NetAppがサポートするプラグインを使用してアプリケーションを保護する

SnapCenter software

NetApp
November 06, 2025

目次

NetAppがサポートするプラグインを使用してアプリケーションを保護する

NetAppがサポートしているプラグイン

NetAppがサポートしているプラグインの概要

使用するアプリケーションには、MongoDB、ORASCPM (Oracle アプリケーション)、SAP ASE、SAP MaxDB、ストレージ プラグインなどのNetApp対応プラグインを使用し、 SnapCenterを使用してこれらのアプリケーションをバックアップ、復元、またはクローン化できます。NetAppがサポートしているプラグインは、NetApp SnapCenterソフトウェアのホスト側コンポーネントとして動作し、アプリケーションに対応したリソースのデータ保護と管理を提供します。

NetAppがサポートしているプラグインをインストールすると、SnapCenterとNetApp SnapMirrorテクノロジを使用して別のボリュームのバックアップ セットのミラー コピーを作成し、NetApp SnapVaultテクノロジを使用して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。NetAppがサポートしているプラグインは、WindowsとLinuxのどちらの環境でも使用できます。

SnapCenterCLIでは、NetAppがサポートしているプラグイン コマンドはサポートされません。

NetApp は、 SnapCenterに組み込まれたプラグイン フレームワークを使用してONTAPストレージ上のデータボリュームのデータ保護操作を実行するためのストレージ プラグインを提供します。

NetAppでサポートされているプラグインは、「ホストの追加」ページからインストールできます。

"ホストを追加し、リモート ホストにプラグイン パッケージをインストールします。"

SnapCenterサポート ポリシーは、プラグイン フレームワーク、コア エンジン、および関連 API のサポートをカバーします。プラグインのソース コードおよびプラグイン フレームワーク上に構築された関連スクリプトはサポートの対象外となります。

NetAppがサポートしているプラグインの機能

データ保護操作には、MongoDB、ORASCPM、Oracle Applications、SAP ASE、SAP MaxDB、ストレージ プラグインなどのNetAppがサポートするプラグインを使用できます。

- データベース、インスタンス、ドキュメント、表領域などのリソースを追加します。
- 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。

データ保護操作には、 NetAppがサポートするプラグインを使用できます。

- ONTAPクラスタ間でストレージ ボリュームの整合グループSnapshotを作成します。
- 組み込みのプレ / ポスト スクリプト フレームワークを使用して、カスタム アプリケーションをバックアップします。

  ONTAPボリューム、LUN、またはqtreeをバックアップできます。

- SnapCenterポリシーを使用して、既存のレプリケーション関係（SnapVault / SnapMirror /ユニファイドレプリケーション）を利用して、プライマリで作成されたSnapshotをONTAPセカンダリに更新します。

  ONTAPプライマリおよびセカンダリには、 ONTAP FAS、 AFF、 ASA、 ONTAP Select、またはCloud Volumes ONTAP を使用できます。

- ONTAPボリューム、LUN、またはファイル全体をリカバリします。

  ブラウズ機能またはインデックス機能が製品に組み込まれていないため、それぞれのファイル パスを手動で指定する必要があります。

  qtreeまたはディレクトリのリストアはサポートされていませんが、バックアップ範囲がqtreeレベルで定義されている場合は、qtreeに限りクローニングとエクスポートを実行できます。

NetAppがサポートしているプラグインの特長

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。MongoDB、ORASCPM (Oracle アプリケーション)、SAP ASE、SAP MaxDB、ストレージ プラグインなどのNetApp対応プラグインを操作するには、 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、リカバリ、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**スナップショットテクノロジー

  SnapCenterでは、NetAppがサポートしているプラグインで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。Snapshotはストレージ スペースを最小限しか消費しません。

NetAppがサポートするプラグインには、次のような利点もあります。

- 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。
- Windows環境でファイルシステムと整合性のあるSnapshotを作成できます。

NetAppがサポートしているプラグイン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。NetAppがサポートしているプラグイン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
VMホストへの物理およびNFSの直接マウント（VMDKとRDM LUNはサポートされていません）。	FC接続LUN
VMホストへの物理およびNFSの直接マウント（VMDKとRDM LUNはサポートされていません）。	iSCSI接続LUN
VMホストへの物理およびNFSの直接マウント（VMDKとRDM LUNはサポートされていません）。	NFS接続ボリューム
VMware ESXi	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。

NetAppがサポートしている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 attribute show
  - lun create
  - lun delete
  - lun geometry
  - lun igroup add
  - lun igroup create
  - lun igroup delete
  - 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 resize
  - lun serial
  - lun show
  - ネットワークインターフェース
  - 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 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 create
- vserver export-policy delete
- vserver export-policy rule create
- vserver export-policy rule show
- vserver export-policy show

- 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

NetAppがサポートしているプラグインでSnapMirrorおよびSnapVaultレプリケーションを使うためのストレージ 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" 。

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確実に作成できます。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. 整合グループSnapshotを保持するかどうかを決定し、保持する場合は整合グループSnapshotを削除する適切なオプションを決定します。
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。

NetAppがサポートしているプラグインのバックアップ戦略

NetAppがサポートしているプラグイン リソースのバックアップ スケジュール

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。リソースをバックアップする回数が多いほど、リストア時にSnapCenterが使用する必要のあるアーカイブ ログの数が少なくなります。これにより、リストア処理の時間を短縮できます。

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。

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。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とRPOは、データ保護戦略に関与します。

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

  バックアップ頻度（バックアップを実行する間隔）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。SnapCenter GUI で [設定] > [ポリシー] をクリックすると、ポリシーにアクセスできます。

- バックアップ スケジュール

  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）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。SnapCenter GUI でリソース グループのスケジュールにアクセスするには、[リソース] をクリックし、適切なプラグインを選択して、[表示] > [リソース グループ] をクリックします。

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。

通常、選択するバックアップ ジョブの数は、リソースが配置されているボリュームの数に応じて決まります。たとえば、あるボリュームに小規模なリソースのグループを配置しており、別のボリュームに1つの大規模なリソースを配置している場合は、小規模なリソース用のバックアップ ジョブと大規模なリソース用のバックアップ ジョブを1つずつ作成できます。

手動で追加した**NetApp**がサポートしているプラグイン 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NetAppがサポートしているプラグイン リソースのリストア戦略には、2つのタイプがあります。

手動で追加したNetAppがサポートしているプラグイン 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。

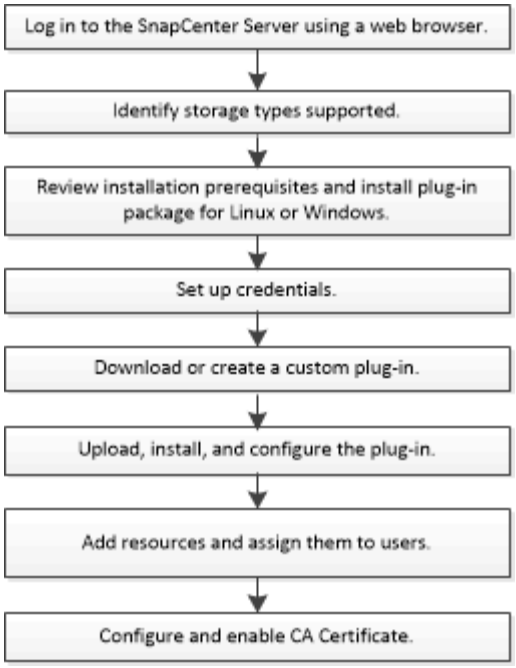
ファイルレベルのリストア

- ボリューム、qtree、またはディレクトリからファイルをリストア
- 選択したLUNのみをリストア

NetAppがサポートしているプラグインのインストール準備

SnapCenter NetAppがサポートしているプラグインのインストール ワークフロー

NetAppがサポートしているプラグイン リソースを保護する場合は、NetAppがサポートしているSnapCenterプラグイン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。NetAppがサポートするプラグインは、Windows、Linux、および AIX 環境でサポートされます。

ストレージおよび Oracle アプリケーションは AIX でサポートされます。

- Linux、Windows、または AIX ホストに Java 11 がインストールされている必要があります。

  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。
- MongoDB、ORASCPM、Oracle Applications、SAP ASE、SAP MaxDB、ストレージ プラグインなどのNetAppでサポートされているプラグインは、ホスト追加操作が実行されるクライアント ホストで使用できる必要があります。

全般

iSCSIを使用している場合は、iSCSIサービスが実行されている必要があります。

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。
- SnapCenterでクラスタ ノードを管理する場合は、クラスタ内のすべてのノードに対する管理者権限があるユーザが必要です。

- Microsoft Windows 用のSnapCenterプラグインを手動で選択する必要があります。

  "Windows用JAVAをダウンロード"

Linuxおよび**AIX**ホスト

ストレージおよび Oracle アプリケーションは AIX でサポートされます。

- 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Linuxホストにインストールしておく必要があります。

  SnapCenter ServerホストにWindows Server 2019またはWindows Server 2016を使用している場合は、Java 11をインストールする必要があります。要件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。

  "Linux用JAVAをダウンロード"

  "AIX用JAVAをダウンロード"

  "NetApp Interoperability Matrix Tool"

- 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。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。

  Sudoバージョン1.8.7以降を使用していることを確認します。

```
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
```

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ホストの要件

SnapCenter Plug-ins Package for AIXをインストールする前に、ホストが要件を満たしていることを確認する必要があります。

ストレージおよび Oracle アプリケーションは AIX でサポートされます。

SnapCenter Plug-ins Package for AIXに含まれているSnapCenter Plug-in for UNIXでは、同時ボリューム グループはサポートされません。

項目	要件
オペレーティング システム	AIX 7.1以降
ホスト上のSnapCenterプラグインに必要な最小RAM	4 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 IBM Java 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" 。

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
- */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" 。

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	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 Java 11 Oracle Java および OpenJDK は、SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp対応プラグイン、および Windows ホストにインストールできるその他のカスタム アプリケーションにのみ必要です。 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" 。

Linuxおよび**AIX**用の**SnapCenter**プラグインパッケージをインストールするためのホスト要件

Linux または AIX 用のSnapCenterプラグイン パッケージをインストールする前に、ホストが要件を満たしていることを確認する必要があります。

ストレージおよび Oracle アプリケーションは AIX でサポートされます。

項目	要件
オペレーティング システム	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server（SLES）
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB

項目	要件
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または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"

NetAppがサポートしているプラグイン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。

開始する前に

- LinuxまたはAIXホスト

  Linux または AIX ホストにプラグインをインストールするための資格情報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。

- NetAppがサポートしているプラグイン アプリケーション

  プラグインは、選択または作成されたクレデンシャルをリソースの追加時に使用します。データ保護操作中にリソースが資格情報を必要としない場合は、資格情報を なし に設定できます。

タスク概要

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. *資格情報*ページで、資格情報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	認証に使用するパスワードを入力します。
Authentication Type	使用する認証タイプを選択します。

フィールド	操作
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 および AIX ユーザーのみに適用されます。

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。

NetAppがサポートしているプラグインのインストール

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

ホストを追加するには、 SnapCenter のホストの追加ページを使用し、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

- この操作は、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。

- 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。
- 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以降でカスタム アプリケーションのグループ管理サービス アカウントを設定する"

- Windows ホストの場合は、必ず Windows 用SnapCenterプラグインを選択する必要があります。

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。
- クラスタ（WSFC）にプラグインをインストールする場合、プラグインはクラスタのすべてのノードにインストールされます。

手順

1. 左側のナビゲーション ペインで、[ホスト] を選択します。
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*を選択します。
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 タイプを選択します。 • Windows • Linux • AIX NetAppがサポートするプラグインは、Windows、Linux、AIX 環境で使用できます。 ストレージおよび Oracle アプリケーションは AIX でサポートされます。

フィールド	操作
ホスト名	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。 Windows環境の場合、信頼されないドメイン ホストのIPアドレスがサポートされるのは、そのIPアドレスがFQDNに解決される場合のみです。 スタンドアロン ホストのIPアドレスまたはFQDNを入力できます。 SnapCenterを使用してサブドメインの一部であるホストを追加する場合は、FQDNを指定する必要があります。
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名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. *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。

   リストから次のプラグインをインストールできます。

   - MongoDB
   - ORASCPM（Oracle Applicationsとして表示）
   - SAP ASE
   - SAP MaxDB
   - ストレージ

6. (オプション) 他のプラグインをインストールするには、[その他のオプション] を選択します。

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	NetAppがサポートするプラグインは、Windows システムまたは Linux システムのいずれかにインストールできます。 • 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SnapCenterプラグインパッケージおよびAIX用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`。 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。

フィールド	操作
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*を選択します。

「事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、ホストがプラグインのインストール要件を満たしているかどうかを確認するための検証が行われます。ディスク容量、RAM、PowerShellバージョン、.NETバージョン、場所（Windowsプラグインの場合）、Javaバージョン（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。

エラーがディスク容量またはRAMに関連している場合は、次の場所にあるweb.configファイルを更新できます。 `C:\Program Files\NetApp\SnapCenter WebApp`デフォルト値を変更します。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SnapManager.Web.UI.dll.config を更新する場合は、両方のノードでファイルを更新し、 SnapCenterアプリケーション プールを再起動する必要があります。

Windowsのデフォルトパスは `C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config`

Linuxのデフォルトパスは `/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config`

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] を選択します。

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。

インストール固有のログファイルは次の場所にあります。 `/custom_location/snapcenter/`ログ。

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

Install-SmHostPackage PowerShell コマンドレットを使用して、Linux、Windows、または AIX 用のSnapCenterプラグイン パッケージを複数のホストに同時にインストールできます。

開始する前に

ホストを追加するユーザには、ホストに対する管理権限が必要です。

ストレージおよび Oracle アプリケーションは AIX でサポートされます。

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**NetApp**がサポートしているプラグインのインストール

NetAppがサポートしているプラグインは、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NetAppがサポートしているプラグインをインストールできます。

手順

1. C:\ProgramData\NetApp\SnapCenter\Package RepositoryにあるSnapCenter Plug-ins Package for Linuxのインストール ファイル（snapcenter_linux_host_plugin.bin）を、NetAppがサポートしているプラグインのインストール先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. 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" 。

5. SnapCenterにログインし、UIまたはPowerShellコマンドレットを使用して、NetAppがサポートしているプラグインをアップロードします。

   NetAppがサポートするプラグインは、UIからアップロードできます。"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"セクション。

   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" 。

NetAppがサポートしているプラグインのインストール 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**NetApp**がサポートしているプラグイン 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**NetApp**がサポートしているプラグイン 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

NetAppがサポートしているプラグインを使用するための前提条件

ユーザがSnapCenter NetAppがサポートしているプラグイン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。
- ホストを追加し、プラグインをインストールしてアップロードします。
- 必要に応じて、Java 11をプラグインのホストにインストールします。
- データ パス（LIF）が複数ある場合、またはdNFS構成を使用している場合は、データベース ホストでSnapCenter CLIを使用して次の作業を実行できます。
  - デフォルトでは、データベース ホストのすべての IP アドレスが、クローン ボリュームのストレージ仮想マシン (SVM) の NFS ストレージ エクスポート ポリシーに追加されます。IPアドレスを1つにするか、一部のIPアドレスに制限する場合は、Set-PreferredHostIPsInStorageExportPolicy CLIを実行します。
  - SVM に複数のデータ パス (LIF) がある場合、 SnapCenter はNFS クローン ボリュームをマウントするための適切なデータ パス (LIF) を選択します。ただし、データ パス（LIF）を1つに特定する場合は、Set-SvmPreferredDataPath CLIを実行する必要があります。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 リファレンス ガイド" 。
- 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。
- ポート9090がホストの他のアプリケーションで使用されていないことを確認します。

  SnapCenterで必要な他のポートに加え、ポート9090をNetAppがサポートしているプラグイン用に確保しておく必要があります。

NetAppがサポートしているプラグイン リソース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、SnapCenterでバックアップやクローンを作成するデータベース、Windowsファイルシステム、VMなどです。
- SnapCenterリソース グループは、ホストまたはクラスタ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、コピーの保持、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。

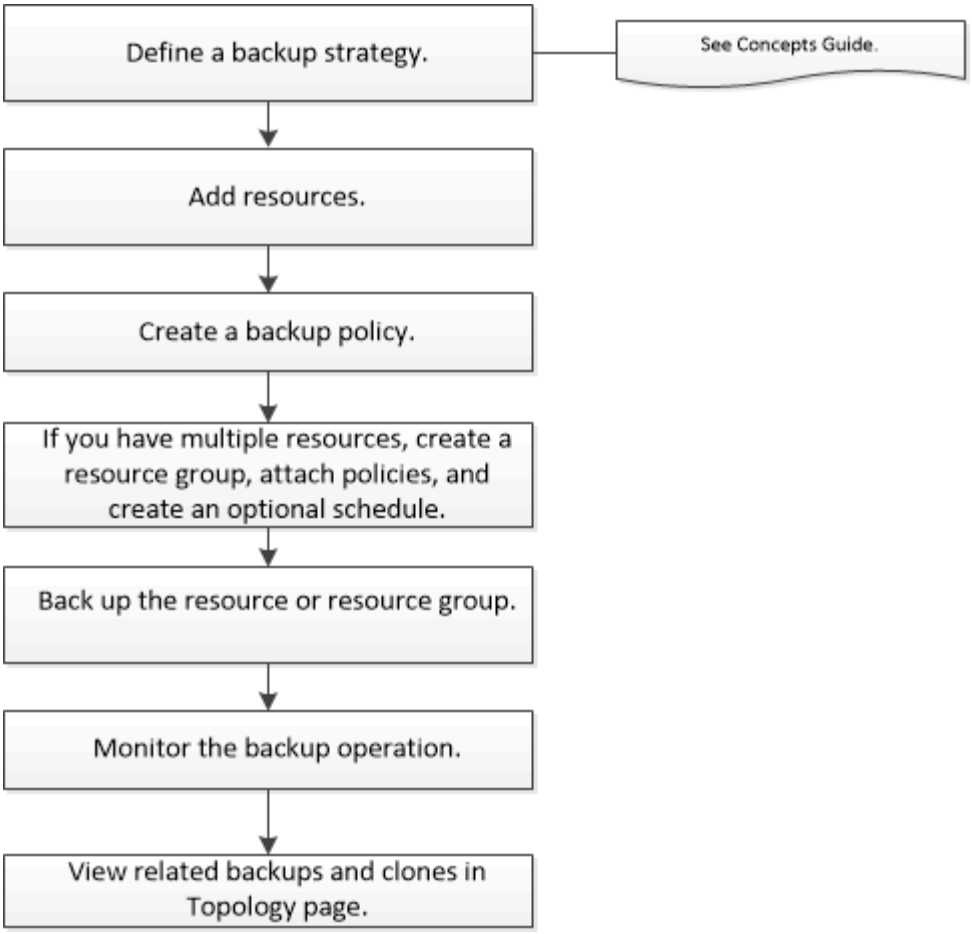
リソース グループは、保護する対象と、それを日時でいつ保護するかを定義するものと考えてください。ポリシーとは、それをどのように保護したいかを定義するものと考えてください。たとえば、すべてのデータベースまたはホストのすべてのファイルシステムをバックアップする場合、すべてのデータベースまたはホストのすべてのファイルシステムを含むリソース グループを作成します。このリソース グループに、日次ポリシーと毎時ポリシーの2つのポリシーを適用します。リソース グループを作成してポリシーを適用する際に、ファイルベースのバックアップを1日1回実行するようにリソース グループを設定し、別のスケジュールでSnapshotベースのバックアップを1時間おきに実行するように設定します。

NetAppがサポートしているプラグイン リソースのバックアップ

NetAppがサポートしているプラグイン リソースのバックアップ

バックアップのワークフローには、計画、バックアップするリソースの特定、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コマンドレットのヘルプを使用するか、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド"

NetAppがサポートしているプラグインへのリソースの追加

バックアップまたはクローンを作成するリソースを追加する必要があります。環境によっては、バックアップまたはクローンを作成するデータベース インスタンスやそのコレクションもリソースに含まれます。

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、クレデンシャルの追加などのタスクを完了しておく必要があります。
- SnapCenter Serverにプラグインをアップロードしておく必要があります。

手順

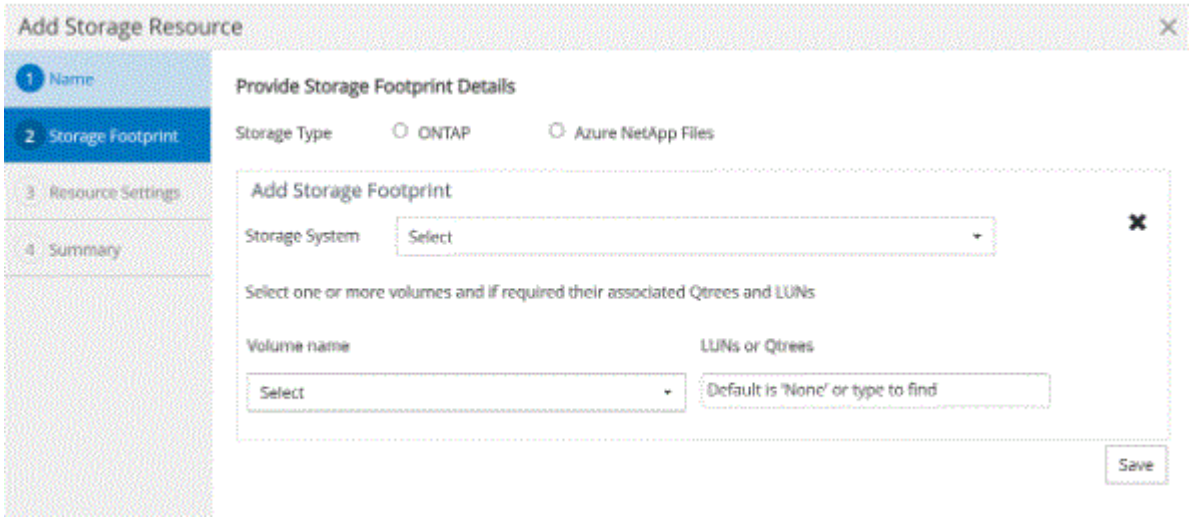
1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[リソースの追加] を選択します。
3. [Provide Resource Details]ページで、次の操作を実行します。

フィールド	操作
Name	リソースの名前を入力します。
ホスト名	ホストを選択します。
タイプ	タイプを選択します。タイプは、プラグイン定義ファイルにあるユーザ定義のタイプです。たとえば、データベースやインスタンスなどになります。 選択したタイプに親がある場合は、親の詳細を入力します。たとえば、タイプがデータベースでその親がインスタンスの場合、インスタンスの詳細を入力します。
資格情報名	クレデンシャルを選択するか、新しいクレデンシャルを作成します。
Mount Paths	リソースのマウント先のマウント パスを入力します。これは、Windowsホストにのみ適用されます。

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 システムを選択し、1 つ以上のボリューム、LUN、および qtree を選択して、[保存] を選択します。

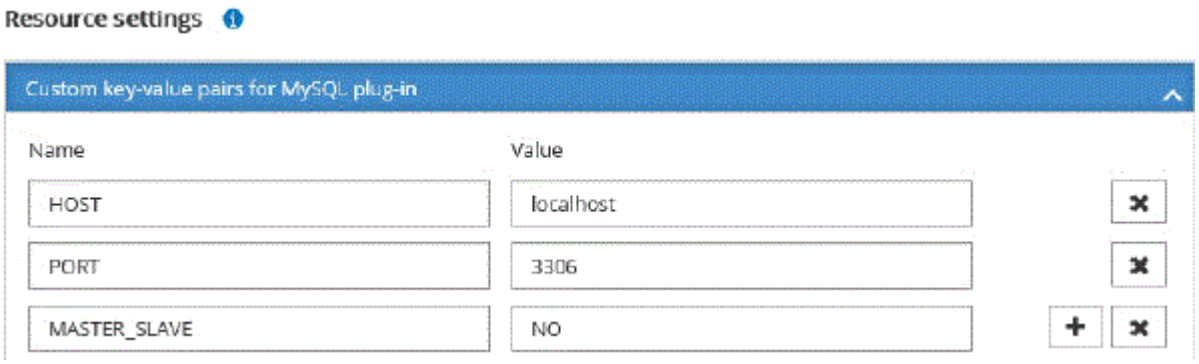
   オプション: + アイコンをクリックして、他のストレージ システムからボリューム、LUN、qtree を追加します。

   NetAppがサポートしているプラグインでは、リソースの自動検出はサポートされていません。物理環境と仮想環境のストレージの詳細も自動検出されません。リソースの作成時に、物理環境と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。



5. [Resource Settings]ページで、リソースのカスタムのキーと値のペアを指定します。

カスタム キー名が大文字であることを確認します。



それぞれのプラグインパラメータについては、"リソースを設定するためのパラメータ"

6. 概要を確認し、[完了] を選択します。

結果

リソースは、タイプ、ホストまたはクラスタ名、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。

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。

終了後の操作

アセットへのアクセスを他のユーザに許可する場合は、SnapCenter管理者が対象のユーザにアセット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。

リソースを追加したあとで、リソースの詳細を変更できます。NetAppがサポートしているプラグイン リソースにバックアップが関連付けられている場合、リソース名、リソース タイプ、およびホスト名のフィールドを変更することはできません。

リソースを設定するためのパラメータ

プラグインを手動で追加する場合は、[Resource Settings]ページで次のパラメータを使用してリソースを設定できます。

Plug-in for MongoDB

Resource Settings：

- MongoDB_APP_SERVER=（リソース タイプが共有クラスタの場合）またはMongoDB_ReplicaSet_SERVER=（リソース タイプがレプリカセットの場合）
- OPLOG_PATH=（MongoDB.propertiesfileから指定する場合はオプション パラメータ）
- MONGODB_AUTHENTICATION_TYPE=（LDAP認証の場合はPLAIN、それ以外の場合はNone）

MongoDB.propertiesファイルには、次のパラメータを指定する必要があります。

- DISABLE_STARTING_STOPPING_SERVICES=

- N：プラグインによってサービスの開始と停止が実行される場合。
- サービスの開始/停止がユーザーによって実行される場合は Y。
- オプション パラメータのデフォルト値はNに設定されています。

- OPLOG_PATH_= (SnapCenterでカスタムのキーと値のペアとしてすでに提供されている場合のオプションのパラメーター)。

Plug-in for MaxDB

Resource Settings：

- XUSER_ENABLE (Y|N)は、データベース ユーザがパスワードを要求されないように、MaxDBでxuserの使用を有効または無効にします。
- HANDLE_LOGWRITER (Y|N)は、ログライターの一時停止（N）またはログライターの再開（Y）の処理を実行します。
- DBMCLICMD (path_to_dbmcli_cmd)は、MaxDB dbmcliコマンドへのパスを指定します。設定されていない場合は、検索パスでdbmcliが使用されます。

Windows環境では、パスを二重引用符（"…"）で囲む必要があります。

- SQLCLICMD (path_to_sqlcli_cmd)は、MaxDB sqlcliコマンドへのパスを指定します。パスが設定されていない場合は、検索パスでsqlcliが使用されます。
- MaxDB_UPDATE_HIST_LOG (Y|N)は、MaxDB履歴ログを更新するかどうかを、MaxDBバックアップ プログラムに指示します。
- MAXDB_CHECK_SNAPSHOT_DIR: 例、SID1:directory[,directory…]; [SID2:directoary[,directory…] は、Snap Creator スナップショット コピー操作が成功したことを確認し、スナップショットが作成されたことを確認します。

  これはNFSにのみ該当します。ディレクトリは、.snapshotディレクトリが格納されている場所を指している必要があります。複数のディレクトリをカンマで区切って指定できます。

  MaxDB 7.8以降のバージョンでは、データベースのバックアップ要求はバックアップ履歴でFailedとマークされます。

- MAXDB_BACKUP_TEMPLATES: 各データベースのバックアップ テンプレートを指定します。

  テンプレートが存在し、外部タイプのバックアップ テンプレートである必要があります。MaxDB 7.8以降でSnapshot統合を有効にするには、MaxDBバックグラウンド サーバ機能があり、外部タイプのMaxDBバックアップ テンプレートがすでに設定されている必要があります。

- MAXDB_BG_SERVER_PREFIX: バックグラウンド サーバー名のプレフィックスを指定します。

  MAXDB_BACKUP_TEMPLATESパラメータが設定されている場合は、MaxDB_BG_SERVER_PREFIXパラメータも設定する必要があります。プレフィックスを設定しない場合は、デフォルト値 na_bg_ が使用されます。

SAP ASE 用プラグイン

Resource Settings：

- SYBASE_SERVER（data_server_name）には、Sybaseデータ サーバ名を指定します（isqlコマンドの-Sオプション）。たとえば、p_testのように指定します。
- SYBASE_DATABASES_EXCLUDE（db_name）では、「all」要素を使用するとデータベースを除外できます。

  複数のデータベースを指定するには、セミコロンで区切ったリストを使用します。例：pubs2;test_db1。

- SYBASE_USER: user_nameには、isqlコマンドを実行できるオペレーティング システム ユーザを指定します。

  UNIXの場合は必須です。このパラメータは、Snap Creator Agentのstartコマンドとstopコマンドを実行するユーザ（通常はrootユーザ）とisqlコマンドを実行するユーザが異なる場合に必須です。

- SYBASE_TRAN_DUMP db_name:directory_pathは、Snapshotの作成後にSybaseトランザクション ダンプを実行できるようにします。例：pubs2:/sybasedumps/ pubs2

  トランザクション ダンプが必要な各データベースを指定する必要があります。

- Sybase_Tran_dump_compress (Y|N)は、Sybaseトランザクション ダンプのネイティブ圧縮を有効または無効にします。
- Sybase_ISQL_CMD（例：/opt/Sybase/OCS-15_0/bin/isql）は、isqlコマンドへのパスを定義します。
- SYBASE_EXCLUDE_TEMPDB (Y|N)を使用すると、ユーザが作成した一時データベースを自動的に除外できます。

Plug-in for Oracle Applications（ORASCPM）

Resource Settings：

- SQLPLUS_CMDには、SQLplusへのパスを指定します。
- ORACLE_DATABASESは、バックアップするOracleデータベースと対応するユーザ（database:user）を一覧表示します。
- CNTL_FILE_BACKUP_DIRには、制御ファイルのバックアップ先ディレクトリを指定します。
- ORA_TEMPには、一時ファイルのディレクトリを指定します。
- ORACLE_HOMEには、Oracleソフトウェアがインストールされているディレクトリを指定します。
- ARCHIVE_LOG_ONLYには、アーカイブ ログをバックアップするかどうかを指定します。
- ORACLE_BACKUPMODE は、オンライン バックアップを実行するかオフライン バックアップを実行するかを指定します。
- ORACLE_EXPORT_PARAMETERS は、*/bin/su <sqlplus* を実行しているユーザー> *-c sqlplus /nolog <cmd>* の実行中に、上記で定義された環境変数を再エクスポートするかどうかを指定します。これは通常、sqlplus を実行しているユーザーが、*connect / as sysdba* を使用してデータベースに接続するために必要なすべての環境変数を設定していない場合に発生します。

NetAppがサポートしているプラグイン リソースのポリシーの作成

SnapCenterを使用してNetAppがサポートしているプラグイン固有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。

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、NetAppがサポートしているプラグインのデータ保護戦略の定義に関する説明を参照してください。

- データ保護の準備が完了している必要があります。

  データ保護の準備作業には、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があります。

- ミラー処理またはバックアップ処理を実行するには、Storage Virtual Machine（SVM）をユーザに割り当てる必要があります。

  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。

- 保護するリソースを手動で追加しておく必要があります。

タスク概要

- 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。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。
- ポリシーで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。
- 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。

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

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は、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、次の手順を実行します。

   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 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。

   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、バックアップ タイプ 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。

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。 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。 最大保持値は 1018 です。保持数を、使用しているONTAPバージョンがサポートする値よりも大きい値に設定すると、バックアップが失敗します。
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。

b. ポリシーラベルを選択します。

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
ローカル スナップショット コピーを作成した後、**SnapMirror** を更新します	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。 ONTAPの保護関係のタイプがミラーとバックアップの場合、このオプションのみを選択すると、プライマリで作成されたSnapshotがデスティネーションに転送されませんが、デスティネーションのリストに表示されます。このスナップショットを復元操作を実行するために宛先から選択すると、次のエラー メッセージが表示されます: 選択したボールト/ミラー バックアップにはセカンダリ ロケーションは使用できません。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。 トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 見る"[TopologyページでのNetAppがサポートしているプラグイン リソースに関連するバックアップとクローンの表示"] 。

フィールド	操作
ローカルスナップショットコピーを作成した後、**SnapVault** を更新します	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。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。トポロジ ページの 更新 ボタンをクリックすると、 ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 SnapLock がSnapLock Vault と呼ばれるONTAPのセカンダリにのみ設定されている場合、[トポロジ] ページの [更新] ボタンをクリックすると、 ONTAPから取得されたセカンダリのロック期間が更新されます。 SnapLock Vault の詳細については、「Vault の保存先でスナップショットを WORM にコミットする」を参照してください。 見る"[Topology]ページでのNetAppがサポートしているプラグイン リソースに関連するバックアップとクローンの表示"] 。
エラー再試行回数	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。これを使用することで、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。

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. [Resources]ページで、[New Resource Group]を選択します。
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。 注意: リソース グループ名は 250 文字を超えてはなりません。
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* または *resource group_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。

4. オプション: [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。

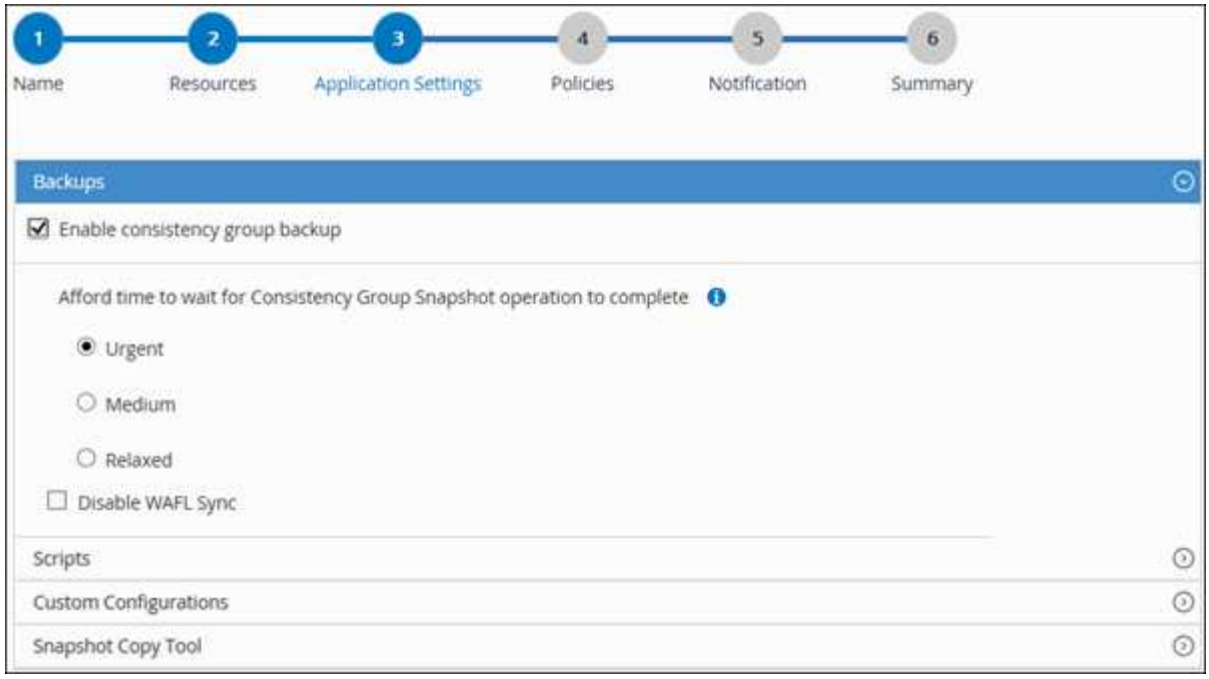
5. *利用可能なリソース*セクションからリソースを選択し、右矢印を選択してそれらを*選択したリソース*セクションに移動します。
6. オプション: アプリケーション設定 ページで、次の操作を行います。

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

      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	Snapshot処理が完了するまでの待機時間として、[Urgent]、[Medium]、または[Relaxed]のいずれかを選択します。 [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. [Scripts]の矢印を選択し、休止、Snapshot、および休止解除の処理を行うプリコマンドとポスト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. [Custom Configurations]の矢印を選択し、このリソースを使用するすべてのデータ保護処理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。

c. 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。 このオプションは、SnapCenter Plug-in for SAP HANA Databaseには適用されません。
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。

を選択してポリシーを作成することもできます + 。

ポリシーは、「選択したポリシーのスケジュールを構成する」セクションにリストされます。

b. スケジュールの設定*列で*を選択します + 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。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] を選択します。

リソース グループを作成し、 **ASA r2** システム上の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。

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データ保護処理を実行するには、Storage Virtual Machine（SVM）接続とクレデンシャルを作成しておく必要があります。

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、一意な名前と管理LIFの一意なIPアドレスが必要です。

手順

1. Open-SmConnectionコマンドレットを使用して、PowerShell Core接続セッションを開始します。

   PowerShellセッションを開く例を次に示します。

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

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。

   新しいストレージ システム接続を作成する例を次に示します。

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -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。

   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例を次に示します。

   ```
   PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

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" 。

NetAppがサポートしている個々のプラグイン リソースのバックアップ

どのリソース グループにも含まれていない、NetAppがサポートしているプラグイン リソースは、[Resources]ページから個別にバックアップすることができます。リソースのバックアップはオンデマンドで実行できるほか、リソースにポリシーが適用されてスケジュールが設定されていれば、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。

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。

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。

   クリック  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。そのあとにをクリックすると、フィルタ ペインが閉じます。
3. バックアップするリソースをクリックします。
4. [リソース] ページで、カスタム名を使用する場合は、[スナップショット コピーにカスタム名形式を使用する] チェック ボックスをオンにし、スナップショット名の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。

   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。

      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	Snapshot処理が完了するまでの待機時間として、[Urgent]、[Medium]、または[Relaxed]のいずれかを選択します。 [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。

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ジョブに必要なカスタム値のペアを入力します。

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。
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. 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。

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。

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] をクリックします。

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*をクリックします。

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ている場合は、[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。

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\
```

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、リソースを追加します。

リソースを追加する例を次に示します。

```
Add-SmResource -HostName 'scc55.sccore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_vol1_scc55_sccore_test_com";"QTREENAME"="qtree
Vol1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

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。

   新しいバックアップ ポリシーを作成する例を次に示します。

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'
-PluginPolicyType DummyPlugin  -description 'testPolicy'
```

4. 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。

   この例では、ポリシーとリソースを指定して新しいリソース グループを作成しています。

```
Add-SmResourceGroup -ResourceGroupName
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'
-Resources
@(@{"Host"="scc55.sccore.test.com";"Uid"="QTREE2";"PluginName"="Dumm
yPlugin"},@{"Host"="scc55.sccore.test.com";"Uid"="QTREE";"PluginName
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'
-usesnapcenterwithoutfilesystemconsistency
```

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。

```
New-SMBackup -DatasetName
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy
test2
```

6. Get-SmBackupReportコマンドレットを使用して、バックアップ ジョブのステータスを表示します。

   この例では、指定した日に実行されたすべてのジョブの概要レポートを表示しています。

```
Get-SmBackupReport -JobId 149

BackedUpObjects           : {QTREE2, QTREE}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 1
SmJobId                   : 149
StartDateTime             : 1/15/2024 1:35:17 AM
EndDateTime               : 1/15/2024 1:36:19 AM
Duration                  : 00:01:02.4265750
CreatedDateTime           : 1/15/2024 1:35:51 AM
Status                    : Completed
ProtectionGroupName       :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows
SmProtectionGroupId       : 1
PolicyName                : test2
SmPolicyId                : 4
BackupName                :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-
15-2024_01.35.17.4467
VerificationStatus        : NotApplicable
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
PluginCode                : SCC
PluginName                : DummyPlugin
PluginDisplayName         : DummyPlugin
JobTypeId                 :
JobHost                   : scc55.sccore.test.com
```

NetAppがサポートしているプラグイン リソースのリソース グループのバックアップ

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。

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 ストレージに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。

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 [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ことができます。そのためには、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。そのあとにをクリックすると、フィルタ ペインが閉じます。

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] をクリックします。
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ている場合は、[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*をクリックします。
5. 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。

     "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"

   - VMDK上のアプリケーション データをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープ サイズが不足していると、バックアップが失敗することがあります。Javaヒープ サイズを増やすには、スクリプト ファイル/opt/netapp/init_scripts/scvserviceを探します。その脚本では、 `do_start method`コマンドは、 SnapCenter VMware プラグイン サービスを開始します。このコマンドを次のように更新します。 `Java -jar -Xmx8192M -Xms4096M 。

NetAppがサポートしているプラグインでのリソースの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。

NetAppがサポートしているプラグイン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NetAppがサポートしているプラグイン リソースに関連する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。[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。

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。

  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もトポロジ 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が含まれません。

- 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、4個のバックアップのみを保持するポリシーを使用して6個のバックアップを作成した場合、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もトポロジ 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が含まれません。

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. [Summary Card]で、プライマリ ストレージとセカンダリ ストレージ上にあるバックアップとクローンの数の概要を確認します。

   [Summary Card]セクションには、バックアップとクローンの総数が表示されます。

   更新ボタンをクリックすると、ストレージのクエリが実行されて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、名前変更、削除の各処理を実行します。

   セカンダリ ストレージ システム上のバックアップは、名前変更または削除できません。

   プライマリ ストレージ システムにあるバックアップは名前を変更できません。

7. クローンを削除する場合は、表でクローンを選択し、 をクリックして削除します。

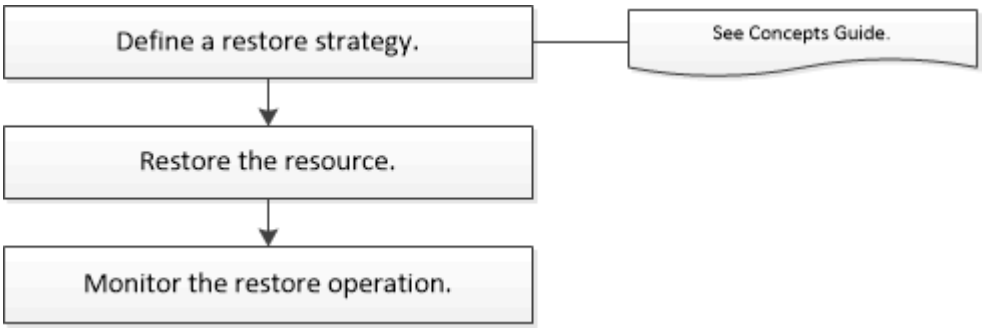
NetAppがサポートしているプラグイン リソースのリストア

NetAppがサポートしているプラグイン リソースのリストア

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。

タスク概要

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コマンドレットのヘルプを使用するか、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

リソースのバックアップのリストア

SnapCenterを使用してリソースをリストアすることができます。リストア処理の機能は、使用するプラグインによって異なります。

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。
- 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Storage Virtual Machine（SVM）をSnapCenter管理者がユーザに割り当てる必要があります。
- 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。

タスク概要

- デフォルトのリストア処理でリストアされるのは、ストレージ オブジェクトのみです。アプリケーションレベルのリストア処理は、その機能がNetAppがサポートしているプラグインで提供されている場合にのみ実行できます。
- 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。

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、ホストまたはクラスタ名、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。

   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。

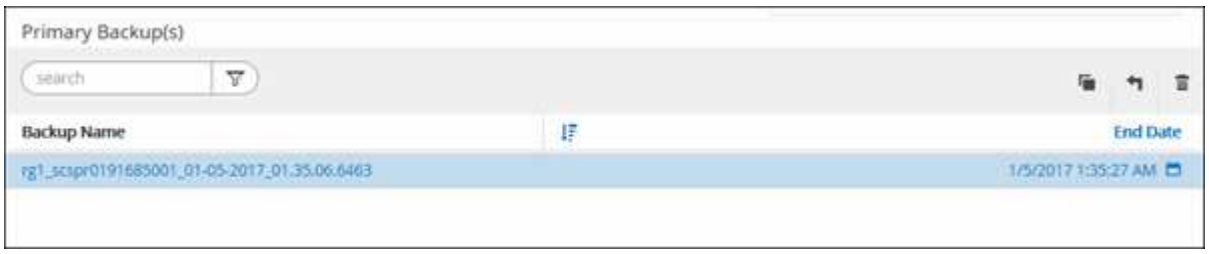
   リソースが保護されていない場合は、[全体的なステータス] 列に [保護されていません] と表示されます。

   全体的なステータス 列のステータス「保護されていません」は、リソースが保護されていないか、リソースが別のユーザーによってバックアップされたことを意味します。

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. 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、 。



6. [復元範囲] ページで、[完全なリソース] または [ファイル レベル] のいずれかを選択します。
   a. *完全なリソース*を選択した場合は、リソースのバックアップが復元されます。

      リソースにストレージ容量としてボリュームまたはqtreeが含まれている場合、それらのボリュームまたはqtreeの以降の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。

   b. ファイル レベル を選択した場合は、すべて を選択するか、ボリュームまたは qtree を選択して、選択したボリュームまたは qtree に関連するパスをコンマで区切って入力できます。
      - ボリュームとqtreeは複数選択できます。
      - リソース タイプがLUNの場合は、LUN全体がリストアされます。複数のLUNを選択できます。+ 注意: 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. 事前操作 ページで、復元ジョブを実行する前に実行する復元前コマンドとマウント解除コマンドを入力します。
8. **Post ops** ページで、復元ジョブを実行した後に実行するマウント コマンドと復元後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。

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1つまたは複数のバックアップに関する情報を取得します。

   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。

```
PS C:\> 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
```

   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。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

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" 。

NetAppがサポートしているプラグインでのリソースの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。

NetAppがサポートしているプラグイン リソースのバックアップのクローニング

NetAppがサポートしているプラグイン リソースのバックアップのクローニング

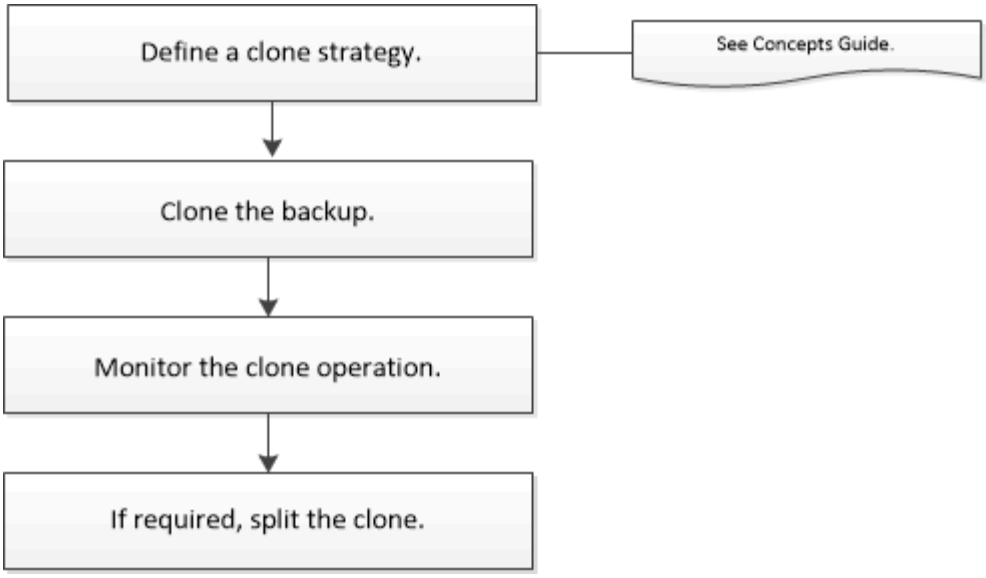
クローニング ワークフローには、クローニング処理の実行と処理の監視が含まれます。

タスク概要

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コマンドレットのヘルプを使用するか、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

バックアップからのクローニング

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。クローニング処理の機能は、使用するプラグインによって異なります。

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。
- デフォルトのクローニング処理でクローニングされるのは、ストレージ オブジェクトのみです。アプリケーション レベルのクローニング処理は、その機能がNetAppがサポートしているプラグインで提供されている場合にのみ実行できます。
- 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。

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、ホストまたはクラスタ名、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. [Locations]ページで、次の操作を実行します。

フィールド	操作
Clone server	ソース ホストがデフォルトで入力されています。 別のホストを指定する場合は、クローンのマウント先の、プラグインがインストールされたホストを選択します。
Clone suffix	クローン デスティネーションがソースと同じ場合は必須です。 クローニングされた新しいリソース名に付けるサフィックスを入力します。サフィックスにより、クローニングされたリソースがホストで一意になります。 たとえば、rs1_cloneのように指定します。元のリソースと同じホストにクローニングする場合、クローニングされたリソースを元のリソースと区別するためにサフィックスを指定する必要があります。これを行わないと処理は失敗します。

   リソースとしてLUNを選択し、セカンダリ バックアップからクローニングする場合、デスティネーション ボリュームのリストが表示されます。1つのソースについて複数のデスティネーション ボリュームを選択することができます。

7. *設定*ページで、次の操作を実行します。

フィールド	操作
イニシエーター名	ホスト イニシエータ名（IQDNまたはWWPN）を入力します。
Igroup protocol	[Igroup protocol]を選択します。

[Settings]ページは、ストレージ タイプがLUNの場合にのみ表示されます。

8. [Scripts]ページで、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。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。

   例えば：

   - 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

     Linux マシン上のボリュームまたは qtree のマウント コマンド:
     mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>

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。

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。

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. Get-SmBackupコマンドレットまたはGet-SmResourceGroupコマンドレットを使用して、クローニングできるバックアップのリストを表示します。

   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    11:02:32
AM                    Full Backup
   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 グループに関する情報を表示しています。

```
PS C:\> Get-SmResourceGroup

    Description                 :
    CreationTime                : 10/10/2016 4:45:53 PM
    ModificationTime            : 10/10/2016 4:45:53 PM
    EnableEmail                 : False
    EmailSMTPServer             :
    EmailFrom                   :
    EmailTo                     :
    EmailSubject                :
    EnableSysLog                : False
    ProtectionGroupType         : Backup
    EnableAsupOnFailure         : False
    Policies                    : {}
    HostResourceMaping          : {}
    Configuration               :
SMCoreContracts.SmCloneConfiguration
    LastBackupStatus            : Completed
    VerificationServer          :
    EmailBody                   :
    EmailNotificationPreference : Never
    VerificationServerInfo      :
    SchedulerSQLInstance        :
    CustomText                  :
    CustomSnapshotFormat        :
    SearchResources             : False
    ByPassCredential            : False
    IsCustomSnapshot            :
    MaintenanceStatus           : Production
    PluginProtectionGroupTypes  : {SMSQL}
    Tag                         :
```

```
    IsInternal                    : False
    EnableEmailAttachment         : False
    VerificationSettings          : {}
    Name                          : NFS_DB
    Type                          : Group
    Id                            : 2
    Host                          :
    UserName                      :
    Passphrase                    :
    Deleted                       : False
    Auth                          : SMCoreContracts.SmAuth
    IsClone                       : False
    CloneLevel                    : 0
    Hosts                         :
    StorageName                   :
    ResourceGroupNames            :
    PolicyNames                   :

    Description                   :
    CreationTime                  : 10/10/2016 4:51:36 PM
    ModificationTime              : 10/10/2016 5:27:57 PM
    EnableEmail                   : False
    EmailSMTPServer               :
    EmailFrom                     :
    EmailTo                       :
    EmailSubject                  :
    EnableSysLog                  : False
    ProtectionGroupType           : Backup
    EnableAsupOnFailure           : False
    Policies                      : {}
    HostResourceMaping            : {}
    Configuration                 :
SMCoreContracts.SmCloneConfiguration
    LastBackupStatus              : Failed
    VerificationServer            :
    EmailBody                     :
    EmailNotificationPreference   : Never
    VerificationServerInfo        :
    SchedulerSQLInstance          :
    CustomText                    :
    CustomSnapshotFormat          :
    SearchResources               : False
    ByPassRunAs                   : False
    IsCustomSnapshot              :
    MaintenanceStatus             : Production
    PluginProtectionGroupTypes    : {SMSQL}
```

```
    Tag                             :
    IsInternal                      : False
    EnableEmailAttachment           : False
    VerificationSettings            : {}
    Name                            : Test
    Type                            : Group
    Id                              : 3
    Host                            :
    UserName                        :
    Passphrase                      :
    Deleted                         : False
    Auth                            : SMCoreContracts.SmAuth
    IsClone                         : False
    CloneLevel                      : 0
    Hosts                           :
    StorageName                     :
    ResourceGroupNames              :
    PolicyNames                     :
```

3. New-SmCloneコマンドレットを使用して、クローン リソース グループまたは既存のバックアップからクローニング処理を開始します。

   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。

```
New-SmClone -BackupName
Verify_delete_clone_on_qtree_windows_scc54_10-04-2016_19.05.48.0886
-Resources @{"Host"="scc54.sccore.test.com";"Uid"="QTREE1"}  -
CloneToInstance scc54.sccore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sccore.test.com' -igroupprotocol 'mixed'
```

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}
    SmJobError          :
```

NetAppがサポートしているプラグインでのリソース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。

著作権に関する情報

商標に関する情報