Maintaining and Troubleshooting Avaya Control Manager

Release 9.0.1
Issue 2
January 2021

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. 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 set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time as indicated in the order, Documentation, or as authorized by Avaya in writing. 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.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service,

or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

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

Service Provider

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction 7
Purpose 7
Change history 7
Chapter 2: Database maintenance procedures 9
Database maintenance overview 9
Control Manager databases that require backup 9
Backing up Control Manager databases 10
Database recovery modes 12
Setting the recovery model of a database to simple 12
Renaming a Control Manager application server and SQL Server hostname in Multiplex HA configurations 14
Configuring TLS and TDE for Avaya Control Manager Multiplex HA configurations 16
Shrinking a log file 19
Administering autogrowth and autoshrink settings for log files 21
Chapter 3: Server maintenance procedures 25
Restoring Control Manager from the restricted to normal mode 25
Updating the Windows OS and SQL software on a working system 25
About rebooting servers 27
Rebooting servers in a Multiplex HA 2x2 configuration 27
Rebooting servers in a Multiplex HA 2x1 configuration 29
Rebooting servers in a Multiplex HA 1x2 configuration 30
Rebooting servers in an Enterprise non-HA configuration 32
Rebooting servers in an Enterprise HA configuration 33
Stopping and starting services using the Health Monitoring tool 35
Updating the Java version 35
Correcting the Windows time setting on Control Manager servers 38
Renewing the expired certificate 41
Uninstalling the Control Manager system 41
Removing the prerequisite components manually 42
Removing the Control Manager services manually 43
Removing the Control Manager databases manually 45
Chapter 4: Configuration maintenance procedures 49
Getting Control Manager licenses 49
Installing Control Manager licenses 50
No one-X license found 51
Chapter 5: Troubleshooting tools 52
Control Manager health monitoring 52
Starting the Health Monitor Status tool 52
Starting the Health Monitor Status tool in a non-system drive 53

Diagnostic Monitor..... 54
Health Monitor Status tool icon..... 76
About File Integrity..... 77
Checking the File Integrity logs..... 77
Generating logs using the File Integrity Checking script..... 78
Chapter 6: General troubleshooting information..... 79
Control Manager services descriptions..... 79
Usage Metering data not sent from Control Manager..... 81
Excessive Sphere services database queries..... 82
Failed to connect to the database server..... 83
Problems when loading Avaya one-X® Agent profiles..... 84
Avaya one-X Agent password error..... 84
Successful bulk job with attributes assignment failed..... 85
Announcement media file does not play on Control Manager..... 85
Announcement does not play the media file when clicking on the Play button..... 86
Troubleshooting Control Sphere..... 86
Sphere link cannot redirect to proper page..... 86
Sphere search engine is not connected to the Tomcat..... 87
Sphere feeder is not able to connect to the database..... 87
Chapter 7: Troubleshooting installation problems..... 90
Failure installing one of the prerequisites..... 90
Control Manager services are not starting..... 90
Esent database error during installation..... 91
Firewall issues..... 92
The default language is not applied when you launch Control Manager for the first time..... 92
Unable to log in to the Control Manager user interface..... 93
Authentication failed..... 93
No more licenses..... 94
Unable to connect to other Avaya products..... 95
Synchronizer issues..... 95
The Synchronizer application does not show any locations..... 95
Synchronization from Communication Manager is not starting..... 96
Application pool error messages..... 96
Cannot view WebLM licenses in License Tracker..... 97
Chapter 8: Troubleshooting performance problems..... 100
Users experience lengthy delays accessing Communication Manager administration objects..... 100
Unable to access station status from Communication Manager objects..... 102
Unable to change Reason Codes from two-digit to single-digit..... 103
Requested feature is not supported in configured Oceana version: Messaging..... 104
Chapter 9: Troubleshooting failover problems..... 105
Failover procedure for Multiplex HA application server configurations..... 105
About failover..... 107
HA failover..... 107

Failover for application servers..... 107
Server status during normal operation..... 109
Summary of how service is impacted when server failover occurs..... 109
Server failover scenarios..... 110
Data center failover scenarios..... 116
Server recovery procedures (Enterprise only)..... 121
Avaya one-X® Agent recovery procedures..... 124
Chapter 10: Troubleshooting Licensing problems..... 126
License server service not starting 126
No valid license found error when you login to Control Manager..... 126
User cannot access Avaya Oceana® admin screens when Control Manager is in grace mode... 127
Control manager showing grace mode warning message 127
Chapter 11: Resources..... 129
Documentation..... 129
Finding documents on the Avaya Support website..... 130
Accessing the port matrix document..... 131
Avaya Documentation Center navigation..... 131
Training..... 132
Viewing Avaya Mentor videos..... 133
Support..... 134
Using the Avaya InSite Knowledge Base..... 134

Chapter 1: Introduction

Purpose

This document contains maintenance procedures, best practices, and troubleshooting procedures for the routine maintenance and required troubleshooting of Control Manager. Routine maintenance practices include regularly scheduled backup and restoration, daily monitoring, patch installation, and verification testing. People who perform maintenance and troubleshooting tasks, such as service engineers and administrators, may find this document useful.

Change history

New in this release

Issue	Date	Summary of changes
2.0	January 2021	Added a new topic. See Announcement media file does not play on Control Manager on page 85.
1.0	September 2020	• Added the procedural steps in Starting the Health Monitor Status tool in a non-system drive on page 53. • Added the Database tab details in Diagnostic Monitor on page 54. • Added SQL Server and Port as a new option. See Diagnostic Monitor on page 54. • Added SQL Server and Port details as a new filed description. See Diagnostic Monitor on page 54. • Added the procedural steps to check the File Integrity Checking logs. See Checking the File Integrity logs on page 77. • Added the procedural steps to check the File Integrity Checking logs. See Checking the File Integrity logs on page 77. • Added information about the task. See Generating logs using the File Integrity Checking script on page 78. • Added information as a new condition. See Failed to connect to the database server on page 83. • Added error message details as a new condition. See Failed to connect to the database server on page 83.

Table continues…

Issue	Date	Summary of changes
		• Added the Requested feature details as a new condition. See Requested feature is not supported in configured Oceana version: Messaging on page 104. • Added courses availability details. See Training on page 132.

Chapter 2: Database maintenance procedures

Database maintenance overview

It is the customer's responsibility for the maintenance of the SQL databases used with Control Manager. Customers must have database administrators (DBA) available to follow the database maintenance best practices for the customer. Customers must use official Microsoft SQL documentation for database best practices and consult with Microsoft SQL database experts.

This chapter contains information and tasks to which the customer can refer to help maintain the Control Manager databases. Customers that have database administrators may choose to follow different recommendations not shown here, but this chapter gives the customer a few specific items that can help with database maintenance.

Control Manager databases that require backup

To help prevent data loss and recover from user error, Avaya recommends that you back up all Control Manager databases daily, including system databases. Regular daily backups help reduce the chance of running out of disk space because of transaction logs or other space-wasting processes. Use standard Microsoft SQL backup tools to back up the databases. The following table lists the databases on the Control Manager system that must be backed up.

Note:

The ACCCMAVP and ACCCMONEXDB module are licensed Control Manager features and might not be installed in your deployment. If your deployment is not licensed for these features, these databases do not appear on the list and you do not have to back them up.

Database name	Purpose	Notes
ACCCM	Main Control Manager database	You must back up this database.
ACCCMAVP	Control Manager Voice Portal/Experience Portal application management database	You must back up this database only if the Control Manager Voice Portal/Experience Portal module is licensed and enabled.

Table continues…

Database name	Purpose	Notes
ACCCMONEXDB	Control Manager centralized Avaya one-X® Agent administration database	You must back up this database only if the Control Manager Avaya one-X® Agent Centralized Administration Management module is licensed and enabled.
ACCCMSYNC	Synchronizes the database between Communication Manager and Control Manager.	You must back up this database.
ACCCMCMSYSLOG	Stores the Communication Manager syslog entries.	You must back up this database.

Backing up Control Manager databases

About this task

To help prevent data loss and recover from user error, Avaya recommends that you back up all Control Manager databases daily, including system databases. Regular daily backups help reduce the chance of running out of disk space because of transaction logs or other space-wasting processes.

In addition to regular backups, do backups in the following scenarios:

- New installations — In Multiplex HA 2x2 or 1x2 configurations, you must back up all of the databases installed on the SQL server that is associated with the primary application server. You must then restore the databases on the secondary SQL server. A backup is not done when installing a Multiplex HA 2x1 configuration.
- Upgrades — If you are upgrading from an older version of Microsoft SQL Server software, you must back up the database data and then restore (migrate) it to the new Microsoft SQL Server software.
- Server maintenance — If you are planning server maintenance, you must back up the database data in case the server becomes unusable after maintenance and you have to move the data to a new system.

Procedure

1. On the SQL server used for Control Manager, open the SQL Management Studio application.
2. On the Connect to Server window, provide the following information and log on to the system as administrator:
   - Server type
   - Server name
   - Authentication

- User name
- Password

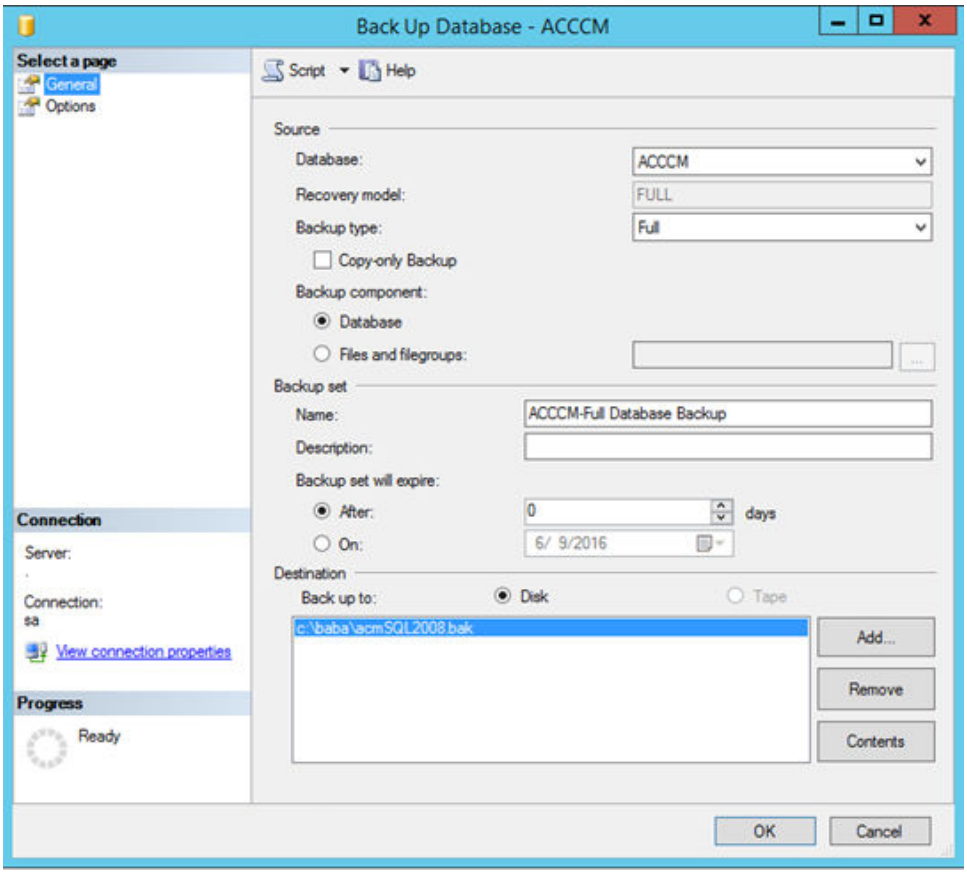
3. In the Object Explorer pane, expand the Databases navigation tree and select the ACCCM database.

   Important:

   When selecting the databases for backup, keep track of any custom named databases in the table shown above. For releases 8.0.x.x and newer, you must not have custom database names.

4. Right-click the database and select **Tasks** > **Back Up**.

   The system displays the following screen:



5. In the Back Up Database screen, perform the following steps:

   a. In the Select a page pane, select **General**.

   b. In the right pane, from the **Backup type** drop-down list, select **Full**.

   c. In the Destination section, select the directory where you want to store the backup file. Ensure that the filetype is set to `.bak`.

   d. Click **OK** to begin the database backup process.

The system starts the backup of the database.

6. Repeat these steps to back up all of the databases.

Important:

Remember to keep track of any custom named databases in the table shown above.

Database recovery modes

To minimize potential data loss, you must operate the Control Manager databases in full recovery mode. The databases you must set to full recovery mode is different depending on the configuration:

- When using the regular Microsoft SQL Server software in a non-HA, set the ACCCM, ACM_BILLING, and ACCCMAVP databases in full recovery mode.
- When using the Microsoft SQL Server AlwaysOn feature in a Multiplex HA configuration, set all Control Manager databases to full recovery mode.

When a database operates in full recovery mode, transaction log files can grow excessively large unless you properly size the transaction logs and back up transaction logs on a regular basis. Avaya advises you to perform frequent transaction log backups (that is, once or twice per day), but less frequent full backups. You may need to increase the frequency of transaction log backups if you continue to see excessive file growth. Failure to follow these requirements can result in data loss or service disruptions, or both.

Setting the recovery model of a database to simple

About this task

By default, the recovery model for Control Manager databases is set to Full. The Control Manager sync service activity can affect the size of the transaction log. If you are unable to back up the transaction log, you can stop excessive log growth by putting the database into simple recovery mode.

Caution:

Putting a database into simple recovery removes the ability to perform point in time recovery and there may be data loss in the event of an outage. Do not use simple recovery mode where failure recovery is critical.

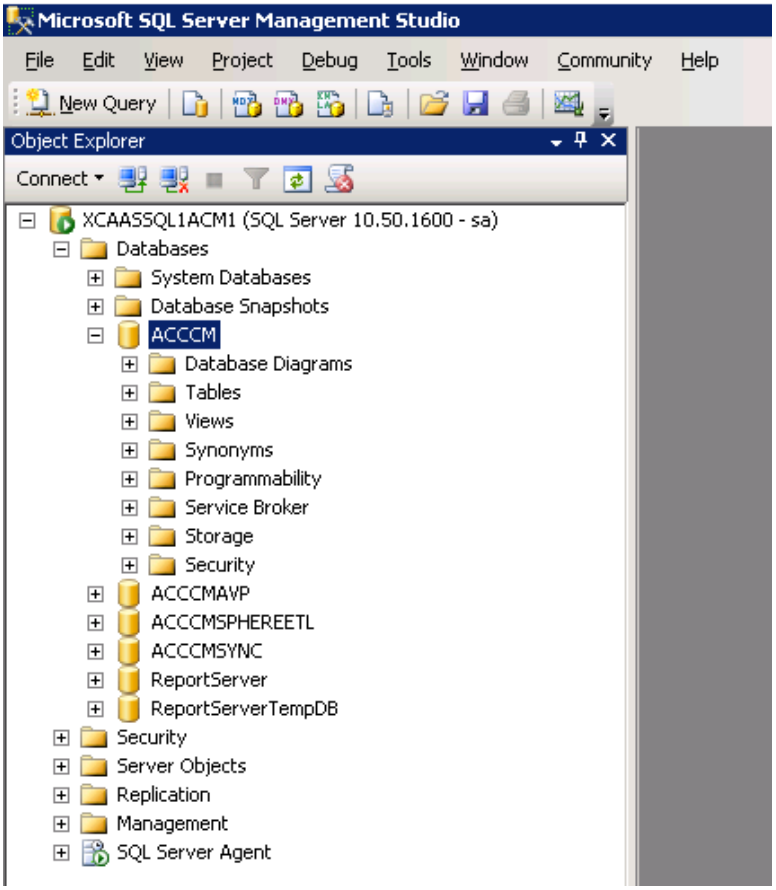
Important:

The procedure shown here is an example of how you change the recovery model of a database. Not all examples works for all customers. The customer DBA must approve any changes that involve the database recovery model.

Procedure

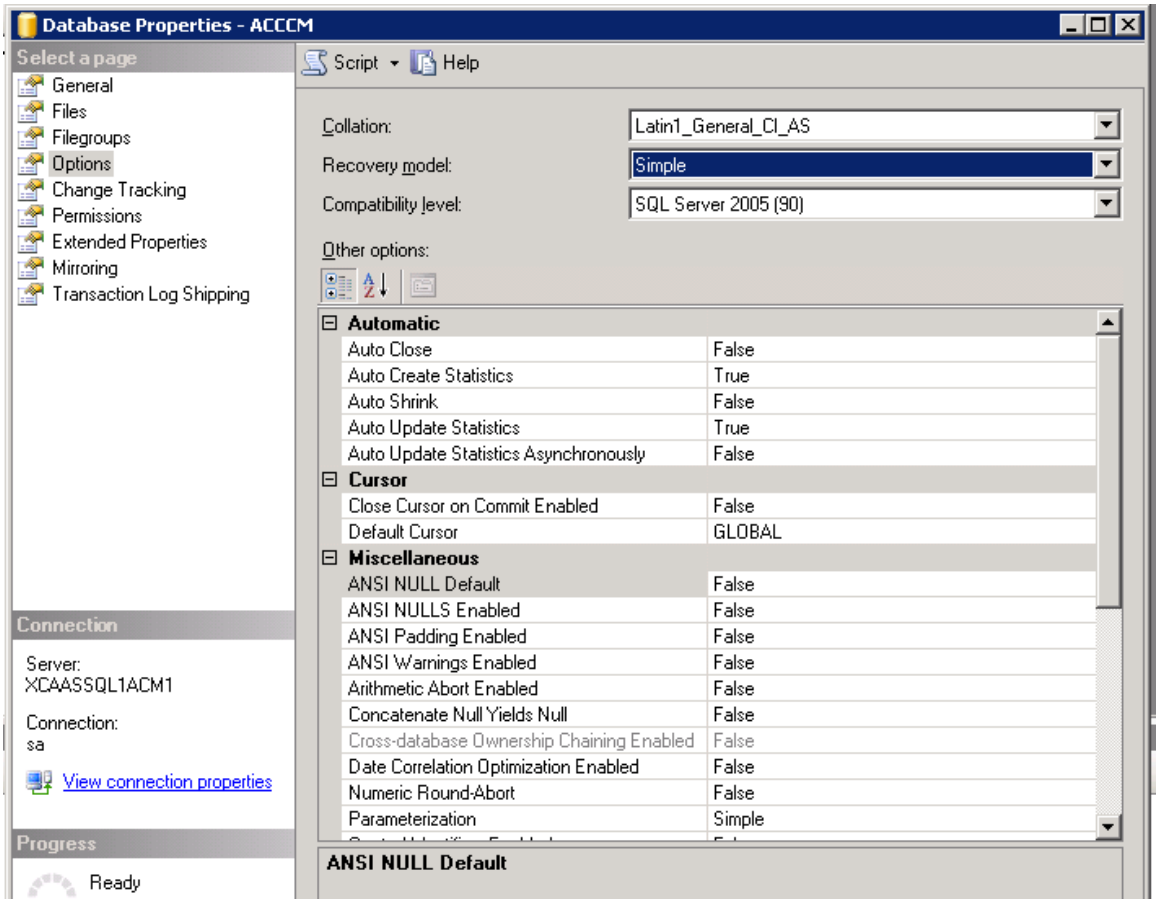
1. Connect to the SQL Server Instance using the SQL Server Management Studio.
2. In the Object Explorer window, expand **Databases**.

   The system displays a screen similar to the following:



3. Right-click the database you want to change and select **Properties**.
4. In the Select a page window, select **Options**.

   The system displays a screen similar to the following:



5. In the right pane, set the **Recovery model** option to **Simple**.
6. Click **OK**.
7. Repeat this procedure for every database you want to change to simple recovery.

Renaming a Control Manager application server and SQL Server hostname in Multiplex HA configurations

About this task

In a Multiplex HA 1x2 or 2x2 configuration, you can rename a computer that hosts a standalone instance of SQL Server.

Before you begin

Procedure

1. Log on to Windows as administrator on the primary database server (ACM-SQL-1).
2. Open the SQL Server Management Studio. The system displays the Microsoft SQL Server Management Studio screen.

3. Navigate to **Object Explorer** > **Availability Group** and open **Always On Availability Group**.
    a. Under **Availability Database**, right-click a database and select **Remove Database from Availability Group**. Repeat this step for all databases.
    b. Open **Availability Group Listeners** and delete **Listener IP Address**.
    c. Open **Availability Replicas**, right-click **Secondary Replica**, and then click **Remove from Availability Group**. Repeat this step to delete all the secondary replicas.
    d. Right-click on the Availability group and click **Delete**.
4. Open **SQL Server Configuration Manager**.
    a. In the left panel, click **SQL Server Service**.
    b. Double-click **SQL Server (MSSQLSERVER)** and click the **AlwaysOn High Availability** tab.
    c. Deselect the **Enable AlwaysOn Availability Group** option and click **Apply**.
    d. Repeat this step on the secondary database server (ACM-SQL-2).
5. Open **Server Manager**.
6. Navigate to **Tools** > **Failover Cluster Manager**.
    a. Right-click **Failover Cluster Manager** and select **Connect to cluster**.
    b. Right-click the cluster that you want to delete and click **Move Actions**.
    c. Click **Destroy cluster**.
7. Modify the IP addresses of the primary and secondary database servers.
8. Rename the computer names of the primary and secondary database servers.
9. Restart the primary and secondary database servers.
10. Update the new names for SQL instances on the primary and secondary database servers. For more information, on the Microsoft Documentation website, see Rename a Computer that Hosts a Stand-Alone Instance of SQL Server. See Link Disclaimer on page 2.
11. Update new IP address for SQL Server Network Configuration.
12. Reconfigure the AlwaysOn on SQL Server with new the IP and hostname for AlwaysOn Group and Listener IP.
13. Modify IPs and rename the computer names of the primary and secondary application servers.
14. Reconfigure certificates.
15. Navigate to **Diagnostics** > **Database tab** and update the new listener IP of the Availability Group.
16. Restart the primary and secondary servers.

Next steps

Configuring TLS and TDE for Avaya Control Manager Multiplex HA configurations

Before you begin

Ensure that you install Control Manager in Multiplex HA with Microsoft SQL AlwaysOn mode.

Enabling Transparent Data Encryption (TDE) for databases in Microsoft SQL Server AlwaysOn is slightly different than those needed on standard Microsoft SQL Server databases. Complete the following steps to set up and verify Transport Layer Security (TLS) 1.2 and TDE on primary and secondary database replicas, which are part of Availability Groups (AAG/BAG):

Procedure

1. Use the following Microsoft SQL queries to create and enable encryption certificates on the primary and secondary database replicas.
   a. Run the following Microsoft SQL query to create a TDE certificate and apply it to the primary replica of AAG/BAG

```
USE MASTER
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '[StrongPassword]'
GO

CREATE CERTIFICATE ACMTDECert
WITH SUBJECT = 'ACM TDE Certificate for all user database in the
Availability Group'

USE MASTER
GO
BACKUP CERTIFICATE ACMTDECert
TO FILE = 'C:\ACMTDECert_File.cer'
WITH PRIVATE KEY (FILE = 'C:\ACMTDECert_Key.pvk' ,
ENCRYPTION BY PASSWORD = '[StrongPassword]' )
GO


USE [ACCCM]
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE ACMTDECert
GO


USE [ACCCMAVP]
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE ACMTDECert
GO


USE [ACCCMCMSYSLOG]
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE ACMTDECert
GO
```

```
USE [ACCCMONEXDB]
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE ACMTDECert
GO

USE [ACCCMSPHEREETL]
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE ACMTDECert
GO

USE [ACCCMSYNC]
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE ACMTDECert
GO
```

b. Run the following Microsoft SQL query to copy the certificate on to the secondary database replica of AAG/BAG.

```
USE MASTER
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '[StrongPassword]'
GO


USE MASTER
GO
CREATE CERTIFICATE ACMTDECert
FROM FILE = 'C:\ACMTDECert_File.cer'
WITH PRIVATE KEY (FILE = 'C:\ACMTDECert_Key.pvk',
DECRYPTION BY PASSWORD = '[StrongPassword]' );
```

c. Run the following query to enable TDE on the primary database replica of AAG/BAG.

```
ALTER DATABASE [ACCCM]
SET ENCRYPTION ON

ALTER DATABASE [ACCCMAVP]
SET ENCRYPTION ON

ALTER DATABASE [ACCCMCMSYSLOG]
SET ENCRYPTION ON

ALTER DATABASE [ACCCMONEXDB]
SET ENCRYPTION ON

ALTER DATABASE [ACCCMSPHEREETL]
SET ENCRYPTION ON

ALTER DATABASE [ACCCMSYNC]
SET ENCRYPTION ON
```

d. Run the following query on the primary and secondary replicas to verify whether TDE is enabled.

2. To set up up TLS 1.2, open a text editor and create a file named `tls1.2_enable.reg`.
3. Enter the following code in the `tls1.2_enable.reg` file:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\SSL 2.0]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\SSL 2.0\Client]
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.0]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.0\Client]
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.0\Server]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.1]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.1\Client]
"DisabledByDefault"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.1\Server]
"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.2]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000
"Enabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.2\Server]
"DisabledByDefault"=dword:00000000
"Enabled"=dword:00000001
```

4. Copy the file on to all application and database servers in the Multiplex HA configuration.
5. Right-click the file and select **Merge** to enable TLS 1.2 on each server where you copy this file.

   Ensure that you perform this step on both application and database servers so that you enable TLS 1.2 on both clients and servers.
6. Install the security patch on database servers based on the SQL server version installed on these servers, to support TLS 1.2. For more information, on the Microsoft Support website, see TLS 1.2 support for Microsoft SQL Server. See Link disclaimer on page 2.
7. Install Wireshark on the application servers.
8. Complete the following steps and verify using Winshark whether TLS 1.2 is used for connection with the database servers:
   a. To add a location, do the following:
      - Log in to the ACCCM portal.
      - Navigate to the **Location** option.
      - Enter a name and description for the location and then click **Save**.

b. To add a user, do the following:
   - Log in to the ACCCM portal.
   - Navigate to the User portal and click the **+** icon to add a user.
   - Enter the required details for this user and then click **Save**.

c. To delete a user, do the following:
   - Log in to the ACCCM portal.
   - Navigate to the User portal and select the user that you created in the previous step.
   - Open the **Expand** icon options and click **Delete user**.

9. Verify whether the adding a location, adding a user, and deleting the user operations are synced to both database servers within AAG.

Shrinking a log file

About this task

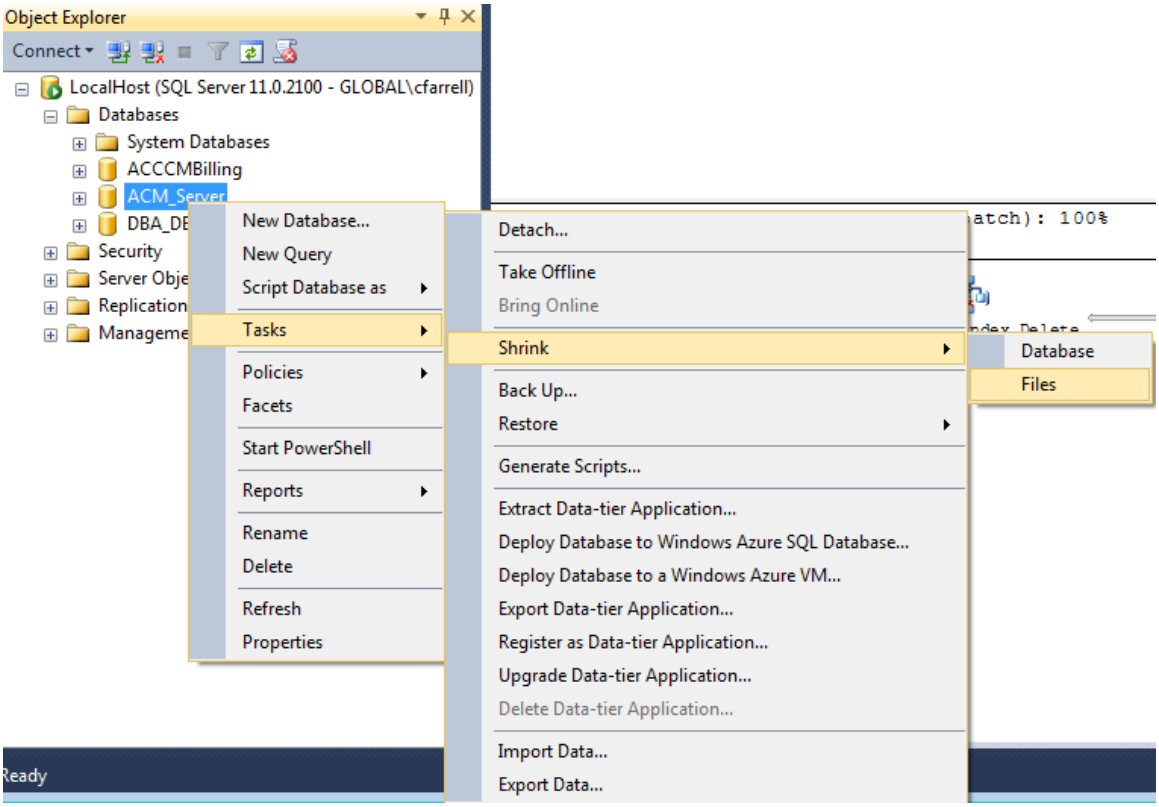
After the transaction log has been backed up or the database has been put into the simple recovery mode, you can reduce the amount of space the transaction log takes by shrinking the file.

Important:

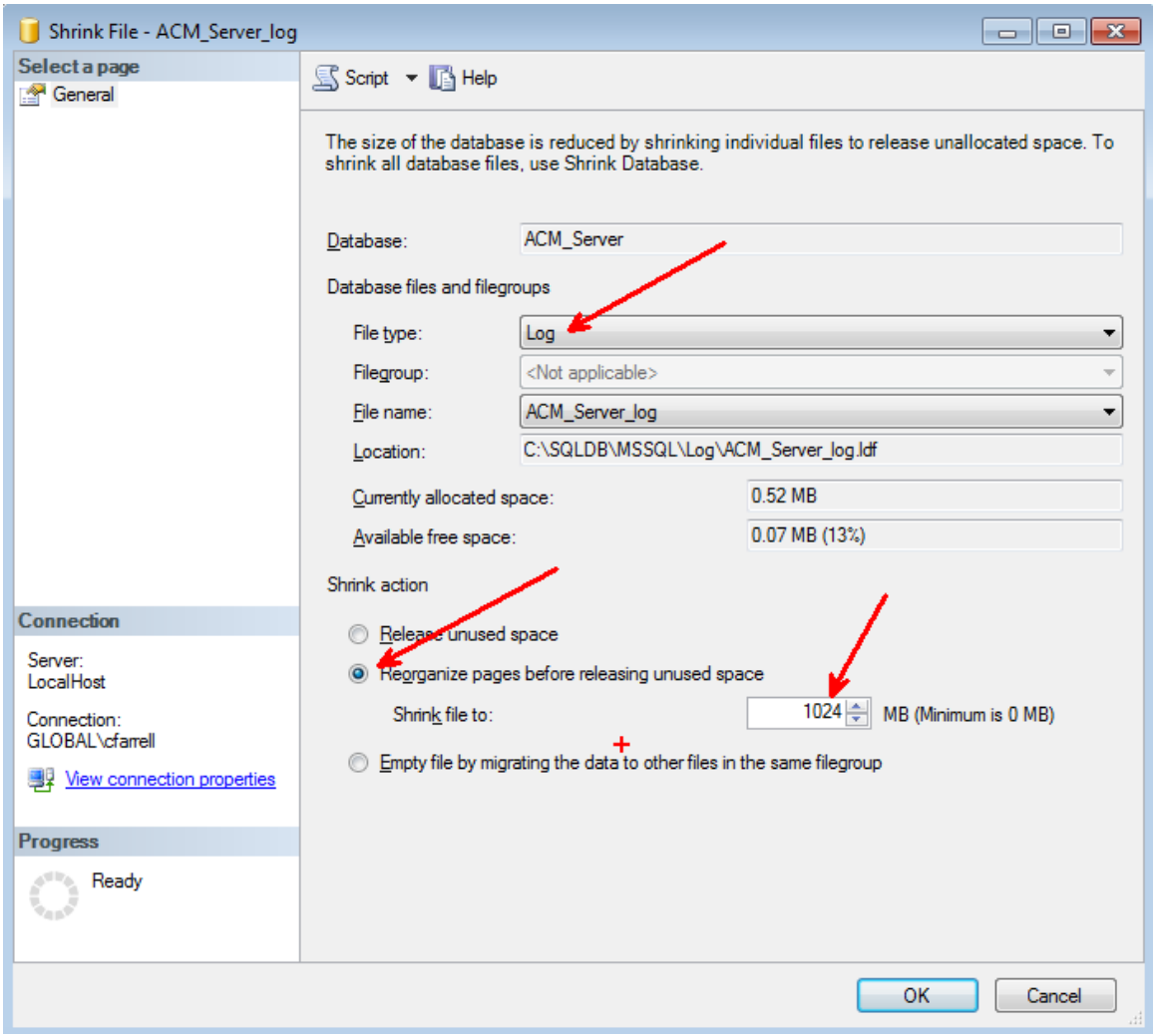
The procedure shown here is an example of how you can shrink a log file. Not all examples works for all customers. The customer DBA must approve any changes that involve shrinking a log file.

Procedure

1. Connect to the SQL Server Instance using the SQL Server Management Studio.
2. In the Object Explorer window, expand **Databases**.
3. Right-click the database and select **Task** > **Shrink** > **Files** as shown in the following screen:



The system displays the following screen:



4. Set the **File type** option to **Log**.
5. Set the **Shrink action** option to **Reorganize pages before releasing unused space**.
6. In the **Shrink file to** option, enter the number of Megabytes to which you want to shrink the file. In the example above, the size is set to 1024 MB.
7. Click **OK**.

Administering autogrowth and autoshrink settings for log files

About this task

Use this procedure to set size limitations for log files.

You must turn on the autogrowth option for log files. However, you must also monitor the growth of log files to ensure that the log files are not using up too much of your available free space. Do not rely upon autogrowth to perfectly manage database growth. Manually grow the database during a low usage maintenance window when storage levels are at 80%. Avoid the possibility that an auto-grow process potentially occurs during high usage hours.

You must turn off the autoshrink option.

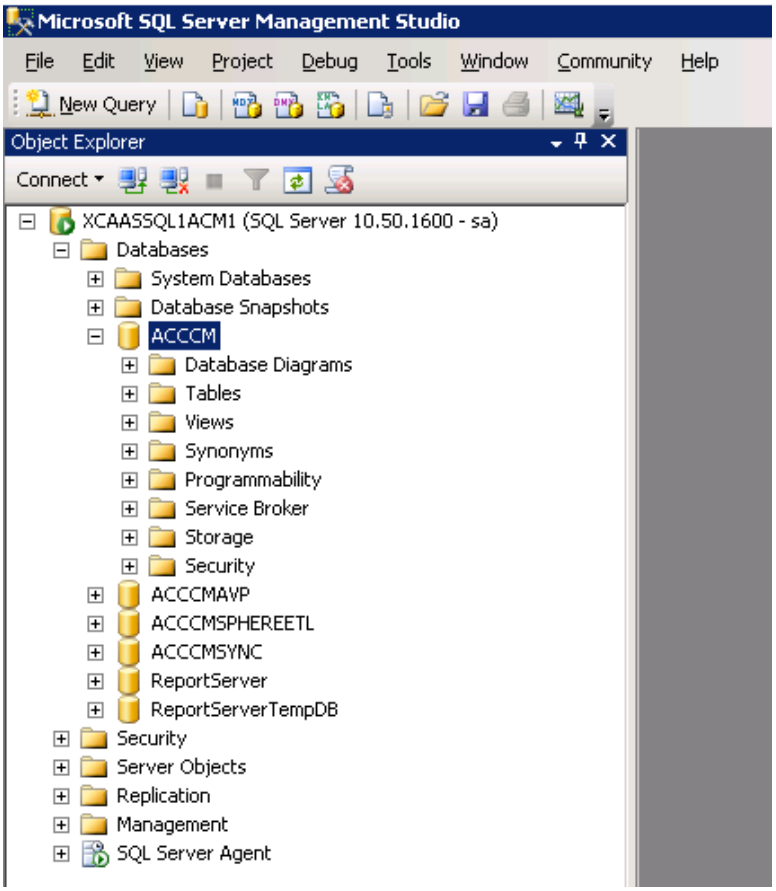
Important:

The procedure shown here is an example of how you can administer autogrowth. Not all examples works for all customers. The customer DBA must approve any changes that involve the autogrowth options.

Procedure

1. Connect to the SQL Server Instance using the SQL Server Management Studio.
2. In the Object Explorer window, expand **Databases**.

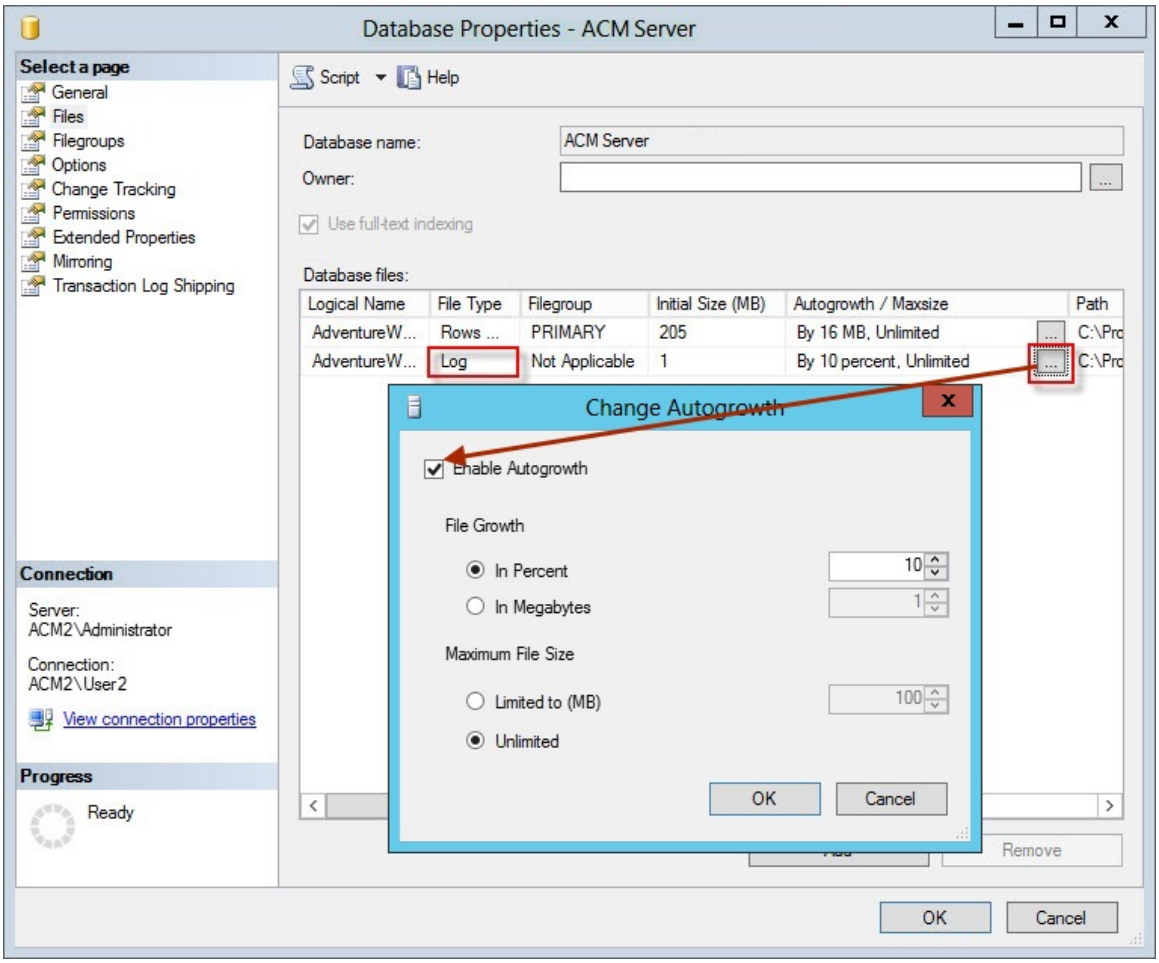
   The system displays a screen similar to the following:



3. Right-click the database and select **Properties**.
4. In the **Database Properties** screen, in the **Select a page** pane, select **Files**.

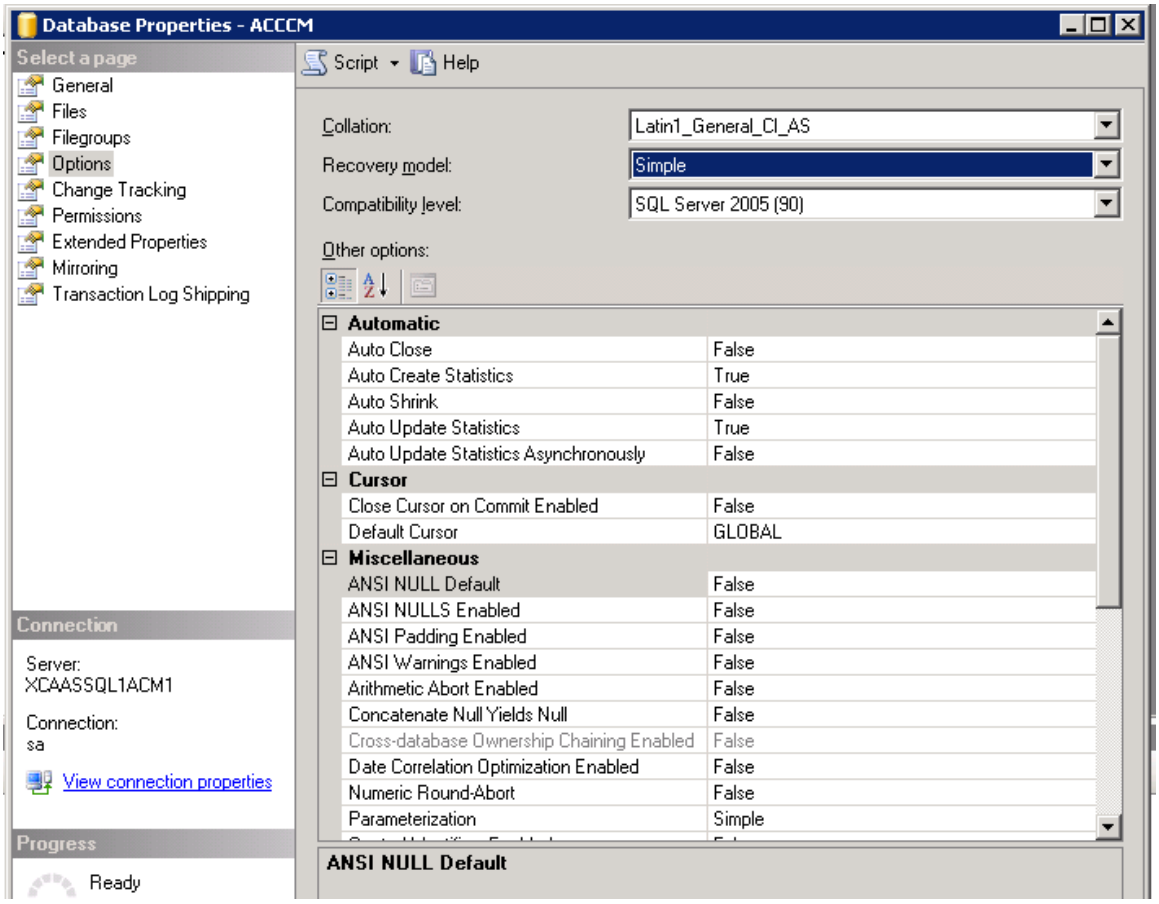
5. In the right pane, under **Database files** in the **File Type**, select **Log**.
6. Click the **…** (ellipsis) button.

   See the following example:



7. In the **Change Autogrowth** screen, set the following options:
   - Select the **Enable Autogrowth** option.
   - Set **File Growth** to **In Megabytes**.
   - Set **Limited to (MB)** to 10000 (10 GB).
8. Click **OK**.
9. In the **Select a page** pane, select **Options**.

   The system displays the following screen:



10. In the **Automatic** options, confirm that **Auto Shrink** is set to **False**.
11. In the **Database Properties** screen, click **OK**.

Chapter 3: Server maintenance procedures

Restoring Control Manager from the restricted to normal mode

About this task

Use the following procedure to restore Control Manager to the normal mode when Control Manager is in the restricted mode.

Procedure

1. Log on as administrator on the Windows server where Control Manager is installed.
2. In System Tray, select **Control Manager** and then right-click **Health Monitoring Tool**.
3. In the **Health Monitoring Tool** window, click the **WebLM Server** tab.
4. In the **WebLM Address** field, enter a valid URI of the WebLM server.
5. To validate the connection, click **Test**.
6. Click **Save**.
7. Log into the Control Manager Server again.

Updating the Windows OS and SQL software on a working system

About this task

Caution:

This task is service interrupting. Schedule this task when there is no traffic, during low traffic periods, or during a scheduled maintenance period. Notify users that the system is down during this maintenance period.

Use this task when you want to update the Microsoft Windows OS or the Microsoft SQL software on a working system. The list of possible updates requiring this procedure includes any of the following update activities:

- Routine updates to the Microsoft Windows software.

- Routine updates to the Microsoft SQL software.
- Upgrades to a new version of Microsoft Windows.
- Upgrades to a new version of Microsoft SQL.

Important:

Any upgrade to a new Windows OS or new SQL software must be supported by this release of Control Manager. For more information about supported versions of third-party software, see *Planning for an Avaya Control Manager Deployment*.

Throughout these procedures, you are instructed to use the Health Monitoring tool to stop and start services on the application servers. This tool is documented in Stopping and starting services using the Health Monitoring tool on page 35.

Procedure

1. Log on to Windows as administrator on the primary database server (ACM-SQL-1).
2. Stop replication on the primary database server (ACM-SQL-1).
3. Log on to Windows as administrator on the secondary application server (ACM-APP-2).
4. Stop the services using the Health Monitoring tool.
5. Log on to Windows as administrator on the primary application server (ACM-APP-1).
6. Stop the services using the Health Monitoring tool.
7. Update the Windows OS software and SQL software on the primary and secondary database servers (ACM-SQL-1 and ACM-SQL-2).
8. Reboot the primary and secondary database servers (ACM-SQL-1 and ACM-SQL-2).
9. For a Legacy HA deployment, reconfigure replication on the primary database server (ACM-SQL-1) based on the procedures in “Configuring replication” chapter in *Installing Avaya Control Manager for Enterprise - Legacy High Availability*.
10. Update the Windows OS software on the primary and secondary application servers (ACM-APP-1 and ACM-APP-2).
11. Reboot the primary and secondary application servers (ACM-APP-1 and ACM-APP-2).
12. For a Legacy HA deployment, confirm that the Control Manager services are in the correct status based on the “Configuring HA services” chapter in *Installing Avaya Control Manager for Enterprise - Legacy High Availability*.
13. For a Multiplex HA deployment:
    - Verify that all of the services are running on the primary application server (ACM-APP-1), except for the HA Service.
    - Verify that none of the independent services are running on the secondary application server (ACM-APP-2). For a list of those services, see *Installing Avaya Control Manager for Enterprise - Multiplex High Availability*.

About rebooting servers

Caution:

This task is service interrupting. Schedule this task when there is no traffic, during low traffic periods, or during a scheduled maintenance period. Notify users that the system is down during this maintenance period.

Use the procedures in this section to reboot the servers in a Control Manager configuration. There is a different procedure for each type of configuration. Best practices suggest you must reboot the servers every 30 days.

Throughout these procedures, you are instructed to use the Health Monitoring tool to stop and start services on the application servers. This tool is documented in Stopping and starting services using the Health Monitoring tool on page 35.

Related links

Rebooting servers in a Multiplex HA 2x2 configuration on page 27
Rebooting servers in a Multiplex HA 2x1 configuration on page 29
Rebooting servers in a Multiplex HA 1x2 configuration on page 30
Rebooting servers in an Enterprise non-HA configuration on page 32
Rebooting servers in an Enterprise HA configuration on page 33

Rebooting servers in a Multiplex HA 2x2 configuration

About this task

Caution:

This task is service interrupting. Schedule this task when there is no traffic, during low traffic periods, or during a scheduled maintenance period. Notify users that the system is down during this maintenance period.

In general, a Multiplex HA 2x2 configuration does not require any specific shut down and rebooting order. However, the procedure shown here does follow a logical pattern just for consistency.

Throughout these procedures, you are instructed to use the Health Monitoring tool to stop and start services on the application servers. This tool is documented in Stopping and starting services using the Health Monitoring tool on page 35.

Procedure

1. Log on to Windows as administrator on the primary application server (ACM-APP-1).
2. Stop the services using the Health Monitoring tool.
3. Log on to Windows as administrator on the secondary application server (ACM-APP-2).
4. Stop the services using the Health Monitoring tool.
5. Log on to Windows as administrator on the primary database server (ACM-SQL-1).

6. Navigate to **Start** > **Run**.
7. Enter `services.msc` and press **Enter**.
8. In the Services window, right-click all of the SQL services and select **Stop**.
9. Reboot the primary database server (ACM-SQL-1).
10. Log on to Windows as administrator on the secondary database server (ACM-SQL-2).
11. Navigate to **Start** > **Run**.
12. Enter `services.msc` and press **Enter**.
13. In the Services window, right-click all of the SQL services and select **Stop**.
14. Reboot the secondary database server (ACM-SQL-2).
15. Log on to Windows as administrator on the primary database server (ACM-SQL-1).
16. Open the **Server Manager**.
17. Navigate to **Tools** > **Failover Cluster Manager**.
18. Right-click **Failover Cluster Manager**, select **Connect to cluster**, and select your cluster from the drop-down list.
19. Click **OK**.
20. Double-click your cluster and select **Nodes**.
21. Verify that all nodes are up.
22. Open the **Microsoft SQL Server Configuration Manager**.
23. Navigate to **SQL Server services**.
24. Right-click **SQL Server *ServerName*** and select **Properties**.
25. Select the **AlwaysOn High Availability** tab.
26. Verify that the **Windows failover cluster name** has the proper value and select the **Enable AlwaysOn Availability Group** option.
27. Click **OK**.
28. Restart the SQL Server Service and the SQL Server Agent Service.
29. Log on to Windows as administrator on the secondary database server (ACM-SQL-2).
30. Open the **Microsoft SQL Server Configuration Manager**.
31. Navigate to **SQL Server services**.
32. Right-click **SQL Server *ServerName*** and select **Properties**.
33. Select the **AlwaysOn High Availability** tab.
34. Verify that the **Windows failover cluster name** has the proper value and select the **Enable AlwaysOn Availability Group** option.
35. Click **OK**.

36. Restart the SQL Server Service and the SQL Server Agent Service.
37. Reboot the primary application server (ACM-APP-1).
38. Log on to Windows as administrator on the primary application server (ACM-APP-1).
39. Open the **Services** tab as described in Diagnostic Monitor on page 54.
40. Verify that all Control Manager services are started.
41. Reboot the secondary application server (ACM-APP-2).
42. Log on to Windows as administrator on the secondary application server (ACM-APP-2).
43. Open the **Services** tab as described in Diagnostic Monitor on page 54.
44. Verify that all Control Manager services are started except for the Audit Log Server, AD Sync, Sync Service, License Tracker Service, and Schedule Server. These services must be set to **Disabled** so that the services does not start automatically. Do not start these services unless instructed during a failover scenario.

Rebooting servers in a Multiplex HA 2x1 configuration

About this task

Caution:

This task is service interrupting. Schedule this task when there is no traffic, during low traffic periods, or during a scheduled maintenance period. Notify users that the system is down during this maintenance period.

In general, a Multiplex HA 2x1 configuration does not require any specific shut down and rebooting order. However, the procedure shown here does follow a logical pattern just for consistency.

Throughout these procedures, you are instructed to use the Health Monitoring tool to stop and start services on the application servers. This tool is documented in Stopping and starting services using the Health Monitoring tool on page 35.

Procedure

1. Log on to Windows as administrator on the primary application server (ACM-APP-1).
2. Stop the services using the Health Monitoring tool.
3. Log on to Windows as administrator on the secondary application server (ACM-APP-2).
4. Stop the services using the Health Monitoring tool.
5. Log on to Windows as administrator on the primary database server (ACM-SQL-1).
6. Navigate to **Start** > **Run**.
7. Enter `services.msc` and press **Enter**.
8. In the Services window, right-click all of the SQL services and select **Stop**.
9. Reboot the primary database server (ACM-SQL-1).

10. Log on to Windows as administrator on the primary database server (ACM-SQL-1).
11. Navigate to **Start** > **Run**.
12. Enter `services.msc` and press **Enter**.
13. Verify that all SQL services are started and that you can log on to the database.
14. Reboot the primary application server (ACM-APP-1).
15. Log on to Windows as administrator on the primary application server (ACM-APP-1).
16. Open the **Services** tab as described in Diagnostic Monitor on page 54.
17. Verify that all Control Manager services are started.
18. Reboot the secondary application server (ACM-APP-2).
19. Log on to Windows as administrator on the secondary application server (ACM-APP-2).
20. Open the **Services** tab as described in Diagnostic Monitor on page 54.
21. Verify that all Control Manager services are started except for the Audit Log Server, AD Sync, Sync Service, License Tracker Service, and Schedule Server. These services must be set to **Disabled** so that the services does not start automatically. Do not start these services unless instructed during a failover scenario.

Rebooting servers in a Multiplex HA 1x2 configuration

About this task

Caution:

This task is service interrupting. Schedule this task when there is no traffic, during low traffic periods, or during a scheduled maintenance period. Notify users that the system is down during this maintenance period.

In general, a Multiplex HA 1x2 configuration does not require any specific shut down and rebooting order. However, the procedure shown here does follow a logical pattern just for consistency.

Throughout these procedures, you are instructed to use the Health Monitoring tool to stop and start services on the application servers. This tool is documented in Stopping and starting services using the Health Monitoring tool on page 35.

Procedure

1. Log on to Windows as administrator on the primary application server (ACM-APP-1).
2. Stop the services using the Health Monitoring tool.
3. Log on to Windows as administrator on the primary database server (ACM-SQL-1).
4. Navigate to **Start** > **Run**.
5. Enter `services.msc` and press **Enter**.
6. In the Services window, right-click all of the SQL services and select **Stop**.

7. Reboot the primary database server (ACM-SQL-1).
8. Log on to Windows as administrator on the secondary database server (ACM-SQL-2).
9. Navigate to **Start** > **Run**.
10. Enter `services.msc` and press **Enter**.
11. In the Services window, right-click all of the SQL services and select **Stop**.
12. Reboot the secondary database server (ACM-SQL-2).
13. Log on to Windows as administrator on the primary database server (ACM-SQL-1).
14. Open the **Server Manager**.
15. Navigate to **Tools** > **Failover Cluster Manager**.
16. Right-click **Failover Cluster Manager**, select **Connect to cluster**, and select your cluster from the drop-down list.
17. Click **OK**.
18. Double-click your cluster and select **Nodes**.
19. Verify that all nodes are up.
20. Open the **Microsoft SQL Server Configuration Manager**.
21. Navigate to **SQL Server services**.
22. Right-click **SQL Server *ServerName*** and select **Properties**.
23. Select the **AlwaysOn High Availability** tab.
24. Verify that the **Windows failover cluster name** has the proper value and select the **Enable AlwaysOn Availability Group** option.
25. Click **OK**.
26. Restart the SQL Server Service and the SQL Server Agent Service.
27. Log on to Windows as administrator on the secondary database server (ACM-SQL-2).
28. Open the **Microsoft SQL Server Configuration Manager**.
29. Navigate to **SQL Server services**.
30. Right-click **SQL Server *ServerName*** and select **Properties**.
31. Select the **AlwaysOn High Availability** tab.
32. Verify that the **Windows failover cluster name** has the proper value and select the **Enable AlwaysOn Availability Group** option.
33. Click **OK**.
34. Restart the SQL Server Service and the SQL Server Agent Service.
35. Reboot the primary database server (ACM-SQL-1).
36. Log on to Windows as administrator on the primary application server (ACM-APP-1).

37. Open the **Services** tab as described in Diagnostic Monitor on page 54.
38. Verify that all Control Manager services are started.

Rebooting servers in an Enterprise non-HA configuration

About this task

Caution:

This task is service interrupting. Schedule this task when there is no traffic, during low traffic periods, or during a scheduled maintenance period. Notify users that the system is down during this maintenance period.

Throughout these procedures, you are instructed to use the Health Monitoring tool to stop and start services on the application servers. This tool is documented in Stopping and starting services using the Health Monitoring tool on page 35.

Procedure

1. Log on to Windows as administrator on the application server (ACM-APP-1).
2. Stop the services using the Health Monitoring tool.
3. Log on to Windows as administrator on the database server (ACM-SQL-1).
4. Navigate to **Start** > **Run**.
5. Enter `services.msc` and press **Enter**.
6. In the Services window, right-click all of the SQL services and select **Stop**.
7. Reboot the database server (ACM-SQL-1).
8. Log on to Windows as administrator on the database server (ACM-SQL-1).
9. Navigate to **Start** > **Run**.
10. Enter `services.msc` and press **Enter**.
11. Verify that all SQL services are started and that you can log on to the database.
12. Reboot the application server (ACM-APP-1).
13. Log on to Windows as administrator on the application server (ACM-APP-1).
14. Open the **Services** tab as described in Diagnostic Monitor on page 54.
15. Verify that all Control Manager services are started.

Rebooting servers in an Enterprise HA configuration

About this task

Caution:

This task is service interrupting. Schedule this task when there is no traffic, during low traffic periods, or during a scheduled maintenance period. Notify users that the system is down during this maintenance period.

Throughout these procedures, you are instructed to use the Health Monitoring tool to stop and start services on the application servers. This tool is documented in Stopping and starting services using the Health Monitoring tool on page 35.

Procedure

1. Log on to Windows as administrator on the secondary application server (ACM-APP-2).
2. Stop the services using the Health Monitoring tool.
3. Log on to Windows as administrator on the primary application server (ACM-APP-1).
4. Stop the services using the Health Monitoring tool.
5. Log on to Windows as administrator on the primary database server (ACM-SQL-1).
6. Stop replication on the primary database server (ACM-SQL-1).
7. Navigate to **Start** > **Run**.
8. Enter `services.msc` and press **Enter**.
9. In the Services window, right-click all of the SQL services and select **Stop**.
10. Log on to Windows as administrator on the secondary database server (ACM-SQL-2).
11. Navigate to **Start** > **Run**.
12. Enter `services.msc` and press **Enter**.
13. In the Services window, right-click all of the SQL services and select **Stop**.
14. Reboot the primary database server (ACM-SQL-1).
15. Log on to Windows as administrator on the primary database server (ACM-SQL-1).
16. Navigate to **Start** > **Run**.
17. Enter `services.msc` and press **Enter**.
18. Verify that all SQL services are started and that you can log on to the database.
19. Reboot the secondary database server (ACM-SQL-2).
20. Log on to Windows as administrator on the secondary database server (ACM-SQL-2).
21. Navigate to **Start** > **Run**.
22. Enter `services.msc` and press **Enter**.

23. Verify that all SQL services are started and that you can log on to the database.
24. Reboot the primary application server (ACM-APP-1).
25. Log on to Windows as administrator on the primary application server (ACM-APP-1).
26. Verify that the connectionString variable in `C:\Windows\System32\NAV360Config.xml` points to the primary database server (ACM-SQL-1).
27. Open the **Services** tab as described in Diagnostic Monitor on page 54.
28. Verify that all Control Manager services are started except for the HA-related services: Audit Log Server, License Tracker Service, Sync Service, Sphere Feeder, AD Sync, Schedule Server, CM Syslog Server, and HA Service. These services must be set to Manual so that the services does not start automatically. Do not start these services yet.
29. Reboot the secondary application server (ACM-APP-2).
30. Log on to Windows as administrator on the secondary application server (ACM-APP-2).
31. Verify that the connectionString variable in `C:\Windows\System32\NAV360Config.xml` points to the primary database server (ACM-SQL-1).
32. Open the **Services** tab as described in Diagnostic Monitor on page 54.
33. Verify that all Control Manager services are started except for the HA-related services: Audit Log Server, License Tracker Service, Sync Service, Sphere Feeder, AD Sync, Schedule Server, CM Syslog Server, and HA Service. These services must be set to Manual so that the services does not start automatically. Do not start these services yet.
34. Start replication on the primary database server (ACM-SQL-1). Verify that the replication process is complete before continuing with any other steps.
35. Log on to Windows as administrator on the primary application server (ACM-APP-1).
36. Start the remaining services using the Health Monitoring tool.
37. Log on to Windows as administrator on the secondary application server (ACM-APP-2).
38. Navigate to **Start** > **Run**.
39. Enter `services.msc` and press **Enter**.
40. Right-click **ACCCM HA Service** and click **Start**.
41. Open the HA log files on both application servers (ACM-APP-1 and ACM-APP-2) and confirm that there are no errors in the log files.

Stopping and starting services using the Health Monitoring tool

About this task

Use the Health Monitoring tool to automatically stop and start Control Manager services. The tool automatically stops and starts the services in the proper order and saves time compared to stopping and starting individual services.

Procedure

1. Log on as administrator on the Windows server where Control Manager is installed.
2. Right-click the Health Monitoring tool status icon.

   Depending on whether there are any services stopped that require starting, the sub-menu shows either **Start Services** or **Stop Services**.
3. Click **Start Services** or **Stop Services**.

   The system either stops any services that are currently running or starts any services that are not running.

Updating the Java version

About this task

Caution:

This task is service interrupting. Schedule this task when there is no traffic, during low traffic periods, or during a scheduled maintenance period. Notify users that the system is down during this maintenance period.

Control Manager supports only specific versions of Java Runtime Environment (JRE), also known as OpenJDK. However, some customers require an updated version of OpenJDK, often for security reasons. Use this procedure to delete the standard OpenJDK software and install a new customer-required OpenJDK software.

Important:

Avaya recommends that you do not update the version of OpenJDK. If the customer security policy requires an update, you may update the OpenJDK. This procedure can be used only for an updated build number without changing the OpenJDK minor or major number. For example, OpenJDK 1.8_172 can be updated to OpenJDK 1.8_192, but OpenJDK 1.8 cannot be updated to OpenJDK 1.9.

Before you begin

You must download the OpenJDK software from the following web site:

https://www.azul.com/downloads/zulu/zulu-windows/

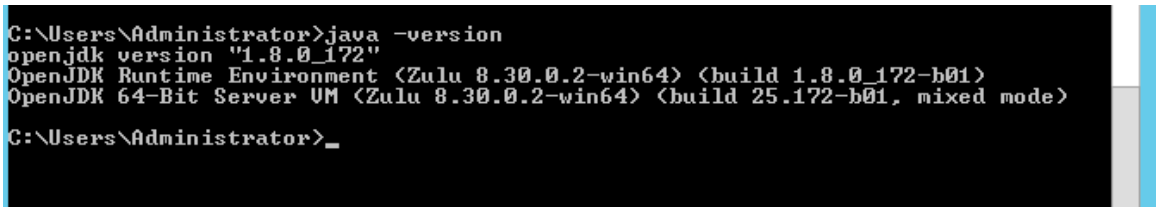
Navigate to the list of archived versions of the software. You must select a Java Version 8, 64-bit Server version of the software. You cannot use any other versions of the software.

Procedure

1. Log on to Windows as administrator on the primary application server (ACM-APP-1).
2. Open a command line window.
3. Enter the following command:

   `java -version`

   The system displays the version of the OpenJDK installation. See the following example:

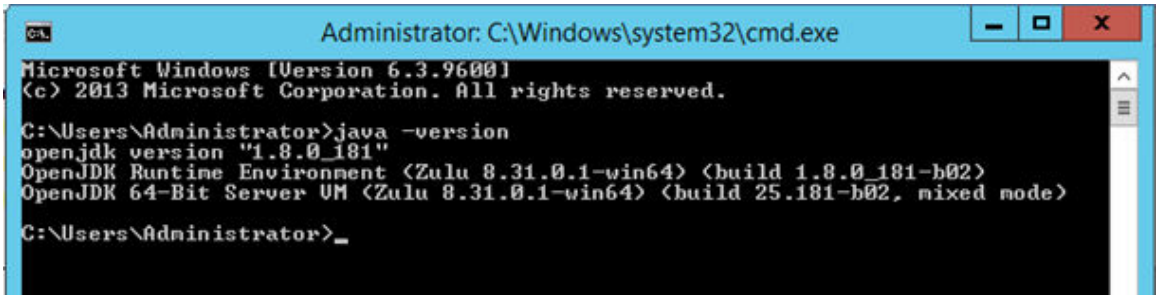
4. Navigate to **Start** > **Control Panel** > **Programs and Features**.
5. Click on the current version of the OpenJDK software.
6. Click **Uninstall**. For any options, use the default entries.

   The uninstall program displays a warning message about requiring a reboot to update files or services.
7. Click **OK**.

   The uninstall program displays a warning message that you must restart your system.
8. Click **Yes** to restart the system now.
9. Log on to Windows as administrator on the server.
10. Navigate to the **Program Files** folder for the OpenJDK software installed on the server.
11. Right-click the top-level folder and select **Delete**.
12. Navigate to the folder where you have downloaded the new OpenJDK software.
13. Right-click the OpenJDK executable install file and select **Run as Administrator**. Accept all of the default installation options.
14. Confirm that the new OpenJDK software is installed by doing the following steps:
    a. Enter the following command:

       `java -version`

       The system displays the new version of the OpenJDK installation. See the following example:



b. Navigate to **Start** > **Control Panel** > **Programs and Features**.

c. Confirm that the new OpenJDK software is in the list of programs.

15. In Windows Explorer, right-click on **This PC** and select **Properties**.

    The system displays the basic information about the computer.

16. Click **Change settings**.

    The system displays the System Properties dialog.

17. Click the **Advanced** tab.

18. Click **Environment Variables**.

    The system displays the Environment Variables dialog.

19. In the **System variables** section, double-click the **Path** variable.

    The system opens the **Path** variable in the Edit environment variable dialog.

20. Add the following line to the **Path** variable:

    `C:\Program Files\Zulu\zulu-8\bin; C:\Program Files\Zulu\zulu-8\jre\bin`

21. Click **OK**.

22. In the **System variables** section, double-click the **JRE_HOME** variable.

    The system opens the **JRE_HOME** variable in the Edit environment variable dialog.

23. Add the following line to the **JRE_HOME** variable:

    `C:\Program Files\Zulu\zulu-8`

24. Click **OK** on each Environment Variable dialog to save your changes.

25. Navigate to **Start** > **Shut Down** > **Restart** to restart the server.

26. Log on to Windows as administrator on the server.

27. Navigate to *`InstallDirectory`*`\Avaya Control Manager\Services\Tomcat\bin`.

28. Right-click on `tomcat8w.exe` and select **Open**.

29. Select the **Java** tab.

30. In the **Java Virtual Machine** option, click **Browse** to locate the `jvm.dll` file you just installed.
31. Click **OK**.
32. Navigate to **Start** > **Run**.
33. Enter `services.msc` and press **Enter**.
34. In the Services window, right-click **Tomcat** and select **Start**.
35. Repeat this procedure on the secondary application server (ACM-APP-2).

Correcting the Windows time setting on Control Manager servers

About this task

Caution:

This task is service interrupting. Schedule this task when there is no traffic, during low traffic periods, or during a scheduled maintenance period. Notify users that the system is down during this maintenance period.

When a Control Manager system was first installed, the Windows time setting must have set up accurately on all of the servers in the deployment. If that was not done correctly, or if the Windows time settings on the different servers are no longer correct, use this procedure to correct the Windows time setting.

Be aware of the following potential interactions when you adjust the Windows time setting on your servers:

Time Change Direction	Server Type	Interaction
Moving time forward	Application servers	Reports, such as License Tracker reports, might have empty gaps of time in reports. Scheduled activities might not run at the expected times if the time period has been skipped with the new time setting. Log portal entries and activities might have gaps in time.
	SQL database servers	All data timestamps have gaps in time.

Table continues…

Time Change Direction	Server Type	Interaction
Moving time backward	Application servers	Reports, such as License Tracker reports, might have duplicate lines of data because the time was rolled back. Scheduled activities might run twice because the time was rolled back. Those activities include skill set changes, synchronization, imports, bulk activities, and delayed saves. Log portal entries and activities might have duplicate entries because the time was rolled back.
	SQL database servers	All data timestamps might have “future” dates after the time is rolled back.

Throughout these procedures, you are instructed to use the Health Monitoring tool to stop and start services on the application servers. This tool is documented in Stopping and starting services using the Health Monitoring tool on page 35.

Procedure

1. For a non-HA system, do the following steps:
   a. Log on to Windows as administrator on the application server (ACM-APP-1).
   b. Stop the services using the Health Monitoring tool.
   c. Shut down the IIS Service.
   d. Correct the date and time on the application server (ACM-APP-1).
   e. Reboot the application server (ACM-APP-1).
   f. Log on to Windows as administrator on the SQL database server (ACM-SQL-1).
   g. Correct the date and time on the SQL database server (ACM-SQL-1).
   h. Reboot the SQL database server (ACM-SQL-1).
2. For an Enterprise HA system, do the following steps:
   a. Log on to Windows as administrator on the primary application server (ACM-APP-1).
   b. Stop the services using the Health Monitoring tool.
   c. Log on to Windows as administrator on the secondary application server (ACM-APP-2).
   d. Stop the services using the Health Monitoring tool.
   e. Shut down the IIS Service.
   f. Correct the date and time on the primary and secondary application servers (ACM-APP-1 and ACM-APP-2).
   g. Reboot the primary and secondary application servers (ACM-APP-1 and ACM-APP-2).

h. Stop the services using the Health Monitoring tool.
i. Reboot the primary and secondary UI servers (ACM-UI-1 and ACM-UI-2).
j. Log on to Windows as administrator on the primary SQL database server (ACM-SQL-1).
k. Shut down the IIS Service.
l. Correct the date and time on the primary SQL database server (ACM-SQL-1).
m. Log on to Windows as administrator on the secondary SQL database server (ACM-SQL-2).
n. Shut down the IIS Service.
o. Correct the date and time on the secondary SQL database server (ACM-SQL-2).
p. Reboot the primary and secondary SQL database servers (ACM-SQL-1 and ACM-SQL-2).

3. For an Enterprise Multiplex HA system, do the following steps:
   a. Log on to Windows as administrator on the primary application server (ACM-APP-1).
   b. Stop the services using the Health Monitoring tool.
   c. For a Multiplex HA 2x2 or 2x1 configuration, log on to Windows as administrator on the secondary application server (ACM-APP-2).
   d. Stop the services using the Health Monitoring tool.
   e. Shut down the IIS Service.
   f. Correct the date and time on the primary and secondary application servers (ACM-APP-1 and ACM-APP-2).
   g. Reboot the primary and secondary application servers (ACM-APP-1 and ACM-APP-2).
   h. Log on to Windows as administrator on the primary SQL database server (ACM-SQL-1).
   i. Shut down the IIS Service.
   j. Correct the date and time on the primary SQL database server (ACM-SQL-1).
   k. For a Multiplex HA 2x2 or 1x2 configuration, log on to Windows as administrator on the secondary SQL database server (ACM-SQL-2).
   l. Shut down the IIS Service.
   m. Correct the date and time on the secondary SQL database server (ACM-SQL-2).
   n. Reboot the primary and secondary SQL database servers (ACM-SQL-1 and ACM-SQL-2).

Renewing the expired certificate

About this task

Use the following procedures to renew the expired certificate.

Procedure

1. Open IIS on the ACM application.
2. Under **Connection**, click **Host Name**.
3. In the center window pane, double-click **Server Certificates**.
4. In the **Center Window** pane, click the expired certificate and then click the **Renew** option.
5. Select **Renew** an existing certificate then click **Next**.
6. On the Specify online certificate server authority page, click **Select** and then select your own CA which has the same name in the `Issued By` column on step 4 and click **OK**.
7. Click **Finish**.

   The system extends the expiration date of certificate to five months.
8. To configure Port 443, refer to *Enabling SSL for secure browser access* in the *Installing Avaya Control Manager* guide.
9. To configure Port 9011, run the following command on Power Shell to delete the old binding:

   ```
   netsh http delete sslcert ipport=0.0.0.0:9011
   ```
10. To bind the certificate, follow the *Binding the certificate to SSL port 9011* section in the *Installing Avaya Control Manager Enterprise - Non-HA* guide.

Uninstalling the Control Manager system

About this task

To uninstall the Control Manager software, perform this procedure on every server that has Control Manager software.

Procedure

1. Log on to Windows on one of the Control Manager servers.
2. Stop the services using the Health Monitoring tool.
3. Open a console window.
4. Log on to the console as a root user.
5. Open Windows Explorer and locate the Control Manager software you downloaded from the Avaya support site.

6. Right-click the Control Manager executable file and select **Run as Administrator**. The name of the file is similar to the following example:

   `ACM.ReleaseNumber.BuildNumber.exe`

   - **Welcome to the Prerequisites Wizard** - If the system displays this screen, you step through one or two more prerequisites screens where software might be installed on your system. Click **Next** to advance to the next screen.
   - **Welcome to the Avaya Control Manager *Release Number Build Number* Setup Wizard** - This is the final introductory screen you see before configuring the installation parameters.

7. On the Modify, Repair or Remove installation screen, click Remove.

   The system removes the following components from the Control Manager server:

Component	Action
Databases	The wizard does not delete any existing databases or database users.
Web sites	The wizard removes the websites from IIS and files on the file system.
Services	The wizard removes Windows services and all files on the file system.

8. Repeat this procedure on all servers that have Control Manager software.

Next steps

At the end of the removal process, the wizard removes the Control Manager system from the server. However, the wizard retains the prerequisites and database related components in the system. You must remove these components manually.

Related links

Removing the prerequisite components manually on page 42
Removing the Control Manager services manually on page 43
Removing the Control Manager databases manually on page 45

Removing the prerequisite components manually

About this task

The Control Manager installation wizard might not remove the prerequisite components if the services are installed as part of the Control Manager installation process.

For example, Tomcat is installed under the following Windows folder:

`Program Files (x86)\Avaya\Avaya Control Manager`

This folder cannot be deleted unless Tomcat is removed. If you do remove Tomcat as described below, you must manually delete the following registry key:

`HKLM\SOFTWARE\Wow6432Node\Apache Software Foundation`

Procedure

1. Log on to the Control Manager application server as Administrator.
2. Navigate to **Start** > **Control Panel** > **All Control Panel Items** and click **Programs and Features**.
3. On the Uninstall or change a program screen, right-click on the prerequisite application that you want to uninstall and click **Uninstall**.

   The system removes the selected component from the server.
4. Repeat this procedure for prerequisite applications, including Tomcat.
5. To confirm that Tomcat has been uninstalled, open the Registry editor and confirm that the following registry key has been deleted:

   `HKLM\SOFTWARE\Wow6432Node\Apache Software Foundation`
6. If the Tomcat (Apache) registry key has not been deleted, delete it manually from the registry.

Removing the Control Manager services manually

About this task

The Control Manager installation wizard might not remove all Control Manager services if the services were installed as part of the Control Manager installation process. You must remove the Control Manager services manually.

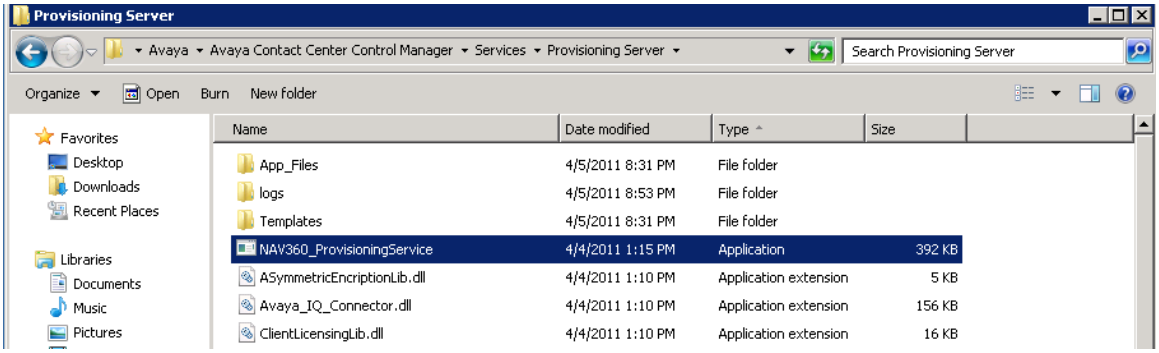
Before you begin

Confirm that all Control Manager services have been stopped as described in *Uninstalling the Control Manager system*.

Procedure

1. Log on to the Control Manager application server as Administrator.
2. Navigate to the folder of the service you want to remove. For example, to remove Provisioning Server, navigate to **Avaya** > **Avaya Control Manager** > **Services** and click the **Provisioning Server** folder.

   The system displays the following screen:



3. On the Provisioning Server screen, locate the service executable file.

   Note:

   The service executable file is marked as application under the **Type** column.

4. Open the Windows command line interface using the **Run as administrator** option.
5. At the prompt, enter the following command:

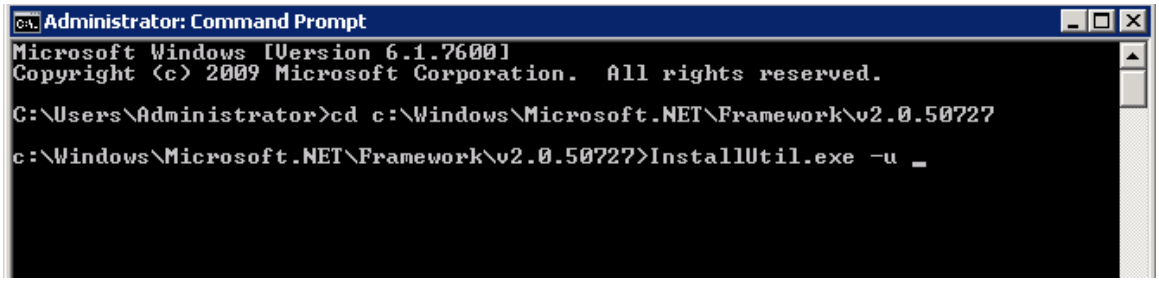
   ```
   cd c:\windows\microsoft.net\framework\v2.0.50727
   ```

6. At the prompt, enter the following command:

   Important:

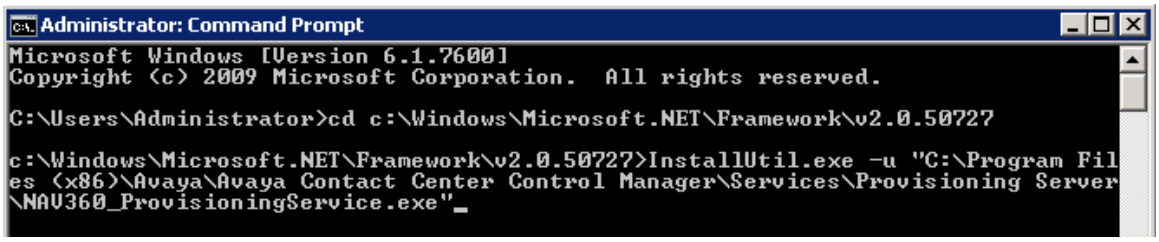
   Do not press the ENTER key after you enter this command.

   ```
   installUtil.exe – u
   ```



7. Drag the Provisioning Server exe file from the service folder and drop it in to the command line window.

   See the following example:



8. Press **Enter**.

The system uninstalls the selected service.

Important:

The manual uninstall does not update the Control Manager installation wizard. If you attempt to reinstall the service again through the installation wizard, the wizard does not recognize the service because the service was uninstalled from the system. The wizard marks it as a service that exists on the server.

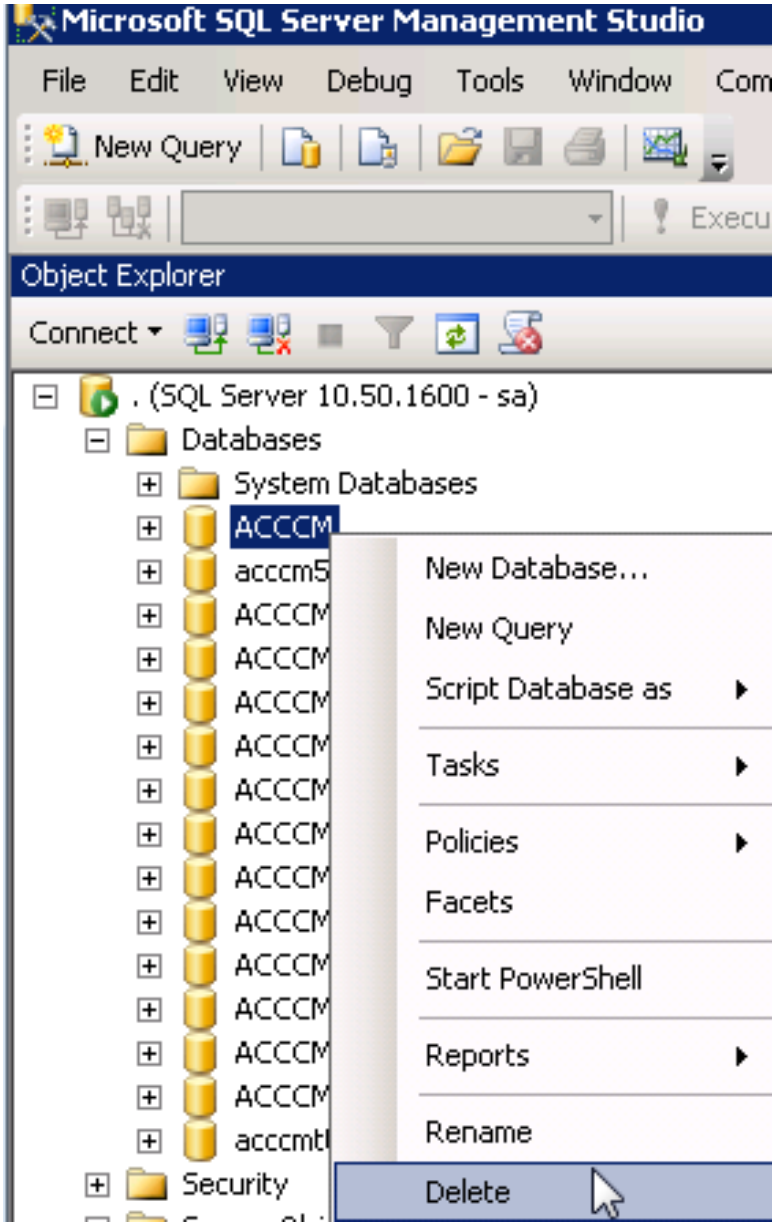
Removing the Control Manager databases manually

About this task

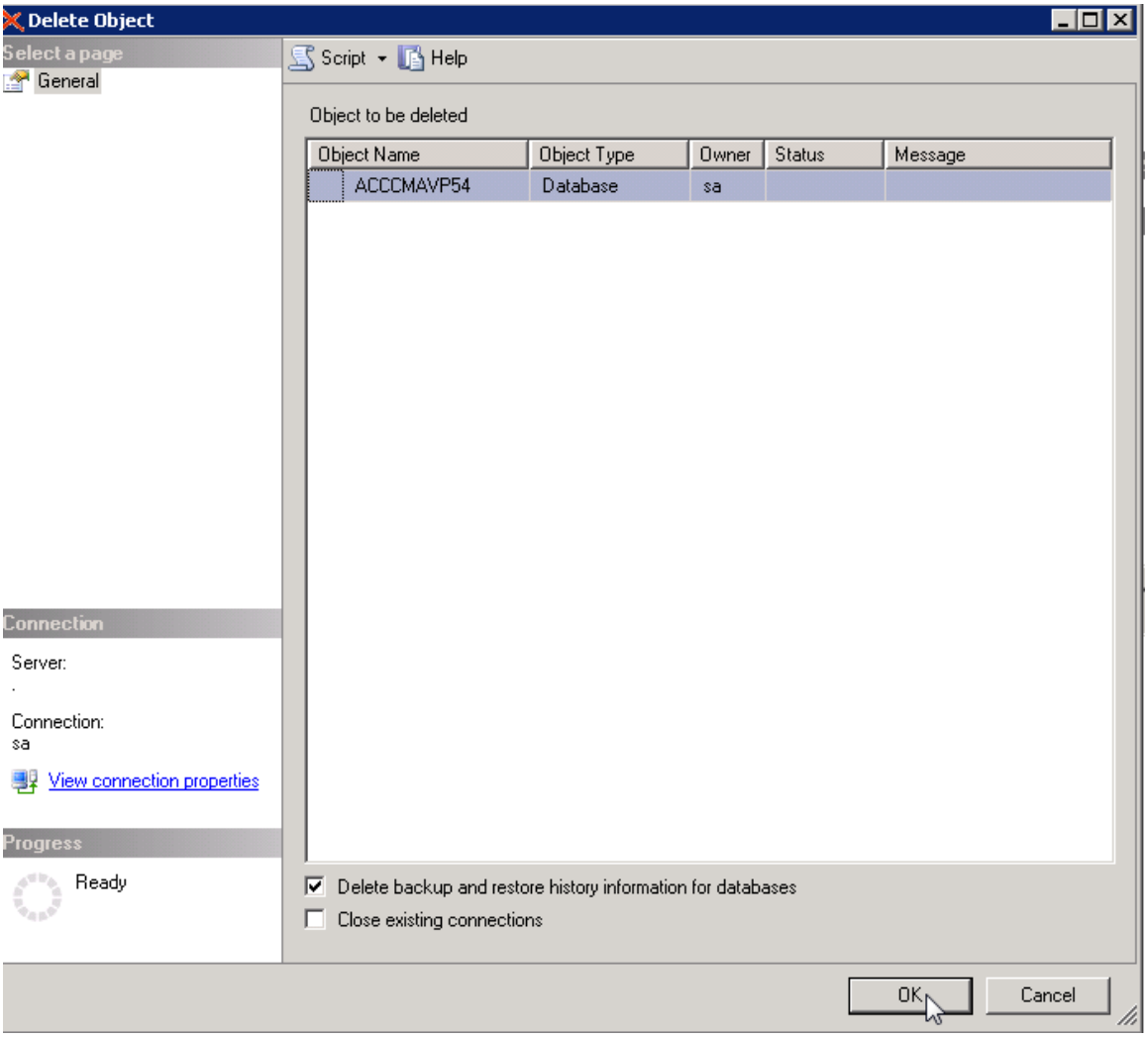
The Control Manager installation program does not remove the Control Manager databases during the removal process of the Control Manager system. You must remove the Control Manager databases manually.

Procedure

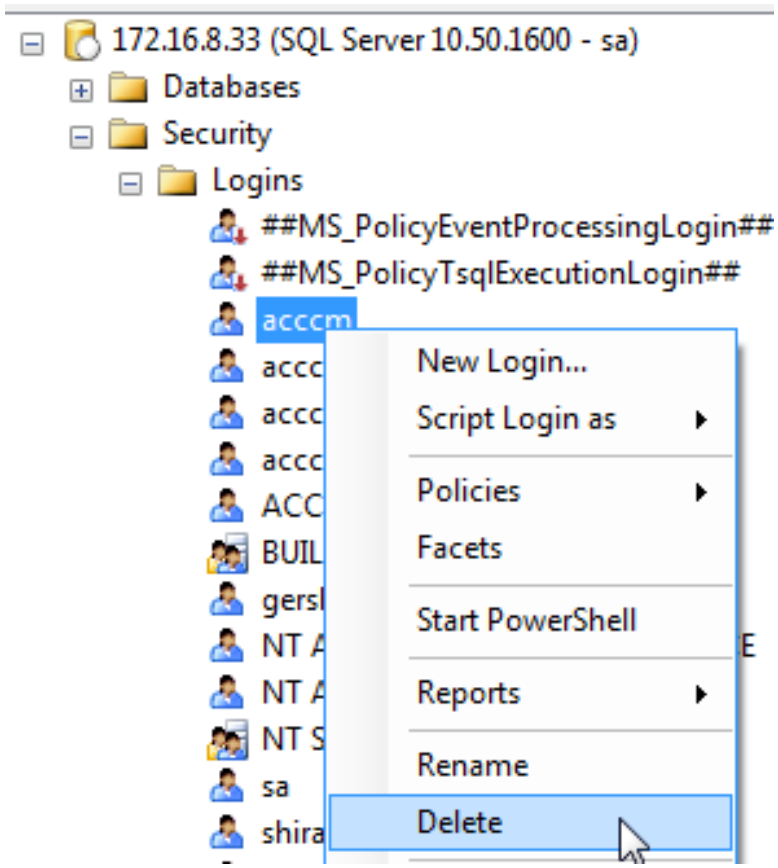
1. Open SQL Management Studio on one of the database servers.
2. Log on with an SA account or as an account with similar permissions.
3. Navigate to the **ACCCM** folder and select **Delete** as shown in the following example:



The system displays the following screen:



4. In the Delete Object screen, select the Close existing connection option if there are services that are still connected to the Control Manager database.
5. Click **OK**.
6. To delete a database user, navigate to the main Security > Logins folder under the Server.
7. Right-click the ACCCM user and select Delete as shown in the following example;



8. Repeat this procedure for the following databases and database users:
   - ACCCMAVP
   - ACCCMONEXDB
   - ACCCMSYNC
   - ACCCMCMSYSLOG
   - ACM_BILLING or ACCCMBilling
9. Repeat this procedure for all database servers.

Chapter 4: Configuration maintenance procedures

Getting Control Manager licenses

About this task

When log in for the first time, Control Manager operates in Grace mode for 30 days without applying license and a banner is displayed indicating the remaining days in the Grace mode. Ensure to configure WebLM server with valid license within the Grace period.

There are many reasons why you might need to get new licenses for :

- When upgrading (migrating) from Control Manager 7.x or Control Manager 8.x systems to Control Manager 9.0.
- When activating new connectors for additional Avaya products.
- Before making Control Manager 9.0 operational.

For Control Manager 9.0 WebLM server must have valid control manager license installed. This WebLM server can be configured in Control Manager post installation or upgrade.

Control Manager operates in Grace mode for 30 days until a WebLM server with valid license is configured.

If WebLM license is not configured in 30 days grace period also then Control Manager enters in restricted mode and user can not login. In such case WebLM server can be configured through Health Monitoring tool. For more information see the section *Troubleshooting tools* in the *Maintaining and Troubleshooting Avaya Control Manager 9.0* guide.

Note:

Without a valid WebLM license Control Manager 9.0 goes into 30 days grace mode.

Before you begin

Ensure that Control Manager license is already installed on WebLM server.

Note:

For more information on installing license on WebLM server see WebLM documentation.

Procedure

1. On the Control Manager web portal, navigate to **Configuration** > **Licenses** > **WebLM Server**

2. Click **Add**.
3. Fill in the WebLM address.

   For example, https://<WebLM_Server_Address>:52233/WebLM/LicenseServer
4. To check the connectivity click **Test**, if the connection is successful then click **Save**.
5. Restart the License Server service.
   a. In the **Run** window, type **`services.msc`**.
   b. Services window opens navigate to **ACCCM License Server** and right click and restart.

   Ensure that a WebLM server with valid control manager license is always configured with Control Manager. If WebLM server is not configured then see the section *Testing the installation*

   If Control Manager displays any licensing related warning or error and WebLM server is already configured then see the guide *Avaya Control Manager Maintaining and Troubleshooting* for steps for troubleshooting the issues.

Installing Control Manager licenses

About this task

When log in for the first time, Control Manager operates in Grace mode for 30 days without applying license and a banner is displayed indicating the remaining days in the Grace mode. Ensure to configure WebLM server with valid license within the Grace period.

There are many reasons why you might need to get new licenses for :

- When upgrading (migrating) from Control Manager 7.x or Control Manager 8.x systems to Control Manager 9.0.
- When activating new connectors for additional Avaya products.
- Before making Control Manager 9.0 operational.

For Control Manager 9.0 WebLM server must have valid control manager license installed. This WebLM server can be configured in Control Manager post installation or upgrade.

Control Manager operates in Grace mode for 30 days until a WebLM server with valid license is configured.

If WebLM license is not configured in 30 days grace period also then Control Manager enters in restricted mode and user can not login. In such case WebLM server can be configured through Health Monitoring tool. For more information see the section *Troubleshooting tools* in the *Maintaining and Troubleshooting Avaya Control Manager 9.0* guide.

Note:

Without a valid WebLM license Control Manager 9.0 goes into 30 days grace mode.

Before you begin

Get your license file(s) as described in Getting Control Manager licenses on page 49.

Procedure

1. On the Control Manager web portal, navigate to **Configuration** > **Licenses** > **WebLM Server**
2. Click **Add**.
3. Fill in the WebLM address and its version.
4. To check the connectivity click **Test**, if the connection is successful then click **Save**.

No one-X license found

Condition

When I launch the ACM log-in page, I see the following error message:

```
No one-X license found
```

Cause

This error occurs if the **one-X Agent** field displays Not Licensed in **ACM** > **Provisioning Service** > **Connectors** tab.

Solution

- The one-X agent field in **ACM** > **Provisioning Service** > **Connectors** tab takes the values either from the one-X Agent or the AAFD database.
- You must ensure that the values are present as appropriate in the one-X Agent or the AAFD database for ACM to apply the one-X Agent license.

Chapter 5: Troubleshooting tools

Control Manager health monitoring

Health Monitoring (HM) provides several features to better help diagnose problems. This tool provides the following features:

- Ability to start and stop Control Manager services from Task-tray icon
- Generates regular diagnostic reports
- Log management which include the ability to purge older log files
- Provides at a glance diagnostics health checks
- Provides resource tracking for Control Manager Services and Web Portals
- System and Application metric collection
- Task-tray icon which indicates Control Manager version, deployment type and status info (including HA state)
- Validation checking on key indicators

Components

Health Monitoring has the following components:

- Diagnostic Monitor

  A thin GUI client which displays important diagnostics and metric.

- Health Monitor Service (HMS)

  A windows services which periodically gathers diagnostics information on behalf of its clients (i.e. DM).

- Health Monitor Status Icon

  A Window Task Tray icon which presents status information to the User.

Starting the Health Monitor Status tool

About this task

By default, the Health Monitor Status tool is running on all Control Manager application servers. However, you can exit from the tool, so use this procedure to restart the Health Monitor Status tool.

Before you begin

Before you use the tool, you must set the **Run the program as an Administrator** option in the tool properties as described in this task. Once you have set this option, you do not have to set the option again.

Procedure

1. Log on to Windows as administrator on the application server.
2. Navigate to `c:\Program Files (x86)\Avaya\Avaya Control Manager \Services\ACCCM Health Monitoring`.
3. Right-click the `HealthMonitorStatus.exe` file.
4. Select **Properties**.
5. Under the **Compatibility** tab, select the **Run the program as an Administrator** option.
6. Click **OK**.
7. Right-click the `HealthMonitorStatus.exe` file.
8. Click **Run**.

   The Health Monitor Status tool opens. The Health Monitor Status icon displays on the system tray on the Windows server.
9. Repeat these steps on the other application server, if using HA.

Starting the Health Monitor Status tool in a non-system drive

About this task

Use the following steps if Control Manager in installed in a non-system drive (other than the C drive):

Procedure

1. Log on to Windows as administrator on the application server.
2. Navigate to a non-system drive. For instance, if you installed Control Manager on the D drive of the Windows server, go to **D Drive** > **Program Files (x86)** > **Avaya** > **Avaya Control Manager** > **Services** > **ACCCM Health Monitoring**.
3. Right-click the `HealthMonitorStatus.exe` file and select the **Run as administrator** option.

   The systems launches the Health Monitor Status tool. The **Health Monitor Status** icon displays on the system tray.

Diagnostic Monitor

About the Diagnostic Monitor

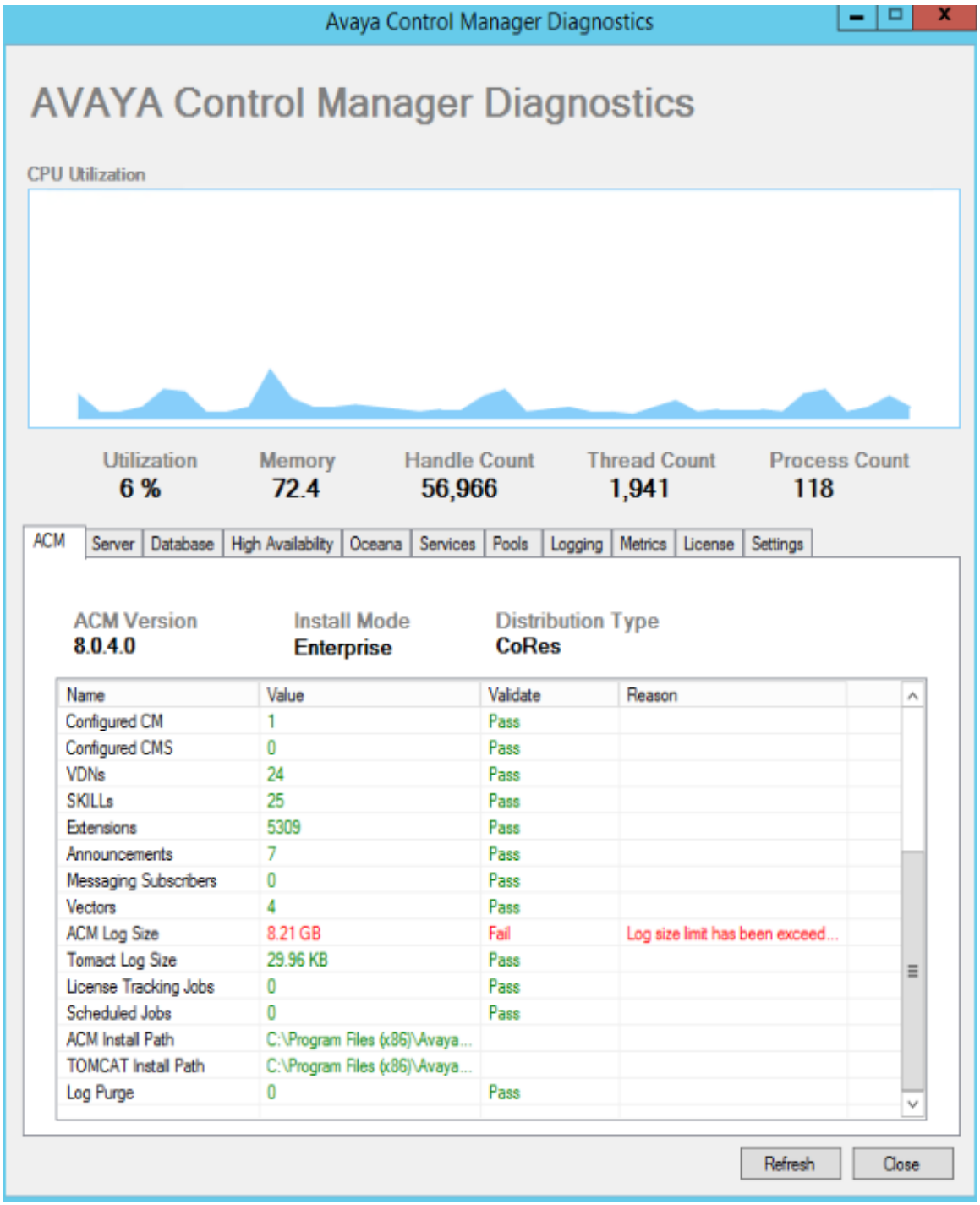
The Health Monitor Status tool Diagnostic Monitor provides general system status and access to specific areas of the Control Manager deployment.

The top half of the Diagnostic Monitor screen provides a real-time graph of the system CPU along with other important metrics like Memory usage. These indicators allow you to quickly understand the overall health of the server. This information updates automatically and is displayed no matter which tab you select.

The bottom half of the Diagnostic Monitor screen has several tabs that contain more specific information related to Control Manager and its environment.

ACM

The **ACM** (Control Manager) tab shows information about the overall Control Manager deployment. Any values that exceed the stated capacity threshold display a failure.



Option	Description
ACM Version	The Control Manager release installed on the server.
Install Mode	The type of deployment installed on the server.

Table continues…

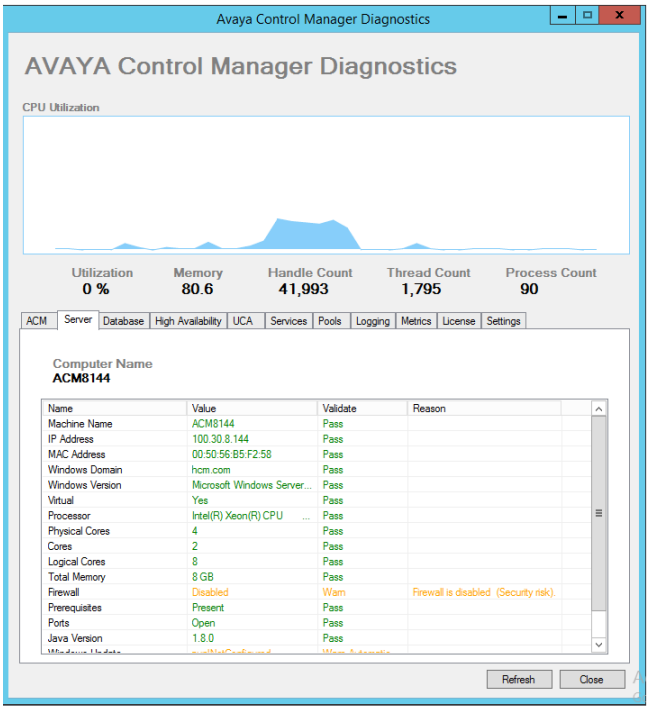
Option	Description
Install Distribution Type	The distribution method selected when you installed the Control Manager software on the server. The values are CoRes (All), Application (Services), and Web (UI). • CoRes (“All” on the installation screens) • Application (“Services” on the installation screens) • Web (“UI” on the installation screens)
Deployment Type	Whether the deployment is HA or Standard.
High Availability Role	Indicates the current role of a HA deployment.
Administrator Accounts	Number of administrator users.
Agents	Number of administered agents.
Locations	Number of administered locations.
Virtual Groups	Number of administered virtual groups.
Configured CM	Number of administered Communication Manager systems.
Configured CMS	Number of administered Call Management System servers.
VDNs	Number of administered VDNs.
Skills	Number of administered skills.
Extensions	Number of administered extensions.
Announcements	Number of administered announcements.
Messaging Subscribers	Number of administered voice messaging subscribers.
Vectors	Number of administered vectors.
ACM Log Size	The total size of all log files under the Control Manager installation folder.
Tomcat Log Size	The total size of all log files under the Tomcat installation folder.
License Tracking Jobs	The total number of license tracking entities administered in Control Manager.
Scheduled Jobs	The total number of scheduled jobs administered to run in Control Manager.
ACM Install Path	The installation path for the Control Manager software.
Tomcat Install Path	The installation path for Tomcat.

Table continues…

Option	Description
Log Purge	The administered setting for purging log files. This value is administered on the **Settings** tab. 0 = Disabled 1 = Purge files older than 2 weeks 2 = Purge files older than 1 month 3 = Purge files older than 3 months 4 = Purge files older than 6 months 5 = Purge files older than 1 year

Server

The **Server** tab shows information relating to the server and the Windows operating system. Validation checking is done on all data points with errors or warnings shown for any anomalies.



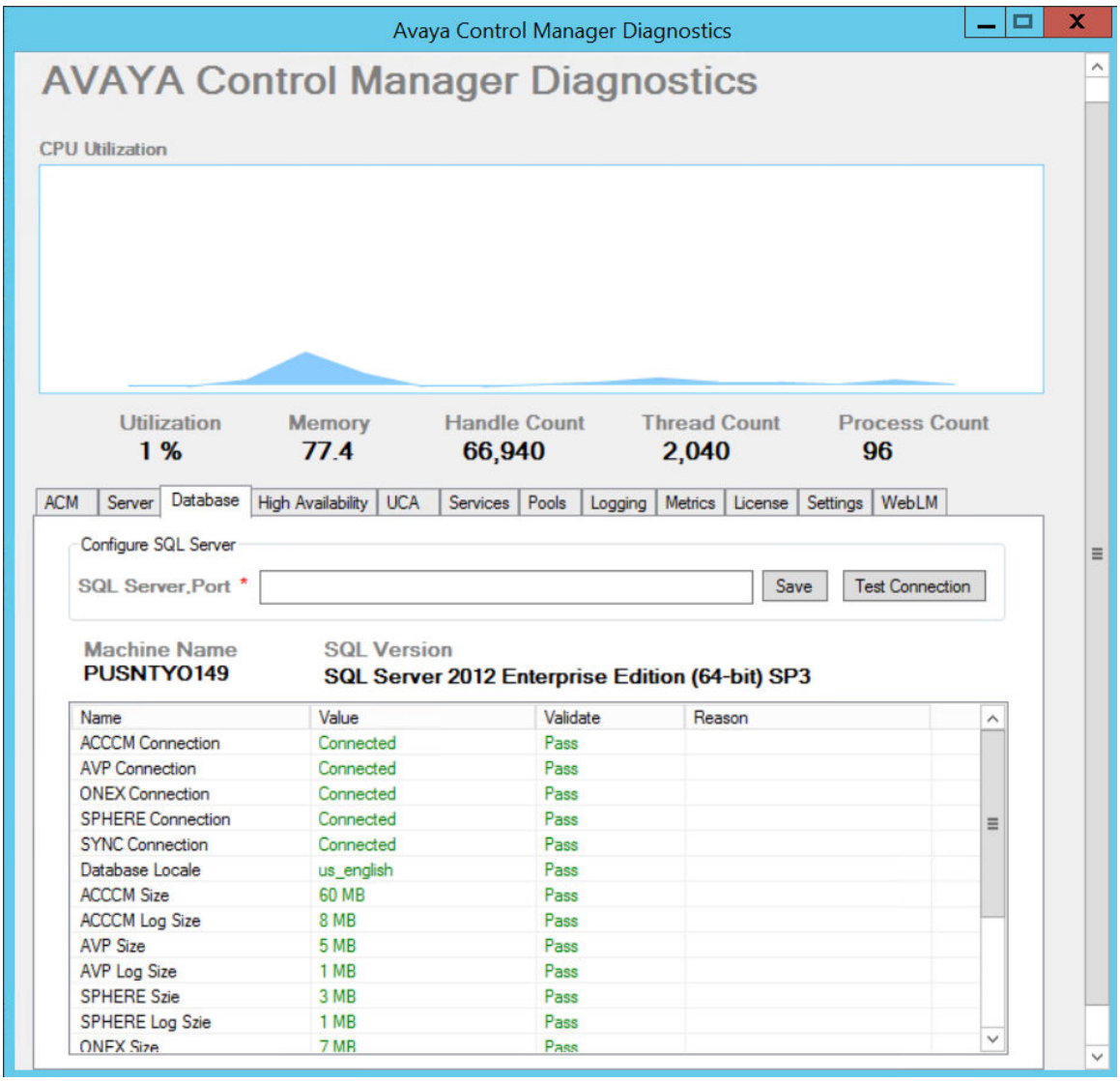
Option	Description
Machine Name	The host name of the server.
IP Address	The IP address of the server.
MAC Address	The MAC address of the server.
Windows Domain	The name of the Windows Domain. An empty field indicates the server belongs to a Workgroup.

Table continues…

Option	Description
Windows Version	The full name of the Windows OS.
Virtual	Indicates whether Control Manager is running on a virtual OS.
Processor	The full name of the processor.
Cores	Number of cores.
Logical Cores	Number of logical cores.
Physical Cores	Number of physical cores.
Total Memory	Total amount of RAM.
Firewall	Indicates whether the Windows firewall is enabled.
Prerequisites	Indicates whether all the required prerequisites have been installed.
Ports	Indicates whether any of the main Control Manager ports have been blocked.
Java Version	The installed Java version.
Windows update	Indicates whether Windows update is configured.
Windows Processes	The total number of processes running on the OS.

Database

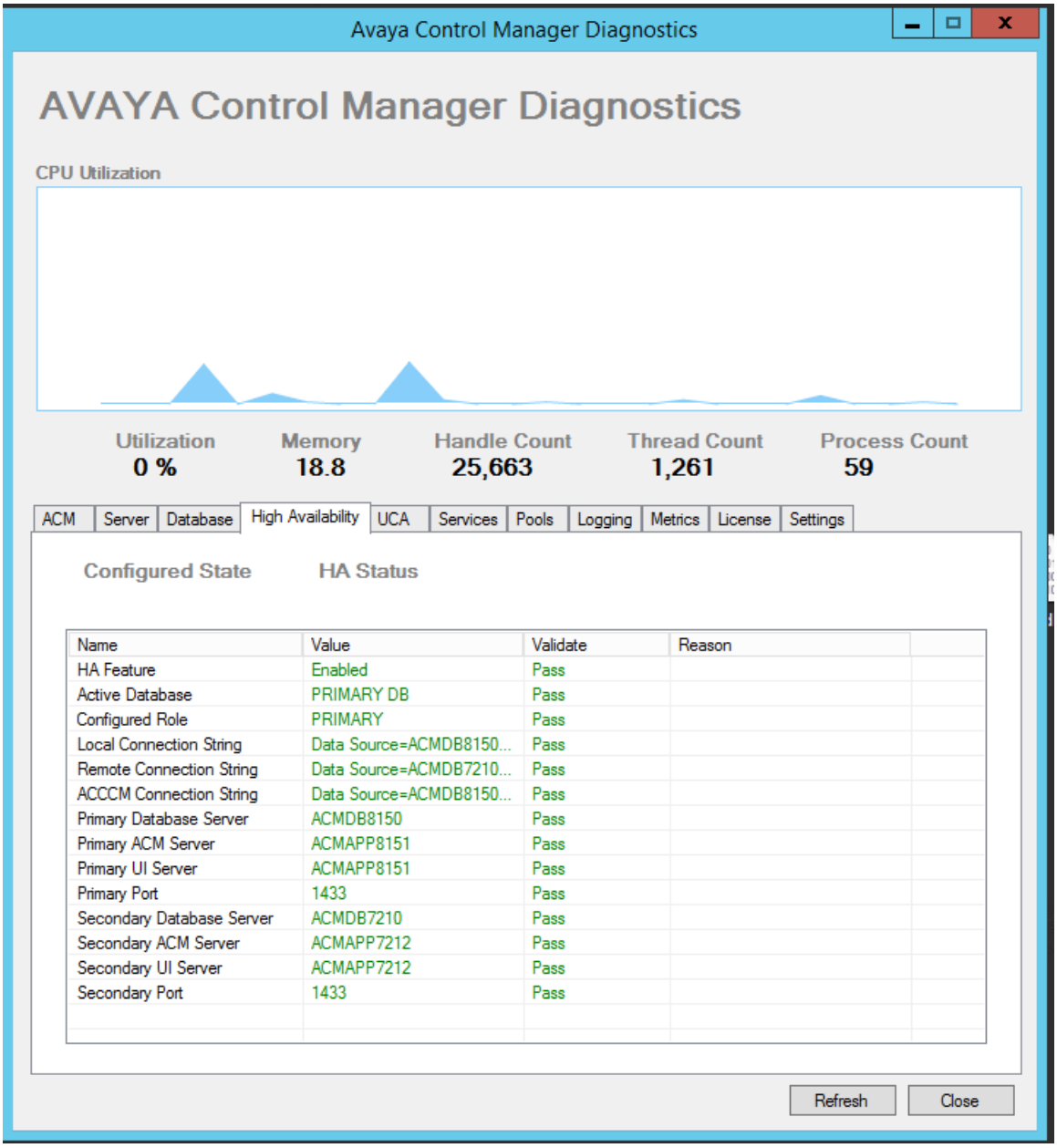
The **Database** tab shows information relating to the SQL Server database including the connection status to each Control Manager database.


Avaya Control Manager Diagnostics
AVAYA Control Manager Diagnostics
CPU Utilization
Utilization
1 %
Memory
77.4
Handle Count
66,940
Thread Count
2,040
Process Count
96
ACM
Server
Database
High Availability
UCA
Services
Pools
Logging
Metrics
License
Settings
WebLM
Configure SQL Server
SQL Server,Port *
Save
Test Connection
Machine Name
PUSNTYO149
SQL Version
SQL Server 2012 Enterprise Edition (64-bit) SP3
Name
Value
Validate
Reason
ACCCM Connection
Connected
Pass
AVP Connection
Connected
Pass
ONEX Connection
Connected
Pass
SPHERE Connection
Connected
Pass
SYNC Connection
Connected
Pass
Database Locale
us_english
Pass
ACCCM Size
60 MB
Pass
ACCCM Log Size
8 MB
Pass
AVP Size
5 MB
Pass
AVP Log Size
1 MB
Pass
SPHERE Szie
3 MB
Pass
SPHERE Log Szie
1 MB
Pass
ONEX Size
7 MB
Pass

Option	Description
SQL Server,Port	Use this option if you want to: • carry out a phased upgrade of the SQL server. • back up and replicate the database instances to different SQL servers. • change the SQL server for any reason. Enter the SQL server Hostname/IP-Address with the Port number separated by a comma (,) in this field. For instance, enter the alternate ACM SQL address in this field as `Hostname/IP-Address,Port number` and click **Save** to update the SQL server configuration in Control Manager. To verify the connection, click **Test Connection**. You must stop all ACM services before updating the SQL server connection details and then start the ACM to continue operating with Control Manager. The Control Manager system re-points to the new SQL server with SQL connection status including the host name, instance, port, and connection status.
Version	The SQL Server version.
Machine Name	The hostname of the SQL Server database server.
Clustered	Indicates whether the SQL Server is configured to run in a cluster.
ACCCM Connection	Indicates whether you have a valid connection to the ACCCM database.
AVP Connection	Indicates whether you have a valid connection to the AVP database.
ONEX Connection	Indicates whether you have a valid connection to the ONEX database.
SPHERE Connection	Indicates whether you have a valid connection to the SPHERE database.
SYNC Connection	Indicates whether you have a valid connection to the SYNC database.
Database Locale	The locale of the database software.
ACCCM Size	The size of the ACCCM database in MB.
ACCCM log Size	The size of the ACCCM log file in MB.
AVP Size	The size of the AVP database in MB.
AVP log Size	The size of the AVP log file in MB.
SPHERE Size	The size of the SPHERE database in MB.
SPHERE log Size	The size of the SPHERE log file in MB.
ONEX Size	The size of the ONEX database in MB.
ONEX log Size	The size of the ONEX log file in MB.
SYNC Size	The size of the SYNC database in MB.
SYNC log Size	The size of the SYNC log file in MB.

High Availability

The **High Availability** tab shows information related to the HA configuration.



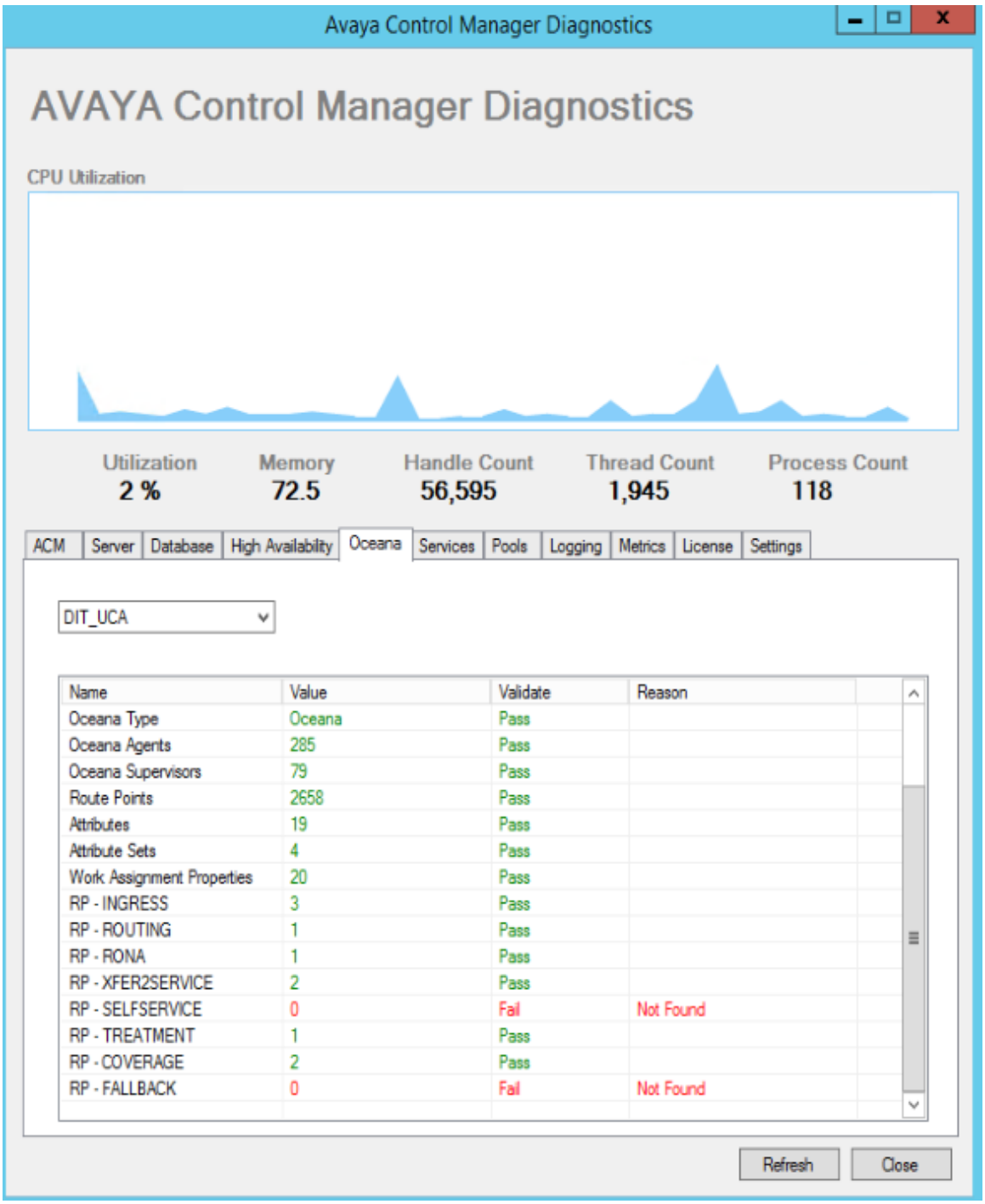
Option	Description
HA Feature	Indicates whether HA is enabled or disabled.
Active Database	Indicates which database is currently active.
Configured Role	Indicates if the original server role was Primary or Secondary.

Table continues…

Option	Description
Local Connection String	The connection string for the first database server that was configured when installing HA.
Remote Connection String	The connection string for the second database server that was configured when installing HA.
ACCCM Connection String	The connection string for the currently-connected database server.
Primary Database Server	The hostname of the primary database server.
Primary ACM Server	The hostname of the primary application server.
Primary UI Server	The hostname of the primary UI server.
Primary Port	The port number of the primary database server.
Secondary Database Server	The hostname of the secondary database server.
Secondary ACM Server	The hostname of the secondary application server.
Secondary UI Server	The hostname of the secondary UI server.
Secondary Port	The port number of the secondary database server.

Oceana

The **Oceana** tab shows information related to Avaya Oceana® features. Use the drop-down box to select the UCA server you want to diagnose.



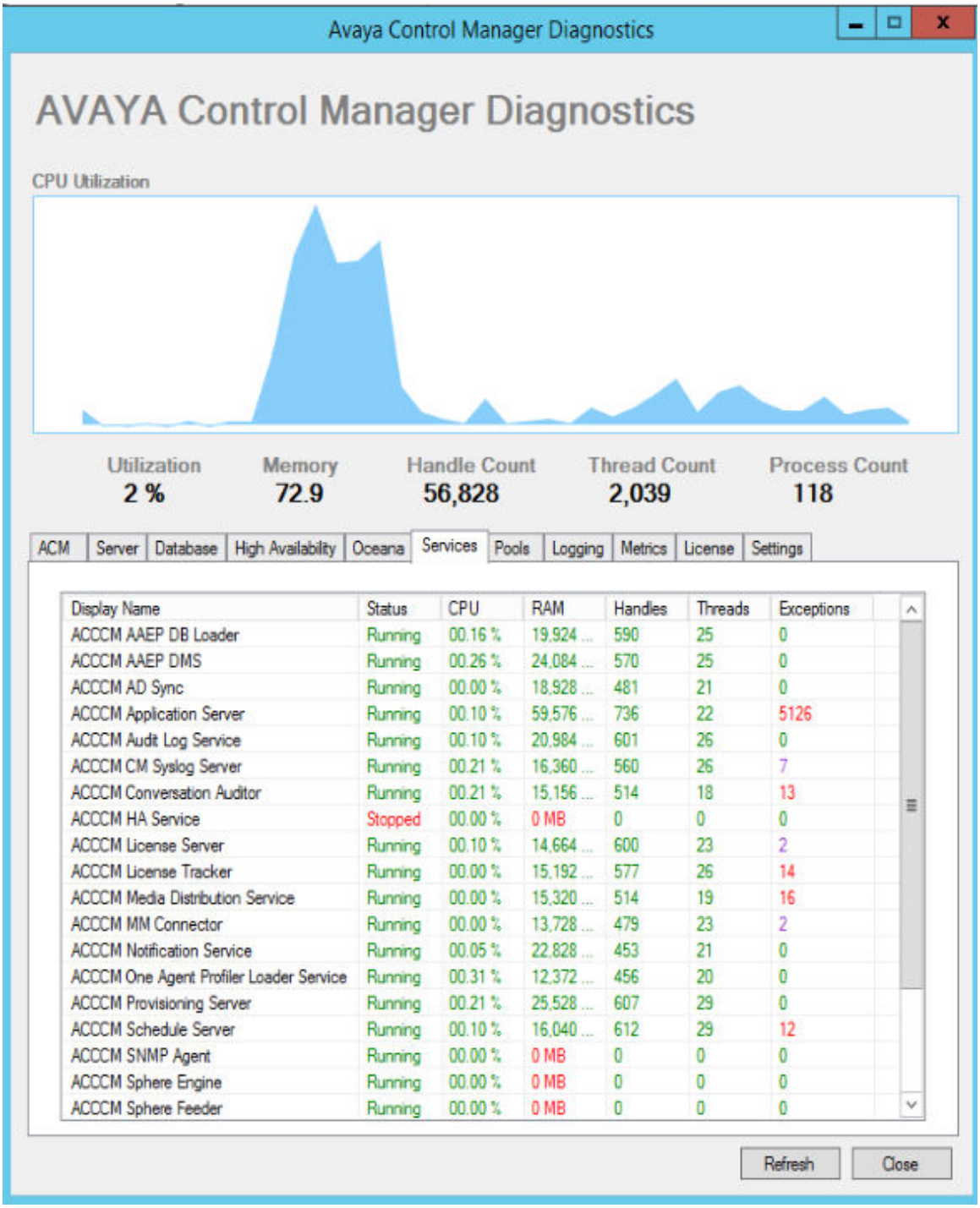
Option	Description
Oceana Service	Indicates whether the Avaya Oceana® server is currently running.
Oceana Name	The name of the Avaya Oceana® server connector.
Oceana URL	The URL of the Avaya Oceana® server.

Table continues…

Option	Description
Oceana Version	The version of the Avaya Oceana® software.
Oceana Type	The type of installation, Avaya Oceana® (Oceana) or Avaya Workspaces for Elite (Workspaces for Elite).
Oceana Agents	Number of administered Avaya Oceana® agents in UCA.
Oceana Supervisors	Number of administered Avaya Oceana® supervisors in UCA.
Route Points	Number of administered routing points in UCA.
Attributes	Number of administered attributes in UCA.
Attribute Sets	Number of administered attribute sets in UCA.
Works Assignment Properties	Number of administered Work Assignment properties in UCA.
RP-INGRESS	Number of administered ingress route points.
RP-ROUTING	Number of administered route points.
RP-RONA	Number of administered Redirection on No Answer (RONA) route points.
RP-XFER2SERVICE	Number of administered transfer to service route points.
RP-TREATMENT	Number of administered call treatment route points.
RP-COVERAGE	Number of administered Call Coverage route points.
RP-FALLBACK	Number of administered fallback route points.

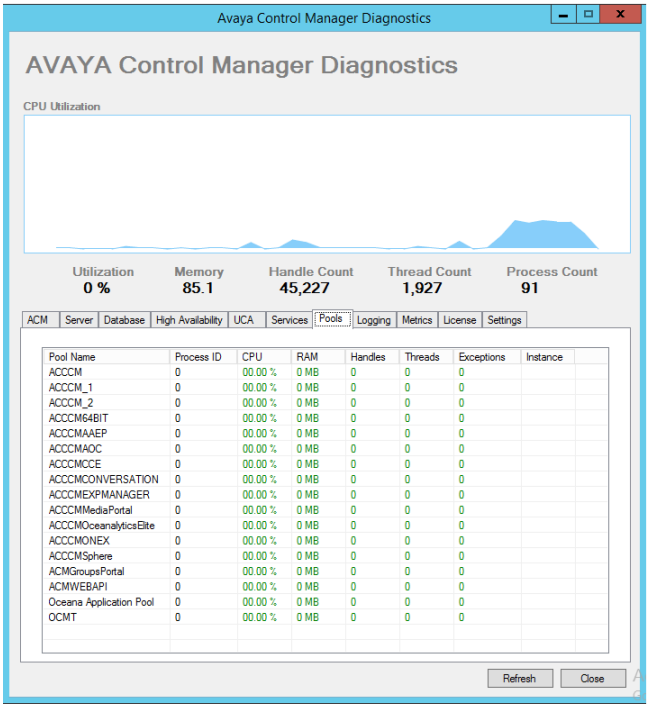
Services

The **Services** tab tracks status and resource information for each of the Control Manager services. Services that are not running or have metrics that exceed threshold limits are highlighted in orange and red. This tab is particularly useful for investigating memory leaks.



Pools

The **Pools** tab tracks status and resource information for each of the Control Manager Application Pools in IIS. Pools that have metrics that exceed threshold limits with be highlighted in orange and yellow. This tab is primarily used for investigating memory leaks.

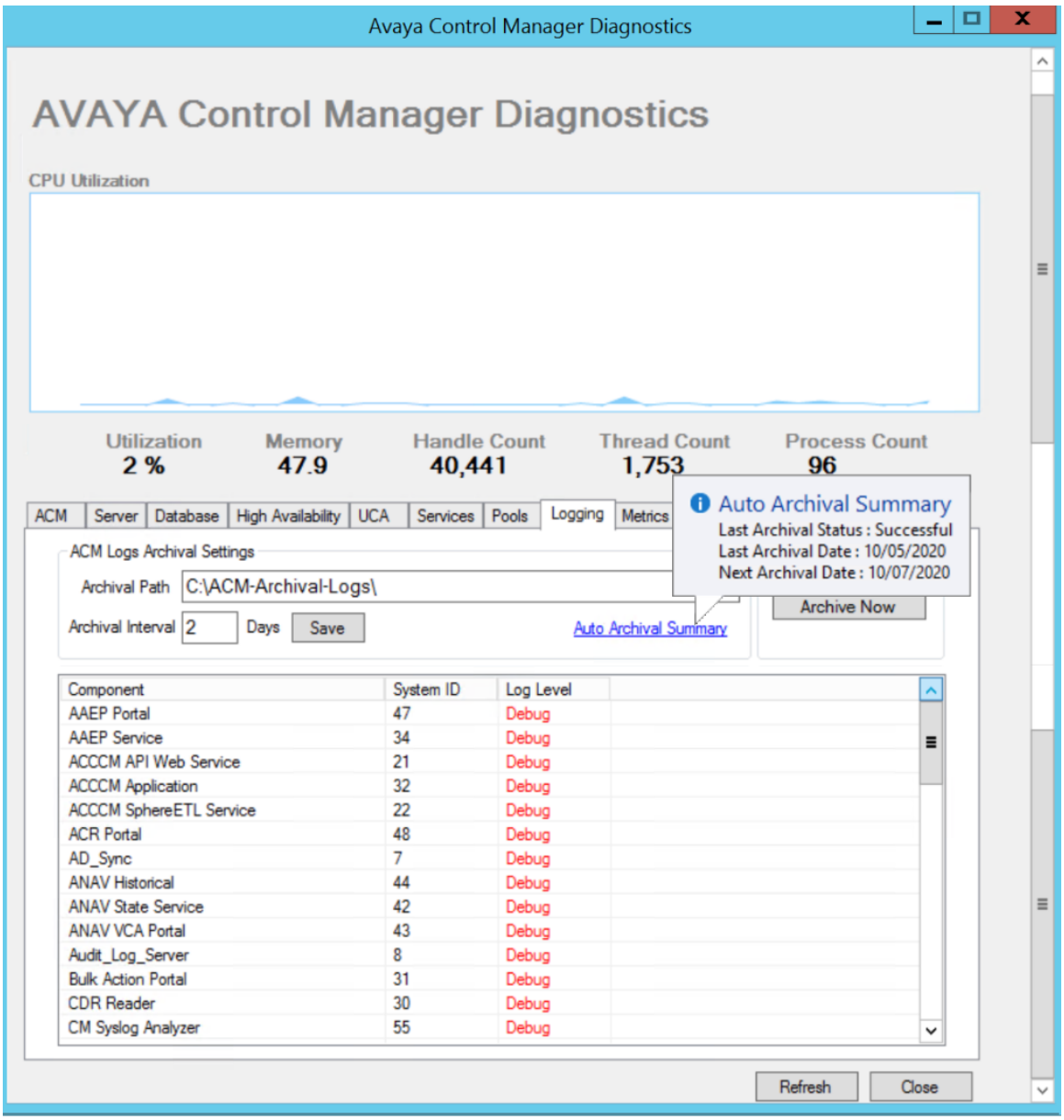


Logging

The **Logging** tab shows the current log level for each component in Control Manager. You can also change logs levels for specific components by right-clicking the component and selecting the desired log level. You can configure the ACM logs archival and retentions settings in the *ACM Logs Archival Settings* section.

ACM Logs Archival :

ACM Logs can be archived on the configured local or remote shared directory location. Archival can happen on configured periodic intervals and On-Demand as well.



Note:

- Enable port 1235 to save the logs archival settings and to perform Archive Now operation.
- The health monitoring service manages archiving of logs. Ensure that the Health Monitoring service is always running for logs archival functionality.

Table 1: ACM Logs Archival Settings

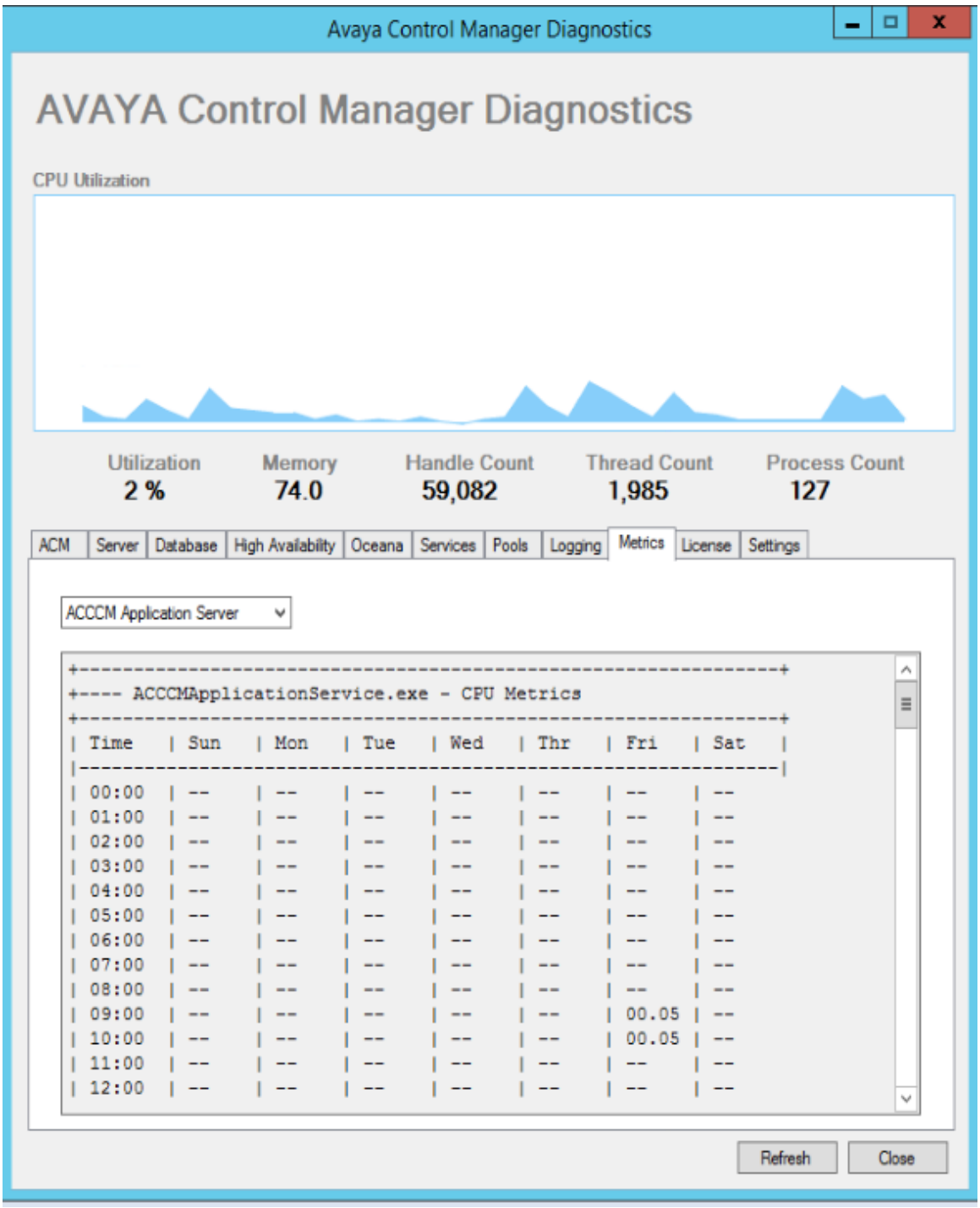
Option	Description
Archival Path	This is either a physical or network file system directory path to store Archived files. Physical Path: This is the absolute path of the ACM archival folder from local machine. For example: `c:\ACM-Archived-Logs\` Network Path: This is the network path to access the folder shared from a remote machine. For example: `\\<<Server-name>>\ACM-Archived-Logs` Ensure that you provide appropriate Write and Remove permissions to the User Account existing on ACM system while sharing the folder from the Remote machine. Change the Health Monitoring service logon account to ACM User Account with appropriate permissions on the remote network path. Complete the following steps to change the User account for Health Monitoring service: • Go to **Services**. • Right-click on **Health Monitoring service** and navigate to **Properties** > **Log on tab**. • Click **This account** and enter the Administration credentials. • Click **Save** and Restart the services. Following are the supported archival path format: • `c:\<<foldername>>\<<foldername>>` • `\\<<ServerName>>\C$\` • `\\<<IP_ADDRESS>>\C$\` • `\\<<ServerName>>\Shared\Test` • `\\<<IP_ADDRESS>>\Shared\Test`
Archival Interval	Archival of the logs happens automatically on a configured periodic interval. Periodic interval can be set in days. **Note:** • The auto logs archival are performed on the scheduled date at midnight between 00 AM to 01 AM. • Archival Path and Archival Interval are mandatory fields. If you want to stop the Archival of logs and remove the settings, clear both the fields and click **Save**.

Table continues…

Option	Description
Delete Archived Logs Older Than	The specified number of days after which all ACM logs, which are archived on the archival path for a longer time than the specified value, are deleted. For example, if you specify 10 days in this field, then the ACM logs that are older than 10 days are automatically deleted. By default, this field is empty. You can enter up to a maximum of 999 days.
Auto Archival Summary	Hover the mouse over this link to view the Last Archival Status, Last Archival Date, and scheduled Next Archival Date.
Archive Now	Click this button to Archive ACM log files whenever required. Archive Now operation does not have any impact on schedule of the periodic Archival. **Note:** By default, Archival Now button is disabled. Save the Archival Path field to enable the Archival Now button.
Archive Files	Archiving of ACM logs generates a compressed archive file with the following name format at the archival path: `ACM_Logs_<ArchiveDateTime>.` Extract the logs for ACM portals and services from the archive file.

Metrics

The **Metrics** tab shows the CPU, memory, handle, and thread metrics for all Control Manager services. Use the drop-down box to select the service you want to display.

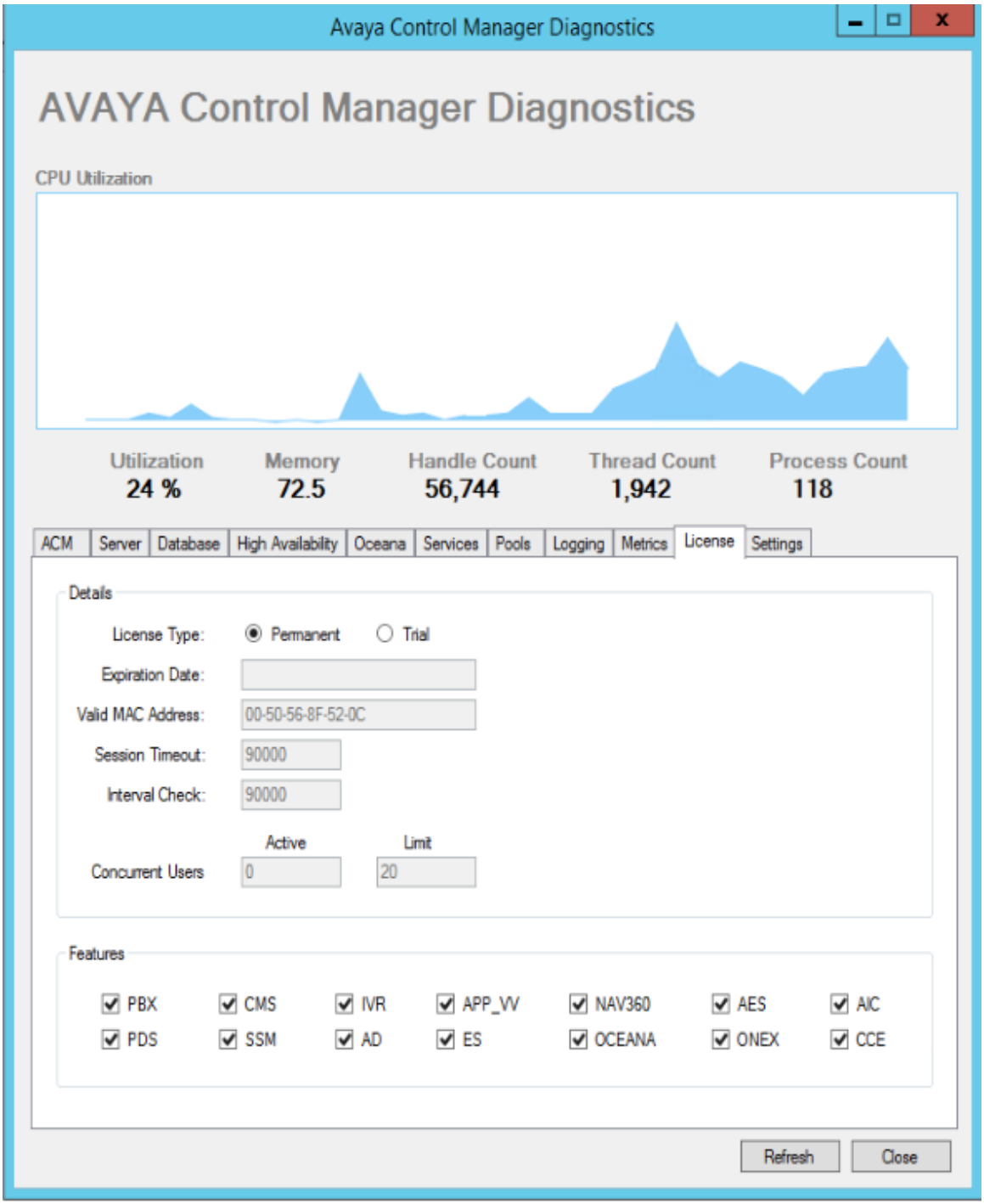


License

The **License** tab shows you the configuration of the license file located in the `Services\ACCCM License Server` folder. You can see the license type (permanent or trial) and what features have been enabled. The tab also shows how many concurrent users are logged in with respect to the overall limit.

Note:

The **Valid MAC Address** option is only populated if the MAC address found in the license file matches the MAC address of the local server.



Settings

The **Settings** tab allows you to customize the Health Monitor Status properties and generate reports.

Setting or Feature	Description
Service Setting	
Polling Interval	The interval at which the Health Monitor Status tool gathers application data, system data, and metrics.
Capture Metrics	Enable this feature to have the Health Monitor Status tool capture metrics for each Control Manager service. This feature is disabled by default so it does not impact performance during normal operation.
Automatically start ACM Services	When enabled, the Health Monitor Status tool automatically starts the other Control Manager services when the server starts up. For HA deployments, the Health Monitor Status tool also takes responsibility for starting Control Manager services that have been set to manual start-up mode based on the current HA configuration and status. For example, manual services are automatically started on the primary servers in a sunny day scenario, but not on the secondary servers. This is a very useful feature that removes the need for manual intervention by the user, particularly in the event of an unexpected reboot of which the user may not be aware.
Log Settings	
Delete logs older than	When enabled, this feature periodically purge obsolete log files in the Control Manager and Tomcat folders. The options are: • Never • Purge files older than 2 weeks • Purge files older than 1 month • Purge files older than 3 months • Purge files older than 6 months • Purge files older than 1 year
Clear Log Files	Click this button to purge all log files in the Control Manager and Tomcat folders.
Restore Defaults	Click this button to restore the default log level of WARN on all Control Manager components.
Control Manager Reports	
Generate	Click this button to generate the diagnostic and metric reports. The reports are saved to the `Services\ACCCM Health Monitoring \Metrics` folder.
Generate reports on Exit	When selected, the Health Monitor Status tool automatically generates diagnostic and metrics reports when you close the Health Monitoring tool.
Generate daily reports	When selected, the Health Monitor Status tool automatically generates daily diagnostic and metrics reports at midnight.
Oceana Reports	

Table continues…

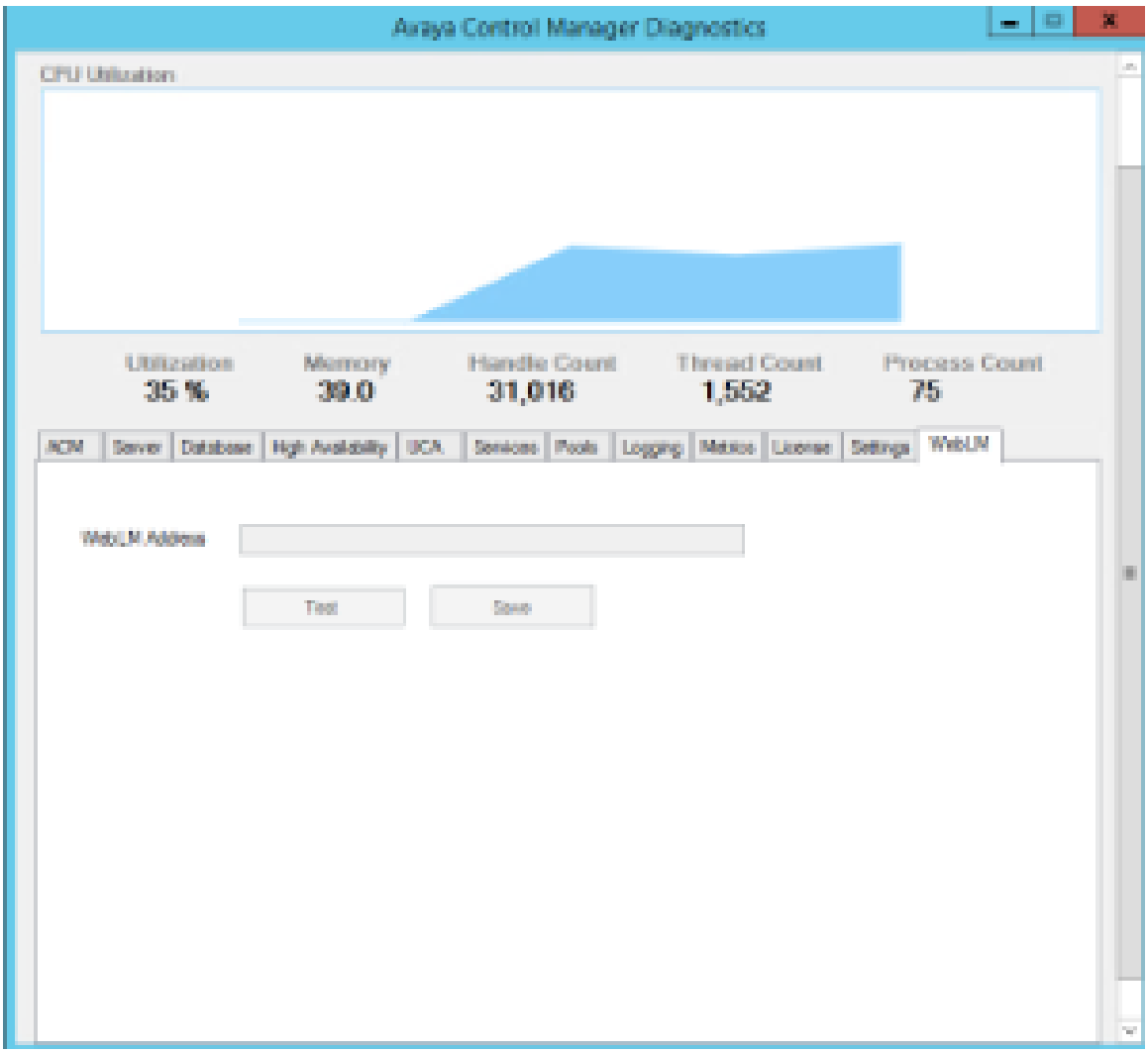
Setting or Feature	Description
Agent	Writes a list of all the Avaya Oceana® agents found in UCA to the `Services\ACCCM Health Monitoring\Oceana` folder.
Supervisor	Writes a list of all the Avaya Oceana® supervisors found in UCA to the `Services\ACCCM Health Monitoring\Oceana` folder.
Attribute	Writes a list of all the attributes found in UCA to the `Services\ACCCM Health Monitoring\Oceana` folder.
Provider	Writes a list of all the providers found in UCA to the `Services\ACCCM Health Monitoring\Oceana` folder.
Attribute Set	Writes a list of the Attribute Sets found in UCA to the `Services \ACCCM Health Monitoring\Oceana` folder.
Agent Detail	Generates an Agent Detail report for a specific agent based on the agent ID and saves it in the `Services\ACCCM Health Monitoring \Oceana` folder.
Supervisor	Generates a Supervisor Detail report for a specific agent based on the supervisor ID and saves it in the `Services\ACCCM Health Monitoring\Oceana` folder.
Attribute	Generates an Attribute Detail report for a specific agent based on the attribute ID and saves it in the `Services\ACCCM Health Monitoring\Oceana` folder.
Route Point	Writes a list of all the Avaya Oceana® route points found in UCA to the `Services\ACCCM Health Monitoring\Oceana` folder.
Administrator	Writes a list of all the Avaya Oceana® administrators found in UCA to the `Services\ACCCM Health Monitoring\Oceana` folder.

WebLM Server

The **WebLM Server** tab allows you to configure the WebLM server details.

Note:

After WebLM server configuration is done and saved, restart ACCCM License Server.



Options	Description
WebLM Address	Enter a valid URI of the WebLM server. For example, https://<WebLM_Server_IpAddress>:52233/WebLM/LicenseServer
Test	Click **Test** to verify the WebLM server address.
Save	Click **Save** WebLM server details.

Note:

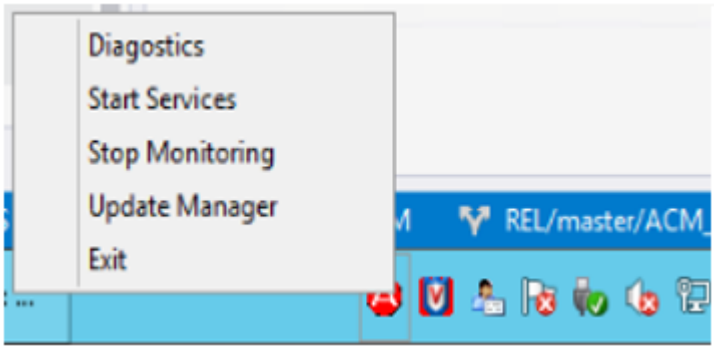
Control Manager administrator updates WebLM server details here only if Control Manager is in restricted mode and administrator can not login into Control Manager web portal.

Otherwise administrator can navigate to **Configuration portal** > **License** > **WebLM Server** and configure WebLM server details.

Health Monitor Status tool icon

About the Health Monitor Status tool icon

The Health Monitor Status tool icon is located in the Windows Task Tray. The icon uses colors to display an at-a-glance system status and is used to access features of the Health Monitor Status tool.



The features you can access include the following:

- Status — The icon changes colors and appearance to reflect the status of the system.
- Notifications — The icon displays pop-up notifications to alert you when significant events have occurred, for example, HA failover.
- Tooltips — The icon updates its tool tips to reflect the status, configuration, and release of the Control Manager system.

Icon status indicators

Indicator	Description
	Normal Operation — All of the Control Manager services are up and running in a normal scenario (sunny day).
	High Availability Mode – All services are up and running, but Control Manager is communicating with the secondary database server because the primary database server is not in operation (rainy day). The primary database server requires service.
	Partially Up — All of the critical Control Manager have started but one of more of the secondary services are down.
	Partially Up — Control Manager is communicating with the secondary database server because the primary database server is not in operation (rainy day). The primary database server requires service.
	No Connection — Unable to connect to the Health Monitoring service. To correct, confirm whether the Health Monitor service is running.
	System Down — A connection was established to the Health Monitoring service but one or more critical services are down.

Status Icon Menu

When you right-click on the Status Icon, you have access to the following commands:

Command	Description
Exit	Terminates the Status Icon application.
Start/Stop Monitoring	Toggles between starting and stopping the Health Monitor Status tool.
Start/Stop Services	Toggles between starting and stopping all Control Manager services. **Important:** For HA deployments, this command also starts or stops services that have been set to manual start-up mode. Using this command ensures that the correct services are started on both the primary and secondary servers without any need for further manual intervention.
Update Manager	Launches the patch Update Manager.
High Availability	Launches the High Availability Configuration utility.
Diagnostics	Launches the Health Monitor Status tool Diagnostic Monitor user interface.

About File Integrity

The Control Manager build install creates a file hash of the required important files, including the files that are responsible for the BAU operation of Control Manager. The system validates the file integrity for every transaction to ensure that only the file upholding its integrity is used and not just any random file or possibly corrupted file. This tool identifies the following discrepancies:

- Files that are tampered
- Files that are renamed
- Files that are added or delete

With the File Integrity Checking script to can generate a baseline file that contains the SHA512 checksum key of all Control Manager files with `.dll`, `.exe`, `.aspx`, `.cshtml`, and `.sh` extensions. While installing Control Manager, the system executes File Integrity Checker.ps1 script to capture SHA512 checksum under `Program Files (x86)\Avaya\Avaya Control Manager\Apps\File Integrity\Logs`.

Related links

Checking the File Integrity logs on page 77
Generating logs using the File Integrity Checking script on page 78

Checking the File Integrity logs

About this task

Use the following to check the File Integrity Checking logs:

Procedure

1. Go to **Program Files (x86)** > **Avaya** > **Avaya Control Manager** > **Apps** > **File Intergrity** and click the **Logs** folder.

   The system displays the log files:

   - **HashCheckOutputRecent**. The system creates this log file only while installing Control Manager and every subsequent recent run.
   - **HashCheckOutputPrevious**. The system creates this log file output when you run the installer for the second time and if the DLL has tampered.
   - **HashCheckOutput_<ACMVersion>_DDMMYYYYHHMMSS**. The system creates this log file output in the subsequent installation with the ACM version and a timestamp that is created after previous log files.
   - **ExceptionsCheck.txt**. The system creates this log output file either when you run the file manually or if any exception occurred during the run.

   Each time you generate logs using the File Integrity Checking script, Control Manager generates the `HashCheckOutputRecent.log` latest file and renames the earlier files as per date time stamp.

2. After the manual execution of the Power Shell script, the system displays the results with color codes. Text that appears in green represents no difference from the last installation. Text that appears in red represents the difference from the last installation.

Related links

About File Integrity on page 77

Generating logs using the File Integrity Checking script

About this task

Control Manager generates logs automatically at the time of installation or upgrade. You can manually use the File Integrity Checking script if any exception occurred during the installation.

Before you begin

You must have an appropriate tool to run the Power Shell script.

Procedure

1. Go to **Program Files (x86)** > **Avaya** > **Avaya Control Manager** > **Apps** > **File Intergrity** and click the **Logs** folder.
2. Run the script using the power shell tool to generate the logs and compare with the logs which captured in the Previous run.

Related links

About File Integrity on page 77

Chapter 6: General troubleshooting information

Control Manager services descriptions

Use this information to better understand for what purpose each of the Control Manager services are used. Note that the abbreviation ACCCM is an internal representation that means Control Manager.

Important:

Not all deployments use all of the services shown in this table.

Service Display Name	Service File Name	Description
ACCCM AAEP DB Loader	NAV360Proxy_DBLoader.exe	Loads the Control Manager Avaya Experience Portal (ACMAAEP) data from the database.
ACCCM AAEP DMS	NAV360Proxy_DataMemoryStorage.exe	Maintains data from the database loader that provides data to the Remote API.
ACCCM AD Sync	NAV360_ADSynchronizer.exe	Periodically synchronizes Active Directory (AD) users from supported Windows LDAP integrations. The AD users are mapped to Control Manager users and extensions.
ACCCM Application Server	ACCCMApplicationService.exe	A core Control Manager façade business logic service where requests and responses between all portals are processed and forwarded to the provisioning service, Control Manager database, Avaya Oceana® UCA server, authentication requests, and other services as required. The Application Server also serves as a bridge between the Control Manager services and the web interface.

Table continues…

Service Display Name	Service File Name	Description
ACCCM Audit Log Service	NAV360_AuditLogService.exe	Tracks changes between Control Manager and Communication Manager by polling those systems at regular intervals. The service gathers a subset of audit data from the Communication Manager history log (configuration change log) that was done directly on the Communication Manager system. The service provides an option to synchronize these changes to Control Manager based on the change log. The changes can be viewed on the Communication Manager portal screens.
ACCCM CM Syslog Server	ACM.CM.Syslog.Server.exe	Used as a listener to receive Syslog events from Communication Manager and store the events in the database. Events that are relevant to Communication Manager configuration changes, log on events, and log out events are stored in the Control Manager Syslog database. The service is used as a facade to all Syslog portal UI requests by querying this database.
ACCCM Conversation Auditor	ACCMCSFlowAuditionService.exe	Used by Conversation Sphere to audit conversations.
ACCCM HA Service	HA_Service.exe	Used to maintain Control Manager connections to the database and to maintain services status for HA deployments.
ACCCM Health Monitoring Server	HealthMonitoringServer.exe	Monitors system health for the items tracked by Control Manager.
ACCCM License Server	NAV360_LicenseService.exe	Loads Control Manager licenses and implements restrictions in the Control Manager system based on those licenses.
ACCCM License Tracker	NAV360_LicenseUsageTrackerService.exe	Connects configured systems to track and get license related information.
ACCCM Media Distribution Service	MediaPortalService.exe	Used to distribute media files for the Control Manager Media portal features.
ACCCM Notification Service	ServerHostService.exe	Sends notifications as configured in Control Manager.
ACCCM One Agent Profiler Loader Service	AvayaOneAgentProfilerLoaderService.exe	Loads Avaya one-X® Agent agent profiles.

Table continues…

Service Display Name	Service File Name	Description
ACCCM Provisioning Server	NAV360_ProvisioningService.exe	The service that provisions changes originating from Control Manager to all supported systems. Processes almost every non-UCA related save action, which saves objects in configured systems such as CMS and Communication Manager. Each Control Manager-supported object (users, extensions, and so on) has its own flow when saving to the different systems (Communication Manager, CMS, WFO, and so on) supported for these objects.
ACCCM Schedule Server	SchedulingServerHoster.exe	Used by the Delayed Save feature of the scheduler. Tracks and executes commands that are scheduled to run later.
ACCCM SNMP Agent	ACCCM SNMP Agent	SNMP Agent
ACCCM Sphere Engine	ACCCM Sphere Engine.exe	Used by Control Sphere for searching on data indexed in the Solr search platform.
ACCCM Sphere Feeder	ACCCM Sphere.exe	Used by Control Sphere for indexing entity data into the Solr search platform.
ACCCM Sync Service	NAV360_SyncService.exe	Periodically synchronizes objects from supported and configured systems, such as Communication Manager, so that the objects can be administered from the Control Manager user interface. This is done by listing all of the objects in the synced source and comparing those objects to what exists in Control Manager.
ACCCM UCA Proxy	ACCCMUCAProxyService.exe	Connects to UCA to fetch json data.
Apache Tomcat 8	Tomcat8	Control Manager Tomcat Instance that hosts the Solr application.

Usage Metering data not sent from Control Manager

Condition

The operations administrator sees the following message when trying to run Usage Metering reports:

```
Failed to generate daily usage summary
```

Cause

Usage Metering collects data daily at 3am local time. If the Control Manager system has been out of service all day, there may not be any data to collect.

Solution

The operations administrator must manually upload the raw usage data into the Usage Metering system. For more information, see Usage Metering documentation.

Excessive Sphere services database queries

Condition

You see hundreds or thousands of queries every minute into the Control Manager database because of the Sphere service

Cause

Sphere services are used when searching for specific entities, for example, a particular extension or VDN. The Sphere Feeder gets data from audit log service table. It reads the `<InstallLocation>\Services\ACCCM Sphere\ACCCM Sphere Feeder\config \auditLog.properties` file for the last audit log row that was indexed. The service then analyzes the data and indexes it to put into the sphere database. This query is run every time the service indexes the data.

You can edit the configuration file in the Sphere Feeder to run less often.

Solution

1. Log on to Windows as administrator on the primary application server (ACM-APP-1).
2. Open the following file for editing:

   `<InstallLocation>\Services\ACCCM Sphere\ACCCM Sphere Feeder\config \sphereFeederConfig.xml`
3. Change this value from the default of 60 seconds to a value in the range of 300 to 900 seconds (5 to 15 minutes) to increase the interval of the re-indexing process.
4. Save and close the file.
5. Go to **Start** > **Run**.
6. Enter `services.msc` and press **Enter**.
7. In the Services window, right-click **ACCCM Sphere Feeder** and select **Restart**.

   Important:

   You must restart the Sphere Feeder service before the new interval takes effect. Note that the interval starts when you restart the service. For example, if you set the interval for 900 seconds and restart the service at 9 PM, the sphere service re-index every 15 minutes starting at 9 PM. Consider how often you want to re-index and at what times of day you want the re-index to run when you select a new value.

   The system restarts the Sphere Feeder service.
8. Repeat this procedure on the secondary application server (ACM-APP-2), if using HA.

Failed to connect to the database server

Condition

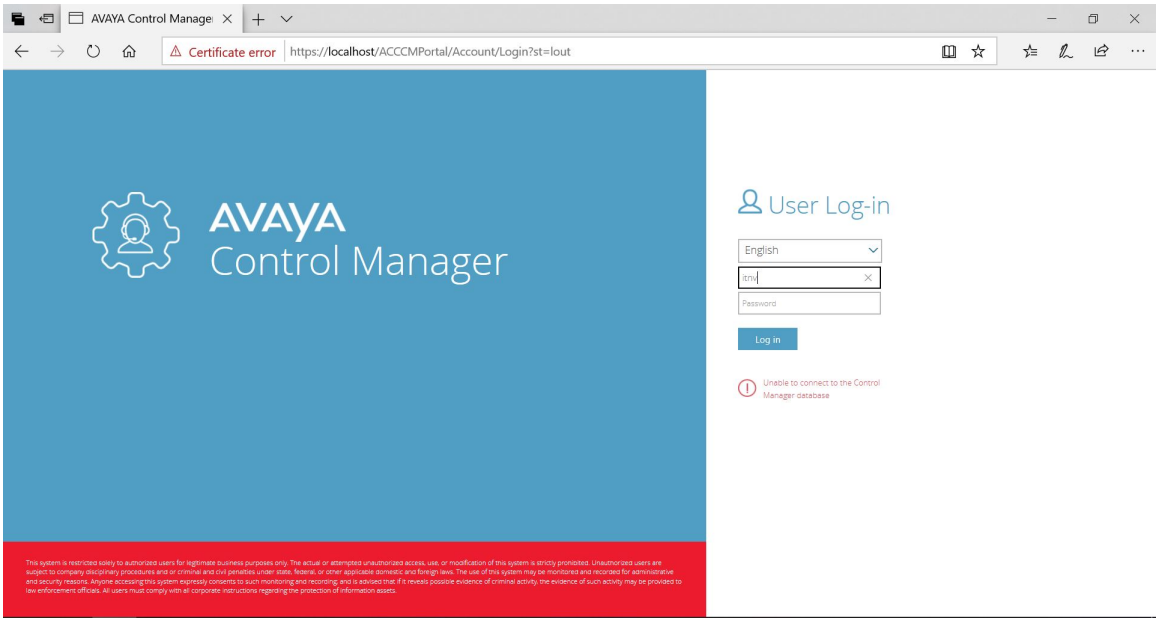
Failed to connect to the database server.

Control Manager displays the following error message when the SQL server is down:

Failed to connect to the database server.

Cause

You see this error message on the Control Manager web log-in screen when the Control Manager database server is offline.



Solution

Check the status of the database server.

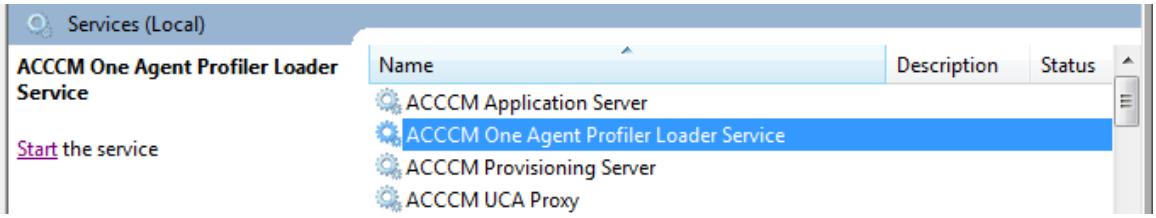
To check the status of the database server, in the Windows server, open **Health Monitor System** from the Windows **System Tray**. In **Health Monitor System**, go to the **Database** tab and check for the connection status. If the database is operational then, check for the connection between Control Manager and the database server. Ensure that the database server is active and accessible from Control Manager at any given time.

For more information about managing database, go to the *Database* section in this guide.

Problems when loading Avaya one-X® Agent profiles

Condition

The ACCCM One Agent Profile Loader service loads Avaya one-X® Agent profiles into the database. If any of the agent profiles fail while saving the profiles, the service is unable to process the next agent profile.



Cause

This condition occurs because the profile directory is not removed when there is a failure, causing the loading process to get stuck repeatedly on the failed profile when the service is executed at its next scheduled loading time.

With Control Manager Release 8.1, the system now creates a special failure folder to save information about those failing profiles. Doing this allows the profile loader to continue with its process, essentially skipping those failed profiles but saving the information in a special folder.

The failure folder that shows which profile failed can be found either under either `\Sites \Default Web Site\ACCCMONEXCFG\App_Data\Failure` or `\Avaya \NAV360_One_X_Manager\AvayaOneXCFG\App_Data\Failure`.

Solution

Review the profiles found in the failure folders to determine which options are not correct in the profiles.

Avaya one-X Agent password error

Condition

Unable to save the password

Solution

Avaya one-X Agent user's password must not contain a colon (:).

Successful bulk job with attributes assignment failed

Condition

The following are the possible conditions:

- An administrator sees the following error(s) on the Control Manager user interface.
- A Service Engineer sees the following error(s) in the Control Manager logs (especially logs of the UCA Proxy Service).

```
*org.openspaces.core.UpdateOperationTimeoutException: Timeout expired after waiting for
a transactional proper matching entry; nested exception is
com.j_spaces.core.client.OperationTimeoutException: Timeout expired after waiting for a
transactional proper matching entryorg.
```

```
openspaces.core.SpaceMemoryShortageException: Memory shortage at: host: x.x.x.x,
container: ucaStoreSpace_container1_1, space caStoreSpace, total memory: 247 mb, used
memory: 236 mb; nested exception is Memory shortage at: host: x.x.x.x, container:
ucaStoreSpace_container1_1, space ucaStoreSpace, total memory: 247 mb, used memory: 236
mb*
```

Cause

Due to issues in the UCA server (Oceana). The possible reason is shortage of resources assigned for the UCA server.

Solution

Contact the Oceana administrator.

Announcement media file does not play on Control Manager

Condition

- Control Manager displays the following error message while playing announcement:

  Failed to play announcement media file.

- ACCCM Media Server displays the following log:

  "Could not create SSL/TLS secure channel.

Cause

This error occurs if there are discrepancies in the configuration of the certificate, which is used for two-way authentication with Avaya Aura® Media Server.

Solution

1. Check the debug logs of the SOAP service on Avaya Aura® Media Server and download the logs from Element Manager of AMS. After downloading the logs, navigate to the following path for more detailed logs:

   `\log\soapserverDebug.txt`

2. If you have certificate discrepancies on the Control Manager Server, enable the **CAPI2** log in Event Viewer by completing the following procedure:
   a. Open Microsoft Windows Event Viewer.
   b. Navigate to **Applications and Services Logs** > **Microsoft** > **Windows** > **CAPI2** > **Operational**.
   c. Right-click **Operational** and click **Enable Log**.

Announcement does not play the media file when clicking on the Play button

Condition

While trying to play an announcement, the media file does not get played despite configuring the prerequisites correctly.

Cause

The media file URI has the FQDN of the Control Manager server as the host address. If the FQDN host address does not match with the common name specified in the certificate of the Control Manager server, then the audio control cannot gain access to the URL, resulting in not playing the audio file.

Solution

Check the common name (CN) of the Control Manager server in the certificate configured for the IIS HTTPS binding. If any discrepancy, correct the certificate to set CN to FQDN.

Troubleshooting Control Sphere

Sphere link cannot redirect to proper page

Cause

The URL of sphere search is not updated completely.

Solution

1. Log on to Windows as administrator on the primary application server (ACM-APP-1).
2. Navigate to **Start** > **Run**.
3. Enter `cmd.exe` and press **Enter**.
4. Navigate to `C:\Program Files (x86)\Avaya\Avaya Control Manager \Services\ACCCM Sphere\ACCCM SphereEngine\sphereConfig`.

5. Open `sphereSearchServerConfig.xml` for editing.
6. Change this URL:

```
<launcherUrl>
<![CDATAhttps://<ControlManagerServerName>/acccm/App_Communicators/
tag_server_launcher.aspx]>
</launcherUrl>
```

   to this URL:

```
<launcherUrl>
<![CDATAhttps://<ControlManagerFQDN>/acccm/App_Communicators/
tag_server_launcher.aspx]>
</launcherUrl> ]></launcherUrl>)
```

   For example, change:

```
<launcherUrl>
<![CDATAhttps://ACM8140/acccm/App_Communicators/tag_server_launcher.aspx]>
</launcherUrl>
```

   to:

```
<launcherUrl>
<![CDATAhttps://ACM8140.hcm.com/acccm/App_Communicators/tag_server_launcher.aspx]>
</launcherUrl>
```

7. Save and close the file.
8. Navigate to **Start** > **Run**.
9. Enter `services.msc` and press **Enter**.
10. Right-click **ACCCM Sphere Engine** and click **Restart**.
11. Log on to the Control Manager user interface.
12. In the **Search** box, search for user.
13. Click on the user's link after it is displayed.

    The user's detail page is displayed.

Sphere search engine is not connected to the Tomcat

Solution

1. Ensure that the Tomcat server is up and running.
2. Click on the tomcat configuration manager in your environment
3. Ensure Tomcat is running

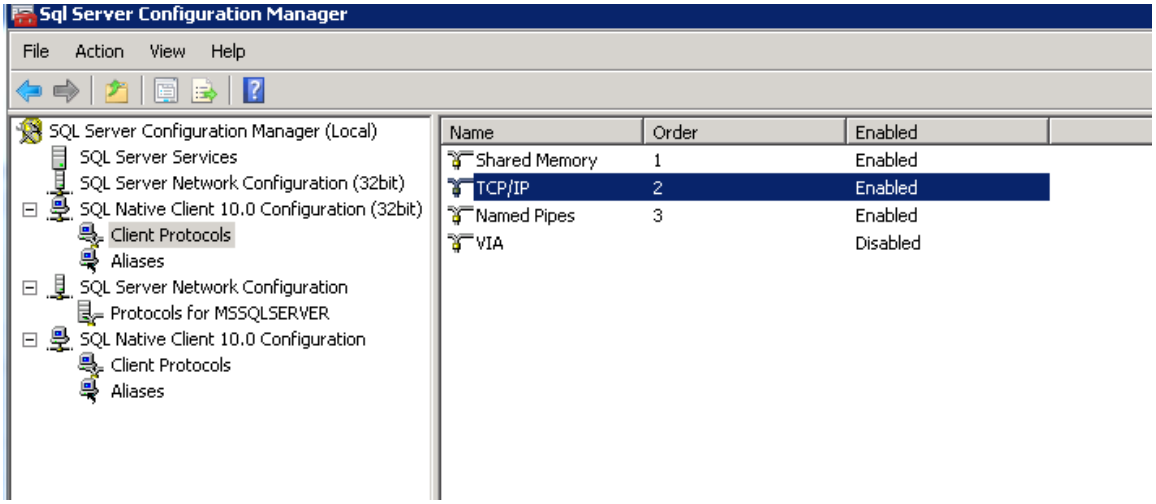
Sphere feeder is not able to connect to the database

Cause

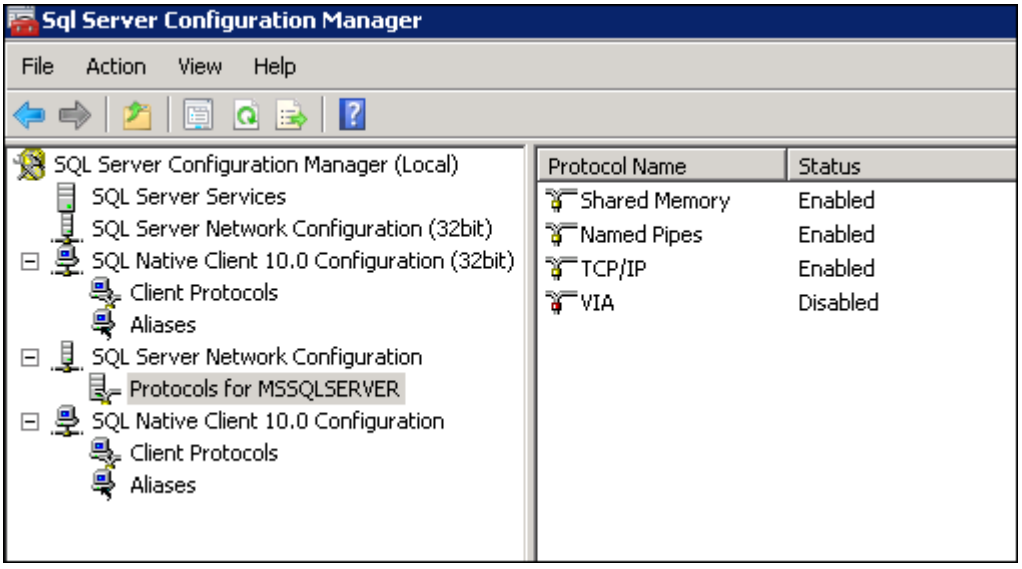
If there is a database connection error in the log file of the feeder, ensure the TCPIP connection is open on your SQL server.

Solution

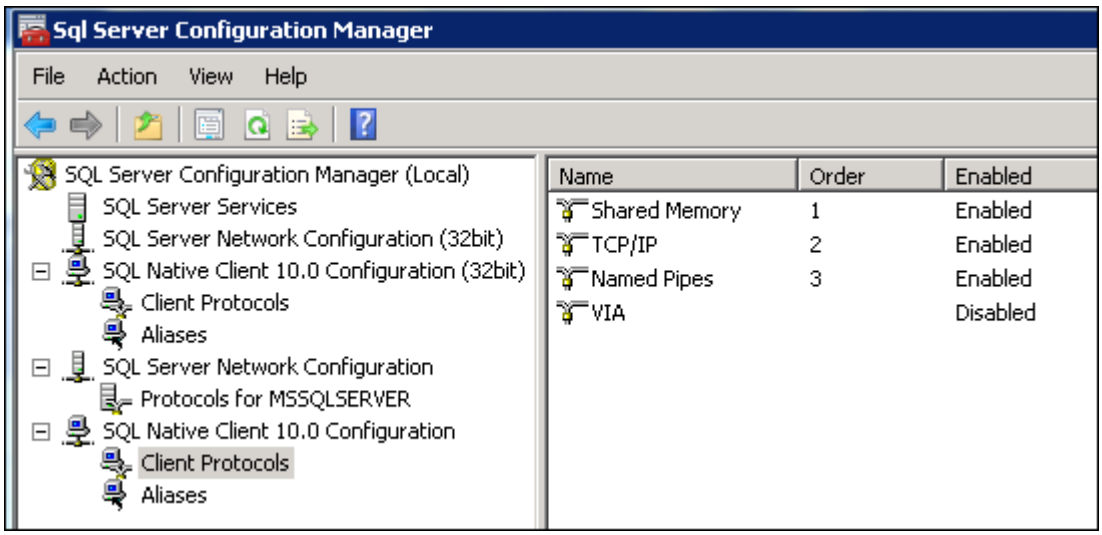
1. Open SQL Configuration Manager.
2. In the SQL Server tree, ensure that TCP/IP is enabled in each of the following sections:
   - **SQL Native Client 10.0 Configuration (32bit)** > **Client Protocols**



   - **SQL Server Network Configuration** > **Protocols for MSSQLSERVER**



   - **SQL Native Client 10.0 Configuration** > **Client Protocols**



3. If TCP/IP is not activated, than activate it, and restart the SQL Server.

Chapter 7: Troubleshooting installation problems

Failure installing one of the prerequisites

Condition

One of the prerequisites that you select to install fails during the Control Manager installation and the system displays an error message.

Solution

1. Stop the installation.

   The installation wizard rolls back automatically.

2. Install the prerequisite by running the software separately.

   The system extracts all the installation files to the disk when you start the installation wizard. The files are extracted to the following path, shown in two ways:

   `C:\Users\`*`InstallUserID`*`\AppData\Roaming\Avaya\Avaya Control Manager\install`

   `%APPDATA%\Avaya\Avaya\Avaya Control Manager\install`

   You can access these files only when the install wizard has initiated the installation process. To access the prerequisite, you must start the wizard, copy the prerequisite file from the location data, and then close the wizard.

3. Run the Control Manager installation wizard again.

Control Manager services are not starting

Condition

Control Manager services are not starting.

Solution

If one of the following services does not start:

- Provisioning service
- Sync service

Verify that the Control Manager License Server is running.

Solution

If the Notification service does not start, the installation of Control Manager software might not have been done on a fresh installation of the Microsoft Windows server software. Confirm that the installation of Microsoft Windows server software was a fresh installation immediately prior to the installation of Control Manager software. If you cannot confirm a fresh installation of the Microsoft Windows server software, uninstall the Control Manager and Microsoft Windows server software and reinstall the software.

Note:

On an upgraded system, you must not reinstall the Microsoft Windows or Control Manager software.

Esent database error during installation

Condition

During installation of the Control Manager software, you get an SQL database error as shown in the following example:

```
InstallSchema - databaseName: ACCCM, dacpacName: C:\Program Files (x86)\Avaya\Avaya
Control Manager\Database\ACCCM.dacpac
InstallSchema() - Exception Error !!
 . . .
 . . .
SaveInstallParameters() - DatabaseHost: 127.0.0.1, DatabasePort: 1433, DatabaseUser:
sa, DatabaseName: ACCCM
SaveInstallParameters() - EXCEPTION
SaveInstallParameters() - MSG: Cannot open database "ACCCM" requested by the login. The
login failed.
Login failed for user 'sa'.
 . . .
 . . .
InstallDatabases() - ACCCM Installed FAILED
CustomAction ACMDBLibWix.CA.dllInstallDatabases returned actual error code 1603 (note
this may not be 100% accurate if translation happened inside sandbox)
Action ended 19:23:01: ACMDBLibWix.CA.dllInstallDatabases. Return value 3.
Action ended 19:23:01: INSTALL. Return value 3.
Property(S): RADIOBUTTONGROUP_1_PROP = STANDARD
Property(S): RADIOBUTTONGROUP_1_PROP_2 = Custom
Property(S): AppsShutdownOption = All
```

Cause

This error is related to the Windows native database engine (Esent) and its interaction with the Microsoft SQL software startup options.

Solution

1. Using VMware snapshot tools, return your application servers and database servers to their original configuration before you installed the Control Manager software.
2. Log on as administrator to the primary database server (ACM-SQL-1).
3. Open the Microsoft SQL Server Manager.

4. Run the following command to stop and start the database server:

   net start MSSQLSERVER /x /T661 /T834

5. Repeat this procedure on the secondary database server (ACM-SQL-2).
6. Reinstall the Control Manager software.
7. Verify that you do not get the same Esent error.

Firewall issues

Condition

Communication is blocked between the different servers usually between the database servers and the application servers.

Cause

The correct Windows firewall ports are not open.

Solution

1. Log on to Windows on the servers where communication is failing.
2. Go to **Start** > **Run**.
3. Enter `WF.msc` and press **Enter**.
4. In the Windows Firewall with Advanced Security screen, in the left pane, right-click **Inbound Rules**, and then click **New Rule** in the action pane.
5. In the Rule Type dialog box, select **Port**, and then click **Next**.
6. In the Protocol and Ports dialog box, select **TCP**. Select **Specific local ports**, and then enter the port number of the database instance, such as 1433 for the default instance.
7. Click **Next**.
8. In the Action dialog box, select **Allow the connection**, and then click **Next**.
9. In the Profile dialog box, select any profiles that describe the computer connection environment when you want to connect to the Database Engine, and then click **Next**.
10. In the Name dialog box, enter a name and description for this rule, and then click **Finish**.

The default language is not applied when you launch Control Manager for the first time

Condition

The default language which user selected while installing Control Manager is not displayed when launching Control Manager for the first time.

Cause

The default language is not displayed if the browser does not have Control Manager cookies.

Solution

1. Open your browser, for example chrome.
2. Open browser settings.
3. Navigate to **Languages** tab.
4. Click **More Actions** on the language, like the language you have chosen while installing Control Manager.
5. **Select Move** to the top.
6. Close Settings.
7. Reload Control Manager web page.

Unable to log in to the Control Manager user interface

Authentication failed

Condition

When trying to log in to the Control Manager Web portal, you get an error message stating that the authentication failed.

Solution

1. Log on as administrator to the application server or UI server.
2. Navigate to `c:\windows\system32` folder and locate the `NAV360CONFIG.XML` file.
3. Open the file in a text editor.

   A file similar to the following is displayed:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<configuration>
<connectionString>Data Source=ACMDBSERVER;Initial Catalog=ACMDBNAME;User
ID=ACMdbuser;Password=ACMdbpassword</connectionString>
</configuration>
```

4. Ensure that the connection string details match the database settings as shown in the following table:

   Important:

   The database setting must be the same that you entered during the installation process.

String	Description
ACMDBSERVER	The database server that hosts the Avaya Control Manager database. If you are using a database with an instance, the server name must include ”/”. For example, myServer/SQLexpress.
ACMDBNAME	The name of the Avaya Control Manager database.
ACMdbuser	The database user that Avaya Control Manager uses to access the Avaya Control Manager database.
ACMdbpassword	The user password. After the first successful log-in, the system encrypts the password.

5. You can create an ODBC on the Avaya Control Manager server and check if the connection string details are correct. If the connection details are wrong, you can edit the details and save the file.

No more licenses

Condition

When trying to log in to the Avaya Control Manager Web portal, you get a message stating that there are no more licenses.

Solution

1. Got o **Start** > **Run**.
2. In the run box, enter **`services.msc`** and press **Enter**.
3. In the **Services** window, check whether the **ACCCM License Server** License Server is running.
4. If it is not running, right-click **ACCCM License Server** and click **Start**.
5. If the Avaya Control Manager License Server service does not start, navigate to the License Server folder on the Avaya Control Manager server and check the log files of the service.

   The default path of the log folder for the License Server is: *`InstallDrive`*`:\Program Files (x86)\Avaya\Avaya Control Manager\Services\ACCCM License Server\Logs`

   The log file must show the following:

```
06/04/2011 16:09:14 |DEBUG |NAV360_LicenseService.ConfigReader.Init |Got Config
file
06/04/2011 16:09:14 |DEBUG |NAV360_LicenseService.LicenseService..ctor |
Initialized ConfigReader
06/04/2011 16:09:14 |DEBUG |LicenseDBManager.DBManager..ctor |Connection string
was set
06/04/2011 16:09:14 |DEBUG |
LicenseDBManager.InfoProvider.GetAllLicenseServicesAddresses |Got 1 License
Services addresses
06/04/2011 16:09:14 |DEBUG |NAV360_LicenseService.LicenseService.OnStart |The
service starts listening on port 35353
06/04/2011 16:09:14 |DEBUG |NAV360_LicenseService.LicenseService.OnStart |about
```

```
to initialize LicensingService singleton instance
06/04/2011 16:09:15 |DEBUG |NAV360_LicenseService.LicenseService.OnStart |
Initialized LicensingService singleton instance
06/04/2011 16:09:15 |DEBUG |NAV360_LicenseService.LicenseService.OnStart |
Starting to listen
```

If you get a different log structure and error messages, contact Avaya Support.

6. Ensure that the `License.lic` file is in the root directory of the License Server folder.

   If the log file shows that the service is up and running, there is a problem with the license file. In such case, contact Avaya Support for help.

Unable to connect to other Avaya products

Condition

The system services, such as synchronizer or provisioning are not able to establish a connection to other Avaya products.

Solution

Ensure that you have configured the following parameters correctly:

- User name
- Password

  When components are upgraded, the upgrade procedures often require a change of passwords. Ensure that passwords are updated after an upgrade.
- PIN code, if required
- Connection port

  For example, the Communication Manager port is configured under the system parameter page. The default Communication Manager port is 5023.

Synchronizer issues

The Synchronizer application does not show any locations

Condition

When launching the Synchronizer application, the location list is empty.

Solution

Assign at least one Avaya Aura® Communication Manager system to the location and restart the Synchronizer application. See the following example of errors in the log file:

```
06/04/2011 16:09:14 |DEBUG |NAV360_LicenseService.ConfigReader.Init |Got Config file
06/04/2011 16:09:14 |DEBUG |NAV360_LicenseService.LicenseService..ctor |Initialized
ConfigReader
06/04/2011 16:09:14 |DEBUG |LicenseDBManager.DBManager..ctor |Connection string was set
06/04/2011 16:09:14 |DEBUG |
LicenseDBManager.InfoProvider.GetAllLicenseServicesAddresses |Got 1 License Services
addresses
06/04/2011 16:09:14 |DEBUG |NAV360_LicenseService.LicenseService.OnStart |The service
will start listening on port 35353
06/04/2011 16:09:14 |DEBUG |NAV360_LicenseService.LicenseService.OnStart |about to
initialize LicensingService singleton instance
06/04/2011 16:09:15 |DEBUG |NAV360_LicenseService.LicenseService.OnStart |Initialized
LicensingService singleton instance
06/04/2011 16:09:15 |DEBUG |NAV360_LicenseService.LicenseService.OnStart |Starting to
listen
```

Synchronization from Communication Manager is not starting

Condition

Synchronization from Communication Manager does not start. Synchronizer shows 0% progress.

Cause

This is a configuration issue. If the Control Manager Default Sync Team option is not enabled, the synchronizer does not start and you cannot see any progress.

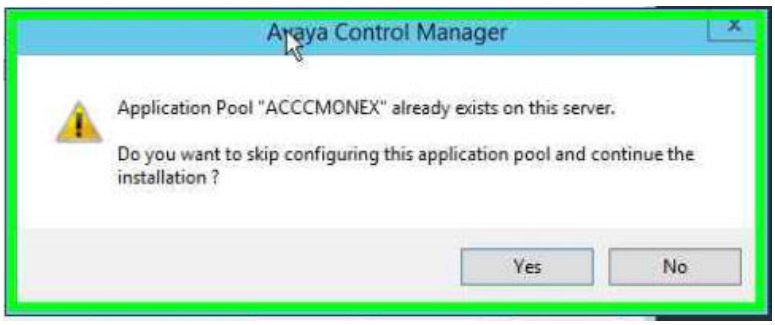
Solution

1. After installing Control Manager, you must perform the following configurations:
   - Add a location
   - Add the organization tree
   - Add a site
   - Add a department
   - Add a team
2. When adding a team, verify that the Default Sync Team option is selected.

Application pool error messages

Condition

When upgrading the Control Manager software, the system displays one or more error messages similar to the following:



Click **Yes** to any application pool messages you get and continue with the upgrade. Use the following procedure to change the configuration of the skipped application pools.

Solution

1. After the upgrade is finished, log on to the Windows operating system.
2. On the server desktop, open IIS Manager.
3. Navigate to **Sites** > **Default Web Site**.

   The system displays the installed Control Manager Web applications. The Web applications all start with the name “ACM” or “ACCCM”.
4. Confirm that each Control Manager Web application has the correct physical path by clicking the **Basic Settings** option of each Web application.
5. If the physical path for each Web application does not contain the installation directory selected during the installation, you must change the physical path.
6. After verifying or correcting the Web application physical paths, restart the Default Web Site or reboot the server

Cannot view WebLM licenses in License Tracker

Condition

When using License Tracker, you cannot see any of the WebLM licenses.

Cause

This may be caused when the system environment variables cannot find the Java executable file.

Use the following procedure to test and see if you need to update the system environment variables with the path to the Java executable file.

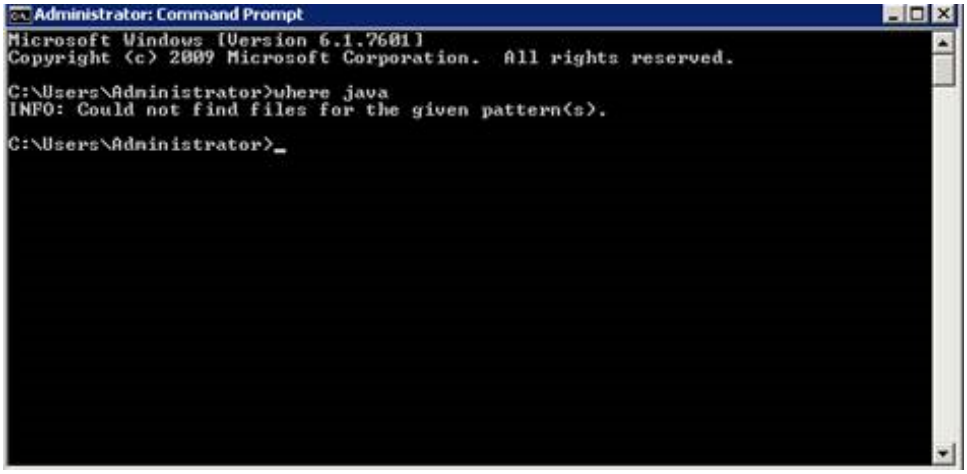
Solution

1. Log on to the Windows system as Administrator.
2. Open a command prompt window.
3. Enter the following command:

   ```
   where java
   ```

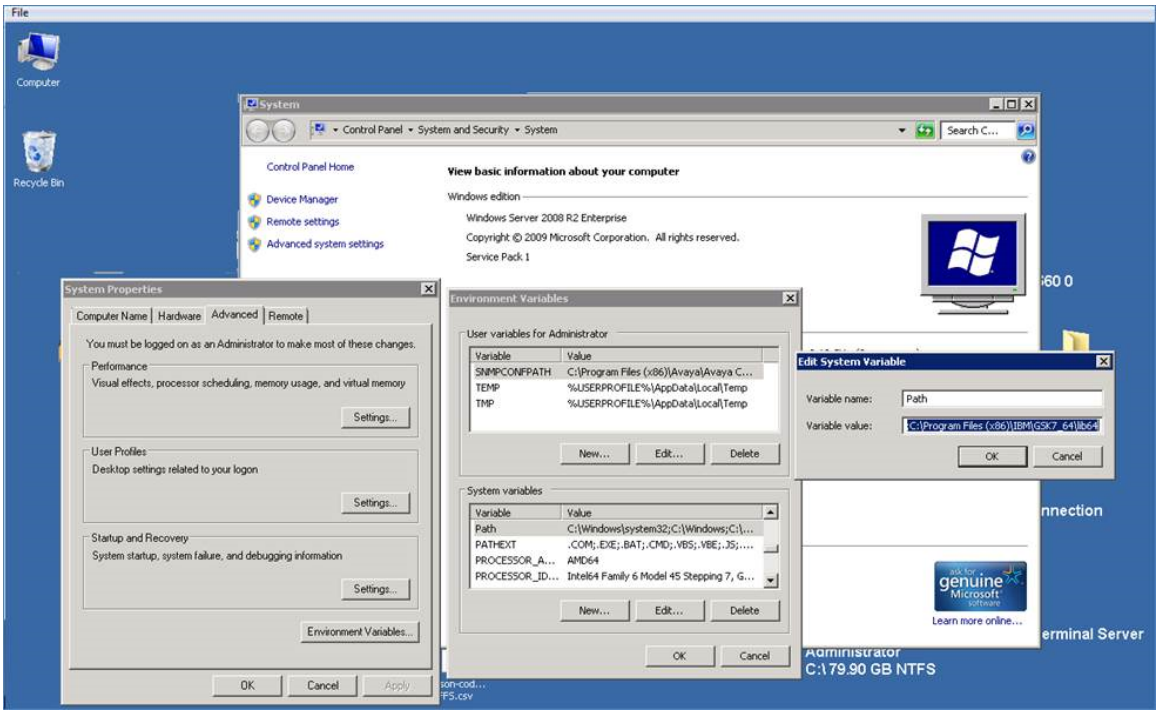
One of the following occurs:

- If the system displays the proper path to the Java executable, this procedure does not fix the condition. Contact Avaya Support for assistance.
- If the system displays a “not found” message as shown below, continue with this procedure.



4. In Windows, navigate to **Advanced System Settings** > **Environment Variables**.
5. In the **System variables** section, locate the variable with **PATH** in its name and highlight it.
6. Select **Edit**.

   See the following example of the screens used to administer the environment variable.



7. Add the path for the Java executable to the **PATH** variable.

Note:

The Java path is usually found at:

DRIVE:\Program Files\Zulu\zulu-8\bin\java.exe

8. Click **OK** three times to save the change to the environment variable.
9. Restart the server.
10. Test that you can now see WebLM licenses using License Tracker.

Chapter 8: Troubleshooting performance problems

Users experience lengthy delays accessing Communication Manager administration objects

Condition

Control Manager users experience excessive delays waiting for administrative pages to load for Communication Manager objects. For example, if users see long delays when displaying pages, you can improve performance by adjusting the Activelink Idle Connection Timeout value on Control Manager and the simultaneous login limit value on Communication Manager.

Cause

The user account administered on Communication Manager that is associated withControl Manager must be a dedicated user, and this causes considerable overhead. This condition required the addition of an Activelink Idle Connection Timeout parameter in certain configuration files to help reduce the delays.

Important:

This condition might also be related to the user account administered on Communication Manager for the association with Control Manager. The user account must be a dedicated user and must not be used for any other purpose than to associate Communication Manager with Control Manager. For more information, see “Creating a Communication Manager user for Control Manager” in *Configuring Avaya Control Manager*.

Solution

Increasing the Communication Manager simultaneous login limit

If you increase the Activelink Idle Connection Timeout value to a value between 1,000 and 600,000, you must also increase the simultaneous login limit value in Communication Manager. For more information about login limit administration, see *Avaya Aura® Communication Manager Feature Description and Implementation*.

1. Log on to the Communication Manager System Management interface.
2. Navigate to **Administration** > **Server (Maintenance)**.
3. Click **Security** > **Login Account Policy**.
4. In the **Login Limits** section, set the **Maximum Number of Simultaneous logins for a user** parameter to 12 for a non-HA configuration and to 20 for an HA configuration.

5. Click **Submit**.

Configuring the Control Manager Activelink Idle Connection Timeout

The ActiveLink Idle Connection Timeout is a Control Manager parameter used to control the time window for which a communication link between Control Manager and a Communication Manager system can be kept open. This parameter defines the timeout for disconnecting idle ActiveLink connections from Communication Manager.

The default timeout is 1 millisecond, with a maximum value of 600,000 ms (10 minutes). By adjusting the timeout value, you can improve performance when accessing Communication Manager web pages. If you do configure a timeout value higher than 1,000, you must also increase the Communication Manager simultaneous login limit value as shown later in this procedure.

You must configure the Activelink Idle Connection Timeout value in all of the following configuration files:

Component	File
Provisioning server	*InstallPath*\Services\ACCCM Prov Srv \NAV360_ProvisioningService.exe.config
Application server	*InstallPath*\Services\ACCCM Application \ACCCMApplicationService.exe.config
Nav360 synchronizer service	*InstallPath*\Services\ACCCM Synchronizer \NAV360_SyncService.exe.config
Nav360 synchronizer	*InstallPath*\Services\ACCCM Synchronizer \NAV360_Synchronizer.exe.config
Audit Log server	*InstallPath*\Services\ACCCM Audit Log Server \NAV360_AuditLogService.exe.config
Conversation Sphere flow auditing service	*InstallPath*\Services\ACCCM CS Flow Auditing Service \ACCMCSFlowAuditionService.exe.config
License tracker	*InstallPath*\Services\ACCCM License Tracker \NAV360_LicenseUsageTrackerService.exe.config
Schedule server	*InstallPath*\Services\ACCCM Schedule Server \ScheduleServerHoster.exe.config
Sphere indexer	*InstallPath*\Services\ACCCM Sphere\ACCCM Sphere Indexer \ACM_SphereImporter.exe.config
Users portal	*InstallPath*\Web\ACCCM WEB\web.config
Conversation Sphere	*InstallPath*\Web\ACCCM Conversation\ACCCMConversationSphere \web.config
Avaya Oceana® bulk administration	*InstallPath*\Apps\AvayaOceanaBulkAdministration \AvayaOceanaBulkAdministration.exe.config

6. Open the first configuration file listed in the table above.
7. In the <appSettings> section of the file, add a new line for the Activelink Idle Connection Timeout. The line must use the following format:

   ```
   <add key="cm_aict_CommunicationManagerIPAddress"
   value="TimeoutValueInMilliseconds"/>
   ```

Where *CommunicationManagerIPAddress* is the IP address of the Communication Manager system and *TimeoutValueInMilliseconds* is the timeout value in milliseconds. The default timeout setting is 1 millisecond. You can increase the value to as much as 600,000 milliseconds (10 minutes). After editing the configuration file, it must look like the following example:

```
<?xml version="1.0"?>
<configuration>
  <appSettings>
        <add key="cm_aict_162.30.234.10" value="1000"/>
  </appSettings>
</configuration>
```

8. Save and close the file.
9. Repeat this procedure for all of the configuration files. Ensure that you use the same Activelink Idle Connection Timeout value in every configuration file.
10. Restart all of the Control Manager services associated with the configuration files you edited and reset the IIS server.

Unable to access station status from Communication Manager objects

Condition

INVALID TERMINAL TYPE

Cause

This error is occurs when you attempt to gain access to Control Manager from where the server is installed.

Solution

In the `web.config` file, add an interval between two commands. Use the following steps to fix the issue.

1. Navigate to the following directory on the system `C:\Program Files (x86)\Avaya \Avaya Control Manager\Web\ACM UC Portal\web.config`.
2. Open the `web.config` file.

   The file displays the web.config file.
3. In the `<appSettings>` section, add a new line for the Communication Manager command time-out.

   The line must use the following format

   ```
   <add key="CMCommandTimeoutInterval" value="[timeoutintervalinmilisecound]" />
   ```

The file looks as the following:

```
<?xml version="1.0" encoding="utf-8"?>
    <configuration>
        <appSettings>
<add key="CMCommandTimeoutInterval" value="1000" />
    </appSettings>
</configuration>
```

4. Go to the `<appSettings>` section and change the default time out setting in milliseconds. For example, change the value to `2000`.

   The default time out setting is 1000 milliseconds. The maximum value is 3000 milliseconds (3 seconds).

5. Save and close the `web.config` file.
6. Restart the IIS server.

Unable to change Reason Codes from two-digit to single-digit

Condition

Unable to change Reason Codes from two-digit to single-digit.

Cause

Avaya one-X® Agent supports only a two-digit Reason code for ACCCM one-X Agent integration.

Solution

To change the system to support a single-digit Reason Code, you must change the following configuration files:

- `web.config` in the ACCCM ONEX CFG folder.
- `AvayaOneAgentProfilerLoaderService.exe.config`

1. To change the settings in the `web.config` file, do the following:
   a. Navigate to **Avaya** > **Avaya Control Manager** > **Web** > **ACCCM ONEX CFG** folder.
   b. Open the `web.config` file.

      The file displays the code lines.

   c. In the `web.config` file, look up for the following lines:

      ```
      <add key="2digitauxliary" value="true"/>
      <add key="2digitlogout" value="true"/>
      <add key="2digitwork" value="true"/>
      ```

   d. Set the value to false.
   e. Save and close the `web.config` file.

2. To change the settings in the `AvayaOneAgentProfilerLoaderService.exe.config` file, do the following:
   a. Navigate to the **Avaya** > **Avaya Control Manager** > **Services** > **ACCCM OneAgentProfilerLoaderService** and look for the `AvayaOneAgentProfilerLoaderService.exe.config` file.
   b. Open the `AvayaOneAgentProfilerLoaderService.exe.config` file.

      The file displays the code lines.
   c. In the `AvayaOneAgentProfilerLoaderService.exe.config` file, look up for the following lines:

      ```
      <add key="2digitauxliary" value="true"/>
      <add key="2digitlogout" value="true"/>
      <add key="2digitwork" value="true"/>
      ```
   d. Set the value to false.
   e. Save and close the `AvayaOneAgentProfilerLoaderService.exe.config` file.
3. Restart the services.

Requested feature is not supported in configured Oceana version: Messaging

Condition

If user sees the message as "Feature not supported on current oceana version".

Cause

The particular feature is not supported on Oceana version.

Solution

Change the settings to the correct Oceana Version.

Chapter 9: Troubleshooting failover problems

Failover procedure for Multiplex HA application server configurations

About this task

The load balancer in a Multiplex HA configuration evenly distributes all administrator login requests automatically across both Control Manager application servers (ACM-APP-1 and ACM-APP-2). If one of the application servers goes down, subsequent login requests are automatically redirected to the operating application server. For those users connected to the failed application server, they must log on again to the Control Manager user interface.

When the application servers are installed, one application server is designated as the primary application server (ACM-APP-1) and the other application server is designated as the secondary application server (ACM-APP-2). Initially, the following services, called the “independent services”, run only on the primary application server (ACM-APP-1):

- Audit Log
- AD Sync
- Sync Service
- License Tracker
- Schedule Server

If the primary application server (ACM-APP-1) fails, subsequent login requests are automatically redirected to the secondary application server (ACM-APP-2). Those users that were connected to the primary application server (ACM-APP-1) that failed are redirected to the secondary application server (ACM-APP-2). Users must log on again to the Control Manager user interface. In this case, the system switches these independent services on the secondary application server to the Running state. When the primary application server is operational again, the system pauses these independent services on the primary application servers.

If the secondary application server (ACM-APP-2) goes down, subsequent login requests are automatically redirected to the primary application server (ACM-APP-1). Those users that were connected to the secondary application server (ACM-APP-2) that failed are redirected to the primary application server (ACM-APP-1). Users must log on again to the Control Manager user interface. Since the independent services noted above are still running on the primary application server (ACM-APP-1), the system administrator only needs to repair the secondary application server (ACM-APP-2) to get it operational again. At that time, log on requests are distributed across both application servers.

Procedure

Primary Application Server (ACM-APP-1) Failure

1. Log on to Windows as administrator on the operational secondary application server (ACM-APP-2).
2. Go to **Start** > **Run**.
3. Enter `services.msc` and press **Enter**.
4. After 10 mins, the following independent services are changed to running state automatically:
   - Audit Log
   - AD Sync
   - Sync Service
   - License Tracker
   - Schedule Server
5. Repair and restart the failed primary application server (ACM-APP-1), and wait until all ACM services on ACM-APP-1 are in running state except independent services.
6. Log on to Windows as administrator on the secondary application server (ACM-APP-2).
7. Go to **Start** > **Run**.
8. Enter `services.msc` and press **Enter**.
9. Right-click the following independent services and select **Stop**:
   - Audit Log
   - AD Sync
   - Sync Service
   - License Tracker
   - Schedule Server
10. Log on to Windows as administrator on the repaired primary application server (ACM-APP-1).
11. Go to **Start** > **Run**.
12. Enter `services.msc` and press **Enter**.
13. After 10 mins, the following independent services are changed to running state automatically:
    - Audit Log
    - AD Sync
    - Sync Service
    - License Tracker

- Schedule Server

Secondary Application Server (ACM-APP-2) Failure

14. Repair and restart the failed secondary application server (ACM-APP-2).
15. Log on to Windows as administrator on the secondary application server (ACM-APP-2).
16. Go to **Start** > **Run**.
17. Enter `services.msc` and press **Enter**.
18. Right-click the following independent services and confirm that the services are in pause state:
    - Audit Log
    - AD Sync
    - Sync Service
    - License Tracker
    - Schedule Server

About failover

This section describes how failover is handled when failures occur with Control Manager components.

Note:

Recovery procedures for the different server types are described in *Server recovery procedures*.

HA failover

Failover for application servers

When the Control Manager software is installed on the primary and secondary application servers (ACM-APP-1 and ACM-APP-2), the HA Service is automatically installed. The HA Service provides an active/active communication path between the primary and secondary application servers (ACM-APP-1 and ACM-APP-2). When the heartbeat fails to receive updates from the designated primary application server (ACM-APP-1), the HA Service concludes that the system is not operational or at least no longer healthy enough to provide service. This event triggers an automatic failover from the primary application server (ACM-APP-1) to the secondary application

server (ACM-APP-2). Since both the Control Manager primary and secondary application servers are identical in functionality and configuration, the failover is seamless.

The primary application server (ACM-APP-1) runs its primary database connection path against the primary database server (ACM-SQL-1). The secondary application server (ACM-APP-2) also runs its primary database connection path against the primary database server (ACM-SQL-1).

In addition, the Control Manager HA service running on the individual servers monitors the active database connection from the primary application server (ACM-APP-1) to the primary database server (ACM-SQL-1), as well as the connection from the secondary application server (ACM-APP-2) to the primary database server (ACM-SQL-1). The HA service takes the appropriate failover action when the database connection is lost.

For example, if a failover occurs in the primary database server (ACM-SQL-1) in a Control Manager Active/Active HA deployment, the Control Manager HA service automatically does the following:

- Updates the Control Manager connection strings on both the primary and secondary application servers (ACM-APP-1 and ACM-APP-2).
- Stops the License Tracker, Audit Log, AD Sync, CM Syslog Server, Schedule Server, Sphere Feeder, and Sync Service services on the primary application server (ACM-APP-1).
- Starts the License Tracker, Audit Log, AD Sync, CM Syslog Server, Schedule Server, Sphere Feeder, and Sync Service services on the secondary application server (ACM-APP-2).

The following table shows the configuration files that contain the database connection strings that are required to successfully implement the Control Manager HA deployment. Editing of these files are described throughout this document.

Connection Strings (location)	Primary Application Server (ACM-APP-1)	Secondary Application Server (ACM-APP-2)
NAV360 Database (`NAV360Config.xml`)	ACM-SQL-1 (DB1)	ACM-SQL-1 (DB1)
HA Primary Database (`configuration.xml`)	ACM-SQL-1 (DB1)	ACM-SQL-2 (DB2)
HA Secondary Database (`configuration.xml`)	ACM-SQL-2 (DB2)	ACM-SQL-2 (DB2)
HA Avaya one-X® Agent Web Primary Database (`configuration.xml`)	ACM-SQL-1 (DB1)	ACM-SQL-1 (DB1)
HA Avaya one-X® Agent Web Secondary Database (`configuration.xml`)	ACM-SQL-2 (DB2)	ACM-SQL-2 (DB2)
HA Avaya one-X® Agent CFG Primary Database (`configuration.xml`)	ACM-SQL-1 (DB1)	ACM-SQL-1 (DB1)
HA Avaya one-X® Agent CFG Secondary Database (`configuration.xml`)	ACM-SQL-2 (DB2)	ACM-SQL-2 (DB2)
HA Avaya one-X® Agent Profile Loader Primary Database (`configuration.xml`)	ACM-SQL-1 (DB1)	ACM-SQL-1 (DB1)
HA Avaya one-X® Agent Profile Loader Secondary Database (`configuration.xml`)	ACM-SQL-2 (DB2)	ACM-SQL-2 (DB2)

Server status during normal operation

For an Enterprise configuration during normal operation, the Control Manager reference architecture requires that the deployment adhere to the following operational and start-up standards on the application servers.

Application servers

Control Manager Service	ACM-APP-1		ACM-APP-2	
	Status	Startup	Status	Startup
HA Service	Running	Manual	Running	Manual
ACCCM Sync Service	Running	Manual	Stopped	Manual
ACCCM CM Syslog Server	Running	Manual	Stopped	Manual
ACCCM Sphere Feeder	Running	Manual	Stopped	Manual
ACCCM AD Sync	Running	Manual	Stopped	Manual
ACCCM Audit Log Service	Running	Manual	Stopped	Manual
ACCCM License Tracker	Running	Manual	Stopped	Manual
ACCCM Schedule Server	Running	Manual	Stopped	Manual

Summary of how service is impacted when server failover occurs

The following tables summarize how failures impact service for each of the failover scenarios given in this section.

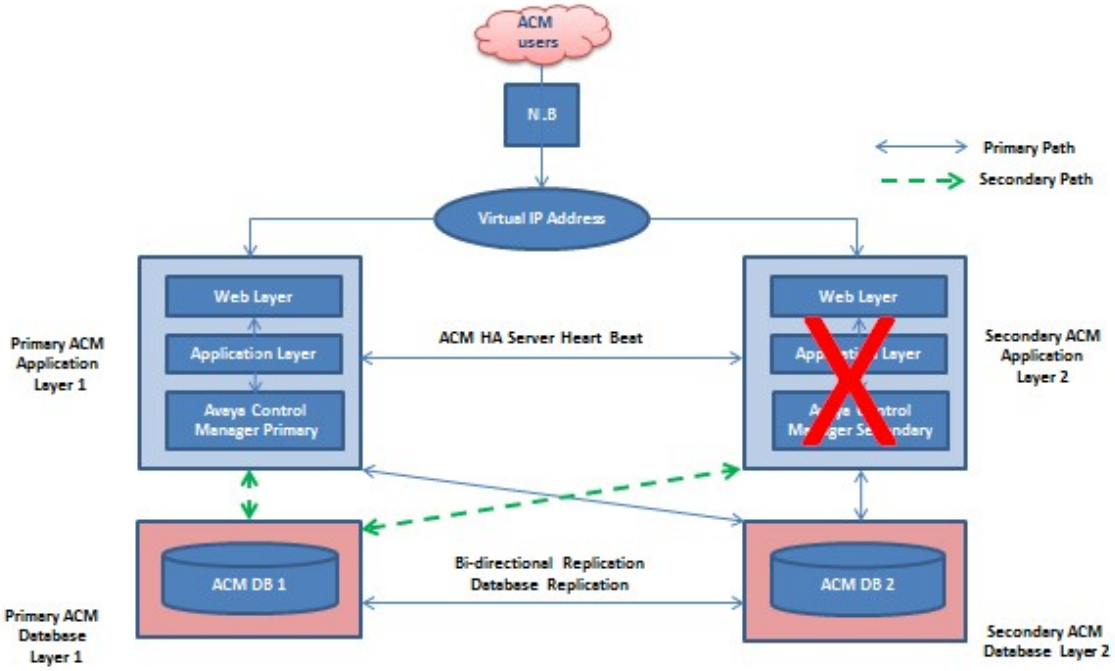
Service Impact	Description
Low	No operational impact, full operational experience is available through an alternative route.
Medium	A smaller operational impact is experienced as some functionality is not fully available or the operator has to extract required information through a different path which is different to normal operational experience.
High	A severe operational impact is experienced and operational elements are not available with no alternative approach in place.

Failure Condition	Service Impact	Description
Loss of primary application server (ACM-APP-1)	Medium	Operations are performed by the secondary application server (ACM-APP-2). Log file analysis must be performed through Log files.
Loss of secondary application server (ACM-APP-2)	Low	Full operational experience using the primary application server (ACM-APP-1).
Loss of both application servers (ACM-APP-1 and ACM-APP-2)	High	Operations cannot be performed on any servers when both are down. Catastrophic failure.
Lose of primary database server (ACM-SQL-1)	Medium	Full operational experience using the secondary database server (ACM-SQL-2). When bidirectional replication is being used, Create, Update, and Delete operations are replicated to the primary database server (ACM-SQL-1) upon recovery.

Server failover scenarios

Failover when the secondary application server fails

The following diagram shows what happens when the secondary application server (ACM-APP-2) fails for an Enterprise configuration:



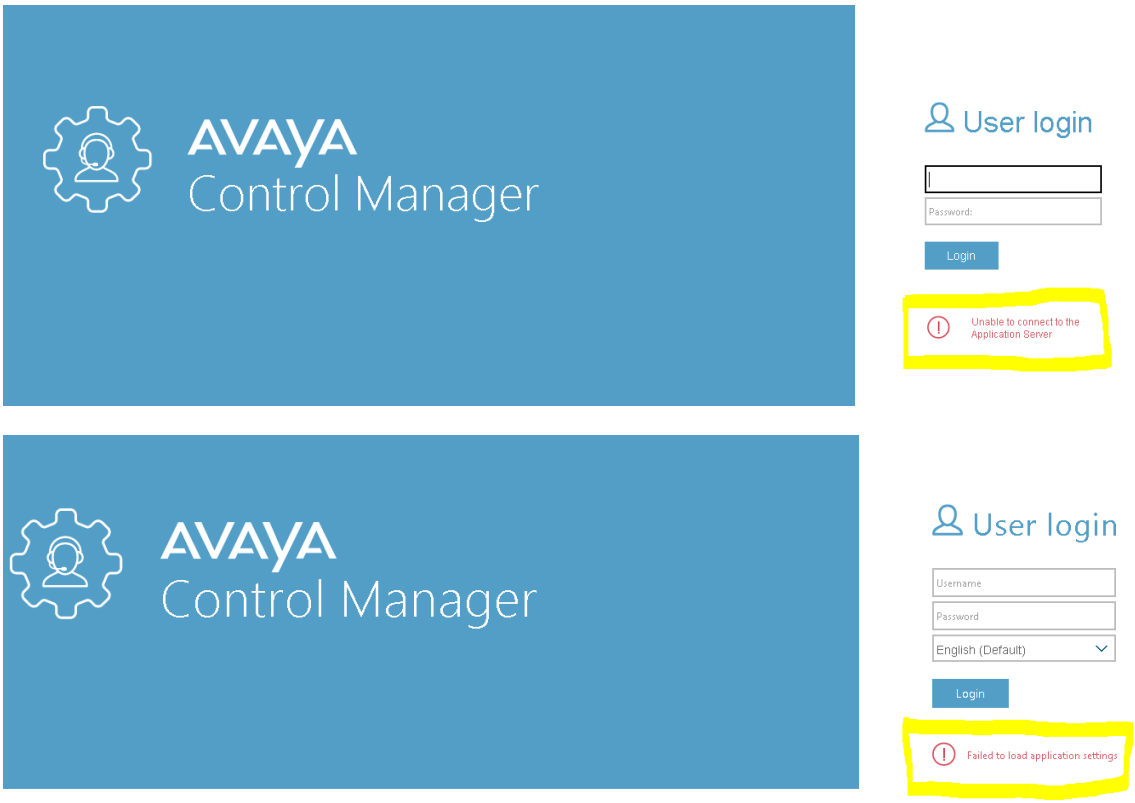
When the secondary application server (ACM-APP-2) fails, the following conditions occur:

- The HA Service on the primary application server (ACM-APP-1) detects a loss of the heartbeat connection between the primary and secondary application servers (ACM-APP-1 and ACM-APP-2).
- Per the reference architecture, the services now operate as follows after the failure:

Control Manager Service	ACM-APP-1	ACM-APP-2
ACCCM Sync Service	Running	Out of Service
ACCCM CM Syslog Server	Running	Out of Service
ACCCM Sphere Feeder	Running	Out of Service
ACCCM AD Sync	Running	Out of Service
ACCCM Audit Log Service	Running	Out of Service
ACCCM License Tracker	Running	Out of Service
ACCCM Schedule Server	Running	Out of Service

- The database replication process continues working as normal since neither of the SQL database servers (ACM-SQL-1 or ACM-SQL-2) have failed.
- From an end-user perspective:
  - For an Enterprise configuration, after the loss of the secondary application server (ACM-APP-2), new URL requests from a user to the secondary application server (ACM-APP-2) result in an error.

- The user might also see one of the error messages shown in the following examples:



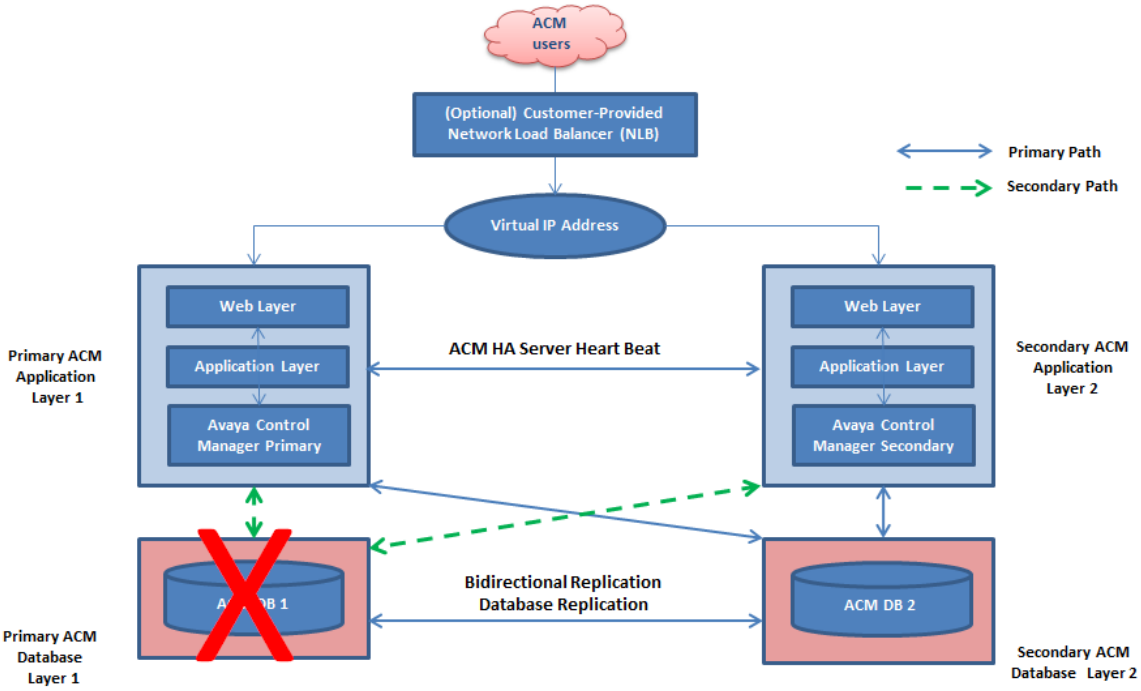
- For an Enterprise configuration, the loss of the secondary application server (ACM-APP-2) means that users must now perform administration work on the primary application server (ACM-APP-1).

Note:

For an Enterprise configuration, recovery procedures for the different server types are described in *Server recovery procedures*.

Failover when the primary database server fails and the secondary database server takes over operations

For an Enterprise configuration, the following diagram show what happens when the primary database server (ACM-SQL-1) fails and the secondary database server (ACM-SQL-2) takes over operations:



When the primary database server (ACM-SQL-1) fails and the secondary database server (ACM-SQL-2) takes over operation, the following occurs:

- For an Enterprise configuration, when the HA Service on the primary application server (ACM-APP-1) detects the failure in the primary database server (ACM-SQL-1):
  1. The HA Service on the primary application server (ACM-APP-1) automatically switches the database connection to the secondary database server (ACM-SQL-2).
  2. The HA Service on the primary application server (ACM-APP-1) notifes the HA Service on the secondary application server (ACM-APP-2) about the failure.
  3. The HA Service on the secondary application server (ACM-APP-2) automatically switches the database connection to the secondary database server (ACM-SQL-2).
- In this failure scenario on the primary database server (ACM-SQL-1), the following service status is required based on the reference architecture:

Control Manager Service	ACM-APP-1		ACM-APP-2	
	Status	Start-up	Status	Start-up
HA Service	Running	Manual	Running	Manual
ACCCM Sync Service	Stopped	Manual	Running	Manual
ACCCM CM Syslog Server	Stopped	Manual	Running	Manual
ACCCM Sphere Feeder	Stopped	Manual	Running	Manual
ACCCM AD Sync	Stopped	Manual	Running	Manual
ACCCM Audit Log Service	Stopped	Manual	Running	Manual

Table continues…

Control Manager Service	ACM-APP-1		ACM-APP-2	
	Status	Start-up	Status	Start-up
ACCCM License Tracker	Stopped	Manual	Running	Manual
ACCCM Schedule Server	Stopped	Manual	Running	Manual

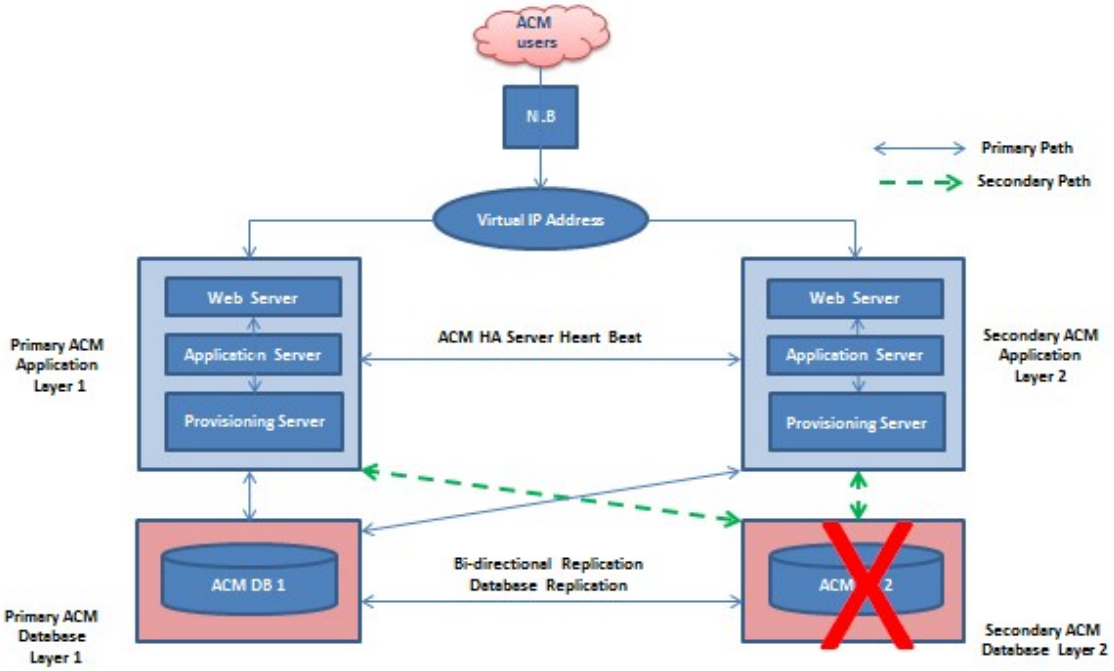
- For an Enterprise configuration, both application servers (ACM-APP-1 and ACM-APP-2), continue to be fully operational in this scenario. Any user requests arriving through the application servers (ACM-APP-1 or ACM-APP-2) are serviced as normal per the configuration settings on the secondary database server (ACM-SQL-2) as opposed to the primary database server (ACM-SQL-1).
- For an Enterprise configuration, any Move, Add, Change, or Delete activity on Control Manager updates the secondary database server (ACM-SQL-2). Upon recovery, updates are replicated automatically from the secondary database server (ACM-SQL-2) to the primary database server (ACM-SQL-1).

Note:

For an Enterprise configuration, recovery procedures for the different server types are described in *Server recovery procedures*.

Failover when the secondary database server fails

For an Enterprise configuration, the following diagram shows what happens when the secondary database server (ACM-SQL-2) fails:



When the secondary database server (ACM-SQL-2) fails, the following conditions occur:

- Since the primary application server (ACM-APP-1) is connected to the primary database server (ACM-SQL-1) as the primary database connection path, there is no change to any service or configuration in the primary application server `NAV360Config.xml` file. The primary application server (ACM-APP-1) continues working as normal, but it has lost any connection to its backup database server (ACM-SQL-2).
- Since the secondary application server (ACM-APP-2) is connected to the primary database server (ACM-SQL-1) as the primary database connection path, there is no change to any service or configuration in the secondary application server `NAV360Config.xml` file. The secondary application server (ACM-APP-2) continues working as normal, but it has lost any connection to its backup database server (ACM-SQL-2).
- For an Enterprise configuration, from the end user perspective, the user gets operational access from either the primary or secondary application servers (ACM-APP-1 or ACM-APP-2).

When the secondary database server (ACM-SQL-2) has been recovered, the databases configured for replication gets synchronized automatically by Microsoft SQL, provided that the outage is recovered within the retention period of the replication distributor. If the secondary database server (ACM-SQL-2) is recovered outside of this retention period, the subscription must be initialized manually from the primary database server (ACM-SQL-1).

After the secondary database server (ACM-SQL-2) is recovered, the secondary database connection path can be activated again in case the primary database server fails.

Note:

For an Enterprise configuration, recovery procedures for the different server types are described in *Server recovery procedures*.

Fixing log on delays after failover

About this task

After failover, users may experience a delay in logging on to the administrative interface. To address this, use this procedure to update the License Service startup order after a failover.

Important:

After the failover is corrected, you must change the order of the License server back to the normal order and restart the service on the primary application server (ACM-APP-1).

Procedure

1. Log on to the Control Manager administrative interface.
2. Navigate to **Configuration** > **Services** > **License**.

   You must see two entries: one for the primary application server (ACM-APP-1) and the secondary application server (ACM-APP-2).
3. Change the service order for the primary to secondary and secondary to primary.

4. Log on to Windows as administrator on the secondary application server (ACM-APP-2).
5. Go to **Start** > **Run**.
6. Enter `services.msc` and press **Enter**.
7. In the Services window, right-click **ACCCM Application Service** and select **Restart**.

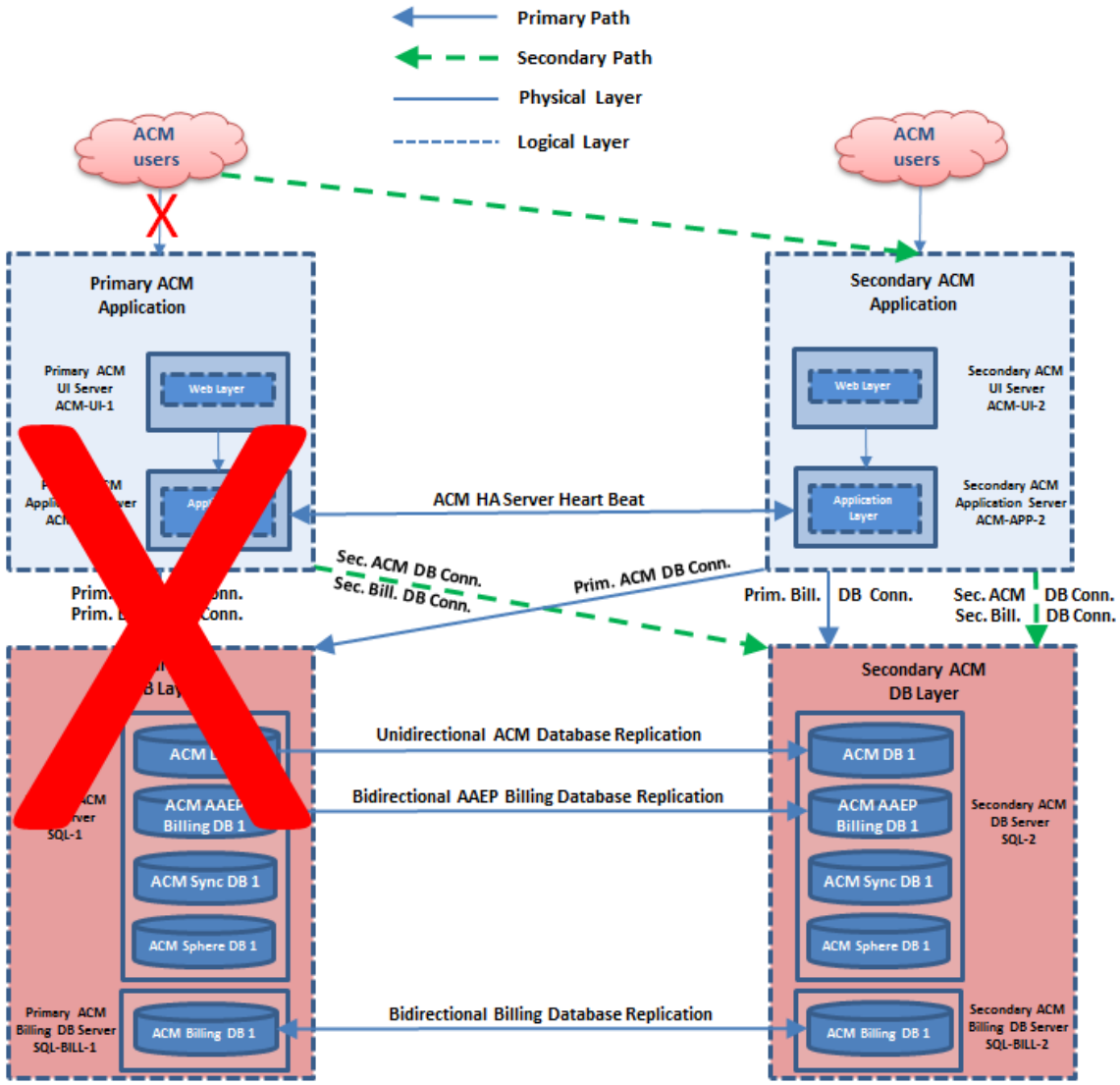
Next steps

After the failover has been corrected, you must change the order of the License server back to the normal order and restart the service on the primary application server (ACM-APP-1).

Data center failover scenarios

Failover when the primary data center fails and the secondary data center server takes over operations

The following diagram shows what happens when the primary data center fails and the secondary data center takes over operations:



When the primary data center fails and the secondary data center takes over operation, the following occurs:

- For an Enterprise configuration, users that try to access the primary application server (ACM-APP-1) or that are already connected and logged on to the primary application server sees an error that indicates the Web page cannot be displayed. To continue performing administration work, an end user must log in to the secondary application server (ACM-APP-2).
- The following service status is required based on the reference architecture:

Control Manager Service	ACM-APP-1		ACM-APP-2	
	Status	Startup	Status	Startup
HA Service	N/A	Manual	Running	Manual
ACCCM Sync Service	N/A	Manual	Running	Manual
ACCCM CM Syslog Server	N/A	Manual	Running	Manual
ACCCM Sphere Feeder	N/A	Manual	Running	Manual
ACCCM AD Sync	N/A	Manual	Running	Manual
ACCCM Audit Log Service	N/A	Manual	Running	Manual
ACCCM License Tracker	N/A	Manual	Running	Manual
ACCCM Schedule Server	N/A	Manual	Running	Manual

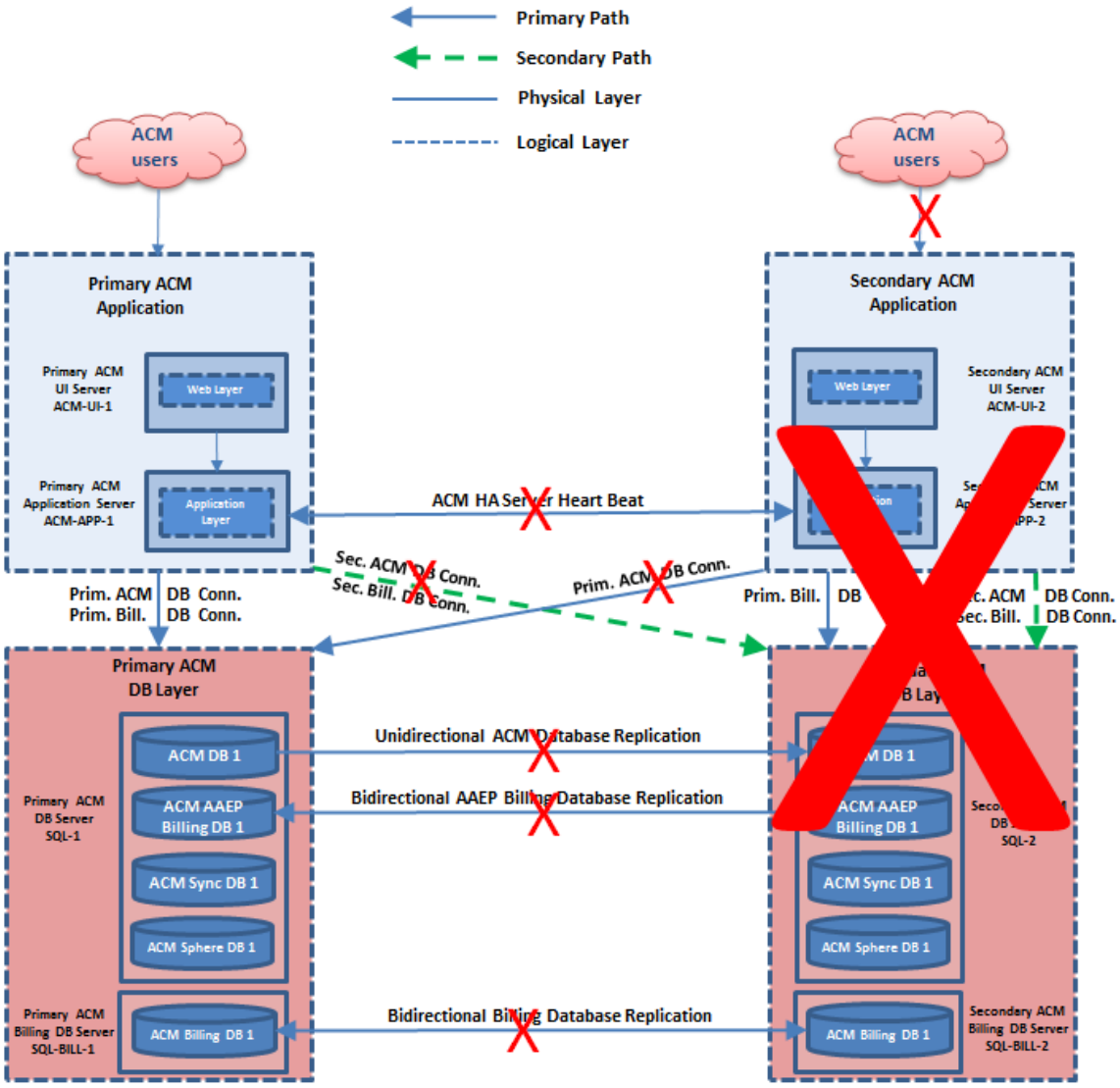
- For an Enterprise configuration, any Move, Add, Change, or Delete activity on Control Manager updates the secondary database server (ACM-SQL-2). Upon recovery, updates are replicated automatically from the secondary database server (ACM-SQL-2) to the primary database server (ACM-SQL-1).

Note:

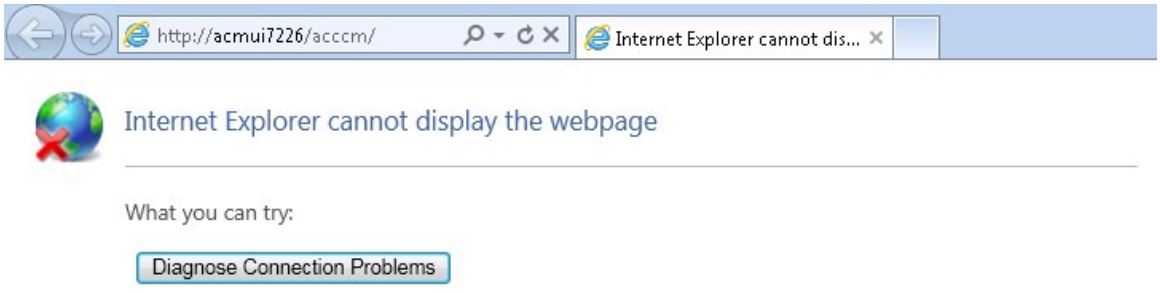
For an Enterprise configuration, recovery procedures for the different server types are described in *Server recovery procedures*.

Failover when the secondary data center fails and the primary data center remains in operation

The following diagram shows what happens when the secondary data center fails and the primary data center remains in operation:



- For an Enterprise configuration, for most users, they cannot notice the failure unless they happen to normally log in to the ACM-APP-2 server in the secondary data center. Users that try to access the secondary application server or are already connected and logged into the secondary application server, ACM-APP-2 sees the following or similar error message:



- For an Enterprise configuration, to continue performing administration work, an end user must log in to the primary application server (ACM-APP-1).
- The following service status is required based on the reference architecture:

Control Manager Service	ACM-APP-1		ACM-APP-2	
	Status	Startup	Status	Startup
HA Service	Running	Manual	N/A	Manual
ACCCM Sync Service	Running	Manual	N/A	Manual
ACCCM CM Syslog Server	Running	Manual	N/A	Manual
ACCCM Sphere Feeder	Running	Manual	N/A	Manual
ACCCM AD Sync	Running	Manual	N/A	Manual
ACCCM Audit Log Service	Running	Manual	N/A	Manual
ACCCM License Tracker	Running	Manual	N/A	Manual
ACCCM Schedule Server	Running	Manual	N/A	Manual

- Since the primary application server (ACM-APP-1) is connected to the primary database server (ACM-SQL-1) as the primary database connection path, there is no change to any service or configuration in the primary application server `NAV360Config.xml` file. The primary application server (ACM-APP-1) continues working as normal, but it has lost any connection to its backup database server (ACM-SQL-2).
- For an Enterprise configuration, since the primary database server (ACM-SQL-1) is still operational, the primary application server (ACM-APP-1) continues using the primary database connection path to the primary database server (ACM-SQL-1).

When the secondary database server (ACM-SQL-2) has been recovered, the databases configured for replication gets synchronized automatically by Microsoft SQL, provided that the outage is recovered within the retention period of the replication distributor. If the secondary database server (ACM-SQL-2) is recovered outside of this retention period, the subscription must be initialized manually from the primary database server (ACM-SQL-1).

After the secondary database server (ACM-SQL-2) is recovered, the secondary database connection path can be activated again in case the primary database server fails. The HA Service can be restarted on both Data Center 1 and Data Center 2.

For an Enterprise configuration, to bring the connection from the application servers (ACM-APP-1 and ACM-APP-2) back to the primary database server (ACM-SQL-1), you must do a manual recovery. To manually recover the primary database server connection path, see *Server recovery procedures*.

Server recovery procedures (Enterprise only)

Recovering the primary application server while the secondary application server is running

About this task

Use this procedure to bring the failed server back into operation within the HA configuration.

Important:

This procedure does not explain how to repair the server from the failure. See Control Manager installation documentation for information about reinstalling or replacing the failed server.

Procedure

1. Bring the repaired server into operation within the configuration.
2. Stop the HA Service on both of the application servers (ACM-APP-1 and ACM-APP-2).
3. Confirm that the `Nav360config.xml` file on the secondary application server (ACM-APP-2) is pointing the database connection back to the primary database server (ACM-SQL-1).
4. Confirm that the `Nav360config.xml` file on the primary application server (ACM-APP-1) is pointing the database connection back to the primary database server (ACM-SQL-1).
5. Stop the License Tracker, Audit Log, AD Sync, CM Syslog Server, Schedule Server, Sphere Feeder, and Sync Service services on the secondary application server (ACM-APP-2).
6. Start the License Tracker, Audit Log, AD Sync, CM Syslog Server, Schedule Server, Sphere Feeder, and Sync Service services on the primary application server (ACM-APP-1).

   The following table shows the normal operation status for these services:

Control Manager Service	ACM-APP-1	ACM-APP-2
ACCCM Sync Service	Running	Stopped
ACCCM CM Syslog Server	Running	Stopped
ACCCM Sphere Feeder	Running	Stopped
ACCCM AD Sync	Running	Stopped
ACCCM Audit Log Service	Running	Stopped
ACCCM License Tracker	Running	Stopped
ACCCM Schedule Server	Running	Stopped

7. Start the HA Service on both application servers (ACM-APP-1 and ACM-APP-2).

Recovering the secondary application server while the primary application server is running

About this task

Use this procedure to bring the failed server back into operation within the HA configuration.

Important:

This procedure does not explain how to repair the server from the failure. See Control Manager installation documentation for information about reinstalling or replacing the failed server.

Procedure

1. Bring the repaired server into operation within the configuration.
2. Stop the HA Service on both of the application servers (ACM-APP-1 and ACM-APP-2).
3. Confirm that the `Nav360config.xml` file on the secondary application server (ACM-APP-2) is pointing the database connection back to the primary database server (ACM-SQL-1).
4. Confirm that the `Nav360config.xml` file on the primary application server (ACM-APP-1) is pointing the database connection back to the primary database server (ACM-SQL-1).
5. Stop the License Tracker, Audit Log, AD Sync, CM Syslog Server, Schedule Server, Sphere Feeder, and Sync Service services on the secondary application server (ACM-APP-2).
6. Start the License Tracker, Audit Log, AD Sync, CM Syslog Server, Schedule Server, Sphere Feeder, and Sync Service services on the primary application server (ACM-APP-1).

   The following table shows the normal operation status for these services:

Control Manager Service	ACM-APP-1	ACM-APP-2
ACCCM Sync Service	Running	Stopped
ACCCM CM Syslog Server	Running	Stopped
ACCCM Sphere Feeder	Running	Stopped
ACCCM AD Sync	Running	Stopped
ACCCM Audit Log Service	Running	Stopped
ACCCM License Tracker	Running	Stopped
ACCCM Schedule Server	Running	Stopped

7. Start the HA Service on both of the application servers (ACM-APP-1 and ACM-APP-2).

Recovering the primary database server while the secondary database server is running

About this task

Use this procedure to bring the failed server back into operation within the HA configuration.

Important:

This procedure does not explain how to repair the server from the failure. See Control Manager installation documentation for information about reinstalling or replacing the failed server.

Procedure

1. Bring the repaired server into operation within the configuration.

   Once the primary database server (ACM-SQL-1) has been recovered and all of the Microsoft SQL services are up and running, the databases configured for bidirectional replication automatically gets synchronized between the database servers (ACM-SQL-2 and ACM-SQL-1) using the Microsoft SQL replication services.

   Any actions performed on the secondary database server (ACM-SQL-2) while the primary database server (ACM-SQL-1) was unavailable now gets automatically replicated when the primary database server (ACM-SQL-1) is back in service.

   Before you switch back to the primary database server (ACM-SQL-1), verify that the synchronization status of all publications on the primary database server (ACM-SQL-1) report `No replicated transactions are available`.

   Important:

   Perform the following steps out of hours to bring the database connection path for the primary and secondary application servers (ACM-APP-1 and ACM-APP-2) back to the ACM-SQL-1 server as the primary connection path.

2. Stop the HA Service on both of the application servers (ACM-APP-1 and ACM-APP-2).
3. Reconfigure the `Nav360config.xml` file on the secondary application server (ACM-APP-2) and point the database connection back to the primary database server (ACM-SQL-1).
4. Reconfigure the `Nav360config.xml` file on the primary application server (ACM-APP-1) and point the database connection back to the primary database server (ACM-SQL-1).
5. Stop the License Tracker, Audit Log, AD Sync, CM Syslog Server, Schedule Server, Sphere Feeder, and Sync Service services on the secondary application server (ACM-APP-2).
6. Start the License Tracker, Audit Log, AD Sync, CM Syslog Server, Schedule Server, Sphere Feeder, and Sync Service services on the primary application server (ACM-APP-1).

   The following table shows the normal operation status for these services:

Control Manager Service	ACM-APP-1	ACM-APP-2
ACCCM Sync Service	Running	Stopped
ACCCM CM Syslog Server	Running	Stopped
ACCCM Sphere Feeder	Running	Stopped

Table continues…

Control Manager Service	ACM-APP-1	ACM-APP-2
ACCCM AD Sync	Running	Stopped
ACCCM Audit Log Service	Running	Stopped
ACCCM License Tracker	Running	Stopped
ACCCM Schedule Server	Running	Stopped

7. Start the HA Service on both of the application servers (ACM-APP-1 and ACM-APP-2).

Recovering the secondary database server while the primary database server is running

About this task

Use this procedure to bring the failed server back into operation within the HA configuration.

Important:

This procedure does not explain how to repair the server from the failure. See Control Manager installation documentation for information about reinstalling or replacing the failed server.

Procedure

Bring the repaired server into operation within the configuration.

Once the secondary database server (ACM-SQL-2) has been recovered and all of the Microsoft SQL services are up and running, the databases configured for replication will automatically get synchronized between the database servers (ACM-SQL-2 and ACM-SQL-1) using the Microsoft SQL replication services.

Any actions performed on the primary database server (ACM-SQL-1) while the secondary database server (ACM-SQL-2) was unavailable will now get automatically replicated when secondary database server (ACM-SQL-2) is back in service.

After the secondary database server (ACM-SQL-2) recovery, the secondary database connection path can be utilized again, if potential failures on the primary database server (ACM-SQL-1).

Avaya one-X® Agent recovery procedures

About this task

Users may experience a delay when logging on to the system after a failure. You must update the License Service startup order to fix the problem.

Note:

The steps in this procedure must be reversed for recovery to a sunny day configuration.

Procedure

1. Log on to the Control Manager administration interface.

2. Navigate to **Configuration** > **Services** > **License**.

   You must see two entries, one for the primary application server (ACM-APP-1) and the secondary application server (ACM-APP-2).

3. Change the order of the services so that the primary application server (ACM-APP-1) points to the secondary application server (ACM-APP-2), and that the secondary application server (ACM-APP-2) points to the primary application server (ACM-APP-1).
4. Log on to Windows on the secondary application server (ACM-APP-2).
5. Navigate to **Start** > **Run**.
6. Enter `services.msc` and press **Enter**.

   The system displays a list of services.

7. In the Services window, right-click the ACCCM Application Server service and select **Restart**.

Chapter 10: Troubleshooting Licensing problems

License server service not starting

Condition

License server service not starting

Cause

WebLMNet.dll related error in logs of license server service.

Solution

Install C++ Redistributable 2013 and 2015-2019(x86) on Control Manager server and then try to start license server service.

No valid license found error when you login to Control Manager

Condition

No valid license found error when you login to Control Manager.

Cause

Control Manager is in Restricted Mode and Grace period of 30 days is over

Solution

1. Install valid Control Manager license on WebLM server and configure WebLM server in Control Manager through Health Monitoring tool.
2. On the Control Manager server, start Health Monitoring Diagnostics from system tray.
3. Click on **WebLM Server** tab.
4. Enter WebLM server URL in this format, for example https://<WebLM_Server_IPAddress>:52233/WebLM/LicenseServer
5. Click **Test** to verify connectivity.
6. Click **Save**.

7. Restart ACCCM license server service.

User cannot access Avaya Oceana® admin screens when Control Manager is in grace mode

Condition

User receives licensing related error messages while administering features like Avaya Oceana® admin screens when Control Manager is in Grace mode

Cause

Valid license file is not installed on WebLMServer or WebLM server is down or WebLMis being upgraded. This WebLMis configured with Control Manager.

Solution

To continue Control Manager to work in Grace Mode with all features, Work around to this issue is either remove WebLM configuration from Control Manager or install valid license file on WebLM server and restart license service on Control Manager server.

Control manager showing grace mode warning message

Condition

Control manager showing grace mode warning message

Cause

No valid license details received from WebLMWebLM server due to:

- Incorrect WebLM server is configured
- Valid Control Manager license file is not installed on WebLM server
- Control Manager is not able to reach WebLM server due to network issues
- Installed Control Manager's major version (9 in 9.x.x.x) does not match the major version of Control Manager (9 in 9.x.x.x) recorded with the WebLM license installed on the WebLM server. If the major version does not match, then Control Manager enters in the Grace mode

Solution

1. Configure WebLM Server in Control Manager, test connection and if connection is successful then restart license server service. Ensure that you have valid control manager license file installed on WebLM server.
2. If WebLM server is already configured then check whether valid Control Manager license is installed on WebLM server and ACM is able to communicate with it by testing WebLM server connectivity.

3. Navigate to **Configuration** > **License** > **WebLM Server** and edit the existing WebLM server and click **Test**. If connection is not successful then verify that WebLM server is active and reachable from Control Manager.
4. Check whether Control Manager server in WebLM license file has reached to its limit. If yes, either free some licenses by shutting down Control Manager or request for new license.
5. If test connection to the WebLM server is not successful or anytime WebLM server is shutdown or being upgraded then remove the WebLM configuration from Control Managerand restart the license service for continuous access in Grace mode.

Chapter 11: Resources

Documentation

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

Title	Description
Overview	
Avaya Control Manager Overview and Specification	This document describes the features and specifications for the Control Manager product.
Planning	
Planning for an Avaya Control Manager Deployment (formerly known as *Avaya Control Manager Customer Requirements*)	This document describes the planning and prerequisites that customers must follow before deploying Control Manager.
New Installation	
Installing Avaya Control Manager	This document describes how to install, configure, and test the non-HA and Multiplex HA deployments of Control Manager.
Upgrades	
Upgrading Avaya Control Manager	This document describes how to upgrade the Enterprise, and non-HA Enterprise, Control Manager systems from an earlier release to the current release. The document includes upgrade checklist, upgrade procedures, and verification procedures for each supported upgrade path.
Configuration	
Configuring Avaya Control Manager	This document describes how to configure Control Manager to work with other Avaya products.
Avaya Control Manager Release Notes	This document contains any special release information, upgrade steps, and known issues.
Avaya Control Manager Port Matrix	This document describes the port usage for Control Manager.
Administration	
Using Avaya Control Manager to Administer Avaya Products	This document describes how to use Control Manager to administer features on Avaya products.
Administering Avaya one-X® Agent Using Avaya Control Manager	This document describes how to use Control Manager to administer Avaya one-X® Agent.

Table continues…

Title	Description
Administering an Avaya Experience Portal Sample Application Using Avaya Control Manager	This document describes how to use Control Manager with Experience Portal.
Administering Avaya Control Manager for Avaya Agent for Desktop	This document describes how to use Control Manager to administer Avaya Agent for Desktop.
Events and Alarms	
Avaya Control Manager Events, Alarms, and Errors Reference	This document describes the SNMP notifications for Control Manager.
Using	
Using Avaya Control Manager Conversation Sphere	This document describes how to use Control Manager Conversation Sphere to administer vectors, strategies, and call flows.
Using Avaya Control Manager Central License and Traffic Tracker	This document describes how to use Control Manager Central License and Traffic Tracker.
Maintenance and Troubleshooting	
Maintaining and Troubleshooting Avaya Control Manager	This document describes maintenance procedures and troubleshooting scenarios for Control Manager.
Documents to be downloads from the support site	
Using the Avaya Control Manager SOAP API	This document describes how to use the SOAP version of the Control Manager API.
Using the Avaya Control Manager REST API	This document describes how to use the REST version of the Control Manager API.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or more of the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
7. Click **Enter**.

Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
  - Click **Filters** to select a product and then type key words in **Search**.
  - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** ( ).

Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

- Create, rename, and delete a collection.
- Add topics from various documents to a collection.
- Save a PDF of selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

Training

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

Course code	Course title
Technical Design	
3320W	Avaya Customer Engagement Platforms Overview (includes Avaya Control Manager Product Information Documents (PIDs))
3330W	Avaya Customer Engagement Administration and Applications Overview (includes Avaya Control Manager PIDs)
3420W	Avaya Oceana® Design Fundamentals (includes Avaya Control Manager PIDs)
3371T	APDS Avaya Customer Engagement Solutions Online Test
3470T	Avaya Oceana® Design Fundamentals Online Test
Technical Services	

Table continues…

Course code	Course title
2092W	Configuring Avaya Control Manager for Cloud Service Providers
2092T	Avaya Control Manager Instance Configuration and Administration Test for Cloud Service Providers
5307T	Avaya Control Manager Implementation and Support Test for Cloud Service Providers
70920W	Installing Avaya Control Manager
7093W	Upgrading and Supporting Avaya Control Manager for Cloud Service Providers
70940W	Configuring Avaya Control Manager for Enterprise
70950W	Upgrading and Supporting Avaya Control Manager for Enterprise
70910W	Administering Avaya Control Manager for Enterprise
7091T	Administering Avaya Control Manager R8 Online Test
5306	Avaya Control Manager Implementation and Support Test
24310W	Administering Avaya Analytics™ for Oceana®
24320W	Administering Avaya Oceana®

The following courses are also available on the Avaya Control Manager website at https://ACM_host/ACCCMPortal. After logging into the website, go to **Personal Settings** > **Training**.

Course code	Course title
24320W	Administering Avaya Oceana® Basics
24310W	Administering Avaya Analytics™ for Avaya Oceana® Basics
70910W	Administering Avaya Control Manager for Enterprise

Viewing Avaya Mentor videos

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

About this task

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

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

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

In the right pane, the page displays a list of available videos.

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

Note:

Videos are not available for all products.

Support

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

Using the Avaya InSite Knowledge Base

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

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

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

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

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.

5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Index

A

accessing port matrix 131
announcements 85, 86
application pool 96
authentication failed 93
autogrowth settings 21
autoshrink settings 21
Avaya one-X Agent
    profile loader 84
Avaya support website 134

B

backing up 10
backup 9
bulk job 85

C

certificate
    renewal 41
changing recovery model to simple 12
collection
    delete 131
    edit name 131
    generating PDF 131
    sharing content 131
content
    publishing PDF output 131
    searching 131
    sharing 131
    sort by last updated 131
    watching for updates 131
Control Manager 16
control manager showing grace mode warning message . 127

D

database maintenance 9
database recovery modes 12
databases 10
database server failure 83
delays accessing Communication Manager pages ... 100, 102
Diagnostic Monitor 54
documentation center 131
    finding content 131
    navigation 131
documentation portal 131
    finding content 131
    navigation 131
document changes 7

E

Esent database error 91

F

failed attributes 85
failover
    application servers 107
    Multiplex HA 105
    primary data center fails 116
    secondary application server fails 110
    secondary database server fails 114
    secondary data center fails 118
    software load balancer 105
failover scenarios
    overview 107
    primary database server fails 112
    service impact 109
failure recovery
    primary application server 121
    primary database server 122
    secondary application server 122
    secondary database server 124
failure scenarios
    server start-up requirements 109
file integrity 77
File Integrity logs
    checking 77
file integrity script 78
finding content on documentation center 131
finding port matrix 131

G

generating logs 78

H

health monitoring 52
Health Monitoring tool 35
Health Monitor Status 52
    non-system drive 53

I

InSite Knowledge Base 134
installation failure 90

J

Java troubleshooting 97

Java version 35

L

licenses 94
license server service not starting 126
license tracker troubleshooting 97
licensing 49, 50
login limits 100, 102
logon delays 115

M

messaging 104
migrating the database 10
My Docs 131

N

no valid license found error 126

O

one-X license 51

P

password error 84
play 85, 86
port matrix 131
prerequisites 90
profile loader 84

R

reason codes 103
rebooting servers 27
    Enterprise HA configuration 33
    Enterprise non-HA configuration 32
    Multiplex HA 1x2 configuration 30
    Multiplex HA 2x1 configuration 29
    Multiplex HA 2x2 configuration 27
recovery
    Avaya one-X Agent 124
recovery modes 12
related documentation 129
removing
    Control Manager databases 45
    Control Manager services 43
    prerequisite components 42
renaming computers
    Multiplex 1x2 configuration 14
    Multiplex HA 2x2 configuration 14
restoring Control Manager
    restricted mode 25
restoring the database 10

S

searching for content 131
services descriptions 79
setting the Windows time 38
sharing content 131
shrinking a log file 19
simple recovery model 12
software load balancer 105
sort documents by last updated 131
sphere feeder
    connection error 87
    database 87
Sphere link cannot redirect to proper page 86
Sphere queries excessive 82
sphere search engine 87
start services 35
status icon 76
stop services 35
support 134
synchronizer application 95

T

TDE 16
the default language is not applied when you launch Control Manager for the first time 92
TLS 16
TLS support 16
Tomcat 87
training 132
transparent data encryption 16
transport layer security 16
troubleshooting 90, 93, 95
    connections to Avaya products. 95
    Control Manager services 90
    control sphere 87
    firewall 92
    Java 97
    license tracker 97
    synchronization with Communication Manager 96
troublshooting 94
two-digit to one-digit 103

U

uninstalling Control Manager software 41
updating
    Java version 35
    SQL software 25
    Windows OS 25
Usage Metering 81
user cannot access Oceana admin screens when ACM is in grace mode 127

V

videos 133

W

watch list 131
Windows time setting 38