Upgrading to Avaya Control Manager 8.1 for Enterprise - Legacy High Availability

Release 8.1
Issue 2
October 2019

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

Third Party Components

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

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

Service Provider

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

This document describes how to upgrade Avaya Control Manager Releases 8.0.x to Release 8.1 for Enterprise in Legacy High Availability (HA) distributed configurations. The configurations include the Legacy HA deployment on two application servers and two database servers using the Microsoft SQL database software. This legacy feature is supported in Release 8.1, but is expected to be deprecated in some future release. Legacy HA operates in Single or Dual Data Center environments.

Upgrade of Control Manager software is done by Avaya personnel with assistance from customer administrators.

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 Manager software 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 paths

Upgrades to Control Manager Release 8.1 are done using the following methods:

The following table describes each possible upgrade scenario and which type of upgrade process you must use.

Current system	Upgraded system	See procedures in the following chapter:
Control Manager 7.1.2.2 with Superpatch 1 or 2 on any older Microsoft Windows Server OS version and any older Microsoft Windows SQL Server version	Control Manager 8.1.x.x on Microsoft Windows Server OS 2012 R2 and Microsoft Windows SQL Server 2012 or 2014	*Upgrading a system using database migration*
Control Manager 7.1.2.2 with Superpatch 1 or 2 on any older Microsoft Windows Server OS version and any older Microsoft Windows SQL Server version	Control Manager 8.1.x.x on Microsoft Windows Server OS 2016 and Microsoft Windows SQL Server 2014, 2016, or 2017	*Upgrading a system using database migration*
Control Manager 7.1.2.2 with Superpatch 1 or 2 on any older Microsoft Windows Server OS version and any older Microsoft Windows SQL Server version	Control Manager 8.1.x.x on Microsoft Windows Server OS 2016 and Microsoft Windows SQL Server 2016 or 2017	*Upgrading a system using database migration*
Control Manager 8.0.x.x (8.0.4.x for deployments that include the Avaya Oceana® Solution) on Microsoft Windows Server OS 2012 R2 and Microsoft Windows SQL Server 2012 or 2014	Control Manager 8.1.x.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.x.x (8.0.4.x for deployments that include the Avaya Oceana® Solution) on Microsoft Windows Server OS 2012 R2 and Microsoft Windows SQL Server 2012 or 2014	Control Manager 8.1.x.x on Microsoft Windows Server OS 2016 and Microsoft Windows SQL Server 2014, 2016, or 2017	*Upgrading a system using database migration*

Table continues…

Current system	Upgraded system	See procedures in the following chapter:
Control Manager 8.0.x.x (8.0.4.x for deployments that include the Avaya Oceana® Solution) on Microsoft Windows Server OS 2016 and Microsoft Windows SQL Server 2016 or 2017	Control Manager 8.1.x.x on Microsoft Windows Server OS 2016 and Microsoft Windows SQL Server 2016 or 2017	*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 Release 8.0.4.x before you can upgrade to Release 8.1. See the following documents for more information about upgrading to Release 8.0.4.x:

- *Upgrading to Avaya Control Manager 8.0.4 for Enterprise - Non-High Availability*
- *Upgrading to Avaya Control Manager 8.0.4 for Enterprise - High Availability*

Note:

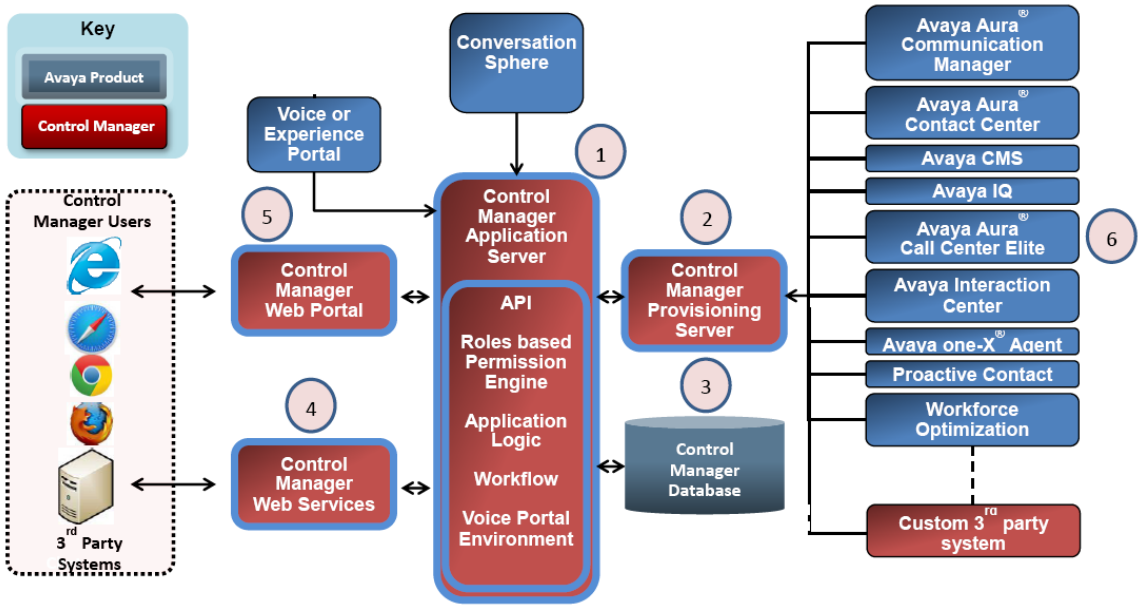
When upgrading a Legacy HA deployment, you must remove replication between the two systems, upgrade the primary system, followed by the secondary system, then re-enable replication between the two systems. The upgrade process for a Legacy HA system is explained in detail later in this document.

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.

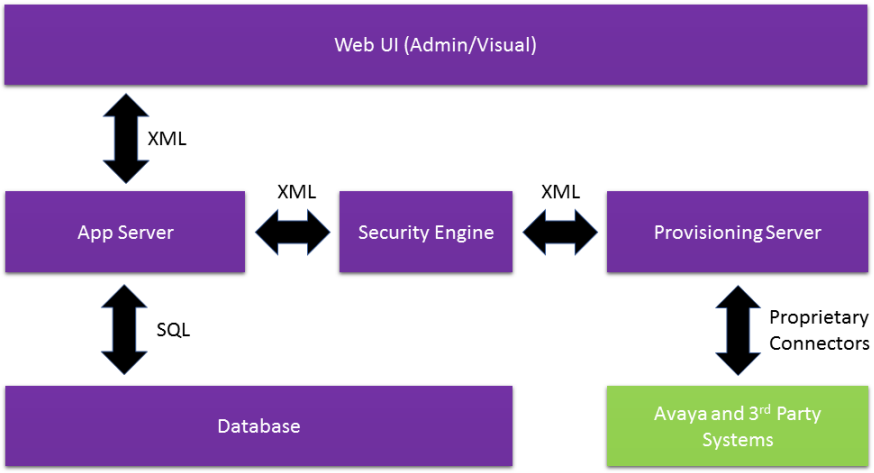
Control Manager uses the system architecture, software integrations, and software components to provide a multi-channel contact center solution.

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



Call-out	Component	Description
1	Application Server	The Control Manager application server is the component that 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	The Control Manager Provisioning server is responsible for provisioning components from Control Manager with the different Avaya Team Engagement and Customer Engagement 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	This is 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 Control Manager Web Portal is the management interface that provides complete access to all the features of Control Manager. The Web Portal resides on the application servers. The Web Portal can be used in a variety of scenarios ranging from product-specific managements to overall suite management.
6	Connectors	Control Manager Connectors are used to integrate and manage the Avaya Team Engagement and Customer Engagement 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: Reference configurations

About reference configurations

The Legacy HA configuration supports Single and Dual Data Center environments.

Important:

You cannot mix Multiplex HA configuration elements with Legacy HA configurations.

Legacy HA configurations

Reference configurations for Legacy HA deployments

The Avaya Control Manager Legacy HA reference configuration uses two identical Control Manager deployments that operate in an Active/Active mode and consist of the following servers:

- Primary application server (ACM-APP-1), and primary database (ACM-SQL-1) server
- Secondary application server (ACM-APP-2), and secondary database (ACM-SQL-2) server

Note:

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

Control Manager software is installed on the primary application server (ACM-APP-1) and secondary application server (ACM-APP-2).

The primary application servers represent the primary application logical layer. The secondary application servers represent the secondary application logical layer. There are two Control Manager SQL database servers (ACM-SQL-1/ACM-SQL-2) deployed in an Active/Active mode.

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 administrative users.

In an HA configuration, a service failure, hardware, network, or database failure can initiate a switchover if the following conditions are met:

- The primary and secondary Control Manager application servers are in a running state.
- Legacy HA is enabled on the Control Manager application servers.
- The Control Manager primary database server and secondary database server are synchronized using either bidirectional or unidirectional replication.
  - Bidirectional replication is used for Enterprise deployments that are not part of an Avaya Oceana® Solution Geo Redundant HA deployment.
  - Unidirectional replication is used for Enterprise deployments that are part of an Avaya Oceana® Solution Geo Redundant HA deployment.

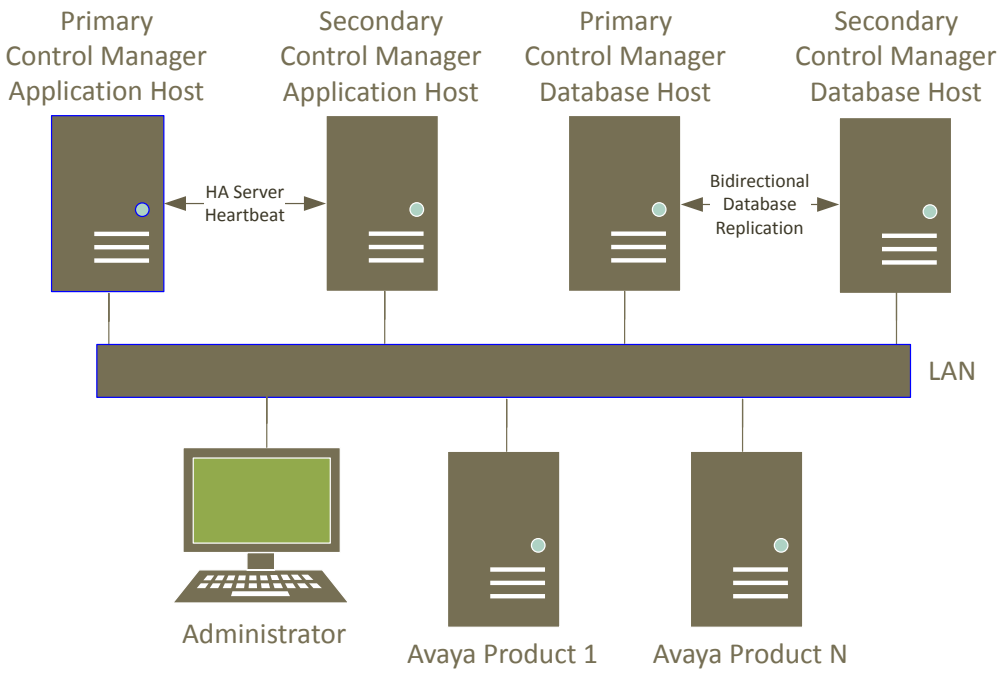
If the primary Control Manager application server fails and if the switchover conditions are met, a complete server switchover occurs to the secondary Control Manager application server. The seven mutually exclusive services (Audit Log, Sync, Schedule Server, and so on) on the secondary server are started which carries the activity load during the outage.

Deployment considerations for a single data center

Control Manager Legacy HA for Enterprise 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).

In a basic Control Manager Legacy 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 a Legacy HA environment have identical configurations, providing the full Control Manager capabilities.

The following architecture diagram illustrates a typical single data center using a Legacy HA configuration.



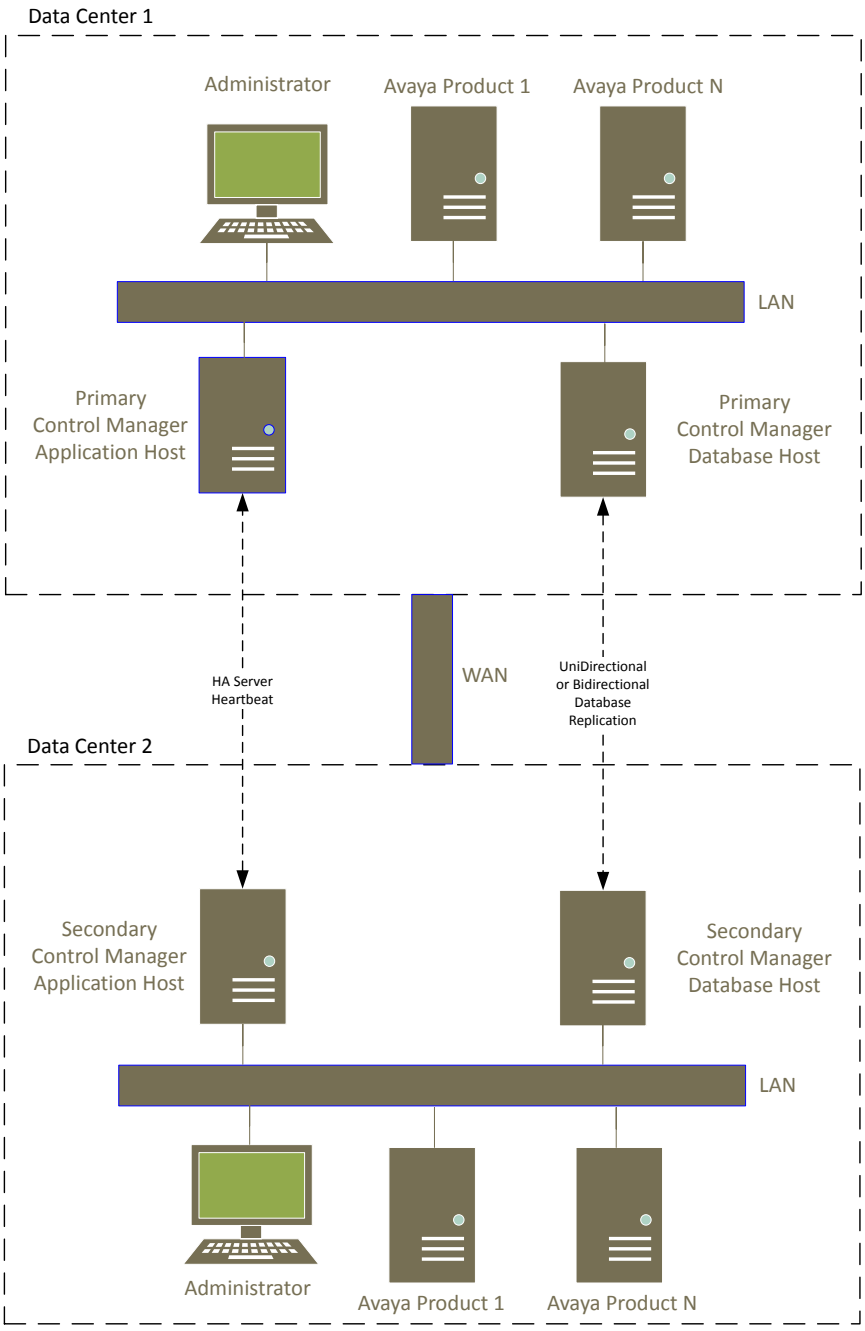
Deployment considerations in a dual data center or disaster recovery configuration

Note:

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

Control Manager Legacy HA for Enterprise deployments using non-ESS Communication Manager systems 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.

The following architecture diagram illustrates a typical dual data center using a Legacy HA configuration.



With Legacy HA:

- The primary and secondary Control Manager application servers are in a running state.
- Legacy HA is enabled on the Control Manager application servers.

- The Control Manager primary database server and secondary database server are synchronized using either bidirectional or unidirectional replication.
  - Bidirectional replication is used for Enterprise deployments that are not part of an Avaya Oceana® Solution Geo Redundant HA deployment.
  - Unidirectional replication is used for Enterprise deployments that are part of an Avaya Oceana® Solution Geo Redundant HA deployment.

Using Legacy 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 a Legacy HA configuration have identical deployments, providing full Control Manager capabilities.

Legacy HA 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 Legacy HA database pair, and between Control Manager and the managed systems.

Requirements for Legacy HA deployments

To prevent failure in the data replication, ensure that the following requirements are met for deploying Control Manager in an Active/Active Legacy 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 Legacy HA deployments, the Control Manager functional components – Web Server, Application Server, and Provisioning Server – are all installed and deployed on

the same server. Separating these components to different servers is not a supported configuration.

- Control Manager Legacy 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 Legacy HA must be configured only in a 1+1 configuration.
- Both the primary and secondary Control Manager application 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.

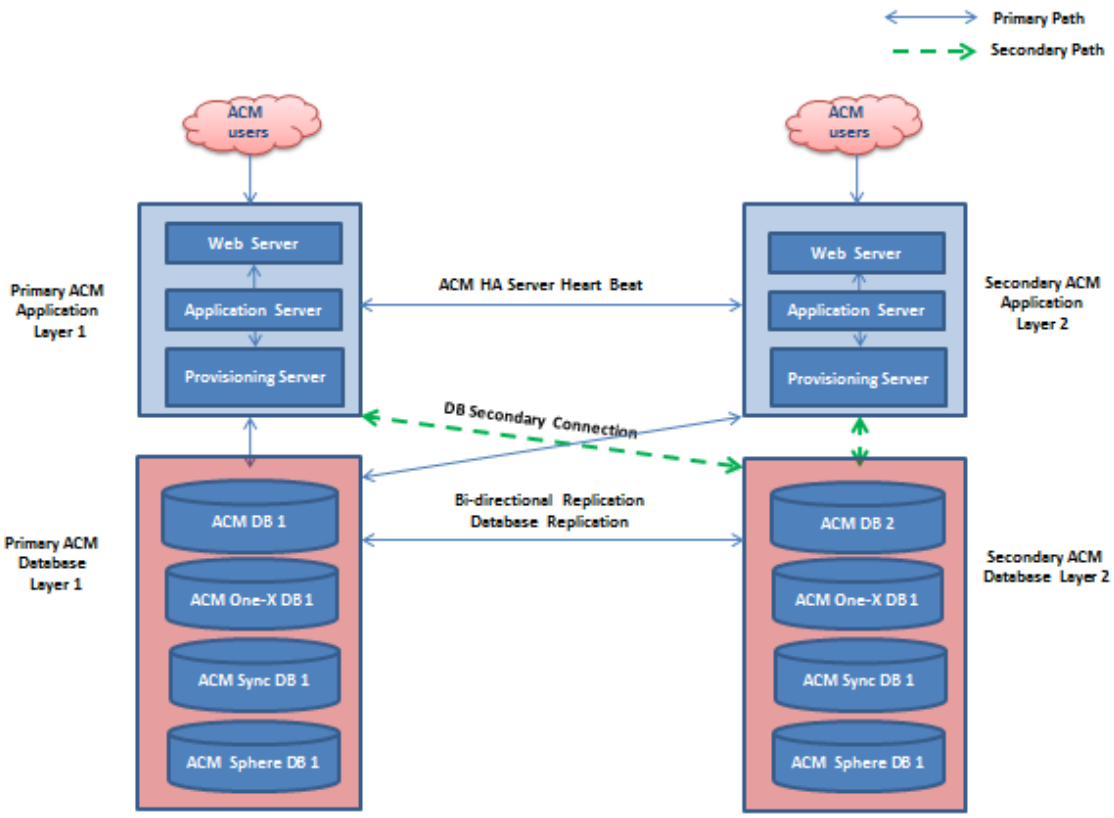
Deploying Control Manager using dedicated IP addresses

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 database instances is synchronized to all of the other database 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 in a Legacy HA deployment

Control Manager Legacy HA for Enterprise deployments using non-ESS Communication Manager systems leverages the bidirectional transactional replication feature that is available in Microsoft SQL server software. This means is that, under normal operating conditions, any change to the databases on the primary database server (ACM-SQL-1) will be automatically pushed out to the databases on the secondary database server (ACM-SQL-2). The same applies in reverse: any changes made to the databases on the secondary database server (ACM-SQL-2) result in an automated update to the databases on the primary database server (ACM-SQL-1).

Control Manager Legacy HA for Enterprise deployments using Survivable ESS Communication Manager systems leverages the unidirectional and bidirectional transactional replication feature that is available in Microsoft SQL server software. This means is that, under normal operating conditions, any change to the databases on the primary database server (ACM-SQL-1) will be automatically pushed out to the databases on the secondary database server (ACM-SQL-2). However, the same does not apply in reverse for just the ACCCM database: any changes made to the ACCCM database on the secondary database server (ACM-SQL-2) must be manually updated to the ACCCM database on the primary database server (ACM-SQL-1); all other supported databases are updated using bidirectional replication.

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

Within a Control Manager Legacy HA environment, each Control Manager instance is working with a dedicated database layer. The two Microsoft SQL database servers (ACM-SQL-1 and 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 Legacy HA for Enterprise supports in a single or dual data center when not using a Survivable ESS Communication Manager system.

Database	Replication	Direction
ACCCM	Transactional	Bidirectional
ACCCMONEXDB	Transactional	Bidirectional
ACCCMCMSYSLOG	Transactional	Bidirectional
ACCCMSYNC	Transactional	Bidirectional

The following table illustrates the replication strategy for each of the SQL databases that Control Manager Legacy HA for Enterprise supports in a single or dual data center when using a Survivable ESS Communication Manager system.

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

Note:

The ACCCMAVP database is not replicated.

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]
ACCCMCMSYSLOG	CM_Syslog_RawMessages_Temp

Switchover and Failover methods

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.

Interactions when using HA deployments

Interaction	Solution
Access to Avaya Aura® Contact Center administration is only available when a user is connected to the application server where the Sync service is running.	Users that need to access Avaya Aura® Contact Center administration must manually connect to the application server where the Sync service is running.

Chapter 4: Requirements

Hardware and VMware requirements

Control Manager is available in the following configurations:

- Dual host Legacy HA configuration, using a pair of application servers and a pair of database servers when using standard Microsoft SQL database software.

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 meet these specifications to support the software.

When performing an upgrade of Control Manager that is already on Microsoft Windows 2012 R2, you must confirm that the current hardware or VMware servers meet these specifications to support the software.

When performing an upgrade of Control Manager and also upgrading to Microsoft Windows 2016, you must confirm that the current hardware or VMware servers meet these specifications to support the software.

Related links

Dual host server configuration on page 22

Dual host server configuration

The Dual host server configuration supports the Control Manager software on one server and the standard Microsoft SQL database software on a separate server.

The following tables list the minimum hardware and virtual machine requirements for the Dual host server configuration.

Important:

When deploying an HA configuration, you must have identical servers for each server type, application host and database host.

Requirements for application server — Enterprise configurations

Important:

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

The following table lists the minimum virtual machine resource requirements:

VMware resource	Value
vCPU Cores	4
Minimum CPU speed	2.4 GHz x64 processor or equivalent
Memory	12 GB
Storage reservation	300 GB or higher
Shared NICs	One @ 1,000 Mbps
Static or Dynamic resource requirements	Static

The following table lists the minimum hardware server requirements:

Hardware component	Value
Processor	Single Quad Core Processor (4 CPUs)
RAM	12 GB
Hard disk[1]	300 GB free space
Network interface controller	Single Ethernet

Requirements for SQL database server

The following table lists the minimum virtual machine resource requirements:

VMware resource	Value
vCPU Cores	4
Minimum CPU speed	2.4 GHz x64 processor or equivalent
Memory	12 GB
Storage reservation	300 GB or higher
Shared NICs	One @ 1,000 Mbps
Static or Dynamic resource requirements	Static

The following table lists the minimum hardware server requirements:

Hardware component	Value
Processor	Single Quad Core Processor (4 CPUs)
RAM	12 GB
Hard disk[1]	300 GB free space
Network interface controller	Single Ethernet

[1] IOPS is 3000 (average read + average write) requests per second. Ratio of average write-to-read is 19-to-1.

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 24
Supported server operating system software requirements on page 24
Supported database server software requirements on page 26
Supported Microsoft Windows OS and Microsoft SQL combinations on page 29
Supported client Web browser and client operating system software requirements on page 29
Certificate requirements on page 30
Java Runtime Environment requirements on page 30
Transport Layer Security (TLS) support on page 30

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 https://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 2016 Standard Edition (required when using the Microsoft SQL AlwaysOn feature)

- Microsoft Windows Server 2016 Datacenter Edition (required when using the Microsoft SQL AlwaysOn feature)
- Microsoft Windows Server 2012 R2 Standard Edition when using the regular Microsoft SQL software
- Microsoft Windows Server 2012 R2 Datacenter Edition when using the regular Microsoft SQL software

For Microsoft Windows server software and Microsoft SQL server software combinations supported on Control Manager, see Supported Microsoft Windows OS and Microsoft SQL combinations on page 29.

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.

IPv4 and IPv6 support

Control Manager supports both IPv4 and IPv6 within a Control Manager deployment. IPv4 is the default setup on all Windows servers in a Control Manager deployment. If a customer wants to use IPv6, they must administer their Windows servers to operate in a Dual Stack environment. That is, the customer must activate IPv6 support in addition to IPv4 on their Control Manager servers and within their network.

To use IPv6 between Control Manager servers and other Avaya products and solutions that also support IPv6, the other Avaya products and solutions must also support IPv6 and be administered to use IPv6 either exclusively or in a Dual Stack environment with both IPv4 and IPv6.

The following table lists the connections supported between Control Manager and other Avaya products and other related systems when using IPv6. Note that not all connections support IPv6. All of the listed connections are supported by default with IPv4.

Connection from Control Manager to...	IPv6 Status
Control Manager installer to database connections	Supported
Control Manager inter-process communication	Supported
HTTPS on the web client	Supported
HTTPS on the API client	Supported
SNMP	Supported
SMTP	Supported
SQL Server database connection	Supported
Legacy HA heartbeat between application servers	Supported
Active Directory authentication	Supported

Table continues…

Connection from Control Manager to...	IPv6 Status
Active Directory sync	Supported
WebLM	Not Supported
Avaya Agent for Desktop	Not Supported
Avaya Analytics™	Supported
Call Center Elite Multichannel database	Not Supported
CMS and CMS database	Supported
Communication Manager	Supported
Avaya Aura® Contact Center	Not Supported[2]
Experience Portal	Not Supported
Interaction Center, Interaction Center database (Microsoft SQL Server), and Interaction Center database (Oracle)	Not Supported
Avaya IQ	Not Supported
Avaya Aura® Messaging	Supported
Modular Messaging	Not Supported
Avaya Oceana® Solution	Supported
Avaya one-X® Agent	Not Supported
Proactive Contact	Not Supported
System Manager, Session Manager, and Presence Services	Supported
Avaya Workspaces (for Call Center Elite)	Supported
WFO	Not Supported

Supported database server software requirements

When using the Control Manager Legacy HA configuration, the customer must install one of the following regular Microsoft SQL server software editions on every database server:

- Microsoft SQL Server 2017 Enterprise Edition
- Microsoft SQL Server 2016 Enterprise Edition SP2
- Microsoft SQL Server 2014 Standard Edition SP2
- Microsoft SQL Server 2014 Enterprise Edition SP2
- Microsoft SQL Server 2012 Standard Edition SP4
- Microsoft SQL Server 2012 Enterprise Edition SP4

[2] Avaya Aura® Contact Center 7.0.3 does not support IPv6.

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 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 full administrative 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 and conditions:

- 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
  - ACCCMONEXUSER
  - ACCCMSPHERE
  - ACCCMSYNC
  - UserCMSysLog
- It is the responsibility of the customer to provide database servers that have enough computing resources to handle the required performance of the Control Manager database software in addition to the shared database software. This requirement applies to both non-HA and HA configurations. Avaya cannot make recommendations in this area since Avaya does not know what shared 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 22.
- 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 Windows OS and Microsoft 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 2016 and any of the supported Microsoft SQL Server 2017 editions
- Microsoft Windows Server OS 2016 and any of the supported Microsoft SQL Server 2016 SP2 editions
- Microsoft Windows Server OS 2016 and any of the supported Microsoft SQL Server 2014 SP2 editions
- Microsoft Windows Server OS 2012 R2 and any of the supported Microsoft SQL Server 2014 SP2 editions
- Microsoft Windows Server OS 2012 R2 and any of the supported Microsoft SQL Server 2012 SP4 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
- Google Chrome 70
- Microsoft Edge 40
- Microsoft Internet Explorer 11
- Mozilla Firefox 65.0

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 application servers in an HA configuration (ACM-APP-1 and ACM-APP-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.

Transport Layer Security (TLS) support

Control Manager supports TLS 1.2 for secure communications for database connections and connections to other Avaya products. The following table lists the TLS 1.2 connections supported for Control Manager.

Connection from Control Manager to...	TLS 1.2 Status
Control Manager installer to database connections	Supported
Control Manager inter-process communication	Some internal services use non-HTTPS channels
HTTPS on the web client	Supported
HTTPS on the API client	Supported
SQL Server database connection	Supported
Legacy HA heartbeat between application servers	Supported
Active Directory authentication	Supported
Active Directory sync	Supported
WebLM	Not Supported
Avaya Agent for Desktop	Supported
Avaya Analytics™	Supported
Call Center Elite Multichannel database	Not Supported

Table continues…

Connection from Control Manager to...	TLS 1.2 Status
CMS	Supported via SSH
CMS Informix database	Not Supported
Communication Manager	SSH strong cipher support for OSSI connections
Avaya Aura® Contact Center	Not Supported
Experience Portal	Supported
Interaction Center API	Not Supported
Interaction Center database (Microsoft SQL Server)	Supported
Interaction Center database (Oracle)	Supported
Avaya IQ	Not Supported
Avaya Aura® Messaging	Supported
Modular Messaging	Not Supported
Avaya Oceana® Solution	Supported
Avaya one-X® Agent	Supported
Presence Services	Supported
Proactive Contact	Not Supported
Session Manager	Supported
System Manager	Supported
Avaya Workspaces (for Call Center Elite)	Supported
WFO	Supported (uses Windows shared folder permissions to secure)

Virtualization support

Avaya Control Manager operates on the following virtualized software platforms:

- VMware vSphere ESXi 6.7
- VMware vSphere ESXi 6.5
- VMware vSphere ESXi 6.0
- VMware vSphere ESXi 5.x
- 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

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

- New installations.
- When upgrading (migrating) from any Release 7.x system.
- When activating new connectors for additional Avaya products.
- When the MAC addresses of the servers have changed.
- When you want a new license file to increase the web session inactivity timeout value. The default value is 15 minutes.

You do not need to get a new license when upgrading from Release 8.0.x to Release 8.1.

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.

Server	MAC IDs
ACM-APP-1	
ACM-APP-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 5: Worksheets

Server worksheet — Legacy HA configuration

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	IP address
Primary application server	ACM-APP-1		
Secondary application server	ACM-APP-2		
Primary database server	ACM-SQL-1		
Secondary database server	ACM-SQL-2		

Chapter 6: Installing prerequisite software

About software installation prerequisites

Upgrades from Control Manager Release 7.1.x

For an upgrade from Control Manager Release 7.1.x, the customer must first upgrade to Control Manager Release 8.0.4.x. After upgrading to Release 8.0.4.x, you can use the procedures in this document to upgrade to Release 8.1. See the following documents for more information about upgrading a Release 7.1.x system to Release 8.0.4.x:

- *Upgrading to Avaya Control Manager 8.0.4 for Enterprise - Non-High Availability*
- *Upgrading to Avaya Control Manager 8.0.4 for Enterprise - High Availability*
- *Upgrading to Avaya Control Manager 8.0.4 for Partner Cloud Powered by Avaya xCaaS*

Upgrades from Control Manager Release 8.0.x.x when also 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/

- Non-HA and Legacy HA Deployments — Install and configure Microsoft Internet Information Services (IIS) for the Web server component. For more information, see Installing and configuring IIS on the Microsoft Windows Server 2016 OS on page 36 or Installing and configuring IIS on the Microsoft Windows Server 2012 OS on page 40.

- Legacy HA Deployments — Install the regular Microsoft SQL Server software on both database hosts in a Legacy HA deployment. For more information, see Installing the regular Microsoft SQL Server software on page 46.
- Legacy HA Deployments — Install certificates on both application servers in a Legacy HA deployment. For more information, see Installing certificates on page 56.

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), upgrade to Microsoft Windows OS 2012 R2 software as described in Upgrading Windows 2012 to Windows 2012 R2 on page 69.
- 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 2016 OS

About this task

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

- In an Enterprise Legacy HA configuration, you must install the IIS software on both application servers (ACM-APP-1 and ACM-APP-2).

Before you begin

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

Microsoft .NET Version 4.7.2 or higher software is required for Control Manager. Microsoft .NET Version 4.7.2 is included with the ISO image of the Control Manager software. You must determine whether .NET 4.7.2 or higher is installed on the servers where you installed IIS. To determine whether .NET 4.7.2 or higher is already installed, see the following Microsoft article:

https://docs.microsoft.com/en-us/dotnet/framework/migration-guide/how-to-determine-which-versions-are-installed

Important:

You must install the Microsoft .NET patches for Microsoft .NET 4.7.2 or higher to pick up the latest security fixes.

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**.

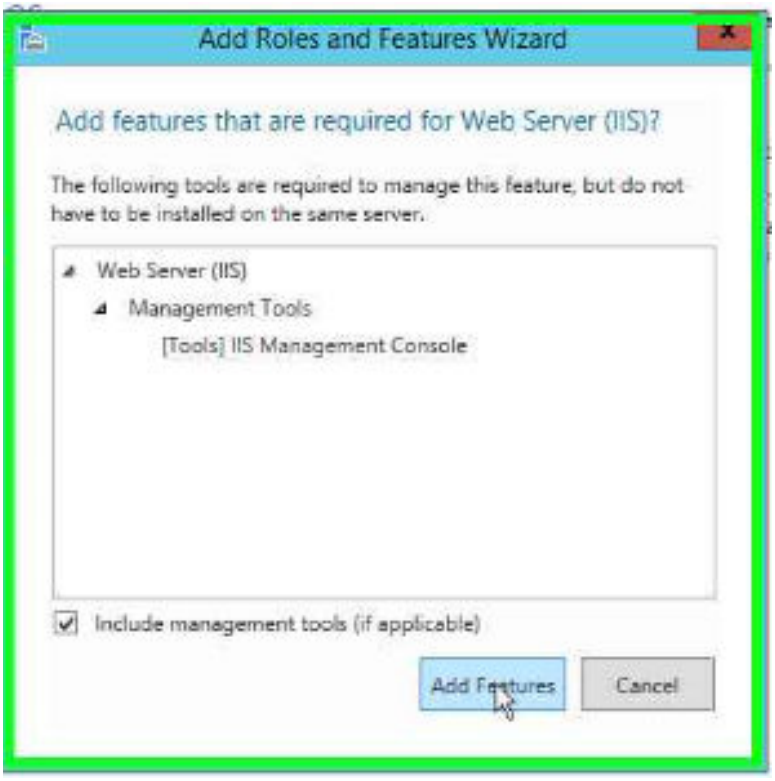
   The system displays the Select destination server screen. Confirm that the default selection is **Select a server from the server pool** and that the **Server Pool** list has the server where you are installing IIS.

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. Repeat this procedure on any other servers that require the IIS software.

Next steps

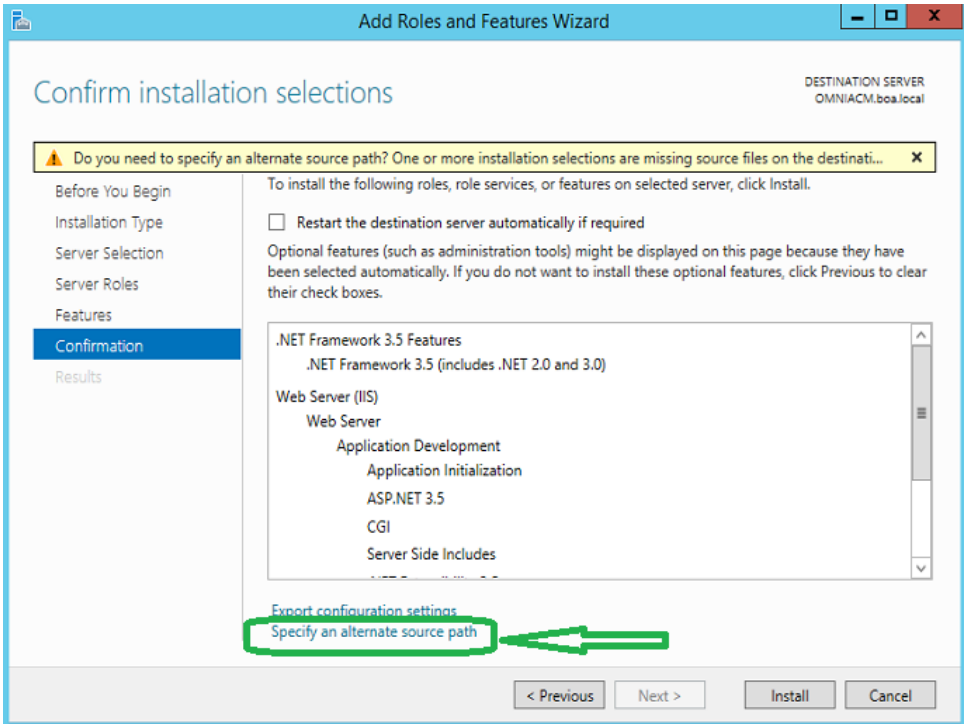
Important:

You must install the Microsoft .NET patches for Microsoft .NET 4.7.2 or higher 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:



Control Manager Release 8.1 only supports Transport Layer Security (TLS) 1.2 or newer. 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 and 1.1 per Avaya security requirements if those versions still exist on the system.

You can manually disable TLS 1.0 and 1.1 by editing the registry on every server where you installed IIS. Use the article that 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 2012 OS

About this task

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

- In an Enterprise Legacy HA configuration, you must install the IIS software on both application servers (ACM-APP-1 and ACM-APP-2).

Before you begin

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

Microsoft .NET Version 4.7.2 or higher software is required for Control Manager. Microsoft .NET Version 4.7.2 is included with the ISO image of the Control Manager software. You must determine whether .NET 4.7.2 or higher is installed on the servers where you installed IIS. To determine whether .NET 4.7.2 or higher is already installed, see the following Microsoft article:

https://docs.microsoft.com/en-us/dotnet/framework/migration-guide/how-to-determine-which-versions-are-installed

Important:

You must install the Microsoft .NET patches for Microsoft .NET 4.7.2 or higher to pick up the latest security fixes.

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**.

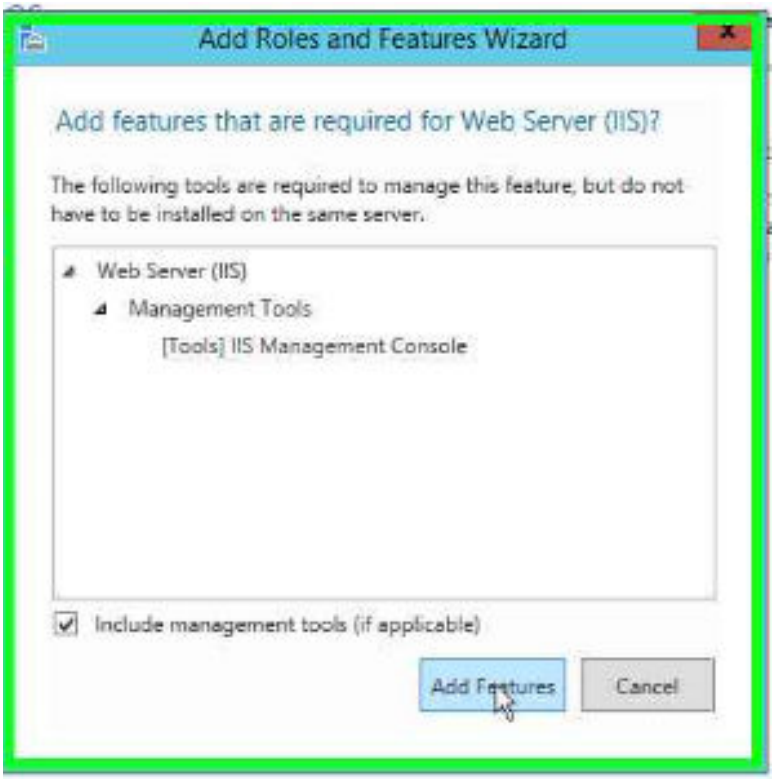
   The system displays the Select destination server screen. Confirm that the default selection is **Select a server from the server pool**.

5. Click **Next**.

   The system displays the Select server roles screen.

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

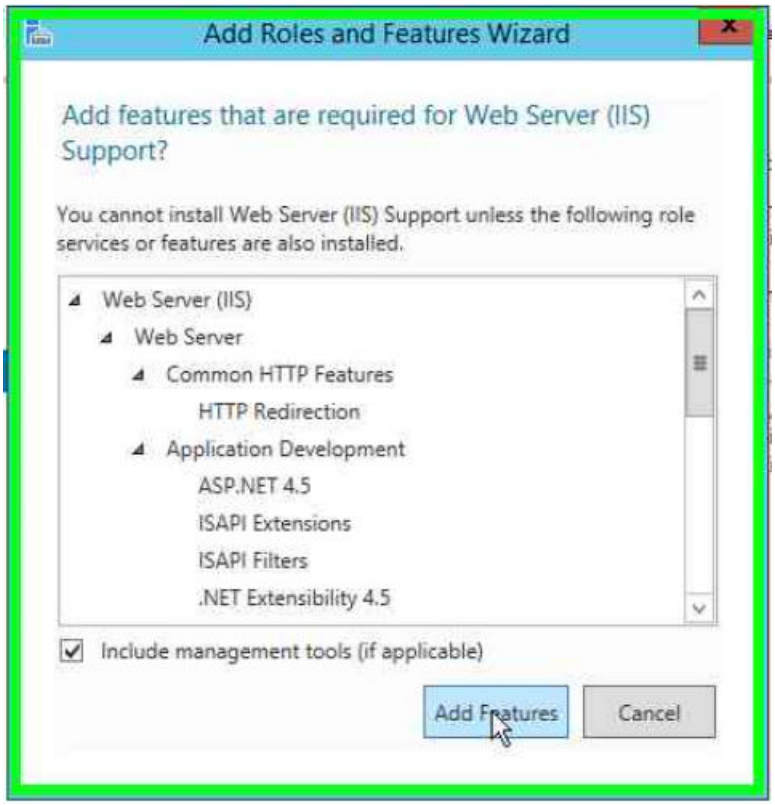
   After selecting the **Web Server IIS** option, the system displays the following screen:



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. Repeat this procedure on any other servers that require the IIS software.

Next steps

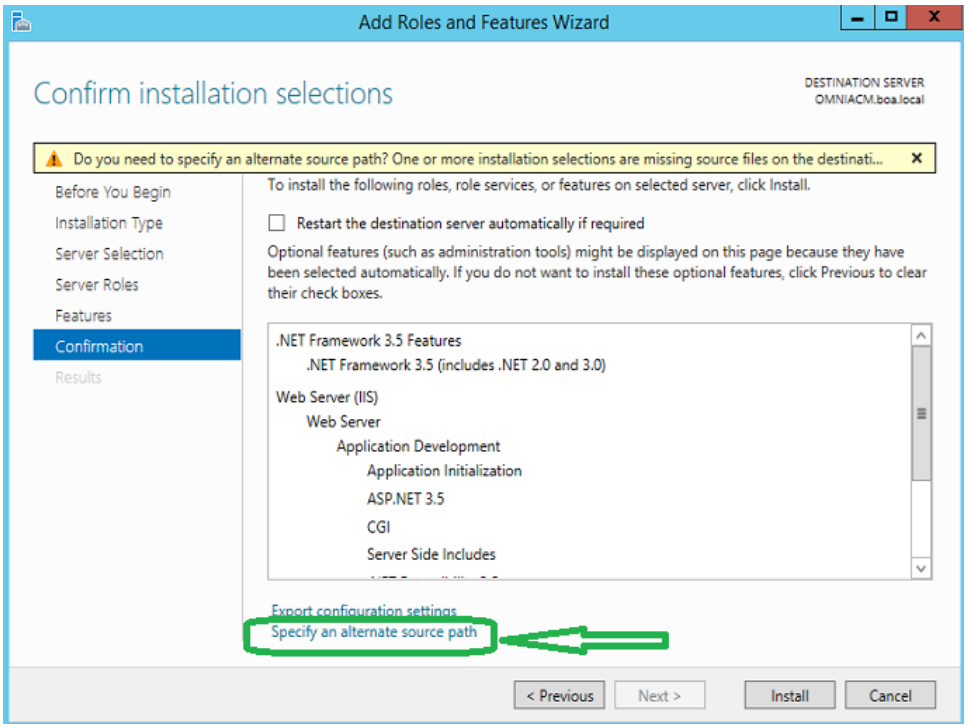
Important:

You must install the Microsoft .NET patches for Microsoft .NET 4.7.2 or higher 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:



Control Manager Release 8.1 only supports Transport Layer Security (TLS) 1.2 or newer. 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 and 1.1 per Avaya security requirements if those versions still exist on the system.

You can manually disable TLS 1.0 and 1.1 by editing the registry on every server where you installed IIS. Use the article that 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 regular Microsoft SQL Server software

The Control Manager deployment must have a local database or a remote database running supported regular 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 regular Microsoft SQL Server software on the following servers in a Control Manager deployment:

Important:

The customer cannot use the regular Microsoft SQL Server Express edition when installing a Legacy HA configuration.

In a Legacy HA configuration, the customer must install the regular Microsoft SQL Server software on both the primary and secondary database servers.

Detailed instructions for installing the regular Microsoft SQL Server 2017 software are available from Microsoft at:

https://docs.microsoft.com/en-us/sql/sql-server/install/planning-a-sql-server-installation?view=sql-server-2017

You must search the Microsoft web site for installation instructions for other versions of Microsoft SQL Server software.

Considerations when installing the regular Microsoft SQL software

Important:

The customer must agree to create a user login ID on the SQL database servers that is a full administrative 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

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.

After initial installation and configuration of the Microsoft SQL Server software, you must then install the Control Manager software before you complete the final configuration of the Microsoft SQL Server software. These final configuration procedures are found in the chapters *Configuring replication* and *Configuring Legacy HA services*.

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.

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 database servers

About this task

After you install the regular Microsoft SQL Server software, you must configure replication on the two database servers you will use for Legacy HA service. For this procedure, designate one database server as your primary database server (ACM-SQL-1) and the other server as your secondary database server (ACM-SQL-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:

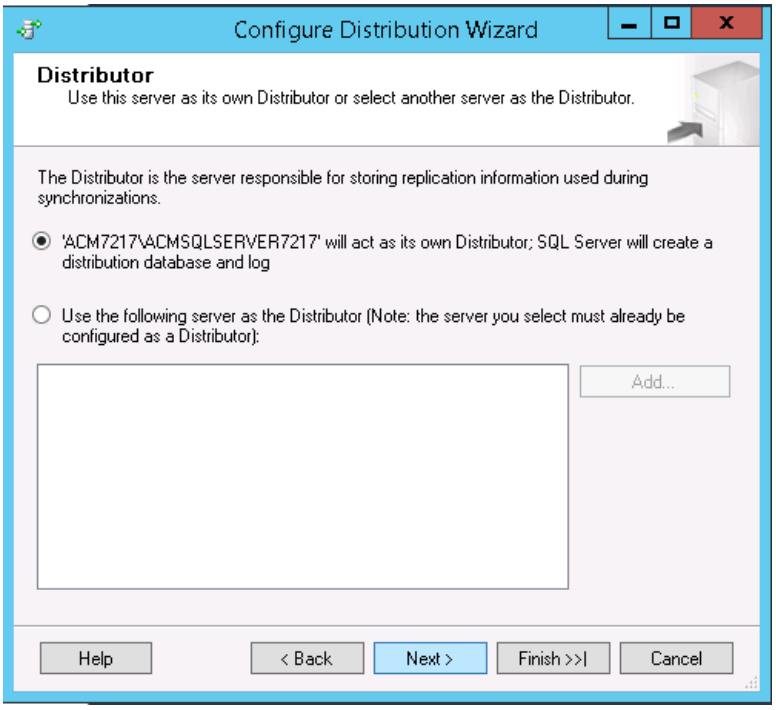
If you see the **Configure Distribution** option in the menu items, it means that replication has not been configured on the server. If **Configure Distribution** is not displayed, replication has been configured and you can skip this procedure.

5. Select **Configure Distribution**.

   The system displays the Configure Distribution Wizard welcome screen.

6. Click **Next**.

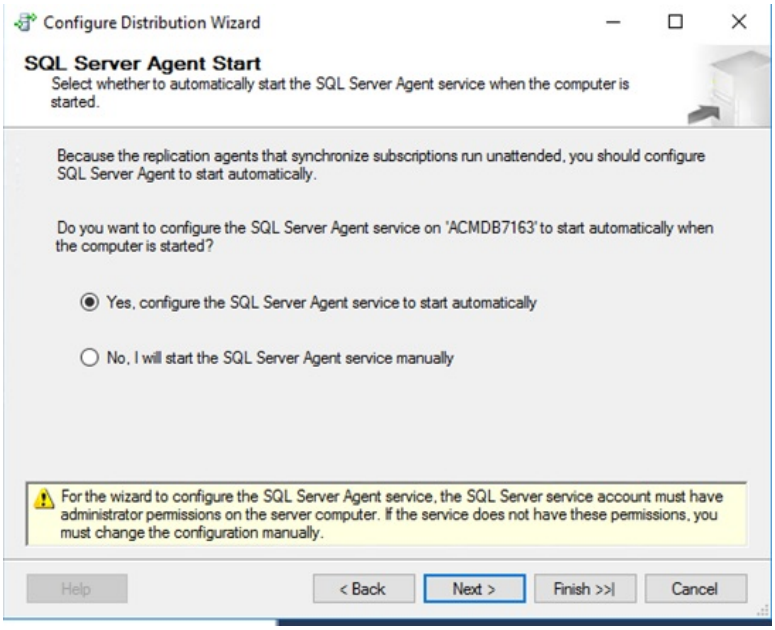
   The system displays the Distributor screen.



7. Select the first option, **"*DatabaseID*" will act as its own Distributor**. The variable *DatabaseID* represents the actual name of the database server.

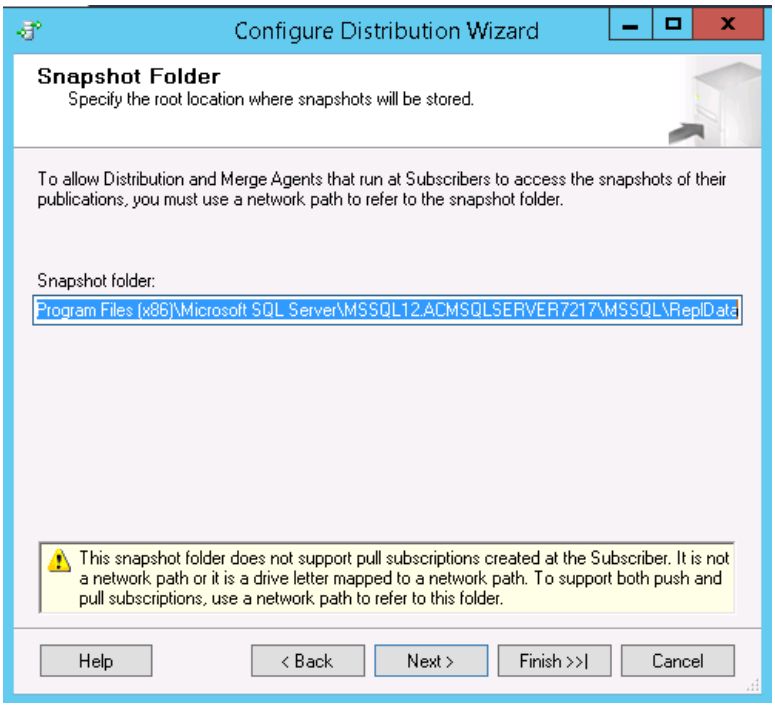
8. Click **Next**.

   The system displays the SQL Server Agent Start screen.



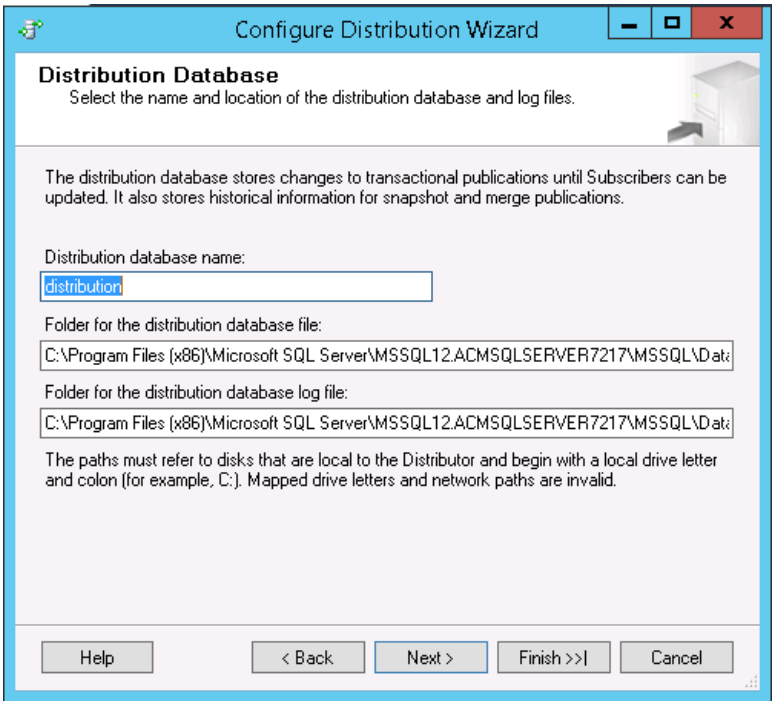
9. Click **Next**.

   The system displays the Snapshot Folder screen. Note the path to the snapshot folder. You must use it later in this procedure.



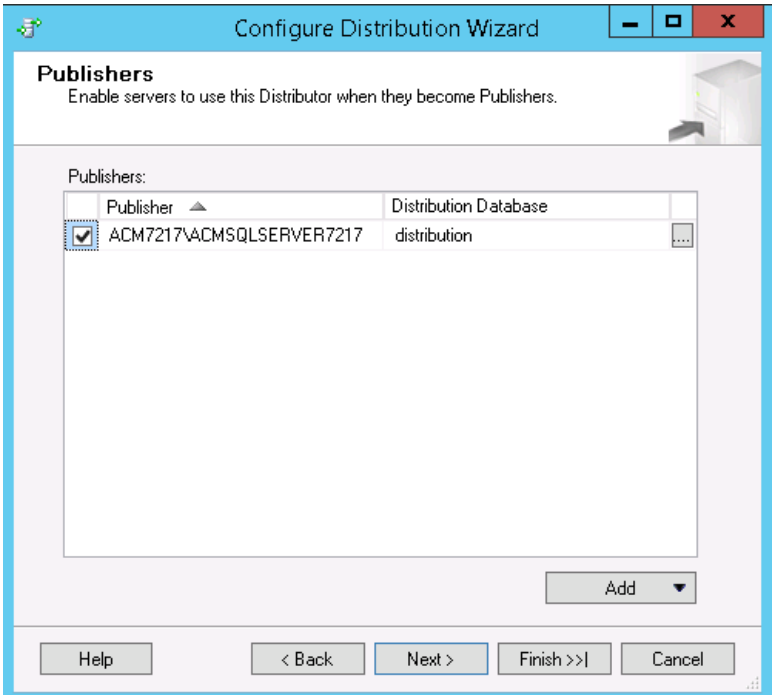
10. Click **Next**.

    The system displays the Distribution Database screen:



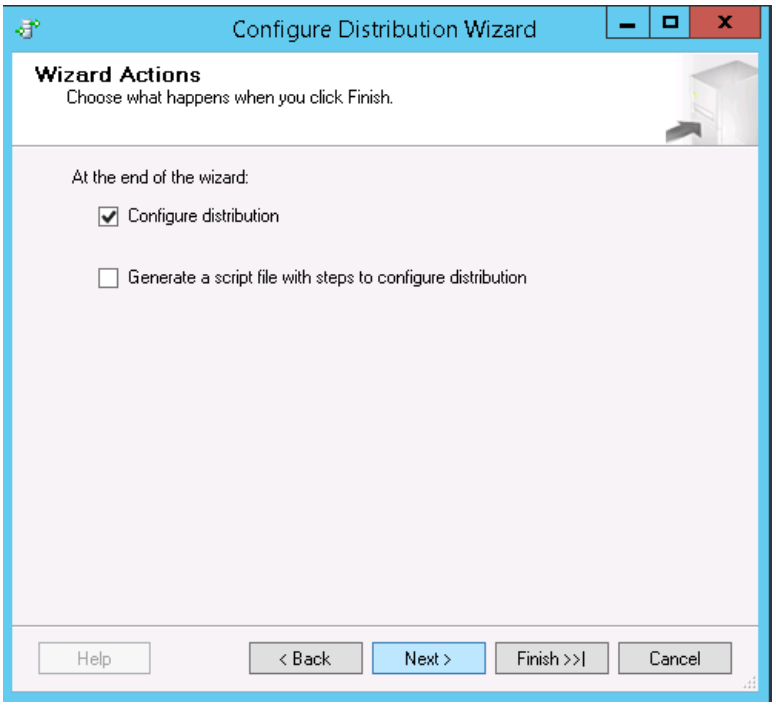
11. Enter the **Distribution database name** and the folders where the data and the log file will reside.
12. Click **Next**.

    The system displays the Publishers screen.



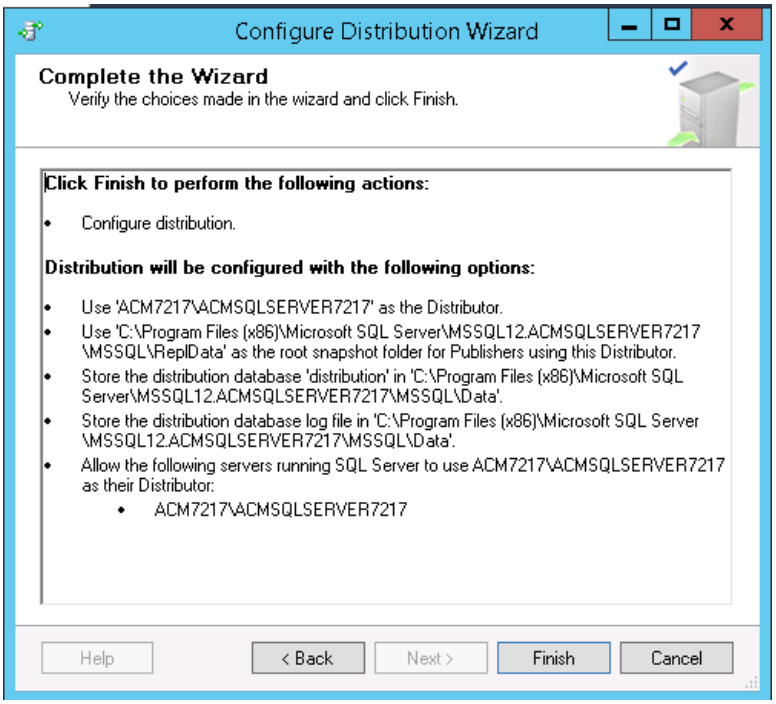
13. Click **Next**.

    The system displays the Wizard Actions screen.



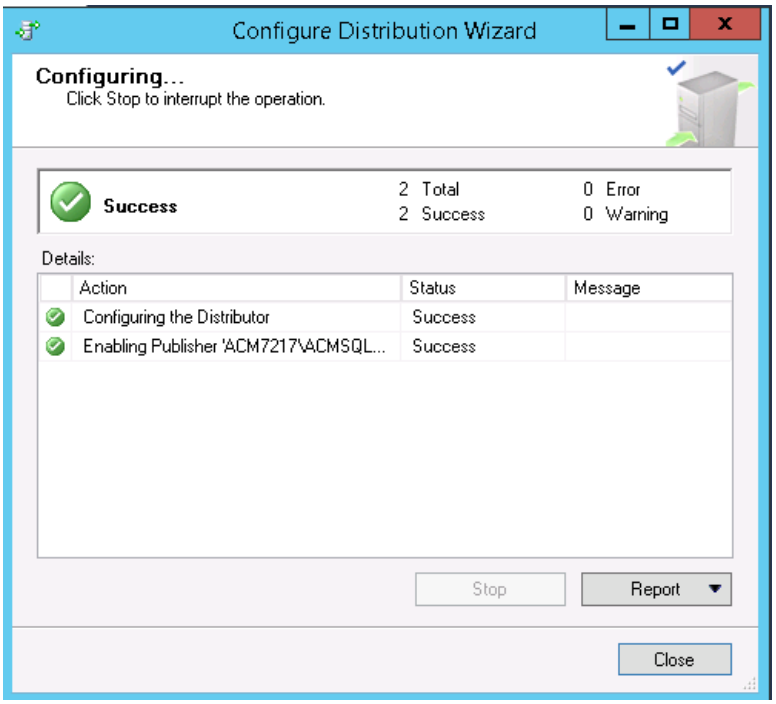
14. Click **Next**.

    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`
    - Microsoft SQL Server 2017 — `C:\Program Files (x86)\Microsoft SQL Server\MSSQL14.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`
- Microsoft SQL Server 2017 — `C:\Program Files\Microsoft SQL Server\MSSQL14.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`
- Microsoft SQL Server 2017 — `C:\Program Files (x86)\Microsoft SQL Server\MSSQL14.[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`
- Microsoft SQL Server 2017 — `C:\Program Files\Microsoft SQL Server\MSSQL14.[Instance Name]\MSSQL\ReplData`

18. Right-click on the folder and select **Properties**.

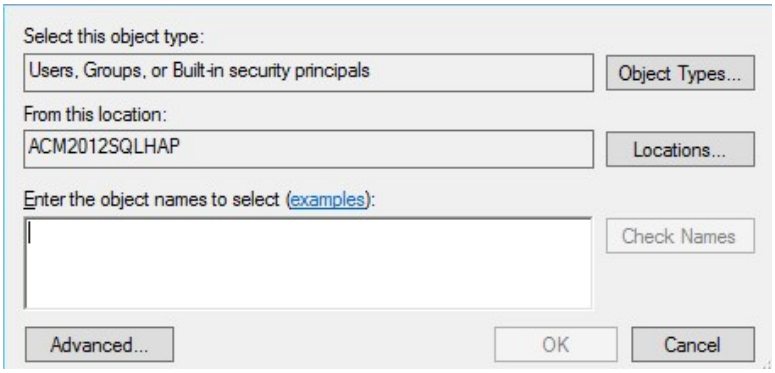
    The system displays the ***FolderName*** Properties screen.

19. Select the **Security** tab.
20. Click **Edit**.

    The system displays the Permissions for ***FolderName*** **Properties** screen.

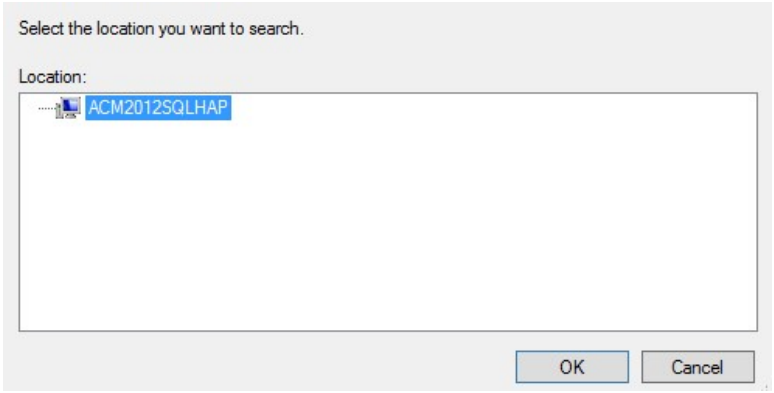
21. Click **Add**.

    The system displays the Select Users, Computers, Service Accounts, or Groups screen.



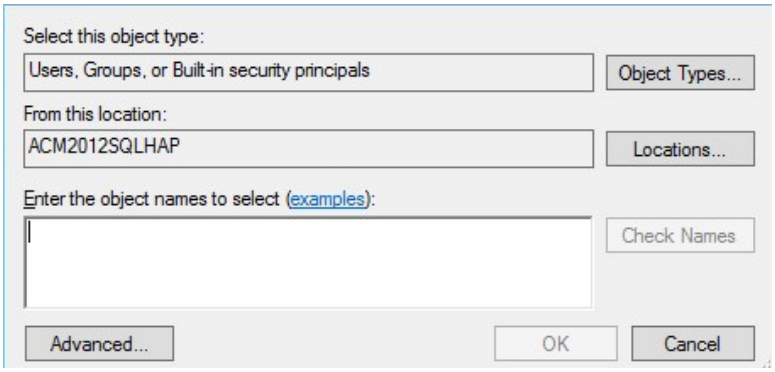
22. Click **Locations**.

    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. Repeat steps 18–29 depending on which version of Microsoft SQL software you are using. Select one of the following folders when you repeat Steps 18–29:

    For Microsoft SQL Server (x86) edition when using an instance name:

    - Microsoft SQL Server 2012 — `C:\Program Files (x86)\Microsoft SQL Server\110`
    - Microsoft SQL Server 2014 — `C:\Program Files (x86)\Microsoft SQL Server\120`
    - Microsoft SQL Server 2016 — `C:\Program Files (x86)\Microsoft SQL Server\130`
    - Microsoft SQL Server 2017 — `C:\Program Files (x86)\Microsoft SQL Server\140`

    For Microsoft SQL Server (x64) edition when using an instance name:

    - Microsoft SQL Server 2012 — `C:\Program Files\Microsoft SQL Server\110`
    - Microsoft SQL Server 2014 — `C:\Program Files\Microsoft SQL Server\120`
    - Microsoft SQL Server 2016 — `C:\Program Files\Microsoft SQL Server\130`
    - Microsoft SQL Server 2017 — `C:\Program Files\Microsoft SQL Server\140`

31. Log on to the secondary SQL database server (ACM-SQL-2).

32. Repeat Steps 17-30 on the secondary SQL database server (ACM-SQL-2).

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.

The customer must install certificates on both Control Manager application servers in an HA configuration (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 57
Submitting the CSR to a CA for signing on page 60
Installing the signed certificate on page 62
Binding the certificate to SSL port 9011 on page 64
Installing the root certificate on page 65
Enabling SSL for secure browser access on page 66

Generating a Certificate Signing Request in IIS

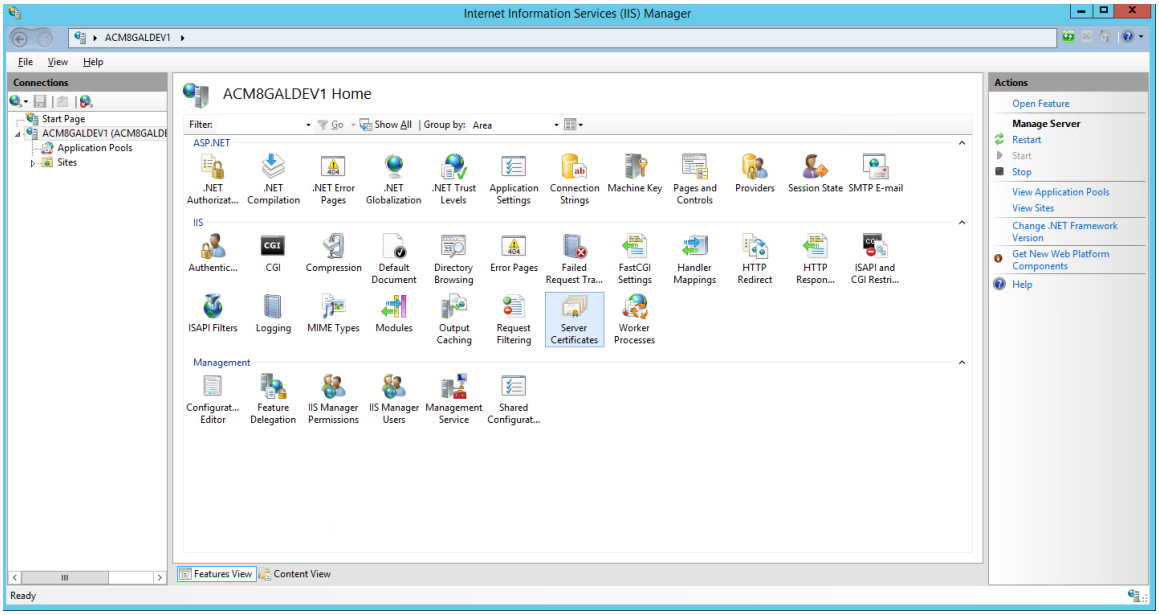
Before you begin

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

Procedure

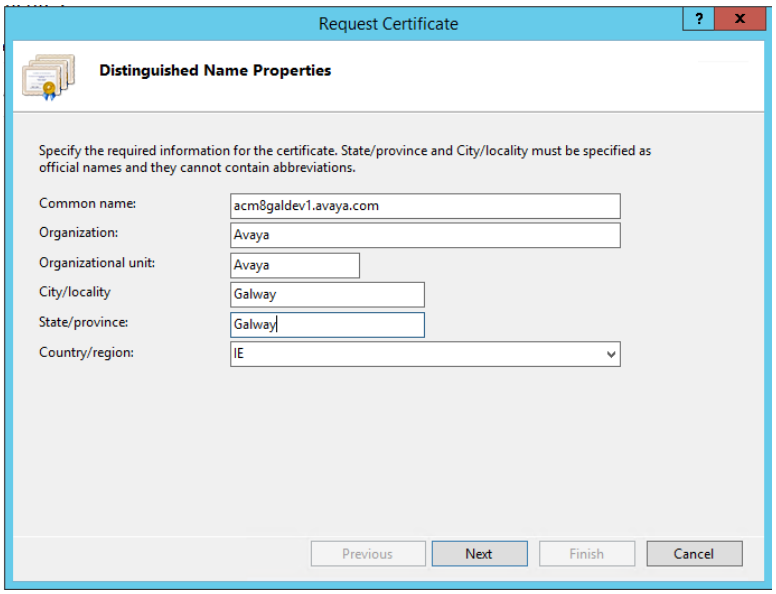
1. Open the Microsoft IIS Manager tool.
2. Click on the Control Manager server shown in the **Connections** tree.

   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.



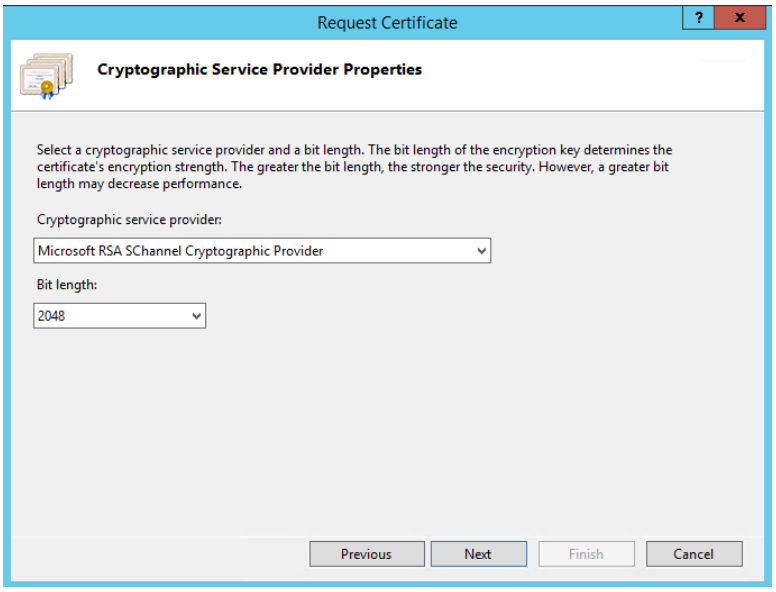
5. Administer the requested parameters. Enter the server name or FQDN of the Control Manager server in the **Common name** field.

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.

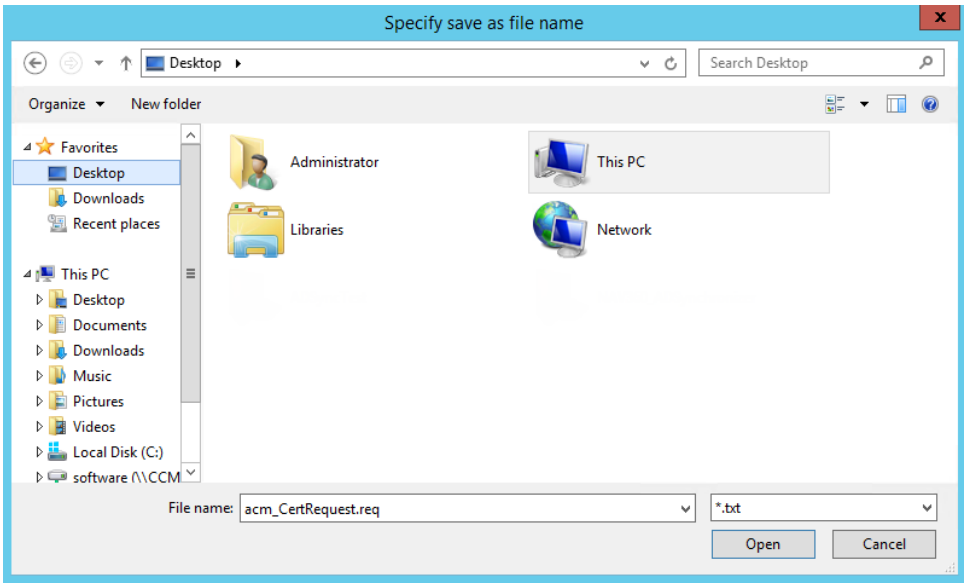
6. Click **Next**.

   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.

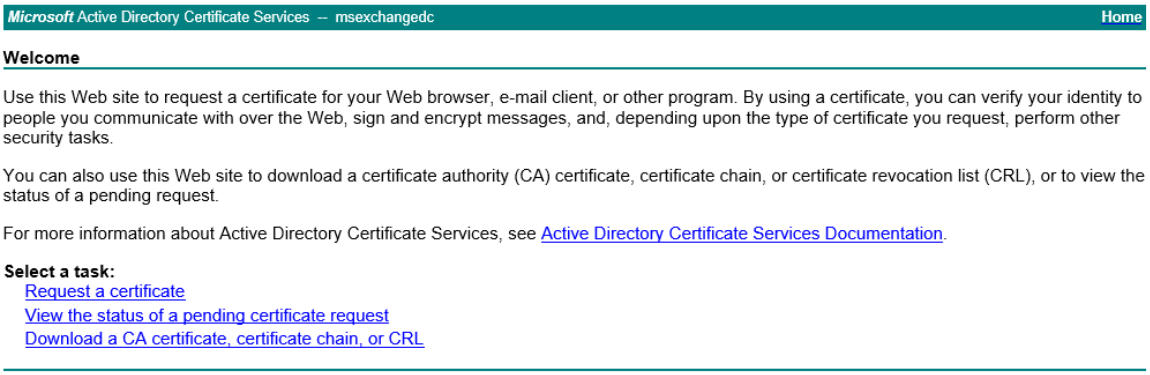
Before you begin

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:

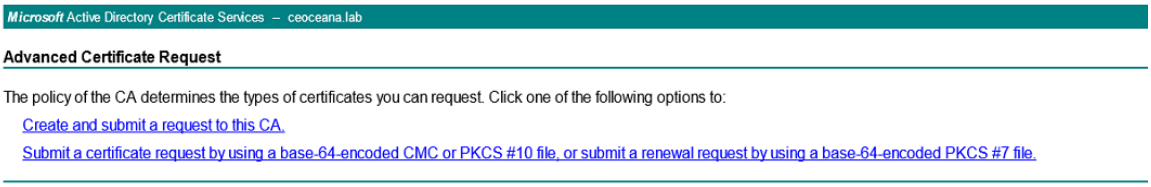


2. Click **Request a certificate**, or other similar option.

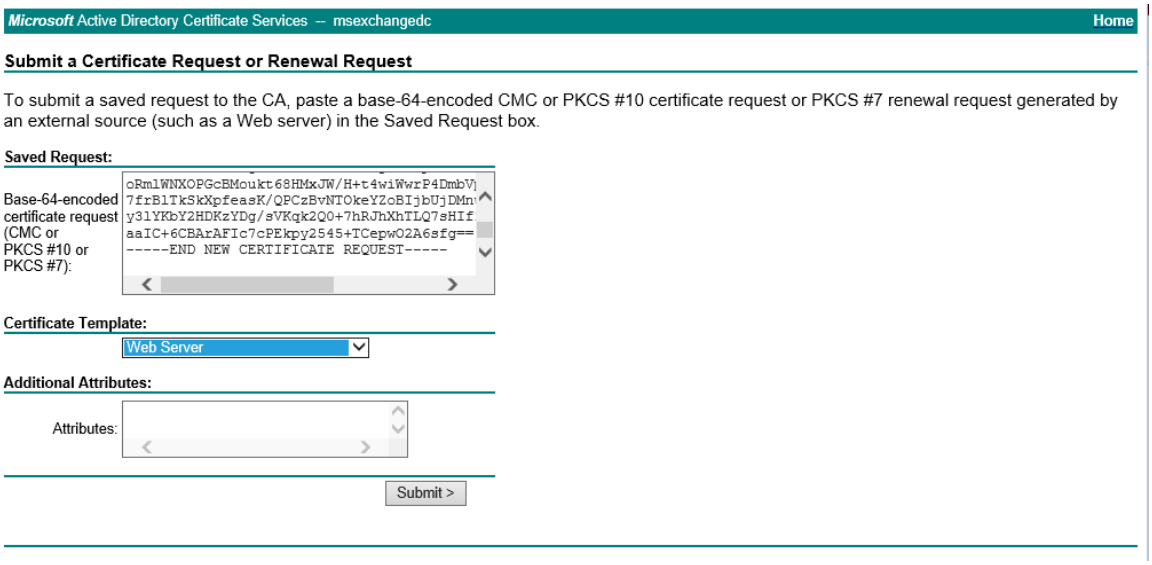
   The system displays a page similar to the following:

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:

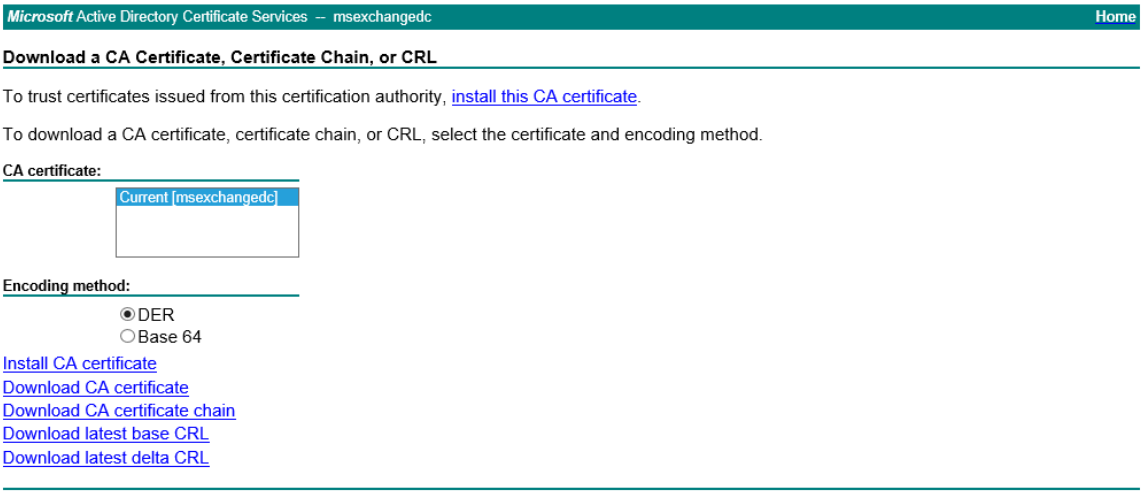


7. Select **Web Server** under the **Certificate Template** option, or similar option.
8. Click **Submit**.

   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:



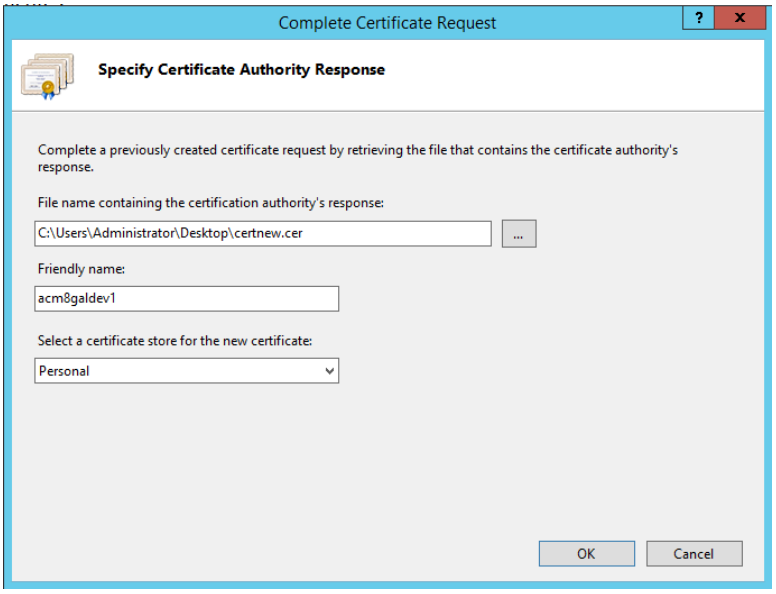
11. Click **Download CA Certificate**.
12. Copy the signed certificate and the root certificate to the Control Manager server.
13. Repeat this procedure for every Control Manager server that is required to have certificates.

Installing the signed certificate

Procedure

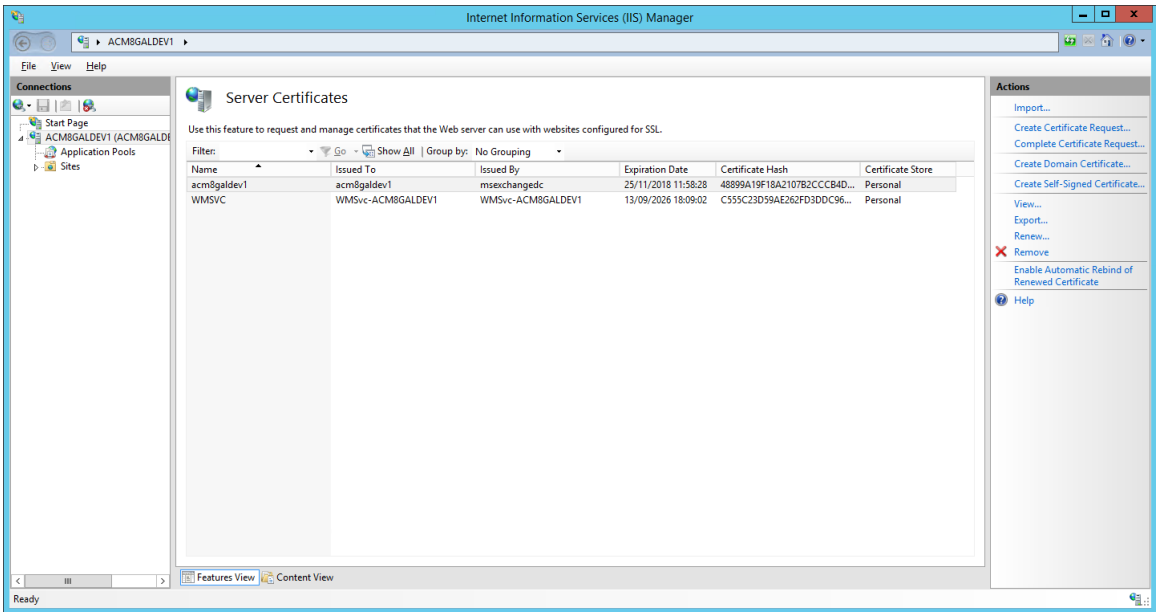
1. Return to the Microsoft IIS Manager tool.
2. On the Server Certificates page, click **Complete Certificate Request**.

   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

About this task

Perform this procedure for either Multiplex HA deployments or Legacy HA deployments. This procedure is not needed for a non-HA deployment. You must perform this procedure on the primary and secondary application servers of a Multiplex HA or Legacy HA 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 primary application server (ACM-APP-1).
2. Run the following command in Windows Power Shell. The command must be entered on a single line.

   `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 in a certificate, do the following steps:
     a. On the server desktop, click **Tools** > **Internet Information Services Manager**.
     b. Navigate to **Server** > **Server Certificates**.
     c. Right-click the active SSL certificate and select **View**.
     d. On the Certificate screen, click the **Details** tab.
     e. Copy the thumbprint value from the display area, remove all spaces, and enter it as the `certhash` value.
     f. Close the Certificate screen.
   - *`<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
   ```

3. Repeat this procedure on the secondary application server (ACM-APP-2). 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.

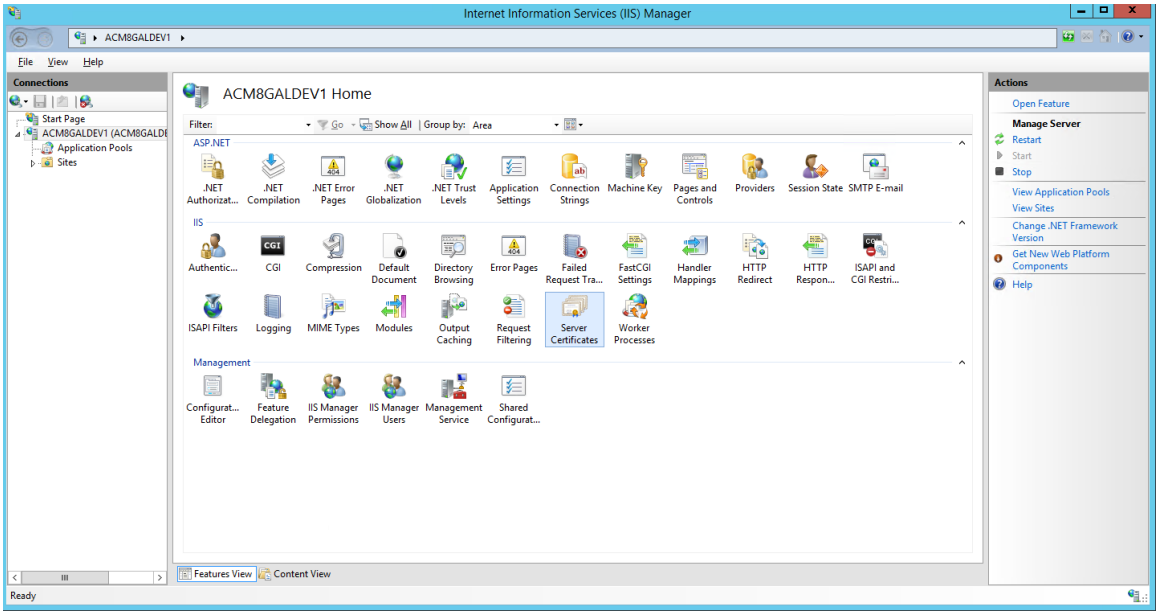
20. Click **Browse** to locate the root certificate you requested from the CA.
21. Click **Next**.
22. Select **Place all certificates in the following store**.
23. Click **Browse** and select **Trusted Root Certification Authorities**.
24. Click **Next**.
25. Click **Finish**.

Enabling SSL for secure browser access

Procedure

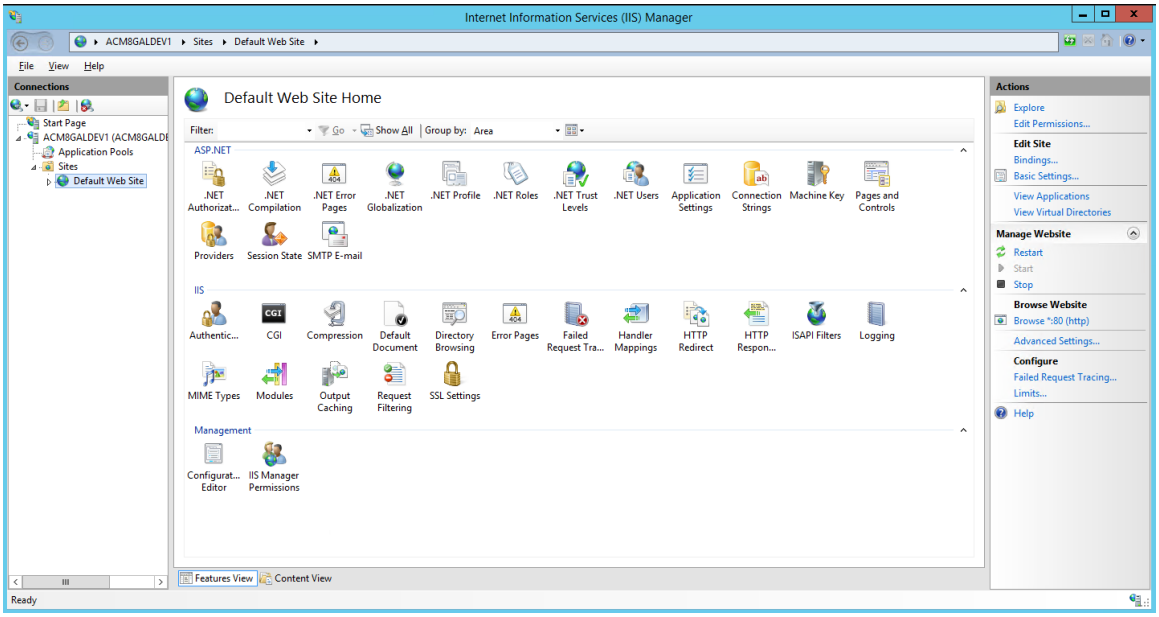
1. Log on to Windows as administrator on the primary application server (ACM-APP-1).
2. Open the Microsoft IIS Manager tool.
3. Click on the Control Manager primary application server (ACM-APP-1) server as shown in the **Connections** tree.

   The system displays a screen similar to the following example:



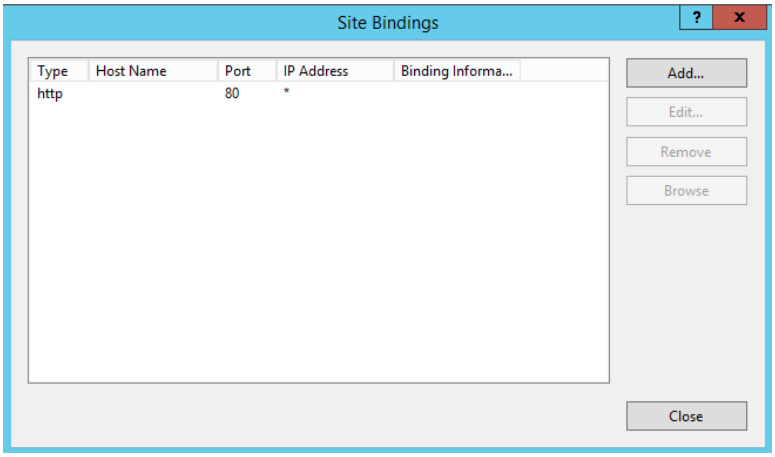
4. Expand the **Sites** folder and select **Default Web Site**.

   See the following example:



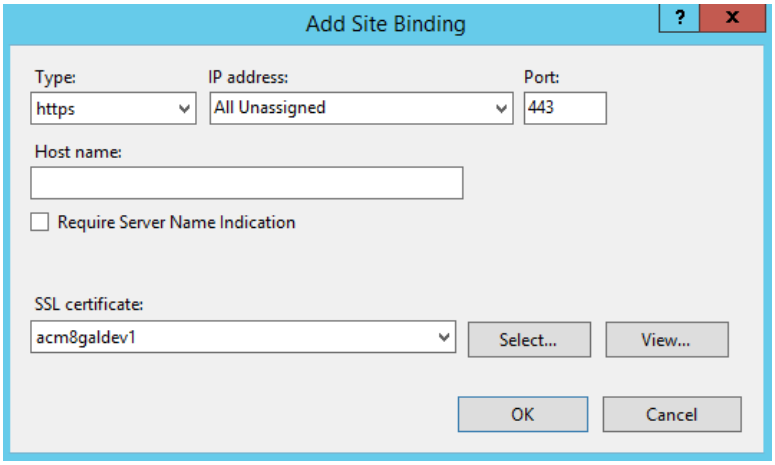
5. Select **Bindings** from the **Actions** menu on the right side of the screen.

   The system displays the Site Bindings screen.



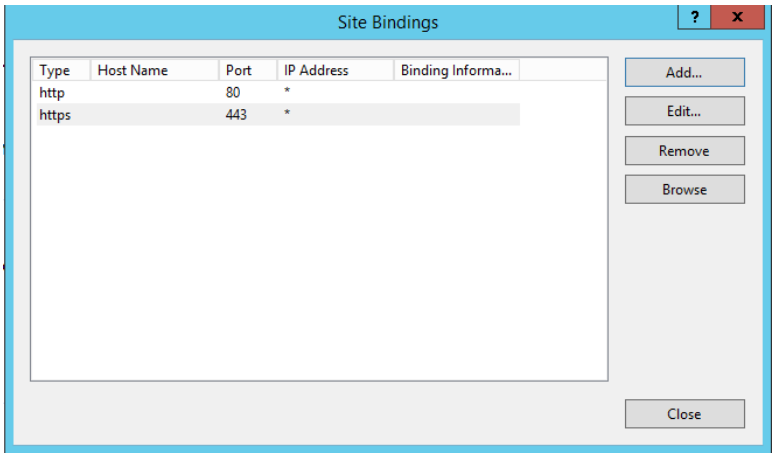
6. Click **Add**.

   The system displays the Add Site Binding screen:



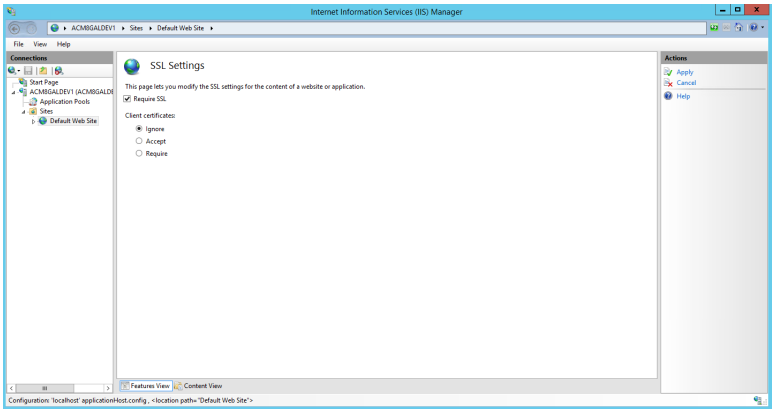
7. Administer the following parameters:
   - Set **Type** to **https**.
   - Set **IP address** to **All Unassigned**.
   - Set **Port** to **443**.
   - Leave **Host name** blank.
   - In the **SSL certificate** field, click **Select** to browse to the signed certificate you requested from the CA.
8. Click **OK**.

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



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

    The system displays the SSL Settings screen:



11. Select the **Require SSL** option.
12. Select **Apply** from the **Actions** menu on the right side of the screen.
13. 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

The upgrade process using a database migration is as follows:

- The customer uses the VMware tools to take a snapshot of the old system before starting the upgrade process. Take the snapshot while the system is in shutdown mode, not in running mode. Refer to VMware documentation for procedures to take a snapshot of the system.
- Avaya personnel back up the Control Manager databases on the old Windows SQL Server system.
- The customer installs the required hardware and deploys the required number of servers or virtual machines for the new system. When upgrading from a non-HA All-in-One server deployment, you cannot reuse that server. When upgrading from a non-HA Dual server deployment, you can reuse the application host and the database host in the new deployment. See *Hardware and VMware 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 and configures the Microsoft Windows 2016 or 2012 R2 OS software if the customer is using the regular Microsoft SQL Server software. For more information, see Supported server operating system software requirements on page 24.
- The customer installs and configures the Microsoft SQL 2017, 2016, 2014, or 2012 software if the customer is using the regular Microsoft SQL Server software. For more information, see Supported database server software requirements on page 26 and Supported Microsoft Windows OS and SQL combinations on page 29.
- Avaya personnel restore (migrate) the data from the old system to the new Windows SQL Server installation.

- The customer downloads the Control Manager software. Avaya personnel can download the software if the customer gives Avaya access to the customer's systems.
- 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 configure data replication, HA services, and failover schemes for single data center and dual data center deployments. For more information, see the chapters *Configuring replication* and *Configuring Legacy HA services*.
- Avaya personnel test the installed software to confirm proper operation. For more information, see the chapter *Testing the installation*.

Upgrade checklist

Task	✔
Plan the Control Manager deployment with the customer. ⚠ **Caution:** Upgrades are service affecting. Do upgrades during no or low traffic periods, or during a regular maintenance period. Warn the customer that until the upgrade is completely finished and the system has been validated for operation, no customer administrators should attempt to log on to the system.	
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 2016 or 2012 R2 Server OS software • Microsoft SQL Server 2017, 2016, 2014, or 2012 software	

Table continues…

<table>
<tr><th>Task</th><th>✔</th></tr>
<tr><td>
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.
<table>
<tr><th>Application Server</th><th>MAC IDs</th></tr>
<tr><td>ACM-APP-1</td><td></td></tr>
<tr><td>ACM-APP-2</td><td></td></tr>
</table>
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).
</td><td></td></tr>
<tr><td>
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.
• The Avaya Modular Messaging connector in an HA deployment as described in Configuring Avaya Control Manager.
• Avaya one-X® Agent settings such as AUX or Work codes.
• Save a backup of the Avaya one-X® Agent portal <code>web.config</code> file and use it on the upgraded system.
</td><td></td></tr>
<tr><td>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.</td><td></td></tr>
<tr><td>Ensure that the end user and enterprise environments can support Control Manager.</td><td></td></tr>
</table>

Table continues…

Task	✔
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.	
Test the upgrade and troubleshoot any upgrade 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 or upgrade the Control Manager software. Reenable the virus software after you complete the installation or upgrade.
- Temporarily disable JRE automatic updates on the Control Manager servers. Reenable JRE automatic updates after you complete the installation or upgrade.
- Avaya recommends that you install the Control Manager software on a non-system drive. That is, not the same drive where the Windows operating system 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.

Caution:

Upgrades are service affecting. Do upgrades during no or low traffic periods, or during a regular maintenance period. Warn the customer that until the upgrade is completely finished and the system has been validated for operation, no customer administrators should attempt to log on to the system.

Important:

The customer must agree to create a user login ID on the SQL database servers that is a full administrative 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
ACCCMONEXDB	Stores the Avaya one-X® Agent users and profile details.	ACM-SQL-1, ACM-SQL-2
ACCCMSYNC	Synchronizes the database between Communication Manager and Control Manager.	ACM-SQL-1, ACM-SQL-2

Table continues…

Database	Description	Located on server
ACCCMCMSYSLOG	Stores the Communication Manager Syslog entries. Configuration of Syslog is documented in *Configuring Avaya Control Manager*.	ACM-SQL-1, ACM-SQL-2

Each Control Manager instance is working with the primary Control Manager database layer. The primary database server (ACM-SQL-1) is replicated using a replication mechanism with the secondary database server (ACM-SQL-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 Portal application management database	You must back up this database only if the Control Manager Voice Portal/Experience Portal module is licensed and enabled.
ACCCMONEXDB	Control Manager centralized Avaya one-X® Agent administration database	You must back up this database only if the Control Manager Avaya one-X® Agent Centralized Administration Management module is licensed and enabled.
ACCCMSYNC	Synchronizes the database between Communication Manager and Control Manager.	You must back up this database.
ACCCMCMSYSLOG	Stores the Communication Manager syslog entries.	You must back up this database.

Backing up Control Manager databases

About this task

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

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

- 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.

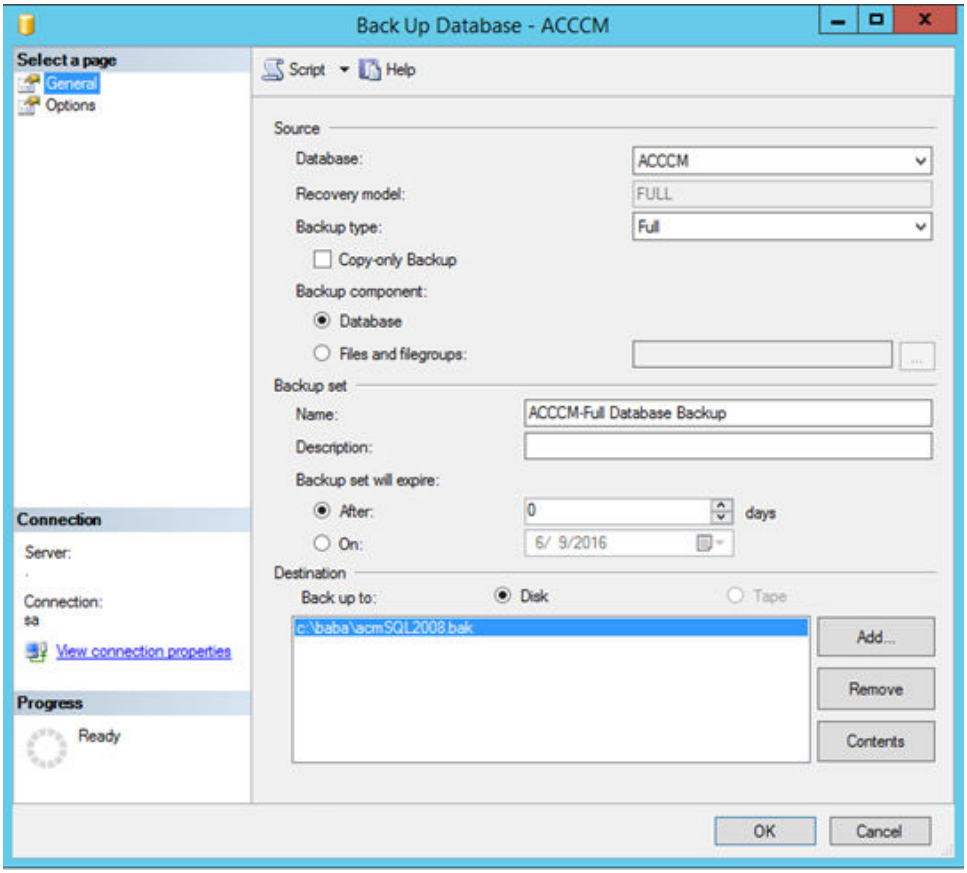
Procedure

1. On the SQL server used for Control Manager, open the SQL Management Studio application.
2. On the Connect to Server window, provide the following information and log on to the system as administrator:
   - Server type
   - Server name
   - Authentication
   - User name
   - Password
3. In the Object Explorer pane, expand the Databases navigation tree and select the ACCCM database.

   Important:

   When selecting the databases for backup, keep track of any custom named databases in the table shown above. For releases 8.0.x.x and newer, you will should not have custom database names.
4. Right-click the database and select **Tasks** > **Back Up**.

   The system displays the following screen:



5. In the Back Up Database screen, perform the following steps:
   a. In the Select a page pane, select **General**.
   b. In the right pane, from the **Backup type** drop-down list, select **Full**.
   c. In the Destination section, select the directory where you want to store the backup file. Ensure that the filetype is set to `.bak`.
   d. Click **OK** to begin the database backup process.

      The system starts the backup of the database.
6. Repeat these steps to back up all of the databases.

Important:

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

Restoring (migrating) the Control Manager databases

About this task

You must restore data for the following scenarios:

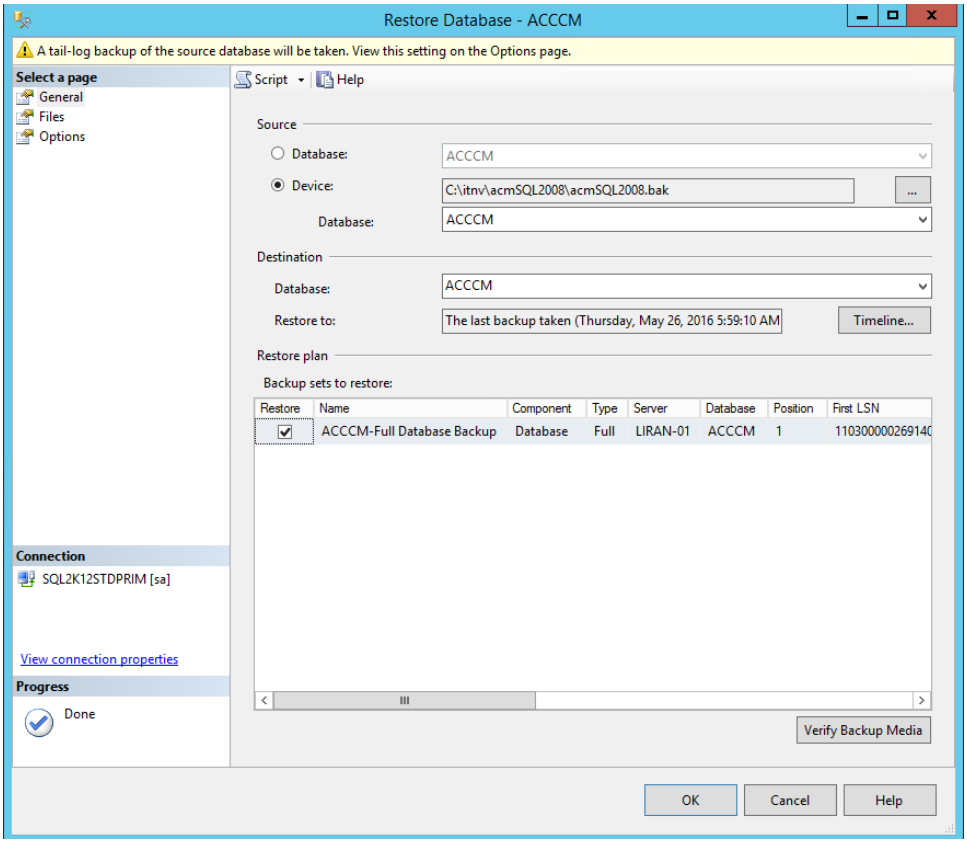
- After you install or upgrade the Control Manager software on the secondary application server (ACM-APP-2), you must restore (migrate) the backed up databases onto the database server on which you backed up the databases.
- After the new database server is installed, you must restore (migrate) the database data from the old database server onto the new database server.

Procedure

1. On the new database server, 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:



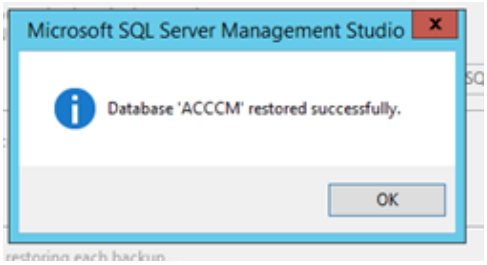
5. Select the database to restore (migrate) in the **Backup sets to restore** section, for example, **ACCCM**.

   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. 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 on the primary application server (ACM-APP-1) in a Legacy HA configuration. During the installation, you will administer links to the primary and secondary database servers (ACM-SQL-1 and ACM-SQL-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.

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

Verify that the Microsoft .NET 4.7.2 or higher software has been installed before you attempt to install the Control Manager software. Microsoft .NET Version 4.7.2 is included with the ISO image of 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:\acccminstaller*VersionNumber*.*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 **Enterprise**.
6. Click **Next**.

   The system displays the **Installation Type** screen.
7. Select the following parameters:
   - **Installation Type** — Select **New Installation**.
   - Select **High Availability**.

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 application server (ACM-APP-1), configure the following parameters:
   - **Server Role** — Select **Primary Server**.
   - **HA Mode** — Select **Standard**.
   - **Distribution Type** — Select **All**.
   - **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 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 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 primary SQL database server (ACM-SQL-1), 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, IP 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.

      IP 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.

      IP 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**.
13. For the secondary SQL database server (ACM-SQL-2), 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, IP 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.

  IP 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.

  IP 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* and *Installing Control Manager licenses*.
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.

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

About this task

Use this procedure to install the Control Manager software on the secondary application server (ACM-APP-2) in a Legacy HA configuration. During the installation, you will administer links to the primary and secondary database servers (ACM-SQL-1 and ACM-SQL-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.

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

Verify that the Microsoft .NET 4.7.2 or higher software has been installed before you attempt to install the Control Manager software. Microsoft .NET Version 4.7.2 is included with the ISO image of 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 **Enterprise**.
6. Click **Next**.

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

7. Select the following parameters:
   - **Installation Type** — Select **New Installation**.
   - Select **High Availability**.

   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 application server (ACM-APP-2), configure the following parameters:
   - **Server Role** — Select **Secondary Server**.
   - **HA Mode** — Select **Standard**.
   - **Distribution Type** — Select **All**.
   - **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 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 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 secondary SQL database server (ACM-SQL-2), 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, IP 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.

      IP 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.

      IP 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 primary SQL database server (ACM-SQL-1), 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, IP 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.

  IP 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.

  IP 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. 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* and *Installing Control Manager licenses*.

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

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

- New installations.
- When upgrading (migrating) from any Release 7.x system.
- When activating new connectors for additional Avaya products.
- When the MAC addresses of the servers have changed.
- When you want a new license file to increase the web session inactivity timeout value. The default value is 15 minutes.

You do not need to get a new license when upgrading from Release 8.0.x to Release 8.1.

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.

Before you begin

Get your license file(s) as described in Getting Control Manager licenses on page 32.

Procedure

1. Log on to one of the server(s) that for which you received a license file.
2. Copy the license file to the following location on the server:

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

Important:

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

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

   Note:

   The license server must start before any other services are started.
7. In the Services window, confirm that the **ACCCM License Server** service has started.
8. If the **ACCCM License Server** has not started, right-click **ACCCM License Server** and select **Start**.

   The system starts the service.
9. 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`
10. 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.

Next steps

Continue with Testing the restore (migration) on page 94.

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. For more information, see the chapter *Testing the Control Manager installation*.

3. Verify that you can use the SYNC application to perform a manual sync. For more information, see *Configuring Avaya Control Manager*.

Next steps

For deployments using Legacy HA, continue with the chapters *Configuring replication* and *Configuring Legacy HA services*.

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. Take the snapshot while the system is in shutdown mode, not in running mode. Refer to VMware documentation for procedures to take a snapshot of the system.
- The customer backs up the Control Manager databases.
- The customer downloads the Control Manager software. Avaya personnel can download the software if the customer gives Avaya access to the customer's systems.
- Avaya personnel upgrade the primary application server (ACM-APP-1).
- Avaya personnel upgrade the secondary application server (ACM-APP-2).
- Avaya personnel enable data replication, HA services, and failover schemes.
- Avaya personnel test the upgraded software to confirm proper operation.

Upgrade checklist

<table>
<tr><th>Task</th><th>✔</th></tr>
<tr><td>Plan the Control Manager upgrade with the customer.
Caution:
Upgrades are service affecting. Do upgrades during no or low traffic periods, or during a regular maintenance period. Warn the customer that until the upgrade is completely finished and the system has been validated for operation, no customer administrators should attempt to log on to the system.</td><td></td></tr>
<tr><td>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.</td><td></td></tr>
<tr><td>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.
<table>
<tr><th>Application Server</th><th>MAC IDs</th></tr>
<tr><td>ACM-APP-1</td><td></td></tr>
<tr><td>ACM-APP-2</td><td></td></tr>
</table>
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).</td><td></td></tr>
</table>

Table continues…

Task	✔
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*. • Avaya one-X® Agent settings such as AUX or Work codes. • Save a backup of the Avaya one-X® Agent management portal (one-X Web) and Avaya one-X® Agent configuration portal (one-X CFG) configuration files and use it on the upgraded system.	
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.	
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 69.	
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.	
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 or upgrade the Control Manager software. Reenable the virus software after you complete the installation or upgrade.
- Temporarily disable JRE automatic updates on the Control Manager servers. Reenable JRE automatic updates after you complete the installation or upgrade.
- Avaya recommends that you install the Control Manager software on a non-system drive. That is, not the same drive where the Windows operating system 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.

Caution:

Upgrades are service affecting. Do upgrades during no or low traffic periods, or during a regular maintenance period. Warn the customer that until the upgrade is completely finished and the system has been validated for operation, no customer administrators should attempt to log on to the system.

Important:

The customer must agree to create a user login ID on the SQL database servers that is a full administrative 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
ACCCMONEXDB	Stores the Avaya one-X® Agent users and profile details.	ACM-SQL-1, ACM-SQL-2
ACCCMSYNC	Synchronizes the database between Communication Manager and Control Manager.	ACM-SQL-1, ACM-SQL-2
ACCCMCMSYSLOG	Stores the Communication Manager Syslog entries. Configuration of Syslog is documented in *Configuring Avaya Control Manager*.	ACM-SQL-1, ACM-SQL-2

Each Control Manager instance is working with the primary Control Manager database layer. The primary database server (ACM-SQL-1) is replicated using a replication mechanism with the secondary database server (ACM-SQL-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 Portal application management database	You must back up this database only if the Control Manager Voice Portal/Experience Portal module is licensed and enabled.
ACCCMONEXDB	Control Manager centralized Avaya one-X® Agent administration database	You must back up this database only if the Control Manager Avaya one-X® Agent Centralized Administration Management module is licensed and enabled.
ACCCMSYNC	Synchronizes the database between Communication Manager and Control Manager.	You must back up this database.
ACCCMCMSYSLOG	Stores the Communication Manager syslog entries.	You must back up this database.

Backing up Control Manager databases

About this task

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

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

- 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.

Procedure

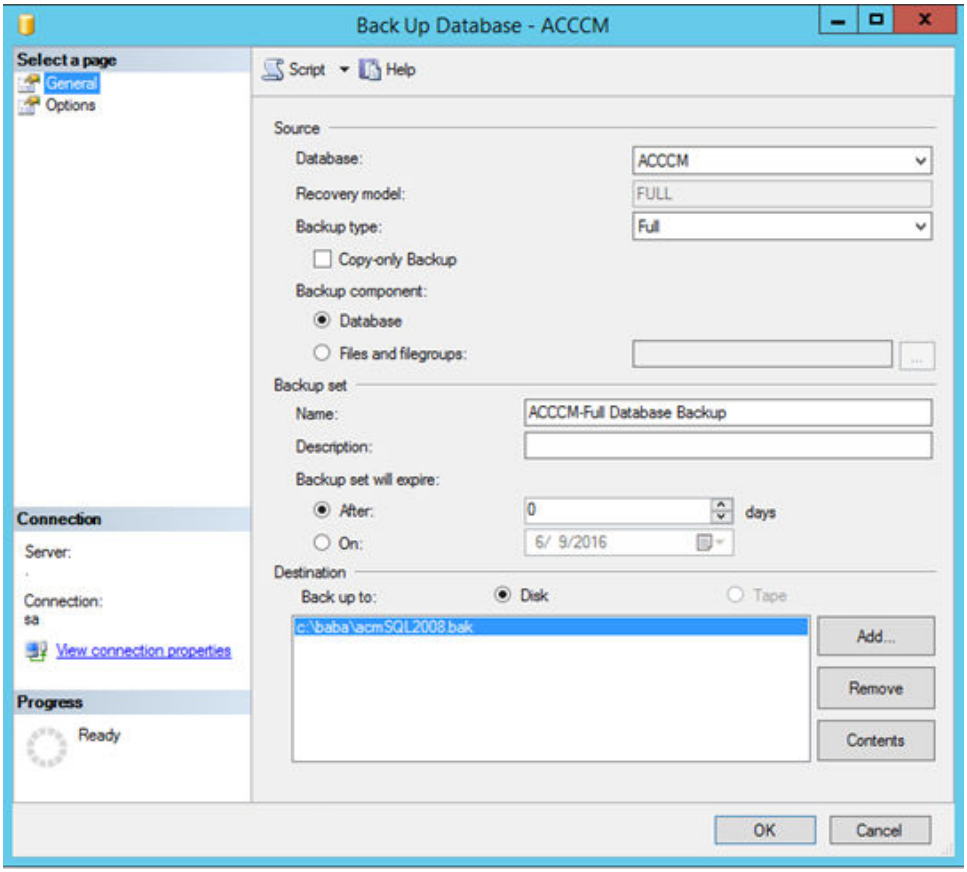
1. On the SQL server used for Control Manager, open the SQL Management Studio application.

2. On the Connect to Server window, provide the following information and log on to the system as administrator:
   - Server type
   - Server name
   - Authentication
   - User name
   - Password
3. In the Object Explorer pane, expand the Databases navigation tree and select the ACCCM database.

   Important:

   When selecting the databases for backup, keep track of any custom named databases in the table shown above. For releases 8.0.x.x and newer, you will should not have custom database names.
4. Right-click the database and select **Tasks** > **Back Up**.

   The system displays the following screen:



5. In the Back Up Database screen, perform the following steps:
   a. In the Select a page pane, select **General**.
   b. In the right pane, from the **Backup type** drop-down list, select **Full**.
   c. In the Destination section, select the directory where you want to store the backup file. Ensure that the filetype is set to `.bak`.
   d. Click **OK** to begin the database backup process.

      The system starts the backup of the database.
6. Repeat these steps to back up all of the databases.

   Important:

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

Removing replication from SQL servers

About this task

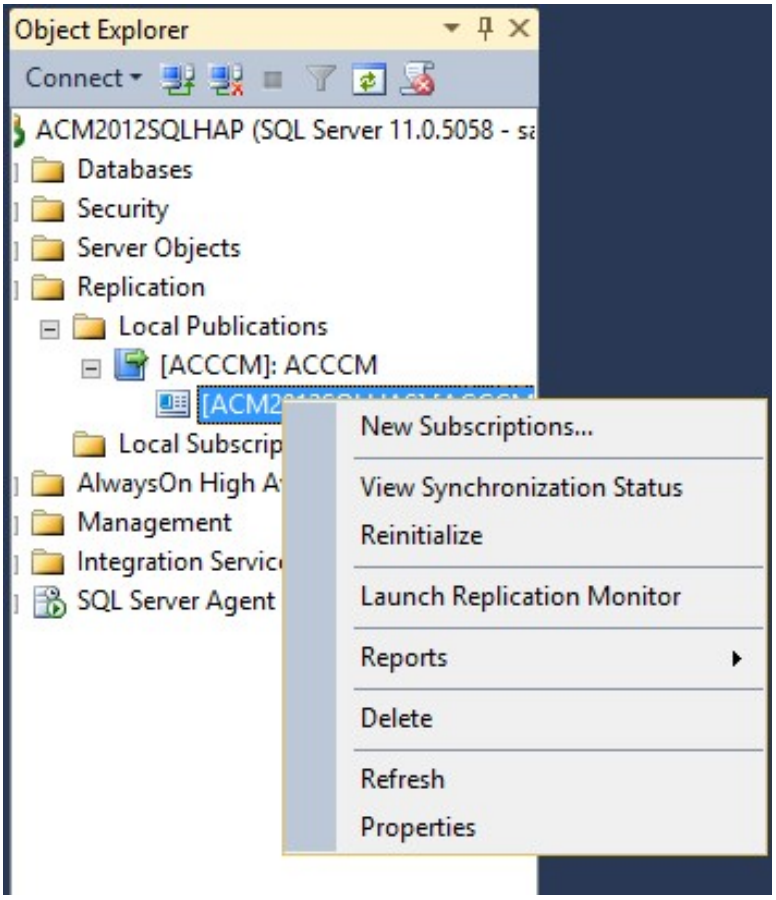
You must remove replication for the following reasons:

- When doing an in-place upgrade for a legacy HA deployment that will continue to use legacy HA after the upgrade. Before upgrading the Control Manager software, you must remove replication between the database servers, then reconfigure replication after you install the Control Manager software.

Procedure

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

   The system displays the Microsoft SQL Server Management Studio screen.
3. In the Object Explorer, navigate to **Replication** > **Local Publications**.
4. Expand the publication you want to remove so you can see all of its subscriptions. See the following example:



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

   A warning message is shown.
6. Verify that the option to connect to the subscriber is selected and click **Yes**.
7. You will be asked to provide credentials to connect to the secondary SQL server.
8. Click **Connect** and the subscription will be removed.
9. If there is more than one subscription, repeat Steps 4-7 for each subscription.
10. When all the subscriptions are removed, right-click on the publication and select **Delete**.
11. When the dialog box comes up, select **Yes**.

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

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

   The system stops any services that are currently running.

   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.

   Important:

   For Legacy HA deployments, the tool stops all services, and the tool starts services that have been set to Automatic start-up mode. Using the tool ensures that the correct number of services are started on both the primary and secondary application servers without any need for manual intervention.
4. Repeat this procedure on all servers that have Control Manager software.

Upgrading Control Manager software

About this task

Use this procedure if you are upgrading any 8.0.x releases (or when upgrading an 8.0.4.x release that is part of an Avaya Oceana® Solution deployment. You must upgrade the Control Manager servers in the following order:

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

Note:

After you upgrade the Control Manager software on the primary application server (ACM-APP-1), repeat this procedure to upgrade the Control Manager software on the secondary

application server (ACM-APP-2). You use the same procedure for both application servers, so the order of the screens in the procedure will be slightly different between the two servers.

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 Microsoft .NET 4.7.2 or higher software has been installed before you attempt to install the Control Manager software. Microsoft .NET Version 4.7.2 is included with the ISO image of 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:\acccminstaller*VersionNumber*.*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 **Enterprise**.
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.
9. For the primary application server (ACM-APP-1), configure the following parameters:
   - **Server Role** — Select **Primary Server**.
   - **HA Mode** — Select **Standard**.
   - **Distribution Type** — Select **All**.
   - **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 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 application server. Do not use the FQDN of the server.

10. For the secondary application server (ACM-APP-2), configure the following parameters:
    - **Server Role** — Select **Secondary Server**.
    - **HA Mode** — Select **Standard**.
    - **Distribution Type** — Select **All**.
    - **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 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 application server. Do not use the FQDN of the server.
11. Click **Next**.

    Important:

    If you are installing software on the primary application server (ACM-APP-1), the system displays the Primary SQL Server screen first followed by the Secondary SQL Server screen. If you are installing software on the secondary application server (ACM-APP-2), the system displays the Secondary SQL Server screen first followed by the Primary SQL Server screen.

12. For the primary SQL database server (ACM-SQL-1), 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, IP 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.

      IP 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.

      IP 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.

13. For the secondary SQL database server (ACM-SQL-2), 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, IP 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.

  IP 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.

  IP 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* and *Installing Control Manager licenses*.
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.
25. Repeat this procedure on the secondary application server.

Next steps

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

Installing Control Manager licenses

About this task

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

- New installations.
- When upgrading (migrating) from any Release 7.x system.
- When activating new connectors for additional Avaya products.
- When the MAC addresses of the servers have changed.
- When you want a new license file to increase the web session inactivity timeout value. The default value is 15 minutes.

You do not need to get a new license when upgrading from Release 8.0.x to Release 8.1.

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.

Before you begin

Get your license file(s) as described in Getting Control Manager licenses on page 32.

Procedure

1. Log on to one of the server(s) that for which you received a license file.
2. Copy the license file to the following location on the server:

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

   Important:

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

   Note:

   The license server must start before any other services are started.
7. In the Services window, confirm that the **ACCCM License Server** service has started.
8. If the **ACCCM License Server** has not started, right-click **ACCCM License Server** and select **Start**.

   The system starts the service.
9. 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

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

Chapter 9: Configuring replication

About replication in a Legacy HA deployment

Control Manager Legacy HA for Enterprise deployments using non-ESS Communication Manager systems leverages the bidirectional transactional replication feature that is available in Microsoft SQL server software. This means is that, under normal operating conditions, any change to the databases on the primary database server (ACM-SQL-1) will be automatically pushed out to the databases on the secondary database server (ACM-SQL-2). The same applies in reverse: any changes made to the databases on the secondary database server (ACM-SQL-2) result in an automated update to the databases on the primary database server (ACM-SQL-1).

Control Manager Legacy HA for Enterprise deployments using Survivable ESS Communication Manager systems leverages the unidirectional and bidirectional transactional replication feature that is available in Microsoft SQL server software. This means is that, under normal operating conditions, any change to the databases on the primary database server (ACM-SQL-1) will be automatically pushed out to the databases on the secondary database server (ACM-SQL-2). However, the same does not apply in reverse for just the ACCCM database: any changes made to the ACCCM database on the secondary database server (ACM-SQL-2) must be manually updated to the ACCCM database on the primary database server (ACM-SQL-1); all other supported databases are updated using bidirectional replication.

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

Within a Control Manager Legacy HA environment, each Control Manager instance is working with a dedicated database layer. The two Microsoft SQL database servers (ACM-SQL-1 and 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 Legacy HA for Enterprise supports in a single or dual data center when not using a Survivable ESS Communication Manager system.

Database	Replication	Direction
ACCCM	Transactional	Bidirectional
ACCCMONEXDB	Transactional	Bidirectional
ACCCMCMSYSLOG	Transactional	Bidirectional
ACCCMSYNC	Transactional	Bidirectional

The following table illustrates the replication strategy for each of the SQL databases that Control Manager Legacy HA for Enterprise supports in a single or dual data center when using a Survivable ESS Communication Manager system.

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

Note:

The ACCCMAVP database is not replicated.

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]
ACCCMCMSYSLOG	CM_Syslog_RawMessages_Temp

Configuring SQL replication on the primary and secondary database servers (ACM-SQL-1 and ACM-SQL-2)

About this task

Use this task after you have had to remove replication for an upgrade or when doing a recovery.

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:

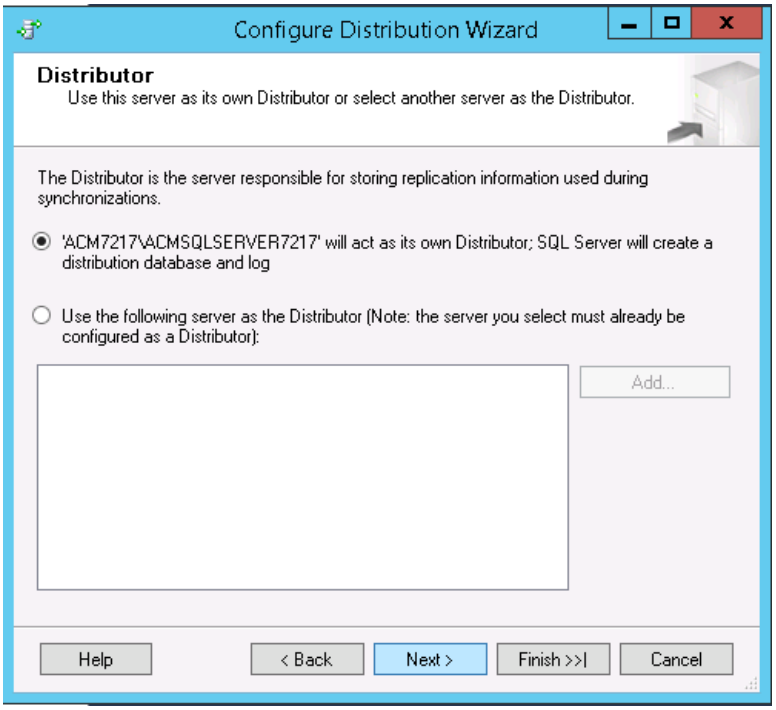
   If you see the **Configure Distribution** option in the menu items, it means that replication has not been configured on the server. If **Configure Distribution** is not displayed, replication has been configured and you can skip this procedure.

5. Select **Configure Distribution**.

   The system displays the Configure Distribution Wizard welcome screen.

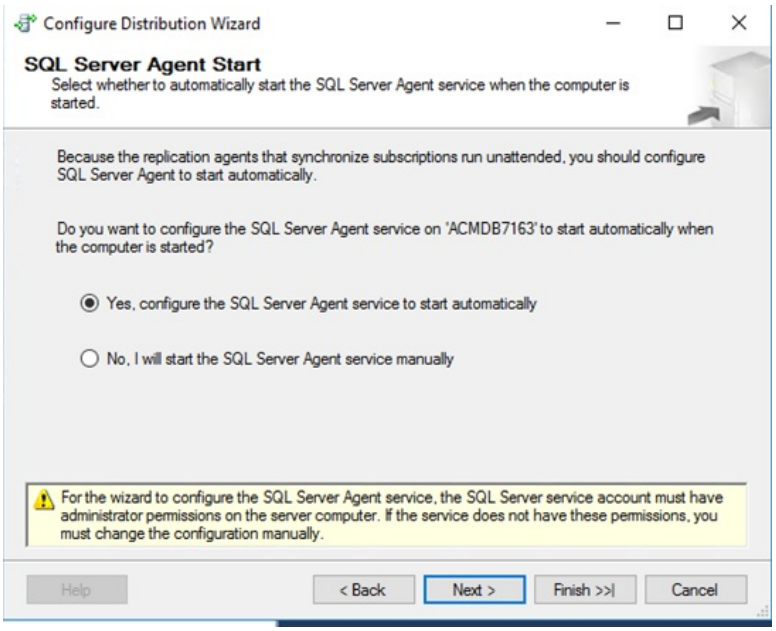
6. Click **Next**.

   The system displays the Distributor screen.



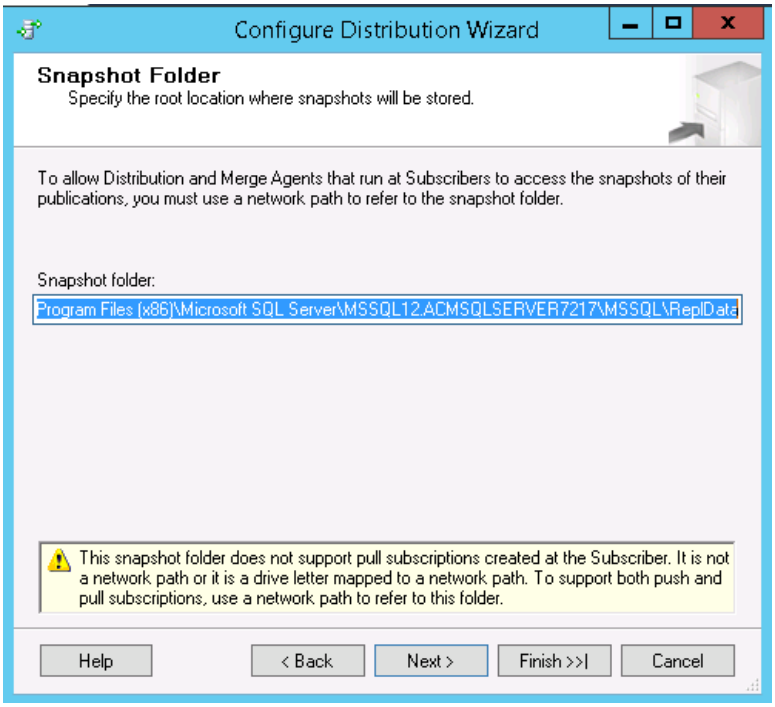
7. Select the first option, **"*DatabaseID*" will act as its own Distributor**. The variable *DatabaseID* represents the actual name of the database server.
8. Click **Next**.

   The system displays the SQL Server Agent Start screen.



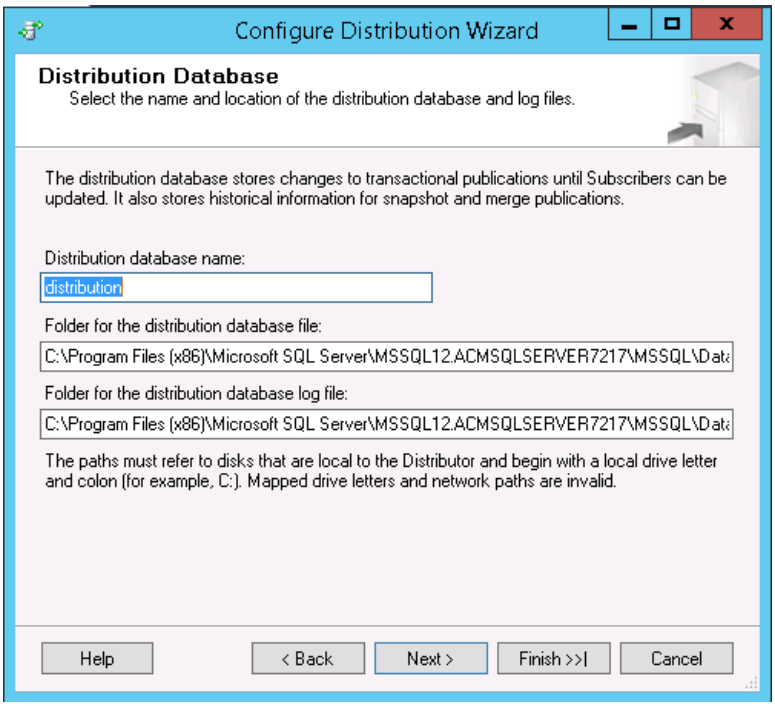
9. Click **Next**.

The system displays the Snapshot Folder screen. Note the path to the snapshot folder. You must use it later in this procedure.



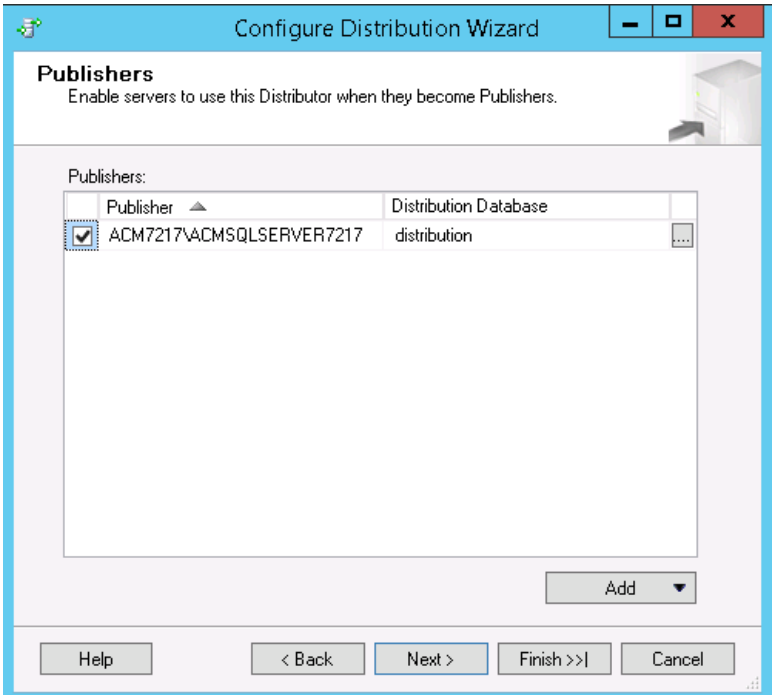
10. Click **Next**.

    The system displays the Distribution Database screen:



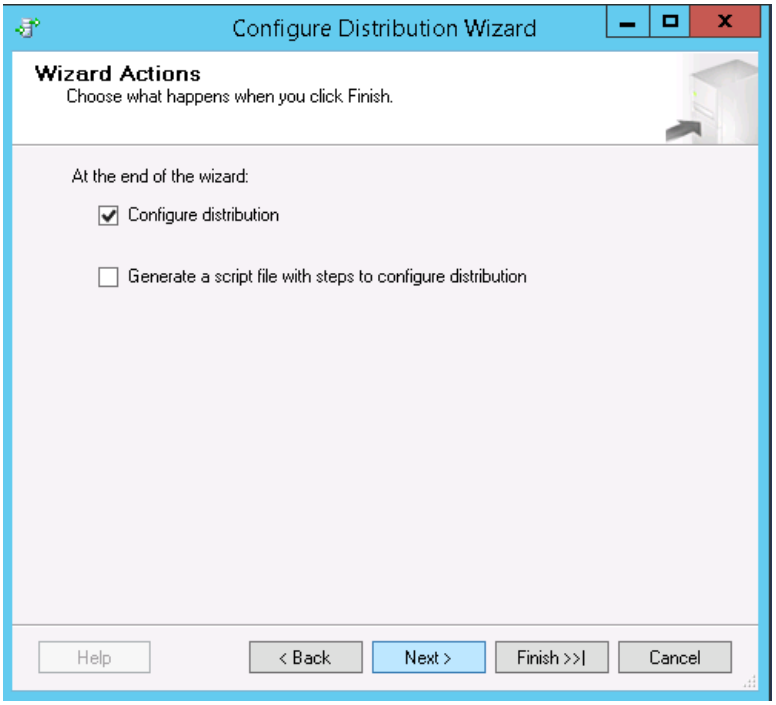
11. Enter the **Distribution database name** and the folders where the data and the log file will reside.
12. Click **Next**.

    The system displays the Publishers screen.



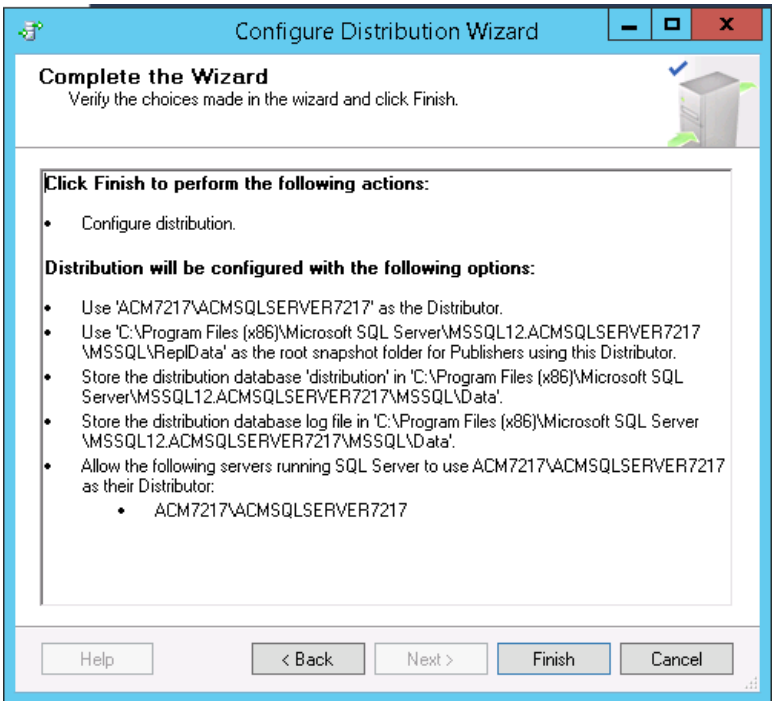
13. Click **Next**.

    The system displays the Wizard Actions screen.



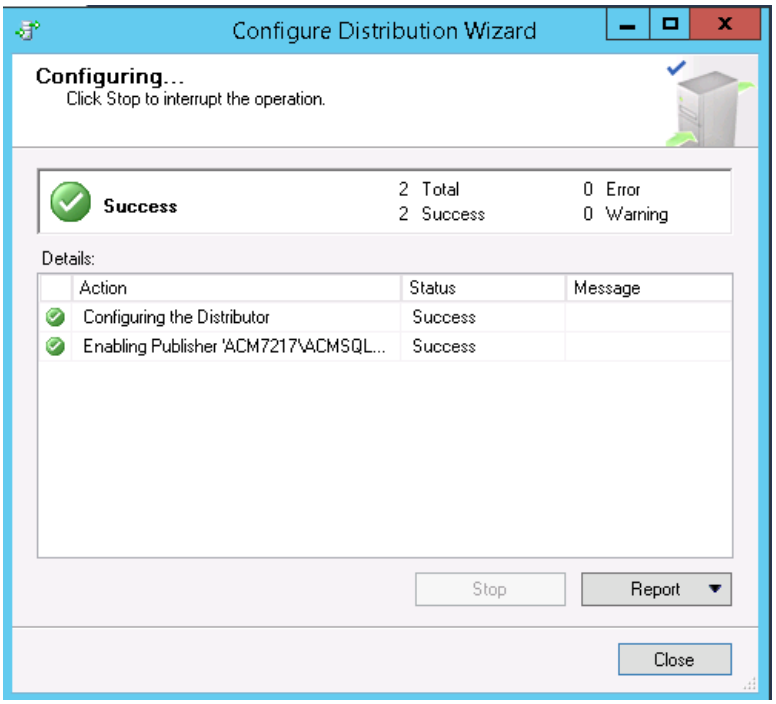
14. Click **Next**.

    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`
    - Microsoft SQL Server 2017 — `C:\Program Files (x86)\Microsoft SQL Server\MSSQL14.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`
- Microsoft SQL Server 2017 — `C:\Program Files\Microsoft SQL Server\MSSQL14.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`
- Microsoft SQL Server 2017 — `C:\Program Files (x86)\Microsoft SQL Server\MSSQL14.[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`
- Microsoft SQL Server 2017 — `C:\Program Files\Microsoft SQL Server\MSSQL14.[Instance Name]\MSSQL\ReplData`

18. Right-click on the folder and select **Properties**.

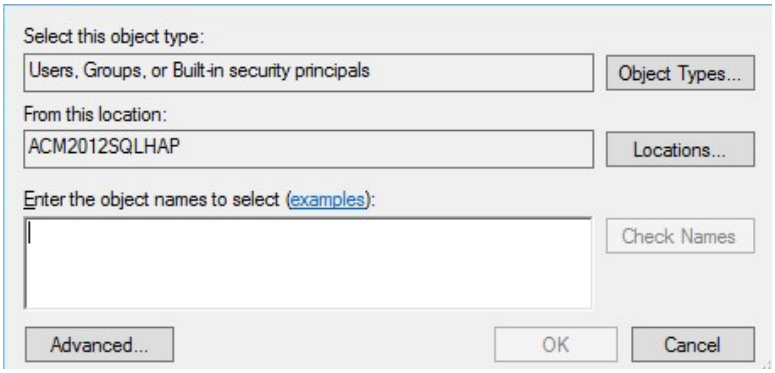
    The system displays the ***FolderName*** Properties screen.

19. Select the **Security** tab.
20. Click **Edit**.

    The system displays the Permissions for ***FolderName*** **Properties** screen.

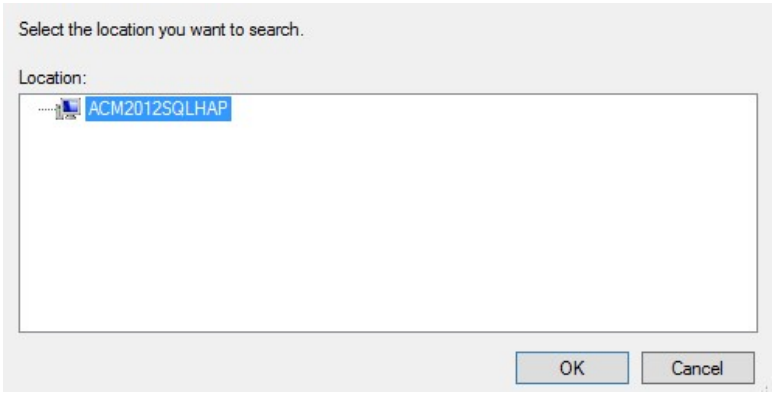
21. Click **Add**.

    The system displays the Select Users, Computers, Service Accounts, or Groups screen.



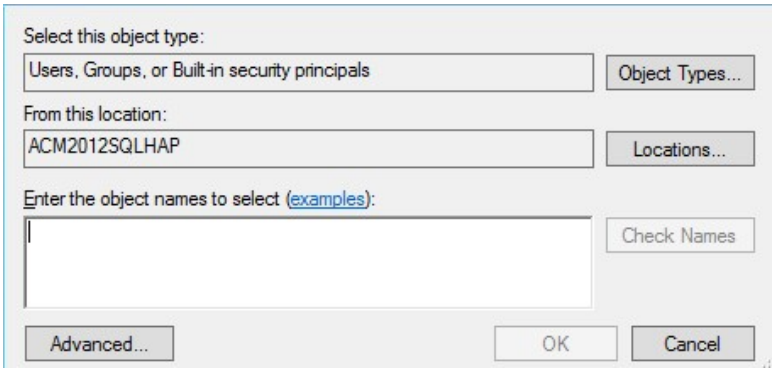
22. Click **Locations**.

    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. Repeat steps 18–29 depending on which version of Microsoft SQL software you are using. Select one of the following folders when you repeat Steps 18–29:

    For Microsoft SQL Server (x86) edition when using an instance name:

    - Microsoft SQL Server 2012 — `C:\Program Files (x86)\Microsoft SQL Server\110`
    - Microsoft SQL Server 2014 — `C:\Program Files (x86)\Microsoft SQL Server\120`
    - Microsoft SQL Server 2016 — `C:\Program Files (x86)\Microsoft SQL Server\130`
    - Microsoft SQL Server 2017 — `C:\Program Files (x86)\Microsoft SQL Server\140`

    For Microsoft SQL Server (x64) edition when using an instance name:

    - Microsoft SQL Server 2012 — `C:\Program Files\Microsoft SQL Server\110`
    - Microsoft SQL Server 2014 — `C:\Program Files\Microsoft SQL Server\120`
    - Microsoft SQL Server 2016 — `C:\Program Files\Microsoft SQL Server\130`
    - Microsoft SQL Server 2017 — `C:\Program Files\Microsoft SQL Server\140`

31. Log on to the secondary SQL database server (ACM-SQL-2).
32. Repeat Steps 17-30 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
ACCCMONEXDB	Publisher	Subscriber
ACCCMCMSYSLOG	Publisher	Subscriber
ACCCMSYNC	Publisher	Subscriber

Note:

The ACCCMAVP database is not replicated.

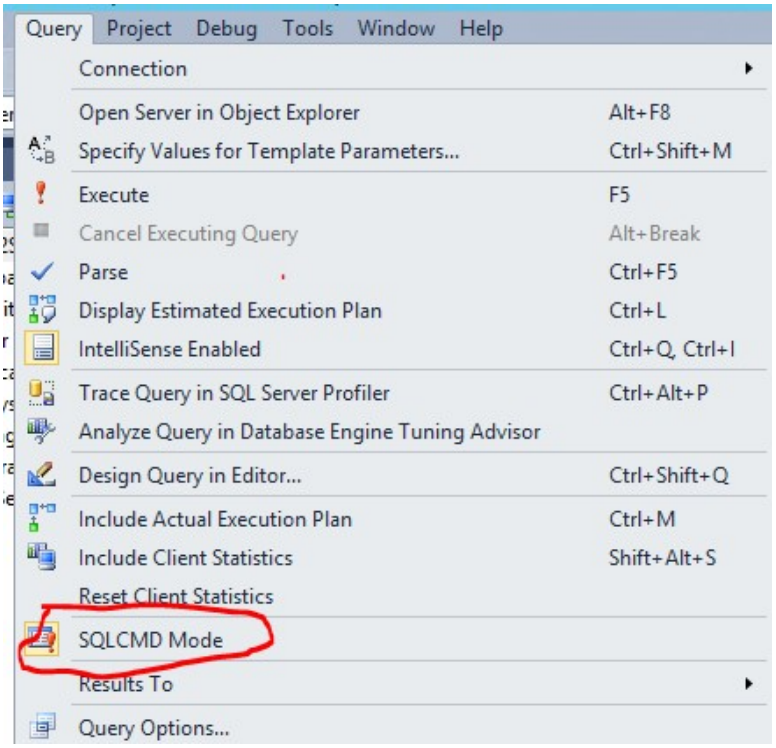
Before you begin

Get the transactional replication setup scripts from the Control Manager ISO installation file.

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 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**.



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).

Table continues…

Configuration Option	Description
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, ACCCMONEXDB, 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

The following is an example of the header in the SQL file:

```
/*

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)
```

8. Save the changes to the file.
9. Set up the options you wish to apply to this replication setup.

   Use the information in the following table to edit the values in this section of the SQL script:

Setup Option	Description
declare @IgnorePublicationExistence bit = 0/1	0 — The default of 0 will cause the script to exit if the database has already been published. 1 — Set the value to 1 to have the script continue even if the database has been published already. Setting the value to 1 is useful where you need to add tables to the publication or you wish to rerun they script having resolved an error
:SETVAR updateable bit = 0/1	0 — Set to 0 if you are using unidirectional replication. This is the required setting for an xCaaS or Avaya Oceana® Solution Geo Redundant HA deployment. 1 — Set to 1 if you are using bidirectional replication. This is the setting for a basic Enterprise Legacy HA deployment.
declare @ignoretableswithnoprimarykey bit = 0/1	0 — The default value of 0 will cause the script to exit if any tables in the source database lacks a primary key. 1 — Setting this value to 1 will override this behavior. Use the value of 1 for Enterprise Legacy HA deployments. **Note:** Any table missing a primary key will not be added to the publication.
declare @AddTables bit = 0/1	0 — Set to 0 to not include tables in the publication. In most cases, do not set this option to 0. 1 — The default value of 1 will include tables in the publication. This is the setting you should use unless directed otherwise by support personnel.
declare @addviews bit = 0/1	0 — The default value of 0 will not include views in the publication. 1 — Set to 1 to include views in the publication.
declare @addstoredprocedures bit = 0/1	0 — The default value of 0 will not include stored procedures in the publication. 1 — Set to 1 to include stored procedures in the publication.
declare @addfunctions bit = 0/1	0 — The default value of 0 will not include functions in the publication. 1 — Set to 1 to include functions in the publication.

The following is an example of the SQL script with the required options highlighted:

```
--SQL Variables Section

--Continue if the database has already been published, defaults to 0. Set to 1 if
you want to add new tables etc
--to database already replicated
declare @IgnorePublicationExistence bit = 0;

--Set to 0 for uni-directional replication, 1 for bi-directional replication
:SETVAR updateable 1

--If tables do not have a primary key defined they cannot be replicated
--Set to 1 to ignore tables without keys and continue, set to 0 to raise error
and stop script.
declare @ignoretableswithnoprimarykey bit = 1;

--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
```

10. Save the changes to the script file.
11. 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.
12. Once the script has completed, check the output tab in SQL Management Studio for any errors.
13. Repeat this procedure for the following Control Manager databases:
    - ACCCM
    - ACCCMONEXDB
    - ACCCMCMSYSLOG
    - ACCCMSYNC

    Note:

    The ACCCMAVP database is not replicated.

Enabling replication on the database servers

About this task

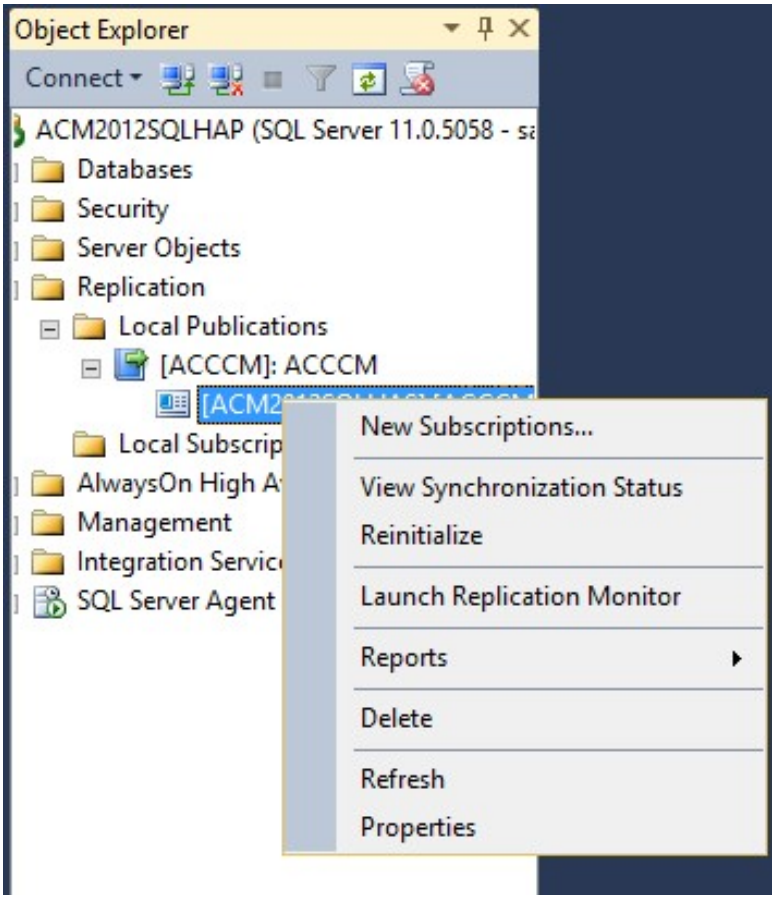
After configuring each of the Control Manager databases for replication, perform the following task on each of the Control Manager databases to verify the overall health of the replication environment.

Procedure

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

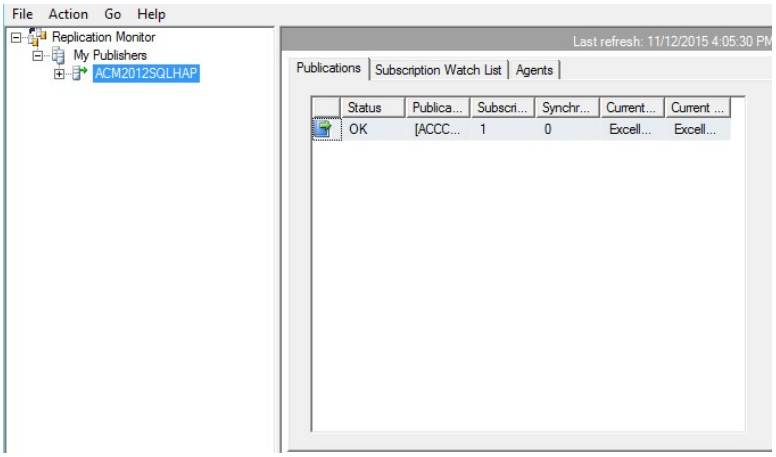
   The system displays the Microsoft SQL Server Management Studio screen.

2. Right-click on the Replication folder of the subscription that was previously created. See the following example:

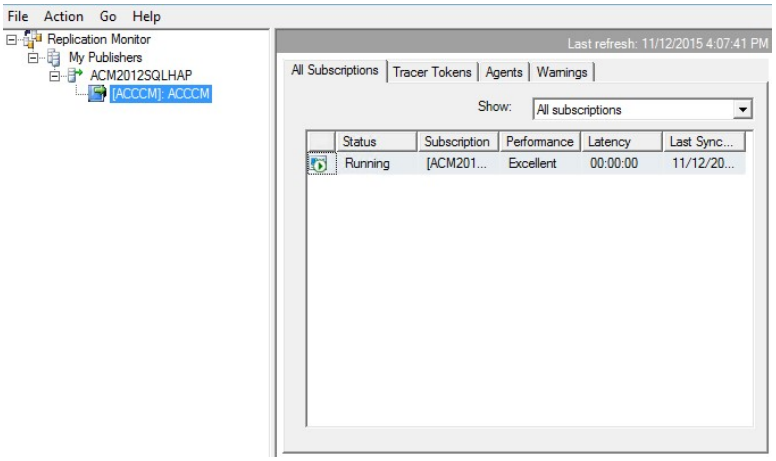


3. Select **Launch Replication Monitor**.

   The system displays the Replication Monitor screen.

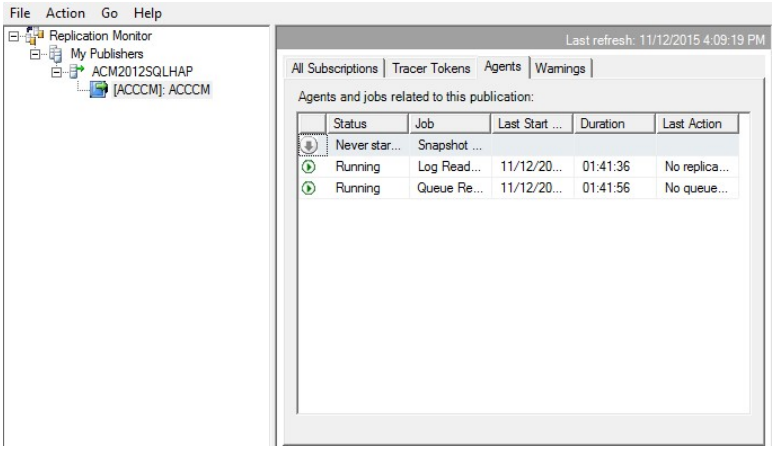


4. In the left pane under **My Publishers**, select the Control Manager **Publication** node and expand the folders to get a list of the subscriptions on the primary database server (ACM-SQL-1). See the following example:



5. Select the **Agents** tab.

   The system displays the following screen:



6. Right-click on **Snapshot Agent** job and click **Start Agent**.

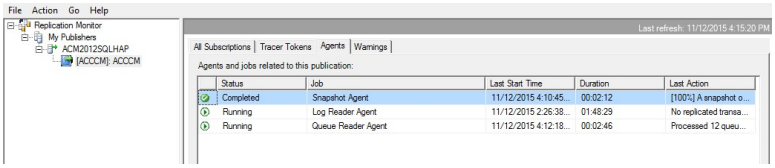
   This updates the agent settings. The process can take up to 30 minutes.

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:



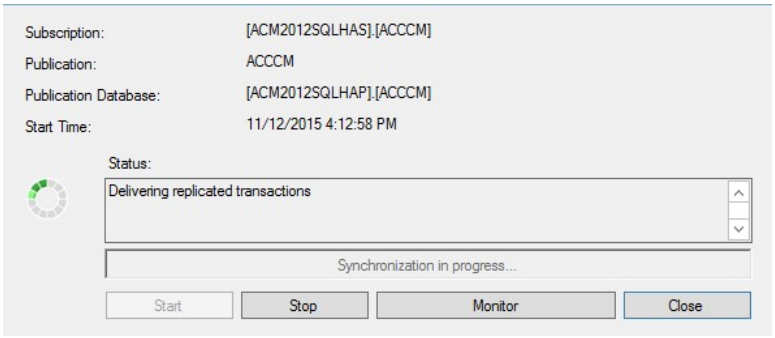
9. When the **Snapshot Agent** job reaches 100% in the **Last Action** column, close the window.

10. Repeat steps 1 through 9 for each database that requires replication.

11. Do one of the following to view synchronization status:

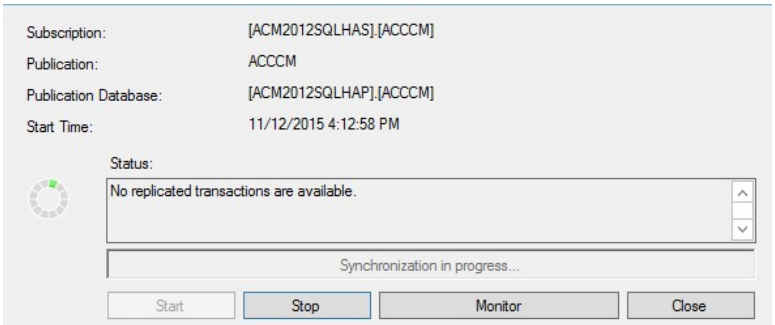
    - On the primary database server (ACM-SQL-1), in **Object Explorer**, expand the **Local Publications** folder, right-click on the **Subscription**, and choose **View Synchronization Status**.
    - On the secondary database server (ACM-SQL-2), in **Object Explorer**, expand the **Local Subscriptions** 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.

Next steps

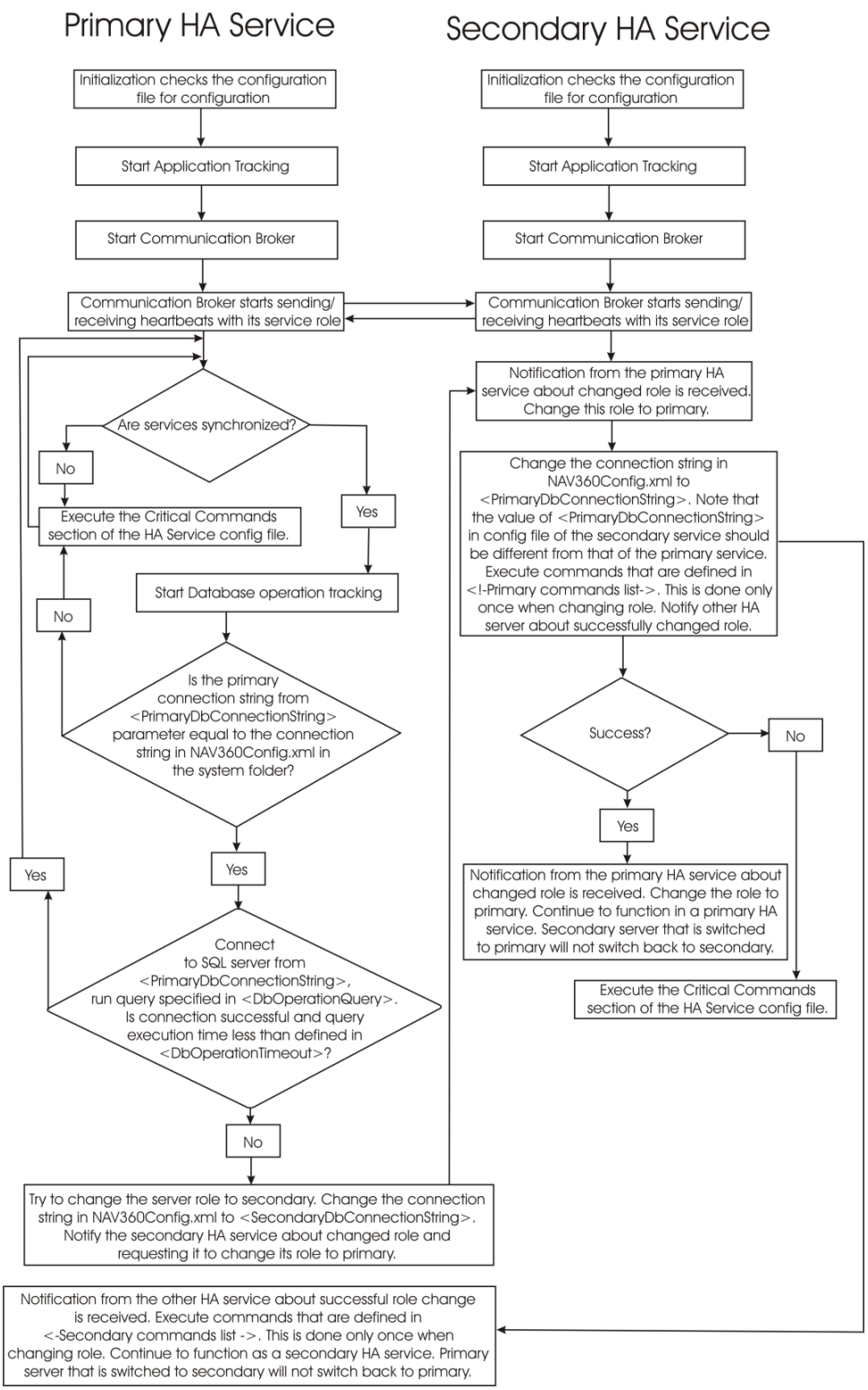
After you finish setting up replication, enable the firewall software.

Continue with the chapter *Configuring Legacy HA services*.

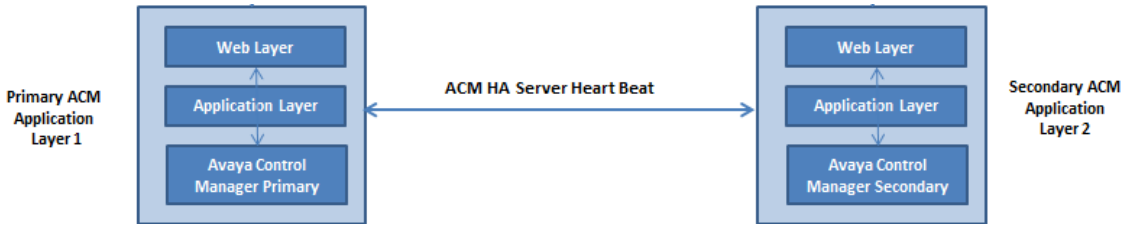
Chapter 10: Configuring Legacy HA services

About Legacy HA services

The key to any Control Manager Legacy 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 Legacy HA

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 Legacy 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).

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

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

   The system stops any services that are currently running.

   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.

   Important:

   For Legacy HA deployments, the tool stops all services, and the tool starts services that have been set to Automatic start-up mode. Using the tool ensures that the correct number of services are started on both the primary and secondary application servers without any need for manual intervention.
4. 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 database 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 database server (ACM-SQL-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 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. Add the following lines to the `<Applications>` section of the `configuration.xml` file. Doing this supports proper failover for the Experience Portal (IVR) and Call Center Elite Multichannel features.

Note:

Note the following when editing this file:

- The `ACMSQL1` and `ACMSQL2` Data Source variables must be replaced with the actual database server names.

- The `PlainTextPassword` variables must be replaced with the plain text password for the database. When the HA services are started, the plain text password will be securely encrypted.

```
<Application name="IVR1">
<configFileName>InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager\Web
\ACCCM IVR WEB\Web.config</configFileName>
<configParamName>//connectionStrings/add[@name='nav360IVRConnectionString']</
configParamName>
<configParamAttributeName>connectionString</configParamAttributeName>
<primaryConnStr>Data Source=ACMSQL1;Initial Catalog=ACCCMAVP;Integrated
Security=False;User ID=ACCCMAVP;Password="PlainTextPassword"</primaryConnStr>
<secondaryConnStr>Data Source=ACMSQL2;Initial Catalog=ACCCMAVP;Integrated
Security=False;User ID=ACCCMAVP;Password="PlainTextPassword"</secondaryConnStr>
<dbOperationQuery>SELECT 1</dbOperationQuery>
<dbOperationTimeout>7000</dbOperationTimeout>
</Application>
```

```
<Application name="IVR2">
<configFileName>InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager\Web
\ACCCM IVR WEB\Web.config</configFileName>
<configParamName>//connectionStrings/add[@name='nav360ConnectionString']</
configParamName>
<configParamAttributeName>connectionString</configParamAttributeName>
<primaryConnStr>Data Source=ACMSQL1;Initial Catalog=ACCCM;User
ID=ACCCM;Password="PlainTextPassword"</primaryConnStr>
<secondaryConnStr>Data Source=ACMSQL2;Initial Catalog=ACCCM;User
ID=ACCCM;Password="PlainTextPassword"</secondaryConnStr>
<dbOperationQuery>SELECT 1</dbOperationQuery>
<dbOperationTimeout>7000</dbOperationTimeout>
</Application>
```

```
<Application name="EMC nav360ConnectionString">
<configFileName>InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager\Web
\ACCCM EMC\Web.config</configFileName>
<configParamName>//connectionStrings/add[@name='nav360ConnectionString']</
configParamName>
<configParamAttributeName>connectionString</configParamAttributeName>
<primaryConnStr>Data Source=ACMSQL1;Initial Catalog=ACCCM;User
ID=ACCCM;Password="EncryptedPassword"</primaryConnStr>
<secondaryConnStr>Data Source=ACMSQL2;Initial Catalog=ACCCM;User
ID=ACCCM;Password="EncryptedPassword"</secondaryConnStr>
<dbOperationQuery>SELECT 1</dbOperationQuery>
<dbOperationTimeout>7000</dbOperationTimeout>
</Application>
```

16. 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. Add the following lines to the `<Applications>` section of the `configuration.xml` file. Doing this supports proper failover for the Experience Portal (IVR) and Call Center Elite Multichannel features.

    Note:

    Note the following when editing this file:

    - The `ACMSQL1` and `ACMSQL2` Data Source variables must be replaced with the actual database server names.
    - The `PlainTextPassword` variables must be replaced with the plain text password for the database. When the HA services are started, the plain text password will be securely encrypted.

```
<Application name="IVR1">
<configFileName>InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager\Web
\ACCCM IVR WEB\Web.config</configFileName>
<configParamName>//connectionStrings/add[@name='nav360IVRConnectionString']</
configParamName>
<configParamAttributeName>connectionString</configParamAttributeName>
<primaryConnStr>Data Source=ACMSQL1;Initial Catalog=ACCCMAVP;Integrated
Security=False;User ID=ACCCMAVP;Password="PlainTextPassword"</primaryConnStr>
<secondaryConnStr>Data Source=ACMSQL2;Initial Catalog=ACCCMAVP;Integrated
Security=False;User ID=ACCCMAVP;Password="PlainTextPassword"</secondaryConnStr>
<dbOperationQuery>SELECT 1</dbOperationQuery>
<dbOperationTimeout>7000</dbOperationTimeout>
</Application>
```

```
<Application name="IVR2">
<configFileName>InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager\Web
\ACCCM IVR WEB\Web.config</configFileName>
<configParamName>//connectionStrings/add[@name='nav360ConnectionString']</
configParamName>
<configParamAttributeName>connectionString</configParamAttributeName>
<primaryConnStr>Data Source=ACMSQL1;Initial Catalog=ACCCM;User
ID=ACCCM;Password="PlainTextPassword"</primaryConnStr>
<secondaryConnStr>Data Source=ACMSQL2;Initial Catalog=ACCCM;User
ID=ACCCM;Password="PlainTextPassword"</secondaryConnStr>
<dbOperationQuery>SELECT 1</dbOperationQuery>
<dbOperationTimeout>7000</dbOperationTimeout>
</Application>
```

```
<Application name="EMC nav360ConnectionString">
<configFileName>InstallDrive:\Program Files (x86)\Avaya\Avaya Control Manager\Web
\ACCCM EMC\Web.config</configFileName>
<configParamName>//connectionStrings/add[@name='nav360ConnectionString']</
configParamName>
<configParamAttributeName>connectionString</configParamAttributeName>
<primaryConnStr>Data Source=ACMSQL1;Initial Catalog=ACCCM;User
ID=ACCCM;Password="PlainTextPassword"</primaryConnStr>
<secondaryConnStr>Data Source=ACMSQL2;Initial Catalog=ACCCM;User
ID=ACCCM;Password="PlainTextPassword"</secondaryConnStr>
<dbOperationQuery>SELECT 1</dbOperationQuery>
<dbOperationTimeout>7000</dbOperationTimeout>
</Application>
```

16. Save and close the file.

HA Service for the Avaya one-X® Agent server configuration

If Avaya one-X® Agent is part of the Control Manager HA environment, perform the procedures in this section to configure the HA Service on the Avaya one-X® Agent server.

Note:

If you are not using Avaya one-X® Agent in your HA environment, edit the HA configuration file to remove the Application section in the file.

The Avaya one-X® Agent database of Control Manager has its own database connection strings that are separate from the Control Manager related database connection strings. Perform the following procedures to configure the Avaya one-X® Agent failover configuration for both the primary and the secondary application servers (ACM-APP-1 and ACM-APP-2).

Related links

Configuring the Avaya one-X Agent Web portal connection string on page 146
Configuring the Avaya one-X Agent primary database server (ACM-SQL-1) connection string in the web.config files on the secondary application server (ACM-APP-2) on page 148
Configuring the Avaya one-X Agent CFG connection string on both application servers on page 149
Configuring the Avaya one-X Agent Profile Loader connection string on both application servers on page 150
Configuring the Avaya one-X Agent Profile Loader Service configuration file on the secondary application server (ACM-APP-2) on page 152

Configuring the Avaya one-X® Agent Web portal connection string

About this task

Use this task to configure the Avaya one-X® Agent database connection string that the primary Control Manager Web portal uses.

Procedure

1. Log on to Windows on the primary application server (ACM-APP-1).
2. Navigate to the Control Manager Avaya one-X® Agent `web.config` file located at:

   [Install Location]`\Web\ACCCM ONEX WEB\web.config`
3. Open the `web.config` file.
4. Navigate to the `configuration.xml` file located at:

   [Install Location]`:\Program Files (x86)\Avaya\Avaya Control Manager \Services\ACCCM HA Service\configuration.xml`

5. Open the `configuration.xml` file for editing. See the following example of the lines used for the Avaya one-X® Agent Web portal connection:

```
================================================

<!-- Supported applications list -->

<Application name="ACCCM ONEX WEB">

<configFileName>InstallDrive:\Program Files (x86)\Avaya\Avaya
Control Manager\Web\ACCCM ONEX WEB\web.config</configFileName>

<configParamName>//configuration//appSettings/add[@key='DB'] </
configParamName>

<configParamAttributeName>value</configParamAttributeName>

<primaryConnStr>Data Source=SQL1;Initial Catalog=ACCCMONEXDB;User
ID=ACCCMONEXUSER;Password="EncryptedPassword"</primary ConnStr>

<secondaryConnStr>Data Source=SQL2;Initial Catalog=ACCCMONEXDB;User
ID=ACCCMONEXUSER;Password="EncryptedPassword"</secondaryConnStr>

<dbOperationQuery>select * from csuser</dbOperationQuery>

<dbOperationTimeout>5000</dbOperationTimeout>

</Application>
```

6. Copy the required connection strings from the `web.config` file to the required section in the `configuration.xml` file.
7. Enter the SQL user name and the original encrypted password into the connection strings in the `configuration.xml` file.

   Note:

   You must make sure that the connection strings entered are correct and include the correct Avaya one-X® Agent SQL user name and encrypted password.

8. Save and close the `configuration.xml` file.
9. Close the `web.config` file.
10. Repeat this procedure on the secondary application server (ACM-APP-2).

    Important:

    On the secondary application server (ACM-SQL-2), the `primaryConnStr` must point to `DataSource=SQL1` and the `secondaryConnStr` must point to `DataSource=SQL2`.

Configuring the Avaya one-X® Agent primary database server (ACM-SQL-1) connection string in the web.config files on the secondary application server (ACM-APP-2)

About this task

You must configure the Avaya one-X® Agent connection string to the primary database server (ACM-SQL-1) in the `web.config` file on the secondary application server (ACM-APP-2).

Procedure

1. Log on to Windows on the secondary application server (ACM-APP-2).
2. Open the following file using a text editor:

   InstallLocation\Web\ACCCM ONEX WEB\web.config
3. Enter the connection string for the primary database server (ACM-SQL-1). See the following example, where *[SQL1]* is the FQDN of the primary database server (ACM-SQL-1) and *[EncryptedPassword]* is the password for the primary database server (ACM-SQL-1).

   ```
   <add key="DB" value="Data Source=[SQL1];Initial Catalog=ACCCMONEXDB;User
   ID=ACCCMONEXUSER;Password=[EncryptedPassword]" />
   ```
4. Save and close the file.
5. Open the following file using a text editor:

   InstallLocation\Web\ACCCM ONEX CFG\web.config
6. Enter the Local_Pub connection string for the primary database server (ACM-SQL-1) . See the following example, where *[SQL1]* is the FQDN of the primary database server (ACM-SQL-1) and *[EncryptedPassword]* is the password for the primary database server (ACM-SQL-1).

   ```
   <connectionStrings>
   <add name="Local" connectionString="Data Source=[SQL1],
   1433;MultipleActiveResultSets=True;Initial Catalog= ACCCMONEXDB;Integrated
   Security=True" providerName="System.Data.SqlClient"/>
   <add name="Local_Pub" connectionString="Data Source=[SQL1],1433;Initial Catalog=
   ACCCMONEXDB;Persist Security Info=True;User
   ID=ACCCMONEXUSER;Password=[EncryptedPassword];;MultipleActiveResultSets=True"
   providerName="System.Data.SqlClient"/>
   </connectionStrings>
   ```
7. Save and close the file.

Configuring the Avaya one-X® Agent CFG connection string on both application servers

About this task

Use this task to configure the integration CFG folder for Avaya one-X® Agent.

Important:

You must do this procedure on both application servers.

Procedure

1. Log on to Windows on the primary application server (ACM-APP-1).
2. Navigate to the Control Manager Avaya one-X® Agent `web.config` file located at:

   [Install Location]\Web\ACCCM ONEX CFG\web.config
3. Open the `web.config` file.
4. Navigate to the `configuration.xml` file located at:

   [Install Location]:\Program Files (x86)\Avaya\Avaya Control Manager \Services\ACCCM HA Service\configuration.xml
5. Open the `configuration.xml` file for editing. See the following example of the lines used for the Avaya one-X® Agent CFG connection:

```
================================================

<!-- Supported applications list -->

<Application name="ACCCM ONEX CFG">

<configFileName>InstallDrive:\Program Files (x86)\Avaya\Avaya
Control Manager\Web\ACCCM ONEX CFG\web.config</configFileName>

<configParamName>//configuration//connectionStrings/
add[@name='Local_Pub']</configParamName>

<configParamAttributeName>connectionString</
configParamAttributeName>

<primaryConnStr>Data Source=SQL1;Initial
Catalog=ACCCMONEXDB;Persist Security Info=True;User
ID=ACCCMONEXUSER;Password="EncryptedPassword";MultipleActiveResultS
ets=True</primary ConnStr>

<secondaryConnStr>Data Source=SQL2;Initial
Catalog=ACCCMONEXDB;Persist Security Info=True;User
ID=ACCCMONEXUSER;Password="EncryptedPassword";MultipleActiveResultS
ets=True</secondaryConnStr>

<dbOperationQuery>select * from csuser</dbOperationQuery>
```

```
<dbOperationTimeout>5000</dbOperationTimeout></Application>
</Application>
```

6. Copy the required connection strings from the `web.config` file to the required section in the `configuration.xml` file.
7. Enter the SQL user name and the original encrypted password into the connection strings in the `configuration.xml` file.

   Note:

   You must make sure that the connection strings entered are correct and include the correct Avaya one-X® Agent SQL user name and encrypted password.
8. Save and close the `configuration.xml` file.
9. Close the `web.config` file.
10. Log on to Windows on the secondary application server (ACM-APP-2).
11. Repeat Steps 2–9 on the secondary application server (ACM-APP-2).

Configuring the Avaya one-X® Agent Profile Loader connection string on both application servers

About this task

Use this task to configure the Profile Loader connection string for Avaya one-X® Agent.

Important:

You must do this procedure on both application servers.

Procedure

1. Log on to Windows on the primary application server (ACM-APP-1)
2. Locate the Control Manager Avaya one-X® Agent `AvayaOneAgentProfilerLoaderService.exe.config` file located at:

   `[Install Location]\Services\ACCCM OneAgentProfilerLoaderService\AvayaOneAgentProfilerLoaderService.exe.config`
3. Open the `AvayaOneAgentProfilerLoaderService.exe.config` file.
4. Navigate to the `configuration.xml` file located at:

   `[Install Location]:\Program Files (x86)\Avaya\Avaya Control Manager\Services\ACCCM HA Service\configuration.xml`
5. Open the `configuration.xml` file for editing. See the following example of the lines used for the Avaya one-X® Agent Profile Loader Service connection:

   ```
   ================================================
   ```

```
<!-- Supported applications list -->

<Application name="ONEX PROFILE LOADER">

<configFileName>InstallDrive:\Program Files (x86)\Avaya\Avaya
Control Manager\Services\ACCCM OneAgentProfilerLoaderService
\AvayaOneAgentProfilerLoaderService.exe.config\</configFileName>

<configParamName>//configuration//connectionStrings/
add[@name='Local_Pub']</configParamName>

<configParamAttributeName>connectionString</
configParamAttributeName>

<primaryConnStr>Data Source=SQL1;Initial
Catalog=ACCCMONEXDB;Persist Security Info=True;User
ID=ACCCMONEXUSER;Password="EncryptedPassword";MultipleActiveResultS
ets=True</primary ConnStr>

<secondaryConnStr>Data Source=SQL2;Initial
Catalog=ACCCMONEXDB;Persist Security Info=True;User
ID=ACCCMONEXUSER;Password="EncryptedPassword";MultipleActiveResultS
ets=True</secondaryConnStr>

<dbOperationQuery>select * from csuser</dbOperationQuery>

<dbOperationTimeout>5000</dbOperationTimeout></Application>

</Application>
```

6. Copy the required connection strings from the `AvayaOneAgentProfilerLoaderService.exe.config` file to the required section in the `configuration.xml` file.
7. Enter the SQL user name and the original encrypted password into the connection strings in the `configuration.xml` file.

   Note:

   You must make sure that the connection strings entered are correct and include the correct Avaya one-X® Agent SQL user name and encrypted password.
8. Save and close the `configuration.xml` file.
9. Close the `AvayaOneAgentProfilerLoaderService.exe.config` file.
10. Log on to Windows on the secondary application server (ACM-APP-2).
11. Repeat Steps 2–9 on the secondary application server (ACM-APP-2).

    Important:

    For the `configuration.xml` connection strings to the secondary application server (ACM-SQL-2), the `primaryConnStr` must point to `DataSource=SQL1` and the `secondaryConnStr` must point to `DataSource=SQL2`.

Configuring the Avaya one-X® Agent Profile Loader Service configuration file on the secondary application server (ACM-APP-2)

About this task

You must configure the Avaya one-X® Agent `sphereFeederConfig.xml` file with the secondary application server FQDN.

Procedure

1. Log on to Windows on the secondary application server (ACM-APP-2).
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 ACCCM One Agent Profile Loader Service and select **Stop**.
5. Open the following file using a text editor:

   InstallLocation`\Services\ACCCM\ OneAgentProfilerLoaderService \AvayaOneAgentProfilerLoaderService.exe.config`
6. Enter the connection string for the primary database server (ACM-SQL-1). See the following example, where *[ConnectionString]* is the connection string and *[SQL1]* is the FQDN of the primary database server (ACM-SQL-1).

   ```
   <add name="Local_Pub" [ConnectionString]="Data Source=[SQL1],1433;Initial
   Catalog=ACCCMONEXDB;Persist Security Info=True;User
   ID=ACCCMONEXUSER;Password="encryptedPW";MultipleActiveResultSets=True"
   providerName="System.Data.SqlClient" />
   ```
7. Save and close the file.
8. Navigate to **Start** > **Run**.
9. Enter `services.msc` and press **Enter**.

   The system displays a list of services.
10. In the Services window, right-click the ACCCM One Agent Profile Loader Service and select **Start**.

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 on page 64 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.

Chapter 11: 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 on the 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 on the Control Manager application servers.

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. Select the user interface language you want to use. The default language is English.
3. Enter your user name in the **Username** field. Enter `itnv` if you are logging in for the first time.
4. Enter your password in the **Password** field. Enter `itnv` if you are logging in for the first time.

   Important:

   The first time you login, the system prompts you to enter a new password.

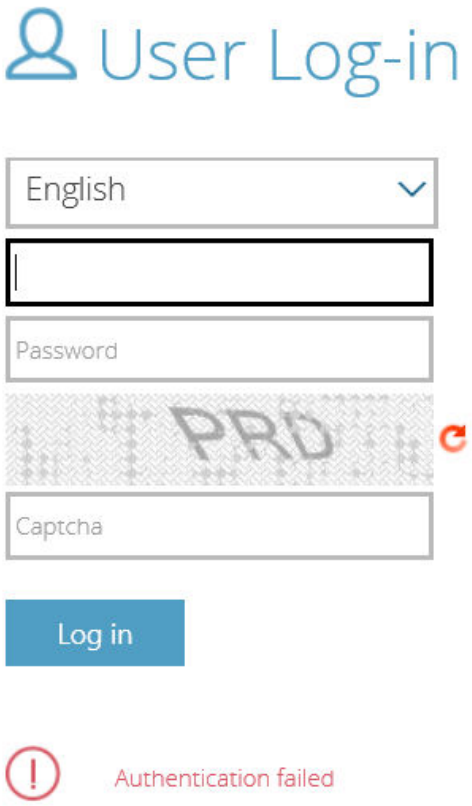
   Remember this password since it is now the new password for your only user ID until you create new Control Manager users.

   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 **Log in**.

   Note:

   If you incorrectly enter your logon credentials three times, the system will require you to enter your correct user name and password along with a CAPTCHA string of characters before attempting to log on again.



Verifying the TLS version

About this task

Control Manager Release 8.1 only supports Transport Layer Security (TLS) 1.2 or newer. TLS 1.2 is installed automatically when you install the IIS software. 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.

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.

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 12: Resources

Documentation

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

Title	Description
Overview	
Avaya Control Manager Overview and Specification	This document describes the features and specifications for the Control Manager product.
Planning	
Planning for an Avaya Control Manager Deployment (formerly known as *Avaya Control Manager Customer Requirements*)	This document describes the planning and prerequisites that customers must follow before deploying Control Manager.
New Installations	
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 - Multiplex High Availability	This document describes how to install, configure, and test an Enterprise Control Manager system that is using Microsoft SQL AlwaysOn for database server high availability and multiple Control Manager application servers for high availability, along with an optional deployment of a software load balancer.
Installing Avaya Control Manager for Enterprise - Legacy High Availability	This document describes how to install, configure, and test a Legacy 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	

Table continues…

Title	Description
Upgrading to Avaya Control Manager 8.1 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 8.1 for Enterprise - Multiplex High Availability	This document describes how to upgrade an Enterprise Control Manager system from an earlier release to a system that is using Microsoft SQL AlwaysOn for database server high availability and multiple Control Manager application servers for high availability, along with an optional deployment of a software load balancer. The document includes upgrade checklist, upgrade procedures, and verification procedures for each supported upgrade path.
Upgrading to Avaya Control Manager 8.1 for Enterprise - Legacy High Availability	This document describes how to upgrade a Legacy 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 8.1 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 one-X® Agent Using Avaya Control Manager	This document describes how to use Control Manager to administer Avaya one-X® Agent.
Administering an Avaya Aura® Experience Portal Sample Application Using Avaya Control Manager	This document describes how to use Control Manager with an Experience Portal.
Administering Avaya Control Manager for Avaya Agent for Desktop	This document describes how to use Control Manager to administer Avaya Agent for Desktop.
Events and Alarms	
Avaya Control Manager Events, Alarms, and Errors Reference	This document describes the SNMP notifications for Control Manager.
Using	

Table continues…

Title	Description
Using Avaya Control Manager Conversation Sphere	This document describes how to use Control Manager Conversation Sphere to administer vectors, strategies, and call flows.
Using Avaya Control Manager Central License and Traffic Tracker	This document describes how to use Control Manager Central License and Traffic Tracker.
Using the Avaya Control Manager SOAP API	This document describes how to use the SOAP version of the Control Manager API.
Using the Avaya Control Manager REST API	This document describes how to use the REST version of the Control Manager API.
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. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select 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**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.

5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or more of the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

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

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://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, and Twitter.
- 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
70920W	Installing Avaya Control Manager
7093W	Upgrading and Supporting Avaya Control Manager for Cloud Service Providers
70940W	Configuring Avaya Control Manager for Enterprise
70950W	Upgrading and Supporting Avaya Control Manager for Enterprise
70910W	Administering Avaya Control Manager for Enterprise
7091T	Administering Avaya Control Manager R8 Online Test

Table continues…

Course code	Course title
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 https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

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

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

Note:

Videos are not available for all products.

Support

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

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

Using the Avaya InSite Knowledge Base

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

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

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

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

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

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Appendix A: Upgrade process for Avaya one-X Agent

Upgrading to Avaya one-X® Agent Release 2.5.13 when upgrading from Control Manager Release 7.1.2.2

About this task

When you are upgrading from Avaya one-X® Agent Release 2.5.8 to Release 2.5.13 when also upgrading from Control Manager Release 7.1.2.2 installed on Microsoft SQL 2008, follow the steps shown in this process to do the upgrades in the correct order.

Most of the procedures shown in this process are found within this document.

Procedure

1. Verify that the Avaya one-X® Agent Release 2.5.8 system is in proper working order.
2. Verify that the Control Manager Release 7.1.2.2 system is in proper working order.
3. Upgrade the Avaya one-X® Agent system to Release 2.5.13.
4. Do a database backup on the Control Manager Release 7.1.2.2 system. For more information, see Backing up Control Manager databases on page 77.
5. Install Microsoft SQL 2012 Server software on a new hardware database server. For more information, see the chapter “Installing prerequisite software”.
6. Restore the backed up databases onto the new Microsoft SQL 2012 server. For more information, see Restoring (migrating) the Control Manager databases on page 79.
7. Install the new Control Manager software on the new Windows 2012 OS server. When installing the new Control Manager software, configure the Control Manager to connect to the new Microsoft SQL 2012 server. For more information, see procedures for installing Control Manager software.

Next steps

Verify that all of the following features are functioning on the new Avaya one-X® Agent Release 2.5.13 system:

- Calls inbound and outbound
- Call transfer
- Conference

- Drag and drop
- IM
- Screen popup
- Directory
- Launch application
- Change AUX state and logout state
- Outlook contacts
- Click to dial on (IE)
- Work handling
- Follow-up
- Change of Avaya one-X® Agent to Control Manager and Control Manager to Avaya one-X® Agent is properly reflected

Index

M

O

P

R

S

T

U

V

W