Upgrading to Avaya Experience Portal 8.1

Release 8.1.2.1
Issue 1
March 2024

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

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

Contents

Chapter 1: Introduction 7
Purpose 7
Chapter 2: Avaya Experience Portal system upgrade overview 8
System upgrade overview 8
Upgrading a system that uses Avaya Enterprise Linux 9
Upgrading the Primary EPM on Avaya Enterprise Linux 9
Upgrading an Auxiliary EPM on Avaya Enterprise Linux 10
Upgrading a Media Processing Platform (MPP) on Avaya Enterprise Linux 10
Upgrading a single server Experience Portal system on Avaya Enterprise Linux 11
Upgrading a system that uses Red Hat Enterprise Linux Server 12
Upgrading the Primary EPM on Red Hat Enterprise Linux Server 12
Upgrading an Auxiliary EPM on Red Hat Enterprise Linux Server 14
Upgrading a Media Processing Platform (MPP) on Red Hat Enterprise Linux Server 16
Upgrading the single server Experience Portal system on Red Hat Enterprise Linux Server 17
Chapter 3: Upgrading the operating system 20
Operating system upgrade overview 20
Default Red Hat umask 22
Platform Vendor Independent Check 22
High level packages required for the installation of Experience Portal 8.1 23
Backing up data 25
Staging the Experience Portal 6.x or 7.x backup files on the Primary EPM before upgrading Experience Portal 27
Preparing to connect to Avaya Enterprise Linux using an Ethernet cable 28
Upgrading Avaya Enterprise Linux using an ISO image file 29
Upgrading Avaya Enterprise Linux from the software installation DVD 32
State of identity variables in Master Software Image and on first boot 35
Upgrading Red Hat Enterprise Linux Server on the dedicated EPM server 36
Upgrading Red Hat Enterprise Linux Server on a dedicated MPP server 38
Upgrading Red Hat Enterprise Linux Server on a single server system 39
Taking an MPP offline using the EPM web interface 42
Stopping the MPP service 42
Preventing loss of reporting data prior to upgrading MPP 43
Chapter 4: Software upgrade prerequisites 44
Prerequisites checklist for upgrading Experience Portal 44
Minimum server hardware requirements 47
Disk space requirements 47
Space requirement for upgrading the primary EPM on Red Hat Enterprise Linux 47
Space requirement for upgrading the primary EPM on Avaya Enterprise Linux 48
License Requirements 49

Verifying the Linux version number ... 50
Verifying communication between the upgraded Experience Portal servers ... 51
Ensuring new SMS and Email records are created after upgrades ... 53
Checking for stale or hung mount points ... 54
Verifying server time synchronization ... 55
Updating the external database configuration ... 56
Installing the Oracle JDBC driver ... 57
Chapter 5: Upgrading the EPM and MPP software on different servers ... 59
Upgrading the Primary EPM server ... 59
EPM software upgrade overview ... 59
Upgrading the Primary EPM software interactively ... 59
Copying and restoring the backup files ... 64
Upgrading an Auxiliary EPM server ... 65
Auxiliary EPM software upgrade overview ... 65
Upgrading the Auxiliary Experience Portal software interactively ... 66
Upgrading the MPP software ... 70
MPP software upgrade overview ... 70
Upgrading the MPP software interactively ... 71
Reestablishing the link between the EPM and the upgraded MPP ... 74
Chapter 6: Upgrading the Experience Portal software on a single server ... 75
Experience Portal software upgrade on a single server overview ... 75
Upgrading the Experience Portal software interactively on a single server ... 75
Reestablishing the link between the EPM and the MPP ... 79
Chapter 7: Optional: Updating the co-resident application server ... 81
Optional: Updating the co-resident application server ... 81
Chapter 8: Configuring and testing an upgraded Avaya Experience Portal system ... 84
Avaya Experience Portal system configuration checklist for a system upgraded to 8.1 ... 84
Upgrading the Experience Portal license ... 85
Running the sample application ... 87
Configure and run the Application Interface test client ... 88
Configuring Experience Portal for outcall ... 88
Running the Application Interface test client VPAppIntfClient.sh ... 88
Testing an individual MPP ... 92
External time sources ... 93
Configuring the Primary EPM server to point to an external time source ... 94
Enabling FIPS ... 95
Importing server identity certificates ... 96
Non-English language support ... 96
Non-English character support on the EPM web pages ... 96
Chapter 9: Troubleshooting upgrade issues ... 101
Upgrade installation log files ... 101
Primary EPM root certificate is signed with a weak hashing algorithm warning ... 102
Changing the Product ID for an existing Experience Portal system ... 102

Invalid password for database user 103
Time synchronization problems 103
Reloading the Experience Portal environment variables 103
Recovering Avaya Enterprise Linux configuration information after an upgrade 104
Restoring the previous operating system after an upgrade 104
Checklist for restoring the software on Avaya Enterprise Linux 104
Restoring the software on a dedicated Primary EPM server or a single-server EPM system running Red Hat Enterprise Linux Server 109
Restoring the software on an Auxiliary EPM server running Red Hat Enterprise Linux Server 110
Restoring a dedicated MPP server on Red Hat Enterprise Linux Server 110
Chapter 10: Preupgrade worksheets 112
Primary EPM server upgrade worksheet 112
Auxiliary EPM server upgrade worksheet 116
MPP server upgrade worksheet 119
Single EPM server upgrade worksheet 121
Chapter 11: Resources 125
Documentation 125
Finding documents on the Avaya Support website 127
Avaya Documentation Center navigation 128
Viewing Avaya Mentor videos 129
Support 130

Chapter 1: Introduction

Purpose

This document describes how to upgrade to Avaya Experience Portal 8.1.

Anyone who upgrades and configures the Avaya Experience Portal system must read and understand the information in this document.

This document is intended for anyone who is involved with installing, configuring, and upgrading Avaya Experience Portal. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

Chapter 2: Avaya Experience Portal system upgrade overview

System upgrade overview

You can upgrade to Experience Portal 8.1.x from the following versions:

Experience Portal	Note
• **R6.0.3** • **R7.0** • **R7.0.1** • **R7.0.2** • **R7.1** • **R7.2** • **R7.2.3**	For OVA based Experience Portal R6.x or R7.x systems: • You must first upgrade to R8.1.x and then upgrade to R8.1.2.1. • You must apply the AVL patch >= 2402 before upgrading from R8.1.x to R8.1.2.1. • You must deploy fresh Experience Portal R8.1 OVAs because in-place OVA upgrades are not supported.
• **R8.0**	For upgrades from Experience Portal R8.0 to R8.1, in-place upgrades are supported through Avaya Experience Portal ISO.
• **R8.1**	–

Important:

- The upgrade procedure for systems that use Avaya-provided Linux is different from the upgrade procedure for systems that use customer-provided Red Hat Enterprise Linux. For Avaya-provided Linux upgrades, you must download the supported Avaya-provided Linux from the AvayaSupport site.
- Note that as with any upgrade, the OS of the system must meet the requirements of the new version of Experience Portal. If it does not, then the OS must also be upgraded.

Note:

- Experience Portal upgrades or migrations from on-premise deployments to cloud deployments arer not supported in AEP 8.1.

For an Experience Portal system that includes multiple zones, Avaya recommends that you upgrade Experience Portal on a zone by zone basis. That is, you upgrade the servers in one zone before upgrading the servers in a different zone. Once the zone is fully upgraded, the zone is

fully operational. However, Avaya recommends that once you start upgrading a system, upgrade all zones as soon as possible to avoid any compatibility issues that might occur.

To support an upgrade without service interruption, the system must have more than a single MPP.

- When upgrading with a single MPP, there is service interruption but there no loss of data.
- When upgrading with multiple MPPs:

The following services are not interrupted:	There following services are interrupted:
- Inbound calls - Outbound calls - Inbound email messages - Outbound email messages	- EPM web interface - Report data collection - SNMP Agent - Telephony port reallocation - Inbound SMS messages - Outbound SMS messages

Experience Portal supports upgrades on HP DL 360 G9 and Dell R630 servers that are provided with Experience Portal R6.0, 7.0, 7.1, or 7.2.

For information on Avaya Solutions Platform (ASP) 110 and 130 server support, see the *Avaya Experience Portal Overview and Specification* guide.

Note:

- You must download the Avaya Experience Portal ISO from the Avaya Support site only.

Upgrading a system that uses Avaya Enterprise Linux

Upgrading the Primary EPM on Avaya Enterprise Linux

About this task

This topic provides information about the tasks that you must perform to upgrade the Primary EPM server.

Before you begin

1. If you use an external database for reports, upgrade the external database schema before upgrading theExperience Portal components.

   For more information, see Updating the external database configuration on page 56.

2. Verify that the prerequisites have been met.

   For more information, see Software upgrade prerequisites overview for upgrading to Experience Portal on page 44.

3. Backup the Experience Portal data.

For more information, see Backing up data on page 25.

Note:

You must take a backup of Experience Portal data for both Avaya Enterprise Linux and Red Hat Enterprise Linux upgrades.

4. If Externally Signed Security Certificates are configured in the current Experience Portal solution, ensure the following:
   - The Certificate Authority (CA) trusted certificate is available.
   - The required PKCS#12 (.p12) files for each EPM & MPP server are available and ready for import into their respective servers.
   - The passwords for the supplied .p12 files are known as they will be required when importing into AAEP.

Procedure

1. Upgrade Avaya Enterprise Linux on the Primary EPM server. For more information, see Upgrading Avaya Enterprise Linux from the software installation DVD on page 32 or Upgrading Avaya Enterprise Linux using an ISO image file on page 29.
2. Upgrade the Primary EPM software to Experience Portal 8.1.

   For more information, see Upgrading the Primary EPM server on page 59.

Upgrading an Auxiliary EPM on Avaya Enterprise Linux

About this task

This topic provides information about the tasks that you must perform to upgrade an Auxiliary EPM server.

Before you begin

Verify that the prerequisites have been met. For more information, see Software upgrade prerequisites overview for upgrading to Experience Portal on page 44.

Procedure

1. Upgrade Avaya Enterprise Linux on the Auxiliary EPM server.

   For more information, see Upgrading Avaya Enterprise Linux from the software installation DVD on page 32 or Upgrading Avaya Enterprise Linux using an ISO image file on page 29.
2. Upgrade the Auxiliary Experience Portal system to Experience Portal 8.1.

   For more information, see Upgrading an Auxiliary EPM server on page 65.

Upgrading a Media Processing Platform (MPP) on Avaya Enterprise Linux

About this task

This topic provides information about the tasks that you must perform to upgrade an MPP server.

Before you begin

Verify that the prerequisites have been met. For more information, see Software upgrade prerequisites overview for upgrading to Experience Portal on page 44.

Procedure

1. Change the state of the MPP to offline.

   For more information, see Taking an MPP offline using the EPM web interface on page 42.

2. Upgrade Avaya Enterprise Linux on the MPP server.

   For more information, see Upgrading Avaya Enterprise Linux from the software installation DVD on page 32 or Upgrading Avaya Enterprise Linux using an ISO image file on page 29.

3. Upgrade the MPP to Avaya Experience Portal 8.1.

   For more information, see Upgrading the MPP software on page 70.

4. Log on to the EPM web interface.
5. Navigate to the **MPP Manager** page, and change the mode of the MPP to **Online**.
6. On the **MPP Manager** page, click **Start** to start the MPP server.

Upgrading a single server Experience Portal system on Avaya Enterprise Linux

About this task

This topic provides information about the tasks that you must perform to upgrade a single server Experience Portal system.

Before you begin

Verify that the prerequisites have been met. For more information, see Chapter 6: Upgrading the Experience Portal software on a single server on page 75.

Procedure

1. Change the mode of the MPP server to **Offline**.

   For more information, see Taking an MPP offline using the EPM web interface on page 42.

2. Upgrade Avaya Enterprise Linux on the Experience Portal system.

   For more information, see Upgrading Avaya Enterprise Linux from the software installation DVD on page 32 or Upgrading Avaya Enterprise Linux using an ISO image file on page 29.

3. Upgrade the Experience Portal software to Avaya Experience Portal 8.1.

   For more information, see Experience Portal software upgrade on a single server on page 75.

4. Log on to the EPM web interface.
5. Navigate to the **MPP Manager** page, and change the mode of the MPP to **Online**.
6. On the **MPP Manager** page, click **Start** to start the MPP.

Upgrading a system that uses Red Hat Enterprise Linux Server

Upgrading the Primary EPM on Red Hat Enterprise Linux Server

About this task

Perform the following steps to upgrade the Primary EPM server that uses the customer-provided Red Hat Enterprise Linux Server.

Before you begin

Verify that the prerequisites have been met. For more information, see Prerequisites checklist for upgrading Experience Portal on page 44.

Procedure

1. Create a backup of the Experience Portal system.

   Save the backup folder to an external server that is not part of the Experience Portal system. For more information, see Backing up data on page 25.

   Important:

   Experience Portal currently supports RHEL 7.x 64-bit and RHEL 8.x 64-bit OS versions.

   If you are using RHEL 7.8 64-bit or newer 7.x update, or RHEL 8.2 64-bit or newer update, you do not need to perform an OS upgrade.

2. If you upgrade to Experience Portal 8.1 from Experience Portal 6.x or 7.x, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server.

   For more information, see Upgrading Red Hat Enterprise Linux Server on the dedicated EPM server on page 36.

3. If you upgrade to Experience Portal 8.1 from Experience Portal 6.x or 7.x, you must stage the database backup and configuration files on the fresh installation RHEL server.

   For more information on database backup and configuration files, see Backing up data on page 25.

   a. Rename the `vp_backupaa` backup file to `vp_upgrade.export` and copy the file to `/var/lib/pgsql/vp_upgrade.export`.

b. Copy the `version.xml` file to `/opt/Avaya/InstallAgent/config/version.xml`.

   Create the directory if it does not already exist. For example, `mkdir -p /opt/Avaya/InstallAgent/config/`.

c. Rename the `voiceportal_info.jsp` to `voiceportal_info.php` and copy to `/var/www/html/voiceportal_info.php`.

   Create the directory if it does not already exist. For example, `mkdir -p /var/www/html/`.

d. Copy the `PG_VERSION` file to `/var/lib/pgsql/data/PG_VERSION`.

   Create the directory if it does not already exist. For example, `mkdir -p /var/lib/pgsql/data/`.

4. Disable the firewall on the Experience Portal server.
5. Configure a yum repository that has required Experience Portal packages
6. Install the Avaya Experience Portal 8.1 Primary EPM software.

   For more information, see Prerequisites checklist for upgrading Experience Portal on page 44 and Upgrading the Primary EPM software interactively on page 59.

   Important:

   Use the interactive upgrade method by running the **`aepinstall`** script.

   Ensure that you assign the same host name and IP address to the server before the upgrade.

7. If you are upgrading from Avaya Experience Portal 6.x or 7.x, do the following to establish whether a new EP Signing Certificate needs to be generated:

   a. In the EPM web interface, navigate to **Security** > **Certificates** > **EP Signing Certificate** > **Certificate**.

   b. Inspect the **Security Certificate** > **Basic Constraints** > **CA entry**.

      If the CA entry is set to false, do the following:

      - Create a new EP Signing Certificate by navigating to the **Security** > **Certificates** > **EP Signing Certificate** > **Certificate** and clicking **Generate** .
      - Initiate a manual reboot of EPM by using SSH on the EPM server and initiating a reboot via the Linux command line.
      - Delete the MPP server and add the MPP server back again, using the same name and IP. Then, click **Trust new certificate**.
      - Click **Save**.

Note:

This step is required only if the EP Signing Certificate is enabled. For customers with EP Signing Certificate (custom identity certificates) disabled, this step is not required.

The EP Signing Certificate can be generated on the Experience Portal server or it can be issued by an external Certificate Authority (CA) and uploaded to the Experience Portal server. If it is issued by an external CA, then customers need to request a new EP Signing Certificate from the external CA that has Basic Constraints with a CA value set to true.

8. Run the **`setup_vpms.php`** script on each MPP server to authorize the new security certificate on the Primary EPM and to allow the MPPs to communicate with it.
9. In the System Monitor page, if it shows that the MPP needs to be restarted, restart the MPP from the **MPP Manager** page.

Note:

If your Auxiliary EPM has outcalls in progress, skip the following step.

10. Re-establish the communication link between the upgraded EPM and the Auxiliary EPM servers:
    a. Log in to Linux on each Auxiliary EPM server.
    b. Run the **`setup_vpms.php`** script.
    c. Log in to the EPM web interface.
    d. On the EPM navigation pane, click **EPM Servers**.
    e. Click the EPM server that you have upgraded.

       The system displays the **Change EPM Server** page.
    f. Click **Trust new certificate**.
    g. Click **Save**.

Upgrading an Auxiliary EPM on Red Hat Enterprise Linux Server

About this task

Perform the following steps to upgrade each Auxiliary EPM system that uses the customer-provided Red Hat Enterprise Linux Server.

Before you begin

Verify that the prerequisites have been met. For more information, see Prerequisites checklist for upgrading Experience Portal on page 44.

If upgrading from Avaya Experience Portal 6.x or 7.x, note the following:

- The upgrade is treated as a fresh install where the same IP and Auxiliary EPM name used in Avaya Experience Portal 6.x or 7.x, must be configured in the Primary EPM UI.

- While upgrading theAuxiliary EPM server, you are prompted for the following details related to the Primary EPM server:
  - IP address of the Primary EPM server: This IP address is required so that the system can retrieve the security certificate. To ensure that the system retrieves the updated certificate from the Primary server, first upgrade the Primary server.
  - vpcommon password: The vpcommon password specified during the Avaya Experience Portal 6.x or 7.x Primary EPM installation. With this user account, the Auxiliary EPM server has limited access to the main Experience Portal database.

Important:

If upgrading from Avaya Experience Portal 6.x or 7.x and the vpcommon password is *not* known, you need to reset the password *before* upgrading the Auxiliary EPM. For more information on changing the user account password, see the *Changing PostgreSQL user account passwords* section in the *Administering Avaya Experience Portal* document.

Procedure

1. Disable the firewall on the Auxiliary Experience Portal server.
2. Configure a yum repository that has required Experience Portal packages.
3. Install the Avaya Experience Portal 8.1 Auxiliary EPM software.

   For more information, see Upgrading the Auxiliary Experience Portal software interactively on page 66.

   Important:

   You must use the interactive upgrade method by running the **`aepinstall`** script. Ensure that when you are prompted for the password to configure the Auxiliary EPM server, enter the same password that you used to upgrade the Primary EPM.
4. Trust the new security certificate for the upgraded Auxiliary. Do the following:

   Note:

   If you are upgrading from Avaya Experience Portal 6.x or 7.x, the trust relationship may already be established, therefore the following steps may not be required.

   a. Log in to the EPM web interface.
   b. On the EPM navigation pane, click **EPM Servers**.
   c. Click the Auxiliary EPM server that you upgraded.

      The system displays the **Change EPM Server** page.
   d. Click **Trust new certificate**.
   e. Click **Save**.
5. Restart all the MPPs.

Upgrading a Media Processing Platform (MPP) on Red Hat Enterprise Linux Server

About this task

Use this procedure to upgrade each MPP server that uses the customer-provided Linux operating system.

Before you begin

Verify that the prerequisites have been met. For more information, see Prerequisites checklist for upgrading Experience Portal on page 44.

Procedure

1. Log on to the EPM web interface.
2. Click **System Management** > **MPP Manager**.
3. On the **MPP Manager** page, click **Stop** to stop the MPP.
4. Schedule a report data download so that EPM collects all calls records from the MPP server.

   For more information, see Preventing loss of reporting data prior to upgrading MPP on page 43.
5. Take the MPP offline.

   For more information, see Taking an MPP offline using the EPM web interface on page 42.
6. If you upgrade to Experience Portal 8.1 from Experience Portal 6.x or 7.x, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server.

   For more information, see Upgrading Red Hat Enterprise Linux Server on a dedicated MPP server on page 38.
7. Disable the firewall on the MPP server.
8. Configure a yum repository that has the required Experience Portal packages.
9. Install the Experience Portal 8.1 MPP software.

   For more information, see Upgrading the MPP software interactively on page 71.

   Important:

   You must use the interactive upgrade method by running the **`aepinstall`** script.
10. Trust the new security certificate for the MPP. Do the following:
    a. Log in to the EPM web interface.
    b. On the EPM navigation pane, click **MPP Servers**.
    c. Click the MPP server name that you upgraded.

       The system displays the **Change MPP Server** page.

d. Click **Trust new certificate**.

e. Click **Save**.

11. On the EPM navigation pane, click **MPP Manager**.
12. Change the mode of the MPP to **Online**.
13. Click **Start** to start the MPP.

Upgrading the single server Experience Portal system on Red Hat Enterprise Linux Server

About this task

Perform the following procedure to upgrade a single server Experience Portal system that uses the customer provided Linux software.

Before you begin

Verify that the prerequisites have been met. For more information, see Prerequisites checklist for upgrading Experience Portal on page 44.

Procedure

1. Log on to the EPM web interface.
2. On the **MPP Manager** page, click **Stop** to stop the MPP.
3. Schedule a report data download so that EPM collects all calls records from the MPP server.

   For more information, see Preventing loss of reporting data prior to upgrading MPP on page 43.
4. Change the state of the MPP to **Offline**. For more information, see Taking an MPP offline using the EPM web interface on page 42.
5. Create a backup of the Experience Portal system.

   Ensure that you save the backup folder on an external server that is not a part of the Experience Portal system. For more information, see Backing up data on page 25.
6. If you upgrade to Experience Portal 8.1 from Experience Portal 6.x or 7.x, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server.

   For more information, see Upgrading Red Hat Enterprise Linux Server on the dedicated EPM server on page 36.
7. If you upgrade to Experience Portal 8.1 from Experience Portal 6.x or 7.x, you must manually stage the database backup and configuration files on the fresh installation RHEL server.

For more information on database backup and configuration files, see Backing up data on page 25.

a. Rename the `vp_backupaa` backup file to `vp_upgrade.export` and copy the file to `/var/lib/pgsql/vp_upgrade.export`.

b. Copy the `version.xml` file to `/opt/Avaya/InstallAgent/config/version.xml`.

   Create the directory if it does not already exist. For example, `mkdir -p /opt/Avaya/InstallAgent/config/`.

c. Rename the `voiceportal_info.jsp` to `voiceportal_info.php` and copy to `/var/www/html/voiceportal_info.php`.

   Create the directory if it does not already exist. For example, `mkdir -p /var/www/html/`.

d. Copy the `PG_VERSION` file to `/var/lib/pgsql/data/PG_VERSION`.

   Create the directory if it does not already exist. For example, `mkdir -p /var/lib/pgsql/data/`.

8. Disable the firewall on the Experience Portal server.
9. Configure a yum repository that has required Experience Portal packages.
10. Install the Experience Portal 8.1 EPM and MPP software.

    For more information, see Upgrading the Experience Portal software interactively on a single server on page 75.

    Important:

    You must use the interactive upgrade method by running the **`aepinstall`** script.

11. If you are upgrading from Avaya Experience Portal 6.x or 7.x, and the MPP server status is displayed as **Not Responding** in the System Monitor page, do the following to complete additional steps to reestablish communication between the primary EPM and MPP:

    a. Log in to Linux on the MPP server.

    b. Run the `setup_vpms.php` script.

    c. Click **System Management** > **MPP Manager**.

    d. Delete the MPP server and add the MPP server back again, using the same name and IP.

    e. Click **Trust new certificate**.

    f. Click **Save**.

12. Trust the new security certificate for the MPP if not already completed as part of the previous step. Do the following:

    a. Log in to the EPM web interface.

b. On the EPM navigation pane, click **MPP Servers**.
c. Click the MPP server name that you upgraded.

   The system displays the **Change MPP Server** page.
d. Click **Trust new certificate**.
e. Click **Save**.

13. On the EPM navigation pane, click **MPP Manager**.
14. Change the mode of the MPP to **Online**.
15. Click **Start** to start the MPP.

Chapter 3: Upgrading the operating system

Operating system upgrade overview

Important:

- Upgrading Avaya Enterprise Linux operating system to 8.1 is mandatory because of the requirement for Java 1.8 and a 64-bit operating system.
- Avaya recommends that you upgrade the operating system to get the latest fixes and any security updates.

For upgrades, Avaya Experience Portal supports the following operating systems:

- Red Hat Enterprise Linux 7.x 64-bit or newer 7.x update
- Red Hat Enterprise Linux 8.x 64-bit or newer update
- Avaya Enterprise Linux AvayaLinux-RH8*.iso.

For customers on Red Hat Enterprise Linux Server 6.x or Avaya Enterprise Linux 6.x, it is necessary to upgrade the operating system rather than only upgrade the Experience Portal application.

To upgrade to Avaya Enterprise Linux AvayaLinux-RH8*.iso, Red Hat Enterprise Linux 7.x 64-bit or newer 7.x update, or Red Hat Enterprise Linux 8.x 64-bit or newer update:

- Upgrade Avaya Enterprise Linux if you have opted for the Avaya bundled server offer. There are two upgrade methods for Avaya Enterprise Linux:
  - Upgrade using an ISO image file: This upgrade method provides an auto upgrade of Avaya Enterprise Linux.
  - Upgrade with the software installation DVD: This upgrade method provides an auto-upgrade option to upgrade Avaya Enterprise Linux.
- For Experience Portal 6.x or 7.x upgrades on Avaya Enterprise Linux:
  - Upgrade Avaya Enterprise Linux using the Avaya Enterprise Linux ISO release aligned with the target Experience Portal 8.x release

- For Experience Portal 8.x upgrades on Avaya Enterprise Linux:
  - Upgrading Avaya Enterprise Linux using the Avaya Enterprise Linux ISO is not supported, however applying the latest Avaya Enterprise Linux security patch will provide the same functionality:
    - For example, upgrading Avaya Enterprise Linux 8.1 AvayaLinux-RH8* to AVL 8.1.x AvayaLinux-RH*.iso is not supported.
    - Use the upgrade option during the Avaya Enterprise Linux patch install which applies all the required changes to support the product on the original Avaya Enterprise Linux. For example, `./setup.sh -v 8.1.x`.
- Do a fresh installation of a supported version of Red Hat Enterprise Linux Server if you have opted for the software-only offer and are upgrading from versions prior to Experience Portal 7.2.x.

  For upgrades from Avaya Experience Portal 6.x or 7.x to 8.1, in-place OVA upgrades are not supported. The 8.1 OVAs must be deployed.

  For upgrades from Avaya Experience Portal 8.0 to 8.1, in-place upgrades are supported via ISO.

  Note:

  This note is for Software-only customers.

  Experience Portal does not bundle any packages that are obtained from Red Hat. Experience Portal provides a Prerequisite installer that installs all the Red Hat Enterprise Linux packages that are needed to install Experience Portal, provided that customers configure a valid yum repository on the system that contains all the required Experience Portal prerequisites. Customers can either run the Experience Portal Prerequisite installer standalone outside of installation or alternatively run the Prerequisite installer within the Experience Portal installer.

  All OS packages required by Experience Portal are standard Red Hat Enterprise Linux packages except for php-process. The yum repository or repositories configured on the system must contain standard Red Hat Enterprise Linux packages plus php-process.

  Note:

  Red Hat Enterprise Linux Server does not support upgrading from 32-bit to 64-bit versions of Red Hat Enterprise Linux Server.

  To save your Experience Portal configuration while doing a fresh installation of a supported version of Red Hat Enterprise Linux Server, ensure that you create a backup of Experience Portal from **System Backup** menu in EPM. Ensure that you save the backup folder on a server that is not part of the Experience Portal system.

  For more information about backing up Experience Portal data from the **System Backup** menu in EPM, see the *Administering Avaya Experience Portal* guide on the Avaya Support site.
- Upgrade or perform a fresh installation of the Primary EPM, Auxiliary EPM and MPP software depending on whether the OS is upgraded or freshly installed.

Important:

- You cannot run an older version of the Experience Portal EPM or MPP software on a server running the upgraded operating system. Therefore, ensure that you upgrade the Primary EPM, Auxiliary EPM, and MPP software to Avaya Experience Portal 8.1.
- Experience Portal 8.x supports outcall using the Axis 2 based Web Service named VPAppIntfService. Experience Portal 8.x does not support outcall using the Axis 1.4 based Web Service named AppIntfWS that was supported in prior releases of Experience Portal (6.x and earlier).

  Ensure that you upgrade all applications that are using Outcall Axis1.4 based web service named AppIntfWS to instead use Outcall Axis 2 based Web Service named VPAppIntfService.
- If your Experience Portal system has Auxiliary EPMs, you can upgrade the Primary EPM while the Auxiliary EPMs continue to process outcalls.

If your Experience Portal system consists of multiple servers, you can upgrade the EPM server operating system and Experience Portal software even while the MPPs are in the running state. In addition, if you have multiple MPPs, you can upgrade an MPP while the other MPPs are in the running state.

Default Red Hat umask

Avaya Experience Portal 8.1.1 requires default umask to be set to `027`. You can set this in the `/etc/profile` and `/etc/bashrc` scripts.

Avaya Linux and OVAs have default umask set to `027`. Fresh installs and upgrades will verify that umask is set to `027`. If umask is not set, then the installer asks if you want to set it to `027`. If you answer 'yes', the installer applies this setting to the OS. If you answer 'no', the installer exits.

Platform Vendor Independent Check

The Platform Vendor Independent Check (PVI checker) is the same utility that is executed by the AEP installer (aepinstall.sh). The PVI checker (pvicheck.sh) can be run by customers outside of installation. That is, a customer can check the prerequisites or preinstall these packages before installing Experience Portal.

The PVI checker is located under Support/PrereqCheckerInstaller of the Experience Portal media.

Note:

Experience Portal does not bundle any packages that are obtained from Red Hat. Experience Portal provides a PVI checker that installs all Red Hat Enterprise Linux packages that are needed to install Experience Portal, provided that customers configure a valid yum repository on the

system that contains all required Experience Portal prerequisites. Customers can either run the Experience Portal PVI checker standalone outside of installation or alternatively run the PVI checker within the Experience Portal installer. All OS packages required by Experience Portal are standard Red Hat Enterprise Linux packages. Since Avaya Enterprise Linux for Experience Portal 8.x already contains all the required prerequisites, this note primarily applies to software-only customers.

PVI checker

The PVI checker can be executed by running the `bash pvichecker.sh` script. This checks all the pre-requisites required such as non-root account, hostname resolvable, required Red Hat RPM packages installed, and then lists the ones that passed or failed.

If the PVI checker is invoked with the `-install` parameter, that is running `pvicheck.sh -install` , it installs any missing RPMs, provided a yum repository is configured. It also performs other correction tasks like adding hostname to `/etc/hosts` and disabling firewall.

The PVI checker can also be invoked with the `-headless` parameter which suppresses the need for user input.

High level packages required for the installation of Experience Portal 8.1

The following lists the high level packages that are required for the installation of Experience Portal 8.1.

Note:

If these packages are not already installed on the OS and a yum repository is configured, the Experience Portal installer will install them.

These packages do not include dependencies that may be required to install these packages. The exact dependency list will vary and depends on what the customer has installed on their OS.

You can view the full list of RPMs required for Avaya Experience Portal 8.1 by running `pvicheck.sh`.

Red Hat 7.x and Red Hat 8.x pre-requisite RPMs:

policycoreutils-python-utils.noarch

libgcc.x86_64

libgcc.i686

libstdc++.x86_64

libstdc++.i686

glibc.x86_64

glibc.i686

openssl.x86_64

openssl-libs.i686

httpd.x86_64
mod_ssl.x86_64
httpd-tools.x86_64
php-common.x86_64
php-cli.x86_64
php.x86_64
php-soap.x86_64
php-xml.x86_64
php-pgsql.x86_64
php-process.x86_64
java-1.8.0-openjdk.x86_64
libicu.x86_64
java-1.8.0-openjdk-headless.x86_64
java-1.8.0-openjdk-devel.x86_64
chrony.x86_64
net-tools.x86_64
hostname.x86_64
sysstat.x86_64
bc.x86_64
tcpdump.x86_64
wget.x86_64
perl.x86_64
libidn.i686
krb5-libs.i686
fontconfig.i686
openldap.i686
gd.i686
libatomic.i686
cairo.x86_64
lsof.x86_64
libpng12.i686
libpng12.x86_64
pam.i686

libcap.i686

mlocate.x86_64

bind-utils.x86_64

traceroute.x86_64

dos2unix.x86_64

unzip.x86_64

zip.x86_64

nfs-utils.x86_64

libxml2.x86_64

binutils.x86_64

libpwquality.x86_64

libcurl.i686

mozjs52.i686

mozjs52.x86_64

pcre.i686

Red Hat 7.x pre-requisite RPMs

python3.x86_64

Red Hat 8.x pre-requisite RPMs

compat-openssl10.i686

compat-openssl10.x86_64

libnsl2.i686

libnsl2.x86_64

libnsl.i686

libnsl.x86_64

nspr.i686

mozjs60.i686

Backing up data

About this task

Red Hat Enterprise Linux Server does not support upgrading from 32-bit to 64-bit versions of Red Hat Enterprise Linux Server.

To save your Experience Portal configuration while doing a fresh installation of a supported version of Red Hat Enterprise Linux Server, ensure that you create a backup of Experience Portal.

Note:

Backing up data is a customer responsibility.

Procedure

1. Backup the Experience Portal database. For the upgrade procedure, you must use the **System Management > System Backup** menu in the EPM Web interface to create the backup.

   For more information on system backup, see *Administering Avaya Experience Portal* on the Avaya Support site.

2. If you are upgrading from Experience Portal 6.x or 7.x on a supported version of Red Hat Enterprise Linux, you must manually backup the Avaya Experience Portal configuration files from the Primary EPM for the installation script to automate the upgrade.

   - `$AVAYA_IA_HOME/config/version.xml`

     For example, `/opt/Avaya/InstallAgent/config/version.xml`

   - `/opt/Tomcat/apache-tomcat-*/webapps/ROOT/voiceportal_info.jsp`
   - `$POSTGRESQL_HOME/data/PG_VERSION`

     For example, `/var/lib/pgsql/data/PG_VERSION`

   - `/var/www/html/easg_info.php` (Optional)
   - `$POSTGRESQL_HOME/vp_upgrade.export`

     For example, `/var/lib/pgsql/vp_upgrade.export`

3. If you have manually modified any Voice Portal or Experience Portal properties files, back up those files. You must manually merge the changes after the upgrade is complete.
4. If any Tomcat configuration files in `/opt/Tomcat/tomcat/config` have been manually modified, back up those configurations so that you can manually merge them back after the Experience Portal upgrade is complete.
5. **(Optional)** If you have previously changed the **Session timeout (minutes)** in **Home** > **User Management** > **Login Options**, record these settings before upgrading Experience Portal.
6. **(Optional)** If you have previously changed the **Purge and Retention** options in **Home** > **System Configuration** > **EPM Servers** > **Alarm/Log Options** , record these settings before upgrading Experience Portal.
7. **(Optional)** If you had previously enabled **Organizations** for the system, record these settings under **User Management** > **Organizations**.
8. **(Optional)** If you have previously deployed and configured any Managed Applications, re-install and deploy the managed application after the upgrade is complete.

It is recommended to take a backup of the managed application, for example, Avaya Proactive Outreach Manager, as per the managed application documentation.

9. **(Optional)** If you have previously deployed and configured the co-residing application server, create a backup of the deployed application and application support runtime libraries files from the co-resident application server before the system is upgraded.

   Note:

   For major version upgrades of Tomcat, it is also recommended that the deployed applications and application support runtime libraries are re-generated for the updated version of Tomcat.

Staging the Experience Portal 6.x or 7.x backup files on the Primary EPM before upgrading Experience Portal

About this task

If upgrading to Experience Portal 8.1 from Experience Portal 6.x or 7.x on a Red Hat Enterprise Linux Server, you must manually stage the database backup and configuration files on the fresh installation RHEL server of the Primary EPM. You must do this before you run the aepinstall.sh script for upgrading the Primary EPM server to Experience Portal 8.1.

For more information on the database backup and configuration files, see Backing up data on page 25.

Note:

This procedure is only applicable to Red Hat Enterprise Linux upgrades from Experience Portal 6.x or 7.x. It is not required for Avaya Enterprise Linux upgrades. Staging of the files is required only for the Primary EPM.

Procedure

1. Rename the `vp_backupaa` backup file to `vp_upgrade.export` and copy the file to `/var/lib/pgsql/vp_upgrade.export`.
2. Copy the `version.xml` file to `/opt/Avaya/InstallAgent/config/version.xml`.

   Create the directory if it does not already exist.

   For example, `mkdir -p /opt/Avaya/InstallAgent/config/`.
3. Rename the `voiceportal_info.jsp` to `voiceportal_info.php` and copy to `/var/www/html/voiceportal_info.php`.

   Create the directory if it does not already exist.

   For example, `mkdir -p /var/www/html/`.
4. Copy the `PG_VERSION` file to `/var/lib/pgsql/data/PG_VERSION`.

Create the directory if it does not already exist.

For example, `mkdir -p / var/lib/pgsql/data/.`

Preparing to connect to Avaya Enterprise Linux using an Ethernet cable

To install Avaya Enterprise Linux on a server using an Ethernet cable connection from a laptop, you must configure the laptop to establish communication between the laptop and the server.

About this task

Use the procedure to prepare the laptop to connect to Avaya Enterprise Linux using a Ethernet cable.

Before you begin

- Install the Avaya provided hardware on the server.
- Ensure that eth1, which is also called port 2, is available for use when you connect to the server using a network cable.
- Obtain the following equipment for the remote connection:
  - Telnet client and secure shell (SSH) client programs installed on the laptop.

    Note:

    PuTTY is a popular, free program that can function as both a Telnet client and as an SSH client.
  - An Ethernet or a CAT5 network cable that connects the laptop to the Services port on the server, eth1.

Procedure

1. Connect an Ethernet (or CAT5) network cable from the laptop to the temporary services port eth1.

   Note:

   The eth1 port is also called port 2.
2. Configure the laptop with the following settings:

   `ipaddress=192.11.13.5`

   `netmask=255.255.255.252`
3. Verify link connectivity between the system and the server.
   a. At the command line prompt, enter the `ping 192.11.13.6` command.
   b. Check the LED on the temporary Services port and the LED on the network card of the laptop.

The LED light flashes green when the link is connected.

c. The screen displays the response from the server that shows that the server is operational.

4. Insert the Enterprise Linux Installer software into a DVD drive on the Experience Portal server.
5. Reboot the server so that the server starts from the Avaya Enterprise Linux Installer software.

Next steps

Install or upgrade Avaya Enterprise Linux.

Upgrading Avaya Enterprise Linux using an ISO image file

About this task

Use this procedure to upgrade Avaya Enterprise Linux using an ISO image file. The upgrade is initiated from `AvayaLinux-RH8*.iso`, which is the Avaya Experience Portal 8.1 Linux Installer ISO image file that you must copy or move to the `/var` directory during the course of the upgrade process.

This upgrade method is non-interactive and provides an automatic upgrade of Avaya Enterprise Linux.

Note:

For OVA based systems, in-place upgrades of Experience Portal 6.x or 7.x OVA deployments to 8.x are not supported. You must deploy fresh Experience Portal 8.x OVAs.

Before you begin

- The upgrade requires 2GB free space in the /var directory to copy temporary files for the operating system upgrade. This space requirement is in addition to the space that is required for the database upgrade and migration of data, and will be proportional to the pre-upgrade volume of data. If the free space is not available in the `/var` directory, the installer does not proceed with the operating system installation.
- Note the Fully Qualified Filename (FQFN) of the Avaya Experience Portal 8.1 Linux Installer ISO image. During the installation process, the installer may prompt for the FQFN of the ISO image.
- Ensure that no network cable is connected to the maintenance port (eth1) of the server. The installer runs the autoupgrade utility while upgrading Avaya Enterprise Linux without media.
- If you plan to use a direct connection to upgrade Avaya Enterprise Linux, connect a keyboard and monitor to the server.

Warning:

If the upgrade fails, you might require physical access to the server in order to return the server to a working state.

Important:

If you have installed a Tomcat application server on the Experience Portal server, the software on the Application server might get deleted during the operating system upgrade. Back up the configuration files, data files, Web applications, libraries, and binaries from the directory where the Application server is installed. For more information about the required backup files, contact the application developer.

Procedure

1. Log in to Linux on the Experience Portal server.
   - If you upgrade through the console:
     - Log in to the local Linux console as a user with root privileges.
   - If you upgrade through a network connection to eth0 or log on remotely:
     - Log in to Linux as a non-root user, for example, cust, and then change to a user with root privileges by entering the **`su - root`** command.
2. Copy the Avaya Experience Portal 8.1 Linux Installer ISO image to a folder on the system, and mount the ISO image to the desired directory by entering the mount command.

   For example, run the **`mount -o ro,loop`** *<AvayaLinux-RH8*.iso>* **`/mnt/cdrom`** command, where:
   - *<AvayaLinux-RH8*.iso>* is the name of the Avaya Experience Portal 8.1 Linux Installer ISO image
   - /mnt/cdrom is the mount point associated with the ISO image
3. Run the `bash` **`/mnt/cdrom/Avaya/vpupgrade.sh`** command to run the Pre-upgrade tool.

   This tool prepares the system for the upgrade.
4. Type `y` and press `Enter` to confirm that you want to run the tool.

   The tool confirms whether you want to upgrade the operating system without media.
5. Type `yes` and press `Enter` to proceed with an autoupgrade without media.
6. If you have performed an upgrade on the system earlier using the ISO image file, the upgrade script prompts if you want to delete the `/var/avlupgrade` directory.
   - If you do not want to delete the `/var/avlupgrade` directory, you will need to exit the upgrade process by performing the following steps:
     - Type `no` and press `Enter`.
     - At the **Do you want to continue** prompt, type `y` and press `Enter` to exit the installation process.
     -
   - To delete the `/var/avlupgrade` directory and continue with the upgrade, type `yes` and press `Enter`.

The upgrade script may prompt for the FQFN of the Avaya Experience Portal 8.1 Linux Installer ISO image.

7. If prompted, type the FQFN where:

   FQFN is the full filename, including path, to the Avaya Experience Portal 8.1 Linux Installer ISO image, which you have copied to the system at the beginning of the task.

8. Press `Enter`.

   The upgrade script prompts you to copy or move the files from the ISO image to /var, the static partition.

9. Type `copy` to copy the ISO files or type `move` to move the ISO files, and press `Enter`.

   The upgrade script copies/moves the files from the ISO image to the static partition.

10. Type `y` and press `Enter` to confirm that you want the utility to prepare the system for the upgrade.

11. Type `y` and press `Enter` to reboot the server.

    The upgrade process starts automatically after the server is rebooted.

12. When the upgrade process is complete and the server responds to ping from a command line, log in to Linux on the Avaya Experience Portal server.

    Note:

    The network login root is disabled after upgrading Avaya Enterprise Linux.

    - Use cust account followed by su - or su - root.
    - If you upgrade through the console, log in to the local Linux console as root.
    - If you upgrade through a regular network connection to eth0, log in to Linux as a non-root user cust and enter the **`su -`** command to change to the user root.

    Avaya Enterprise Linux will enforce an Avaya First Login Experience. It will prompt for a new bootloader password and change the root and cust passwords. The sroot and craft password will be controlled via EASG as soon as Experience Portal is installed. You do not need to change them at this point.

    For more details, see State of identity variables in Master Software Image and on first boot. on page 35

13. If the server is an MPP and you have moved the MPP logs to a new directory or a partition using the `mppMoveLogs.sh` script, add the mount point to the `/etc/fstab` file. For more information, see *Administering Avaya Experience Portal*.

14. Configure the Avaya Enterprise Linux time settings.

    For more information, see Verifying server time synchronization on page 55.

Next steps

After you upgrade Avaya Enterprise Linux, upgrade to Avaya Experience Portal 8.1.

Upgrading Avaya Enterprise Linux from the software installation DVD

About this task

Use this procedure to upgrade Avaya Enterprise Linux from the Avaya Enterprise Linux software installation DVD. This upgrade method provides both non-interactive as well as automatic upgrade of Avaya Enterprise Linux.

Before you begin

If you plan to use a direct connection to upgrade Avaya Enterprise Linux, ensure that you connect a keyboard and monitor to the server.

If you plan to use a Ethernet connection from a laptop, configure the laptop as described in Preparing to connect to Avaya Enterprise Linux using an Ethernet cable on page 28.

Important:

If you have installed a Tomcat application server on the Experience Portal server, the software on the Application server might get deleted during the OS upgrade. Back up the configuration files, data files, Web applications, libraries, and binaries from the directory where the Application server is installed. For more information about the required backup files, contact the application developer.

Procedure

1. Log in to Linux on the Experience Portal server.
   - If you upgrade through the console:
     - Log in to the local Linux console as a user with root privileges.
   - If you upgrade through a network connection to eth0 or log on remotely:
     - Log in to Linux as a non-root user, for example, cust, and then change to a user with root privileges by entering the **`su - root`** command.
   - If you upgrade through a Ethernet connection to eth1:
     - Use a secure shell (SSH) client, such as PuTTY, to open an SSH connection to the IP address 192.11.13.6.
     - If you are an Avaya Services representative, log in to Linux as cust and change to the user root by entering the **`su - root`** command.
     - Or log in to Linux as a non-root user, and enter the **`su -`** command to change to the root user.
2. Insert the Avaya Enterprise Linux software installation DVD in to the server's DVD device.
3. If the DVD device is not automatically mounted, mount the drive by entering the **`mount /mnt/cdrom`** command.

   `/mnt/cdrom` is the mount point associated with the DVD device in the fstab file.

   If you cannot mount the DVD on Avaya Enterprise Linux, see *Troubleshooting Avaya Experience Portal* to troubleshoot the issue.

4. Run the `bash` **`/mnt/cdrom/Avaya/vpupgrade.sh`** command to run the Pre-upgrade tool.

   The tool confirms whether you want to upgrade the OS without media.

5. Type `no` and press `Enter` to confirm that you want to upgrade the OS with media.

   The tool prepares the system for the upgrade.

6. Type `y` and press `Enter` to confirm that you want to run the tool.

   The tool confirms whether you want to enable the autoupgrade option.

7. Type `n` and press `Enter` to disable autoupgrade, or type `y` and press `Enter` to enable autoupgrade.

   Important:

   If you upgrade through a network connection to eth0, ensure that you enable autoupgrade.

8. Press `Enter` to complete the preupgrade tool.

9. Type `Y` and press `Enter` to restart the server.

   If you upgrade through a network connection to eth0, and select the autoupgrade option, the system runs the upgrade procedure after the system restarts. Skip to Step 12 for further instructions.

   If you upgrade through a console, the system displays the Avaya Enterprise Linux installer Welcome screen after the system restarts.

10. In the Avaya Enterprise Linux installer Welcome screen, type `2` and press `Enter` at the boot prompt to select the **Upgrade** option.

    The installer displays the Warning screen.

    Important:

    You must enter your selection on the Welcome screen within 60 seconds. Otherwise, the installer searches for an Ethernet connection on the eth1 interface.

    If the connection is not detected, the installer continues with autoupgrade if you have selected the autoupgrade option. The installer ejects the DVD and reboots if you have not selected the autoupgrade option.

    Note:

    Instead of displaying the Warning screen, the Avaya Enterprise Linux installer might display the **No Disks found! /dev/sda missing** error. To resolve the issue, type `n` and press `Enter` at the **Eject CD/DVD before rebooting** prompt.

11. If you upgrade through an Ethernet connection to eth1:

    a. In the command line, enter the `ping -t 192.11.13.6` command to determine when the server completes the reboot.

b. After the server responds to the ping command, type `Ctrl-C` to stop the ping command.

c. Open a telnet client, such as PuTTY, and connect to the IP address 192.11.13.6.

Important:

You must start the telnet session within 5 minutes of the server responding to ping. If you do not start the telnet session, the installer ejects the DVD and reboots the server.

Note:

To use the Windows command telnet as the telnet client:

- Enter the **`telnet`** command.
- At the Microsoft Telnet> prompt, enter the **`set term vt100`** command.
- At the Microsoft Telnet> prompt, enter the **`open 192.11.13.6`** command.

Note: When using telnet connection, the install screen might not display the information clearly.

The installer displays the Warning screen.

d. Type `u` and press `Enter` at the **Specify your choice** prompt to select the **Upgrade** option.

The installer displays the Warning screen.

12. On the Warning screen, type `yes` and press `Enter` to confirm that you want to upgrade Avaya Enterprise Linux.

Note:

If you upgrade remotely, you do not see the Warning screen, and the installer selects the **Remote Install/Upgrade** option by default.

13. When the installer completes the upgrade procedure, the server ejects the DVD, and the server reboots automatically.

If you upgrade remotely, the upgrade procedure is completed when the server ejects the DVD and the server responds to ping from a command line.

14. Remove the Avaya Enterprise Linux installation DVD from the drive.

15. When the server reboots, log in to Linux on the Avaya Experience Portal server.

Note:

The network login root is disabled after upgrading Avaya Enterprise Linux.

- If you upgrade through the console, log in to the local Linux console as root.
- If you upgrade through a regular network connection to eth0, log in to Linux as a non-root user cust and enter the **`su -`** command to change to the user root.

- If you upgrade through an Ethernet connection to eth1, you must perform the following:
  - Use a secure shell (SSH) client, such as PuTTY, to open an SSH connection to the IP address 192.11.13.6.
  - Log in to Linux as a non-root user, cust.
  - Enter the **su -** command to change to the user root.

  The Enterprise Linux Installer creates craft and sroot accounts but they are disabled with no predefined password. The craft and sroot accounts are Avaya Service Accounts and can only be enabled via EASG control. You should use the cust and root accounts to login to the server. Avaya Enterprise Linux has assigned a default password for both accounts.

  For more details, see State of identity variables in Master Software Image and on first boot. on page 35

16. If the server is an MPP and you have moved the MPP logs to a new directory or partition using the `mppMoveLogs.sh` script, add the mount point to the `/etc/fstab` file. For more information, see *Administering Avaya Experience Portal* on the Avaya Support site.
17. Configure the Avaya Enterprise Linux time settings.

    For more information, see Verifying server time synchronization on page 55.

Next steps

After you upgrade Avaya Enterprise Linux, upgrade to Avaya Experience Portal 8.1.

State of identity variables in Master Software Image and on first boot

After you install and configure Avaya Enterprise Linux, the Enterprise Linux Installer creates user accounts. The sroot and craft account passwords are disabled with no predefined password, unless EASG is enabled. You should use cust and root accounts to login to the server.

User name	Group	Purpose	Status of Account
sroot	root	Avaya Services root access	Disabled
root	root	Customer root access	Enabled
craft	susers	Avaya Services non-root access	Disabled
cust	susers	Customer non-root access	Enabled

First boot

You will not be able to use the Avaya Service accounts, craft and sroot, to gain access to the server once the server is upgraded to Avaya Enterprise Linux 8.x. The craft and sroot accounts will be controlled via EASG as soon as Experience Portal is installed.

The craft and sroot users are disabled unless EASG is enabled. In this case, the craft and sroot users will use challenge/response authentication.

This applies to both non-OVA and OVA deployments.

First root login

The root and cust users which have default values in the software image, are forced to be updated on first root login. These accounts that are needed to log into a newly created system use pre-defined passwords:

Account	User Name	Password
Non-root access	cust	custpw
Root access	root	rootpw

After you login to the server as root using the default password, Avaya Enterprise Linux will enforce an Avaya First Login Experience which will prompt for a new bootloader, root and cust passwords.

To support headless configuration, root & cust are not forced to be updated on first boot, but are forced to be updated on the first root login.

Upgrading Red Hat Enterprise Linux Server on the dedicated EPM server

About this task

The following steps are guidelines to install a supported version of Red Hat Enterprise Linux Server, and provide instructions for making selections when the default values are not suitable.

Before you begin

If you are upgrading to Experience Portal 8.1 from Experience Portal 6.x or 7.x, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server.

Important:

- Ensure that you backup all the Experience Portal data, including the database.

  Important:

  For more information on creating a backup, see Backing up data on page 25.
- Verify that the prerequisites have been met. For more information, see Prerequisites overview for upgrading Experience Portal on page 44
- Log in to Linux on the EPM server and turn off the automatic process restart feature for Tomcat by entering the `chkconfig tomcat off` command.

Procedure

1. Reboot the server so that it boots from the media of a supported version of Red Hat Enterprise Linux Server.

   The system displays the **Welcome to Red Hat Enterprise Linux** screen.

2. Select the **Install Red Hat Enterprise Linux** option.
3. Select **English** as the language to use during the installation process.
4. Select the U.S. English keyboard option.
5. Select **Installation Destination** and select the disk to install Red Hat Enterprise Linux.
6. Select **Network and Host name**.
7. Enter the host name and select **Apply**.

   Note:

   All network configuration including the hostname and IP (and other properties specified in steps 7 and 8) must remain the same.
8. To configure the network:
   a. Ensure that `eth0/ens192`, the main Ethernet interface, is enabled.
   b. On the **IPv4 Settings** tab, configure the following settings using the values specified on the installation worksheet:
      - Static IP address
      - Netmask
      - Gateway
      - DNS servers
      - Search domains
9. Enter the applicable timezone.
10. Select **Begin Installation**.
11. Enter the root password. Ensure that you enter the value that you have specified in the installation worksheet.
12. Complete the installation and reboot the system.
13. After the system reboots, complete the post-installation configuration procedures.
    a. Accept the **License Agreement** and **Finish Configuration** (RHEL 8.x).
    b. Set the system clock.
    c. Create a non-root account. Ensure that you use the value that you have specified in the installation worksheet.

       Note:

       After the Experience Portal software is installed, use a non-root account to log in and then change to `root` account by using the **`su -`** command.
    d. Disable the firewall.
    e. Set default umask to `027` in the `/etc/profile` and `/etc/bashrc` scripts.

f. Configure a yum repository that has required Experience Portal packages.

Upgrading Red Hat Enterprise Linux Server on a dedicated MPP server

Before you begin

If you are upgrading to Experience Portal 8.x from Experience Portal 6.x or 7.x, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server.

- Verify that the prerequisites have been met. For more information, see Software upgrade prerequisites overview for upgrading on page 44
- Log on to the EPM web interface.
- From the **MPP Manager** page, stop the MPP.
- Take the MPP offline before you upgrade the operating system as described in Taking an MPP offline using the EPM web interface on page 42.
- Log in to the Linux server and turn off the automatic process restart feature for the MPP service by entering the `chkconfig mpp off` command.

Procedure

1. Reboot the server so that it boots from the media of a supported version of Red Hat Enterprise Linux Server.

   The system displays the **Welcome to Red Hat Enterprise Linux** screen.
2. Select the **Install Red Hat Enterprise Linux** option.
3. Select **English** as the language to use during the installation process.
4. Select the U.S. English keyboard option.
5. Select **Installation Destination** and select the disk to install Red Hat Enterprise Linux..
6. Select **Network and Host name**.
7. Enter the host name and select **Apply**.

   Note:

   All network configuration including the hostname and IP (and other properties specified in steps 7 and 8) must remain the same.
8. To configure the network:
   a. Ensure that `eth0/ens192`, the main Ethernet interface, is enabled.
   b. On the **IPv4 Settings** tab, configure the following settings using the values specified on the installation worksheet:
      - Static IP address

- Netmask
- Gateway
- DNS servers
- Search domains

9. Enter the applicable timezone.
10. Select **Begin Installation**.
11. Enter the root password. Ensure that you enter the value that you have specified in the installation worksheet.
12. Complete the installation and reboot the system.
13. After the system reboots, complete the post-installation configuration procedures.
    a. Accept the **License Agreement** and **Finish Configuration** (RHEL 8.x).
    b. Set the system clock.
    c. Create a non-root account. Ensure that you use the value that you have specified in the installation worksheet.

       Note:

       After the Experience Portal software is installed, use a non-root account to log in and then change to `root` account by using the **`su -`** command.

    d. Disable the firewall.
    e. Set default umask to `027` in the `/etc/profile` and `/etc/bashrc` scripts.
    f. Configure a yum repository that has required Experience Portal packages.

Upgrading Red Hat Enterprise Linux Server on a single server system

About this task

This procedure provides instructions on how to install a supported version of Red Hat Enterprise Linux Server.

Before you begin

Important:

If you are upgrading to Experience Portal 8.1 from Experience Portal 6.x or 7.x, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server.

If you have installed a co-resident Application server on the original Experience Portal server and:

- If the operating system is upgraded in a way which preserves data, such as a minor OS upgrade, then the original co-resident Application server is preserved. In this scenario, although it is not mandatory to update the co-resident Application server, it is recommended that the application server is upgraded to pick up the latest Tomcat features and security fixes.
- If a fresh install of the operating system was performed, such as performing a new installation of Red Hat Enterprise Linux 64-bit to replace the 32-bit system, or the operating system was otherwise upgraded in a way that does not preserve data on the system, then the original co-resident Application server is not preserved and must be manually upgraded to restore Application server functionality. In such a scenario, prior to upgrading the operating system, manually back up any configuration files, data files, Web applications and components, libraries, and binaries that you want to preserve from the original Application server. These files may then be restored as needed when the new Application server is installed. For more information about the required backup files, contact the application developer.

- Ensure that you backup all the Experience Portal data, including the database.

  Important:

  For more information on creating a backup, see Backing up data on page 25
- Verify that the prerequisites have been met. For more information, see Prerequisites checklist for upgrading Experience Portal on page 44.
- Log on to the EPM Web interface.
- From the **MPP Manager** page, stop the MPP.
- Perform the steps described in Preventing loss of reporting data prior to upgrading MPP on page 43.
- Take the MPP offline before you upgrade the operating system as described in Taking an MPP offline using the EPM web interface on page 42.
- Log in to Linux on the Experience Portal server and turn off the automatic process restart feature for the MPP service by entering the `chkconfig mpp off` command.
- Turn off the automatic process restart feature for Tomcat by entering the `chkconfig tomcat off` command.

Procedure

1. Reboot the server so that it boots from the media of a supported version of Red Hat Enterprise Linux Server.

   The system displays the **Welcome to Red Hat Enterprise Linux** screen.
2. Select the **Install Red Hat Enterprise Linux** option.
3. Select **English** as the language to use during the installation process.
4. Select the U.S. English keyboard option.

5. Select **Installation Destination** and select the disk to install Red Hat Enterprise Linux..
6. Select **Network and Host name**.
7. Enter the host name and select **Apply**.

   Note:

   All network configuration including the hostname and IP (and other properties specified in steps 7 and 8) must remain the same.
8. To configure the network:
   a. Ensure that `eth0/ens192`, the main Ethernet interface, is enabled.
   b. On the **IPv4 Settings** tab, configure the following settings using the values specified on the installation worksheet:
      - Static IP address
      - Netmask
      - Gateway
      - DNS servers
      - Search domains
9. Enter the applicable timezone.
10. Select **Begin Installation**.
11. Enter the root password. Ensure that you enter the value that you have specified in the installation worksheet.
12. Complete the installation and reboot the system.
13. After the system reboots, complete the post-installation configuration procedures.
    a. Accept the **License Agreement** and **Finish Configuration** (RHEL 8.x).
    b. Set the system clock.
    c. Create a non-root account. Ensure that you use the value that you have specified in the installation worksheet.

       Note:

       After the Experience Portal software is installed, use a non-root account to log in and then change to `root` account by using the **`su -`** command.
    d. Disable the firewall.
    e. Set default umask to `027` in the `/etc/profile` and `/etc/bashrc` scripts.
    f. Configure a yum repository that has required Experience Portal packages.

Taking an MPP offline using the EPM web interface

About this task

Use this procedure to take an MPP offline from EPM.

Procedure

1. Log in to EPM using an account with the Administration or Operations user role.
2. On the EPM navigation pane, click **System Management** > **MPP Manager**.
3. On the MPP Manager page, use the selection check box in the MPP server table to select the MPP server to take offline.

   Note:

   If the MPP is in the stopped state, proceed to step 8.
4. Click **Stop** in the **State Commands** group and confirm your selection.

   Note:

   The EPM stops the selected MPP server when the last active call completes or when the grace period expires, whichever condition is met first.
5. Click **Refresh** and verify that the **State** is **Stopped** for the MPP server.
6. If the MPP operational state:
   - Changes to **Stopped**, continue with this procedure.
   - Did *not* change, stop the `mpp` service.
7. Use the selection check box in the MPP server table to reselect the MPP server to take offline.
8. Click **Offline** in the **Mode Commands** group.
9. Click **Refresh** and verify that the **Mode** is **Offline**.

Stopping the MPP service

You must take the MPP offline using the EPM Web interface. However, if you cannot take the MPP service offline because the EPM is not communicating with the MPP, take the MPP offline by stopping the `mpp` service.

About this task

Use this procedure to take the MPP offline by stopping the `mpp` service.

Procedure

1. Log in to the MPP 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. Enter the `/sbin/service mpp stop` command.

Preventing loss of reporting data prior to upgrading MPP

Before you begin

Perform this procedure only if you plan to upgrade a system that is installed on a supported version of Red Hat Enterprise Linux Server.

Procedure

1. Schedule a report data download from the Report Data page of the EPM Web interface.
2. To determine that the report data download is complete, check the Log Viewer for the `Scheduled event completed` message.

Chapter 4: Software upgrade prerequisites

Prerequisites checklist for upgrading Experience Portal

Complete these tasks before you upgrade the Avaya Experience Portal software.

S.No	Description	Prerequisite applicable for	Notes	✔
	Ensure that you partition the hard drive in order to create the required space for the Experience Portal software installation.	All the Experience Portal components	See the partition requirements for the hard drive in *Administering Avaya Experience Portal*.	
	Ensure that you can access the Experience Portal site-specific licensing information from Avaya.	Primary EPM	See License Requirements on page 49.	
	Check to see if there are Experience Portal patches available on the Avaya support website. If patches are available, download the patches before you begin the software upgrade.	All the Experience Portal components. **Note:** Apply the patches after each EP component is upgraded.		

Table continues…

S.No	Description	Prerequisite applicable for	Notes	✔
	Verify that you can access all the target systems using at least one of the following methods: • _____ A computer on the customer's network that has an SSH client to reach the target system. • _____ A keyboard, monitor, and mouse attached directly to the target system. • _____ A cable that connects a second computer that has a keyboard, monitor, mouse, and an SSH client.	All the Experience Portal components		
	Take a backup of the Experience Portal data.	Primary EPM	See Backing up data on page 25.	
	Verify that the Linux operating system is upgraded.	All the Experience Portal components **Note:** Perform this task after the OS install/ update	See Verifying the Linux version number on page 50	
	To connect your Experience Portal system to an external Oracle database, you must install the Oracle JDBC driver.	Primary EPM Auxiliary EPM	See Installing Oracle JDBC driver on page 57.	
	Disable the firewall or anti-virus software on the target systems.	All the Experience Portal components **Note:** Perform this task after the OS Install/ Update		
	Set the default umask to 027.	Primary EPM Auxiliary EPM		

Table continues…

S.No	Description	Prerequisite applicable for	Notes	✔
	If you install the EPM software on a dedicated server, verify that the EPM server can communicate with all the MPP servers.	Primary EPM	See Verifying communication between the upgraded Experience Portal servers on page 51.	
	To ensure that the SMS and email messages are processed throughout the upgrade process, configure the SMS and email processors in your Experience Portal system.	Primary EPM Auxiliary EPM	See Ensuring new SMS and Email records are created after upgrades on page 53.	
	Ensure that you copy and restore the backup data to the Primary EPM.	Primary EPM **Note:** Perform this task after the OS Install/ Update	See Copying and restoring the backup files on page 64.	
	Ensure that none of the mount points are stale or hung.	All the Experience Portal components **Note:** Perform this task after the OS Install/ Update	See Checking for stale or hung mount points on page 54.	
	Verify that the time is synchronized between all the Experience Portal servers. **Important:** If the time is not synchronized between the EPM and MPP servers, the upgrade process might hang.	All the Experience Portal components **Note:** Perform this task after the OS Install/ Update	See Verifying server time synchronization on page 55.	

Table continues…

S.No	Description	Prerequisite applicable for	Notes	✔
	Ensure that you configure a yum respository containing all the required Experience Portal packages. Otherwise the prerequisite installation for the Experience Portal server may fail. This is required for Red Hat Enterprise Linux installations.	All the Experience Portal components		

Minimum server hardware requirements

Customer supplied servers must meet the following minimum specifications in order to run Avaya Experience Portal:

- Compatibility with a supported version of Red Hat Enterprise Linux Server

  For information about hardware compatibility, go to the *Certified Hardware* section of the Red Hat website, http://www.redhat.com.
- Dual Quad Core 1.6 GHz Pentium 4 or equivalent processors
- 4 GB of RAM
- 120 GB Disk, 7200 RPM
- One 100/1000 Base-T Ethernet controller that is full duplex (onboard Network Interface Cards (NICs)
- DVD drive
- Keyboard
- Monitor
- Mouse
- Avaya Secure Access Link (SAL) or Avaya EASG solution

  If you purchase a maintenance agreement with Avaya Services, the Experience Portal system requires SAL or Avaya EASG solution so that Avaya Services can remotely access the system for maintenance purposes. Contact Avaya Support to determine the version of SAL and Avaya EASG supported.

Disk space requirements

Space requirement for upgrading the primary EPM on Red Hat Enterprise Linux

While upgrading Experience Portal on Red Hat Enterprise Linux, the Experience Portal database upgrade uses approximately four times the size of the database backup. For example, a system

with a backup of 10 GB needs approximately 40 GB of free space to successfully upgrade the database.

To prevent upgrade failure due to space constraints, monitor and estimate hard disk space usage during the upgrade process. The system retains some of the files used in the upgrade process for backup. However, you may either delete these files, or move these files to a different location during or after the upgrade to maximize the available hard disk space. The following table describes some of the database files used during upgrade, their locations, their approximate sizes relative to the database backup, and if you can delete or relocate these files safely. Avaya recommends you to retain these files in a different partition or hard drive, for backup purpose.

Description	Location	Size compared to database backup	When it is safe to delete
Experience Portal backup file	You can select the location	–	You may delete this file after you run the script `RestoreProps.sh` successfully.
Database export file	`/var/lib/pgsql/vp_upgrade.export_vp_<date>` Where *<date>* is the date of installation.	Same as the database backup.	After the Experience Portal prerequisite installer successfully installs the updated PostgreSQL database. Ensure that the **PostgreSQL** field indicates **Success**.
Experience Portal database	`/var/lib/pgsql/data`	The size varies from 10% to 100% larger than the database backup directory.	Do not delete this directory. Deleting this directory causes loss of data.

Space requirement for upgrading the primary EPM on Avaya Enterprise Linux

While upgrading Experience Portal on Avaya Enterprise Linux, the Experience Portal database upgrade uses approximately 3.5 times the size of the database backup. For example, a system with a backup of 10 GB requires approximately 35 GB of free space in the `/var` partition for a successful upgrade.

Enter the command `du -sk /var/lib/pgsql/data/base` to determine the database size. The system displays the size of the database in kilobytes.

To prevent upgrade failure due to space constraints, monitor and estimate hard disk space usage during the upgrade process. The system retains some of the files used in the upgrade process for backup. However, you may either delete these files, or move these files to a different location during or after the upgrade to maximize the available disk space. The following table describes some of the database files used during upgrade, their locations, their approximate sizes relative to the database backup, and if you can delete or relocate these files safely. Avaya recommends you retain these files in a different partition or hard drive, for backup purpose.

Description	Location	Size compared to database	When it is safe to delete
Old Experience Portal database	`/var/lib/pgsql/data/base`	Approximately same as the database size	After OS upgrade, and before you run the `aepinstall` command. Ensure that the export file is present at `/var/lib/pgsql/vp_upgrade.export`. **Caution:** Do not move or delete this directory after you run the `aepinstall` command.
Database export file	`/var/lib/pgsql/vp_upgrade.export_vp_<date>` Where *<date>* is the date of installation.	Approximately same as the database size	After the Experience Portal prerequisite installer successfully installs the updated PostgreSQL database. Ensure that the **PostgreSQL** field indicates **Success**.

License Requirements

Before you configure Experience Portal, ensure that Avaya provides the following site-specific items:

- Product ID: The unique product ID for your site. The numeric identifier that Avaya must provide when the EPM software is installed.
- The Experience Portal license file: The file that determines the various licensed features and the capacity available to Experience Portal. For example, the license determines maximum number of telephony ports available to Experience Portal. The file also determines whether the speech applications in the system can use ASR or TTS resources, whether the system can process Email, HTML and SMS messages. You must install the license file on the Avaya WebLM server.

  Note:

  - Before you upgrade the Experience Portal system to a newer version, ensure that you have the license file with required version as per the compatibility matrix below. If you upgrade an Experience Portal system to a newer version and the license version being used is older, the system provides a grace period of 30 days. During the grace period, you must upgrade the license as per the compatibility matrix below; otherwise the system will no longer be functional once the license grace period ends.
  - Experience Portal 8.1.2 includes WebLM Server 8.1 which mandates EULA acceptance for all installed licenses. Prior releases of Experience Portal included older versions of WebLM Server which did not have support for EULA acceptance. As a result, after upgrade, WebLM Server 8.1 will not load any licenses which were installed

prior to upgrade and Experience Portal will go into 30 day grace period till the licenses are manually re-installed or updated.

- Installed licenses: All licenses that were installed on the WebLM Server which is co-resident with Primary EPM need to be re-installed.

  Note:

  The license files can be found on the Primary EPM under `$WEBLMSERVER_HOME/webapps/WebLM/licenses` folder.

- Allocated licenses: All licenses that were allocated to the WebLM Server which is co-resident with Primary EPM need to be re-allocated. To re-allocate the licenses, use one of the below options:
  - Wait for the Enterprise or Master WebLM to push the new allocation licenses as per the periodic license allocation schedule which happens on a weekly interval.
  - Change the periodic license allocation schedule on the Enterprise or Master WebLM for the Local WebLM, to the next closest hour. The Master WebLM then pushes the new allocation licenses to the Local WebLM as per the new schedule. Once the re-allocation occurs, you can update the periodic license allocation schedule as needed.
  - Delete the Local WebLM entry from the Enterprise or Master WebLM, add the Local WebLM again and push the required allocations.

The compatible versions of Experience Portal and WebLM licenses are:

Voice Portal/Experience Portal Version	License Version
Avaya Experience Portal 6.0.x	6
Avaya Experience Portal 7.x	7
Avaya Experience Portal 8.x	8

- If Avaya Services maintains the Experience Portal system, the Avaya Services representative must get the following:
  - The Avaya Service Account authentication file that you can use to create Avaya Service accounts after you install the Experience Portal software.
  - The Listed Directory Number (LDN) in the Avaya Services database for each EPM and MPP server, and each speech server.

Verifying the Linux version number

Procedure

1. On the Experience Portal server, log in to Linux as any user.

2. If you use:
   - Avaya Enterprise Linux Server, enter the `swversion` command to determine the version, and enter the `uname -m` command to determine the architecture.
     - The result must state the version is RHEL 7.x 64-bit or newer 7.x update, or RHEL 8.x 64-bit or newer update.
     - The architecture of Red Hat Enterprise Linux should be x86_64.
     - If you have an earlier version of Avaya Enterprise Linux Server, upgrade the operating system on the server.
   - Red Hat Enterprise Linux Server, enter the `rpm -q redhat-release-server` command to determine the version, and enter the `uname -m` command to determine the architecture.
     - The result must state the version is RHEL 7.x 64-bit or newer 7.x update, or RHEL 8.x 64-bit or newer update for upgrades.
     - The architecture of Red Hat Enterprise Linux should be x86_64.
     - If you have an earlier version of Red Hat Enterprise Linux Server, upgrade the operating system on the server.

Verifying communication between the upgraded Experience Portal servers

If EPM is running on a dedicated server, ensure that EPM can still communicate with all MPP servers, PBXs, and application servers using their IP addresses. Optionally, verify that the EPM can communicate with the servers using their host names.

Procedure

1. Log on to Linux on the Experience Portal Primary EPM server.
2. Verify the Primary EPM server's IP address and host name:
   a. Enter the `hostname -i` command.

      This command must return the server's IP address and not `127.0.0.1`. If this check fails, you must manually map the host names. For more information about the Prerequisite Checker failure with UnknownHostException:localhost, see *Implementing Avaya Experience Portal on multiple servers*.

   b. Enter the `hostname -s` command.

      This command must return the server's host name and not `localhost`. If this check fails, you must manually map the host names to connect the Primary EPM with other servers. For more information, see *Implementing Avaya Experience Portal on multiple servers*.

3. Verify that the Primary EPM server can communicate with all MPP servers:
   a. Enter the `ping -c 4 <mpp_hostname>` command, where:

      <mpp_hostname> is the hostname of the MPP server you are testing.

   b. Wait for the system to respond with the ping details.
   c. If this check fails, you must manually map the hostnames to connect the Primary EPM with other servers. For more information, see *Implementing Avaya Experience Portal on multiple servers*.
   d. If your Experience Portal system contains more than one MPP server, repeat this step for each MPP server.
4. If you have an Auxiliary EPM server, verify that the Primary EPM server can communicate with the Auxiliary EPM server:
   a. Enter the `ping -c 4 <auxiliary_vpms_hostname>` command, where:

      <auxiliary_vpms_hostname> is the hostname of the Auxiliary EPM server.

   b. Wait for the system to respond with the ping details.
   c. If the check fails, enter the `ping -c 4 <Auxiliary_vpms_ipaddress>` command, where:

      <Auxiliary_vpms_ipaddress> is the IP address of the Auxiliary EPM server.

   d. Wait for the system to respond with the ping details.
   e. If both the checks fail, you must manually map the host names.
5. Verify that the Primary EPM server can communicate with the external servers by host name or IP address:
   a. Enter the `ping -c 4 <server_hostname>` command, where:

      <server_hostname> is the hostname of the one of the following external components attached to your Experience Portal system:

      - A PBX server.
      - An application server.
      - A speech server.
      - Communication Manager.
      - Avaya SIP Enablement Services.

   b. Wait for the system to respond with the ping details.
   c. If this check fails, enter the `ping -c 4 <server_ipaddress>` command, where:

      <server_ipaddress> is the IP address of the server whose hostname you specified in the previous **`ping`** command.

   d. Wait for the system to respond with the ping details.

e. If either of these checks fail, you must manually map the hostnames to connect the Primary EPM server with the servers. For more information, see *Implementing Avaya Experience Portal on multiple servers*.

f. Repeat this procedure for each external server in your Experience Portal system.

Ensuring new SMS and Email records are created after upgrades

About this task

This procedure applies to any upgrade which involves a database restore that has SMS/Email call records.

Though the script is executed on the primary EPM, the script may need to be executed multiple times. You will need to specify different EPM names each time. The appropriate script needs to be executed once for each of the EPMs (both primary and auxiliary) in the system. If there is one primary EPM and two auxiliary EPMs, then the script needs to be executed three times- once for the primary EPM and twice for each of the auxiliary EPMs.

Note:

This procedure is not required if the user is upgrading from Avaya Experience Portal 6.x, since SMS/Email was not supported in that release.

Procedure

1. Ensure that you configure at least two SMS/Email processors.

   Note:

   An Experience Portal system that includes multiple zones, must have more than one processor.

2. On the EPM Web interface,
   - For Email records,
     - Click **Multi-Media Configuration** > **Email**.
     - Disable the email processor which is handling the email connections. This will ensure that the primary EPM automatically assigns any email connections to the other processors.
   - For SMS records,
     - Click **Multi-Media Configuration** > **SMS**.
     - Manually assign any SMPP connections that are assigned to the processor (that handles the connections) to some other SMS processor.
     - Disable the SMS processor after you assign the SMPP connections to some other SMS processor. To disable the processor, click on the processor and in the **Change Processor** page, select the **No** option in the **Enable** field.

3. Upgrade the primary or auxiliary EPM.
4. After you upgrade the primary or auxiliary EPM, enable the SMS/Email processor that you had disabled.

   Note:

   For SMS records, also re-assign the SMPP connection back to the SMS processor.

Next steps

To verify if the SMS/Email records are collected correctly in either the system monitor or the reports:

1. Run the **cd $AVAYA_HOME/Support/VP-Tools** command to navigate to the appropriate directory.
2. Run one of the following commands on the primary EPM for each configured EPM name that has a SMS/Email processor:
   - **ResetEmailSMSLocalDB <EPM_name>** command for local databases.
   - **./ResetEmailSMSExtDB "<Database_URL>" <JDBC_Driver> <Database_User_Name> <Experience_Portal_Name> <EPM_Name>** command for external databases.

     Where:

     - "<Database_URL>" is the URL of the external database as it appears on the **Report Database Settings** page of the EPM Web interface.

       Important:

       Put quotation marks around the URL.

     - <JDBC_Driver> is the JDBC driver for the external database as it appears on the **Report Database Settings** page of the EPM web interface.
     - <Database_User_Name> is the user name for the external database as it appears on the **Report Database Settings** page of the EPM web interface.
     - <Experience_Portal_Name> is the name of the Experience Portal system as it appears on the **EPM Settings** page of the EPM web interface.
     - <EPM_name> is the name of the Primary or Auxiliary EPM as it appears on the **EPM Servers** page of the EPM web interface.

Checking for stale or hung mount points

About this task

If you have file systems saved on the Experience Portal servers, check if the mount points are stale or hung. Stale or hung mount points can cause RPM installations to not respond while installing the Experience Portal software. Use this procedure to check for stale or hung mount points on the Experience Portal servers.

Procedure

1. On the Experience Portal server, log in to Linux as any user.
2. Enter the `df` command.

   If the server:

   - Responds to the command: The mount points are working.
   - Does not respond to the command: The mount point is stale or is not responding.

   Note:

   Run the `umount` command to unmount any stale or hung mount points.

Verifying server time synchronization

After you upgrade the operating systems on all Experience Portal servers, you must ensure that the time on all servers is synchronized.

About this task

Use this procedure to ensure that the time on all servers is synchronized.

Note:

Experience Portal only requires that the EPM and MPP servers are synchronized. However, you can also synchronize the servers that Experience Portal connects to, including the Application server, speech servers, and the PBX. For more information, see External time sources on page 93.

Procedure

1. On each Experience Portal server, in the same time frame, run the `date` command.
2. Verify that all Experience Portal servers report the time within a few seconds of each server response. If there is a time difference, verify that the planned MPP servers lag behind the planned EPM server.

   For example, an MPP server time of 2:10:00 and a EPM server time of 2:10:03 is acceptable.
3. If one or more servers differ by more than a few seconds, set the appropriate date and time by running the `date` *`MMDDhhmmYY.ss`* command, where *`MMDDhhmmYY.ss`* is the two-digit month, day, hour, minute, year, and seconds you want to set based on the 24-hour clock.

   For example, to set the date to 2:15:35 p.m. on March 31, 2008, you must enter `date 0331141508.35`.

Updating the external database configuration

If this Experience Portal system is connected to an external database, you must update the external database before you upgrade the EPM software. The older EPM software will continue to operate against the updated database.

About this task

Use this procedure to update the external database configuration.

Note:

The external reporting database schema is updated in Experience Portal 8.1. If you are upgrading from 7.0, run the appropriate script to add 7.1 columns, and then run the script to add 7.2 columns. Finally, run the script to add 8.1 columns.

The .sql files are located in the directory `/Support/ExternalDB/<DBVENDOR>/UpgradeScripts`. Where, <DBVENDOR> can be Oracle, Postgres, MSSQL, or MySQL.

Note:

The administration and maintenance of the external database is a customer responsibility.

Procedure

1. Insert the Experience Portal installation DVD in to the DVD device of the server on which the external database resides.
2. Based on the external database and the upgrade scenario, run the required scripts:
   a. If you use Oracle:
      - For a 7.2/8.0 to 8.1 upgrade scenario, run the **`Oracle_New_Columns_81.sql`** script.
      - For a 7.1 to 7.2 upgrade scenario, run the **`Oracle_New_Columns_72.sql`** script.
      - For a 7.0 to 7.1 upgrade scenario, run the **`Oracle_New_Columns_71.sql`** script.
      - For a 6.0 to 7.1 upgrade scenario, run the **`Oracle_New_Columns_70.sql`** script first and then run the **`Oracle_New_Columns_71.sql`** script.
   b. If you use an external Postgres server:
      - For a 7.2/8.0 to 8.1 upgrade scenario, run the **`New_Columns_81.sql`** script.
      - For a 7.1 to 7.2 upgrade scenario, run the **`New_Columns_72.sql`** script.
      - For a 7.0 to 7.1 upgrade scenario, run the **`New_Columns_71.sql`** script.
      - For a 6.0 to 7.1 upgrade scenario, run the **`NewColumns_70.sql`** script first and then run the **`New_Columns_71.sql`** script.
   c. If you use Microsoft SQL server:
      - For a 7.2/8.0 to 8.1 upgrade scenario, run the **`MSSQL_New_Columns_81.sql`** script.

- For a 7.1 to 7.2 upgrade scenario, run the **MSSQL_New_Columns_72.sql** script.
- For a 7.0 to 7.1 upgrade scenario, run the **MSSQL_New_Columns_71.sql** script.
- For a 6.0 to 7.1 upgrade scenario, run the **MSSQL_New_Columns_70.sql** script first and then run the **MSSQL_New_Columns_71.sql** script.

d. If you use MySQL or MariaDb:

- For a 7.2/8.0 to 8.1 upgrade scenario, run the **MSSQL_81.sql** script.
- For a 7.1 to 7.2 upgrade scenario, run the **MSSQL_72.sql** script.
- For a 7.0 to 7.1 upgrade scenario, no upgrade steps are required.
- MySQL was not supported in 6.0.

Important:

For Microsoft SQL Server, the database user name for Experience Portal must be assigned SELECT, INSERT, UPDATE, DELETE privileges on the newly added VPZones table.

For Postgres, the database user name for Experience Portal must be assigned CONNECT, TEMPORARY ON DATABASE, SELECT, INSERT, UPDATE and DELETE privileges on the newly added VPZones table.

Installing the Oracle JDBC driver

About this task

This procedure only applies to installing Oracle JDBC driver as all other supported database drivers are packaged with Experience Portal.

To have the Oracle JDBC driver installed by the Experience Portal install program, perform the following steps after you install or upgrade Linux. It is recommended that you perform the procedure before you install or upgrade Experience Portal.

The procedure also provides information on how to install the Oracle JDBC driver after you install or upgrade Experience Portal.

Before you begin

To connect your Experience Portal system to an external Oracle database, you must first obtain the JDBC driver from Oracle. The Oracle JDBC driver is not shipped with Experience Portal.

Experience Portal is tested with the following Oracle Releases:

- Oracle 11g Release 2: Download the Oracle JDBC driver from http://www.oracle.com/technetwork/apps-tech/jdbc-112010-090769.html. Download files ojdbc6.jar and orai18n.jar.
- Oracle 12c Release 2 (12.2.0.1): Download the Oracle JDBC driver and UCP downloads from http://www.oracle.com/technetwork/database/features/jdbc/jdbc-ucp-122-3110062.html.
- Oracle 21c (21.1): Download the Oracle JDBC driver and UCP downloads from https://www.oracle.com/database/technologies/appdev/jdbc-ucp-21-1-c-downloads.html. Ensure that

you download the ojdbc8.jar and orai18n.jar files, rather than the ojdbc11.jar file. The ojdbc8.jar and orai18n.jar files support the Java version used by your Experience Portal system.

Important:

Web browsers might change the file extension of the files to .zip when the files are downloaded. Rename the files back to ojdbc6.jar, ojdbc7.jar, ojdbc8.jar, and orai18n.jar.

Avaya recommends the following for better results:

- Use Oracle 11g drivers when you are upgrading to Experience Portal 8.x and connecting to an Oracle 11g database.
- Use Oracle 12c drivers for fresh installation of Experience Portal 8.x and connecting to either an Oracle 11g or 12c database.
- Use Oracle 21c drivers when you are upgrading to Experience Portal 8.x and connecting to an Oracle database greater than 12c.

Procedure

1. Log in to Linux on the Primary Experience Portal server as a root user.
2. Run the **`mkdir ~/OracleJDBC`** command to create the `~/OracleJDBC` folder.
3. Copy the `ojdbc6.jar/ojdbc7.jar/ojdbc8.jar` and `orai18n.jar` driver files to the `~/OracleJDBC` folder.

   Important:

   Do not delete the Oracle JDBC driver files from the `~/OracleJDBC` directory after you install or upgrade Experience Portal. You will need the files if you reinstall or upgrade Experience Portal.
4. If you install the Oracle JDBC driver after you install or upgrade the Experience Portal server, you must do the following:
   a. Run the **`/sbin/service vpms stop`** command to stop the vpms service.
   b. Run the **`cd $AVAYA_HOME/Support/Database`** command to navigate to the appropriate directory.
   c. Run the **`bash InstallOracleJDBC.sh`** command to install the JDBC driver.

      Important:

      Run the **`InstallOracleJDBC.sh`** command only after you download the Oracle driver in the `~/OracleJDBC` directory on the server.
   d. Run the **`/sbin/service vpms start`** command to start the vpms service.
5. Repeat the procedure on each Auxiliary Experience Portal server.

Chapter 5: Upgrading the EPM and MPP software on different servers

Upgrading the Primary EPM server

EPM software upgrade overview

When you install the EPM software, Experience Portal automatically records your answers to basic questions, such as what installation directory you want to use, the name of the EPM server, and what security certificate you want to use. EPM compiles the answers into a file. You can use the file later to upgrade the MPP software using the silent install option. This MPP upgrade option allows you to upgrade with very little user input.

Local WebLM license invalidated in upgrades from AEP 8.0/8.1/8.1.1 to AEP 8.1.2

For upgrades from AEP 8.0/8.1/8.1.1 to AEP 8.1.2 (or later), WebLM is upgraded from 7.1 to 8.1. When the WebLM is upgraded, the WebLM host ID changes, which in turn invalidates the current WebLM AEP license and sets the WebLM UI admin password back to the default value. Any added WebLM users are also deleted.

Licensing enters a 30 day grace mode. Avaya must generate a new license by using the new host ID. The old license file is stored in the `/opt/Avaya/InstallLogs/WebLM71/OldLicense` directory.

Interactive EPM upgrade

You can upgrade to Experience Portal 8.1 using the Manual or Interactive upgrade method.

On the EPM server, launch the Experience Portal installation program and answer the prompts.

During the Interactive upgrade, you can make changes to the configurations.

Tip:

In Experience Portal 7.0.1, the certificate generation code was enhanced to use a more secure hashing algorithm. Avaya recommends that you generate a SHA256 2048 bit server certificate (the new security certificate) to make the systems more secure.

Upgrading the Primary EPM software interactively

Before you begin

- Ensure that you upgrade the operating system on the server as described in Operating system upgrade overview on page 20.

- Complete the Primary EPM server upgrade worksheet on page 112 and have it available to help answer the questions raised during the installation.
- Before you install the software, read the Avaya Experience Portal Release notes on the Avaya Support site. These release notes contain information about the product that is not included in the formal documentation set.
- If upgrading from Avaya Experience Portal 6.x or 7.x, ensure that you have staged the required files as mentioned in Staging the Experience Portal 6.x or 7.x backup files on the Primary EPM before upgrading Experience Portal on page 27.
- Download any patches for Avaya Experience Portal Release 8.1 from the Avaya Support website at http://support.avaya.com.
- Ensure that you have completed the software upgrade prerequisites described in Prerequisites checklist for upgrading Experience Portal on page 44.
- For disk space related information, see Space requirement for upgrading primary EPM on Red Hat Enterprise Linux on page 47 and Space requirements for upgrading primary EPM on Avaya Enterprise Linux on page 48.
- If you have installed a managed application, contact the provider of the managed application to check if you need to perform any additional steps as part of the Experience Portal upgrade.

Note:

You can run the prerequisite installer before installing Experience Portal. For more details, see Platform Vendor Independent Check on page 22

Procedure

1. Log in to the server on which you want to upgrade the Experience Portal software.

   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.

   Note:

   Ensure that you upgrade using the same Linux account that was used during the prior installation. If you upgrade an Experience Portal system by using a Linux account that is different than the account used during the previous install or upgrade, the upgrade might fail.

   This applies to RHEL (software-only) customers. It does not apply to the root and sroot users in Avaya Linux.

Note:

By default, the craft and sroot users are disabled in Avaya Experience Portal 8.1 Avaya Enterprise Linux fresh installations. Avaya Service Login accounts can only access the Avaya Experience Portal system if they are EASG protected.

2. Insert the Avaya Experience Portal 8.1 software installation DVD into the DVD drive of the server.

Tip:

These instructions assume that you are going to access the Experience Portal installation DVD by mounting the appropriate DVD drive on the target system. If you want to access the installation DVD files from a shared network directory or a local directory, you can copy the Experience Portal installation ISO image to that directory. However, that directory must be readable by all users on the system. If the directory is only readable for root users, the installation script will encounter errors and will not complete successfully.

3. Mount the Avaya Experience Portal 8.1 software installation DVD. The **mount** command depends on the server's hardware and operating system.
   - If you are working with Avaya Enterprise Linux, mount the DVD by entering the `mount /mnt/cdrom` command, where `/mnt/cdrom` is the mount point typically associated with the DVD drive in the `fstab` file.
   - If you are working with a supported version of Red Hat Enterprise Linux Server, to mount the DVD:
     - Run the `mkdir -p /media/cdrom` command.

       Note:

       This command is required only if the /media/cdrom mount point does not exist.
     - Run the `mount -o ro /dev/cdrom /media/cdrom` command.

     Warning:

     When Red Hat Enterprise Linux Server automatically mounts the DVD, the files on the DVD are not executable. You must manually mount the Experience Portal installation DVD using the commands shown above.
4. Change to the mount point directory.
5. Enter the `bash aepinstall.sh` command and press `Enter` to start the installation script.

   The `bash aepinstall.sh` script checks to make sure the calling user has root privileges.
6. Press **Enter** to continue.
7. Read through the end user license agreement and select **Y** to accept the terms of the license agreement.

Experience Portal automatically starts the PVI checker, which analyzes your system's hardware and operating system configuration. The PVI checker does the following:

- Checks to ensure that a non-root user account has been created.
- Asks the user to confirm that one of these accounts is the non-root account the user has configured, and to set the password.
- Checks for any missing pre-requisite RPMs and installs any if missing.
- Creates a log file in `/opt/Avaya/InstallLogs/pvicheck.log`.
- Checks if default umask is set to `027`. If it is not set to `027`, the installer asks if you want to set it to `027`. If you select 'yes', the installer applies this setting to the OS. If you select 'no', the installer exits.

8. After the configuration analysis is complete, the PVI checker displays a message stating whether all prerequisite checks passed followed by the first Prerequisite Status page.
9. Press `Enter` to end the installation script.

   During the installation process, Experience Portal creates several log files that you can use to verify what happened during installation. When the installation process is complete, Experience Portal moves these logs to the standard log directory and displays the exact path on the screen. You can view the detailed logs at `$AVAYA_HOME/logs/install_<date>`.
10. Experience Portal begins installing the software. During the install, it displays messages indicating its progress.

    The installation process can appear completed or stopped even though it is still processing and installing the software.

    Please wait until the `aepinstall.sh` script completes installing and displays the message:

    ```
    20210402-17:15:15 Finished Installation
    ```

    The aepinstall.sh script creates a log file at `/opt/Avaya/InstallLogs/aepinstall.log`
11. To unmount and eject the DVD:
    a. Change the directory to a location that is outside the mount point. For example, enter the `cd /` command to change to the root directory.
    b. Unmount the DVD as described in the server documentation.
    c. To eject the Experience Portal installation DVD, press the button on the DVD drive or enter the `eject` command.
12. Check the status of the vpms service and all other services by running the following command:

    `systemctl is-active vpms tomcat sl activemq httpd postgresql epmcompmgr`

A list appears for each service. If the vpms service is running properly, the command displays `active` for all the services in the list.

Next steps

- To verify if the installation or upgrade was successful, go to `http://EPM-Server/VoicePortal` and log into the Experience Portal web interface.

  Where, `EPM-server` is the hostname or the IP address of the system where the primary EPM logon using EPM Administrator account.
- Install any required patches that you download from the Avaya online support website, http://support.avaya.com.
- If upgrading from Experience Portal 6.x or 7.x, establish whether a new EP Signing Certificate needs to be generated:
  - In the EPM web interface, navigate to **Security** > **Certificates** > **EP Signing Certificate**.
  - Inspect the **Security Certificate** > **Basic Constraints** > **CA entry**. If the CA entry is set to *false* then do the following:
    - Create a new EP Signing Certificate: Navigate to **Security** > **Certificates** > **EP Signing Certificate** > **Certificate** tab and select **Generate**.
    - Manually reboot the EPM: SSH onto the EPM server and initiate a reboot via the Linux command line For example, reboot.
    - Remove and re-add the MPP server, using the same name and IP. After the MPP is added, select the **Trust new certificate** option.
    - Click **Save**.
- To use an EPM 8.1 server with an older version of MPP server, run the setup_vpms.php script on the MPP server to authorize the security certificate, and restart the MPP.
- Reestablish the link between the MPP and the EPM as described in Reestablishing the link between the EPM and the MPP on page 79.
- Navigate to the **MPP Manager** page in EPM and restart the MPPs
- If the Auxiliary EPM has outcalls in progress, do not run setup_vpms.php script on the Auxiliary EPM server.
- Upgrade the Auxiliary EPM. For more information, see Auxiliary EPM software upgrade overview on page 65.
- **Important:**

  If you are running outcalls during the upgrade, you must upgrade the Auxiliary EPM before upgrading the MPPs.
- If you wish to change the postgres database password specified by the upgrade utility, run the SetDbPassword.sh script.

  Important:

  If Proactive Outreach Manager is installed on this system, then you must run the script SetDbPassword.sh to change the password for the database user postgres. The Experience Portal upgrade program automatically generates a new password for the

database user postgres. However, Proactive Outreach Manager is already configured to use the old password. To keep Proactive Outreach Manager working, you must change the password for the database user postgres back to the value that you have configured in Proactive Outreach Manager. For more information about configuring the PostgreSQL database user accounts, see *Administering Avaya Experience Portal*.

- Experience Portal 7.2.0.0.x and 7.1.0.0.x includes WebLM Server 7.0 which mandates EULA acceptance for all installed licenses. Due to this, WebLM licenses will need to be re-installed or re-allocated if the system that was upgraded was using a co-residing WebLM server and an Experience Portal version older than 7.1.0.0.x.

Copying and restoring the backup files

Before you begin

- Install a supported version of Red Hat Enterprise Linux Server on the server as described in Operating system upgrade overview on page 20.
- Upgrade the Primary EPM server as described in Upgrading the Primary EPM software interactively on page 59.
- Ensure that you have the location details of the Experience Portal backup files.

Note:

This procedure is applicable only for the Primary EPM server.

Procedure

1. Log in to the server locally as root, or log in remotely as a non-root user and change the user to root by running the su - command.
2. Copy the backup package created before the upgrade to a temporary location on the local hard drive.

   Note:

   This step is applicable only if you did not complete Staging the Experience Portal 6.x or 7.x backup files on the Primary EPM before upgrading Experience Portal on page 27 prior to running the aepinstall.sh script.

   The folder name of backup packages created by Voice Portal is `pkgVP<Version>_<XXXXXXXXXXXXX>` and the folder name for backup packages created by Experience Portal is `pkgEP<Version>_<XXXXXXXXXXXXX>`. Where,

   - `<Version>` is the version number of the software that the backup was created with.
   - `<XXXXXXXXXXXXX>` is a 13 digit timestamp that is not in a human readable format.

   Note:

   The Experience Portal installation script identifies the Experience Portal version and the configuration information available on the server based on the folder name.
3. Restore the database backup.

Note:

This step is applicable only if you did not complete Staging the Experience Portal 6.x or 7.x backup files on the Primary EPM before upgrading Experience Portal on page 27 prior to running the aepinstall.sh script.

For details on *Database Restore Utility*, see *Administering Avaya Experience Portal*

Note:

Restoring the database is applicable to both Red Hat Enterprise Linux and Avaya Enterprise Linux upgrades.

4. If you have previously changed the **Session timeout (minutes)** field in **Home** > **User Management** > **Login Options**, update this field again.

   For more information, see *Administering Avaya Experience Portal*.

5. If you have previously changed the **Purge and Retention** field in **Home** > **System Configuration** > **EPM Servers** > **Alarm/Log Options**, update this field again.

   For more information, see *Administering Avaya Experience Portal*.

6. If you have previously enabled **Organizations** for the system, re-enable it by executing the following script:

   ```
   $AVAYA_HOME/Support/VP-Tools/EnableOrganizations
   ```

   For more information on *Enabling organization level access in Experience Portal*, see *Administering Avaya Experience Portal*.

7. If you are restoring a co-resident application server on the Experience Portal server, follow the steps in Optional: Updating the co-resident application server on page 81.

   Note:

   For major version upgrades of Tomcat, it is also recommended that the deployed applications and application support runtime libraries are re-generated for the updated version of Tomcat.

8. If you have previously deployed and configured any Managed Applications, re-install and deploy the managed application.

Upgrading an Auxiliary EPM server

Auxiliary EPM software upgrade overview

Interactive EPM upgrade

You can upgrade to Experience Portal 8.1 using the Manual or Interactive upgrade method.

On the Auxiliary EPM server, launch the Experience Portal installation program and answer the prompts.

Important:

Upgrade the Primary EPM server before the Auxiliary EPM server. While upgrading the Auxiliary EPM server, you are prompted for the following details related to the Primary EPM server:

- IP address of the Primary EPM server so that the system can retrieve the security certificate. To ensure that the system retrieves the updated certificate from the Primary server, upgrade the Primary server first.
- The vpcommon password that was specified during the Primary EPM upgrade. This user account allows the Auxiliary EPM server limited access to the main Experience Portal database.

During the Interactive upgrade, you can make changes to the configurations.

Upgrading the Auxiliary Experience Portal software interactively

Before you begin

- Upgrade the Primary EPM server before you upgrade the Auxiliary EPM server.
- Complete the Auxiliary EPM server upgrade worksheet on page 116 and have it available to help answer the questions raised during the upgrade.
- Before you install the software, read the Avaya Experience Portal Release notes on the Avaya Support site. These release notes contain information about the product that is not included in the formal documentation set.
- If upgrading from Avaya Experience Portal 6.x or 7.x, the upgrade is treated as a fresh install where the same IP and Auxiliary EPM name, used in Avaya Experience Portal 6.x or 7.x, must be configured.
- If upgrading from Avaya Experience Portal 6.x or 7.x, it is important to know the Primary EPM password for the vpcommon database account. This password is provided during the original installation of the primary EPM. If the password is *not* known, you need to reset the password before upgrading the Auxiliary EPM. For more information on resetting the password, see the *Changing PostgreSQL user account passwords* section in the *Administering Avaya Experience Portal* document.
- Download any patches for Avaya Experience Portal Release 8.1 from the Avaya Support website at http://support.avaya.com.
- Ensure that you upgrade the server operating system as described in Operating system upgrade overview on page 20.
- Ensure that you complete the software upgrade prerequisites described in Prerequisites checklist for upgrading Experience Portal on page 44.
- If you have installed a managed application, contact the provider of the managed application to check if you need to perform any additional steps as part of the Experience Portal upgrade.
- Ensure that you download the Avaya Experience Portal ISO file from the Avaya Support web site and burn it to a DVD if required.

Procedure

1. Log in to the server on which you want to upgrade the Auxiliary EPM software.

   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.

   Note:

   Ensure that you upgrade using the same Linux account that was used during the prior installation. If you upgrade an Experience Portal system by using a Linux account that is different than the account used during the previous install or upgrade, the upgrade might fail.

   This applies to RHEL (software-only) customers. It does not apply to the root and sroot users in Avaya Linux.

2. Insert the Avaya Experience Portal 8.1 software installation DVD into the DVD drive of the server.

   Tip:

   These instructions assume that you are going to access the Experience Portal installation DVD by mounting the appropriate DVD drive on the target system. If you want to access the installation DVD files from a shared network directory or a local directory, you can copy the Experience Portal installation ISO image to that directory. However, that directory must be readable by all users on the system. If the directory is only readable for root users, the installation script will encounter errors and will not complete successfully.

3. Mount the Avaya Experience Portal 8.1 software installation DVD. The **`mount`** command depends on the server's hardware and operating system.

   - If you are working with Avaya Enterprise Linux, mount the DVD by entering the `mount /mnt/cdrom` command, where `/mnt/cdrom` is the mount point typically associated with the DVD drive in the `fstab` file.
   - If you are working with a supported version of Red Hat Enterprise Linux Server, to mount the DVD:
     - Run the `mkdir -p /media/cdrom` command.

       Note:

       This command is required only if the /media/cdrom mount point does not exist.

     - Run the `mount -o ro /dev/cdrom /media/cdrom` command.

Warning:

When Red Hat Enterprise Linux Server automatically mounts the DVD, the files on the DVD are not executable. You must manually mount the Experience Portal installation DVD using the commands shown above.

4. Change to the mount point directory.
5. Enter the `bash aepinstall.sh` command and press `Enter` to start the installation script.

   The `bash aepinstall.sh` script checks to make sure the calling user has root privileges.
6. Press **Enter** to continue.
7. Read through the end user license agreement and select **Y** to accept the terms of the license agreement.

   Experience Portal automatically starts the PVI checker, which analyzes your system's hardware and operating system configuration. The PVI checker does the following:

   - Checks to ensure that a non-root user account has been created.
   - Asks the user to confirm that one of these accounts is the non-root account the user has configured, and to set the password.
   - Checks for any missing pre-requisite RPMs and installs any if missing.
   - Creates a log file in `/opt/Avaya/InstallLogs/pvicheck.log`.
   - Checks if default umask is set to `027`. If it is not set to `027`, the installer asks if you want to set it to `027`. If you select 'yes', the installer applies this setting to the OS. If you select 'no', the installer exits.
8. After the configuration analysis is complete, the PVI checker displays a message stating whether all prerequisite checks passed followed by the first Prerequisite Status page.
9. Press `Enter` to end the installation script.

   During the installation process, Experience Portal creates several log files that you can use to verify what happened during installation. When the installation process is complete, Experience Portal moves these logs to the standard log directory and displays the exact path on the screen. You can view the detailed logs at `$AVAYA_HOME/logs/install_<date>`.
10. Experience Portal begins installing the software. During the install, it displays messages indicating its progress.

    The installation process can appear completed or stopped even though it is still processing and installing the software.

    Please wait until the `aepinstall.sh` script completes installing and displays the message:

```
20210402-17:15:15 Finished Installation
```

The aepinstall.sh script creates a log file at `/opt/Avaya/InstallLogs/aepinstall.log`

11. To unmount and eject the DVD:
    a. Change the directory to a location that is outside the mount point. For example, enter the `cd /` command to change to the root directory.
    b. Unmount the DVD as described in the server documentation.
    c. To eject the Experience Portal installation DVD, press the button on the DVD drive or enter the `eject` command.
12. Load the environment variables created during the installation by logging out of Linux and then logging back in.
    a. Log out of the Linux system.
    b. Log back in to the Linux system.
       - 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 enter the `su - root` command.
13. Check the status of the vpms service and all other services by running the following command:

    `systemctl is-active vpms tomcat sl activemq`

    A list appears for each service. If the vpms service is running properly, the command displays `active` for all the services in the list.

Next steps

- To verify if the installation or upgrade was successful, go to `http://EPM-Server/VoicePortal` and log into the Experience Portal web interface.

  Where, `EPM-server` is the hostname or the IP address of the system where the primary EPM logon using EPM Administrator account.
- Install any required patches that you download from the Avaya online support website, http://support.avaya.com.
- Do the following to re-establish the link between the Primary EPM and the Auxiliary EPM:

  Note:

  If you are upgrading from Avaya Experience Portal 6.x or 7.x, the trust relationship may already be established, therefore the following steps may not be required.

  1. Log in to the EPM web interface using an account with the Administration user role.
  2. On the EPM main menu, click **System Configuration** > **EPM Servers**.
  3. Click the name of the Auxiliary EPM server.
  4. 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.

5. Click **Save**.

- Upgrade the MPP software on the MPP servers as described in Upgrading the MPP software interactively on page 71.

  Note:

  If you log in to the upgraded EPM before you upgrade the MPPs, all MPPs in the system might display **Restart Needed** in the **State** column on the System Monitor and MPP Manager pages. EPM automatically updates the state after you upgrade the MPP software and reconnect the upgraded MPP servers with the EPM.

- Install the Avaya Service Account authentication file. For more information about installing the Avaya Service Account authentication file, see *Troubleshooting Avaya Experience Portal*.
- If you see a `Restart Needed` status on the EPM Manager page, do the following:
  - Run the **`/opt/Avaya/ExperiencePortal/Support/Security-Tools/SetDbPassword.sh`** script on the Auxiliary EPM.
  - Update the password for the vpcommon user of the Primary EPM by running the `update_primary_vpcommon` option.

Upgrading the MPP software

MPP software upgrade overview

Interactive MPP upgrade

After you upgrade the Primary EPM and all Auxiliary EPMs, upgrade the MPP.

On each server, launch the Experience Portal installation program and type the responses to the prompts. The procedure is similar to the interactive EPM software upgrade. For details, see Upgrading the MPP software interactively on page 71.

During the Interactive upgrade, you can make changes to the MPP configurations.

Tip:

In Experience Portal 7.0.1, the certificate generation code was enhanced to use a more secure hashing algorithm. Avaya recommends that you generate a SHA256 2048 bit server certificate (the new security certificate) to make the systems more secure.

Important:

Experience Portal provides the functionality to use an EPM 8.1 server with an already provisioned 7.2.3 MPP. However, it does not support adding an MPP that is at an earlier version to an EPM that is already upgraded to Experience Portal 8.1. If your system is configured to use more than one MPP, you can ensure that while you upgrade an MPP to 8.1, the other existing MPPs (of earlier versions) are functional. If the Experience Portal 8.1 EPM created a new server certificate during the upgrade, you must run the `setup_vpms.php` script on the MPP 7.2.3 server, trust the new certificate on the **Change MPP** page, and restart the MPP.

Upgrading the MPP software interactively

Before you begin

- Ensure that you have upgraded the EPM software on the Primary EPM server as described in EPM software upgrade overview on page 59.
- Ensure that you have upgraded the Auxiliary EPM software on the Auxiliary EPM server as described in Auxiliary EPM software upgrade overview on page 65.
- If upgrading from Avaya Experience Portal 6.x or 7.x, the upgrade is treated as a fresh install where the same IP and MPP name, used in Avaya Experience Portal 6.x or 7.x, must be configured in the Primary EPM UI.
- Download any patches for Avaya Experience Portal Release 8.1 from the Avaya Support website at http://support.avaya.com.
- Complete the MPP server upgrade worksheet on page 119 and have it available to help answer the questions raised during the installation.
- Ensure that the MPP server is offline.
- Ensure that you have upgraded the server operating system as described in Operating system upgrade overview on page 20.
- Prior to running the upgrade for an EPM, verify that the prerequisites have been met. For more information, see Prerequisites overview for upgrading Experience Portal on page 44.

Note:

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

Procedure

1. Log into the server on which you want to upgrade the MPP software.

   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. Insert the Avaya Experience Portal 8.1 software installation DVD into the DVD drive of the server.

   Tip:

   These instructions assume that you are going to access the Experience Portal installation DVD by mounting the appropriate DVD drive on the target system. If you want to access the installation DVD files from a shared network directory or a local directory, you can copy the files from the Experience Portal installation DVD to that

directory. However, that directory needs to be readable by all users on the system because the Experience Portal installation script changes users during the install procedure. If the directory is only readable by the root or sroot user, the installation script encounters errors and does not complete successfully. You must ensure that the directory name does not contain spaces. If there are spaces in the directory name, the installation script encounters errors and does not complete successfully.

3. Mount the Avaya Experience Portal 8.1 software installation DVD. The **mount** command depends on the server's hardware and operating system.
   - If you are working with Avaya Enterprise Linux, mount the DVD by entering the `mount /mnt/cdrom` command, where `/mnt/cdrom` is the mount point typically associated with the DVD drive in the `fstab` file.
   - If you are working with a supported version of Red Hat Enterprise Linux Server, to mount the DVD:
     - Run the `mkdir -p /media/cdrom` command.

       Note:

       This command is required only if the /media/cdrom mount point does not exist.

     - Run the `mount -o ro /dev/cdrom /media/cdrom` command.

     Warning:

     When Red Hat Enterprise Linux Server automatically mounts the DVD, the files on the DVD are not executable. You must manually mount the Experience Portal installation DVD using the commands shown above.
4. Change to the mount point directory.
5. Enter the `bash aepinstall.sh` command and press `Enter` to start the installation script.

   The `bash aepinstall.sh` script checks to make sure the calling user has root privileges.
6. Press **Enter** to continue.
7. Read through the end user license agreement and select **Y** to accept the terms of the license agreement.

   Experience Portal automatically starts the PVI checker, which analyzes your system's hardware and operating system configuration. The PVI checker does the following:
   - Checks to ensure that a non-root user account has been created.
   - Asks the user to confirm that one of these accounts is the non-root account the user has configured, and to set the password.
   - Checks for any missing pre-requisite RPMs and installs any if missing.
   - Creates a log file in `/opt/Avaya/InstallLogs/pvicheck.log`.

- Checks if default umask is set to `027`. If it is not set to `027`, the installer asks if you want to set it to `027`. If you select 'yes', the installer applies this setting to the OS. If you select 'no', the installer exits.

8. After the configuration analysis is complete, the PVI checker displays a message stating whether all prerequisite checks passed followed by the first Prerequisite Status page.
9. Press `Enter` to end the installation script.

   During the installation process, Experience Portal creates several log files that you can use to verify what happened during installation. When the installation process is complete, Experience Portal moves these logs to the standard log directory and displays the exact path on the screen. You can view the detailed logs at `$AVAYA_HOME/logs/install_<date>`.
10. Experience Portal begins installing the software. During the install, it displays messages indicating its progress.

    The installation process can appear completed or stopped even though it is still processing and installing the software.

    Please wait until the `aepinstall.sh` script completes installing and displays the message:

    ```
    20210402-17:15:15 Finished Installation
    ```

    The aepinstall.sh script creates a log file at `/opt/Avaya/InstallLogs/aepinstall.log`
11. To unmount and eject the DVD:
    a. Change the directory to a location that is outside the mount point. For example, enter the `cd /` command to change to the root directory.
    b. Unmount the DVD as described in the server documentation.
    c. To eject the Experience Portal installation DVD, press the button on the DVD drive or enter the `eject` command.
12. To verify that chronyd is operating properly, enter the `chronyc tracking` command.

    The system displays a status message similar to the following:

    ```
    Reference ID    : 0A868E42 (10.134.142.66)
    Stratum         : 4
    Ref time (UTC)  : Thu Sep 17 12:47:44 2020
    System time     : 0.000000488 seconds fast of NTP time
    Last offset     : +0.000008485 seconds
    RMS offset      : 0.000039525 seconds
    Frequency       : 24.108 ppm slow
    Residual freq   : +0.001 ppm
    Skew            : 0.030 ppm
    Root delay      : 0.147401720 seconds
    Root dispersion : 0.003942181 seconds
    Update interval : 1037.7 seconds
    Leap status     : Normal
    ```

    Verify that the Reference ID points to the Primary EPM server.

Next steps

- Install any required patches that you download from the Avaya online support website, http://support.avaya.com.
- Reestablish the connection between the upgraded MPP and the EPM server as described in Reestablishing the link between the EPM and the upgraded MPP on page 74.
- If required, upgrade the MPP software on another server machine by repeating this procedure on that machine.
- Configure and test the Experience Portal system. For more information, see Avaya Experience Portal system configuration checklist for a system upgraded to 8.1 on page 84.

Reestablishing the link between the EPM and the upgraded MPP

After you upgrade the MPP software, you need to reestablish the link between the MPP and the EPM by trusting the MPP's security certificate.

Procedure

1. Log in to the EPM Web interface using an account with the Administration user role.
2. From the EPM main menu, select **System Configuration > MPP Servers**.
3. Click the name of the MPP server that is upgraded.
4. On the **Change MPP Server** page, navigate to the MPP Certificate section, and click **Trust this certificate** if the check box is visible.
5. Click **Save**.
6. On the EPM navigation pane, click **System Management** > **MPP Manager**.
7. If the **Mode** column displays **Offline**, or the **State** column displays **Stopped**, do the following to start the MPP:
   a. Select the check box next to the name of the MPP.
   b. In the Mode Commands group, click **Online**.
   c. Click **Refresh** to verify that the **Mode** column displays **Online** for the MPP.
   d. Select the check box next to the name of the MPP.
   e. In the **State Commands** group, click **Start** and confirm your selection when prompted.
   f. Click **Refresh** to verify that the current state is **Running**.
8. Ensure that the telephony ports are correctly allocated to the MPP server:
   a. On the EPM navigation pane, click **Real-time Monitoring > Port Distribution**.
   b. On the **Port Distribution** page, verify the ports allocated to the MPP in the **Current Allocation** column.
   c. Ensure that the **Mode** and **State** columns display **Online** and **In Service** status respectively.

Chapter 6: Upgrading the Experience Portal software on a single server

Experience Portal software upgrade on a single server overview

Interactive EPM upgrade

The Experience Portal software upgrade on a single server is an Interactive upgrade.

On the EPM server, launch the Experience Portal installation program and answer the prompts.

During the Interactive upgrade, you can make changes to the configurations.

Tip:

In Experience Portal 7.0.1, the certificate generation code was enhanced to use a more secure hashing algorithm. Avaya recommends that you generate a SHA256 2048 bit server certificate (the new security certificate) to make the systems more secure.

Local WebLM license invalidated in upgrades from AEP 8.0/8.1/8.1.1 to AEP 8.1.2

For upgrades from AEP 8.0/8.1/8.1.1 to AEP 8.1.2 (or later), WebLM is upgraded from 7.1 to 8.1. When the WebLM is upgraded, the WebLM host ID changes, which in turn invalidates the current WebLM AEP license and sets the WebLM UI admin password back to the default value. Any added WebLM users are also deleted.

Licensing enters a 30 day grace mode. Avaya must generate a new license by using the new host ID. The old license file is stored in the `/opt/Avaya/InstallLogs/WebLM71/OldLicense` directory.

Upgrading the Experience Portal software interactively on a single server

Before you begin

- Ensure that you upgrade the operating system on the server as described in Operating system upgrade overview on page 20.

Important:

Ensure that you copy and restore the backup data to the Primary EPM. For more information, see Copying and restoring the backup files on page 64.

- Complete the Single EPM server upgrade worksheet on page 121 and have it available to help answer the questions raised during the installation.
- Before you upgrade the software, read the Avaya Experience Portal release notes on the support site at https://support.avaya.com/css/P8/documents/101041248. These release notes contain information about the product that is not included in the formal documentation set.
- If upgrading from Avaya Experience Portal 6.x or 7.x, ensure that you have staged the required files as mentioned in Staging the Experience Portal 6.x or 7.x backup files on the Primary EPM before upgrading Experience Portal on page 27.
- Download any patches for Avaya Experience Portal Release 8.1 from the Avaya Support website at http://support.avaya.com.
- Ensure that you have completed the software upgrade prerequisites described in Prerequisites checklist for upgrading Experience Portal on page 44.
- For disk space related information, see Space requirement for upgrading primary EPM on Red Hat Enterprise Linux on page 47 and Space requirements for upgrading primary EPM on Avaya Enterprise Linux on page 48.
- If you have installed a managed application, contact the provider of the managed application to check if you need to perform any additional steps as part of the Experience Portal upgrade.

Procedure

1. Log into the server on which you want to upgrade the Experience Portal software.

   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.

   Note:

   Ensure that you upgrade using the same Linux account that was used during the prior installation. If you upgrade an Experience Portal system by using a Linux account that is different than the account used during the previous install or upgrade, the upgrade might fail.

   This applies to RHEL (software-only) customers. It does not apply to the root and sroot users in Avaya Linux.

2. Insert the Avaya Experience Portal 8.1 software installation DVD into the DVD drive of the server.

Tip:

These instructions assume that you are going to access the Experience Portal installation DVD by mounting the appropriate DVD drive on the target system. If you want to access the installation DVD files from a shared network directory or a local directory, you can copy the Experience Portal installation ISO image to that directory. However, that directory must be readable by all users on the system. If the directory is only readable for root users, the installation script will encounter errors and will not complete successfully.

3. Mount the Avaya Experience Portal 8.1 software installation DVD. The **mount** command depends on the server's hardware and operating system.
   - If you are working with Avaya Enterprise Linux, mount the DVD by entering the `mount /mnt/cdrom` command, where `/mnt/cdrom` is the mount point typically associated with the DVD drive in the `fstab` file.
   - If you are working with a supported version of Red Hat Enterprise Linux Server, to mount the DVD:
     - Run the `mkdir -p /media/cdrom` command.

       Note:

       This command is required only if the /media/cdrom mount point does not exist.

     - Run the `mount -o ro /dev/cdrom /media/cdrom` command.

     Warning:

     When Red Hat Enterprise Linux Server automatically mounts the DVD, the files on the DVD are not executable. You must manually mount the Experience Portal installation DVD using the commands shown above.
4. Change to the mount point directory.
5. Enter the `bash aepinstall.sh` command and press `Enter` to start the installation script.

   The `bash aepinstall.sh` script checks to make sure the calling user has root privileges.
6. Press **Enter** to continue.
7. Read through the end user license agreement and select **Y** to accept the terms of the license agreement.

   Experience Portal automatically starts the PVI checker, which analyzes your system's hardware and operating system configuration. The PVI checker does the following:
   - Checks to ensure that a non-root user account has been created.
   - Asks the user to confirm that one of these accounts is the non-root account the user has configured, and to set the password.

- Checks for any missing pre-requisite RPMs and installs any if missing.
- Creates a log file in `/opt/Avaya/InstallLogs/pvicheck.log`.
- Checks if default umask is set to `027`. If it is not set to `027`, the installer asks if you want to set it to `027`. If you select 'yes', the installer applies this setting to the OS. If you select 'no', the installer exits.

8. After the configuration analysis is complete, the PVI checker displays a message stating whether all prerequisite checks passed followed by the first Prerequisite Status page.
9. Experience Portal begins installing the software. During the install, it displays messages indicating its progress.

   The installation process can appear completed or stopped even though it is still processing and installing the software.

   Please wait until the `aepinstall.sh` script completes installing and displays the message:

   ```
   20210402-17:15:15 Finished Installation
   ```

   The aepinstall.sh script creates a log file at `/opt/Avaya/InstallLogs/aepinstall.log`
10. To unmount and eject the DVD:
    a. Change the directory to a location that is outside the mount point. For example, enter the `cd /` command to change to the root directory.
    b. Unmount the DVD as described in the server documentation.
    c. To eject the Experience Portal installation DVD, press the button on the DVD drive or enter the `eject` command.
11. Check the status of the vpms service and all other services by running the following command:

    `systemctl is-active vpms tomcat sl activemq httpd postgresql epmcompmgr`

    A list appears for each service. If the vpms service is running properly, the command displays `active` for all the services in the list.

Next steps

- To verify if the installation or upgrade was successful, go to `http://EPM-Server/VoicePortal` and log into the Experience Portal web interface.

  Where, `EPM-server` is the hostname or the IP address of the system where the primary EPM logon using EPM Administrator account.
- If you are configuring Experience Portal with externally signed server identity certificates, see *Administering Avaya Experience Portal* on the Avaya Support site.
- Install any required patches that you download from the Avaya online support website, http://support.avaya.com.

- Reestablish the link between the MPP and the EPM as described in Reestablishing the link between the EPM and the MPP on page 79.
- If you wish to change the postgres database password specified by the auto upgrade utility, run the SetDbPassword.sh script.

  Important:

  If Proactive Outreach Manager is installed on this system, then you must run the script SetDbPassword.sh to change the password for the database user postgres. The Experience Portal upgrade program automatically generates a new password for the database user postgres. However, Proactive Outreach Manager is already configured to use the old password. To keep Proactive Outreach Manager working, you must change the password for the database user postgres back to the value that you have configured in Proactive Outreach Manager. For more information about configuring the PostgreSQL database user accounts, see *Administering Avaya Experience Portal*.
- Install the Avaya Service Account authentication file. For more information about installing the Avaya Service Account authentication file, see *Troubleshooting Avaya Experience Portal*.
- Upgrade the co-resident application server. For more information, see Optional: Updating the co-resident application server on page 81.
- The EPM upgrade must include reinstalling the license file for the local WebLM.

  Note:

  Due to the WebLM update, the system does not retain the license file on upgrade. You are required to configure the appropriate license for Avaya Experience Portal 8.1.

Reestablishing the link between the EPM and the MPP

After you upgrade the Experience Portal software, you need to reestablish the link between the MPP and the EPM by trusting the MPP's security certificate.

Procedure

1. Log in to the EPM web interface using an account with the Administration user role.
2. On the EPM navigation pane, click **System Configuration > MPP Servers**.
3. Click the name of the MPP server.
4. If you are upgrading from Avaya Experience Portal 6.x or 7.x, and the MPP server status is displayed as **Not Responding** in the System Monitor page, perform the following additional steps to reestablish communication between the primary EPM and MPP:
   a. Log in to Linux on the MPP server.
   b. Run the `setup_vpms.php` script.
   c. Click **System Management** > **MPP Manager**.
   d. Delete the MPP server and add the MPP server back again, using the same name and IP, and click **Trust new certificate**.

e. Click **Save**.

5. On the **Change MPP Server** page, navigate to the MPP Certificate section and click **Trust new certificate** if the check box is visible.

   Do this step if not already completed as part of the previous step.

6. Click **Save**.
7. On the EPM navigation pane, click **System Management> MPP Manager**.
8. If the **Mode** column displays **Offline**, do the following to start the MPP:
   a. Select the check box next to the name of the MPP.
   b. In the Mode Commands group, click **Online**.
   c. Click **Refresh** to verify that the **Mode** column displays **Online** for the MPP.
   d. Select the check box next to the name of the MPP.
   e. In the **State Commands** group, click **Start** and confirm your selection when prompted.
   f. Click **Refresh** to verify that the current state is **Running**.

   Note:

   Check the **System Monitor** page. If the **Last Poll** date and time details displays **never**, restart the vpms service.

9. Ensure that the telephony ports are correctly allocated to the MPP server:
   a. From the EPM main menu, select **Real-Time Monitoring > Port Distribution**.
   b. On the **Port Distribution** page, verify the ports allocated to the MPP in the **Current Allocation** column.
   c. Ensure that the **Mode** and **State** columns display **Online** and **In Service** status respectively.

Next steps

Configure the upgraded system as described in Avaya Experience Portal system configuration checklist for a system upgraded to 8.1 on page 84.

Chapter 7: Optional: Updating the co-resident application server

Optional: Updating the co-resident application server

If you have installed a Tomcat application server on the Avaya Experience Portal server, you can choose to update the version of the application server, but it is not required.

Before you begin

- From the EPM main menu, select **Real-time Monitoring > Active Calls** and ensure that the applications hosted by the co-resident application server are not handling any active calls.
- Back up the required configuration files, data files, web applications and associated components, libraries and binaries from the directory where the application server is installed. For more information on the required backup files, contact the application developer.

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. If you use Avaya Enterprise Linux, enter the `/sbin/service appserver stop` command to stop the application server.
3. Navigate to the `Support/AppServer` directory under the Avaya Experience Portal installation directory by entering the `cd $AVAYA_HOME/Support/AppServer` command.

   $AVAYA_HOME is the environment variable pointing to the name of the installation directory specified during the EPM software installation.

   Tip:

   This script is also available in the `Support/AppServer` directory of the Experience Portal installation DVD.

4. Run the installation script by entering the `bash InstallAppServer.sh install_dir` command, where *`install_dir`* is the name of the directory in which you have installed the existing application server.

   For example, to install the application server in the `/opt/AppServer` directory, you would enter `bash InstallAppServer.sh /opt/AppServer`.

5. Follow the prompts displayed by the script.

   When the script has completed, the system displays the message `Application Server Installation complete`.

   Note:

   The installation script also registers the application server as a Linux service so that it will be restarted whenever the server restarts.

6. Start the application server by entering the `/sbin/service appserver start` command.

7. Give the server time to start, and then check the server status by entering the following command:

   `/sbin/service appserver status`.

   The server should respond that the `tomcat` service is running.

8. If you want to administer the tomcat server from the Tomcat Manager Web interface, you need to add a tomcat user as specified in the *Adding Tomcat user accounts* section in the *Implementing Avaya Experience Portal on a single server* guide.

   If you use the Avaya provided application installation script, the script creates the user accounts automatically.

   Note:

   You can access the Tomcat Manager Web Interface from the System Management > Application Server menu in the EPM web interface with the tomcat user account.

9. If you want to administer the server, open a web browser and go to `http://`*`EP-server`*`:7080/manager/html`, where *`EP-server`* is the hostname or IP address of the Experience Portal server.

Next steps

It is recommended that you create a backup of the deployed application and application support runtime libraries files from the older version of Tomcat before it is deleted. These files will be lost if the older version of the Tomcat is deleted. It is also recommended that the deployed applications and application support runtime libraries are re-generated for the updated version of Tomcat.

After you install the application server:

- Deploy the speech applications to the application server as described in your application server documentation.

- You can delete the previous directory structure of the application server. If the new application server is installed in the same root directory as the old application server, make sure that you do not delete the new application server or the symbolic link named *tomcat*, which points to the new application server.

  For example, if you update Tomcat-8.5.42 to Tomcat-8.5.57 in the `/opt/AppServer` directory, where `/opt/AppServer` is the root location of the old application server, you will see the following directory structure:

  - `/opt/AppServer/OLD_apache-tomcat-8.5.57.tar.gz`
  - `/opt/AppServer/apache-tomcat-8.5.57.tar.gz`
  - `/opt/AppServer/tomcat`

  You should only delete `/opt/AppServer/OLD_apache-tomcat-8.5.57.tar.gz`.

  Note:

  The new version does not overwrite the existing directory structure of the application server. Instead, it creates a sub directory for the new version within the directory.

Chapter 8: Configuring and testing an upgraded Avaya Experience Portal system

Avaya Experience Portal system configuration checklist for a system upgraded to 8.1

Step	Description	Notes	
1	Avaya Experience Portal 8.1.2 upgrades the local WebLM co-resident server to WebLM 8.1. If the WebLM server does *not* reside on the Experience Portal EPM server, you can upgrade the WebLM software to version 8.1 or later.	For more information on the latest WebLM GA software, see http://support.avaya.com.	
2	Upgrade the Experience Portal license.	See Upgrading the Experience Portal license on page 85.	
3	Test an existing Experience Portal test application.		
4	Test the basic system by placing a call to a custom speech application or to the sample application.	For more information about the sample application, see Running the sample application on page 87.	
5	Test each MPP server individually.	See Testing an individual MPP on page 92.	
6	Connect the EPM server to an external time source so that all servers in the Experience Portal system are synchronized.	See External time sources on page 93.	
7	Enable FIPS if required. The upgrade script (aepinstall.sh) checks to ensure FIPS is enabled, but if it does not, follow the steps in Enabling FIPS on page 95.	See Enabling FIPS on page 95.	
8	Import server identity certificates.	See Importing server identity certificates on page 96.	

Table continues…

Step	Description	Notes	
9	The EPM can accept input in non-English languages if desired. If you are using Red Hat Enterprise Linux Server, the languages need to be installed with the operating system. If you are using Avaya Enterprise Linux, you can configure it to accept input in Chinese, Japanese, or Korean.	See: • Configuring Chinese on Avaya Enterprise Linux on page 96 • Configuring Japanese on Avaya Enterprise Linux on page 97 • Configuring Korean on Avaya Enterprise Linux on page 99	

Upgrading the Experience Portal license

About this task

Note:

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

Experience Portal provides an initial 30-day grace period for all features with restricted capacity for fresh installs.

Before you begin

Avaya Experience Portal 8.1.2 upgrades the local WebLM co-resident server to WebLM 8.1. If the WebLM server does *not* reside on the Experience Portal EPM server, you can upgrade the WebLM software to version 8.1 or later. For more information on the latest WebLM GA software, see http://support.avaya.com.

Important:

If a Standalone WebLM is being used, you must install the WebLM trusted certificates on the EPM. For more information on installing trusted certificates for secure communications with Standalone Avaya WebLM, see *Administering Avaya Experience Portal*.

Procedure

1. Open the email that contains the Experience Portal license file.
2. Detach the license file from the email and store the license file locally on either the WebLM server or on a computer that is accessible to the Experience Portal servers from a network connection.

   For example, you can install the license file on any server from which you can access the EPM web interface.
3. Log on to the EPM web interface by 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. If the **License Server URL** field is blank or if the location of WebLM has changed, type the location of the license server in the **Location** field.

   The URL must be in the format `https://`*`WebLM-machine`*`:`*`port_num`*`/WebLM/LicenseServer`, where *`WebLM-machine`* is the hostname or IP address of the WebLM server and `:`*`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: `8443` or `52233`.

   If no port number is specified, Experience Portal uses 443 as the port number.

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, you have to 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. Make sure 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 **Log on**.

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

11. Select **Accept the License Terms & Conditions**, and click **Install**.

    WebLM uploads the license file from your computer to the WebLM server and displays the message `License file installed successfully.`

12. Log out of the Web License Manager and close the Web License Manager page.

13. On the EPM Licensing page, click **Apply**.

14. Click **Save** to save the changes.
15. Verify that the new licensing information is correct.

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.

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`.

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 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.

Running the Application Interface test client VPAppIntfClient.sh

About this task

Use this procedure to run the Application Interface test client `VPAppIntfClient.sh`, and verify if the Application Interface test client shows the total and unused ports available for outcalls, and the result of the LaunchVXML operation.

Note:

If FIPS is enabled on the system where `VPAppIntfClient.sh` is being launched, you need to specify the following additional command line arguments:

- `-K <Java Truststore>`: The Java truststore file name including the path which contains all the trusted certificates. If the command is running on Primary EPM, the Primary EPM truststore can be specified using the value EPM_TRUSTSTORE.
- `-O <Java Truststore password>`: The password for the Java truststore file. If the command is running on Primary EPM, the Primary EPM truststore password can be specified using the value EPM_TRUSTSTORE_PASS

Before you begin

Ensure that you configure Avaya Experience Portal for the Application Interface test client as described in Configuring Experience Portal for outcall on page 88.

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.

   a. Password Authentication

   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.

   b. Certificate Authentication

   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. Ensure that the certificate is assigned to the user of Certificate type.

The user must have the Web Services user role.

c. Password and Certificate Authentication

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

Testing an individual MPP

If your system consists of multiple MPP servers, you can test each one individually to make sure they are all running as expected.

Before you begin

Configure the system as described in Avaya Experience Portal system configuration checklist for a system upgraded to 8.1 on page 84.

Procedure

1. From the EPM main menu, select **System Management** > **MPP Manager**.
2. In the MPP server table on the MPP Manager page, click the Selection check box next to all MPP servers *except* the one you want to test.
3. Click the **Stop** button in the **State Commands** group and confirm your selection when prompted.

   Experience Portal stops the selected the MPP servers. This process can take several minutes depending on how many servers there are in your system.
4. After a few minutes, click **Refresh** and verify that the **State** is **Stopped** for all MPP servers except the one you want to test.
5. Call the number you associated with the test application when adding the Experience Portal test application and use that application to verify the selected MPP. For more information about adding the test application, see *Implementing Avaya Experience Portal on multiple servers*.
6. When you are satisfied that the MPP works correctly, in the MPP server table on the MPP Manager page, click the Selection check box next to the MPP server you just tested.

7. Click the **Stop** button in the **State Commands** group and confirm your selection when prompted.
8. In the MPP server table, click the Selection check box next to the new MPP server that you want to test.
9. Click the **Start** button in the **State Commands** group and confirm your selection when prompted.
10. After a few minutes, click **Refresh** and verify that the **State** is **Stopped** for all MPP servers except the one you want to test.
11. Call the number you associated with the test application when adding the Experience Portal test application and use that application to verify the selected MPP. For more information, see *Adding the Avaya Experience Portal test application* topic in the *Implementing Avaya Experience Portal on multiple servers* guide.
12. Repeat steps 6-11 until each MPP server has been tested.
13. When you are finished testing the servers:
    a. Click the Selection check box next to any MPP server whose state is **Stopped**.
    b. Click the **Start** button in the **State Commands** group and confirm your selection when prompted.
    c. After a few minutes, click **Refresh** and verify that the **State** is **Running** for all MPP servers.

    Once the MPP servers start successfully, the basic Experience Portal system is now available.

External time sources

To make sure that the reporting and logging activities across all servers in your network are synchronized to the same time, use the same external time source for the following:

- The server running the Primary EPM software
- Any application servers running on dedicated machines
- All available speech servers
- All PBX switches
- All email servers

You can use a corporate or a public time server as the external time source.

Note:

Avaya only provides guidelines for public time servers. Ensure that the servers you choose are accessible through your corporate firewall. Some public time servers either limit the amount of access a particular site has or charge for their services. If you select a public

time server, make sure that the time server meets all requirements before you change the `chrony.conf` file on the Primary EPM server.

Configuring the Primary EPM server to point to an external time source

Before you begin

Make sure you have the server names or IP addresses of one or two appropriate external time sources. For more information, see External time sources on page 93.

Procedure

1. Log on to Linux on the Experience Portal 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. Open the `/etc/chrony.conf` file in an ASCII text editor.
3. Edit the file to add the primary external time source and an explicit declaration to set the local clock. You can also add a secondary time source for scenarios where the primary source is not found. The format is:

   ```
   server xxxx             // primary external time server
   server yyyy             // optional secondary external time server
   server 127.127.1.0      // set local clock to time received from external server
   fudge 127.127.1.0 stratum 10
   # Record the rate at which the system clock gains/losses time.
   driftfile /var/lib/chrony/drift
   ```

   Where *xxxx* and *yyyy* are either server names or IP addresses of the external time servers you want to use.

   Note:

   The typical settings for `driftfile`. If the `chrony.conf` file at your site has different settings, check with your system administrator before you change them.

   The following uses the external time sources `0.rhel.pool.ntp.org` and `1.rhel.pool.ntp.org`:

   ```
   server 0.rhel.pool.ntp.org // primary external time server
   restrict 0.rhel.pool.ntp.org nomodify
   server 1.rhel.pool.ntp.org          // secondary time server
   restrict 1.rhel.pool.ntp.org nomodify
   server 127.127.1.0                 // set local clock to time received from
   external server
   fudge 127.127.1.0 stratum 10
   # Record the rate at which the system clock gains/losses time.
   driftfile /var/lib/chrony/drift
   ```

4. Save and close the file.

5. Using a text editor of your choice, open the `/etc/ntp/step-tickers` file. The EPM uses this file for initial time setup.
6. Add a line in the file to specify the time source server names or IP addresses.

   For example, if you are using the servers `0.rhel.pool.ntp.org` and `1.rhel.pool.ntp.org`, add the following lines:

   ```
   0.rhel.pool.ntp.org
   1.rhel.pool.ntp.org
   ```
7. Save and close the file.
8. Restart the `chronyd` daemon by entering the `systemctl restart chronyd` command.

   The system returns:

   ```
   Shutting down ntpd: [OK]
   Synchronizing with time server [OK]
   Starting ntpd: [OK]
   ```

Enabling FIPS

About this task

Use this procedure to enable FIPS 140–2 mode.

Important:

Default identity certificates issued by the EP Signing Certificate are no longer supported when FIPS is enabled. You must disable the EP Signing Certificate and install the custom identity certificates on the Experience Portal servers.

For more information on FIPS, see *Administering Avaya Experience Portal*.

Procedure

1. Do the following from a local Linux console as a root user:
   - Enable FIPS at OS level by running the `fips-mode-setup --enable` command.

     Note:

     Software-only customers using RHEL 7 can follow the procedure that is provided in the Red Hat customer portal for controlling FIPS mode in the operating system. For details, see How can I make RHEL 6/7/8 FIPS 140-2 compliant?
   - Run the `reboot` command to reboot the system.

     Note:

     Rebooting the system enables FIPS at the JVM level.
2. Re-login and run the following commands to verify if FIPS is active:

```
cat /proc/sys/crypto/fips_enabled

sysctl crypto.fips_enabled
```

If the output for both of the commands is 1, FIPS is enabled.

```
cat /proc/sys/crypto/fips_enabled
 see: "1"

sysctl crypto.fips_enabled
 see "crypto.fips_enabled = 1"

grep "JVM FIPS" $CATALINA_HOME/logs/catalina.out | tail -n 1
```

If FIPS is enabled, `catalina.out` has the following log:

```
VPServlet::initialize JVM FIPS is enabled
```

Importing server identity certificates

For more information on importing the following identity certificates, see *Administering Avaya Experience Portal*.

- Primary EPM server identity certificate
- Auxiliary EPM server identity certificate
- MPP server identity certificate
- Single server identity certificate

Non-English language support

Non-English character support on the EPM web pages

You can enter non-English characters as field values if you have the appropriate languages installed on the EPM server. If you are using Avaya Enterprise Linux, Avaya provides font files for Chinese, Japanese, and Korean.

Configuring Chinese on Avaya Enterprise Linux

Procedure

1. Log on to Linux on the Experience Portal Primary EPM server in one of the following ways:
   - Log on to the local Linux console as a root user if you are an Avaya Services representative, use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server.
   - 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 Linux font directory by entering the `cd /usr/share/fonts` command.

   Note:

   If the font directory does not already exist, create the directory by entering the `mkdir /usr/share/fonts` command, then navigate to the directory you just created.

3. Copy the Chinese font file to the font directory by entering the `cp $AVAYA_HOME/Support/fonts/zh_CN/TTzh_CN.tar .` command.

   Important:

   Make sure you include the . (period) at the end of the **cp** command to indicate that you want Linux to copy the files to the current directory.

4. Extract the font file by running the `tar -xvf TTzh_CN.tar` command.
5. Copy the system language file to the Linux system configuration directory by running the `cp $AVAYA_HOME/Support/fonts/zh_CN/i18n /etc/sysconfig/` command.
6. Navigate to the Java fonts directory by running the `cd $JAVA_HOME/jre/lib/fonts` command.

   Note:

   If the fonts directory does not already exist, create the directory by entering the `mkdir $JAVA_HOME/jre/lib/fonts` command, then navigate to the directory that you just created.

7. Create the fallback directory by running the `mkdir fallback` command.
8. Navigate to the fallback directory by running the `cd fallback` command.
9. Copy the Chinese font files to the fallback directory by running the `cp /usr/share/fonts/zh_CN/TrueType/*.ttf .` command.

   Important:

   Make sure you include the . (period) at the end of the **cp** command to indicate that you want Linux to copy the files to the current directory.

10. Reboot the EPM server machine by entering the `reboot` command.

Configuring Japanese on Avaya Enterprise Linux

Procedure

1. Log on to Linux on the Experience Portal 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 Linux font directory by entering the `cd /usr/share/fonts` command.

   Note:

   If the font directory does not already exist, create the directory by entering the `mkdir /usr/share/fonts` command, then navigate to the directory you just created.

3. Copy the Japanese font file to the font directory by entering the `cp $AVAYA_HOME/Support/fonts/ja/TTja.tar .` command.

   Important:

   Make sure you include the . (period) at the end of the **cp** command to indicate that you want Linux to copy the files to the current directory.

4. Extract the font file by entering the `tar -xvf TTja.tar` command.
5. Copy the system language file to the Linux system configuration directory by entering the `cp $AVAYA_HOME/Support/fonts/ja/i18n /etc/sysconfig/` command.
6. Navigate to the Java fonts directory by entering the `cd $JAVA_HOME/jre/lib/fonts` command.

   Note:

   If the fonts directory does not already exist, create the directory by entering the `mkdir $JAVA_HOME/jre/lib/fonts` command, then navigate to the directory that you just created.

7. Create the fallback directory by entering the `mkdir fallback` command.
8. Navigate to the fallback directory by entering the `cd fallback` command.
9. Copy the Japanese font files to the fallback directory by entering the `cp /usr/share/fonts/ja/TrueType/*.ttf .` command.

   Important:

   Make sure you include the . (period) at the end of the **cp** command to indicate that you want Linux to copy the files to the current directory.

10. Reboot the EPM server machine by entering the `reboot` command.

Configuring Korean on Avaya Enterprise Linux

Procedure

1. Log on to Linux on the Experience Portal 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 Linux font directory by entering the `cd /usr/share/fonts` command.

   Note:

   If the font directory does not already exist, create the directory by entering the `mkdir /usr/share/fonts` command, then navigate to the directory you just created.
3. Copy the Korean font file to the font directory by entering the `cp $AVAYA_HOME/Support/fonts/ko/TTko.tar .` command.

   Important:

   Make sure you include the . (period) at the end of the **cp** command to indicate that you want Linux to copy the files to the current directory.
4. Extract the font file by entering the `tar -xvf TTko.tar` command.
5. Copy the system language file to the Linux system configuration directory by entering the following command:

   `cp $AVAYA_HOME/Support/fonts/ko/i18n /etc/sysconfig/` command.
6. Navigate to the Java fonts directory by entering the `cd $JAVA_HOME/jre/lib/fonts` command.

   Note:

   If the fonts directory does not already exist, create the directory by entering the `mkdir $JAVA_HOME/jre/lib/fonts` command, then navigate to the directory that you just created.
7. Create the fallback directory by entering the `mkdir fallback` command.
8. Navigate to the fallback directory by entering the `cd fallback` command.
9. Copy the Korean font files to the fallback directory by entering the `cp /usr/share/fonts/ko/TrueType/*.ttf .` command.

   Important:

   Make sure you include the . (period) at the end of the **cp** command to indicate that you want Linux to copy the files to the current directory.

10. Reboot the EPM server machine by entering the `reboot` command.

Chapter 9: Troubleshooting upgrade issues

Upgrade installation log files

The upgrade installation log files contain detailed information about the upgrade installation process.

Avaya Experience Portal creates several log files during the upgrade process.

General installation log files

Log filename	Description
`aepinstall.log`	This is the first log file you should consult if you need to troubleshoot an installation issue. **Note:** This file contains detailed log messages which might appear to be warnings or errors, but can safely be ignored, particularly if those warnings do not appear in the installation summary (ISSummary.log).
`SetIAVersion<component>.log`	Version history of the Experience Portal components installed. The <component> can be VPMS, MPP, or Docs.
`GetIAVersionVPMS.err.log`	Log file containing any warning messages generated while trying to retrieve version information as part of an upgrade. The presence of a warning in this log file does not necessarily indicate an error.

MPP-specific installation log files

Log filename	Description
`av-mpp-<buildnumber>-Install-<date>.log`	`mppinstall.sh` script output.
`av-mpp-<buildnumber>-Install-rpm-<date>.log`	Output from the Red Hat Package Manager (RPM) during the MPP software installation.

EPM-specific installation log files

Log filename	Description
`vpms.cert.gen.out.log`	Results from the security certificate generation process.
`vpms.cert.gen.err.log`	Any internal errors generated from the certificate generation process.

Primary EPM root certificate is signed with a weak hashing algorithm warning

The Experience Portal installer might display a warning message if the existing EPM Root certificate is signed with a weak hashing algorithm. Avaya recommends that you generate a new SHA256 2048 bit root certificate from the **Root Certificate** tab of the **Security** > **Certificate** page in EPM.

You must export the new root certificate and install it on applications such as speech servers, telephone, and LDAP servers to which the Experience Portal needs to make an SSL connection.

Changing the Product ID for an existing Experience Portal system

Before you begin

If you have just installed or upgraded the Experience Portal software and are still logged into the server, verify that you reloaded the environment variables as described in Reloading the Experience Portal environment variables on page 103.

Procedure

1. Log on to Linux on the Experience Portal 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 Support/VP-Tools directory by entering the **`cd /opt/Avaya/ExperiencePortal/Support/VP-Tools`** command.
3. Stop *vpms* service by entering the **`service vpms stop`** command.
4. To run the script:

   On Linux: Enter the `bash ResetProductID New_ProductID` command where New_ProductID is the product ID that you want to use.
5. Restart *vpms* service by entering the **`service vpms restart`** command.
6. Restart all MPPs by entering the **`service mpp restart`**
7. Follow any on-screen instructions displayed by the script.

Invalid password for database user

The EPM auto upgrade fails with the invalid password error.

The most common cause of this error is that the password could not be loaded from configuration or the password validation failed.

Solution

1. Reboot the server
2. Restart the upgrade script by selecting the Interactive EPM upgrade option. The interactive upgrade allows you to create a new user account and password to access the database.

Time synchronization problems

Experience Portal uses *chronyd daemon* to control and synchronize the clocks when the EPM and MPP software is running on different servers. The dedicated MPP servers and the optional auxiliary EPM server point to the primary EPM server as the reference clock.

Note:

If the time difference is too large, chronyd cannot synchronize the client and server clocks immediately. A workaround is to manually synchronize the clocks before starting chronyd. After chronyd starts, it adjusts the clients clock with the server timings slowly. The slow process is by design so that confusion with other processes that are running and depends on the clock can be avoided.

To troubleshoot synchronization errors, perform the following procedures in the order given, advancing to the next procedure only if the problem continues to persist.

Reloading the Experience Portal environment variables

After you install or upgrade an Experience Portal server, you need to load the new environment variables.

Procedure

1. Log completely out of the Linux system.
2. If you are on the console and are working with:
   - Avaya Enterprise Linux, enter the `su - root` command.
   - Red Hat Enterprise Linux Server, enter the `su -` command.

Note:

If you are a remote user, log in to Linux by entering a non-root user name and password at the prompts.

Recovering Avaya Enterprise Linux configuration information after an upgrade

You can still access configuration information from any text files stored on your Experience Portal 6.x or 7.x Avaya Enterprise Linux system even after you upgrade the operating system.

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. Change to the `/root2` directory to access the 6.x or 7.x partition by entering the `cd /root2` command.

   The files from the previous installation are available.

Restoring the previous operating system after an upgrade

Checklist for restoring the software on Avaya Enterprise Linux

If you want to revert an upgraded Experience Portal system running on Avaya Enterprise Linux back to 6.x or 7.x, you must perform the steps mentioned in the following table:

Step	Description	Notes	✔
1	Restore the previous version of Avaya Enterprise Linux on all Experience Portal servers.	See Restoring the Avaya Enterprise Linux operating system on page 105.	

Table continues…

Step	Description	Notes	✔
2	Restore the Primary EPM server.	See Restoring the software on the Primary EPM server or a single-server Experience Portal system running Avaya Enterprise Linux on page 106.	
3	Restore the software on the Auxiliary EPM server.	See Restoring OS on Auxiliary EPM server on page 107.	
4	Restore the MPP servers.	See Restoring the MPP software on a server running Avaya Enterprise Linux on page 108.	

Restoring the Avaya Enterprise Linux operating system

Before you begin

If you are working with an MPP server, take the MPP offline.

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. Verify which partition is the boot partition by entering the `/opt/Avaya/LinuxInstaller/bin/cpartition` command.
3. If the boot partition is not equal to the standby partition (which contains your previous Avaya Enterprise Linux version), revert to the previous boot partition by entering the `/opt/Avaya/LinuxInstaller/bin/cpartition -c` command.

   Note:

   The - o and - p options are not used with the current **cpartition** version. The - c option changes the boot partition from Standby to Active, and makes it permanent.

4. Reboot the server.

Restoring the software on the Primary EPM server or a single-server Experience Portal system running Avaya Enterprise Linux

Before you begin

Ensure that you have restored the operating system as described in Restoring the Avaya Enterprise Linux operating system on page 105.

Procedure

1. Log on to Linux on the Experience Portal 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. Stop the *vpms* service by entering the `systemctl stop vpms` command.

   You will see a series of messages as the command starts to shut down the EPM components. When the command has successfully stopped all relevant components, the system displays the message: `VPMS Shutdown Status: [ OK ] .`

3. Check the status of the `postgres` service by entering the `/sbin/service postgresql status` command.

4. If the `postgres` service is running, stop it by entering the `/sbin/service postgresql stop` command.

5. Navigate to the `pgsql` directory by entering the `cd /var/lib/pgsql` command.

6. Rename the current data directory that contains the 6.x or 7.x data by entering the `mv data data_OLD` command.

7. In the `pgsql` directory, locate the backup directory that Experience Portal created when you installed the new version. The file name has the format `data_vp_<backup_date>_<backup_time>`.

8. Copy this backup directory into the main data directory by entering the `cp -rp data_vp_<backup_date>_<backup_time> data` command.

9. Start the `postgresql` service by entering the `/sbin/service postgresql start` command.

10. Wait for a few seconds for the database to start, then verify that it is running by entering the `/sbin/service postgresql status` command.

11. Start the *vpms* service by entering the `systemctl start vpms` command.

12. If you have previously changed the **Session timeout (minutes)** field in **Home** > **User Management** > **Login Options**, update this field again.

For more information, see *Administering Avaya Experience Portal*.

13. If you have previously changed the **Purge and Retention** field in **Home** > **System Configuration** > **EPM Servers** > **Alarm/Log Options**, update this field again.

    For more information, see *Administering Avaya Experience Portal*.

14. If you have previously enabled **Organizations** for the system, re-enable it by executing the following script:

    ```
    $AVAYA_HOME/Support/VP-Tools/EnableOrganizations
    ```

    For more information on *Enabling organization level access in Experience Portal*, see *Administering Avaya Experience Portal*.

15. If you are restoring a co-resident application server on the Experience Portal server, follow the steps in Optional: Updating the co-resident application server on page 81.

    Note:

    For major version upgrades of Tomcat, it is also recommended that the deployed applications and application support runtime libraries are re-generated for the updated version of Tomcat.

16. If you have previously deployed and configured any Managed Applications, re-install and deploy the managed application.

Restoring the software on the Auxiliary EPM server running Avaya Enterprise Linux

Before you begin

Make sure you have restored the operating system as described in Restoring the Avaya Enterprise Linux operating system on page 105.

Procedure

1. Log in to Linux on the Auxiliary 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. Stop the *vpms* service by entering the `systemctl stop vpms` command.

   You will see a series of messages as the command starts to shut down the EPM components. When the command has successfully stopped all relevant components, the system displays the message: `VPMS Shutdown Status: [ OK ] .`

3. Check the status of the `postgres` service by entering the `/sbin/service postgresql status` command.
4. If the `postgres` service is running, stop it by entering the `/sbin/service postgresql stop` command.
5. Navigate to the `pgsql` directory by entering the `cd /var/lib/pgsql` command.
6. Rename the current data directory that contains the 6.x or 7.x data by entering the `mv data data_OLD` command.
7. In the `pgsql` directory, locate the backup directory that Experience Portal created when you installed the new version. The file name has the format `data_vp_<backup_date>_<backup_time>`.
8. Copy this backup directory into the main data directory by entering the `cp -rp data_vp_<backup_date>_<backup_time> data` command.
9. Start the `postgresql` service by entering the `/sbin/service postgresql start` command.
10. Wait for a few seconds for the database to start, then verify that it is running by entering the `/sbin/service postgresql status` command.
11. Start the *vpms* service by entering the `systemctl start vpms` command.

Restoring the MPP software on a server running Avaya Enterprise Linux

Before you begin

- Make sure you have restored the operating system as described in Restoring the Avaya Enterprise Linux operating system on page 105.
- Make sure you have restored the Primary EPM server.

Procedure

1. Restore the log files.
2. If the server is an MPP and you have moved the MPP logs to a new directory or a partition using the `mppMoveLogs.sh` script, add the appropriate mount point to the `/etc/fstab` file.

   For more information, see *Administering Avaya Experience Portal*

Next steps

At this point, you can:

- Restore another MPP server.
- Start the restored MPP as described in *Administering Avaya Experience Portal*.
- Start multiple restored MPP servers as described in *Administering Avaya Experience Portal*.

Restoring the software on a dedicated Primary EPM server or a single-server EPM system running Red Hat Enterprise Linux Server

About this task

Note:

If your installation uses a dedicated Primary EPM server, you should always restore the Primary EPM server first and then you can restore each Auxiliary EPM and MPP server separately.

Before you begin

Ensure that you have access to the backup files taken before the upgrade. For more information about backing up the existing data, see Backing up data on page 25.

Procedure

1. Install the previous version of Red Hat Enterprise Linux Server using the Red Hat Enterprise Server installation CD-ROM and the exact options you used for the 6.0.x, 7.0.x, or 7.1 software installation.
2. Reinstall the EPM software from your 6.0.x, 7.0.x, or 7.1 software installation DVD.

   Ensure that you select the same options that you selected during the first install.
3. Restore your Experience Portal database from the backup as described in the document *Upgrading to Avaya Experience Portal 8.1*.
4. If you have changed the default log and alarm retention periods, reset those values as described in *Administering Avaya Experience Portal*.
5. If you have previously changed the **Session timeout (minutes)** field in **Home** > **User Management** > **Login Options**, update this field again.

   For more information, see *Administering Avaya Experience Portal*.
6. If you have previously changed the **Purge and Retention** field in **Home** > **System Configuration** > **EPM Servers** > **Alarm/Log Options**, update this field again.

   For more information, see *Administering Avaya Experience Portal*.
7. If you have previously enabled **Organizations** for the system, re-enable it by executing the following script:

   ```
   $AVAYA_HOME/Support/VP-Tools/EnableOrganizations
   ```

   For more information on *Enabling organization level access in Experience Portal*, see *Administering Avaya Experience Portal*.
8. If you are restoring a co-resident application server on the Experience Portal server, follow the steps in Optional: Updating the co-resident application server on page 81.

Note:

For major version upgrades of Tomcat, it is also recommended that the deployed applications and application support runtime libraries are re-generated for the updated version of Tomcat.

9. If you have previously deployed and configured any Managed Applications, re-install and deploy the managed application.

Restoring the software on an Auxiliary EPM server running Red Hat Enterprise Linux Server

Before you begin

If your installation uses a dedicated Primary EPM server, you should always restore the Primary EPM server first and then restore each Auxiliary EPM.

Procedure

1. Install the previous version of Red Hat Enterprise Linux Server using the Red Hat Enterprise Server installation CD-ROM and the exact options you used for the 6.0.x, 7.0.x, or 7.1 software installtion.
2. Reinstall the EPM software from your 6.0.x, 7.0.x, or 7.1 software installation DVD.

   Ensure that you select the same options that you selected during the first install.
3. Reestablish the link between the MPP and the Auxiliary EPM as described in Reestablishing the link between the EPM and the MPP on page 79.

Restoring a dedicated MPP server on Red Hat Enterprise Linux Server

To restore MPP server on Red Hat Enterprise Linux Server, reinstall the operating system and then reinstall the Experience Portal software.

Before you begin

Make sure you have already restored your Primary EPM server.

Procedure

1. Take the MPP offline.

   Note:

   If you cannot stop the MPP through the EPM, log onto the MPP server and stop the process by entering the `/sbin/service mpp stop` command.
2. Install Red Hat Enterprise Linux Server using the Red Hat Enterprise Linux Server installation CD-ROM and the exact options you used for Experience Portal.
3. Reinstall the MPP software from your Experience Portal installation DVD. Verify that you select the same options that you selected during the first install.

4. Restore the MPP log files.
5. If you changed the AVB configuration files, restore the customized files.
6. If all MPP servers have been restored, reestablish the link between the restored EPM server and the restored MPP servers.

Next steps

- Restore another MPP by following this procedure on that MPP.

Chapter 10: Preupgrade worksheets

Primary EPM server upgrade worksheet

Complete this worksheet if you are installing the EPM server on a dedicated Avaya Experience Portal server.

Requirement/ Information Needed	Your value	Notes
Ensure that the hardware meets the minimum requirements. For more information on minimum server machine hardware requirements, see *Avaya Experience Portal* Overview and Specification on http://support.avaya.com.		For minimum hardware requirements, see Minimum (Linux) server machine hardware requirements on page 47.
What access method are you going to use?	_____ Local keyboard, mouse, and monitor _____ Remote access via SSH client	
Server information	IP address _____ Host name _____	The host name cannot contain spaces or periods.
Do you want to enable EASG on the Primary EPM?	_____ Yes _____ No	
For RHEL 7.x or 8.x, verify default umask is set to 027.	_____ Yes	

Table continues…

Requirement/ Information Needed	Your value	Notes
Avaya Enterprise Linux network configuration information	Subnet mask on Corporate LAN _____ Default gateway _____ Primary DNS Server _____ DNS domain name _____ Time zone _____	For more information about the Avaya-provided server installation, see *Implementing Avaya Experience Portal on multiple servers*.
For customer-provided hardware, is Release 7.x or 8.x 64 bit or newer update installed?	_____ Yes _____ No	If No, install Release 7.x or 8.x 64 bit or later as described in *Implementing Avaya Experience Portal on multiple servers*.
Is the default language for Linux set to English?	_____ Yes _____ No	If No, set the default language to English. You can change the default language after Experience Portal is installed.
Can all planned Experience Portal servers communicate with one another?	_____ Yes _____ No	For more information about verifying server communication, see *Implementing Avaya Experience Portal on multiple servers* on http://support.avaya.com.
For Avaya Enterprise Linux, user account passwords	`cust` account password: _____ root account password: _____	
For Red Hat Enterprise Linux Server, user accounts and passwords	root account password: _____ Non-root account name: _____ Non-root account password: _____	

Table continues…

Requirement/ Information Needed	Your value	Notes
Can you log in to the Experience Portal server with the non-root account name and password?	_____ Yes _____ No	The upgrade tool deletes all existing root accounts. Therefore, after the upgrade, the administrator uses the non-root account name and password to log in and: • Install a new Authentication File System (AFS) file. • Activate the Avaya service accounts.
Installation directory, if different from default	_____	Default directory: `/opt/Avaya/ExperiencePortal` Specify an absolute directory path containing only standard English alphanumeric characters and the symbols / (forward slash), _ (underscore), - (hyphen), ~ (tilde), or . (period).
EPM web interface administration user name and password	User name: _____ Password: _____	The Experience Portal administrator uses this account to log in to the EPM web interface to administer the Experience Portal system. The account is assigned the Administration user role as well as the Auditor and User Manager user roles. For details about User Roles, see *Administering Avaya Experience Portal* on http://support.avaya.com.
Do you want to create a database account that can access the report information in the database?	_____ Yes _____ No If Yes, account user name, if different from the default: _____ Password: _____	Default user name is: reportwriter **Note:** The report user name cannot be the same as any of the EPM web interface administration user account names or the report writer user account name.
Third-party SSL certificate information.	Third-party SSL certificate information. The location of the existing certificate: _____ The existing certificate's password: _____	

Table continues…

Requirement/ Information Needed	Your value	Notes
Will Avaya Services maintain this server?	_____ Yes _____ No If Yes, what is the Listed Directory Number (LDN) for this server? _____ Where is the Avaya Service Account authentication file located? _____	For more information on configuring Avaya service accounts, see *Implementing Avaya Experience Portal on multiple servers*.
WebLM information	License server URL, if not located on the EPM server: _____ WebLM password: _____	
The external time sources that the EPM server should be synchronize with, if desired	The name or IP address of primary time source: _____ The name or IP address of secondary time source: _____	

Auxiliary EPM server upgrade worksheet

Complete this worksheet if you are installing the EPM server on an Auxiliary Experience Portal server.

Requirement/ Information Needed	Your value	Notes
Ensure that the hardware meets the minimum requirements. For more information on minimum server machine hardware requirements, see *Avaya Experience Portal* Overview and Specification on http://support.avaya.com.		For minimum hardware requirements, see Minimum (Linux) server machine hardware requirements on page 47.
What access method are you going to use?	_____ Local keyboard, mouse, and monitor _____ Remote access via SSH client	
Server information	IP address _____ Host name _____	The host name cannot contain spaces or periods.
Avaya Enterprise Linux network configuration information	Subnet mask on Corporate LAN _____ Default gateway _____ Primary DNS Server _____ DNS domain name _____ Time zone _____	For more information about the Avaya-provided server installation, see *Implementing Avaya Experience Portal on multiple servers*.

Table continues…

Requirement/ Information Needed	Your value	Notes
For customer-provided hardware, is Release 7.x or 8.x 64 bit or newer update installed?	_____ Yes _____ No	If No, install Release 7.x or 8.x 64 bit or later as described in *Implementing Avaya Experience Portal on multiple servers*.
Is the default language for Linux set to English?	_____ Yes _____ No	If No, set the default language to English. You can change the default language after Experience Portal is installed.
Can all planned Experience Portal servers communicate with one another?	_____ Yes _____ No	For more information about verifying server communication, see *Implementing Avaya Experience Portal on multiple servers* on http://support.avaya.com.
For Avaya Enterprise Linux, user account passwords	`cust` account password: _____ root account password: _____	
For Red Hat Enterprise Linux Server, user accounts and passwords	root account password: _____ Non-root account name: _____ Non-root account password: _____	
Can you log in to the Experience Portal server with the non-root account name and password?	_____ Yes _____ No	The upgrade tool deletes all existing root accounts. Therefore, after the upgrade, the administrator can use the non-root account name and password to log in and: • Install a new Authentication File System (AFS) file. • Activate the Avaya service accounts.
Installation directory, if different from default	_____	Default directory: `/opt/Avaya/ExperiencePortal` Specify an absolute directory path containing only standard English alphanumeric characters and the symbols / (forward slash), _ (underscore), - (hyphen), ~ (tilde), or . (period).

Table continues…

Requirement/ Information Needed	Your value	Notes
Auxiliary EPM database password	_____	For more information about the Primary EPM server installation worksheet, see *Implementing Avaya Experience Portal on multiple servers*.
Do you want to create a database account that can access the report information in the database?	_____ Yes _____ No If Yes, account user name, if different from the default: _____ Password: _____	Default user name is: reportwriter **Note:** The report user name cannot be the same as any of the EPM web interface administration user account names or the report writer user account name.
Do you want to create a report writer database account that allows external Experience Portal servers to write report data into the Experience Portal database on this server.	_____ Yes _____ No If Yes, account username: _____ If Yes, account password: _____	
Third-party SSL certificate information.	Third-party SSL certificate information. The location of the existing certificate: _____ The existing certificate's password: _____	
Will Avaya Services maintain this server?	_____ Yes _____ No If Yes, what is the Listed Directory Number (LDN) for this server? _____ Where is the Avaya Service Account authentication file located? _____	

MPP server upgrade worksheet

Complete the following worksheet for each planned Media Processing Platform (MPP) server on this Experience Portal system.

Requirement or information needed	Your value	Notes
Ensure that the hardware meets the minimum requirements. For more information on minimum server machine hardware requirements, see *Avaya Experience Portal* Overview and Specification on http://support.avaya.com.		For minimum hardware requirements, see Minimum (Linux) server machine hardware requirements on page 47.
What access method are you going to use?	_____ Local keyboard, mouse, and monitor _____ Remote access via SSH client	
Corporate LAN IP address	_____	
PBX LAN IP address, if different from the corporate LAN	_____	
Avaya Enterprise Linux network configuration information	Subnet mask on Corporate LAN _____ Subnet mask on PBX LAN, if different from Corporate LAN _____ Default gateway _____ Primary DNS Server _____ DNS domain name _____ Time zone _____	

Table continues…

Requirement or information needed	Your value	Notes
For Avaya Enterprise Linux, user account passwords	`cust` account password: _____ root account password: _____	
For Red Hat Enterprise Linux Server, user accounts and passwords	root account password: _____ Non-root account name: _____ Non-root account password: _____	
Is the default language for Linux set to English?	_____ Yes _____ No	If No, set the default language to English. You can change the default language after Experience Portal is installed.
Maximum simultaneous calls	_____	The maximum number of calls that this MPP can handle at any one time. It is equivalent to the maximum number of ports that Experience Portal will allocate to this MPP. For assistance in sizing your MPP server capacity and setting the correct value for the **Maximum Simultaneous Calls** parameter for each MPP server, contact your Avaya Services representative or Avaya Business Partner.
Installation directory, if different from default	_____	
Third-party SSL certificate information.	Third-party SSL certificate information. The location of the existing certificate: _____ The existing certificate's password: _____	
Will Avaya Services maintain this server?	_____ Yes _____ No If Yes, what is the Listed Directory Number (LDN) for this server? _____	

Single EPM server upgrade worksheet

Complete this worksheet if you are installing the EPM server on a dedicated Avaya Experience Portal server.

Requirement/ Information Needed	Your value	Notes
Ensure that the hardware meets the minimum requirements. For more information on minimum server machine hardware requirements, see *Avaya Experience Portal* Overview and Specification on http://support.avaya.com.		For minimum hardware requirements, see Minimum (Linux) server machine hardware requirements on page 47.
What access method are you going to use?	_____ Local keyboard, mouse, and monitor _____ Remote access via SSH client	
PBX LAN IP address, if different from the corporate LAN	_____	
Server information	IP address _____ Host name _____	The host name cannot contain spaces or periods.
Avaya Enterprise Linux network configuration information	Subnet mask on Corporate LAN _____ Default gateway _____ Primary DNS Server _____ DNS domain name _____ Time zone _____	For more information about the Avaya-provided server installation, see *Implementing Avaya Experience Portal on multiple servers*.

Table continues…

Requirement/ Information Needed	Your value	Notes
For customer-provided hardware, is Release 7.x or 8.x 64 bit or newer update installed?	_____ Yes _____ No	If No, install Release 7.x or 8.x 64 bit or later as described in *Implementing Avaya Experience Portal on multiple servers*.
Is the default language for Linux set to English?	_____ Yes _____ No	If No, set the default language to English. You can change the default language after Experience Portal is installed.
Maximum simultaneous calls	_____	The maximum number of calls that this MPP can handle at any one time. It is equivalent to the maximum number of ports that Experience Portal will allocate to this MPP. For assistance in sizing your MPP server capacity and setting the correct value for the **Maximum Simultaneous Calls** parameter for each MPP server, contact your Avaya Services representative or Avaya Business Partner.
Can all planned Experience Portal servers communicate with one another?	_____ Yes _____ No	For more information about verifying server communication, see *Implementing Avaya Experience Portal on multiple servers* on http://support.avaya.com.
For Avaya Enterprise Linux, user account passwords	`cust` account password: _____ root account password: _____	
For Red Hat Enterprise Linux Server, user accounts and passwords	root account password: _____ Non-root account name: _____ Non-root account password: _____	

Table continues…

Requirement/ Information Needed	Your value	Notes
Can you log in to the Experience Portal server with the non-root account name and password?	_____ Yes _____ No	The upgrade tool deletes all existing root accounts. Therefore, after the upgrade, the administrator uses the non-root account name and password to log in and: • Install a new Authentication File System (AFS) file. • Activate the Avaya service accounts.
Installation directory, if different from default	_____	Default directory: `/opt/Avaya/ExperiencePortal` Specify an absolute directory path containing only standard English alphanumeric characters and the symbols / (forward slash), _ (underscore), - (hyphen), ~ (tilde), or . (period).
EPM web interface administration user name and password	User name: _____ Password: _____	The Experience Portal administrator uses this account to log in to the EPM web interface to administer the Experience Portal system. The account is assigned the Administration user role as well as the Auditor and User Manager user roles. For details about User Roles, see *Administering Avaya Experience Portal* on http://support.avaya.com.
Do you want to create a database account that can access the report information in the database?	_____ Yes _____ No If Yes, account user name, if different from the default: _____ Password: _____	Default user name is: reportwriter **Note:** The report user name cannot be the same as any of the EPM web interface administration user account names or the report writer user account name.
Third-party SSL certificate information.	Third-party SSL certificate information. The location of the existing certificate: _____ The existing certificate's password: _____	

Table continues…

Requirement/ Information Needed	Your value	Notes
Will Avaya Services maintain this server?	_____ Yes _____ No If Yes, what is the Listed Directory Number (LDN) for this server? _____ Where is the Avaya Service Account authentication file located? _____	For more information on configuring Avaya service accounts, see *Implementing Avaya Experience Portal on multiple servers*.
WebLM information	License server URL, if not located on the EPM server: _____ WebLM password: _____	
The external time sources that the EPM server should be synchronize with, if desired	The name or IP address of primary time source: _____ The name or IP address of secondary time source: _____	

Chapter 11: Resources

Documentation

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

Title	Description	Audience
Avaya 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
Administering Avaya Experience Portal	Provides general information about and procedures for administering and configuring specific Experience Portal functions and features using a web-based interface.	Administrators Implementation engineers
Avaya Experience Portal Overview and Specification	Describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Administrators Sales engineers Implementation engineers Avaya Professional Services
Implementing Avaya Experience Portal on a single server	Provides procedures to install and configure the Avaya Experience Portal software on a single server.	Implementation engineers
Implementing Avaya Experience Portal on multiple servers	Provides procedures to install and configure Avaya Experience Portal software on two or more dedicated servers.	Implementation engineers

Table continues…

Title	Description	Audience
Deploying Avaya Experience Portal in an Avaya Customer Experience Virtualized Environment	Provides procedures for deploying the 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.	Implementation engineers
Upgrading to Avaya Experience Portal 8.1	Describes how to upgrade your Avaya Experience Portal system to Avaya Experience Portal 8.1.	Implementation engineers
Troubleshooting Avaya 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.	Administrators Implementation engineers Avaya Professional Services
Avaya Experience Portal Solutions Guide	Provides a high-level description of Avaya Experience Portal as well as topology diagrams, connectivity details, interoperability concept, product interactions, and failover best practices.	Sales engineers Implementation engineers Avaya Professional Services
Avaya Experience Portal Programmer's Reference	Provides information about designing speech applications for Avaya Experience Portal.	Application Developers
Deploying Avaya Experience Portal on Amazon Web Services	Provides procedures for deploying Avaya Experience Portal as *Software as a Solution* by using the Amazon Web Services Management console.	Administrators Implementation engineers Support Personnel Avaya Professional Services
Deploying Avaya Experience Portal on Google Cloud Platform	Provides procedures for deploying Avaya Experience Portal as *Software as a Solution* by using the Google Cloud Platform.	Administrators Avaya Professional Services Implementation engineers Support Personnel

Table continues…

Title	Description	Audience
Deploying Avaya Experience Portal on Microsoft Azure	Provides procedures for deploying Avaya Experience Portal as *Software as a Solution* by using the Microsoft Azure portal.	Administrators Implementation engineers Support Personnel Avaya Professional Services
Avaya 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 Experience Portal Mobile Web Best Practices White Paper	Provides recommended strategies for deploying Avaya Orchestration Designer Mobile Web applications with Avaya Experience Portal, detailing configuration for security, scalability and high availability.	Avaya Professional Services Implementation engineers
Avaya Experience Portal Call Classifications White Paper	Provides information about the call classification feature in Avaya Experience Portal, detailing the configuration and tuning of the call progress engine.	Sales engineers Implementation engineers
Avaya Experience Portal Dialogflow White Paper	Provides information about connecting Avaya Experience Portal self-service applications to Google Dialogflow. This document provides details on configuration, licensing, and other information to help customers with Dialogflow integration.	Avaya Professional Services Implementation engineers
Avaya Experience Portal Nuance Mix Integration White Paper	Provides information about connecting Avaya Experience Portal to Nuance Mix. This document provides details on configuration, licensing, and other information to help customers with Nuance Mix integration.	Avaya Professional Services Implementation engineers

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.

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

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

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

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

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

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.
- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

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

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.

- Share content in a collection with others through email.
- Receive collection that others have shared with you.

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

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - 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 website.
- 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 website. The available functionality depends on your role.

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

Index

A

Application Interface 88
Application Interface test client 88
applications
  testing 87
ASR servers
  testing 87
Avaya Enterprise Linux
  Auxiliary VPMS overview 10
  Avaya Enterprise Linux 29, 32
  configuring for Chinese input 96
  configuring for Japanese input 97
  configuring for Korean input 99
  EPM overview 9
  recovering configuration information 104
  restoring 4.0.x 105
  restoring previous version 104
  upgrade overview 9, 10
  upgrading 9, 10, 29, 32
Avaya Experience Portal
  configuring 84
  hardware requirements 47
  installing license file 85
  license requirements 49
  upgrade log files 101
  upgrading on multiple servers 74
Avaya Experience Portal servers
  verifying and setting time 55
  verifying communication 51
Avaya support website 130

C

certificates
  importing server identity certificates 96
Chinese, configuring on Avaya Enterprise Linux 96
collection
  delete 128
  edit name 128
  generating PDF 128
  sharing content 128
communication between servers
  verifying 51
configuring Avaya Experience Portal 84
content
  publishing PDF output 128
  searching 128
  sharing 128
  sort by last updated 128
  watching for updates 128
copying and restoring backup files 64
craft 35
cust 35

D

default umask 22
documentation center 128
  finding content 128
  navigation 128
documentation portal 128
  finding content 128
  navigation 128
documentation title
  audience 125
  description 125

E

email
  upgrade 53
email processor 53
enabling FIPS 95
Enterpise Linux Installer
  preparing to install 28
environment variables, reloading 103
EPM
  configuring for non-English input 96
  synchronizing time with MPPs 55
  synchronizing with external time source 93
  upgrade log files 101
  upgrading Red Hat Linux on 36
  worksheet for auxiliary 116
  worksheet for primary 112
  worksheet for single server 121
etc/hosts file
  verifying 51
external database
  verifying before upgrade 56
external time source
  setting for EPM 93

F

finding content on documentation center 128
FIPS
  enabling 95
first boot 35
first root login 35

H

hardware requirements 47
high level packages

high level packages *(continued)*
EPM ... 23
MPP ... 23
hung or stale mount points, checking for ... 54

I

identity variables ... 35
importing server identity certificates ... 96
install
JDBC driver ... 57
installation
Auxiliary EPM server ... 116
high level packages ... 23
MPP server ... 119
primary EPM server ... 112
single EPM server ... 121
testing ... 87
worksheets ... 112, 116, 119, 121
installing
license file ... 85
Invalid Password ... 103

J

Japanese, configuring on Avaya Enterprise Linux ... 97
JDBC driver, install ... 57

K

Korean, configuring on Avaya Enterprise Linux ... 99

L

License compatibility matrix ... 49
license file, installing ... 85
license requirements ... 49
logs
upgrade ... 101
loss of reporting data
preventing ... 43

M

mount point
checking status ... 54
MPP upgrade
upgrade overview ... 10
MPPs
checking
time synchronization with EPM ... 55
reconnecting after upgrade ... 74, 79
testing after initial installation ... 92
time synchronization ... 103
troubleshooting ... 103
upgrade log files ... 101
checking *(continued)*
upgrading ... 74
upgrading Red Hat Linux on ... 38
worksheet for ... 119
My Docs ... 128

N

NTP
external time source ... 93
synchronizing time with ... 103

O

Oracle
JDBC driver ... 57
OS version number, verifying ... 50
outcall test application ... 88
overview ... 8
Avaya Experience Portal configuration ... 84
single server ... 11

P

Password
Invalid password ... 103
Platform Vendor Independent Check ... 22
preparing
Avaya Enterprise Linux Installer ... 28
prereq checker ... 22
prereq installer ... 22
Product ID
changing ... 102
PVI checker ... 22

R

Red Hat Enterprise Linux
check version number ... 50
overview ...
Auxiliary VPMS overview ... 14
MPP upgrade ... 16
Single server upgrade ... 17
VPMS overview ... 12
Red Hat Linux on EPM ... 36
restoring 6.x or 7.x Auxiliary server ... 110
restoring 6.x or 7.x MPP server ... 109
upgrade overview ... 12, 14, 16, 17
upgrading
Red Hat Linux on MPP ... 38
Red Hat Linux on single server ... 39
upgrading EPM ... 36
upgrading MPP ... 38
upgrading single server ... 39
redhat umask ... 22
related documentation ... 125

reloading environment variables 103
requirements
hardware 47
license 49
ResetProductID script 102
restoring
4.0.x Avaya Enterprise Linux 105
6.x or 7.x Red Hat MPP server 109
6.x or 7.x software with Avaya Enterprise Linux 104
6.x Red Hat MPP server 110
root 35
root certificate 102
running Application Interface test client 88

S

searching for content 128
sharing content 128
sms
upgrade 53
sms processor 53
sort documents by last updated 128
space requirement
upgrading primary EPM on Avaya Enterprise Linux 48
upgrading primary EPM on RHEL 47
speech servers
testing 87
sroot 35
staging 6.x or 7.x backup files before upgrading 27
stale or hung mount points, checking for 54
status of
mount points 54
support 130

T

testing 87
Time synchronization problems 103
time, synchronizing between servers 55
timestamps, not synchronized 103
troubleshooting
hashing algorithm warning 102
incorrect timestamps 103
TTS servers
testing 87

U

umask 22
upgrade 53
software prerequisites 44
verifying external database 56
Upgrade 7
upgrade overview 8
upgrading
Avaya Experience Portal on multiple servers 74
MPPs *(continued)*
EPM
upgrade options 59, 75
EPM options 59, 75
log files 101
MPP software 74
MPPs
upgrade options 70
options 70
reconnecting MPP 79
reconnecting MPPs 74
restoring 4.0.x Avaya Enterprise Linux 105
restoring 6.x or 7.x Red Hat MPP server 109, 110
restoring 6.x or 7.x software 104
stopping mpp service 42
taking MPP offline with 4.x 42
upgrading Auxiliary
EPM
Auxiliary upgrade options 65
EPM options 65
upgrading primary EMP on RHEL 47
upgrading primary EPM on Avaya Enterprise Linux 48

V

verifying
communication between Avaya Experience Portal servers 51
OS version number 50
stale or hung mount points 54
time between Avaya Experience Portal servers 55
videos 129

W

watch list 128
WebLM server
installing license file for 85
worksheets
auxiliary EPM server install 116
MPP server 119
primary EPM server install 112
single EPM server install 121
software upgrade prerequisites 44