



## バックアップと復元の実行

---

このセクションでは、次の点について説明します。

- [バックアップと復元の実行 \(1 ページ\)](#)

## バックアップと復元の実行

Cisco Prime Collaboration Assurance のユーザインターフェイスを使用して、定期的なバックアップをスケジュール、

Cisco Prime Collaboration Analytics データは、SSH を使用してリモート サーバ上にバックアップされます。これは Cisco Prime Collaboration Assurance のバックアップ リポジトリを使用しません。分析データは、ユーザインターフェイスを使用してのみバックアップでき、CLI を介してデータを復元することができます。



(注) Cisco Prime Collaboration Analytics のバックアップ用には Linux サーバが推奨されています。

Cisco Prime Collaboration Analytics は Windows サーバでバックアップすることもできます。および Cygwin UNIX シェルのみを使用して提供されます。Windows サーバのバックアップサポートでは、その他の SSH ツールまたは Unix シェルを使用することはできません。

### 関連トピック

[会議の監視](#)

[ビデオ エンドポイントのトラブルシューティング ワークフロー](#)

[ページ ポリシー](#)

[概要](#)

## バックアップと復元の概要

Cisco Prime Collaboration Assurance では、次のページ ポリシーを使用しています。

- 1 日以上経過したすべての会議統計とエンドポイント統計データはページされます。

- **Cisco Prime Collaboration** リリース 11.5 以降の場合

14日以上経過したすべての会議およびトラブルシューティング情報は、1時間ごとにページされます。

- **Cisco Prime Collaboration** リリース 11.6 以前のの場合

30日以上経過したコール品質のイベント履歴および音声/ビデオ電話の監査レポートデータは、ページされます。

**Cisco Prime Collaboration** リリース 12.1 以降の場合

30日以上経過したコール品質イベント履歴とエンドポイントに関連する監査レポートデータは削除されます。

- 14日以上経過したクリア済みアラームおよびイベントは、1時間に1回ページされます。アラームがページされると、すべての関連イベントもページされます。アクティブなイベントとアラームはページされません。
- 14日以上経過しており、ステータスが完了済み、失敗、またはキャンセルのジョブは、1時間に1回ページされます。

バックアップと復元サービスを使用して、データベース、コンフィギュレーションファイル、ログファイルをリモートロケーションとローカルディスクのいずれかにバックアップできます。バックアップサービスでバックアップされるのは次のフォルダのファイルです。

<b>Assurance</b> バックアップのデータタイプ
Assurance データベース
コンフィギュレーションファイル

  

<b>Analytics</b> バックアップのデータタイプ
Analytics データベース
ログファイル
レポート（スケジュール済みレポートとカスタムレポート）
ロゴ

## バックアップ期間

Cisco Prime Collaboration Assurance サーバが管理する対象デバイスの数に応じて、データバックアップの所要時間は次のとおりとなります。

- 最大 150,000 エンドポイント：4 時間
- 最大 80,000 エンドポイント：2.5 - 3 時間
- 最大 20,000 エンドポイント：2 時間

- 最大 3,000 エンドポイント : 1 時間



**Note** ネットワーク遅延が 20 ms を超えると、上記の時間を満たすことができません。

バックアップをスケジュールする場合、この操作によって Cisco Prime Collaboration Assurance のユーザインターフェイスのパフォーマンスが低下する可能性があるため、業務時間外を推奨します。

## FTP、ディスク、SFTP、または TFTP サーバでのリポジトリの作成

Cisco Prime Collaboration のデータをバックアップする前に、リポジトリを作成する必要があります。デフォルトでは、バックアップ サービスは \*.tar.gpg ファイルを設定されたリポジトリに作成します。バックアップされたファイルは圧縮形式になっています。CD-ROM、ディスク、HTTP、FTP、SFTP または TFTP にあるリポジトリを使用できます。

**ステップ 1** インストール中に作成したアカウントを使用して Cisco Prime Collaboration サーバにログインします。デフォルトのログインは *admin* です。

**ステップ 2** 次のコマンドを入力して、ローカルにリポジトリを作成します。

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

次のコマンドを入力して、FTP サーバにリポジトリを作成します。

```
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
```

それぞれの説明は次のとおりです。

- *RepositoryName* とは、ファイルをバックアップする場所を指します。この名前には最大 30 文字までの英数字を指定できます。
- *ftp://ftpserver/directory* とは、FTP サーバおよびサーバ上のディレクトリで、ここにファイルを転送します。FTP の代わりに SFTP、HTTP、または TFTP を使用することもできます。
- ユーザ名と {**plain**|**hash**} パスワードは、FTP、SFTP、または TFTP サーバのユーザ名とパスワードです。**hash** で暗号化されたパスワードを指定し、**plain** で非暗号化されたプレーン テキストのパスワードを指定します。

次に例を示します。

```
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
```

## リポジトリ データの一覧表示

リポジトリ内のデータを一覧表示できます。Cisco Prime Collaboration サーバに *admin* としてログインし、次のコマンドを実行します。

```
admin# show repository RepositoryName
```

次に例を示します。

```
admin# show repository myftp assurance_Sun_Feb_09_14_20_30_CST_2014.tar.gpg
```

# Cisco Prime Collaboration Assurance および Analytics ユーザ インターフェイスを使用したスケジュールのバックアップ

## Cisco Prime Collaboration リリース 11.1 以前の場合

ユーザ インターフェイスから Assurance および Analytics の両方にバックアップをスケジュールし、実行できます。

## Cisco Prime Collaboration リリース 11.5 以降の場合

バックアップするには、管理者としてログインする必要があります。

新しいバックアップ ジョブを作成するには、次のようにします。

---

**ステップ 1** 選択 [システム管理 (System Administration)] > [バックアップ設定 (Backup Settings)]。

**ステップ 2** [Backup] ページで [New] をクリックします。

**ステップ 3** バックアップ ジョブの名前を入力します。

バックアップ名が指定されていない場合、[Backup Title] フィールドは、デフォルトにより日付スタンプに設定されます。

**ステップ 4** ドロップダウン リストから [Backup Category] を選択します。

**ステップ 5** [Assurance Connection Settings] ペインで次の詳細情報を入力します。

sFTP、FTP、またはローカル接続を使用してバックアップを作成できます。

[sFTP] または [FTP] を選択した場合は、次の詳細情報を入力します。

- バックアップ ファイルの格納先サーバの IP アドレス
- バックアップの場所へのパス バックアップは、

(注) 指定されたユーザ ホーム ディレクトリで実行されます。例としては、

フィールドの	[説明 (Description) ]
SSH ユーザ名	SSH のユーザ名を入力します。たとえば、「user1」または任意の名前を指定します。
[パス (Path) ]	パスの名前を入力します。例としては、「/backup」などです。 その後、アシユアランスのバックアップの場所は /backup/assurance_backup になります。
バックアップは、/user1/backup/assurance_backup に保存されます。	

- ポート (sFTP の場合のみ)
- ユーザ名
- パスワード

クレデンシャルを使用して sFTP または FTP 接続をテストするには、[テスト (Test) ] をクリックします。

ローカルを選択した場合は、ローカル マシンにバックアップ ファイルを保存する場所を指定します。

ローカルバックアップの場合は、[Backup History] ドロップダウンリストを使用して、保存するバックアップファイルの数を指定できます。デフォルトでは、最後の2個のバックアップファイルが保存されます。バックアップ ファイルは、最大9個まで保存できます。

[Analytics Connection Settings] ペインは、Cisco Prime Collaboration Analytics を有効にした場合のみ使用することができます。

### Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Analytics は、MSP 展開でサポートされています。

**ステップ 6** [Analytics Connection Settings] ペインで次の詳細情報を入力します。

SSH を使用して Analytics データをバックアップする場合は、リモート サーバのみ使用できます。

- バックアップ ファイルが保存されるリモート サーバの IP アドレス
- バックアップの場所へのパス。相対パスを指定する必要があります。

(注) バックアップは、指定したユーザのホーム ディレクトリで実行されます。例としては、

フィールドの	[説明 (Description) ]
SSH ユーザ名	SSH のユーザ名を入力します。たとえば、「user1」または任意の名前を指定します。
[パス (Path) ]	パスの名前を入力します。例としては、「/backup」などです。 分析のバックアップ先は/backup/pg_basebackup となり、その後にタイムスタンプが続きます (例 : pg_basebackup_201707201255) 。
バックアップは /user1/backup に保存されます。	

Analytics のバックアップ フォルダは次の形式になります。pg\_basebackup の後にタイムスタンプ (例 : pg\_basebackup\_201707201255) 。sFTP サーバ上にユーザが存在しない場合、バックアップは失敗します。

- SSH ポート
- SSH ユーザ名
- SSH パスワード

クレデンシャルを使用して接続をテストするには、[Test] をクリックします。

**ステップ 7** バックアップ開始時刻および繰り返し間隔を指定します。

日付の選択に表示される時刻は、クライアントブラウザの時刻です。

**ステップ 8** (オプション) バックアップステータス通知の送信先となる電子メール ID を入力します。複数の電子メール ID はカンマで区切って指定します。

電子メールを受信するには、Cisco Prime Collaboration Assurance サーバで SMTP サーバの詳細を ([アラームとイベントの電子メール設定 (E-mail Setup for Alarms & Events) ]) で設定します。

#### Cisco Prime Collaboration リリース 11.5 以降の場合

電子メールを受信するには、Cisco Prime Collaboration Assurance サーバで SMTP サーバの詳細を ([アラームおよびレポート管理 (Alarm & Report Administration) ]> [アラームおよびイベント用に電子メールをセットアップ (E-mail Setup for Alarms & Events) ]) で設定します。

**ステップ 9** [Save] をクリックします。

スケジュール設定したバックアップ ジョブが [Backup Management] ページに一覧表示されます。

[Run Now] をクリックすると、即座にバックアップを実行できます。

## トラブルシューティング

**問題：** Cisco Prime Collaboration Assurance のバックアップ ジョブのステータスが、レポートの生成後もエラーと表示される。バックアップ ジョブが Cisco Prime Collaboration Assurance でスケジュールされている場合、バックアップ ファイルは sFTP ロケーションに生成され格納されます。この場所に、ゼロ以外のサイズのファイルが作成されます。Cisco Prime Collaboration Assurance でスケジュールされたジョブのステータスが、実行されるたびにエラーになります。

**期待：** ジョブがエラーにならないか、エラーの原因が存在してエラーになる必要があります。

Cisco Prime Collaboration Assurance のバックアップ ジョブのステータスが、sFTP にレポートが生成されるにもかかわらずエラーと表示されます。その場合は、バックアップ時に sFTP サーバのパスを変更してください。Cisco Prime Collaboration Assurance のレポートに使用する sFTP ロケーションに、非ルートユーザロケーションを設定します。この問題の原因は、GPG キーがユーザフォルダに存在しないことです。

バックアップに使用する sFTP ロケーションには、ルートディレクトリ以外のどのディレクトリを使用してもかまいません（ルートディレクトリでは GPG 暗号化が無効であるため）。

ルートディレクトリの下にある場所を選択した場合は、ルートディレクトリで GPG 暗号化を有効にする必要があります。

## CLI を使用した Cisco Prime Collaboration Assurance データのバックアップ

CLI は SSH を介してのみサポートされます。telnet はサポートされません。Cisco Prime Collaboration サーバで使用されるポートは 26 です。リポジトリを作成した後、*admin* として Cisco Prime Collaboration サーバにログインし、次のコマンドを実行してデータをバックアップします。

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

それぞれの説明は次のとおりです。

- **Backupfilename** : バックアップファイル名（拡張子 *.tar.gpg* なし）。この名前には最大 100 文字までの英数字を指定できます。
- **RepositoryName** : ファイルをバックアップする場所。この名前には最大 30 文字までの英数字を指定できます。

バックアップが完了すると、次のメッセージが表示されます。

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

バックアップファイルには、サフィックスとして末尾にタイムスタンプ (*YYMMDD-HHMM*) とファイル拡張子 *.tar.gpg* が付され、リポジトリに保存されます。

FTP サーバでのバックアップ例：

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

ここで、*myftp* がリポジトリ名です。

## バックアップ履歴の確認

バックアップ履歴を確認できます。Cisco Prime Collaboration Assurance サーバにログインします。

パス : [システム管理 (System Administration)] > [バックアップの設定 (Backup Settings)]

スケジュール済み、または設定済みのすべてのバックアップは、[バックアップの設定 (Backup Settings)] ページにリストされます。[実行履歴 (Run History)] 列から履歴を確認できます。詳細については、列にリストされている各ログのハイパーリンクをクリックしてください。

## 同じシステムでのデータの復元

以降の項では、同じシステムでデータを復元する処理について説明します。

データを復元するには、vSphere クライアントを使用して、VM コンソールから *admin* として Cisco Prime Collaboration アプリケーション サーバにログインします。SSH/Putty プロンプトから復元をトリガーすることを推奨しません。

Cisco Prime Collaboration データを復元するには、次のコマンドを実行します。

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

ここで、*Backupfilename* は、サフィックスとして末尾にタイムスタンプ (YYMMDD-HHMM) とファイル拡張子 .tar.gpg が付いたバックアップファイルの名前です。

FTP サーバでの復元例 :

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

## 新しいシステムでの復元

Cisco Prime Collaboration では、システムのデータをバックアップし、システム全体に障害が発生した場合に別のシステムでデータを復元することができます。

別のシステムからのバックアップを復元するには、次の手順を実行します。

データの復元先のシステムには、バックアップされたシステムと同じ MAC アドレスが必要です (IP アドレスとホスト名は違っていてもかまいません)。

システム (バックアップされた元のシステム) の MAC アドレスを別のシステムに割り当てることができない場合は、Cisco TAC に新しいライセンスファイル (新しい MAC アドレス用) に関する情報をお問い合わせください。

別のシステムからのバックアップを復元するには、vSphere クライアントを使用して VM コンソールを介して管理者としてログインし、「データの復元」の説明に従って復元を実行します。「リポジトリの作成」も参照してください。



**Note** 実行後の要件として、データの復元後にはすべてのデバイスを再検出する必要があります。