Windowsファイルシステムの保護

SnapCenter software

NetApp
November 06, 2025

目次

Windowsファイルシステムの保護 1
SnapCenter Plug-in for Microsoft Windowsの概念 1
SnapCenter Plug-in for Microsoft Windowsの概要 1
SnapCenter Plug-in for Microsoft Windowsの機能 1
SnapCenter Plug-in for Windowsの特長 2
SnapCenterでのWindowsファイルシステムのバックアップ方法 3
SnapCenter Plug-in for Microsoft Windowsでサポートされるストレージ タイプ 3
Windowsプラグインに必要な最小ONTAP権限 6
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 8
Windowsファイルシステムのバックアップ戦略の定義 9
Windowsファイルシステムのクローンのソースとデスティネーション 11
SnapCenter Plug-in for Microsoft Windowsのインストール 11
SnapCenter Plug-in for Microsoft Windowsのインストール ワークフロー 11
SnapCenter Plug-in for Microsoft Windowsのインストール要件 11
ホストの追加とSnapCenter Plug-in for Microsoft Windowsのインストール 16
PowerShell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-in for Microsoft Windowsのインストール 20
コマンドラインからのSnapCenter Plug-in for Microsoft Windowsのサイレント インストール 20
SnapCenterプラグイン パッケージのインストール ステータスの監視 22
CA証明書の設定 23
SnapCenter Plug-in for VMware vSphereのインストール 26
CA証明書を導入する 26
CRLファイルを設定する 26
Windowsファイルシステムのバックアップ 26
Windowsファイルシステムのバックアップ 26
Windowsファイルシステムの使用可能なリソースの確認 28
Windowsファイルシステムのバックアップ ポリシーの作成 29
Windowsファイルシステムのリソース グループの作成 32
ASA r2 システム上の Windows ファイル システムのリソース グループを作成し、二次保護を有効にします。 34
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 37
Windowsファイルシステムの単一リソースのオンデマンド バックアップ 38
Windowsファイルシステムのリソース グループのバックアップ 42
バックアップ処理の監視 43
バックアップ処理のキャンセル 44
[Topology]ページでの関連するバックアップとクローンの表示 45
PowerShellコマンドレットを使用したセカンダリ バックアップ数のクリーンアップ 47
Windowsファイルシステムのリストア 48
Windowsファイルシステムのバックアップのリストア 48

PowerShellコマンドレットを使用したリソースのリストア . . . 53
リストア処理の監視 . . . 56
リストア処理のキャンセル . . . 57
Windowsファイルシステムのクローニング . . . 58
Windowsファイルシステムのバックアップからのクローニング . . . 58
クローニング処理の監視 . . . 64
クローニング処理のキャンセル . . . 65
クローンのスプリット . . . 66

Windowsファイルシステムの保護

SnapCenter Plug-in for Microsoft Windowsの概念

SnapCenter Plug-in for Microsoft Windowsの概要

SnapCenter Plug-in for Microsoft Windowsは、Microsoftファイルシステムのリソ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。Windowsファイルシステムのストレージのプロビジョニング、整合性のあるSnapshotの作成、およびスペースの再生が可能です。Plug-in for Windowsを使用することで、SnapCenter環境でのファイルシステムのバックアップ、リストア、およびクローニングの処理を自動化できます。

Plug-in for Windowsがインストールされている場合は、SnapCenterでNetApp SnapMirrorテクノロジを使用して別のボリュームにバックアップ セットのミラー コピーを作成できるほか、NetApp SnapVaultテクノロジを使用してアーカイブや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できます。

- SnapCenter環境のWindowsホストで実行されている他のプラグインに対してアプリケーション対応のデータ保護が有効になります。
- SnapCenter環境のMicrosoftファイルシステムに対するアプリケーション対応のバックアップ、リストア、クローニングの各処理が自動化されます。
- Windowsホストのストレージ プロビジョニング、整合性のあるSnapshotの作成、およびスペース再生がサポートされます。

Plug-in for Windowsでは、物理LUNとRDM LUNでSMB共有およびWindowsファイルシステムをプロビジョニングできますが、SMB共有でのWindowsファイルシステムのバックアップ処理はサポートされません。

SnapCenter Plug-in for Microsoft Windowsの機能

Plug-in for Windowsをインストールした環境では、SnapCenterを使用してWindowsファイルシステムをバックアップ、リストア、およびクローニングすることができます。これらの処理をサポートするタスクも実行できます。

- リソースの検出
- Windowsファイルシステムのバックアップ
- バックアップ処理のスケジュールの設定
- ファイルシステムのバックアップのリストア
- ファイルシステムのバックアップのクローニング
- バックアップ、リストア、クローニングの各処理を監視する

Plug-in for Windowsでは、SMB共有のファイルシステムのバックアップとリストアはサポートされていません。

SnapCenter Plug-in for Windowsの特長

Plug-in for Windowsは、ストレージ システム上でNetAppのSnapshotテクノロジと統合されます。Plug-in for Windowsの操作には、SnapCenterのインターフェイスを使用します。

Plug-in for Windowsの主な機能は次のとおりです。

- * SnapCenterによる統合グラフィカル ユーザー インターフェイス*

  SnapCenterのインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。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 プロセスとリストア プロセス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。また、SnapCenterでは、バックアップとクローニングの処理に対応したスケジュールとポリシーの一元管理もサポートされます。

- 自動化された中央管理

  日常的なファイルシステムのバックアップ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、リストア処理をセットアップしたりできます。SnapCenterからのEメール アラートの送信を設定して、ファイルシステム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

  Plug-in for Windowsでは、NetAppのSnapshotテクノロジを使用しています。これにより、ファイルシステムを数秒でバックアップし、ホストをオフラインにすることなく迅速にリストアすることが可能です。Snapshotはストレージ スペースを最小限しか消費しません。

Plug-in for Windowsには、上記の主要な機能以外にも次のようなメリットがあります。

- 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。
- 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本番環境ファイルシステムのコピー（スペース効率に優れたコピー）を作成できます。

  FlexCloneのライセンス情報については、以下を参照してください。"SnapCenterのライセンス" 。

- 複数のサーバで同時に複数のバックアップを実行できます。
- PowerShellコマンドレットを使用してバックアップ、リストア、およびクローニングの処理のスクリプトを作成できます。
- ファイルシステムと仮想マシン ディスク（VMDK）のバックアップがサポートされます。
- 物理インフラと仮想インフラがサポートされます。
- iSCSI、ファイバチャネル、FCoE、rawデバイス マッピング（RDM）、非対称LUNマッピング（ALM）、NFSおよびVMFS経由のVMDK、および仮想FCがサポートされます。
- Windows Server 2022でNon-Volatile Memory express（NVMe）がサポートされます。
  - NVMe over TCP/IPで作成されたVMDKレイアウト上のバックアップ、リストア、クローニング、検証の各ワークフロー。

- ESX 8.0 Update 2以降のNVMeファームウェア バージョン1.3をサポートします。仮想マシン ハードウェア バージョン21が必要です。
- Windows Serverフェイルオーバー クラスタリング（WSFC）は、NVMe over TCP/IP上のVMDKを介したアプリケーションではサポートされません。

- サイト全体の障害時でもビジネス サービスの運用を継続できるようにするSnapMirrorアクティブ シンク (当初はSnapMirror Business Continuity [SM-BC] としてリリース) をサポートし、セカンダリ コピーを使用してアプリケーションを透過的にフェイルオーバーできるようにします。SnapMirrorアクティブ同期でフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。

SnapCenterでのWindowsファイルシステムのバックアップ方法

SnapCenterでは、Snapshotテクノロジを使用してWindowsファイルシステムのリソースがバックアップされます。これには、WindowsクラスタのLUN、CSV（クラスタ共有ボリューム）、RDM（rawデバイス マッピング）ボリューム、ALM（非対称LUNマッピング）、およびVMFS / NFS（NFSを使用するVMware Virtual Machine File System）に基づくVMDKにあるリソースが含まれます。

SnapCenterでは、ファイルシステムのSnapshotを作成することによってバックアップを作成します。ボリュームに複数のホストのLUNが含まれている場合は、フェデレーテッド バックアップを使用すると、各LUNを個別にバックアップするよりも迅速かつ効率的に処理できます。ボリュームのSnapshotを1つだけ作成すれば、各ファイルシステムのSnapshotを個別に作成しなくても済むからです。

SnapCenterで作成されるSnapshotには、ストレージ システム ボリューム全体がキャプチャされます。ただし、このバックアップは、バックアップが作成されたホスト サーバに対してのみ有効になります。

他のホスト サーバのデータが同じボリュームに含まれている場合、それらのデータをSnapshotからリストアすることはできません。

Windowsファイルシステムにデータベースが含まれている場合、ファイルシステムをバックアップしてもデータベースがバックアップされるわけではありません。データベースをバックアップするには、いずれかのデータベース用プラグインを使用する必要があります。

SnapCenter Plug-in for Microsoft Windows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。ホストに対応したパッケージ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。

Windows Serverでは、SnapCenterによるプロビジョニングとデータ保護がサポートされます。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
は、https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT["NetApp Interoperability Matrix Tool"^] 。

マシン	ストレージ タイプ	プロビジョニングを使用して	サポートノート
物理サーバ	FC接続LUN	SnapCenterのグラフィカル ユーザ インターフェイス（GUI）またはPowerShellコマンドレット	
物理サーバ	iSCSI接続LUN	SnapCenterのGUIまたはPowerShellコマンドレット	
物理サーバ	Storage Virtual Machine（SVM）上のSMB3（CIFS）共有	SnapCenterのGUIまたはPowerShellコマンドレット	プロビジョニングのみがサポートされます。
VMware VM	FCまたはiSCSI HBAで接続されたRDM LUN	PowerShellコマンドレット	
VMware VM	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	SnapCenterのGUIまたはPowerShellコマンドレット	
VMware VM	仮想マシン ファイルシステム（VMFS）またはNFSデータストア	VMware vSphere	
VMware VM	SVM上のSMB3共有に接続されたゲスト システム	SnapCenterのGUIまたはPowerShellコマンドレット	プロビジョニングのみがサポートされます。
VMware VM	NFSとSANの両方に存在するvVolデータストア	ONTAP Tools for VMware vSphere	

マシン	ストレージ タイプ	プロビジョニングを使用して	サポートノート
Hyper-V VM	仮想ファイバチャネル スイッチで接続された仮想FC（vFC）LUN	SnapCenterのGUIまたはPowerShellコマンドレット	仮想ファイバチャネル スイッチで接続された仮想FC（vFC）LUNのプロビジョニングには、Hyper-V Managerを使用する必要があります。 Hyper-Vのパススルーディスク、およびNetAppストレージでプロビジョニングされたVHD（VHDX）でのデータベースのバックアップはサポートされません。
Hyper-V VM	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	SnapCenterのGUIまたはPowerShellコマンドレット	Hyper-Vのパススルーディスク、およびNetAppストレージでプロビジョニングされたVHD（VHDX）でのデータベースのバックアップはサポートされません。

マシン	ストレージ タイプ	プロビジョニングを使用して	サポートノート
Hyper-V VM	SVM上のSMB3共有に接続されたゲスト システム	SnapCenterのGUIまたはPowerShellコマンドレット	プロビジョニングのみがサポートされます。 Hyper-Vのパススルーディスク、およびNetAppストレージでプロビジョニングされたVHD（VHDX）でのデータベースのバックアップはサポートされません。

Windows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 delete
  - 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
- 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
- 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

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およびSnapVault の更新は、 SnapCenterジョブの一部として実行されます。SnapMirrorアクティブ同期を使用している場合は、 SnapMirrorアクティブ同期と非同期関係の両方に対してデフォルトのSnapMirrorまた

はSnapVaultスケジュールを使用します。

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" 。

Windowsファイルシステムのバックアップ戦略の定義

バックアップを作成する前にバックアップ戦略を定義しておくと、ファイルシステム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。

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。

Windowsファイルシステムのバックアップ スケジュール

バックアップ頻度はポリシーで指定され、バックアップ スケジュールはリソース グループの設定で指定されます。バックアップの頻度または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、リソースの変更率とデータの重要性です。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。

SLA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わる要件です。

使用頻度の高いリソースであっても、フル バックアップは1日に1～2回で十分です。

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頻度) は、一部のプラグインでは スケジュール タイプ と呼ばれ、ポリシー構成の一部です。たとえば、バックアップ頻度を時間ごと、日ごと、週ごと、または月ごとに設定することも、ポリシーをオンデマンドのみのポリシーにする「なし」を指定することもできます。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 グループ設定の一部です。たとえば、週次バックアップのポリシーが構成されたリソース グループがある場合は、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構成できます。 リソース > リソース グループ をクリックすると、リソース グループのスケジュールにアクセスできます。

Windowsファイルシステムで必要なバックアップの数

必要なバックアップの数を左右する要因としては、Windowsファイルシステムのサイズ、使用中のボリュームの数、ファイルシステムの変更率、サービス レベル アグリーメント（SLA）などがあります。

Windowsファイルシステムのバックアップ命名規則

Windowsファイルシステムのバックアップでは、Snapshotのデフォルトの命名規則が使用されます。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`リソース グループ名です。
- `mach1x88`ホスト名です。
- `03-12-2016_23.17.26`日付とタイムスタンプです。

バックアップの作成時に、バックアップを識別するためのタグを追加することもできます。一方、カスタマイズしたバックアップ命名規則を使用する場合は、バックアップ処理の完了後にバックアップの名前を変更する必要があります。

バックアップ保持オプション

バックアップ コピーを保持する日数を選択するか、または保持するバックアップ コピーの数（ONTAPでは最大255個のコピー）を指定することができます。たとえば、組織の必要に応じて、10日分のバックアップ コピーや130個のバックアップ コピーを保持できます。

ポリシーを作成する際に、バックアップ タイプおよびスケジュール タイプの保持オプションを指定できます。

SnapMirrorレプリケーションを設定すると、デスティネーション ボリュームに保持ポリシーがミラーリングされます。

SnapCenter は、スケジュール タイプに一致する保持ラベルを持つ保持されたバックアップを削除します。リソースまたはリソース グループに対してスケジュール タイプが変更されると、古いスケジュール タイプ ラベルのバックアップがシステムに残ることがあります。

バックアップ コピーを長期にわたって保持する場合は、SnapVaultバックアップを使用する必要があります。

Windowsファイルシステムのクローンのソースとデスティネーション

ファイルシステムのクローニングは、プライマリ ストレージから行うこともセカンダリ ストレージから行うこともできます。デスティネーションについても、要件に応じて、バックアップの元の場所のほか、同じホストまたは別のホストの別の場所を選択することが可能です。クローンのデスティネーションのボリュームは、ソースのバックアップと同じである必要があります。

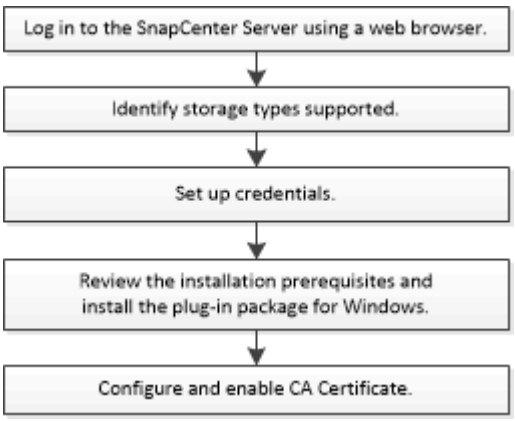
クローン先	説明
元のソースの場所	SnapCenterでは、デフォルトでは、クローニングされたバックアップと同じホストの同じ場所にクローンが格納されます。
別の場所	同じホストまたは別のホストの別の場所にクローンを格納できます。ホストでStorage Virtual Machine（SVM）への接続が設定されている必要があります。

クローニング処理の完了後にクローンの名前を変更することができます。

SnapCenter Plug-in for Microsoft Windowsのインストール

SnapCenter Plug-in for Microsoft Windowsのインストール ワークフロー

データベース ファイルではない Windows ファイルを保護する場合は、Microsoft Windows 用のSnapCenterプラグインをインストールして設定する必要があります。



SnapCenter Plug-in for Microsoft Windowsのインストール要件

Plug-in for Windowsをインストールする前に、特定のインストール要件を確認しておく必要があります。

ユーザがPlug-in for Windowsの使用を開始するためには、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。

- Plug-in for Windowsをインストールするには、SnapCenter admin権限が必要です。

  SnapCenter adminロールには管理者権限が必要です。

- SnapCenter Serverをインストールして設定しておく必要があります。
- 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。
- バックアップ レプリケーションが必要な場合は、SnapMirrorとSnapVaultをセットアップする必要があります。

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" 。 Windows クラスター セットアップを使用している場合は、Windows リモート管理 (WinRM) もインストールして構成する必要があります。
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 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" 。

Plug-in for Windows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、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。

必要なもの

- 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]ページで次の操作を実行します。

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。

フィールド	操作
ユーザー名/パスワード	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\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • 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。
パスワード	認証に使用するパスワードを入力します。

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。

ホストの追加と**SnapCenter Plug-in for Microsoft Windows**のインストール

SnapCenterの[Add Host]ページを使用して、Windowsホストを追加できます。SnapCenter Plug-in for Microsoft Windowsは、指定したホストに自動的にインストールされます。これは推奨されるプラグインのインストール方法です。ホストの追加とプラグインのインストールは、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。

- SnapCenterユーザーを、Windows Server の「サービスとしてログオン」ロールに追加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Windowsファイルシステム用にグループ管理サービス アカウントを設定する"

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。
- Windowsプラグイン
  - Microsoft Windows
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
- クラスタへのプラグインのインストール

  クラスタ（WSFC、Oracle RAC、またはExchange DAG）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。

- Eシリーズ ストレージ

  Eシリーズ ストレージに接続されたWindowsホストにPlug-in for Windowsをインストールすることはできません。

SnapCenterでは、同じホスト（プラグイン ホスト）をSnapCenterに追加することはできません。そのホストがすでにワークグループに属していて、ドメインを別のものに変更しても（またはその逆をしても）、追加することはできません。同じホストを追加する場合は、SnapCenterからホストを削除して再度追加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、[ホスト] をクリックします。
2. 上部で*管理対象ホスト*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	**Windows** タイプのホストを選択します。 SnapCenter Serverがホストを追加し、Plug-in for Windowsをホストにインストールします（プラグインがまだインストールされていない場合）。

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。したがって、ベストプラクティスはFQDNを入力することです。 次のいずれかのIPアドレスまたはFQDNを入力できます。 • スタンドアロン ホスト • Windows Serverフェイルオーバー クラスタリング（WSFC） SnapCenterを使用してホストを追加する際、ホストがサブドメインの一部である場合は、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。 ユーザ名、ドメイン、およびホスト タイプを含むクレデンシャルの詳細は、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表示されます。 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。

   新規導入の場合、プラグイン パッケージは表示されません。

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	デフォルトのパスはC:\Program Files\NetApp\SnapCenterです。 必要に応じて変更できます。SnapCenter Plug-ins Package for Windowsの場合、デフォルト パスはC:\Program Files\NetApp\SnapCenterです。ただし、必要に応じて、デフォルト パスはカスタマイズできます。
クラスター内のすべてのホストを追加する	WSFC内のすべてのクラスタ ノードを追加するには、このチェック ボックスをオンにします。
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	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 名を次の形式で指定します: *domainName\accountName$*。 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。

「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が検証されます。ディスク容量、RAM、PowerShellのバージョン、.NETのバージョン、および場所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`デフォルト値を変更する WebApp。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. インストールの進捗状況を監視します。

PowerShell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-in for Microsoft Windowsのインストール

SnapCenter Plug-in for Microsoft Windowsを複数のホストに一度にインストールする場合は、 `Install-SmHostPackage` PowerShell コマンドレット。

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

手順

1. PowerShellを起動します。
2. SnapCenter Serverホストで、 `Open-SmConnection`コマンドレットを実行し、資格情報を入力します。
3. スタンドアロンホストまたはクラスタをSnapCenterに追加するには、 `Add-SmHost`コマンドレットと必要なパラメータ。

   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" 。
4. 複数のホストにプラグインをインストールするには、 `Install-SmHostPackage`コマンドレットと必要なパラメータ。

   使用することができます `-skipprecheck`プラグインを手動でインストールし、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検証したくない場合は、このオプションを選択します。

コマンドラインからのSnapCenter Plug-in for Microsoft Windowsのサイレント インストール

SnapCenter GUIからリモートでインストールできない場合は、Windowsホスト上でローカルにSnapCenter Plug-in for Microsoft Windowsをインストールできます。Windowsのコマンドラインから、SnapCenter Plug-in for Microsoft Windowsのインストール プログラムをサイレント モードで自動的に実行できます。

開始する前に

- 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 バンドルがインストールされている必要があります。
- PowerShell 7.4.2以降がインストールされている必要があります。

- ホストのローカル管理者である必要があります。

手順

1. インストールの場所から、SnapCenter Plug-in for Microsoft Windowsをダウンロードします。

   たとえば、デフォルトのインストール パスはC:\ProgramData\NetApp\SnapCenter\Package Repositoryです。

   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. プラグインをインストールするホストにインストール ファイルをコピーします。
3. コマンド プロンプトから、インストール ファイルをダウンロードしたディレクトリに移動します。
4. 以下のコマンドを、変数を実際のデータに置き換えて入力します。

   ```
   "snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
   BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
   ISFeatureInstall=SCW
   ```

   例えば：

   ```
   `"C:\ProgramData\NetApp\SnapCenter\Package Repository
   \snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
   \HPPW_SCW_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
   SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
   BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW`
   ```

   Plug-in for Windowsのインストール時に渡されるすべてのパラメータでは、大文字と小文字が区別されます。

   以下の変数に値を入力します。

変数	**Value**
/debuglog"<デバッグログパス>	次の例のように、スイート インストーラー ログ ファイルの名前と場所を指定します: Setup.exe /debuglog"C:\PathToLog\setupexe.log"。
BI_SNAPCENTER_PORT	SnapCenterがSMCoreと通信するポートを指定します。
SUITE_INSTALLDIR	ホストのプラグイン パッケージのインストール ディレクトリを指定します。
BI_SERVICEACCOUNT	SnapCenter Plug-in for Microsoft WindowsのWebサービス アカウントを指定します。

変数	Value
BI_SERVICEPWD	SnapCenter Plug-in for Microsoft WindowsのWebサービス アカウントのパスワードを指定します。
ISFeatureInstall	SnapCenterでリモート ホストに導入するソリューションを指定します。

debuglog パラメータには、 SnapCenterのログ ファイルのパスが含まれます。このログ ファイルにはインストールで実行されるプラグインの前提条件に関するチェック結果が記録されるため、トラブルシューティング情報を入手する手段としてこのログ ファイルに書き込むことを推奨します。

必要な場合、SnapCenter for Windowsパッケージのログ ファイルでその他のトラブルシューティング情報を確認できます。パッケージのログ ファイルは、*%Temp%* フォルダー (例: *C:\temp*) に (古いものから順に) リストされます。

Plug-in for Windowsをインストールすると、SnapCenter Serverではなくホストにプラグインが登録されます。SnapCenter GUIまたはPowerShellコマンドレットを使用してホストを追加することにより、SnapCenter Serverにプラグインを登録できます。ホストを追加すると、プラグインが自動的に検出されます。

SnapCenterプラグイン パッケージのインストール 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"
   ```

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。

SnapCenter Plug-in for VMware vSphereのインストール

データベースまたはファイルシステムが仮想マシン（VM）に格納されている場合や、VMとデータストアを保護する場合は、SnapCenter Plug-in for VMware vSphere仮想アプライアンスを導入する必要があります。

展開方法については、 "導入プロセスの概要" 。

CA証明書を導入する

SnapCenter Plug-in for VMware vSphereで CA 証明書を構成するには、以下を参照してください。 "SSL証明書を作成またはインポートする" 。

CRLファイルを設定する

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリでCRLファイルを探します。SnapCenter Plug-in for VMware vSphere のCRL ファイルのデフォルト ディレクトリは */opt/netapp/config/crl* です。

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ファイルシステムのバックアップ

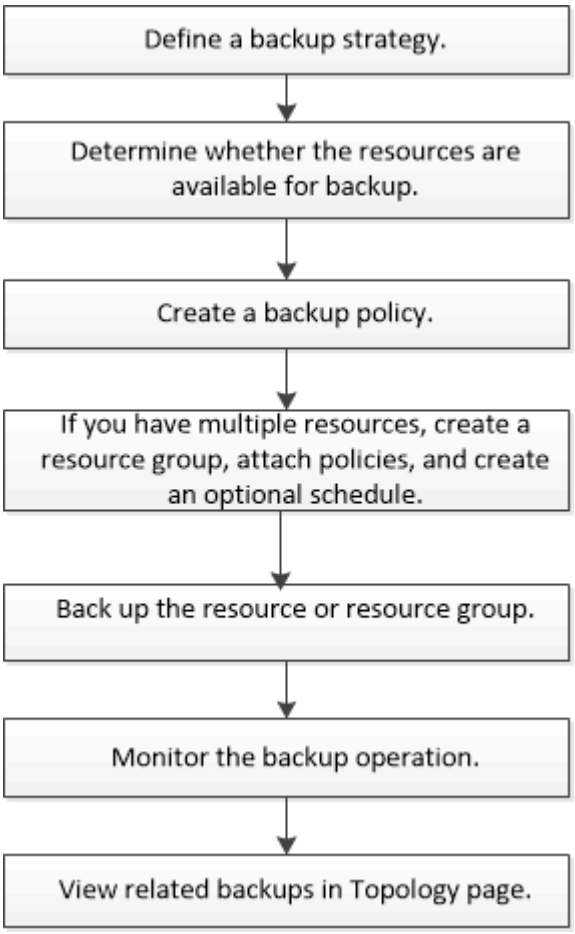
Windowsファイルシステムのバックアップ

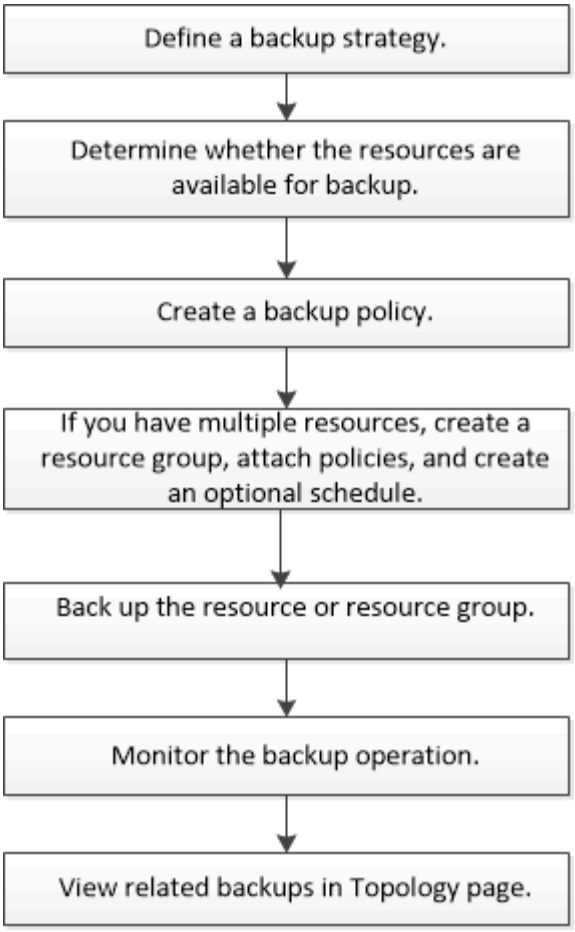
SnapCenter Plug-in for Microsoft Windowsをインストールした環境では、SnapCenterを

使用してWindowsファイルシステムをバックアップすることができます。単一のファイルシステム、または複数のファイルシステムを含むリソース グループをバックアップできます。バックアップは、オンデマンドで実行するか、または定義した保護スケジュールに従って実行できます。

スケジュールを設定して、複数のサーバで同時に複数のバックアップを実行することができます。同じリソースに対してバックアップ処理とリストア処理を同時に実行することはできません。

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。SnapCenterコマンドレットのヘルプまたは "SnapCenterソフトウェア コマンドレット リファレンス ガイド"PowerShell コマンドレットに関する詳細情報が含まれています。

Windowsファイルシステムの使用可能なリソースの確認

リソースとは、インストールしたプラグインで管理されるファイルシステム内のLUNやそれに類するコンポーネントのことです。それらのリソースをリソース グループに追加することで複数のリソースに対してデータ保護ジョブを実行できますが、その前に利用可能なリソースを特定しておく必要があります。利用可能なリソースを検出することで、プラグインのインストールが正常に完了したことの確認にもなります。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、Storage Virtual Machine（SVM）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。
- ファイルがVMware RDM LUNまたはVMDKにある場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。詳細については、以下を参照してください。 "SnapCenter Plug-in for VMware vSphereのドキュメント" 。

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、リストから ファイル システム を選択します。

3. リソースのリストをフィルタリングするホストを選択し、[リソースの更新] をクリックします。

   新たに追加、名前変更、または削除されたファイルシステムが、SnapCenter Serverのインベントリで更新されます。

   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。

Windowsファイルシステムのバックアップ ポリシーの作成

SnapCenterを使用してWindowsファイルシステムをバックアップする前に、リソースの新しいバックアップ ポリシーを作成することができます。また、リソース グループの作成時やリソースのバックアップ時に新しいバックアップ ポリシーを作成することも可能です。

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。"詳細情報"
- データ保護の準備が完了している必要があります。

  データ保護の準備として、SnapCenterのインストール、ホストの追加、リソースの検出、Storage Virtual Machine（SVM）接続の作成などのタスクを完了しておく必要があります。

- Snapshotをミラー セカンダリ ストレージまたはバックアップ セカンダリ ストレージにレプリケートするユーザには、SnapCenter管理者がソースとデスティネーションの両方のボリューム用にSVMを割り当てる必要があります。
- プリスクリプトとポストスクリプトでPowerShellスクリプトを実行する場合は、web.configファイルのusePowershellProcessforScriptsパラメータの値をtrueに設定する必要があります。

  デフォルト値はfalseです。

- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、 "SnapMirrorアクティブ同期のオブジェクト数の制限" 。

タスク概要

- SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.ConfigファイルにあるpredefinedWindowsScriptsDirectoryキーを使用して定義します。

  必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

  キーの値は、API を介して Swagger から表示できます: API /4.7/configsettings

  GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。

- 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] を選択します。
2. [設定]ページで、[ポリシー]を選択します。
3. *新規*を選択します。
4. 「名前」ページで、ポリシー名と詳細を入力します。
5. 「バックアップとレプリケーション」ページで、次のタスクを実行します。

   a. バックアップ設定を選択します。

オプション	説明
File System Consistent Backup	ファイルシステムが配置されたディスク ドライブをバックアップ処理の開始前にSnapCenterで休止し、バックアップ処理の終了後に再開する場合は、このオプションを選択します。
File System Crash-consistent Backup	ファイルシステムが配置されたディスク ドライブをSnapCenterで休止しない場合は、このオプションを選択します。

   b. スケジュール頻度（ポリシー タイプ）を選択します。

   ポリシーではバックアップの頻度のみを指定します。バックアップの具体的なスケジュールは、リソース グループで定義します。したがって、複数のリソース グループで同じポリシーとバックアップ頻度を使用している場合でも、別々のバックアップ スケジュールを設定できます。

   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。

   c. ポリシーラベルを選択します。

   ONTAPによって、選択したSnapshotラベルに一致するセカンダリSnapshotの保持ポリシーが適用されます。

   ローカル **Snapshot** コピーの作成後に**SnapMirror**を更新する を選択した場合は、オプションでセカンダリ ポリシー ラベルを指定できます。ただし、ローカル スナップショット コピーの作成後に**SnapVault**を更新する を選択した場合は、セカンダリ ポリシー ラベルを指定する必要があります。

6. [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）は、このオプションを選択します。 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。 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ページでの関連するバックアップとクローンの表示"] 。
Update SnapVault after creating a 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。[Topology]ページの[Refresh]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のSnapLock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は、[Topology]ページの[Refresh]ボタンをクリックすると、ONTAPから取得したセカンダリのSnapLock有効期限が更新されます。 SnapLock Vaultの詳細については、 "バックアップデスティネーションのSnapshotコピーのWORM状態へのコミット"
Error retry count	レプリケーションの最大試行回数を入力します。この回数を超えると処理が停止します。

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。

7. [保持設定] ページで、オンデマンド バックアップと選択した各スケジュール頻度の保持設定を指定します。

オプション	説明
保持するスナップショットコピーの合計数	SnapCenterで保持するSnapshotの個数を指定する場合は、このオプションを選択します。指定した個数を超えると自動的に削除されます。
スナップショットコピーを保存する	SnapCenterでバックアップ コピーを保持する日数を指定する場合は、このオプションを選択します。指定した日数を過ぎると削除されます。
スナップショットコピーのロック期間	スナップショットのロック期間を選択し、期間を日数、月数、または年数で指定します。 SnapLock保持期間は100年未満にする必要があります。

保持数は2以上に設定する必要があります。保持数の最小値は2です。

最大保持値は 1018 です。保持期間がONTAPバージョンでサポートされている値よりも高い値に設定されている場合、バックアップは失敗します。

8. [Script]ページで、バックアップ処理の前後にSnapCenter Serverで実行するプリスクリプトやポストスクリプトを入力し、それぞれのスクリプトについてSnapCenterでの実行をタイムアウトするまでの時間を入力します。

   たとえば、SNMPトラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。

   プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

9. 概要を確認し、[完了] をクリックします。

Windowsファイルシステムのリソース グループの作成

リソース グループとは、保護する複数のファイルシステムを追加できるコンテナです。リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義し、バックアップ スケジュールを指定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。
- SnapMirrorアクティブ同期を使用しない新しいファイルシステムを、SnapMirrorアクティブ同期を使用するリソースを含む既存のリソース グループに追加することはできません。
- SnapMirrorアクティブ同期のフェイルオーバー モードにある既存のリソース グループに新しいファイルシステムを追加することはできません。リソースを追加できるのは、通常の状態またはフェイルバック状態のリソース グループのみです。

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、リストから ファイル システム を選択します。

   最近SnapCenterにファイル システムを追加した場合は、[リソースの更新] をクリックして、新しく追加されたリソースを表示します。

3. *新しいリソース グループ*をクリックします。
4. ウィザードの[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 グループ名を入力します。 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。
Use custom name format for Snapshot copy	オプション: カスタム スナップショットの名前と形式を入力します。 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の名前の後ろにタイムスタンプが付加されます。
Tag	リソース グループを検索するときに役立つわかりやすいタグを入力します。

5. [Resources]ページで、次の作業を実行します。

   a. ホストを選択してリソースのリストをフィルタリングします。

      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。

   b. [Available Resources]セクションでバックアップするファイルシステムをクリックし、右矢印をクリックして[Added]セクションに移動します。

      同じストレージ ボリューム上のすべてのリソースを自動選択 オプションを選択すると、同じボリューム上のすべてのリソースが選択されます。その状態で[Added]セクションに移動した場合、そのボリュームのすべてのリソースが一緒に移動されます。

   単一のファイル システムを追加するには、[同じストレージ ボリューム上のすべてのリソースを自動選択する] オプションをオフにし、[追加済み] セクションに移動するファイル システムを選択します。

6. [Policies]ページで、次の作業を実行します。

   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。

既存のポリシーを選択し、「詳細」をクリックして、そのポリシーを使用できるかどうかを判断できます。

既存のポリシーが要件を満たしていない場合は、*をクリックして新しいポリシーを作成できます。 * ポリシー ウィザードを起動します。

選択したポリシーが[Configure schedules for selected policies]セクションの[Policy]列に表示されます。

b. 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で、*をクリックします。 * 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. ポリシーが複数のスケジュール タイプ（頻度）に関連付けられている場合は、設定する頻度を選択します。

d. [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、開始日、有効期限、頻度を指定してスケジュールを構成し、[完了] をクリックします。

設定したスケジュールは、[Configure schedules for selected policies]セクションの[Applied Schedules]列に表示されます。

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。Windowsタスク スケジューラとSQL Server Agentからスケジュールを変更しないでください。

7. [Notification]ページで、通知の情報を次のように指定します。

フィールド	操作
メール設定	バックアップ リソース グループを作成し、ポリシーを添付し、スケジュールを構成した後、受信者に電子メールを送信するには、[常に]、[失敗時]、または [失敗または警告時] を選択します。SMTPサーバ、Eメールのデフォルトの件名、および送信先と送信元のEメール アドレスを入力します。
から	Eメール アドレス
To	Eメールの送信先アドレス
Subject	Eメールのデフォルトの件名

8. 概要を確認し、[完了] をクリックします。

オンデマンドでバックアップを実行できるほか、スケジュールに従ってバックアップが開始されます。

ASA r2 システム上の Windows ファイル システムのリソース グループを作成し、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" 。

Windowsファイルシステムの単一リソースのオンデマンド バックアップ

リソース グループに含まれていないリソースは、[Resources]ページからオンデマンドでバックアップすることができます。

タスク概要

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、ストレージ ユーザーに割り当てられているロールに「`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によるファイルシステムのバックアップでは、バックアップするファイルシステムのボリューム マウント ポイント（VMP）にマウントされているLUNはバックアップされません。

Windowsファイルシステムについての作業では、データベース ファイルはバックアップしないでください。バックアップを作成しても整合性に欠け、リストア時にデータが失われる可能性があります。データベース ファイルを保護するには、データベースに適したSnapCenterプラグイン (たとえば、Microsoft SQL Server 用のSnapCenterプラグインや Microsoft Exchange Server 用のSnapCenterプラグインなど) を使用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. [Resources]ページで、リソース タイプとして[File System]を選択し、バックアップするリソースを選択します。
3. ファイル システム - 保護ウィザードが自動的に起動しない場合は、[保護] をクリックしてウィザードを起動します。

   「リソース グループの作成」の作業の説明に従って、保護設定を指定します。

4. オプション: ウィザードのリソース ページで、スナップショットのカスタム名形式を入力します。

   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の名前の後ろにタイムスタンプが付加されます。

5. [Policies]ページで、次の作業を実行します。

   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。

      既存のポリシーを選択し、[詳細] をクリックして、そのポリシーを使用できるかどうかを確認できます。

      既存のポリシーがいずれも要件を満たさない場合は、既存のポリシーをコピーして変更するか、 をクリックしてポリシー ウィザードで新しいポリシーを作成できます。既存のポリシーがいずれも要件を満たさない場合は、既存のポリシーをコピーして変更するか、 をクリックしてポリシー ウィザードで新しいポリシーを作成できます。

      選択したポリシーが[Configure schedules for selected policies]セクションの[Policy]列に表示されます。

   b. 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で、 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、開始日、有効期限、頻度を指定してスケジュールを構成し、[完了] をクリックします。

      設定したスケジュールは、[Configure schedules for selected policies]セクションの[Applied Schedules]列に表示されます。

   "スケジュールを設定した処理は失敗することがあります。"

6. [Notification]ページで、次の作業を行います。

フィールド	操作
メール設定	バックアップ リソース グループを作成し、ポリシーを添付し、スケジュールを構成した後、受信者に電子メールを送信するには、[常に]、[失敗時]、または [失敗または警告時] を選択します。 SMTP サーバー情報、デフォルトの電子メール件名、および「To」および「From」電子メール アドレスを入力します。
から	Eメール アドレス
To	Eメールの送信先アドレス
Subject	Eメールのデフォルトの件名

7. 概要を確認し、[完了] をクリックします。

   データベース トポロジのページが表示されます。

8. *今すぐバックアップ*をクリックします。
9. [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、バックアップに使用するポリシーを[Policy]ドロップダウン リストから選択します。

      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。
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。

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-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。

   この例では、SQLのバックアップ タイプ「FullBackup」を指定して新しいバックアップ ポリシーを作成しています。

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

この例では、Windowsファイルシステムのバックアップ タイプ「CrashConsistent」を指定して新しいバックアップ ポリシーを作成しています。

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Get-SmResourcesコマンドレットを使用してホスト リソースを検出します。

この例では、指定したホスト上でMicrosoft SQLプラグインのリソースを検出しています。

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

この例では、指定したホスト上でWindowsファイルシステムのリソースを検出しています。

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

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SQLデータベース バックアップ リソース グループを作成しています。

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

この例では、ポリシーとリソースを指定して新しいWindowsファイルシステム バックアップ リソース グループを作成しています。

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

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。

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

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。

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

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" 。

Windowsファイルシステムのリソース グループのバックアップ

リソース グループは、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。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ているロールに「`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。
- リソース グループにホストが異なる複数のデータベースが含まれている場合、一部のホストではネットワークの問題が原因でバックアップ処理のトリガーに時間がかかることがあります。PowerShellコマンドレットSet-SmConfigSettingsを使用して、web.configでMaxRetryForUninitializedHostsの値を設定する必要があります。

SnapCenterによるファイルシステムのバックアップでは、バックアップするファイルシステムのボリューム マウント ポイント（VMP）にマウントされているLUNはバックアップされません。

Windowsファイルシステムについての作業では、データベース ファイルはバックアップしないでください。バックアップを作成しても整合性に欠け、リストア時にデータが失われる可能性があります。データベース ファイルを保護するには、データベースに適したSnapCenterプラグイン (たとえば、Microsoft SQL Server 用のSnapCenterプラグインや Microsoft Exchange Server 用のSnapCenterプラグインなど) を使用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、[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。

   SnapCenter Plug-in for Oracle Databaseでは、2つのデータベースが統合されたリソース グループがある場合に、一方のデータベースのデータファイルがNetApp以外のストレージにあると、もう一方のデータベースがNetAppストレージにあっても、バックアップ処理は中止されます。

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を見つけます。 `/opt/netapp/init_scripts/scvservice` 。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` 。

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。

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できます。[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。

SnapMirrorアクティブ同期 (当初はSnapMirror Business Continuity [SM-BC] としてリリース) としてセカンダリ関係がある場合は、次の追加アイコンが表示されます。

-  レプリカサイトが稼働しています。
-  レプリカサイトはダウンしています。
-  セカンダリ ミラーまたはボールト関係が再確立されていません。

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。Oracleデータベースについては、[Summary Card]セクションにログ バックアップの総数も表示されます。

   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。

SnapMirrorアクティブ同期の場合、[更新] ボタンをクリックすると、プライマリ サイトとレプリカ サイトの両方に対してONTAP を照会してSnapCenterバックアップ インベントリが更新されます。週次スケジュールでも、SnapMirrorアクティブ同期関係を含むすべてのデータベースに対してこの処理が実行されます。

- SnapMirrorアクティブ同期とONTAP（バージョン9.14.1のみ）では、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップの関係については、フェイルオーバー後に手動で設定する必要があります。ONTAP 9.15.1以降は、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップが、自動的に設定されます。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。バックアップが作成された後にのみ、「更新」をクリックできます。

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。

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。

プライマリ ストレージのバックアップとクローンの例

PowerShellコマンドレットを使用したセカンダリ バックアップ数のクリーンアップ

Remove-SmBackupコマンドレットを使用して、Snapshotがないセカンダリ バックアップのバックアップ数をクリーンアップできます。コピーの管理トポロジに表示されるスナップショットの合計がセカンダリ ストレージのスナップショット保持設定と一致しない場合に、このコマンドレットを使用することをお勧めします。

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

コマンドレットで使用できるパラメータとその説明に関する情報は、*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. 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. -CleanupSecondaryBackupsパラメータを使用してセカンダリ バックアップ数をクリーンアップします。

   この例では、Snapshotがないセカンダリ バックアップのバックアップ数をクリーンアップしています。

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Windowsファイルシステムのリストア

Windowsファイルシステムのバックアップのリストア

SnapCenterを使用してファイルシステムのバックアップをリストアすることができます。ファイルシステムのリストアは、指定したバックアップのすべてのデータをファイルシステムの元の場所にコピーする複数の段階からなるプロセスです。

開始する前に

- ファイルシステムをバックアップしておく必要があります。
- ファイルシステムに対してバックアップ処理などのスケジュールが設定された処理が現在進行している場合は、リストア処理を開始する前にキャンセルしておく必要があります。
- ファイルシステムのバックアップは元の場所にのみリストアできます。別のパスを指定することはできません。

  ファイルシステムのリストアでは、ファイルシステムの元の場所にあるデータがすべて上書きされ、バックアップからファイル単位でリストアすることはできません。ファイルシステムのバックアップに含まれる単一のファイルをリストアするには、バックアップをクローニングし、クローン内のファイルを使用する必要があります。

- システム ボリュームやブート ボリュームはリストアできません。
- SnapCenterでは、クラスタ グループをオフラインにすることなく、Windowsクラスタのファイルシステムをリストアできます。

タスク概要

- SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.Configファイルにあ

るPredefinedWindowsScriptsDirectoryキーを使用して定義します。

必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

キーの値は、API を介して Swagger から表示できます: API /4.7/configsettings

GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。

- SnapMirrorアクティブ同期でリストア処理を実行するには、プライマリの場所からバックアップを選択する必要があります。
- 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。

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. リソースのリストをフィルタリングするには、[File System]および[Resource Group]のオプションを選択します。
3. リストからリソース グループを選択し、[復元] をクリックします。
4. [Backups]ページで、プライマリとセカンダリのどちらのストレージ システムからリストアするかを選択し、リストアするバックアップを選択します。
5. [Restore]ウィザードで目的のオプションを選択します。
6. リストア処理の実行前や実行後にSnapCenterで実行するプリスクリプトやポストスクリプトのパスと引数を入力できます。

   たとえば、SNMPトラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。

   プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

7. [Notification]ページで、次のいずれかのオプションを選択します。

フィールド	操作
Log SnapCenter server events to storage system syslog	SnapCenter Serverのイベントをストレージ システムのsyslogに記録する場合は、このオプションを選択します。
Send AutoSupport notification for failed operations to storage system	失敗した処理に関する情報をAutoSupportを使用してNetAppに送信する場合は、このオプションを選択します。
メール設定	バックアップの復元後に受信者に電子メールメッセージを送信するには、「常時」、「失敗時」、または「失敗または警告時」を選択します。SMTPサーバ、Eメールのデフォルトの件名、および送信先と送信元のEメール アドレスを入力します。

8. 概要を確認し、[完了] をクリックします。
9. 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。

   リストアしたファイルシステムにデータベースが含まれている場合は、データベースもリストアする必要があります。データベースをリストアしないと、データベースが無効な状態になることがあります。データベースのリストアの詳細については、そのデータベースのデータ保護ガイドを参照してください。

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
```

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" 。

PowerShellコマンドレットを使用したリソースのリストア

リソースのバックアップをリストアするときは、SnapCenter Serverとの接続セッションを開始し、バックアップをリストしてバックアップの情報を取得し、バックアップをリストアします。

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

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザで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" 。

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。

リストア処理のキャンセル

キューに登録されているリストア ジョブはキャンセルできます。

リストア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。

タスク概要

- キューに入れられた復元操作は、[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。
- 実行中のリストア処理はキャンセルできません。
- キューに登録されているリストア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復元操作の場合、「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復元操作をキャンセルできます。

手順

次のいずれかを実行します。

方法	アクション
[Monitor]ページ	1. 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。 2. ジョブを選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	1. 復元操作を開始したら、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。 2. 処理を選択します。 3. 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。

Windowsファイルシステムのクローニング

Windowsファイルシステムのバックアップからのクローニング

SnapCenterを使用してWindowsファイルシステムのバックアップをクローニングすることができます。誤って削除または変更された単一のファイルのコピーが必要な場合は、バックアップをクローニングし、クローン内のファイルを使用できます。

開始する前に

- データ保護の準備として、ホストの追加、リソースの特定、Storage Virtual Machine（SVM）接続の作成などのタスクを完了しておく必要があります。
- ファイルシステムのバックアップを作成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。
- リソース グループはクローニングできません。クローニングできるのは、個々のファイルシステムのバックアップだけです。
- SnapCenterでは、VMDKディスクを使用した仮想マシン上にあるバックアップを物理サーバにクローニングすることはできません。
- 共有LUNやクラスタ共有ボリューム（CSV）LUNなどのWindowsクラスタをクローニングした場合、クローンは指定したホストに専用のLUNとして格納されます。
- クローニング処理では、ボリューム マウント ポイントのルート ディレクトリを共有ディレクトリにすることはできません。
- クローンはアグリゲートのホーム ノード以外のノードには作成できません。
- Windowsファイルシステムのクローニング処理では、定期的なスケジュール（クローン ライフサイクル）は設定できません。バックアップのクローニングはオンデマンドでのみ実行できます。
- クローンが含まれているLUNを新しいボリュームに移動すると、SnapCenterでそのクローンをサポートできなくなります。たとえば、SnapCenterでそのクローンを削除できなくなります。
- 複数の環境間でのクローニングは実行できません。例：物理ディスクから仮想ディスクへ、またはその逆のクローニングなど。

タスク概要

- SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.Configファイルにあるの`PredefinedWindowsScriptsDirectory`キーを使用して定義します。

  必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

  キーの値は、API を介して Swagger から表示できます: API /4.7/configsettings

  GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。

- 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。

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、リストから ファイル システム を選択します。
3. ホストを選択します。

   リソースが保護されていれば、トポロジ ビューが自動的に表示されます。

4. リソース リストからクローニングするバックアップを選択し、クローン アイコンをクリックします。
5. [Options]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。
「マウント ポイントの自動割り当て」または「パスの下のボリューム マウント ポイントの自動割り当て」	マウント ポイントを自動的に割り当てるか、またはパスを指定してボリューム マウント ポイントを自動的に割り当てるかを選択します。 パスの下のボリューム マウント ポイントを自動割り当て: パスの下のマウント ポイントを使用すると、マウント ポイントが作成される特定のディレクトリを指定できます。このオプションを選択する場合は、ディレクトリが空であることを事前に確認しておく必要があります。ディレクトリにバックアップが格納されている場合、そのバックアップはマウント処理後に無効な状態になります。
Archive location	セカンダリ バックアップをクローニングする場合にアーカイブの場所を選択します。

6. [Script]ページで、実行するプリスクリプトやポストスクリプトがあれば指定します。

   プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

7. 概要を確認し、[完了] をクリックします。
8. 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. 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" 。

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。

クローニング処理のキャンセル

キューに登録されているクローニング処理はキャンセルできます。

クローニング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。

タスク概要

- キューに入れられたクローン操作は、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。
- 実行中のクローニング処理はキャンセルできません。
- キューに登録されているクローニング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。
- 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クローン操作をキャンセルできます。

手順

次のいずれかを実行します。

方法	アクション
[Monitor]ページ	1. 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。 2. 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	1. クローン操作を開始したら、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。 2. 処理を選択します。 3. *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。

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"

著作権に関する情報

商標に関する情報