



# IBM DB2の保護

## SnapCenter Software 6.0

NetApp  
July 23, 2024

# 目次

IBM DB2の保護 .....	1
IBM DB2用SnapCenterプラグイン .....	1
SnapCenter Plug-in for IBM DB2のインストールの準備 .....	10
データ保護を準備 .....	33
IBM DB2リソースのバックアップ .....	34
IBM DB2のリストア .....	55
IBM DB2リソースバックアップのクローニング .....	63

# IBM DB2の保護

## IBM DB2用SnapCenterプラグイン

### SnapCenter Plug-in for IBM DB2の概要

SnapCenter Plug-in for IBM DB2 Databaseは、IBM DB2データベースに対応したデータ保護管理を可能にする、NetApp SnapCenterソフトウェアのホスト側コンポーネントです。Plug-in for IBM DB2 Databaseは、SnapCenter環境でのIBM DB2データベースのバックアップ、リストア、およびクローニングを自動化します。

SnapCenterは、シングル・インスタンスおよびマルチ・インスタンスのDB2セットアップをサポートしています。Plug-in for IBM DB2 Databaseは、Linux環境とWindows環境の両方で使用できます。Windows環境では、DB2は手動リソースとしてサポートされます。

Plug-in for IBM DB2 Databaseがインストールされている場合は、SnapCenterとNetApp SnapMirrorテクノロジーを使用して、バックアップセットのミラーコピーを別のボリュームに作成できます。また、本プラグインをNetApp SnapVaultテクノロジーとともに使用して、標準への準拠を目的としたディスクツーディスクのバックアップ・レプリケーションを実行することもできます。

SnapCenter Plug-in for DB2は、ONTAPおよびAzure NetAppのファイルストレージレイアウトでNFSとSANをサポートします。

VMDKまたは仮想ストレージレイアウトはサポートされていません。

### SnapCenter Plug-in for IBM DB2の機能

Plug-in for IBM DB2 Databaseをインストールした環境では、SnapCenterを使用して、IBM DB2データベースとそのリソースをバックアップ、リストア、およびクローニングできます。これらの処理をサポートするタスクを実行することもできます。

- データベースを追加します。
- バックアップを作成します
- バックアップからリストアします
- バックアップをクローニングする。
- バックアップ処理のスケジュールを設定します。
- バックアップ、リストア、クローニングの各処理を監視する。
- バックアップ、リストア、クローニングの各処理のレポートを表示します。

### SnapCenter Plug-in for IBM DB2の機能

SnapCenter は、プラグインアプリケーションと統合されるほか、ストレージシステム上でネットアップのテクノロジーと統合されます。Plug-in for IBM DB2 Databaseを操作するには、SnapCenterグラフィカルユーザーインターフェイスを使用します。

• \* 統一されたグラフィカル・ユーザー・インターフェイス \*

SnapCenter のインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。SnapCenter インターフェイスを使用すると、すべてのプラグインでバックアップ、リストア、クローニングの各処理を一貫した方法で実行できるほか、ダッシュボードビューで概要を把握したり、ロールベースアクセス制御（RBAC）を設定したり、ジョブを監視したりすることができます。

• \* 中央管理の自動化 \*

バックアップ処理のスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理を実行したりできます。SnapCenter から E メールアラートを送信するように設定して、環境をプロアクティブに監視することもできます。

• 無停止のNetApp Snapshotコピーテクノロジー

SnapCenterは、Plug-in for IBM DB2 DatabaseでNetAppスナップショットテクノロジーを使用してリソースをバックアップします。

Plug-in for IBM DB2を使用すると、次のようなメリットもあります。

- バックアップ、リストア、クローニングのワークフローがサポートされます
- セキュリティが RBAC でサポートされ、ロール委譲が一元化されます

また、許可された SnapCenter ユーザにアプリケーションレベルの権限を付与するようにクレデンシャルを設定することもできます。

- NetApp FlexClone テクノロジーを使用して、スペース効率に優れたポイントインタイムコピーを作成し、テストまたはデータの抽出を行います

クローンを作成するストレージシステムに FlexClone ライセンスが必要です。

- バックアップ作成時にONTAPの整合グループ（CG）Snapshot機能がサポートされるようになりました。
- 複数のリソースホストで同時に複数のバックアップを実行できます

1回の操作で、1つのホスト内のリソースが同じボリュームを共有すると、スナップショットが統合されません。

- 外部コマンドを使用してスナップショットを作成する機能。
- XFS ファイルシステムで Linux LVM がサポートされています。

## SnapCenter Plug-in for IBM DB2でサポートされるストレージタイプ

SnapCenter は、物理マシンと仮想マシン（VM）の両方でさまざまなストレージタイプをサポートしています。SnapCenter Plug-in for IBM DB2をインストールする前に、ストレージタイプがサポートされていることを確認する必要があります。

マシン	ストレージタイプ
物理サーバと仮想サーバ	FC 接続 LUN

マシン	ストレージタイプ
物理サーバ	iSCSI で接続された LUN
物理サーバと仮想サーバ	NFS-connected ボリューム

## IBM DB2プラグインに必要な最小限のONTAP権限

必要な最小 ONTAP 権限は、データ保護に使用する SnapCenter プラグインによって異なります。

- フルアクセスコマンド： ONTAP 8.3.0 以降に必要な最小権限

- event generate-autosupport-log を指定します
- ジョブ履歴の表示
- ジョブが停止しました
- LUN
- lun create をクリックします
- lun create をクリックします
- lun create をクリックします
- lun delete
- LUN igroup add
- lun igroup create を追加します
- lun igroup delete
- LUN igroup の名前を変更します
- LUN igroup の名前を変更します
- lun igroup show を参照してください
- LUN マッピングの追加 - レポートノード
- LUN マッピングが作成されます
- LUN マッピングが削除されます
- LUN マッピングの削除 - レポートノード
- lun mapping show
- lun modify を追加します
- LUN のボリューム内移動
- LUN はオフラインです
- LUN はオンラインです
- LUN の永続的予約はクリアします
- LUN のサイズ変更

- LUN シリアル
- lun show をクリックします
- SnapMirror ポリシー追加ルール
- snapmirror policy modify-rule
- snapmirror policy remove-rule」を実行します
- snapmirror policy show の略
- SnapMirror リストア
- snapmirror show の略
- snapmirror show -history の略
- SnapMirror の更新
- SnapMirror の update-ls-set
- snapmirror list-destinations
- バージョン
- volume clone create を実行します
- volume clone show を実行します
- ボリュームクローンスプリット開始
- ボリュームクローンスプリットは停止します
- volume create を実行します
- ボリュームを削除します
- volume file clone create を実行します
- volume file show-disk-usage
- ボリュームはオフラインです
- ボリュームはオンラインです
- volume modify を使用します
- volume qtree create を実行します
- volume qtree delete
- volume qtree modify の略
- volume qtree show の略
- ボリュームの制限
- volume show のコマンドです
- volume snapshot create を実行します
- ボリューム Snapshot の削除
- volume snapshot modify の実行
- volume snapshot modify -snaplock-expiry-time
- ボリューム Snapshot の名前が変更されます

- ボリューム Snapshot リストア
- ボリューム Snapshot の restore-file
- volume snapshot show の実行
- ボリュームのアンマウント
- SVM CIFS です
- vservers cifs share create の場合
- SVM CIFS 共有が削除されます
- vservers cifs shadowcopy show
- vservers cifs share show のコマンドです
- vservers cifs show のコマンドです
- SVM エクスポートポリシー
- vservers export-policy create を参照してください
- vservers export-policy delete
- vservers export-policy rule create
- vservers export-policy rule show
- vservers export-policy show のコマンドを入力します
- Vserver iSCSI
- vservers iscsi connection show
- vservers show のコマンドです
- 読み取り専用コマンド： ONTAP 8.3.0 以降に必要な最小権限
  - Network Interface の略
  - network interface show の略
  - Vserver

## IBM DB2のSnapMirrorおよびSnapVaultレプリケーション用のストレージシステムを準備する

SnapCenter プラグインと ONTAP の SnapMirror テクノロジーを使用すると、バックアップセットのミラーコピーを別のボリュームに作成できます。また、ONTAP SnapVault テクノロジーを使用すると、標準への準拠やその他のガバナンス関連の目的でディスクツォーディスクのバックアップレプリケーションを実行できます。これらのタスクを実行する前に、ソースボリュームとデスティネーションボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenterは、Snapshot処理の完了後にSnapMirrorとSnapVaultの更新を実行します。SnapMirror更新とSnapVault更新はSnapCenter ジョブの一部として実行されるため、ONTAP スケジュールを別途作成しないでください。



ネットアップの SnapManager 製品から SnapCenter に移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリストレージ（ソースボリューム）上のデータがセカンダリストレージ（デスティネーションボリューム）にレプリケートされます。この関係を初期化すると、ONTAP はソースボリュームで参照されるデータブロックをデスティネーションボリュームに転送します。



SnapCenter は、SnapMirror ボリュームと SnapVault ボリュームのカスケード関係をサポートしていません（\*プライマリ\*>\*ミラー\*>\*バックアップ\*）。ファンアウト関係を使用する必要があります。

SnapCenter では、バージョンに依存しない SnapMirror 関係の管理がサポートされます。バージョンに依存しない SnapMirror 関係の詳細およびその設定方法については、を参照してください ["ONTAP のドキュメント"](#)。

## IBM DB2のバックアップ戦略

### IBM DB2のバックアップ戦略の定義

バックアップジョブを作成する前にバックアップ戦略を定義しておく、リソースの正常なリストアやクローニングに必要なバックアップを作成するのに役立ちます。バックアップ戦略の大部分は、サービスレベルアグリーメント（SLA）、目標復旧時間（RTO）、および目標復旧時点（RPO）によって決まります。

このタスクについて

SLA では、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処するために必要なサービスレベルを定義します。RTO は、サービスの停止からビジネスプロセスの復旧までに必要となる時間です。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA、RTO、および RPO は、データ保護戦略に関与します。

手順

1. リソースをバックアップするタイミングを決定します。
2. 必要なバックアップジョブの数を決定します。
3. バックアップの命名方法を決定します。
4. アプリケーションと整合性のあるデータベースの Snapshot をバックアップする Snapshot コピーベースのポリシーを作成するかどうかを決定します。
5. レプリケーションのために NetApp SnapMirror テクノロジを使用するか、または長期保持のために NetApp SnapVault テクノロジを使用するかを決定します。
6. ソースストレージシステムと SnapMirror デスティネーションでの Snapshot の保持期間を決定します。
7. バックアップ処理の前後にコマンドを実行するかどうかを決定し、実行する場合はプリスクリプトまたはポストスクリプトを用意します。

### Linux ホスト上のリソースの自動検出

リソースとは、SnapCenterによって管理されるLinuxホスト上のIBM DB2データベース



とインスタンスです。SnapCenter Plug-in for IBM DB2プラグインをインストールすると、そのLinuxホスト上のすべてのインスタンスのIBM DB2データベースが自動的に検出され、[Resources]ページに表示されます。

サポートされるバックアップのタイプ

Backup typeには、作成するバックアップのタイプを指定します。SnapCenterでは、IBM DB2データベースに対してSnapshotコピーベースのバックアップタイプがサポートされます。

**Snapshot** コピーベースのバックアップ

Snapshotコピーベースのバックアップでは、NetApp Snapshotテクノロジーを利用して、IBM DB2データベースが格納されているボリュームのオンラインの読み取り専用コピーを作成します。

**SnapCenter Plug-in for IBM DB2**での整合グループ**Snapshot**の使用方法

プラグインを使用して、リソースグループの整合性グループのSnapshotを作成できます。整合グループはコンテナであり、複数のボリュームを格納して1つのエンティティとして管理できます。整合グループは、複数のボリュームの同時Snapshotであり、ボリュームグループの整合性のあるコピーを提供します。

ストレージコントローラが整合性のあるSnapshotをグループ化するまでの待機時間を指定することもできます。使用可能な待機時間のオプションは、\* Urgent \*、\* Medium \*、\* Relaxed \* です。また、整合グループSnapshotの処理中にWrite Anywhere File Layout (WAFL) の同期を有効または無効にすることもできます。WAFLの同期により、整合性グループSnapshotのパフォーマンスが向上します。

**SnapCenter**による不要なデータバックアップの削除の管理方法

SnapCenterは、ストレージシステムレベルおよびファイルシステムレベルでの不要なデータバックアップの削除を管理します。

保持設定に基づいて、プライマリストレージまたはセカンダリストレージ上のSnapshotと、IBM DB2カタログ内の対応するエントリが削除されます。

**IBM DB2**のバックアップスケジュールを決定する際の考慮事項

バックアップのスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率です。使用頻度の高いリソースは1時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは1日に1回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービスレベルアグリーメント (SLA)、目標復旧時点 (RPO) などがあります。

バックアップスケジュールには、次の2つの要素があります。

- バックアップ頻度 (バックアップを実行する間隔)

バックアップ頻度は、ポリシー設定の一部であり、一部のプラグインではスケジュールタイプとも呼ばれます。たとえば、毎時、毎日、毎週、または毎月としてバックアップ頻度を設定できます。

- バックアップスケジュール（バックアップが実行されるタイミング）

バックアップスケジュールは、リソースまたはリソースグループの設定の一部です。たとえば、リソースグループのポリシーで週に 1 回のバックアップが設定されている場合は、毎週木曜日の午後 10 時にバックアップが実行されるようにスケジュールを設定できます

## IBM DB2に必要なバックアップジョブの数

必要なバックアップジョブの数を左右する要因としては、リソースのサイズ、使用中のボリュームの数、リソースの変更率、サービスレベルアグリーメント（SLA）などがあります。

## Plug-in for IBM DB2 データヘエスノバックアップノメイメイキソク

Snapshotのデフォルトの命名規則を使用することも、カスタマイズした命名規則を使用することもできます。デフォルトのバックアップ命名規則では、Snapshot名にタイムスタンプが追加されるため、コピーがいつ作成されたかを確認できます。

Snapshotでは、次のデフォルトの命名規則が使用されます。

「resourcegroupname\_hostname\_timestamp」

バックアップリソースグループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- `_dts1_` は リソースグループ名です。
- `mach1x88` はホスト名です。
- `03-12-2015_23.17.26` は日付とタイムスタンプです。

または、\*[Use custom name format for Snapshot copy]\*を選択して、リソースまたはリソースグループを保護しながらSnapshot名の形式を指定することもできます。たとえば、`customtext_resourcegroup_policy_hostname` や `resourcegroup_hostname` などの形式です。デフォルトでは、タイムスタンプのサフィックスがSnapshot名に追加されます。

## IBM DB2のリストアおよびリカバリ戦略

### IBM DB2リソースのリストアおよびリカバリ戦略の定義

データベースのリストアとリカバリを行う前に戦略を定義しておくこと、リストア処理とリカバリ処理を正常に実行できるようになります。



データベースの手動リカバリのみがサポートされます。

## 手順

1. 手動で追加したIBM DB2リソースでサポートされるリストア戦略を確認する
2. 自動検出されたIBM DB2データベースでサポートされているリストア戦略を確認する

## 手動で追加した**IBM DB2**リソースでサポートされるリストア戦略のタイプ

SnapCenterを使用してリストア処理を正常に実行するには、戦略を定義する必要があります。手動で追加したIBM DB2リソースには、2種類のリストア戦略があります。



手動で追加したIBM DB2リソースはリカバリできません。

## リソース全体のリストア

- リソースのすべてのボリューム、qtree、およびLUNをリストアします



リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeでリストア対象として選択されたSnapshotのあとに作成されたSnapshotは削除され、リカバリできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。

## 自動検出された**IBM DB2**でサポートされるリストア戦略のタイプ

SnapCenterを使用してリストア処理を正常に実行するには、戦略を定義する必要があります。

完全リソースリストアは、自動的に検出されたIBM DB2データベースに対してサポートされるリストア戦略です。これにより、リソースのすべてのボリューム、qtree、およびLUNがリストアされます。

## 自動検出された**IBM DB2**のリストア処理のタイプ

SnapCenter Plug-in for IBM DB2は、自動検出されたIBM DB2データベースに対して、Single File SnapRestoreおよびConnect-and-Copyリストアタイプをサポートしています。

**NFS** 環境で単一ファイル **SnapRestore** を実行するシナリオを次に示します。

- [Complete Resource]オプションのみが選択されている場合
- バックアップを SnapMirror または SnapVault セカンダリの場所から選択し、\* Complete Resource \* オプションが選択されている場合

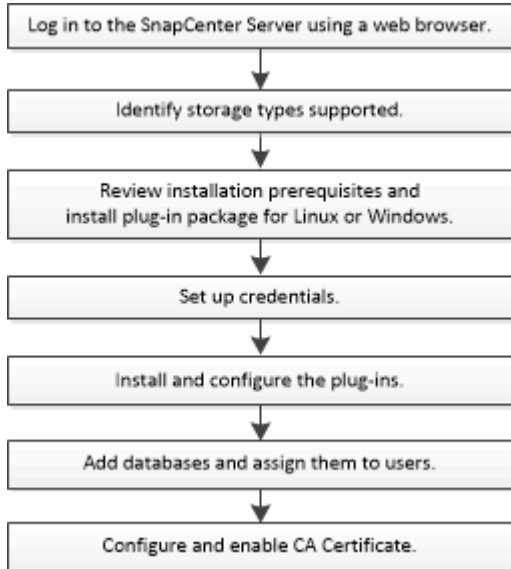
単一ファイル **SnapRestore** は、次のような状況で **SAN** 環境で実行されます。

- [Complete Resource]オプションのみが選択されている場合
- SnapMirror または SnapVault セカンダリストレージからバックアップを選択し、\* Complete Resource \* オプションを選択した場合

# SnapCenter Plug-in for IBM DB2のインストールの準備

## SnapCenter Plug-in for IBM DB2のインストールワークフロー

IBM DB2データベースを保護する場合は、SnapCenter Plug-in for IBM DB2をインストールしてセットアップする必要があります。



ホストを追加して**SnapCenter Plug-in for IBM DB2**をインストールするための前提条件

ホストを追加してプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。SnapCenter Plug-in for IBM DB2は、Windows環境とLinux環境の両方で使用できます。

- Java 11をホストにインストールしておく必要があります。



IBM Javaはサポートされていません。

- Windowsの場合、Plug-in CreatorサービスはWindowsユーザ「LocalSystem」を使用して実行する必要があります。これは、Plug-in for IBM DB2がドメイン管理者としてインストールされている場合のデフォルトの動作です。
- Windowsホストにプラグインをインストールするときに、組み込みでないクレデンシャルを指定した場合やユーザがローカルワークグループに属している場合は、ホストのUACを無効にする必要があります。SnapCenter Plug-in for Microsoft Windowsは、WindowsホストにIBM DB2プラグインを使用してデフォルトで導入されます。
- SnapCenterサーバがPlug-in for IBM DB2ホストの8145ポートまたはカスタムポートにアクセスできる必要があります。

### Windows ホスト

- ローカル管理者権限を持つドメインユーザがあり、リモートホストに対してローカルログイン権限が付与されている必要があります。

- Plug-in for IBM DB2をWindowsホストにインストールすると、SnapCenter Plug-in for Microsoft Windowsが自動的にインストールされます。
- root ユーザまたは root 以外のユーザ用にパスワードベースの SSH 接続を有効にしておく必要があります。
- Java 11をWindowsホストにインストールしておく必要があります。

"すべてのオペレーティングシステム用の Java のダウンロード"

"NetApp Interoperability Matrix Tool で確認できます"

## Linux ホスト

- root ユーザまたは root 以外のユーザ用にパスワードベースの SSH 接続を有効にしておく必要があります。
- Linuxホストに\* mksh \*ライブラリがインストールされている必要があります。
- Java 11をLinuxホストにインストールしておく必要があります。

"すべてのオペレーティングシステム用の Java のダウンロード"

"NetApp Interoperability Matrix Tool で確認できます"

- LinuxホストでIBM DB2データベースを実行している場合は、Plug-in for IBM DB2のインストール時にSnapCenter Plug-in for UNIXが自動的にインストールされます。
- プラグインのインストールには、デフォルトのシェルとして\* bash \*が必要です。

## 補助コマンド

SnapCenter Plug-in for IBM DB2で補助コマンドを実行するには、ファイルにそのコマンドを含める必要があります allowed\_commands.config。

allowed\_commands.config ファイルは、SnapCenter Plug-in for IBM DB2ディレクトリの「etc」サブディレクトリにあります。

## Windows ホスト

デフォルト： C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config

カスタムパス： <Custom\_Directory>\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config

## Linux ホスト

デフォルト： /opt/NetApp/snapcenter/scc/etc/allowed\_commands.config

カスタムパス： <custom\_Directory>/NetApp/snapcenter/scc/etc/allowed\_commands.config

プラグインホストで追加のコマンドを許可するには、allowed\_commands.config エディタ内のファイル。各コマンドを別々の行に入力します。大文字と小文字は区別されません。例：

コマンド:mount

コマンド：umount

完全修飾パス名を指定してください。パス名にスペースが含まれている場合は、パス名を引用符 (") で囲みます。例：

コマンド："C:\Program Files\NetApp\SnapCreator commands\sdcli.exe"

コマンド：myscript.bat

状況に応じて `allowed_commands.config` ファイルが存在しません。コマンドまたはスクリプトの実行はブロックされ、次のエラーでワークフローが失敗します。

"[/mnt/mount-a]の実行は許可されていません。プラグインホストのファイル%sにコマンドを追加して許可します。"

コマンドまたはスクリプトが `allowed_commands.config` をクリックすると、コマンドまたはスクリプトの実行がブロックされ、次のエラーでワークフローが失敗します。

"[/mnt/mount-a]の実行は許可されていません。プラグインホストのファイル%sにコマンドを追加して許可します。"



ワイルドカードエントリ (\*) を使用してすべてのコマンドを許可しないでください。

## Linux ホストの root 以外のユーザに sudo 権限を設定する

SnapCenter 2.0 以降のリリースでは、root 以外のユーザが SnapCenter Plug-ins Package for Linux をインストールしてプラグインプロセスを開始できます。プラグインプロセスは、有効なroot以外のユーザとして実行されます。いくつかのパスにアクセスできるように root 以外のユーザに sudo 権限を設定する必要があります。

- 必要なもの \*
- sudoバージョン1.8.7以降。
- root以外のユーザについては、root以外のユーザの名前とユーザのグループが同じであることを確認してください。
- `/etc/ssh/sshd_config_file` を編集して、メッセージ認証コードアルゴリズム MACs HMAC-sha2-256 および MACs HMAC-sha2-512 を設定します。

構成ファイルを更新したら、sshd サービスを再起動します。

例

```

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256

```

- このタスクについて \*

次のパスにアクセスできるように root 以外のユーザに sudo 権限を設定する必要があります。

- /home/linux\_user/.sc\_netapp / snapcenter\_linux\_host\_plugin.bin
- /custom\_location/NetApp/snapcenter /spl/installing/plugins/uninstall
- /custom\_location/NetApp/snapcenter /spl/bin/spl になります
- 手順 \*

1. SnapCenter Plug-ins Package for Linux をインストールする Linux ホストにログインします。
2. visudo Linux ユーティリティを使用して、 /etc/sudoers ファイルに次の行を追加します。

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl,
/opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



RACセットアップを実行している場合は、他の許可されているコマンドとともに、`/etc/sudoers`ファイルに次のように追加します。`'/RAC/bin/olsnodes'<crs_home>`

`_crs_home_file`の値は、`/etc/oracle/olr.loc_file`から取得できます。

`_linux_user_`は、作成したroot以外のユーザの名前です。

`_checksum_value_`は、次の場所にある`* sc_unix_plugins_checksum.txt *`ファイルから取得できます。


- `C : \ProgramData\NetApp\SnapCenter\Package Repository\SC_UNIX_plugins_checksum.txt` SnapCenter ServerがWindowsホストにインストールされている場合。
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` SnapCenterサーバーがLinuxホストにインストールされている場合。



この例は、独自のデータを作成するための参照としてのみ使用してください。

## SnapCenter Plug-ins Package for Windows をインストールするホストの要件

SnapCenter Plug-ins Package for Windows をインストールする前に、ホストシステムのいくつかの基本的なスペース要件とサイジング要件を確認しておく必要があります。


項目	要件
オペレーティングシステム	Microsoft Windows の場合  サポートされているバージョンの最新情報については、 <a href="#">を参照してください "NetApp Interoperability Matrix Tool で確認できます"</a> 。
ホスト上の SnapCenter プラグインの最小 RAM	1 GB
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	5 GB   十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。



項目	要件
必要なソフトウェアパッケージ	<ul style="list-style-type: none"> <li>• です。 ネットコア8.0.5</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle JavaおよびOpenJDK</li> </ul> <p>サポートされているバージョンの最新情報については、<a href="#">を参照してください "NetApp Interoperability Matrix Tool で確認できます"</a>。</p>

## SnapCenter Plug-ins Package for Linux をインストールするためのホストの要件

SnapCenter Plug-ins Package for Linux をインストールする前に、ホストシステムの基本的なスペースとサイジング要件を理解しておく必要があります。

項目	要件
オペレーティングシステム	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux の場合</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul> <p>サポートされているバージョンの最新情報については、<a href="#">を参照してください "NetApp Interoperability Matrix Tool で確認できます"</a>。</p>
ホスト上の SnapCenter プラグインの最小 RAM	1 GB
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	<p>2 GB</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;">  <p>十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。</p> </div>

項目	要件
必要なソフトウェアパッケージ	<p>Java 11 Oracle JavaおよびOpenJDK</p> <p>Java を最新バージョンにアップグレードした場合は、 /var/opt/snapcenter /etc/sp/etc/spl.properties にある JAVA_HOME オプションが正しい Java バージョンに設定されていること、および正しいパスが指定されていることを確認する必要があります。</p> <p>サポートされているバージョンの最新情報については、を参照してください "<a href="#">NetApp Interoperability Matrix Tool</a> で確認できます"。</p>

## SnapCenter Plug-in for IBM DB2のクレデンシャルを設定する

SnapCenter は、クレデンシャルを使用して SnapCenter 処理を実行するユーザを認証します。SnapCenter プラグインのインストールに必要なクレデンシャル、およびデータベースや Windows ファイルシステムでデータ保護処理を実行するための追加のクレデンシャルを作成する必要があります。

このタスクについて

- Linux ホスト

Linux ホストにプラグインをインストールするためのクレデンシャルを設定する必要があります。

プラグインプロセスをインストールして開始するための sudo 権限がある root ユーザまたは root 以外のユーザのクレデンシャルを設定する必要があります。

\* ベストプラクティス： \* ホストを導入してプラグインをインストールしたあとに Linux のクレデンシャルを作成することは可能ですが、SVM を追加したあとで、ホストを導入してプラグインをインストールする前にクレデンシャルを作成することを推奨します。

- Windows ホスト

プラグインのインストール前に Windows クレデンシャルをセットアップする必要があります。

リモートホストに対する管理者権限を含む、管理者権限でクレデンシャルを設定する必要があります。

個々のリソースグループのクレデンシャルを設定していて、ユーザ名にフル管理者権限がない場合は、少なくともリソースグループとバックアップ権限をユーザ名に割り当てる必要があります。

手順

1. 左側のナビゲーションペインで、\* 設定 \* をクリックします。
2. [ 設定 ] ページで、[\* 資格情報 ] をクリックします。
3. [ 新規作成 ( New ) ] をクリックする。
4. [Credential] ページで、クレデンシャルの設定に必要な情報を指定します。

フィールド	手順
クレデンシャル名	クレデンシャルの名前を入力します。
ユーザ名	<p>認証に使用するユーザ名とパスワードを入力します。</p> <ul style="list-style-type: none"> <li>ドメイン管理者または管理者グループの任意のメンバー</li> </ul> <p>ドメイン管理者、または SnapCenter プラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。Username フィールドの有効な形式は次のとおりです。</p> <ul style="list-style-type: none"> <li>NETBIOS_USERNAME_</li> <li>_ ドメイン FQDN\ ユーザ名 _</li> <li>ローカル管理者（ワークグループのみ）</li> </ul> <p>ワークグループに属するシステムの場合は、SnapCenter プラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザアカウントに昇格された権限がある場合、またはホストシステムでユーザアクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザアカウントを指定できます。Username フィールドの有効な形式は、<i>username</i> です</p> <p>パスワードに二重引用符 (") またはバックティック (`) を使用しないでください。小なり (&lt;) と感嘆符 (!) は使用しないでください。パスワードに記号を追加します。たとえば、lessthan &lt;! 10、lessthan10 &lt;!、backtick 12とします。</p>
パスワード	認証に使用するパスワードを入力します。
認証モード	使用する認証モードを選択します。
sudo 権限を使用する	<p>root 以外のユーザのクレデンシャルを作成する場合は、「* sudo 権限を使用する *」チェックボックスをオンにします。</p> <p> Linux ユーザのみに該当します。</p>

5. [OK] をクリックします。

クレデンシャルの設定が完了したら、[ ユーザとアクセス ( User and Access ) ] ページで、ユーザまたはユ

ーザグループにクレデンシャルのメンテナンスを割り当てることができます。

## Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、管理対象ドメインアカウントからサービスアカウントのパスワードを自動管理するグループ管理サービスアカウント (gMSA) を作成できます。

作業を開始する前に

- Windows Server 2016以降のドメインコントローラが必要です。
- ドメインのメンバーであるWindows Server 2016以降のホストが必要です。

手順

1. GMSA のオブジェクトごとに固有のパスワードを生成するには、KDS ルートキーを作成します。
2. ドメインごとに、Windows ドメインコントローラから次のコマンドを実行します。Add-KDSRootKey -EffectiveImmedient
3. GMSA を作成して構成します。
  - a. 次の形式でユーザグループアカウントを作成します。

```
domainName\accountName$  
.. グループにコンピュータオブジェクトを追加します。  
.. 作成したユーザグループを使用して gMSA を作成します。
```

例：

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 「 Get-ADServiceAccount  
」 コマンドを実行して、サービスアカウントを確認します。
```

4. ホストで gMSA を設定します。
  - a. gMSA アカウントを使用するホストで、Windows PowerShell 用の Active Directory モジュールを有効にします。

そのためには、PowerShell から次のコマンドを実行します。

```

PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                               Name                               Install State
-----
[ ] Active Directory Domain Services      AD-Domain-Services      Available

PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
-----
True      No                Success      {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.

```

- a. ホストを再起動します。
- b. PowerShell コマンド・プロンプトの「Install-AdServiceAccount <gMSA >」から次のコマンドを実行して 'ホストに gMSA をインストールします
- c. 次のコマンドを実行して 'gMSA アカウントを確認します 'Test-AdServiceAccount <gMSA >
5. ホスト上で設定されている gMSA に管理者権限を割り当てます。
6. SnapCenter サーバで設定済みの gMSA アカウントを指定して、Windows ホストを追加します。

SnapCenter サーバーは選択されたプラグインをホストにインストールし、指定された gMSA はプラグインのインストール時にサービスログオンアカウントとして使用されます。

## SnapCenter Plug-in for IBM DB2のインストール

ホストを追加し、プラグインパッケージをリモートホストにインストールする

ホストの追加ページを使用 SnapCenter してホストを追加し、プラグインパッケージをインストールする必要があります。プラグインは、自動的にリモートホストにインストールされます。ホストの追加とプラグインパッケージのインストールは、個々のホストまたはクラスタに対して実行できます。

作業を開始する前に

- SnapCenter ServerホストのオペレーティングシステムがWindows 2019で、プラグインホストのオペレーティングシステムがWindows 2022の場合は、次の手順を実行する必要があります。
  - Windows Server 2019 (OSビルド17763.5936) 以降にアップグレードする
  - Windows Server 2022 (OSビルド20348.2402) 以降にアップグレードする
- SnapCenter Admin ロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが必要です。

- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。
- メッセージキューサービスが実行されていることを確認してください。
- 管理マニュアルには、ホストの管理に関する情報が記載されています。
- Group Managed Service Account ( gMSA ; グループ管理サービスアカウント) を使用している場合は、管理者権限を持つ gMSA を設定する必要があります。

### "IBM DB2用のWindows Server 2016以降でのグループ管理サービスアカウントの設定"


このタスクについて

- SnapCenter サーバをプラグインホストとして別の SnapCenter サーバに追加することはできません。

手順

1. 左側のナビゲーションペインで、 \* Hosts \* (ホスト) をクリックします。
2. 上部で [Managed Hosts] タブが選択されていることを確認します。
3. [追加 (Add) ] をクリックします。
4. Hosts ページで、次の操作を実行します。

フィールド	手順
ホストタイプ	<p>ホストのタイプを選択します。</p> <ul style="list-style-type: none"> <li>• Windows の場合</li> <li>• Linux の場合</li> </ul> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Plug-in for IBM DB2はIBM DB2クライアントホストにインストールされます。このホストはWindowsシステムでもLinuxシステムでもかまいません。</p> </div>
ホスト名	<p>通信ホスト名を入力します。ホストの完全修飾ドメイン名 ( FQDN ) または IP アドレスを入力します。SnapCenter は、 DNS の適切な設定によって異なります。そのため、 FQDN を入力することを推奨します。</p>



フィールド	手順
クレデンシャル	<p>作成したクレデンシャル名を選択するか、新しいクレデンシャルを作成します。このクレデンシャルには、リモートホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。</p> <p>クレデンシャルの詳細を表示するには、指定したクレデンシャル名にカーソルを合わせます。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  クレデンシャル認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。 </div>

5. インストールするプラグインの選択セクションで、インストールするプラグインを選択します。

REST APIを使用してPlug-in for DB2をインストールする場合は、バージョンを3.0として渡す必要があります。例：DB2：3.0

6. (オプション) \* その他のオプション \* をクリックします。

フィールド	手順
ポート	<p>デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。デフォルトのポート番号は8145です。SnapCenter サーバがカスタムポートにインストールされている場合は、そのポート番号がデフォルトポートとして表示されます。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  プラグインを手動でインストールし、カスタムポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理は失敗します。 </div>
インストールパス	<p>Plug-in for IBM DB2はIBM DB2クライアントホストにインストールされます。このホストはWindowsシステムでもLinuxシステムでもかまいません。</p> <ul style="list-style-type: none"> <li>• Windows 用 SnapCenter Plug-ins パッケージのデフォルトパスは C : \Program Files\NetApp\SnapManager です。必要に応じて、パスをカスタマイズできます。</li> <li>• Linux 用 SnapCenter Plug-ins パッケージのデフォルトパスは /opt/NetApp/SnapCenter です。必要に応じて、パスをカスタマイズできます。</li> </ul>

フィールド	手順
インストール前のチェックをスキップします	プラグインを手動でインストール済みで、プラグインのインストール要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスを選択します。
プラグインサービスを実行するには、Group Managed Service Account (gMSA ; グループ管理サービスアカウント) を使用します	<p>Windows ホストの場合、プラグインサービスの実行にグループ管理サービスアカウント (gMSA) を使用する場合は、このチェックボックスをオンにします。</p> <div style="display: flex; flex-direction: column; gap: 10px;"> <div data-bbox="873 552 927 611">  <p data-bbox="987 533 1446 632">gMSA 名を domainName\accountName\$ の形式で指定します。</p> </div> <div data-bbox="873 730 927 789">  <p data-bbox="987 695 1446 825">gMSA は、SnapCenter Plug-in for Windows サービスのログオンサービスアカウントとしてのみ使用されません。</p> </div> </div>

7. [Submit (送信)] をクリックします。

[インストール前チェックをスキップ]チェックボックスを選択していない場合は、プラグインをインストールするための要件をホストが満たしているかどうかを検証するためにホストが検証されます。ディスクスペース、RAM、PowerShellのバージョン、NETバージョン、場所 (Windowsプラグインの場合)、およびJava 11 (WindowsプラグインとLinuxプラグインの場合) が最小要件に照らして検証されます。最小要件を満たしていない場合は、該当するエラーまたは警告メッセージが表示されます。

エラーがディスクスペースまたは RAM に関連している場合は、C : \Program Files\NetApp\SnapManager WebApp にある web.config ファイルを更新してデフォルト値を変更することができます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。



HA セットアップで web.config ファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. ホストタイプが Linux の場合は、フィンガープリントを確認し、\* Confirm and Submit \* をクリックします。

クラスタセットアップでは、クラスタ内の各ノードのフィンガープリントを検証する必要があります。



同じホストを以前に SnapCenter に追加し、フィンガープリントを確認した場合でも、フィンガープリントの検証は必須です。

9. インストールの進行状況を監視します。

- Windowsプラグインの場合、インストールログとアップグレードログは\_C : \Windows\SnapCenter <JOBID>\にありま。
- Linuxプラグインの場合、インストールログは\_/var/opt/snapcenter/logs/SnapCenter Linux\_Host\_Plugin\_Install\_Install\_Linux.log <JOBID>にあり、アップグレードログ



は/var/opt/snapcenter/logs/SnapCenter <JOBID>.logにあります。

完了後

SnapCenter 6.0バージョンにアップグレードする場合は、既存のPerlベースのPlug-in for DB2がリモートプラグインサーバからアンインストールされます。

コマンドレットを使用して、複数のリモートホストに **Linux** または **Windows** 用の **SnapCenter** プラグインパッケージをインストールします

Install-SmHostPackage PowerShell コマンドレットを使用すると、複数のホストに Linux または Windows 向け SnapCenter プラグインパッケージを同時にインストールできます。

作業を開始する前に

プラグインパッケージをインストールする各ホストで、ローカル管理者の権限を持つドメインユーザとして SnapCenter にログインしている必要があります。

手順

1. PowerShell を起動します。
2. SnapCenter サーバホストで、Open-SmConnection コマンドレットを使用してセッションを確立し、クレデンシャルを入力します。
3. Install-SmHostPackage コマンドレットと必要なパラメータを使用して、複数のホストにプラグインをインストールします。

コマンドレットで使用できるパラメータとその説明については、RUN\_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "[SnapCenter ソフトウェアコマンドレットリファレンスガイド](#)"。

プラグインを手動でインストールし、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、-skipprecheck オプションを使用できます。

4. リモートインストールのクレデンシャルを入力します。

コマンドラインインターフェイスを使用して、Linuxホストに**SnapCenter Plug-in for IBM DB2**をインストールする

SnapCenter Plug-in for IBM DB2 Databaseは、SnapCenterのユーザインターフェイス (UI) を使用してインストールする必要があります。ご使用の環境でSnapCenter UIからのプラグインのリモートインストールが許可されていない場合は、コマンドラインインターフェイス (CLI) を使用して、コンソールモードまたはサイレントモードでPlug-in for IBM DB2 Databaseをインストールできます。

作業を開始する前に

- Plug-in for IBM DB2 Databaseは、IBM DB2クライアントが配置されている各Linuxホストにインストールする必要があります。
- SnapCenter Plug-in for IBM DB2 DatabaseをインストールするLinuxホストは、依存するソフトウェア、データベース、およびオペレーティングシステムの要件を満たしている必要があります。

サポートされる構成の最新情報については、 Interoperability Matrix Tool (IMT) を参照してください。

["NetApp Interoperability Matrix Tool で確認できます"](#)

- SnapCenter Plug-in for IBM DB2 Databaseは、SnapCenter Plug-ins Package for Linuxに含まれています。SnapCenter Plug-ins Package for Linuxをインストールする前に、SnapCenterをWindowsホストにインストールしておく必要があります。

このタスクについて

パラメータが指定されていない場合、SnapCenterはデフォルト値でインストールされます。

手順

1. SnapCenter Plug-ins Package for Linuxのインストールファイル (snapcenter\_linux\_host\_plugin.bin) をC:\ProgramData\NetApp\SnapCenter\Package RepositoryからPlug-in for IBM DB2をインストールするホストにコピーします。

このパスには、SnapCenter サーバがインストールされているホストからアクセスできます。

2. コマンドプロンプトで、インストールファイルをコピーしたディレクトリに移動します。
3. プラグインをインストールします。 'path-to\_installation\_bin\_file/ snapcenter\_linux\_host\_plugin.bin -i silent -dport=port\_number\_for\_host-DSERVER\_IP=server\_name\_or\_IP\_address -DSERVER\_HTTPS\_port=port\_number\_for\_server

- -dport には、 SMCORE HTTPS 通信ポートを指定します。
- - DSERVER\_IP は、 SnapCenter サーバの IP アドレスを指定します。
- - DSERVER\_HTTPS\_PORT には、 SnapCenter サーバの HTTPS ポートを指定します。
- -duser\_install\_dir - SnapCenter Plug-ins Package for Linux をインストールするディレクトリを指定します
- DINSTALL\_LOG\_name は、 ログファイルの名前を指定します。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. /<installation directory>/NetApp/snapcenter/scc/etc/SC\_SMS\_Services.propertiesファイルを編集し、plugins\_enabled=DB2:3.0パラメータを追加します。
5. Add-Smhost コマンドレットと必要なパラメータを使用して、ホストを SnapCenter サーバに追加します。






コマンドで利用できるパラメータとその説明については、 RUNNING Get Help command\_name\_ を使用して参照できます。または、を参照することもできます ["SnapCenter ソフトウェアコマンドレットリファレンスガイド"](#)。

## Plug-in for IBM DB2のインストールステータスの監視

SnapCenter プラグインパッケージのインストールの進捗状況は、Jobs ページで監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題があるかどうかを確認できます。

このタスクについて

以下のアイコンがジョブページに表示され、操作の状態を示します。

-  実行中です
-  正常に完了しました
-  失敗しました
-  警告で終了したか、警告が原因で起動できませんでした
-  キューに登録され

手順

1. 左側のナビゲーションペインで、**Monitor** をクリックします。
2. [\* Monitor\*] ページで、[\* Jobs] をクリックします。
3. [ジョブ]ページで、プラグインのインストール処理のみが表示されるようにリストをフィルタリングするには、次の手順を実行します。
  - a. [\* フィルタ\* (Filter\*) ] をクリック
  - b. オプション：開始日と終了日を指定します。
  - c. タイプドロップダウンメニューから、\* プラグインインストール\* を選択します。
  - d. Status ドロップダウンメニューから、インストールステータスを選択します。
  - e. [適用 (Apply) ] をクリックします。
4. インストールジョブを選択し、[\* 詳細\*] をクリックしてジョブの詳細を表示します。
5. [\* ジョブの詳細\*] ページで、[\* ログの表示\*] をクリックします。

## CA 証明書を設定します

### CA 証明書 CSR ファイルを生成します

証明書署名要求 (CSR) を生成し、生成された CSR を使用して認証局 (CA) から取得できる証明書をインポートできます。証明書には秘密鍵が関連付けられます。

CSR はエンコードされたテキストブロックであり、認証された証明書ベンダーに提供されて署名済み CA 証明書を取得します。



CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSR の生成方法については、を参照してください ["CA 証明書 CSR ファイルの生成方法"](#)。



ドメイン（\*.domain.company.com）またはシステム（machine1.domain.company.com）の CA 証明書を所有している場合、CA 証明書 CSR ファイルの生成を省略できます。SnapCenter を使用して既存の CA 証明書を導入できます。

クラスタ構成の場合は、クラスタ名（仮想クラスタ FQDN）とそれぞれのホスト名を CA 証明書に記載する必要があります。証明書を更新するには、証明書を取得する前に Subject Alternative Name（SAN）フィールドに値を入力します。ワイルドカード証明書（\*.domain.company.com）の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

## CA 証明書をインポートする

Microsoft の管理コンソール（MMC）を使用して、SnapCenter サーバと Windows ホストプラグインに CA 証明書をインポートする必要があります。

### 手順

1. Microsoft 管理コンソール (MMC) に移動し、[\* ファイル\*]、[スナップインの追加と削除]の順にクリックします。
2. [スナップインの追加と削除] ウィンドウで、[Certificates] を選択し、[Add] をクリックします。
3. [証明書] スナップインウィンドウで、[Computer account] オプションを選択し、[完了\*] をクリックします。
4. [\* コンソールルート > 証明書-ローカルコンピュータ > 信頼されたルート証明機関 > 証明書\*] をクリックします。
5. [信頼されたルート証明機関] フォルダを右クリックし、[すべてのタスク > \*Import] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

ウィザードウィンドウ	実行する処理
秘密鍵をインポートします	オプション * はい * を選択し、秘密鍵をインポートして、* 次へ * をクリックします。
インポートファイル形式	変更せずに、* 次へ * をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、* Next * をクリックします。
証明書のインポートウィザードを完了しています	概要を確認し、[完了] をクリックしてインポートを開始します。



証明書のインポートは、秘密鍵にバンドルされている必要があります（サポートされている形式は、.pfx、.p12、および\*.p7b）。

7. 「Personal」フォルダについて、手順 5 を繰り返します。

## CA 証明書のサムプリントを取得します

証明書のサムプリントは、証明書を識別する 16 進数の文字列です。サムプリントは、サムプリントアルゴリズムを使用して証明書の内容から計算されます。

### 手順

1. GUI で次の手順を実行します。
  - a. 証明書をダブルクリックします。
  - b. [証明書] ダイアログボックスで、[\* 詳細 \*] タブをクリックします。
  - c. フィールドのリストをスクロールし、[Thumbprint] をクリックします。
  - d. ボックスから 16 進文字をコピーします。
  - e. 16 進数の間のスペースを削除します。

たとえば、サムプリントが「A9 09 50 2D d8 2a 14 33 e6 F8 38 86 b0 0d 42 77 A3 2a 7b」の場合、スペースを削除すると、「a909502dd82ae41433e6f83886b00d4277a32a7b」となります。

2. PowerShell で次の手順を実行します。
  - a. 次のコマンドを実行して、インストールされている証明書のサムプリントを一覧表示し、最近インストールされた証明書を件名で識別します。

```
Get-ChildItem - パス証明書 : \localmachine\My
```

- b. サムプリントをコピーします。

## Windows ホストプラグインサービスを使用して CA 証明書を設定する

CA 証明書に Windows ホストプラグインサービスを設定して、インストールされたデジタル証明書をアクティブ化する必要があります。

SnapCenter サーバおよび CA 証明書がすでに導入されているすべてのプラグインホストで、次の手順を実行します。

### 手順

1. 次のコマンドを実行して、SMCore のデフォルトポート 8145 にバインドされている既存の証明書を削除します。

```
>netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 次のコマンドを実行して、新しくインストールした証明書を Windows
ホストプラグインサービスにバインドします。
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

## Linuxホスト上のSnapCenter IBM DB2 Plug-insサービスのCA証明書の設定

カスタムプラグインキーストアとその証明書のパスワードの管理、CA証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-insの信頼ストアを使用したカスタムプラグインの信頼ストアへのCA署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

カスタムプラグインでは、ファイル「keystore.JKS」を使用します。このファイルは、信頼ストアおよびキーストアとして `_/opt/NetApp/snapcenter / scc /etc/both` にあります。

カスタムプラグインのキーストアのパスワード、および使用中のCA署名済みキーペアのエイリアスを管理します

手順

1. カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントのプロパティファイルから取得できます。

キー「keystore.pass」に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```

キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアに使用されているパスワードと同じパスワードに変更します。

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

`agent.properties` ファイル内のキー `keystore.pass` に対しても同じキーを更新します。

3. パスワードを変更したら、サービスを再起動してください。



カスタムプラグインキーストアのパスワード、および秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

ルート証明書または中間証明書をカスタムプラグインの信頼ストアに設定します

カスタムプラグインの信頼ストアの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

手順

1. カスタムプラグインキーストアを含むフォルダ（ /opt/NetApp/snapcenter / scc など）に移動します
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

```
keytool -list -v キーストア .jks
```

4. ルート証明書または中間証明書を追加します。

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動してください。



ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

**CA** 署名キーペアをカスタムプラグインの信頼ストアに設定します

CA 署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

手順

1. カスタムプラグインキーストア /opt/NetApp/snapcenter / scc などが含まれているフォルダに移動します
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

```
keytool -list -v キーストア .jks
```

4. 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。

```
keytool -importkeystore -srckeystore.root/ snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.JKS -deststoretype JKS `
```

5. キーストアに追加された証明書を表示します。

```
keytool -list -v キーストア .jks
```

6. キーストアに、キーストアに追加された新しい CA 証明書に対応するエイリアスが含まれていることを確認します。

7. CA 証明書用に追加された秘密鍵のパスワードをキーストアのパスワードに変更します。

デフォルトのカスタムプラグインキーストアパスワードは、agent.properties ファイル内のキー keystore.pass の値です。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

・ CA 証明書のエイリアス名が長く、スペースまたは特殊文字（「\*」、「」）が含まれている場合は、エイリアス名を単純な名前に変更します。

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

・ agent.properties ファイルの CA 証明書からエイリアス名を設定します。

この値をキー SCC\_CERTIFICATE\_ALIAS に更新します。

8. CA 署名済みキーペアをカスタムプラグインの信頼ストアに設定したら、サービスを再起動します。

**SnapCenter Custom Plug-ins** の証明書失効リスト（CRL）を設定します

このタスクについて

- ・ SnapCenter カスタムプラグインは、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- ・ SnapCenter カスタムプラグインの CRL ファイルのデフォルトディレクトリは、「/opt/netapp/snapcenter/sscc/etc/crl」です。

手順

1. agent.properties ファイルのデフォルトディレクトリを、キー crl\_path に対して変更および更新できません。

このディレクトリに複数の CRL ファイルを配置できます。着信証明書は各 CRL に対して検証されます。

**Windows**ホスト上の**SnapCenter IBM DB2 Plug-ins**サービス用の**CA**証明書の設定

カスタムプラグインキーストアとその証明書のパスワードの管理、CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名済みキーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

カスタムプラグインは、\_C : \Program Files\NetApp\SnapManager \Snapcenter Plug-in Creator\etc\_bothにある file\_keystore.JKS\_を 信頼ストアおよびキーストアとして使用します。

カスタムプラグインのキーストアのパスワード、および使用中の CA 署名済みキーペアのエイリアスを管理します

手順

1. カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントのプロパテ



ィファイルから取得できます。

key\_keystore.pass\_ に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.JKS
```



Windows のコマンドプロンプトで「keytool」コマンドが認識されない場合は、keytool コマンドを完全なパスに置き換えます。

```
C : \Program Files\Java\<JDK_version >\bin\keytool .exe "-storepasswd -keystore keystore.JKS
```

3. キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアに使用されているパスワードと同じパスワードに変更します。

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.JKS
```

agent.properties ファイル内のキー keystore.pass に対しても同じキーを更新します。

4. パスワードを変更したら、サービスを再起動してください。



カスタムプラグインキーストアのパスワード、および秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

ルート証明書または中間証明書をカスタムプラグインの信頼ストアに設定します

カスタムプラグインの信頼ストアの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

手順

1. カスタムプラグインの keystore\_C : \Program Files\NetApp\Virtual \SnapCenter \Snapcenter Plug-in Creator\etc\備えているフォルダに移動します
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

```
keytool -list -v キーストア .JKS
```

4. ルート証明書または中間証明書を追加します。

```
keytool -import-trustcacerts -alias myRootCA -file/root/USERTrustRSA_Root.cer -keystore keystore.JKS
```

5. カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動してください。



ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

CA 署名キーペアをカスタムプラグインの信頼ストアに設定します

CA 署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

## 手順

1. カスタムプラグインの keystore\_C : \Program Files\NetApp\Virtual \SnapCenter \Snapcenter Plug-in Creator\etc\備えているフォルダに移動します
2. file\_keystore.JKS\_</Z1> を探します。
3. キーストアに追加された証明書を表示します。

```
keytool -list -v キーストア .JKS
```

4. 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。

```
keytool -importkeystore -srckeystore.root/ snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.JKS -deststoretype JKS
```

5. キーストアに追加された証明書を表示します。

```
keytool -list -v キーストア .JKS
```

6. キーストアに、キーストアに追加された新しい CA 証明書に対応するエイリアスが含まれていることを確認します。
7. CA 証明書用に追加された秘密鍵のパスワードをキーストアのパスワードに変更します。

デフォルトのカスタムプラグインキーストアパスワードは、 agent.properties ファイル内のキー keystore.pass の値です。

```
keytool -keypasswd -alias "alias_name_in_ca_cert" -keystore keystore.JKS_
```

8. agent.properties ファイルの CA 証明書からエイリアス名を設定します。

この値をキー SCC\_CERTIFICATE\_ALIAS に更新します。

9. CA 署名済みキーペアをカスタムプラグインの信頼ストアに設定したら、サービスを再起動します。

## SnapCenter Custom Plug-ins の証明書失効リスト (CRL) を設定します

### このタスクについて

- 関連する CA 証明書の最新の CRL ファイルをダウンロードするには、を参照してください ["SnapCenter CA 証明書の証明書失効リストファイルを更新する方法"](#)。
- SnapCenter カスタムプラグインは、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter カスタムプラグインの CRL ファイルのデフォルトディレクトリは、 'C:\Program Files\NetApp\SnapCenter \Snapcenter Plug-in Creator\etc\crl' です。

## 手順

1. agent.properties ファイルのデフォルトディレクトリを、キー crl\_path に対して変更および更新できません。
2. このディレクトリに複数の CRL ファイルを配置できます。

着信証明書は各 CRL に対して検証されます。

プラグインの CA 証明書を有効にします

CA 証明書を設定し、SnapCenter サーバと対応するプラグインホストに CA 証明書を導入する必要があります。プラグインの CA 証明書検証を有効にする必要があります。

作業を開始する前に

- CA 証明書を有効または無効にするには、`run_Set-SmCertificateSetting_cmdlet` を使用します。
- このプラグインの証明書ステータスは、`Get-SmCertificateSettings` を使用して表示できます。





コマンドレットで使用できるパラメータとその説明については、`RUN_Get-Help` コマンド `NAME` を実行して参照できます。または、を参照することもできます "[SnapCenter ソフトウェアコマンドレットリファレンスガイド](#)"。

手順

1. 左側のナビゲーションペインで、\* Hosts \* (ホスト) をクリックします。
2. [Hosts] ページで、[\*Managed Hosts] をクリックします。
3. 1 つまたは複数のプラグインホストを選択します。
4. [\* その他のオプション \*] をクリックします。
5. [証明書の検証を有効にする] を選択します。

完了後

管理対象ホストタブのホストには鍵が表示され、SnapCenter サーバとプラグインホストの間の接続のステータスが南京錠の色で示されます。

-  は、CA 証明書が有効になっておらず、プラグインホストにも割り当てられていないことを示します。
-  CA 証明書が正常に検証されたことを示します。
-  は、CA 証明書を検証できなかったことを示します。
-  接続情報を取得できなかったことを示します。



ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

## データ保護を準備

### SnapCenter Plug-in for IBM DB2を使用するための前提条件

SnapCenter Plug-in for IBM DB2を使用する前に、SnapCenter管理者がSnapCenterサーバをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter サーバをインストールして設定します。
- SnapCenter サーバにログインします。
- 必要に応じて、ストレージシステム接続を追加し、クレデンシャルを作成して、SnapCenter 環境を設定します。

- LinuxホストまたはWindowsホストにJava 11をインストールします。

ホストマシンの環境パス変数に Java パスを設定する必要があります。

- バックアップレプリケーションが必要である場合は、SnapMirror と SnapVault をセットアップします。

## IBM DB2の保護におけるリソース、リソースグループ、ポリシーの使用方法

SnapCenter を使用する前に、実行するバックアップ、クローニング、およびリストアの処理に関連する基本的な概念を理解しておく役立ちます。ここでは、さまざまな処理で扱うリソース、リソースグループ、およびポリシーについて説明します。

- リソースとは、通常はSnapCenterでバックアップまたはクローニングするIBM DB2データベースです。
- SnapCenter リソースグループは、ホスト上のリソースの集まりです。

リソースグループに対して処理を実行すると、リソースグループに対して指定したスケジュールに従って、リソースグループに定義されているリソースに対して処理が実行されます。

単一のリソースまたはリソースグループをオンデマンドでバックアップすることができます。スケジュールされたバックアップを単一のリソースおよびリソースグループに対して実行することもできます。

- ポリシーは、バックアップ頻度、レプリケーション、スクリプト、およびデータ保護処理のその他の特性を指定するものです。

リソースグループを作成するときに、そのグループに対して 1 つ以上のポリシーを選択します。単一のリソースに対してオンデマンドでバックアップを実行するときにもポリシーを選択できます。

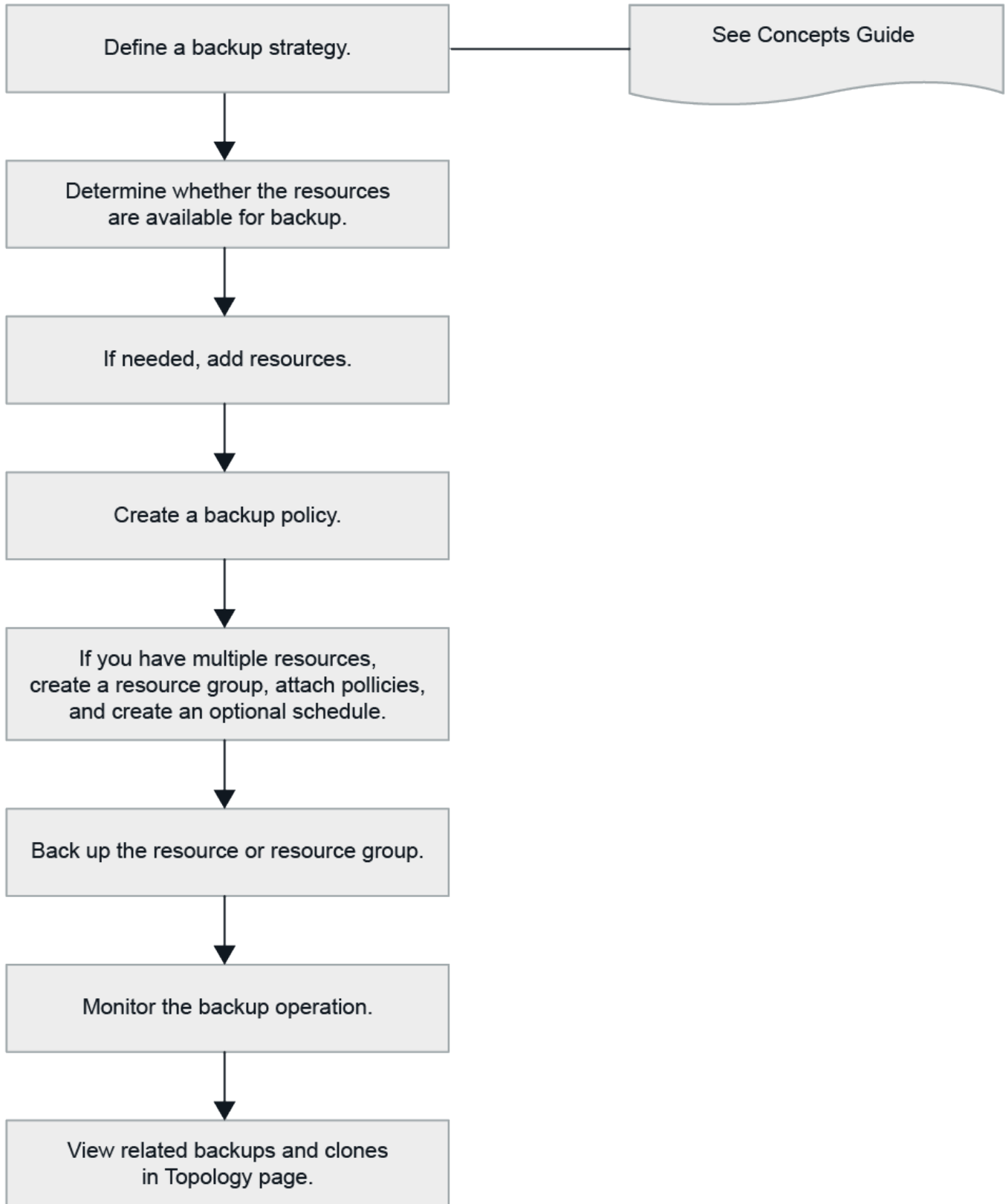
リソースグループは、保護対象となるものを定義するものであり、日と時間の観点から保護する必要がある場合に考えてみてください。ポリシーは、保護方法を定義するものと考えてください。たとえば、すべてのデータベースをバックアップする場合は、ホストのすべてのデータベースを含むリソースグループを作成します。リソースグループに、日次ポリシーと毎時ポリシーの 2 つのポリシーを適用します。リソースグループを作成してポリシーを適用する際に、フルバックアップを毎日実行するようにリソースグループを設定できます。

## IBM DB2リソースのバックアップ

### IBM DB2リソースのバックアップ

リソース（データベース）またはリソースグループのバックアップを作成することができます。バックアップのワークフローには、計画、バックアップするデータベースの特定、バックアップポリシーの管理、リソースグループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

次のワークフローは、バックアップ処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。 <https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html>["SnapCenter ソフトウェアコマンドレット リファレンスガイド"]です。

## データベースを自動的に検出します

リソースとは、SnapCenterで管理されるLinuxホスト上のIBM DB2データベースです。使用可能なIBM DB2データベースを検出したあとに、リソースをリソースグループに追加してデータ保護処理を実行できます。

作業を開始する前に


- SnapCenterサーバのインストール、ホストの追加、ストレージシステム接続のセットアップなどのタスクを完了しておく必要があります。
- SnapCenter Plug-in for IBM DB2では、RDM / VMDK仮想環境にあるリソースの自動検出はサポートされていません。データベースを手動で追加する際に、仮想環境のストレージの情報を指定する必要があります。


このタスクについて

- プラグインをインストールすると、そのLinuxホスト上のすべてのデータベースが自動的に検出されて[リソース]ページに表示されます。
- 自動検出されるのはデータベースだけです。

自動で検出されたリソースは変更または削除できません。

手順

1. 左側のナビゲーションペインで、\*[リソース]\*をクリックし、リストからPlug-in for IBM DB2を選択します。
2. [リソース]ページで、[表示]リストからリソースタイプを選択します。
3. (オプション) \* をクリックします  \* をクリックし、ホスト名を選択します。

次に、\* をクリックします  \* をクリックすると、フィルタペインが閉じます。

4. [\* リソースの更新 \*] をクリックして、ホストで使用可能なリソースを検出します。

リソースは、リソースタイプ、ホスト名、関連するリソースグループ、バックアップタイプ、ポリシー、全体的なステータスなどの情報とともに表示されます。

- データベースがネットアップストレージ上にあり、保護されていない場合は、総体的なステータス列に Not protected と表示されます。
- データベースがネットアップストレージシステム上にあり、保護されている場合に、バックアップ処理が実行されていないと、[全体のステータス]列に[バックアップが実行されていません]と表示されます。それ以外の場合は、前回のバックアップステータスに基づいて、「Backup failed」または「Backup succeeded」に変わります。



データベース名が SnapCenter 以外に変更された場合は、リソースを更新する必要があります。

## プラグインホストにリソースを手動で追加します

自動検出はWindowsホストではサポートされていません。DB2インスタンスとデータベースリソースは手動で追加する必要があります。

作業を開始する前に

- SnapCenterサーバのインストール、ホストの追加、ストレージシステム接続のセットアップなどのタスクを完了しておく必要があります。

このタスクについて

手動検出は、次の構成ではサポートされません。


- RDM と VMDK のレイアウト

手順

1. 左側のナビゲーションペインで\*[リソース]\*を選択し、ドロップダウンリストからSnapCenter Plug-in for IBM DB2を選択します。
2. [リソース]ページで、\*[IBM DB2リソースの追加]\*をクリックします。
3. [Provide Resource Details] ページで、次の操作を実行します。

フィールド	手順
名前	データベース名を指定します。
ホスト名	ホスト名を入力します。
を入力します	データベースまたはインスタンスを選択します。
インスタンス	データベースの親であるインスタンスの名前を指定します。
クレデンシャル	クレデンシャルを選択するか、クレデンシャルの情報を追加します。  これはオプションです。

4. [ストレージフットプリントの入力]ページで、ストレージタイプを選択して1つ以上のボリューム、LUN、およびqtreeを選択し、\*[保存]\*をクリックします。

オプション：「\*」をクリックします  \* アイコンをクリックして、他のストレージ・システムからボリューム、LUN、および qtree を追加します。

5. オプション：[Resource Settings]ページで、WindowsホストのリソースにIBM DB2プラグインのカスタムのキーと値のペアを入力します。
6. 概要を確認し、[完了]をクリックします。

データベースは、ホスト名、関連するリソースグループとポリシー、全体的なステータスなどの情報とともに表示されます。

リソースへのアクセスをユーザに許可する場合は、ユーザにリソースを割り当てる必要があります。これにより、ユーザは、自身に割り当てられたアセットに対して権限のある処理を実行できます。

"ユーザまたはグループを追加し、ロールとアセットを割り当てます"

データベースを追加したら、IBM DB2データベースの詳細を変更できます。

## IBM DB2のバックアップポリシーの作成

SnapCenterを使用してIBM DB2リソースをバックアップする前に、バックアップするリソースまたはリソースグループのバックアップポリシーを作成する必要があります。バックアップポリシーは、バックアップを管理、スケジュール、および保持する方法を規定する一連のルールです。

作業を開始する前に

- バックアップ戦略を定義しておく必要があります。

詳細については、IBM DB2データベースのデータ保護戦略の定義に関する情報を参照してください。

- SnapCenter のインストール、ホストの追加、ストレージシステム接続のセットアップ、リソースの追加などのタスクを実行して、データ保護の準備をしておく必要があります。
- Snapshotをミラーまたはバックアップにレプリケートする場合は、ソースボリュームとデスティネーションボリュームの両方に対応するSVMをSnapCenter管理者がユーザに割り当てておく必要があります。

また、ポリシーでレプリケーション、スクリプト、およびアプリケーションの設定を指定することもできます。これらのオプションを指定しておくことで、別のリソースグループにポリシーを再利用して時間を節約することができます。

このタスクについて

- SnapLock
  - [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。
  - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されなくなります。その結果、ポリシーで指定された数よりも多くのSnapshotが保持される可能性があります。
  - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。



プライマリSnapLock設定はSnapCenterバックアップポリシーで管理され、セカンダリSnapLock設定はONTAPで管理されます。

手順

1. 左側のナビゲーションペインで、\* 設定 \* をクリックします。
2. [設定] ページで、[\* ポリシー \*] をクリックします。
3. [新規作成 (New)] をクリックする。
4. [名前] ページで、ポリシー名と概要を入力します。
5. [Policy type] ページで、次の手順を実行します。
  - a. ストレージタイプを選択します。



- b. [\* カスタム・バックアップ設定\*] セクションで、キー値形式でプラグインに渡す必要がある特定のバックアップ設定を指定します。

プラグインに渡すキーと値の組み合わせを複数指定することができます。

6. [Snapshot] ページで、\* on demand、Hourly、Daily、Weekly、または Monthly \* を選択してスケジュールタイプを指定します。



リソースグループを作成する際に、バックアップ処理のスケジュール（開始日、終了日、頻度）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソースグループを作成できますが、各ポリシーに異なるバックアップスケジュールを割り当てることもできます。

**Schedule frequency**

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand

Hourly

Daily

Weekly

Monthly



午前 2 時にスケジュールを設定した場合、夏時間（DST）中はスケジュールはトリガーされません。

7. [Snapshot settings] セクションで、保持する Snapshot の数を指定します。

状況	作業
一定数の Snapshot を保持	<p>[保持するコピー数]* を選択し、保持する Snapshot の数を指定します。</p> <p>Snapshot の数が指定した数を超えると、最も古いコピーから順に Snapshot が削除されます。</p>



Snapshot コピーベースのバックアップで SnapVault レプリケーションを有効にする場合は、保持数を 2 以上に設定する必要があります。保持数を 1 に設定すると、新しい Snapshot がターゲットにレプリケートされるまで最初の Snapshot が SnapVault 関係の参照 Snapshot になるため、保持処理が失敗する可能性があります。

8. [Retention and backup] ページで、[Backup Type] ページで選択したバックアップタイプとスケジュールタイプの保持設定を指定します。
9. 概要を確認し、[完了] をクリックします。

## リソースグループを作成してポリシーを適用

リソースグループはコンテナであり、バックアップして保護するリソースをここに追加する必要があります。リソースグループを使用すると、特定のアプリケーションに関連付けられているすべてのデータを同時にバックアップできます。リソースグループはす


すべてのデータ保護ジョブに必要です。リソースグループに 1 つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義することも必要です。

このタスクについて

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[\* 新しいリソースグループ\*] をクリックします。
3. [名前] ページで、次の操作を実行します。

フィールド	手順
名前	リソースグループの名前を入力します。   リソースグループ名は 250 文字以内にする必要があります。
タグ	リソースグループを検索するときに役立つラベルを入力します。  たとえば、複数のリソースグループに HR をタグとして追加すると、あとから HR タグに関連付けられたすべてのリソースグループを検索できます。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの名前形式を入力します。  たとえば、customText_resource_group_policy_hostnameやresource_group_hostnameなどです。デフォルトでは、Snapshot名にタイムスタンプが追加されません。

4. Resources ページで、\* Host \* ドロップダウン・リストからホスト名を選択し、\* Resource Type \* ドロップダウン・リストからリソース・タイプを選択します。

これにより、画面上の情報をフィルタリングできます。

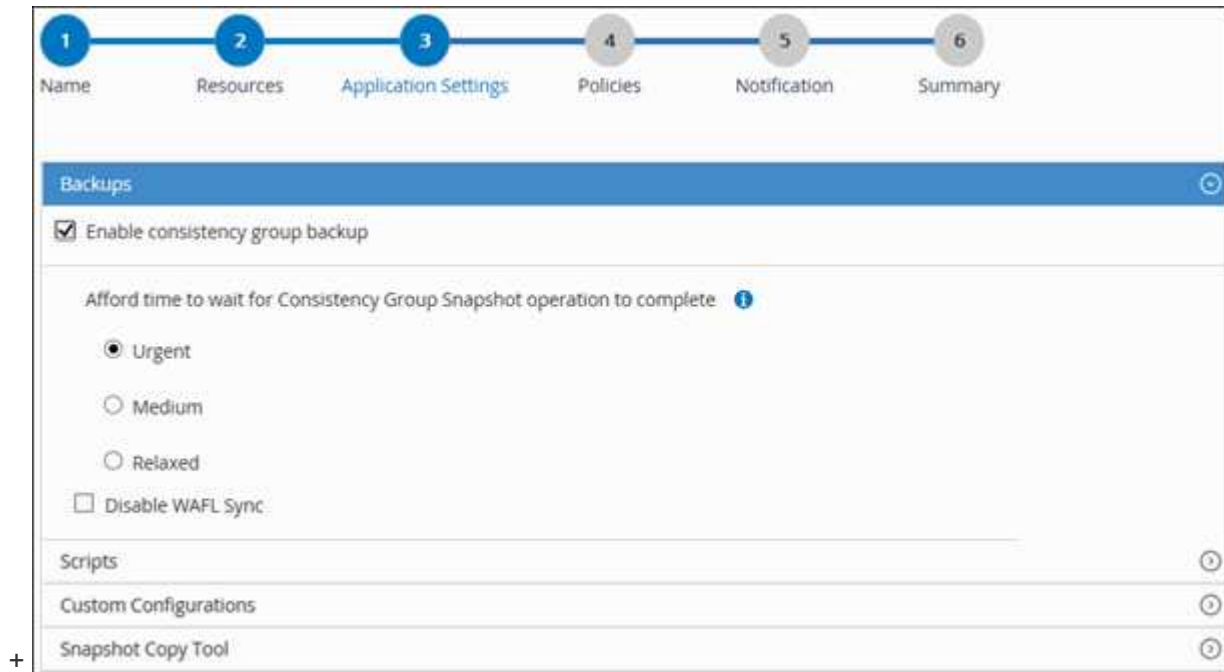
5. [使用可能なリソース ( Available Resources ) ] セクションからリソースを選択し、右矢印をクリックして [ 選択したリソース ( \* Selected Resources ) ] セクションに移動します。

6. [アプリケーションの設定] ページで、次の操作を行います。

- a. [\*Backups] の矢印をクリックして、追加のバックアップ・オプションを設定します。

整合グループのバックアップを有効にし、次の作業を実行します。

フィールド	手順
整合グループのSnapshot処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent、Medium、または Relaxed *を選択します。  Urgent = 5 秒、Medium = 7 秒、Relaxed = 20 秒。
WAFL 同期を無効にします	WAFL 整合ポイントを強制しない場合は、これを選択します。



- a. [Scripts]\*の矢印をクリックし、休止、Snapshot、および休止解除の処理を実行するプリコマンドとポストコマンドを入力します。障害発生時に終了する前に実行するPREコマンドを入力することもできます。
- b. [カスタム構成\*]の矢印をクリックし、このリソースを使用するすべてのデータ保護操作に必要なカスタムキーと値のペアを入力します。

パラメータ	設定	説明
archive_log_enable	(はい / いいえ)	アーカイブログ管理を有効にしてアーカイブログを削除できます。

パラメータ	設定	説明
archive_log_retention の略	日数	アーカイブログを保持する日数を指定します。  この設定は NTAP_SNAPSHOT_RETENTIONS 以上である必要があります。
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブログが格納されているディレクトリのパスを指定します。
archive_log_EXT	ファイル拡張子	アーカイブログファイルの拡張子の長さを指定します。  たとえば、アーカイブログが LOG_BACKUP_0_0_0_0.161518551942 9 で、ファイル拡張子の値が 5 の場合は、ログの拡張子に 5 桁が保持されます。これは 16151 です。
archive_log_recursive_SE arch	(はい / いいえ)	サブディレクトリ内のアーカイブログを管理できます。  アーカイブログがサブディレクトリにある場合は、このパラメータを使用してください。



カスタムのキーと値のペアは、IBM DB2 Linuxプラグインシステムでサポートされ、一元化されたWindowsプラグインとして登録されたIBM DB2データベースではサポートされません。


- c. Snapshotコピーツール\*の矢印をクリックして、スナップショットを作成するツールを選択します。

状況	作業
SnapCenterを使用してPlug-in for Windowsを使用し、スナップショットを作成する前にファイルシステムを整合性のある状態にします。Linuxリソースの場合、このオプションは適用されません。	ファイルシステムの整合性を維持した状態で SnapCenter を選択します。
SnapCenter：ストレージレベルのSnapshotを作成	ファイルシステムの整合性なしで SnapCenter * を選択します。
Snapshotコピーを作成するためにホストで実行するコマンドを入力します。	[その他]*を選択し、ホストで実行するSnapshotを作成するコマンドを入力します。


7. [Policies] ページで、次の手順を実行します。

a. ドロップダウンリストから 1 つ以上のポリシーを選択します。



また、\* をクリックしてポリシーを作成することもできます  \*

ポリシーは、Configure schedules for selected policies セクションに表示されます。

b. Configure Schedules (スケジュールの設定) 列で、\* をクリックします  \* をクリックします。

c. [Add schedules for policy\_name\_] ダイアログボックスで、スケジュールを設定し、[OK] をクリックします。

policy\_name は、選択したポリシーの名前です。

設定されたスケジュールは、[\* Applied Schedules] 列に表示されます。

サードパーティ製バックアップスケジュールが SnapCenter バックアップスケジュールと重複している場合、それらのバックアップスケジュールはサポートされません。

8. [通知] ページの [電子メールの設定 \*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および Eメールの件名を指定する必要があります。SMTP サーバーは、\* Settings \* > \* Global Settings \* で設定する必要があります。

9. 概要を確認し、[完了] をクリックします。

## IBM DB2のバックアップ

どのリソースグループにも含まれていないリソースは、このページからバックアップすることができます。

作業を開始する前に

- バックアップポリシーを作成しておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられた ONTAP ロールには「「SnapMirro all」権限を含める必要があります。ただし、「vsadmin」ロールを使用している場合、「SnapMirro all」権限は必要ありません。
- Snapshot コピーベースのバックアップ処理の場合は、すべてのテナントデータベースが有効でアクティブであることを確認してください。
- 休止、Snapshot、および休止解除の処理を実行するプリコマンドとポストコマンドの場合は、該当するコマンドがプラグインホストのコマンドリストで次のパスから使用できるかどうかを確認する必要があります。

Windowsの場合：C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config



Linuxの場合：/var/opt/snapcenter/scc/allowed\_commands.config



コマンドリストにコマンドがない場合、処理は失敗します。

#### 手順

1. 左側のナビゲーションペインで、\*[リソース]\*を選択し、リストから適切なプラグインを選択します。
2. リソースページで、リソースタイプに基づいて **View** ドロップダウンリストからリソースをフィルタリングします。

を選択します。  をクリックし、ホスト名とリソースタイプを選択してリソースをフィルタリングします。次に、  をクリックしてフィルタペインを閉じます。

3. バックアップするリソースを選択します。
4. [Resource]ページで、\*[Use custom name format for Snapshot copy]\*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。

たとえば、\_customText\_policy\_hostname\_or\_resource\_hostname\_hostname\_1 です。デフォルトでは、Snapshot名にタイムスタンプが追加されます。

5. [アプリケーションの設定] ページで、次の操作を行います。

- [Backups]\*矢印を選択して、追加のバックアップオプションを設定します。

必要に応じて、整合グループのバックアップを有効にし、次の作業を実行します。

フィールド	手順
整合グループ Snapshot 処理が完了するまで待機する時間を設定してください	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent、Medium、または Relaxed *を選択します。Urgent = 5 秒、Medium = 7 秒、Relaxed = 20 秒。
WAFL 同期を無効にします	WAFL 整合ポイントを強制しない場合は、これを選択します。

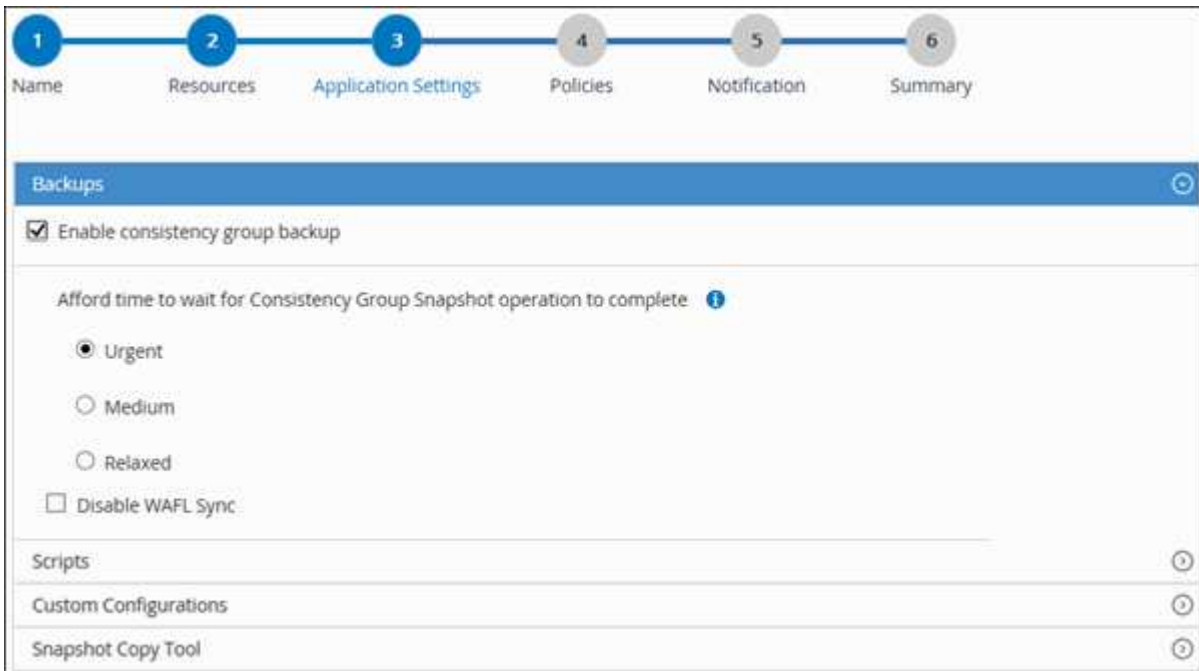
- [Scripts]\*の矢印を選択して、休止、Snapshot、および休止解除の処理のプリコマンドとポストコマンドを実行します。

バックアップ処理を終了する前にプリコマンドを実行することもできます。プリスクリプトとポストスクリプトは SnapCenter サーバで実行されます。

- **[Custom Configurations]**矢印を選択し、このリソースを使用するすべてのジョブに必要なカスタム値のペアを入力します。
- Snapshotコピーツール\*の矢印を選択して、Snapshotを作成するツールを選択します。

状況	作業
SnapCenter：ストレージレベルのSnapshotを作成	ファイルシステムの整合性なしで SnapCenter *を選択します。

状況	作業
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する	ファイルシステムの整合性を維持した状態でSnapCenter を選択します。
Snapshotを作成するコマンドを入力するには	[その他]*を選択し、コマンドを入力してSnapshotを作成します。




6. [Policies] ページで、次の手順を実行します。

a. ドロップダウンリストから 1 つ以上のポリシーを選択します。

 また、\* をクリックしてポリシーを作成することもできます  \*

[ 選択したポリシーのスケジュールを設定 ] セクションに、選択したポリシーが一覧表示されます。

b. を選択します  スケジュールを設定するポリシーの [ スケジュールの設定 ] 列。

c. [Add schedules for policy\_policy\_name\_] ダイアログボックスで、スケジュールを設定し、\*[OK]\* を選択します。

\_policy\_name\_ は、選択したポリシーの名前です。

設定されたスケジュールは、[ 適用されたスケジュール ] 列に一覧表示されます。

7. [通知] ページの [ 電子メールの設定 \* ] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および Eメールの件名を指定する必要があります。SMTP



は、 \* Settings \* > \* Global Settings \* でも設定する必要があります。

8. 概要を確認し、\*[終了]\*を選択します。

リソースのトポロジページが表示されます。

9. [今すぐバックアップ]\*を選択します。

10. Backup（バックアップ）ページで、次の手順を実行します。

a. リソースに複数のポリシーを適用した場合は、[\* Policy] ドロップダウン・リストから、バックアップに使用するポリシーを選択します。

オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されません。

b. 「 \* Backup \* 」を選択します。

11. 操作の進行状況を監視するには、 \* Monitor \* > \* Jobs \* をクリックします。

◦ MetroCluster 構成では、フェイルオーバー後に SnapCenter が保護関係を検出できない場合があります。

詳細については、を参照してください "[MetroCluster のフェイルオーバー後に SnapMirror 関係または SnapVault 関係を検出できません](#)"

## リソースグループをバックアップする

リソースグループは、ホスト上のリソースの集まりです。リソースグループのバックアップ処理は、リソースグループに定義されているすべてのリソースを対象に実行されます。

作業を開始する前に



- ポリシーを適用したリソースグループを作成しておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられた ONTAP ロールには「 'SnapMirro all' 」権限を含める必要があります。ただし、「 vsadmin 」ロールを使用している場合、「 'SnapMirro all' 」権限は必要ありません。

このタスクについて

リソースグループは、リソースページからオンデマンドでバックアップできます。リソースグループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが実行されます。

手順

1. 左側のナビゲーションペインで、\*[リソース]\*を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[\* 表示] リストから [\* リソースグループ\*] を選択します。

リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、 をクリックし、タグを選択します。次に、 をクリックしてフィルタペインを閉じます。

3. [Resource Groups] ページで、バックアップするリソースグループを選択し、\*[Back up Now]\*を選択しま



す。

4. Backup（バックアップ）ページで、次の手順を実行します。
  - a. 複数のポリシーをリソースグループに関連付けている場合は、「\* Policy \*」ドロップダウンリストから、バックアップに使用するポリシーを選択します。

オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されません。

- b. 「\* Backup \*」を選択します。

5. 処理の進捗状況を監視するために、[監視]>\*[ジョブ]\*を選択します。

## IBM DB2用のPowerShellコマンドレットを使用して、ストレージシステム接続とクレデンシアルを作成する

PowerShellコマンドレットを使用してIBM DB2データベースをバックアップ、リストア、またはクローニングするには、Storage Virtual Machine（SVM）接続とクレデンシアルを作成する必要があります。

作業を開始する前に

- PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。
- ストレージ接続を作成するには、Infrastructure Admin ロールに必要な権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

ホスト・プラグインのインストールは 'ストレージ・システム接続の追加中は実行しないでくださいホスト・キャッシュが更新されず' データベース・ステータスが SnapCenter GUI に表示される場合がありますこれは 'バックアップには使用できませんまたは NetApp ストレージには使用できません

- ストレージシステム名は一意である必要があります。

SnapCenter では、異なるクラスターに同じ名前のストレージシステムを複数配置することはサポートされていません。SnapCenter でサポートされるストレージシステムには、それぞれ一意の名前およびデータ LIF の IP アドレスを割り当てる必要があります。

手順

1. [SnapCenterPS]\*をクリックしてPowerShell Coreを起動します。
2. Add-SmStorageConnection コマンドレットを使用して、ストレージシステムへの新しい接続を作成します。

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap  
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Add-SmCredential コマンドレットを使用して新しいクレデンシアルを作成します。

次の例は、Windows クレデンシアルを使用して FinanceAdmin という名前の新しいクレデンシアルを作成する方法を示しています。

```
PS C:\> Add-SmCredential -Name 'FinanceAdmin' -Type Linux
-AuthenticationType PasswordBased -Credential db2hostuser
-EnableSudoPrivileges:$true
```

#### 4. IBM DB2通信ホストをSnapCenterサーバに追加します。

Linux の場合：

```
PS C:\> Add-SmHost -HostType Linux -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

Windows の場合：

```
PS C:\> Add-SmHost -HostType Windows -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

#### 5. パッケージとSnapCenter Plug-in for IBM DB2をホストにインストールします。

Linux の場合：

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
DB2
```

Windows の場合：

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
DB2,SCW
```

#### 6. SQLLIBへのパスを設定します。

Windowsの場合、DB2プラグインはSQLLIBフォルダのデフォルトパス「C:\Program Files\IBM\SQLLIB\bin」を使用します。

デフォルトのパスを上書きする場合は、次のコマンドを使用します。

```
PS C:\> Set-SmConfigSettings -Plugin -HostName '10.232.204.61'
-PluginCode DB2 -configSettings
@{"DB2_SQLLIB_CMD"="<<custom_path>\IBM\SQLLIB\BIN"}
```

コマンドレットで使用できるパラメータとその説明については、RUN\_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます ["SnapCenter ソフトウェアコマンドレットリファレンス](#)

ガイド"。

## PowerShell コマンドレットを使用してデータベースをバックアップします

データベースをバックアップするときは、SnapCenter サーバとの接続を確立してから、リソースの追加、ポリシーの追加、バックアップリソースグループの作成を行って、バックアップを実行します。

作業を開始する前に

- PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。
- ストレージシステム接続を追加し、クレデンシャルを作成しておく必要があります。

手順

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
PS C:\> Open-SmConnection
```

ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmResources コマンドレットを使用して、手動でリソースを追加します。

次に、IBM DB2 インスタンスを追加する例を示します。

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2  
-ResourceType Instance -ResourceName db2inst1 -StorageFootPrint  
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

DB2 データベースの場合：

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2  
-ResourceType Database -ResourceName SALESDB -StorageFootPrint  
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

3. Add-SmPolicy コマンドレットを使用してバックアップポリシーを作成します。
4. Add-SmResourceGroup コマンドレットを使用して、リソースを保護するか、新しいリソースグループを SnapCenter に追加します。
5. New-SmBackup コマンドレットを使用して、新しいバックアップジョブを開始する。

この例は、リソースグループをバックアップする方法を示しています。

```
C:\PS> New-SMBackup -ResourceGroupName  
'ResourceGroup_with_Db2_Resources' -Policy db2_policy1
```

次に、DB2インスタンスをバックアップする例を示します。

```
C:\PS> New-SMBackup -Resources  
@{"Host"="10.32.212.13";"Uid"="DB2INST1";"PluginName"="DB2"} -Policy  
db2_policy
```

次に、DB2データベースをバックアップする例を示します。

```
C:\PS> New-SMBackup -Resources  
@{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCDDB";"PluginName"="DB2"}  
-Policy db2_policy
```

6. Get-smJobSummaryReport コマンドレットを使用して、ジョブのステータス（実行中、完了、または失敗）を監視します。

```
PS C:\> Get-SmJobSummaryReport -JobId 467  
  
SmJobId           : 467  
JobCreatedDateTime :  
JobStartDateTime  : 27-Jun-24 01:40:09  
JobEndDateTime    : 27-Jun-24 01:41:15  
JobDuration       : 00:01:06.7013330  
JobName           : Backup of Resource Group  
'SCDB201WIN_RAVIR1_OPENLAB_NETAPP_LOCAL_DB2_DB2_WINCIR' with policy  
'snapshot-based-db2'  
JobDescription    :  
Status            : Completed  
IsScheduled       : False  
JobError          :  
JobType           : Backup  
PolicyName        : db2_policy  
JobResultData     :
```

7. Get-SmBackupReport コマンドレットを使用して、リストア処理やクローニング処理を実行するバックアップ ID とバックアップ名など、バックアップジョブの詳細を監視します。

```

PS C:\> Get-SmBackupReport -JobId 467

BackedUpObjects      : {WINCIR}
FailedObjects        : {}
IsScheduled           : False
HasMetadata           : False
SmBackupId           : 84
SmJobId              : 467
StartDateTime        : 27-Jun-24 01:40:09
EndDateTime          : 27-Jun-24 01:41:15
Duration              : 00:01:06.7013330
CreatedDateTime      : 27-Jun-24 18:39:45
Status                : Completed
ProtectionGroupName  : HOSTFQDN_DB2_DB2_WINCIR
SmProtectionGroupId  : 23
PolicyName           : db2_policy
SmPolicyId           : 13
BackupName           : HOSTFQDN _DB2_DB2_WINCIR_HOST_06-27-
2024_01.40.09.7397
VerificationStatus   : NotApplicable
VerificationStatuses :
SmJobError           :
BackupType           : SCC_BACKUP
CatalogingStatus     : NotApplicable
CatalogingStatuses  :
ReportDataCreatedDateTime :
PluginCode           : SCC
PluginName           : DB2
PluginDisplayName    : IBM DB2
JobTypeId            :
JobHost              : HOSTFQDN

```

コマンドレットで使用できるパラメータとその説明については、`RUN_Get-Help コマンド NAME` を実行して参照できます。または、を参照することもできます "[SnapCenter ソフトウェアコマンドレットリファレンスガイド](#)"。







## バックアップ処理を監視する

### IBM DB2バックアップ処理の監視


SnapCenterJobs ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

このタスクについて


以下のアイコンがジョブページに表示され、操作の対応する状態を示します。

-  実行中です
-  正常に完了しました
-  失敗しました
-  警告で終了したか、警告が原因で起動できませんでした
-  キューに登録され
-  キャンセルされました

手順

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [\* ジョブ \*] をクリックします。
3. Jobs (ジョブ) ページで、次の手順を実行します。
  - a. をクリックします  バックアップ処理だけが表示されるようにリストをフィルタリングします。
  - b. 開始日と終了日を指定します。
  - c. [\* タイプ] ドロップダウン・リストから、 [**\*Backup**] を選択します。
  - d. [**Status**](ステータス\*) ドロップダウンから、バックアップステータスを選択します。
  - e. [適用 (Apply)] をクリックして、正常に完了した操作を表示する。
4. バックアップジョブを選択し、 [\* 詳細 \*] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスがと表示されます  で、ジョブの詳細をクリックすると、バックアップ処理の子タスクの一部がまだ実行中であるか、警告の兆候がマークされていることがわかります。

5. [ジョブの詳細] ページで、 [\* ログの表示 \*] をクリックします。


**View logs** ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[**Activity**]ペインで、**IBM DB2**データベースに対するデータ保護処理を監視します。

[**アクティビティ (Activity)**] パネルには、最近実行された 5 つの操作が表示されまた、操作が開始された日時と操作のステータスも表示されます。

[**Activity (アクティビティ)**] ペインには、バックアップ、リストア、クローン、およびスケジュールされたバックアップ処理に関する情報が表示されます。

手順


1. 左側のナビゲーションペインで、 \* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. をクリックします  をクリックして、最近の 5 つの操作を表示します。

いずれかの処理をクリックすると、\*[ジョブの詳細]\*ページに処理の詳細が表示されます。

## IBM DB2のバックアップ処理をキャンセルする

キューに登録されているバックアップ処理をキャンセルできます。

- 必要なもの \*
  - 処理をキャンセルするには、 SnapCenter 管理者またはジョブ所有者としてログインする必要があります。
  - バックアップ操作は、 **Monitor** ページまたは **Activity** ペインからキャンセルできます。
  - 実行中のバックアップ処理をキャンセルすることはできません。
  - SnapCenter GUI、 PowerShell コマンドレット、 または CLI コマンドを使用して、バックアップ処理をキャンセルできます。
  - キャンセルできない操作に対しては、 [ジョブのキャンセル] ボタンが無効になっています。
  - ロールの作成中に 'このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できるようにする \* を選択した場合は 'そのロールを使用している間に '他のメンバーのキューに入っているバックアップ操作をキャンセルできます
  - 手順 \*
1. 次のいずれかを実行します。

方法	アクション
監視ページ	<ol style="list-style-type: none"><li>a. 左側のナビゲーションペインで、 * Monitor * &gt; * Jobs * をクリックします。</li><li>b. 操作を選択し、 * ジョブのキャンセル * をクリックします。</li></ol>
アクティビティペイン	<ol style="list-style-type: none"><li>a. バックアップ処理を開始したら、 * をクリックします  * [アクティビティ] パネルには、最近の 5 つの操作が表示されます。</li><li>b. 処理を選択します。</li><li>c. [ジョブの詳細] ページで、 [* ジョブのキャンセル *] をクリックします。</li></ol>




処理がキャンセルされ、リソースが以前の状態に戻ります。

### [Topology]ページでのIBM DB2のバックアップとクローンの表示

リソースのバックアップまたはクローニングを準備する際に、プライマリストレージとセカンダリストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。

このタスクについて

[コピーの管理]ビューの次のアイコンを確認して、プライマリストレージまたはセカンダリストレージ（ミラーコピーまたはバックアップコピー）でバックアップとクローンが使用可能かどうかを判断できます。

- 
 には、プライマリストレージ上にあるバックアップとクローンの数が表示されます。
- 
 には、SnapMirror テクノロジーを使用してセカンダリストレージにミラーリングされたバックアップとクローンの数が表示されます。
- 
 には、SnapVault テクノロジーを使用してセカンダリストレージにレプリケートされたバックアップとクローンの数が表示されます。



表示されるバックアップの数には、セカンダリストレージから削除されたバックアップも含まれます。たとえば、4つのバックアップだけを保持するポリシーを使用して6つのバックアップを作成した場合、バックアップの数は6と表示されます。



mirror-vault タイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップの数にはバージョンに依存しないバックアップは含まれません。

トポロジページでは、選択したリソースまたはリソースグループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を確認し、対象を選択してデータ保護処理を実行できます。

#### 手順

1. 左側のナビゲーションペインで、\*リソース\* をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[\*表示\*] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リソースの詳細ビューまたはリソースグループの詳細ビューでリソースを選択します。

リソースが保護されている場合は、選択したリソースのトポロジページが表示されます。

4. サマリー・カード\*を確認して、プライマリ・ストレージとセカンダリ・ストレージで使用可能なバックアップとクローンの数を確認します。

[サマリカード]セクションには、Snapshotコピーベースのバックアップとクローンの総数が表示されます。

「\*Refresh\*」ボタンをクリックすると、ストレージの照会が開始され、正確な数が表示されます。

SnapLockが有効なバックアップが作成された場合、\*[Refresh]\*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでは、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限がONTAPから取得されます。

オンデマンドバックアップのあと、\*[リフレッシュ]\*ボタンをクリックすると、バックアップまたはクロー



ンの詳細がリフレッシュされます。



5. [コピーの管理]ビューで、プライマリストレージまたはセカンダリストレージから \* バックアップ \* または \* クローン \* をクリックして、バックアップまたはクローンの詳細を表示します。

バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、削除の各処理を実行します。



セカンダリストレージ上のバックアップは、名前変更または削除できません。

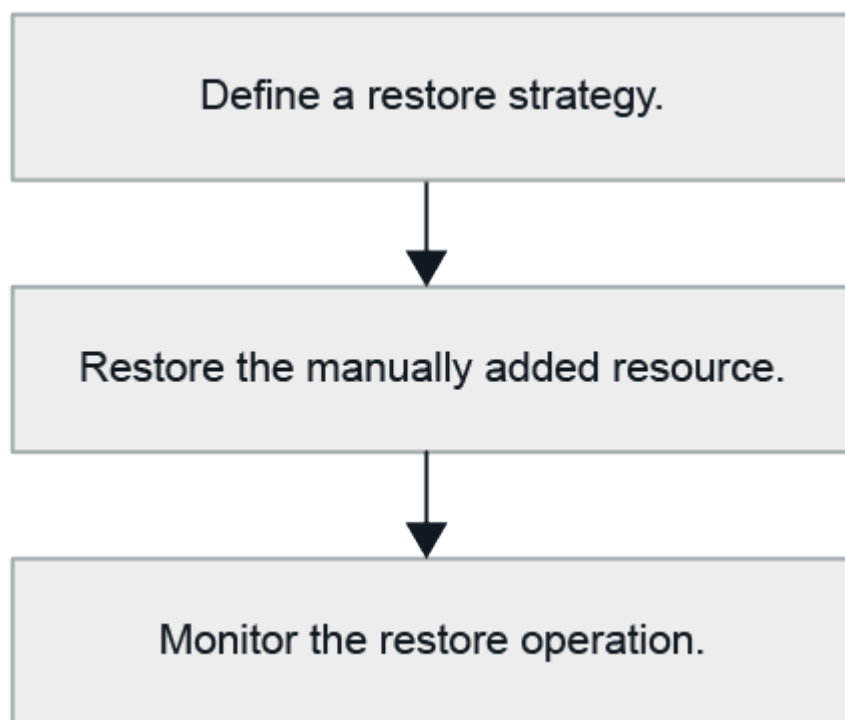
7. クローンを削除する場合は、表でクローンを選択し、をクリックします 。
8. クローンをスプリットする場合は、表でクローンを選択し、をクリックします .

## IBM DB2のリストア

### リストアワークフロー

リストアとリカバリのワークフローには、計画、リストア処理の実行、および処理の監視が含まれます。

次のワークフローは、リストア処理の実行順序を示しています。



PowerShell コマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShell コマンドレットの詳細については、SnapCenter のコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

"SnapCenter ソフトウェアコマンドレットリファレンスガイド"です。

## 手動で追加したリソースバックアップのリストア

SnapCenter を使用して、1 つ以上のバックアップからデータをリストアおよびリカバリできます。

作業を開始する前に

- リソースまたはリソースグループをバックアップしておく必要があります。
- リストアするリソースまたはリソースグループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- リストア前、リストア後、マウント、アンマウントの各コマンドについて、プラグインホストのコマンドリストに以下のパスからコマンドが含まれていないか確認してください。

Windowsの場合：`C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

Linuxの場合：`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドリストにコマンドがない場合、処理は失敗します。

このタスクについて

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソースタイプに基づいて、**View** ドロップダウンリストからリソースをフィルタリングします。

リソースは、タイプ、ホスト、関連付けられているリソースグループとポリシー、およびステータスとともに表示されます。




リストアの実行時は、バックアップがリストアグループのものであっても、リストア対象のリソースを個別に選択する必要があります。

リソースが保護されていない場合は '保護されていない' というメッセージが [全体のステータス] 列に表示されます。これは、リソースが保護されていないこと、またはリソースが別のユーザによってバックアップされていることを意味します。

3. リソースを選択するか、リソースグループを選択してそのグループ内のリソースを選択します。

リソースのトポロジページが表示されます。

4. Manage Copies (コピーの管理) ビューから、プライマリまたはセカンダリ (ミラーまたはバックアップ) ストレージシステムから \* Backups (バックアップ) を選択します。

5. [プライマリ・バックアップ]テーブルで、リストア元のバックアップを選択し、[\*]をクリックします  \*

Primary Backup(s)	
Backup Name	End Date
rg1_scspr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. [Restore Scope]ページで、\*[Complete Resource]\*を選択します。
- a. [Complete Resource]\*を選択すると、IBM DB2データベースの設定済みデータボリュームがすべてリストアされます。

リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeでリストア対象として選択されたSnapshotのあとに作成されたSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたは qtree で他のリソースがホストされている場合、そのリソースも削除されます。

LUN は複数選択できます。



「\* all \*」を選択すると、ボリューム、 qtree 、または LUN 上のすべてのファイルがリストアされます。

7. [リストア前]ページで、リストア・ジョブを実行する前に実行するプリ・リストアおよびアンマウント・コマンドを入力します。
8. [ポスト・オペレーション]ページで、マウントおよびリストア後のコマンドを入力して、リストア・ジョブの実行後に実行します。



休止、Snapshot、および休止解除の処理を実行するプリコマンドとポストコマンドの場合は、Linuxの場合は `/opt/snapcenter/snapcenter/scc/allowed_commands.config_path`、Windowsの場合は `_C : \Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config_` からプラグインホストで使用できるコマンドリストにコマンドが存在するかどうかを確認する必要があります。

9. [通知]ページの [電子メールの設定\*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレスと Eメールの件名を指定する必要があります。また、[\* 設定\* (Settings\*) ]>[\* グローバル設定\* (\* Global Settings\*) ]ページでも SMTP を設定する必要があります。

10. 概要を確認し、[完了]をクリックします。
11. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

完了後

ロールフォワードステータスが「DB PENDING」の場合にのみリカバリが可能です。このステータスは、アーカイブログが有効なDB2データベースに適用されます。

## 自動検出されたデータベースバックアップをリストアおよびリカバリする

SnapCenter を使用して、1 つ以上のバックアップからデータをリストアおよびリカバリできます。

作業を開始する前に

- リソースまたはリソースグループをバックアップしておく必要があります。
- リストアするリソースまたはリソースグループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- リストア前、リストア後、マウント、アンマウントの各コマンドについて、プラグインホストのコマンドリストに以下のパスからコマンドが含まれていないか確認してください。

Windowsの場合：`C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

Linuxの場合：`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドリストにコマンドがない場合、処理は失敗します。

このタスクについて

- 自動検出されたリソースについては、SFSSRでリストアがサポートされます。
- 自動リカバリはサポートされていません。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソースタイプに基づいて、**View**] ドロップダウンリストからリソースをフィルタリングします。

リソースは、タイプ、ホスト、関連付けられているリソースグループとポリシー、およびステータスとともに表示されます。



リストアの実行時は、バックアップがリストアグループのものであっても、リストア対象のリソースを個別に選択する必要があります。


リソースが保護されていない場合は '保護されていない' というメッセージが [全体のステータス] 列に表示されます。これは、リソースが保護されていないこと、またはリソースが別のユーザによってバックアップされていることを意味します。

3. リソースを選択するか、リソースグループを選択してそのグループ内のリソースを選択します。

リソースのトポロジページが表示されます。

4. Manage Copies (コピーの管理) ビューから、プライマリまたはセカンダリ (ミラーまたはバックアップ

) ストレージシステムから \* Backups (バックアップ) を選択します。

5. [プライマリ・バックアップ] テーブルで、リストア元のバックアップを選択し、[\*] をクリックします  \*



Backup Name	End Date
rg1_scopr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. [Restore Scope] ページで \*[Complete Resource]\* を選択し、IBM DB2 データベースの設定済みデータボリュームをリストアします。
7. [リストア前] ページで、リストア・ジョブを実行する前に実行するプリ・リストアおよびアンマウント・コマンドを入力します。

自動検出されたリソースにはアンマウントコマンドは必要ありません。

8. [ポスト・オペレーション] ページで、マウントおよびリストア後のコマンドを入力して、リストア・ジョブの実行後に実行します。

自動検出されたリソースにはマウントコマンドは必要ありません。



休止、Snapshot、および休止解除の処理を実行するプリコマンドとポストコマンドの場合は、Linux の場合は `/opt/snapcenter/snapcenter/scc/allowed_commands.config_path`、Windows の場合は `_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config_` からプラグインホストで使用できるコマンドリストにコマンドが存在するかどうかを確認する必要があります。

9. [通知] ページの [電子メールの設定 \*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレスと Eメールの件名を指定する必要があります。また、[\* 設定 \* (Settings \*) ] > [\* グローバル設定 \* (\* Global Settings \*) ] ページでも SMTP を設定する必要があります。

10. 概要を確認し、[完了] をクリックします。
11. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

完了後

ロールフォワードステータスが「DB PENDING」の場合にのみリカバリが可能です。このステータスは、アーカイブログが有効な DB2 データベースに適用されます。

## PowerShell コマンドレットを使用した IBM DB2 データベースのリストア

IBM DB2 バックアップをリストアするには、SnapCenter サーバとの接続セッションを開始し、バックアップをリスト表示してバックアップ情報を取得し、バックアップをリストアします。

作業を開始する前に

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

手順

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
PS C:\> Open-SmConnection
```

2. Get-SmBackup コマンドレットと Get-SmBackupReport コマンドレットを使用して、リストアするバックアップを特定します。

この例では、リストアできるバックアップが2つあります。

```
PS C:\> Get-SmBackup -AppObjectId
cn24.sscore.test.com\DB2\db2inst1\Library

      BackupId      BackupName      BackupTime
-----
BackupType
-----
      1      Payroll Dataset_vise-f6_08... 8/4/2015 11:02:32 AM
Full Backup
      2      Payroll Dataset_vise-f6_08... 8/4/2015 11:23:17 AM
```

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId          : 113
  SmJobId            : 2032
  StartDateTime      : 2/2/2015 6:57:03 AM
  EndDateTime        : 2/2/2015 6:57:11 AM
  Duration           : 00:00:07.3060000
  CreatedDateTime    : 2/2/2015 6:57:23 AM
  Status             : Completed
  ProtectionGroupName : Clone
  SmProtectionGroupId : 34
  PolicyName         : Vault
  SmPolicyId         : 18
  BackupName         : Clone_SCSPR0019366001_02-02-2015_06.57.08
  VerificationStatus : NotVerified

SmBackupId          : 114
  SmJobId            : 2183
  StartDateTime      : 2/2/2015 1:02:41 PM
  EndDateTime        : 2/2/2015 1:02:38 PM
  Duration           : -00:00:03.2300000
  CreatedDateTime    : 2/2/2015 1:02:53 PM
  Status             : Completed
  ProtectionGroupName : Clone
  SmProtectionGroupId : 34
  PolicyName         : Vault
  SmPolicyId         : 18
  BackupName         : Clone_SCSPR0019366001_02-02-2015_13.02.45
  VerificationStatus : NotVerified
```

### 3. Restore-SmBackup コマンドレットを使用して、バックアップからデータをリストアします。



AppObjectIdは「Host\Plugin\UID」です。UID =<instance\_name>は手動で検出されたインスタンスリソースの場合、UID =<instance\_name>\<database\_name>はIBM DB2データベースリソースの場合です。ResourceIDは、Get-smResourcesコマンドレットで取得できません。

```
Get-smResources -HostName cn24.sscore.test.com -PluginCode DB2
```

この例は、プライマリストレージからデータベースをリストアする方法を示しています。

```
Restore-SmBackup -PluginCode DB2 -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 3
```

この例は、セカンダリストレージからデータベースをリストアする方法を示しています。

```
Restore-SmBackup -PluginCode 'DB2' -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false  
-Archive @( @{"Primary"="<Primary  
Vserver>:<PrimaryVolume>";"Secondary"="<Secondary  
Vserver>:<SecondaryVolume>"}))
```

コマンドレットで使用できるパラメータとその説明については、`RUN_Get-Help コマンド NAME` を実行して参照できます。または、を参照することもできます "[SnapCenter ソフトウェアコマンドレットリファレンスガイド](#)"。







## IBM DB2 リストア処理の監視

Jobs ページを使用して、SnapCenter の各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。


このタスクについて

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

以下のアイコンがジョブページに表示され、操作の状態を示します。

-  実行中です
-  正常に完了しました
-  失敗しました
-  警告で終了したか、警告が原因で起動できませんでした
-  キューに登録され
-  キャンセルされました

手順

1. 左側のナビゲーションペインで、**Monitor** をクリックします。
2. [\* Monitor\*] ページで、[\* Jobs] をクリックします。
3. [\* ジョブ \*] ページで、次の手順を実行します。
  - a. をクリックします  リストをフィルタリングして、リストア処理のみを表示します。
  - b. 開始日と終了日を指定します。



- c. [\* タイプ] ドロップダウン・リストから、[ リストア \*] を選択します。
  - d. [\* Status \*] ドロップダウン・リストから、リストア・ステータスを選択します。
  - e. [ 適用 (Apply) ] をクリックして、正常に完了した操作を表示する。
4. リストアジョブを選択し、\* Details \* をクリックして、ジョブの詳細を表示します。
  5. [\* ジョブの詳細 \*] ページで、[\* ログの表示 \*] をクリックします。

**View logs** ボタンをクリックすると、選択した操作の詳細なログが表示されます。

## IBM DB2リソースバックアップのクローニング

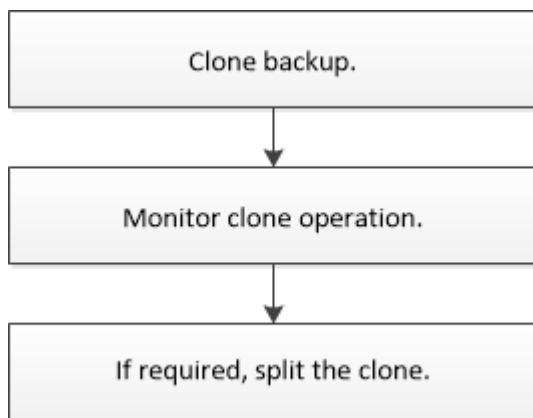
### クローニングワークフロー

クローニングワークフローには、クローニング処理の実行と処理の監視が含まれます。

このタスクについて

- クローンは、ソースIBM DB2サーバ上で作成できます。
- リソースのバックアップをクローニングする理由には次のものがあります。
  - アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のリソースの構造およびコンテンツを使用してテストするため
  - データの抽出と操作を行うツールで、データウェアハウスにデータを取り込むため
  - 誤って削除または変更されたデータをリカバリするため

次のワークフローは、クローニング処理の実行順序を示しています。



PowerShell コマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShell コマンドレットの詳細については、SnapCenter のコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

完了後

自動検出されたDB2リソースをクローニングすると、クローニングされたリソースは手動リソースとしてマークされます。クローンDB2リソースをリカバリするには、\*[リソースをリフレッシュ]\*をクリックします。クローンを削除すると、ストレージとホストもクリーンアップされます。

クローン処理後にリソースを更新せずにクローンを削除しようとする、ストレージとホストはクリーンアップされません。fstabでエントリを手動で削除する必要があります。

## IBM DB2バックアップのクローニング

SnapCenter を使用してバックアップをクローニングすることができます。クローニングはプライマリとセカンダリのどちらのバックアップからも実行できます。

作業を開始する前に

- リソースまたはリソースグループをバックアップしておく必要があります。
- ボリュームをホストするアグリゲートが Storage Virtual Machine (SVM) に割り当てられたアグリゲートリストに含まれていることを確認する必要があります。
- クローニング前またはクローニング後のPREコマンドについては、次のパスから、プラグインホストのコマンドリストにコマンドが含まれているかどうかを確認する必要があります。

Windowsの場合：C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config

Linuxの場合：/opt/NetApp/snapcenter/scc/etc/allowed\_commands.config



コマンドリストにコマンドがない場合、処理は失敗します。

このタスクについて

- クローンスプリット処理の制限事項については、を参照してください "[ONTAP 9 論理ストレージ管理ガイド](#)"。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順


1. 左側のナビゲーションペインで、\*リソース\* をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソースタイプに基づいて、**View** ドロップダウンリストからリソースをフィルタリングします。

リソースは、タイプ、ホスト、関連付けられているリソースグループとポリシー、ステータスなどの情報とともに表示されます。

3. リソースまたはリソースグループを選択します。

リソースグループを選択する場合は、リソースを選択する必要があります。

リソースまたはリソースグループのトポロジページが表示されます。

4. Manage Copies (コピーの管理) ビューから、プライマリまたはセカンダリ (ミラーまたはバックアップ) ストレージシステムから \* Backups (バックアップ) を選択します。
5. 表からデータバックアップを選択し、をクリックします 

6. Location ページで、次のアクションを実行します。

フィールド	手順
クローンサーバ	クローンを作成するホストを選択します。
ターゲットのクローンインスタンス	既存のバックアップからクローニングするターゲットDB2クローンインスタンスIDを入力します。  これは、ANFストレージタイプのリソースにのみ該当します。
ターゲットクローン名	クローンの名前を入力します。  これは、DB2データベースリソースにのみ適用されます。
NFS エクスポートの IP アドレス	クローニングしたボリュームをエクスポートする IP アドレスまたはホスト名を入力します。  これは、NFSストレージタイプリソースにのみ該当します。
容量プール最大 スループット (MiB/秒)	容量プールの最大スループットを入力します。

7. Scripts ページで、次の手順を実行します。



スクリプトはプラグインホストで実行されます。

- a. クローニング処理の前後に実行するプリコマンドやポストコマンドを入力します。
  - クローニング前のコマンド：同じ名前の既存のデータベースを削除します
  - クローニング後のコマンド：データベースの検証やデータベースの起動
- b. ホストにファイルシステムをマウントするには、mount コマンドを入力します。

Linux マシンのボリュームまたは qtree に対する mount コマンド：

NFS の例：

```
mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt
```



休止、Snapshot、および休止解除の処理を実行するプリコマンドとポストコマンドの場合は、Linuxの場合は `_/opt/snapcenter/snapcenter/scc/allowed_commands.config_path`、Windowsの場合は `_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config` からプラグインホストで使用できるコマンドリストにコマンドが存在するかどうかを確認する必要があります。

8. [通知] ページの [電子メールの設定 \*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および Eメールの件名を指定する必要があります。

9. 概要を確認し、[完了] をクリックします。

10. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

完了後

自動検出されたDB2リソースをクローニングすると、クローニングされたリソースは手動リソースとしてマークされます。クローンDB2リソースをリカバリするには、\*[リソースをリフレッシュ]\*をクリックします。クローンを削除すると、ストレージとホストもクリーンアップされます。

クローン処理後にリソースを更新せずにクローンを削除しようとする、ストレージとホストはクリーンアップされません。fstabでエントリを手動で削除する必要があります。

## PowerShellコマンドレットを使用したIBM DB2データベースのバックアップのクローニング

クローニングワークフローには、計画、クローニング処理の実行、および処理の監視が含まれます。

PowerShell コマンドレットを実行できるように PowerShell 環境を準備しておく必要があります。

コマンドレットで使用できるパラメータとその説明については、RUN\_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "[SnapCenter ソフトウェアコマンドレットリファレンスガイド](#)"。

手順

1. Open-SmConnection コマンドレットを使用して、指定したユーザの SnapCenter サーバとの接続セッションを開始します。

```
PS C:\> Open-SmConnection
```

2. Get-SmBackup コマンドレットを使用して、クローニング処理を実行するバックアップを取得します。

この例では、クローニングできるバックアップが 2 つあります。

```
C:\PS> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
-----	-----
1	Payroll Dataset_vise-f6_08... 8/4/2015
11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08... 8/4/2015
11:23:17 AM	

3. 既存のバックアップからクローニング処理を開始し、クローニングされたボリュームをエクスポートする NFS エクスポートの IP アドレスを指定します。

この例では、NFSExportIPsアドレスが10.32.212.14であるバックアップをクローニングしています。

DB2データベースの場合：

```
PS C:\> New-SmClone -Resources @{"Host"="10.32.212.13";"Uid"="db2inst1\BOOKS"} -BackupName  
'scdb201_gdl_openlab_netapp_local_DB2_db2inst1_BOOKS_scdb201_05-15-  
2024_00.29.20.1466' -AppPluginCode DB2 -CloneToInstance '10.32.212.14'  
-CloneInstance db2inst1 -CloneName BOOKS -NFSExportIPs 10.32.212.14
```

DB2インスタンスの場合：

```
PS C:\> New-SmClone -Resources @{"Host"="10.32.212.13";"Uid"="DB2"}  
-BackupName  
'scdb201_gdl_openlab_netapp_local_DB2_db2inst1_BOOKS_scdb201_05-15-  
2024_00.29.20.1466' -AppPluginCode DB2 -CloneToInstance '10.32.212.14'  
-CloneName Db2 -NFSExportIPs 10.32.212.14
```



NFSExportIPs を指定しない場合、デフォルトでクローンターゲットホストにエクスポートされます。

4. Get-SmCloneReport コマンドレットを使用してクローニングジョブの詳細を表示し、バックアップが正常にクローニングされたことを確認します。

クローン ID、開始日時、終了日時などの詳細を確認できます。

```

PS C:\> Get-SmCloneReport -JobId 186

SmCloneId           : 1
SmJobId              : 186
StartDateTime       : 8/3/2015 2:43:02 PM
EndDateTime         : 8/3/2015 2:44:08 PM
Duration             : 00:01:06.6760000
Status               : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName           : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName    : OnDemand_Full_Log
SmBackupPolicyId    : 1
CloneHostName       : SCSPR0054212005.mycompany.com
CloneHostId         : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources     : {Don, Betty, Bobby, Sally}
ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError           :







```


## IBM DB2のクローニング処理の監視

Jobs ページを使用して、SnapCenter のクローニング処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題があるかどうかを確認できます。

このタスクについて

以下のアイコンがジョブページに表示され、操作の状態を示します。

-  実行中です
-  正常に完了しました
-  失敗しました
-  警告で終了したか、警告が原因で起動できませんでした
-  キューに登録され
-  キャンセルされました
- 手順 \*
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [\* Monitor\*] ページで、 [\* Jobs] をクリックします。

3. [\* ジョブ \*] ページで、次の手順を実行します。
  - a. をクリックします  をクリックして、クローニング処理のみが表示されるようにリストをフィルタリングします。
  - b. 開始日と終了日を指定します。
  - c. [Type](タイプ) ドロップダウンリストから '[\*Clone](クローン\*)' を選択します
  - d. [\* Status \*] ドロップダウン・リストから、クローンのステータスを選択します。
  - e. [適用 (Apply)] をクリックして、正常に完了した操作を表示する。
4. クローンジョブを選択し、\* Details \* をクリックして、ジョブの詳細を表示します。
5. [ジョブの詳細] ページで、[\* ログの表示 \*] をクリックします。

## クローンをスプリットします。

SnapCenter を使用して、クローニングされたリソースを親リソースからスプリットできます。スプリットされたクローンは、親リソースに依存しません。

### このタスクについて

- 中間のクローンに対してクローンスプリット処理を実行することはできません。

たとえば、データベースバックアップから clone1 を作成したあとで、Clone1 のバックアップを作成し、そのバックアップ (Clone2) をクローニングできます。Clone2 を作成すると、clone1 は中間クローンであり、clone1 でクローンスプリット処理を実行することはできません。ただし、Clone2 でクローンスプリット処理を実行することはできます。

Clone2 をスプリットしたあとは、clone1 が中間クローンではなくなるため、clone1 でクローンスプリット処理を実行できます。

- クローンをスプリットすると、クローンのバックアップコピーとクローンジョブが削除されます。
- クローンスプリット処理の制限事項については、を参照してください ["ONTAP 9 論理ストレージ管理ガイド"](#)。
- ストレージシステム上のボリュームまたはアグリゲートがオンラインであることを確認します。


### 手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [\* リソース \* (\* Resources \*)] ページで、[表示 (View)] リストから適切なオプションを選択する。

オプション	説明
データベースアプリケーション用	[表示] リストから [*Database] を選択します。
ファイルシステムの場合	[表示] リストから [*パス*] を選択します。

3. リストから適切なリソースを選択します。

リソースのトポロジページが表示されます。

4. ビューで、クローンリソース（データベースやLUNなど）を選択し、\*をクリックします。 
5. スプリットするクローンの推定サイズとアグリゲートで使用可能なスペースを確認し、\* Start \* をクリックします。
6. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

SMCore サービスが再起動すると、クローンスプリット処理が応答しなくなります。Stop-SmJob コマンドレットを実行してクローンスプリット処理を停止し、クローンスプリット処理を再試行する必要があります。

クローンがスプリットされているかどうかを確認するためにポーリング時間を長くしたり、ポーリング時間を短縮したりする場合は、\_SMCoreServiceHost.exe.config\_file の \_CloneSplitStatusCheckPollTime\_Parameter の値を変更して、SMCore がクローンスプリット処理のステータスをポーリングする間隔を設定できます。この値はミリ秒で、デフォルト値は 5 分です。

例：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

バックアップ、リストア、または別のクローンスプリットの実行中は、クローンスプリットの開始処理が失敗します。クローンスプリット処理は、実行中の処理が完了してから再開してください。

#### 関連情報

"「aggregate does not exist」というメッセージが表示されて、SnapCenter クローンまたは検証が失敗する"

## SnapCenterのアップグレード後にIBM DB2データベースクローンを削除またはスプリットする

SnapCenter 4.3 にアップグレードすると、クローンは表示されなくなります。クローンを削除するか、クローンが作成されたリソースのトポロジページからクローンをスプリットします。

このタスクについて



非表示クローンのストレージフットプリントを確認するには、「Get-SmClone-ListStorageFootprint」コマンドを実行します

#### 手順

1. remove-smbbackup コマンドレットを使用して、クローニングしたリソースのバックアップを削除します。
2. remove-smresourcegroup コマンドレットを使用して、クローニングされたリソースのリソースグループを削除します。
3. remove-smprotectresource コマンドレットを使用して、クローニングされたリソースの保護を解除します。
4. [リソース] ページから親リソースを選択します。

リソースのトポロジページが表示されます。



5. Manage Copies（コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはレプリケートされた）ストレージシステムからクローンを選択します。
6. クローンを選択し、をクリックします  クローンを削除するには、をクリックします  をクリックしてクローンをスプリットします。
7. [OK] をクリックします。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。