バックアップの管理

ここでは、次の内容について説明します。

- Cisco Crosswork のバックアップと復元の管理 （1 ページ）
- 災害後の復元 （4 ページ）
- 欠落している SR-TE ポリシーと RSVP-TE トンネルの解決 （5 ページ）
- Cisco NSO を使用した Cisco Crosswork のバックアップ （6 ページ）
- Cisco NSO を使用した復元 （8 ページ）

Cisco Crosswork のバックアップと復元の管理

Cisco Crosswork のバックアップ機能と復元機能は、データ損失を防ぎ、インストールされているアプリケーションと設定を保持します。

（注） Cisco Crosswork バックアッププロセスに Cisco NSO データを含める場合は、ここで説明する手順の代わりに、Cisco NSO を使用した Cisco Crosswork のバックアップ （6 ページ）の手順を実行します。

Cisco Crosswork クラスタのバックアップを作成する場合、またはバックアップからクラスタを復元する場合は、次のガイドラインに従います。

- 最初のログイン時に、バックアップファイルを保存する接続先 SCP サーバーを設定します。この設定は 1 回限りのアクティビティです。このタスクを完了するまで、バックアップを実行したり、復元操作を開始したりできません。
- バックアップ操作または復元操作は、スケジュールされているメンテナンス期間にのみ実行することをお勧めします。これらの操作の実行中、ユーザーは Cisco Crosswork にアクセスしようとしないでください。バックアップではシステムが約 10 分間オフラインになりますが、復元操作に時間がかかることがあります。両方とも、完了するまで他のアプリケーションを一時停止します。これらの一時停止は、データ収集ジョブに影響を与える可能性があります。

- 通常の復元を実行すると、Cisco Crosswork アプリケーションとデータは、バックアップを作成したときと同じバージョンに復元されます。災害後の復元を実行する場合は、バックアップの作成時に使用したものと同じ Cisco Crosswork ソフトウェアイメージを使用する必要があります。異なるバージョンのソフトウェアを使用して作成したバックアップを使用して災害後の復元を実行することはできません。
- ダッシュボードを使用して、プロセスが完了するまで、バックアップまたは復元プロセスの進行状況をモニタします。プロセス中に Cisco Crosswork システムを使用しようとすると、さまざまなサービスが一時停止して頻繁に再起動するため、誤ったコンテンツやエラーが表示されることがあります。
- 一度に実行できるバックアップまたは復元操作は 1 つだけです。
- Cisco Crosswork クラスタと SCP サーバーの両方が同じ IP 環境内に存在する必要があります。たとえば、Cisco Crosswork が IPv6 で通信している場合は、バックアップサーバーも IPv6 で通信している必要があります。
- バックアップサーバーで Cisco Crosswork が作成したバックアップ tarball を移動したり、名前を変更したりしないでください。バックアップサーバーの領域を節約するために、古いバックアップを削除することもできますが、このバージョンのジョブリストには引き続き表示されます。

始める前に

作業を開始する前に、次を確認してください。

- セキュアな SCP サーバーのホスト名または IP アドレスおよびポート番号。
- バックアップファイルの接続先として使用する SCP サーバー上のファイルパス。
- 接続先 SCP サーバーのリモートパスに対するファイルの読み取り/書き込み権限を持つアカウントのユーザークレデンシャル。

ステップ 1 **SCP バックアップサーバーを設定します。**

a) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。
b) [接続先（Destination）] をクリックして、[接続先の編集（Edit Destination）] ダイアログボックスを表示します。表示されたフィールドに関連するエントリを入力します。
c) [保存（Save）] をクリックして、バックアップサーバーの詳細を確認します。

ステップ 2 **バックアップを作成します。**

a) **[アクション（Actions）]** > **[バックアップ（Backup）]** をクリックして、宛先サーバーの詳細が事前に入力された [バックアップ（Backup）] ダイアログボックスを表示します。
b) [ジョブ名（Job Name）] フィールドに、バックアップに該当する名前を入力します。
c) アプリケーションまたはマイクロサービスの問題があるにもかかわらず、Cisco Crosswork にバックアップを作成させる場合は、[強制（Force）] チェックボックスをオンにします。
d) [NOS のバックアップ（Backup NSO）] チェックボックスは必ずオフにします。

Cisco Crosswork バックアッププロセスに Cisco NSO のデータを含める場合は、ここで説明する手順の代わりにCisco NSO を使用した Cisco Crosswork のバックアップ （6 ページ）に示す手順を実行します。

e) （任意）[バックアップの準備状況の確認（Verify Backup Readiness）] をクリックして、バックアップを完了するのに十分な空きリソースが Cisco Crosswork にあることを確認します。Cisco Crosswork は、リモートの接続先が正しく指定されていて、アプリケーションが正常である場合、どのアプリケーションも更新されていないことも確認します。検証に成功すると、この操作には時間がかかることについての警告が Cisco Crosswork に表示されます。[OK] をクリックします。

検証に失敗した場合は、シスコ カスタマー エクスペリエンス チームにお問い合わせください。

f) [バックアップの開始（Start Backup）] をクリックして、バックアップ操作を開始します。Cisco Crosswork は、対応するバックアップジョブセットを作成し、それをジョブリストに追加します。

g) バックアップジョブの進行状況を表示するには、[ジョブセットのバックアップ/復元（Backup Restore Job Sets）] テーブルの検索フィールドにジョブの詳細（ステータスやジョブタイプなど）を入力します。次に、目的のジョブセットをクリックします。

[ジョブの詳細（Job Details）] テーブルに、選択したジョブセットに関する情報（ジョブステータス、ジョブタイプ、開始時刻など）が表示されます。失敗したジョブがある場合は、[ステータス（Status）] 列の近くにある アイコンの上にマウスポインタを合わせると、エラーの詳細が表示されます。

h) リモートサーバへのアップロード中にバックアップが失敗した場合：[ジョブの詳細（Job Details）] パネルの [ステータス（Status）] アイコンのすぐ下にある [バックアップのアップロード（Upload backup）] ボタンをクリックして、アップロードを再試行します。

リモートサーバーの問題が原因でアップロードが失敗した場合は、[バックアップのアップロード（Upload backup）] をクリックする前に、[接続先（Destination）] ボタンを使用して別のリモートサーバーとパスを指定します。

（注） オーケストレータが実行されていたノードを削除または再起動（グレースフルまたはアングレースフル）すると、ノードの再起動時にすべてのバックアップジョブで [バックアップのアップロード（Upload backup）] オプションが無効になります。再度有効にするには、新しいバックアップジョブをトリガーする必要があります。

ステップ 3 バックアップファイルから復元するには、次の手順を実行します。

a) [ジョブ設定のバックアップ/復元（Backup Restore Job Sets）] テーブルから必要なバックアップファイルを選択します。ページの左側にジョブリストが表示され、右側に選択したジョブの詳細が表示されます。

b) [復元（Restore）] をクリックし、接続先サーバーの詳細が事前に入力されている [復元（Restore）] ダイアログボックスを表示します。

c) [ジョブ名（Job Name）] フィールドに、該当する名前を入力します。

d) アプリケーションまたはマイクロサービスの問題があるにもかかわらず、Cisco Crosswork にバックアップを作成させる場合は、[強制（Force）] チェックボックスをオンにします。

e) （オプション）[復元の確認（Verify Restore）] をクリックして、Cisco Crosswork に復元を完了するのに十分な空きリソースがあることを確認します。確認が成功すると、時間がかかる動作の特性に関する警告が Cisco Crosswork に表示されます。[OK] をクリックします。

f) [復元の開始（Start Restore）] をクリックして復元操作を開始します。Cisco Crosswork によって対応する復元ジョブのセットが作成され、ジョブリストに追加されます。

復元操作の進行状況を表示するには、進行状況ダッシュボードへのリンクをクリックします。

g) 復元が完了したら、すべてのアプリケーションのステータスが [Crosswork Manager] 画面に正常と表示されるのを待ってから、操作を実行します。

災害後の復元

ディザスタリカバリは、自然災害または人為的な災害によって Cisco Crosswork クラスタが破壊された後に使用する復元操作です。『*Cisco Crosswork Platform and Applications Installation Guide*』の手順に従って、最初に新しいクラスタを展開する必要があります。

クラスタに誤動作しているハイブリッドノードが 1 つあるか、または 1 つ以上のワーカーノードがある場合は、ディザスタリカバリを実行しないでください。代わりに、クラスタ管理機能を使用してこれらのノードを再展開するか、「Crosswork クラスタの管理」の章の説明に従って新しいノードに置き換えます。

誤動作しているハイブリッドノードが複数ある場合、システムは機能状態になりません。障害が発生したハイブリッドノードを交換または再起動しても、システムが正常に回復する保証はありません。この場合、新しいクラスタを展開した後、古いクラスタから取得した最新のバックアップを使用するとシステム全体を回復できます。詳細については、「Crosswork クラスタの管理」の章を参照してください。

ディザスタリカバリを実行する場合は、次の点に注意してください。

- バックアップを復元する新しい Cisco Crosswork クラスタは、バックアップを作成したものと同じ IP アドレスを使用する必要があります。内部証明書は元のクラスタの IP アドレスを使用するため、このガイドラインは重要です。
- 新しいクラスタには、バックアップを作成したクラスタと同じ数とタイプのノードが必要です。
- 新しいクラスタは、バックアップの作成時に使用したものと同じ Cisco Crosswork のソフトウェアイメージを使用する必要があります。異なるバージョンのソフトウェアを使用して作成されたバックアップを使用してクラスタを復元することはできません。
- 災害が発生する前のシステムの状態を回復できるように、バックアップを最新の状態に保ちます。復元操作では、バックアップが作成されたときにインストールされていたすべてのアプリケーションを復元します。前回のバックアップ以降に追加のアプリケーションやパッチをインストールしてた場合は、別のバックアップを作成します。
- ディザスタリカバリが失敗した場合は、シスコ カスタマー エクスペリエンスにお問い合わせください。

ディザスタリカバリを実行するには、次の手順を実行します。

始める前に

SCP バックアップサーバーから、ディザスタリカバリで使用するバックアップファイルの完全な名前を取得します。このファイルは通常は作成した最新のバックアップファイルです。Cisco Crosswork のバックアップファイル名の形式は次のとおりです。

`backup_JobName_CWVersion_TimeStamp.tar.gz`

ここで、

- *JobName* は、ユーザーが入力したバックアップジョブの名前です。
- *CWVersion* は、バックアップされたシステムの Cisco Crosswork プラットフォームのバージョンです。
- *TimeStamp* は、Cisco Crosswork がバックアップファイルを作成した日時です。

例：`backup_Wednesday_4-0_2021-02-31-12-00.tar.gz`

ステップ 1 新たに展開したクラスタのメインメニューから、**[管理（Administration）]**>**[バックアップと復元（Backup and Restore）]** を選択します。

ステップ 2 **[アクション（Actions）]** > **[災害後の復元（Disaster Restore）]** をクリックして、接続先サーバーの詳細が事前に入力された [災害後の復元（Disaster Restore）] ダイアログボックスを表示します。

ステップ 3 [バックアップファイル名（Backup File Name）] フィールドにバックアップファイル名を入力します。

ステップ 4 [復元の開始（Start Restore）] をクリックして、ディザスタリカバリ操作を開始します。

操作の進行状況を表示するには、進行状況ダッシュボードへのリンクをクリックします。

欠落している SR-TE ポリシーと RSVP-TE トンネルの解決

このトピックの情報は、Cisco Crosswork Optimization Engine がインストールされている場合にのみ適用されます。

設定データベースには、Cisco Crosswork が 認識しているすべての SR-TE ポリシーと RSVP-TE トンネルが含まれています。Cisco Crosswork は、SR-TE ポリシーまたは RSVP-TE トンネルをプロビジョニング、変更、または削除するたびに設定データベースを更新します。設定データベースの CLI ツールを使用して、次の操作を実行できます。

- 設定データベースに対する CSV ファイルの読み取りと書き込み。
- 設定データベースから SR-TE ポリシーと RSVP-TE トンネル情報の入力による CSV ファイルの作成。

設定データベース の CLI ツールは、復元操作後に欠落している SR-TE ポリシーと RSVP-TE トンネルを回復する場合に特に役立ちます。たとえば、`-dump-missing` オプションは、欠落している SR-TE ポリシーと RSVP-TE トンネルのリストを表示する CSV ファイルを生成します。

この CSV ファイルを使用して、欠落している SR-TE ポリシーと RSVP-TE トンネルを特定します。次に、`-load`オプションを使用してトポロジにもう一度ロードします。詳細については、CLI ツールのヘルプを参照してください。

ステップ 1 **optima-pce-dispatcher** コンテナを入力します。

```
kubectl exec -it optima-pce-dispatcher-XXXXXXX-XXXX bash
```

ステップ 2 次のコマンドを実行できます。

a) CLI ツールのヘルプテキストを表示します。

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --help
```

b) 設定データベース内のすべての SR-TE ポリシーと RSVP-TE トンネルを CSV ファイルに保存します。

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --dump /<PathToFile>/dump_file.csv
```

c) 生成された CSV ファイルから内容をロードし、設定データベースにポリシーを書き込みます。

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --load /<PathToFile>/load_file.csv
```

（注） このコマンドは、検出された重複する SR-TE ポリシーまたは RSVP-TE トンネルを上書きし、有効な TE トンネルのみを設定データベースに追加します。重複する SR-TE ポリシーには、同じ組み合わせのヘッドエンド、エンドポイント、および色があります。重複する RSVP-TE トンネルには、同じ組み合わせのヘッドエンドとトンネル名があります。

d) CSV のロードが完了したら、次のように、Cisco Crosswork Optimization Engine を再起動してその UI を設定データベースと同期します。

1. メインメニューから、**[管理（Administration）]** > > **[Crosswork Manager]** > **[Crosswork の正常性（Crosswork Health）]** > **[最適化エンジン（Optimization Engine）]** を選択します。
2. **[optima-ui-service]** > > **[アクション（Action）]** > **[再起動（Restart）]** を選択します。再起動には約 5 分かかります。

e) 再起動後、現在トポロジ内にある SR-TE ポリシーと RSVP-TE トンネルを設定データベースの内容と比較します。欠落している SR ポリシーと RSVP-TE トンネルを CSV ファイルに保存します。この CSV ファイルと次のコマンドを使用して、欠落しているポリシーを設定データベースにロードできます。

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py -dump-missing /<PathToFile>/dump_file.cs
```

Cisco NSO を使用した Cisco Crosswork のバックアップ

現在、NSO バックアップファイルからの復元は手動プロセスです。

始める前に

始める前に、次のことを確認します。

- セキュア SCP サーバーのホスト名または IP アドレスとポート番号がわかっている。
- バックアップファイルの接続先として使用する SCP サーバーのファイルパスがわかっている。
- 接続先 SCP サーバーのストレージフォルダに対する読み取り権限と書き込み権限を持つアカウントのユーザークレデンシャルがわかっている。

また、NSO プロバイダ、NSO プロバイダに関連付けられている Cisco Crosswork のクレデンシャルプロファイル、およびNSOサーバーが次の前提条件を満たしていることを確認します。

- Crosswork の NSO プロバイダ設定でポート 22 に SSH 接続がある。プロバイダでこの接続を有効にしない場合、または誤ったポートで有効にした場合、Cisco Crosswork はバックアップ中に警告メッセージを表示し、Cisco Crosswork が NSO 用ではなく、独自のデータ用のバックアップを作成することを示します。
- NSO プロバイダのクレデンシャルプロファイルには、NSO サーバーで `sudo` 権限を持つユーザーのユーザー ID とパスワードが含まれている。
- NSO サーバーには NCT（NSO クラスタツール）がインストールされており、NSO プロバイダのクレデンシャルプロファイルのユーザーは `nct` コマンドを実行できる。
- NSO サーバーには Python バージョン 3.x がインストールされており、NSO プロバイダのクレデンシャルプロファイルのユーザーは `python3` コマンドを実行できる。
- NSOプロバイダのクレデンシャルプロファイルのユーザーは、NSOサーバーのバックアップフォルダとその中のファイルにフルアクセスできる。この要件は通常、NSOサーバーの `/var/opt/ncs/backups/` フォルダに対する完全な読み取り/書き込みアクセスを意味します。

これらの要件のいずれかが満たされていない場合、バックアップジョブのすべて、または一部が失敗します。

ステップ 1 **SCP バックアップサーバーを設定します。**

a) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。
b) [接続先（Destination）] をクリックして、[接続先の編集（Edit Destination）] ダイアログボックスを表示します。表示されたフィールドに関連するエントリを入力します。
c) [保存（Save）] をクリックして、バックアップサーバーの詳細を確認します。

ステップ 2 **Cisco Crosswork と Cisco NSO のバックアップを作成します。**

a) **[アクション（Actions）]** > **[バックアップ（Backup）]** をクリックして、宛先サーバーの詳細が事前に入力された [バックアップ（Backup）] ダイアログボックスを表示します。
b) [ジョブ名（Job Name）] フィールドに、バックアップに該当する名前を入力します。
c) アプリケーションまたはマイクロサービスの問題があるにもかかわらず、Cisco Crosswork にバックアップを作成させる場合は、[強制（Force）] チェックボックスをオンにします。
d) [NSO のバックアップ（Backup NSO）] チェックボックスはオンのままにしてください。

e) （オプション）[バックアップの確認（Verify Backup）] をクリックして、Cisco Crosswork にバックアップを完了するのに十分な空きリソースがあることを確認します。確認が成功すると、時間がかかる動作の性質に関する警告が Cisco Crosswork に表示されます。[OK] をクリックします。

f) [バックアップの開始（Start Backup）] をクリックして、バックアップ操作を開始します。Cisco Crosswork は、対応するバックアップジョブセットを作成し、それをジョブリストに追加します。

g) バックアップジョブの進行状況を表示するには、[ジョブセットのバックアップ/復元（Backup Restore Job Sets）] テーブルの検索フィールドにジョブの詳細（ステータスやジョブタイプなど）を入力します。次に、必要なジョブセットをクリックします。

[ジョブの詳細（Job Details）] テーブルに、選択したジョブセットに関する情報（ジョブステータス、ジョブタイプ、開始時刻など）が表示されます。失敗したジョブがある場合は、[ステータス（Status）] 列の近くにある アイコンの上にマウスポインタを合わせると、エラーの詳細が表示されます。

Cisco NSO を使用した復元

Cisco Crosswork クラスタとそれに関連する Cisco NSO クラスタをバックアップから復元する場合は、次のガイドラインに従います。

- 復元操作は、スケジュールされているメンテナンス期間にのみ実行することをお勧めします。これらの操作の実行中、ユーザーは Cisco Crosswork や Cisco NSO にアクセスしようとしないでください。Cisco Crosswork の復元操作は時間がかかり、完了するまでは他の Cisco Crosswork アプリケーションが一時停止します。復元中は、Cisco NSO を完全に停止する必要があります。
- Cisco Crosswork と Cisco NSO の両方の復元操作を同時に実行できます。

始める前に

復元するバックアップファイルの完全な名前を SCP サーバーから取得します。このファイルには、Cisco Crosswork と Cisco NSO の両方のバックアップが含まれています。バックアップファイル名の形式は次のとおりです。

`backup_`*`JobName_CWVersion_TimeStamp`*`.tar.gz`

ここで、

- *JobName* は、ユーザーが入力したバックアップジョブの名前です。
- *CWVersion* は、バックアップされたシステムの Cisco Crosswork プラットフォームのバージョンです。
- *TimeStamp* は、Cisco Crosswork がバックアップファイルを作成した日時です。

例：`backup_Wed_4-0_2021-02-31-12-00.tar.gz.`

ステップ 1 リモート SCP バックアップサーバーにログインします（必要な場合）。Linux コマンドラインを使用して、バックアップ先ディレクトリにアクセスし、復元する Cisco NSO 情報を含んでいるバックアップファイルを検索します。次に例を示します。

```
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_4-0_2021-02-31-12-00.tar.gz
```

ステップ 2 `tar-xzvf` を使用して、接続先フォルダの Cisco Crosswork バックアップファイルから Cisco NSO バックアップを抽出します。次に例を示します。

```
[root@localhost~]# tar -xzvf backup_Wed_4-0_2021-02-31-12-00.tar.gz
...
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_4-0_2021-02-31-12-00.tar.gz
-rw-r--r--. 1 root root 8267798605 468c4715-ea09-4c2b-905e-98999d.tar.gz
```

ステップ 3 接続先フォルダの Cisco NSO バックアップファイルを展開します。`/nso/ProviderName/` のフォルダ構造に抽出する Cisco NSO ファイルが表示されます。ここで、`/nso/ProviderName/` は Cisco Crosswork に設定されている Cisco NSO プロバイダの名前です。次の例では、Cisco NSO プロバイダの名前は `nso121` です。

```
tar -xvsf 468c4715-ea09-4c2b-905e-98999d.tar.gz
468c4715-ea09-4c2b-905e-98999d/nso/
468c4715-ea09-4c2b-905e-98999d/nso/nso121/
468c4715-ea09-4c2b-905e-98999d/nso/nso121/log/
468c4715-ea09-4c2b-905e-98999d/nso/nso121/log/nso_backup_result_nso121_Wed.log
468c4715-ea09-4c2b-905e-98999d/nso/nso121/NSO_RESTORE_PATH_nso121
468c4715-ea09-4c2b-905e-98999d/nso/nso121/ncs-5.4.2@backup_Wed_nso121.backup.gz
...
```

ステップ 4 `/nso/ProviderName/` フォルダで拡張子が backup.gz のファイルを見つけます。これが、生成された Cisco NSO バックアップファイルです。前の手順の例では、ファイル名が強調表示されています。

ステップ 5 root 権限を持つユーザーとして Cisco NSO にログインし、コマンドラインにアクセスします。次に、生成された Cisco NSO バックアップファイルを SCP サーバーから Cisco NSO クラスタに指定した復元パスの場所へコピーまたは移動します。次に例を示します。

```
[root@localhost nso121]# ls
log ncs-5.4.2@backup_Wed_nso121.backup.gz NSO_RESTORE_PATH_nso121
[root@localhost nso121]# more NSO_RESTORE_PATH_nso121
/var/opt/ncs/backups/
[root@localhost nso121]#
...
```

ステップ 6 Cisco NSO の復元操作は、NSO が実行されていないときにのみ実行できます。Cisco NSO クラスタコマンドラインで、次のコマンドを実行して Cisco NSO を停止します。

```
$/etc/init.d/ncs stop
```

ステップ 7 NCS が停止したら、次のコマンドと生成された Cisco NSO バックアップファイルの名前を使用して復元操作を開始します。次に例を示します。

```
#ncs-backup --restore ncs-5.4.2@backup_Wed_nso121.backup.gz
```

このコマンドの実行に問題がある場合は、まず `sudo su` 権限を付与します。

ステップ 8 復元が完了したら、次のコマンドを使用して Cisco NSO を再起動します。このコマンドは完了するまでに数分かかる場合があります。

```
$/etc/init.d/ncs start
```

ステップ 9 Cisco Crosswork クラスタと Cisco NSO クラスタの両方をバックアップから復元したら、Cisco NSO プロバイダを Cisco Crosswork に再度追加します。

（注） NSO バックアップが実行されてからデバイスの設定が変更された可能性があります。NSO 設定をデバイスと同期させるには、変更された可能性があるすべてのデバイスに対して *sync-from* 操作を実行します。