IBM Db2の保護

SnapCenter software

NetApp
November 06, 2025

目次

IBM Db2の保護

SnapCenter Plug-in for IBM Db2

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提供する、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 6.0 は IBM Db2 10.5 以降をサポートしています。
- SnapCenter 6.0.1 は IBM Db2 9.7.x 以降をサポートしています。また、 SnapCenter 6.0.1 以降では、AIX 上の IBM Db2 がサポートされます。

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とWindowsのどちらの環境でも使用できます。Windows環境では、Db2は手動リソースとしてサポートされます。

Db2 pureScale 環境および Db2 マルチノード (DPF) システムはサポートされていません。

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、このプラグインをNetApp SnapVaultテクノロジとともに使用して、標準への準拠を目的としたディスクツーディスク 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 Filesストレージ レイアウトでNFSとSANをサポートします。

VMDK、vVol、RDM 仮想ストレージ レイアウトがサポートされています。

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、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も実行できます。

- 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します。
- 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します。
- 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の特長

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NetAppの数々のテクノロジと統合されます。Plug-in for IBM Db2 Databaseの操作には、SnapCenterのグラフィカル ユーザ インターフェイスを使用します。

- 統合されたグラフィカルユーザーインターフェース

  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。どのプラグインでも、SnapCenterのインターフェイスから、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。

- 自動化された中央管理

  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からのEメール アラートの送信を設定して、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**スナップショット コピー テクノロジー

  SnapCenterでは、Plug-in for IBM Db2 DatabaseでNetApp Snapshotテクノロジを使用してリソースがバックアップされます。

Plug-in for IBM Db2を使用すると、次のメリットもあります。

- バックアップ、リストア、および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。

  クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルのアクセス権を付与することもできます。

- NetApp FlexCloneテクノロジを使用して、テストまたはデータ抽出に使用するリソースのコピー（スペース効率に優れたポイントインタイム コピー）を作成できます。

  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。

- バックアップの作成でONTAPの整合グループ（CG）のSnapshot機能がサポートされます。
- 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回の処理で、1つのホストの複数のリソースが同じボリュームを共有する場合に複数のSnapshotが統合されます。

- 外部コマンドを使用してSnapshotを作成できます。
- XFSファイルシステム上のLinux LVMがサポートされます。

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かどうか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	• FC接続LUN • iSCSI接続LUN • NFS接続ボリューム
VMware ESXi	• FCまたはiSCSI HBAで接続されたRDM LUNホスト バス アダプタ（HBA）のスキャンは、SnapCenterがホストに存在するすべてのホスト バス アダプタをスキャンするため、完了までに時間がかかることがあります。 */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* にある **LinuxConfig.pm** ファイルを編集して、**SCSI_HOSTS_OPTIMIZED_RESCAN** パラメータの値を 1 に設定し、HBA_DRIVER_NAMES にリストされているHBA のみを再スキャンすることができます。 • iSCSIイニシエータでゲスト システムに直接接続されたiSCSI LUN • NFSデータストア上のVMDK • VMFS上にVMDKが作成されました • ゲスト システムに直接接続されたNFSボリューム • NFSとSANの両方に存在するvVolデータストア vVolデータストアは、ONTAP Tools for VMware vSphereでのみプロビジョニングできます。

IBM Db2プラグインに必要な最小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。

- 全アクセス コマンド: ONTAP 9.12.1 以降に必要な最小限の権限
  - event generate-autosupport-log
  - job history show
  - job stop
  - lun

- lun create
- lun create
- lun create
- lun delete
- lun igroup add
- lun igroup create
- lun igroup delete
- lun igroup rename
- lun igroup rename
- lun igroup show
- lun mapping add-reporting-nodes
- lun mapping create
- lun mapping delete
- lun mapping remove-reporting-nodes
- lun mapping show
- lun modify
- lun move-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- lun resize
- lun serial
- lun show
- snapmirror policy add-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- snapmirror restore
- snapmirror show
- snapmirror show-history
- snapmirror update
- snapmirror update-ls-set
- snapmirror list-destinations
- version
- volume clone create
- volume clone show
- volume clone split start

- volume clone split stop
- volume create
- volume destroy
- volume file clone create
- volume file show-disk-usage
- volume offline
- volume online
- volume modify
- volume qtree create
- volume qtree delete
- volume qtree modify
- volume qtree show
- volume restrict
- volume show
- volume snapshot create
- volume snapshot delete
- volume snapshot modify
- volume snapshot modify-snaplock-expiry-time
- volume snapshot rename
- volume snapshot restore
- volume snapshot restore-file
- volume snapshot show
- volume unmount
- vserver cifs
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy show
- vserver cifs share show
- vserver cifs show
- vserver export-policy
- vserver export-policy create
- vserver export-policy delete
- vserver export-policy rule create
- vserver export-policy rule show
- vserver export-policy show
- vserver iscsi
- vserver iscsi connection show

- vserver show
- 読み取り専用コマンド: ONTAP 8.3.0以降に必要な最小限の権限
  - ネットワークインターフェース
  - network interface show
  - SVM

IBM Db2でのSnapMirrorレプリケーションとSnapVaultレプリケーションのためのストレージ システムの準備

SnapCenterプラグインと一緒にONTAP SnapMirrorテクノロジを使用すると、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を使用すれば、標準への準拠やその他のガバナンス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に対する更新を実行します。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。

NetApp 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、ソース ボリュームで参照されるデータ ブロックがデスティネーション ボリュームに転送されます。

SnapCenter は、 SnapMirrorとSnapVaultボリューム間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 > ボールト)。ファンアウト関係を使用する必要があります。

SnapCenterは、バージョンに依存しないSnapMirror関係の管理をサポートしています。バージョンに依存しないSnapMirror関係とその設定方法の詳細については、 "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と、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。

タスク概要

SLAとは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。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. Snapshotコピーベースのポリシーを作成して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 システムおよびSnapMirrorデスティネーションでのSnapshotの保持期間を確認します。
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で管理する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 SAP 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て[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

バックアップ タイプでは、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テクノロジを利用して、IBM Db2データベースが格納されたボリュームのオンラインの読み取り専用のコピーが作成されます。

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 グループの整合グループSnapshotを作成することができます。整合グループとはボリュームのコンテナであり、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。整合グループには複数のボリュームの同時に作成されたSnapshotが格納されるため、一連のボリュームのコピーの整合性が確保されます。

ストレージ コントローラが整合性を確保しながらSnapshotをグループ化するのを待機する時間も指定できます。利用可能な待機時間のオプションは、「緊急」、「中」、「緩和」です。また、整合グループSnapshotの処理でWrite Anywhere File Layout（WAFL）の同期を有効にするか無効にするかも選択できます。WAFLの同期を有効にすると、整合グループ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

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 ストレージのSnapshotが削除され、IBM Db2のカタログ内の対応するエントリも削除されます。

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日時）

  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、週次バックアップのポリシーが設定されているリソースグループがある場合、毎週木曜日の午後10時にバックアップするようにスケジュールを設定できます。

SAP Db2の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データベースのバックアップの命名規則

Snapshotのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。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ので、コピーが作成されたタイミングを特定できます。

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、[スナップショット コピーにカスタム名形式を使用する] 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スナップショット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、Snapshot名にタイムスタンプのサフィックスが追加されます。

IBM Db2のリストアとリカバリの戦略

IBM Db2リソースのリストアとリカバリの戦略の定義

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します。
2. 自動検出されたIBM Db2データベースでサポートされるリストア戦略を確認します。

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、戦略を定義しておく必要があります。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

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のリストア用のSnapshotが選択されたあとに作成された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。

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、戦略を定義しておく必要があります。

リソースの完全なリストアは、自動検出されたIBM Db2データベースに対してサポートされているリストア戦略です。この戦略では、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では、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のリストア タイプがサポートされます。

NFS環境で**Single File SnapRestore**を実行するシナリオは、次のとおりです。

- *完全なリソース*オプションのみを選択した場合
- 選択したバックアップがSnapMirrorまたはSnapVaultのセカンダリロケーションからのものであり、*完全なリソース*オプションが選択されている場合

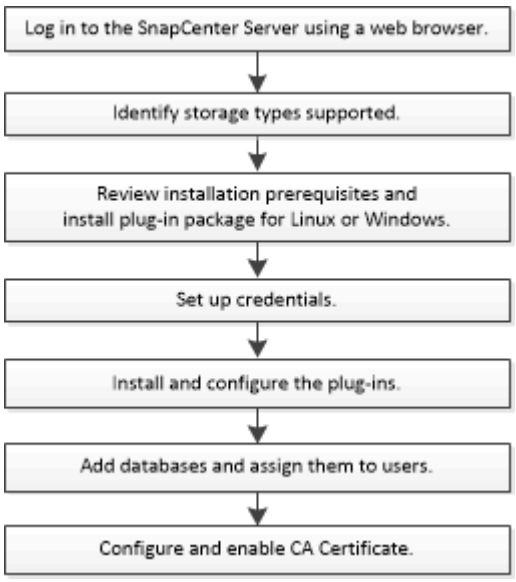
SAN環境で**Single File SnapRestore**を実行するシナリオは、次のとおりです。

- *完全なリソース*オプションのみを選択した場合
- バックアップがSnapMirrorまたはSnapVaultのセカンダリロケーションから選択され、*完全なリソース*オプションが選択されている場合

SnapCenter Plug-in for IBM Db2のインストール準備

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。



Windows、**Linux**、または **AIX** 用のホストを追加し、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。Windows、Linux、AIX 環境でサポートされる IBM Db2 用のSnapCenterプラグイン。

- 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 Windows および Linux ホストではサポートされていません。

- Windows の場合、プラグイン クリエーター サービスは、“LocalSystem” Windows ユーザーを使用して実行する必要があります。これは、IBM Db2 用プラグイン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際、組み込みでないクレデンシャルを指定する場合や、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。WindowsホストにIBM Db2プラグインをインストールすると、SnapCenter Plug-in for Microsoft Windowsもデフォルトで導入されます。
- SnapCenter Server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があり、リモート ホストに対してローカル ログインのアクセス許可があるドメイン ユーザが必要です。
- 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以外のユーザに対してパスワード 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。

  "Windows用JAVAをダウンロード"

  "NetApp Interoperability Matrix Tool"

Linuxおよび**AIX**ホスト

- rootユーザまたはroot以外のユーザに対してパスワード 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Linuxホストにインストールしておく必要があります。

  "Linux用JAVAをダウンロード"

  "AIX用JAVAをダウンロード"

  "NetApp Interoperability Matrix Tool"

- 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** を使用する必要があります。

補助コマンド

SnapCenterプラグイン for IBM Db2 で補足コマンドを実行するには、そのコマンドを *allowed_commands.config* ファイルに含める必要があります。

- Windows ホスト上のデフォルトの場所: *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Linux ホスト上のデフォルトの場所: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

プラグイン ホストで補足コマンドを許可するには、エディターで *allowed_commands.config* ファイルを開きます。各コマンドを別々の行に入力します。コマンドでは大文字と小文字は区別されません。完全修飾パス名を指定し、パス名にスペースが含まれている場合は引用符 (") で囲んでください。

例えば：

command: mount

command: umount

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

command: myscript.bat

allowed_commands.config ファイルが存在しない場合、コマンドまたはスクリプトの実行はブロックされ、ワークフローは次のエラーで失敗します。

"[/mnt/mount -a] の実行は許可されていません。Authorize by adding the command in the file %s on the plugin host.」

コマンドまたはスクリプトが *allowed_commands.config* に存在しない場合、コマンドまたはスクリプトの実行はブロックされ、ワークフローは次のエラーで失敗します。

"[/mnt/mount -a] の実行は許可されていません。Authorize by adding the command in the file %s on the plugin host.」

すべてのコマンドを許可するには、ワイルドカード エントリ (*) を使用しないでください。

Linuxホストの**root**以外のユーザへの**sudo**権限の設定

SnapCenter、非ルート ユーザーが Linux 用のSnapCenterプラグイン パッケージをインストールし、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
- umask が 0027 の場合、java フォルダーとその中のすべてのファイルに 555 の権限があることを確認します。そうしないと、プラグインのインストールが失敗する可能性があります。
- 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* ファイルを編集して、メッセージ認証コード アルゴリズム (MAC hmac-sha2-256 および MAC hmac-sha2-512) を設定します。

  この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/installation/plugins/uninstall
- /custom_location/NetApp/snapcenter/spl/bin/spl

手順

1. SnapCenter Plug-ins Package for Linuxをインストールする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/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

RAC をセットアップしている場合は、他の許可されたコマンドとともに、/etc/sudoers ファイルに次の行を追加する必要があります: '/<crs_home>/bin/olsnodes'

crs_home の値は、*/etc/oracle/olr.loc* ファイルから取得できます。

LINUX_USER は、作成した非 root ユーザーの名前です。

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。

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

この例は、独自のデータを作成する際の参照としてのみ使用してください。

AIXホストの**root**以外のユーザへの**sudo**権限の設定

SnapCenter 4.4以降では、root以外のユーザがSnapCenter Plug-ins Package for AIX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
- umask が 0027 の場合、java フォルダーとその中のすべてのファイルに 555 の権限があることを確認します。そうしないと、プラグインのインストールが失敗する可能性があります。
- */etc/ssh/sshd_config* ファイルを編集して、メッセージ認証コード アルゴリズム (MAC hmac-sha2-256 および MAC hmac-sha2-512) を設定します。

  この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/*AIX_USER*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /custom_location/NetApp/snapcenter/spl/bin/spl

手順

1. SnapCenter Plug-ins Package for AIXをインストールするAIX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 HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

RAC をセットアップしている場合は、他の許可されたコマンドとともに、/etc/sudoers ファイルに次の行を追加する必要があります: '/<crs_home>/bin/olsnodes'

crs_home の値は、*/etc/oracle/olr.loc* ファイルから取得できます。

AIX_USER は、作成した非 root ユーザーの名前です。

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。

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

この例は、独自のデータを作成する際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 システムのスペースとサイジングに関する基本的な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	Microsoft Windows サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要な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て、ログ 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、保護対象の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は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。

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

SnapCenter Plug-ins Package for Linuxをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な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	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server（SLES） サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。

項目	要件
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	2 GB 十分なディスク スペースを割り当てて、ログ 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、保護対象の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は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	Java 11 Oracle JavaおよびOpenJDK 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/spl/etc/spl.propertiesにあるJAVA_HOMEオプションが正しいJavaバージョンと正しいパスに設定されていることを確認する必要があります。 サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。

SnapCenter Plug-in for IBM Db2のクレデンシャルの設定

SnapCenterは、クレデンシャルを使用してSnapCenterの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使用するクレデンシャルと、データベースやWindowsファイルシステムでのデータ保護処理に使用するクレデンシャルをそれぞれ作成する必要があります。

タスク概要

- Linuxホスト

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

  このクレデンシャルは、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo権限があるroot以外のユーザに対して設定します。

  ベスト プラクティス: ホストをデプロイしてプラグインをインストールした後でも Linux の認証情報を作成できますが、ベスト プラクティスとしては、SVM を追加した後、ホストをデプロイしてプラグインをインストールする前に認証情報を作成します。

- Windowsホスト

  プラグインのインストール前にWindowsクレデンシャルを設定する必要があります。

このクレデンシャルには、管理者権限（リモート ホストに対する管理者権限を含む）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する場合で、ユーザ名に完全なadmin権限が割り当てられていない場合は、少なくともリソース グループとバックアップの権限を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*をクリックします。
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	操作
資格情報名	クレデンシャルの名前を入力します。
ユーザ名	認証に使用するユーザ名とパスワードを入力します。 • 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 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。ユーザ名フィールドの有効な形式は次のとおりです。 ◦ *NetBIOS*\ユーザー名 ◦ ドメイン*FQDN*\ユーザー名 • ローカル管理者（ワークグループの場合のみ） 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。ユーザー名フィールドの有効な形式は次のとおりです: *UserName* パスワードには二重引用符 (") やバッククォート (`) を使用しないでください。未満記号（<）と感嘆符（!）を組み合わせて使用したりしないでください。たとえば、lessthan<!10、lessthan10<!、バックティック`12 などです。

フィールド	操作
パスワード	認証に使用するパスワードを入力します。
Authentication Mode	使用する認証モードを選択します。
Use sudo privileges	非 root ユーザーの資格情報を作成する場合は、[**sudo** 権限を使用する] チェックボックスをオンにします。 Linuxユーザのみに該当します。

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、必要に応じて[User and Access]ページでユーザやユーザ グループにクレデンシャル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、作成したグループ管理サービス アカウント（gMSA）を通じて、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できます。

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. KDSルート キーを作成し、gMSA内のオブジェクトごとに一意のパスワードを生成します。
2. 各ドメインについて、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 -EffectiveImmediately
3. gMSAを作成して設定します。
   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$
. . コンピュータ  オブジェクトをグループに追加します。
. . 作成したユーザ  グループを使用してgMSAを作成します。
```

次に例を示します。

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. 走る `Get-ADServiceAccount`サービス アカウントを確認するコマンド。
```

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。

      これを行うには、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。 `Install-AdServiceAccount <gMSA>`

   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. ホスト上の設定済みgMSAに管理者権限を割り当てます。

6. SnapCenter Server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 Serverにより、選択したプラグインがホストにインストールされ、プラグインのインストール時には指定したgMSAがサービスのログオン 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

ホストの追加とリモート ホストへのプラグイン パッケージのインストール

SnapCenterの[Add Host]ページを使用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、ホストごとまたはクラスタごとに実行できます。

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
- この処理は、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実行する必要があります。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、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。
- メッセージ キュー サービスが実行中であることを確認する必要があります。
- ホストの管理については、管理に関するドキュメントを参照してください。
- グループ管理サービス アカウント（gMSA）を使用する場合は、管理者権限でgMSAを設定する必要があります。

  "Windows Server 2016 以降で IBM Db2 用のグループ管理サービス アカウントを構成する"

タスク概要

- SnapCenter Serverをプラグイン ホストとして別のSnapCenter Server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、[ホスト] をクリックします。
2. 上部の*管理対象ホスト*タブが選択されていることを確認します。
3. *[追加]*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	操作
ホストタイプ	ホストのタイプを選択します。 • Windows • Linux 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。
ホスト名	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が機能するためには、DNSが適切に設定されている必要があります。そのため、FQDNを入力することを推奨します。
Credentials	作成したクレデンシャルの名前を選択するか、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。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。 クレデンシャルの認証モードは、[Add Host]ウィザードで指定するホスト タイプによって決まります。

5. [Select Plug-ins to Install]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	操作
ポート	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 Server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。 プラグインを手動でインストールしてカスタム 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、処理が失敗します。
Installation Path	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。 • Windows 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは C:\Program Files\ NetApp\ SnapCenterです。必要に応じて、パスをカスタマイズできます。 • Linux 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは /opt/ NetApp/snapcenter です。必要に応じて、パスをカスタマイズできます。
Skip preinstall checks	プラグインを手動でインストール済みで、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、このチェックボックスをオンにします。
Use group Managed Service Account (gMSA) to run the plug-in services	Windowsホストで、グループ管理サービス アカウント（gMSA）を使用してプラグイン サービスを実行する場合は、このチェック ボックスをオンにします。 gMSA名をdomainName\accountName$の形式で指定します。 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す。

7. *送信*をクリックします。

[Skip prechecks]チェック ボックスを選択していない場合、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のバージョン、場所（Windowsプラグインの場合）、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、対応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\SnapCenter WebAppにあるweb.configファイルを更新してデフォルト値を変更できます。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のセットアップで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、[確認して送信] 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。

> 前述の手順で同じホストがSnapCenterに追加され、フィンガープリントが確認された場合でも、フィンガープリントの検証は必須です。

9. インストールの進捗状況を監視します。
   - 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 ログは次の場所にあります: *C:\Windows\ SnapCenter plugin\Install*<JOBID>\
   - Linux プラグインの場合、インストール ログは次の場所にあります: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log、アップグレード ログは次の場所にあります: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log

終了後の操作

SnapCenter 6.0 以降にアップグレードする場合、既存の PERL ベースの Db2 用プラグインはリモート プラグイン サーバー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た複数のリモート ホストへの**SnapCenter Plug-ins Package for Linux / Windows**のインストール

Install-SmHostPackage PowerShellコマンドレットを使用すると、複数のホストにSnapCenter Plug-ins Package for Linux / Windowsを同時にインストールできます。

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に対するローカル管理者権限を持つドメイン ユーザとして、SnapCenterにログインしておく必要があります。

手順

1. PowerShellを起動します。
2. SnapCenter Server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関する情報は、*Get-Help command_name* を実行す

ると取得できます。あるいは、 "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済みで、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た**Linux**ホストへの**SnapCenter Plug-in for IBM Db2**のインストール

SnapCenter Plug-in for IBM Db2 Databaseは、SnapCenter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。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環境では、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。

開始する前に

- Plug-in for IBM Db2 Databaseは、IBM Db2クライアントがあるLinuxホストごと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ホストは、依存するソフトウェア、データベース、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に関する最新の情報については、Interoperability Matrix Tool（IMT）を参照してください。

  "NetApp Interoperability Matrix Tool"

- 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。

タスク概要

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 Server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 プロンプトから、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 は SMCore HTTPS 通信ポートを指定します。
   - -DSERVER_IP は、 SnapCenter Server の IP アドレスを指定します。

- -DSERVER_HTTPS_PORT は、 SnapCenter Server の HTTPS ポートを指定します。
- -DUSER_INSTALL_DIR は、Linux 用のSnapCenterプラグイン パッケージ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. /<インストール ディレクトリ>/ 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、SnapCenter Serverにホストを追加します。

   コマンドで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、 "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

[Jobs]ページを使用して、SnapCenterプラグイン パッケージのインストールの進捗状況を監視できます。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発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録

手順

1. 左側のナビゲーション ペインで、[モニター] 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. ジョブ ページで、プラグインのインストール操作のみがリスト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. *フィルター*をクリックします。
   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、[プラグインのインストール] を選択します。

d. [Status]ドロップダウン メニューから、インストールのステータスを選択します。

e. *適用*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証明書の設定

CA証明書CSRファイルの生成

証明書署名要求（CSR）を生成し、生成したCSRを使用して認証局（CA）から取得した証明書をインポートできます。証明書には秘密キーが関連付けられます。

CSRはエンコードされたテキストのブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。

CA 証明書の RSA キーの長さは最低 3072 ビットである必要があります。

CSRを生成するための情報については、 "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は、CA 証明書 CSR ファイルの生成をスキップできます。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、クラスタ名（仮想クラスタFQDN）と、それぞれのホスト名がCA証明書に記載されている必要があります。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。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証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenter Server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] をクリックします。

2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。

3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] 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 コンピューター > 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] > [インポート] を選択して、インポート ウィザードを起動します。

6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*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、[次へ] をクリックします。
証明書のインポート ウィザードの完了	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。

インポートする証明書は秘密キーと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 です)。

7. 「個人用」フォルダに対して手順5を繰り返します。

CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための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て、「拇印」をクリックします。
   d. ボックスから16進数の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、拇印が「a9 09 50 2d d8 2a e4 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」になります。

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表示し、最近インストールされた証明書をサブジェクト名で識別します。

      Get-ChildItem -Path 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 サービスでの**CA**証明書の設定

インストールされているデジタル証明書をアクティブ化するには、Windowsホスト プラ

グイン サービスを使用してCA証明書を設定する必要があります。

SnapCenter Serverと、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、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

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

   例えば：

   ```
    > 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 サービスとバインドします。

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

   例えば：

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

Linuxホストでの**SnapCenter IBM Db2**プラグイン サービスの**CA**証明書の設定

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には、 SnapCenterプラグイン サービスを使用して、プラグイン キーストアとその証明書のパスワードを管理し、CA 証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、*/opt/ NetApp/snapcenter/scc/etc* にあるファイル「keystore.jks」を使用します。

プラグインキーストアのパスワードと使用中の**CA**署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

   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キー
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 ファイルのキー KEYSTORE_PASS も同様に更新します。

3. パスワードを変更したら、サービスを再起動します。

プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは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プラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグイン キーストアが含まれるフォルダーに移動します: /opt/ NetApp/snapcenter/scc/etc。
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. ルート証明書か中間証明書を追加します。

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
.
ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。
```

ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアに**CA**署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグイン キーストア /opt/ NetApp/snapcenter/scc/etc が含まれるフォルダーに移動します。

2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. 秘密キーと公開キーの両方が設定された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の一覧を表示します。

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. 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、キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

   デフォルトのプラグイン キーストア パスワードは、agent.properties ファイルのキー 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、スペースや特殊文字 （「*」、「」）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に対して更新します。

8. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

プラグインの証明書失効リスト（**CRL**）を構成する

タスク概要

- SnapCenterプラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter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/scc/etc/crl」です。

手順

1. キーCRL_PATHに対して、agent.propertiesファイルのデフォルト ディレクトリを変更、更新できます。

   このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

WindowsホストでのSnapCenter IBM Db2プラグイン サービスのCA証明書の設定

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には、 SnapCenterプラグイン サービスを使用して、プラグイン キーストアとその証明書のパスワードを管理し、CA 証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、*C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* にあるファイル *keystore.jks* を使用します。

プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

   これはキー_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

   > Windows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キー エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

   *keytool -keypasswd -alias "*証明書内のエイリアス名*" -keystore keystore.jks*

   agent.properties ファイルのキー KEYSTORE_PASS も同様に更新します。

4. パスワードを変更したら、サービスを再起動します。

   > プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは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プラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ_C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_に移動します。
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

keytool -list -v -keystore keystore.jks

4. ルート証明書か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. ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。

ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアに**CA**署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ_C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_に移動します。
2. ファイル *keystore.jks* を見つけます。
3. キーストアに追加された証明書の一覧を表示します。

   keytool -list -v -keystore keystore.jks

4. 秘密キーと公開キーの両方が設定された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の一覧を表示します。

   keytool -list -v -keystore keystore.jks

6. 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、キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

   デフォルトのプラグイン キーストア パスワードは、agent.properties ファイルのキー KEYSTORE_PASS の値です。

   *keytool -keypasswd -alias "CA*証明書のエイリアス名*" -keystore keystore.jks*

8. *agent.properties* ファイル内の 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に対して更新します。

9. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

SnapCenterプラグインの証明書失効リスト（**CRL**）を構成する

タスク概要

- 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、 "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プラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter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. キー CRL_PATH に対して、*agent.properties* ファイル内のデフォルト ディレクトリを変更および更新できます。
2. このディレクトリには、複数のCRLファイルを格納できます。

   受信する証明書については、それぞれのCRLに対して検証が行われます。

プラグインの**CA**証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインでCA証明書の検証を有効にする必要があります。

開始する前に

- 実行 *Set-SmCertificateSettings* コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- *Get-SmCertificateSettings* を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、 "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、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. プラグイン ホストを1つまたは複数選択します。
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。

終了後の操作

[Managed Hosts]タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Serverとプラグイン ホスト間の接続のステータスを示します。

- * * は、CA 証明書が有効になっていないか、プラグイン ホストに割り当てられていないことを示します。
- * * は 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。
- * * は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場合は、データ保護処理が正常に完了しています。

データ保護の準備

SnapCenter Plug-in for IBM Db2を使用するための前提条件

ユーザがSnapCenter Plug-in for IBM Db2を使用するためには、SnapCenter管理者が事前にSnapCenter Server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 Serverをインストールして設定します。
- SnapCenter Serverにログインします。
- SnapCenter環境を設定するために、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。

  Javaパスは、ホスト マシンの環境パス変数で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、リストアの各処理に関連する基本的な概念を理解しておくと役立ちます。ここでは、これらの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、一般にはSnapCenterでバックアップまたはクローニングするIBM Db2データベースのことです。
- 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。また、スケジュールされたバックアップを単一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、スクリプトといった、データ保護処理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。

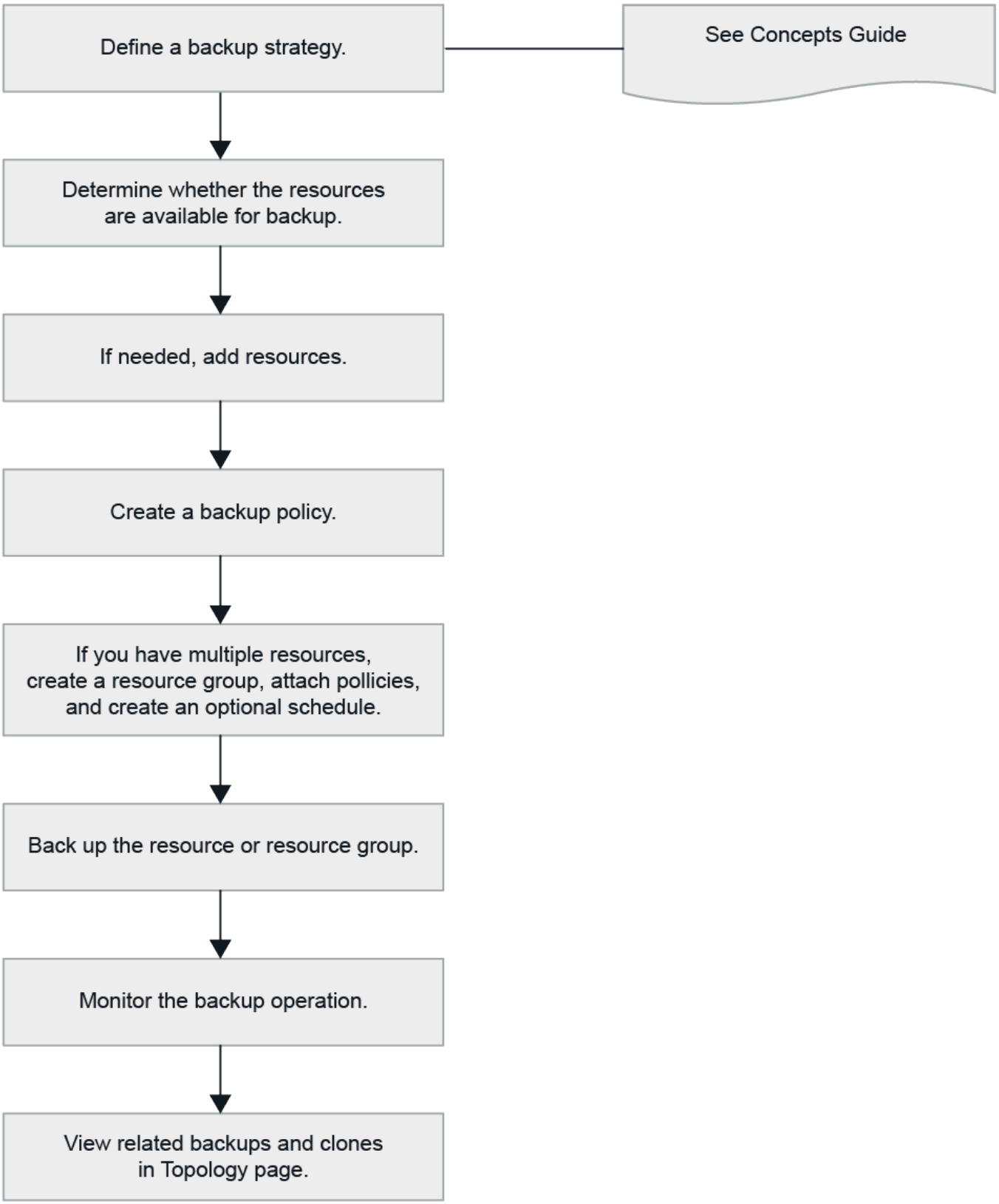
リソース グループでは、保護する対象と保護するタイミング（日時）を定義できます。ポリシーでは、保護する方法を定義できます。たとえば、すべてのデータベースをバックアップする場合は、ホストのすべてのデータベースを含むリソース グループを作成します。このリソース グループに、日次ポリシーと毎時ポリシーの2つのポリシーを適用します。リソース グループを作成してポリシーを適用する際に、フル バックアップを1日1回実行するようにリソース グループを設定できます。

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"^] 。

データベースの自動的検出

リソースとなるのは、ホスト上でSnapCenterによって管理されているLinuxホスト上のIBM Db2データベースです。使用できるIBM Db2データベースを検出したあとに、それらの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。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の作成などのタスクを事前に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が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。

タスク概要

- 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検出されて[Resources]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。

自動検出されたリソースを変更または削除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 [リソース] をクリックし、リストから [IBM Db2 用プラグイン] を選択します。
2. [Resources]ページで、[View]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、ホスト名を選択します。

   をクリックします フィルター パネルを閉じます。

4. ホスト上で利用可能なリソースを検出するには、[リソースの更新] をクリックします。

   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NetAppストレージにあって保護されていない場合は、[Overall Status]列に「Not protected」と表示されます。
   - データベースがNetAppストレージ システム上にあって保護されており、バックアップ処理が実行されていない場合は、[Overall Status]列に「Backup not run is displayed」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、ステータスが「バックアップに失敗しました」または「バックアップに成功しました」に変わります。

SnapCenterの外部でデータベースの名前が変更された場合は、リソースを更新する必要があります。

手動でのプラグイン ホストへのリソースの追加

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。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の設定などのタスクを完了しておく必要があります。

タスク概要

手動検出は、次の構成ではサポートされていません。

- RDMおよびVMDK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	操作
Name	データベース名を指定します。
Host Name	ホスト名を入力します。
タイプ	データベースまたはインスタンスを選択します。
Instance	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。
Credentials	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 フットプリントの提供] ページで、ストレージ タイプを選択し、1 つ以上のボリューム、LUN、および qtree を選択して、[保存] をクリックします。

   オプション：をクリックすることもできます  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、qtree を追加します。

5. オプション: リソース設定ページで、Windowsホスト上のリソースについては、IBM Db2プラグインのカスタム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るようになります。

"ユーザまたはグループの追加と、ロールとアセットの割り当て"

データベースの追加が完了したら、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のリソースをバックアップする前に、バックアップ対象の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 ポリシーとは、バックアップをどのように管理し、スケジューリングし、保持するかを定める一連のルールです。

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 システム接続の作成、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。
- ユーザが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 ボリューム両方のSVMをSnapCenter管理者がユーザに割り当てる必要があります。

  ポリシーで、レプリケーション、スクリプト、アプリケーション設定を指定することもできます。そ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。

タスク概要

- SnapLock
  - [Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで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が削除されません。その結果、ポリシーで指定した数よりも多くの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が、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、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、[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*をクリックします。
4. 「名前」ページで、ポリシー名と詳細を入力します。
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、キーと値の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ペアを複数指定することができます。

6. スナップショットとレプリケーション ページで、次のアクションを実行します。

a. オンデマンド、時間別、日次、週次、または*月次*を選択して、スケジュールの頻度を指定します。

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。

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実行されません。

a. スナップショット設定セクションで、次のアクションを実行します。

状況	操作
特定の数のSnapshotを保持	*保持するコピー*を選択し、保持するスナップショットの数を指定します。 Snapshotの数が指定した数を超えると、古いものから順にSnapshotが削除されます。
Snapshotを特定の日数だけ保持	*コピーの保持期間*を選択し、スナップショットを削除する前に保持する日数を指定します。
スナップショットコピーのロック期間	スナップショット コピーのロック期間 を選択し、日、月、または年を指定します。 SnapLock保持期間は100年未満にする必要があります。

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ことがあります。

b. ポリシーラベルを指定します。

リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしなくても実行できます。

7. [セカンダリ レプリケーション オプションの選択] セクションで、次のセカンダリ レプリケーション オプションの 1 つまたは両方を選択します。

フィールド	操作
Update SnapMirror after creating a local Snapshot copy	別のボリュームにバックアップ セットのミラー コピーを作成する場合（SnapMirrorレプリケーション）は、このフィールドを選択します。 このオプションは、SnapMirrorアクティブ同期に対して有効にする必要があります。
Update SnapVault after creating a local Snapshot copy	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（SnapVaultバックアップ）を実行する場合は、このオプションを選択します。
Error retry count	処理が停止されるまでに試行できるレプリケーションの最大回数を入力します。

セカンダリ ストレージでSnapshotの上限に達しないように、ONTAPでセカンダリ ストレージのSnapMirror保持ポリシーを設定する必要があります。

8. 概要を確認し、[完了] をクリックします。

リソース グループの作成とポリシーの適用

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ことで、特定のアプリケーションに関連す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 グループはいずれのデータ保護ジョブにも必要になります。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。

タスク概要

- 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が、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、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. [Name]ページで、次の操作を実行します。

フィールド	操作
Name	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文字以内で指定する必要があります。

フィールド	操作
Tags	リソース グループを検索しやすくするために、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。
Use custom name format for snapshot copy	Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。 たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

4. [リソース] ページで、[ホスト] ドロップダウン リストからホスト名を選択し、[リソース タイプ] 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。

   画面の情報がフィルタリングされます。

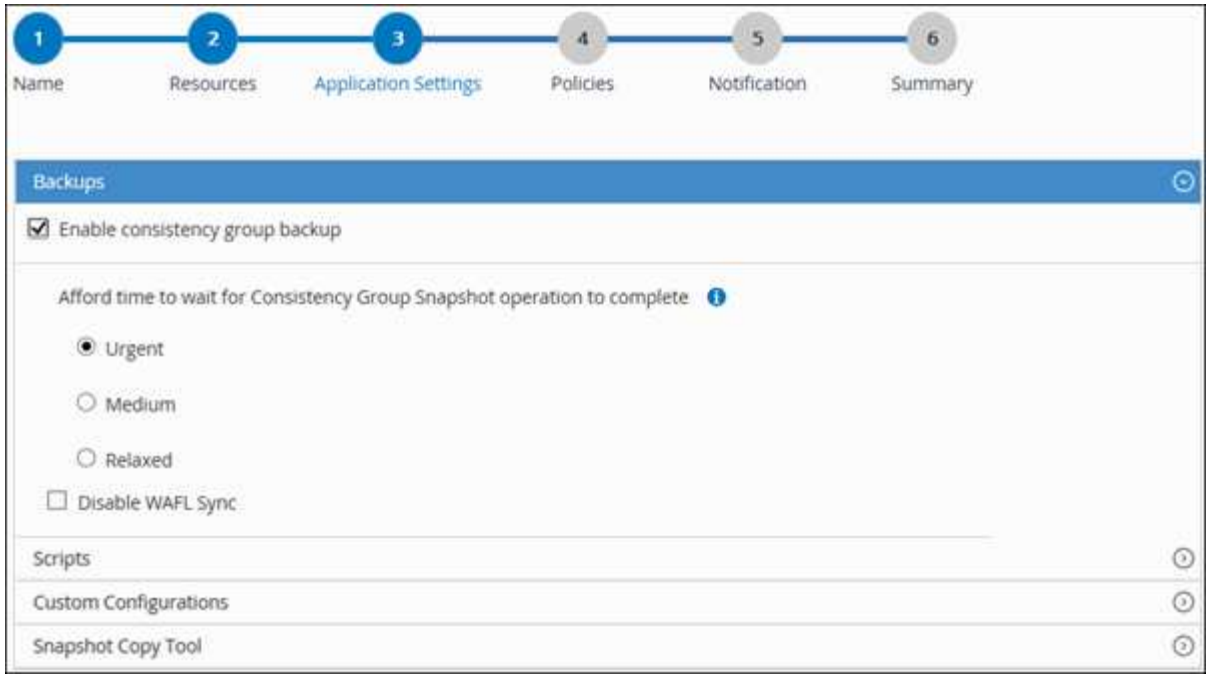
5. *利用可能なリソース*セクションからリソースを選択し、右矢印をクリックして*選択したリソース*セクションに移動します。
6. [Application Settings]ページで、次の操作を実行します。

   a. 追加のバックアップ オプションを設定するには、[バックアップ] 矢印をクリックします。

      整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for Consistency Group snapshot operation to complete	スナップショット操作が完了するまでの待機時間を指定するには、「緊急」、「中」、または「緩和」を選択します。 [Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

+



a. *スクリプト*矢印をクリックし、静止、スナップショット、および静止解除操作の事前および事後コマンドを入力します。障害の発生時に終了前に実行するプリコマンドも入力できます。

b. *カスタム構成*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の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	（Y / N）	アーカイブ ログ管理を有効にし、アーカイブ ログを削除します。
ARCHIVE_LOG_RETENTION	number_of_days	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 ログが含まれるディレクトリへのパスを指定します。
ARCHIVE_LOG_EXT	file_extension	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、file_extension 値が 5 の場合、ログの拡張子は 5 桁、つまり 16151 になります。

パラメータ	設定	説明
ARCHIVE_LOG_RECURSIVE_SE ARCH	（Y / N）	サブディレクトリ内のアーカイブ ログの管理を有効にします。 アーカイブ ログがサブディレクトリの下にある場合は、このパラメータを使用する必要があります。

カスタムのキーと値のペアは、IBM Db2 Linuxプラグイン システムではサポートされますが、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. スナップショット 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。

あなたが望むなら...	操作
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（このオプションはLinuxリソースには適用されません）	• ファイル システムの一貫性を備えたSnapCenter * を選択します。
SnapCenterでストレージ レベルのSnapshotを作成する	• ファイル システムの整合性のないSnapCenter * を選択します。
Snapshotを作成するためにホストで実行するコマンドを入力する	*その他*を選択し、スナップショットを作成するためにホスト上で実行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。

をクリックしてポリシーを作成することもできます + 。

ポリシーが[Configure schedules for selected policies]セクションのリストに表示されます。

b. スケジュールの設定列で*をクリックします。 + * 設定するポリシーの。

c. ポリシー *policy_name* のスケジュールの追加ダイアログ ボックスでスケジュールを構成し、[**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。

構成されたスケジュールは、「適用されたスケジュール」列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複してい

る場合、サポートされません。

8. 通知ページの 電子メール設定 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、設定 > グローバル設定 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。

リソース グループを作成し、 **ASA r2** システム上の **IBM Db2** リソースの二次保護を有効にします。

ASA r2 システム上にあるリソースを追加するには、リソース グループを作成する必要があります。リソース グループの作成時にセカンダリ保護をプロビジョニングすることもできます。

開始する前に

- ONTAP 9.x リソースとASA r2 リソースの両方を同じリソース グループに追加していないことを確認する必要があります。
- ONTAP 9.x リソースとASA r2 リソースの両方を含むデータベースが存在しないことを確認する必要があります。

タスク概要

- 二次保護は、ログインしたユーザーに **SecondaryProtection** 機能が有効になっているロールが割り当てられている場合にのみ使用できます。
- セカンダリ保護を有効にすると、プライマリおよびセカンダリ整合性グループの作成中にリソース グループはメンテナンス モードになります。プライマリおよびセカンダリのコンシステンシー グループが作成されると、リソース グループのメンテナンス モードが解除されます。
- SnapCenter はクローン リソースの二次保護をサポートしていません。

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、[新しいリソース グループ] をクリックします。
3. [Name]ページで、次の操作を実行します。
   a. [Name]フィールドにリソース グループの名前を入力します。

      リソース グループ名は250文字以内で指定する必要があります。

   b. あとでリソース グループを検索できるように、[Tag]フィールドに1つ以上の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。

   c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

d. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。

必要に応じて、プレフィックスを含め、アプリケーションで設定されたのとまったく同じ宛先を使用する必要があります。

4. [リソース] ページで、[ホスト] ドロップダウン リストからデータベース ホスト名を選択します。

[Available Resources]セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources]のリストには表示されません。

5. [使用可能なリソース] セクションからASA r2 リソースを選択し、[選択したリソース] セクションに移動します。
6. アプリケーション設定ページで、バックアップ オプションを選択します。
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。

をクリックし てポリシーを作成することもできます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

b. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。

c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[**OK**] をクリックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

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

8. 選択したポリシーに対して二次保護が有効になっている場合は、「二次保護」ページが表示されるので、次の手順を実行する必要があります。

a. レプリケーション ポリシーのタイプを選択します。

同期レプリケーション ポリシーはサポートされていません。

b. 使用する整合性グループのサフィックスを指定します。

c. [宛先クラスタ] および [宛先 SVM] ドロップダウンから、使用するピア クラスタと SVM を選択します。

クラスターと SVM のピアリングはSnapCenterではサポートされていません。クラスタと SVM のピアリングを実行するには、System Manager またはONTAP CLI を使用する必要があります。

リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは [セカンダリ保護リソース] セクションに表示されます。

1. [Verification]ページで、次の手順を実行します。
   a. ロケータのロード をクリックして、 SnapMirrorまたはSnapVaultボリュームをロードし、セカンダリストレージで検証を実行します。
   b. クリック + ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で をクリックします。
   c. [Add Verification Schedules policy_name]ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

   d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証] を選択します。
   e. [OK]をクリックします。

   設定した検証スケジュールが、[Applied Schedules]列にリストされます。

2. 通知ページの 電子メール設定 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。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。

   Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtpServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

3. 概要を確認し、[完了] をクリックします。

IBM Db2用のPowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成

PowerShellコマンドレットを使用してIBM Db2データベースのバックアップ、リストア、クローニングを行う前に、Storage Virtual Machine（SVM）接続とクレデンシャルを作成する必要があります。

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ロールの権限が必要です。
- 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。

  ストレージ システム接続の追加中は、ホスト プラグインのインストールが進行中であってはなりません。ホスト キャッシュが更新されず、 SnapCenter GUI にデータベースのステータスが「バックアップに使用できません」または「 NetAppストレージ上にありません」と表示される可能性があるためです。

- ストレージ システムの名前は一意である必要があります。

  SnapCenterでは、別々のクラスタに属している場合でも、複数のストレージ システムに同じ名前を付けることはサポートされません。SnapCenterでサポートする各ストレージ システムには、一意な名前とデータLIFの一意なIPアドレスが必要です。

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、新しいクレデンシャルを作成します。

   この例は、Windowsクレデンシャルを使用してFinanceAdminという名前の新しいクレデンシャ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
-EnableSudoPrevileges:$true
```

4. SnapCenter ServerにIBM Db2通信ホストを追加します。

   Linux：

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

   Windows：

```
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：

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

   Windows：

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

6. SQLLIBのパスを設定します。

   Windows の場合、Db2 プラグインは SQLLIB フォルダーのデフォルト パス「C:\Program Files\IBM\SQLLIB\BIN」を使用します。

   デフォルト 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関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

Db2 データベースをバックアップする

データベースをバックアップするときは、SnapCenter Server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。

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関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「`snapmirror all`」権限が含まれている必要があります。ただし、「`vsadmin`」ロールを使用している場合は、「`snapmirror 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、プラグイン ホストで次のパスから使用できるコマンド リストにコマンドがあるかどうかを確認する必要があります。
  - Windows ホスト上のデフォルトの場所: *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*

◦ Linux ホスト上のデフォルトの場所: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

コマンドがコマンド リストに存在しない場合、処理は失敗します。

SnapCenter UI

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 表示 ドロップダウン リストからリソースをフィルターします。

   選択をクリックし、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ーします。次に選択できますフィルター パネルを閉じます。

3. バックアップするリソースを選択します。
4. [リソース] ページで、[スナップショット コピーにカスタム名形式を使用する] を選択し、スナップショット名に使用するカスタム名形式を入力します。

   たとえば、*customtext_policy_hostname* または *resource_hostname* です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

5. [Application Settings]ページで、次の操作を実行します。

   ◦ 追加のバックアップ オプションを設定するには、[バックアップ] 矢印を選択します。

   必要に応じて、整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for "Consistency Group Snapshot" operation to complete	スナップショット操作が完了するまでの待機時間を指定するには、「緊急」、または「中」、または「緩和」を選択します。[Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

   ◦ *スクリプト*矢印を選択して、静止、スナップショット、および静止解除操作の事前および事後コマンドを実行します。

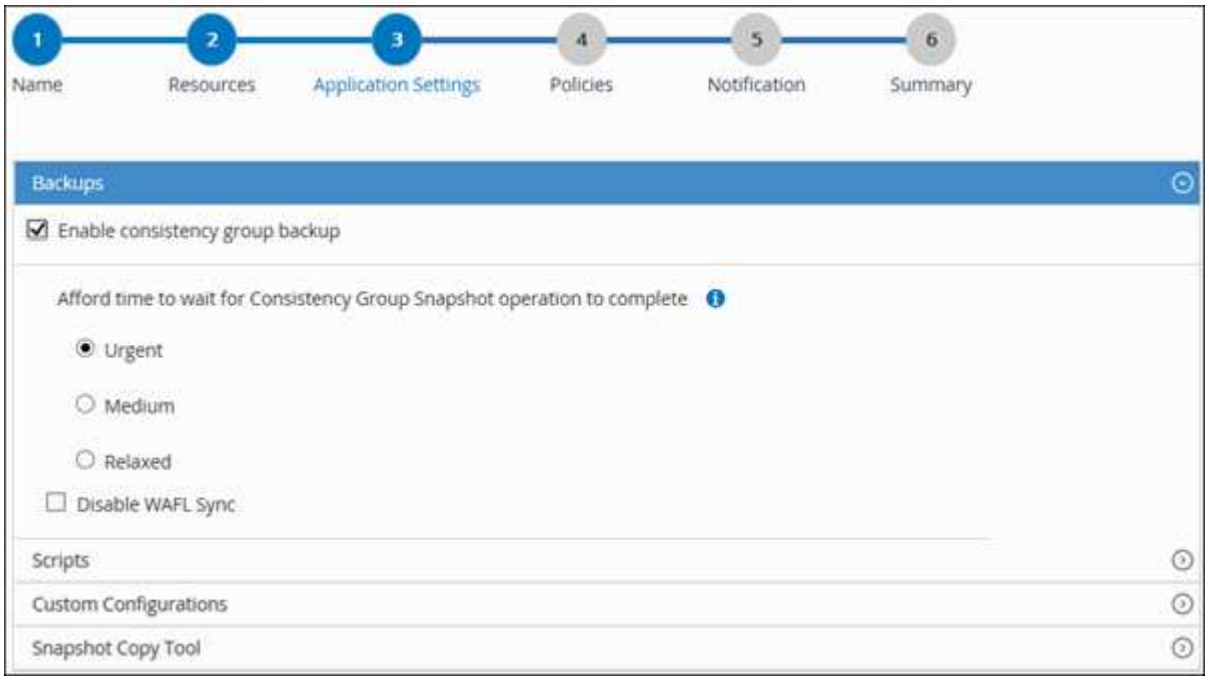
   バックアップ処理を終了する前のプリコマンドも実行できます。プリスクリプトとポストスクリプトはSnapCenter Serverで実行されます。

   ◦ カスタム構成矢印を選択し、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。

   ◦ スナップショット コピー ツール 矢印を選択して、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでストレージ レベルのSnapshotを作成する	• ファイル システムの整合性のないSnapCenter * を選択します。

あなたが望むなら...	操作
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 システムの一貫性を備えたSnapCenter * を選択します。
Snapshotを作成するためのコマンドを入力する	*その他*を選択し、スナップショットを作成するコマンドを入力します。



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。

      をクリックしてポリシーを作成することもできます + 。

      [Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

   b. を選択 + スケジュールを構成するポリシーの [スケジュールの構成] 列で、

   c. ポリシー *policy_name* のスケジュールの追加 ダイアログ ボックスでスケジュールを構成し、[**OK**] を選択します。

      policy_name は選択したポリシーの名前です。

   設定したスケジュールが[Applied Schedules]列にリストされます。

7. 通知ページの 電子メール設定 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、設定 > グローバル設定 でも設定する必要があります。

8. 概要を確認し、[完了] 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]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、[ポリシー] 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、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

    b. *バックアップ*を選択します。

11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

    ◦ MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

      詳細については、以下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関係を検出できない"

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Server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、手動リソースを追加します。

   次の例では、IBM Db2インスタンスを追加する方法を示しています。

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Instance -ResourceName db2inst1 -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"Stora
geSystem"="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";"Stora
geSystem"="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. リソースを保護するか、Add-SmResourceGroupコマンドレットを使用してSnapCenterに新しいリソース グループを追加します。
5. New-SmBackupコマンドレットを使用して、新しいバックアップ ジョブを開始します。

   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
   ```

   次の例では、Db2インスタンスをバックアップしています。

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

   次の例では、Db2データベースをバックアップしています。

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCDB";"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、失敗）を確認します。

```
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、リストアやクローニングの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関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

リソース グループのバックアップ

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。

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関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「`snapmirror all`」権限が含まれている必要があります。ただし、「`vsadmin`」ロールを使用している場合は、「`snapmirror all`」権限は必要ありません。

タスク概要

リソース グループは、[Resources]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行われます。

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、をクリックして、タグを選択します。次に選択できますフィルター パネルを閉じます。
3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] を選択します。
4. [Backup]ページで次の手順を実行します。
   a. リソース グループに複数のポリシーを関連付けた場合は、[ポリシー] 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、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

   b. *バックアップ*を選択します。
5. モニター > ジョブ を選択して、操作の進行状況を監視します。

IBM Db2バックアップ処理の監視

SnapCenterの[Jobs]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、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録
- キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] 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]ページで、次の手順を実行します。
   a. をクリックして、 リストの内容をバックアップ処理だけに絞り込みます。
   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*バックアップ*を選択します。
   d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
   e. 正常に完了した操作を表示するには、[適用] をクリックします。
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は ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

   ログを表示 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]ペインでの**IBM Db2**データベースに対するデータ保護処理の監視

[Activity]ペインには、最後に実行された5つの処理が表示されます。また[Activity]ペインには、処理が開始された日次と処理のステータスが表示されます。

[Activity]ペインには、バックアップ、リストア、クローニング、スケジュールされたバックアップの各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. クリックアクティビティ ペインで、最新の 5 つの操作を表示します。

   いずれかの操作をクリックすると、*ジョブの詳細*ページに操作の詳細が表示されます。

IBM Db2のバックアップ処理のキャンセル

キューに登録されているバックアップ処理は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管理者か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、[モニター] ページまたは [アクティビティ] 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はキャンセルできません。
- バックアップ処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。

- キャンセルできない操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられた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
[Monitor]ページ	a. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 b. 操作を選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	a. バックアップ操作を開始したら、*をクリックします。 * アクティビティ ペインで、最新の 5 つの操作を表示します。 b. 処理を選択します。 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。

処理がキャンセルされ、リソースは処理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。

タスク概要

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）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

-  プライマリ 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表示します。
-  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ているバックアップとクローンの数を表示します。
-  SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップとクローンの数を表示します。

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、バックアップを4個保持するポリシーを使用してバックアップを6個作成した場合、バックアップの数は6個と表示されます。

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。

[Topology]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参照し、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. *概要カード*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の概要を確認します。

   概要カード セクションには、スナップショット コピー ベースのバックアップとクローンの合計数が表示されます。

   更新 ボタンをクリックすると、ストレージのクエリが開始され、正確な数が表示されます。

   SnapLock対応バックアップが取得された場合、[更新] 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も、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

   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有効期限はONTAPから取得されます。

   オンデマンド バックアップ後、[更新] 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更新されます。

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。

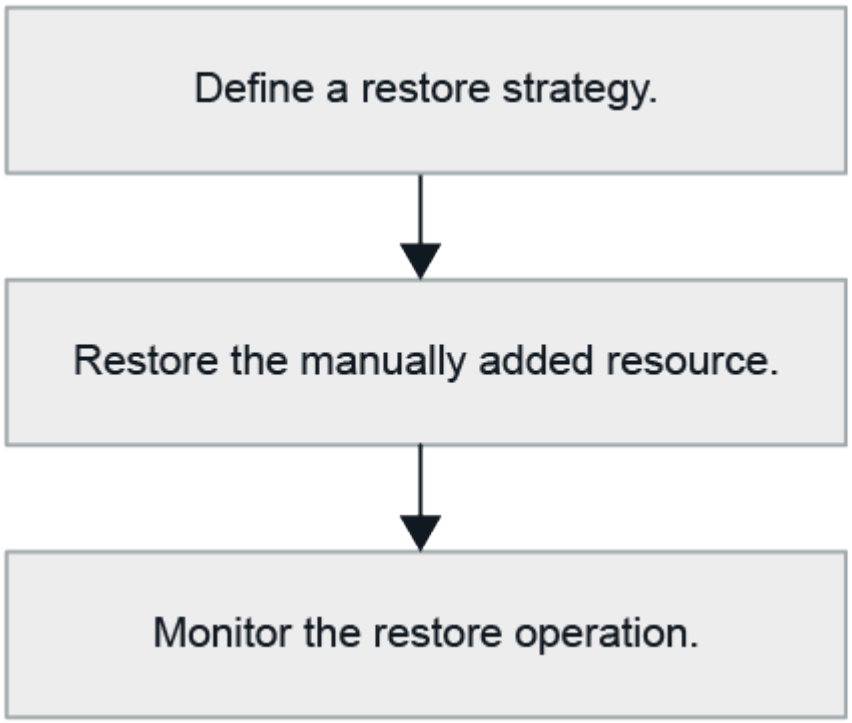
8. クローンを分割する場合は、テーブルからクローンを選択し、 。

IBM Db2のリストア

リストアのワークフロー

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" 。

手動で追加されたリソース バックアップのリストア

SnapCenterを使用して1つまたは複数のバックアップからデータをリストアおよびリカバリすることができます。

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を実行する場合は、プラグイン ホストで

次のパスから使用可能なコマンド 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。

- Windows ホスト上のデフォルトの場所: *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Linux ホスト上のデフォルトの場所: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- 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が、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、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。

SnapCenter UI

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 [表示] ドロップダウン リストからリソースをフィルターします。

   リソースは、タイプ、ホスト、関連するリソース 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。

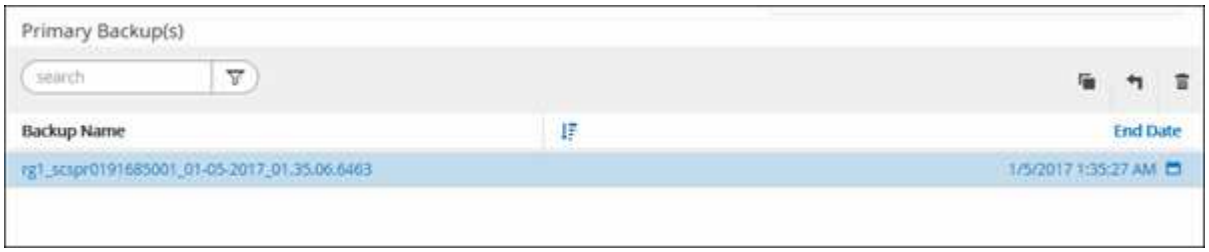
   リストアの実行時は、バックアップがリストア グループに対するものであっても、リストア対象のリソースを個別に選択する必要があります。

   リソースが保護されていない場合は、「全体ステータス」列に「保護されていません」と表示されます。この状態になるのは、リソースが保護されていない場合と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場合です。

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. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボールト化された) ストレージ システムから [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、復元するバックアップを選択し、*をクリックします。 *。



6. 復元範囲ページで、*完全なリソース*を選択します。

   a. *完全なリソース*を選択すると、IBM Db2 データベースのすべての構成済みデータ ボリュームが復元されます。

      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のリストア用のSnapshotが選択されたあとに作成された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。

      複数のLUNを選択できます。

      すべて 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復元されます。

7. [Pre ops]ページで、リストア ジョブの実行前に実行するリストア前の処理とアンマウントのコマン

ドを入力します。

8. [Post ops]ページで、リストア ジョブの実行後に実行するマウントとリストア後の処理のコマンドを入力します。
9. 通知ページの 電子メール設定 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、[設定] > [グローバル設定] ページでも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. モニター > ジョブ をクリックして、操作の進行状況を監視します。

終了後の操作

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

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよび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.sccore.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 -FromDateTime "1/29/2015" -ToDateTime
"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。ここで、UID = <instance_name> は手動で検出された DB2 インスタンス リソース用であり、UID = <instance_name>\<databse_name> は IBM Db2 データベース リソース用です。ResourceIDは、Get-smResourcesコマンドレットで取得できます。

```
Get-smResources  -HostName cn24.sccore.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.sccore.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.sccore.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関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

自動検出されたデータベース バックアップのリストアとリカバリ

SnapCenterを使用して1つまたは複数のバックアップからデータをリストアおよびリカバリすることができます。

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を実行する場合は、プラグイン ホストで次のパスから使用可能なコマンド 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。
  - Windows ホスト上のデフォルトの場所: *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Linux ホスト上のデフォルトの場所: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

ⓘ コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- 自動検出されたリソースについては、SFSR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が、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、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 [表示] ドロップダウン リストからリソースをフィルターします。

   リソースは、タイプ、ホスト、関連するリソース 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 グループに対するものであっても、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。

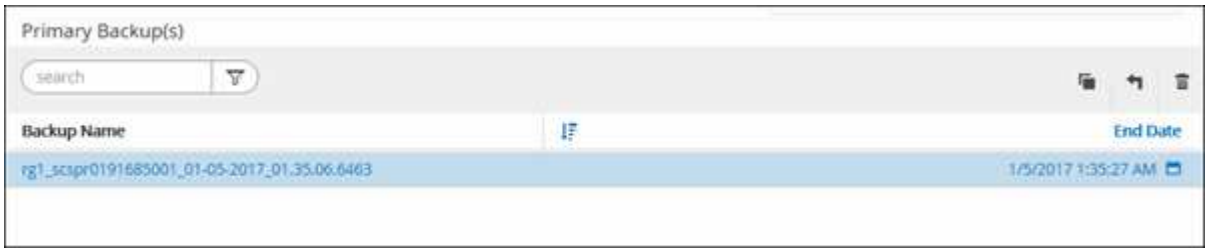
   リソースが保護されていない場合は、「全体ステータス」列に「保護されていません」と表示されます。この状態になるのは、リソースが保護されていない場合とリソースが別のユーザによってバックアップされている場合です。

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. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボールト化された) ストレージ システムから [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、復元するバックアップを選択し、*をクリックします。 *。



6. 「復元範囲」ページで、「完全なリソース」を選択して、IBM Db2 データベースの構成済みデータ ボリュームを復元します。
7. [Pre ops]ページで、リストア ジョブの実行前に実行するリストア前の処理とアンマウントのコマンドを入力します。

   自動検出されたリソースについては、アンマウント コマンドは必須ではありません。

8. [Post ops]ページで、リストア ジョブの実行後に実行するマウントとリストア後の処理のコマンドを入力します。

   自動検出されたリソースについては、マウント コマンドは必須ではありません。

9. 通知ページの 電子メール設定 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、[設定] > [グローバル設定] ページでも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. モニター > ジョブ をクリックして、操作の進行状況を監視します。

終了後の操作

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。

IBM Db2リストア処理の監視

[Job]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発生していないかどうかを確認できます。

タスク概要

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。

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録
- キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] 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. ジョブ ページで、次の手順を実行します。
   a. をクリックし てリストをフィルタリングし、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*復元*を選択します。
   d. *ステータス*ドロップダウンリストから、復元ステータスを選択します。
   e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. 復元ジョブを選択し、[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。

   ログを表示 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リソースのバックアップのクローニング

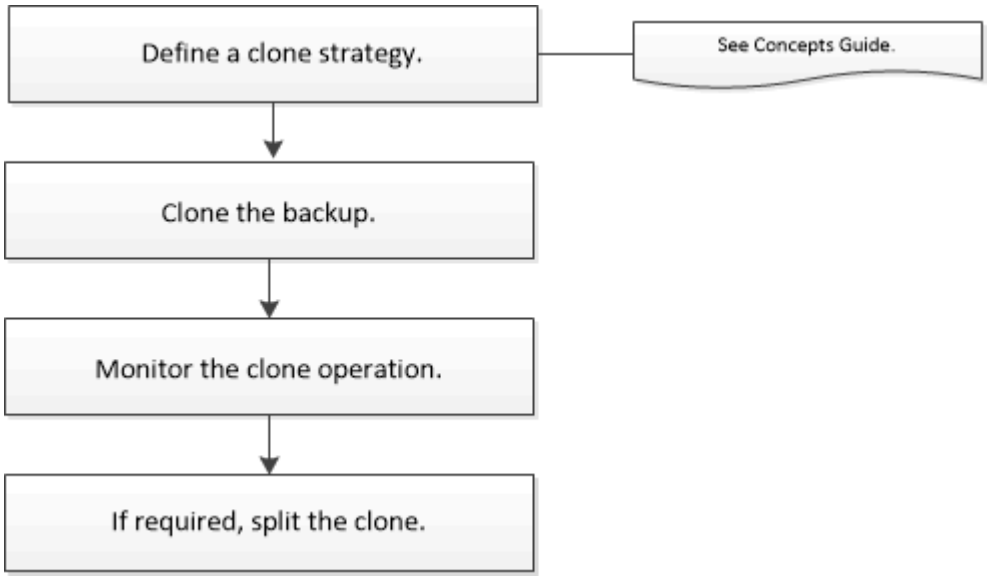
クローニングのワークフロー

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。

タスク概要

- ソースIBM Db2サーバでクローニング処理を実行できます。
- 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。

終了後の操作

自動検出されたDb2リソースをクローニングすると、クローン リソースは手動リソースとしてマークされます。クローンされた Db2 リソースを回復するには、「リソースの更新」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と、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。

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）の割り当て済みアグリゲート リストに含まれていることを確認します。
- 代替ホスト上に Db2 のクローンを作成するときは、他のホスト上の元のマウント パスと同じクローン マウント パスの n-1 ディレクトリ構造を作成する必要があります。マウント パスには *755* 実行権限が必要です。
- クローニング前またはクローニング後のコマンドについては、プラグイン ホストの次のパス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。
  - Windows ホスト上のデフォルトの場所: *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Linux ホスト上のデフォルトの場所: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- FlexCloneボリューム分割操作の詳細については、以下を参照してください。https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html["親ボリュームからのFlexCloneボリュームのスプリット"] 。
- 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が、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、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。

SnapCenter UI

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 [表示] ドロップダウン リストからリソースをフィルターします。

   リソースは、タイプ、ホスト、関連するリソース 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 グループを選択した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. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボールト化された) ストレージ システムから [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、クリックします。  。
6. [Location]ページで、次の操作を実行します。

フィールド	操作
Clone server	クローンをどのホスト上に作成するかを選択します。
Target Clone Instance	既存のバックアップからクローニングするターゲットの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。
Target Clone Name	クローンの名前を入力します。 これは、Db2データベース リソースにのみ該当します。
NFS Export IP Address	クローン ボリュームをエクスポートするホスト名またはIPアドレスを入力します。 これは、NFSストレージ タイプのリソースにのみ該当します。
Capacity Pool Max. Throughput (MiB/s)	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の削除
   - 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`

8. 通知ページの 電子メール設定 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. モニター > ジョブ をクリックして、操作の進行状況を監視します。

終了後の操作

自動検出されたDb2リソースをクローニングすると、クローン リソースは手動リソースとしてマークされます。クローンされた Db2 リソースを回復するには、「リソースの更新」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と、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

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. クローニングできるバックアップの一覧を表示するには、Get-SmBackupコマンドレットか Get-SmResourceGroupコマンドレットを使用します。

   この例では、使用可能なすべてのバックアップに関する情報を表示しています。

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

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

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

この例では、指定したリソース グループとそのリソース、および関連ポリシーに関する情報を表示しています。

```
PS C:\> Get-SmResourceGroup -ListResources –ListPolicies

Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
```

```
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeOut : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
```

```
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. 既存のバックアップからのクローニング処理を開始するには、New-SmCloneコマンドレットを使用します。

   この例では、指定したバックアップからすべてのログを含めてクローンを作成しています。

```
PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

   この例では、指定したMicrosoft SQL Serverインスタンスのクローンを作成しています。

```
PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. クローニング ジョブのステータスを表示するには、Get-SmCloneReportコマンドレットを使用します。

   この例では、指定したジョブIDのクローン レポートを表示しています。

```
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}
```

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、 "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のクローニング処理の監視

SnapCenterのクローニング処理の進捗状況を、[Jobs]ページで監視できます。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発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録
- キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] 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. ジョブ ページで、次の手順を実行します。
   a. をクリックし  てリストをフィルタリングし、クローニング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*クローン*を選択します。
   d. *ステータス*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. 正常に完了した操作を表示するには、[適用] をクリックします。
4. クローンジョブを選択し、[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。

クローンのスプリット

SnapCenterを使用して、クローン 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から独立します。

タスク概要

- 中間クローンではクローン スプリット処理を実行できません。

  たとえば、データベース バックアップからクローン1を作成したあとで、クローン1のバックアップを作成し、そのバックアップ（クローン2）をクローニングできます。クローン2を作成すると、クローン1は中間クローンになり、クローン1ではクローン スプリット処理を実行できなくなります。ただし、クローン2に対してはクローン スプリット処理を実行できます。

  クローン2をスプリットすると、クローン1は中間クローンではなくなるため、クローン1に対してクローン スプリット処理を実行できるようになります。

- クローンをスプリットすると、その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。
- FlexCloneボリューム分割操作の詳細については、以下を参照してください。 "親ボリュームからのFlexCloneボリュームのスプリット" 。
- 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*ページで、表示リストから適切なオプションを選択します。

オプション	説明
データベース アプリケーションの場合	表示リストから*データベース*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. *コピーの管理*ビューから、クローンされたリソース（データベースやLUNなど）を選択し、*をクリックします。  *。
5. 分割するクローンの推定サイズとアグリゲート上で必要な空き容量を確認し、[開始] をクリックします。
6. モニター > ジョブ をクリックして、操作の進行状況を監視します。

   SMCoreサービスが再起動されると、クローン スプリット処理は応答を停止します。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てから、クローン スプリット処理を再試行してください。

   クローンが分割されているかどうかを確認するためのポーリング時間を長くしたり短くしたりする場合は、*SMCoreServiceHost.exe.config* ファイルの *CloneSplitStatusCheckPollTime* パラメータの値を変更して、SMCore がクローン分割操作のステータスをポーリングする時間間隔を設定できます。値はミリ秒単位で、デフォルト値は5分です。

   例えば：

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

   バックアップ、リストア、または別のクローン スプリットが実行中の場合、クローン スプリットの開始処理は失敗します。クローン スプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

"アグリゲートが存在しないためにSnapCenterのクローニングや検証が失敗する"

SnapCenterアップグレード後のIBM Db2データベースのクローンの削除またはスプリット

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。クローンを作成したリソースの[Topology]ページで、クローンの削除やスプリットを実行できます。

タスク概要

非表示のクローンのストレージ フットプリントを見つける場合は、次のコマンドを実行します。 `Get-SmClone -ListStorageFootprint`

手順

1. remove-smbackup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. [Resources]ページで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]ビューで、プライマリまたはセカンダリ（ミラー先またはレプリケート先）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、クリックします  クローンを削除するには、または  クローンを分割します。
7. [OK]をクリックします。