Perform Backup and Restore

This section explains the following:

Perform Backup and Restore

You can schedule periodic backups using the Cisco Prime Collaboration Assurance user interface.

Cisco Prime Collaboration Analytics data is backed up on a remote server using SSH. It does not use the Cisco Prime Collaboration Assurance backup repository. You can backup and restore the analytics data through User Interface.

Related Topics

Monitor Conferences
Troubleshooting Workflow for Video Endpoints
Purge Policies
Concepts

Overview of Backup and Restore

Cisco Prime Collaboration Assurance uses the following purge policy:

- All conference and endpoint statistics data older than one day are purged.
- **For Cisco Prime Collaboration Release 11.5 and later**

  All conference and troubleshooting details older than 14 days are purged every hour.
- **For Cisco Prime Collaboration Release 11.6 and earlier**

  Call quality event history and audio/video phone audit report data older than 30 days are purged.

  For Cisco Prime Collaboration Release 12.1 and later

  Call quality event history and endpoint related audit report data older than 30 days are purged.
- 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.

- 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:

Type of Data for Assurance Backup
Assurance database
Configuration files

Type of Data for Analytics Backup
Analytics database
Log files
Reports (Scheduled Reports and Custom Reports)
Logos

Backup Time Period

Depending on the number of managed devices in the Cisco Prime Collaboration Assurance server, the data backup should take:

- Upto 150,000 endpoints - 4 hours
- Upto 80,000 endpoints - 3 - 2.5 hours
- Upto 20,000 endpoints - 2 hours
- Upto 3,000 endpoints - 1 hour

Note To achieve the preceding time periods, the network latency should not be more than 20 ms.

We recommend you to schedule backups during the non-business hours, because, this operation can slow down the Cisco Prime Collaboration Assurance user interface performance.

Create a Repository on FTP, Disk, SFTP, or TFTP Server

You must create a repository before backing up the Cisco Prime Collaboration 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.

For Cisco Prime Collaboration Release 11.6 and earlier

Procedure

Step 1 Log in to the Cisco Prime Collaboration 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
  ```

List the Repository Data

You can list the data within a repository. Log in to the Cisco Prime Collaboration 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
```

Schedule Backup using Cisco Prime Collaboration Assurance and Analytics User Interface

You can backup and restore the assurance, and analytics data through user interface.

To create a new backup job:

Procedure

Step 1 Choose **System Administration** > **Backup settings**.

Step 2 On 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** from the drop-down list.

Step 5 In the **Assurance Connection Settings** pane, enter the following details.

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 The backup is taken in the specified user home directory. For example,

Field	Description
SSH Username	Enter a name for the SSH Username. For example, user1 or provide any desired name.
Path	Enter a name for the path. For example, /backup Then, the Assurance backup location will be /user1/backup/assurance_backup.
The backup is saved in /user1/backup/assurance_backup.	

- 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 up to nine backup files.

The Analytics Connection Settings pane is available only if you have enabled Cisco Prime Collaboration Analytics.

For Cisco Prime Collaboration Release 11.5 and later

Cisco Prime Collaboration Analytics if enabled on MSP deployment can be backed up.

Step 6 In the **Analytics Connection Settings** pane, enter the following details.

You can use only a remote server to backup the Analytics data using SSH.

- IP address of the remote server where the backup files need to be saved
- Path to the backup location. You must provide relative path.

Note The backup is taken in the specified user home directory. For example,

Field	Description
SSH Username	Enter a name for the SSH Username. For example, user1 or provide any desired name.
Path	Enter a name for the path. For example, /backup Then, the Analytics backup location will be /backup/pg_basebackup (followed by timestamp (for example, pg_basebackup_201707201255)).
The backup is saved in /user1/backup.	

The Analytics backup folder will be in the following format: pg_basebackup (followed by the timestamp (for example, pg_basebackup_201707201255)). The backup fails if the user does not exist on the sFTP server.

- SSH Port
- SSH Username
- SSH Password

Click **Test** to test the connection using the credentials.

Step 7 Specify the backup start time and recurrence interval.

The time displayed in the date picker is the client browser time.

Step 8 (Optional) Enter the email IDs to which the backup status notification needs to be sent. Separate the email IDs using comma.

Configure the SMTP server details in the Cisco Prime Collaboration Assurance server (**E-mail Setup for Alarms & Events**) to receive emails.

For Cisco Prime Collaboration Release 11.5 and later

Configure the SMTP server details in the Cisco Prime Collaboration Assurance server (**Alarm & Report Administration** > **E-mail Setup for Alarms & Events**) to receive emails.

Step 9 Click **Save**.

The scheduled backup job is listed on the **Backup Management** page.

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

Troubleshooting

Issue: Cisco Prime Collaboration Assurance backup job status shows failure even after generating the reports. The backup files are generated and stored in a sFTP location when a backup job is scheduled in the Cisco Prime Collaboration Assurance. A non-zero size file is created at the location. The job scheduled in the Cisco Prime Collaboration Assurance is in the failed state every time it is executed.

Expectation: The job must not fail or if it fails there must be reasons for failure.

The Cisco Prime Collaboration Assurance backup job status displays failure in spite of generating reports in sFTP. Hence, while backing up, modify the path of the sFTP server. Use a non-root user location for setting up the sFTP location for reports in the Cisco Prime Collaboration Assurance. The issue is due to the absence of the GPG key in the user folder.

The sFTP location for backup can be any other directory other than the root directory since GPG encryption is not enabled for the root directory.

If you choose the location under the root directory, then you must enable GPG encryption in the root directory.

Check the Backup History

You can check the backup history. Log in to the Cisco Prime Collaboration Assurance server.

Path: **System Administration** > **Backup Settings**

All the backups scheduled or configured are listed on the Backup Settings page. You can check the history from the **Run History** column. Click the hyperlink on each log listed in the column for more information.

Restore Data on the Same System

You can execute restore for both Assurance and Analytics from the user interface. Backup is performed in Cisco Prime Collaboration Assurance User Interface through **Backup Management**. The backup data can be restored using the Cisco Prime Collaboration Assurance Serviceability.

Note

- The system reboots after successful Cisco Prime Collaboration Assurance restore.
- Restore might fail in the following conditions -
  1. When connection to the remote server fails.
  2. If Analytics fails to stop.
  3. If the server does not have enough space for backup.

To start restore

Procedure

Step 1 Choose **Maintenance** > **Restore**.

Step 2 Select the **Restore Category** from the drop-down list. You have two options to restore:

- **Assurance & Analytics** – You can restore files for Assurance and Analytics.
- **Assurance** – You can restore files only for Assurance.

Step 3 In the **Assurance Connection Settings** pane, enter the following details.

You can use sFTP or local connection to restore.

Assurance backup data resides in the local PC server or in the remote sFTP server.

Step 4 From **Restore Connection**,

a) If you select **sFTP**, enter the following details:

1. **IP Address** of the server where the backup file resides.
2. **Path** to the restore location.

Field	Description
SSH Username	Enter a name for the SSH Username. For example, user1 or provide any desired name.
Path	Enter a name for the path. For example, the path that you provide should be **/backup/assurance_backup/{backup filename}**. Where, • /backup can be any desired name. This is the path given while taking a backup. • /assurance_backup - folder should be in this format.

3. **Port**
4. **Username**
5. **Password**

Click **Test Connection** to test the sFTP connection using the credentials.

b) If you select **Local**, enter the following details:

1. Specify the location or **Restore Path** including the filename. This is the location where the backup resides on the local machine.
2. You can specify the number of restore files to be saved, using the **Restore History** drop-down list.

Step 5 **Note** The **Analytics Connection Settings** pane is available only if you have enabled Cisco Prime Collaboration Analytics.

In the **Analytics Connection Settings** pane, enter the following details.

You can use only a remote server to restore the Analytics data using SSH configuration. The credentials used is only related to SSH and not sFTP.

Analytics backup data always resides only in a remote server and in order to download the data from the remote server, you MUST provide SSH details of the remote server.

a. **Remote IP Address** of the remote server where Analytics backup data resides.

b. **Path** in the remote sever where the Analytics backup data resides. You must provide the relative path.

For restore, provide the path excluding the logged in user home directory. For example,

Field	Description
SSH Username	Enter a name for the SSH Username. For example, user1 or provide any desired name.
Path	Enter a name for the path. For example, the path that you provide should be **/backup/pg_basebackup** (followed by the timestamp (for example, pg_basebackup_201707201255)). Where, • /backup can be any desired name. This is the path given while taking a backup. • /pg_basebackup - folder should be in this format.

c. **SSH Port** of the remote server.

d. **SSH Username** of the remote server.

e. **SSH Password** of the remote server.

Click **Test Connection** to test the connection using the credentials.

Step 6 Click **Start Restore**.

A message indicating "After successful PCA Restore, system reboot will be performed. Do you want to continue?" appears.

- Click **OK** to perform Cisco Prime Collaboration Assurance restore.
- Click **Cancel** to exit the Cisco Prime Collaboration Assurance restore process.

Note Time taken for restoration is based on the file size.

Restore on a New System

Cisco 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 through the VM console using vSphere Client and perform restore as described in Restore Data. See also, Create a Repository.

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