Performing Backup and Restore

Performing Backup and Restore

Prime Collaboration Assurance allows you to backup and restore your data. You can schedule periodic backups using the Prime Collaboration Assurance user interface, or run backup commands manually by logging in to the system as an admin user (CLI user). However, you must manually run restore commands by logging in to the system as an admin user.

Note

- CLI is supported only through SSH; telnet is not supported. The port used for Prime Collaboration Assurance is 26.
- The **application stop cpcm** command takes 10 minutes to complete execution and **application start cpcm** takes 10 to 15 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.

If you have installed Prime Collaboration Analytics, you must first perform the backup of the analytics data before backing up the assurance data. The same sequence has to followed while restoring the data. For information about Prime Collaboration Analytics backup and restore, see *Backup and Restore for Prime Collaboration Analytics* chapter in Cisco Prime Collaboration Assurance Guide.

For information about Prime Collaboration Provisioning backup and restore, see "*Provisioning Database Backup and Restore*" chapter in Cisco Prime Collaboration Provisioning Guide.

Note Not all information covered in this section is applicable to Prime Collaboration Assurance Standard mode. See Standard and Advanced Prime Collaboration Assurance for information about feature support in Standard and Advanced modes.

Prime Collaboration Assurance uses the following purge policy:

- All session and endpoint statistics data older than one day are purged. For more details, see the section Monitoring Sessions in the Cisco Prime Collaboration Assurance Guide - Advanced.
- All session and troubleshooting details older than 14 days are purged every hour. For more details see the section Diagnostics for Video Endpoints in the Cisco Prime Collaboration Assurance Guide - Advanced.
- Call quality event history and audio/video phone audit report data older than 30 days are purged. For more details, see the section Voice Reports in the Cisco Prime Collaboration Assurance Guide - Advanced.
- 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 the Concepts chapter in Cisco Prime Collaboration Assurance Guide - Advanced.
- 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

Note The data backup may take a long time (up to12 hours), depending on the number of managed devices in the Prime Collaboration Assurance server. It is recommended that you schedule backups during the non-business hours, because, this operation will severely slow down the Prime Collaboration Assurance UI performance.

Creating a Repository on FTP, Disk, 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.

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 the local:

```
admin# config t
admin(config)# repository RepositoryName
admin(config-Repository)# url disk:
admin(config-Repository)# exit
admin(config)# exit
```

Enter the following commands to create a repository on FTP server:

```
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, 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
  ```

Scheduling Backup using Prime Collaboration User Interface

You can schedule and run backup for both Assurance and Provisioning from the user interface. You can use SFTP, FTP, or local connection to create backup.

You must be logged in as an administrator to perform backup.

To create a new backup job:

Step 1 Choose **Administration** > **Backups**.

Step 2 In the Backup page, click **New**.

Step 3 Enter a name for the backup job.
If backup name is not specified, the Backup Title field is defaulted with date stamp.

Step 4 Select the Backup Category.

Step 5 Enter the Connection settings.
You can use SFTP, FTP, or local connection to create backup.

If you select SFTP or FTP, provide the following details:

- IP address of the server where the backup files need to be saved
- Path to the backup location
  Note While backing up using SFTP, ensure you provide relative path.
- Port (for SFTP only)
- Username
- Password

Click **Test** to test the SFTP or FTP connection using the credentials.

If you select local, specify the location to save the backup files on your local machine.

For a local backup, you can specify the number of backup files to be saved, using the Backup History drop-down list. By default, the last two backup files are saved. You can save upto nine backup files.

Step 6 Specify the backup start time and recurrence interval.
The time displayed in the date picker is the client browser time.

Step 7 (Optional) Enter the e-mail IDs to which the backup status notification needs to be sent. You must separate the e-mail IDs using comma.

Step 8 Click **Save**.
The scheduled backup job is listed in the Backup Management page.

You can click **Run Now** to run the backup immediately.

Backup using CLI

Backup and Restore using CLI 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.
- Make backup of data in a system and restore it on a different system: For more information, see Restoring on a New System.

Restoring on the Same System

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

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, in case of backup on the ftp server:

```
admin# backup assurance repository myftp application cpcm
```

where, myftp is a repository name.

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, to restore on the ftp server:

```
admin# restore assurance_Sun_Feb_09_14_20_30_CST_2014.tar.gpg repository myftp application
 cpcm
```

Restoring on a New 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.

To restore the backup from another system:

Ensure that the system to which data is restored must have the same MAC address as that of the system that was backed up (IP address and the hostname can be different).

In the case you are unable to assign the MAC address of the original system (that was backed up) to another system, contact Cisco TAC for information on a new license file (for a new MAC address).

To restore the backup from another system, log in as administrator and perform restore as described in Restoring Data. See also, Creating a Repository on FTP, Disk, SFTP, or TFTP Server.

Note As a post requirement, you must rediscover all the devices after restoring the data.

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 myftp
assurance_Sun_Feb_09_14_20_30_CST_2014.tar.gpg
```

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