Troubleshooting Avaya one-X® Client Enablement Services

Release 6.2.5
Issue 1
April 2016

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 may generally make available to users of its products and Hosted Services. 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 websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. 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 website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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 You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail

account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of 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). You 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").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, 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 website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Overview

Troubleshooting overview

This Troubleshooting guide is intended for system administrators or system maintenance technicians. It is assumed that they have the necessary access and expertise to use the various products discussed in this guide such as Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Aura® System Manager.

The document addresses the unexpected issues the system administrators or the users encounter and the proposed solutions.

This guide is divided in following 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 while using the Avaya one-X® Mobile client application.
5. Chapter 5 discusses the issues faced 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. The chapter provides information on the alarm name, the alarm text, the alarm level, the trigger component, the problem description, and the troubleshooting steps.

Troubleshooting tools

Troubleshooting handset server installation

- IBM Java VM
- MX Client Utilities such as JConsole, JVisual VM
- IBM Support Assistant toolset

Websphere Application Server (WAS)

- Health status check agents that are a part of IBM Support Assistant

Related links

WebSphere log files on page 84

Related product documents

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

Product name	Documentation
Communication Manager	See the appropriate guide from the Avaya support site.
Modular Messaging	See the appropriate guide from the Avaya support site.
Avaya Aura® Messaging	See the appropriate guide from the Avaya support site.
Conferencing	See 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	See the appropriate guide from the Avaya support site.

You can also see the following 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*

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service

request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Troubleshooting implementation issues

Troubleshooting the Avaya one-X® Client Enablement Services installation

About this task

To troubleshoot problems while installing 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 enterprise process to obtain support.

Unable to gain access to 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

Use the `xm list` command to view 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 on to System Domain (Domain-0) as `admin/admin01`.
2. Type **`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`, 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 appropriate Client Enablement Services template.
- **Kernel mismatch**: Restart 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**: Restart cdom from System Platform Web Console. In the left pane, click **Virtual Machine Management** > **Manage**. Click the **cdom** link and then click **Reboot** and start 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. Restart cdom from System Platform Web Console and start 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 gain access to System Manager
  - Ensure that LDAP is functional.

Linux installation fails

The Linux installation might 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.
- Installation failures:
  - Insufficient memory

  - Insufficient disk size
  - Wrong RHEL version
  - Missing RPM in the system
  - Configuration management tools are enabled
  - Other issues
- Post-installation configuration failures:
  - *cesadmin* user authorization failure
  - Network IP address or FQDN is blank on the Network Settings Web page
  - Other issues

Troubleshooting steps

Procedure

Select the solution that matches the reason for Linux failure:

- **Checksum mismatch**: Download the installer files again.
- Installation failures:
  - *Insufficient memory*: Check the available RAM on the system, and then install Client Enablement Services.
  - *Insufficient disk size*: Check the available disk size in the `/opt` and `/home` partitions on the system, and then install Client Enablement Services.
  - *Wrong RHEL version*: Ensure that you have installed the supported RHEL version.
  - *Missing RPM in the system*: Install the missing RPM packages using the yum or rpm utilities.
  - *Configuration management tools are enabled*: Disable any configuration management tools on the RHEL system
  - *Other issues*: Check the logs in the `/var/log/ces/install` directory.
- Post-installation configuration failures
  - *cesadmin user authorization failure*: Ensure that you are using the correct *cesadmin* user password. If you forget the password, change the password using the RHEL passwd utility in the root account.
  - *Network IP address or FQDN is blank on the Network Settings Web page*: Set up the hosts IP address and FQDN, reboot the Linux server, and restart the Client Enablement Services post-installation configuration tool.
  - *Other issues*: Check the logs in the `/var/log/ces/install` directory.

Unable to rollback Client Enablement Services on Linux

After you upgrade Client Enablement Services on Linux, you are unable to rollback Client Enablement Services if you face any issues.

Troubleshooting steps

About this task

Currently, you cannot rollback the installation of Client Enablement Services on Linux if something goes wrong. However, you can downgrade Client Enablement Services to the version that you were using before the upgrade using the following steps.

When you upgrade Client Enablement Services, the system automatically performs a backup of the existing database and installation settings. The backup file is stored in the `/opt/avaya/backups/ces` directory.

Procedure

1. If the Client Enablement Services upgrade on Linux is not satisfactory, you must uninstall Client Enablement Services using the steps documented in the section on uninstalling Client Enablement Services on Linux in *Implementing Avaya one-X® Client Enablement Services*.
2. Install the version of Client Enablement Services that you were using prior to the upgrade.
3. After you complete the Client Enablement Services installation, run the post-installation configuration tool.
4. In the Install using Migration Archive window, specify the path of the backup file, that is, the file in the `/opt/avaya/backups/ces` directory that the system created when you started the upgrade, and continue with the post-installation configuration.

   The system restores the database backup and the installation settings that Client Enablement Services was using prior to the upgrade.

Template installation pauses indefinitely

The Client Enablement Services template installation pauses indefinitely. Additionally, the `post_install_config.log` file in the `/opt/vsp/log` directory on the system on which you are installing the template logs the following error:

```
./runinstallapps.sh /opt/IBM/WebSphere/AppServer /opt/avaya/1xp avaya ******
< /opt/vsp/bin/input.txt
WASX7023E: Error creating "SOAP" connection to host "localhost"; exception information:
com.ibm.websphere.management.exception.ConnectorNotAvailableException: [SOAPException:
faultCode=SOAP-ENV:Client; msg=Error opening socket: javax.net.ssl.SSLHandshakeException:
com.ibm.jsse2.util.g: PKIX path building failed:
java.security.cert.CertPathBuilderException: PKIXCertPathBuilderImpl could not build a
valid CertPath.; internal cause is:
java.security.cert.CertPathValidatorException: The certificate issued by O=AVAYA,
```

```
OU=MGMT, CN=default is not trusted; internal cause is:
java.security.cert.CertPathValidatorException: Certificate chaining error;
targetException=java.lang.IllegalArgumentException: Error opening socket:
javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.g: PKIX path building failed:
java.security.cert.CertPathBuilderException: PKIXCertPathBuilderImpl could not build a
valid CertPath.; internal cause is:
java.security.cert.CertPathValidatorException: The certificate issued by O=AVAYA,
OU=MGMT, CN=default is not trusted; internal cause is:
java.security.cert.CertPathValidatorException: Certificate chaining error]
```

Troubleshooting steps

Before you begin

If you are using System Manager, you must verify the certificates on System Manager before you install Client Enablement Services.

Procedure

1. Revisit the expiry date of the System Manager certificates.
2. Regenerate the certificates on System Manager.
3. Cancel the current Client Enablement Services installation.
4. Restart cdom from System Platform Web Console.
5. Start the Client Enablement Services installation.

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
- You did not restart cdom after deleting the existing template

Troubleshooting steps

Procedure

Perform the following:

- Log on to System Platform Web Console and ensure that the Client Enablement Services virtual machine is running.

- Log on to the CLI of the Client Enablement Services virtual machine as an administrator. If the log in fails, restart the Client Enablement Services virtual machine using System Platform Web Console and try logging in again.
- Log on to the CLI of the Client Enablement Services virtual machine as a root user and run 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 `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 restart the cdom using System Platform Web Console and start the installation again.
- If you are installing a new template, you must restart the cdom using 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 restart the cdom using System Platform Web Console, after you delete the existing template.

Troubleshooting steps

About this task

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

Procedure

1. Delete the template.
2. Restart Tomcat by performing the following steps:
   a. Log on to the cdom as `admin/admin01`.
   b. Type **`su -`** to log in as root.
   c. At the prompt, type `/sbin/service tomcat restart`
3. Log on to System Platform Web Console.
4. Install the template.

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

You cannot log on 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 Administrator Security Group.
- Ensure that the database is running.
  - If the database is not running, log on to the CLI of the Client Enablement Services server as root user.
  - Change to the dbinst user using the `su – dbinst` command.
  - Run the `db2start` command.
  - Change to the root user and restart WAS by using the `service 1xp restart` command.
- If you are using secure LDAP, verify that the LDAP certificate is imported in the Client Enablement Services trust store. You can perform this by using the Presence Services Adapter web admin page in **Servers** > **Presence**.

Administration application displays an error after template installation

When the password of the LDAP service account has a $ (dollar) 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 must avoid using special characters in the LDAP service account password such as $ (dollar). You must also avoid using the hypen (-) in the user name.

Proposed solution

Procedure

1. Change the password of the LDAP service account.
2. Delete the existing template.
3. Reboot the dom-0.
4. Reinstall the template.

   For more information on each step, see *Implementing Avaya one-X® Client Enablement Services* guide.

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

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

Troubleshooting steps

Procedure

1. Log on to the CLI of the server on which you installed Handset Server.
2. Check if Handset Server is running and the current configuration is correct using the `sh /opt/avaya/HandsetServer/bin/configure_hs.sh status` command.
   - If Handset Server is not running, start Handset Server using the `service xinetd start` command.
   - If Handset Server is running, restart Handset Server using the `service xinetd restart` command. Restart 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 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 unavailable status indicates that Transcoding Service is unable to connect to Transcoding Server or the Transcoding Server configuration has a problem.

Troubleshooting steps

Procedure

Perform the following:

- 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. Transcoding Server can function on both the loopback and the Client Enablement Services IP address.

SSL connection between servers fails

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

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

Troubleshooting steps

Procedure

1. Log on to cdom and the Client Enablement Services system using the SSH terminal as user `craft/craft01` and then change 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 the time zone 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 `/vspdata/log/vsp/vsp-all.log` 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`
- `/etc/xinetd.d/onexces`

Handset Server files

The Handset Server installer configures xinetd service for traffic routing. The system saves the Handset Server specific configuration settings in the `onexces` file located in the `/etc/xinetd.d` directory. As the first troubleshooting action, ensure that the system correctly saves the configuration in the `/etc/xinetd.d/onexces` file. If the configuration information is correct, check xinetd routing.

IHS files

You can check the IHS log files in the following locations to troubleshoot connectivity issues:

- `/opt/IBM/HTTPServer/logs/error_log`
- `/opt/IBM/HTTPServer/logs/access_log`

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

Enabling the VNC server for maintenance

Before you begin

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

About this task

By default, the VNC server is installed on System Platform deployments. However, for RHEL deployments, you must install the VNC server.

Procedure

1. Log on to the Client Enablement Services server using the 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.
3. (Optional) Type the password, and confirm the password.

   The VNC server session starts in non-graphical mode.

   As the VNC server session does not run in graphical mode, you must stop the VNC server.
4. Stop the VNC server session using the `vncserver -kill :1` command.
5. To enable the VNC server to start in graphical mode, edit the `xstartup` file, which 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`
6. Save the changes.

7. To start the VNC server again, type the `vncserver` command.
8. In the VNC client, type the IP address of the Client Enablement Services server.
9. Log in with the VNC server password that you created in Step 3.

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, use the Login page to reach one of the pages of the Client Enablement Services administration application.

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

After you install the Client Enablement Services template and 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 to the administration application using the service account

Sometimes the administrator is unable to log in to 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 an 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 to the administration application, but able to log in to the server CLI

Sometimes the administrator is unable to log in to the administration application or the client application, but able to log in to 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, participants who are on hold might not hear the on-hold music. To fix this problem, 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 does not import all users.

Proposed solution

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 the 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 the 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. The administrator must assign the mobile resource separately to the users after data migration is complete. For more information about assigning a mobile telephony resource to a user section, see *Administering Avaya one-X® Client Enablement Services* .

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 a 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 the `/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 the servers 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 system administrator sets the logger to the star sign (*) and the level 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, restart 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 ***** (star) 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 download to the Avaya one-X® Mobile client application.

Proposed resolution

Procedure

1. In the administration application, click the **Servers** tab.
2. In 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. In the left navigation pane, select **Voice Messaging**.
8. Click **Restart** to stop and restart the service.
9. Restart the WAS.
   a. Log in to the Client Enablement Services server using the SSH terminal.
   b. On the shell prompt, type the **`service 1xp restart`** command to restart the Client Enablement Services server.

      To stop the server, the system prompts you to enter your user name and password.
   c. Enter your admin_user_name and admin_user_password.

      The system stops and restarts the Client Enablement Services server.
10. Select the **Servers** tab.
11. In 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 check your changes.

    The results of the test should display the Modular Messaging server as connected.

Users not present in the unprovisioned user list

The user is not present in the unprovisioned users list on the **Users** > **Unprovisioned users** page in the Client Enablement Services administration application.

Proposed solution

Procedure

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

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

   For more information on scheduling Enterprise Directory synchronization, see *Administering Avaya one-X® Client Enablement Services*.
5. To verify whether the user is present in the unprovisioned users list, select the **Users** tab in the administration application.
6. 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 *Administering Avaya one-X® Client Enablement Services*.

Users are not imported on enterprise directory synchronization

If the LDAP settings specified during the Client Enablement Services server installation are not correct, server is unable to import users on enterprise directory synchronization. If the **Contains User Accounts** check box is not selected for the specified LDAP domains, server is unable to import users.

Proposed solution

Procedure

1. Verify the content of the `/opt/vsp/bak/preinstall.properties` file on the Client Enablement Services server host.
2. Verify that all user domains have the **LDAP_DOMAIN_CONTAINS_USERS_X** property set to **true**.

   In this property, **X** is the domain index in the `preinstall.properties` configuration file.

For a split domain configuration, you must verify this step for the user domain.

3. If the setting mentioned in Step 2 is set to **false** for one or more user domains, you must reinstall the Client Enablement Services server with correct LDAP settings.

   In case of a split Active Directory configuration, the **Contains user accounts** check box must be selected for the user domain. In case of multiple Active Directory domains, the **Contains user accounts** check box must be selected for all user domains on the LDAP details page.

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

Before you follow these steps, ensure that 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 value of the **Far-end domain** field 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 the same.
2. Verify that the value of the **Far-end Listen Port** field on Communication Manager and the value mentioned in the **Port** field for the SIP Local server on the Client Enablement Services administration application are the same.
3. Verify that the value of the **Near-end Listen Port** field 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 the 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 the same. The protocol should be using either TCP or TLS.

5. Verify that the value of the **Authoritative Domain** field 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 the 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 information 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 you cannot see the ONE-X mapping for a user extension in Communication Manager even if you configured a mobile telephony resource 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 more information on assigning a mobile telephony resource to the user, see *Administering Avaya one-X® Client Enablement Services* .

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.

   Verify that the **Type** field displays the type of the server, that is **cm**, and the **State** field displays the **Connected** status.
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 connection is Idle or Down, click **Restart** to reconnect the adapter.

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.

   Check that the ONE-X mapping for the extension of the user has two zeros appended before the extension. For example, 00<*extension of the user*>.

7. On the Status Station <extension> page, verify the value of the **one-X Server Status** field.

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

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 the Status Station<extension> page, verify the value of the **one-X Server Status** field.

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

Proposed solution 3

Procedure

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

   Each station that Client Enablement Services controls requires one PBFMC and one EC500 license, regardless of the number of ONE-X mappings that the station 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 the Status Station<extension> page, verify the value of the **one-X Server Status** field.

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

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

When a user enters a mobile number on the account information page in the client application, the system does not map the ONE-X mapping for that mobile number 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 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`**.

      Where xxxx is the mobile number that is mapped on Communication Manager.

      The system displays all numbers that are mapped on Communication Manager for the user. If this number is already mapped to some other extension, Communication Manager displays the extension.

2. If the existing mapping is a manual mapping of the user extension for features such as EC500 and CSP on Communication Manager, go to the Change off-pbx18 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 *Administering Avaya one-X® Client Enablement Services*.

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 sets to the 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 more information about assigning a telephony resource to the user, see *Administering Avaya one-X® Client Enablement Services*.

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`**

Where xxxx is the mobile number that is mapped on Communication Manager.

The system displays all numbers that are mapped in Communication Manager for users. If this number is already mapped to some other extension, Communication Manager displays the extension.

2. If the existing mapping is a manual mapping of the user extension for features such as EC500 and CSP on Communication Manager, go to the Change off-pbx18 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 *Administering Avaya one-X® Client Enablement Services*.
4. Update the mobile number on the Mobile Telephony resource page for the user whose mobile number you want to update.

   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 require one PBFMC license and one EC500 license. Therefore, when you delete a user from the Client Enablement Services server, the system also deletes the ONE-X mapping for the user on Communication Manager.

However, sometimes even though the administrator deletes the user from the Client Enablement Services server, the user account still requires a license on Communication Manager. The user account retains the ONE-X mapping and controls 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.

   When you change the COR of the station, Communication Manager immediately removes the ONE-X mapping and the Client Enablement Services server control of the station.
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 synchronization 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 is restored, the user mappings are restored automatically on Communication Manager and all features are enabled.

The link connects automatically in approximately 10 to 15 minutes, and this connection 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, restart the Communication Manager service adapter from the Client Enablement Services administration application.

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 the 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 difficult to administer.

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 the directory to `/opt/avaya/1xP/`.
4. Run 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 the following:

```
[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.
```

Handset server does not start after a system restart

Handset server does not start 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 xinetd start`**

   The handset server starts.

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, the 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, the user 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*. The email address must not have any special character such as +, !, #.

If the administrator is unable to contact the user, the administrator must perform the following procedure.

Procedure

1. In the administration application, select the **Users** tab.
2. From the left pane, select **Provisioned Users**.
3. On the Provisioned Users page, select the user whose mobile telephony resource you want to update.
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 about mobile telephony resource fields, see *Administering Avaya one-X® Client Enablement Services* .
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 a mobile number in the 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: `Unable to Validate Phone Number`.

This problem occurs 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. In the Client Enablement Services administration application, select the **Servers** tab.

2. In 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 to make the number 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`** where*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 to the Avaya one-X® Mobile client application

The user cannot 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 a telephony resource and a mobile telephony resource are assigned to the user.
   a. Click the **Users** tab.
   b. In the left pane, select **Provisioned Users**.
   c. Select the user whose resource you want to verify.
   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 more information about assigning a resource, see *Administering Avaya one-X® Client Enablement Services.*
3. In the Client Enablement Services administration application, click the **Monitors** tab and verify that the handset service is 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 xinetd 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 upgraded the Client Enablement Services server from Release 6.1, perform the following steps after you complete the upgrade.

If you newly installed the Client Enablement Services server, perform the following steps after you provision all users. For more information about provisioning a user, see *Administering Avaya one-X® Client Enablement Services*.

Procedure

1. In the Client Enablement Services administration application, select the **Monitors** tab.
2. In 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 xinetd restart`**
5. The user should try again to log in to the client application.

Mobile client application prompts the user to enter the 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 the account information again after the system administrator enables the user account.

Proposed solution

Procedure

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

For more information about logging off and deleting user sessions, see *Administering Avaya one-X® Client Enablement Services*.

Call logs not visible

You cannot see the call logs 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**.

Messaging adapter is still in connected state after the voice messaging server is stopped

In the Client Enablement Services administration application, under the **Monitors** tab, the voice messaging adapter is still in the connected state even when the voice messaging server is down. The voice messaging adapter must be in the down state.

Proposed solution

Procedure

1. Log in to the Client Enablement Services administration application.
2. Click the **Servers** tab.
3. In the left pane, click **Voice Messaging**.
4. On the Voice Messaging page, click the name of a messaging server in the **Handle** field.
5. Click **Test**.

   The server displays the real status of the messaging service. You can also refresh the server status on the **Monitors** tab.

Avaya one-X® Mobile client application does not accept the voice mail pin

When the user tries to install and configure the Avaya one-X® Mobile client application on a mobile device, the client application might not accept the voice mail pin that the user enters. In this case, 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 installed Modular Messaging, apply proposed solution 1.

If you installed Avaya Aura® Messaging, apply proposed solution 1.

Proposed solution 1

Procedure

1. Log in to the Modular Messaging MSS administration application.
2. In the left navigation pane, in **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, in **Subscriber Features and Services**, set the value in the**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 system overrides the Restrict Client Access control if you set the **Privacy Enforcement Level** value to **Full** in the Voice Mail System Configuration (VMSC) program on the Messaging Application Server (MAS).

   For more on information about managing a class of service, see *Avaya Modular Messaging for Avaya MSS Release 5.2 Installation and Upgrades*.

   For more on information about privacy enforcement level, see *Avaya Modular Messaging Release 5.2 with the Avaya MSS MAS Administration Guide*.

Proposed solution 2

Procedure

1. Log in to the Messaging server system management interface.
2. In the left navigation pane, in **Messaging System (Storage)**, click the **Class of Service** link.
3. Verify that the Class of Service assigned to the user has all the required permissions.

   If the Class of Service assigned to the user does not have the required permissions, you can assign a different class of service to the user.

   For more information about managing a class of service, see the *Administering Avaya Aura® Messaging* guide.
4. In the left navigation pane, in **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 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 that is 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 you restart the Presence Services server, 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. Restarting the WAS using the **`service 1xp stop`** command also does not work.

Sometimes, the presence adapter is connected, but the presence status does not get updated 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**.

Presence Services server stuck in the starting state

The Presence Services server can get stuck in the **Starting** state due to following reasons among others:

- Incorrect Presence Services adapter version used.
- Presence Services server is unable to resolve the FQDN of System Manager or vice versa.
- Presence Services is unable to retrieve the System Manager certificate because of incorrect or expired enrollment password.

Proposed solution

About this task

If you used an incorrect Presence Services adapter version, you must recreate the Presence Services adapter. If the Presence Services adapter is being used by users, then you must manually remove the Presence Services resource for all users, stop the Presence Services adapter, remove the Presence Services adapter, create the new Presence Services adapter, and then add all resources. Alternatively, use the procedure described in Client Enablement Services 6.2 SP4 release notes on *Migration process for the presence services from existing PS to PS 7.0* if the enterprise has number of users.

For the other reasons, change the PostgresSQL settings in Presence Services by using the following steps.

Procedure

1. Log in to the Presence Services server CLI as a root user.
2. Open the data directory using the **cd /var/lib/pgsql/data** command.
3. In the data directory, use the **vi pg_hba.conf** command to modify the pg_ hba.conf file and add the exact IP address ranges with proper masking bit at the end of the file.

   For example, host all all <IP address of the Client Enablement Services server>/32 md5.
4. In the data directory, use the **vi postgresql.conf** command to modify the postgresql. conf file and set **listen_addresses = '*'**.
5. Restart the postgres sql service using the **service postgresql restart** command.
6. Verify the Presence Services connection in the Client Enablement Services administration application.

Telephony adapter stuck in the starting state

Communication Manager supports subscriptions to only 10 Client Enablement Services servers simultaneously. The telephony adapter can get stuck if you integrate the same Communication Manager system with more than 10 Client Enablement Services servers.

Proposed solution

About this task

Remove the unused subscriptions to Client Enablement Services.

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 coresident Handset server installation, log in to the Client Enablement Services server or in case of a standalone Handset server installation, log in to the Handset server.
2. Restart the Handset server using the command: **service xinetd 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.

User experiences delay while logging in to Avaya one-X® Mobile

Customers might observe long Avaya one-X® Mobile login delays, 20 to 30 seconds, for users provisioned with a Voice Messaging resource while nearly no delay, up to 5 seconds, for users without a provisioned Voice Messaging resource.

Proposed solution

The login delay might occur when Client Enablement Services establishes SMTP and IMAP connections. The Voice Messaging server might not have a configured DNS server. Hence, for the Client Enablement Services host name to perform a DNS lookup might take several seconds.

Procedure

If the DNS server is not set up on the Voice Messaging server as configured in the `/etc/resolv.conf` file, then the administrator must add the Client Enablement Services host name and IP address into `/etc/hosts` on the Voice Messaging server.

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 more information about deleting provisioned users, see *Administering Avaya one-X® Client Enablement Services*.
9. Provision the user again.

   For more information about provisioning an unprovisioned user, see *Administering Avaya one-X® Client Enablement Services*.

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

When the system administrator sets the **Extension Contact Logging (SipService)** property in **System profile** to **24*7** in the Client Enablement Services administration application, the dialed string conversion number displayed on the administration application differs from the number displayed on the client application.

For example, in the Client Enablement Services administration application Dial plan page, you configure a dial plan so 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, the number displays 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 Avaya one-X® Mobile client application displays the presence of a SIP user 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 value in the **Type of 3PCC Enabled** field 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

The system administrator is unable to monitor the audio transcoding service from the Monitors page in the administration application. The system display the 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 the 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, perform the following steps:

   a. Log in to the WebSphere administration console.
   b. From the left navigation pane, click **Applications**.
   c. Click **Application Types**.
   d. Click **WebSphere enterprise applications**.
   e. On the Enterprise Applications page, select the check box adjacent to **1X_Adapter_AudioTranscoding**.
   f. Click **Stop**.
   g. 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 pause indefinitely waiting for the database to start. This pause can happen if the database has encountered problems, and the system displays the 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**

   When you exit, the system reverts the user back to the previous login state, which is the root user.
6. Start the WAS using the command: **service 1xp start**

   The system displays a message similar to the following message:

```
Starting WebSphere Application Server - server1 ...
waiting for db2
. db2 running
ADMU0116I: Tool information is being logged in file
  /opt/IBM/WebSphere/AppServer/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 long time to execute, say 20 minutes or so, or the process pauses indefinitely..

Proposed solution

Procedure

1. Log in to the Client Enablement Services server CLI as root.
2. Run the command **ps –ef | grep onexps** to obtain 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.

You can observe this problem 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 a 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 due to 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*’

      Type these commands in the CLI, and do 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.

Unable to delete a disabled user account or delete any resource assigned to the user account

Administrator is unable to delete a user account or any resource assigned to the user even if the user account is in a disabled state and does not have an active session. The system displays the following error message when the administrator tries to delete the user:

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

Proposed solution

Before you begin

Ensure that the user account is in a disabled state and there is no active session displayed on the Users page in the Avaya one-X® Client Enablement Services administration application.

About this task

If you cannot delete or modify a user or user resource, you have to force delete the user. You must follow this procedure even when you want to modify a resource assigned to the user, but the system displays an error message. After force deleting a user, provision the user and assign all the resources.

For more information about provisioning a user resource and assigning resources to a user, see *Administering Avaya one-X® Client Enablement Services*.

Procedure

1. Log in the administration application.
2. Click the **System** tab.
3. From the left navigation pane, select **Logging**.
4. In the **General Logging** section, select **All**.
5. In the **Aspect Logging** section, perform the following:
   a. In the **Aspect** drop-down list, select **user**.

b. In the **Level** drop-down list, select **Detail**.
c. In the **User ID** field, enter the user account name, and click **Add**.

   The system displays the aspect logging in the **List of Current Aspect Loggers** table.
d. In the **Aspect** drop-down list, select **client**.
e. In the **Level** drop-down list, select **Detail**.
f. In the **User ID** field, enter the user account name, and click **Add**.

   The system displays the aspect logging in the **List of Current Aspect Loggers** table.
g. In the **Aspect** drop-down list, select **api**.
h. In the **Level** drop-down list, select **Detail**.
i. In the **User ID** field, enter the user account name, and click **Add**.

   The system displays the aspect logging in the **List of Current Aspect Loggers** table.

6. Click **Save**.
7. Click the **Users** tab.
8. From the left navigation pane, select **Provisioned Users**.
9. Search for and select the user you want to delete.
10. Click **Force Delete**.

    The system deletes the user.
11. Collect all logs generated as a result of the force delete action.

    These logs are helpful to determine the root cause of this problem.

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.

User is able to log in the client application with the old password

If you have changed the password for a user in enterprise directory but the user is still able to log in the client application using the old password, change the password cache time out settings on the application server.

Proposed solution

Procedure

1. Log on to the IBM web console.
2. In the left pane, under **Security**, click **Global security**.
3. On the Global security page, in the **Authentication** section, click **Authentication cache settings**.
4. Under **General Properties**, set the **Cache timeout** to `60` minutes.
5. Click **Apply**, and log out of the web console.
6. Change the password of the user in the LDAP.
7. Log in to the Client Enablement Services administration application.
8. Click the **Scheduler** tab.
9. In the left pane, click **Enterprise Directory Synchronization**.
10. Click **Run Full Sync Now** for a full synchronization to run immediately and incorporate the password changes.

    The user is able to successfully log in to the client application with the new password. If the user is logged in the client application when you change the password, the 60 minutes of timeout settings begins from the time the user logs out of the client application.

Administrator is unable to log in to the administration application, and users are unable to log in to 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 empty disk space on the database 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 did not stop when the enterprise directory synchronization process began. As a result, the server either responds very slowly or stops responding.

Proposed solution

Procedure

1. For data safety, perform a manual database backup.
    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 to 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 the same value, remove the duplicate value and set the attributes 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 Session Manager is connected or not.

      - If Session Manager is connected, perform Step 2.
      - If Session Manager is not connected, check the network connectivity between the two servers and also check if Session Manager is functional.
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 functional and is reachable by the Client Enablement Services server.

      For example, to check if the telephony adapter is functional, 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 that 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 the system tries to stop the server.
    c. Enter your admin_user_name and the admin_user_password.

    This command stops and restarts the Client Enablement Services server.

Monitoring Client Enablement Services server performance

You can use the IBM console to monitor the performance of the Client Enablement Services server. Administrators can monitor performance when experiencing slow response from the system, or to collect data on performance metric, and generate performance reports.

Proposed solution

About this task

In WebSphere® Application Server, there are a number of tools that administrators can use to monitor the performance of the application server.

See the IBM website for more information about performance monitoring tools.

Call drops immediately after the receiver answers the call

If a call made from one extension to another extension drops immediately after the call is answered, check the IP parameters on Communication Manager.

Proposed solution

Procedure

1. In Communication Manager, enter the command **`display system-parameters features`**.
2. On page 19 of the FEATURE-RELATED SYSTEM PARAMETERS screen, under the **IP PARAMETERS** section, set the **Initial INVITE with SDP for secure calls?** field to **y**.

   Default value of this field is `y`.

   Note that this field is available only when the **Media encryption** field is enabled in Communication Manager license through web interface.

Administrator is unable to log in to the administration application

Attempt to login to the Client Enablement Services server fails and the server displays the following message:

```
SRVE0232E:Internal Server Error. Exception Message: [Filter
[PostLoginFilter]: filter is unavailable.]
```

This problem happens if the DB2 services are not running when the administrator starts the upgrade process.

Proposed solution

Procedure

Administrator must perform a manual check before starting the upgrade process.

For more information about backing up the database, see *Administering Avaya one-X® Client Enablement services*.

Unable to view call details in the desk phone call logs

When you disable the deskphone ringer on the Avaya one-X® Mobile client application, the deskphone ringer turns off but the deskphone 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 deskphone logs all calls when you enable the deskphone ringer OFF option on the Avaya one-X® Mobile client application.

Internal API Error when performing Communication Manager Telephony Synchronization

When you perform Communication Manager Telephony Synchronization, you receive the following error: `Exception in Internal Client API`

Proposed solution

The Client Enablement Services server allocates *30* seconds, default value, to each service. However, the sync operation takes more time. Hence, this affects a lot of enabled users and causes network delays while connecting to the Communication Manager server.

You must increase the value of the *acp.sync.request.timeout* property. Increasing this value does not affect the work of other services.

Procedure

1. Log in to the Client Enablement Services server CLI as *root*.
2. Change to the `/opt/avaya/1xp` directory using the **`cd /opt/avaya/1xp`** command.
3. Open the `system.properties` file using the **`vi system.properties`** command.
4. Change the value of the *acp.sync.request.timeout* property to <*new time*>.
5. Run the **`./run_config_jython.pl`** command.

6. Restart the server using the **service 1xp restart** command.

Calculating the necessary time for the Communication Manager synchronization

About this task

You can increase the time in the *acp.sync.request.timeout* property until the error disappears. You do not need to increase the time by more than 500 000 ms, that is, 8 minutes. Alternatively, you can calculate using the below steps.

Procedure

1. Calculate the required time using the `trace.log` file.
2. Add the *fwservice* protocol logger with *traffic* level.
3. Perform Communication Manager synchronization.
4. Open the Client Enablement Services `trace.log` file in the `/opt/IBM/WebSphere/AppServer/profiles/default/logs/server1` directory using the **vi /opt/IBM/WebSphere/AppServer/profiles/default/logs/server1/trace.log** command.
5. Find the beginning of the sync operation (INVOKE: synchronizedMobileData USER:)

   Example: [5/20/13 10:34:15:714 EDT] 00000067 fwservice 1 INVOKE: synchronizedMobileData USER:

   Start time: 10:34:15:714
6. Search operation is completed. (INVOKE: synchronizedMobileData RETURN:)

   Example: [5/20/13 10:34:55:723 EDT] 00000067 fwservice 1 INVOKE: synchronizedMobileData RETURN:

   End time: 10:34:55:723
7. Calculate the difference between the end time and the start time.

   Example: 10:34:55:723 - 10:34:15:714 = 40 009 ms.
8. Increase this value to resolve the error.

   Example: Add 10000 ms = 10 sec

   New time = 50000, which is sufficient time to complete the synchronization.

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 might 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 might 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.

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 deskphone, while **Block all calls** on your mobile phone is disabled, the call might get simultaneously routed to your voice mail and your mobile phone, thus registering a call entry. Hence, you should always use **Block all calls** on your mobile phone to send all calls to voice mail.

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.

iPhone application shuts down abnormally after reconnecting to Wi-Fi

After you log in to the application, turn off Wi-Fi. Clear your account details by tapping **Settings** > **Account Information** > **Clear Account**. After you reconnect to Wi-Fi, while logging in, the application shuts down abnormally.

Proposed solution

Procedure

Restart the application.

Error on validation of voice mail PIN or mobile number on Android

If a user enters an invalid voice mail PIN for the first time, then re-enters the valid voice mail PIN, the application displays the `Voicemail box failed due to invalid password` message.

You might also face this issue when you enter an invalid mobile number for the first time, and then re-enter the correct mobile number.

Proposed solution

Procedure

After correcting the mobile number or voice mail PIN, ignore the error messages and restart the application.

Verifying if Avaya one-X® Mobile connects to Client Enablement Services directly or using BlackBerry Enterprise Server

Socket connection uses the following types of transport:

- BlackBerry Enterprise Server (BES) using MDS
- BIS (Direct TCP)
- Wi-Fi
- WAP

Procedure

1. Check the logs for the *HssConnectionAttemptListener* instance.

   For example:

   ```
   HssConnectionAttemptListener.attempting(): Attempting - Connection Profile #0
   attemptNumber = 1 url = tls://cesdev.vanguard.com:
   7777;deviceside=false;ConnectionUID=T21210889 IPPP< /> MDS(4)< />
   ```

   - *MDS* indicates that Avaya one-X® Mobile connects to Client Enablement Services using BlackBerry Enterprise Server
   - If you select the **Secure** option on the Login screen as **On**, the URL always has the *tls://* prefix, else the prefix is *socket://*.

2. Use the logs to check the sequence in which the connection attempts occur.

   For example, check the following log snippet:
   `ConnectionProfile.setupConnectionFactory(): MDS(4) WAP 2.0(3) TCP`

```
Cellular(1) TCP WIFI(6) < /> WAP(2) BISB(5) < /> 1< /> 0< />
ACCESS_READ_WRITE (3)< /> 500< /> 30000< /> false< /> false< />
true< />
```

In the log snippet, connection attempts occur in the sequence: MDS->WAP2->TCP Cellular->TCP-Wifi-> WAP 1.0 -> BIS. If a transport method fails, only then the application attempts to use the next option.

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.

User cannot log in to Avaya one-X® Communicator as the Login window continues to load

Proposed solution

If the user observes Avaya one-X® Communicator login failure in the Client Enablement Services mode when the Login window continues to load without the **Cancel** option, there might be some hung threads in Client Enablement Services that result in the problem.

Procedure

Administrator must restart Client Enablement Services using the **`service 1xp restart`** command.

Chapter 6: Avaya one-X® Client Enablement Services Logging Matrix

Logging overview

Client Enablement Servicesprovides the following types of Logging for system analysis and debugging purposes.

- General high-level system logging
- Protocol-level logging
- Aspect-level, also called component-level logging
- Non-Avaya or Internal logging

Logging provides the following types of log files:

- `trace.log`. Contains General, Protocol, and Aspect level logging
- `systemOut.log`. Contains General level logging.
- `stopServer.log`. Contains Service Stop logs.
- `startServer.log`. Contains Service Start logs.
- `systemErr.log`. Contains Error logs.

All the log files are generated at the location: `/opt/IBM/WebSphere/AppServer/profiles/default/logs/server1/`

Logging matrix

Use the logging matrix to decide which logging you should enable to get more information on an issue. The default logging enabled is sufficient to show errors and exceptions that occur in a production environment, but not sufficient to debug problems.

Use this matrix as a guide to which logging you should enable for an issue in any component in Client Enablement Services. You can set the **Aspect Logging** for a service and for users. If the aspect logger does not have a User ID, the logger logs information for the service. If the aspect logger has a User ID, the logger logs information about a specific user. To log information for all users, use `*` as the User ID.

Problem component	Changes in the logging level		
	Logging type	Value	Level
Client application	Aspect	client	Detail
	Aspect	api	Detail
Messaging	Protocol	imap	Traffic
	Aspect	mmclient	Detail
	Aspect	mmservice	Detail
	Aspect	mmsystem	Detail
	Other	com.avaya.acp.service.mm.*	All
Conferencing	Protocol	bcapi	Traffic
	Protocol	spectel	Traffic
	Aspect	mxclient	Detail
	Aspect	mxservice	Detail
	Aspect	mxsystem	Detail
	Other	com.avaya.acp.service.mx.*	All
Directory Service	Aspect	dirstores	Detail
	Aspect	ldapclient	Detail
Licensing	Protocol	weblm	Traffic
	Aspect	licensing	Detail
Presence	Protocol	lps	Traffic
	Aspect	prsncclient	Detail
	Aspect	prsncservice	Detail
	Aspect	prsncsystem	Detail
	Other	com.avaya.apas.lps.*	All
	Other	com.avaya.acp.service.apas.connector.*	All
Contact Logger	Aspect	contactlog	Detail
Mobility (EC500)	Protocol	cmapi	Traffic
	Protocol	jtapi	Traffic
	Aspect	cmtelephony	Detail
Missing events from client service	Protocol	fwclient	Traffic

Other loggers

SIP Communication Manager adapter

- com.avaya.onex.service.sipcm.provider.SipCMSwitch
- com.avaya.onex.service.sipcm.provider.SipSessionManager
- com.avaya.onex.service.sipcm.callcontrol.SipMsgRouter

Handset server

- com.avaya.onex.hss.*
- com.avaya.onex.hss.cache.HandsetUserCacheElement

User assistant

- com.avaya.onex.userassistant.AssistantUser

WebSphere log files

Log type	Details
Application logs	WebSphere logs all logging related to the Client Enablement Services application to the `$WAS_HOME/profiles/default/logs/server1/trace.log` file.
Process logs	Native code, including JVM, write data to the process log files. By default, the process log files are stored as `$WAS_HOME/profiles/default/logs/server1/native_stderr.log` and `$WAS_HOME/profiles/default/logs/server1/native_stdout.log`.
JVM log settings	Monitor the health of the running application server using the `System.out` log file. Use the `System.err` log file when performing problem analysis. This file contains exception stack trace information.
Start and stop server logs	Log files generated on start or stop of WebSphere creates logs at `$WAS_HOME/profiles/default/logs/server1/`.
First failure data capture logs	The first failure data capture (FFDC) log file saves information that is generated from a processing failure. This file is located at `$WAS_HOME/profiles/default/logs/ffdc/`.

Related links

Troubleshooting tools on page 12

Chapter 7: Alarms

Alarms overview

Avaya one-X® Client Enablement Services generates alarms and SNMP traps to notify users of system events. Alarms are grouped based on categories. Each alarm category reveals 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.

Adding an SNMP destination for SAL gateway

About this task

If Avaya provides maintenance coverage for the system and alarm notification to Avaya is required, configure traps to be sent to SAL. The SAL gateway acts as an NMS. SAL gateway captures the traps and sends the traps to Avaya Services using INADs traps.

Procedure

1. Click the **System** tab.
2. In the left pane, click **SNMP Destinations**.
3. On the SNMP Destination page, click **Add New SNMP Trap Destination**.
4. On the Add New SNMP Destination Configuration page, enter following details:
   - **Handle**. cdomSALGW
   - **Enable**. selected
   - **Device**. SSG because the traps are sent in INADS format
   - **Host**. IP address of the SAL Gateway on System Platform
   - **Port**. 162 (default)

- **Notification Type**. Trap
- **SNMP version**. 2c

Note:

Leave all other fields blank or set defaults to **None**.

5. Click **OK** to save your changes.

   The system displays a new SAL Gateway SNMP trap destination in the list of SNMP Trap destinations.

Next steps

Generate a test trap after specifying the SNMP Trap destination to test that the SAL gateway and Avaya one-X® Client Enablement Services are configured properly. When you clean up the performance statistics, Client Enablement Services generates an SNMP trap.

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 functional. This is a Core Services alarm that Avaya one-X® Client Enablement Services uses.

Proposed solution

About this task

You do not need to perform any corrective action.

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 that the product license requirements for Avaya one-X® Client Enablement Services are met.

Proposed solution

About this task

You do not need to perform any corrective action. The log `SystemOut.log` is in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DLICN00401*.

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 that the product license requirements for Avaya one-X® Client Enablement Services are met.

Proposed solution

The log `SystemOut.log` is in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DLICN00402*.

About this task

1. In the Client Enablement Services Administration application, click the **System** tab .
2. In the left navigation pane, select **License Server**.
3. Verify the following on the License server page:
   - Verify that the WebLM server is configured.
   - Verify that the connection is functional.
   - Verify that a sufficient number of license units are 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 are not met for 30 days or more. In the restricted mode, you cannot perform some operations.

Proposed Solution

The log `SystemOut.log` is in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DLICN00403*.

About this task

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

For task specific details, see the system log files. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server` directory. Check for *DSCHD00003*.

av1xTrapQSCHE00003

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

Problem description

WebSphere scheduler is not initialized correctly, so it is not possible to use it for any task.

Proposed solution

About this task

The WebSphere Scheduler is not functioning. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server` directory. Check for *DSCHD00005* and *DSCHD00002*.

Common alarms

av1xTrapQCOMM00001

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

Problem description

The requested service is started.

Proposed solution

About this task

You do not need to perform any corrective action.

av1xTrapQCOMM00002

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

Problem description

The requested service is shut down.

Proposed solution

About this task

You do not need to perform any corrective action.

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

You do not need to perform any corrective action.

---

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

You do not need to perform any corrective action.

---

av1xTrapQCOMM00005

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

Problem description

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

Proposed solution

About this task

You do not need to perform any corrective action.

---

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 is resumed. The **Monitors** feature on the Client Enablement Services administration application initiates this alarm.

Proposed solution

About this task

You do not need to perform any corrective action.

---

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 is suspended. The **Monitors** feature on the Client Enablement Services administration application initiates this alarm.

Proposed solution

About this task

You do not need to perform any corrective action.

---

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

You do not need to perform any corrective action.

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

You do not need to perform any corrective action.

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 the dial plan will not be available.

Proposed solution

About this task

Correct the dial plan configuration in the administration application.

For more information about dial plans, see *Administering Avaya one-X® Client Enablement Services*.

Conferencing alarms

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

You do not need to perform any corrective action.

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 are successfully started for the specified user.

Proposed Solution

About this task

You do not need to perform any corrective action.

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 are successfully stopped for the specified user.

Proposed solution

About this task

You do not need to perform any corrective action.

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 information about assigning a conferencing resource to a user, see *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 the Client Enablement Services user using the specified criteria. No data is available to this user if the user is logged in to Client Enablement Services.

In this message, the {0} is the data used to retrieve the user identity and the {1} indicates how {0} is interpreted, either as ANI, PIN, or moderator code.

Proposed solution

About this task

The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server` directory . Check for *DCONF08002*.

If the repair steps do not fix the problem, go to the Avaya Support website at http://support.avaya.com to open a service request.

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 Client Enablement Services Contact Service. This occurs when searching for a user using Phone or UserId via Contact service.

Proposed solution

About this task

Determine if the connection to the Contact Service is disconnected and can be brought back online. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server` directory. Check for *DCONF08003*.

---

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 because the bridge was disconnected from Client Enablement Services.

Proposed solution

About this task

Determine if the connection to the Contact Service is disconnected and can be brought back online. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server` directory. Check for *DCONF09000*.

---

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 try connecting to the server again. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server` directory. Check for *DCONF09001*.

---

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 because the bridge conference was disconnected on Client Enablement Services.

Proposed solution

About this task

Determine why the bridge was disconnected and make sure the bridge can connect. Repeat the original operation. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server` directory. Check for *DCONF09002*.

---

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. This occurs when you add or update bridge participants.

Proposed solution

About this task

Check the settings, make the necessary changes, and try connecting to the server again. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server` directory. Check for *DCONF09003*.

---

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, or 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. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCONF09004*.

---

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

The conference bridge sends an exception that causes a data conversion failure. This failure might have disconnected the bridge.

Proposed solution

About this task

Determine why the bridge disconnected and resolve this issue. If the bridge did not disconnect, check the log files to find out the reason for this failure. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCONF09005*.

---

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 to identify the reason and try to resume services. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCONF09006*.

---

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 try again to suspend services. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCONF09007*.

---

av1xTrapQCONF00016

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

Problem description

An attempt to create a conferencing resource failed. The possible reasons are lack of memory or corrupted or missing resource data.

Proposed solution

About this task

Verify the availability of sufficient system memory and the user configuration on the Client Enablement Services administration application. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCONF09008*.

For more information on assigning a conferencing resource to a user, see *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

Check the log files to determine the reason for this failure. Correct the problem and retry the operation. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCONF09009*.

---

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

Check the log files to determine the reason for this failure. Correct the problem and retry the operation. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCONF09010*.

---

av1xTrapQCONF00019

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

Problem description

The Conferencing service connection to the ContactLog service is unavailable due to a failure in establishing the channel. The system continues to try to make the connection using the auto-retry feature.

Proposed solution

About this task

Check the log files to determine the reason for this failure. Correct the problem, and retry the operation. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCONF09011*.

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 are temporarily stored for playback and display.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG00203*.

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG00204*.

---

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG00205*.

---

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG00206*.

---

av1xTrapQVMSG00008

Alarm name	`av1xTrapQVMSG00008`
Alarm text	`Failure on ContactService data retrieval:{0} criteria: {1}.`
Alarm level	WARNING - may impact 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. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG08001*.

---

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. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG09001*.

---

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 to the server failed because of lack of permissions.

Proposed solution

About this task

Get the required permissions from the system administrator and try again. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG09002*. To check if correct rights are used, see the *Creating a directory for voice messaging server* chapter in *Administering Avaya one-X® Client Enablement Services*.

---

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

An encoding or decoding error occurred on the message in transit and the message got distorted or lost.

Proposed solution

About this task

Check the log files to identify the cause of the problem, rectify the problem, and retry the operation. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG09003*.

---

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 failed for the indicated resource.

Proposed solution

About this task

Check the log files to identify the cause of the problem, rectify the problem, and retry the operation. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG09004*.

---

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 meet the total number of requests from the Client Enablement Services clients.

Proposed solution

The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG09005*.

Procedure

1. In the Client Enablement Services administration application, select the **Servers** tab.
2. In 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 about the issue. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG09006*. Go to the Avaya Support website at http://support.avaya.com to open a service request.

---

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 log in to the Voice Messaging server are incorrect.

Proposed solution

About this task

On the administration application, correct and reset the credentials for the Voice Messaging service. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG09007*.

For more information about Voice Messaging servers, see *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 that the IMAP port is enabled and the firewall does not have any issues. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG09008*.

For more information about Voice Messaging servers, see *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 parameters are provided and correct. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DVMSG09009*.

For more information about Voice Messaging server, see *Administering Avaya one-X® Client Enablement Services*.

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

Retrieve the log files to find the cause of the failure. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for

DVMSG99000. Go to the Avaya Support website at http://support.avaya.com to open a service request.

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 is functional.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00003*.

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00004*.

---

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. A work manager acts as a thread pool for application components in WebSphere.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00006*.

---

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 and is accessible. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00901*.

---

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. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00902*. Correct the problem, and retry the operation.

You can also contact the database administrator or go to the Avaya Support website at http://support.avaya.com to open a service request.

---

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. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00903*. Correct the problem, and retry the operation.

You can also contact the database administrator or go to the Avaya Support website at http://support.avaya.com to open a service request.

---

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. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00904*. Correct the problem, and retry the operation.

You can also contact the database administrator or go to the Avaya Support website at http://support.avaya.com to open a service request.

---

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. A work manager acts as a thread pool for application components in WebSphere.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00905*.

---

av1xTrapQCLOG00009

Alarm name	`av1xTrapQCLOG00009`
Alarm text	`Failure obtaining ContactLogger DB trim transaction size.`
Alarm level	ERROR - impacts 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. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00906*. Correct the problem, and retry the operation.

You can also contact the database administrator, or go to the Avaya Support website at http://support.avaya.com to open a service request.

---

av1xTrapQCLOG00010

Alarm name	`av1xTrapQCLOG00010`
Alarm text	`Failure obtaining ContactLogger DB trim pause value.`
Alarm level	ERROR - impacts system operation
Trigger component	Contact Logger Service

Problem description

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

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00907*.

---

av1xTrapQCLOG00011

Alarm name	`av1xTrapQCLOG00011`
Alarm text	`Failure writing ContactLogger DB trim transaction size.`
Alarm level	ERROR - impacts 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. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00908*. Correct the problem, and retry the operation.

You can also contact the database administrator or go to the Avaya Support website at http://support.avaya.com to open a service request.

---

av1xTrapQCLOG00012

Alarm name	`av1xTrapQCLOG00012`
Alarm text	`Failure writing ContactLogger DB trim pause value.`
Alarm level	ERROR - impacts 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. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00909*. Correct the problem, and retry the operation.

You can also contact the database administrator or go to the Avaya Support website at http://support.avaya.com to open a service request.

---

av1xTrapQCLOG00013

Alarm name	`av1xTrapQCLOG00013`
Alarm text	`Failure acquiring Admin Interface to System Service.`
Alarm level	ERROR - impacts system operation
Trigger component	Contact Logger Service

Problem description

The Contact Logger service failed to communicate with the System service.

Proposed solution

The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DCLOG00910* to understand which service does not work.

Procedure

Restart Client Enablement Services.

The Contact Logger service operates using default values for data generated from the 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 is started.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory.

---

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 the required tasks.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory.

---

av1xTrapDCLOG01901

Alarm name	`av1xTrapDCLOG01901`
Alarm text	`Contact Logger DB cleanup failed.`
Alarm level	ERROR - impacts system operation
Trigger component	Contact Logger Service

Problem description

The Contact Log Cleanup function failed to successfully complete the required tasks.

Proposed solution

About this task

Retrieve the log files to find the cause of the failure. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Correct the problem, and retry the operation.

You can also contact the database administrator or go to the Avaya Support website at http://support.avaya.com to open a service request.

Modular Messaging Alarms

av1xTrapQMMLD00001

Alarm name	`av1xTrapQMMLD00001`
Alarm text	`Resolution failed on ContactService data retrieval.`
Alarm level	WARNING - may impact system operation
Trigger component	Voice Messaging Synchronization

Problem description

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

Proposed solution

About this task

The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DMMLD08001*.

av1xTrapQMMLD00002

Alarm name	`av1xTrapQMMLD00002`
Alarm text	`Resolution failed on UserService data retrieval.`
Alarm level	WARNING - may impact system operation
Trigger component	Voice Messaging Synchronization

Problem description

An attempt to locate a contact information through the User service using extension or mailbox failed during data retrieval.

Proposed solution

About this task

The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DMMLD08002*.

---

av1xTrapQMMLD00003

Alarm name	`av1xTrapQMMLD00003`
Alarm text	`Exception on Contact Service for{0} criteria:{1}.`
Alarm level	ERROR - impacts system operation
Trigger component	Voice Messaging Synchronization

Problem description

The messaging synchronization process failed when connecting to the Contact Service using the userid.

Proposed solution

About this task

The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DMMLD08003*.

---

av1xTrapQMMLD00004

Alarm name	`av1xTrapQMMLD00004`
Alarm text	`Access to MM LDAP store failed with exception.`
Alarm level	ERROR - impacts system operation
Trigger component	Voice Messaging Synchronization

Problem description

The synchronization process to the selected Voice Messaging server failed.

Proposed solution

About this task

Check the log files for the cause of the failure. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DMMLD09001*. 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	Voice 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. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DMMLD09002*. 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

The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DMMLD09003*. Check the service and restart the Client Enablement Services server if the service 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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory.

---

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 by displaying the results.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory.

---

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory.

---

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 required results.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory.

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 phone number.

Proposed solution

About this task

The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DMMLD08001*.

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 extension or mailbox.

Proposed solution

About this task

The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DMMLD08002*.

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 userid.

Proposed Solution

About this task

The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DMMLD08003*.

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

The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DTELE09003*.

Procedure

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

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

   For more information about modifying telephony servers, see *Administering Avaya one-X® Client Enablement Services*.

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

The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DTELE09006*. Go to the Avaya Support website at http://support.avaya.com to open a service request.

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

The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DTELE09007*.

Procedure

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

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

   For more information about modifying telephony servers, see *Administering Avaya one-X® Client Enablement Services*.

---

av1xTrapQTELE00005

Alarm name	`av1xTrapQTELE00005`
Alarm text	`Invalid dialplan for server.`
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

The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DTELE09009*. Go to the Avaya Support website at http://support.avaya.com to open a service request.

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 set up for the same extension.

Proposed solution

The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DTELE08007*.

Procedure

Check the configuration for each user listed and if the users are assigned respective extensions.

Client Enablement Services supports only one user for an extension.

For more information about assigning a telephony resource to a user, see *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	ERROR - impacts system operation
Trigger component	Telephony Server

Problem description

Licenses are not available on Communication Manager. You cannot provision users for mobile telephony in the Client Enablement Services administration application.

Proposed Solution

About this task

The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DTELE09010*. Go to the Avaya Support website at http://support.avaya.com to open a service request.

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSVFW00005*.

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSVFW00006*.

---

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSVFW00010*.

---

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSVFW00018*.

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSVFW00042*.

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSVFW00043*.

av1xTrapQSVFW00007

Alarm name	`av1xTrapQSVFW00007`

Alarm text	`Core WAR shutting down with adapters still running.`
Alarm level	FATAL
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 must not happen.

Proposed solution

About this task

The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSVFW00019*.

Restart the Client Enablement Services server because the server does not support the restarting of Core WAR with other adapters running.

For more information about restarting Client Enablement Services, see *Administering Avaya one-X® Client Enablement Services*.

---

av1xTrapQSVFW00008

Alarm name	`av1xTrapQSVFW00008`
Alarm text	`Database down.`
Alarm level	FATAL
Trigger component	Service Framework

Problem description

The Client Enablement Services database is not running.

Proposed solution

About this task

The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSVFW00045*.

To get access to the Client Enablement Services database, contact the local database administrator, or go to the Avaya Support website at http://support.avaya.com to open a service request.

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 functional.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSVFW00046*.

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 the maximum capacity.

Proposed solution

About this task

Retrieve the log files to find the cause of the failure. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Correct the problem, and retry the operation.

You can also contact the database administrator or go to the Avaya Support website at http://support.avaya.com to open a service request.

User Alarms

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 updated.
- Users moved - number of users whose group assignment was changed.
- Users marked for deletion - number of users identified as removed but whose record is not deleted.
- Users deleted - number of user records deleted, which were marked for deletion.
- Database errors - number of errors during database reads or updates.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DUSER00012*.

av1xTrapQUSER00002

Alarm name	`av1xTrapQUSER00002`
Alarm text	`Invalid property metadata.`
Alarm level	ERROR - impacts system operation
Trigger component	User Service

Problem description

An invalid property description record is found in the database.

Proposed solution

About this task

The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DPROP00001*.

Property description records are created at installation time and must be valid. If this error occurs after installing Client Enablement Services, go to the Avaya Support website at http://support.avaya.com to open a service request.

If this error occurs later, the records might be tampered with or corrupted and the records must be restored.

---

av1xTrapQUSER00003

Alarm name	`av1xTrapQUSER00003`
Alarm text	`Cannot schedule work.`
Alarm level	ERROR - impacts system operation
Trigger component	User Service

Problem description

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

Proposed solution

About this task

Check the log files for errors that caused this problem. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DUSER00201*.

---

av1xTrapQUSER00004

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

Trigger component	User Service

Problem description

A work task recorded an unexpected error.

Proposed solution

About this task

The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DUSER00202*.

If the repair steps do not fix the problem, go to the Avaya Support website at http://support.avaya.com to open a service request.

---

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 in the database. This happens when group selectors are taken from database.

Proposed solution

About this task

Check the log files for errors that caused the problem. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DUSER00203*.

---

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 caused the problem. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DUSER00204*.

---

av1xTrapQUSER00007

Alarm name	`av1xTrapQUSER00007`
Alarm text	`Cannot obtain users marked for deletion.`
Alarm level	ERROR - impacts system operation
Trigger component	User Service

Problem description

If the selected user record is marked for deletion in the User Service synchronization, the administrator cannot gain access to the user record.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DUSER00205*.

---

av1xTrapQUSER00008

Alarm name	`av1xTrapQUSER00008`
Alarm text	`Cannot create work manager.`
Alarm level	FATAL
Trigger component	User Service

Problem description

The User service cannot create the Work Manager for executing asynchronous work tasks. A work manager acts as a thread pool for application components in WebSphere.

Proposed solution

About this task

Check the log files for errors that caused the problem. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DUSER00300*.

If the repair steps do not fix the problem, go to the Avaya Support website at http://support.avaya.com to open a service request.

---

av1xTrapQUSER00009

Alarm name	`av1xTrapQUSER00009`
Alarm text	`Cannot obtain channel to System Service.`
Alarm level	ERROR - impacts system operation
Trigger component	User Service

Problem description

The User service is unable to obtain access to 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 caused the problem. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DUSER00301*.

If the repair steps do not fix the problem, go to the Avaya Support website at http://support.avaya.com to open a service request.

---

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 gain access to 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 caused the problem. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DUSER00302*.

If the repair steps do not fix the problem, go to the Avaya Support website at http://support.avaya.com to open a service request.

---

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 within the maximum number of attempts for logging in.

Proposed solution

About this task

Provide the correct login 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 WARNING - may impact system operation

Trigger component User Service

Problem description

The specified user failed to successfully log in to the system.

Proposed solution

Procedure

1. Validate the user login ID and password.

   The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory.

2. Provide the correct login ID and password to the user, and ask the user to try again.

TRAP_DUSER00109

Alarm name TRAP_DUSER00109

Alarm text `There is a login attempt from an unauthorized device.`

Alarm level WARNING – impacts system access

Trigger component Handset Service

Problem description

Login attempted from an unauthorized device. The device ID of the new device does not match the device ID stored on the Client Enablement Services server.

Proposed solution

Procedure

1. In the administration application, select the **Users** tab.
2. From the left navigation pane, select **Provisioned Users**.
3. Search for and select the user.
4. In the **Mobile Telephony** group box, click **Add**.
5. On the Add Resource page, in the **Device ID** field, enter the unique device ID to identify the mobile phone of the user or if you do not know the device ID, leave the field blank.

   The device ID is populated automatically when the users logs in the client application the first time.

6. Click **Save** to save your changes.

   For more information about assigning a mobile telephony resource to a user, see *Administering Avaya one-X® Client Enablement Services*.

TRAP_DUSER00110

Alarm name	TRAP_DUSER00110
Alarm text	Exceeding licensed active users on Client Enablement Services Server.
Alarm level	Warning - might impact system performance
Trigger component	Handset server or Handset service

Problem description

The Client Enablement Services server supports 2000 active users. Server generates this alarm when 2000 users are already logged in the client application, and one or more users try to log in the client application.

Proposed solution

Procedure

You do not need to perform any corrective action.

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSTAT00002*.

---

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSTAT00004*.

---

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSTAT00005*.

---

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

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSTAT00006*.

---

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 could not 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. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSTAT00101*.

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

For more information about scheduling statistics cleanup, see*Administering Avaya one-X® Client Enablement Services*.

For more information about statistics configuration, see *Administering Avaya one-X® Client Enablement Services*.

For more information about deleting the performance statistics records, see Unable to administer the statistics table on page 42.

---

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 could not 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. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSTAT00102*.

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

For more information about scheduling statistics cleanup, see *Administering Avaya one-X® Client Enablement Services*.

For more information about statistics configuration, see *Administering Avaya one-X® Client Enablement Services*.

For more information about deleting the feature usage statistics records, see Unable to administer the statistics table on page 42.

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 uses default values for the service configuration.

Proposed solution

About this task

Check if the database is available. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DSTAT00103*.

Active Directory Alarms

av1xTrapQDIRS00001

Alarm name	`av1xTrapQDIRS00001`
Alarm text	`Could not establish connection to the LDAP server.`
Alarm level	INFO - General information
Trigger component	Active Directory Server

Problem description

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

Proposed solution

About this task

Retrieve the log files to find the cause of the failure. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory. Check for *DDIRS00302*. Correct the problem and retry the operation.

You can also contact the database administrator or go to the Avaya Support website at http://support.avaya.com to open a service request.

---

av1xTrapQDIRS00002

Alarm name	`av1xTrapQDIRS00002`
Alarm text	`Error during communication with the LDAP server.`
Alarm level	INFO - General information
Trigger component	Active Directory Server

Problem description

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

Proposed solution

About this task

Retrieve the log files to find the cause of the error. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory. Check for `DDIRS00304`.

---

av1xTrapQDIRS00003

Alarm name	`av1xTrapQDIRS00003`
Alarm text	`User Identity Server not available or disabled.`
Alarm level	INFO - General information
Trigger component	Active Directory Server

Problem description

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

Proposed solution

About this task

Retrieve the log files to find the cause of the failure. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory. Check for *DDIRS00310*. Correct the problem and retry the operation.

You can also contact the database administrator or go to the Avaya Support website at http://support.avaya.com to open a service request.

---

av1xTrapQDIRS00005

Alarm name	`av1xTrapQDIRS00005`
Alarm text	`Server is not known to the system or misconfigured.`
Alarm level	INFO - General information
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 properly configured on the system.

Proposed solution

About this task

Retrieve the log files to find the cause of the failure. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory. Check for *DDIRS00314*. Correct the problem and retry the operation.

You can also contact the database administrator or go to the Avaya Support website at http://support.avaya.com to open a service request.

---

av1xTrapQDIRS00007

Alarm name	`av1xTrapQDIRS00007`
Alarm text	`Security Domain Primary Server not available or disabled.`
Alarm level	INFO - General information
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. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory. Check for *DDIRS00318*. Correct the problem and retry the operation.

You can also contact the database administrator or go to the Avaya Support website at http://support.avaya.com to open a service request.

---

av1xTrapQDIRS00008

Alarm name	`av1xTrapQDIRS00008`
Alarm text	`Directory Synchronization Task failed.`
Alarm level	INFO - General information
Trigger component	Active Directory Server

Problem description

The Enterprise Directory synchronization between the Active Directory server and the Client Enablement Services database could not complete.

Proposed solution

About this task

Retrieve the log files to find the cause of the failure. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory. Check for *DDIRS00320*. Correct the problem and retry the operation.

You can also contact the database administrator or go to the Avaya Support website at http://support.avaya.com to open a service request.

---

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 is complete.

Proposed solution

About this task

No corrective action is required. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory.

AcpMIB.TRAP_DDIRS00323

Alarm name	AcpMIB.TRAP_DDIRS00323
Alarm text	`There was a fatal error during one of the parts of the synchronization.`
Alarm level	INFO - General information
Trigger component	Active directory

Problem description

There was a fatal error during one of the parts of the synchronization.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory.

AcpMIB.TRAP_DDIRS00324

Alarm name	AcpMIB.TRAP_DDIRS00324
Alarm text	`There are users present in more than one domain.`
Alarm level	INFO - General information
Trigger component	Active directory

Problem description

There are users present in more than one domain. This check is performed during the synchronization.

Proposed solution

About this task

You do not need to perform any corrective action. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory.

Contact Service Alarms

av1xTrapDCONS00401

Alarm name	`av1xTrapDCON00401`
Alarm text	`Startup failed. Could not connect to User Service.`
Alarm level	FATAL
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. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory. 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	FATAL

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. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory. 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 FATAL

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. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory. 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 FATAL

Trigger component	Contact Service

Problem description

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

A work manager acts as a thread pool for application components in WebSphere.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory. Correct the problem and retry the operation.

You can also call Avaya Technical Support for assistance.

---

av1xTrapDCONS00405

Alarm name	`av1xTrapDCON00405`
Alarm text	`Startup failed. Could not schedule new Work.`
Alarm level	FATAL
Trigger component	Contact Service

Problem description

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

This alarm happens if it is not possible to schedule Contact service start up using the Contact service Work Manager in WebSphere.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1/`directory. 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.

User details are updated from the voice messaging server successfully.

Proposed Solution

About this task

No corrective action is required. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory.

---

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.

User details are not updated successfully from the voice messaging server.

Proposed Solution

About this task

Inspect log files to determine the reason for this failure. The logs are `SystemOut.log` and `traces.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. 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.

The log is `SystemOut.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory.

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.

The log is `SystemOut.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory.

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. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory. Check for *DDBBU00200*. 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. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory.

AcpMIB.TRAP_DDBBU00202

Alarm name	AcpMIB.TRAP_DDBBU00202
Alarm text	`Database backup request rejected: a database backup is already running.`
Alarm level	ERROR - impacts system operation
Trigger component	Database Backup

Problem description

Database backup request was rejected as a database backup is already running.

Proposed Solution

About this task

Notify the database administrator. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1` directory.

av1xTrapDDBBU00203

Alarm name	`AcpMIB.TRAP_DDBBU00203`
Alarm text	`There is not enough disk space to take the db backup.`
Alarm level	ERROR - impacts system operation
Trigger component	Database Backup

Problem description

The database backup task failed because there is not enough disk space to take the database backup.

Proposed solution

Procedure

1. Log in to the Client Enablement Services CLI as a craft user and the switch to the root user.
2. To view the free disk space, run the command: **`df`**

   The value in **Use %** column displays the disk space already filled. The occupied disk space must not exceed 75% of the available disk space. If the **Use%** column value is approaching 75%, follow steps 3 and 4.

3. Copy the files that are needed from the `/opt/avaya/dbbackup/` folder to an external location.
4. Delete the files that are not required in the `/opt/avaya/dbbackup/` folder to free the disk space.

Presence alarms

AcpMIB.TRAP_DPRES09001

Alarm name	AcpMIB.TRAP_DPRES09001
Alarm text	`Communication error on LPS/IPS layer. Error trapped during LPS/IPS command execution (report to administrator). Error is [{0}]. Look at the logs.`
Alarm level	ERROR - impacts system operation
Trigger component	Presence Services

Problem description

Communication error on LPS/IPS layer.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory.

AcpMIB.TRAP_DPRES08001

Alarm name	AcpMIB.TRAP_DPRES08001
Alarm text	`Command error on LPS/IPS communication layer. Warning trapped during LPS/IPS command execution. Warning is [{0}].`
Alarm level	ERROR - impacts system operation
Trigger component	Presence Services

Problem description

This is warning if there is error during command execution to Presence Services.

Proposed Solution

About this task

Retrieve the log files to find the cause of the failure. The logs are `SystemOut.log` and `SystemError.log` in the `$WAS_HOME/profiles/default/logs/server1/` directory.

Other alarms

v1xTRAPDUSER00111

Alarm name	v1xTRAPDUSER00111
Alarm text	`Default certificate detected in HSS key store. In order to avoid security issues - please replace it.`
Alarm level	WARNING - may impact system security
Trigger component	Certificates

Problem description

Default certificate detected in HSS key store.

Proposed Solution

Replace default certificates with 3rd party or System Manager certificates.

For more information on replacing default certificates with 3rd party or System Manager certificates, see “Migrating the IBM HTTP Server keystore to Handset Service” in *Implementing Avaya one-X® Client Enablement Services*.

About this task

You need to replace default certificates, if you have installed Client Enablement Services without configuring System Manager.

Default certificates might cause security issues on your system.

v1xTRAPDCSDK00012

Alarm name	v1xTRAPDCSDK00012

Alarm text	`Default certificate detected in IBM HTTP Server. In order to avoid security issues - please replace it.`
Alarm level	WARNING - may impact system security.
Trigger component	Certificates

Problem description

Default certificate detected in IBM HTTP Server.

Proposed Solution

Replace default certificates with 3rd party or System Manager certificates.

About this task

You need to replace default certificates, if you have installed Client Enablement Services without configuring System Manager.

Default certificates may cause security issues on your system.

Index

Numerics

A

B

C

D

E

F

H

I

L

M

O

P

Q

S

T

U

V

W