CHAPTER 6

Performing Backup and Restore

Prime Collaboration allows you to make a backup of your data and restore it. However, you must manually run backup and restore commands by logging in to the system as an admin user (CLI user).

Note

- CLI is supported only through SSH; telnet is not supported. The port used for Prime Collaboration Assurance is 26, for Prime Collaboration Provisioning it is 22.
- The **application start cpcm** command takes 10 to15 minutes to complete execution and **application stop cpcm** takes 10 minutes to complete execution.

Overview of Backup and Restore

Although the Prime Collaboration Assurance and Prime Collaboration Provisioning applications(UI) are converged, you must perform backups on the respective Assurance and Provisioning servers.

Only Prime Collaboration Assurance backup and restore are covered here. For information on Prime Collaboration Provisioning backup and restore, see "Provisioning Database Backup and Restore" in *Cisco Prime Collaboration 9.0 Provisioning Guide*.

Prime Collaboration Assurance uses the following purge policy:

- All session and endpoint statistics data older than one day are purged. For more details, see “Monitoring Sessions” in *Cisco Prime Collaboration 9.0 Network Monitoring, Reporting, and Diagnostics Guide*.
- All session and troubleshooting details older than 14 days are purged every hour. For more details, see “Video Endpoints” in *Cisco Prime Collaboration 9.0 Network Monitoring, Reporting, and Diagnostics Guide*.
- Call quality event history and audio/video phone audit report data older than 30 days are purged. For more details, see “Voice Reports” in *Cisco Prime Collaboration 9.0 Network Monitoring, Reporting, and Diagnostics Guide*.
- Cleared alarms and events that are older than 14 days are purged every hour. If an alarm is purged, all associated events are also purged. Active events and alarms are not purged. For more details, see *Cisco Prime Collaboration 9.0 Fault Management Guide*.
- Jobs that are older than 14 days and have a status of completed, failed, or cancelled are purged every hour.

The backup and restore service allows you back up the database, configuration files, and log files to either a remote location or a local disk. Files in following folders are backed up by the backup service:

Folder Name	Type of Data
emms database	Database
cpcm/conf	Configuration files
cpcm/export	Troubleshooting and endpoint utilization reports
cpcm/logs and tomcat/logs	Assurance application and Tomcat log files
jre/lib/security	Keystore files

Backup and Restore can be performed in the following ways:

- Make backup of data in a system and restore it on the same system: For more information, see Restoring on the Same System, page 6-2.
- Make backup of data in a system and restore it on a different system: For more information, see Restoring on a Different System, page 6-4.

Restoring on the Same System

The following sections describe the process of backing up data and restoring it on the same system.

Creating a Repository on an FTP, SFTP, or TFTP Server

You must create a repository before backing up the data. By default, the backup service creates a *.tar.gpg file under the configured repository. The backed-up file is in a compressed format. The repository can be on CD-ROM, disk, HTTP, FTP, SFTP, or TFTP.

To create a repository:

Step 1 Log in to the Prime Collaboration Assurance server with the account that you created during installation. The default login is *admin*.

Step 2 Enter the following commands to create a repository on a disk:

```
admin# config t
admin(config)# repository RepositoryName
admin(config-Repository)# url ftp://ftpserver/directory
admin(config-Repository)# user UserName password {plain | hash} Password
admin(config-Repository)# exit
admin(config)# exit
```

Where:

- *RepositoryName* is the location to which files should be backed up. This name can contain a maximum of 30 alphanumeric characters.
- *ftp://ftpserver/directory* is the FTP server and the directory on the server to which the file is transferred. You can also use SFTP, HTTP, disk, or TFTP instead of FTP.

- *UserName* and {**plain** | **hash**} *Password* are the username and password for the FTP, SFTP, or TFTP server. **hash** specifies an encrypted password, and **plain** specifies an unencrypted plain text password.

For example:

```
admin# config t
admin(config)# repository tmp
admin(config-Repository)# url ftp://ftp.cisco.com/incoming
admin(config-Repository)# user john password plain john!23
admin(config-Repository)# exit
admin(config)# exit
```

Backing Up Data

After creating the repository, Log in to the Prime Collaboration Assurance server as admin and run the following command to back up the data:

```
admin# backup Backupfilename repository RepositoryName application cpcm
```

Where,

- *Backupfilename*—Name of the backup file (without the extension-.tar.gpg). This name can be a maximum of 100 alphanumeric characters.
- *RepositoryName*—Location to which the files are be backed up. This name can contain a maximum of 30 alphanumeric characters.

The following message appears after the backup is complete:

```
% Creating backup with timestamped filename: Backupfilename-Timestamp.tar.gpg
```

The backup file is suffixed with the time stamp (YYMMDD-HHMM) and file extension .tar.gpg and saved in the repository. For example:

```
admin# backup cmbackup repository tmp application cpcm
```

The following message appears after the backup is complete:

```
% Creating backup with timestamped filename: cmbackup-110218-0954.tar.gpg
```

Restoring Data

To restore the data, Log in to the Prime Collaboration Assurance server as admin and run the following command:

```
admin# restore Backupfilename repository RepositoryName application cpcm
```

Where*, Backupfilename* is the name of the backup file suffixed with the timestamp (*YYMMDD-HHMM*) and file extension .tar.gpg.

For example:

```
admin# restore cmbackup-110218-0954.tar.gpg repository tmp application cpcm
```

Restoring on a Different System

Prime Collaboration allows you to back up the data of a system and restore the data in another system in the event of total system failure.

Before you back up files, change the “qovr” database instance password in the system where you perform backup and use the same password in the new system (where you restore the files).

However, the process to create a backup is the same as in the case of Backing Up Data, page 6-3 (See also, Creating a Repository on an FTP, SFTP, or TFTP Server, page 6-2).

To change the “qovr” database instance password of a system in execution, before backup:

Step 1 Log in to the system as a root user.

Step 2 Stop the Prime Collaboration Assurance server:

```
/opt/emms/emsam/bin/cpcmcontrol.sh stop
```

(the process takes 10 minutes to complete)

Step 3 Run the following command:

```
perl opt/CSCOpx/bin/dbpasswd.pl dsn=qovr npwd=”new password”
```

Use this new qovr database password in the new system where you restore the files.

Step 4 Start the Prime Collaboration Assurance server:

```
/opt/emms/emsam/bin/cpcmcontrol.sh start
```

(the process takes 15 minutes to complete)

Step 5 Log in as administrator and perform backup as described in Backing Up Data, page 6-3 (See also, Creating a Repository on an FTP, SFTP, or TFTP Server, page 6-2).

To restore the backup from another system, the following prerequisites must be met:

- Ensure that that the system to which data is restored must have the same IP address, hostname and same MAC adddress as that of the system that was backed up.

  In the case you are unable to assign the MAC address of that system (the original system that was backedup) to another system, contact Cisco TAC for information on a new license file (for a new MAC address).
- Change the “qovr” database instance password in the system where you perform backup and use the same password in the new system (where you restore the files)
- For ESX 4.1, you must assign the static MAC address of the backed up system to a new system that is used for restoring data. However, for ESX 5.0, there is no such condition and you can assign any dynamic MAC address as a static MAC address to the new system that is used for restoring data.

To change the “qovr” database instance password system in execution, before restore:

Step 1 Log in to the system as a root user.

Step 2 Stop the Prime Collaboration Assurance server:

```
/opt/emms/emsam/bin/cpcmcontrol.sh stop
```

(the process takes 10 minutes to complete)

Step 3 Run the following command:

```
perl opt/CSCOpx/bin/dbpasswd.pl dsn=qovr npwd="new password"
```

For the new password, use the same qovr database password value that you had entered in the original machine where the data was backedup.

Step 4 Start the Prime Collaboration Assurance server:

```
/opt/emms/emsam/bin/cpcmcontrol.sh start
```

(the process takes 15 minutes to complete)

Step 5 Log in as administrator and perform restore as described in Restoring Data, page 6-3.

Listing the Repository Data

You can list the data within a repository, Log in to the Prime Collaboration Assurance server as admin and run the following command:

admin# **show repository** *RepositoryName*

For example:

```
admin# show repository tmp
cmbackup-110218-0954.tar.gpg
admin#
```

Checking the Backup History

You can check the backup history, Log in to the Prime Collaboration Assurance server as admin and run the following command:

```
admin# show backup history
```

For example:

```
admin# show backup history
Fri Feb 18 09:54:39 UTC 2011: backup cmbackup-110218-0954.tar.gpg to repository
temp: success
Fri Feb 18 18:29:48 UTC 2011: backup cmbackup-110218-1829.tar.gpg to repository
tmp: success
admin#
```