CHAPTER 3

Cisco HCS 8.6(2)ES2

This chapter provides information on the following topics:

New Components for Cisco HCS 8.6(2)ES2

For a list of new Cisco HCS components that are supported in Cisco HCS 8.6(2)ES2, see the *Compatibility Matrix for Cisco Hosted Collaboration Solution*. In that document, you can search for the word *New* to locate any new components.

Upgrade and Migration

To identify compatibility information for Cisco HCS components before you upgrade to Cisco HCS 8.6(2)ES2, see the *Compatibility Matrix for Cisco Hosted Collaboration Solution.*

For More Information

Upgrading Components for Cisco Hosted Collaboration Solution - http://www.cisco.com/en/US/products/ps11363/prod_installation_guides_list.html

IP Multimedia Subsystem

As a service provider, you may have IP Multimedia Subsystem (IMS) in your network, which is the core network to provide routing and other common services such as billing, provisioning, and so on. In Cisco HCS, the IMS network is placed at the aggregation layer, and Cisco Unified Border Element (SP Edition) is the interface point between IMS and the Cisco HCS.

You can connect with the IMS interwork by using one of the following deployment models:

- Peering-based business trunking—The IMS and NGCN networks connect as peers through Interconnect Border Control Functions (IBCF). The business subscribers are not necessarily provisioned in HSS. The point of interconnection between the peer network and IMS is the IMS Ici interface. This configuration is supported in Cisco HCS 8.6(1).
- ISC Interface Interconnect Model—In the ISC interface interconnect model, the Cisco Unified Border Element (SP Edition) is inserted between S-CSCF and Unified CM, which is specific to Cisco HCS. Unified CM can be connected to S-CSCF without Cisco Unified Border Element (SP Edition); however, in Cisco HCS, Cisco Unified Border Element (SP Edition) provides DTMF feature interworking. DNS configurations and Cisco Unified Border Element (SP Edition) configurations have requirements that related to the name of the application server, as stated in "Configuration" section on page 3-4.

Tip In Cisco HCS 8.6(2)ES2, Cisco Unified Border Element (SP Edition) provisioning is not part of Cisco HCS management functions. Cisco Unified Border Element (SP Edition) provides HTTP-based provisioning interfaces, which may be used by Cisco HCS to push the configuration files and manage the Cisco Unified Border Element (SP Edition) configuration.

In Cisco HCS 8.6(2)ES2, an additional model is introduced for integrating with IMS network. In this model, Unified CM appears as an application server in the IMS network for the mobile phones, and an ISC interface is used between IMS and Cisco HCS.

The following features are introduced in Unified CM 8.6(2)ES2:

- IMS integration ISC interface compliance
- Full Support of P-Charging-Vector

The key requirement for the ISC interface is the support of Route header for application sequencing so that the mobile service provider can combined features delivered by multiple application servers for the same call. Other significant requirements include the support of P-Charging-Vector and P-Charging-Function addresses.

Unified CM as Application Server in IMS

The IMS Application Server requirements are based on the IMS ISC interface (3GPP specification TS 24.229 v 9). The deployment includes a Cisco Unified Border Element (SP Edition) between IMS and the Unified CM Application Server. The Cisco Unified Border Element (SP Edition) is inserted to support the media anchoring, DTMF conversion, and some SIP header manipulations.

The ISC interface is defined as call-processing control interface between S-CSCF and the application server. This interface runs SIP (normal protocol) as defined by RFC 3261, with additional enhancements for origination or termination of the call leg toward the application server.

When the initial request (INVITE) is received on a SIP ISC trunk, the top most route header must correspond to the Unified CM (the ISC trunk configuration will have the ability to specify this URI to validate the route header), and there is at least one other route header (corresponding to S-CSCF).

The P-Charging-Vector header is defined by 3GPP to correlate charging records generated from different entities that are related to the same session. It contains the parameters ICID and IOI.

The Unified CMs will use cluster ID, concatenated with a unique number as the ICID. The IOI identifies both originating and terminating networks involved in a session/transaction.

Features and Services Support

All DTMF-based features offered to mobile clients in earlier Cisco HCS releases are applicable for IMS-integrated clients in the Cisco HCS 8.6(2)ES2 ISC interface model. However, signaling-based midcall features are not supported over the ISC interface in Cisco HCS 8.6(2)ES2.

IMS application servers provide originating services and terminating services. The following Unified CM services exist:

- Originating Services—The call anchoring service enables Single Number Reach (SNR) features, enterprise dial plan, and class of service features, and DTMF features. In Cisco HCS 8.6(2)ES2, when a mobile number is called, the call is forked to the mobile and shared deskphone. Both phones ring.
- Terminating services—Call anchoring service enables SNR features and DTMF features.

Unified CM can support the existing native Mobility features through ISC interface to a mobile subscriber:

- Enterprise dial plan (including extension dialing)
- Enterprise policy (class of service via calling search space)
- Single Number Reach through both enterprise directory numbers (DN)
- Single Number Reach even when a user dials the mobile directory number (Also rings the shared devices)
- Call moves between mobile phones and desk phones
- Single voicemail and messages waiting indicator (MWI)
- Mobile BLF presence status
- DTMF-based midcall features (hold/resume/transfer/conference/park/dust)
- Some shared line features, including remote-in-use from desk phone and barge from shared desk phone

For IMS, integrated Mobile feature support in Unified CM includes:

- Midcall Enterprise Feature Access Support Using DTMF—You can configure DTMF feature codes as service parameters: enterprise hold (default equals *81), enterprise exclusive hold (default equals *82), resume (default equals *83), transfer (default equals *84), conference (default equals *85) and dusting (default equals *74).

Call Flows

The following call flows are supported in an IMS network for Cisco HCS:

- Basic calls:
  - IMS mobile device to Cisco HCS deskphone
  - Cisco HCS deskphone to IMS mobile device
  - IMS mobile device to IMS device
  - IMS mobile device to PSTN phone
  - PSTN phone to IMS mobile device
- Mobility Features:
  - Single Number Reach (SNR) - Deskphone pickup and Remote Destination Pickup, cases for the following call flows:
    - IMS to Cisco HCS SNR deskphone
    - IMS to Cisco HCS SNR MSISDN

  - IMS (SNR MSISDN) to Cisco HCS
  - IMS (SNR MSISDN) to Cisco HCS (SNR MSISDN)
- Midcall transfer (DTMF), midcall conference (DTMF), midcall hold/resume (DTMF)
- Call park (DTMF)
- Call move
- Dual-mode mobility client (iPhone, Nokia)

Configuration

In the service provider IMS network, the mobile subscribers are provisioned in the Home Subscriber Server (HSS). The Public-id of the IMS subscriber must match the Mobility Identity of the Unified CM IMS client. The Initial Filter Criteria is an IMS provisioning element, provisioned in IMS client's Mobile Identity. This element triggers the Unified CM Application Server for originating and terminating services.

In Cisco HCS, the Cisco Unified Border Element (SP Edition) is placed in the ISC interface in between the Unified CM and SCSF. This requires Cisco Unified Border Element (SP Edition) to be configured with specific adjacencies for the ISC interface. The configuration must ensure that the route header requirements of ISC interface are properly handled. While there are multiple ways of configuring, we recommended that Cisco Unified Border Element (SP Edition) transparently passes the route headers in both directions. This means when IMS sends the call with route header UnifiedCMas@CiscoHCS.cisco.com to Cisco Unified Border Element (SP Edition), the following actions occur:

- IMS network ensures that UnifiedCMas@CiscoHCS.cisco.com resolves to configured Cisco Unified Border Element (SP Edition) adjacency.

  ```
  Example: UnifiedCMas@CiscoHSC.cisco.com
  ```

- Within Cisco HCS, UnifiedCMas@CiscoHCS.cisco.com resolve to Unified CM, and Cisco Unified Border Element (SP Edition) sends it to Unified CM with the same route header. The Cisco Unified Border Element (SP Edition) adjacency configuration ensures that this route header is used to select the Unified CM adjacency.

For Unified CM to work with IMS, you must configure the IMS clients and ISC trunks:

- A new phone type, IMS-integrated Mobile (Basic), exists. This phone type is similar to Cisco MobileClient. Be aware that not all Mobility Identity (MI) functionality is available for the IMS client. DTMF and other features for the IMS-integrated Mobile are similar to Cisco MobileClient features (hold/exclusive hold/resume/conference/transfer/dusting).
- A new SIP trunk type, ISC, exists. In this release, the ISC trunk in Unified CM is added to support route header. Unified CM uses the top route header in the initial INVITE to determine how to handle the request, either as an originating call, as a terminating call, or as a regular SIP call.

  In addition to ISC trunk, standard SIP trunk is also required for the IMS network. This is to ensure that the IMS network as part of the aggregation layer for Cisco HCS can support non-IMS client calls.

Video Support

Cisco HCS 8.6(2)ES2 supports existing desktop video endpoints in a point-to-point (two-party) mode for intracompany or intercompany calls. Cisco HCS 8.6(2)ES2 supports multipoint video conferences, as in ad hoc, rendezvous, or scheduled conferences, through a customer-dedicated MCU that registers

directly to Cisco Unified Communications Manager. Architectural requirements for video in Cisco HCS focus on the management infrastructure and, in the case of intercompany video, in the Cisco Unified Border Element (SP Edition).

Tip An MCU is a multimedia conference bridge media resource that joins multiple participants into a single call. It can accept any number of connections for a given conference, up to the maximum number of streams allowed for a single conference on that endpoint.

Cisco TelePresence MCUs include a built-in web server that allows for complete configuration, scheduling, control, and monitoring of the system and conferences. Similarly, Cisco TelePresence MCUs have a built-in IVR that allows for conference setup. In this deployment model, the MCU is simply a route pattern from Unified CM that allows users to make calls to the MCU to create or join conferences through the IVR. When a conference is scheduled through the MCU web interface, the MCU resources and the conference ID get reserved so that the participants can join the conference at the specified time by dialing directly into the MCU.

Cisco HCS 8.6(2)ES2 also supports multipoint video conferences through a customer-dedicated MCU that registers directly to Unified CM. Unified CM allocates video media resources from an MCU that is registered with the Unified CM cluster for ad hoc or meet me conferences when a conference is set up from any video endpoint, in the same way that audio conferences are set up through the use of conference, join, or cBarge softkeys. If two parties are engaged in a video call and the call is escalated to a multipoint call, Unified CM attempts to allocate video-capable bridges. If a bridge is not available, Unified CM terminates the video session leaving only a multipoint audio call. If a phone that supports audio only gets added to a video conference, the MCU conference resources are used, but the phone is added as audio only.

Cisco HCS 8.6(2)ES2 can support CAST-capable endpoints that display video either through Cisco Unified Video Assistant 2.2 or later releases of Cisco Unified Personal Communicator 8.0. Cisco HCS 8.6(2)ES2 can also support endpoints that support video natively through video codecs that are directly on the endpoint.

Cisco HCS 8.6(2)ES2 can support third-party SIP video endpoints. In this case, the Unified CM configuration for these video endpoints is similar to third-party SIP phones that are supported through Unified CM.

Unified CM terminates the video session, leaving only a multipoint audio call. If a phone that supports audio only gets added to a video conference, the MCU conference resources are used, but the phone is added as audio only.

Two-way interactive video calls are supported as intra-customer calls, inter-Cisco HCS customer calls where Cisco Unified Communications Manager Session Management Edition supports the aggregation layer, or SCCP to SCCP video calls or SIP to SIP video calls. Cisco HCS 8.6(2)ES2 can support the following types of endpoints:

- CAST-capable endpoints that display video either through Cisco Unified Video Assistant 2.2 or later releases of Cisco Unified Personal Communicator 8.0
- Endpoints that support video natively through video codecs that are directly on the endpoint
- Third-party video endpoints that use SIP

Note To determine the video endpoints that are supported with Cisco HCS 8.6(2)ES2, see the *Compatibility Matrix for Cisco Hosted Collaboration Solution (HCS)*.

Limitations, Restrictions, and Considerations for Video

- Cisco HCS 8.6(2) does not support Cisco TelePresence Video Communication Server (Cisco VCS).
- For static call admission control (CAC), location and region processing already exists for video and works in Cisco HCS 8.6(2)ES2 the same way it works in the compatible release of Unified CM 8.6. Cisco HCS 8.6(2) does not support RSVP CAC.
- Cisco HCS 8.6(2) does not support alpha dialing.
- Unified CM can support up to five simultaneous SDP m-lines:
  - Bidirectional audio.
  - Bidirectional personal video (also known as presenter video).
  - Unidirectional presentation video (H.239)—Cisco Unified Border Element (SP Edition) supports presentation video for intercompany calls or intracompany calls.
  - BFCP (Binary Floor Control Protocol) presentation control channel—For intracompany video calls, BFCP is supported, including with video conferences using the Cisco TelePresence (high-end) MCUs. For intercompany calls, BFCP is supported with Cisco Unified Border Element (SP Edition) in Version XE3.3.
  - FECC (far-end camera control)—For intercompany calls, FECC is supported with Cisco Unified Border Element (SP Edition) in Version XE3.3, which is supported with Cisco HCS 8.6(2)ES2.
- Cisco HCS 8.6.(2)ES2 supports video encryption for point-to-point video calls between high-end CTS endpoints only.

  For example, Cisco TelePresence System EX40 and EX60 endpoints support video encryption only when they are registered to Cisco VCS, so video encryption is not supported with these endpoints in Cisco HCS 8.6. These endpoints can support audio encryption when these devices are registered directly to Unified CM; that is, if encryption is configured. For example, MCUs that register directly to Unified CM do not provide video encryption.
- TelePresence Interoperability Protocol is a peer-to-peer protocol that, if supported by both peers in a video call, gets negotiated over the RTCP stream independently of Cisco HCS or Unified CM. This protocol provides extended functions for video participants. When MTP resources are involved in the media path, RTCP gets processed in the following ways:
  - Unified CM-based MTPs—Not passed
  - IOS-based MTPs—Some passed
  - Cisco Unified Border Element (SP Edition)—Passed

  RTCP support is required for TelePresence Inter operability Protocol. No configuration is required in Unified CM to make this protocol work.
- All intracompany video is passed directly end to end. Cisco HCS 8.6(2)ES2 supports all point-to-point functionality.
- Cisco recommends that you use DHCP option 150 for TFTP/Unified CM support.
- For Cisco HCS, Cisco recommends high-bandwidth video (for example, 384 kbps or greater) between devices in the same site and recommends low-bandwidth video (for example, 128 kbps) between devices at different sites. The Cisco Unified Video Advantage Wideband Codec at 7 Mbps is recommended only for calls between devices at the same site.
- For Cisco HCS, Cisco recommends that WAN connections operate at link speeds of 768 kbps or greater.

Cisco Unified Communications Domain Manager—Configuration Options for Video

The following section describes where you can configure the Cisco HCS-specific options for video endpoints. This section assumes that you have installed (or plan to install) the video endpoint according to the documentation that accompanies your endpoint.

- Bulk Loader—You add video endpoints through the base data bulk loader. Third-party SIP video endpoints use the Generic Desktop Video Endpoint, Generic Multiple Screen Room System, and Generic Single Screen Room System options. Cisco video endpoints are identified by the product name.
- EMCC Region Max Video Call Bit Rate (Includes Audio)—You configure in the EMCC Parameters Configuration page.
- Enable video—You configure in Feature Group Templates for endpoints that support video.
- Video WAN Bandwidth (Kbps)—You configure when you add building configuration to Cisco Unified Communications Domain Manager.

Tip Device-specific parameters (product-specific configuration parameters) for endpoints are manually configured in Cisco Unified Communications Manager.

You cannot provision the Cisco TelePresence MCU or Cisco ISR PVDM-3 in Cisco Unified Communications Domain Manager. You configure the Cisco ISR-G2 PVDM-3 video conference bridge and transcoders and manually add them in Cisco Unified Communications Manager. You must manually set up and register the Cisco TelePresence MCUs in Unified CM.

Recommendations to Ensure That Cisco TelePresence System EX40 and EX60 Endpoints Can Boot to Unified CM (Instead of Cisco VCS)

To ensure that the Cisco TelePresence System EX40 and Cisco TelePresence System EX60 endpoints can boot to Unified CM, perform the following tasks:

- Make sure that the endpoint has a supported firmware load that is compatible with the version of Unified CM that you are running.
- Configure the endpoint so that it is locally configured to use CDP to set the proper VLAN.
- Set DHCP option 150 to force the endpoints to connect/boot to Unified CM.

  Configure E20/EX60/EX90 endpoints through the provisioning wizard to boot to Unified CM. Selecting Unified CM automatically enables CDP to assign the proper VLAN and detect DHCP option 150, which ensures that the endpoint uses TFTP and Unified CM.

Requirements for Cisco Unified Video Advantage or Cisco Unified Personal Communicator CAST Support

For CAST-based video support through Cisco Unified Video Advantage or Cisco Unified Personal Communicator, endpoints must support a firmware load that allows CAST to work with SIP. The endpoints must support an ethernet phone port in which the PC for the Cisco Unified Video Advantage or Cisco Unified Personal Communicator is attached.

Tip The CAST software implements a security feature where it uses CDP to determine that the CAST client is attached only by the switch port; this prevents an attacker in the network from acquiring video on behalf of the phone.

For More Information

- For information on security for the SIP endpoint, go to http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/8_5_1/secsipvideo.pdf
- *Compatibility Matrix for Cisco Hosted Collaboration Solution*
- *Deployment Guide for Cisco Unified Communications Domain Manager*
- *Bulk Loader Guide for Cisco Unified Communications Domain Manager*

Service Fulfillment

This section contains information on the following topics:

Cisco Unified Communications Domain Manager 8.0.0

Cisco Unified Communications Domain Manager supports new and updated functionality for the following areas:

Tip Depending on the feature, you may review changes for the interfaces, bulk loader, or model.

Cisco Extension Mobility Cross Cluster

Cisco Extension Mobility Cross Cluster (EMCC) extends the system current Cisco Extension Mobility functionality to allow the user to log in to a device from within a connected cluster anywhere in the world. This enables the user to retain the settings, services, and lines that are available with the home location of the user.

The system automates most of the EMCC provisioning to enable this feature to work on all dial plans across multiple Cisco Unified Communications Manager (Unified CM) clusters that are managed by the same platform instance. The system automates provisioning of the home cluster when the Unified CM clusters are managed by separate platforms; that is, cross-cluster configuration across multiple platforms is not supported. The system provides a report of the EMCC configuration on the home cluster and information on what needs to be provisioned in the visiting cluster in order to fully support EMCC.

EMCC Considerations

Review the following EMCC considerations:

- A user from the home cluster goes to the visiting cluster and logs in to a phone. The two clusters can be in different countries/territories.

- The user cannot be authenticated in the visiting cluster; but, because the cluster is EMCC enabled and the phone is subscribed to the EMCC service, the cluster searches for the user in defined EMCC remote clusters.
- After the user (also subscribed to the EMCC service) is authenticated, the phone is unregistered from the visiting cluster and reregistered to the home cluster.
- The geolocation of the phone gets sent to the home cluster, which allows the home cluster to associate the relevant roaming device pool to the user phone by using the geolocation filter.
- The phone behaves exactly as if the user logged in at the home cluster, and all settings and preferences are preserved.
- Calls to the home cluster emergency numbers as well as the visiting cluster emergency numbers breakout at the visiting cluster (physical location).
- Various other elements such as trunks, EMCC countries, and so on, must be configured on both the home and visiting clusters to ensure the feature functions.

Interface Changes

Under Network > PBX Devices, the following interface changes support EMCC:

- The EMCC Server check box displays after you select a Unified CM server to manage.
- The EMCC button displays after you enable EMCC.
- The Home Cluster Setup button displays
- The EMCC Countries button displays.
- The Remote Cluster Management page supports the addition of a new remote cluster or the modification of an existing remote cluster for EMCC.
- The EMCC Parameters page supports the configuration of the EMCC feature parameters and the intercluster service profile.
- The Roaming Device Pool Management screen allows you to add, modify, delete or import roaming device pools to the cluster (or to copy them to other clusters).
- The View EMCC Configuration page shows the existing configuration for the home cluster.
- The EMCC Group Management page allows you to add or remove clusters and countries to an EMCC group (or to modify/delete an existing EMCC group).

Bulk Loader Changes

The following bulk loader changes support EMCC:

- Under the Network workbook, in the Add CUCM Clusters, Add CUCM Subscribers, and Modify CUCM Subscribers sheets, the column EMCC Role was added to the workbook.
- Under the Network workbook, the sheets Add EMCC Countries, Add EMCC Remote Clusters, Add GeoLocation Filter, and Add EMCC Feature Parameters were added to the workbook.
- Under the Location workbook, the sheet Add GeoLocation was added to workbook to support EMCC.

For More Information

- *Deployment Guide for Cisco Unified Communications Domain Manager*
- *Bulk Loader Guide for Cisco Unified Communications Domain Manager*

Supplementary Services for the Cisco Voice Gateway (VG2xx)

You can enable supplementary services, including voicemail, call forwarding, conferencing and speed dials on a Cisco VG2xx analog gateway (SCCP). You can then manage Supplementary Services at the location level as analog line features. The availability of supplementary services depends on whether the service is enabled in the relevant feature group, as well as whether the service is supported by SCCP.

Interface Changes

To configure supplementary services for Cisco Voice Gateway (VG2xx), select **Network > IOS Devices** in Cisco Unified Communications Domain Manager.

For More Information

- *Deployment Guide for Cisco Unified Communications Domain Manager*
- *IOS Model Guide for Cisco Unified Communications Domain Manager*

Speed Dial With Busy Lamp Field (BLF) Call Pickup

An administrator or user can associate a speed dial busy lamp field button on a Cisco Unified IP Phone to a directory number. This phone is known as the call pickup initiator phone. This association allows Unified CM to notify a phone user when a call is waiting to be picked up from the directory number. If auto call pickup is enabled for the BLF, the user presses the BLF button on the call pickup initiator phone to pick up the incoming call. If auto call pickup is not enabled, the phone must remain off hook, or the user must press the Answer key to pick up the call.

The call pickup functionality is available only for speed dial busy lamp fields and is not available for call park busy lamp fields.

Interface Changes

The following options are now supported in Cisco HCS 8.6(2)ES2:

- Under Location Administration > Phone Management, click a phone. Click the **Manage Busy Lamp Fields** button; then, click the **Add** button to display the Call Pickup setting.
- Under Location Administration > End Users, click a user. Click the **Roaming Profile** button and then the **Manage Busy Lamp Fields** button; then, click the **Add** button to display the Call Pickup setting.
- In the Self Care interface, click **My Phones**; then, click **Unique Device Name**. Click the **Busy Lamp button** to display the Call Pickup setting.

For More Information

- *Deployment Guide for Cisco Unified Communications Domain Manager*
- *Self Care Guide for Cisco Unified Communications Domain Manager*

Schedule Enhancements for Bulk Loader

With this enhancement, you can schedule data and model bulk loaders for immediate execution.

Interface Changes

On the Bulk Load File Selection page in Cisco Unified Communications Domain Manager, a new checkbox, Execute immediately, displays. You can check the checkbox to immediately schedule data or model loaders for immediate execution.

(Select **General Tools > Bulk Load**, Click the **Schedule new job** button; then, check **Execute immediately**.)

Database Changes

The database schema for the loader table has changed to add a single Boolean field named immediate, which is set to FALSE by default.

Platform Manager and Cisco Unified Presence 8.6(4)

You cannot use the Platform Manager administrative interface in Cisco Hosted Collaboration Mediation Fulfillment to upgrade to Cisco Unified Presence 8.6(4). To upgrade to Cisco Unified Presence 8.6(4), you must use the Cisco Unified Presence administrative interface to start the upgrade. For more information on Cisco Unified Presence 8.6(4) upgrades, see the Cisco Unified Presence upgrade documentation at

http://www.cisco.com/en/US/docs/voice_ip_comm/cups/8_6/english/install_upgrade/upgrade/guide/Upgrade_Guide_for_Cisco_Unified_Presence_Release_8.6.html

Service Assurance

Service assurance provides enhanced event management NBI support for Prime Central for Cisco Hosted Collaboration Solution Assurance.

NBI Enhancement for Prime Central for Cisco HCS, 1.0

The enhanced Event Management Northbound Interface (NBI) supports multiple SNMP gateway subscriptions. The maximum subscriptions allowed at one time is five. The gateway subscriptions support the ability to filter the incoming traps. A Python client script supports subscribe and unsubscribe calls into the Event Management NBI. In addition, MIB definition for SNMP notifications generated by the NBI is also supported.

This chapter contains the following sections:

Location of Patch

Obtain the patch from the **HCS862 ES2** forum on the Cisco File Exchange Transfer server:

https://upload.cisco.com/cgi-bin/swc/fileexg/main.cgi?CONTYPES=IPCBU-forum

Installing and Executing Patch Script

This section describes the procedure to install and execute the patch script. The client scripts are made available on the Prime Central VM upon on the execution of the patch script.

The patch script can be executed either on Prime Central server or Event Collector server. The script then installs the required files on both Prime Central and Event Collector machines.

The script need not be run on both the machines; it needs to be installed on only one machine.

Note We recommend that you unsubscribe all active subscriptions before you install this patch. Perform the subscription requests, again, after the installation is complete.

Installing the Patch Script

The patch file is a tar file, which has to be installed either on the Prime Central or Event Collector machine. Copy the tar file to the destination machine (Prime Central or Event Collector). On the destination machine, perform the following procedure:

Step 1 Log in as a root user.

Step 2 Copy the tar file on to any location on the Prime Central or Event Collector machine.

Step 3 Run the following command:

```
tar -xf patch-tar-file.tar -C /opt/hcm_installer
```

Executing the Patch Script

You must run the script on either Prime Central or Event Collector machine. If you log in to Prime Central and run the script, Prime Central is the source machine and Event Collector becomes the destination machine. Once you run the script, the following sequence of events occurs:

1. The script establishes a connection between the source and the destination machine.
2. It checks and pushes the required files over the destination machine.
3. It then establishes an SSH connection with the destination machine, and installs the files required.

All of the above activities, including installation, takes approximately 2 minutes.

The script need not be run on both the machines; it needs to be installed on only one machine.

Note If your settings requires passwords to be entered while establishing a connection, you will be prompted for the root password 4 times.

You may choose to run the script on either of the two machines. Depending on the source machine, see one of the following sections:

- Running the Script on Prime Central Machine, page 3-12
- Running the Script on Event Collector Machine, page 3-13

Running the Script on Prime Central Machine

On the Prime Central machine, perform the following steps:

Step 1 Log in as root user.

Step 2 Run the following command

```
[root@machine-name ~]# cd /opt/hcm_installer/scripts/hcm_install_scripts/patch
[root@machine-name patch]# ./pc4hcs_patch_push.py --ec-hostname <IP or hostname>
```

Running the Script on Event Collector Machine

On the Event Collector machine, perform the following steps:

Step 1 Log in as root user.

Step 2 Run the following command

```
[root@machine-name ~]# cd /opt/hcm_installer/scripts/hcm_install_scripts/patch
[root@machine-name patch]# ./pc4hcs_patch_push.py --prime-hostname <IP or hostname>
```

Executing Client Script

After you run the patch script, the client scripts are installed on Prime Central VM.

The scripts are located at the following location in the Prime Central VM: **/opt/pc4hcs_nbi_client.**

This section explains the various arguments and scenarios involved in subscribing and unsubscribing to traps. This section contains the following topics:

Subscribing

To subscribe, the following arguments are required:

- subscribe—Specifies that this is a subscribe command
- prime-ip—IP or hostname of the Prime Central VM
- prime-admin-password—Prime password used at the time of installation of Prime VM
- snmp-gateway-ip—IP or hostname to which traps should be sent
- snmp-gateway-port—Port to which traps should be sent
- where-clause—where clause to set the filter on; this is optional

Step 1 Log in as root user.

Step 2 Run the following command:

```
./pc4hcs_nbi_client.py [--subscribe | --unsubscribe]
                       --prime-ip
                       --prime-password
                       --where-clause
                       --snmp-gateway-port
                       --snmp-gateway-ip
```

The request returns the **customer-*token***.

Here's an example of subscribe request:

```
[root@hcslab-mike pc4hcs_nbi_client]# ./pc4hcs_nbi_client.py --subscribe --prime-ip
10.10.10.10 --prime-password Admin123@ --snmp-gateway-port 162 --snmp-gateway-ip
20.20.20.20 --where-clause "ServiceName = 'HCM SA Cluster'"
```

The following value is returned:

```
Customer_9
```

Note Retain the customer value to unsubscribe to gateway at a later time.

Using Where Clause for Subscribe Request

Using the where clause argument is optional; however, if you do not use the where clause, all the traps, without any filtering done, will be forwarded through the gateway. If you do specify the where clause, only traps that match the where clause criteria will be sent for the subscription. The argument snmp-gateway-ip specifies the destination IP to which traps will be sent.

Unsubscribing

To unsubscribe, the following arguments are required:

- unsubscribe—Specifies that this is an unsubscribe command
- prime-ip—IP or hostname of the Prime Central server
- prime-password—Prime Central admin password
- customer-token—The customer token that was returned when you subscribed to receiving traps. If you do not have the customer-token, follow the steps outlined in the "Recovering Subscription Tokens" section on page 3-15.

Step 1 Log in as root user.

Step 2 Run the following command:

```
./pc4hcs_nbi_client.py [--subscribe | --unsubscribe]
                       --prime-ip
                       --prime-password
                        --customer-token
```

The following message is returned:

```
Un-Subscribe request successful.
```

Here is an example of unsubscribe request:

```
[root@hcslab-mike pc4hcs_nbi_client]# ./pc4hcs_nbi_client.py --unsubscribe --prime-ip
172.16.10.126 --prime-password Admin123@ --customer-token Customer_9
```

The following message is returned:

```
Un-Subscribe request successful.
```

Recovering Subscription Tokens

When you subscribe to receiving traps and execute a subscribe request, a subscription token is returned. This token must be retained to unsubscribe at a later time. If you do not have the subscription token, follow these steps to recover the token:

1. To recover the token, you need to be logged into a VM that has Prime Central installed.
2. You must either log in as Oracle user or su to Oracle, and then log onto the primedb database.
3. Specify the `--prime-admin-password` you specified at the time of installation.

Step 1 Log on to the primedb database.

Step 2 Run the following command:

su - oracle -c '$ORACLE_HOME/bin/sqlplus primedba/\"*<prime-admin-password>***\"@primedb'**

The query command returns the ID, destination, status, and customer token. Match the customer token with the destination you wish to unsubscribe.

The following fields indicate the status of the gateway:

- 1—The gateway is up
- 0—The gateway is down

Here is an example of recovery command:

```
[root@hcslab-mike pc4hcs_nbi_client]# su - oracle -c '$ORACLE_HOME/bin/sqlplus
primedba/\"Admin123@\"@primedb'
```

The following values are returned:

```
SQL> select * from SNMPGATEWAYS;

ID DESTINATION                    STATUS CUSTOMERTOKEN
1 172.16.10.126:163               1 Customer_85
2 172.16.10.125:162               1 Customer_9
3                                 0
4                                 0
5                                 0
```

Recovering Active Subscription and Nonactive Gateway

Follow the steps explained below to recover active subscription and nonactive gateway:

Step 1 On PrimeCentral, log on to the Oracle database.

Step 2 Issue this command for updating the DB:

```
update SNMPGATEWAYS set DESTINATION=null,  STATUS=0,  CUSTOMERTOKEN=null where
ID=active-subscription-ID;
```

Step 3 On Event Collector, remove the following files:

If the destination ID is 1, use

```
rm -rf $OMNIHOME/etc/NCO_GATE.trapdest
rm -rf $OMNIHOME/var/NCO_GATE.pid
```

If the destination ID is a value other than 1, use

```
rm -rf $OMNIHOME/etc/NCO_GATE_trap-destination-ID.trapdest
rm -rf $OMNIHOME/var/NCO_GATE_trap-destination-ID.pid
```

Step 4 Issue the kill command if the gateway is still up:

```
ps -ef | grep snmp
kill -9 <pid of gateway to be brought down>
```

Tip Identify the pid from the gateway line, when you issued the command **ps -ef | grep snmp**:

For example, identify the pid from the following:

```
netcool 30445 30443 0 12:49 ? 00:00:00
/opt/IBM/tivoli/netcool/omnibus/bin/linux2x86/nco_g_snmp -name NCO_GATE -snmpgateway
sadev-rod:166
```

Do not kill this one; it does not stop the gateway:

```
netcool 30443 25808 0 12:49 ? 00:00:00 /bin/bash
/opt/IBM/tivoli/netcool/omnibus/bin/hcs_snmp_gateway_start 1
```

Recovering from Inconsistent Oracle DB State

Sometimes, when you issue a subscription or un-subscription request, your machine hangs and times out. In such a scenario, verify whether it is in an inconsistent state:

Step 1 Open the log **/opt/<install_dir>/apache-servicemix-4.4.1-fuse-00-08/data/log/servicemix.log**. Look for the following arguments:

OALL8 is in an inconsistent state; Nested exception is java.sql.SQLException: OALL8 is in an inconsistent state.

Step 2 Reboot the oracle database:

```
su - primeusr -c 'emdbctl stop; emdbctl start'
```

Recovering from Duplicate Customer Tokens

When you subscribe to receiving traps, and execute a subscribe request, a subscription token is returned. This token must be retained to unsubscribe at a later time. If you need to recover from duplicate customer tokens, follow this procedure:

1. To recover the token, you must be logged in to a VM that has Prime Central installed.
2. You must either log in as Oracle user or su to Oracle, and then log on to the primedb database.
3. Specify the `--prime-admin-password` you specified at the time of installation.

Step 1 Log on to the Oracle database.

Step 2 Run the following command to update the database:

```
update SNMPGATEWAYS set DESTINATION=null,  STATUS=0,  CUSTOMERTOKEN=null where ID=#;
```

In the argument **`where ID=#`**, # is the active subscription ID that you want to remove from the DB.

Step 3 On Event Collector, remove the following files:

If the ID you want to remove is 1, use

```
rm -rf $OMNIHOME/etc/NCO_GATE.trapdest
```

If the ID you want to remove is a value other than 1, use

```
rm -rf $OMNIHOME/etc/NCO_GATE_#.trapdest
```

Step 4 Issue the kill command if the gateway is still up:

```
ps -ef | grep snmp
      kill -9 <pid of gateway to be brought down>
```

Tip Identify the pid from the gateway line, when you issued the command **`ps -ef | grep snmp`**:

For example, identify the pid from the following:

```
netcool 30445 30443 0 12:49 ? 00:00:00
/opt/IBM/tivoli/netcool/omnibus/bin/linux2x86/nco_g_snmp -name NCO_GATE -snmpgateway
sadev-rod:166
```

Do not kill this one; it does not stop the gateway:

```
netcool 30443 25808 0 12:49 ? 00:00:00 /bin/bash
/opt/IBM/tivoli/netcool/omnibus/bin/hcs_snmp_gateway_start 1
```

MIB Definition for NBI SNMP Notification

After you run the patch script, the MIB file is installed on Prime Central VM. The MIB defines an SNMP v2 notification that is aligned with the SNMP v2 notifications generated by Prime Central for HCS.

The MIB file is located at the following location in the Prime Central VM: <prime-install-directory>/prime-hcs/sdk/CISCO-HCS-SA-NBI-MIB.my.

Northbound clients that intend to process the SNMP notifications from Prime Central for HCS can use the MIB definition to implement this feature.

For more information, see the documentation that ships with the product used to process the received SNMP notifications.