<p style="text-align:right">C H A P T E R **5**</p>

# Backing Up and Reinitializing Hosted Unified Communications Services Components

This chapter explains how to backup and reinitialize the Hosted Unified Communications Services (Hosted UCS) platform components. It also provides some recommendations for upgrading to a newer version. This chapter includes the following sections:

# Backing Up Cisco Unified Communications Manager and Cisco PGW

This section outlines the process for storing a known, reliable configuration before a platform upgrade and includes the following topics:

- Backing-up Cisco Unified Communications Manager, page 5-2
- Restoring Cisco Unified Communications Manager and Cisco PGW Configuration, page 5-3
- Restoring the Cisco PGW Configuration, page 5-4
- Restoring the Cisco PGW to Clean Status, page 5-5

After backup, the stored configuration can be restored onto a Hosted UCS platform component, if required. For example, restoring the initial static configuration for the Cisco Unified CM or Cisco PGW eliminates the time-consuming reconfiguration process.

## Backing-up Cisco Unified Communications Manager

To use Disaster Recovery System (DRS) for backing up and restoring configuration, complete the following steps.

**Procedure**

**Step 1**    Go to **Disaster Recovery System**, using the Cisco Unified CM OS admin credentials. **(CCM7.x)**.

**Step 2**    Create a backup device on the Cisco Unified CM, to add a network based backup device with access credentials.

**Step 3**    Choose **Manual Backup > Select the Device Name.**

**Step 4**    Check the **CCM** check box.

**Step 5**    Click **Start Backup**.

After approximately five to ten minutes, you should see the TAR file in Backup Device folder.

## Backing Up the Cisco PGW

✎ **Note**    If your Cisco PGW 2200 Softswitch is a continuous service system, (active-standby) ensure that you perform backup procedures on both Cisco PGW 2200 Softswitches.

✎ **Note**    You can run the various backup operations that are described in the following sections only when you are logged in to your system as mgcusr. You cannot perform any backup operation while you are logged in as root.

To perform a manual backup operation, enter the following UNIX command on the Cisco MGC:

```
mgcbackup -d path [-r retries -t retry_time]
```

Where:

- *path*—The full path of the directory in which to store the backup file; for example, a directory on a remote server that you have mounted on your system, or the local tape drive.

> **Note** Cisco recommends that you do not store backup files on your local Cisco MGC host, because storage of backup files on the local host reduces the amount of disk space available to process call data and does not ensure that the data is safe in the event of a natural disaster.

- *retries*—The number of times to check for an active provisioning session on the Cisco MGC before aborting the backup operation. The default value is 0 and the maximum value is 100.

> **Note** A backup operation cannot start while there is an active provisioning session on the Cisco MGC.

- *retry_time*—The number of seconds to wait between checks for an active provisioning session on the Cisco MGC. The default value is 30 seconds and the maximum value is 3600 seconds.

For example, to perform a manual backup operation where the backup file is saved to a directory path called /dev/rmt/h0, with a maximum of three attempts, each 60 seconds apart, you would enter the following UNIX command:

```
mgcbackup -d /dev/rmt/h0 -r 3 -t 60
```

The backup file is stored in the specified directory path in the following format:

```
mgc_hostname_yyyymmdd_hhmmss_backup
```

Where:

- *hostname*—The name of the Cisco MGC host, such as MGC-01.
- *yyyymmdd*—The date the backup file is created, in a year-month-day format, such as 20011130.
- *hhmmss*—The time the backup file is created, in an hour-minute-second format, such as 115923.

For more information on backup operations, see the "Backing Up System Software" in Chapter 3 of the *Cisco PGW 2200 Softswitch Release 9.8 Operations, Maintenance, and Troubleshooting Guide* at the following URL:

http://www.ciscosystems.cg/en/US/docs/voice_ip_comm/pgw/9.8/Maintenance/Guide/r9chap3.html#wp1229244

# Restoring Cisco Unified Communications Manager and Cisco PGW Configuration

This section explains how to restore the configuration for Cisco Unified CM and the Cisco PGW. It includes the following topics:

- Restoring Cisco Unified Communications Manager Configuration, page 5-4
- Restoring the Cisco PGW Configuration, page 5-4
- Listing the Cisco PGW Backup Files, page 5-4
- Restoring the Cisco PGW Backup File, page 5-4

# Restoring Cisco Unified Communications Manager Configuration

To restore Cisco Unified CM, follow the Disaster Recovery System (DRS) restore process and then restart the Publisher and the Subscribers.

# Restoring the Cisco PGW Configuration

This restoration method uses a script to restore the configuration data for the Cisco MGC software, UNIX administrative files, and the Main Memory Database (MMDB).

**Note**     These procedures assume that you have backed up your system configuration data regularly. The procedures for system configuration backup can be found in Backing Up the Cisco PGW, page 5-2.

# Listing the Cisco PGW Backup Files

To list the backup files in a particular directory path, enter the following UNIX command on the Cisco MGC:

**mgcrestore -d** *path* **-l**

Where *path* is the directory path in which you have stored backup files, such as a directory on a remote server or a local tape drive.

The system returns a response similar to the following:

```
Backup files in /var/cisco
------------------------------------------------
mgc_venus_20011010_153003_backup
mgc_venus_20011011_153003_backup
mgc_venus_20011012_153003_backup
```

# Restoring the Cisco PGW Backup File

CiscoMGC service on the PGW must be stopped before restoring a backup file.

Log on PGW as root user and run the following command to stop mgc service.

```
PGW-ENT2M% /etc/init.d/CiscoMGC stop
```

To restore the configuration data stored in a particular backup file, enter the following UNIX command on the affected Cisco MGC to run the restore script:

**mgcrestore -d** *path* **-f** *filename*
Where:

- *path*—The directory path to the location where your backup files are stored.
- *filename*—The file name of the backup file you want to restore.

For example, to restore a backup file called mgc_venus_20011012_153003_backup stored in a directory path called /var/cisco, you would enter the following command:

```
mgcrestore -d /var/cisco -f mgc_venus_20011012_153003_backup
```
After restoring the backup file, start the mgc service on PGW as root user.

```
PGW-ENT2M% /etc/init.d/CiscoMGC start
```
For more information on backup operations, see "Restoring Procedures for Cisco MGC Software Release 9.1(5) and up" in Chapter 5 of the Cisco PGW 2200 Softswitch Release 9.8 Operations, Maintenance, and Troubleshooting Guide at the following URL:
http://www.ciscosystems.cg/en/US/docs/voice_ip_comm/pgw/9.8/Maintenance/Guide/r9chap6.html#wp1722661

# Restoring the Cisco PGW to Clean Status

To clear the Cisco PGW and restore it to its original static configuration, complete the following steps.

**Procedure**

**Step 1**    Logon to the Cisco PGW using Reflexion Host – Unix.

On test systems: username=*mgcusr*. password=*cisco*.

**Step 2**    Enter the text shown in boldface:

```
GL-D-PGW% mml
GL-D-PGW mml> prov-sta::srcver="pure-static",dstver="iBVSconfig",confirm
  MGC-01 - Media Gateway Controller 2005-06-30 14:09:55.352 BST
M  COMPLD
 "PROV-STA"
;
```

**Note**    pure-static in the MML command above is an example name of the static configuration MML session on the PGW. If you have static MML configuration session saved on your PGW, use that session name to restore PGW static configurations

```
GL-D-PGW mml> prov-cpy
  MGC-01 - Media Gateway Controller 2005-06-30 14:10:02.164 BST
M  COMPLD
"PROV-CPY"
;
GL-D-PGW mml> quit
```
In this example, the entry iBVSconfig is a temporary name. The exact name is not important.

# Backing up and Restoring USM

The USM automatically backups the database within the cluster and between active and standby USM servers. USM always maintains four copies of the database, two in each headend. If a copy of the database needs to be saved offsite, you can set up an export copy of the database.

In most cases to date, offsite backup has occurred once every 24 hours. This should occur at a time of low provisioning traffic, such as in the early hours of the morning.

For the backup to be useful as part of a disaster recovery plan, the USM backup needs to be in a consistent state with those taken for the Cisco PGW and Cisco Unified CM, along with IP Unity if they are included in the Hosted UCS platform. To ensure a consistent state, there should be a USM transaction freeze while the platform is being backed up.

If all the backups are taken at the same time, it becomes possible to time-shift the entire platform back to the latest backup without any misalignment between USM and the servers that it controls.

**Note**    To use the CLI, a client capable of SSH is required. The most common SSH clients include Putty (Windows platform) or the SSH client in a terminal (UNIX / Linux or Mac OS X platform).

**Note**    The default login username is usmcli and the default password is voss. If you are unable to login using the default login details, please contact your dedicated support person so that they can reset the default password and verify that this functionality has been enabled for your system.

It is important to ensure that the commands below are carried out on the active VoSS server. These commands do not, and should not, be run on the inactive VoSS director.

To use the CLI, do the following:

**Step 1**    SSH to the cluster/standalone system and login as the user usmcli. You will be presented with a prompt as follows:

```
Password:
Welcome to the VOSS-USM Standalone Console
=>
```

**Step 2**    To enter enable mode (similar to other networking hardware) type enable as follows:

```
=>> enable
=>#
```

The prompt should changes from "=>>" to "=>#" to reflect this change.

**Step 3**    Type "dbbackup" command on the CLI as follows:

```
=># dbbackup
```

**Note**    Only the database is backed up.  Any other configuration information currently such as DNS Configuration, syslogs, Any Manual Changes (i.e. changes to file content), bulk loader sheets etc., must be backed up manually by copying those files.

**Note**    If you are rebuilding a system however, these files would be recreated during the installation of the platform and software.

The USM database backup is performed as shown in Figure 5-1.

*Figure 5-1          Backup USM database using CLI*



## Restoring USM

Before restoring USM batabase backup, you must stop the relevant services on the USM system.

**Procedure:**

**Step 1**   Log on USM as root user.

**Step 2**   Stop all services and restart Postgress: (Standalone, on cluster environment you just need to restart postgress). In a Standalong USM system, run the following command to stop all the services:

```
for svc in usm-autoregister loader_scheduler extdhcp apache2 usm_batch selfcare memcached
estraier iptparent iptqueue iptdevmn voss-monit voss-imq postgresql-standalone postgresql;
do /etc/init.d/${svc} stop; done
```

If USM is deployed as a clutster, use the following command to stop the services:

```
/etc/init.d/heartbeat-wrapper stop
Restart postgresql services:
/etc/init.d/postgresql-stanalone restart
/etc/init.d/postgresql restart
```

**Step 3**   Perform the restore, see example below:

```
/opt/VOSS/usm/scripts/deployment/db-backup-restore.py --restore
/root/db-backup-ipt-2010-02-11.sql
```

**Step 4**   After restoring backup file start all USM services. In a Standalone USM system, run the following command to start all the services:

```
for svc in voss-monit iptdevmn iptqueue iptparent estraier memcached usm_batch selfcare
apache2 extdhcp loader_scheduler usm-autoregister; do /etc/init.d/${svc} start; done
```

If USM is deployed as a clutster, use the following command to start the services:

```
/etc/init.d/heartbeat-wrapper start
```

# Clearing a Cisco Unified Communications Manager Cluster

This section describes the process for clearing a Cisco Unified CM cluster, in preparation to re-build the Hosted UCS platform.

The order of the clearing steps is not important and further clearing steps may be required on some Hosted UCS platforms. For example, you may need to delete organizations within the Movius server, using the Movius server Sysconfig GUI.

When you start the rebuild process, you must complete all stages. It is not possible to go back after you have cleared one component in the architecture.

You must clear the Cisco Unified CM before a rebuild to ensure that there will be no data duplication or mismatch between USM and the Cisco Unified CM.

You can quickly restore the Cisco Unified CM publisher to its initial state by restoring a CUCM backup file.

When no DRS backup file is available, to clear the Cisco Unified CM and avoid any interdependency issues, complete the following steps.

**Procedure**

**Step 1**  Delete phone devices.
Choose 50 phones for the search list to allow deletion of 50 phones at a time.

**Step 2**  From the **Call Routing > Translation Patterns** menu, delete Translation Patterns, 50 at a time.

**Step 3**  From the **Device > CTI Route Points** menu, delete any CTI route points used.

**Step 4**  From the **Call Routing > Route/Hunt > Route Pattern** menu, delete all route patterns.

**Step 5**  From the **Call Routing > Route/Hunt > Route List** menu, delete all route lists.

**Step 6**  From the **RoutePlan > Route/Hunt > Route Group** menu, delete all route groups.

**Step 7**  From the **Device > Trunks** menu, delete all trunks.

**Step 8**  From the **Device > Gatekeepers** menu, delete all gatekeepers.

**Step 9**  From the **Device > Gateways** menu, delete all gateways.

**Step 10**  From the **Media Resources > MediaResourceGroupList** menu, delete all media resource group lists.

**Step 11**  From the **Media Resources > MediaResourceGroup** menu, delete all media resource groups.

**Step 12**  From the **System > Locations** menu, delete all locations (show 50 at a time).

> **Note**  The Cisco Unified CM does not allow to delete the default locations, device pools and regions. Do not attempt to delete default configurations.

**Step 13**  From the **Media Resource > Conference Bridge** menu, delete any conference bridges that are not required.

Keep the conference bridges that are required by USM.

**Step 14**    From the **Application > CiscoCM Attendant Console > Pilot Points** menu, delete pilot points used if any.

**Step 15**    From the **System > Device Pool** menu, delete all device pools, except Default.

**Step 16**    From the **System > Region** menu, delete all regions except Default.

**Step 17**    From the **Call Routing > Route/Hunt > Hunt Pilot** menu, delete all hunt pilots used.

**Step 18**    From the **Call Routing > Route/Hunt > Hunt List** menu, delete any hunt lists used.

**Step 19**    From the **Call Routing > Route/Hunt > Line Group** menu, delete any line groups used.

**Step 20**    Delete all users, either one-by-one via the CCMAdmin group or in bulk using the BAT Tool facilities.

**Step 21**    From the **Call Routing > Directory Numbers** menu, delete any directory numbers used.

**Step 22**    From the **Call Routing > Call Pickup** Group, delete any call pickup numbers used.

**Step 23**    From the **Call Routing > Call Park** menu, delete an call park numbers used.

**Step 24**    From the **System > Cisco Unified CM Groups** menu, delete all Cisco Unified CM groups except Default.

**Step 25**    From the **Device > Device Settings > Device Profile** menu, delete all profiles, including "Logout" service.

**Step 26**    From the **Call Routing > Route Plan Report** menu, search for unassigned DNs and select **Delete All Found Items** at the bottom of the search page.

This allows deletion of 150 unassigned DNs at a time.

**Step 27**    For voice-mail profiles, voice-mail pilot numbers, and MWI numbers, unless these need to be maintained.

**Step 28**    From the **Call Routing > Class of Control > Calling Search Space** menu, delete all CSSs except **IncomingToCluster**.

**Step 29**    From the **Call Routing > Class of Control > Partitions** menu, delete all partitions.

**Step 30**    From the **Call Routing > Route Plan Report** menu, search for assigned DNs and delete DNs one at a time.

✎

**Note**    If issues occur, use the dependency record feature to search for components that might be preventing deletion of records.

# Initializing the Cisco PGW

This section describes the clearing process for the Cisco PGW by deleting the USM-created file before rebuilding a Hosted UCS platform.

You must clear the Cisco PGW before reloading a Hosted UCS platform. Clearing the Cisco PGW means clearing out USM data but not other configuration information that may have been set up on the Cisco PGW servers independently of USM.

To initialize the Cisco PGW, complete the following steps.

**Procedure**

**Step 1**   Logon to the active Cisco PGW.

Log in over Telnet or SSH, using a terminal console program, such as PuTTY.

On test systems, the user account/password is mgcusr/cisco.

To configure the up arrow operate to add back previous lines, use the following:

```
PGW % setenv TERM vt100
```

**Step 2**   To verify that you are logged into the active Cisco PGW, enter the following commands:

```
PGW % mml
mml > rtrv-ne
```

**Step 3**   To create a binary backup to allow rollback if required, choose your own filename.

For example, *270710-01bin*.

```
mml> prov-sta::srcver="active",dstver="270710-01bin"
mml> prov-stp
```

**Step 4**   To create a text backup for diagnostics if required, choose your own filename.

For example,*270710-01text*.

```
mml>prov-exp:all:dirname="270710-01text"
```

**Step 5**   Restore the process, if rollback is required:

```
mml> prov-sta::srcver="270710-01bin ",dstver="270710-03bin "
mml> prov-dply (Dual server PGW platform)
or
mml> prov-cpy (Single server PGW platform)
```

**Step 6**   For the Cisco PGW reset process (dial plans only), enter the following commands:

```
mml> quit
% cd /opt/CiscoMGC/etc/cust_specific
% ls –la
```

This gets a list of files stored including Text file.

```
% cd /opt/CiscoMGC/etc/cust_specific/270710-01text
% ls
```

**Step 7**   Make a note for all four-character mml files loaded by USM.

For example, copy ICCM.mml, P974.mml, XXXX.mml, XXXX.mml into Notepad.

```
% mml
mml> prov-sta::srcver="active",dstver="270710-02bin"
mml> numan-dlt:dialplan:custgrpid="XXXX"
```

where *XXXX* is the name of each four-character mml file.

**Step 8**   Repeat this process until all XXXX.mml files have been deleted. If you hit a dependency, go to the next file and cycle through until all files are deleted.

**Note**   All the dial plans are not deletable manually due to interdependencies between dial plan. Cisco recommends to back up PGW static configuration and restore the PGW static configuration when PGW needs to be cleaned up.

**Step 9**   Reload the ICCM dial plan as an empty file:

```
mml> numan-add:dialplan:custgrpid="ICCM",overdec="YES"
mml> prov-dply (Dual server PGW platform)
or
mml> prov-cpy (Single server PGW platform)
```

**Step 10**   On completion, take a further backup of the Cisco PGW.

This will be the static configuration of the Cisco PGW if, for example, the Cisco PGW needs to cleared by deleting static settings.

**Step 11**    To create a binary back-up to allow rollback if required, choose your own filename.

For example, *VSR2-151007Static-HB-01bin*.

```
mml> prov-sta::srcver="active",dstver="2710001-01bin"
mml> prov-stp
```

# Initializing USM

This section explains how to clear an existing USM platform that has already been loaded with dial plans and data.

Clear the USM database when you are planning to rebuild the Hosted UCS platform. The clearing process is much faster than deleting all the data manually through the USM GUI and even faster than the Delete Bulk Loader tool or Operations tools. This is especially the case if USM has many customers and locations already loaded.

To clear a USM cluster, complete the following steps.

⚠
**Caution**    There is no way to undo a destroy procedure, so check whether you are on the correct server.

✎
**Note**    The consequences of running this command are great. Please ensure that you fully understand the impact of running this command prior to using it

**Procedure**

**Step 1**    SSH to the cluster/standalone system and login as the user usmcli.
You will be presented with a prompt as follows:

```
Password:
Welcome to the VOSS-USM Standalone Console
=>>
```

**Step 2**    To enter enable mode (similar to other networking hardware) type enable as follows:

```
=>> enable
=>#
```
The prompt should changes from "=>>" to "=>#" to reflect this change.

**Step 3**    Type "reset app" command on the CLI as follows:

```
=># reset app
    Really reset the application? ? [y/N] : y
    clearing status...
    Application reset complete.
=>#
```

**Step 4**    Reboot the USM system.

```
=># reboot
```

**Note**  You only need to destroy Standalone VOSS system or VOSSDir1 because USM automatically replicates to the other servers.