Troubleshooting Avaya Aura® System Manager

Release 6.2
Issue 1.0
July 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.

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® System Manager 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

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

the Avaya Support Web site: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Overview

The section provides detailed information to help you resolve issues with Avaya Aura® System Manager. The troubleshooting section is intended for those who use System Manager to maintain, manage, and service Avaya applications and systems.

Some of the Avaya adopting products that System Manager currently supports:

- Avaya Aura® Session Manager
- Avaya Aura® Presence Services
- Avaya Aura® Communication Manager
- Avaya B5800 Branch Gateway
- Avaya Aura® Call Center Elite
- Avaya Aura® Contact Center
- CS 1000

Chapter 2: 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.

Chapter 3: 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 topics:

Proposed solution on page 11

Proposed solution

Procedure

1. Through the command prompt 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 topics:

Proposed Solution on page 12

Proposed Solution

If you do not have the Conferencing solution 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 the System Manager Web Console as a user that has 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 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 topics:

[System Manager generates hundreds of alarms](#) on page 12

Chapter 4: System Platform errors

System Platform fails to detect the short hostname prior to template install

Symptoms that identify the issue

After the installation of the System Manager template from the System Platform Web Console, the template installation rolls back.

Cause of the issue

In System Manager 6.1, you must enter only the FQDN as the hostname. However, you can still enter the short name in the hostname field. After you install the System Manager template using the System Platform Web Console, System Manager runs a post install script for validation. The script delays by 30 minutes or fails to recognize the shortname for the **Hostname** field. As a result, the template installation rolls back.

Related topics:

Proposed Solution on page 15

Proposed Solution

Procedure

1. Open the `SystemManager.ovf` file from the build location.
2. To detect the short hostnames prior to the System Manager template installation, add an XML attribute to the OVF templates in System Platform for template fields similar to the following:

```
<ovf:Property ovf:key="smgr.hostname" ovf:type="string"
ovf:qualifiers="MinLen(1)"
                              ovf:def-value="" ovf:userConfigurable="true"
ovf:requirefqdn="true" or ovf:requireip="true" or generic
attribute=”----” >
<ovf:Description>Hostname: System Manager FQDN</ovf:Description>
</ovf:Property>
```

System Platform detects the use of shortnames in the fields before the System Manager post install script validates.

3. In the `SystemManager.ovf` file, change the checksum, sha1sum and update the `sha1sum_report.txt` file in the build location.

   System Manager captures the new parameters and uses them in the post install script for validation.

Chapter 5: 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 topics:

Proposed solution on page 17

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 PKCS#12 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 6.1* on the Avaya Support Site at http://support.avaya.com.

Chapter 6: 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 import XML file.

Related topics:

Proposed solution on page 19

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:

  i. Select the user and click **View**.

ii. On the User Profile View page, ensure that the timezone offset information in the **Time Zone** field. 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>
```

Chapter 7: 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 topics:

[Proposed solution](#) on page 21

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>
```

Chapter 8: Element Manager errors

Removed Communication Manager reappears on the System Manager Web Console

Symptoms that identify the issue

Communication Manager that was removed earlier, reappears on the System Manager Web Console.

Cause of the issue

In System Manager, the problem occurs when:

a. Two Communication Manager systems with the same name exists.

b. Out of the two Communication Manager systems, you manually add one system and the other system gets added from **Elements** > **Inventory** > **Inventory Management** > **Discovery**.

c. You remove the two Communication Manager systems.

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

Related topics:

Proposed Solution on page 23

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 that has 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 does 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 ID of Communication Manager that 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 RTS fails

Symptoms that identify the issue	Deletion of Communication Manager from Runtime Topology System (RTS) fails if the Communication Manager system is part of an Uniform Dialing Plan (UDP) Group.
Cause of the issue	When you attempt to delete Communication Manager from RTS, 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 RTS.

Related topics:

[Proposed solution](#) on page 25

Proposed solution

Procedure

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

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

Note:

Do not search for the GLS Group **UDP Group**.

Index