CHAPTER 1

Introduction to Cisco Hosted Collaboration Mediation Fulfillment

Cisco Hosted Collaboration Solution (HCS) is a next-generation unified communications and collaboration platform for service providers who want to offer unique Cisco collaboration technologies using hosted and managed models. Cisco HCS is a distributed system, consisting of Cisco hardware and software products, that work together to enable service providers to offer the following services to their customers:

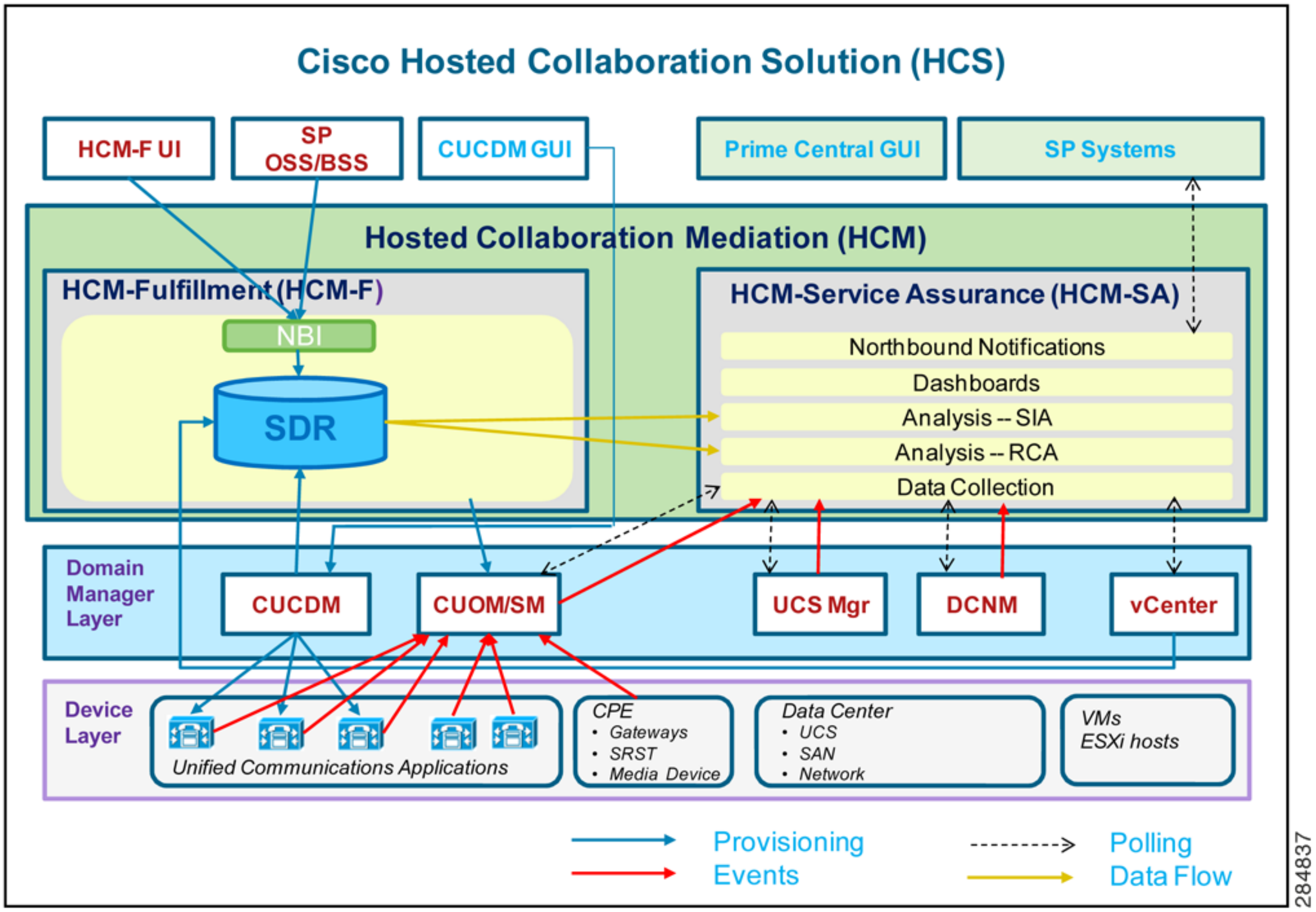
- Voice
- Video
- Messaging and presence
- Audio conferencing
- Mobility service
- Collaboration

Functional Overview of Cisco HCS

Cisco HCS provides tools to provision, manage, and monitor the entire architecture to deliver service in an automated way, assuring reliability and security throughout SP operations. Cisco HCS optimizes data center (DC) environments, reducing the operation footprints of service provider (SP) environments.

Figure 1-1 on page 1-2 illustrates a high-level view of Cisco HCS.

Figure 1-1 Cisco HCS Functional Overview



The device layer contains the devices that deliver the Cisco HCS services to the customers and end users. Examples of services are voice, video, messaging and presence, and audio conferencing.

The domain manager layer contains the domain managers that manage the services and devices. The domain managers perform the provisioning of the devices and services. The domain managers also perform fault management and performance management for the devices.

Hosted Collaboration Mediation (HCM) performs centralized management for the entire Cisco HCS solution. HCM interacts with all the domain managers.

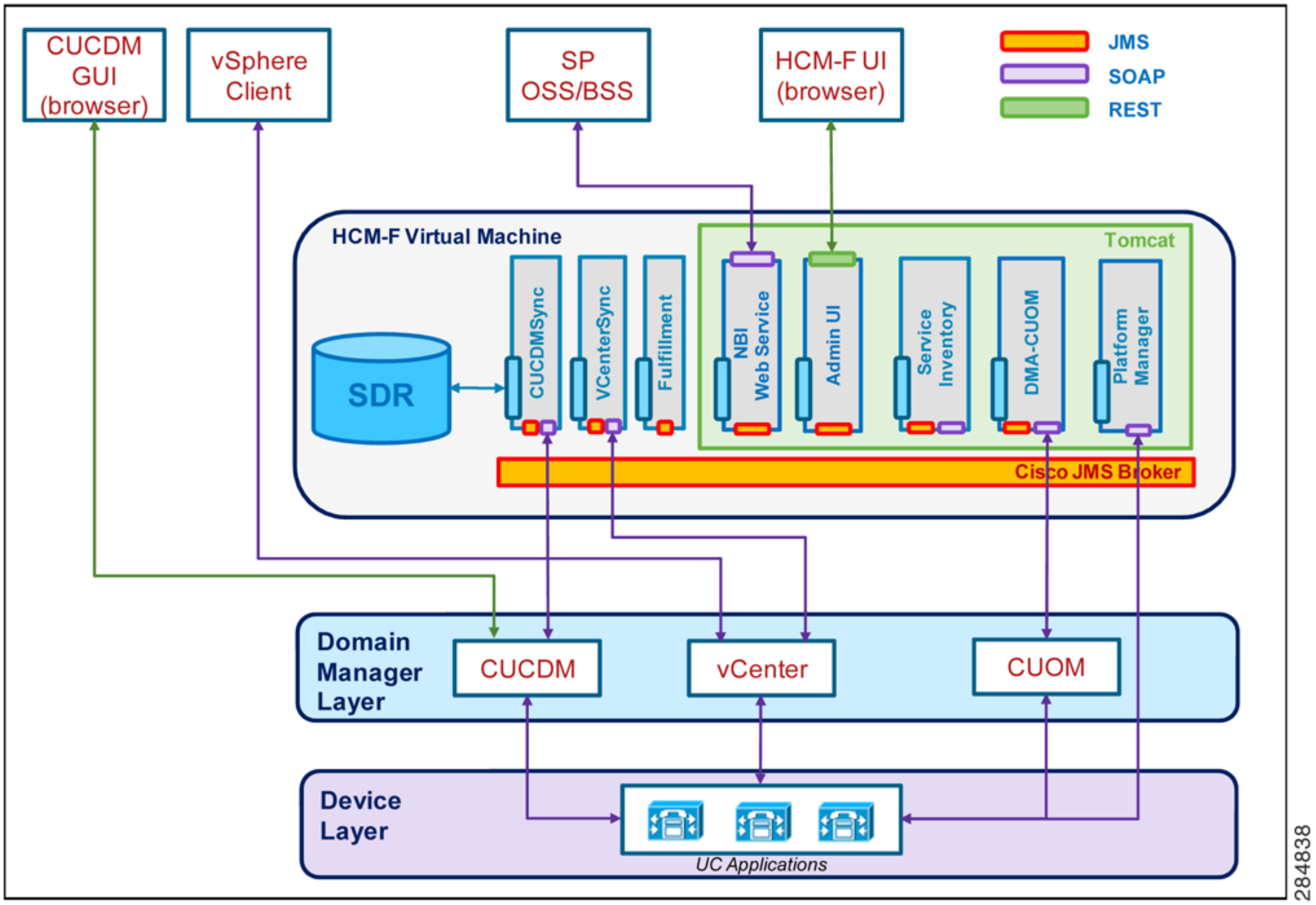
HCM also performs aggregation and provides a central connection to the SP cloud. HCM provides northbound interface (NBI) services to integrate Cisco HCS with the SP business support system (BSS), operational support system (OSS), and manager of managers (MoM).

HCM comprises two portions: Cisco HCM-Fulfillment (HCM-F) and Cisco HCM-Service Assurance (HCM-SA). This document focuses on the functions of the Cisco HCM-F portion of Cisco HCS.

Overview of Cisco HCM-F

Figure 1-2 on page 1-3 illustrates the architecture of Cisco HCM-F.

Figure 1-2 Cisco HCM-F Architecture



Cisco HCM-F 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.
  - Northbound Interface (NBI) service allows changes to the SDR through the SP BSS or OSS
- **Cisco HCM-F Administrative UI:** Allows configuration, management and monitoring of Cisco HCM-F services. It also allows the application of manual changes to the SDR.
- **Services for automatic configuration of the Cisco Unified Operations Manager (CUOM):**
  - HCS Fulfillment service

  - HCS DMA-CUOM service

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

- **HCS Northbound Interface (NBI) API service:** Provides an interface to the service provider BSS or OSS.
- **Billing services through Service Inventory:** Provides the service provider with reports on customers, subscribers, and devices. These reports are used by the service provider to generate billing records for their customers.

Cisco HCM-F Component Descriptions

This section provides an overview of the different components and services that constitute Cisco HCM-F.

Cisco HCS Shared Data Repository

The Shared Data Repository 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

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

- HCM-Fulfillment — Supports a series of events for the Cisco HCM-F northbound interface API, and provides data storage for the Cisco HCM-F UI
- HCM-Service Assurance — Supports event enrichment

One Cisco HCS Shared Data Repository gets 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:

- The Cisco HCM-F northbound interface API
- VCenterSync 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 OSS/BSS, interact with the Cisco HCS Shared Data Repository through Cisco HCM-F northbound interface APIs.

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

For More Information

- Cisco HCS CUCDMSync Service, page 1-5
- Cisco HCS VCenterSync Service, page 1-5

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.

you can configure the CUCDMSync Service though the Infrastructure Manager administrative interface. You can enable automatic synchronization by checking the Sync Enable check box. When you check Sync Enabled, data gets automatically synchronized from Cisco Unified Communications Domain Manager to the Cisco HCS Shared Data Repository. You cannot delete or modify data that gets synchronized from Cisco Unified Communications Domain Manager from the Cisco HCS administrative interface or the Cisco HCS NBI. You can only make changes to synchronized data from Cisco Unified Communications Domain Manager itself. If you disable synchronization, you can update the data from the Cisco HCS administrative interface or the Cisco HCS NBI. Before you disable synchronization, review the following considerations:

- You can modify the service provider, but you cannot delete it.
- Deleting a customer does not "cascade delete" the clusters or customer equipment associated with the customer that you delete.
- Deleting a cluster "cascade deletes" the application instances (servers) that are associated with the cluster that you delete.

You can trigger the system to synchronize immediately by triggering a manual synchronization on the Infrastructure Manager administrative interface. You can synchronize for a single customer, for a list of customers, or for all customers. You can also synchronize the service provider information.

To review the results of a synchronization request, you can view jobs that get created in the Infrastructure Manager administrative interface (**Administration > Jobs**). You may see more than one job in the queue because jobs are categorized by entity type; for example, you may see multiple jobs for data centers. Jobs get automatically deleted after 24 hours.

For details on configuration tasks that you can perform for the CUCDMSync Service through the Infrastructure Manager administrative interface, see the "CUCDM Sync Services" section on page 7-5.

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.

You configure vCenter support in the Infrastructure Manager administrative interface for Cisco UCS Manager, computing hardware (ESXiHosts), virtual machines, VMware clusters (collections of ESXiHosts and virtual machines), and VMware data centers (collections of VMware clusters).

When you check the Sync Enabled check box on the vCenter configuration page, automatic vCenter synchronization occurs if the vCenter sync service is running on the Cisco HCM-F platform. If you synchronize data, you cannot delete the following data through the Cisco HCS NBI or the administrative interface. You must delete the data directly on the vCenter server itself.

- VMware Data Center
- VMware Cluster
- Virtual Machine
- ESXi Host (Exception: You can modify the blade link.)

You can modify the vCenter but not delete it. You can modify a data center that contains at least one vCenter with Sync Enabled, but you cannot delete it.

When you uncheck the Sync Enabled check box, you can delete or modify the following configuration in the Infrastructure Manager administrative interface:

- vCenter
- VMware Data Center
- VMware Cluster
- Virtual Machine
- ESXi host

In this case, when you delete data from the Infrastructure Manager administrative interface, all children get "cascade deleted." For example, when you delete a VMware data center, all VMware clusters, which are children of that VMware data center, and all virtual machines and ESXi hosts, which are children of those VMware clusters, get deleted. When ESXi hosts or virtual machines get deleted, you lose the linkages.

You can perform manual synchronizations by configuring a synchronization request in the Infrastructure Manager administrative interface. Manual synchronization requests trigger an immediate synchronization of the data. You can specify the type of immediate synchronization that occurs. For example, you can select for the following options:

- Service Provider – Data for all data centers and customers in the system get synchronized.
- Customer – Only data for the selected customers get synchronized.
- Data Center – Data for all vCenters in the data center get synchronized.
- vCenter – Data only for the selected vCenter get synchronized.

To review the results of a synchronization request, you can view Jobs that get created in the Infrastructure Manager administrative interface (**Administration > Jobs**).

For instructions on how to configure manual or automatic synchronization through the Infrastructure Manager administrative interface, see the "vCenter Sync Services" section on page 7-6.

Each vCenter has a certificate that is used to authenticate the connection. The vCenter sync service does not validate the vCenter certificate by default. To enable certificate validation, run the following command from the CLI on the Cisco HCM-F platform:

set hcs vcentersync require-vcenter-certificate enable

After running this command, you must restart the Cisco HCS VCenterSync Service. If certificate validation is enabled, import the certificate to the Cisco HCS server trust store, as described in the following procedure:

Step 1 Using Firefox, browse to the vSphere server at https://<your-vsphere-server>:8443. Select **Firefox > Options > Options**. Click **Advanced**; then, click the **Encryption** tab. Click **View Certificates**.

Step 2 Find the server to which you browsed; click on it; then, click **Export**. Save the PEM file to a file.

Step 3 Import the vSphere certificate to the Cisco HCM-F platform:

a. From the CLI on the Cisco HCM-F platform, you enter the command **set cert import** with the following parameters:

- type — mandatory cert type, which is normally set to trust.
- name — mandatory unit name, which is set to tomcat.
- caCert — optional name of the caCert, which is set to the certificate name.

For example, you may enter *set cert import trust tomcat <name of your certificate>*.

b. After you run the command, the CLI prompts you to paste in the certificate. Using any text editor, open the .crt file you saved. Copy and paste the entire contents of the file at the CLI prompt.

c. After you upload the certificate, restart the Cisco HCS VCenterSync Service through the CLI.

Cisco HCS Fulfillment Service

The Cisco HCS Fulfillment Service is a standalone Java application. It performs two functions:

- To trigger provisioning of the CUOM: The Fulfillment service automatically detects data changes in the SDR related to devices, and triggers the DMA-CUOM to provision those devices on the CUOM.
- To automatically link a virtual machine to an application instance within the SDR.

The following sections describe these two functions of the Fulfillment service.

Role of the Fulfillment Service in the Configuration of the CUOM

The key role of the HCS Fulfillment service is to detect changes on the SDR and instruct the DMA-CUOM to configure the CUOM to reflect those changes. The Fulfillment service detects when devices are added, deleted, or modified in the SDR.

The Fulfillment service automatically detects data changes in 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

When new devices are added to the SDR, the Fulfillment service instructs the DMA-CUOM to configure the CUOM to start monitoring those devices. The Fulfillment service also detects when devices are deleted or changed in the SDR and instructs the DMA-CUOM to make the required changes to the CUOM configuration to reflect those changes in the SDR.

Linking Virtual Machines to Application Instances

A second function of the Fulfillment service is to link a virtual machine (VM) to an application instance within the SDR. Service Assurance uses the VM link to an application instance to perform fault correlation and event enrichment. This function is enabled by default, but you can disable it through the administration CLI.

This function supports HCM-Service Assurance functions. If this function is enabled and you are using overlapping hostnames, the results will be somewhat unpredictable, and you can disable it through the CLI. However, you are recommended not to use overlapping hostnames.

For information on CLI commands, see the "Command Line Interface for Cisco HCM-F" section on page 10-1.

Cisco HCS Domain Manager Adapter for the CUOM

In the Cisco HCS architecture, Domain Managers (DMs) are components that manage, monitor, or control other solution services. Examples of DMs are the CUOM, the CUCDM, and vCenter.

The Cisco Unified Operations Manager (CUOM) is an existing Cisco network management server for Cisco voice products. In the Cisco HCS solution, the CUOM is a DM that performs monitoring of Cisco HCS network applications and devices. The CUOM receives SNMP traps from the monitored devices and forwards them to the Event Collector for processing.

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

A second function of the DMA is to monitor CUOM limits and generate a trap when thresholds are reached.

The DMA-CUOM 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-CUOM to configure the CUOM to reflect changes on the SDR.

The DMA-CUOM can perform the following configuration changes on the CUOM:

- Add device
- Update device credentials
- Delete device

For instance, when a new device is added through vCenter and configured through the CUCDM, the VCenterSync service and the CUCDMSync service update the SDR with the change. The Fulfillment service detects the change in the SDR and instructs the DMA-CUOM to begin monitoring the new device. The DMA-CUOM then reads the device details from the SDR and programmatically configures the device (through SOAP) for monitoring in the CUOM.

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

- The CUOM must be added on the Cisco HCM-F Infrastructure Manager Administrative UI. The CUOM must be configured with an IP address on the SP space, and hostname, as well as the ADMIN credentials.
- The customer (or application cluster or customer equipment) is manually related to a CUOM in the Cisco HCM-F UI.

- 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 CUCDM 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.

For instructions on how to perform configuration tasks through the Infrastructure Manager administrative interface, see the "Infrastructure Manager Configuration" section on page 7-1.

Configuration of Trap Destinations

For the CUOM to monitor UC applications and customer equipment devices, these devices must be configured with a trap destination to the correct CUOM. The DMA-CUOM does not automatically configure the trap target in any UC applications or CPE devices. These devices must be manually configured to forward traps to the correct CUOM. The CUOM must also be ***manually*** configured with a trap destination to the Event Collector for processing. The Event Collector is a component of Cisco HCS-Service Assurance (HCM-SA) solution.

SNMP Trap Flow

The DMA-CUOM configures the CUOM to monitor UC Applications and customer equipment devices, but it does not collect SNMP traps from the devices. After the CUOM has been configured to monitor the devices, it collects traps from the monitored devices, aggregates the traps and forwards them to the Event Collector in HCM- SA. The Event Collector collects the traps from the CUOM and other DMs in the Cisco HCS solution and processes the traps. The HCM-SA solution aggregates all the traps from all the DMs, performs event enrichment, and displays the results on the Prime Central for HCS GUI. HCM-SA also provides an NBI API for integration with the SP MoM.

For information on how to configure trap destinations on the CUOM, refer to the CUOM documentation.

Cisco HCS Service Inventory Service

Cisco HCS Service Inventory is an application that provides reports for service providers for billing purposes. These reports contain data on customers, subscribers, devices, and other details that are currently provisioned on Cisco Unified Communications Domain Manager. Service Inventory automatically transfers the report files at regular configurable intervals to remote SFTP servers. The service providers use these reports to generate billing records for their customers.

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 for information. Cisco Unified Communications Domain Manager 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.

The reports use a Cisco common format. For more information on this format and the data that is generated, see *Cisco Service Inventory Common Format Specification.*

For instructions on how to perform configuration and scheduling tasks through the Service Inventory administrative interface, see the "Service Inventory Configuration" section on page 6-1.

Cisco HCS Platform Manager Service

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

- Cisco Unified Presence
- Cisco Unified Communications Manager
- Cisco Unity Connection

The Platform Manager allows you to manage and monitor the installation, upgrade and restart 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 Presence 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.

For instructions on how to perform configuration tasks for the Platform Manager, see the "Platform Manager Configuration" section on page 8-1.

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:8443.

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

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

- Service Inventory
- Infrastructure Manager
- Platform Manager

Service Inventory

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 Service Inventory billing reports. Service Inventory transfers these report files to remote servers using SFTP. Service providers use these reports to generate bills for their customers.

For more information on the Service Inventory application, see Cisco HCS Service Inventory Service, page 1-9.

For information on configuration tasks you can perform through the Service Inventory Administrative Interface, see the “Service Inventory Configuration” section on page 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.

For information on configuration tasks you can perform through the Infrastructure Manager Administrative Interface, see the “Infrastructure Manager Configuration” section on page 7-1.

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.

For more information on the functions of the Platform Manager, see “Cisco HCS Platform Manager Service” section on page 1-10.

For information on configuration tasks you can perform through the Platform Manager Administrative Interface, see the “Platform Manager Configuration” section on page 8-1.

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 an 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

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.

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.

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 HCS North Bound Interface Web Service APIs, see the *Developer Guide for Cisco Hosted Mediation Collaboration Fulfillment*.

Related Topics

- Installation of Cisco HCM-F, page 2-1
- Services on the Cisco HCM-F Platform, page 3-1
- Backup and Restore for Cisco HCM-F, page 4-1
- The Cisco HCM-F Administrative Interface, page 5-1
- Service Inventory Configuration, page 6-1
- Infrastructure Manager Configuration, page 7-1
- Platform Manager Configuration, page 8-1
- Command Line Interface for Cisco HCM-F, page 10-1
- Service Inventory Common Format, page 13-1