Cisco Hosted Collaboration Mediation Fulfillment Planning Guide, Release 10.6(1)

First Published: June 30, 2015

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

CONTENTS

Preface

CHAPTER 1

Preface

Purpose

This document provides instructions for planning Cisco HCM-F in Cisco Hosted Collaboration Solution (HCS), including information on HCM-F services and resource requirements.

Audience

This document provides information for service providers who are responsible for planning Cisco HCM-F in Cisco Hosted Collaboration Solution (HCS). This guide requires knowledge of Cisco Hosted Collaboration Solution (Cisco HCS).

Organization

The following table provides the organization of this guide.

Part	Description
Part 1	Introduction Contains information on Cisco HCM-F installation, services, backup and restore, and integration within Cisco HCS.

Part	Description
Part 2	The Cisco HCM-F Administrative Interface Contains field descriptions and procedures for Service Inventory, Infrastructure Manager, and Platform Manager.
Part 3	Troubleshooting and Monitoring Contains information on troubleshooting and monitoring Cisco HCM-F.
Part 4	Service Inventory Report Format Contains information on the service report format for Service Inventory.

Note Use this document in conjunction with the *Developer Guide for Cisco Hosted Collaboration Mediation Fulfillment*.

Conventions

This document uses the following conventions.

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A non quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in screen font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
`italic screen` font	Arguments for which you supply values are in italic screen font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.

Convention	Description
< >	Non printing characters, such as passwords, are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver Means the *described action saves time*. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means *the information contains useful tips*.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that can result in equipment damage or loss of data.

Warnings use the following conventions:

Warning This warning symbol means danger. You are in a situation that can cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.

Obtain Documentation and Submit Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance please contact us by sending email to export@cisco.com.

CHAPTER 1

Planning Considerations

Prerequisites

Before you plan the initial system requirements and planned growth for the Cisco Hosted Collaboration Solution (HCS). To make sure you have seen the Collaboration Sizing Tool at tools.cisco.com/cucst

You should also review the following documents:

- *Cisco Hosted Collaboration Solution, Release 10.6(1) Solution Reference Network Design Guide*
- *Cisco Hosted Collaboration Solution, Release 10.6(1) Capacity Planning Guide*

VMware Planning Considerations

Use VMware's Distributed Resource Scheduler and high availability features to improve the resiliency of HCM-F nodes. For more information, see www.vmware.com.

Note VMware's Distributed Resource Scheduler is not supported for UC applications.

Service Inventory planning considerations

Service Inventory is a Cisco HCM-F service that queries Cisco Unified Communications Domain Manager 10.6(1) daily and reports detailed configurations of customers, subscribers, and devices for all Unified Communications Manager and Cisco Unity Connection application instances. The Service Inventory report also provides a summary of all customers, UC clusters, users, and end devices deployed within HCS.

Note For deployments of both Cisco Unified Communications Domain Manager 8.x and Cisco Unified Communications Domain Manager 10.x, Service Inventory pulls customer information from both and generates a report file (or files) for all customers.

Complete the following steps when planning service inventory:

Procedure

Step 1 Plan to deploy an SFTP server (and an optional backup SFTP server) with adequate capacity to receive Service Inventory report files. A typical compressed file size would be 8-10 MB for 200,000 users.

Step 2 Decide whether the files will be pushed or pulled, scheduled or automatic.

Step 3 Decide which application you will use to parse the detailed inventory data into a form that can be used by your business system.

Note For details on Service Inventory reports and their formatting, see the *Cisco Hosted Collaboration Solution, Release 10.6(1) Maintain and Operate Guide*.

License Planning Considerations

HCS License Manager

HCS License Manager is an HCM-F service that provides centralized license management for HCS. HCS License Manager extends the functionality of Prime License Manager (formerly Enterprise Licence Manager) beyond the scope of one enterprise for use by service providers. HCS License Manager is used to assign each cluster to an Prime License Manager. HCS License Manager aggregates license usage by each cluster from each Prime License Manager into a License Summary report.

Consider the steps in the following procedure for HCS License Manager planning:

- Use one HCS License Manager for each installation of HCS.
- Set up each Prime License Manager in the HCS License Manager.
- Load HCS licenses on a Prime License Manager before configuring the Prime License Manager on an HCS License Manager
- When new customers are onboarded, their clusters must be assigned to an Prime License Manager through the HCS License Manager. Do not use the native management interface of Prime License Manager to assign a cluster. Always use the HCS License Manager to assign clusters to Prime License Manager.

Prime License Manager

Prime License Manager manages licensing for Unified Communications Manager clusters, and Cisco Unity Connection servers for multiple customers deployed in HCS. Typically, multiple customers are assigned to the same Prime License Manager server. HCS License Manager allows a customer's clusters to be assigned to different Prime License Managers.

HCS licenses are registered to and loaded and activated onto the Prime License Managers deployed in HCS. The Prime License Managers deploy the HCS licenses to the UCM clusters and Unity Connection servers that are assigned.

Take the following actions for Prime License Manager planning:

Procedure

Step 1 Determine if you need multiple instances of Prime License Manager, which would be the case in either of the following scenarios:

- If a Service Provider has resellers and wants to segregate the HCS licenses it provides to each reseller
- If there will be more than 1000 Unified Communications application clusters in the HCS deployment

Step 2 Install the Prime License Manager on the same management network as HCM-F so that Prime License Manager can access all Unified Communications application clusters.

Step 3 Install standalone Prime License Managers in the HCS Management domain. Set up each customer domain firewall to allow Prime License Manager to connect to UCM and Unity Connection through the HTTPS port 443 from the HCS management domain.

Step 4 Plan for appropriate usage of the Prime License Manager web interface:

- For initial configuration, to generate license requests, to load license files, and to display license usage by cluster if desired.
- To assign a cluster (using only the HCS License Manager) to a Prime License Manager instance so that the HCS License Manager can set the appropriate deployment mode to the cluster and consolidate license usage for all customers and clusters.

Platform Manager Planning Considerations

Platform Manager is a Cisco Hosted Collaboration Mediation Fulfillment service that allows you to schedule and monitor the automated installation, upgrade, restart and backup of multiple application instances across customers for the following applications:

- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco Unified Presence / Cisco Unified IM and Presence

Take the following actions for Platform Manager planning as you onboard each customer or cluster:

- Determine the number of server groups needed.
- Select server groups for backup tasks that will avoid overloading blade hardware or I/O bandwidth to data storage LUNs.
- Put all servers (for example, Publishers) on a specific ESXi-Host or blade into a common server group. This way the backup of the servers on the host is done serially, minimizing the backup CPU load on the host.
- Spread the SFTP servers assigned to backup groups across different storage LUNs so that backup transfer load is spread out.
- Ensure that no more than two applications are backed up on a specific blade at any one time.

For details on Platform Manager, see the *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide, Release 10.6(1)*.

Use Prime Collaboration Deployment with UC Applications

Cisco Prime Collaboration Deployment helps you manage Unified Communications (UC) applications (release 10.x and later). Its primary high-level functions are to:

- Migrate a cluster of UC servers to a new cluster (such as MCS to virtual, or virtual to virtual).

  Tip Cisco Prime Collaboration Deployment does not delete the source cluster VMs after migration is complete. You can fail over to the source VMs if there is a problem with the new VMs. When you are satisfied with the migration, you can manually delete the source VMs.

- Perform operations on clusters (8.6(1) or later), such as:
  - Upgrade
  - Switch version
  - Restart
- Fresh install a new release 10.x UC cluster

- Change IP addresses or hostnames in release 10.x clusters (for a network migration).

  Cisco Prime Collaboration Deployment supports simple migration and network migration. Changing IP addresses or hostnames is not required for a simple migration. For more information, see the *Cisco Prime Collaboration Deployment Administration Guide*.

The following tables identify the functions supported by Cisco Prime Collaboration Deployment, Platform Manager, and Infrastructure Platform Automation. Each table identifies the UC applications and versions that the functions support. Support for UC applications and their versions is irrespective of Cisco HCS releases.

Table 1: Cisco Prime Collaboration Deployment Functions for UC Applications 10.x and later

Product and Functions	Cluster Discovery	Migration to 10.x Cluster	Upgrade Task (Upgrade Application Server or Install COP Files)	Restart Task	Switch Version Task	Fresh Install a New 10.x Cluster	Readdress Task (Change Hostname or IP Addresses for One or More Nodes in a Cluster)
Cisco Unified Communications Manager	6.1(5), 7.1(3), 7.1(5), 8.0(1), 8.0(2), 8.0(3), 8.5(1), 8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2)	6.1(5), 7.1(3), 7.1(5), 8.0(1), 8.0(2), 8.0(3), 8.5(1), 8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2)	8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2)	8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1), 10.5(1), 10.5(2)	8.6(1), 8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(x), 10.5(1), 10.5(2)	10.x, 10.5(1), 10.5(2)	10.x
Cisco Unified Presence	8.5, 8.6	8.5(4), 8.6(3), 8.6(4), 8.6(5)	8.6(3), 8.6(4), 8.6(5)	8.6(3), 8.6(4), 8.6(5)	8.6(3), 8.6(4), 8.6(5)	—	—
IM and Presence Service	—	—	—	—	—	10.x, 10.5(1), 10.5(2)	Not Supported

Product and Functions	Cluster Discovery	Migration to 10.x Cluster	Upgrade Task (Upgrade Application Server or Install COP Files)	Restart Task	Switch Version Task	Fresh Install a New 10.x Cluster	Readdress Task (Change Hostname or IP Addresses for One or More Nodes in a Cluster)
Cisco Unified Contact Center Express	8.5(1), 9.0, 9.0(2), 10.x	Not Supported	9.0(2), 10.x	9.0(2), 10.x	9.0(2), 10.x	10.5(x)	10.5(x)
Cisco Unity Connection	8.6(1), 8.6(2), 9.x, 10.x	Not Supported	From 8.6(x) to 8.6(x) From 8.6(x) to 9.x From 9.x to 9.x From 10.0(1) to 10.x	8.6(1), 8.6(2), 9.x, 10.x	8.6(1), 8.6(2), 9.x, 10.x	10.5(x)	10.5(x)

Table 2: HCM-F Platform Manager Functions (for pre-10.x UC Applications)

Product and Functions	Cluster Discovery	Migration to 10.x Cluster	Upgrade Task (Upgrade Application Server or Install COP Files)	Restart Task	Switch Version Task	Fresh Install a New 10.x Cluster	Readdress Task (Change Hostname or IP Addresses for One or More Nodes in a Cluster)
Cisco Unified Communications Manager	8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1)	Not Supported	8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1)	8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1)	8.6(2), 9.0.(1), 9.1(1), 9.1(2), 10.0(1)	Not Supported	Not Supported

Product and Functions	Cluster Discovery	Migration to 10.x Cluster	Upgrade Task (Upgrade Application Server or Install COP Files)	Restart Task	Switch Version Task	Fresh Install a New 10.x Cluster	Readdress Task (Change Hostname or IP Addresses for One or More Nodes in a Cluster)
Cisco Unified Presence	8.6	Not Supported	8.6(3), 8.6(4), 8.6(5)	8.6	8.6	Not Supported	Not Supported
IM and Presence Service	9.0.(1), 9.1(1), 9.1(2), 10.0(1)	Not Supported	9.0.(1), 9.1(1), 9.1(2), 10.0(1)	9.0.(1), 9.1(1), 9.1(2), 10.0(1)	9.0.(1), 9.1(1), 9.1(2), 10.0(1)	Not Supported	Not Supported
Cisco Unified Contact Center Express	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Cisco Unity Connection	8.6(2) , 9.x, 10.0(1)	Not Supported	From 8.6(x) to 8.6(x) From 8.6(x) to 9.x From 9.x to 9.x From 9.x to 10.x From 10.0(1) to 10.x	8.6(2), 9.x, 10.0(1)	8.6(2), 9.x, 10.0(1)	Not Supported	Not Supported

Table 3: Infrastructure Platform Automation Functions

UC Application	VMware Cloning from Golden Template	Readdress Task (Change Hostname or IP Addresses for One or More Nodes in a Cluster)
Cisco Unified Communications Manager	9.0.(1), 9.1(1), 9.1(2), 10.0(1)	9.0.(1), 9.1(1), 9.1(2), 10.0(1)
Cisco Unified Presence	Not Supported	Not Supported

UC Application	VMware Cloning from Golden Template	Readdress Task (Change Hostname or IP Addresses for One or More Nodes in a Cluster)
IM and Presence Service	10.0.(1)	10.0.(1)
Cisco Unified Contact Center Express	Not Supported	Not Supported
Cisco Unity Connection	9.x and 10.0.(1)	9.x and 10.0(1)

Cisco supports virtualized deployments of Cisco Prime Collaboration Deployment. The application is deployed using an OVA that contains the pre-installed application. This OVA is obtained with a licensed copy of Cisco Unified Communications Manager software. For information about how to extract and deploy the PCD_VAPP.OVA file, see the *Cisco Prime Collaboration Administration Guide*.

In your Cisco HCS environment, install only one instance of Cisco Prime Collaboration Deployment, which must have the following:

- Access to all Cisco Unified Communications Manager clusters for all customers, including those behind a NAT
- A fixed, non-overlapping IP address

Use the **Cluster Discovery** feature to find application clusters on which to perform fresh installs, migration, and upgrade functions. Perform this discovery on a blade-by-blade basis.

Note If you use Cisco Prime Collaboration Deployment to migrate Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service to the 10.5(x) (or later) version of those applications, remember to update the version in Cisco Unified Communications Domain Manager. Select the new version in the **Version** drop list for each application in the Cisco Unified Communications Domain Manager user interface.

For more information about features, installation, configuration and administration, best practices, and troubleshooting, see the following documents:

- *Cisco Prime Collaboration Administration Guide*: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html
- *Release Notes for Cisco Prime Collaboration Deployment*: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html

Infrastructure Platform Automation (IPA) Planning Considerations

Infrastructure Platform Automation (IPA) is an application designed to be an optional tool used to assist in the automation of the provisioning steps for on-boarding customers inside both the Cisco Unified

Communications Manager application and the Cisco Unity Connection by using an XML configuration file that is loaded in Infrastructure Manager within the Cisco HCM-F interface. The automation process includes Virtual Machine cloning from golden templates and running change identity on the Cisco Unified Communications Manager or Cisco Unity Connection Publisher and Subscriber Virtual Machines. If the Virtual Machines are pre-cloned, for example by Cloud-O or manually, IPA performs only identity operations on Virtual Machines.

IPA supports deployment of IM and Presence nodes in a Cisco Unified Communications Manager cluster.

Golden templates are master copies of Cisco Unified Communications Manager and Cisco Unity Connection that you can reuse or install on multiple virtual machines. They are built on a source system controlled by a service provider. Golden templates are built one for publisher and one for subscriber. After golden templates are built, IPA automates the process of cloning, identity, and post-installation operations of the virtual machine.

Note IPA requires the Cisco Nexus 1000V Switch for VMware vSphere and vSphere Enterprise Plus to function. This impacts Micro Node deployments which only require a vNetwork Standard Switch (vSwitch) and vSphere Standard. For more information on vNetwork Distributed Switch concepts see Overview of vNetwork Distributed Switch concepts (1010555) at the VMware Knowledge Base.

Take the following actions for IPA planning:

Procedure

Step 1 Create golden templates one time for the Cisco Unified Communications Manager Publisher, Cisco Unified Communications Manager Subscriber, and Cisco Unity Connection nodes for IPA use. For details on creating golden templates, see the *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide, Release 10.6(1)*.

Step 2 Carefully gather the detailed configuration defined by the XML configuration file. The XML configuration file requires details for the customer organization, Cisco Unified Communications Manager and Cisco Unity Connection applications, and Virtual Machines.

Note IPA can only be used in data center deployments. On-premises setup is not supported by IPA because there is no access to the EXSi host.

Note Be aware that IPA version 9.2.1 does not create the IM and Presence server; you need to create it manually.

For details on IPA, see the *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide, Release 10.6(1)*.

API Gateway Proxy Planning Considerations

The API Gateway Proxy, which provides a single point of integration for the HCS Management Fulfillment APIs, runs on a web services node and provides a routing proxy that is based upon customer information stored in the Shared Data Repository (SDR). The API Gateway Proxy provides access to Service Fulfillment APIs of HCS management components HCM-F, Cisco Unified Communications Domain Manager, and Unified CCDM. It leverages infrastructure information in the Shared Data Repository to route API requests to the appropriate application. The API Gateway also provides an Application Reference Directory that provides a list of unique URLs for every routable application.

Notice of deprecation: API Gateway Planning is going to be removed in a future release.

Take the following actions for API Gateway Proxy planning:

Procedure

Step 1 Determine if you will use the automated provisioning system that communicates through the API Gateway Proxy or manual provisioning with the GUI interface.

Step 2 Deploy the API Gateway Proxy only if one of the following scenarios exists:

- You want to manage some fulfillment activities from your in-house portal.
- You want to automate HCS Fulfillment by integrating one or more of your in-house systems with HCM-F or Cisco Unified Communications Domain Manager.

If neither of these scenarios apply, you do not need to deploy the API Gateway Proxy.

Step 3 For high availability, implement at least two instances of the API Gateway Proxy web services node, including the following: use a load balancer to provide a single virtual IP address and balance the traffic flowing to the API Gateway Proxy nodes. The load balancer must be sourced by the service provider.

Step 4 Use a DNS to support API Gateway Proxy deployment to avoid a 10-second delay each time a new session is established between the gateway and other HCS components.

Note Redundancy is provided as N+1 multinode in conjunction with a partner-deployed load balancer.

For details, refer to the *Cisco Hosted Collaboration Solution API Gateway Proxy Developer Guide*.

API Gateway Planning Considerations

The API Gateway provides a single point of integration for the Cisco HCS Management Fulfillment APIs. The API Gateway provides access to Service Fulfillment APIs of HCS management components Cisco Unified Communications Domain Manager 10.6(1) and CCDM.

Take the following actions for API Gateway planning:

Procedure

Step 1 Determine if you will use the automated provisioning system that communicates through the API Gateway, or manual provisioning with the GUI interface.

Step 2 Determine if you will use a load balancer to provide a single virtual IP address and balance the traffic flowing to the API Gateway nodes. The load balancer must be sourced by the service provider.

Cisco Unified Communications Domain Manager 8.1(x) Planning Considerations

Cisco Unified Communications Domain Manager is an integral part of the service fulfillment subsystem. It is primarily responsible for the configuration and registration of users, subscribers, and endpoints with the back-end Cisco Unified Communications Manager, Cisco Unity Connection, and Cisco Unified Communications IM and Presence Service servers. Cisco Unified Communications Domain Manager provides the day-to-day service and device provisioning and management tools. One instance supports all deployment sizes up to 200,000 subscribers.

Consider the steps in the following procedure for Cisco Unified Communications Domain Manager planning:

Procedure

Step 1 Determine if WebEx and Contact Center is integrated.

Step 2 Set up Cisco Unified Communications Domain Manager redundancy at the initial install; it cannot be introduced later. Cisco Unified Communications Domain Manager is deployed as one Unified Communications Domain Manager Master or Active instance and one Disaster Recovery (DR) instance hosted across two data centers, and management must be able to route to both. There is an added layer of High Availability that is provided by VMware HA for both the active and standby Cisco Unified Communications Domain Manager node. Redundancy is provided by the active sync of data between the active Cisco Unified Communications Domain Manager node and the standby Cisco Unified Communications Domain Manager node.

Step 3 Determine which dial plan to use. See the "Customer-specific dial plan" section in this document.

Step 4 For user activations, decide if you use automated system activations based on system inventory or the Cisco Unified Communications Domain Manager administrator interface.

Step 5 Decide if you want to use the Cisco Unified Communications Domain Manager user self-care portal. If yes, you need to allow access for customers or end users.

Step 6 Check to see what the static deployment requirements are on Cisco Unified Communications Manager clusters before managing a cluster from Cisco Unified Communications Domain Manager. Gather the following information:

a) Location of the Cisco Unified Communications Domain Manager
b) Determine latency between Cisco Unified Communications Domain Manager and UC applications, which must be within defined limits. The maximum supported latency is 200 ms Round Trip Time (RTT).

Note A higher latency (for example 250 ms RTT) may work in certain instances, but this must be tested before deployment.

Step 7 Determine if extra languages are required for the system other than English.

Step 8 Determine if custom branding is desired.

Step 9 For a Shared Instance deployment:

a) A single Cisco Unified Communications Domain Manager can manage both types of clusters (dedicated and shared instance) in one HCS deployment.
b) You can provision a single Cisco Unified Communications Domain Manager with separate service providers for a shared instance cluster and a standard cluster.

Note License Manager and SI reporting do not provide tenant-specific information.

Cisco Unified Communications Domain Manager Planning Considerations

Cisco Unified Communications Domain Manager 10.6(1) is an integral part of the service fulfillment subsystem. It is primarily responsible for the configuration and registration of users, subscribers, and endpoints with the back-end Cisco Unified Communications Manager, Cisco Unity Connection, and IM and Presence Service servers. Cisco Unified Communications Domain Manager 10.6(1) provides the day-to-day service and device provisioning and management tools. One instance supports all deployment sizes up to 200,000 subscribers.

Consider the steps in the following procedure for Cisco Unified Communications Domain Manager 10.6(1) planning:

Procedure

Step 1 Determine if WebEx and Contact Center will be integrated.

Step 2 Cisco Unified Communications Domain Manager 10.6(1) is deployed either as a single node, or a cluster of multiple nodes with High Availability (HA) and/or Disaster Recovery (DR) qualities. Each node can be assigned one or more of the following functional roles:

- WebProxy – load balancing across multiple application roles
- Application – transactional business logic
- Database – persistent storage of data

The following combined roles are defined:

- Standalone – combines the Application and Database roles for use in a non-clustered environment
- Unified – similar to the Standalone role combining Application and Database roles, but clustered with other nodes to provide HA and DR capabilities.

Step 3 Determine which dial plan to use. See the "Customer specific dial plan" section in this document

Step 4 For user activations, decide if you will use automated system activations based on system inventory or the Cisco Unified Communications Domain Manager 10.6(1) admin interface.

Step 5 Decide if you want to use the Cisco Unified Communications Domain Manager 10.6(1) user self-care portal. If yes, you need to allow access for customers or end users.

Step 6 Check to see what the static deployment requirements are on Cisco Unified Communications Manager clusters before managing a cluster from Cisco Unified Communications Domain Manager 10.6(1). Gather the following information:

a) Location of the Cisco Unified Communications Domain Manager 10.6(1)
b) Determine latency between Cisco Unified Communications Domain Manager 10.6(1) and UC applications, which must be within defined limits. The maximum supported latency is 200 ms Round Trip Time (RTT).

Note A higher latency (e.g. 250 ms RTT) may work in certain instances, but this must be tested prior to deployment.

Step 7 Determine if additional languages are required for the system other than English.

Step 8 Determine if custom branding is desired.

Step 9 For a Shared Instance deployment:

a) A single Cisco Unified Communications Domain Manager 10.6(1) can manage both types of clusters (dedicated and shared instance) in one HCS deployment.

b) You can provision a single Cisco Unified Communications Domain Manager 10.6(1) with separate service providers for a shared instance cluster and a standard cluster.

   Note License Manager and SI reporting do not provide tenant-specific information.

Cisco Unified Communications Domain Manager 8.1(x) Resource Requirements

The following table lists the resource requirements for the listed SF components.

HCS				
Fulfillment component	**vCPU**	**RAM (GB)**	**Storage (GB)**	**IOPS**
CUCDM	7	32	325 (includes a 100 GB dedicated backup partition)	300 during provisioning and 650 during database backup
HCM-F	4	16 (Res). Web service node (if used) uses 8 MB of RAM	80	200
Prime License Manager	1	4	50	-
CCDM	8	32	100	775 (DB server) 565 (web server)

Note For current updates to the above requirements see the *Cisco Hosted Collaboration Solution Compatibility Matrix*.

Resource Requirements

The following table lists the resource requirements for the listed SF components.

HCS 10.6(1)					
Fulfillment component	**vCPU**	**RAM (GB)**	**Storage**	**IOPS**	**OS**

HCS 10.6(1)					
CUCDM 10.1.1 Multi-node	4vCPU @ 2GHz	8GB	370GB partitioned as follows: • 20GB for OS • 40GB for application • 10GB for logs • 50GB for compressed backups • 250GB for database	300	
WebProxy Nodes	2vCPU @ 2GHz	4GB	150GB		
HCM-F	4 x 1.8 GHz	16 (Res)	80	200	
PLM	1 vCPU x 1.8 GHz	4	50	-	
CCDM	8	32	100	775 (DB server) 565 (web server)	Microsoft Windows

The Database storage partition is sized at the initial installation to support the maximum deployment size for the release. Further increase in the size of the partition is not required as new customers are on-boarded.

To set up the disk requirements, the disk should be set up on the VMWare GUI Resources tab where a disk can be created. This task should be done after the OVA import but prior to the boot of the system.

Compatibility considerations

See the Service Fulfillment compatibility table in *Cisco Hosted Collaboration Solution Compatibility Matrix*.

Call Detail Records

Service Providers (SPs) can use Usage-based billing, using call detail records (CDRs) or Call Manager Management Records (CMRs) for the enterprise.

If a service provider is interested in usage type billing, they can direct CDRs from Unified Communications Manager to their billing system. If Cisco Prime Collaboration Assurance is configured as a management application, the Cisco HCS Provisioning Adapter (CHPA) service configures any CUCM (release 9.0(1) or higher) to send CDRs to Cisco Prime Collaboration Assurance. The option also exists to work with our third-party vendor to consume CDRs and CMRs to produce necessary billing information or invoices.

The Cisco TelePresence Exchange System collects and displays call detail records (CDRs) for calls that are placed on the system. From the administration console, you can view CDR details for the system and export a comma-separated value (.csv) file of that information.

The Cisco TelePresence Exchange System retains CDRs for up to 30 days from the recorded end time of the CDR. The system automatically purges CDRs that exceed this 30-day limit. If the total number of CDRs retained by the system reaches 100,000, the system retains only the most recent 100,000 records and automatically purges the rest.

The Cisco TelePresence Exchange System also provides an Application Programming Interface (API) for managing and retrieving call records. For more details, see the *API User Guide for the Cisco TelePresence Exchange System*.

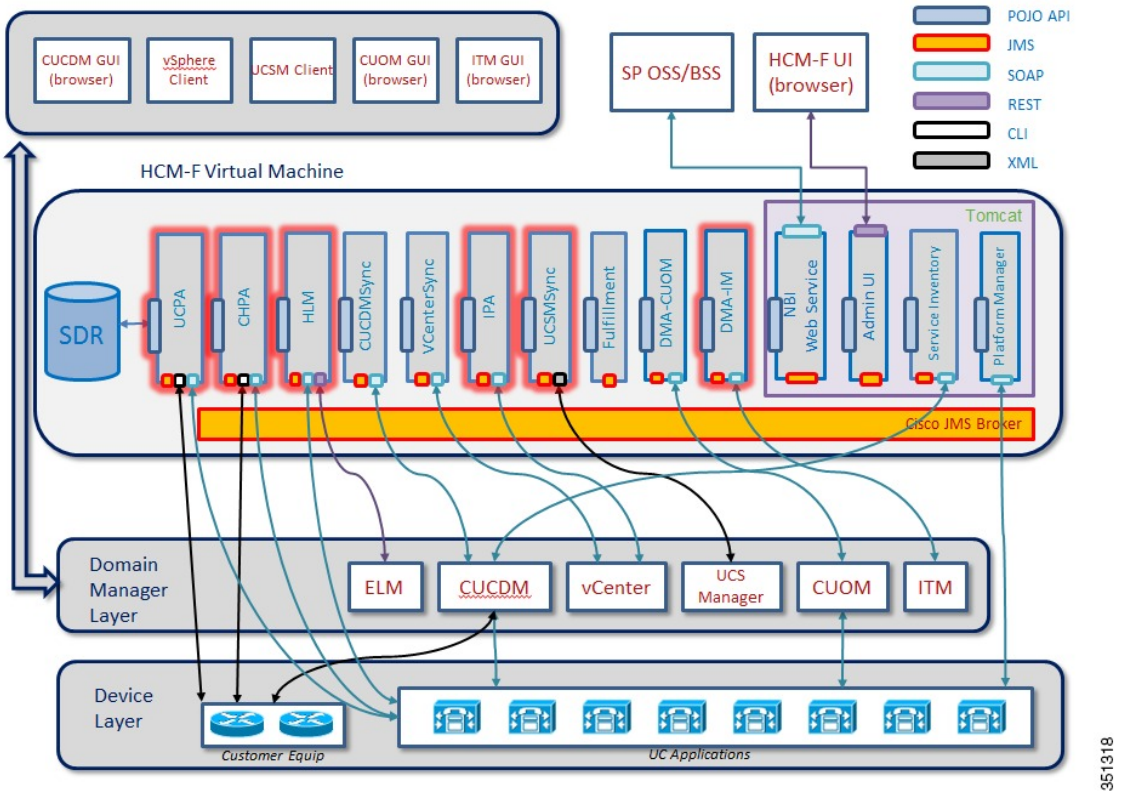
CHAPTER 2

Overview

Cisco HCM-F application node overview

The following figure illustrates the architecture of Cisco HCM-F application node.

Figure 1: Cisco HCM-F application node architecture



Cisco HCM-F application node delivers the following main functions and services:

- **Centralized database for the Cisco HCS solution:** the Shared Data Repository (SDR)
- **Synchronization of the SDR with domain managers:** Multiple synchronization services populate the SDR and keep it updated when configuration changes are applied through these domain managers: The following services populate and update the SDR:
    - CUCDMSync service updates the SDR when configuration changes are applied through the Cisco Unified Communications Domain Manager (CUCDM).
    - VCenterSync service updates the SDR when configuration changes are applied through vCenter.
    - HCS UCSMSync service monitors configuration data of Cisco UCS Managers and maintains syncrhonization between the Cisco HCS Shared Data Repository.
- **North Bound Interface (NBI):** Populates and updates SDR
- **Cisco HCM-F Administrative UI:** Allows configuration of Cisco HCM-F services.

- Services for automatic configuration of the Prime Collaboration Assurance (PCA):
    - HCS Fulfillment service
    - HCS DMA-SA service

      Note Based on data extracted from the SDR, these two services work together to automatically configure the PCA to monitor Unified Communications Applications and customer equipment.

    - HCS Provisioning Adapter Service

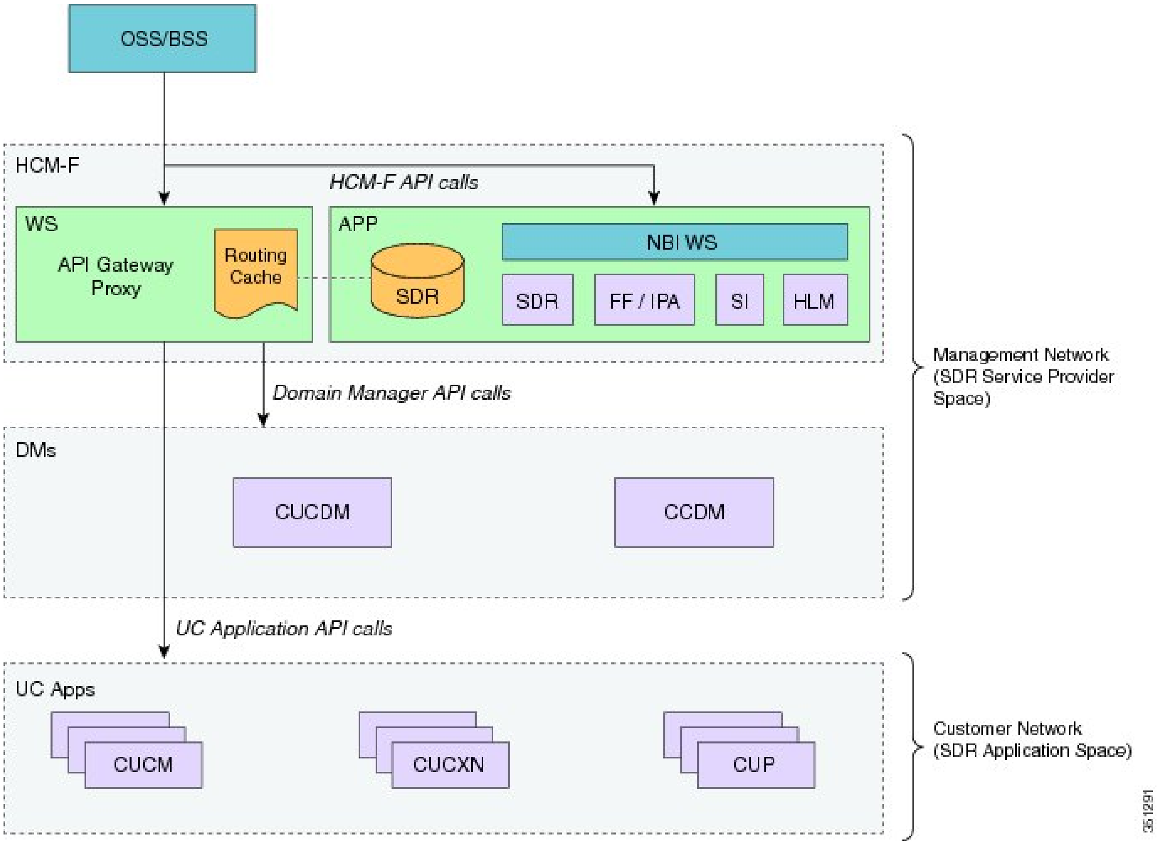
      Note Fulfillment and CHPA work together to automatically configure CUCM applications with the data needed for those applications to be monitored by PCA. Other applications such as CUCxn and CUP must be manually configured to be monitored by PCA.

- **HCS Infrastructure Platform Automation (IPA) service:** provides Infrastructure Platform Automation of UC application VM creation.
- **HCS License Manager (HLM) service:** manages licenses for UC applications.
- **HCS Northbound Interface (NBI) API service:** provides an interface to the service provider BSS or OSS through a SOAP web services interface.
- **Unity Connection Provisioning Adapter service:** For deployments without CUCDM, UCPA uses the UCCxn REST interface to pull customer data directly from the UCCxn server for input into Service Inventory reports.
- **Service Inventory:** Provides the service provider with reports on customers, subscribers, and devices. These reports may be used by the service provider to audit customer admin provisioning, and generate billing reports and change reports for their customers, based on MACD operations.

Cisco HCM-F WS node

The following figure illustrates the architecture of Cisco HCM-F Web Services (WS) node.

Figure 2: Cisco HCM-F WS node architecture



In release 9.2(1) the Cisco HCM-F web services node is an API Gateway Proxy node that delivers the following main functions and services:

- Cisco HCM-F API Gateway Proxy provides a single point of access for all fulfillment related APIs through the API Gateway Proxy Service.
- Cisco HCM-F application node provides a repository for Cisco HCS related application infrastructure information. From the Shared Data Repository (SDR) to the API Gateway Proxy Service.
  - Customers
  - Clusters
  - Application Instance
  - Network Address
  - Credentials

- API Gateway Proxy nodes leverage infrastructure information in the Shared Data Repository to direct API requests to the appropriate application.
- In release 9.2(1), only provisioning related APIs are supported.

Cisco HCS Shared Data Repository

The Shared Data Repository (SDR) is the central database for Cisco HCS. This repository stores data that is common to multiple Cisco HCS components.

The Shared Data Repository provides Cisco HCS with the following benefits:

- Reduces duplicate data entry and data inconsistency
- Integrates Cisco HCS components, which provides architectural stability
- Shared Data Repository is utilized by HCS License Manager, Service Inventory, and Platform Manager

The Cisco HCS Shared Data Repository supports the following functional areas:

- HCM-Fulfillment — Allows a service provider to provision a new enterprise customer with voice, video and other collaboration and mobility services, as required.
- HCM-Service Assurance — Supports fault and performance management.

One Cisco HCS Shared Data Repository is installed when you install Cisco HCM-F on the Cisco HCM-F platform.

Internal components of the Cisco HCS Shared Data Repository identify the type of client that is communicating with the database; for example, the Cisco HCS Shared Data Repository can identify whether the client serves as a sync agent. Because of this ability to identify the client, the Cisco HCS Shared Data Repository assists with debugging by allowing the Cisco HCS Shared Data Repository to record the client name in log messages. An internal component of the Cisco HCS Shared Data Repository prevents clients that are accessing the same data from overwriting changes that occur at the same time. In addition, the Cisco HCS Shared Data Repository provides clients with change notification.

The following sources update the Cisco HCS Shared Data Repository:

- Cisco Unified Communications Domain Manager
- The Cisco HCM-F northbound interface API
- VCenterSync, UCSMSync, and CUCDMSync—These synchronization services read data from the data source and write the data to the Cisco HCS Shared Data Repository
- The Cisco HCM-F administrative interface

External clients, such as the service provider Operations Support System (OSS)/Business Support System (BSS), interact with the Cisco HCS Shared Data Repository through Cisco HCM-F northbound interface APIs.

The Cisco HCS Shared Data Repository indicates whether data is read-only to clients such as the Cisco HCS administrative interface. In this case, the administrative interface indicates that the administrator cannot edit the content.

API Gateway Proxy

The API Gateway Proxy provides a single-point of integration to HCS Fulfillment APIs. It runs on an HCM-F Web Services node. The API Gateway Proxy uses a routing/proxy that is based upon customer information stored in the Shared Data Repository (SDR). The API Gateway Proxy provides access to Service Fulfillment APIs of supported applications. The API Gateway Proxy leverages infrastructure information in the Shared Data Repository to route API requests to the appropriate application. The API Gateway Proxy also provides an Application Reference Directory that provides a list of unique URLs for every routable application from Cisco HCM-F.

Notice of deprecation: API Gateway Planning is going to be removed in a future release.

For more information, see the *API Gateway Proxy Developer Guide* .

API Gateway High Availability

To ensure that the API Gateway Proxy is highly available, you can deploy two or more nodes of the API Gateway Proxy with a partner-provided load balancer. The API Gateway Proxy nodes run completely independent of one another. If a node fails, API Proxy service transparently continues on the other node.

Infrastructure Platform Automation Description

Infrastructure Platform Automation (IPA) automates the provisioning steps for on-boarding customers inside both the Cisco Unified Communications Manager application and the Cisco Unity Connection by using an XML configuration file that is loaded in Infrastructure Manager within the Cisco Hosted Collaboration Mediation-Fulfillment (HCM-F) interface. The automation process includes Virtual Machine cloning and running identity on the Cisco Unified Communications Manager or Cisco Unity Connection Publisher and Subscriber Virtual Machines. If the Virtual Machines are pre-cloned, for example by Cloud-O or manually, IPA performs only identity operations on Virtual Machines.

Both Unified Communications Manager clusters and Cisco Unity Connection clusters can have only one Publisher, and only one Unity Subscriber node per cluster is supported. The IPA XML must always contain the Unified Communications Manager Cluster information, but the Cisco Unity Connection Cluster information is optional. You can deploy Cisco Unified Communications Manager without Cisco Unity Connection but not the reverse. Cisco Unity Connection Publishers and Subscribers both use the skip install process. Cisco Unity Connection and Cisco Unified Communications Manager share the same ISO file for installation, but they each have their own OVA file which must be used for deploying VMs for IPA use.

Note IPA supports only specific versions of Cisco Unified Communications Manager and Cisco Unity Connection cluster deployments. See the *Cisco Hosted Collaboration Solution Compatibility Matrix* for details on which Cisco HCM-F version works with Cisco Unified Communications Manager and Cisco Unity Connection versions. The cluster ID is one of the manual parameters, and you must configure the cluster on the Cisco Unified Communications Manager or Cisco Unity Connection before configuring in the Cisco Unified Communications Domain Manager.

Note Cisco Prime Collaboration Deployment helps you manage Unified Communications (UC) applications (release 10.x and later). Its primary high-level functions are to:

- Migrate a cluster of UC servers to a new cluster (such as MCS to virtual, or virtual to virtual).

  Tip Cisco Prime Collaboration Deployment does not delete the source cluster VMs after migration is complete. You can fail over to the source VMs if there is a problem with the new VMs. When you are satisfied with the migration, you can manually delete the source VMs.

- Perform operations on clusters (8.6(1) or later), such as:
  - Upgrade
  - Switch version
  - Restart
- Fresh install a new release 10.x UC cluster
- Change IP addresses or hostnames in release 10.x clusters (for a network migration).

  Cisco Prime Collaboration Deployment supports simple migration and network migration. Changing IP addresses or hostnames is not required for a simple migration. For more information, see the *Cisco Prime Collaboration Deployment Administration Guide*.

For additional information on Prime Collaboration Deployment and HCS see Use Prime Collaboration Deployment with UC Applications, on page 4

Cisco HCS Fulfillment service

The Cisco HCS Fulfillment service is a standalone Java application. It performs the following functions:

- To trigger provisioning of Cisco Prime Collaboration Assurance, the fulfillment service automatically detects data changes in the SDR related to devices, and triggers the DMA-SA to provision those devices.
- To trigger the Cisco HCS Provisioning Adapter (CHPA) service to add some Cisco Prime Collaboration Assurance configuration to Cisco Unified Communication Manager application nodes.
- To automatically link a virtual machine to an application instance within the SDR, a blade to an ESXi Host, and a customer to Cisco Prime Collaboration Assurance.

The following sections describe the functions of the fulfillment service.

Role of Fulfillment service in Domain Manager configuration

The Cisco HCS Fulfillment service responds to notifications of changes sent by the SDR and instructs the Domain Manager Adaptors (DMAs) to set up the Domain Managers to reflect those changes. The Fulfillment service responds to change notification when devices are added, deleted, or modified in the SDR.

The Fulfillment service responds to data changes in the SDR related to the following types of devices:

- Application instances (such as Cisco Unified Communications Manager, Cisco Unity Connection, and Cisco Unified Presence)
- Customer equipment

For example, when new devices are added to the SDR, the Fulfillment service instructs the DMA-SA to start monitoring those devices. The Fulfillment service also responds when devices are deleted or changed in the SDR and instructs the DMA-SA to make the required changes to the Prime Collaboration configuration to reflect those changes in the SDR. The Fulfillment service also triggers the CHPA to perform configuration changes on the Cisco Unified Communications Manager for monitoring by Prime Collaboration.

Automatic linking

A second function of the Fulfillment service is to automatically link various parts of the configuration together. HCM-F obtains provisioning data from several sources, including Cisco Unified Communications Domain Managers, UCS Managers, and vCenters. Service Assurance requires data from these 3 sources to be linked in certain ways to enable accurate fault correlation and root cause analysis.

Virtual Machine to Application Instance Links

The fulfillment service links virtual machines to the associated application instance. These application instances run on virtual machines that are synced into the Shared Data Repository from vCenter. The fulfillment service examines the primary hostname from the virtual machine and the network address hostname from the application instance. If these hostnames match, the virtual machine and application instance pair are linked in the database. This procedure works if non-overlapping hostnames are used in the HCS deployment. Non-overlapping hostnames means that each virtual machine in the deployment uses a unique hostname. Overlapping hostnames means that the same hostname may be used for two different customers. If overlapping hostnames are used in the deployment, then the virtual-machine-to-application-instance linkage must be done manually.

Note The fulfillment service auto-linking is disabled by default. When enabled, auto-linking only recognizes the number of customers assigned to the fulfillment service. Auto-linking does not recognize or consider device counts.

Unified communications applications are synced into the SDR from Cisco Unified Communications Domain Manager.

Manual link virtual machine to an application instance for overlapping hostnames

To manually link a virtual machine to an application instance, follow this procedure:

Note This procedure is very time-consuming even for relatively small numbers of cluster applications. Cisco strongly recommends using non-overlapping hostnames.

Procedure

Step 1 On the CUCDM configuration page, uncheck **Sync Enabled, Save**, and wait 1 minute for the configuration change to take effect.

Step 2 On each Cluster Application configuration page, uncheck the **Auto Link to Virtual Machine** checkbox.

Step 3 Select the associated Virtual Machine from the drop-down box and Save.

Step 4 Repeat for all Cluster Applications.

Step 5 When finished, return to the CUCDM configuration page and check **Sync Enabled** checkbox and **Save**. This will not over-write the manual linkages you just made.

Cisco Prime Collaboration Assurance to customer linking

The Fulfillment service can be configured to automatically link each new customer configured in the SDR with Cisco Prime Collaboration Assurance. which monitors that customer's applications. Cisco Prime Collaboration Assurance has a current capacity (the number of customers and devices currently monitoring) and a maximum capacity. If configured, the fulfillment service automatically links the customer that has the lowest current capacity and has not exceeded the maximum capacity. If Cisco Prime Collaboration Assurance is not configured below the maximum capacity, no automatic linkage is made.

Blade to ESXiHost linking

The Fulfillment service will automatically link Blades configured in UCS Manager with ESXiHosts configured in vCenter. This linkage is done using the UUID associated with both the Blade and the ESXiHost. If the UUID matches, the link is made. This linkage is enabled by default, and is recommended by Cisco. This automatic linkage can be disabled if desired.

Disable automatic blade to ESXi Host linkage

Follow this procedure to disable automatic blade to ESXi Host linkage:

Procedure

Step 1 On the vCenter configuration page, uncheck Sync Enabled checkbox and Save. Wait for 10 seconds for the change to take effect.

Step 2 On each ESXi Host configuration page, uncheck Auto Link to Blade checkbox.

Step 3 Select the associated Blade from the drop-down box and Save.

Step 4 Repeat for all ESXi Hosts.

Step 5 When finished, return to the vCenter configuration page and check the Sync Enabled checkbox and Save. This will not overwrite the manual linkages you just made.

Cisco Prime Collaboration Assurance

Overview

Cisco Prime Collaboration Assurance is a member of the Cisco Unified Communications family of products. It provides a comprehensive and efficient solution for network management and allows you to provision and monitor Cisco Unified Communications deployments.

Cisco Prime Collaboration Assurance monitors and evaluates the current status of both the IP communications infrastructure and the underlying transport infrastructure in your network. Cisco Prime Collaboration Assurance uses open interfaces such as Simple Network Management Protocol (SNMP) and hypertext transfer protocol (HTTP) to remotely poll data from different devices in the IP communications deployment.

Cisco Prime Collaboration Assurance does not deploy any agent software on the devices being monitored and therefore is not disruptive to system operations.

Cisco Prime Collaboration Assurance increases productivity of network managers by enabling them to isolate problems quickly using the following tools:

- Fault Monitor---Provides access to devices views, event summaries, device and event details, as well as access to other management tools on devices, clusters, and phones. This component makes navigating fault management easier and allows you to quickly view relevant information. You can set the context views based on site or device group.
- Service Level View---Displays a logical topology view of your IP telephony implementation. This logical view focuses on the cluster call-control relationships.
- Diagnostics---Provides access to key diagnostic tools and reports in one location. Distinct monitoring and diagnostic workflows allow you to quickly identify network data for analysis.
- Reports:
  - Event history
  - Audio IP phones
  - Personalized reports
  - Service quality history
  - Video IP phones
- Clickable information in notification messages---Includes context-sensitive links to more detailed information about service outages
- Context-sensitive links to other Cisco tools---Help you manage IP communications implementations

Cisco Prime Collaboration Assurance also performs the following functions:

- Supports device pools---Collects this information for various reports and displays. Service-quality and phone registration-related events can contain data at the device pool level.
- Supports event customizations---Event severity and description customizations are available across all displays and reports. You can also control events using suppression at the component level.
- Presents service-quality events---Uses information from Cisco Unified Service Monitor when it is also deployed for the following purposes:

    - Displays Mean Opinion Scores (MOSs) associated with poor voice quality between pairs of endpoints involved in a call. These endpoints can be Cisco Unified IP phones, Cisco Unity messaging systems, or voice gateways. It also displays other associated details about the voice-quality problem.
    - Enables you to perform a probable path trace between the two endpoints and reports on any outages or problems on intermediate nodes in the path.

- Highlights current connectivity-related and registration-related outages affecting Cisco Unified IP phones in the network. In addition, Cisco Prime Collaboration Assurance provides contextual information that enables you to locate and identify the IP phones involved.
- Tracks IP communication devices and IP phone inventory---Tracks Cisco Unified IP phone status changes and creates a variety of reports that document move, add, and change operations on Cisco Unified IP phones in the network. All phone reports and personalized reports now show device pool and partition information for the IP phones.
- Provides easy to use, scalable reports---Displays large networks using visual cues in map views, as well as tabular reports to access management details of clusters and devices.

Migration

If not already done so, we recommend that you migrate from Cisco Prime Unified Operations Manager to Cisco Prime Collaboration using the Cisco HCM-F CLI command:

utils migrate cuom_to_prime_collab

This moves all devices at once, retaining the association level to the domain manager.

You can also migrate individual clusters, customer equipment, or customers using the Cisco HCM-F GUI or the Cisco Unified Communications Domain Manager GUI.

Supported solutions

Cisco Prime Collaboration Assurance supports various solutions:

- Call processing services
- Contact center services
- Voice messaging services
- Cisco Unified Presence services
- Conferencing services
- Mobility services
- Video/TelePresence services
- Endpoints (IP phones and soft clients)
    - Other voice application services
    - Infrastructure services

Supported Devices

Device	8.6.2	9.0.1/9.1.1	9.2.1	10.0(1)	10.1(1)	10.1(2)	10.6(1)	Comment
CUCM	CUOM	CUOM	CUOM	PCA	PCA	PCA	PCA	
CUCXN	CUOM	CUOM	CUOM	PCA	PCA	PCA	PCA	
CUxAC				PCA	PCA	PCA	PCA	Attendant Console, 3rd party, basic monitoring only
CUP	CUOM	CUOM	CUOM	PCA	PCA	PCA	PCA	
Contact Center: UCCE	CUOM	CUOM	CUOM	PCA	PCA	PCA	PCA	
Contact Center: CVP	CUOM	CUOM	CUOM	PCA	PCA	PCA	PCA	
CUBE-ENT		CUOM	CUOM	PCA	PCA	PCA	PCA	
CUBE-SP			CUOM (manual)	PCA	PCA	PCA		
Finesse		CUOM	CUOM	PCA	PCA	PCA	PCA	
MediaSense		CUOM	CUOM	PCA	PCA	PCA	PCA	
CER				PCA	PCA	PCA	PCA	
vPGW				PCA	PCA	PCA		3rd party, basic monitoring only
HCM-F		CUOM (manual)	CUOM (manual)	PCA	PCA	PCA	PCA	All multi-node components. 3rd party, basic monitoring only
EIM/CIM				PCA	PCA	PCA	PCA	
VCS (E & C)				PCA	PCA	PCA	PCA	
CTX				PCA	PCA	PCA	PCA	
TP Server				PCA	PCA	PCA	PCA	
MCU				PCA	PCA	PCA	PCA	
IVR				PCA	PCA	PCA	PCA	
CTMS				PCA	PCA	PCA	PCA	Cisco TelePresence Multipoint Switch
TMS				PCA	PCA	PCA	PCA	
TP Video Endpoint				PCA	PCA	PCA	PCA	
CUIC	IM (manual)	IM (manual)	IM (manual)			PCA	PCA	Not monitored post-9.2

Device	8.6.2	9.0.1/9.1.1	9.2.1	10.0(1)	10.1(1)	10.1(2)	10.6(1)	Comment
vCenter	IM (manual)	IM	IM			PCA	PCA	Not monitored post-9.2
CCDM	IM (manual)	IM	IM				PCA	AKA: CCMP, Exony Not monitored post-9.2
CUCDM	IM (manual)	IM	IM			PCA	PCA	Not monitored post-9.2
CUOM	IM (manual)	IM	IM					No part of HCS post-9.2

Cisco HCS Domain Manager Adapter for Cisco Prime Collaboration Assurance

In the Cisco HCS architecture, Domain Managers are components that manage, monitor, or control other solution services. Examples of domain managers are Cisco Prime Collaboration Assurance, the Unified Communications Domain Manager, and vCenter.

Cisco Prime Collaboration Assurance is a Cisco network management server for Cisco voice products. In the Cisco HCS solution, it is a domain manager that performs monitoring of Cisco HCS network applications and devices. It receives events from the monitored devices and forwards them to the Event Collector for processing.

The Domain Manager Adapter for the Cisco Prime Collaboration Assurance (DMA-SA) integrates into the Cisco HCS solution. The DMA is an interface between the SDR and Cisco Prime Collaboration Assurance. The key function of the DMA is to automatically configure Cisco Prime Collaboration Assurance to monitor Cisco HCS devices and applications based on data from the SDR.

A second function of the DMA is to monitor Cisco Prime Collaboration Assurance limits and generate an HCM-F alarm when thresholds are reached.

The DMA-SA relies on the HCS Fulfillment service to detect changes on the SDR. The HCS Fulfillment service monitors the SDR database for changes. In response to those changes, the HCS Fulfillment service then instructs the DMA-SA to configure the Cisco Prime Collaboration Assurance to reflect changes on the SDR.

The DMA-SA can perform the following configuration changes:

- Add device
- Update device credentials
- Delete device

For instance, when a new device is added through vCenter and configured through the Unified Communications Domain Manager, the VCenterSync service and the CUCDMSync service update the SDR with the change. The Fulfillment service responds to the change in the SDR and instructs the DMA-SA to begin monitoring the new device. The DMA-SA then reads the device details from the SDR and programmatically configures the device (through SOAP) for monitoring in Cisco Prime Collaboration Assurance. The CHPA also configures devices for monitoring.

Note that for the devices to be configured for monitoring, the following conditions must also be met:

- Cisco Prime Collaboration Assurance must be added on the Cisco HCM-F Infrastructure Manager Administrative UI. It must also be configured with an IP address in the service provider space and a hostname, using ADMIN credentials.
- The customer (or application cluster or customer equipment) is linked to Cisco Prime Collaboration Assurance. This function can be performed manually through the Cisco HCM-F UI, or automatically by the Fulfillment service. The automatic function can be enabled or disabled with the command line interface (CLI) using the command **set hcs link auto-primecollab-linkage**. The state of this function can be displayed using the command **show hcs link auto-primecollab-linkage**.
- Credentials have been added for the device in the Cisco HCM-F UI HCM-F Infrastructure Manager Administrative Interface. Credentials for the devices can be added in two ways:
    - You can define a set of default credentials for each device type (**Hosted Collaboration Solution** > **Infrastructure Manager** > **Administration** > **Default Credentials**). When a new device is synchronized from the Unified Communications Domain Manager through the CUCDMSync, the default credentials associated with that device type will be automatically assigned to the new device. This is the recommended method and works well if all devices have the same SNMP credentials.
    - You can assign credentials to specific devices after they are synchronized to the SDR. This can be done on the Cluster Application page (**Hosted Collaboration Solution** > **Infrastructure Manager** > **Customer Management** > **Customer** > **Cluster** > **Cluster Application**). This method should be used for devices that have different SNMP credentials from the defaults.

Event Destination Setup

For Cisco Prime Collaboration Assurance to monitor UC applications and customer equipment devices, these devices must be configured with event destinations (SNMP trap, syslog, or RTMT API) to Cisco Prime Collaboration Assurance. The CHPA automatically configures event destinations on the Cisco Unified Communications Manager, but other devices must be manually configured to forward events to Cisco Prime Collaboration Assurance. Cisco Prime Collaboration Assurance must also be *manually* configured with a trap destination to the Cisco HCS partner OSS system for processing.

Event Flow

The DMA-SA configures Cisco Prime Collaboration Assurance to monitor UC Applications and customer equipment devices, but it does not collect events from the devices. After Cisco Prime Collaboration Assurance has been configured to monitor the devices, it collects events from the monitored devices, aggregates them and forwards them to the HCS partner OSS system in HCM- SA. HCM-SA also provides an NBI API for integration with the service provider MoM.

For information on how to configure event destinations on Cisco Prime Collaboration Assurance, refer to the appropriate documentation.

Cisco HCS Service Inventory

Cisco HCS Service Inventory is an application that provides reports for service providers for billing and audit purposes. These reports contain data on customers, subscribers, devices, and other details that are currently provisioned on Cisco Unified Communications Domain Manager. In addition, Service Inventory can generate reports directly from Cisco Unified Communications Manager and Cisco Unity Connection application servers for customers that are provisioned in Cisco HCM-F that do not have a Unified Communications Domain Manager configured. Service Inventory automatically transfers the report files daily to remote SFTP servers. The service providers use these reports to generate billing records for their customers.

Important Currently, Service Inventory can generate reports from a Cisco Unified Communications Manager and Cisco Unity Connection running UC Application Software Version 8.6 or later.

You can configure and schedule the report generation through the Service Inventory administrative interface. Through this interface, you can also manage credentials and configure general settings for Service Inventory.

At the time that is specified in the Service Inventory configuration, Service Inventory sends a real-time query request to Cisco Unified Communications Domain Manager or the appropriate UC Application for information. Cisco Unified Communications Domain Manager or the UC Application generates the necessary files and sends the files to Service Inventory through SFTP. Service Inventory creates a backup of the files, creates the report, and transfers the report to the SFTP servers that are configured in the Service Inventory administrative interface.

The generated report contains data for the previous 24 hours, up to and including the end time that you specify on the Overview page in the Service Inventory administrative interface. The generated reports get backed up for a configured amount of time. The default is 60 days.

On Demand reporting

Service Inventory provides On Demand Inventory and Location reporting. These On Demand reports allow the administrator to generate reports at any time without having to alter the reporting schedule. Location Summary reports generate a report to indicate the number of devices and subscribers per location.

Note Location reports require an Inventory report to be available on the system or an error will be generated.

Three types of customer/reseller reports can also be generated, SI reports, Summary reports and MACD reports.

The reports use a Cisco common format. For more information on this format and the data that is generated, see the *Cisco Hosted Collaboration Solution, Release 10.6(1) Maintain and Operate Guide*.

For instructions on how to perform configuration and scheduling tasks through the Service Inventory administrative interface, see the *Cisco Hosted Collaboration Solution, Release 10.6(1) Maintain and Operate Guide*.

Cisco HCS Platform Manager

The Platform Manager is an installation, upgrade, restart and backup management client for the following Cisco Unified Communications applications:

- Cisco Unified Communications Manager IM and Presence Service
- Cisco Unified Communications Manager
- Cisco Unity Connection

The Platform Manager allows you to manage and monitor the installation, upgrade, restart and backup of these servers. You can access the Platform Manager through the Cisco HCM-F administrative interface.

The Platform Manager organizes servers into server groups. All of the servers in a server group can be upgraded, switched, and restarted at the same time. Server groups are user-defined and consist of servers from multiple clusters. All of the servers in a particular group, however, must have the same product. for example, you cannot mix Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service nodes in the same server group.

Server groups allow you to logically join together different servers on which you want to perform common tasks as a group, such as installation, upgrades, and restarts.

The Platform Manager allows you to configure the system server inventory as well as select, schedule, and monitor upgrades of one or more servers across one or more clusters.

The server inventory can also be automatically synchronized from the Shared Data Repository so that it does not have to be manually configured.

The Platform Manager offers a wide range of different user-defined servers types to accommodate the management of potentially thousands of servers.

After you have configured all of your servers and server groups within Platform Manager, you can create a variety of tasks that help you streamline any installation, upgrade, or restart process. You can also automate backup tasks of your system using the Backup Schedule feature.

For instructions on how to perform Platform Manager configuration tasks , see the *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide, Release 10.6(1)*.

Cisco HCM-F Real-Time Monitoring Tool

Cisco HCM-F Real-Time Monitoring Tool (RTMT) runs as a client-side application and uses HTTPS to monitor system performance. RTMT can connect directly to a device through HTTPS to troubleshoot system problems. Tasks such as alarm and performance monitoring updates continue to run on the server in the background even when RTMT is not connected to the server.

HCM-F installation for Release 9.2.1 consists of one application server (node) and may contain either a single or multiple web services (WS) nodes. While RTMT can provide troubleshooting support for more than one server, you can connect to and monitor only one server per RTMT session.

RTMT allows you to perform the following tasks:

- Monitor a set of predefined management objects and performance counters that monitor the health of the server to which RTMT is connected.
- Configure and update alert settings for the management objects and performance counters (in the form of email messages).

  The HCM-F server monitors the alert conditions and when values go over or below user-configured thresholds, generates alerts. RTMT does not need to be running on your computer in order for alerts to be generated by the server. Alerts are displayed in RTMT in the form of alert logs.
- Collect and download or view traces. Traces can be viewed in the viewers that are built into RTMT.
- View syslog messages in SysLog Viewer.

For more information on RTMT, see the *Administration Guide for Cisco HCM-F Real-Time Monitoring Tool* and *Cisco Hosted Collaboration Mediation Fulfillment Maintain and Operate Guide*.

Cisco HCM-F administrative interface

The Cisco HCM-F administrative interface is the user interface to the Cisco HCM-F services. It allows you to perform management and configuration tasks on the Cisco HCM-F services.

From any user PC in your network, you can browse into a server that is running the Cisco HCM-F administrative interface and log in with administrative privileges: https://your-HCM-F-server:<portnumber>.

The Cisco HCM-F administrative interface uses HTTPS to secure the communication between the browser and the web server.

The Cisco HCM-F administrative interface provides the following administrative interfaces:

- Service Inventory
- Infrastructure Manager
- Platform Manager
- HCS License Manager

Service Inventory Administrative Interface

The Service Inventory administrative interface allows you to perform configuration and scheduling tasks on the Service Inventory application. This interface allows you to configure and schedule the generation and transmission of three types of Service Inventory billing reports, SI reports, Summary reports and MACD reports. Service Inventory transfers these report files to remote servers using SFTP. Service providers use these reports to generate bills and audit their customers.

For more information on the Service Inventory application and configuration tasks you can perform through the Service Inventory Administrative Interface, see the *Cisco Hosted Collaboration Mediation Fulfillment Maintain and Operate Guide, Release 10.6(1)*.

Infrastructure Manager

The Infrastructure Manager Administrative Interface allows you to provision and query the Cisco HCS Shared Data Repository. The Cisco HCS Shared Data Repository is a repository of data that represents the Cisco HCS configuration of data centers, customers, and management components in the service provider network. This repository is then used by HCM-Service Assurance to provide more effective, detailed, and accurate operational alarms and events.

Platform Manager

The Platform Manager Administrative Interface is the user interface to the Platform Manager service. This service is an upgrade management client, which allows you to manage upgrades for Cisco Unified Presence, Cisco Unified Communications Manager, and Cisco Unity Connection in the Cisco HCS.

The Platform Manager allows you to organize the servers in groups. Then, you can create a variety of tasks to manage and monitor the installation, upgrade and restart process of multiple servers. You can also automate backup tasks of your system using the Backup Schedule feature.

For more information on the functions of the Platform Manager, see Cisco HCS Platform Manager, on page 31.

For instructions on how to perform Platform Manager configuration tasks , see the *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide, Release 10.6(1)*.

Cisco HCS North Bound Interface Web Service API

The Cisco HCS North Bound Interface Web Service is a set of SOAP APIs that expose Cisco HCM-F functionality to the service provider OSS/BSS. These APIs provide the ability to configure, service, and control a Cisco HCM-F deployment.

The APIs comprise the following distinct categories:

- Shared Data Repository Web Service API
- Fulfillment Web Service API
- Service Inventory Web Service API
- HCS License Manager Web Service API

Shared Data Repository Web Service API

This web service is the external interface to the Cisco HCS Shared Data Repository.

This web service offers CRUD (Create, Read, Update, Delete) APIs to view and modify data in the HCS Shared Data Repository.

For more information on the Shared Data Repository Web Service API, see the *Developer Guide for Cisco Hosted Mediation Collaboration Fulfillment*.

Fulfillment Web Service API

This web service API controls Cisco HCM-F related tasks, such as starting manual synchronization jobs, restarting jobs, and non-CRUD Share Data Repository operations.

For more information on the Fulfillment Web Service API, see the *Developer Guide for Cisco Hosted Mediation Collaboration Fulfillment.*

Service Inventory Web Service API

This web service is the external interface to the Service Inventory application. It allows you to schedule, configure, and execute the generation of Service Inventory billing reports.

For more information on the Service Inventory Web Service APIs, see the *Developer Guide for Cisco Hosted Mediation Collaboration Fulfillment*.

HCS License Manager Web Service API

This web service provides an interface for HCM-F administrators to perform license management. The license management functionality includes getting or setting the global deployment mode, creating or deleting an HCS Licence Manager, assigning a customer or UC cluster to an HCS Prime License Manager, and more.

For more information on the HCS License Manager Web Service API, see the *Developer Guide for Cisco Hosted Mediation Collaboration Fulfillment.*

CHAPTER 3

Services

Service descriptions

After the installation of the Cisco HCM-F platform, most services start automatically. You can configure services by setting service parameters for each service. If necessary, for example, for troubleshooting purposes, you may need to stop and start (or restart) a service. You perform these task by using the command line interface (CLI) on the Cisco HCM-F platform.

This section describes the network services that exist of the Cisco HCM-F platform and are grouped by the following functional areas:

- Cisco HCS services, on page 37
- Performance and Monitoring services, on page 39
- Backup and Restore services, on page 40
- System services, on page 40
- Platform Services, on page 40

Cisco HCS services

This section describes the Cisco HCS services that are specific to Cisco HCS.

Cisco CDM Database service

The Cisco CDM Database service supports the Shared Data Repository.

Cisco HCS Shared Data Repository Change Notification service

The Cisco HCS Shared Data Repository Change Notification service informs other services of data changes in the HCS Shared Data Repository.

Cisco JMS Broker service

The Cisco JMS Broker service provides a messaging infrastructure that other services use to communicate with each other. The broker is used by services such as CUCDMSync, VCenterSync, Fulfillment and DMA-SA.

Cisco HCS Admin UI service

The Cisco HCS Admin UI service supports the administrative interface.

Cisco HCS API Gateway Proxy web service

The API Gateway Proxy provides a single point of integration for the Cisco HCM-F APIs from a web services node and provides access to Service Fulfillment APIs of supported applications.

Cisco HCS CUCDMSync service

The Cisco HCS CUCDMSync service, which maintains synchronization of provisioned Cisco HCS data between Cisco Unified Communications Domain Manager and the Cisco HCS Shared Data Repository, copies data from the Cisco Unified Communications Domain Manager to the Cisco HCS Shared Data Repository. The CUCDMSync service supports automatic and manual synchronization.

Cisco HCS DMA-SA service

The Cisco HCS DMA-SA service is an interface between the HCS Shared Data Repository and Cisco Prime Collaboration Assurance. The key function of the DMA is to automatically configure Cisco Prime Collaboration Assurance to monitor Cisco HCS devices and application instances such as Cisco Unified Communication Manager, Cisco Unified Presence, and Cisco Unity Connection based on data from the HCS Shared Data Repository.

Cisco HCS DMA-CUOM Servlet service

The Cisco HCS DMA-CUOM Servlet service listens for Cisco Unified Operations Manager NBI notifications and forwards them to the main DMA-Cisco Unified Operations Manager service. This makes the provisioning work the DMA-CUOM does slightly more efficient, and it also allows DMA-CUOM to be notified when the devices in Cisco Unified Operations Manager are altered.

Cisco HCS Fulfillment service

The Cisco HCS Fulfillment service triggers provisioning of Cisco Prime Collaboration Assurance by automatically detecting data changes in the SDR related to devices. It triggers the DMA-SA to provision those devices on Cisco Prime Collaboration Assurance. The Cisco HCS Fulfillment service also coordinates provisioning done by CHPA. In addition, it automatically links blades to ESXi Hosts, Cisco Prime Collaboration Assurance customers, and virtual machines to application instances within the HCS Shared Data Repository.

Cisco HCS IPA service

The Cisco HCS IPA service creates the Infrastructure Platform Automation job within the HCM-F jobs table and communicates the job ID to the NBI.

Cisco HCS License Manager service

HCS License Manager provides centralized license management for Cisco HCS. HCS License Manager leverages the functionality of Prime License Manager and extends beyond the scope of a single enterprise for use in the service provider.

HCS License Manager utilizes the Cisco HCM-F framework. There will be one HCS License Manager per install of Cisco HCS.

Cisco HCS North Bound Interface Web service

The Cisco HCS North Bound Interface Web service is a set of SOAP APIs that expose Cisco HCM-F functionality to the service provider OSS/BSS. These APIs provide the ability to configure, service, and control a Cisco HCM-F deployment.

HCS NBI REST FF Web Service

Provides a REST API similar to the existing NBI API. In particular, this REST API is used for the interface to Cisco Unified Communications Domain Manager

HCS NBI REST HCS Shared Data Repository Web Service

Provides a REST API similar to the existing NBI API. In particular, this REST API is used for the interface to Cisco Unified Communications Domain Manager. This service provides access to the HCS Shared Data Repository database.

Cisco Platform Manager service

The Cisco Platform Manager service supports the Platform Manager administrative interface.

Cisco HCS Provisioning Adapter service

The Cisco HCS Provisioning Adapter service provisions credentials and SNMP information, as well as provisions remote Syslog data on Cisco Unified Communications Manager devices.

Cisco HCS Shared Data Repository UI service

The Cisco HCS Shared Data Repository UI service supports the Infrastructure Manager administrative interface.

Cisco HCS Service Inventory

The Cisco HCS Service Inventory supports Service Inventory reporting features.

Cisco HCS SI UI

The Cisco HCS SI UI supports the Service Inventory administrative interface.

Cisco HCS UCSMSync service

The Cisco HCS UCSMSync service monitors configuration data of Cisco UCS Managers and maintains synchronization between the Cisco HCS Shared Data Repository. Cisco HCM-Service Assurance uses the UCS Manager configuration to perform fault correlation and event enrichment.

Cisco HCS VCenterSync service

The Cisco HCS VCenterSync service monitors configuration data on one or more vCenter servers, copies data from the vCenter servers to the Cisco HCS Shared Data Repository, and maintains synchronization between the vCenter servers and the Cisco HCS Shared Data Repository. Cisco HCM-Service Assurance uses the vCenter configuration to perform fault correlation and event enrichment.

Cisco Unity Connection Provisioning Adapter service

For deployments without CUCDM, UCPA uses the UCCxn REST interface to pull customer data directly from the UCCxn server for input into Service Inventory reports.

Performance and Monitoring services

This section describes the Performance and Monitoring services.

Cisco AMC service

The Alert Manager and Collector service allows you to retrieve real-time information that exists on the server.

Cisco Audit Event service

The Cisco Audit Event service monitors and logs any configuration change to the Cisco HCM-F platform by a user or as a result of the user action.

Cisco Log Partition Monitoring Tool

The Cisco Log Partition Monitoring Tool service supports the Log Partition Monitoring feature, which monitors the disk usage of the log partition on the Cisco HCM-F platform by using configured thresholds and a polling interval.

Cisco RIS Data Collector

The Real-Time Information Server (RIS) maintains real-time information, such as critical alarms generated.

Cisco RTMT Web service

The Cisco RTMT Web service is a performance and monitoring service that activates trace for the RTMT servlets. Running this trace creates the server-side log for RTMT client queries.

Backup and Restore services

This section describes the Backup and Restore services.

Cisco DRF Local

The Cisco DRF Local service supports the Cisco DRF Local Agent, which acts as the workhorse for the DRF Master Agent. Components register with the Cisco DRF Local Agent to use the disaster recovery framework. The Cisco DRF Local Agent executes commands that it receives from the Cisco DRF Master Agent. Cisco DRF Local Agent sends the status, logs, and command results to the Cisco DRF Master Agent.

Cisco DRF Master

The Cisco DRF Master Agent service supports the DRF Master Agent, which works with the CLI to schedule backups, perform restorations, view dependencies, check status of jobs, and cancel jobs, if necessary. The Cisco DRF Master Agent also provides the storage medium for the backup and restoration process.

System services

This section describes the System services.

Cisco CDP

Cisco CDP advertises the voice application to other network management applications, so the network management application can perform network management tasks for the voice application.

Cisco Trace Collection service

The Cisco Trace Collection service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces. If you stop this service, you cannot collect or view traces on the Cisco HCM-F platform.

For SysLog Viewer and trace and log collection, the Cisco Trace Collection Servlet and the Cisco Trace Collection service must run on the server.

Platform Services

This section describes the Platform Services.

Cisco CDP Agent

This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the Cisco HCM-F platform. This service implements the CISCO-CDP-MIB.

Cisco Certificate Expiry Monitor

This service periodically checks the expiration status of certificates that the system generates and sends notification when a certificate gets close to its expiration date.

Cisco Configuration Manager

This service manages administration and configuration settings used by the other services.

Cisco Syslog Agent

This service supports gathering of syslog messages that various components generate. This service implements the CISCO-SYSLOG-MIB.

Cisco Tomcat

The Cisco Tomcat service supports the web server.

Cisco Tomcat Stats Servlet

The Cisco Tomcat Stats servlet collects the Tomcat statistics.

Host Resources Agent

This service provides SNMP access to host information, such as storage resources, process tables, and installed software base. This service implements the HOST-RESOURCES-MIB.

MIB2 Agent

This service provides SNMP access to variables, which are defined in RFC 1213, that read and write variables; for example, system and interfaces.

SNMP Master Agent

This service, which acts as the agent protocol engine, provides authentication, authorization, access control, and privacy functions that relate to SNMP requests.

Tip After you complete SNMP configuration in the CLI, you must restart the SNMP Master Agent service.

System Application Agent

This service provides SNMP access to the applications that are installed and executing on the system. This implements the SYSAPPL-MIB.

Infrastructure Platform Automation Description

Infrastructure Platform Automation (IPA) automates the provisioning steps for on-boarding customers inside both the Cisco Unified Communications Manager application and the Cisco Unity Connection by using an XML configuration file that is loaded in Infrastructure Manager within the Cisco Hosted Collaboration Mediation-Fulfillment (HCM-F) interface. The automation process includes Virtual Machine cloning and running identity on the Cisco Unified Communications Manager or Cisco Unity Connection Publisher and Subscriber Virtual Machines. If the Virtual Machines are pre-cloned, for example by Cloud-O or manually, IPA performs only identity operations on Virtual Machines.

Both Unified Communications Manager clusters and Cisco Unity Connection clusters can have only one Publisher, and only one Unity Subscriber node per cluster is supported. The IPA XML must always contain the Unified Communications Manager Cluster information, but the Cisco Unity Connection Cluster information is optional. You can deploy Cisco Unified Communications Manager without Cisco Unity Connection but not the reverse. Cisco Unity Connection Publishers and Subscribers both use the skip install process. Cisco

Unity Connection and Cisco Unified Communications Manager share the same ISO file for installation, but they each have their own OVA file which must be used for deploying VMs for IPA use.

Note IPA supports only specific versions of Cisco Unified Communications Manager and Cisco Unity Connection cluster deployments. See the *Cisco Hosted Collaboration Solution Compatibility Matrix* for details on which Cisco HCM-F version works with Cisco Unified Communications Manager and Cisco Unity Connection versions. The cluster ID is one of the manual parameters, and you must configure the cluster on the Cisco Unified Communications Manager or Cisco Unity Connection before configuring in the Cisco Unified Communications Domain Manager.

Note Cisco Prime Collaboration Deployment helps you manage Unified Communications (UC) applications (release 10.x and later). Its primary high-level functions are to:

- Migrate a cluster of UC servers to a new cluster (such as MCS to virtual, or virtual to virtual).

  Tip Cisco Prime Collaboration Deployment does not delete the source cluster VMs after migration is complete. You can fail over to the source VMs if there is a problem with the new VMs. When you are satisfied with the migration, you can manually delete the source VMs.

- Perform operations on clusters (8.6(1) or later), such as:
  - Upgrade
  - Switch version
  - Restart
- Fresh install a new release 10.x UC cluster
- Change IP addresses or hostnames in release 10.x clusters (for a network migration).

  Cisco Prime Collaboration Deployment supports simple migration and network migration. Changing IP addresses or hostnames is not required for a simple migration. For more information, see the *Cisco Prime Collaboration Deployment Administration Guide*.

For additional information on Prime Collaboration Deployment and HCS see Use Prime Collaboration Deployment with UC Applications, on page 4

Infrastructure Manager Sync Services Introduction

The following sections introduce the sync services available within Infrastructure Manager.

Cisco HCS VCenterSync services

The Cisco HCS VCenterSync service monitors configuration data on one or more vCenter servers, copies data from the vCenter servers to the Cisco HCS Shared Data Repository, and maintains synchronization between the vCenter servers and the Cisco HCS Shared Data Repository. Cisco HCM-Service Assurance uses the vCenter configuration to perform fault correlation, impact analysis, and event enrichment.

The following list outlines the data that is synced from vCenter:

- VMware Data Center
- VMware Clusters
- Virtual Machines
- ESXi Hosts

The VCenterSync service synchronizes configuration changes in vCenter using a notification mechanism and configuration changes in vCenter are synced in immediately.

Note You must configure Virtual Machines in a VMware Cluster on the vCenter itself (not in the SDR or Infrastructure Manager) for VCenterSync to work.

Cisco HCS UCSMSync services

The Cisco UCSMSync service monitors configuration data on one or more UCS Managers, copies data from the UCS Managers to the Cisco HCS Shared Data Repository, and maintains synchronization between the UCS Managers and the Cisco HCS Shared Data Repository. Cisco HCM-Service Assurance uses the UCS Manager configuration to perform fault correlation, impact analysis, and event enrichment.

The following section outlines the data that is synced from UCS Manager:

- Chassis
- Blades
- Linkage between Blade and ESXi Host

The UCSMsync service synchronizes configuration changes in UCS Manager using a polling mechanism, based on the polling interval. The default polling interval is 15 minutes. You can change the polling interval in the UCS Manager configuration page in Infrastructure Manager.