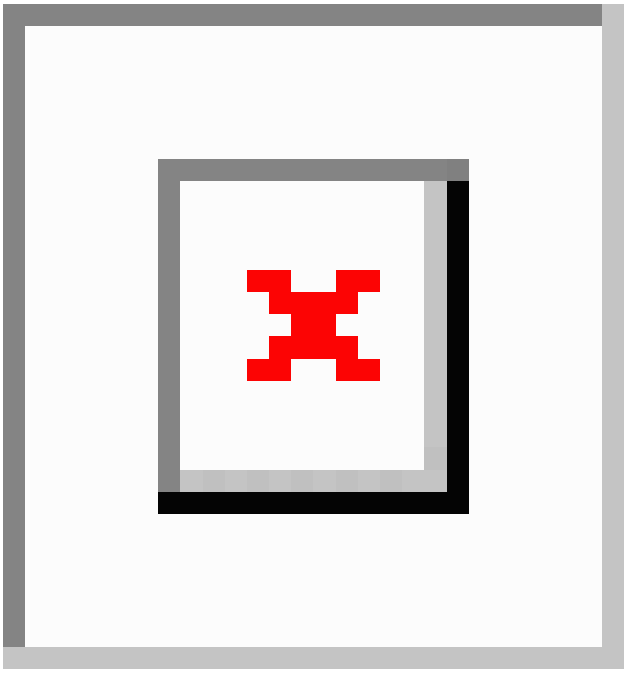
Planning Overview

- Cisco HCM-F application node overview, on page 1
- Cisco HCM-F WS node , on page 3
- Cisco HCS Shared Data Repository, on page 4
- API Gateway Proxy, on page 5
- API Gateway High Availability, on page 6
- Infrastructure Platform Automation Description, on page 6
- Cisco HCS Fulfillment service, on page 7
- Cisco Prime Collaboration Assurance, on page 10
- Cisco HCS Domain Manager Adapter for Cisco Prime Collaboration Assurance, on page 13
- Cisco HCS Service Inventory, on page 14
- Cisco HCS Platform Manager, on page 15
- Cisco HCM-F Real-Time Monitoring Tool , on page 16
- Cisco HCM-F administrative interface, on page 16
- Cisco HCS North Bound Interface Web Service API, on page 18

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

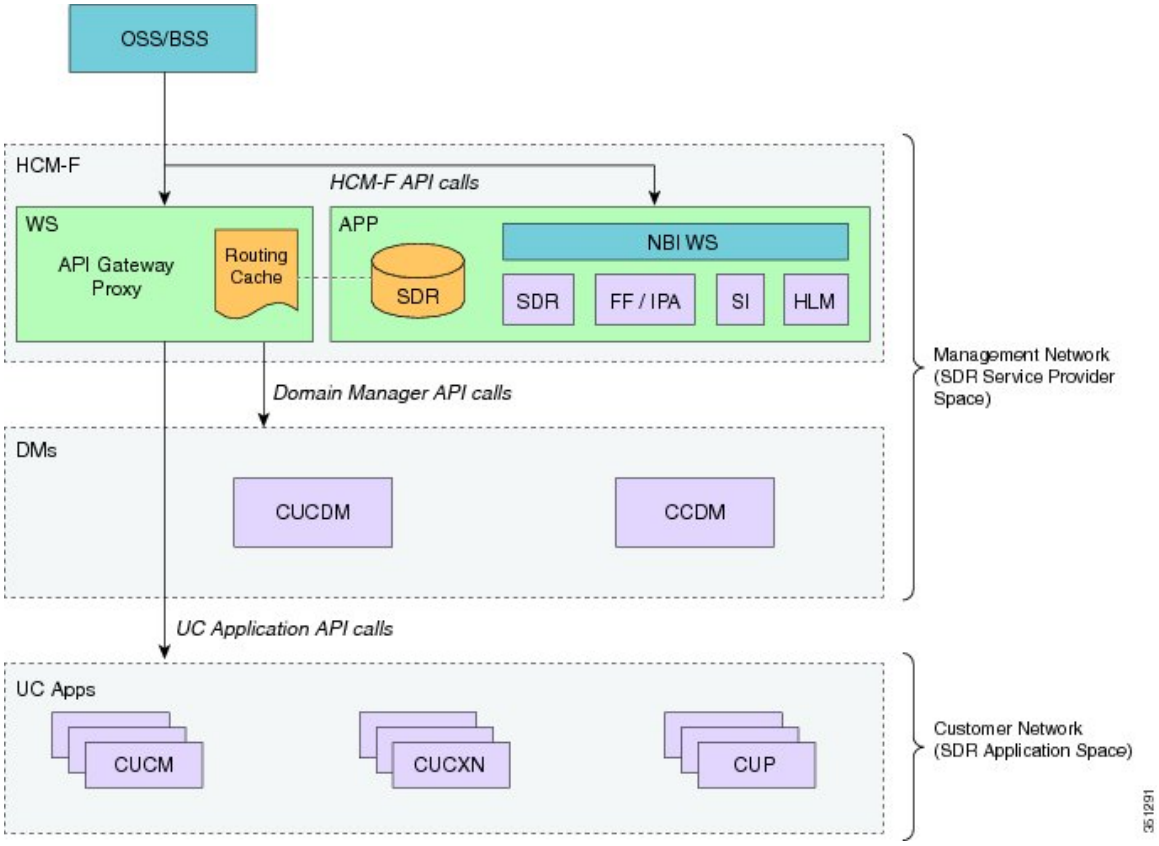
Note Fulfillment and CHPA work together to automatically configure CUCM applications with the data needed for those applications to be monitored by PCA. Other applications such as CUCxn and CUP must be manually configured to be monitored by PCA.

- **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

Note The HCM-F API Gateway Proxy service is deprecated and will be removed in a future release. Cisco recommends using the Cisco Unified CDM 10.6(x) API to access service fulfillment information. See *Cisco Unified Communications Domain Manager, Release 10.6(2) API Reference Guide*.

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 on 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.

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 service provider-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 onboarding 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 V after migration is complete. You can fail over to the source VMs if there is problem with the new VMs. When you are satisfied with the migration, you manually delete the source VMs.

- Perform operations on clusters, 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 Prime Collaboration Deployment for UC Applications

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.
- Device 360° View—Provides concise summary information for any device when you rest your mouse over a device IP address, then click the quick view icon. You can view device information such as status and location, view modules, alarms, and interfaces on the device, and invoke tools such as ping and traceroute for the device.
- 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	

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
Contact Center: CVP	CUOM	CUOM	CUOM	PCA	PCA	PCA	PCA	
CUBE-ENT		CUOM	CUOM	PCA	PCA	PCA	PCA	
Finesse		CUOM	CUOM	PCA	PCA	PCA	PCA	
MediaSense		CUOM	CUOM	PCA	PCA	PCA	PCA	
CER				PCA	PCA	PCA	PCA	
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
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 service provider 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 service provider 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 11.5 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 11.5 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 11.5(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 11.5(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 15.

For instructions on how to perform Platform Manager configuration tasks, see the *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide, Release 11.5(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 Default Deployment Mode, creating or deleting an HCS License Manager, assigning a customer or UC cluster to an HCS Prime License Manager, and more.

Note If the Default Deployment Mode is not provided in the License Manager and you have also not specified any deployment mode while adding License Manager, then HCMF will not set any deployment mode for License manager.

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