



# Microsoft Exchange Serverデータベースの保護

## SnapCenter Software 6.0

NetApp  
September 23, 2024

# 目次

Microsoft Exchange Serverデータベースの保護 .....	1
SnapCenter Plug-in for Microsoft Exchange Serverの概念 .....	1
SnapCenter Plug-in for Microsoft Exchange Serverのインストール .....	11
SnapCenter Plug-in for VMware vSphereのインストール .....	31
データ保護の準備 .....	32
Exchangeリソースのバックアップ .....	34
Exchangeリソースのリストア .....	58

# Microsoft Exchange Serverデータベースの保護

## SnapCenter Plug-in for Microsoft Exchange Serverの概念

### SnapCenter Plug-in for Microsoft Exchange Serverの概要

SnapCenter Plug-in for Microsoft Exchange Serverは、Exchangeデータベースに対応したデータ保護管理を可能にする、NetApp SnapCenterソフトウェアのホスト側コンポーネントです。Plug-in for Exchangeを使用すると、SnapCenter環境でのExchangeデータベースのバックアップとリストアが自動化されます。

Plug-in for Exchangeがインストールされている場合は、SnapCenterとNetApp SnapMirrorテクノロジーを使用して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したり、NetApp SnapVaultテクノロジーを使用して標準への準拠やアーカイブ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したりできます。

Exchangeデータベース全体ではなく、Eメールまたはメールボックス全体をリストアおよびリカバリする場合は、Single Mailbox Recovery (SMBR) ソフトウェアを使用できます。NetApp@Single Mailbox Recoveryは、2023年5月12日に販売終了 (EOA) になりました。NetAppは、2020年6月24日に導入されたマーケティング用パーツ番号を通じて、メールボックスの容量、メンテナンス、サポートを購入したお客様をサポート対象期間中も引き続きサポートします。

NetApp Single Mailbox Recoveryは、Ontrackが提供するパートナー製品です。Ontrack PowerControlsには、NetApp Single Mailbox Recoveryと同様の機能が用意されています。お客様は、新しいOntrack PowerControlsソフトウェアライセンスとOntrack PowerControlsメンテナンスおよびサポート更新をOntrackから (licensingteam@ontrack.com経由で) 購入して、メールボックスをきめ細かくリカバリできます。

Plug-in for ExchangeはSnapMirror Active Sync (当初はSnapMirror Business Continuity [SM-BC]としてリリース) をサポートしています。これにより、サイト全体に障害が発生してもビジネスサービスの運用を継続でき、アプリケーションがセカンダリコピーを使用して透過的にフェイルオーバーできるようになります。SnapMirror Active Sync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。

SnapMirror Active Syncの非対称モード、フェイルオーバーモード、または二重モード以外のモードがサポートされます。これは、最適パスがプライマリ側のLUNの所有者ノードからのみ作成されるソリューションを意味します。セカンダリクラスタパス上のI/Oは、プライマリクラスタにプロキシ経由で処理されます。同期レプリケーションは、プライマリからセカンダリへの単方向です。

### SnapCenter Plug-in for Microsoft Exchange Serverの機能

Plug-in for Exchangeを使用して、Exchange Serverデータベースのバックアップとリストアを実行できます。

- Exchange Database Availability Group (DAG ; データベース可用性グループ) 、データベース、およびレプリカセットのアクティブなインベントリの表示と管理
- バックアップ自動化の保護設定を提供するポリシーを定義
- リソースグループへのポリシーの割り当て
- 個々のDAGとデータベースを保護

- プライマリおよびセカンダリのExchangeメールボックスデータベースをバックアップする
- プライマリバックアップとセカンダリバックアップからのデータベースのリストア

## SnapCenter Plug-in for Microsoft Windowsおよびfor Microsoft Exchange Server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 プロビジョニングとデータ保護がサポートされます。サポートされるバージョンの最新情報については <https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT>、NetApp Interoperability Matrix Tool<sup>^</sup>]を参照してください。

マシン	ストレージタイプ	を使用してプロビジョニング	サポートのメモ
物理サーバ	FCセツソク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セツソクLUN	SnapCenter GUIまたはPowerShellコマンドレット	
VMware VM	FCまたはiSCSI HBAで接続されたRDM LUN	PowerShellコマンドレット	物理的な互換性のみ   VMDKはサポートされません。
VMware VM	iSCSIイニシエータによってゲストシステムに直接接続されたiSCSI LUN	SnapCenter GUIまたはPowerShellコマンドレット	 VMDKはサポートされません。

マシン	ストレージタイプ	を使用してプロビジョニング	サポートのメモ
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 GUIまたはPowerShellコマンドレット	<p>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をプロビジョニングするには、Hyper-V Managerを使用する必要があります。</p> <p> Hyper-V のパススルーディスク、およびネットアップストレージでプロビジョニングされたVHD (x) でのデータベースのバックアップはサポートされていません。</p>
Hyper-V VM	iSCSIイニシエータによってゲストシステムに直接接続されたiSCSI LUN	SnapCenter GUIまたはPowerShellコマンドレット	<p> Hyper-V のパススルーディスク、およびネットアップストレージでプロビジョニングされたVHD (x) でのデータベースのバックアップはサポートされていません。</p>

## Exchange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。

- フルアクセスコマンド： ONTAP 8.3.0 以降に必要な最小権限
  - event generate-autosupport-log

- ジョブ履歴の表示
- ジョブの停止
- LUN
- LUNの作成
- LUNの作成
- LUNの作成
- lun delete
- LUN igroupの追加
- lun igroup create
- lun igroup delete
- LUN igroupの名前変更
- LUN igroupの名前変更
- lun igroup show
- LUNマッピングの追加-レポートノード
- LUNマッピングの作成
- LUNマッピングの削除
- lun mapping remove-reporting-nodes
- lun mapping show
- LUN変更
- ボリューム内でのLUNの移動
- LUNオフライン
- LUNオンライン
- LUN永続的予約のクリア
- LUNのサイズ変更
- LUNシリアル
- lun show
- SnapMirrorポリシーadd-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- SnapMirrorリストア
- snapmirror show
- snapmirror show-history
- SnapMirrorの更新
- snapmirror update-ls-set

- snapmirror list-destinations
- バージョン
- ボリュームのクローン作成
- volume clone show
- ボリュームクローンスプリットの開始
- ボリュームクローンスプリットの停止
- ボリュームの作成
- ボリュームの削除
- volume file clone create
- volume file show-disk-usage
- ボリュームはオフライン
- ボリュームはオンライン
- ボリュームの変更
- ボリュームqtreeの作成
- volume qtree delete
- volume qtree modify
- volume qtree show
- ボリュームの制限
- volume show
- ボリュームSnapshotの作成
- ボリュームSnapshotの削除
- ボリュームSnapshotの変更
- volume snapshot modify -snaplock-expiry-time
- ボリュームSnapshotの名前変更
- ボリュームSnapshotリストア
- ボリュームSnapshotリストア-ファイル
- volume snapshot show
- ボリュームのアンマウント
- SVM CIFS
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy show
- vserver cifs share show
- vserver cifs show
- SVM export-policy
- vserver export-policy create

- vservers export-policy delete
- vservers export-policy rule create
- vservers export-policy rule show
- vservers export-policy show
- SVM iSCSI
- vservers iscsi connection show
- vservers show
- 読み取り専用コマンド： ONTAP 8.3.0 以降に必要な最小権限
  - ネットワークインターフェイス
  - 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ONTAP SnapMirrorテクノロジーを併用すると、バックアップセットのミラーコピーを別のボリュームに作成できます。また、ONTAP SnapVaultテクノロジーを併用すると、標準への準拠やその他のガバナンス関連の目的でディスクツーディスクのバックアップレプリケーションを実行できます。これらのタスクを実行する前に、ソースボリュームとデスティネーションボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

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



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

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



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

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



SnapCenter は \* sync-mirror \* レプリケーションをサポートしていません。

## Exchange Serverリソースのバックアップ戦略を定義する

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こと、データベースの正常なリストア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、Service Level Agreement (SLA；サービスレベルアグリーメント)、Recovery Time Objective (RTO；目標復旧時間)、Recovery Point Objective (RPO；目標復旧時点) によって決まります。

SLAは、期待されるサービスレベルと、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）への対処方法を定義したものです。RTOは、サービスの停止後にビジネスプロセスをリストアする必要があるまでの時間です。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、RPOがバックアップ戦略に影響します。

### Exchangeデータベースでサポートされるバックアップのタイプ

SnapCenterを使用してExchangeメールボックスをバックアップするには、リソースタイプ（データベースやDatabase Availability Group (DAG；データベース可用性グループ) など）を選択する必要があります。Snapshotテクノロジーを使用して、リソースが配置されているボリュームのオンラインの読み取り専用コピーが作成されます。

バックアップタイプ	説明
フルバックアップとログバックアップ	<p>データベースと、切り捨てられるログを含むすべてのトランザクションログがバックアップされます。</p> <p>フルバックアップが完了すると、Exchange Serverはデータベースにコミット済みのトランザクションログを切り捨てます。</p> <p>通常は、このオプションを選択する必要があります。ただし、バックアップ時間が短い場合は、フルバックアップでトランザクションログバックアップを実行しないように選択できます。</p>
フルバックアップ	<p>データベースおよびトランザクションログがバックアップされます。</p> <p>切り捨てられたトランザクションログはバックアップされません。</p>
ログバックアップ	<p>すべてのトランザクションログがバックアップされます。</p> <p>データベースにコミット済みの切り捨てられたログはバックアップされません。フルデータベースバックアップの間にトランザクションログを頻繁にバックアップするようにスケジュールを設定すると、リカバリポイントをきめ細かく選択できます。</p>

## データベースプラグインのバックアップスケジュール

バックアップ頻度（スケジュールタイプ）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し、使用頻度の低いリソースは1日に1回バックアップすることもできます。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、期待されるサービスレベルと、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）への対処方法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影響します。

使用頻度の高いリソースであっても、フルバックアップを1日に1~2回以上実行する必要はありません。たとえば、定期的なトランザクションログバックアップで十分な場合は、必要なバックアップを作成できます。データベ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トランザクション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。

バックアップスケジュールには、次の2つの部分があります。

- 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 `_schedule type__` と呼ばれます。ポリシーでは、バックアップ頻度として、毎時、毎日、毎週、または毎月を選択できます。頻度を選択しない場合は、オンデマンドのみのポリシーが作成されます。ポリシーにアクセスするには、`* Settings * > * Policies *` をクリックします。

- 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タイミング）は、リソースグループ設定の一部です。たとえば、リソースグループのポリシーで週単位のバックアップが設定されている場合は、毎週木曜日の午後10時にバックアップが実行されるようにスケジュールを設定できます。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 * > * リソースグループ *` をクリックします。

## データベースに必要なバックアップジョブの数

必要なバックアップジョブの数を左右する要因には、リソースのサイズ、使用されているボリュームの数、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。

## バックアップの命名規則

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

Snapshotでは、次のデフォルトの命名規則が使用されます。

```
resourcegroupname_hostname_timestamp
```

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

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

この例では、各構文要素に次の意味があります。

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

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

### 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ことも、保持するバックアップコピーの数（ONTAPの最大コピー数255）を指定することもできます。たとえば、組織で、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する必要があるとします。

ポリシーの作成時に、バックアップタイプと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、保持されているバックアップの保持ラベルがスケジュールタイプと一致する場合には、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のスケジュールタイプを変更した場合、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。

### Exchange Serverのソースストレージボリュームにトランザクションログバックアップを保持する期間

SnapCenter Plug-in for Microsoft Exchange Serverでは、最新の状態へのリストア処理を実行するためにトランザクションログバックアップが必要です。この場合、2つのフルバックアップの間の任意の時点の状態にデータベースがリストアされます。

たとえば、Plug-in for Exchangeで午前8時にフルバックアップとトランザクションログバックアップが、午後5時に別のフルバックアップとトランザクションログバックアップが作成された場合、最新のトランザクションログバックアップを使用して、午前8時から午後5時の任意の時点にデータベースをリストアできます。トランザクションログが使用できない場合、Plug-in for Exchangeはポイントインタイムリストア処理のみを実行できます。この場合、Plug-in for Exchangeはフルバックアップがフルバックアップを完了した時点のフルバックアップが完了した時点でデータベースをリストアできます。

通常、最新の状態へのリストア処理が必要になるのは1~2日です。デフォルトでは、SnapCenterの保持期間は最低2日です。

## Exchangeデータベースのリストア戦略を定義する

Exchange Serverのリストア戦略を定義しておく、データベースを正常にリストアできます。

### Exchange Serverでのリストア処理のソース

プライマリストレージ上のバックアップコピーからExchange Serverデータベースをリストアできます。

データベースはプライマリストレージからのみリストアできます。

### Exchange Serverでサポートされるリストア処理のタイプ

SnapCenterを使用すると、Exchangeリソースに対してさまざまなタイプのリストア処理を実行できます。

- 最新の状態へのリストア
- 過去のポイントインタイムへのリストア

#### 最新の状態へのリストア

最新の状態へのリストア処理では、障害発生時点までデータベースがリカバリされます。SnapCenterでは、この処理が次の順序で実行されます。

1. 選択したフルデータベースバックアップからデータベースをリストアします。
2. バックアップされたすべてのトランザクション・ログ、および最新のバックアップ以降に作成された新しいログが適用されます。

トランザクションログは先に移動され、選択したデータベースに適用されます。

リストアの完了後、Exchangeは新しいログチェーンを作成します。

\* ベストプラクティス： \* リストアの完了後に、新しいフルバックアップとログバックアップを実行することを推奨します。

最新の状態へのリストア処理では、連続するトランザクションログセットが必要です。

最新の状態へのリストアの実行後は、リストアに使用したバックアップをポイントインタイムリストア処理でのみ使用できます。

すべてのバックアップに対して最新の状態へのリストア機能を実行する必要がない場合は、バックアップポリシーを使用してシステムのトランザクションログバックアップの保持を設定できます。

#### 過去のポイントインタイムへのリストア

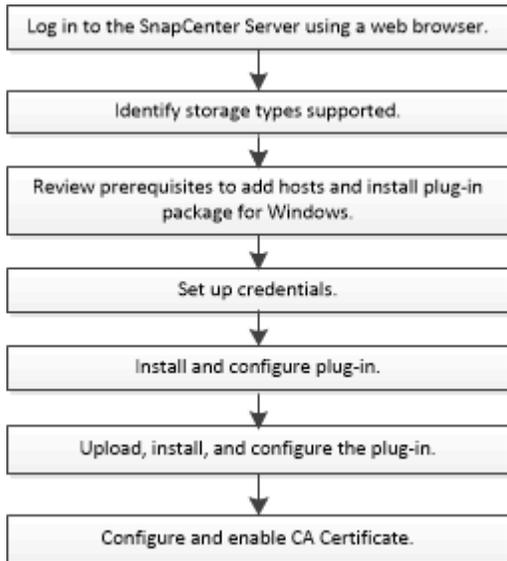
ポイントインタイムリストア処理では、データベースは過去の特定の時刻にのみリストアされます。ポイントインタイムリストア処理は、次の状況で実行されます。

- データベースは、バックアップトランザクションログの所定の時間にリストアされます。
- データベースがリストアされ、一部のバックアップトランザクションログのみが適用されます。

# SnapCenter Plug-in for Microsoft Exchange Serverのインストール

## SnapCenter Plug-in for Microsoft Exchange Serverのインストールワークフロー

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



ホストを追加して**SnapCenter Plug-in for Microsoft Exchange Server**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。

- 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。
- ローカル管理者Privilegesを持つドメインユーザと、リモートホストに対するローカルログイン権限が必要です。
- スタンドアロン構成およびデータベース可用性グループ構成にMicrosoft Exchange Server 2013、2016、または2019を使用している必要があります。
- Windowsホストにプラグインをインストールするときに、組み込みでないクレデンシャルを指定した場合やユーザがローカルワークグループに属している場合は、ホストのUACを無効にする必要があります。
- SnapCenter 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を持つユーザが必要です。
- Exchange Serverの管理権限を持つユーザが必要です。
- SnapManager for Microsoft Exchange ServerおよびSnapDrive for Windowsがすでにインストールされている場合は、SnapCenterを使用したデータ保護を確実にを行うために、同じExchange ServerにPlug-in for Exchangeをインストールする前に、SnapDrive for Windowsで使用するVSSハードウェアプロバイダの登録を解除する必要があります。
- SnapManager for Microsoft Exchange Server と Plug-in for Exchange が同じサーバにインストールされている場合は、SnapManager for Microsoft Exchange Server で作成されたすべてのスケジュールを

Windows スケジューラから一時停止または削除する必要があります。

- ホストをサーバから完全修飾ドメイン名 (FQDN) に解決できる必要があります。hosts ファイルが解決可能になるように変更され、短縮名と FQDN の両方が hosts ファイルに指定されている場合は、SnapCenter hosts ファイルに次の形式でエントリを作成します： `_<IP_address><host_fqdn><host_name>_`。
- 次のポートがファイアウォールでブロックされていないことを確認してください。ブロックされていないと、ホストの追加処理が失敗します。この問題を解決するには、ダイナミックポート範囲を設定する必要があります。詳細については、を参照してください "[Microsoftのドキュメント](#)"。
  - ポート範囲50000~51000 (Windows 2016およびExchange 2016の場合)
  - Windows Server 2012 R2およびExchange 2013のポート範囲6000~6500
  - Windows 2019のポート範囲49152~65536

ポート範囲を特定するには、次のコマンドを実行します。



- netsh int ipv4 show dynamicport tcp
- netsh int ipv4 show dynamicport udp
- netsh int ipv6 show dynamicport tcp を実行します
- netsh int ipv6 show dynamicport udp

## 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、基本的なホストシステムのスペース要件とサイジング要件を理解しておく必要があります。

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

項目	要件
必要なソフトウェアパッケージ	<ul style="list-style-type: none"> <li>• です。 ネットコア8.0.5</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle JavaおよびOpenJDK</li> </ul> <p>サポートされているバージョンの最新情報については、を参照して "<a href="#">NetApp Interoperability Matrix Tool</a>" ください。</p> <p>用。 NET固有のトラブルシューティング情報。を参照してください。 "インターネットに接続されていない従来型システムでは、SnapCenter のアップグレードまたはインストールが失敗します。"</p>

### 必要なExchange Serverの権限

SnapCenter で Exchange サーバまたは DAG を追加し、ホストまたは DAG に SnapCenter Plug-in for Microsoft Exchange Server をインストールできるようにするには、最小限の権限と権限を持つユーザのクレデンシャルを SnapCenter に設定する必要があります。

ドメインユーザには、ローカル管理者権限、リモートExchangeホストに対するローカルログイン権限、DAG内のすべてのノードに対する管理権限が必要です。ドメインユーザに必要な最小権限は次のとおりです。

- Add-MailboxDatabaseCopy
- Dismount -データベース
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- MOVE-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly : \$true
- マウント-データベース
- New-MailboxDatabase
- 新規- PublicFolderDatabase
- Remove-MailboxDatabase
- 削除-MailboxDatabaseCopy
- 削除- PublicFolderDatabase
- 再開- MailboxDatabaseCopy

- Set-AdServerSettings
- set-MailboxDatabase-allowfilerestore : \$true
- MailboxDatabaseCopyの設定
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

## 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、基本的なホストシステムのスペース要件とサイジング要件を理解しておく必要があります。

項目	要件
オペレーティングシステム	Microsoft Windows  サポートされているバージョンの最新情報については、を参照して " <a href="#">NetApp Interoperability Matrix Tool</a> " ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
ホスト上のSnapCenterプラグインのインストールとログの最小スペース	5GB  <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>十分なディスクスペースを割り当て、logsフォルダによるストレージ消費量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、最近実行した処理のログは作成されません。</p> </div>
必要なソフトウェアパッケージ	<ul style="list-style-type: none"> <li>• です。 ネットコア8.0.5</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle JavaおよびOpenJDK</li> </ul> <p>サポートされているバージョンの最新情報については、を参照して "<a href="#">NetApp Interoperability Matrix Tool</a>" ください。</p> <p>用。 NET固有のトラブルシューティング情報。を参照してください。 "<a href="#">インターネットに接続されていない従来型システムでは、SnapCenterのアップグレードまたはインストールが失敗します。</a>"</p>

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

SnapCenter は、クレデンシャルを使用して SnapCenter 処理を実行するユーザを認証します。プラグインパッケージのインストールに使用するクレデンシャルと、データベースでデータ保護処理を実行するためのクレデンシャルをそれぞれ作成する必要があります。

### タスクの内容

Windowsホストにプラグインをインストールするには、クレデンシャルを設定する必要があります。Windowsのクレデンシャルは、ホストを導入してプラグインをインストールしたあとに作成することもできますが、SVMを追加したあと、ホストの導入とプラグインのインストールを開始する前に作成することを推奨します。

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）を設定します。

個々のリソースグループのクレデンシャルを設定し、ユーザ名に完全なadmin権限がない場合は、少なくともリソースグループとバックアップ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. [ 新規作成 ( New ) ] をクリックする。

[クレデンシャル]ウィンドウが表示されます。

4. [Credential]ページで、次の手順を実行します。

フィールド	操作
クレデンシャル名	クレデンシャルの名前を入力します。

フィールド	操作
ユーザ名	<p>認証に使用するユーザ名を入力します。</p> <ul style="list-style-type: none"> <li>ドメイン管理者または管理者グループの任意のメンバー</li> </ul> <p>ドメイン管理者またはSnapCenterプラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。ユーザ名フィールドの有効な形式は次のとおりです。</p> <ul style="list-style-type: none"> <li>◦ NetBIOS\UserName</li> <li>◦ Domain FQDN\UserName</li> </ul> <ul style="list-style-type: none"> <li>ローカル管理者（ワークグループのみ）</li> </ul> <p>ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。[Username]フィールドの有効な形式は次のとおりです。</p> <p>UserName</p>
パスワード	<p>認証に使用するパスワードを入力します。</p>
認証	<p>認証モードとして[Windows]を選択します。</p>

5. [OK]\*をクリックします。

## Windows Server 2016以降でのgMSAの設定

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

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

- KDSルートキーを作成して、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。
- ドメインごとに、Windows ドメインコントローラから次のコマンドを実行します。Add-KDSRootKey -EffectiveImmediant

### 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。
```

例えば、

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

### 4. ホストでgMSAを設定します。

- a. gMSAアカウントを使用するホストで、Windows PowerShell用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で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サーバで設定済みのgMSAアカウントを指定してWindowsホストを追加します。

選択したプラグインがSnapCenterサーバにインストールされ、指定したgMSAがプラグインのインストール時にサービスのログオンアカウントとして使用されます。

## ホストを追加して**Plug-in for Exchange**をインストールする

SnapCenterの[ホストの追加]ページを使用して、Windowsホストを追加できます。Plug-in for Exchangeは指定したホストに自動的にインストールされます。プラグインのインストールには、この方法を推奨します。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ときに、組み込みでないクレデンシャルを指定する場合は、ユーザがローカルワークグループに属している場合は、ホストのUACを無効にする必要があります。
- メッセージキューサービスが実行されている必要があります。
- 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。詳細については、[を参照してください "Microsoft Exchange Server 2016 以降でグループマネージドサービスアカウントを設定します"](#)。

### タスクの内容

- SnapCenterサーバをプラグインホストとして別のSnapCenterサーバに追加することはできません。
- 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せん。
- ExchangeノードがDAGの一部である場合、SnapCenterサーバにノードを1つだけ追加することはできません。
- クラスタ (Exchange DAG) にプラグインをインストールする場合は、ネットアップ LUN 上にデータベースがないノードがある場合でも、クラスタのすべてのノードにインストールされます。

SnapCenter 4.6以降では、SCEはマルチテナンシーをサポートしており、次の方法でホストを追加できます。

ホスト追加処理	4.5以前	4.6以降
IPを使用しないDAGをクロスドメインまたは別のドメインに追加する	サポート対象外	サポート対象

ホスト追加処理	4.5以前	4.6以降
同じドメインまたはクロスドメインに存在する一意の名前を持つ複数のIP DAGを追加する	サポート対象	サポート対象
クロスドメインに同じホスト名またはDB名を持つIPまたはIPを使用しないDAGを複数追加する	サポート対象外	サポート対象
同じ名前でもクロスドメインのIP/IPを使用しないDAGを複数追加する	サポート対象外	サポート対象
同じ名前でもクロスドメインの複数のスタンドアロンホストを追加する	サポート対象外	サポート対象

Plug-in for ExchangeはSnapCenter Plug-ins Package for Windowsに依存し、同じバージョンである必要があります。Plug-in for Exchangeのインストール時には、SnapCenter Plug-ins Package for Windowsがデフォルトで選択され、VSSハードウェアプロバイダとともにインストールされます。

SnapManager for Microsoft Exchange ServerおよびSnapDrive for Windowsがすでにインストールされている場合は、また、Plug-in for Exchangeを同じExchangeサーバにインストールする場合は、SnapDrive for Windowsで使用するVSSハードウェアプロバイダの登録を解除する必要があります。これは、Plug-in for ExchangeおよびSnapCenter Plug-ins Package for WindowsとともにインストールされたVSSハードウェアプロバイダとの互換性がないためです。詳細については、を参照してください "[Data ONTAP VSS ハードウェアプロバイダを手動で登録する方法](#)"。

#### 手順

1. 左側のナビゲーションペインで、\* Hosts \* (ホスト) をクリックします。
2. 上部で [Managed Hosts] 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、次の手順を実行します。

フィールド	操作
ホストタイプ	<p>ホストタイプとして * windows * を選択します。</p> <p>SnapCenter サーバによってホストが追加され、Plug-in for Windows と Plug-in for Exchange がまだインストールされていない場合はホストにインストールされます。</p> <p>Plug-in for Windows および Plug-in for Exchange のバージョンが同じである必要があります。以前に別のバージョンの Plug-in for Windows がインストールされていた場合、SnapCenter のインストール時にこのバージョンが更新されます。</p>

フィールド	操作
ホスト名	<p>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。</p> <p>SnapCenter は、DNS の適切な設定によって異なります。そのため、Fully Qualified Domain Name (FQDN ; 完全修飾ドメイン名) を入力することを推奨します。</p> <p>信頼されていないドメインホストのIPアドレスは、そのIPアドレスがFQDNに解決される場合のみサポートされます。</p> <p>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。</p> <p>次のいずれかのIPアドレスまたはFQDNを入力できます。</p> <ul style="list-style-type: none"> <li>• スタンドアロンホスト</li> <li>• Exchange DAG</li> </ul> <p>Exchange DAGの場合は、次の操作を実行できます。</p> <ul style="list-style-type: none"> <li>◦ DAG名、DAG IPアドレス、ノード名、またはノードIPアドレスを指定してDAGを追加します。</li> <li>◦ いずれかのDAGクラスタノードのIPアドレスまたはFQDNを指定して、IPのないDAGクラスタを追加します。</li> <li>◦ 同じドメインまたは別のドメインに存在するIPのないDAGを追加します。IP/IPを含まないDAGは、同じ名前でもドメインが異なる複数追加することもできます。</li> </ul> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> スタンドアロンホストまたはExchange DAG (ドメイン間または同じドメイン) の場合は、ホストまたはDAGのFQDNまたはIPアドレスを指定することを推奨します。</p> </div>

フィールド	操作
クレデンシャル	<p>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。</p> <p>このクレデンシャルには、リモートホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。</p> <p>指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>資格情報認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。</p> </div>

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。

Plug-in for Exchange を選択すると、SnapCenter Plug-in for Microsoft SQL Server の選択が自動的に解除されます。Microsoftでは、Exchangeに必要なメモリ使用量やその他のリソース使用量を考慮して、SQL ServerとExchangeサーバを同じシステムにインストールしないことを推奨しています。

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	<p>デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。</p> <p>デフォルトのポート番号は8145です。SnapCenterサーバがカスタムポートにインストールされている場合は、そのポート番号がデフォルトポートとして表示されます。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>プラグインを手動でインストールし、カスタムポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理は失敗します。</p> </div>
インストールパス	<p>デフォルトのパスはです C:\Program Files\NetApp\SnapCenter。</p> <p>必要に応じてパスをカスタマイズできます。</p>
DAG内のすべてのホストを追加	<p>DAGを追加する場合は、このチェックボックスをオンにします。</p>

フィールド	操作
インストール前チェックをスキップ	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選択します。
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	<p>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選択します。</p> <p>gMSA 名を <i>domainName\accountName\$</i> の形式で指定します。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>gMSAは、SnapCenter Plug-in for Windowsサービスのログオンサービスアカウントとしてのみ使用されません。</p> </div>

7. [Submit (送信) ] をクリックします。

[Skip prechecks]チェック ボックスをオフにしていると、ホストがプラグインをインストールするための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。最小要件を満たしていない場合は、該当するエラーまたは警告メッセージが表示されます。

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



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

8. インストールの進行状況を監視します。

#### ネットTCP通信用のカスタムポートの設定

SnapCenter 6.0リリース以降、SnapCenter Plug-in for Windowsでは、デフォルトでポート909がネットTCP通信に使用されます。ポート909が使用中の場合は、ネットTCP通信用に別のポートを設定できます。

#### 手順

1. `_C : \Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vsproviders\navssprv.exe.config`にある `_NetTCPPort_key`の値を必要なポート番号に変更します。  
`<add key="NetTCPPort" value="new_port_number" />`
2. `C : \Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\SnapDriveService.dll.config`にある `_NetTCPPort_key`の値を必要なポート番号に変更します。  
`<add key="NetTCPPort" value="new_port_number" />`
3. 次のコマンドを実行して、Data ONTAP VSSハードウェアプロバイダサービスの登録を解除します。  
`"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\navssprv.exe" -r service -u`

サービスが `_services.msc_` のサービスのリストに表示されていないことを確認します。

4. 次のコマンドを実行して、 `_Data ONTAP VSS Hardware Provider_service` を登録します。 `"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"`

サービスが `_services.msc_` のサービスのリストに表示されていることを確認します。

5. `_Plug-in for windows_service` を再起動します。

## PowerShellコマンドレットを使用したSnapCenter ServerホストからのPlug-in for Exchangeのインストール

Plug-in for Exchange は SnapCenter の GUI からインストールする必要があります。GUI を使用しない場合は、SnapCenterサーバホストまたはリモートホストでPowerShellコマンドレットを使用できます。

開始する前に

- SnapCenter サーバがインストールおよび設定されている必要があります。
- ホストのローカル管理者、または管理者権限を持つユーザである必要があります。
- この処理は、SnapCenter Admin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。
- Plug-in for Exchange をインストールする前に、サポートされている構成のインストール要件と種類を確認しておく必要があります。
- Plug-in for Exchange をインストールするホストには Windows ホストを使用する必要があります。

手順

1. SnapCenter サーバホストで、 `_Open-SmConnection_cmdlet` 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。
2. Plug-in for Exchange をインストールするホストを追加するには、 `_Add-SmHost_cmdlet` と必要なパラメータを使用します。

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

ホストはスタンドアロンホストでもDAGでもかまいません。DAG を指定する場合は、 `-IsDAG_parameter` が必要です。

3. 必要なパラメータを指定して、 `_Install-SmHostPackage_cmdlet` を使用し、 Plug-in for Exchange をインストールします。

このコマンドは、指定したホストに Plug-in for Exchange をインストールし、 SnapCenter にプラグインを登録します。

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

Plug-in for Exchange は、 SnapCenter ユーザーインターフェイス内からインストールする必要があります。ただし、何らかの理由でインストールできない場合は、 Windows のコマンドラインから、 Plug-in for Exchange 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

- Microsoft Exchange Serverリソースをバックアップしておく必要があります。
- SnapCenter プラグインパッケージをインストールしておく必要があります。
- をインストールする前に、以前のリリースの SnapCenter Plug-in for Microsoft SQL Server を削除する必要があります。

詳細については、を参照してください ["SnapCenter Plug-in をプラグインホストから手動で直接インストールする方法"](#)。

手順

1. プラグインホストに `_C : \temp_folder` が存在し、ログインしているユーザにフルアクセス権があるかどうかを確認します。
2. `C : \ProgramData\NetApp\SnapCenter \Package_Repository` から SnapCenter Plug-in for Microsoft Windows をダウンロードします。

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

3. 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。
4. ローカルホストのWindowsコマンドプロンプトで、プラグインのインストールファイルを保存したディレクトリに移動します。
5. 次のコマンドを入力してプラグインをインストールします。

```
_snapcenter_windows_host_plugin.exe "/silent/debuglog "<Debug_Log_Path>" /log" <Log_Path>"  
b_SNAPCENTER_port=<Num>Suite_INSTALLDIR="<Install_Directory_Path>"  
BV_ServiceAccount=<domain\administrator> BV_SERVICEPCPWD = <SCW> インストール、 ISW<
```

例：

```
C : \ProgramData\NetApp\SnapCenter \Package_Repository_snapcenter_windows_host_plugin.exe  
"/silent/debuglog" C : \HPPW_SCSQL_Install.log "/log" C : \temp\temp\b_SNAPCENTER_PORT = 8145  
Suite_INSTALLDIR=" C : \Program Files\NetApp\SnapManager SnapCenter \BIT_VISPRI 管理者パスワードです
```



Plug-in for Exchange 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。

変数には次の値を入力します。

変数	値
	次の例のように、スイートインストーラログファイルの名前と場所を指定します。  <code>Setup.exe /debuglog "C:\PathToLog\setupexe.log</code>
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。
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 によってリモートホストに導入される解決策を指定します。

- Windows タスクスケジューラ、メインインストールログファイル `C:\Installdebug.log`、およびその他のインストールファイルを `C:\Temp` で監視します。
- `%temp%` ディレクトリを監視して、`_msiexe.exe_installers` がエラーなしでソフトウェアをインストールしているかどうかを確認します。



Plug-in for Exchange をインストールすると、SnapCenter サーバ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で、SnapCenter サーバ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

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

タスクの内容

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中
- 完了しました
- 失敗
-

 完了（警告あり）または警告のため開始できませんでした

-  キューに登録済み

#### 手順

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

## CA証明書の設定

### CA証明書CSRファイルの生成

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

CSRはエンコードされたテキストのブロックであり、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RSAキーの長さは3072ビット以上にする必要があります。

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

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

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

### CA証明書のインポート

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

## 手順

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

ウィザードウィンドウ	操作
秘密キーのインポート	オプション * はい * を選択し、秘密鍵をインポートして、* 次へ * をクリックします。
インポートファイル形式	変更せずに、* 次へ * をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、* Next * をクリックします。
証明書のインポートウィザードの完了	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。



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

7. 「Personal」フォルダに対して手順5を繰り返します。

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

## 手順

1. GUIで次の手順を実行します。
  - a. 証明書をダブルクリックします。
  - b. [証明書] ダイアログボックスで、[\* 詳細 \*] タブをクリックします。
  - c. フィールドのリストをスクロールし、[Thumbprint] をクリックします。
  - d. ボックスから16進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、サムプリントが「A9 09 50 2D d8 2a 14 33 e6 F8 38 86 b0 0d 42 77 A3 2a 7b」の場合、

スペースを削除すると、「a909502dd82ae41433e6f83886b00d4277a32a7b」となります。

2. PowerShellから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 - パス証明書 : \localmachine\My
```

- b. サムプリントをコピーします。

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

### 手順

1. 次のコマンドを実行して、SMCoreのデフォルトポート8145を使用して既存の証明書バインディングを削除します。

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

例：

```
> netsh http delete sslcert ipport=0.0.0.0:8145  
. 次のコマンドを実行して、新しくインストールした証明書を  
Windowsホストの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：

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

プラグインに対してCA証明書を有効にする

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

開始する前に

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

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

手順

1. 左側のナビゲーションペインで、 `* Hosts *` (ホスト) をクリックします。
2. [Hosts] ページで、 [`*Managed Hosts`] をクリックします。
3. 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

[管理対象ホスト] タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバ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おらず、プラグインホストにも割り当てられていないことを示します。
- \*\*  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。

## ExchangeとSnapCenterが共存するようにSnapManager 7.xを設定する

SnapCenter Plug-in for Microsoft Exchange ServerをSnapManager for Microsoft Exchange Serverと共存させるには、SnapManager for Microsoft Exchange ServerがインストールされているExchange ServerにSnapCenter Plug-in for Microsoft Exchange Serverをインストールし、SnapManager for Exchangeのスケジュールを無効にして、SnapCenter Plug-in for Microsoft Exchange Serverを使用して新しいスケジュールとバックアップを設定する必要があります。

開始する前に

- SnapManager for Microsoft Exchange ServerおよびSnapDrive for Windowsがすでにインストールされており、SnapManager for Microsoft Exchange Serverのバックアップがシステム上およびSnapInfoディレク

トリに存在します。

- 不要になったSnapManager for Microsoft Exchange Serverで作成したバックアップを削除または再利用しておく必要があります。
- SnapManager for Microsoft Exchange Serverで作成したすべてのスケジュールをWindowsスケジューラで一時停止または削除しておく必要があります。
- SnapCenter Plug-in for Microsoft Exchange ServerとSnapManager for Microsoft Exchange Serverは同じExchange Serverに共存できますが、既存のSnapManager for Microsoft Exchange Server環境をSnapCenterにアップグレードすることはできません。

SnapCenterにはアップグレードオプションがありません。

- SnapCenterでは、SnapManager for Microsoft Exchange ServerバックアップからのExchangeデータベースのリストアはサポートされていません。

SnapCenter Plug-in for Microsoft Exchange Serverのインストール後にSnapManager for Microsoft Exchange Serverをアンインストールせずに、あとでSnapManager for Microsoft Exchange Serverのバックアップをリストアする場合は、追加の手順を実行する必要があります。

## 手順

1. すべての DAG ノードで PowerShell を使用して、SnapDrive for Windows VSS ハードウェアプロバイダが登録されているかどうかを確認します。 *vssadmin list providers*

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
Version: 7. 1. 4. 6845
```

2. SnapDrive ディレクトリから、SnapDrive for Windows から VSS ハードウェアプロバイダの登録を解除します。 *navssprv.exe -r service -u*
3. VSS ハードウェアプロバイダが削除されたことを確認します。 *vssadmin list providers*
4. SnapCenter に Exchange ホストを追加し、SnapCenter Plug-in for Microsoft Windows および SnapCenter Plug-in for Microsoft Exchange Server をインストールします。
5. すべての DAG ノードの SnapCenter Plug-in for Microsoft Windows ディレクトリで、VSS ハードウェアプロバイダが登録されていることを確認します： *vssadmin list providers*

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
  Provider type: Hardware
  Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
  Version: 7. 0. 0. 5561
```

6. SnapManager for Microsoft Exchange Server のバックアップスケジュールを停止します。
7. SnapCenter GUI を使用して、オンデマンドバックアップの作成、スケジュールされたバックアップの設定、保持の設定を行います。
8. SnapManager for Microsoft Exchange Server をアンインストールします。

SnapManager for Microsoft Exchange Server を今すぐアンインストールしないで、SnapManager for Microsoft Exchange Server のバックアップをリストアする場合は、次の手順を実行します。

- a. すべての DAG ノードから SnapCenter Plug-in for Microsoft Exchange Server の登録を解除します。  
\_navssprv.exe -r service -u \_

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
Windows>navssprv.exe -r service -u
```

- b. C : \Program Files\NetApp\SnapManager \SnapDrive\_directory から、すべての DAG ノードに SnapDrive for Windows を登録します。 \_navssprv.exe -r service -c hostname \\username -p password\_

## 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。

展開の詳細については、を参照してください ["導入の概要"](#)。

### CA証明書の導入

SnapCenter Plug-in for VMware vSphereでCA証明書を設定する方法については、を参照してください ["SSL証明書を作成またはインポートします"](#)。

### CRLファイルの設定

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリでCRLファイルを検索します。VMware vSphere用 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/config/crl\_です。

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

## データ保護の準備

バックアップ、クローニング、リストアなどのデータ保護処理を実行する場合は、事前に戦略を定義し、環境をセットアップする必要があります。また、SnapVault サーバで SnapMirror テクノロジと SnapCenter テクノロジを使用するように設定することもできます。

SnapVaultテクノロジとSnapMirrorテクノロジを利用するには、ストレージデバイスのソースボリュームとデスティネーションボリューム間のデータ保護関係を設定して初期化する必要があります。これらのタスクは、NetAppSystem Managerを使用するか、ストレージコンソールのコマンドラインを使用して実行できます。

- 詳細はこちら \*

### "REST APIの使用"

## SnapCenter Plug-in for Microsoft Exchange Serverを使用するための前提条件

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

- SnapCenterサーバをインストールして設定します。
- SnapCenter にログインします。
- SnapCenter環境を設定するために、ストレージシステム接続を追加または割り当て、クレデンシャルを作成します。



SnapCenter では、異なるクラスタにある同じ名前の SVM は複数サポートされません。SnapCenter でサポートする SVM には、それぞれ一意の名前を付ける必要があります。

- ホストを追加し、SnapCenter Plug-in for Microsoft WindowsとSnapCenter Plug-in for Microsoft Exchange Serverをインストールして、リソースを検出（更新）します。
- SnapCenter Plug-in for Microsoft Windows を使用して、ホスト側のストレージをプロビジョニングします。
- SnapCenterサーバを使用してVMware RDM LUN上にあるExchangeデータベースを保護する場合は、SnapCenter Plug-in for VMware vSphereを導入してプラグインをSnapCenterに登録する必要があります。詳細については、SnapCenter Plug-in for VMware vSphere のドキュメントを参照してください。



VMDKはサポートされません。

- Microsoft Exchangeツールを使用して、既存のMicrosoft Exchange Serverデータベースをローカルディスクからサポート対象のストレージに移動します。
- バックアップレプリケーションが必要な場合は、SnapMirror関係とSnapVault関係をセットアップします。

SnapCenter 4.1.1 ユーザの場合、SnapCenter Plug-in for VMware vSphere 4.1.1 のドキュメントには、仮想化されたデータベースとファイルシステムの保護に関する情報が記載されています。NetAppデータブローカー1.0および1.0.1のドキュメントには、SnapCenter 4.2.xのユーザ向けに、LinuxベースのNetAppデータブローカー仮想アプライアンス（オープン仮想アプライアンス形式）が提供するSnapCenter Plug-in for VMware vSphereを使用した仮想データベースおよびファイルシステムの保護に関する情報が記載されています。SnapCenter 4.3.xのユーザ向けに、SnapCenter Plug-in for VMware vSphere 4.3のドキュメントには、LinuxベースのSnapCenter Plug-in for VMware vSphere仮想アプライアンス（オープン仮想アプライアンス形式）を使用した仮想データベースとファイルシステムの保護に関する情報が記載されています。

## "SnapCenter Plug-in for VMware vSphereのドキュメント"

### Exchange Serverを保護するためのリソース、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、リストア、および再シードの処理に関連する基本的な概念を理解しておくことが役立ちます。ここでは、さまざまな処理のリソース、リソースグループ、およびポリシーを操作します。

- リソースとは、通常は、SnapCenterでバックアップするメールボックスデータベースまたはMicrosoft Exchangeデータベース可用性グループ（DAG）です。
- SnapCenterリソースグループは、ホストまたはExchange DAG上のリソースの集まりであり、リソースグループにはDAG全体または個々のデータベースを含めることができます。

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その処理が実行されます。

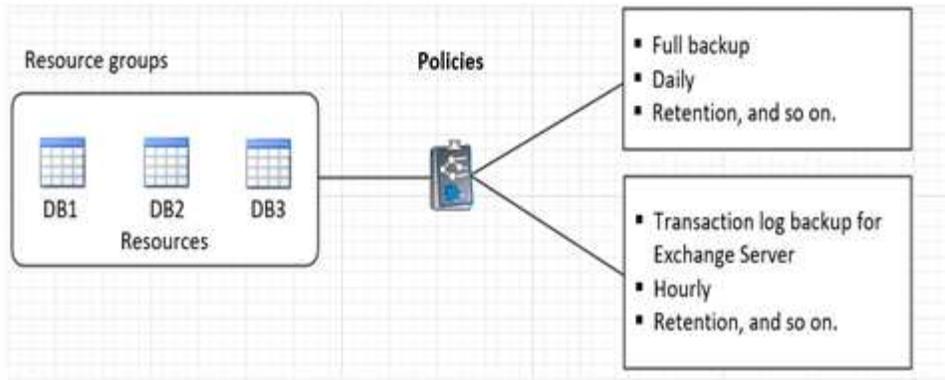
単一のリソースまたはリソースグループをオンデマンドでバックアップできます。単一のリソースおよびリソースグループに対してスケジュールされたバックアップを実行することもできます。

リソースグループは、以前はデータセットと呼ばれていました。

- ポリシーは、バックアップ頻度、コピーの保持、スクリプト、およびデータ保護処理のその他の特性を指定します。

リソースグループを作成するときに、そのグループのポリシーを1つ以上選択します。単一のリソースに対してオンデマンドでバックアップを実行する場合は、ポリシーを1つ以上選択することもできます。

リソースグループは、保護対象となるものと、曜日と時間の観点から保護する場合を定義するものと考えてください。ポリシーは、保護する方法を定義するポリシーと考えてください。たとえば、ホストのすべてのデータベースをバックアップする場合は、ホストのすべてのデータベースを含むリソースグループを作成します。そのあとに、日次ポリシーと時間次ポリシーの2つのポリシーをリソースグループに適用できます。リソースグループを作成してポリシーを適用する際に、フルバックアップを1日1回実行するようにリソースグループを設定し、別のスケジュールでログバックアップを1時間ごとに実行するように設定します。次の図は、データベースのリソース、リソースグループ、およびポリシーの関係を示しています。



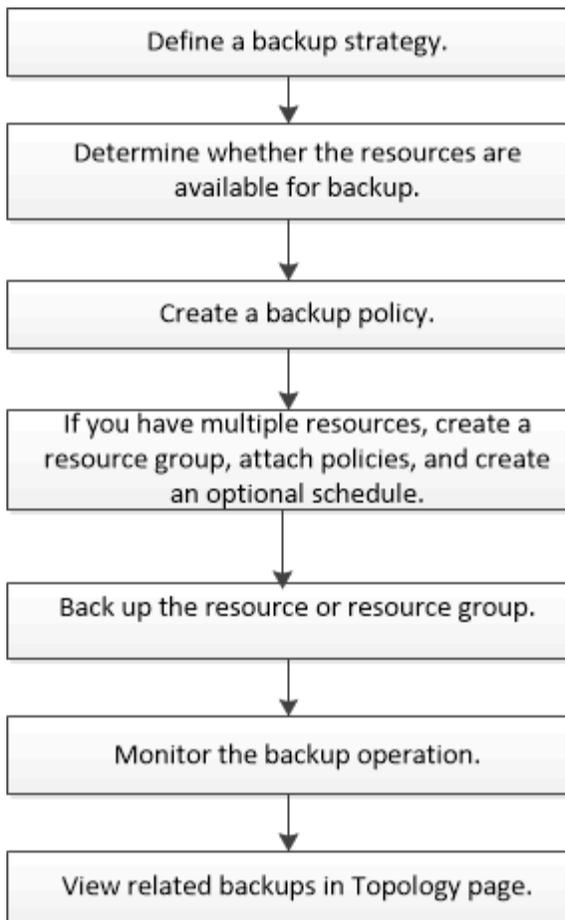
## Exchangeリソースのバックアップ

### バックアップのワークフロー

SnapCenter Plug-in for Microsoft Exchange Serverをインストールした環境では、SnapCenterを使用してExchangeリソースをバックアップできます。

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。同じボリューム上でのアクティブバックアップコピーとパッシブバックアップコピーはサポートされていません。

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。



## Exchangeデータベースとバックアップの検証

SnapCenter Plug-in for Microsoft Exchange Serverではバックアップの検証は行われませんが、Exchangeに付属のEseutilツールを使用して、Exchangeデータベースおよびバックアップを検証できます。

Microsoft Exchange Eseutilツールは、Exchangeサーバに付属のコマンドラインユーティリティです。このユーティリティを使用すると、整合性チェックを実行して、Exchangeデータベースおよびバックアップの整合性を検証できます。

\* ベストプラクティス： \* 最低 2 つのレプリカを含む DAG 構成の一部であるデータベースに対して、整合性チェックを実行する必要はありません。

詳細については、を参照してください "[Microsoft Exchange Server のマニュアル](#)"。

## Exchangeリソースをバックアップに使用できるかどうかの確認

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データベース、Exchangeデータベース可用性グループです。これらのリソースをリソースグループに追加してデータ保護ジョブを実行できますが、その前に使用可能なリソースを特定しておく必要があります。使用可能なリソースを確認することで、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サーバのインストール、ホストの追加、ストレージシステム接続の作成、クレデンシャルの追加、Plug-in for Exchangeのインストールなどのタスクを完了しておく必要があります。
- Single Mailbox Recoveryソフトウェアの機能を利用するには、Single Mailbox RecoveryソフトウェアがインストールされているExchange Server上にアクティブ・データベースを配置しておく必要があります。
- データベースがVMware RDM LUN上にある場合は、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、を ["SnapCenter Plug-in for VMware vSphereのドキュメント"](#) 参照してください。

## タスクの内容

- [詳細] ページの [全体のステータス \*] オプションが [バックアップに使用できない] に設定されている場合は、データベースをバックアップできません。次のいずれかに該当する場合、\* Overall Status \* オプションはバックアップに使用できない状態に設定されます。
  - データベースが NetApp LUN 上にない。
  - データベースが正常な状態でない。

データベースがmount、unmount、reseed、またはrecovery pending状態のときは正常な状態ではありません。
- Database Availability Group (DAG ; データベース可用性グループ) がある場合は、DAGからバックアップジョブを実行して、グループ内のすべてのデータベースをバックアップできます。

## 手順

1. 左側のナビゲーションペインで、[リソース] をクリックし、[リソース] ページの左上にあるプラグインのドロップダウンリストから [Microsoft Exchange Server\*] 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 \* データベース \*、\* データベース可用性グループ \*、または \* リソース・グループ \* を選択します。

すべてのデータベースとDAGは、それぞれのDAGまたはホスト名とともにFQDN形式で表示されるため、複数のデータベースを区別できます。

をクリック  し、ホスト名とExchangeサーバを選択してリソースをフィルタリングします。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. [リソースの更新] をクリックします。

新しく追加、名前変更、または削除されたリソースは、SnapCenterサーバインベントリに更新されます。



SnapCenter以外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。

リソースは、リソース名、データベース可用性グループ名、データベースが現在アクティブなサーバ、コピーがあるサーバ、前回のバックアップ時刻、全体的なステータスなどの情報とともに表示されます。

- データベースがネットアップ以外のストレージにある場合は、[Overall Status]列に「Not available for backup」と表示されます。

DAG では、アクティブなデータベースコピーがネットアップ以外のストレージにある場合に、少なくとも 1 つのパッシブデータベースコピーがネットアップストレージにあると、「全体のステータス」

列には保護されていないと表示されます。

ネットアップ以外のストレージタイプのデータベースでは、データ保護処理を実行できません。

- データベースがネットアップストレージ上にあり、保護されていない場合は、「\* Overall Status \*」列に保護されていないことが表示されます。
- データベースがネットアップストレージシステム上にあり、保護されている場合、ユーザインターフェイスの「バックアップ実行なし」というメッセージが「総合ステータス」列に表示されます。
- データベースがネットアップストレージシステム上にあり、保護されている場合に、データベースのバックアップがトリガされると、ユーザインターフェイスの「Backup succeeded」というメッセージが「\* Overall Status \*」列に表示されます。

## Exchange Serverデータベースのバックアップポリシーの作成

SnapCenterを使用してMicrosoft Exchange Serverリソースをバックアップする前に、Exchange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できます。また、リソースグループの作成時や単一のリソースのバックアップ時にバックアップポリシーを作成することもできます。

開始する前に

- データ保護戦略を定義しておく必要があります。

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

- SnapCenter のインストール、ホストの追加、リソースの特定、ストレージシステム接続の作成などのタスクを実行して、データ保護の準備をしておく必要があります。
- Exchange Serverリソースをリフレッシュ（検出）しておく必要があります。
- Snapshotをミラーまたはバックアップにレプリケートする場合は、SnapCenter管理者がソースボリュームとデスティネーションボリュームの両方のStorage Virtual Machine (SVM) をユーザに割り当てておく必要があります。
- 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、ファイルでパラメータの値をtrueに設定する必要があります `usePowershellProcessforScripts web.config`。

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、[を参照してください "SnapMirrorアクティブ同期のオブジェクト数の制限"](#)。

タスクの内容

- バックアップポリシーは、バックアップを管理および保持する方法、およびリソースまたはリソースグループをバックアップする頻度を規定する一連のルールです。また、スクリプト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することで、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できます。
- フルバックアップの保持は、特定のポリシーに固有です。フルバックアップの保持数が4のポリシーAを使用するデータベースまたはリソースでは、4つのフルバックアップが保持され、同じデータベースまたはリソースのポリシーBには影響しません。保持数を3に設定すると、3つのフルバックアップが保持される場合があります。

- ログバックアップの保持はポリシーに関係なく有効で、データベースまたはリソースのすべてのログバックアップに適用されます。したがって、ポリシーBを使用してフルバックアップを実行する場合、ログ保持設定は、ポリシーAで同じデータベースまたはリソース上に作成されたログバックアップに影響しません。同様に、ポリシーAのログ保持設定は、同じデータベース上にポリシーBで作成されたログバックアップに影響しません。
- 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/4.7/configsettingsを介してスワッガーから表示できます

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

\* ベストプラクティス： \* 維持するフルバックアップとログバックアップの総数に基づいて、セカンダリ保持ポリシーを設定することを推奨します。セカンダリの保持ポリシーを設定する場合は、異なるボリュームにあるデータベースとログの場合、各バックアップに3つのSnapshotを保持でき、データベースとログが同じボリュームにある場合は、各バックアップに2つのSnapshotを保持できることに注意してください。

- SnapLock

- [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。

Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、保持されるSnapshotの数がポリシーで指定されている数よりも多くなる可能性があります。

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



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

#### 手順

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

状況	操作
データベースファイルと必要なトランザクションログをバックアップする	<p>[フルバックアップおよびログバックアップ*]を選択します。</p> <p>データベースはログを切り捨ててバックアップされ、切り捨てられたログを含むすべてのログがバックアップされます。</p> <p> これは推奨されるバックアップタイプです。</p>
データベースファイルとコミットされていないトランザクションログをバックアップする	<p>[* Full backup*]を選択します。</p> <p>データベースはログを切り捨ててバックアップされ、切り捨てられたログはバックアップされません。</p>
すべてのトランザクションログをバックアップする	<p>「* Log backup *」を選択します。</p> <p>アクティブファイルシステム上のすべてのトランザクションログがバックアップされ、ログの切り捨ては行われません。</p> <p>ライブログと同じディスクに_scebackupinfo_directoryが作成されます。このディレクトリには、Exchangeデータベースの増分変更へのポインタが格納されており、完全なログ・ファイルとは異なります。</p>
トランザクションログファイルを切り捨てずに、すべてのデータベースファイルとトランザクションログをバックアップする	<p>Copy Backup (バックアップのコピー) *を選択します。</p> <p>すべてのデータベースとすべてのログがバックアップされ、ログの切り捨ては行われません。このバックアップタイプは、通常、レプリカの再シードや問題のテストや診断に使用します。</p>



ログバックアップに必要なスペースは、up-to-the-minute (UTM；最新の状態へのリストア)ではなく、フルバックアップの保持に基づいて定義する必要があります。



Exchangeボリューム (LUN) を扱う場合は、ログとデータベースに対して個別のバックアップポリシーを作成し、同じラベルを使用して、ログポリシーのkeep (retention)をデータベースポリシーの2倍の数に設定します。詳細については、[を参照してください](#)。"SnapCenter for Exchangeバックアップでは、バックアップデスティネーションログボリュームに保持されるSnapshotの半分だけが保持されます"

b. [Database Availability Group Settings]セクションで、処理を選択します。

フィールド	操作
アクティブなコピーをバックアップ	<p>選択したデータベースのアクティブコピーのみをバックアップする場合は、このオプションを選択します。</p> <p>Database Availability Group (DAG ; データベース可用性グループ) の場合は、DAG内のすべてのデータベースのアクティブコピーのみがバックアップされます。</p> <p>パッシブコピーはバックアップされません。</p>
バックアップジョブの作成時に選択するサーバ上のコピーをバックアップする	<p>選択したサーバ上のデータベースのコピー (アクティブとパッシブの両方) をバックアップする場合は、このオプションを選択します。</p> <p>DAGの場合は、選択したサーバ上のすべてのデータベースのアクティブコピーとパッシブコピーの両方がバックアップされます。</p>



クラスタ構成では、ポリシーで設定された保持設定に従って、バックアップがクラスタの各ノードで保持されます。クラスタの所有者ノードが変更された場合、以前の所有者ノードのバックアップが保持されます。保持期間はノードレベルでのみ適用されます。

- c. [スケジュール頻度]セクションで、1つ以上の頻度タイプを選択します。\* オンデマンド\*、\* 毎時\*、\* 毎日\*、\* 毎週\*、および\* 毎月\*。



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) を指定できます。これにより、ポリシーとバックアップ頻度が同じである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ができます。



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

## 6. [Retention]ページで、保持を設定します。

表示されるオプションは、以前に選択したバックアップタイプと頻度タイプによって異なります。



最大保持数は、ONTAP 9.4以降のリソースでは1018、ONTAP 9.3以前のリソースでは254です。保持数を使用しているONTAPバージョンでサポートされる値よりも大きい値に設定すると、バックアップは失敗します。



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可能性があります。

- a. [Log backups retention settings]セクションで、次のいずれかを選択します。

状況	操作
特定の数のログバックアップのみを保持	<p>ログを保持するフルバックアップの数を * 選択し、最新の状態へのリストアを実行するフルバックアップの数を指定します。</p> <p>up-to-the-minute (UTM；最新の状態へのリストア) の保持は、フルバックアップまたはログバックアップで作成されたログバックアップに適用されます。たとえば、過去5回のフルバックアップのログバックアップを保持するようにUTM保持設定が設定されている場合、過去5回のフルバックアップのログバックアップが保持されます。</p> <p>フルおよびログバックアップの一部として作成されたログフォルダは、UTMの一部として自動的に削除されます。ログフォルダを手動で削除することはできません。たとえば、フルバックアップまたはフルバックアップの保持設定が1か月に設定され、ログバックアップの保持期間が10日に設定されている場合、これらのバックアップの一部として作成されたログフォルダはUTMに従って削除されます。そのため、ログフォルダは10日間しか保持されず、その他のバックアップはすべてポイントインタイムリストアの対象としてマークされます。</p> <p>最新の状態へのリストアを実行しない場合は、UTM保持の値を0に設定できます。これにより、ポイントインタイムリストア処理が有効になります。</p> <p>ベストプラクティス：[Full backup retention settings]セクションの[Total Snapshots (フルバックアップ)]の設定と同じにすることを推奨します。これにより、フルバックアップごとにログファイルが保持されます。</p>
バックアップコピーを特定の日数だけ保持	<p>「* Keep log backups for last *」オプションを選択し、ログバックアップコピーを保持する日数を指定します。</p> <p>フルバックアップが保持される日数までのログバックアップが保持されます。</p>
Snapshotロック期間	<p>[Snapshotコピーロック期間]*を選択し、日、月、または年を選択します。</p> <p>SnapLock保持期間は100年未満にする必要があります。</p>

バックアップタイプとして \* Log backup \* を選択した場合は、フルバックアップの最新の状態へのリストア保持設定の一部としてログバックアップが保持されます。

- b. [Full backup retention settings]セクションで、オンデマンドバックアップの場合は次のいずれかを選択し、フルバックアップの場合は1つを選択します。

フィールド	操作
特定の数のSnapshotのみを保持	<p>保持するフルバックアップの数を指定する場合は、*保持するSnapshotコピーの総数*オプションを選択し、保持するSnapshot（フルバックアップ）の数を指定します。</p> <p>フルバックアップの数が指定した数を超えると、指定した数を超えるフルバックアップが削除され、最も古いコピーから順に削除されます。</p>
フルバックアップを特定の日数だけ保持	[Keep Snapshot copies for]*オプションを選択し、Snapshot（フルバックアップ）を保持する日数を指定します。
Snapshotロック期間	<p>[Snapshotコピーロック期間]*を選択し、日、月、または年を選択します。</p> <p>SnapLock保持期間は100年未満にする必要があります。</p>

DAG構成のホストにログバックアップのみのデータベースがあり、フルバックアップがない場合は、次の方法でログバックアップが保持されます。

- デフォルトでは、SnapCenter は DAG 内の他のすべてのホストでこのデータベースの最も古いフルバックアップを検出し、フルバックアップの前に作成されたこのホスト上のすべてのログバックアップを削除します。
- ログバックアップのみを使用する DAG 内のホストのデフォルトの保持設定を上書きするには、`_C : \Program Files\NetApp\SnapManager WebApp\web.config_file` にキー \* `MaxLogBackupOnlyCountWithoutFullBackup` \* を追加します。

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

この例の値が10の場合、ホストで保持できるログバックアップは最大10個です。

7. [Replication]ページで、次のセカンダリレプリケーションオプションのいずれかまたは両方を選択します。

フィールド	操作
ローカルSnapshot作成後にSnapMirrorを更新する	<p>バックアップセットのミラーコピーを別のボリューム（SnapMirror）に保持する場合は、このオプションを選択します。</p> <p>セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。</p> <p>このオプションは、SnapMirrorのアクティブな同期に対して有効にする必要があります。</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> プライマリのみのポリシーは、Exchange ONTAPボリュームに対してSnapMirrorのアクティブな同期が設定されている場合は使用できません。SnapCenterではこれが許可されていません。「ミラー」オプションを有効にする必要があります。</p> </div> <p>[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。</p> <p>を参照して "<a href="#">[Topology]ページでのExchangeバックアップの表示</a>"</p>
ローカルSnapshot作成後にSnapVaultを更新	<p>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。</p>
セカンダリポリシーラベル	<p>Snapshotラベルを選択します。</p> <p>選択したSnapshotラベルに応じて、ラベルに一致するセカンダリSnapshot保持ポリシーがONTAPによって適用されます。</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> ローカル Snapshot コピーの作成後に「* SnapMirror を更新」を選択した場合は、必要に応じて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 Snapshot コピーの作成後に「* Update SnapVault」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。</p> </div>
エラー時の再試行回数	<p>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。</p>



セカンダリストレージのSnapshotの最大数に達しないように、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. スクリプトページで、バックアップ処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

- プリスクリプトのバックアップ引数には、「\$Database」および「\$ServerInstance」が含まれます。
- PostScript バックアップ引数には、「\$Database」、「\$ServerInstance」、「\$BackupName」、「\$LogDirectory」、「\$LogSnapshot」が含まれます。

スクリプトを実行して、SNMPトラップの更新、アラートの自動化、ログの送信などを行うことができます。



プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts\_pathから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。

## Exchange Serverの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すべてのデータ保護ジョブに必要です。また、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と保護スケジュールを定義する必要があります。

### タスクの内容

- 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/4.7/configsettingsを介してスワッガーから表示できます

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

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期が設定されていない新しいデータベースを、SnapMirrorアクティブ同期が設定された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 Active Syncのフェイルオーバーモードでは、既存のリソースグループに新しいデータベースを追加することはできません。リソースグループに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 Microsoft Exchange Server 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 [\* データベース \*] を選択します。



最近 SnapCenter にリソースを追加した場合は、[\* リソースの更新 \*] をクリックして、新しく追加したリソースを表示します。

3. [New Resource Group] をクリックします。

4. [名前] ページで、次の操作を実行します。

フィールド	操作
名前	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文字以内にする必要があります。
タグ	リソースグループをあとで検索する際に役立つラベルを1つ以上入力します。  たとえば、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。
Snapshotコピーにカスタムの名前形式を使用する	オプション：Snapshotのカスタムの名前と形式を入力します。  たとえば、 _customtext_resourcegroup_policy_hostname_or_resourcegroup_hostname_hostname_or_resourcegroup_hostname_hostname_1 のようになります。デフォルトでは、Snapshot名にタイムスタンプが追加されます。

5. Resources ページで、次の手順を実行します。

- a. リソースタイプとデータベース可用性グループをドロップダウンリストから選択して、使用可能な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、リソースリストを更新するまで[Available Resources]のリストに表示されません。

[Available Resources]セクションと[Selected Resources]セクションに、データベース名とホストのFQDNが表示されます。このFQDNは、データベースが特定のホストでアクティブであり、このホストでバックアップを作成しない可能性があることを示します。バックアップ・ジョブ作成時に選択するサーバ上の \* バックアップ・コピーのバックアップ・オプションを選択した場合に、バックアップを作成するサーバ選択オプションから 1 つ以上のバックアップ・サーバを選択する必要があります。

- b. 検索テキストボックスにリソースの名前を入力するか、スクロールしてリソースを探します。
- c. [使用可能なリソース]セクションから [選択したリソース]セクションにリソースを移動するには、次のいずれかの手順を実行します。

- 同じボリューム上のすべてのリソースを [ 選択したリソース ] セクションに移動するには、 \* 同一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 \* を選択します。
- [ 使用可能なリソース ] セクションからリソースを選択し、右矢印をクリックして [ 選択したリソース ] セクションに移動します。

SnapCenter for Microsoft Exchange Serverのリソースグループに含めることができるデータベースは、Snapshotあたり30個までです。1つのリソースグループに30を超えるデータベースがある場合は、追加のデータベース用に2つ目のSnapshotが作成されます。そのため、メインバックアップジョブの下に2つのサブジョブが作成されます。セカンダリレプリケーションが設定されたバックアップで、SnapMirrorまたはSnapVaultの更新の実行中に、両方のサブジョブの更新が重複する場合があります。ログにジョブが完了したことが記録されている場合でも、メインのバックアップジョブは無期限に実行され続けます。

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 。



バックアップ・ジョブ作成時に選択するサーバ上の \* バックアップ・コピーがポリシーに含まれている場合は、サーバ選択オプションが表示され、1つ以上のサーバを選択できます。サーバ選択オプションでは、選択したデータベースがNetAppストレージ上にあるサーバのみが表示されます。

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

- b. [選択したポリシーのスケジュールを設定]セクションで、スケジュールを設定するポリシーの\*列にある\*をクリックし  ます。
- c. [Add schedules for policy\_name\_] 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設定し、 [\*OK] をクリックします。

この処理は、ポリシーに指定されている頻度ごとに実行する必要があります。設定されたスケジュールは、[ 選択したポリシーのスケジュールの設定 ] セクションの [ 適用されたスケジュール \* ] 列に一覧表示されます。

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

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

また、送信者と受信者のEメールアドレス、およびEメールの件名を指定する必要があります。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 ( Attach Job Report ) ] を選択します。

Eメール通知を使用する場合は、GUIまたはPowerShell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 Set-SmSmtperver。

コマンドレットで使用できるパラメータとその説明については、 RUN\_Get-Help コマンド NAME を実行して参照できます。または、『Software Cmdlet Reference Guide ^』も参照して

<https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html#snapcenter> ください。

8. 概要を確認し、[完了]をクリックします。

## Exchangeデータベースのバックアップ

いずれのリソースグループにも含まれていないデータベースは、[Resources]ページからバックアップできます。

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。
- バックアップ処理で使用されるアグリゲートを、データベースで使用されるSVMに割り当てておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられるロールには「'SnapMirro all」権限を含める必要があります。ただし、「vsadmin」ロールを使用している場合、「'SnapMirro all」権限は必要ありません。
- ネットアップストレージとネットアップ以外のストレージ上にアクティブ/パッシブデータベースコピーのあるデータベースまたはデータベース可用性グループのバックアップを実行する場合は、また、ポリシーのバックアップ・ジョブ作成時間 \* オプションで、サーバ上のバックアップ・アクティブ・コピー \* またはバックアップ・コピーを選択した場合、バックアップ・ジョブは警告状態になります。NetAppストレージ上のアクティブ/パッシブデータベースコピーのバックアップは成功し、ネットアップ以外のストレージ上のアクティブ/パッシブデータベースコピーのバックアップは失敗します。

\* ベストプラクティス： \* アクティブデータベースとパッシブデータベースのバックアップは同時に実行しないでください。競合状態が発生し、いずれかのバックアップが失敗する可能性があります。

## 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 [Microsoft Exchange Server 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 \* データベース \* または \* データベース可用性グループ \* のいずれかを選択します。

[Resources]ページの  アイコンは、データベースがネットアップ以外のストレージにあることを示します。



DAGで、アクティブなデータベースコピーがネットアップ以外のストレージにあり、少なくとも1つのパッシブデータベースコピーがNetAppストレージにある場合は、データベースを保護できます。

をクリックし 、ホスト名とデータベースタイプを選択してリソースをフィルタリングします。次に、\*をクリックしてフィルタペインを閉じることができます .

- データベースをバックアップする場合は、データベース名をクリックします。
    - i. Topology ビューが表示されたら、**Protect** をクリックします。
    - ii. [Database - Protect Resource]ウィザードが表示されたら、手順3に進みます。
  - データベース可用性グループをバックアップする場合は、データベース可用性グループの名前をクリックします。
3. カスタムのSnapshot名を指定する場合は、[リソース]ページで\*[Snapshotコピーにカスタムの名前形式を使用する]\*チェックボックスを選択し、Snapshot名に使用するカスタムの名前形式を入力します。

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

4. [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 。



バックアップ・ジョブ作成時に選択するサーバ上の \* バックアップ・コピーがポリシーに含まれている場合は、サーバ選択オプションが表示され、1つ以上のサーバを選択できます。サーバ選択オプションでは、選択したデータベースがNetAppストレージ上にあるサーバのみが表示されます。

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

- b. スケジュールを設定するポリシーの[スケジュールの設定]列で\*\*をクリックします .
- c. [Add schedules for policy\_name] ウィンドウで、スケジュールを設定し、[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。

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

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

また、送信者と受信者のEメールアドレス、およびEメールの件名を指定する必要があります。リソース上で実行されたバックアップ処理のレポートを添付する場合は、 [ ジョブレポートの添付 ( Attach Job Report ) ] を選択します。



Eメール通知を使用する場合は、GUIまたはPowerShellコマンド `Set-SmSmSmtServer` 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。

6. 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ページが表示されます。

7. [ 今すぐバックアップ ] をクリックします。

8. Backup (バックアップ) ページで、次の手順を実行します。

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

オンデマンドバックアップ用に選択したポリシーにバックアップスケジュールが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に指定した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。

9. ページ下部の[Activity]ペインでジョブをダブルクリックして[Job Details]ページを表示し、バックアップの進捗状況を監視します。

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

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

- 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ヒープサイズが十分でないと、バックアップが失敗することがあります。

Java の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。このスクリプトでは、 `DO_START_METHOD_Command` によって、 `SnapCenter VMware` プラグインサービスが開始されます。このコマンドを次のように更新します。 `_java -jar -Xmx8192M -Xms4096M`

## 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、指定したユーザのSnapCenterサーバとの接続セッションを開始します。

```
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、フルバックアップとログバックアップのExchangeバックアップタイプ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。

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy  
-PolicyType Backup -PluginPolicytype SCE -SceBackupType  
FullBackupAndLogBackup -BackupActiveCopies
```

この例では、1時間ごとのフルバックアップとログバックアップのExchangeバックアップタイプ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。

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy  
-PolicyType Backup -PluginPolicytype SCE -SceBackupType  
FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly  
-RetentionSettings  
{'BackupType'='DATA';'ScheduleType'='Hourly';'RetentionCount'='10'}
```

この例では、Exchangeログのみをバックアップする新しいバックアップポリシーを作成します。

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup  
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

## 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 Exchange Serverプラグインのリソースを検出しています。

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

## 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Exchange Server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。

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

この例では、ポリシーとリソースを指定して、新しいExchange Database Availability Group (DAG ; データベース可用性グループ) バックアップリソースグループを作成しています。

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode
SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database Availability Group";"Names"="DAGSCE0102"}
```

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。

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

この例では、セカンダリストレージに新しいバックアップを作成します。

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

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。

次に、指定した日付に実行されたすべてのジョブのジョブ概要レポートを表示する例を示します。

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

次に、特定のジョブIDのジョブサマリレポートを表示する例を示します。

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

コマンドレットで使用できるパラメータとその説明については、RUN\_Get-Help コマンド *NAME* を実行して参照できます。または、『Software Cmdlet Reference Guide ^』を参照してください

## Exchange リソースグループをバックアップする

リソースグループはホストまたはExchange DAG上のリソースの集まりであり、リソースグループにはDAG全体または個々のデータベースを含めることができます。リソースグループは[リソース]ページでバックアップできます。

開始する前に

- ポリシーを適用してリソースグループを作成しておく必要があります。
- バックアップ処理で使用されるアグリゲートを、データベースで使用されるStorage Virtual Machine (SVM) に割り当てておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられるロールには「'SnapMirror all」権限を含める必要があります。ただし、「vsadmin」ロールを使用している場合、「'SnapMirror all」権限は必要ありません。
- リソースグループに異なるホストの複数のデータベースが含まれている場合、ネットワークの問題が原因で、一部のホストでのバックアップ処理の開始に時間がかかることがあります。PowerShellコマンドレットを使用して、の値を設定します `MaxRetryForUninitializedHosts web.config Set-SmConfigSettings`。
- リソースグループに、ネットアップストレージとネットアップ以外のストレージ上にアクティブ/パッシブデータベースコピーのあるデータベースまたはデータベース可用性グループが含まれていて、ポリシーでバックアップジョブの作成時に選択するサーバでアクティブ/パッシブデータベースコピーのバックアップ\* または \* バックアップコピーの選択が完了している場合：その後、バックアップジョブが警告状態になります。

NetAppストレージ上のアクティブ/パッシブデータベースコピーのバックアップは成功し、ネットアップ以外のストレージ上のアクティブ/パッシブデータベースコピーのバックアップは失敗します。

タスクの内容

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、スケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが実行されます。

手順

1. 左側のナビゲーションペインで、[\* リソース]をクリックし、リストから [Microsoft Exchange Server プラグイン\*] を選択します。
2. [リソース]ページで、[\* 表示]リストから [\* リソースグループ\*] を選択します。

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

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

オンデマンドバックアップ用に選択したポリシーにバックアップスケジュールが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に指定した保持設定に基づいて保持されません。

- b. [バックアップ] をクリックします。
5. ページ下部の[Activity]ペインでジョブをダブルクリックして[Job Details]ページを表示し、バックアップの進捗状況を監視します。

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

PowerShellコマンドレットを使用してバックアップとリストアを実行する前に、Storage Virtual Machine (SVM) 接続とクレデンシアルを作成する必要があります。

開始する前に

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

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

- ストレージシステム名は一意である必要があります。

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

手順

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

この例では、PowerShellセッションを開きます。

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

2. 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 `Add-SmStorageConnection` 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 -SVM test_vs1 -Protocol Https  
-Timeout 60
```

3. コマンドレットを使用して、新しいRun Asアカウントを作成し `Add-Credential` ます。

この例では、Windowsクレデンシャルを使用してExchangeAdminという名前の新しいRun Asアカウントを作成します。

```
PS C:> Add-SmCredential -Name ExchangeAdmin -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ついては、RUN\_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "[SnapCenter ソフトウェアコマンドレットリファレンスガイド](#)"。

## バックアップ処理の監視

[SnapCenterJobs]ページを使用して、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

### タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

-  実行中
-  完了済み
-  失敗
-  完了（警告あり）または警告のため開始できませんでした
-  キューに登録済み
-  キャンセル済み

### 手順

1. 左側のナビゲーションペインで、**Monitor** をクリックします。
2. [モニター] ページで、[\* ジョブ \*] をクリックします。
3. Jobs (ジョブ) ページで、次の手順を実行します。
  - a. をクリックして、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、[\*Backup] を選択します。
  - d. [Status](ステータス\*) ドロップダウンから、バックアップステータスを選択します。
  - e. [適用 (Apply)] をクリックして、正常に完了した操作を表示する。
4. バックアップジョブを選択し、[\* 詳細 \*] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスは表示されますが 、ジョブの詳細をクリックすると、バックアップ処理の子タスクの一部が進行中であるか、警告サインが表示されていることがあります。

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

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

### [Activity]ペインでの処理の監視

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

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

#### 手順

1. 左側のナビゲーションペインで、 \* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [Activity]ペインでをクリックすると、  最新の5つの処理が表示されます。

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

## Exchangeデータベースのバックアップ処理をキャンセルします

キューに登録されているバックアップ処理をキャンセルできます。

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

アクセス元	アクション
監視ページ	<ol style="list-style-type: none"><li>a. 左側のナビゲーションペインで、 * Monitor * &gt; * Jobs * をクリックします。</li><li>b. 操作を選択し、 * ジョブのキャンセル * をクリックします。</li></ol>

アクセス元	アクション
[Activity]ペイン	<ul style="list-style-type: none"> <li>a. バックアップ処理を開始したら、[Activity]ペインの**をクリックし<sup>▲</sup>て、最新の5つの処理を表示します。</li> <li>b. 処理を選択します。</li> <li>c. [ジョブの詳細] ページで、[* ジョブのキャンセル*] をクリックします。</li> </ul>

処理がキャンセルされ、リソースが以前の状態に戻ります。

## PowerShellコマンドレットを使用したExchangeバックアップの削除

Remove-SmBackupコマンドレットを使用すると、他のデータ保護処理にExchangeバックアップが不要になった場合にExchangeバックアップを削除できます。

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

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

### 手順

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

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

2. コマンドレットを使用して、1つ以上のバックアップを削除します Remove-SmBackup。

この例では、バックアップIDを使用してバックアップを2つ削除しています。

```
Remove-SmBackup -BackupIds 3,4
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"):
```

## [Topology]ページでのExchangeバックアップの表示

リソースのバックアップを準備する際には、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の図を表示すると役立つことがあります。

### タスクの内容

[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可能なすべてのバックアップを確認できます。これらのバックアップの詳細を表示し、選択してデータ保護処理を実行できます。

プライマリストレージと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）のどちらにバックアップがあるかを確認するには、[コピーの管理]ビューの次のアイコンを確認します。

-  プライマリストレージで使用可能なバックアップの数が表示されます。
-  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の数が表示されます。
-  SnapVaultテクノロジーを使用してセカンダリストレージにレプリケートされたバックアップの数が表示されます。
  - 表示されるバックアップの数には、セカンダリストレージから削除されたバックアップも含まれません。

たとえば、バックアップを4つだけ保持するポリシーを使用して6つのバックアップを作成した場合、バックアップの数は6と表示されます。

\* ベストプラクティス： \* 正しい数のレプリケートされたバックアップが表示されるように、トポロジを更新することを推奨します。

セカンダリ関係がSnapMirrorのアクティブな同期（当初はSnapMirrorビジネス継続性[SM-BC]としてリリース）である場合は、次のアイコンも表示されます。

-  レプリカサイトが稼働していることを示します。
-  レプリカサイトがダウンしていることを示します。
-  セカンダリのミラー関係やバックアップ関係が再確立されていないことを示します。

#### 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、データベース、リソース、またはリソースグループを \*View\* ドロップダウン・リストから選択します。
3. データベ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]セクションで、プライマリストレージとセカンダリストレージにあるバックアップ数の概要を確認します。

[Summary Card]セクションには、バックアップの総数とログバックアップの総数が表示されます。

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

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

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

SnapMirrorのアクティブな同期の場合、\*[リフレッシュ]\*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をONTAPに照会して、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は、SnapMirrorのアクティブな同期関係を含むすべてのデータベースに対してもこの処理が実行されます。

- SnapMirrorのアクティブな同期（ONTAP 9.14.1のみ）では、フェイルオーバー後に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関係または非同期ミラーバックアップ関係を手動で設定する必要があります。ONTAP 9.15.1以降では、新しいプライマリデスティネーションに対して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。フェイルオーバー後。
- 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。[リフレッシュ]\*をクリックできるのは、バックアップが作成されてからです。

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の \* バックアップ \* ] をクリックして、バックアップの詳細を表示します。

バックアップ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、名前変更、削除の各処理を実行します。



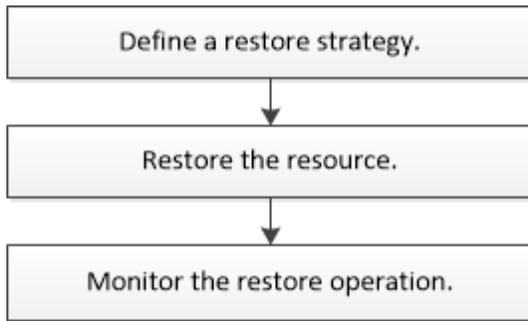
セカンダリストレージにあるバックアップは、名前の変更や削除はできません。Snapshotの削除は、ONTAPの保持設定で処理されます。

## Exchangeリソースのリストア

### リストアのワークフロー

SnapCenterを使用すると、1つ以上のバックアップをアクティブファイルシステムにリストアして、Exchangeデータベースをリストアできます。

次のワークフローは、Exchangeデータベース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、バックアップとリストア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、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](#)"。

## Exchangeデータベースをリストアするための要件

SnapCenter Plug-in for Microsoft Exchange ServerのバックアップからExchange Serverデータベースをリストアする前に、いくつかの要件を満たしていることを確認する必要があります。



リストア機能を完全に使用するには、SnapCenter ServerとSnapCenter Plug-in for Exchange Serverの両方を4.6にアップグレードする必要があります。

- データベースをリストアするには、Exchange Serverがオンラインで実行されている必要があります。
- データベースがExchange Server上に存在している必要があります。



削除したデータベースのリストアはサポートされていません。

- データベースのSnapCenterスケジュールを一時停止する必要があります。
- SnapCenter ServerおよびSnapCenter Plug-in for Microsoft Exchange Serverホストが、リストアするバックアップを含むプライマリストレージとセカンダリストレージに接続されている必要があります。

## Exchangeデータベースのリストア

SnapCenterを使用して、バックアップされたExchangeデータベースをリストアできます。

開始する前に

- リソースグループ、データベース、またはDatabase Availability Group (DAG ; データベース可用性グループ) をバックアップしておく必要があります。
- Exchangeデータベースを別の場所に移行した場合、古いバックアップに対してリストア処理を実行できません。
- 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、SnapCenter管理者がユーザ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両方にSVMを割り当てておく必要があります。
- DAGで、アクティブなデータベースコピーがネットアップ以外のストレージにある場合に、NetAppストレージにあるデータベースのパッシブコピーバックアップからリストアするには、そのパッシブコピー (NetAppストレージ) をアクティブコピーとして作成し、リソースを更新してリストア処理を実行しま

す。

コマンドを実行して Move-ActiveMailboxDatabase、データベースのパッシブコピーをアクティブデータベースコピーとして設定します。

このコマンドについては、を参照して "[Microsoftのドキュメント](#)" ください。

#### タスクの内容

- データベースに対してリストア処理を実行すると、データベースは同じホストに再度マウントされ、新しいボリュームは作成されません。
- DAGレベルのバックアップは、個々のデータベースからリストアする必要があります。
- Exchangeデータベース (.edb) ファイル以外のファイルが存在する場合、フルディスクリストアはサポートされません。

Plug-in for Exchangeでは、ディスクにレプリケーションに使用するExchangeファイルなどのExchangeファイルが含まれている場合、ディスク上でフルリストアは実行されません。フルリストアがExchangeの機能に影響を及ぼす可能性がある場合、Plug-in for Exchangeは単一ファイルのリストア処理を実行しません。

- Plug-in for Exchangeでは、BitLockerで暗号化されたドライブをリストアできません。
- 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/4.7/configsettingsを介してスワッガーから表示できます

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

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

## SnapCenter UI

### 手順

1. 左側のナビゲーションペインで、リソースページの左上にある \* リソース \* をクリックします。
2. ドロップダウンリストからExchange Serverプラグインを選択します。
3. [リソース] ページで、[表示] リストから [\* データベース \*] を選択します。
4. リストからデータベースを選択します。
5. [Manage Copies]ビューで、[Primary Backups]テーブルから\*を選択し、\*\*をクリックします 。
6. [Options] ページで、次のいずれかのログバックアップオプションを選択します。

オプション	説明
すべてのログバックアップ	フルバックアップ後に使用可能なすべてのログバックアップをリストアするには、「* All log backups *」を選択して最新の状態へのバックアップリストア処理を実行します。
次のログバックアップまで：	「* までログバックアップ」を選択してポイントインタイムリストア処理を実行します。このリストア処理では、選択したログまでのログバックアップに基づいてデータベースがリストアされます。   ドロップダウンリストに表示されるログの数は、UTMに基づいています。たとえば、フルバックアップの保持が5でUTM保持が3の場合、使用可能なログバックアップの数は5ですが、ドロップダウンにはリストア処理を実行するためのログが3つだけ表示されます。
次の日付まで	リストアしたデータベースにトランザクション・ログを適用する日時を指定するには、[指定の期限まで *] を選択します。このポイントインタイムリストア処理では、指定した日時の最後のバックアップまで記録されたトランザクションログエントリがリストアされます。
なし	ログ・バックアップを行わずにフル・バックアップのみをリストアする必要がある場合は、「* なし」を選択します。

次のいずれかの操作を実行できます。

- \* リストア後にデータベースをリカバリしてマウント \* - このオプションはデフォルトで選択されています。

- \* リストア前にバックアップ内のトランザクション・ログの整合性を検証しない \* - デフォルトでは、SnapCenter はリストア処理を実行する前にバックアップ内のトランザクション・ログの整合性を検証します。

\* ベストプラクティス： \* このオプションは選択しないでください。

7. スクリプトページで、リストア処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

リストアプレスクリプトの引数には、\$Databaseと\$ServerInstanceがあります。

リストアポストスクリプトの引数には、\$Database、\$ServerInstance、\$BackupName、\$LogDirectory、および\$TargetServerInstanceがあります。

スクリプトを実行して、SNMPトラップの更新、アラートの自動化、ログの送信などを行うことができます。



プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts\_pathからの相対パスである必要があります。

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

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

9. 概要を確認し、[完了] をクリックします。

10. ページ下部の[Activity]パネルを展開すると、リストアジョブのステータスを確認できます。

リストア・プロセスを監視するには、\* Monitor \* > \* Jobs \* ページを使用します。

バックアップからアクティブデータベースをリストアするときに、レプリカとアクティブデータベースの間に遅延があると、パッシブデータベースが一時停止状態または障害状態になることがあります。

状態の変化は、アクティブデータベースのログチェーンがフォークし、レプリケーションを中断する新しいブランチを開始したときに発生します。Exchange Serverはレプリカの修正を試みますが、修正できない場合は、リストア後に新しいバックアップを作成し、レプリカを再シードする必要があります。

## PowerShellコマンドレット

### 手順

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

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

2. コマンドレットを使用して、リストアする1つ以上のバックアップに関する情報を取得します `Get-SmBackup`。

次に、使用可能なすべてのバックアップに関する情報を表示する例を示します。

```
PS C:\> Get-SmBackup

BackupId      BackupName
BackupTime    BackupType
-----
-----
341           ResourceGroup_36304978_UTM...
12/8/2017 4:13:24 PM Full Backup
342           ResourceGroup_36304978_UTM...
12/8/2017 4:16:23 PM Full Backup
355           ResourceGroup_06140588_UTM...
12/8/2017 6:32:36 PM Log Backup
356           ResourceGroup_06140588_UTM...
12/8/2017 6:36:20 PM Full Backup
```

### 3. 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。

この例では、最新の状態へのバックアップをリストアしています。

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
-IsRecoverMount:$true
```

この例では、ポイントインタイムバックアップをリストアしています。

```
C:\ PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
-IsRecoverMount:$true -LogRestoreType ByTransactionLogs -LogCount 2
```

この例では、セカンダリストレージのバックアップをプライマリストーリーにリストアします。

```
C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2'
-BackupId 81 -IsRecoverMount:$true -Confirm:$false
-archive @{Primary="paw_vs:vol1";Secondary="paw_vs:vol1_mirror"}
-logrestoretype All
```

パラメータを使用 `-archive` すると、リストアに使用するプライマリボリュームとセカンダリボリュームを指定できます。

パラメータを指定する `-IsRecoverMount:$true` と、リストア後にデータベースをマウントできます。

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

## メールとメールボックスのきめ細かなリカバリ

Single Mailbox Recovery (SMBR) ソフトウェアを使用すると、Exchangeデータベース全体の代わりに、メールまたはメールボックスをリストアおよびリカバリできます。

1つのメールをリカバリするためだけにデータベース全体をリストアすると、多くの時間とリソースが消費されます。SMBRを使用すると、Snapshotのクローンコピーを作成し、Microsoft APIを使用してSMBRにメールボックスをマウントすることで、メールを迅速にリカバリできます。SMBRの使用方法については、を参照してください "[SMBRアドミニストレーションガイド](#)"。

SMBRの追加情報については、次の資料を参照してください。

- "[SMBRを使用して単一アイテムを手動でリストアする方法 \(Ontrack電源制御リストアにも適用可能\)](#)"
- "[SnapCenter を使用して SMBR のセカンダリストレージからリストアする方法](#)"
- "[SMBR を使用した SnapVault からの Microsoft Exchange メールのリカバリ](#)"

## セカンダリストレージからExchange Serverデータベースをリストアする

バックアップしたExchange Serverデータベースは、セカンダリストレージ (ミラーまたはバックアップ) からリストアできます。

プライマリストレージからセカンダリストレージにSnapshotをレプリケートしておく必要があります。

### タスクの内容

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

### 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 [Microsoft Exchange Server プラグイン \*] を選択します。
2. [リソース] ページで、[\*View] ドロップダウン・リストから [\*Database] または [\*Resource Group] を選択します。
3. データベースまたはリソースグループを選択します。

データベ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] セクションで、セカンダリ・ストレージ・システム (ミラーまたはバックアップ) から \*バックアップ\* を選択します。
5. リストからバックアップを選択し、をクリックします 。

6. [Location]ページで、選択したリソースをリストアするデスティネーションボリュームを選択します。
7. リストア・ウィザードを完了し、概要を確認してから「[\* 終了 \*]」をクリックします

## Exchangeのパッシブノードレプリカの再シード

コピーが破損している場合などにレプリカコピーを再シードする必要がある場合は、SnapCenterの再シード機能を使用して最新のバックアップに再シードできます。

開始する前に

- SnapCenterサーバ4.1以降およびPlug-in for Exchange 4.1以降を使用している必要があります。
- レプリカの再シードは、バージョン4.1より前のSnapCenterではサポートされていません。
- 再シードするデータベースのバックアップを作成しておく必要があります。

\* ベストプラクティス：ノード間の遅延を回避するために、再シード処理を実行する前に新しいバックアップを作成するか、最新のバックアップを実行しているホストを選択することを推奨します。

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[Microsoft Exchange Server プラグイン \*]を選択します。
2. [Resources]ページで、[View]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
単一のデータベースを再シードするには	[表示]リストから[*Database]を選択します。
DAG内のデータベースを再シードするには	ビューリストから * データベース可用性グループ * を選択します。

3. 再シードするリソースを選択します。
4. Manage Copies（コピーの管理）ページで、\* Reseed-\* をクリックします。
5. 再シードウィザードで問題のあるデータベースコピーのリストから、再シードするデータベースコピーを選択し、\* Next \* をクリックします。
6. Host ウィンドウで、再シードするバックアップを含むホストを選択し、\* Next \* をクリックします。
7. [通知]ページの[電子メールの設定 \*]ドロップダウンリストから、電子メールを送信するシナリオを選択します。

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

8. 概要を確認し、[完了]をクリックします。
9. ページ下部の[Activity]パネルを展開すると、ジョブのステータスを表示できます。



データベースのパッシブコピーがネットアップ以外のストレージにある場合、再シード処理はサポートされません。

## ExchangeデータベースヨウノPowerShellコマンドレットヲシヨウシタレプリカノサイ シード

PowerShellコマンドレットを使用すると、同じホスト上の最新のコピーまたは代替ホストからの最新のコピーを使用して、正常でないレプリカをリストアできます。

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

### 手順

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

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

2. コマンドレットを使用して、データベースを再シードし reseed-SmDagReplicaCopy ます。

この例では、ホスト「mva-rx200.netapp.com」上のexecdbというデータベースの失敗したコピーを、そのホスト上の最新のバックアップを使用して再シードします。

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database  
execdb
```

この例では、代替ホスト「mva-rx201.netapp.com."」上のデータベース (production/copy) の最新のバックアップを使用して、execdbという名前のデータベースの失敗したコピーを再シードします。

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database  
execdb -BackupHost "mva-rx201.netapp.com"
```

## リストア処理の監視

[Jobs]ページを使用して、さまざまなSnapCenterリストア処理の進捗状況を監視できます。処理の進捗状況を確認して、処理が完了するタイミングや問題が発生していないかを確認できます。

### タスクの内容

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]ページには、処理の状態を示す次のアイコンが表示されます。

-  実行中

-  完了しました
-  失敗
-  完了（警告あり）または警告のため開始できませんでした
-  キューに登録済み
-  キャンセル済み

#### 手順

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [\* Monitor\*] ページで、 [\* Jobs] をクリックします。
3. [\* ジョブ \*] ページで、次の手順を実行します。
  - a. をクリックし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、 [ リストア \*] を選択します。
  - d. [\* Status \*] ドロップダウン・リストから、 リストア・ステータスを選択します。
  - e. [ 適用 (Apply) ] をクリックして、正常に完了した操作を表示する。
4. リストアジョブを選択し、 \* Details \* をクリックして、ジョブの詳細を表示します。
5. [\* ジョブの詳細 \*] ページで、 [ \* ログの表示 \* ] をクリックします。

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

## Exchangeデータベースのリストア処理をキャンセルします

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管理者またはジョブ所有者としてログインする必要があります。

#### タスクの内容

- キューに登録されたリストア処理は、 **Monitor** ページまたは **Activity** ペインからキャンセルできます。
- 実行中のリストア処理はキャンセルできません。
- キューに格納されているリストア処理は、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用してキャンセルできます。
- キャンセルできないリストア処理の場合、 [ ジョブのキャンセル ] ボタンは使用できません。
- ロールの作成中に [ 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オブジェクトを表示して操作できる ] を選択した場合は、そのロールを使用している間に、他のメンバーのキューに登録されているリストア操作をキャンセルできます。

#### ステップ

次のいずれかを実行します。

アクセス元	アクション
監視ページ	<ol style="list-style-type: none"> <li>1. 左側のナビゲーションペインで、 * Monitor * &gt; * Jobs * をクリックします。</li> <li>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。</li> </ol>
[Activity]ペイン	<ol style="list-style-type: none"> <li>1. リストア処理を開始したら、[Activity]ペインをクリックして、  最新の5つの処理を表示します。</li> <li>2. 処理を選択します。</li> <li>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。</li> </ol>

## 著作権に関する情報

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

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

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

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

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

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

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

## 商標に関する情報

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