Upgrading to Avaya Control Manager 8.0.4 for Partner Cloud Powered by Avaya xCaaS

Release 8.0.4
Issue 1
October 2018

© 2018, Avaya Inc.
All Rights Reserved.

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. 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. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

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

The following applies 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 ... 8
Purpose ... 8
Chapter 2: Overview ... 9
Supported upgrade scenarios ... 9
Architecture overview ... 10
Chapter 3: Requirements ... 13
Hardware and VMware requirements ... 13
Multi-server configuration ... 13
Software requirements ... 17
Latest software updates and patch information ... 17
Supported server operating system software requirements ... 18
Operating system considerations ... 18
Supported database server software requirements ... 18
Supported Microsoft Window OS and SQL combinations ... 21
Supported client Web browser and client operating system software requirements ... 21
Certificate requirements ... 22
Java Runtime Environment requirements ... 22
Virtualization support ... 22
Amazon Web Services support ... 23
Getting Control Manager licenses ... 23
Chapter 4: Reference configurations ... 25
Reference configurations for xCaaS deployments ... 25
Deployment considerations for a single data center ... 28
Deployment considerations in a dual data center or disaster recovery configuration ... 28
Requirements for HA deployments ... 29
Databases installed ... 30
Deploying Control Manager using a virtual IP address and optional Network Load Balancer ... 31
Deploying Control Manager using dedicated IP addresses ... 32
About replication ... 33
Switchover and Failover methods ... 36
Chapter 5: Worksheets ... 37
Server worksheet — Multiple host configurations ... 37
Chapter 6: Installing prerequisite software ... 39
Software installation prerequisites for the customer ... 39
Installing and configuring IIS on the Microsoft Windows Server 2012 OS ... 41
Installing and configuring IIS on the Microsoft Windows Server 2016 OS ... 46
Installing the Microsoft SQL Server software ... 51
Installing certificates ... 53
Generating a Certificate Signing Request in IIS ... 54

Submitting the CSR to a CA for signing.... 56
Installing the signed certificate.... 59
Binding the certificate to SSL port 9011 for HA.... 60
Installing the root certificate.... 61
Enabling SSL for secure browser access.... 62
Upgrading Windows 2012 to Windows 2012 R2.... 65
Preparing the license server for startup.... 66
Chapter 7: Upgrading a system using database migration.... 68
Upgrade process overview.... 68
Upgrade checklist.... 69
Installation and upgrade considerations.... 71
Control Manager databases that require backup.... 72
Backing up Control Manager databases.... 73
Restoring (migrating) the Control Manager databases.... 76
Installing Control Manager software on the primary application server (ACM-APP-1).... 78
Installing Control Manager software on the secondary application server (ACM-APP-2).... 84
Installing the Control Manager software on the primary UI server (ACM-UI-1).... 90
Installing Control Manager software on the secondary UI server (ACM-UI-2).... 95
Installing Control Manager licenses.... 101
Recreating scheduled jobs.... 102
Upgrading the Control Manager billing software.... 103
Uninstalling the billing software.... 103
Installing billing software on the Control Manager servers.... 104
Configuring the billing software.... 107
Configuring extension number delimiters to support billing count accuracy.... 108
Billing configuration changes to the secondary data center.... 111
Configuring the billing engine startup and recovery properties.... 114
Testing the restore (migration).... 118
Chapter 8: Upgrading a system using an in-place upgrade.... 120
Upgrade process overview.... 120
Upgrade checklist.... 121
Installation and upgrade considerations.... 122
Databases installed.... 123
Control Manager databases that require backup.... 124
Backing up Control Manager databases.... 125
Removing replication on the SQL servers.... 127
Stopping the Control Manager services.... 129
Uninstalling Control Manager patches.... 129
Upgrading Control Manager software in an HA configuration.... 131
Installing Control Manager licenses.... 138
Upgrading the Control Manager billing software.... 139
Uninstalling the billing software.... 139
Installing billing software on the Control Manager servers.... 139

Configuring the billing software.... 143
Configuring extension number delimiters to support billing count accuracy.... 143
Billing configuration changes to the secondary data center.... 146
Configuring the billing engine startup and recovery properties.... 149
Chapter 9: Configuring replication.... 154
About replication.... 154
Verifying that Microsoft Distributed Transaction Coordinator (DTC) is installed and configured... 156
Configuring SQL replication on the primary and secondary database servers (ACM-SQL-1 and ACM-SQL-2).... 157
Configuring the publication for database replication on the primary SQL database server (ACM-SQL-1).... 165
Enabling replication on the database servers.... 169
Chapter 10: Configuring HA services.... 173
About HA services.... 173
Control Manager Services for High Availability.... 175
Stopping the Control Manager services.... 176
Configuring the sphereFeederConfig.xml file on the secondary application server (ACM-APP-2).... 177
Configuring the HA Service on the primary UI server (ACM-UI-1).... 177
Configuring the configuration.xml file on the primary UI server (ACM-UI-1).... 178
Configuring the HA Service on the primary application server (ACM-APP-1).... 180
Configuring the configuration.xml file on the primary application server (ACM-APP-1).... 181
Configuring the HA Service on the secondary UI server (ACM-UI-2).... 183
Configuring the configuration.xml file on the secondary UI server (ACM-UI-2).... 184
Configuring the HA Service on the secondary application server (ACM-APP-2).... 186
Configuring the configuration.xml file on the secondary application server (ACM-APP-2).... 187
Starting the HA services after editing the configuration files.... 189
Chapter 11: Configuring the Experience Portal billing.... 191
Configuring the Experience Portal billing service on the primary application server (ACM-APP-1).... 191
Configuring the Experience Portal billing service on the secondary application server (ACM-APP-2).... 192
Chapter 12: Testing the installation.... 194
Starting the Control Manager License Server.... 194
Logging on to the Control Manager user Interface.... 194
Testing the HA installation.... 196
Verifying the TLS version.... 198
Rollback to the initial HA service configuration.... 199
Checking basic sanity after an upgrade.... 199
Chapter 13: Resources.... 201
Documentation.... 201
Finding documents on the Avaya Support website.... 202
Avaya Documentation Portal navigation.... 203

Training..... 204
Viewing Avaya Mentor videos..... 205
Support..... 205
Using the Avaya InSite Knowledge Base..... 205

Chapter 1: Introduction

Purpose

This document describes how to upgrade Avaya Control Manager release 7.1.101.x and 8.0.x to Release 8.0.4 in High Availability (HA) configurations for Partner Cloud Powered by Avaya xCaaS(xCaaS, also known as Service Provider) solutions. Upgrade of Control Manager software is done by Avaya personnel with assistance from customer administrators. In an xCaaS configuration, Control Manager is part of a solution that includes Avaya Aura® products and xCaaS.

This document provides the following information:

- An overview of deployments and product architecture
- Information about reference configurations
- Hardware and software requirements
- Checklists and worksheets
- Prerequisite third-party software installation procedures for the customer
- Control ManagerSoftware upgrade and data migration procedures
- Replication configuration procedures
- HA services configuration procedures
- Test procedures

For information about troubleshooting upgrade problems, see *Maintaining and Troubleshooting Avaya Control Manager*.

Chapter 2: Overview

Supported upgrade scenarios

Upgrades to Control Manager 8.0.4 are done using two methods:

- Using Microsoft SQL database migration to back up and restore the databases from the old system onto a new set of servers. You *must* use this method if you are also upgrading the Microsoft Windows Server OS and Microsoft SQL Server software at the same time you are upgrading the Control Manager software.
- Using the Control Manager installation program to perform an in-place upgrade on the current set of servers. You will use this method if all you are doing is upgrading Control Manager software and are *not* upgrading the Microsoft Windows Server OS and Microsoft SQL Server software.

Current system	Upgraded system	See procedures in the following chapter:
Control Manager 7.1.101.x (with Control Manager patches 1, 3, 5, 6, and 7, and MIBC patches 1 and 2) on any supported Microsoft Windows Server OS version and any Microsoft Windows SQL Server version	Control Manager 8.0.4.x on Microsoft Windows Server OS 2012 R2 and Microsoft Windows SQL Server 2012 or 2014	*Upgrading a system using database migration*
Control Manager 8.0.1.1 on Microsoft Windows Server OS 2012 R2 and Microsoft Windows SQL Server 2012 or 2014	Control Manager 8.0.4.x on Microsoft Windows Server OS 2012 R2 and Microsoft Windows SQL Server 2012 or 2014	*Upgrading a system using an in-place upgrade*
Control Manager 8.0.2.x on Microsoft Windows Server OS 2012 R2 and Microsoft Windows SQL Server 2012 or 2014	Control Manager 8.0.4.x on Microsoft Windows Server OS 2012 R2 and Microsoft Windows SQL Server 2012 or 2014	*Upgrading a system using an in-place upgrade*
Control Manager 8.0.3.x on Microsoft Windows Server OS 2012 R2 and Microsoft Windows SQL Server 2012 or 2014	Control Manager 8.0.4.x on Microsoft Windows Server OS 2012 R2 and Microsoft Windows SQL Server 2012 or 2014	*Upgrading a system using an in-place upgrade*

Note:

Any Control Manager systems with releases older than those shown in the first column must first be upgraded to the release shown in the first column before you can upgrade to Release 8.0.4.x.

Note:

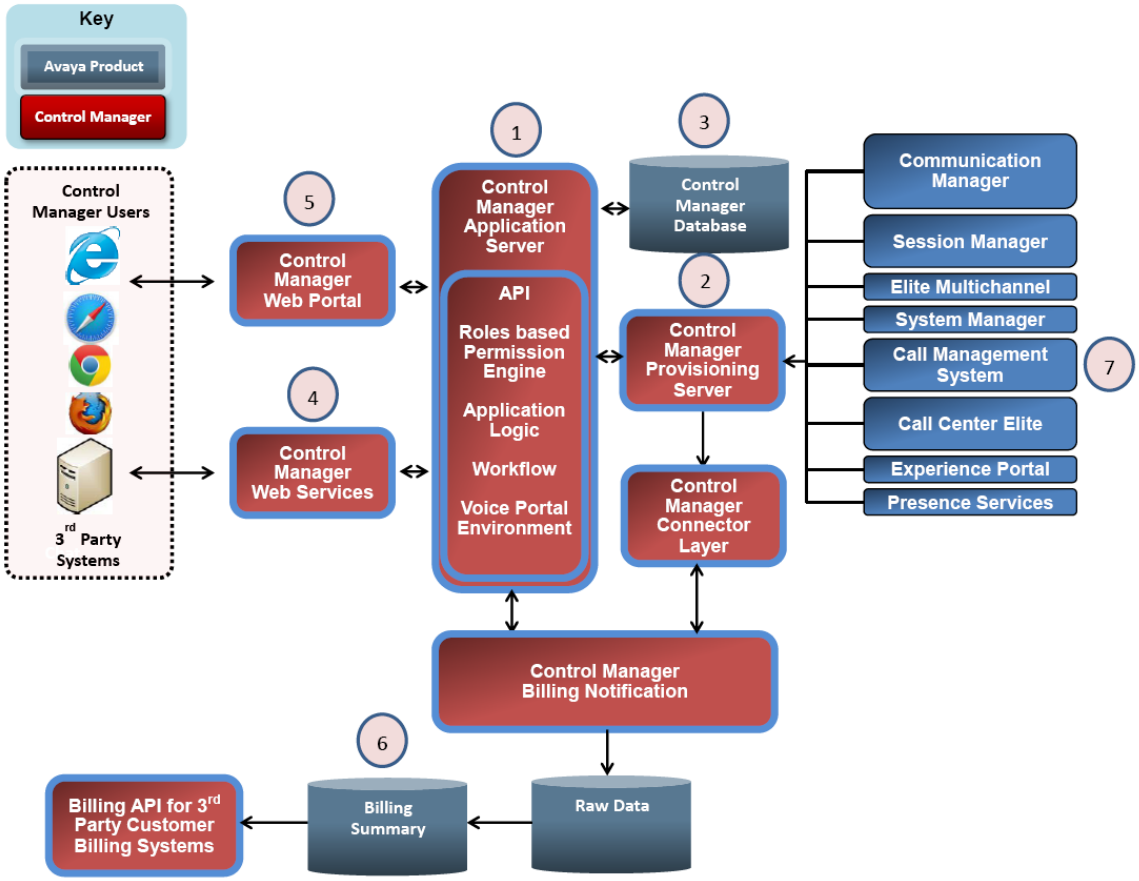
When upgrading an HA deployment, you must upgrade the primary system, followed by the secondary system, then enable replication between the two systems. The upgrade process for an HA system is explained in detail later in this document.

Architecture overview

The Control Manager provisioning server integrates Control Manager with different Avaya products and systems through various connectors. These connectors are part of the overall solution subject to the type of active Control Manager connectors made active.

Control Manager uses the system architecture, software integrations, and software components to provide a multi-channel contact center solution.

The key components for a Control Manager solution include those shown in the following diagram and table:

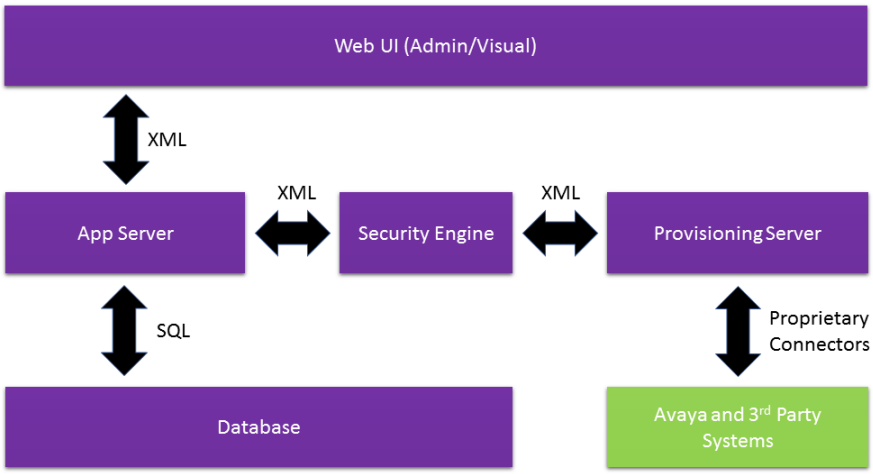


	Component	Description
1	Application Server	Performs the business logic (or the programming) between the end user interface and the database as well as providing the security engine for Control Manager.
2	Provisioning Server	Responsible for provisioning components from Control Manager with the different Partner Cloud Powered by Avaya xCaaS applications. The provisioning server integrates Control Manager with the different Avaya applications through the various supported connectors allowing the provisioning of information from across the environment.
3	Database	The main Microsoft SQL database that stores the Control Manager system configuration and the pointers to data objects from adjunct systems, such as Communication Manager, required by Control Manager to pull complete data in real time when needed.
4	Web Services	A set of web services that developers use for integrating the Control Manager provisioning server to add, delete, or modify configurations from within the Avaya environment.
5	Web Portal	The management interface that provides complete access to all the features of Control Manager. The Web portal can be used in a variety of

Table continues…

	Component	Description
		scenarios ranging from product-specific managements to overall suite management.
6	Billing Database	Provides billing services for service providers.
7	Connectors	Used to integrate and manage the Partner Cloud Powered by Avaya xCaaS applications.

The High-Level Solution Topology platforms, including all available solution connectors provides a centralized operational management from a single Web browser portal.



Layer	Components
Web	Web Interface Interface API
Application	Application Server Provisioning Server Security Engine
Data layer	Database Third-party systems

Chapter 3: Requirements

Hardware and VMware requirements

Control Manager is available in the following configurations:

- Multi-server

When performing a new installation of Control Manager or an upgrade from a Microsoft Windows 2008 deployment, you must install new hardware or VMware servers that follow these specifications.

When performing an upgrade of Control Manager that is already on Microsoft Windows 2012, you must confirm that the current hardware or VMware servers meet these specifications.

Related links

Multi-server configuration on page 13

Multi-server configuration

The Multi-server configurations for xCaaS are known as Footprints 1, 2, and 3:

- Footprints 1 and 2 use four virtual servers, and must include the Control Manager Billing software to collect usage data. Each set of four servers must be duplicated in a Control Manager HA configuration across dual data centers.
- Footprint 3 uses two virtual servers, and must include the Usage Metering (UM) Collector software for collection of usage data. The UM Collector software with Footprint 3 is not installed on a Control Manager server, but it requires configuration data from the Control Manager system for collecting its usage data. Each set of two servers can be duplicated in a Control Manager HA configuration across dual data centers, or can use VMware HA services in a single data center.
- Footprint 3 can also be used in a lab environment to create a test two server deployment without installing UM Collector software or VMware HA. This reduced configuration cannot be used in a production environment.

Important:

For xCaaS 2.0.1.1 and earlier releases, the Control Manager Billing software was a required feature of xCaaS when using Footprints 1 or 2. For new xCaaS 2.1 and later deployments, you must use Footprint 3 with the UM Collector software. When upgrading to xCaaS 3.0 from prior releases, you can continue to use the Control Manager Billing software on Footprints 1 and 2 or you have the option to migrate to using the UM Collector software. See *Deploying*

Partner Cloud Powered by Avaya xCaaS or *Administering Partner Cloud Powered by Avaya xCaaS* for procedures to migrate to the UM Collector software.

The xCaaS configurations are available using virtualized systems only.

VMware Footprint 1 (large)

VMware Footprint 1 supports the full advertised capacity of the xCaaS solution. Footprint 1 consists of four virtual servers (logical server name in parentheses), duplicated for HA.

- Primary application server (ACM-APP-1)
- Secondary application server (ACM-APP-2)
- Primary UI server (ACM-UI-1)
- Secondary UI server (ACM-UI-2)
- Primary database server (ACM-SQL-1)
- Secondary database server (ACM-SQL-2)
- Primary billing database server (ACM-SQL-BILL-1)
- Secondary billing database server (ACM-SQL-BILL-2)

VMware Footprint 2 (small)

VMware Footprint 2 requirements can support up to 25% of the total advertised capacity of the xCaaS solution. That is, up to 5000 total concurrent Contact Center agents or 25,000 total Unified Communication users. The small footprint can also be used for a laboratory or test environment. Footprint 2 consists of four virtual servers (logical server name in parentheses), duplicated for HA:

- Primary application server (ACM-APP-1)
- Secondary application server (ACM-APP-2)
- Primary UI server (ACM-UI-1)
- Secondary UI server (ACM-UI-2)
- Primary database server (ACM-SQL-1)
- Secondary database server (ACM-SQL-2)
- Primary billing database server (ACM-SQL-BILL-1)
- Secondary billing database server (ACM-SQL-BILL-2)

VMware Footprint 3 (required for UM Collector software)

Footprint 3 is the standard Control Manager configuration used in combination with UM Collector software. It is a reduced footprint variant of Footprint 1 with the UI and Application servers consolidated in a single VMware server, but still supports the capacities of Footprint 1. Footprint 3 consists of two virtual servers (logical server name in parentheses), duplicated for HA in a dual data center or by using VMware HA in a single data center:

- Primary application server (ACM-APP-1 — includes ACM-UI-1 server capabilities)
- Secondary application server (ACM-APP-2 — includes ACM-UI-2 server capabilities)
- Primary database server (ACM-SQL-1)
- Secondary database server (ACM-SQL-2)

Note:

Footprint 3 can also be used in a lab environment to create a test two server deployment without installing UM Collector software or VMware HA. This reduced configuration cannot be used in a production environment.

Requirements for application servers (ACM-APP-1 and ACM-APP-2) — Footprints 1 and 2

The following table lists the minimum virtual machine resource requirements for the application servers in an xCaaS configuration.

Important:

The application servers must be dedicated to Control Manager software. You cannot install any other application software on this server.

VMware resource	Application Servers	
	Footprint 1	Footprint 2
vCPU Cores	4	2
Minimum CPU speed	2.4 GHz Xeon E5620 or equivalent	2.4 GHz Xeon E5620 or equivalent
Memory	16 GB	12 GB
Storage reservation	180 GB	120 GB
Shared NICs	One @ 1,000 Mbps	One @ 1,000 Mbps
Static or Dynamic resource requirements	Static	Static

Requirements for UI servers (ACM-UI-1 and ACM-UI-2) — Footprints 1 and 2

The following table lists the minimum virtual machine resource requirements for the application servers in an xCaaS configuration.

Important:

The UI servers must be dedicated to Control Manager software. You cannot install any other application software on this server.

VMware resource	UI Servers	
	Footprint 1	Footprint 2
vCPU Cores	4	2
Minimum CPU speed	2.4 GHz Xeon E5620 or equivalent	2.4 GHz Xeon E5620 or equivalent
Memory	16 GB	12 GB
Storage reservation	80 GB	50 GB
Shared NICs	One @ 1,000 Mbps	One @ 1,000 Mbps
Static or Dynamic resource requirements	Static	Static

Requirements for combined application and UI servers (ACM-APP-1 and ACM-APP-2) — Footprint 3

The following table lists the minimum virtual machine resource requirements for the combined application and UI servers in an xCaaS configuration.

Important:

The combined application/UI servers must be dedicated to Control Manager software. You cannot install any other application software on this server.

VMware resource	Combined Application and UI Servers
	Footprint 3
vCPU Cores	4
Minimum CPU speed	2.4 GHz Xeon E5620 or equivalent
Memory	16 GB
Storage reservation	200 GB
Shared NICs	One @ 1,000 Mbps
Static or Dynamic resource requirements	Static

Requirements for SQL database servers (ACM-SQL-1 and ACM-SQL-2) — All Footprints

The following table lists the minimum virtual machine resource requirements for the application servers in an xCaaS configuration.

VMware resource	SQL Database Servers		
	Footprint 1	Footprint 2	Footprint 3
vCPU Cores	4	4	4
Minimum CPU speed	2.4 GHz Xeon E5620 or equivalent	2.4 GHz Xeon E5620 or equivalent	2.4 GHz Xeon E5620 or equivalent
Memory	32 GB	16 GB	32 GB
Storage reservation	700 GB	400 GB	700 GB
Shared NICs	One @ 1,000 Mbps	One @ 1,000 Mbps	One @ 1,000 Mbps
Static or Dynamic resource requirements	Static	Static	Static

Requirements for Control Manager billing database servers (ACM-SQL-BILL–1 and ACM-SQL-BILL-2) — Footprints 1 and 2

The following table lists the minimum virtual machine resource requirements for the billing database servers in an xCaaS configuration that is using Control Manager Billing.

Important:

The billing database servers must be dedicated to Control Manager software. You cannot install any other application software on this server.

VMware resource	Control Manager Billing Database Servers	
	Footprint 1	Footprint 2
vCPU Cores	4	4
Minimum CPU speed	2.4 GHz Xeon E5620 or equivalent	2.4 GHz Xeon E5620 or equivalent
Memory	64 GB	32 GB
Storage reservation	1 TB	500 MB
Shared NICs	One @ 1,000 Mbps	One @ 1,000 Mbps
Static or Dynamic resource requirements	Static	Static

Software requirements

Customers must install specific versions of the operating system (OS), IIS software, and database software before Avaya personnel install and configure the Control Manager software.

During normal operation, users must also use specific Web browser software to access the administrative interface of Control Manager.

When performing a new installation of Control Manager, you must install new software that follow these specifications.

When performing a database migration upgrade from an older version of the Microsoft Windows Server OS, you must install new software that follow these specifications.

When performing an in-place upgrade of Control Manager that is already on Microsoft Windows 2012, you must confirm that the current software meet these specifications.

Related links

Latest software updates and patch information on page 17
Supported server operating system software requirements on page 18
Operating system considerations on page 18
Supported database server software requirements on page 18
Supported Microsoft Window OS and SQL combinations on page 21
Supported client Web browser and client operating system software requirements on page 21
Certificate requirements on page 22
Java Runtime Environment requirements on page 22

Latest software updates and patch information

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest

release notes, Product Support Notices (PSNs), and Product Correction Notices (PCNs) for the product or solution on the Avaya Support web site at http://support.avaya.com/.

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you need to download and install any updates or patches.

Supported server operating system software requirements

The customer must install one of the following Microsoft Windows server software editions on every Control Manager server in the deployment:

- Microsoft Windows Server 2012 R2 Standard Edition
- Microsoft Windows Server 2012 R2 Datacenter Edition
- Microsoft Windows Server 2016 Standard Edition
- Microsoft Windows Server 2016 Datacenter Edition

Control Manager supports English, German, and Japanese Microsoft Windows Server operating system installations. No other languages are currently supported.

Operating system considerations

Host names in server hosts file

You should add the host name and FQDN of every Control Manager server and adjunct integrated as part of the deployment to the `hosts` file of every Control Manager server. If you do this and DNS fails, the servers and adjuncts can still communicate with each other using the host name entered during installation.

IP support

Control Manager supports IPv4. Control Manager does not support IPv6.

Supported database server software requirements

The customer must install one of the following Microsoft SQL server software editions on every database server in the Control Manager deployment:

- Microsoft SQL Server 2012 Standard Edition SP4
- Microsoft SQL Server 2012 Enterprise Edition SP4
- Microsoft SQL Server 2014 Standard Edition SP2
- Microsoft SQL Server 2014 Enterprise Edition SP2
- Microsoft SQL Server 2016 Enterprise Edition SP2

Important:

When installing Microsoft SQL Server 2012 or 2014 versions, you must ensure that the software build of that version supports TLS 1.2. See the following web site for more information:

https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server

The Microsoft SQL Server software must be installed on the following host types:

- The database hosts in a Multi-server configuration

The Microsoft SQL Server software must be installed on servers that are using the Microsoft Windows Server operating system software. You cannot use any other operating system software.

Important:

The customer must agree to create a user login ID on the SQL database servers that is a member of the Sysadmin server role. This user login ID is used during installation of the Control Manager software. Create the user login ID and its password and note these items for later use. This login is used during installation only; it is not used by the application during operation.

Important:

When creating database user passwords while installing the SQL software or while upgrading the Control Manager software, the customer must agree to use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

Requirements when using a shared database

Under certain conditions, the Control Manager database may be shared with other database applications. To qualify for a shared database, you must adhere to the following requirements:

- The database names used with the shared database software must not be identical to the database names used for the Control Manager databases.
- The user names used to access the Control Manager databases must not be used in the shared database software. The following Control Manager database user names must be reserved for Control Manager:
  - ACCCM
  - ACCCMAVP
  - ACCCMSPHERE
  - ACCCMSYNC
  - UserCMSysLog
- It is the responsibility of the customer to provide a database server that has enough computing resources to handle the required performance of the Control Manager database software in addition to the shared database software. Avaya cannot make recommendations in this area since Avaya does not know what database software might be used.

- The customer must not use a server configuration smaller than the minimum configurations shown in Hardware and VMware requirements on page 13.
- Avaya cannot make recommendations concerning High Availability (HA) deployments with a shared database.
- The “sa” or “sysadmin” roles must be provided to the Control Manager installer for user and database creation.

Control Manager database collation support

The Control Manager software supports the following Windows operating systems:

- English
- German
- Japanese

Microsoft SQL Server database collation is supported for all supported user interface languages. Control Manager has been tested with the following SQL Server level collation settings:

- English (SQL_Latin1_General_CP1_CI_AS)
- German (Latin1_General_CI_AS)
- Japanese (Japanese_CI_AS)

Caution:

When upgrading from one version of SQL software to another version of SQL software, you must not change the collation settings on the new database to be different from the settings on the old database. Changing collation settings when migrating data from the old database might cause the upgrade to fail.

Use the following SQL query to determine which database collation settings are being used:

```
USE Master
 GO
 SELECT
 NAME as 'db',
 COLLATION_NAME as 'db collation name',
 (select serverproperty('collation')) as 'ms sql instance collation',
 case COLLATION_NAME when (select serverproperty('collation')) then 1 else 0 end as 'if
all 1 then upgrade '

FROM sys.Databases
 where NAME like '%ACCCM%'
 ORDER BY DATABASE_ID ASC
 GO
```

The system displays an output similar to the following:

```
ACCCM    SQL_Latin1_General_CP1_CI_AS    SQL_Latin1_General_CP1_CI_AS    1
ACCCMSYNC    SQL_Latin1_General_CP1_CI_AS    SQL_Latin1_General_CP1_CI_AS    1
ACCCMAVP    SQL_Latin1_General_CP1_CI_AS    SQL_Latin1_General_CP1_CI_AS    1
ACCCMONEXDB    SQL_Latin1_General_CP1_CI_AS    SQL_Latin1_General_CP1_CI_AS    1
ACCCMSPHEREETL    SQL_Latin1_General_CP1_CI_AS    SQL_Latin1_General_CP1_CI_AS    1
ACCCMCMSYSLOG    SQL_Latin1_General_CP1_CI_AS    SQL_Latin1_General_CP1_CI_AS    1
```

Proceed with the upgrade only if you see a “1” in the last column for all of the Control Manager. If any of the databases display a “0” in the last column, you must change the collation settings for that database.

Database engine collation should match the database collation to ensure consistency in collation used across the system.

Supported Microsoft Window OS and SQL combinations

Control Manager supports several versions of Microsoft Windows OS and Microsoft SQL software. The following combinations of OS and SQL software are supported:

- Microsoft Windows Server OS 2012 R2 and any of the supported Microsoft SQL Server 2012 SP4 editions
- Microsoft Windows Server OS 2012 R2 and any of the supported Microsoft SQL Server 2014 SP2 editions
- Microsoft Windows Server OS 2016 and any of the supported Microsoft SQL Server 2014 SP2 editions
- Microsoft Windows Server OS 2016 and any of the supported Microsoft SQL Server 2016 SP2 editions

Supported client Web browser and client operating system software requirements

The client OS used to access the Control Manager user interface must support the following client Web browsers:

- Apple Safari 10 and 11.0.1
- Google Chrome 69
- Microsoft Edge 40 and 41
- Microsoft Internet Explorer 11
- Mozilla Firefox 62

Note:

By design, Single Sign-on (SSO) functionality is available only with Internet Explorer.

You must allow pop-ups on all browsers used to access the Control Manager user interface.

Avaya recommends that you use a screen resolution of 1920 x 1080 when using the Control Manager UI. Lower screen resolutions may cause portions of the screen to not display properly.

Control Manager supports browser usage within a Citrix XenApp environment.

Certificate requirements

The Control Manager browser interface requires that the customer install signed certificates to provide secure access (HTTPS). The signed certificates can be provided by a public or private Certificate Authority (CA). To install certificates on the Control Manager servers, the servers must have access to the CA. Self-signed certificates cannot be used in a production system.

The customer must install certificates on both Control Manager UI servers (ACM-UI-1 and ACM-UI-2).

Java Runtime Environment requirements

Control Manager supports only specific versions of Java Runtime Environment (JRE). This version of Control Manager installs OpenJDK Runtime Environment (Zulu 8_30_0_2_x64, build 1.8.172, 64-bit).

Important:

Updating to an unsupported version of JRE can cause Control Manager to stop working and can require the reinstallation of the Control Manager server.

Virtualization support

Avaya Control Manager operates on the following virtualized software platforms:

- VMware vSphere ESXi 5.x
- VMware vSphere ESXi 6.0
- VMware vSphere ESXi 6.5
- IBM Bluemix IAAS offer, VMware Hypervisor option

Note:

VMware support includes VMware HA and vMotion.

Caution:

When using ESXi, ensure that the guest OS does not assign a new MAC address during startup. If the host gets a new MAC address, it could cause the Control Manager license service to not start and access to the Control Manager might fail.

Caution:

Control Manager software is not currently distributed using an Open Virtualization Archive (OVA) file. Any older OVA files must be discarded and not used to install Control Manager

software. Verify that you have downloaded the latest version of Control Manager software, which is provided as an ISO download.

Amazon Web Services support

Control Manager supports installation on Amazon Web Services (AWS). Support for AWS is limited to Elastic Compute Cloud (EC2)-hosted application and database servers, with the SQL database server being separately installed on an EC2 instance. The AWS Relational Database Service (RDS)-based SQL server is not supported because of restrictions imposed by AWS RDS. The EC2 virtual machine selected should have a resource footprint equal to or greater than the hardware and VMware requirements published for Control Manager.

Getting Control Manager licenses

About this task

You must get new licenses for Control Manager under the following conditions:

- New installations.
- When upgrading (migrating) from any Release 7.x system.

You do not have to get a new license when upgrading from one version of 8.0.x to another version of 8.0.x.

Licenses for Control Manager software can be installed at the same time you install the Control Manager software. However, if you do not have a license file when you install the Control Manager software, you must install the license file after you install the Control Manager software before the system will be operational. Without valid license files, the license service will not start and no users will be able to log on to the Control Manager user interface.

Procedure

1. Log on to the server(s) shown in the table below.
2. Go to **Start** > **Run**.
3. Run the command **`getmac`** and press **Enter**.
4. Record the MAC IDs in the following table:

   Important:

   If the server has multiple NICs (Ethernet ports), you must get the MAC IDs for all NICs on the server and submit those MAC IDs when you request a license file. Also, the License services must have full access to the license file.. That is, the file must be readable by the user that is running the Control Manager License services.

Application Server	MAC IDs
ACM-APP-1	
ACM-APP-2	
ACM-UI-1	
ACM-UI-2	

5. Email the MAC IDs to licenseadmin@avaya.com to get the Control Manager licenses.
6. After you receive the license files, put them in a secure place until you install the Control Manager software.

Important:

The license file must be named `license.lic`.

Chapter 4: Reference configurations

Reference configurations for xCaaS deployments

xCaaS supports two different HA configurations:

- The HA configuration used with Usage Metering (UM) Collector uses the features of VMware HA in a single data center setup.
- The Control Manager HA reference configuration used with Control Manager Billing uses two identical Control Manager deployments that operate in an Active/Active mode.

Note:

Active/Active refers to the deployment of Control Manager servers in an HA setup. Both of the Control Manager instances are active and either one can be used.

There are three virtual server configurations available with xCaaS:

- Footprint 1
- Footprint 2
- Footprint 3

In Footprints 1 and 2, the primary UI and application servers represent the primary application logical layer. The secondary UI and application servers represent the secondary application logical layer. There are two Control Manager Microsoft SQL Server database servers (ACM-SQL-1/ACM-SQL-2) deployed in an Active/Active mode, and two billing database Microsoft SQL Server servers (ACM-SQL-BILL-1 and ACM-SQL-BILL-2) deployed in an Active/Active mode.

Footprints 1 and 2 consist of the following servers:

- Primary UI server (ACM-UI-1), primary application server (ACM-APP-1), primary database server (ACM-SQL-1), and primary billing database server (ACM-SQL-BILL-1) installed on four virtual machines.
- Secondary UI server (ACM-UI-2), secondary application server (ACM-APP-2), secondary database server (ACM-SQL-2), and secondary billing database server (ACM-SQL-BILL-2) installed on four virtual machines.
- Control Manager software is installed on the primary UI server (ACM-UI-1), primary application server (ACM-APP-1), secondary UI server (ACM-UI-2), and secondary application server (ACM-APP-2).

In Footprint 3, there are two ways to deploy with HA:

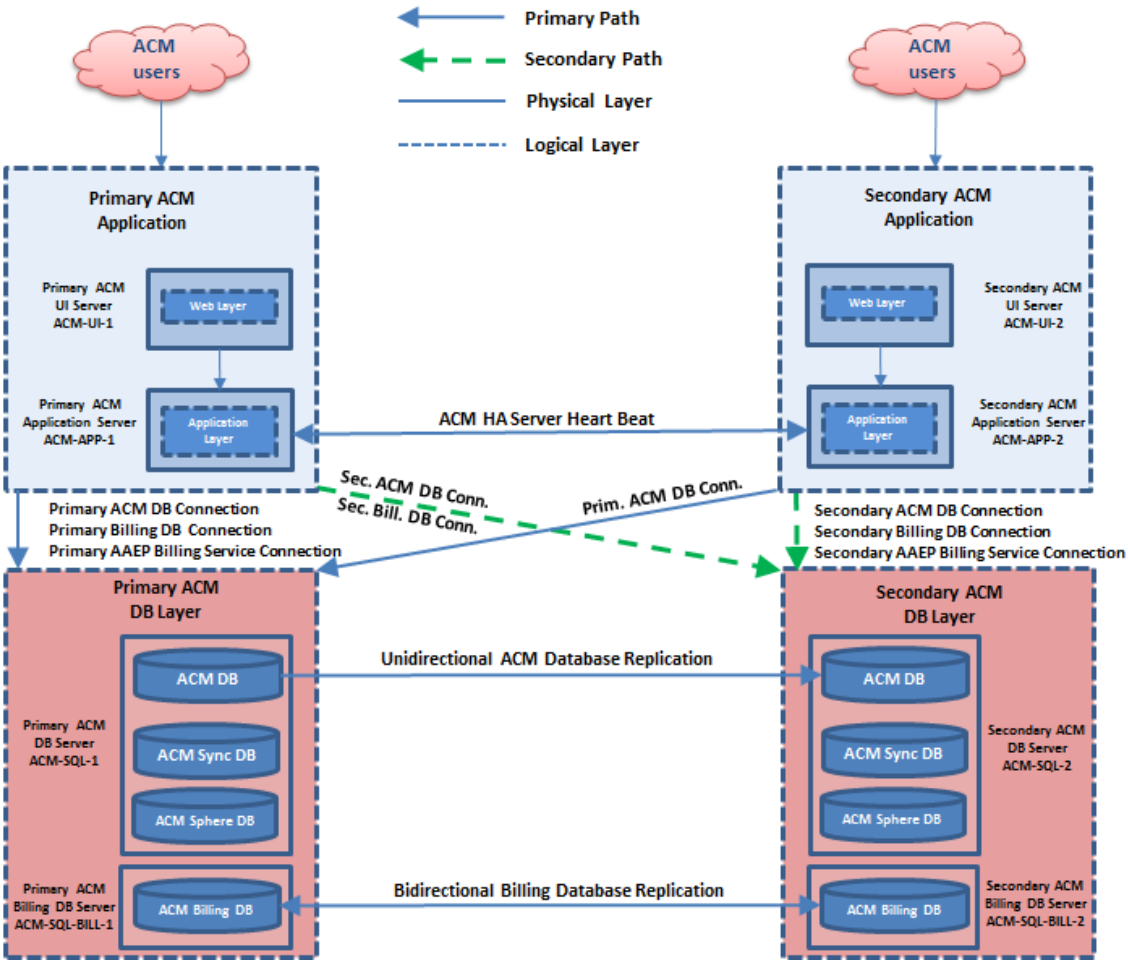
- xCaaS deployments that use Usage Metering (UM) Collector software support single data center deployments using the HA features of VMware. You would deploy a single Control Manager system using xCaaS. There will be no Control Manager failover since there is only one set of servers. Any failover is handled by VMware HA. For more information, see VMware HA documentation.
- For the more traditional HA configuration, the primary application server represents the primary application and UI logical layer. The secondary application server represents the secondary application and UI logical layer. There are two Control Manager Microsoft SQL Server database servers (ACM-SQL-1/ACM-SQL-2) deployed in an Active/Active mode.

Footprint 3 consists of the following servers:

- Primary application/UI server (ACM-APP-1), primary database server (ACM-SQL-1), and primary billing database server (ACM-SQL-BILL-1) installed on three virtual machines.
- Secondary application/UI server (ACM-APP-2), secondary database server (ACM-SQL-2), and secondary billing database server (ACM-SQL-BILL-2) installed on three virtual machines.

Note:

Footprint 3 can also be used in a lab environment to create a test two server deployment without installing UM Collector software or VMware HA. This reduced configuration cannot be used in a production environment.



One of the Control Manager systems is designated as the Primary and the other as the Secondary. Both Control Manager systems are completely active and work in parallel, and both of them provide service simultaneously to administration users.

In an HA configuration, a data center or database failure can initiate a failover if the following conditions are met:

- The primary and secondary Control Manager UI and application servers are in a running state.
- HA is enabled on the Control Manager UI and services servers.
- The Control Manager primary database server and secondary database server are synchronized using unidirectional replication.
- The Control Manager primary billing database server and secondary billing database server are synchronized using bidirectional replication.

Deployment considerations for a single data center

Control Manager HA leverages the transactional replication feature that is available in Microsoft SQL Standard Edition or Enterprise Edition server software. This means is that, under normal operating conditions, any change to any of the defined databases (ACM-SQL-1) will be automatically pushed out to the corresponding database (ACM-SQL-2). The same applies in reverse. Any change made on the ACM-SQL-2 databases will result in an automated update to the corresponding ACM-SQL-1 database.

In a basic Control Manager HA deployment, the primary and secondary Control Manager systems are located in a single data center. Both the primary and secondary Control Manager systems in an HA environment have identical configurations, providing the full Control Manager capabilities.

xCaaS deployments that use Usage Metering (UM) Collector software support single data center deployments using the HA features of VMware. You would deploy a single Control Manager system using xCaaS. There will be no Control Manager failover since there is only one set of servers. Any failover is handled by VMware HA. For more information, see VMware HA documentation.

Note:

Footprint 3 can also be used in a lab environment to create a test two server deployment without installing UM Collector software or VMware HA. This reduced configuration cannot be used in a production environment.

Deployment considerations in a dual data center or disaster recovery configuration

Note:

Dual data centers are also known as Geo-Redundant data centers.

Control Manager HA leverages the transactional replication feature that is available in Microsoft SQL Standard Edition or Enterprise Edition server software. This means is that, under normal operating conditions, any change to any of the defined databases (ACM-SQL-1) will be automatically pushed out to the corresponding database (ACM-SQL-2). However, the same does not apply in reverse. Any change made on the ACM-SQL-2 databases must be manually updated on the corresponding ACM-SQL-1 database.

In a standard xCaaS dual data center HA configuration, the Control Manager primary database server and secondary database server are synchronized using unidirectional replication.

Using HA eliminates the need to manually duplicate the administration of a secondary system. The systems can be within the data center or over a WAN.

Both the primary and secondary Control Manager Systems in an HA configuration have identical deployments, providing full Control Manager capabilities.

High Availability is available with a single data center or a dual data center. However, for a dual data center, the following network configuration must be in place:

- Equal to or greater than 1 Gbps bandwidth.
- Reliable network (no application level handling of network disconnects is provided).
- Latency:
  - Less than or equal to 50 ms — Recommended.
  - 50–100 ms — Some delays in navigation and simple operations. Complex operations, like editing or saving SIP users that traverse multiple systems, may take substantially longer.
  - 100–150 ms — Further performance degradation possible.

This latency information is provided as guidance. Actual performance will depend on the actual network latency between Control Manager and the databases, between the HA database pair, and between Control Manager and the managed systems.

Requirements for HA deployments

To prevent failure in the data replication, ensure that the following requirements are met for deploying Control Manager in an Active/Active HA configuration:

Caution:

Host names of Control Manager application and UI servers must only contain alphabetic letters and numbers and are limited to a length of 15 characters. Host names cannot contain any special characters, such as hyphens (-) or underscores (_). Confirm that you are using a valid host name before you install the Control Manager software because you cannot change the host name after installing the Control Manager software.

Host names of Control Manager database servers must follow the requirements set forth by Microsoft in the following article:

https://support.microsoft.com/en-us/help/909264/

- For the supported HA deployments, the Control Manager functional components – Web Server, Application Server, and Provisioning Server – are installed on different servers. On a Multiple host configuration, the Web Server component is installed on a dedicated server (ACM-UI-1 and ACM-UI-2), and the Application Server and Provisioning Server components are installed on another server (ACM-APP-1 and ACM-APP-2).
- Control Manager HA is available only if the servers are installed using Microsoft SQL Standard Edition or Enterprise Edition Server software.
- The Control Manager software version must be identical on both the primary and secondary application servers.

- You have designated the primary and the secondary systems.
- Control Manager application servers work in parallel and communicate with the SQL servers in an Active/Active setup.
- In an Active/Active deployment, Control Manager servers ACM-APP-1 (primary) and ACM-APP-2 (secondary) use ACM-SQL-1 as their primary Control Manager SQL database.
- Control Manager HA must be configured only in a 1+1 configuration.
- Both the primary and secondary Control Managerapplication servers must have the same hardware configuration.
- Both systems must be connected to the same sources. For example, the secondary system must be connected to the same Communication Manager system as the primary.
- Both the primary and secondary systems must have SNMP alarming administered so that alarms are sent from either system.

Databases installed

In a Control Manager installation, the following Control Manager databases are installed by default:

Database	Description	Located on server
ACCCM	Stores the Control Manager system configuration.	ACM-SQL-1, ACM-SQL-2
ACCCMAVP	Stores the Experience Portal database. **Note:** This database is installed but not used in xCaaS.	ACM-SQL-1, ACM-SQL-2
ACCCMSYNC	Synchronizes the database between Communication Manager and Control Manager.	ACM-SQL-1, ACM-SQL-2
ACM_BILLING or ACCCMBilling	Stores the Control Manager database.	ACM-APP-1, ACM-APP-2, ACM-SQL-BILL-1, ACM-SQL-BILL-2

Important:

This document uses the database names ACM_BILLING and ACCCMBilling. If the system has been upgraded from a previous version, the database name is probably named ACCCMBilling. Regardless of which name is being used, ensure that you use the correct database name within these procedures.

Each Control Manager instance is working with the primary Control Manager database layer. The primary database server (ACM-SQL-1) for Application and the primary billing database server

(ACM-SQL-BILL-1) for Billing. The primary database server (ACM-SQL-1) is replicated using a unidirectional replication mechanism with the secondary database server (ACM-SQL-2). The primary billing database server (ACM-SQL-BILL-1) is replicated using a bidirectional replication mechanism with the secondary billing database server (ACM-SQL-BILL-2).

Deploying Control Manager using a virtual IP address and optional Network Load Balancer

Control Manager supports the Active/Active HA mode with a virtual IP address. The virtual IP address balances the users between the two Control Manager instances through an optional external customer-supplied Network Load Balancer (NLB).

Note:

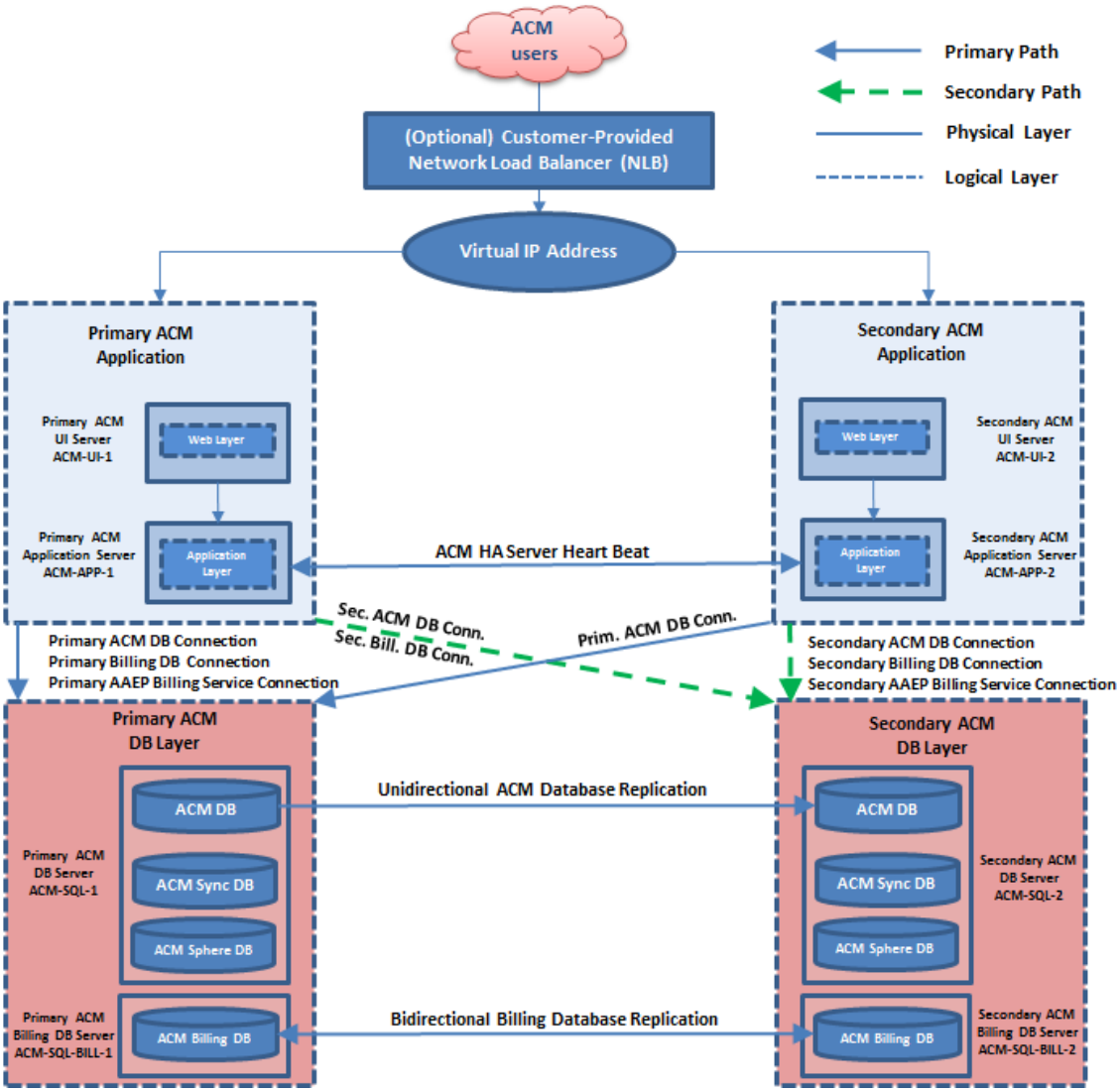
Avaya makes no recommendations concerning NLBs. Customers must provide consultants to Avaya personnel when implementing an NLB in the deployment.

Depending on the NLB you plan to use, ensure that it maintains session persistence.

With an HA deployment, two instances of Control Manager are installed with one instance defined as the primary Control Manager and another instance defined as a secondary Control Manager.

A single IP address is used to connect to either of the Control Manager deployments. If the primary Control Manager stops, the virtual IP address will be automatically assigned to the secondary Control Manager.

The following graphic shows an overview of the Control Manager HA solution mode deployed with a Virtual IP address.



Deploying Control Manager using dedicated IP addresses

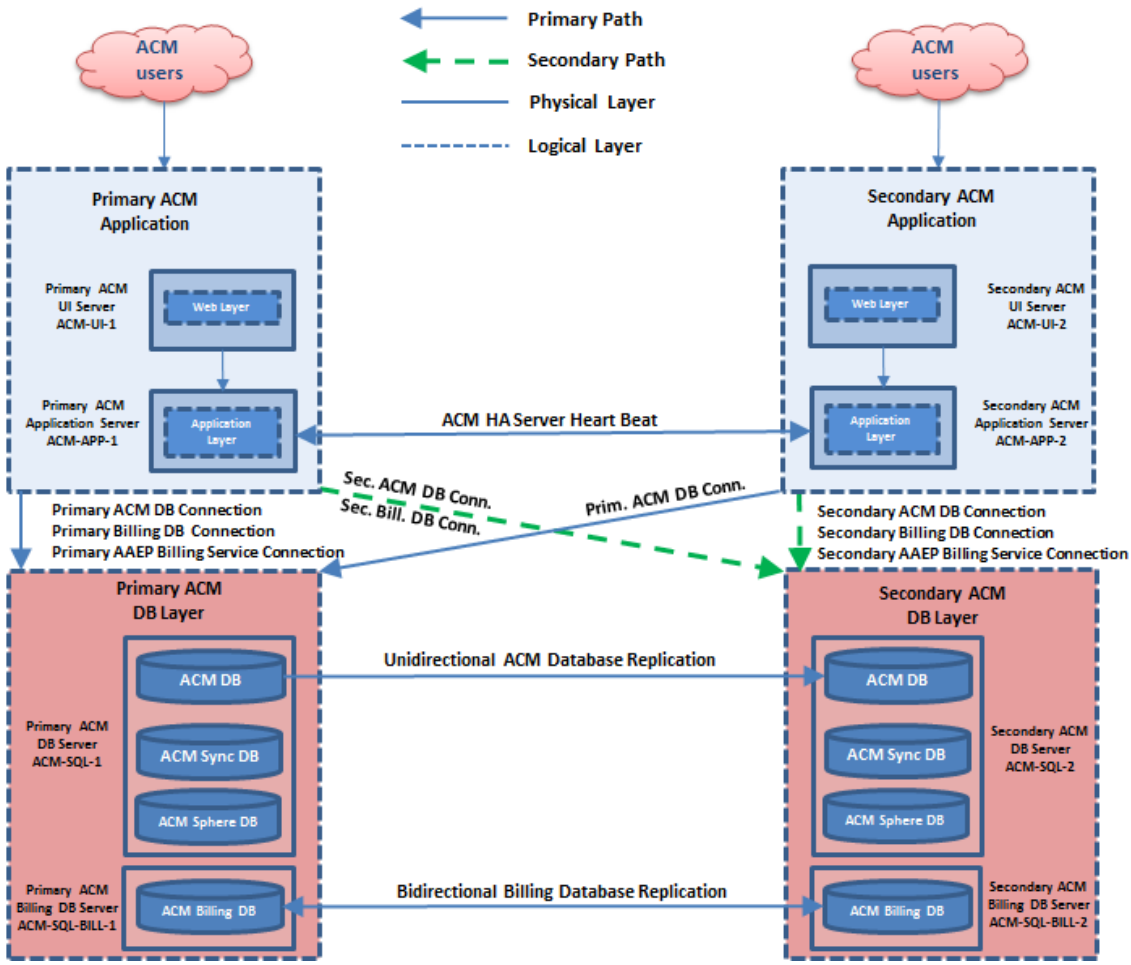
Control Manager supports an Active/Active HA configuration with a dedicated IP address. With a dedicated IP address, two instances of Control Manager are installed each with a unique IP address. Both instances are completely active and are working in parallel.

With dedicated IP addresses, users can browse to a dedicated IP address for each server, allowing users to decide which instance of Control Manager to use where every instance is running a full set of Control Manager application layer services.

Each Control Manager instance works with the primary Control Manager database layer (ACM-SQL-1), which is replicated using a replication mechanism with the secondary Control Manager

database instance (ACM-SQL-2). Every change that is made on one of the Control Manager instances is synced between all the other instances of Control Manager within the environment.

The following graphic shows an overview of the Control Manager HA configuration deployed with a dedicated IP address.



About replication

Important:

When deploying xCaaS with Usage Metering (UM) Collector software and the VMware HA feature, you can skip this information about replication.

Control Manager HA uses the transactional replication with updateable subscriptions feature that is available in Microsoft SQL Server software. This means is that under normal operating conditions, any change to the defined databases on the primary database server (ACM-SQL-1) will be automatically pushed out to the secondary database server (ACM-SQL-2). However, since

unidirectional replication is used, any change made on the secondary database server (ACM-SQL-2) must be manually updated on the primary database server (ACM-SQL-1).

Per the reference architecture, the database primary connection path for ACM-APP-1 and ACM-APP-2 is to point to the same ACM-SQL-1 database server. The secondary connection path for ACM-APP-1 is to point to ACM-SQL-2.

Per the reference architecture, the database primary connection path for ACM-UI-1 and ACM-UI-2 is to point to the same ACM-SQL-1 database server. The secondary connection path for ACM-UI-1 is to point to ACM-SQL-2.

Within a Control Manager HA environment, each Control Manager instance is working with a dedicated database layer. The two Microsoft SQL database servers (ACM-SQL-1/ACM-SQL-2) host the following databases and are set up for transactional database replication.

The following table illustrates the replication strategy for each of the SQL databases that Control Manager HA supports in a dual data center.

Database	Replication	Direction
ACCCM	Transactional	Unidirectional (DC 1 to DC 2 only)
ACCCMCMSYSLOG	Transactional	Bidirectional
ACM_BILLING	Transactional	Bidirectional
ACCCMSYNC	Transactional	Bidirectional

Important:

This document uses both database names ACM_BILLING and ACCCMBilling. If the system has been upgraded from a previous version, the database name is probably named ACCCMBilling. Regardless of which name is being used, ensure that you use the correct database name within these procedures.

Note:

The following table lists which database tables within the Control Manager databases do not replicate:

Control Manager Database	Database Tables
ACCCM	[Audit_Log_Service_Temp_InsertSource_Audit] [CMAuditLogs_Temp] [Extensions_Details_Temp] [Extensions_Temp] Log_Messages [Skills_Temp]

Table continues…

Control Manager Database	Database Tables
	[tmp_License_Usage_Tracker_History] [tmp_Traffic_Measure_Occupancy_History] [tmp_Traffic_Measure_Trunks_History] [VDNs_Temp]
ACM_BILLING or ACCCMBilling	Configured_Stations vpapplog cdr tblProfileUsagePerLocationPerSiteMonthly_ProfilePivotConfiguration tblProfileUsagePerLocationPerSiteMonthly_ProfilePivot Agent_Ranges tblProfileUsagePerLocationPerSiteByHour tblProfileUsagePerLocationByHour tblPreProcAction t_sdr Staffed_Agents sdr RptPickLicenseWeeklyLocation RptPickLicenseWeekly RptPickLicenseMonthlyLocation RptPickLicenseMonthly RptPickLicenseDaily Rpt_PeakAaepUsageByMin Rpt_PeakAaepUsageByDay Registered_Stations PickLicense5MinLocation PickLicense5Min Locations_CM_Servers Locations License_Usage_Tracker_History Extension_Ranges Dial_Plans vpperformance

Table continues…

Control Manager Database	Database Tables
ACCCMCMSYSLOG	CM_Syslog_RawMessages_Temp

Switchover and Failover methods

Important:

When deploying xCaaS with Usage Metering (UM) Collector software and the VMware HA feature, you can skip this information about switchover and failover.

The primary purpose of HA is to ensure an uninterrupted data stream between Control Manager and the associated Avaya applications. There are two methods for system switchover and failover:

Method	Description
Manual Switchover	Switches the role between the primary and secondary components. This switchover type is typically used for planned maintenance activities. Alternatively, you can manually switchover if a failure on a primary component is not detected automatically.
Automatic Failover	Automatic Failover is a process that enables the secondary components to automatically take over the role of the primary components in the event of a failure detected on the primary components. Automatic Failover provides uninterrupted access to the system during a failure. HA uses the HA Service (Heartbeat) to ensure automatic failover and does not need manual switchover.

Chapter 5: Worksheets

Server worksheet — Multiple host configurations

Footprints 1 and 2

Use the following table to track the host names and IP addresses for the different servers.

Caution:

Host names of Control Manager application and UI servers must only contain alphabetic letters and numbers and are limited to a length of 15 characters. Host names cannot contain any special characters, such as hyphens (-) or underscores (_). Confirm that you are using a valid host name before you install the Control Manager software because you cannot change the host name after installing the Control Manager software.

Host names of Control Manager database servers must follow the requirements set forth by Microsoft in the following article:

https://support.microsoft.com/en-us/help/909264/

Server	Logical label	Host name	IPv4 address
Primary application server	ACM-APP-1		
Secondary application server	ACM-APP-2		
Primary UI server	ACM-UI-1		
Secondary UI server	ACM-UI-2		
Primary database server	ACM-SQL-1		
Secondary database server	ACM-SQL-2		
Primary billing database server	ACM-SQL-BILL-1		
Secondary billing database server	ACM-SQL-BILL-2		

Footprint 3

Use the following table to track the host names and IP addresses for the different servers.

Caution:

Host names of Control Manager application and UI servers must only contain alphabetic letters and numbers and are limited to a length of 15 characters. Host names cannot contain any special characters, such as hyphens (-) or underscores (_). Confirm that you are using a valid host name before you install the Control Manager software because you cannot change the host name after installing the Control Manager software.

Host names of Control Manager database servers must follow the requirements set forth by Microsoft in the following article:

https://support.microsoft.com/en-us/help/909264/

Server	Logical label	Host name	IPv4 address
Primary application server	ACM-APP-1		
Secondary application server (not used with VMware HA or in lab test environment)	ACM-APP-2		
Primary database server	ACM-SQL-1		
Secondary database server (not used with VMware HA or in lab test environment)	ACM-SQL-2		

Chapter 6: Installing prerequisite software

Software installation prerequisites for the customer

Upgrades from Control Manager Releases 7.1.2.2 or 7.1.101

For an upgrade from Control Manager Release 7.1.2.2, the customer must install the software shown in the following list and in this chapter. The installation of prerequisite software must be done on a new set of servers before Avaya personnel migrate the data from the old system, upgrade the Control Manager software, and configure the Control Manager software.

- Install the Microsoft Windows operating system on all servers in the deployment. After installing the operating system, run the Microsoft Windows Update program to install any recent updates to the core software. See the software requirements for more information about the different supported server operating systems.

  Caution:

  Host names of Control Manager application and UI servers must only contain alphabetic letters and numbers and are limited to a length of 15 characters. Host names cannot contain any special characters, such as hyphens (-) or underscores (_). Confirm that you are using a valid host name before you install the Control Manager software because you cannot change the host name after installing the Control Manager software.

  Host names of Control Manager database servers must follow the requirements set forth by Microsoft in the following article:

  https://support.microsoft.com/en-us/help/909264/

- Install and configure Microsoft Internet Information Services (IIS) for the Web server component. This software must be installed on the servers noted in Installing and configuring IIS on the Microsoft Windows Server 2012 OS on page 41 or Installing and configuring IIS on the Microsoft Windows Server 2016 OS on page 46.
- The Microsoft SQL Server software must be installed on the database hosts in a Multi-server deployment.
- Certificates must be installed on the application hosts in a Multi-server deployment.

Upgrades from Control Manager Release 8.0.x and when upgrading the Microsoft OS and SQL software

For an upgrade from Control Manager Release 8.0.x when you are also upgrading the Microsoft Windows Server OS and the Microsoft SQL Server software, the customer must install the software shown in the following list and in this chapter. The installation of prerequisite software

must be done on a new set of servers before Avaya personnel migrate the data from the old system, upgrade the Control Manager software, and configure the Control Manager software.

- Install the Microsoft Windows operating system on all servers in the deployment. After installing the operating system, run the Microsoft Windows Update program to install any recent updates to the core software. See the software requirements for more information about the different supported server operating systems.

  Caution:

  Host names of Control Manager application and UI servers must only contain alphabetic letters and numbers and are limited to a length of 15 characters. Host names cannot contain any special characters, such as hyphens (-) or underscores (_). Confirm that you are using a valid host name before you install the Control Manager software because you cannot change the host name after installing the Control Manager software.

  Host names of Control Manager database servers must follow the requirements set forth by Microsoft in the following article:

  https://support.microsoft.com/en-us/help/909264/

- Install and configure Microsoft Internet Information Services (IIS) for the Web server component. This software must be installed on the servers noted in Installing and configuring IIS on the Microsoft Windows Server 2012 OS on page 41 or Installing and configuring IIS on the Microsoft Windows Server 2016 OS on page 46.
- The Microsoft SQL Server software must be installed on the database hosts in a Multi-server deployment.
- Certificates must be installed on the application hosts in a Multi-server deployment.

Upgrades from 8.0.x.x when not upgrading the Microsoft OS and SQL software

For an upgrade from Control Manager Release 8.0.x.x when not upgrading the Microsoft OS and SQL software, the customer must do the following:

- Confirm that the software shown in this chapter is installed and working on the current set of Control Manager servers.
- If the current system is on Microsoft Windows 2012 (not 2012 R2), the customer must upgrade to Microsoft Windows OS 2012 R2 software as described in Upgrading Windows 2012 to Windows 2012 R2 on page 65.
- The customer must check the Java version and correct any incompatibility with the Java version. The customer must remove any unsupported versions, if present.

Installing and configuring IIS on the Microsoft Windows Server 2012 OS

About this task

The customer must install the Microsoft IIS software on the following Control Manager servers depending on your configuration:

- In a full xCaaS four-server configuration, you must install the IIS software on the Web UI servers (ACM-UI-1 and ACM-UI-2).
- In a reduced xCaaS two- or three-server configuration where the Control Manager software and the Web server software is on the same server, you must install the IIS software on the application servers (ACM-APP-1 and ACM-APP-2).

The Microsoft .NET Version 4.7 or later software is required for Control Manager. As part of installing IIS, you must determine whether .NET 4.7 or later is installed on the servers where you installed IIS. This process is detailed in this procedure, including how to download .NET 4.7 or later and how to install .NET 4.7 or later if it is not already installed.

Important:

You must install the Microsoft .NET patches to pick up the latest security fixes.

Before you begin

Have the operating system media available in case you must install specific software from the operating system for IIS.

Procedure

1. On the server desktop, click **Server Manager > Dashboard**.

   The system displays the WELCOME TO SERVER MANAGER screen.

2. Click **Add Roles and features**.

   The system displays the Before you begin screen.

3. Click **Next**.

   The system displays the Select installation type screen. Confirm that the default selection is **Role-based or feature-based installation**.

4. Click **Next**.

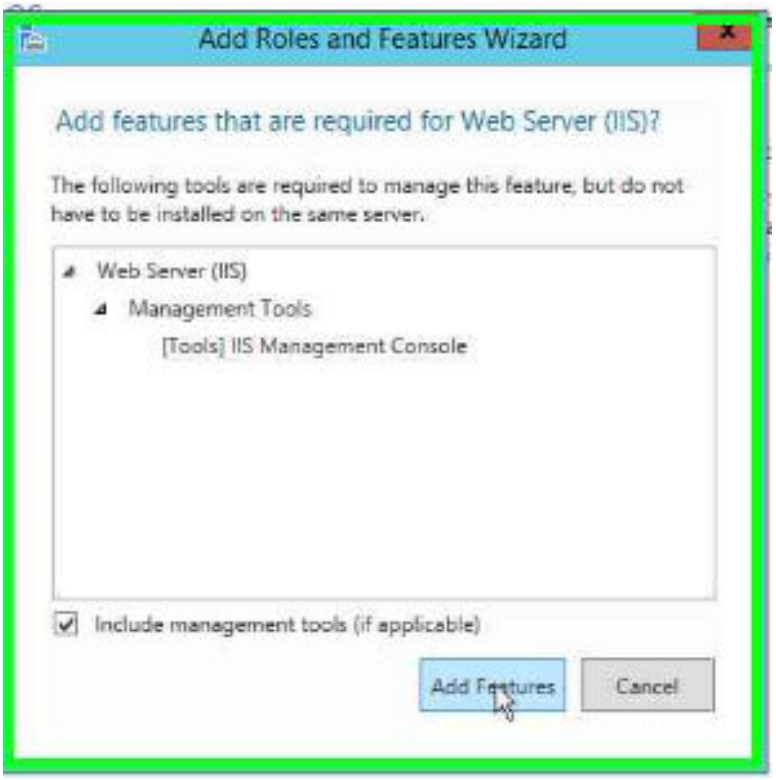
   The system displays the Select destination server screen. Confirm that the default selection is **Select a server from the server pool**.

5. Click **Next**.

   The system displays the Select server roles screen.

6. Select **Application Server** and **Web Server IIS**.

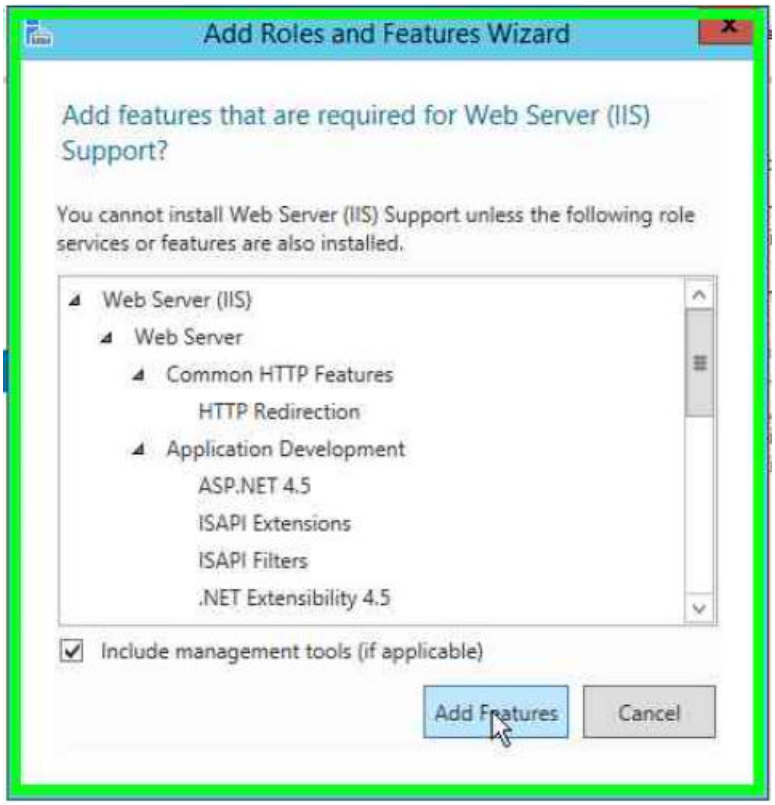
   After selecting the **Web Server IIS** option, the system displays the following screen:



7. Click **Add Features**.
8. Click **Next**.

   The system displays the Select features screen.
9. Select the following features:
   - **.NET Framework 3.5 Features**
   - **.NET Framework 4.5 Features (2 of 7 installed)** > **ASP.NET 4.5**
10. Click **Next** twice until you get to the Application Server > Role Services screen under Select role services.
11. Select **Web Server IIS**.

    After selecting the **Web Server IIS** option, the system displays the following screen:



12. Click **Add Features**.
13. Click **Next**.

    The system displays the Web Server Role (IIS) screen.
14. Click **Next**.

    The system displays the Web Server Type (IIS) > Role Services screen.
15. Confirm that the following options are selected by scrolling through all of the available options. Select any options that are not selected by default.

    Note:

    If an Add Features screen is displayed at any time, click **Add Features** to continue with the feature selection process.

    - Web Server
    - Common HTTP Features
      - Default Document
      - Directory Browsing
      - HTTP Errors
      - Static Content

  - HTTP Redirection
- Health and Diagnostics
  - HTTP Logging
  - Logging Tools
  - Request Monitor
  - Tracing
- Performance
  - Static Content Compression
- Security
  - Request Filtering
  - Basic Authentication
  - Client Certificate Mapping Authentication
  - Digest Authentication
  - IIS Client Certificate Mapping Authentication
  - IP and Domain Restrictions
  - URL Authorization
  - Windows Authentication
- Application Development
  - .NET Extensibility 3.5
  - .NET Extensibility 4.5
  - Application Initialization
  - ASP.NET 3.5
  - ASP.NET 4.5
  - CGI
  - ISAPI Extensions
  - ISAPI Filters
  - Server Side Includes
  - WebSocket Protocol
- Management Tools
  - IIS Management Console
  - IIS Management Compatibility
    - IIS 6 Metabase Compatibility

    - IIS 6 Management Console
    - IIS 6 Scripting Tools
    - IIS 6 WMI Compatibility
  - IIS Management Scripts and Tools

16. Click **Install**.
17. When the installation is complete, click **Close**.
18. Reboot the server before installing any other software.
19. Perform the following steps to confirm whether .NET 4.7 or later is installed on the server and install the software if it is not installed:
    a. Log on to the Windows OS.
    b. Navigate to **Start** > **Run**.
    c. In the Open screen, enter **`regedit.exe`**.
    d. In the registry editor, open the following subkey:

       `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP \v4\Full`

    e. Check the **Release** value. The value that indicates .NET 4.7 is 460805. If this value is shown, you can skip the rest of this procedure. If that value is not shown, you must continue with this procedure and manually install .NET 4.7 or later.
    f. Navigate to the Microsoft Download center and search for the “Microsoft .NET Framework 4.7” installation program.
    g. Right-click the downloaded installation file and select **Run as administrator**.
    h. Agree to the license terms and install the software.
20. Repeat this procedure on any other servers that require the IIS software.

Next steps

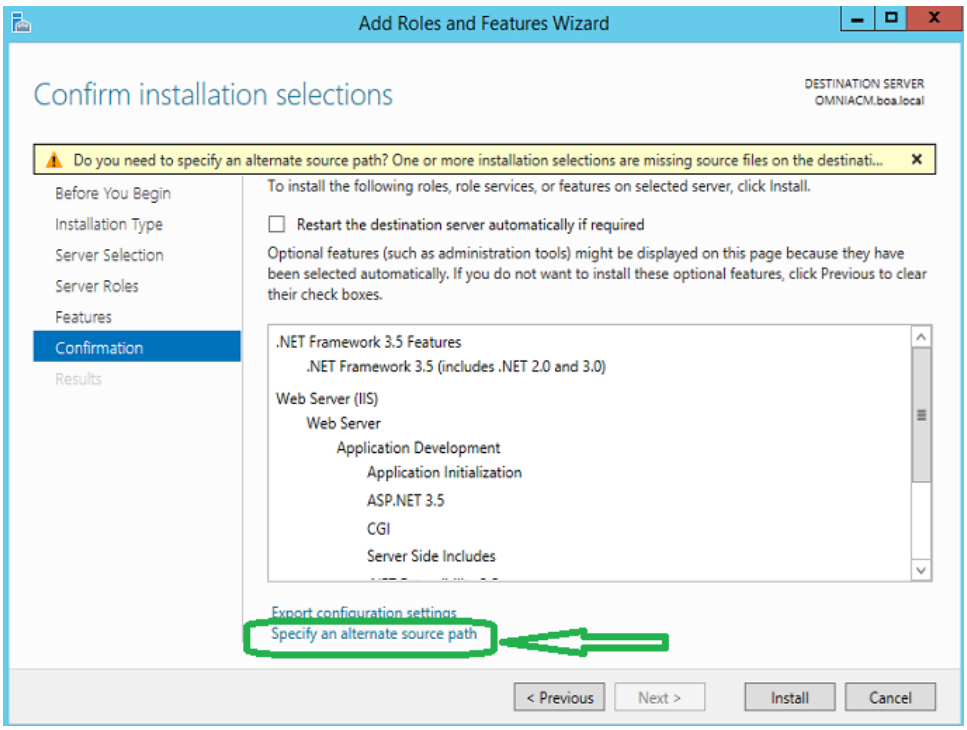
Important:

You must install the Microsoft .NET patches to pick up the latest security fixes.

When installing the Microsoft Windows Server OS for a new installation or for an upgrade from Microsoft Windows 2008, verify that you install the ASP.Net 3.5 role and the ASP.Net 4.5 role using the Microsoft Windows Server OS installation software disc or downloaded ISO image. When installing the roles, you must specify an alternate source path. The alternate source path is:

```
<Windows_Source>\sources\sxs
```

Use the **Specify an alternate source path** option as shown on the IIS installation screens in the following example:



Transport Layer Security (TLS) 1.2 and 1.1 are installed automatically when you install the IIS software. After you install the IIS software, you must disable TLS 1.0 per Avaya security requirements if it still exists on the system.

You can manually disable TLS 1.0 by editing the registry on every server where you installed IIS. Use the article found at the following web site, which explains how to edit the registry and disable TLS 1.0 and 1.1:

https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings

Installing and configuring IIS on the Microsoft Windows Server 2016 OS

About this task

The customer must install the Microsoft IIS software on the following Control Manager servers depending on your configuration:

- In a full xCaaS four-server configuration, you must install the IIS software on the Web UI servers (ACM-UI-1 and ACM-UI-2).
- In a reduced xCaaS two- or three-server configuration where the Control Manager software and the Web server software is on the same server, you must install the IIS software on the application servers (ACM-APP-1 and ACM-APP-2).

The Microsoft .NET Version 4.7 or later software is required for Control Manager. As part of installing IIS, you must determine whether .NET 4.7 or later is installed on the servers where you

installed IIS. This process is detailed in this procedure, including how to download .NET 4.7 or later and how to install .NET 4.7 or later if it is not already installed.

Important:

You must install the Microsoft .NET patches to pick up the latest security fixes.

Before you begin

Have the operating system media available in case you must install specific software from the operating system for IIS.

Procedure

1. On the server desktop, click **Server Manager > Dashboard**.

   The system displays the WELCOME TO SERVER MANAGER screen.

2. Click **Add Roles and features**.

   The system displays the Before you begin screen.

3. Click **Next**.

   The system displays the Select installation type screen. Confirm that the default selection is **Role-based or feature-based installation**.

4. Click **Next**.

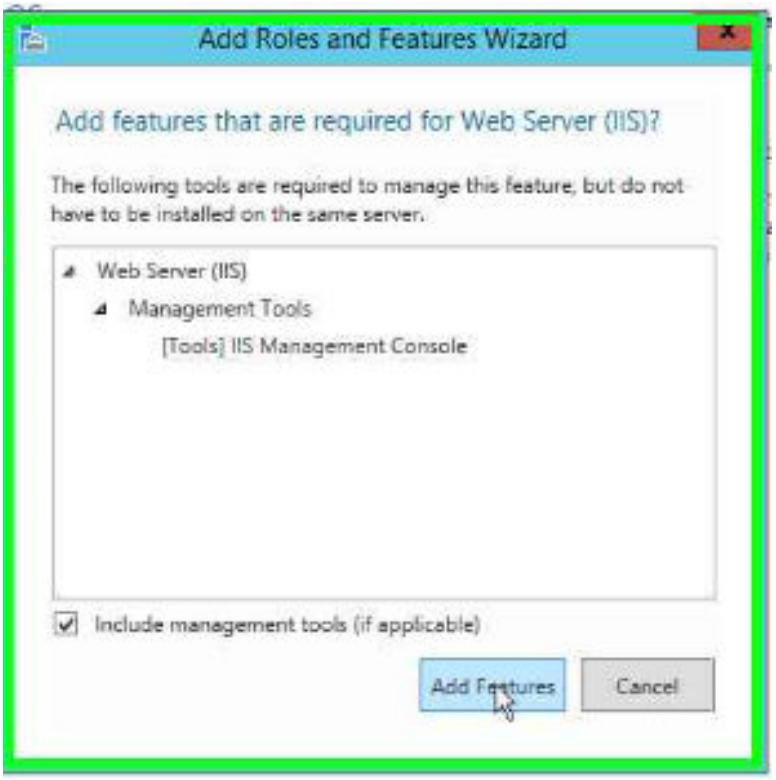
   The system displays the Select destination server screen. Confirm that the default selection is **Select a server from the server pool** and that the **Server Pool** list has the server where you are installing IIS.

5. Click **Next**.

   The system displays the Select server roles screen.

6. Select **Web Server (IIS)**.

   The system displays the following screen:



7. Click **Add Features**.
8. Click **Next**.

   The system displays the Select features screen.
9. Select the following features:
   - **.NET Framework 3.5 Features** > **.NET Framework 3.5 (includesNET 2.0 and 3.0)**
   - **.NET Framework 4.6 Features (2 of 7 installed)** > **ASP.NET 4.6**
10. Click **Next**.

    The system displays the Web Server Role (IIS) screen.
11. Click **Next**.

    The system displays the Web Server Type (IIS) > Role Services screen.
12. Confirm that the following options are selected by scrolling through all of the available options. Select any options that are not selected by default.

    Note:

    If an Add Features screen is displayed at any time, click **Add Features** to continue with the feature selection process.

    - Web Server

- Common HTTP Features
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - Static Content
  - HTTP Redirection
- Health and Diagnostics
  - HTTP Logging
  - Logging Tools
  - Request Monitor
  - Tracing
- Performance
  - Static Content Compression
- Security
  - Request Filtering
  - Basic Authentication
  - Client Certificate Mapping Authentication
  - Digest Authentication
  - IIS Client Certificate Mapping Authentication
  - IP and Domain Restrictions
  - URL Authorization
  - Windows Authentication
- Application Development
  - .NET Extensibility 3.5
  - .NET Extensibility 4.5
  - Application Initialization
  - ASP.NET 3.5
  - ASP.NET 4.5
  - CGI
  - ISAPI Extensions
  - ISAPI Filters
  - Server Side Includes

- WebSocket Protocol
- Management Tools
  - IIS Management Console
  - IIS Management Compatibility
    - IIS 6 Metabase Compatibility
    - IIS 6 Management Console
    - IIS 6 Scripting Tools
    - IIS 6 WMI Compatibility
- IIS Management Scripts and Tools

13. Click **Install**.
14. When the installation is complete, click **Close**.
15. Reboot the server before installing any other software.
16. Perform the following steps to confirm whether .NET 4.7 or later is installed on the server and install the software if it is not installed:
    a. Log on to the Windows OS.
    b. Navigate to **Start** > **Run**.
    c. In the Open screen, enter **`regedit.exe`**.
    d. In the registry editor, open the following subkey:

    ```
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP
    \v4\Full
    ```

    e. Check the **Release** value. The value that indicates .NET 4.7 is 460805. If this value is shown, you can skip the rest of this procedure. If that value is not shown, you must continue with this procedure and manually install .NET 4.7 or later.
    f. Navigate to the Microsoft Download center and search for the “Microsoft .NET Framework 4.7” installation program.
    g. Right-click the downloaded installation file and select **Run as administrator**.
    h. Agree to the license terms and install the software.
17. Repeat this procedure on any other servers that require the IIS software.

Next steps

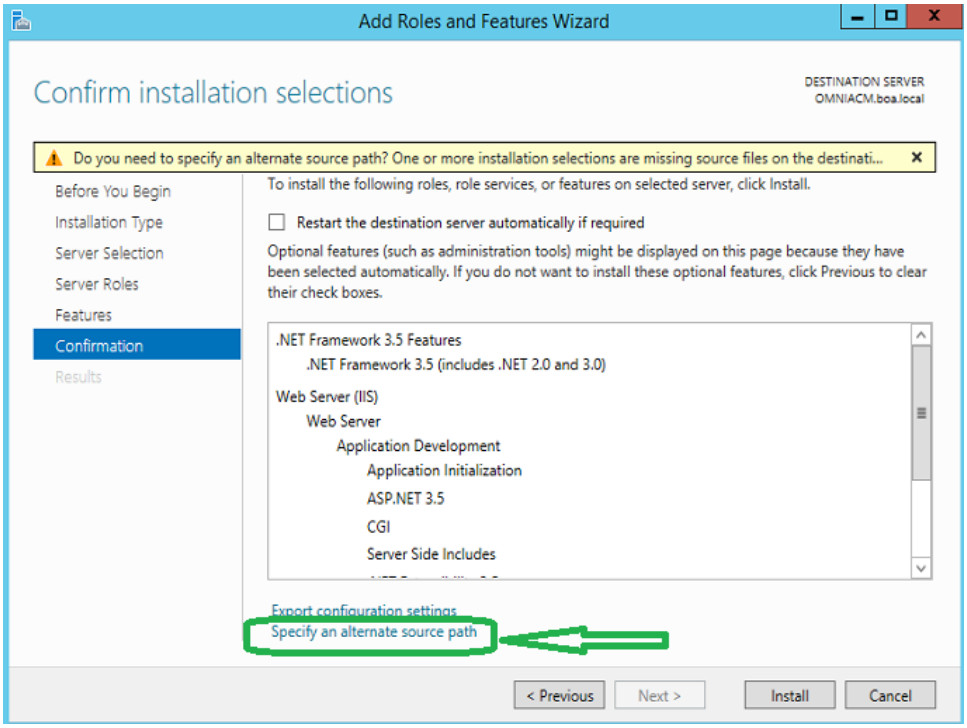
Important:

You must install the Microsoft .NET patches to pick up the latest security fixes.

When installing the Microsoft Windows Server OS for a new installation or for an upgrade from Microsoft Windows 2008, verify that you install the ASP.Net 3.5 role and the ASP.Net 4.5 role using the Microsoft Windows Server OS installation software disc or downloaded ISO image. When installing the roles, you must specify an alternate source path. The alternate source path is:

```
<Windows_Source>\sources\sxs
```

Use the **Specify an alternate source path** option as shown on the IIS installation screens in the following example:



Transport Layer Security (TLS) 1.2 and 1.1 are installed automatically when you install the IIS software. After you install the IIS software, you must disable TLS 1.0 per Avaya security requirements if it still exists on the system.

You can manually disable TLS 1.0 by editing the registry on every server where you installed IIS. Use the article found at the following web site, which explains how to edit the registry and disable TLS 1.0 and 1.1:

https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings

Installing the Microsoft SQL Server software

The Control Manager deployment must have a local database or a remote database running supported Microsoft SQL Server software on a server that is also using the supported Microsoft Windows Server operating system. The customer is responsible for installing the supported Microsoft SQL Server software on the following servers in a Control Manager deployment:

Important:

The customer cannot use Microsoft SQL Server Express edition when installing an HA configuration.

In an xCaaS deployment, the customer must install the Microsoft SQL Server database software on the following servers (logical server names in parentheses):

- Primary SQL server (ACM-SQL-1)
- Primary Billing SQL server (ACM-SQL-BILL-1)
- Secondary SQL server (ACM-SQL-2)
- Secondary Billing SQL server (ACM-SQL-BILL-2)

Detailed instructions for installing the Microsoft SQL Server software are available from Microsoft at:

https://msdn.microsoft.com/en-us/library/cc281837(v=sql.110).aspx

Considerations when installing the Microsoft SQL software

Important:

The customer must agree to create a user login ID on the SQL database servers that is a member of the Sysadmin server role. This user login ID is used during installation of the Control Manager software. Create the user login ID and its password and note these items for later use. This login is used during installation only; it is not used by the application during operation.

Important:

When creating database user passwords while installing the SQL software or while upgrading the Control Manager software, the customer must agree to use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

Note:

When installing the Microsoft SQL Server software, Microsoft notes that placing both log and data files on the same device can cause contention for that device, resulting in poor performance. Placing the log files on separate drives than the database data allows the I/O activity to occur at the same time for both the data and log files.

When installing the Microsoft SQL Server Standard or Enterprise software, the customer must select the following features:

- Database Engine Services
- SQL Server Replication
- Management Tools — Basic
- Reporting Services

Additionally, the customer should install the Management tools feature on at least one of the servers to allow you to manage your database server instances.

When installing Control Manager on Amazon Web Services (AWS), you might need to manually enable TCP/IP for the ODBC connectivity between the Control Manager software and the Microsoft SQL software. If you do not enable TCP/IP, you may see the following error message when installing the Control Manager software when testing the ODBC connection:

```
[Microsoft][ODBC SQL Server Driver][DBNetLib]SQL Server does not exist
or access denied
```

To enable TCP/IP after installing the Microsoft SQL software:

1. Navigate to **Start** > **All Programs** > **Microsoft SQL Server** > **Configuration Tools** > **SQL Server Configuration Manager**.
2. Expand **SQL Server Network Configuration** > **Select Protocol** for your SQL server.
3. In the right-hand pane, select **Enable TCP/IP**.
4. Restart the SQL service.

Installing certificates

The Control Manager browser interface requires that the customer install signed certificates to provide secure access (HTTPS). The signed certificates can be provided by a public or private Certificate Authority (CA).

Caution:

Certificates generated using System Manager will work for Control Manager. However, if the Control Manager system is hosted on a WAN, NLAN, or WLAN, Control Manager may not be able to validate the certificate and the user might see a “Certificate not valid” warning message when logging on to Control Manager.

Important:

Certificates must be installed whether it is a new installation or an upgrade. The certificates must be installed before you install or upgrade the Control Manager software.

In a Multi-server configuration, the customer must install certificates on both Control Manager UI servers (ACM-UI-1 and ACM-UI-2). For HA deployments, you must also bind the certificate to port 9011 on both servers.

In a reduced footprint configuration that has the application and UI functions on one server, the customer must install certificates on both Control Manager application servers (ACM-APP-1 and ACM-APP-2). For HA deployments, you must also bind the certificate to port 9011 on both servers.

Related links

Generating a Certificate Signing Request in IIS on page 54
Submitting the CSR to a CA for signing on page 56
Installing the signed certificate on page 59
Binding the certificate to SSL port 9011 for HA on page 60
Installing the root certificate on page 61
Enabling SSL for secure browser access on page 62

Generating a Certificate Signing Request in IIS

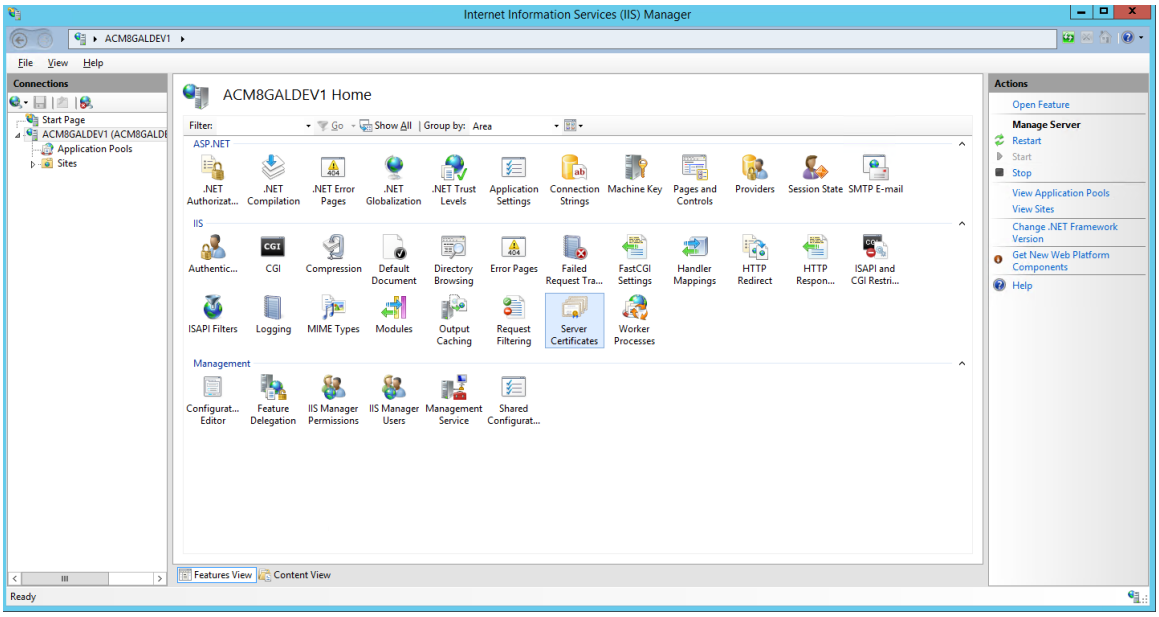
Before you begin

Confirm that Microsoft IIS is installed before you install a certificate.

Procedure

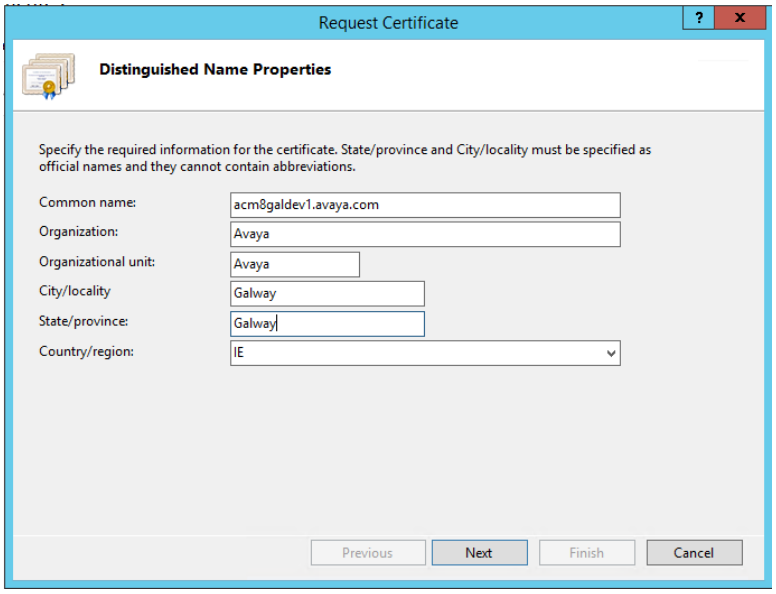
1. Open the Microsoft IIS Manager tool.
2. Click on the Control Manager server shown in the **Connections** tree.

   The system displays a screen similar to the following example:



3. Double-click **Server Certificates**.
4. Click on **Create Certificate Request**.

   The system displays a screen similar to the following example. The values you enter are specific to your installation.



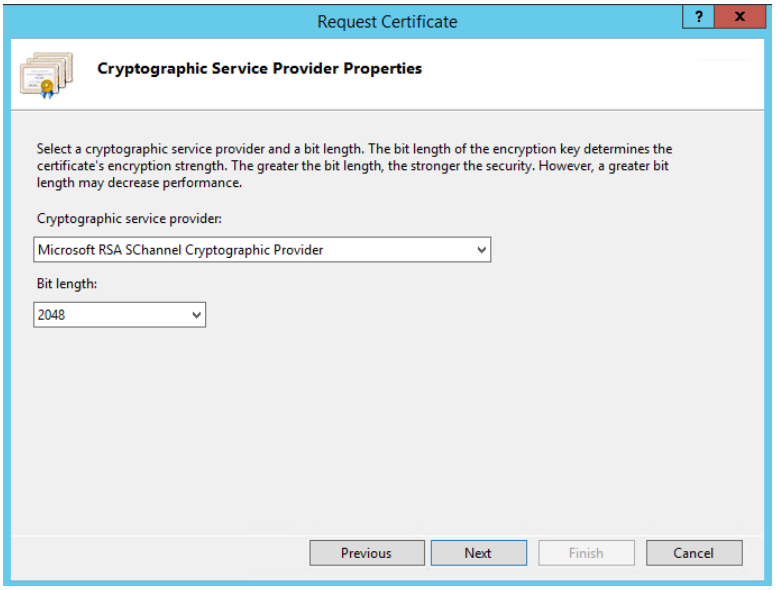
5. Administer the requested parameters. Enter the server name or FQDN of the Control Manager server in the **Common name** field.

   Caution:

   If the name entered in the **Common name** field does not match the host name of the Control Manager server, the certificate will not be valid and users will not be able to access the system using their browser.

6. Click **Next**.

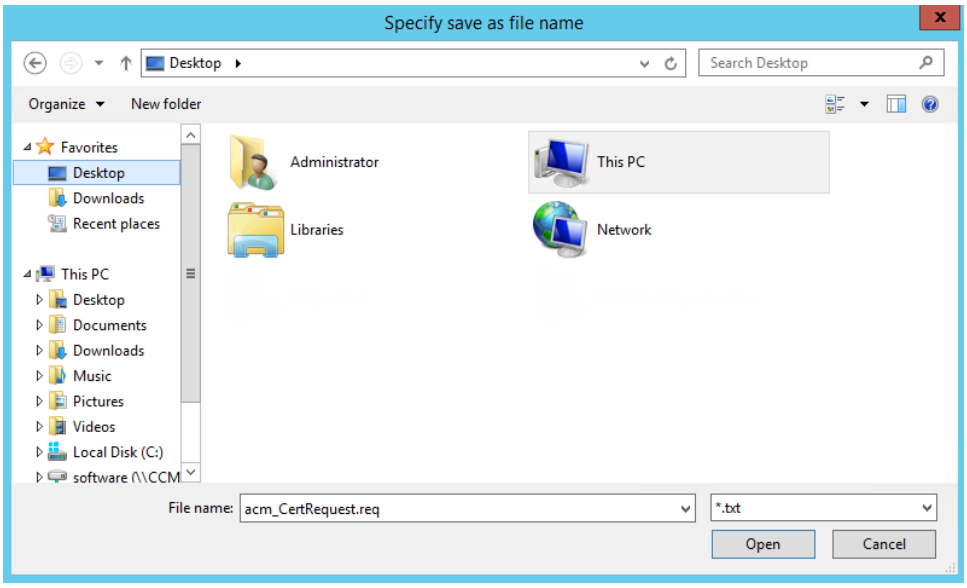
   The system displays the following screen:



7. Set the **Bit length** option to 2048.

8. Click **Next**.

   The system displays the Save As dialog:



9. Specify a file name that represents the name of the Control Manager server for which you are requesting a certificate. If you are requesting more that one certificate, make the names unique.
10. Click **Open**.
11. Click **Finish**.

Submitting the CSR to a CA for signing

About this task

The screens shown in this procedure are just examples of what you will see from a typical CA. The screens you see will be different depending on your CA provider.

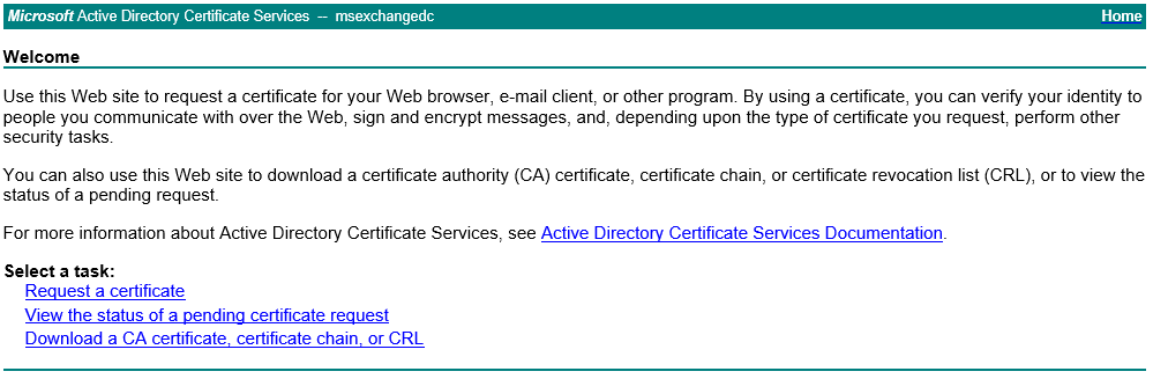
Before you begin

Generate your CSRs before doing this procedure.

Procedure

1. Log on to a CA signing page.

   The system displays a page similar to the following:

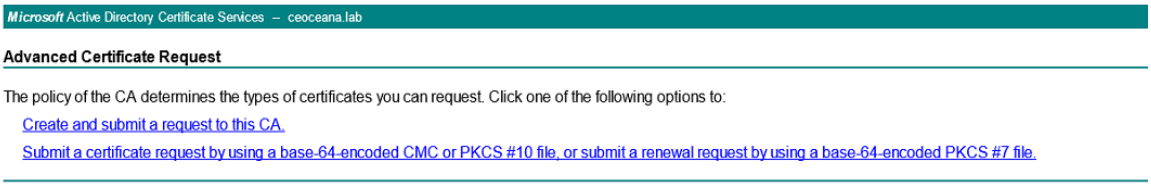


2. Click **Request a certificate**, or other similar option.

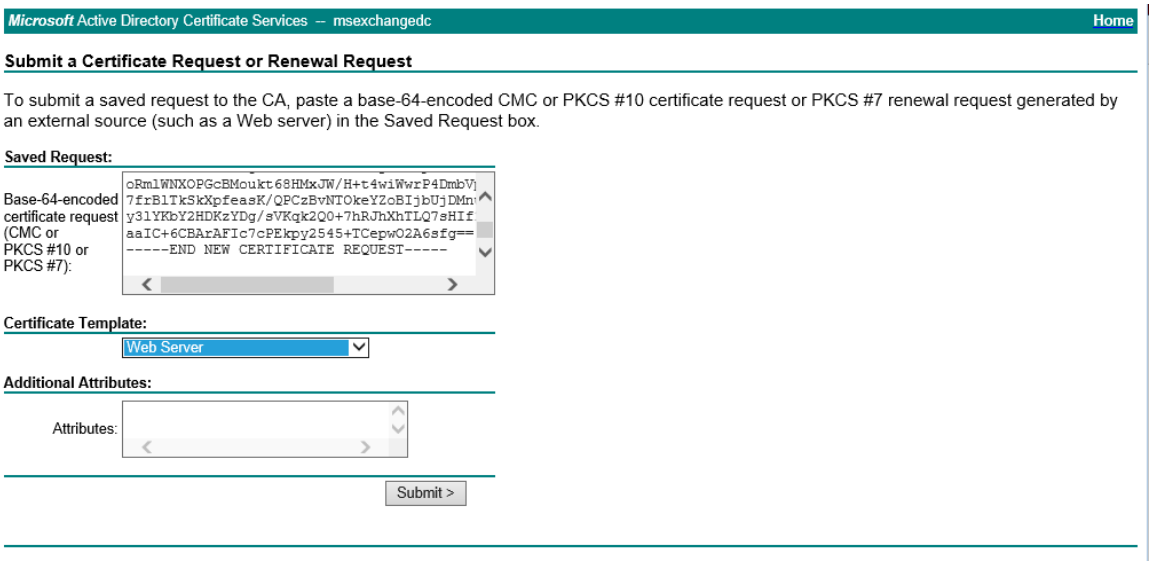
   The system displays a page similar to the following:

3. Open the CSR you created in the previous procedure in a text editor.
4. Click **advanced certificate request**, or similar option.

   The system displays a page similar to the following:



5. Click the second option, **Submit a certificate request by using....**.
6. Paste the details of your CSR into the **Saved Request** area as shown in the following example:

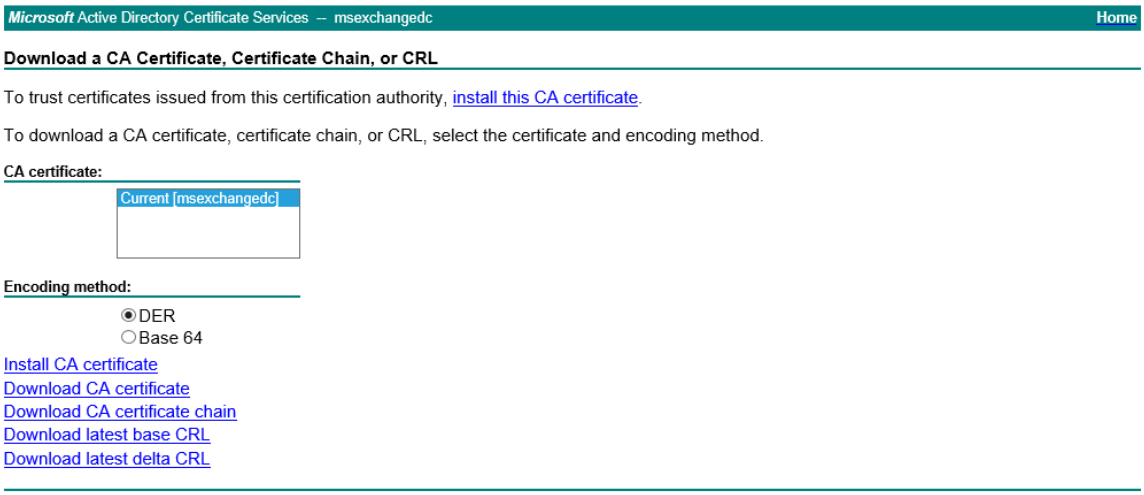


7. Select **Web Server** under the **Certificate Template** option, or similar option.
8. Click **Submit**.

   The system displays the Certificate Issued screen, or something similar:

9. Select the **DER encoded** option and click **Download certificate**.
10. From the same CA site Welcome screen, download the root certificate by clicking the **Download a CA certificate, certificate chain, or CRL** option, or some option similar to this.

    The system displays a screen similar to the following example:



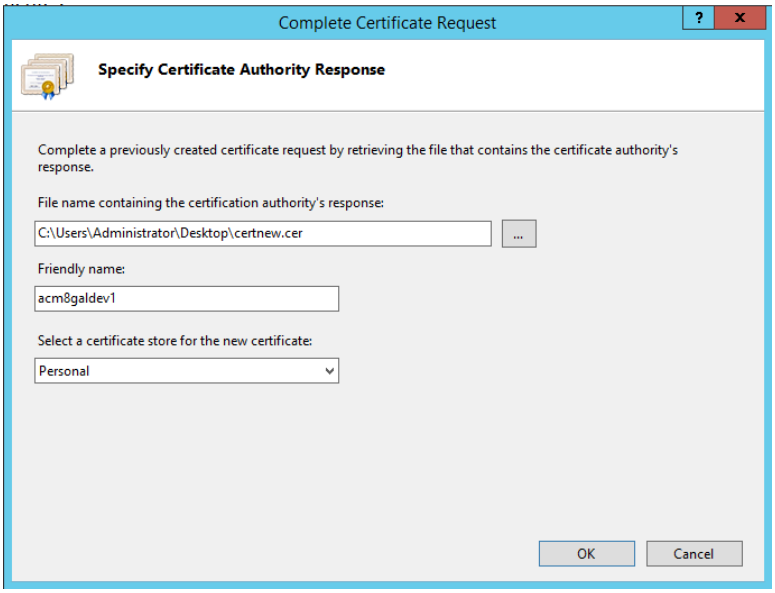
11. Click **Download CA Certificate**.
12. Copy the signed certificate and the root certificate to the Control Manager server.
13. Repeat this procedure for every Control Manager server that is required to have certificates.

Installing the signed certificate

Procedure

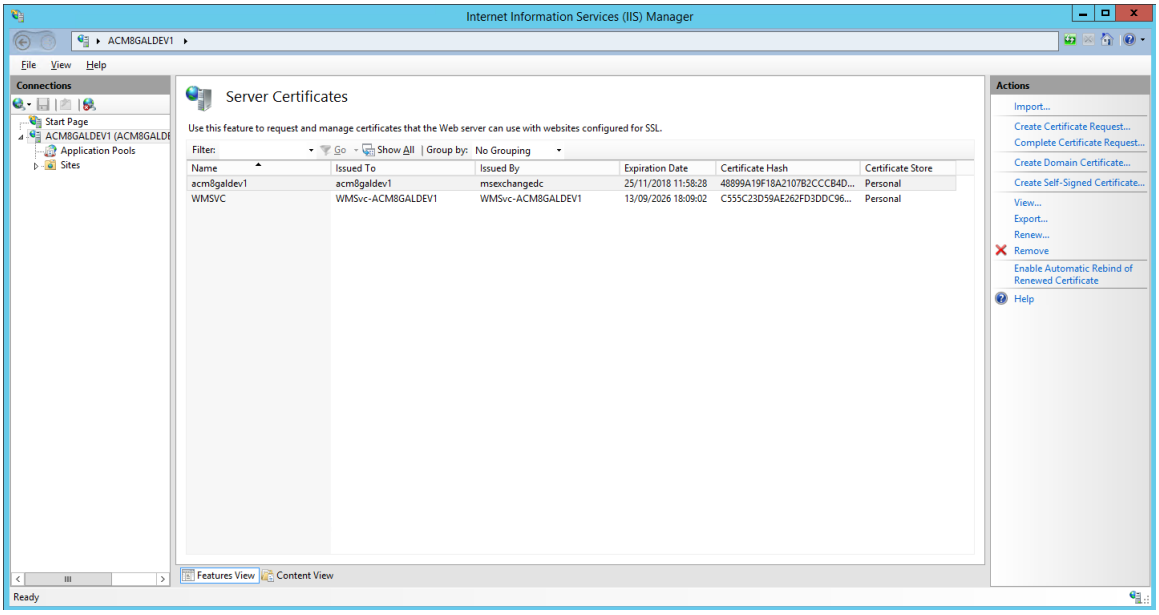
1. Return to the Microsoft IIS Manager tool.
2. On the Server Certificates page, click **Complete Certificate Request**.

   The system displays the following screen:



3. In the **Field name containing...** field, select the signed certificate you copied onto the Control Manager server.
4. Click **OK**.

   The signed certificate should now show on the Server Certificates screen. See the following example:



Binding the certificate to SSL port 9011 for HA

About this task

Perform this procedure for HA deployments only. You must perform this procedure on the primary and secondary application servers in an Enterprise deployment. You must perform this procedure on the primary and secondary application servers and on the primary and secondary UI servers in an xCaaS deployment.

For more information about this procedure, see the following Microsoft article:

https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-configure-a-port-with-an-ssl-certificate

Procedure

1. Log on to Windows as an administrator on the Control Manager server where you are installing certificates.
2. Open a command window as administrator using `cmd.exe`.
3. Run the following command:

```
netsh http add sslcert ipport=0.0.0.0:9011
certhash=<ThumbprintValueNoSpaces>
appid={<GUID>}
```

Where:

- The option `ipport` must be `0.0.0.0:9011`.
- *<ThumbprintValueNoSpaces>* is the Thumbprint value found within the certificate. To find the Thumbprint value, go to the personal certificate store and select the certificate you just imported. Right-click and open the certificate. Click on the **Details** tab and set the **Show** option to **<All>**. Copy the thumbprint value from the certificate, remove all spaces, and enter it as the `certhash` value.
- *<GUID>* is a unique ID that identifies the owning application. You can generate the GUID by using Windows Power Shell with the `[guid]::NewGuid()` command. The results must be pasted within curly braces as shown in the above example.

If successful, the system displays the following message:

```
SSL Certificate successfully added
```

4. Repeat this procedure on the secondary application server in an Enterprise deployment. Repeat this procedure secondary application server and on the primary and secondary UI servers in an xCaaS deployment. Do not reuse GUID values across the different servers.

Installing the root certificate

Procedure

1. Log on to Windows on the Control Manager server where you must install certificates.
2. Select **Start** > **Run**.
3. Enter **mmc** and click **OK**.

   The system displays the Microsoft Management Console.
4. In the console window, select **File** > **Add/Remove Snap-in**.

   The system displays the Add or Remove Snap-ins screen.
5. Select **Certificates** and click **Add**.

   The system displays the Certificates snap-in screen.
6. Select **Computer account** and click **Next**.

   The system displays the Select Computer screen.
7. Select **Local Computer** and click **Finish**.

   The system displays the Add or Remove Snap-ins screen.
8. Click **OK**.

   The system displays the Microsoft Management Console again showing that the Certificates snap-in has been added.
9. Expand the **Certificates** folder.

10. Select **Intermediate Certification Authorities** > **All Tasks** > **Import**.

    The system displays the Certificate Import Wizard Welcome screen.
11. Click **Next**.

    The system displays the File to Import screen.
12. Click **Browse** to locate the root certificate you requested from the CA.
13. Click **Next**.
14. Select **Place all certificates in the following store**.
15. Click **Browse** and select **Intermediate Certification Authorities**.
16. Click **Next**.
17. Click **Finish**.
18. Select **Trusted Root Certification Authorities** > **All Tasks** > **Import**.

    The system displays the Certificate Import Wizard Welcome screen.
19. Click **Next**.

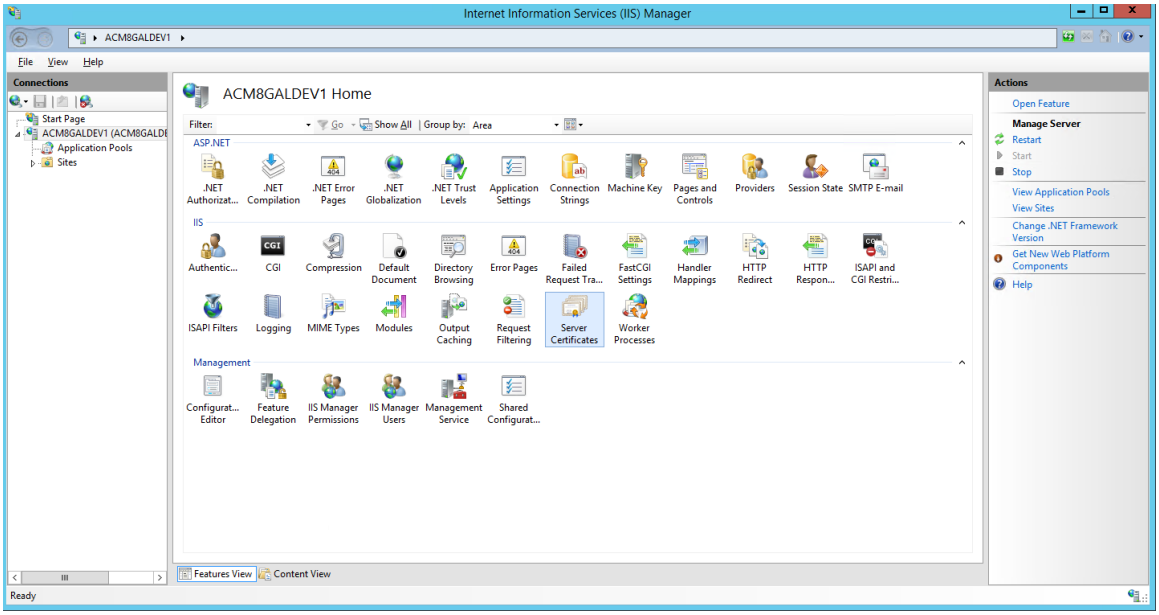
    The system displays the File to Import screen.
20. Click **Browse** to locate the root certificate you requested from the CA.
21. Click **Next**.
22. Select **Place all certificates in the following store**.
23. Click **Browse** and select **Trusted Root Certification Authorities**.
24. Click **Next**.
25. Click **Finish**.

Enabling SSL for secure browser access

Procedure

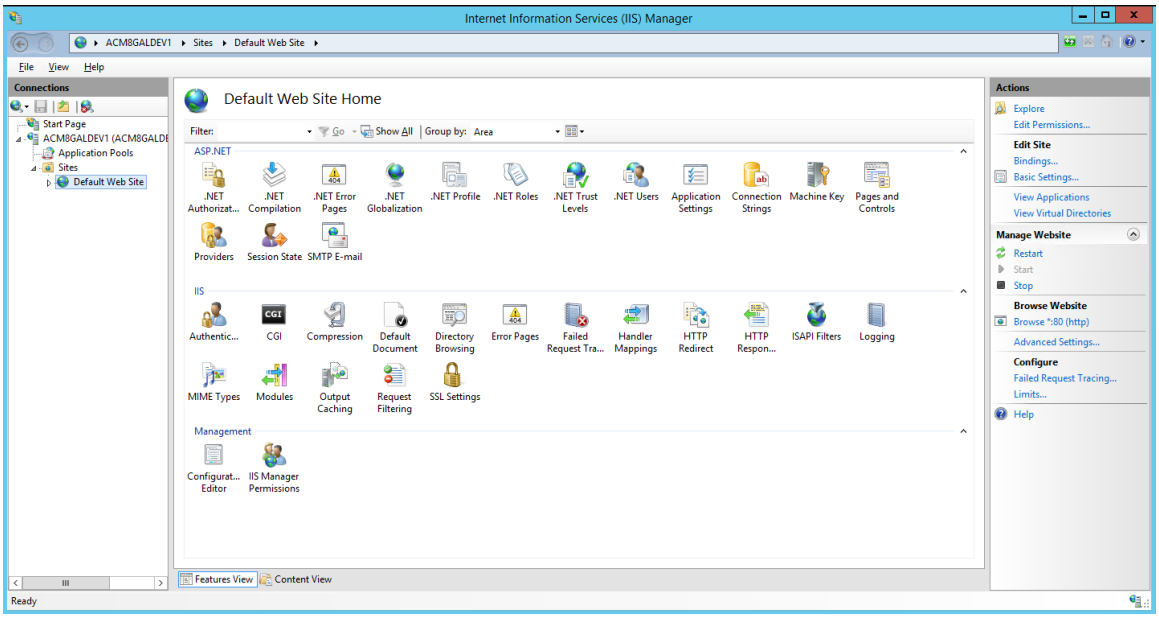
1. Open the Microsoft IIS Manager tool.
2. Click on the Control Manager server shown in the **Connections** tree.

   The system displays a screen similar to the following example:



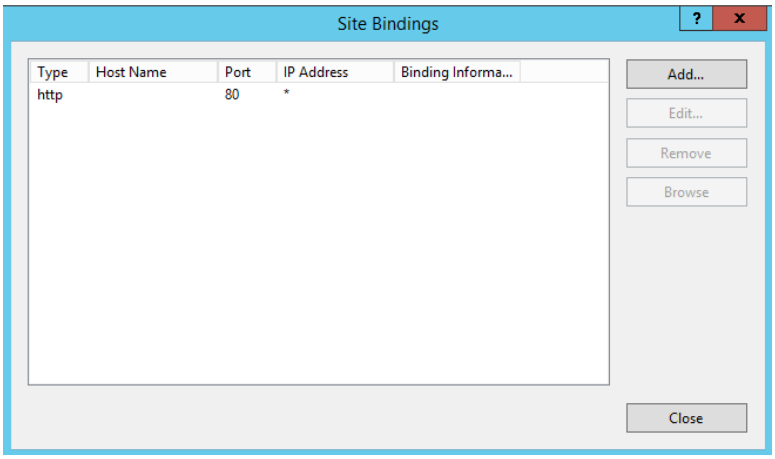
3. Expand the **Sites** folder and select **Default Web Site**.

   See the following example:



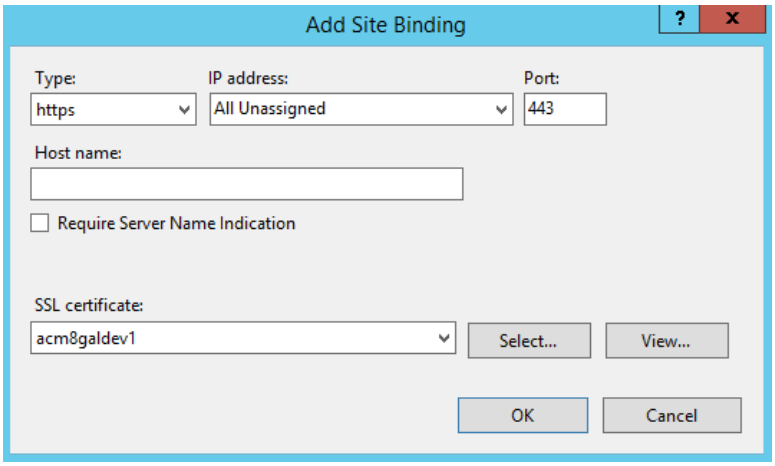
4. Select **Bindings** from the **Actions** menu on the right side of the screen.

   The system displays the Site Bindings screen.



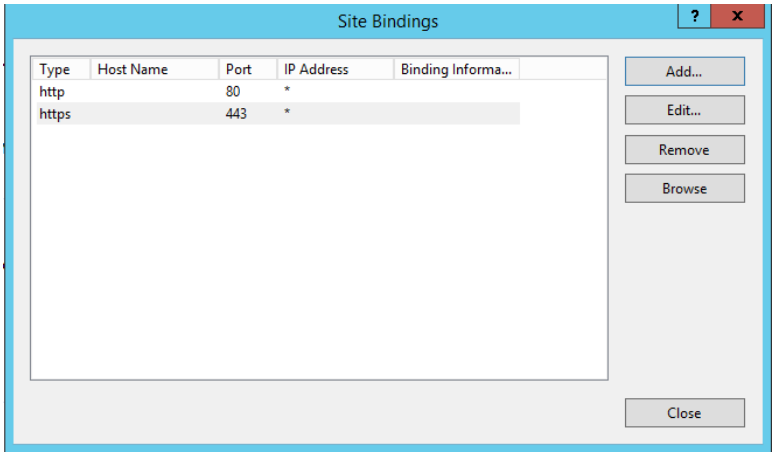
5. Click **Add**.

   The system displays the Add Site Binding screen:



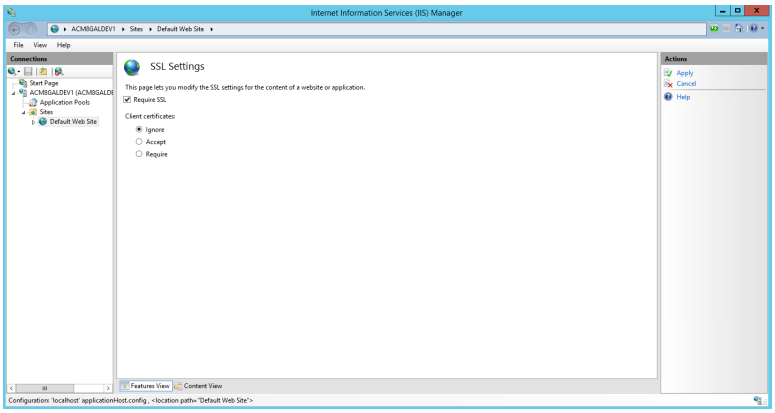
6. Administer the following parameters:
   - Set **Type** to **https**.
   - Set **IP address** to **All Unassigned**.
   - Leave **Host name** blank.
   - In the **SSL certificate** field, click **Select** to browse to the signed certificate you requested from the CA.
7. Click **OK**.

   The system displays the Site Bindings screen again showing the HTTPS type:



8. Click **Close**.
9. On the Default Web Site Home page, double-click the **SSL Settings** option.

   The system displays the SSL Settings screen:



10. Select the **Require SSL** option.
11. Select **Apply** from the **Actions** menu on the right side of the screen.
12. You can now exit from the IIS Manager tool.

Upgrading Windows 2012 to Windows 2012 R2

About this task

Control Manager supports only Microsoft Windows OS 2012 R2, not Microsoft Windows OS 2012. If you are upgrading from a system that is on Microsoft Windows OS 2012, you must first upgrade the OS to Microsoft Windows OS 2012 R2.

After upgrading, you must also check the Java version for compatibility and correct any incompatibilities.

Before you begin

Determine which version of Microsoft Windows OS 2012 is on the current system. If the current system has Microsoft Windows OS 2012 R2, you can skip this procedure.

Procedure

1. Upgrade the OS as described in the following Microsoft article:

   https://technet.microsoft.com/en-us/library/dn303416.aspx
2. Log on to Windows.
3. Navigate to **Start** > **Control Panel** > **Programs and Features**.
4. Right-click the Java SE Development Kit program and select **Uninstall**.

   The system uninstalls the Java software.
5. Navigate to **Start** > **Run**.
6. Enter **`regedit`** in the Open window.

   The system displays the Registry Editor window.
7. Navigate to **HKEY_CURRENT_USER** > **SOFTWARE** > **JavaSoft**.
8. Right-click **FIUCancel** and select **Delete**.

Preparing the license server for startup

About this task

To prepare the License Server so that Avaya can start it after installing Control Manager software, you must confirm that the System Cryptography settings on Windows is disabled.

Procedure

1. Log on to the system using the administrative credentials.
2. Start Local Group Policy Editor by performing the following actions:
   a. Click **Start** > **Run**.
   b. In the **Run** dialog box, type gpedit.msc.
   c. Click **OK**.
3. In the left pane, navigate to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.
4. In the right pane, double-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
5. The system displays the System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing screen.

6. Verify that the options is disabled.
7. If the option is not disabled, click **Disabled** and then click **OK**.
8. Close the Local Group Policy Editor.

Chapter 7: Upgrading a system using database migration

Upgrade process overview

Using a database migration is required when upgrading under the following conditions:

- The system is currently running Control Manager Release 7.1.101 on any OS or SQL combination.
- The system is currently running Control Manager Release 8.0.x but the customer wants to also update their OS or SQL software as part of the upgrade.

The upgrade process when the customer is on Control Manager Release 7.1.101 is as follows:

- The customer must use the VMware tools to take a snapshot of the old system before starting the upgrade process.
- Avaya personnel back up the Control Manager databases on the old Windows SQL Server system.
- Avaya personnel back up the Control Manager billing database.
- The customer installs the required hardware and deploys the required number of virtual machines for the new system. See *Hardware requirements* in the *Requirements* chapter.

  Caution:

  Host names of Control Manager application and UI servers must only contain alphabetic letters and numbers and are limited to a length of 15 characters. Host names cannot contain any special characters, such as hyphens (-) or underscores (_). Confirm that you are using a valid host name before you install the Control Manager software because you cannot change the host name after installing the Control Manager software.

  Host names of Control Manager database servers must follow the requirements set forth by Microsoft in the following article:

  https://support.microsoft.com/en-us/help/909264/

- The customer installs the Microsoft Windows 2012 R2 or 2016 OS software. For more information, see Supported server operating system software requirements on page 18.
- The customer installs the Microsoft SQL 2012, 2014, or 2016 software. For more information, see Supported database server software requirements on page 18 and Supported Microsoft Windows OS and SQL combinations on page 21.

- Avaya personnel restore (migrate) the data from the old system to the new Windows SQL Server installation.
- Avaya personnel download the Control Manager software.
- Avaya personnel install and configure the Control Manager software on the new servers, directing the Control Manager database to the SQL database server with the restored database.
- Avaya personnel enable data replication, HA services, and failover schemes.
- Avaya personnel test the upgraded software to confirm proper operation.

Upgrade checklist

Task	✔
Plan the Control Manager deployment with the customer.	
Read the *Avaya Control Manager Release Notes* before you start any work. Follow any special instructions for the installation or upgrade concerning required service packs, patches, and so on.	
Confirm that the customer has installed the following components: • Hardware servers • Microsoft Windows 2012 R2 or 2016 Server OS software • Microsoft SQL Server 2012, 2014, or 2016 software	
Ensure that all product licenses are in place. When upgrading from a 7.x system, you must get new license files. When upgrading from an 8.x system, you do not need to get new license files. The software and license file for Control Manager are typically sent to the customer once the order is completed in SAP. In order to obtain the license, send a message to licenseadmin@avaya.com with the following information: • Copy of the original Purchase Order (PO) or an existing license file. • MAC address of all servers where the Control Manager software is going to be installed. **Important:** If the server has multiple NICs (Ethernet ports), you must get the MAC IDs for all NICs on the server and submit those MAC IDs when you request a license file. **Application Server** / **MAC IDs** ACM-APP-1 ACM-APP-2 ACM-UI-1	

Table continues…

Task	✔
Application Server / **MAC IDs** ACM-UI-2 / **Note:** If all required information is included in the request, license requests are usually provided within 1 to 2 business days (Monday through Friday, not including public holidays and weekends).	
Record information about the following manually-configured parameters that might need to be reconfigured after the upgrade: • Any LDAP or SSO configuration made to configuration files that are not stored in the database or are not migrated from the old system. • Communication Manager timeout values added to Control Manager service or Web portal configuration files to compensate for network delays. • Scheduled jobs created in Control Manager 7.x are not migrated automatically when doing a database migration to Control Manager 8.x. Control Manager 8.x has a new scheduled job portal that differs from its earlier releases. The scheduled jobs created in 7.x must be recreated manually after upgrade. You must manually record the details about every scheduled job on the old system before you start the upgrade. Use the procedure found in Recreating scheduled jobs on page 102 to migrate the 7.x active scheduled jobs to the new scheduled job portal. • The Avaya Modular Messaging connector in an HA deployment as described in *Configuring Avaya Control Manager*.	
Download the Control Manager software package from the Avaya support site. The software package is an ISO image that you must unpack into an executable file using standard ISO unpacking tools.	
Ensure that the end user and enterprise environments can support Control Manager.	
Ensure that you have installed and configured Communication Manager.	
Ensure that all prerequisite software for Control Manager has been installed and configured.	
If you have scanning software installed on the server, ensure that you disable the scanning software before you upgrade the Control Manager software. You can enable the scanning software after the upgrade is complete.	
Back up the database on the Windows SQL Server 2008 system. This backup is used to restore (migrate) data to the new system. See the sections *Control Manager databases that require backup* and *Backing up Control Manager databases* in this chapter.	
Confirm that the Windows time and date is set accurately before you install Control Manager software.	
Install the new system. For details, see *Upgrading from an HA Microsoft 2008 system*.	
Migrate (restore) the data from the old Windows SQL Server 2008 database to the new Windows SQL 2012 or 2014 database server.	
Test the upgrade and troubleshoot any upgrade issues.	

Table continues…

Task	✔
Configure the Control Manager deployment with any new features added with the upgrade. For details, see *Configuring Avaya Control Manager*.	
Complete the initial administration for any new features added with the upgrade. For details, see *Using Avaya Control Manager to Administer Avaya Products*.	

Installation and upgrade considerations

Consider the following items when installing or upgrading the Control Manager software:

- Read the *Avaya Control Manager Release Notes* before you start any work. Follow any special instructions for the installation or upgrade concerning required service packs, patches, and so on. Review all of the fixed issues to note any changes that might affect the installation or upgrade.
- Do not install Windows updates on the system while installing the Control Manager software. You can either disable the Windows updates or install all the available updates before you install the Control Manager software.
- Ensure that the client system supports the minimum resolution of 1920x1080 pixels or higher to run the Web browser.
- Temporarily disable any virus software while you install the software. During operation, exclude scanning of any SQL or Control Manager folders. Reenable the virus software after you complete the installation.
- Temporarily disable JRE automatic updates on the Control Manager servers.
- Avaya recommends that you install the Control Manager software on a non-system drive. That is, not the same drive where the OS is installed, which is typically the C: drive. On the drive where you do install the Control Manager software, change the permissions of the Avaya directory and provide full control to the network account. In this case, the network account corresponds to the user of the Control Manager application pool. All other processes use the Service user name.
- Perform **`nslookup`** and reverse **`nslookup`** between all servers in the deployment. If there are any errors, check the DNS setup on the network.
- Use the PSTool program to confirm that the SID is unique for each application, UI, and database servers.
- Inform the customer that when upgrading from previous versions, any permissions which are new in the current release and were previously granted to all users (by virtue of not having a way of excluding users) are granted to all users by default. The customer must reapply permissions on the new system and revoke permissions for any users that should not have access.

Important:

The customer must agree to create a user login ID on the SQL database servers that is a member of the Sysadmin server role. This user login ID is used during installation of the Control Manager software. Create the user login ID and its password and note these items for later use. This login is used during installation only; it is not used by the application during operation.

Important:

When creating database user passwords while installing the SQL software or while upgrading the Control Manager software, the customer must agree to use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

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.
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.

Table continues…

Database name	Purpose	Notes
		Note: The ACCCMCMSYSLOG database did not exist in 7.1.2.2, so there is no need to back up that database when upgrading from 7.1.2.2.
ACM_BILLING or ACCCMBilling	Stores the Control Manager billing database.	You must back up this database only if using the Control Manager Billing feature used with the xCaaS solution.

Important:

This document uses the database names ACM_BILLING and ACCCMBilling. If the system has been upgraded from a previous version, the database name is probably named ACCCMBilling. Regardless of which name is being used, ensure that you use the correct database name within these procedures.

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, you should also do backups for the following reasons:

- 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 should back up the database data in case the server becomes unusable after maintenance and you have to move the data to a new system.

Before you begin

Prior to Control Manager Release 8.x, you could rename the Control Manager databases to match any custom name that the customer might want. With Release 8.x, Control Manager requires standard fixed database names that cannot be changed.

When backing up data from an older system that might have custom database names, you must determine what the names were on the old system. If the database names were changed and do not match the standard fixed names, you must make sure that you back up the custom databases using the custom names, but restore the database information to the standard fixed database names.

Use the following table to track any differences between the standard database names and custom database names.

Standard Database Name	Custom Database Name
ACCCM	
ACCCMAVP	
ACCCMSYNC	
ACCCMCMSYSLOG	
ACM_BILLING or ACCCMBilling	

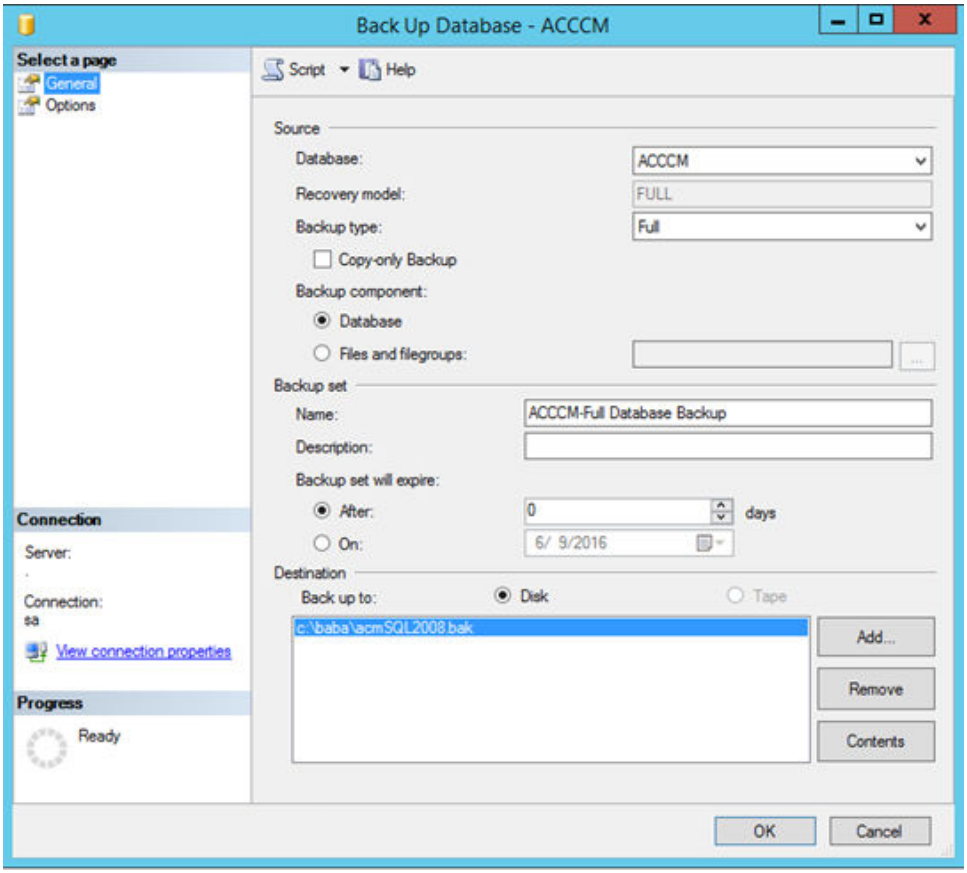
Procedure

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.
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 the other databases.

Important:

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

Restoring (migrating) the Control Manager databases

About this task

After the new Microsoft SQL Server system is installed, you must restore (migrate) the database data from the old Microsoft SQL Server system onto the new Microsoft SQL Server system.

Before you begin

Prior to Control Manager Release 8.x, you could rename the Control Manager databases to match any custom name that the customer might want. With Release 8.x, Control Manager requires standard fixed database names that cannot be changed.

When migrating data from an older system that might have custom database names, you must determine what the names were on the old system. If the database names were changed and do not match the standard fixed names, you must make sure that you back up the custom databases using the custom names, but restore the database information to the standard fixed database names.

Use the following table to track any differences between the standard database names and custom database names.

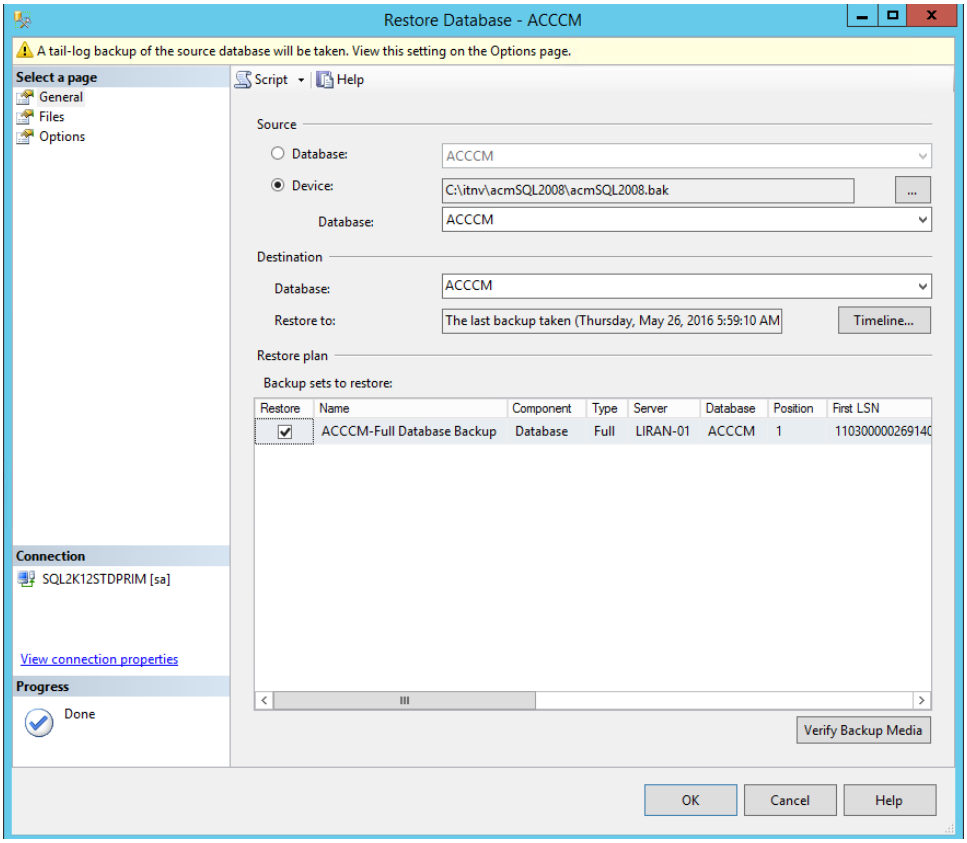
Standard Database Name	Custom Database Name
ACCCM	
ACCCMAVP	
ACCCMSYNC	
ACCCMCMSYSLOG	
ACM_BILLING	

Procedure

1. On the new Control Manager Microsoft SQL Server system, 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. Right-click on **Databases** and select **Restore database**.
4. For **Source**, choose **Device** and browse to the location where you backed up the database on the old Microsoft SQL Server system.

   If the old system was using custom database names, verify that you are selecting the correct database name.

   The system displays the following screen:



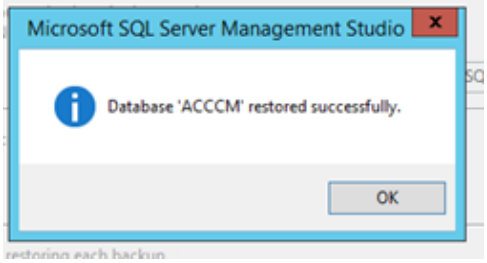
5. Select the database to restore (migrate) in the **Backup sets to restore** section, for example, **ACCCM**.

   Important:

   When selecting the databases for restore, use the standard database names as shown in the table above.

6. Select the **Options** page.
7. Administer the following parameters:
   - Under **Restore options**, select **Overwrite the existing database (WITH REPLACE)**.
   - Under **Tail-Log backup**, deselect **Take tail-log backup before restore**.
8. Click **OK**.

   When the database is restored (migrated), the system displays the following message:



9. Do the following steps to set the database compatibility level to 2012:
   a. Right-click on the restored database and select **Properties**.
   b. In the Database Properties screen, select the **Options** menu.
   c. In the **Compatibility Level** field, select **SQL Server 2012 (110)**.
   d. Click **OK**.
10. Repeat these steps for the remaining databases.

Installing Control Manager software on the primary application server (ACM-APP-1)

About this task

Use this procedure to install the Control Manager software for the following configurations:

- Install Control Manager application software on the primary application server (ACM-APP-1) in a standard four-server configuration.
- Install Control Manager application and UI software on the primary application server (ACM-APP-1) in a reduced three-server configuration (no dedicated UI server).
- Install Control Manager application and UI software on the primary application server (ACM-APP-1) in a reduced Dual host configuration (no dedicated UI server and no billing server).

Before you begin

Download the Control Manager software from the Avaya support site and copy it to every server where you are installing the software. The software package is an ISO image that you must unpack into an executable file using standard ISO unpacking tools. Using the MD5 Checksum, verify the data integrity of the downloaded file before you start the installation.

Ensure that the client system supports the minimum resolution of 1920x1080 pixels or higher to run the Web browser.

Verify that the .NET 4.5.2 software has been install before you attempt to install the Control Manager software.

Confirm that the Windows time and date is set accurately before you install Control Manager software.

Note:

For installation wizard logging, ensure that you have full administrative rights to access the server and to create files on the drive where you install the Control Manager software. You must initiate the installation by choosing the **Run as Administrator** option.

Note:

The Control Manager installation setup appends the installation logs to the following log file:

`InstallDrive:\acccminstallerVersionNumber.BuildNumber.log`

Caution:

Host names of Control Manager application and UI servers must only contain alphabetic letters and numbers and are limited to a length of 15 characters. Host names cannot contain any special characters, such as hyphens (-) or underscores (_). Confirm that you are using a valid host name before you install the Control Manager software because you cannot change the host name after installing the Control Manager software.

Host names of Control Manager database servers must follow the requirements set forth by Microsoft in the following article:

https://support.microsoft.com/en-us/help/909264/

Procedure

1. Log on to the server.
2. Open Windows Explorer and locate the Control Manager software you downloaded from the Avaya support site.
3. 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`

   The system starts the installation. Depending on whether this is a first-time new installation, a reinstallation, or an upgrade, the system displays one or more of the following screens:

   - **Welcome to the Prerequisites Wizard** — If the system displays this screen, you will step through one or two more prerequisites screens where software might be installed on your system. Click **Next** to advance to the next screen.
   - **License Agreement** — If the system displays this screen, select **I accept the terms in the License Agreement** and click **Next**. You may see additional prerequisites screens after the **License Agreement** screen. 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 will see before configuring the installation parameters.
4. Click **Next**.

   The system displays the **Install Mode** screen.
5. On the Install Mode screen, select **Service Provider**.

6. Click **Next**.

   The system displays the **Installation Type** screen.

7. Select the following parameters:

   - **Installation Type** — Select **New Installation**.
   - Select **High Availability** for a traditional HA deployment. Select **Standard** when deploying a UM Collector software installation using VMware HA or when deploying a non-production lab system.

   Note:

   When upgrading a system using database migration, you must select **New Installation**. This is because the upgrade by data migration consists of a new software installation followed by a data migration from the old system. The installation software will recognize that you are using a migrated database and handle the upgrade properly.

8. Click **Next**.

   The system displays the **Server Type** screen.

   Important:

   If you are deploying UM Collector software in a VMware HA configuration or in a non-production lab system, the system displays the **Distribution Setup** screen instead of the **Server Type** screen. Set the **Distribution Type** parameter to **All** and click **Next** to continue with the **SQL and ACM Database screen**.

9. For the primary server, configure the following parameters:

   - **Server Role** — Select **Primary Server**.
   - **HA Mode** — Select **Standard**.
   - **Distribution Type** — Select **UI** if the deployment has a dedicated UI server. Select **Services** if the deployment has a combined application and UI server.
   - **Primary Application Server Name** — Enter the host name or IP address of the primary application server. Do not use the FQDN of the server.
   - **Primary UI Server Name** — Enter the host name or IP address of the primary UI server. If you are using a three-server configuration without a dedicated UI server, enter the host name or IP address of the primary application server. Do not use the FQDN of the server.
   - **Secondary Application Server Name** — Enter the host name or IP address of the secondary application server. Do not use the FQDN of the server.
   - **Secondary UI Server Name** — Enter the host name or IP address of the secondary UI server. If you are using a three-server configuration without a dedicated UI server, enter the host name or IP address of the secondary application server. Do not use the FQDN of the server.

10. Click **Next**.

    The system displays the **SQL and ACM Database** screen.

11. For the SQL and Control Manager (ACM) database, configure the following parameters:

    - In the **SQL Server** and **SQL Port** fields, you can enter the information in several different formats using simple host names and TCP port numbers, IPv4 addresses, and named instances. See the following examples:

      Host Name in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Host Name\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Note:

      You cannot use an FQDN in the **SQL Server** field.

    - **SQL Admin Username** – Enter the name of a login that has Sysadmin rights on the database server.
    - **SQL Admin Password** – Enter the password for the user entered in the Username field.
    - **ACM DB Password** – Do one of the following steps:
      - For a new installation, enter a password for the Control Manager databases. The password you enter here is used for all of the Control Manager databases created during installation.
      - For an upgrade, enter the password for the Control Manager databases that was assigned on the old system.

      Important:

      Because this release of Control Manager has specific password length and character requirements, and that the same password is used for all databases, passwords from older systems may not meet those requirements for an upgrade. If this upgrade incompatibility exists, you must first log on to the SQL system and change the passwords to a compatible version before starting the upgrade.

      Important:

      When creating database user passwords while installing the SQL software, the customer must use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

12. Click **Next**.
13. For the secondary SQL server, configure the following parameters:
    - In the **Secondary SQL** and **SQL Port** fields, you can enter the information in several different formats using simple host names and TCP port numbers, IPv4 addresses, and named instances. See the following examples:

      Host Name in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Host Name\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Note:

      You cannot use an FQDN in the **SQL Server** field.
    - **SQL Admin Username** – Enter the name of a login that has Sysadmin rights on the database server.
    - **SQL Admin Password** – Enter the password for the user entered in the Username field.
    - **ACM DB Password** – Do one of the following steps:
      - For a new installation, enter a password for the Control Manager databases. The password you enter here is used for all of the Control Manager databases created during installation.
      - For an upgrade, enter the password for the Control Manager databases that was assigned on the old system.

      Important:

      Because this release of Control Manager has specific password length and character requirements, and that the same password is used for all databases, passwords from older systems may not meet those requirements for an upgrade. If this upgrade incompatibility exists, you must first log on to the SQL system and change the passwords to a compatible version before starting the upgrade.

      Important:

      When creating database user passwords while installing the SQL software, the customer must use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.
14. Click **Next**.

Note:

The installation software uses ODBC to test the database connection using the connection details administered in the previous dialog. If the test is successful, the installation program continues. If the test is not successful, you must go back and fix the incorrect connection details.

The system displays the **Select Installation Folder** screen.

15. Click **Browse**.
16. Browse to the location where you want to install the Control Manager software.

    Avaya recommends that you install the Control Manager software on a non-system drive. That is, not the same drive where the OS is installed, which is typically the C: drive.
17. After you select the install location, click **OK**.
18. Click **Next**.

    The system displays the **Configure Language and License** screen.
19. Configure the following parameters:
    - **System Language** – Select the language you want the Control Manager user interface to use as the default language. Individual users can select a different language when they log on, but this option sets the default language.
    - **License File** — Click **Load License**, browse to the location of the Control Manager license file you requested before starting the installation, select the license file, and click **Open**. The system closes the dialog box indicating the successful license upload.

      Important:

      The license file must be named:

      `license.lic`

      If you did not get the license file before you began installing the Control Manager software, you can install it later using the procedures found in Getting Control Manager licenses on page 23 and Installing Control Manager licenses on page 101.
20. Click **Next**.

    The system displays the **Ready to Install** screen.
21. You can review or change the installation settings by clicking **Back** repeatedly to step through all of the screens.
22. Click **Install** to begin the installation.

    The installation process can take up to an hour, depending on how many components the system must install.

    During the software installation, the system displays the **Installing Avaya Control Manager** screen.

Upon successful installation, the system displays the **Completing the Avaya Control Manager Setup Wizard** screen.

23. Click **Finish** to close the installation wizard.
24. Restart the server.

Next steps

To verify the installation, see the chapter *Testing the Control Manager installation*.

Installing Control Manager software on the secondary application server (ACM-APP-2)

About this task

Use this procedure to install the Control Manager software for the following configurations:

- Install Control Manager application software on the secondary application server (ACM-APP-2) in a standard four-server configuration.
- Install Control Manager application and UI software on the secondary application server (ACM-APP-2) in a reduced three-server configuration (no dedicated UI server).
- Install Control Manager application and UI software on the secondary application server (ACM-APP-2) in a reduced Dual host configuration (no dedicated UI server and no billing server).

Important:

You can skip this procedure under the following conditions:

- When deploying xCaaS with Usage Metering (UM) Collector software and the VMware HA feature.
- When deploying xCaaS in a lab environment.

Before you begin

Download the Control Manager software from the Avaya support site and copy it to every server where you are installing the software. The software package is an ISO image that you must unpack into an executable file using standard ISO unpacking tools. Using the MD5 Checksum, verify the data integrity of the downloaded file before you start the installation.

Ensure that the client system supports the minimum resolution of 1920x1080 pixels or higher to run the Web browser.

Verify that the .NET 4.5.2 software has been install before you attempt to install the Control Manager software.

Confirm that the Windows time and date is set accurately before you install Control Manager software.

Note:

For installation wizard logging, ensure that you have full administrative rights to access the server and to create files on the drive where you install the Control Manager software. You must initiate the installation by choosing the **Run as Administrator** option.

Note:

The Control Manager installation setup appends the installation logs to the following log file:

`InstallDrive:\acccminstallerVersionNumber.BuildNumber.log`

Caution:

Host names of Control Manager application and UI servers must only contain alphabetic letters and numbers and are limited to a length of 15 characters. Host names cannot contain any special characters, such as hyphens (-) or underscores (_). Confirm that you are using a valid host name before you install the Control Manager software because you cannot change the host name after installing the Control Manager software.

Host names of Control Manager database servers must follow the requirements set forth by Microsoft in the following article:

https://support.microsoft.com/en-us/help/909264/

Procedure

1. Log on to the server.
2. Open Windows Explorer and locate the Control Manager software you downloaded from the Avaya support site.
3. 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`

   The system starts the installation. Depending on whether this is a first-time new installation, a reinstallation, or an upgrade, the system displays one or more of the following screens:

   - **Welcome to the Prerequisites Wizard** — If the system displays this screen, you will step through one or two more prerequisites screens where software might be installed on your system. Click **Next** to advance to the next screen.
   - **License Agreement** — If the system displays this screen, select **I accept the terms in the License Agreement** and click **Next**. You may see additional prerequisites screens after the **License Agreement** screen. 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 will see before configuring the installation parameters.
4. Click **Next**.

   The system displays the **Install Mode** screen.
5. On the Install Mode screen, select **Service Provider**.

6. Click **Next**.

   The system displays the **Server Type** screen.

   Important:

   If you are deploying UM Collector software in a VMware HA configuration or in a non-production lab system, the system displays the **Distribution Setup** screen instead of the **Server Type** screen. Set the **Distribution Type** parameter to **All** and click **Next** to continue with the **SQL and ACM Database screen**.

7. For the secondary server, configure the following parameters:
   - **Server Role** — Select **Secondary Server**.
   - **HA Mode** — Select **Standard**.
   - **Distribution Type** — Select **UI** if the deployment has a dedicated UI server. Select **Services** if the deployment has a combined application and UI server.
   - **Primary Application Server Name** — Enter the host name or IP address of the primary application server. Do not use the FQDN of the server.
   - **Primary UI Server Name** — Enter the host name or IP address of the primary UI server. If you are using a three-server configuration without a dedicated UI server, enter the host name or IP address of the primary application server. Do not use the FQDN of the server.
   - **Secondary Application Server Name** — Enter the host name or IP address of the secondary application server. Do not use the FQDN of the server.
   - **Secondary UI Server Name** — Enter the host name or IP address of the secondary UI server. If you are using a three-server configuration without a dedicated UI server, enter the host name or IP address of the secondary application server. Do not use the FQDN of the server.

8. Click **Next**.

   The system displays the **SQL and ACM Database** screen.

9. For the SQL and Control Manager (ACM) database, configure the following parameters:
   - In the **SQL Server** and **SQL Port** fields, you can enter the information in several different formats using simple host names and TCP port numbers, IPv4 addresses, and named instances. See the following examples:

     Host Name in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

     IPv4 Address in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

     Host Name\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

     IPv4 Address\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

Note:

You cannot use an FQDN in the **SQL Server** field.

- **SQL Admin Username** – Enter the name of a login that has Sysadmin rights on the database server.
- **SQL Admin Password** – Enter the password for the user entered in the Username field.
- **ACM DB Password** – Do one of the following steps:
  - For a new installation, enter a password for the Control Manager databases. The password you enter here is used for all of the Control Manager databases created during installation.
  - For an upgrade, enter the password for the Control Manager databases that was assigned on the old system.

Important:

Because this release of Control Manager has specific password length and character requirements, and that the same password is used for all databases, passwords from older systems may not meet those requirements for an upgrade. If this upgrade incompatibility exists, you must first log on to the SQL system and change the passwords to a compatible version before starting the upgrade.

Important:

When creating database user passwords while installing the SQL software, the customer must use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

10. Click **Next**.
11. For the primary SQL server, configure the following parameters:
    - In the **Primary SQL Server** and **SQL Port** fields, you can enter the information in several different formats using simple host names and TCP port numbers, IPv4 addresses, and named instances. See the following examples:

      Host Name in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Host Name\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

Note:

You cannot use an FQDN in the **SQL Server** field.

- **SQL Admin Username** – Enter the name of a login that has Sysadmin rights on the database server.
- **SQL Admin Password** – Enter the password for the user entered in the Username field.
- **ACM DB Password** – Do one of the following steps:
  - For a new installation, enter a password for the Control Manager databases. The password you enter here is used for all of the Control Manager databases created during installation.
  - For an upgrade, enter the password for the Control Manager database that was assigned on the old system.

Important:

Because this release of Control Manager has specific password length and character requirements, and that the same password is used for all databases, passwords from older systems may not meet those requirements during an upgrade. If this upgrade incompatibility occurs, you must log on to the SQL system and change the passwords to a compatible version before continuing with the upgrade.

Important:

When creating database user passwords while installing the SQL software, the customer must use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

12. Click **Next**.

    Note:

    The installation software uses ODBC to test the database connection using the connection details administered in the previous dialog. If the test is successful, the installation program continues. If the test is not successful, you must go back and fix the incorrect connection details.

    The system displays the **Select Installation Folder** screen.

13. Click **Browse**.
14. Browse to the location where you want to install the Control Manager software.

    Avaya recommends that you install the Control Manager software on a non-system drive. That is, not the same drive where the OS is installed, which is typically the C: drive.

15. After you select the install location, click **OK**.

16. Click **Next**.

    The system displays the **Configure Language and License** screen.

17. Configure the following parameters:

    - **System Language** – Select the language you want the Control Manager user interface to use as the default language. Individual users can select a different language when they log on, but this option sets the default language.

    - **License File** — Click **Load License**, browse to the location of the Control Manager license file you requested before starting the installation, select the license file, and click **Open**. The system closes the dialog box indicating the successful license upload.

      Important:

      The license file must be named:

      `license.lic`

      If you did not get the license file before you began installing the Control Manager software, you can install it later using the procedures found in Getting Control Manager licenses on page 23 and Installing Control Manager licenses on page 101.

18. Click **Next**.

    The system displays the **Ready to Install** screen.

19. You can review or change the installation settings by clicking **Back** repeatedly to step through all of the screens.

20. Click **Install** to begin the installation.

    The installation process can take up to an hour, depending on how many components the system must install.

    During the software installation, the system displays the **Installing Avaya Control Manager** screen.

    Upon successful installation, the system displays the **Completing the Avaya Control Manager Setup Wizard** screen.

21. Click **Finish** to close the installation wizard.

22. Restart the server.

Next steps

To verify the installation, see the chapter *Testing the Control Manager installation*.

Installing the Control Manager software on the primary UI server (ACM-UI-1)

About this task

Use this procedure to install the Control Manager UI software on the primary Control Manager UI server (ACM-UI-1) in an HA configuration.

Important:

You can skip this procedure under the following conditions:

- When deploying xCaaS with Usage Metering (UM) Collector software and the VMware HA feature.
- If you are using the reduced server configurations where you do not have a dedicated UI server.
- When deploying xCaaS in a lab environment.

Before you begin

Download the Control Manager software from the Avaya support site and copy it to every server where you are installing the software. The software package is an ISO image that you must unpack into an executable file using standard ISO unpacking tools. Using the MD5 Checksum, verify the data integrity of the downloaded file before you start the installation.

Ensure that the client system supports the minimum resolution of 1920x1080 pixels or higher to run the Web browser.

Verify that the .NET 4.5.2 software has been install before you attempt to install the Control Manager software.

Confirm that the Windows time and date is set accurately before you install Control Manager software.

Note:

For installation wizard logging, ensure that you have full administrative rights to access the server and to create files on the drive where you install the Control Manager software. You must initiate the installation by choosing the **Run as Administrator** option.

Note:

The Control Manager installation setup appends the installation logs to the following log file:

`InstallDrive:\acccminstallerVersionNumber.BuildNumber.log`

Caution:

Host names of Control Manager application and UI servers must only contain alphabetic letters and numbers and are limited to a length of 15 characters. Host names cannot contain any special characters, such as hyphens (-) or underscores (_). Confirm that you are using a valid host name before you install the Control Manager software because you cannot change the host name after installing the Control Manager software.

Host names of Control Manager database servers must follow the requirements set forth by Microsoft in the following article:

https://support.microsoft.com/en-us/help/909264/

Procedure

1. Log on to the server.
2. Open Windows Explorer and locate the Control Manager software you downloaded from the Avaya support site.
3. 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`

   The system starts the installation. Depending on whether this is a first-time new installation, a reinstallation, or an upgrade, the system displays one or more of the following screens:

   - **Welcome to the Prerequisites Wizard** — If the system displays this screen, you will step through one or two more prerequisites screens where software might be installed on your system. Click **Next** to advance to the next screen.
   - **License Agreement** — If the system displays this screen, select **I accept the terms in the License Agreement** and click **Next**. You may see additional prerequisites screens after the **License Agreement** screen. 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 will see before configuring the installation parameters.
4. Click **Next**.

   The system displays the **Install Mode** screen.
5. On the Install Mode screen, select **Service Provider**.
6. Click **Next**.

   The system displays the **Installation Type** screen.
7. Select the following parameters:

   - **Installation Type** — Select **New Installation**.
   - Select **High Availability** for a traditional HA deployment. Select **Standard** when deploying a UM Collector software installation using VMware HA or when deploying a non-production lab system.

   Note:

   When upgrading a system using database migration, you must select **New Installation**. This is because the upgrade by data migration consists of a new software installation followed by a data migration from the old system. The installation software will recognize that you are using a migrated database and handle the upgrade properly.
8. Click **Next**.

The system displays the **Server Type** screen.

9. For the primary server, configure the following parameters:
   - **Server Role** — Select **Primary Server**.
   - **HA Mode** — Select **Standard**.
   - **Distribution Type** — Select **UI** if the deployment has a dedicated UI server. Select **Services** if the deployment has a combined application and UI server.
   - **Primary Application Server Name** — Enter the host name or IP address of the primary application server. Do not use the FQDN of the server.
   - **Primary UI Server Name** — Enter the host name or IP address of the primary UI server. If you are using a three-server configuration without a dedicated UI server, enter the host name or IP address of the primary application server. Do not use the FQDN of the server.
   - **Secondary Application Server Name** — Enter the host name or IP address of the secondary application server. Do not use the FQDN of the server.
   - **Secondary UI Server Name** — Enter the host name or IP address of the secondary UI server. If you are using a three-server configuration without a dedicated UI server, enter the host name or IP address of the secondary application server. Do not use the FQDN of the server.
10. Click **Next**.

    The system displays the **SQL and ACM Database** screen.
11. For the SQL and Control Manager (ACM) database, configure the following parameters:
    - In the **SQL Server** and **SQL Port** fields, you can enter the information in several different formats using simple host names and TCP port numbers, IPv4 addresses, and named instances. See the following examples:

      Host Name in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Host Name\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Note:

      You cannot use an FQDN in the **SQL Server** field.
    - **SQL Admin Username** – Enter the name of a login that has Sysadmin rights on the database server.
    - **SQL Admin Password** – Enter the password for the user entered in the Username field.

- **ACM DB Password** – Do one of the following steps:
  - For a new installation, enter a password for the Control Manager databases. The password you enter here is used for all of the Control Manager databases created during installation.
  - For an upgrade, enter the password for the Control Manager databases that was assigned on the old system.

  Important:

  Because this release of Control Manager has specific password length and character requirements, and that the same password is used for all databases, passwords from older systems may not meet those requirements for an upgrade. If this upgrade incompatibility exists, you must first log on to the SQL system and change the passwords to a compatible version before starting the upgrade.

  Important:

  When creating database user passwords while installing the SQL software, the customer must use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

12. Click **Next**.
13. For the secondary SQL server, configure the following parameters:
    - In the **Secondary SQL** and **SQL Port** fields, you can enter the information in several different formats using simple host names and TCP port numbers, IPv4 addresses, and named instances. See the following examples:

      Host Name in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Host Name\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Note:

      You cannot use an FQDN in the **SQL Server** field.
    - **SQL Admin Username** – Enter the name of a login that has Sysadmin rights on the database server.
    - **SQL Admin Password** – Enter the password for the user entered in the Username field.

- **ACM DB Password** – Do one of the following steps:
  - For a new installation, enter a password for the Control Manager databases. The password you enter here is used for all of the Control Manager databases created during installation.
  - For an upgrade, enter the password for the Control Manager databases that was assigned on the old system.

  Important:

  Because this release of Control Manager has specific password length and character requirements, and that the same password is used for all databases, passwords from older systems may not meet those requirements for an upgrade. If this upgrade incompatibility exists, you must first log on to the SQL system and change the passwords to a compatible version before starting the upgrade.

  Important:

  When creating database user passwords while installing the SQL software, the customer must use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

14. Click **Next**.

    Note:

    The installation software uses ODBC to test the database connection using the connection details administered in the previous dialog. If the test is successful, the installation program continues. If the test is not successful, you must go back and fix the incorrect connection details.

    The system displays the **Select Installation Folder** screen.

15. Click **Browse**.
16. Browse to the location where you want to install the Control Manager software.

    Avaya recommends that you install the Control Manager software on a non-system drive. That is, not the same drive where the OS is installed, which is typically the C: drive.

17. After you select the install location, click **OK**.
18. Click **Next**.

    The system displays the **Configure Language and License** screen.

19. Configure the following parameters:
    - **System Language** – Select the language you want the Control Manager user interface to use as the default language. Individual users can select a different language when they log on, but this option sets the default language.

- **License File** — Click **Load License**, browse to the location of the Control Manager license file you requested before starting the installation, select the license file, and click **Open**. The system closes the dialog box indicating the successful license upload.

  Important:

  The license file must be named:

  `license.lic`

  If you did not get the license file before you began installing the Control Manager software, you can install it later using the procedures found in Getting Control Manager licenses on page 23 and Installing Control Manager licenses on page 101.

20. Click **Next**.

    The system displays the **Ready to Install** screen.

21. You can review or change the installation settings by clicking **Back** repeatedly to step through all of the screens.

22. Click **Install** to begin the installation.

    The installation process can take up to an hour, depending on how many components the system must install.

    During the software installation, the system displays the **Installing Avaya Control Manager** screen.

    Upon successful installation, the system displays the **Completing the Avaya Control Manager Setup Wizard** screen.

23. Click **Finish** to close the installation wizard.

24. Restart the server.

Next steps

To verify the installation, see the chapter *Testing the Control Manager installation*.

Installing Control Manager software on the secondary UI server (ACM-UI-2)

About this task

Use this procedure to install the Control Manager UI software on the secondary Control Manager UI server (ACM-UI-2) in an HA configuration.

Important:

You can skip this procedure under the following conditions:

- When deploying xCaaS with Usage Metering (UM) Collector software and the VMware HA feature.
- If you are using the reduced server configurations where you do not have a dedicated UI server.
- When deploying xCaaS in a lab environment.

Before you begin

Download the Control Manager software from the Avaya support site and copy it to every server where you are installing the software. The software package is an ISO image that you must unpack into an executable file using standard ISO unpacking tools. Using the MD5 Checksum, verify the data integrity of the downloaded file before you start the installation.

Ensure that the client system supports the minimum resolution of 1920x1080 pixels or higher to run the Web browser.

Verify that the .NET 4.5.2 software has been install before you attempt to install the Control Manager software.

Confirm that the Windows time and date is set accurately before you install Control Manager software.

Note:

For installation wizard logging, ensure that you have full administrative rights to access the server and to create files on the drive where you install the Control Manager software. You must initiate the installation by choosing the **Run as Administrator** option.

Note:

The Control Manager installation setup appends the installation logs to the following log file:

`InstallDrive:\acccminstallerVersionNumber.BuildNumber.log`

Caution:

Host names of Control Manager application and UI servers must only contain alphabetic letters and numbers and are limited to a length of 15 characters. Host names cannot contain any special characters, such as hyphens (-) or underscores (_). Confirm that you are using a valid host name before you install the Control Manager software because you cannot change the host name after installing the Control Manager software.

Host names of Control Manager database servers must follow the requirements set forth by Microsoft in the following article:

https://support.microsoft.com/en-us/help/909264/

Procedure

1. Log on to the server.
2. Open Windows Explorer and locate the Control Manager software you downloaded from the Avaya support site.

3. 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`

   The system starts the installation. Depending on whether this is a first-time new installation, a reinstallation, or an upgrade, the system displays one or more of the following screens:

   - **Welcome to the Prerequisites Wizard** — If the system displays this screen, you will step through one or two more prerequisites screens where software might be installed on your system. Click **Next** to advance to the next screen.
   - **License Agreement** — If the system displays this screen, select **I accept the terms in the License Agreement** and click **Next**. You may see additional prerequisites screens after the **License Agreement** screen. 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 will see before configuring the installation parameters.
4. Click **Next**.

   The system displays the **Install Mode** screen.
5. On the Install Mode screen, select **Service Provider**.
6. Click **Next**.

   The system displays the **Installation Type** screen.
7. Select the following parameters:

   - **Installation Type** — Select **New Installation**.
   - Select **High Availability** for a traditional HA deployment. Select **Standard** when deploying a UM Collector software installation using VMware HA or when deploying a non-production lab system.

   Note:

   When upgrading a system using database migration, you must select **New Installation**. This is because the upgrade by data migration consists of a new software installation followed by a data migration from the old system. The installation software will recognize that you are using a migrated database and handle the upgrade properly.
8. Click **Next**.

   The system displays the **Server Type** screen.
9. For the secondary server, configure the following parameters:

   - **Server Role** — Select **Secondary Server**.
   - **HA Mode** — Select **Standard**.
   - **Distribution Type** — Select **UI** if the deployment has a dedicated UI server. Select **Services** if the deployment has a combined application and UI server.

- **Primary Application Server Name** — Enter the host name or IP address of the primary application server. Do not use the FQDN of the server.
- **Primary UI Server Name** — Enter the host name or IP address of the primary UI server. If you are using a three-server configuration without a dedicated UI server, enter the host name or IP address of the primary application server. Do not use the FQDN of the server.
- **Secondary Application Server Name** — Enter the host name or IP address of the secondary application server. Do not use the FQDN of the server.
- **Secondary UI Server Name** — Enter the host name or IP address of the secondary UI server. If you are using a three-server configuration without a dedicated UI server, enter the host name or IP address of the secondary application server. Do not use the FQDN of the server.

10. Click **Next**.

    The system displays the **SQL and ACM Database** screen.

11. For the SQL and Control Manager (ACM) database, configure the following parameters:

    - In the **SQL Server** and **SQL Port** fields, you can enter the information in several different formats using simple host names and TCP port numbers, IPv4 addresses, and named instances. See the following examples:

      Host Name in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Host Name\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Note:

      You cannot use an FQDN in the **SQL Server** field.

    - **SQL Admin Username** – Enter the name of a login that has Sysadmin rights on the database server.
    - **SQL Admin Password** – Enter the password for the user entered in the Username field.
    - **ACM DB Password** – Do one of the following steps:
      - For a new installation, enter a password for the Control Manager databases. The password you enter here is used for all of the Control Manager databases created during installation.
      - For an upgrade, enter the password for the Control Manager databases that was assigned on the old system.

Important:

Because this release of Control Manager has specific password length and character requirements, and that the same password is used for all databases, passwords from older systems may not meet those requirements for an upgrade. If this upgrade incompatibility exists, you must first log on to the SQL system and change the passwords to a compatible version before starting the upgrade.

Important:

When creating database user passwords while installing the SQL software, the customer must use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

12. Click **Next**.
13. For the secondary SQL server, configure the following parameters:
    - In the **Secondary SQL** and **SQL Port** fields, you can enter the information in several different formats using simple host names and TCP port numbers, IPv4 addresses, and named instances. See the following examples:

      Host Name in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Host Name\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Note:

      You cannot use an FQDN in the **SQL Server** field.
    - **SQL Admin Username** – Enter the name of a login that has Sysadmin rights on the database server.
    - **SQL Admin Password** – Enter the password for the user entered in the Username field.
    - **ACM DB Password** – Do one of the following steps:
      - For a new installation, enter a password for the Control Manager databases. The password you enter here is used for all of the Control Manager databases created during installation.
      - For an upgrade, enter the password for the Control Manager databases that was assigned on the old system.

Important:

Because this release of Control Manager has specific password length and character requirements, and that the same password is used for all databases, passwords from older systems may not meet those requirements for an upgrade. If this upgrade incompatibility exists, you must first log on to the SQL system and change the passwords to a compatible version before starting the upgrade.

Important:

When creating database user passwords while installing the SQL software, the customer must use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

14. Click **Next**.

    Note:

    The installation software uses ODBC to test the database connection using the connection details administered in the previous dialog. If the test is successful, the installation program continues. If the test is not successful, you must go back and fix the incorrect connection details.

    The system displays the **Select Installation Folder** screen.

15. Click **Browse**.
16. Browse to the location where you want to install the Control Manager software.

    Avaya recommends that you install the Control Manager software on a non-system drive. That is, not the same drive where the OS is installed, which is typically the C: drive.

17. After you select the install location, click **OK**.
18. Click **Next**.

    The system displays the **Configure Language and License** screen.

19. Configure the following parameters:
    - **System Language** – Select the language you want the Control Manager user interface to use as the default language. Individual users can select a different language when they log on, but this option sets the default language.
    - **License File** — Click **Load License**, browse to the location of the Control Manager license file you requested before starting the installation, select the license file, and click **Open**. The system closes the dialog box indicating the successful license upload.

      Important:

      The license file must be named:

      `license.lic`

If you did not get the license file before you began installing the Control Manager software, you can install it later using the procedures found in Getting Control Manager licenses on page 23 and Installing Control Manager licenses on page 101.

20. Click **Next**.

    The system displays the **Ready to Install** screen.

21. You can review or change the installation settings by clicking **Back** repeatedly to step through all of the screens.

22. Click **Install** to begin the installation.

    The installation process can take up to an hour, depending on how many components the system must install.

    During the software installation, the system displays the **Installing Avaya Control Manager** screen.

    Upon successful installation, the system displays the **Completing the Avaya Control Manager Setup Wizard** screen.

23. Click **Finish** to close the installation wizard.

24. Restart the server.

Next steps

To verify the installation, see the chapter *Testing the Control Manager installation*.

Installing Control Manager licenses

About this task

You must get install licenses for Control Manager under the following conditions:

- New installations.
- When upgrading (migrating) from any Release 7.x system.

You do not have to install a new license when upgrading from one version of 8.0.x to another version of 8.0.x, for example, 8.0.1 to 8.0.3.

Licenses for Control Manager software can be installed at the same time you install the Control Manager software. However, if you do not have a license file when you install the Control Manager software, you must install the license file after you install the Control Manager software before the system will be operational. Without valid license files, the license service will not start and no users will be able to log on to the Control Manager user interface.

Procedure

1. Get your license files as described in Getting Control Manager licenses on page 23.
2. Log on to one of the server(s) that for which you received a license file.

3. Copy the license file to the following location on the servers:

   `[Install Location]\Services\ACCCM License Server`

   Important:

   The license file must be named `license.lic`.

4. Reboot the server.
5. Log on to each of the server(s) that for which you received a license file.
6. Go to **Start** > **Run**.
7. Enter **`services.msc`** and press **Enter**.

   Note:

   The license server must start before any other services are started.

8. In the Services window, confirm that the **ACCCM License Server** service has started.
9. If the **ACCCM License Server** has not started, right-click **ACCCM License Server** and select **Start**.

   The system starts the service.

10. If the service fails to start, verify the service log files for details on any errors. The default location of the License Server log file is:

    `[Install Location]\Services\ACCCM License Server\logs`

11. Repeat this procedure for every server that requires a license file.

Recreating scheduled jobs

About this task

Scheduled jobs created in Control Manager 7.x are not migrated automatically when doing a database migration to Control Manager 8.x. Control Manager 8.x has a new scheduled job portal that differs from its earlier releases. The scheduled jobs created in 7.x must be recreated manually after upgrade. You must manually record the details about every scheduled job on the old system before you start the upgrade. Use this procedure to migrate the 7.x active scheduled jobs to the new scheduled job portal.

Before you begin

Verify that you have the details about the old scheduled jobs. If you do not have any information about the old jobs, create the new jobs as you would normally.

Procedure

1. Log on to the Control Manager system.
2. Navigate to **Bulk Action** > **Scheduled Bulk Jobs**.

3. Click **Add**.
4. In the **Choose location** drop-down, select the location for the Bulk Action Job.
5. In the **Action Name** field, enter a name for the job. Use the same name as you had on the old system.
6. In the **Action Type** drop-down, select **Edit**.
7. In the **Entity Type** drop-down, select **User**.
8. For the execution time option, use the following information to decide on a time.

   Scheduled jobs in Control Manager 8.x have extra options that were not in 7.x. The time Zone for the schedule should be the time zone of the Control Manager application host. Locations can be left empty and the interval should be zero when the recurrence is daily, weekly, or once. Create Daily/Weekly/Specific Dates schedules in 8.x as shown below:

   - Daily Schedule: Create a schedule with Recurrence as Daily, Finish type as Finite, and Start and Finish Date/time as was done in the 7.x schedule's start and end date.
   - Weekly Schedule: Create a schedule with Recurrence as Weekly, Finish type as Finite and Start and Finish Date/time as was done in the 7.x schedule's start and end date.
   - Specific Dates schedule: Create a schedule by adding multiple entries with Recurrence as Once and Start Date/time as was done in the 7.x schedule's specific dates.
9. Click **Next Step** twice to skip Step 2 of the Scheduled Bulk Jobs setup.
10. In Step 3, select the skills to update. Choose the Location at the top right corner to display the skills that need to be updated.
11. Click **Next Step** fout times to skip Steps 4–6 of the Scheduled Bulk Jobs setup.
12. In Step 7, select the agents for the job. Choose the Location at the top right corner to display the agents that need to be updated.
13. Click **Submit** to create the job.
14. Repeat this procedure for any other scheduled jobs you need to recreate.

Upgrading the Control Manager billing software

Uninstalling the billing software

About this task

When upgrading the billing software, you must first uninstall the previous version of the software.

Procedure

1. Log on to Windows on one of the Control Manager servers.
2. Navigate to **Start** > **Run**.
3. Enter `services.msc` and press **Enter**.

   The system displays a list of services.
4. In the Services window, right-click the **AAEP Billing Service** and **CM Billing Service** and select **Stop**.
5. Navigate to **Start** > **Control Panel** > **Programs and Features**.
6. On the Uninstall or change a program screen, right-click the **ACM Billing** program and click **Uninstall**.

   The system removes the selected component from the server.
7. Repeat this procedure on all servers that have Control Manager software.

Installing billing software on the Control Manager servers

Important:

When deploying xCaaS with Usage Metering (UM) Collector software, you can skip this entire chapter.

About this task

You must install the Control Manager Billing software on the following servers depending on your configuration:

- For the standard four-server configuration, you must install the Control Manager Billing software on the primary and secondary application servers (ACM-APP-1 and ACM-APP-2), the primary and secondary UI servers (ACM-UI-1 and ACM-UI-2), and the primary and secondary billing servers (ACM-SQL-BILL-1 and ACM-SQL-BILL-2).
- For the three-server configuration, you must install the Control Manager Billing software on the combined primary and secondary application/UI servers (ACM-APP-1 and ACM-APP-2) and the primary and secondary billing servers (ACM-SQL-BILL-1 and ACM-SQL-BILL-2).

Before you begin

Verify that the following servers are installed:

- The billing database servers installed with a supported version of Microsoft SQL Standard or Enterprise database software with SSRS.
- The Control Manager database servers installed with a supported version of Microsoft SQL database software.

Download the Control Manager software from the Avaya support site. Copy the software to every server where you are installing the software. The billing software is an executable file packaged within the Control Manager ISO image. You must unpack the ISO image into an executable file

using standard ISO unpacking tools. This download may include patches for the billing software which must be installed after installing the core billing software.

Procedure

1. Log on to the server.
2. Open Windows Explorer and locate the Control Manager billing software files you downloaded from the Avaya support site.
3. Right-click the Control Manager executable file and select **Run as Administrator**. The name of the file is similar to the following example:

   `ACM BILLING_ReleaseNumber_BuildNumber.exe`

   The system starts the installation and displays the **License Agreement** screen.
4. Select **I accept the terms in the License Agreement**.
5. Click **Next**.

   The system displays the **Prerequisites** screen.

   By default, the system checks for preinstalled components as prerequisites. If the prerequisite installation components exist in the system, the installation wizard skips the installation of existing prerequisite installation setup. If one or more component is missing, the installation wizard installs the missing components as part of the installation process.
6. Do one of the following steps:
   - If one or more of the prerequisites are selected and need to be installed, click **Next** and the system installs the prerequisite software.
   - If none of the prerequisites are selected, click **Finish**.

   The system displays the **Welcome to the ACM Billing Setup Wizard** screen.
7. Click **Next**.

   The system displays the **Configure how ACM BILLING** will be installed screen.
8. Select the following features based on the server where you are installing the billing software:

   Important:

   Do not uncheck the **MainFeature** menu item to deselect features. Deselect features one at a time.

   - Application servers (ACM-APP-1 and ACM-APP-2) on a standard four-server configuration — Select the following features: **Services** > **AAEPBilling**, **Services** > **ACCCMBillingEngine**, **DB Scripts** > **BillingDB**, and **DB Scripts** > **ACMDB**. Leave all other features deselected.
   - UI servers (ACM-UI-1 and ACM-UI-2) on a standard four-server configuration — Select the following features: **Web**. Leave all other features deselected.
   - Combined application/UI servers (ACM-APP-1 and ACM-APP-2) on a three-server configuration — Select all of the features except for **Services** > **BillingReports**

- Billing database servers (ACM-SQL-BILL-1 and ACM-SQL-BILL-2) — Select the following features: **Services** > **BillingReports**. Leave all other features deselected.

9. Click **Next**.

   The system displays the **Installation Type** screen.

10. In **Select the Type of Deployment**, select **New Installation**.
11. Click **Next**.

    The system displays the **Avaya ACM Billing Database** screen.

12. Administer the following parameters:
    - **Server Name** – Enter the host name of the primary or secondary server. Do not use the FQDN of the server. You can use the IP address of the server.
    - **Port** – Enter the port number for the connection the SQL billing server. The default port number is 1433.
    - **Database Name** – Enter the Control Manager Billing database name, ACM_BILLING.

      Important:

      When upgrading from a previous Control Manager release, ensure that you select the name of the database migrated from the previous system.

    - **Username** – Enter the database user ID that was created for the installation. The user ID is used for connecting to the SQL database server.
    - **Password** – Enter the password of the user.

    Important:

    Use the SQL Server Management Studio tool to confirm that any user name and password combination used here are able to access the SQL server.

13. Click **Next**.

    The system displays the **Avaya ACM Database** screen.

14. Administer the following parameters:
    - **Server Name** – Enter the host name of the primary or secondary database server (ACM-SQL-1 or ACM-SQL-2). Do not use the FQDN of the server. You can use the IP address of the server.
    - **Port** – Enter the port number of SQL database server. The SQL database server uses 1433 as the default port.
    - **Database Name** – Enter the Control Manager database name, ACCCM.
    - **Username** – Enter the database user ID that was created for the installation. The user ID is used for connecting to the SQL database server.
    - **Password** – Enter the password of the user.

Important:

Use the SQL Server Management Studio tool to confirm that any user name and password combination used here are able to access the SQL server.

15. Click **Next**.

    The system displays the **Avaya ACM Billing Login User** screen.

16. Enter the user name and password used to access the Control Manager billing system. This creates an SQL Server login ID in the existing Control Manager SQL Server and database user for the existing Control Manager database, with the database role set to “db_reader” only. This login ID for the Linked Server is used to retrieve data from the distributed Control Manager SQL server.

    Important:

    Use the SQL Server Management Studio tool to confirm that any user name and password combination used here are able to access the SQL server.

17. Click **Next**.

    The system displays the **Ready to Install** screen.

18. You can review or change the installation settings by clicking **Back** repeatedly to step through all of the screens.

19. Click **Install** to begin the installation.

    Upon successful installation, the system displays the **Completing the ACM BILLING Setup Wizard** screen.

20. Click **Finish** to close the installation wizard.

21. Repeat this procedure on the rest of the application servers, the UI servers, and the billing servers.

Next steps

Install any billing software patches included with the download.

To verify the installation, see the chapter *Testing the Control Manager installation*.

Configuring the billing software

About this task

After you install the billing software on the application servers, you must configure the `isStationEnabled` parameter in the `BillingEngineConfig.xml` file. You must do this so that Communication Manager stations are not queried during the billing process.

Procedure

1. Log on to Windows on the ACM-APP-1 primary application server.
2. Go to the following folder:

`<InstallationDrive>:\Program Files (x86)\Avaya\ACM BILLING\Services\ACCCMBillingEngine`

3. Open the `BillingEngineConfig.xml` file for editing.
4. Change the `<isStationEnabled>` option to `False`. See the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<configurations>
        <!-- connection string of ACCCM Billing database -->
    <connectionString>Data Source=10.10.7.175;Initial Catalog=ACCCMBilling;User ID=sa;Password=I9OsdaObBwrqmtulpL/3wQ==</connectionString>
        <!-- synchronize with cm will be in seconds -->
    <intervalperiodsec>300</intervalperiodsec>
        <!-- protocol telnet: 0, ssh: 1-->
    <protocol>0</protocol>
        <!-- port 5022, 5023 -->
    <port>5022</port>
        <!-- time in seconds that the system waiting for response from CM -->
    <cmcalltimeout>180</cmcalltimeout>
        <!-- time in seconds between sending request to same CM in same iteration (time between getting agents and station lists) -->
    <timeintervalbetweensamecmcalls>6</timeintervalbetweensamecmcalls>
        <!-- True/False. True - if need to synchronize stations from CM. -->
    <isStationEnabled>False</isStationEnabled>
        <!-- connection string of ACCCM Billing database -->
        <!-- synchronize with cm will be in seconds -->
        <!-- protocol telnet: 0, ssh: 1 -->
        <!-- port 5022, 5023 -->
        <!-- time in seconds that the system waiting for response from CM -->
        <!-- time in seconds between sending request to same CM in same iteration (time between getting agents and station lists) -->
        <!-- True/False. True - if need to synchronize stations from CM. -->
</configurations>
```

5. Save and close the file.
6. Repeat this procedure on the ACM-APP-2 secondary application server.

Configuring extension number delimiters to support billing count accuracy

About this task

To enable proper billing counts for agents that are provisioned with the Avaya one-X® Agent telecommuter or road warrior station types that use special character delimiters (punctuation) in the extension numbers, you must use a script that removes those delimiters from the data sent to the Control Manager billing software. The procedure shown here configures the most common delimiters, which are hyphen (-), period (.), and an empty space ( ). If the customer's Communication Manager system uses other delimiters, add those delimiters to the script when you create and run the script. You can only add five delimiters to the script. If the customer later adds more delimiters to extensions, you must run the script again.

You must perform this procedure on both the ACM-SQL-BILL-1 and ACM-SQL-BILL-2 servers.

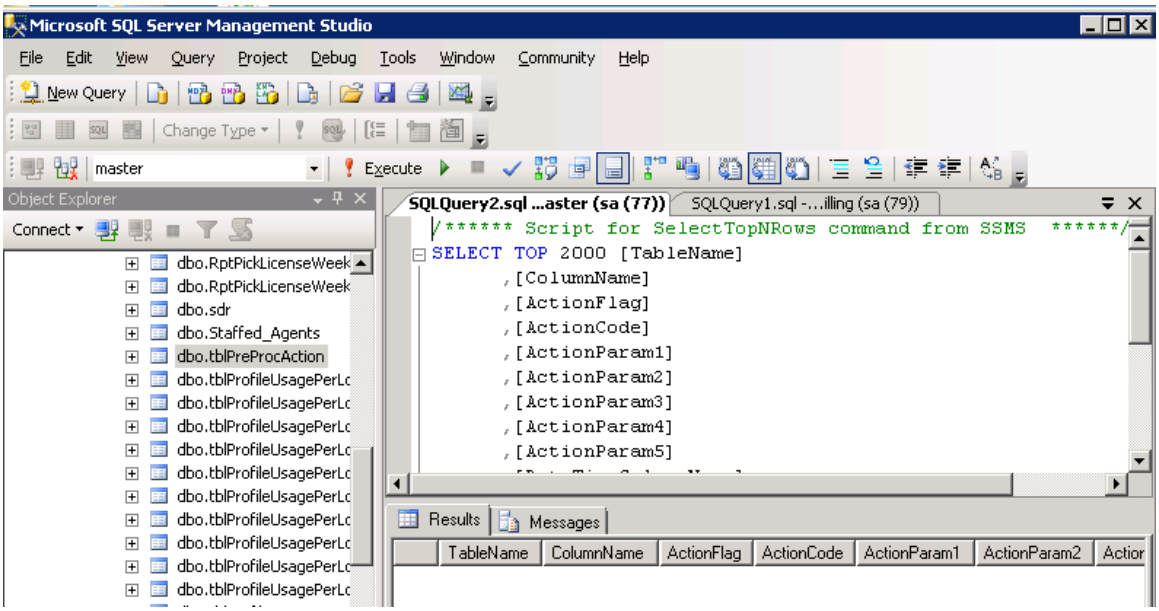
Before you begin

Check the dial plan on every Communication Manager system being used and determine all of the delimiters used in the dial plan. See the following example of a dial plan on Communication Manager:

```
change dialplan parameters                                          Page   1 of   1
                              DIAL PLAN PARAMETERS

                 Local Node Number: __                    ETA Node Number: ___
   UDP-ARS Calls Considered Offnet? n                 ETA Routing Pattern: ____
        UDP Extension Search Order: local-extensions-first



Retry ARS/AAR Analysis If All-Location Entry Inaccessible? n

 EXTENSION DISPLAY FORMATS
                              SAT              Inter-Location   Intra-Location
        6-Digit Extension:    xx.xx.xx         xx.xx.xx         xx.xx.xx
        7-Digit Extension:    xxx-xxxx         xxx-xxxx         xxx-xxxx
        8-Digit Extension:    xx.xx.xx.xx      xx.xx.xx.xx      xx.xx.xx.xx
        9-Digit Extension:    xxx-xxx-xxx      xxx-xxx-xxx      xxx-xxx-xxx
       10-Digit Extension:    xxx-xxx-xxxx     xxx-xxx-xxxx     xxx-xxx-xxxx
       11-Digit Extension:    xxxx-xxx-xxxx    xxxx-xxx-xxxx    xxxx-xxx-xxxx
       12-Digit Extension:    xxxxxx-xxxxxx    xxxxxx-xxxxxx    xxxxxx-xxxxxx
       13-Digit Extension:    xxxxxxxxxxxxx    xxxxxxxxxxxxx    xxxxxxxxxxxxx

Punctuation marks include '-', '.', ' ' NOTE: Blanks appear as dots on the SAT
```

Procedure

1. Log on to Windows on the ACM-SQL-BILL-1 server.
2. Open SQL Management Studio.
3. Log on with an SA account or as an account with similar permissions
4. Navigate to the **ACM_BILLING** (or **ACCCMBilling**) database.
5. Expand the database tables.
6. Right-click the **dbo.tblPreProcAction** table.
7. Click **Select Top 2000 Rows** to see if the table has been populated. See the following example:



8. If the table is empty and you need to run the script to configure delimiters for a Communication Manager system, click **New Query.**

   The system displays the New SQL Query window.

9. Using the Windows clip board, copy and paste the following lines into the new query window:

```
INSERT INTO [dbo].[tblPreProcAction]
           ([TableName]
           ,[ColumnName]
           ,[ActionFlag]
           ,[ActionCode]
           ,[ActionParam1]
           ,[ActionParam2]
           ,[ActionParam3]
           ,[ActionParam4]
           ,[ActionParam5]
           ,[DateTimeColumnName])
     VALUES
           ('Registered_Stations'
           ,'extension'
           ,'ON'
           ,'REMOVE_CHAR'
           ,'-'
           ,'.'
           ,' '
           ,null
           ,null
           ,'datetime')
GO
```

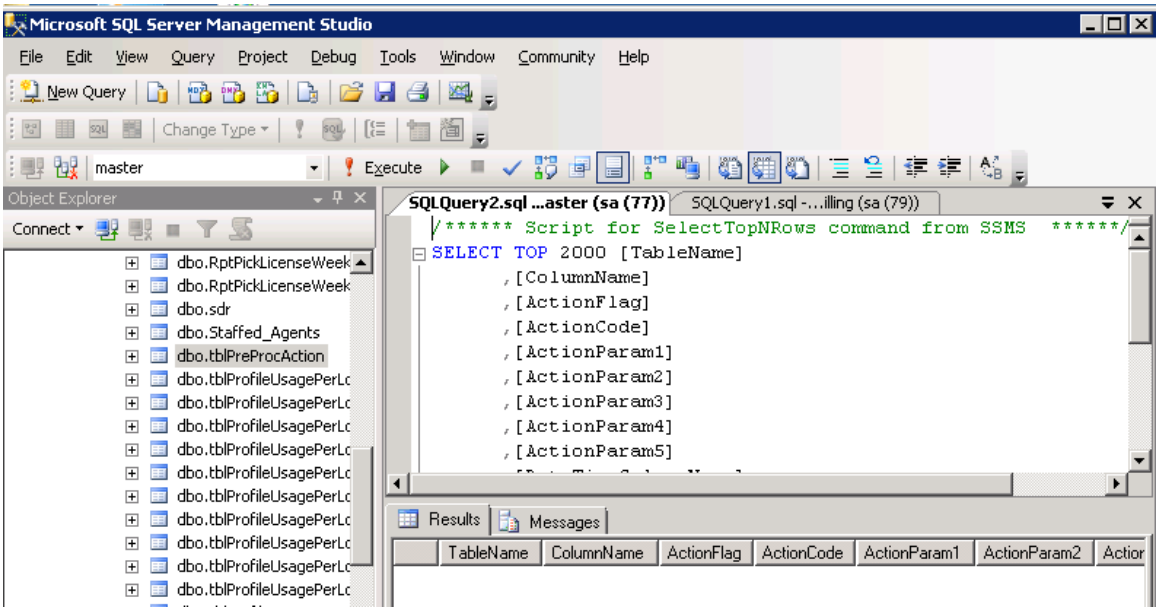
   In this example, the script configures the three default delimiters, hyphen (-), period (.), and space ( ), from the Communication Manager configuration for Communication Manager extension displays.

10. If the customer's dial plan contains any other character delimiters, add those characters to the script in the lines marked as "null".

    Note:

    You can only configure five delimiters.

11. Click **Execute** to run the script.
12. Right-click the **dbo.tblPreProcAction** table again.
13. Click **Select Top 2000 Rows** to see if the table has been populated. You should now see a display similar to the following example:



14. Repeat this procedure on the ACM-SQL-BILL-2 server.

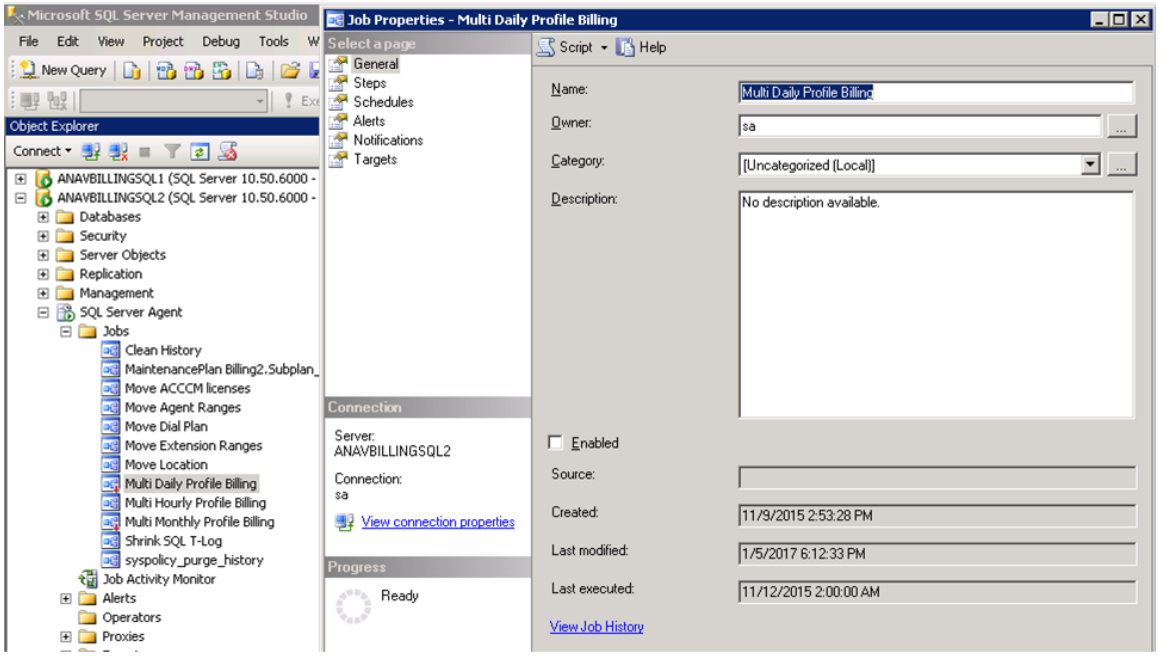
Billing configuration changes to the secondary data center

About this task

This procedure provides high-level steps to configure the billing configuration on the secondary data center. For more information, see *Failover Management for Partner Cloud Powered by Avaya xCaaS*.

Procedure

1. Disable the schedule for the Multi Daily Profile Billing job in the secondary billing database by performing the following steps:
   a. Open Microsoft SQL Management studio and connect to secondary billing database.
   b. Navigate to **SQL Server Agent** > **Jobs**.
   c. Right-click the **Multi Daily Profile Billing** job and either click **Disable** or select **Properties**. If you select **Properties**, the system displays the Job Properties – Multi Daily Profile Billing window.



d. Select **Disable** on the Job Properties – Multi Daily Profile Billing window.

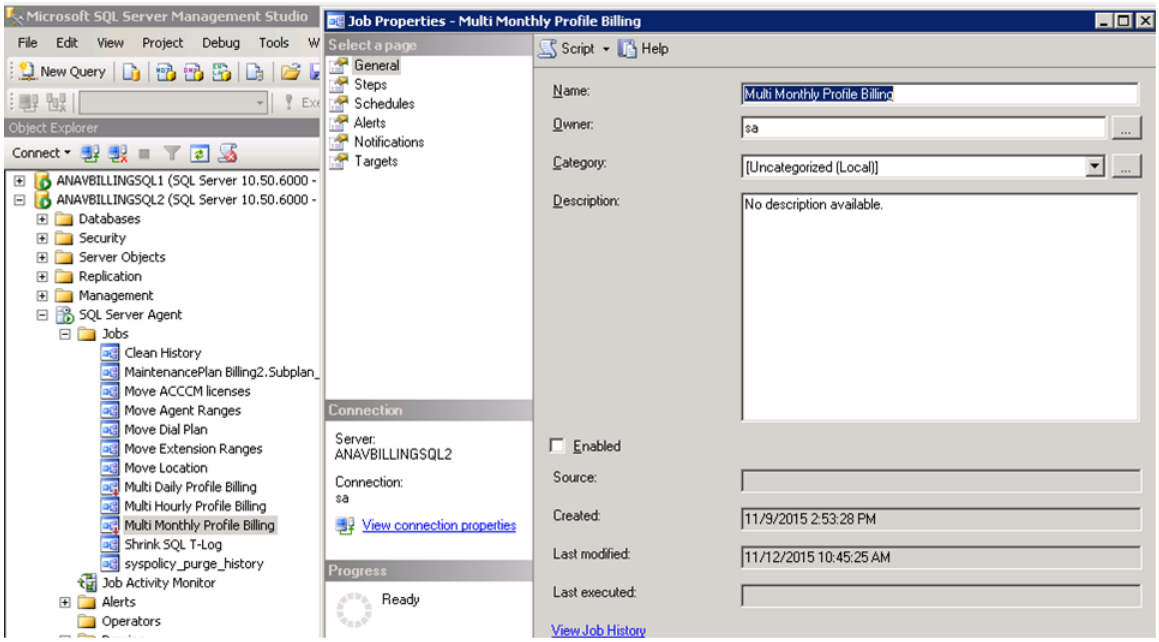
e. Click **OK** to save the changes.

2. Disable the schedule for the Multi Monthly Profile Billing job in the secondary billing database by performing the following steps:

   a. Open Microsoft SQL Management studio and connect to secondary billing database.

   b. Navigate to **SQL Server Agent** > **Jobs**.

   c. Right-click the **Multi Monthly Profile Billing** job and either click **Disable** or select **Properties**. If you select **Properties**, the system displays the Job Properties – Multi Monthly Profile Billing window.



d. Select **Disable** on the Job Properties – Multi Monthly Profile Billing window.

e. Click **OK** to save the changes.

3. Log on to the Control Manager application server in the secondary data center (ACM-APP-2) and verify that the Control Manager License Tracker Service is set to manual and is not running (that is, stopped) in the secondary application server (ACM-APP-2):

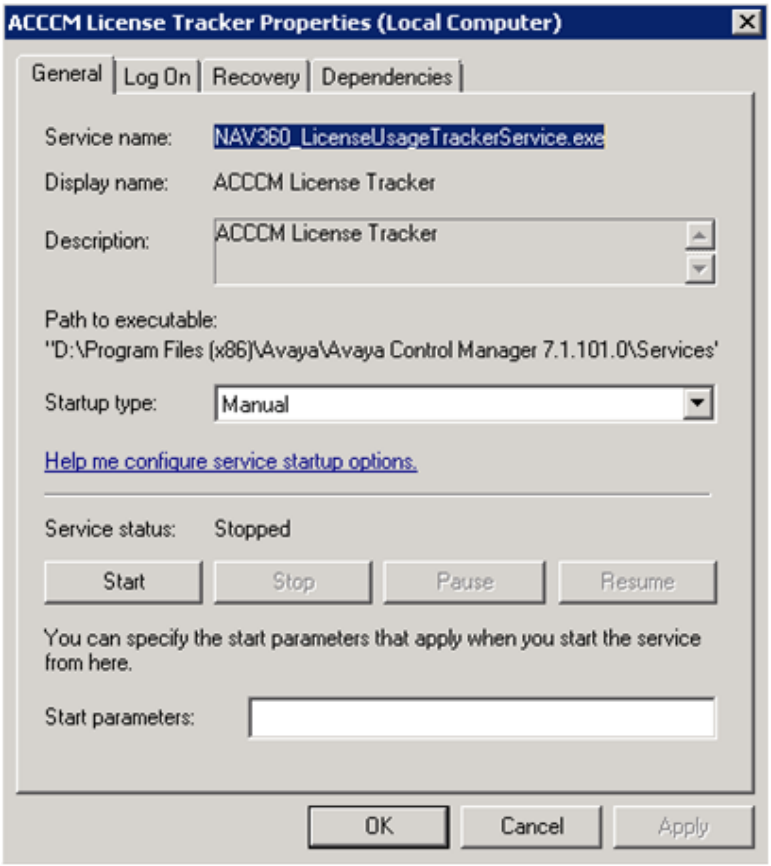
   a. Go to **Start** > **Run**.

   b. Enter `services.msc` and press **Enter**.

      The system displays a list of services.

   c. Locate the **ACCCM License Tracker** and **ACCCMAudit Log** services and verify that the **Startup Type** is set to **Manual** for both services and that the services are not running (that is, blank).

   d. If the service is not set up correctly, double-click the service name and make the appropriate changes.



Configuring the billing engine startup and recovery properties

About this task

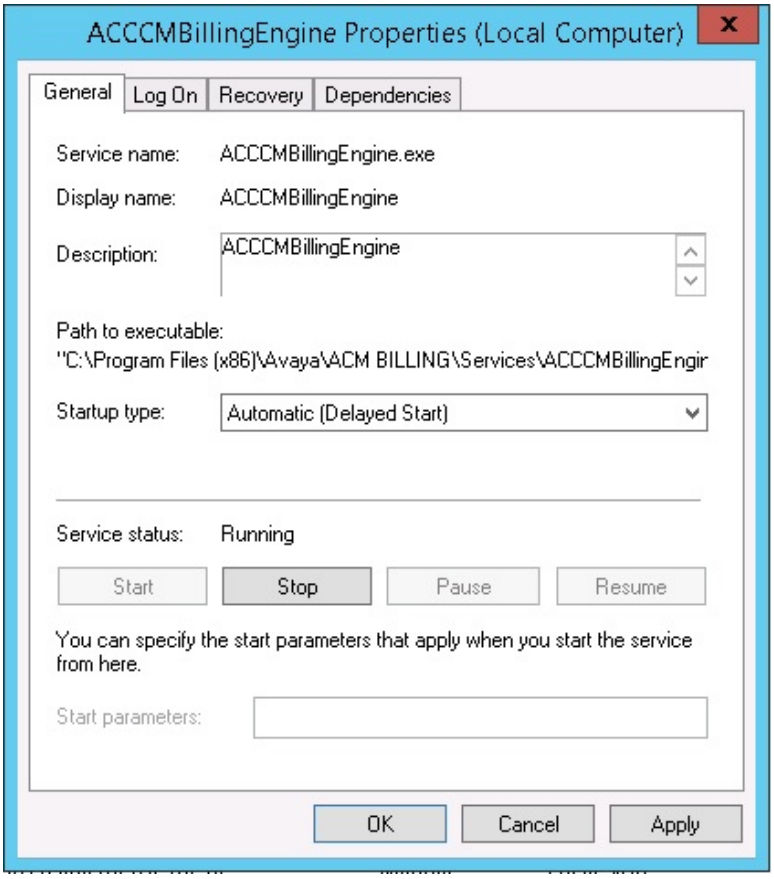
After you install the billing software, you must set the startup and recovery properties for the ACCCMBillingEngine and AAEPBilling services. These properties are used in failure recovery scenarios. You must set these properties on both the primary and secondary Control Manager application servers (ACM-APP-1 and ACM-APP-2).

Procedure

1. Log on to Windows on the primary application server (ACM-APP-1).
2. Go to **Start** > **Run**.
3. Enter `service.msc` and press **Enter**.

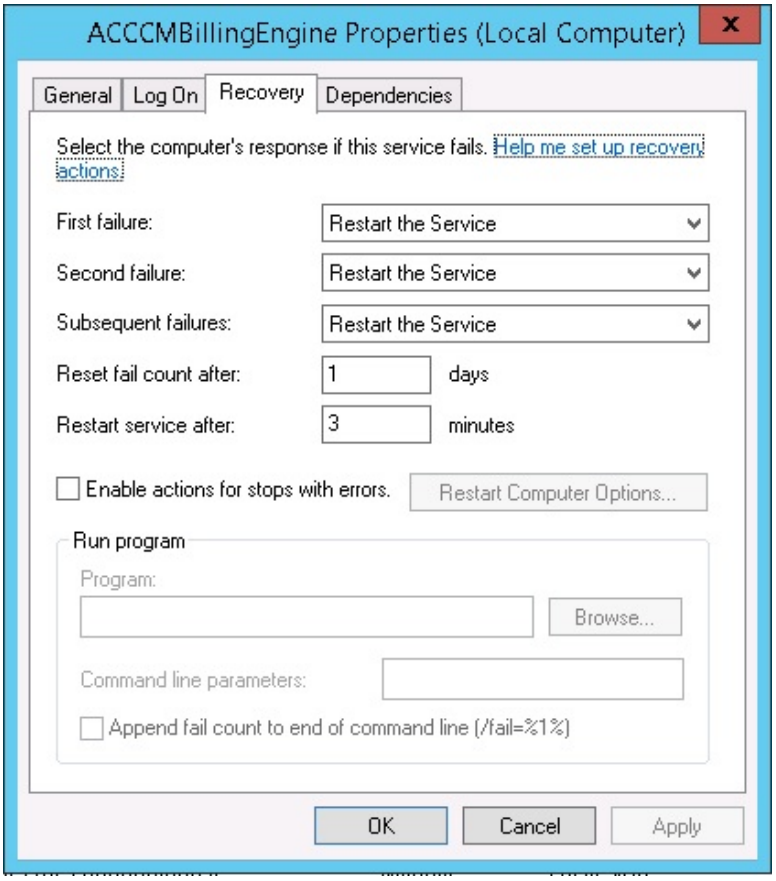
   The system displays the list of services.
4. Right-click the **ACCCMBillingEngine** service and click **Properties**.

   The system displays the following screen:



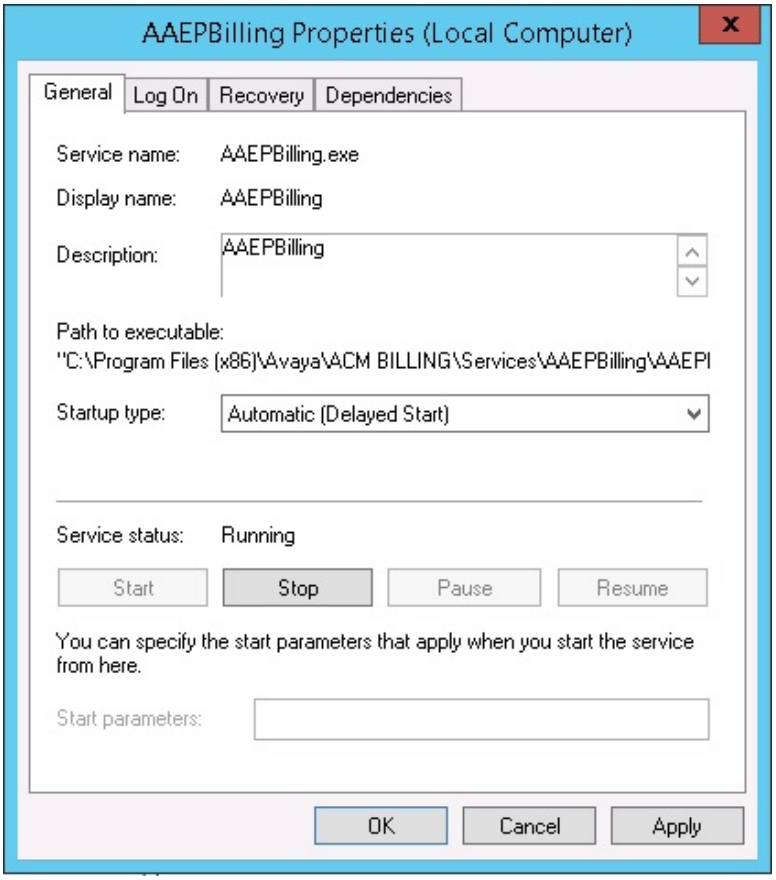
5. Set the **Startup type** option to **Automatic (Delayed Start)**.
6. Select the **Recovery** tab.

   The system displays the following screen:



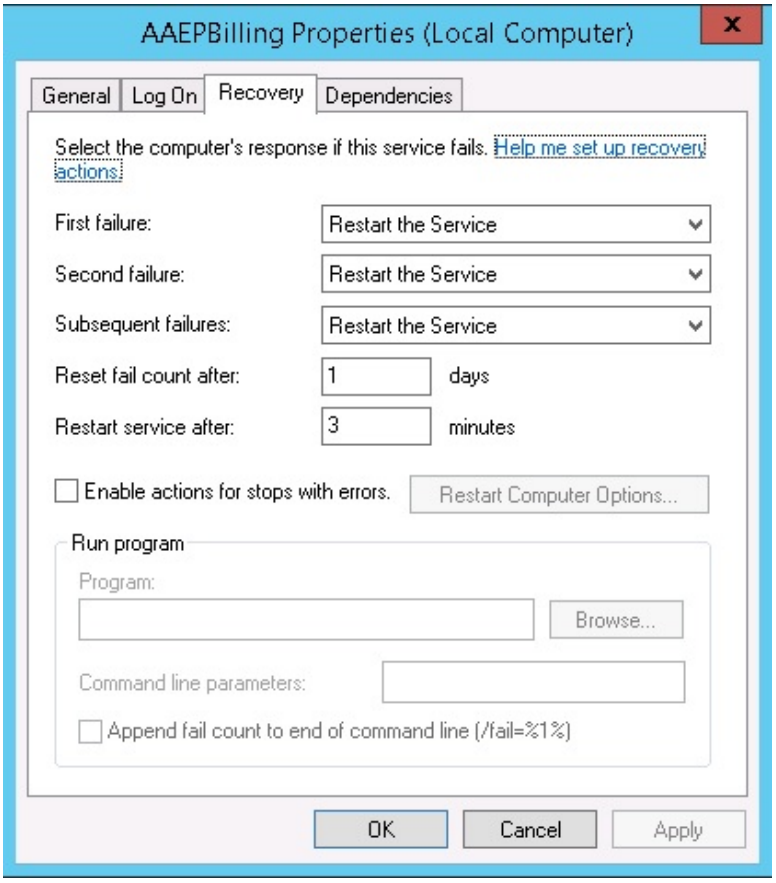
7. Administer the following options:
   - Set **First failure** to **Restart the Service**.
   - Set **Second failure** to **Restart the Service**.
   - Set **Subsequent failures** to **Restart the Service**.
   - Set **Reset fail count** after to **1**.
   - Set **Restart service after** to **3**.
8. Click **OK**.
9. Right-click the **AAEPBilling** service and click **Properties**.

   The system displays the following screen:



10. Set the **Startup type** option to **Automatic (Delayed Start)**.
11. Select the **Recovery** tab.

    The system displays the following screen:



12. Administer the following options:
    - Set **First failure** to **Restart the Service**.
    - Set **Second failure** to **Restart the Service**.
    - Set **Subsequent failures** to **Restart the Service**.
    - Set **Reset fail count** after to **1**.
    - Set **Restart service after** to **3**.
13. Click **OK**.
14. Repeat this procedure on the secondary application server (ACM-APP-2).

Testing the restore (migration)

About this task

Perform this procedure to verify that the restore was successful and that the data migration was successful.

Procedure

1. Verify that all Control Manager services are running.
2. Verify that you can log on to the Control Manager user interface. See the chapter *Testing the Control Manager installation* for more information.
3. Verify that you can use the SYNC application to perform a manual sync. See *Configuring Avaya Control Manager* for more information.

Chapter 8: Upgrading a system using an in-place upgrade

Upgrade process overview

Using an in-place upgrade is required when upgrading under the following conditions:

- The system is currently running Control Manager Release 8.0.x on any supported OS or SQL combination.
- The customer does not want to upgrade their OS or SQL software.

The upgrade process is as follows:

- The customer must use the VMware tools to take a snapshot of the old system before starting the upgrade process. Refer to VMware documentation for procedures to take a snapshot of the system.
- The customer backs up the Control Manager databases.
- The customer backs up the billing database.
- Avaya personnel download the Control Manager software.
- If you are upgrading from a Control Manager 8.0.3 system that has the 8.0.3.0.1 patch installed, Avaya personnel must uninstall the patch before upgrading the Control Manager software to 8.0.4. See the instructions for uninstalling this patch in Uninstalling Control Manager patches on page 129.
- Avaya personnel upgrade the primary application server (ACM-APP-1).
- Avaya personnel upgrade the secondary application server (ACM-APP-2).
- Avaya personnel upgrade the primary UI server (ACM-UI-1).
- Avaya personnel upgrade the secondary UI server (ACM-UI-2).
- Avaya personnel enable data replication, HA services, and failover schemes.
- Avaya personnel test the upgraded software to confirm proper operation.

Upgrade checklist

Task	✔
Plan the Control Manager upgrade with the customer.	
Read the *Avaya Control Manager Release Notes* before you start any work. Follow any special instructions for the installation or upgrade concerning required service packs, patches, and so on.	
Ensure that all product licenses are in place. When upgrading from an 8.x system, you do not need to get new license files. The software and license file for Control Manager are typically sent to the customer once the order is completed in SAP. In order to obtain the license, send a message to licenseadmin@avaya.com with the following information: • Copy of the original Purchase Order (PO) or an existing license file. • MAC address of all servers where the Control Manager software is going to be installed. **Important:** If the server has multiple NICs (Ethernet ports), you must get the MAC IDs for all NICs on the server and submit those MAC IDs when you request a license file. **Application Server** / **MAC IDs** ACM-APP-1 ACM-APP-2 ACM-UI-1 ACM-UI-2 **Note:** If all required information is included in the request, license requests are usually provided within 1 to 2 business days (Monday through Friday, not including public holidays and weekends).	
Record information about the following manually-configured parameters that might need to be reconfigured after the upgrade: • Any LDAP or SSO configuration made to configuration files that are not stored in the database or are not migrated from the old system. • Communication Manager timeout values added to Control Manager service or Web portal configuration files to compensate for network delays. • The Avaya Modular Messaging connector in an HA deployment as described in *Configuring Avaya Control Manager*.	
Download the Control Manager software package from the Avaya support site. The software package is an ISO image that you must unpack into an executable file using standard ISO unpacking tools.	

Table continues…

Task	✔
Ensure that the end user and enterprise environments can support Control Manager.	
If you are upgrading the Windows operating system from Windows 2012 to Windows 2012 R2, ensure that you have followed all steps shown in Upgrading Windows 2012 to Windows 2012 R2 on page 65.	
Ensure that you have installed and configured Communication Manager.	
Ensure that all prerequisite software for Control Manager has been installed and configured.	
If you have scanning software installed on the server, ensure that you disable the scanning software before you upgrade the Control Manager software. You can enable the scanning software after the upgrade is complete.	
If you are upgrading from a Control Manager 8.0.3 system that has the 8.0.3.0.1 patch installed, Avaya personnel must uninstall the patch before upgrading upgrade the Control Manager software to 8.0.4. See the instructions for uninstalling this patch in Uninstalling Control Manager patches on page 129.	
Confirm that the Windows time and date is set accurately before you install Control Manager software.	
Begin the upgrade process using the appropriate Control Manager software upgrade procedure that matches the customer requirements.	
Test the installation and troubleshoot any installation issues.	
Configure the Control Manager deployment with any new features added with the upgrade. For details, see *Configuring Avaya Control Manager*.	
Complete the initial administration for any new features added with the upgrade. For details, see *Using Avaya Control Manager to Administer Avaya Products*.	

Installation and upgrade considerations

Consider the following items when installing or upgrading the Control Manager software:

- Read the *Avaya Control Manager Release Notes* before you start any work. Follow any special instructions for the installation or upgrade concerning required service packs, patches, and so on. Review all of the fixed issues to note any changes that might affect the installation or upgrade.
- Do not install Windows updates on the system while installing the Control Manager software. You can either disable the Windows updates or install all the available updates before you install the Control Manager software.
- Ensure that the client system supports the minimum resolution of 1920x1080 pixels or higher to run the Web browser.
- Temporarily disable any virus software while you install the software. During operation, exclude scanning of any SQL or Control Manager folders. Reenable the virus software after you complete the installation.

- Temporarily disable JRE automatic updates on the Control Manager servers.
- Avaya recommends that you install the Control Manager software on a non-system drive. That is, not the same drive where the OS is installed, which is typically the C: drive. On the drive where you do install the Control Manager software, change the permissions of the Avaya directory and provide full control to the network account. In this case, the network account corresponds to the user of the Control Manager application pool. All other processes use the Service user name.
- Perform **`nslookup`** and reverse **`nslookup`** between all servers in the deployment. If there are any errors, check the DNS setup on the network.
- Use the PSTool program to confirm that the SID is unique for each application, UI, and database servers.
- Inform the customer that when upgrading from previous versions, any permissions which are new in the current release and were previously granted to all users (by virtue of not having a way of excluding users) are granted to all users by default. The customer must reapply permissions on the new system and revoke permissions for any users that should not have access.

Important:

The customer must agree to create a user login ID on the SQL database servers that is a member of the Sysadmin server role. This user login ID is used during installation of the Control Manager software. Create the user login ID and its password and note these items for later use. This login is used during installation only; it is not used by the application during operation.

Important:

When creating database user passwords while installing the SQL software or while upgrading the Control Manager software, the customer must agree to use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

Databases installed

In a Control Manager installation, the following Control Manager databases are installed by default:

Database	Description	Located on server
ACCCM	Stores the Control Manager system configuration.	ACM-SQL-1, ACM-SQL-2
ACCCMAVP	Stores the Experience Portal database.	ACM-SQL-1, ACM-SQL-2

Table continues…

Database	Description	Located on server
	Note: This database is installed but not used in xCaaS.	
ACCCMSYNC	Synchronizes the database between Communication Manager and Control Manager.	ACM-SQL-1, ACM-SQL-2
ACM_BILLING or ACCCMBilling	Stores the Control Manager database.	ACM-APP-1, ACM-APP-2, ACM-SQL-BILL-1, ACM-SQL-BILL-2

Important:

This document uses the database names ACM_BILLING and ACCCMBilling. If the system has been upgraded from a previous version, the database name is probably named ACCCMBilling. Regardless of which name is being used, ensure that you use the correct database name within these procedures.

Each Control Manager instance is working with the primary Control Manager database layer. The primary database server (ACM-SQL-1) for Application and the primary billing database server (ACM-SQL-BILL-1) for Billing. The primary database server (ACM-SQL-1) is replicated using a unidirectional replication mechanism with the secondary database server (ACM-SQL-2). The primary billing database server (ACM-SQL-BILL-1) is replicated using a bidirectional replication mechanism with the secondary billing database server (ACM-SQL-BILL-2).

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	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
	Portal application management database	
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. **Note:** The ACCCMCMSYSLOG database did not exist in 7.1.2.2, so there is no need to back up that database when upgrading from 7.1.2.2.
ACM_BILLING or ACCCMBilling	Stores the Control Manager billing database.	You must back up this database only if using the Control Manager Billing feature used with the xCaaS solution.

Important:

This document uses the database names ACM_BILLING and ACCCMBilling. If the system has been upgraded from a previous version, the database name is probably named ACCCMBilling. Regardless of which name is being used, ensure that you use the correct database name within these procedures.

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, you should also do backups for the following reasons:

- 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 should back up the database data in case the server becomes unusable after maintenance and you have to move the data to a new system.

Before you begin

Prior to Control Manager Release 8.x, you could rename the Control Manager databases to match any custom name that the customer might want. With Release 8.x, Control Manager requires standard fixed database names that cannot be changed.

When backing up data from an older system that might have custom database names, you must determine what the names were on the old system. If the database names were changed and do

not match the standard fixed names, you must make sure that you back up the custom databases using the custom names, but restore the database information to the standard fixed database names.

Use the following table to track any differences between the standard database names and custom database names.

Standard Database Name	Custom Database Name
ACCCM	
ACCCMAVP	
ACCCMSYNC	
ACCCMCMSYSLOG	
ACM_BILLING or ACCCMBilling	

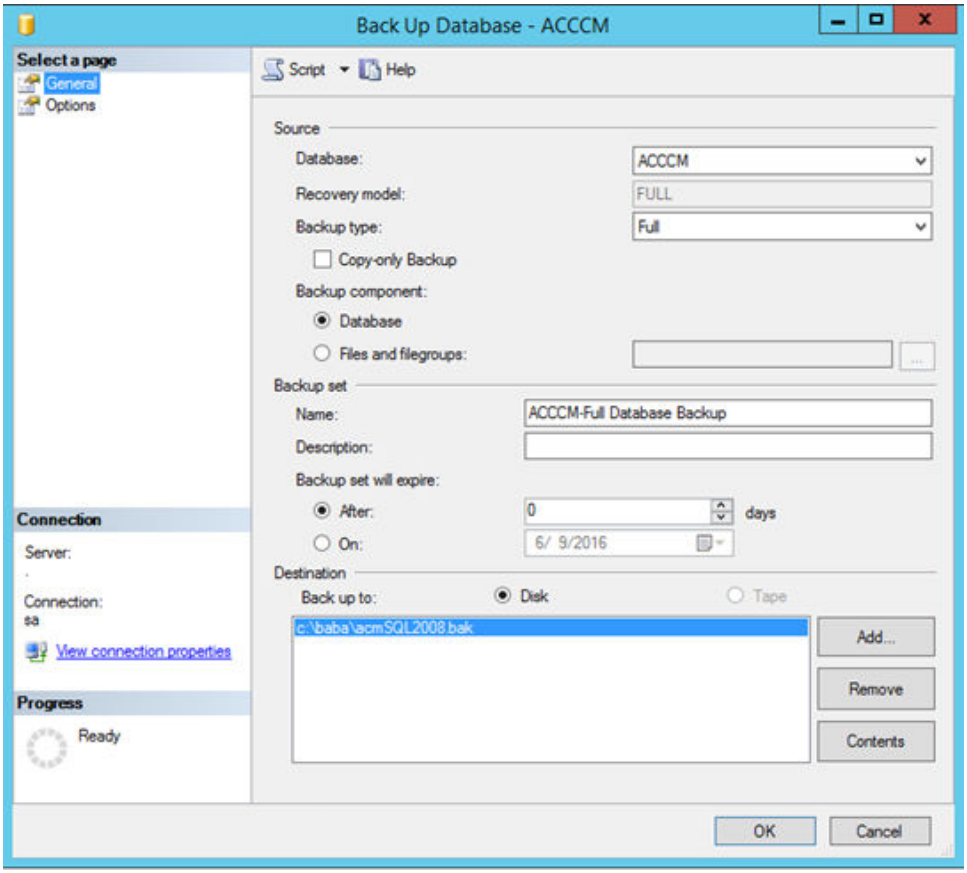
Procedure

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.
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 the other databases.

Important:

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

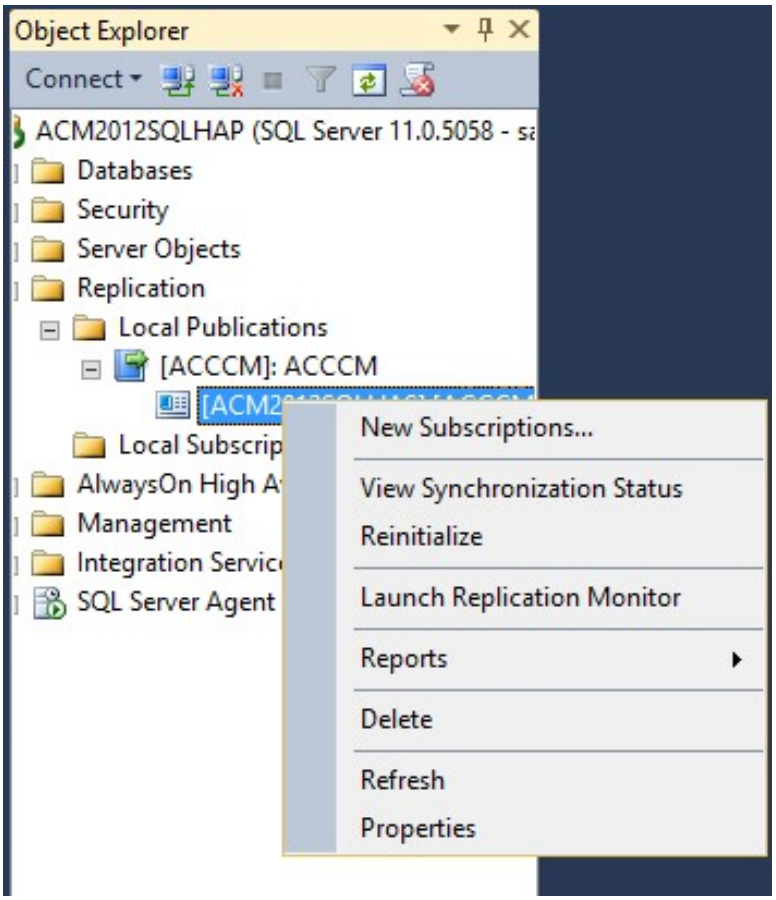
Removing replication on the SQL servers

Procedure

1. Open the SQL Server Management Studio of the primary database server, ACM-SQL-1.

The system displays the Microsoft SQL Server Management Studio screen.

2. In the Object Explorer, navigate to **Replication** > **Local Publications**.
3. Expand the publication you want to remove so you can see all of its subscriptions. See the following example:



4. Right-click the first subscription and select **Delete**.

   A warning message is shown.
5. Verify that the option to connect to the subscriber is selected and click **Yes**.
6. You will be asked to provide credentials to connect to the secondary SQL server.
7. Click **Connect** and the subscription will be removed.
8. If there is more than one subscription, repeat Steps 4-7 for each subscription.
9. When all the subscriptions are removed, right-click on the publication and select **Delete**.
10. When the dialog box comes up, select **Yes**.
11. From a new Query window in Management Studio, execute the command below to remove all the replication system objects from the database. It should be done for all replicated Control Manager databases.

```
Exec sp_removedbreplication @dbname = '{Database Name}'
```

Replication should now be completely removed from the database.

Caution:

Verify that replication is completely removed. This includes, but is not limited to, triggers on tables created by replication that start with `sp_MSsync_upd_trig_`*`TableName`* or any other element that may cause data locks on the database. Any of these triggers that have not been removed can cause an upgrade to fail.

Stopping the Control Manager services

About this task

To stop the Control Manager services, 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. Navigate to **Start** > **Run**.
3. Enter `services.msc` and press **Enter**.

   The system displays a list of services.
4. In the Services window, right-click each of the Control Manager services (those with ACCCM in the name) and the Tomcat services and select **Stop**.

   Important:

   Open Windows Task Manager and check the **Services** tab to verify that all Control Manager services are stopped. Check the **Details** tab to verify that no files or folders are locked. If any executables or services are still up on any of the Control Manager folders, right-click the item and end the process.
5. Repeat this procedure on all servers that have Control Manager software.

Uninstalling Control Manager patches

About this task

Use this procedure to uninstall the Control Manager 8.0.3.0.1 patch before you upgrade the Control Manager software to 8.0.4.

Important:

You can skip this procedure when upgrading from Control Manager 8.0.1.x or 8.0.2.x. There are no patches on these releases that you must uninstall.

Before you begin

Download the Control Manager 8.0.3.0.1 patch installation zip file from the Avaya support site and copy it to every server from which you are uninstalling a patch. Unzip the downloaded file to a location you can access (for example, the desktop). Using the MD5 Checksum, verify the data integrity of the downloaded file before you start the uninstall process.

Verify that the customer has used VMware tools to take a snapshot of the old system before starting the uninstall process. Customers must refer to VMware documentation for procedures to take a snapshot of the system.

Verify that the customer has backed up all Control Manager databases as shown in Control Manager databases that require backup on page 72 and Backing up Control Manager databases on page 73.

Procedure

1. Remove replication as shown in Removing replication on the SQL servers on page 127.
2. Stop all Control Manager services as shown in Stopping the Control Manager services on page 129.
3. Log on to the server.
4. Open Windows Explorer and locate the patch installation program `PatchInstaller.exe`.
5. Right-click the patch installation program and select **Run as Administrator**.

   The system displays the patch installation program. The system automatically recognizes that the 8.0.3.0.1 patch was previously installed.
6. Enter the database user name and password. These credentials were used when you previously installed Control Manager.
7. Click **Uninstall**.

   The system begins the patch uninstallation procedure.
8. Follow the on-screen prompts to uninstall the 8.0.3.0.1 patch.
9. Repeat this procedure for all other servers in the deployment that have Control Manager software.

Next steps

Continue with the Control Manager software upgrade.

Upgrading Control Manager software in an HA configuration

About this task

Use this procedure if you are upgrading an HA configuration for any of the following Control Manager releases:

- 8.0.1.x
- 8.0.2.x
- 8.0.3.x

You must upgrade the Control Manager servers in the following order:

- Primary application server, ACM-APP-1
- Secondary application server, ACM-APP-2
- Primary UI server, ACM-UI-1
- Secondary UI server, ACM-UI-2

Before you begin

Download the Control Manager software from the Avaya support site and copy it to every server where you are installing the software. The software package is an ISO image that you must unpack into an executable file using standard ISO unpacking tools. Using the MD5 Checksum, verify the data integrity of the downloaded file before you start the installation.

Because this release of Control Manager has specific password length and character requirements, and that the same password is used for all databases, passwords from older systems may not meet those requirements for an upgrade. If this upgrade incompatibility exists, you must first log on to the SQL system and change the passwords to a compatible version before starting the upgrade.

Important:

When creating database user passwords while installing the SQL software, the customer must use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

Ensure that the client system supports the minimum resolution of 1920x1080 pixels or higher to run the Web browser.

Verify that the .NET 4.5.2 software has been install before you attempt to install the Control Manager software.

Confirm that the Windows time and date is set accurately before you install Control Manager software.

Note:

For installation wizard logging, ensure that you have full administrative rights to access the server and to create files on the drive where you install the Control Manager software. You must initiate the installation by choosing the **Run as Administrator** option.

Note:

The Control Manager installation setup appends the installation logs to the following log file:

`InstallDrive:\acccminstallerVersionNumber.BuildNumber.log`

Caution:

Host names of Control Manager application and UI servers must only contain alphabetic letters and numbers and are limited to a length of 15 characters. Host names cannot contain any special characters, such as hyphens (-) or underscores (_). Confirm that you are using a valid host name before you install the Control Manager software because you cannot change the host name after installing the Control Manager software.

Host names of Control Manager database servers must follow the requirements set forth by Microsoft in the following article:

https://support.microsoft.com/en-us/help/909264/

Procedure

1. Log on to the server.
2. Open Windows Explorer and locate the Control Manager software you downloaded from the Avaya support site.
3. 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`

   The system starts the installation. Depending on whether this is a first-time new installation, a reinstallation, or an upgrade, the system displays one or more of the following screens:

   - **Welcome to the Prerequisites Wizard** — If the system displays this screen, you will step through one or two more prerequisites screens where software might be installed on your system. Click **Next** to advance to the next screen.
   - **License Agreement** — If the system displays this screen, select **I accept the terms in the License Agreement** and click **Next**. You may see additional prerequisites screens after the **License Agreement** screen. 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 will see before configuring the installation parameters.
4. Click **Next**.

   The system displays the **Install Mode** screen.
5. On the Install Mode screen, select **Service Provider**.
6. Click **Next**.

   The system displays the **Installation Type** screen.

7. Administer the following parameters:
   - **Installation Type** — Select the release you are upgrading from.
   - Select the **High Availability** option.
8. Click **Next**.

   The system displays the **Server Type** screen.

   Important:

   If you are deploying UM Collector software in a VMware HA configuration or in a non-production lab system, the system displays the **Distribution Setup** screen instead of the **Server Type** screen. Set the **Distribution Type** parameter to **All** and click **Next** to continue with the **SQL and ACM Database screen**.
9. For the primary server, configure the following parameters:
   - **Server Role** — Select **Primary Server**.
   - **HA Mode** — Select **Standard**.
   - **Distribution Type** — Select **UI** if the deployment has a dedicated UI server. Select **Services** if the deployment has a combined application and UI server.
   - **Primary Application Server Name** — Enter the host name or IP address of the primary application server. Do not use the FQDN of the server.
   - **Primary UI Server Name** — Enter the host name or IP address of the primary UI server. If you are using a three-server configuration without a dedicated UI server, enter the host name or IP address of the primary application server. Do not use the FQDN of the server.
   - **Secondary Application Server Name** — Enter the host name or IP address of the secondary application server. Do not use the FQDN of the server.
   - **Secondary UI Server Name** — Enter the host name or IP address of the secondary UI server. If you are using a three-server configuration without a dedicated UI server, enter the host name or IP address of the secondary application server. Do not use the FQDN of the server.
10. Click **Next**.

    The system displays the **SQL and ACM Database** screen.
11. For the SQL and Control Manager (ACM) database, configure the following parameters:
    - In the **SQL Server** and **SQL Port** fields, you can enter the information in several different formats using simple host names and TCP port numbers, IPv4 addresses, and named instances. See the following examples:

      Host Name in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

Host Name\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

IPv4 Address\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

Note:

You cannot use an FQDN in the **SQL Server** field.

- **SQL Admin Username** – Enter the name of a login that has Sysadmin rights on the database server.
- **SQL Admin Password** – Enter the password for the user entered in the Username field.
- **ACM DB Password** – Do one of the following steps:
  - For a new installation, enter a password for the Control Manager databases. The password you enter here is used for all of the Control Manager databases created during installation.
  - For an upgrade, enter the password for the Control Manager databases that was assigned on the old system.

Important:

Because this release of Control Manager has specific password length and character requirements, and that the same password is used for all databases, passwords from older systems may not meet those requirements for an upgrade. If this upgrade incompatibility exists, you must first log on to the SQL system and change the passwords to a compatible version before starting the upgrade.

Important:

When creating database user passwords while installing the SQL software, the customer must use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

12. Click **Next**.

    Depending on where you are in the upgrade process, the system displays Primary SQL Server screen or the Secondary SQL Server screen.

13. For the primary SQL server, configure the following parameters:

    - In the **Primary SQL Server** and **SQL Port** fields, you can enter the information in several different formats using simple host names and TCP port numbers, IPv4 addresses, and named instances. See the following examples:

      Host Name in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

Host Name\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

IPv4 Address\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

Note:

You cannot use an FQDN in the **SQL Server** field.

- **SQL Admin Username** – Enter the name of a login that has Sysadmin rights on the database server.
- **SQL Admin Password** – Enter the password for the user entered in the Username field.
- **ACM DB Password** – Do one of the following steps:
  - For a new installation, enter a password for the Control Manager databases. The password you enter here is used for all of the Control Manager databases created during installation.
  - For an upgrade, enter the password for the Control Manager database that was assigned on the old system.

Important:

Because this release of Control Manager has specific password length and character requirements, and that the same password is used for all databases, passwords from older systems may not meet those requirements during an upgrade. If this upgrade incompatibility occurs, you must log on to the SQL system and change the passwords to a compatible version before continuing with the upgrade.

Important:

When creating database user passwords while installing the SQL software, the customer must use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

14. For the secondary SQL server, configure the following parameters:
    - In the **Secondary SQL** and **SQL Port** fields, you can enter the information in several different formats using simple host names and TCP port numbers, IPv4 addresses, and named instances. See the following examples:

      Host Name in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      IPv4 Address in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

      Host Name\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

IPv4 Address\Named Instance in the **SQL Server** field and the TCP port number for the SQL database in the **SQL Port** field.

Note:

You cannot use an FQDN in the **SQL Server** field.

- **SQL Admin Username** – Enter the name of a login that has Sysadmin rights on the database server.
- **SQL Admin Password** – Enter the password for the user entered in the Username field.
- **ACM DB Password** – Do one of the following steps:
  - For a new installation, enter a password for the Control Manager databases. The password you enter here is used for all of the Control Manager databases created during installation.
  - For an upgrade, enter the password for the Control Manager databases that was assigned on the old system.

Important:

Because this release of Control Manager has specific password length and character requirements, and that the same password is used for all databases, passwords from older systems may not meet those requirements for an upgrade. If this upgrade incompatibility exists, you must first log on to the SQL system and change the passwords to a compatible version before starting the upgrade.

Important:

When creating database user passwords while installing the SQL software, the customer must use passwords that are 8-14 alphanumeric characters long, with upper case and lower case letters. Because of limitations with the Control Manager installation software, the customer must not use long and complex database passwords.

15. Click **Next**.

Note:

The installation software uses ODBC to test the database connection using the connection details administered in the previous dialog. If the test is successful, the installation program continues. If the test is not successful, you must go back and fix the incorrect connection details.

The system displays the **Select Installation Folder** screen.

16. Click **Browse**.
17. Browse to the location where you want to install the Control Manager software.

    Avaya recommends that you install the Control Manager software on a non-system drive. That is, not the same drive where the OS is installed, which is typically the C: drive.

18. After you select the install location, click **OK**.
19. Click **Next**.

    The system displays the **Configure Language and License** screen.
20. Configure the following parameters:
    - **System Language** – Select the language you want the Control Manager user interface to use as the default language. Individual users can select a different language when they log on, but this option sets the default language.
    - **License File** — Click **Load License**, browse to the location of the Control Manager license file you requested before starting the installation, select the license file, and click **Open**. The system closes the dialog box indicating the successful license upload.

      Important:

      The license file must be named:

      `license.lic`

      If you did not get the license file before you began installing the Control Manager software, you can install it later using the procedures found in Getting Control Manager licenses on page 23 and Installing Control Manager licenses on page 101.
21. Click **Next**.

    The system displays the **Ready to Install** screen.
22. You can review or change the installation settings by clicking **Back** repeatedly to step through all of the screens.
23. Click **Install** to begin the installation.

    The installation process can take up to an hour, depending on how many components the system must install.

    During the software installation, the system displays the **Installing Avaya Control Manager** screen.

    Upon successful installation, the system displays the **Completing the Avaya Control Manager Setup Wizard** screen.
24. Click **Finish** to close the installation wizard.
25. Restart the server.
26. Repeat this procedure on the secondary application server, the primary UI server, and the secondary UI server.

Next steps

Readminister replication and HA services as described in the chapter *Configuring replication* and the chapter *Configuring HA Services*.

To verify the installation, see the chapter *Testing the Control Manager installation*.

Installing Control Manager licenses

About this task

You must get install licenses for Control Manager under the following conditions:

- New installations.
- When upgrading (migrating) from any Release 7.x system.

You do not have to install a new license when upgrading from one version of 8.0.x to another version of 8.0.x, for example, 8.0.1 to 8.0.3.

Licenses for Control Manager software can be installed at the same time you install the Control Manager software. However, if you do not have a license file when you install the Control Manager software, you must install the license file after you install the Control Manager software before the system will be operational. Without valid license files, the license service will not start and no users will be able to log on to the Control Manager user interface.

Procedure

1. Get your license files as described in Getting Control Manager licenses on page 23.
2. Log on to one of the server(s) that for which you received a license file.
3. Copy the license file to the following location on the servers:

   `[Install Location]\Services\ACCCM License Server`

   Important:

   The license file must be named `license.lic`.
4. Reboot the server.
5. Log on to each of the server(s) that for which you received a license file.
6. Go to **Start** > **Run**.
7. Enter **`services.msc`** and press **Enter**.

   Note:

   The license server must start before any other services are started.
8. In the Services window, confirm that the **ACCCM License Server** service has started.
9. If the **ACCCM License Server** has not started, right-click **ACCCM License Server** and select **Start**.

   The system starts the service.
10. If the service fails to start, verify the service log files for details on any errors. The default location of the License Server log file is:

    `[Install Location]\Services\ACCCM License Server\logs`
11. Repeat this procedure for every server that requires a license file.

Upgrading the Control Manager billing software

Uninstalling the billing software

About this task

When upgrading the billing software, you must first uninstall the previous version of the software.

Procedure

1. Log on to Windows on one of the Control Manager servers.
2. Navigate to **Start** > **Run**.
3. Enter `services.msc` and press **Enter**.

   The system displays a list of services.
4. In the Services window, right-click the **AAEP Billing Service** and **CM Billing Service** and select **Stop**.
5. Navigate to **Start** > **Control Panel** > **Programs and Features**.
6. On the Uninstall or change a program screen, right-click the **ACM Billing** program and click **Uninstall**.

   The system removes the selected component from the server.
7. Repeat this procedure on all servers that have Control Manager software.

Installing billing software on the Control Manager servers

Important:

When deploying xCaaS with Usage Metering (UM) Collector software, you can skip this entire chapter.

About this task

You must install the Control Manager Billing software on the following servers depending on your configuration:

- For the standard four-server configuration, you must install the Control Manager Billing software on the primary and secondary application servers (ACM-APP-1 and ACM-APP-2), the primary and secondary UI servers (ACM-UI-1 and ACM-UI-2), and the primary and secondary billing servers (ACM-SQL-BILL-1 and ACM-SQL-BILL-2).
- For the three-server configuration, you must install the Control Manager Billing software on the combined primary and secondary application/UI servers (ACM-APP-1 and ACM-APP-2) and the primary and secondary billing servers (ACM-SQL-BILL-1 and ACM-SQL-BILL-2).

Before you begin

Verify that the following servers are installed:

- The billing database servers installed with a supported version of Microsoft SQL Standard or Enterprise database software with SSRS.
- The Control Manager database servers installed with a supported version of Microsoft SQL database software.

Download the Control Manager software from the Avaya support site. Copy the software to every server where you are installing the software. The billing software is an executable file packaged within the Control Manager ISO image. You must unpack the ISO image into an executable file using standard ISO unpacking tools. This download may include patches for the billing software which must be installed after installing the core billing software.

Procedure

1. Log on to the server.
2. Open Windows Explorer and locate the Control Manager billing software files you downloaded from the Avaya support site.
3. Right-click the Control Manager executable file and select **Run as Administrator**. The name of the file is similar to the following example:

   `ACM BILLING_ReleaseNumber_BuildNumber.exe`

   The system starts the installation and displays the **License Agreement** screen.
4. Select **I accept the terms in the License Agreement**.
5. Click **Next**.

   The system displays the **Prerequisites** screen.

   By default, the system checks for preinstalled components as prerequisites. If the prerequisite installation components exist in the system, the installation wizard skips the installation of existing prerequisite installation setup. If one or more component is missing, the installation wizard installs the missing components as part of the installation process.
6. Do one of the following steps:
   - If one or more of the prerequisites are selected and need to be installed, click **Next** and the system installs the prerequisite software.
   - If none of the prerequisites are selected, click **Finish**.

   The system displays the **Welcome to the ACM Billing Setup Wizard** screen.
7. Click **Next**.

   The system displays the **Configure how ACM BILLING** will be installed screen.
8. Select the following features based on the server where you are installing the billing software:

Important:

Do not uncheck the **MainFeature** menu item to deselect features. Deselect features one at a time.

- Application servers (ACM-APP-1 and ACM-APP-2) on a standard four-server configuration — Select the following features: **Services** > **AAEPBilling**, **Services** > **ACCCMBillingEngine**, **DB Scripts** > **BillingDB**, and **DB Scripts** > **ACMDB**. Leave all other features deselected.
- UI servers (ACM-UI-1 and ACM-UI-2) on a standard four-server configuration — Select the following features: **Web**. Leave all other features deselected.
- Combined application/UI servers (ACM-APP-1 and ACM-APP-2) on a three-server configuration — Select all of the features except for **Services** > **BillingReports**
- Billing database servers (ACM-SQL-BILL-1 and ACM-SQL-BILL-2) — Select the following features: **Services** > **BillingReports**. Leave all other features deselected.

9. Click **Next**.

   The system displays the **Installation Type** screen.

10. In **Select the Type of Deployment**, select **New Installation**.
11. Click **Next**.

    The system displays the **Avaya ACM Billing Database** screen.

12. Administer the following parameters:
    - **Server Name** – Enter the host name of the primary or secondary server. Do not use the FQDN of the server. You can use the IP address of the server.
    - **Port** – Enter the port number for the connection the SQL billing server. The default port number is 1433.
    - **Database Name** – Enter the Control Manager Billing database name, ACM_BILLING.

      Important:

      When upgrading from a previous Control Manager release, ensure that you select the name of the database migrated from the previous system.

    - **Username** – Enter the database user ID that was created for the installation. The user ID is used for connecting to the SQL database server.
    - **Password** – Enter the password of the user.

    Important:

    Use the SQL Server Management Studio tool to confirm that any user name and password combination used here are able to access the SQL server.

13. Click **Next**.

    The system displays the **Avaya ACM Database** screen.

14. Administer the following parameters:
    - **Server Name** – Enter the host name of the primary or secondary database server (ACM-SQL-1 or ACM-SQL-2). Do not use the FQDN of the server. You can use the IP address of the server.
    - **Port** – Enter the port number of SQL database server. The SQL database server uses 1433 as the default port.
    - **Database Name** – Enter the Control Manager database name, ACCCM.
    - **Username** – Enter the database user ID that was created for the installation. The user ID is used for connecting to the SQL database server.
    - **Password** – Enter the password of the user.

    Important:

    Use the SQL Server Management Studio tool to confirm that any user name and password combination used here are able to access the SQL server.
15. Click **Next**.

    The system displays the **Avaya ACM Billing Login User** screen.
16. Enter the user name and password used to access the Control Manager billing system. This creates an SQL Server login ID in the existing Control Manager SQL Server and database user for the existing Control Manager database, with the database role set to “db_reader” only. This login ID for the Linked Server is used to retrieve data from the distributed Control Manager SQL server.

    Important:

    Use the SQL Server Management Studio tool to confirm that any user name and password combination used here are able to access the SQL server.
17. Click **Next**.

    The system displays the **Ready to Install** screen.
18. You can review or change the installation settings by clicking **Back** repeatedly to step through all of the screens.
19. Click **Install** to begin the installation.

    Upon successful installation, the system displays the **Completing the ACM BILLING Setup Wizard** screen.
20. Click **Finish** to close the installation wizard.
21. Repeat this procedure on the rest of the application servers, the UI servers, and the billing servers.

Next steps

Install any billing software patches included with the download.

To verify the installation, see the chapter *Testing the Control Manager installation*.

Configuring the billing software

About this task

After you install the billing software on the application servers, you must configure the `isStationEnabled` parameter in the `BillingEngineConfig.xml` file. You must do this so that Communication Manager stations are not queried during the billing process.

Procedure

1. Log on to Windows on the ACM-APP-1 primary application server.
2. Go to the following folder:

   `<InstallationDrive>:\Program Files (x86)\Avaya\ACM BILLING\Services\ACCCMBillingEngine`

3. Open the `BillingEngineConfig.xml` file for editing.
4. Change the `<isStationEnabled>` option to `False`. See the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<configurations>
        <!-- connection string of ACCCM Billing database -->
    <connectionString>Data Source=10.10.7.175;Initial Catalog=ACCCMBilling;User ID=sa;Password=I9OsdaObBwrqmtulpL/3wQ==</connectionString>
        <!-- synchronize with cm will be in seconds -->
    <intervalperiodsec>300</intervalperiodsec>
        <!-- protocol telnet: 0, ssh: 1-->
    <protocol>0</protocol>
        <!-- port 5022, 5023 -->
    <port>5022</port>
        <!-- time in seconds that the system waiting for response from CM -->
    <cmcalltimeout>180</cmcalltimeout>
        <!-- time in seconds between sending request to same CM in same iteration (time between getting agents and station lists) -->
    <timeintervalbetweensamecmcalls>6</timeintervalbetweensamecmcalls>
        <!-- True/False. True - if need to synchronize stations from CM. -->
    <isStationEnabled>False</isStationEnabled>
        <!-- connection string of ACCCM Billing database -->
        <!-- synchronize with cm will be in seconds -->
        <!-- protocol telnet: 0, ssh: 1 -->
        <!-- port 5022, 5023 -->
        <!-- time in seconds that the system waiting for response from CM -->
        <!-- time in seconds between sending request to same CM in same iteration (time between getting agents and station lists) -->
        <!-- True/False. True - if need to synchronize stations from CM. -->
</configurations>
```

5. Save and close the file.
6. Repeat this procedure on the ACM-APP-2 secondary application server.

Configuring extension number delimiters to support billing count accuracy

About this task

To enable proper billing counts for agents that are provisioned with the Avaya one-X® Agent telecommuter or road warrior station types that use special character delimiters (punctuation) in the extension numbers, you must use a script that removes those delimiters from the data sent to the Control Manager billing software. The procedure shown here configures the most common delimiters, which are hyphen (-), period (.), and an empty space ( ). If the customer's Communication Manager system uses other delimiters, add those delimiters to the script when you create and run the script. You can only add five delimiters to the script. If the customer later adds more delimiters to extensions, you must run the script again.

You must perform this procedure on both the ACM-SQL-BILL-1 and ACM-SQL-BILL-2 servers.

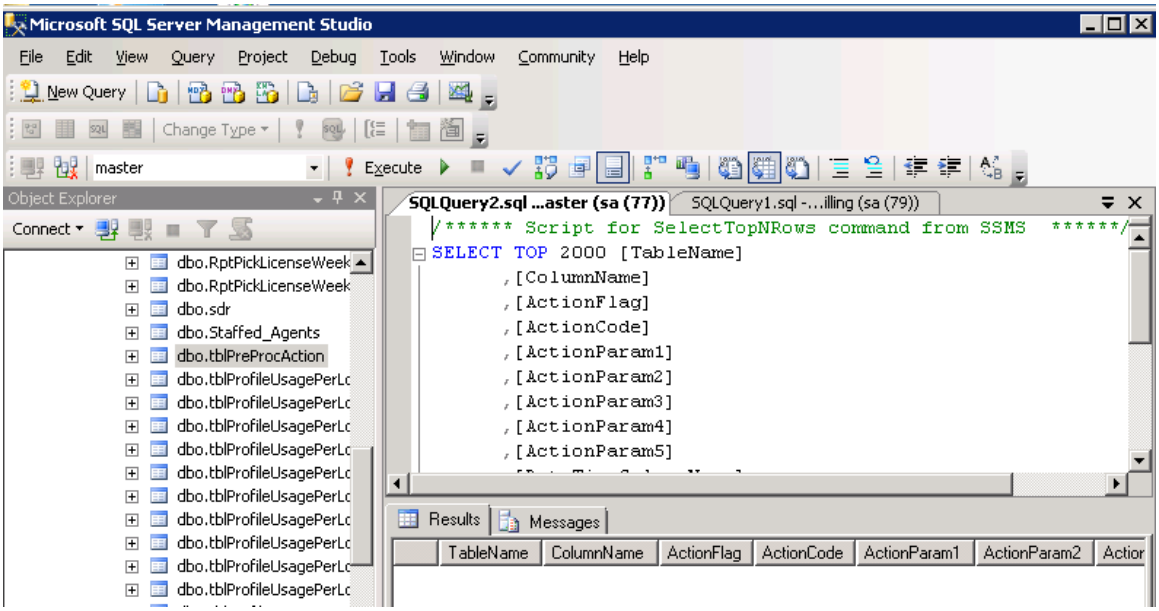
Before you begin

Check the dial plan on every Communication Manager system being used and determine all of the delimiters used in the dial plan. See the following example of a dial plan on Communication Manager:

```
change dialplan parameters                                      Page   1 of   1
                             DIAL PLAN PARAMETERS

                Local Node Number: __                   ETA Node Number: ___
   UDP-ARS Calls Considered Offnet? n               ETA Routing Pattern: ____
        UDP Extension Search Order: local-extensions-first



Retry ARS/AAR Analysis If All-Location Entry Inaccessible? n

 EXTENSION DISPLAY FORMATS
                             SAT             Inter-Location  Intra-Location
        6-Digit Extension:   xx.xx.xx        xx.xx.xx        xx.xx.xx
        7-Digit Extension:   xxx-xxxx        xxx-xxxx        xxx-xxxx
        8-Digit Extension:   xx.xx.xx.xx     xx.xx.xx.xx     xx.xx.xx.xx
        9-Digit Extension:   xxx-xxx-xxx     xxx-xxx-xxx     xxx-xxx-xxx
       10-Digit Extension:   xxx-xxx-xxxx    xxx-xxx-xxxx    xxx-xxx-xxxx
       11-Digit Extension:   xxxx-xxx-xxxx   xxxx-xxx-xxxx   xxxx-xxx-xxxx
       12-Digit Extension:   xxxxxx-xxxxxx   xxxxxx-xxxxxx   xxxxxx-xxxxxx
       13-Digit Extension:   xxxxxxxxxxxxx   xxxxxxxxxxxxx   xxxxxxxxxxxxx

Punctuation marks include '-', '.', ' ' NOTE: Blanks appear as dots on the SAT
```

Procedure

1. Log on to Windows on the ACM-SQL-BILL-1 server.
2. Open SQL Management Studio.
3. Log on with an SA account or as an account with similar permissions
4. Navigate to the **ACM_BILLING** (or **ACCCMBilling**) database.
5. Expand the database tables.
6. Right-click the **dbo.tblPreProcAction** table.
7. Click **Select Top 2000 Rows** to see if the table has been populated. See the following example:



8. If the table is empty and you need to run the script to configure delimiters for a Communication Manager system, click **New Query.**

   The system displays the New SQL Query window.

9. Using the Windows clip board, copy and paste the following lines into the new query window:

```
INSERT INTO [dbo].[tblPreProcAction]
           ([TableName]
           ,[ColumnName]
           ,[ActionFlag]
           ,[ActionCode]
           ,[ActionParam1]
           ,[ActionParam2]
           ,[ActionParam3]
           ,[ActionParam4]
           ,[ActionParam5]
           ,[DateTimeColumnName])
     VALUES
           ('Registered_Stations'
           ,'extension'
           ,'ON'
           ,'REMOVE_CHAR'
           ,'-'
           ,'.'
           ,' '
           ,null
           ,null
           ,'datetime')
GO
```

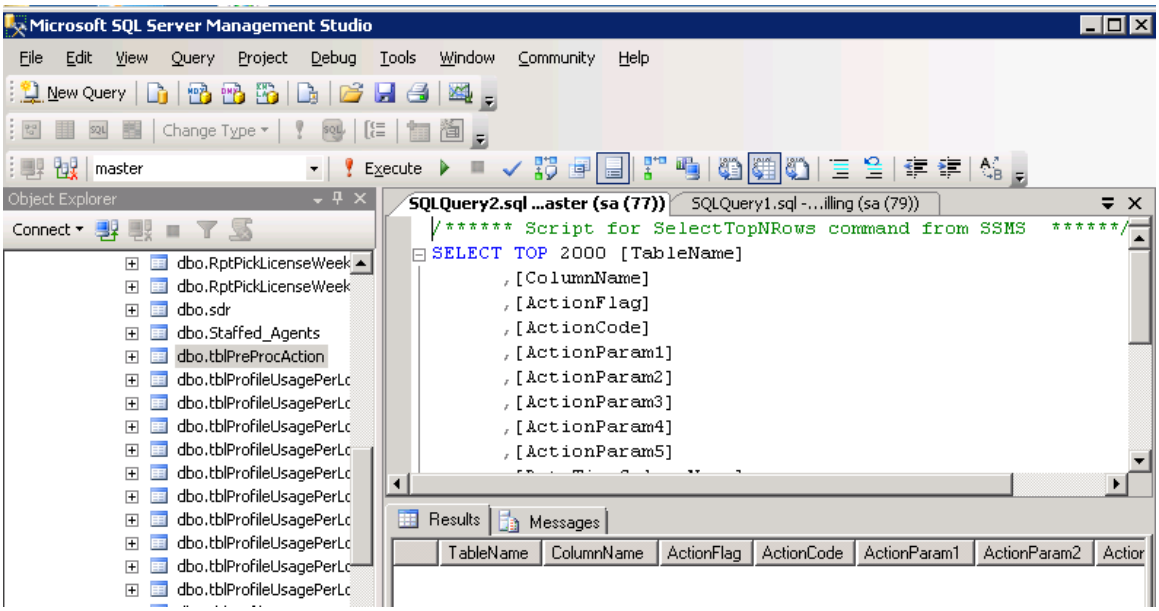
   In this example, the script configures the three default delimiters, hyphen (-), period (.), and space ( ), from the Communication Manager configuration for Communication Manager extension displays.

10. If the customer's dial plan contains any other character delimiters, add those characters to the script in the lines marked as "null".

Note:

You can only configure five delimiters.

11. Click **Execute** to run the script.
12. Right-click the **dbo.tblPreProcAction** table again.
13. Click **Select Top 2000 Rows** to see if the table has been populated. You should now see a display similar to the following example:



14. Repeat this procedure on the ACM-SQL-BILL-2 server.

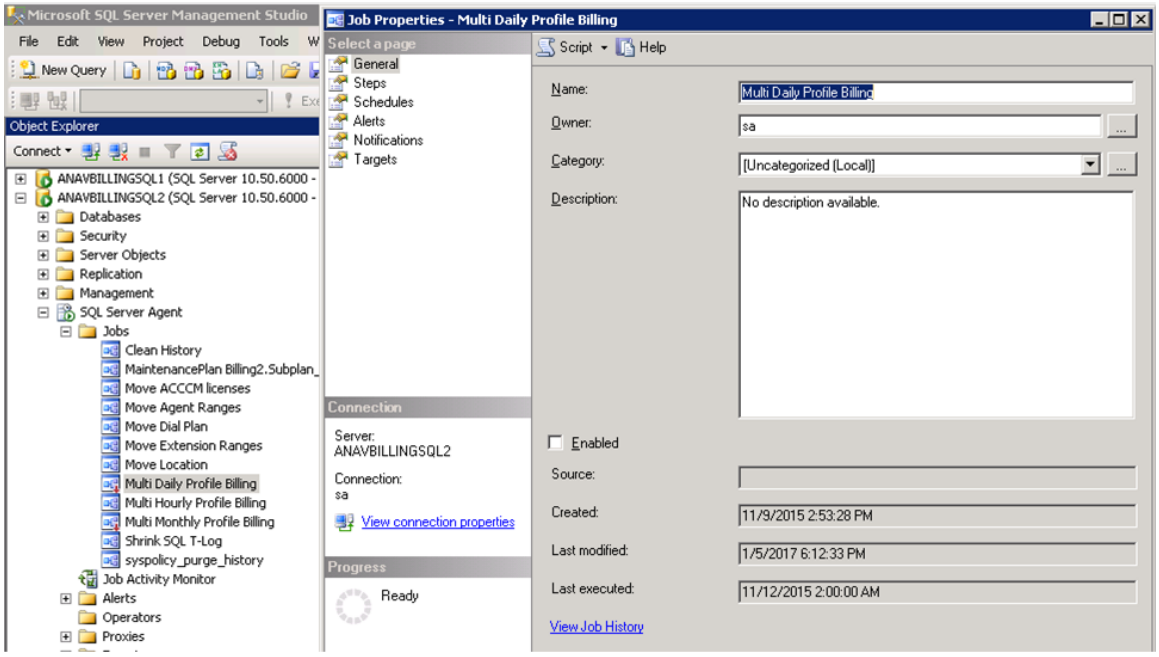
Billing configuration changes to the secondary data center

About this task

This procedure provides high-level steps to configure the billing configuration on the secondary data center. For more information, see *Failover Management for Partner Cloud Powered by Avaya xCaaS*.

Procedure

1. Disable the schedule for the Multi Daily Profile Billing job in the secondary billing database by performing the following steps:
   a. Open Microsoft SQL Management studio and connect to secondary billing database.
   b. Navigate to **SQL Server Agent** > **Jobs**.
   c. Right-click the **Multi Daily Profile Billing** job and either click **Disable** or select **Properties**. If you select **Properties**, the system displays the Job Properties – Multi Daily Profile Billing window.



d. Select **Disable** on the Job Properties – Multi Daily Profile Billing window.

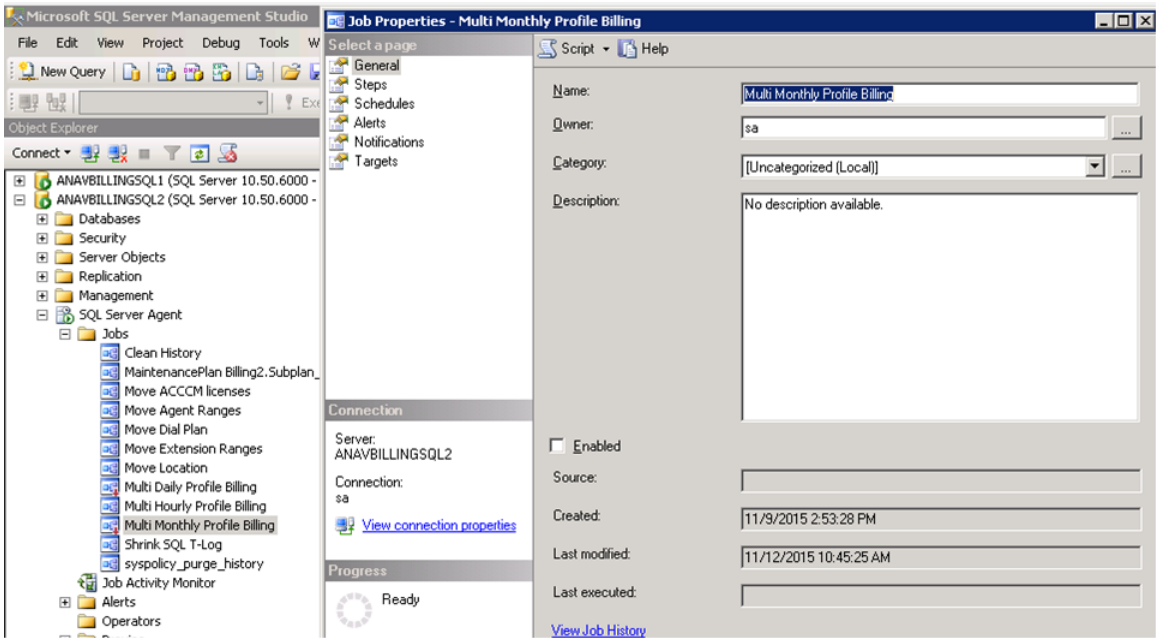
e. Click **OK** to save the changes.

2. Disable the schedule for the Multi Monthly Profile Billing job in the secondary billing database by performing the following steps:

   a. Open Microsoft SQL Management studio and connect to secondary billing database.

   b. Navigate to **SQL Server Agent** > **Jobs**.

   c. Right-click the **Multi Monthly Profile Billing** job and either click **Disable** or select **Properties**. If you select **Properties**, the system displays the Job Properties – Multi Monthly Profile Billing window.



d. Select **Disable** on the Job Properties – Multi Monthly Profile Billing window.

e. Click **OK** to save the changes.

3. Log on to the Control Manager application server in the secondary data center (ACM-APP-2) and verify that the Control Manager License Tracker Service is set to manual and is not running (that is, stopped) in the secondary application server (ACM-APP-2):

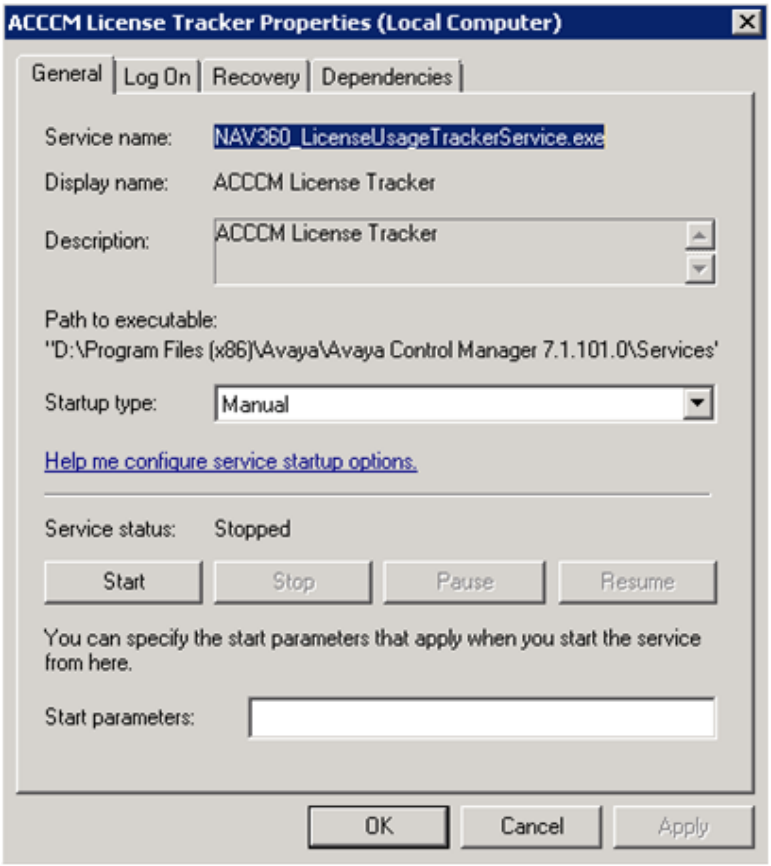
   a. Go to **Start** > **Run**.

   b. Enter `services.msc` and press **Enter**.

      The system displays a list of services.

   c. Locate the **ACCCM License Tracker** and **ACCCMAudit Log** services and verify that the **Startup Type** is set to **Manual** for both services and that the services are not running (that is, blank).

   d. If the service is not set up correctly, double-click the service name and make the appropriate changes.



Configuring the billing engine startup and recovery properties

About this task

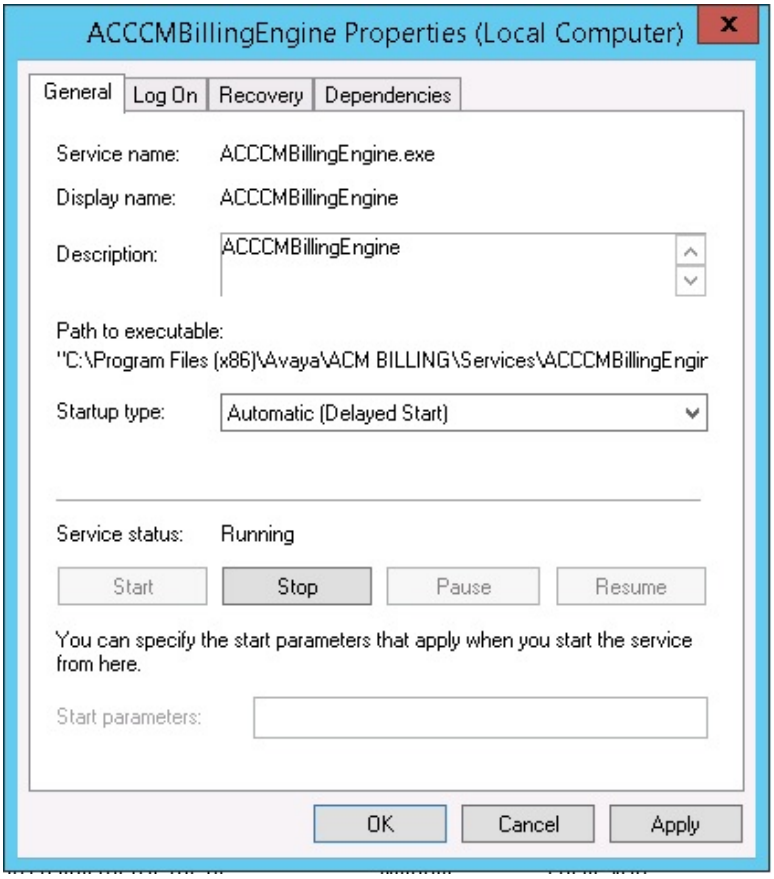
After you install the billing software, you must set the startup and recovery properties for the ACCCMBillingEngine and AAEPBilling services. These properties are used in failure recovery scenarios. You must set these properties on both the primary and secondary Control Manager application servers (ACM-APP-1 and ACM-APP-2).

Procedure

1. Log on to Windows on the primary application server (ACM-APP-1).
2. Go to **Start** > **Run**.
3. Enter `service.msc` and press **Enter**.

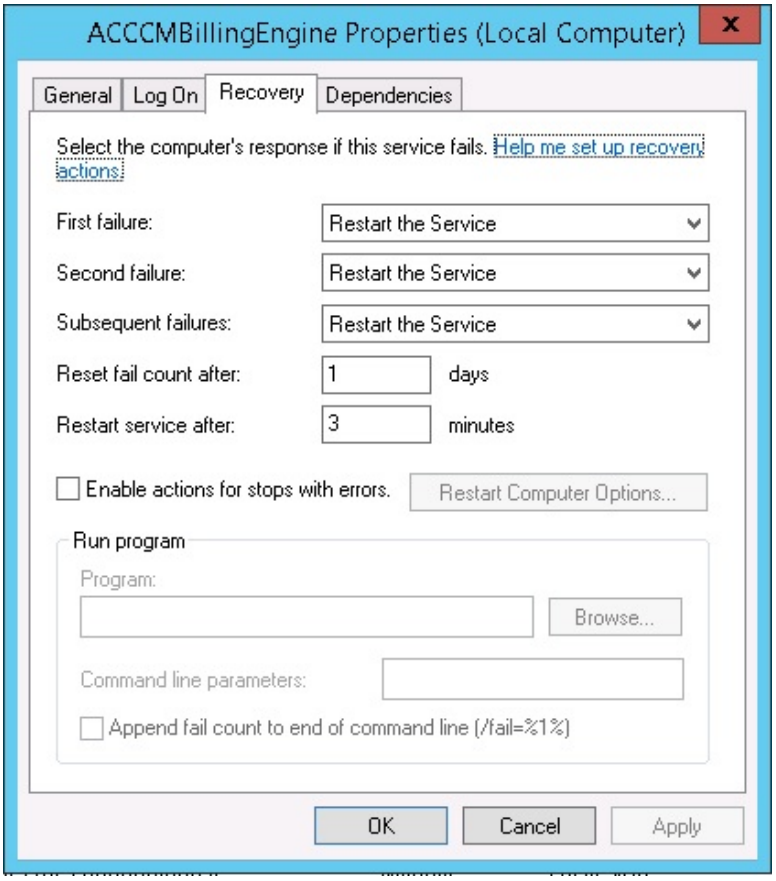
   The system displays the list of services.
4. Right-click the **ACCCMBillingEngine** service and click **Properties**.

   The system displays the following screen:



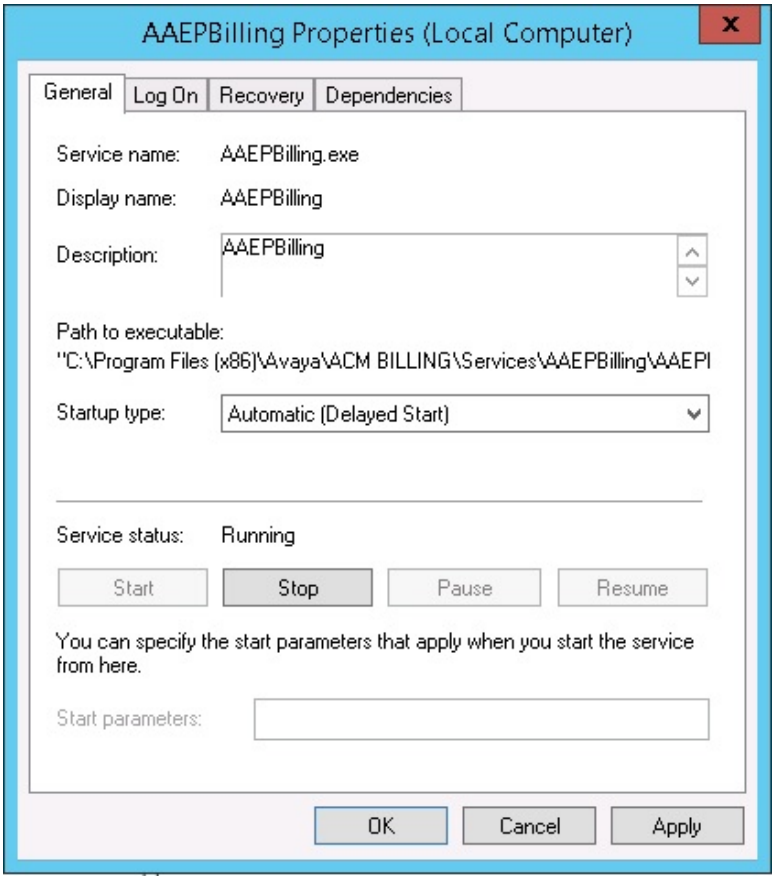
5. Set the **Startup type** option to **Automatic (Delayed Start)**.
6. Select the **Recovery** tab.

   The system displays the following screen:



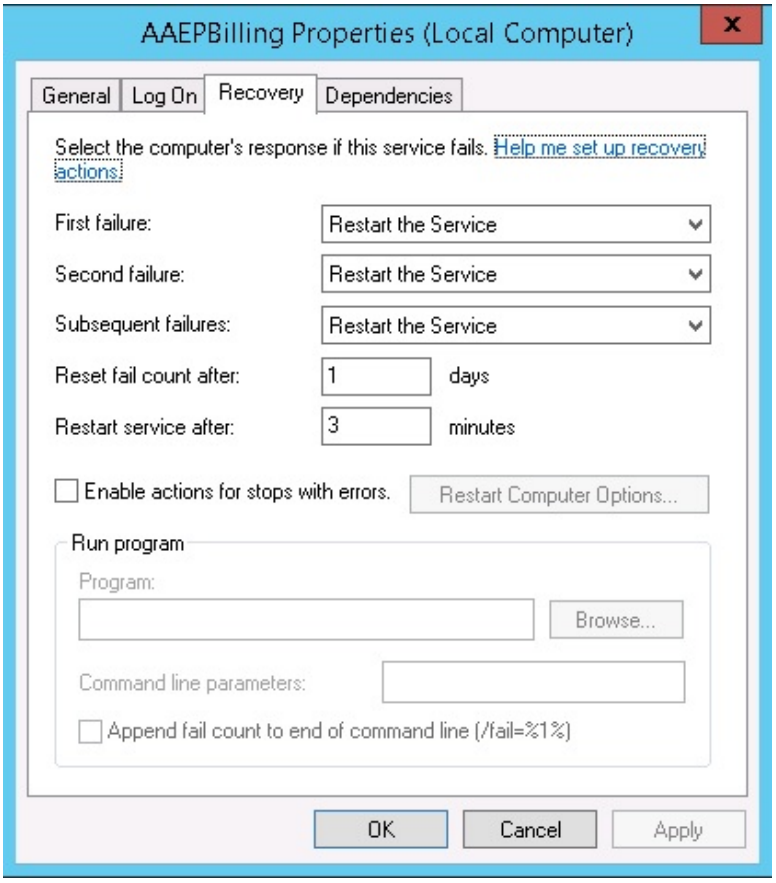
7. Administer the following options:
   - Set **First failure** to **Restart the Service**.
   - Set **Second failure** to **Restart the Service**.
   - Set **Subsequent failures** to **Restart the Service**.
   - Set **Reset fail count** after to **1**.
   - Set **Restart service after** to **3**.
8. Click **OK**.
9. Right-click the **AAEPBilling** service and click **Properties**.

   The system displays the following screen:



10. Set the **Startup type** option to **Automatic (Delayed Start)**.
11. Select the **Recovery** tab.

    The system displays the following screen:



12. Administer the following options:
    - Set **First failure** to **Restart the Service**.
    - Set **Second failure** to **Restart the Service**.
    - Set **Subsequent failures** to **Restart the Service**.
    - Set **Reset fail count** after to **1**.
    - Set **Restart service after** to **3**.
13. Click **OK**.
14. Repeat this procedure on the secondary application server (ACM-APP-2).

Chapter 9: Configuring replication

About replication

Important:

When deploying xCaaS with Usage Metering (UM) Collector software and the VMware HA feature, you can skip this information about replication.

Control Manager HA uses the transactional replication with updateable subscriptions feature that is available in Microsoft SQL Server software. This means is that under normal operating conditions, any change to the defined databases on the primary database server (ACM-SQL-1) will be automatically pushed out to the secondary database server (ACM-SQL-2). However, since unidirectional replication is used, any change made on the secondary database server (ACM-SQL-2) must be manually updated on the primary database server (ACM-SQL-1).

Per the reference architecture, the database primary connection path for ACM-APP-1 and ACM-APP-2 is to point to the same ACM-SQL-1 database server. The secondary connection path for ACM-APP-1 is to point to ACM-SQL-2.

Per the reference architecture, the database primary connection path for ACM-UI-1 and ACM-UI-2 is to point to the same ACM-SQL-1 database server. The secondary connection path for ACM-UI-1 is to point to ACM-SQL-2.

Within a Control Manager HA environment, each Control Manager instance is working with a dedicated database layer. The two Microsoft SQL database servers (ACM-SQL-1/ACM-SQL-2) host the following databases and are set up for transactional database replication.

The following table illustrates the replication strategy for each of the SQL databases that Control Manager HA supports in a dual data center.

Database	Replication	Direction
ACCCM	Transactional	Unidirectional (DC 1 to DC 2 only)
ACCCMCMSYSLOG	Transactional	Bidirectional
ACM_BILLING	Transactional	Bidirectional
ACCCMSYNC	Transactional	Bidirectional

Important:

This document uses both database names ACM_BILLING and ACCCMBilling. If the system has been upgraded from a previous version, the database name is probably named

ACCCMBilling. Regardless of which name is being used, ensure that you use the correct database name within these procedures.

Note:

The following table lists which database tables within the Control Manager databases do not replicate:

Control Manager Database	Database Tables
ACCCM	[Audit_Log_Service_Temp_InsertSource_Audit] [CMAuditLogs_Temp] [Extensions_Details_Temp] [Extensions_Temp] Log_Messages [Skills_Temp] [tmp_License_Usage_Tracker_History] [tmp_Traffic_Measure_Occupancy_History] [tmp_Traffic_Measure_Trunks_History] [VDNs_Temp]
ACM_BILLING or ACCCMBilling	Configured_Stations vpapplog cdr tblProfileUsagePerLocationPerSiteMonthly_ProfilePivotConfiguration tblProfileUsagePerLocationPerSiteMonthly_ProfilePivot Agent_Ranges tblProfileUsagePerLocationPerSiteByHour tblProfileUsagePerLocationByHour tblPreProcAction t_sdr Staffed_Agents sdr RptPickLicenseWeeklyLocation RptPickLicenseWeekly RptPickLicenseMonthlyLocation RptPickLicenseMonthly RptPickLicenseDaily

Table continues…

Control Manager Database	Database Tables
	Rpt_PeakAaepUsageByMin Rpt_PeakAaepUsageByDay Registered_Stations PickLicense5MinLocation PickLicense5Min Locations_CM_Servers Locations License_Usage_Tracker_History Extension_Ranges Dial_Plans vpperformance
ACCCMCMSYSLOG	CM_Syslog_RawMessages_Temp

Verifying that Microsoft Distributed Transaction Coordinator (DTC) is installed and configured

About this task

The SQL servers use Microsoft DTC as part of the bidirectional replication process. Before configuring replication, verify that Microsoft DTC has been installed and configured correctly.

Procedure

1. Access the ACM-SQL-1 server using Windows.
2. Press **Start**, enter **Component Services** in the data entry field, and press **Enter**.

   The system displays the Server Manager window.
3. Navigate to **Component Services** > **Computers** > **my Computer** > **Distributed Transaction Coordinator** > **Local DTC**.
4. Right-click on **Local DTC** and select **Properties**.
5. Select the **Security** tab.
6. In **Security Settings**, enable **Network DTC Access** and **Allow Remote Clients**. If these options are not enabled, the client machines cannot access the DTC on this machine
7. In **Transaction Manager Communication**, enable **Allow Inbound**, **Allow Outbound**, and **No Authentication required**.
8. Click **OK**.

The DTC prompts you to restart it.

9. Click **Yes**, unless you want to schedule the restart for another time.

   The DTC restarts.

10. Click on the **Services** item on the menu on the left hand side.
11. On the right hand side, scroll down to the **Distributed Transaction Coordinator** service and confirm that it has started and its startup type is set to automatic.
12. Restart the SQL server.
13. Repeat this procedure on the secondary SQL server (ACM-SQL-2).

Configuring SQL replication on the primary and secondary database servers (ACM-SQL-1 and ACM-SQL-2)

Before you begin

Use the following procedure to stop HA Services on both the primary and secondary application servers:

1. Log on to the Windows on the primary application server (ACM-APP-1).
2. Go to **Start** > **Run**.
3. Enter `services.msc` and press **Enter**.
4. In the Services window, right-click the **ACCCM HA Service** and select **Stop**.
5. Repeat this procedure on the secondary application server (ACM-APP-2).

Procedure

1. Open SQL Management Studio on the primary SQL database server (ACM-SQL-1).
2. Log on to the primary SQL database server (ACM-SQL-1) with an SA account or as an account with similar permissions.
3. Navigate to the **Replication** folder and expand the folder.
4. Right-click the **Replication** folder.

   The system displays the Replication sub-menu.

   Important:

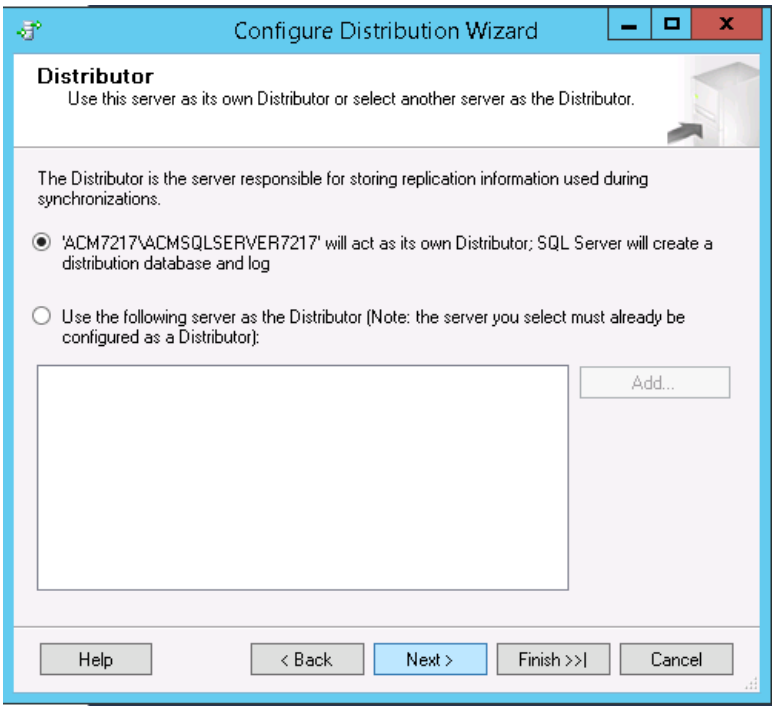
   If you see the **Configure Distribution** option in the menu items, it means that replication has not been configured on the server. If **Configure Distribution** is not displayed, replication has been configured and you can skip this procedure.

5. Select **Configure Distribution**.

   The system displays the Configure Distribution Wizard welcome screen.

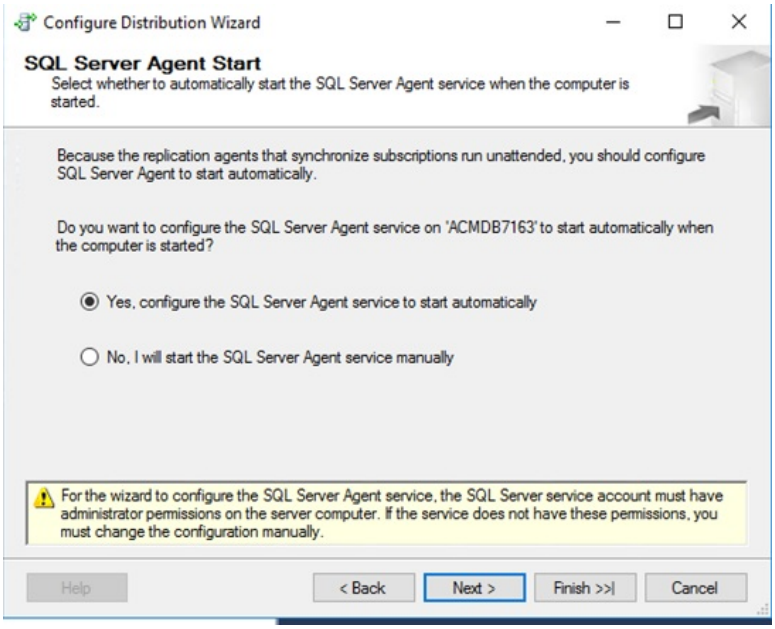
6. Click **Next**.

   The system displays the Distributor screen.



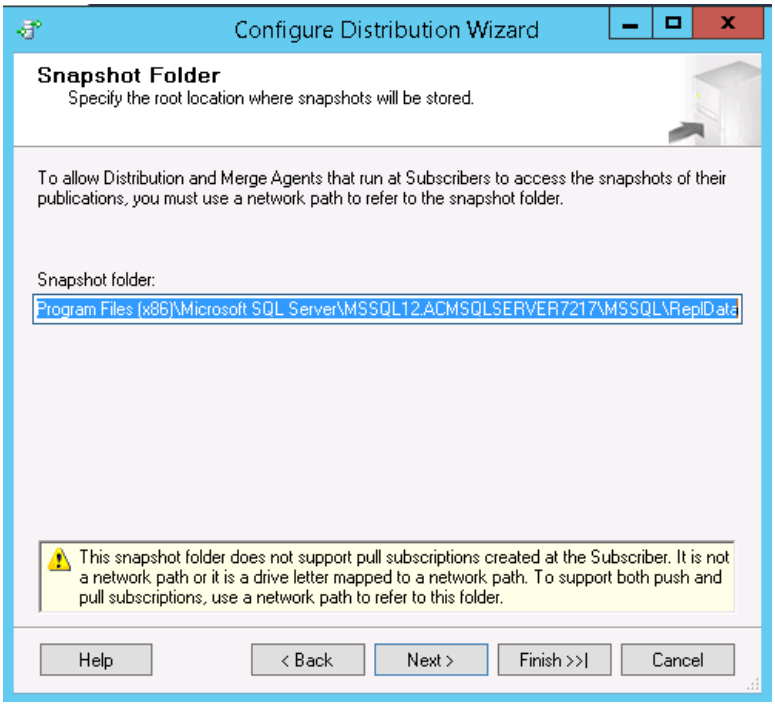
7. Select the first option, **"*DatabaseID*" will act as its own Distributor**. The variable *DatabaseID* represents the actual name of the database server.
8. Click **Next**.

   The system displays the SQL Server Agent Start screen.



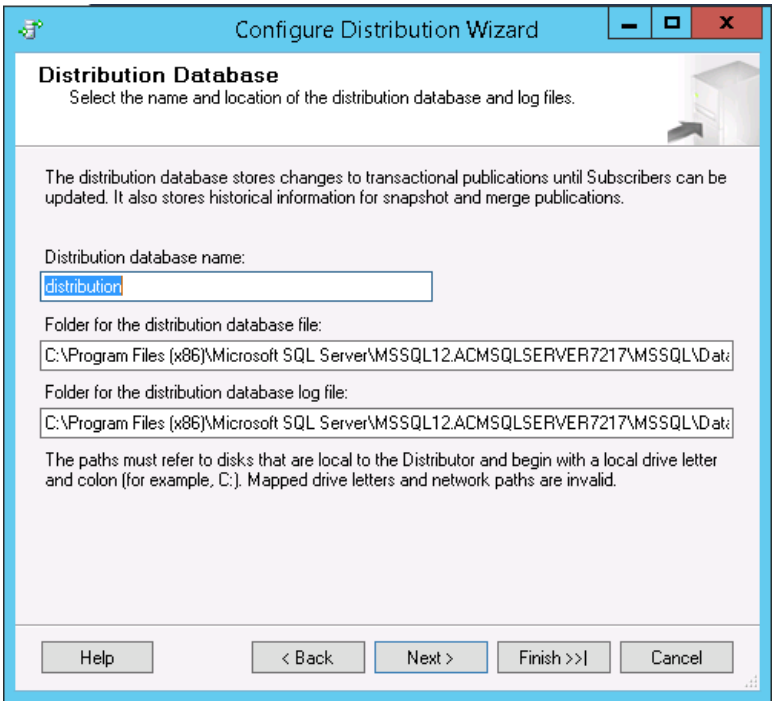
9. Click **Next**.

   The system displays the Snapshot Folder screen. Note the path to the snapshot folder. You must use it later in this procedure.



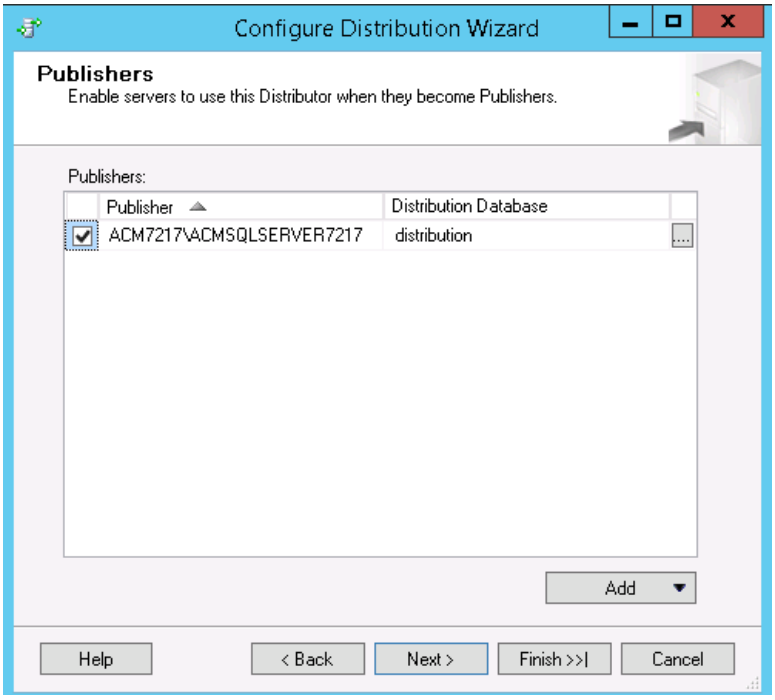
10. Click **Next**.

    The system displays the Distribution Database screen:



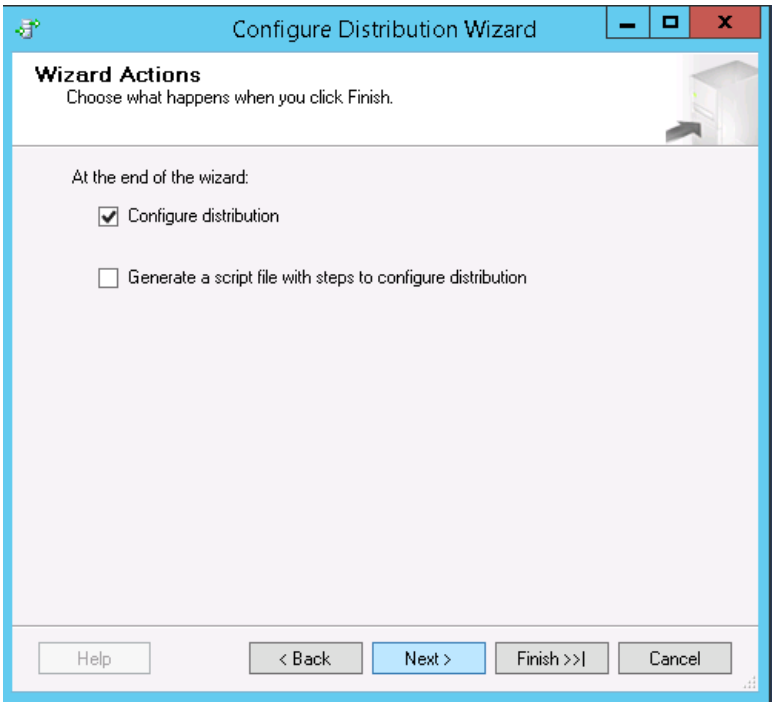
11. Enter the **Distribution database name** and the folders where the data and the log file will reside.
12. Click **Next**.

    The system displays the Publishers screen.



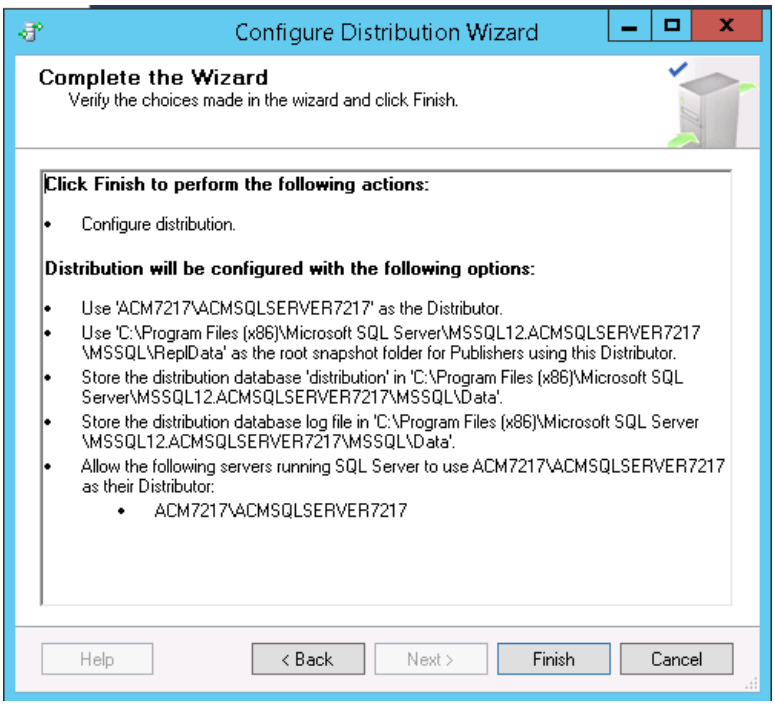
13. Click **Next**.

    The system displays the Wizard Actions screen.



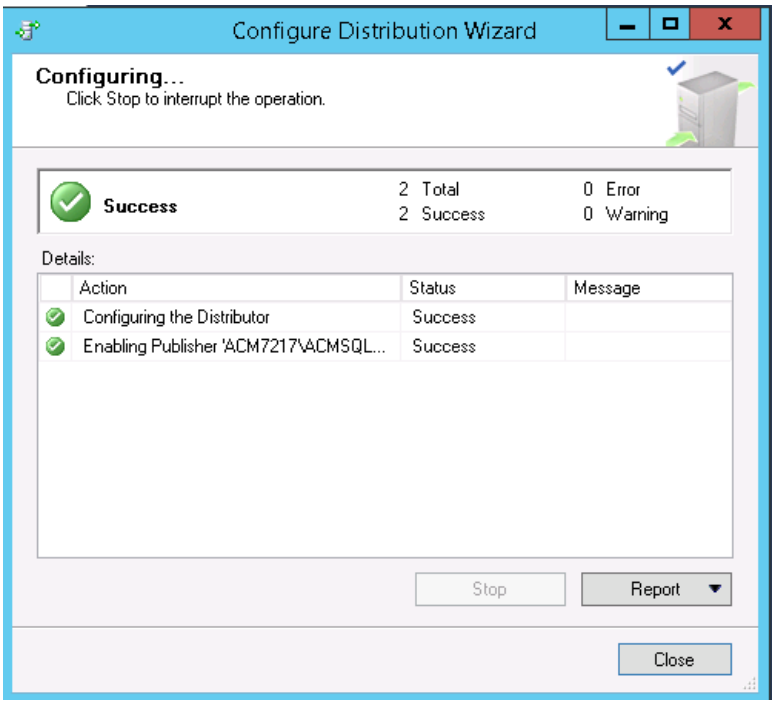
14. Click **Next**.

    The system displays the Complete the Wizard screen.



15. Click **Finish**.

    When the process completes, a new database gets created with the name specified in the Distribution Database screen. To confirm that the database was created, expand the System Database node and you shall be able to view the distribution database. See the following example:



16. Click **Close**.
17. Open Windows Explorer the primary SQL database server (ACM-SQL-1) and navigate to the snapshot folder path that depends on which version of Microsoft SQL Server you are using and whether you are using an instance name.

    For Microsoft SQL Server (x86) edition when not using an instance name:

    - Microsoft SQL Server 2012 — `C:\Program Files (x86)\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\ReplData`
    - Microsoft SQL Server 2014 — `C:\Program Files (x86)\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\ReplData`
    - Microsoft SQL Server 2016 — `C:\Program Files (x86)\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\ReplData`

    For Microsoft SQL Server (x64) edition when not using an instance name:

    - Microsoft SQL Server 2012 — `C:\Program Files\Microsoft SQL Server \MSSQL11.MSSQLSERVER\MSSQL\ReplData`
    - Microsoft SQL Server 2014 — `C:\Program Files\Microsoft SQL Server \MSSQL12.MSSQLSERVER\MSSQL\ReplData`

- Microsoft SQL Server 2016 — `C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\ReplData`

For Microsoft SQL Server (x86) edition when using an instance name:

- Microsoft SQL Server 2012 — `C:\Program Files (x86)\Microsoft SQL Server\MSSQL11.[Instance Name]\MSSQL\ReplData`
- Microsoft SQL Server 2014 — `C:\Program Files (x86)\Microsoft SQL Server\MSSQL12.[Instance Name]\MSSQL\ReplData`
- Microsoft SQL Server 2016 — `C:\Program Files (x86)\Microsoft SQL Server\MSSQL13.[Instance Name]\MSSQL\ReplData`

For Microsoft SQL Server (x64) edition when using an instance name:

- Microsoft SQL Server 2012 — `C:\Program Files\Microsoft SQL Server\MSSQL11.[Instance Name]\MSSQL\ReplData`
- Microsoft SQL Server 2014 — `C:\Program Files\Microsoft SQL Server\MSSQL12.[Instance Name]\MSSQL\ReplData`
- Microsoft SQL Server 2016 — `C:\Program Files\Microsoft SQL Server\MSSQL13.[Instance Name]\MSSQL\ReplData`

18. Right-click on the folder and select **Properties**.

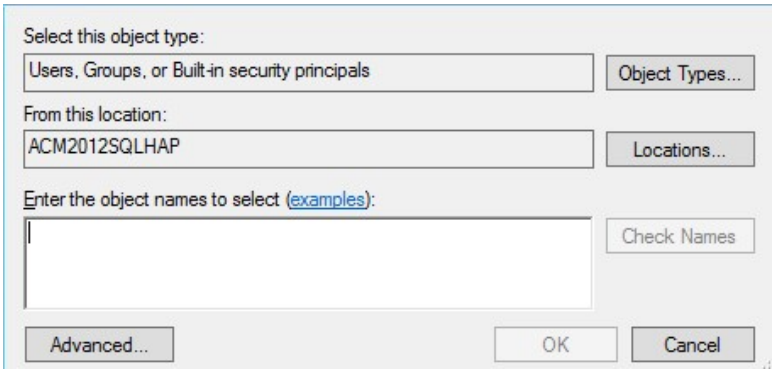
    The system displays the ***FolderName*** Properties screen.

19. Select the **Security** tab.
20. Click **Edit**.

    The system displays the Permissions for ***FolderName*** **Properties** screen.

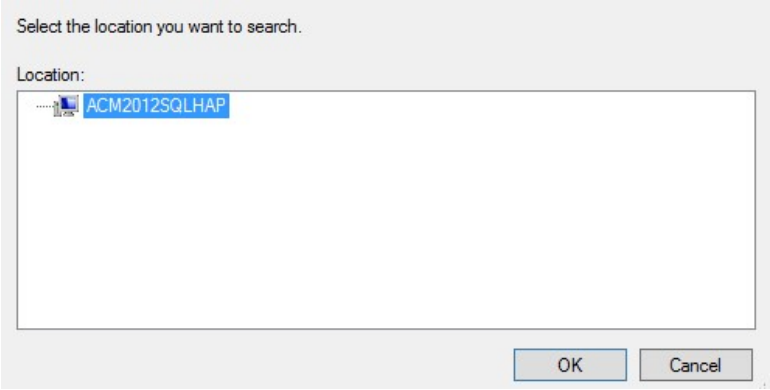
21. Click **Add**.

    The system displays the Select Users, Computers, Service Accounts, or Groups screen.



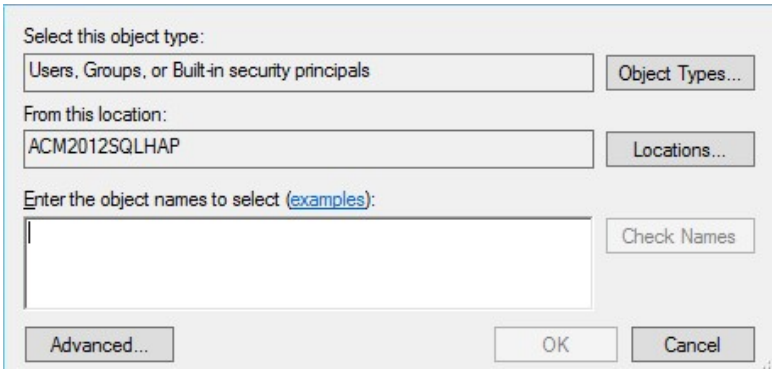
22. Click **Locations**.

    The system displays the Locations screen.



23. Select the server you are configuring.
24. Click **OK**.

    The system displays the Select Users or Groups screen.



25. Enter the following text into the **Enter the object names to select** field:

    For SQL without an instance, enter: `nt service\sqlserveragent`

    For SQL with an instance, enter the account used to log on to the instance of SQL Server Agent service. For example, enter: `nt service\sqlagent$[InstanceName]`
26. Click **OK**.

    The system displays the Permissions for ***FolderName*** screen.
27. Select the NT service user entered above and verify that the system allows modify permissions.
28. Click **OK**.

    The system displays the ***FolderName* Properties** screen.
29. Click **OK**.
30. Log on to the secondary SQL database server (ACM-SQL-2).
31. Repeat Steps 17-29 on the secondary SQL database server (ACM-SQL-2).

Configuring the publication for database replication on the primary SQL database server (ACM-SQL-1)

About this task

This task configures replication for each supported Control Manager SQL database. This task must be performed on only the primary SQL database server (ACM-SQL-1). You must repeat this procedure for each of the databases listed in the following table:

Database	ACM-SQL-1 Primary Transactional Replication	ACM-SQL-2 Secondary Transactional Replication
ACCCM	Publisher	Subscriber
ACCCMCMSYSLOG	Publisher	Subscriber
ACCCMSYNC	Publisher	Subscriber

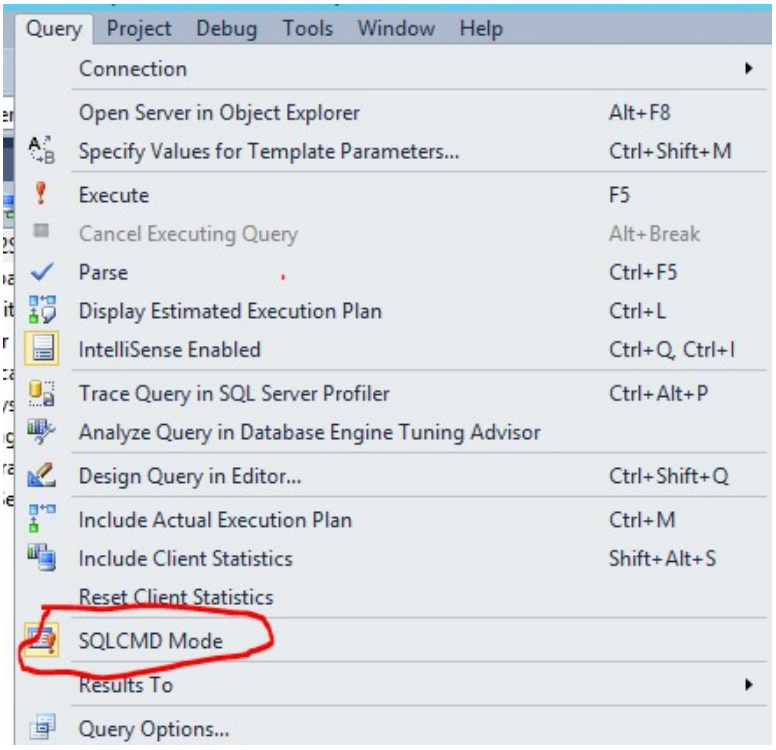
Before you begin

Download the transactional replication setup scripts from the Avaya support site.

Disable any firewall software running between the servers before setting up replication. After you finish setting up replication, enable the firewall software.

Procedure

1. Extract the files from the downloaded zip file to a single folder on the primary database server ACM-SQL-1. There are several script files, but those additional scripts are run from the main `trans_replication_manual.sql` script file.
2. Open the SQL Management Studio on the primary database server ACM-SQL-1.
3. Log on with an SA account or as an account with similar permissions.
4. Select **File** > **Open** and navigate to the folder where you extracted the files from the transaction replication setup zip file.
5. Select and open the file `trans_replication_manual.sql`.
6. From the Query menu select the option **SQLCMD Mode**.



The Query text area should change, with some lines being highlighted. See the following example:

```
/*

SQLCMD Header Area
This can only be run in SQLCMD mode
If lines begining with ":" are not highlighted you are in the wrong mode

*/
:ON Error Exit

--Source Server Details Netbiosname, SQLServer Username and password
--User Should have admin rights on Server

:SETVAR SourceServerName "SourceServerName"
:SETVAR SourceServerUser "SourceServerUser"

:SETVAR SourceServerPassword "SourceServerPassword"

--Destination Server Details Netbiosname, SQLServer Username and password
--User Should have admin rights on Server

:SETVAR DestServerName "DestServerName"
:SETVAR DestServerUser "DestServerUser"

:SETVAR DestServerPassword "DestServerPassword"

-- The Name of the database you wish to replicate
:SETVAR DatabaseName "DatabaseName"

--The full path this scripts is located in, do not include trailing backslash "\"
:SETVAR FilePath "C:\Full_Path_to_Setup_Files"
```

```
:connect $(SourceServerName) -U $(SourceServerUser) -P
$(SourceServerPassword)
```

7. The following configuration options should be set in the header of the SQL file:

Configuration Option	Description
SourceServerName	Net Bios name of the primary database server (ACM-SQL-1).
SourceServerUser	The database server login name used to connect to the primary database server. It should be “sa” or another user with sysadmin rights.
SourceServerPassword	The password associated with the login for the primary database server
DestServerName	The net bios name of the secondary database server (ACM-SQL-2)
DestServerUser	The database server login name used to connect to the secondary database server. It should be “sa” or another user with sysadmin rights.
DestServerPassword	The password associated with the login for the secondary database server.
DatabaseName	The name of the database you wish to have replicated. The default database names are ACCCM, ACCCMCMSYSLOG, and ACCCMSYNC.
File Path	This is the full path that SQL Files were extracted to in step 1. Do not include a trailing backslash,“\” in the path

8. Set up the options you wish to apply to this replication setup. See the following example:

```
set NOCOUNT ON;

--SQL Variables Section

--Continue if the database has already been published, defaults to 0.
--to database already replicated
declare @IgnorePublicationExistence bit = 0;

--Set to 0 for uni-directional replication, 1 for bi-directional repli
:SETVAR updateable 1

--If tables do not have a primary key defined they cannot be replicate
--Set to 1 to ignore tables without keys and continue, set to 0 to rea
declare @ignoretableswithnoprimarykey bit = 0;

--Set to 1 to include tables in replication
declare @AddTables bit = 1;

--Set to 1 to include views in replication
declare @addviews bit = 0

--Set to 1 to include strored procedures in replication
declare @addstoredprocedures bit = 0

--Set to 1 to include functions in replication
declare @addfunctions bit = 0


--Start of script body, do not edit anything below this line
```

Setup Options	Description
@IgnorePublicationExistence	The Default of 0, will cause the script to exit if the database has already been published. Set the value to 1 to have the script continue even if the database has been published already. This is useful where you need to add to tables to the publication or you wish to rerun they script having resolved an error
updateable	The default of 1 will setup bi-directional replication. Only set to 0 if you want the replication to be one way.
@ignoretableswithnoprimarykey	The default value of 0 will cause the script to exit if any tables in the source database lacks a primary key. Setting this value to 1 will override this behavior. Please note the

Table continues…

Setup Options	Description
	table missing a primary key will not be added to the publication
@addtables	Set to 1 to include tables in publication. Default value 1
@addviews	Set to 1 to include views in publication. Default value 0
@addstoredprocedures	Set to 1 to include stored procedures in publication. Default value 0
@addfunctions	Set to 1 to include user defined functions in publication. Default value 0

9. Run the script by pressing **F5**. Depending on the option selected and the size of the database, the script may take some time to run.
10. Once the script has completed, check the output tab in SQL Management Studio for any errors.
11. Repeat this procedure for the following Control Manager databases:
    - ACCCM
    - ACCCMCMSYSLOG
    - ACCCMSYNC

Next steps

After you finish setting up replication, enable the firewall software.

Enabling replication on the database servers

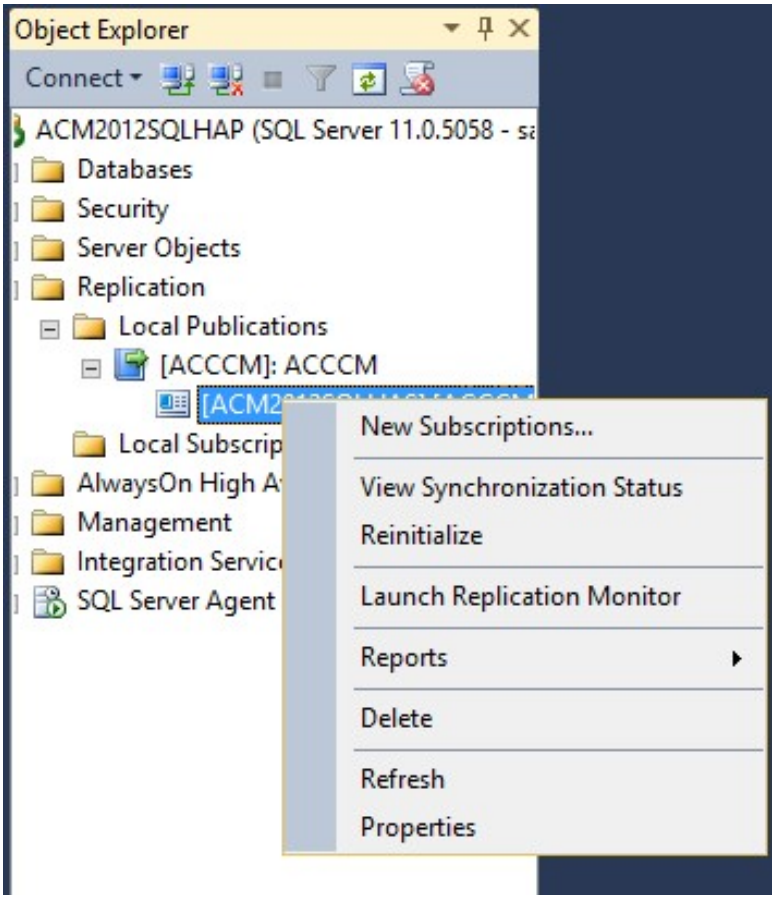
About this task

After configuring each of the Control Manager databases for replication, perform the following task on each of the Control Manager databases to verify the overall health of the replication environment.

Procedure

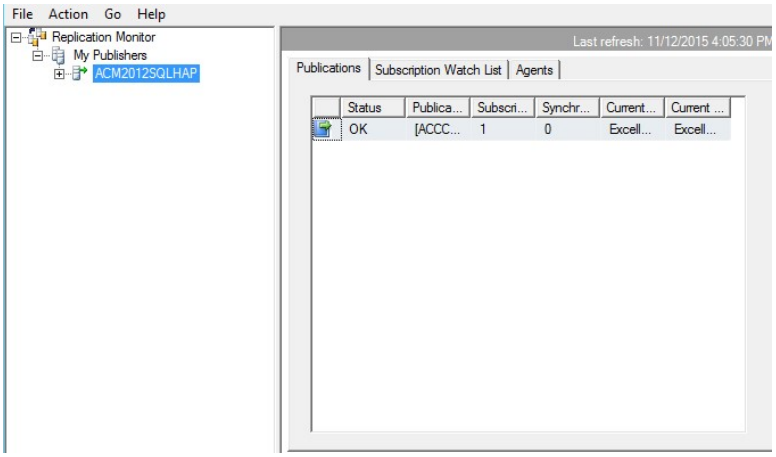
1. Open the SQL Server Management Studio of the primary database server (ACM-SQL-1).

   The system displays the Microsoft SQL Server Management Studio screen.
2. Right-click on the Replication folder of the subscription that was previously created. See the following example:

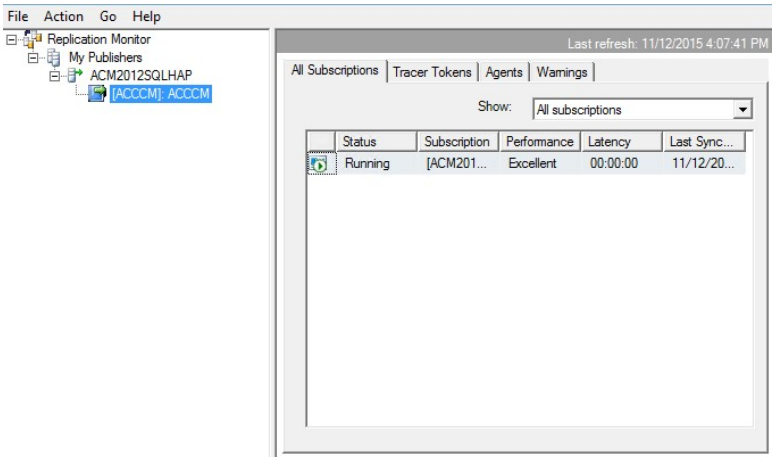


3. Select **Launch Replication Monitor**.

   The system displays the Replication Monitor screen.

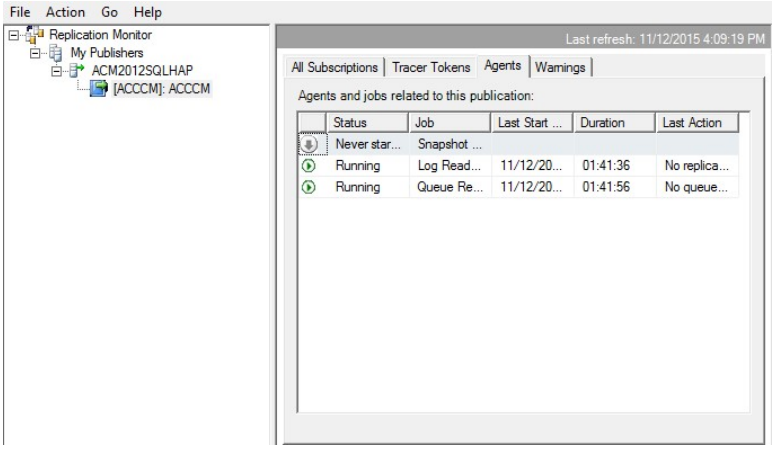


4. In the left pane under **My Publishers**, select the Control Manager **Publication** node and expand the folders to get a list of the subscriptions on the primary database server (ACM-SQL-1). See the following example:



5. Select the **Agents** tab.

   The system displays the following screen:



6. Right-click on **Snapshot Agent** job and click **Start Agent**.

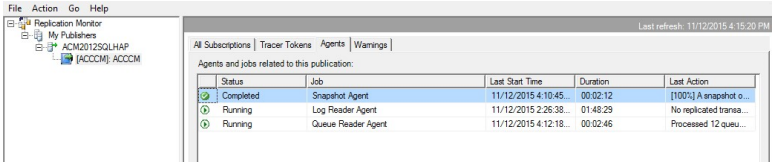
   This updates the agent settings. The process can take up to 30 minutes.

7. Immediately after you start the snapshot agent, if you see an error message displayed in the **Status** column of the **Queue Reader Agent** job, do the following:

   a. Right-click on that **Queue Reader Agent** job and click **Stop Agent**.

   b. Right-click on that **Queue Reader Agent** job again and click **Start Agent**.

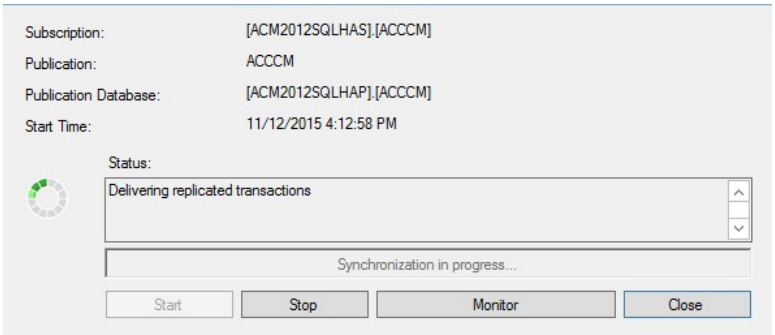
8. Refresh the page by navigating to another tab. The system displays the following screen:



9. When the **Snapshot Agent** job reaches 100% in the **Last Action** column, close the window.

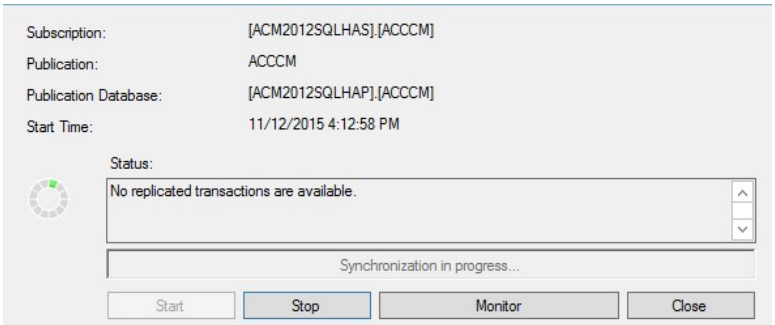
10. Repeat steps 1 through 9 for each database that requires replication.
11. Do one of the following to view synchronization status:
    - On the primary database server (ACM-SQL-1), in **Object Explorer**, expand the **Local Publications** folder, right-click on the **Subscription**, and choose **View Synchronization Status**.
    - On the secondary database server (ACM-SQL-2), in **Object Explorer**, expand the **Local Subscriptions** folder, right-click on the **Subscription**, and choose **View Synchronization Status**.

    The system displays the **View Synchronization Status** screen. See the following example:



    If the Status field displays Applied script ScriptName, it means that the initial action of copying over the data from the primary database server (ACM-SQL-1) to the secondary database server (ACM-SQL-2) is in progress. If you see a different message, wait a few minutes until you confirm that data is being copied from one server to the other server.

    When you see the message **No replicated transactions are available**, the initial synchronization of data between the two database servers has completed. See the following example:



12. Repeat step 11 for each Database Publication.

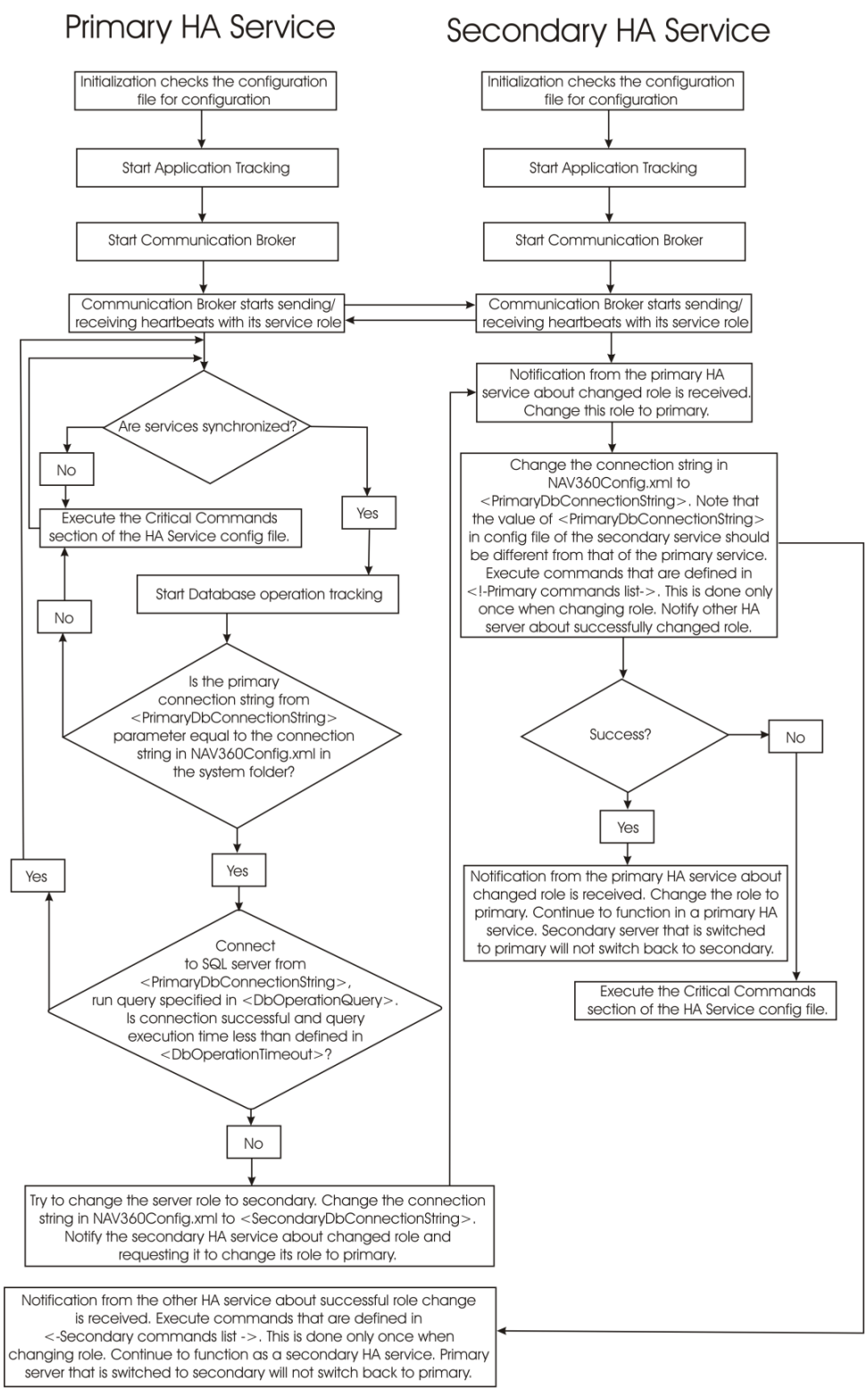
Chapter 10: Configuring HA services

About HA services

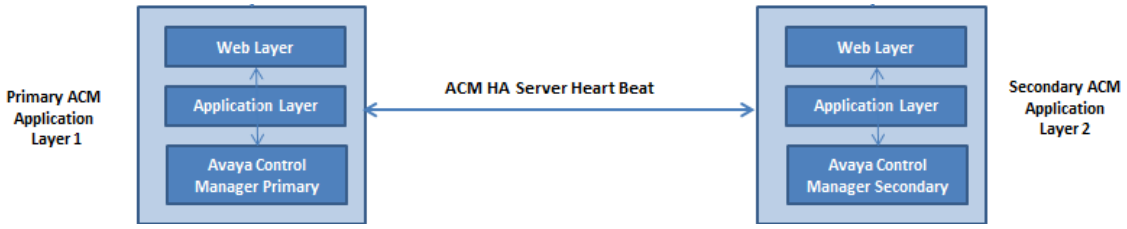
Important:

When deploying xCaaS with Usage Metering (UM) Collector software and the VMware HA feature, you can skip this entire chapter.

The key to any Control Manager HA configuration is that the service always needs to be operational with no downtime and being able to transfer from one Control Manager server to another server seamlessly. What makes this happen in Control Manager is a service called the HA Service Heartbeat.


Primary HA Service
Secondary HA Service
Initialization checks the configuration file for configuration
Start Application Tracking
Start Communication Broker
Communication Broker starts sending/ receiving heartbeats with its service role
Are services synchronized?
No
Yes
Execute the Critical Commands section of the HA Service config file.
Start Database operation tracking
No
Is the primary connection string from <PrimaryDbConnectionString> parameter equal to the connection string in NAV360Config.xml in the system folder?
Yes
Yes
Connect to SQL server from <PrimaryDbConnectionString>, run query specified in <DbOperationQuery>. Is connection successful and query execution time less than defined in <DbOperationTimeout>?
No
Try to change the server role to secondary. Change the connection string in NAV360Config.xml to <SecondaryDbConnectionString>. Notify the secondary HA service about changed role and requesting it to change its role to primary.
Notification from the other HA service about successful role change is received. Execute commands that are defined in <-Secondary commands list ->. This is done only once when changing role. Continue to function as a secondary HA service. Primary server that is switched to secondary will not switch back to primary.
Initialization checks the configuration file for configuration
Start Application Tracking
Start Communication Broker
Communication Broker starts sending/ receiving heartbeats with its service role
Notification from the primary HA service about changed role is received. Change this role to primary.
Change the connection string in NAV360Config.xml to <PrimaryDbConnectionString>. Note that the value of <PrimaryDbConnectionString> in config file of the secondary service should be different from that of the primary service. Execute commands that are defined in <!-Primary commands list->. This is done only once when changing role. Notify other HA server about successfully changed role.
Success?
No
Yes
Notification from the primary HA service about changed role is received. Change the role to primary. Continue to function in a primary HA service. Secondary server that is switched to primary will not switch back to secondary.
Execute the Critical Commands section of the HA Service config file.

Both the Control Manager application servers (ACM-APP-1 and ACM-APP-2) have a heart beat service connection between them which is established and monitored by the Control Manager HA Service running on both machines.



Control Manager Services for High Availability

Under normal operating conditions, the two application servers (ACM-APP-1 and ACM-APP-2) will function in an Active/Active mode, meaning that both applications servers are working in parallel.

The primary application server runs its primary database connection path against the primary database server (ACM-SQL-1) whereas the secondary application server also runs its primary database connection against the primary database server (ACM-SQL-1). This is an architectural requirement to make the Control Manager High Availability failover mechanisms work properly.

The following overview outlines the relevant services that have an interconnection with the Control Manager HA setup and are actively monitored by the HA service. Under normal operating conditions, the following service status is required.

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

Note:

Except for HA Service, none of the services can be up and running on both of the application servers (ACM-APP-1 and ACM-APP-2) at the same time

Note:

After every power restart (recovery) of the application servers, confirm that the states of these services are as shown in the table above.

The HA service monitors the primary database connections from both application servers (ACM-APP-1 and ACM-APP-2) to the primary database server (ACM-SQL-1). The service takes the appropriate action in the event of a database connection failure. The database connection strings are defined in each of the `NAV360Config.xml` file on each application server. The `NAV360Config.xml` file must always reflect the primary database connection paths on each of the primary and secondary application servers (ACM-APP-1 and ACM-APP-2).

The following overview outlines the relevant services that have an interconnection with the Control Manager HA setup and are actively monitored by the HA service. Under normal operating conditions, the following service status is required.

Control Manager Service	ACM-UI-1		ACM-UI-2	
	Status	Start-up	Status	Start-up
HA Service	Running	Manual	Running	Manual

Stopping the Control Manager services

About this task

To stop the Control Manager services, 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. Navigate to **Start** > **Run**.
3. Enter `services.msc` and press **Enter**.

   The system displays a list of services.
4. In the Services window, right-click each of the Control Manager services (those with ACCCM in the name) and the Tomcat services and select **Stop**.

   Important:

   Open Windows Task Manager and check the **Services** tab to verify that all Control Manager services are stopped. Check the **Details** tab to verify that no files or folders are locked. If any executables or services are still up on any of the Control Manager folders, right-click the item and end the process.

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

Configuring the sphereFeederConfig.xml file on the secondary application server (ACM-APP-2)

About this task

You must configure the `sphereFeederConfig.xml` file with the secondary application server FQDN.

Procedure

1. Log on to Windows on the secondary application server (ACM-APP-2).
2. Open the following file using a text editor:

   InstallLocation`\Services\ACCCM Sphere\ACCCM Sphere Feeder\config\sphereFeederConfig.xml`

3. Enter the FQDN and port number of the secondary application server (ACM-APP-2) into the database section of the file. See the following example:

```
<database>
    <serverType>sqlserver</serverType>
    <serverName>FQDN:PortNumber</serverName>
    <databaseName>ACCCM</databaseName>
    <userName>ACCCMSPHERE</userName>
    <password>EncryptedPassword</password>
  </database>
```

4. Save and close the file.

Configuring the HA Service on the primary UI server (ACM-UI-1)

About this task

To configure the HA service on the primary UI server (ACM-UI-1) you must configure the `HA_Service.exe.config` file with the secondary UI server IP address.

Important:

The `HA_Service.exe.config` file is automatically populated after doing a new installation. Make changes to the file using this procedure only when the populated file is not correct for your installation.

Before you begin

Verify that Control Manager Services have started at least once before you configure the primary UI server HA Service.

Procedure

1. On the primary UI server (ACM-UI-1) open the following file using a text editor:

   `InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager <Rel#>\Services\ACCCM HA Service\HA_Service.exe.Config`

2. Enter the FQDN of the secondary UI server (ACM-UI-2) into the `HA_Service.exe.Config` file. See the following example:

   `<value>https://ACM-UI-2_FQDN:9011/ACCCM HA Service</value>`

3. Save and close the file.

Configuring the configuration.xml file on the primary UI server (ACM-UI-1)

About this task

Important:

The `configuration.xml` file is automatically populated after doing a new installation. Make changes to the file using this procedure only when the populated file is not correct for your installation.

Procedure

1. Locate the primary database connection strings within the configuration file. These connection strings must be updated and must match the string located in the existing `NAV360Config.xml` files on both the primary and secondary UI servers (ACM-UI-1 and ACM-UI-2).

2. Copy the database connection string from the `C:\Windows\System32\NAV360Config.xml` file on the primary UI server (ACM-UI-1).

3. Before making any changes in the `configuration.xml` file, create a backup copy of the file. For example, enter the following command:

   `copy InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager\Services\ACCCM HA Service\configuration.xml InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager\Services\ACCCM HA Service\Backup_configuration.xml`

4. Paste the connection string into the required area in the `configuration.xml` file. Edit the connections strings so that within the primary UI server (ACM-UI-1) the primary connection string points to the primary database server (ACM-SQL-1), and the secondary

connection string points to the secondary database server (ACM-SQL-2). See the following examples:

```
<PrimaryDbConnectionString>DataSource=ACMSQL1;Initial
Catalog=ACCCM;User ID=acccadmin;Password="EncryptedPassword"</
PrimaryDbConnectionString>
```

```
<SecondaryDbConnectionString>DataSource=ACMSQL2;Initial
Catalog=ACCCM;User ID=acccadmin;Password="EncryptedPassword"</
SecondaryDbConnectionString>
```

5. Locate the Service Default Role and enter “primary” into the service as shown in the following example:

   ```
   <ServiceDefaultRole>primary</ServiceDefaultRole>
   ```

6. Locate the database operational interval <DbOperationInterval> and adjust the interval that the HA Service will check the connectivity status of the Control Manager database. Set this value to either 15 or 30 seconds. See the following example:

   ```
   <DbOperationInterval>15</DbOperationInterval>
   ```

7. Locate the heartbeat service interval <HeartBeatInterval> and adjust the interval that the HA service on the primary UI server will communicate with the HA service on the secondary UI server. Set this value to either 15 or 30 seconds. See the following example:

   ```
   <HeartBeatInterval>15<HeartBeatInterval>
   ```

8. Add the FQDN, port number, and name of the HA Service to the primary UI server (ACM-UI-1). The default port number is 9011 and the default service name is ACCCM HA Service. See the following example:

   ```
   <ServiceHost>ACM-UI-1_FQDN</ServiceHost>
   ```

   ```
   <ServicePort>9011</ServicePort>
   ```

   ```
   <ServiceName>ACCCM HA Service</ServiceName>
   ```

9. Add the FQDN, port number, and name of the HA Service to the secondary UI server (ACM-UI-2). The default port number is 9011 and the default service name is ACCCM HA Service. See the following example:

   ```
   <RemoteServiceHost>ACM-UI-2_FQDN</RemoteServiceHost>
   ```

   ```
   <RemoteServicePort>9011</RemoteServicePort>
   ```

   ```
   <RemoteServiceName>ACCCM HA Service</RemoteServiceName>
   ```

10. Confirm that the Database Operation Timeout is set to the default value of 4000 as shown in the following example:

    ```
    <DbOperationTimeout>4000</DbOperationTimeout>
    ```

11. Confirm that the Database Operation Query is set to the default value of “select top 1 * from locations” as shown in the following example:

    ```
    <DbOperationQuery>SELECT TOP 1 * from Locations</DbOperationQuery>
    ```

12. Confirm that the Primary Command lists are set as shown in the following example:

    ```
    <Commands retries="1" type="primary">
    </Commands>
    ```

13. Confirm that the Secondary Command lists are set as shown in the following example:

    ```
    <Commands retries="1" type="secondary">
    </Commands>
    ```

14. Confirm that the Critical Command lists are set as shown in the following example:

    ```
    <CriticalErrorCommands retries="1">
    </CriticalErrorCommands>
    ```

15. Save and close the file.

Configuring the HA Service on the primary application server (ACM-APP-1)

About this task

To configure the HA service on the primary application server (ACM-APP-1), you must configure the `HA_Service.exe.config` file with the secondary application server IP address.

Important:

The `HA_Service.exe.config` file is automatically populated after doing a new installation. Make changes to the file using this procedure only when the populated file is not correct for your installation.

Before you begin

Verify that Control Manager Services have started at least once before you configure the primary application server HA Service.

Procedure

1. On the primary application server (ACM-APP-1), open the following file using a text editor:

   ```
   InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager
   \Services\ACCCM HA Service\HA_Service.exe.Config
   ```

2. Enter the FQDN of the secondary application server (ACM-APP-2) into the `HA_Service.exe.Config` file. See the following example:

   ```
   <value>https://ACM-APP-2_FQDN:9011/ACCCM HA Service</value>
   ```

3. Save and close the file.

Configuring the configuration.xml file on the primary application server (ACM-APP-1)

Procedure

1. Locate the primary database connection strings within the configuration file. These connection strings must be updated and must match the string located in the existing `NAV360Config.xml` files on both the primary and secondary application servers (ACM-APP-1 and ACM-APP-2).
2. Copy the database connection string from the `C:\Windows\System32\NAV360Config.xml` file on the primary application server (ACM-APP-1).
3. Before making any changes in the `configuration.xml` file, create a backup copy of the file. For example, enter the following command:

   `copy [InstallLocation]\Services\ACCCM HA Service\configuration.xml [InstallLocation]\Services\ACCCM HA Service\Backup_configuration.xml`

4. Paste the connection string into the required area in the `configuration.xml` file. Edit the connections strings so that within the primary application server (ACM-APP-1), the primary connection string points to the primary database server (ACM-SQL-1), and the secondary connection string points to the secondary database server (ACM-SQL-2). See the following examples:

   ```
   <PrimaryDbConnectionString>DataSource=ACMSQL1;Initial Catalog=ACCCM;User ID=acccadmin;Password="EncryptedPassword"</PrimaryDbConnectionString>
   ```

   ```
   <SecondaryDbConnectionString>DataSource=ACMSQL2;Initial Catalog=ACCCM;User ID=acccadmin;Password="EncryptedPassword"</SecondaryDbConnectionString>
   ```

5. Locate the Service Default Role and enter “primary” into the service as shown in the following example:

   ```
   <ServiceDefaultRole>primary</ServiceDefaultRole>
   ```

6. Locate the database operational interval <DbOperationInterval> and adjust the interval that the HA Service will check the connectivity status of the Control Manager database. Set this value to either 15 or 30 seconds. See the following example:

   ```
   <DbOperationInterval>15</DbOperationInterval>
   ```

7. Locate the heartbeat service interval <HeartBeatInterval> and adjust the interval that the HA service on the primary application server will communicate with the HA service on the secondary application server. Set this value to either 15 or 30 seconds. See the following example:

   ```
   <HeartBeatInterval>15<HeartBeatInterval>
   ```

8. Add the FQDN, port number, and name of the HA Service to the primary application server (ACM-APP-1). The default port number is 9011 and the default service name is ACCCM HA Service. See the following example:

   ```
   <ServiceHost>ACM-APP-1_FQDN</ServiceHost>
   ```

   ```
   <ServicePort>9011</ServicePort>
   ```

   ```
   <ServiceName>ACCCM HA Service</ServiceName>
   ```

9. Add the FQDN, port number, and name of the HA Service to the secondary application server (ACM-APP-2). The default port number is 9011 and the default service name is ACCCM HA Service. See the following example:

   ```
   <RemoteServiceHost>ACM-APP-2_FQDN</RemoteServiceHost>
   ```

   ```
   <RemoteServicePort>9011</RemoteServicePort>
   ```

   ```
   <RemoteServiceName>ACCCM HA Service</RemoteServiceName>
   ```

10. Confirm that the Database Operation Timeout is set to the default value of 4000 as shown in the following example:

    ```
    <DbOperationTimeout>4000</DbOperationTimeout>
    ```

11. Confirm that the Database Operation Query is set to the default value of “select top 1 * from locations” as shown in the following example:

    ```
    <DbOperationQuery>SELECT TOP 1 * from Locations</DbOperationQuery>
    ```

12. Confirm that the Primary Command lists are set as shown in the following example:

    ```
    <command type="service" action="stop">ACCCM Audit Log Service</
    command>
    ```

    ```
    <command type="service" action="stop">ACCCM License Tracker</
    command>
    ```

    ```
    <command type="service" action="stop">ACCCM Sync Service</command>
    ```

    ```
    <command type="service" action="stop">ACCCM Sphere Feeder</command>
    ```

    ```
    <command type="service" action="stop">ACCCM AD Sync</command>
    ```

    ```
    <command type="service" action="stop">ACCCM Schedule Server</
    command>
    ```

    ```
    <command type="service" action="stop">ACCCM CM Syslog Server</
    command>
    ```

13. Confirm that the Secondary Command lists are set as shown in the following example:

    ```
    <command type="service" action="stop">ACCCM Audit Log Service</
    command>
    ```

    ```
    <command type="service" action="stop">ACCCM License Tracker</
    command>
    ```

```
<command type="service" action="stop">ACCCM Sync Service</command>
<command type="service" action="stop">ACCCM Sphere Feeder</command>
<command type="service" action="stop">ACCCM AD Sync</command>
<command type="service" action="stop">ACCCM Schedule Server</
command>
<command type="service" action="stop">ACCCM CM Syslog Server</
command>
```

14. Confirm that the Critical Command lists are set as shown in the following example:

```
<command type="service" action="stop">ACCCM Audit Log Service</
command>
<command type="service" action="stop">ACCCM License Tracker</
command>
<command type="service" action="stop">ACCCM Sync Service</command>
<command type="service" action="stop">ACCCM Sphere Feeder</command>
<command type="service" action="stop">ACCCM AD Sync</command>
<command type="service" action="stop">ACCCM Schedule Server</
command>
<command type="service" action="stop">ACCCM CM Syslog Server</
command>
```

15. Save and close the file.

Configuring the HA Service on the secondary UI server (ACM-UI-2)

About this task

To configure the HA service on the secondary UI server (ACM-UI-2), you must configure the `HA_Service.exe.config` file with the primary UI server IP address.

Important:

The `HA_Service.exe.config` file is automatically populated after doing a new installation. Make changes to the file using this procedure only when the populated file is not correct for your installation.

Before you begin

Verify that Control Manager Services have started at least once before you configure the secondary application server HA Service.

Procedure

1. On the secondary UI server (ACM-UI-2), open the following file using a text editor:

   `InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager <Rel#>\Services\ACCCM HA Service\HA_Service.exe.Config`

2. Enter the FQDN of the primary UI server (ACM-UI-1) into the `HA_Service.exe.Config` file. See the following example:

   `<value>https://ACM-UI-1_FQDN:9011/ACCCM HA Service</value>`

3. Save and close the file.

Configuring the configuration.xml file on the secondary UI server (ACM-UI-2)

About this task

Important:

The `configuration.xml` file is automatically populated after doing a new installation. Make changes to the file using this procedure only when the populated file is not correct for your installation.

Procedure

1. Locate the primary and secondary database connection strings within the configuration file. These connection strings must be updated and must match the string located in the existing `NAV360Config.xml` files on both the primary and secondary UI servers (ACM-UI-1 and ACM-UI-2).

2. Copy the database connection string from the `C:\Windows\System32\NAV360Config.xml` file on the secondary UI server (ACM-UI-2).

3. Before making any changes in the `configuration.xml` file, create a backup copy of the file. For example, enter the following command:

   `copy InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager\Services\ACCCM HA Service\configuration.xml InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager\Services\ACCCM HA Service\Backup_configuration.xml`

4. Paste the connection string into the required area in the `configuration.xml` file. Edit the connections strings so that within the secondary UI server (ACM-UI-2), both the primary and the secondary connection string points to the secondary database server (ACM-SQL-2). See the following examples:

```
<PrimaryDbConnectionString>DataSource=ACMSQL2;Initial
Catalog=ACCCM;User ID=acccadmin;Password="EncryptedPassword"</
PrimaryDbConnectionString>
```

```
<SecondaryDbConnectionString>DataSource=ACMSQL2;Initial
Catalog=ACCCM;User ID=acccadmin;Password="EncryptedPassword"</
SecondaryDbConnectionString>
```

5. Locate the Service Default Role and enter “secondary” into the service as shown in the following example:

```
<ServiceDefaultRole>secondary</ServiceDefaultRole>
```

6. Locate the database operational interval <DbOperationInterval> and adjust the interval that the HA Service will check the connectivity status of the Control Manager database. Set this value to either 15 or 30 seconds. See the following example:

```
<DbOperationInterval>15</DbOperationInterval>
```

7. Locate the heartbeat service interval <HeartBeatInterval> and adjust the interval that the HA service on the secondary UI server will communicate with the HA service on the primary UI server. Set this value to either 15 or 30 seconds. See the following example:

```
<HeartBeatInterval>15<HeartBeatInterval>
```

8. Add the FQDN, port number, and name of the HA Service to the secondary UI server (ACM-UI-2). The default port number is 9011 and the default service name is ACCCM HA Service. See the following example:

```
<RemoteServiceHost>ACM-UI-2_FQDN</RemoteServiceHost>
```

```
<RemoteServicePort>9011</RemoteServicePort>
```

```
<RemoteServiceName>ACCCM HA Service</RemoteServiceName>
```

9. Add the FQDN, port number, and name of the HA Service to the primary UI server (ACM-UI-1). The default port number is 9011 and the default service name is ACCCM HA Service. See the following example:

```
<ServiceHost>ACM-UI-1_FQDN</ServiceHost>
```

```
<ServicePort>9011</ServicePort>
```

```
<ServiceName>ACCCM HA Service</ServiceName>
```

10. Confirm that the Database Operation Timeout is set to the default value of 4000 as shown in the following example:

```
<DbOperationTimeout>4000</DbOperationTimeout>
```

11. Confirm that the Database Operation Query is set to the default value of “select top 1 * from locations” as shown in the following example:

```
<DbOperationQuery>SELECT TOP 1 * from Locations</DbOperationQuery>
```

12. Confirm that the Primary Command lists are set as shown in the following example:

```
<Commands retries="1" type="primary">
</Commands>
```

13. Confirm that the Secondary Command lists are set as shown in the following example:

```
<Commands retries="1" type="secondary">
</Commands>
```

14. Confirm that the Critical Command lists are set as shown in the following example:

```
<CriticalErrorCommands retries="1">
</CriticalErrorCommands>
```

15. Save and close the file.

Configuring the HA Service on the secondary application server (ACM-APP-2)

About this task

To configure the HA service on the secondary application server (ACM-APP-2), you must configure the `HA_Service.exe.config` file with the primary application server IP address.

Important:

The `HA_Service.exe.config` file is automatically populated after doing a new installation. Make changes to the file using this procedure only when the populated file is not correct for your installation.

Before you begin

Verify that Control Manager Services have started at least once before you configure the secondary application server HA Service.

Procedure

1. On the secondary application server (ACM-APP-2), open the following file using a text editor:

   InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager \Services\ACCCM HA Service\HA_Service.exe.Config

2. Enter the FQDN of the primary application server (ACM-APP-1) into the `HA_Service.exe.Config` file. See the following example:

   <value>https://*ACM-APP-1_FQDN*:9011/ACCCM HA Service</value>

3. Save and close the file.

Configuring the configuration.xml file on the secondary application server (ACM-APP-2)

Procedure

1. Locate the primary and secondary database connection strings within the configuration file. These connection strings must be updated and must match the string located in the existing `NAV360Config.xml` files on both the primary and secondary application servers (ACM-APP-1 and ACM-APP-2).
2. Copy the database connection string from the `C:\Windows\System32\NAV360Config.xml` file on the secondary application server (ACM-APP-2).
3. Before making any changes in the `configuration.xml` file, create a backup copy of the file. For example, enter the following command:

   `copy [InstallLocation]\Services\ACCCM HA Service\configuration.xml [InstallLocation]\Services\ACCCM HA Service\Backup_configuration.xml`

4. Paste the connection string into the required area in the `configuration.xml` file. Edit the connections strings so that within the secondary application server (ACM-APP-2), both the primary and the secondary connection string points to the secondary database server (ACM-SQL-2). See the following examples:

   ```
   <PrimaryDbConnectionString>DataSource=ACMSQL2;Initial Catalog=ACCCM;User ID=acccadmin;Password="EncryptedPassword"</PrimaryDbConnectionString>
   ```

   ```
   <SecondaryDbConnectionString>DataSource=ACMSQL2;Initial Catalog=ACCCM;User ID=acccadmin;Password="EncryptedPassword"</SecondaryDbConnectionString>
   ```

5. Locate the Service Default Role and enter “secondary” into the service as shown in the following example:

   ```
   <ServiceDefaultRole>secondary</ServiceDefaultRole>
   ```

6. Locate the database operational interval <DbOperationInterval> and adjust the interval that the HA Service will check the connectivity status of the Control Manager database. Set this value to either 15 or 30 seconds. See the following example:

   ```
   <DbOperationInterval>15</DbOperationInterval>
   ```

7. Locate the heartbeat service interval <HeartBeatInterval> and adjust the interval that the HA service on the secondary application server will communicate with the HA service on the primary application server. Set this value to either 15 or 30 seconds. See the following example:

   ```
   <HeartBeatInterval>15<HeartBeatInterval>
   ```

8. Add the FQDN, port number, and name of the HA Service to the primary application server (ACM-APP-1). The default port number is 9011 and the default service name is ACCCM HA Service. See the following example:

   ```
   <RemoteServiceHost>ACM-APP-1_FQDN</RemoteServiceHost>
   ```

   ```
   <RemoteServicePort>9011</RemoteServicePort>
   ```

   ```
   <RemoteServiceName>ACCCM HA Service</RemoteServiceName>
   ```

9. Add the FQDN, port number, and name of the HA Service to the secondary application server (ACM-APP-2). The default port number is 9011 and the default service name is ACCCM HA Service. See the following example:

   ```
   <ServiceHost>ACM-APP-2_FQDN</ServiceHost>
   ```

   ```
   <ServicePort>9011</ServicePort>
   ```

   ```
   <ServiceName>ACCCM HA Service</ServiceName>
   ```

10. Confirm that the Database Operation Timeout is set to the default value of 4000 as shown in the following example:

    ```
    <DbOperationTimeout>4000</DbOperationTimeout>
    ```

11. Confirm that the Database Operation Query is set to the default value of “select top 1 * from locations” as shown in the following example:

    ```
    <DbOperationQuery>SELECT TOP 1 * from Locations</DbOperationQuery>
    ```

12. Confirm that the Primary Command lists are set as shown in the following example:

    ```
    <command type="service" action="start">ACCCM Audit Log Service</
    command>
    ```

    ```
    <command type="service" action="start">ACCCM License Tracker</
    command>
    ```

    ```
    <command type="service" action="start">ACCCM Sync Service</command>
    ```

    ```
    <command type="service" action="start">ACCCM Sphere Feeder</
    command>
    ```

    ```
    <command type="service" action="start">ACCCM AD Sync</command>
    ```

    ```
    <command type="service" action="start">ACCCM Schedule Server</
    command>
    ```

    ```
    <command type="service" action="start">ACCCM CM Syslog Server</
    command>
    ```

13. Confirm that the Secondary Command lists are set as shown in the following example:

    ```
    <command type="service" action="start">ACCCM Audit Log Service</
    command>
    ```

    ```
    <command type="service" action="start">ACCCM License Tracker</
    command>
    ```

```
<command type="service" action="start">ACCCM Sync Service</command>
<command type="service" action="start">ACCCM Sphere Feeder</
command>
<command type="service" action="start">ACCCM AD Sync</command>
<command type="service" action="start">ACCCM Schedule Server</
command>
<command type="service" action="start">ACCCM CM Syslog Server</
command>
```

14. Confirm that the Critical Command lists are set as shown in the following example:

```
<command type="service" action="start">ACCCM Audit Log Service</
command>
<command type="service" action="start">ACCCM License Tracker</
command>
<command type="service" action="start">ACCCM Sync Service</command>
<command type="service" action="start">ACCCM Sphere Feeder</
command>
<command type="service" action="start">ACCCM AD Sync</command>
<command type="service" action="start">ACCCM Schedule Server</
command>
<command type="service" action="start">ACCCM CM Syslog Server</
command>
```

15. Save and close the file.

Starting the HA services after editing the configuration files

About this task

To activate all of the changes you made in the configuration files, you must start the HA services on both application servers.

Procedure

1. Log on to Windows on the primary application server (ACM-APP-1).
2. Go to **Start** > **Run**.
3. Enter `services.msc` and press **Enter**.
4. In the Services window, right-click the **ACCCM HA Service** service and select **Start**.

The system starts the service.

Important:

The HA Service will start only if you have properly done the procedure Binding the certificate to SSL port 9011 for HA on page 60 when installing certificates. If the HA Service does not start, confirm that this procedure was done.

5. In the Services window, right-click the following services and select **Start**:
   - **ACCCM Sync Service**
   - **ACCCM CM Syslog Server**
   - **ACCCM Sphere Feeder**
   - **ACCCM AD Sync**
   - **ACCCM Audit Log Service**
   - **ACCCM License Tracker**
   - **ACCCM Schedule Server**

   The system starts the services.
6. Log on to Windows on the secondary application server (ACM-APP-2).
7. Go to **Start** > **Run**.
8. Enter `services.msc` and press **Enter**.
9. In the Services window, right-click the **ACCCM HA Service** service and select **Start**.

   The system starts the service.
10. In the Services window, right-click the following services and select **Stop**:
    - **ACCCM Sync Service**
    - **ACCCM CM Syslog Server**
    - **ACCCM Sphere Feeder**
    - **ACCCM AD Sync**
    - **ACCCM Audit Log Service**
    - **ACCCM License Tracker**
    - **ACCCM Schedule Server**

    The system stops the services.
11. Repeat this procedure on the primary UI server (ACM-UI-1) and the secondary UI server (ACM-UI-2).

Chapter 11: Configuring the Experience Portal billing

Configuring the Experience Portal billing service on the primary application server (ACM-APP-1)

About this task

Important:

When deploying xCaaS with Usage Metering (UM) Collector software and the VMware HA feature, you can skip this entire chapter.

To configure the Experience Portal billing service on the primary application server (ACM-APP-1), you must configure the `AAEPBilling.exe.config` file.

Before you begin

Get the host name or IP address of the primary Control Manager SQL billing server.

Procedure

1. Log on to Windows on the primary application server (ACM-APP-1).
2. Open the following file using a text editor:

   ```
   C:\Program Files (x86)\Avaya\ACM Billing\Services\AAEPBilling
   \AAEPBilling.exe.config
   ```

   See the following example:

```
AAEPBilling.exe.config
<?xml version="1.0"?>
<configuration>
  <connectionStrings>
    <add name="connStr_MSSQL_Target" connectionString="Data Source=anavbillingsql1 ; Initial Catalog=ACM_BILLING;
  </connectionStrings>
  <appSettings>
    <!-- When to start sync, hh:ss, 24h format -->
    <add key="SyncStartTimeOfDay" value="01:30" />
    <!-- Sync interval time. Default 1440 - one day -->
    <add key="SyncInterval" value="1440"/>
    <!-- SqlBulkCopy batch size. Default value 25000. -->
    <add key="BulkCopyBatchSize" value="25000"/>
    <!-- The time in seconds to wait for the command to execute, for source database. The default is 30 seconds. -
    <add key="CommandTimeoutSourceDB" value="30"/>

    <!-- Log Settings START -->
    <add key="LogName" value="AAEPBilling"/>
    <add key="LogLevel" value="Info"/> <!-- No_Log, Fatal, Error, Warn, Info, Trace, Debug -->
    <add key="LogPath" value=""/>
    <add key="MaxArchiveFiles" value="10"/>
    <add key="MaxFileSize" value="10"/> <!-- in MB -->
    <!-- Log Settings END -->
    <!--  When to start sync, hh:ss, 24h format  -->
    <!--  Sync interval time. Default 1440 - one day  -->
    <!--  SqlBulkCopy batch size. Default value 25000.  -->
    <!--  Log Settings START  -->
    <!--  in MB  -->
    <!--  Log Settings END -->
  </appSettings>
```

3. Verify administration of the following parameters. If the parameters are not already administered, set them to the following values:
   - Set the **Data Source** parameter to the host name or IP address of the primary Control Manager SQL billing server.
   - Set the **SyncStartTimeOfDay** parameter to 01:30.
   - Set the **SyncInterval** parameter to 1440.
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 **AAEPBilling** and select **Restart**.

   The system restarts the service.

Configuring the Experience Portal billing service on the secondary application server (ACM-APP-2)

About this task

To configure the Experience Portal billing service on the secondary application server (ACM-APP-2), you must configure the `AAEPBilling.exe.config` file.

Before you begin

Get the host name or IP address of the secondary Control Manager SQL billing server.

Procedure

1. Log on to Windows on the secondary application server (ACM-APP-2).
2. Open the following file using a text editor:

   `C:\Program Files (x86)\Avaya\ACM Billing\Services\AAEPBilling\AAEPBilling.exe.config`

   See the following example:

```
AAEPBilling.exe.config
<?xml version="1.0"?>
<configuration>
  <connectionStrings>
    <add name="connStr_MSSQL_Target" connectionString="Data Source=anavbillingsql1 ; Initial Catalog=ACM_BILLING;
  </connectionStrings>
  <appSettings>
    <!-- When to start sync, hh:ss, 24h format -->
    <add key="SyncStartTimeOfDay" value="01:30" />
    <!-- Sync interval time. Default 1440 - one day -->
    <add key="SyncInterval" value="1440"/>
    <!-- SqlBulkCopy batch size. Default value 25000. -->
    <add key="BulkCopyBatchSize" value="25000"/>
    <!-- The time in seconds to wait for the command to execute, for source database. The default is 30 seconds. -
    <add key="CommandTimeoutSourceDB" value="30"/>

    <!-- Log Settings START -->
    <add key="LogName" value="AAEPBilling"/>
    <add key="LogLevel" value="Info"/> <!-- No_Log, Fatal, Error, Warn, Info, Trace, Debug -->
    <add key="LogPath" value=""/>
    <add key="MaxArchiveFiles" value="10"/>
    <add key="MaxFileSize" value="10"/> <!-- in MB -->
    <!-- Log Settings END -->
    <!--  When to start sync, hh:ss, 24h format  -->
    <!--  Sync interval time. Default 1440 - one day  -->
    <!--  SqlBulkCopy batch size. Default value 25000.  -->
    <!--  Log Settings START  -->
    <!--  in MB  -->
    <!--  Log Settings END -->
  </appSettings>
```

3. Verify administration of the following parameters. If the parameters are not already administered, set them to the following values:
   - Set the **Data Source** parameter to the host name or IP address of the secondary Control Manager SQL billing server.
   - Set the **SyncStartTimeOfDay** parameter to 01:30.
   - Set the **SyncInterval** parameter to 1440.
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 **AAEPBilling** and select **Restart**.

   The system restarts the service.

Chapter 12: Testing the installation

Starting the Control Manager License Server

About this task

To test the installation and to start the system, start the Control Manager License Server. The License service must be started successfully on both primary and secondary application servers.

Before you begin

Confirm that certificates have been installed.

Procedure

1. Go to **Start** > **Run**.
2. Enter `services.msc` and press **Enter**.

   Note:

   The license server must start before any other services are started.
3. In the Services window, right-click **ACCCM License Server** and select **Start**.

   The system starts the service.
4. If the service fails to start, verify the service log files for details on any errors. The default location of the License Server log file is:

   `[Install Location]\Services\ACCCM License Server\logs`

Logging on to the Control Manager user Interface

Before you begin

Confirm that certificates were installed as described in the Control Manager installation and upgrade documents.

Procedure

1. Open your browser and enter the following URL in the address field:

   `https://<server name>/ACCCMPortal`

   Where *<server name>* is the host name or FQDN of the Control Manager system.

The system displays the following screen:

2. Enter your username (enter `itnv` if you are logging in for the first time) in the **Username** field.
3. Enter your password (enter `itnv` if you are logging in for the first time) in the **Password** field.
4. Select the user interface language for which you want to use.

   Important:

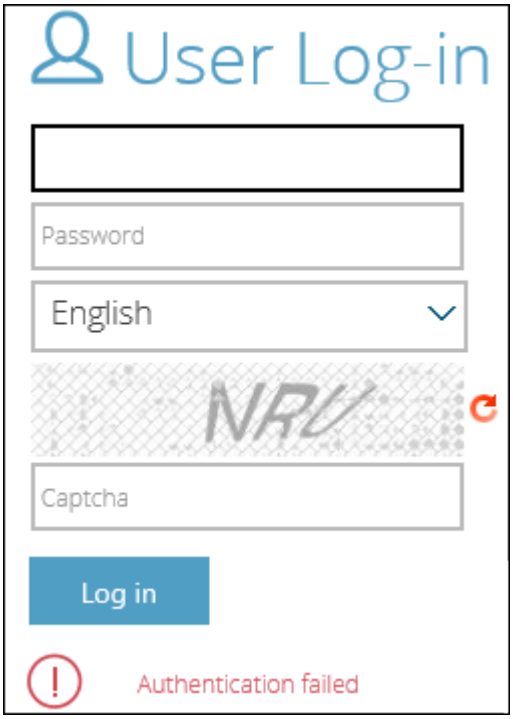
   The first time you login, the system prompts you to enter a new password.

   Remember this password since it is now the new password for your only user ID until you create new Control Manager users.

   You must create system administrator users. Do not use the default itnv or admin user IDs for your day to day tasks. Create administrator users and assign roles to those users. For a multi-tenant deployment, it is essential to use tenant-specific user IDs.
5. Click **Login**.

   Note:

   If you incorrectly enter your password three times, the system will require you to enter a CAPTCHA string of characters before attempting to login again.



Testing the HA installation

About this task

This section layout the steps Avaya recommends for testing the HA Service and explains the different results that are expected.

Before you begin

Install Telnet client software before running these tests. You need the Telnet client to test the connections between servers.

Procedure

1. License tracker and Audit log Services should be started on the primary application server (ACM-APP-1), and stopped on the secondary application server (ACM-APP-2).
2. Set these services to Manual Start on both of the application servers.
3. Make sure that the `NAV360config.xml` files on the primary and secondary application servers are both pointing to the primary ACM-SQL-1 server.
4. Start the HA service on the primary application server ACM-APP-1.
5. Start the HA service on the secondary application server ACM-APP-2.
6. Check the two logs created in each of the log folders of the HA Service on both of the primary and secondary application servers.

Application Server	HA Service Log Error
ACM-APP-1	*[Install Location]*\Services\ACCCM HA Service\Logs\
ACM-APP-2	*[Install Location]*\Services\ACCCM HA Service\Logs\

In case of an error log the first time, it may be a result of having to encrypt passwords entered in the configuration file.

7. Continue to monitor the `NAV360Config.xml` file to see if the database connection string has changed and if the services on the application servers have stopped and started. If the error log continues to get updated (check the time stamp of the file), something is wrong. Refer to the following steps:

   a. If you see additional logs created with “error” or “critical error” in the file name stamp, stop the HA services on the application servers and check the HA configuration for any mistakes and if required reconfigure everything back to the initial setting and try again.

   b. In the case that port 9011 might be blocked by a firewall or is not available, confirm that you can telnet from one application server to the other application server. Do this by starting the HA services and entering the following at the command prompt on both the primary and secondary application servers:

      `telnet remoteAPPserverIPaddress 9011`

      The result should be a blank screen. If you get an error, it confirms there is a connection or port issue.

   c. If no logs are created at all, you must add permissions on the “AVAYA” installation folder. Usually this can be done by setting full (security) permissions on the folder for “everyone”.

      If the services will not start, you have a configuration error, usually relating to database connection strings and\or IP addresses in the `configuration.xml` or `HA_service.exe.config` file.

      Note:

      You might receive an error log the first time around on account of having to encrypt passwords that you entered into the configuration file. If this happens, continue to monitor the `NAV360Config.xml` files to see if a database string change has occurred and if the services have stopped and started.

      If the error log continues to get updated (check the time stamp of the file), something is misconfigured.

8. Stop the MSSQL Service on the primary database server to simulate a database failure. If the installation was successful, the following occurs:

   a. The `NAV360Config.xml` files have been updated with the secondary database connection string (ACM-SQL-2) string on the primary application server (ACM-APP-1)

and on the secondary application server (ACM-APP-2) i.e. the secondary NAV360 files were initially configured with the primary SQL connection string, in which a failover would cause the HA service on the secondary application to change the connection strings to the secondary DB strings).

b. The seven services (License Tracker, Audit Log, AD Sync, CM Syslog Server, Schedule Server, Sphere Feeder, Sync Service) have Stopped on the primary application server and started on the secondary application server.

Note:

If only one service has started on the secondary application server, wait 5-8 minutes and then check if the second service has started.

9. Troubleshoot the installation using the following procedure:

   a. The services (License Tracker and Audit Log) did not stop on the primary application server. This could be caused by no error logs appearing after stopping the MSSQL Service. Check all connection strings in the `HA Service` and `NAV360Config.xml` files.

   b. Nothing has changed on secondary application server which could a configuration error regarding the adjunct server on one or both of the HA server configuration files from one or both of the application servers. For example, the wrong Service name was entered in the `configuration.xml` file or the wrong IP addresses were added to the file.

   c. Another failure could be that port 9011 is closed or blocked on both of the servers.

Verifying the TLS version

About this task

HTTPS requires that you use TLS Version 1.2. Use this procedure to verify that you are using TLS Version 1.2

Procedure

1. Open a supported web browser.
2. Log on to the Control Manager administrative user interface.
3. Right-click the browser window and click **Properties**.
4. In the Properties window, confirm that the connection is using TLS 1.2. If you are not using TLS 1.2, you must install TLS 1.2 on the Microsoft Windows system.

Rollback to the initial HA service configuration

About this task

This section will show the steps required to roll back the environment to the initial HA service configuration after a failover scenario has concluded and the connection to the primary SQL server has been restored.

Before you begin

Before performing a rollback, the primary SQL Service and Agent must be back up and started.

Procedure

1. Stop both HA services on the primary and secondary application servers (ACM-APP-1 and ACM-APP-2).
2. Make sure that the HA services on the application servers are set to “manual” and not “automatic\Automatic Delayed” start. This is to insure that the services do not start automatically during the rollback procedure.
3. Make sure to update the `NAV360Config.xml` file located in `c:\Windows\System32` back to the primary database connection string. Confirm that the same database connection string has been entered into the HA Service `configuration.xml` file.
4. Check that the `NAV360config.xml` file located in `c:\Windows\syswow64` was also updated from the change you made to the first file. If your Hard link is still in place, the file should have been updated when you saved the file in System32. Do this on both the primary application and secondary application servers.
5. Stop the seven services (License Tracker Audit Log,AD Sync, CM Syslog Server, Schedule Server, Sphere Feeder, Sync Service) on the secondary application server, and start the seven services (License Tracker Audit Log,AD Sync, CM Syslog Server, Schedule Server, Sphere Feeder, Sync Service) on the primary application server.
6. Delete the logs from the HA Services log folder on both the primary and secondary application servers.
7. Start the primary HA service, followed by the secondary HA service
8. Go through the testing procedure as outlined in the previous section. If no errors are received or you have only two logs files (no error or critical error log file), you have successfully rolled back the HA service.

Checking basic sanity after an upgrade

Procedure

After an upgrade, make spot checks on some of the known administration data to confirm that the upgrade was successful. At a minimum, check the following items:

- Locations

- Profiles
- Templates
- Groups
- Schedules
- Avaya one-X® Agent administration
- Bulk jobs

Chapter 13: 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.
Avaya Control Manager Customer Requirements	This document describes the prerequisites that customers must follow before having Control Manager installed and the database maintenance procedures customers should follow during normal operation.
Installation	
Installing Avaya Control Manager for Enterprise - Non-High Availability	This document describes how to install, configure, and test a non-HA Enterprise Control Manager system.
Installing Avaya Control Manager for Enterprise - High Availability	This document describes how to install, configure, and test an HA Enterprise Control Manager system.
Installing Avaya Control Manager for Partner Cloud Powered by Avaya xCaaS	This document describes how to install, configure, and test an xCaaS Control Manager system.
Deploying Contact Center Applications on Amazon Web Services	This document describes general information about how you must deploy a variety of Avaya Contact Center applications on Amazon Web Services.
Upgrades	
Upgrading to Avaya Control Manager 8.0.4 for Enterprise - Non-High Availability	This document describes how to upgrade a non-HA Enterprise Control Manager system from an earlier release to the current release. The document includes upgrade checklist, upgrade procedures, and verification procedures for each supported upgrade path.
Upgrading to Avaya Control Manager 8.0.4 for Enterprise - High Availability	This document describes how to upgrade an HA Enterprise Control Manager system from an earlier release to the current release. The document includes upgrade checklist, upgrade procedures, and verification procedures for each supported upgrade path.

Table continues…

Title	Description
Upgrading to Avaya Control Manager 8.0.4 for Partner Cloud Powered by Avaya xCaaS	This document describes how to upgrade an xCaaS Control Manager system 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 Control Manager Central License and Traffic Tracker	This document describes how to use Control Manager Central License and Traffic Tracker.
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 API	This document describes how to use the Control Manager API.
Maintenance and Troubleshooting	
Maintaining and Troubleshooting Avaya Control Manager	This document describes maintenance procedures and troubleshooting scenarios for Control Manager.

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://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 an appropriate release number.
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 displays the documents only from the selected category.

7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at http://documentation.avaya.com/.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open http://support.avaya.com/.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- 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 **My Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add content 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 content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **My Content** > **Watch list** menu, and do the following:
  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - 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 portal.
- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.

- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. 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® Solution Design Fundamentals (includes Avaya Control Manager PIDs)
3371T	APDS Avaya Customer Engagement Solutions Online Test
3470T	Avaya Oceana® Solution Design Fundamentals Online Test
Technical Services	
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
7092W	Installing Avaya Control Manager
7093W	Upgrading and Supporting Avaya Control Manager for Cloud Service Providers
7094W	Configuring Avaya Control Manager for Enterprise
7095W	Upgrading and Supporting Avaya Control Manager for Enterprise
7090W	Implementing and Supporting Avaya Control Manager for Enterprise
7091W	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® Solution

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Support

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

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

Amazon Web Services 23
architecture
    overview 10
audience 8

B

backing up 73, 125
backup 72, 124
billing configuration for secondary data center 111, 146
billing count accuracy 108, 143
billing engine
    recovery properties 114, 149
    startup properties 114, 149
bind port 9011 60

C

certificates 22, 53
Certificate Signing Request 54
checklist 69, 121
client operating system 21
collation 20
collection
    delete 203
    edit name 203
    generating PDF 203
    sharing content 203
configuration.xml
    configuring on the primary application server 181
    configuring on the primary UI server 178
    configuring on the secondary application server 187
    configuring on the secondary UI server 184
configuring
    billing software 107, 143
content
    publishing PDF output 203
    searching 203
    sharing 203
    watching for updates 203
CSR 54

D

database
    collation 20
    shared 19
databases 30, 73, 123, 125
    restoring 76
dedicated IP addresses 32
disaster recovery 28
documentation portal 203
    finding content 203
    navigation 203
dual data center 28

E

enabling
    SSL 62
Experience Portal billing service
    configuring on ACM-APP-1 191
    configuring on ACM-APP-2 192
extension number delimiters 108, 143

F

failover 36
finding content on documentation portal 203

H

hardware requirements
    multiple host 13
HA requirements 29
HA services
    configuring primary application server 180
    configuring primary UI server 177
    configuring secondary application server 177, 186
    configuring secondary UI server 183
    Control Manager services 175
    overview 173
    rollback 199
    starting 189
    testing the installation 196

I

InSite Knowledge Base 205
installation
    considerations 71, 122
    prerequisites 39
installing
    certificates 53
    IIS 41, 46
    Microsoft SQL Server 51
    root certificate 61
    signed certificate 59
installing billing software 104, 139
installing Control Manager software 78, 84
installing UI software 90, 95

J

Java Runtime Environment 22

L

latest software patches 17
license server 66, 194
licensing 23, 101, 138
logging on 194

M

Microsoft DTC 156
migrating the database 68, 69, 73, 76, 125
migration testing 118
My Docs 203

N

network load balancer 31

O

OS considerations 18

P

patch information 17
patch uninstall 129
PCN 17
prerequisites 39
PSN 17
publication 165
purpose 8

R

reference configuration 25
related documentation 201
release notes for latest software patches 17
removing replication 127
replication 33, 154, 165
    enabling 169
    removing 127
    SQL 157
requirements
    client Web browser 21
    database software 18
    hardware 13
    Java Runtime Environment 22
    operating system 18
    software 17
restore testing 118
restoring databases 76
restoring the database 68, 69, 73, 76, 125
roll back HA services 199
root certificate 61

S

scheduled jobs 102
searching for content 203
secure browser access 62
server worksheet 37
shared database 19
sharing content 203
signed certificate 59
single data center 28
software patches 17
starting the license server 194
stopping Control Manager services 129, 176
submitting CSR to CA 56
support 205
switchover 36

T

testing the migration 118
testing the restore 118
TLS version 198
topology
    overview 12
training 204

U

uninstalling
    billing software 103, 139
uninstall patches 129
upgrade
    considerations 71, 122
upgrade checklist 69, 121
upgrade process
    database migration 68
    in-place upgrade 120
upgrade scenarios 9
upgrade verification 199
upgrading
    Windows 65
upgrading Control Manager software 131

V

verifying
    TLS version 198
videos 205
virtual IP address 31
virtualization support 22

W

watch list 203
Windows OS and SQL combinations 21
worksheet
    multiple host configuration 37