Microsoft Exchange Serverデータベースの保護

SnapCenter software

NetApp
November 06, 2025

目次

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データベースに対するアプリケーション対応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をインストールすると、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 バックアップ レプリケーションを実行できます。

Exchangeデータベース全体ではなく、メールやメールボックスの単位でリストアとリカバリを実行する場合は、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。2020年6月24日に導入された販売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、サポートを購入されたお客様には、サポート対象の期間中は引き続きサポートを提供いたします。

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の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。

Exchange 用プラグインは、サイト全体に障害が発生した場合でもビジネス 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。

SnapMirrorアクティブ同期の非対称モード、フェイルオーバー モード、または非二重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であ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、プロキシ経由でプライマリ クラスタに提供されます。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一方向です。

- SnapCenter環境のMicrosoft Exchange Serverデータベースとデータベース可用性グループ（DAG）に対するアプリケーション対応のバックアップとリストアの各処理が自動化されます。
- SnapCenter Plug-in for VMware vSphereを展開し、そのプラグインをSnapCenterに登録すると、RDM LUN 上の仮想化された Exchange Server がサポートされます。

SnapCenter Plug-in for Microsoft Exchange Serverの機能

Plug-in for Exchangeを使用すれば、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データベース可用性グループ（DAG）、データベース、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
- バックアップを自動化するための保護設定を可能にするポリシーの定義
- リソース グループへのポリシーの割り当て
- 個々のDAGとデータベースの保護
- プライマリおよびセカンダリExchangeメールボックス データベースのバックアップ
- プライマリおよびセカンダリ 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**SnapCenter Plug-in 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、 https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT [NetApp相互運用性マトリックス ツール^]。

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	
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	VMDK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	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。

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。

- 全アクセス コマンド: ONTAP 9.12.1 以降に必要な最小限の権限

- event generate-autosupport-log
- job history show
- job stop
- lun
- lun create
- lun create
- lun create
- lun delete
- lun igroup add
- lun igroup create
- lun igroup delete
- lun igroup rename
- lun igroup rename
- lun igroup show
- lun mapping add-reporting-nodes
- lun mapping create
- lun mapping delete
- lun mapping remove-reporting-nodes
- lun mapping show
- lun modify
- lun move-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- lun resize
- lun serial
- lun show
- snapmirror policy add-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- snapmirror restore
- snapmirror show
- snapmirror show-history
- snapmirror update
- snapmirror update-ls-set
- snapmirror list-destinations

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

- vserver export-policy rule show
- vserver export-policy show
- vserver iscsi
- vserver iscsi connection show
- vserver show

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

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" 。

Exchange Serverリソースのバックアップ戦略の定義

バックアップ ジョブを作成する前にバックアップ戦略を定義しておくと、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、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、バックアップ戦略に関与します。

Exchangeデータベースでサポートされるバックアップ 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、データベースやデータベース可用性グループ（DAG）などのリソース タイプを選択する必要があります。Snapshotテクノロジを通じて、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 / ログ バックアップ	データベースと、切り捨てられた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。 フル バックアップが完了すると、Exchange Serverにより、データベースにコミット済みのトランザクション ログが切り捨てられます。 通常はこのオプションを選択します。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することもできます。
フル バックアップ	データベースとトランザクション ログがバックアップされます。 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。
ログ バックアップ	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。 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 バックアップの合間にトランザクション ログを頻繁にバックアップするスケジュールを設定すると、リカバリ ポイントをより細かく選択できます。

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。たとえば、定期的なトランザクション ログ バックアップを実行すれば、必要なバックアップが作成されます。データベースを頻繁にバックアップするほど、 SnapCenterが復元時に使用するトランザクション ログが少なくなり、復元操作が高速化されます。

バックアップ スケジュールには、次の2つの要素があります。

- バックアップ頻度

  バックアップ頻度 (バックアップを実行する頻度) 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。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。頻度を選択しなかった場合は、オンデマンドのみのポリシーが作成されます。 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。

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としては、リソースのサイズ、使用中のボリュームの数、リソースの変更率、サービス レベル アグリーメント（SLA）などがあります。

バックアップの命名規則

Snapshotのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則ではSnapshot名にタイムスタンプが追加されるので、コピーが作成されたタイミングを特定できます。

Snapshotでは、次のデフォルトの命名規則が使用されます。

```
resourcegroupname_hostname_timestamp
```

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

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

この例では、各構文要素に次の意味があります。

- *dts1* はリソース グループ名です。
- *mach1x88* はホスト名です。
- *03-12-2015_23.17.26* は日付とタイムスタンプです。

または、[スナップショット コピーにカスタム名形式を使用する] を選択して、リソースまたはリソース グル

ープを保護しながらスナップショット名の形式を指定することもできます。たとえば、customtext_resourcegroup_policy_hostnameやresourcegroup_hostnameなどの形式です。デフォルトでは、Snapshot名にタイムスタンプのサフィックスが追加されます。

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。

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 が午前 8 時に完全バックアップとトランザクション ログ バックアップを実行し、午後 5 時にもう一度完全バックアップとトランザクション ログ バックアップを実行した場合、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 時までの任意の時点にデータベースを復元できます。トランザクション ログが使用できない場合、Plug-in for Exchange は、Plug-in for Exchange が完全バックアップを完了した時点にデータベースを復元するポイントインタイム リストア操作のみを実行できます。

通常、最新の状態へのリストア処理に必要なのは1～2日分のみです。デフォルトでは、SnapCenterの保持期間は最短の2日間です。

Exchangeデータベースのリストア戦略の定義

Exchange Serverのリストア戦略を定義しておくと、その定義に従ってデータベースを実行することができます。

Exchange Serverでのリストア処理のソース

プライマリ ストレージにあるバックアップ コピーからExchange Serverデータベースをリストアすることができます。

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を使用して、Exchangeの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
- 過去のある時点（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がリストアされます。
2. バックアップされたすべてのトランザクション ログと、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 ログは再生されて選択したすべてのデータベースに適用されます。

   リストアの完了後、Exchangeにより新しいログ チェーンが作成されます。

   > ベスト プラクティス: 復元が完了したら、新しい完全バックアップとログ バックアップを実行することをお勧めします。

   最新の状態へのリストア処理を実行するには、連続したトランザクション ログ セットが必要です。

   最新の状態へのリストアを実行すると、リストアに使用したバックアップは、ポイントインタイム リストア処理にしか使用できなくなります。

   すべてのバックアップに最新の状態へのリストア機能を使用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 バックアップ保持を設定できます。

過去のある時点（ポイントインタイム）へのリストア

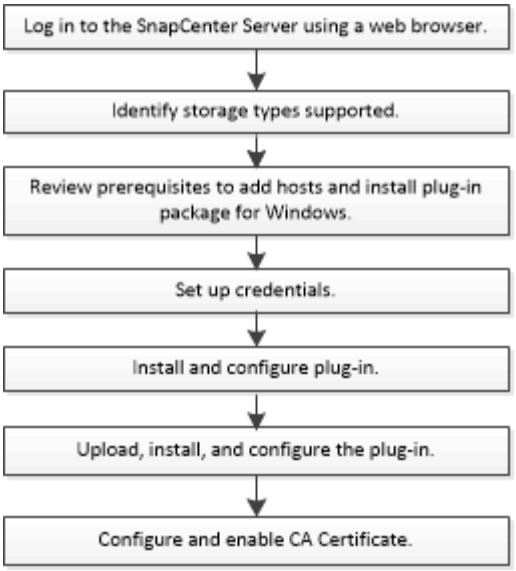
ポイントインタイム リストア処理では、データベースが過去の特定の時点にリストアされます。ポイントインタイム リストア処理は次の状況で発生します。

- バックアップ トランザクション ログの所定の時点までデータベースがリストアされた。
- 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 ログだけが適用された。

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。
- ローカル管理者権限があり、リモート ホストに対してローカル ログインのアクセス許可があるドメイン ユーザが必要です。
- 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でクラスタ ノードを管理する場合は、クラスタ内のすべてのノードに対する管理者権限があるユーザが必要です。
- Exchange Serverの管理権限があるユーザが必要です。
- SnapManager for Microsoft Exchange ServerとSnapDrive for Windowsがすでにインストールされている場合は、SnapCenterを使用してデータを確実に保護するために、同じExchange ServerにPlug-in for Exchangeをインストールする前にSnapDrive for Windowsが使用するVSSハードウェア プロバイダの登録を解除しておく必要があります。
- 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で作成したすべてのスケジュールをWindowsスケジューラで中断または削除する必要があります。
- サーバからホストを完全修飾ドメイン名（FQDN）に解決できる必要があります。ホスト ファイルが解決可能になるように変更され、ホスト ファイルで短縮名と FQDN の両方が指定されている場合は、SnapCenterホスト 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ます。ブロックされていると、ホストの追加処理に失敗します。この問題を解決するには、動的ポート範囲を設定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。 "Microsoftのドキュメント" 。

- Windows 2016とExchange 2016のポート範囲は50,000～51,000です。
- Windows Server 2012 R2とExchange 2013のポート範囲は6,000～6,500です。
- Windows 2019のポート範囲は49,152～65,536です。

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
- 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、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	Microsoft Windows サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	5 GB 十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。

項目	要件
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK Java 11 Oracle Java および OpenJDK は、SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp対応プラグイン、および Windows ホストにインストールできるその他のカスタム アプリケーションにのみ必要です。 サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。

必要とされる**Exchange Server**の権限

SnapCenterでExchange ServerまたはDAGを追加し、SnapCenter Plug-in for Microsoft Exchange Serverをホストまたは DAGにインストールできるようにするには、最小限の権限とアクセス許可を持つユーザのクレデンシャルを使用してSnapCenterを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、および 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-Database
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:$true
- Mount-Database
- New-MailboxDatabase
- New-PublicFolderDatabase
- Remove-MailboxDatabase
- Remove-MailboxDatabaseCopy

- Remove-PublicFolderDatabase
- Resume-MailboxDatabaseCopy
- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore:$true
- Set-MailboxDatabaseCopy
- 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、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	Microsoft Windows サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	5 GB 十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。

項目	要件
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK Java 11 Oracle Java および OpenJDK は、SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp対応プラグイン、および Windows ホストにインストールできるその他のカスタム アプリケーションにのみ必要です。 サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。

SnapCenter 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。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、データベースでのデータ保護処理に使用するクレデンシャルをそれぞれ作成する必要があります。

タスク概要

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可能ですが、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する場合で、ユーザ名に完全なadmin権限が割り当てられていない場合は、少なくともリソース グループとバックアップの権限を割り当てる必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[資格情報]をクリックします。
3. *新規*をクリックします。

   [Credential]ウィンドウが表示されます。

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	認証に使用するユーザ名を入力します。 • 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` • ローカル管理者（ワークグループの場合のみ） ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。ユーザー名フィールドの有効な形式は次のとおりです。 `UserName`
パスワード	認証に使用するパスワードを入力します。
認証	認証モードとして[Windows]を選択します。

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、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**Plug-in for Exchange**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。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。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など、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。
- メッセージ キュー サービスが実行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、"Windows Server 2016 以降で Microsoft Exchange Server のグループ管理サービス アカウントを構成する" 。

タスク概要

- SnapCenter Serverをプラグイン ホストとして別のSnapCenter Serverに追加することはできません。
- ホストの追加とプラグイン パッケージのインストールは、ホストごとまたはクラスタごとに実行できます。
- ExchangeノードがDAGの一部である場合、SnapCenter Server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、NetApp LUN上にデータベースのないノードがあったとしても、クラスタのすべてのノードにプラグインがインストールされます。

SnapCenter 4.6以降では、SCEがマルチテナンシー対応になったので、次の方法でホストを追加できます。

ホストの追加処理	**4.5**以前	**4.6**以降
クロス ドメインまたは別のドメインのIPレスDAGを追加	サポート対象外	サポート
同一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	サポート	サポート

ホストの追加処理	**4.5**以前	**4.6**以降
クロス ドメインで同一のホスト名やDB名を持つ複数のIP DAGまたはIPレスDAGを追加	サポート対象外	サポート
クロス ドメインで同一の名前を持つ複数のIP DAGまたはIPレスDAGを追加	サポート対象外	サポート
クロス ドメインで同一の名前を持つ複数のスタンドアロン ホストを追加	サポート対象外	サポート

Plug-in for ExchangeはSnapCenter Plug-ins Package for Windowsに依存するため、同一の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とSnapDrive for WindowsがすでにインストールされているExchange ServerにPlug-in for Exchangeをインストールする場合は、SnapDrive for Windowsで使用されているVSSハードウェア プロバイダは、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るハードウェア プロバイダと互換性がないため、登録を解除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。 "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、[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	ホストタイプとして*Windows*を選択します。 SnapCenter Serverがホストを追加し、Plug-in for WindowsとPlug-in for Exchange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）。 Plug-in for WindowsとPlug-in for Exchangeのバージョンは同じである必要があります。異なるバージョンのPlug-in for Windowsが以前にインストールされていた場合は、SnapCenterのインストール時にバージョンが更新されます。

フィールド	操作
ホスト名	ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。 SnapCenterが機能するためには、DNSが適切に設定されている必要があります。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。 信頼されないドメイン ホストのIPアドレスがサポートされるのは、そのIPアドレスがFQDNに解決される場合のみです。 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。 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 • Exchange DAG Exchange DAGの場合は、次の操作を実行できます。 ◦ DAG名、DAGの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を追加する。 ◦ 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レスDAGクラスタを追加する。 ◦ 同一ドメインまたは別のドメインに存在するIPレスDAGを追加する。同じ名前で異なるドメインの複数のIP DAGまたはIPレスDAGを追加することもできます。 スタンドアロン ホストまたはExchange DAG（クロス ドメインまたは同一ドメイン）の場合は、ホストまたはDAGのFQDNかIPアドレスを指定することを推奨します。

フィールド	操作
Credentials	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモート ホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 指定したクレデンシャル名にカーソルを合わせると、クレデンシャルの詳細を確認できます。 クレデンシャルの認証モードは、ホスト追加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。

   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で必要とされる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 Server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	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`。 必要に応じて変更できます。
Add all hosts in the DAG	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。

フィールド	操作
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。

   [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。

NET TCP通信用のカスタム ポートの設定

デフォルトでは、 SnapCenter 6.0 リリース以降、Windows 用のSnapCenterプラグインは、NET TCP 通信にポート 909 を使用します。ポート909が使用中の場合は、NET 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\vssproviders\navssprv.exe.config* にある *NetTCPPort* キー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* キー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. 以下のコマンドを実行して、*Data ONTAP VSS Hardware Provider* 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`

services.msc のサービス リストにサービスが表示されていないことを確認します。

4. 以下のコマンドを実行して、*Data ONTAP VSS Hardware Provider* サービスを登録します。
`"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"`

   services.msc のサービス リストにサービスが表示されているかどうかを確認します。

5. *Plug-in for Windows* サービスを再起動します。

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 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 Server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 Server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、インストール要件とサポートされる構成のタイプ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としてwindowsホストを使用する必要があります。

手順

1. SnapCenter Server ホストで、*Open-SmConnection* コマンドレットを使用してセッションを確立し、資格情報を入力します。
2. 必要なパラメータを指定した *Add-SmHost* コマンドレットを使用して、Exchange 用プラグインをインストールするホストを追加します。

   コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

   ホストとしてスタンドアロン ホストまたはDAGを指定できます。DAG を指定する場合、*-IsDAG* パラメータは必須です。

3. 必要なパラメータを指定した *Install-SmHostPackage* コマンドレットを使用して、Exchange 用プラグインをインストールします。

   このコマンドを実行すると、指定したホストにPlug-in for Exchangeがインストールされて、SnapCenterに登録されます。

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 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。
- インストール前に、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、以下を参照してください。 "SnapCenterプラグイン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* フォルダーが存在し、ログインしたユーザーがそのフォルダーにフル アクセス権を持っているかどうかを検証します。
2. *C:\ProgramData\ NetApp\ SnapCenter \Package* リポジトリから Microsoft Windows 用のSnapCenterプラグインをダウンロードします。

   このパスには、SnapCenter Serverがインストールされているホストからアクセスできます。
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"<デバッグログパス>*" /log"*<ログパス>*" BI_SNAPCENTER_PORT=*<番号> *SUITE_INSTALLDIR="*<インストールディレクトリパス>*" BI_SERVICEACCOUNT=*<ドメイン\管理者> *BI_SERVICEPWD=*<パスワード> *ISFeatureInstall=HPPW,SCW,SCE*

   例えば：

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

   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	Value
/debuglog"<デバッグログパス>	インストーラのログ ファイルの名前と場所を次のように指定します。 *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。
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。

6. Windows タスク スケジューラ、メインのインストール ログ ファイル *C:\Installdebug.log*、および *C:\Temp* 内の追加のインストール ファイルを監視します。
7. *%temp%* ディレクトリを監視して、*msiexe.exe* インストーラー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 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。

SnapManager 7.x for ExchangeとSnapCenterの共存の設定

SnapCenter Plug-in for Microsoft Exchange ServerとSnapManager for Microsoft Exchange Serverを共存させるには、SnapManager for Microsoft Exchange Serverがインストールされているのと同じ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で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とSnapDrive for Windowsがすでにインストールされていて、SnapManager for Microsoft Exchange Serverのバックアップがシステムの*SnapInfo*ディレクトリに保存されている必要があります。
- SnapManager for Microsoft Exchange Serverで作成した不要な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に共存させることができますが、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 オプションが用意されていません。

- SnapCenterでは、SnapManager for Microsoft Exchange Serverのバックアップからのデータベースのリストアが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、SnapManager for Microsoft Exchange Serverのバックアップをあとから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 プロバイダー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ーの登録を解除します：*navssprv.exe -r service –u*
3. VSS ハードウェア プロバイダーが削除されたことを確認します: *vssadmin list providers*
4. ExchangeホストをSnapCenterに追加して、SnapCenter Plug-in for Microsoft Windowsと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ディレクトリから、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、スケジュール済みバックアップの設定、保持設定の指定を行います。
8. SnapManager for Microsoft Exchange Serverをアンインストールします。

   SnapManager for Microsoft Exchange Serverをすぐにアンインストールせずに、SnapManager for Microsoft Exchange Serverのバックアップをあとから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 Microsoft Exchange Server 用SnapCenterプラグイン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\ SnapDrive* ディレクトリから、すべての DAG ノードにSnapDrive for Windows を登録します: *navssprv.exe -r service -a 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。

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。SnapMirrorテクノロジとSnapVaultテクノロジを使用できるようにSnapCenter Serverをセットアップ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 デバイス上のソース 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、初期化する必要があります。この作業を実行するには、NetApp System 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ます。

詳細情報

"REST APIの使用"

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

ユーザがPlug-in for Exchangeを使用するためには、SnapCenter管理者が事前にSnapCenter Serverをインストールして設定し、前提条件となるタスクを実行する必要があります。

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

> SnapCenterでは、別々のクラスタに属している場合でも、複数のSVM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SVMには、すべて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 Serverを使用してVMware RDM LUN上の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のツールを使用して、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である場合は、SnapMirror関係とSnapVault関係をセットアップします。

SnapCenter Plug-in for VMware vSphere 4.1.1のドキュメントには、SnapCenter 4.1.1のユーザ向けに、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。NetApp Data Broker 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 Data Broker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 4.3のドキュメントには、SnapCenter 4.3.xのユーザ向けに、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の保護におけるソース、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、再シードの各処理に関連する基本的な概念を理解しておくと役立ちます。ここでは、これらの処理で扱うリソース、リソース グループ、およびポリシーについて説明します。

- リソースとは、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のリソース 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。

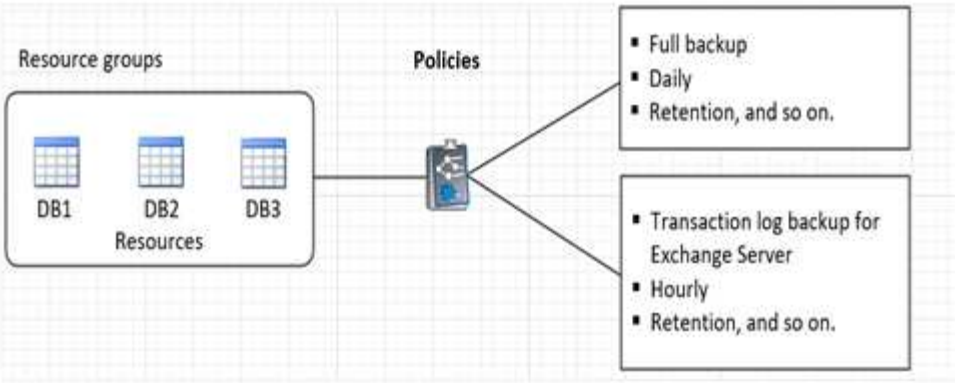
  リソース グループに対して処理を実行すると、リソース グループに指定したスケジュールに従って、リソース グループに定義されているリソースに対して処理が実行されます。

  単一のリソースまたはリソース グループをオンデマンドでバックアップすることができます。また、スケジュールされたバックアップを単一リソースおよびリソース グループに対して実行することもできます。

  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、スクリプトといった、データ保護処理の特性を指定するものです。

  リソース グループを作成するときに、そのグループに対して1つ以上のポリシーを選択します。オンデマンドで単一リソースのバックアップを実行するときにも、1つ以上のポリシーを選択できます。

リソース グループは、保護する対象と、それを日時でいつ保護するかを定義するものと考えてください。ポリシーとは、それをどのように保護したいかを定義するものと考えてください。たとえば、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。このリソース グループに、日次ポリシーと毎時ポリシーの2つのポリシーを適用します。リソース グループを作成してポリシーを適用する際に、フル バックアップを1日1回実行するようにリソース グループを設定し、別のスケジュールでログ バックアップを1時間おきに実行するように設定します。次の図は、データベースのリソース、リソース グループ、ポリシーの関係を示しています。



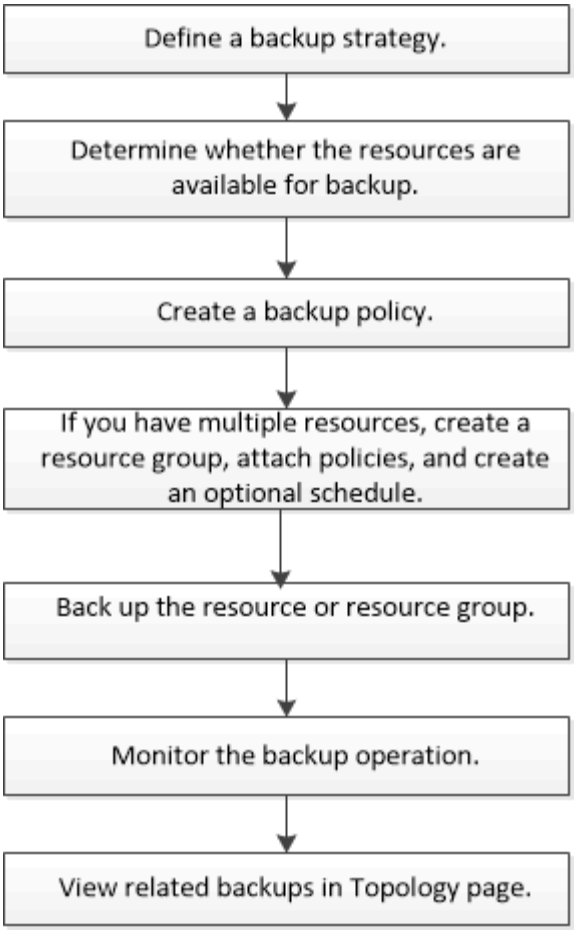
Exchangeリソースのバックアップ

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することができます。

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の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に付属するEseutilツールを使用して、Exchangeのデータベースとバックアップを検証できます。

Microsoft Exchange Eseutilツールは、Exchange Serverに付属するコマンドライン 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のデータベースと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: 少なくとも 2 つのレプリカを持つデータベース可用性グループ (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、 "Microsoft Exchange Server ドキュメント" 。

Exchangeの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やExchangeデータベース可用性グループのことです。リソースをリソース グループに追加することで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 Serverのインストール、ホストの追加、ストレージ システム接続の作成、クレデンシャルの追加、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にアクティブな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。その "SnapCenter Plug-in for VMware vSphereのドキュメント"詳細情報があります。

タスク概要

- 詳細ページの*全体的なステータス*オプションがバックアップ不可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、全体的なステータス オプションはバックアップに利用できませんに設定されます。
  - 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。

    データベースの状態がマウント、アンマウント、再シード、リカバリ保留中のいずれかのときは、正常な状態ではありません。
- データベース可用性グループ（DAG）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] ページの左上隅にあるプラグイン 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、完全修飾ドメイン名（FQDN）形式でそれぞれのDAG名やホスト名が表示されるので、データベースが複数あっても識別できます。

   クリックホスト名と Exchange Server を選択して、リソースをフィルターします。そのあとにをクリックすると、フィルタ ペインが閉じます。
3. *リソースの更新*をクリックします。

   新たに追加、名称変更、削除されたリソースが、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。

   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。

   - データベースが他社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 データベース コピーがNetApp以外のストレージ上にあり、少なくとも 1 つのパッシブ データベース コピーがNetAppストレージ上にある場合、全体的なステータス 列に「保護さ

れていません」と表示されます。

他社ストレージ タイプにあるデータベースには、データ保護処理を実行できません。

- データベースがNetAppストレージ上にあり、保護されていない場合は、[全体的なステータス] 列に [保護されていません] と表示されます。
- データベースがNetAppストレージ システム上にあり、保護されている場合、ユーザー インターフェイスの 全体的なステータス 列に「バックアップは実行されていません」というメッセージが表示されます。
- データベースがNetAppストレージ システム上にあり、保護されており、データベースのバックアップがトリガーされた場合、ユーザー インターフェイスの [全体的なステータス] 列に [バックアップが成功しました] というメッセージが表示されます。

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 ポリシーを作成することができます。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可能です。

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説明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リソースを更新（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ユーザには、SnapCenter管理者がユーザに対してソースとデスティネーションの両方のボリューム用にStorage Virtual Machine（SVM）を割り当てておく必要があります。
- PowerShellスクリプトをプレスクリプトとポストスクリプトで実行したい場合は、`usePowershellProcessforScripts`パラメータをtrueに設定する `web.config`ファイル。

  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

- バックアップ ポリシーとは、バックアップを管理および保持する方法やリソースやリソース グループをバックアップする頻度を定めた一連のルールです。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しておくことで、別のリソース グループにポリシーを再利用して時間を節約することができます。
- フル バックアップの保持設定は、ポリシーごとに固有です。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やリソースでは4つのフル バックアップが保持され、同じデータベースやリソースのポリシーBには影響しません。ポリシーBの保持数が3であれば、ポリシーBを使用すると3つのフル バックアップが保持されます。

- ログ バックアップの保持設定はポリシーの違いを超えて影響を及ぼし、データベースや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と、そのログ保持設定は、同じデータベースやリソースの、ポリシーAで作成されたログ バックアップに影響します。同様に、ポリシーAのログ保持設定は、同じデータベースの、ポリシーBで作成されたログ バックアップに影響します。
- 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。

  ベスト プラクティス: 保持する完全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構成することをお勧めします。セカンダリ保持ポリシーについては、データベースとログが異なるボリュームにある場合はそれぞれのバックアップに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それぞれのバックアップに2つのSnapshotを保持できることを念頭に置いて設定してください。

- 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、SnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[ポリシー]をクリックします。
3. *新規*をクリックします。
4. 「名前」ページで、ポリシー名と詳細を入力します。
5. 「バックアップ タイプとレプリケーション」ページで、次の手順を実行します。

   a. バックアップ タイプを選択します。

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	*完全バックアップとログバックアップ*を選択します。 データベースはログを切り捨てるかたちでバックアップされ、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。 これは推奨されるバックアップ タイプです。
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	*完全バックアップ*を選択します。 データベースはログを切り捨てるかたちでバックアップされ、切り捨てられたログはバックアップされません。
すべてのトランザクション ログをバックアップ	*ログバックアップ*を選択します。 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。 ライブ ログと同じディスクに *scebackupinfo* ディレクトリが作成されます。このディレクトリには、Exchangeデータベースの変更内容の差分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。
トランザクション ログ ファイルの切り捨てなしで、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	*バックアップのコピー*を選択します。 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。通常このタイプのバックアップは、レプリカの再シードのほか、問題のテストや診断のために使用します。

ログ バックアップに必要なスペースは、最新の状態（UTM）保持設定ではなく、フル バックアップ保持設定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個別のバックアップ ポリシーを作成して、同じラベルを使用し、ラベルごとにログ ポリシーのkeep（保持）の値をデータベース ポリシーの値の2倍に設定します。詳細については、"SnapCenter for Exchange バックアップは、Vault の宛先ログボリュームにスナップショットの半分のみを保存します。"

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

フィールド	操作
アクティブコピーをバックアップする	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。 データベース可用性グループ（DAG）については、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。 パッシブ コピーはバックアップされません。
Back up copies on servers to be selected at backup job creation time	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。 DAGについては、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。

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に保持されます。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。保持設定はノード 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、オンデマンド、時間別、日次、週次、*月次*の 1 つ以上の頻度タイプを選択します。

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

午前 2 時にスケジュールを設定した場合、夏時間 (DST) 中はスケジュールは実行されません。

a. ポリシーラベルを選択します。

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

b. [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	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保持する場合（SnapMirror）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。 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。 Exchange ONTAPボリュームに対してSnapMirrorアクティブ同期が設定されている場合は、プライマリのみのポリシーは使用できません。SnapCenterではこれが許可されていません。「Mirror」オプションを有効にする必要があります。 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Exchangeバックアップの表示"] 。
Update SnapVault after creating a local Snapshot	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。
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。

6. [Retention]ページで、保持設定を指定します。

   表示されるオプションは、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。

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

   SnapVaultレプリケーションを有効にする場合は、保持数を2以上に設定する必要があります。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。

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	*ログが保持される完全バックアップの数*を選択し、最新の状態に復元可能な完全バックアップの数を指定します。 最新の状態（UTM）保持設定は、フル バックアップまたはログ バックアップを通じて作成されたログ バックアップに適用されます。たとえば、UTM保持設定が過去5回分のフル バックアップのログ バックアップを保持するようになっている場合、過去5回分のフル バックアップのログ バックアップが保持されます。 フル / 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処理の流れの中で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 バックアップやフル / ログ バックアップの保持設定が1カ月に設定され、UTM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環として作成されたログ フォルダは、UTM保持設定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。 最新の状態へのリストアを実行しない場合は、UTM保持設定の値を0に設定します。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。 ベスト プラクティス: この設定は、完全バックアップの保持設定セクションのスナップショットの合計数 (完全バックアップ) の設定と同じにすることが最適です。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。
バックアップ コピーを特定の日数だけ保持	最後のログ バックアップを保持する 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。 フル バックアップが保持される日数まで、ログ バックアップが保持されます。
Snapshot locking period	*スナップショット コピーのロック期間*を選択し、日、月、または年を選択します。 SnapLock保持期間は100年未満にする必要があります。

バックアップ タイプとして [ログ バックアップ] を選択した場合、ログ バックアップは完全バックアップの最新保持設定の一部として保持されます。

b. [Full backup retention settings]セクションで、次のいずれかをオンデマンド バックアップ用に選択し、続けてフル バックアップ用にもいずれかを選択します。

フィールド	操作
Retain only a specific number of Snapshots	保持する完全バックアップの数を指定する場合は、「保持するスナップショット コピーの合計数」オプションを選択し、保持するスナップショット (完全バックアップ) の数を指定します。 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、最も古いコピーから順に削除されます。
Retain full backups for a specific number of days	スナップショット コピーの保存期間 オプションを選択し、スナップショット (完全バックアップ) を保存する日数を指定します。
プライマリスナップショットのロック期間	*プライマリ スナップショット コピーのロック期間*を選択し、日、月、または年を選択します。 SnapLock保持期間は100年未満にする必要があります。
セカンダリスナップショットのロック期間	*セカンダリ スナップショット コピーのロック期間*を選択し、日、月、または年を選択します。

DAG構成のホストにフル バックアップがなくログ バックアップのみのデータベースがある場合は、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完全バックアップを見つけ、完全バックアップの前にこのホストで作成されたすべてのログ バックアップを削除します。
- *C:\Program Files\ NetApp\ SnapCenter WebApp\web.config* ファイルにキー **MaxLogBackupOnlyCountWithoutFullBackup** を追加することで、ログ バックアップのみを使用する DAG 内のホスト上のデータベースに対する上記のデフォルトの保持動作をオーバーライドできます。

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

この例では、値が10になっています。これは、ホストで保持できるログ バックアップが最大10個であることを意味します。

7. [Script]ページで、バックアップ処理の前またはあと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。

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

  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。

8. 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 グループはいずれのデータ保護ジョブにも必要になります。リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプと保護スケジュールを定義することも必要です。

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。

- 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するリソースを含む既存のリソース グループにSnapMirrorアクティブ同期を使用しない新しいデータベースを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 モードである既存のリソース 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 ウィンドウで [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。

> SnapCenterに最近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. [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。
Tags	リソース グループを検索しやすくするために、ラベルを入力します。 たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。
Use custom name format for Snapshot copy	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* または *resourcegroup_hostname* です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

5. [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、使用可能なリソースのリストをフィルタします。

      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。

      [Available Resources]セクションと[Selected Resources]セクションに、データベース名がホストの完全修飾ドメイン名（FQDN）とともに表示されます。このFQDNは、データベースが特定のホスト上でアクティブであり、このホスト上にはバックアップが作成されない可能性があることを示すためのものです。ポリシーで「バックアップ ジョブの作成時に選択されるサーバー上のコピーをバックアップする」オプションを選択した場合は、バックアップを実行するサーバー選択オプションから 1 つ以上のバックアップ サーバー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見つけます。
   c. 次のいずれかの手順を実行し、リソースを[Available Resources]セクションから[Selected Resources]セクションに移動します。
      - 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」を選択します。
      - 「利用可能なリソース」セクションからリソースを選択し、右矢印をクリックして「選択したリソース」セクションに移動します。

        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の数は、1つのSnapshotにつき最大30個です。1つのリソース グループに30個を超えるデータベースがある場合は、超過分のデータベース用に2つ目のSnapshotが作成されます。それに伴い、メ

インのバックアップ 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やSnapVaultの更新中に、両方のサブジョブの更新が同時に実行される場合があります。ログにジョブの完了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 + 。

      ポリシーに「バックアップ ジョブの作成時に選択されるサーバー上のコピーをバックアップする」オプションが含まれている場合は、1 つ以上のサーバーを選択するためのサーバー選択オプションが表示されます。サーバ選択オプションには、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。

      [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. 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 *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、[**OK**] をクリックします。

      この操作は、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。構成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を構成する] セクションの [適用されたスケジュール] 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。

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

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

   電子メール通知の場合は、GUIまたはPowerShellコマンドを使用してSMTPサーバーの詳細を指定する必要があります。 `Set-SmSmtpServer` 。

   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" 。

8. 概要を確認し、[完了] をクリックします。

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

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

開始する前に

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

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

- ストレージ システムの名前は一意である必要があります。

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

手順

1. PowerShell接続セッションを開始するには、 `Open-SmConnection`コマンドレット。

   PowerShellセッションを開く例を次に示します。

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

2. ストレージシステムへの新しい接続を作成するには、 `Add-SmStorageConnection`コマンドレット。

   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. 新しい実行アカウントを作成するには、 `Add-Credential`コマンドレット。

   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アカウントを作成する例を次に示します。

   ```
   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" 。

Exchangeデータベースのバックアップ

データベースがどのリソース グループにも含まれていない場合は、[Resources]ページからデータベースまたはデータベース可用性グループを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、データベースが使用する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。
- NetAppおよび非NetAppストレージ上にアクティブ/パッシブ データベース コピーを持つ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、ポリシーで アクティブ コピーをバックアップする または バックアップ ジョブの作成時に選択されるサーバー上のコピーをバックアップするオプションを選択すると、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、他社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を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 ウィンドウで、[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] を選択します。

   リソースページでは、  アイコンは、データベースがNetApp以外のストレージ上にあることを示します。

   DAG内で、アクティブ データベース コピーが他社ストレージにあり、1つ以上のパッシブ 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。

   クリック  *、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ーします。 *をクリックします フィルター パネルを閉じます。

   - 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. トポロジ ビューが表示されている場合は、[保護] をクリックします。
     ii. [Database - Protect Resource]ウィザードが表示された場合は、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 スナップショット名を指定する場合は、[リソース] ページで [スナップショット コピーにカスタム名形式を使用する] チェック ボックスをオンにし、スナップショット名に使用するカスタム名形式を入力します。

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

      ポリシーに「バックアップ ジョブの作成時に選択されるサーバー上のコピーをバックアップする」オプションが含まれている場合、1 つ以上のサーバーを選択するためのサーバー選択オプションが表示されます。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。

      [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. クリック *  * 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。

5. 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。リソースに対して実行されたバックアップ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。

6. 概要を確認し、[完了] をクリックします。

データベース トポロジの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]ページで次の手順を実行します。
   a. リソースに複数のポリシーを適用している場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

      オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

   b. *バックアップ*をクリックします。
9. バックアップの進捗状況を監視するには、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]ページを表示します。
   - MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

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

   - VMDK上のアプリケーション データをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープ サイズが不足していると、バックアップが失敗することがあります。

     Java ヒープ サイズを増やすには、スクリプト ファイル */opt/netapp/init_scripts/scvservice* を見つけます。このスクリプトでは、*do_start method* コマンドによって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、Exchangeのバックアップ タイプとしてフル バックアップとログ バックアッ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、Exchangeのバックアップ タイプとして1時間ごとのフル バックアップとログ バックアッ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 ポリシーを作成しています。

```
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_Lo
g_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データベース可用性グループ（DAG）のバックアップ 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_Lo
g_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ています。

```
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。

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。

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

この例では、ジョブIDを指定してジョブ サマリ レポートを表示しています。

```
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関する情報は、*Get-Help command_name* を実行すると取得できます。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" 。

Exchange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、[Resources]ページでバックアップできます。

開始する前に

- ポリシーを適用したリソース 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、データベースが使用する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。
- 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、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が遅れることがあります。の値を設定する必要があります `MaxRetryForUninitializedHosts`で `web.config`を使用することにより `Set-SmConfigSettings`PowerShell コマンドレット。
- リソース グループに、 NetAppおよび非NetAppストレージ上にアクティブ/パッシブ データベース コピーを持つデータベースまたはデータベース可用性グループを含め、ポリシーで アクティブ コピーをバックアップ または バックアップ ジョブの作成時に選択されるサーバー上のコピーをバックアップ オプションを選択した場合、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、他社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。

タスク概要

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

手順

1. 左側のナビゲーション ウィンドウで、[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、をクリックします。 *、タグを選択します。 *をクリックします フィルター パネルを閉じます。
3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] をクリックします。
4. [Backup]ページで次の手順を実行します。
   a. リソース グループに複数のポリシーを関連付けている場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

      オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

b. *バックアップ*をクリックします。

5. バックアップの進捗状況を監視するには、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]ページを表示します。

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。

Exchangeデータベースのバックアップ処理のキャンセル

キューに登録されているバックアップ処理はキャンセルできます。

必要なもの

- 処理をキャンセルするには、SnapCenter管理者かジョブ所有者としてログインする必要があります。
- バックアップ操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のバックアップ処理はキャンセルできません。
- バックアップ処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。
- キャンセルできない操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたバックアップ操作をキャンセルできます。

手順

1. 次のいずれかを実行します。

方法	アクション
[Monitor]ページ	a. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 b. 操作を選択し、「ジョブのキャンセル」をクリックします。

方法	アクション
[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、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に立ちます。

タスク概要

[Topology]ページに、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をすべて表示できます。これらのバックアップの詳細を参照し、対象を選択してデータ保護処理を実行できます。

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の数を表示します。
-  SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップの数を表示します。
  - 表示されるバックアップの数には、セカンダリ ストレージから削除されたバックアップも含まれます。

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

ベスト プラクティス: 複製されたバックアップの正しい数が表示されるようにするには、トポロジを更新することをお勧めします。

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 リストからデータベース、リソース、またはリソース グループを選択します。
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[Topology]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 ストレージ上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およびログ バックアップの総数が表示されます。

   更新 ボタンをクリックすると、ストレージのクエリが開始され、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フェイルオーバー後の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 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。

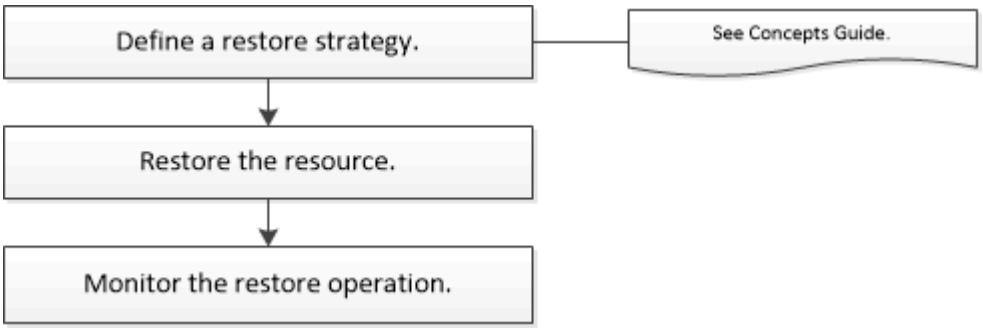
セカンダリ ストレージ上のバックアップは、名前変更または削除できません。Snapshotの削除は、ONTAPの保持設定で処理されます。

Exchangeリソースのリストア

リストアのワークフロー

SnapCenterを使用して、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することにより、Exchangeデータベースをリストアすることができます。

次のワークフローは、Exchangeデータベースの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、 "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際の要件

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、以下の要件を満たしていることを確認する必要があります。

すべてのリストア機能を使用するには、SnapCenter ServerとSnapCenter Plug-in for Exchange データベースの両方を4.6にアップグレードする必要があります。

- Exchange Serverがオンラインで、稼働し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スケジュールは、一時停止する必要があります。
- SnapCenter ServerとSnapCenter Plug-in for Microsoft Exchange Serverホストが、リストア対象のバックアップが格納されているプライマリ 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することができます。

開始する前に

- リソース グループ、データベース、またはデータベース可用性グループ（DAG）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するリストア処理は実行できません。
- Snapshotをミラーまたはバックアップにレプリケートするユーザには、SnapCenter管理者がユーザに対して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。
- DAG内で、アクティブ データベース コピーが他社ストレージにある場合に、NetAppストレージにあるパッシブ データベース コピーの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 コピーとして設定し、リソースを更新してリストア処理を実行します。

  実行 `Move-ActiveMailboxDatabase`パッシブ データベース コピーをアクティブ データベース コピーとして作成するコマンド。

  その "Microsoftのドキュメント"このコマンドに関する情報が含まれています。

タスク概要

- 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。

  レプリケーションに使用するファイルなどのExchangeファイルが含まれているディスクでは、Plug-in for Exchangeによるディスクのフル 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により単一ファイルのリストア処理が実行されます。

- Plug-in for Exchangeでは、BitLockerで暗号化されたドライブは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 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。
- 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。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで、リソース ページの左上隅にある 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. コピーの管理ビューで、プライマリバックアップテーブルから*バックアップ*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
All log backups	完全バックアップ後に利用可能なすべてのログ バックアップを復元するために、最新のバックアップ復元操作を実行するには、[すべてのログ バックアップ] を選択します。
By log backups until	ポイントインタイム復元操作を実行するには、[ログ バックアップまで] を選択します。これにより、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復元されます。 ドロップダウン リストに表示されるログの数は、UTMに基づきます。たとえば、フル バックアップの保持数が5でUTMの保持数が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できるログが3つだけ表示されます。
By specific date until	復元されたデータベースにトランザクション ログが適用される日時を指定するには、[特定の日付まで] 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、指定した日時のバックアップまでに記録されたトランザクション ログのエントリがリストアされます。
None	ログ バックアップなしで完全バックアップのみを復元する必要がある場合は、[なし] を選択します。

次のいずれかを実行します。

- 復元後にデータベースを回復してマウントする - このオプションはデフォルトで選択されています。

◦ 復元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 は復元操作を実行する前に、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. [Script]ページで、リストア処理の前またはあと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 プリ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、$TargetServerInstanceがあります。

   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。

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

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

9. 概要を確認し、[完了] をクリックします。
10. 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表示できます。

    モニター > ジョブ ページを使用して、復元プロセスを監視する必要があります。

レプリカとアクティブ データベースの間に遅延がある場合に、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、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が開始されたときに発生します。Exchange Serverによりレプリカの修正が試みられますが、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. 指定されたユーザーに対してSnapCenter Serverとの接続セッションを開始するには、 `Open-SmConnection`コマンドレット。

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

2. 復元したい1つ以上のバックアップに関する情報を取得するには、 `Get-SmBackup`コマンドレット。

   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
--------                       ----------
----------                     ----------
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. バックアップからデータを復元するには、 `Restore-SmBackup`コマンドレット。

   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 ストレージにリストアしています。

```
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
```

   その `-archive`パラメータを使用すると、復元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。

   その `-IsRecoverMount:$true`パラメータを使用すると、復元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" 。

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データベース全体ではなく、メールやメールボックスの単位でリストアとリカバリを実行できます。

1件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のは、大量の時間とリソースを消費することになります。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の使い方については、 "SMBR 管理ガイド" 。

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で単一アイテムを手動でリストアする方法（Ontrack PowerControlsの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復元する方法"
- "SMBR を使用してSnapVaultから Microsoft Exchange メールを回復する"

セカンダリ ストレージからの**Exchange Server**データベースのリストア

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。

手順

1. 左側のナビゲーション ウィンドウで、[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] ドロップダウン リストから [データベース] または [リソース グループ] 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 (ミラーまたはボールト) 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、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. 復元ウィザードを完了し、概要を確認して、[完了] 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

コピーの破損時など、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

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。

+ ノード間の遅延を回避するには、再シード操作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持つホストを選択します。

手順

1. 左側のナビゲーション ウィンドウで、[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	表示リストから*データベース*を選択します。
DAG内のデータベースを再シードする	表示リストから*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. 「コピーの管理」ページで、「再シード」をクリックします。
5. 再シード ウィザードの正常でないデータベース コピーのリストから、再シードするものを選択し、[次へ] をクリックします。
6. ホスト ウィンドウで、再シードするバックアップがあるホストを選択し、[次へ] をクリックします。
7. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

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

パッシブ データベース コピーが他社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データベース用のPowerShellコマンドレットを使用したレプリカの再シード

PowerShellコマンドレットを使用すると、同じホスト上にある最新のコピーまたは代替

ホスト上にある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. 指定されたユーザーに対してSnapCenter Serverとの接続セッションを開始するには、 `Open-SmConnection`コマンドレット。

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

2. データベースを再シードするには、 `reseed-SmDagReplicaCopy`コマンドレット。

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

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

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

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

リストア処理の監視

[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。

Exchangeデータベースの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。

著作権に関する情報

商標に関する情報