Troubleshooting Avaya Aura® System Manager

Release 10.2.x
Issue 4
April 2026

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

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

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

© 2013-2026, Avaya LLC
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for troubleshooting errors for Avaya Aura® System Manager and Avaya Aura® applications that System Manager supports.

This document is intended for people who perform troubleshooting tasks.

Change history

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

Issue	Date	Summary of changes
4	April 2026	Added the following section: • CSRF error in SAML Authentication flow on page 37
3	January 2025	Updated Troubleshooting Appliance Virtualization Platform on page 8.
2	December 2024	Added following section for Release 10.2.1: Identifying Communication Manager when you run a sychronization on page 41.
1	December 2023	Initial issue of Release 10.2 document.

Chapter 2: Solution Deployment Manager and Appliance Virtualization Platform errors

Troubleshooting Appliance Virtualization Platform

Appliance Virtualization Platform does not install

Perform the following as appropriate:

- Ensure you are connected to the services port on the server with the following network configuration on the laptop:
  - IP address: 192.11.13.6
  - Netmask: 255.255.255.248
  - Gateway: 192.168.13.1
- Defective USB drive. Place the `avp81ks.cfg` kickstart file on another USB, and connect the USB to the server.
- Unsupported server: Release 7.1 and later does not support S8500 and S8800 servers. Change to a Release 10.2.x supported server. For more information about supported server, see .Supported servers section in *Upgrading Avaya Aura® Appliance Virtualization Platform* document.
- Duplicate IP address for Appliance Virtualization Platform management interface already on the network. Remove the duplicate IP address, and reinstall Appliance Virtualization Platform.
- USB stick left plugged in on HP servers. Remove the USB stick, and reboot the server.
- Deployments take longer duration or fail. Ensure the network settings and network configuration is correct for the virtual machine being deployed.

Virtual machine deployment fails during the sanity check

- Ensure IP forwarding is enabled on AVP Utilities while deploying virtual machines from the services port with the Solution Deployment Manager client.
- Ensure System Manager Solution Deployment Manager or Solution Deployment Manager client can connect to the management IP address of the application being deployed.
- Ensure the server is physically connected. If Out of Band Management is enabled, ensure the Appliance Virtualization Platform host and the virtual machines are deployed with Out of Band Management configurations.

Virtual machine deployment fails

Ensure you accept EULA by gaining access to Appliance Virtualization Platform using SSH, and accepting the EULA.

Cannot SSH to Appliance Virtualization Platform

SSH has shutdown. Activate SSH from AVP Utilities or from Solution Deployment Manager. For more information, see Activating SSH from AVP Utilities.

On the monitor, the screen displays a warning message in red and then goes blank

During the Appliance Virtualization Platform installation, the monitor displays a blank screen, which is a normal behavior. No action is required.

Related links

Activating SSH from AVP Utilities on page 9
Enabling IP forwarding using Services Port VM for AVP Utilities on page 10

Activating SSH from AVP Utilities

About this task

For security purpose, SSH access to Appliance Virtualization Platform shuts down in the normal operation. You must activate SSH on Appliance Virtualization Platform.

When you install or preinstall Appliance Virtualization Platform on a server, SSH is enabled. After you accept the license terms during Appliance Virtualization Platform installation, SSH shuts down within 24 hours. After SSH shuts down, you must reactivate SSH by using the **`AVP_SSH enable`** command from AVP Utilities.

Before you begin

Start an SSH session.

Procedure

1. Log in to the AVP Utilities virtual machine running on Appliance Virtualization Platform with administrator privilege credentials.
2. Type the following:

   ```
   AVP_SSH enable
   ```

   Within 3 minutes, the SSH service starts on the Appliance Virtualization Platform, and runs for two hours from AVP Utilities. After two hours, you must reactivate SSH from AVP Utilities.

   When SSH is enabled, you can use an SSH client, such as PuTTY, to gain access to Appliance Virtualization Platform on customer management IP address or the services port IP address of 192.168.13.6.
3. **(Optional)** To find the status of SSH, type `AVP_SSH status`.
4. To disable SSH, type `AVP_SSH disable`.

Related links

Troubleshooting Appliance Virtualization Platform on page 8

Enabling IP forwarding using Services Port VM for AVP Utilities

About this task

IP Forwarding is always disabled after an installation, regardless of the mode of deployment. Use the following procedure to enable IP Forwarding.

Note:

For security reasons, you must always disable IP forwarding after finishing your task.

Procedure

1. Start an SSH session.
2. Log in to AVP Utilities as admin.
3. In the command line, perform one of the following:
   - To enable IP forwarding, type `IP_Forward enable`.
   - To disable IP forwarding, type `IP_Forward disable`.
   - To view the status of IP forwarding, type `IP_Forward status`.

Example

```
IP_Forward enable
Enabling IP Forwarding
Looking for net.ipv4.ip_forward in /etc/sysctl.conf
Status of IP Forwarding
..Enabled
```

Related links

Troubleshooting Appliance Virtualization Platform on page 8

Unable to add a host in Solution Deployment Manager

Unable to add an ESXi host in Solution Deployment Manager

If you are unable to add an ESXi host in Solution Deployment Manager, check for the following:

Solution

- Ensure FQDN of ESXi host is properly configured with a short hostname and domain name.
- Ensure the ESXi host certificate is valid.
- If host is added in Solution Deployment Manager using FQDN, ensure FQDN is reachable and is a part of the certificate SAN.
- If FQDN is not reachable, add that entry in DNS or in the `/etc/hosts` file of System Manager.

When using Solution Deployment Manager Client, add the entry in `C:\Windows\System32\drivers\etc\hosts`.

- If FQDN is not present in SAN, regenerate the ESXi host certificate.

  For information about regenerating certificate, see the VMware documentation.

- If host is added in Solution Deployment Manager using IP Address, ensure the IP Address is reachable and is a part of the certificate SAN.

Unable to add an Appliance Virtualization Platform host in Solution Deployment Manager

If you are unable to add an Appliance Virtualization Platform host in Solution Deployment Manager, check for the following:

Solution

- Ensure Appliance Virtualization Platform is installed using Kickstart config file.
- Ensure Appliance Virtualization Platform hostname is fully qualified.
- Ensure the IP or FQDN that is used to add Appliance Virtualization Platform in Solution Deployment Manager is reachable.
- Do not check certificate for Appliance Virtualization Platform as Solution Deployment Manager regenerates the certificate, if it is not as per standards.

Unable to connect to Appliance Virtualization Platform host from vSphere Web Client

Condition

The vSphere Web Client throws an SSL verification failure error when you gain access to the Appliance Virtualization Platform host for which you regenerated the certificate.

Cause

The vSphere Web Client might use the old certificate of the Appliance Virtualization Platform host from the cache instead of the regenerated certificate.

Use the following procedure if the system displays an SSL verification error when you gain access to the Appliance Virtualization Platform host from vSphere Web Client.

Solution

1. Restart the Appliance Virtualization Platform host.
2. Using vSphere Web Client, gain access to the Appliance Virtualization Platform host.

Related links

Restarting Appliance Virtualization Platform or an ESXi host on page 12

Restarting Appliance Virtualization Platform or an ESXi host

About this task

The restart operation fails, if you restart the host on which System Manager itself is running. If you want to restart the host, you can do this either through vSphere Web Client or through the Solution Deployment Manager client.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
4. Click **More Actions** > **Lifecycle Action** > **Host Restart**.
5. On the confirmation dialog box, click **Yes**.

   The system restarts the host and virtual machines running on the host.

Related links

Unable to connect to Appliance Virtualization Platform host from vSphere Web Client on page 11

The Solution Deployment Manager client installation fails

Cause

Port 443 that is required to install the Solution Deployment Manager client installation and use the Solution Deployment Manager functionality is busy.

Applications such as, Skype use port 443. You must release the port, and configure Skype to use a different port.

Solution

1. To stop the Skype application, click **Quit Skype**.
2. To configure Skype to use a different port, on the Skype interface, do the following:
   a. Click **Tools** > **Connections options**.
   b. Clear the **Use port 80 and 443 for additional incoming connections** check box.
   c. In the left pane, click the **Connections** tab.
   d. In **Use port for incoming connections** field, provide a different port number.
   e. Click **Save**.

Uninstalling the Solution Deployment Manager client manually

About this task

Use the procedure to uninstall the client manually, if you are unable to remove the client by using Add/Remove Programs, Uninstall. or change a program from `Control Panel\Programs\Programs and Features`.

Uninstall the Solution Deployment Manager client before you install a new version of the client on your computer.

Procedure

1. In the Run window, type `services.msc`, and stop the Solution Deployment Manager service.

   If the Solution Deployment Manager service does not stop properly, reboot the machine.

2. At the windows command prompt, log in as administrator, and type `sc delete sdm` to delete the Solution Deployment Manager service.

3. Delete the following registry entry:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Avaya\SDMClient
   ```

4. Delete the Solution Deployment Manager client installation directory and the content in the directory.

   If the client is installed at the default location, then delete `C:\Program Files\Avaya\AvayaSDMClient`.

5. Delete the Solution Deployment Manager client shortcut from the `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Avaya\AvayaSDMClient` location and the desktop.

Virtual machine deployment fails on Solution Deployment Manager

Error and Cause

The system can display one of the following errors.

#	Error	Cause
1	`Error Code-HTTNFCLEASE_ERROR_STATE:: HTTPNFC is in error state. Cannot Create VM. Cannot complete the operation because the file or folder [server-local-disk] vmname/ vmname.vmdk already exists null`	This error occurs if some residue files are already present on the virtual machine.
2	`Create VM task failed with Exception com.vmware.vim25.RestrictedVersion`	This error occurs if write permissions are not present.

Error 1: Solution

Redeploy the virtual machine.

Error 2: Solution

Ensure the standard license is installed on the ESXi host.

Reestablish connection fails for the virtual machine on Solution Deployment Manager

Error and Cause

Error	Cause
`"Get Trust Status" failed.`	This error occurs if: • IP Address is not present in the **Application IP** column in the **Applications** tab of the Application Management page on Solution Deployment Manager. • Incorrect IP Address is present in the **Application IP** column in the **Applications** tab of the **Application Management** page on Solution Deployment Manager.

Solution

1. Perform one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
   - On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. To populate the IP address, refresh the virtual machine host. On the **Platforms** tab, select the host and click **Refresh**.

   The system displays the IP Address in the **Application IP** column on the **Applications** tab.

   If the IP Address is not displayed, proceed to the next step.

4. Ensure the VMware tools are installed and running.

Unable to establish trust with virtual machine

Cause

Solution Deployment Manager might not be able to establish trust, if the:

- Virtual machine has been moved from one datastore to another.
- Datastore name is changed.

Solution

1. Open AVP/ESXi hosting the virtual machine using VMware Web Console or vSphere Client.
2. Select the Virtual Machine and click **Edit**.

   Virtual Machine must be in powered on state.

   The system displays the Edit Settings or Virtual Machine Properties page.
3. Click **CD/DVD Drive 1** or **CD/DVD Drive 2**. Check if any iso path is attached, and do one of the following:
   - If the iso path does not exist or if the datastore mentioned is older, then remove the complete path from the text box, and select **Client Device**. If the option is not available, select **Host Device**.
   - If the iso path is attached, remove the iso, and select **Client Device**. If the option is not available, select **Host Device**.
4. Click **Save**.
5. Perform Trust Establishment.

Virtual machine operations are not functional

Cause

Virtual machine name has special characters, such as, Percent(%), Forward-Slash(/), and Backward-Slash(\).

Solution

1. Rename the virtual machine using vSphere Web client.
2. After renaming the virtual machine, refresh the virtual machine host. To refresh, on the **Platforms** tab, select the platform and click **Refresh**.

   After platform refresh, retry the virtual machine operation.

Virtual machine refresh or re-establish trust fails on Solution Deployment Manager

Error and Cause

The system can display one of the following errors.

#	Error	Cause
1	`Error Occured while file transfer`	This error occurs if ovf_file is not present.
2	`SMGR_VM_1008 - Plugin execution exited with Error Invalid VM IP address`	

Error 1: Solution

1. Log in to the virtual machine.
2. Go to `/opt/avaya/common_services`, verify that ovf_file is present.

   This file is required to perform further operations on Solution Deployment Manager. If the file is not present, contact Avaya Support website at http://support.avaya.com/.

Error 2: Solution

1. Perform one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
   - On the desktop, click the SDM icon (), and then click **Application Management**.
2. In **Application Management Tree**, select a location.
3. To populate the IP address, refresh the virtual machine host. On the **Platforms** tab, select the host and click **Refresh**.

   The system displays the IP Address in the **Application IP** column on the **Applications** tab.

   If the IP Address is not displayed, proceed to the next step.
4. Ensure the VMware tools are installed and running.

Appliance Virtualization Platform patch installation fails

Error

`Patch failed in "Verify AVP State".`

Solution

Perform one of the following:

- If Appliance Virtualization Platform is accessible, refresh the Appliance Virtualization Platform host and verify if the Appliance Virtualization Platform version is updated.
- If Appliance Virtualization Platform is not accessible, do one of the following:
  - Wait for 10-15 minutes and check the Appliance Virtualization Platform again.
  - Access the Direct Console. To do this, connect the monitor to the server directly and check for any error on the console.

SSL verification error for Appliance Virtualization Platform

When you gain access to the Appliance Virtualization Platform host from the VMware Embedded Host Client, the system might display an SSL verification error.

Solution

If the system displays an SSL verification error, accept the new certificate on the browser.

Chapter 3: Launching errors

System Manager Web Console fails to open

Symptoms that identify the issue	System Manager web console fails to open and does not display any error.
Cause of the issue	If you log in to System Manager from the web console when the CND service is not running, the login page fails to open and displays an error message.

Proposed solution

Procedure

1. To start the CND service, enter `service cnd start`.
2. To start the JBoss service, enter `service jboss start`.

Tip:

If you run the **`init 6`** command, the system starts all services including CND.

Unable to gain access to the Web console of the secondary System Manager

Symptoms that identify the issue	The system denies access to the web console of the secondary server after changing IPFQDN on the primary System Manager server.
Cause of the issue	The system denies access to the secondary System Manager server when you perform the following steps: 1. Log on to the primary System Manager and complete the following: a. Convert the primary System Manager to standalone.

For all Geographic Redundancy related procedures, see the Geographic Redundancy section in *Administering Avaya Aura® System Manager*.

b. Change the IPFQDN.

2. Install the System Manager OVA on the standalone server that you designate as the secondary System Manager.
3. Configure Geographic Redundancy.
4. On the primary System Manager, enable Geographic Redundancy replication.
5. Log on to System Manager web console of the secondary System Manager.

   The system denies access to the web console of the secondary System Manager server.

Proposed solution

Procedure

1. Start an SSH session.
2. On the secondary System Manager server, open the command prompt.
3. Run the following command:

   ```
   sh $MGMT_HOME/CommonConsole/fixSecondaryDashboardIssue.sh
   ```

   The system displays the web console of the secondary System Manager server.

Unlocking System Manager CLI user login account

Condition

Before Release 10.1.0.2, when a user logs into the CLI and types an incorrect password for three consecutive times, the user account gets locked. However, the user account unlocks automatically after a specific period of time.

From Release 10.1.0.2, if a user logs into the CLI and the user account gets locked, the user account does not unlock automatically.

Solution

1. Log in to System Manager CLI as root.
2. Run the following command:

   ```
   faillock --dir /var/log/faillock --user cust_user --reset
   ```

System Manager unlocks the user account.

Chapter 4: Geographic Redundancy related errors

Geographic Redundancy configuration and reconfiguration operations fail

Configuration and reconfiguration of Geographic Redundancy operations performed from the secondary System Manager server fail.

Related links

Proposed solution on page 21

Proposed solution

About this task

When you configure or reconfigure Geographic Redundancy using the user password of the primary System Manager server, the operation fails if the password includes an ampersand (&).

Procedure

Log on to the primary System Manager server, and change the user password to remove the & character.

This limitation applies only for configuring or reconfiguring Geographic Redundancy operations. Therefore, perform the step only when the primary System Manager user that is used to perform one of these operations contains an & character in the password. After the operation is complete, you can change the password again to include & character.

Logon to System Manager web console fails

The primary System Manager and the secondary System Manager displays the Login page or an inappropriate page when power supply fails or when an unexpected incident occurs.

Related links

Proposed solution on page 22

Proposed solution

Procedure

1. Perform the following steps on the secondary System Manager:
   a. Install the System Manager OVA.

      Ensure that the software version of the secondary System Manager server is the same as the earlier System Manager version.

   b. Configure Geographic Redundancy.

      For instructions, see *Administering Avaya Aura® System Manager*.
2. Perform the following steps on the primary System Manager:
   a. Install the System Manager OVA.

      Ensure that the software version of the primary System Manager server is the same as the earlier System Manager version.

   b. Perform one of the following steps:
      - Perform the cold Standby procedure and use the System Manager data that you last restored.

        For instructions, see Recovering the primary System Manager server from disaster section in *Administering Avaya Aura® System Manager*.
      - If secondary System Manager server is running, perform the disaster recovery on primary System Manager server.

        For instructions, see Recovering the primary System Manager server from disaster section in *Administering Avaya Aura® System Manager*.

Multiple entries for the same Serviceability Agent

After you migrate System Manager from System Platform to Virtualized Environment, the Serviceability Agents page on System Manager web console might display duplicate entries of the same serviceability agent in the Agents list.

Related links

Proposed solution on page 23

Proposed solution

Before you begin

Start an SSH session.

Procedure

1. Log on to System Manager as root.
2. On the command line interface, run the following command available in the `$MGMT_HOME/remoteSnmpConfig/utility` location:

   ```
   recoverAgent.sh
   ```

3. At the prompt, enter the IP address of the Serviceability Agent that has duplicate entries.

   The system cleans up the corresponding serviceability agent entries from all the related tables. On the next heartbeat from the serviceability agent, the system recreates the entry in the System Manager database. On the Serviceability Agents page of the System Manager web console, consider the entry of the serviceability agent as the new entry. You must activate the Serviceability Agent again. Any earlier log harvest request is lost and you must create the request again.

Synchronizing mode for GR replication and data replication

The system displays the same Synchronizing mode for the Geographic Redundancy replication and data replication status.

Related links

Proposed solution on page 23

Proposed solution

Procedure

1. Verify if the virtual FQDN and System Manager FQDN are the same.

   The virtual FQDN and System Manager FQDN must be unique and different.

2. Install System Manager and provide unique and different values for VFQDN and System Manager FQDN. For instructions, see *Deploying Avaya Aura® System Manager*.

Note:

If the System Manager installation is not an option, contact Avaya Support Team for resolution.

Geographic Redundancy reconfiguration fails

The Geographic Redundancy reconfiguration from the secondary server to the primary server fails with an error `The primary server already had the secondary server IP configuration`.

Related links

Proposed solution on page 24

Proposed solution

Procedure

1. Log on to the web console of the primary System Manager server.
2. Do the following:
   - Verify that the secondary System Manager server entry exists in the following locations:
     - **Services** > **Inventory** > **Manage Elements**
     - **Administrators** > **Elements**
   - Click **Services** > **Geographic Redundancy** and verify that the **Convert To Standalone** button is enabled.

   If the symptoms do not exist on the primary System Manager, contact the Avaya support team.

   If the symptoms exist on the primary System Manager, move to the next step.
3. Convert the primary System Manager server to the standalone server.

   For instructions, see *Administering Avaya Aura® System Manager*.
4. Log on to the web console of the primary System Manager server when the application server starts.
5. On the web console of the primary System Manager server that is converted to standalone server, verify that the secondary System Manager server entry is removed in the following locations:
   - **Services** > **Inventory** > **Manage Elements**
   - **Administrators** > **Elements**

6. Log on to the web console of the secondary System Manager server.
7. Configure Geographic Redundancy.

   For instructions, see *Administering Avaya Aura® System Manager*.

Managed by status is Unknown for Session Manager

On **Services** > **Inventory** > **Manage Elements** of System Manager, when you select Session Manager and click **Get Current Status**, the system displays the Managed By status as Unknown and the Reachable status as Yes.

Related links

Proposed solution on page 25

Proposed solution

Procedure

1. Verify if System Manager can resolve the IP address to FQDN for Session Manager.

   This means, verify if you can reverse lookup Session Manager from System Manager. If System Manager fails to resolve the IP address to FQDN, perform the next step.
2. Verify if System Manager can resolve the network configurations such as, the DNS IP address entry for Session Manager.
3. If System Manager resolves network configurations, and Get Current Status still displays the Managed By status as Unknown and the Reachable status as Yes, contact the Avaya Support Team.

Geographic Redundancy replication status is Auto Disable

In the **Secondary Server Configured** area of the **Services** > **Geographic Redundancy**, the **Last Action** column displays Auto Disable.

For details, click the Help icon. Auto Disable might be due to network connectivity errors. Also, click **Services** > **Events** > **Alarms** for alarms.

Related links

Proposed solution on page 26

Proposed solution

Procedure

1. Enable the Geographic Redundancy replication. For instructions, see *Administering Avaya Aura® System Manager*.
2. To report the error to the Avaya Support Team, perform the following steps:
   a. Log in to System Manager CLI as root.
   b. Run the following commands:

      ```
      # collectLogs -Db
      # sh /opt/Avaya/vsp/validategeo.sh <IP address of secondary System Manager>
      ```

      The system creates the `LogsBackup_<time stamp>.tar.gz` file at the `/swlibrary` location.
   c. Attach the log file and the output from Step 2 when you report the error.

System Manager fails to synchronize with the Communication Manager main server settings

When the primary System Manager server and Communication Manager main server become nonfunctional, the secondary System Manager server and Communication Manager survivable core server become active. During the failback, to retain the administration changes made to the Communication Manager main server and to avoid any data corruption on System Manager, perform the following procedure:

Solution

1. Log on to the System Manager web console.
2. On the User Management page, select the users you added when the survivable core server is active.
3. Export users.

   The system exports the users you select to the XML and Excel file. The XML file contains the name of the Communication Manager survivable core server. You must change the survivable core server name to point to the main server.

   For more information about exporting users in bulk, see *Administering Avaya Aura® System Manager*.
4. To delete the users you exported in Step 3, select the users, and click **Delete**.
5. Open the XML or Excel file and change the Communication Manager name from the survivable remote server to the main server.
6. Import the users back on the primary System Manager server.
7. On the Manage Elements page, delete the survivable remote server entry.

Chapter 5: Alarm errors

Alarms fail to reach ADC through SAL Gateway

Symptoms that identify the issue	Alarms fail to reach ADC through SAL Gateway. However, events log in System Manager displays the generation of alarms.
Cause of the issue	When you configure System Manager as Managed Element for SAL Gateway, the system displays the following error message: `Latest SAL model for System Manager is not pushed on this System Platform box, current model shows as SystemMgr_2.0.0.1 As a result, you fail to enable the Alarm option.`

Related links

Proposed solution on page 27

Proposed solution

Procedure

1. Through the command line interface (CLI), log on to the Console Domain (C-DOM) of System Platform.
2. At the command prompt, enter the following commands:
   - `cd /opt/avaya/SAL/gateway/upgradeScripts`
   - `/upgradeSALModels.sh`

   The system populates the latest models. SAL Gateway automatically reflects the Solution Element Identifiers (SEID) attached to the latest model.
3. Configure System Manager as managed element for SAL Gateway.

   Alarms start flowing to ADC from System Manager.

System Manager generates hundreds of alarms

Symptoms that identify the issue

The sys_ConfRefreshConfig job fails with the following errors in the jboss server.log:

- A scheduled job failed to execute. Please see logs for more details.
- Illegal Argument Exception: Lookup is incorrect. Reason : javax.naming.NameNotFoundException: conferencing-ear-6.0.0.0.267 not bound

Cause of the issue

.

- Mismatch of version in the conferencing-ear file
- If any SSL negotiation error occurs, the system logs any further database queries in the postgres log files that causes the current issue.
- If the system is a 6.0.x upgraded setup, mismatch of JNDI name between the scheduler and Conferencing.

Related links

Proposed solution on page 28

Proposed solution

If you do not have Conferencing deployed in your environment, disable the job to stop the logs or alarms.

About this task

Use this procedure to disable a scheduled job.

Procedure

1. Log on to System Manager web console with user privileges to make changes on the Scheduler Web page. For example, *admin*.
2. Click **Monitoring** > **Scheduler**.
3. Click **Pending Jobs** and look for *sys_ConfRefreshConfig*.

   The system schedules the *sys_ConfRefreshConfig* job to run once per minute. If you do not find this job in the list of pending jobs, it means the job is disabled.
4. Check the status of the *sys_ConfRefreshConfig* job in the **Job Status** column. If the status is enabled, select the job and click **More Actions** > **Disable**.

   The system disables the *sys_ConfRefreshConfig* job.
5. If you do not find the job on the Pending jobs page, click **Completed jobs** and search for the job. Verify if the job is in disabled state. If the job is still in enabled state, repeat Step 4.

You must disable any on-demand jobs created for sys_ConfRefreshConfig from both the pending jobs and the completed jobs list.

6. If the system does not open the Completed jobs page due to the stale entries:
   a. To delete the entries, enter the following command on the avmgmt database:

      ```
      DELETE FROM Sched_Job_Status jobStatus WHERE
      jobStatus.status_Id NOT IN( SELECT status.status_Id FROM
      Sched_Jobs jobs , Sched_Job_Status status WHERE jobs.job_Id
      = status.job_Id AND status.end_Time_Stamp = (SELECT
      MAX(st.end_Time_Stamp) FROM Sched_Job_Status st WHERE
      st.exit_Status NOT IN (0,1) AND jobs.job_Id = st.job_Id GROUP
      BY st.job_Id )) AND jobStatus.exit_Status NOT IN (0,1)
      ```

   b. To verify the number of times the job gets executed, run the following query:

      ```
      SELECT count(*) from sched_job_status;
      ```

      Verify that the value of the count is less. The Completed jobs displays the list of all the jobs that includes, *ConfRefreshConfig*. If the ConfRefreshConfig job is in disabled state, enable the job and allow the job to run twice.

      The system stops the generation of alarms related to ConfRefreshConfig.

Related links

System Manager generates hundreds of alarms on page 28

Session Manager is unavailable in the Serviceability Agents list

After you migrate System Manager from System Platform to Virtualized Environment and register the Session Manager element with System Manager, the Serviceability Agents page on the System Manager web console does not display Session Manager in the Agents list.

Related links

Proposed solution on page 29

Proposed solution

Before you begin

Start an SSH session.

Procedure

1. Log on to Session Manager.

2. On the command line interface of Session Manager, run the following command:

   ```
   service spiritAgent restart
   ```

   The system starts the Serviceability Agent service and displays Session Manager in the Agents list on the Serviceability Agents page of System Manager web console.

Alarm fails to show on the System Manager UI

There is a Test Alarm feature on the Manage Serviceability Agents page for agents and System Manager, which is used to test end-to-end alarming. If someone tries to generate a test alarm from the agent or System Manager from the Manage Serviceability Agents page, and if there is some issue in the system, then the alarm raised by the agent or System Manager is not seen on the System Manager UI.

Cause

- Target not configured in `/var/net-snmp/snmpd.conf`
- Target added but with wrong configurations

Related links

Proposed Solution on page 30

Proposed Solution

Before you begin

Check the status of snmpd and spiritAgent services and ensure they are running on the agent and on System Manager without errors before troubleshooting other possibilities. If they are not running correctly, the entry does not appear on the System Manager UI.

About this task

Check for configuration of target address of System Manager in `/var/net-snmp/snmpd.conf`. If it does not show, it may be missed or `/var/net-snmp/snmpd.conf` is not in the correct state and needs a repair.

If the target is not configured in `/var/net-snmp/snmpd.conf`, use the following procedure to rectify alarms not shown on System Manager Alarms UI.

Procedure

1. Create the correct User Profile and Target Profile under **Services** > **Inventory** > **Manage Serviceability Agents**.
2. Select the agent whose alarm is not seen on System Manager UI.
3. Verify that the target is added in `/var/net-snmp/snmpd.conf`. If not, then `snmpd.conf` must be in a bad state.

4. To correct the state of the file, go to **Elements** > **Manage Serviceability Agents**. Select the agent and click **Repair Serviceability Agent**.
5. Wait for 15-20 minutes. If you find the agent is not repaired, you can try the CLI way of repair. Do the following:
    a. Run the following command on System Manager with root: **`sh $MGMT_HOME/remoteSnmpConfig/utility/recoverAgent.sh <IP address of the agent>`**

        Note:

        If the System Manager is between 8.1.x and 8.1.2, then restart JBoss after step 5.

        If the System Manager is 8.1.3 or any other version other than 8.1.x to 8.1.2, then JBoss restart is not needed.

    b. If it is not System Manager, login on agent and perform: **`sh $SPIRIT_HOME/scripts/utils/reinitilizeSnmpdConfiguration.sh`**
    c. On the agent, run the following command: **`service spiritAgent restart`**.
6. Check if the target address is seen on `/var/net-snmp/snmpd.conf`. If yes, there may be a mismatch with what is set in TrapListener Configuration Parameters under **Services** > **Configurations** > **Settings** > **SMGR** > **TrapListener** and what is set in `/etc/snmp/snmpd.conf`.
7. If the target is added but with wrong configurations, use the following procedure to rectify the issue of alarms not shown on System Manager Alarms UI:
    a. Check the **UserName**, **Authentication Protocol**, **Authentication Password**, **Privacy Protocol**, and **Privacy Password** under **Services** > **Configurations** > **Settings** > **SMGR** > **TrapListener**.
    b. Ensure you create the same User and Target profiles on the Manage Serviceability Agents page as in step 6a.
    c. Push the same User and Target profiles to the agent.
    d. Confirm that `/var/net-snmp/snmpd.conf` file is updated with the mentioned pushed UserName and Target.

Chapter 6: Certification errors

System Manager does not support third-party certificates

Symptoms that identify the issue	System Manager does not support third-party trust certificates.

Related links

Proposed solution on page 32

Proposed solution

Before you begin

- Obtain the certificate that has the System Manager hostname as CN, and signed by the third-party Certificate Authority (CA).
- If required, store the third-party certificate and subordinate CA certificates in a PKCS12 container with the corresponding private key.

About this task

To install and use the third-party certificate for System Manager web interface, perform the following high level steps:

Procedure

1. Replace the System Manager web server certificate with a third-party certificate.
2. Update the trust stores for internal services, clients, or managed elements with third-party root and subordinate CA certificate.

   For more information, see *Application notes for supporting third-party certificate in Avaya Aura® System Manager 6.3.x and 7.0.x* on the Avaya Support website at http://support.avaya.com.

Chapter 7: Bulk import and export errors

Import utility fails to import the users of specific time zone

Symptoms that identify the issue	Using the import utility, when you import the users with the (+01:00) Amsterdam, Berlin, Rome, Belgrade, Prague, Brussels, Sarajevo time zone, the system fails to import the user data.
Cause of the issue	Bulk import feature does not take the timezone string that the User Management page displays. Also, the bulk import feature expects the timezone offset information to be present for the timezone attribute in the import XML file.

Related links

Proposed solution on page 33

Proposed solution

The system does not display the timezone information of the user that you import on the User View profile page. Therefore, for each imported user, you must manually update the timezone information.

Before you begin

- Log on to the System Manager web console.
- Import the user data.

  To import the user data, click **Users** > **User Management** > **Manage Users** and click **More Actions** > **Import Users**.

Procedure

To successfully import the users, perform one of the following procedures:

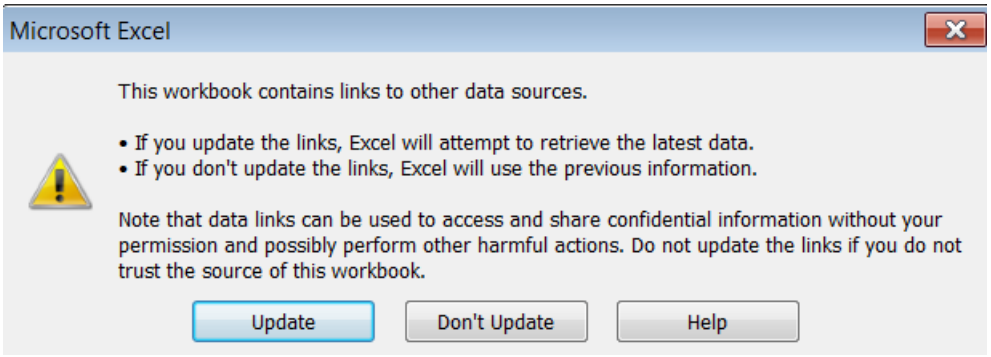
- Click **Users** > **User Management** > **Manage Users** and perform the following:
  a. Select the user and click **View**.
  b. On the User Profile View page, in the **Time Zone** field, ensure that the timezone offset information is available. For example, (+01:00) Amsterdam, Berlin, Rome, Belgrade, Prague, Brussels, Sarajevo.

- For each user, in the import XML file, remove the timeZone attribute tag. For example, remove:

```
<timeZone>(+01:00) Amsterdam, Berlin, Rome, Belgrade, Prague, Brussels, Sarajevo</
timeZone>
```

Microsoft Excel data link error

Microsoft Excel 2010 displays a data link error.



Related links

Proposed solution on page 34

Proposed solution

About this task

You can ignore data link error that Microsoft Excel 2010 displays. However, perform the following procedure to avoid this error the next time you open an Excel file.

Procedure

1. On the Excel worksheet, close the warning message.
2. On the **Data** menu, click **Edit Links**.
3. On the Edit Links dialog box, click **Startup Prompt**.
4. Click **Don't display the alert and don’t update automatic links** and click **OK**.
5. Click **Close**.
6. Save the Excel file.
7. Close the Excel file and open the file again.

   The system does not display the data link error message now.

Data entry warning in Microsoft Excel

The data type of the cell in Excel is text. If you provide a number in the cell, Excel displays the `Number Stored as Text` message. Ignore the warning and do not change the data type of the cell.

Related links

Proposed solution on page 35

Proposed solution

About this task

You can ignore data entry warning that Microsoft Excel 2007 or later displays. However, perform this procedure to turn off the warning message.

Procedure

1. Based on the version, do one of the following:
   - In Microsoft Office Excel 2007, click **Excel Options**.
   - In Microsoft Office Excel 2010, click **File** > **Options** > **Excel Options**.

   For other Microsoft Office Excel versions, use the appropriate options.
2. In Microsoft Office Excel 2010, in the left navigation pane, click **Formulas** and clear the **Numbers formatted as text or preceded by an apostrophe** check box.
3. Click **OK**.

Chapter 8: Miscellaneous errors

Authentication of the LDAP user to System Manager fails

Symptoms that identify the issue	Authentication of the LDAP user to System Manager fails.
Cause of the issue	The customer LDAP has login names with DN in the format, `cn=<loginname>,oc=<oc-value>,dc=<dc-value>,dc=<dc-value>`. The login name does not have the domain information.

Related links

Proposed solution on page 36

Proposed solution

Using the Subject Mapping table, you can map an LDAP user to a System Manager user. Therefore, System Manager authenticates the LDAP username without @domain and then maps to the correct user in System Manager.

Before you begin

- Obtain the System Manager login name and the corresponding identities.
- Log on to System Manager.

Procedure

1. To map the users in the User Management and the LDAP, enter the user name in the **CSSecurityIdentity** table.
2. To populate the **CSSecurityIdentity** table, use the bulk import functionality as shown in the sample XML file.

```
<?xml version="1.0" encoding="UTF-8"?>
<delta:deltaUserList xmlns:delta="http://xml.avaya.com/schema/deltaImport"
xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd ">
  <delta:userDelta>
    <loginName>janedoe@avaya.com</loginName>
    <securityIdentity>
```

```
      <identity>janedoe</identity>
      <realm>admin</realm>
      <type>principalname</type>
    </securityIdentity>
  </delta:userDelta>
</delta:deltaUserList>
```

SSO login to remote machine fails

For System Manager deployments involving remote machines such as, CS 1000 servers and solutions based on the System Manager Single Sign On (SSO) client, the SSO between System Manager and the remote machine fails.

During the data migration or IP-FQDN change, the system does not import the LDAP attribute containing the SSO cookie domain value back to the directory. Therefore, the System Manager SSO login to the remote machine fails. You must enable SSO after the data migration or the IP-FQDN change.

Related links

Reimporting the SSO cookie domain value on page 38

CSRF error in SAML Authentication flow

Error Scenario

When System Manager connects to an external Identity Provider (IdP) for SAML authentication, login failures may occur with the following error message: **Cross site request forgery could be present in your request**.

Possible Causes and Checks to be done

- Incomplete or incorrect TLS certificate trust chain in the SMGR truststore.
- IdP resolves to multiple IP addresses, and each IP presents a different certificate chain that leads to the root certificate.
- SSL inspection or proxy interference changes TLS or SAML traffic.
- DNS resolves IdP to multiple IP addresses with inconsistent routing.
- Time synchronization issues cause invalid SAML assertions.
- Firewall restrictions block access to required SAML Authentication server.

Recommended Solutions

1. Import the full certificate chain (leaf and intermediate CA) for IdP into System Manager truststore. Do not rely only on root CA or intermediate CA.
2. If System Manager resolves IdP FQDN to multiple IPs and each IP presents a different root or intermediate certificate chain, ensure that the full certificate chain for each resolved IP is imported into System Manager truststore. This ensures trust validation succeeds across

all resolved IdP IPs and prevents intermittent TLS or SAML failures caused by inconsistent certificate chains.

3. If you cannot add the certificate chain for all IPs to System Manager truststore, map the IdP FQDN in System Manager hosts file to a static, controlled IP resolution to ensure consistent routing to a known IP or server.
4. Ensure NTP is correctly configured on System Manager to prevent clock drift that could break SAML assertion validation.
5. Ensure that the customer's network firewall rules allow System Manager to connect to the SAML Authentication server.

Reimporting the SSO cookie domain value

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the navigation pane, click **Security** > **Policies**.
3. In the Single Sign-on Cookie Domain section, click **Edit**.
4. In the **Single Sign-on Cookie Domain**, select the appropriate domain based on the FQDN of the deployed servers.
5. Click **Save**.
6. Log out and close all browser windows you opened when logging on to the System Manager server.
7. To accept the updated cookies from the new Single Sign-On (SSO) cookie domain name, clear the browser cache.

Backup failure

Backup failure due to lack of disk space in /swlibrary

Condition

If the backup is not successful due to lack of disk space in `/swlibrary`, check the `/var/log/Avaya/mgmt/pem/pemDebugLog.log` file and search for the following string:

```
Caused by: java.io.IOException: No space left on device
```

Solution

1. Clean up space in `/swlibrary`.

Note:

Do not delete the `wildfly_java_tmp` directory.

2. Move the backup archives located at `/swlibrary/backup/` to the remote machine.
3. Delete unused SDM artifacts, such as OVAs and patches that are not required.

   To delete SDM artifacts from the System Manager web console, click **Services** > **Solution Deployment Manager** > **Software Library Management** > **Manage Files** > **Select and Delete files**.
4. Delete any files, such as OVAs for patch binaries copied manually.

Resetting the System Manager password

Resetting the System Manager password from the System Manager web console

About this task

If System Manager is configured with any other user having the System Administrator role, use the following procedure to reset the password from the System Manager web console.

Procedure

1. On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, the System Manager URL.
2. In the **User ID** field, type the user name having the System Administrator role.
3. In the **Password** field, type the password.
4. Click **Log On**.
5. On the System Manager web console, click **Users** > **Administrators** > **Administrative Users**.
6. On the Administrative Users page, in the **User ID** column, click on user id to reset password for the admin user.
7. On the User Details (admin) page, in the Password Reset section, do the following:
   a. In the **Password** field, type the password.
   b. In the **Re-enter password** field, retype the password.
8. Click **Commit** to save the changes.
9. Log out after the password is reset.

Resetting the System Manager password through Avaya services personnel account

About this task

Use the following procedure to reset the password through the Avaya services personnel account or the Avaya Technician account.

This procedure is applicable for System Manager Release 7.1.2.x and later.

Procedure

1. On the web browser, type `https://<Fully Qualified Domain Name>/services/`, the System Manager URL.

   If EASG is disabled, the system displays the message: `EASG is disabled`
2. In the **Username** field, type `init`.
3. Click **Next**.

   The system displays the **Challenge**, **Product ID**, and **Response** fields. The **Challenge** and **Product ID** fields are read only.
4. In **Response**, paste the response for the EASG challenge.
5. Click **Login**.

   The system validates the challenge and response. If authentication is successful, the system displays the System Manager web console.
6. On the System Manager web console, click **Users** > **Administrators** > **Administrative Users**.
7. On the Administrative Users page, in the **User ID** column, click on user id to reset password for the admin user.
8. On the User Details (admin) page, in the Password Reset section, perform the following:
   a. In the **Password** field, type the password.
   b. In the **Re-enter password** field, retype the password.
9. Click **Commit** to save the changes.
10. Log out after the password is reset.

Resetting the System Manager password using the local-login workflow

About this task

Use the following procedure to reset the password from the System Manager web console using the local-login workflow.

This procedure is applicable for System Manager Release 6.3.x and later.

Procedure

1. On the web browser, type `https://<Fully Qualified Domain Name>/local-login`, the System Manager URL.
2. If System Manager is on release:
   a. 6.3.x to 7.0.x, enter the CLI admin user credentials.
   b. 7.1.x and later, enter the CLI user credentials created during deployment.

      From System Manager Release 7.1.x and later, the CLI default user *admin* is disabled.
3. On the Password Reset page, enter the credentials.
4. Click **Save** to reset the password.
5. Log out after the password is reset.
6. On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, the System Manager URL.
7. Log in to the System Manager web console using the new credentials.

   The System Manager web console redirects to change the password.
8. Change the System Manager password and log in to the web console successfully.

Identifying Communication Manager when you run a sychronization

Condition

When you run a synchronization, it can be difficult to identify a specific Communication Manager in the case of duplex pairs.

Solution

See the logs after enabling the operation log.

From 10.2.1 onwards, the IP address and hostname of the Communication Manager are logged.

Chapter 9: Element Manager errors

Removed Communication Manager reappears on System Manager web console

Symptoms that identify the issue

Communication Manager that was removed earlier, reappears on System Manager web console.

Cause of the issue

In System Manager, the problem occurs when:

1. Two Communication Manager systems with the same name exist.
2. Out of the two Communication Manager systems, you manually add one system and the other system gets added from **Services** > **Inventory** > **Inventory Management** > **Collect Inventory**.
3. You remove the two Communication Manager systems.

   The system removes the entry of Communication Manager from **Services** > **Inventory** > **Manage Elements**. However, System Manager still displays the two Communication Manager voice systems on the **Services** > **Inventory** > **Synchronization** > **Communication System** page.

Related links

Proposed Solution on page 42

Proposed Solution

Assume the IPTCM database has two entries of Communication Manager systems with rtsappids 50 and 100. Use this procedure to remove the Communication Manager system with the rtsappid 100 and reinstate the entry of the legitimate Communication Manager with rtsappid 50.

Procedure

1. To set the rtsappid to null and the name to any arbitrary value for Communication Manager having rtsappid 100, run the following query:

```
update ipt_cm set cmname='ABC',rtsappid= null where id = 100;
```

2. To modify the IP addresses in the **ipt_cm_conn** table, run the following query:

```
update ipt_cm_conn set ipaddress1='1.1.1.1' , ipaddress2='1.1.1.1' where id =
100;
```

3. To run the maintenance job for Communication Manager on the System Manager web console, click **Services** > **Scheduler** > **Pending Jobs**.

   The system removes the entry cm_id=100 from the tables **ipt_cm** and **ipt_cm_conn**.

4. To add the entry of the Communication Manager system again, from Runtime Topology System (RTS), provide the IP address and the name of the legitimate Communication Manager system.

   Note:

   If the details you enter do not match with the legitimate Communication Manager, the system adds a new entry for the Communication Manager in the **ipt_cm** table.

5. To retrieve the Communication Manager ID you entered in step 4, from the **rts_applicationsystem** table, run the following query:

```
select id,name from rts_applicationsystem;
```

   The Communication Manager ID is the rtsappid for the **ipt_cm** table.

6. To update the rtsappid in the **ipt_cm** table with the ID you retrieved from the previous step, run the following query:

```
update ipt_cm set rtsappid=? where id = 50;
```

   Verify if the synchronization is working for Communication Manager.

   The system modifies the rtsappid for Communication Manager.

Deletion of Communication Manager from System Manager inventory fails

Symptoms that identify the issue	Deletion of Communication Manager from the System Manager inventory fails if the Communication Manager system is part of a Uniform Dialing Plan (UDP) Group.
Cause of the issue	When you attempt to delete Communication Manager from the System Manager inventory, the system checks for the resource name UDP Group instead of UDP_Group. If the system fails to find UDP_Group, Communication Manager does not get deleted from the System Manager inventory.

Related links

Proposed solution on page 44

Proposed solution

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. To delete Communication Manager from the System Manager inventory that is part of a UDP group:
   a. Select the check box for the Communication Manager system that has **Type** set to `UDP_Group`.

      You set **Type** to `UDP_Group` from **Users** > **Groups & Roles** on the Group management page.

   b. Click **Delete**.

Note:

Do not search for **UDP Group**.

Chapter 10: Enhanced Access Security Gateway

Enhanced Access Security Gateway (EASG) overview

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

Managing EASG from CLI

About this task

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

Before you begin

Log in to the application CLI interface.

Procedure

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

   The system displays the status of EASG.

2. To enable EASG, do the following:

   a. Run the command: **`EASGManage --enableEASG`**.

      The system displays the following message:

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

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

```
for additional information for registering products and
establishing remote access and alarming.
```

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

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

3. To disable EASG, do the following:

a. Run the command: **`EASGManage --disableEASG`**.

The system displays the following message:

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

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

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

Viewing the EASG certificate information

Procedure

1. Log in to the application CLI interface.
2. Run the command: **`EASGProductCert --certInfo`**.

   The system displays the EASG certificate details, such as, product name, serial number, and certificate expiration date.

EASG site certificate

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

Managing site certificates

Before you begin

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

4. You must have the following before loading the site certificate:
   - Login ID and password
   - Secure file transfer tool, such as WinSCP
   - Site Authentication Factor

Procedure

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

Chapter 11: Resources

System Manager documentation

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

Title	Description	Audience
Design		
Avaya Aura® System Manager Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Administering Avaya Aura® System Manager	Administering System Manager applications and install patches on System Manager applications.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Certificate Management	Understand certificate management.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Data Privacy Guidelines	Describes how to administer System Manager to fulfill Data Privacy requirements.	System administrators and IT personnel
Using		
Using the Solution Deployment Manager client	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Avaya Aura® System Manager Solution Deployment Manager Job-Aid	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Implementation		
Upgrading Avaya Aura® System Manager	Upgrade Avaya Aura® System Manager.	Implementation personnel
Deploying Avaya Aura® System Manager in Virtualized Environment	Deploy System Manager applications in Virtualized Environment.	Implementation personnel

Table continues…

Title	Description	Audience
Deploying Avaya Aura® System Manager in Software-Only and Infrastructure as a Service Environments	Deploy System Manager applications in Software-Only and Infrastructure as a Service environments.	Implementation personnel
Maintenance and Troubleshooting		
Avaya Aura® System Manager SNMP Whitepaper	Monitor System Manager using SNMP.	System administrators and IT personnel
Troubleshooting Avaya Aura® System Manager	Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators and IT personnel

Finding documents on the Avaya Support website

Procedure

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

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

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

Accessing the port matrix document

Procedure

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

This field is not available if there is only one release for the product.

5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

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

Important:

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

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

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

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

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

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

Training

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

Course code	Course title
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

Viewing Avaya Mentor videos

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

About this task

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

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

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

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

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 52

Using the Avaya InSite Knowledge Base

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

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.

- Links to other pertinent information.

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

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

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

Related links

Support on page 52

Index

H

I

K

L

M

N

P

R

S

T

U

V

W