Troubleshooting Avaya one-X® Client Enablement Services

Release 6.1 SP3
v1.0
October 2012

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

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

License type(s)

Named User License (NU). End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

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

Copyright

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

Third-party components

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

The open source license text file, `OpenSourceLicense.txt`, is available in the Licenses folder on the Avaya one-X® Client Enablement Services server: `/Licenses/OpenSourceLicense.txt`.

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 one-X® Client Enablement Services, Communication Manager, Modular Messaging, and Conferencing are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Troubleshooting overview

Troubleshooting overview

The Troubleshooting guide lists the unexpected issues the system administrators or the users encounter, and the proposed solutions for these issues. It is assumed that the system administrator or the system maintenance technician will use this guide, and they have the necessary access and expertise to use the various products discussed in this guide such as Communication Manager, Session Manager, and System Manager.

This guide is divided into four chapters.

1. Chapter 1 provides a brief overview of the troubleshooting guide and lists the related product documents.
2. Chapter 2 discusses the issues faced during installation and after installing Client Enablement Services and the troubleshooting steps.
3. Chapter 3 discusses the issues faced during administration and configuration of Client Enablement Services and the troubleshooting steps.
4. Chapter 4 discusses the issues faced by the users while using the Avaya one-X® Mobile client application.
5. Chapter 5 discusses the issues faced by the users while using the Avaya one-X® Communicator client application.
6. Chapter 6 lists the alarms generated by the system to notify the administrator of various system events. For each alarm, there is information on the alarm name, alarm text, alarm level, trigger component, problem description, and the troubleshooting steps.

Related product documents

To troubleshoot other Avaya products integrated with Avaya one-X® Client Enablement Services, refer to the troubleshooting guides or other relevant guides of these products on the Avaya support site http://www.avaya.com.

Product name	Documentation
Communication Manager	Refer the appropriate guide from the Avaya support site.
Modular Messaging	Refer the appropriate guide from the Avaya support site.
Avaya Aura® Messaging	Refer the appropriate guide from the Avaya support site.
Conferencing	Refer the appropriate guide from the Avaya support site.
Presence Services	*Troubleshooting Avaya Aura® Presence Services*
Session Manager	*Maintaining and Troubleshooting Avaya Aura® Session Manager*
System Manager	Refer the appropriate guide from the Avaya support site.

You can also refer to other guides from the Client Enablement Services documentation suite.

- *Administering Avaya one-X® Client Enablement Services*
- *Implementing Avaya one-X® Client Enablement Services*
- *Avaya one-X® Client Enablement Services Overview*
- *Using Avaya one-X® Mobile on BlackBerry (touch screen model)*
- *Using Avaya one-X® Mobile on BlackBerry (non-touch screen model)*
- *Using Avaya one-X® Mobile on Android*
- *Using Avaya one-X® Mobile on iPhone*

Chapter 2: Troubleshooting implementation issues

Troubleshooting the Avaya one-X® Client Enablement Services installation

About this task

If you have a problem when you install Client Enablement Services, perform the following actions:

Procedure

1. Review the topics in the following sections for possible resolutions to your problem.
2. Retry the action. Carefully follow the instructions in the documentation.
3. Retrieve the log files and review all applicable error messages.
4. Note the sequence of steps and events that led to the problem and the messages that the system displays.
5. If possible, capture screen shots that show what happens when the issue occurs.

Tip:

If the proposed solutions do not resolve your problem or if your problem is not included in this section, follow your corporate process to obtain support.

Unable to access System Platform Web Console

You cannot reach System Platform Web Console. Also, when you try to ping Console Domain, you do not get a response.

Troubleshooting steps

At the **xm list** command, the system displays information about the virtual machines that are currently running on a Linux operating system.

The system displays only three virtual machines: System Domain shown as `Domain-0`, Client Enablement Services shown as `onexps`, and Console Domain shown as `udom`.

A state of `r` indicates that the virtual machine is running. A state of `b` indicates that the virtual machine is blocked.

Note:

The blocked state does not indicate a problem with the virtual machine but that the virtual machine is currently not using any CPU time.

Other possible virtual machine states are:

- p: paused
- s: shutdown
- c: crashed

If the virtual machine is in the p, s, or c state, you cannot reach System Platform Web Console. Therefore, you cannot ping Console Domain.

For more information, see *Installing and Configuring Avaya Aura™ System Platform*.

Procedure

1. Log in to System Domain (Domain-0) as `admin/admin01`.
2. Enter **su -** to log in as root.
3. At the prompt, type **xm list**.
4. On the Linux screen, type `exit` to log off as root.
5. Type `exit` again to log off from System Domain (Domain-0).
6. If the state of Console Domain is not `r` or `b`, then you must reinstall System Platform and ensure that Console Domain is accessible.

Template installation fails

The template installation can fail for any of the following reasons:

- **Checksum mismatch**: The system returns this error on the initial pages during the installation when the system cannot verify the *Checksum* of image files.
- **Memory allocation error**: The system returns this error on the initial pages during the installation due to insufficient memory. The system displays the following error message: `Insufficient resources to install this template (Insufficient memory. Requested 8192MB (more), available free space 6488MB).`
- **Kernel mismatch**: The system returns this error on the last page during the installation.
- **Post-install plug-in failed**: The system returns this error on the last page during the installation or when the installation is stuck at this step.
- The template installation plug-in is stuck at the last stage for more than an hour.

Troubleshooting steps

Procedure

Select the solution that matches the reason for template failure:

- **Checksum mismatch**: Download the template files again.
- **Memory allocation error**: Check the available RAM on the system and then install the Client Enablement Services template.
- **Kernel mismatch**: Reboot Domain-0 from System Platform Web Console. In the left pane, click **Server Management** > **Server Reboot/Shutdown** and then click **Reboot**.
- **Post-install plug-in failed**: Reboot cdom from System Platform Web Console. In the left pane, click **Virtual Machine Management** > **Manage**. Click the **cdom** link and then click **Reboot** and try the installation again.
- If the plug-in is stuck during the installation of the template and the in-progress status does not change, check if you can reach the Client Enablement Services IP address using the ping command. If the ping command indicates that the Client Enablement Services IP address is not reachable, cancel the existing template installation. Reboot cdom from System Platform Web Console and try the installation again.

- If you do not know the reason for template failure, perform the following actions:
  - Check if all the required files are downloaded.
  - Check if the file permissions are correct.
  - Check if the System Manager server and the Client Enablement Services server are having the same time stamp.
  - Ensure that Client Enablement Services can access System Manager
  - Ensure that LDAP is functional.
  - Check if the LDAP service account password includes special characters such as $, #, {, ", and -. If the password includes special characters, and you install the Client Enablement Services template, the template installation is stuck at the last stage for a long time.

Template installed but Avaya one-X® Client Enablement Services does not run

Even after the installation of the template is complete, Client Enablement Services might not run due to any of the following reasons:

- Input error
- Unexpected syntax in input
- Post-install plug-in failed
- Cdom not restarted after you delete the existing template

Troubleshooting steps

Procedure

Perform the following:

- Log in to the System Platform Web Console and ensure that the Client Enablement Services virtual machine is running.
- Log in to the CLI of the Client Enablement Services virtual machine as an administrator. If login fails, reboot the Client Enablement Services virtual machine using the System Platform Web Console and try logging in again.
- Log in to the CLI of the Client Enablement Services virtual machine as a root user and execute the `service 1xp restart` command.

- Check the vsp logs in the `/opt/vsp/log` directory for any failure.
  - `post_install_config.log`: Logs the results of the installation
  - `restore_template.log`: Logs the results of the template restore. The system performs the restore after installation upgrades.
- Check the Client Enablement Services `trace.log` file in the `/opt/IBM/WebSphere/AppServer/profiles/default/logs/server1` directory.
- If the plug-in is stuck during the installation of the template, and the in-progress status does not change, you must reboot the cdom using the System Platform Web Console and try the installation again.
- Check if the LDAP service account password includes special characters such as $, #, {, ", and -. If the password includes special characters, when you log in to the Client Enablement Services administration application, the system displays an error message.
- If you are installing a new template, you must restart the cdom using the System Platform Web Console after you delete the existing template.

Out-of-memory error

If you reinstall the template by deleting and installing the template multiple times, the system might display an out-of-memory space permanent generation (PermGen) error.

The system displays the error if you did not reboot the cdom using the System Platform Web Console, after you delete the existing template.

Troubleshooting steps

About this task

Perform the troubleshooting steps given here to ensure that a PermGen error does not occur.

Procedure

1. Delete the template.
2. Restart Tomcat by performing the following steps:
   a. Log in to the cdom as `admin/admin01`.
   b. Enter **su -** to log in as root.
   c. At the prompt, type `/sbin/service tomcat restart`

3. Log in to the System Platform Web Console.
4. Install the template.

Unable to log in to the Avaya one-X® Client Enablement Services Web administration portal

You cannot log in to the Client Enablement Services Web administration portal, or you get a 500 internal error on login.

Troubleshooting steps

Procedure

Perform the following:

- Ensure that the LDAP server is connected and running.
- Ensure that the user name and password are correct.
- Ensure that the user name is part of the Administrator Security Group.
- Ensure that the database is running.
  - If the database is not running, log in to the CLI of the Client Enablement Services server as root user.
  - Switch to dbinst user using the `su – dbinst` command.
  - Run the `db2start` command.
  - Switch to the root user and restart WAS by using the `service 1xp restart` command.

Template installation complete, but the administration application displays error

When the password of the LDAP service account has a $ sign, and you install the Client Enablement Services template, the template installation gets stuck at the last stage for a long time. After the installation is complete, the system does not display any problem.

However, when you log in to the Client Enablement Services administration application, the system displays following error message:

```
SRVE0255E: A WebGroup/Virtual Host to handle /admin/ has not been
defined.
```

```
SRVE0255E: A WebGroup/Virtual Host to handle xx.xx.xx.xx has not been
defined.
```

In this example, xx.xx.xx.xx is the IP address of the Client Enablement Services server.

Therefore, you should avoid using special characters in the LDAP service account password such as $, #, {, " , hypen (-), and 'space'. You should also avoid using hypen (-) in user name.

Proposed solution

Procedure

1. Change the password of the LDAP service account.
2. Delete the existing template.
3. After deleted the template, reboot the dom-0.
4. Reinstall the template.

   For more information on the detailed steps for each, see *Implementing Avaya one-X® Client Enablement Services* guide.

Unable to log in to the Avaya one-X® Mobile client

You have installed the Handset Server. However, the user is unable to log in to the Avaya one-X® Mobile client.

Troubleshooting steps

Procedure

1. Log in to the CLI of the server on which you installed the Handset Server.
2. Check the `handset_server.properties` file in the `/opt/avaya/HandsetServer` directory to ensure all the values are correct.

3. Check if the Handset Server is running using the `ps –ef | grep HandsetServer` command.
   - If the Handset Server is not running, start the Handset Server using the `service handset_server start` command.
   - If the Handset Server is running, restart the Handset Server using the `service handset_server restart` command. Restart the Handset Service from the Client Enablement Services administration client using the Monitors tab, and then update the user to log in to the Avaya one-X® Mobile client.
4. If the user is still unable to login, perform the following:
   a. Quit the currently running Handset Server process using the command `Kill -9 <PID>`.
   b. Start the Handset Server.
   c. Restart the Handset Service from the Client Enablement Services administration client using the **Monitors** tab, and then update the user to log in to the Avaya one-X® Mobile client.

Transcoding Service cannot connect to the Transcoding Server

On the Monitor Audio Transcoding Services Web page of the Client Enablement Services administration website, check whether the status of the **State** field is set to **Unavailable**.

The status indicates that the Transcoding Service is unable to connect to the Transcoding Server or the Transcoding Server configuration has a problem.

Troubleshooting steps

Procedure

Perform the following:

- Check whether the Transcoding Server is running as mentioned in Verifying whether the Transcoding Server is running.
- Open the `TranscodingServer.properties` file from the `opt/avaya/1xp/transcodingserver/config` directory. Ensure that the value of the *transcoding.server.port* property is the same as the value specified in the

Transcoding Server Address: Port field on the Modify Audio Transcoding Web page of the Client Enablement Services administration website.

- Check whether the system creates the `/tmp/transcoding` directory for the **Destination of converted audio messages** property on the Modify Audio Transcoding Web page of the Client Enablement Services administration website. This directory must be present on the server.
- Check the host IP address at **Servers** > **Audio Transcoding** > **Transcoding Server Address**. By default, the address is the same as the loopback IP address. The Transcoding Server can function on both the loopback and the Client Enablement Services IP address.

Secure SSL connection between servers fails

If you do not synchronize the time stamps, the secure SSL connection between the servers fails.

Time synchronization ensures that time stamps for all integrated systems are consistent.

Troubleshooting steps

Procedure

1. Log in to the cdom and the Client Enablement Services systems using the SSH terminal as user `craft/craft01` and then switch the user to root using the **`su - root`** command and *root01* password.
2. Check the date on both the systems using the `date` command.
   If the time zone differs, you must use NTP for both cdom and Client Enablement Services to correct this mismatch.

Trace errors using log files

This topic lists the log files that you can use to trace errors during the troubleshooting process.

Console domain log files

- Log files in the `/var/log/vsp` directory
- Files in the `/vspdata/template/onexps_template` directory

Client Enablement Services domain log files

- Log files in the `/opt/vsp/log` directory
- IBM log files in the `/opt/IBM/WebSphere/AppServer/profiles/default/logs/server1` directory

Client Enablement Services domain files that are updated during the template installation

- `/opt/avaya/1xp/AcpInstallationConfig.sql`
- `/opt/avaya/1xp/AcpInstallationWebLM.sql`
- `/opt/avaya/1xp/config.properties`
- `/opt/avaya/1xp/installapps.py`
- `/opt/avaya/1xp/SIP_local_update.sql`
- `/opt/avaya/HandsetServer/handset_server.properties`

Handset Server log files

The Handset Server log files are located in the `/opt/avaya/HandsetServer/logs` directory.

- To check all logs, view the `hs.log` file.
- To check only the error information, view the `hs_errors.log` file.
- To check only the I/O logging information, view the `hs_io.log` file.

To view the properties for the Handset Server log files, check the `log4j.properties` file located in the `/opt/avaya/HandsetServer` directory.

Commands for use in Avaya one-X® Client Enablement Services

- To start the Client Enablement Services server, on the shell prompt, type the **`service 1xp start`** command.
- To stop the Client Enablement Services server, on the shell prompt, type the **`service 1xp stop`** command. The system prompts you to enter your user name and password when the system tries to stop the server.

- To restart the Client Enablement Services server, on the shell prompt, type the **`service 1xp restart`** command. The system prompts you to enter your user name and password when the system tries to stop the server.
- If you fail to access the `https://<one-X CES IP or FQDN>/mobileapps` page from Avaya one-X® Mobile or a browser, you must check the `access_log` file using the `tail -f /opt/IBM/HTTPServer/logs/access_log` command.

Enabling VNC server for maintenance

Before you begin

You must stop or configure the firewall (iptables) to allow VNC access. If the iptables are running or not configured to allow a VNC connection, you cannot access the system using VNC.

Procedure

1. Log in to the Client Enablement Services server using SSH terminal as user `craft/craft01` and then change the user to root using the **`su - root`** command and *root01* password.
2. Start the VNC server using the `vncserver` command.

   Note:

   When you run this command for the first time, you must set a password.

   a. To allow access to the desktop, you must edit the `xstartup` file. This file is located in the home directory of the user in the `~/.vnc/xstartup` path.

      Uncomment the following lines, that is, remove the # sign:

      - `#unset SESSION_MANAGER`
      - `#exec /etc/X11/xinit/xinitrc`

   b. To change the access password, type `vncpasswd`.
3. Stop the VNC server using the `vncserver –kill :1` command.

Chapter 3: Troubleshooting administration and configuration issues

Avaya one-X® Client Enablement Services server page error

When you try to access any page of the Client Enablement Services administration application except the Login page using the browser history, you might get the following error message:

```
Error encountered while initializing the page.
```

Proposed solution

Procedure

To clear the error message and access the page you want to, click on any tab or link on the Client Enablement Services administration application screen.

Therefore, as a best practice you should not use the browser history to access any page of the Client Enablement Services administration application except the Login page.

Client Enablement Services server does not start when you reboot the server from the CDOM

After the installation of the Client Enablement Services template, when you try to reboot the Client Enablement Services virtual machine from the System Platform Web console, the Client Enablement Services server does not start even though the CDOM displays the template state as `running`.

Proposed solution

Procedure

1. Log in to the DOM-0 CLI as root.

   Dom-0 is the primary domain of the server on which the System Platform is installed.

2. Reboot the DOM-0 using the command **reboot**.

Unable to log in the administration application using the service account

Sometimes the administrator is unable to log in the administration application using the service account. The system displays an error message:

```
You do not have the permissions required to access this page.
```

The `trace.log` file also displays authorization failed message.

Proposed solution

Procedure

1. Log in to the CLI of the Client Enablement Services server.
2. Restart the WAS using the command: **service 1xp restart**

Unable to log in the administration application, but able to log in the server CLI

Sometimes the administrator is unable to log in the administration application or the client application, but able to log in the Client Enablement Services server CLI.

Proposed solution

Procedure

1. Log in to the CLI of the Client Enablement Services server.
2. Restart the WAS using the command: **`service 1xp restart`**

Unable to listen to the on-hold music

During a bridge conference, if the participants on hold are not able to listen to the on-hold music, follow the steps in the proposed solution.

Proposed solution

Procedure

1. In the Client Enablement Services administration application, select the **Servers** tab.
2. From the left pane, select **Conferencing**.
   The Conferencing Servers page displays a list of the Conferencing servers configured on the Client Enablement Services server.
3. Click the name of a Conferencing server in the **Handle** column to display the View Conferencing Server page for the Conferencing server.
4. In the **BCAPI Host** field, configure the parameter music.source=<x> using the syntax <network address>, music.source=<x>.
   For example, *192.168.1.100, music.source=1*
5. Click **Save**.
6. Click the **Monitors** tab.
7. From the left pane, select **Conferencing**.
8. Click **Restart** to stop and restart the services.

All users not imported in user data migration

User Data migration from Avaya one-X® Portal server Release 5.2 or Client Enablement Services server Release 6.1 server does not import all users.

Proposed resolution

Procedure

1. Ensure that the names of the servers in the Avaya one-X® Portal server Release 5.2 or the source Client Enablement Services server and the target Client Enablement Services server Release 6.1 are same.
2. Ensure that the system profile and group profile names and properties in the Avaya one-X® Portal server Release 5.2 or the source Client Enablement Services server and in the target Client Enablement Services server Release 6.1 are same.
3. In the target Client Enablement Services server Release 6.1 administration application, go to the **Users** > **Unprovisioned users** page, and ensure that users you are migrating are listed in the Unprovisioned users page.

   Mobile resource migration is not a part of data migration. Administrator should assign the mobile resource separately to the users after data migration is complete. For detailed information, see *Assigning a Mobile Telephony resource to a user* section in the *Administering Avaya one-X® Client Enablement Services* guide.

System Manager certificate is not imported after installation

If the System Manager certificate is not imported after Client Enablement Services installation or if there is any change in the System Manager Host or IP address, you should check the Presence Services server.

Proposed solution

About this task

Perform the following steps when the Presence Services is in running state.

Procedure

1. Ensure that the System Manager host and port details are included in the`/opt/avaya/1xp/config.properties` file.
   For example:
   ```
   smgr.host=135.9.2 x.xx
   smgr.port=443
   ```
2. Reassign the certificate from System Manager.
   a. In the SSH terminal session on the Client Enablement Services 6.1 server, log in as root.
   b. Go to `/opt/avaya/1xp` directory using the command: `cd /opt/avaya/1xp`
   c. Renew the certificate using the command: `./run_config_smgr_jython.pl <smgr_enrollment_password>`
   d. Restart the Client Enablement Services server.
3. Verify whether the System Manager and Presence Services server are reachable by the FQDN.
   If they are not reachable, add entries to `/etc/hosts`.

CPU usage spikes and the administrator is unable to log in to the administration application

When the system administrator sets a high level of logging in the Logging page in the administration application, the CPU usage spikes abnormally and the system administrator is unable to log in to the administration application.

For example, if in the **Current Other Loggers** section, the logger is set to ***** and level is set to **ALL**, the CPU usage spikes abnormally.

On the Client Enablement Services server CLI, type the command: **`top`**

The system displays the CPU usage as 750%.

Proposed solution

Procedure

1. Log in to the DOM-0 CLI as root.
   Dom-0 is the primary domain of the server on which the System Platform is installed.
2. Reboot the DOM-0 using the command: **`reboot`**.

3. If the WAS does not start, you have to start the WAS using the command: **`service 1xp start`**

   The WAS takes approximately 10 minutes to start.
4. Log in to the administration application.
   The administration application might be slow in performance.
5. Click the **System** tab.
6. From the left navigation pane, select **Logging**.
7. In the **Other Loggers** section, set the level of ***** logger to **Off**.
8. Click **Save**.

Modular Messaging connection error

When you upgrade the Client Enablement Services server, you might get a Modular Messaging connection failure error and voice mail do not get downloaded to the Avaya one-X® Mobile client application.

Proposed resolution

Procedure

1. In the administration application, click the **Servers** tab.
2. From the left navigation pane, select **Voice Messaging**.
3. Click the name of a Modular Messaging server in the **Handle** column to display the Modify Voice Messaging Server Configuration page for the server.
4. In the **SSL Certificate** field, click **Retrieve SSL Certificate**.
   The button in the **SSL Certificate** field changes to **Remove SSL Certificate**.
5. Click **Save** to update the server.
6. Click the **Monitors** tab.
7. From the left navigation pane, select **Voice Messaging**.
8. Click **Restart** to stop and restart the service.
9. Restart the WAS.
   a. SSH in to the Client Enablement Services terminal using Putty.
   b. On the shell prompt, type the **`service 1xp restart`** command to restart the Client Enablement Services server.

The system prompts you to enter your user name and password when it tries to stop the server.

c. Enter your admin_user_name and admin_user_password.
This stops and restarts the Client Enablement Services server.

10. Select the **Servers** tab.
11. From the left navigation pane, select **Voice Messaging**.
12. Click the name of a Modular Messaging server in the **Handle** column to display the Modify Voice Messaging Server Configuration page for the server.
13. Click **Test** to run a short test of your changes.
The results of the test should display the Modular Messaging server as connected.

Users not present in the Unprovisioned user list

User is not present in the Unprovisioned Users list in the **Users** > **Unprovisioned users** page in the Client Enablement Services administration application.

Proposed solution

Procedure

1. Log in to the LDAP.
2. Ensure that the user is present in the LDAP.
3. In LDAP ensure that the user is a member of the Client Enablement Services User Security group.
4. In the administration application, select the **Scheduler** tab.
5. In the left navigation pane, select **Enterprise Directory Synchronization**.
6. Click **Run Incremental Sync Now** for an incremental synchronization to run immediately.

   To track the status of this operation, refresh the page.

   For detailed information on scheduling Enterprise Directory synchronization, see *Scheduling Enterprise Directory Synchronization* section in the *Administering Avaya one-X® Client Enablement Services* guide.
7. To verify whether the user is present in the unprovisioned users list, in the administration application, select the **Users** tab.
8. In the left navigation pane, select **Unprovisioned Users**.

You can search the unprovisioned users on the Client Enablement Services system on the Unprovisioned Users page.

For more information on provisioning a user, see *Provisioning an unprovisioned user* section in the *Administering Avaya one-X® Client Enablement Services* guide.

Unable to connect to Communication Manager

If the Client Enablement Services server is not able to connect to the Communication Manager system configured on the Client Enablement Services administration application after you make changes to the Trunk group or the Signaling group on Communication Manager, the system displays the following error:

`CM` *`XXX.XXX.XXX.XXX`* `not accepting SIP messages from server` *`YYY.YYY.YYY.YYY`*

In this error message, *XXX.XXX.XXX.XXX* is the IP address of Communication Manager and *YYY.YYY.YYY.YYY* is the IP address of the Client Enablement Services server.

Proposed solution

Before you begin

Follow these steps only when the **Allow Direct Connection to CM** check box is selected on the **Servers** > **Telephony Servers** page in the Client Enablement Services administration application.

Procedure

1. Verify that the **Far-end domain** field value mentioned for the SIP signaling group on Communication Manager and the value mentioned in the **Domain** field for the SIP Local server on the Client Enablement Services administration application are same.
2. Verify that the **Far-end Listen Port** field value on Communication Manager and the value mentioned in the **Port** field for the SIP Local server on the Client Enablement Services administration application are same.
3. Verify that the **Near-end Listen Port** field value on Communication Manager and the value mentioned in the **SIP Remote Port** field for the Telephony server on the Client Enablement Services administration application are same.
4. Ensure that the protocol configured for SIP signaling group on Communication Manager and the **SIP Local** configuration on Client Enablement Services

administration application are same. The protocol should be using either TCP or TLS.

5. Verify that the **Authoritative Domain** field value on the change ip-network-region page on Communication Manager and the value mentioned in the **Domain** field for the Telephony server in the Client Enablement Services administration application are same.
6. If you have connected the Client Enablement Services server using secure connection or TLS over SIP trunk to Communication Manager, ensure that the certificate from Client Enablement Services is installed on Communication Manager.

   For more details on installing a certificate on Communication Manager, see *Administering Avaya Aura® Communication Manager*.

ONE-X mapping of user extension not visible on Communication Manager

Sometimes the ONE-X mapping for a user extension is not visible in Communication Manager even if a mobile telephony resource is configured for the user in the Client Enablement Services administration application.

The extension of the user is set in Communication Manager as a ONE-X mapping when the system administrator configures the mobile number of the user in the mobile telephony resource page in the Client Enablement Services administration application.

For detailed steps on assigning a mobile telephony resource to the user, see Chapter 4, “User Administration,” in the *Administering Avaya one-X® Client Enablement Services* guide.

Proposed solution 1

Procedure

1. In the administration application, select the **Monitors** tab.
2. From the left navigation pane, select **Telephony**.
3. Verify that the **State** of the SipService is **Available**.
   If the service is not available, click **Restart** to restart the service.
4. Check the Communication Manager adapter to verify if the connection between Client Enablement Services and Communication Manager is directly established.

   The **Type** field displays the type of the server, that is **cm** and the **State** field should be **Connected**.

5. Check the Session Manager adapter to verify if the connection between Client Enablement Services and Communication Manager is through Session Manager.

   The **Type** field displays the type of the server, that is **cm** or **sm** and the **State** field should be **Connected**. In a set up where the connection is through Session Manager, you must verify the state of Session Manager and Communication Manager both.

   If the system displays the connection as Idle or Down, click **Restart** to bring the adapter to connected state.

6. In Communication Manager, use the command **`display off-pbx-telephone station-mapping <extension of the user>`** to verify that the user account is controlled by Client Enablement Services.
   There should be a ONE-X mapping for the extension of the user with two zeros appended before the extension of the user. For example, 00<*extension of the user*>.

7. On page Status Station<extension>, verify the value of the field **one-X Server Status**.
   The field value should be set to one of the following: **trigger**, **normal**, **voicemail**, or **no-ring**. If the field value is **N/A**, it means that the station is not controlled by Client Enablement Services.

Proposed solution 2

Procedure

1. In the administration application, select the **Users** tab.
2. From the left navigation pane, select **Provisioned Users**.
3. On the Provisioned Users page, search for the user whose ONE-X Mapping is not visible on Communication Manager.
4. Click **Disable** to change the user state.
5. When the user state changes to disabled, click **Enable** to enable the user state.
6. In Communication Manager, use the command **`display off-pbx-telephone station-mapping <extension of the user>`** to verify that the user account is controlled by Client Enablement Services.
   There should be a ONE-X mapping for the extension of the user with two zeros appended before the extension of the user. For example, 00<*extension of the user*>.
7. On page Status Station<extension>, verify the value of the field **one-X Server Status**.

The field value should be set to one of the following: **trigger**, **normal**, **voicemail**, or **no-ring**. If the field value is **N/A**, it means that the station is not controlled by Client Enablement Services.

Proposed solution 3

Procedure

1. On Communication Manager, check if unused PBFMC licenses and EC500 licenses are available.

   Each station when controlled by Client Enablement Services consumes 1 PBFMC and 1 EC500 license, regardless of the number of ONE-X mappings that it acquires. If these licenses are not available, add these licenses on Communication Manager first and then perform the following steps.
2. In the administration application, select the **Users** tab.
3. From the left navigation pane, select **Provisioned Users**.
4. On the Provisioned Users page, search for the user whose ONE-X Mapping is not visible on Communication Manager.
5. Click **Disable** to change the user state.
6. When the user state changes to disabled, click **Enable** to enable the user state.
7. In Communication Manager, use the command **`display off-pbx-telephone station-mapping <extension of the user>`** to verify that the user account is controlled by Client Enablement Services.
   There should be a ONE-X mapping for the extension of the user with two zeros appended before the extension of the user. For example, 00<*extension of the user*>.
8. On page Status Station<extension>, verify the value of the field **one-X Server Status**.
   The field value should be set to one of the following: **trigger**, **normal**, **voicemail**, or **no-ring**. If the field value is **N/A**, it means that the station is not controlled by Client Enablement Services.

ONE-X mapping of mobile number entered in the client application not visible in Communication Manager

When a user enters the mobile number on the account information page in the client application, the ONE-X mapping for that mobile number does not get mapped on

Communication Manager if the same number is already mapped on Communication Manager for another extension number.

The client application displays an error message when users try to do this mapping.

Proposed solution

Procedure

1. Ensure that the mobile number is not mapped to any other extension on Communication Manager.
   a. Log in to Communication Manager.
   b. Type the command: **`list off-pbx-telephone station-mapping xxxx`**

      In this command, xxxx is the mobile number that is mapped on the Communication Manager for a user.

      The system displays all numbers that are mapped on Communication Manager for the user. If this number is already mapped for some other extension, Communication Manager displays the extension for which number is mapped.
2. If the existing mapping is a manually mapping for the user extension for features such as EC500, CSP on Communication Manager, access the Change off-pbx-telephone station-mapping xxxx page and remove the mapping.

   xxxx is the station assigned to the user extension.
3. If the existing mapping is a ONE-X mapping, perform the following steps:
   a. In the administration application, disable the user whose extension is already mapped to the mobile number.
   b. Update the mobile number on the Mobile Telephony resource page.

      The system administrator can also keep the mobile number field blank if there is no information on the new mobile number of the user.
   c. Enable the user.

   For more information on enabling a user, disabling a user, and assigning a mobile telephony resource to the user, see Chapter 4, “User Administration,” in the *Administering Avaya one-X® Client Enablement Services* guide.
4. Update the mobile number on the Mobile Telephony resource page for the user who is trying to update the mobile number or the system administrator can request the user to add the mobile number in the client application.

ONE-X mapping is getting set to termination mode in Communication Manager

When the system administrator configures the mobile number of a user in the administration application, the ONE-X mapping for that mobile number gets set to termination mode in Communication Manager if the same number is already mapped in Communication Manager for another extension number.

The mobile number of the user is set in Communication Manager as a ONE-X mapping when either the system administrator configures the mobile number of the user on the mobile telephony resource page in the Client Enablement Services administration application or the user enters the mobile number on the account information page in the client application.

To view the ONE-X Mapping on Communication Manager, the system administrator must assign a mobile telephony resource to the user in the administration application.

For detailed steps on assigning a telephony resource to the user, see Chapter 4, “User Administration,” in the *Administering Avaya one-X® Client Enablement Services* guide.

Proposed solution

Procedure

1. Ensure that the number is not mapped for any other extension in Communication Manager.
   a. Log in to Communication Manager.
   b. Type the command: **`list off-pbx-telephone station-mapping xxxx`**

      In this step, xxxx is the number that is mapped in Communication Manager for a user.

      The system displays all numbers that are mapped in Communication Manager for users. If this number is already mapped for some other extension, Communication Manager displays the extension for which number is mapped.
2. If the existing mapping is manually mapped for the user extension for features such as EC500, CSP in Communication Manager, access the Change off-pbx-telephone station-mapping xxxx page and remove the mapping.
3. If the existing mapping is a ONE-X mapping, perform the following steps:
   a. In the administration application, disable the user whose extension is already mapped to the mobile number.
   b. Update the mobile number to the new mobile number of the user on the Mobile Telephony resource page.

The system administrator can also keep the mobile number field blank if there is no information on the new mobile number of the user.

c. Enable the user.

For more information on enabling a user, disabling a user, and assigning a telephony resource to a user, see Chapter 4 “User Administration,” in the *Administering Avaya one-X® Client Enablement Services* guide.

4. Update the mobile number on the Mobile Telephony resource page for the user for whom you are trying to update the mobile number.
The number is now set in Both mode in Communication Manager for the user extension.

Unable to clear ONE-X Mappings on Communication Manager

All provisioned users on the Client Enablement Services server consume one PBFMC license and one EC500 license. Therefore, it is important that when you delete a user from the Client Enablement Services server, the ONE-X mapping for the user on Communication Manager is also deleted.

This ONE-X mapping is deleted automatically from Communication Manager when a user is deleted from the Client Enablement Services server. However, it might happen that even though the user is deleted from the Client Enablement Services server, the user account still consumes a license on Communication Manager by retaining the ONE-X mapping and control of the user extension on the Client Enablement Services server.

Proposed solution

Procedure

1. Create a new COR on Communication Manager.
2. Open the COR using the command: **`change COR<COR number assigned to the user extension>`**
3. On page 3 of the COR, set the **one-X Server Access** field to **N**.
4. Assign this COR to the station whose ONE-X mapping you have to delete.

   The ONE-X mapping and Client Enablement Services control are not required now. However, you must note the old COR number before changing the COR number.

   On changing the COR of the station, the ONE-X mapping is immediately removed and the Client Enablement Services server control of the station is removed on Communication Manager.

5. Ensure that the mappings are removed on Communication Manager by using the command **`display off-pbx-telephone station-mapping xxxx`**
   In this command, xxxx is the extension of the station.
6. Change the COR of the station to the old COR value.
   Old COR value is the value of the COR before you created and assigned a new COR to the user extension.

Client Enablement Services user mapping is not in sync with Communication Manager

When you restart Communication Manager, the one-X mappings on Communication Manager are lost and features enabled by Client Enablement Services on extensions of users are disabled temporarily. However, when the link between Client Enablement Services and Communication Manager comes up, the user mappings are restored automatically on Communication Manager and all features are enabled.

The link comes up automatically in approximately 10 to 15 minutes, and this time depends on the number of users provisioned on the Client Enablement Services server.

Proposed solution

About this task

If the mappings are not restored automatically, you should restart the Communication Manager service adapter from the Client Enablement Services administration application. Perform the following steps:

Procedure

1. Click the **Monitors** tab.
2. In the left pane, select **Telephony**.
3. In the section that displays the details of Communication Manager Service, click **Restart** in the **Action** box.
   The system restarts the Communication Manager service adapter.

Unable to administer statistics table

When you enable collection for Performance statistics and Feature Usage statistics in the Client Enablement Services administration application, you must also schedule the cleanup

settings for these statistics. If you do not schedule the cleanup settings, the statistics table becomes very large in size and it becomes impossible to administer the table.

If you forget to schedule the cleanup settings or the scheduler did not run and the statistics table has become very large in size, you can use a shell script to reset the statistics.

Proposed solution

Procedure

1. On the Client Enablement Services server, log in as a dbinst user.
2. Type `su - dbinst`.
3. Change directory to `/opt/avaya/1xP/`.
4. Enter the command **`./reset_stats.sh roinst`**
   This script cleans up all statistics data.

   Note:

   You should execute this script as a database instance user. This script receives the read only user name of the database as a parameter.

   On successful execution of the script, the output is similar to as below.

```
[dbinst@<machine_name> 1xp]$ ./reset_stats.sh roinst
Clean stats
Database Connection Information

 Database server        = DB2/LINUXX8664 9.7.0
 SQL authorization ID   = DBINST
 Local database alias   = ACPDB

DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
DB20000I  The SQL DISCONNECT command completed successfully.
Set permissions on statistics for roinst
   Database Connection Information

 Database server        = DB2/LINUXX8664 9.7.0
 SQL authorization ID   = DBINST
 Local database alias   = ACPDB

DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.
DB20000I  The SQL command completed successfully.

DB20000I  The SQL DISCONNECT command completed successfully.
DB20000I  The TERMINATE command completed successfully.
```

Two handset server process running

There are two handset server processes running. This problem happens in a co-resident handset server installation.

Proposed solution

Procedure

1. List all process IDs using the command **`ps –ef | grep Rout*`**
2. Find the process ID of the two handset server processes from the list.
3. Kill the process IDs using the command **`kill -9 <pid>`**
4. Start the handset server using the command **`service handset_server start`**
5. In the Client Enablement Services administration application, go to the **Monitors** tab > Handset page.
6. Click **Restart** to restart the handset service adapter.
7. Verify that the handset server is connected to the handset services.
   a. Type the command **`cd $HSPATH/logs`**.
   b. In the `server.log` file, ensure that the file displays the message: `pipeline is up`

Handset server not up after a system restart

Handset server does not come up after a Client Enablement Services system restart or a WAS restart.

Proposed solution

Procedure

1. Log in to the machine where you have installed the handset server.
2. Run the command **`service handset_server start`**

The handset server comes up.

Unable to trim handset server log file

Due to the stdout logging, the startup scripts are piping all data to the `server.log` file. As a result, the administrator is unable to trim the log file.

Proposed solution

Procedure

1. In the Handset server, open the `/opt/avaya/HandsetServer/log4j.properties` file.
2. Change the `log4j.rootLogger=ALL, console, acp_appender, acp_appender_errors` line to `log4j.rootLogger=ALL, acp_appender, acp_appender_errors`
   This removes the stdout logging. The log4j logging logs the files in the location `/appsvr/logs` because the server is now running under the appsvr account.

   The logs are also getting trimmed because they are under the control of the RollingFileAppender of log4j.

Unable to save mobile telephony resource for a user

The **Mobile SMS Address** field on the Update Resource page for the Mobile Telephony resource assigned to a user displays the SMS address configured by the user in the Avaya one-X® Mobile client application. However, if the user does not configure the SMS address properly or the SMS address is incomplete, administrator cannot update the Mobile Telephony resource for the user.

The Client Enablement Services administration application displays a similar error message: `Value of property is invalid /SipCM.1.2/siptelephony.1.2/CM/tel.resource.mobile.smsaddress: xyz@`

In this example, user has entered only *xyz@* in the **SMS address** field in the Avaya one-X® Mobile client application. Therefore, the administration application displays only *xyz@* in the **Mobile SMS Address** field.

Proposed solution

About this task

The administrator should tell the user to enter a proper SMS address in the Avaya one-X® Mobile client application. For example, *xxxxx@abc.com*. If the administrator is unable to contact the user, administrator should follow these steps:

Procedure

1. In the administration application, select the **Users** tab.
2. From the left pane, select **Provisioned Users**.
3. On the Provisioned Users page, search for and select the user for whom you want to update the mobile telephony resource.
4. On the View User page, click **Disable** in the **State** field.
   The system disables the user account in the Client Enablement Services system.
5. In the **Mobile Telephony** box, click **Update**.
6. On the Update Resource page, click **Delete**.
   The system displays the View User page.
7. In the **Mobile Telephony** group box, click **Add**.
8. On the Add Resource page, update the fields with the updated information.
   For more information on field descriptions, see Chapter 4 “User Administration,” in the *Administering Avaya one-X® Client Enablement Services* guide.
9. Click **OK** to save your changes.
10. On the View User page, click **Enable** in the **State** field.
    The system enables the user account in the Client Enablement Services system.

Unable to configure mobile number in Avaya one-X® Mobile client application

The Avaya one-X® Mobile client application displays an error message when the user tries to configure the mobile number or ring phone number in the client application. The system displays the following error message: `Unable to Validate Phone Number`.

This problem happens if the mobile number the user is trying to configure is not routable as per the ARS table configured in Communication Manager or the same mobile number is already mapped to any other extension on Communication Manager.

Proposed solution 1

Procedure

1. On the Client Enablement Services administration application, select the **Servers** tab.
2. From the left navigation pane, select **Dial Plan**.
3. On the Dial Plans page, click the dial plan configured for the user.
4. On the Modify Dial Plan page, enter the mobile number the user is trying to configure in the **Number to Transform** field and click **Transform**.
   In the output of the **Conversion from configured string to PBX (Extension to Cellular Feature)** field, the system should display the number that is routable as per the ARS table configured in Communication Manager.

   If the number displayed is not routable as per the ARS table configured in Communication Manager, the administrator should either modify the dial plan in the Client Enablement Services administration application or make changes in the ARS routing table of Communication Manager such that the number becomes routable.

Proposed solution 2

About this task

Perform the following steps to ensure that the mobile number the user is trying to configure is not mapped to any extension on Communication Manager.

Procedure

1. Log in to Communication Manager.
2. Type the command: **`list off-pbx-telephone station-mapping xxxx`**

   In this command *xxxx* is the mobile number of the user.

   If the mobile number is already mapped to an extension on Communication Manager, the system displays the mobile number and the extension the mobile number is mapped to.
3. Delete the existing mapping in Communication Manager, so that the user can configure the same mobile number in the client application.

User unable to log in the Avaya one-X® Mobile client application

User is not able to log in to the Avaya one-X® Mobile client application. The application displays the following error message: `No Route to Server`.

Proposed solution

Procedure

1. Ensure that the user is provisioned in the Client Enablement Services administration application.
   a. Select the **Users** tab.
   b. From the left pane, select **Provisioned Users**.
      The system displays the various criteria you can use to search a provisioned user.
   c. Search for the user using one of the search criteria, and click **Search** to display a list of the desired users.
2. Ensure that the Telephony resource and the Mobile telephony resource are assigned to the user.
   a. Click the **Users** tab.
   b. From the left pane, select **Provisioned Users**.
   c. Search for and select the user for whom you want verify the resource.
   d. Verify whether the current state of the user account is **Enabled**.
   e. Verify whether the **Telephony** group box displays the details of the telephony resource assigned to the user and the **Mobile Telephony** group box displays the details of the mobile telephony resource assigned to the user.
      If one or both resources are not assigned to the user, assign the resource to the user. For detailed steps on assigning a resource to a user, see *Assigning a Telephony resource to a user* section and *Assigning a Mobile Telephony resource to a user* section in the *Administering Avaya one-X® Client Enablement Services guide.*
3. From the **Monitors** tab in the Client Enablement Services administration application, ensure that the Handset server and Handset services are running properly.
4. In Communication Manager, use the command **`display off-pbx-telephone station-mapping`** to verify that the user account is registered by Client Enablement Services.

5. Restart the Handset server using the command **`service handset_server restart`**
6. In the Client Enablement Services administration application, select the **Monitors** tab > **Handset**, and click **Restart** to restart the Handset service.
7. The user should try again to log in to the client application.

User unable to log in the Avaya one-X® Mobile client application after Client Enablement Services installation or upgrade

After the Client Enablement Services server installation or upgrade, user is unable to log in the client application, and the application displays the following error message: `Server not responding. Try again later.`

Proposed solution

About this task

If you have upgraded the Client Enablement Services server from Release 6.1, follow these steps after you complete the upgrade.

If you have done a fresh installation of the Client Enablement Services server, follow these steps after you complete the provisioning process for all users. For more information on provisioning a user, see the *Provisioning a user* section in the *Administering Avaya one-X® Client Enablement Services* guide.

Procedure

1. In the Client Enablement Services administration application, select the **Monitors** tab.
2. From the left navigation pane, select **Handset**.
3. On the Monitor Non Adapter Services page, click **Restart** to restart the Handset service.
4. Restart the Handset server using the command **`service handset_server restart`**
5. The user should try again to log in to the client application.

Unable to view the Avaya one-X® Mobile build

Unable to view the Avaya one-X® Mobile build on the hosted HTTP server, where the build was uploaded.

Proposed solution

Procedure

1. On the Client Enablement Services administration application, go to the **System** tab > Mobile Applications page.
2. Verify that the corresponding build has been uploaded on the server.
3. On the Mobile Applications page, click the link in the **Version** column to display the Mobile Application Configuration page for a mobile application.
4. Ensure that the **Release Status** of the build is **Active**.
5. Ensure that a higher version of the same build is not present in the **Active** state on the server.
6. If the problem still persists, delete the build and reload the build to the HTTP server.

   For more information on uploading a build, see the *Mobile Applications* section in the *Administering Avaya one-X® Client Enablement Services* guide.

Mobile client application prompts the user to enter account information again

When the system administrator disables a user account while the user had an active Avaya one-X® Mobile client application session, the client application prompts the user to enter account information again after the system administrator enables the user account.

Proposed solution

Procedure

The system administrator must always kill the user sessions before disabling a user.

For detailed steps, see the *Logging off and Killing user sessions* section in the *Administering Avaya one-X® Client Enablement Services* guide.

Call logs not visible

Call logs are not visible in the Avaya one-X® Mobile client application.

Proposed solution

Procedure

1. On the Client Enablement Services administration application, click the **Users** tab.
2. In the left navigation pane, click **System Profile**.
3. On the System Profile page, ensure the **Extension Contact Logging (SipService)** property is set to **24*7**.
4. In the left navigation pane, click **Group Profile**.
5. On the System Profile page, ensure the **Extension Contact Logging (SipService)** property is set to **24*7**.

Voice messaging server certificate imported successfully, but the administration application still displays the Retrieve SSL Certificate button

Administrator must import the SSL certificate when configuring a voice messaging server in the Client Enablement Services administration application. Even after a successful import of the SSL certificate, if the administration application still displays the **Retrieve SSL Certificate** button, you must check the **IMAP Host** field for any leading or trailing space.

Proposed solution

Procedure

1. Log in the Client Enablement Services administration application.
2. Select the **Servers** tab.
3. From the left pane, select **Voice Messaging**.
4. Click the name of a voice messaging server in the **Handle** column to display the Modify Voice Messaging Server Configuration page for the server.
5. Check the **IMAP Host** field for any leading or trailing space. If there is any leading or trailing space, you must delete the space.
6. In the **SSL Certificate** section, click **Retrieve SSL Certificate** .
   The button label must change to **Remove SSL Certificate**. This label indicates that the security certificate exists for the voice messaging server.
7. Click **Save**.

Voice mail pin not accepted by the client application

When the user tries to install and configure the Avaya one-X® Mobile client application on a mobile device and the client application does not accept the voice mail pin entered by the user, you must check the subscriber features of the class of service defined for the user in the Modular Messaging server or the Avaya Aura® Messaging server.

If you have a Modular Messaging installation, follow the procedure in proposed solution 1.

If you have an Avaya Aura® Messaging installation, follow the procedure in proposed solution 2.

Proposed solution 1

Procedure

1. Log in to the Modular Messaging MSS administration application.
2. From the left navigation pane, under **Messaging Administration**, click the **Classes-of-Service** link.
3. On the Manage Class-of-Service page, select the COS for which the user mailbox is configured from the list of COS .

4. Click **Edit the Selected COS**.
5. On the Edit a Class-of-Service page, under **Subscriber Features and Services**, set the value to **Restrict Client Access** field to **No**.

   If this parameter is set to **No**, subscribers can access their mailboxes from IMAP4 and POP3 clients, Modular Messaging Outlook Client, and Modular Messaging Restricted Outlook Client.

   If this parameter is set to **Yes**, subscribers can access their mailboxes only from Avaya proprietary interfaces or clients.

   The Restrict Client Access control is overridden if the **Privacy Enforcement Level** value is set to **Full** in the Voice Mail System Configuration (VMSC) program on the Messaging Application Server (MAS).

   For more on information on managing a class of service, see the *Administering classes of service* section in the *Avaya Modular Messaging for Avaya MSS Release 5.2 Installation and Upgrades* guide.

   For more on information on privacy enforcement level, see the *Messaging Dialog Box* section in the *Avaya Modular Messaging Release 5.2 with the Avaya MSS MAS Administration Guide* guide.

Proposed solution 2

Procedure

1. Log in to the Messaging server system management interface.
2. From the left navigation pane, under **Messaging System (Storage)**, click the **Class of Service** link.
3. Verify that the Class of Service assigned to the user has all required permissions. If the Class of Service assigned to the user does not have required permissions, you can assign a different class of service to the user.

   For more on information on managing a class of service, see the *Administering Avaya Aura® Messaging* guide.
4. From the left navigation pane, under **Reports (Storage)**, select **Users**.
5. On the Reports page, click the link in the **Mailbox** column for the user.
6. On the User Management > Properties for <user name> page, verify the following:
   a. The **Password** field has a value.
   b. The **User must change voice messaging password at next logon** check box is not selected.
   c. The **Locked out from voice messaging** check box is not selected.

7. Ensure that the user can receive and read the voice mails from the desk phone of the user using this password.

ARS digit included in the call log entry when callback is made through the client application

When the user makes a callback call using the Avaya one-X® Mobile client application, the call log entry in the History page displays the called number with the ARS number appended to the original number.

For example, when the user calls the number 9049007970 from the client application, the call log entry displays this number as +9199049007970. In this example, 9 is the ARS number and it has been appended to the called number. The call log entry should display the number as +919049007970.

Proposed solution

Procedure

1. In the Client Enablement Services administration application, select the **Servers** tab.
2. In the left navigation pane, select **Telephony**.
3. On the Telephony Servers page, select a Telephony server in the **Handle** column.
4. On the View Telephony Server page, select the **Remove ARS from dialed number before converting to display string** check box.
5. Click **Save**.

Presence service is not in connected state after restart of the Presence Services server

Sometimes when the Presence Services server is restarted, the Presence service of the Client Enablement Services server does not connect automatically. Even if the administrator tries to stop the Presence service from the Monitors page on the administration application, the service enters a stop phase that does not end. If the administrator tries to restart the WAS using the **`service 1xp stop`** command, this also does not work.

Sometimes, the presence adapter is connected, but the presence status does not get updated properly on the Avaya one-X® Mobile client application.

Proposed solution

About this task

To fix this problem, you must restart the Client Enablement Services server from System Platform.

Procedure

1. Log in to System Platform.
2. On the left pane, click **Virtual Machine Management** > **Manage**.
3. On the Virtual Machine List page, click the link of the Client Enablement Services virtual machine.
4. On the Virtual Machine Configuration Parameters page, click **Reboot**.

Avaya one-X® Mobile login failure

Sometimes, when the user launches the Avaya one-X® Mobile client application, the client application might get stuck at the login page.

Proposed solution

Procedure

1. In case of a co resident Handset server installation, SSH in to the Client Enablement Services terminal using Putty or in case of a standalone Handset server installation, log in to the Handset server.
2. Restart the Handset server using the command **`service handset_server restart`**.
3. In the Client Enablement Services administration application, select the **Monitors** tab.
4. In the left navigation pane, select **Handset**.
5. Click **Restart** to restart the Handset service.

Unable to edit personal contact resource assigned to a user

After upgrading the Client Enablement Services server, the system administrator is unable to edit the personal contact resource assigned to a user or delete the user, if the user had a personal contact resource assigned before the system upgrade.

The system displays the following error message: `User <user name> is enabled and it may be active; Logoff sessions and disable the user`.

Proposed solution

Procedure

1. Log in to the Client Enablement Services server CLI.
2. Stop the server using the command: **`service 1xp stop`**
3. Connect to the database using the command: **`su – dbinst`**
4. Stop the database using the command: **`db2stop`**
5. Start the database using the command: **`db2start`**
6. Start the Client Enablement Services server using the command: **`service 1xp start`**
7. Log in to the Client Enablement Services administration application.
8. Delete the user.

   For detailed steps, see the *Deleting provisioned users* section in the *Administering Avaya one-X® Client Enablement Services* guide.
9. Provision the user again.

   For detailed steps, see the *Provisioning an unprovisioned user* section in the *Administering Avaya one-X® Client Enablement Services* guide.

Dialed string conversion number displayed on the administration application not same as the number displayed on the client application

This problem happens when the system administrator sets the **Extension Contact Logging (SipService)** property in **System profile** is set to **24*7** in the Client Enablement Services administration application.

For example, in the Client Enablement Services administration application Dial plan page, you configure a dial plan such that the number 09860695400 is transformed as +919860695400 in the **Conversion from ANI to displayed string in Client** field. But, when the user makes a call back to this number, it is displayed as +09860695400 in the client application.

Proposed solution

Procedure

1. In the Client Enablement Services administration application, select the **Servers** tab.
2. In the left navigation pane, select **Telephony**.
3. On the Telephony Servers page, select a Telephony server in the **Handle** column.
4. On the View Telephony Server page, select the **Remove ARS from dialed number before converting to display string** check box.
5. Click **Save**.

Multiple Avaya one-X® Mobile sessions active in the administration application

In Client Enablement Services administration application, multiple mobile sessions are active for a user on the View user page.

Proposed solution

Procedure

1. In the Client Enablement Services administration application, select the **Users** tab.
2. In the left navigation pane, select **Provisioned Users**.
3. Search for and select the user whose session you want to end.
4. In the Sessions section, you can either log off the user session or kill the sessions:
   - click **Logoff Session** to log off the user from the current session.
   - click **Kill All Sessions** to kill all sessions of the user.
5. Click **Finished**.

Presence displayed as offline in the Avaya one-X® Mobile client application

Sometime the presence for a SIP user on the Avaya one-X® Mobile client application is displayed as Offline.

Proposed solution

Procedure

1. Log in to the System Manager administration application.
2. In the **Users** section, select **User Management**.
3. From the left navigation pane, click **Manage Users**.
4. On the User Management page, click **Advanced Search**.
5. In the **Criteria** field, enter the name of the user and click **Search**.
6. In the **Users** section, select the check box adjacent to the user name and click **Edit**.
7. On the User Profile Edit:<e-mail address of the user> page, click the **Communication Profile** tab.
8. Click the show/hide button in the **Endpoint Profile** section.

9. Click the **Endpoint Editor** button adjacent to the **Extension** field.
10. On the Edit Endpoint page, in the **General Options** tab, verify that the **Type of 3PCC Enabled** field value is set to **Avaya**.

    This value is available for SIP endpoints.
11. In the **Feature Options** tab, verify that the **IP SoftPhone** check box is selected.
12. Click **Done**.
13. On the User Profile Edit:<e-mail address of the user> page, click **Commit** if you have made any changes or click **Cancel**.

Unable to use voice mail features on Avaya one-X® Mobile client applications

To edit the voice mail resource assigned to a user, the administrator performs the following:

1. Disables a user while the user is logged in to the mobile application.
2. Kills the user sessions.
3. Deletes the voice mail resource.
4. Enables the user.
5. Adds the voice mail resource again.

After this sequence of events, the user might get the following error message after the user logs in to the client application: `Voicemail box administration failed`.

Proposed solution

Procedure

1. In the Client Enablement Services administration application, select the **Monitors** tab.
2. In the left navigation pane, select **Handset**.
3. Click **Restart** to restart the Handset service.

Unable to monitor audio transcoding service from the administration application

System administrator is unable to monitor the audio transcoding service from the Monitors page in the administration application. System display following error message:

```
Error encountered while initializing the page.
Exception in Internal Client API.
```

Proposed solution

Procedure

1. Log in to the Client Enablement Services CLI.
2. Restart the audio transcoding server using the command: **`service transcoding_server restart`**
   The system stops the audio transcoding server, and starts the server.
3. Verify the status of the audio transcoding server using the command: **`service transcoding_server status`**
   The system displays the status of server as running.
4. Log in to the Client Enablement Services administration application.
5. Click the **Monitors** tab.
6. From the left navigation pane, select **Audio Transcoding**.
   If the system displays the same error message, follow the steps below.
7. Log in to the WebSphere administration console.
8. From the left navigation pane, click **Applications**.
9. Click **Application Types**.
10. Click **WebSphere enterprise applications**.
11. On the Enterprise Applications page, select the check box adjacent to **1X_Adapter_AudioTranscoding**.
12. Click **Stop**.
13. When the stop process is complete, click **Start**.

WAS start or restart does not initialize the Client Enablement Services service due to database failure

Sometimes the **service 1xp start** or **service 1xp restart** commands to start or restart the WAS get paused indefinitely waiting for the database to start. This can happen if the database has encountered problems.

The system displays following message:

```
Starting WebSphere Application Server - server1 ...
waiting for db2
....
```

Proposed solution

Procedure

1. Press Ctrl + C to exit the process.
2. Connect to the database using the command: **su – dbinst**
3. Stop the database using the command: **db2stop**
4. Start the database using the command: **db2start**
   The system displays the message: `DB2START processing was successful`.
5. Exit the dbinst session using the command: **exit**
   This automatically brings the user to the previous login state that is the root user.
6. Start the WAS using the command: **service 1xp start**
   The system displays message similar as below:

```
Starting WebSphere Application Server - server1 ...
waiting for db2
. db2 running
ADMU0116I: Tool information is being logged in file
  /opt/IBM/WebSphere/AppServer70/profiles/default/logs/server1/
startServer.log
ADMU0128I: Starting tool with the default profile
ADMU3100I: Reading configuration for server: server1
ADMU3200I: Server launched. Waiting for initialization status.
```

WAS restart takes a longer time

When you restart the WAS using the **service 1xp restart** command, sometimes the command takes a longer time to execute, say 20 minutes or long or the process gets paused indefinitely.

Proposed solution

Procedure

1. Log in the Client Enablement Services server CLI as root.
2. Run the command **ps –ef | grep onexps** to get the process ID (pid) of the process running with UID as 'appsvr'.
3. Kill the restart process using the command: **kill -9 <pid>**
4. Reboot the Cdom from the CLI of the Cdom or the Web console.
5. Log in to the Client Enablement Services server CLI as root.
6. Stop the server using the command: **service 1xp stop**.
7. Start the server using the command: **service 1xp start**.

Heap dumps generated by the WAS makes the server unresponsive

The heap dumps generated by the WAS occupies all free disk space, and the Client Enablement Services server becomes unresponsive.

This problem is observed in Client Enablement Services Release 6.1 SP 1.

Proposed solution

Procedure

1. Log in to the System Manager administration application.
2. Under **Elements**, click **Routing** on the main page.

3. From the left navigation pane, select **SIP Entities**.
4. From the list of SIP entities on the SIP Entities page, click the SIP entity created for the Client Enablement Services server.
5. On the SIP Entity Details page, in the **SIP Link Monitoring** section, select **Link Monitoring Disabled** in the **SIP Link Monitoring** field.
6. Click **Commit**.

Message temp directory not copied on CDOM backup restore

When the system administrator restores the CDOM backup on the Client Enablement Services server, the Message temp directory of the voice messaging server might not be copied if the Message temp directory name has special characters.

Proposed solution

Procedure

1. Create a directory for the Voice Messaging server.

   Do not use special characters in the Message temp directory name.

   For more information, see the *Creating a directory for the Voice Messaging server* section in the *Administering Avaya one-X® Client Enablement Services* guide.
2. Modify the **Messages Temp Directory** field value of the Voice Messaging server on the Client Enablement Services administration application.

   For more information, see the *Modifying the Voice Messaging servers* section in the *Administering Avaya one-X® Client Enablement Services* guide.

Unable to delete a user from the administration application

Sometimes the administrator is unable to delete a user from the administration application even though the user is in the disabled state. The system displays the following error message:

```
User <user name> is enabled and it may be active; Logoff sessions and disable the user.
```

This problem happens because the handset services caches the user instance.

Proposed solution

Before you begin

The user must log off from the mobile client application before you follow these steps.

Procedure

1. Log in the administration application.
2. Click the **Users** tab.
3. From the left navigation pane, select **Provisioned Users**.
4. Search for and select the user you want to delete.
5. On the View User page, in the **Sessions** section, click **Kill All Sessions** to kill all active sessions of the user.
6. Click the **Monitors** tab.
7. From the left navigation pane, select **Handset**.
8. Click **Restart** to stop and restart the handset service.
9. Click the **Users** tab.
10. From the left navigation pane, select **Provisioned Users**.
11. Search for and select the user you want to delete.
12. On the View User page, click **Disable**.
    The system displays the message: `User has been disabled`
13. Click **Delete**.

Unable to enable or delete a user from the administration application

Sometimes, the system administrator is unable to enable a user who is in disabled state or delete the user from the Client Enablement Services administration application. The system displays an error message: `No user: <User name>`

This problem might occur because of data inconsistency. There might have been a change in the LDAP structure at the time of enterprise directory synchronization for the user.

Proposed solution

Before you begin

You need root access to connect to the database.

Procedure

1. Log in to the Client Enablement Services server through a putty terminal.
2. Type the command **`su –dbinst`**
3. To launch the db2 CLI, type **`db2`**
4. In the db2 command prompt, perform the following commands:
   a. connect to ACPDB.
   b. set schema ACP.
   c. update “user” set “acpStatus” =’p’ where “moniker” = '*replace-this-with-user-handle*’

      You must type these commands in the CLI, and not copy and paste the commands from this document. The quotes and double quotes in the document might have different ASCII codes than in the command line and might cause an error. In this command, the variable *replace-this-with-user-handle* is the handle of the user who you want to enable or delete. Note that this value must be surrounded by single quotes.
   d. disconnect ACPDB.
5. Exit the CLI by using the command **`quit`**.
6. Log out dbinst.
7. Stop the Client Enablement Services server using the command: **`service 1xp stop`**
8. Start the Client Enablement Services server using the command: **`service 1xp start`**
9. In the Client Enablement Services administration application, perform an enterprise directory synchronization.

   For more information, see the *Scheduling Enterprise Directory Synchronization* section in the *Administering Avaya one-X® Client Enablement Services* guide.
10. Log in to the Client Enablement Services administration application and enable the user.

    For more information, see the *Enabling or disabling a user account* section in the *Administering Avaya one-X® Client Enablement Services* guide.

User account deleted in the enterprise directory displays in the provisioned users list

After you delete a user account from the enterprise directory, and run an incremental enterprise directory synchronization on the Client Enablement Services administration application, the user account is still listed in the provisioned users list.

Proposed solution

About this task

You must run a full enterprise directory synchronization after you delete a user account from the enterprise directory.

Procedure

1. In the Client Enablement Services administration application, select the **Scheduler** tab.
2. In the left pane, select **Enterprise Directory Synchronization**.
3. Click **Run Full Sync Now** for a full enterprise directory synchronization.
4. Select the **Users** tab.
5. In the left pane, select **Provisioned Users**.
6. Search the user account you deleted from the enterprise directory.
   The user account is not in the provisioned users list.

Administrator is unable to log in the administration application, and users are unable to log in the client application

Sometimes the WAS stops responding or gets paused indefinitely, and the administrator is unable to log in the administration application. Users are also unable to log in the client application.

This problem might happen when the database stops responding or the response is very slow because the database empty disk space is very less or the disk space is full.

This problem might also happen if two or more conflicting commands are issued simultaneously. For example, if an administrator issues the service restart command and

another administrator begins the enterprise directory synchronization from the administration application almost at the same time or soon after the service restart command. In this case, all services had not stopped when the enterprise directory synchronization process begun. As a result, the server either responds very slowly or stops responding.

Proposed solution

Procedure

1. For data safety, perform a manual database backup using following steps:
   a. Log in to the Client Enablement Services server CLI as root.
   b. Stop the server using the command: **`service 1xp stop`**
   c. Log in as a dbinst user.
   d. Type: **`su - dbinst`**
   e. To start the db2 CLI, type **`db2`**
   f. Type: **`update dbm cfg using DIAGLEVEL 4`**
   g. Type: **`force application all`**
   h. Wait for a minute and stop the database using the command **`db2stop`**
   i. Start the database using the command **`db2start`**
   j. Connect to ACPDB.
   k. mtrk –i –v –d >db2mtrk1.log
   l. As a root user, execute: **`ipcs –a > ipcs1.log`**
   m. As a dbinst user, execute:**`db2`**
      This starts the db2 CLI.
   n. Type: **`select * from “ACP”.“systemConfig”`**
   o. Type: **`quiesce database immediate force connections`**
   p. Type: **`connect reset`**
   q. Backup database ACPDB to ‘<backup directory>' without prompting.
   r. Connect to ACPDB.
   s. Type: **`unquiesce database`**
   t. Type: **`connect reset`**
   u. Type: **`terminate`**
      Verify that the database backup file is created at the location specified.
2. Log in as a dbinst user.
3. Stop the database using the command **`db2stop`**
4. Start the database using the command **`db2start`**
5. Type: **`db2mtrk –i –v –d > db2mtrk2.log`**
6. Log in as root user, and type: **`ipcs –a > ipcs2.log`**

7. Start the server using the command: **service 1xp start**
8. Log in as a dbinst user.
9. In the db2 command prompt, connect to ACPDB.
10. Set schema ACP.
11. Create a temporary tablespace and table.
    This table is used to temporarily store personal contact addresses.
    a. Type: **create regular tablespace tempAddr in database partition group ibmdefaultgroup pagesize 4K managed by system using ('/home/dbinst/ACPDB/NODE0000/TEMPADDR') extentsize 32 prefetchsize 32 bufferpool ACP4K**
    b. Type: **create regular tablespace tempAddr in database partition group ibmdefaultgroup pagesize 4K managed by system using ('/home/dbinst/ACPDB/NODE0000/TEMPADDR') extentsize 32 prefetchsize 32 bufferpool ACP4K**
12. Temporarily save the personal contact addresses using the command: **insert into "tempAddress" (select * from "contactAddress" where "contactInfoId" in (select "id" from "contactInfo" where "type" = 'p'))**
13. Type: **select count(*) from "tempAddress"**
14. Clean all contact addresses using the command: **drop table "contactAddress"**
15. Recreate the contact address table and relations.
    a. Type: **create table "contactAddress" ("id" char (32) not null constraint "contactAddressPk" primary key, "type" char (1), "qualifier" char (1), "position" int not null default 0, "urlScheme" varchar (20), "addressString" varchar (512), "addressMatchString" varchar (512), "contactInfoId" char (32) not null, "isForInternalUse" char (1) default '0', "rowVersion" bigint, "source" varchar(255)) in contactAddr**
    b. Type: **alter table "contactAddress" add constraint "contactAddressFk1" foreign key ("contactInfoId") references "contactInfo" ("id") on delete cascade**
    c. Type: **create index "caTypeIx" on "contactAddress" ("type")**
    d. Type: **create index "caAddressMatchIx" on "contactAddress" ("addressMatchString")**
    e. Type: **create index "caAddressIx" on "contactAddress" ("addressString")**
    f. Type: **create index "caConInfoIdIx" on "contactAddress" ("contactInfoId")**

g. Type: **commit**

16. Add back the personal contact addresses using the command: **insert into "contactAddress" select * from "tempAddress"**
17. Start the Client Enablement Services server using the command: **service 1xp start**
18. Log in the administration application.
19. Select the **System** tab.
    a. From the left navigation pane, select **Enterprise Directory**.
    b. Click the name of a domain in the Modify LDAP Attribute Mappings to display the attribute names and their default values.
    c. Check that the LDAP attributes for **Email** and **Email2** do not point to the same LDAP attribute.
    If LDAP attribute map setting for both **Email** and **Email2** attribute has same value, remove the duplicate value and set it to a different value.
    d. Click **Save** to modify the mapping to that value.
20. Select the **Scheduler** tab.
    a. From the left navigation pane, select **Enterprise Directory**.
    b. Click **Run Full Sync Now** for an incremental synchronization to run immediately and incorporate these changes.
    c. Go back to the db2 CLI, and delete the temp table using the command: **drop table "tempAddress"**

Session Manager state is displayed as idle

In the Client Enablement Services administration application, the system displays the state of Session Manager as idle. The state is displayed as idle when either the Session Manager is down or the connection to Communication Manager through Session Manager fails and a direct connection is established between Client Enablement Services and Communication Manager.

Proposed solution

Procedure

1. Check if Session Manager is connected to the Client Enablement Services server.

a. In the Client Enablement Services administration application, select the **Servers** tab.
b. In the left navigation pane, select **Auxiliary Servers**.
c. On the Auxiliary Servers page, click the name of a Session Manager in the **Handle** field to test the connection.
d. Click **Test**.
The system displays whether the Session Manager is connected or not.

- If the Session Manager is connected, perform step 2.
- If the Session Manager is not connected, check the network connectivity between the two servers and also check if the Session Manager is up.

2. Restart the SIP Service adapter to restore connection through Session Manager.
   a. Select the **Servers** tab.
   b. In the left navigation pane, select **Telephony**.
   c. Under the **SipService** section, click **Restart** in the **Actions** box.

Adapter status is Starting or Not Connected

The status of an adapter in the **Monitors** page in the administration application is **Starting** or **Not Connected**.

Proposed solution

Procedure

1. Test the adapter in the **Servers** tab in the administration application to check if the system displays any errors.
   a. If there are no errors, in the **Monitors** tab, click **Restart** to restart the adapter.
   b. If there are errors, check if the sever is up and is reachable by the Client Enablement Services server.
   For example, to check if the telephony adapter is up, click **Test** on the **Servers** > **Telephony** > **View Telephony Servers** page.
2. In case of secure connection, check if all the required certificates are present in the Client Enablement Services keystore.
   a. In the administration application, select the **Servers** tab.
   b. From the left navigation pane, select **Presence**.
   c. On the Presence Servers page, check if the certificate is listed.
3. Check if the user names and passwords entered in the server page are correct.

For example, for a voice messaging server verify the **IMAP Login ID**, **IMAP Password**, **SMTP Login ID**, **SMTP Password**, **LDAP Login ID**, and **LDAP Password** are correct.

4. Check if the port value entered in the servers page in the administration application is correct.
5. If all values are correctly configured, but the adapter does not show the status as **Connected**, restart the WAS.
   a. SSH in to the Client Enablement Services terminal using Putty.
   b. On the shell prompt, type the **`#service 1xp restart`** command to restart the Client Enablement Services service.
      The system prompts you to enter your username and password when it tries to stop the server.
   c. Enter your admin_user_name and the admin_user_password.
      This stops and restarts the Client Enablement Services server.

Unable to view call details in the desk phone call logs

Disabling the desk phone ringer on the Avaya one-X® Mobile application causes the desk phone ringer to be turned off, but the desk phone does not log the caller name and number in the call logs.

Proposed solution

Procedure

1. Log in to Communication Manager.
2. Type the command **`display system-parameters features`**
3. On the FEATURE-RELATED SYSTEM PARAMETERS screen, set the **Keep Bridged Information on Multiline Displays During Calls?** field to **y**.
   The desk phone logs all calls when the desk phone ringer OFF option is enabled on the Avaya one-X® Mobile client application.

Chapter 4: Troubleshooting Avaya one-X® Mobile client applications

Keypad is displayed on the Home screen after login

Proposed solution

Procedure

1. Log out from the Avaya one-X® Mobile application.
2. Log in again using your login credentials.

Intermittent splash ring heard even after call is disconnected

Proposed solution

Procedure

If you have selected **Use one-X Mobile for All calls** on the **Settings** > **Call Settings** screen, the destination number may hear an intermittent splash ring even after the call has been disconnected. Between Avaya one-X® Mobile disconnecting the mobile call and launching the call back call, the mobile network may get a connection to the destination number.

Voice mail PIN does not change

Proposed solution

Procedure

The application does not send you any notification after your administrator changes your voice mail PIN. Wait for a period of 24 hours for the changes to take effect. Till then, you can continue to download voice mails using the old voice mail PIN.

Avaya one-X® Mobile displays incorrect user-interface elements

Note:

This issue is noted for Avaya one-X® Mobile on iPhone only.

Proposed solution

Procedure

1. From the native applications screen of your mobile device, tap **Settings**.
2. On the Settings screen, tap **General**.
3. Tap **International**.
4. Tap **Language**.
5. Tap **English**.
   The system sets the language setting to English (United States).

Availability status does not change

The availability status of a contact marked as **VIP** or **Favorite** does not change if the contact is marked as **VIP** or **Favorite** using Avaya one-X® Communicator.

Proposed solution

Procedure

If you use both Avaya one-X® Mobile and Avaya one-X® Communicator, make sure to always mark the contacts as **VIP** or **Favorite** using the Avaya one-X® Mobile application. The system updates the availability status on both applications.

Auto-Manage set using Avaya one-X® Mobile does not get updated on Avaya one-X® Communicator

Proposed solution

Procedure

The **Auto-Manage** setting should be managed independently on Avaya one-X® Mobile and Avaya one-X® Communicator.

Busy availability status not updated for an active call

If **Auto-Manage** is disabled on either Avaya one-X® Mobile or Avaya one-X® Communicator, the **Busy** availability status is not updated for active calls.

Proposed solution

Procedure

User defined availability status takes precedence over **Auto-Manage**. When using both, Avaya one-X® Mobile and Avaya one-X® Communicator, keep the **Auto-Manage** setting enabled for each application to allow availability status updates for an active call.

Unable to update the availability status through Avaya one-X® Communicator if the user-defined availability status is set using Avaya one-X® Mobile for the same user.

Proposed solution

Procedure

The availability status set using Avaya one-X® Mobile takes precedence over Avaya one-X® Communicator. You should keep the **Auto-Manage** setting enabled on Avaya one-X® Mobile whenever user-defined status is not required.

Call gets simultaneously routed to voice mail and mobile device

Proposed solution

Procedure

If you have enabled **Send All Calls** on your desk phone, while **Block all calls** on your mobile device is disabled, the call may get simultaneously routed to your voice mail

and your mobile device, thus registering a call entry. Hence, you should always use **Block all calls** on your mobile device to send all calls to voice mail.

Unable to view call details in the desk phone call logs

Disabling the desk phone ringer on the Avaya one-X® Mobile application causes the desk phone ringer to be turned off, but the desk phone does not log the caller name and number in the call logs.

Proposed solution

Procedure

Contact your administrator to set the **Keep Bridged Information on Multiline Displays During Calls?** field to **y**.
Your desk phone logs all calls even when the desk phone ringer is disabled on the Avaya one-X® Mobile application.

When minimized, Avaya one-X® Mobile does not get updated on your mobile device

After you log into Avaya one-X® Mobile, and then minimize it, the application does not maintain an active session with the Avaya one-X® Client Enablement Services server, and hence does not get updated to display the new voice mails and call logs.

Proposed solution

Procedure

1. To get SMS alerts when a new voice mail arrives, do the following:
   a. Tap **Home** on the bottom tab of your Avaya one-X® Mobile screen.
   b. Tap **Settings**.
   c. Tap **Message Notification**, and then tap **All**.
      You will receive SMS alerts for all voice mails.

Note:

Tap **Urgent Only** to receive SMS alerts for only those voice mails marked as urgent.

2. To get the updated call logs, you must bring the application to the foreground of your mobile device.

Call back does not work

Proposed solution

Procedure

Contact your administrator to disable the **Automatic Exclusion by COS** setting on Communication Manager for your user extension.

Chapter 5: Troubleshooting Avaya one-X® Communicator

Availability status does not change

The availability status of a contact marked as **VIP** or **Favorite** in Avaya one-X® Communicator does not change if the contact is marked as **VIP** or **Favorite** using Avaya one-X® Mobile.

Proposed solution

Procedure

If you use Avaya one-X® Communicator and Avaya one-X® Mobile, make sure to always mark the contacts as **VIP** or **Favorite** using the Avaya one-X® Communicator application. The system updates the availability status for both applications.

Auto-Manage set using Avaya one-X® Communicator does not get updated on Avaya one-X® Mobile

Proposed solution

Procedure

Auto-Manage must be set independently for Avaya one-X® Communicator and Avaya one-X® Mobile.

Busy availability status not updated for an active call

The system does not update the **Busy** availability status for an active call if the availability status is set to **Auto-Manage** on Avaya one-X® Communicator, and the availability status on Avaya one-X® Mobile is set manually for the same user.

Proposed solution

Procedure

The availability status that is set manually for Avaya one-X® Mobile takes precedence over the availability status that is set to **Auto-Manage** for Avaya one-X® Communicator. When using both, Avaya one-X® Communicator and Avaya one-X® Mobile, keep the **Auto-Manage** setting consistent for both the applications.

Unable to update the availability status through Avaya one-X® Communicator if the user-defined availability status is set using Avaya one-X® Mobile for the same user.

Proposed solution

Procedure

The availability status set using Avaya one-X® Mobile takes precedence over Avaya one-X® Communicator. You should keep the **Auto-Manage** setting enabled on Avaya one-X® Mobile whenever user-defined status is not required.

Chapter 6: Alarms

Alarms overview

Avaya one-X® Client Enablement Services generates alarms, SNMP traps, to notify users of system events. Alarms are grouped by categories. Each alarm category identifies the system component that generates the alarm.

Alarms are written to log files that are located at the following locations:

- `/opt/IBM/WebSphere/AppServer/profiles/default/logs/server1/SystemOut.log`
- `/opt/IBM/WebSphere/AppServer/profiles/default/logs/server1/trace.log`
- `/opt/IBM/WebSphere/AppServer/profiles/default/logs/acp_alarm.log`

  The acp_Alarm.log file contains only alarms.

Core Services Alarms

CoreServicesMIB.CS_WD_PROCESS_UP

Event name	`CoreServicesMIB.CS_WD_PROCESS_UP`
Event text	`Process is up`
Event level	XXX
Trigger component	Core Services startup

Problem description

Notification that the process for Core Services is up and running. This is a Core Services alarm that is used by Avaya one-X® Client Enablement Services.

Proposed Solution

About this task

No corrective action is required.

Licensing Alarms

av1xTrapQLICE00001

Alarm name	`av1xTrapQLICE00001`
Alarm text	`Entering license normal mode: license requirements are met.`
Alarm level	INFO - General information
Trigger component	Licensing server

Problem description

Normal mode means the product license requirements for Avaya one-X® Client Enablement Services have been met.

Proposed Solution

About this task

No corrective action is required.

av1xTrapQLICE00002

Alarm name	`av1xTrapQLICE00002`
Alarm text	`Entering license error mode: license requirements are not met.`
Alarm level	ERROR - impacts system operation

Trigger component Licensing server

Problem description

Error mode indicates the product license requirements for Avaya one-X® Client Enablement Services have not been met.

Proposed Solution

About this task

1. In the Client Enablement Services Administration application, click the **System** tab .
2. From the left navigation pane, select **License Server**.
3. Verify the following on the License server page:
   - Verify that a WebLM server is configured.
   - Verify the connection is up.
   - Verify that there are a sufficient number of license units available for Client Enablement Services.

     You must have one license unit for each provisioned user on Client Enablement Services.

---

av1xTrapQLICE00003

Alarm name `av1xTrapQLICE00003`

Alarm text `Entering license restricted mode: license requirements are not met; restricting activity.`

Alarm level ERROR - impacts system operation

Trigger component Licensing server

Problem description

Restricted mode means that product license requirements for Client Enablement Services have not been met for 30 days or more. In restricted mode, some operations are prohibited.

Proposed Solution

About this task

1. In the Client Enablement Services Administration application, click the **System** tab .
2. From the left navigation pane, select **License Server**.
3. Verify the following on the License server page:
   - Verify that a WebLM server is configured.
   - Verify the connection is up.
   - Verify that there are a sufficient number of license units available for Client Enablement Services.

     You must have one license unit for each provisioned user on Client Enablement Services.

Scheduler Alarms

av1xTrapQSCHE00001

Alarm name	`av1xTrapQSCHE00001`
Alarm text	`Scheduler task failed.`
Alarm level	ERROR - impacts system operation
Trigger component	Scheduler

Problem description

A scheduled task failed during execution.

Proposed Solution

About this task

See the system log files for task specific details.

av1xTrapQSCHE00002

Alarm name	`av1xTrapQSCHE00002`
Alarm text	`Cannot find WAS scheduler JNDI name.`
Alarm level	ERROR - may impact system operation
Trigger component	Scheduler

Problem description

The Scheduler cannot find the name of the Scheduler JNDI name on the Web application server.

Proposed Solution

About this task

The Scheduler JNDI configuration is incorrectly configured. This only occurs when the JNDI configuration is modified in the WebSphere administration console. Reset the JNDI configuration to its original settings.

av1xTrapQSCHE00003

Alarm name	`av1xTrapQSCHE00003`
Alarm text	`WAS scheduler not available.`
Alarm level	ERROR - may impact system operation
Trigger component	Scheduler

Problem description

Notification that the Web Application Server Scheduler application is not available to the Scheduler.

Proposed Solution

About this task

The WebSphere Scheduler is not functioning. See the `SystemErr.log` file for details.

Common Alarms

av1xTrapQCOMM00001

Alarm name	`av1xTrapQCOMM00001`
Alarm text	`Service start.`
Alarm level	INFO - General information
Trigger component	Common components

Problem description

The requested service was started.

Proposed Solution

About this task

No corrective action is required.

av1xTrapQCOMM00002

Alarm name	`av1xTrapQCOMM00002`
Alarm text	`Service shutdown.`
Alarm level	INFO - General information
Trigger component	Common components

Problem description

The requested service was shut down.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCOMM00003

Alarm name	`av1xTrapQCOMM00003`
Alarm text	`Provider connected.`
Alarm level	INFO - General information
Trigger component	Common components

Problem description

The administrator successfully connected the service provider to Avaya one-X® Client Enablement Services.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCOMM00004

Alarm name	`av1xTrapQCOMM00004`
Alarm text	`Provider created.`
Alarm level	INFO - General information
Trigger component	Common components

Problem description

The administrator successfully added the service provider to Avaya one-X® Client Enablement Services.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCOMM00005

Alarm name	`av1xTrapQCOMM00005`
Alarm text	`Provider disconnected.`
Alarm level	INFO - General information
Trigger component	Common components

Problem description

The service provider was disconnected from Avaya one-X® Client Enablement Services.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCOMM00006

Alarm name	`av1xTrapQCOMM00006`
Alarm text	`Provider load.`
Alarm level	INFO - General information
Trigger component	Common components

Problem description

The provider server configuration load for the service provider on Client Enablement Services is in progress.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCOMM00007

Alarm name	`av1xTrapQCOMM00007`
Alarm text	`Provider resume.`
Alarm level	INFO - General information
Trigger component	Common components

Problem description

The running of the service provider on Client Enablement Services has resumed. The **Monitors** feature on the Client Enablement Services administration application initiates this alarm.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCOMM00008

Alarm name	`av1xTrapQCOMM00008`
Alarm text	`Provider suspend.`
Alarm level	INFO - General information
Trigger component	Common components

Problem description

The running of the service provider on Client Enablement Services was suspended. The **Monitors** feature on the Client Enablement Services administration application initiates this alarm.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCOMM00009

Alarm name	`av1xTrapQCOMM00009`
Alarm text	`Provider shutdown.`
Alarm level	INFO - General information
Trigger component	Common components

Problem description

The administrator successfully shut down the service provider on Client Enablement Services.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCOMM00010

Alarm name	`av1xTrapQCOMM00010`
Alarm text	`Interface started.`
Alarm level	INFO - General information
Trigger component	Common components

Problem description

The administrator has successfully started the interface to the service provider on Client Enablement Services.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCOMM00011

Alarm name	`av1xTrapQCOMM00011`
Alarm text	`Interface shutdown.`
Alarm level	INFO - General information
Trigger component	Common components

Problem description

Notification that the administrator successfully shut down the interface to the service provider on Client Enablement Services.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCOMM00012

Alarm name	`av1xTrapQCOMM00012`
Alarm text	`Dialplan <dialplan name> is invalid.`
Alarm level	WARNING - may impact system operation
Trigger component	Any component

Problem description

Notification that the system detected an invalid dial plan, and that dial plan will not be available.

Proposed Solution

About this task

Correct the dial plan configuration in the administration application.

For more information on dial plans, see “Dial Plan” in Chapter 3, “Server administration,” in *Administering Avaya one-X® Client Enablement Services*.

Conferencing Alarms

av1xTrapQCONF00001

Alarm name	`av1xTrapQCONF00001`
Alarm text	`Obtained Work Manager for Conferencing.`
Alarm level	INFO - General Information
Trigger component	Conferencing Service

Problem description

Notification that the Conferencing Service successfully acquired the Work Manager.

Proposed Solution

About this task

No corrective action is required.

av1xTrapQCONF00002

Alarm name	`av1xTrapQCONF00002`
Alarm text	`Cleanup resources for user: {0}.`
Alarm level	INFO - General Information
Trigger component	Conferencing Service

Problem description

Notification that the Conferencing service cleanup resources on Client Enablement Services are available to the specified user ID.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCONF00003

Alarm name	`av1xTrapQCONF00003`
Alarm text	`Start resource: {0}.`
Alarm level	INFO - General Information
Trigger component	Conferencing Service

Problem description

Notification that the Conferencing services resources on Client Enablement Services were successfully started for the specified user.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCONF00004

Alarm name	`av1xTrapQCONF00004`
Alarm text	`Stop resource: {0}.`
Alarm level	INFO - General Information
Trigger component	Conferencing Service

Problem description

Notification that the Conferencing service resources on Client Enablement Services were successfully stopped for the specified user.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCONF00005

Alarm name `av1xTrapQCONF00005`

Alarm text `No resource located for userid {0} - cannot associate participant {1}.`

Alarm level WARNING - may impact system operation

Trigger component Conferencing Service

Problem description

The participant in the bridge conference is translated into the indicated user id, but the user id is not currently associated with the MX (Meeting Exchange) or Avaya Aura® Conferencing Standard Edition adapter on Client Enablement Services.

Proposed Solution

About this task

Using the Client Enablement Services administration application, associate the user with the Conferencing server.

For more details, see “Assigning a Conferencing resource to a user” in Chapter 4, “User administration,” in *Administering Avaya one-X® Client Enablement Services*.

---

av1xTrapQCONF00006

Alarm name `av1xTrapQCONF00006`

Alarm text `Exception on user identity assessment via User Service for {0} criteria: {1} - no association to participant is possible.`

Alarm level ERROR - impacts system operation

Trigger component Conferencing Service

Problem description

An incoming participant to a bridge conference with a Client Enablement Services user using the specified criteria. No data will be available to this user if the user is logged in to Client Enablement Services.

The {0} in this message is the data used to retrieve the user identity and the {1} indicates how {0} was interpreted (ANI, PIN, moderator code).

Proposed Solution

About this task

Check the criteria and make the appropriate changes. If the problem persists, contact Avaya Technical Support.

---

av1xTrapQCONF00007

Alarm name `av1xTrapQCONF00007`

Alarm text `Exception on user identity assessment via Contact Service - no association to participant is possible.`

Alarm level ERROR - impacts system operation

Trigger component Conferencing Service

Problem description

Notification that the Conferencing service resource cannot be assigned to the specified user in the Client Enablement Services Contact Service.

Proposed Solution

About this task

Determine if the connection to the Contact Service is disconnected and if it can be brought back online.

av1xTrapQCONF00008

Alarm name `av1xTrapQCONF00008`

Alarm text `Conference data conversion failed for [{0}]- possible bridge disconnection.`

Alarm level ERROR - impacts system operation

Trigger component Conferencing Service

Problem description

Notification that data conversion for a bridge connection failed on [{0}], where [{0}] is the bridge that was disconnected, the Conferencing service, possibly because the bridge was disconnected on Client Enablement Services.

Proposed Solution

About this task

Determine if the bridge connection is disconnected and if it can be brought back online.

av1xTrapQCONF00009

Alarm name `av1xTrapQCONF00009`

Alarm text `Invalid configuration <Conference server name> - review configuration and retry.`

Alarm level ERROR - impacts system operation

Trigger component Conferencing Service

Problem description

One or more of the configuration settings on the specified Conferencing server contain invalid values.

Proposed Solution

About this task

Check the settings, make the necessary changes, and retry the server.

av1xTrapQCONF00010

Alarm name av1xTrapQCONF00010

Alarm text Participant data conversion failed <Conference server name> - possible bridge disconnection.

Alarm level ERROR - impacts system operation

Trigger component Conferencing Service

Problem description

Data conversion for a bridge conference failed on the specified Conferencing service, possibly because the bridge conference was disconnected on Client Enablement Services.

Proposed Solution

About this task

Determine why the bridge was disconnected and make sure it can connect. Repeat the original operation.

av1xTrapQCONF00011

Alarm name av1xTrapQCONF00011

Alarm text Bridge connection failed <Conference server name> - review configuration and retry.

Alarm level ERROR - impacts system operation

Trigger component Conferencing Service

Problem description

The bridge connection failed on the specified Conferencing service because one or more of the configuration settings on the Conferencing server contain invalid values.

Proposed Solution

About this task

Check the settings, make the necessary changes, and retry the server.

av1xTrapQCONF00012

Alarm name `av1xTrapQCONF00012`

Alarm text `Participant failed to add to conference <conference id> - no data to participant <user id> is possible - gather logs for problem analysis.`

Alarm level ERROR - impacts system operation

Trigger component Conferencing Service

Problem description

A user was identified, but this user could not be associated with the specified conference. Some possible reasons are lack of memory, bridge disconnection, and either the conference or the participant terminated before this operation could be completed.

Proposed Solution

About this task

Check the log files for the conference to analyze the problem.

av1xTrapQCONF00013

Alarm name `av1xTrapQCONF00013`

Alarm text `Data conversion failed due to exception from Bridge <Conference server name> - possible bridge disconnection.`

Alarm level ERROR - impacts system operation

Trigger component Conferencing Service

Problem description

An exception was received from the conference bridge causing a data conversion failure. This failure may have disconnected the bridge.

Proposed Solution

About this task

Determine why the bridge disconnected and resolve this issue. If the bridge did not disconnect, inspect the log files to find out the reason for this failure.

---

av1xTrapQCONF00014

Alarm name `av1xTrapQCONF00014`

Alarm text `Resume of services failed <Conference server name> - review logs for reason and retry.`

Alarm level ERROR - impacts system operation

Trigger component Conferencing Service

Problem description

An attempt to resume bridge conferencing services failed.

Proposed Solution

About this task

Review the log files for the cause and retry to resume services.

---

av1xTrapQCONF00015

Alarm name `av1xTrapQCONF00015`

Alarm text `Suspend of services failed <Conference server name> - review logs for reason and retry.`

Alarm level ERROR - impacts system operation

Trigger component Conferencing Service

Problem description

An attempt to suspend bridge conferencing services failed.

Proposed Solution

About this task

Review the log files for the cause and retry to suspend services.

---

av1xTrapQCONF00016

Alarm name	`av1xTrapQCONF00016`
Alarm text	`Resource creation failed : userid x resourceid <resource id> mismatch.`
Alarm level	WARNING - may impact system operation
Trigger component	Conferencing Service

Problem description

An attempt to create a conferencing resource failed. Possible reasons are lack of memory or the resource data is either corrupted or missing.

Proposed Solution

About this task

Verify the availability of sufficient system memory. Verify the user configuration on the Client Enablement Services administration application.

For more information on user configuration, see “Assigning a Conferencing resource to a user” in Chapter 4, “User administration,” in *Administering Avaya one-X® Client Enablement Services*.

---

av1xTrapQCONF00017

Alarm name	`av1xTrapQCONF00017`
Alarm text	`ContactLog subscription failed.`
Alarm level	ERROR - impacts system opeartion
Trigger component	Conferencing Service

Problem description

The subscription of the Conferencing service to the ContactLog service failed.

Proposed Solution

About this task

Inspect log files to determine the reason for this failure. Correct the problem and retry the operation.

---

av1xTrapQCONF00018

Alarm name	`av1xTrapQCONF00018`
Alarm text	`ContactLog posting failed.`
Alarm level	ERROR - impacts system operation
Trigger component	Conferencing server

Problem description

Conferencing services was unable to post to the ContactLog service.

Proposed Solution

About this task

Inspect log files to determine the reason for this failure. Correct the problem and retry the operation.

---

av1xTrapQCONF00019

Alarm name	`av1xTrapQCONF00019`
Alarm text	`Contact Logging connection not possible; failure establishing channel (auto-retry in progress).`
Alarm level	WARNING - may impact system operation
Trigger component	Conferencing Service

Problem description

The Conferencing service connection to the ContactLog service is unavailable because there was a failure in establishing the channel. The system continues to try to make the connection via auto-retry.

Proposed Solution

About this task

Inspect log files to determine the reason for this failure. Correct the problem, and retry the operation.

---

av1xTrapQCONF00020

Alarm name `av1xTrapQCONF00020`

Alarm text `Failed to obtain Work Manager (will proceed with ordinary threads)- gather logs, review WAS configuration and restart the service.`

Alarm level WARNING - may impact system operation

Trigger component Conferencing Service

Problem description

The Conferencing service could not acquire the Work Manager.

Proposed Solution

About this task

In the log files, check the WAS configuration and restart the service.

---

av1xTrapQCONF00021

Alarm name `av1xTrapQCONF00021`

Alarm text `Failed to start Work Item via Work Manager - gather logs, review WAS configuration and restart the service.`

Alarm level WARNING - may impact system operation

Trigger component Conferencing Service

Problem description

The Conferencing service could not start the Work Item in the Work Manager.

Proposed Solution

About this task

In the log files, check the WAS configuration and restart the service.

Voice Messaging Alarms

av1xTrapQVMSG00003

Alarm name	`av1xTrapQVMSG00003`
Alarm text	`Message work directory <work directory name>.`
Alarm level	INFO - General Information
Trigger component	Voice Messaging server

Problem description

The name of the configured directory in which message parts is temporarily stored for playback, display, etc.

Proposed Solution

About this task

No corrective action is required.

av1xTrapQVMSG00004

Alarm name	`av1xTrapQVMSG00004`

Alarm text `Creating message work directory at {0}.`

Alarm level INFO - General information

Trigger component Voice Messaging server

Problem description

The actual location of the Voice Messaging service {0} created the work directory.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQVMSG00005

Alarm name `av1xTrapQVMSG00005`

Alarm text `Loading configuration for voice message provider: {0} on {1}.`

Alarm level INFO - General information

Trigger component Voice Messaging server

Problem description

The indicated configuration {0} is associated with the indicated provider {1}.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQVMSG00006

Alarm name `av1xTrapQVMSG00006`

Alarm text `Removing storage for temporary message parts.`

Alarm level INFO - General information

Trigger component Voice Messaging server

Problem description

The Voice Messaging service is removing the temporary message part storage area.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQVMSG00008

Alarm name `av1xTrapQVMSG00008`

Alarm text `Failure on ContactService data retrieval:{0} criteria:{1}.`

Alarm level ERROR - impacts system operation

Trigger component Voice Messaging server

Problem description

An attempt to retrieve the indicated data {0} from the Contact Service using the indicated criteria {1} failed.

Proposed Solution

About this task

Assess if the indicated criteria {1} is viable from the Contact Service perspective and correct if necessary.

---

av1xTrapQVMSG00010

Alarm name `av1xTrapQVMSG00010`

Alarm text `Access not possible - check file/directory rights.`

Alarm level ERROR - impacts system operation

Trigger component Voice Messaging server

Problem description

An attempt to access the server failed because of lack of permissions.

Proposed Solution

About this task

Get the required permissions from the System Administrator and try again.

---

av1xTrapQVMSG00009

Alarm name `av1xTrapQVMSG00009`

Alarm text `Access to {0} was not possible - check file/directory rights.`

Alarm level ERROR - impacts system operation

Trigger component Voice Messaging server

Problem description

The Voice Messaging server denied access to the specified file or directory.

Proposed Solution

About this task

Give the Voice Messaging server permissions to access the specified file or directory.

---

av1xTrapQVMSG00011

Alarm name `av1xTrapQVMSG00011`

Alarm text `Message encoding/decoding error during [{0}](message is mal-formed or removed while in transit).`

Alarm level ERROR - impacts system operation

Trigger component Voice Messaging server

Problem description

There was an encoding or decoding error on the message while the message was in transit and the message became distorted or lost.

Proposed Solution

About this task

Check the log files to find the cause of this problem. Correct the problem and retry the operation.

---

av1xTrapQVMSG00012

Alarm name `av1xTrapQVMSG00012`

Alarm text `Unexpected exception on method:{0} for resourceid {1}.`

Alarm level ERROR - impacts system operation

Trigger component Voice Messaging server

Problem description

An attempt to perform the indicated operation (method) failed for the indicated resource.

Proposed Solution

About this task

Check the logs files to find the cause of this problem. Correct the problem and retry the operation.

---

av1xTrapQVMSG00013

Alarm name `av1xTrapQVMSG00013`

Alarm text `Exceeded number of client connections to voice message provider: <provider name> - increase client connections. try again.`

Alarm level WARNING - may impact system operation

Trigger component Voice Messaging server

Problem description

The total number of client connections to the indicated Voice Messaging server is not sufficient to satisfy the total number of requests from the Client Enablement Services clients.

Proposed Solution

Procedure

1. In the Client Enablement Services administration application, select the **Servers** tab.
2. From the left navigation pane, select **Voice Messaging**.
3. On the Voice Messaging page, click the name of a Modular Messaging server in the **Handle** field.

   The system displays the Modify Voice Messaging Server Configuration page for the server.
4. Increase the number of client connections on the Voice Messaging server.
5. Click **Save**.

av1xTrapQVMSG00014

Alarm name `av1xTrapQVMSG00014`

Alarm text `Failure on client connection release - gather logs and report problem.`

Alarm level ERROR - impacts system operation

Trigger component Voice Messaging server

Problem description

The system failed to successfully release a client connection to the Voice Messaging server.

Proposed Solution

About this task

Collect the system log files that pertain to this issue and call Avaya Technical Support for assistance.

av1xTrapQVMSG00015

Alarm name `av1xTrapQVMSG00015`

Alarm text `Failure on client connection start - check: userid/password for voice message provider and restart provider.`

Alarm level ERROR - impacts system operation

Trigger component Voice Messaging server

Problem description

The credentials to access the Voice Messaging service are incorrect.

Proposed Solution

About this task

On the administration application, correct and reset the credentials for the Voice Messaging service.

For more information on Voice Messaging server, see “Voice Messaging servers” in Chapter 3 “Server administration,” in *Administering Avaya one-X® Client Enablement Services*.

av1xTrapQVMSG00016

Alarm name `av1xTrapQVMSG00016`

Alarm text `Unknown voice mail provider: (connection not possible via IMAP) - check: address/hostname, IMAP port enablement, firewalls.`

Alarm level ERROR - impacts system operation

Trigger component Voice Messaging server

Problem description

The system does not recognize the Voice Messaging server. Therefore, the IMAP connection is not possible.

Proposed Solution

About this task

Check the IP address and the host name parameters of the Voice Messaging server. Also check the IMAP port is enabled and that there are no issues with the firewall.

For more information on Voice Messaging server, see “Voice Messaging servers” in Chapter 3 “Server administration,” in *Administering Avaya one-X® Client Enablement Services*.

---

av1xTrapQVMSG00017

Alarm name `av1xTrapQVMSG00017`

Alarm text `Invalid provider configuration. incomplete or invalid IMAP configuration.`

Alarm level ERROR - impacts system operation

Trigger component Voice Messaging server

Problem description

The IMAP configuration for the Voice Messaging server is invalid. The IMAP configuration is either incomplete or incorrect.

Proposed Solution

About this task

Check the IMAP configuration for the Voice Messaging server, and make sure all of parameters are provided and correct.

For more information on Voice Messaging server, see “Voice Messaging servers” in Chapter 3 “Server administration,” in *Administering Avaya one-X® Client Enablement Services*.

---

av1xTrapQVMSG00019

Alarm name `av1xTrapQVMSG00019`

Alarm text `Failed to obtain Work Manager (will proceed with ordinary threads) - gather logs, review WAS configuration, and restart service.`

Alarm level INFO - General information

Trigger component Voice Messaging server

Problem description

The Voice Messaging server did not acquire the Work Manager.

Proposed Solution

About this task

In the log files, check the WAS configuration and restart the service.

---

av1xTrapQVMSG00023

Alarm name `av1xTrapQVMSG00023`

Alarm text `Unexpected exception from voice message provider - gather logs and report problem.`

Alarm level ERROR - impacts system operation

Trigger component Voice Messaging server

Problem description

Client Enablement Services returned an unexpected exception from the Voice Message server.

Proposed Solution

About this task

Collect the system log files that pertain to this issue, and call Avaya Technical Support for assistance.

Contact Logging Alarms

av1xTrapQCLOG00001

Alarm name	`av1xTrapQCLOG00001`
Alarm text	`ContactLogger channel started.`
Alarm level	INFO - General information
Trigger component	Contact Logger Service

Problem description

The Contact Logger service channel started up.

Proposed Solution

About this task

No corrective action is required.

av1xTrapQCLOG00002

Alarm name	`av1xTrapQCLOG00002`
Alarm text	`ContactLogger channel stopped.`
Alarm level	INFO - General information
Trigger component	Contact Logger Service

Problem description

The Contact Logger service channel stopped running.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCLOG00003

Alarm name	`av1xTrapQCLOG00003`
Alarm text	`Successfully obtained reference to CoreWorkManager.`
Alarm level	INFO - General information
Trigger component	Contact Logger Service

Problem description

The Contact Logger service successfully acquired a reference to the Work Manager.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCLOG00004

Alarm name	`av1xTrapQCLOG00004`
Alarm text	`Database failure during Contact Log insert.`
Alarm level	ERROR - impacts system operation
Trigger component	Contact Logger Service

Problem description

The database failed or communication to the database failed while the service was attempting to insert a record.

Proposed Solution

About this task

Determine if the database is running if access is possible.

---

av1xTrapQCLOG00005

Alarm name	`av1xTrapQCLOG00005`
Alarm text	`Database failure during Contact Log deletion.`
Alarm level	ERROR - impacts system operation
Trigger component	Contact Logger Service

Problem description

The database failed or communication to the database failed while the Contact Logger service was attempting to remove a record.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator or call Avaya Technical Support for assistance.

---

av1xTrapQCLOG00006

Alarm name	`av1xTrapQCLOG00006`
Alarm text	`Database failure during Contact Log update.`
Alarm level	ERROR - impacts system operation
Trigger component	Contact Logger Service

Problem description

The database failed or communication to the database failed while the Contact Logger service was attempting to update a record.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator or call Avaya Technical Support for assistance.

---

av1xTrapQCLOG00007

Alarm name	`av1xTrapQCLOG00007`
Alarm text	`Database failure during Contact Log retrieval.`
Alarm level	ERROR - impacts system operation
Trigger component	Contact Logger Service

Problem description

The database failed or communication to the database failed while the Contact Logger service was attempting to retrieve a record.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator or call Avaya Technical Support for assistance.

---

av1xTrapQCLOG00008

Alarm name	`av1xTrapQCLOG00008`

Alarm text `Failed to obtain WorkManager using ordinary threads.`

Alarm level INFO - General information

Trigger component Contact Logger Service

Problem description

The Contact Logger service did not acquire a reference to Work Manager using ordinary threads.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQCLOG00009

Alarm name `av1xTrapQCLOG00009`

Alarm text `Failure obtaining ContactLogger DB trim transaction size.`

Alarm level WARNING - may impact system operation

Trigger component Contact Logger Service

Problem description

The Contact Logger service failed while attempting to obtain the Contact Logger database trim transaction size.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator, or call Avaya Technical Support for assistance.

av1xTrapQCLOG00010

Alarm name `av1xTrapQCLOG00010`

Alarm text `Failure obtaining ContactLogger DB trim pause value.`

Alarm level INFO - General information

Trigger component Contact Logger Service

Problem description

The Contact Logger service failed while getting the Contact Logger database trim pause values.

Proposed Solution

About this task

No corrective action is required.

av1xTrapQCLOG00011

Alarm name `av1xTrapQCLOG00011`

Alarm text `Failure writing ContactLogger DB trim transaction size.`

Alarm level WARNING - may impact system operation

Trigger component Contact Logger Service

Problem description

The Contact Logger service failed while attempting to write the Contact Logger trim transaction size to the database.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator or call Avaya Technical Support for assistance.

av1xTrapQCLOG00012

Alarm name `av1xTrapQCLOG00012`

Alarm text `Failure writing ContactLogger DB trim pause value.`

Alarm level WARNING - may impact system operation

Trigger component Contact Logger Service

Problem description

The Contact Logger service failed while attempting to write the Contact Logger trim pause value to the database.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator or call Avaya Technical Support for assistance.

av1xTrapQCLOG00013

Alarm name `av1xTrapQCLOG00013`

Alarm text `Failure acquiring Admin Interface to System Service.`

Alarm level WARNING - may impact system operation

Trigger component Contact Logger Service

Problem description

The Contact Logger service failed to communicate with System Service.

Proposed Solution

Procedure

Restart Client Enablement Services.

The Contact Logger service will operate using the default values for data which are coming from System Service.

av1xTrapDCLOG01001

Alarm name	`av1xTrapDCLOG01001`
Alarm text	`Contact Logger DB cleanup started.`
Alarm level	INFO - general information
Trigger component	Contact Logger Service

Problem description

The Contact Log Cleanup function has started to run.

Proposed Solution

About this task

No corrective action is required.

av1xTrapDCLOG01002

Alarm name	`av1xTrapDCLOG01002`
Alarm text	`Contact Logger DB cleanup done.`
Alarm level	INFO - general information
Trigger component	Contact Logger Service

Problem description

The Contact Log Cleanup function has completed its tasks.

Proposed Solution

About this task

No corrective action is required.

av1xTrapDCLOG01901

Alarm name	`av1xTrapDCLOG01901`
Alarm text	`Contact Logger DB cleanup failed.`
Alarm level	WARNING - may impact system operation
Trigger component	Contact Logger Service

Problem description

The Contact Log Cleanup function failed to successfully complete its tasks.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator or call Avaya Technical Support for assistance.

Modular Messaging Alarms

av1xTrapQMMLD00001

Alarm name	`av1xTrapQMMLD00001`
Alarm text	`Resolution failed on ContactService data retrieval.`
Alarm level	ERROR - impacts system operation

Trigger component Modular Messaging Synchronization

Problem description

An attempt to locate a contact information through the Contact service using the indicated data criteria failed during data retrieval.

Proposed Solution

About this task

Assess if the indicated data and criteria should have been resolved and adjust the user data so the next synchronization is successful.

---

av1xTrapQMMLD00002

Alarm name `av1xTrapQMMLD00002`

Alarm text `Resolution failed on UserService data retrieval.`

Alarm level ERROR - impacts system operation

Trigger component Modular Messaging Synchronization

Problem description

An attempt to locate a contact information through the User service using the indicated data criteria failed during data retrieval.

Proposed Solution

About this task

Assess if the indicated data and criteria should have been resolved and adjust the user data so the next synchronization is successful.

---

av1xTrapQMMLD00003

Alarm name `av1xTrapQMMLD00003`

Alarm text `Exception on Contact Service for{0} criteria:{1}.`

Alarm level ERROR - impacts system operation

Trigger component Modular Messaging Synchronization

Problem description

The messaging synchronization process failed when accessing Contact Service using the indicated data and criteria.

Proposed Solution

About this task

Assess if the indicated data and criteria should have been resolved and adjust the user data so the next synchronization is successful.

---

av1xTrapQMMLD00004

Alarm name `av1xTrapQMMLD00004`

Alarm text `Access to MM LDAP store failed with exception.`

Alarm level ERROR - impacts system operation

Trigger component Modular Messaging Synchronization

Problem description

The synchronization process to the selected Modular Messaging server failed.

Proposed Solution

About this task

Check the log files for the cause of the failure. Correct the problem and retry the operation.

---

av1xTrapQMMLD00005

Alarm name `av1xTrapQMMLD00005`

Alarm text `Update to ContactService with MM LDAP email handle failed for {0} resolution {1}.`

Alarm level ERROR - impacts system operation

Trigger component Modular Messaging Synchronization

Problem description

The synchronization process failed to update the Contact service with the indicated messaging e-mail handle.

Proposed Solution

About this task

Check the log files for the cause of the failure. Correct the problem and retry the operation.

---

av1xTrapQMMLD00006

Alarm name `av1xTrapQMMLD00006`

Alarm text `Failure during System Interface load for {0} - service is probably not running (check and retry).`

Alarm level ERROR - impacts system operation

Trigger component Modular Messaging Synchronization

Problem description

The synchronization process failed during the indicated interface load. Typically, this occurs because the indicated service is not running.

Proposed Solution

About this task

Check the service and start it if it is not running. Retry the system interface load.

---

av1xTrapDMMLD01001

Alarm name `av1xTrapDMMLD01001`

Alarm text `MM LDAP loader - Scheduler task: started`

Alarm level INFO - General information

Trigger component Modular Messaging Synchronization

Problem description

The scheduler task started on the Modular Messaging LDAP loader.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapDMMLD01002

Alarm name `av1xTrapDMMLD01002`

Alarm text `MM LDAP loader - Scheduler task: ended : result={0} {1}.`

Alarm level INFO - General information

Trigger component Modular Messaging Synchronization

Problem description

The scheduler task ended on the messaging LDAP loader with the results.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapDMMLD01003

Alarm name `av1xTrapDMMLD01003`

Alarm text `MM LDAP loader - server {0}:started.`

Alarm level INFO - General information

Trigger component Modular Messaging Synchronization

Problem description

The Modular Messaging synchronization process to the indicated server has started.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapDMMLD01004

Alarm name	`av1xTrapDMMLD01004`
Alarm text	`MM LDAP loader - server {0}: ended: processed {1} records.`
Alarm level	INFO - General information
Trigger component	Modular Messaging Synchronization

Problem description

The Modular Messaging synchronization process terminated with the indicated results.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapDMMLD08001

Alarm name	`av1xTrapDMMLD08001`
Alarm text	`Resolution failed on ContactService retrieval:{0} criteria:{1}.`
Alarm level	WARNING - may impact system operation
Trigger component	Modular Messaging Synchronization

Problem description

The Modular Messaging synchronization failed to retrieve data from the Contact Service using the indicated data and criteria.

Proposed Solution

About this task

Verify the data in Contact Service and Active Directory are correct. Adjust the data to ensure that future synchronization processes are successful.

---

av1xTrapDMMLD08002

Alarm name	`av1xTrapDMMLD08002`
Alarm text	`Resolution failed on UserService data retrieval:{0} criteria:{1}.`
Alarm level	WARNING - may impact system operation
Trigger component	Modular Messaging Synchronization

Problem description

The Modular Messaging synchronization failed to retrieve data from the User Service using the indicated data and criteria.

Proposed Solution

About this task

Verify the data in Contact Service and Active Directory are correct. Adjust the data to ensure that future synchronization processes are successful.

---

av1xTrapDMMLD08003

Alarm name	`av1xTrapDMMLD08003`
Alarm text	`Exception on Contact Service for {0} criteria: {1}.`
Alarm level	ERROR - impacts system operation
Trigger component	Modular Messaging Synchronization

Problem description

The system returns an unexpected error when accessing the Contact Service using the indicated criteria.

Proposed Solution

About this task

Verify the data in Contact Service and Active Directory are correct. Adjust the data to ensure that future synchronization processes are successful.

Telephony Alarms

av1xTrapQTELE00001

Alarm name	`av1xTrapQTELE00001`
Alarm text	`Invalid value for property on provider.`
Alarm level	ERROR - impacts system operation
Trigger component	Telephony Server

Problem description

The administrator entered an invalid value when configuring Communication Manager for the Telephony server.

Proposed Solution

Procedure

1. In the Administration application, select the **Servers** tab.
2. From the left pane, select **Telephony**.
3. On the Telephony Servers page, in the **Server Type** field, select the version of the Communication Manager installed on your system.
4. Click **Test** to run a short test of your changes.

The results of the test are displayed 6 immediately so you can make any necessary changes. Validate the information and get additional information about the expected values. Update the provider values accordingly.

For more information, see “Modifying Telephony servers” in Chapter 3, “Server administration,” in *Administering Avaya one-X® Client Enablement Services*.

av1xTrapQTELE00002

Alarm name	`av1xTrapQTELE00002`
Alarm text	`Unable to start provider.`
Alarm level	ERROR - impacts system operation
Trigger component	Telephony Server

Problem description

The administrator cannot start the Telephony server.

Proposed Solution

Procedure

1. In the Administration application, select the **Servers** tab.
2. From the left pane, select **Telephony**.
3. On the Telephony Servers page, in the **Server Type** field, select the version of the Communication Manager installed on your system.
4. Click **Test** to run a short test of your changes.
   The results of the test are displayed 6 immediately so you can make any necessary changes. Validate the information and get additional information about the expected values. Update the provider values accordingly.

   For more information, see “Modifying Telephony servers” in Chapter 3, “Server administration,” in *Administering Avaya one-X® Client Enablement Services*.
5. Restart the application and if the problem persists, contact Avaya Technical Support.

av1xTrapQTELE00003

Alarm name	`av1xTrapQTELE00003`
Alarm text	`Detected problems trying to notify user.`
Alarm level	ERROR - impacts system operation
Trigger component	Telephony Server

Problem description

The Telephony server detected problems when it tried to send a notification to the user.

Proposed Solution

About this task

Contact Avaya Technical Support.

av1xTrapQTELE00004

Alarm name	`av1xTrapQTELE00004`
Alarm text	`Invalid configuration of the provider.`
Alarm level	ERROR - impacts system operation
Trigger component	Telephony Server

Problem description

The Telephony server is not configured properly for Client Enablement Services.

Proposed Solution

Procedure

1. In the Administration application, select the **Servers** tab.
2. From the left pane, select **Telephony**.
3. On the Telephony Servers page, in the **Server Type** field, select the version of the Communication Manager installed on your system.

4. Click **Test** to run a short test of your changes.
   The results of the test are displayed 6 immediately so you can make any necessary changes. Validate the information and get additional information about the expected values. Update the provider values accordingly.

   For more information, see “Modifying Telephony servers” in Chapter 3, “Server administration,” in *Administering Avaya one-X® Client Enablement Services*.

av1xTrapQTELE00005

Alarm name `av1xTrapQTELE00005`

Alarm text `Unable to find Contact Service system channel.`

Alarm level ERROR - impacts system operation

Trigger component Telephony Server

Problem description

The Telephony server cannot locate the Contact Service system channel on Client Enablement Services.

Proposed Solution

About this task

Contact Avaya Support.

av1xTrapQTELE00006

Alarm name `av1xTrapQTELE00006`

Alarm text `Having more than one user using the same extension can cause problems. Users: <list of users> have extension <extension number>.`

Alarm level WARNING - may impact system operation

Trigger component Telephony Server

Problem description

Multiple users are setup for the same extension.

Proposed Solution

Procedure

Check the configuration for each one of the users listed, and see if they have the extension that should have been assigned to them.

Client Enablement Services supports only one user per extension.

For more information, see “Assigning a Telephony resource to a user” in Chapter 4, “User administration,” in *Administering Avaya one-X® Client Enablement Services*.

av1xTrapQTELE00007

Alarm name `av1xTrapQTELE00007`

Alarm text `Licenses are not available on CM. User <extension number> cannot be provisioned for mobile telephony.`

Alarm level WARNING - may impact system operation

Trigger component Telephony Server

Problem description

Licenses are not available on Communication Manager. User cannot be provisioned for mobile telephony in the Client Enablement Services administration application.

Proposed Solution

About this task

Contact Avaya Support about Communication Manager licenses for mobile telephony.

Service Framework Alarms

av1xTrapQSVFW00001

Alarm name	`av1xTrapQSVFW00001`
Alarm text	`Starting service.`
Alarm level	INFO - General Information
Trigger component	Service Framework

Problem description

Client Enablement Services is starting the selected service.

Proposed Solution

About this task

No corrective action is required.

av1xTrapQSVFW00002

Alarm name	`av1xTrapQSVFW00002`
Alarm text	`Shutting down service.`
Alarm level	INFO - General Information
Trigger component	Service Framework

Problem description

Client Enablement Services is stopping the selected service.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQSVFW00003

Alarm name	`av1xTrapQSVFW00003`
Alarm text	`Install adapter complete.`
Alarm level	INFO - General information
Trigger component	Service Framework

Problem description

Client Enablement Services successfully installed the selected adapter.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQSVFW00004

Alarm name	`av1xTrapQSVFW00004`
Alarm text	`Completely started adapter.`
Alarm level	INFO - General information
Trigger component	Service Framework

Problem description

Client Enablement Services successfully started the selected adapter.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQSVFW00005

Alarm name	`av1xTrapQSVFW00005`
Alarm text	`Updating adapter record version identifier for bug fix.`
Alarm level	INFO - General information
Trigger component	Service Framework

Problem description

Client Enablement Services is updating the record version of the selected adapter to fix a defect.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQSVFW00006

Alarm name	`av1xTrapQSVFW00006`
Alarm text	`New adapter-related records being written to the database.`
Alarm level	INFO - General information
Trigger component	Service Framework

Problem description

Client Enablement Services is writing new records for the selected adapter to the database.

Proposed Solution

About this task

No corrective action is required.

av1xTrapQSVFW00007

Alarm name	`av1xTrapQSVFW00007`
Alarm text	`Core WAR shutting down with adapters still running.`
Alarm level	ERROR - impacts system operation
Trigger component	Service Framework

Problem description

Client Enablement Services is shutting down the Core WAR while some adapters are still running. This can happen if the administrator tries to use the WebSphere administration console to stop Core WAR. Under normal conditions, this should never happen.

Proposed Solution

About this task

Restart the Client Enablement Services server because restarting the Core WAR with other adapters running is not supported.

For more information, see “Restarting Client Enablement Services” in Chapter 11, “Miscellaneous tasks,” in *Administering Avaya one-X® Client Enablement Services*.

av1xTrapQSVFW00008

Alarm name	`av1xTrapQSVFW00008`
Alarm text	`Database down.`
Alarm level	INFO - General Information
Trigger component	Service Framework

Problem description

The Client Enablement Services database is not running.

Proposed Solution

About this task

If you require access to the Client Enablement Services database, contact the local database administrator.

---

av1xTrapQSVFW00009

Alarm name	`av1xTrapQSVFW00009`
Alarm text	`Database up.`
Alarm level	INFO - General Information
Trigger component	Service Framework

Problem description

The Client Enablement Services database is up and running.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapDSVFW00049

Alarm name	`av1xTrapDSVFW00049`
Alarm text	`Service Down (threadpool is filled up).`
Alarm level	ERROR - impacts system operation
Trigger component	Service Framework

Problem description

The specified Client Enablement Services service is not running because the thread pool has reached its capacity.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator or call Avaya Technical Support for assistance.

User Alarms

av1xTrapQUSER00010

Alarm name `av1xTrapQUSER00010`

Alarm text `Cannot register with Directory Service for synchronization.`

Alarm level ERROR - impacts system operation

Trigger component User Service

Problem description

The User service is unable to access a critical component This might cause some operations to fail or produce incorrect results.

Proposed Solution

About this task

Check the log files for errors that contributed to the problem. Call Avaya Technical Support.

av1xTrapQUSER00001

Alarm name `av1xTrapQUSER00001`

Alarm text `User Service incremental synchronization results: 87 users checked, <#> users modified, <#> users moved, <#> users marked for deletion, <#> users deleted, <#> database errors.`

Alarm level INFO - General information

Trigger component User Service

Problem description

A summary of the changes made to the provisioned users during an Enterprise Directory synchronization including:

- Users checked - number of users found in the Enterprise Directory.
- Users modified - number of user records that were updated.
- User moved - number of users whose group assignment was changed.
- User marked for deletion - number of users who have been identified as being removed but whose record is not yet deleted.
- Users deleted - number of user records, previously marked for deletion, which were deleted.
- Database errors - number of errors encountered during database reads or updates.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQUSER00002

Alarm name `av1xTrapQUSER00002`

Alarm text `Invalid property metadata.`

Alarm level WARNING - may impact system operation

Trigger component User Service

Problem description

An invalid property description record was found in the database.

Proposed Solution

About this task

Property description records are created at installation time and these records should always be valid. If this error occurs after installing Client Enablement Services, contact Avaya Technical Support. If this error occurs later, the record may have been tampered with or corrupted and it must be restored.

---

av1xTrapQUSER00003

Alarm name	`av1xTrapQUSER00003`
Alarm text	`Cannot schedule work.`
Alarm level	WARNING - may impact system operation
Trigger component	User Service

Problem description

An important task could not be executed because of an error scheduling the task with the Work Manager.

Proposed Solution

About this task

Check the log files for errors that contributed to this problem.

---

av1xTrapQUSER00004

Alarm name	`av1xTrapQUSER00004`
Alarm text	`Unhandled Exception in work task.`
Alarm level	ERROR - impacts system operation
Trigger component	User Service

Problem description

There was an unexpected error in a work task.

Proposed Solution

About this task

Contact Avaya Technical Support.

---

av1xTrapQUSER00005

Alarm name	`av1xTrapQUSER00005`
Alarm text	`Cannot obtain criteria for group synchronization; no group assignments will be made.`
Alarm level	ERROR - impacts system operation
Trigger component	User Service

Problem description

The User Service encountered an unexpected error from the database.

Proposed Solution

About this task

Check the log files for errors that contributed to the problem.

---

av1xTrapQUSER00006

Alarm name	`av1xTrapQUSER00006`
Alarm text	`Cannot update user during synchronization.`
Alarm level	ERROR - impacts system operation
Trigger component	User Service

Problem description

The User service encountered an unexpected error reading or updating the database.

Proposed Solution

About this task

Check the log files for errors that contributed to the problem.

---

av1xTrapQUSER00007

Alarm name	`av1xTrapQUSER00007`
Alarm text	`Cannot obtain users marked for deletion.`
Alarm level	INFO - General information
Trigger component	User Service

Problem description

The selected user record was marked for deletion in the User Service synchronization. The administrator cannot access a user record that is marked for deletion.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapQUSER00008

Alarm name	`av1xTrapQUSER00008`
Alarm text	`Cannot create work manager.`
Alarm level	ERROR - impacts system operation
Trigger component	User Service

Problem description

The User service cannot create the Work Manager for executing asynchronous work tasks.

Proposed Solution

About this task

Check the log files for errors that contributed to the problem. Call Avaya Technical Support.

---

av1xTrapQUSER00009

Alarm name	`av1xTrapQUSER00009`
Alarm text	`Cannot obtain channel to System Service.`
Alarm level	XXX
Trigger component	User Service

Problem description

The User service is unable to access a critical component This may cause some operations to fail or produce incorrect results.

Proposed Solution

About this task

Check the log files for errors that contributed to the problem. Call Avaya Technical Support.

---

av1xTrapDUSER00106

Alarm name	`av1xTrapDUSER00106`
Alarm text	`The maximum number of failed login attempts has occurred for user.`
Alarm level	ERROR - impacts system access
Trigger component	User Service

Problem description

A user failed to enter the correct login information after the allowed number of attempts.

Proposed Solution

About this task

Provide the correct log-in ID and password to the user and ask the user to try again.

av1xTrapDUSER00107

Alarm name	av1xTrapDUSER00107
Alarm text	A login attempt by user {x} has failed.
Alarm level	ERROR - impacts system access
Trigger component	User Service

Problem description

The specified user failed to successfully login to the system.

Proposed Solution

Procedure

1. Validate the user log-in ID and password.
2. Provide the correct log-in ID and password to the user, and ask the user to try again.

Statistics Alarms

av1xTrapDSTAT00001

Alarm name	av1xTrapDSTAT00001
Alarm text	Statistic Service Started.

Alarm level	INFO - General information
Trigger component	Statistics Service

Problem description

The Statistics Service started successfully on Client Enablement Services.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapDSTAT00002

Alarm name	`av1xTrapDSTAT00002`
Alarm text	`Statistic Service Stopped.`
Alarm level	INFO - General information
Trigger component	Statistics Service

Problem description

The Statistics Service stopped successfully on Client Enablement Services.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapDSTAT00003

Alarm name	`av1xTrapDSTAT00003`
Alarm text	`Scheduler task to trim performance statistics completed successfully. {0}Records deleted.`
Alarm level	INFO - General information

Trigger component Statistics Service

Problem description

The scheduler successfully deleted the reported {0} number of performance statistics records from the Client Enablement Services database. All records older than the configured retention time are trimmed.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapDSTAT00004

Alarm name `av1xTrapDSTAT00004`

Alarm text `Scheduler task to trim Feature usage statistics completed successfully. {0}Records deleted.`

Alarm level INFO - General information

Trigger component Statistics Service

Problem description

The scheduler successfully deleted the reported number {0} of feature usage statistics records from the Client Enablement Services database. All records older than the configured retention time are trimmed.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapDSTAT00005

Alarm name `av1xTrapDSTAT00005`

Alarm text `Scheduler task to trim Performance statistics records failed.`

Alarm level WARNING - may impact system operation

Trigger component Statistics Service

Problem description

The Scheduler was unable to delete performance statistics records from the Client Enablement Services database.

Proposed Solution

About this task

Check the log files to find the reason for the failure.

You can also delete performance statistics records from the database if the table gets too big and trim cannot be performed using the **Scheduler** tab in the Client Enablement Services administration application.

For more information on statistics cleanup, see “Scheduling Statistics Cleanup” in Chapter 5, “Scheduler administration,” in *Administering Avaya one-X® Client Enablement Services*.

For more information on configuring statistics, see “Statistics configuration” in Chapter 6, “System administration,” in *Administering Avaya one-X® Client Enablement Services*.

For more information on deleting the performance statistics records, see Unable to administer statistics table on page 39.

---

av1xTrapDSTAT00006

Alarm name `av1xTrapDSTAT00006`

Alarm text `Scheduler task to trim Feature usage statistics records failed.`

Alarm level WARNING - may impact system operation

Trigger component Statistics Service

Problem description

The Scheduler was unable to delete feature usage statistics from the Client Enablement Services database.

Proposed Solution

About this task

Check the log files to find the reason for the failure.

You can also delete feature usage statistics records from the database if the table gets too big and trim cannot be performed using the **Scheduler** tab in the Client Enablement Services administration application.

For more information on statistics cleanup, see “Scheduling Statistics Cleanup” in Chapter 5, “Scheduler administration,” in *Administering Avaya one-X® Client Enablement Services*.

For more information on configuring statistics, see “Statistics configuration” in Chapter 6, “System administration,” in *Administering Avaya one-X® Client Enablement Services*.

For more information on deleting the feature usage statistics records, see Unable to administer statistics table on page 39.

av1xTrapDSTAT00007

Alarm name	`av1xTrapDSTAT00007`
Alarm text	`Cannot access Statistics system configuration. Using defaults.`
Alarm level	WARNING - may impact system operation
Trigger component	Statistics Service

Problem description

The Statistics Service could not obtain system configuration from the Client Enablement Services database. The Statistics Service is using default values for the service configuration.

Proposed Solution

About this task

Check if the database is available.

Active Directory Alarms

av1xTrapQDIRS00001

Alarm name	`av1xTrapQDIRS00001`
Alarm text	`Could not establish connection to the LDAP server.`
Alarm level	ERROR - impacts system operation
Trigger component	Active Directory Server

Problem description

The Active Directory server could not establish a connection to the LDAP server.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator, or call Avaya Technical Support for assistance.

av1xTrapQDIRS00002

Alarm name	`av1xTrapQDIRS00002`
Alarm text	`Error during communication with the LDAP server.`
Alarm level	WARNING - may impact system operation
Trigger component	Active Directory Server

Problem description

The Active Directory server received an error while it was communicating with the LDAP server.

Proposed Solution

About this task

Retrieve the log files to find the cause of the error.

---

av1xTrapQDIRS00003

Alarm name	`av1xTrapQDIRS00003`
Alarm text	`User Identity Server not available or disabled.`
Alarm level	ERROR - impacts system operation
Trigger component	Active Directory Server

Problem description

The User Identity server is either unavailable to the Active Directory server or the User Identity server is not running.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator or call Avaya Technical Support for assistance.

---

av1xTrapQDIRS00004

Alarm name	`av1xTrapQDIRS00004`
Alarm text	`No Enterprise User Store Server available or disabled.`
Alarm level	ERROR - impacts system operation
Trigger component	Active Directory Server

Problem description

The Enterprise User Store server is either unavailable to the Active Directory server or the Enterprise User Store server is not running.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator or call Avaya Technical Support for assistance.

---

av1xTrapQDIRS00005

Alarm name `av1xTrapQDIRS00005`

Alarm text `Server is not known to the system or misconfigured.`

Alarm level ERROR - impacts system operation

Trigger component Active Directory Server

Problem description

The server that the Active Directory server is attempting to contact is either not installed on the system or the server is not configured properly on the system.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator or call Avaya Technical Support for assistance.

---

av1xTrapQDIRS00006

Alarm name `av1xTrapQDIRS00006`

Alarm text `Server is in the disabled state.`

Alarm level ERROR - impacts system operation

Trigger component Active Directory Server

Problem description

The server that the Active Directory server is attempting to contact is disabled on the system.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator, or call Avaya Technical Support for assistance.

---

av1xTrapQDIRS00007

Alarm name `av1xTrapQDIRS00007`

Alarm text `Security Domain Primary Server not available or disabled.`

Alarm level ERROR - impacts system operation

Trigger component Active Directory Server

Problem description

The Security Domain Primary server that the Active Directory server is attempting to contact is either not available to the Active Directory server or the Security Domain Primary server is disabled on the system.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator, or call Avaya Technical Support for assistance.

av1xTrapQDIRS00008

Alarm name	`av1xTrapQDIRS00008`
Alarm text	`Directory Synchronization Task failed.`
Alarm level	ERROR - impacts system operation
Trigger component	Active Directory Server

Problem description

The Enterprise Directory Synchronization between the Active Directory server and the Client Enablement Services database failed to complete.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also contact the database administrator, or call Avaya Technical Support for assistance.

av1xTrapDDIRS00322

Alarm name	`av1xTrapDDIRS00322`
Alarm text	`Directory Synchronization Task succeeded.`
Alarm level	INFO - General information
Trigger component	Active Directory Server

Problem description

The Enterprise Directory Synchronization between the Active Directory server and Client Enablement Services database was successfully completed.

Proposed Solution

About this task

No corrective action is required.

Contact Service Alarms

av1xTrapDCONS00405

Alarm name	`av1xTrapDCON00405`
Alarm text	`Startup failed. Could not schedule new Work.`
Alarm level	ERROR - impacts system operation
Trigger component	Contact Service

Problem description

The Contact Service failed to start because it could not schedule new work.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also call Avaya Technical Support for assistance.

av1xTrapDCONS00401

Alarm name	`av1xTrapDCON00401`
Alarm text	`Startup failed. Could not connect to User Service.`
Alarm level	ERROR - impacts system operation
Trigger component	Contact Service

Problem description

The Contact Service failed to start because it could not connect to the User Service.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also call Avaya Technical Support for assistance.

---

av1xTrapDCONS00402

Alarm name `av1xTrapDCON00402`

Alarm text `Startup failed. Could not connect to Directory Service.`

Alarm level ERROR - impacts system operation

Trigger component Contact Service

Problem description

The Contact Service failed to start because it could not connect to the Directory Service.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also call Avaya Technical Support for assistance.

---

av1xTrapDCONS00403

Alarm name `av1xTrapDCON00403`

Alarm text `Startup failed. Could not register at Directory Service.`

Alarm level ERROR - impacts system operation

Trigger component Contact Service

Problem description

The Contact Service failed to start because it could not register at the Directory Service.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also call Avaya Technical Support for assistance.

---

av1xTrapDCONS00404

Alarm name `av1xTrapDCON00404`

Alarm text `Startup failed. Could not create Work Manager.`

Alarm level ERROR - impacts system operation

Trigger component Contact Service

Problem description

The Contact Service failed to start because it could not create a Work Manager.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. Correct the problem and retry the operation.

You can also call Avaya Technical Support for assistance.

---

av1xTrapDCONS00406

Alarm name `av1xTrapDCON00406`

Alarm text `Update VoicemailHandles successful.`

Alarm level	INFO - General Information
Trigger component	Contact Service

Problem description

The Contact Service successfully updated the specified voice mail server names.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapDCONS00407

Alarm name	`av1xTrapDCON00407`
Alarm text	`Update VoicemailHandles failed.`
Alarm level	ERROR - impacts system operation
Trigger component	Contact Service

Problem description

The Contact Service failed to update the specified voice mail server names.

Proposed Solution

About this task

Inspect log files to determine the reason for this failure. Correct the problem and retry the operation.

Database Backup Alarms

av1xTrapDDBBU00001

Alarm name	`av1xTrapDDBBU00001`
Alarm text	`Database backup about to start.`
Alarm level	INFO - General information
Trigger component	Database Backup

Problem description

The Database Backup task is starting. The database is unavailable until the backup is completed.

Proposed Solution

About this task

No corrective action is required.

av1xTrapDDBBU00002

Alarm name	`av1xTrapDDBBU00002`
Alarm text	`Database backup completed successfully.`
Alarm level	INFO - General information
Trigger component	Database Backup

Problem description

The Database Backup task has successfully completed. The database is now available.

Proposed Solution

About this task

No corrective action is required.

---

av1xTrapDDBBU00003

Alarm name	`av1xTrapDDBBU00003`
Alarm text	`Database backup failure message including return code and error text.`
Alarm level	ERROR - impacts system operation
Trigger component	Database Backup

Problem description

The Database Backup task failed. This message includes the return code and error information about the failure.

Proposed Solution

About this task

Use the return code and error information to determine the cause of the failure. Contact the database administrator or Avaya Technical Support if necessary.

---

av1xTrapDDBBU00004

Alarm name	`av1xTrapDDBBU00004`
Alarm text	`Database backup failed.`
Alarm level	ERROR - impacts system operation
Trigger component	Database Backup

Problem description

The Database Backup task failed.

Proposed Solution

About this task

Notify the database administrator.

Index

Numerics

A

B

C

D

E

H

I

L

M

N

O

P

Q

S

T

U

V

W