Avaya Aura® Contact Center Troubleshooting

Release 6.4
44400-712
Issue 05.03
December 2014

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: http://support.avaya.com 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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 type(s)

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.

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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You 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.

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: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

Avaya, the Avaya logo, Avaya one-X® Portal, Avaya Aura® Communication Manager, Avaya Aura® Experience Portal, Avaya Aura® Orchestration Designer, Avaya Aura® Session Manager, Avaya Aura® System Manager, and Application Enablement Services are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

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

Contents

Chapter 1: New in this release

The following sections describe what is new in *Avaya Aura® Contact Center Troubleshooting* (44400-712) for Release 6.4.

Features

See the following sections for information about feature changes:

Agent Desktop log file and workflow collection

The Agent Desktop log file and workflow collection feature allows agents to easily collect all Agent Desktop logs and relevant screen captures. Agents can upload this information directly to the Contact Center Multimedia (CCMM) server with a single click. This feature makes it easier for support staff to quickly gather all the information they need to debug issues on Agent Desktop. For more information about Agent Desktop log file and workflow collection, see Agent Desktop troubleshooting on page 83.

Agent validation audits

Avaya Aura® Contact Center automatically audits the agent and supervisor configuration data for discrepancies. The agent validation audit does not require user interaction or configuration; it runs automatically for two intervals each day at 11:00 AM and 11:00 PM. Avaya Aura® Contact Center reports any detected discrepancies in the Contact Center Manager Server database to the contact center Administrator. Avaya Aura® Contact Center also generates Invalid Agent Audit report data and stores the data in Contact Center Manager Server database views accessible to the customer for reporting.

For more information, see Agent and Supervisor configuration troubleshooting on page 208.

Avaya Aura® Unified Communications platform

Contact Center uses industry-standard SIP and CSTA (TR/87 over SIP) interfaces to communicate with SIP-enabled systems such as the Avaya Aura® Unified Communications platform. Integrating Contact Center with the Avaya Aura® Unified Communications platform using SIP infrastructure supports multi-nodal communication between customers and contact center agents. This integration gives Contact Center access to and control of the Avaya Aura® Unified Communications phones. The Avaya Aura® Unified Communications platform benefits from Contact Center skill-based routing, call treatments, reporting, and the graphical Orchestration Designer. Avaya Aura® Agent Desktop supports Avaya Aura® Unified Communications phones and continues to support voice, email, and Web chat contact types.

For more information about troubleshooting the Avaya Aura® Unified Communications platform to support Contact Center, see Avaya Aura platform troubleshooting on page 108.

Incomplete agents

When an incomplete agent record occurs in the Contact Center Manager Administration database, the agent appears grey. You must remove the agent. For more information, see Viewing incomplete agents on page 195.

Mission Critical High Availability

Avaya Aura® Contact Center supports campus High Availability for fault tolerant and mission critical contact centers. Contact Center supports the following levels of campus High Availability:

- Mission Critical High Availability for SIP-enabled contact centers.
- Hot-standby High Availability for AML-based contact centers. Application Module Link (AML) is an internal protocol used by Contact Center Manager Server to communicate directly with Avaya Communication Server 1000.
- Warm standby High Availability.

The level of Contact Center application High Availability you can achieve depends on your complete enterprise contact center solution. Avaya Aura® Contact Center also supports geographic redundancy and resiliency.

Contact Center supports High Availability (HA) resiliency for Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), Contact Center Multimedia (CCMM), Avaya Media Server, and Contact Center Manager Administration (CCMA).

For more information about troubleshooting Mission Critical High Availability, see High Availability troubleshooting on page 93.

Chapter 2: Introduction

The *Avaya Aura® Contact Center Troubleshooting* (44400-712) guide contains the fundamental concepts and procedures required to troubleshoot the server and client software.

The troubleshooting procedures in this guide are intended for users who are familiar with contact centers and who are trained to handle software errors. Users must be aware of the planning and engineering, installation, and configuration involved for the features licensed for their contact center. To handle software errors not covered in this guide, contact Avaya support.

All hardware diagnostics are the responsibility of the platform manufacturer. This guide does not document hardware troubleshooting procedures.

This guide does not document scripting troubleshooting procedures. For information on how to handle scripting errors, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (44400-510).

Prerequisites

Procedure

- Read *Avaya Aura® Contact Center Installation* (44400-311).
- Read *Avaya Aura® Contact Center Fundamentals and Planning* (44400-211).
- Read *Avaya Aura® Contact Center Routine Maintenance* (44400-514).
- Understand the features that you purchased for your contact center.
- Install, or migrate to, the Avaya Aura® Contact Center Release 6.4 software.
- Commission the Contact Center Release 6.4 software, see *Avaya Aura® Contact Center Commissioning* (44400-312).
- Download the latest version of this book from www.avaya.com/support.

Related resources

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

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 3: Troubleshooting fundamentals

This section contains the fundamental concepts required to troubleshoot the server software in Avaya Aura® Contact Center Release 6.4.

Handling errors

About this task

For all errors, record the following information:

- all error messages, ideally by taking a screenshot of the error message
- the system configuration
- actions taken before the error occurred
- actions taken after the error occurred

If the problem persists, contact your Avaya customer support representative.

Monitoring log files

About this task

You need to review log files to determine where errors occur and how to address them. You require this information if you need to contact Avaya to assist with troubleshooting.

Chapter 4: Troubleshooting planning

This section describes the information required for you to locate devices and applications that can require troubleshooting in Avaya Aura® Contact Center.

You can troubleshoot problems better by planning for events in advance and having up-to-date information available when network or device problems occur and troubleshooting is required.

Prerequisites for Troubleshooting planning

Procedure

- Know your network configuration.
- Understand the normal behavior of your network.

Site network map

Your site network map identifies where each device is physically located. This helps you locate the users and applications that are affected by a problem. You can use your map to systematically search each part of your network for problems.

Logical connections

If you use virtual LANs (VLANs), you need to know how your network devices are connected logically as well as physically.

Device configuration information

Maintain online and paper copies of device configuration information. Make sure that all online data is stored with your site's regular data backup. If your site does not have a backup system, copy the information onto a backup disc (CD, DVD) and store it offsite.

Other important network data

For a complete picture of your network, have the following information available:

- **Administration passwords for all systems**: Store all administration passwords in a safe place. Keep previous passwords in case you restore a device to a previous software version and need to use the old password that was valid for that version.
- **Device inventory**: The inventory shows you the device type, IP address, ports, MAC addresses, and attached devices at a glance.
- **MAC address-to-port number list**: If your LAN switches or PABXs are not managed devices, you must keep a list of the MAC addresses that correlate to the ports on your LAN switches and PABXs. Generate and keep a paper copy of this list, which is required for deciphering captured packets.
- **Change control**: Maintain a change control system for all critical systems. Permanently store change control records.
- **Contact details**: Store, online and on paper, the details of all support contracts, support numbers, engineer details, and telephone and fax numbers.

Determining baseline information for your network

You can use a baseline analysis, which is an important indicator of overall network health, to identify problems. A baseline can serve as a useful reference of network traffic during normal operation, which you can then compare to captured network traffic while you troubleshoot network problems. A baseline analysis speeds the process of isolating network problems.

By running tests on a healthy network, you compile normal data to compare against the results that you get when your network is in trouble. For example, use the network ping command between each node to discover how long it typically takes to receive a response from devices on the network.

Certain applications enable you to collect days and weeks of data and set a baseline for later comparison with a network having performance issues or outages.

Chapter 5: General troubleshooting

This section describes the general troubleshooting procedures that you perform when investigating basic problems in Avaya Aura® Contact Center.

Prerequisites for general troubleshooting

Procedure

- Ensure that the power is on for all servers and devices.
- Ensure that the PABX is operational and that all components are securely seated in the chassis.
- Ensure that all power leads and data cables are firmly connected at both ends.
- Ensure that all ports are properly configured.
- Ensure that all servers and their services are running.
- Ensure that all servers in the contact center solution can communicate by hostname and fully qualified domain name (FQDN). Verify this using a ping command.

Troubleshooting hardware problems

About this task

All hardware diagnostics are the responsibility of the platform manufacturer. No hardware procedures are documented in this guide.

Procedure

Check the manufacturer's instructions and recommendations. Contact the manufacturer if necessary.

Troubleshooting hardware errors

About this task

You can try to resolve some hardware errors by disconnecting the system, simplifying the setup, and restarting the system.

Procedure

1. Log users off the LAN and turn off the server.
2. Disconnect the power cord and unplug the telephone cables.
3. Simplify the server configuration to one monitor, one DVD and one hard disk drive, and one keyboard and mouse.
4. Remove all third-party options.
5. Reinstall options one at a time, checking the system after each installation.
6. Reconnect the power cord and telephone cables.
7. Restart the system. If the system does not function, see Troubleshooting when the system does not turn on on page 21.

Troubleshooting when the system does not turn on

About this task

You can check a number of things when the system does not turn on. There can be several reasons why the server is not functioning.

Procedure

1. Ensure that all cables and power cords are firmly plugged into their proper ports.
2. Ensure that all parts of the system are turned on and properly configured.
3. If the server is plugged into a switched multiple-outlet box, ensure that the switch on the outlet box is turned on.
4. Plug a different electrical device (such as a printer) into the power outlet, and turn it on to verify that there is power coming from the outlet.
5. Unplug the power cord, wait 20 seconds, plug it in again, and restart the system.
6. If the system still does not function, contact the server manufacturer.

Troubleshooting operating system start-up errors

About this task

Operating system start-up errors are often related to memory and hard disk drive capacity issues.

Procedure

Determine if the server has enough memory and hard disk drive capacity.

Troubleshooting low disk space on the operating system drive

About this task

If the Operating System drive (C:) on the Avaya Aura® Contact Center (AACC) server runs low on disk space, it can cause a range of problems. Some services can generate log files, for example, and this can fill up the disk space. On AACC servers, Internet Information Service (IIS) can generate a significant number of log files over an extended period.

Procedure

1. Check the `C:\inetpub\logs\LogFiles\W3SVC1` directory to see if the IIS log files are using excessive disk space.
2. If the IIS log files are using excessive disk space, download the solution document about the C drive running out of disk space from the Avaya support site, support.avaya.com. Follow the instructions in the solution document to configure the Operating System to purge the IIS log files.

Troubleshooting connection errors

About this task

Connection errors frequently involve loose or missing connections.

Procedure

Verify that all cables and boards are securely plugged into their appropriate connectors or slots.

Removing added options

About this task

You can have difficulty troubleshooting server issues if there are conflicts with added options.

Procedure

Remove all added options, and change only one component at a time.

Troubleshooting power cord errors

About this task

You can resolve many power errors by unplugging and plugging in the power cords.

Procedure

1. Unplug the power cords of the server.
2. Wait 20 seconds.
3. Plug the power cords in.
4. Restart the system.

Resolving a failed ping

About this task

If you test the contact center server subnet connection using the ping command, and the test fails, then follow these steps to verify that the server's contact center subnet NIC is configured and identified correctly.

Procedure

1. Plug a crossover network cable into the network card in the Client PC.
2. Plug the other end into the contact center subnet card in the server.
3. To restore the IP address information of the client PC after this procedure, record the TCP/IP address, subnet mask, and gateway of the client PC.
4. Configure the client PC with an IP address that is part of the same subnet as the IP address assigned to the ELAN subnet card. For example, if the server contact center subnet card has the IP address 1.1.1.1, then assign the client PC an IP address of 1.1.1.2.
5. Set the client PC to have a subnet mask of 255.0.0.0. Leave the gateway blank.

6. Open an command prompt window on the client PC and ping the server ELAN subnet card. For example, if the server ELAN subnet card has the IP address 1.1.1.1, then type `ping 1.1.1.1` and press `Enter`.

   If the ping test succeeds, then you know that you have correctly identified the contact center subnet card in the network control panel.

7. From the server, repeat the steps described in the procedure Retesting the ELAN subnet and contact center server subnet network connection on page 112. If the test fails, then verify that the network is set up correctly.

Refreshing your servers

Before you begin

- Ensure that you log on as webadmin, because only the default administrator can add, edit, delete, and refresh servers in Contact Center Manager Administration.
- You must log on using the Contact Center Manager Administration server name instead of the IP address, as the SOAP files are configured to use the server name. You can save the Contact Center Manager Administration server URL by adding it to your list of Internet Explorer favorites.
- Ensure that you have configured the Contact Center Manager Administration server name as Trusted Site with the relevant Active X Download values selected.

About this task

If a new license file was issued and accepted by Contact Center Manager Server, or if you connect to a different License Manager (that is, a new or standby License Manager server), you must refresh your servers.

If you changed the password of sysadmin in the Server Utility on CCMS, you must change the password on the CCMS server entry in CCMA.

When you refresh a server, you refresh Contact Center Manager Server data associated with that server in Active Directory Lightweight Directory Services (AD-LDS), such as release number, feature list, and networking information.

Procedure

1. Start Internet Explorer.
2. In the **Address** box, type the Contact Center Manager Administration server name. For example, http://< Contact Center Manager Administration Server name>.
3. Press `Enter`.

   The Contact Center Manager Server main window appears.

4. Enter your webadmin user ID and password.
5. Click **Login**.

   The Contact Center Manager Administration main window appears.

6. Select **Configuration**.
7. On the menu bar, click **Server** > **Refresh All Servers**.
8. Click **Yes**.

   The system refreshes all servers in the system tree. A message appears in the information bar at the bottom of the screen which lists the refreshed servers and the servers that did not refresh. An entry specifying the servers that you refresh also appears in the Audit Trail.

Using the Log Archiver utility

Before you begin

- Ensure that there is enough space at the archive location to store the archive files.
- If you are using a network archive location, ensure that there are automatic logon privileges for the selected location.

About this task

Use the Log Archiver (LA) utility to ensure that all active log files are archived on the Contact Center server. Use the LA utility to view both current and archived logs to diagnose problems on the server.

The log files for Contact Center Manager Server, Contact Center Manager Administration, Contact Center Multimedia and the Communication Control Toolkit are preconfigured in the LA utility. You can also add any other log files from the server to the LA utility.

Procedure

1. On the Contact Center Manager Server, select **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Components** > **CC Log Archiver**.
2. To add a log file to one of the tabs, in the Contact Center Log Archiver window, click **Add**.

   In this example, on the CCMS tab, the Add New Rule to CCMS dialog box opens.
3. Select the log file to add using the **Browse** buttons for the **Directory to watch** and **File or wildcard pattern** fields.
4. Select **A matching file is renamed** from the **Take action when a matching file is** list.
5. Select **Archive the file** from the **Action to take** list. These two settings apply to the majority of Contact Center log files.

   Important:

   If you select **A matching file is changed or created** from the **Take action when** list, you can generate an excessive amount of archive files.
6. Click **Add**.
7. Click the **Settings** tab.
8. In the **Archive Location** field, click **Browse** to select the location where archive files are stored.

9. In the **Archive Management** group, click the **Cleanup Settings** button.
10. To configure archive management, set disk space restriction and schedule file deletion. Avaya recommends you use the default settings, unless the archive files take up too much disk space.
11. Click **OK**.
12. Click **Mirror Settings**.
13. You can configure a DVD drive or an FTP server to mirror archive files.
14. To save changes on all tabs, click **Save All**.

Procedure job aid

Name	Description
Archive Location	The location where archived files are saved. Confirm there is enough space to store archived log files at this location. The Log Archiver service must have automatic logon privileges if you use a network Archive Location. The default Archive Location is `D:\Avaya\Logs\Archive`.
Refresh	Refresh the displayed information. The Current Location shows available disk space and space required by the Log Archiver based on Cleanup Settings. The Saved Location shows the total number and size of archives at the Archive Location. If you change the Archive Location, the Current Location can be different from the Saved location.
Cleanup Settings	Cleanup Settings provide three ways to purge archive files. Maximum Archive Size: Total disk space of archive files can not exceed the specified value. The default is 10GB. When the total disk space reaches the Maximum Archive Size, files are deleted as defined by the Reduce total size by value. The default is 2GB. Minimum Free Disk Space: Archive files never reduce the free disk space below the specified value. The default is 10% of the total disk space. When the limit is reached, files are deleted as defined by the Total free space desired value. The default is 15%.

Name	Description
	If both Maximum Archive Size and Minimum Free Disk Space are enabled, the setting that provides the most free disk space is used. The Log Archiver only increases disk space by deleting archive files. It cannot increase disk space for other applications. Periodical: Run a scheduled cleanup task. The default settings schedule the cleanup late in the evening, to avoid peak server activity; repeat every day; and delete archives older than two weeks.
Mirror Settings	You can configure Mirror Settings to archive to an FTP server and a DVD drive. Select Automatic FTP Mirroring or Automatic Disc Mirroring to archive files to the specified location. Use the Manual Copy tab to make copies of archive files.
View Archive Location	Open the Archive Location in Windows Explorer.
Delete	Delete all archives older than the specified date.
Archive All Files Now	Create an archive of all active log files. Select Include previous logs to include backup log files as well as the active files.
Set Events	Open the Events window to enter Windows Event Log Message IDs. When one of these events is triggered, the Log Archiver runs Archive All Files Now. For example, it creates an archive of all active log files.
Disable Archiving	Disable all automatic archiving operations.

Chapter 6: Installation troubleshooting

This section describes the procedures required to troubleshoot installation problems in Avaya Aura® Contact Center.

Prerequisites for installation troubleshooting

Procedure

Read *Avaya Aura® Contact Center Installation* (44400-311) guide.

Troubleshooting installation

About this task

The Avaya Aura® Contact Center installer initiates a series of individual application installations with each one creating its own log file. If an application installation fails, the Avaya Aura® Contact Center installer identifies which application has failed and notifies the user.

Procedure

1. Take a screenshot of the error for reference if you later need to contact technical support.
2. Identify the application that is experiencing the issue.
3. Examine the log files to determine you can easily correct the error.
4. If additional support is required.
   - Archive the error screenshots.
   - Archive all logs below the `C:\Avaya\Logs\Sysops` folder.
   - Send the archived screenshots and logs to the appropriate support personnel.

Log Files

Installation logs are located in `C:\Avaya\Logs\Sysops`. The following table shows the Avaya Aura® Contact Center installation sequence and the paths to related log files.

Procedure job aid

Table 1: Installation Log File Paths

Installation Sequence	Log File Location
AACC Installer	`C:\Avaya\Logs\Sysops`
Third party	`C:\Avaya\Logs\Sysops\MsiLogs`
CC applications	`C:\Avaya\Logs\Sysops\MsiLogs`
CC patches	`C:\Avaya\Logs\Sysops\MsiLogs\ProductUpdates`

Table 2: Installer Log Files

Log File	Details
`CC_Install_Data.xml`, `CC_Install_Log.xml`	• Location: `C:\Avaya\Logs\Sysops` • Created during contact center application installation • Contains customer configuration data entered during the interview phase • Contains machine specific info, for example the IP address and computer name
`Install_success_temp.html`, `Install_fail_temp.html`	• Location: `C:\Program Files\Avaya\Resources\HTML\` • Contains a high level summary of application installation status
`CC8_ProductInstaller.log`	• Location: `C:\Avaya\Logs\Sysops` • Contains detailed low level commands for the application designer

Table 3: Third Party Log Files

Application	Msi log file
AD-LDS	`CCMAADAM.log`
Policy Agent	`CCMAIISPolicyAgentComponents.log`
Tomcat	`ContactCenterTomcatInstall.log`
Cache	`Cache_x64.log`
Crystal Reports Server Embedded	`RAS.msi.log`
JRE	`jre1.6.0_xx.log`
Primary Interop Assemblies	No log generated

Application	Msi log file
ODBCDriver_2007.1_x86.exe	ODBCDriver_2007.1_x86.exe.log
Sybase Open Client	No log generated
Visual Studio 2008 runtime	No log generated
WebServicesFramework.msi	No log generated

Table 4: CC Patching Log Files

Log File	Details
CCPatches.log	• Location: C:\Avaya\Logs\Sysops\Product Updates • Contains history of patches installed or uninstalled on the system
PatchScript.log	• Location: C:\Avaya\Logs\Sysops\Product Updates\<ComponentName>\<PatchName> For example, C:\Avaya\Logs\Sysops\Product Updates\CCT\AvayaAura_CCT_6.0.201.0\PatchScript.log • Contains custom actions during patch installation or uninstallation, such as registry creation, service shutdown or startup, generated on patch install or uninstall
Nisoppep.log	• Location: C:\Avaya\Logs\Sysops\Product Updates\<ComponentName>\<PatchName> For example, C:\Avaya\Logs\Sysops\Product Updates\CCT\AvayaAura_CCT_6.0.201.0\nisoppep.log • Contains details of files updated during a patch installation or uninstallation
MSI_INSTALL.LOG	• Location: C:\Avaya\Logs\Sysops\Product Updates\<ComponentName>\<PatchName> For example, C:\Avaya\Logs\Sysops\Product Updates\CCT\AvayaAura_CCT_6.0.201.0\MSI_INSTALL.LOG • Contains details install actions performed by the patch MSI file
MSI_REMOVE.LOG	• Location: C:\Avaya\Logs\Sysops\Product Updates\<ComponentName>\<PatchName> For example, C:\Avaya\Logs\Sysops\Product Updates\CCT\AvayaAura_CCT_6.0.201.0\MSI_INSTALL.LOG • Contains details uninstall actions performed by the patch MSI file

Contact Center component install error messages

About this task

Troubleshoot error messages that appear during installation for particular Contact Center components (for example, CCMS, CCMA, CCT).

Procedure

1. Take a screenshot of the error message for future reference.
2. Click **OK**.

   An exit code (Install Failure) window appears with a path to the log file directory, `C:\Avaya\Logs\Sysops\MsiLogs`.
3. Click **OK**.

   The Main installation stops. A window appears with a summary of the installation. The failing component appears last in the summary with a red ‘X’ to indicate an error. Successful components appear with a green check mark.
4. Open the component log in `C:\Avaya\Logs\Sysops\MsiLog`. For example, if the CCT installation fails, open CommunicationControlToolkit.log.
5. Search the component log in `C:\Avaya\Logs\Sysops\MsiLog` for the text from the error message in step 1.
6. Review the log leading up to this message to find information on what caused the error.
7. For additional help, archive the error screenshots, archive all logs in `C:\Avaya\Logs\Sysops` folder and send the archived screenshots and logs to support personnel.

Installing a Contact Center patch

About this task

Troubleshoot if a Contact Center patch does not successfully install. A window titled Patch Install Failure appears during installation.

Procedure

1. Take a screenshot of the error message for future reference.
2. In the message, note the name of the patch that has failed to install.
3. To proceed with Contact Center installation and install the patch a later time, click **Yes**.

   If there are no other errors, the installation completes and a status window appears.
4. A red X appears beside the patch installation phase in the status window to indicate the failure.

Troubleshooting a Contact Center Manager Server Configuration Error

About this task

If an error occurs during the CCMS Server Configuration execution, the installer displays a error when the install completes. Follow this procedure to troubleshoot the error.

Procedure

1. Search `D:\Avaya\Logs\CCMS\CC_ServerConfig.log` for ERROR to identify cause of error.

   Possible causes of the error include the following:

   - If the log file contains errors referring to database connection problems, the cache database was not running during CCMS Configuration.
   - `C:\Avaya\Logs\Sysops\CC_Install_Data.xml` file is malformed, not present, or missing data.
2. Confirm Cache is running.
3. Run the CCMS Server Configuration utility, and verify or correct the configuration data.
4. Click **Apply All**.

Troubleshooting error messages during or after server installation

About this task

Error messages during or after server installation can occur if files are copied incorrectly. Error messages during installation can also occur if conflicts arise with other programs running on the server during installation.

Procedure

1. Close any other programs currently running on the server.
2. Uninstall the software.
3. Reinstall the software.

Troubleshooting configuration errors after server installation

About this task

Configuration errors can occur if values were not entered correctly in the Installation Data window.

Procedure

1. From the **Start** menu, choose **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
2. In the Server Configuration Utility window, enter the correct values for your server.

Troubleshooting server installation failure with Windows Server 2008 Release 2

About this task

Contact Center Multimedia installation can fail when the optional components of Windows Server 2008 Release 2 are installed.

Procedure

1. Uninstall Windows Server 2008 Release 2 64-bit Edition.
2. Reinstall Windows Server 2008 Release 2 64-bit Edition, without the optional components on DVD 2 of the Windows Server 2008 Release 2 64-bit Edition installation DVDs.
3. When you are prompted to install DVD 2, click **Cancel** and then click **OK**.

Contact Center and third-party software port conflicts

About this task

If you installed Communication Control Toolkit (CCT) or the WebLM license file on your Contact Center server, the default ports of these applications can have conflicts with third-party software. Both CCT and WebLM use Apache Tomcat. The default port for the Contact Center Tomcat Instance is 8081. For information about changing the default port, see the Apache Tomcat documentation.

Chapter 7: Migration troubleshooting

This section describes the procedures required to troubleshoot migration problems in Avaya Aura® Contact Center Release 6.4.

Avaya Aura® Contact Center supports only the Windows Server 2008 Release 2 operating system platform, so Contact Center does not support software upgrades using the operating system from previous contact center releases.

A migration procedure migrates the statistical and configuration data from one server to another. You can migrate your existing customer data to Contact Center Release 6.4 on a new Windows server. You can migrate all your configuration and statistical data to the new server so no data is lost in the move.

Prerequisites for Migration troubleshooting

Procedure

- Always back up the server database prior to any maintenance activity.
- Read *Avaya Aura® Contact Center Upgrade and Patches* (44400-410).

Task Flow Executor does not start after a migration

About this task

If the Task Flow Executor (TFE) does not appear in the UP state after a migration, then you must validate all scripts to correct the problem. For more information about validating scripts, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (44400-510).

Procedure

Validate all scripts.

Troubleshooting when migrating a CCMM database with a changed CCMA server name

Before you begin

- Ensure that you are using x64 version of Windows Server 2008 Release 2.

About this task

Troubleshoot when you migrate a Contact Center Multimedia (CCMM) database with an out of date Contact Center Manager Administration (CCMA) server name, so you cannot open CCMM Web Administration.

Important:

If the CCMA server name in the CCMM database is different from the CCMA you are using to open the CCMM Admin, you are not be able to open the CCMM administration tool.

Procedure

1. Log on to the server onto which you migrated the CCMM database.
2. Click **Start** > **Avaya** > **Contact Center** > **Multimedia Server** > **Multimedia Dashboard** to open the CCMM Dashboard utility.
3. On the CCMM Dashboard, right-click **CCMA Server** in the lower left and click **Edit**.
4. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
5. In the **Password** box, type the password. The default password is `__ccmm!`.
6. Click **Login**.
7. Enter the new CCMA server name or the new CCMA IP address.
8. Click **OK**.
9. From your web browser, log on to CCMA Web Administration and access CCMM Administration.

Chapter 8: Contact Center Manager Server troubleshooting

This section describes the troubleshooting procedures that you perform when dealing with Contact Center Manager Server problems in Avaya Aura® Contact Center.

Prerequisites for server administration troubleshooting

Procedure

Ensure that you know the License file location and Contact Center License Manager IP address.

Resetting the Contact Center License Manager Grace Period

Before you begin

- Ensure that you locate the license file in the `D:\Avaya\Contact Center\License Manager\bin` folder on the server. The license file is called plservrc.
- Ensure that the IP addresses used for the Primary and Secondary Contact Center License Manager are on the same contact center server subnet and the contact center server subnet is at the top of the binding order on the CCMS and LM servers.

About this task

When a communication error occurs between Contact Center Manager Server (CCMS) and Contact Center License Manager (LM), CCMS continues normal operation for the duration of the Grace Period.

The grace period is 30 days. If a communication problem occurs between CCMS and LM, 30 days are available for the CCMS to continue normal operation. After you resolve the communication problem, the grace period automatically reverts to 30 days. For example, if the communication problem is resolved in two days, the grace period returns to 30 days after two days of successful connection to LM.

When the server enters the Grace Period, CCMS continues to generate an event until either the Grace Period expires or the communication problem between the server and LM is resolved.

If, at any stage, the grace period expires, CCMS shuts down and locks. You cannot restart CCMS without resetting the grace period.

You can reset the Grace Period to 30 days at any time. When a communication error occurs, CCMS sends an event to the Server Utility detailing that there was an error, the time already elapsed in the Grace Period, and a lock code that you can return to Avaya to get the Grace Period reset.

For CCMS, you must apply separate unlocking codes for both the CCMS Control Service and the ASM Service.

Within the grace period, you have the same capabilities as if you were the only client of LM. You can request the maximum licenses that are available from LM. When communication is re-established, the licenses are acquired automatically from LM (if they are available).

When a licensing error is detected, you must check that the Contact Center License Manager service is running, and verify the status of the LM server and network communications. During the grace period, alarms are sent every 6 hours notifying the time elapsed in the grace period.

If you reestablish communications during the grace period, CCMS sends a notification to the Windows Event Log on the server and the Alarm Monitor. While communication is reestablished, alarms are sent every 6 hours notifying the time elapsed in the grace period.

During the grace period, you can shut down, start up, or restart CCMS without otherwise affecting its operation.

If you cannot fix the connection between LM and CCMS within the 30 day grace period, contact your Avaya Customer Service Representative to determine if you need an emergency license file on your system.

The emergency license file expires after 30 days and ensures operation of the Contact Center Manager Server only on a temporary basis. You must install the emergency license file through the LM Configuration tool. If you are using corporate licensing, it is possible that you need to change the CCMS Configuration in cases where LM is on a different server than it was previously.

Procedure

1. From the Event Viewer, make a copy of the lock code and send this code to Avaya Support.

   Avaya Support provides you with an unlock code that you must apply to the Contact Center Manager Server.

2. Open the Contact Center License Grace Period Reset application.
3. Enter the unlock code you received from Avaya Support.
4. Click **Apply**.
5. Click **Exit**.
6. Repeat Step 1 on page 37 through Step 5 on page 37 for both Contact Center Manager Server Control Service and ASM Service.

Troubleshooting when the Contact Center Manager Server hosts file contains multiple instances of each site

About this task

If you delete any site entry from the hosts file, then you must restart the Contact Center Manager Server configuration manager service to ensure that it updates the database with the changes.

Procedure

1. On the Contact Center Manager Server, go to `C:\WINDOWS\system32\drivers\etc` and open the hosts text file.
2. Delete the multiple entries of the site, and then click **File** > **Save**.
3. Select **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
4. Save and apply all changes.
5. Restart the server.
6. Open the hosts text file and confirm that the file is accurate and there are no multiple instances of any site.

Troubleshooting error messages during an IP address change in Server Configuration

Before you begin

- Ensure all contact center services are shut down. In the System Control and Monitor Utility (SCMU), stop CCMS services before all other contact center services are stopped.

About this task

Troubleshoot when you receive a Server Configuration message during an IP address change. The message informs you that CCMS services must be stopped prior to changing IP addresses. If you receive this Server Configuration message during an IP address change, some contact center services are still running.

Procedure

1. Open Windows Task Manager.
2. Click the **Processes** tab.
3. Under **Image Name**, if NBNmSRVC.exe is present, select **NBNmSRVC.exe** and click **End Process**.

   All contact center services are now stopped and you can change an IP address in Server Configuration.

Chapter 9: Avaya Media Server troubleshooting

This section describes the troubleshooting procedures that you perform when dealing with Avaya Media Server (Avaya MS) problems in Avaya Aura® Contact Center.

Prerequisites for Avaya Media Server troubleshooting

Procedure

- Read *Avaya Aura® Contact Center Installation* (44400-311).
- Read *Avaya Aura® Contact Center Commissioning* (44400-312).
- Read *Avaya Aura® Contact Center Server Administration* (44400-610).

Troubleshooting Avaya Media Server performance issues

Before you begin

- Complete Avaya Media Server commissioning and acceptance testing. Use Avaya Media Server to process routed Customer contacts in your SIP-enabled contact center.
- If you are using the Agent Greeting feature, complete Agent Greeting acceptance testing before performing this task.

About this task

Installing Contact Center Services For Avaya Media Server (CCSA) automatically enables Avaya Media Server debug tracing. Avaya Media Server is a software-based media processing platform. All media processing is performed in software on the host CPUs. Avaya Media Server therefore does not support debug tracing in production systems. If you are experiencing performance issues with Avaya Media Server, ensure debug tracing (Debug Logging) is disabled. You must disable Avaya Media Server trace debugging in production systems.

Procedure

1. Log on to Avaya Media Server Element Manager.
2. Navigate to **System Configuration** > **Debug Tracing** > **General Settings**.

3. From the **Debug Logging** drop-down list, select **Disabled**.
4. Repeat this procedure on each Avaya Media Server in your commissioned solution.

Troubleshooting when dialing into recorder fails

About this task

Troubleshoot when dialing into a recorder fails by reviewing the possible reasons for the error.

Procedure

1. Verify that Agent Greeting is correctly licensed and enabled on Avaya Aura® Contact Center.
2. Verify that Agent Greeting is correctly licensed on Avaya Media Server.
3. Verify that dial-in number is configured correctly on the switch to route calls to Avaya Media Server primary server.
4. Verify that SIP Proxy (SIP Enablement Services or Session Manager, depending on Communication Manager version) is configured as a SIP Trusted Node on Avaya Media Server.
5. Verify that dial-in number is set correctly in the **Contact Center Manager Administration Configuration** > **Agent Greeting** settings page.
6. Verify that Contact Center Manager Administration and Contact Center Manager Server connection details are configured correctly in Avaya Media Server Element Manager.
7. Wait at least 10 minutes after completing any settings changes to confirm if the problem is resolved (the Agent Greeting application refreshes settings from Avaya Media Server and Contact Center Manager Administration at 10 minute intervals).

Troubleshooting NIC interface problems on the Linux server

About this task

Troubleshoot when the NIC interface on the Avaya Media Server Linux server becomes unresponsive. This problem can occur while using Broadcom bnx2 NIC card driver version 1.9.3. The following procedure provides examples of commands for troubleshooting an RHEL 5.x system.

Procedure

1. On the Linux server, use the **`ethtool`** command to check the NIC parameters. For example:

   ```
   ethtool –i eth0
   ```

2. If the system displays the following information, you must update the NIC driver.

```
driver: bnx2
version: 1.9.3
firmware-version: 5.2.3 NCSI 2.0.11
```

3. Update the NIC driver by installing the latest RHEL updates.
4. Use the **ethtool** command to verify that you have the latest NIC driver. For example:

```
ethtool –i eth0
```

Troubleshooting contact centers with limited network bandwidth

Before you begin

- Ensure G.729 is enabled as an audio codec in Avaya Media Server Element Manager. For more information, see *Avaya Aura® Contact Center Commissioning* (44400-312).

About this task

In solutions where network bandwidth is limited, use G.729 as the voice codec on either the customer leg or the agent leg of the call.

Important:

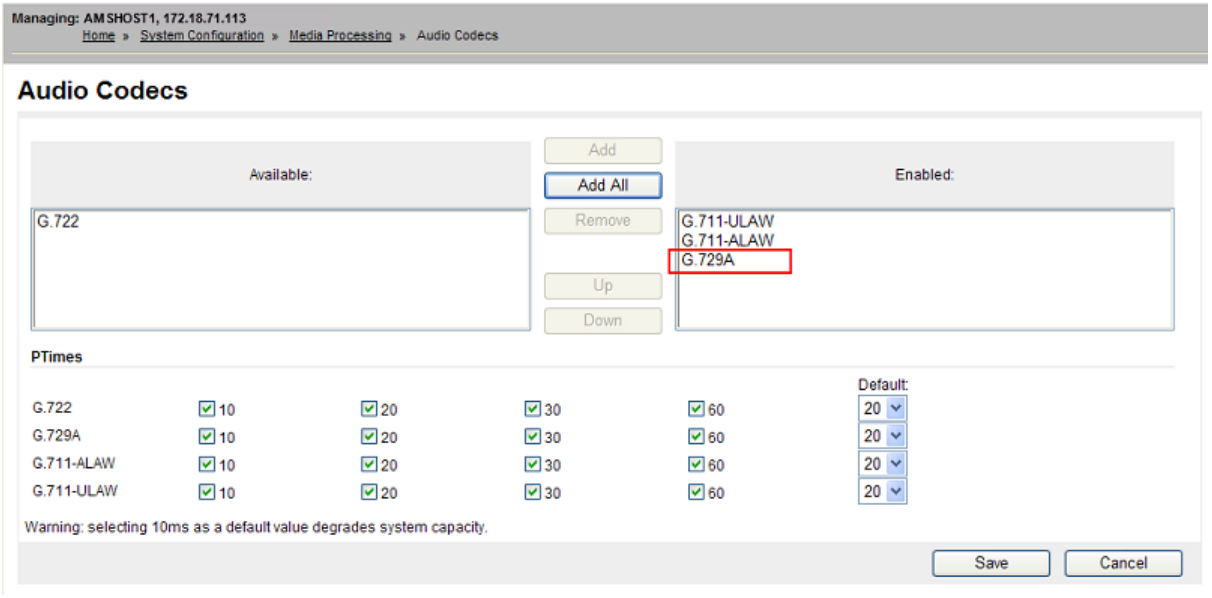
- Using G.729 as the voice codec on both legs of Contact Center calls is not supported. This can result in voice quality issues.
- Voice codecs must use a packet size (ptime) of 20 milliseconds (ms). Packet sizes larger than 20ms are not supported.

Follow the procedure below if you want to use G.729 as the voice codec on either the customer leg or the agent leg of Contact Center calls. This requires configuration on both Avaya Media Server and Communication Manager. Use Communication Manager network regions to achieve a particular codec on either the customer leg or the agent leg of the call.

Procedure

1. To enable the G.729 codec on Avaya Media Server, log on to Avaya Media Server Element Manager.
2. In the navigation pane, click **System Configuration** > **Menu Processing** > **Audio Codecs**.

   To use G.729 as the voice codec on the agent leg of the call, ensure G.729 appears in the **Enabled** list.



3. Access the System Access Terminal (SAT) on your Communication Manager.
4. Use the **`change ip-codec-set`** command to change the audio codec preference.

   To use G.729 as the voice codec on the customer leg of the call, ensure G.729 appears in the list.

```
change ip-codec-set 1                                    Page   1 of   2

                              IP Codec Set

    Codec Set: 1

    Audio          Silence        Frames    Packet
    Codec          Suppression    Per Pkt   Size(ms)
1:  G.729              n             2         20
2:  G.711MU            n             2         20
3:  G.711A             n             2         20
4:
5:
6:
7:
```

Troubleshooting when volume of announcements is low

Before you begin

- Check each prompt for consistent volume and quality through playback of the prompt.

About this task

If the phones in your contact center play announcements at a low volume, use the following procedure to increase the volume.

Procedure

1. Log on to Avaya Media Server Element Manager.
2. Navigate to **System Configuration** > **Media Processing** > **Advanced Settings**.
3. In the **Announcement Volume Adjustment (db)** field, enter the announcement prompt volume level adjustment in decibels (db).

   Note:

   The default value is -10 db. The range is from -24 to 24 db.
4. Restart the server for the changes to take effect.

   Adjust the volume in small increments. For example, increase the volume from the default value of -10 db to -5db, until you are satisfied with the volume level. You can keep checking the volume by calling in to the contact center.

Chapter 10: Database Integration Service troubleshooting

This section describes the troubleshooting procedures that you perform when handling Database Integration Service problems in Avaya Aura® Contact Center.

Handling Database Integration Wizard errors

About this task

There is a list of errors that you can receive when you are running the Database Integration Wizard (DIW). The Job Aid below lists each of the error messages and gives a brief explanation of how to handle each error.

Procedure

Review the Database Integration Wizard error messages on page 44 table and determine how to proceed.

Procedure job aid

Table 5: Database Integration Wizard error messages

Error message	Description
Already Connected (when setting and testing the HDX connection)	Contact Center Manager Database Integration is already connected to HDX.
Already Connected (when configuring the database)	The selected DSN is already connected.
Authorization Failed	The user details supplied are incorrect. This indicates that the version of Contact Center Manager Database Integration is different to the version of HDX. Contact Avaya Support.
Error	The connection cannot be performed.

Error message	Description
	Contact Avaya support.
Incompatible Version	The version information supplied is incorrect. This indicates that the version of Contact Center Manager Database Integration is different to the version of HDX. Contact Avaya support.
Invalid Object	HDX Server object cannot be found. This indicates that the HDX Server service is not running.
Invalid Provider ID	The provider ID entered is invalid. Ensure that the provider ID is within the valid range of 0 to 1999999999.
The Host could not be found.	A server with the host name or IP address given cannot be found on the network. Enter a new host name or IP address.
Too Many Connections	All HDX connections are being used. Deregister another HDX provider to free a connection.

Ensuring you have the correct access permissions to the database

About this task

The connection to the database requires access permissions. For example, if the database security is configured to use its own integral user accounts, then a user can be specified in the Database Integration Wizard and the ODBC Data Source Name (DSN). However, if the database security is configured for Domain or Workgroup authentication, then the Contact Center Manager Server Host Application Integration service and the Database Integration Wizard need to use the correct context when connecting.

The Database Integration service runs by default in the local system context and therefore does not have access permissions to the database on another server in the customer network using Domain or Workgroup authentication.

Procedure

To enable access to the database, follow one of the recommendations below:

- Use Local or Domain Policy to assign permissions to the Local System context of the Contact Center Manager Host Application Integration service.
- Configure the Contact Center Manager Host Application Integration service to start with the <Domain>/<User> context with the appropriate permissions.
- Configure the database permissions for the Contact Center Manager Server computer access context.

- Contact your Customer Network Administrator or your Database Administrator for further information about configuring the correct access permissions for connection to the database.

Ensuring access to the database over a network

About this task

The Database Integration service runs as a Windows service using the predefined Local System account on the server. A service that runs in the context of the Local System account inherits the security context of the Windows Service Control Manager. This account has extensive privileges on the local computer and acts as the computer on the network. This account has limited access to network resources (such as shares) because it has no credentials and must connect to the network using a null security session. For example, it is unlikely that the account has sufficient security credentials to access a Microsoft Access database, owned by an authenticated user, on a network share created in the context of the user.

Procedure

Contact your Network Administrator.

For information on making a remote share available using a null session share, see the Microsoft Web site.

Chapter 11: Network Control Center troubleshooting

This section describes the troubleshooting procedures that you perform when handling Network Control Center (NCC) issues in Avaya Aura® Contact Center.

Prerequisites for Network Control Center troubleshooting

Procedure

Ensure that you are aware of your NCC configuration.

Troubleshooting call routing problems

About this task

Troubleshoot call routing problems if your server cannot route calls to or receive calls from other sites. You need to review several issues to determine why the server cannot route calls.

If you experience issues with networking calls, Avaya also provides a network trace utility (NtwkTraceMon) that customer support staff can use to help you troubleshoot your problem.

Procedure

1. Verify that the source server did not filter the server.
2. Verify that the dialable DN is configured correctly at the source server.
3. Ensure that network skillsets and routing tables are received at the server. If not, see Verifying the connection to the NCC on page 47.

Verifying the connection to the NCC

About this task

Verify the connection to the NCC if calls are not being routed properly.

Procedure

1. At the NCC, start the Nbconfig utility. Run **nbconfig -admin**.
2. Check the Address and Site tables to ensure that they are configured correctly:
   - The IP addresses are unique and correct.
   - The site names are correct.
   - The site names in the Site table match the site names in the Sites window on the NCC.
3. Add any missing sites and, if any information is incorrect, remove the affected site and add it again.
4. At the server, start the Nbconfig utility, and verify that the Address table and the Site table match those on the NCC.
5. At the server, use the Nbconfig utility to ensure that the NCC site is defined correctly. If any of this information is incorrect, see Resetting all site and address settings on page 48.
6. At the server, open a DOS window and type the following command: `ping nnn.nnn.nnn.nnn`

   where nnn.nnn.nnn.nnn is the Contact Center Subnet IP address of the NCC. If the NCC cannot be found, then use the **tracert** command to find out where the error is occurring.
7. Restart the NCC.
8. If the problem continues, contact your Avaya customer support representative.

Resetting all site and address settings

Before you begin

Important:

To complete this procedure, you need to shut down all Contact Center Manager Server services.

About this task

Reset all site and address settings if the contents of the Address table and Site table are incorrect or if the two servers do not communicate even though they can ping each other.

If this procedure does not resolve the problem, run nicomsetup at the NCC and define all sites again using nbconfig -admin.

Procedure

1. Log on to the server with CCMS installed.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Shutdown**.
3. Open a command window and at the DOS prompt, type **cd D:\Avaya\Contact Center\Manager Server\iccm\bin**.

4. Enter **nicomsetup** to reset all communication settings.
5. Restart Contact Center Manager Server.
6. On the NCC, run **`nbconfig -admin`**.
7. Select the **Force Synchronization** check box on the Site Table tab, and then click **OK**.

Troubleshooting when network skillsets are not distributed from the NCC to all sites

Before you begin

- Determine the reason why network skillsets are not being distributed from the NCC to all sites.

About this task

This problem can occur for the following reasons:

- **An existing entity has the same name**: If a server has a variable named Sales, then you cannot add a network skillset named Sales. Avaya recommends that skillset names include the characters _sk to identify them as skillsets and to avoid potential conflicts with other entities.
- **The configured limit for number of skillsets was reached**: For more information about historical statistics configuration, see the *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611) guide.
- **One or more sites is running Avaya Aura® Contact Center Web Client Release 4.2 or earlier**: Network skillsets configured for longest idle agent or average speed of answer are not propagated to servers running Avaya Aura® Contact Center Web Client 4.2 or earlier.

Procedure

1. If an existing entity has the same name as a network skillset, contact your network administrator to resolve naming problems.
2. If you have reached the configured limit for number of skillsets, use either client application to check the historical statistics configuration parameters. and change the configured limit of skillsets. If you change the configured limit of skillsets, you must force synchronization of the site information from the NCC.
3. If one or more sites is running Avaya Aura® Contact Center Web Client 4.2 or earlier, install a supported Web client at any site that requires upgrading.

Troubleshooting when calls for a network skillset are not sent to other sites

Before you begin

- Determine the reason why calls for a network skillset are not being sent to other sites.

About this task

This problem can occur if your scripts are not updated to route calls to the network skillset. When an administrator at the NCC defines a network skillset at the NCC, the NCC propagates the new skillset to all servers in the network. However, scripts are not automatically updated to route calls to the network. Calls continue to be queued to the local copy of the network skillset.

To route calls to other sites, you must add the script command Queue To Network Skillset. For more information about using network skillsets in scripts, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (44400-510).

This error can also occur under the following circumstances:

- The NACD package is not enabled on the CS 1000 PABX at the source site.
- A non-ISDN trunk is encountered.
- The dialable DN (set in the Network Communication Parameters window) for the destination is not set to the correct MCDN network CDN.
- A call is abandoned.

Procedure

If the NACD package is not enabled on the CS 1000 PABX at the source site, install and configure NACD.

Troubleshooting when filtering is preventing calls from being sent to a destination site

Before you begin

- Determine the reason why filtering is preventing calls from being sent to a destination site.

About this task

This problem can occur for the following reasons:

- The NACD package is not enabled on the CS 1000 PABX at the source or at the destination site.
- The dialable DN for the destination site is configured incorrectly.
- The MCDN network CDN is not configured correctly at the destination site. The MCDN network CDN must be configured on the telephony PABX as a CDN (see *Avaya Aura® Contact Center Configuration – Avaya CS1000 Integration* (44400-512)), and it must be configured and acquired as an MCDN network CDN on the server.

- The server at the destination site is not active.
- The network skillset at the destination site is in Night Service mode or Transition Service mode. The site is filtered until an agent with the skillset logs on and the queue at the destination site is active.
- The number of failed attempts set in the Number of Retries box for a skillset is reached. When this happens, the source site removes the destination site from all routing tables for the time configured in the Filter Timer period (minimum of 5 minutes, maximum of 12 hours). After the Filter Timer period, the destination site is no longer filtered.

Procedure

1. If the NACD package is not enabled on the telephony PABX at the source or at the destination site, install and configure NACD.
2. If the dialable DN for the destination site is configured incorrectly, reconfigure the network communication parameters.
3. If the MCDN network CDN is not configured correctly at the destination site, reconfigure the MCDN network CDN as a CDN.
4. If the server at the destination site is not active, ask the contact person at the remote site whether the server is up.
5. If the network skillset at the destination site is in Night Service mode or Transition Service mode, wait until an agent with the skillset logs on and the queue at the destination site is active.
6. If the number of failed attempts set in the Number of Retries box for a skillset is reached and the source site removes the destination site from all routing tables for the time configured in the Filter Timer period, wait until the Filter Time period is reached or, if the problem is resolved before the Filter Timer period is reached, manually stop filtering the site.

Troubleshooting problems collecting network call-by-call statistics

Before you begin

- Determine the reason why your system is having problems collecting network call-by-call statistics.

About this task

This problem can occur for the following reasons:

- **The server or NCC does not have enough disk space**: The historical statistics configuration calculation determines if you have adequate storage space to save the amount of call-by-call data you choose. When historical data is stored and consolidated, each server (including the NCC) checks every 15 minutes to ensure that you have adequate storage space. This is applicable at each server, including the NCC. Call-by-call data is purged when data reaches the age you configure (in the Historical Statistics Configuration window) or when disk space becomes insufficient. This enables more recent call-by-call data to be stored; but if you have

less disk space than calculated, it can result in less long-term data stored. An event is logged in Fault Management if this occurs. An event is also logged in Fault Management if network call-by-call data transfer to the NCC takes longer than 15 minutes.

Important:

If the NCC goes down for an extended period, pegging occurs at each local server that is storing network call-by-call data. This can use a substantial amount of resources at each local server.

- **The call-by-call information is not sent to the NCC**: If you recently changed your call-by-call storage options, the change does not take effect until the information is sent to the NCC and propagated to all sites. This can take several minutes after making a change.

Procedure

1. If the server or NCC does not have enough disk space, reconfigure storage information in the Historical Statistics Configuration window.
2. If the call-by-call information is not being sent to the NCC because you recently changed your call-by-call storage options, wait a few minutes for the change to take effect.

Troubleshooting incorrect times on reports

Before you begin

- Check the time set at each telephony PABX regularly to ensure that the times are synchronized.
- Verify that each site on the Sites page of the Configuration component in Contact Center Manager Administration has the relative time to GMT configured correctly.
- If you change the time zone through the Date/Time control panel, restart each server in Contact Center Manager.

About this task

Troubleshoot incorrect times on reports when errors occur because the times set at multiple servers are not synchronized.

Whether sites are in the same time zone or in multiple time zones, if the times at various telephony PABXs are not synchronized, the network call-by-call report does not display accurate information. In some cases, for example, destination events can appear to occur before source events. You must regularly check the time set at each telephony PABX and change the date and time when necessary, to ensure exact synchronization.

Procedure

1. Log on to the PABX console.
2. Enter **Id 2**.
3. Type `ttad` to display the date and time.
4. To change the date or time, type `stad`, and then enter the correct date and time in the following format: DD-MM-YYYY 00:00. Use the 24-hour clock format for the time.

5. Press `Enter`.
6. Log off the PABX console.

Troubleshooting call routing problems when agent reservations are canceled before network calls are presented

About this task

The number of times an agent is reserved must be approximately equal to the number of NACD and network calls answered by the agent. If it is not, then it is possible that your Agent Reserve Timer value is too low.

Normally, when an agent is reserved for a call, but the call is answered locally or routed to another server, the local server notifies the remote server, and the remote server cancels the agent reservation. However, if a communication problem prevents notification of the remote server, the agent remains in the reserved state indefinitely. To prevent this from happening, the remote server cancels the reservation after a period of time configured on the Agent Reserve Timer.

If the Agent Reserve Timer is too low, the agent can be unreserved before the call is presented to the agent, but after the call arrives at the remote server. When that happens, the agent's ReservedForCall statistic is incremented, but the agent's NetworkCallsAnswered statistic is not.

Procedure

If agent reservations are being cancelled before network calls are presented, increase the value of the Agent Reserve Timer and.

Troubleshooting call routing problems with Landing Pads in Universal Networking

Before you begin

- Determine the type of call routing problem that is occurring with Landing Pads in Universal Networking.

About this task

Every site that is licensed for Universal Networking can configure CDN or DNIS Landing Pads. When a request is received at a target network node, a Landing Pad is taken from the idle list and reserved for that call until the source site routes the call to it. Landing Pads are required for the duration of a network call. When the call arrives at the target Landing Pad, the Landing Pad is returned to the idle list to wait for the next call. A relatively small number of Landing Pads is sufficient to receive several incoming Universal Networking calls at a target node.

There are several possible call routing problems that can occur with Landing Pads in Universal Networking:

- **All Landing Pads are busy**: If the incoming network call rate exceeds the available Landing Pads, then Event 49033 is logged to the Event Browser at the source site stating All Landing Pads Busy at <TargetSiteName>. The Network Communication Parameters page in Contact Center Manager Administration for the source site displays a similar message for the configurable time that the target is filtered. This message is an indication that not enough Landing Pads are configured for the target site in question. This applies to both CDN and DNIS Landing Pads. CDN Landing Pads must be acquired before Contact Center Manager Server can use them.
- **No DNIS Network CDN is available**: To route a Universal Networking call with a DNIS Landing Pad to a target network node, the DNIS Network CDN at the target network node must be configured and acquired. If the DNIS Network CDN at the target network node is not configured and acquired, then Event 49034 is logged to the Event Browser at the source stating No DNIS Network CDN available at <TargetSiteName>. The Network Communication Parameters page in Contact Center Manager Administration for the source site displays a similar message for the configurable time that the target is filtered.
- **General problems with Universal Networking**: If no Universal Networking calls are routed or if other problems with Universal Networking calls occur, it can be related to the state of the dependent NT Services.
- **Acquisition status errors are occurring for Landing Pad CDNs and the DNIS Network CDN**: The Contact Center Manager Administration CDNs (Route Points) page has an acquired Status column for Landing Pad CDNs and the DNIS Network CDN. This column displays the status of the CDN on the telephony PABX. Possible values are Acquired, Acquire Pending, Not Acquired, or Acquired Failed. If the telephony PABX properly acquires the CDN in question, but one of the Contact Center Manager Server components is not aware of the acquisition, then an acquisition status error can occur. A Landing Pad CDN or the DNIS Network CDN status is Acquired, but there is a problem with the operation of the CDN (for example, after system restarts). In this case, an event appears in the Event Browser indicating UNE_Service is not aware of the acquisition status of CDN <CDN_Number>.

Procedure

1. If the error message `All Landing Pads Busy at` <TargetSiteName> appears, check that all CDN Landing Pads are acquired.
2. If the Event Browser displays **Event 49034** stating `No DNIS Network CDN available` at <TargetSiteName>, configure and acquire the DNIS Network CDN at the target network node.
3. If general problems are occurring with Universal Networking, open the NT Services manager and verify that the following services are up:
   - CCMS ASM_Service
   - CCMS TFE_Service
   - CCMS NBMSM_Service
   - CCMS OAMCMF_Service
   - CCMS UNE_Service

If you cannot start these services manually from the NT Services manager, you might need to reboot the system to solve the problem.

4. If acquisition status errors are occurring for Landing Pad CDNs and the DNIS Network CDN, deacquire and reacquire the CDN <CDN_Number> noted in the error message.

Troubleshooting when network calls unexpectedly take priority over local calls

About this task

If your Contact Center system uses the Network Skill-Based Routing (NSBR) option, you can transfer voice contacts between Contact Centers. A network skillset is common to all Contact Center Manager Servers in a network. A Network Control Center (NCC) administrator creates a network skillset, and NCC automatically propagates the network skillset to all sites. When a script queues a contact to a network skillset, the contact can be routed to a server on the network.

You can assign priority levels to contacts. The default priority value for contacts on the NCC server is different from the default priority value on other servers in the network. If you do not assign priorities to contacts, routing issues can occur. If both local and network calls are routed using the default priority values, the network call always takes priority over the local call.

Procedure

Ensure that the **`WITH PRIORITY`** command is used to route both local and network calls.

For more information, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (44400-510).

Chapter 12: Licensing Troubleshooting

This section describes the troubleshooting procedures that you perform when handling licensing problems in Avaya Aura® Contact Center.

Checking the contents of the Contact Center License Manager registry

Before you begin

- Ensure that you are trained and qualified to edit the Contact Center License Manager registry.
- Back up the Contact Center License Manager registry before making any changes.

About this task

Check that the contents of the Contact Center License Manager registry on the Multimedia Contact Server identify the Contact Center License Manager server. See HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\Nortel\LM\LSHost.

If the contents of the LSHost registry key are invalid, change the Contact Center License Manager key in the Multimedia Administrator. See Changing the name of the Contact Center License Manager server in Contact Center Multimedia on page 63.

Procedure

1. On the server, choose **Start** > **Run**.
2. In the **Run** box, type `Regedit`.
3. In the Registry Editor application, expand **My Computer**.
4. Expand **HKEY_LOCAL_MACHINE**.
5. Expand **Software**, **Wow6432Node**, **Nortel**, **LM** and **LSHost**.

   The <IP Address of Contact Center License Manager Real application> or < Contact Center License Manager server name> is displayed in the LSHost data.

   The <IPAddress>:<port number> or <servername>:<port number> is displayed in the LSHost data.
6. Note the IP address for the Contact Center License Manager.

Configuring the Contact Center License Manager alarm interval

About this task

Add licenses by contacting your distributor to upgrade your license and then change and install your Contact Center License Manager file.

Procedure

1. Log on to the server where the Contact Center License Manager software is installed.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **License Manager** > **Real Time Usage**.
3. On the Real Time Usage page, in the **Critical License Usage %** box, type the percentage usage above which a critical alarm is generated. The default value is 90%. The critical alarm event ID is 61160.
4. In the **Major License Usage %** box, type the percentage usage above which a major alarm type is generated. The default value is 80%. The major alarm event ID is 61161.
5. In the **Send Alarm Interval (sec)** box, type the interval at which the alarm is generated. The minimum and default value is 10 seconds. The maximum is 999 seconds. An alarm is generated (at this interval) only when Contact Center license usage is above the major license usage level.
6. Click **Apply** to restart the Contact Center License Manager server.
7. Click **Yes**.
8. Click **OK** to close the window.
9. Click **Exit**.

Checking the link to the Contact Center License Manager server

Before you begin

- Ensure that you are trained and qualified to edit the Contact Center License Manager registry.
- Back up the Contact Center License Manager registry before making any changes.

About this task

Ping the Contact Center License Manager server identified in the registry key to ensure that no network problems exist. If you cannot ping the Contact Center License Manager server, change the Contact Center License Manager key using the Multimedia Administrator, see Changing the name of the Contact Center License Manager server in Contact Center Multimedia on page 63, or debug

the network to see why Contact Center Multimedia cannot contact the Contact Center License Manager server.

Procedure

1. On the server, choose **Start** > **Run**.
2. In the **Run** box type `cmd`.
3. In the command prompt window, type `ping lmservername`, where lmservername is the IP address of the Contact Center License Manager server that you determined in step 6 of Checking the contents of the Contact Center License Manager registry on page 56.

Reviewing the Contact Center License Manager file

About this task

Review the Contact Center License Manager file to determine whether the necessary licenses for your Contact Center Multimedia operation are present. If required, add the necessary licenses to the Contact Center License Manager file on the Contact Center License Manager server.

If the license file does not contain the lines LM_MMP or LM_MMS, then Contact Center Multimedia does not work.

Procedure

1. On the **Start** menu of your Contact Center Manager Server, choose **All Programs** > **Avaya** > **Contact Center** > **License Manager** > **Configuration**.
2. In the Contact Center Licensing window, click the **Real Time Usage** tab.
3. Review these entries in the file `D:\Avaya\lm\bin\plservrc` on the License Manager server.

   For example, if the file contains hqvD950dcWZqbmxtoc3V3dnaC9uvNHk +WJlxtaimKiihIbkfyGG1Nw5OVl5 aWFg= #CCM 6.0 00:04:75:f8:0b:8d LM_MMPN (1) 60 secs, then the existence of LM_MMPN indicates that Multimedia is licensed nodally.

Adding licenses to your current Contact Center License Manager file

Before you begin

- Contact your distributor to upgrade your license.
- Ensure that you have your new License Manager file.

About this task

Add licenses by contacting your distributor to upgrade your license and then install your newContact Center License Manager file.

You must restart the CCMM Starter service and the CCMM License service once you have added the new Contact Center License Manager file.

If you are using a remote Avaya WebLM server, see the Avaya WebLM documentation for instructions on applying your updated license file on the WebLM server.

Procedure

1. Log on to the server where the Contact Center License Manager software is installed.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **License Manager** > **Configuration**.
3. On the License Manager Configuration Utility window, click **Browse**.
4. Navigate the file system and locate the new license file.
5. Click **Open**.
6. On the License Manager Configuration Utility window, Click **Apply**.
7. If you are using a WebLM license file ignore the **LMConfig** dialog box for now. Otherwise, skip to Step 12.
8. On the **Start** menu, click **All Programs** > **Administrative Tools** > **Services**.
9. Right-click the **Contact Center Tomcat Instance** service, and click **Stop**.
10. Right-click the **Contact Center Tomcat Instance** service, and click **Start**.
11. Close the Services window.
12. On the LMConfig dialog, click **Yes** to restart the Contact Center License Manager server.
13. Click **OK** to close the window.
14. Click **Exit**.

Reviewing the Contact Center License Manager log files

About this task

Review the Contact Center License Manager log files to look for any errors that have occurred. If you are unable to find or diagnose the cause of the errors, contact Avaya technical support.

Procedure

1. On the Contact Center License Manager server, review the log file specified in the registry at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nortel\LM\Server\Logfile`.

2. On the Contact Center Multimedia server, review the log file specified at location `D:\Avaya\Logs\Common Components\CC_LMClient_1.log` and `D:\Avaya\Logs\CCMM\CCMM_LMService_1.log`.
3. On the Contact Center Multimedia server, review the CCMM Starter Service log file specified in `D:\Avaya\Contact Center\Multimedia Server\Server Applications\LICENSING\CCMMStartService.exe.config` in the variable *logFilename*.

Resetting the Licensing grace period

About this task

If there is a communication error between Contact Center Multimedia and the Contact Center License Manager, normal operation of Contact Center Multimedia can run for a defined grace period. Normal operations such as shutting down the server, starting up the server, or restarting the services do not affect the grace period.

The defined grace period is 30 days. When the 30 days expires, the Contact Center Multimedia services shut down and cannot be restarted until the grace period is reset.

If a communication problem occurs between the CCMM and the LM, 30 days are available for the CCMM to continue normal operation. After you resolve the communication problem, the grace period automatically reverts to 30 days. For example, if the communication problem is resolved in two days, the grace period returns to 30 days after two days of successful connection to the LM.

The Application log section of the Windows Event Viewer shows when grace period time has elapsed. When the grace period expires, the event 61154 Fatal Error appears in the Windows Event Viewer.

You can contact Avaya to reset the grace period. Schedule the grace period reset outside of normal contact center working hours.

Procedure

1. On the Multimedia Contact Server, choose **Start** > **Administrative Tools** > **Event Viewer**.
2. Double-click the event where the grace period has decreased (Error 61151) or expired (Error 61154).
3. In the Event Properties dialog box, copy the lock code. The lock code appears immediately after the text `Lock code =` in the **Description** box.
4. Send the Lock code you copied to Avaya Technical Support.

   Avaya Technical Support supplies you with an unlock code.
5. After Avaya Technical Support supplies you with an unlock code, on the Multimedia Contact Server, choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **Grace Period Reset**.
6. In the Avaya Contact Center License Grace Period Reset application, in the **Enter the code received from Avaya** box, type or copy the code received from Avaya.

7. Click **Apply**.
8. Ensure that the status changes to Code decrypted successfully.
9. Click **Exit**.
10. On the Start menu, choose **Administrative Tools** > **Services**.
11. Stop the CCMM Starter service.
12. Stop the CCMM License service.
13. Start the CCMM License service.
14. Start the CCMM Starter service.

Chapter 13: Contact Center Multimedia troubleshooting

This section describes the troubleshooting procedures that you perform when handling Contact Center Multimedia problems in Avaya Aura® Contact Center.

Prerequisites for Contact Center Multimedia troubleshooting

Procedure

- Verify your selected servers before installing Contact Center Multimedia. This verification includes making sure the computers conform to the specifications listed in *Avaya Aura® Contact Center Fundamentals and Planning* (44400-211).
- Ensure that the operating system is installed and functioning properly.
- Ensure that both the active and standby servers are set with the current local date and time for installation and switching Primary servers to work correctly.
- Ensure that server names and IP addresses match.
- Ensure that the US English option is selected in the Windows 2008 Server Regional Options control dialog box (on the Regional Options tab and the Advanced tab).
- Ensure that you get technical support for all hardware issues. Hardware diagnostics are the responsibility of the hardware vendor.
- Ensure that you verify the manufacturer's instructions before you perform any hardware-related procedure.

Troubleshooting Multimedia licensing configuration errors

About this task

The Contact Center License Manager server contains the files required to determine what features and functionality are enabled in the contact center. If licensing is working properly, the enabled bit in the cls.Licenses table for the Contact Center Multimedia caché database is 1.

Procedure

1. Verify the Multimedia services are started.
2. Check the contents of the license registry.
3. Check the connection between the Multimedia server and the License server.
4. Check the name of the License server in the Multimedia Administrator.
5. Choose the correct license type.
6. Check the licenses in your contact center.
7. Review the license log files.

Verifying the Multimedia services are started

About this task

Verify that the Contact Center Multimedia License Service and the Contact Center Multimedia Starter Service are both Started.

Procedure

1. On the Windows **Start** menu of the server, choose **Administrative Tools** > **Services**.
2. Next to CCMM License Service, verify that the **Status** is Started and the **Startup Type** is Automatic.
3. Next to CCMM Starter Service, verify that the **Status** is Started and the **Startup Type** is Automatic.

Changing the name of the Contact Center License Manager server in Contact Center Multimedia

About this task

Change the name of the Contact Center License Manager server in Contact Center Multimedia only if the Contact Center License Manager server identified in the registry key does not match the Contact Center License Manager server configured in the Multimedia Administrator. These names must match in order for Contact Center to function properly.

Procedure

1. Log on to the Contact Center Manager Administration application.
2. Click **Multimedia**.
3. In the left column, click **General Administration**.

4. Click **Server Settings**.
5. In the Server Settings window, click the **Contact Center License Server**.
6. Click **Edit**.
7. Change the name or the port number for the Contact Center License server. The default port number is 3998.
8. In the **Backup Server** box, type the name for the backup Contact Center License Manager server, if you have one.
9. Click **Save**.
10. On the **Start** menu, choose **Administrative Tools** > **Services**.
11. Stop the CCMM Starter service.
12. Stop the CCMM License service.
13. Start the CCMM License service.
14. Start the CCMM Starter service.

Changing the license type

About this task

Change the license type on the Contact Center Multimedia server only if necessary to ensure that the type of license (Nodal or Corporate) on the Contact Center License Manager server, specified in the registry at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nortel\LM\Type, matches the license type defined in Contact Center Multimedia, specified in the registry on the Multimedia server in HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nortel\LM\Type.

Procedure

1. Log on to the Contact Center Manager Administration application.
2. Click **Multimedia**.
3. In the left column, click **General Administration**.
4. Click **General Settings**.
5. Under **License Type** box, choose the license type (NODAL or CORP).
6. Click **Save**.
7. On the **Start** menu, choose **Administrative Tools** > **Services**.
8. Stop the CCMM Starter service.
9. Stop the CCMM License service.
10. Start the CCMM License service.
11. Start the CCMM Starter service.

Troubleshooting database access errors

About this task

If the system cannot access the database, you need to check for several potential issues.

Procedure

1. Ensure that the Multimedia services are running.
2. Ensure that you can connect to the database.
3. Check the size of the database in the `D:\Avaya\Contact Center\Databases\CCMM \MULTIMEDIA\DATA\Cache.Dat` file, where D is the database drive. Ensure there is sufficient disk space available.

Logging on errors

About this task

If you cannot log on to Contact Center Multimedia, you need to check that the database is running.

Procedure

Verify that the database is running.

Troubleshooting an ODBC error

About this task

An ODBC error can occur when there is a delay in the database startup.

Procedure

Wait a few minutes, and then try to perform the task you were attempting again.

Reviewing Email Manager Event Logs

About this task

Email Manager Event Logs are the primary tool for dealing with problems that can occur while using Email Manager.

Procedure

1. On the server, select **Start** > **Administrative Tools** > **Event Viewer**.

2. Expand **Custom views**.
3. Review the event messages where the Source is E-mail.

Troubleshooting when the Email Manager cannot log on to a mailbox

About this task

When the Email Manager cannot log on to a mailbox, there are several possibilities for this problem to occur.

Procedure

1. Log on to the mailbox using an email client.
2. Verify that the domain name, account name, mailbox name, and password match the email server settings.
3. Verify that the email server is running and that it is set up properly.
4. Review the log files.
5. Use telnet to verify the user names on the server.

Verifying the user names on the server

About this task

Verify the user names on the server by logging on to the email server. If the log on is successful, a message appears:

```
+OK X1 NT-POP3 Server mail009 (IMail 7.04 997957-16) user billing
+OK send your password pass abc123
+OK maildrop locked and ready
```

If the log on is not successful, a message appears:

```
+OK X1 NT-POP3 Server mail009 (IMail 7.04 998172-17) user billing
+OK send your password pass 123abc
-ERR Invalid userid/password
```

Procedure

1. On the **Start** menu of the email Server, choose **Run**.
2. Type `telnet <mailserver> 110` (where 110 is the port number for POP3), and then press `Enter`.
3. Log on to the email server.

4. Review the message to determine whether or not the log on is successful.

Troubleshooting when the Multimedia Email Manager Inbox does not receive email

About this task

Troubleshoot when the Multimedia Email Manager Inbox does not receive email by verifying that the email server is working properly and that the host names of the external mail servers are correctly recorded on the Multimedia server.

Procedure

1. Log on to the Contact Center Manager Administration application.
2. Click **Multimedia**.
3. In the left column, click **General Administration**.
4. Click **Server Settings**.
5. Click the **Inbound Mail Server**.

   The inbound mail server can be a POP3 server or an IMAP server.
6. Click **Edit**.
7. Under Edit Inbound E-mail Server, check the name of the server and the port number of the server and change if required.
8. Click **Save**.
9. Click the **Outbound SMTP Server**.
10. Click **Edit**.
11. Under Edit Outbound SMTP E-mail Server, check the name of the server and the port number of the server and change if required.
12. Click **Save**.

Troubleshooting when Asian characters are not supported in email

Before you begin

- Download the x64 version of the Windows Server 2008 Release 2 Multilingual User Interface Language pack from www.microsoft.com.

About this task

Troubleshoot to ensure Asian characters are supported in email by installing the Windows Server 2008 Release 2 Multilingual User Interface Language Packs.

Procedure

1. Click **Start** > **Control Panel** > **Clock** > **Language** > **Region**
2. Click **Install or uninstall display languages**.
3. Click **Install display languages**.
4. Click **Browse** to locate the language pack that you downloaded.
5. Click **Next** to install the language pack.
6. If you are prompted to insert your Windows Server DVD, insert the Windows Server 2008 Release 2 64-bit Edition DVD into the DVD drive.
7. Reboot your server, if required.

Troubleshooting the corruption of outgoing email

Before you begin

Determine which one of the following types of coding is required for your system:

- US-ASCII American Standard Code for Information Interchange
- windows-1250 Windows Eastern European
- windows-1251 Windows Cyrillic
- windows-1252 Windows Latin-1
- windows-1253 Windows Greek
- windows-1254 Windows Turkish
- windows-1257 Windows Baltic
- ISO-8859-1 Latin Alphabet No. 1
- ISO-8859-2 Latin Alphabet No. 2
- ISO-8859-4 Latin Alphabet No. 4
- ISO-8859-5 Latin/Cyrillic Alphabet
- ISO-8859-7 Latin/Greek Alphabet
- ISO-8859-9 Latin Alphabet No. 5
- ISO-8859-13 Latin Alphabet No. 7
- ISO-8859-15 Latin Alphabet No. 9
- KOI8-R KOI8-R, Russian
- UTF-8 Eight-bit UCS Transformation Format

- UTF-16 Sixteen-bit UCS Transformation Format, byte order identified by an optional byte-order mark
- UTF-16BE Sixteen-bit Unicode Transformation Format, big-endian byte order
- UTF-16LE Sixteen-bit Unicode Transformation Format, little-endian byte order

About this task

Troubleshoot the corruption of outgoing email by changing the encoding. The Email Manager, by default, encodes outgoing email using UTF-8. On some systems, for email message to be sent successfully, the platform encoding needs to be modified to match the encoding of the sending language family.

Acceptable encoding values are available at http://docs.oracle.com/javase/1.5.0/docs/guide/intl/encoding.doc.html

Procedure

1. Log on to the Contact Center Manager Administration application.
2. Click **Multimedia**.
3. In the left column, click **Email**.
4. Click **General Settings**.
5. Under **Encoding**, in the **Encoding for agent initiated emails** list, select the type of encoding you want to use.
6. Click **Save**.
7. On the **Start** menu of the Multimedia server, choose **Administrative Tools** > **Services**.
8. Right-click **CCMM Email Manager service**, and then click **Restart**.
9. Close the window.

Troubleshooting outgoing email errors with MS Exchange 2007

Before you begin

- Ensure that you are using Microsoft Exchange 2007 on your email server.

About this task

Troubleshoot when outgoing email is not sent when using Microsoft Exchange 2007 to send email from the Contact Center Multimedia agent desktops. If you are using Microsoft Exchange 2007, you must ensure that additional configuration is performed on the Contact Center Multimedia Server and the Microsoft Exchange server.

If you are using Microsoft Exchange 2003, additional configuration is not required.

Procedure

1. Log on to the Contact Center Manager Administration application.

2. Click **Multimedia**.
3. In the left column, click **General Administration**.
4. Click **Server Settings**.
5. Select the **Outbound SMTP Server**.
6. Click **Edit**.
7. Under **Advanced SMTP Settings**, select **Base 64 Encoded Authentication**.
8. Click **Save**.
9. Log on to the Microsoft Exchange 2007 server.
10. Open the Exchange Management Console.
11. Click **Server Configuration** > **Hub Transport** > **Receive Connectors Tab**.
12. Right-click the **Default <Servername>** and click **Properties**.
13. Click the **Authentication** tab.
14. Ensure that only the following options are checked for authentication:
    - Basic Authentication
    - Exchange Server Authentication
    - Integrated Windows Authentication
15. Close the Exchange Management Console.

Troubleshooting when the system fails to send an auto-acknowledgement or email response to a customer

About this task

Troubleshoot to determine the reason why the system failed to send an auto-acknowledgement or email response to a customer by reviewing the possible reasons the error occurred.

Procedure

Verify the following:

- An auto-acknowledgement is configured in the Multimedia Administrator.
- The SMTP service is running on the email server.
- The Contact Center E-mail Manager service is running on the Contact Center Multimedia server.
- The email address of the customer is correct.

Troubleshooting an unsupported authentication mechanism

About this task

Troubleshoot an unsupported authentication mechanism if, after submitting the EHLO command, the server responds with error codes 500, 501, or 502. These error codes indicate that SMTP Authentication is not supported on that mail server.

If you receive a message 504 Authentication mechanism unsupported after the AUTH LOGIN command, it is possible that your mail server conducts SMTP Authentication by either not encoding the logon credentials or by using CRAMMD5 encoding.

You must not select TLS encryption if the server responds with these error codes.

Procedure

Contact your distributor for further details.

Troubleshooting when Contact Center Multimedia fails to un-install

About this task

Troubleshoot when Contact Center Multimedia fails to un-install from a Voice and Multimedia Contact Server.

When un-installing all Contact Center applications from a Voice and Multimedia Contact Server, Contact Center Multimedia sometimes fails to un-install.

Procedure

Run the **Uninstall Contact Center** utility again.

Chapter 14: Communication Control Toolkit troubleshooting

This section describes the troubleshooting procedures that you perform when handling Communication Control Toolkit issues.

Prerequisites for Communication Control Toolkit troubleshooting

Procedure

- Ensure that you are aware of the configurations of your Communication Control Toolkit server software before you begin.
- Communication Control Toolkit configuration is one of the following:
  - Communication Control Toolkit on Avaya Communication Server 1000 -Contact Center
  - Communication Control Toolkit on Avaya Communication Server 1000 - Knowledge Worker
  - Communication Control Toolkit with Microsoft Office Communication Server
  - Communication Control Toolkit with the Avaya Aura® Unified Communications platform - Contact Center

Stopping the Telephony service

About this task

When you cannot stop the Telephony service when using an Avaya Communication Server 1000 platform, you must disable remote access and restart the server.

Procedure

1. Disable the Remote Access connection manager and Remote Access Auto connection manager services.
2. Restart the server for these changes to take effect.

Adding the Administrator to the Communication Control Toolkit console

About this task

If you receive an error when you try to add the Administrator to the Communication Control Toolkit console, do not attempt to make any changes.

Procedure

Contact your Avaya support prime for assistance.

Importing XML data from the CCT Administrator Snap-in to the CCT database

About this task

The CCT Administrator Snap-in sometimes cannot import XML data into the Communication Control Toolkit database if the format selected in the CCT Administrator Snap-in Data Import/Export tool is not correct.

Procedure

In the CCT Administrator Snap-in, in the Data Import/Export tool, check the format selected matches the format of the input file.

Launching the CCT Web Administration page from CCMA

About this task

The CCT Web Administration does not load if Tomcat is not running or the Internet browser is not configured correctly.

Procedure

1. Check that Tomcat is running.
2. Check whether the browser is configured to allow javascript.
3. If the Windows 2008 Server firewall is on, check that the most recent Avaya Aura® Contact Center firewall policy to open contact center ports is applied.

Launching CCT Web Administration page without any data

About this task

The CCT Web Administration does not display data if the relevant services are not running.

Procedure

1. In SCMU , check that the CCT DAL service is running .
2. Check that Caché is running.

Displaying the Agent Desktop with no CCT resources

About this task

In an AML-based contact center, Agent Desktop sometimes does not display CCT terminals due to CCT configuration issues.

Procedure

1. Check the agent, user, terminal and address resource assignment in CCT Web Administration.
2. If CCT is on a standalone server, ensure the correct deployment type is configured in CCT Administrator Snap-in.
3. Ensure there are no issues on the PABX.

Hotdesking does not work

About this task

If hotdesking is not working, check the configuration in CCT Web Administration.

Procedure

1. Check that the agent is created in CCMA and is assigned to a CCT domain user.
2. Check that the correct addresses are assigned to each terminal in CCT Web Administration.
3. Check that each terminal is assigned to a workstation in CCT Web Administration.
4. Check that the terminals for hotdesking are assigned to a terminal group in CCT Web Administration.
5. Check that the windows users for hotdesking are assigned to a user group in CCT Web Administration.
6. Check that the terminal group is assigned to the user group in CCT Web Administration.

Associating agents in CCMA to users after a migration

About this task

If there are agents visible in CCMA after a migration without users associated to them, then there is possibly a mismatch between the first name and last name of the user and the first name and last name of the agent.

In the current release, when an agent is created, CCMA uses the CCT windows user first name and last name as the agent's first name and last name. Therefore in a migration from a previous release when this one to one mapping of user first name and last name and agent first name and last name was not used, CCMA displays agents without their associated windows user.

Procedure

1. Check the first name and last name of the windows user matches the first name and last name of the agent.
2. If it does not match, edit the name to match or create a new user to match the agent details.

Logging off agents after a switchover in a contact center with a CS 1000 PABX

About this task

If an Agent is on a call when a High Availability switchover occurs, the call does not appear on Agent Desktop after the switchover is complete. The result is the Agent can see that the call is missing, but cannot log off until after the call is finished. The agent cannot log off while on a call. The log off request remains pending in the Avaya Communication Server 1000 until the call ends.

Procedure

1. The Agent attempts to log off.
2. The Agent waits until the call is finished and then the agent is automatically logged off.

Troubleshooting following a power outage

About this task

Following a power outage, view the Windows event logs to determine if any service did not stop gracefully during the power outage.

Procedure

1. On the Communication Control Toolkit server, open the Windows Event Viewer.

2. Determine if any events were created to indicate a service failure by reviewing the following logs:
   - Windows error reporting
   - hdmp
   - mdmp
   - Java hotspot
3. Follow up on any specific errors described in the event logs.

Troubleshooting when the cache service is unavailable after a server reset

About this task

The cache service is grayed out after the server is reset during a restoration of the Communication Control Toolkit database.

Procedure

Contact Avaya support if cache is not running.

Troubleshooting when the CMF Web service link fails

About this task

CCT uses a polling mechanism to monitor the status of the Web service connection to Contact Management Framework (CMF). Failure of the Web service link or restarting of CMF triggers a Shutdown event to the CCT server. You can configure tolerance of the polling mechanism by modifying the settings in the `Nortel.CCT.Service.exe.config` file.

Procedure

1. Open the `Nortel.CCT.Service.exe.config` file.

   The file is located in `<AACC Drive>:\Avaya\Contact Center\CCT`.
2. Modify the *LinkTimeout* value in the `Nortel.CCT.Service.exe.config` file.

   The *LinkTimeout* value represents the timeout in seconds for polling of the link to CMF.

   The default value is 8 seconds.
3. Modify the *LinkErrorThreshold* value in the `Nortel.CCT.Service.exe.config` file.

   The *LinkErrorThreshold* value defines the number of failed link polling messages that the system can send before triggering a Shutdown event.

The default value is 3. Therefore, the default maximum outage is 24 seconds at the default *LinkTimeout* value of 8 seconds.

Chapter 15: Using CCT Reference Client for troubleshooting

In addition to using the Reference Client to verify the Communication Control Toolkit installation, you can use the Communication Control Toolkit Reference Client as a diagnostic tool with Avaya Aura® Contact Center. The Reference Client application is designed to troubleshoot your client applications.

If the Reference Client demonstrates the functionality you require, but your custom client application does not, then there is a problem in your client application. Otherwise, there is a problem with the Communication Control Toolkit server software.

You can use the Reference Client application to do the following:

- Verify the server settings, if required.
- View agent, device, or contact details.
- View the Reference Client event log.
- Test telephone functions.

Logging on to the Reference Client

About this task

Log on to the Reference Client to diagnose problems with the client application.

Procedure

1. Log on to the server with the Local Administrator user ID and password.
2. From the **Start** menu, choose **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **RefClient**.
3. Click **OK**.
4. From the **Session** menu, choose **Connect As**.
5. In the **User ID** box, enter your user ID.
6. In the **Domain** box, enter the host name of your Communication Control Toolkit server or the domain name for your user ID.
7. In the **Password** box, enter your password.

8. Click **OK**.

   The available devices list displays a list of lines and their associated DNs.

Viewing agent, device, and contact details

About this task

You can view information about the agents in the contact center, the associated devices, and the current contact using the Reference Client. The agent details show the information about the agent that is configured in Contact Center Manager Administration.

Procedure

1. On the View menu of the Reference Client application, click **Agent Details** to view the agent details.
2. On the View menu of the Reference Client application, click **Device Details** to view information about your current device.
3. On the View menu of the Reference Client application, click **Contact Details** to view information about the current contacts using the Reference Client during a call.

Viewing the Reference Client event log during a call

About this task

You can view the event log during a call to help diagnose any issues you experience when you connect to your phone.

Procedure

1. Log on to the Reference Client.
2. From the **View** menu, choose **Event Log**.
3. Keep the Event Log dialog box open while you make a call using the Reference Client.
4. In the **Available Desktop Devices** box, choose a terminal that you configured.
5. Choose the address from which you want to make a call.
6. In the **Destination Address** box, enter the address you want to call.
7. Click **Originate**.

Viewing the Reference Client server settings

About this task

You can view your server settings using the Reference Client.

Procedure

1. Log on to the Reference Client.
2. From the **Preferences** menu, choose **Server**.

Making the phone busy

About this task

You can make the phone busy using the Reference Client.

Procedure

1. Log on to the Reference Client.
2. Click **DND** (do not disturb).
3. Click **Set** "**do not disturb**".

Forwarding a call

About this task

You can forward a call using the Reference Client.

Procedure

1. Log on to the Reference Client.
2. Click **FWD**.
3. Click **Set/Change Forwarding Instructions…**

Generating DTMF digits while on a call

About this task

You can use the Reference Client to generate DTMF digits while on a call.

Procedure

1. Log on to the Reference Client.
2. Click **DTMF**.

Attaching contact data

About this task

You can use the Reference Client to attach contact data while on a call.

Procedure

1. Log on to the Reference Client.
2. Click **Data**.

Calling a supervisor

About this task

You can call a supervisor using the Reference Client.

Procedure

1. Log on to the Reference Client.
2. Click **Call Supervisor**.

Calling a supervisor while on an ACD or CDN call

About this task

You can use the Reference Client to call a supervisor while on an ACD or CDN call.

Procedure

1. Log on to the Reference Client.
2. Click **Emergency**.

Setting an activity code

About this task

You can set an activity code using the Reference Client.

Procedure

1. Log on to the Reference Client.
2. Click **Activity**.

Troubleshooting when the Reference Client cannot make a call in a contact center with a CS 1000 PABX

About this task

Troubleshoot using the following procedure if the Reference Client application receives the signaling when a phone is taken off the hook, but the Reference Client fails when an attempt is made to make a call from the phone.

Procedure

Ensure that the SECU prompt on the PABX is set to yes in LD17.

Troubleshooting when Reference Client terminals appear out of service

About this task

Troubleshoot when Reference Client terminals appear out of service and Reference Client does not control acquired TNs (AML) or SIP Lines (CS1000 SIP). Agent logon using Reference Client fails, and calls do not appear on Reference Client when the acquired TNs or SIP Lines monitored by the Reference Client receive a call on the deskphone.

Procedure

Ensure that controlled TNs (AML) or SIP Lines (CS1000 SIP) are acquired by the PABX.

Chapter 16: Agent Desktop troubleshooting

Troubleshoot Agent Desktop to address errors that occur when the agent is working on the application.

Enabling and Configuring Agent Desktop Dashboard

The Agent Desktop Dashboard feature enables agents to collect and upload log files or videos to the CCMM server. Agents can also use the Dashboard to check the connectivity of Agent Desktop with the Contact Center servers.

When an agent clicks **ZIP Log Files** on the dashboard, Agent Desktop collects the following in a single .ZIP file:

- a screenshot of the agent's Windows desktop
- the Agent Desktop log file
- the XML configuration files
- a list of processes running on the desktop computer

The agent can then click the **Upload** button to upload the .ZIP file to the CCMM Server.

Alternatively, the agent can capture a screen sequence to log a series of steps that resulted in the issue they are reporting. When an agent clicks **Capture Video** on the dashboard, Agent Desktop collects a screen capture of the agent's Windows desktop every second until they click **Finish Recording**. Agent Desktop creates a zip file of these screen captures, and the agent can click **Upload Video** to upload the file to the CCMM server. The screen sequence capture has a default maximum of 60 seconds. During log file and screen sequence captures, the Dashboard relocates to bottom corner of the screen, so it does not interfere with the screen capture. When Agent Desktop completes the operation, it displays the Dashboard Message screen, identifying the folder to which it saved the log files.

The default server location for the uploaded log files is `D:\Avaya\Logs\CCMM\AADS`. The ZIP file name is `Agent<logonID>.zip`, where `<logonID>` is the agent's log on ID. Contact Center uses the same upload mechanism as it uses for agent attachments, so there is no additional configuration needed.

Each file uploaded by an agent overwrites their previous one. Each time an agent uploads a file, Contact Center moves the previous version to the archive location, using a new default rule defined in the CCMS Log Archive tool.

Enabling the Agent Desktop Dashboard is a global option that you can select in the CCMM Administration Client under **Agent Desktop General Settings**. Optionally, you can choose to have the dashboard password protected, so that agents cannot initiate the function independently. You cannot change the default password; it is always `__avaya`.

On existing Voice-only telephony toolbar installations, the Agent Desktop Dashboard feature creates the log files, but does not upload them because there is no CCMM server. Agent Desktop stores the log files in the folder that the agent specifies in the **Local Logs Location** field.

Content of the log ZIP file

The log zip file that the Agent Desktop Dashboard generates is typically between 400–500 kbs, and contains the following content:

A screen capture of the agent's desktop:

This shows the complete Windows desktop at the time the agent clicked the **ZIP Log Files** button.

The Agent Desktop log file:

The timestamp option that an administrator selects determines the amount of information that Agent Desktop collects in the log file. It is also possible to set a time limit on the log messages collected, so thatAgent Desktop includes only recent events in the ZIP file.

XML configuration files:

These are the three XML configuration files associated with the current agent session: CCADApplicationSettings.xml, CCADUserSettings.xml, and CCADIntrinsicSettings.xml.

A list of processes:

This text file lists all processes currently running on the agent's desktop computer. The process information includes the process name, the process ID, and the physical memory, virtual memory, peak memory, handles, and threads for that process.

Content of the Video log file

A video log file contains a sequence of screen captures of the agent's Windows desktop, in .JPG format, one for every second while recording continues. The default maximum recording time is 60 seconds, which limits the size of the file for upload. However, depending on the screen resolution, video log files can be quite large. For example, if a desktop with a screen resolution of 1440x900 generates a screen capture .JPG file of 322Kb, 60 seconds of recording creates a video log file of approximately 19Mb.

Logging Levels

It is possible to modify the logging levels on an individual agent's desktop, through settings on the Dashboard. Enabling additional logging can impact the CPU usage and disk space on the agent desktop PC. Agents must configure these settings only under the guidance of a system administrator or support staff.

Enable Enhanced CCT logging:

When you enable this option, Agent Desktop includes messages from the CCT server relating to CCT events in the logs.

Enable Presence logging:

When you enable this option, Agent Desktop includes additional Presence related messages in the logs. These include XMPP Messaging Protocol Logs from the Avaya Presence Services or any log messages related to Microsoft OCS or Lync server.

Enable Web Stats Logging:

When you enable this option, Agent Desktop captures log messages relating to Agent Desktop interactions with the CCWS service (Contact Center Web Stats), including data that the service returns.

Enable Method Entry/Exit logging:

When you enable this option, Agent Desktop includes messages that identify when the execution of Agent Desktop methods begin and end.

Enable WNDPROC logging:

When you enable this option, it turns on WNDPROC message logging, which displays log messages whenever the agent manipulates user interface elements, for example if they resize or drag the screen around.

Enable Reason Code logging:

When you enable this option, Agent Desktop includes log messages for when After Call Work, Not Ready Reason, and Activity Codes change. For example, if the administrator changes the NRRC then the logs show all the NRRC's as available at that time.

AAAD Logging Level:

You can select the level of logging that Agent Desktop captures. Selecting 1 enables the minimum level of logging, capturing critical events only. Selecting 6 enables the maximum level of logging, capturing every possible event.

Server network connections

Agents can use the Primary Servers and Standby Servers tabs to check the network connectivity between their desktop PC and the Contact Center servers. The connection test is based on an ICMP ping to the servers hosting the Contact Center applications. The list of servers shows all the Contact Center applications, even if they are co-resident systems.

If the Dashboard can ping an application server, it shows "Reachable" on a green background. If it cannot ping a server, it shows "Not Reachable" on a red background.

The Agent Desktop Dashboard displays the Standby server tab only if you have a HA system.

Prerequisites for Agent Desktop troubleshooting

Procedure

- Read the *Avaya Aura® Contact Center Server Administration* (44400-610) guide.
- Read the *Avaya Aura® Agent Desktop User Guide* (44400-114) guide.

Configuring the Agent Desktop Dashboard global settings

Before you begin

- Log on to Contact Center Manager Administration and open Multimedia Administration.

About this task

Follow this procedure to enable agents to use the Agent Desktop Dashboard and to configure how agents can use it.

Procedure

1. On the Multimedia Administration tool, select **Agent Desktop Configuration**.
2. In the left pane, click **User Settings**.
3. Click **Enable AAAD Dashboard**.
4. If you want to control agents' access to the Agent Desktop Dashboard, click **Password Protect AAAD Dashboard**.

Logging on to Agent Desktop

About this task

Troubleshoot when you encounter problems logging on to Agent Desktop by reviewing the possible reasons for the error.

Procedure

1. Verify that IIS is running.
2. Verify that ASP and ASP.NET are enabled.
3. Verify that the user has access rights to the Web applications.
4. Verify that the Contact Center Multimedia services are running.
5. Verify that the software for .NET Framework and .NET service pack 4.0 is installed on the clients.
6. Verify that the agent ID is valid.
7. Verify that the agent password is valid, or is the default password.
8. Verify that you have not exceeded the number of Agent Desktop or Outbound Campaign Management Tool licenses in your Contact Center.
9. Verify that Domain Naming Service (DNS) is working.
10. Verify that you can ping the server which includes Contact Center Multimedia (multimedia solution) or the server which includes Communication Control Toolkit (voice only solution) using the server name.
11. Verify that you have a two way trust with the server domain which includes Contact Center Multimedia (multimedia solution) or the server domain which includes Communication Control Toolkit (voice only solution).
12. Verify that there is no existing call active on your deskphone. If a call exists, release this call before logging on to Agent Desktop.

Troubleshooting Agent Desktop click-once deployment errors

Before you begin

Ensure you installed the Agent Desktop prerequisites.

About this task

Troubleshoot if you encounter problems installing Agent Desktop using the click-once deployment method.

Procedure

1. If the install fails to run on one desktop PC, but runs on another one, clear the Internet Explorer browser history.
   a. On the Internet Explorer Tools menu, select Internet Options.
   b. On the Internet Options dialog, in the General settings tab, under Browsing History, click **Delete**.
   c. Click **OK**.
2. If clearing the browser history does not resolve the problem, reboot the desktop PC and try the installation again.
3. If restarting the desktop PC does not resolve the problem, contact Avaya support.

Troubleshooting a forgotten agent password

About this task

Troubleshoot when an agent forgets their password by resetting the password to the default setting. You can use the Multimedia Administrator application to reset the password to the default agent password, which is the agent ID or assign any password.

Procedure

1. Log on to the Contact Center Manager Administration application.
2. Click **Multimedia**.
3. In the left column, click **General Administration**.
4. Click **Agent Settings**.
5. In the table displayed, select the agent for the password change or reset.
6. Under **Edit Agent Details**, click **Set Password** and type the new password in the **New Password** and **Confirm Password** boxes.
7. Click **Save**.

Connecting to the CCT server

About this task

Troubleshoot if there are problems on the Communication Control Toolkit server and you see the error message “Cannot connect to CCT Server”. You need to review the possible reasons why you have a problem connecting to the CCT server.

Procedure

1. On the Communication Control Toolkit server, check that the CCT Server service is started. For more information, see *Avaya Aura® Contact Center Commissioning* (44400-312).
2. In the Multimedia Administrator application, check that the Communication Control Toolkit server configuration is correct.
3. Make sure that ASP.NET is enabled on the Contact Center Multimedia server. For more information, see *Avaya Aura® Contact Center Commissioning* (44400-312).

Troubleshooting an Invalid Credentials error

About this task

Troubleshoot if you receive an error message indicating Invalid Credentials. The windows user is not configured for Communication Control Toolkit authentication.

Procedure

1. Ensure that you have followed the Communication Control Toolkit configuration steps in this guide.
2. If the user is outside the Communication Control Toolkit domain, then use a local account on the Communication Control Toolkit server to launch the Agent Desktop. You must add the local Communication Control Toolkit user to the resources and map the resources.

Logging on agents to CCMS

About this task

Troubleshoot the error “Cannot login to CCMS” if a voice agent cannot login to CCMS because another agent is already logged on to that telephone.

Procedure

Log off the first agent, or map the agent who cannot log in to a different terminal.

Troubleshooting when the Login button shows no agent

About this task

Troubleshoot when the Login button shows no agent by first determining the cause for this error. There are two possible reasons why the Login button shows no agent:

- The agent is not mapped to a contact center user.
- Agent objects are not replicated.

Procedure

1. If the agent is not mapped to a contact center user, you must map the Windows user to a contact center user for handling contacts.
2. If the agent objects are not replicated, you must ensure that Server Configuration and Contact Management Framework are both configured on Contact Center Manager Server and on Communication Control Toolkit when new patches are installed.

Troubleshooting when Agent Desktop closes unexpectedly

About this task

Troubleshoot when Agent Desktop closes unexpectedly. When you log on to Agent Desktop, a call is already present and you are unable to release this call. This problem occurs when Agent Desktop closes unexpectedly during a customer call. Use the following procedure to resolve the issue.

Note:

This issue occurs in SIP-enabled Contact Centers only.

Procedure

1. If Agent Desktop closes unexpectedly, restart Agent Desktop and log on to Agent Desktop again.
   - If Agent Desktop closes unexpectedly during a customer call, the call remains visible on Agent Desktop but you are unable to release the call. The system displays a **Release Contact Failed** dialog box, which informs you that you must release the call using your deskphone.
   - If Agent Desktop closes unexpectedly during a Multimedia contact, the contact (with the exception of a Web communications contact) is lost.
2. In order to release the call and regain Agent Desktop call control, release the call using your deskphone.

Important:

If you are using Agent Desktop with an embedded softphone only, the call must be released by the customer.

Troubleshooting when the Originate key is disabled

About this task

If the Originate key is disabled on the telephony toolbar in the Agent Desktop, a terminal is not mapped to the logged-on agent, or the mapped terminal is out of service.

Procedure

1. If a terminal is not mapped to the logged-on agent, map the user to the terminal.
2. If the mapped terminal is out of service, restart the TAPI connector, and restart the Telephony service on the Communication Control Toolkit server.

Note:

The TAPI connector does not apply to SIP-enabled Contact Centers.

Working Emergency and Supervisor keys on the phone

About this task

If the Emergency and Supervisor keys are disabled, the keys used for Emergency and Supervisor calls on phones are not configured or the telephony port property of Supervisor is incorrect.

Note:

The ASP, EMR, AAG, and AMG keys are available only in AML-based Contact Centers.

Procedure

1. Configure two keys on the agent phone: ASP (call supervisor) and EMR (emergency).
2. Ensure that the supervisor phone is configured as a supervisor phone, and then configure two keys: AAG (answers the call from the agent ASP key) and AMG (answers the call from the agent EMR key).
3. Configure the telephony port property to be the position ID of the supervisor phone. In Contact Center Manager Administration, right-click Supervisor, and then choose Supervisor details.

Working Transfer and Conference buttons on the telephony toolbar

About this task

Troubleshoot disabled buttons by enabling them using the line features available during Communication Control Toolkit installation or maintenance procedures.

Procedure

Enable transfer and conference functions using the TN details.

Troubleshooting agent statistics

About this task

Troubleshoot disabled agent and skillset related statistics. Agent Desktop displays live agent and skillset related statistics.

Procedure

Ensure that Contact Center Web Statistics (CCWS) is enabled on the CCMS server.

Opening an attachment in Agent Desktop

About this task

Troubleshoot opening an inbound attachment with Agent Desktop in the E-mail Display section.

Procedure

1. Open Internet Explorer.
2. Select **Tools** > **Internet Options** > **Programs**.
3. Confirm the default web browser is Internet Explorer.

Troubleshooting pop-up critical error messages

About this task

Troubleshoot when Agent Desktop displays a pop-up message box containing “An error has occurred and Agent Desktop cannot continue. Please ask your administrator to examine your AgentDesktopLog.txt file”. This error can indicate that the Agent Desktop client computer is low on memory.

Ensure the Agent Desktop client computer meets the Avaya Aura® Contact Center hardware specification. For more information about the client hardware specification, see *Avaya Aura® Contact Center Fundamentals and Planning* (44400-211).

Important:

This procedure requires a computer restart to apply the changes.

Procedure

1. Log on to the Avaya Aura® Agent Desktop computer.
2. Click **Start** > **Settings** > **Control Panel** > **System**.
3. On the **Advanced** tab, under **Performance**, click **Settings**.
4. On the **Advanced** tab, under **Virtual memory**, click **Change**.
5. Under **Drive [Volume Label]**, click the drive that contains the paging file that you want to change.
6. Under **Paging file size for selected drive**, click the **Custom size** check box.
7. In the **Initial size (MB)** box, type the required amount initial virtual memory.
8. In the **Maximum size (MB)** box, type the maximum required amount of virtual memory.

   Increase the maximum amount of virtual memory for Agent Desktop to function.
9. Click **Set**.
10. When you are prompted to restart the computer, click **Yes**.

Troubleshooting when a white line appears on Agent Desktop

About this task

Troubleshoot when a white line appears on Agent Desktop. The occurs occasionally on Windows client computers using the classic theme.

Procedure

1. On the Windows 7 client computer, click **Start** > **Control Panel**.
2. Under **Appearance and Personalization**, click **Change the theme**.
3. In the right pane, under **Basic and High Contrast Themes**, select **Windows 7 Basic**.
4. Close the Control Panel window.

Chapter 17: High Availability troubleshooting

Troubleshooting High Availability must be done to address errors that occur when active servers do not switch over as expected or when the standby server fails to shadow the active server.

The Windows events log contains extensive High Availability diagnostic information.

Prerequisites for High Availability troubleshooting

Procedure

- Read *Avaya Aura® Contact Center Installation* (44400-311).
- Read *Avaya Aura® Contact Center Commissioning* (44400-312).
- Read *Avaya Aura® Contact Center Server Administration* (44400-610).

Troubleshooting Mission Critical High Availability

About this task

Troubleshoot Mission Critical High Availability (HA) resiliency for a pair of High Availability servers in a campus SIP-enabled contact center environment that uses an Avaya Aura® Communication Manager and an Avaya Aura® Session Manager.

In a Mission Critical campus High Availability solution, a CCMS or CCT service failure, hardware, network, or database failure can initiate a switchover but only in the following situations:

- The active server is in the active mode.
- The active server is running. All the critical CCMS and CCT services are monitored and running.
- The active server has Enable Switchover enabled.
- The active and standby servers can communicate with the trusted server.
- The active server database and standby server database are synchronized. The standby server database is shadowing the active server database, and is up to date.

If the Contact Center Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an active server, a switchover occurs. If the Contact Center Administrator uses

the System Control and Monitor Utility (SCMU) to stop a monitored service on an active server, a switchover does not occur. If a critical service is down or restarts on the active server, a switchover does not occur.

High Availability Utility

Configure High Availability resiliency for CCMS and CCT using the High Availability (HA) utility in the Database Utilities. The High Availability utility is used to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

SMMC system tray

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your High Availability environment. The SMMC system tray has the following main menu options and action items:

- Start HA System
- Stop HA System
- Disable Switchover
- Enable Switchover
- Launch SCMU
- System Information
- Database Information
- Disable Auto Startup
- Re-enable HA System

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar.

High Availability utility and SMMC system tray

To commission High Availability, use the High Availability utility to configure High Availability IP addresses and to configure which server is the active server and which is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and High Availability functionality.

Troubleshooting High Availability

To troubleshoot High Availability, use the System Management and Monitoring Component (SMMC) utility, Windows Events logs, and the System Control and Monitor Utility (SCMU) to diagnose High Availability issues. Then use the High Availability utility in to resolve the diagnosed issues.

Procedure

1. Log on to the active server.
2. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **System Information**.
3. Examine the **System Information** dialog to determine the cause of High Availability related issues.
4. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Database Information**.

5. Examine the **Database Information** dialog to determine the cause of High Availability related issues.
6. Repeat these steps on the standby server.

Procedure job aid

The following examples are from a functional High Availability pair of servers.

Use the System Management and Monitoring Component (SMMC) utility to diagnose High Availability issues. Use the High Availability (HA) Utility in the Database Utilities to resolve the diagnosed issues.

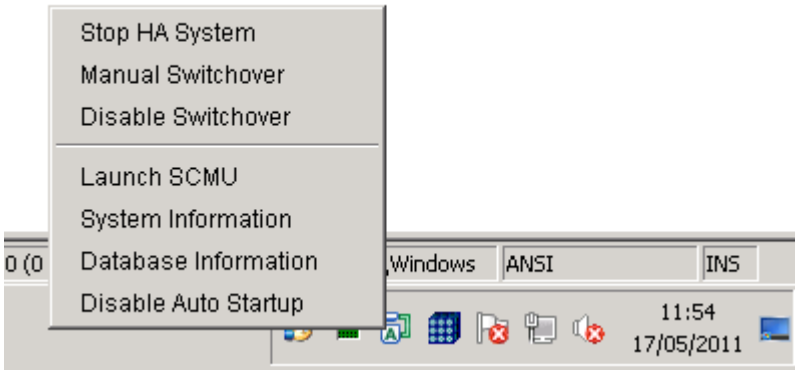


Figure 1: Example of using SMMC on a functional active server

In a High Availability solution, the SMMC system tray icon displays “A” to indicate that the server is configured as a High Availability active server. You can use SMMC on active server to perform a Manual Switchover to the standby server.

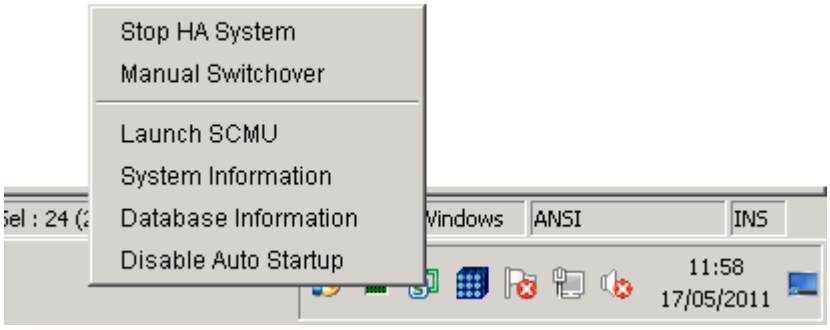


Figure 2: Example of using SMMC on a functional standby server

In a High Availability solution, the SMMC system tray icon displays “S” to indicate that the server is configured as a High Availability standby server. The standby server has different SMMC system tray menu options to the active server.

You can use SMMC system tray to display system and database information, and to diagnose High Availability related issues.

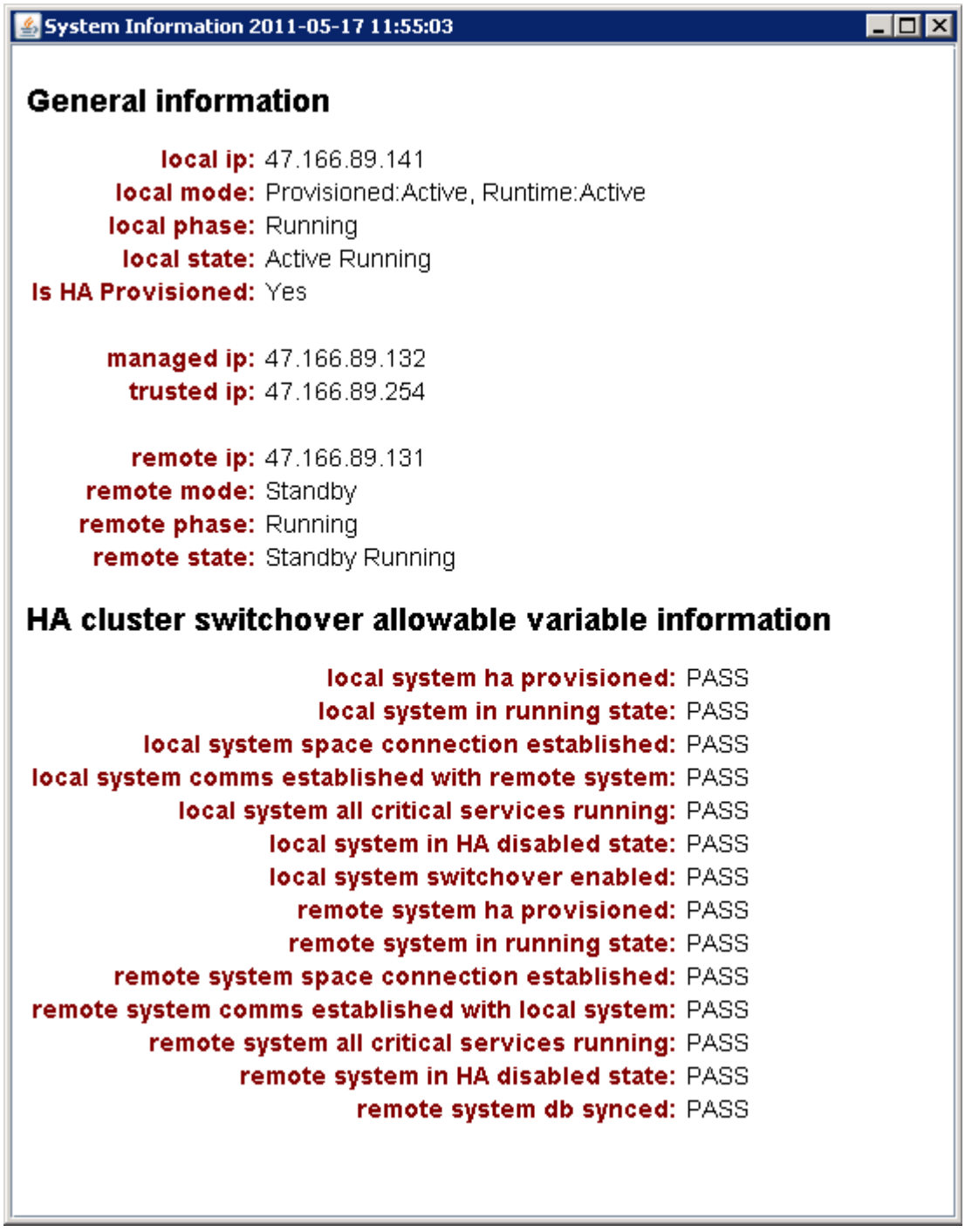


Figure 3: Example of a functional Mission Critical High Availability active server System Information dialog

Examine the System Information dialogs on the active server and standby server dialogs to ensure they mirror each other. The Trusted IP address and Managed IP address must be the same on both

servers. Examine the “General Information” section to ensure that your High Availability solution is configured correctly, and to determine why High Availability last stopped. When in Stopped state, System Information displays a “Local last known stop reason”.

On the active server, examine “local system switchover enabled” to confirm that switchover is supported and enabled.

On the active server, examine “local system all critical services running” to confirm that all the necessary services are running. If any critical service is not running, use the System Control and Monitor Utility (SCMU) to investigate further.

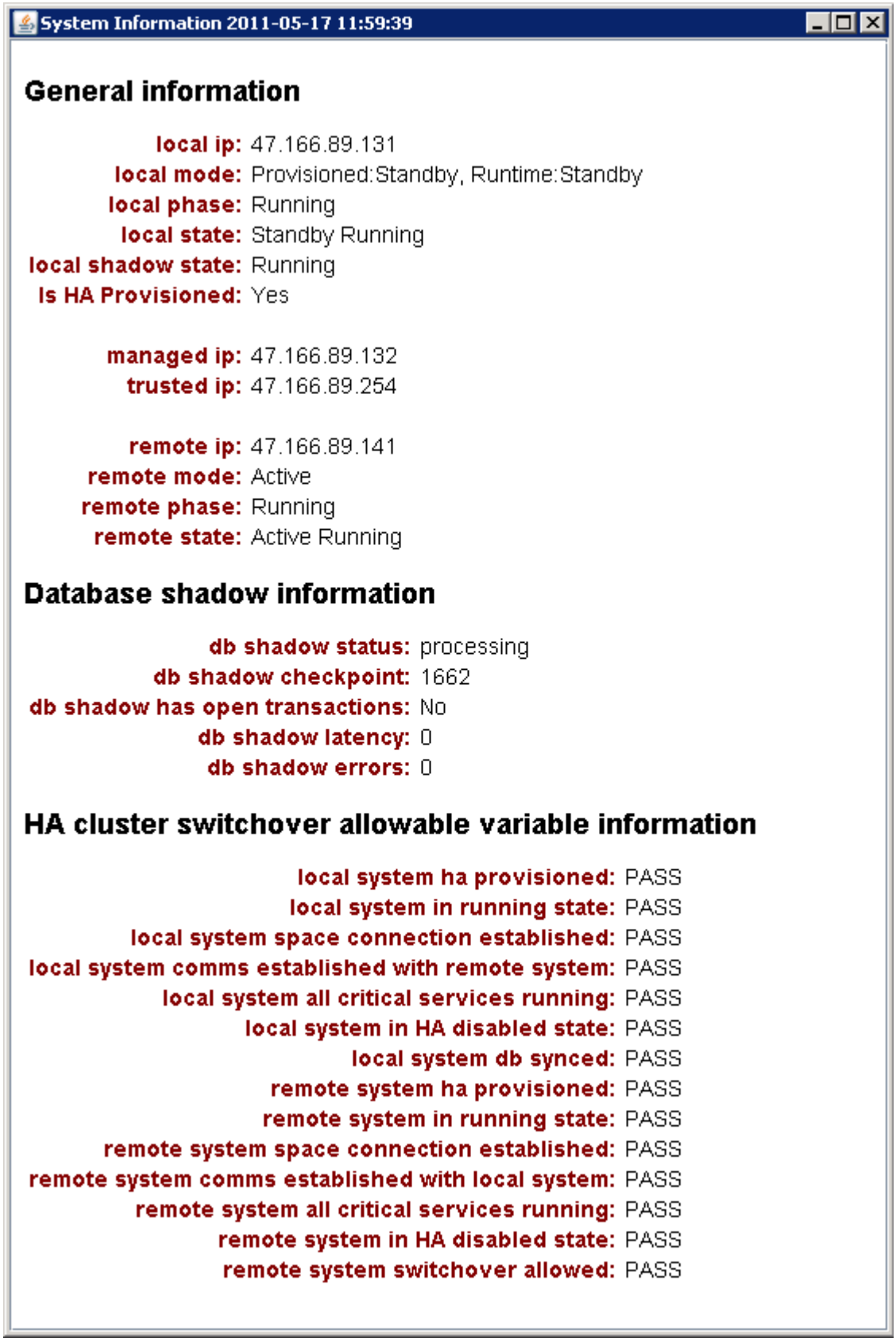


Figure 4: Example of a functional Mission Critical High Availability standby server System Information

dialog

The standby server system information dialog displays Database Shadowing information. Examine the “Database shadow information” section to determine if the network in your High Availability solution is causing shadowing issues.

Examine “local system comms established with remote system” to confirm that the SMMC on the standby server can communicate with the SMMC on the active server, and visa versa.

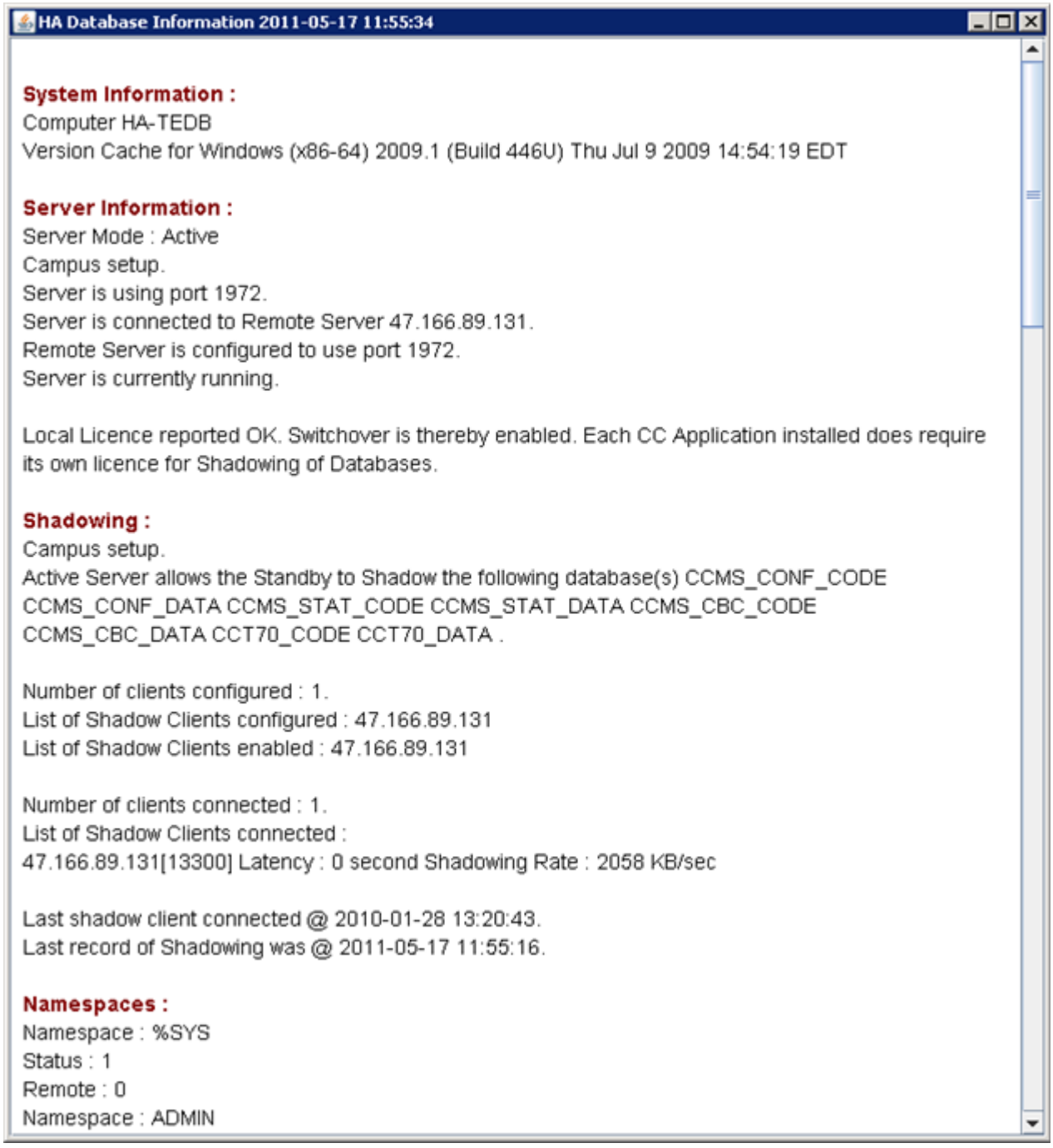


Figure 5: Example of a functional Mission Critical High Availability active server Database Information dialog

The Database Information dialog displays information about the database ports, namespaces and the number of Shadow Clients connected to a the High Availability server. On the active server a Shadow Client can also be a Remote Geographic Node server on a remote site, accessed using a Wide Area Network (WAN).

Troubleshooting when shadowing fails to start

About this task

You must backup the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock time on the active and standby servers are synchronized.

Procedure

1. Use the Database Maintenance utility to make a new backup of the active server database.
2. Use the Database Maintenance utility to restore the database to the standby server.
3. Re-commission High Availability on the standby server.
4. Use the High Availability utility to enable shadowing.

Troubleshooting when SMMC fails to start

About this task

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your High Availability environment.

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar. The SMMC system tray is a graphical interface for the underlying SMMC system. If the SMMC system fails or stops, the SMMC system tray can display a “No connection to SMMC” message. You can use the SMMC system tray menu to restart the SMMC system.

Procedure

1. Log on to the High Availability server.
2. On the Windows System Tray, right-click the System Management and Monitoring Component (SMMC) system tray icon, and select **Start SMMC**.

Troubleshooting when services fail to start

About this task

The active and standby servers use a Trusted IP address to verify network connectivity. If the active server cannot communicate with the standby server it attempts to communicate with the Trusted IP address.

In Hot standby and Warm standby High Availability solutions, if the active server cannot communicate with the Trusted IP address on startup then no Avaya Aura® Contact Center services start on that server.

Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

Procedure

Verify the active and standby servers can communicate with the Trusted IP address.

Troubleshooting using shadow only High Availability mode

Before you begin

- Configure High Availability on the active Contact Center Manager Server (CCMS) server.
- Backup the active server databases and restore the database on to the standby server.
- Using the High Availability Utility, configure High Availability on the standby server.

About this task

Use the High Availability shadow-only mode to troubleshoot your High Availability solution. In shadow-only mode, the standby server shadows (replicates) the database of the active server, but High Availability switchover is not enabled. In shadow-only mode, if the active server fails, the standby server must be manually configured as the active server and manually started.

Procedure

1. Log on to the standby server.
2. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Start Shadowing**.

   The standby server shadows (replicates) the database of the active server and switchover is not enabled.

Example

You can use the High Availability shadowing only mode to swap the roles of the active and standby servers around.

For example, if the standby system is in shadow-only mode, you can shut down the active and re-commission the standby server as the new active. This is not a mission critical switchover, and voice contact control is lost during the switchover. Email contacts persist during this manual switchover.

Outline initial High Availability (HA) setup:

1. On the active server, configure HA and create a backup of all the databases.
2. On the backup server, restore all the database backups.
3. On the active server, from the SMMC system tray menu, select Start HA system.
4. On the active server, ensure the active server is fully started.

5. On the standby server, update the server configure IP address and save it.
6. On the standby server, using the HA utility, verify the local configuration, configure it as the standby server and save it.
7. On the standby server, from the SMMC system tray menu, select Start Shadowing.

To swap the roles of the active and standby High Availability servers around:

1. On the standby server, ensure database shadowing is up-to-date and working.
2. On the active server, from the SMMC system tray menu, stop the HA system.
3. On the standby server, using the HA utility, modify the role of the standby server to be the active server.
4. On the old active server, using the HA utility, modify the role of the server to be the standby server.
5. On the new active server, from the SMMC system tray menu, start HA.
6. On the new active server, create a backup of all the databases.
7. On the old active server, restore all the database backups.
8. On the old active server, update the server configure IP address and save it.
9. On the old active server, using the HA utility, verify the local configuration, configure it as the standby server and save it.
10. On the new standby server, from the SMMC system tray menu, select Start Shadowing.

At this point the active and standby servers have now swapped roles. The old active is now the new standby and it is configured in shadow-only mode.

Troubleshooting shadowing failures

About this task

Troubleshoot when the standby server does not shadow the active server. The standby set of Avaya Aura® Contact Center applications monitors and shadows the active applications in the system and does not process calls. The standby CCMS monitors the active CCMS. The standby CCT monitors the active CCT. The standby CCMM monitors the active CCMM. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, the standby applications recognize the failure and start processing contacts.

Procedure

1. Verify that the standby server is installed exactly the same as the active server. The standby and active servers must have the exact same patch level and the same hard disk drive partitions.
2. Verify that the Cache service is running on the standby server.
3. Verify that you have installed a Standby Server license to enable High Availability.
4. Verify that the standby server can communicate with the active server by name and IP address.

5. Verify that you can ping the Managed IP address of the active server from the standby server and from a client computer.
6. Verify that the static IP address of the active and standby servers are configured correctly in the High Availability configuration utility.
7. Ensure that the standby server is configured exactly the same as the active server. Backup the active server database and restore this database onto the standby server.
8. If the contact center uses an Avaya Aura® Application Enablement Services and Avaya Aura® Session Manager, use the Contact Center System Management and Monitoring Component (SMMC) system tray System Information display to examine the status of the High Availability solution.
9. Verify that both the active and standby servers can ping the Trusted IP address.
10. Examine the Windows Event Viewer on the active and standby servers for High Availability, network, or Contact Center-related error messages.

Troubleshooting switchover failure

About this task

Troubleshoot when the active server does not switch over to the standby server. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, the standby applications recognize the failure and start processing contacts.

Procedure

1. Verify that the standby server can shadow the active server.
2. Verify that the switchover check box on both servers is selected.
3. Verify that the standby server is installed exactly the same as the active server. The standby and active servers must have the exact same patch level and the same hard disk drive partitions.
4. Verify that you have installed a Standby Server license to enable High Availability.
5. Verify that the standby server can communicate with the active server by name and IP address.
6. Verify that you can ping the Managed IP address of the active server from the standby server and from a client computer.
7. Verify that the static IP address of the active and standby servers are configured correctly in the High Availability configuration utility.
8. If the contact center uses an Avaya Aura® Application Enablement Services and Avaya Aura® Session Manager, use the Contact Center System Management and Monitoring Component (SMMC) system tray System Information display to examine the status of the High Availability solution.

9. Ensure that the standby server is configured exactly the same as the active server. Backup the active server database and restore this database onto the standby server.
10. Verify that both the active and standby servers can ping the Trusted IP address.
11. Examine the Windows Event Viewer on the active and standby servers for High Availability, network, or Contact Center related error messages.

Troubleshooting when network outages occur in a High Availability Contact Center

About this task

Troubleshoot when a Contact Center component or network link fails.

The High Availability-System Management and Monitoring Component (SMMC) monitors network communications, network latency, and contact center components. If the High Availability Network Timeout threshold value is not suitable for your network then outages can occur. You must configure the High Availability SMMC Network Timeout threshold value high enough to be tolerant of normal network latency, but low enough to be responsive if a network failure occurs. Avaya recommends that you analyze your network performance after running HA for a number of days. Use the Network Analyzer utility to analyze the SMMC logs and verify whether your Network Timeout value is set correctly for your network performance. This procedure shows you how to determine what your current network threshold value is.

Procedure

1. Log on to the High Availability server.
2. Retrieve the Active server SMMC log files from `Avaya\Logs\Common Components\SMMC\CC_SMMC_NM_x.log`, where `x` indicates a running numeric identifier between 1 and 9.
3. Copy the SMMC log files into the same folder as the Network Log Analyzer utility:

   ```
   D:\Avaya\Contact Center\Manager Server\CCSMMC\util
   ```

4. On the Active server, open a command prompt and navigate to the same folder as the Network Analyzer utility.
5. At the command prompt enter:

   ```
   NetworkLogAnalyser.exe CC_SMMC_NM_1.log CC_SMMC_NM_2.log...
   ```

6. The Network Log Analyzer utility processes the SMMC statistical network data in the log files and recommends a Network Timeout value. For example:

   ```
   $> NetworkLogAnalyser.exe CC_SMMC_NM_1.log

   ....

   ....

   ===== OUTAGES PACKET DATA ANALYSIS END ====
   ```

```
Recommendation:
---------------
Network Timeout= 2× Max(Outage_Duration)= 2× 325ms = 650ms
```

While processing the statistical data, the Network Log Analyzer utility also produces a comma-separated file (network-analysis.csv) that can be imported in to Microsoft Excel using the“network-analysis.xlsm” spreadsheet.

7. Open the file `network-analysis.xlsm` using Microsoft Excel and ensure that you have macros turned on. Follow the instructions given in the spreadsheet.
8. From the resulting chart and recommended Network Timeout value, determine what the suitable Network Timeout value for your network is and update accordingly.

Troubleshooting High Availability Avaya Media Server and G450 configuration

About this task

If phone control and speech paths are lost after a HA switchover, verify your G450 Media Gateway configuration.

If your G450 Media Gateway is installed on the same network subnet as your High Availability Linux-based Avaya Media Server cluster, then you must disable ARP Inspection on the G450. If an Avaya Media Server fails, the G450 can then communicate with the other Avaya Media Server in that cluster.

Procedure

On the G450, disable ARP spoofing protection by entering the CLI command: `no ip arp inspection`.

Troubleshooting High Availability Avaya Media Server and G6xx configuration

About this task

If phone control and speech paths are lost after a HA switchover, verify your G6XX Media Gateway network configuration.

In Avaya Aura® Contact Center High Availability solutions that contain High Availability Linux-based Avaya Media Servers and a G6xx Media Gateway, the Avaya Media Servers must be installed in a different network subnet to the G6xx Media Gateway.

Procedure

Verify that the Avaya Media Servers are installed in a different network subnet to the G6xx Media Gateway.

Troubleshooting active server resources

About this task

Avaya Communication Server 1000 resources acquired by the CCMS are not deacquired at the time of a failure, and the login state of voice agents is maintained when the backup CCMS comes online. This means that in the event of a CCMS outage, there is no need for agents to cycle their voice login state. The standby CCMS starts up and shows the correct state of every agent's voice terminal as they were at the time of the active CCMS outage. There is no impact to calls that are in progress between a customer and an agent.

CCMS does not deacquire Avaya Communication Server 1000 resources when stopped by the High Availability utility therefore caution must be exercised when starting a CCMS in a High Availability environment to ensure the Avaya Communication Server 1000 resources are available to it.

CCMS de-acquires Avaya Communication Server 1000 resources when stopped by the System Control and Monitor Utility (SCMU).

Procedure

Ensure the active Contact Center Manager Server has full control privileges over Avaya Communication Server 1000 resources by using the System Control and Monitor Utility (SCMU) to completely stop all CCMS servers in the contact center.

Chapter 18: Avaya Aura platform troubleshooting

Troubleshooting the Avaya Aura® Unified Communications platform must be done to address errors that occur when the Avaya Aura® Contact Center cannot control phone calls or route calls to agents.

Prerequisites for Avaya Aura platform troubleshooting

Procedure

- Ensure that your servers, client computers, and network meet the minimum system requirements. For more information about hardware and network requirements, see *Avaya Aura® Contact Center Fundamentals and Planning* (44400-211).
- Complete the Avaya Aura® Unified Communications platform pre-installation checklist. For more information about the checklist, see *Avaya Aura® Contact Center Installation Checklist* (44400-310).
- Complete the SIP-enabled Contact Center pre-installation checklist. For more information, see *Avaya Aura® Contact Center Installation Checklist* (44400-310).
- Ensure that you have installed Contact Center correctly. For more information about installing Contact Center, see *Avaya Aura® Contact Center Installation* (44400-311).
- Read *Avaya Aura® Contact Center Commissioning* (44400-312).
- Read *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (44400-521).

Troubleshooting Communication Manager stations

About this task

To ensure proper integration and Contact Center control, Avaya Aura® Communication Manager stations (phones) must be configured as follows:

- Restrict Last Appearance must be enabled on all agent stations
- Call Forwarding is not supported on agent stations
- Priority call feature is not support on agent stations

Perform the following checks on each Communication Manager station to be controlled by Contact Center and used as an agent phone.

Procedure

1. Verify **Restrict Last Appearance** is enabled on all agent stations, for example; **Restrict Last Appearance? y**.
2. Verify **IP Softphone** is enabled on all agent stations, for example; **IP SoftPhone? y**.

Troubleshooting treatments when dialing the Contact Center Route Point Address

About this task

Add the Contact Center Manager Server to the list of trusted hosts on the Avaya Aura® Session Manager (SM) server. Add a Contact Center Manager Server (CCMS) routing entry to the SM server. This indicates to SM which host (SIP entity) to send calls to, based on the dialed number. Add contact details for the CCMS routing entry. This configures the SM server to send calls to the CCMS when the calls match the map.

If you dial the Contact Center Route Point Address (RPA) and do not receive any treatments, perform the following checks.

Procedure

1. Verify that the Contact Center Manager Server is a trusted host of the Session Manager (SM) server.
2. Verify that the Session Manager (SM) server has a routing entry to the Contact Center Manager Server.
3. Verify that the Session Manager (SM) server has contact details for the Contact Center Manager Server routing entry.

Troubleshooting routing calls from Contact Center to agents on Communication Manager

About this task

If you cannot route calls from the Contact Center to agents on the Avaya Aura® Communication Manager, perform the following checks.

On the SIP Enablement Services (SES) server, add a route entry to the Communication Manager. The SES re-directs SIP contacts that match the route entry pattern to the Communication Manager.

Add the Contact Center Manager Server to the list of trusted hosts on the SIP Enablement Services (SES) server. SES does not authenticate SIP requests from trusted hosts.

Procedure

1. Verify that there is a routing entry from the SES to the Communication Manager.
2. Verify that the Contact Center Manager Server is a trusted host of the SIP Enablement Services (SES) server.

Troubleshooting when agents cannot log on to Agent Desktop

About this task

If agents cannot log on to Avaya Aura® Agent Desktop, perform the following checks.

Procedure

1. Verify that TR87 is enabled on the Avaya Aura® Application Enablement Services (AES) server.
2. Verify that you imported certificates into the AES server.
3. Ensure that the Contact Center Manager Server is a trusted host on the AES server.
4. Ensure network connectivity is configured between the Avaya Aura® Unified Communications platform, CCMS, and Agent Desktop computers in the network and that all computers can ping each other.
5. Ensure that all Avaya Aura® Unified Communications platform and Contact Center servers can communicate with each other by host name, Fully Qualified Domain Name (FQDN), and IP address. Ensure that they can ping each other.

Chapter 19: Networking troubleshooting

This section describes the procedures required to troubleshoot networking problems in Avaya Aura® Contact Center.

Troubleshooting network connection problems

Before you begin

- Ensure that you have a laptop or PC that is near the server and can be connected directly to the server. In this procedure, the laptop or PC is referred to as the client.
- Ensure that you are using a direct connect (crossover) network cable that connects two PCs to be directly without a hub between them.

About this task

If you test the contact center server subnet and ELAN subnet connection using the ping command, and the test fails, then follow these steps to verify that the server ELAN subnet and contact center server subnet cards are configured and identified correctly.

When Contact Center Manager Server is used with Avaya Communication Server 1000, time changes on the Contact Center Manager Server can cause communication issues on the ELAN subnet. This can cause defaulting calls for short durations and can typically self-recover after a number of minutes. For more information, see Disabling the time synchronization features on the operating system on page 113.

Procedure

1. Resolve the failed ping.
2. Retest the ELAN subnet and contact center server subnet network connection.
3. Disable the time synchronization features on the operating system.

Resolving a failed ping

About this task

If you test the contact center server subnet and ELAN subnet connection using the ping command, and the test fails, then follow these steps to verify that the server ELAN subnet and contact center server subnet cards are configured and identified correctly.

Procedure

1. Plug the crossover network cable into the network card in the client.
2. Plug the other end into the ELAN subnet card in the server.
3. If you must restore the IP address information of the client after this procedure, then record the TCP/IP address, subnet mask, and gateway of the client.
4. Configure the client with an IP address that is part of the same subnet as the IP address assigned to the ELAN subnet card. For example, if the server ELAN subnet card has the IP address 1.1.1.1, then assign the client an IP address of 1.1.1.2.
5. Set the client PC to have an subnet mask of 255.0.0.0. Leave the gateway blank.
6. Open an MS-DOS prompt window on the client and try to ping the server ELAN subnet card. For example, if the server ELAN subnet card has the IP address 1.1.1.1, then type `ping 1.1.1.1` and press `Enter`.

   If the ping test succeeds, then you know that you have correctly identified the ELAN subnet card in the network control panel. The other network card, if present, must be the contact center server subnet card.
7. From the server, repeat the steps described in the procedure “Retesting the ELAN subnet and contact center server subnet network connection.” If the test fails, then verify that the network is set up correctly

Retesting the ELAN subnet and contact center server subnet network connection

About this task

If you test the contact center server subnet and ELAN subnet connection using the ping command, and the test fails, then follow these steps to verify that the server ELAN subnet and contact center server subnet cards are configured and identified correctly.

Procedure

1. Ensure you are logged on to the server as Administrator.
2. From the **Start** menu, choose **All Programs** > **Accessories** > **Command Prompt**.

3. In the Command Prompt window, type `ping` followed by the ELAN subnet IP address for the PABX, and then press `Enter`. For example, enter `ping 12.38.3.8`

   The display indicates whether the ping was successful. If you do not receive a successful ping message, then no connection was made.

4. To test the contact center server subnet card, type `ping` followed by the contact center server subnet IP address of another PC on the contact center server subnet, and then press `Enter`. For example, enter `ping 47.2.13.9`

   The display indicates whether the ping was successful. If you do not receive a successful ping message, then no connection was made.

5. Type `exit`, and then press `Enter` to close the Command Prompt window

Disabling the time synchronization features on the operating system

About this task

When Contact Center Manager Server is used in the Avaya Communication Server 1000 environment you must disable all time synchronization features of the operating system to avoid potential call processing outages because time synchronization between Contact Center Manager Server and Avaya Communication Server 1000 and not using time modification features of the operating system such as Time servers of daylight savings configuration.

If you disable the Date and Time features after you disable the Windows Time service, the Startup type for the Windows Time service is set to Automatic.

Procedure

1. Choose **Start** > **Control Panel** > **Clock** > **Language** > **Region**.
2. In the **Date and Time** section, click **Change the time zone**.
3. In the Date and Time dialog box, click **Change time zone**.
4. Clear the **Automatically adjust clock for Daylight Saving Time** check box.
5. Click **OK**.
6. Click the **Internet Time** tab.
7. Click **Change settings**.
8. Clear the **Synchronize with an Internet time server** check box.
9. Click **OK**.
10. Click **Apply** to save your changes.
11. Click **OK**.

Troubleshooting network connectivity

About this task

Troubleshoot network connectivity errors between the components of the Contact Center suite by reviewing error logs, then determining the appropriate solution to the network connectivity error.

In the CCT_Server_0.log file, various errors indicate that the Contact Management Framework is not responding to requests from Communication Control Toolkit clients, and that there are problems with the network connectivity for all of the Contact Center servers. If you find the following out-of service text in CCT_Server_0.log, the error indicates that the connection between Contact Center Multimedia and Contact Center Manager Server is out of service due to network issues.

[Peer] Service Provider Status Change Event - Provider: CCMM, Status: MasterApplicationFailure

[ActiveProvider CCMM] Service provider has gone out-of-service

[Peer] Service Provider Status Change Event - Provider: ContactManager, Status: MasterApplicationFailure

[ContactManager] Service provider has gone out-ofservice

You can also determine if there are network problems on the site by examining the following files for the text java.net.SocketExemption:

- On the Contact Center Manager Server, review `D:\Avaya\Contact Center\Common Components\CMF\logs\OAMContainer0.log`.
- On the Communication Control Toolkit server, review `D:\Avaya\Contact Center\Common Components\CMF\logs\ClientContainer.log`.
- On the Communication Control Toolkit server, review `D:\Avaya\Contact Center\Common Components\CMF\logs\SPContainer.log`.

Procedure

1. Check the network cable for faults. Cable faults are often difficult to identify and can be intermittent, therefore replacing the faulty cable with a known good cable is the best solution.
2. Check the network card speed and duplex settings. Communication Control Toolkit to Contact Center Manager Server settings must match the required PABX and hub settings, and be in the same network segment. Also, Contact Center Manager Server and the PABX settings must match the required PABX and hub settings, and be in the same network segment.
3. Check the physical network card for faults.
4. Check the network hub. Check both hardware and software (if applicable) problems in your hub.
5. If your hub is a switched hub, ensure that a virtual LAN separation is not present at a hardware or software level. If a virtual LAN separation is present, the performance of the connection between Communication Control Toolkit and Contact Center Manager Server is minimal.
6. Ensure the ability for Windows to turn off the network card to save power is disabled. Windows Server 2008 has a power management setting for network cards.

7. Ensure the network card has the latest driver software.

Troubleshooting loss of IP connectivity between NCC and a CCMS local node

About this task

A local node can lose IP connectivity with Network Control Center (NCC), if there is a change in your corporate network topology or routing policies. Loss of IP connectivity between NCC and the local node can occur if the local node was installed on a previous release of Avaya Aura® Contact Center and subsequently upgraded to the most recent release of Avaya Aura® Contact Center. In earlier releases of Avaya Aura® Contact Center, when the administrator added the server to the Avaya Aura® Contact Center network, NCC created a persistent IP route on the local node.

To clear the persistent route, remove the node from NCC and run the Server Configuration utility on the local node.

Procedure

1. Remove the local node from NCC.
2. Log on to the local node server.
3. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
4. Click **Apply All**.
5. Add the local node to NCC again.

Chapter 20: Contact Center Manager Administration troubleshooting

This section describes procedures required to address various problems relating to Contact Center Manager Administration, including:

- Installation or upgrade problems
- Communication problems between CCMA and CCMS
- General CCMA problems
- Client PC problems
- Real-time Statistics Multicast (RSM) problems
- Real-Time Reporting problems
- Historical reporting problems
- Configuration Tool problems
- Access and Partition Management problems
- Agent Desktop Display problems

Prerequisites for troubleshooting Contact Center Manager Administration

Procedure

- Ensure that you have downloaded the latest Service Packs for both Contact Center Manager Server and Contact Center Manager Administration. You can download the latest patches or documentation from www.avaya.com/support.
- Ensure that you check the Windows Event Viewer log and note any relevant information related to the problem you are handling. You might need this to resolve the problem, or to communicate information to Avaya support.
- Ensure that you have installed an Avaya-supported remote access tool on the Contact Center Manager Administration server.

Logging on problems due to AD-LDS password encryption error

About this task

Troubleshoot when you receive a failed to login message when attempting to log on to Contact Center Manager Administration.

If, during Contact Center Manager Administration installation, AD-LDS installation failed and error messages occurred following the iceAdmin password prompt, this can indicate that the EncryptPasswordForCCMAUsers setting is set to restrict accessibility only to the user account that created the certificate during installation.

To address this problem, you need to change the policy setting under the Security options on the Contact Center Manager Administration server and provide access to the RSA Machine Keys to all users in the administrators group.

Procedure

1. Review the certificate created during installation of the Contact Center Manager Administration in `C:\Documents and Settings\All Users\Application Data \Microsoft\Crypto\RSA\MachineKeys`.
2. Under the **Security** options, set the local policy for Default owner for objects created by members of the administrator group to all members of the administrator group.
3. Save the certificate.
4. Uninstall and reinstall Contact Center Manager Administration.

Logging on problems result in computer requires restart error message

About this task

Troubleshoot when you attempt to log on to Contact Center Manager Administration and you receive an error message prompting you to restart the computer.

This problem can be caused when the browser tries to download a new version of the HRCtrl ActiveX control that is in use or any control that has an existing version installed which is different than the version attempting to be downloaded.

Procedure

1. Click **Cancel** to reject the request to restart the computer.
2. Close all Internet Explorer browser windows.
3. Open a new Internet Explorer browser window.

4. Go to the same Contact Center Manager Administration URL that resulted in the prompt to restart the computer.

   The control downloads and no prompt to restart the computer appears.

Troubleshooting when Citrix server performance is slow

Before you begin

- Review *Avaya Aura® Contact Center Fundamentals and Planning* (44400-211).

About this task

Troubleshoot when you use a Citrix server and the server performance and speed are slow.

This problem can be caused by numerous agents launching Agent Desktop Display (ADD). Each Agent Desktop Display uses 20 MB of RAM. If the server is performing slowly, you might need to increase the amount of RAM available on the Citrix server.

Procedure

1. Determine the RAM requirements for the Citrix server.
2. Upgrade the RAM available on the Citrix server.

Refreshing servers

Before you begin

- Ensure that you have logon privileges as an administrator, who has permissions to add, edit, delete and refresh servers in Contact Center Manager Server.
- Ensure that you determine whether you need to refresh all servers in the system tree or just a single server in the system tree, based on the reasons described below.

About this task

Troubleshoot if CCMA does not function correctly after upgrading from NES Symposium Web Client (SWC) or after making a change to the Contact Center Manager Server, such as performing an upgrade, installing or uninstalling a service pack, receiving a new license file, or making a change to a standby CCMS. For example, if pages and tabs load incorrectly, new components and features are unavailable, or scripting errors occur, you might need to refresh your Contact Center Manager Servers. To troubleshoot these errors, you need to refresh one or all servers in the system tree.

Although Contact Center Manager Administration automatically refreshes all servers every 12 hours, Avaya recommends that you manually refresh servers following an upgrade, to ensure that Contact Center Manager Administration functions correctly.

When you refresh a server, you refresh Contact Center Manager Server data associated with that server in Active Directory Lightweight Directory Services (AD-LDS), such as the release number, feature list, and networking information.

If you change the password of sysadmin in the Server Utility, you must also change the password in that server.

Use the Refresh All Servers option to refresh all servers at the same time when:

- You upgrade from a previous version of Contact Center Manager Administration.
- You change the Contact Center Manager Administration server to connect to a standby Contact Center Manager Server.
- There is a feature change to the Contact Center Manager Server. This is because the change is not reflected in the browsers until all browsers using CCMA are refreshed.

Use the Refresh Server option to refresh only the Contact Center Manager Server that incurred a change when:

- You upgrade the Contact Center Manager Server.
- You install or uninstall a Service Pack (SP) on the Contact Center Manager Server.
- A new license file is issued and accepted by Contact Center Manager Server, or you connect to a different License Manager server (that is, a new or standby License Manager server).

Procedure

1. Log on to Contact Center Manager Administration.
2. Select **Configuration**.
3. If you want to refresh all servers in the system tree:
   - On the menu bar, choose **Server** > **Refresh All Servers**.
4. If you want to refresh a single server in the system tree:
   - On the system tree, click the server that you want to refresh.
   - On the menu, choose **Server** > **Refresh All Servers**.
5. Click **Yes**.
6. Click **Yes**.

   The system refreshes the selected servers. A message appears in the information bar at the bottom of the screen that lists the servers that successfully refreshed and the servers that did not refresh. An entry specifying the servers that were successfully refreshed also appears in the Audit Trail.

Downloading ActiveX controls and CCMA starts slowly

About this task

Troubleshoot if downloading ActiveX controls causes the Contact Center Manager Administration web client to load slowly. This can occur when the client PC cannot contact the Verisign Web site. The ActiveX controls are digitally signed and the system attempts to verify that the digital signature is valid by accessing the Verisign Web site. If verification is not possible, the attempt times out and the download of the ActiveX controls proceeds normally.

The ActiveX controls can be distributed to a client PC during installation, using the ActiveXControl MSI package.

Procedure

When starting Contact Center Manager Administration, if a delay of longer than a minute occurs during the download of ActiveX controls, contact Avaya Technical Support.

Solving CCMA replication errors related to problems with AD-LDS

About this task

Troubleshoot if Contact Center Manager Administration replication fails and if you selected Enable Active Directory - Lightweight Directory Services (AD-LDS) replication during installation but did not provide the name of the AD-LDS instance, for example NES Symposium Web Client (SWC), for replication during AD-LDS setup.

AD-LDS is installed during the installation of Contact Center Manager Administration. AD-LDS is not removed during the uninstallation of Contact Center Manager Administration because AD-LDS is a windows component that is incorporated into the operating system and uninstallation of AD-LDS can cause the operating system to fail.

The DVD Controller manages all contact center uninstallation processes. The AD-LDS Instance, CCMA Database, is removed from the system during the uninstallation of Contact Center Manager Administration. However, the AD-LDS instance is not removed from the system and Contact Center Manager Administration replication does not work if you do not provide the name of the AD-LDS instance for replication during AD-LDS setup.

Procedure

If Contact Center Manager Administration replication fails and if you selected Enable AD-LDS replication during installation but did not provide the name of the AD-LDS instance, for example NES Symposium Web Client (SWC), for replication during AD-LDS setup, manually uninstall AD-LDS.

Removing the AD-LDS instance on CCMA on a standby server in a replication environment

About this task

Use this procedure to remove the AD-LDS instance from CCMA on a standby server if CCMA is not configured correctly or if AD-LDS Replication is not functioning. After removing the AD-LDS instance, restore AD-LDS. For more information on the AD-LDS restoration process, see Restoring the AD-LDS instance in a domain on CCMA on a standby server in a replication enviroment on

page 123 or Restoring the AD-LDS instance in a workgroup on CCMA on a standby server in a replication enviroment on page 137.

CCMA on a standby server (secondary AD-LDS instance) is a replica of CCMA on an active server (primary AD-LDS instance). Therefore, removing and restoring the AD-LDS instance on the secondary server does not result in any data loss.

Note:

You cannot perform this procedure on CCMA on the active server (primary AD-LDS instance) as the DVD controller applies the primary AD-LDS instance.

Procedure

1. Remove the existing AD-LDS instance from the standby server.
   a. Click **Start** > **Control Panel** > **Programs**.
   b. Click **Programs and Features**.
   c. Select **AD LDS Instance SymposiumWC** from the list of installed programs.
   d. Click **Uninstall**.

      The system displays the Active Directory Lightweight Directory Services Removal Wizard dialog box.
   e. Click **Yes** to continue.

      The system removes the AD-LDS instance from the standby server.
2. Remove the configuration of the standby server from the primary server instance.
   a. On the primary server, click **Administrator Tools** > **ADSI Edit**.

      The system displays the ADSI Edit dialog box.
   b. From the **Action** menu, select **Connect to**.

      The system displays the Connection Settings dialog box.
   c. In the Connection Point section, select **Select a well known Naming Context**.
   d. From the **Select a well known Naming Context** drop-down list, select **Configuration**.
   e. In the Computer section, select **Select or type a domain or server**.
   f. In the **Select or type a domain or server** drop-down list, enter `localhost:389`.

      Note:

      The default port number is 389. This port is configured during DVD installation and might be different on your system. Ensure that the port number matches the port number used during the DVD installation.
   g. Click **OK**.

      Using the ASDI Edit dialog box, you can browse to all servers that are associated with this replication set. The ASDI Edit dialog box contains an entry for active and standby servers and also lists any unused old servers or any Remote Geographic Node (RGN) servers that are available.

h. In the ASDI Edit dialog box, expand **Configuration** > **CN=Configuration container** > **CN=Sites**.

i. Expand **CN=Default-First-Site-Name**.

j. Expand **CN=Servers** to see the list of servers in the replication configuration set.

k. Under **CN=Servers**, select CCMA on the standby server that you want to remove.

The system displays the servers in the following format:

```
CN = <OldStandbyCCMAServerName>$SymposiumWC
```

l. Double-click the server to view the properties of the server that you have to remove.

m. In the Properties window, check the **dNSHostName** line to ensure that you have selected the correct server.

n. Right-click the `CN=<OldStandbyCCMAServerName>$SymposiumWC` container and select **Delete**.

Caution:

Ensure that you do not delete the active server entry from the list of server objects.

The system displays an ADSIEdit dialog box.

o. Click **Yes** to continue.

The system deletes the old standby server entry from the primary server.

3. On the secondary server, run the AD-LDS setup wizard.

a. Click **Start** > **Administrative Tools** > **Active Directory Lightweight Directory Services Setup Wizard**.

b. Restore the AD-LDS instance on CCMA on the standby server.

For more information on the AD-LDS restoration process, see Restoring the AD-LDS instance in a domain on CCMA on a standby server in a replication enviroment on page 123 or Restoring the AD-LDS instance in a workgroup on CCMA on a standby server in a replication enviroment on page 137.

Ensure that the port numbers specified in the wizard match the port numbers specified during the DVD installation.

To check the port numbers, run the following command on the primary server:

```
C:\Windows\ADAM>dsdbutil
dsdbutil: list instances
```

Restoring the AD-LDS instance in a domain on CCMA on a standby server in a replication enviroment

About this task

Use this procedure to restore the AD-LDS instance in a domain, after removing the AD-LDS on CCMA on a standby server. For more information, see Removing the AD-LDS instance on CCMA on a standby server in a replication environment on page 120.

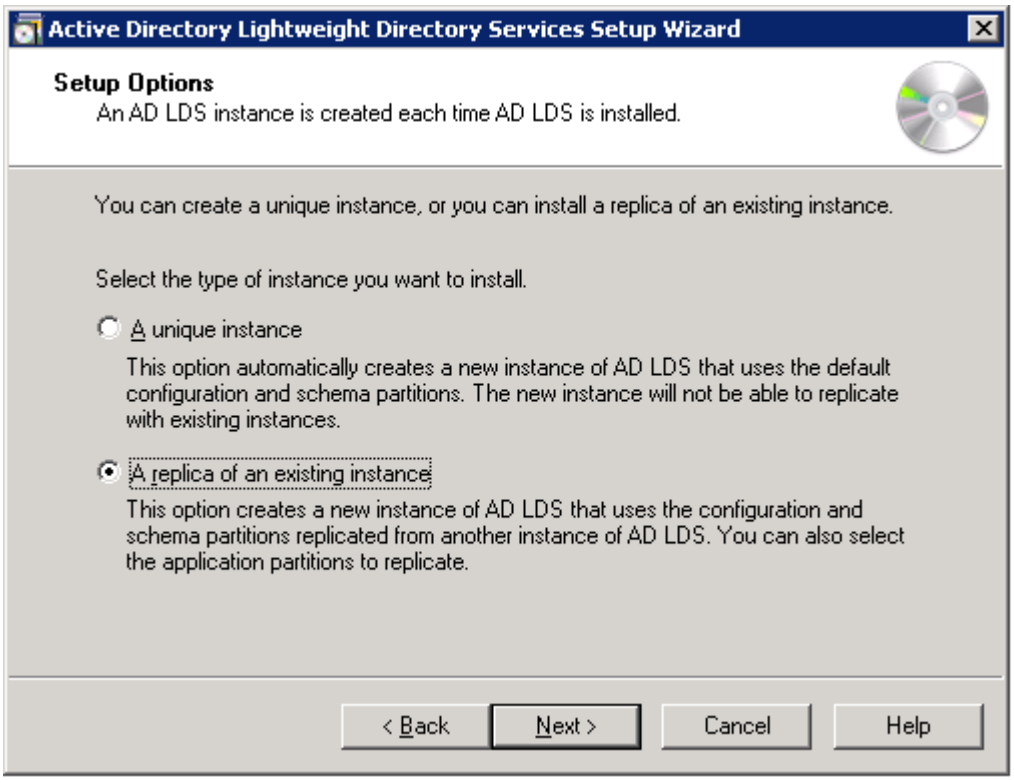
Procedure

1. Click **Start** > **Administrative Tools** > **Active Directory Lightweight Directory Services Setup Wizard**.

   The system displays the Active Directory Lightweight Directory Services Setup Wizard screen.

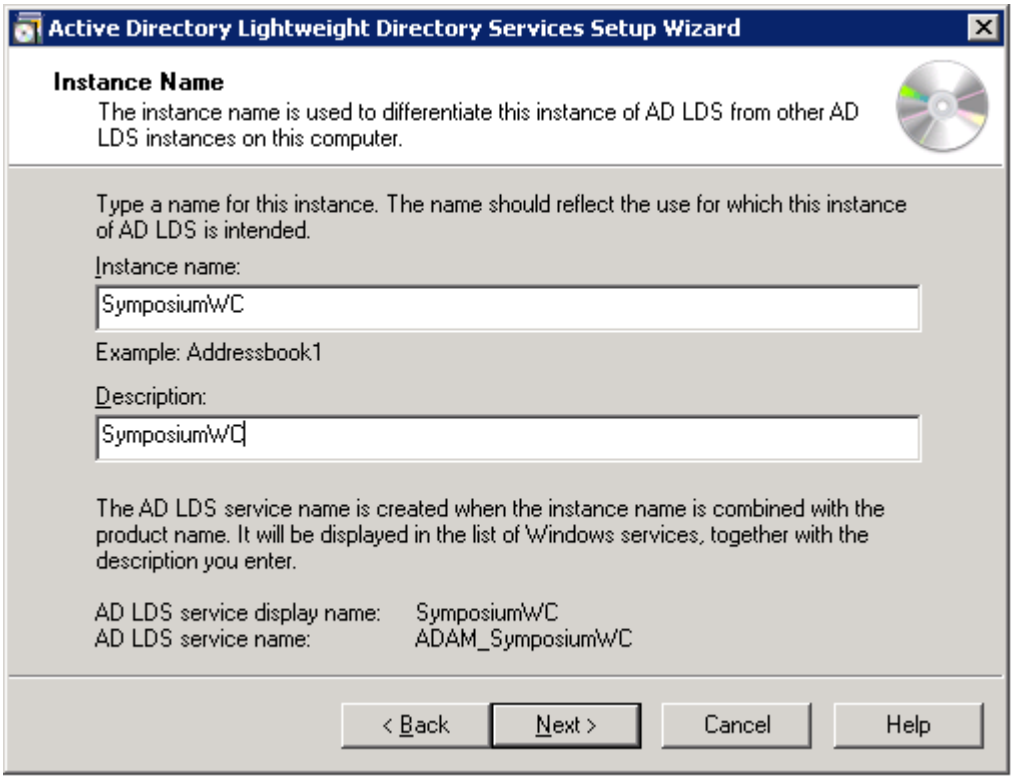
2. Click **Next**.

3. In the Setup Options dialog box, select **A replica of an existing instance**.



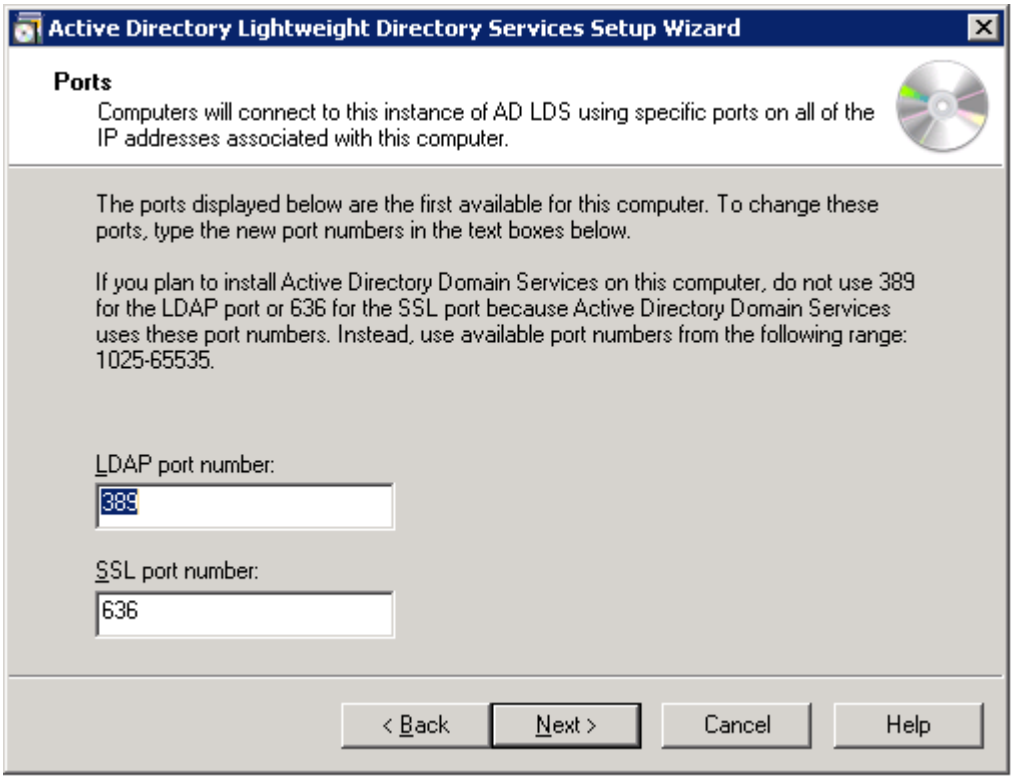
4. Click **Next**.
5. In the Instance Name dialog box, in the **Instance name** box, type `SymposiumWC`.

   SymposiumWC is the default AD-LDS instance name.



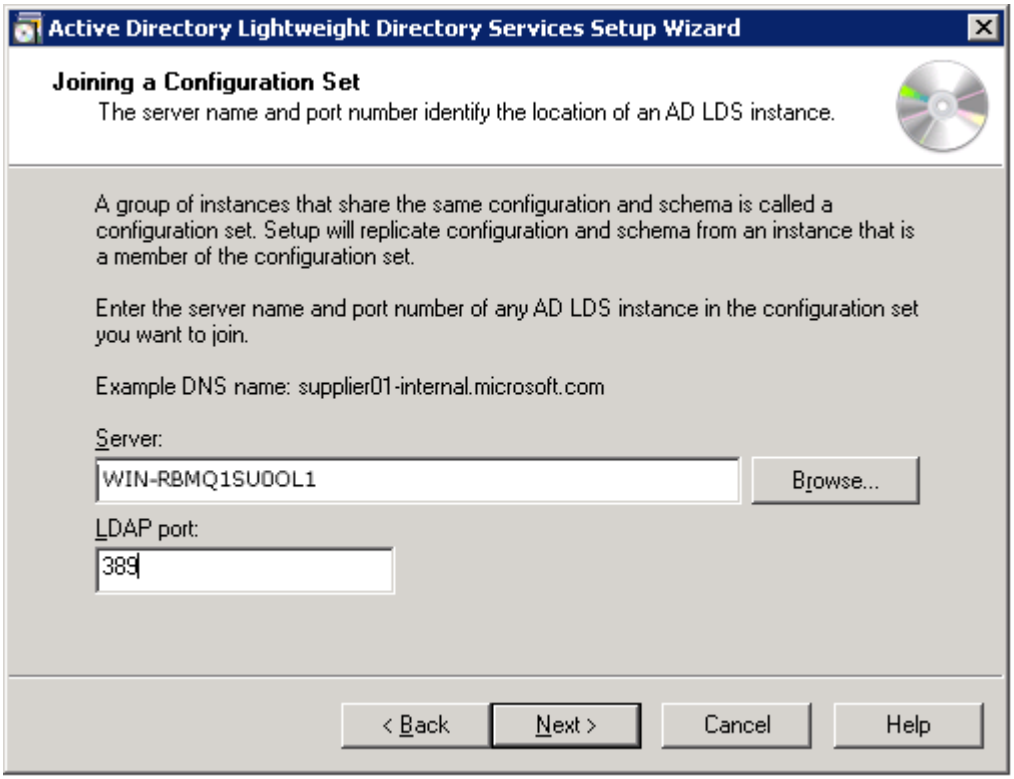
6. In the **Description** box, type `SymposiumWC`.
7. Click **Next**.

8. In the Ports dialog box, if no other applications use the ports, accept the default values in the **LDAP port number** and **SSL port number** boxes.



9. Click **Next**.
10. In the Joining a Configuration Set dialog box, in the **Server** box, type the FQDN name of the primary Voice and Multimedia Contact Server that you want to replicate.

    An example of entering the primary Voice and Multimedia Contact Server name:



11. On the Joining a Configuration Set window, in the **LDAP Port** box, type the port number on the AD-LDS instance on the primary Voice and Multimedia Contact Server.

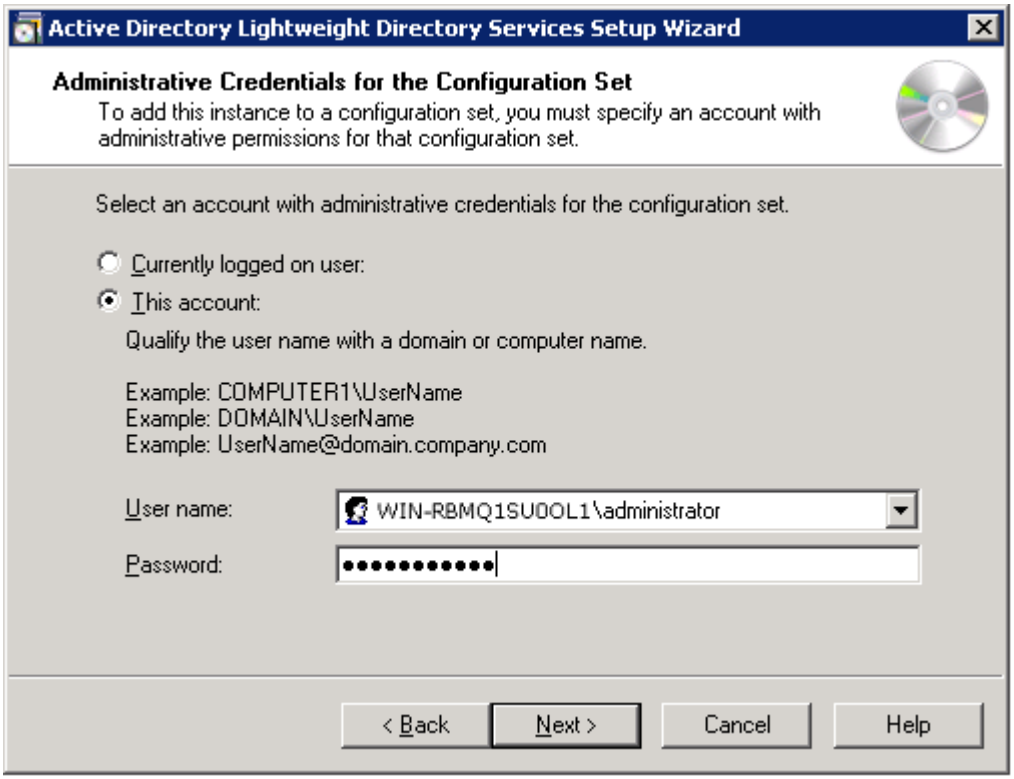
    The default is port number 389.

12. Click **Next**.
13. In the Administrative Credentials for the Configuration Set window, select **This account**.
14. In the **User name** box, type the server name of the primary Voice and Multimedia Contact Server followed by its Administrator name in the format `<primary Voice and Multimedia Contact Server name>\Administrator`.

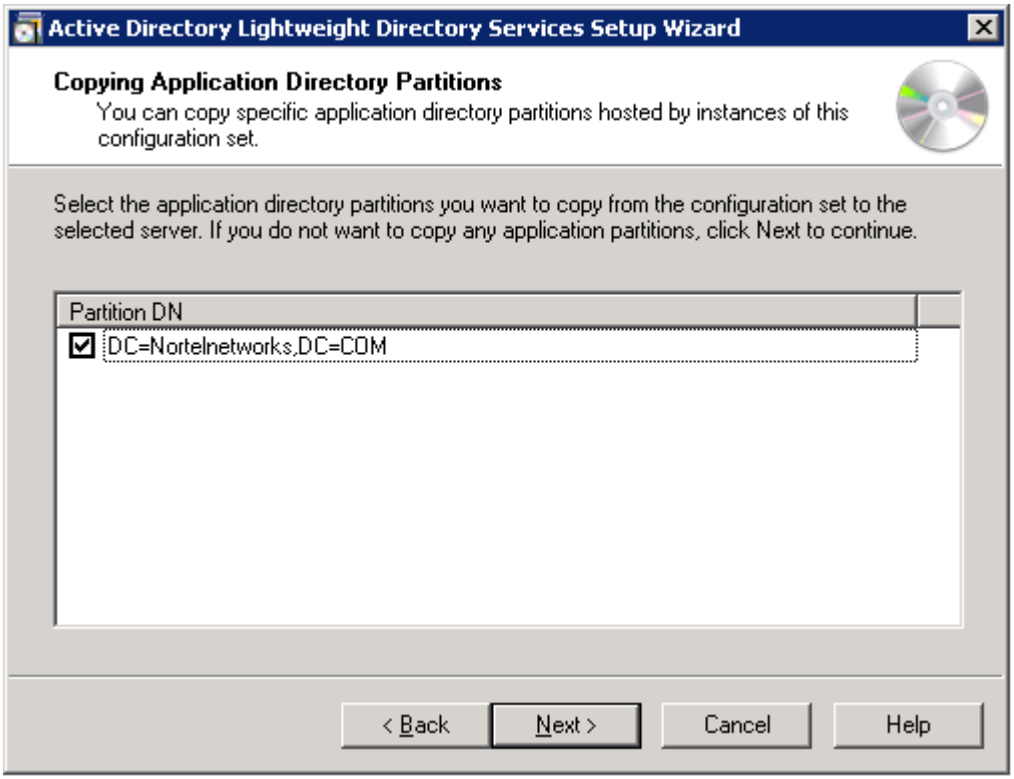
    For example, enter `WIN-RBMQ1SU0OL1\Administrator`.

    If you have created another administrator account for Contact Center, then enter the details (name and password) of that primary Voice and Multimedia Contact Server server administrator account. Your administrator account must have full administrative privileges.

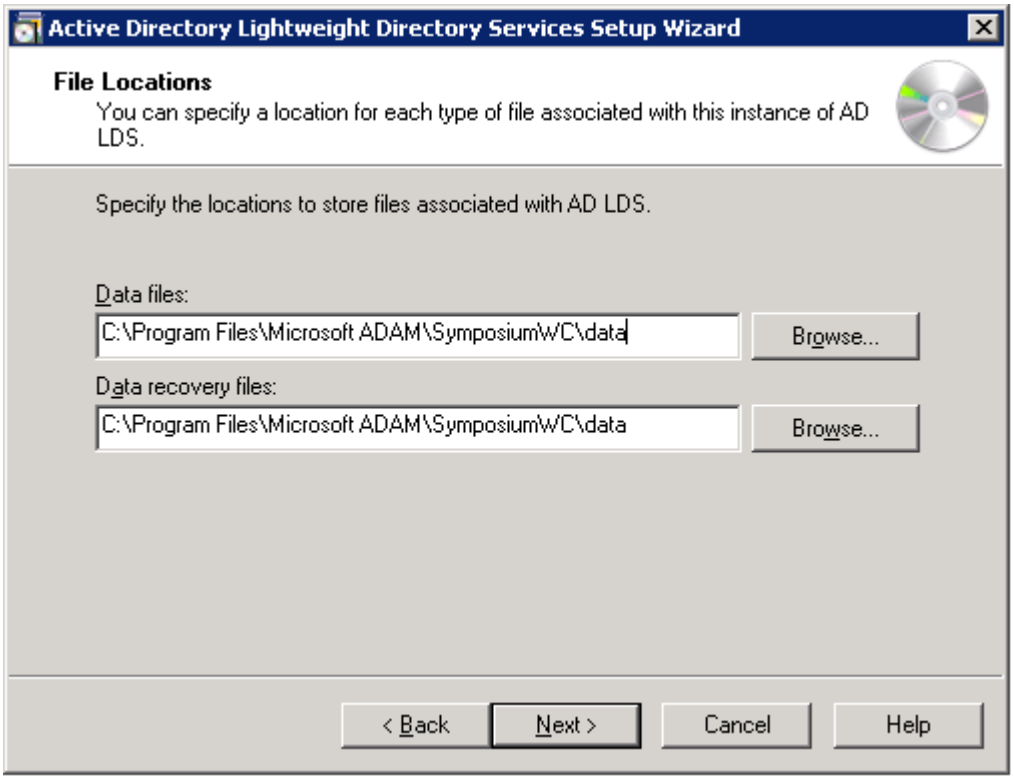
    An example of entering the administrative credentials:



15. In the **Password** box, type the password for this user account.
16. Click **Next**.
17. In the Copying Application Directory Partitions dialog box, in the **Partition DN** list, select **DC=Nortelnetworks,DC=COM**.

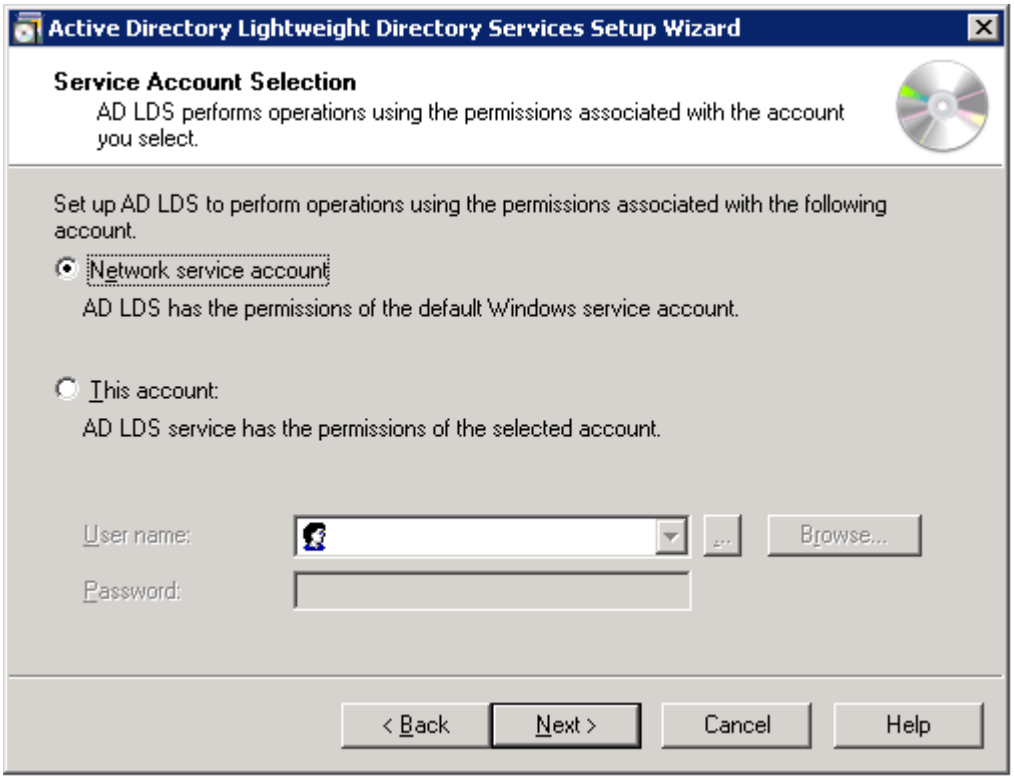


18. Click **Next**.
19. In the File Location dialog box, accept the default values.

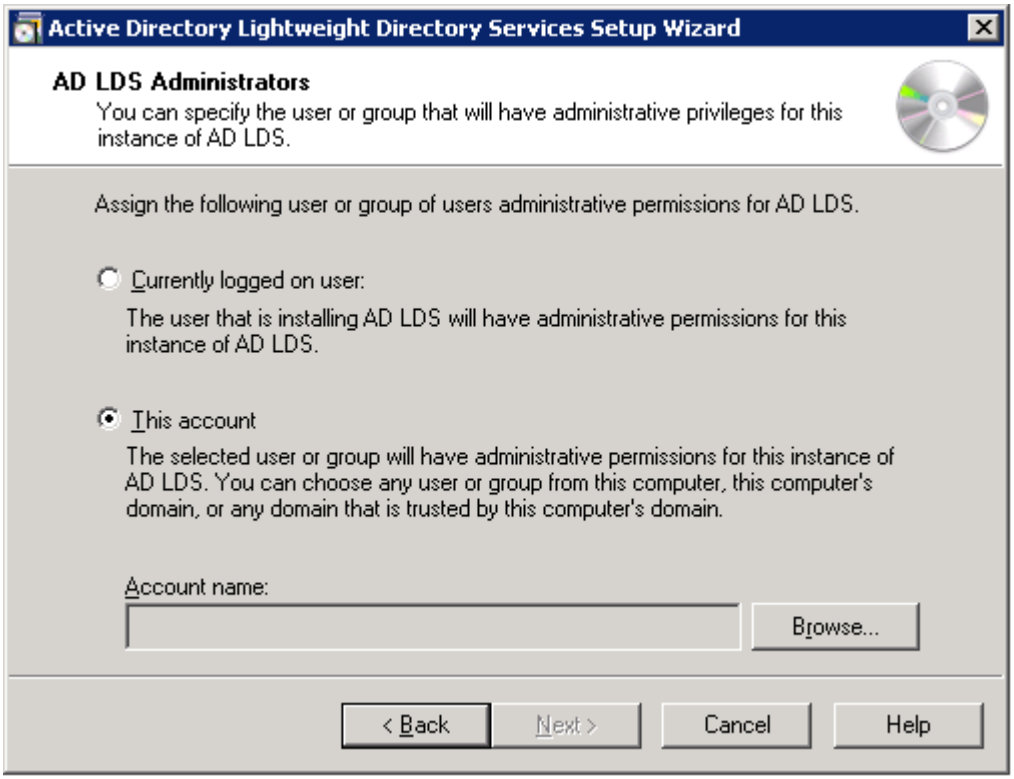


20. Click **Next**.
21. In the Service Account Selection dialog box, select **Network service account**.

    An example of using a domain and selecting Network service account:

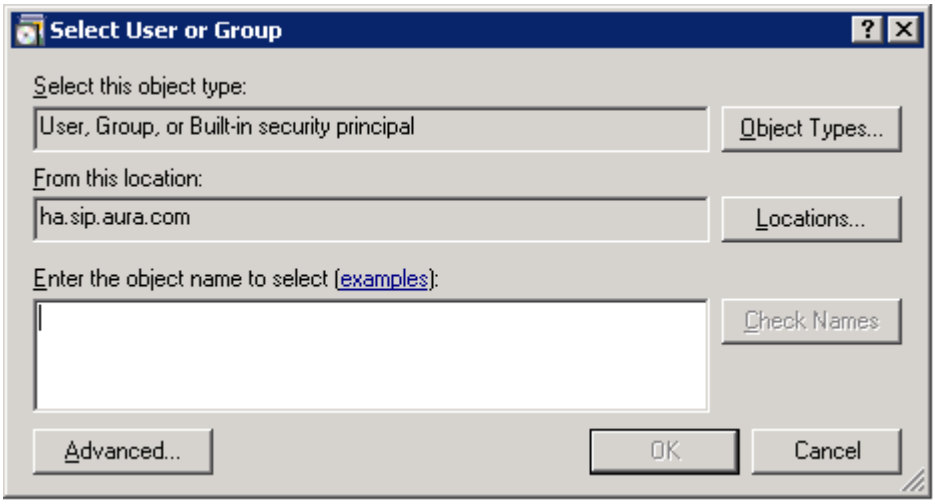


22. Click **Next**.
23. In the AD LDS Administrators dialog box, select **This account**.

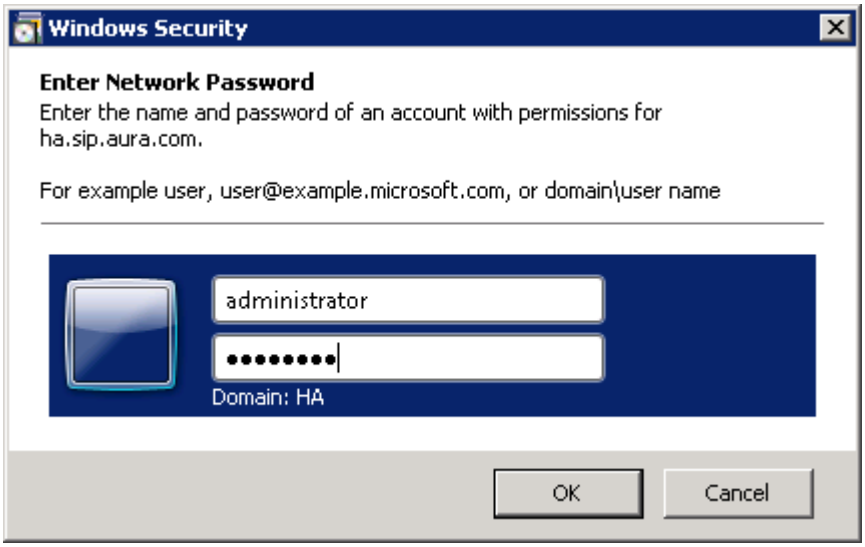


24. Click **Browse** to locate the CCMA AD-LDS replication account.

    The system displays the Select User or Group dialog box. Ensure that the location is the local domain.

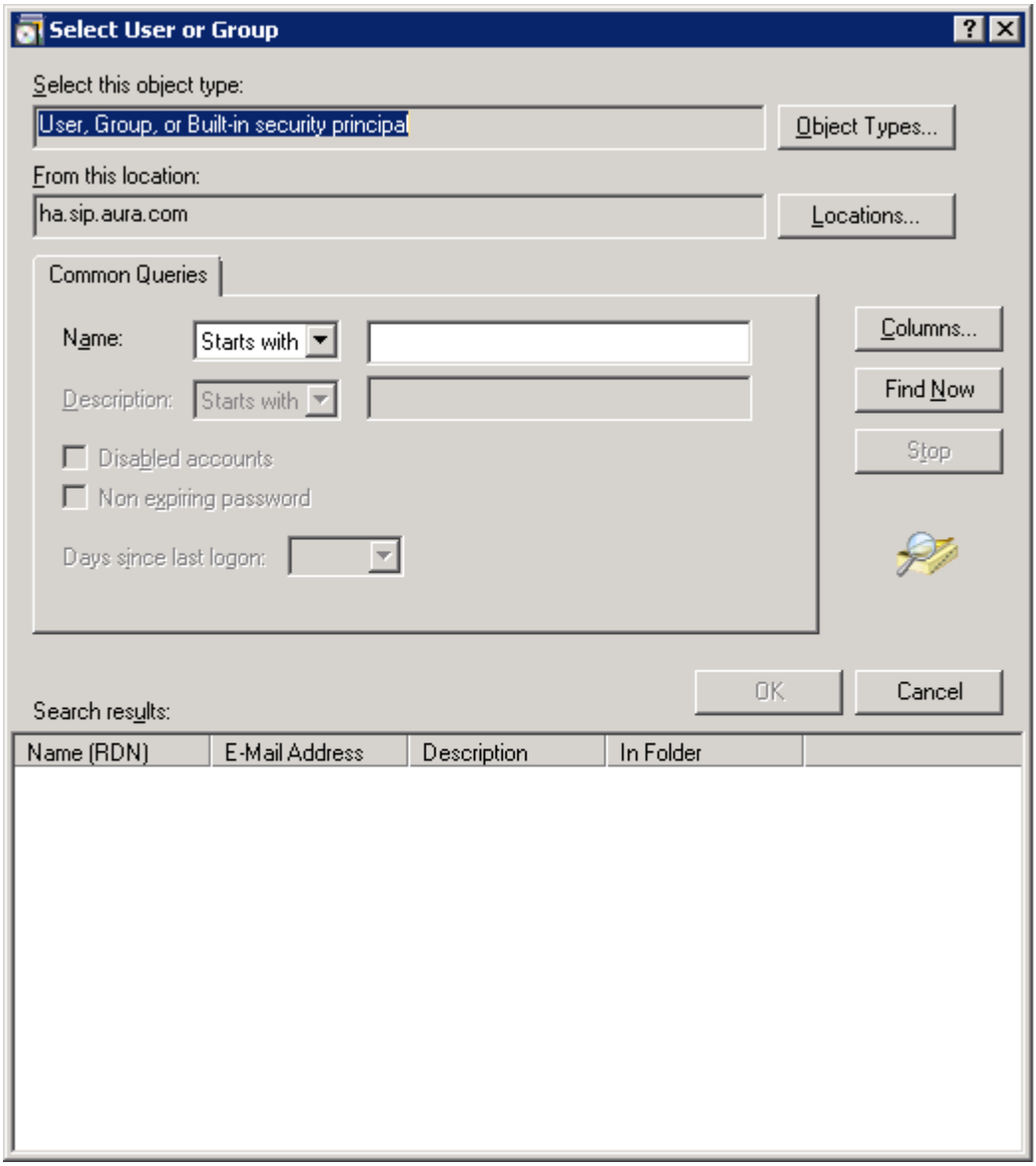


25. In the Select User or Group dialog box, click **Advanced**.
26. In the Windows Security dialog box, type a logon name and password of an account with permissions to access your domain.



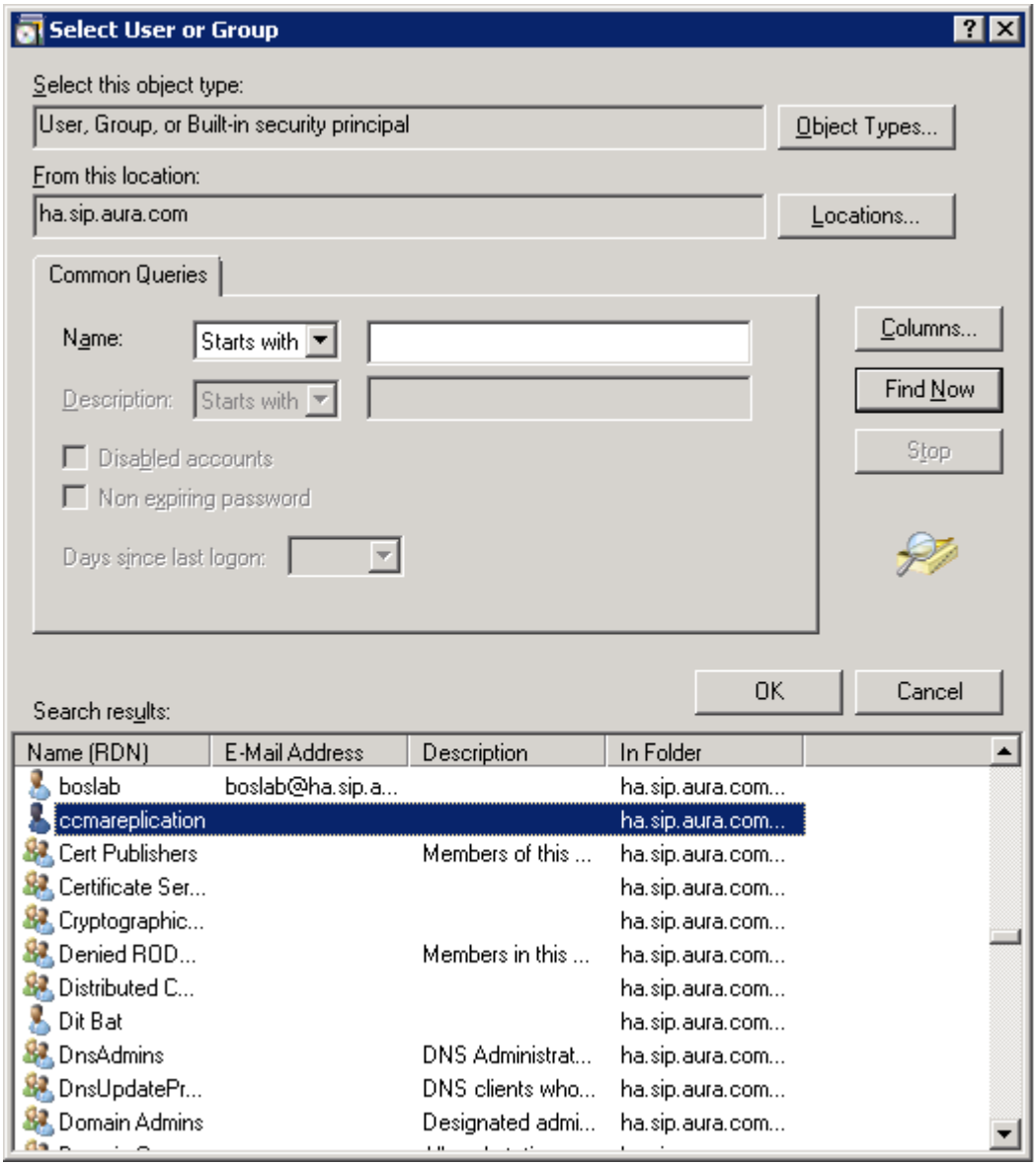
27. Click **OK**.

    The system displays the advanced Select User or Group dialog box.



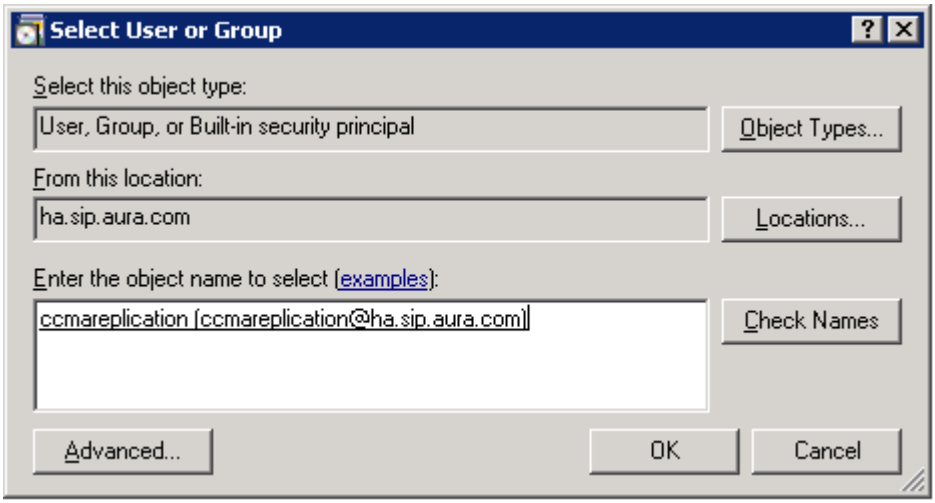
28. In the advanced Select User or Group dialog box, click **Find Now**.
29. From the **Search results** list, select the CCMA replication account.

    An example of selecting a domain CCMA replication account:



30. In the advanced Select User or Group dialog box, click **OK**.

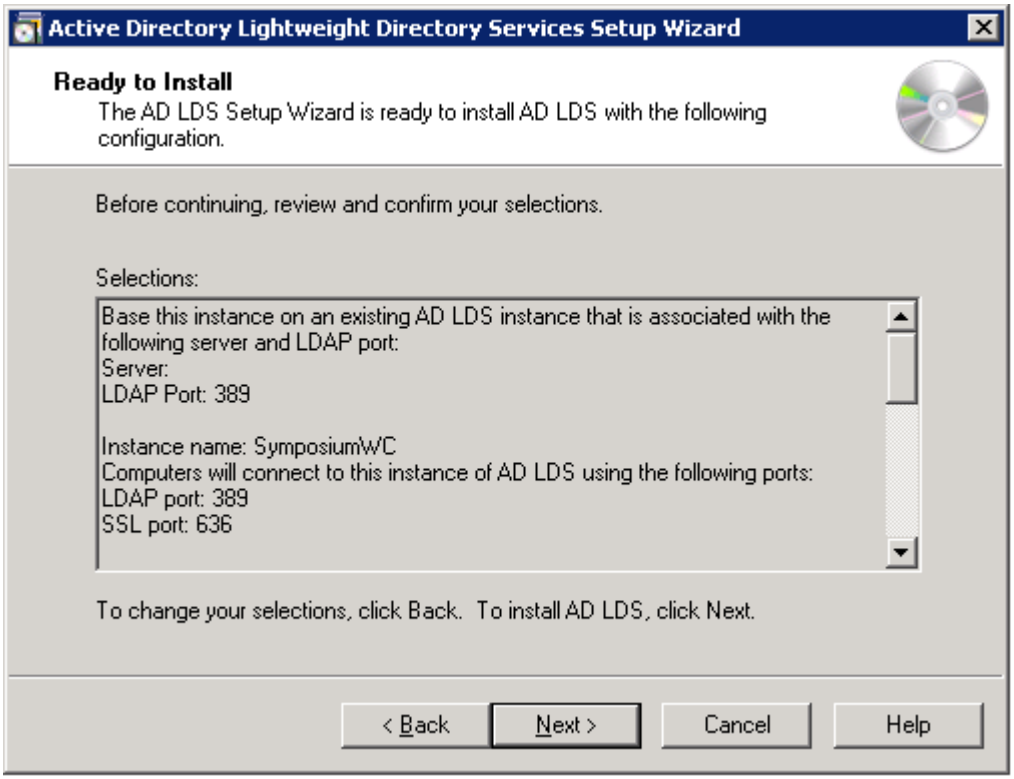
    An example of selecting a CCMA replication account:



31. In the Select User or Group dialog box, click **OK**.

    An example of selecting a domain CCMA replication account:

32. Click **Next**.



33. Confirm the installation components, and click **Next**.
34. After the installation is complete, click **Finish**.
35. If prompted, restart the server.

Restoring the AD-LDS instance in a workgroup on CCMA on a standby server in a replication enviroment

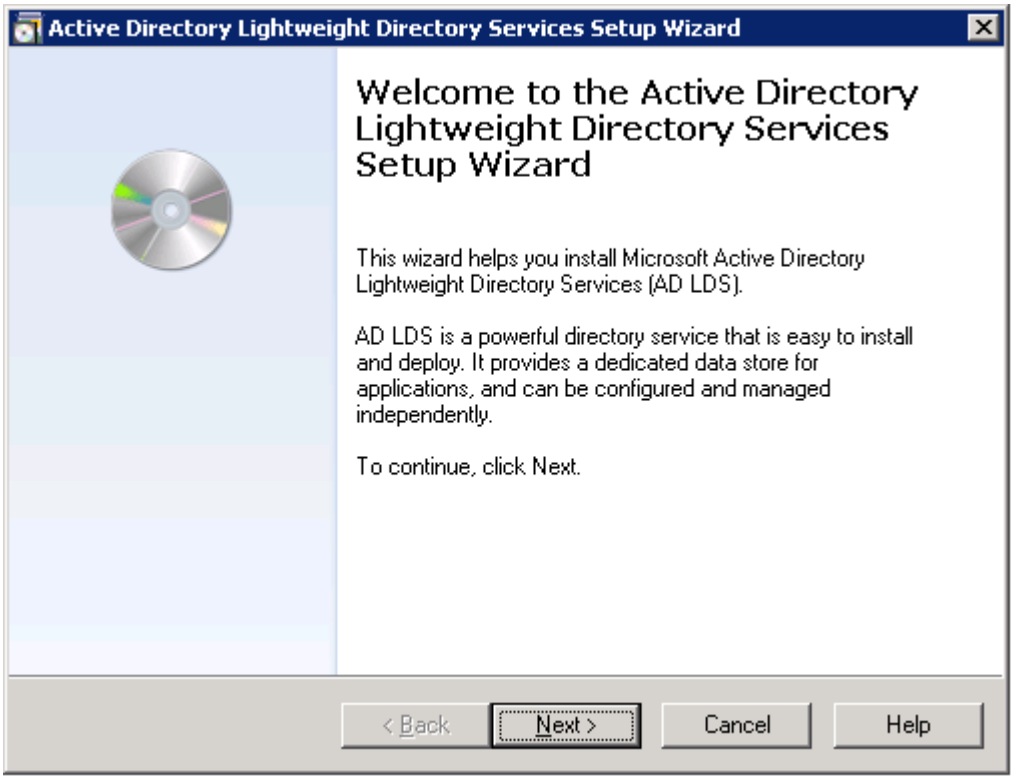
About this task

Use this procedure to restore the AD-LDS instance in a workgroup, after removing the AD-LDS on CCMA on a standby server. For more information, see Removing the AD-LDS instance on CCMA on a standby server in a replication environment on page 120.

Procedure

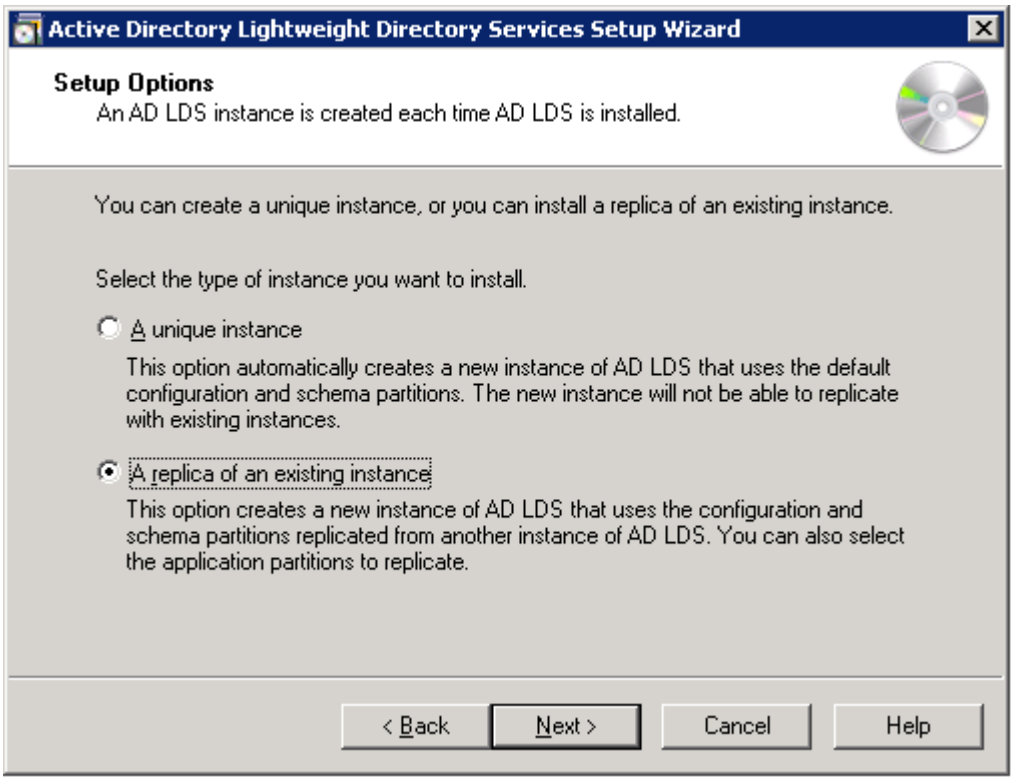
1. Click **Start** > **Administrative Tools** > **Active Directory Lightweight Directory Services Setup Wizard**.

   The system displays the Active Directory Lightweight Directory Services Setup Wizard screen.


Active Directory Lightweight Directory Services Setup Wizard
Welcome to the Active Directory Lightweight Directory Services Setup Wizard
This wizard helps you install Microsoft Active Directory Lightweight Directory Services (AD LDS).
AD LDS is a powerful directory service that is easy to install and deploy. It provides a dedicated data store for applications, and can be configured and managed independently.
To continue, click Next.
< Back
Next >
Cancel
Help

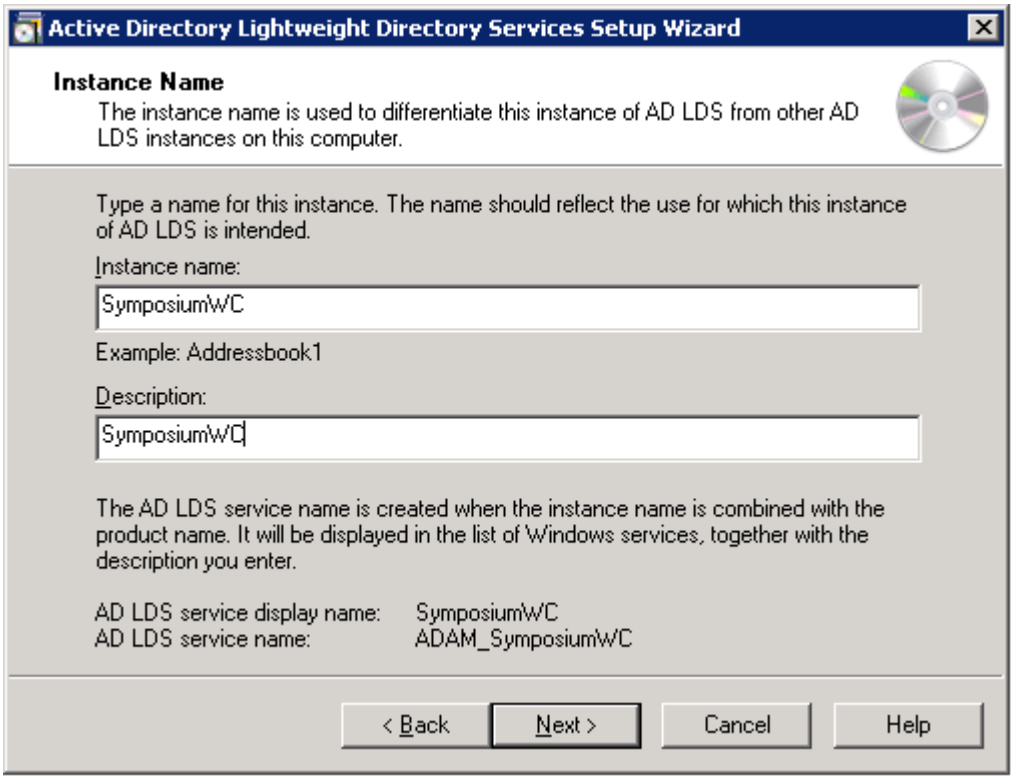
2. Click **Next**.

3. In the Setup Options dialog box, select **A replica of an existing instance**.



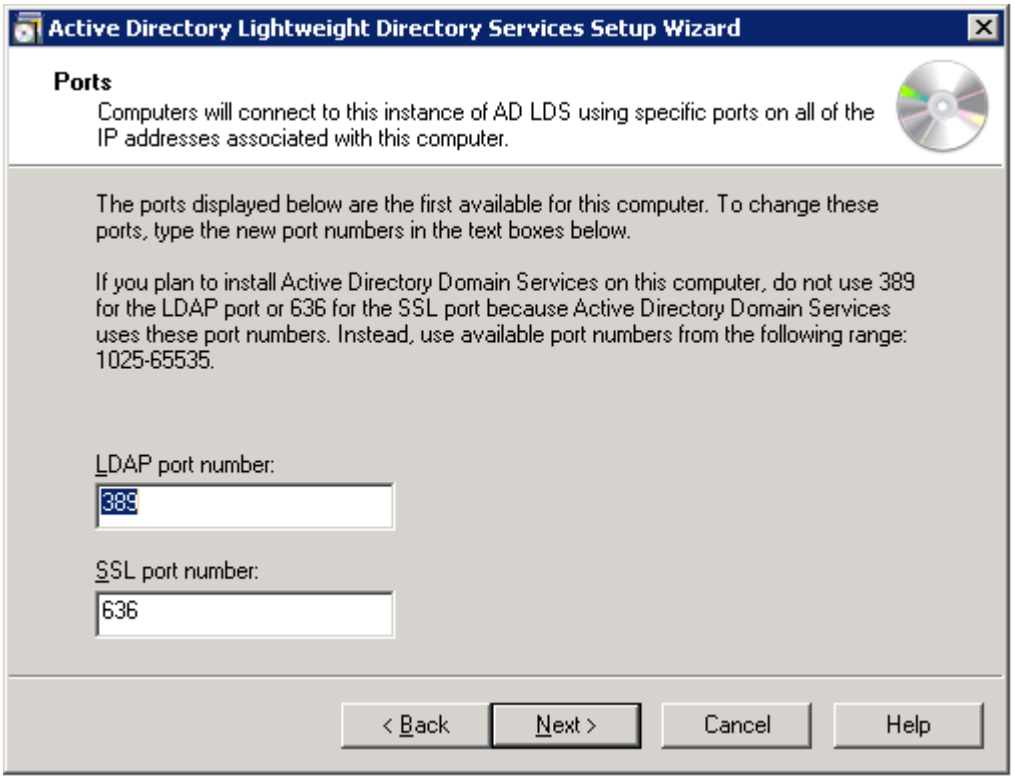
4. Click **Next**.
5. In the Instance Name dialog box, in the **Instance name** box, type `SymposiumWC`.

   SymposiumWC is the default AD-LDS instance name.



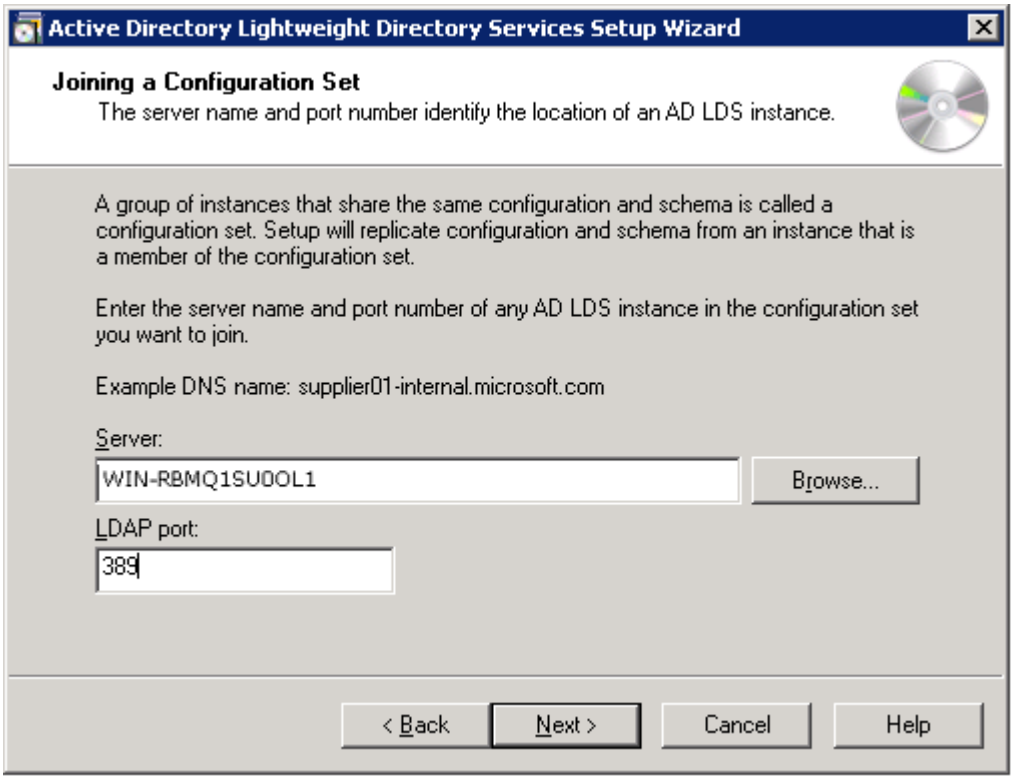
6. In the **Description** box, type `SymposiumWC`.
7. Click **Next**.

8. In the Ports dialog box, if no other applications use the ports, accept the default values in the **LDAP port number** and **SSL port number** boxes.



9. Click **Next**.

10. In the Joining a Configuration Set dialog box, in the **Server** box, type the name of the primary Voice and Multimedia Contact Server to replicate.



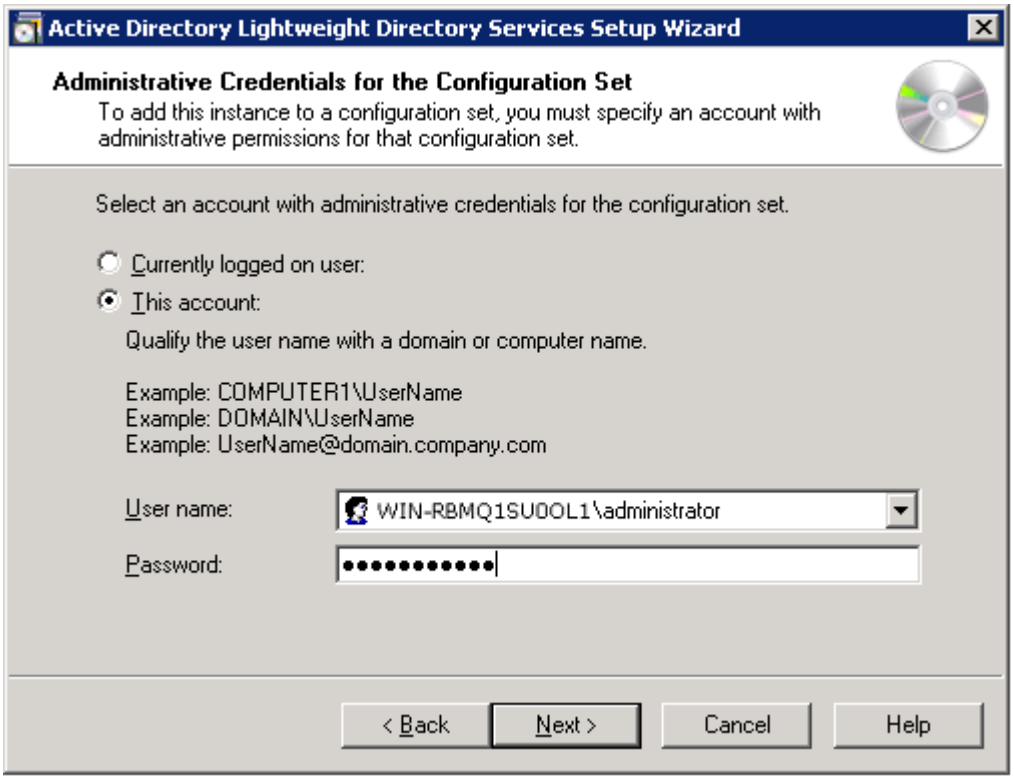
11. On the Joining a Configuration Set window, in the **LDAP Port** box, type the port number on the AD-LDS instance on the primary Voice and Multimedia Contact Server.

    The default is port number 389.

12. Click **Next**.
13. In the Administrative Credentials for the Configuration Set window, select **This account**.
14. In the **User name** box, type the server name of the primary Voice and Multimedia Contact Server followed by its Administrator name in the format `<primary Voice and Multimedia Contact Server name>\Administrator`.

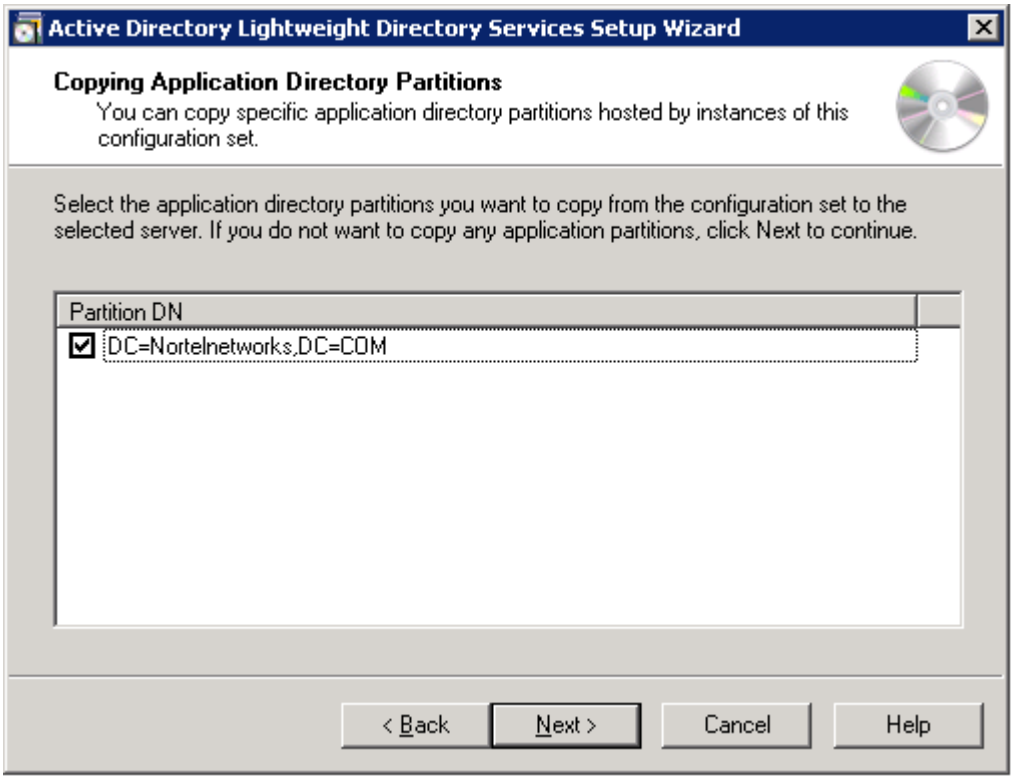
    For example, enter `WIN-RBMQ1SU0OL1\Administrator`.

    If you have created another administrator account for Contact Center, then enter the details (name and password) of that primary Voice and Multimedia Contact Server server administrator account. Your administrator account must have full administrative privileges.



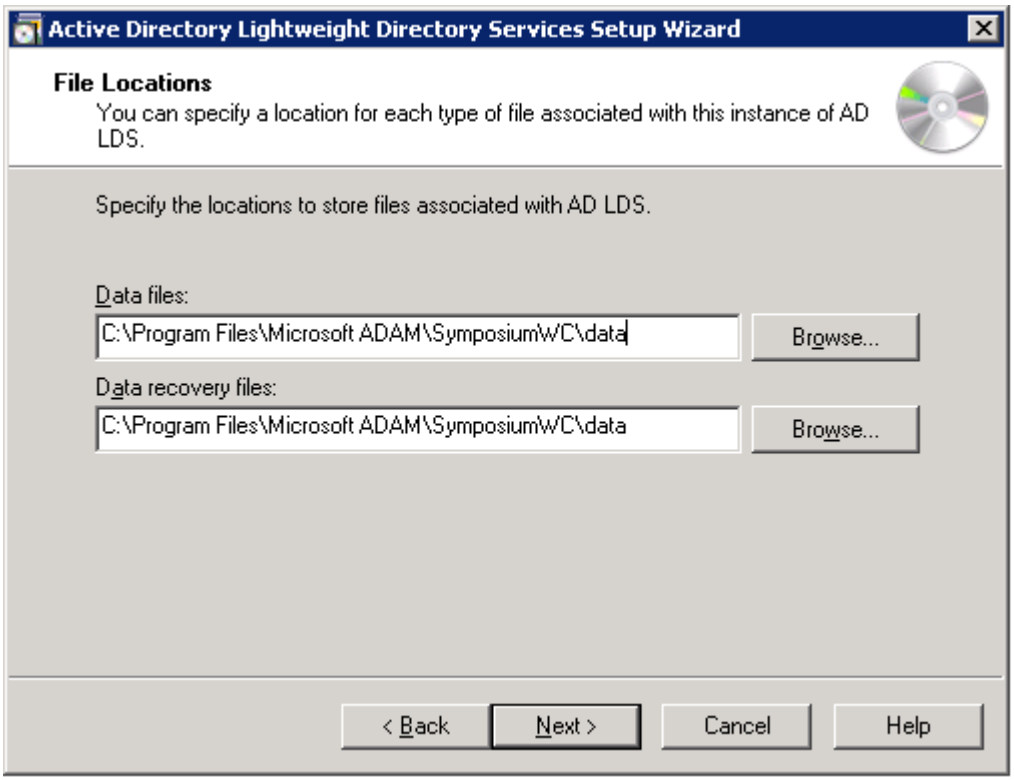
15. In the **Password** box, type the password for this user account.
16. Click **Next**.

17. In the Copying Application Directory Partitions dialog box, in the **Partition DN** list, select **DC=Nortelnetworks,DC=COM**.



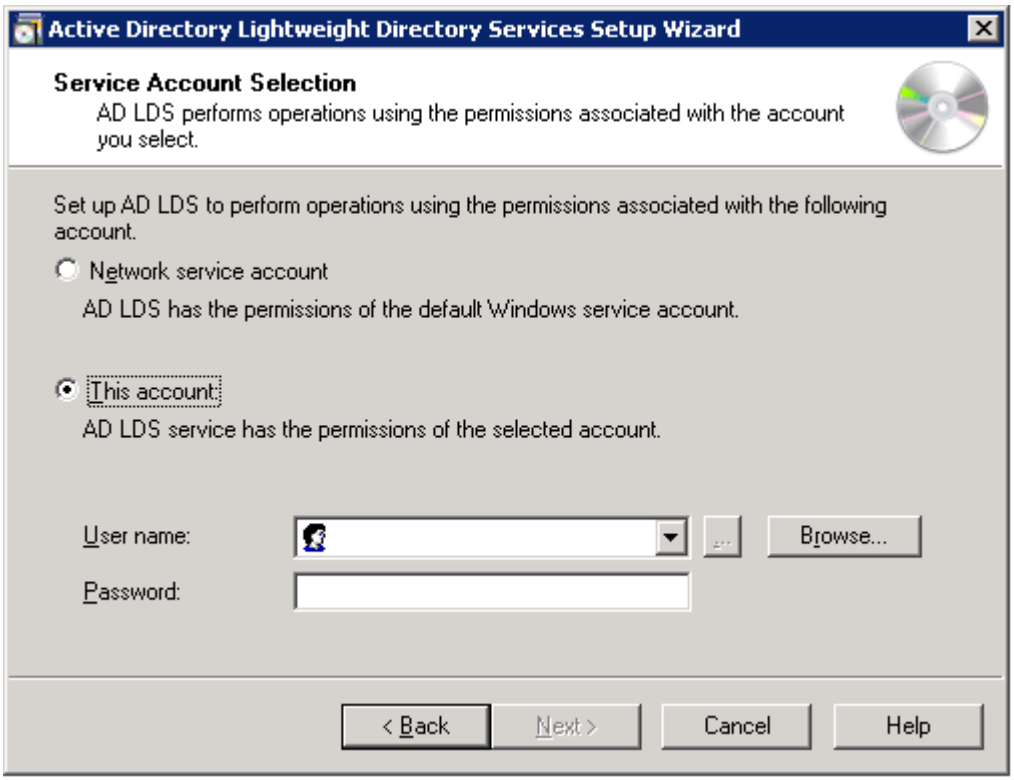
18. Click **Next**.

19. In the File Location dialog box, accept the default values.



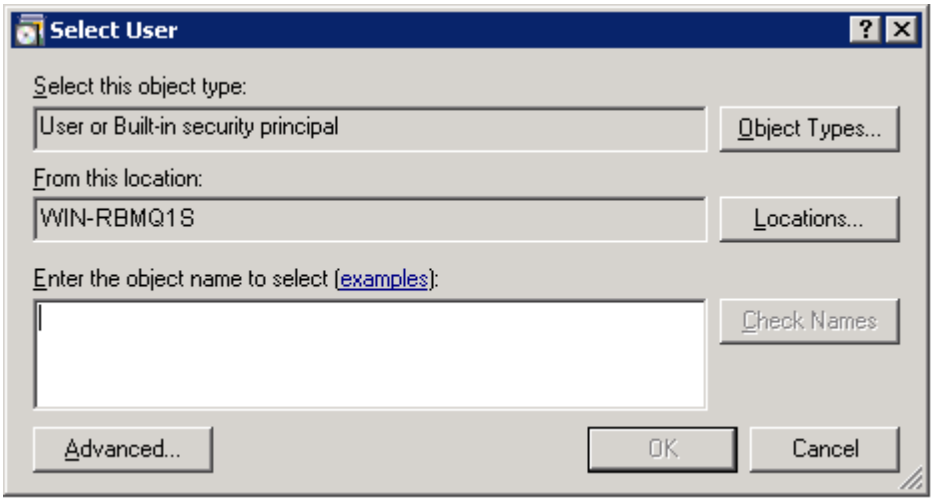
20. Click **Next**.

21. In the Service Account Selection dialog box, select **This account**.



22. In the Service Account Selection dialog box, click **Browse** to locate the service account.

    The system displays the Select User dialog box.



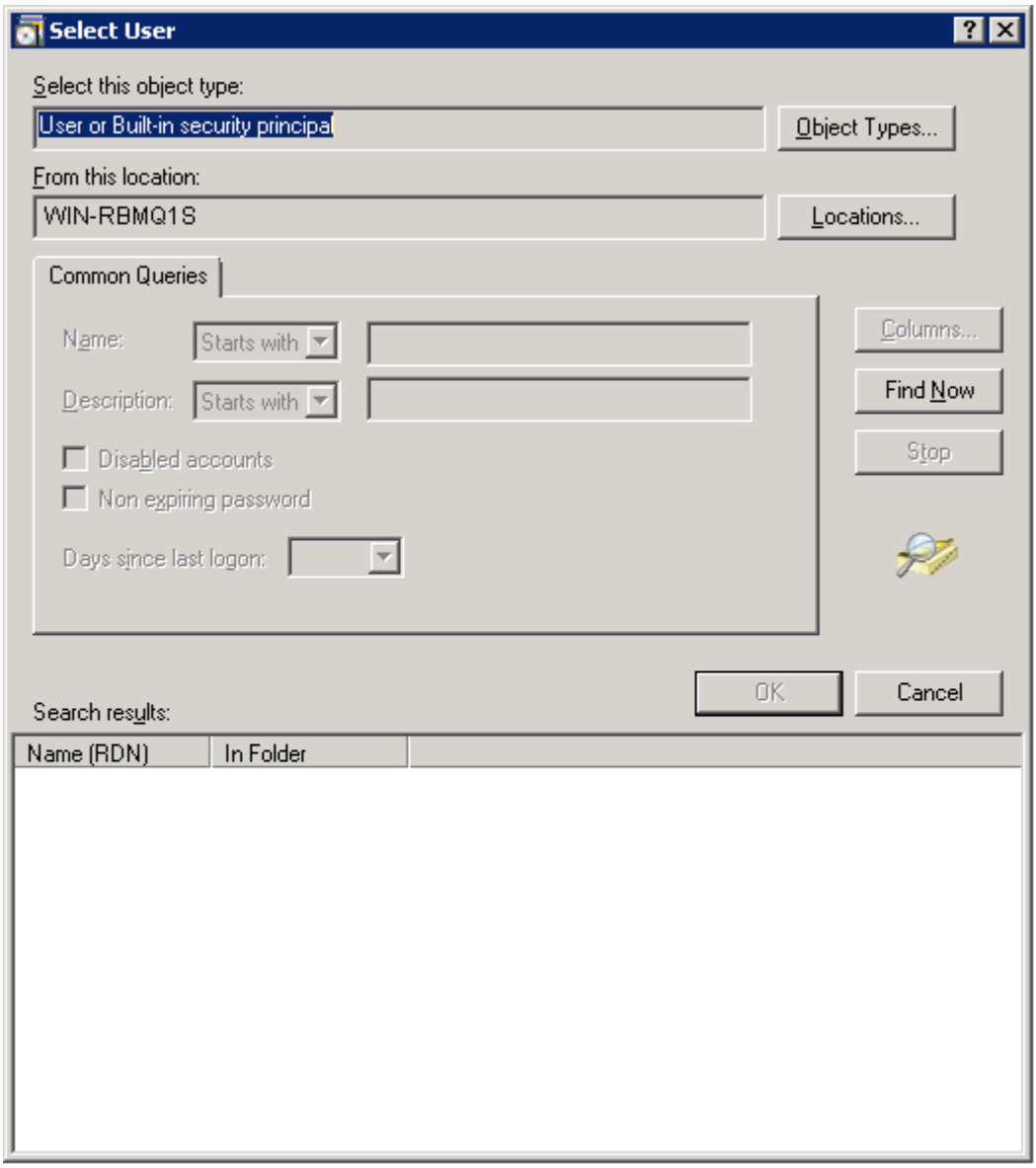
Note:

Ensure that the **From this location** box displays the local server name, which is the computer on which you install AD-LDS. If the **From this location** box does not display

the name of the Contact Center Manager Administration on the standby server, click **Locations** and browse to the server name.

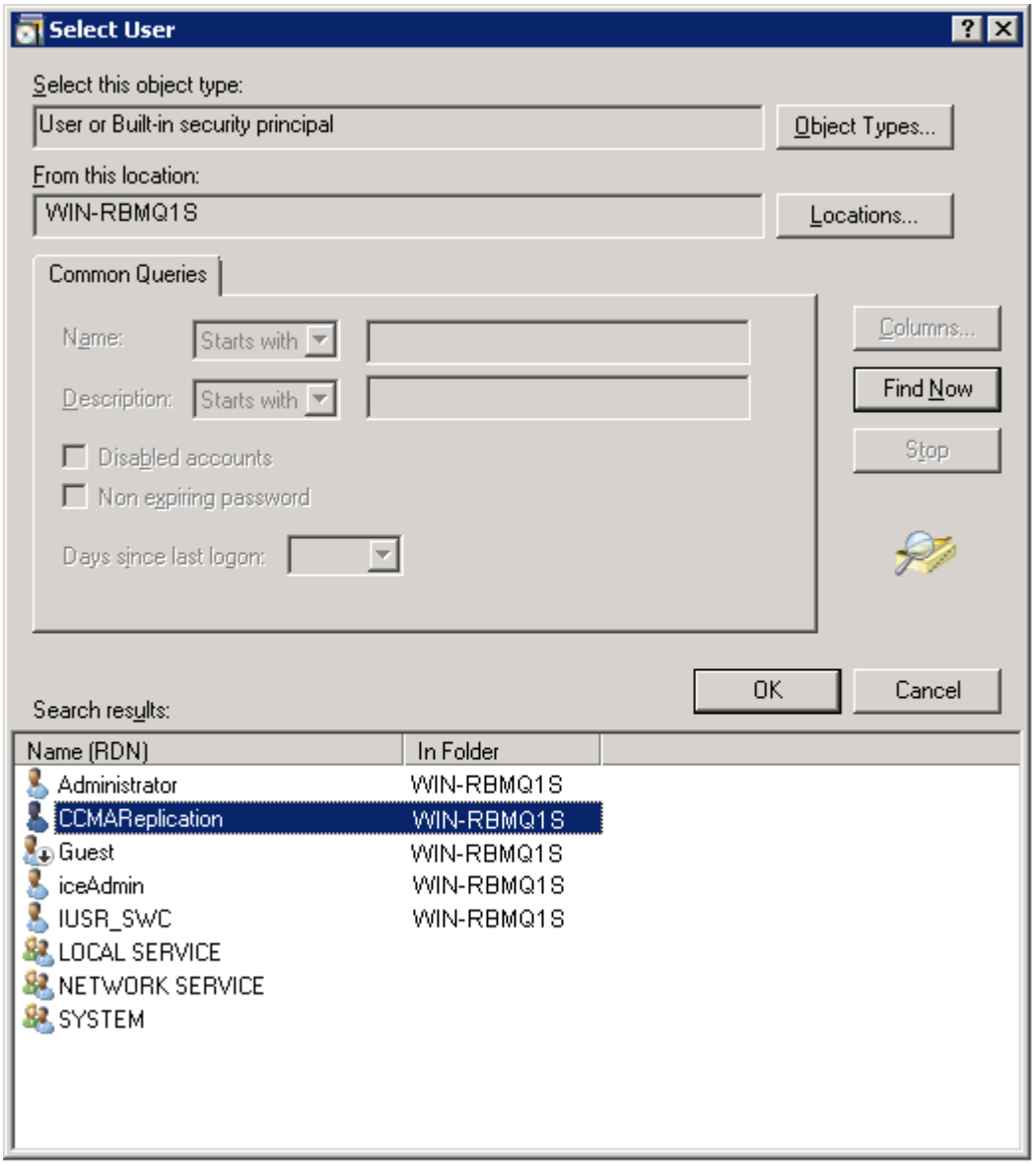
23. In the Select User dialog, click **Advanced**.

    The system displays the advanced Select User dialog box.



24. In the advanced Select User dialog box, click **Find Now**.

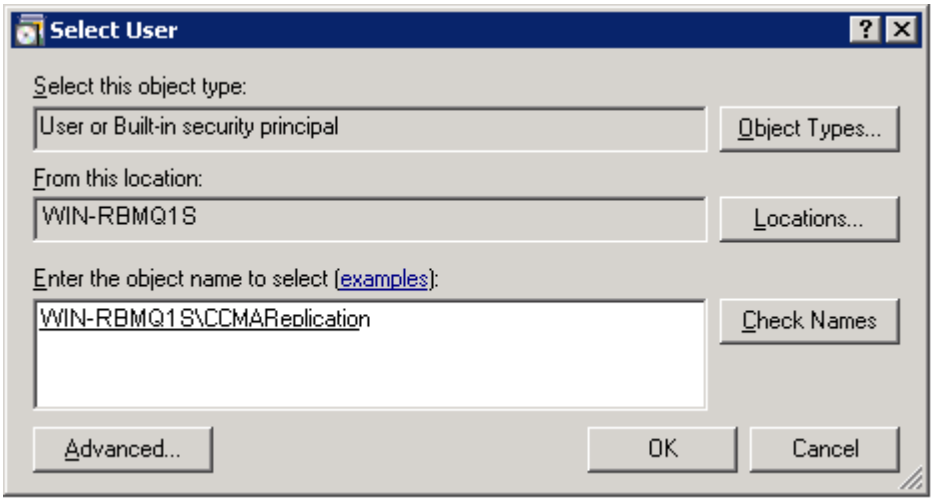
    The system displays the list of available users in the **Search results** list.



25. In the advanced Select User dialog box, from the **Search results** list, select the workgroup CCMA replication service account.
26. In the advanced Select User dialog box, click **OK**.

    The system displays the Select User dialog box.

    An example of selecting a workgroup CCMA replication service account:



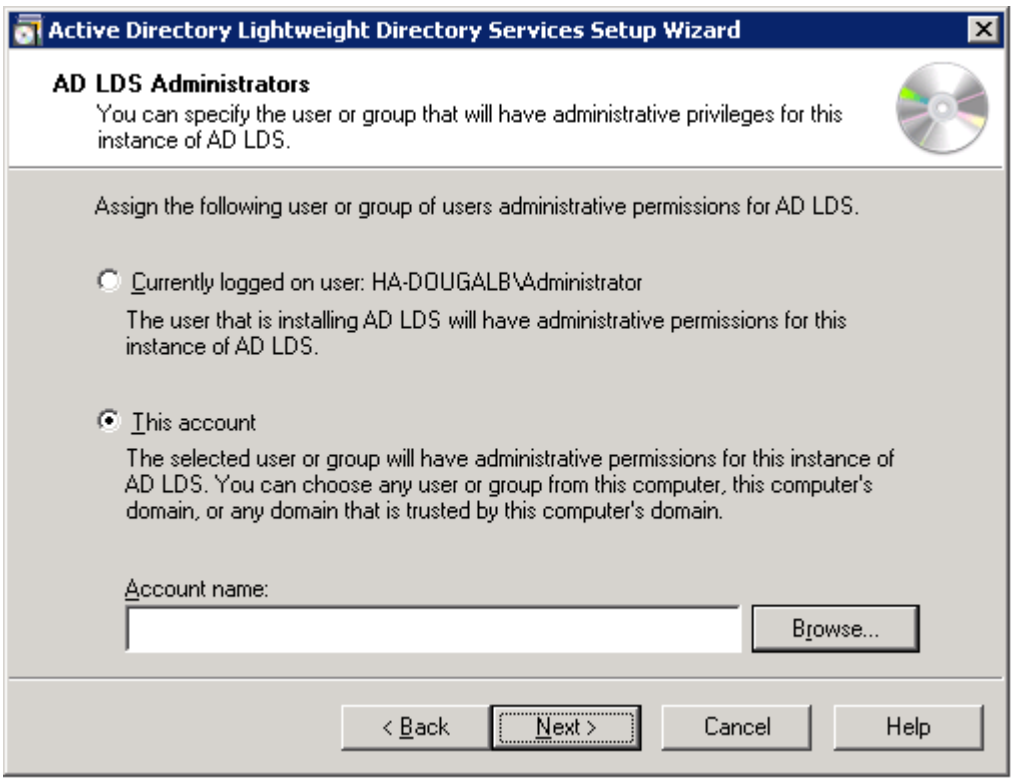
27. In the Select User dialog box, click **OK**.

    The system displays the Service Account Selection dialog box.

28. In the Service Account Selection dialog box, click **Next**.

    The system displays the AD LDS Administrators dialog box.

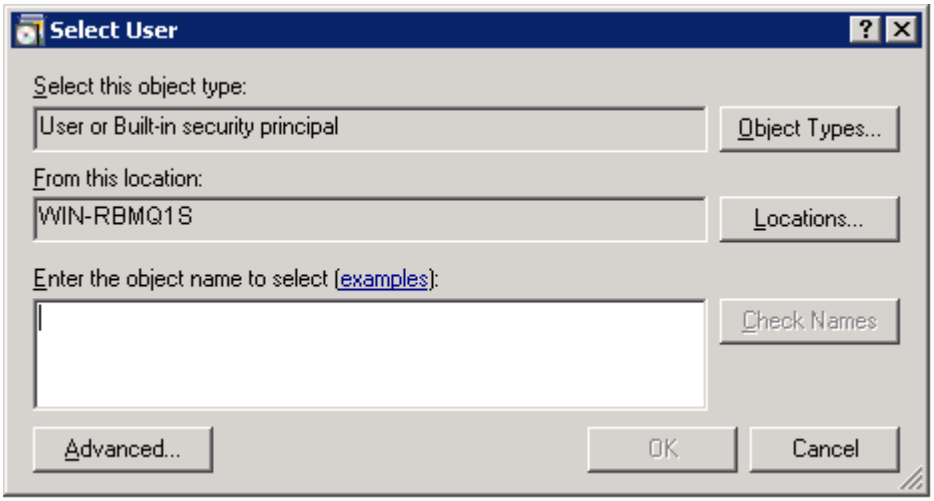
29. In the AD LDS Administrators dialog box, select **This account**.



30. Click **Browse** to locate the CCMA AD-LDS replication account.

The system displays the Select User dialog box. Ensure that the location is the Voice and Multimedia Contact Server.

An example of using a workgroup and selecting a CCMA AD-LDS replication account:



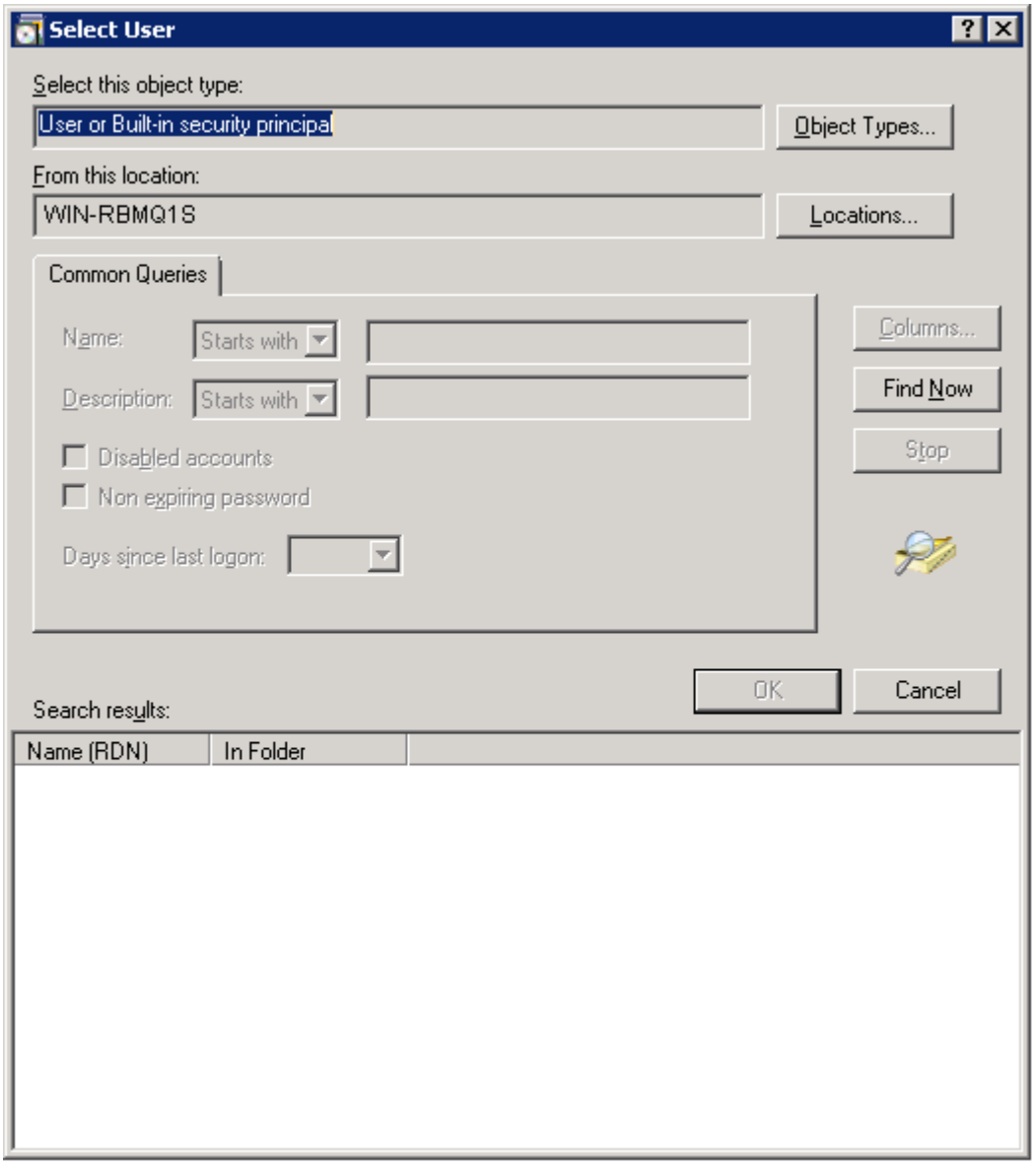
Note:

Ensure that the **From this location** box displays the local server name, which is the computer on which you install AD-LDS. If the **From this location** box does not display the name of the Contact Center Manager Administration on the standby server, click **Locations** and browse to the server name.

31. In the **Select User** dialog box, click **Advanced**.

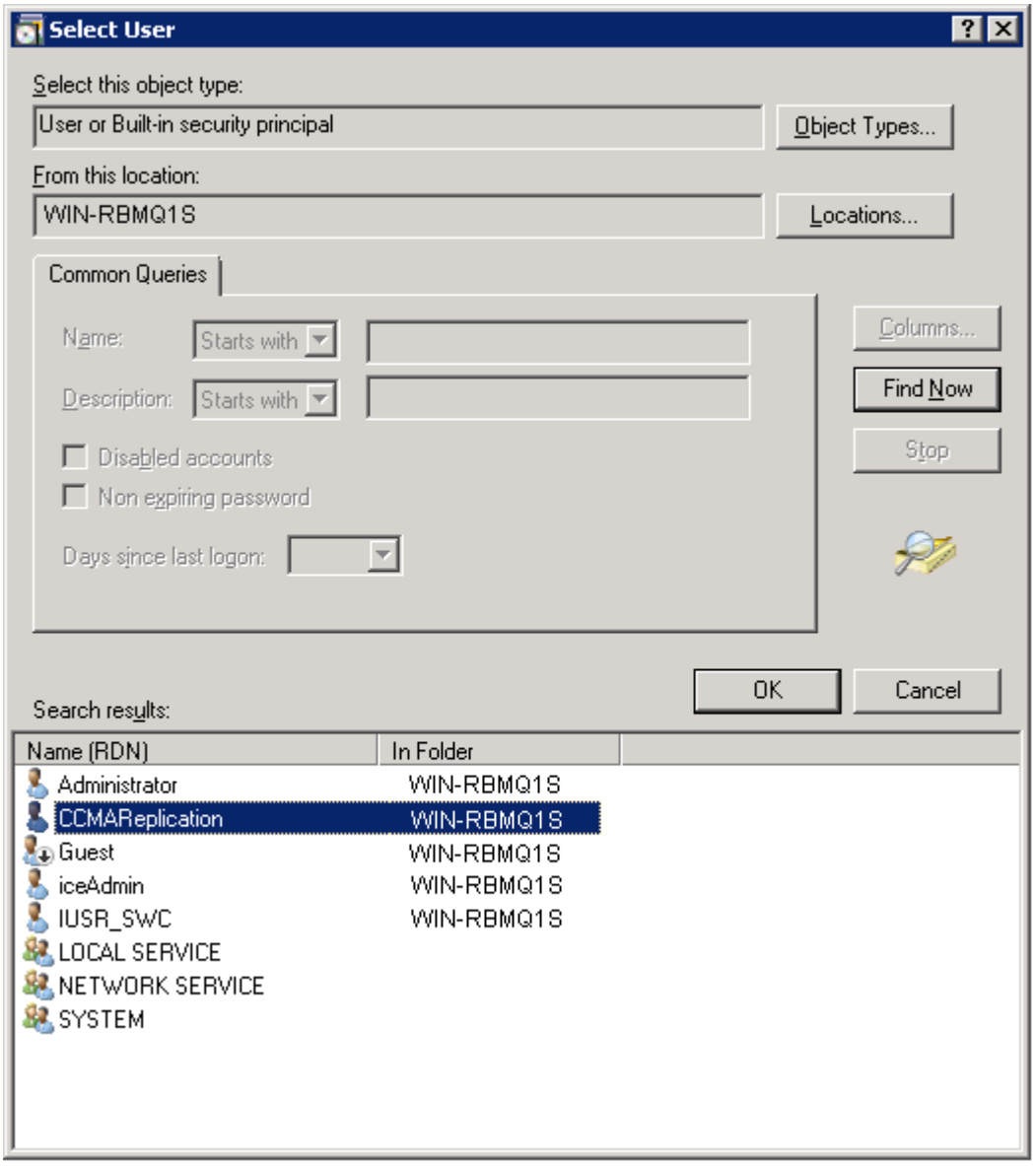
    The system displays the advanced Select User dialog box. Ensure that the location is the Voice and Multimedia Contact Server.

    An example of using a workgroup and selecting a CCMA AD-LDS replication account:



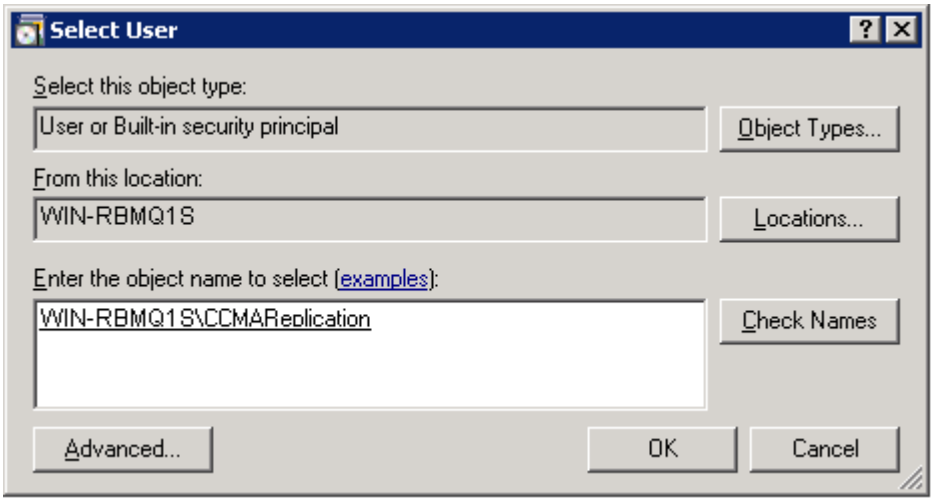
32. In the advanced **Select User** dialog box, click **Find now** to display the list of user accounts.

    An example of using a workgroup and selecting a CCMA AD-LDS replication account:



33. From the **Search results** list, select the workgroup CCMA AD-LDS replication account.
34. In the advanced Select User dialog box, click **OK**.

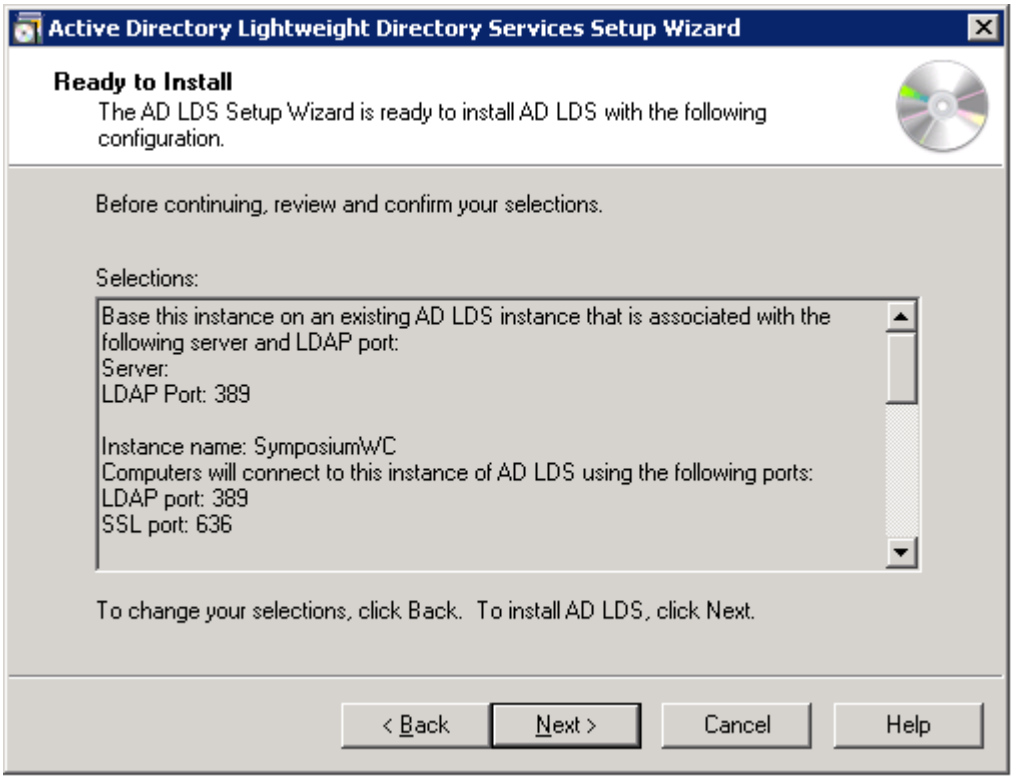
    The system displays the Select User dialog box. An example of selecting a workgroup CCMA AD-LDS replication account:



35. In the Select User dialog box, click **OK**.

36. Click **Next**.

    The system displays the Ready to Install dialog box.



37. Confirm the installation components, and click **Next**.
38. After the installation is complete, click **Finish**.
39. If prompted, restart the server.

Launching Orchestration Designer

About this task

Troubleshoot when Orchestration Designer (OD) fails to load after launch, and an error appears stating “An error has occurred while reading CCMS” or “Unable to contact CCMA server”. If these errors appear, you might need to increase the CCMA Timeout value in Orchestration Designer from 8 minutes to a higher value.

The CCMA Timeout value is specific to each solution, and can depend on a number of factors such as server specification, contact center call rates, database load reporting or administration changes), differences between physical virtual platforms, number of OD applications, and the number of script variables.

You can increase the CCMA Timeout value, and lower the value after a period of additional observation. For example, initially increase the CCMA Timeout value to 20 minutes. If after additional observation your solution requires the value to be set to 12 minutes, you can decrease the value from 20 minutes to 14 minutes.

If the problem persists, contact Avaya technical support.

Before you begin

- Read *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (44400-510).

Procedure

1. Launch Orchestration Designer.
2. In Orchestration Designer, click **Window** > **Preferences**.
3. On the **Preferences** window, expand **Contact Center** > **CCMA Connection**.
4. Under **Service Connection Values**, in the **CCMA Timeout (minutes)** box, increase the value to 20 minutes.
5. Click **Apply**.
6. Click **OK**.
7. Relaunch Orchestration Designer and verify that Orchestration Designer now loads successfully.

Troubleshooting errors when launching Orchestration Designer with SSL configured

About this task

Troubleshoot when launching Orchestration Designer with SSL configured.

Procedure

1. Examine the following log file:

   ```
   c:\SCE.txt
   ```

   Look for this error:

   ```
   The https URL hostname does not match the Common Name (CN) on the
   server certificate. To disable this check (NOT recommended for
   production) set the CXF client TLS configuration property
   "disableCNCheck" to true.
   ```

2. If the error exists in the log file, the certificate was not issued using the FQDN of the CCMA server. Re-issue the certificate. For more information about re-issuing the certificate, see “Enabling HTTPS security for CCMA” in *Avaya Aura® Contact Center Server Administration* (44400-610).

Rebooting CCMA: IIS worker process errors

About this task

On the server, after you install software updates and reboot the server, a dialog box appears indicating that the IIS worker process closed due to a Windows error. These types of errors are for information, and indicate that the IIS worker process crashed. The server stores the errors, and the IIS worker reports the errors when a user logs on after a reboot. These errors might have occurred in the past and can appear several times, with times and dates for previous time periods.

There is no impact to the Contact Center Manager Administration installation or application.

Procedure

1. In the dialog box, click **Don’t Send**.
2. If not previously reported, report the IIS Lockups specified in the error dialog box to Avaya Technical Support.

Checking .NET configuration in IIS

About this task

If you do not configure ASP.NET correctly prior to installing Contact Center Manager Administration, problems can occur. You must enable ASP.NET web services.

Procedure

1. Click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. In the left pane of the Internet Information Services (IIS) Manager, select the server name.
3. In the right pane, under **IIS**, click **ISAPI and CGI Restrictions**.
4. Ensure that the following Web Service Extension is present and that the status is **Allowed**.
   - ASP.NET v2.0.50727
   - ASP.NET v4.0.30319
5. If the status of either extension is **Not Allowed**, right-click the extension and click **Allow**.
6. Close Internet Information Services (IIS) Manager.

Identifying errors after CCMA server is added to Domain Server

Before you begin

- Ensure that you have read the *Avaya Aura® Contact Center Server Administration* (44400-610) guide.

About this task

Troubleshoot errors that can occur after a Contact Center Manager Administration server is added to a Domain Server with a strict security policy.

Procedure

1. If you cannot see the Login screen, ensure that you have WRITE permissions on the `Windows\Temp` folder.
2. If you cannot log on to Contact Center Manager Administration server, ensure that you have IUSR_SWC READ access to the `<x:>\Program Files\Avaya` directory.
3. If you cannot launch the Report Creation Wizard, ensure that you have Users Group or Network Service or IUSR_SWC READ permissions on the `Windows\assembly` directory.
4. If you cannot import a report created by the Report Creation Wizard, ensure that you have Network Service or Users group READ access to the `<x:>\Avaya` directory.
5. If the Report Creation Wizard is performing slowly, ensure that you have Network Service READ/Execute access to `<x:>\Program Files\Avaya` directory. Ensure that you add Network Service or Users Group or IUSR_SWC READ permissions to `Program Files(x86)\Business Objects\Business Objects Enterprise 12.0\Win32_x86\clientSDKOptions.xml`.

Identifying communication errors with Contact Center Manager Server

About this task

Troubleshoot communication errors with Contact Center Manager Server by testing for the various issues that can cause the communication errors and, after testing, taking appropriate action as required.

Procedure

1. Check to ensure that the Contact Center Manager Server IP address being used is valid.
2. Ping the Contact Center Manager Server, by name and by IP address.
3. Contact your system administrator if you are unable to successfully ping the Contact Center Manager Server.

4. Check your cabling.
5. Check the IP addresses for the Contact Center Manager Administration servers and the servers in Contact Center Manager Server.
6. Check the versions on the servers in Contact Center Manager Server, and confirm that they are compatible with Contact Center Manager Administration.

Changing the computer name of the Contact Center Manager Server on the CCMA server

About this task

Change the computer name of the Contact Center Manager Server on the Contact Center Manager Administration server if you:

- change the computer name and/or IP address of the Contact Center Manager Server
- change to a standby Contact Center Manager Server with a new name

If not using the managed IP address, you must reconfigure the Contact Center Manager Administration server to connect to a secondary Contact Center Manager Server, with a different computer name and IP address. Contact Center Manager Administration can then continue to communicate with a new standby Contact Center Manager Server and retrieve all of the data stored in the application server for that server.

Procedure

1. Log on to Contact Center Manager Administration as the webadmin user.
2. Open the **Configuration** component.
3. In the left pane, right-click the server with altered network settings.
4. Click **Edit Properties**.

   This enables the text fields for the servers name, IP address, login ID and password.
5. Enter the new details and click **Submit**.

Solving connection errors following a computer name change on a server

Before you begin

Ensure that you have administrator privileges.

About this task

On a Voice and Multimedia Contact Server or a Voice Contact Server, after you change the computer name, you must perform the following tasks to reset the name so that Contact Center Manager Server and Contact Center Manager Administration function properly.

You must update your Domain Name Server (DNS) or HOSTS table to reflect the new name of the server for your Contact Center Manager Administration to function correctly.

Procedure

1. Run the Contact Center Manager Server Computer Name Sync utility.
2. Run the iceAdmin PasswordChange utility and reset the iceAdmin password.

Resetting the iceAdmin password after a CCMA server name change

Before you begin

- Ensure that you have administrator privileges.
- Use System Control and Monitor Utility (SCMU) to stop all Contact Center Manager Administration services.
- Reset Internet Information Services (IIS) (using the `iisreset` command) on the Contact Center Manager Administration server.

About this task

You must update your Domain Name Server (DNS) or HOSTS table to reflect the new name of the Contact Center Manager Administration server for your Contact Center Manager Administration to function correctly.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
2. In the left pane, click **Avaya**.
3. In the **Avaya Applications Configuration** window, click **IceAdmin Password Change**.
4. In the **Old Password** box, type the old password.
5. In the **New Password** box, reenter the old password for the iceAdmin user account. This resets the iceAdmin password.
6. In the **Confirm Password** box, type the password again.
7. If your Contact Center Manager Administration server is a member of an active domain, the **Domain Account** option is enabled on the **iceAdmin Password Change** window.
8. If the domain account button is disabled, proceed to step 15.

   OR

To export scheduled reports to a domain network PC, proceed to step 9.

9. Click **Domain Account**.
10. In the **Optional Domain Account Setup** window, from the **Select Domain Name** list, select the name of the domain to add.
11. In the **Enter Domain Account** box, type the domain account. Obtain the domain account name and password from your network administrator.
12. In the **Enter Domain Account Password** box, type the domain account password. You must enter the correct domain account password. If the password is incorrect, the system does not proceed.
13. In the **Confirm Domain Account Password** box, retype the domain account password.
14. Click **OK**.

    The iceAdmin Password Change window reappears and activates all scheduled reports using the domain account instead of the local iceAdmin account
15. Click **OK**.

    The system verifies that you typed the same password both times, and then resets the password for both iceAdmin and IUSR_SWC.
16. Use System Control and Monitor Utility (SCMU) to start Contact Center Manager Administration.

Troubleshooting client PC communication problems with the CCMA server

Before you begin

Ensure that you have administrator privileges and that your username and password are valid.

About this task

There are a number of issues that can cause client PCs to be unable to communicate with the Contact Center Manager Administration server. You must identify the source of your problem before determining the solution.

Procedure

1. Test the communication from the client to the Contact Center Manager Administration server.
2. Verify that Web users have permissions on all directories in the Contact Center Manager Administration Web site. When Contact Center Manager Administration is installed, it uses the default settings stored in IIS. If Web users do not have permissions, contact your site administrator for details about changing the settings in IIS.

3. If you configure a Domain Name Server (DNS), verify that the computer name of the Contact Center Manager Administration server is registered on the DNS. If the computer name is not registered on your DNS, then Contact Center Manager Administration does not function properly.
4. If you did not configure a DNS server, verify that you added the computer name of the Contact Center Manager Administration server to the HOSTS table on each client PC that accesses Contact Center Manager Administration.
5. Check if Internet Explorer uses a proxy server.
6. Ensure that the IIS service is running on the Contact Center Manager Administration server.
7. Ensure that AD-LDS is installed and running on the Contact Center Manager Administration server.
8. Confirm that the event viewer logs are configured correctly on the Contact Center Manager Administration server.

Testing communication from the client to the CCMA server

About this task

If the client cannot connect to the Contact Center Manager Administration server, and you have already checked to make sure that the Contact Center Manager Administration username and password are valid, you need to test communication.

Procedure

1. Ping the Contact Center Manager Administration server.
2. Check the IP addresses for the Contact Center Manager Administration servers and the servers in Contact Center Manager Server.
3. Check your cabling.
4. Make sure the Web site is active on the Contact Center Manager Administration server.
5. Try to connect to Contact Center Manager Administration using a Web browser on the CCMA server.
6. Make sure the computer name of the Contact Center Manager Administration server is registered on the DNS server.
7. If the Web site is active, the IP addresses are valid, and you are unable to successfully ping the Contact Center Manager Administration server, contact your system administrator.

Checking if Internet Explorer uses a Proxy Server

About this task

If the client cannot connect to the Contact Center Manager Administration server, check whether Internet Explorer uses a Proxy Server.

Procedure

1. On the Internet Explorer menu bar, choose **Tools** > **Internet Options** > **Connections** > **LAN Settings**.
2. If the **Use a proxy server for your LAN** check box is selected, contact your Proxy Server administrator to verify that there are no restrictions preventing you from accessing the Contact Center Manager Administration server.

Adding the computer name of the CCMA server to the HOSTS table on each client PC if you have not configured a DNS

Before you begin

- Ensure that you carefully review the detailed information about HOSTS in the supporting Microsoft documentation. Incorrectly modifying a HOSTS table on the client PC can cause extensive network problems.

About this task

Avaya recommends that the Contact Center Manager Administration server host name be resolved by the corporate DNS. However, if you did not configure a name resolution server during the operating system installation, then the client PCs that connect to Contact Center Manager Administration cannot find the Contact Center Manager Administration server. If this occurs, you must manually update the HOSTS table on each client PC with the name and contact center server subnet network interface IP address of the Contact Center Manager Administration server.

When you use server names to connect to a Contact Center Manager Administration server in TCP/IP networks, the server name must be associated with an IP address. The HOSTS table carries out this association, which is called host name resolution.

The HOSTS table consists of a list of IP addresses followed by a computer name: 123.4.56.100 webclient.Avaya.com. At the end of the file, type the IP address and computer name of the Contact Center Manager Administration server. Separate the two values by using the space or tab key. HOSTS tables are case-sensitive. After you edit and save the HOSTS file, the system automatically reads your new settings. If you edit the sample HOSTS file, then save the file with no extension to enable the system to recognize your changes.

Based on the operating system installed on the client PC, sample host tables are located in various directories. With the Windows 2008 Release 2 installation, for example, sample HOSTS tables are provided in the following directory: [x]:\WINDOWS\system32\drivers\etc.

Procedure

On each client PC, use a text editor to modify the HOSTS tables by entering the computer name and IP address of the Contact Center Manager Administration server.

Important:

You do not have to use HOSTS tables for name resolution if the name of the Contact Center Manager Administration server is registered on a DNS server.

Verifying that IIS is running on the Contact Center Manager Administration server

About this task

Verify that IIS is running on the Contact Center Manager Administration server.

Procedure

1. On the Contact Center Manager Administration server, choose **Start** > **Administrative Tools** > **Services**.
2. In the right pane of the **Services** window, select the **IIS Admin Service**.
3. In the **Status** column, verify that the IIS Admin Service is **Started**.

Verifying that AD-LDS is installed on the Contact Center Manager Administration Server

About this task

Verify that Microsoft Active Directory Lightweight Directory Services (AD-LDS) is installed on the Contact Center Manager Administration Server.

Procedure

1. Click **Start** > **Control Panel** > **Programs**.
2. Click **Programs and Features**.
3. In the **Programs and Features** window, verify that **AD LDS Instance SymposiumWC** is displayed.

Resolving trust relationship error when installing AD-LDS

Before you begin

- Ensure you read *Avaya Aura® Contact Center Installation* (44400-311).

About this task

Resolve the trust relationship error that occurs when installation of AD-LDS fails and the trust relationship between the domain and the workstation is broken.

Procedure

1. Use the DVD controller to uninstall Contact Center Manager Administration.
2. Remove the workstation from the domain and add it to a workgroup.
3. Add the workstation to the domain, to re-establish the trust relationship between the domain and the workstation.
4. Use the DVD controller to install Contact Center Manager Administration.

Troubleshooting CCMA replication

About this task

If your CCMA server uses AD-LDS replication, you can use the AD-LDS Replication Diagnostics Tool (repadmin.exe) to diagnose replication related issues and to display the replication settings for a primary CCMA server.

To retrieve the replication settings for a primary CCMA server, enter:

```
repadmin /options localhost:389
```

A primary CCMA server with replication enabled and with no flags set gives the following result:

```
Current DSA Options: (none)
```

A primary CCMA server with replication disabled gives the following result:

```
Current DSA Options: DISABLE_OUTBOUND_REPL
```

If CCMA displays the error message “The source server is currently rejecting replication requests”, you must enable replication on the primary CCMA.

If your CCMA server supports High Availability and uses AD-LDS replication, you must enable replication on the primary CCMA server. Use the AD-LDS Replication Diagnostics Tool (repadmin.exe) to enable replication on the primary CCMA server. The Repadmin option {+|-}DISABLE_OUTBOUND_REPL, stops (+) or restarts (-) outbound replication.

Procedure

1. Log on to the primary Contact Center Manager Administration server.
2. Click **Start** > **Run**.

3. In the **Run** dialog box, type `cmd`.
4. Click **OK**.
5. Navigate to the AD-LDS directory, typically located at c:\Windows\adam.
6. To enable outbound replication, type `repadmin /options localhost:389 -DISABLE_OUTBOUND_REPL`.

Identifying the source of Internet Explorer problems

About this task

Identify the source of Internet Explorer problems by checking various items. Depending on the source of the problem, you might need to reinstall the correct version of Internet Explorer on the client PC or you might need to re-configure Internet Explorer on the client PC.

Procedure

1. Check that Internet Explorer version installed on the client PC is a 32–bit supported version.
2. Check that you configured security in Internet Explorer correctly.
3. If you receive error messages from Internet Explorer indicating that your Web site cannot run Out of Process components, enable Out of Process components.
   - Create a script called AspAllowOutOfProcComponents.vbs using any text editor. Insert the following commands:

     ```
     Set objWebService = GetObject ('IIS://LocalHost/w3svc')
     ' Enable AspAllowOutOfProcComponents. objWebService.Put
     'AspAllowOutOfProcComponents', True
     ' Save the changed value to the metabase. objWebService.SetInfo
     ```

   - Save the script.
   - In Windows Explorer, double-click the script.
4. If all of the above steps do not resolve the problem, reinstall Internet Explorer on the client PC.

Troubleshooting when CCMA Web interface is distorted

About this task

Troubleshoot when the display of the Contact Center Manager Administration Web interface is distorted. Distortion occurs when your display settings are not optimized for the Contact Center Manager Administration Web interface. You need to check the display settings on your computer and, if required, resize the font.

Procedure

1. Click **Start** > **Control Panel** > **Appearance**.
2. In the **Appearance** window, click **Display**.
3. Click **Adjust resolution**.
4. In the **Resolution** list, select at least **1024 × 768** pixels.
5. Click **Make text and other items larger or smaller**.
6. Ensure **Smaller - 100% (default)** is selected.
7. Click **Apply**.
8. In Internet Explorer, on the **Page** menu, click **Text Size** > **Medium**.
9. If the text or content display in Internet Explorer is too large, select **Text Size** > **Smaller**.

Disabling pop-up blockers

About this task

Troubleshoot when you cannot launch a window in Contact Center Manager Administration and a message displays indicating that pop-ups were blocked on this page. For all components of Contact Center Manager Administration to function correctly, you must disable pop-up blockers on Internet Explorer.

Procedures to disable pop-up blockers vary, depending on the type of pop-up blocker you have. If the procedure here does not disable your pop-up blocker, contact the pop-up blocker provider.

Procedure

1. Open Internet Explorer.
2. If you use Google, on the Google toolbar, click on the **Popup blocker** icon and confirm that the icon indicates **Site popups allowed**.
3. If you use Yahoo, on the Yahoo toolbar, click on the button that displays the tooltip **Pop-Up Blocker Is On** or **Pop-Up Blocker Is Off**. In the expanded menu, ensure that the option **Enable Pop-Up Blocker** is unchecked.
4. If you use Windows XP Service Pack 2, click on **Tools** > **Pop-up Blocker** > **Turn Off Pop-up Blocker**.

Troubleshooting when CCMA logon screen displays ERROR:UNKNOWN!

About this task

Troubleshoot when you attempt to launch Contact Center Manager Administration and the logon screen displays ERROR:UNKNOWN! You need to ensure that the display settings for Internet Explorer are configured for Western European (ISO).

Procedure

1. Open Internet Explorer.
2. In the **Internet Explorer** browser window, select **View** > **Encoding**.
3. In the **Encoding** selection menu, ensure that **Western European (ISO)** is selected.
4. Close all windows.

Troubleshooting when CCMA logon screen displays User account is expired

About this task

Troubleshoot when you attempt to open Contact Center Manager Administration in a Security Framework environment, and the logon screen displays User account is expired. This normally happens when the user account on the Primary Security Server (System Manager) expires.

Procedure

Follow the System Manager documentation to reset the Administrator user password. You can find the System Manager documentation on the Avaya support site.

Troubleshooting when CCMA logon page displays Connect Login prompt

About this task

Troubleshoot when attempting to launch the Contact Center Manager Administration logon screen, and the Connect to <CCMA server name> logon window appears, prompting you for a username and password. This indicates that the IUSR_SWC password configured in IIS does not match the specified password for your user account in Computer Management. You need to re-run the iceAdmin password change utility to reset the IUSR_SWC password.

Procedure

Run the iceAdmin PasswordChange utility and reset the iceAdmin password.

Troubleshooting when CCMA logon screen displays User account is expired

About this task

Troubleshoot when you attempt to open Contact Center Manager Administration in a Security Framework environment, and the logon screen displays User account is expired. This normally happens when the user account on the Primary Security Server (System Manager) expires.

Procedure

Follow the System Manager documentation to reset the Administrator user password. You can find the System Manager documentation on the Avaya support site.

Troubleshooting when CCMA Web services fail to execute

About this task

Troubleshoot when you attempt to log on to Contact Center Manager Administration and Web services fail and an error message appears. This error can occur when the client PC has `Windows/System32/vbscript.dll` version 5.6 installed, but it is not the registered version of vbscript.dll, which is version 5.0.

Procedure

Register `Windows/System32/vbscript.dll`.

Forgetting the iceAdmin password

Before you begin

- Ensure that you are logged on to the CCMA server as an administrator.
- If you want to export scheduled reports to a domain account or use the domain account setup function to reset the domain account password, obtain the domain account name and password from your network administrator.

About this task

Troubleshoot when you forget the iceAdmin password by resetting it. This is a two-step procedure, since you must reset the password in Windows, and then you must reset the password using the iceAdmin Password Change utility that is provided with Contact Center Manager Administration.

Procedure

1. On the Contact Center Manager Administration server, choose **Start** > **Administrative Tools** > **Computer Management**.
2. In the left pane of the **Computer Management** window, click the plus sign (+) beside **Local Users and Groups**.
3. Click the **Users** folder.
4. Right-click the **iceAdmin** user.
5. On the menu, select **Set Password**.
6. In the **Set Password** window, type the new password and confirm the password.
7. Click **OK**.
8. Close all windows.
9. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
10. In the left pane, click **Avaya**.
11. In the Avaya Applications Configuration window, click **IceAdmin Password Change**.
12. In the iceAdmin Password Change window, in the **Old Password** box, type the same password that you typed in step 6.
13. In the **New Password** box, type a new password for the iceAdmin user account.
14. In the **Confirm Password** box, type the new password again.
15. If your Contact Center Manager Administration server is a member of an active domain, the Domain Account option is enabled on the iceAdmin Password Change window. If you want to export scheduled reports to a domain account or use the domain account setup function to reset the domain account password, click **Domain Account**.

    OR

    If you do not want to export scheduled reports to a domain account, or if the Domain Account button is disabled, go to step 21.
16. In the Optional Domain Account Setup dialog box, from the **Select Domain Name** list, select the name of the domain to add.
17. In the **Enter Domain Account** box, type the domain account name that you obtained from the network administrator.
18. In the **Enter Domain Account Password** box, type the domain account password.
19. In the **Confirm Domain Account Password** box, retype the domain account password.

20. Click **OK**.

    The iceAdmin Password Change window reappears and activates all scheduled reports using the domain account instead of the local iceAdmin account.

21. Click **OK**.

    The system verifies that you typed the same password both times and registers the new password in all required components.

Troubleshooting Terminal Services Real-time display errors

About this task

Troubleshoot when no Agent Real-time display appears in a Terminal Services environment. This occurs because only one user can log on at a time for unicast reporting. Enabling Unicast in a Terminal Services environment results in an error if you launch the same Real-time display on a duplicate Terminal Services session.

If you want to use unicast transmission for statistics from the Contact Center Manager Server to the Contact Center Manager Administration server for reporting purposes, you must disconnect the Terminal Services session.

An alternative for using unicast transmission in a Terminal Services environment is using multicast transmission. This must be selected on the Contact Center Manager Administration server, under Transmission.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Click **Start** > **Administrative Tools** > **Terminal Services Manager**.
3. In the Terminal Services Manager window, in the right pane, click the **Sessions** tab.
4. In the right pane, right-click the session to disconnect and select **Disconnect** from the menu.
5. Click **OK**.
6. Close the Terminal Services Manager window.

Troubleshooting when the Real-Time Data Collector service does not update

About this task

Troubleshoot when a nodal server is removed and added again to the Network Control Center, but the Real-Time Data Collector service does not update the change. If this happens, the old site ID is

not deleted and multicast information occurs for two site IDs. The Contact Center Manager Administration server Windows Event Viewer displays event number 500 and Contact Center Manager Administration runs slowly. All Contact Center Manager Server computers configured on Contact Center Manager Administration are affected until the Real-Time Data Collector service on Contact Center Manager Server is restarted.

Procedure

1. In Windows Event Viewer, note all event number 500 references and note the Contact Center Manager Server computers affected.
2. Restart the Real-Time Data Collector service on each of the Contact Center Manager Server computers affected.
3. Restart the iceRTD service on the Contact Center Manager Administration server.

Troubleshooting RTD data errors following backup and restore on a Stratus server

About this task

Troubleshoot when you have performed a backup and restore on a Stratus server and the Real-time Display is not displaying correct data.

This problem occurs because the Real-time Display displays all of the agents in the merged filter belonging to both servers and the data results are incorrect.

Procedure

Create one filter for each server. Do not merge data from two servers in one filter.

Troubleshooting when LMService license grant and release events are not logged

About this task

Troubleshoot when Contact Center Manager Administration LMService events 18002, 18003, 18004 and 18005 are not logged to the Windows security event log on Contact Center Manager Administration when the user opens or closes a Report Creation Wizard browser session. This problem occurs if the Audit Object Access security policy was not configured to audit the success and failure attempts.

Procedure

1. On the Contact Center Manager Administration server, choose **Start** > **Administrative Tools** > **Local Security Policy**.

2. In the left pane of the Local Securities Settings window, expand the **Local Policies** folder by clicking the plus (+) sign next to Local Policies.
3. In the left pane of the **Local Policies** folder, click the **Audit Policy** subfolder.

   A list of audit policies appears in the right pane.
4. In the right pane of the **Local Policies** folder, double-click **Audit Object Access**.
5. In the Audit Object Access Properties window, select **Success**.

   A check mark appears next to the Success option.
6. In the Audit Object Access Properties window, select **Failure**.

   A check mark appears next to the **Failure** option.
7. Click **Apply**.
8. Click **OK**.
9. Close all windows.

Installing ActiveX controls

About this task

Troubleshoot when errors occur because the Internet Explorer security setting for Automatic prompting for ActiveX controls is set to **Disable**.

Procedure

1. Open Internet Explorer.
2. From the menu, select **Tools** > **Internet Options**.
3. Select the **Security** tab.
4. Click the **Trusted Sites** icon.
5. Click **Custom Level**.
6. In the Security Settings window, under the **ActiveX controls and plug-ins** heading, for **Automatic prompting for ActiveX controls**, select **Enable**.
7. Click **OK**.
8. Click **Yes**.
9. Restart Internet Explorer.

   After the security setting is set to **Enable** and Internet Explorer restarts, when the browser encounters an ActiveX control, a dialog box appears, asking the user if they want to install the control. To install the control, click **Install**.

Opening technical documentation .pdf files through CCMA

About this task

Troubleshoot when you have copied the latest user guides to the Contact Center Manager Administration server but you cannot open the user guides through Contact Center Manager Administration. You must change the security permissions of the folder where the guides are stored.

Procedure

1. On the Contact Center Manager Administration server, browse to the folder where the guides are stored:

   `<drive>:\Avaya\Contact Center\Manager Administration\Apps \documentation\guides`.

2. Right-click the **Guides** folder and select **Properties**.
3. In **Properties**, select the **Security** tab.
4. Click **Advanced**.
5. In **Advanced Security Settings for guides**, click **Change Permissions**.
6. Select **Replace all child object permissions with inheritable permissions from this object**.
7. Click **OK**.
8. Close all windows.

Troubleshooting when performance issues occur when you install Microsoft Service Packs or Hot Fixes

About this task

Troubleshoot when you have installed Microsoft Service Packs or Hot Fixes and performance issues occur. These issues can occur if Automatic Private IP Addressing (APIPA) is enabled on the Contact Center Manager Administration server. You need to disable APIPA.

APIPA is a feature available with Windows 2000 and Windows 2008 operations systems that automatically assigns an IP address to an unconfigured network card. The assigned IP address is in the range 169.254.0.0 to 169.254.255.255.

APIPA is automatically disabled in Contact Center Manager Administration Release 6.0 SP0202 and up. When you install Microsoft Service Packs or Hot Fixes, it is possible that the APIPA setting is overwritten.

If APIPA is enabled on the Contact Center Manager Administration server and the server contains an unconfigured network card, the server is assigned an IP address for that network card. The Contact Center Manager Administration server can then provide this IP address to Contact Center Manager Server. This results in Contact Center Manager Server attempting to send notifications to

the Contact Center Manager Administration server on an invalid IP address. The notifications time out and the following can occur:

- Contact Center Manager Server does not acquire TNs
- ASM and TFE services remain in the Starting state
- Performance on Contact Center Manager Server degrades
- OAM Service does not respond to update requests from client

The following information message appears in the system event log:

- `<date time> Dhcp Warning None 1007 N/A WCHICAP Your computer has automatically configured the IP address for the Network Card with network address <###>. The IP address being used is 169.254.###.###`

  .

If the IPAutoconfigurationEnabled entry is not present, the system takes up a default value of 1, which indicates that APIPA is enabled.

Procedure

1. On the Contact Center Manager Administration server, choose **Start** > **Run**.
2. In the Run dialog box, in the **Open** field, type `regedit`, and then click **OK**.
3. In the Registry Editor, navigate to:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip \Parameters`.
4. Right-click the **Parameters** folder and select **New** > **DWORD Value**.
5. Type `IPAutoconfigurationEnabled` as the name.
6. Right-click `IPAutoconfigurationEnabled` and click **Modify**.
7. In the Edit DWORD Value dialog box, in the **Value Data** box, type `0` (zero).
8. In the **Base** section, select the **Hexadecimal** option.
9. Click **OK**.
10. Restart the Contact Center Manager Administration server.

Troubleshooting Real-time Statistics Multicast from the CCMA server

Before you begin

- Ensure that you check with your network administrator for acceptable IP multicast addresses for your network. The IP multicast addresses that you select for RSM sending and receiving must be within the 224.0.1.0 and 239.255.255.255 range.

About this task

Troubleshoot Real-time Statistics Multicast (RSM) from the Contact Center Manager Administration server by checking various causes for errors. The source of errors can originate in the following network components:

- the client PC
- the Contact Center Manager Administration server
- the Contact Center Manager Server
- Local Area Network (LAN)
- Wide Area Network (WAN)

Procedure

1. Ensure that the LAN or WAN supports multicast traffic. Contact your network administrator to confirm that the routers have multicast capabilities.
2. Verify that you can send and receive data between Contact Center Manager Server, the Contact Center Manager Administration server, and the Contact Center Manager Administration clients.
3. Confirm that the Real-time Statistics Multicast components send data to the same IP multicast address.
4. Ensure that the IP Receive address for the Contact Center Manager Administration server matches the IP Send multicast address setting in Contact Center Manager Server.

Using ICERTDTrace to trace IP multicast data

About this task

Use ICERTDTrace to trace IP multicast data, to assist you in determining whether your network is configured properly for IP multicasting, and to help you identify where Real-Time Reporting or Agent Desktop Display problems originate. ICERTDTrace.exe is a diagnostic tool provided with Real-Time Display configurations of Contact Center Manager Administration.

Use ICERTDTrace.exe to test that the Contact Center Manager Administration server is sending and receiving multicast to and from the Contact Center Manager Server.

Procedure

1. To trace data sent from Contact Center Manager Server to the Contact Center Manager Administration server, at the command prompt type the following command: `icertdtrace -r IPreceive <IP Multicast receive address> -s <CCMS site name> -t <statistic type>` where *<statistic type>* is an agent, application, skillset, ivr, nodal, or route. The multicast address must be specified if the -s or -t options are used. The -s or -t options can be used separately.

   The output log file is printed to the screen at run time to a text file at the following location: `<drive>:\Avaya\Contact Center\Manager Administration\Server \IPRcvLog.txt`.

2. To trace data sent from Contact Center Manager Administration server to clients, type the following command: `icertdtrace -r IPSend <IP Multicast send address> -s <CCMS server name> -t <statistic type>` where *<statistic type>* is an agent, application, skillset, ivr, nodal, or route statistic. The multicast address must be specified if the-s or -t options are used. The -s or -t options can be used separately.

   The output log file is printed to the screen at run time to a text file at the following location: `<drive>:\Avaya\Contact Center\Manager Administration\Server \IPSndLog.txt`.

Receiving, but not sending, multicast

About this task

Troubleshoot when the server is receiving, but not sending, multicast by checking that the ICERtd Service is running and by checking for event log errors relating to machine names or IP addresses.

Procedure

1. Check that the ICERtd Service is running.
2. In the Windows Event Viewer, check the application event log for errors relating to machine names or IP addresses.
3. Verify that the configured Contact Center Manager Servers can be reached by their specified names by pinging each individual name and verifying that the IP address that the system uses in the ping is the same as the one that appears in the Contact Center Manager Administration Configuration window.

Troubleshooting Server Utility Event Browser failure

About this task

If Server Utility Event browser fails to retrieve events for an application, verify the Windows Event Viewer application settings. In the case of Windows Event Viewer failure, you receive the error message: Failed to Retrieve; Fault Management Server Error.

Procedure

1. Click **Start** > **Administrative Tools** > **Event Viewer**.
2. Select the required application.
3. On the **Event Viewer** menu bar, select **Action** > **Properties**.
4. Click the **General** tab.
5. In the **Log** size section, verify that the value in **Maximum log size** is not set to high.

6. In the **When maximum log size is reached section**, select **Overwrite events as needed**.
7. Click **Apply**.
8. Click **OK**.

Testing the RSM service on Contact Center Manager Server

About this task

Test the RSM service using the Multicast Receive utility (mRcv.exe), if you are having problems with real-time displays. The mRcv.exe utility displays statistical information according to the settings specified in a configuration tool called mRcv.ini.

Because the mRcv.exe utility tests the RSM service send capabilities one port at a time, you must specify the IP address and port utility that monitor the MCast section of the mRcv.ini file. The only portion of the mRcv.ini file that can be modified is the [MCast] section at the bottom of the file. The port numbers listed within the section bordered by the number (#) symbols in the mRcv.ini file are for reference only and list all of the acceptable port numbers that you can use in your test.

The IP address field must be the multicast IP address of the Contact Center Manager Server. The port number corresponds to the port number of the statistic that you want to test.

For example, to test receipt of Skillset - Interval to date data using mRcv.exe, check the port number for Skillset - Interval to date in the mRcv.ini file, and then change the port number for Skillset - Interval to date in the mRcv.ini file, and then change the Port=setting in the [MCast] section to that port number. If Skillset - Interval to date = 6040 in the mRcv.ini file, the [MCast] section of the mRcv.ini file must be modified as follows:

```
[MCast]
IP=234.5.6.7
Port=6040
```

Procedure

1. On Contact Center Manager Server, choose **Start** > **All Programs** > **Accessories** > **Windows Explorer**.
2. Navigate to the folder

   `<drive>:\Avaya\Contact Center\Manager Server\iccm\bin\mRcv.ini`.
3. Using a text editor, open mRcv.ini.
4. In the mRcv.ini file, modify the IP address or the port number or both.
5. Save the mRcv.ini file.
6. Click **Start** > **All Programs** > **Accessories** > **Windows Explorer**.
7. Navigate to the folder <drive>:\Avaya\ Contact Center\Manager Server\iccm\bin.
8. Double-click mRcv.exe.

The mRcv.exe utility opens in a console window. If data is multicasted out, the command prompt window is populated with incoming data from the port and IP address that you specified in the mRcv.ini file. All non-RSM data is identified as “Not recognized by RSM”.

9. If you want to save the mRcv.exe utility data, run mRcv.exe from the command prompt `<drive>:\Avaya\Contact Center\Manager Server\iccm\bin \mRcv.ini>log.txt`.

   The log file with the name log.txt is saved in the same folder as mRcv.exe.

Troubleshooting if no data is multicasted out

About this task

Troubleshoot if no data is multicasted out by ensuring that all types of statistics are selected in the MulticastCtrl.exe file.

Updates do not take effect until the Contact Center Manager Server Statistical Data Processor (SDP) service is restarted.

Procedure

1. Select **Start** > **All Programs** > **Accessories** > **Windows Explorer**.
2. Navigate to the folder `<drive>:\Avaya\Contact Center\Manager Server\iccm \bin`.
3. Double-click **MulticastCtrl.exe**.
4. In the RTD Multicast controller window, ensure that all types of statistics are selected.
5. Click **Apply**.

Interpreting Real-time Statistics Multicast error messages on the client PC

About this task

Troubleshoot when error messages appear on the client PC by reviewing and interpreting the message.

When you first launch a display and the system is retrieving data, an icon appears on the display, indicating whether the Contact Center Manager Administration server supports multicast clients, unicast clients, or both.

A unicast session is defined as a single data stream between the CCMA server and the client.There are a maximum of twelve possible sessions between the server and a client, two for each of the data types agent, skillset, application, nodal, IVR and route. The two sessions available are interval-

to-date and moving window. Multiple displays that use the same data stream running on a client share a stream e.g a skillset tabular and skillset graphical display share a session.

Multicast communication transmits messages to multiple recipients at the same time. Multicast transmits only one stream of data to the network where it is replicated to many receivers.

After the display is launched, the icon indicates the transmission mode that is being used to launch the display. M–multicast, U–unicast.

Procedure

Review the error message and interpret it using Real-time Statistics Multicast error messages on page 179.

Procedure job aid

Table 6: Real-time Statistics Multicast error messages

Error message	Description
No unicast sessions available	This error normally appears on a client computer when an attempt to open a unicast channel fails and the client is not receiving multicast data. The absence of a unicast icon indicates that the unicast connection was not successfully established and the client PC is not receiving data packets. You must close the display and try to launch it again later. If the problem persists, you might need to increase the number of unicast connections that the Contact Center Manager Administration server allows, if prior engineering analysis permits this.
No relevant data	This error normally appears on a client computer when it is receiving data, but the data is not relevant for the current display (for example, when the information is not available within the user partitions or the current filter blocks the data from the display). The presence of the unicast icon indicates that a unicast connection was successfully established and the client PC is receiving data packets.
No data is available on the network	This window appears on a client computer when it is not receiving any data. There is no icon at the top of the window, indicating that the display is not receiving any data. The Transmit Mode = Multicast note implies that the server supports only multicast, but, in this case, the client PC is not receiving multicast data. This can be the result of a network problem, or it can mean that the server can support unicast, but it has not been enabled. Report the problem to your administrator to check the Contact Center Manager Administration server settings and enable unicast, if necessary.
The characters * and 0 appears in the display	Occasionally, the statistics in a real-time display might stop updating and the characters * and 0 appear instead of the variable fields. In a unicast environment, this indicates that the server has stopped sending data to this client. You must close and reopen the display. In a multicast environment, this can indicate that the server is no longer sending the multicast stream. If the problem persists, you need to run a trace on the Contact Center Manager Administration server.

Displaying Agent Real-time displays with a Gigabit NIC card

Before you begin

- Ensure that your contact center is not busy; if possible, perform this procedure when your contact center is not open.

About this task

Troubleshoot when no Agent Real-time display appears due to problems with the Gigabit NIC card. A Real-time display issue occurs when the Receive Side Scaling (RSS) feature is enabled on the Gigabit NIC card. Multicast data cannot be received by Contact Center Manager Administration. You need to disable the RSS feature to view the Agent Real-time display.

Procedure

1. On the Contact Center Manager Administration server, choose **Start** > **Control Panel** > **Network and Internet** > **Network Sharing Center**.
2. Click **Change adapter settings**.
3. Right-click the Gigabit NIC card and click **Properties**.
4. In the Local Area Connection Properties window, on the **Networking** tab, click **Configure**.
5. In the Gigabit NIC card properties page, click the **Advanced** tab.
6. Click **Receive Side Scaling**, and confirm that it is **Disabled**.
7. Click **OK**.

Displaying Real-time data

About this task

Troubleshoot when opening a Real-time display and no data appears.

You need to check the following:

- On the Contact Center Manager Administration server, the Contact Center Manager Server IP address can be resolved correctly to the server name.
- On the Contact Center Manager Administration server, the Contact Center Manager Server name can be resolved correctly to the expected IP address.
- On the Contact Center Manager Server, the RSM Compression option has not been selected in the RTD Multicast Controller window. If this option is selected during configuration, real-time displays and Agent Desktop Displays do not function in Contact Center Manager Administration.

Procedure

1. On the Contact Center Manager Administration server, click **Start** > **Run**.

2. Type `cmd`.
3. Click **OK**.
4. In the Command Prompt window, type `ping <Contact Center Manager Server name>`.
5. Press `Enter`.

   The Contact Center Manager Server IP address and the packets sent and received are displayed. If unexpected results are returned, check your DNS setting and the local host file on the server for incorrect entries.
6. In the Command Prompt window, type `ping <Contact Center Manager Server IP address>`.
7. Press `Enter`.

   The Contact Center Manager Server name and the packets sent and received are displayed. If unexpected results are returned, check your DNS setting and the local host file on the server for incorrect entries.
8. On the Contact Center Manager Server, choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Multicast Stream Control**.
9. In the RTD Multicast Controller window, deselect the **RSM Compression** option.
10. Click **Apply**.
11. Click **OK**.
12. Close all windows.
13. Stop and start the Statistical Data Propagator (SDP) service, to activate the new RSM settings on the Contact Center Manager Server.

Launching Real-time displays with negative values or long data strings

About this task

Troubleshoot when Real-time displays cannot launch and other displays that can launch display negative values or long data strings. If you select the RSM Compression check box when you configure Contact Center Manager Server, Real-time displays and Agent Desktop Displays do not function in Contact Center Manager Administration. On the Contact Center Manager Server, ensure that the RSM Compression check box is clear in the RTD Multicast Controller window.

Procedure

1. On the Contact Center Manager Server, choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Multicast Stream Control**.

2. In the RTD Multicast Controller window, in the **Compression** section, deselect the **RSM Compression** option.
3. Click **Apply**.
4. Click **OK**.
5. Close all windows.
6. Stop and start the Statistical Data Propagator (SDP) service, to activate the new RSM settings on the Contact Center Manager Server.

Displaying names in Real-time displays

About this task

Troubleshoot when no names (for example, agent names, answering skillset names, route names, IVR queue names, skillset and application names) appear in Real-time displays. Names appear as *UNKNOWN*, or they appear incorrectly in the Real-time displays. If this happens, there might be a problem with one or more of the following:

- permissions in IIS
- network settings
- configuration of the DNS server
- delays in the network
- information storage in the RTD cache

Procedure

1. Verify that Contact Center Manager Server is running. Check the Windows Event Viewer log for network errors.
2. Check that IIS permissions are correctly configured. See Checking that IIS permissions are correctly configured on page 183.
3. Set the IP address field in IIS to All Unassigned. See Setting the IP address field in IIS to All Unassigned on page 184.
4. Check address configurations for Host Headers. See Checking address configurations for Host Headers on page 184.
5. Ensure the anonymous user account has the correct permissions. See Ensuring the anonymous user account has the correct permissions on page 185.
6. Verify that the information cache stored in the Contact Center Manager Administration server exists and contains the correct information. See Verifying the RTD information cache is storing correct information on page 185.

Displaying new agents as *UNKNOWN* in Real-time displays

Before you begin

- Ensure that you know the ports that are being used by all Avaya and third-party products installed on your network.

About this task

Troubleshoot when a new agent is added but appears as *UNKNOWN* in Real-time displays.

This problem occurs if you install Veritas Backup Exec and use the default settings. The default installation of Veritas Backup Exec uses the TCP port 10000, which is the default port that the Avaya Aura® Contact Center Web Client Toolkit NameService uses. This port conflict results in Web Client errors that require you to restart the ICERTD Service to refresh the cache. To avoid this port conflict, you must change the default port that Veritas Backup Exec uses before you use the application.

Procedure

1. Change the default port in use by Veritas Backup Exec to a port that is not being used by any Avaya or third-party product installed on your network.
2. Verify that a port conflict no longer exists by using Veritas Backup Exec and then viewing the Real-time displays.

   If new agents still appear as *UNKNOWN*, contact Avaya support.

Checking that IIS permissions are correctly configured

About this task

Check that IIS permissions are correctly configured if names are not appearing in Real-time displays.

Procedure

1. On the Contact Center Manager Administration server, type the following in the Internet Explorer address bar: `http://localhost`

   If IIS is configured correctly, you see the logon page. If the following error appears, IIS permissions are configured incorrectly, and you need to go to step 2 of this procedure: `HTTP 403.6 - Forbidden: IP address rejected.`
2. If an error message appeared after Step 1, choose **Start** > **Administrative Tools** > **Internet Information Services (IIS)**.
3. In the left pane of the Internet Information Services (IIS) Manager window, click the plus (+) sign next to **<Computer_Name>** for the local computer.

   The heading expands and a series of folders appears.

4. Click **Default Web Site.**
5. Select the Default Web Site main window.
6. In the **IP Address and Domain Name Restrictions** section of the window, click **Edit**.
7. In the IP Address and Domain Name Restrictions window, ensure that the local host address 127.0.0.1 is added to the list of allowed computers.
8. Click **OK**.

Setting the IP address field in IIS to All Unassigned

About this task

Set the IP address field in IIS to All Unassigned if names are not appearing in Real-time displays.

Procedure

1. On the Contact Center Manager Administration server, choose **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager.**
2. In the left pane of the Internet Information Services (IIS) Manager window, click the plus (+) sign next to **<Computer_Name>** for the local computer.

   The heading expands and a series of folders appears.
3. Right-click **CCMA Web Site** and then select **Properties** from the menu.
4. In the CCMA Web Site Properties window, in the IP address list, ensure that **All Unassigned** is selected.
5. Click **OK**.

Checking address configurations for Host Headers

About this task

Check address configurations for Host Headers if names are not appearing in Real-time displays.

Procedure

1. On the Contact Center Manager Administration server, choose **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. In the left pane of the Internet Information Services (IIS) Manager window, click the plus (+) sign next to **<Computer_Name>** for the local computer.

   The heading expands and a series of folders appears.
3. Select **Default Web Site** and then click **Edit Binding**.

4. In the Site binding window, an entry appears for the * address only and the **Host Name** field is empty. If the **Host Name** field is populated, or if entries for IP addresses other than * appear, you must have an entry for localhost.
5. Click **OK**.

Ensuring the anonymous user account has the correct permissions

About this task

Ensure that the anonymous user account has the correct permissions if names are not appearing in Real-time displays. If your anonymous user account was modified, this can cause *UNKNOWN* to appear in standard agent display. If the user specified is not the Default user, then the new user must have access to all of the files under the <Install drive>\Avaya\Contact Center\Manager Administration\Apps folder. The user must be able to access the “common\soaplisten” files.

Procedure

1. On the Contact Center Manager Administration server, choose **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. In the left pane of the Internet Information Services (IIS) Manager window, click the plus (+) sign next to **<Computer_Name>** for the local computer.

   The heading expands and a series of folders appears.
3. Select **Default Web Site** and then open **Authentication**.
4. In the Authentication window, select click **Anonymous Authentication** and then click **Edit**.
5. Ensure that the anonymous user is a member of one of the groups with access to the required files, specifically common\soaplisten files.
6. Click **OK**.

Verifying the RTD information cache is storing correct information

About this task

Verify that the RTD information cache stored on the Contact Center Management Administration server is storing the correct information if names are not appearing in Real-time displays.

Procedure

1. Log on to the Web client as the webadmin user.

2. In Internet Explorer, go to `http://<app_srv_name>/supportutil/rtdcache.asp` where <*app_srv_name*> is the URL of the application server.
3. Enter the name of the Contact Center Manager Administration server.

   The following information populates the window:

   - a list of active unicast clients
   - details of the data in the agent cache
   - details of the agent template cache
   - details of the skillset template cache
   - details of the application template cache
   - details of the IVR template cache
   - details of the route template cache
   - details of the nodal template cache
4. If the correct information is not displayed, there is a problem with the RTD cache. Contact your administrator.

   OR

   If the correct information is displayed, the RTD cache is not the problem. Contact Avaya support.

Displaying sites in Network Consolidated Real-Time Displays

About this task

Troubleshoot when a networked site does not appear in the Network Consolidated Real-Time Display.

This can occur if a server is added by IP address instead of by name. If a server is added by IP address, the nodal displays for the site do not function correctly.

Another reason for this problem can be that the Network Consolidated Real-Time Displays do not display data for a Contact Center Manager site configured on the Contact Center Manager Administration server with a fully qualified hostname (for example, CCMS_test1.enterprise.europe.Avaya.com).

Procedure

1. If necessary, modify the server configuration to ensure that the server is added by name.
2. If necessary, modify the server configuration to use a non-fully qualified hostname (for example, CCMS1_test1).

Validating the number of contacts waiting in an RTD against a query result

About this task

Troubleshoot if the number of contacts waiting in an application or skillset Real-time display does not match the Agent Desktop Contact Query result. This can occur for several reasons.

- If a contact routes to a site where no agents are logged in for a skillset, then the contact counts against the application but not against the skillset.
- A contact that an agent reschedules, so that it is no longer queueing to a skillset, counts against the application but not against the skillset.
- The an agent might have transferred the contact to a different skillset than that initially set by Contact Center Multimedia rules.
- The flow application or script might not treat the contact with “queue to skillset”, but instead treats the contact with “queue to agent”.
- The flow application or script might be queuing to multiple skillsets.

Procedure

To determine the number of calls or email messages waiting, view the appropriate application or skillset Real-time display.

Managing memory leaks in Agent RTD when running Internet Explorer 8.0

About this task

A memory leak occurs in the iexplore.exe file when you are running traffic and generating Agent Real-time displays when you use Internet Explorer 8.0.

Procedure

1. In Internet Explorer 8, choose **Tools** > **Internet Options**.
2. Click the **Advanced** tab.
3. Clear the check box beside **Disable Script Debugging (Internet Explorer)**.
4. Clear the check box beside **Disable Script Debugging (Other)**.
5. Click **OK**.

Launching multiple RTD displays

About this task

When your first browser launches a RTD display, the second browser cannot launch the same type RTD display (private or public). The error code 4097 - Transmission error appears in the second browser window.

Unicast has this limitation. It supports only one instance of the browser. The second instance of the browser attempts to use the IP from the first instance.

Procedure

Only use one browser to review unicast data in your system.

Connecting to the data source

About this task

Troubleshoot when you try to run historical reports and you receive an error message in the ad hoc report preview window indicating “There is a problem connecting to the data source.”

This problem can occur if the bindings order of the ELAN subnet network card and the contact center server subnet network card on the Contact Center Manager Server are not set up correctly. This problem can also occur if you do not refresh your server.

Procedure

1. Ensure that you configure the bindings order of the network interface cards so that the contact center server subnet card comes first, then the ELAN subnet card, and then the virtual adapters for remote access.
2. If necessary, refresh your server. See Refreshing servers on page 118.

Editing the sysadmin password in Contact Center Manager Administration

About this task

Edit the sysadmin password in Contact Center Manager Administration using the following procedure.

Procedure

1. Log on to Contact Center Manager Administration.
2. Open the **Configuration** component.

3. In the left pane, right-click the Contact Center Manager Server that is experiencing the problem.
4. Click **Edit Properties**.
5. In the **Login ID** box, change the Login ID to `sysadmin`.
6. In the **Password** box, type the same sysadmin password that is defined on Contact Center Manager Administration.
7. Click **Submit**.
8. Refresh the same Contact Center Manager Server.
9. On the system tree, click the Contact Center Manager Server.
10. On the menu bar, select **Server** > **Refresh Server**.
11. Click **Yes**.
12. Click **Yes**.
13. On the Launchpad, select **Logout**.
14. Log back on to Contact Center Manager Administration.

Editing the sysadmin password using Server Utility

About this task

Edit the sysadmin password using Server Utility with the following procedure.

Procedure

1. Using the Server Utility, log on to Contact Center Manager Server.
2. Double-click **User Administrator** > **Users** screen.
3. Double-click on the name of the user that logs on to the server through Contact Center Manager Administration. The Login ID of this user is configured in the Desktop tab and is the same as the Login ID configured in the Server Properties page on Contact Center Manager Administration.
4. Click the **Desktop** tab, and note the access class of the user.
5. Use Server Utility to delete this user.
6. Redefine this user, using the same Login ID, Password, and access class.
7. Log on to Contact Center Manager Administration.
8. Open the **Configuration** component.
9. Refresh the same Contact Center Manager Server.
10. On the system tree, click the Contact Center Manager Server.

11. On the menu bar, select **Server** > **Refresh Server**.
12. Click **Yes**.
13. Click **Yes**.
14. On the Launchpad, select **Logout**.
15. Log back on to Contact Center Manager Administration.

Printing scheduled reports

Before you begin

- Ensure that you are logged on as a user with administrator privileges.

About this task

Troubleshoot when you cannot print scheduled reports from the Historical Reporting component.

Procedure

On the Contact Center Manager Administration server, add and configure a local printer.

Synchronizing user-imported reports because network drive access is denied

Before you begin

- Ensure that you know whether Contact Center Manager Administration is on a workgroup or a domain.

About this task

Troubleshoot when you cannot synchronize user-imported reports and network drive access is denied. This problem occurs because the Contact Center Manager Administration account is unable to read the report template on the network drive.

This can occur due to the following reasons:

- You have not shared the source report folder on the network drive with read permissions, for the Contact Center Manager Administration account.
- You have configured the Contact Center Manager Administration on a workgroup and the network PC is on a domain, or vice-versa.

You need to verify network access. The verification process is different for Contact Center Manager Administration on a workgroup and Contact Center Manager Administration on a domain.

Procedure

1. If Contact Center Manager Administration is on a workgroup, on the Contact Center Manager Administration server, go to the MS-DOS prompt and run the **net use** command as follows:

   ```
   NET USE \\<computername>\<sharename> password of iceAdmin /
   USER:iceAdmin
   ```

   If you cannot map a network drive, check the permission on the report folder on the network drive.

   If you can map a network drive, but the synchronization status displays the message "Access denied on the network drive, contact Avaya support".

2. If Contact Center Manager Administration is on a domain, go to the MS-DOS prompt and run the **net use** command as follows:

   ```
   NET USE \\<computername>\<sharename>password of IIS domain account /
   USER:domain name\IIS Domain Account Name
   ```

   If you cannot map a network drive, check the permission on the report folder on the network drive.

   If you can map a network drive, but the synchronization status displays the message "Access denied on the network drive, contact Avaya support".

Synchronizing user-imported reports because cannot copy to CCMA server

About this task

Troubleshoot when you cannot synchronize user-imported reports and you cannot copy to the Contact Center Manager Administration server.

This can occur for either of the following reasons:

- The report is being run while you are trying to synchronize it.
- The report template file that was copied during the last successful synchronization had read-only attributes on the network folder.

Procedure

1. Ensure that the report is not running.
2. Change the attributes of the report template on the network drive to ensure that it is not read-only, and then save the report in Crystal software.
3. On Contact Center Manager Administration server, run the Synchronize User Imported Report Templates again.

Importing user-created report templates because of ASP script timeout error

Before you begin

- Install Crystal Reports on your local hard drive.

  Note:

  Do not install Crystal Reports software on the Contact Center Manager Administration Server.

Note:

Contact Center Manager Administration installs and uses Crystal Reports Server Embedded 2008 or later. You can generate Contact Center reports using Crystal Reports client software compatible with Crystal Reports Server Embedded 2008 or later.

About this task

Troubleshoot when you cannot import user-created report templates because of an ASP script timeout error. If the report templates were created in Crystal Reports 8.5 or earlier, and because Crystal Reports 9 onwards are Unicode-compliant, this can cause a delay or failure when importing and generating reports on Contact Center Manager Administration.

If you receive an ASP script timeout error when you attempt to import user-created report templates, you need to re-save any report templates that cannot be imported.

To import user-created Crystal Reports templates into CCMA, you must save the templates on your local hard drive.

Procedure

1. On the same PC on which you installed Crystal Reports, create a new directory named *<OldVersionTemplates>*.
2. Copy all custom report templates created in Crystal Reports 8.5 or earlier versions into the *<OldVersionTemplates>* directory.
3. Create a *<NewVersionTemplates>* directory to save the updated templates.
4. Start Crystal Reports.
5. Select **File** > **Open**.
6. Select the *<OldVersionTemplates>* directory.
7. Select the required report file and click **Open**.
8. Select **File** > **Save As**.
9. Navigate to the *<NewVersionTemplates>* folder.
10. Click **Save**.

    To save additional Crystal Report templates, repeat step 5 on page 192 through step 10 on page 192 for each of the report templates in the *<OldVersionTemplates>* directory.

11. After you have resaved all of the old report templates into the *<NewVersionTemplates>* directory, copy the *<NewVersionTemplates>* folder to the desired PC from which you want to import the report templates.

Retrieving large number of agents for Historical Reports

About this task

Troubleshoot when you access the Historical Reporting component and attempt to retrieve a large number of agents in the selection criteria and a blank list is returned.

Procedure

In the Real-Time Reporting settings, increase the OAM Timeout value (for example, set the OAM Timeout value to 40000 for 4000 configured agents).

Obtaining a license to open a Report Creation Wizard session

About this task

Troubleshoot when you cannot obtain a license to open a Report Creation Wizard session. Check the License Manager Service configuration and look for Windows Event log entries with an LMService source.

Check with the Contact Center Manager Server administrator for the License Manager interface log file name and location.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
2. Click **LMService Configuration**.
3. Verify that the License Manager Server IP address and port numbers are correct.
4. Click **OK** to submit your changes, if any.
5. In the Windows event log, look for any entries with a source of `LMService`.
6. From the Contact Center Manager Administration install directory (or the directory indicated by the Contact Center Manager Server administrator), and using a text editor, open the log file `CCMA_LMService_1.log`.
7. Review and note any entries.
8. Close the `CCMA_LMService_1.log` file.

Finding Access and Partition Management information

About this task

Troubleshoot when you cannot find Access and Partition management information after you restore your backup file of Contact Center Manager Administration data. This occurs when you use the Windows Backup Utility to create your backup file and two of the AD-LDS files do not back up successfully.

You must ensure that the following AD-LDS files are included for all users in the Windows Backup Utility, and then you must backup and restore your Contact Center Manager Administration data again:

- `C:\Program Files (x86)\Microsoft ADAM\instance1\data\adamntds.dit`
- `C:\Program Files (x86)\Microsoft ADAM\instance1\data\ebd*.log`

Procedure

1. Click **Start** > **All Programs** > **Accessories** > **System Tools** > **Backup**.

   The Backup and Restore Wizard appears.
2. Click **Advanced Mode**.
3. Click the **Restore and Manage Media** tab.
4. In the Restore and Manage Media window, in the left-hand pane, expand the backup file that you use to restore your Contact Center Manager Administration data files by clicking the plus (+) sign next to the media item.
5. In the expanded list of the Contact Center Manager Administration backup files, ensure that the following files are listed:
   - `C:\Program Files (x86)\Microsoft ADAM\instance1\data\adamntds.dit`
   - `C:\Program Files (x86)\Microsoft ADAM\instance1\data\ebd*.log`
6. If the two AD-LDS files in step 5 appear in the expanded list, go to step 12.

   If the two AD-LDS files in step 5 do not appear in the expanded list, go to step 7.
7. In the Windows Backup Utility, click **Tools** > **Options**.
8. In the Options window, click the **Exclude Files** tab.
9. In the Exclude Files window, under **Files excluded for all users** select the following AD-LDS files and click **Remove**:
   - `C:\Program Files (x86)\Microsoft ADAM\instance1\data\adamntds.dit`
   - `C:\Program Files (x86)\Microsoft ADAM\instance1\data\ebd*.log`
10. Click **OK**.
11. Close all windows to exit the Windows Backup Utility.

12. Create a new backup file of your Contact Center Manager Administration data files, and restore the backup file again. Ensure that the following two files are selected when you perform the backup:
    - `C:\Program Files (x86)\Microsoft ADAM\instance1\data\adamntds.dit`
    - `C:\Program Files (x86)\Microsoft ADAM\instance1\data\ebd*.log`

Viewing agents or skillsets

About this task

When you cannot view available agents and skillsets in the User Defined Partition view, agent or skillset information might not display. If a server that is not fully operational is listed for this partition, then agent or skillset information for remaining servers might not display properly.

Procedure

Ensure that all servers configured on Contact Center Manager Administration are fully operational.

Viewing incomplete agents

About this task

If during the import of agents, the agents are not completely imported into the Contact Center Manager Administration application, they appear as grey icons.

You can filter the agent list by complete and incomplete agents.

You cannot modify the incomplete agents; you must delete them.

Procedure

1. Open the **Agents** page.
2. Select an incomplete agent.
3. Right-click, then choose **Delete**.

Troubleshooting when User Defined Historical Reports shows data for the day instead of the selected interval in reports migrated from earlier versions of Contact Center

About this task

Troubleshoot when a user defined historical report shows data for the day instead of the selected interval. This can happen when the data field used for data range filtering is a Date field and not a DateTime field because the report is using the Convert DateTime to Date feature which is not supported in AACC 6.0 or later.

You must verify the issue is caused by the data field being a Date Field instead of a DateTime field.

Procedure

1. On the Contact Center Manager Administration server, select **Start** > **Administrative Tools** > **Event Viewer**.
2. Expand the **Windows Logs** folder.
3. Select application.
4. Find **Event ID 61714** from **Source CCMADisplayReport** or **CCMAReportSevice**. The event provides the Date Field, Report Name, Report Group, Report User and Server Name.
5. Open the report in Crystal Reports.
6. Select **File** > **Report Options**.
7. In **Report Options**, select **To Date-Time** in the **Convert Date-Time** list.
8. Select the valid **ODBC Data Source** for the report.
9. If needed, provide a **User ID** and **Password** to access the data source.
10. Create a new formula to convert the datetime field back to date.

    For example, if the field used is the Timestamp from the iApplicationStat table, the formula is

    CDate({iApplicationStat.Timestamp})
11. Replace the current database field on the report with the new formula.
12. If groups are based on the same field, change the group to use the new formula field.

Troubleshooting when User Defined Historical Reports shows data for the day instead of the selected interval in reports in AACC using 3rd party databases

About this task

Troubleshoot when a user defined historical report shows data for the day instead of the selected interval. This can happen when the data field used for data range filtering is a Date field and not a DateTime field, and the report was imported as an interval report, but the timestamp field selected is not a DateTime field.

You must verify the issue is caused by the data field being a Date Field instead of a DateTime field.

Procedure

1. On the Contact Center Manager Administration server, select **Start** > **Administrative Tools** > **Event Viewer**.
2. Expand the **Windows Logs** folder.
3. Select application.
4. Find **Event ID 61714** from **Source CCMADisplayReport** or **CCMAReportSevice**. The event provides the Date Field, Report Name, Report Group, Report User and Server Name.
5. Import the report selecting a **Report Data Range** other than **Interval** or select another **DateTime** field as the **Timestamp** field.

Troubleshooting when Contact Center Management No Supervisors Defined error messages occur

About this task

Troubleshoot when you receive No Supervisors Defined error messages after you add supervisors in Contact Center Management, exit the component, return to the component, and select the same server in Contact Center Manager Server on which you defined the supervisors, but the supervisors are not there.

This problem can occur when the bindings order of the ELAN subnet network card and the contact center server subnet network card on the server in Contact Center Manager Server are not set up correctly. You must configure the bindings order of the network interface cards so that the contact center server subnet card comes first, then the ELAN subnet card, and then the virtual adapters for remote access. Ensure that all Contact Center Manager Administration procedures are on the Contact Center Manager Server.

Procedure

1. On the Contact Center Manager Server, choose **Start** > **Control Panel** > **Network and Internet**.

2. Click **Network and Sharing Center**.
3. Click **Change adapter settings**.
4. In the Network Connections window, press `Alt`. A hidden menu displays.
5. From the **Advanced** menu, click **Advanced Settings**.
6. In the **Connections** box, ensure that the contact center server subnet connection is listed first. If it is not listed first, adjust the order to ensure that it appears first in the list.
7. Save your changes and close all windows.
8. Restart the Contact Center Manager Server.

Displaying long Column Names text and data in historical reports

About this task

Troubleshoot when you run a historical report and the Column Names text and data run over the line, making the report unreadable.

This problem is caused when the generic text printer installed on the Contact Center Manager Administration server conflicts with the historical report formatting.

Procedure

1. On the Contact Center Manager Administration server, remove the generic text printer.
2. Install a printer driver that is compatible with Crystal Reports (for example, the HP LaserJet 4000 Series).

Displaying last column in a historical report

About this task

Troubleshoot when you run an Agent Performance report and the last column of the report is cut off in the Ad hoc Crystal Report Viewer.

This problem is caused because the report does not fit on letter-size paper.

Procedure

1. Create a new default printer and change the paper size to Legal.
2. Print the Agent Performance report using the new default printer.

Displaying historical reports updates slowly

About this task

Troubleshoot when it takes a very long time for the list of agent IDs in the Selection Criteria pane to populate.

This problem can occur when the contact center server subnet address and the ELAN subnet address are both listed in the DNS entries for the Contact Center Manager Server.

Procedure

1. Check the DNS entries for the Contact Center Manager Server.
2. If both the contact center server subnet address and the ELAN subnet address are listed, remove the ELAN subnet address.

Troubleshooting when the scheduled report export fails on the network drive

About this task

Troubleshoot when the scheduled report export fails on the network drive. This problem occurs because the Contact Center Manager Administration scheduled report account (iceAdmin or the domain account) cannot write to the specified folder in the output file text box. This occurs for one of the following reasons:

- The scheduled report account or account password used for the shared folder on the client does not match the scheduled report account or account password on the Contact Center Manager Administration server.
- You specified an invalid path when scheduling the report.
- The network directory folder does not have read/change permissions.
- A network problem occurs when connecting to the directory folder.

To resolve the problem, use the iceAdmin Password Change Utility to reset the scheduled report account or account password. This resets all of the scheduled reports to use the correct account name and password when exporting reports.

To verify network access from Contact Center Manager Administration, use the scheduled report account (iceAdmin or the domain account) and password for this account to map the network drive to which the report is to be exported. Alternatively, you can use the net use command to verify whether you can map to the directory folder on the network drive from the Contact Center Manager Administration server.

Procedure

1. On the Contact Center Manager Administration server, go to the MS-DOS prompt and run the net use command as follows.

   If you use iceAdmin as your scheduled report folder, type:

```
NET USE \\<computername>\<sharename> password of iceAdmin /
USER:iceAdmin
```

If you use the domain account as your Scheduled report folder, type:

```
NET USE \\<computername>\<sharename>password of iceAdmin /
USER:<domain account name>
```

2. If you cannot map the network drive, check the permission on the report folder on the network drive. If you can map the network drive, try to create a file on the network folder.
3. If you cannot create a file on the network folder, check the share permissions on the network folder from the network PC. It must be set to Read/Change for the account that you have set up on the network PC.

   If you can create a file on the network folder, but the scheduled report export still fails, contact Avaya support.

Activating scheduled reports

About this task

Troubleshoot when you cannot activate scheduled reports in Contact Center Manager Administration.

This problem occurs when the Internet Information Services (IIS) default security account under anonymous access is not a member of the backup operators group, or if you need to reset your scheduled report account (iceAdmin or the domain account) password.

Procedure

Reset the scheduled report account or account password using the iceAdmin Password Change utility. See Resetting the scheduled report account or account password using the iceAdmin Password Change utility on page 200.

Resetting the scheduled report account or account password using the iceAdmin Password Change utility

Before you begin

- If you have a domain account, ensure that you know the domain account name and password. If necessary, contact your network administrator for this information.

About this task

Reset the scheduled report account or account password using the iceAdmin Password Change utility, if you cannot activate scheduled reports in Contact Center Manager Administration.

Procedure

1. On the Contact Center Manager Administration server, choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
2. In the left pane, click **Avaya**.
3. In the Avaya Applications Configuration window, click **IceAdmin Password Change**.
4. In the iceAdmin Password Change window, in the **Old Password** box, type the old password.
5. In the **New Password** box, retype the old password for the iceAdmin user account. This resets the iceAdmin password.
6. In the **Confirm Password** box, type the password again.

   If your Contact Center Manager Administration server is a member of an active domain, the Domain Account option is enabled on the iceAdmin Password Change window.
7. If you do not want to export scheduled reports to a domain account, or if the Domain Account button is disabled, go to step 12.

   OR

   If you want to export scheduled reports to a domain account, and the Domain Account button is enabled, click **Domain Account**.
8. From the **Select Domain Name** list, select the name of the domain to add.
9. In the **Enter Domain Account** box, type the domain account provided by your network administrator.
10. In the **Enter Domain Account Password** box, type the domain account password provided by your network administrator.
11. In the **Confirm Domain Account Password** box, type the domain account password again.
12. Click **OK**.

    The system verifies that you typed the same password both times, and then resets the password in all required components.
13. Close all windows.

Displaying and printing historical reports only in portrait orientation

About this task

Troubleshoot if the historical reports always display and print in portrait orientation even if the report template is designed for landscape mode. This can result in report data columns being truncated.

This problem is caused by a printer driver on the Contact Center Manager Administration server.

Procedure

1. On the Contact Center Manager Administration server, choose **Start** > **Devices and Printers**.
2. Select the **Microsoft Office Document Image Writer** printer, right-click and select **Remove device** from the menu.

Troubleshooting missing fonts in Report Creation Wizard

About this task

Troubleshoot when there are fonts missing from the font list on the Configuration Settings page and the Report Layout page in Report Creation Wizard.

The fonts that are available in Report Creation Wizard are the fonts that are installed on the Contact Center Manager Administration server. There are restrictions on the type of fonts available in Report Creation Wizard and fonts that do not meet these requirements are not available.

Procedure

Verify with the administrator that the fonts installed on the Contact Center Manager Administration server meet the following requirements:

- The font must be a TrueType font.
- The font must support the following styles: Regular, Bold, Italic, Underlined, and Strikethrough.
- The font must support ANSI or Symbol character sets. The font can also support other character sets.

Troubleshooting Configuration Tool problems

About this task

Troubleshoot Configuration Tool problems by ensuring that you do not exceed the restrictions and limits set in the Parameters tab of the Historical Statistics window in Contact Center Manager Server. For example, if you have a limit of 240 configured CDNs in the Historical Statistics, you cannot upload more than 240 CDNs using the Contact Center Manager Server Configuration Tool spreadsheet.

Procedure

1. On the Contact Center Manager Server, open the Historical Statistics window and note the limits set on the **Parameters** tab.
2. If you use a client PC to upload or download configuration data, ensure that the Contact Center Manager Administration application can be accessed from the client with the Contact Center Manager Administration Server Name.

3. Ensure that you are aware of the number of worksheet columns that your version of Microsoft Excel supports (for example, 256 columns). The number of agent to skillset assignments and agent to supervisor assignments that you can upload from the Configuration Tool spreadsheets is restricted to the maximum number of worksheet columns available in Microsoft Excel.
4. Open **Tools** > **Macro** > **Security** and ensure that the **Security level** is set to **Medium** and that **Macros** are enabled.

Receiving email notifications

Before you begin

- Ensure that you know the SMTP Server details. If necessary, contact your network administrator for this information.

About this task

Troubleshoot when email notifications are not received after a scheduled report succeeds or fails. The email address is defined for each report.

If the email was not sent, then the failure is logged in the Event Viewer on the Contact Center Manager Administration server.

Procedure

1. On the Contact Center Manager Administration server, select Start, Administrative Tools, Event Viewer.
2. In the left pane of the Event Viewer window, expand Windows Logs and select Application.
3. Select the event with the following details: **Level: Warning**, **Source: CCMAReportService**, **Event ID: 61706**.
4. In **Event Properties**, on the **General** tab, look for Email = <status> - <email To Address>, where that status can be **OK** or **Failed**.
5. If the email status is **OK**, confirm that the <email to Address> is correct.
6. If the email <status> is **Failed**, look for Error = Email: Failed to send email notification, which is followed by an error message. The following table provides details for known errors:
7.

Error message	Description
The remote name could not be resolved.	Confirm that the SMTP Server entered is correct.
Unable to connect to remote server.	Confirm that the SMTP Server and port entered are correct. If the CCMA server was entered as the SMTP Server, ensure the SMTP Server is installed and configured.
The SMTP server requires a secure connection or the client	The SMTP Server requires SSL. Update the email notification settings such that SSL Required is selected.

Error message	Description
was not authenticated. The server response was: 5.7.0 Must issue a STARTTLS command first.	
Mailbox unavailable. The server response was: 5.7.3 Requested action aborted; user not authenticated.	The User Name or Password entered for accessing the SMTP Server are invalid. Update the email notification settings with a valid email account and ensure the password is correct.

8. Repeat Step 3 on page 203 through Step 6 on page 203 for each event.

Upgrading Agent Desktop Display

About this task

Troubleshoot when you cannot upgrade Agent Desktop Display from Avaya Aura® Contact Center Web client to Contact Center Manager Administration on client PCs.

This problem can occur if you have proxy settings turned on when you attempt to upgrade Agent Desktop Display. You need to ensure that proxy settings are turned off before you upgrade Agent Desktop Display. If your network security policy requires, you must turn proxy settings back on after you complete the Agent Desktop Display upgrade.

Procedure

1. On Internet Explorer, choose **Tools** > **Internet Options**.
2. In the Internet Options window, on the **Connections** tab, click **LAN Settings**.
3. In the Local Area Network (LAN) Settings window, clear the checkbox next to **Use a proxy server for your LAN**.
4. Click **OK**.
5. Close all windows.

Displaying data in Agent Desktop Displays

About this task

Troubleshoot when you launch Agent Desktop Display and no data appears.

This problem can occur if you select the RSM Compression option in the RTD Multicast Controller window when you configure Contact Center Manager Server. If you select the RSM Compression option, real-time displays and Agent Desktop Displays do not function in Contact Center Manager Administration.

Procedure

1. On the Contact Center Manager Server, choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Multicast Stream Control**.
2. In the RTD Multicast Controller window, in the **Compression** section, deselect **RSM Compression**.
3. Click **Apply**.
4. Click **OK**.
5. Close all windows.
6. Stop and start the Statistical Data Propagator (SDP) service.

Installing Sybase Open Client 12.5

Before you begin

- Ensure that you have administrator privileges in Windows Server 2008.
- Use the same administrator account to log on to the Contact Center Manager Administration server each time you install a Contact Center Manager Administration component.

About this task

Install Sybase Open Client 12.5 to access and control the content of the Contact Center Manager Administration database.

Procedure

1. Log on to Contact Center Manager Administration server as the administrator.
2. Insert the Contact Center installation DVD into the DVD drive.
3. If the Contact Center DVD installer main menu appears, click **Cancel**.
4. Using Windows Explorer, browse in the DVD folder to **ThirdParty** > **Sybase Open Client**.
5. In the **Sybase Open Client** folder, double-click **setup.exe**.
6. Select **Standard Install**.
7. Click **Next**.
8. In the **Choose the installation directory** box, accept the default location.
9. On the Choose Directory dialog box, click **Next**.
10. On the Summary dialog box, click **Next**.
11. On the Create Directory dialog box, click **Yes** to confirm the name of the directory to which to copy the files.

12. If you upgrade to Sybase version 12.5, the system asks if you want to overwrite the following existing Sybase.DLL files. Click **Yes** when prompted to replace or reinstall these Sybase files:
    - Replace mchelp.dll version 12.0 with version 12.5.0.0
    - Replace mclib.dll version 12.0 with version 12.5.0.0
    - Replace Language Modules version 12.0 with version 12.5
    - Reinstall Component Sybase Central 3.2.0
13. If the system prompts you to replace the optional Power Dynamo file, click **Yes**. Replace the optional Power Dynamo file, replace version 3.0.0 with version 3.5.2.
14. If the system prompts you to replace any other DLLs, including system DLLs, such as msvcrt40.dll version 4.20, click **No**. Do not replace any system DLLs.
15. A message box appears that states the system does not need this update. Click **OK**.
16. On the Sybase Installer Confirmation dialog box, click **Yes** to restart the system before you configure the installed components.
17. Click **OK**.
18. Close the Control Panel window.

Updating the Sybase ODBC driver

Before you begin

- Install Sybase Open Client 12.5.

About this task

Update the Sybase Database Connectivity (ODBC) driver to ensure that you use the latest version.

Procedure

1. Click **Start** > **Run**.
2. In the **Open** box, type `cmd`.
3. Click **OK**.
4. At the prompt, type `iisreset`.
5. Press `Enter`.
6. At the **MS-DOS** prompt, navigate to the root directory of the Sybase folder on the DVD.

   For example, `<x>: \ThirdParty` (*<x>* is the location of the DVD).
7. Change to the directory containing the Sybase Open Client hotfixes.

   For example, **`cd Sybase Open Client – Hotfixes`**.
8. Type the following **`xcopy`** command:

```
xcopy EBF11113\*.* %SYBASE% /S /E /V /Y > C:\EBF11113.TXT
```

9. Press `Enter`.

Variable definitions

Name	Description
EBF11113	The directory containing the Sybase ODBC driver.
<*SYBASE*>	The environment variable containing the directory location of the Sybase Open Client 12.5 software installed on the Contact Center Manager Administration server (for example, `c:\sybase`).
`C:\EBF11113.TXT`	The log file that you can use to verify that all the files are copied correctly.

Verifying that the system successfully updated the driver

Before you begin

- Update the Sybase ODBC driver. See Updating the Sybase ODBC driver. on page 206

About this task

Verify that the system successfully updated the Sybase ODBC driver to ensure that the Contact Center Manager Administration server software can interact with the database.

Perform this step only if you plan to use a Contact Center Manager Server Release 6.0 to report statistics.

Procedure

1. On the target server, browse to `C:\Windows\SysWOW64`.
2. Double-click **ODBC Data Source Administrator** to start the 32-bit version of the driver.
3. In the ODBC Data Source Administrator dialog box, click the **Drivers** tab.
4. On the **Drivers** page, scroll down until you locate the correct **Sybase ASE ODBC** driver, which is **4.10.00.49**.
5. Click **OK**.
6. If the ODBC driver version is not 4.10.00.49, open the log file `C:\EBF11113.txt` to see any error messages were recorded during the xcopy command.

Chapter 21: Agent and Supervisor configuration troubleshooting

Avaya Aura® Contact Center automatically audits the agent and supervisor configuration data for discrepancies. The agent validation audit does not require user interaction or configuration; it runs automatically for two intervals each day at 11:00 AM and 11:00 PM. Avaya Aura® Contact Center reports any detected discrepancies in the Contact Center Manager Server database to the contact center Administrator. Avaya Aura® Contact Center also generates Invalid Agent Audit report data and stores the data in Contact Center Manager Server database views accessible to the customer for reporting. The agent validation audit is performed by the CCMS HDM Service.

When an agent or supervisor configuration discrepancy is detected:

- Avaya Aura® Contact Center raises a MS Windows event (EventID 64141). The event is also sent as a Simple Network Management Protocol (SNMP) trap. The contact center Administrator can register to receive notification of this event.
- If High Availability email notification is configured, Avaya Aura® Contact Center sends an email message to the configured Administrator email address.
- Avaya Aura® Contact Center stores the details of the discrepancy in the Invalid Agent Audit report data. The contact center Administrator can use this data to actively look for agent and supervisor configuration data discrepancies.

When a configuration data discrepancy is reported or detected, contact Avaya Support and ask them to run the *Agent Configuration Validation Tool* to fix the discrepancies.

You can manually fix some of the more basic discrepancies using Contact Center Manager Administration. For example, you can fix agent first name, last name, and Telset Login ID discrepancies.

The agent and supervisor configuration data is automatically audited for the following anomalies:

Anomaly Detected	Description
ContactTypesByAgent: Agent not in NIUser	The agent has contact types, but does not have a Login ID and User Type.
ContactTypesByAgent: ContactType not in NIContactTypes	The agent has an invalid Contact Type.
ConactTypesByAgent: Has deleted ContactType	The agent has a deleted Contact Type.
SkillsetByAgent: Agent not in NIUser	The agent has skillsets, but does not have Login ID and User Type.

Anomaly Detected	Description
SkillsetByAgent: Skillset not in NISkillset	The agent has an invalid skillset.
SkillsetByAgent: Has deleted Skillset	The agent has a deleted skillset.
URIByAgent: UserID not in NIUser	The agent has a URI, but does not have Login ID and User Type.
URIByAgent: Has Duplicate URI	The agent has a duplicate URI.
URIByAgent: URI Type is invalid	The agent has a URI with invalid type i.e. not a Voice, IM or CTI URI type.
URIByAgent: Agent URI assigned to CDN	The agent has a URI that is also defined as a CDN URI.
SupervisorAgent: Agent not in NIUser	The agent has a Supervisor, but does not have Login ID and User Type.
SupervisorAgent: Supervisor not in NIUser	The supervisor has an agent, but does not have Login ID and User Type.
SupervisorAgent: Supervisor Invalid Type	The supervisor record has an invalid supervisor type. Valid value="P".
SupervisorAgent: Agent Has multiple Supervisors	The agent has multiple supervisors in Supervisor Agent.
NIUser: UserID not in NBUser	The user has a LoginID, User Type but does not have personal detail e.g. Name.
NIUser: UserType Invalid	The user Type not defined as one of the following: Agent, Expert, Supervisor, Supervisor/Agent, Supervisor/Expert.
NIUser: Agent not in SkillsetByAgent	The agent has no skillsets.
NIUser: Agent not in UriByAgent	The agent has no URI. (SIP-enabled solution only.)
NIUser: Agent not in SupervisorAgent	The agent has no supervisor.
NIUser: Agent not in ContactTypesByAgent	The agent has no contact types.
NIUser: Supervisor Has Skillsets	Supervisor has skillsets.
NIUser: Supervisor Has ContactTypes	Supervisor has contact types.
NIUser: TelsetLoginID Invalid	Empty, or invalid Agent login id.
NIUser: TelsetLoginID Assigned multiple agents	Duplicate Agent login id.
NIUser: LocalUserID Invalid	Internal Local UserID value is invalid e.g. blank or null.
NIUser: LocalUserID Assigned multiple agents	Internal Local UserID value is assigned to multiple user records.
NBUser: UserID Not Agent, Supervisor or Desktop User	User has master record, but not configured as Agent, Supervisor or desktop user.
NBUser: Invalid First Name	User first name has invalid characters. There is a leading space or tab in the name.
NBUser: Invalid Last Name	User last name has invalid characters. There is a leading space or tab in the name.

Anomaly Detected	Description
PCUserUser: UserID not in NBUser	A desktop user has no master record. There is no name defined for the user.
GroupUserMapping: UserID not in NBUser	A user with access class has no master record. There is no name defined for the user.
AgentByTaskFlow: UserID not in NIUser	A Task Flow/Script is referencing an invalid Agent.
AgentByTaskFlowVariable: UserID not in NIUser	A script variable is referencing an invalid agent.

Creating a User Validation Status report

Before you begin

- When creating an external report, configure the Cache DSNs on your client PC for Contact Center Manager Server.
- To create a Report Creation Wizard Advanced ODBC report, use the ODBC DSN created by Contact Center Manager Administration (CCMA).

About this task

Create a User Validation Status report so that you can monitor the agent and supervisor configuration data for discrepancies. You can use the follow views to create an advanced Report Creation Wizard report:

- dbo.UserValidationStatus – Contains the data from the last run.
- dbo.UserValidationReport – Contains the data for the last 24 hours.

Report Creation Wizard is a Web-based interface in which you can create reports. You can access the Report Creation Wizard from the Historical Reporting component of Contact Center Manager Administration.

If no data is returned from the views, the agent and supervisor configuration data is valid and does not contain any detectable discrepancies.

Procedure

1. Log on to Contact Center Manager Administration.
2. From the **Launchpad**, click **Historical Reporting**.
3. In the left pane, click the Contact Center Manager Server on which to create, edit, or view the Report Creation Wizard report.
4. From the **Report** menu, select **Report Creation Wizard**.
5. In the **Report Type** window, select the Create Advanced Report (via ODBC) option.
6. In the **Data Source** window, from the **DSNs Available** list, double-click on an appropriate CCMS DSN.

   The selected DSN moves to the **DSNs Selected** list.

7. The **User ID** and **Password** boxes automatically contain the values you enter during the server configuration.
8. Click **Next**.
9. In the **Table Selection** window, from the **Tables Available** list, double-click a table. The table moves from the **Tables Available** list to the **Tables Selected** list. Double-click **UserValidationStatus**.
10. Click **Next**.
11. In the **Field Selection** window, in the **Fields** list, double-click a field to add to the report.

    Select the following fields:

    - InvalidCode — Description of anomaly reported on the Agent/Supervisor record in the database
    - IsSupervisor — Is the configured user a supervisor
    - LocalUserID — An internal id maintained for agent/supervisor
    - TelsetLoginID — Agent/Supervisor Login ID
    - UserGivenName — First Name of the Agent/Supervisor
    - UserID — Internal agent identifier
    - UserSurName — Agent/Supervisor Last Name
    - UserType — Agent, Supervisor, Supervisor/Agent, Expert, Supervisor/Expert
    - sTimeStamp — Last reported timestamp of the anomalies

    The selected field moves from the **Fields** list to the **Fields Selected** list. By default the table name is appended to the field name after you add the field to the **Fields Selected** list. To remove the table name, click the **Toggle Table Name** icon.
12. To change the order of the selected fields, use the up and down arrows
13. To modify the properties of a selected field, in the **Selected Fields** list, click a field, and then in the **Width** box, type a new width.

    A default width of 50 pixels applies to all selected fields. The **Title** box is a read-only field.
14. Click **Next**.
15. To select a field to group by, in the **Grouping** window, from the **Fields** list, double-click a field.

    The selected field moves to the **Group** by list.
16. Click **Next**.
17. In the **Summaries** window, from the Fields list, select a field.
18. From the **Summation Type** list, select a summation type.

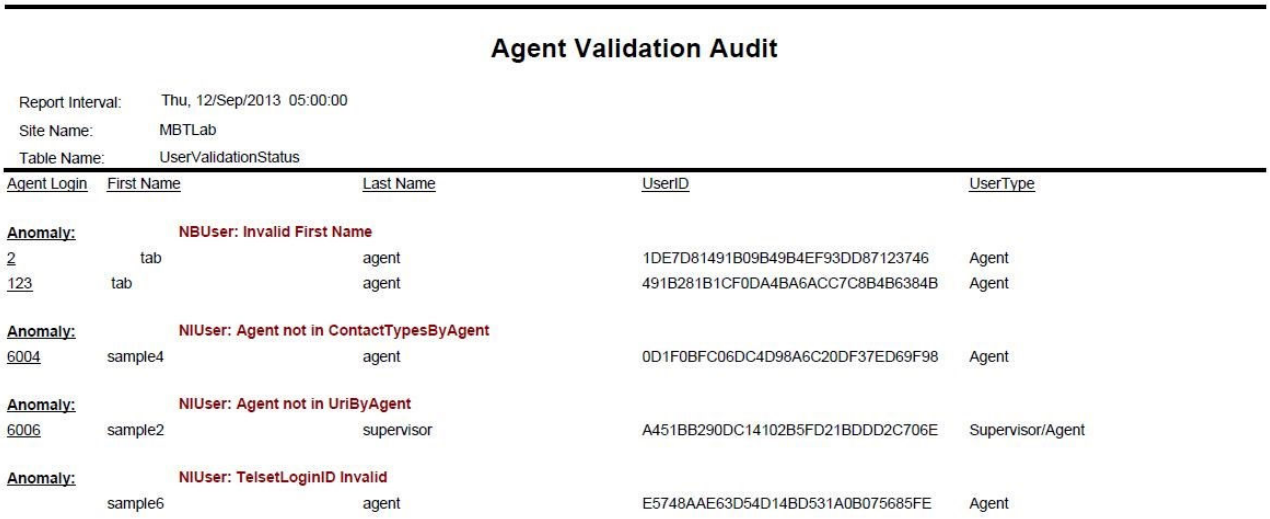
    As you select the fields in the **Fields** list, the **Summation Type** list dynamically updates to show the types available for the selected field.

19. From the **Groups** list, select the check box for each report section in which the summary appears on the report.
20. Click **Add**.

    The summary appears in the **Summary Data** list.
21. Click **Next**.
22. In the **Report Layout** window, view or modify the report
23. On the toolbar, click the **Save Report** icon.
24. In the **Save RCW Report** dialog box, choose a folder in which to save the report.
25. In the **Report Name** box, enter a name for the report. Enter `Agent Validation Audit`.
26. Click **Save**.

Example

Example of Agent Validation Audit report:



Agent Validation Audit

Report Interval: Thu, 12/Sep/2013 05:00:00
Site Name: MBTLab
Table Name: UserValidationStatus

Agent Login	First Name	Last Name	UserID	UserType
Anomaly:	**NBUser: Invalid First Name**			
2	tab	agent	1DE7D81491B09B49B4EF93DD87123746	Agent
123	tab	agent	491B281B1CF0DA4BA6ACC7C8B4B6384B	Agent
Anomaly:	**NIUser: Agent not in ContactTypesByAgent**			
6004	sample4	agent	0D1F0BFC06DC4D98A6C20DF37ED69F98	Agent
Anomaly:	**NIUser: Agent not in UriByAgent**			
6006	sample2	supervisor	A451BB290DC14102B5FD21BDDD2C706E	Supervisor/Agent
Anomaly:	**NIUser: TelsetLoginID Invalid**			
	sample6	agent	E5748AAE63D54D14BD531A0B075685FE	Agent

In this example, data is returned from the view, so the configuration data does contain discrepancies.

Chapter 22: Avaya Communication Server 1000 PABX troubleshooting

This section describes the troubleshooting procedures that you perform when handling Avaya Communication Server 1000 PABX issues in Avaya Aura® Contact Center. This section provides information about how and where to check for the status of the various configuration elements and parameters mentioned in the checklists.

Prerequisites for Avaya Communication Server 1000 troubleshooting

Procedure

Read the *Avaya Aura® Contact Center Configuration – Avaya CS1000 Integration* (44400-512) guide.

Verifying that the server is up

About this task

Verify that the server is up to determine where subsystem link problems are occurring. Problems can relate to the Contact Center Manager Server, the PABX, or on the Contact Center Manager Administration server.

Procedure

1. On the Contact Center Manager Server, in the SCMU utility, check that all components have the status Started.
2. On the PABX, check that the ELAN subnet connection to the PABX is functioning. See Verifying the ELAN subnet connection between the server and PABX on page 214.
3. Verify that you can successfully log on to the Contact Center Manager Administration server.

Verifying the ELAN subnet connection between the server and PABX

About this task

Verify that the ELAN subnet connection between the server and the PABX is functioning.

Procedure

1. On the PABX, in LD 48, enter the following command: `stat ELAN`.
2. Verify that the status for the ELAN subnet connected to the server is ACTIVE, EMPTY and APPL ACTIVE.
3. If there are multiple ELAN subnets, check the ELAN subnet connection for each IP address.

Result

Example

>ld 48

LNK000

.stat elan

SERVER TASK: ENABLED

ELAN #: 16

APPL_IP_ID: 47.166.111.14

LYR7: ACTIVE EMPTY APPL ACTIVE

ELAN #: 17

APPL_IP_ID: 47.166.111.13

LYR7: ACTIVE EMPTY APPL ACTIVE

Verifying the ACCESS Link between the Contact Center Manager Server and Avaya CallPilot®

About this task

Verify that the ACCESS Link between the Contact Center Manager Server and Avaya CallPilot® is functioning.

Procedure

1. On CallPilot®, select **System Utilities** > **Support Tools** > **CallPilot Processing Utilities** > **Trace Viewer <nbtview>**.

2. In Trace Control, on Meridian Link Services (MLS), select **MLink_Trace** for messages on Meridian Link Services (MLS).
3. Select **NBAPE** for messages on ACCESS Link.
4. On the Contact Center Manager Server, select **Start** > **Run**, enter **tsm_oam**, and then select option 3.
5. For VSM and MLSM session traces:
   - From the OAM menu, select option 2, and then enter `0` at the prompt.
   - Note the Session ID for VSM_Service and Meridian Link Services (MLS) SP (CallPilot® Application).
   - Press `Return` to go back to the OAM menu.
   - Select option 5, enter the Session ID, and then respond to the prompts as appropriate.
6. For AML traces:
   - From the OAM menu, select option 7.
   - From the AML Trace menu, select option 4.
7. For Access Protocol traces:
   - From the OAM menu, select option 9.
   - Select option 3 to enable the trace.
8. For Access Protocol Debug traces:
   - From the OAM menu, select option 10.
   - Select option 3 to enable the trace.

Verifying the PABX loop, shelves, and cards

About this task

Verify that the PABX loop, shelves, and cards are functioning.

Procedure

1. On the PABX, in LD 32, use the following command: `stat n1 n2 n3` where n1 is the loop, n2 is the shelf, and n3 is the card that contains either agents or voice ports.
2. The status for real agents must be LOG IN or LOG OUT, depending on the state of the agent.
3. The status for CallPilot® voice ports must always be LOG IN. If it is not, disable and enable the port on CallPilot® to trigger the auto-logon.

Result

Example

Command on the PABX:

Loop

ld 32

NPR000

.stat 24

SUPER LOOP

000 DSBL 038 BUSY

Real agents status (2500 set agents):

.stat 24 0 0

00 = UNIT 00 = IDLE (L500 LOG IN)

01 = UNIT 01 = IDLE (L500 LOG IN)

02 = UNIT 02 = IDLE (L500 LOG IN)

03 = UNIT 03 = IDLE (L500 LOG IN)

04 = UNIT 04 = IDLE (L500 LOG IN)

05 = UNIT 05 = IDLE (L500 LOG IN)

06 = UNIT 06 = IDLE (L500 LOG IN)

07 = UNIT 07 = IDLE (L500 LOG IN)

08 = UNIT 08 = IDLE (L500 LOG IN)

09 = UNIT 09 = IDLE (L500 LOG IN)

10 = UNIT 10 = IDLE (L500 LOG IN)

11 = UNIT 11 = IDLE (L500 LOG IN)

12 = UNIT 12 = IDLE (L500 LOG IN)

13 = UNIT 13 = IDLE (L500 LOG IN)

14 = UNIT 14 = IDLE (L500 LOG IN)

15 = UNIT 15 = IDLE (L500 LOG IN)

Voice Ports status (SL1 sets):

.stat 4 0 3

00 = UNIT 00 = IDLE (BCS LOG IN)

01 = UNIT 01 = IDLE (BCS LOG IN)

02 = UNIT 02 = IDLE (BCS LOG IN)

03 = UNIT 03 = IDLE (BCS LOG IN)

04 = UNIT 04 = IDLE (BCS LOG IN)

05 = UNIT 05 = IDLE (BCS LOG IN)

06 = UNIT 06 = IDLE (BCS LOG IN)

07 = UNIT 07 = IDLE (BCS LOG IN)

Verifying that CallPilot® ports are enabled

About this task

Verify that the CallPilot® ports are enabled.

Procedure

1. On the CallPilot® client, navigate to **CallPilot Manager**.
2. Select **Channel Monitor** link.
3. Verify that the channels are in **Idle** state.

   ACCESS channels appear in blue and Give IVR channels appear in green.

Verifying that the CDN is acquired

About this task

Verify that the CDN is acquired.

Procedure

1. In Contact Center Manager Administration, on the Launchpad click **Configuration**.
2. Select **CDN (Route Points)**.
3. Verify that the CDN status is **Acquired**.
4. On the PABX, in LD 23, enter the command `REQ PRT`.
5. Enter the command `TYPE CDN`.

   The following values appear on the printout:

   - AACQ = YES
   - ASID = ELAN connected to Contact Center Manager Server
   - CNTL = YES

Result

Example

ld 23

ACD000

MEM AVAIL: (U/P): 3591770 USED: 405925 TOT:

3997695
DISK RECS AVAIL: 2682
ACD DNS AVAIL: 23758 USED: 242 TOT: 24000
REQ PRT
TYPE cdn
CUST 0
CDN 2003
TYPE CDN
CUST 0
CDN 2003
FRRT
SRRT
FROA NO
MURT
DFDN 7700
CEIL 2047
OVFL NO
TDNS NO
RPRT YES
AACQ YES
ASID 16
SFNB 1 2 3 4 5 6 9 10 11 12 13 15 16
17 18 19
USFB 1 2 3 4 5 6 7 9 10 11 12 13 14 15
CALB 0 1 2 3 4 5 6 7 8 9 11
CNTL YES
VSID
HSID
CWTH 1
BYTH 0
OVTH 2047
STIO
TSFT 20

Verifying that the correct script is activated

Before you begin

- Orchestration Designer must be installed on the client and server.

About this task

Verify that the correct script is activated.

Procedure

1. Log on to the Contact Center Manager Administration.
2. Click **Scripting**.
3. From the **Service Creation** Menu, choose **Launch Orchestration Designer**.

   The Orchestration Designer Contact Center list opens.
4. In the Orchestration Designer Contact Center pane, expand **Contact Center Manager Administration server name** > **Contact Center Manager Server name** > **Application [Full Control]**.

   A list of existing scripts on that Contact Center Manager Server appears.
5. Verify that the script is in Active state, as indicated by a green checkmark on the script icon.
6. If the script is not active, right-click on the script and select **Activate**.

   The system activates the script. The script status changes to Active when the activation process finishes successfully.

Verifying that the IVR ACD-DN is acquired

About this task

Verify that the IVR ACD-DN is acquired.

Procedure

1. Log on to the Contact Center Manager Administration.
2. Click **Configuration**.
3. Select **IVR ACD-DN**.
4. Verify that the IVR ACD-DN status is **Acquired**.
5. On the PABX, in LD 23, enter the command `REQ PRT`.
6. Enter the command `TYPE ACD`.

   The following values appear on the printout:

   - AACQ = YES

- ASID = ELAN connected to Contact Center Manager Server
- IVR = YES
- TRDN = default treatment DN, if any

Result

Example

ld 23

ACD000

MEM AVAIL: (U/P): 3591770 USED: 405925 TOT: 3997695

DISK RECS AVAIL: 2682

ACD DNS AVAIL: 23758 USED: 242 TOT: 24000

REQ PRT

TYPE acd

CUST 0

ACDN 7725

TYPE ACD

CUST 0

ACDN 7725

MWC YES

IMS YES

CMS YES

IMA YES

IVMS YES

EES NO

VSID 7

MAXP 48

SDNB NO

BSCW NO

AACQ YES

ASID 16

SFNB 1 2 3 4 5 6 9 10 11 12 13 15 16 17 18 19

USFB 1 2 3 4 5 6 7 9 10 11 12 13 14 15

CALB 0 1 2 3 4 5 6 7 8 9 11

ALOG YES

RGAI NO

ACAA NO

FRRT

...

CCBA NO

IVR YES

TRDN 3600

CWNT NONE

Verifying that Give IVR voice ports are acquired by the TN in CallPilot®

About this task

Verify that the Give IVR voice ports are acquired by the TN in CallPilot®.

Procedure

1. Log on to the Contact Center Manager Administration.
2. Select **Phonesets and Voice Ports**.
3. Verify that the Voice Ports status is **Acquired Login**.
4. In the CallPilot® Manager, select **Channel Monitor link**.
5. Verify that the Give IVR channels are in **Idle** state.
6. On the PABX, in LD 20, use the following commands: `REQ TNB` and `TYPE 2008`.

   The following values appear on the printout:

   - ACQ AS = TN
   - ASID = ELAN connected to Contact Center Manager Server

Result

Example

DES CLPLT

TN 024 1 13 26

TYPE 2008

CDEN 8D

CTYP XDLC

CUST 0

FDN

TGAR 1
LDN NO
NCOS 3
RNPG 0
SCI 0
SSU
XLST
SCPW
CLS CDT ...
CPND_LANG ENG
HUNT
SPID NONE
AST 00 01
IAPG 0
AACS YES
ACQ AS: TN,AST-DN,AST-POSID
ASID 16
SFNB 1 2 3 4 5 6 11 12 13 18 22
SFRB
USFB 1 2 3 4 5 6 7 9 10 11 12 13 14 15
CALB 0 1 2 3 4 5 6 8 9 10 11 12
FCTB
ITNA NO
DGRP
PRI 01
DNDR 0
DTMK
KEY 00 ACD 5990 0 5356
AGN
01 SCN 5386 0 MARP
CPND
NAME CallPilot
XPLN 27

DISPLAY_FMT FIRST,LAST

02 MSB

03 NRD

04 TRN

05 AO3

06

07

Verifying that ACCESS voice ports are acquired by the TN and CallPilot® class ID or channel

About this task

Verify that the ACCESS voice ports are acquired by the TN and CallPilot® class ID or channel.

Procedure

1. Log on to the Contact Center Manager Administration.
2. Select **Phonesets and Voice Ports**.
3. Verify that the Voice Ports status is **Acquired Login**.
4. On the CallPilot® client, in the CallPilot® Manager, select **Channel Monitor link**.
5. Verify that the ACCESS channels are in **Idle** state.
6. On the PABX, in LD 20, use the following commands:
   - `REQ TNB`
   - `TYPE 2008`

   The following values appear on the printout:
   - ACQ AS = TN
   - ASID = ELAN connected to Contact Center Manager Server

Verifying that the system default Treatment DN is configured correctly

About this task

Verify that the system default Treatment DN is configured correctly.

Procedure

1. Log on to Contact Center Manager Administration.
2. Click **Configuration**.
3. Verify that the default treatment DN specified in the Global Settings window is configured correctly.

Verifying that treatment DNs are defined in the CallPilot® SDN table

About this task

Verify that treatment DNs are defined in the CallPilot® SDN table.

Procedure

1. In CallPilot®, in the **Configuration Manager**, select **System** > **Service Directory Number**.
2. Verify that the table contains an entry for each treatment DN, in which the Application Name is the name of the application created in Application Builder.

Verifying that IVR ACD-DNs match on the PABX, Contact Center Manager Administration, and the voice-processing system

Before you begin

- In CallPilot®, ensure that you have configured the ACCESS IVR ACD-DN in the Service DN table in CallPilot® Manager.

About this task

Verify that the IVR ACD-DNs match on the PABX, Contact Center Manager Administration, and the voice-processing system. The ACD-DNs must match in the following locations:

- Channel Information page in CallPilot® Manager
- PABX DN
- Contact Center Manager Administration script
- IVR ACD-DNs window in Contact Center Manager Administration

Procedure

1. In CallPilot® Manager, select **System** > **Service Directory Number**and check the value specified in the **Service DN** field.

2. On the PABX, in LD 20, enter the following command: `REQ DNB`.
3. On Contact Center Manager Administration, verify that the Give Controlled Broadcast script command specifies the DN defined in the CallPilot® SDN table: **Give Controlled Broadcast 4604**.
4. Navigate to **Contact Center Manager Administration Launchpad** > **Configuration** > **IVR ACD-DNs**, and verify the following:
   - The IVR ACD-DN number matches the ACD-DN defined on the PABX and in the CallPilot® SDN table.
   - The status for the IVR ACD-DN is **Acquired**.

Verifying that voice port TNs match on the PABX, Contact Center Manager Administration, and the voice-processing system

About this task

Verify that the voice port TNs match on the PABX,Contact Center Manager Administration, and the voice-processing system. The configuration of the TNs belonging to the ACD-DNs must match in the following locations:

- Channel Information page in CallPilot® Manager
- PABX DN
- IVR ACD-DNs acquired by Contact Center Manager Administration

Procedure

1. In CallPilot® Manager, select **Configuration Wizard**, and then click **Next**.
2. Select **CallPilot Individual Feature Configuration (Express Mode)**, and then click **Next**.
3. Choose **Switch Configuration**, and then click **Next**.
4. Note the value in the **TN** column.
5. On the PABX, in LD 20, enter the following command: `REQ DNB`.
6. Navigate to **Contact Center Manager Administration, Phonesets and Voice Ports**, and verify the following:
   - The **Channel** column for the voice port contains a unique number.
   - The status for the IVR ACD-DN is **Acquired Login**.

Verifying that channels for ACCESS voice ports match on the server and the voice-processing system

About this task

Verify that the channels for the ACCESS voice ports match on the server and the voice-processing system. The channel number for a specific TN must match the channel number for the same TN in the Voice Ports window on Contact Center Manager Administration. The channel number is the number shown in the Class ID column in the CallPilot® Channel Monitor.

Procedure

1. In CallPilot® Manager, select **Configuration Wizard**.
2. Select **CallPilot Individual Feature Configuration (Express Mode)**, and then click **Next**.
3. Choose **Switch Configuration**, and then click **Next**.
4. Note the value in the **Class ID** column.
5. Navigate to **Contact Center Manager Administration** > **Phonesets and Voice Ports**, and verify the following:
   - Each TN has a unique number in the Channel column.
   - The status for the voice port is **Acquired Login**.

Chapter 23: SIP Contact Center troubleshooting

This section describes the troubleshooting procedures that you perform when handling SIP issues in an Avaya Aura® Contact Center.

Prerequisites for SIP Contact Center troubleshooting

Procedure

- Ensure SIP Contact Center software is installed correctly, see *Avaya Aura® Contact Center Installation* (44400-311).
- Ensure SIP Contact Center software is configured correctly, see *Avaya Aura® Contact Center Commissioning* (44400-312).

Responding when dialing a Route Point

Before you begin

- Ensure the Contact Center Manager Administration server is configured.

About this task

When a Route Point is dialed, the customer is placed on a conference call in the Avaya Media Server and ringback is the first treatment. If a Route Point is dialed and there is no audible response or error code, check the Route Point has been acquired on the Contact Center Manager Administration server.

Procedure

Check the Route Point is acquired. For more information, see Configuring and acquiring a CDN (route point) in *Avaya Aura® Contact Center Manager Administration – Client Administration* (44400-611)

Logging on to Agent Desktop

About this task

When an agent cannot login to Agent Desktop, the agent is presented with an internal server error message. There can be many reasons for this error, however one resolution is to check the transport type for the SIP CTI Proxy Server is correct. Ensure the SIP settings in the server configuration utility are correct.

Procedure

If your contact center uses an Avaya Aura® Application Enablement Services server, check the transport type for the SIP CTI Proxy setting in the Server Configuration utility is set to TLS. For more information, see Configuring the Signaling Server for SIP CTI in the *Avaya Aura® Contact Center Server Administration* (44400-610) guide.

Troubleshooting when hold/unhold causes calls to be dropped after seventy seconds

About this task

If hold/unhold causes calls to be dropped after seventy seconds, there is a problem with the SIP terminal configuration.

Procedure

Check the agent's SIP terminal configuration in the Contact Center Manager Administration server.

Playing ringback into an active call

About this task

If ringback or an announcement is played in an active call, there is a problem with the SIP terminal configuration.

Procedure

Check the agent's SIP terminal configuration in Contact Center Manager Administration.

Call processing fails due to suspected Avaya Media Server failure

About this task

If there is an issue with call processing which has been narrowed down to Media Application failure, follow these sequence of steps.

Procedure

1. First ping the Avaya Media Server to ensure it is on the network.
2. If it is on the network, log on to the Avaya Media Server and ensure there are no alarms in the Alarms window in Element Manager.
3. If there are no alarms, ensure the Avaya Media Server handled the INVITE correctly. Turn on logging and check the timestamp of the failed call in the sipmcDebug.txt file.
4. If there is no INVITE in the logs, there is a problem with the lower level components of the Avaya Media Server (i.e. the SIP stack).

Handling 486 Busy Here error messages

About this task

If there is no ringback on a call and message 486 Busy Here is in the CCMS_SGM_SIPMessages.log, the CCMS cannot establish communication with the Avaya Media Server.

Procedure

1. Ensure the Firewall is turned off on the Avaya Media Server. Avaya Media Server cannot function correctly with a Firewall turned on.
2. Ensure Domain policies are correct as per defined by your system administrator.

Handling 404 Not Found error messages

About this task

If there is no ringback on a call and error message 404 Not Found is in the `CCMS_SGM_SIPMessages.log`, CCMS cannot establish communication with the Avaya Media Server. This indicates that the Avaya Media Server services did not install correctly, or that Avaya Media Server is using the wrong port. The Avaya Media Server port must be 5070 when Avaya Media Server is co-resident with Contact Center Manager Server.

Procedure

1. Verify the Contact Center Services (Announcement, Conference, Dialog) exist in Packaged Applications in the Element Manager. If they do not exist, the Contact Center Services installer did not run, or failed to run successfully.
2. Run the Contact Center Services installer.
3. If Avaya Media Server is co-resident with Contact Center Manager Server, ensure the Avaya Media Server port is 5070.

Handling 480 Temporarily Unavailable error messages

About this task

If there is no ringback on a call and error message 480 Temporarily Unavailable is in the `CCMS_SGM_SIPMessages.log` file, the Contact Center Manager Server cannot establish communication with the Avaya Media Server. This is due to an one of the following license issues with Avaya Media Server:

- Not licensed
- Licensed incorrectly
- Licensed but the license is not saved and confirmed.

Procedure

1. To verify this look for any alarms in the Avaya Media Server Alarms window. If there are no issues there, use the Avaya Media Server logs to pinpoint the problem.
2. Apply a license to the Avaya Media Server, save and confirm the license.

Handling 488 error messages

About this task

Error message 488 error (SDP fault) error message is in the CCMS_SGM_SIPMessages.log file. This is due to video codecs enabled on the Avaya Media Server.

Procedure

Remove all video codes from the Avaya Media Server.

Troubleshooting when digits entered for IVR Play and Collect are not recognized

About this task

Avaya Media Server collect digits and sends them to the Contact Center Manager Server, but the relevant IVR is not acted upon.

Procedure

1. On the Avaya Media Server, log on to Element Manager.
2. In the navigation pane, click **System Configuration** > **Media Processing** > **Digit Relay (DTMF)**.
3. On the **Digit Relay (DTMF)** page, select **RFC2833**.
4. On the **Digit Relay (DTMF)** page, select **INFO digits**. **INFO digits** must be enabled after enabling **RFC2833**. **RFC2833** must appear first on the list.
5. Click **Save**.

Troubleshooting when no terminals or addresses appear in Agent Desktop

About this task

No terminals or addresses appear in the Communication Control Toolkit reference client (RefClient) or in Avaya Aura® Agent Desktop and as a result, Agents cannot log on.

Procedure

In Contact Center Manager Administration, ensure every agent has a unique SIP URI.

Handling subscribed Resource Availability error messages

About this task

Agents cannot log on and a subscribedResourceAvailability CSTA error message is in the `CCMS_SGM_SIPMessages.log` file. This error suggests that the Avaya Aura® Application Enablement Services server has ran out of agent desktop licenses.

Procedure

Increase the Avaya Aura® Application Enablement Services **Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)** license count.

Handling TLS server certificate time zone issues

About this task

Signing a Transport Layer Security (TLS) security certificate on a server which is in a different time zone, especially ahead of the server which is to use the certificate, results in a failure in create a server certificate for Avaya Aura® Application Enablement Services.

Procedure

Ensure that the servers, including the Certificate Authorities and Avaya Aura® Application Enablement Services, are in the same time zone.

Handling missing TLS certificates

About this task

The Avaya Aura® Contact Center SIP Gateway Manager (SGM) Windows service fails to start and a “Failed to read or convert the security information - See previous logs for details” message is in the `SGM_SIPSp.log` file.

A possible cause of this is that the Certificate Manager steps which create a certificate store on the server has not been performed or the Transport Layer Security (TLS) security certificates have not been added to the store when created.

Procedure

1. Create a certificate store on the Contact Center Manager Server. For more information see, *Avaya Aura® Contact Center Commissioning* (44400-312).
2. Create the root and signed certificates. For more information see, *Avaya Aura® Contact Center Commissioning* (44400-312).

Troubleshooting CCMS and AES TLS communication issues

About this task

The Avaya Aura® Contact Center SIP Gateway Manager (SGM) windows service is running but agents cannot log on. A possible cause of this is that the Transport Layer Security (TLS) connection between the Contact Center Manager Server and Avaya Aura® Application Enablement Services is not functioning correctly.

Procedure

1. Create a certificate store on the Contact Center Manager Server. For more information see, *Avaya Aura® Contact Center Commissioning* (44400-312).
2. Create the root and signed certificates. For more information see, *Avaya Aura® Contact Center Commissioning* (44400-312).
3. Ensure the name entered when creating the certificate store or certificate name [FQDN] are the same as the one entered in the Application Enablement Services trusted server property.
4. Check the certificate name by launching the Certificate Manager, go to the templates tab and check the CN value. It must match the name of the server on which it resides and match the value that has been entered into the Application Enablement Services trusted server property. The Common Name (CN) is case sensitive.
5. Using Contact Center Manager Server - Server Configuration, ensure that TLS is selected, the port is 4723 and the correct IP address of the Application Enablement Services in the SIP-CTI box.

Troubleshooting when an agent goes not-ready to a presented call

About this task

When a call is routed to a Communication Control Toolkit reference client or Avaya Aura® Contact Center, the agent automatically goes to the Not-Ready state.

There are a number of possible causes for this problem.

Procedure

1. Ensure the agent is logged into the phone set or station.

   Avaya Aura® Contact Center solutions with the following settings and resources automatically block agents from logging on to Avaya Aura® Agent Desktop unless they have already logged on to their desktop phone:

   - Avaya Aura® Communication Manager is Release 6.2 or later.

- Avaya Aura® Application Enablement Services (AES) TSAPI CTI Link, ASAI Link Version setting is 5 or later.
- The agent station is not a SIP phone.

To block agents from unnecessarily changing to the Not Ready state, use these settings and resources.

2. Examine the SIP traces for the “P-Charging-Vector Required” error message. If this error message is present, log on to Avaya Aura® Communication Manager and on the Sat prompt, change the IMS field on the signaling-group to “n”.
3. Examine the SIP traces for the “407 Proxy Authentication Required” error message. If this error message is present, and if you are using an Avaya Aura® SIP Enablement Services server, ensure the Contact Center Manager Server is added to the authorized list in the SIP Enablement Services. For more information, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (44400-521).
4. Verify that the Avaya Aura® Session Manager to Avaya Aura® Communication Manager routing policy and dial pattern match your agent extension numbers. For more information, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (44400-521).
5. If you implemented SRTP in your contact center, verify your Avaya Aura® Contact Center SRTP configuration:
   a. Verify the SRTP configuration in the Aura PABX. For more information about configuring SRTP on the Aura PABX, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (44400-521).
   b. Verify the SRTP configuration on Contact Center. For more information on configuring SRTP on Contact Center, see *Avaya Aura® Contact Center Commissioning* (44400-312)
   c. Verify that the group policy for Agent Desktop embedded softphone settings has the correct encryption settings. For more information on the group policy for embedded softphone, see *Avaya Aura® Contact Center Installation* (44400-311)

Troubleshooting Agent Greeting recording

About this task

Troubleshoot using the following procedure when a tone is audible at the end of your Agent Greeting recording. This problem occurs when the DTMF tone generated by the # key is recorded. You press the # key to terminate a recording.

Procedure

1. Access the System Access Terminal (SAT) on your Communication Manager.

2. Using the `display signaling group x` command, where x is the number of your Communication Manager SIP Signaling Group, ensure the **DTMF over IP** setting is set to **rtp-payload**.

Troubleshooting non-skillset call monitoring in a Contact Center that uses beep tone

About this task

Contact Center blocks supervisor/agents from monitoring calls if there is a problem with playing beep tone. If your Contact Center uses beep tone, and supervisor/agents cannot monitor calls, first disable beep tone.

Procedure

1. Disable beep tone in CCMA and test non-skillset call monitoring. If you cannot observe a call, refer to Troubleshooting non-skillset call monitoring in a Contact Center that does not use beep tone on page 236.
2. From a Communication Manager station, manually dial the announcements to ensure that the announcements are uploaded correctly.
3. Check that the announcement files are in the correct format. If you are not sure whether it is in the correct format, replace your announcement file with the sample file provided by Avaya. The sample files are stored in the following location: `D:\Avaya\Contact Center\Common Components\wavs`.
4. Ensure that the Non-Skillset Call Monitoring values in CCMA correspond to those configured on the Communication Manager.
5. Ensure that CCMA is using the correct IP address for the Communication Manager.
    a. In the Application Enablement Services Management Console, select **Communication Manager Interface** > **Switch Connections**. Check that this IP address is the correct Communication Manager IP address.
    b. Ensure that the Non-Skillset Call Monitoring Announcement IP Address in CCMA matches this IP address.
6. Create a new Communication Manager CTI station.
    a. Create a new CTI station with a different extension number.
    b. Go to the **Non-Skillset Call Monitoring** tab in **Global Settings** on CCMA and change the **Proxy URI** field to use the SIP URI associated with this newly created CTI station.
    c. Save this new setting and try performing the non-skillset observe and or barge-in again.
    d. If monitoring works with the new CTI station, delete the original CTI station on the Communication Manager. Either re-create the original CTI station or continue to use the new one.

Troubleshooting non-skillset call monitoring in a Contact Center that does not use beep tone

About this task

If your Contact Center does not use beep tone, or non-skillset call monitoring does not work after you disable beep tone, follow this procedure.

Procedure

1. Ensure that the supervisor/agent logged on to Contact Center before performing a non-skillset observe or barge-in.
2. From the agent extension, try making a direct call to the supervisor/agent's extension.
3. From the agent extension, try conferencing the supervisor/agent into a call.
4. Check that the CTI links between Contact Center, Application Enablement Services and Session Manager are connected.
    a. On the Contact Center server, click **Start** > **All Programs** > **Avaya** > **Manager Server** > **SGM Management Client**.
    b. Confirm that Contact Center can communicate with Application Enablement Services (**CTI Proxy**) and Session Manager (**Voice Outbound Proxy**). Ensure both are **CONNECTED**.

Chapter 24: Troubleshooting with Avaya Grep

Avaya Grep is an Avaya Aura® Contact Center tool that extracts call-specific messages from the Contact Center logs, and reports on them to facilitate debugging of call issues. You download the Contact Center log files from the Avaya Aura® Contact Center server to your local PC. You can then use Avaya Grep to search across all the log files for all call events for a given Contact Center Call ID. Avaya Grep also suggests additional parameters to search on, based on the first pass of the logs with the Call ID.

By default, Avaya Grep generates three types of output:

- a summary log file, for each log file you selected to search, with only the messages matching the search criteria you entered
- a summary report, which records the search parameters you entered, and highlights all the warning or error messages encountered in the search
- a sip sequence report, which shows a ladder diagram of the call flow along with the list of detailed messages

Optionally, you can combine the messages matching your search into a single log file sorted by timestamp, which highlights the interaction between the different Avaya Aura® Contact Center components.

Important:

The Contact Center SIP contact model is a complex call flow that uses a Back to Back User Agent (BBUA) at the core. Because all Contact Center resources join an Avaya MS conference with the original customer call, a single customer-agent interaction can contain multiple separate SIP calls. This complexity increases where the contact center implements services such as IVR or recorded announcements, where agents transfer or conference calls, or where the contact center uses Avaya Aura® Shuffling.

This chapter explains how Avaya Grep assists debugging by pulling relevant SIP messaging from many disparate Contact Center logs. It does not provide instructions on how to interpret the call flow from the reports and summary logs.

The Avaya Grep tool has the following tabs:

- **Call Detail**: You use this tab to create reports by specifying search parameters, and which Contact Center log files to search and include in the reports.
- **Search**: You use this tab to search for Call IDs.

- **Convert**: You use this tab to convert raw SIP message traces from various sources into a message format used by SIP Message viewers to open and view log messages. You can also use this tab to convert AML (HEX) Call ID to a decimal equivalent Contact Center Call ID.

You install the Avaya Grep tool by extracting the Avaya Grep zip file to a location on your local machine. You start the tool by running the `AvayaGrep.exe` application. If you frequently review Contact Center files for debugging call issues, create a shortcut on your desktop for `AvayaGrep.exe`.

Note:

When debugging SIP voice contacts, Avaya Grep searches and reports only on call-related messages. Avaya Grep has minimal capability for debugging non-call related functions, such as agent login or logout, agent ready or not ready, and acquire or de-acquire Control Directory Numbers (CDNs).

Input log files and locations

For a full analysis of a SIP contact, you must copy the relevant log files from the Contact Center server. You can copy them from either:

- the current log file location (default `D:\Avaya\Logs\`)
- the log file archive location (default `D:\Avaya\Logs\Archive`)

The following table lists the logs you copy from the Contact Center server. An asterisk indicates that you need all logs starting with that string.

Table 7: Log Files to download from the Contact Center server for analysis with Avaya Grep

Files	Location
CCMS_SGM_AmlSp*	`D:\Avaya\Logs\CCMS`
CCMS_SGM_SipSp*	`D:\Avaya\Logs\CCMS`
CCMS_SGM_SipMessages*	`D:\Avaya\Logs\CCMS`
CCMS_AML*	`D:\Avaya\Logs\CCMS`
CCMS_TFE*	`D:\Avaya\Logs\CCMS`
CCMS_ASM*	`D:\Avaya\Logs\CCMS`
CCT_SERVER*	`D:\Avaya\Logs\CCT`
CCMS_EB*	`D:\Avaya\Logs\CCMS`
CMF_OAM*	`D:\Avaya\Logs\CCMS`

Not all logs contain all the search parameters that Avaya Grep supports. The following table indicates which log files you need if you want to find a Call ID using a particular search parameter.

Table 8: Log Files required to use Avaya Grep search parameters

Search Parameter	Required log files
SIP Call Leg ID	CCMS_SGM_SipSp*
Agent DN	CCMS_SGM_AmlSp*

Search Parameter	Required log files
CSTA/TR87 Call ID	CCMS_SGM_SipSp*
Customer Phone No.	CCMS_SGM_SipMessages* and CCMS_SGM_SipSp*

Output reports and summary logs

To output reports and summary logs, Avaya Grep creates a new folder named from the Call IDs that you use to search the source logs. Avaya Grep creates this folder as a subfolder of the Output Folder you specify. For example, if you generate reports for Call ID 12345678 and set the output folder to C:\AvayaGrep\Logs, Avaya Grep creates the folder C:\AvayaGrep\Logs\12345678. If you then generate reports for two Call IDs 12345678 and 09123456, Avaya Grep creates a new folder C:\AvayaGrep\Logs\12345678–09123456.

The reports and summary log filenames include the date and time at which Avaya Grep created them. Each time you generate reports and summaries for a particular Call ID, Avaya Grep adds them to the folder for that Call ID. You can choose to clear all existing logs when you run reports.

The following table lists the summary log output file names for each set of input logs.

Table 9: Avaya Grep summary log output file names

Contact Center Filenames	Summary log filename
CCMS_SGM_AmlSp*	AmlSp_ddmmyy_hhmm.log
CCMS_SGM_SipSp*	SipSp_ddmmyy_hhmm.log
CCMS_SGM_SipMessages*	SipMsg_ddmmyy_hhmm.log
CCMS_AML*	Aml_ddmmyy_hhmm.log
CCMS_TFE*	Tfe_ddmmyy_hhmm.log
CCMS_ASM*	ASM_ddmmyy_hhmm.log
CCT_SERVER*	CCT_ddmmyy_hhmm.log
CCMS_EB*	EB_ddmmyy_hhmm.log
CMF_OAM*	CMF_ddmmyy_hhmm.log

Installing Avaya Grep

About this task

You must install the Avaya Grep tool on your desktop to create summary logs and reports for Contact Center SIP contacts.

Procedure

1. On your local PC, create a folder for Avaya Grep, for example `C:\Program Files\Avaya\AvayaGrep`.
2. From the support site http://support.avaya.com, download the latest Avaya Grep tool to the folder you created on your local PC.

3. Extract the `Avaya Grep.ZIP` file to the folder.
4. On your desktop, create a shortcut for the Avaya Grep executable, `AvayaGrep.exe`.

Downloading the Contact Center log files from the server

Before you begin

- Decide how you are going to copy files from the Contact Center server to your local PC (for example, network shared drive, memory key).
- Verify the location of the log files folder on the Contact Center server: the default location is `D:\Avaya\Logs`.

About this task

Copy the SIP contact log files from the Contact Center server to your desktop, so that you can search and report on them using Avaya Grep. If you are debugging a particular event, you can download just a subset of the log files from the server. For example, you can download just the logs that cover the time of the event. You must download the files listed in Table 7: Log Files to download from the Contact Center server for analysis with Avaya Grep on page 238 only because Avaya Grep processes only these files.

Procedure

1. On the Contact Center server, copy the required log files.
2. Copy these files to the Avaya Grep Logs folder, for example `C:\Program Files\Avaya\AvayaGrep\Logs`.

Using Call Details to create summary log files and reports

Before you begin

Start Avaya Grep by clicking `AvayaGrep.exe`.

About this task

Use Avaya Grep to search the files downloaded from the Contact Center server for Contact Center SIP contact-specific log messages. Click the **Call Details** tab and specify a Call ID for which to search the log files and generate reports.

If Avaya Grep detects additional call parameters that can improve the summaries and reports, the Additional Parameters Detected dialog box appears. You can use these additional parameters to complete generating summaries and reports. This process provides a comprehensive search for all log messages from the call flow.

Procedure

1. Click the **Call Details** tab.

2. In the Call Properties section, in the **CC Call ID** field, enter one Contact Center Call ID for which you want to search the downloaded log files.

   Note:

   You must enter a Call ID to search the log files. If you do not know the Call ID, use the **Search** tab to find it.

3. Under **AACC Log Files**, specify the log files from which you want Avaya Grep to extract messages. You can select or clear the log files to include using the following methods:
   - Select all log files using **Select** > **All**.
   - Select default log file types using **Select** > **Default**.
   - Select a custom range by clicking individual log files.

   Note:

   Some log files are dependent on others being selected. It you select a log file that has dependencies, Avaya Grep automatically selects the associated files.

4. Select **CombineLogs** to combine messages from all the selected log files into a single log file sorted by timestamp, which highlights the time sequence of SIP messages through the call flow.
5. In the AACC Log section, under **File Type**, select whether to search standard log files, .ZIP files, or both from the log folder where you downloaded the Contact Center logs.
6. Under **Log Folder**, specify the folder containing all the Avaya Aura® Contact Center log files that you want to search for the specified Call ID.
7. Select the **Include subfolders** check box to search subfolders of the **Log Folder**.
8. Under **Output Folder**, specify the destination folder where you want to save the summary logs and reports from Avaya Grep.

   Avaya Grep automatically creates a sub-folder in this folder, using the Call ID as a folder name.

9. Select **Clear Logs** to remove any summary log files and reports that you generated for the selected Call ID in previous searches.

   Use this option if you want to re-create the summary logs and reports using new parameters or additional log files.

10. Click **Grep Logs**.
11. If Avaya Grep displays the Additional Parameters Detected dialog, you can click **YES** to return to the **Call Details** tab with the additional parameters pre-populated. Click **Grep Logs** to re-run the query with the additional parameters.

    Avaya Grep extracts all the messages matching the specified parameters from the log files you specified. Avaya Grep creates a folder in the **Output Folder** location, containing the summary logs and reports. Avaya Grep automatically opens this folder on your desktop.

Using Search to find Call IDs

Before you begin

- Start Avaya Grep by double-clicking `AvayaGrep.exe`.

About this task

Use the **Search** tab to find Call IDs for a call flow when you have other information about the call such as the Call Leg Id of a SIP message, the CSTA/TR87 Call ID, the Agent's DN, or the Customer phone number.

Procedure

1. Click the **Search** tab.
2. In the Search Parameter section, select a known parameter from the call flow you want to debug.

   Select one of the following:

   - **SIP Call leg Id**
   - **Agent DN**
   - **CSTA/TR87 Call Id**
   - **Customer Phone No.**

   Avaya Grep displays a message identifying the log files required to complete a search using this parameter.
3. In the text field matching the parameter you selected, enter the value of the parameter on which you want to search.
4. Ensure that the Avaya Aura® Contact Center source logs required for this search are present in the **Log Folder**.

   For example, if you select Agent DN, you need to ensure that the log folder (or its sub-folders) contains the `CCMS_SGM_AmlSp*` logs.
5. Click **Search Logs**.

   Avaya Grep searches the CC logs and displays the results in the Search Results panel. The Search Results panel displays all Call IDs related to the search parameter, along with the timestamp of the first occurrence in the logs.
6. From the Search Results rows, select the check box for a Call ID that you need to debug.

   Note:

   Selecting a check box changes **Search Logs** to **Grep Logs**. To change **Grep Logs** back to **Search Logs**, clear the selected check box.
7. Click **Grep Logs**.
8. On the Run Grep on this call dialog, click **Yes**.

9. If Avaya Grep displays the Additional Parameters Detected dialog, you can click **YES** to return to the **Call Details** tab with the additional parameters pre-populated. Click **Grep Logs** to re-run the query with the additional parameters.

   Avaya Grep extracts all the messages matching the specified parameters from the log files you specified. Avaya Grep creates a folder in the **Output Folder** location, containing the summary logs and reports. Avaya Grep automatically opens this folder on your desktop.

Debugging contacts using the Avaya Grep report

Before you begin

- Create a report using the Avaya Grep Call Details tab.
- Open the log folder for the Call ID for which you created a report.

About this task

Review the Avaya Grep report to find warning or error log events for a Call ID. This is a useful report to use to start your debugging, because it displays only the log messages that identify problems in the call flow.

Procedure

1. In the log folder for the Call ID for which you created log summaries and reports, double-click the `AvayaGrepReport.html` file.
2. Review the **Grep Parameters** and **Matchings Detected** sections to verify the Call ID and additional parameters with which you generated the summary.
3. Review the **Warnings/Errors & Exceptions** list to see all log entries for this contact that contain a SIP error, warning, or exception.

   Using this you can quickly jump to messages that identify problems in the call flow.

Debugging contacts using the SIP sequence report

Before you begin

- Create a report using the Avaya Grep Call Details tab.
- Open the log folder for the Call ID for which you created a report.

About this task

Use the SIP sequence report to review all the messaging for the selected contact. The SIP Sequence report shows a ladder diagram of the SIP messaging between the systems in the call flow. It also lists all the events collated from the logs on which you generated the report.

You can use the Marking feature highlight messages in which you are interested. This is useful when you are looking at a long call flow. You can easily locate log events you already examined and that are relevant to your investigation.

Procedure

1. In the log folder for the Call ID for which you created a report, double-click the `SipSequence.html` file.
2. If you see an Internet Explorer message stating that it has restricted this webpage from running ActiveX controls, click the message and select **Allow Blocked Content**.
3. Review the ladder diagram for all the SIP messages for the contact on which you created this report. The row above the ladder diagram shows the SIP devices that exchange messages in this call flow.
4. Select any SIP message, on the diagram, for which you require more information. The lower pane automatically scrolls to that message in the summary log, showing the message details.
5. To highlight a message in which you are interested:
   a. Click the **Mark Colour** box and select a color.
   b. Click **Marking: on**.
   c. In the ladder diagram, click the SIP message that you want to mark.

Debugging contacts using the CombineLogs file

Before you begin

- Create a report using the Avaya Grep Call Details tab.
- Open the log folder for the Call ID for which you created the report.

About this task

Use the CombineLogs file to debug messages from all the logs in time sequence. This is a detailed debugging report for when you want to look at the sequence of messages between all the SIP entities in the call flow.

Procedure

1. In the log folder for the Call ID for which you created a report, double-click the `CombineLogs_ddmmyyy_hhmm.log` file (where ddmmyyyy is the date in day month year format and hhmm is the time in hour minute format).
2. Review the content of the file to understand the precise order of SIP messages for the Call ID and other parameters for which you generated the report.

Using Convert to create readable logs from other systems

Before you begin

- Start Avaya Grep by clicking `AvayaGrep.exe`.

About this task

Use the **Convert** tab to convert raw SIP message traces from Avaya Media Server, traceSM, or AS5300, into a message format used by SIP message viewers, such as Snooper and Snoopy.

Procedure

1. Click the **Convert** tab.
2. Select the source file that you want to convert.
   a. Under **Source Type**, select one of the following types:
      - **AMS (sip.txt)**
      - **traceSM**
      - **AS5300**
   b. In the **Source File** box, specify the raw SIP message traces source file.
   c. In the **Destination File** box, specify the destination file where you want to save the converted files generated by Avaya Grep.
3. Click **Snoopify**.

   Avaya Grep converts the raw SIP message traces into the format used by SIP Message viewers, such as Snooper and Snoopy, and saves the file with the filename specified in **Destination File**.

Using Convert to change Call IDs from AML Hexadecimal format to decimal format

Before you begin

- Start Avaya Grep by clicking `AvayaGrep.exe`.

About this task

Use the **Convert** tab to change a Call ID in AML Hexadecimal format to decimal format, so that you can use it in the **Call Details** tab to create summary logs and reports.

Procedure

1. Under **AML / CC CallId**, enter an AML (HEX) Call ID in **AML CallId** .
2. Click the left arrow key to convert the HEX Call Id to a decimal equivalent Contact Center Call ID.

Entering a full, 12-digit AML Call ID returns an 8-digit Contact Center Call ID.

Chapter 25: Contacting Technical Support

This section describes the information that you need to locate before contacting Avaya Technical Support. Contact Technical Support only if you are unable to resolve the issue using the information and steps provided in this guide.

Gathering information for Technical Support

Gather all relevant information and have it available before contacting Avaya Technical Support. For all errors, record the error messages, the system configuration, and actions taken before and after the error occurred. If the problem persists, contact your Avaya customer support representative.

Be prepared to answer the following questions:

- When did the problem begin?
- How often does the problem occur?
- Is this a new install?
- Has the solutions database been searched? If so, were any related solutions found?
- Is there currently a workaround for this issue?
- Have you made any recent changes or upgrades to the system or network (for example, a modification to the configuration or code)? If so, when exactly were these changes made? Who made these changes (provide first and last name, if possible)?

Ensure that you can provide the following information to Avaya Technical Support:

- a copy of your configuration files
- a detailed network topology diagram
- log files

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W