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

Release 7.2.3
Issue 1
September 2019

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

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

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 or an Instance of the Software.

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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

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

Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

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: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for deploying the Avaya 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.

The primary audience for this document is anyone who is involved with installing, configuring, and verifying Avaya Aura® Experience Portal in a VMware® vSphere™ 5.5 or 6.0 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.

Chapter 2: Architecture overview

Avaya Customer Experience Virtualized Environment overview

Avaya Customer Experience Virtualized Environment integrates Avaya Aura® Contact Center applications 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.

Experience Portal server configuration options

The Experience Portal 7.2 release for the virtualized environment supports both multiple server and single server setups.

- The multiple server setup includes two or more virtual machines, one dedicated to running the Primary EPM software and at least one dedicated to the MPP software.
- In a single server setup, the Primary EPM and the MPP software are located on the same virtual machine. The single server configuration can be deployed with an optional co-resident application server.

Virtualized components

Software component	Description
ESXi Host	The physical machine running the ESXi Hypervisor software.
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer at the same time.
vSphere Client	vSphere Client is an application that installs and manages virtual machines. vSphere Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. The application is installed on a personal computer or accessible through a web interface. The installable vSphere Client is not available in vSphere 6.5 and later releases.
vSphere Web Client	Using a Web browser, vSphere Web Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used.
vSphere Client (HTML5)	vSphere Client (HTML5) is available in vSphere 6.5. Using a Web browser, it connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. This is the only vSphere client administration tool after the next vSphere release.
vCenter Server	vCenter Server provides centralized control and visibility at every level of the virtual infrastructure. vCenter Server provides VMware features such as High Availability and vMotion.
Appliance Virtualization Platform	Avaya-provided virtualization turnkey solution that includes the hardware and all the software including the VMware hypervisor.
Solution Deployment Manager	Centralized software management solution of Avaya that provides deployment, upgrade, migration, and update capabilities for the Avaya Aura® virtual applications.
Open Virtualization Appliance (OVA)	The virtualized OS and application packaged in a single file that is used to deploy a virtual machine.

Deployment guidelines

- Deploy maximum number of virtualized environment 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.
- Create a tiered or segmented cluster infrastructure that isolates critical applications, such as CMS, from other virtual machines.
- 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.

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 servers, 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 either ESXi 5.5 or ESXi 6.0 with the latest updates.

Configuration tools and utilities

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

- Experience Portal OVAs.

  You can download Experience Portal OVAs from the Avaya Product Licensing and Delivery System (PLDS) website.
- A computer with the VMware vSphere client that can route to the VMware server.
- The Avaya Enhanced Access Security Gateway (EASG) or Secure Access Link (SAL) tool.

  Avaya service technicians use EASG or SAL to remotely log in to the servers that are under a service agreement.

- The order number of the customer.
- The Avaya WebLM license server OVA, Avaya WebLM license server, or the built-in Avaya WebLM for Primary EPM.

  Note:

  Do not use the Avaya WebLM license server if you install the local WebLM installed with Experience Portal .

  WebLM manages the licensing of Experience Portal. For more information about the Avaya WebLM OVA, see *Deploying Avaya Aura® Experience Portal in an Avaya Customer Experience Virtualized Environment* on the Avaya Support website at https://support.avaya.com.

Experience Portal Virtual Machine resource requirements

Before you deploy each Experience Portal virtual machine, ensure that the following set of resources are available on the ESXi host.

VMware resource	Value
CPU	4 virtual sockets 1 core per socket
vCPU reservation	9500 MHz
Memory reservation	4 GB
Storage reservation	160 GB
Shared NICs	1 Gbps or more

VMware software requirements

The following VMware software versions are supported along with any available updates:

- VMware ESXi 5.5
- VMware ESXi 6.0
- VMware vCenter Server 5.5
- VMware vCenter Server 6.0

VMware vCenter Server is compatible with the same or older release of ESXi, but not compatible with a newer release of ESXi. For example: ESXi 6.0 is compatible with vCenter Server 6.0 or later, however, it is not compatible with vCenter Server 5.5. See VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php to view compatibility with other solution releases.

Compatible Web browsers

Experience Portal supports the following Web browsers:

- Microsoft Internet Explorer 11
- Mozilla FireFox latest version

Capacity

The Experience Portal capacity limits and port sizing details are documented in *Application Notes for Avaya Aura® Experience Portal 7.2 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 type	Parameter	Value
Primary EPM Auxiliary EPM	Destination directory	`/opt/Avaya/ExperiencePortal`
Primary EPM	Initial Experience Portal Admin user name and password	Username: epadmin Password: epadmin01
Primary EPM Auxiliary EPM MPP	Root access to Linux	Username: root Password: rootpw Username: root Changed password:
Primary EPM Auxiliary EPM MPP	Change root access to Linux	Username: root Default password: rootpw Changed password: ________
Primary EPM Auxiliary EPM MPP	Non-root access to Linux	Username: cust Password: custpw Changed password:
Primary EPM Auxiliary EPM MPP	Change non-root access to Linux	Username: cust Password: custpw Changed password: ________

Table continues…

OVA type	Parameter	Value
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.

Table continues…

Required data	Value for the system	Note
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.
EASG	Value: ————————	

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

As of EP 7.2 WebLM can be configured on the Primary EPM OVA.

You may also deploy the Avaya WebLM OVA packaged for VMware if you do not have a WebLM server that is being used to license an Experience Portal system. You can also use the WebLM built into the Primary EPM.

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://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.

In a single server setup, you must install only the Primary EPM OVA and then enable the co-resident MPP.

In a multiple server setup, you must deploy the OVA files in the following order:

1. Avaya WebLM OVA. If you do not already have a WebLM server, skip this step to use the WebLM built into the Primary EPM.
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 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 desired disk format to store the virtual machine and the virtual disk.

Note:

Using Thick Provision Lazy Zero disks is suggested. 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 invalid network settings during the deployment procedure, the system prompts you to configure the network settings again after you restart the virtual machine and log in to the console as the root user.

14. Configure EASG.

    The system displays the EASG Acceptance of Terms page. Perform one of the following steps:

    - Select **Yes** to enable EASG.

      With the **Enable EASG** option, you gain access to all Avaya Services Login during the primary EPM installation.

    - Select **No** to disable EASG.

      With the **Disable EASG** option, you cannot log in to the Experience Portal server with any Avaya Services Login during the primary EPM installation.

    The system applies this selection to other systems within the Experience Portal system including MPP and auxiliary EPMs. If you restore a backup later, either as part of an Experience Portal upgrade, or a normal backup/restore procedure, the system might override your selection by using the one restored from the backup.

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

16. **(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.

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 root user and check for errors. If any deployment errors are detected, Experience Portal alerts you about the errors when you log in as a root user to the console or SSH as session.

   Note:

   On the root login, the Avaya First Login Experience will run forcing the user to set the boot loader password and to change the root and cust passwords. The default passwords for root and cust accounts are rootpw and custpw respectively. You can gain access to the sroot and craft accounts if EASG is enabled.
3. Deploy MPP servers.
4. If you plan to deploy auxiliary EPM servers, configure the primary EPM server to support one or more auxiliary EPM servers.
5. (Optional) Deploy auxiliary EPM servers.
6. (Optional) Enable the co-resident MPP.

Related links

Configuring the primary EPM server to support one or more auxiliary EPM servers on page 73

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 Thick Provision 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 root user.

During Auxiliary EPM software installation, the system sets the EASG state as the same EASG state of the Primary EPM if the Auxiliary EPM server does not have an EASG state. If the Auxiliary EPM server is set to disable EASG, ensure that you have access to the system without the Avaya Service Logins. Ensure that you have root access without using the sroot user.

14. Verify the deployment properties and complete the deployment procedure.
15. **(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.

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 root user and check for errors. If any deployment errors are detected, Experience Portal alerts you about the errors when you log in as a root user to the console or SSH as session.

   Note:

   On the root login, the Avaya First Login Experience will run forcing the user to set the boot loader password and to change the root and cust passwords. The default passwords for root and cust accounts are rootpw and custpw respectively. You can gain access to the sroot and craft accounts if EASG is enabled, and only by Avaya technicians.
3. Configure the password for the database user vpcommon on the virtual machine.
4. Deploy MPP servers.

Related links

Configuring the primary EPM server to support one or more auxiliary EPM servers on page 73

Configuring a password for database user vpcommon on an auxiliary EPM server on page 74

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 Thick Provision 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 root user.
    >
    > During MPP software installation, the system sets the EASG state as the same EASG state of the Primary EPM if the Auxiliary EPM server does not have an EASG state. If the MPP server is set to disable EASG, ensure that you have access to the system without the Avaya Service Logins. Ensure that you have root access without using the root.

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

15. **(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.

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 root user and check for errors. If any deployment errors are detected, Experience Portal alerts you about the errors when you log in as a root user to the console or SSH as session.

Note:

On the root login, the Avaya First Login Experience will run forcing the user to set the boot loader password and to change the root and cust passwords. The default passwords for root and cust accounts are rootpw & custpw respectively. You can gain access to the sroot and craft accounts if EASG is enabled, and only by Avaya technicians.

3. Configure the MPP server.

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. After configuring the product ID, the system prompts whether you want to enable EASG. Perform one of the following steps:
    - Select **Yes** to enable EASG.

      With the **Enable EASG** option, you gain access to all Avaya Services Login during the primary EPM installation.

- Select **No** to disable EASG.

  With the **Disable EASG** option, you cannot log in to the Experience Portal server with any Avaya Services Login during the primary EPM installation.

5. Verify the details about the Experience Portal OVA template.
6. Verify and accept the license agreement.
7. Enter a unique name for the new virtual machine.
8. Select the resource pool if the host has resource pools.
9. 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.
10. Select the required disk format to store the virtual machine and the virtual disks.

    Note:

    Using Thick Provision Lazy Zero disks is suggested. For more information about thin vs thick deployments and best practices for VMware features, see *Avaya Customer Experience Virtualized Environment Solution Description*.
11. 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.
12. Verify the deployment properties and complete the deployment procedure.
13. **(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.

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 root user and check for errors. If any deployment errors are detected, Experience Portal alerts you about the errors when you log in as a root user to the console or SSH as session.

   Note:

   On the root login, the Avaya First Login Experience will run forcing the user to set the boot loader password and to change the root and cust passwords. You can gain access to the sroot and craft accounts if EASG is enabled.

Related links

[Configuring the Primary EPM and the network parameters](#) on page 27
[Configuring the Auxiliary EPM and the network parameters](#) on page 28
[Configuring MPP and the network parameters](#) on page 30

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.

14. Configure the EASG.

    The system displays the EASG Acceptance of Terms page. Perform one of the following steps:

    - Select **Yes** to enable EASG.

      The **Enable EASG** option does not allow the Avaya Services Logins access to the system through EASG.

    - Select **No** to disable EASG.

      The **Disable EASG** option does not block the Avaya Services Logins from accessing the system. If you select this option, ensure that you have access to the system without the Avaya Services Login, and ensure that you get the root access without using root.

    The system applies this selection to other systems within the Experience Portal system including MPP and auxiliary EPMs. If you restore a backup later, either as part of an Experience Portal upgrade, or a normal backup/restore procedure, the system might override your selection by using the one restored in the backup.

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.
3. (Optional) Enable the co-resident MPP.

Related links

Deploying the Experience Portal OVAs directly on the ESXi server with vSphere Client on page 25

Configuring the primary EPM server to support one or more auxiliary EPM servers on page 73

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`.

    During Auxiliary EPM software installation, the system sets the EASG state as the same EASG state of the Primary EPM if the Auxiliary EPM server does not have an EASG state. If the Auxiliary EPM server is set to disable EASG, ensure that you have access to the system without the Avaya Service Logins. Ensure that you have root access without using the sroot.
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 links

Deploying the Experience Portal OVAs directly on the ESXi server with vSphere Client on page 25
Configuring the primary EPM server to support one or more auxiliary EPM servers on page 73
Configuring a password for database user vpcommon on an auxiliary EPM server on page 74

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`.

    During MPP software installation, the system sets the EASG state as the same EASG state of the Primary EPM if the Auxiliary EPM server does not have an EASG state. If the MPP server is set to disable EASG, ensure that you have access to the system without the Avaya Service Logins. Ensure that you have root access without using the root.

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 links

Deploying the Experience Portal OVAs directly on the ESXi server with vSphere Client on page 25

Deploying the EPM OVA on a single server

About this task

For a single server deployment, you need to install only the Primary EPM OVA. The Primary EPM OVA contains a co-resident MPP that is disabled by default.

Procedure

1. Deploy the Primary EPM OVA. For more information, see Deploying the Primary EPM OVA with vCenter on page 18 or Deploying the Experience Portal OVAs directly on the ESXi server with vSphere Client on page 25.
2. Enable the co-resident MPP.

Related links

Enabling the co-resident MPP on page 31

Disabling the co-resident MPP on page 32

Optional: Single server Avaya Aura Experience Portal and Application server configuration on page 32

Enabling the co-resident MPP

Before you begin

Ensure that you have deployed the Primary EPM OVA on a single server virtual machine.

About this task

The Primary EPM OVA contains a co-resident MPP that is disabled by default. For a single server deployment, you must enable the co-resident MPP.

Procedure

1. Log in to the Linux console as root.
2. Navigate to `/opt/Avaya/VE/bin`.
3. Run the command **`# bash configureMPP.sh enable`**.

Related links

Deploying the EPM OVA on a single server on page 31

Disabling the co-resident MPP

About this task

The Primary EPM OVA contains a co-resident MPP that is disabled by default. However, if you have enabled the co-resident MPP, you can disable it by following these procedures.

Procedure

1. Log in to the Linux console as root.
2. Navigate to `/opt/Avaya/VE/bin`.
3. Run the command **`# bash configureMPP.sh disable`**.

Related links

Deploying the EPM OVA on a single server on page 31

Optional: Single server Avaya Aura® Experience Portal and Application server configuration

If you install Avaya Aura® Experience Portal, EPM, and the media server software on the same server, you can also install a Tomcat application on that server. Avaya supports Tomcat 8.x or later versions.

Avaya Aura® Experience Portal includes an installation script for the Tomcat 8.5.42 application server. You can also do a manual installation of this Tomcat application server.

For detailed information about installing a Tomcat application server on the Experience Portal server, see *Implementing Avaya Aura® Experience Portal on a single server*.

Related links

Deploying the EPM OVA on a single server on page 31

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.

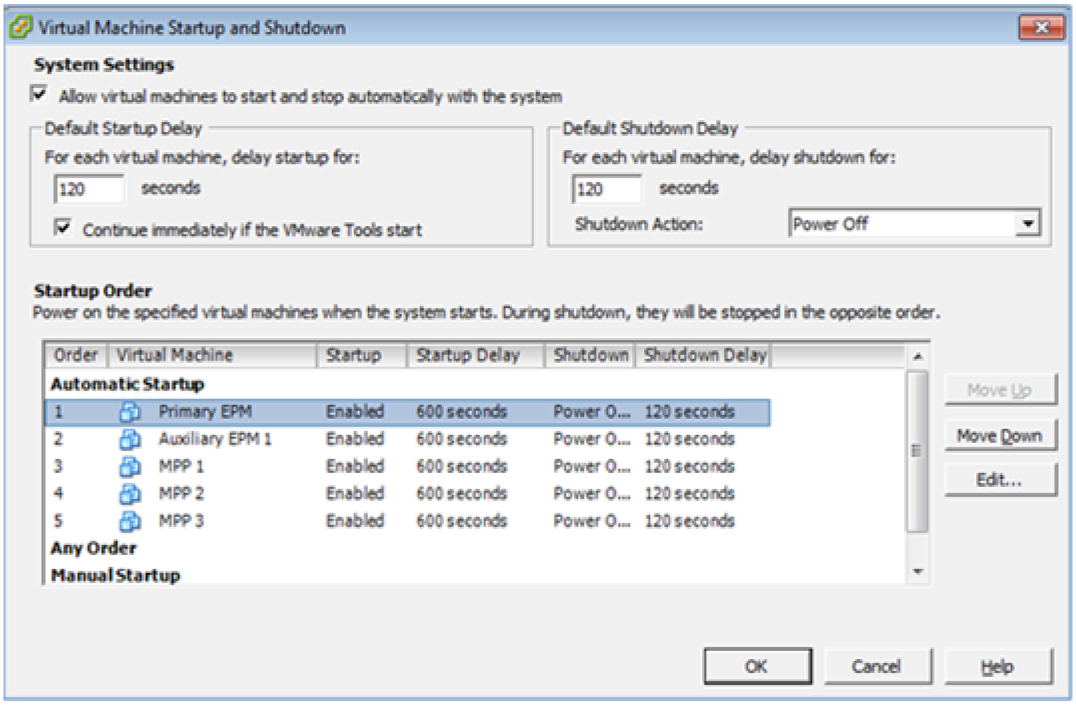
Procedure

1. In the navigation pane, click the host where the virtual machine is located.
2. Click **Configure**.
3. In Virtual Machines, click **VM Startup/Shutdown**, and then click **Properties**.

   The software displays the Edit VM Startup and Shutdown window.
4. Click **Automatically start and stop the virtual machines with the system**.
5. Click **OK**.

Example

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



Virtual Machine Startup and Shutdown

System Settings

☑ Allow virtual machines to start and stop automatically with the system

Default Startup Delay

For each virtual machine, delay startup for:

120 seconds

☑ Continue immediately if the VMware Tools start

Default Shutdown Delay

For each virtual machine, delay shutdown for:

120 seconds

Shutdown Action: Power Off

Startup Order

Power on the specified virtual machines when the system starts. During shutdown, they will be stopped in the opposite order.

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Automatic Startup					
1	Primary EPM	Enabled	600 seconds	Power O...	120 seconds
2	Auxiliary EPM 1	Enabled	600 seconds	Power O...	120 seconds
3	MPP 1	Enabled	600 seconds	Power O...	120 seconds
4	MPP 2	Enabled	600 seconds	Power O...	120 seconds
5	MPP 3	Enabled	600 seconds	Power O...	120 seconds
Any Order					
Manual Startup					

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 EASG as described in Enhanced Access Security Gateway on page 33.	
2	Log in to the EPM Web interface as described in Logging in to the Experience Portal web interface on page 49. If you are an Avaya Services representative, log in as described in Logging into the using the Avaya Services init account.	

Table continues…

Step	Description	✔
3	Install the Experience Portal license file as described in Installing a license file on page 49. **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	Add H.323 connections or add at least one SIP connection. For more information, see *Administering Avaya Aura® Experience Portal*.	
5	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*.	
6	(Optional) Add one or more Automatic Speech Recognition (ASR) servers. For more information, see *Administering Avaya Aura® Experience Portal*.	
7	Add one or more Text-to-Speech (TTS) servers. For more information, see *Administering Avaya Aura® Experience Portal*.	

Table continues…

Step	Description	✔
8	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 73. • Configure the auxiliary EPM as described in Configuring password for database user vpcommon on an auxiliary EPM on page 74. • Verify that the primary EPM and auxiliary EPM servers can communicate with each other using either of the following options: - A Domain Name Server (DNS) to translate hostnames to their corresponding IP addresses - The /etc/hosts file to map the IP addresses and hostnames **Note:** For more information on verifying communication between the primary EPM server and all other servers, see *Implementing Avaya Aura® Experience Portal on multiple servers*.	
9	If you have deployed auxiliary EPM servers, add the auxiliary EPM servers. For more information, see *Administering Avaya Aura® Experience Portal*.	
10	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*.	
11	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*.	
12	To enable multi-tenancy in Experience Portal, run the `EnableOrganizations` command. For more information, see *Administering Avaya Aura® Experience Portal*.	
13	Start all MPP servers. For more information, see *Administering Avaya Aura® Experience Portal*.	
14	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 75.	

Enhanced Access Security Gateway (EASG)

EASG provides a secure method for Avaya services personnel to access Avaya Aura® Experience Portal both remotely and on-site. 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.

The EASG authentication method is based on cryptographic signature verification of responses using the certificates issued by Avaya.

The following are the key points for EASG implementation:

- The old ASG (Avaya Security Gateway) is obsolete. The ASG RPM (asgtools) is removed during the Avaya Aura® Experience Portal installation process.
- The Avaya Service Account authentication file is no longer used to control access to services logins.
- Avaya Services Logins supported in Avaya Aura® Experience Portal EASG are init, inads, craft, and sroot. EASG does not affect the permissions associated with Avaya Services Logins. For more information, see Avaya Services Logins supported by EASG on page 37.

Note:

The rasaccess account is disabled and not supported.

Related links

Avaya Service Logins supported by EASG on page 37
Avaya Aura Experience Portal 7.x product certificate on page 38
EASG Acceptance of Terms on page 38
EASG states on page 39
Enabling EASG on page 40
Disabling EASG on page 41
Displaying EASG status on page 42
EASG built-in utilities on page 43
EASG Challenge-Response Authentication on page 44
EASG Site Certificate Management on page 44

Avaya Service Logins supported by EASG

User name	Group	Purpose
sroot	root, avayavpgroup	Avaya Services root access
craft	susers, avayavpgroup	Avaya Services non-root access
init	susers	Avaya Services non-root access
inads	susers	Avaya Services non-root access
init	Administration, Auditor, User manager, Privacy manager roles	EPM service user account

Related links

Enhanced Access Security Gateway (EASG) on page 36

Avaya Aura® Experience Portal 7.x product certificate

Avaya Aura® Experience Portal 7.2 installer installs a dedicated Avaya Aura® Experience Portal 7.x product certificate at the `/etc/asg/Product.p7b` directory in each server. The product certificate is x509v3 compliant and is derived from Avaya IT Root CA. It uniquely identifies the major releases of Avaya Aura® Experience Portal 7.x to the Avaya EASG backend server.

Product certificate contents

To view the contents of the product certificate, you must run the `EASGProductCert --certInfo` command.

Example:

```
EASGProductCert --certInfo
Subject: CN=Avaya Aura Experience Portal 7.2, OU=EASG, O=Avaya Inc.
Serial Number: 10001
Expiration: Jul 27 04:00:00 2031 GMT
Trust Chain:
1. O=Avaya, OU=IT, CN=AvayaITrootCA2
2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
4. CN=Product EASG Intermediate CA, OU=EASG, O=Avaya Inc.
5. CN=Avaya Aura Experience Portal 7.2, OU=EASG, O=Avaya Inc.
```

Product certificate update

Every major release requires the generation of a new EASG product certificate. The Avaya Aura® Experience Portal 7.x product certificate that is shipped with the 7.x release is the EASG product certificate for all Avaya Aura® Experience Portal 7.x releases.

If the product certificate is deleted, modified, or replaced illegally, Avaya can no longer provide remote access support to the customer.

If the Avaya Aura® Experience Portal 7.x product certificate is revoked by the Avaya backend server, only a software patch or new software release can replace the revoked certificate.

Product certificate monitoring

The Avaya Aura® Experience Portal 7.x EASG product certificate is valid for 15 years. The primary EPM raises major alarms when the product certificate approaches the following expiration days:

- EASG Product certificate expiration pending:
  - 365 days
  - 180 days
  - 30 days
- EASG Product Certificate expired.

Related links

Enhanced Access Security Gateway (EASG) on page 36

EASG Acceptance of Terms

Avaya Aura® Experience Portal displays the following EASG Acceptance of Terms during the installation of the primary EPM of Avaya Aura® Experience Portal. The message displays only if the user has not configured EASG on the primary EPM or when `EASGConfigure.sh` script is run on any Avaya Aura® Experience Portal server.

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 Avaya Logins you are preventing Avaya access to your system. This is not
recommended, as it impacts Avaya’s
ability to provide support for the product. Unless the customer is well versed in
managing the product themselves,
Avaya Logins should not be disabled.
```

Important:

The EASG selection you make during the primary EPM installation is applied to other systems within the Experience Portal system including new MPPs and auxiliary EPMs which are subsequently installed.

Related links

Enhanced Access Security Gateway (EASG) on page 36

EASG states

The following are the valid EASG states:

- Enabled EASG: The state that the user selects to enable EASG during the primary EPM installation or run the EASGConfigure.sh script provided by Experience Portal to enable EASG. When EASG is enabled, access to all Avaya Services Logins will be EASG protected.
- Disabled EASG: The state that the user selects to disable EASG during the primary EPM installation or run the EASGConfigure.sh script provided by Experience Portal to disable EASG. When EASG is disabled, it will not be possible to login to the Avaya Aura® Experience Portal server with any Avaya Services Login.

Important:

- The user uses the EASGConfigure.sh script to enable or disable EASG after installing Experience Portal.
- Users with root privileges or users who belong to the susers group can run the EASGConfigure.sh script to enable or disable EASG.

Note:

The primary EPM software installation will always display the Acceptance of Terms prompt to enable or disable EASG, if EASG is not installed. The auxiliary EPM and MPP software installation will query the primary EPM EASG state and set the same EASG state, if EASG is not installed.

Related links

Enhanced Access Security Gateway (EASG) on page 36

Enabling EASG

About this task

Use the EASGConfigure.sh script to enable EASG on an Avaya Aura® Experience Portal server. After EASG is enabled, the Avaya Services Logins accounts are EASG protected. Use the challenge-response authentication to log in to the Avaya Aura® Experience Portal server.

Note:

- Using EASGConfigure.sh script to enable EASG on an Avaya Aura® Experience Portal server does not enable EASG on other existing servers in the Avaya Aura® Experience Portal system. To enable EASG on other servers, run the script on each server.
- Users with root privileges or users who belong to the susers group can run the EASGConfigure.sh to enable EASG.

Before you begin

- Ensure that the server has a non-Avaya service account with root privilege or a user that belongs to the susers group to run the EASGConfigure.sh script.
- You cannot log in to the Experience Portal server with an Avaya Services Login account if the current state of the server is disabled.

Procedure

1. Log on to the Avaya Aura® Experience Portal Linux server locally as a user with root privilege or as a user who belongs to the susers group. Or, log in remotely as a non-root user and then change the user to a user with root privileges or a user that belongs to the susers group by entering the **`su -`** command.
2. Navigate to the `$AVAYA_HOME/Support/Security-Tools/EASG` directory where the script is located.
3. Run the **`bash EASGConfigure.sh --enable`** command. The script displays the Acceptance of terms prompt for enabling EASG.

   Example:

```
bash EASGConfigure.sh --enable
Invocation at Tue Apr 25 16:35:50 PDT 2017
LOG FILE: /opt/Avaya/ExperiencePortal/logs/EASGConfigure/EASGConfigure.sh.
2017-04-25.log
Enhanced Access Security Gateway (EASG)
EASG is disabled
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.
Do you want to enable EASG [yes/no]?
```

4. Type one of the following:
    - `yes` to accept the EASG terms.
    - `no` to cancel.
5. Review the output and debug log from the `/opt/Avaya/ExperiencePortal/logs/EASGConfigure` directory to ensure that the script completes successfully.

Related links

Enhanced Access Security Gateway (EASG) on page 36

Disabling EASG

About this task

Use the EASGConfigure.sh script to disable EASG on an Avaya Aura® Experience Portal server.

After EASG is disabled:

- Avaya Services Logins accounts will be blocked from logging in to the Avaya Aura® Experience Portal server.
- EPM service account init will be blocked from logging in to the primary EPM.

Note:

- Using the EASGConfigure.sh script to disable EASG on an Avaya Aura® Experience Portal server does not disable EASG on other existing servers in the Avaya Aura® Experience Portal system. To disable EASG on other servers, run the script on each server.
- Users with root privileges or users who belong to the susers group can run the EASGConfigure.sh to disable EASG.

Before you begin

Ensure that the server has a non-Avaya service account with root privilege or a user that belongs to susers group to run the EASGConfigure.sh script.

Procedure

1. Log on to the Avaya Aura® Experience Portal Linux server locally as a user with root privileges or as a user who belongs to the susers group. Or, log in remotely as a non-root user and then change the user to a user who belongs to the susers group by entering the **`su -`** command.
2. Navigate to the `$AVAYA_HOME/Support/Security-Tools/EASG` directory where the script is located.
3. Run the **`bash EASGConfigure.sh --disable`** command. The script displays the Acceptance of terms prompt for disabling EASG.

Example:

```
bash EASGConfigure.sh --disable
Invocation at Tue Apr 25 16:39:51 PDT 2017
LOG FILE: /opt/Avaya/ExperiencePortal/logs/EASGConfigure/EASGConfigure.sh.
2017-04-25.log
Enhanced Access Security Gateway (EASG)
EASG is enabled
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.
```

4. Type one of the following:
   - `yes` to accept the EASG terms.
   - `no` to cancel.
5. Review the output and debug log from `/opt/Avaya/ExperiencePortal/logs/EASGConfigure` directory to ensure that the script completes successfully.

Related links

Enhanced Access Security Gateway (EASG) on page 36

Displaying EASG status

About this task

Use the EASGConfigure.sh script to display the current EASG state on an Avaya Aura® Experience Portal server. The current EASG state can be either enabled or disabled.

Before you begin

If the current EASG state of the Avaya Aura® Experience Portal server is disabled, it will not be possible to log into the Experience Portal server with any Avaya Services Login accounts. Ensure that the server has a non-Avaya service account with root privilege or a user that belongs to the susers group to run the EASGConfigure.sh script.

Procedure

1. Log on to the Avaya Aura® Experience Portal Linux server locally as root or as a user who belongs to the susers group. 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 `$AVAYA_HOME/Support/Security-Tools/EASG` directory where the script is located.
3. Run one of the following commands:
   - **`bash EASGConfigure.sh`**
   - **`bash EASGConfigure.sh --status`**

   The script displays the current EASG state.

Related links

Enhanced Access Security Gateway (EASG) on page 36

EASG built-in utilities

Note:

You must always use the Avaya Aura® Experience Portal wrapper script EASGConfigure.sh to enable or disable EASG.

EASGProductCert

The EASGProductCert script is available to all users by default. It has two modes of operation:

- The script can print details about the product certificate.
- The script can check for product certificate expiration.

The following is a sample screen shot of the EASGProductCert command line arguments usage:

```
EASGProductCert --lessThanDays <number_of_days>
EASGProductCert --certInfo
Where:
--lessThanDays:
Determines if the certificate will expire within the number of days indicated by
<number_of_days>.  A return code of 1 indicates
 that the EASG Product Certificate will expire within <number_of_days>. A return code
of 0 indicates that the EASG Product
Certificate will not expire in <number_of_days>.  Finally, if an error is encountered,
a return code of 2 is issued.
--certInfo:
Display information about the EASG Product Certificate.
```

The following is a sample screen shot of running EASGProductCert with **`--certInfo`**:

```
EASGProductCert --certInfo
Subject: CN=Avaya Aura Experience Portal 7.2, OU=EASG, O=Avaya Inc.
Serial Number: 10001
Expiration: Jul 27 04:00:00 2031 GMT
Trust Chain:
1. O=Avaya, OU=IT, CN=AvayaITrootCA2
2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
4. CN=Product EASG Intermediate CA, OU=EASG, O=Avaya Inc.
5. CN=Avaya Aura Experience Portal 7.2, OU=EASG, O=Avaya Inc.
```

EASG Status

The EASGStatus script is available to all users by default. It displays the current EASG state as enabled or disabled.

EASGSiteCertManage

The EASGSiteCertManage is restricted to root access or users who belong to the susers group. Users who belong to the susers group can use **`sudo EASGSiteCertManage`** to run the script. The site certificates are primarily used by on-site technicians who do not have access to Avaya network when they are on the customer's premises. The **`EASGSiteCertManage`** command can be run with no options to get documentation about its usage.

Related links

Enhanced Access Security Gateway (EASG) on page 36

EASG Challenge-Response Authentication

EASG challenge generation

When EASG is enabled, an attempt to access the product via an Avaya Service Login will result in providing the following information:

- Challenge String: The new EASG Challenge String is the legacy ASG challenge format with the Product Certificate ID appended at the front. The Product Certificate ID is the serial number of the Avaya Aura® Experience Portal 7.x product certificate.
- Product ID String: The new Product ID string is a GUID (globally unique identifier) which is generated by the EASG RPM, with the EASG RPM version number appended at the end.

The following is a sample screen shot of the challenge and Product ID when trying to access the system using Avaya service account:

```
Challenge: 10001-85132972
Product ID: 09f2c551f32e4c808b7fd3c544365a8f01
Response:
```

EASG response generation

The Avaya EASG Web Mobile interface has been enhanced to accept all the existing challenge inputs for both ASG and EASG challenges. Avaya EASG Web Mobile then provides this information to the Avaya EASG backend server and displays the appropriate responses to the user.

The new EASG response strings can reach up to a maximum 512 bytes strings. There is a Copy Response to Clipboard button on the Avaya EASG Web Mobile web page which the user can use to copy the response string and paste it to the Linux login shell.

EASG response validation

If an EASG Response is not submitted to the product within 5 minutes of the EASG Challenge String being provided, the challenge shall expire. Any EASG response submitted against an expired challenge fails validation and the login will fail.

If the EASG Response validation succeeds, then the Avaya service account user is allowed access to the system with the permissions associated with the Avaya Service Login name. The Linux system log `/var/log/messages` will record an authentication through the success message of the product certificate.

If the EASG Response validation fails, the user will be denied access to the system and the challenge is depreciated. Any subsequent login attempt needs a new challenge. The Linux system log `/var/log/messages` will record an authentication failed message.

Related links

Enhanced Access Security Gateway (EASG) on page 36

EASG Site Certificate Management

Avaya technicians use the EASG Site Certificate when they do not have access to Avaya network to generate responses. The technicians generate the EASG Site Certificate by using the EASG Site Manager tool. After the technician generates the EASG Site Certificate successfully, the technician usually sends it to the customer with the instructions on how to install the Site Certificate.

Note:

The EASG Site Manager tool is based on version 7 and later.

Related links

Enhanced Access Security Gateway (EASG) on page 36
Generating a site certificate on page 45
Installing the Site Certificate on page 45
Displaying the site certificate content on page 46
Deleting a Site Certificate on page 47
Generating a Site Certificate response on page 48

Generating a site certificate

About this task

Use this procedure to generate a site certificate on the EASG site manager tool. The EASG site manager tool can issue only a single valid site certificate per technician at a given time. A new site certificate request will overwrite any previously valid site certificate if one exists.

Note:

The EASG site certificate will expire 2 weeks from the date of creation.

Procedure

1. Click the EASG Site Cert tab on the EASG Site Manager tool.
2. Click the **New** button to generate a new EASG Site Certificate.

   Once you generate the site certificate successfully, a message displays at the bottom of EASG Site Manager window. The message shows how long the site certificate is valid and where it is located.

Related links

EASG Site Certificate Management on page 44

Installing the Site Certificate

About this task

Use this procedure to install the EASG Site Certificate on the Avaya Aura® Experience Portal server.

The Linux system log `/var/log/messages` will record a successful Site Certificate installation message.

Procedure

1. Log on to the Avaya Aura® Experience Portal Linux server locally as root or a user who belongs to the susers group. Or log in remotely as a non-root user and then change the user to root by entering the **`su -`** command.
2. Upload the site certificate to the Avaya Aura® Experience Portal Linux server.

3. Run the EASG built-in tool **`EASGSiteCertManage`** to install the uploaded site certificate.
4. Run the **`(sudo) EASGSiteCertManage --add <filename> --saf <SAF>`** command.

   Where,

   - sudo: If the user who runs this command belongs to the susers group, **`sudo`** needs to be added in front of EASGSiteCertManage. If the user is a root privilege user, there is no need to add **`sudo`**.
   - Filename: The location of the Site Certificate.
   - SAF: The Site Authentication Factor code which is a 10 to 20 character alphanumeric string. The SAF is required for technician access when the technician later generates a response.

   Example:

   ```
   [root@EP72PRI voiceportal]# EASGSiteCertManage --add
   /home/voiceportal/test.p7b --saf 1234567890
   Site Certificate installed successfully.
   ```

Related links

EASG Site Certificate Management on page 44

Displaying the site certificate content

About this task

Use this procedure to display all the installed EASG Site Certificates on the Avaya Aura® Experience Portal server and to display the content of an installed EASG Site Certificate.

Procedure

1. Log on to the Avaya Aura® Experience Portal Linux server locally as root or a user who belongs to the susers group. Or, log in remotely as a non-root user and then change the user to root by entering the **`su -`** command.
2. To display a list of installed site certificates, run the **`(sudo) EASGSiteCertManage --list`** command.

   If the user who runs this command belongs to the susers group, **`sudo`** needs to be added in front of EASGSiteCertManage. If the user is a root privilege user, there is no need to add **`sudo`**.

   Example:

   ```
   [root@EASG voiceportal]# EASGSiteCertManage --list
   Valid Site Certificates:
     1. test.p7b
   ```
3. To display the content of a Site Certificate, run the **`(sudo) EASGSiteCertManage --show <SiteCertName>`** command.

Where,

- sudo: If the user who runs this command belongs to the susers group, **sudo** needs to be added in front of EASGSiteCertManage. If the user is a root privilege user, there is no need to add **sudo**.
- SiteCertName: The name of the Site Certificate

Example:

```
[root@EASG voiceportal]# EASGSiteCertManage --show test.p7b

Subject: CN=Avaya Technician test, OU=EASG, O=Avaya Inc.
User Name: test
Expiration: Feb 16 00:51:39 2017 GMT
Trust Chain:
1. O=Avaya, OU=IT, CN=AvayaITrootCA2
2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
4. CN=Site EASG Intermediate CA, OU=EASG, O=Avaya Inc.
5. CN=Avaya Technician dchen, OU=EASG, O=Avaya Inc.
```

Related links

EASG Site Certificate Management on page 44

Deleting a Site Certificate

About this task

The expired EASG Site Certificates will be automatically deleted by the Avaya Aura[®] Experience Portal system. Use this procedure to manually delete the installed EASG Site Certificate.

The Linux system log `/var/log/messages` will record a Site Certificate deletion message.

Procedure

1. Log on to the Avaya Aura[®] Experience Portal Linux server locally as root or as a user who belongs to the susers group. Or, log in remotely as a non-root user and then change the user to root by entering the **su -** command.
2. Run the **(sudo) EASGSiteCertManage --delete <SiteCertName>** command.

   Where,

   - sudo: If the user who runs this command belongs to the susers group, **sudo** needs to be added in front of EASGSiteCertManage. If the user is a root privilege user, there is no need to add **sudo**
   - SiteCertName: The name of the Site Certificate.

   Example:

   ```
   [root@EASG voiceportal]# EASGSiteCertManage --delete test.p7b
   Successfully removed Site Cert: test.p7b
   ```

Related links

EASG Site Certificate Management on page 44

Generating a Site Certificate response

About this task

Use this procedure to generate a Site Certificate response on the EASG Site Manager tool.

Procedure

1. Log in to the Avaya Aura® Experience Portal system using one of the Avaya Service Logins.

   The login shell displays the Challenge and Product ID.
2. On the EASG Site Manager tool, click the Authenticate tab.
3. Select **EASG (Certificate Based Authentication)** and click **OK**.

   The EASG Authentication window appears.
4. Enter the appropriate information in the fields.
5. Click **Generate Response** to create the response.
6. Click **Copy Response** to copy the response to the computer clipboard.
7. Paste the response into the login shell.

   The login is successful.

   The Linux system log `/var/log/messages` will record an authentication through the site certificate success message.

Related links

EASG Site Certificate Management on page 44
EASG Authentication field descriptions on page 48

EASG Authentication field descriptions

Name	Description
Equipment	The Product ID that displays in the login shell when you log in to the Avaya Aura® Experience Portal system using one of the Avaya Service Logins.
EquipLogin	The Avaya Service Login accounts (init, inads, craft, or sroot).
SAF PIN	The SAF code that the customer enters when the Site Certificate is installed.
Challenge	The challenge that displays in the login shell when you log in to the Avaya Aura® Experience Portal system using one of the Avaya Service Logins.
Response	The response that displays after you generate the response.

Related links

Generating a Site Certificate response on page 48

Logging in to the Experience Portal Web interface

About this task

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

Procedure

1. Open a compatible web browser and type **http://<EPM-server>//VoicePortal (useinput)**.
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, confirm the new password for the epadmin account.
9. Click **Submit**.

   The system returns you to the logon screen where you can login with the new password.

Installing the license file

You require a license file for the Experience Portal operation. The license file defines all features 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.

In Experience Portal 7.2, you can activate the WebLM license server on the Primary EPM OVA.

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 on 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 URL of the license server in the **License Server URL** 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, accept the WebLM license, and then 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.

Generating a new Primary EPM server security certificate

About this task

Use the SetupServerCertificate.sh script to generate a new SHA256 signature hash 2048 bits self-signed server certificate for the Primary EPM without re-installing the Experience Portal software.

In Avaya Aura® Experience Portal 7.2, the new script SetupServerCertificate.sh has replaced the old script GenerateServerCertificate.sh.

SetupServerCertificate.sh supports the following parameters:

- –generate: Generates a new SHA256 signature hash 2048 bits self-signed server certificate.
- –import: Allows the user to import a third-party certificate to replace the current server certificate.
- –display: Displays the current server certificate.

Before you begin

- Ensure that the Primary EPM server is not processing any multi channel messages such as Emails, SMS or HTML.
- If a managed application is installed, you might need to perform additional steps before and after the server certificate is updated. For more information, see the documentation of the managed application.

Important:

- The certificate is in PKCS12 format. The certificate must be formatted as a PKCS#12 file, which includes a certificate and the corresponding key. This certificate is encrypted and requires a password. If the certificate is not self-signed, then the PKCS#12 file must include all CA certificates.
- If **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication` which is also called serverAuth, and `Client Authentication` which is also called clientAuth, for the usage.
- The certificate must have a valid Common Name that represents the EP server host name.
- If the Subject Alternate Name is specified in the X509 V3 certificate extension, the certificate must contain valid DNS and IP Address entries that are associated with the EP server host name.
- The certificate must reside on a local server or on an NFS-mounted drive that is locally accessible.

Procedure

1. Log on to Linux on the Primary EPM server.
    - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.
    - Otherwise, log on remotely as a non-root user, and then change the user to root by entering the `su - root` command.
2. Navigate to the `$AVAYA_HOME/Support/Security-Tools` directory.
3. Enter the **`bash SetupServerCertificate.sh -generate`** command.

    The system displays a message indicating that the services will be restarted and asks whether the user wants to proceed.

    The following is a sample message:

    ```
    This utility will configure the Experience Portal certificate.
    During this process, the following services will be restarted if they are
    configured:
    - epmcompmgr
    - vpms
    - mmsserver
    - avpSNMPAgentSvc
    - httpd
    - mpp
    Do you wish to proceed? [Y/n]
    ```

    Note:

    If any service is not configured or not running on the server while the script is running, the script will not restart these services after a new certificate is installed.
4. Enter `Y` to proceed.

    The script then displays the newly generated SHA256 signature hash 2048 bits certificate content of the security certificate.
5. Enter one of the following:
    - `Y` to accept the imported certificate.
    - `n` to cancel.

    The script restarts all related services and displays a message indicating a new server certificate is installed successfully.
6. Enter the **`bash SetupServerCertificate.sh -display`** command to verify the contents of the newly generated server certificate.
7. Do the following to accept the new certificate on all Auxiliary EPMs and MPPs:
    a. On each auxiliary EPM and MPP, log in to the console as a `root` user.
    b. Navigate to the `$AVAYA_HOME/Support/VP-Tools` directory.
    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.

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

Generating a new Auxiliary EPM server security certificate

About this task

Use the SetupServerCertificate.sh script to generate a new SHA256 signature hash 2048 bits self-signed server certificate for the Auxiliary EPM without re-installing the Experience Portal software.

In Avaya Aura® Experience Portal 7.2, the new script SetupServerCertificate.sh has replaced the old script ImportServerCertificate.sh.

SetupServerCertificate.sh supports the following parameters:

- –generate: Generates a new SHA256 signature hash 2048 bits self-signed server certificate.
- –import: Allows the user to import a third-party certificate to replace the current server certificate.
- –display: Displays the current server certificate.

Before you begin

- Ensure that the Auxiliary EPM server is not processing any multi channel messages such as Emails, SMS or HTML.
- If a managed application is installed, you might need to perform additional steps before and after the server certificate is updated. For more information, see the documentation of the managed application.

Procedure

1. Log on to Linux on the Auxiliary EPM server.
   - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.
   - Otherwise, log on remotely as a non-root user, and then change the user to root by entering the `su - root` command.
2. Navigate to the `$AVAYA_HOME/Support/Security-Tools` directory.
3. Enter the **`bash SetupServerCertificate.sh -generate`** command.

   The system displays a message indicating that the services will be restarted and asks whether the user wants to proceed.

   The following is a sample message:

   ```
   This utility will configure the Experience Portal certificate.
   During this process, the following services will be restarted if they are
   configured:
   - epmcompmgr
   - vpms
   - mmsserver
   - avpSNMPAgentSvc
   ```

```
- httpd
- mpp
Do you wish to proceed? [Y/n]
```

Note:

If any service is not configured or not running on the server while the script is running, the script will not restart these services after a new certificate is installed.

4. Enter `Y` to proceed.

   The script then displays the newly generated SHA256 signature hash 2048 bits certificate content of the security certificate

5. Enter one of the following:

   - `Y` to accept the imported certificate.
   - `n` to cancel.

   The script restarts all related services and displays a message indicating a new server certificate is installed successfully.

6. Enter the **`bash SetupServerCertificate.sh -display`** command to verify the contents of the newly generated server certificate.

7. Do the following to re-establish the link between the Primary EPM and the Auxiliary EPM:

   a. Log on to the EPM web interface by using an account with the Administration user role.

   b. On the EPM main menu, click **System Configuration** > **EPM Servers**.

   c. Click the name of the Auxiliary EPM server.

   d. On the Change EPM Server page, navigate to the **Auxiliary EPM Certificate** section, and select the **Trust new certificate** check box if the check box is visible.

   e. Click **Save**.

   f. On the EPM main menu, click **Real-Time Monitoring** > **System Monitor**.

   g. **(Optional)** If the Config of the MPP displays **Restart needed**, restart the MPP.

Generating a new MPP server security certificate

Before you begin

- Ensure that the MPP server is not handling any calls.
- If a managed application is installed, you might need to perform additional steps before and after the server certificate is updated. For more information, see the documentation of the managed application.
- In Avaya Aura® Experience Portal 7.2, the new script SetupServerCertificate.sh has replaced the old script GenerateServerCertificate.sh.

Note:

SetupServerCertificate.sh supports the following parameters:

–generate: Generates a new SHA256 signature hash 2048 bits self-signed server certificate.

–import: Allows the user to import a third-party certificate to replace the current server certificate.

–display: Displays the current server certificate.

About this task

Use the SetupServerCertificate.sh script to generate a new SHA256 signature hash 2048 bits self-signed server certificate for the MPP without the need to re-install the Experience Portal software.

Procedure

1. Log in to Linux on the MPP server.
    - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.
    - Otherwise, log on remotely as a non-root user, and then change the user to root by entering the `su - root` command.
2. Navigate to `$AVAYA_HOME/Support/Security-Tools` directory.
3. Enter the `bash SetupServerCertificate.sh -generate` command.

    The system prompts a message indicating the services will be restarted and asks if the user wants to proceed.

    The following shows a sample message:

    ```
    This utility will configure the Experience Portal certificate.
    During this process, the following services will be restarted if they are
    configured:
    - epmcompmgr
    - vpms
    - mmsserver
    - avpSNMPAgentSvc
    - httpd
    - mpp
    Do you wish to proceed? [Y/n]
    ```

    Note:

    If any service is not configured or is not running on the server while the script is run, it will not be restarted by the script after a new certificate is installed.
4. Enter `Y` to proceed.

    The script then displays the newly generated SHA256 signature hash 2048 bits certificate content of the security certificate.
5. Enter `Y` to accept the certificate or enter `n` to cancel.

The script restarts all related services and displays a message indicating a new server certificate is installed successfully.

6. Enter the `bash SetupServerCertificate.sh -display` command to verify the contents of the newly imported server certificate.
7. Reestablish the link between the Primary EPM and the MPP:
    a. Log in to the EPM Web interface using an account with the Administration user role.
    b. From the EPM main menu, select **System Configuration** > **MPP Servers**.
    c. Click the name of the MPP server.
    d. On the **Change MPP Server** page, navigate to the **MPP Certificate** section and select the **Trust new certificate** check box if the check box is visible.
    e. Click **Save**.

Generating a new Single server security certificate

Before you begin

- Ensure that the Single EP server is not processing any multi channel messages such as Emails, SMS, or HTML.
- Ensure that the MPP is not processing any traffic.
- If a managed application is installed, you might need to perform additional steps before and after the server certificate is updated. For more information, see the documentation of the managed application.
- In Avaya Aura® Experience Portal 7.2, the new script SetupServerCertificate.sh has replaced the old script GenerateServerCertificate.sh.

  Note:

  SetupServerCertificate.sh supports the following parameters:

  –generate: Generates a new SHA256 signature hash 2048 bits self-signed server certificate.

  –import: Allows the user to import a third-party certificate to replace the current server certificate.

  –display: Displays the current server certificate.

About this task

Use the SetupServerCertificate.sh script to generate a new SHA256 signature hash 2048 bits self-signed server certificate for the EPM without the need to re-install the Experience Portal software.

Procedure

1. Log in to Linux on the Single EP server.
    - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.

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

2. Navigate to `$AVAYA_HOME/Support/Security-Tools` directory.
3. Enter the `bash SetupServerCertificate.sh -generate` command.

   The system prompts a message indicating the services will be restarted and asks if the user wants to proceed.

   The following shows a sample message:

   ```
   This utility will configure the Experience Portal certificate.
   During this process, the following services will be restarted if they are
   configured:
   - epmcompmgr
   - vpms
   - mmsserver
   - avpSNMPAgentSvc
   - httpd
   - mpp
   Do you wish to proceed? [Y/n]
   ```

   Note:

   If any service is not configured or is not running on the server while the script is run, it will not be restarted by the script after a new certificate is installed.

4. Enter `Y` to proceed.

   The script then displays the newly generated SHA256 signature hash 2048 bits certificate content of the security certificate.

5. Enter `Y` to accept the certificate or enter `n` to cancel.

   The script restarts all related services and displays a message indicating a new server certificate is installed successfully.

6. Enter the `bash SetupServerCertificate.sh -display` command to verify the contents of the newly generated server certificate.
7. Accept the new certificate on the MPP as described in the following steps:

   a. Log in to the console as root user on the Single server.

   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.

Importing a Primary EPM server security certificate

About this task

Use the SetupServerCertificate.sh script to import a self-signed or third-party signed certificate for the Primary EPM without re-installing the Experience Portal software.

In Avaya Aura® Experience Portal 7.2, the new script SetupServerCertificate.sh has replaced the old script ImportServerCertificate.sh.

SetupServerCertificate.sh supports the following parameters:

- –generate: Generates a new SHA256 signature hash 2048 bits self-signed server certificate.
- –import: Allows the user to import a third-party certificate to replace the current server certificate.
- –display: Displays the current server certificate.

Before you begin

- Ensure that the Primary EPM server is not processing any multi-channel messages such as Emails, SMS, or HTML.
- If a managed application is installed, you might need to perform additional steps before and after the server certificate is updated. For more information, see the documentation of the managed application.

Important:

- The certificate is in PKCS12 format. The certificate must be formatted as a PKCS#12 file, which includes a certificate and the corresponding key. This certificate is encrypted and requires a password. If the certificate is not self-signed, then the PKCS#12 file must include all CA certificates.
- If **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication` which is also called serverAuth, and `Client Authentication` which is also called clientAuth, for the usage.
- The certificate must have a valid Common Name that represents the EP server host name.
- If the Subject Alternate Name is specified in the X509 V3 certificate extension, the certificate must contain valid DNS and IP Address entries that are associated with the EP server host name.
- The certificate must reside on a local server or on an NFS-mounted drive that is locally accessible.

Procedure

1. Log on to Linux on the Primary EPM server.
    - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.

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

2. Navigate to the `$AVAYA_HOME/Support/Security-Tools` directory.
3. Enter the **`bash SetupServerCertificate.sh -import`** command.

   The system displays a message indicating that the services will be restarted and asks whether the user wants to proceed.

   The following is a sample message:

   ```
   This utility will configure the Experience Portal certificate.
   During this process, the following services will be restarted if they are
   configured:
   - epmcompmgr
   - vpms
   - mmsserver
   - avpSNMPAgentSvc
   - httpd
   - mpp
   Do you wish to proceed? [Y/n]
   ```

   Note:

   If any service is not configured or not running on the server while the script is running, the script will not restart these services after a new certificate is installed.

4. Enter `Y` to proceed.

   The script then prompts you to enter the file path and the name of the security certificate.

5. Type the file path and name of the security certificate, and press `Enter`.
6. At the prompt, type the password for the security certificate, and press `Enter`.

   The system displays the imported certificate content.

7. Enter one of the following:
   - `Y` to accept the imported certificate.
   - `n` to cancel.

   The script restarts all related services and displays a message indicating a new server certificate is installed successfully.

8. Enter the **`bash SetupServerCertificate.sh -display`** command to verify the contents of the newly imported server certificate.
9. Do the following to accept the new certificate on all Auxiliary EPMs and MPPs:
   a. On each auxiliary EPM and MPP, log in to the console as a `root` user.
   b. Navigate to the `$AVAYA_HOME/Support/VP-Tools` directory.
   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.

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

Importing an Auxiliary EPM server security certificate

About this task

Use the SetupServerCertificate.sh script to import a self-signed or third-party certificate for the Auxiliary EPM without re-installing the Experience Portal software.

In Avaya Aura® Experience Portal 7.2, the new script SetupServerCertificate.sh has replaced the old script ImportServerCertificate.sh.

SetupServerCertificate.sh supports the following parameters:

- –generate: Generates a new SHA256 signature hash 2048 bits self-signed server certificate.
- –import: Allows the user to import a third-party certificate to replace the current server certificate.
- –display: Displays the current server certificate.

Before you begin

- Ensure that the Auxiliary EPM server is not processing any multi-channel messages such as Email, SMS, or HTML.
- If a managed application is installed, you might need to perform additional steps before and after the server certificate is updated. For more information, see the documentation of the managed application.

Important:

- The certificate must be in PKCS12 format. The certificate must be formatted as a PKCS#12 file, which includes a certificate and the corresponding key. This certificate is encrypted and requires a password. If the certificate is not self-signed, then the PKCS#12 file must include all CA certificates.
- If **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication` which is also called serverAuth, and `Client Authentication` which is also called clientAuth, for the usage.
- The certificate must have a valid Common Name that represents the EP server host name.
- If the Subject Alternate Name is specified in the X509 V3 certificate extension, the certificate must contain valid DNS and IP Address entries that are associated with the EP server host name.
- The certificate must reside on a local server or on an NFS-mounted drive that is locally accessible.

Procedure

1. Log on to Linux on the Auxiliary EPM server.

   - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.

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

2. Navigate to `$AVAYA_HOME/Support/Security-Tools` directory.
3. Enter the **`bash SetupServerCertificate.sh -import`** command.

   The system displays a message indicating that the services will be restarted and asks whether the user wants to proceed.

   The following is a sample message:

   ```
   This utility will configure the Experience Portal certificate.
   During this process, the following services will be restarted if they are
   configured:
   - epmcompmgr
   - vpms
   - mmsserver
   - avpSNMPAgentSvc
   - httpd
   - mpp
   Do you wish to proceed? [Y/n]
   ```

   Note:

   If any service is not configured or not running on the server while the script is running, the script will not restart these services after a new certificate is installed.
4. Enter `Y` to proceed.

   The script then prompts you to enter the file path and the name of the security certificate.
5. Type the file path and name of the security certificate, and press `Enter`.
6. At the prompt, type the password for the security certificate, and press `Enter`.

   The system displays the imported certificate content.
7. Enter one of the following:
   - `Y` to accept the imported certificate.
   - `n` to cancel.

   The script restarts all related services and displays a message indicating a new server certificate is installed successfully.
8. Enter the **`bash SetupServerCertificate.sh -display`** command to verify the contents of the newly imported server certificate.
9. Do the following to re-establish the link between the Primary EPM and the Auxiliary EPM:
   a. Log on to the EPM web interface by using an account with the Administration user role.
   b. On the EPM main menu, click **System Configuration** > **EPM Servers**.
   c. Click the name of the Auxiliary EPM server.
   d. On the Change EPM Server page, navigate to the **Auxiliary EPM Certificate** section, and select the **Trust new certificate** check box if the check box is visible.

e. Click **Save**.

f. On the EPM main menu, click **Real-Time Monitoring** > **System Monitor**.

g. **(Optional)** If the Config of the MPP displays **Restart needed**, restart the MPP.

Importing an MPP server security certificate

About this task

Use this procedure to import a self-signed or third-party signed certificate for the Primary EPM without re-installing the Avaya Aura® Experience Portal software.

In Avaya Aura® Experience Portal 7.2, the new script SetupServerCertificate.sh has replaced the old script ImportServerCertificate.sh.

SetupServerCertificate.sh supports the following parameters:

- –generate: Generates a new SHA256 signature hash 2048 bits self-signed server certificate.
- –import: Enables the import of a third-party certificate to replace the current server certificate.
- –display: Displays the current server certificate.

Before you begin

- Ensure that the MPP server is not handling any calls.
- You may need to perform additional steps before and after the server certificate is updated, if a managed application is installed. For more information, see the documentation of the managed application.

Important:

- The certificate is in PKCS12 format. The certificate must be formatted as a PKCS#12 file, which includes a certificate and the corresponding key. This certificate is encrypted and requires a password. If the certificate is not self-signed, then the PKCS#12 file must include all CA certificates.
- If **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication`, which is also called serverAuth, and `Client Authentication`, which is also called clientAuth, for the usage.
- The certificate must have a valid Common Name that represents the EP server host name.
- If the Subject Alternate Name is specified in the X509 V3 certificate extension, the certificate must contain valid DNS and IP Address entries that are associated with the EP server host name.
- The certificate must reside on a local server or on an NFS-mounted drive that is locally accessible.

Procedure

1. Log on to Linux on the MPP server.

   - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.

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

2. Run the **`bash SetupServerCertificate.sh -import`** command.

   The system displays a message such as:

   ```
   This utility will configure the Experience Portal certificate.
   During this process, the following services will be restarted if they are
   configured:
   - epmcompmgr
   - vpms
   - mmsserver
   - avpSNMPAgentSvc
   - httpd
   - mpp
   Do you wish to proceed? [Y/n]
   ```

   Note:

   If any service is not configured or not running on the server while the script is running, the script does not restart these services after a new certificate is installed.

3. Enter `Y` to proceed.

4. At the prompt, type the file path and name of the security certificate, and press `Enter`.

5. At the prompt, type the password for the security certificate, and press `Enter`.

   The system displays the imported certificate content.

6. Enter one of the following:

   - `Y` to accept the imported certificate.

   - `n` to cancel.

   The script restarts all related services and displays a message indicating a new server certificate is installed successfully.

7. Run the **`bash SetupServerCertificate.sh -display`** command to verify the contents of the newly imported server certificate.

8. To re-establish the link between the Primary EPM and the MPP, do the following:

   a. Log on to the EPM web interface by using an account with the Administration user role.

   b. On the EPM main menu, click **System Configuration** > **MPP Servers**.

   c. Click the name of the MPP server.

d. On the Change MPP Server page, navigate to the **MPP Certificate** section, and select the **Trust new certificate** check box.

e. Click **Save**.

Importing a Single server security certificate

About this task

Use the SetupServerCertificate.sh script to import a self-signed or third-party certificate for the Single EP server without re-installing the Experience Portal software.

In Avaya Aura® Experience Portal 7.2, the new script SetupServerCertificate.sh has replaced the old script ImportServerCertificate.sh.

SetupServerCertificate.sh supports the following parameters:

- –generate: Generates a new SHA256 signature hash 2048 bits self-signed server certificate.
- –import: Allows the user to import a third-party certificate to replace the current server certificate.
- –display: Displays the current server certificate.

Before you begin

- Ensure that the Single EP server is not processing any multi-channel messages such as Emails, SMS, or HTML.
- Ensure that the MPP is not processing any traffic.
- If a managed application is installed, you might need to perform additional steps before and after the server certificate is updated. For more information, see the documentation of the managed application.

Important:

- The certificate must be in PKCS12 format. The certificate must be formatted as a PKCS#12 file, which includes a certificate and the corresponding key. This certificate is encrypted and requires a password. If the certificate is not self-signed, then the PKCS#12 file must include all CA certificates.
- If **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication` which is also called serverAuth, and `Client Authentication` which is also called clientAuth, for the usage.
- The certificate must have a valid Common Name that represents the EP server host name.
- If the Subject Alternate Name is specified in the X509 V3 certificate extension, the certificate must contain valid DNS and IP Address entries that are associated with the EP server host name.
- The certificate must reside on a local server or on an NFS-mounted drive that is locally accessible.

Procedure

1. Log on to Linux on the Single EP server.
   - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.
   - Otherwise, log on remotely as a non-root user, and then change the user to root by entering the `su - root` command.
2. Navigate to `$AVAYA_HOME/Support/Security-Tools` directory.
3. Enter the **`bash SetupServerCertificate.sh -import`** command.

   The system displays a message indicating that the services will be restarted and asks whether the user wants to proceed.

   The following is a sample message:

   ```
   This utility will configure the Experience Portal certificate.
   During this process, the following services will be restarted if they are
   configured:
   - epmcompmgr
   - vpms
   - mmsserver
   - avpSNMPAgentSvc
   - httpd
   - mpp
   Do you wish to proceed? [Y/n]
   ```

   Note:

   If any service is not configured or not running on the server while the script is running, the script will not restart these services after a new certificate is installed.
4. Enter `Y` to proceed.

   The script then prompts you to enter the file path and the name of the security certificate.
5. Type the file path and name of the security certificate, and press `Enter`.
6. At the prompt, type the password for the security certificate, and press `Enter`.

   The system displays the imported certificate content.
7. Enter one of the following:
   - `Y` to accept the imported certificate.
   - `n` to cancel.

   The script restarts all related services and displays a message indicating a new server certificate is installed successfully.
8. Enter the **`bash SetupServerCertificate.sh -display`** command to verify the contents of the newly imported server certificate.

9. Do the following to accept the new certificate on the MPP:
    a. Log in to the console as a `root` user.
    b. Navigate to the `$AVAYA_HOME/Support/VP-Tools` directory.
    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.

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

Third-party signed security certificates

Use this section to install a third-party signed security certificate, which replaces the certificate signed by the EPM Root certificate on each server. Experience Portal uses these certificates for mutual authentication with external servers such as SIP proxies and application servers. For email, HTML, and SMS applications, Primary and Auxiliary EPMs can mutually authenticate with applications servers. For voice applications, MPPs can mutually authenticate with application servers, speech servers, and telephony servers.

You must perform the installation procedures on each server to replace the security certificates signed by the EPM Root certificate.

Related links

Importing a Primary EPM Third-Party Signed Security Certificate on page 66
Importing an Auxiliary EPM Third-Party Signed Security Certificate on page 68
Importing a MPP Third-Party Signed Security Certificate on page 70
Importing a Single server Third-Party Signed Security Certificate on page 72

Importing a Primary EPM Third-Party Signed Security Certificate

Before you begin

- Ensure that signing is disabled for the EPM Root certificate. (Select Disable Signing on the EPM Certificates page).
- Ensure that the Primary EPM server is not processing any multi-channel messages such as Emails, SMS or HTML.
- If a managed application is installed, you might need to perform additional steps before and after the server certificate is updated. For more information, see the documentation of the managed application.
- In Avaya Aura® Experience Portal 7.2, a new script ImportExternalServerCertificate.sh has replaced the old script ImportServerCertificate.sh.

About this task

Use the ImportExternalServerCertificate.sh script to import a self-signed or third party signed certificate which will replace the certificate signed by the EPM Root certificate.

Procedure

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

   - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.

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

2. Navigate to `$AVAYA_HOME/Support/Security-Tools` directory.

3. Enter the `bash ImportExternalServerCertificate.sh` command.

   The system prompts a message indicating the services will be restarted and asks if the user wants to proceed.

   The following shows a sample message:

   ```
   This utility will replace the certificate signed by the EPM Root certificate on
   the Experience Portal server.
   Use this script to replace the certificates used for secure external server
   communication when the EPM Root Certificate Disable Signing is in effect.
   When EPM Root Certificate Disable Signing is in effect, the EPM Root Certificate
   is removed.
   During this process, the following services will be restarted if they are
   configured:
   - epmcompmgr
   - vpms
   - mmsserver
   - avpSNMPAgentSvc
   - appserver
   - httpd
   - mpp
   Do you wish to proceed? [Y/n]
   ```

   Note:

   If any service is not configured or is not running on the server while the script is run, it will not be restarted by the script after a new certificate is installed.

4. Enter `Y` to proceed.

   The script then prompts you to enter the file path and the name of the security certificate.

5. Type the file path and name of the security certificate, and press `Enter`.

   Note:

   - The certificate is in PKCS12 format. The certificate must be formatted as PKCS#12 file. A PKCS#12 file includes a certificate and the corresponding key. The certificate is encrypted and requires a password. If the certificate is not self-signed, then the PKCS#12 file must include all CA certificates.

   - If the **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication`, also called as serverAuth, and `Client Authentication`, also called as clientAuth, for the usage.

    - The certificate should have a valid Common Name that represents the EP server host name. If the Subject Alternate Name is specified in the X509 V3 certificate extension, it should contain valid DNS and IP Address entries that are associated with the EP server host name.
    - The certificate resides on the local server or on an NFS-mounted drive that is locally accessible.

   The system prompts you to enter the password for the security certificate.

6. Type the password for the security certificate, and press `Enter`.

   The system displays the imported certificate content.

7. Enter `Y` to accept the imported certificate or enter `n` to cancel.

   The script restarts all related services and displays a message indicating a new External Server certificate is installed successfully.

Related links

Third-party signed security certificates on page 66

Importing an Auxiliary EPM Third-Party Signed Security Certificate

Before you begin

- Ensure that signing is disabled for the EPM Root certificate. (Select Disable Signing on the EPM Certificates page.)
- Ensure that the Auxiliary EPM server is not processing any multi-channel messages such as Emails, SMS, or HTML.
- Ensure that the task Importing a Primary EPM Third-Party Signed Security Certificate has completed successfully.
- If a managed application is installed, you might need to perform additional steps before and after the server certificate is updated. For more information, see the documentation of the managed application.
- In Avaya Aura® Experience Portal 7.2, a new script ImportExternalServerCertificate.sh has replaced the old script ImportServerCertificate.sh.

About this task

Use the ImportExternalServerCertificate.sh script to import a self-signed or third party certificate to replace the certificate signed by the EPM Root certificate.

Procedure

1. Log in to Linux on the Auxiliary EPM server.
    - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.
    - Otherwise, log on remotely as a non-root user, and then change the user to root by entering the `su - root` command.

2. Navigate to `$AVAYA_HOME/Support/Security-Tools` directory.
3. Enter the `bash ImportExternalServerCertificate.sh` command.

   The system prompts a message indicating the services will be restarted and asks if the user wants to proceed.

   The following shows a sample message:

   ```
   This utility will replace the certificate signed by the EPM Root certificate on
   the Experience Portal server.
   Use this script to replace the certificates used for secure external server
   communication when the EPM Root Certificate Disable Signing is in effect.
   When EPM Root Certificate Disable Signing is in effect, the EPM Root Certificate
   is removed.
   During this process, the following services will be restarted if they are
   configured:
   - epmcompmgr
   - vpms
   - mmsserver
   - avpSNMPAgentSvc
   - appserver
   - httpd
   - mpp
   Do you wish to proceed? [Y/n]
   ```

   Note:

   If any service is not configured or is not running on the server while the script is run, it will not be restarted by the script after a new certificate is installed.

4. Enter `Y` to proceed.

   The script then prompts you to enter the file path and the name of the security certificate.

5. Type the file path and name of the security certificate, and press `Enter`.

   Note:

   - The certificate is in PKCS12 format. The certificate must be formatted as PKCS#12 file. A PKCS#12 file includes a certificate and the corresponding key. The certificate is encrypted and requires a password. If the certificate is not self-signed, then the PKCS#12 file must include all CA certificates.
   - If the **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication`, also called as serverAuth, and `Client Authentication`, also called as clientAuth, for the usage.
   - The certificate should have a valid Common Name that represents the EP server host name. If the Subject Alternate Name is specified in the X509 V3 certificate extension, it should contain valid DNS and IP Address entries that are associated with the EP server host name.
   - The certificate resides on the local server or on an NFS-mounted drive that is locally accessible.

   The system prompts you to enter the password for the security certificate.

6. Type the password for the security certificate, and press `Enter`.

The system displays the imported certificate content.

7. Enter `Y` to accept the imported certificate or enter `n` to cancel.

   The script restarts all related services and displays a message indicating a new External Server certificate is installed successfully.

Related links

Third-party signed security certificates on page 66

Importing a MPP Third-Party Signed Security Certificate

Before you begin

- Ensure that the MPP server is not handling any calls.
- Ensure that signing is disabled for the EPM Root certificate. (Select Disable Signing on the EPM Certificates page).
- Ensure the task Importing a Primary EPM Third-Party Signed Security Certificate has completed successfully
- If there is an Auxiliary EPM in the Experience Portal system, make sure the task Importing an Auxiliary EPM Third-Party Signed Security Certificate has completed successfully.
- If a managed application is installed, you might need to perform additional steps before and after the server certificate is updated. For more information, see the documentation of the managed application.
- In Avaya Aura® Experience Portal 7.2, a new script ImportExternalServerCertificate.sh has replaced the old script ImportServerCertificate.sh.

About this task

Use the ImportExternalServerCertificate.sh script to import a self-signed or third party certificate to replace the certificate signed by the EPM Root certificate:

Procedure

1. Log in to Linux on the MPP server.
   - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.
   - Otherwise, log on remotely as a non-root user, and then change the user to root by entering the `su - root` command.
2. Navigate to `$AVAYA_HOME/Support/Security-Tools` directory.
3. Enter the `bash ImportExternalServerCertificate.sh` command.

   The system prompts a message indicating the services will be restarted and asks if the user wants to proceed.

   The following shows a sample message:

```
This utility will replace the certificate signed by the EPM Root certificate on
the Experience Portal server.
Use this script to replace the certificates used for secure external server
```

```
communication when the EPM Root Certificate Disable Signing is in effect.
When EPM Root Certificate Disable Signing is in effect, the EPM Root Certificate
is removed.
During this process, the following services will be restarted if they are
configured:
- epmcompmgr
- vpms
- mmsserver
- avpSNMPAgentSvc
- appserver
- httpd
- mpp
Do you wish to proceed? [Y/n]
```

Note:

If any service is not configured or is not running on the server while the script is run, it will not be restarted by the script after a new certificate is installed.

4. Enter `Y` to proceed.

   The script then prompts you to enter the file path and the name of the security certificate.

5. Type the file path and name of the security certificate, and press `Enter`.

   Note:

   - The certificate is in PKCS12 format. The certificate must be formatted as PKCS#12 file. A PKCS#12 file includes a certificate and the corresponding key. The certificate is encrypted and requires a password. If the certificate is not self-signed, then the PKCS#12 file must include all CA certificates.
   - If the **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication`, also called as serverAuth, and `Client Authentication`, also called as clientAuth, for the usage.
   - The certificate should have a valid Common Name that represents the EP server host name. If the Subject Alternate Name is specified in the X509 V3 certificate extension, it should contain valid DNS and IP Address entries that are associated with the EP server host name.
   - The certificate resides on the local server or on an NFS-mounted drive that is locally accessible.

   The system prompts you to enter the password for the security certificate.

6. Type the password for the security certificate, and press `Enter`.

   The system displays the imported certificate content.

7. Enter `Y` to accept the imported certificate or enter `n` to cancel.

   The script restarts all related services and displays a message indicating a new External Server certificate is installed successfully.

Related links

Third-party signed security certificates on page 66

Importing a Single server Third-Party Signed Security Certificate

Before you begin

- Ensure that the Single EPM server is not processing any multi-channel messages such as Emails, SMS or HTML.
- Ensure that the MPP is not processing any traffic.
- Ensure that signing is disabled for the EPM Root certificate. (Select Disable Signing on the EPM Certificates page.)
- If a managed application is installed, you might need to perform additional steps before and after the server certificate is updated. For more information, see the documentation of the managed application.
- In Avaya Aura® Experience Portal 7.2, a new script ImportExternalServerCertificate.sh has replaced the old script ImportServerCertificate.sh.

About this task

Use the ImportExternalServerCertificate.sh script to import a self-signed or third party certificate to replace the certificate signed by the EPM Root certificate.

Procedure

1. Log in to Linux on the Single EPM server.
    - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.
    - Otherwise, log on remotely as a non-root user, and then change the user to root by entering the `su - root` command.
2. Navigate to `$AVAYA_HOME/Support/Security-Tools` directory.
3. Enter the `bash ImportExternalServerCertificate.sh` command.

    The system prompts a message indicating that the services will be restarted and asks if the user wants to proceed.

    The following shows a sample message:

    ```
    This utility will replace the certificate signed by the EPM Root certificate on
    the Experience Portal server.
    Use this script to replace the certificates used for secure external server
    communication when the EPM Root Certificate Disable Signing is in effect.
    When EPM Root Certificate Disable Signing is in effect, the EPM Root Certificate
    is removed.
    During this process, the following services will be restarted if they are
    configured:
    - epmcompmgr
    - vpms
    - mmsserver
    - avpSNMPAgentSvc
    - appserver
    - httpd
    - mpp
    Do you wish to proceed? [Y/n]
    ```

Note:

If any service is not configured or is not running on the server while the script is run, it will not be restarted by the script after a new certificate is installed.

4. Enter `Y` to proceed.

   The script then prompts you to enter the file path and the name of the security certificate.

5. Type the file path and name of the security certificate, and press `Enter`.

   Note:

   - The certificate is in PKCS12 format. The certificate must be formatted as PKCS#12 file. A PKCS#12 file includes a certificate and the corresponding key. The certificate is encrypted and requires a password. If the certificate is not self-signed, then the PKCS#12 file must include all CA certificates.
   - If the **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication`, also called as serverAuth, and `Client Authentication`, also called as clientAuth, for the usage.
   - The certificate should have a valid Common Name that represents the EP server host name. If the Subject Alternate Name is specified in the X509 V3 certificate extension, it should contain valid DNS and IP Address entries that are associated with the EP server host name.
   - The certificate resides on the local server or on an NFS-mounted drive that is locally accessible.

   The system prompts you to enter the password for the security certificate.

6. Type the password for the security certificate, and press `Enter`.

   The system displays the imported certificate content.

7. Enter `Y` to accept the imported certificate or enter `n` to cancel.

   The script restarts all related services and displays a message indicating a new External Server certificate is installed successfully.

Related links

Third-party signed security certificates on page 66

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 Avaya Enterprise Linux, the Avaya Service accounts will not be available after the Avaya Enterprise Linux upgrade. The Avaya Service accounts will be available through EASG configuration during the Experience Portal upgrade.

   - Log on to the local Linux console as root.
   - Or log on remotely as a non-root user and then change the user to root by entering the `su - root` command.
2. Navigate to the `Support/Security-Tools` directory by running the `cd $AVAYA_HOME/Support/Security-Tools` command.
3. Enter `./SetDbPassword.sh add_primary_vpcommon`.

   The system prompts you to enter a password.
4. Enter a new password that you want to use for the vpcommon user account.

   The script prompts if you want to restart the services. If you select Y then the script will restart them automatically.

Next steps

1. Configure the vpcommon PostgreSQL database user account on the auxiliary EPM server.
2. 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/Security-Tools` directory by entering the `cd $AVAYA_HOME/Support/Security-Tools` command.
3. Enter the `./SetDbPassword.sh update_primary_vpcommon` command to update the vpcommon user account.

   The system prompts you to enter the password that you have assigned to the vpcommon user account on the primary EPM server.
4. Enter the vpcommon password.

The script now prompts if you want to restart the services, if you select Y then the script will restart them automatically.

5. Restart the PostgreSQL service by entering the `service postgresql restart` command.
6. Restart the vpms service by entering the `service vpms restart` command.
7. Restart the mmsserver service by entering the `service mmsserver restart` command.

Next steps

Add the auxiliary EPM server to Experience Portal Manager.

Related links

Configuring the primary EPM server to support one or more auxiliary EPM servers on page 73

Changing the time zone on Avaya Linux

About this task

Use this procedure to change the time zone on the EPM or VPMS server.

Procedure

1. Log in to the Avaya Linux server.
2. Change to the `root` user account. For example, run this command: **`su root`**.
3. Navigate to the `/usr/share/zoneinfo/` directory on Avaya Linux and locate the time zone that you want to configure.

   The directory structure contains the names and time zones for different regions of the world. For example, the `/usr/share/zoneinfo/Europe` directory contains a Dublin time zone file with a time zone value: "`Europe/Dublin`".
4. If the virtual machine BIOS has the Universal Time Coordinated (UTC) set as `true`, enable UTC while setting the timezone on Avaya Linux. The UTC in the Linux configuration file must match the BIOS settings.

   Validate if the system BIOS or Hardware clock is using UTC time by running this command: **`hwclock --debug`**.

   If UTC is enabled, you will see this line:

   ```
   Hardware clock is on UTC time
   ```
5. Create a backup copy of the `/etc/sysconfig/clock` file.

   For example, to create a backup copy called `clockORIG`, run the command:

   ```
   cp -p /etc/sysconfig/clock /etc/sysconfig/clockORIG
   ```

6. Using the `root` user account, 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.

   For example, run the following commands to change to the Dublin time zone:

   `ZONE=”Europe/Dublin”`

   `UTC=true`
7. Save the changes in the updated `/etc/sysconfig/clock` file.
8. Update the time zone data on the system by running this command: **`tzdata-update`**
9. If the system is an EPM, restart the vpms service by running this command: **`/sbin/service vpms restart`**
10. Log on to the Avaya Aura® Experience Portal web console and navigate to **Home** > **System Configuration** > **Zones**.
11. Click **Default** and select the new time zone from the list.

    For example, select **(GMT+00:00) Europe/Dublin** from the list.
12. Click **Apply** and then click **Save**.

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 **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 **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. 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. If you run the test application as a VoiceXML 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 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 links

Test Application result for Call Classification option on page 80
Test Application result for Call Conferencing option on page 81
Test Application result for Call Merge option on page 81

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

Related links

Running the sample application on page 79

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, enter 9 with the phone number. Otherwise, the call fails.

Related links

Running the sample application on page 79

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. This option is not supported for H.323.

Related links

Running the sample application on page 79

Configure and run the Application Interface test client

Use the Application Interface test client to validate the Application Interface web service and the Experience Portal outcall functionality. The Application Interface test client is available in `$AVAYA_HOME/Support/OutCallTest/VPAppIntfClient`.

Related links

Configuring Experience Portal for outcall on page 82

Running the Application Interface test client VPApplntfClient.sh on page 82

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 VXML and 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. The VPAppIntfService Web service version authenticates users that are configured as Experience Portal users. The user must have the Web Services role.

Related links

Configure and run the Application Interface test client on page 81

Running the Application Interface test client VPApplntfClient.sh

Before you begin

Ensure that you configure Experience Portal for the Application Interface test client as described in Configuring Experience Portal for outcall on page 82.

Procedure

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

   If you are an Avaya Services representative, and use Avaya Enterprise Linux, the Avaya Service accounts will not be available after the Avaya Enterprise Linux upgrade. The Avaya Service accounts will be available through EASG configuration during the Experience Portal upgrade.

   - Log on to the local Linux console as root.
   - Or log on remotely as a non-root user and then change the user to root by entering the `su - root` command.
2. Navigate to the Application Interface test client directory by entering the `cd $AVAYA_HOME/Support/OutCallTest/VPAppIntfClient` command.

3. Use the following examples to show calling Application Interface test client using different authentication schemes:

   a. Password Authentication

      Enter the `./VPAppIntfClient.sh —n <outcall-username> —p <outcall password>` command to request the number of available outbound ports.

      - <outcall-username> is an Experience Portal user configured on the Users page of the EPM web interface..
      - <outcall password> is the password for <outcall-username> that is configured on the Users page of the EPM web interface.

      Note:

      The user must have the Web Services user role.

   b. Certificate Authentication

      Enter the `./VPAppIntfClient.sh -y certificate -k <Java Keystore> —o <Java Keystore password>` command to request the number of available outbound ports.

      - -y: <certificate> the authentication type is certificate.
      - -k: <Java Keystore> the Java keystore file name including the path. The Java keystore should contain the User identity certificate including the private key.
      - -o: <Java Keystore password> the password for the Java keystore file.

      Note:

      Import the User identity certificate to the EPM and ensure that the certificate is assigned to a user of Certificate type.

      The user must have the Web Services user role.

   c. Password and Certificate Authentication

      Enter the `./VPAppIntfClient.sh -n <outcall-username> -p <outcall password> -y password+certificate -k <Java Keystore> —o <Java Keystore password>` command to request the number of available outbound ports.

      - <outcall-username> is an Experience Portaluser configured on the Users page of the EPM web interface..
      - <outcall password> is the password for <outcall-username> that is configured on the Users page of the EPM web interface..
      - -y: <password+certificate> the authentication type is password and certificate.
      - -k: <Java Keystore> the Java keystore file name including the path. The Java keystore should contain the User identity certificate including the private key.
      - -o: <Java Keystore password> the password for the Java keystore file.

Note:

Import the User identity certificate to the EPM and ensure that the certificate is assigned to the <outcall-username> and the user authentication type is Password and Certificate.

The user must have the Web Services user role.

4. Verify that the Application Interface test client displays a response that shows the total ports and unused ports available for outcalls.

   For example:

   Mon Jun 03 16:55:26 PDT 2017:VPAppIntfServiceClient: queryResources succeeded, Total Resources = 0, Unused H323 = 0, Unused SIP = 0

   Mon Jun 03 16:55:26 PDT 2017: VPAppIntfServiceClient: exiting

5. Use the following examples to show calling Application Interface test client using different authentication schemes.

   Password Authentication

   a. Enter the `./VPAppIntfClient.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 Experience Portal username configured with the Web Services role on the Users page of the EPM web interface..
      - <outcall password> is the password assigned to the outcall-username above that was configured on the Users page of the EPM web interface.

      Note:

      The user must have the Web Services user role.

      Certificate Authentication

   b. Enter the `./VPAppIntfClient.sh -R 1 -A <application-name> -T <number-to-dial> -y certificate -k <Java Keystore> —o <Java Keystore 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.
      - -y: <certificate> the authentication type is certificate.
      - -k: <Java Keystore> the Java keystore file name including the path. The Java keystore should contain the User identity certificate including the private key.

- -o: <Java Keystore password> the password for the Java keystore file.

Note:

Import the User identity certificate to the EPM and ensure that the certificate is assigned to the user of Certificate type.

The user must have the Web Services user role.

Password and Certificate Authentication

c. Enter the `./VPAppIntfClient.sh -R 1 -A <application-name> -T <number-to-dial> -n <outcall-username> -p <outcall password> -y password+certificate -k <Java Keystore> —o <Java Keystore password>`command to initiate an outcall and launch a VoiceXML application, where:

- <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 Experience Portal user name configured from EPM Web interface.
- <outcall password> is the password for <outcall-username> that is configured from the EPM Web interface.
- -y: <password+certificate> the authentication type is password + certificate.
- -k: <Java Keystore> the Java keystore file name including the path. The Java keystore should contain the User identity certificate including the private key.
- -o: <Java Keystore password> the password for the Java keystore file.

Note:

Import the User identity certificate to the EPM, ensure that the certificate is assigned <outcall-username>, and the user authentication type is **Password and Certificate**.

The user must have the Web Services user role.

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 Application Interface test client 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:

```
Mon Jun 03 17:00:31 PDT 2017: VPAppIntfServiceClient: launchVXML succeeded, SessionID = scaaep134-2013155001030-5, TotalRes = 100, UnusedH323 = 0, UnusedSIP = 99

Mon Jun 03 17:00:31 PDT 2017: VPAppIntfServiceClient: exiting
```

Related links

Configure and run the Application Interface test client on page 81

Chapter 7: Upgrading Experience Portal

Upgrade overview

This chapter describes the procedures to upgrade Experience Portal in the virtualized environment. To upgrade existing Experience Portal OVA-based systems to Experience Portal 7.2, you can do one of the following:

- Deploy new virtual machines and restore the existing data. This is the traditional upgrade method and described in detail in this chapter.
- Perform an in-place upgrade of the Experience Portal software. This method is described in *Upgrading to Avaya Aura Experience Portal.*

The in-place upgrade procedure is similar to the upgrade of physical bundled systems. It uses the `vpupgrade.sh` script to upgrade Avaya Linux, if applicable, and the autoupgradevp script to upgrade Experience Portal.Avaya Linux is upgraded during the in-place upgrade. The VMware tools will also be automatically updated to VMwareTools-10.0.0-3000743.

Note:

The VM properties in the VMWare Client VM Summary tab are set during the OVA build. The system will not update these properties, if you perform the upgrade using the ISO image or the Experience Portal media. You must get the Experience Portal version either by using the **`iaversion.php`** or through Experience Portal Manager.

Upgrading Primary EPM

Before you begin

If you have a new license file, upgrade the license.

Procedure

1. Create a backup of the Experience Portal system by using the System Backup Web page in EPM. .

   For more information about backing up an Experience Portal system from the **System Backup** menu in EPM, see *Administering Avaya Aura® Experience Portal*.

   Before you proceed, take the backup of the virtual machine.

2. Shut down the Experience Portal virtual machine.

   Note:

   If you want to restore the Experience Portal virtual machine later, you do not need to delete the virtual machine. Keeping the virtual machine in its shut-down state enables you to restore the machine if required.

3. Deploy the new Primary EPM OVA on a new virtual machine.

   Important:

   During the deployment process, give the new Experience Portal virtual machine the same network configuration, including IP address and hostname, as the old virtual machine.

4. Create the vpcommon user account.

   The OVA deployment does not create the vpcommon user. Therefore, you must manually create this user after deploying the Primary EPM OVA. For more information about creating the vpcommon user, see Configuring Primary EPM server to support one or more Auxiliary EPM servers on page 73.

   Important:

   When creating the vpcommon user, use a password that is different from the one that is used on the server from which the backup, in step 1, is created. If you use the same password that is used during the backup, the restore that is required in the next step might fail.

5. Restore the backup on the new Experience Portal virtual machine using command line interface.

   For more information about restoring data backed up from the **System Backup** menu in EPM, see *Administering Avaya Aura® Experience Portal*

6. Restart the new Experience Portal virtual machine.

7. Reconfigure the Avaya Service accounts.

   For more information about re-configuring the Avaya Service accounts, see *Upgrading to Avaya Aura® Experience Portal 7.2*.

8. Run the **`setup_vpms.php`** command on the MPP server to authorize the security certificate so that the MPPs running on a previous version are functional with the upgraded EPM.

9. Trust the new security certificate for the MPP from the **System Configuration** > **MPP Servers** > **Change MPP Server** page.

10. Repeat steps 2 and 3 for each additional MPP in the system.

    On upgrading the Primary EPM OVA, the co-resident MPP resets to the disabled state. You must re-enable the co-resident MPP.

For procedure to re-enable the co-resident MPP, see Enabling the co-resident MPP. on page 31

For more information about reconfiguring the Avaya Service accounts, see *Upgrading to Avaya Aura® Experience Portal 7.2*.

Upgrading Auxiliary EPM

Procedure

1. Shut down the Auxiliary EPM virtual machine.
2. Deploy the Auxiliary EPM OVA on a new virtual machine.

   Important:

   During the deployment process, give the new Experience Portal virtual machine the same network configuration, including IP address and hostname, as the old virtual machine.
3. Configure the password of the vpcommon user that you created during the Primary EPM upgrade.

   For more information about configuring the `vpcommon` password, see Configuring password for database user vpcommon on an auxiliary EPM on page 74.
4. Log on to the EPM Web interface.
5. To trust the new security certificate for the Auxiliary, click **System Configuration** > **EPM Servers** > **Change EPM Server**.

Next steps

(Optional) Delete the old Auxiliary EPM VM once you confirm the new Auxiliary EPM to be working and functional.

Upgrading MPP

Before you begin

If your system has more than one MPP, you can upgrade one MPP at a time to allow the other MPPs to function with the upgraded EPM.

Procedure

1. Log on to the EPM Web interface.
2. To stop the MPP server, click **System Management** > **MPP Manager**.

3. Schedule a report data download from the Report Data pagepage in EPM so that EPM collects the calls records from the MPP servers.
4. When the report download is complete, click **System Management** > **MPP Manager** .
5. When the MPP is offline, shut down the MPP virtual machine.
6. Deploy the MPP OVA on a new virtual machine.

   Important:

   During the deployment process, give the new Experience Portal virtual machine the same network configuration, including IP address and hostname, as the old virtual machine.
7. Log on to the EPM Web interface.
8. To trust the new security certificate for the MPP, click **System Configuration** > **MPP Servers** > **Change MPP Server** .
9. To change the MPP status to the online mode, click **System Management** > **MPP Manager** .
10. To start the MPP server, click **System Management** > **MPP Manager** .

Next steps

(Optional) Delete the MPP once you confirm the new MPP to be working and functional.

Chapter 8: 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 Red Hat 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 Red Hat 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 Red Hat crash utility, see White paper: Red Hat Crash Utility.

Note:

When you run the vmss2core tool as the sroot user, ignore the "**you are not root**" message.

IP address fields clipped when deploying via vCenter

When you deploy the Experience Portal OVA via vCenter, the installer displays a Properties window where you have to enter the Linux network and Experience Portal specific parameters. Several of the fields on the Properties window accept input in the IP address format. On some systems, the vSphere Client program might clip the IP address fields so that only the first three octets of the address are visible. You might have to scroll the Properties window to see the fourth octet of the IP address.

System prompt to configure Experience Portal after deploying OVA with vCenter

When you deploy the Experience Portal OVA with vCenter, the vSphere Client OVF deployment wizard prompts you to enter the configuration values. The values are applied to the virtual machine only after you boot the virtual machine for the first time. It can take several minutes during the initial boot for the configuration process to complete. During the configuration process, if you log in to Linux remotely, the system might display a message stating that Experience Portal has not been configured. If the system prompts you to configure Experience Portal, do the following:

1. Respond with a `no` to the system prompt.
2. Log out of the remote Linux session.
3. After the boot process is complete, log in to Linux through the console.
4. Verify that the system does not display deployment errors on the console.

After the Experience Portal configuration process is complete on the virtual machine, the system does not prompt you to configure Experience Portal when you log in to Linux remotely.

ProductID must be configured for the VM to power on

If you enter an invalid or blank Product ID during the Primary EPM OVA deployment, the system displays an error message when the virtual machine is powered on. The error message is a follows:

```
Property 'ProductID' must be configured for the VM to power on
```

To correct the error, perform the following steps:

1. Log into vSphere Client.
2. Right-click on the virtual machine being deployed, and select the **Edit Settings** option.
3. Select the **Options** tab.
4. Select **vApp Options** > **Properties**.

   The system display the properties specified during the OVA deployment.
5. Enter the correct information in the **Product ID** field.
6. Click **OK** to save the changes.
7. Power on the virtual machine.

Chapter 9: Resources

Documentation

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

Title	Description	Audience
Avaya Aura® Experience Portal Documentation Roadmap	Lists all the documents related to Experience Portal and describes the organization of content across the documents.	Avaya Professional Services Implementation engineers
Avaya Aura® Experience Portal Overview and Specification	Describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Implementation engineers
Implementing Avaya Aura® Experience Portal on a single server	Provides procedures to install and configure the Avaya Aura® Experience Portal software on a single server.	Implementation engineers
Implementing Avaya Aura® Experience Portal on multiple servers	Provides procedures to install and configure Avaya Aura® Experience Portal software on two or more dedicated servers.	Implementation engineers
Upgrading to Avaya Aura® Experience Portal 7.2	Describes how to upgrade your Avaya Aura® Experience Portal 7.1 to 7.2.	Implementation engineers
Administering Avaya Aura® Experience Portal	Provides general information about and procedures for administering and configuring specific Experience Portal functions and features using a web-based interface.	Implementation engineers

Table continues…

Title	Description	Audience
Troubleshooting Avaya Aura® Experience Portal	Provides general information about troubleshooting and resolving system problems. This document also provides detailed information and procedures for finding and resolving specific problems.	Implementation engineers
Avaya Aura® Experience Portal Security White Paper	Provides information about the security strategy for Experience Portal, and provides suggestions that companies can use to improve the security of the Experience Portal systems and applications.	Avaya Professional Services Implementation engineers
Avaya Aura® Experience Portal 7.2 Mobile Web Best Practices White Paper	Provides recommended strategies for deploying Avaya Aura® Orchestration Designer Mobile Web applications with Avaya Aura® Experience Portal 7.2, detailing configuration for security, scalability and high availability.	Avaya Professional Services Implementation engineers
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 7.2 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

Related links

Finding documents on the Avaya Support website on page 96

Avaya Documentation Portal navigation on page 96

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Related links

Documentation on page 94

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

Navigate to the **My Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.

- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **My Content** > **Watch list** menu, and do the following:

  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Related links

Documentation on page 94

Training

The following courses are available on the Avaya Learning website at http://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	

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

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*.

Related links

Performance Monitor on page 99
vMotion: Host migration and storage vMotion on page 100
High Availability on page 100
VM Snapshots on page 101
Fault Tolerance on page 101

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:

- Performance Monitoring Utilities: resxtop and esxtop: http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.monitoring.doc%2FGUID-A31249BF-B5DC-455B-AFC7-7D0BBD6E37B6.html
- Interpreting esxtop Statistics: http://communities.vmware.com/docs/DOC-9279

Related links

Experience Portal specific best practices for VMware features on page 99

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.

Related links

Experience Portal specific best practices for VMware features on page 99

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.

Related links

Experience Portal specific best practices for VMware features on page 99

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.

Related links

Experience Portal specific best practices for VMware features on page 99

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.

Related links

Experience Portal specific best practices for VMware features on page 99

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 Client

The vSphere 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