Installing and Upgrading Guide for Cisco Hosted Collaboration Solution for Contact Center, Release 12.0(1)

First Published: 2019-01-11

Last Modified: 2019-07-04

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Change History

Change	See
Initial Release of the Document for Release 12.5(1)	
Removed prerequisite and modified note in the Section, Before you begin Modified features list	Install Microsoft SQL Server
Added new procedure	Verification of the Downloaded ISO
Updated the procedure	Disable Port Blocking

About this Guide

This document describes how to install the core and shared components, and software for a new Cisco HCS for Contact Center solution, or to upgrade an existing Cisco HCS for Contact Center solution.

Audience

This guide is intended for users who install and upgrade Cisco HCS for Contact Center solution.

This guide assumes that you are already familiar with Cisco Contact Center products. You must acquire the necessary knowledge and experience regarding deployment and management of virtual machines before you deploy components on VMware virtual machines. Therefore, you must have a sound knowledge of the VMware infrastructure.

Cisco HCS for Contact Center is a subset of Core HCS, this document assumes that the HCS infrastructure is ready to set up the contact center. Therefore, components such as UCDM, CUBE Enterprise, and PCA must be installed as part of HCS setup.

Related Docs

Design Considerations and guidelines for deploying a Cisco HCS for Contact Center solution including various components and subsystems. See, https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-implementation-design-guides-list.html

Post-installation procedure for Cisco HCS for Contact Center, See https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices

- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at https://cway.cisco.com/mynotifications.

Documentation Feedback

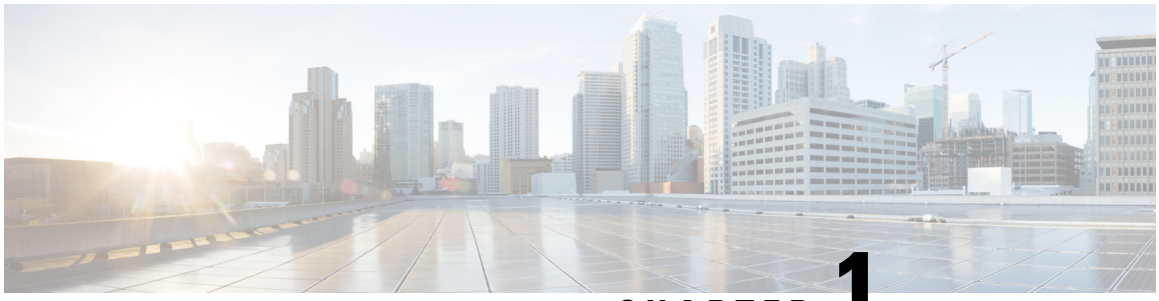
To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems, Inc. </title></html>`
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.



CHAPTER 1

Preparation

Important Consideration

Note By default, Windows Defender is enabled on Windows Server 2016. Windows Server 2016 upgrade will prompt to uninstall the antivirus due to compatibility issue with Windows Defender. To proceed with the upgrade, uninstall the antivirus. For more information on Windows Defender antivirus compatibility, see https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/windows-defender-antivirus-compatibility.

Before proceeding with ICM application installation, ensure that you follow the antivirus guidelines specified in the Section, Antivirus Guidelines of the Security Guide for Cisco Unified ICM/Contact Center Enterprise at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Installation Approach

Cisco HCS for Contact Center service, delivers Cisco Unified Contact Center Enterprise (Unified CCE) in a virtualized environment on Cisco Unified Computing System (UCS).

Cisco HCS for Contact Center offers the same shared management (service fulfillment and assurance) and aggregation (carrier trunks) that is common for all customer instances and used for other Cisco HCS services.

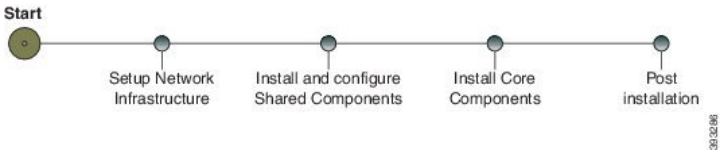
Cisco Core components include, Unified CVP, Unified CCE, Unified Communication Manager, Cisco Finesse, Unified Intelligence Center, CUBE-E. Install the core components using the golden template process as the standard approach.

Install the shared management and aggregation layer that consists of Unified Communication Domain Manager (UCDM), Cisco Unified Contact Center Domain Manager (Unified CCDM), Cisco Prime Collaboration - Assurance (PCA), and Cisco Adaptive Security Appliance (ASA). This combines the Cisco HCS components with multiple network connections and routes requests to a dedicated customer instance.

Install the network infrastructure layer that includes the implementation of UCS platform.

After you install the above, as part of post installation you can configure the customer instances for the supported deployment models. Depending upon your HCS for Contact Center deployment model, you can configure dedicated customer instances of 500, 2000, 4000, 12000, or 24000 agents and shared customer instances of 100 or 500 agents.

The following workflow describes the high-level installation sequence for Cisco HCS for Contact Center.



Related Topics

Shared Component Installation, on page 7
Core Components Installation Approach, on page 45

System Installation Dependencies

The components within each release set are compatible with each other and will interoperate correctly. The overall system may not be operational until you install all components or until you complete the initial configuration or setup.

For Nexus, ASA, and CUBE Enterprise supported release version, see https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html.

For information on all other component hardware and software versions and compatibility, see *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html.

Automation Software

Note Automation software is required for golden templates only.

Software	Version	Download	Notes
GoldenTemplateTool zip file	12.0(1)	Go to https://communities.cisco.com/docs/DOC-31448 https://communities.cisco.com/docs/DOC-35671 Golden Template Tool Click **Download**. Then select HCS for CC deployment scripts. https://communities.cisco.com/docs/DOC-52685 https://communities.cisco.com/docs/DOC-58521 HCS-CC_11.6.1-GoldenTemplateTool.zip	Download and extract the `GoldenTemplateTool.zip` file to run the automation tool. For more information, see *Automated Cloning and OS Customization* section in *Configuring Guide for Cisco HCS for Contact Center* https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.
PowerCLI		http://downloads.vmware.com/	Use PowerCLI to run the automation script.
OVF Tool	32-bit	https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL420&productId=491	
WinImage	8.5 , 32-bit	See http://winimage.com/download.htm. **Note** WinImage is shareware. If you choose to not purchase a licensed copy, you will see pop-ups when you run this tool. Clicking **No** at the pop-ups will allow you to proceed.	WinImage creates a floppy image (.flp file) from the platformConfig.xml file. This file contains parameters for customizing VOS primary and secondary nodes.

Hardware Requirements

HCS for Contact Center supports the following configurations:

For information on the TRC server support for this release, see the *Virtualization for Cisco HCS for Contact Center* guide at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/hcs_cc_virt.html

HyperFlex M5 Support

Cisco HyperFlex HX-Series System provides a unified view of the storage across all nodes of the HyperFlex HX cluster via the HX Data Controller Platform. For optimal performance, it is recommended that all VMs

are mapped to the single unified datastore. This mapping enables the HX Data Platform to optimize storage access based on the workload and other operating parameters.

For more information, see the documentation on Cisco HyperFlex HX Data Platform at https://www.cisco.com/c/en/us/support/hyperconverged-systems/hyperflex-hx-data-platform-software/products-installation-guides-list.html.

For information on installing collaboration software, see the *Cisco Collaboration on Virtual Servers* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Specification Based Hardware Support

Cisco HCS for Contact Center supports specification based hardware, but limits this support only to the UCS B-Series blade hardware. This section provides supported server hardware, component version, and storage configurations.

For more information on specification based hardware such as CPU types, see the*Collaboration Virtualization Hardware* guide at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-hardware.html

Additional Hardware Specification

The following table lists the additional hardware specification for HCS for Contact Center.

Server	Components	Description
Cisco Unified Border Element Enterprise Gateway	CUBE-E	ISR G2 with a combination of TDM and VXML. 29*xx*, 39*xx* series routers.
Cisco Unified SIP Proxy	CUSP	Services Module with Services Ready Engine
Adaptive Security Appliance	ASA	Cisco ASA 55*xx* series For small contact center it should be 5585 or 5580.

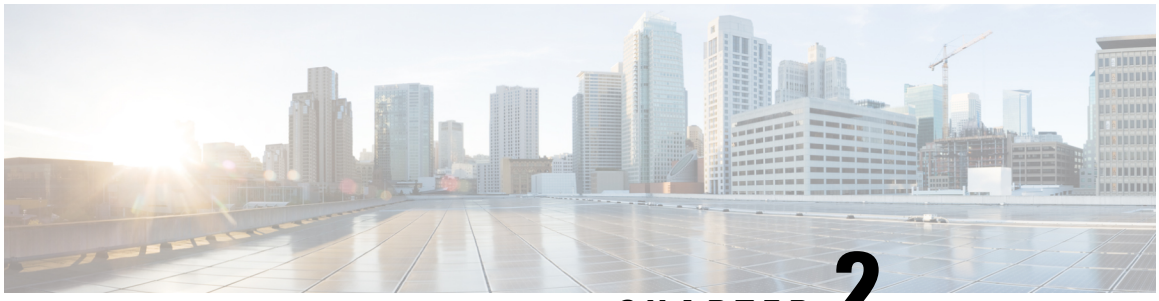
Network Infrastructure

This section provides information on how to setup the network infrastructure for Cisco HCS for Contact Center. This section does not provide detailed installation instructions for individual components installation. For details information on installation, see Cisco Hosted Collaboration Solution, Installation Guide.

- Install and configure the Cisco UCS Server and Cisco UCS Manager.
- Install and configure the SAN Storage.
- Install and configure the MDS Series Switch.

  You can install the MDS Series Switch any time after the Nexus 7000 and 5500 switch.
- Install and configure the vCenter.

- Install and configure the Cisco Nexus 1000V Series Switch.



CHAPTER 2

Shared Component Installation

Configure an Identity Provider (IdP)

To support SSO for the contact center solution, configure an Identity Provider (IdP) that is compliant with the Security Assertion Markup Language 2.0 (SAML v2) Oasis standard. The IdP stores user profiles and provides authentication services to the contact center solution.

Note For a current list of supported Identity Provider products and versions, see the *Contact Center Enterprise Compatibility Matrix*.

This section provides sample configuration information for Microsoft AD FS.

Follow this sequence of tasks to configure the Identity Provider.

Sequence	Task
1	Install and Configure Active Directory Federation Services, on page 7
2	Set Authentication Type. See Authentication Types, on page 8.

Install and Configure Active Directory Federation Services

Follow Microsoft instructions and guidelines to install Microsoft Active Directory Federation Services (AD FS).

For example, see *Active Directory Federation Services Overview* at https://technet.microsoft.com/en-us/library/hh831502(v=ws.11).aspx

- For AD FS in Windows Server (AD FS 3.0), see the *AD FS Content Map* at http://aka.ms/adfscontentmap and *AD FS Technical Reference* at https://technet.microsoft.com/en-us/library/dn303410(v=ws.11).aspx.

Note Cisco IdS does not support AD FS Automatic Certificate Rollover. If the AD FS certificate gets rolled over, then re-establish the trust relationship between the IdS and AD FS.

Authentication Types

Cisco Identity Service supports form-based authentication of the Identity Provider.

For information on enabling form-based authentication in ADFS, see Microsoft documentation:

- For ADFS 3.0 see https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/

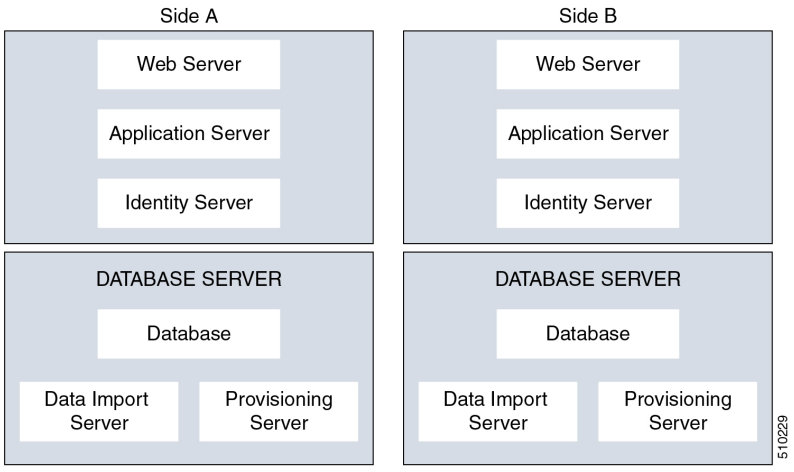
For Kerberos authentication to work, ensure to disable the form-based authentication.

- In AD FS on Windows Server , set the Authentication Type to Forms-based authentication (FBA). Refer to the following Microsoft TechNet article, http://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspx
- In AD FS on Windows Server, set the Authentication Policy to Forms Authentication. Refer to the following Microsoft TechNet article, https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/

Install and Configure Unified CCDM

For Cisco HCS for Contact Center, implement a dual-tier (distributed) system, as shown in the following figure. This system keeps the Web/Application and Identity Components of the Unified CCDM separated from the database server components.

Figure 1: Unified CCDM Dual-Tier Deployment



For dual-sided systems, complete the installation of the Unified CCDM servers on side A, before you begin the installation on side B.

Related Topics

Deploy Unified CCDM Database Server, on page 14
Deploy Unified CCDM Web Server, on page 19
Configure Unified CCDM, on page 22

Common Procedures for Deploying Unified CCDM Servers

Configure Windows

Complete the following procedure to configure Windows on all the Unified CCDM servers.

Related Topics

Configure Windows Feature Requirements, on page 9
Turn off FIPS Compliance, on page 10
Disable UAC, on page 10

Configure Windows Feature Requirements

Procedure

Step 1 Select **Server Manager** > **Manage** > **Add Roles and Features**.

Step 2 On the **Before you begin** page, click **Next**.

Step 3 On the **Select Installation Type** page, select the **Role-based or feature-based installation** option, then click **Next**.

Step 4 On the **Select destination server** page, select the **Select a server from the server pool** option, then click **Next**.

Step 5 On the **Select server roles** page, check the following check boxes:

- Application Server
- Select **File and Storage Services** > **File and iSCSI Services** and check the **File Server** check-box
- Web Server (IIS)

Step 6 Click **Next**.

Step 7 On the **Select features** page, check the **.Net Framework 4.5 Features** check box, then click **Next**.

Step 8 On the **Application server** page, click **Next**.

Step 9 On the **Select role services** page, check the following check boxes:

- .NET Framework 4.5
- COM+ Network Access
- Incoming Network Transactions
- Outgoing Networking Transactions

- TCP Port Sharing
- Web Server (IIS) Support
- Message Queuing Activation
- Named Pipes Activation
- TCP Activation

Step 10 Click **Next**.

Step 11 On the **Web server roles (IIS)** page, click **Next**.

Step 12 On the **Select role services** page, select the required role services, then click **Next**.

Step 13 Click **Specify an alternate source path**, then enter `\sources\sxs` this is available at Microsoft Windows 2016 Installer DVD or ISO. Click **OK**.

Step 14 Click **Install**.

Step 15 After installation, restart the server.

Turn off FIPS Compliance

Procedure

Step 1 Open the **Local Security Policy** application.

Step 2 Open the **Local Policies** folder, and then double-click **Security Options** to view the list of policies.

Step 3 Ensure that you disable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** policy.

Disable UAC

User Account Control (UAC) protects the operating system from malicious programs. When enabled, UAC may cause issues with the software used to install Unified CCDM. Disable UAC on all servers before you install the Unified CCDM. Complete the following procedure to disable UAC.

Procedure

Step 1 Select **Start** > **Control Panel** > **System and Security** > **Action Center** > **Change User Account Control settings**.

Step 2 Set **UAC** to **Never Notify**.

Step 3 Click **OK**.

Step 4 Restart your machine to commit to the new UAC settings.

You have now disabled UAC and are ready to install the Unified CCDM.

Note Re-enable UAC after you complete the Unified CCDM installation.

Associate Unified CCDM Component Servers with Service Provider AD Domain

Complete the following procedure to associate the Unified CCDM Component servers with Service Provider AD Domain.

Procedure

Step 1 Sign in to the machine using a local administrator account.
Step 2 Select **Start** > **Administrative Tools** > **Server Manager**.
Step 3 Select **Local Server** in the left panel and click **WORKGROUP** to change system properties.
Step 4 In the **Computer Name** tab, click **Change**.
Step 5 Select the **Domain** option to change the member from **Workgroup** to **Domain**.
Step 6 Enter the fully qualified Service Provider domain name and click **OK**.
Step 7 In the **Windows Security** pop-up window, validate the domain credentials and click **OK**.
Step 8 After successful authentication, click **OK**.
Step 9 Reboot the server and sign in with domain credentials.

Configure Secondary Drive

DO THIS FOR Virtual Machines that require an additional hard drive to archive data.

Procedure

Step 1 Open **Computer Management**.
Step 2 Expand **Storage** in the left pane, click **Disk Management**.
Step 3 Right-click **Disk 1** and choose **Online**.
Step 4 Right-click **Disk 1** and choose **Initialize Disk**.
Step 5 In Initialize Disk pop up window, under Select disks. Check **Disk 1** and choose **MBR (Master Boot Record)** under **Use the following partition style for the selected disks** pane. Click **OK**.
Step 6 Create a new disk partition as follows: right-click the disk you just initialized, choose **New Simple Volume**, and run the wizard.

Install the Diagnostic Framework for System CLI

Procedure

Step 1 To install the Diagnostic Framework component, start the Unified CCDM Installer, click **Support Tools** and select **Diagnostic Framework**.

The **Domain Manager: Diagnostic Framework Install Shield Wizard** window displays.

Step 2 Click **Next** to go through each window in turn.

Step 3 Accept the license agreement, then click **Next**.

Step 4 In the **Certificate** window, select the type of certificate installed with the Diagnostic Framework.

- **Self Signed:** A new certificate will be generated by the installer. This type of certificate should be used only for lab or test deployments.
- **Trusted Certificate:** An existing certificate, issued by a valid certificate server, will be associated at a later date. This option should be used for production deployments.

Step 5 Click **Next**.

Step 6 In the **wsmadmin Password Information** window, enter and confirm the password for the **wsmadmin** user, which is created to access the Unified System CLI tool. Click **Next**.

Step 7 In the **Ready to Install the Program** window, click **Install**.

Step 8 After installation, click **Finish**.

Step 9 Unmount the ISO image.

Configure SNMP Traps

Simple Network Management Protocol (SNMP) traps may be raised from Unified CCDM by configuring Windows to send selected events to an SNMP monitor. Configure Windows using a Windows utility called evntwin.exe. This utility converts events written to the Windows Event log into SNMP traps that are raised and forwarded by the Windows SNMP service to an SNMP management tool.

To configure SNMP traps for use with Unified CCDM, follow these steps:

- Enable Windows SNMP Feature, on page 12
- Configure SNMP Service for Trap Forwarding, on page 13
- Configure Windows Events to Forward to SNMP, on page 13

Enable Windows SNMP Feature

Enabling the SNMP feature in Windows is required to configure the Windows event forwarding to SNMP. In the Unified CCDM servers, enable the SNMP feature as follows:

Procedure

Step 1 Select **Server Manager** > **Manage** > **Add Roles and Features**.

Step 2 On the **Before you begin** page, click **Next**.

Step 3 On the **Select Installation Type** page, select the **Role-based or feature-based installation** option, then click **Next**.

Step 4 On the **Select destination server** page, select the **Select a server from the server pool** option, then click **Next**.

Step 5 On the **Select server roles** page, click **Next** .

Step 6 On the **Select features** page, check the **SNMP Service** . Check the **SNMP WMI Provider** check box, then click **Next**.

Step 7 Click **Install** to complete the SNMP deployment.

Step 8 Close the **Server Manager** application.

Configure SNMP Service for Trap Forwarding

Configure the SNMP service to forward traps to the management tool, which is used to report and alert.

Procedure

Step 1 In the MMC console, select **Files > Add/Remove Snap-in...**

Step 2 From the **Available Snap-ins** list, select **Services** and click **Add**.

Step 3 In the **Services** dialog box, select **Local computer** and click **Finish**.

Step 4 Click **OK**.
The **Services(Local)** node will be added to the **Console Root** node.

Step 5 Select **Services(Local)** and in the **Services(Local)** tab that is displayed, right-click **SNMP Services** and then select **Properties**.
The **SNMP Service Properties** dialog box is displayed.

Step 6 In the **Traps** tab, in the **Community Name** field, enter **`public`**, then click **Add to list**.

Step 7 Click **Add**.

Step 8 In the **SNMP Service Configuration** dialog box, enter the hostname or IP address of the system, which receives the trap information—The server hosting the management agents or reporting and alerting tools. Click **Add** to add the trap destination.

Step 9 If there is more than one system, it is required to receive the trap information, configure SNMP services for the trap forwarding on all systems.

Step 10 Click **OK**.

Configure Windows Events to Forward to SNMP

Finally, use the `evntwin.exe` tool to configure the Windows events to be forwarded as SNMP traps. Any event that is raised in the Windows Event Log may be configured to generate an SNMP trap.

Procedure

Step 1 In the **Run** command, enter **`evntwin.exe`**.

Step 2 Select **Custom**, then click **Edit**.

Step 3 In the **Event Sources** list, expand the **Application** source to see the available Unified CCDM events. The Unified CCDM events and their uses are listed in the following table.

Event Source	Description
Unified CCDM Application Server Monitoring	The core monitoring service for the application server—This posts connection change events to the event log.
Unified CCDM Data Import Server Monitoring	The data import service used for importing data from CCE etc.
Unified CCDM Partition Table Manager Monitoring	Connection monitoring for the partition manager service, which creates partitioning tables in the database.
Unified CCDM Provisioning Server Monitoring	Service used for provisioning changes on remote equipment, for example, CCE etc.
Unified CCDM Partition Table Manager	Core application service to create partitioning tables in the database.
X_ANALYTICALDATA, X_HIERARCHY, X_IMPORTER etc.	Individual services configured in Windows for Unified CCDM—These can be used for subscribing to standard service events. For example, start/stop events etc.

Step 4 Configure an event source for generating SNMP traps, select the event source, wait a few moments, then click **Add** once it is enabled. In the **Properties** window, specify the required trap properties, then click **OK**.

Step 5 After setting the required SNMP traps, click **Apply**.

Deploy Unified CCDM Database Server

Follow the procedure to install the Unified CCDM database server on side A and side B.

Before you begin

Download the OVA files. Use `UCCDM_12.0_Win2012R2_vm11_v1.0.ova` to create the golden template.

Create a naming convention for the Unified CCDM Web server, as the hostname of the Unified CCDM Web server is required to install and configure the Unified CCDM Database server.

Note Do not use hyphens in the server name.

Procedure

Step 1 Create Virtual Machine for the Unified CCDM Database server.

Step 2 Install Microsoft Windows server.

Step 3 Configure Windows.

Step 4 Associate Unified CCDM component servers with the service provider AD domain.

Step 5 Configure secondary drive.

Step 6 Install Microsoft SQL server.

Step 7 Configure Distributed Transaction Coordinator (DTC).

Step 8 Configure Windows Server Firewall for SQL Server.

Step 9 Install SQL Server Management Studio.

Step 10 Install the Unified CCDM Database server.

Note Before installing the Unified CCDM Database server on side B, install the Unified CCDM Web server on side A.

Step 11 Add SQL sign-in for the Unified CCDM Web server.

Step 12 Install the Unified CCDM Portal Database.

Step 13 Install the diagnostic framework for the system CLI.

Step 14 Configure SNMP traps.

Note
- Back up the SQL Server databases regularly and truncate the transaction logs to prevent them from becoming excessively large.
- Schedule backups when there is no user activity.

Related Topics

Create Virtual Machines, on page 59
Install Microsoft Windows Server
Configure Windows , on page 9
Associate Unified CCDM Component Servers with Service Provider AD Domain, on page 11
Configure Secondary Drive, on page 11
Install Microsoft SQL Server
Configure DTC, on page 16
Configure Windows Server Firewall for SQL Server, on page 16
Install Unified CCDM Database Server, on page 16
Add SQL Login for Unified CCDM Web Server, on page 19
Install Unified CCDM Portal Database, on page 17
Install the Diagnostic Framework for System CLI , on page 12
Configure SNMP Traps, on page 12

Procedures for Deploying Unified CCDM Data Server

Configure DTC

Procedure

Step 1 Open the **Component Services** application.

Step 2 Expand **Component Services** > **Computers** > **My Computer** > **Distributed Transaction Coordinator**.

Step 3 Right click **Local DTC** and select **Properties**.

Step 4 Select the **Security** tab.

Step 5 In the **Security** tab, configure:

a) Ensure that **Security Settings** has **Network DTC Access** checked, and **Transaction Manager Communication** has **Allow Inbound** and **Allow Outbound** checked.

b) Set the **Transaction Manager Communication** to **No Authentication Required**.

c) Click **OK**.

Configure Windows Server Firewall for SQL Server

Procedure

Step 1 Open the **Server Manager** application.

Step 2 Select **Tools** > **Windows Firewall with Advanced Security** and click **Inbound Rules**.

Step 3 In the **Actions** pane, click **New Rule**.

Step 4 Select **Port** as the rule type and click **Next**.

Step 5 Select **TCP** as the protocol and enter `1433` as the specific local ports, then **Next**.

Step 6 Select `Allow the connection`. Click **Next**.

Step 7 Select the profile options that are appropriate to your deployment and click **Next**.

Step 8 Enter a name for the rule and click **Finish** to create the rule.

Install Unified CCDM Database Server

Procedure

Step 1 Mount the Unified CCDM ISO image to the virtual machine.

Step 2 Double-click the ISO image.

Step 3 In the **Cisco Unified CCDM Installation** window, from the **Server Installation** list, select the **Database server** component.
System runs the prerequisite check.

Step 4 Ensure all the prerequisites are checked. After the prerequisite check, click **Install**.

Step 5 In the **Domain Manager: Database Components - InstallShield wizard** window, click **Next**.

Step 6 Accept the license agreement, then click **Next**.

Step 7 In the **Cryptography Configuration** window, enter and confirm the passphrase using 6 to 35 characters, then click **Next**.

This passphrase encrypts system passwords and must be identical across all servers within a cluster. Enter the same password in the **Confirm Passphrase** field.

Step 8 In the **Configure Database** window, configure:

a) In the **Catalog** field, enter the name of the Unified CCDM database catalog. The default catalog name is Portal.

b) In the **Authentication** field, select the authentication mode to connect to the Unified CCDM database.

- **Windows Authentication** - This is the default authentication mode.
- **SQL Authentication** - Select this option only if you are using a database server on a different domain. For this option, enter the SQL Server Username and Password.

c) Click **Next**.

Step 9 In the **Destination Folder** window, accept the default location to install the database server, then click **Next**.

Step 10 In the **Ready to Install Program** window, click **Install**.

Step 11 After the installation, uncheck the **Launch Database Management Utility** check box. You can manually set up the database, later.

Step 12 Click **Finish**.

Note Repeat the steps to set up the Unified CCDM Database server on Side B.

Install Unified CCDM Portal Database

Complete the following procedure to set up the database server:

Procedure

Step 1 Open **Database Installer**.

Step 2 On the **Database Setup** page, click **Next**.

Step 3 From the **Database setup** page, select **Install a new database**.

Step 4 Click **Next**.

Step 5 On the **SQL Server Connection Details** page, enter:

a) In the **Server Name** field, enter the name of the Unified CCDM database server. The default server name is Local.

b) From the **Database Name** drop-down list, enter the name of the Unified CCDM database catalog. The default database name is Portal.

c) In the **Authentication** field, select the authentication mode to connect to the Unified CCDM database.

- **Windows Authentication** - This is the default authentication mode.

- **SQL Authentication** - Select this option only if you are using a database server on a different domain. For this option, enter the SQL Server Username and Password.

d) Click **Next**.

Step 6 Click **Test Connection** to ensure the connection is established to the SQL Server, then click **OK**.

Step 7 Click **Next**.

Step 8 In the **Optimize System Databases** window, then click **Next**.

Step 9 For installation of the portal database server on Side B, check the **Replicated Configuration** check box.

a) In the **Setup Replication** window, select **Replicated Configuration** and enter:

- In the **Share Name** field, enter the name. The default share name is **ReplData Folder**.
- In the **Folder Path** field, enter the path. The default path is `C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\repldata`.

b) Click **Next**.

Step 10 In the **Configure the Location of Data Files** window, for non-customized installation of SQL Server, accept the defaults and click **Next**. For the custom installation of SQL Server, configure the data files:

a) Check the file group or file groups check box which you want to change.
b) Browse the file group or file groups location.
c) Enter the size for the selected file group or file groups.

Note Uncheck the **Set Initial Size to Max Size** check box to specify the initial size.

d) Click **Update**.
e) Click **Default** to restore all file groups to default settings.
f) Click **Next**.

Step 11 In the **Configure Local Administrator Details** window. Enter the password and confirm, then click **Next**.

Note You cannot retrieve or reset the password.

Step 12 In the **Configure SQL Server Agent Service Identity** window, configure:

a) In the **Account Type** field, enter the user account type. For a distributed installation, this must be a domain user account.
b) In the **User Name** field, enter the user name. The default username is **sql_agent_user**.
c) Optional, for a single sided single server system, check the **Automatically create the user account if missing** check box to automatically create a local user.
d) Enter and confirm the password.

Ensure that the password meets the system's complexity requirements.

e) Click **Next**.

- **User Name** - Enter the name of the user account. Default value is sql_agent_user. If you selected the Account Type as Domain, enter the domain user account name instead. If you have specified a domain user, you will need to prefix the user name with the domain name, followed by a backslash.
-

Step 13 In the **Configure the Location of the Identity Database Data Files** window, check all the file group check boxes to set the location, then click **Next**.

Step 14 In Ready to Install the database page, Click **Next**.

Step 15 Click **Close**.

Step 16 Start the following Unified CCDM services under the Windows services:

- CCDM: Data Import Server
- CCDM: Partition Table Manager
- CCDM: Provisioning Server

Step 17 Repeat the steps to set up database for Unified CCDM Data Server on Side B.

Add SQL Login for Unified CCDM Web Server

In distributed deployment, create SQL logins to establish connection between the Unified CCDM web server and data server.

Procedure

Step 1 Log in to the Cisco Unified CCDM database server using domain administrator credentials.

Step 2 Open the **SQL Server Management Studio** window.

Step 3 Select **Security** > **Logins**.

Step 4 Right-click the **Logins** option and click **New Logins**.

Step 5 To add SQL logins for Side A and Side B Unified CCDM web servers, configure the following settings on the **General** page:

a) In the **Login Name** field, enter the machine name. The default name is **<DOMAIN>\<Unified CCDM-WEB SERVER HOSTNAME>$**.

b) Select the **Windows Authentication** unless you are connecting to a server on another domain.

c) Set the **Default language** to **English**.

Step 6 On the **Server Roles** page, check the **public** and **sysadmin** check boxes.

Step 7 On the **User Mapping** page, configure the settings:

a) From the **Users Mapped to this Login** options, check the **Portal** and **IdSvr3Config** check boxes.

b) From the **Database role membership for Portal** options, check the **portalapp_role**, **portalreporting_role**, **portalrs_role**, and **public** check boxes to grant the portal login credentials.

c) From the **Database role membership for IdSvr3Config** options, check the **db_owner** and **public** check boxes.

Step 8 Click **OK**.

Step 9 Repeat the steps to add SQL login for the Unified CCDM Web Servers for Side B.

Deploy Unified CCDM Web Server

Follow the procedure to install the Unified CCDM Web server on side A and side B.

Before you begin

Download the OVA files. Use `UCCDM_12.0_Win2012R2_vm11_v1.0.ova` to create the golden template.

Note Do not use hyphens in the server name.

Procedure

Step 1 Create Virtual Machine for the Unified CCDM Web server.

Step 2 Install Microsoft Windows Server.

Step 3 Configure Windows.

Step 4 Associate Unified CCDM component servers to respective service provider AD domain.

Step 5 Configure the secondary drive.

Step 6 Install the Unified CCDM Web server.

Note Before installing Unified CCDM Web server on Side B, install the Unified CCDM Data server on Side B.

Step 7 Install the Unified CCDM Identity server on the Web server.

Note Before installing Unified CCDM Identity Server, install the Unified CCDM Web Server and Data server.

Step 8 Install the diagnostic framework for the system CLI.

Step 9 Configure SNMP traps.

Related Topics

Create Virtual Machines, on page 59
Install Microsoft Windows Server
Configure Windows , on page 9
Associate Unified CCDM Component Servers with Service Provider AD Domain, on page 11
Configure Secondary Drive, on page 11
Install Unified CCDM Web Server, on page 20
Install CCDM Identity Server on Web Server, on page 21
Install the Diagnostic Framework for System CLI , on page 12
Configure SNMP Traps, on page 12

Install Unified CCDM Web Server

Complete the following procedure to install the App or Web server component:

Before you begin

Complete the Unified CCDM Data server installation.

Procedure

Step 1 Mount the Unified CCDM ISO image to the virtual machine.

Step 2 Double-click the ISO image.

Step 3 In the **Cisco Unified CCDM Installation** window, select **App/Web Server** and wait until it completes all prerequisite checks, then click **Install**.

Step 4 In the **Domain Manager: Application Server Components - IntsallShield Wizard** window, click **Next**.

Step 5 Accept the license agreement, then click **Next**.

Step 6 In the **Cryptography Configuration** window, enter and confirm the passphrase using 6 to 35 characters, then click **Next**.

This passphrase encrypts system passwords and must be identical across all servers within a cluster. Enter the same password in the **Confirm Passphrase** field.

Step 7 In the **Destination Folder** field, retain the default location, then click **Next**.

Step 8 In the **Configure Database** window:

a) In the **SQLServer Name** field, enter the Side A database server hostname. The default option is valid only for the All-in-One deployment type.

Note When you install the app or web server on Side B, enter the Side B database server hostname.

b) From the **Catalog Name** list, select the name that is used while installing the Database Server component. The default value is Portal.

c) In the **Connect Using** pane, select the appropriate sign-in option:

- **Windows authentication** - This is a default option.
- **SQL Server authentication** - Select this option only if you are using a database catalog on a different domain.

Note For this option, enter the SQL Server Username and Password.

Step 9 In the **Ready to Install the Program** window, click **Install**. When the installation completes, click **Finish**.

Step 10 Click **Yes** to restart your system for the changes to take effect.

Note In a dual-sided Unified CCDM deployment, repeat this installation for side B replication. Before installing side B, complete the side A installation for all the components.

Install CCDM Identity Server on Web Server

Complete the following procedure to install the Identity server on CCDM App or Web Server.

Procedure

Step 1 In the **Cisco Unified CCDM Installation** window, select **Identity Server** and wait for the prerequisite checks, click **Install**.

Step 2 In the **Identity Server setup Wizard** window, click **Next**.

Step 3 Accept the license agreement, then click **Next**.

Step 4 In the **Destination Folder** field, retain the default location for the Identity Server Installation, then click **Next**.

Step 5 Click **Finish**.

Configure Unified CCDM

Unified CCDM cluster configuration is to establish the communications channel between different Unified CCDM components. This configuration helps each Unified CCDM component to connect to the appropriate channels during failure.

Procedure

Step 1 Launch the Integrated Configuration Environment.

Step 2 Set up Unified CCDM Servers.

Step 3 Configure Replication.

Step 4 Obtain Digital Certificates.

Step 5 Log into Unified CCDM.

Related Topics

Obtain Digital Certificate , on page 25
Login to Unified CCDM, on page 28

Procedures for Configuring Unified CCDM

Launch the Integrated Configuration Environment

Complete the following procedure to launch the Integrated Configuration Environment (ICE) in the Unified CCDM data server.

Procedure

Step 1 Open the **Integrated Configuration Environment** application.

Step 2 On the **Database Connection** page, enter:

a) The **Server Name** field default value is **current machine**.
b) In the **Database Name** field, accept the default value (Portal).
c) In the **Authentication** field, accept the default value.

Step 3 Click **Test** to test the connection to the database server for the first time. If the test fails, check the **Database Connection** settings.

Step 4 Click **OK** to open the ICE.

When ICE starts, the Cluster Configuration tool is the default tool. You can use the **Tool** drop-down list in the toolbar to switch to other ICE tools.

Set up Unified CCDM Servers

Complete the following procedure to set up Unified CCDM servers.

Procedure

Step 1 Open the **Integrated Configuration Environment** application.

Step 2 In the **Select Deployment Type** window, select the **Two Tier** option, then click **Next**.

Step 3 In the **Configure Redundancy** window, select **Dual-Sided system**, then click **Next**.

Step 4 For the two-tier deployment, enter the number of web servers for each side. For dual-sided configurations, configure the equal number of app or web servers for each side of the system, then click **Next**.

Step 5 In the **Configure Servers** window, enter:

a) In the **Primary Server** pane, enter the name and IP address of the primary database server.

b) In the **Secondary Server** pane, enter the name and IP address of the secondary database server, then click **Next**.

Step 6 In the **Configure Application Servers (1)** window, enter:

a) In the **Primary Server** pane, enter the name, IP address, and FQDN of the primary web server.

b) In the **Secondary Server** pane, enter the name, IP address, and FQDN of the secondary web server, then click **Next**.

Note Enter the FQDN in lowercase.

Step 7 In the **Configure Database Connection** window, enter:

a) In the **Catalog** field, enter the name of the Unified CCDM Relational database. The default catalog name is Portal.

b) In the **Authentication** field, select the authentication mode to connect to the Unified CCDM relational database.

- **Windows Authentication** - This is the default authentication mode.
- **SQL Authentication** - Select this option only if you are using a database server on a different domain. Enter the SQL Server username and password.

Step 8 Click **Next**.

Step 9 Optional, click **Print** to print the deployment summary.

Step 10 Verify deployment details, then click **Next**.

Displays a confirmation message.

Step 11 Click **Exit**.

Step 12 Click **Save**.

Configure Replication

Procedure

Step 1 Launch the Integrated Configuration Environment for Unified CCDM Database Server.

Step 2 From the **Tool** drop-down list, select **Replication Manager**.

The dual-sided Unified CCDM deployment, Replication Manager helps to replicate SQL Servers between Unified CCDM databases.

Step 3 Set up SQL Server replication for the Unified CCDM databases.

Step 4 Monitor the general health of SQL Server replication between Unified CCDM databases.

Setup

Procedure

Step 1 Click the **Setup** tab to see the replication setup details and configure or disable replication.

Step 2 In the **CCDM Database Server Properties** pane, check the **Identity Database Replication Enabled** check-box.

Step 3 In the **Distributor Properties** pane, retain the default values.

Note The distributor is created on the Unified CCDM Database Subscriber Server.

Step 4 Click **Configure** to start the replication process.

Note After replication, all the options are dimmed except **Disable**.

Monitor

The Monitor option monitors the general health of SQL Server Replication between Unified CCDM databases. The monitor can also start or stop various replication agents. This option shows the agent details only if SQL Server Replication is currently configured.

Procedure

Step 1 Click the **Monitor** tab.

Step 2 After Unified CCDM replication, top-left pane shows a list of **Publishers** and their publications.

Step 3 Select the **Publication** to see **Subscriptions** or **Agents** details.
The **Agents** tab lists **Snapshot Agent**, **Log Reader Agent**, and **Queue Reader Agent** that are available for the selected publication.

Step 4 In the **Sessions in the 24 Hours** pane, you can see the session details of the subscriptions or agents.

Step 5 In the **Actions in selected session** pane, shows the actions during the selected session and also provides the information about the agent's failure.

Note You can start or stop the replication agents, select the **Agents** tab, right-click on the status of the agent and select **Start** or **Stop**.

Configuring SSL for Unified CCDM

Follow these steps, to configure SSL for the Unified CCDM web application:

Sequence	Task
1	Obtain Digital Certificate , on page 25
2	Export the Certificate in PFX Format , on page 27
3	Configure SSL for the Web Application, on page 27

Obtain Digital Certificate

You can obtain a digital certificate in one of the following ways:

- purchase from an external certificate authority, for public use
- generate internally, for secure use within the issuing organization

Note Use a digital certificate with a key length of at least 2048 bits. Some recent browsers may reject certificates with shorted key lengths.

If you do not already have a suitable certificate, you can request or generate one as follows:

1. Open **Internet Information Services (IIS) Manager** and select the web server in the folder hierarchy.
2. Select the **Features View** tab, and in the IIS group, click **Server Certificates**.
3. Create a internal or external digital certificate.

Note The Common Name is the application domain name. Ensure that you enter the Common Name exactly as it is specified. The Common Name is derived as follows:

- For deployments with a registered address (including load-balanced deployments): enter the registered address, starting from www. For example, if your registered address is `https://www.Unified CCDM.com`, enter `www.Unified CCDM.com`.
- For deployments with a single internal address (including load-balanced deployments): enter the part of the address after https://. For example, if your internal address is `https://UnifiedCCDM.intranet.local`, enter `Unified CCDM.intranet.local`
- For deployments where the web servers will be accessed directly with no load-balancing: enter the fully qualified domain name of the server being configured. For example, `webserver1.mydomain.com`.

Related Topics

Request an External Certificate , on page 26
Generate an Internal Certificate, on page 26

Request an External Certificate

Procedure

Step 1 In the **Actions** pane, select **Create Certificate Request** to display the **Request Certificate** dialog box.

Step 2 In the **Common Name** field, enter the application domain name as defined above.

Step 3 Complete the other fields as appropriate, and click **Next**.

Step 4 In the **Cryptographic Service Provider Properties** dialog box leave the default **Cryptographic Service Provider**.

Step 5 Select a bit length of at least 2048. Click **Next**.

Step 6 Specify a file name for the certificate, and then click **Finish**.

Step 7 When you receive the certificate from the certificate authority, repeat step 1 and step 2 above to show the Server Certificates and Action panes, and in the **Action** pane, select **Complete Certificate Request**.

Step 8 Enter the file name of the certificate, and a friendly name of your choice and click **OK**.

Generate an Internal Certificate

Procedure

Step 1 Select **Create Domain Certificate** in the **Actions** pane to display the **Distinguished Name Properties** dialog box.

Step 2 In the **Common Name** field, enter the application domain name as defined above.

Step 3 Complete the other fields as appropriate, and click **Next**.

Step 4 In the **Online Certification Authority** dialog box specify the **Online Authority** and a friendly name.

Step 5 Click **Finish**.

Export the Certificate in PFX Format

Procedure

Step 1 In IIS Manager, select the **Features View** tab, and in the IIS group, click on **Server Certificates**.

Step 2 Select the certificate in the **Actions** pane and click **Export**.

Step 3 In the **Export Certificate** dialog box, do the following:

a) Enter a file name in the **Export to** field or click **Browse** to select the folder in which you want the exported certificate stored.

b) If you want to protect the exported certificate with a password, enter a password in the **Password** field.

c) Click **OK**.

The certificate is exported as a PFX file.

Configure SSL for the Web Application

Procedure

Step 1 In a web browser, navigate to `https://<web-address>/SSLConfig`, where `<web-address>` is the web address of your Unified CCDM deployment.

Example:

For example, if your web address is `https://Unified CCDM.intranet.local`, enter `https://UnifiedCCDM.intranet.local/SSLConfig`.

Step 2 In the **Authentication** dialog box, enter the user name and password of a Windows domain user with administrator rights on the domain.

Step 3 On the **SSL Certificate Configuration** page, click **Choose File** and browse to the PFX file you created in the previous section. Click **Open** to select the file.

Step 4 If the PFX file is password-protected, enter the password in **Password** field. If not, leave **Password** field empty.

Step 5 Click **Upload** to start the SSL configuration.

When the SSL configuration is complete, the following message is shown:

```
SSL Configuration Complete.
```

Login to Unified CCDM

Procedure

Step 1 To access the Unified CCDM portal, enter *https://<webserver FQDN>/Portal* in browser.
This displays the **Unified CCDM** web page.

Step 2 To sign in to a new system, use **`Administrator`**' as the username and enter the password you entered when you installed Unified CCDM.

Related Topics

Procedures for Configuring Unified CCDM, on page 22

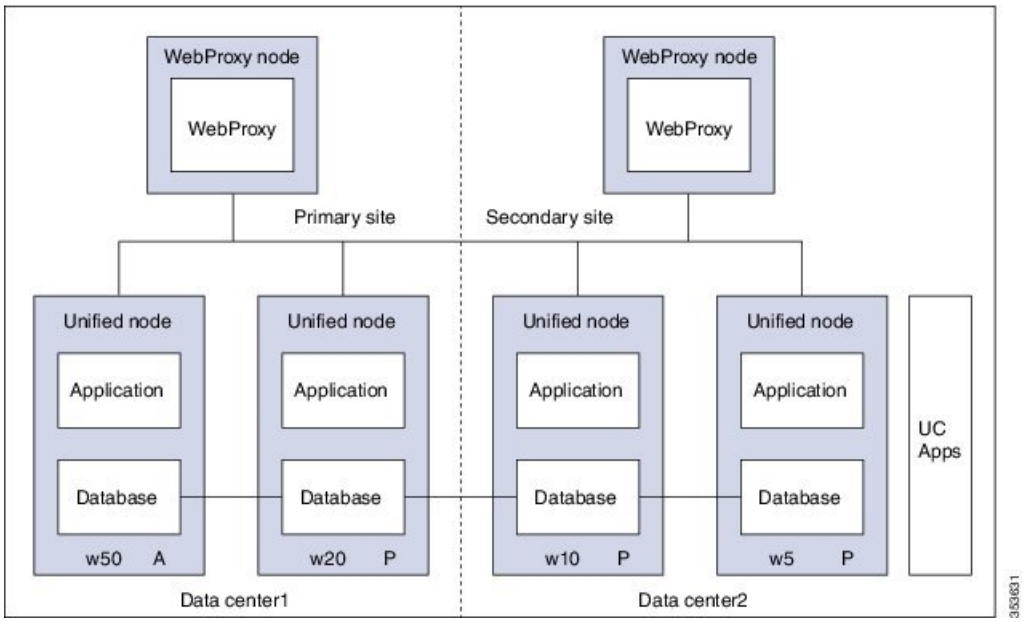
Install and Configure Unified Communication Domain Manager

Cisco HCS for Contact Center, implements the VOS-based—Unified Communication Domain Manager multinode deployment. In this deployment, install four (or more) Unified instances and two (or more) WebProxy instances. These instances are clustered and split over two different geographical locations to provide high availability and disaster recovery.

- A WebProxy role installs only the front-end web server together with an ability to distribute load among multiple middleware nodes.
- A Unified node comprises of application and database roles on a single node.
- WebProxy and Unified nodes can be contained in separate firewalled networks.
- Database synchronization takes places between all database roles, therefore it provides disaster recovery and high availability.
- All nodes in the cluster are active.

Following figure shows the multinode implementation of the Unified Communication Domain Manager:

Figure 2: Graphical Representation of Geo-Redundant Cluster



The functional roles of each node are:

- **WebProxy:** It does load balancing across multiple application roles.
- **Application:** It is a transactional business logic.
- **Database:** It is a persistent data store.

Related Topics

Multinode Installation, on page 29

Multinode Cluster Hardware Specifications

For information about implementing virtual machines within the HCS solution, see Cisco HCS Virtual Machine Requirements.

Multinode Installation

Install a multinode consisting of either four or six Unified instances of and two WebProxy instances.

- A WebProxy node installs only the front-end web server, with the ability to distribute load among multiple middleware nodes.
- A Unified node consists of the Application and Database roles on one node. For geo-redundancy, there are two or four Unified nodes in the Primary Site and two Unified nodes in the Disaster Recovery (DR) Site in active-active setup.

  Cisco Hosted Collaboration Solution supports three configurations of Cisco Unified Communications Domain Manager 10.x+. These configurations provide the service provider with options for scale and Geo-Redundancy support.

Configuration	Number of Unified Nodes	Number of Proxy Nodes	Supported Scale (# Subscribers)	Geo-Redundancy (Y/N)
Standalone CUCDM	1	0	20,000	NA
Multi-Node CUCDM (across Data Centers)	4	2	200,000	Yes (Active-Active)
	6	2	200,000	Yes (Active-Passive)
Multi-Node CUCDM (One Data Center)	4	2	200,000	No

Note

- For geo-redundant Multinode Cluster deployment with six Unified Nodes, there are four Unified nodes in the Primary Site and two Unified nodes in the Disaster Recovery (DR) Site in active-standby setup.
- Installation of the template and upgrade takes approximately two hours. You can follow the progress on the GUI transaction list.

Before you begin

If you received the product on DVD, extract the Unified CDM ISO to get the platform-install ISO and the Unified CDM template file.

If you selected electronic software delivery, use the link that you received to download the product ISO file. Mount the Unified CDM ISO to get the platform-install ISO and the Unified CDM template file.

Optionally, download or extract language pack template files to support languages other than English.

Procedure

Step 1 Install the WebProxy instances.

For each WebProxy instance, create a new VM using the platform-install OVA. Use the instructions shown in Create Virtual Machines from OVA Files, on page 33. For role, select **(3) WebProxy**. Specify the appropriate data center (Primary/DR site) for each WebProxy instance.

Step 2 Install the Unified instances.

For each Unified instance, create a new VM using the platform-install OVA. Use the instructions shown in Create Virtual Machines from OVA Files, on page 33. For role, select **(2) Unified**. Specify the appropriate data center (Primary/DR Site) for each Unified instance.

The following Unified nodes are required in the cluster:

- One Unified node as the Primary node at the Primary site
- One Unified node as the Secondary node at the Primary site

Note For six Unified Node Multi Cluster deployment there are three Unified node as the Secondary node at the Primary site

- Two Unified nodes as the Secondary nodes at the DR site

Step 3 Prepare each node to be added to the cluster. On each WebProxy and Unified node, except for the primary Unified node, run the **cluster prepnode** command.

Step 4 Add nodes to the cluster.

a) Log in to the primary Unified node.
b) Add the Unified and WebProxy nodes to the cluster with the **cluster add <ip_addr>** command.
c) Verify the list of nodes in the cluster with the **cluster list** command.

Step 5 Add the network domain.

a) Configure the domain with the **cluster run all network domain <domain_name>** command.
b) Verify the configured network domain with the **cluster run all network domain** command.
Each node shows the domain that you configured.
c) Verify the DNS configuration with the **cluster run all network dns** command.
Each node responds with the DNS server address.
d) Attempt to contact each node in the cluster with the **cluster run all diag ping <hostname>** command.
e) (Optional) Shut down all the nodes with the **cluster run all system shutdown** command. Take a snapshot of each node. Restart each node.

Step 6 Determine whether security updates are required by running the **cluster run all security check** command on each cluster.

Step 7 If at least one update is required for any cluster, run the **cluster run all security update** command on every cluster.

Step 8 Install VMware tools on each node.

a) In vSphere, right-click the name of the appropriate VM.
b) Select **Guest** > **Install/Upgrade VMware Tools**.

If you are prompted to disconnect the mounted CD-ROM, click **Yes**.

c) Log in to each node and run the **app install vmware** command.

Step 9 Configure the cluster.

a) Provide a weight for each database server with the **database weight add <database_ip> <priority>** command.

Use weights of 40, 30, 20, and 10 for the four Unified nodes and weights of 60, 50, 40, 30, 20, and 10 for the six Unified nodes. The higher the value, the more priority.

For Multinode Cluster deployment with four Unified Nodes in a geo-redundant system containing two data center infrastructures in two physical locations the following weights are used:

- Specify a weight of 40 for the Primary node at the Primary site
- Specify a weight of 30 for the Secondary node at the Primary site
- Specify weights of 20 and 10 for the Secondary nodes at the DR site

For Multinode Cluster deployment with six Unified Nodes in a geo-redundant system containing two data center infrastructures in two physical locations the following weights are used:

- Specify a weight of 60 for the Primary node at the Primary site
- Specify a weight of 50 for the Secondary node at the Primary site
- Specify a weight of 40 for the Secondary node at the Primary site
- Specify a weight of 30 for the Secondary node at the Primary site
- Specify weights of 20 and 10 for the Secondary nodes at the DR site

Note For information on web weight used for Web Proxy node, refer *Cisco Unified Communications Domain Manager Best Practices Guide*.

b) Select a Primary Unified node and set it up as the Primary Unified node with the following command: **cluster provision primary <IP address of primary database node>**.

Allow approximately 2 hours for the operation to complete for two WebProxy and four Unified nodes.

If no primary node exists, you are prompted to select a node to be the primary node.

c) When provisioning is complete, verify the status of the cluster with the **cluster status** command.

If a service is down, run the **cluster run <node_ip> app start** command to restart the service.

d) (Optional) If required, set the web weights configurations (Active-Active, Active-Standby, Standalone). From the primary Unified node, run the required web weight commands for the Web Proxy nodes. See Multi Data Center Deployments in the *Cisco Unified Communications Domain Manager Best Practices Guide* for detailed information.

e) (Optional) If required, enable or disable Self-service or admin web services on the web proxy nodes. This may be required for security purposes.The commands must be run on the relevant web proxy node. It is not advisable to run the commands on a standalone system, but only on a cluster. The commands will automatically reconfigure and restart the nginx process, which results in some downtime. Request URLs to a disabled service will redirect the user to the active service.

- To disable or enable admin or Self-service web services on the web proxy node: use **web service disable <selfservice|admin>** or **web service enable <selfservice|admin>** command.
- To list web services on the web proxy node: use the **web service list** command.

f) (Optional) Shut down all the nodes gracefully, snapshot and restart:

1. From the selected primary Unified node, run **cluster run notme system shutdown**.
2. From the selected primary Unified node, run **system shutdown**.
3. Take a VMWare snapshot of each node and then remove any previous snapshot.
4. Restart each node.

Step 10 Initialize the database and clear all data with the **voss cleardown** command on the primary database node.

Step 11 Import the template.

a) Copy the template file to the primary Unified node with the **scp <template_file> platform@<unified_node_ip_address>:media** command.

b) Log in to the primary Unified node and import the template with the **app template media/<template_file>** command.

The following message appears: `Services have been restarted. Please ignore any other messages to restart services.` The template upgrade automatically restarts necessary applications.

c) When prompted to set the sysadmin password, provide and confirm a password.
d) When prompted to set the hcsadmin password, provide and confirm a password.

Step 12 (For Cisco Unified CDM 10.6(1) only) Install the Macro_Update.template file on secondary Unified nodes.

a) Upload the new Macro_Update.template file to the `media` directory on the Unified CDM server via SFTP.

1. From the VM console, enter **sftp platform@<cucdm10 hostname>**.
2. Enter **cd media**.
3. Enter **put Macro_Update_xx.template**.

b) Enter the following command: **app template media/Macro_Update_xx.template**.
The template installs on each secondary node in less than a minute.

Step 13 (Optional) Install language templates for languages other than English.

a) Copy the language template file to any Unified node with the **scp <language_template_file> platform@<unified_node_ip_address>:./media** command.
b) Log in to the Unified node and install the template with the **app template media/<language_template_file>** command.

Example:

For example, to install French, `app template media/CUCDMLanguagePack_fr-fr.template`.

Create Virtual Machines from OVA Files

You can import the OVA file into VMware vCenter Server. One OVA file is used to deploy all the functional roles. You choose the specific role when the installation wizard is run.

Procedure

Step 1 Sign in to vSphere to access the ESXi Host.
Step 2 Choose **File > Deploy OVF Template**.
Step 3 Choose **Source**, browse to the location of the .ova file, and click **Next**.
Step 4 On the Name and Location page, enter a Name for this server.
Step 5 Choose the resource pool in which to locate the VM.
Step 6 Choose the data store you want to use to deploy the new VM.
Step 7 On the **Disk Format** page, choose **Thick provisioned Eager Zeroed format** for the virtual disk format.

Note In production environments, "thick provisioning" is mandatory. Thick provisioned Lazy Zero is also supported, but Thin provisioned is not supported.

Step 8 On the Network Mapping, choose your network on which this VM will reside.

Step 9 Do not select **Power on after deployment**.

Step 10 On the **Ready to Complete** page, click **Finish** to start the deployment.

Step 11 After the VM is created, verify the memory, CPU, and disk settings against the requirements shown in Multinode Cluster Hardware Specifications, on page 29.

Step 12 Power on the VM.

Step 13 Select the following options in the installation wizard:

Option	Option name	Description
1	IP	The IP address of the server.
2	netmask	The network mask for the server.
3	gateway	The IP address of the network gateway.
4	DNS	The DNS server is optional. Ensure that the DNS server is capable of looking up all hostnames referred to, including NTP server and remote backup locations.
5	NTP	The NTP server is mandatory to ensure that time keeping is accurate and synchronized among nodes in the same cluster.
6	hostname	The hostname, not the fully qualified domain name (FQDN).
7	role	• A WebProxy role installs only the front-end web server together with ability to distribute load among multiple middleware nodes. • An Application node is the main transaction processing engine and includes a web server which can operate by itself, or route transactions from a web node. • A Database node provides persistent storage of data. • A Standalone node consists of the Web, Application, and Database roles on one node. • A Unified node consists of the Web, Application, and Database roles on one node. On installation, the system needs to be clustered with other nodes and the cluster provisioned.
8	data center	The system's geographic location (data center name, city, country that a customer can use to identify the system location). You cannot change this setting once set.
9	platform password	Platform password must be at least eight characters long and must contain both uppercase and lowercase letters and at least one numeric or special character.
13	install	Completes the installation configuration and installs .

When the installation of the OVA is complete, a sign-in prompt for the platform user is displayed.

What to do next

Return to Multinode Installation, on page 29 to complete the overall installation procedure.

Create the HCM-F Device

After you create the HCM-F device, data synchronization begins if there is a network connection and the NBI REST service is running on the HCM-F server.

Before you begin

- Install and configure HCM-F. For more information, see the **Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide**

  .
- Verify that the NBI REST SDR Web Service is running
  1. Sign in to the HCM-F CLI as the user administrator.
  2. Run the **utils service list** command. Verify that the Cisco HCS NBI REST SDR Web Service is running.
  3. If not running, start it with the **utils service start Cisco HCS NBI REST SDR Web Service** command.

Procedure

Step 1 Sign in to as hcsadmin@sys.hcs.

Step 2 Create a new HCM-F instance:

a) Select **Device Management** > **HCM-F** and click **Add**.
b) Enter the HCM-F hostname.
c) Enter the HCM-F administrator Username.
d) Enter the HCM-F administrator Password.
e) Select the HCM-F Version v10_0 from the drop-down list.
f) Click **Save**.

Step 3 If the previous step fails:

- Verify that HCM-F Hostname is correct
- Verify that HCM-F administrator Username and administrator Password are correct
- Verify that HCM-F Version is correct
- Verify that the domain is set correctly using the CLI:
  a. `ssh platform@<cucdm hostname>`
  b. **network domain**

Step 4 After a couple of minutes, verify that the initial synchronization between and HCM-F is successful:

a) Select **Provider Management** > **Advanced** > **SDR Service Provider**.
b) The sync is successful if the default entry, "Service Provider Name", appears.

What to do next

If the initial sync is not working after following the previous steps, verify that the HCM-F REST API is working by browsing to the following: `http://<hcmf_app_node_host>/sdr/rest/<hcmf_version>/entity/ServiceProvider`. This command returns the JSON representation of the predefined service provider instance in the HCM-F Shared Data Repository (SDR). If you get an error, log in as the administrator on the HCM-F app node CLI and verify that the REST service is running:

To display the services, run the command: **utils service list**.

In the output, you see `Cisco HCS NBI REST SDR Web Service[STARTED].`

If this service is not started, start it with the command: **utils service start Cisco HCS NBI REST SDR Web Service**

For data sync failures, try importing the new HCM-F:

1. Select **Device Management** > **HCM-F** and click the HCM-F device.
2. Update the Hostname and click **Save**.
3. Import the new HCM-F:
   a. Select **Device Management** > **Advanced** > **Perform Actions**.
   b. In the Action field, select Import.
   c. In the Device field, select the HCM-F server.
   d. Click **Save** and wait a few minutes.
4. Check the provider under **Provider Management** > **Advanced** > **SDR Service Provider**.

Create a Provider

Note In Cisco Unified CDM 10.6(2) or later, the provider name is set to the current service provider name in HCM-F. You can decouple the provider name in Cisco Unified CDM from the service provider name in HCM-F.

Procedure

Step 1 Log in to as hcsadmin@sys.hcs.

Step 2 Select **Provider Management** > **Providers**.

Step 3 Click **Add**.

Step 4 On the **Service Provider Details** tab, complete the following fields:

Field	Description
Name	The name of the provider. This field is mandatory. **Note** Once you have saved the provider, you cannot change the provider name.

Field	Description
	Note Any spaces in the provider name are converted to underscores in the provider local administrator name and email, if **Create Local Admin** is checked.
Description	A description of the provider.
Domain Name	The domain of the provider. For example, provider.com. Used when creating the default local administrator so the administrator can sign in with an email ID such as ProviderAdmin@provider.com. This field is mandatory.
Create Local Admin	Controls whether a default local administrator is created.
Cloned Admin Role	The HCS default provider role used to create a new role prefixed with the provider name. The created provider role, shown in **Default Admin Role** field, is assigned to the default local administrator. This field appears only if **Create Local Admin** is checked.
Default Admin Role	The created provider role that is assigned to the default local administrator. This field is read only and appears only if **Create Local Admin** is checked.
Default Admin Password	The password to assign to the default local administrator. This mandatory field appears only if **Create Local Admin** is checked.
Repeat Default Admin Password	Confirm the default local administrator password. This mandatory field appears only if **Create Local Admin** is checked.

Step 5 On the **Contact Information** tab, enter address, email, and phone information as appropriate.

Step 6 Click **Save**.

The provider hierarchy node in , the Service Provider name in SDR, and optionally a default provider administrator are created.

Add Reseller

Procedure

Step 1 Login to the Cisco Unified Communications Domain Manager as the Provider admin. Enter provider admin's email address as username, it is case sensitive.

Example:

<provider_name>Admin@<domain_name>.

Step 2 Navigate to **Reseller Management** > **Resellers** from the menu.

Step 3 Click **Add**.

Step 4 Provide necessary details in the following:

a) Enter **Name**.

b) Enter **Description**.
c) Enter **Domain Name**.
d) Check **Create Local Admin** check box.
e) Keep the default values for **Clone Admin role** and **Default Admin Role**.
f) Enter **Default Admin** password and confirm in **Confirm** password text box.

Step 5 Click **Save**.

What to do next

Integrate Unified Communication Domain Manager with the customer instance. For more information, see the *Configuration Guide for Cisco Hosted Collaboration Solution for Contact Center* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/tsd-products-support-series-home.html

Install and Configure Session Border Controller

For complete installation and configuration instructions, see https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

Installing and Configuring Prime Collaboration Assurance and Analytics

To verify the supported version of Prime Collaboration Assurance and Analytics for this release of Cisco HCS, see the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

For complete installation and configuration instructions, see the *Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide* at https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.html.

The *Cisco Prime Collaboration Quick Start Guide* explains all aspects of installing and configuring Prime Collaboration Assurance in Advanced mode (so that you can select the Managed Service Provider deployment):

- Licensing
- Deployment models
- Deploying OVAs
- Configuring OVAs
- Required post installation tasks

Important

- The Prime Collaboration Assurance 12.1 and above MSP mode supports large and very large OVA. See the *Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide* for detailed information.

Log in to Prime Collaboration

Invoke Prime Collaboration Assurance using the client browser.

To log in to the Prime Collaboration application:

Procedure

Step 1 Open a browser session from your machine. Specify the IP address of either Prime Collaboration Assurance application.

Step 2 Enter any one of the following: `http://IP Address` or `https://IP Address`.

Note HTTPS is enabled by default for Prime Collaboration Assurance. Based on the browser you are using, one of the following appears:

- In Windows Internet Explorer, the Certificate Error: Navigation Blocked window.
- In Mozilla Firefox, the Untrusted Connection window.

These windows appear because Prime Collaboration uses a self-signed certificate.

Step 3 Remove the SSL certificate warning. See Removing SSL Certificate Warning at http://docwiki.cisco.com/wiki/troubleshooting_cisco_prime_collaboration

The Prime Collaboration login page appears.

Step 4 In the Prime Collaboration login page, you must log in as a globaladmin, using the same the credentials that you specified during the configuration.

Enabling HCM-F and Prime Collaboration Assurance to Communicate

The HCM-F versions compatible with Prime Collaboration Assurance is specified in the table. Prime Collaboration Assurance 11.6 and above version supports enhanced security.

To install the patch file for Prime Collaboration Assurance and Analytics use the link Download Software.

To install the .cop file on HCM-F use the link https://upload.cisco.com/cgi-bin/swc/fileexg/main.cgi.

See the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for details on the supported HCMF .cop file and PCA patch file.

Note

- Different versions of Prime Collaboration Assurance running in the same environment are not supported.
- HCM-F does not support uninstalling of ES files.
- Cisco Hosted Collaboration Solution supports a single HCM-F with one or more PCA for monitoring customer and devices.

Install and Configure ASA Firewall and NAT

Cisco Adaptive Security Appliance (ASA) Firewall partitions a single ASA into multiple virtual devices that keeps customer traffic separate and secure, and also makes configuration easier. All customer traffic is first sent to the firewall before forwarding to the computer resources.

Related Topics

Setup ASA, on page 40
Configure Multiple Context Modes, on page 41

Setup ASA

To initiate the basic setup in Cisco ASA, access the command-line interface and configure the credentials.

Procedure

Step 1 Connect a PC to the console port using console cable. Connect to console using a terminal emulator and set 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control.

Step 2 Press **Enter**.

Displays the following prompt:

```
hostname>
```

This indicates you are in user EXEC mode.

Step 3 Enter the following commands to access privileged EXEC mode:

```
hostname>enable
Password:
hostname#
```

Note Default, password is blank. Press **Enter** key to continue.

Step 4 Enter the following commands to access the global configuration mode:

```
hostname#configure terminal
hostname(config)#
```

Step 5 Enter `hostname` command to configure the hostname:

Example:

```
hostname(config)#hostname CISCOASA
CISCOASA(config)#
```

Step 6 Enter `enable passsword` command to configure the password:

```
CISCOASA(config)#enable password <enter the password>
```

Example:

```
CISCOASA(config)#enable password Password1234
CISCOASA(config)#exit
```

Step 7 Enter the following commands to save configuration:

```
hostname# copy running-config startup-config
```

Configure Multiple Context Modes

Procedure

Step 1 Enable the multiple context modes.

Step 2 Enable the interfaces.

Step 3 Configure the security contexts.

Step 4 Optional, in configure mode, enter `hostname(config)#mac-address auto` command to assign the MAC addresses to the context interfaces automatically.

Step 5 Configure interfaces in the context.

Related Topics

Enable Multiple Context Modes, on page 41
Enable Interfaces, on page 41
Configure Security Contexts, on page 42
Configure Interfaces in the Context, on page 42

Enable Multiple Context Modes

Procedure

Enter the following commands:

```
hostname#changeto system
hostname#configure terminal
hostname(config)#mode multiple
```

Note After you enable the multiple context mode, optionally you can configure the classes for resource management. You need not to create classes for HCS as you can use the default class.

Enable Interfaces

Complete the following procedure to configure interfaces:

Procedure

Step 1 Navigate to interface management 0/0 and enter the following commands:

```
hostname(config)#interface management 0/0
hostname(config-if)#no shut
```

Step 2 Navigate to interface gigabitethernet 0/0 and enter the following commands:

```
hostname(config)#interface gigabitethernet 0/0
hostname(config-if)#no shut
```

Configure Security Contexts

Complete the following procedure to configure security contexts:

Procedure

Step 1 Configure the admin context name in the global configuration mode:

```
hostname(config)#admin-context admin
```

Step 2 Navigate to the context admin:

```
hostname(config)#context admin
```

Step 3 Configure the admin context definitions:

```
hostname(config-ctx)#description admin Context for admin purposes
```

a) Allocate interface management 0/0 for admin context.

```
hostname(config-ctx)#allocate-interface management0/0 invisible
```

b) Create `admin.cfg` in disk 0.

```
hostname(config-ctx)#config-url disk0:/admin.cfg
```

Configure Interfaces in the Context

Complete the following procedure to configure interfaces in the admin context:

Procedure

Step 1 Navigate to admin context in configure mode:

```
hostname#changeto context admin
```

Step 2 Navigate to the interface management:

```
hostname/admin#configure terminal
hostname/admin(config)#interface management 0/0
```

Step 3 Enter a name for management interface of the admin context:

```
hostname/admin(config-if)#nameif management
```

Enter the IP address of the management interface:

```
hostname/admin(config-if)#ip address ip_address subnet_mask
hostname/admin(config-if)#exit
```

Example:

```
hostname/admin(config-if)#ip address 209.165.200.225 255.255.255.224
```

Step 4 Configure the following in global configuration mode to allow SSH to the admin context:

a) Generate an RSA key pair that is required for SSH. The modulus size value is 1024.

```
hostname/admin(config)#crypto key generate rsa modulus modulus_size
```

b) Save the RSA keys to persistent flash memory.

```
hostname/admin(config)#write memory
```

c) Enables local authentication for SSH access.

```
hostname/admin(config)#aaa authentication ssh console LOCAL
```

d) Create a user in the local database for SSH access.

```
hostname/admin(config)#username abcd password xxxx
```

e) Enter the IP address of the management interface from which the ASA accepts SSH connections.

```
hostname/admin(config)# ssh ip_address subnet_mask management
```

Example:

```
hostname/admin(config)# ssh 209.165.200.225 255.255.255.224 management
```

f) Set the duration to idle SSH session before the ASA disconnects the session.

```
hostname/admin(config)#ssh timeout 5
```

g) Enable HTTPS server and default port is 443.

```
hostname/admin(config)#http server enable
```

h) Enter the same IP address of management interface to access through HTTPS.

```
hostname/admin(config)# http server ip_address subnet_mask
```

i) Enter Default Static Route.

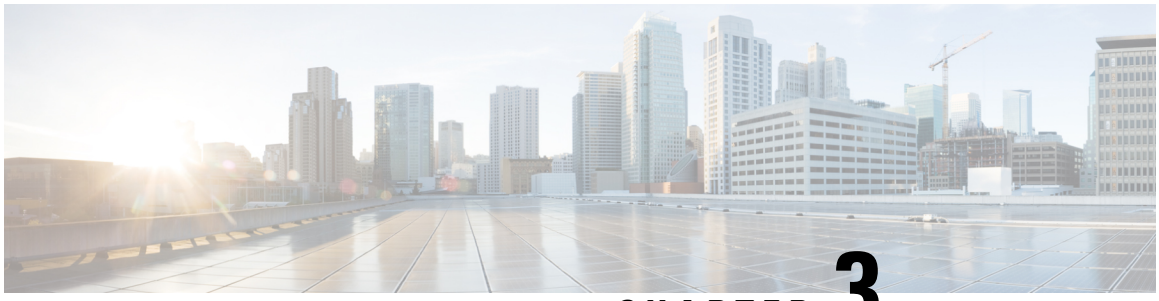
```
hostname/admin(config)# route management 0.0.0.0 0.0.0.0 ip_address
```

Example:

```
hostname/admin(config)#http server 209.165.200.225 255.255.255.224
hostname/admin(config)#route management 0.0.0.0 0.0.0.0 209.165.200.226
```

What to do next

Integrate Cisco ASA with the customer instance. For more information, see the *Configuration Guide for Cisco Hosted Collaboration Solution for Contact Center* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/tsd-products-support-series-home.html



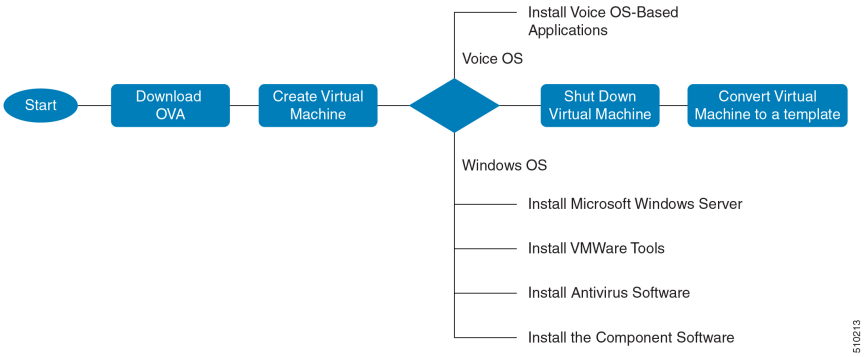
CHAPTER 3

Core Component Installation

Core Components Installation Approach

You can use golden templates to clone and deploy contact center core components as virtual machines (VM) on servers.

Figure 3: High-Level Golden Template Workflow



Note If you chose to create virtual machines directly on destination servers, do not convert the virtual machine to a template. For VOS based machines, see *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Core Component Voice Gateway Installation

For instructions on deploying the Cisco CSR 1000v OVA using vSphere, see the Cisco CSR 1000v Series Cloud Services Router Software Configuration Guide at: https://www.cisco.com/c/en/us/td/docs/routers/

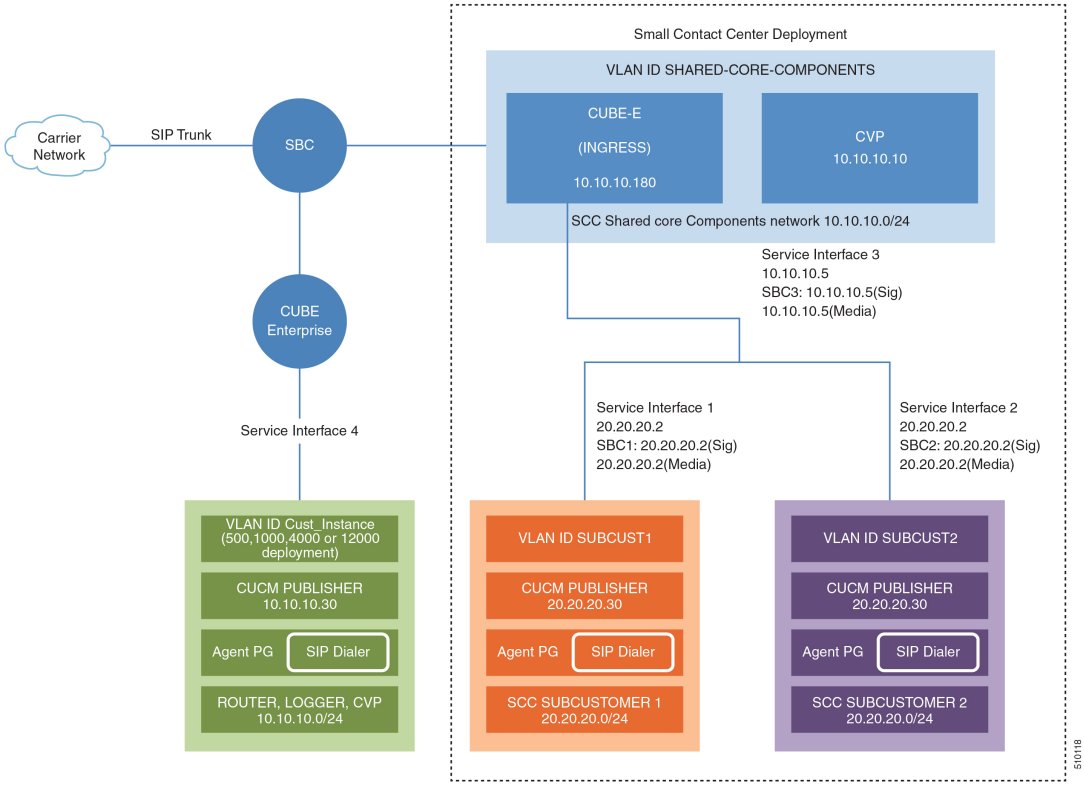
csr1000/software/configuration/b_CSR1000v_Configuration_Guide/b_CSR1000v_Configuration_Guide_chapter_011.html#d41950e959a1635

For information on Integrated Services Routers, see https://www.cisco.com/c/en/us/td/docs/routers/access/4400/release/xe-16-rn/isr4k-rel-notes-xe-16_3.html

Note If the SBC supports CUBE Enterprise with Multi-VRF, you can send calls directly from the SBC to the CVP without a dedicated CUBE Enterprise for the HCS for Contact Center instances. However, using the aggregation SBC without a dedicated CUBE Enterprise affects performance and scalability.

The following figure shows the CUBE Enterprise topology for HCS deployment.

Figure 4: CUBE Enterprise Topology for HCS Deployment Models



Configure Service Interface for Carrier Network

To create the service interface for carrier network, perform the following instructions.

```
interface GigabitEthernet1
ip address 192.168.10.2 255.255.255.0
negotiation auto
```

Configure Codec List

To configure codec list, perform the following instructions.

```
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8
codec preference 3 g729br8
codec preference 5 g711alaw
```

Note For Small Contact Center deployments, you may configure the carrier interface as a VRF.

Golden Template Requirements

Contact center core components vary for each deployment model. The following table provides information about the golden templates for required core components.

Table 1: Golden Templates for HCS for Contact Center Core Components

Golden Templates	2000 Agents	4000 Agents	12000 Agents	Small Contact Center
Unified CCE Rogger	Yes	Yes	—	Yes
Unified CCE Router	—	—	Yes	—
Unified CCE Logger	—	—	Yes	—
Unified CCE AW-HDS-DDS	Yes	Yes	—	Yes
Unified CCE AW-HDS	—	—	Yes	—
Unified CCE HDS-DDS	—	—	Yes	—
Unified CCE Agent PG	—	—	—	Yes
Unified CCE VRU PG	—	—	—	Yes
Unified CCE PG	Yes	Yes	Yes	—
Unified CVP Server	Yes	Yes	Yes	Yes
Unified CVP OAMP Server	Yes	Yes	Yes	Yes
Unified CVP Reporting Server	Yes	Yes	Yes	Yes
Cisco Finesse	Yes	Yes	Yes	Yes

Golden Templates	2000 Agents	4000 Agents	12000 Agents	Small Contact Center
Cisco Unified Intelligence Center Coresident Deployment	Yes	—	—	—
Cisco Unified Intelligence Center	—	Yes	Yes	Yes
Live Data Reporting System	—	Yes	Yes	Yes
Cisco Identity Service	—	Yes	Yes	Yes
Cisco Unified Communications Manager	Yes	Yes	Yes	Yes

Table 2: Golden Templates for HCS for Contact Center Core Components

Golden Templates	2000 Agents	4000 Agents	12000 Agents	24000 Agents	Small Contact Center
Unified CCE Rogger	Yes	Yes	—	—	Yes
Unified CCE Router	—	—	Yes	Yes	—
Unified CCE Logger	—	—	Yes	Yes	—
Unified CCE AW-HDS-DDS	Yes	Yes	—	—	Yes
Unified CCE AW-HDS	—	—	Yes	Yes	—
Unified CCE HDS-DDS	—	—	Yes	Yes	—
Unified CCE Agent PG	—	—	—	—	Yes
Unified CCE VRU PG	—	—	—	—	Yes
Unified CCE PG	Yes	Yes	Yes	Yes	—
Unified CVP Server	Yes	Yes	Yes	Yes	Yes

Golden Templates	2000 Agents	4000 Agents	12000 Agents	24000 Agents	Small Contact Center
Unified CVP OAMP Server	Yes	Yes	Yes	Yes	Yes
Unified CVP Reporting Server	Yes	Yes	Yes	Yes	Yes
Cisco Finesse	Yes	Yes	Yes	Yes	Yes
Cisco Unified Intelligence Center Coresident Deployment	Yes	—	—	—	—
Cisco Unified Intelligence Center	—	Yes	Yes	Yes	Yes
Live Data Reporting System	—	Yes	Yes	Yes	Yes
Cisco Identity Service	—	Yes	Yes	Yes	Yes
Cisco Unified Communications Manager	Yes	Yes	Yes	Yes	Yes

Create Golden Template for Unified CCE Rogger

Before you begin

Download OVA files. Use `UCCE_11.5_Win2012_vmv9_v1.0.ova` to create the golden template.

Download the OVA files. Use `UCCE_11.6_Win2012_vmv9_v1.0.ova` to create the golden template.

Download the OVA files. Use `UCCDM_12.0_Win2012R2_vm11_v1.0.ova` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CCE Rogger using the OVA.

Step 2 Install Microsoft Windows server.

Step 3 Install an anti-virus software.

Step 4 Install Microsoft SQL server.

Step 5 Install Unified Contact Center Enterprise.

Step 6 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Microsoft Windows Server
Install Antivirus Software, on page 63
Install Microsoft SQL Server
Install Unified Contact Center Enterprise, on page 143
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Unified CCE Router

Before you begin

Download the OVA files. Use `UCCDM_12.0_Win2012R2_vm11_v1.0.ova` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CCE Router using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install Unified Contact Center Enterprise.
Step 5 Convert the virtual machine to a template.

Related Topics

Create Virtual Machines, on page 59
Install Microsoft Windows Server
Install Antivirus Software, on page 63
Install Unified Contact Center Enterprise, on page 143
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Unified CCE Logger

Before you begin

Download the OVA files. Use `UCCDM_12.0_Win2012R2_vm11_v1.0.ova` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CCE Logger using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install Microsoft SQL server.
Step 5 Install Unified Contact Center Enterprise.

Step 6 Convert the virtual machine to a template.

Related Topics

Create Virtual Machines, on page 59
Install Microsoft Windows Server
Install Antivirus Software, on page 63
Install Microsoft SQL Server
Install Unified Contact Center Enterprise, on page 143
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Unified CCE AW-HDS-DDS

Before you begin

Download the OVA files. Use `UCCDM_12.0_Win2012R2_vm11_v1.0.ova` to create the golden template.

Note After you deploy OVA for 500 agents deployment (HCS for Contact Center 2000 reference only), edit the settings and change the Memory to 8GB and MHz Reservation to 3200.

Procedure

Step 1 Create a virtual machine for Unified CCE AW-HDS-DDS using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install Microsoft SQL server.
Step 5 Install Unified Contact Center Enterprise.
Step 6 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Microsoft Windows Server
Install Antivirus Software, on page 63
Install Microsoft SQL Server
Install Unified Contact Center Enterprise, on page 143
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Unified CCE AW-HDS

Before you begin

Download the OVA files. Use `UCCDM_12.0_Win2012R2_vm11_v1.0.ova` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CCE AW-HDS using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install Microsoft SQL server.
Step 5 Install Unified Contact Center Enterprise.
Step 6 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Microsoft Windows Server
Install Antivirus Software, on page 63
Install Microsoft SQL Server
Install Unified Contact Center Enterprise, on page 143
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden template for Unified CCE HDS-DDS

Before you begin

Download the OVA files. Use `UCCDM_12.0_Win2012R2_vm11_v1.0.ova` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CCE HDS-DDS using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install Microsoft SQL server.
Step 5 Install Unified Contact Center Enterprise.
Step 6 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Microsoft Windows Server
Install Antivirus Software, on page 63
Install Microsoft SQL Server
Install Unified Contact Center Enterprise, on page 143
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Unified CCE PG

Before you begin

Download the OVA files. Use `UCCDM_12.0_Win2012R2_vm11_v1.0.ova` to create the golden template.

Note For 500 agents deployment of the HCS for Contact Center 2000 agent reference, select the **Small PG** OVA.

Procedure

Step 1 Create a virtual machine for Unified CCE PG using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install Unified Contact Center Enterprise.
Step 5 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Microsoft Windows Server
Install Antivirus Software, on page 63
Install Unified Contact Center Enterprise, on page 143
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Unified CVP Server

Before you begin

Download OVA files. Use `UCCE_11.5_Win2012_vmv9_v1.0.ova` to create the golden template.

Download the OVA files. Use `UCCE_11.6_Win2012_vmv9_v1.0.ova` to create the golden template.

Download the OVA files. Use `UCCDM_12.0_Win2012R2_vm11_v1.0.ova` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CVP Server using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install the Unified CVP Server.
Step 5 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Microsoft Windows Server
Install Antivirus Software, on page 63
Install Unified CVP Server, on page 144
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Unified CVP OAMP Server

Before you begin

Download OVA files. Use `UCCE_11.5_Win2012_vmv9_v1.0.ova` to create the golden template.

Download the OVA files. Use `UCCE_11.6_Win2012_vmv9_v1.0.ova` to create the golden template.

Download the OVA files. Use `UCCDM_12.0_Win2012R2_vm11_v1.0.ova` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CVP OAMP Server using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install the Unified CVP OAMP server.
Step 5 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Microsoft Windows Server
Install Antivirus Software, on page 63
Install Unified CVP OAMP Server, on page 144
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Unified CVP Reporting Server

Before you begin

Download OVA files. Use `UCCE_11.5_Win2012_vmv9_v1.0.ova` to create the golden template.

Download the OVA files. Use `UCCE_11.6_Win2012_vmv9_v1.0.ova` to create the golden template.

Download the OVA files. Use `UCCDM_12.0_Win2012R2_vm11_v1.0.ova` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CVP Reporting server using the OVA.

Step 2 Install Microsoft Windows server.

Step 3 Install an anti-virus software.

Step 4 Install the Unified CVP Reporting server.

Step 5 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Microsoft Windows Server
Install Antivirus Software, on page 63
Install Unified CVP Reporting Server, on page 145
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Cisco Finesse

Before you begin

Download the OVA files. Use `Finesse_12.0.1_VOS12.0.1_vmv11_v1.3` to create the golden template.

Note For Small Contact Center 100 agents dedicated sub-customer deployment and 500 agents deployment (HCS for Contact Center 2000 reference and Small Contact Center 500 agent deployment), select the Finesse **500 agents** OVA.

After you deploy OVA for 500 agents deployment (HCS for Contact Center 2000 reference and Small Contact Center 500 agent deployment) change the vCPU value to 4.

Procedure

Step 1 Create a virtual machine for Cisco Finesse.

Step 2 Install **Cisco Finesse**.

Step 3 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Voice OS-Based Applications
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Cisco Unified Intelligence Center Coresident Deployment

Before you begin

Cisco Unified Intelligence Center coresident deployment includes Cisco Unified Intelligence Center, Live Data, and Identity Service components.

Download the OVA files. Use `CUIC_12.0.1_vmv11_v2.13` to create the golden template.

Note After you deploy OVA for 500 agents deployment (HCS for Contact Center 2000 reference only), edit the settings and change the memory to 12 GB.

Procedure

Step 1 Create a virtual machine for Cisco Unified Intelligence Center coresident deployment using the OVA.

Step 2 To install **Cisco Unified Intelligence Center with Live Data and Ids**, follow the installation procedure in the **Install Voice OS based Application** and select **Cisco Unified Intelligence Center with Live Data and Ids** in the **Product Deployment Selection** page .

Step 3 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Voice OS-Based Applications
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Cisco Unified Intelligence Center

Before you begin

Download the OVA files. Use `CUIC_12.0.1_vmv11_v2.13` to create the golden template.

Procedure

Step 1 Create a virtual machine for Cisco Unified Intelligence Center using the OVA.

Step 2 To install **Cisco Unified Intelligence Center**, follow the installation procedure in the **Install Voice OS based Application** and select **Cisco Unified Intelligence Center** in the **Product Deployment Selection** page.

Step 3 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Voice OS-Based Applications

Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Live Data Reporting System

Before you begin

Download the OVA files. Use `UCCELD_12.0_VOS_vmv11_v1.0.ova` to create the golden template.

Note See related links to run the steps.

Procedure

Step 1 Create a virtual machine for Live Data Reporting System using the OVA.

Step 2 Select **Live Data** in the **Product Deployment Selection** page .

Step 3 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Voice OS-Based Applications
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Cisco Identity Service

Before you begin

Download the OVA files. Use `IDS_12.0_VOS_vmv11_v1.0` to create the golden template.

Procedure

Step 1 Create a virtual machine for Cisco Identity Service using the OVA.

Step 2 To install **Cisco Identity Service (Ids)**, follow the installation procedure in the **Install Voice OS based Application** and select **Cisco Identity Service (Ids)** in the **Product Deployment Selection** page.

Step 3 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Voice OS-Based Applications
Convert the Virtual Machine to a Golden Template, on page 68

Create Golden Template for Cisco Unified Communications Manager

Before you begin

Download the OVA files. Use `cucm_11.5_vmv8_v1.1` to create the golden template.

Note Select the **2500 agents** OVA for SCC 100 agents dedicated sub-customer deployment and 500 agents deployment (HCS for Contact Center 2000 reference and Small Contact Center 500 agent deployment). After you deploy the OVA edit the settings and change the vCPU value to 2.

Procedure

Step 1 Create a virtual machine for Cisco Unified Communications Manager using the OVA.

Step 2 To install **Cisco Unified Communications Manager**, follow the installation procedure in the **Install Voice OS based Application** and select **Cisco Unified Communications Manager** in the **Product Deployment Selection** page.

Step 3 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 59
Install Voice OS-Based Applications
Convert the Virtual Machine to a Golden Template, on page 68

Common Procedures for Golden Templates

Related Topics

Create Golden Template for Unified CCE Rogger, on page 49
Create Golden Template for Unified CCE Router, on page 50
Create Golden Template for Unified CCE Logger, on page 50
Create Golden Template for Unified CCE AW-HDS-DDS, on page 51
Create Golden Template for Unified CCE AW-HDS, on page 51
Create Golden template for Unified CCE HDS-DDS, on page 52
Create Golden Template for Unified CCE PG, on page 53
Create Golden Template for Unified CVP Server, on page 53
Create Golden Template for Unified CVP OAMP Server, on page 54
Create Golden Template for Unified CVP Reporting Server, on page 54
Create Golden Template for Cisco Finesse, on page 55
Create Golden Template for Cisco Unified Intelligence Center Coresident Deployment, on page 56
Create Golden Template for Cisco Unified Intelligence Center, on page 56
Create Golden Template for Cisco Identity Service, on page 57
Create Golden Template for Cisco Unified Communications Manager, on page 58

Download OVA Files

Open Virtualization Format files (OVAs) are required for golden templates. Cisco HCS for Contact Center uses the OVAs that define the basic structure of the corresponding VMs that are created. The structure definition Includes the CPU, RAM, disk space, reservation for CPU, and reservation for memory.

Note The VMs and software components are optimized for Cisco HCS for Contact Center. You must use the OVAs for Cisco HCS for Contact Center.

Before you begin

You must have a valid service contract associated with your Cisco.com profile

Procedure

Step 1 Go to the *Hosted Collaboration Solution for Contact Center* Download Software page on Cisco.com.

Step 2 Select the required software type.

Step 3 Click **Download** and save the OVA file to your local drive. When you create VMs, select the OVA required for the application.

Create Virtual Machines

Procedure

Step 1 Launch the VMware vSphere client and select **File** > **Deploy OVF Template**.

Step 2 Browse to the location on your local drive, where you have stored the OVA. Click **Open** to select the OVA file, click **Next**.

Step 3 On the **OVF Template Details** page, click **Next**.

Step 4 On the **Name and Location** page, in the **Name** field, enter the name of virtual machine, then click **Next**.

Note Enter a maximum of 32 characters; spaces and special characters are not allowed.

Step 5 On the **Deployment Configuration** page, select the appropriate configuration from the drop-down list, click **Next**.

Step 6 On the **Resource Pool** page, select the required resource pool, then click **Next**.

Note Skip this step if you do not have a resource pool allocated in the host server.

Step 7 On the **Storage** page, select a data store you want to deploy in the new virtual machine, then click **Next**.

Step 8 On the **Disk Format** page, select **Thick provisioned Lazy Zeroed**, then click **Next**.

Note Thin provision format is used for the template creation process, it is not supported for production use.

Step 9 On the **Network Mapping** page, select the appropriate network from the **Destination Network** drop-down list, then click **Next**.

Note For Unified Contact Center Enterprise machines, confirm that **Network Mapping** page is correct:

- Public to Visible Network
- Private to Private Network

Step 10 Click **Finish**.

Mount ISO Files

Upload ISO image to data store:

1. Select the host in the vSphere client and click **Configuration**. Then click **Storage** in the left panel.
2. Select the datastore that will hold the ISO file.
3. Right click and select **Browse datastore**.
4. Click the **Upload** icon and select **Upload file**.
5. Browse to the location on your local drive where you saved the ISO file, and upload the ISO to the datastore.

Mount the ISO image:

1. Right-click the VM in the vSphere client and select **Edit virtual machine settings**.
2. Click **Hardware** and select **CD|DVD Drive 1**.
3. Check **Connect at power on** (Device status panel upper right).
4. Click the **Datastore ISO File** radio button and then click **Browse**.
5. Navigate to the data store where you uploaded the file.
6. Select the ISO file and click **OK**.

Unmount ISO File

Procedure

Step 1 Right-click the virtual machine in the vSphere client and select **Edit virtual machine settings**.

Step 2 Click **Hardware** and select **CD/DVD Drive 1**.

Step 3 Select **Client Device** and click **OK**.

Install Microsoft Windows Server

Complete the following procedure to install Microsoft Windows Server on the virtual machines deployed.

Note Before installing 12.5(1) ICM on SQL Server , make sure to install ODBC Driver 13 for SQL Server® manually.

Procedure

Step 1 Mount the Microsoft Windows Server ISO image to the virtual machine.

Check the **Connect at power on** check box when mounting the ISO.

Step 2 Power on the VM.

Step 3 Enter the Language, Time and Currency Format, and Keyboard settings. Click **Next**.

Step 4 Click **Install Now**.

Step 5 If prompted, enter the product key for Windows Server and click **Next**.

Step 6 Select the Desktop Experience option for the Windows Server and click **Next**.

Step 7 Accept the license terms and click **Next**.

Step 8 Select **Custom: Install Windows only (advanced)**, select **Drive 0** to install Microsoft Windows Server, and then click **Next**.

The installation begins. After the installation is complete, the system restarts without prompting.

Step 9 Enter and confirm the password for the administrator account, and then click **Finish**.

Step 10 Enable Remote Desktop connections as follows:

a) Navigate to **Control Panel** > **System and Security** > **System**.
b) Click **Remote Settings**.
c) Click the **Remote** tab.
d) Select the **Allow remote connections to this computer** radio button. The Remote Desktop Connection dialog displays a notification that the Remote Desktop Firewall exception is enabled. Click **OK**.

Step 11 Open the **Network and Sharing Center**, and in the View your basic network info and set up connections section, click **Ethernet**.

Step 12 In the Ethernet Status window, click **Properties**.

Step 13 In the **Ethernet Properties** dialog box, configure the network settings and the Domain Name System (DNS) data:

a) Uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
b) Select Internet Protocol Version 4 (TCP/IPv4) and click **Properties**.
c) Select **Use the following IP Address**.
d) Enter the IP address, subnet mask, and default gateway.
e) Select **Use the following DNS Server Address**.
f) Enter the preferred DNS server address, and click **OK**.

Step 14 Navigate to **Control Panel** > **System and Security** > **System**. Follow the instructions:

a) Click**Change Settings**.
b) In Computer name tab, click **Change**.

c) Change the name of the computer from the name randomly generated during Microsoft Windows Server installation. The name does not contain underscores or spaces.
d) Select **Domain** radio button to change the member from Workgroup to Domain.
e) Enter qualified domain name and click **OK**.
f) In the Windows security dialog, validate the domain credentials and click **OK**.
g) On successful authentication, click **OK**.
h) Reboot the server and sign in with domain credentials.

Restart your system for the change to take effect.

Microsoft Windows Server is installed. In addition, Internet Explorer 11 is installed automatically.

Note If you want to install Unified CCE on a multilingual version of Windows Server, refer to Microsoft documentation for details in installing Microsoft Windows Server Multilingual language packs.

If Unified CCE language pack is applied on Chinese Windows OS machine, set the screen resolution to 1600 x 1200.

Install VMware Tools for Windows

Procedure

Step 1 From the vSphere Client, right-click the virtual machine, select **Power**, and click **Power On**.

Step 2 Click the **Summary** tab.

In the General section, the VMware Tools field indicates whether VMware Tools are:

- installed and current
- installed and not current
- not installed

Step 3 Click the **Console** tab to make sure that the guest operating system starts successfully. Log in if prompted.

Step 4 Right-click the virtual machine, select **Guest OS**, and then click **Install/Upgrade VMware Tools**. The **Install/Upgrade VMware Tools** window appears with the option - Interactive Tools Upgrade and Automatic Tools Upgrade.

a) To install/upgrade the VMware tools manually, select the **Interactive Tools Upgrade** option, and click **OK**. Follow the on-screen instructions to install/upgrade the VMware tools, and restart the virtual machine when prompted.
b) To install/upgrade the VMware tools automatically, select the **Automatic Tools Upgrade** option, and click **OK**. This process takes a few minutes to complete, and restart the virtual machine when prompted.

Install Antivirus Software

Perform this procedure for both golden-template and for direct-install options.

Install any of the antivirus software products supported by HCS for CC for Contact Center.

For more information on the anitvirus software and versions supported by HCS for CC for Contact Center, see *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html.

Install any of the antivirus software products supported by Enterprise Chat and Email. For more information on the anitvirus software and versions supported by Enterprise Chat and Email, see the *System Requirements for Enterprise Chat and Email* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-implementation-design-guides-list.htm.

Important Update antivirus software, manually - do not enable automatic updates.

Tip To allow required access to installation program files or folders, perform file-blocking exclusions in the antivirus product file-and-folder protection rules. To do this in McAfee VirusScan:

- Launch the VirusScan console.
- Right-click **Access Protection**, then select **Properties**.
- In the **Anti-virus Standard Protection** category, make sure that the Prevent IRC communication check box is unchecked in the **Block** column.

Important HCS for CC for Contact Center supports Symantec Endpoint Protection.

Be aware that in the firewall component of Symantec Endpoint Protection 12.1, the Network Threat Protection feature, must be disabled. If it remains enabled, which is the default, both sides of the duplexed router shows up in simplex mode, thus blocking communications between each side of the router. This blocking impacts all deployment types.

If you retain the default (enabled) start services on side A and B of the router, a Symantec message pops up in the system tray indicating: The client will block traffic from IP address [side A router address] for the next 600 seconds(s). This message also appears in the client management security log. The Symantec Network Threat Protection traffic log indicates that a default firewall rule called “Block_all” was dynamically enabled. The result in both sides of the router come up in simplex mode.

To avoid the issue, you must disable the **Symantec** firewall and restart both sides of the router. To do this, double click the Symantec icon in the system tray and select **Change Settings**. Then configure settings for Network Threat Protection and uncheck the **Enable Firewall** check box at the top of the Firewall tab.

Disabling Port Blocking

On computers that run Unified CVP Server components, such as Call Server and Reporting server, which has an anti-virus software configured to block ports, exclude Unified CVP processes and `tomcat6.exe`. In addition, exclude Voice Browser.exe for the call server process.

Note If you use an anti-virus software other than McAfee Virus Scan, perform the equivalent exclusions in port blocking rules for that software.

Procedure

Step 1 Launch **McAfee**.

Step 2 In the **VirusScan Console**, double-click **Access Protection**, then choose **Anti-virus Standard Protection**.

Step 3 Choose **Prevent IRC communication** from the list, then click **Edit**.

Step 4 Add `tomcat6.exe`, `tomcat5.exe`, `VoiceBrowser.exe` to the **Processes to Exclude** , then click **Ok**.

Step 5 Click **Ok**.

Install Microsoft SQL Server

Install Microsoft SQL Server and store the SQL Server log and temporary files on the same vDisk as the operating system when using **default** (two) vDisk design. If you choose to use more than two virtual disks, then the tempDB cannot be on the same vDisk as the solution database.

For further information about the database placement and performance tuning the SQL installation, see the Microsoft documentation.

Before you begin

Note Microsoft SQL Server does not contain SQL Server Management Studio in the default toolkit. To rerun the SQL Server setup to install Management Studio, navigate to: **SQL Selection Center** > **Installation** > **Install SQL Server Management Tools**. If your computer has no internet connection, download and install SQL Server Management Studio manually.

Procedure

Step 1 Mount the Microsoft SQL Server ISO image to the virtual machine. For more information, see Mount ISO Files, on page 60.

Step 2 Select **Installation** in the left pane and then click **New SQL Server stand-alone installation or add features to an existing installation**. Click **OK**.

Step 3 On the **Product Key** page, enter the product key and then click **Next**.

Step 4 Accept the **License Terms** and then click **Next**.

Step 5 Optional: On the **Microsoft Update** page, check the **Use Microsoft Update to check for updates** check box, and then click **Next**.

Note If you do not check the **Use Microsoft Update to check for updates** option, click **Next** on the **Product Updates** page.

Step 6 On the **Install Rules** page, click **Next**.

In this step, the installation program checks to see that your system meets the hardware and software requirements. If there are any issues, warnings or errors appear in the **Status** column. Click the links for more information about the issues.

Step 7 On the **Feature Selection** page, select only the following, and click **Next**:

- **Database Engine Services**
- **Client Tools Connectivity**
- **Client Tools Backwards Compatibility**
- **Client Tools SDK**
- **SQL Client Connectivity SDK**

If you intend to use Outbound Option High Availability two-way replication, be sure to select the Replication feature on this page. For more information about replication, see the *Outbound Option Guide for Unified Contact Center Enterprise*.

Step 8 On the **Instance Configuration** page, select **Default Instance** and click **Next.**

Step 9 On the **Server Configuration** page, click the **Services Account** tab.

a) Associate the SQL services with the virtual account.

- For the SQL Server Agent service, in the Account Name field, select **NT Service\SQLSERVERAGENT**. If you have enabled Outbound Option High Availability, this account must have the system administrator privilege.
- For the SQL Server Database Engine, in the Account Name field, select **NT Service\MSSQLSERVER**.

Note While you can use the Network or Local Services account instead of the Virtual account, using the Virtual account provides security.

b) For the remaining services, accept the default values.

c) In the **Start Up Type** column, for the **SQL Server Agent service** account, select **Automatic** from the list.

d) Enable **Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service**.

Note Unified ICM Installer automatically enables the **Grant Perform Volume Maintenance Task** for the NT service account.If it is not enabled automatically then you must enable **Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service** manually on the SQL server.

Step 10 On the **Server Configuration** page, click the **Collation** tab.

a) In the Database Engine section, click **Customize**.

b) Select the **Windows Collation designator and sort order** radio button.
c) Select the appropriate collation. Typically, you choose the SQL Server collation that supports the Windows system locale most commonly used by your organization; for example, "Latin1_General" for English.

Note See the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for details about collations used for other languages.

The database entry is related to the collation that you select. For example, if you set the collation for Latin1_General, but you select Chinese language at sign-in. When you enter field values in Chinese, the application displays the `unsupported character` error, because the database does not support the characters.

Important It is critical to select the correct collation setting for the language display on your system. If you do not select the correct collation during installation, you must uninstall and reinstall Microsoft SQL Server.

d) Check the **Binary** check box.
e) Click **OK**, and then click **Next**.

Step 11 On the **Database Engine Configuration** page:

a) On the Server Configuration tab, click the **Mixed Mode** radio button.
b) Enter the password for the SQL Server system administrator account, and confirm by reentering it.
c) Click **Add Current User** to add the user who is installing the SQL Server as an administrator.
d) On the **TempDB** tab, set the **Initial size** and **Autogrowth** for Rogger, Logger, AW-HDS-DDS, AW-HDS, and HDS-DDS. For information about values for respective components Increase Database and Log File Size for TempDB, on page 67.

For more information about the SQL Server TempDB Database and its use, see the Microsoft SQL Server documentation.

e) Click **Next**.

Step 12 On the **Ready to Install** page, click **Install**.

Step 13 On the **Complete** page, click **Close**.

Step 14 Enable Named Pipes and set the sort order as follows:

a) Open the SQL Server Configuration Manager.
b) In the left pane, navigate to **SQL Native Client 11.0 Configuration (32bit)** > **Client Protocols**.
c) In the right pane, confirm that **Named Pipes** is **Enabled**.
d) Right-click **Client Protocols** and select **Properties**.
e) In the **Enabled Protocols** section of the **Client Protocols Properties** window, use the arrow buttons to arrange the protocols in the following order:

1. Named Pipes
2. TCP/IP

f) Check the **Enable Shared Memory Protocol** and then click **OK**.
g) In the left pane, navigate to **SQL Server Network Configuration** > **Protocols for MSSQLSERVER**.
h) In the right pane, right-click **Named Pipes** and select **Enable**.

Note By default, Microsoft SQL Server dynamically resizes its memory. The SQL Server reserves the memory based on process demand. The SQL Server frees its memory when other processes request it, and it raises alerts about the memory monitoring tool.

Cisco supports the Microsoft validation to dynamically manage the SQL Server memory. If your solution raises too many memory alerts, you can manually limit SQL Server's memory usage. Set the maximum and minimum limit of the SQL memory using the **maximum memory usage** settings in the **SQL Server Properties** menu.

For more information about the SQL Server memory settings and its use, see the Microsoft SQL Server documentation.

Step 15 Set the SQL Server's default language to English as follows:

a) Launch SQL Server Management Studio.
b) In the left pane, right-click the server and select **Properties**.
c) Click **Advanced**.
d) In the **Miscellaneous** section, set the **Default Language** to **English**.
e) Click **OK**.

Important Set the SQL Server default language to English because Cisco Unified Contact Center Enterprise requires a US date format (MDY). Many European languages use the European date format (DMY) instead. This mismatch causes queries such as `select * from table where date = '2012-04-08 00:00:00'` to return data for the wrong date. Handle localization in the client application, such as Cisco Unified Intelligence Center.

Step 16 Restart the SQL Server service as follows:

a) Navigate to the **Windows Services** tool.
b) Right-click **SQL Server (MSSQLSERVER)** and click **Stop**.
c) Right-click **SQL Server (MSSQLSERVER)** and click **Start**.

Step 17 Ensure that the SQL Server Browser is started, as follows:

a) Navigate to the **Windows Services** tool.
b) Navigate to the SQL Server Browser.
c) Right-click to open the **Properties** window.
d) Enable the service, change the startup type to **Automatic**, and click **Apply**.
e) To start the service, click **Start**, and then click **OK**.

What to do next

⚠

Caution Do not change the SQL port number. Retain the default port numbers as 1433 for TCP and 1434 for UDP connections. In case you change the port numbers, the applications like CCEAdmin will not work.

Increase Database and Log File Size for TempDB

To get the benefits of TempDB multiple data files support in CCE components, configure the following values as suggested for respective components.

CCE Component	vCPU	TempDB Data Files			TempDB Transaction Log File	
		Number of Files	Initial Size	Autogrowth	Initial Size	Autogrowth
Rogger	4	4	800MB	100MB	600MB	10MB
Logger	4	4	800MB	100MB	600MB	10MB
AW-HDS-DDS	4	4	800MB	100MB	600MB	10MB
AW-HDS	8	8	400MB	100MB	600MB	10MB
HDS-DDS	8	8	400MB	100MB	600MB	10MB

Convert the Virtual Machine to a Golden Template

Perform this procedure for the golden-template install option.

Note VMware uses the term *Template*. HCS for Contact Center uses the term *Golden Template* for templates consisting of application and operating systems that are used for HCS for Contact Center.

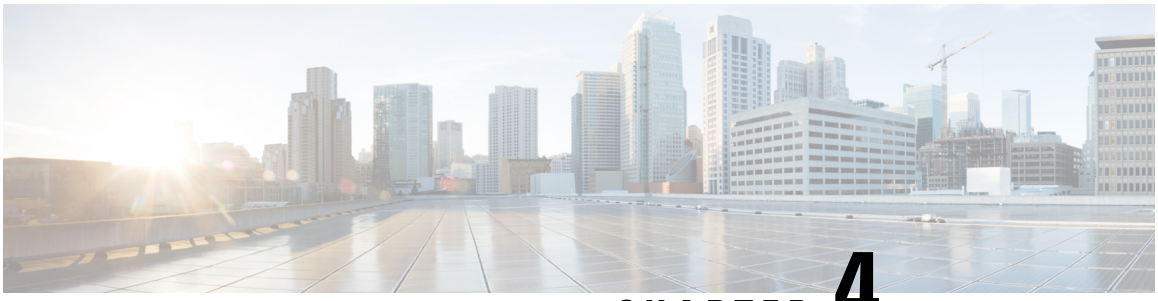
Before you begin

Ensure that the Windows-based template virtual machine is in the WORKGROUP.

Procedure

Step 1 If the VM is not already powered off, from the **VM** menu, select **Power** > **Shut down the guest**.

Step 2 From the VMware vCenter **Inventory** menu, right-click the virtual machine and choose **Template** > **Convert to Template**.



CHAPTER 4

Post-Installation

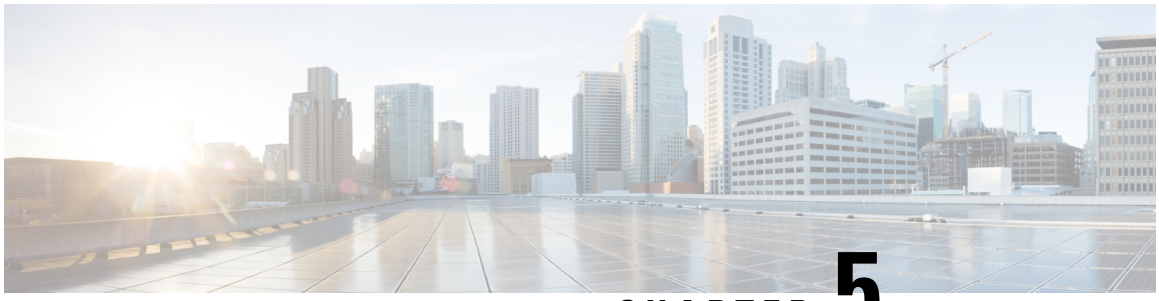
Post-Installation Tasks

After you install the Cisco HCS for Contact Center components, configure the customer instance for each deployment model that you choose. For more details on the customer instance configurations, see *Configure Customer Instance* chapter in *Configuring Guide for Cisco HCS for Contact Center* https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

Before you configure the customer instance, do:

- Clone and OS customization
- Automated cloning and OS customization
- Manual cloning and OS customization

For more information on these steps, see *Configuring Guide for Cisco HCS for Contact Center* https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.



CHAPTER 5

Upgrade

Overview of the Upgrade Workflow

Current Deployment Type	Target Deployment Type	Upgrade Process
HCS for CC 500	HCS for CC 2000	Migration CC Upgrade
HCS for CC 1000	HCS for CC 2000	Migration CC Upgrade
HCS for CC 4000	HCS for CC 4000	Standard CC Upgrade
HCS for CC 12000	HCS for CC 12000	Standard CC Upgrade

Note

- All upgrades from 11.6 to 12.0 are Standard CC upgrades. However if you are upgrading from the 500 Agent deployment type (deprecated in 11.5(1) and removed and unsupported from 11.6(1)), use the Migration CC Upgrade procedure.
- The Small Contact Center (SCC) deployment uses the HCS for CC 4000 deployment type and follows same upgrade process.

Perform the Cisco HCS for Contact Center upgrade in the same sequence as the upgrade and validation steps are described in this document.

For more information, see *Cisco Hosted Collaboration Solution Documentation*, https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

The following upgrade paths are supported:

- Unified CCE 10.5(x) to 12.0(x)
- Unified CCE 11.0(x) to 12.0(x)

- Unified CCE 11.5(x) to 12.0(x)
- Unified CCE 11.6(x) to 12.0(x)

Upgrade from 12.0(x) to 12.5(1) is supported in this release. Use EDMT during this upgrade process.

Upgrading Management Components

Upgrade HCM-F

Before you begin

Before upgrading a Cisco HCM-F application node, perform the following tasks.

- Create a valid DRF backup of your HCM-F.
- From the command-line interface on the application node, run **show hcs cluster nodes** to verify that the node is at the pre-upgrade version.
- Obtain the upgrade media for upgrading the HCM-F platform: upgrade disk or a downloaded executable file.

Procedure

Step 1 If you downloaded the executable file from Cisco.com, perform one of the following steps.

- Prepare to upgrade from a local folder.
  a. Copy the upgrade file to a temporary folder on a local hard drive.
  b. Open an SFTP client and connect to the HCM-F server using your adminsftp user ID and password.
  c. Run the **cd upgrade** command to navigate to the upgrade folder.
  d. Run the **put [upgrade file name]** command to transfer the file.
- Prepare to load an ISO file.
  a. Copy the upgrade ISO to a data store that is accessible by your virtual machine.
  b. Attach the ISO image to the CD/DVD drive of the virtual machine.
- Put the upgrade file on an FTP or SFTP server that is accessible by the virtual machine that you are upgrading.

Step 2 Copy the contents of the upgrade disk or downloaded files to the virtual machine that you are upgrading. Ensure that the upgrade filename begins with 'HCS.'

Step 3 On the virtual machine that you are upgrading, log in to the HCM-F command-line interface and run the **utils system upgrade initiate** command.

Step 4 Choose the source from which you want to upgrade.

- Remote file system via SFTP
- Remote file system via FTP
- Local DVD/CD
- Local Upload Directory

Step 5 Follow system prompts for the upgrade option you chose.
The system prompts you when the upgrade is complete.

Step 6 If you did not choose to automatically switch versions, run the **utils system switch-version** command. Enter `yes` to reboot the server and switch to the new software version.

Step 7 From the HCM-F command-line interface, run the **show version active** command to verify that the software version is the upgraded version.

Step 8 If you performed step 6, run the **utils service list** command to view services. Then run **utils service start [service name]** to restart any services that were stopped before the upgrade.

Validate the HCM-F Upgrade

Perform the following steps to validate the upgrade of Cisco HCM-F.

Procedure

Step 1 Verify that no error logs were created during or after the upgrade.

Step 2 Run the **show version active** command to verify that the active version is the upgraded version.

Step 3 Run the **utils service list** command to verify that all services are running as they were before the upgrade.

Step 4 Sign in to the administration interface and click the **About** link to verify that the interface displays the upgraded version.

Step 5 Verify that all synchronization is successful for Service Provider, Data Center, vCenter, Customer, and UCS Manager.

Step 6 Verify that Hosted License Manager does not contain post-upgrade errors. Also verify that licenses are assigned to the proper customers.

Step 7 Depending on which you used for the upgrade, ensure that Platform Manager or Prime Collaboration Deployment is running.

Step 8 Verify that Service Inventory is running.

Upgrade UCDM

Procedure

Step 1 Create a backup using the platform command-line interface. You can back up the cluster or back up each node individually.

Step 2 Turn off any scheduled imports.

Step 3 Check for running imports. Either wait for them to complete or cancel them.

Step 4 Upgrade multinode environment. See, *Upgrade a Multinode Environment* section in *Cisco Hosted Collaboration Solution Upgrade and Migration Guide* https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

The *Cisco Unified Communications Domain Manager Planning and Install Guide* also contains installation instructions for multinode environments. You can find the guide on the **Component Documentation** tab here: https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-version-10-6-1/model.html.

Validate the Unified CDM Upgrade

Take the following steps to validate the upgrade of Unified CDM in a multinode or standalone environment.

Procedure

Step 1 Sign in to the user interface as hcsadmin, and click **About** > **Extended Version** to verify the upgrade.

Step 2 Reactivate the scheduled imports that you turned off before upgrading.

Step 3 Use the command-line interface on the primary node to run the **cluster status** command.
The command returns a list of clusters and their status.

Step 4 Attempt to associate a phone with a user:

a) In Unified CDM, navigate to **Subscriber Management** > **Phone** and add a phone.
b) Add a line to the phone.
c) Navigate to **Subscriber Management** > **Agent Line** and identify the new phone as an agent line.
d) In Unified CM, navigate to **User Management** > **Application User** and verify that the new phone is associated with pguser.

Upgrade Prime Collaboration Assurance

Cisco supports the upgrade to Cisco Prime Collaboration Assurance 11.6 or later version.

To upgrade Prime Collaboration Assurance, follow the steps in the "Overview of Data Migration Assistant" topic in the *Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide* : https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.html.

Note For downloading the Prime Collaboration patch, refer to the Dowload Software page. Navigate to **Products > Cloud and System Management > Collaboration and Unified Communications Management > Prime Collaboration**.

Validate the Upgrade of Prime Collaboration Assurance

Take the following steps to validate the upgrade of Prime Collaboration Assurance.

Validation consists of adding a Contact Center customer component and verifying that the component is in Managed state. In this example, we add the Customer Voice Portal component.

Procedure

Step 1 Sign in to HCM-F as an administrator.

Step 2 Add a cluster.

a) Navigate to **Cluster Management** > **Cluster** and click **Add New**.
b) Enter the cluster name.
c) Select the customer associated with the cluster.
d) Select **CC** as the cluster type.
e) Select the cluster application version.
f) In the **Application Monitoring the Cluster** field, select the hostname of the Prime Collaboration Assurance instance.
g) Click **Save**.

Step 3 Add the Customer Voice Portal component.

a) Navigate to **Application Management** > **Cluster Application**.
b) In the General Information section, complete the following steps:
   - Click **Add New**.
   - In the **Application Type** field, select **CVP**.
   - Provide the hostname for the Customer Voice Portal component.
   - Select the appropriate cluster.
   - Click **Save**.
c) In the Credentials section, complete the following steps:
   - Click **Add New**.
   - In the **Credential Type** field, select **SNMP_V2**.
   - Provide the community string for the Customer Voice Portal component.
   - Select the **Read Only** access type.
   - Click **Save**.
   - Click **Add New**.
   - In the **Credential Type** field, select **ADMIN**.
   - Provide the administrator credentials. For Customer Voice Portal, the User ID is wsmadmin. Use the password that is configured for the OAMP web interface.
   - Select the **Read Only** access type.

- Click **Save**.

d) In the Network Addresses section, complete the following steps:

- Click **Add New**.
- In the **Network Space** field, select **Application Space**.
- Provide the IPv4 address and the hostname.
- Click **Save**.
- Click **Add New**.
- In the **Network Space** field, select **Service Provider Space**.
- Provide the NAT IPv4 address and the hostname.
- Click **Save**.

Step 4 Navigate to the **Current Inventory** (Inventory > Inventory Management) page.
The **State** column shows the Customer Voice Portal as **Managed**.

Upgrade Unified CCDM

To upgrade Cisco Unified Contact Center Domain Manager, follow the installation steps in the *Installation and Configuration Guide for Cisco Unified Contact Center Domain Manager*: https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

Validate the Unified CCDM Upgrade

Take the following steps to verify the upgrade of Unified CCDM.

Verification Task	Success Criteria
Provisioning Tests for Unified CCE	
Log in to the side A web server (portal). Create a Skill Group to test the provisioning from the side A web server. Run this test for each configured Unified CCE instance.	You can successfully create the Skill Group, and it is visible on side A, and on side B if applicable.
Log in to the side A web server (Portal). Create an Agent to test the provisioning from the side A web server. Run this test for each configured Unified CCE instance.	You can successfully create an Agent, and it is visible on side A, and on side B if applicable.
Create a Skill Group on the Administrative Workstation using the Cisco Skill Group Explorer tool. After a few minutes, verify that the Skill Group was imported into Unified CCDM.	The Skill Group is visible on side A, and on side B if applicable.
Replication Tests for Dual-Sided Deployments	

Verification Task	Success Criteria
Log in to the side B web server (Portal). Create a Skill Group to test Unified CCE provisioning from the side B web server. Run this test for each configured Unified CCE instance.	You can successfully create the Skill Group, and it is visible on side A.
Create a Skill Group on the Administrative Workstation using the Cisco Skill Group Explorer tool. After a few minutes, verify that the Skill Group was imported into Unified CCDM.	The Skill Group is visible on side A and on side B.
Log in to the side B web server (Portal). Create an IP phone to test Unified CM provisioning from the side B web server.	The IP phone is visible on side A and on side B.

Standard CC Upgrade

Upgrading Unified Customer Voice Portal Components

Upgrade the Unified Customer Voice Portal

Follow these steps to upgrade Cisco Unified Customer Voice Portal.

Procedure

Step 1 Back up the Unified CVP Operations Console configuration.

Step 2 Install the upgrade software.
For more information, see the "Unified CVP Upgrade" chapter in the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

Validate the Customer Voice Portal Upgrade

Follow these steps to validate the upgrade of Cisco Unified Customer Voice Portal.

Procedure

Step 1 Log in to the Operations Console.

Step 2 Validate the version of each component.

Step 3 Verify that all services are running.

Step 4 Make a test inbound PSTN call to an agent.

Upgrading Gateway Components

Upgrade Gateway Components

Follow the steps to upgrade Cisco Unified Border Element (SP Edition), Cisco Unified Border Element (Enterprise Edition), or a virtual peripheral gateway (vPGW). For more information, see the following topics and guides:

- For upgrading Cisco Unified Border Element Enterprise see *Common Upgrade Tasks* section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
- Upgrade the IOS on the Cisco ASR 1006 for Cisco Unified Border Element (SP Edition), on page 78
- Upgrading the Cisco ASR 1000 Series Router for Cisco Unified Border Element (SP Edition), on page 78
- The *vPGW Documentation* guides on the **Component Documentation** tab: https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-version-10-6-1/model.html

Procedure

Step 1 Back up all the gateways.

Step 2 Use the gateway consoles to back up component configurations.

Step 3 Upgrade the gateways.

Upgrading the Cisco ASR 1000 Series Router for Cisco Unified Border Element (SP Edition)

Cisco Unified Border Element (SP Edition) is used as a demarcation between the Cisco HCS network and an outside network, such as IMS, PSTN, or other SIP network. The ASR 1000 Series router is connected to the aggregation switches at the aggregation layer.

To upgrade this component, follow the procedures in the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*: https://www.cisco.com/c/en/us/support/routers/asr-1000-series-aggregation-services-routers/products-installation-and-configuration-guides-list.html.

When you have a redundant Cisco Unified Border Element (SP Edition) deployed, upgrade the component using the procedures in *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model* : https://www.cisco.com/c/en/us/support/routers/asr-1000-series-aggregation-services-routers/products-installation-and-configuration-guides-list.html.

To upgrade the ROMmon image on a Cisco ASR 1000 Series router, see the *Cisco ASR 1000 Series Routers ROMmon Upgrade Guide*: https://www.cisco.com/c/en/us/support/routers/asr-1000-series-aggregation-services-routers/products-maintenance-guides-list.html.

Upgrade the IOS on the Cisco ASR 1006 for Cisco Unified Border Element (SP Edition)

Use this procedure to upgrade Cisco Unified Border Element (SP Edition) ASR 1006 from version IOS 15.3(3)S to IOS 15.3(3)S4.

Before you begin

1. Ensure Cisco Unified Border Element (SP Edition) is configured for inter-chassis redundancy, with one Cisco ASR 1006 Aggregation Service Router in the Active state and the other in the Standby state.
2. Save the current configuration and download the software image to the boot flash of both of the ASR 1006 devices. It takes about 15 minutes.

Procedure

Step 1 Enter the CLI command **show redundancy application group <RG Group Id>** to determine which Session Border Controller (SBC) is Active. The Primary SBC is the Active chassis and the Secondary SBC is the Standby chassis.

Step 2 Download the new software version to the Primary and Secondary SBCs.

Step 3 On the Secondary SBC, enter the CLI command **boot system bootflash: <new image>** to change the boot variable to point to the new image.

Step 4 On the Primary SBC, perform an SBC sync from configuration mode. Enter the sbc configuration by running the CLI command **sbc <name of SBC>** and then run the CLI command **sync**.

Step 5 On the Secondary SBC, enter the CLI command **write memory** to save the running configuration.

Step 6 On the Primary SBC, enter the CLI command **redundancy > application redundancy > group # > shutdown** to shut down the redundancy group.
The Secondary SBC immediately becomes the Active Cisco Unified Border Element and all active calls are preserved. There is no service outage when the switchover of the Active SBC takes place.

Step 7 On the Primary SBC, change the boot variable to point to new software image and save the running configuration.

Step 8 Reload the Primary chassis for upgrade and wait for this SBC to come up with upgraded version.
It can take 10 to 12 minutes after the box is reloaded before the SBC reinitializes with the upgraded version.

Step 9 On the Secondary SBC, shut down the redundancy and immediately run the CLI command **no shutdown** of the redundancy group on the Primary SBC. Keep the duration between shutting down the redundancy group in the Secondary SBC and the **no shutdown** command in the Primary box as minimal as possible.
This step causes a service outage of approximately 4 minutes. The Primary box becomes the Active Cisco Unified Border Element (SP Edition) with upgraded software and starts servicing the calls.

Step 10 Save the running configuration in the Primary SBC.

Step 11 Reload the Secondary chassis for upgrade. When prompted to save the configuration before proceeding with the reload, enter “No” so that after the upgrade the Secondary SBC comes up in Standby mode.

Validate the Upgrade of Gateway Components

This section describes the steps to verify the upgrade of Cisco Unified Border Element (SP Edition), Metaswitch Perimeta Session Border Controller, Cisco Unified Border Element (Enterprise Edition), or a virtual peripheral gateway (vPGW).

Procedure

Step 1 Use Telnet or SSH to access the gateways and verify the version you upgraded to.

Step 2 Make an inbound call to an agent and verify the prompts. You can run the **debug voip dial peer** command to ensure that the inbound call uses the correct dial peer.

Upgrading the Unified Component

Upgrading the Unified Component

Follow the steps to upgrade the Cisco Unified Contact Center Enterprise Central Controller.

Unless otherwise indicated, the following steps reference topics in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Procedure

Step 1 Upgrade the Administration and Data server that is connected to Side A.
For more information, see the "Migrate HDS Database and Upgrade the Unified CCE Administration & Data Server" topic.

Step 2 Perform Enhancement of TempDB.

For more information, see the **Performance Enhancement of TempDB** section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Step 3 Reduce the reserved unused space for HDS

For more information, see the **Reduce Reserved Unused Space for HDS** section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Step 4 Bring the Side A logger and call router into service.
For more information, see the "Bring Upgraded Side A into Service" topic.

Step 5 Upgrade Cisco Unified Intelligence Center reporting templates.
For more information, see the *Installation and Upgrade Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html.

Step 6 Upgrade the Unified CCE Administration Client.
For more information, see the "Upgrade Unified CCE Administration Client" topic.

Step 7 Upgrade the gateways.
For more information, see the "Upgrade Peripheral Gateways" section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Step 8 Upgrade the Outbound Option Dialer.
For more information, see the "Upgrade Outbound Option Dialer" section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Step 9 Upgrade the CTI server.

For more information, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html

Upgrading Reporting Components

Upgrade Cisco Unified Intelligence Center

To upgrade Cisco Unified Intelligence Center, see the *Installation and Upgrade Guide for Cisco Unified Intelligence Center*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html.

Validate the Upgrade of Unified Intelligence Center

Take the following steps to validate the upgrade of Cisco Unified Intelligence Center.

Procedure

Step 1 Open the Unified OS Administration web page at the following URL, where [server-name] is the hostname or IP address of the node: `https://[server-name]/cmplatform`.

Step 2 Sign in with administrator credentials.

Step 3 Navigate to **Settings** > **Version** and verify the software version on the active and inactive partitions.

Upgrading Desktop Components

Upgrade Finesse

To upgrade Cisco Finesse, see the *Cisco Finesse Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html.

Note ES69 provides the ability to connect a maximum of two versions of Finesse to the same PG during the upgrade or migration process to facilitate the migration of agentsand supervisors to the new Finesse version. However, this mode of operation isnot supported for production use beyond the upgrade or migration phase.

Validate the Finesse Upgrade

Take the following steps to validate the upgrade of Cisco Finesse.

Procedure

Step 1 Ensure that the version of Finesse is the version you upgraded to. From the command line interface, you can run the **show status** command to verify the version.

Step 2 In the Finesse console, verify that all services are up.

Step 3 Log in to an agent and run desktop-initiated tests such as Call Hold, Transfer, and Conference.

Upgrade Desktop Clients

(Optional). To upgrade CTI OS Agent and Supervisor desktops, see the *CTI OS System Manager Guide for Cisco Unified ICM/Contact Center Enterprise*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Validate the Upgrade of Desktop Clients

Take the following steps to validate the upgrade of CTI OS Agent and Supervisor desktops.

Procedure

Step 1 Validate the version of each desktop.

Step 2 Sign in to an agent and run desktop-initiated tests such as Call Hold, Transfer, and Conference.

Upgrading Call-Processing Components

Upgrading Cisco Virtualized Voice Browser Components

Upgrade Cisco Virtualized Voice Browser

To upgrade the Cisco Virtualized Voice Browser, follow the steps in the "Cisco Virtualized Voice Browser Upgrade" chapter in the *Installation and Upgrade Guide for Cisco Virtualized Voice Browser Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-installation-guides-list.html

Validate the Cisco Virtualized Voice Browser Upgrade

Follow these steps to validate the upgrade of Cisco Virtualized Voice Browser portal.

Procedure

Step 1 Log into Cisco Virtualized Voice Browser portal.

Step 2 Check the existing configuration.

Upgrade Cisco Unified Communications Manager

Take the following steps to upgrade Cisco Unified Communications Manager.

Procedure

Step 1 Upgrade Cisco Unified CM.
For more information, see the *Upgrade Guide for Cisco Unified Communications Manager*: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Step 2 Uninstall and then reinstall the JTAPI client on the Cisco Unified CM peripheral gateway.
For more information, see the "Upgrade Cisco JTAPI Client on the Unified Communications Manager PG" topic in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Validate the Upgrade of Cisco Unified Communications Manager

Take the following steps to validate the upgrade of Cisco Unified Communications Manager.

Procedure

Step 1 In Cisco Unified CDM, add an IP phone. For more information, see the *Cisco Hosted Collaboration Solution End-User Provisioning Guide*: https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html.

Step 2 In Cisco Unified CM, verify that the phone was added.

Migration CC Upgrade

Migration to 2000 Agents Deployment Model

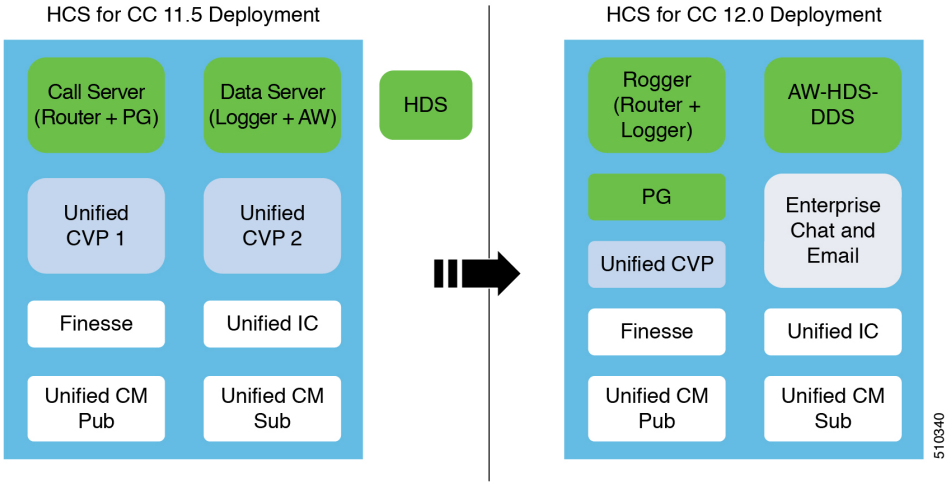
Common Ground Migration Process

The migration process for HCS for CC 500 and 1000 to 2000 agents deployment is designed for minimal Contact Center downtime. While you are upgrading Side A, Side B remains operational. After you upgrade Side A, contact center activity resumes on Side A while you upgrade Side B.

In Release 11.0(1), CS for CC 500 and 1000 agents deployment is moving to a new deployment model (HCS for CC: 2000 Agents). In release 11.5(1), HCS for CC 500 (deprecated in 11.5 and removed and unsupported from 11.6) is moving to a new deployment model (HCS for CC: 2000 Agents).The upgrade process also includes steps to migrate to this new model.

The layout of the VMs on the hardware changes as shown in the following diagram.

Figure 5: HCS for CC Deployment



Things to note include the following:

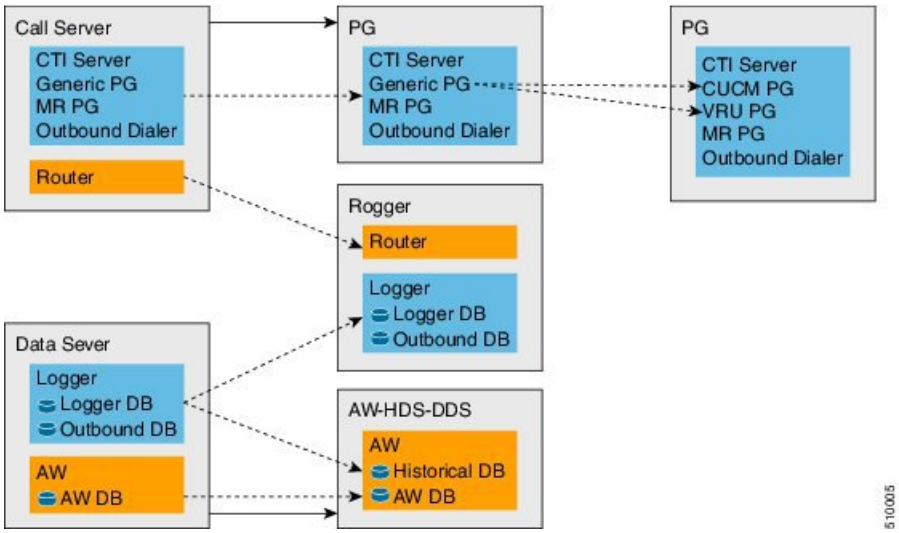
- The on-box Unified CCE Call Server and Data Server VMs change to on-box Unified CCE Rogger, PG, and AW-HDS-DDS.
- Two Unified CVP Servers are replaced with one Unified CVP Server that can support up to 3000 ports.
- Enterprise Chat and Email (ECE) can be coresident on box or deployed off box.

Note

- On-box ECE is supported on the B200 M4, C240 M4SX and C240 M5SX hardware only.
- On-box ECE is not supported in 2000 agent deployment model for two 500 agent instances in single pair of server

When you migrate to the HCS for CC 2000 Agent model, the Unified CCE Call Server and Data Server are migrated as shown in the following diagram.

Figure 6: HCS for CC Migration



Important The upgrade requires four maintenance windows:

- One maintenance window to shut down services on Side A to prepare for upgrade.
- A second maintenance window in the middle of the upgrade to cut over from Side B to Side A. You must bring down Side B before you bring up Side A.
- A third maintenance window after you upgrade Side B to synchronize Side A to Side B.
- A fourth maintenance window to finish migrating the Unified CCE Call Server to a Unified CCE PG.

This guide steps you through the upgrade and migration process for HCS for CC 2000 agents deployment, which includes the following major tasks:

- Meeting the system requirements for upgrade.
- Performing preupgrade tasks.
- Installing the Unified CCE Rogger.
- Migrating the Unified CCE Data Server to a Unified CCE AW-HDS-DDS.
- Migrating the Unified CCE Call Server to a Unified CCE PG.
- Upgrading all components on Side A.
- Cutting over from Side A to Side B, during which you bring Side B down and then bring Side A up.
- Migrating and upgrading all components on Side B.
- Synchronizing Side A and Side B.
- Performing postupgrade procedures.

Prerequisites and Important Considerations

- If your deployment includes Cisco Unified WIM and EIM, you must shut it down during the upgrade. Enterprise Chat and Email replaces Unified WIM and EIM in Release 11.6(1). Unified WIM and EIM is not supported from HCS for CC 11.5(1) onwards. After the upgrade is complete, you can install Enterprise Chat and Email.
- Live Data does not work during the migration and upgrade.
- Make sure that you have backups of Side A and Side B Call Servers, Data Servers, and Unified CVP Servers before you begin your upgrade.
- Use the Disaster Recover System (DRS) application to back up Finesse and Unified Intelligence Center system data.
  - Finesse: To access the DRS application, direct your browser to `https://FQDN of Finesse server:8443/drf/`. For more information, see the online help provided with the DRS application.
  - Unified Intelligence Center: To access the DRS application, direct your browser to `https://IP address of Unified Intelligence Center:8443/drf`. For more information, see the online help provided with the DRS application.
- After you begin the migration and upgrade process, you cannot back out of it. If you want to go back to the previous release, you must restore your VMs from your backup.
- Optionally, you can stage the Unified CCE Rogger off box before you begin the migration and upgrade to lessen your downtime.
- Plan out your hostnames. You may want to change the hostnames of the migrated Unified CCE components (Unified CCE Call Server, which becomes the Unified CCE PG, and Unified CCE Data Server, which becomes the Unified AW-HDS-DDS). If you change these hostnames, you must update them in other places (such as Finesse, PG Setup, and private network DNS entries).
- Make sure that you are running the minimum supported version of ESXi. For information about supported ESXi versions, see the *Virtualization for Cisco HCS for Contact Center* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/hcs_cc_virt.html.

Supported Upgrade

You can upgrade to this HCS for CC release from any version of HCS for CC Release 11.0(x).

Before you upgrade HCS for CC, you must upgrade on-box or off-box Unified Communication Manager Publisher and Subscribers to a version supported by this release of HCS for CC.

For information about supported versions, see the .

Hardware Refresh with Common Ground Upgrade

If you are performing a hardware refresh as part of the upgrade process, you must first prepare the target servers:

- Prepare Customer Site Servers
- *Virtualization for Cisco HCS for Contact Center* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/hcs_cc_virt.html

After you configure the servers, you can move the VMs to the servers and complete the common ground upgrade process.

NTP Configuration Requirements

HCS for Contact Center relies on time synchronization. Properly configuring NTP is critical for reliability of reporting data and cross-component communication. It's important to implement the requirements outlined in NTP and Time Synchronization.

Preupgrade Tasks

Perform the tasks in the following table in the order that they are listed.

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

Step	Task
1.	In the Unified CCE Administration **System Inventory** tool, check the status of the alerts for the hosts and for each virtual machine (VM). Resolve any issues. Make sure that inventory alerts are at 0 before you continue.
2.	Shut down Enterprise Chat and Email (ECE).
Reduce the impact of Side A services shutdown. Stopping Side A services to upgrade the components may force agents to sign out of their desktops and cause IP phones to rehome. If customers require agents to be active during the upgrade, you can reduce the impact of Side A shutdown by completing these preupgrade tasks.	
3.	Force phones to rehome to the Side B Unified Communications Manager Subscriber. Perform this step if the device pool for the agent phones contains only the Side A Unified Communications Manager Subscriber 1. In Unified Communications Manager Administration, add the Side B Unified Communications Manager Subscriber 2 as preferred and change the Subscriber 1 to secondary. Reset the phones after you change the device pool. You can skip this step if the device pool for the agent phones is configured with the Side A Unified Communications Manager Subscriber 1 as preferred and the Side B Unified Communications Manager Subscriber 2 as secondary. When you shut down Side A, Unified Communications Manager forces logout for agents using phones logged in to Subscriber 1 and rehomes their phones to Subscriber 2.
4.	Direct agents to sign in to the Side B Finesse Secondary node.
5.	Configure the Cisco IOS Enterprise Ingress Voice Gateway dial-peer priority so that calls are sent to the Side B Unified CVP Servers first, and then to the Side A Unified CVP Servers.

Step	Task
6.	To maintain reporting capabilities during the Side A upgrade, configure Unified Intelligence Center historical and real-time data sources to one of the following: • Side B Unified CCE AW-HDS-DDS Server • External HDS with Side B as the Central Controller preferred side See Configure Unified Intelligence Center Data Sources for External HDS, on page 88 for steps to configure Unified Intelligence Center data sources. For the **Datasource Host** and **Database Name** fields, enter values for the Side B Unified CCE AW-HDS-DDS Server with Side B as the Central Controller preferred side.
Complete Finesse preupgrade tasks	
7.	Save your current desktop layout configuration. Sign in to Finesse Administration on the primary Finesse node (`https://FQDN of primary Finesse server/cfadmin`). Copy the layout XML file from the Manage Desktop Layout gadget on the **Desktop Settings** tab. Save it as a text file on your local system. **Note** If you are currently running the default layout, the layout automatically upgrades to the new layout. To use the layout from the previous version, copy and paste the layout XML to the Manage Desktop Layout gadget after the upgrade is complete.
Complete Unified CVP preupgrade tasks	
8.	Complete the pre-upgrade tasks on Side A and Side B Unified CVP Servers and Operations Console Server. See Unified CVP Preupgrade Tasks, on page 90.
Complete Unified Communications Manager preupgrade tasks	
9.	Complete Unified Communications Manager preupgrade tasks. See Unified Communications Manager Preupgrade Tasks, on page 90.

Configure Unified Intelligence Center Data Sources for External HDS

Perform this procedure only if your deployment includes an external HDS and you wish to have a longer retention period.

Before you begin

Configure the Unified Intelligence Center SQL user for the External HDS databases before configuring the data sources (applicable for 4000 Agents and 12000 Agents). For more information, see Configure Unified Intelligence Center SQL User Account on the External HDS, on page 89

Procedure

Step 1 Sign in to Unified Intelligence Center with your Cisco Intelligence Center administrator account (https://<hostname/ IP address of CUIC Publisher>:8444/cuicui).

Step 2 Select **Configure** > **Data Sources**.

Step 3 Click **Data Sources** in the left panel.

Step 4 Select the **UCCE Historical** data source. Click **Edit**.

a) In the **Datasource Host** field, enter the IP Address of the external HDS server.
b) In the **Port** field, enter the AW SQL server port number. The default is **1433**.
c) In the **Database Name** field, enter **{instance}_hds**.
d) Leave the **Instance** field blank.
e) Select the **Timezone**.
f) In the **Database User ID**, enter the user name that you configured for the Cisco Unified Intelligence Center SQL Server user account.
g) Enter and confirm the SQL Server User **password**.
h) Select the **Charset** based on the collation of SQL Server installation.
i) Click **Test Connection**.
j) Click **Save**.

Step 5 Click the **Secondary** tab to configure Unified CCE Historical Data Source.

a) Check the **Failover Enabled** checkbox.
b) In the **Datasource Host** field, enter the IP address of the second external HDS server.
c) In the **Port** field, enter **1433**.
d) In the **Database Name** field, enter **{instance}_hds**.
e) Complete other fields as in the Primary tab.
f) Click **Test Connection**.
g) Click **Save**.

Step 6 Repeat this procedure for the **UCCE Realtime** datasource .

The **Database Name** for the Realtime Data Source is **{instance}_hds** .

Configure Unified Intelligence Center SQL User Account on the External HDS

Procedure

Step 1 Launch Microsoft SQL Server Management Studio .

Step 2 Navigate to **Security** >**Logins**, right-click **Logins** and select **New Login**.

This login is used when you configure the data sources for Cisco Unified Intelligence Center reporting.

Step 3 On the General Screen:

a) Enter the Login Name.
b) Select **SQL Server authentication**.
c) Enter and confirm the Password.
d) Uncheck **Enforce password policy**.

Step 4 Click **User Mapping**.

a) Check the databases associated with the AWdb.
b) Choose each database and associate it with the **db_datareader** and **public** role, and click **OK**.

Step 5 Click **OK**.

Unified CVP Preupgrade Tasks

Unified CVP Server and Unified CVP OAMP Server Preupgrade Tasks

Procedure

Step 1 Close all programs.

Step 2 Stop any third-party services and applications that are running on the server.

Step 3 Back up the `C:\Cisco\CVP` folder for all Unified CVP Servers.

Step 4 Back up the Operations Console as follows:

a) Log in to Operations Console.

b) On the Operations Console page, click **System** > **Export System Configuration** > **Export**, and save the CVP-OpsConsole-Backup.zip file.

c) Manually copy the sip.properties file from the directory `<CVP_HOME>\conf`. (Unified CVP Operations Console cannot export the sip.properties file.)

d) Copy the exported configuration and custom files onto network storage media or a portable storage media.

Unified Communications Manager Preupgrade Tasks

Procedure

Step 1 Ensure that you have the necessary license files for the new release.

Step 2 Back up your system. For more information, see the *Administration Guide for Cisco Unified Communications Manager* at this address: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Step 3 Obtain the upgrade file from Cisco.com and save it to an FTP or SFTP server. Folder names and filenames that you enter to access the upgrade file are case-sensitive. For more information, see the *Release Notes for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html

Prepare Side A for Upgrade

Before you begin, complete all tasks listed in Preupgrade Tasks, on page 87.

The user account that performs the upgrade must have access to PG Explorer and Network Trunk Group Explorer in Configuration Manager. Use the User List tool in Configuration Manager to provide access. For more information, see the Configuration Guide for Cisco Unified ICM/Contact Center Enterprise at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Perform the tasks in the following table during a maintenance window and in the order they are listed.

Important Make sure that you have backups of all components before you proceed.

Step	Task
1.	Sign in to Unified CCE Administration on the Side A Unified CCE Data Server. Select **System** > **Deployment**. **Note** When you sign in to Unified CCE Administration, a screen appears that contains warnings about virtual machine mismatches. You can ignore these warnings and close the screen. Switch out of the HCS for Contact Center 500 or HCS for Contact Center 1000 deployment model and into **UCCE 4000 Agents Rogger**.
2.	Disable configuration changes. Set the following registry key to **1** on the Side A Unified CCE Call Server: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance` The change is replicated to the other side automatically.
3.	On each of the following VMs, select **Unified CCE Service Control** on the desktop. Stop the Unified CCE services and change **Startup** to **Manual**: • Side A Unified CCE Call Server • Side A Unified CCE Data Server • External HDS associated with Side A (if used)
4.	If Outbound Option is used, on the Side B Unified CCE Call Server, select **Unified CCE Service Control** on the desktop. Stop the Dialer service and change **Startup** to **Manual**.

Migrate and Upgrade Side A

Before you begin, check the following to confirm that call activity has ended on Side A:

- In Unified CVP Diagnostic Portal, check that no Side A ports are in use.
- In the Unified Communications Manager RTMT tool, check that phones have migrated to Side B.

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

For best results, place upgrade media ISOs on local data stores. Make sure to remove them when the upgrade is complete.

Step	Task
Upgrade the Side A Unified CVP VMs	
1.	Remove the Unified CVP Server 2A VM.
2.	Update the Cisco IOS Enterprise Ingress Voice Gateway dial-peer configuration to remove Unified CVP Server 2A.
3.	Upgrade Unified CVP Server 1A. See Upgrade the Unified Customer Voice Portal, on page 77.
4.	Validate the Unified CVP upgrade. See Validate the Customer Voice Portal Upgrade, on page 77
Upgrade Side A Cisco Voice Gateway IOS Version if needed	
5.	Upgrade the Side A Cisco Voice Gateway IOS version to the minimum required by the upgraded HCS for CC release (or later). See Upgrade Cisco Voice Gateway IOS Version, on page 100. See the *HCS for CC Compatibility Information* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html.
Upgrade the Side A Finesse and Unified Intelligence Center VMs	
6.	Upgrade the VMware version on the Finesse Primary VM. See Upgrade the Virtual Machine Hardware Version, on page 104.
7.	Update the settings on the Finesse Primary VM. See Update VMware Settings for Cisco Finesse, on page 104.
8.	Upgrade the Finesse Primary node. See Upgrade Finesse, on page 81
9.	Upgrade the VMware version on the Unified Intelligence Center Publisher VM. See Upgrade the Virtual Machine Hardware Version, on page 104.
10.	Update the settings on the Unified Intelligence Center Publisher VM. See Update VMware Settings for Cisco Unified Intelligence Center, on page 104.
11.	Upgrade the Unified Intelligence Center Publisher node. See Upgrade Cisco Unified Intelligence Center, on page 81
Prepare for Side A Migration to HCS for CC 2000 Agent Rogger Deployment	
12.	Back up and export the Logger database and the Outbound Option (if used). See Back Up Database, on page 106.

Step	Task
13.	Back up and export your network configuration. See Back Up Network Configuration, on page 107.
Install the Side A Unified CCE Rogger (if not previously staged off box)	
14.	Create a VM for the Side A Unified CCE Rogger. Select **Rogger** from the drop-down list.
15.	Install Microsoft Windows Server on the Side A Unified CCE Rogger VM.
16.	Install VMware tools on the Side A Unified CCE Rogger VM.
17.	Configure the network adapters for the Side A Unified CCE Rogger. See Configure Network Adapters for Unified CCE Rogger and Unified CCE PG, on page 118 .
18.	Install antivirus software on the Side A Unified CCE Rogger.
19.	Configure the database drive for the Side A Unified CCE Rogger. See Configure Database Drive, on page 119.
20.	Set persistent static routes. See Set Persistent Static Routes, on page 121.
21.	Run Windows updates. See Run Windows Updates, on page 121.
22.	Add the Unified CCE Rogger to the domain.
23.	Install Microsoft SQL Server.
24.	Install Cisco Unified Contact Center Enterprise.
Configure the Side A Unified CCE Rogger	
25.	Add a UCCE Instance in Web Setup. See Add a UCCE Instance, on page 107.
26.	Configure SQL Server for the Logger database on the Unified CCE Rogger. See Configure SQL Server for CCE Components, on page 121.
27.	Configure the Logger database and log. See Configure the Logger Database and Log, on page 107.
28.	Import the Logger and Outbound Option databases that you backed up and exported in step 24. See Import the Logger and Outbound Databases, on page 108.

Step	Task
29.	Setup two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. See Two-Way Outbound Option Database Replication, on page 110
30.	Add a Unified CCE Router component in Web Setup. See Add a Unified CCE Router Component, on page 110.
31.	Add a Unified CCE Logger component in Web Setup. See Add a Unified CCE Logger Component, on page 111.
Convert the Side A Unified CCE Data Server and Unified CCE Call Server	
32.	Upgrade the VMware version on the Side A Data Server VM. See Upgrade the Virtual Machine Hardware Version, on page 104.
33.	Update the settings on the Side A Data Server VM. See Update VMware Settings on the Unified CCE Data Server, on page 112.
34.	Convert the Side A Unified CCE Data Server to a Unified CCE AW-HDS-DDS. See Convert Unified CCE Data Server to Unified CCE AW-HDS-DDS, on page 113.
35.	Update the real-time and historical data sources for Unified Intelligence Center to point to the Unified CCE AW-HDS-DDS. You must update the historical data source database name from <*instancename*>_sideA to <*instancename*>_awdb.
36.	Upgrade the VMware version on the Side A Call Server VM. See Upgrade the Virtual Machine Hardware Version, on page 104.
37.	Update the settings on the Side A Call Server VM. See Update VMware Settings on the Unified CCE Call Server, on page 114.
38.	Remove the Router from the Side A Unified CCE Call Server. See Remove the Router from the Unified CCE Call Server, on page 115. **Note** If CTI OS Server is present, use `\icm\CTIOS_bin\SETUP.exe` to remove it also. CTI OS is no longer supported. The Call Server is now a PG.
40.	Disable configuration changes on the Unified CCE Rogger. Change the following registry key to 1: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance`

Step	Task
41.	Run the Unified CCE Release installer on the Side A Unified CCE AW-HDS-DDS (former Data Server). See Upgrade , on page 122.
43.	Modify the Side A PG to point to the Unified CCE Rogger. See Modify the PG, on page 115.
44.	Modify the dialer to point to the Unified CCE Rogger (if using Outbound Option). See Modify the Dialer, on page 115.
Optional: Upgrade the External HDS associated with Side A (if used)	
45.	Upgrade the VMware version on the External HDS associated with Side A. See Upgrade the Virtual Machine Hardware Version, on page 104.
46.	Run the Unified CCE Release installer the External HDS associated with Side A. See Upgrade , on page 122.
47.	Update the Central Controller connectivity to point to the Unified CCE Rogger. See Update the Central Controller Connectivity, on page 116.
Optional: Install language pack	
48.	Install the language pack on the Side A Unified CCE Rogger, AW-HDS-DDS (former Data Server), PG (former Call Server), and External HDS associated with Side A (if used). See Install the Language Pack, on page 116.
Upgrade the Side A Unified Communications Manager Publisher and Subscriber 1	
49.	Upgrade the Side A Unified Communications Manager Publisher. See Upgrade Cisco Unified Communications Manager, on page 83
Optional: Change hostnames of the Unified CCE components	

Step	Task
50.	Optional: Change the hostnames of the Unified CCE components (AW-HDS-DDS and PG). **Note** You can perform this task when you reboot each component as part of the upgrade. If you do change the hostnames, also change them in the following places: • Cisco Finesse • PG Setup • Unified Intelligence Center - Historical and real-time • Private network DNS entries • Live Data—If you change the hostname of the AW-HDS-DDS (former Data Server), Live Data no longer connects to the AW-HDS-DDS after the Data Server hostname is removed from DNS. To fix this, do the following: 1. Run the following CLI command on the CUIC-LD-IdS Publisher: **unset live-data aw-access primary** 2. Restart Cisco Tomcat on the Side A AW-HDS-DDS.

Cisco Unified Customer Voice Portal Upgrade Procedures

Update VMware Settings for the Unified CVP Server

Update the virtual machine settings on the Unified CVP Reporting Server to match the 11.5(1) OVA file.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Select the hard disk to modify. In the **Disk Provisioning** pane, increase the provisioned size to 250 GB.
b) Click **Memory** and update the **Memory Size** to 10 GB .
c) Click **Video Card** and update the **Total video memory** to 8 MB.

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** to 3000 MHz.
b) Click **Memory** and update the **Reservation** to 10240 MB.

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

Step 6 Power on the virtual machine.

Step 7 Open the **Disk Management Tool** (right-click **Start** and choose **Disk Management** from the context menu).

Step 8 Select the C drive.

Step 9 In the **Disk 0** row, right- click **(C:)** and select **Extend Volume**.

The Extend Volume Wizard opens.

Step 10 Click **Next**.

Step 11 Accept the default settings and click **Next**.

Step 12 Click **Finish**.

Step 13 Restart the server.

Upgrade the Unified CVP Server

When you upgrade the Unified CVP Server, you must upgrade Unified Call Studio to the same version.

Procedure

Step 1 To retain the default media file format for this Unified CVP release, which is U-Law, skip Step 2 and proceed to Step 3.

Step 2 If you are changing from the U-Law to A-Law format:

a) Navigate to the `C:\Cisco\CVP\conf` location.

b) Convert the custom media files, such as custom applications and Whisper Agent-Agent Greeting (WAAG), and applications that are in U-Law to A-Law.

c) In the `cvp_pkgs.properties` file, add the **cvp-pkgs.PromptEncodeFormatALaw = 1** property at line 7 to enable the A-Law flag.

Note Ensure that you leave a space before and after the "=" sign.

Step 3 If you are changing from U-Law or A-Law to G729 format:

a) Navigate to the `C:\Cisco\CVP\conf` location.

b) In the `cvp_pkgs.properties` file, add the **cvp-pkgs.PromptEncodeFormatG729 = 1** property at line 7 to enable the G729 flag.

Note Ensure that you leave a space before and after the "=" sign.

Step 4 Mount the Unified CVP ISO image.

Step 5 From the CVP\Installer_Windows folder of the new release of Unified CVP installation DVD, run **setup.exe**. Follow the prompts as the installer guides you through the upgrade process.

Step 6 Restart the server.

What to do next

1. Transfer script and media files:
   a. Log in to the Operations Console and select **Bulk Administration** > **File Transfer** > **Scripts and Media**.
   b. In the **Select device type** field, select the Gateway.
   c. Move all Gateways to **Selected**.

d. Select **Default Gateway files**.

e. Select **Transfer**, and then select **OK** on the popup window.

Note If you have separate Ingress and VXML gateways, you must select the appropriate files and script for each component.

f. After configuring the application services in the gateways, log in to the gateway and use the Cisco IOS CLI command **call application voice load <service_Name>** to load the gateway download transferred files into the Cisco IOS memory for each Unified CVP service.

2. Restore any backed-up third-party libraries.

3. Re-license Unified CVP Servers with a license for the new version.

Restore any backed-up third-party libraries.

Update VMware Settings for the Unified CVP OAMP Server

Update the virtual machine settings on the Unified CVP Reporting Server to match the 11.5(1) OVA file.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Click **Memory** and update the **Memory Size** to 4 GB.

b) Click **Video Card** and update the **Total video memory** to 8 MB.

Step 4 Click the **Resources** tab.

a) Click **Memory** and update the **Reservation** field to 4096 MB.

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

Step 6 Power on the virtual machine.

Upgrade the Unified CVP Operations Console

The default media files are overwritten during the Unified CVP upgrade. Customized media files, such as whisper announcements and agent greetings, are not overwritten; they retain the format they had in previous releases.

Procedure

Step 1 To retain the default media file format for this Unified CVP release, which is U-Law, skip Step 2 and proceed to Step 3.

Step 2 If you are changing from the U-Law to A-Law format:

a) Navigate to the `C:\Cisco\CVP\conf` location.

b) Convert the custom media files, such as custom applications and Whisper Agent-Agent Greeting (WAAG), and applications that are in U-Law to A-Law.

c) In the `cvp_pkgs.properties` file, add the **cvp-pkgs.PromptEncodeFormatALaw = 1** property at line 7 to enable the A-Law flag.

Note Ensure that you leave a space before and after the "=" sign.

Step 3 If you are changing from U-Law or A-Law to G729 format:

a) Navigate to the `C:\Cisco\CVP\conf` location.

b) In the `cvp_pkgs.properties` file, add the **cvp-pkgs.PromptEncodeFormatG729 = 1** property at line 7 to enable the G729 flag.

Note Ensure that you leave a space before and after the "=" sign.

Step 4 Mount the Unified CVP ISO image.

Step 5 From the `CVP\Installer_Windows` folder of the Unified CVP installation DVD for this release, run `setup.exe`.

Step 6 Follow the instructions on the screen.

Step 7 Restart the server.

Obtain and Transfer the Upgrade License for Unified CVP

The Unified CVP Server and the Unified CVP Reporting Server require an updated license. The Operations Console runs without requiring a license.

Before you begin

To upgrade software, enter your contract number into the Cisco Product Upgrade Tool (PUT): https://tools.cisco.com/gct/Upgrade/jsp/index.jsp. If there is an entitlement to upgrade, the tool returns a Product Authorization Key (PAK); if not, the tool displays the option to purchase a PAK.

Use the PAK to generate a license file, using the Product License Registration Portal on Cisco.com: https://tools.cisco.com/SWIFT/LicensingUI/Home.

Save the license file locally so that you can transfer it using the Operations Console.

Procedure

Step 1 In the Operation Console, go to **Bulk Administration** > **File Transfer** > **Licenses**.

Step 2 In the **Device Association** panel, select the device type from the drop-down list. For example select Unified CVP Reporting Server or Unified CVP Server.

Step 3 Move the objects you want to license from **Available** to **Selected**.

Step 4 In the Licenses Files panel, select **Select new file** and then browse to the location where you saved the upgrade license.

Step 5 Click **Transfer**.

Cisco Enterprise Voice Gateway Upgrade Procedures

Upgrade Cisco Voice Gateway IOS Version

Perform this procedure for each gateway on the side you are upgrading.

For more information, see https://www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/upgrade.pdf.

Upgrade the Cisco Voice Gateway IOS version to the minimum version (or later) required by HCS for CC. See the *HCS for CC Compatibility Information* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html.

Procedure

Step 1 Copy the new image from the remote TFTP server into flash memory, making sure that you specify your own TFTP server's IP address and Cisco IOS filename.

Step 2 Verify that the new image was downloaded.

Step 3 Boot using the new image. Update the gateway config to boot using the new version.

Step 4 Reload the gateway to use the new image.

Unified CVP Reporting Server Upgrade Procedures

Unified CVP Reporting Server Preupgrade Tasks

Procedure

Step 1 Back up the Informix database by running C:\Cisco\CVP\bin\cvpbackup.bat.

This backs up the database to E:\cvp-db-backup\cvp-backup-data.gz.

Step 2 Turn off the scheduled purge, as follows:

a) Open **Administrative Tools** > **Task Scheduler**.
b) In the **Active Tasks**, double-click one of the Unified CVP tasks.
c) Select all of the Unified CVP-related tasks, right-click, and choose **Disable**

Step 3 Ensure that Unified CVP Reporting Server is not part of any domain and is part of a workgroup. Add it to the domain after the upgrade, if necessary.

Unload Data From Reporting Database

Note While the Cisco CVP CallServer service is stopped, no reporting data is sent to the Unified CVP Reporting Server.

Procedure

Step 1 Log in to the Unified CVP Reporting Server as 'cvp_dbadmin' user.

Step 2 Stop the **Cisco CVP Call Server** service from the Windows Service Manager.

Note Ensure that enough disk space is available to unload data. To check the disk space (in MB), run the query:

```
select sum(tabsize(tabname)) from systables where tabid>99
```

Step 3 Access the Unified CVP installation file.

Step 4 From the command prompt, change the directory to the migration folder.

Note You can also copy the migration folder to local disk and run the unload script directly.

Step 5 Locate the `migrate_unload.bat` file.

By default, the data is exported to `c:\migration`. Ensure that this path exists. If you want to change the default path, then update the path in *unl.sql*:

```
create procedure unld(path char(128) default "c:\migration\") RETURNING char(128)
```

Step 6 Run the following command to unload the Reporting Server database:

```
migrate_unload.bat
```

After running the script, a set of .unl files is created under the path provided. The .unl files are exported to `c:\migration` folder. This folder must have full access permission for cvp_dbadmin user.

Step 7 Copy the exported migration folder to the Unified CVP Reporting Server database.

Note Reduce the retention period for data and execute a purge to reduce the data to migrate.

Step 8 Start **Cisco CVP Call Server** service from Windows Service Manager.

Uninstall the Unified CVP Component from the Reporting Server VM

Before you begin

- Shut down all applications and close all open files.
- Close the Unified CVP component and related files.

Procedure

Step 1 Click **Start** > **Control Panel** > **Programs and Features**.

Step 2 Click **Cisco Unified Customer Voice Portal / Cisco Unified Call Studio**, and then click **Uninstall**.

Step 3 Click **Next**.

After uninstallation, the **Uninstall Complete** screen appears. Reboot the server.

Note The Unified CVP uninstallation procedure does not clean up all the files and folders, such as log files, media files, and folders that are generated postinstallation. Media folders with same names are replaced during the CVP installation process. User-created media files and folders remain unchanged during CVP upgrade. Create all the media folders in `wwwroot` and use the relative paths to simplify the migration process for the future releases that support a-law and mu-law files.

Update VMware Settings for the Unified CVP Reporting Server

Update the virtual machine settings on the Unified CVP Reporting Server to match the 11.5(1) OVA file.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

Step 4 Click the **Resources** tab.

a) Click **Memory** and update the **Reservation** field to 6144 MB.

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

Step 6 Power on the virtual machine.

Step 7 Open the **Disk Management Tool** (right-click **Start** and choose **Disk Management** from the context menu).

Step 8 Select the C drive.

Step 9 In the **Disk 0** row, right- click **(C:)** and select **Extend Volume**.

The Extend Volume Wizard opens.

Step 10 Click **Next**.

Step 11 Accept the default settings and click **Next**.

Step 12 Click **Finish**.

Step 13 Restart the server.

Load Data to Reporting Server Database

Procedure

Step 1 Open the Unified CVP installation file.

Step 2 Navigate to **CVP** > **Migration**.

Step 3 From the command prompt, change the directory to the migration folder.

Tip You can also copy the migration folder to the local disk and run the load script directly.

Step 4 On the local disk, locate the Unified CVP database backup file (cvpdb.tar) that you want to load into the Unified CVP database.

Note This is the backup file that you created when you unloaded data from the Unified CVP database.

Step 5 By default, the data is exported to c:\migration. Ensure that this path exists. If you want to change the default path, then update the path in *ld.sql*:

```
ld(path char(128) default "c:\migration\") RETURNING char(256)
```

Step 6 Run the following command as an administrator to load the Unified CVP database: `migrate_load.bat.`

Note If the backup cvpdb.tar file is located in `c:\cvpdata`, you must execute the script load as `migrate_load.bat`.

This script loads all the three Unified CVP Reporting databases with the previous call data to the Unified CVP Reporting database.

Step 7 Run the following command as an administrator to load the Unified CVP database: `migrate_load.bat -p <absolute path to tar file>.`

Note If the backup cvpdb.tar file is located in `c:\cvpdata`, you must execute the script load as `migrate_load.bat -p c: \cvpdata\cvpdb.tar`.

This script loads all the three Unified CVP Reporting databases with the previous call data to the Unified CVP Reporting database.

Save and Deploy the Unified CVP Reporting Server

Procedure

Step 1 On the Unified CVP OAMP server, open the Operations Console and log in.

Step 2 Navigate to **Device Management** > **Unified CVP Reporting Server**.

Step 3 Click the hostname of the Unified CVP Reporting Server.

Step 4 Click **Save and Deploy**.

Common Software Upgrade Procedures

Upgrade the Virtual Machine Hardware Version

Perform the following procedure on the VSphere Web Client on the Finesse and Unified Intelligence Center VMs.

Procedure

Step 1 Shut down the virtual machine.

Step 2 Right-click the virtual machine and choose **Compatibility > Upgrade VM Compatibility**.

Step 3 Click **Yes** to confirm upgrade.

Step 4 From the **Compatible with (*)** drop-down list, choose **ESXi 5.1 and later**.

Step 5 Click **OK** to save the settings.

Step 6 Power on the virtual machine.

Update VMware Settings for Cisco Finesse

Update the virtual machine settings for the Finesse Primary and Finesse Secondary VMs to match the OVA file.

Procedure

Step 1 Use the following CLI command to shut down the virtual machine: **utils system shutdown**

Step 2 Right-click the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Click **Memory** and update the **Memory Size** to 10 GB.

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** field to 5000 MHz.

b) Click **Memory** and update the **Reservation** field to 10240 MB.

Step 5 Change the Guest operation system version from “Red Hat Enterprise Linux 6 (64-bit)” to “CentOS 4/5/6/7 (64-bit)”.

Step 6 Click **OK**.

Step 7 Power on the virtual machine.

Update VMware Settings for Cisco Unified Intelligence Center

Update the settings on the Unified Intelligence Center Publisher and Subscriber to match the 11.5(1) OVA file.

Update the settings on the Unified Intelligence Center Publisher and Subscriber to match the OVA file.

Procedure

Step 1 Use the following CLI command to shut down the virtual machine: **utils system shutdown**

Step 2 Right-click the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Select the hard disk to modify. In the **Disk Provisioning** pane, change the **Provisioned Size** to 200 GB.
b) Click **Memory** and update the **Memory Size** to 16 GB.

Note If you deploy two 500 agent instances in single pair of blade then update the **Memory Size** to 10GB

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** field to 5500 MHz.
b) Click **Memory** and update the **Reservation** field to 16384 MB.

Step 5 Change the Guest operation system version from “Red Hat Enterprise Linux 6 (64-bit)” to “CentOS 4/5/6/7 (64-bit)”.

Step 6 Click **OK** to save your changes.

Step 7 Power on the virtual machine.

Upgrade VOS-Based Contact Center Applications from a Remote File System

Finesse and Unified Intelligence Center 11.0 support aligned partitions, but only with a fresh installation. When you upgrade from a previous release, the platform detects the unaligned partitions and displays the following error: `ERROR-UNSUPPORTED: Partitions unaligned`.

You can run Finesse and Unified Intelligence Center with the unaligned partitions without functional impact. To experience the benefits of aligned partitions, you must you perform a fresh installation after upgrade.

Procedure

Step 1 Upgrade VMware Settings

Before you perform an upgrade to 11.x, modify the following virtual machine settings (Red Hat Enterprise Linux version, Network Adapter, Memory and Video Card) as follows:

a) Power down the virtual machine.
b) From **VMWare VSphere**, select the virtual machine > **Edit Settings**. The Virtual Machine Properties window appears.
c) In the **Options** tab, select **General Options** and update the **Guest Operating System** from Red Hat Enterprise Linux 4(32-bit) to Red Hat Enterprise Linux 6(64-bit). Click **OK**.
d) Again select the virtual machine > **Edit Settings**.
e) In the **Hardware** tab, update the following parameters:

Memory > **Memory Size** > **10GB**.

Video Card > **Total Video Memory** > **8MB**.

f) Power on the virtual machine and continue with the upgrade.

Step 2 SSH to your Finesse, Unified Intelligence Center, or Unified Communications Manager system, or open it in the VM console in VSphere.

Step 3 Log in with the platform administration account.

Step 4 From the CLI, run the command **utils system upgrade initiate**.

Step 5 Choose **SFTP** or **FTP**.

Step 6 Follow the instructions provided by the `utils system upgrade initiate` command.

Step 7 Provide the location and credentials for the remote site.

Step 8 Enter SMTP server information when prompted. If you do not have an SMTP server, skip this step.

Step 9 At the Automatically switch versions if the upgrade is successful prompt, type **yes**.

Step 10 Verify that the upgrade was successful, as follows:

- **Finesse:** Sign in to the Finesse Agent Desktop (`https://<FQDN of Finesse server>/desktop`).

  Note After Finesse restarts, wait approximately 20 minutes before signing in to the desktop.

- **Unified Intelligence Center:** Sign in to Unified Intelligence Center (`https://<hostname>:8444/cuic`).
- **Unified Communications Manager:** Verify on the sign-in screen in the console.

Migration Procedures

Back Up Database

You must perform both a SQL backup of the Logger database and an ICMDBA backup of the configuration from the Logger database on the Data Server. Later in the migration process, the configuration backup will be imported into the Unified CCE Rogger. The SQL backup, which contains the historical data, will be imported into the Unified CCE AW-HDS-DDS.

Back up the databases on to a network share.

Procedure

Step 1 Use Microsoft SQL Server Backup and Restore utilities to back up and export the Logger and Outbound Option (if used) databases.

You can then use the backup to restore the historical data to the Unified CCE AW-HDS-DDS.

Step 2 On Side A, use ICMDBA to export the Logger database.

Note When upgrading side B, ensure ICMDBA export is performed from the Side B Logger database.

Step 3 Note the HDS customizable values.

Step 4 Copy the backup files to a shared location.

Back Up Network Configuration

Back up your network configuration to use when setting persistent static routes on the Unified CCE Rogger.

Procedure

Make note of the local static route configuration on the Unified CCE Call Server.

When you install and configure the Unified CCE Rogger, configure the local static routes to match this configuration.

Note This procedure assumes that the private network will be the same.

Configure Unified CCE Rogger

Add a UCCE Instance

Procedure

Step 1 Launch **Web Setup** in the VM you want installed or upgraded.

Step 2 Sign in as a domain user with local administrator permission.

Step 3 Click **Instance Management** and then click **Add**.

Step 4 In the **Add Instance** dialog box, choose the customer facility and instance.

Step 5 In the **Instance Number** field, enter 0.

Step 6 Click **Save**.

Configure the Logger Database and Log

Procedure

Step 1 Launch **ICMdba**.

Step 2 Navigate to **Server** > **Instance**.

Step 3 Right-click the instance name and choose **Create**.

Step 4 In the **Select Component** dialog box, choose the logger you are working on (Logger A or Logger B). Click **OK**.

Step 5 At the prompt "SQL Server is not configured properly. Do you want to configure it now?", click **Yes**.

Step 6 On the **Configure** page, in the **SQL Server Configurations** pane, check the defaults for Memory (MB) and Recovery Interval. Click **OK**.

Step 7 On the **Stop Server** page, click **Yes** to stop the services.

Step 8 In the **Select Logger Type** dialog box, choose **Enterprise**. Click **OK** to open the **Create Database** dialog box.

Step 9 Create the Logger database and log as follows:

a) In the **DB Type** field, choose the side (A or B).
b) In the **Storage** pane, click **Add**.
c) Click **Data**.
d) Choose the E drive.
e) Enter 130000 MB in the **Size** field.
f) Click **OK** to return to the **Create Database** dialog box.
g) Click **Add** again.
h) Choose the E drive.
i) Enter 3072 MB in the **Size** field.
j) Click **OK** to return to the **Create Database** dialog box.

Step 10 In the **Create Database** dialog box, click **Create**. Then click **Start**.

When you see the successful creation message, click **OK** and then **Close**.

Import the Logger and Outbound Databases

Import the Logger and Outbound Option (if used) databases that you previously exported to a network share.

Note Do not import the SQL backup of the Logger database into the Unified CCE Rogger. The SQL backup contains the historical data from the Data Server. Depending on the amount of data, it may be larger than the allocated disk size on the Rogger VM.

Procedure

Step 1 Launch **ICMdba**.

Step 2 Select the Unified CCE Rogger VM under Servers and expand the tree to <*instance name*>_sideA.

Step 3 Choose **Data** > **Import**.

Step 4 Browse to the location where you stored the backup of the Logger database and click **Open**.

Step 5 Click **OK** and then click **Import**.

Step 6 Click **Start** and then click **OK** on all messages that appear.

Step 7 Repeat the above steps for Side B.

Step 8 If you use Outbound Option and want to keep your Outbound Option customer database, restore the database with the Microsoft SQL Server Backup and Restore utilities. Repeat to set up Outbound Option database for Side B.

For more information see the *Outbound Option Guide for Unified Contact Center Enterprise* guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

Note Size of the Outbound Option database should not exceed 10 GB.

During the Technology Refresh upgrade, run the EDMT tool for each of the Logger and HDS databases to migrate data to the new version.

For detailed information on running the EDMT tool to migrate the data, see *Synchronizing or Updating Data from Logger or HDS Production Server to Staged 12.0(1) Server During Cut-over* in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide, Release 12.0(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Related Topics

Two-Way Outbound Option Database Replication, on page 110

Outbound Option for High Availability: Preliminary Two-Way Replication Requirements

If you plan to set up Outbound Option for High Availability two-way replication, there are several preliminary requirements.

Assign Privileges to Select Users

You must:

- Create a Microsoft SQL Server user and assign that user the sysadmin privilege. The username and password must be the same on Logger Side A and Logger Side B. (You use this username and password when you run Web Setup to configure Outbound Option and enable Outbound Option High Availability).
- Assign the sysadmin privilege to the NT authority/System user.

Verify Replication Feature Selected During Microsoft SQL Server Installation

If you intend to use Outbound Option High Availability Replication, you must select Replication as a feature when you install Microsoft SQL Server. To confirm the selection of the Replication feature:

1. From the Microsoft SQL Server installation disk, run `setup.exe`.
2. Select **Tools**, and click **Installed SQL Server Discovery Report**.
3. Confirm that the Replication feature is listed. If the feature is not listed, run the following command:

   ```
   setup.exe /q /Features=Replication /InstanceName=<instancename> /ACTION=INSTALL
   /IAcceptSQLServerLicenseTerms
   ```

   in which you enter the applicable instance name for your Microsoft SQL Server installation as the `<Instance Name>`.

Create an Outbound Option Database on Logger Side A and Side B

If you have enabled Outbound Option on Logger Side A in a previous release, you must:

- Stop all Logger services on Logger Side A.
- Perform a full database backup for the Outbound Option database on Logger Side A and restore it to Logger Side B. Use SQL Server Management Studio (SSMS) to complete this task.

If you have not enabled Outbound Option in a previous release, you must create an Outbound Option database on Logger Side A and Logger Side B. Use the ICMDBA utility to complete this task.

Note If the database replication fails and it is resolved, the Outbound Option HA must be enabled again. In such a case, you must again synchronize the databases on the Active and Standby sides. Perform a full database backup for the Outbound Option database on Active side and restore it to the Standby side.

Define Logger Public Interface Hostname on Logger Side A and Logger Side B

As you configure Outbound Option for High Availability, you must define the Logger Public Interface Hostname on both sides of the Logger. IP addresses are not allowed.

Make Campaign Manager and Dialer Registry Setting Customizations on Both Side A and Side B

If you customize any Campaign Manager and Dialer registry settings on one side, you must make the same updates for the registry settings on the other side.

Stop the Logger Service Before Enabling or Disabling Outbound Option High Availability

Before you enable or disable Outbound Option High Availability, stop the Logger service on the applicable side or sides.

Two-Way Outbound Option Database Replication

If you choose to enable Outbound Option, you can also enable Outbound Option High Availability. Outbound Option High Availability supports two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B.

You create an Outbound Option database on Side A and Side B either by:

- Using the ICMDBA tool (if you haven't set up Outbound Option at all).
- Backing up the Outbound Option database on Logger Side A and restoring it to Logger Side B (if you have already set up Outbound Option on Side A).

Also, create a Microsoft SQL Server user and assign that user the sysadmin privilege. The username and password must be the same on Logger Side A and Logger Side B. (You use this username and password when you run Web Setup to configure Outbound Option and enable Outbound Option High Availability.)

You then use Web Setup to configure the Loggers to support Outbound Option and Outbound Option High Availability.

Related Topics

Configure SQL Server for CCE Components, on page 121
Import the Logger and Outbound Databases, on page 108

Add a Unified CCE Router Component

Procedure

Step 1 Launch **Web Setup**.

Step 2 Choose **Component Management** > **Routers**.

Step 3 Click **Add**.

Step 4 On the **Deployment** page:

a) Select the appropriate side (Side A or Side B).
b) Select **Duplexed**.
c) Click **Next**.

Step 5 On the **Router Connectivity** page:

a) Configure the Private Interfaces and Public (Visible) Interfaces. Use the same hostname for Side A Normal and High Priority and the same hostname for Side B Normal and High Priority.
b) Click **Next**.

Step 6 On the **Enable Peripheral Gateways** page:

a) In the **Enable Peripheral Gateways** field, enter 1-3.
b) Click **Next**.

Step 7 On the **Router Options** page:

a) Check the **Enable Quality of Service (QoS)** check box.
b) Check the **Enable Application Gateway** check box.
c) Click **Next**.

Note This step applies to Side A only.

Step 8 On the **Router Quality of Service** page, accept the default values and click **Next**.

Step 9 On the **Summary** page, confirm the Router Summary is correct and then click **Finish**.

Add a Unified CCE Logger Component

You can (optionally) configure the Logger to enable Outbound Option and Outbound Option High Availability. Outbound Option High Availability facilitates two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Use the ICMDBA tool to create an outbound database on Side A and Side B; then set up the replication by using Web Setup.

Note Before you configure the Logger for Outbound Option High Availability:

- Create a Microsoft SQL Server user and assign that user the sysadmin privilege. You must use the same username and password on Logger Side A and Logger Side B. (You use this username and password in the following procedure to configure Outbound Option and enable Outbound Option High Availability.)
- Assign the sysadmin privilege to the NT authority/System user.

Procedure

Step 1 Launch **Web Setup**.

Step 2 Choose **Component Management** > **Loggers**.

Step 3 Click **Add**. Choose the Instance.

Step 4 On the **Deployment** page:

a) Select the appropriate side (Side A or Side B).
b) Select **Duplexed**.
c) Click **Next**.

Step 5 On the **Central Controller Connectivity** page:

a) Enter the hostnames for Side A and Side B for the Router Private Interface and Logger Private Interface.
b) Click **Next**.

Step 6 On the **Additional Options** page, click the **Enable Outbound Option** check box.

Step 7 Click the **Enable High Availability** check box to enable Outbound Option High Availability on the Logger.Checking this check box enables Outbound Option High Availability two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Two-way replication requires that you check this check box on the Additional Options page for both Logger Side A and Side B. If you disable two-way replication on one side, you must also disable it on the other side. You must enable Outbound Option in order to enable Outbound Option High Availability. Similarly, if you want to disable Outbound Option and you have enabled Outbound Option High Availability, you must disable High Availability (uncheck the **Enable High Availability** check box) before you can disable Outbound Option (uncheck the **Enable Outbound Option** check box).

Step 8 If you enable High Availability, enter a valid public server hostname address for **Logger Side A** and **Logger Side B**. Entering a server IP address instead of a server name is not allowed.

Step 9 If you enable High Availability, enter the **SQL Server Admin Credentials (Username and Password)**, which are required to establish two-way replication. The username and password must be the same on Logger Side A and Logger Side B, and the user must have the SQL Server System Admin privilege. SQL replication requires that the correct SQL system admin username and password be in place when setting up Outbound Option High Availability. Changing the password for the SQL user used to set up SQL replication in Outbound Option High Availability causes replication to fail until you disable High Availability and re-enable it with the new username and password. Because of this requirement, be careful about how andwhen you change the password for this user.

Step 10 Click **Next**.

Step 11 Review the **Summary** page, and click **Finish**.

Update VMware Settings on the Unified CCE Data Server

Update the virtual machine settings on the Side A and Side B Unified CCE Data Servers to match the OVA for the Unified CCE AW-HDS-DDS.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Click **Memory** and update the **Memory Size** to 16 GB.
b) Click **Video Card** and update the **Total video memory** to 8 MB.

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** field to 5000 MHz.
b) Click **Memory** and update the **Reservation** to 16384 MB.

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

Step 6 Power on the virtual machine.

Convert Unified CCE Data Server to Unified CCE AW-HDS-DDS

Before you begin

Make sure that you can restore from the network share to which you backed up the databases.

Stop the SQL Server service. Then, delete the SQL server data and log files to ensure that you have enough space to perform this procedure.

Procedure

Step 1 Rename the database.

a) Ensure that the SQL backup of the Side A Logger is copied to the AW-HDS-DDS network shared folder.
b) Restart the SQL Server service.
c) Open MS SQL Management Studio and run the following queries under the master database:

- `RESTORE FILELISTONLY from Disk='Path of the backup\<instancename>_sideA.bak'`

  Identify the logical filenames.

- ```
  Restore database <instance name>_hds
  from disk='Path of the backup\<instance name>_sideA.bak'
  with
  Move '<instancename>_sideA_data0' to
  'E:\MSSQL\DATA\<instancename>_hds_data0.mdf',
  Move '<instancename>_sideA_log0' to
  'E:\MSSQL\DATA\<instancename>_hds_log0.ldf',Stats=5
  ```

  Note Use the drive letter that the database is installed on.

  <instance name>_hds is the new database instance and <instance name>_sideA_data0 and log0 filenames are the results from the previous query.

d) In the **SQL Management Studio** window, select the <instance name>_hds database. Click **Properties**, and then select the **Files** pane. Change the logical filenames according to the HDS database:

- `<instance name>_sideA-log0` to `<instance name>_hds_log0`
- `<instance name>_sideA_data0` to `<instancename>_hds_data0`

e) Open a new query tab for the `<instance name>_hds` database and run the following query:

- Truncate table Logger_Type
- Truncate table Recovery
- Truncate table Logger_Admin
  ```

Step 2 Edit the Distributor.

a) Open Web Setup.
b) Select **Component Management** > **Administration and Data server component**.
c) Edit the Administration and Data server component to convert it to AW-HDS-DDS, as follows:

- Change the **Server Role** from **AW** to **AW-HDS-DDS**.
- Change the **Central Controller Connectivity** for the Router and Logger to use the hostnames for the side A and B Unified CCE Rogger VMs.

Step 3 Remove the Logger.

a) Open Web Setup.
b) Select **Component Management** > **Logger component**.
c) Select **Logger** and then click **Delete**.

Step 4 Remove the network adapter previously used for the private network.

a) In vSphere Client, right-click the virtual machine and choose **Edit Settings**.
b) Click the **Hardware** tab.
c) Remove the network adapter associated with the private network.

Update VMware Settings on the Unified CCE Call Server

Update the virtual machine settings on the Side A and Side B Unified CCE Call Servers to match the OVA for the Unified CCE PG.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Click **CPUs**. Update the **Number of Virtual Sockets** to 2 and the **Cores per socket** to 1.
b) Click **Memory** and update the **Memory Size** to 6 GB.
c) Click **Video Card** and update the **Total video memory** to 8 MB.

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** field to 4000 MHz.
b) Click **Memory** and update the **Reservation** to 6144 MB.

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

Step 6 Power on the virtual machine.

Remove the Router from the Unified CCE Call Server

Procedure

Step 1 On the Unified CCE Call Server, open Web Setup.
Step 2 Select **Component Management** > **Router component**.
Step 3 Select **Router** and then click **Delete**.

Modify the PG

Procedure

Step 1 Open Peripheral Gateway Setup.
Step 2 Select **PG1**.
Step 3 Click **Edit**.
Step 4 Click **Next** until you reach the **Peripheral Gateway Network Interfaces** dialog box.
Step 5 Update the Side A and Side B Router visible interfaces to point to the Unified CCE Rogger VMs.
Step 6 Click **Finish**.
Step 7 Repeat Step 2 through Step 6 for PG2.

Modify the Dialer

Perform this procedure if you use Outbound Option.

Procedure

Step 1 Launch the **Peripheral Gateway Setup**.
Step 2 In the **Instance Component** section, select **Dialer**.
Step 3 Click **Edit** and then click **Next**.
Step 4 In the **Outbound Option Dialer Properties** dialog box,
a. Enter the IP address for the Unified CCE Rogger in Side A in the **Campaign Manager server A** field.
b. Enter the IP address for the Unified CCE Rogger in Side B in the **Campaign Manager server B** field.
Step 5 Click **Next**.
Step 6 In the **Check Setup Information** dialog box, verify that the information is correct and then click **Next**.
Step 7 Check the **Yes, start the Unified ICM/CC Node Manager** check box and then click **Finish**.

Update the Central Controller Connectivity

Procedure

Step 1 Launch **Web Setup**.

Step 2 Choose **Component Management** > **Administration & Data Servers**.

Step 3 Check the **Administration & Data Server** check box and then click **Edit**.

Step 4 Click **Next** until you reach the Central Controller Connectivity page.

Step 5 On the Central Controller Connectivity page:

a) In the **Router Side A** and **Logger Side A** fields, enter the hostname of the Side A Rogger.
b) In the **Router Side B** and **Logger Side B** fields, enter the hostname of the Side B Rogger.
c) Click **Next**.

Step 6 Click **Finish**.

Install the Language Pack

If a customer requires a language other than the default (English), download the HCS for CC Language Pack executable from the Unified Contact Center Download Software page.

Install Language Pack

Install the Language Pack on the Unified CCE Data Servers and on any External HDS servers after upgrading them.

After you install the Language Pack, the Unified CCE Administration Sign In page has a language drop-down menu that lists all available languages. Select a language to display the user interface and the online help in that language.

Uninstall Language Pack

You can uninstall the Language Pack from Windows **Control Panel > Programs and Features > Uninstall or change a program**.

Unified Communications Manager Upgrade Procedures

Upgrade JTAPI on the PG

If you upgrade Unified Communications Manager, you must also upgrade the JTAPI client that resides on the Side A and Side B PGs.

You must install the new JTAPI client using the Unified Communications Manager Administration application. For more information, see the *Install Cisco JTAPI Client on Unified Communications Manager PG* section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* available here https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Procedure

Step 1 Uninstall the old JTAPI client from each Call Server:
a) Stop PG1A/PG1B.
b) Go to **Control Panel** > **Programs and Features**.
c) Uninstall the Cisco Unified Communications Manager JTAPI Client , following all prompts.

Step 2 To launch the Unified Communications Manager Administration application, enter the following URL in a Web browser on each Unified CCE Call Server: `https://<IP address of Unified Communications Manager Publisher>/ccmadmin`.

Step 3 Enter the username and password that you created when you installed and configured Unified Communications Manager.

Step 4 Select **Application** > **Plug-ins**.

Step 5 Click **Find** to see the list of applications.

Step 6 Click the download link next to **Cisco JTAPI 32-bit Client for Windows**.

Step 7 Choose **Run this program from its current location**. Click **OK**.

Step 8 If a Security Warning box appears, click **Yes** to install.

Step 9 When asked for the Cisco TFTP Server IP Address, enter the IP address of the Unified Communications Manager Publisher. Click **Next**.

Step 10 Choose **Next** or **Continue** through the remaining setup windows. Accept the default installation path.

Step 11 Click **Finish**.

Step 12 Start the PGs.

Transfer Unified CVP Scripts and Media Files

Create the notification destination and deploy to all of the Unified CVP devices.

Procedure

Step 1 Log in to the Operations Console and select **Bulk Administration** > **File Transfer** > **Scripts and Media**.

Step 2 In the **Select device type** field, select the Gateway.

Step 3 Move all Gateways to **Selected**.

Step 4 Select **Default Gateway files**.

Step 5 Select **Transfer**, and then select **OK** on the popup window.

If you have separate Ingress and VXML gateways, you must select the appropriate files and script for each component.

Step 6 Click **File Transfer Status** to monitor transfer progress.

Step 7 After configuring the application services in the gateways, log in to the gateway and use the Cisco IOS CLI command **call application voice load <service_Name>** to load the gateway download transferred files into the Cisco IOS memory for each Unified CVP service.

Configure Network Adapters for Unified CCE Rogger and Unified CCE PG

The Unified CCE Rogger and the Unified CCE PG each have two network adapters. You must identify them by MAC address and Network Label, rename them, configure them, and set the interface metric value.

Procedure

Step 1 Identify the MAC addresses and labels for the network adapters as follows:

a) From vSphere, select and right-click the VM.
b) Select **Edit Settings**. In the **Hardware** tab, click **Network adapter 1**. In the right panel, write down the last few digits of MAC addresses and note whether the label is PCCE Public or PCCE Private. For example, Network adapter 1 may have a MAC address that ends in 08:3b and the network label PCCE Public.
c) Repeat for Network adapter 2, noting its MAC address and label.
d) From the VM console, type **ipconfig /all** from the command line. This displays the adapter names and physical addresses.
e) Note the adapter names and physical addresses and match them with the MAC addresses and labels that you noted in VMware. For example, in ipconfig/all, Local Area Connection 2 may have a physical address that ends in 08-3b.
f) Match the MAC address of the network adapter that VMware identified as PCCE Public with the corresponding physical address of Local Area Connector. In this example, the physical address of Local Area Connection 2 (08-3b) matches the MAC address (08-3b) of Network adapter 1. This means that Local Area Connection 2 is PCCE Public.

Note Adapters may have a different name than Local Area Connection.

Step 2 Locate and rename the network adapters in Windows as follows:

a) In Windows, open the **Control Panel** > **Network and Sharing Center** and click **Change adapter settings**.
b) Right-click **Local Area Connection** and select **Rename**. Rename it to **PCCE Public** or **PCCE Private**, based on the matching you did above.
c) Right-click **Local Area Connection 2** and select **Rename**. Rename it to **PCCE Public** or **PCCE Private**, based on the matching you did above. In the example above, **Local Area Connection 2** is renamed to PCCE Public.

Step 3 Set the Properties for PCCE Public as follows:

a) Right-click **PCCE Public** and select **Properties**.
b) In the **Networking** tab, uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
c) Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
d) In the **General** tab for Internet Protocol Version 4, select **Use the following IP address** and enter **IP address**, **Subnet mask**, **Default gateway**, and DNS servers.
e) Click **OK** and **Close** to exit.

Step 4 Set the Properties for PCCE Private as follows:

a) Right-click **PCCE Private** and select **Properties**.
b) In the **Networking** tab, uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
c) Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
d) In the **General** tab for Internet Protocol Version 4, select **Use the following IP address** and enter **IP address** and **Subnet mask**.
e) Click **Advanced**.

f) Click the **DNS** tab and uncheck *Register this connection's addresses in DNS*.
g) In the DNS server, add a new A record that resolves to the private IP address. Also, create an associated pointer record for reverse lookups.

Note For hostnames in A records, append the letter p to indicate that it is a private address.

h) Click **OK** to exit.

Step 5 Assign an interface metric value for the network adapter:

a) Select the network adapter and right-click **Properties**.
b) In the **Networking** tab, select the appropriate Internet Protocol version and click **Properties**.
c) In the **Internet Protocol Version Properties** dialog box, click **Advanced**.
d) In the **IP Settings** tab, uncheck the **Automatic metric** checkbox and type a low value in the **Interface metric** text box.

Note A low value indicates a higher priority. Make sure that the Public Network card should have a lower value compared to the Private Network card.

By default, the value of the Interface Metric property for a network adapter is automatically assigned and is based on the link speed.

e) Click **OK** to save the settings.

Repeat the steps to assign an interface metric value for the internal/private cluster communication network adapter.

Configure Database Drive

Note Complete this procedure to create a virtual drive, if the virtual drive was not automatically created in the VM.

Procedure

Step 1 Add a virtual drive as follows:

Using Vsphere client:

a) Right-click the virtual machine and click **Edit Settings**.
b) In the **Hardware** tab, click on **Add**.

The **Add Hardware** window appears.

c) You can select the type of device you wish to add. Select **Hard Disk**, and then click **Next**.
d) Select the **Create a new virtual disk** option, and then click **Next**.
e) In the **Capacity** section, use the **Disk Size** box to assign the desired disk space, and then click **Next**.

Note Virtual machine templates for Logger, Rogger, AW, and HDS servers do not have a SQL database drive preprovisioned. The following reference table must be used to assign disk space to the virtual machine based on the type of validation errors will occur:

Virtual Machine Template	Default Second Disk Size
Logger	500 GB
Rogger	150 GB
AW-HDS-DDS	750 GB
AW-HDS	500 GB
HDS-DDS	500 GB
CVP Reporting Server	438 GB

You can custom size the SQL database disk space to meet the data retention requirements on an external AW-HDS-DDS server only, as calculated by the Database Estimator tool.

f) On the **Disk Provisioning** section choose **Thick provision Lazy Zeroed format**. Click **Next**.
g) In the **Advanced Options** section, retain the default options and then click **Next**.
h) In the **Ready to Complete** section, click **Finish** to create the hard disk.
i) Click **OK** to confirm the changes.

The Recent Tasks window at the bottom of the screen displays the progress.

Step 2 In Windows, navigate to **Disk Management**.

Step 3 Right-click on the **Disk 1** box and select **Online**.

Step 4 Initialize Disk 1 as follows:

a) Right-click on the **Disk 1** box and select **Initialize Disk**.
b) Check the **Disk 1** checkbox.
c) Select the **MBR (Master Boot Record)** radio button.
d) Click **OK**.

Step 5 Create a new disk partition as follows:

a) Right-click the graphic display of **Disk 1** and select **New Simple Volume**.
b) Click **Next** on the first page of the **New Simple Volume Wizard**.
c) On the **Specify Volume Size** page, retain the default volume size. Click **Next**.
d) On the **Assign Drive Letter or Path** page, assign drive letter (E). Click **Next**.
e) On the **Format Partition** page, format the partition as follows:

1. Select the **Format this volume with the following settings** radio button.
2. Click **Format Disk**.
3. Select File System as **NTFS** and click **Start**.
4. Select **Default** from the **Allocation unit size** drop-down menu.
5. Enter a value in the **Volume label** field.
6. Check the **Perform a quick format** checkbox.

7. Click **Next**.

f) Click **Finish**.

A popup window displays a message that you need to format the disk before you can use it.

The format is complete when the status changes to Healthy.

Step 6 Format the disk.

a) Click **Format disk**.
b) Click **Start**.
A popup displays a warning that formatting will erase all data on the disk.
c) Click **OK**.
d) When the format is complete, click **OK** to close the popup window.

Set Persistent Static Routes

To create a persistent static route with the **route add** command, you need the destination subnet, the subnet mask, the local gateway IP, and the interface number of the local Private Network interface:

`route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p`

You must launch the DOS prompt as an administrator to run the commands in this procedure.

Procedure

Step 1 On each , or PG VM, run `ipconfig /all`.
Record the `IPv4 Address`, `Subnet Mask`, and `Physical Address` (MAC address) for the Private Network interface.

Step 2 On each of these VMs, run `route print -4`.
Record the `Interface` for the Private Network. You can identify the correct interface by looking for its `Physical Address` (MAC address).

Step 3 On each of these VMs, run `route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p` to add a persistent static route for the remote Private Network.

Run Windows Updates

Procedure

Go to **Settings** > **Update & Security** and run Microsoft Windows Update.

Configure SQL Server for CCE Components

Configure SQL Server on both the Unified CCE Rogger and the Unified CCE AW-HDS-DDS.

Procedure

Step 1 Click the **Windows Start** icon, and then select the Downward Arrow icon to display all applications.

Step 2 Open **Microsoft SQL Server Management Studio**.

Step 3 Log in.

Step 4 Expand **Security** and then **Logins**.

Step 5 If the BUILTIN\Administrators group is not listed:

a) Right-click **Logins** and select **New Login**.
b) Click **Search** and then **Locations** to locate BUILTIN in the domain tree.
c) Type **Administrators** and click **Check Name** and then **OK**.
d) Double-click **BUILTIN\Administrators**.
e) Choose **Server Roles**.
f) Ensure that **public** and **sysadmin** are both checked.

Upgrade

- Make sure that the Windows update is not running in parallel when you install the release 12.0(1).
- The minimum disk space required to perform the upgrade is 2175 MB.
- During the upgrade process, the installer takes a backup of the existing configuration database. This backup is available in `drive\temp\<instance name_logger side><Major_CC Minor_ AW Minor>`.

Note The values for Major, CCMinor, AWMinor that are used in the backup folder name, are derived from the 11.0, 11.5 or 11.6 schema version of the system being upgraded (These are stored in the Version table of the CCE database and would translate into 181,3,3 for upgrades from 11.0(x) systems and 188,0,0 for 11.5(x) and 188.1.1 for 11.6(1) upgrades).

For example: `C:\Temp\Inst_sideA_181_3_3` from 11.0(x) upgrade, `C:\Temp\Inst_sideA_188_0_0` from 11.5(x) upgrades, and `C:\Temp\Inst_sideA_188_1_1` from 11.6(x) upgrades.

Note Note: This backup may fail if the space required to backup configuration data as calculated by the installer is not available on the system. This is independent of the minimum space requirement listed above.

Cut Over from Side B to Side A

Perform the following tasks during a maintenance window, in the order that they are listed.

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

Step	Task
Configure the Cisco Voice Gateway dial-peer priority	
1.	Reverse the Cisco IOS Enterprise Ingress Voice Gateway dial-peer priority configuration so that calls are sent to the Side A Unified CVP server first and then to Side B.
2.	Change the Unified CVP scripts as required so they do not point to DNs and labels on Unified CVP Server 2B.
Bring down Side B	
3.	On each of the following VMs, select **Unified CCE Service Control** on the desktop. Stop the Unified CCE services and change **Startup** to **Manual**: • Side B Unified CCE Call Server • Side B Unified CCE Data Server • External HDS with Side B as the Central Controller preferred side (if used)
4.	Power off the Finesse Secondary node VM in the vSphere client.
5.	Power off the Unified Intelligence Center Subscriber VM in the vSphere client.
6.	Transfer the Unified CVP scripts and media files to the gateways that are not currently in use on Side A. See Transfer Unified CVP Scripts and Media Files, on page 117.
7.	Shut down the following Unified CVP VMs from their Windows OS in the following order: **1.** Unified CVP Server 1B **2.** Unified CVP Server 2B **3.** Unified CVP Reporting Server **Important** At this point, Courtesy Callback no longer works. Unified CVP Reporting does not work unless you have an external Unified CVP Reporting Server.
8.	Power off the Unified Communications Manager Subscriber 2 VM in the vSphere client.
Bring up Side A	

Step	Task
9.	On each of the following VMs, select **Unified CCE Service Control** on the desktop. Start the Unified CCE services and change **Startup** to **Automatic**: • Side A Unified CCE Rogger • Side A Unified CCE AW-HDS-DDS (former Data Server) • Side A PG (former Call Server) • External HDS with Side A as the Central Controller (if used) Verify that services are started.
10.	If you changed the Unified Communications Manager device pool settings as part of the preupgrade, restore the original settings.
11.	Direct agents to sign in to the Side A Finesse Primary node.
12.	Change Unified Intelligence Center historical and real-time data sources to point to the Side A Unified CCE AW-HDS-DDS. See Configure Unified Intelligence Center Data Sources for External HDS, on page 88 for steps on how to configure Unified Intelligence Center data sources. Use the IP address of the Unified CCE AW-HDS-DDS.

Migrate and Upgrade Side B

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

For best results, place the upgrade media ISOs on local data stores. Make sure to remove them when the upgrade is complete.

Step	Task
Start the Side B Unified CVP components	
1.	Start Unified CVP Server 1B and then start the Unified CVP Reporting Server. **Note** You do not need to start Unified CVP Server 2B as it is removed during the migration.
Upgrade the Side B Unified CVP Servers	
2.	Remove the Unified CVP Server 2B VM.
3.	Update the Cisco IOS Enterprise Ingress Voice Gateway dial-peer configuration to remove Unified CVP Server 2B.

Step	Task
4.	Upgrade Unified CVP Server 1B. See Upgrade the Unified Customer Voice Portal, on page 77.
Upgrade Side B Cisco Voice Gateway IOS Version if needed	
5.	Upgrade the Side B Cisco Voice Gateway IOS version to the minimum required by the upgraded HCS for CC release (or later). See Upgrade Cisco Voice Gateway IOS Version, on page 100. See the *HCS for CC Compatibility Information* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.htmlfor IOS support information.
Upgrade the Side B Finesse and Unified Intelligence Center VMs	
6.	Power on the Finesse Secondary node VM in the vSphere client.
7.	Upgrade the VMware version on the Finesse Secondary VM. See Upgrade the Virtual Machine Hardware Version, on page 104.
8.	Update the settings on the Finesse Secondary VM. See Update VMware Settings for Cisco Finesse, on page 104.
9.	Upgrade the Finesse Secondary node. See Upgrade Finesse, on page 81
10.	Power on the Unified Intelligence Center Subscriber VM in the vSphere client.
11.	Upgrade the VMware version on the Unified Intelligence Center Subscriber VM. See Upgrade the Virtual Machine Hardware Version, on page 104.
12.	Update the settings on the Unified Intelligence Center Subscriber VM. See Update VMware Settings for Cisco Unified Intelligence Center, on page 104.
13.	Upgrade the Unified Intelligence Center Subscriber. See Upgrade Cisco Unified Intelligence Center, on page 81 **Note** Your configuration information migrates automatically to the upgraded version in the active partition.
Prepare for Side B Migration to HCS for CC 2000 Agent Rogger Deployment	
14.	Back up and export the Side B SQL database. See Back Up Database, on page 106.
Install the Side B Unified CCE Rogger	

Step	Task
15.	Create a VM for the Side B Unified CCE Rogger. Select **CCE Rogger** from the drop-down list.
16.	Install Microsoft Windows Server on the Side B Unified CCE Rogger VM.
17.	Install VMware tools on the Side B Unified CCE Rogger VM.
18.	Configure the network adaptors for the Side B Unified CCE Rogger. See Configure Network Adapters for Unified CCE Rogger and Unified CCE PG, on page 118 .
19.	Install antivirus software on the Side B Unified CCE Rogger.
20.	Configure the database drive for the Side B Unified CCE Rogger. See Configure Database Drive, on page 119.
21.	Set persistent static routes. See Set Persistent Static Routes, on page 121.
22.	Run Windows updates. See Run Windows Updates, on page 121.
23.	Add the Unified CCE Rogger to the domain.
24.	Install Microsoft SQL Server.
25.	Install Cisco Unified Contact Center Enterprise.
Configure the Side B Unified CCE Rogger	
26.	Add a UCCE Instance in Web Setup. See Add a UCCE Instance, on page 107.
27.	Configure SQL Server for the Logger database. See Configure SQL Server for CCE Components, on page 121.
28.	Configure the Logger database and log. See Configure the Logger Database and Log, on page 107.
29.	Import the Side B SQL database that you previously backed up in step 24. See Outbound Option for High Availability: Preliminary Two-Way Replication Requirements, on page 109
30.	Add a Unified CCE Router component in Web Setup. See Add a Unified CCE Router Component, on page 110.
31.	Add a Unified CCE Logger component in Web Setup. See Add a Unified CCE Logger Component, on page 111.

Step	Task
Convert the Side B Unified CCE Data Server and Unified CCE Call Server	
32.	Upgrade the VMware version on the Side B Data Server VM. See Upgrade the Virtual Machine Hardware Version, on page 104.
33.	Update the settings on the Side B Data Server VM. See Update VMware Settings on the Unified CCE Data Server, on page 112.
34.	Convert the Side B Unified CCE Data Server to a Unified CCE AW-HDS-DDS. See Convert Unified CCE Data Server to Unified CCE AW-HDS-DDS, on page 113.
35.	Update the real-time and historical data sources for Unified Intelligence Center to point to the Unified CCE AW-HDS-DDS. You must update the historical data source database name to <*instancename*>_awdb.
36.	Upgrade the VMware version on the Side B Call Server VM. See Upgrade the Virtual Machine Hardware Version, on page 104.
37.	Update the settings on the Side B Call Server VM. See Update VMware Settings on the Unified CCE Call Server, on page 114.
38.	Remove the Router from the Side B Unified CCE Call Server. See Remove the Router from the Unified CCE Call Server, on page 115. **Note** If CTI OS Server is present, remove it as well. CTI OS is no longer supported. The Call Server is now a PG.
39.	Run the Unified CCE installer on the Side B Unified CCE Rogger. See Upgrade , on page 122.
40.	Disable configuration changes on the Side B Unified CCE Rogger. Change the following registry key to 1: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterB\Router\CurrentVersion\Configuration\Global\DBMaintenance`
41.	Run the Unified CCE installer on the Side B Unified CCE AW-HDS-DDS (former Data Server). See Upgrade , on page 122.
42.	Run the Unified CCE installer on the Side B PG (former Call Server). See Upgrade , on page 122.
43.	Modify the Side B PG to point to the Unified CCE Rogger. See Modify the PG, on page 115.

Step	Task
44.	Modify the dialer to point to the Unified CCE Rogger (if using Outbound Option). See Modify the Dialer, on page 115.
Optional: Upgrade the External HDS associated with Side B (if used)	
45.	Upgrade the VMware version on the External HDS associated with Side B. See Upgrade the Virtual Machine Hardware Version, on page 104.
46.	Run the Unified CCE installer on the External HDS associated with Side B. See Upgrade , on page 122.
47.	Update the Central Controller connectivity to point to the Unified CCE Rogger. See Update the Central Controller Connectivity, on page 116.
Optional: Install language pack	
48.	Install the language pack on the Side B Unified CCE Rogger, AW-HDS-DDS, PG (formerly Call Server), and External HDS (if used). See Install the Language Pack, on page 116.
Upgrade Side B Unified Communications Manager Subscriber 2	
49.	Power on the Unified Communications Manager Subscriber 2 VM in the vSphere client.
50.	Upgrade the Side B Unified Communications Manager Subscriber 2. See Upgrade Cisco Unified Communications Manager, on page 83
51.	Upgrade JTAPI on the Side B PG (formerly Call Server). See Upgrade JTAPI on the PG, on page 116.
Optional: Change hostnames of the Unified CCE components	

Step	Task
52.	Optional: Change the hostnames of the Unified CCE components (AW-HDS-DDS and PG). **Note** You can perform this task when you reboot each component as part of the upgrade. If you do change the hostnames, you must also change them in the following places: • Finesse • PG Setup • Unified Intelligence Center - Historical and real-time • Private network DNS entries • Live Data—If you change the hostname of the AW-HDS-DDS (former Data Server), Live Data no longer connects to the AW-HDS-DDS after the Data Server hostname is removed from DNS. To fix this, do the following: 1. Run the following CLI command on the CUIC-LD-IdS Publisher: **unset live-data aw-access secondary** 2. Restart Cisco Tomcat on the Side B AW-HDS-DDS.

Sync Side A to Side B

Perform these tasks during the third maintenance window to sync Side A and Side B.

Step	Task
1	Set the following registry key to 0 on either the Side B Unified CCE Rogger: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router B\Router\CurrentVersion\Configuration\Global\DBMaintenance`
2	On each of the following VMs, select **Unified CCE Service Control** on the desktop. Start the Unified CCE services and change Startup to Automatic, in this order: 1. Side B Unified CCE Rogger 2. Side B Unified CCE AW-HDS-DDS 3. Side B PG 4. External HDS with Side B as the Central Controller preferred side (if used) Verify that the services are started.

Migrate Call Server to Unified CCE PG

Perform these tasks in a maintenance window. Perform these tasks on the Side A PG (former Call Server) and then on the Side B PG and in the order they are listed.

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

Note You can continue the maintenance window that you used to sync Side A and Side B or you perform them in a later maintenance window.

Step	Task
For the Side A PG (formerly Call Server):	
1.	Add a new CUCM PG. See Add a New CUCM PG, on page 131.
2.	Remove the Dialed Number configuration. See Remove Dialed Number Configuration, on page 131.
3.	Remove the Agent Targeting Rule configuration. See Remove Agent Targeting Rule Configuration, on page 132.
4.	Remove the Network Trunk configuration. See Remove Network Trunk Configuration, on page 132.
5.	Remove the Label configuration. See Remove Label Configuration, on page 133.
6.	Remove the Unified CVP PIMs from PG Explorer. See Remove Unified CVP PIMs, on page 133.
7.	Install CUCM PG3. See Install the CUCM PG, on page 133.
8.	Install CG3. See Install CG3, on page 135.
9.	Modify PG1 to VRU PG. See Modify PG1 to VRU PG , on page 135.
10.	Uninstall CG1. See Uninstall CG1, on page 136.
11.	In Finesse Administration, configure the CTI port information in CTI Server Settings for Side A. Restart the Cisco Tomcat service and the Cisco Finesse Tomcat service.

Step	Task
For the Side B PG (formerly Call Server):	
12.	Repeat Step 7 through Step 10 for the Side B PG.
13.	In Finesse Administration, configure the CTI port information in CTI Server Settings for Side B. Restart the Cisco Tomcat service and the Cisco Finesse Tomcat Service.
Redo Dialed Number, Agent Targeting Rule, and Network Trunk Group configuration as required	

Add a New CUCM PG

Procedure

Step 1 In the **Configuration Manager** window, expand **Tools** > **Explorer Tools**.

Step 2 Open **PG Explorer**.

Step 3 Click **Add PG** and then enter the following values in the **Logical Controller** pane:

- In the **Name** field, enter **`CUCM_PG`**.
- For **Client type**, choose **CUCM**.
- Enter **Primary CTI Address** and **Secondary CTI Address** as mentioned in the generic PG.

Step 4 Delete the peripheral that was automatically created in the previous step.

Step 5 Click **Save**.

Step 6 Drag the CUCM peripheral from the Generic PG to the CUCM PG.

A message appears asking if you are sure you want to move the peripheral to a different PG. Click **Yes** to confirm.

Step 7 Rename the Generic PG to VRU PG and change the Client type to **VRU**.

Step 8 Click **Save**.

Note Make sure to record the Logical Controller ID of the new CUCM PG. You need to enter it when you install the PG.

Remove Dialed Number Configuration

Before you begin

Dialed numbers that are mentioned in any scripts must be removed from the scripts before you perform this procedure. Make sure that they are removed from all versions (not just the active scripts).

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.
Step 2 In Configuration Manager, expand **Tools** > **List Tools**.
Step 3 Open **Dialed Number / Script Selector List**.
Step 4 Select **Routing Client** as the existing VRU for Unified CVP 2A / Unified CVP 2B and then click **Retrieve**.
Step 5 Select each dialed number associated to the routing client and then click **Delete**.
Step 6 Click **Save**.

Remove Agent Targeting Rule Configuration

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.
Step 2 Expand **List Tools**.
Step 3 Select **Agent Targeting Rule**.
Step 4 Remove the Routing Client for Unified CVP 2A and Unified CVP 2B.
Step 5 Click **Save**.

Remove Network Trunk Configuration

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.
Step 2 Expand **Explorer Tools**.
Step 3 Select **Network Trunk Group Explorer**.
Step 4 From the **PG** list, select **VRU_PG** and then click **Retrieve**.
Step 5 Expand **GENERIC** and click any trunk group that appears beneath it.
Step 6 Click **Multiple**.
Step 7 In the **Delete Multiple** dialog box, select all of the CVP 2A and CVP 2B trunk groups and then click **Delete**.
Step 8 Click **OK**.
Step 9 Click **Save**.

Remove Label Configuration

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 Expand **List Tools**.

Step 3 Select **Label List**.

Step 4 Remove the labels associated with Unified CVP 2A and Unified CVP 2B.

Remove Unified CVP PIMs

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 Expand **Tools** > **Explorer Tools**.

Step 3 Open **PG Explorer**.

Step 4 Select **VRU PG**.

Step 5 Delete the PIMs for Unified CVP 2A and Unified CVP 2B.

Step 6 Click **Save**.

Install the CUCM PG

Procedure

Step 1

Step 2 On the PG (former Call Server), choose **Start** > **All Programs** > **Unified CCE Tools** > **Peripheral Gateway Setup**.

Step 3 In the **Instance Component** section, click **Add**.

Step 4 Click **Peripheral Gateway**.

Step 5 In the **Peripheral Gateways Properties** dialog, do the following:

a) Check the **Production Mode** check box.
b) Check the **Auto start at system start up** check box.
c) Check the **Duplexed Peripheral Gateway** check box.
d) From the **PG Node Properties ID** drop-down list, select **PG3**.
e) Select the appropriate side (Side A or Side B).
f) In the **Client Type Selection** section, add **CUCM** to the Selected Types.
g) Click **Next**.

Step 6 In the **Peripheral Gateway Managers** section of the **Peripheral Gateway Component Properties** dialog box, click **Add**.

Step 7 Select **CUCM** and **PIM1** and click **OK**.

Step 8 Check the **Enabled** check box.

Step 9 In the **Peripheral Name** field, enter CM.

Step 10 In the **Peripheral ID** field, enter the Peripheral ID that the system generated in Step 8 after the CUCM PG was added.

Step 11 In the **Agent Extension Length** field, enter the extension length for this deployment.

Step 12 In the **CUCM Parameters** section, do the following:

a) In the **Service** field, enter the hostname of the Unified Communications Manager Subscriber.
b) In the **User ID** field, enter pguser.
c) In the **User Password** field, enter the password of the user that will be created on Unified Communications Manager.
d) In the **Mobile Agent Codec** field, choose either **G711 ULAW/ALAW** or **G.729**.

Step 13 Click **OK**.

Step 14 In the **Logical controller ID** field, enter the Logical controller ID of the CUCM PG that you created previously in PG Explorer.

Step 15 In the **CTI Call Wrapup Data delay** field, enter 0. Click **Next**.

Step 16 In the **Device Management Protocols Properties** dialog box, do the following:

a) For Side A PG:
   - Select **Side A preferred**.
   - For Side A properties, select **CallRouter is local**.
   - For Side B properties, select **CallRouter is remote (WAN)**.

b) For Side B PG:
   - Select **Side B preferred**.
   - For Side A properties, select **CallRouter is remote (WAN)**.
   - For Side B properties, select **CallRouter is local**.

c) For both sides:
   - Accept the default in the Usable Bandwidth (kbps) field.
   - Accept the default in the Heartbeat Interval (100ms) field.

d) Click **Next**.

Step 17 In the **Peripheral Gateway Network Interfaces** dialog box, complete the interface fields:

a) Enter the Private and Visible network interface hostnames. For the PG, use the same hostnames for private and private high. For the Router, enter the hostname of the Unified CCE Rogger Side A for the Router visible A and Router visible A high interfaces. Enter the hostname of the Unified CCE Rogger Side B for the Router visible B and Router visible B high interfaces.
b) For the Side A PG, in the **Private Interfaces** section, click **QoS**. Check **Enable QoS** and click **OK**.
c) For both the Side A and Side B PGs, in the **Visible Interfaces** section, click **QoS**. Check **Enable QoS** and click **OK**.

d) Click **Next**.

Step 18 In the **Check Setup Information** dialog box, click **Next**.

Step 19 In the **Setup Complete** dialog box, click **Finish**.

Install CG3

Procedure

Step 1 Launch **Peripheral Gateway Setup**.

Step 2 In the **Instance Components** section, click **Add**.

Step 3 In the Component Selection dialog box, click **CTI Server**.

a) Check **Production mode**.
b) Check **Auto start at system startup**.
c) Check **Duplexed CTI Server**.
d) From the CG node properties pane ID list, choose **CG3**.
e) Enter 3 in the CG node properties ICM system ID field.
f) Click the appropriate side.
g) Click **Next**.

Step 4 In the CTI Server Component Properties dialog box, do the following:

a) For Side A, enter `42027` for non-secured connection and `42030` for secured connection in the Client Connection Port Number field.
b) For Side B, enter `43027` for non-secured connection and `43030` for secured connection in the Client Connection Port Number field.

Note Before establishing secured connection between components, ensure that the security certificate management process is completed. For more information on secured connections, see Security Guide for Cisco Unified ICM/Contact Center Enterprise

Step 5 Click **Next**.

Step 6 In the CTI Server Network Interface Properties dialog box, fill in all interface fields and then click **Next**.

Step 7 Check your setup information and then click **Next**.

Step 8 Click **Finish**.

Modify PG1 to VRU PG

Procedure

Step 1 Open Peripheral Gateway Setup.

Step 2 Select **PG1**.

Step 3 Click **Edit**.

Step 4 In the **Client Type Selection** section, remove **CUCM**.

Step 5 Click **Next**.

Step 6 In the **Peripheral Gateway Component Properties** dialog box, remove the CUCM PIMs that were used for connecting to CUCM and click **Next**.

Step 7 In the **Device Management Protocol Properties** dialog box, click **Next**.

Step 8 In the **Peripheral Gateway Network Interfaces** dialog box, enter the hostname or IP address of the Unified CCE Rogger Side A for the Router visible A and Router visible A high interfaces. Enter the hostname or IP address of the Unified CCE Rogger Side B for the Router visible B and Router visible B high interfaces.

Step 9 Click **Next**.

Step 10 In the **Check Setup Information** dialog box, click **Next**.

Step 11 Check the **Yes, start the Unified ICM/CC Node Manager** check box and click **Finish**.

Uninstall CG1

Procedure

Step 1 Open Peripheral Gateway Setup.

Step 2 Select **CG1**.

Step 3 Click **Delete**.

Step 4 Click **OK**.

Switch into HCS for Contact Center Deployment

Step	Task
1.	In **Unified CCE Administration** > **Deployment**, switch into the HCS for Contact Center: 2000 Agents deployment type.
2.	Validate the HCS for Contact Center deployment in Unified CCE Administration. See Validate HCS for Contact Center Deployment and Build System Inventory, on page 136.
3.	Direct agents to sign in to the correct Finesse node.

Validate HCS for Contact Center Deployment and Build System Inventory

Validate the HCS for Contact Center deployment using the Unified CCE Administration Deployment tool.

As you complete the procedure, you are prompted only for missing information; you may not need to perform each step.

Postupgrade Tasks

You can perform these postupgrade tasks in any order.

Component	Task
Finesse	Complete postupgrade tasks for the Finesse desktop layout. See Finesse Desktop Layout Postupgrade Tasks, on page 137. Finesse server need a restart after the upgrade of peripheral gateways (PG).
Unified CVP	Upgrade Call Studio. Upgrade Unified Call Studio, on page 137
	Optional: Synchronize the metadata files for the Unified CVP REST API using the sync-up tool. See Initiate Metadata Synchronization for Unified CVP Rest API, on page 138.
All	Optional: Upgrade ESXi. See Upgrade VMware vSphere ESXi, on page 139.

Finesse Desktop Layout Postupgrade Tasks

If you do not use a custom desktop layout, do the following after upgrading Cisco Finesse:

1. Click **Restore Default Layout** on the Manage Desktop Layout gadget to add all updates from the new default desktop layout.
2. Disable the Agent Queue Statistics gadget from the default desktop layout for the Agent role. This gadget is not supported for the Agent role in HCS for CC deployments.
3. **Optional:** Enable Live Data Report gadgets for the Agent role.

If you use a custom desktop layout, do the following after upgrading Finesse:

1. Add optional Live Data Report gadgets for the Agent role after upgrading Cisco Finesse.
2. If you want to restore a previous layout for the desktop, sign in to the Administration Console on the primary Finesse node. Copy and paste your saved layout XML into the Manage Desktop Layout gadget.

Upgrade Unified Call Studio

Before you begin

Obtain a new license for Unified Call Studio because licenses for earlier versions are invalid with the latest version.

Note Upgrade of Call Studio is supported through the migration process.

Procedure

Step 1 Open Call Studio, right-click any existing project in the Navigator view, choose **Export**.

The **Export** wizard opens.

Step 2 Navigate to **General** > **File System**, and click **Next**.

Note From the list displayed by the Export wizard, select multiple projects to export them simultaneously.

Step 3 Browse to the directory where the projects will be exported and click **OK** and then click **Finish**.

Step 4 Uninstall the Call Studio software.

For more information, see the Unified CVP/Call Studio Uninstallation section.

Step 5 Install the Call Studio software.

For more information, see the Install Unified Call Studio section.

Install Unified Call Studio

Procedure

Step 1 Mount the Unified CVP software (including CVP Studio) installer ISO image, and run setup.exe.

Step 2 On the **Welcome** screen, click **Next**.

Note If you click **Cancel** here or on the dialog screens that follow before the **Ready to Install the Program** screen, the installation is canceled. The **Exit Setup** dialog box appears.

Step 3 Review **Copyrights to Products** used by Call Studio and click **Next**.

Step 4 Review and accept the license agreement, and click **Next**.

Step 5 On the Choose Destination Location screen, select the folder where setup will install files. By default, it is `C:\Cisco\CallStudio`.

Step 6 On the **InstallShield Wizard Complete** screen, click **Install**.

Step 7 Click **Finish** to exit the wizard.

The Call Studio software is installed on your computer.

Initiate Metadata Synchronization for Unified CVP Rest API

In the Unified CVP REST API architecture, information of media files on Media Server and VXML applications on a VXML server is saved on a WSM Server as metadata in Derby database. This metadata information is created, updated, and deleted by the REST API calls. There may be situations where the metadata may go out of sync with files on VXML Servers and Media Servers. Examples are addition and deletion of Unified CVP Servers, deployment of apps and media files by a tool other than the REST API, and Unified CVP Media Server or the VXML server upgraded from a version where the REST API was not supported.

A command line tool “metasynch.cmd” is available at `C:\Cisco\CVP\wsm\CLI` to enable synchronization of metadata with the files on VXML Servers and Media Servers. The tool internally uses the Synch up API to perform the synchronization. It takes three arguments- WSM user name, WSM user password, and server type (MEDIA, VXML or VXML_ STANDALONE). Based on the server type information, all servers of the

respective server type are synchronized. If the server type argument is not provided, metadata is synchronized with all media servers and VXML servers configured in OAMP.

In case of an upgrade, the media files and VXML applications are present in the Media Servers and VXML Servers but corresponding metadata information is not present in the WSM Server. The absence of metadata information limits a user from using the REST API to access, update, and delete existing media files and VXML applications on the Media Server and the VXML Server.

Synchronize Metadata Files Using Sync-Up Tool

To invoke **`metasynch.cmd`**, complete the following steps.

Procedure

Step 1 On the Unified CVP OAMP Server, navigate to the `C:\Cisco\CVP\wsm\CLI` location.

Step 2 Run the **metasynch.cmd** file with following arguments:

- **wsm username**
- **wsm password**

Example:

```
metasynch.cmd wsmusername wsmpassword MEDIA
```

Usage : metasynch [options] username password [servertype]

servertype : MEDIA/VXML

options : -help -? print this help message

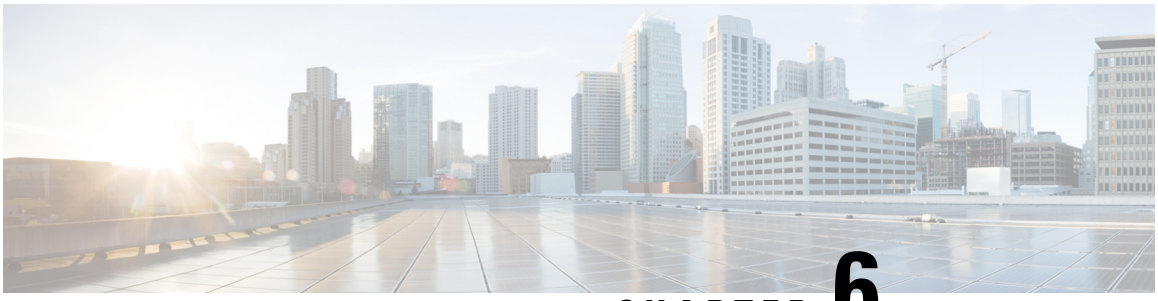
Note The server type argument should be MEDIA, VXML type. If the server type argument is not provided, the metadata is synched with all the VXML applications on VXML servers and all media files on Media servers. Logs for synch command tool can be found at the following location:

```
C:\Cisco\CVP\wsm\CLI\log\SyncTool.log
```

Upgrade VMware vSphere ESXi

If you use VMware vCenter Server in your deployment, upgrade VMware vCenter Server before upgrading VMware vSphere ESXi.

Upgrade VMWare vSphere ESXi on Side A and Side B servers to the latest version supported with this release of HCS for CC. HCS for CC uses standard upgrade procedures, which you can find using VMware documentation (https://www.vmware.com/support/pubs/).



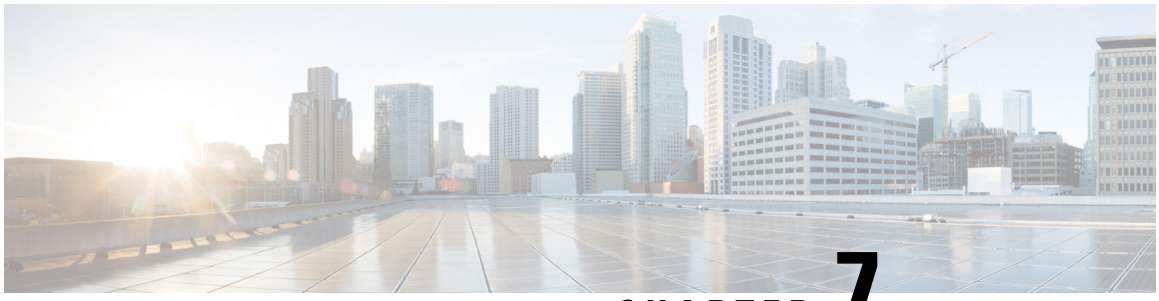
CHAPTER 6

Uninstall Unified CCE Release 12.0(1)

Uninstallation of base CCE

Uninstallation of Cisco Unified ICM/CCE base 12.0 is not supported for CCE components that are deployed on Windows Server using the ICM-CCE-Installer. However, support for uninstallation and re-installation of client installer packages like Administration Client and Internet Script Editor continues.

Note The option to roll back to previous versions is only available with maintenance releases.



CHAPTER 7

Appendix

Core Components Server

Install Unified Contact Center Enterprise

Procedure

Step 1	Add the virtual machine template into the domain.
Step 2	Mount the Unified Contact Center Enterprise ISO image to the virtual machine.
Step 3	From the `ICM-CCE-CCH` Installer directory, run `setup.exe` and follow the InstallShield procedures.
Step 4	In the **Select the installation method** window, select **Fresh Install**, then click **Next**.
Step 5	In the **Maintenance Release (MR)** window, keep the **Maintenance Release Location** field blank, then click **Next**.
Step 6	In the **Installation Location** window, select the drive `C`, then click **Next**.
Step 7	In the **Ready to Copy Files** window, click **Install**.
Step 8	In the **Installation Complete** window, click **Yes, I want to restart my computer now**, then click **Finish**.
Step 9	Run the mandatory update before applying any ES, if you have a fresh install or Technology Refresh upgrade planned for PCCE or UCCE 12.0(1), on the Windows Server 2016. You can download the `CCE 12.0 Mandatory Update for Fresh Install/Tech Refresh` from https://software.cisco.com/download/home/268439622/type/280840583/release/12.0(1).
Step 10	Apply the Unified Contact Center Enterprise maintenance release, if applicable.
Step 11	Unmount the Unified Contact Center Enterprise ISO image.
Step 12	Move the virtual machine template back to the workgroup.

Related Topics

Create Virtual Machines, on page 59

Mount ISO File

Create Golden Template for Unified CCE Rogger, on page 49

Create Golden Template for Unified CCE Router, on page 50
Create Golden Template for Unified CCE Logger, on page 50
Create Golden Template for Unified CCE AW-HDS-DDS, on page 51
Create Golden Template for Unified CCE AW-HDS, on page 51
Create Golden template for Unified CCE HDS-DDS, on page 52
Create Golden Template for Unified CCE PG, on page 53

Install Unified CVP Server

Procedure

Step 1 Mount the Unified CVP ISO image to the virtual machine.

Step 2 Copy the current Engineering Specials (ES) to the local drive.

Note Ignore this step if there are no Engineering Specials.

Step 3 From the `CVP\Installer_Windows` directory, run `setup.exe`.

Step 4 In the **Install Shield Wizard** window:

a) Accept the license agreement and click **Next**.
b) In the **Select Packages** window, select **CVP Server**, then click **Next**.
c) In the **Voice Prompt Encode Format Type** window, select **U-Law Encoded Wave Format**, then click **Next**.
d) In the **Choose Destination Location** window, select the folder locations for the CVP Installation Folder and the Media Files Installation Folder, then click **Next**.
e) In the **X.509 Certificate** window, enter the information that you want to include in the certificate.
f) In the **Ready to Install the Program** window, click **Install**.
g) Click **Yes, I want to restart my computer now**, Click **Finish**.

Step 5 Copy the required **Cisco Unified CVP Engineering Special** file to the desktop.

Step 6 If Unified CVP Engineering Specials are available, follow the Install Shield wizard. Ignore this step if there are no Engineering Specials.

Step 7 Add any custom media files to the appropriate location.

Step 8 Unmount the ISO image.

Related Topics

Mount ISO File
Create Golden Template for Unified CVP Server, on page 53

Install Unified CVP OAMP Server

Procedure

Step 1 Mount the Unified CVP ISO image to the virtual machine.

Step 2 From the `CVP\Installer_Windows` directory, run `setup.exe`.

Step 3 Accept the license agreement, click **Next**.

Step 4 In the **Select Packages** window, select the **Operations Console** option, then click **Next**.

Step 5 In the **Voice Prompt Encode Format Type** window, select **U-Law Encoded Wave Format** and click **Next**.

Step 6 On the **Choose Destination Location** window, accept the default locations, then click **Next**.

Step 7 In the **X.509 certificate** window, enter the information that you want to include in the certificate, then click **Next**.

Step 8 In the **Ready to Install** window, click **Install**.

Step 9 Enter the operations console password that meets the criteria detailed on the **Operations Console Password** window, then click **Next**.

Step 10 Click **Yes, I want to restart my computer**, then click **Finish**.

Step 11 Unmount the Unified CVP ISO image.

Related Topics

Mount ISO File

Create Golden Template for Unified CVP OAMP Server, on page 54

Install Unified CVP Reporting Server

Procedure

Step 1 Mount the Unified CVP ISO image to the virtual machine.

Step 2 Copy the current Engineering Specials (ES) to the local drive.

Note Ignore this step if there are no Engineering Specials.

Step 3 From the `CVP\Installer_Windows` directory, run `setup.exe`.

Step 4 In the **Install Shield Wizard** window:

a) Accept the license agreement, then click **Next**.

b) In the **Select Packages** window, select **Reporting Server**, then click **Next**.

c) In the **Choose Destination Location** window, select the folder location for the CVP Installation Folder, then click **Next**.

d) In the **X.509 certificate** window, enter the information that you want to include in the certificate, then click **Next**.

e) In the **Choose the Database data and backups drive** window, enter the name of the drive (typically E), and click **Next**.

f) In the **Database size selection** window, select **Standard (250GB)** or **Premium (375GB)**, then click **Next**.

Note Select **Standard** for 500 agent deployment and **Premium** for other HCS agent deployments.

g) In the **Ready to Install** window, click **Install**.

h) Enter the CVP Reporting Server password when prompted.

It can take some time for the database to install.

i) Restart the server after installation.

Step 5 Copy the required CVP Engineering Special file to the desktop.

Step 6 If Unified CVP Engineering Specials are available, follow the Install Shield wizard to install them. Ignore this step if there are no Engineering Specials.

Step 7 Unmount the ISO image.

Related Topics

Mount ISO File

Create Golden Template for Unified CVP Reporting Server, on page 54

Install Publishers/Primary Nodes of VOS-Based Contact Center Applications

Before you begin

DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, Cisco Finesse and Cisco Identity Service (IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Procedure

Step 1 Create a virtual machine for your VOS-based contact center application using the OVA.

Step 2 Mount the ISO image for the software to the virtual machine.

Step 3 Select the virtual machine, power it on, and open the console.

Step 4 Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.

b) In the **Success** screen, select **OK**.

c) In the **Product Deployment Selection** screen:

If your product is any one of the following, choose the product and click **OK**.

- Cisco Unified Communications Manager
- Cisco Finesse
- Cisco Virtualized Voice Browser

If your product is Cisco Unified Intelligence Center, you can choose from one of the following options:

- Cisco Unified Intelligence Center
- Live Data
- Cisco Identity Service (IdS)
- Cisco Unified Intelligence Center with Live Data and IdS
- For the 2000 agent reference design, choose the coresident deployment option **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center with Live Data and Cisco Identity Service (IdS) on the same server.

- For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center** , **Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

d) In the **Proceed with Install** screen, select **Yes**.
e) In the **Platform Installation Wizard** screen, select **Proceed**.
f) In the **Apply Patch** screen, select **No**.
g) In the **Basic Install** screen, select **Continue**.
h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

Note For Live Data servers, use the same timezone for all the nodes.

i) In the **Auto Negotiation Configuration** screen, select **Continue**.
j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the **DHCP Configuration** screen, select **No**.
l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
m) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.
n) Enter your DNS client configuration. Select **OK**.
o) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
p) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
q) In the **First Node Configuration** screen, select **Yes**.
r) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.
s) In the **Security Configuration** screen, enter the security password and select **OK**.
t) In the **SMTP Host Configuration** screen, select **No**.
u) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
v) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

Step 5 Unmount the ISO image.

Related Topics

Create Virtual Machines, on page 59
Mount ISO File

Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications

Note This task is required for installation of the subscriber/secondary nodes of the three VOS-based contact center applications: Cisco Finesse, Cisco Unified Communications Manager, and Cisco Unified Intelligence Center.

Before you begin

DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, and Cisco Finesse. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Before you install the subscriber/secondary nodes, you must install the publisher/primary nodes and configure the clusters.

Procedure

Step 1 Create a virtual machine for your VOS-based contact center application using the OVA.

Step 2 Mount the ISO image for the software to the virtual machine.

Step 3 Select the virtual machine and power it on, and open the console.

Step 4 Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.

b) In the **Success** screen, select **OK**.

c) In the **Product Deployment Selection** screen:

If your product is any one of the following, choose the product and click **OK**.

- Cisco Unified Communications Manager
- Cisco Finesse
- Cisco Virtualized Voice Browser

If your product is Cisco Unified Intelligence Center, you can choose from one of the following options:

- Cisco Unified Intelligence Center
- Live Data
- Cisco Identity Service (IdS)
- Cisco Unified Intelligence Center with Live Data and IdS
- For the 2000 agent reference design, choose the coresident deployment option **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center with Live Data and Cisco Identity Service (IdS) on the same server.
- For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center** , **Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

Step 5 Follow the Install wizard, making selections as follows:

a) In the **Proceed with Install** screen, select **Yes**.
b) In the **Platform Installation Wizard** screen, select **Proceed**.
c) In the **Apply Patch** screen, select **No**.
d) In the **Basic Install** screen, select **Continue**.
e) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

Note For Live Data servers, use the same timezone for all the nodes.

f) In the **Auto Negotiation Configuration** screen, select **Continue**.
g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.
i) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
j) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.
k) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
l) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
m) In the **First Node Configuration** screen, select **No**.
n) In the warning screen, select **OK**.
o) In the **Network Connectivity Test Configuration** screen, select **No**.
p) In the **First Node Access Configuration** screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select **OK**.
q) In the **SMTP Host Configuration** screen, select **No**.
r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

Step 6 Unmount the ISO image.

Related Topics

Create Virtual Machines, on page 59
Mount ISO File