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

Chapter 2: Architecture overview

Avaya Customer Experience Virtualized Environment overview

Avaya Customer Experience Virtualized Environment integrates Avaya Aura® Contact Center with VMware® virtualized server architecture. Avaya Customer Experience Virtualized Environment provides the following benefits:

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

For existing customers who have a VMware IT infrastructure, Avaya Customer Experience Virtualized Environment provides an opportunity to upgrade to the next release level of collaboration using their own VMware infrastructure.

The Avaya Customer Experience Virtualized Environment project is only for VMware and is not intended to include any other industry hypervisor.

Note:

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

- server and host
- reservations and configuration values

Customer deployment

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

The customer provides the servers and the VMware infrastructure including the VMware licenses.

Software delivery

The software is delivered as one or more pre-packaged Open Virtualization Appliance (OVA) files that are posted on the Avaya Product Licensing and Download System (PLDS). Each OVA contains the following components:

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

Patches and upgrades

A minimum patch level can be required for each supported application. See the compatibility matrix tool at http://support.avaya.com/CompatibilityMatrix/Index.aspx for more information regarding the application patch requirements.

Important:

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

Performance and capacities

The OVA template is built with configuration values which optimize performance and follow recommended Best Practices.

Caution:

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

VMware components

VMware Software Component	Description
ESXi Host	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.
vSphere Client	The client application that is installed on a personal computer or accessible through a Web interface. It connects to a vCenter server or directly to an ESXi host in the case where vCenter Server is not used. Enables the installation and management of virtual machines.
vCenter Server	vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. Virtual machines are managed through vSphere Client software which provides alarming and performance monitoring of ESXi hosts and virtual machines. vCenter Server provides VMware features such as High Availability and vMotion.

Deployment guidelines

The high-level deployment steps are:

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

The following are deployment guidelines for the virtual appliances:

- Deploy as many virtual appliances on the same host as possible.
- Deploy the virtual appliances on the same cluster if the cluster goes beyond the host boundary.
- Segment redundant elements on a different cluster. For example, CMS HA.
- Create a tiered or segmented cluster infrastructure that isolates critical applications, such as CMS, from other VMs.
- Ensure that you have enough resources for rainy day scenarios or conditions. Do not configure resources only for traffic or performance on an average day.
- Do not over-subscribe resources. Over-subscribing affects performance.
- Monitor the blade, host, and virtual appliance performance.

Important:

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

Chapter 3: Planning and configuration

Planning

Ensure that the following activities have been completed before deploying the virtual appliance:

#	Action	Notes	✔
1	Coordinate with service providers.		
2	All required licenses have been purchased and are accessible.		
3	Staging and verification activities have been planned and resources assigned.		

Server hardware and resources

VMware offers compatibility guides that list system, I/O, storage/SAN and backup compatibility with VMware infrastructure. See http://www.vmware.com/resources/guides.html to view VMware certified compatibility guides and product interoperability matrixes.

The VMware-certified servers must be running ESXi 5.0 and any of its updates, or ESXi 5.1 and any of its updates.

Configuration tools and utilities

Ensure that the following tools and utilities are available before you deploy Experience Portal:

- The Experience Portal OVAs, which you can download from the Avaya Product Licensing and Delivery System (PLDS) website.
- A computer with VMware vSphere Client that can route to the VMware server.

- The Avaya Access Security Gateway (ASG) tool. Avaya Service technicians use ASG to remotely log in to servers that are under service agreement.
- The customer order number.
- The Avaya WebLM license server OVA or a WebLM license server.

Note:

You do not need the Avaya WebLM license server OVA if you have installed a WebLM license server that is not already in use to license an Experience Portal system.

WebLM manages the licensing of Experience Portal. For more information about the Avaya WebLM OVA, see *Avaya WebLM using VMware® in the Virtualized Environment Deployment Guide* on the Avaya Support website at https://www.support.avaya.com.

Experience Portal Virtual Machine resource requirements

The following table provides VMware resource requirements for the Experience Portal (Primary EPM, MPP, and Auxiliary EPM) configuration.

VMware Resource	Values
vCPU Cores	4
vCPU reservation	2400 MHz
Minimum CPU speed	2.9 GHz Intel Xeon E5-26900 or equivalent
Memory	4096 MB
Memory reservation	4096 MB
Storage reservation	100 GB
Shared NICs	One @ 1000 Mbps

VMware software requirements

For optimal results, use the following VMware software versions:

- VMware vSphere ESXi 5.0 or ESXi 5.1
- VMware vCenter Server 5.0 or 5.1 (optional)

ESXi 5.0 can be added under vCenter Server 5.0 and vCenter Server 5.1. However, ESXi 5.1 can be added only under vCenter Server 5.1. See *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php to view compatibility with other solution releases.

Capacity

The Experience Portal capacity limits and port sizing details are documented in *Application Notes for Avaya Aura® Experience Portal 6.0 on VMware vSphere*. You can download the document from the Avaya Support website at http://support.avaya.com.

Default configuration data

The following table identifies the default parameters that are provided by the OVA files.

OVA file name	Parameter	Value
Primary EPM Auxiliary EPM MPP	Destination directory	`/opt/Avaya/ExperiencePortal`
Primary EPM	Initial Experience Portal Admin username and password	Username: epadmin Password: epadmin01
Primary EPM Auxiliary EPM MPP	Root access to Linux	Username: sroot Password: sroot01
Primary EPM Auxiliary EPM MPP	Non-root access to Linux	Username: craft Password: craft01
Primary EPM Auxiliary EPM	Password for postgres database account	Automatically generated
Primary EPM Auxiliary EPM	Create database account that can read report data	No
Primary EPM Auxiliary EPM	Create database account that can write report data	No
Primary EPM	Support auxiliary EPM servers	No
Primary EPM Auxiliary EPM MPP	Security Certificate	Automatically generated

Customer configuration data worksheet

The following table identifies the key configuration information that you must enter throughout the Experience Portal deployment and configuration process.

Required data	Value for the system	Note
Fully qualified domain name (FQDN) of the virtual machine	Value: ————————	
IP address of the virtual machine	Value: ————————	
Netmask of the virtual machine	Value: ————————	
IP address of the network gateway	Value: ————————	
IP address of the DNS server that is assigned to the virtual machine	Value: ————————	The semicolon-separated list of DNS servers for the virtual machine. This information is optional.
Default search list	Value: ————————	The semicolon separated list of Search Domains. This information is optional.
Product ID	Value: ————————	The 10-digit, alphanumeric Product ID. You are prompted for this information only during the primary EPM OVA deployment.
IP address of the primary EPM	Value: ————————	You are prompted for this information only during only during the auxiliary EPM OVA and MPP OVA deployment.

Note:

Complete this worksheet for each virtual machine that you plan to deploy.

Chapter 4: Deploying Experience Portal

Overview

The Experience Portal virtualized environment offer consists of the following three OVA files:

- Primary EPM
- Auxiliary EPM
- MPP

You must also deploy the Avaya WebLM OVA packaged for VMware if you do not have a WebLM server that is not being used to license an Experience Portal system. For more information about Avaya WebLM OVA, see *Avaya WebLM using VMware® in the Virtualized Environment Deployment Guide* on the Avaya Support website at https://www.support.avaya.com.

The Experience Portal OVA files support the following two methods of deployment:

- vCenter deployment through a vSphere client
- Direct deployment to the ESXi server through a vSphere client

You can select one of the two methods of deployment based on your VMware environment.

You must deploy the OVA files in the following order:

1. Avaya WebLM OVA if you do not already have a WebLM server
2. Primary EPM OVA
3. Auxiliary EPM OVA and MPP OVA in any order after you deploy and configure the Primary EPM OVA

Deploying the Experience Portal OVAs with vCenter

Deploying the Primary EPM OVA with vCenter

About this task

If vSphere Client is connected to vCenter, use this procedure to deploy the Primary EPM OVA.

Note:

The following steps are guidelines to deploying the OVA. The deployment screens might differ based on your VMware configuration.

Procedure

1. Connect to the vCenter server through the vSphere client.
2. In the vSphere Client window, select **File** > **Deploy OVF Template**.
3. In the Deploy OVF Template window, perform one of the following to select the Primary EPM OVA file, and click **Next**:
   - If you have downloaded the OVA file to a location accessible from your computer, click **Browse** to select the location.
   - If the OVA file is located on an HTTP server, enter the full URL in the **Deploy from a file or URL** field.

   Important:

   Ensure that you use a high speed network, 1-Gbps or more, to connect to the source location of the OVA file. A slow network connection might increase the deployment time or cause the deployment to time-out.
4. Verify the details of the primary EPM OVA template.
5. Verify and accept the license agreement.
6. Enter a unique name for the new virtual machine.
7. Select the inventory location for the virtual machine.
8. Select the host or cluster on which you want to deploy the virtual machine if you did not make a selection at the start of the deployment process.
9. Select the resource pool if the host or cluster has resource pools.
10. Select the datastore location to store the virtual machine files.

    The datastore can be local to the host or a mounted shared storage, such as Network Filesystem Storage (NFS) or Storage Area Network (SAN). The virtual

machine configuration file and virtual disk files are stored in the datastore. Select a datastore that can store the virtual machine and the virtual disk files.

11. Select the required disk format to store the virtual machine and the virtual disk.

    Note:

    Deploy thick disks which are lazy-zeroed. For more information about thin vs thick deployments and best practices for VMware features, see *Avaya Customer Experience Virtualized Environment Solution Description*.

12. If the deployment wizard displays the **Network Mapping** window, verify the Destination VM Networks setting, and update the details if required.

    Note:

    Based on your VMware configuration, the wizard might prompt you to verify and change the Network Mapping details.

13. Configure the network settings by entering values for the following fields:

    - Fully qualified domain name of this virtual machine
    - IP address of this virtual machine
    - Netmask of this virtual machine
    - IP address of the network gateway
    - (Optional) IP addresses of the DNS servers (separate addresses with ';')
    - (Optional) List of Search Domains (separate domains with ';')
    - Product ID of the Experience Portal system

    Note:

    If you enter incorrect network settings during the deployment procedure, you will be prompted to configure the network settings again after you restart the virtual machine and log in to the console as the sroot user.

14. **(Optional)** To automatically start the virtual machine after the deployment procedure is complete, select the **Power on after deployment** check box in the Ready to Complete window.

    If you do not select this check box, you can manually start the virtual machine after the deployment procedure is complete.

15. Verify the deployment properties and complete the deployment procedure.

Next steps

1. If you did not select the option to start the virtual machine automatically, start the virtual machine.
2. Log in to the virtual machine console as the sroot user and check for errors.

3. During the deployment procedure, Experience Portal generates a default security certificate. You can import a security certificate instead of using the default security certificate.
4. Deploy MPP servers.
5. If you plan to deploy auxiliary EPM servers, configure the primary EPM server to support one or more auxiliary EPM servers.
6. (Optional) Deploy auxiliary EPM servers.

Related topics:

[Importing a security certificate](#) on page 41

[Configuring the primary EPM server to support one or more auxiliary EPM servers](#) on page 42

Deploying the Auxiliary EPM OVA with vCenter

Before you begin

Deploy and configure the Primary EPM OVA.

Configure the primary EPM server to support one or more auxiliary EPM servers.

About this task

If vSphere Client is connected to vCenter, use this procedure to deploy the Auxiliary EPM OVA.

Note:

The following steps are guidelines to deploying the OVA. The deployment screens might differ based on your VMware configuration.

Procedure

1. Connect to the vCenter server through the vSphere client.
2. In the vSphere Client window, select **File** > **Deploy OVF Template**.
3. In the Deploy OVF Template window, perform one of the following to select the Auxiliary EPM OVA file, and click **Next**:
   - If you have downloaded the OVA file to a location accessible from your computer, click **Browse** to select the location.
   - If the OVA file is located on an HTTP server, enter the full URL in the **Deploy from a file or URL** field.

Important:

Ensure that you use a high speed network, 1-Gbps or more, to connect to the source location of the OVA file. A slow network connection might increase the deployment time or cause the deployment to time-out.

4. Verify the details of the auxiliary EPM OVA template.
5. Verify and accept the license agreement.
6. Enter a unique name for the new virtual machine.
7. Select the inventory location for the virtual machine.
8. Select the host or cluster on which you want to deploy the virtual machine if you did not make a selection at the start of the deployment process.
9. Select the resource pool if the host or cluster has resource pools.
10. Select the datastore location to store the virtual machine files.

    The datastore can be local to the host or a mounted shared storage, such as Network Filesystem Storage (NFS) or Storage Area Network (SAN). The virtual machine configuration file and virtual disk files are stored in the datastore. Select a datastore that can store the virtual machine and the virtual disk files.
11. Select the required disk format to store the virtual machine and the virtual disks.

    Note:

    Deploy thick disks which are lazy-zeroed. For more information about thin vs thick deployments and best practices for VMware features, see *Avaya Customer Experience Virtualized Environment Solution Description*.
12. If the deployment wizard displays the **Network Mapping** window, verify the Destination VM Networks setting, and update the details if required.

    Note:

    Based on your VMware configuration, the wizard might prompt you to verify and change the Network Mapping details.
13. Configure the network settings by entering values for the following fields:
    - Fully qualified domain name of this virtual machine
    - IP address of this virtual machine
    - Netmask of this virtual machine
    - IP address of the network gateway
    - (Optional) IP addresses of the DNS servers (separate addresses with ‘;’)
    - (Optional) List of Search Domains (separate domains with ‘;’)
    - Hostname (FQDN) or IP address of the Primary EPM server

Note:

If you enter incorrect network settings during the deployment procedure, you will be prompted to configure the network settings again after you restart the virtual machine and log in as the sroot user.

14. **(Optional)** To automatically start the virtual machine after the deployment procedure is complete, select the **Power on after deployment** check box in the Ready to Complete window.

    If you do not select this check box, you can manually start the virtual machine after the deployment procedure is complete.

15. Verify the deployment properties and complete the deployment procedure.

Next steps

1. If you did not select the option to start the virtual machine automatically, start the virtual machine.
2. Log in to the Virtual Machine console as the sroot user and check for errors.
3. Configure the password for the database user vpcommon on the virtual machine.
4. During the deployment procedure, Experience Portal generates a default security certificate. You can import a security certificate instead of using the default security certificate.
5. Deploy MPP servers.

Related topics:

Importing a security certificate on page 41
Configuring the primary EPM server to support one or more auxiliary EPM servers on page 42
Configuring a password for database user vpcommon on an auxiliary EPM server on page 43

Deploying the MPP OVA with vCenter

Before you begin

Deploy and configure the Primary EPM OVA.

About this task

If vSphere Client is connected to vCenter, use this procedure to deploy the MPP OVA.

Note:

The following steps are guidelines to deploying the OVA. The deployment screens might differ based on your VMware configuration.

Procedure

1. Connect to the vCenter server through the vSphere client.
2. In the vSphere Client window, select **File** > **Deploy OVF Template**.
3. In the Deploy OVF Template window, perform one of the following to select the MPP OVA file, and click **Next**:
   - If you have downloaded the OVA file to a location accessible from your computer, click **Browse** to select the location.
   - If the OVA file is located on an HTTP server, enter the full URL in the **Deploy from a file or URL** field.

   Important:

   Ensure that you use a high speed network, 1-Gbps or more, to connect to the source location of the OVA file. A slow network connection might increase the deployment time or cause the deployment to time-out.
4. Verify the details of the MPP OVA template.
5. Verify and accept the license agreement.
6. Enter a unique name for the new virtual machine.
7. Select the inventory location for the virtual machine.
8. Select the host or cluster if you have not selected a host at the start of the deployment process.
9. Select the resource pool if the host or cluster has resource pools.
10. Select the datastore location to store the virtual machine files.

    The datastore can be local to the host or a mounted shared storage, such as Network Filesystem Storage (NFS) or Storage Area Network (SAN). The virtual machine configuration file and virtual disk files are stored in the datastore. Select a datastore that can store the virtual machine and the virtual disk files.
11. Select the required disk format to store the virtual machine and the virtual disks.

    Note:

    Deploy thick disks which are lazy-zeroed. For more information about thin vs thick deployments and best practices for VMware features, see *Avaya Customer Experience Virtualized Environment Solution Description*.
12. If the deployment wizard displays the **Network Mapping** window, verify the Destination VM Networks setting, and update the details if required.

    Note:

    Based on your VMware configuration, the wizard might prompt you to verify and change the Network Mapping details.

13. Configure the network settings by entering values for the following fields:
    - Fully qualified domain name of this virtual machine
    - IP address of this virtual machine
    - Netmask of this virtual machine
    - IP address of the network gateway
    - (Optional) IP addresses of the DNS servers (separate addresses with ';')
    - (Optional) List of Search Domains (separate domains with ';')
    - Hostname (FQDN) or IP address of the Primary EPM server

    Note:

    If you enter incorrect network settings during the deployment procedure, you will be prompted to configure the network settings again after you restart the virtual machine and log in as the sroot user.
14. **(Optional)** To automatically start the virtual machine after the deployment procedure is complete, select the **Power on after deployment** check box in the Ready to Complete window.

    If you do not select this check box, you can manually start the virtual machine after the deployment procedure is complete.
15. Verify the deployment properties and complete the deployment procedure.

Next steps

1. If you did not select the option to start the virtual machine automatically, start the virtual machine.
2. Log in to the Virtual Machine console as the sroot user and check for errors.
3. Configure the MPP server.
4. During the deployment procedure, Experience Portal generates a default security certificate. You can import a security certificate instead of using the default security certificate.

Related topics:

Importing a security certificate on page 41

Deploying the Experience Portal OVAs directly on the ESXi server with vSphere Client

About this task

Use this procedure to deploy all three Experience Portal OVA files directly on the ESXi server with vSphere Client.

You must deploy and configure the Primary EPM OVA before you deploy the Auxiliary EPM OVA or the MPP OVA.

Note:

The deployment screens might differ based on your VMware configuration.

Procedure

1. Connect to the ESXi host server through the vSphere client.
2. Select **File** > **Deploy OVF Template**.
3. On the Deploy OVF Template window, perform one of the following to select the OVA file:
   - If you have downloaded the OVA file to a location accessible from your computer, click **Browse** to select the location.
   - If the OVA file is located on an http server, enter the full URL in the **Deploy from a file or URL** field.

   Important:

   Ensure that you use a high speed network, 1-Gbps or more, to connect to the source location of the OVA file. A slow network connection might increase the deployment time or cause the deployment to time-out.
4. Verify the details about the Experience Portal OVA template.
5. Verify and accept the license agreement.
6. Enter a unique name for the new virtual machine.
7. Select the resource pool if the host has resource pools.
8. Select the data store location to store the virtual machine files.

   The datastore can be local to the host or a mounted shared storage, such as Network Filesystem Storage (NFS) or Storage Area Network (SAN). The virtual machine configuration file and virtual disk files are stored in the datastore. Select a datastore that can store the virtual machine and all of the virtual disk files.
9. Select the required disk format to store the virtual machine and the virtual disks.

Note:

Deploy thick disks which are lazy-zeroed. For more information about thin vs thick deployments and best practices for VMware features, see *Avaya Customer Experience Virtualized Environment Solution Description*.

10. If the deployment wizard displays the **Network Mapping** window, verify the Destination VM Networks setting, and update the details if required.

    Note:

    Based on your VMware configuration, the wizard might prompt you to verify and change the Network Mapping details.

11. **(Optional)** Select the **Power on after deployment** check box in the Ready to Complete window, to automatically start the virtual machine after the deployment.

    If you do not select this check box, you can manually start the virtual machine after the deployment procedure is complete.

12. Verify the deployment properties and complete the deployment procedure.

Next steps

1. If you did not select the option to start the virtual machine automatically, start the virtual machine.
2. Log in to the Experience Portal virtual machine console as the sroot user. At the prompt, configure the network parameters and the Experience Portal parameters.

Related topics:

Configuring the Primary EPM and the network parameters on page 28
Configuring the Auxiliary EPM and the network parameters on page 30
Configuring MPP and the network parameters on page 31

Configuring the Primary EPM and the network parameters

About this task

After you deploy the Primary EPM virtual machine directly on an ESXi host, you must configure the Primary EPM.

Note:

Ensure that you start the virtual machine after the deployment procedure is complete.

Procedure

1. Use vSphere Client to gain access to the console of the primary EPM virtual machine.

2. Log in to the local Linux console as sroot.
   The console displays the message **Networking has not been configured. Would you like to configure it now? (Y/n)**.
3. Type `Y`, and press `Enter`.
4. Type the Fully Qualified Domain Name (FQDN) of the virtual machine, and press `Enter`.
5. Type the IP address of the virtual machine, and press `Enter`.
6. Type the netmask of the virtual machine, and press `Enter`.
7. Type the gateway address of the virtual machine, and press `Enter`.
8. Type the semicolon separated addresses of the Domain Name Servers (DNS), and press `Enter`.

   To delete previous entries and have a blank entry, enter a period.
9. Type the semicolon separated list of search domains, and press `Enter`.

   Press `Enter` without adding any input if you plan to use the default search domain.

   To delete previous entries and have a blank entry, enter a period.
10. Confirm the network settings, type `1`, and press `Enter` to apply the network settings.
    The console displays the progress information as the network configuration completes, and displays the message **Experience Portal has not been configured. Would you like to configure it now? (Y/n)**.
11. Type `Y`, and press `Enter`.
12. Enter the Product ID of the Experience Portal system.
13. Confirm the Product ID, type `1`, and press `Enter` to apply the configuration values.
    The configuration process starts.

    The console displays the configuration successful message when the configuration process is complete.

Next steps

1. During the deployment procedure, Experience Portal generates a default security certificate. You can import a security certificate instead of using the default security certificate.
2. If you plan to deploy Auxiliary EPM servers, configure the primary EPM server to support one or more auxiliary EPM servers.

Related topics:

[Importing a security certificate](#) on page 41

Configuring the primary EPM server to support one or more auxiliary EPM servers on page 42

Configuring the Auxiliary EPM and the network parameters

About this task

After you deploy the Auxiliary EPM virtual machine directly on an ESXi host, you must configure the Auxiliary EPM.

Note:

Ensure that you start the virtual machine after the deployment procedure is complete.

Procedure

1. Use vSphere Client to gain access to the console of the Auxiliary EPM virtual machine.
2. Log in to the Linux console as sroot.
   The console displays the message **Networking has not been configured. Would you like to configure it now? (Y/n)**.
3. Type `Y`, and press `Enter`.
4. Type the Fully Qualified Domain Name (FQDN) of the virtual machine, and press `Enter`.
5. Type the IP address of the virtual machine, and press `Enter`.
6. Type the netmask of the virtual machine, and press `Enter`.
7. Type the gateway address of the virtual machine, and press `Enter`.
8. Type the semicolon separated addresses of the Domain Name Servers (DNS), and press `Enter`.

   To delete previous entries and have a blank entry, enter a period.
9. Type the semicolon separated list of search domains and press `Enter`.

   Press `Enter` without adding any input if you plan to use the default search domain.

   To delete previous entries and have a blank entry, enter a period.
10. Confirm the network settings, type `1`, and press `Enter` to apply the network settings.
    The console displays the progress information as the network configuration completes, and displays the message **Experience Portal has not been configured. Would you like to configure it now? (Y/n)**.
11. Type `Y`, and press `Enter`.
12. Enter the host name or IP address of the Primary EPM server, and press `Enter`.

13. Type `1`, and press `Enter` to apply the configuration values.
    The configuration process starts.

    The console displays the configuration successful message when the configuration process is complete.

Next steps

1. Configure the password for the database user vpcommon on the virtual machine.
2. During the deployment procedure, Experience Portal generates a default security certificate. You can import a security certificate instead of using the default security certificate.

Related topics:

Importing a security certificate on page 41
Configuring the primary EPM server to support one or more auxiliary EPM servers on page 42
Configuring a password for database user vpcommon on an auxiliary EPM server on page 43

Configuring MPP and the network parameters

About this task

After you deploy the MPP virtual machine directly on an ESXi host, you must configure the MPP.

Note:

Ensure that you start the virtual machine after the deployment procedure is complete.

Procedure

1. Use vSphere Client to gain access to the console of the MPP virtual machine.
2. Log in to the Linux console as sroot.
   The console displays the message **Networking has not been configured. Would you like to configure it now? (Y/n)**.
3. Type `Y`, and press `Enter`.
4. Type the Fully Qualified Domain Name (FQDN) of the virtual machine, and press `Enter`.
5. Type the IP address of the virtual machine, and press `Enter`.
6. Type the netmask of the virtual machine, and press `Enter`.
7. Type the gateway address of the virtual machine, and press `Enter`.

8. Type the semicolon separated addresses of the Domain Name Servers (DNS), and press `Enter`.

   To delete previous entries and have a blank entry, enter a period.

9. Type the semicolon separated list of search domains, and press `Enter`.

   Press `Enter` without adding any input if you plan to use the default search domain.

   To delete previous entries and have a blank entry, enter a period.

10. Confirm the network settings, type `1`, and press `Enter` to apply the network settings.
    The console displays the progress information as the network configuration completes, and displays the message **Experience Portal has not been configured. Would you like to configure it now? (Y/n)**.

11. Type `Y`, and press `Enter`.

12. Enter the host name or IP address of the primary EPM server, and press `Enter`.

13. Type `1`, and press `Enter` to apply the configuration values.

    The configuration process starts.

    The console displays the configuration successful message when the configuration process is complete.

Related topics:

[Importing a security certificate](#) on page 41

Chapter 5: Configuration

Configuring the virtual machine automatic startup settings

About this task

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

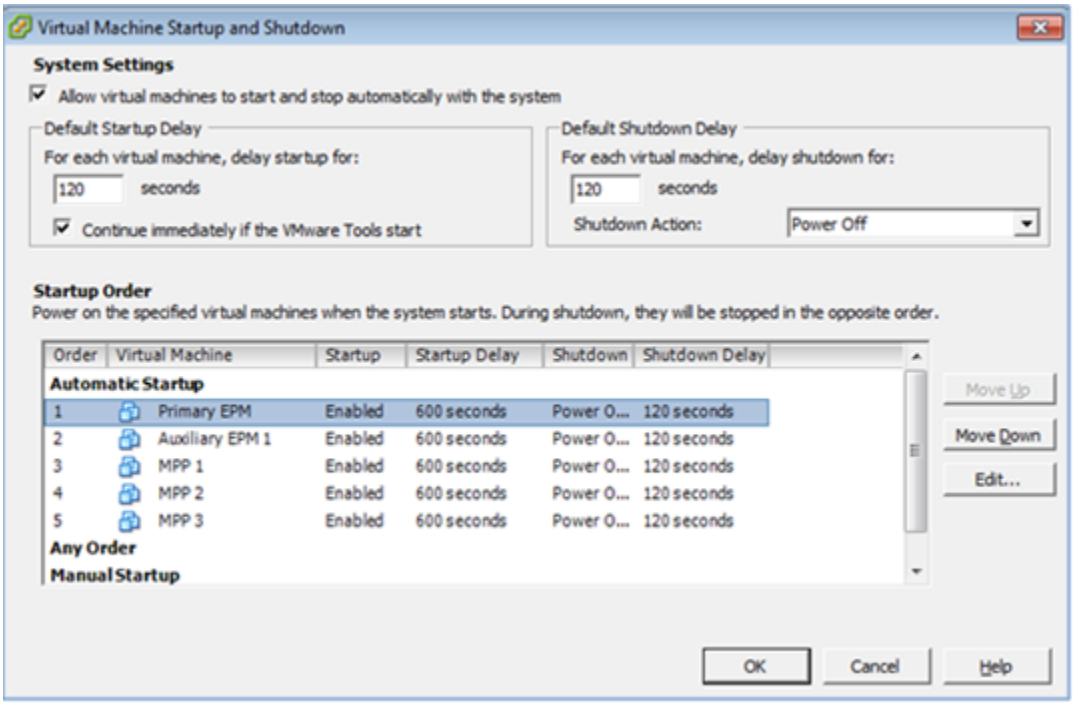
In high availability (HA) clusters, the VMware HA software ignores the startup selections.

Procedure

1. In the vSphere Client inventory, select the host where the virtual machine is located.
2. Click the **Configuration** tab.
3. In the **Software** section, click **Virtual Machine Startup/Shutdown**.
4. Click **Properties** in the upper right corner of the screen.
5. In the **System Settings** section, select **Allow virtual machines to start and stop automatically with the system**.
6. In the **Manual Startup** section, select the virtual machine.
7. Use the **Move up** button to move the virtual machine under **Automatic Startup**.
8. Click **OK**.

Example

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



Configuring and initializing the Experience Portal system

Experience Portal basic system configuration overview

After you deploy the Experience Portal OVA files, you can configure and test an Experience Portal system.

Important:

Complete the following steps in the specified order or you might encounter errors during the configuration procedures.

Step	Description	✔
1	If the Avaya Services team will access the system, set up the Avaya Services access requirements as described in Configuring the Avaya Service accounts on page 36.	
2	Log in to the EPM Web interface as described in Logging in to the Experience Portal web interface on page 38.	

Step	Description	✔
	If you are an Avaya Services representative, log in as described in Logging in to the EPM Web interface using the Avaya Services init account on page 38.	
3	Install the Experience Portal license file as described in Installing a license file on page 39. **Note:** Experience Portal provides 10 telephony ports in the 30-day grace period after deployment. After the grace period expires, and if you have not installed a valid license file, the Experience Portal system stops processing calls.	
4	During the deployment process, Experience Portal generates a default security certificate. All servers in the Experience Portal set up use this security certificate to identify the Experience Portal server. If you want to import a certificate instead of using the default security certificate, follow the procedures described in Importing a security certificate on page 41.	
5	Add H.323 connections or add at least one SIP connection. For more information, see *Administering Avaya Aura® Experience Portal*.	
6	Add the MPP servers. **Note:** Ensure that you select the **Restart Automatically** option on the Add MPP server page in EPM so that the MPP is available to take calls in the following conditions: • The virtual machine starts automatically when the host is restarted. • The VMware High Availability feature is in use and the host starts up on a different ESxi host. For more information, see *Administering Avaya Aura® Experience Portal*.	
7	(Optional) Add one or more Automatic Speech Recognition (ASR) servers. For more information, see *Administering Avaya Aura® Experience Portal*.	
8	Add one or more Text-to-Speech (TTS) servers. For more information, see *Administering Avaya Aura® Experience Portal*.	

Step	Description	✔
9	If you deploy one or more auxiliary EPM servers, you must perform the following: • Configure the primary EPM virtual machine as described in Configuring primary EPM server to support one or more auxiliary EPM servers on page 42. • Configure the auxiliary EPM as described in Configuring password for database user vpcommon on an auxiliary EPM on page 43.	
10	If you have deployed auxiliary EPM servers, add the auxiliary EPM servers. For more information, see *Administering Avaya Aura® Experience Portal*.	
11	Connect the EPM server to an external time source so that all servers in the Experience Portal system are synchronized. For more information on external time sources, see *Implementing Avaya Aura® Experience Portal on multiple servers*.	
12	EPM accepts inputs in non-English languages. For more information on how to configure non-English languages, see *Implementing Avaya Aura® Experience Portal on multiple servers*.	
13	To enable multi-tenancy in Experience Portal, run the `EnableOrganizations` command. For more information, see *Administering Avaya Aura® Experience Portal*.	
14	Start all MPP servers. For more information, see *Administering Avaya Aura® Experience Portal*.	
15	If the system/virtual machine BIOS has the Universal Time Coordinated (UTC) set as True, you must configure the UTC while setting the time zone on Avaya Linux. For more information, see Changing the timezone and date on Avaya Redhat Linux on page 44.	

Configuring the Avaya Service accounts

Before you begin

Ensure that you have the Avaya Service Account authentication file that is generated by the Authentication File System (AFS) tool.

Important:

After you configure the Avaya Service account, customers who use Avaya Enterprise Linux cannot log in to Experience Portal server with the sroot account and must use the root

account. Before you configure the account, log in to the Experience Portal server with the root account to ensure that the password is set correctly.

Note:

When you run the AFS tool, select **New System – Product: Avaya Aura Experience Portal Release: 6.x** to generate the AFS file.

Procedure

1. Log in to Linux on the Experience Portal server as sroot.
2. Copy the Avaya Service Account authentication file to the `/tmp` directory on the server.
3. Navigate to the `Support/VP-Tools` directory by entering the **`cd /opt/$AVAYA_HOME/Support/VP-Tools`** command.
4. Run the `bash AddServiceAccounts /<authentication_file_path>/authentication_file_name` command.

   authentication_file_path is the fully-qualified path to the authentication file that you have copied to the server and *authentication_file_name* is the name of the authentication file that you copy to the server.
5. Press `Enter` to continue the procedure.
   The following warning message is displayed:

```
Primary EPM found; creating EPM admin user init
Creating EPM service account
Checking System [EP,EP,]
  Added SDResource name=init type=USER desc=
    Added SDPropertyContainer name=Default category=Default desc=
      Added SDProperty name=roles
      Added SDProperty name=createTime
Return value for adding EPM admin user init: 0
Loading file /tmp/AF-7000112969-080808-155712.xml
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.

Utility has completed.  Please review the information above for possible
errors
```

Note:

This is an informational message and needs no corrective action.

The AddServiceAccounts script changes the following Linux accounts so that you can log in to the EPM servers only by using the Avaya Services authentication procedure:

User name	Group	Purpose
sroot	root	Avaya Services root access
craft	susers	Avaya Services non-root access

In addition, the script creates the EPM user account init. The init account has Administration, Auditor, and User Manager user roles.

Next steps

Repeat this procedure for each Experience Portal server on which you want to configure the Avaya Service accounts.

Logging in to the EPM Web interface using the Avaya Services init account

Procedure

1. Open an Internet Explorer (IE) browser and enter the URL of your Experience Portal system.

   The URL is: `http://EPM-server/VoicePortal`.

   EPM-server is the hostname or the IP address of the system where the primary EPM software is installed.

   Note:

   Enable TLS security in your IE browser.

2. In the **User Name** field, enter `init`.
3. Click **Submit**.
4. Use the challenge information to generate the appropriate response password for the init account, and enter the password in the **Password** field.
5. Click **Logon**.
   The system logs you in to EPM.

Logging in to the Experience Portal Web interface

The Experience Portal Manager (EPM) Web interface is the main interface to the Experience Portal system.

Procedure

1. Open an Internet Explorer browser and enter the URL for your Experience Portal system.

   The URL is: `http://EPM-server/VoicePortal`.

EPM-server is the hostname or IP address of the system where the primary EPM software is installed.

Note:

You must enable TLS security in your IE browser.

2. In the **User Name** field, enter `epadmin`, which is the default user name for the Administration account that is created automatically during the installation procedure.
3. Click **Submit**.
4. In the **Password** field, enter `epadmin01`, which is the default password that is created automatically during the installation procedure.
5. Click **Logon**.
   The system prompts you to enter the current password and change the default password.
6. Enter the current password.
7. Enter a new password for the epadmin account.
8. In the **Confirm Password** field, enter the new password for the epadmin account.
9. Click **Logon**.
   The system logs you in to EPM.

Installing the license file

You require a license file for the Experience Portal operation. The license file defines the telephony ports and the ASR and TTS connections that you are authorized to use. Avaya sends the Experience Portal license file separately in an email message.

Before you begin

Note:

If you do not receive a license file from Avaya, contact your Avaya representative or Avaya Partner representative.

Ensure you have installed the Avaya WebLM license server OVA, or you have an existing, external WebLM license server.

Procedure

1. Open the email message that contains the Experience Portal license file.

2. Detach the license file from the email message, and store the license file on a computer that can access the Experience Portal servers from a network connection.

   You can install the license file on any server from which you can gain access to the EPM Web interface.

3. Log in to the EPM Web interface using an account with the Administration user role.

4. From the EPM main menu, select **Security** > **Licensing**.
   The Licensing page displays the license information and the location of the License server.

5. Type the location of the license server in the **Location** field.

   The URL must be in the format `https://`*`WebLM-machine`*`:`*`port_num`*`/WebLM/LicenseServer`, where:

   - *`Weblm-machine`* is the hostname or IP address of the WebLM server.
   - `:`*`port_num`* is an optional parameter that consists of a colon followed by the port number for the WebLM server. If WebLM uses the default configuration, specify `52233`.

6. Click **Verify**.
   The browser opens a separate window and displays the Avaya WebLM page, which contains a **License Administration** link.

7. Click **License Administration**.
   The system displays the Web License Manager Logon page.

8. If you have done a fresh installation of the WebLM server, do the following:

   a. Enter the default user name `admin`.
   b. Enter the default password `weblmadmin`.
   c. Press `Enter` or click the arrow button to log in.
   d. Enter the details on the Change Password page. Ensure that you type `weblmadmin` in the **Current Password** field.
   e. Click **Submit**.
   f. On the Logon page, log in with your new password.

9. If you have an existing WebLM server, you have to do the following:

   a. Type the user name.
   b. Type the password.
   c. Click **Continue**.

10. On the Install License page, click **Browse** to locate the Experience Portal license file.

11. Select the license file, and click **Install**.
    WebLM uploads the license file from your computer to the WebLM server and displays the message `License file installed successfully.`

12. Log out of the Web License Manager, and close the Web License Manager page.
13. On the EPM Licensing page, click **Apply**.
14. Click **OK** to confirm the change.
15. Verify that the new licensing information is correct.

Importing a security certificate

About this task

Experience Portal uses the SSL protocol to establish a secure connection between servers. This secure connection requires a security certificate. During the deployment process, Experience Portal generates a self-signed certificate.

To use a certificate from a company such as VeriSign, you can import the certificate. The certificate must be in PKCS12 format.

Procedure

1. Log in to Linux on the Primary Experience Portal server.

   Log in to Linux locally as sroot, or log in remotely as a non-root user and enter the **`su - sroot`** command to change to root user.
2. Stop the vpms service by entering the **`/sbin/service vpms stop`** command.
3. Stop the httpd service by entering the **`/sbin/service httpd stop`** command.
4. Navigate to the `bin` directory by entering the **`cd /opt/Avaya/VE/bin`** command.
5. Enter the **`bash ImportCertificate.sh`** command.
6. When prompted, type the file path and name of the security certificate, and press `Enter`.
7. When prompted, type the password for the security certificate, and press `Enter`. The security certificate is imported to the Experience Portal system.
8. Start the httpd service by entering the **`/sbin/service httpd start`** command.
9. Start the vpms service by entering the **`/sbin/service vpms start`** command.
10. Accept the new certificate on all auxiliary EPMs and MPPs as described in the following steps:
    a. On each auxiliary EPM and MPP log in to the console as sroot user.
    b. Navigate to `$AVAYA_HOME/Support/VP-Tools`.

c. Run the **./setup_vpms.php <Primary EPM>** command where Primary EPM is the IP address or hostname of the primary EPM.
d. Type `Y`, and press `Enter` to accept the new certificate.

Note:

For NTP service, type `Y`, and press `Enter` to use EPM for NTP service.

Related topics:

Configuring the primary EPM server to support one or more auxiliary EPM servers on page 42

Configuring the primary EPM server to support one or more auxiliary EPM servers

About this task

You must configure the vpcommon PostgreSQL database user account on the Primary EPM server before you can add the Auxiliary server to the EPM.

Procedure

1. Log in to Linux on the primary EPM server.

   If you are an Avaya Services representative, and use theAvaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Navigate to the `Support/VP-Tools/SetDbPassword` directory by running the **cd /opt/Avaya/ExperiencePortal/Support/VP-Tools/SetDbPassword** command.
3. Enter `./SetDbPassword.sh add_vpcommon -p` *password*, where *password* is the new password you want to use for the vpcommon user account.

Next steps

1. Configure the outcall user account and password in the EPM Settings page.

Note:

From the EPM main menu, select **System Configuration** > **EPM Servers** > **EPM Settings**, and configure the outcall user account.

2. Configure the vpcommon PostgreSQL database user account on the auxiliary EPM server.
3. Add the auxiliary EPM server to Experience Portal Manager.

Configuring a password for database user vpcommon on an auxiliary EPM server

About this task

Before you add an auxiliary EPM to the primary EPM, you must configure the vpcommon PostgreSQL database user account on the auxiliary EPM server.

Procedure

1. Log in to Linux on the auxiliary EPM server.
2. Navigate to the `Support/VP-Tools/SetDbPassword` directory by entering the `cd /opt/Avaya/ExperiencePortal/Support/VP-Tools/SetDbPassword` command.
3. Enter the `./SetDbPassword.sh update –u vpcommon -p` *password* command to update the vpcommon user account.

   password is the password that you have assigned to the vpcommon user account on the primary EPM server.
4. Enter the `service vpms restart` command to restart the vpms service.

Next steps

Add the auxiliary EPM server to Experience Portal Manager.

Related topics:

Importing a security certificate on page 41
Configuring the primary EPM server to support one or more auxiliary EPM servers on page 42

Changing the timezone and date on Avaya Linux

Before you begin

Navigate to the `/usr/share/zoneinfo/` directory on Avaya Linux and find the correct timezone that you want to configure. The directory contains the names and timezones for different regions of the world.

About this task

If the system/virtual machine BIOS has the Universal Time Coordinated (UTC) set as **true**, you must configure the UTC while setting the time zone on Avaya Linux.

The UTC in the Linux configuration file must match the BIOS settings.

Procedure

1. Log in to Avaya Linux.
2. Create a backup copy of the `/etc/sysconfig/clock` file.

   For example run the **`cp -p /etc/sysconfig/clock /etc/sysconfig/clockORIG`** command to create a backup copy called clockORIG.
3. Open the `/etc/sysconfig/clock` file and edit the zone. If applicable, set the UTC value to **true** or **false** to match the BIOS settings.
4. Save the changes.
5. Link the appropriate zoneinfo file to the `/etc/localtime` file.

   For example, if you set the time zone to America/Los_Angeles, you must link the timezone to the `/etc/localtime` file by running the **`# ln -sf /usr/share/zoneinfo/America/Los_Angeles /etc/localtime`** command.
6. If the system is an EPM, restart the vpms service by running the **`/sbin/service vpms restart`** command.

Chapter 6: Post-deployment verification and testing

Adding the Experience Portal test application

Before you begin

If you want to test Automatic Speech Recognition (ASR) resources, ensure that you add one or more ASR servers to the Experience Portal system.

If you want to test Text-to-Speech (TTS) resources, ensure that you add one or more TTS servers to the Experience Portal system.

About this task

You can use the sample application that is installed with Experience Portal to test how the system handles telephony resource requests.

- If you run the sample application as a VoiceXML application, Experience Portal uses the default CCXML page installed on the MPP server to provide basic CCXML controls. The VoiceXML application tests:
  - ASR resources
  - TTS resources
  - Bridge transfers
  - Blind transfers
  - Supervised transfers
  - Several audio prompt formats
  - Audio prompt recording and playback
- If you run the sample application as a CCXML application, Experience Portal uses a more advanced CCXML page that provides all the functionality of the VoiceXML application and you can test the following CCXML features:
  - Call conferencing
  - Call classification
  - Call merge for calls using a SIP connection

Procedure

1. From the EPM main menu, select **System Configuration** > **Applications**.
2. On the Applications page, click **Add**.
   EPM displays the Add Application page.
3. In the **Name** field, type the name you want to use to identify the application on the system. After you save the application, this name cannot be changed.
   For example, type `Test_App`.
4. Enter the required parameters for the application.
   The following table provides information on the parameters that you must enter for each application type.

Application type	Required parameters
VoiceXML application	In the **MIME Type** field, select **VoiceXML**. In the **VoiceXML URL** field, type `http://` *`MPP_Identifier`*`/mpp/misc/avptestapp/intro.vxml`, where *`MPP_Identifier`* is the hostname or IP address of any one of the MPP servers in the Experience Portal system.
CCXML application	In the **MIME Type** field, select **CCXML**. In the **CCXML URL** field, type `http://` *`MPP_Identifier`*`/mpp/misc/avptestapp/root.ccxml`, where *`MPP_Identifier`* is the hostname or IP address of any one of the MPP servers in the Experience Portal system.

5. Click **Verify** to make sure that the system can locate the sample application page.
   If EPM can find the specified page, EPM displays the page in a separate browser window. If this check succeeds, continue with this procedure. Otherwise, correct the information in the **VoiceXML URL** or **CCXML URL** field and repeat this step until the system can locate the sample application page.

   Note:

   Instead of opening the file in a separate window, the browser might prompt you to save the file as a text file. You can choose to save the file and use text editor to open the file.

6. If you want to test ASR resources, complete the following steps:
   a. Select the type of ASR server you want to use from the **ASR** drop-down list.
   b. From the **Languages** list, select **English(US) en-us**.
7. If you want to test TTS, complete the following steps:
   a. Select the type of TTS server you want to use from the **TTS** drop-down list.

b. From the **Voices** list, select one or more of the **English(US)** voices.

8. To associate one or more incoming numbers with this application, enter the appropriate information in the **Application Launch** group.
9. If you want to test transcriptions, go to the **Transcription** section of the **Reporting Parameters** group and set the transcription parameters.

   Note:

   You can set the transcription parameters only if you have the Privacy Manager user role.

10. Click **Save**.
    EPM displays the Applications page with the test application listed in the table.

Running the sample application

Procedure

1. Call the test application number.
   The test application number is the number that you specify when you add the test application to the Experience Portal system.
2. When the system answers the call, press:
   - 1 for Automatic Speech Recognition (ASR)
   - 2 for Text-to-Speech (TTS)
   - 3 for Bridge Transfer
   - 4 for Blind Transfer
   - 5 for Consultative Transfer
   - 6 for Audio test
   - 7 to Exit
3. If you run the test application as a CCXML application, press:
   - 1 for Automatic Speech Recognition (ASR)
   - 2 for Text-to-Speech (TTS)
   - 3 for Bridge Transfer
   - 4 for Blind Transfer
   - 5 for Consultative Transfer

- 6 for Audio test
- 7 to test Conferencing
- 8 to test Merge
- 9 to test Call Classification
- 0 to Exit

Next steps

After you run the application, you can create reports to verify the application's performance and, if you have enabled transcriptions, view the transcription data.

Related topics:

Test Application result for Call Classification option on page 48
Test Application result for Call Conferencing option on page 49
Test Application result for Call Merge option on page 49

Test Application result for Call Classification option

When you run the test application as a CCXML application, and press 9 to test call classification, the application plays the following prompts based on the call status:

Call Status	Prompt
Line is busy	The busy tone is detected.
Invalid number is detected	Fail to create call.
Call is connected and human voice is heard	Detected live voice.
Call is connected and a recorded message is detected	Detected answering machine.
Call is connected and fax is detected	Detected fax.
Call is connected and sit tone is detected	The sit tone is detected.
Trunks are busy	The fast busy tone is detected.
Call classification detection does not	Timeout is detected.

Call Status	Prompt
detect anything within the specified timeout period	
Error occurs during call classification detection	Error occurs while detecting.
Call is not answered	No answer is detected.

Test Application result for Call Conferencing option

When you run the test application as a CCXML application, and press 7 to test call conferencing, the application plays the following prompts based on the call status:

Call Status	Prompt
Call to destination fails	Fail to create call.
Call is successful	Thank you. **Note:** When the call conference is successful, the application plays additional prompts. For H323, you need to enter 9 with the phone number. Otherwise, the call fails.

Test Application result for Call Merge option

When you run the test application as a CCXML application, and press 8 to test call merging, the application plays the following prompts based on the call status:

Call Status	Prompt
The application detects H.323 connection	This option is not supported in H.323. Please use SIP.
Merge is successful.	Thank you. **Note:** After playing the thank you prompt, the application merges the call.

Call Status	Prompt
	This option is not supported for H.323.

Configure and run the outcall test application

Use the outcall test application to validate the Application Interface web service and the Experience Portal outcall functionality. Avaya provides an installation script that automatically installs the outcall test application when Experience Portal is installed. There are two versions of outcall test applications. These versions are:

- Outcall test application version 1.4 that is available in `$AVAYA_HOME/Support/OutCallTest/AppIntfWS-Client`.
- Outcall test application version 2 that is available in`$AVAYA_HOME/Support/OutCallTest/VPAppIntfClient`.

Related topics:

Configuring Experience Portal for outcall on page 50
Running the outcall test application AppIntfWS-Client on page 51

Configuring Experience Portal for outcall

About this task

Important:

This configuration is required only if you use Experience Portal to perform outcalls or the Application Interface web service to launch CCXML applications.

Procedure

1. Ensure that at least one of the ports in the system is configured to allow outbound calls. For more information on configuring ports, see *Administering Avaya Aura® Experience Portal*.
2. For AppIntfWS-Client, ensure that you have configured a user name and password in the **System Configuration** > **EPM Servers** > **EPM Settings** page of EPM. This is the authentication information that the system uses to access the Application Interface web service.

Running the outcall test application AppIntfWS-Client

Before you begin

Ensure that you configure Experience Portal for the outcall application as described in Configuring Experience Portal for outcall on page 50.

Procedure

1. Log in to Linux locally as sroot, or log in remotely as a non-root user and change the user to root by entering the `su - sroot` command.
2. Navigate to the Outcall test application directory by entering the `cd $AVAYA_HOME/Support/OutcallTest/AppIntfWS-Client` command.
3. Enter the `./runclient.sh –n <outcall-username> –p <outcall password>` command to request the number of available outbound ports.
   - <outcall-username> is the user name that you assign to the outcall user in the **System Configuration > EPM Servers > EPM Settings** page.
   - <outcall password> is the password that you assign to the outcall user in the **System Configuration > EPM Servers > EPM Settings** page.
4. Verify that the outcall test application displays a response that shows the total ports and unused ports available for outcalls.
   For example:

   Fri Oct 17 15:21:02 PDT 2008: TestClient: queryResources succeeded, TotalRes = 25, UnusedH323 = 15, UnusedSIP = 10

   Fri Oct 17 15:21:02 PDT 2008: TestClient: exiting.
5. Enter the `./runclient.sh –R 1 –A <application-name> –T <number-to-dial> –n <outcall-username> –p <outcall password>` command to initiate an outcall and launch a VoiceXML application.
   - <application-name> is the name of the application that you specify on the application page.
   - <number-to-dial> is the phone number to place the outcall to.
   - <outcall-username> is the user name that you assign to the outcall user on the **System Configuration > Applications > Add Application** page.
   - <outcall password> is the password that you assign to the outcall user in the **System Configuration > EPM Servers > EPM Settings** page.
6. Verify that the dialed phone number rings.
7. Answer the phone and verify that the specified application handles the call.

Note:

The application handles the call in the same way as when an actual user calls into the system.

8. Verify that the outcall test application displays the following:
   - A response that shows the result of the LaunchVXML operation.
   - The total ports and the unused ports available for outcalls.

   For example:

   Fri Oct 17 15:24:58 PDT 2008: TestClient: launchVXML succeeded, SessionID = sys-mpp-2008291222458-2, TotalRes = 24, UnusedH323 = 12, UnusedSIP = 12

   Fri Oct 17 15:24:58 PDT 2008: TestClient: exiting.

Chapter 7: Troubleshooting

Troubleshooting logs for Experience Portal deployment

The following set of logs, applicable to both vCenter or direct ESXi deployment types, are available in the `/opt/Avaya/VE/logs` directory:

- `reconfigureNetwork.<YYYY-MM-DD>.log`: This log contains information on the network configuration and re-configuration activities. If network re-configuration/ configuration fails, use this log to understand and debug the root cause.
- `reconfigureSystem.<YYYY-MM-DD>.log`: This log records the various activities during the first boot up of the virtual machine post the OVA deployment. This log contains information about the networking state, condition and status of the custom services invoked (related to the OVA), and EP configuration state and status.
- `DeployExperiencePortal.<YYYY-MM-DD>.log`: This log records activities related to the Experience Portal deployment based on the DeployExperiencePortal program. The DeployExperiencePortal program determines if the deployed OVA is a primary EPM, auxiliary EPM, or MPP.
- `DeployPrimaryEPM.<YYYY-MM-DD>.log`, `DeployAuxiliaryEPM.<YYYY-MM-DD>.log`, or `DeployMPP.<YYYY-MM-DD>.log`: This log records activities related to the primary EPM, auxiliary EPM, and MPP deployment. If there are issues in the deployments, use this log to debug the issues.

VMware generated core images on Experience Portal virtual machine images

VMware provides technical assistance for debugging virtual machine issues such as VM kernel panic, virtual machine that hangs, and so on. When you log a service request, you must send the performance snapshots to troubleshoot the issue. You can execute the **`vm-support`** command to collect the virtual machine logs. The **`vm-support`** command also creates a .tar file for sending the logs to VMware. You can debug the core image by using the RedHat Crash Utility as described in Collecting performance snapshots using vm-support.

VMware also provides a utility to help you to take an initial look at virtual machine issues such as VM kernel panic, slow response time, virtual machine that hangs, and so on. The utility, called vmss2core, is a command line tool for creating virtual machine core file that you can use with the RedHat crash utility. For the **`vmss2core`** command, see VMware Knowledge Base, which includes the vmss2core technical link. The vmss2core tool generates a vmcore

core file, using the virtual machine's .vmsn file from a snapshot, or the .vmss file from a suspended virtual machine. For the RedHat crash utility, see White paper: RedHat Crash Utility.

Appendix A: Experience Portal specific best practices for VMware features

The following sections describe the Experience Portal-specific best practices for VMware features.

For more information on the general best practices for performance and VMware features, see *Customer Experience Virtualized Environment Solution Description*.

Performance Monitor

Use the esxtop tool on the ESXi host to monitor the performance of your virtual machines.

The following articles provide useful information on esxtop:

- Using esxtop to identify storage performance issues: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1008205
- Interpreting esxtop Statistics: http://communities.vmware.com/docs/DOC-9279

vMotion: Host migration and storage vMotion

The following are best practices for Experience Portal:

- If you use either host vMotion or storage vMotion for an MPP virtual machine, take the MPP offline prior to the migration to prevent call delays.
- If you use either host vMotion or storage vMotion for a live MPP virtual machine, ensure that during the migration there is minimal load on the underlying datastores.

  Ongoing datastore-heavy operations might overload the datastores and negatively impact virtual machines that use the datastores. Ongoing datastore-heavy operations include concurrent storage vMotion migrations or deployment of multiple OVAs or virtual machines.
- On a MPP handling heavy load with 100+ calls running a basic application using speech resources, all active calls might encounter a 3 to 6 second delay during the migration with loss of audio packets.
- Both primary and auxiliary EPMs might experience a 3 to 6 second delay in response time to Web Service requests.

- Migrate one virtual machine at a time to reduce impact on the performance of the virtual machine.
- Follow networking best practices, and use a separate vSwitch attached to a dedicated network for vMotion.
- Do not configure Experience Portal virtual machines to automatically migrate using Distributed Resource Scheduling.

High Availability

The following are best practices specific to Experience Portal:

- Each MPP must be configured with **Restart Automatically** set to **Yes** in EPM. To check the MPP setting, go to **EPM** > **System Configuration** > **MPP Servers** and click the name of the MPP server.
- Virtual servers that were running on a failed ESXi host will experience downtime until the virtual servers are started on another host in the HA cluster.

VM Snapshots

The following are best practices specific to Experience Portal:

- Experience Portal is a real-time application. Ensure that Experience Portal is not running when you take a snapshot or revert to a snapshot.
- To prevent the side effects, shutdown the virtual machine when you take or revert back to a snapshot. Otherwise, the running systems may experience side effects such as dropped calls, web sessions, and servers out of sync.
- If you take a snapshot of a live EPM virtual machine, and if you revert the snapshot, you must restart the EPM service from the command line to resynchronize the Experience Portal environment.

  Note:

  Log in to the console as sroot and run the `service vpms restart` command.
- If you take a snapshot of a live MPP virtual machine, and if you revert the snapshot, you must restart the MPP to re-synchronize the system.

Note:

Restart the MPP from the System Management > MPP Manager page in EPM.

- After reverting to a snapshot, and when the system is running, ensure that you delete all snapshots for the virtual machine in Snapshot Manager. The overhead of running with snapshots can impact the performance of the system.

Fault Tolerance

The Fault Tolerance feature is not supported with virtual machines using more than 1 CPU. All Experience Portal virtual servers are configured with 4 CPUs. Therefore, fault tolerance cannot be configured.

Glossary

AFS	Authentication File System. AFS is an Avaya Web system that allows you to create Authentication Files for secure Avaya Global Services logins for supported non-Communication Manager Systems.
Application	A software solution development by Avaya that includes a guest operating system.
Avaya Appliance	A physical server sold by Avaya running a VMware hypervisor that has several virtual machines, each with its virtualized applications. The servers can be staged with the operating system and application software already installed. Some of the servers are sold as just the server with DVD or software downloads.
Blade	A blade server is a stripped-down server computer with a modular design optimized to minimize the use of physical space and energy. Although many components are removed from blade servers to save space, minimize power consumption and other considerations, the blade still has all of the functional components to be considered a computer.
ESXi	A virtualization layer that runs directly on the server hardware. Also known as a *bare-metal hypervisor.* Provides processor, memory, storage, and networking resources on multiple virtual machines.
Hypervisor	A hypervisor is also known as a Virtual Machine Manager (VMM). A hypervisor is a hardware virtualization technique which runs multiple operating systems on the same shared physical server.
MAC	Media Access Control address. A unique identifier assigned to network interfaces for communication on the physical network segment.
OVA	Open Virtualization Appliance. An OVA contains the virtual machine description, disk images, and a manifest zipped into a single file. The OVA follows the Distributed Management Task Force (DMTF) specification.
PLDS	Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.
Reservation	A reservation is the amount of physical RAM, CPU cycles, or memory that are reserved for a virtual machine.
RFA	Remote Feature Activation. RFA is an Avaya Web system that you use to create Avaya License Files. These files are used to activate software including features, capacities, releases, and offer categories. RFA also

	creates Authentication Files for secure Avaya Global Services logins for Communication Manager Systems.
SAN	Storage Area Network. A SAN is a dedicated network that provides access to consolidated data storage. SANs are primarily used to make storage devices, such as disk arrays, accessible to servers so that the devices appear as locally attached devices to the operating system.
Snapshot	Capture a virtual appliance configuration in time. Creating a snapshot can affect service. Some Avaya virtual appliances have limitations and others have specific instructions for creating snapshots.
Storage vMotion	A VMware feature that migrates virtual machine disk files from one data storage location to another with limited impact to end users.
vCenter 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.
HA	High Availability. A VMware feature for supporting virtual application failover by migrating the application from one ESXi host to another. Since the entire host fails over, several applications or virtual machines can be involved. The failover is a reboot recovery level which can take several minutes.
vSphere Client	vSphere Client is VMware’s computer cloud virtualization operating system.

Index

U

V

W