Troubleshooting Avaya Aura® Experience Portal

April 2012

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

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

Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”). (see “Third-party Components” for more information).

Copyright

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

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

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

Trademarks

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

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: Diagnostic procedures

Troubleshooting categories

When the Avaya Aura® Experience Portal system experiences problems, the problems are detected in one of the following categories:

Customer-reported problems: The administrator must collect specific information from customer and the system, regarding what actually happened, and how the system behaved

System generated alarms: Avaya Aura® Experience Portal events and alarms provide a way to troubleshoot problems which occur on the Avaya Aura® Experience Portal system. Major and Critical alarms combined with Error and Fatal events identify the large issues. Minor alarms and Warning events can identify small issues.

Call report analysis: The analysis of standard reports reveals the problems so that you can avoid the system failure. For this reason, you must use the system report capabilities to generate and analyze the standard reports.

Avaya Aura® Experience Portal system status

Avaya Aura® Experience Portal generates events and alarms when you make changes in the Avaya Aura® Experience Portal system. Some of these notifications are purely informational, however, others indicate errors. There are two ways to monitor Avaya Aura® Experience Portal events and alarms:

- View internally generated Avaya Aura® Experience Portal events and alarms through the EPM Web interface as described in the *Viewing Avaya Aura® Experience Portal system status* topic in the *Administering Avaya Aura® Experience Portal* guide.
- Use third party network management software to receive SNMP notifications when certain error conditions occur, as described in the *SNMP Agents and Traps* topic in the *Administering Avaya Aura® Experience Portal* guide.

You can also generate an Audit Log report to view recent system configuration changes and login activities as described in the *Creating an Audit Log report* topic in the *Administering Avaya Aura® Experience Portal* guide.

Related topics:

Checking the status of MPPs on page 10

Checking the status of MPPs

The following table provides the tasks you need to perform to check the status of the MPPs in a Avaya Aura® Experience Portal system.

#	Task	✔
1	Log into the EPM as described in the *Logging in to the Avaya Aura® Experience Portal web interface* topic in the *Administering Avaya Aura® Experience Portal* guide.	
2	Check the operational states of all MPPs as described in the *Checking the operational state for one or more MPPs* topic in the *Administering Avaya Aura® Experience Portal* guide. If the operational state of an MPP is: • Running but the MPP is not taking calls, check for a synchronization problem between the EPM and the MPP as described in Identifying synchronization problems between the EPM and an MPP on page 19. • Not running and you did not intentionally place it in this state, continue with this procedure.	
3	Check the alarm status for all MPPs as described in the *Viewing alarms by alarm category* topic in the *Administering Avaya Aura® Experience Portal* guide. If the <System name> Details tab on the System Monitor page indicates any alarm conditions, click a red or yellow alarm symbol. The Alarm Monitor page helps identify which system component is having problems. **Note:** The Alarms column displays one of the following alarm status indicators for all MPP: • Green: There are no active major or critical alarms • Yellow: There are one or more active minor alarms • Red: There are one or more active major or critical alarms	
4	Generate an alarm report, as described in the *Creating an alarm report* topic in the *Administering Avaya Aura® Experience Portal* guide.	

#	Task	✔
	Examine the alarm report for the alarms generated by the system component in question. All alarms have associated events, which are identified in the alarm report. To obtain more details about a particular event, click the event in the **Event Code** column of the report.	
5	Generate an event log report using the Log Viewer, as described in the *Creating an event report* topic in the *Administering Avaya Aura® Experience Portal* guide. Examine the Log Report to see if you can identify other related events that occurred during the same time.	

Related topics:

[Avaya Aura Experience Portal system status](#) on page 9
[Event and alarm logs](#) on page 16
[Identifying synchronization problems between the EPM and an MPP](#) on page 19

Checking the status of port connections

If all MPP servers are correctly functioning and do not indicate any error or alarm conditions, the next step is to check the Port Distribution page. This page provides information about the status of port connections to the Communication Manager.

Note:

For information about configuring the Communication Manager for:

- H.323, see *Avaya Configuration Note 3910*.
- SIP, see *Avaya Configuration Note 3911*.

These configuration notes are available on the Avaya Support site, http://support.avaya.com.

Solution

Procedure

1. Log in to the EPM Web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the EPM main menu, select **Real-Time Monitoring** > **Port Distribution**.
3. If the **Current Allocation** column shows that:

MPP port allocation	Next step
None of the MPPs have allocated ports	No MPP servers have allocated ports on page 12
One or more MPPs do not have allocated ports.	One or more MPPs have no allocated ports on page 13
One or more licensed ports have not been allocated to an MPP.	One or more licensed ports have not been allocated to an MPP server on page 15

No MPP servers have allocated ports

The Port Distribution page shows that none of the MPP servers in the system have allocated ports. This problem can occur because:

- Avaya Aura® Experience Portal cannot connect to the Avaya license server.
- The Avaya Aura® Experience Portal license has expired.
- The Avaya Aura® Experience Portal license server is down.
- The specified gatekeeper address or alternative gatekeeper address is incorrect.

Proposed Solution

Procedure

1. Log in to the EPM Web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the EPM main menu, select **Security** > **Licensing**.
3. On the Licensing page, verify the following:
   - Connection to the Avaya license server.
   - Expiry date on theAvaya Aura® Experience Portal license.
   - Status of the Avaya Aura® Experience Portal license server.
4. From the EPM main menu, select **System Configuration** > **VoIP Connections**.
5. On the VoIP Connections page, check the gatekeeper and alternate gatekeeper addresses.

One or more MPPs have no allocated ports

The Port Distribution page shows that one or more of the MPPs in the system do not have allocated ports. This problem can occur because:

- The MPP has stopped, is not responding, or is offline.
- Avaya Aura® Experience Portal does not have sufficient licensed port connections to support the MPP servers in the system.

Proposed Solution 1

About this task

Check the operational status of each MPP that does not have allocated ports.

Procedure

1. Log in to the EPM Web interface using an account with the Administration or Operations user role.
2. From the EPM main menu, select **Real-Time Monitoring** > **System Monitor**.
3. On the <System name> Details tab, check the **Mode** and **State** column for the MPP servers in the system.

   If the mode of one or more MPP servers is listed as Offline, or if the state is listed as Halted, Not Responding, Restart Needed, or Stopped, continue with Step 4. If all MPP servers are up and running, continue with Proposed Solution 2 on page 14.
4. From the EPM main menu, select **System Management** > **MPP Manager**.
5. On the MPP Manager page, use the Selection check box in the MPP server table to select which MPP you want to change.
6. If you want to:
   - Bring an MPP online:
     1. Click **Online** in the **Mode Commands** group.
     2. Use the Selection check box in the MPP server table to select the MPP.
     3. Click **Start** in the **State Commands** group.
   - Start a stopped or halted MPP, click **Start** in the **State Commands** group.
   - Restart an MPP, click **Restart** in the **State Commands** group.
   - Reboot an MPP, click **Reboot** in the **State Commands** group.

7. When you have finished setting the operational mode, click **Refresh** to ensure the mode is correctly set up.
8. If the MPP does not respond to command through the EPM, reboot the physical MPP server manually.
9. From the EPM main menu, select **Real-Time Monitoring** > **System Monitor**.
10. If all MPP servers are listed as Online and Running, from the EPM main menu, select **Real-Time Monitoring** > **Port Distribution**.
11. Verify that all MPP servers now have allocated ports. If there is still a problem, continue with Proposed Solution 2.

Proposed Solution 2

About this task

Verify that you have created enough VoIP connections.

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** > **VoIP Connections**.
3. If you are using:

VoIP connection type	Next steps
H.323 only	1. Go to the H.323 tab and count the number of stations defined in the **Stations** column. 2. If there are fewer stations than ports, either add more H.323 connections or add more stations to one or more existing connections.
SIP only	1. Go to the SIP tab and look at the **Maximum Simultaneous Calls** defined for the active SIP connection. 2. If the maximum number of calls is less than the total number of licensed ports, click the connection name to open the Change SIP Connection page and increase the maximum number of calls for the connection.
H.323 and SIP	1. Go to the H.323 tab and count the number of stations defined in the **Stations** column. 2. Go to the SIP tab and look at the **Maximum Simultaneous Calls** defined for the active SIP connection.

VoIP connection type	Next steps
	3. If the number of defined stations plus the maximum number of SIP calls does not equal the number of licensed ports available, either increase the number of H.323 stations or the maximum number of SIP calls.

One or more licensed ports have not been allocated to an MPP server

The Port Distribution page shows that one or more licensed ports are not allocated to an MPP server. This problem can occur because:

- The MPP is in Offline or Test mode.
- The maximum call capacity for the MPP is too low.

Proposed Solution 1

About this task

Check the operational status of each MPP that does not have allocated ports. Change the operational status to Online.

Procedure

1. Log in to the EPM Web interface using an account with the Administration or Operations user role.
2. Select **Real-Time Monitoring** > **System Monitor**.
3. On the <System name> Details tab, check the status of the MPP servers in the system.

   If one or more MPP servers is down, continue with Step 4. If all MPP servers are up and running, continue with Proposed Solution 2.
4. From the EPM main menu, select **System Management** > **MPP Manager**.
5. On the MPP Manager page, use the Selection check box in the MPP server table to select which MPP you want to change.
6. Click the desired operational state button in the **Mode Commands** group. You can select:
   - **Test** if the MPP server is currently in Offline mode.
   - **Online** if the MPP server is currently in Offline mode.

7. When you have finished setting the operational mode, click **Refresh** to ensure the mode is correctly set up.

Proposed Solution 2

About this task

Check the maximum call capacity of the MPP. Change the value.

Procedure

1. Log in to the EPM Web interface using an account with the Administration user role.
2. From the EPM main menu, select **Real-Time Monitoring** > **System Monitor** and go to the appropriate <System name> Details tab.
3. In the **Server Name** column, click the name of the MPP whose details you want to view.
4. On the <MPP name> Details page, review the value of the **Maximum Call Capacity** field.

   If this value is too low, Avaya Aura® Experience Portal will not allocate enough ports to the MPP. To increase the number of allocated ports, you must increase the value of the **Maximum Simultaneous Calls** field on the Change MPP Server page.
5. From the EPM main menu, select **System Configuration** > **MPP Server**.
6. On the MPP Servers page, click the name of the MPP you want to reconfigure in the **Name** column.
7. On the Change MPP Server page, update the value in the **Maximum Simultaneous Calls** field.

   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. For more information, see the *MPP server capacity* topic in the *Administering Avaya Aura® Experience Portal* guide.
8. Click **Save** to save your changes.

Event and alarm logs

Other places to look for indications of problems are the event and alarm logs. You can use the Log Viewer and the Alarm Manager to generate reports that can help to diagnose and resolve problems with the system.

When you generate these reports, use the information you collected regarding the time the problems occurred and what components might be involved. As you examine the events and alarms that the system generated on those components during the time the problems occur, you can get a good sense of what the problem is and how to resolve it. Use the event and alarm codes in these reports to diagnose any further problems.

For more information about generating:

- Event reports, see the *Creating an event report* topic in the *Administering Avaya Aura® Experience Portal* guide.
- Alarm reports, see the *Creating an alarm report* topic in the *Administering Avaya Aura® Experience Portal* guide.

You can also use the information from these reports to help identify the call sessions that experienced the problems. Once you identify call sessions, you can check the transcriptions for those call sessions to further diagnose the problem.

Related topics:

Checking the call session on page 21

Cannot generate a log or alarm report

If you cannot generate a Log Report or an Alarm Report within the EPM Web interface, you can still view and examine the event and alarm logs for the EPM. The EPM log file contains the same information as displayed in the Log Report and Alarm Report.

Note:

Examine the EPM log file directly *only* if you cannot use the EPM Web interface to generate a Log Report or Alarm Report.

Proposed Solution

Procedure

In a text editor, open the EPM log file from the following location:
`$AVAYA_VPMS_HOME/logs/avaya.vpms.log`

Checking the application for proper function and behavior

Procedure

1. Check the resources being used by all current applications in the system by selecting **Real-Time Monitoring** > **Active Calls** from the EPM main menu.
2. In Avaya Aura® Experience Portal, create an Application Detail report or Application Summary report. These reports let you view application messages and any `log` tag messages downloaded with the report data.

   For more information, see *Application activity reports* and *Accessing VoiceXML and CCXML Log tag data through Avaya Aura® Experience Portal* topics in the *Administering Avaya Aura® Experience Portal* guide.
3. To view the transcriptions of the call sessions using the Session Detail report.

   For more information, see the *Viewing application transcription data* topic in the *Administering Avaya Aura® Experience Portal* guide.
4. Review the log files for the application server and any Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) servers used by the application.

Enabling Avaya Voice Browser Logging

About this task

Enable Avaya Voice Browser (AVB) logging if you need more information about the application problems that you encountered.

Important:

Enabling AVB logging can cause performance degradation.

Procedure

If you want to:

- Enable AVB logging for all MPPs in your Avaya Aura® Experience Portal system, see the *Setting the global grace period and trace level parameters* topic in the *Administering Avaya Aura® Experience Portal* guide.
- Enable AVB logging on a specific MPP, see the *Changing an MPP* topic in the *Administering Avaya Aura® Experience Portal* guide.

Identifying synchronization problems between the EPM and an MPP

Procedure

1. Log in to the EPM Web interface using an account with the Administration user role.
2. From the EPM main menu, select **Real-Time Monitoring** > **System Monitor** and go to the appropriate <System name> Details tab.
3. In the **Server Name** column, click the name of the MPP.
4. On the <MPP name> Details page, click **Service Menu** in the **Miscellaneous** group.
   The MPP Service Menu opens in a new browser window.
5. Arrange the browser windows so that you can see both the <MPP name> Details page and the MPP Service Menu home page.
6. Compare the following fields on the two pages:

EPM Field and Group	MPP Service Menu Field/Table
Current State in the Operational State group	Run State in the MPP Status table
Current State in the Configuration group	Configuration State in the MPP Status table
Last Successful Poll in the General Information group	Time of last heartbeat in the MPP Status table

Next steps

If these fields do not match, follow the procedure described in Synchronizing the EPM and an MPP on page 19.

Synchronizing the EPM and an MPP

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 Maintenance** > **Log Viewer**.
3. In the Log Viewer page, create an event report for the **EPM** and the MPP you want to synchronize as described in the *Creating an event report* topic in the *Administering Avaya Aura® Experience Portal* guide.

Tip:

When you specify the report criteria, in the **Date and Time** group, make sure the report starts before the last successful poll of the MPP. You can find this date on the <MPP name> Details page.

4. Examine the resulting report for any messages that contain the word "heartbeat" or "poll" and see if these messages have exact information to solve the problem.

   For more information, see the *Events and alarms* topic in the *Administering Avaya Aura® Experience Portal* guide.

5. For more information related to the report, log on to the MPP Service Menu for the MPP:

   a) From the EPM main menu, select **Real-Time Monitoring** > **System Monitor** .
   b) In the **Server Name** column, click the name of the MPP.
   c) On the <MPP name> Details page, click **Service Menu** in the **Miscellaneous** group.

6. Click **Logs** in the MPP Service Menu menu bar.
7. On the Log Directories page, click **MMS**.
8. On the Log Files page, click **MmsServer.log**.
9. Examine the log file to see if the MMS web server has been receiving heartbeat requests from the EPM.
10. If the log file shows that heartbeat requests are received, log onto Linux on the MPP server.
11. Verify that the `mpp` service is running by entering the `/sbin/service mpp status` command.
12. If the `mpp` service is not running, enter the `/sbin/service mpp start` command.
13. Navigate to the httpd logs directory by entering the `cd /var/log/httpd` command.
14. Examine the following log files to see if Apache has been receiving heartbeat requests from the EPM server:

    - `error_log`
    - `ws_access_log`
    - `ws_error_log`

15. If the log files show that heartbeat requests are received, reboot the MPP server.
16. Examine the `$CATALINA_HOME/logs/catalina.out` log file to see if any errors were generated during the reboot.

17. If the problem still exists after the MPP server restarts, reboot the EPM server.

Related topics:

System does not answer or produces only busy signals on page 66

Checking the call session

About this task

You can use information gathered from callers and from event and alarm reports to identify particular call sessions that had problems. Once you identify the problem sessions, use the Call Detail report to view session information.

Procedure

1. Create a Call Detail report as described in the *Creating a Call Detail report* topic in the *Administering Avaya Aura® Experience Portal* guide.
2. Click the **View Session Details** icon at the end of the appropriate row.
3. On the Session Details page for the session, review the call session details for information about the problem that occurred during the session.

Next steps

If you still cannot determine the problem from an examination of the call session, more information is available in the session log file.

Related topics:

Viewing the session log file on page 21

Viewing the session log file

About this task

The log file for the session is called `$AVAYA_MPP_HOME/logs/process/SessMgr/SessionSlot-XXX.log`, where *XXX* is the value of the **Slot** field on the Session Details page.

Procedure

1. On the Session Details page for the call, go to the **Server Information** group.
2. Get the value of the session slot from the **Slot** field.

3. To view the log file through Avaya Aura® Experience Portal:
   a) Log into the MPP Service Menu.
   b) From the MPP Service Menu, select **Logs**.
   c) On the Log Directories page, click **SessMgr**.
   d) On the Log Files page, click **View** or **Download** for the `SessionSlot-`*XXX*`.log` entry that matches the one you want to view.

      As the session log files are large in size, these files might take time to display or save to the location you select for **Download**.

Finding the version numbers for the Avaya Aura® Experience Portal software

About this task

If you need to contact technical support, you should have the version numbers for the Avaya Aura® Experience Portal software available.

Procedure

1. Log in to the EPM Web interface using an account with the Administration, Operations, or Maintenance user role.
2. Click **Help** at the top of any EPM page and select **About**.
   The EPM displays the About Avaya Aura Experience Portal page, which shows the version numbers of the EPM and MPP software.
3. To get the version number for the WebLM server:
   a) From the EPM main menu, select **Security** > **Licensing**.

      Depending on the user role associated with your account, the EPM Web interface displays the Licensing page or the View Licensing page.
   b) Click **Verify**.
      The EPM opens a new browser window displaying the License Administration page for the WebLM license server, which displays the version number for that server.

Chapter 2: Troubleshooting worksheets

Collecting information related to a problem

If problems are reported by customers trying to call in to the system or problems related to outcalls, collect as much information as you can. The following steps include the questions that you need to answer about the problem and the information to collect.

#	Task	✔
1	Obtain the following information from the caller: What number did the caller dial (the DNIS)? What number was the caller calling from (the ANI)? What time (and day) did the caller try to call the system, and what time zone was the caller calling from? How did the system respond when the caller tried to call in? For example, did the system: • Give a busy signal? • Ring but not answer? • End the call unexpectedly in the middle of the session? • Produce garbled or unrecognizable output? • Fail to recognize the responses of the caller? • Suddenly stop responding to the caller?	
2	Using the information from the caller: • Try to reproduce the system response. • Collect whatever additional information that you can from your own observations of the system responses. If you can reproduce the system response and the problem, you can easily troubleshoot the problem.	
3	Check the Avaya Aura® Experience Portal system to see if any component see if any component fails or is not functioning correctly. For example, check the MPP status.	
4	Check the event and alarm logs.	
5	Check the transcription of the call session to learn exactly what happened with the call.	

#	Task	✔
6	If you are unable to troubleshoot the problem and need to contact customer support: • Collect and pack the diagnostic logs on the MPP as described in Packing MPP logs and transcriptions in a TAR file on page 159. • Get the version numbers of the Avaya Aura® Experience Portal software as described in Finding the version numbers for the Avaya Aura Experience Portal software on page 22.	

Related topics:

Event and alarm logs on page 16
Checking the call session on page 21
Packing MPP logs and transcriptions in a TAR file on page 159

Information needed for Services to initiate troubleshooting

When you need to contact customer support, collect as much information as you can. The following steps include the questions that you need to answer about the problem and the information to collect.

Note:

Steps 3 to 11 are mandatory.

#	Task	✔
1	You must update Avaya Aura® Experience Portal with the most recent Service Pack installed on the system. You can get the latest Service Pack from the Avaya Support site at http://support.avaya.com.	
2	Check if the issue is a known issue that is listed as Product Support Notice (PSN). PSN's are posted on the Avaya support site at http://support.avaya.com under the appropriate release in Avaya Aura® Experience Portal product category.	
3	Detailed description of the issue.	
4	Release information of the Avaya Aura® Experience Portal on which you are facing the issue.	
5	Is the system a fresh install or an upgrade. In case of an upgrade, from which version is the system upgraded.	
6	Version of the RHEL or Avaya Linux installed.	

#	Task	✔
7	Total Number of EPM and MPPs deployed; along with the port and license information.	
8	Versions and license information of CM (PBX/switch), ASR and TTS.	
9	Remote access details for accessing the machine remotely to debug the problem.	
10	Warning and Errors seen in the logs. Export the alarm logs/Log Report from EPM web page.	
11	Collect the EPM and MPP logs. For details see, Collecting logs from EPM on page 25 and Collecting logs from MPP on page 26.	
12	Special instructions, if any.	

Related topics:

Collecting logs from EPM on page 25
Collecting logs from MPP on page 26

Collecting logs from EPM

Procedure

1. Log in to the EPM web interface using an account with the Administration user role.
2. Collect the logs from the Alarm Manager menu:
   a) From the EPM main menu, select System Maintenance > Alarm Manager.
   b) Enter the appropriate time when the failure occurred in the **Date and Time** field.
   c) Click **OK** to generate the alarm report.
   d) Export the report.
3. Collect the logs from the Log Viewer menu:
   a) From the EPM main menu, select System Maintenance > Log Viewer.
   b) Enter the appropriate time when the failure occurred in the **Date and Time** field.
   c) Click **OK** to generate the report.
   d) Export the report.
4. Collect the logs from the Reports menu:
   a) From the EPM main menu, select Reports > Standard Reports.
   b) Click on the Call Detail report.

c) Enter the appropriate time around when the failure occurred in the **Date and Time** field.
d) Click **OK** to generate the report.
e) Click **Export** and then select **Export as XLS format** or **Export as PDF format** to export the report in the desired format.
f) Repeat this procedure for the Session Detail report.

5. Collect all log files from `/opt/Avaya/ExperiencePortal/VPMS/logs`.
6. Collect the `catalina.*` files from the `$CATALINA_HOME/logs` folder.

Collecting logs from MPP

Procedure

On each MPP, enter the `getmpplogs.sh --logs --transcriptions --debugfiles` command to get the MPP logs.
The filename of the stored logs and the path appears.

Chapter 3: Troubleshooting EPM issues

Authorized user cannot log in to EPM

An authorized individual cannot log in to the EPM. This problem typically occurs because:

- The user does not have the correct login ID or password.
- The user entered the login ID or password incorrectly more than the allowable number of times, and the account is locked.

Proposed Solution

Procedure

1. Verify that the user has entered the correct login ID and password.
2. Check to see if the account is locked.

   For more information, see the *Unlocking a locked user account* topic in the *Administering Avaya Aura® Experience Portal* guide.
3. If the account is locked, have a system administrator unlock it or wait for the lockout period to end.

   You can set the Lockout period on the **Login Options** web page.

User cannot log in to the EPM Web interface remotely

If you cannot log into the EPM Web interface remotely, the primary EPM server may have lost its network connection or Tomcat may not be running.

To investigate this, you need to check the physical network connection and test the communication between the primary EPM server and the MPP servers. This procedure assumes that:

- Your Avaya Aura® Experience Portal deployment consists of the EPM and MPP software running on two or more dedicated servers.
- ICMP is not disabled on your system and you can **ping** one server from another.

Proposed Solution

Procedure

1. Log into Linux on another server in the Avaya Aura® Experience Portal network and enter the `ping` *`epm_identifier`* command, where *`epm_identifier`* is the hostname or IP address for the primary EPM server.
2. If the **ping** is unsuccessful:
   a) Go to the physical primary EPM server and make sure that the network cable is properly connected.
   b) Enter the **ping** command again.
3. If the primary EPM server responds to the **ping** command, log into Linux on the primary EPM server as any user.
4. Enter the `ping` *`mpp_identifier`* command, where *`mpp_identifier`* is the hostname or IP address for one of the MPP servers.
5. If the **ping** command is unsuccessful, repeat the **ping** command specifying another MPP in the Avaya Aura® Experience Portal system until you receive a successful `ping` message or you have tried contacting all available MPP servers..

   If any MPP servers on the system respond to the **ping** command, then the network is functioning and the issue could be caused by problems with Tomcat on the primary EPM server. Follow the procedures in Troubleshooting vpms service issues on page 29.
6. If you cannot ping any MPP servers from the primary EPM server, restart the network connection for the primary EPM server. If there is:
   - More than one network connection, enter the `/sbin/service network restart` command.
   - A single network connection, enter the commands:
     1. `ifconfig eth`*`xx`* `down`
     2. `ifconfig eth`*`xx`* `up`

Where *xx* is the name of the ethernet connection that you are restarting. The default for an Avaya-provided server is `eth0`.

EPM pages do not display or have garbled content

If the EPM pages do not display at all or display garbled content, Tomcat may not be running or may have one or more processes that are hung or not functioning correctly.

Note:

If none of the following recommended actions resolves the problem, contact your Avaya technical support representative for assistance.

Proposed Solution

Procedure

1. Ensure that the *vpms* service and all its required components are running.
2. Ensure that the Axis Web services container is running.
3. Check for PostgreSQL issues.

Troubleshooting vpms service issues

If the EPM pages do not display properly, this issue can be caused by problems with the *vpms* service or one of its components.

Proposed Solution 1: Verifying the vpms service status

Procedure

1. Check the status of the *vpms* service by entering the `service vpms status` command.
   If the *vpms* service is running properly, the command displays the messages indicating that the `tomcat`, `SL`, and `ActiveMQ` services are all running. It ends with the message: `Overall Status: VPMS is running`.
2. If the *vpms* service is:

- Not running, start it as described in Proposed Solution 2: Start the vpms service on page 30, below.
- Running, there may be a problem with one of the required components. Restart the *vpms* service as described in Proposed Solution 3: Restart the vpms service on page 30, below.

Proposed Solution 2: Start the vpms service

Procedure

1. Start the *vpms* service by entering the `/sbin/service vpms start` command.
   You will see a series of messages as the command starts several EPM components. When the command has successfully started all relevant components, it displays the message: `VPMS Start Status: [ OK ]`.
2. Try to log into the EPM Web interface again.
3. If the problem persists, there may be an issue with Tomcat. Check the status of the individual Tomcat processes as described in Proposed Solution 4: Checking the Tomcat processes on page 31, below.

Proposed Solution 3: Restart the vpms service

Procedure

1. Restart the *vpms* service by entering the `/sbin/service vpms restart` command.
   You will see a series of messages as the command starts to shut down EPM components. When the command has successfully stopped all relevant components, it displays the message: `VPMS Shutdown Status: [ OK ]`.

   The command immediately starts the relevant components. When it has finished, it displays the message: `VPMS Start Status: [ OK ]`.
2. Wait for several minutes to let the service initialize, then verify that there is only one *vpms* service by entering the *`service vpms status`* command.
3. Try to log into the EPM Web interface again.
4. If the problem persists, there may be an issue with Tomcat. Check the status of the individual Tomcat processes as described in Proposed Solution 4: Checking the Tomcat processes on page 31, below.

Proposed Solution 4: Checking the Tomcat processes

About this task

If Tomcat is running but one or more of its processes are not functioning correctly, you can have problems with loading the EPM pages. To check Tomcat processes and verify that the processes are running:

Procedure

1. At the Linux command line prompt, enter the `ps -ax | grep java` command. The system should respond with output similar to the following:

   ```
   9841 pts/0 S 0:36      /usr/java/j2sdk1.5.0_12/bin/java -
   server -Xmx1024m
   -XX:MaxNewSize=30m -XX:NewSize=30m  -XX:+UseParNewGC -XX:
   +UseConcMarkSweepGC
   -XX:CMSInitiatingOccupancyFraction=60 -
   XX:ThreadStackSize=1536  -Djava.awt.headless=true
   -Djava.endorsed.dirs=/opt/Tomcat/apache-tomcat-5.5.23/
   common/endorsed -classpath
   /usr/java/j2sdk1.5.0_12/lib/tools.jar:/opt/Tomcat/apache-
   tomcat-5.5.23
   ```

2. In a Web browser window, enter the URL `http://`*`epm_host_address`*`/index.jsp`, where *`epm_host_address`* is the fully qualified domain name or IP address of the primary EPM server.
   The browser should display the Apache Jakarta Project page.
3. If the system responded with the expected output, examine the Tomcat log file for indications that Tomcat is experiencing errors or other problems that might be affecting its performance. This log file is located at `$CATALINA_HOME/logs/catalina.out`.
4. If the system does not respond with the expected output, verify that the Axis Web services container is configured properly as described in Verifying Axis configuration on page 31.

Verifying Axis configuration

Axis is a Web services container that runs on top of Tomcat. If Tomcat is running but Axis is not configured properly, you can experience problems with the EPM Web interface.

Note:
Because Axis runs on top of Tomcat, if Tomcat is not running, neither is Axis.

Related topics:

Reinstalling the primary EPM software on a dedicated EPM server on page 133
Reinstalling the EPM software in a single server system on page 135

Proposed Solution

Procedure

1. In your Web browser, enter the URL `http://epm_host_address/axis`

   Where *epm_host_address* is the fully qualified domain name or IP address of the EPM server.
2. On the Apache Axis configuration page, click **Validation**.
3. On the Axis Happiness Page, verify that:
   - Under **Needed Components**, all components are listed as **Found**.
   - Under **Optional Components**, there are no optional components missing that you consider required.
4. Click **Back**.
5. On the Apache Axis configuration page, click **List**.
6. On the And now...Some Services page, verify that all the following services are listed:
   - LogServer-1.0 (wsdl)
   - AdminService (wsdl)
   - AppIntfWS (wsdl)
   - Version (wsdl)
   - Report (wsdl)
   - EPReport4 (wsdl)
   - AlarmServer-1.0 (wsdl)
   - AlarmRetrieverServer-1.0 (wsdl)
   - AlarmConfigServer-1.0 (wsdl)
   - LogRetrieverServer-1.0 (wsdl)
7. If any required components or services are not listed, reinstall the EPM.
8. Is Axis configured properly?
   - If yes, verify that PostgreSQL is running properly, as described in Troubleshooting PostgreSQL issues on page 33.

- If no, reinstall the EPM software.

Troubleshooting PostgreSQL issues

PostgreSQL is the database server that provides access to the databases required by the EPM Web interface. If PostgreSQL is not running or is experiencing difficulties, the EPM pages can exhibit unexpected behavior or cease to respond at all.

Note:

The Avaya Aura® Experience Portal internal database should not be modified. If you want to modify the database, contact your Avaya technical support representative for assistance.

The following solutions help to identify and troubleshoot issues with PostgreSQL.

Proposed Solution 1: Verifying the PostgreSQL status

Procedure

1. At the Linux command line prompt, enter the `/sbin/service postgresql status` command.
2. Does the system display a message that the PostgreSQL service is running?
   - If yes, verify that the `postmaster` process is running as described in Proposed Solution 2: Verifying that the postmaster process is running on page 33.
   - If no, start the PostgreSQL service as described in Proposed Solution 3: Starting PostgreSQL on page 34.

Proposed Solution 2: Verifying that the postmaster process is running

Procedure

1. At the Linux command line prompt, enter the `ps -edf | grep postgres` command.
2. Is the `postmaster` process listed?
   - If yes, and the problem with the EPM pages continues, reboot the EPM server. If the problem continues, contact your Avaya technical support representative for assistance.

- If no, try stopping and restarting PostgreSQL as described in Proposed Solution 4: Stopping and restarting PostgreSQL on page 34.

Proposed Solution 3: Starting PostgreSQL

Procedure

1. At the Linux command line prompt, start PostgreSQL by entering the `/sbin/service postgresql start` command.
   The system responds with a series of messages indicating that the PostgreSQL service is started.
2. Did this resolve the problem, and does the system now display EPM pages properly?
   - If yes, no further action is required.
   - If no, reboot the EPM server. If the problem continues, contact your Avaya technical support representative for assistance.

Proposed Solution 4: Stopping and restarting PostgreSQL

About this task

If PostgreSQL is running but does not appear to be functioning correctly, you can try stopping and restarting PostgreSQL.

Procedure

1. At the Linux command line prompt, stop PostgreSQL by entering the `/sbin/service postgresql stop` command.
   The system responds with a series of messages indicating that the PostgreSQL service is stopped.
2. At the Linux command line prompt, restart PostgreSQL by entering the `/sbin/service postgresql start` command.
   The system responds with a series of messages indicating that the PostgreSQL service is started.
3. Did this resolve the problem, and does the system now display EPM pages properly?
   - If yes, no further action is required.

- If no, reboot the EPM server. If that does not resolve the problem, contact your Avaya technical support representative for assistance.

Cannot view or use a EPM page

You cannot view or use the desired EPM pages. This problem typically occurs because you are assigned with a user role that does not permit access to certain pages. This is not an error, but a system design feature.

Proposed Solution

About this task

Procedure

To gain access to those pages, you must obtain a user account with a different user role.

Cannot access or view certain features in EPM

You cannot access or view the desired EPM features and options. This is not an error, but a system design feature.

This problem typically occurs because of the following reasons:

- The role assigned to you does not permit access to certain features or options on the EPM pages. For example, the role assigned to you has permissions to add a user account but does not permit to delete any user accounts.
- You are not assigned with the correct role.
- The role assigned to you is not configured for appropriate access. For example, where a reporting role should permit you to generate all the reports, it was not configured correctly to do so. It allows you to generate standard reports but does not permit to generate a custom report or schedule a report.

With the role based access, you can perform only those actions for which you have access permissions. The options for performing other actions are either not displayed or disabled on the EPM pages for that particular feature.

Proposed Solution

About this task

Procedure

To gain access to those pages, you must obtain a user account with a different user role.

EPM screen not displayed after restoring Avaya Aura® Experience Portal on a new server

EPM screen is not displayed after restoring Avaya Aura® Experience Portal on a new server. This problem typically occurs when the postgres password on the new EPM server is different from the password configured on the primary EPM server.

Related topics:

Proposed Solution on page 36

Proposed Solution

Before you begin

- Make sure you have taken back up of Avaya Aura® Experience Portal data on the backup server.
- Make sure you have restored the Avaya Aura® Experience Portal backup data on a new server.
- EPM and Tomcat application server are running.

Procedure

1. Log in to Linux on the primary or auxiliary EPM server. If you are an Avaya Services representative and are using Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server:
   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and enter the `su - root` command to change the user to sroot.

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

2. Navigate to the `Support/VP-Tools/SetDbPassword` directory.

   Enter the `cd $AVAYA_HOME/Support/VP-Tools/SetDbPassword` command. `$AVAYA_HOME` is an environmental variable pointing to the name of the installation directory specified during the Avaya Aura® Experience Portal software installation.

   The default value is `/opt/Avaya/ExperiencePortal`.

3. To run the script:

   Enter the `bash SetDbpassword.sh update -u` *`username`* `-p` *`password`* command.

   Where:

   - *`username`* is the name of the user account whose password you want to change.
   - *`password`* is the new password you want to use for this account.

   For example, to set the `postgres` password to NewPostgres1, you must enter the `bash SetDbpassword.sh update -u postgres -p NewPostgres1` command.

   If you change the password for the postgres account, Avaya Aura® Experience Portal stops and then restarts the EPM service.

4. Verify if the service has started.

   Enter the `/sbin/service vpms status` command.

EPM pages display ??? in the fields

If one or more EPM pages display ??? in the fields, the language settings in the Web browser are incorrect.

Proposed Solution

Procedure

1. In Internet Explorer, select **Tools** > **Internet Options**.

2. In the Internet Options dialog box, select the **General** tab.
3. Click **Languages** and make sure that the list includes US English.

EPM running out of disk space

If the EPM server runs out of disk space, the system can be configured to retain a large amount of historical data.

Note:
If none of the following recommended actions resolve the problem, contact your Avaya technical support representative for assistance.

Prerequisites

About this task

Prior to following any of the proposed solutions, you need to check the disk space usage. This will help you determine which proposed solution to follow.

Note:
Do not delete files from the server without analyzing the possible outcome.

Procedure

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

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and change the user to root by entering the su - command.
2. Isolate the directory that uses the maximum disk space.
   a) Enter the **du –b --max-depth=1 -h /** command to display a list of top level directories on the server along with the currently-occupied disk space.
   The table below is an example of the output:

```
[sroot@vp-a11 /]# du –b --max-depth=1 -h /
20K /mnt
12M /tmp
1.8G /home
```

```
5.9M /bin
24K /root
9.3G /opt
995M /var
16G /
[sroot@vp-a11 /]#
```

b) Check the output to determine which directory uses the maximum disk space. In the example given above, the `/opt` directory uses the maximum space.

c) To further isolate the directory that uses the maximum space, enter the **`du –b --max-depth=1 -h /`**<*directory name*> command where <*directory name*> is the directory uses the maximum space.
For example, enter the **`du –b --max-depth=1 -h /opt`** command to check the directories under the`/opt` directory.

Note:

Repeat the command to locate the specific directory or file that uses the maximum disk space.

3. Analyze the information, and based on the observations follow up with the possible solutions, as mentioned in the steps below.
4. If the `/var` directory uses maximum disk space, it is possible that the retention period for the report data (Call/Session, Application, and/or Performance), Alarm Logs, Event Log, or Audit Logs are set too high. When Avaya Aura® Experience Portal is initially installed, the retention period for these tables are set to default values. Depending on the system load and applications being run, these values may need change to retain less data and thereby use less disk space.

Note:

The database that Avaya Aura® Experience Portal uses is located in the `/var` directory.

a) From the EPM menu, select **Real Time Monitoring > System Monitor**.

b) In the **Server Name** column, select the link for EPM.

c) Use the **<EPM> Details** page to view the detailed database status of the primary EPM server. The **Database Status** section shows the database tables that use the most disk space and the corresponding size, in bytes. The database tables are listed in descending order as per the size.

d) Choose the **Proposed Solution** based on which table or tables is using more disk space than expected:

- Use **Proposed Solution 1** for the following tables:
  - CDR
  - SDR
  - vpapplog
  - vpperformance

- Use **Proposed Solution 2** for the following tables:
  - alarmrecord
  - cslog
  - csadminauditlog
- Use **Proposed Solution 3** for the vpreportresults table

5. If the `/opt/Avaya/InstallAgent/download` directory uses the maximum disk space, use **Proposed Solution 4** to free up disk space by removing the old ISO image files. Avaya Aura® Experience Portal stores a copy of the Avaya Aura® Experience Portal ISO image file in this directory.

   The ISO image file is used during a managed upgrade . As newer versions of Avaya Aura® Experience Portal are installed, the older ISO image files are not removed.

6. If the `/opt` directory uses maximum disk space, then it is possible that there is a file that is abnormally using a lot of disk space. Avaya Aura® Experience Portal is installed in this directory (`/opt/Avaya/ExperiencePortal`) by default. There are no Avaya Aura® Experience Portal related files in the `/opt` directory that use a large amount of disk space. But depending on other applications running on the EPM server, there may be components using the disk space.
7. If another directory uses the maximum disk space, contact your Avaya technical support representative for assistance.

Important:

Do not delete files unless the directory or file that uses the maximum disk space is identified.

Proposed Solution 1: Adjust report data retention and free disk space

Procedure

1. Log in to the EPM web interface using an account with the Administration user role.

Important:

As an alternative to steps 2 and 3, you can run the **`PurgeReportDataLocalDB`** and **`PurgeReportDataExtDB`** scripts. These scripts recover the disk space used by the database tables. The time taken to recover the disk space depends on the amount of data in the database tables. However, this activity purges all data in the CDR, SDR, vpapplog, and vpperformance tables. All existing data in these tables is permanently lost. For more information, see the *Purging report data from a local Avaya Aura® Experience Portal database* and *Purging Avaya*

Aura® Experience Portal report data from an external database topics in the *Administering Avaya Aura® Experience Portal* guide.

2. From the EPM menu, select **System Configuration > Report Data**.
   a) On the **Report Data Configuration** page, verify that the **Purge Records** option in the **Report Database Record Data** section is set to **Yes**.
   b) Depending on which table or tables has high disk use, adjust the Call/Session (CDR and SDR), Application (vpapplog), or Performance (vpperformance) retention period to a smaller number of days.
   c) Click **Apply** to save your changes.

      The scheduled purge tasks for the Call/Session, Application, and Performance logs are run at 02:00 hours by default, to purge records from the tables that are older than the configured retention period.

      For more information on retention periods and the purging of old records, see the *Report Data Configuration page field descriptions* topic in the *Administering Avaya Aura® Experience Portal* guide.
3. After the scheduled purge task is completed (which is typically the day after you make changes to the **Report Data Configuration** page in EPM), stop the *vpms* service.
4. To run the script:

   Enter the `$AVAYA_HOME/Support/VP-Tools/CleanLogsLocalDB <table name>` command.

   The above command enables you to recover the unused disk space allocated to that table, where <table name> is the name of the table from which you want to recover disk space.

   For example: **`$AVAYA_HOME/Support/VP-Tools/CleanLogsLocalDB vpperformance`**

Proposed Solution 2: Adjust Alarm/Log/Audit retention and free disk space

Procedure

1. Log in to the EPM web interface using an account with the Administration user role.
2. From the EPM menu, select **System Configuration > Alarm/Log Options**.
3. On the **Alarm/Log Options** page, depending on which table or tables has the maximum disk use:

a) Verify that the **Purge Enabled** option in the Alarms, Logs, or Audit Logs section is set to **Yes**.
b) Adjust the **Retention Period** in the Alarms, Logs, or Audit Logs section to a smaller number of days.
c) Click **Apply** to save your changes.

   The scheduled purge tasks for Alarms, Logs, or Audit Logs are run to purge records from the tables that are older than the configured retention period at midnight by default.

   For more information on retention periods and the purging of old records, refer to the *Alarm/Log Options page field descriptions* topic in the *Administering Avaya Aura® Experience Portal* guide.

4. After the scheduled purge task is completed, (which is typically the day after you make changes to the **Alarm/Log Options** page in EPM) stop the VPMS services.
5. To run the script:

   Enter the `$AVAYA_HOME/Support/VP-Tools/CleanLogsLocalDB <table name>` command.

   The above command enables you to recover the unused disk space allocated to that table, where <*table name*> is the name of the table (alarmrecord, cslog, or csadminauditlog) from which you want to recover disk space.

   For example: **`$AVAYA_HOME/Support/VP-Tools/CleanLogsLocalDB alarmrecord`**.

   Note:

   The script may also take several minutes to run, depending on how much disk space is being recovered.
6. Enter the command.

   The above script enables you to recover the unused disk space allocated to that table, where <*table name*> is the name of the table (alarmrecord, cslog, or csadminauditlog) from which you want to recover disk space.

   For example: **`$AVAYA_HOME/Support/VP-Tools/CleanLogLocalDB alarmrecord`**

   Note:

   The script may also take several minutes to run, depending on how much disk space is being recovered.

Proposed Solution 3: Adjust scheduled report output retention and free disk space

Procedure

1. Log in to Linux on the primary or auxiliary EPM server. If you are an Avaya Services representative, and are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:
   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and enter the `su - root` command to change the user to sroot.

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and enter the `su -` command to change the user to root.
2. From the EPM menu, select **System Configuration > Report Data**.
3. On the **Report Data Configuration** page, edit the **Scheduled Reports** section as follows:
   a) Set the **Output Folder Size** to a lower number in order to reduce the amount of disk space that the scheduled reports can use.
   b) Set all the **Output Retention (days)** settings to lower numbers to reduce the number of days the reports are retained and the amount of disk space the scheduled reports use.
   c) Click **Apply** to save your changes.

   The scheduled purge tasks for the reports are run at 02:00 hours by default, to purge records from the tables that are older than the configured retention period.

Proposed Solution 4: Remove older copies of the Avaya Aura® Experience Portal ISO image file

Procedure

1. Log in to the EPM using an administrative account and open a command window.
2. Change directories to the location of the ISO image files:
   `cd $AVAYA_IA_HOME/download`
3. Remove all ISO image files except the file with the newest version.

EPM server fails due to hardware problems

The EPM server fails due to hardware problems, and you need to move the software to a different server.

Proposed Solution

Procedure

Move the EPM software to a new server, as described in the *Move the EPM software to a different server machine* topic in the *Administering Avaya Aura® Experience Portal* guide.

SIP: The root CA certificate will expire in {0} days

When the root certificate on the EPM expires, you need to generate a new certificate by using the **`UpdateRootCertificate.sh`** script.

Related topics:

Proposed Solution on page 44

Proposed Solution

Procedure

1. Log onto Linux on the primary EPM server.

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

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

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

2. Navigate to the Support/VP-Tools directory by entering the **`cd $AVAYA_HOME/Support/VP-Tools`** command.

   $AVAYA_HOME is the environment variable pointing to the name of the installation directory specified during the Avaya Aura® Experience Portal software installation. The default value is`/opt/Avaya/ExperiencePortal`.

   Tip:

   This script is also available in the Support/VP-Tools directory of the Avaya Aura® Experience Portal installation DVD.

3. To run the script:

   Enter the `UpdateRootCertificate` command to generate a new security certificate.

4. Type `Y` and press `Enter` when prompted, to restart the `vpms` service.

   Note:

   - Restart all MPPs for the new security certificate to take effect.
   - If the Avaya Aura® Experience Portal system uses SIP Connection over TLS, then ensure that the SIP Connection server is updated with the newly generated certificate.

Chapter 4: Troubleshooting MPP issues

Isolating an MPP for troubleshooting

Before you begin

If desired, on the Communication Manager PBX for the system, create a special hunt group for maintenance numbers.

Make sure that at least one H.323 station has been defined as a maintenance number as described in the *Defining maintenance stations for an H.323 connection* topic in the *Administering Avaya Aura® Experience Portal* guide.

About this task

If your system has multiple MPPs, and a single MPP appears to be having problems, you can isolate the suspect MPP to facilitate the troubleshooting process. If you isolate an MPP in Test mode, you can direct test calls to that MPP only.

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** > **Applications**.
3. On the Applications page, in the **Launch** column, ensure that at least one speech application is specifically associated with the maintenance stations defined for the H.323 connection.
4. If no application is assigned to handle the maintenance stations:
   - Add a new application as described in the *Adding a speech application to Avaya Aura® Experience Portal* topic in the *Administering Avaya Aura® Experience Portal* guide, ensure you specify the maintenance stations in the **Application Launch** group on the Add Application page.
   - Change an existing application so that it is specifically associated with the maintenance station as described in the *Adding a speech application to Avaya Aura® Experience Portal* topic in the *Administering Avaya Aura® Experience Portal* guide, ensure you specify the maintenance stations in the **Application Launch** group on the Change Application page.

Related topics:

Monitoring call progress in real time on page 72

Checking the basic status of an MPP

If the MPP is not functioning correctly, check the basic status of the MPP and its key processes.

Note:

These strategies assume that you have logged in to the EPM and have checked the <System name> Details tab on the System Monitor page.

Related topics:

Check the configuration state of the MPP on page 51

Proposed Solution

Procedure

1. Check the operational state of the MPP.
2. Check the configuration state of the MPP.
3. Check the states of the critical MPP processes.

Checking the operational state of an MPP

If the EPM <System name> Details tab on the System Monitor page indicates that the operational state of the MPP is any state other than **Running**, you can verify the operational state.

Related topics:

Check the configuration state of the MPP on page 51

Proposed Solution 1: if you can log in to the MPP Service Menu

Procedure

1. Log in to the MPP Service Menu, as described in the *Logging in to the MPP Service Menu* topic in the *Administering Avaya Aura® Experience Portal* guide.
2. In the **MPP Status** table on the MPP Service Menu home page, look at the value of the **Run state** field. If this field is:
   - **Running**, the problem lies in the communication between the primary EPM server and the MPP. Verify that the servers can communicate as described in the *Verifying communication between the primary EPM server and all other servers* topic in the *Implementing Avaya Aura® Experience Portal on multiple servers* guide.
   - Any other state, start the MPP as described in Changing the operational state for one or more MPPs. If you cannot start the MPP, check the status of the httpd daemon process. For more information, see Checking the state of an MPP process on page 54.

Proposed Solution 2: if you cannot log in to the MPP Service Menu

Procedure

1. If you cannot log in to the MPP Service Menu, enter the `stat.php` command on the MPP to determine the operational state of the MPP.
2. Check the status of the httpd daemon process. For more information, see For more information, see Checking the state of an MPP process on page 54.

MPP operational states

State	Description
Booting	The MPP is in the process of restarting and is not yet ready to take new calls. It is not responding to heartbeats and last MPP state was Rebooting. If the MPP remains in this state for more than 10 minutes, the state changes to Not Responding.

State	Description
Degraded	The MPP is running but it is not functioning at full capacity. This usually means that: • Some of the H.323 or SIP telephony resources assigned to the MPP are not registered with the switch. To check them, see the *Viewing telephony port distribution* topic in the *Administering Avaya Aura® Experience Portal* guide. • Enough ports have gone out of service to trigger a fatal alarm. The percentage of out of service ports that trigger such an alarm is specified in the **Out of Service Threshold** group on the VoIP Settings page. • A critical process has stopped on the MPP server. If an MPP has issued a fatal event and remains in that state for three minutes, Avaya Aura® Experience Portal automatically restarts the MPP in an attempt to fix the problem. If the problem persists after the restart, Avaya Aura® Experience Portal tries to restart the MPP up to two more times. If after three restarts the MPP is still encountering fatal errors, the state changes to Error.
Error	The MPP has encountered a severe problem and cannot recover.
Halted	The MPP is no longer responding to heartbeats because it received a **`Halt`** command. The MPP cannot be restarted until its server machine has been manually restarted.
Halting	The MPP is responding to heartbeats but is not taking new calls. Avaya Aura® Experience Portal shuts down the corresponding server machine after all calls in progress are completed or the grace period ends, whichever comes first. Once an MPP has halted, you must manually turn on the corresponding server machine before the MPP can be restarted.
Never Used	The MPP has never successfully responded to a heartbeat request. New MPPs start to receive heartbeat requests during the next polling interval after they have been configured. This state occurs when an MPP has either not yet been sent a heartbeat request after it was added or the MPP did not respond to the heartbeat request.
Not Responding	The MPP is not responding to heartbeat requests and it has not received a **`Restart`** or **`Halt`** command. You should manually check the MPP server machine.
Rebooting	The MPP is responding to heartbeats but is not taking new calls. Avaya Aura® Experience Portal reboots the corresponding server machine after all calls in progress are completed or the grace period ends, whichever comes first.
Recovering	The MPP has encountered a problem and is attempting to recover.
Restart Needed	This state is most often reached when the MPP has encountered a problem that it cannot recover from and it requires a manual restart. However, it may also appear for an MPP when the EPM software has been upgraded and the

State	Description
	MPP software has not. In that case, the state should update automatically when you upgrade the MPP software.
Running	The MPP is responding to heartbeat requests and is accepting new calls.
Starting	The MPP is responding to heartbeats but not taking new calls because it is transitioning from the Stopped state to the Running state.
Stopped	The MPP is responding to heartbeats but is not taking new calls. The MPP enters this state while it initializes after it restarts or when a **Stop** command is received. Avaya Aura® Experience Portal will restart the MPP automatically if the MPP: • Stopped unexpectedly and the **Auto Restart** option is selected for that MPP. In this case, Avaya Aura® Experience Portal restarts the MPP immediately. • Has a specified restart schedule. In this case, Avaya Aura® Experience Portal restarts the MPP when the scheduled restart time arrives whether the MPP stopped because of an explicit **Stop** command or because the MPP encountered a problem and was not configured to restart automatically.
Stopping	The MPP is responding to heartbeats but is not taking new calls. Avaya Aura® Experience Portal stops the corresponding server machine after all calls in progress are completed or the grace period ends, whichever comes first.

Check the configuration state of the MPP

Procedure

1. Verify on the MPP Service Menu home that the **Configuration state** field in the **MPP Status** table says **Configuration OK**.
2. If the value of the **Configuration state** field is *not* **Configuration OK**, locate the indicated state in the following table and perform the corrective action.

Configuration state	Corrective action
No Configuration	This state is most commonly seen just after the mpp daemon has started. If the **Telephony configuration needed** state does not automatically replace this state, see MPP is in an unexpected operational state on page 63.
Telephony configuration needed	The MPP has received configuration parameters from the EPM, but has not yet been assigned any ports. If the MPP is in the Running operational state, but the **Configuration state** remains in this state, check the Port

Configuration state	Corrective action
	Distribution page to see if any ports have been assigned to the MPP. If the MPP has assigned ports, check the Log Viewer for errors that might prevent the EPM from sending port information to the MPP. For more information, see the *Creating an event report* topic in the *Administering Avaya Aura® Experience Portal* guide.
Restart Needed	An administrator has made a change to the system that requires that the MPP be restarted. Restart the MPP, as described in the *Restarting one or more MPP servers* topic in the *Administering Avaya Aura® Experience Portal* guide.
Reboot Needed	An administrator has made a change to the system that requires that the MPP be rebooted. Reboot the MPP. For more information, and the procedure, see the *Changing the operational state for one or more MPPs* topic in the *Administering Avaya Aura® Experience Portal* guide.

3. In the menu on the left, click **Diagnostics**.
4. On the Diagnostics page, click **Check connections to servers**.
5. On the Check Server Connections page, verify the status of the connections to the ASR, TTS, telephony, and application servers.
6. If the connection status is okay, click **Resources** in the main menu.
7. On the Resources page, click **Telephony**.

   Tip:

   If you cannot log in to the MPP Service Menu, you can use the administrative scripts described in Administrative scripts available on the MPP on page 55 to view the MPP status and configured telephony and speech server resources.
8. If the appropriate telephony resources table displays data and if one or more of the switch settings for the Communication Manager are not correct, troubleshoot the indicated problem between the Communication Managerand the MPP:
   a) Create a log report and check for telephony errors logged on the EPM.
   b) Check the Session Manager log files for telephony-related errors.
9. If the appropriate telephony resources table does not display data:
   a) From the EPM main menu, select **Real-Time Monitoring** > **Port Distribution**.
   b) Verify that there are ports allocated to the MPP.

Related topics:

Checking the status of port connections on page 11
Checking the basic status of an MPP on page 48
Checking the operational state of an MPP on page 48
Checking the states of the critical MPP processes on page 53
Administrative scripts available on the MPP on page 55
System does not answer or produces only busy signals on page 66

Checking the states of the critical MPP processes

When you troubleshoot MPP issues, if the operational state of the MPP is **Running**, check the states of the critical MPP processes.

Related topics:

Check the configuration state of the MPP on page 51
Checking the state of an MPP process on page 54

Proposed Solution

Procedure

1. Log into Linux on the MPP server as any user.
2. Enter the `ps -e | grep` *`process_name`* command, where *`process_name`* is the name of the process whose state you want to check.

   The critical processes are:

   - `ccxml`
   - `EventMgr`
   - `vxmlmgr`
3. If a state of any process is other than **Running**, check the `$AVAYA_MPP_HOME/logs/core` directory for any files related to the problem.

   If you find any related files, contact your Avaya technical support representative for assistance.
4. If all three processes indicate that they are running, check the configuration state of the MPP.

Checking the state of an MPP process

Procedure

1. Log into Linux on the MPP server as any user.
2. Enter the `ps -e | grep` *`process_name`* command, where *`process_name`* is the name of the process whose state you want to check.

   The MPP processes are:

Process Name	Descriptive Name	Notes
`ccxml`	CCXML Interpreter	This process controls all call handling behavior for each VoiceXML application that runs on the MPP. It also controls each request to obtain or release a telephony resource for a given VoiceXML application. **Note:** Experience Portal uses the Oktopous™ ccXML Interpreter. The **CCXML URL** field is not applicable for AMS.
`CdhService`	Call Data Handler (CDH)	This process is a web service that runs when the EPM is downloading Call Detail Records (CDRs) and Session Detail Records (SDRs).
`EventMgr`	Event Manager	This process collects events from other MPP processes and sends them to the network log web service on the EPM.
`httpd`	Apache Web Server	This process enables the other web services running on the MPP. The first Apache Web Server process started by the daemon runs as root. The root process starts the processes that run as the `avayavp` user in the avayavpgroup group.
`MmsServer`	MPP Management Service (MMS)	This process is a web service interface that allows the EPM server to send commands to the MPP server. It runs only when the EPM is polling or sending commands to the MPP.
`mppmaint`	MPP Maintenance Utility	This is a `cron` process runs the MPP Maintenance Utility daily at 04:00 a.m. to purge CDRs, SDRs, and transcriptions data based on the retention period specified in the EPM.

Process Name	Descriptive Name	Notes
mppmon	MPP Monitor	This process runs as root and monitors the httpd service and restarts them.
mppsysmgr	System Manager	This process handles the majority the tasks required to manage the MPP. For example, this process monitors system resources such as CPU usage, memory usage, and disk usage. If any of these values exceed the baseline set in the EPM, the System Manager issues an alarm message. When instructed by the EPM, the System Manager starts or stops all MPP processes and distributes EPM configuration updates to all MPP processes as they occur.
Session Manager	Session Manager	This process runs as root and integrates and controls the interaction between the MPP and media resources, as well as between the speech application and the ASR, TTS, and telephony components.
TransService		This process uploads any transcription data to the Avaya Aura® Experience Portal database.
vxmlmgr	VoiceXML Manager	This process works with the Session Manager to run multiple VoiceXML dialog sessions. It also interfaces with the CCXML, telephony, ASR, and TTS subsystems. The VoiceXML Manager and the Session Manager communicate by sending messages. The Session Manager is responsible for interpreting these messages and routing the calls to the appropriate platform subsystems on behalf of the VoiceXML Manager.

For an active process, the system returns the process id and CPU time.

Related topics:

Checking the states of the critical MPP processes on page 53

Administrative scripts available on the MPP

The following administrative scripts are available on the MPP. You can run any of these scripts from a command line on the MPP machine:

Script/Executable	Type	Description
`app.php`	php	Summary of the application information downloaded from the EPM.
`appstat.php`	php	The statistics of all applications running on the MPP since the MPP was last started or the application changed. **Note:** This information also appears on the Application Statistics page in the MPP Service Menu.
`asr.php`	php	Summary of the ASR server information downloaded from the EPM. **Note:** This script provides a summary, not a complete list of all properties for the ASR servers.
`authorize_epm.php` *`epm_host_address`*	php	Downloads the EPM certificate that is used for the mutual authentication with the Web Service and the EPM. **Note:** This script has been replaced by `$AVAYA_HOME/Support/VP-Tools/setup_vpms.php` script.
`dirclean.sh`	bash	Removes all application error handlers that were downloaded from the EPM. **Note:** This script is automatically called when the MPP service is stopped. When the MPP service is restarted, the event handlers are downloaded again to ensure that the latest copy is always available on the MPP.
`dropcall.php` *`station_id,switch name`*	php	Causes a specific station to drop its current call. Specify: • *station_id*: the station number • *switch name*: the name of the H.323 Connection under which the station is defined. **Tip:** You can generate a list of stations with the `listst.php` script.
`dropsession.php` *`session_id`*	php	Causes the MPP to drop the session whose Session ID is specified in *session_id*.

Script/Executable	Type	Description
`dumpRecords`	exe	Dumps the contents of an MPP's Call Detail Record (CDR) or Session Detail Record (SDR) bin file.
`getmpplogs.sh`	bash	Automatically combines the MPP logs in a TAR.GZ file so that you can archive them or send them to your Avaya support representative. For details about using this script, see Packing MPP logs and transcriptions using getmpplogs.sh on page 160. **Tip:** You can restore these logs with the `restorempplogs.sh` script.
`installstatus.php [--history]`	php	Lists the MPP version and release number. If you use the optional `--history` parameter, it lists the installation history starting with Avaya Aura® Experience Portal release 4.0.
`listcalls.php`	php	Lists the active calls on the MPP.
`listsessions.php`	php	Lists all sessions on the MPP.
`listss.php`	php	Summarizes the speech server resources currently available to the MPP, including the number of resources that the MPP server can use without shorting other MPP servers in the system (known as the H value) and the total number of ports that the MPP needs if the system is operating under a full call load (the M value). **Note:** This information also appears on the Speech Servers page in the MPP Service Menu.
`listst.php`	php	Lists the configured stations and their statuses.
`mppMoveLogs.sh`	bash	Moves the current MPP logs directory to a different drive or partition and creates a symbolic link so that all future MPP logs will be written to the new location. For more information, see Moving the MPP logs to a different location on page 157.
`mpprollback.sh`	bash	Rolls the MPP installation back to the previously installed version. **Tip:** The Version page in the MPP Service Menu displays the current installed release and the available rollback version.

Script/Executable	Type	Description
`restorempplogs.sh`	bash	Restores the MPP logs archived by the `getmpplogs.sh` script. For details, see Restoring packed MPP log files on page 162.
`SMDump`	exe	Dumps Telephony, ASR, and TTS status detail. **Note:** The `SessionManager` process must be running and you must be logged in as `root` or `sroot` to run this executable.
`stat.php`	php	Lists the MPP state and the running state of its monitored processes.
`tts.php`	php	Summary of the TTS server information downloaded from the EPM. **Note:** This script provides a summary, not a complete list of all properties for the TTS servers.
`usr.php`	php	Displays a list of the users downloaded from the EPM. **Note:** User roles and passwords are encrypted in this list.
`xml.php`	php	Dumps out two XML configurations: • Configuration loaded from the `$AVAYA_MPP_HOME/config/mppconfig.xml` • Configuration downloaded from the EPM

Related topics:

Check the configuration state of the MPP on page 51

Advanced troubleshooting scripts available on the MPP

Caution:

Only run these scripts under explicit instructions from your Avaya technical support representative. Under other circumstances, use the EPM to start, stop, or configure any MPP in the Avaya Aura® Experience Portal system to ensure that the EPM and the MPP stay synchronized.

The available advanced troubleshooting scripts are:

Script	Type	Description
`config.php <file.xml>`	php	Overrides the current configuration with the configuration specified in `file.xml`.
`installstatus.pl`	perl	This script has been replaced by `installstatus.php [--history]` and is installed for backwards compatibility only.
`launchccxml.php`	php	Launches an outbound call for a CCXML application. **Important:** You can use the Application Interface web service to launch such calls. For details, see *The Application Interface web service* topic in the *Administering Avaya Aura® Experience Portal* guide.
`launchvxml.php`	php	Launches an outbound call for a VoiceXML application. **Important:** You should use the Application Interface web service to launch such calls.
`msgs.php`	php	Lists statistics about the data sent between MPP processes. **Note:** This information also appears on the Process Messages page in the MPP Service Menu.
`mppuninstall.sh`	bash	Uninstalls the MPP.
`param.php` *`parameter_name`*	php	Downloads the value of the specified MPP configuration parameter and displays it. The parameter must be a simple name/value parameter and not a parameter table.
`procstop.php` *`processname`*	php	Instructs the MPP System Manager to stop the process named in *processname*. *processname* can be: • `ccxml` • `vxmlmgr`
`start.php`	php	Instructs the MPP System Manager to start all MPP processes, such as `ccxml`, `vxmlmgr`.

Script	Type	Description
`stationin.php` *`station_id,switch name`*	php	Instructs the MPP System Manager to bring a station into service. Specify: • *station_id*: the station number • *switch name*: the name of the H.323 Connection under which the station is defined. **Tip:** You can generate a list of stations with the `listst.php` script.
`stationout.php` *`station_id,switch name`*	php	Instructs the MPP System Manager to bring a station out of service. Specify: • *station_id*: the station number • *switch name*: the name of the H.323 Connection under which the station is defined. **Tip:** You can generate a list of stations with the `listst.php` script.
`stop.php`	php	Instructs the MPP System Manager to stop all MPP processes, such as `ccxml`, `vxmlmgr`.

Symptoms of common MPP problems

The key to diagnosing and resolving MPP problems is to quickly identify the component causing the problem. The following table provides examples of the most common system response errors. Use these examples as a starting point to identify and isolate the problem component in cases where the problem component is not obvious.

Symptoms	Possible causes	Where to go for more help
The system does not respond as expected.	Hyperthreading may not be enabled on the Avaya Aura® Experience Portal servers.	If hyper threading is not enabled, see Verifying if hyperthreading is enabled on the HP ProLiant DL360 G7 on page 65.
The system is not taking calls. All MPPs are unresponsive.	The WebLM license has expired, or the system is not able to contact the license server.	Verify that your license is valid and that the EPM can contact the Avaya license server. For more information, see the *Avaya Aura® Experience Portal licenses* topic in the

Symptoms	Possible causes	Where to go for more help
		Administering Avaya Aura® Experience Portal guide.
	One or more system resources, such as the CPU usage, disk space, or available memory, might be overtaxed.	On the EPM, check the status of the system resources for the MPP. For more information, see the **Resource Status** group on the <MPP name> Details page.
	Network or PBX problems might be causing the ports to go to the Out-of-Service state.	On the EPM, check the status of the telephony ports. For more information, see the Port Distribution page.
	Network problems might be preventing MPPs from running the speech applications.	On the EPM, verify that you can reach the root document of the speech application. For more information, see the Change Application page.
The system either does not answer or produces only busy signals.	One or more MPPs might be out-of-service or experiencing other problems.	Troubleshoot the MPP as described in System does not answer or produces only busy signals on page 66.
The system answers, but then immediately hangs up on the caller.	The number the caller dialed (DNIS) might not have a valid URI for a speech application assigned.	Verify the DNIS and URI settings for the application. For more information, see System answers and then hangs up on page 69.
	The MPP might be having trouble routing the caller to the proper application, fetching pages or resources, or interpreting the application pages.	Troubleshoot the MPP according to the guidelines provided in System answers and then hangs up on page 69.
The system answers the call, but does not recognize or respond to caller inputs.	The MPP receiving the call might be experiencing difficulties.	Troubleshoot the MPP according to the guidelines provided in the *Viewing Avaya Aura® Experience Portal system status* topic in the *Administering Avaya Aura® Experience Portal* guide.
	System encryption settings might be out of sync.	Troubleshoot the EPM according to the guidelines provided in Encryption settings are not synchronized on page 69.
	The ASR might be malfunctioning.	Use the EPM Alarm Monitor page to determine whether any ASR resources are having difficulty. For more information, see the *Viewing Avaya Aura® Experience Portal*

Symptoms	Possible causes	Where to go for more help
		system status topic in the *Administering Avaya Aura® Experience Portal* guide.
The system answers, but either becomes silent or responds with gibberish or other unusable output.	The MPP receiving the call might be experiencing difficulties.	Check the MPP basic status, as described in Checking the basic status of an MPP on page 48. If the state is not **Running**, see MPP is in an unexpected operational state on page 63.
	The network traffic might be too heavy for the bandwidth allowed. This can cause audio "stuttering."	Use one or more network traffic monitoring tools to assess the amount of bandwidth being consumed at the time that problems are experienced. Take steps to increase network bandwidth.
	System encryption settings might be out of sync.	Troubleshoot the EPM according to the guidelines provided in Encryption settings are not synchronized on page 69.
	The speech application might not be functioning as designed.	Debug the speech application. For more information, see the documentation for your application development tool. You can also check for system resource availability, such as CPU usage, disk space, and memory usage, on the application server. If the application was created with Avaya Aura ®Orchestration Designer, you can run an Application report in the EPM. For more information, see the *Application activity reports* topic in the *Administering Avaya Aura® Experience Portal* guide.
	One or more system resources might be unavailable or not functioning properly.	Use the EPM <System name> Details tab on the System Monitor page to identify and isolate the system resource that is causing the problem. For more information, see the *Viewing Avaya Aura® Experience Portal system status* topic in the *Administering Avaya Aura® Experience Portal* guide.
	The audio codec on the switch may not match the	Use the EPM VoIP Settings page to check the MPP Native Format drop-down setting. If it is set to audio/basic,

Symptoms	Possible causes	Where to go for more help
	Voice over IP (VoIP) audio settings.	then the codec set on the switch must include G711MU. If it is set to audio/x-alaw-basic, then the codec set on the switch must include G711A.
Converse-on data is not being received at the beginning of a call where it is expected.	The application might not be configured for Converse-on data.	• Verify that the application itself is designed to handle Converse-on data. • Verify that the application is configured on the Avaya Aura® Experience Portal system to handle Converse-on data. For more information, see the *Changing speech application settings through Avaya Aura® Experience Portal* topic in the *Administering Avaya Aura® Experience Portal* guide.
	The Converse-on data might not be making it to the application.	Troubleshoot the Converse-on data processing according to the guidelines provided in Converse-on data is not received on an H.323 connection on page 70.

MPP is in an unexpected operational state

The <System name> Details tab on the System Monitor page in the EPM shows the MPP operational state as Not Responding, Degraded, or Error.

Related topics:

SSL certificate requirements on page 78

Proposed Solution 1

About this task

Use this solution if the httpd daemon is not running or is experiencing problems.

Procedure

1. At the Linux command line prompt, check the status of the `httpd daemon` process by entering the `/sbin/service httpd status` command.
2. If the `httpd daemon` process is not running, start it by entering the `/sbin/service httpd start` command.

3. If the `httpd daemon` process is running, stop it and then restart it:
   a) Stop the `httpd daemon` process by entering the `/sbin/service httpd stop` command.

      The system should respond with a message that ends with `[OK]` to indicate that the service has stopped.
   b) Restart the `httpd daemon` process by entering the `/sbin/service httpd start` command.

      The system should respond with a message that ends with `[OK]` to indicate that the service has started.
4. If these steps do not resolve the issues with the httpd daemon, continue with the solutions in Troubleshooting the httpd daemon process on page 73.

Proposed Solution 2

About this task

Use this solution if the mpp daemon is not running or is experiencing problems

Procedure

1. At the Linux command line prompt, check the status of the `mpp daemon` process by entering the `/sbin/service mpp status` command.
2. If the systems responds with a message that the service is not running, start it by entering the `/sbin/service mpp start` command.
3. If the service is running, stop and then restart it:
   a) Stop the `mpp daemon` process by entering the `/sbin/service mpp stop` command.

      The system should respond with a message that ends with `[OK]` to indicate that the service has stopped.
   b) Restart the `mpp daemon` process by entering the `/sbin/service mpp start` command.

      The system should respond with a message that ends with `[OK]` to indicate that the mppsysmgr daemon has started.
4. If these steps do not resolve the issues with the mpp daemon, continue with the solutions in Troubleshooting the mpp daemon process on page 76.

Proposed Solution 3

About this task

Use this solution if one or more system resources is overtaxed, such as the CPU usage, disk space, or available memory.

Procedure

1. Log in to the EPM Web interface using an account with the Administration user role.
2. From the EPM main menu, select **Real-Time Monitoring** > **System Monitor**.
3. Go to the <System name> Details tab on the System Monitor page, where <System Name> matches the name of the Avaya Aura® Experience Portal system that contains the MPP whose MPP Service Menu you want to access.
4. From the MPP Service Menu, select **Resources**.
5. Check the status of the system resources for the MPP.

Proposed Solution 4

About this task

Use this solution for problems with the SSL certificate.

Procedure

1. Check to see if an SSL certificate has been installed on the MPP.
2. If the installed SSL certificate has problems, download a new copy of the SSL certificate from the EPM.
3. Verify that the SSL certificate has been accepted on the EPM.

Verifying if hyperthreading is enabled on the HP ProLiant DL360 G7

If the Avaya Aura® Experience Portal system does not respond as expected, hyperthreading may not be enabled on the Avaya Aura® Experience Portal servers.

Whether your system is equipped with a single processor or multiple processors, you must enable hyperthreading on the HP ProLiant DL360 G7. Hyperthreading makes each processor operate like two separate devices and increases system performance without having to add an additional processor to the system.

In the Avaya-provided or bundled server offer, hyperthreading is enabled by default. If you have opted for the Customer-provided server offer, verify if hyperthreading is enabled on the server. To enable hyperthreading, refer to the specific server documentation.

Proposed Solution

About this task

To verify if hyperthreading is enabled on the HP ProLiant DL360 G7:

Procedure

1. Ensure that the server has an attached monitor and keyboard as this procedure cannot be preformed remotely.
2. Reboot the **HP ProLiant DL360 G7** server.
3. During the bootup, press **F9** to access **Configuration/Setup Utility**.
4. Using the **Down Arrow** key, highlight **System Options** and press the **Enter** key.
5. From the **System Options** menu, use the **Down Arrow** key to highlight **Processor Options** and press the **Enter** key.
6. Verify if **Intel® Hyperthreading® Options** is selected.

   Note:
   If the **Intel® Hyperthreading® Options** is disabled, contact the system administrator to enable it.
7. Press the **Esc** key to exit the **Processor Options** menu.
8. Press the **Esc** key to exit the **System Options** menu.
9. On the **Configuration/Setup Utility** menu, use the **Down Arrow** key to highlight **Exit Setup** and press the **Enter** key.

System does not answer or produces only busy signals

A variety of system problems can cause the MPP to not answer a call or respond with a busy signal. For example, one or more MPPs might be out-of-service or experiencing other problems.

The following solutions can help you to resolve the majority of these cases. If none of these solutions help to identify and resolve the problem, contact your Avaya technical support representative for assistance.

Related topics:

Synchronizing the EPM and an MPP on page 19

Check the configuration state of the MPP on page 51

Proposed Solution 1

Procedure

1. Log into the EPM using any valid EPM user account.
2. Verify that the operational state of the MPP is **Running**.
3. Verify that ports are being assigned to the MPP.
4. Create an alarm report for that MPP and resolve any issues noted in the alarms.

   For more information, see as described in the *Creating an alarm report* topic in the *Administering Avaya Aura® Experience Portal* guide.
5. On the Applications pages, check the **Launch** column to make sure that there is an application with the DNIS (the number that the caller dialed) assigned.

   If no application has the DNIS assigned, assign the number to an application as described in the *Creating an alarm report* topic in the *Administering Avaya Aura® Experience Portal* guide.

Proposed Solution 2

Procedure

1. Log in to the MPP Service Menu, as described in the *Logging in to the MPP Service Menu* topic in the *Administering Avaya Aura® Experience Portal* guide.

   Note:

   If you cannot log in to the MPP Service Menu, check the status of the httpd daemon process.
2. On the MPP Service Menu home page, verify that the value of the **Run state** field in the **MPP Status** table is **Running**.
   - If the operational state displayed in this field differs from the operational state displayed on the <System name> Details tab on the System Monitor page, synchronize the EPM and the MPP to resolve connection problems.
   - If the **Run state** field does *not* say **Running**, start the MPP or troubleshoot the problem that is keeping the MPP from starting.
3. On the MPP Service Menu home page, verify that the value of the **Configuration state** field in the **MPP Status** table is **Configuration OK**.

   If the **Configuration state** field does *not* say **Configuration OK**, check the configuration state of the MPP.

4. Check the state of all critical processes.

Proposed Solution 3

Procedure

1. On the MPP Service Menu, click **Resources**.
2. On the Resources page, click **Telephony**.

   Tip:

   You can also use the `listst.php` administrative script to obtain this information about the MPP.
3. On the Telephony Resources page, verify that all channels display a state of **In-Service** in the **Channel State** column.
4. If a channel does *not* display **In-Service**, troubleshoot the problem between the Communication Manager and the MPP:
   - On the EPM, check the H.323 connection settings, especially the password as described in the *H.323 connections in Avaya Aura® Experience Portal* topic in the *Administering Avaya Aura® Experience Portal* guide.
   - On the EPM, check the information for the channel (port) or channels that seem to be experiencing problems as described in the *Viewing telephony port distribution* topic in the *Administering Avaya Aura® Experience Portal* guide.
   - Check theCommunication Manager to see if it displays the same status for the affected channels (ports) as the MPP does, as described in your Communication Manager documentation.
   - If you cannot resolve the problem using any of these strategies, contact your Avaya technical support representative for assistance.
5. Check the `SessionManager` logs for errors that indicate the system has had problems gaining access to Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) resources:
   a) On the MPP Service Menu, click **Logs**.
   b) On the Log Directories page, click **SessMgr**.
   c) Click on the log you want to view.

      The available log types are:
      - `SessionManager.log`: Contains data related to events that are not specifically associated with a single session.
      - `SessionSlot-###.log`: Contains data related to Session Manager operations for individual sessions. The ### represents the unique cookie,

or identifier, that you can use to find related Session Manager, CCXML interpreter, and Avaya Voice Browser logs.

System answers and then hangs up

Related topics:

Avaya Aura Experience Portal system status on page 9

Proposed Solution

Procedure

1. Verify that the URI for each application that is assigned the DNIS (the number that the caller dialed) is valid, as described in the *Changing speech application settings through Avaya Aura® Experience Portal* topic in the *Administering Avaya Aura® Experience Portal* guide.
   If you cannot verify any URI settings, troubleshoot the problem with the URI settings.
2. If you created your applications in Orchestration Designer, use the EPM to create an Application report containing the application messages, as described in the *Application activity reports* topic in the *Administering Avaya Aura® Experience Portal* guide.
3. Use the Session Detail report to examine session details for the affected calls, as described in the *Creating a Session Detail report* topic in the *Administering Avaya Aura® Experience Portal* guide.

Encryption settings are not synchronized

If the encryption settings on the Avaya Aura® Experience Portal system and on the Communication Manager do not agree, the system can fail to either prompt callers or recognize responses, even though the MPPs seem otherwise to be healthy. This condition is evident when the system answers calls but then fails to respond further.

For more information about the encryption settings on:

- Avaya Aura® Experience Portal, see the *H.323 connections in Avaya Aura® Experience Portal* topic in the *Administering Avaya Aura® Experience Portal* guide.
- Communication Manager, see your Communication Manager documentation set.

Proposed Solution

About this task

Both Avaya Aura® Experience Portal and Communication Manager must have encryption enabled or both must have encryption disabled.

Procedure

1. Ensure that the encryption settings on the Avaya Aura® Experience Portal system and on the Communication Manager match.
2. If you are using:
   - H.323 connections, make sure that you have configured Communication Manager as described in *Avaya Configuration Note 3910*.
   - SIP connections, make sure that you have configured Communication Manager as described in *Avaya Configuration Note 3911*.

Converse-on data is not received on an H.323 connection

If converse-on data is not received at the beginning of a call using an H.323 connection, the system may have encountered the following problems:

- The application is not configured for Converse-on data.
- The Converse-on data was not sent to the application.

If both the application and the EPM are configured correctly for Converse-on, but at run-time, the Converse-on data is not processed, you must troubleshoot to find out where the data is getting lost.

Related topics:

Avaya Aura Experience Portal system status on page 9

Proposed Solution

Procedure

1. On the MPP, navigate to the `$AVAYA_MPP_HOME/logs/process/SessMgr` directory and open the `SessionSlot###.log` files.

   Where ### is a three-digit ID number.

2. To see if Converse-on data is received by the MPP, check the Session Manager logs for entries that contain the following text:

   ```
   waiting for ConverseOnData
   received converse on digits
   ```

3. If the Session Manager logs indicate that Converse-on data is:
   - Not received, go to Step 4.
   - Received, go to Step 5.
4. Verify with the Communication Manager programmer or administrator that the vector is properly configured and is sending the expected data.
5. Navigate to the `$AVAYA_MPP_HOME/logs/process/VB` directory and open the `SessionSlot###.log` files.

   Where *###* is a three-digit ID number.
6. To verify that the Converse-on data is added to the query string that is sent to the application, search the VB logs for the term "converse":

   In these logs, the Converse-on digits collected by the Session Manager should be part of a query string sent to the application server as:

   ```
   &session vpconverseondata=###...
   ```

   Where *###...* is the sequence of digits sent.
7. On the application server, verify that the Converse-on data is being received.

   Contact your application developer if you need assistance.

PHP script fails to run with Aborted error message

When a PHP script fails to run and the system generates an error message that says `Aborted (core dumped)`, there are several possible causes. For example, the user may not be logged into Linux with the proper permissions.

Proposed Solution

Procedure

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

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

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

2. Verify that the user is a member of avayavpgroup by entering the `cat /etc/group | grep avayavpgroup` command.
   The system displays the list of users that are members of avayavpgroup.
3. If the user does not appear in the list of group members, add the user to the avayavpgroup by entering the `gpasswd -a` *`username`* `avayavpgroup` command, where *`username`* is the user ID you want to add to the group.
4. Verify that the following files and their parent directories have the group set to avayavpgroup and read-write permissions set:
   - `$AVAYA_MPP_HOME/tmp/mgtlib.php.out`
   - `$AVAYA_MPP_HOME/logs/process/SysMgr/logfile.log`
5. If one or both the files or directories do not have the correct group or permissions, set them to read-write for the avayavpgroup.
6. If these actions do not resolve the problem, contact your Avaya technical support representative for assistance.

Monitoring call progress in real time

If your Avaya Aura® Experience Portal system encounters problems during the progress of a call, you can set up your system to monitor call progress in real time.

Related topics:

Isolating an MPP for troubleshooting on page 47

MPP server logs on page 154

Proposed Solution

Procedure

1. If your system uses H.323 connections, you must configure the MPP server you want to monitor to use the Test operational mode so that you are certain your test calls will go to the correct MPP.
2. Verify that you have the trace logging for the MPP enabled and set to the appropriate levels.
   a) Log in to the EPM Web interface using an account with the Administration user role.
   b) From the EPM main menu, select **System Configuration** > **MPP Server**.

c) On the MPP Servers page, click the name of the MPP you want to monitor in the **Name** column.
d) On the Change MPP Server page, go to the **Categories and Trace Levels** section and set the appropriate options.
e) When you are finished, click **Save**.

3. If you want to clear all log files so that you can easily see what data is being added:
   a) Log in to the MPP Service Menu as described in the *Logging in to the MPP Service Menu* topic in the *Administering Avaya Aura® Experience Portal* guide.
   b) From the MPP Service Menu, select **Logs**.
   c) Click **Clear log files in all the directories**.
4. Log in to Linux on the MPP server that you want to monitor using an account that is a member of the avayagroup.
5. If you want to monitor:
   - Live output to the Session Manager log file, enter the commands `cd $AVAYA_MPP_HOME/logs/process/SessMgr` and `tail –f SessionManager.log`
   - Live output to the session slot log file, enter the commands `cd $AVAYA_MPP_HOME/logs/process/SessMgr` and `tail –f SessionSlot-####.log`
6. Make a test call and observe the data output.

   Tip:
   Depending on the trace logging level you have selected for the MPP, the information might scroll by faster than you can read it. If that happens, use the **`vi`** command.
7. If the `SessionManager.log` file does not contain the information you need to solve your problem, review the other MPP server log files.

Troubleshooting the httpd daemon process

The MPP uses the Apache Web server for performing operations. The Apache Web server is identified on the system and controlled by the `httpd daemon` process process. Therefore, if you suspect problems with the Apache Web server, check the status of the `httpd daemon` process.

Note:

These strategies assume that you have checked the Avaya Aura® Experience Portal system status on the <System name> Details tab of the System Monitor page.

Problems with the `httpd daemon` process can manifest in the following ways:

- The EPM indicates that the operational state of the MPP is **Not Responding** or **Unknown**.
- When you log in to the MPP Service Menu, the browser window displays an error message that the page cannot be displayed, the server cannot be found, or there is a DNS error.
- An improper system shutdown left a locked process file.
- The MPP key and/or certificate is corrupted.

If none of these solutions help to identify and resolve the problem, contact your Avaya technical support representative for assistance.

Proposed Solution 1: Restarting the httpd daemon process

Procedure

1. At the Linux command line prompt, check the status of the `httpd daemon` process by entering the `/sbin/service httpd status` command.
2. If the `httpd daemon` process is not running, start it by entering the `/sbin/service httpd start` command.
3. If the `httpd daemon` process is running, stop it and then restart it:
   a) Stop the `httpd daemon` process by entering the `/sbin/service httpd stop` command.

      The system should respond with a message that ends with `[OK]` to indicate that the service has stopped.
   b) Restart the `httpd daemon` process by entering the `/sbin/service httpd start` command.

      The system should respond with a message that ends with `[OK]` to indicate that the service has started.
4. If the system responds with a message stating that the service cannot be started because there are locked files:
   a) Delete the lock file by entering the `rm /var/lock/subsys/httpd` command.
   b) Start the service again by entering the `/sbin/service httpd start` command.

   If the service still does not start, see Proposed Solution 2: Examining the httpd daemon process MPP log files on page 75.

5. Let the service run for several minutes, and then check the status by entering the `/sbin/service httpd status` command.

   If the service is:

   - Running, wait and see if the problems reoccur. If they do, see Proposed Solution 2: Examining the httpd daemon process MPP log files on page 75.
   - Stopped , see Proposed Solution 2: Examining the httpd daemon process MPP log files on page 75.

Proposed Solution 2: Examining the httpd daemon process MPP log files

Procedure

1. In an ASCII editor, open the following log files:
   - `/var/log/error_log`
   - `/var/log/httpd/ws_error_log`
2. Search both log files for the following error messages:
   - `>Unable to configure RSA server private key`
   - `>SSL Library Error: 185073780 error:0B080074:x509`
   - `certificate routines:X509_check_private_key:key values`
   - `mismatch`
3. If you find these errors in either log file, reinstall the MPP software to create a new certificate on the MPP.

   When you reconnect the MPP and the EPM, these errors should be resolved. For details, see Reinstalling the MPP software on page 127.
4. If you do not find these errors in either log file, see Proposed Solution 3: Examining the httpd daemon process log files on page 75.

Proposed Solution 3: Examining the httpd daemon process log files

Procedure

1. Log into Linux on the EPM server.

2. In an ASCII editor, open the EPM log file `/opt/Avaya/ExperiencePortal/vpms/logs/avaya.vpms.log`.
3. Search for error messages relating to the `httpd daemon` process.
4. If you do not find any messages relating to the problem, In an ASCII edit, open the log file `$CATALINA_HOME/logs/catalina.out`.
5. Search for error messages relating to the `httpd daemon` process.
6. If you do not find any messages relating to the problem, contact Avaya technical support.

Troubleshooting the mpp daemon process

The MPP uses the `mpp daemon` process to start and control the various processes that enable the MPP to function as it should. If this process does not start, stops working, or experiences other problems, the MPP does not respond as it should. Therefore, if you are having problems with the MPP and you have confirmed that the `httpd daemon` process is running correctly as described in Troubleshooting the httpd daemon process on page 73, the next step is to check the status of the `mpp daemon` process.

Problems with the `mpp daemon` process can manifest in the following ways:

- An improper system shutdown left a locked process file.
- A conflict exists with permissions for the `mppsysmgr` directory or log file.

Proposed Solution 1: Restarting the mpp daemon process

Procedure

1. At the Linux command line prompt, check the status of the `mpp daemon` process by entering the `/sbin/service mpp status` command.
2. If the systems responds with a message that the service is not running, start it by entering the `/sbin/service mpp start` command.
3. If the service is running, stop and then restart it:
   a) Stop the `mpp daemon` process by entering the `/sbin/service mpp stop` command.

      The system should respond with a message that ends with `[OK]` to indicate that the service has stopped.
   b) Restart the `mpp daemon` process by entering the `/sbin/service mpp start` command.

The system should respond with a message that ends with `[OK]` to indicate that the mppsysmgr daemon has started.

4. If the system responds with a message stating that the service cannot be started because there are locked files:
   a) Delete the lock file by entering the `rm /var/lock/subsys/mppsysmgr` command.
   b) Try to start the service again by entering the `/sbin/service mpp start` command.

   If the service still does not start, see Proposed Solution 2: Examining the mpp daemon process log files on page 77.
5. Let the service run for several minutes, and then check the status again by entering the `/sbin/service mpp status` command.

   If the service status is not running, or if the problems reoccur, see Proposed Solution 2: Examining the mpp daemon process log files on page 77.

Proposed Solution 2: Examining the mpp daemon process log files

Procedure

1. In an ASCII editor, examine the `$AVAYA_MPP_HOME/logs/process/SysMgr/logfile.log` log file.
2. If you find relevant error messages in the file, perform the troubleshooting procedures described for that error message.
3. If you cannot find any relevant error messages or if the troubleshooting procedures do not resolve the problems, see Proposed Solution 3: Checking for core files on page 77.

Proposed Solution 3: Checking for core files

Procedure

1. Log into Linux on the MPP server.
2. Navigate to the `$AVAYA_MPP_HOME/logs/core` directory and check to see if there are any `mppsysmgr*` core files in that directory.
3. If the directory contains core files, delete the `$AVAYA_MPP_HOME/logs/process/SysMgr/` directory.

This solution resolves problems with permissions on the log file or directory.

4. Reboot the MPP server.
5. If you do not find any core files, or if deleting the files does not solve the problem, contact Avaya technical support.

Troubleshooting SSL Issues

SSL certificate requirements

The MPP and EPM use SSL mutual authentication to protect the data exchanged between the Web Services on both servers. Mutual authentication requires that certificates be exchanged between the servers. If the certificates do not exist or are corrupted, the EPM is not able to establish contact with the MPP.

MPP configuration for mutual authentication requires that:

- The MPP has its own key and certificate. This certificate is used when the MPP Web services or the MPP Service Menu is accessed. During the installation of MPP software, you are prompted to either provide the certificate or have the installation create one for you.
- The MPP has a valid copy of the EPM SSL certificate downloaded to register the EPM as a recognized certificate authority. The EPM SSL certificate is downloaded during MPP software installation. However, if the MPP SSL certificate and key appear valid and you are still having trouble with exchange of data between the MPP and the EPM, you can validate, and redownload the EPM SSL certificate.
- The MPP configuration file,`mpp.conf`, must have the correct paths to the SSL certificate and key files. The httpd daemon uses this file at startup to establish communications between the MPP and the EPM. If the paths in this file are not valid, the two servers cannot establish secure communications.

For more information about Apache and SSL, see SSL/TLS Strong Encryption.

Related topics:

Validating the EPM SSL certificate copy on the MPP on page 79

MPP SSL certificate and key location

The MPP key and certificate files are located at:

- `/etc/httpd/conf/ssl.key/server.key`
- `/var/www/html/cert.pem`

Sample MPP SSL certificate

```
-----BEGIN CERTIFICATE-----
MIICfDCCAeWgAwIBAgIBADANBgkqhkiG9w0BAQQFADA5MQwwCgYDVQQLEwNNUFAx
DjAMBgNVBAoTBUF2YXlhMRkwFwYDVQQDExBtbHZvaWNlcG9ydGFsLWE5MB4XDTA1
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQCU36+QLX56yDK0l4wkb8Ai
VQQKEwVBdmF5YTEZMBcGA1UEAxMQbWx2b2ljZXBvcnRhbC1hOTCBnzANBgkqhkiG
zPEZEzz12iYGBB7EzvN8WsbUVU+7hN1ojNsidt25gTu8ol2Pnz4pnonGAc3xowAo
9w0BAQEFAAOBjQAwgYkCgYEAt9166cK3sMldlsq83aFwwykCeItEA/XDZbyYewKP
z2T6RDS2TD+EwDKQjuxo8h1upDVFgherJdK4Ks+PvbnN6yIxW39wOU8Gl3JbWJgR
1WrRVjelUg5hpVcHxkdkRynkmM8bJBvaohqS5NMiygBfUXaz+Qx7wWVevkM7qdeM
MDkyOTE2MTExM1oXDTE1MDkyNzE2MTExM1owOTEMMAoGA1UECxMDTVBQMQ4wDAYD
GMMCAwEAAaOBkzCBkDAdBgNVHQ4EFgQUUH67bdY3lHOTZVx6u34wj1roPvwwYQYD
WSz+QXogX265wzyYXZDQuGZ9hRm0nhQjXv20C6EfNK8T+g03/NfqqxqjJdKrelya
VR0jBFowWIAUUH67bdY3lHOTZVx6u34wj1roPvyhPaQ7MDkxDDAKBgNVBAsTA01Q
UDEOMAwGA1UEChMFQXZheWExGTAXBgNVBAMTEG1sdm9pY2Vwb3J0YWwtYTmCAQAw
WZg0Cm00qzzk9qWf9SKpbg==
-----END CERTIFICATE-----
```

Sample MPP SSL key

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC33XrpwrewyV2WyrzdoXDDKQJ4i0QD9cNlvJh7Ao/PZPpENLZM
P4TAMpCO7GjyHW6kNUWCF6sl0rgqz4+9uc3rIjFbf3A5TwaXcltYmBHVatFWN6VS
hrG6+y5IISWLlioeMNFnBKxTwQIzNaInXwJBALGUL7Q8EVzODlaojEZclo6WZycT
AoGAcad/tgX+RFKE/pQ94QZNTOYJt/fmSEhfy4CkBM3VlY7GwOiQk1tkNOZMw3xR
dvBIl0qyt7LnwY6a9yOsp8u2BAl1YEI/+7FR41pRIGL+d8FtXDlVm7XINpsZjn1f
qO7TPdOoIXA3bkyT5wXgtEb2cb8XbpF2oUaJDOxI1FHCzbkCQQDi963DoOOgYQgc
jVMrzJ7woKuSnX/6qeoKsc5lrYc37fBBV6bjnocp8sV+tBTUJ/RW3aAVS8LyrsRV
xFMgBsCNGbj66iW7utkCQQCNmuapAYmxp4paNW+Y46iGGKy+DhjOSqRF6+msDy4a
w33OtD0dAkEAz2JdKLIbwgL5M1yZNGPUzQ3RaLOXPF68IV68V4rEBjwQrvCon+Jh
DmGlVwfGR2RHKeSYzxskG9qiGpLk0yLKAF9RdrP5DHvBZV6+Qzup14wYwwIDAQAB
a6pnfuJXM7GCD6XG2I+HUOAOjJpZhAQaSaGkkRvV0wZWfHT8IEkp5yjvBFECQHtl
+DDC6iljQ40ASFkYHgN1eWlnk1HkvOTOTht5AnMDQpoVsQCR354aGzxiqaCvioNr
FtSo8Zs9AdWlCiBxKUTAqfxTPlhITlbyzOYVwolag4SR
-----END RSA PRIVATE KEY-----
```

If these files appear valid, check the Apache logs for possible errors. If these files are missing or appear to be corrupted, either reinstall the certificates, or reinstall the MPP software to generate new self-signed certificates. For more information on the Apache logs, see MPP server logs on page 154.

Validating the EPM SSL certificate copy on the MPP

About this task

During MPP installation, the installation script creates a symbolic link to this file, which Apache uses to access the certificate. If that symbolic file does not exist, a connection cannot be

established between the MPP and the EPM. Therefore, you must also verify that the symbolic link exists on the MPP.

Procedure

1. Compare the MPP certificate to the one on the EPM by entering the `curl http://EPM-server/cert.pem` command, where *EPM-server* is the domain name or IP address of the system where the primary EPM software is installed.
2. At the Linux command line prompt, enter the `cat $AVAYA_MPP_HOME/web/ssl.crt/vpms.crt` command.

   The system should respond with a message similar to the following:

   ```
   -----BEGIN CERTIFICATE-----
   MIICfDCCAeWgAwIBAgIBADANBgkqhkiG9w0BAQQFADA5MQwwCgYDVQQLEwNN
   UFAx
   DjAMBgNVBAoTBUF2YXlhMRkwFwYDVQQDExBtbHZvaWNlcG9ydGFsLWE5MB4X
   DTA1
   DAYDVR0TBAUwAwEB/
   zANBgkqhkiG9w0BAQQFAAOBgQCU36+QLX56yDK0l4wkb8Ai
   VQQKEwVBdmF5YTEZMBcGA1UEAxMQbWx2b2ljZXBvcnRhbC1hOTCBnzANBgkq
   hkiG
   zPEZEzz12iYGBB7EzvN8WsbUVU
   +7hN1ojNsidt25gTu8ol2Pnz4pnonGAc3xowAo
   9w0BAQEFAAOBjQAwgYkCgYEAt9166cK3sMldlsq83aFwwykCeItEA/
   XDZbyYewKP
   z2T6RDS2TD+EwDKQjuxo8h1upDVFgherJdK4Ks
   +PvbnN6yIxW39wOU8Gl3JbWJgR
   1WrRVjelUg5hpVcHxkdkRynkmM8bJBvaohqS5NMiygBfUXaz
   +Qx7wWVevkM7qdeM
   MDkyOTE2MTExM1oXDTE1MDkyNzE2MTExM1owOTEMMAoGA1UECxMDTVBQMQ4w
   DAYD
   GMMCAwEAAaOBkzCBkDAdBgNVHQ4EFgQUUH67bdY3lHOTZVx6u34wj1roPvww
   YQYD
   WSz+QXogX265wzyYXZDQuGZ9hRm0nhQjXv20C6EfNK8T+g03/
   Nfqqxqj JdKrelya
   VR0jBFowWIAUUH67bdY3lHOTZVx6u34wj1roPvyhPaQ7MDkxDDAKBgNVBAsT
   A01Q
   UDEOMAwGA1UEChMFQXZheWExGTAXBgNVBAMTEG1sdm9pY2Vwb3J0YWwtYTmC
   AQAw
   WZg0Cm00qzzk9qWf9SKpbg==
   -----END CERTIFICATE-----
   ```
3. Change to the directory in which the SSL certificate from the EPM resides by entering the `cd $AVAYA_MPP_HOME/web/ssl.crt/` command.
4. List all files in this directory by entering the `ls -al` command.

   You should see a symbolic link to the `vpms.crt` file, similar to the following entry:

   ```
   lrwxrwxrwx  1 sroot  root   8 Oct  7 18:21 36c998fa.0 ->
   vpms.crt
   ```

The "l" at the beginning and the"-> vpms.crt" text at the end indicate that the symbolic file has been created. In this example, the file is named36c998fa.0.

Note:

This file is created and named automatically by the installation script, using a hash security encryption scheme.

5. Did the system respond correctly to both these commands?
   - If yes, an SSL certificate is correctly installed on the MPP. No further action is required, unless you want to ensure that the certificate is valid. In that case, you can reinstall the certificate.
   - If no, the SSL certificate either is not installed or is invalid. Try reinstalling the certificate.

Related topics:

SSL certificate requirements on page 78

Validating the MPP configuration file for the SSL certificates

About this task

The MPP configuration file,mpp.conf, contains, among other things, the paths for the SSL certificates, both for the MPP and for the EPM.

Important:

The EPM expects to find the MPP certificate at /var/www/html/cert.pem. If you change this location, the EPM may not be able to find the certificate.

Procedure

1. Log in to the MPP server whose configuration file you want to validate.
2. At the Linux command line prompt, enter the cat $AVAYA_MPP_HOME/config/mpp.conf command.
   The system displays the contents of the entire MPP configuration file.
3. Locate the entry for the MPP SSL certificate and key in the Global section.
   The entry should be identical to the following:

```
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
SSLCertificateFile /var/www/html/cert.pem
```

4. Locate the entry for the MPP SSL certificate and key in the Virtual Host section.
   The entry should be identical to the following:

```
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
SSLCertificateFile "/etc/httpd/conf/ssl.crt/server.crt"
```

5. Locate the entry for the EPM SSL certificate download.

   This entry should look similar or identical to:

   ```
   SSLCACertificatePath "/opt/Avaya/ExperiencePortal/MPP/web/ssl.crt"
   ```

6. If any of these entries are different from what you have actually configured on your system, use a text editor to edit the `mpp.conf` file to reflect the actual configuration.
7. If you manually edit the `mpp.conf` file, you must restart the `httpd daemon` process to activate the changes:
   a) Stop the `httpd daemon` process by entering the `/sbin/service httpd stop` command.

      The system should respond with a message that ends with `[OK]` to indicate that the service has stopped.
   b) Restart the `httpd daemon` process by entering the `/sbin/service httpd start` command.

      The system should respond with a message that ends with `[OK]` to indicate that the service has started.

Reinstalling the SSL certificate from the EPM

Procedure

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

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

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

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.
2. At the Linux command line prompt, enter the `$AVAYA_HOME/Support/VP-Tools/setup_vpms.php` *`myhost`* command, where *`myhost`* is the server name or IP address where the EPM software is installed.
   The MPP queries the EPM for the SSL certificate, and if the certificate is located, asks for confirmation that you want to install it:

   ```
   Please enter 'y' to accept this certificate as an authorized
   controller of the MPP server, or enter 'n' to abort. [y]?
   ```

3. Enter `y`.

The system responds with the following message and prompt:

```
The httpd daemon (Apache) must be restarted to complete the
certificate's installation.
Enter 'y' if you would like httpd restarted now. [y]
```

4. Enter y.
   The system responds with the following message and prompt:

   ```
   The NTP daemon should be configured to use the EPM as the NTP
   server.
   Enter 'y' if you would like the NTP daemon configured with
   this EPM. [y]
   ```

5. If you want the EPM server to be configured as the NTP server for this MPP, enter y. Otherwise, enter n.

   The Network Time Protocol (NTP) allows the clock on the EPM server to be used as the reference point for synchronizing the clocks of all servers in the Avaya Aura® Experience Portal network. Because this can make troubleshooting and other maintenance activities more efficient, you can select this option.

6. Does the MPP indicate that the certificate was installed successfully?

   - If yes, and if the problems the system was experiencing do not recur, no further action is required.
   - If yes, but the problems persist, pursue other possible solutions or contact your Avaya technical support representative for assistance.
   - If no, try rebooting the MPP. If that does not resolve the problem, contact your Avaya technical support representative for assistance.

Chapter 5: Troubleshooting general issues

Troubleshooting completetimeout issues with Nuance servers and the VoiceXML Conformance Suite

If you are running the VoiceXML Conformance Suite with Nuance OSR or Recognizer servers and your changes to the VoiceXML recognition property `completetimeout` are being ignored, set the `completetimeout` parameter to zero (0) in each server's configuration file.

For details about this parameter, consult your Nuance documentation.

Proposed Solution for Nuance OpenSpeech Recognizer (OSR) servers

Procedure

1. On each Nuance OSR server, log in to the operating system and navigate to the directory in which the Nuance `OSSserver.cfg` file is stored.
2. In an ASCII editor, open the `OSSserver.cfg` file.
3. Find the `server.mrcp`*n*`.mrcpdefaults.completetimeout` parameter and set it to zero (0), as shown below:

```
server.mrcp1.mrcpdefaults.completetimeout     VXIString     0
server.mrcp2.mrcpdefaults.completetimeout     VXIString     0
```

4. Save and close the file.
5. Stop and then restart the Nuance OSR server.
6. Repeat this procedure for any other Nuance OSR servers in the Avaya Aura® Experience Portal system.

Proposed Solution for Nuance Recognizer servers

Procedure

1. On each Nuance Recognizer server, log in to the operating system and navigate to the directory in which the Nuance NSS`server.cfg` file is stored.
2. In an ASCII editor, open the NSS`server.cfg` file.
3. Find the `server.mrcp`*n*`.mrcpdefaults.completetimeout` parameter and set it to zero (0), as shown below:

```
server.mrcp1.mrcpdefaults.completetimeout     VXIInteger     0
server.mrcp2.mrcpdefaults.completetimeout     VXIInteger     0
```

4. Save and close the file.
5. Stop and then restart the Nuance Recognizer server.
6. Repeat this procedure for any other Nuance Recognizer servers in the Avaya Aura® Experience Portal system.

Runtime error in the online help search functionality

If you are using Internet Explorer 6 (IE6) SP2 or later, and you encounter a run-time error while using the search functionality in the online help, the debug option may be enabled.

Proposed Solution

Procedure

1. In Internet Explorer, select **Tools** > **Internet Options**.
2. In the **Internet Options** dialog box, select the **Advanced** tab.
3. In the **Browsing** group:
   a) Select the **Disable script debugging (Internet Explorer)** check box.
   b) Clear the selection of the **Display a notification about every script error** check box.
4. Click **OK**.
5. Restart Internet Explorer.

Web site’s security certificate error when accessing Avaya Aura® Experience Portal URL

If you are using Internet Explorer 7.0 (IE 7.0) or later and you encounter an error while accessing the URL to the Avaya Aura® Experience Portal server, the security certificates may not be added as Trusted Sites.

Proposed Solution

Procedure

1. In Internet Explorer, enter the URL for the Avaya Aura® Experience Portal server. An error message regarding the Web site’s security certificate appears on the web page.
2. Click **Continue to this website (not recommended)** link on the error page.
3. Click the **Certificate Error** in the toolbar.

   Note:

   The **Certificate Error** appears on the tool bar next to the URL that you have entered.
4. Click **View certificates** on the **Untrusted Certificate** page.
5. Click **Install Certificate** in the **Certificate** dialog box.
6. In the **Certificate Import Wizard**:
   a) Click **Next**.
   b) Select **Automatically select the certificate store based on the type of certificate** option.
   c) Click **Next**.
   d) Click **Finish**.
   e) Click **Yes** on the **Security Warning** message.
7. Click **OK** to close the **Certificate Import Wizard**.
8. Click **OK** to close the **Certificate** dialog box.
9. Restart Internet Explorer and enter the URL for the Avaya Aura® Experience Portal server.

File cannot be found error when exporting a Report

This error occurs only if you are using Internet Explorer.

When exporting a report, if you select the **Open** option in the **File Download** dialog box and `This file cannot be found` error is displayed, it could be due to a setting in Internet Explorer.

Related topics:

[Proposed Solution](#) on page 88

Proposed Solution

Procedure

1. In Internet Explorer, select **Tools** > **Internet Options**.
2. In the **Internet Options** dialog box, select the **Advanced** tab.
3. In the **Security** group, clear the selection of the **Do not save encrypted pages to disk** check box.
4. Click **OK**.
5. Restart Internet Explorer.

Graphing software not installed

The Call Flow Visualization graph that you can access from the **Application Summary Report** depends upon a third party component called Graphviz. To view the **Call Flow Visualization** graph, you must manually install Graphviz. The InstallGraphviz.sh script is located on the Avaya Aura® Experience Portal installation DVD.

Proposed Solution

Procedure

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

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

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

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

2. Enter the **`bash $AVAYA_HOME/Support/graphviz/InstallGraphviz.sh`** command.

Long TTS prompt does not play when Nuance is configured to MRCP V2 (TLS)

There is a known issue with initializing the TTS resource for a long TTS prompt when you configure Nuance server with MRCP V2 (TLS).

Proposed Solution

To resolve this, perform one of the following actions:

- Set the TTS parameter that is, **Prosody Volume** or **Prosody Rate** on the Change Application page, to an audible volume range that is greater than zero and less than 100.

  Note:

  You must set the **Prosody Volume** and **Prosody Rate** values to 50.

- Initialize short prompt first.

Setting the **Prosody Volume** and **Prosody Rate** values to 50 ensures that:

- The TTS resource is properly initialized for the request.
- All prompts from different speech server with different default volume settings, that include prerecord prompts, are played at the same volume.

Prompt (with barge-in enabled) times out before playing completely

If the default value of session timeout (60 sec) is shorter than the prompt, and barge-in is enabled in the application, the recognition event reaches timeout before the prompt is played completely.

Related topics:

Proposed Solution on page 90

Proposed Solution

About this task

Note:

This modification is required only if the customized application has a long play prompt with barge-in enabled, that exceeds the recognition session timeout.

To prevent timeout before the long prompt play is complete:

Procedure

1. Log in to the NSS speech server.
2. Navigate to the `$NSSSVRSDK` directory.
   - In Linux, the environment variable`$NSSSVRSDK` points to

     `/usr/local/Nuance/SpeechServer_5/server/config` (for NSS 5.0.x)

     Or

     `/usr/local/Nuance/Speech_Server/server/config` (for NSS 5.1.x)
   - In Windows, the environment variable `$NSSSVRSDK` points to `C:\Program Files\Nuance\SpeechServer 5.0\server\config`.
3. In an ASCII editor, open the `NSSserver.cfg` file.
4. Modify the following parameters:

   server.mrcp2.sip.sessionTimeout VXIInteger 120000

   server.mrcp1.rtsp.sessionTimeout VXIInteger 120000

Note:

The timeout value should be greater than the prompt play length.

5. Save and close the file.
6. Restart the NSS speech server.

TTS servers have different volume for the same pre-recorded prompts

Since the default volume settings in different speech servers are different, the volume of a pre-recorded prompt may vary for each TTS server.

To make this volume consistent, you can configure the TTS prosody volume from the Add Application or Change application page in EPM.

Proposed Solution

To resolve this, perform one of the following actions:

- Set the TTS parameter that is, **Prosody Volume** or **Prosody Rate** on the Change Application page, to an audible volume range that is greater than zero and less than 100.

  Note:

  You must set the **Prosody Volume** and **Prosody Rate** values to 50.

- Initialize short prompt first.

Setting the **Prosody Volume** and **Prosody Rate** values to 50 ensures that:

- The TTS resource is properly initialized for the request.
- All prompts from different speech server with different default volume settings, that include prerecord prompts, are played at the same volume.

Chapter 6: Troubleshooting installation and upgrade issues

Installation log files

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

Avaya Aura® Experience Portal creates several log files during the installation process. If the installation process:

- Completes successfully, Avaya Aura® Experience Portal copies the log files to `$AVAYA_HOME/logs/install_date`, where `$AVAYA_HOME` is the environment variable pointing to the installation path you specified on the Installation Destination installation screen and *`date`* is the date the installation process was run. The default installation directory is `/opt/Avaya/ExperiencePortal`.
- Does not complete successfully, Avaya Aura® Experience Portal copies the log files to `/opt/_Avaya_Voice-Portal_temp`.

General installation log files

Log filename	Description
`VP_Install.log`	Main log containing output from all EPM and MPP installation processes. This is the first log file you should consult if you need to troubleshoot an installation issue.
`ISOpt.log`	InstallShield generated log containing internal data.
`installSequence.log`	Subset of ISOpt.log
`prereqchecker.log`	Detailed information from the Prerequisite Checker.
`prereqchecker.out.log`	Results from the Prerequisite Checker.
`prereqchecker.err.log`	Any internal errors encountered by the Prerequisite Checker.
`prereqinstaller.log`	Detailed information from the Prerequisite Installer.
`prereqinstaller.out.log`	Results from the Prerequisite Installer.

Log filename	Description
prereqinstaller.err.log	Any internal errors encountered by the Prerequisite Installer.
SetIAVersion<component>.log	Version history of the Avaya Aura® Experience Portal components installed. The component can be the EPM, MPP or Docs.

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.
mpp.cert.gen.out.log	Results from the security certificate generation process.
mpp.cert.gen.err.log	Any internal errors generated from the certificate generation process.
mpp.cert.imp.out.log	Results from the security certificate import process.
mpp.cert.imp.err.log	Any internal errors generated from the certificate import process.
mpp.key.import.out.log	Results from the public key import process from the EPM.
mpp.key.import.err.log	Any internal errors generated from the public key import process from the EPM.

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.
vpms.cert.imp.out.log	Results from the security certificate import process.

Log filename	Description
`vpms.cert.imp.err.log`	Any internal errors generated from the certificate import process.

Fixing Prerequisite Checker failures

Solution

Procedure

1. Examine the Prerequisite Checker pages to determine exactly what problems were encountered.

   Tip:

   If the error is `UnknownHostException: localhost`, see Prerequisite Checker fails with UnknownHostException:localhost on page 95.

2. Upgrade your system to meet the minimum hardware and operating system requirements for Avaya Aura® Experience Portal, as described in the *Minimum server machine hardware requirements* topic of the *Planning for Avaya Aura® Experience Portal* guide.

Next steps

After you upgrade your system, you can resume the Avaya Aura® Experience Portal installation script at the current point as long as you did *not* exit the installation script or restart your Avaya Aura® Experience Portal server. If you want to:

- Resume the script, type 2 and press `Enter` until you go past the first Prerequisite Status page. Avaya Aura® Experience Portal reruns the Prerequisite Checker and you can then continue with the installation instructions.
- Quit the installation script, type 3 and press `Enter`, then type `1` and press `Enter` to confirm.

Prerequisite Checker fails with UnknownHostException:localhost

If you receive an error during the prerequisite check for the `localhost`, or a `faultString` reporting `UnknownHostException:localhost` during Avaya Aura® Experience Portal

installation or upgrade, it is likely that the `/etc/hosts` file of the server is not properly set up. As a result, the installation script cannot deploy certain Avaya Aura® Experience Portal components correctly.

The `/etc/hosts` file is a simple text file that associates IP addresses with one or more hostnames. The format is one line per IP address, with the associated hostnames separated by white space (spaces or tabs).

Solution

Procedure

1. Log into Linux on the EPM server.

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

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

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

2. Back up the original file prior to editing it by entering the `cp /etc/hosts /etc/hosts.bak` command.
3. With the ASCII text editor of your choice, open the `/etc/hosts` file.
4. Verify that:

   - The first line contains `127.0.0.1 localhost localhost.localdomain`, with the IP address and hostnames separated by spaces or tabs
   - If the file has other entries, each entry must in the form *`IP_address hostname1 hostname2...`*, where *`IP_address`* is the IP address of a server in the Avaya Aura® Experience Portal system and *`hostname1 hostname2...`* is one or more hostnames, separated by tabs or spaces, to associate with the IP address.

Example

The following shows a properly-formatted `/etc/hosts` file with two MPP servers:

```
127.0.0.1        localhost     localhost.localdomain       #Required first line
123.123.123.122  vpms_server_hostname                      #Primary EPM server IP
addy and hostname
123.123.123.123  first_mpp     first_ mpp.domainname.com   #First MPP server
123.123.123.124  second_ mpp   second_ mpp.domainname.com  #Second MPP server
```

Fixing Prerequisite Installer failures

The Prerequisite Installer installs additional software required for Avaya Aura® Experience Portal such as the Apache Web Server, Tomcat, and php. The majority of this software comes from RPMs installed by the Prerequisite Installer.

These failures are generally the result of installing Avaya Aura® Experience Portal on a server running a:

- More recent version of Red Hat Enterprise Linux than Release 6.0 32 bit or later. Although Avaya Aura® Experience Portal does support updates to Red Hat Enterprise Linux, some system RPMs in the newer updates can conflict with some of the RPMs that Avaya Aura® Experience Portal is attempting to install.
- Customized Red Hat Enterprise Linux installation that is missing an RPM required by one of the Avaya Aura® Experience Portal prerequisite RPMs.

Solution

Procedure

1. Examine the Prerequisite Installer report to determine exactly what problems were encountered and what log file, if any, is available for more information.
   For an example of one such error, see Sample Prerequisite Installer error message on page 98.
2. If you are using Red Hat Enterprise Linux Server 6.0 and the Prerequisite Installer fails for any of the php RPMs, install the following RPMs from your Red Hat installation CD-ROM or the Red Hat support web site:
   - `php-domxml`
   - `php`
   - `php-pear`
3. If that does not solve the problem, see Identifying RPM issues on page 100 for more information.

Next steps

After you fix any prerequisite software issues, you can resume the Avaya Aura® Experience Portal installation script at the current point as long as you did *not* exit the installation script or restart your Avaya Aura® Experience Portal server. If you want to:

- Resume the script, type 2 and press `Enter` until you go past the first Installation Status page. Avaya Aura® Experience Portal reruns the Prerequisite Installer and you can then continue with the installation instructions.
- Quit the installation script, type 3 and press `Enter`, then type 1 and press `Enter` to confirm.

Sample Prerequisite Installer error message

The following is an example of the error messages produced by the Prerequisite Installer when the installer encounters a more recent version of the JDK than Avaya Aura® Experience Portal was about to install. You can use this example as a guideline for solving any Prerequisite Installer issues you encounter.

```
================================================================================
Installation Status
================================================================================ -
Third-Party Software============================================================ | -
Network Time Protocol (NTP)------------------------------Already Completed | - GNU
MP (Arbitrary Precision Library)----------------------Already Completed | - XML
Library-----------------------------------------------Already Completed | -
Internationalized Domain Name Support Library-------------Already Completed | - cURL
(File Download Utility)-----------------------------Already Completed | - GnuPG
Common Error Library--------------------------------Already Completed | - General
Purpose Crypto Library----------------------------Already Completed | - XML File
Transform Library-----------------------------------Already Completed | -
ActiveMQ--------------------------------------------------Already Completed | -
TrueType Font Rendering Engine----------------------------Already Completed | - Font
Configuration and Customization Library--------------Already Completed | - Password
quality-control module-------------------------------------Success | - Shared
Library for X Window System-----------------------Already Completed | - Java(TM) 2
SDK Standard Edition--------------------------------------Failed
```

The following line indicates the start of the error information:

```
| | Error: RPM Installation failed with the following detail. | |
================================== | | jdk-1.5.0_12-fcs.i586.rpm install | | -
original directory='/mnt/cdrom/external' | | - RPM install directory='/mnt/cdrom/
external/J2SDK' | | - RPM name ='jdk-1.5.0_12-fcs.i586.rpm' | | - LOG file = '/tmp/
Avaya/install-rpm.log' | | ---------------------------------- | | >>>>>>Starting
RPM installation: 'rpm -U --replacepkgs jdk-1.5.0_12- | | fcs.i586.rpm'
```

The following two lines show the installed JDK version and why it does not match the version Avaya Aura® Experience Portal needs to install:

```
| | package jdk-1.5.0_14-fcs (which is newer than jdk-1.5.0_12-fcs) is | | Already
Completed | | >>>>>>RPM Installation failed: Exit Code: 2 | |
==================================
```

The following three lines restate the error that the version found was not the version expected:

```
| | RPM installation check: Expecting 'Found' = 'Expected'. | | Expected:
jdk-1.6.0_07-fcs.i586.rpm | | Found: jdk-1.5.0_14-fcs Out of Date | | Non-compliant
Java SDK found. Enter "rpm -e j2sdk" in the command line | | to uninstall the SDK,
then run the prerequisite installer again.
================================================================================
Install aborted due to installation failure.
================================================================================
```

To resolve this issue:

1. If you want to verify that this version is actually installed, enter the `rpm -q jdk` command.
2. Before you remove the more recent RPM version that you have installed, check the Avaya online support Web site, http://support.avaya.com, to make sure that a solution to this issue has not been posted. If no solution is available:
    a. Look at the `RPM installation check` line, which is the third highlighted line in the example. In this case, the Prerequisite Installer expected that the version it found installed on the system would be identical to the version it was installing. The solution is to remove the more recent version and let the Prerequisite Installer install the JDK version Avaya Aura® Experience Portal requires.
    b. To remove the installed JDK version, enter the `rpm -e jdk` command.
    c. Once the JDK version has been removed, return to the Avaya Aura® Experience Portal installation script and resume the installation.

Mounting a DVD on Avaya Linux

When you run the **`mount/mnt/cdrom`** command on Avaya Linux, you may see the `mount: No medium found` error.

This error occurs because the wrong physical device is mapped to the `/mnt/cdrom` mount point in the `/etc/fstab` file.

Proposed Solution

Procedure

1. Log in to Linux on the Experience Portal server as a user with root privileges.

2. Run the **cat/proc/sys/dev/cdrom/info** command. The system displays the following information table about your DVD device:

```
drive name:         sr0  hda
drive speed:        0    24
drive # of slots:   1    1
Can close tray:     1    1
...
```

3. Find the **drive name** row in the information table above.
4. In the **drive name** row, go to the last column. For example, the column you should be looking for contains the `hda` value .
5. Run the **ls -l /dev | grep cdrom** command. It displays the following list of device special files associated with your DVD devices.

```
lrwxrwxrwx 1 sroot root 4 Aug 31 08:11 cdrom -> scd0
lrwxrwxrwx 1 sroot root 3 Aug 16 11:16 cdrom-hda -> hda
lrwxrwxrwx 1 sroot root 4 Aug 31 08:11 cdrom-sr0 -> scd0
```

6. Find the line for the drive name that you found earlier.

   Note:
   In the example shown above, you should find the line that ends with `cdrom-hda -> hda`.

7. In the line that ends with `cdrom-hda -> hda`, find the device special file name.

   Note:
   In the example shown above, the device special file name is `cdrom-hda`.

8. Open the **/etc/fstab** file in a text editor.
9. Find the `/dev/cdrom /mnt/cdrom iso9660 noauto,owner,ro 0 2` line in the text editor.
10. Change **/dev/cdrom** with the path of the device special file that you just found.

    Note:
    In the example given above, the corrected line reads as follows:
    `/dev/cdrom-hda /mnt/cdrom iso9660 noauto,owner,ro 0 2`

11. Save and close the file.

Identifying RPM issues

If you have installed Red Hat Enterprise Linux Server 6.0, you should also verify that the correct RPMs are installed on your system. Avaya Aura® Experience Portal requires Release 6.0 32 bit or later. If you registered with Red Hat to automatically receive updates, there might be a conflict with one or more of the updated RPMs.

The Avaya Aura® Experience Portal installation includes a file that lists the RPMs and version numbers in Release 6.0 32 bit or later. This file is installed in `$AVAYA_HOME/Support/RedHat-RPM-Lists` and on the Avaya Aura® Experience Portal installation DVD under `Support/RedHat-RPM-Lists`.

You can generate a listing of the RPMs that are currently installed on your system and then compare the RPMs you have installed against what has been verified. Other versions than the ones verified might cause your Avaya Aura® Experience Portal system not to operate.

Note:

If the list of RPMs installed on your system does not exactly match the list of RPMs in the file on the Avaya Aura® Experience Portal installation DVD under `Support/RedHat-RPM-Lists`, it does not necessarily mean there is a problem. However, if you are still experiencing problems after you have reviewed the installation log files and initial configuration settings, you might bring your system inline with the verified list of RPMs to see if that solves the problem.

Solution

Procedure

1. On each Avaya Aura® Experience Portal server, log in to Linux as root.
2. Enter the `cat /etc/issue` command.
3. Verify that the version is Release 6.0 32 bit or later.
4. To get a list of the RPMS installed on your system and redirect the list to a file, enter the `rpm -qa | sort> /tmp/rpmlist.txt` command.
   When the system has finished generating `rpmlist.txt`, it stores the file in the `/tmp` directory.
5. To find any differences between the RPMs currently installed and the RPMs that are required for Avaya Aura® Experience Portal, enter the `diff /tmp/rpmlist.txt $AVAYA_HOME/Support/RedHat-RPM-Lists/*.txt` command.
6. To display the differences file, enter the `cat /tmp/diffrpms.txt` command.
7. Review the reported differences and bring the installed RPMs inline with the ones listed in a file on Avaya Aura® Experience Portal installation DVD under `Support/RedHat-RPM-Lists`.
8. If you need the correct version of an RPM, download it from Red Hat web site, http://www.redhat.com.
9. Once you have identified the problems and downloaded any required RPMs:

- To upgrade an RPM to a different version, enter the `rpm -u path/rpmname` command, where *path/rpmname* is the complete filename and path of the RPM you are updating.
- To install an RPM, enter the `rpm -i path/rpmname` command, where *path/rpmname* is the complete filename and path of the RPM you are installing.
- To remove an RPM, enter the `rpm -e rpmname` command, where *rpmname* is the name of the RPM you are removing.

Important:
Do not specify a file path when you remove an RPM.

Installation Progress Bar stops at 25% completed

If the **Installation Progress Bar** does not advance beyond 25% completed and the Post Installation Summary screen states that no summary information could be found, then InstallShield has encountered an internal error and the Avaya Aura® Experience Portal installation or upgrade was not successful.

This error condition is shown in the following example:

```
Installation Progress Note: The last portion of the install might take several
minutes to complete. Please be patient and wait for the Post Installation Summary to
be displayed. Installing Avaya Aura Experience Portal . Please wait...
|-----------|-----------|-----------|------------| 0% 25% 50% 75% 100% ||||||||||
--------------------------------------------------------------------------------
Post Installation Summary The Avaya Aura Experience Portal installation has
completed. Review the following information. If there are errors or warnings, then
please review the installation logs. No summary information could be found; please
check the log files for more information Press 3 to Finish or 5 to Redisplay [3]
java.io.IOException: java.io.IOException: /opt/_Avaya_Voice-Portal_temp/
MoveLogFiles: not found at java.lang.UNIXProcess.<init>(UNIXProcess.java:143) at
java.lang.Runtime.execInternal(Native Method) at
java.lang.Runtime.exec(Runtime.java:566) at
com.installshield.util.Java2ProcessExec.processExec(Unknown Source) at
com.installshield.util.ProcessExec.executeProcess(Unknown Source) at
com.installshield.wizardx.actions.ExecWizardAction.executeProcess(Unknown Source)
at com.installshield.wizardx.actions.ExecWizardAction.run(Unknown Source) at
java.lang.Thread.run(Thread.java:534)
```

In this case, no Avaya Aura® Experience Portal software was actually installed or upgraded.

Solution

Procedure

1. Type 3 to finish the aborted installation or upgrade process.
2. Return to the beginning of the installation or upgrade procedure you were following and rerun the Avaya Aura® Experience Portal installation script `installvp`.

EPM install finishes with an Axis error

A known issue with Axis sometimes affects the EPM software installation. If this problem occurs, the EPM software installer displays either `Exception: AxisFault` or `Warning: Axis may not be accepting new applications properly`, as shown in the following Post Installation Summary screens.

First sample Post Installation Summary screen:

```
Installing EPM... Possible Error during operation: Register vpappLog with Axis -
Start error description - Exception: AxisFault faultCode: {http://
schemas.xmlsoap.org/soap/envelope/}Server.generalException faultSubcode:
faultString: Couldn't find an appropriate operation for XML QName {http://
xml.apache.org/axis/wsdd/}deployment faultActor: faultNode: faultDetail: {http://
xml.apache.org/axis/}hostname:takuma.avaya.com - End error description - Possible
Error during operation: Deploy Core Services (Part 2/2) - Start error description -
Error: Could not deploy network log server: 255 Error: Could not deploy alarm server:
255 - End error description -
```

Second sample Post Installation Summary screen showing the `Warning: Axis may not be accepting new applications properly` message:

```
Installing Documentation... ...done installing Documentation Installing EPM...
Possible Error during operation: Start Tomcat - Start error description - Warning:
Axis may not be accepting new applications properly - End error description - ...done
installing EPM Installing MPP... ...done installing MPP
```

In this case, you need to:

Solution

Procedure

1. Type 3 to finish the incomplete installation process.

2. Return to the beginning of the installation procedure you were following and rerun the Avaya Aura® Experience Portal installation script `installvp`.

Install hangs at Post Installation Summary screen

A known InstallShield issue sometimes causes the software installation to hang, especially if there is a long delay between steps.

In this case, the Post Installation Summary screen displays:

```
Post Installation Summary The Avaya Aura Experience Portal installation has
completed. Review the following information. If there are errors or warnings, then
please review the installation logs. Installing Documentation... Press 3 to Finish
or 5 to Redisplay [3]
```

Solution

Procedure

Restart the installation script from the beginning, making sure that you do not pause too long between steps.
The Post Installation Summary screen should display messages similar to the following:

```
Post Installation Summary The Avaya Aura Experience Portal installation has
completed. Review the following information. If there are errors or warnings,
then please review the installation logs. Installing Documentation... ...done
installing Documentation Installing EPM... ...done installing EPM Installing
MPP... ...done installing MPP Press 3 to Finish or 5 to Redisplay [3] Moving
installation logs to: /opt/Avaya/ExperiencePortal/logs/
install_2008-01-21.000 [sroot@vpms-server cdrom]# reboot
```

MPP installation is hanging

Any hung or stale NFS mount points can cause RPM installations to hang while installing the Avaya Aura® Experience Portal software.

Solution

Procedure

1. On the MPP server, enter the `df` command.
2. If the server:
   - Responds to this command, then all NFS mount points are operational. Make sure that the EPM and MPP clocks are properly synchronized as described in Time synchronization problems on page 109.
   - Does not respond to the command, continue with this procedure.
3. Enter the `umount -l` command to unmount any file systems.
4. Close the Avaya Aura® Experience Portal installation script.
5. If the automount feature is enabled, disable it by commenting out the appropriate lines in the server's `/etc/fstab` file.
6. Reboot the server.
7. Restart the installation script from the beginning.

MPP could not import EPM key

The EPM installs correctly but the Public Key Verification screen displayed during the MPP installation contains the error:

`Failed to import key from specified host. Please check the following: URL: http://`*`EPM-server`*`/cert.pem`

The most common cause of this error is that the `iptables` firewall is enabled on the primary EPM server.

Solution

Procedure

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

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

   - Log in to the local Linux console as sroot.

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

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

2. Determine whether the `iptables` firewall is active by entering the `service iptables status` command.
3. If the firewall is:
   - Running, disable it by entering the `chkconfig --del iptables` command and proceed to Step 4.
   - Not running, try to manually download the certificate by entering the `curl http://`*`EPM-server`*`/cert.pem` command, where *`EPM-server`* is the domain name or IP address of the system where the primary EPM software is installed.

     If the command displays the lines `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`, regardless of what information is displayed between those lines, continue with this procedure. Otherwise, contact your Avaya Services representative.
4. Restart the *vpms* service by entering the `/sbin/service vpms restart` command.
   You will see a series of messages as the command starts to shut down EPM components. When the command has successfully stopped all relevant components, it displays the message: `VPMS Shutdown Status: [ OK ]`.

   The command immediately starts the relevant components. When it has finished, it displays the message: `VPMS Start Status: [ OK ]`.
5. Verify that you can log in to the EPM Web interface as described in the *Logging in to the Avaya Aura® Experience Portal web interface* topic in the *Administering Avaya Aura® Experience Portal* guide.
6. Return to the MPP server and either continue the current installation or restart the installation process.

File system check (fsck) reports number of day's error

If a file system check (fsck) is performed during the boot up process and indicates an error of extremely large number of days since the file system was checked, it is likely that:

- The system's clock was set backwards manually.
- NTP was reconfigured and then restarted at the time of OS or software installation.

This following is an example of the error message:

```
Sep 20 13:34:35 i3250-mpp fsck: RHE4.0-AV11.3EP2 has gone 49706 days without being
checked, check forced.
Sep 20 13:34:35 i3250-mpp fsck: RHE4.0-AV11.3EP2:
```

Related topics:

Solution on page 107

Solution

Procedure

You can ignore the number of days reported since the last check. Regardless of the exact number of days since the file system was last checked, fsck performs this check and reports the file system errors.

Changing PostgreSQL user account passwords

Before you begin

If you have just installed the EPM software and are still logged into the EPM server, make sure that the environment variables are properly loaded.

About this task

Avaya Aura® Experience Portal uses the following PostgreSQL user accounts:

Default account name	Description
postgres	The EPM server uses this account to log in to the Avaya Aura® Experience Portal database to store and retrieve data and to install new updates or patches. The database administrator can use this account to log in to the local `VoicePortal` database and perform database administration tasks. You can set the password for this account, but you cannot add other accounts of this type, delete this account, or change the account name. **Important:** Contact the Avaya Services representative to modify the local VoicePortal database as the database contains critical configuration information used to run the system.

Default account name	Description
report	This user account can only read those tables in the Experience Portal database that store report data. Speech application developers can use this account to log in to the database to create custom reports using any SQL-enabled report generation tool. You can have any number of accounts of this type with any account names.
reportwriter	This user account can only change the data in the tables that store report data in the Experience Portal database on the auxiliary EPM server. You can have any number of accounts of this type with any account names. **Important:** Contact the Avaya Services representative to modify the tables that store report data in the local VoicePortal database.
vpcommon	This account allows the auxiliary EPM server limited access to the main Experience Portal database, and it is required if you plan to configure an auxiliary EPM server. You can delete this account or set the password for this account, but you cannot add other accounts of this type or change the account name.

The `SetDbpassword` script allows you to change all account passwords and add and delete all accounts except for postgres, which cannot be deleted.

Note:

This script replaces the `UpdateDbPassword` script that was included with Avaya Aura® Experience Portal 4.0 or 4.1.

Procedure

1. Log in to Linux on the primary or auxiliary EPM server. If you are an Avaya Services representative and are using Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server:
   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and enter the `su - root` command to change the user to sroot.

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

2. Navigate to the `Support/VP-Tools/SetDbPassword` directory.

   Enter the `cd $AVAYA_HOME/Support/VP-Tools/SetDbPassword` command. `$AVAYA_HOME` is an environmental variable pointing to the name of the installation

directory specified during the Avaya Aura® Experience Portal software installation.

The default value is `/opt/Avaya/ExperiencePortal`.

3. To run the script:

   Enter `bash SetDbpassword.sh update -u` *`username`* `-p` *`password`* command.

   Where:

   - *`username`* is the name of the user account whose password you want to change.
   - *`password`* is the new password you want to use for this account.

   For example, to set the `postgres` password to NewPostgres1, you must enter the `bash SetDbpassword.sh update -u postgres -p NewPostgres1` command.

   If you change the password for the postgres account, Avaya Aura® Experience Portal stops and then restarts the *vpms* service.

Next steps

If you change the password for the vpcommon account on the primary EPM server, you must also change the password on the auxiliary EPM server.

Time synchronization problems

Avaya Aura® Experience Portal uses Network Time Protocol (NTP) 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.

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

Determining whether the servers are synchronized

Procedure

1. Simultaneously log in to Linux on the EPM server, each MPP server, and, if configured, the optional auxiliary EPM server.
2. On each server, during the same time enter the `date` command.

3. Verify that each MPP server and the optional auxiliary EPM server are synchronized with the primary EPM server.
4. If you find one or more unsynchronized servers, follow the procedure Verify that the NTP service is operating properly on page 110 below.

Verify that the NTP service is operating properly

Procedure

1. If necessary, log in to Linux on each unsynchronized MPP or auxiliary EPM server.

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

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

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.
2. Enter the `/sbin/service ntpd status` command.

   If the server returns a message stating that the NTP service is running, continue with this procedure. Otherwise, go to Synchronizing the MPP or auxiliary EPM clock with the primary EPM on page 111.
3. To verify that the NTP service is operating properly, enter the `/usr/sbin/ntpq -np` command.
4. A status message similar to the following appears:

   ```
   remote refid st t when poll reach delay offset jitter
   ==============================================================================
   ======= 123.123.123.123 LOCAL(0) 6 u 23 64 1 0.354 0.361 0.004
   ```

   If the `jitter` value displayed is 4000, go to Synchronizing the MPP or auxiliary EPM clock with the primary EPM on page 111.

   Note:

   The remote IP address displayed should point to the primary EPM server.

Synchronizing the MPP or auxiliary EPM clock with the primary EPM

Procedure

1. If you are working with an MPP server and the MPP software is running, stop it using the EPM Web interface:
   a) Log in to the EPM Web interface using an account with the Administration or Operations user role.
   b) From the EPM main menu, select **System Management** > **MPP Manager**.
   c) On the MPP Manager page, click the selection box associated with the MPP that you want to stop, then click **Stop** in the **State Commands** group.
   d) Confirm the action when requested.
   e) Wait until the operational state changes to Stopped.

      To check this, click **Refresh** and look at the **State** field.

      Note:

      The operational state changes when the last active call completes or the operational grace period expires, whichever comes first.
2. If necessary, log in to Linux on the server.

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

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

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.
3. If you are working with:

   - An MPP server, stop the `mpp` process by entering the `/sbin/service mpp stop` command.
   - The auxiliary VPMS server, stop the *`vpms`* service by entering the `/sbin/service vpms stop` command.
4. Restart the NTP process by entering the `/sbin/service ntpd restart` command.

   The system returns:

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

Note:

After you restart the NTP process, wait up to 10 minutes for the server to synchronize with the EPM.

5. After you give the servers enough time to synchronize themselves, verify that the process worked by entering the `/usr/sbin/ntpq -np` command.
   A status message similar to the following appears:

```
remote refid st t when poll reach delay offset jitter
==============================================================================
========= 123.123.123.123 LOCAL(0) 6 u 23 64 1 0.354 0.361 0.004
```

Note:

The remote IP address displayed should point to the primary EPM server.

6. If the `jitter` value is still set to 4000, go to Advanced time synchronization troubleshooting on page 112 below. Otherwise continue with this procedure.
7. If you are working with:
   - An MPP server, start the `mpp` process by entering the `/sbin/service mpp start` command.
   - The auxiliary VPMS server, start the *`vpms`* service by entering the `/sbin/service vpms start` command.
8. Verify the service has started by entering the `/sbin/service mpp status` or `/sbin/service vpms status` command.

Advanced time synchronization troubleshooting

Procedure

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

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.
2. Using an ASCII text editor, open the following files on the server and ensure that the hostname or the IP address of the primary EPM server is correct:
   - `/etc/ntp.conf`

- `/etc/ntp/step-tickers`

3. If the IP address or hostname is incorrect in either of the above files, fix it then save and close the files. Otherwise simply close the files.
4. If the primary EPM server is synchronized with an external clock, verify that the `/etc/ntp.conf` file on the primary EPM server is properly set up. For details, see External time sources.
5. If you made any changes to the files:
   a) Stop the appropriate service by entering the `service mpp stop` or `/sbin/service vpms stop` command.
   b) Restart the NTP process by entering the `/sbin/service ntpd restart` command.
      The system returns:
      ```
      Shutting down ntpd: [OK] Synchronizing with time server [OK] Starting ntpd: [OK]
      ```
      Note:
      After you restart the NTP process, wait up to 10 minutes for the server to synchronize with the EPM.
   c) After you give the servers enough time to synchronize themselves, verify that the process worked by entering the `/usr/sbin/ntpq -np` command.
      A status message similar to the following appears:
      ```
      remote refid st t when poll reach delay offset jitter
      ==============================================================================
      ============ 123.123.123.123 LOCAL(0) 6 u 23 64 1 0.354 0.361 0.004
      ```
      Note:
      The remote IP address displayed should point to the primary EPM server.
6. If the `jitter` value is still set to 4000:
   a) Reboot the server.
   b) Enter the `/usr/sbin/ntpq -np` command.
   c) If the `jitter` value is still set to 4000, reinstall the MPP or auxiliary EPM software.

Time Synchronization between external database and EPM servers

If you connect a Avaya Aura® Experience Portal system to an external database, you may want to make sure that you synchronize the time so that it is same across all servers. While Avaya Aura® Experience Portal only requires that the EPM and MPP server time be synchronized, you can also synchronize all the servers that Avaya Aura® Experience Portal connects to. For

more information, see the *External time sources* topic in the *Implementing Avaya Aura® Experience Portal on multiple servers* guide.

Chapter 7: Restoring the previous operating system after an upgrade

Restore Avaya Aura® Experience Portal 5.0 or 5.1 on Avaya Enterprise Linux

If you want to revert an upgraded Avaya Aura® Experience Portal system running on Avaya Enterprise Linux back to 5.0 or 5.1 , you need to:

Step	Description	✔
1	Restore the previous version of Avaya Enterprise Linux on all Avaya Aura® Experience Portal servers as described in Restoring the Avaya Enterprise Linux 5.0 or 5.1 operating system on page 116.	
2	Restore the 5.0 or 5.1 EPM server as described in Restoring the 5.0 or 5.1 software on the EPM server or a single-server Avaya Aura Experience Portal system running Avaya Enterprise Linux on page 116.	
3	Restore the 5.0 or 5.1 MPP servers as described in Restoring the 5.0 or 5.1 MPP software on a server running Avaya Enterprise Linux on page 118.	

Related topics:

Restoring the Avaya Enterprise Linux 5.0 or 5.1 operating system on page 116

Restoring the 5.0 or 5.1 software on the EPM server or a single-server Avaya Aura Experience Portal system running Avaya Enterprise Linux on page 116

Restoring the 5.0 or 5.1 MPP software on a server running Avaya Enterprise Linux on page 118

Restoring the Avaya Enterprise Linux 5.0 or 5.1 operating system

Before you begin

If you are working with an MPP server, take the MPP offline as described in Taking the MPP offline using the 5.0 or 5.1 VPMS web interface.

Procedure

1. Log in to Linux on the Voice Portal server.

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

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

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

2. 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 5.0 or 5.1 software on the EPM server or a single-server Avaya Aura® Experience Portal system running Avaya Enterprise Linux

Before you begin

Make sure you have restored the operating system as described in Restoring the Avaya Enterprise Linux 5.0 or 5.1 operating system on page 116.

Procedure

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

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

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

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

2. Check the status of the `postgres` service by entering the `/sbin/service postgresql status` command.
3. If the `postgres` service is running, stop it by entering the `/sbin/service postgresql stop` command.
4. Stop the *vpms* service by entering the `/sbin/service vpms stop` command. You will see a series of messages as the command starts to shut down EPM components. When the command has successfully stopped all relevant components, it displays the message: `VPMS Shutdown Status: [ OK ]`.
5. Navigate to the `pgsql` directory by entering the `cd /var/lib/pgsql` command.
6. Rename the current data directory that contains the Avaya Aura® Experience Portal 5.0 or 5.1 data by entering the `mv data data_vp4` command.
7. In the `pgsql` directory, locate the back up directory that Avaya Aura® Experience Portal created when you installed the new version. The file name has the format `data_vp_<backup_date>_<backup_time>`.
8. Copy this back up 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 `/sbin/service vpms start` command.
    You will see a series of messages as the command starts several EPM components. When the command has successfully started all relevant components, it displays the message: `VPMS Start Status: [ OK ]`.

Restoring the 5.0 or 5.1 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 5.0 or 5.1 operating system on page 116.
- Make sure you have restored the EPM server.

Procedure

1. Restore the log files you packed for that MPP as part of System backup.
2. If your Avaya Aura® Experience Portal administrator moved the 5.0 or 5.1 MPP logs to a new directory or partition using the `mppMoveLogs.sh` script, make sure that the appropriate mount point appears in the `/etc/fstab` file as described in the *Moving the MPP logs to a different location* topic in the *Administering Avaya Aura® Experience Portal* guide.

Next steps

At this point, you can: or

- Restore another MPP server.
- Start the restored MPP as described in the *Starting an MPP server* topic in the *Administering Avaya Aura® Experience Portal* guide.
- Start multiple restored MPP servers as described in the *Starting all MPP servers* topic in the *Administering Avaya Aura® Experience Portal* guide.

Restoring Avaya Aura® Experience Portal 5.0 or 5.1 on a dedicated EPM server or a single-server Avaya Aura® Experience Portal system running Red Hat Enterprise Linux

Before you begin

Make sure you have access to the back up files created, as described in the *Backing up your existing Avaya Aura® Experience Portal 5.0 or 5.1 data* topic in the *Upgrading Avaya Aura® Experience Portal 5.0 or 5.1 to Release 5.1* guide.

About this task

Note:

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

Procedure

1. Install Red Hat Enterprise Linux 5.4 using the Red Hat installation CD-ROM and the exact options you used for Avaya Aura® Experience Portal 5.0 or 5.1 .
2. Reinstall the EPM software from your 5.0 or 5.1 Avaya Aura® Experience Portal installation DVD.

   Make sure that you select the same options that you selected during the first install.
3. Restore your Avaya Aura® Experience Portal database from the backup you made, as described in the *Backing up your existing Avaya Aura® Experience Portal 5.0 or 5.1 data* topic in the *Upgrading Avaya Aura® Experience Portal 5.0 or 5.1 to Release 5.1* guide.
4. If you changed the default log and alarm retention periods, reset those values as described in the *Setting log data retention periods* topic in the *Administering Avaya Aura® Experience Portal* guide.

Restoring a dedicated 5.0 or 5.1 MPP server on Red Hat Enterprise Linux

To restore 5.0 or 5.1 , you need to reinstall the operating system and then reinstall the Avaya Aura® Experience Portal software.

Before you begin

Make sure you have access to the back up files created, as described in the *Backing up your existing Avaya Aura® Experience Portal 5.0 or 5.1 data* topic in the *Upgrading Avaya Aura® Experience Portal 5.0 or 5.1 to Release 5.1* guide.

Make sure you have already restored your EPM server as described in Restoring Avaya Aura Experience Portal 5.0 or 5.1 on a dedicated EPM server or a single-server Avaya Aura Experience Portal system running Red Hat Enterprise Linux on page 118.

Procedure

1. Take the MPP offline as described in Taking the MPP offline using the 5.0 or 5.1 VPMS web interface.

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 5.4 using the Red Hat installation CD-ROM and the exact options you used for Avaya Aura® Experience Portal 5.0 or 5.1 .
3. Reinstall the MPP software from your Avaya Aura® Experience Portal installation DVD. Verify that you select the same options that you selected during the first install.
4. Restore the log files you packed for that MPP as part of the back up process described in the *Backing up your existing Avaya Aura® Experience Portal 5.0 or 5.1 data* topic in the *Upgrading Avaya Aura® Experience Portal 5.0 or 5.1 to Release 5.1* guide.
5. If you changed the AVB configuration files, restore the customized files you saved during the back up process described in the *Backing up your existing Avaya Aura® Experience Portal 5.0 or 5.1 data* topic in the *Upgrading Avaya Aura® Experience Portal 5.0 or 5.1 to Release 5.1* guide.

Next steps

- Restore another MPP by following this procedure on that MPP.
- If all MPP servers have been restored, reestablish the link between the restored EPM server and the restored MPP servers. For more information, see the *Reestablishing the link between the EPM and the upgraded MPP* topic in the *Upgrading Avaya Aura® Experience Portal 4.0 or 4.1 to Release 5.0* guide.

Chapter 8: Taking the MPP offline using the 5.0 or 5.1 EPM Web interface

About this task

Before you work with an MPP server, you need to take the MPP offline. This procedure explains how to do so using the EPM Web interface that is included with Voice Portal release 4.1 and higher.

Procedure

1. Log in to the EPM Web interface using an account with the Administration or Operations user role.
2. From the EPM main menu, select **System Management** > **MPP Manager**.
3. On the MPP Manager page, use the Selection check box in the MPP server table to select which MPP server you want to take offline.
4. Click the **Stop** button in the **State Commands** group and confirm your selection when prompted.
   Avaya Aura® Experience Portal stops the selected the MPP server when the last active call completes or the grace period expires, whichever comes first.
5. After a few minutes, click **Refresh** and verify that the **State** is **Stopped** for the MPP server you want to upgrade.
6. If the MPP operational state:
   - Changed to **Stopped**, continue with this procedure.
   - Did *not* change, you need to stop the `mpp` service as described in Stopping the MPP service on page 123.
7. Use the Selection check box in the MPP server table to reselect the MPP server you want to take offline.
8. Click **Offline** in the **Mode Commands** group.
9. Click **Refresh** and verify that the **Mode** is **Offline** for the MPP server you want to upgrade.

Chapter 9: Stopping the MPP service

Procedure

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

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

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

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

2. Enter the `/sbin/service mpp stop` command.

Chapter 10: Uninstalling and reinstalling Avaya Aura Experience Portal

Uninstalling Tomcat application server

Use this procedure if you need to uninstall a Tomcat Application server that you manually installed on the same machine as the Avaya Aura® Experience Portal software.

Procedure

1. Log in to Linux on the Voice Portal server.

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

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

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.
2. Stop the application server by entering the `service appserver stop` command.
3. Wait for 30 seconds, then make sure that the application server stopped successfully by entering the `/sbin/service appserver status` command.
4. If this command returns the message `appserver (pid` *`pid`*`) is running`:

   a) Make a note of the process ID *`pid`*.

   b) Enter the `kill` *`pid`* command, where *`pid`* is the process ID returned by the **`service`** command.
5. Unregister the service by entering the `chkconfig --del appserver` command.
6. Enter the `cd /etc/init.d` command.
7. Delete the application server script file by entering the `rm appserver` command.
8. Enter the `cd /etc/profile.d` command.

9. Delete the configuration files by entering the `rm appserver.*` command.

   If the system prompts for confirmation, type `Y` and press `Enter`.

10. Delete the application server files by entering the `rm -rf tomcat-install-directory` command, where *`tomcat-install-directory`* is the top-level directory under which Tomcat is installed.

    If you installed the application server using the automatic installation script included with Avaya Aura® Experience Portal, or if you used the default installation directory given in the manual installation procedure, enter `rm -rf /opt/Tomcat/AppServer`

Reinstalling the EPM and MPP software in a single server system

About this task

Follow this procedure if you want to reinstall both the EPM and MPP software on a system in which the EPM and the MPP reside on the same server.

Procedure

1. If your site uses customized scripts, do the following to ensure you do not lose those scripts when the installation procedure writes over the scripts for the Database Backup utility:
   a) Navigate to the backup directory located in $AVAYA_HOME by entering the cd `$AVAYA_HOME/Support/Database/DBbackup` command.
   b) Copy all the files in this directory to a temporary directory.
2. If you changed the values for event and alarm record retention in the Avaya Aura® Experience Portal database, do the following to ensure that you can correct those values after the installation procedure resets them to the default values:
   a) From the EPM main menu, select **System Configuration** > **Alarm/Log Options**.
   b) On the Viewer Settings page, take note of the current values.

      The default for **Purge Enabled** is **Yes** for all record types, and the default retention times are:

      - 7 days for alarm records
      - 15 days for event records
      - 180 days for audit log records
3. Log in to Linux on the Voice Portal server.

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

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

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

4. Stop the *vpms* service by entering the `/sbin/service vpms stop` command. You will see a series of messages as the command starts to shut down EPM components. When the command has successfully stopped all relevant components, it displays the message: `VPMS Shutdown Status: [ OK ]`.
5. Delete the Tomcat directory by entering the `rmdir` *`TomcatHome`*`/apache-tomcat-5.5.20` command, where *`TomcatHome`* is the directory in which the Tomcat servlet engine software is installed. The default is `/opt/Tomcat`.
6. The reinstallation procedure is identical to the upgrade procedure because the installation script will find a previous version of the EPM on the server. The fact that the previous version is the same release as you want to install makes no difference to the installation script.
7. Reestablish the connection between the reinstalled MPP and the EPM.
8. If you copied your customized Database Backup utility scripts to a temporary location at the beginning of this procedure, copy your customized files back to the `/var/lib/pgsql/DBbackup` directory.
9. Restore your customized retired alarm and event settings on the Viewer Settings page in the EPM.

Reinstalling the MPP software

About this task

Follow this procedure if you want to reinstall the MPP software on a dedicated server or on a single server system when you do not want to reinstall the EPM and the MPP software. If you want to reinstall both the EPM and MPP software in a single server system, see Reinstalling the EPM and MPP software in a single server system on page 126.

Note:

The reinstallation procedure is identical to the upgrade procedure because the installation script will find a previous version of the MPP on the server.

Procedure

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

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

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

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

2. Insert the Avaya Aura® Experience Portal 6.0 software installation DVD into the DVD drive of the server.

   Tip:

   These instructions assume that you are going to access the Avaya Aura® 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 Avaya Aura® Experience Portal installation DVD to that directory. However, that directory needs to be readable by all users on the system because the Avaya Aura® Experience Portal installation script changes users during execution. If the directory is only readable by the root or sroot user, the installation script will encounter errors and will not complete successfully. You also need to ensure the directory name does not contain spaces. If there are spaces in the directory name, the installation script will encounter errors and will not complete successfully.

3. Mount the Avaya Aura® Experience Portal 6.0 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 device in the `fstab` file.
   - If you are working with Red Hat Enterprise Linux Server 6.0, to mount the DVD:
     - Enter the `mkdir /media/cdrom` command.

       Note:

       This command is required only if the /mnt/cdrom mount point is not created.

     - Enter the `mount /dev/cdrom /media/cdrom` command.

   Warning:

   When Red Hat Enterprise Linux Server 6.0 automatically mounts the DVD, the files on the DVD are not executable. You must manually mount the Avaya Aura® Experience Portal installation DVD using the commands shown above.

If the **mount** commands shown above do not work, consult your server documentation for the appropriate **mount** command.

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

   Important:

   When choosing installation options, be sure to wait for the next prompt before pressing a key. The installation stores your key presses in a buffer and enters all of them after the current processing completes. For example, if you press the `Enter` key repeatedly while the system is performing its prerequisite checks, you may unintentionally skip options you want to change. If that happens, use the **Previous** option on any screen to go back and change your earlier choices.
6. On the Installation Destination screen, press `Enter` to upgrade the software in the same location as the previous release.

   Important:

   You must not change the installation directory when upgrading to a new release.
7. Press `Enter` to move to the next screen.
8. On the Experience Portal Feature Selection screen:
   a) Type `1` and press `Enter` to clear **EPM**.
      The screen refreshes with only **Documentation** selected.
   b) Type `2` and press `Enter` to select **MPP**.
      The screen refreshes with both **MPP** and **Documentation** selected.
   c) Press `Enter` to confirm your selections.
9. Press `Enter` to move to the next screen.
10. On the Version Confirmation screen, verify that the **New Version** column indicates that you are about to upgrade to release 6.0 of the MPP software.
11. Press `Enter` to move to the next screen.
12. Read through the end user license agreement.
13. On the final End User License Agreement page, type `1` and press `Enter` to select option **1 - I accept the terms of the license agreement**.
    The screen refreshes with **1 - I accept the terms of the license agreement** as the selected option.
14. Press `Enter` to accept the agreement.
15. Press `Enter` to move to the next screen.
    Experience Portal automatically starts the Prerequisite Checker, which analyzes your system's hardware and operating system configuration.
16. After the configuration analysis is complete, the Prerequisite Checker displays a message stating whether all prerequisite checks passed followed by the first

Prerequisite Status page. Press `Enter` to view the rest of the Prerequisite Status pages.

If any prerequisite installations fail, examine the Prerequisite Status pages carefully to determine which checks failed. You must correct these issues before you can continue with this procedure.

17. When all prerequisite checks pass, press `Enter` to move to the next screen. Experience Portal automatically starts the Prerequisite Installer, which attempts to install the required software on the Avaya Aura® Experience Portal server.
18. After the Prerequisite Installer completes installing the required software, it displays a message stating whether all prerequisite installs were successful followed by the first Installation Status page. Press `Enter` to view the rest of the Installation Status pages.

    If any prerequisite installations fail, examine the Installation Status pages carefully to determine which installations failed. You must correct these issues before you can continue with this procedure.
19. When all prerequisites are successfully installed, press `Enter` to move to the next screen.
20. Press `Enter` to move to the next screen.
21. On the Primary EPM Server Location screen, specify the server name or IP address of the EPM server. If you want to:
    - Use the existing EPM server and port number that is displayed in square brackets [ ] after the installation prompt, press `Enter`.
    - If no existing EPM location exists or you want to change the location of the EPM server, type the server name or IP address where the EPM software is installed. If you used a port other than the default EPM port (80), append `:`*`port_number`* to the address. When you are done, press `Enter` to submit the new address.

      For example, to specify the machine with the server name `EPM_Server` on the default port, type `EPM_Server`. To specify the same server on port 86, type `EPM_Server:86`.

    Note:

    The previous releases of the EPM software defaulted to port 8080. If you used the default EPM port in both cases, you need to remove the **:8080** from the existing EPM location.

    The MPP installation uses this information to retrieve the public key from the EPM. The public key provides authentication between the EPM and MPP servers to help secure your Avaya Aura® Experience Portal system.
22. Press `Enter` to move to the next screen.
23. On the Public Key Verification screen, if you recorded the fingerprint information from the EPM security certificate during the primary EPM software installation,

compare it to the Public Key fingerprint information presented in this screen. The fingerprint information from Public Key should match the fingerprint information from the EPM security certificate.

If the public key could not be downloaded, see MPP could not import EPM key on page 105.

24. Press `Enter` to move to the next screen.
25. Avaya Aura® Experience Portal uses SSL protocol to establish a secure connection between its servers. This connection requires a security certificate that can be created by Avaya Aura® Experience Portal or purchased from a third-party company. On the Security Certificate screen:
    - If you want Avaya Aura® Experience Portal to create a security certificate:
        1. Verify that option **1 - Create a new certificate for this server** is selected. If not, type `1` and press `Enter`.
        2. Press `Enter` to confirm that selection.
    - If you want Avaya Aura® Experience Portal to use a certificate from a company such as VeriSign, you can import the certificate as long as the certificate is in PKCS12 format and the certificate resides on the local server or on a locally accessible NFS-mounted drive. To do so:
        1. Verify that option **2 - Import a certificate from a specified location** is selected. If not, type `2` and press `Enter`.
        2. Press `Enter` to confirm that selection.
        3. Type the full file path and name of the security certificate and press `Enter`.

           The screen displays the location that you entered for your verification.
        4. Type the password for the security certificate and press `Enter`.
26. Press `Enter` to move to the next screen.
27. On the Security Certificate Verification screen, verify the security certificate and press `Enter` to move to the next screen.

    Tip:

    When you add the MPP to Avaya Aura® Experience Portal through the EPM, the EPM displays the MPP security certificate. You should record the fingerprint information from this security certificate so that you can compare it to the one displayed in the EPM.
28. On the Pre Installation Summary screen, verify the installation information and press `Enter` to install the Avaya Aura® Experience Portal software.

Avaya Aura® Experience Portal displays the Installation Progress screen and 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. Wait until Avaya Aura® Experience Portal displays the Post Installation Summary screen.

29. On the Post Installation Summary screen, verify that the **Installation Progress Bar** has reached 100% and that the message `...done installing` *`feature_name`* appears for each feature that you selected on the Experience Portal Feature Selection screen.

    Note:

    If the **Installation Progress Bar** on the Installation Progress screen stops at 25% and the Post Installation Summary screen states that no summary information could be found, see Solution on page 103.

30. Press `Enter` to end the installation script.
    During the installation process, Avaya Aura® Experience Portal creates several log files that you can use to verify what happened during installation. When the installation process is complete, Avaya Aura® Experience Portal moves those logs to the standard log directory and displays the exact path on the screen. For more information, see Upgrade installation log files on page 168.

31. Enter the `/sbin/service mpp status` command to verify that the MPP system manager is running.
    The MPP server returns the message `mppsysmgr (pid <`*`pid`*`>) is running`, where <*pid*> is the process id.

32. To unmount and eject the DVD:
    a) Change directories to anything outside the mount point. For example, you could enter the `cd /` command to change to the root directory.
    b) Unmount the DVD device as described in your server documentation.
    c) To eject the Avaya Aura® Experience Portal installation DVD, press the button on the DVD device or enter the `eject` command.

33. Load the environment variables created during the installation by logging out of Linux and then logging back in as a non-root user. To do so:
    a) Log out the Linux system.
    b) Log back in to Linux by entering a non-root user name and password at the prompts.
    c) Log back in as root or `sroot`. To do so:
       - If you are working with Avaya Enterprise Linux, enter the `su - sroot` command.
       - If you are working with Red Hat Enterprise Linux Server 6.0, enter the `su -` command.

34. To verify that NTP is operating properly on the MPP enter the `/usr/sbin/ntpq -np` command.
    A status message similar to the following is displayed:

    ```
    remote refid st t when poll reach delay offset jitter
    ==============================================================
    123.123.123.123 127.127.1.0 6 u 23 64 1 0.354 0.361 0.004
    ```

    Make sure that:

    - The remote IP address points to the primary EPM server.
    - The jitter value is *not* 4000.

Next steps

Reestablish the connection between the reinstalled MPP and the EPM as described in the *Reestablishing the link between the EPM and the upgraded MPP* topic in the *Upgrading from Voice Portal 4.0 or 4.1 to Release 5.0* guide.

Reinstalling the primary EPM software on a dedicated EPM server

About this task

Follow this procedure if the primary EPM software resides on a dedicated server. If your EPM software resides on the same server as the MPP software, see Reinstalling the EPM and MPP software in a single server system on page 126. If you want to reinstall the auxiliary EPM software, see Reinstalling the auxiliary EPM software on page 136.

Procedure

1. If your site uses customized scripts, do the following to ensure you do not lose those scripts when the installation procedure writes over the scripts for the Database Backup utility:
   a) Navigate to the backup directory located in $AVAYA_HOME by entering the cd `$AVAYA_HOME/Support/Database/DBbackup` command.
   b) Copy all the files in this directory to a temporary directory.
2. If you changed the values for event and alarm record retention in the Avaya Aura® Experience Portal database, do the following to ensure that you can correct those values after the installation procedure resets them to the default values:
   a) From the EPM main menu, select **System Configuration** > **Alarm/Log Options**.
   b) On the Viewer Settings page, take note of the current values.

The default for **Purge Enabled** is **Yes** for all record types, and the default retention times are:

- 7 days for alarm records
- 15 days for event records
- 180 days for audit log records

3. Log in to Linux on the Experience Portal primary EPM server.

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

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

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

4. Stop the *vpms* service by entering the `/sbin/service vpms stop` command. You will see a series of messages as the command starts to shut down EPM components. When the command has successfully stopped all relevant components, it displays the message: `VPMS Shutdown Status: [ OK ]`.

5. Delete the Tomcat directory by entering the `rmdir` *`TomcatHome`*`/apache-tomcat-5.5.20` command, where *`TomcatHome`* is the directory in which the Tomcat servlet engine software is installed. The default is `/opt/Tomcat`.

6. The reinstallation procedure is identical to the upgrade procedure because the installation script will find a previous version of the EPM on the server. The fact that the previous version is the same release as you want to install makes no difference to the installation script. Therefore, you can reinstall the EPM software as described in the *EPM software upgrade overview* in the *Upgrading* from Avaya Aura® Experience Portal 4.0 *or* 4.1 *to Release* 6.0 guide.

7. After you reinstall the EPM software, relink each MPP server in your Avaya Aura® Experience Portal configuration with the new EPM.

8. If you copied your customized Database Backup utility scripts to a temporary location at the beginning of this procedure, copy your customized files back to the `/var/lib/pgsql/DBbackup` directory.

9. Restore your customized retired alarm and event settings on the Viewer Settings page in the EPM.

Related topics:

Verifying Axis configuration on page 31

Reinstalling the EPM software in a single server system

About this task

Follow this procedure if you want to reinstall just the EPM software on a system in which the EPM and the MPP reside on the same server. If you want to:

- Reinstall both the EPM and MPP software on a single server system, see Reinstalling the EPM and MPP software in a single server system on page 126.
- Reinstall the EPM software on a dedicated server, see Reinstalling the primary EPM software on a dedicated EPM server on page 133.

Procedure

1. If your site uses customized scripts, do the following to ensure you do not lose those scripts when the installation procedure writes over the scripts for the Database Backup utility:
   a) Navigate to the backup directory located in $AVAYA_HOME by entering the cd `$AVAYA_HOME/Support/Database/DBbackup` command.
   b) Copy all the files in this directory to a temporary directory.
2. If you changed the values for event and alarm record retention in the Avaya Aura® Experience Portal database, do the following to ensure that you can correct those values after the installation procedure resets them to the default values:
   a) From the EPM main menu, select **System Configuration** > **Alarm/Log Options**.
   b) On the Viewer Settings page, take note of the current values.
   The default for **Purge Enabled** is **Yes** for all record types, and the default retention times are:
      - 7 days for alarm records
      - 15 days for event records
      - 180 days for audit log records
3. Log in to Linux on the Voice Portal server.
   If you are an Avaya Services representative, and are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:
      - Log in to the local Linux console as sroot.
      - Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.

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

4. Stop the *vpms* service by entering the `/sbin/service vpms stop` command. You will see a series of messages as the command starts to shut down EPM components. When the command has successfully stopped all relevant components, it displays the message: `VPMS Shutdown Status: [ OK ]`.
5. Delete the Tomcat directory by entering the `rmdir` *`TomcatHome`*`/apache-tomcat-5.5.20` command, where *`TomcatHome`* is the directory in which the Tomcat servlet engine software is installed. The default is `/opt/Tomcat`.
6. The reinstallation procedure is identical to the upgrade procedure because the installation script will find a previous version of the EPM on the server. Therefore, you can reinstall just the EPM software as described in the *Upgrading* from Avaya Aura® Experience Portal4.0*or*4.1*to Release* 6.0 guide.
7. Reestablish the connection between the reinstalled EPM and the MPP as described in the *Reconnecting an existing MPP server with the EPM server* topic in the *Administering Avaya Aura® Experience Portal* guide.
8. If you copied your customized Database Backup utility scripts to a temporary location at the beginning of this procedure, copy your customized files back to the `/var/lib/pgsql/DBbackup` directory.
9. Restore your customized retired alarm and event settings on the Viewer Settings page in the EPM.

Related topics:

Verifying Axis configuration on page 31

Reinstalling the auxiliary EPM software

About this task

Follow this procedure if your EPM software resides on a dedicated server. If your EPM software resides on the same server as the MPP software, see Reinstalling the EPM and MPP software in a single server system on page 126.

Procedure

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

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

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

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

2. Stop the *vpms* service by entering the `/sbin/service vpms stop` command. You will see a series of messages as the command starts to shut down EPM components. When the command has successfully stopped all relevant components, it displays the message: `VPMS Shutdown Status: [ OK ]`.
3. Delete the Tomcat directory by entering the `rmdir` *`TomcatHome`*`/apache-tomcat-5.5.20` command, where *`TomcatHome`* is the directory in which the Tomcat servlet engine software is installed. The default is `/opt/Tomcat`.
4. Insert the Avaya Aura® Experience Portal 6.0 software installation DVD into the DVD drive of the server.

   Tip:

   These instructions assume that you are going to access the Avaya Aura® 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 Avaya Aura® Experience Portal installation DVD to that directory. However, that directory needs to be readable by all users on the system because the Avaya Aura® Experience Portal installation script changes users during execution. If the directory is only readable by the root or `sroot` user, the installation script will encounter errors and will not complete successfully.
5. Mount the Avaya Aura® Experience Portal 6.0 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 device in the `fstab` file.
   - If you are working with Red Hat Enterprise Linux Server 6.0, to mount the DVD:
     - Enter the `mkdir /media/cdrom` command.

       Note:

       This command is required only if the /mnt/cdrom mount point is not created.

     - Enter the `mount /dev/cdrom /media/cdrom` command.

       Warning:

       When Red Hat Enterprise Linux Server 6.0 automatically mounts the DVD, the files on the DVD are not executable. You must manually mount the Avaya Aura® Experience Portal installation DVD using the commands shown above.

   If the **`mount`** commands shown above do not work, consult your server documentation for the appropriate **`mount`** command.

6. Change to the mount point directory.
7. Enter the `bash installvp` command and press `Enter` to start the installation script.

   Important:

   When choosing installation options, be sure to wait for the next prompt before pressing a key. The installation stores your key presses in a buffer and enters all of them after the current processing completes. For example, if you press the `Enter` key repeatedly while the system is performing its prerequisite checks, you may unintentionally skip options you want to change. If that happens, use the **Previous** option on any screen to go back and change your earlier choices.
8. On the Installation Destination screen, press `Enter` to upgrade the software in the same location as the previous release.

   Important:

   You must not change the installation directory when upgrading to a new release.
9. Press `Enter` to move to the next screen.
10. On the Experience Portal Feature Selection screen, press `Enter` to accept the default installation options of **EPM** and **Documentation**.
11. Press `Enter` to move to the next screen.
12. On the Version Confirmation screen, verify that:
    - The **New Version** column indicates that you are installing release 6.0 .
    - The **Install Type** column says **Upgrade** for all selected features.

    Note:

    The reinstallation procedure is identical to the upgrade procedure because the installation script will find a previous version of the EPM on the server. The fact that the previous version is the same release as you want to install makes no difference to the installation script.
13. Press `Enter` to move to the next screen.
14. Read through the end user license agreement.
15. On the final End User License Agreement page, type `1` and press `Enter` to select option **1 - I accept the terms of the license agreement**.
    The screen refreshes with **1 - I accept the terms of the license agreement** as the selected option.
16. Press `Enter` to accept the agreement.
17. Press `Enter` to move to the next screen.
    Experience Portal automatically starts the Prerequisite Checker, which analyzes your system's hardware and operating system configuration.

18. After the configuration analysis is complete, the Prerequisite Checker displays a message stating whether all prerequisite checks passed followed by the first Prerequisite Status page. Press `Enter` to view the rest of the Prerequisite Status pages.

    If any prerequisite installations fail, examine the Prerequisite Status pages carefully to determine which checks failed. You must correct these issues before you can continue with this procedure.

19. When all prerequisite checks pass, press `Enter` to move to the next screen. Experience Portal automatically starts the Prerequisite Installer, which attempts to install the required software on the Avaya Aura® Experience Portal server.

20. After the Prerequisite Installer completes installing the required software, it displays a message stating whether all prerequisite installs were successful followed by the first Installation Status page. Press `Enter` to view the rest of the Installation Status pages.

    If any prerequisite installations fail, examine the Installation Status pages carefully to determine which installations failed. You must correct these issues before you can continue with this procedure.

21. When all prerequisites are successfully installed, press `Enter` to move to the next screen.

22. On the Primary EPM Server Location screen, specify the server name or IP address of the EPM server. If you want to:

    - Use the existing EPM server and port number that is displayed in square brackets [ ] after the installation prompt, press `Enter`.
    - If no existing EPM location exists or you want to change the location of the EPM server, type the server name or IP address where the EPM software is installed. If you used a port other than the default EPM port (80), append `:`*`port_number`* to the address. When you are done, press `Enter` to submit the new address.

      For example, to specify the machine with the server name `EPM_Server` on the default port, type `EPM_Server`. To specify the same server on port 86, type `EPM_Server:86`.

    Note:

    The previous releases of the EPM software defaulted to port 8080. If you used the default EPM port in both cases, you need to remove the **:8080** from the existing EPM location.

    The MPP installation uses this information to retrieve the public key from the EPM. The public key provides authentication between the EPM and MPP servers to help secure your Avaya Aura® Experience Portal system.

23. Press `Enter` to move to the next screen.

24. On the Public Key verification screen, perform the following:

If you recorded the fingerprint information from the EPM security certificate during the primary EPM software installation, compare it to the Public Key fingerprint information presented in this screen. The fingerprint information from Public Key should match the fingerprint information from the EPM security certificate. If the public key could not be downloaded, see the topic *Reinstalling the auxiliary EPM software* in the *Administering Avaya Aura Experience Portal* guide.

25. Press `Enter` to move to the next screen.
26. On the Database Login Check for Auxiliary EPM screen, type the password for the user you specified for the auxiliary EPM to access the external Avaya Aura® Experience Portal database user when you installed the EPM software on the primary server and press `Enter`.
27. Press `Enter` to move to the next screen.
    Avaya Aura® Experience Portal makes sure that it can contact the primary EPM server, and that the password you entered matches the one specified when the primary server was installed. If the connection can be established and the password is correct, Avaya Aura® Experience Portal continues to the next screen.
28. On the Database Logins screen, type a password for the postgres user account and press `Enter`.

    The EPM server uses this account to log in to the Avaya Aura® Experience Portal database to store and retrieve data and to install new updates or patches. The database administrator can use this account to log in to the local `VoicePortal` database and perform database administration tasks.
29. To confirm the password, type the password again and press `Enter`.
30. You can create a PostgreSQL database user account on the auxiliary EPM server that can read the report data in the Avaya Aura® Experience Portal database. If you:
    - Want to create the report reader database account:
        1. Type `1` and press `Enter`.
        2. Press `Enter` to confirm your selection.
        3. To display the account name in square brackets ([ ]), press `Enter` at the installation prompt. Otherwise, type a unique user name for the account and press `Enter`.
        4. Type a password for the account and press `Enter`.
        5. Confirm the password by typing it again and pressing `Enter`.
    - Do not want to create the report reader account:
        1. Verify that option **2 - No** is selected. If it is not selected, type 2 and press `Enter`.
        2. Press `Enter` to confirm your selection.

Note:

This user account can only read those tables in the Avaya Aura® Experience Portal database that store report data. You should create this account if you plan to set up an external database on this server that is shared by multiple Avaya Aura® Experience Portal systems and you want to create custom reports for the database using an SQL-enabled report generation tool.

31. Press `Enter` to move to the next screen.
32. You can create a PostgreSQL database user account on the auxiliary EPM server that can allow external systems to write report data into the Avaya Aura® Experience Portal database on this server.

    You should create this account it you plan to set up an external database on this server that is shared by multiple Avaya Aura® Experience Portal systems.

    - If you want to create the report writer database account:

        1. Type `1` and press `Enter`.
        2. Press `Enter` to confirm your selection.
        3. To display the account name in square brackets ([ ]), press `Enter` at the installation prompt. Otherwise, type a unique user name for the account and press `Enter`.
        4. Type a password for the account and press `Enter`.
        5. Confirm the password by typing it again and pressing `Enter`.

    - If you do not want to create the report writer account, press `Enter`.

    Note:

    This user account can only change the data in the tables that store report data in the Experience Portal database on the auxiliary EPM server.

33. Press `Enter` to move to the next screen.
34. Avaya Aura® Experience Portal uses SSL protocol to establish a secure connection between its servers. This connection requires a security certificate that can be created by Avaya Aura® Experience Portal or purchased from a third-party company. On the Security Certificate screen:

    - If you want Avaya Aura® Experience Portal to create a security certificate:

        1. Verify that option **1 - Create a new certificate for this server** is selected. If not, type `1` and press `Enter`.
        2. Press `Enter` to confirm that selection.

    - If you want Avaya Aura® Experience Portal to use a certificate from a company such as VeriSign, you can import the certificate as long as the certificate is in PKCS12 format and the certificate resides on the local server or on a locally accessible NFS-mounted drive. To do so:

1. Verify that option **2 - Import a certificate from a specified location** is selected. If not, type 2 and press `Enter`.
2. Press `Enter` to confirm that selection.
3. Type the full file path and name of the security certificate and press `Enter`.

   The screen displays the location that you entered for your verification.
4. Type the password for the security certificate and press `Enter`.

35. Press `Enter` to move to the next screen.
36. On the Security Certificate Verification screen, verify the security certificate and press `Enter` to move to the next screen.

    Tip:

    When you add the auxiliary EPM to Avaya Aura® Experience Portal through the EPM, the EPM displays the auxiliary EPM's security certificate. You should record the fingerprint information from this security certificate so that you can compare it to the one displayed in the EPM.
37. On the Pre Installation Summary screen, verify the installation information and press `Enter` to install the Avaya Aura® Experience Portal software.
    Avaya Aura® Experience Portal displays the Installation Progress screen and 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. Wait until Avaya Aura® Experience Portal displays the Post Installation Summary screen.
38. On the Post Installation Summary screen, verify that the **Installation Progress Bar** has reached 100% and that the message `...done installing` *`feature_name`* appears for each feature that you selected on the Experience Portal Feature Selection screen.

    Note:

    If the **Installation Progress Bar** on the Installation Progress screen stops at 25% and the Post Installation Summary screen states that no summary information could be found, see Installation Progress Bar stops at 25% completed.
39. Press `Enter` to end the installation script.
    During the installation process, Avaya Aura® Experience Portal creates several log files that you can use to verify what happened during installation. When the installation process is complete, Avaya Aura® Experience Portal moves these logs to the standard log directory and displays the exact path on the screen. For more information, see Installation log files on page 93.
40. To unmount and eject the DVD:

a) Change directories to anything outside the mount point. For example, you could enter the `cd /` command to change to the root directory.
b) Unmount the DVD device as described in your server documentation.
c) To eject the Avaya Aura® Experience Portal installation DVD, press the button on the DVD device or enter the `eject` command.

41. Load the environment variables created during the installation by logging out of Linux and then logging back in as a non-root user. To do so:
    a) Log out the Linux system.
    b) Log back in to Linux by entering a non-root user name and password at the prompts.
    c) Log back in as root or `sroot`. To do so:
        - If you are working with Avaya Enterprise Linux, enter the `su - sroot` command.
        - If you are working with Red Hat Enterprise Linux Server 6.0, enter the `su -` command.
42. Reestablish the link between the primary EPM server and the auxiliary EPM server as described in the *Relinking the primary and auxiliary EPM servers* topic in the *Administering Avaya Aura® Experience Portal* guide.

Reinstalling the Avaya Service Account authentication file

Before you begin

Make sure you have the Avaya Service Account authentication file generated by the Authentication File System (AFS) tool.

Note:

- When running the AFS tool, be sure to select **New System – Product: Avaya Aura Experience Portal Release: 6.x** to generate the AFS file. This step is required for Avaya Aura® Experience Portal fresh install or for upgrade from Voice Portal 5.x to Avaya Aura® Experience Portal 6.0.
- If an AFS file resides in the server prior to upgrade, it needs to be removed manually.

  To delete the existing installed AFS file, execute the following command on the server console: **`rm –f /etc/asg/lacfile`**.

Procedure

1. Log in to Linux on the Voice Portal server.

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

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

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

2. Copy the Avaya Service Account authentication file to the `/tmp` directory on the server.
3. Navigate to the `Support/VP-Tools` directory by entering the `cd $AVAYA_HOME/Support/VP-Tools` command.
4. Enter the `bash AddServiceAccounts` *`authentication_file_path`* command, where *`authentication_file_path`* is the fully-qualified path to the authentication file you copied to the server.
5. Press `Enter` to continue adding Avaya service accounts for this system.
   The following warning message is displayed:

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

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

Note:

This is an informational message and needs no corrective action.

The AddServiceAccounts script changes the following Linux accounts so that you can only log into them using the Avaya Services challenge/response authentication procedure:

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

In addition, the script creates the EPM user account init, which has Administration, Auditor, and User Manager privileges and uses the same Avaya Services challenge/response authentication procedure.

Next steps

The AF ID (Avaya Service Account authentication file ID) on the system must match the information in the Avaya Services database.

Chapter 11: Validating Application Interface web service with Outcall test application

Verifying communication with the Application Interface web service

About this task

Important:

Ensure that Avaya Aura® Experience Portal is configured for the Outcall test application as described in the *Configuring Avaya Aura® Experience Portal for the Outcall test application* topic in the *Implementing Avaya Aura® Experience Portal on multiple servers* guide.

Procedure

1. Log in to Linux on the Voice Portal server.

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

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

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

2. Navigate to the Outcall test application directory by entering the `cd $AVAYA_HOME/Support/OutcallTest/AppIntfWS-Client` command.

3. Enter the `./runclient.sh –n <outcall-username> –p <outcall password>` command to request the number of available outbound ports, where:

   - <outcall-username> is the user name assigned to the outcall user in the **System Configuration > EPM Servers > EPM Settings** page.
   - <outcall password> is the password assigned to the outcall user in the **System Configuration > EPM Servers > EPM Settings** page.

4. Verify that the Outcall test application displays a response that shows the total ports and unused ports available for outcalls.
   Fri Oct 17 15:21:02 PDT 2008: TestClient: queryResources succeeded, TotalRes = 25, UnusedH323 = 15, UnusedSIP = 10

   Fri Oct 17 15:21:02 PDT 2008: TestClient: exiting.

Verifying outcalls and application launching with the Application Interface web service

About this task

Important:

Ensure that Avaya Aura® Experience Portal is configured for the Outcall test application as described in the *Configuring Avaya Aura® Experience Portal for the Outcall test application* topic in the *Implementing Avaya Aura® Experience Portal on multiple servers* guide.

Procedure

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

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.
2. Navigate to the Outcall test application directory by entering the `cd $AVAYA_HOME/Support/OutcallTest/AppIntfWS-Client` command.
3. Enter the `./runclient.sh –R 1 –A <application–name> T <number-to-dial> –n <outcall-username> –p <outcall password>` command to initiate an outcall and launch the Avaya Aura® Experience Portal test application, where:
   - <application–name> is the same test application name as it was entered on the application page.
   - <number-to-dial> is the phone number to place the outcall to.
   - <outcall-username> is the user name assigned to the outcall user in the **System Configuration > EPM Servers > EPM Settings** page.

- <outcall password> is the password assigned to the outcall user in the **System Configuration > EPM Servers > EPM Settings** page.

4. Verify that the dialed phone number rings.
5. Answer the phone and verify that the Avaya Aura® Experience Portal test application is handling the call.

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

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

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

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

Additional Application Interface web service validations with Outcall test application

About this task

Avaya Aura® Experience Portal supports Axis 1.4 and Axis 2.0 web services that provide outcall functionality and the ability to launch CCXML and VXML applications.

Note:
Axis 1.4 uses Digest authentication to authenticate web service client requests while Axis 2.0 uses Basic authentication. This applies to the Application Interface web service as well as the Application Logging web service.

The Outcall test application supports the following parameters which you can use to validate or query the Application Interface web service:

Note:
Use the `VPAppIntfClient <parameter> command.` For example:

- To query the resources: `VPAppIntfClient -S sys-vpms-a1 -R 4`
- To launch a CCXML application: `VPAppIntfClient -S 123.234.12.34 -R 2 -x tel: -C ccxmltest -t 15`
- To initiate an outcall and launch a VXML application: `VPAppIntfClient -S sys-vpms-a1 -R 1 -T 1234 -F 1122 -A test -t 10`

- To launch a CCXML application: `VPAppIntfClient -S 123.234.12.34 -R 2 -x tel: -C ccxmltest -t 15`
- To send an event to a CCXML application: `VPAppIntfClient -S sys-vpms-a1 -R 3 -s sys-mpp-a12-2006286000025-26 -e`

Note:

The Axis 1.4 web service compliant client is available and can be used by executing `runClient` command. The parameters required are the same as described for VPAppIntfClient.

Parameter	Description	Function
-S	server-name	Sets the server-name or IP address where the EPM Application Interface Web Service is running.
-R	request	Sets the request type that will be issued. Using the following definitions: 1 = LaunchVXML, 2 = LaunchCCXML,3 = SendCCXMLEvent, 4 = QueryResources, 5 = GetStatus.
-T	toURI	Sets the toURI value that is used when sending LaunchVXML requests. The default value is "tel:2100". The number can be prefixed with "tel:", "sip:", or "sips" as a suggestion of the type of resource to use.
-F	fromURI	Sets the fromURI value that is used when sending LaunchVXML requests. The default value is "1234567".
-A	applicationName	Sets the application name value that is used when LaunchVXML requests are sent. The default value is "test".
-C	applicationName	Sets the application name value that is used when", LaunchCCXML requests are sent. The default value is "ccxmltest".

Parameter	Description	Function
-U	appURLParams	Sets the application URL parameters that will be used when LaunchVXML or LaunchCCXML requests are sent. The default value is null.
-t	timeout	Sets the timeout value that is used when LaunchVXML or LaunchCCXML requests are sent. The default value is "30" seconds.
-x	hint	Sets the string that is used as a hint for what type of resources are going to be needed by the CCXML application. Values should be "tel:", "sip:", or "sips". The default value is "tel".
-s	sessionId	Sets the session ID string that is used when sending events to a CCXML application using the request SendCCXMLEvent.
-e	eventName	Sets the event name string that is used when sending events to a CCXML application using the request SendCCXMLEvent.
-n.	name	Sets the user name for the authenticated request. The matching value for this parameter must be set as the username for the Outcall Application on the System Config web page. The default value is "outcall"
-p	password	Sets the password for the authenticated request. The matching value for this parameter must be set as the password for the Outcall Application on the System Config web page. The default value is "ocpassword1".

Parameter	Description	Function
-Z	automated	Sets the test into automated mode. The value for this parameter is the number of iterations to perform. The default is 0.
-d	debugLevel	Sets the global debug level for logging output. Valid values are OFF, ERROR, WARN, INFO, and DEBUG
-h		Displays this message and then exits the application
-v		Displays version information and then exits.

Chapter 12: Avaya Aura Experience Portal log files

EPM server logs

The following logs detail EPM server activities:

Database log tables

These logs are stored in the Avaya Aura® Experience Portal database.

Log	Location	Comments
Alarm table	Database	Contains alarm data from EPM and MPPs.
Application log table	Database	Contains Orchestration Designer errors and application specific log data.
Report tables	Database	Contains call and performance report data.
System log table	Database	Contains log data from EPM and MPPs.

EPM PostgreSQL logs

These logs are stored in the `/var/lib/pgsql/data/pg_log/postgresql-`*ddd*`.log` directory, where *ddd* is a three letter abbreviation for the day the log was created.

This log contains log data specific to the PostgreSQL database. It is in ASCII format and can be viewed with any text editor.

EPM logs

These logs are stored in the `$AVAYA_VPMS_HOME/logs/` directory.

Log name	Comments
`avaya.vpms.log`	Contains log data including debug information. Non-debug log entries are copied to the EPM database. All logs are in ASCII format and can be viewed with any text editor.
`avaya.networklogserver.log`	

Tomcat logs

These logs are stored in the `$CATALINA_HOME/logs/` directory. All logs are in ASCII format and can be viewed with any text editor.

Log name	Comments
`catalina.out`	Contains Tomcat-generated log data and console data.
`localhost_log.`*`yyyy-mm-dd`*`.txt`	Contains data from EPM web pages.

Apache/httpd logs

These logs are stored in the `/var/log/httpd` directory.

Log name	Comments
`access_log`	Records all requests processed by the MPP.
`error_log`	Records diagnostic information and any errors the MPP encounters while processing requests. If the MPP does not start or operate properly, you can usually find details about what went wrong in this file and the `ssl_error_log` file.
`ssl_access_log`	Records all requests processed by the MPP.
`ssl_error_log`	Records diagnostic information and any errors the MPP encounters while processing requests. If the MPP does not start or operate properly, you can usually find details about what went wrong in this file and the `error_log` file.
`ssl_request_log`	Records all requests processed by the MPP.

MPP server logs

The following logs are on each Media Processing Platform (MPP) running in the Avaya Aura® Experience Portal system. All logs are in ASCII format and can be viewed with any text editor.

- Apache/httpd logs on page 155
- MPP process logs on page 155

- MPP records logs on page 157
- MPP transcription logs on page 157

Apache/httpd logs

These logs are stored in the `/var/log/httpd` directory.

Log name	Comments
`access_log`	Records all requests processed by the MPP.
`error_log`	Records diagnostic information and any errors the MPP encounters while processing requests. If the MPP does not start or operate properly, you can usually find details about what went wrong in this file and the `ssl_error_log` file.
`ssl_access_log`	Records all requests processed by the MPP.
`ssl_error_log`	Records diagnostic information and any errors the MPP encounters while processing requests. If the MPP does not start or operate properly, you can usually find details about what went wrong in this file and the `error_log` file.
`ssl_request_log`	Records all requests processed by the MPP.
`ws_access_log`	Records all requests for Avaya Aura® Experience Portal Web services.
`ws_error_log`	Records information concerning the MPP Web Services MMS, CdhService, and TransService, including errors when these services process requests. If the EPM cannot contact the MPP, look in this file first.

MPP process logs

The process logs contain event and trace messages from the MPP subsystems. By default, they are stored in subdirectories under the `$AVAYA_MPP_HOME/logs/process/` directory, and they are accessible from the Log Directories page of the MPP Service Menu.

Note:

The maximum size for each log and the number of logs to retain is set in the **Trace Logger** group of the MPP Settings page.

Directory name	Log name	Comments
`Administration`	`mppmaint.log`	This file records the actions of the `mppmaint` process, which runs daily to purge the MPP of outdated Call Detail Record (CDR), Session Detail Record (SDR), and session transcription records.

Directory name	Log name	Comments
CXI	CCXML-global-*x*.log	This file contains data related to events that are not specifically associated with a CCXML single session. If there is more than one CXI process, the *x* represents the number of processes.
	CCXML-SessionSlot-###.log, where ### represents the unique log identifier.	This file contains data related to CCXML operations for individual sessions. The unique identifier can be used to find related Session Manager and Avaya Voice Browser logs.
CdhService	CDHService.log	These files record the actions of the CDHService Web Service, which enables the EPM to download CDR and SDR records from the MPP.
ServiceMenu	ServiceMenu.log	This file records the actions of the Service Menu process.
EventMgr	EventMgr.log	This file records the actions of the Event Manager, which collects events from other MPP processes and sends them to the network log web service on the EPM.
MMS	MmsServer.log	This file contains messages from the MMS Web Service, which is accessed by the EPM to send commands, configuration changes, and heartbeat requests the MPP.
OCWSServer	OCWSServer.log	This file contains messages produced by Application Logging web service, which is used to make outbound calls on the MPP.
SessMgr	SessionManager.log	This file contains data related to events that are not specifically associated with a single session.
	SessionSlot-###.log, where ### represents a unique log identifier	This file contains data related to Session Manager operations for individual sessions.
SysMgr	logfile.log	This file records messages produced by the System Manager process.
TransService	transervice.log	This file contains messages from the TransService Web Service, which is accessed by the EPM to download transcription and utterance files from the MPP for inclusion in the Session Detail report.

Directory name	Log name	Comments
VB	`globalx.log`	This file contains data related to events that are not specifically associated with a single session. If there is more than one AVB process, the *x* represents the number of processes.
	`SessionSlot-###.log`, where *###* represents a unique log identifier	This file contains data related to AVB operations for individual sessions.

MPP records logs

The record logs contain Call Detail Records (CDRs) and Session Detail Records (SDRs). All data is sent to the EPM. These logs are stored in the `$AVAYA_MPP_HOME/logs/records/` directory, and the log names are:

- `<name>_cdr_<#>_<date>.bin`
- `<name>_sdr_<#>_<date>.bin`

MPP transcription logs

These logs contain session transcription data.

You can access these log files by creating a Session Detail report through the EPM. For more information, see Checking the call session on page 21 and the *Creating a Session Detail report* topic in the *Administering Avaya Aura® Experience Portal* guide.

The transcriptions are stored in the `$AVAYA_MPP_HOME/logs/<yyyy>/<mm>/<dd>/transcriptions/` directory.

If utterances are saved for an application, they are stored in the `$AVAYA_MPP_HOME/logs/transcriptions/<yyyy>/<mm>/<dd>/utterances/<session-id>` directory.

Related topics:

Moving the MPP logs to a different location on page 157
Packing MPP logs and transcriptions in a TAR file on page 159
Packing MPP logs and transcriptions using getmpplogs.sh on page 160
Restoring packed MPP log files on page 162

Moving the MPP logs to a different location

About this task

If you need to free up space on an MPP server, you can use the `mppMoveLogs.sh` script to create a new directory and move the MPP logs to that directory.

Procedure

1. If necessary, install the target drive or create the target partition as described in your operating system documentation.

   Important:

   Do *not* create the new directory on this drive or partition, as the script will fail if a directory already exists.

   The drive or partition must be local to the MPP server and it must contain either 2 GB of free space or as large in size as the current `$AVAYA_MPP_HOME/logs` directory, whichever value is greater.

   Tip:

   For a good tutorial about creating a partition, see http://tldp.org/HOWTO/html_single/Partition/.

2. If you created a new partition, add an entry for the partition in the `/etc/fstab` file so that it is automatically mounted when the system is booted.

   If the partition for the directory will only host the Avaya Aura® Experience Portal log directory, you can improve security by setting its properties in the `/etc/fstab` file to `rw,nosuid,noexec,auto,nouser,async,noatime,nodev`. For more information about these options, see http://www.faqs.org/docs/securing/chap5sec45.html.

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

4. Stop the MPP whose logs you want to move:

   a) From the EPM main menu, select **System Configuration** > **MPP Server**.
   b) On the MPP Servers page, click the Selection check box next to the name of the MPP you want to stop.
   c) Click **Stop** in the **State Commands** group
   d) Confirm the action when requested.
   e) Wait until the operational state becomes Stopped. To check this, click **Refresh** and look at the **State** field.

      Note:

      The operational state changes when the last active call completes or the grace period expires, whichever comes first.

5. Log in to Linux on the Experience Portal MPP server.

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

   - Log in to the local Linux console as sroot.

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

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

6. Enter the `bash mppMoveLogs.sh [-logdir directory_name]` command, where `-logdir directory_name` is an optional parameter specifying the directory name that you want to use.

   If you do not specify this parameter on the command line, the script prompts you for the directory name during execution. If the directory you specify already exists, the script returns an error message and fails. This ensures that no existing files will be overwritten by the script.

   When the script completes successfully, all of the current logs will reside in the new location, and all future logs will be stored in the new location.

7. Restart the MPP:

   a) From the EPM main menu, select **System Configuration** > **MPP Server**.
   b) On the MPP Servers page, click the Selection check box next to the name of the MPP you want to start.
   c) Click **Start** in the **State Commands** group
   d) Wait until the operational state becomes Running. To check this, click **Refresh** and look at the **State** field.

Packing MPP logs and transcriptions in a TAR file

About this task

You can use the Diagnostics in the MPP Service Menu to pack the logs, transcriptions, and debug files into a single TAR file for further diagnostics and troubleshooting.

Note:

You can use the `getmpplogs.sh` script to customize which files are packed.

Procedure

1. Log into the MPP Service Menu.
2. From the MPP Service Menu, select **Diagnostics**.
3. On the Diagnostics page, click **Pack Files**.
4. On the Pack Files Options page, select the files you want to pack. You can select any or all of the following:

- Select all check box: Pack all available files.
- **Logs**: Pack all the MPP log files.
- **Transcriptions and utterances**: Pack all the transcriptions and utterances saved by the applications running on the MPP.
- **Debug files**: Pack all the debug (trace) data recorded on the MPP.

5. Click **Pack**.
   Avaya Aura® Experience Portal creates a TAR file with the format `<hostname>_<date and time stamp>_MPP.tar` that contains all of the selected information. In addition, Avaya Aura® Experience Portal creates a TAR file for each MPP component with the format `<MPP component>_<hostname>_<date and time stamp>_MPP.tar`.

   Avaya Aura® Experience Portal displays the TAR file names at the bottom of the page.
6. To save any TAR file, right-click the file name and select **Save As** from the pop-up menu.

Next steps

If you need to restore the packed log files, use the `restorempplogs.sh` script.

Packing MPP logs and transcriptions using getmpplogs.sh

The `getmpplogs.sh` script packs system information files, logs, and transcriptions into one TAR file.

About this task

Note:
You can also pack the log files from the Diagnostics page in the MPP Service Menu.

Procedure

1. Log in to Linux on the Experience Portal MPP server.
   If you are an Avaya Services representative, and are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:
   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.

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

Note:

You can run this script as an avayagroup member, but if you run this script while logged in as `root` or sroot, it collects additional log files.

2. Navigate to the MPP `bin` directory by entering the `cd $AVAYA_MPP_HOME/bin` command.
3. Enter the `getmpplogs.sh` command with the desired options. You can select:

Option	Purpose
--web	To export a TAR file from the `$AVAYA_MPP_HOME/web/admin/AEPSupport` directory that can be accessed from the web browser. If this command option is not used, the TAR file can be found in the `$AVAYA_MPP_HOME/tmp/AEPSupport/` directory.
--logs	To export system information and MPP logs, Apache logs, and system event logs. The system information exported is: • hostname • system uptime • system CPU and memory information • network configuration • storage usage • `/etc/hosts` file • currently running processes • CPU activity information • RPM database information • MPP specific configuration
--transcriptions	To export system information and all the transcriptions and utterances.
--debugfiles	To export only the system information and all the latest core files from each MPP component with libraries and debug symbols.
--help	To display the above `getmpplogs.sh` commands. **Note:** This parameter cannot be combined with any other parameters.

Except for the --help option, you can specify any combination of parameters when you run the `getmpplogs.sh` script. The types of files that are packed in the TAR file depends on the combination of the command options that you use.

For example, to pack all transcriptions, system information, and debug files in a TAR file stored in the `$AVAYA_MPP_HOME/web/admin/AEPSupport` directory, enter the `getmpplogs.sh --web --transcriptions --debugfiles` command.

Next steps

If you need to restore the packed log files, use the `restoreempplogs.sh` script.

Restoring packed MPP log files

About this task

You can use the `restoreempplogs.sh` script to restore the MPP log files that were packed using either the `getmpplogs.sh` script or the Pack Files Options page available from the MPP Service Menu.

The `restoreempplogs.sh` script:

- Stops the MPP service
- Restores the call data records
- Restores the installation logs
- Restores the process logs, if available
- Restores the transcriptions and utterances, if available
- Restarts the MPP service

Procedure

1. If the MPP was started through the EPM:
   a) Log in to the EPM Web interface using an account with the Administration or Operations user role.
   b) From the EPM main menu, select **System Management** > **MPP Manager**.
   c) On the MPP Manager page, use the Selection check box in the MPP server table to select which MPPs you want to change.
   d) Click **Stop** in the **State Commands** group.
   e) After the grace period expires, click **Refresh** to ensure that the state is now **Stopped**.
2. Log in to Linux on the Experience Portal MPP server.

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

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

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

3. Restore the log files by entering the `bash restorempplogs.sh <path/file.tar>` command, where <*path/file.tar*> is the fully qualified path and file name of the TAR file created by the **Pack** command or the `getmpplogs.sh` script.

   If the script finds the TAR file, it displays the following:

   ```
   This utility will restore records of type: Records Installation logs
   Process logs Transcriptions & Utterances from a tar file generated by the
   getmpplogs script. If the directories for these records already exist, then
   the directory will be renamed to <directory-YYYYMMDD-HHMM> before the
   restore. Press Enter to continue, or press Control-c to cancel
   ```

4. Press `Enter` to run the script and restore the log files. The script produces output similar to the following:

   ```
   Extracting files from '/opt/Avaya/ExperiencePortal/MPP/tmp/AEPSupport/cl-
   mpplab-02_Apr_24_2007_14_12_17_MPP.tar.gz'... Depending on the amount of
   data, this may take several minutes. Stopping services... Checking service
   'mpp' - stopping: 'mpp' - Restoring 'Records' Moving existing '/opt/Avaya/
   ExperiencePortal/MPP/logs/records' to '/opt/Avaya/ExperiencePortal/MPP/
   logs/records-20070424-1419'... Restoring '/tmp/untar/logs/records' to '/
   opt/Avaya/ExperiencePortal/MPP/logs/records'... Restoring directory and
   file permissions... - Restoring 'Installation logs' Moving existing '/opt/
   Avaya/ExperiencePortal/MPP/logs/install' to '/opt/Avaya/ExperiencePortal/
   MPP/logs/install-20070424-1419'... Restoring '/tmp/untar/logs/install' to
   '/opt/Avaya/ExperiencePortal/MPP/logs/install'... Restoring directory and
   file permissions... - Restoring 'Process logs' Moving existing '/opt/
   Avaya/ExperiencePortal/MPP/logs/process' to '/opt/Avaya/ExperiencePortal/
   MPP/logs/process-20070424-1419'... Restoring '/tmp/untar/logs/process' to
   '/opt/Avaya/ExperiencePortal/MPP/logs/process'... Restoring directory and
   file permissions... - Restoring 'Transcriptions & Utterances' Moving
   existing '/opt/Avaya/ExperiencePortal/MPP/logs/transcriptions' to '/opt/
   Avaya/ExperiencePortal/MPP/logs/transcriptions-20070424-1419'...
   Restoring '/tmp/untar/transcriptions' to '/opt/Avaya/ExperiencePortal/MPP/
   logs/transcriptions'... Restoring directory and file permissions... Log
   Restoration Complete! INFO: The service 'mpp' will not be automatically
   restarted by this script. If you wish to restart this service, use the
   command: /sbin/service mpp start
   ```

5. If the hostname of the current machine is different than the hostname stored in the log files, the `restorempplogs.sh` script displays a warning message alerting you that the names of the log files in the `$AVAYA_MPP_HOME/logs/records` and `$AVAYA_MPP_HOME/logs/transcription` directories need to be changed so that the hostname included in the filename matches the server's new hostname.

   When you rename these files:

   - Use the short name for the server instead of the fully qualified domain name.

- Make sure that the hostname you specify matches the exact server hostname, including case.

Note:

If you do not change the log file names, then these records will not be accessible to the EPM server and therefore will not be accessible to any reports created through the EPM.

Application server logs

Application server logs are available only when you use Orchestration Designer to create the speech application and are running it in a Tomcat environment.

All application server logs are in ASCII format. You can view them in any text editor.

Application server servlet container logs

The logs contain log data from the servlet container. You can find these log files in the following locations:

- *$CATALINA_HOME*/logs/catalina.out
- *$CATALINA_HOME*/logs/localhost_log.*date*.txt

For more information on setting the number of application server failover logs in the EPM settings, see the*EPM Settings and View EPM Settings Page field descriptions* topic in the *Administering Avaya Aura® Experience Portal* guide.

Note:

If you install or upgrade Avaya Aura® Experience Portal and this log already exists, Avaya Aura® Experience Portal automatically renames the existing file as catalina.*nnn*, where *nnn* is a unique sequential identifier starting with 000. It then creates a new version of catalina.out and writes all log entries from the current installation forward into that file.

Orchestration Designer errors and application reports log

This log file only exists if Orchestration Designer cannot write data to the EPM when its session ends. The next time Orchestration Designer ends, it again tries to write its log data to the EPM, so the information in this log is eventually transferred to the EPM.

You can find this log file in the following location: *$CATALINA_HOME*/webapps/*app_name*/data/logs/savereport.log

Note:

If application reporting is disabled, no data is logged. Otherwise, all report data is sent to the EPM.

Orchestration Designer trace log

If the query string includes`ddtrace=true`, this log contains application specific trace data.

You can find this log file in the following location: *`$CATALINA_HOME/`*`logs.log`

You can change the location, format, and contents of this log, in the `webapps/`*`app_name`*`/data/ddlog4j.properties` file.

Third party logs for ASR and TTS servers

The following third party logs contain vendor specific data for the Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) servers.

ASR, TTS, and NSS Server Logs for Nuance

These logs are available in the following locations for Linux and Windows:

- **Linux**: `/usr/local/Nuance/Speech_Server/server/logs`
- **Windows**: `C:\Program Files\Nuance\Speech Server\Server\logs`

  You can use these paths for ASR, TTS and NSS servers. For more information about interpreting the log files, see your Nuance documentation.

LSS, ASR, and TTS Server Logs for Loquendo

These logs are available in the following locations for Linux and Windows:

- **Linux**: You can use the following path for:
  - LSS: `/var/opt/Loquendo/Platform/logs`
  - ASR: `/var/opt/Loquendo/Platform/logs/LASR`
  - TTS: `/var/opt/Loquendo/Platform/logs/LTTS`
- **Windows**: You can use the following path for:
  - LSS: `C:\Documents and Settings\Administrator\Application Data\Loquendo\Platform`
  - ASR: `C:\Program Files\Loquendo\LTTS7\logs`
  - TTS: `C:\Program Files\Loquendo\LTTS7\logs`

Installation log files

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

Avaya Aura® Experience Portal creates several log files during the installation process. If the installation process:

- Completes successfully, Avaya Aura® Experience Portal copies the log files to `$AVAYA_HOME/logs/install_`*`date`*, where `$AVAYA_HOME` is the environment variable pointing to the installation path you specified on the Installation Destination installation screen and *`date`* is the date the installation process was run. The default installation directory is `/opt/Avaya/ExperiencePortal`.
- Does not complete successfully, Avaya Aura® Experience Portal copies the log files to `/opt/_Avaya_Voice-Portal_temp`.

General installation log files

Log filename	Description
`VP_Install.log`	Main log containing output from all EPM and MPP installation processes. This is the first log file you should consult if you need to troubleshoot an installation issue.
`ISOpt.log`	InstallShield generated log containing internal data.
`installSequence.log`	Subset of ISOpt.log
`prereqchecker.log`	Detailed information from the Prerequisite Checker.
`prereqchecker.out.log`	Results from the Prerequisite Checker.
`prereqchecker.err.log`	Any internal errors encountered by the Prerequisite Checker.
`prereqinstaller.log`	Detailed information from the Prerequisite Installer.
`prereqinstaller.out.log`	Results from the Prerequisite Installer.
`prereqinstaller.err.log`	Any internal errors encountered by the Prerequisite Installer.
`SetIAVersion<component>.log`	Version history of the Avaya Aura® Experience Portal components installed. The component can be the EPM, MPP or Docs.

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.
mpp.cert.gen.out.log	Results from the security certificate generation process.
mpp.cert.gen.err.log	Any internal errors generated from the certificate generation process.
mpp.cert.imp.out.log	Results from the security certificate import process.
mpp.cert.imp.err.log	Any internal errors generated from the certificate import process.
mpp.key.import.out.log	Results from the public key import process from the EPM.
mpp.key.import.err.log	Any internal errors generated from the public key import process from the EPM.

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.
vpms.cert.imp.out.log	Results from the security certificate import process.
vpms.cert.imp.err.log	Any internal errors generated from the certificate import process.

Upgrade installation log files

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

Avaya Aura® Experience Portal creates log files during the upgrade process. If the upgrade process:

- Completes successfully, Avaya Aura® Experience Portal copies the log files to `$AVAYA_HOME/logs/install_`*`date`*, where `$AVAYA_HOME` is the environment variable pointing to the installation path you specified on the Installation Destination installation screen and *`date`* is the date the installation process was run. The default installation directory is `/opt/Avaya/VoicePortal`.
- Does not complete successfully, Avaya Aura® Experience Portal copies the log files to `/opt/_Avaya_Voice-Portal_temp`.

General installation log files

Log filename	Description
`EP_Install.log`	Main log containing output from all EPM and MPP installation processes. This is the first log file you should consult if you need to troubleshoot an installation issue.
`ISLog.log`	InstallShield generated log containing internal data.
`ISOpt.log`	InstallShield generated log containing internal data.
`installSequence.log`	Subset of ISLog.log
`prereqchecker.log`	Detailed information from the Prerequisite Checker.
`prereqchecker.out.log`	Results from the Prerequisite Checker.
`prereqchecker.err.log`	Any internal errors encountered by the Prerequisite Checker.
`prereqinstaller.log`	Detailed information from the Prerequisite Installer.
`prereqinstaller.out.log`	Results from the Prerequisite Installer.
`prereqinstaller.err.log`	Any internal errors encountered by the Prerequisite Installer.
`SetIAVersion<component>.log`	Version history of the Avaya Aura® Experience Portal components installed. The component can be the EPM, MPP or Docs.

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.
mpp.cert.gen.out.log	Results from the security certificate generation process.
mpp.cert.gen.err.log	Any internal errors generated from the certificate generation process.
mpp.cert.imp.out.log	Results from the security certificate import process.
mpp.cert.imp.err.log	Any internal errors generated from the certificate import process.
mpp.key.import.out.log	Results from the public key import process from the EPM.
mpp.key.import.err.log	Any internal errors generated from the public key import process from the EPM.

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.
vpms.cert.imp.out.log	Results from the security certificate import process.
vpms.cert.imp.err.log	Any internal errors generated from the certificate import process.

Index

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X