SnapCenterプラグインとBlueXP backup and recoveryによる VMware の 3-2-1 データ保護

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/netapp-solutions-cloud/vmware/vmw-hybrid-321-dp-scv.html on August 18, 2025. Always check docs.netapp.com for the latest.

目次

SnapCenterプラグインとBlueXP backup and recoveryによる VMware の 3-2-1 データ保護 . . . 1
概要 . . . 1
ユースケース . . . 1
NetApp ONTAPデータストレージ . . . 1
SnapCenter Plug-in for VMware vSphere . . . 2
仮想マシンのBlueXP backup and recovery . . . 2
高レベルアーキテクチャ . . . 5
ソリューションの展開 . . . 6
ONTAPクラスタ間のSnapMirror関係を確立する . . . 6
SnapCenter Plug-in for VMware vSphereを構成する . . . 19
BlueXP backup and recoveryでオブジェクト ストレージへのバックアップを構成する . . . 29
データ損失の場合の仮想マシンの復元 . . . 40
まとめ . . . 45
追加情報 . . . 45

SnapCenterプラグインとBlueXP backup and recoveryによる VMware の 3-2-1 データ保護

3-2-1 バックアップ戦略は業界で認められたデータ保護方法であり、貴重なデータを保護するための包括的なアプローチを提供します。この戦略は信頼性が高く、予期しない災害が発生した場合でも、データのコピーが利用可能であることを保証します。

概要

この戦略は、次の 3 つの基本ルールで構成されます。

1. データのコピーを少なくとも 3 つ保存してください。これにより、1 つのコピーが失われたり破損したりした場合でも、少なくとも 2 つのコピーが残っているので、それを頼りにすることができます。
2. 2 つのバックアップ コピーを異なるストレージ メディアまたはデバイスに保存します。ストレージ メディアを多様化することで、デバイス固有またはメディア固有の障害から保護することができます。 1 つのデバイスが破損したり、ある種類のメディアに障害が発生したりしても、他のバックアップ コピーは影響を受けません。
3. 最後に、少なくとも 1 つのバックアップ コピーがオフサイトにあることを確認します。オフサイト ストレージは、オンサイト コピーが使用できなくなる可能性のある火災や洪水などの局所的な災害に対するフェイルセーフとして機能します。

このソリューション ドキュメントでは、SnapCenter Plug-in for VMware vSphere (SCV) を使用してオンプレミスの仮想マシンのプライマリ バックアップとセカンダリ バックアップを作成し、仮想マシン用のBlueXP backup and recoveryを使用してデータのコピーをクラウド ストレージまたはStorageGRIDにバックアップする 3-2-1 バックアップ ソリューションについて説明します。

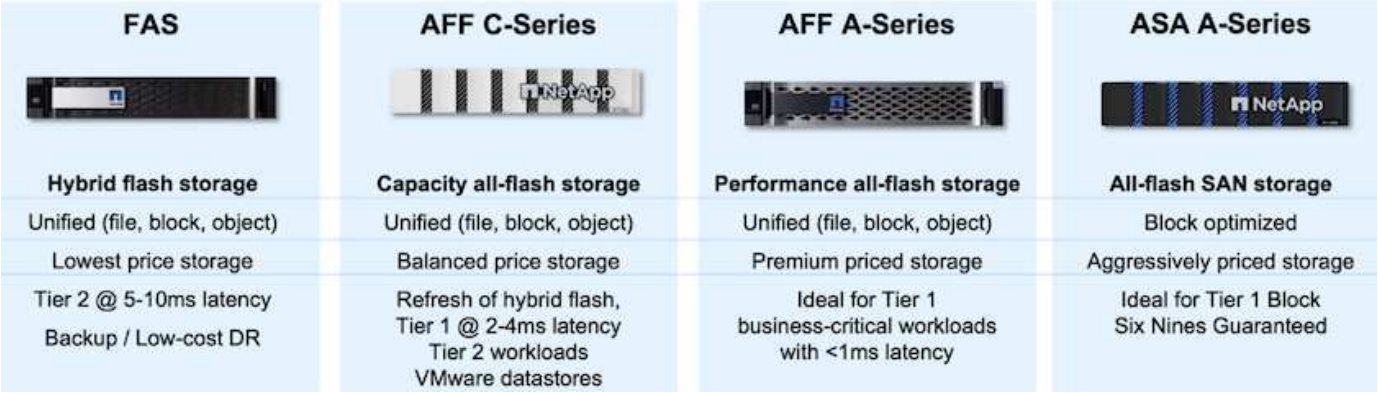
ユースケース

このソリューションは、次のユースケースに対応します。

- SnapCenter Plug-in for VMware vSphereを使用して、オンプレミスの仮想マシンとデータストアをバックアップおよび復元します。
- ONTAPクラスターでホストされ、仮想マシン用のBlueXP backup and recovery。

NetApp ONTAPデータストレージ

ONTAP は、SAN プロトコルまたは NAS プロトコルのどちらでアクセスする場合でも統合ストレージを提供する、NetApp の業界をリードするストレージ ソリューションです。 3-2-1 バックアップ戦略により、オンプレミスのデータが複数のメディア タイプで保護されることが保証され、 NetApp は高速フラッシュから低コストのメディアに至るまでのプラットフォームを提供します。



NetAppのハードウェアプラットフォームの詳細については、以下をご覧ください。 "NetAppデータストレージ" 。

SnapCenter Plug-in for VMware vSphere

SnapCenter Plugin for VMware vSphere は、VMware vSphere と緊密に統合され、仮想マシンのバックアップとリストアの管理を容易にするデータ保護サービスです。このソリューションの一部として、 SnapMirror は、セカンダリONTAPストレージ クラスタ上に仮想マシン データの 2 番目の不変バックアップ コピーを作成するための高速で信頼性の高い方法を提供します。このアーキテクチャを導入すると、プライマリ バックアップの場所またはセカンダリ バックアップの場所から仮想マシンの復元操作を簡単に開始できるようになります。

SCV は、OVA ファイルを使用して Linux 仮想アプライアンスとして展開されます。プラグインはリモート プラグイン アーキテクチャを使用するようになりました。リモート プラグインは vCenter サーバーの外部で実行され、SCV 仮想アプライアンス上でホストされます。

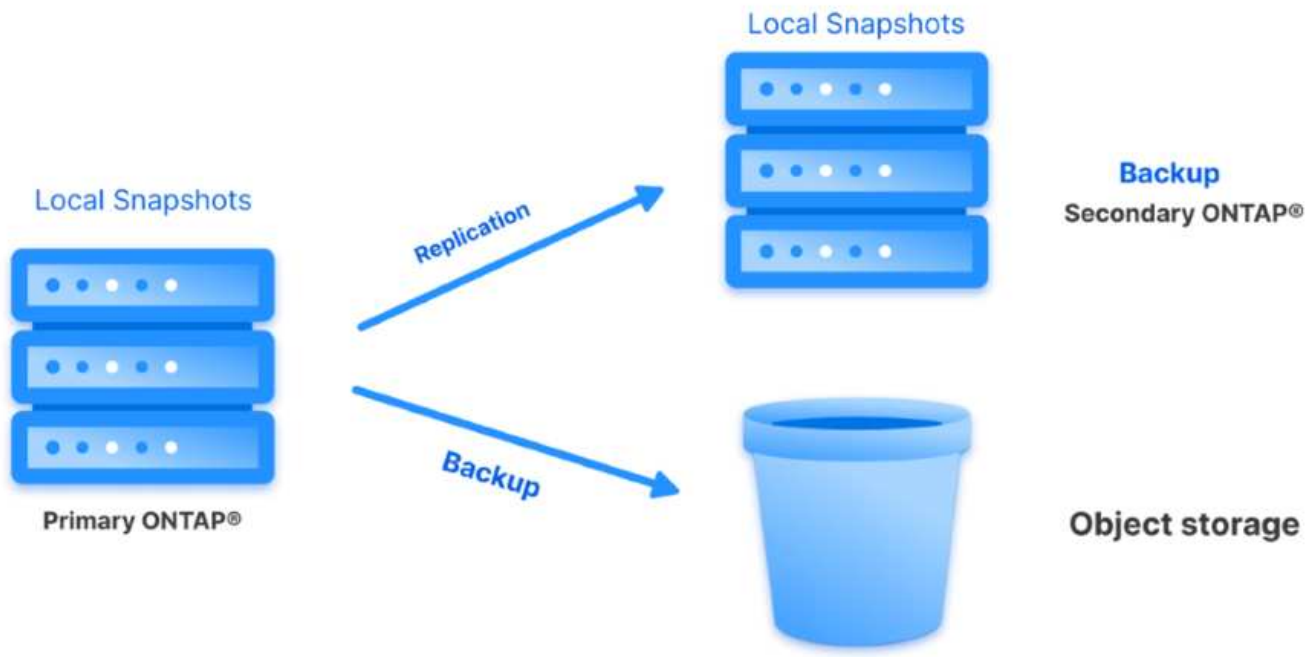
SCVの詳細については、 "SnapCenter Plug-in for VMware vSphereのドキュメント" 。

仮想マシンのBlueXP backup and recovery

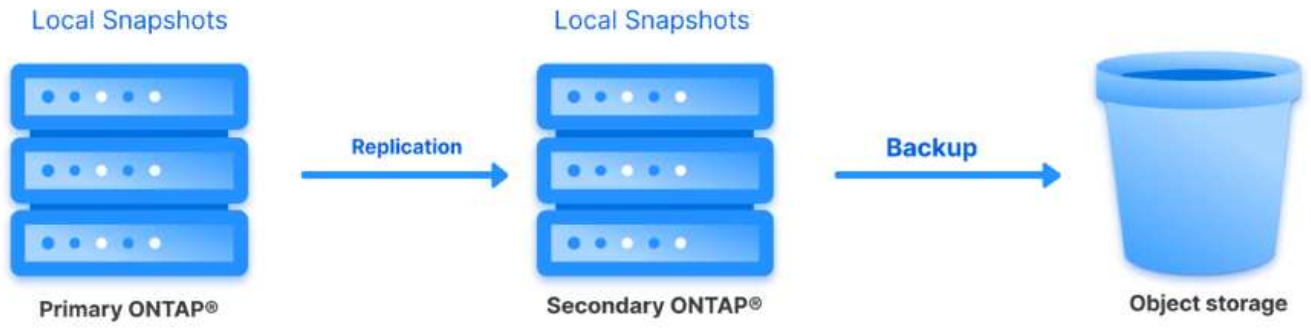
BlueXP backup and recoveryは、オンプレミスとクラウド環境の両方にわたる幅広いバックアップおよびリカバリ操作に対して単一のコントロール プレーンを提供する、クラウド ベースのデータ管理ツールです。NetApp BlueXP backup and recoveryスイートの一部である機能は、VMware vSphere (オンプレミス) 用のSnapCenterプラグインと統合して、データのコピーをクラウド内のオブジェクト ストレージに拡張します。これにより、プライマリまたはセカンダリ ストレージ バックアップから取得されたデータの 3 番目のコピーがオフサイトに作成されます。 BlueXP backup and recoveryを使用すると、オンプレミスのこれら 2 つの場所のいずれかからデータのコピーを転送するストレージ ポリシーを簡単に設定できます。

BlueXP Backup and Recovery でソースとしてプライマリ バックアップとセカンダリ バックアップのいずれかを選択すると、次の 2 つのトポロジのいずれかが実装されます。

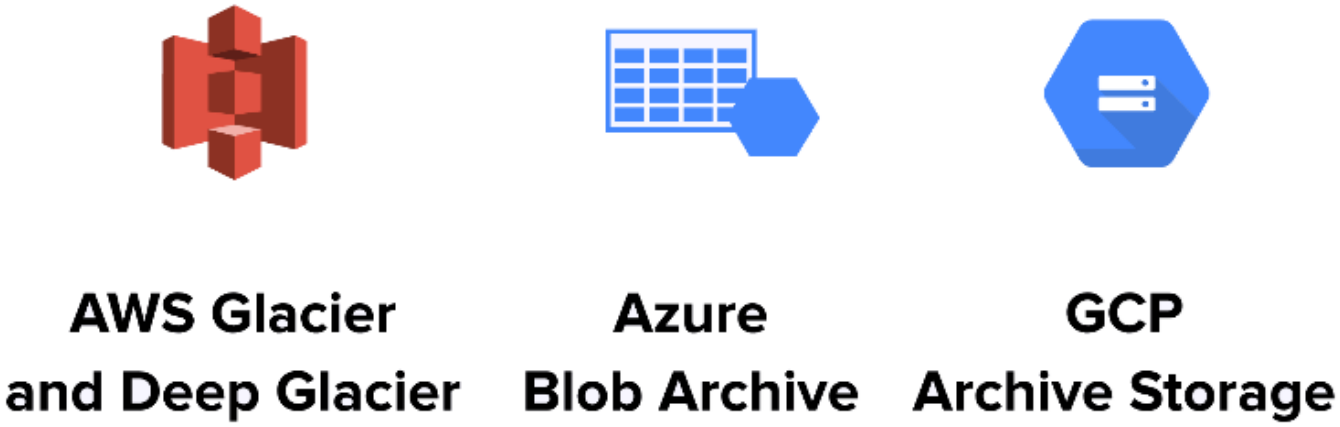
ファンアウト トポロジ – SnapCenter Plug-in for VMware vSphereによってバックアップが開始されると、ローカル スナップショットが直ちに作成されます。次に、SCV は最新のスナップショットをセカンダリONTAPクラスタに複製するSnapMirror操作を開始します。 BlueXP Backup and Recovery では、ポリシーによって、選択したクラウド プロバイダーのオブジェクト ストレージに転送されるデータのスナップショット コピーのソースとしてプライマリONTAPクラスターが指定されます。



カスケード トポロジ – SCV を使用してプライマリ データ コピーとセカンダリ データ コピーを作成する方法は、上記のファンアウト トポロジと同じです。ただし、今回は、オブジェクト ストレージへのバックアップがセカンダリONTAPクラスターから実行されるように指定するポリシーがBlueXP Backup and Recovery に作成されます。



BlueXP backup and recoveryでは、オンプレミスのONTAPスナップショットのバックアップ コピーを AWS Glacier、Azure Blob、GCP アーカイブ ストレージに作成できます。



さらに、オブジェクト ストレージのバックアップ ターゲットとしてNetApp StorageGRIDを使用することもできます。 StorageGRIDの詳細については、 "StorageGRIDランディングページ" 。

ソリューション展開の概要

このリストには、このソリューションを構成し、SCV およびBlueXP backup and recoveryからバックアップと復元操作を実行するために必要な高レベルの手順が示されています。

1. プライマリおよびセカンダリ データ コピーに使用するONTAPクラスタ間のSnapMirror関係を構成します。
2. VMware vSphere 用のSnapCenterプラグインを構成します。
   a. ストレージシステムを追加する
   b. バックアップ ポリシーの作成
   c. リソース グループの作成
   d. 最初のバックアップジョブを実行する
3. 仮想マシンのBlueXP backup and recoveryを構成する
   a. 作業環境を追加する
   b. SCVおよびvCenterアプライアンスの検出
   c. バックアップ ポリシーの作成
   d. バックアップを有効にする
4. SCV を使用してプライマリ ストレージとセカンダリ ストレージから仮想マシンを復元します。
5. BlueXPバックアップと復元を使用して、オブジェクト ストレージから仮想マシンを復元します。

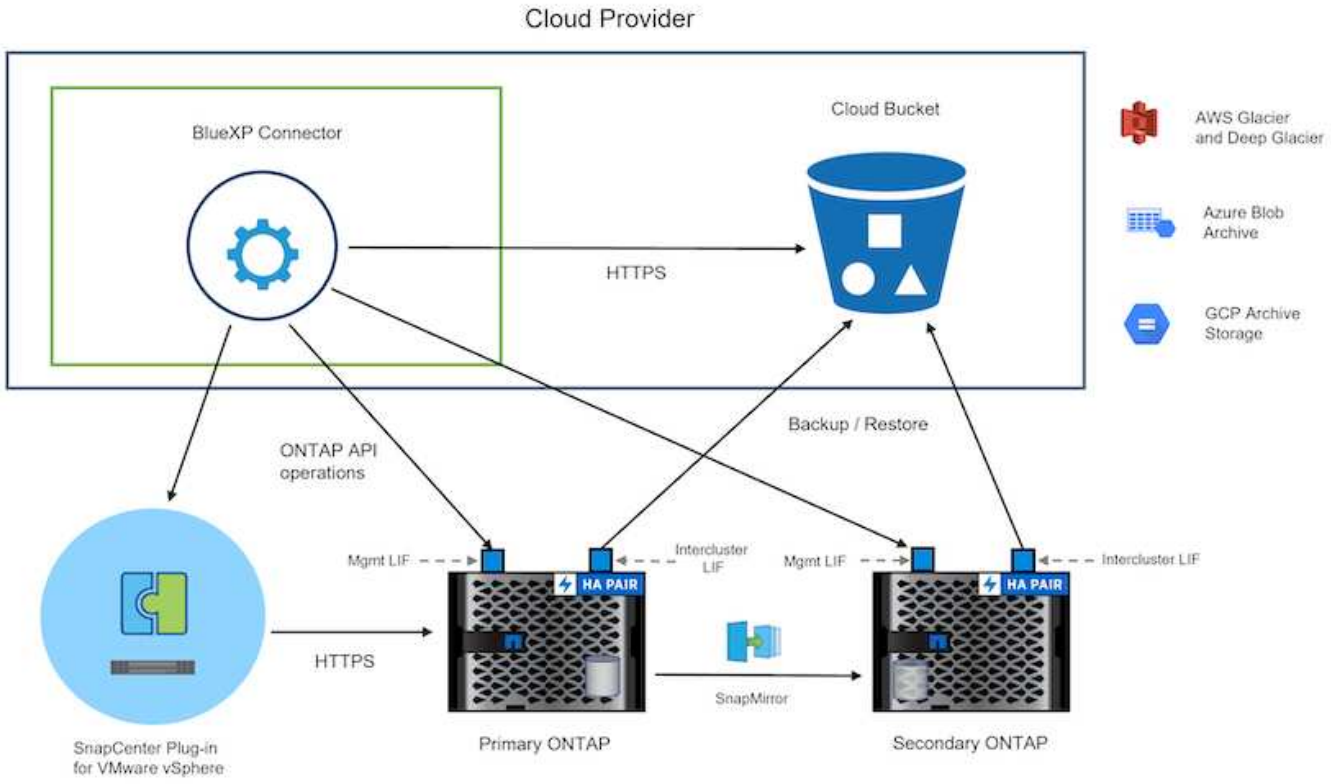
前提条件

このソリューションの目的は、VMware vSphere で実行され、 NetApp ONTAPによってホストされる NFS データストアに配置されている仮想マシンのデータ保護を実証することです。このソリューションでは、次のコンポーネントが構成され、使用できる状態になっていることを前提としています。

1. VMware vSphere に接続された NFS または VMFS データストアを備えたONTAPストレージ クラスター。 NFS と VMFS の両方のデータストアがサポートされています。このソリューションでは NFS データストアが利用されました。
2. NFS データストアに使用されるボリュームに対してSnapMirror関係が確立されたセカンダリONTAP ストレージ クラスタ。
3. オブジェクト ストレージ バックアップに使用されるクラウド プロバイダー用にBlueXPコネクタがインストールされています。
4. バックアップされる仮想マシンは、プライマリONTAPストレージ クラスタにある NFS データストア上にあります。
5. BlueXPコネクタとオンプレミスのONTAPストレージ クラスタ管理インターフェイス間のネットワーク接続。
6. BlueXPコネクタとオンプレミスの SCV アプライアンス VM 間、およびBlueXPコネクタと vCenter 間のネットワーク接続。
7. オンプレミスのONTAPクラスタ間 LIF とオブジェクト ストレージ サービス間のネットワーク接続。
8. プライマリおよびセカンダリONTAPストレージ クラスタ上の管理 SVM 用に設定された DNS。詳細については、 "ホスト名解決に使用するDNSの設定" 。

高レベルアーキテクチャ

このソリューションのテスト/検証は、最終的な展開環境と一致する場合も一致しない場合もあるラボで実行されました。



ソリューションの展開

このソリューションでは、オンプレミス データ センターにある VMware vSphere クラスター内の Windows および Linux 仮想マシンのバックアップとリカバリを実行するために、 SnapCenter Plug-in for VMware vSphereとBlueXP backup and recoveryを利用するソリューションを展開および検証するための詳細な手順を示します。このセットアップの仮想マシンは、 ONTAP A300 ストレージ クラスタによってホストされる NFS データストアに保存されます。さらに、別のONTAP A300 ストレージ クラスタは、 SnapMirrorを使用して複製されたボリュームのセカンダリ デスティネーションとして機能します。さらに、Amazon Web Services と Azure Blob でホストされているオブジェクト ストレージが、データの 3 番目のコピーのターゲットとして使用されました。

SCV によって管理されるバックアップのセカンダリ コピーのSnapMirror関係の作成と、SCV とBlueXP backup and recoveryの両方でのバックアップ ジョブの構成について説明します。

SnapCenter Plug-in for VMware vSphereの詳細については、 "SnapCenter Plug-in for VMware vSphereのドキュメント" 。

BlueXP backup and recoveryの詳細については、 "BlueXP backup and recoveryドキュメント" 。

ONTAPクラスタ間のSnapMirror関係を確立する

SnapCenter Plug-in for VMware vSphereは、 ONTAP SnapMirrorテクノロジを使用して、セカンダリSnapMirrorおよび/またはSnapVaultコピーのセカンダリONTAPクラスタへの転送を管理します。

SCV バックアップ ポリシーには、 SnapMirrorまたはSnapVault関係を使用するオプションがあります。主な違いは、 SnapMirrorオプションを使用する場合、ポリシーでバックアップ用に構成された保持スケジュールがプライマリ ロケーションとセカンダリ ロケーションで同じになることです。 SnapVaultはアーカイブ用に設計されており、このオプションを使用すると、セカンダリONTAPストレージ クラスタ上のスナップショッ

ト コピーに対してSnapMirror関係を使用して個別の保持スケジュールを確立できます。

SnapMirror関係の設定は、多くの手順が自動化されているBlueXPで実行することも、System ManagerとONTAP CLI を使用して実行することもできます。これらすべての方法について以下で説明します。

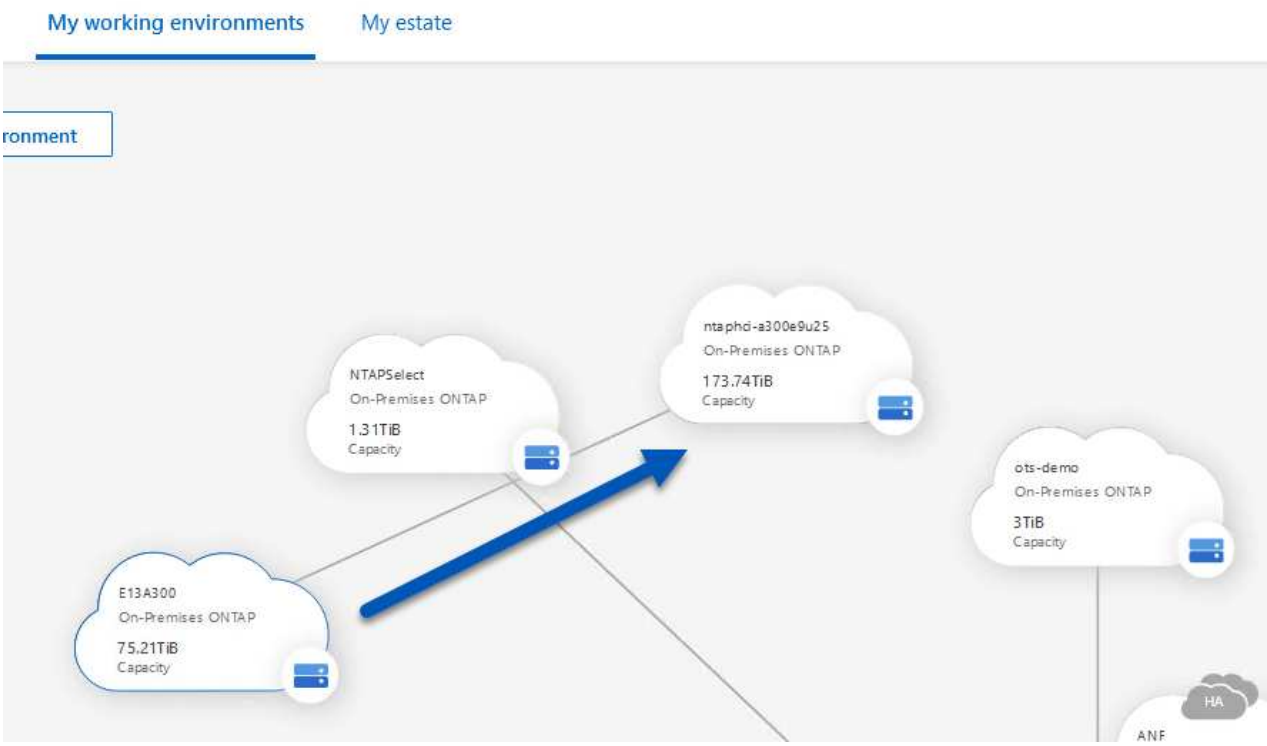
BlueXPと**SnapMirror**関係を確立する

BlueXP Web コンソールから次の手順を完了する必要があります。

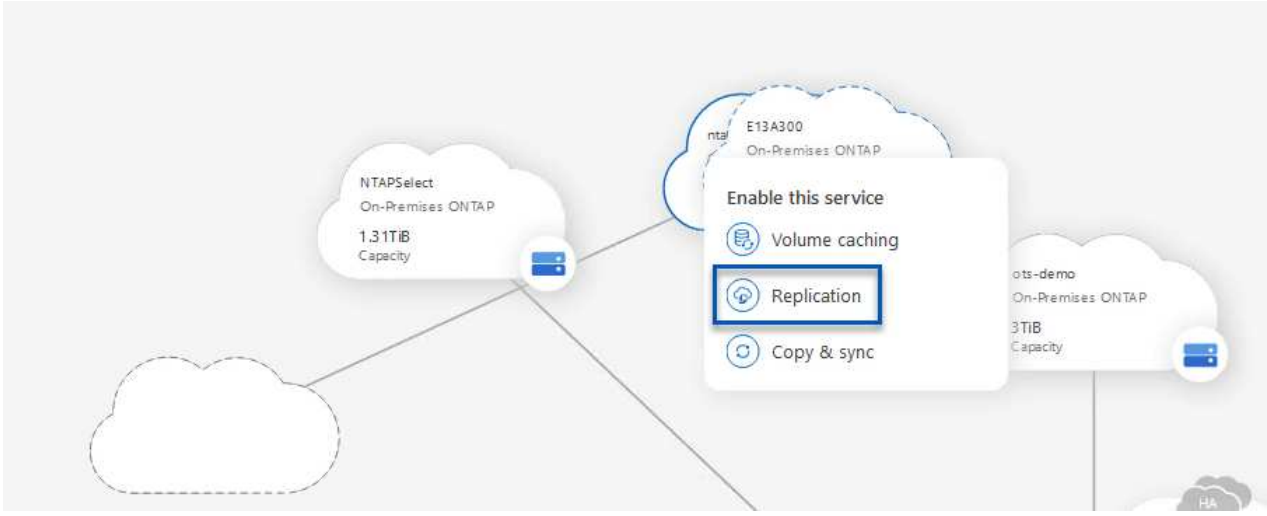
プライマリおよびセカンダリ**ONTAP**ストレージ システムのレプリケーション設定

まず、 BlueXP Web コンソールにログインし、Canvas に移動します。

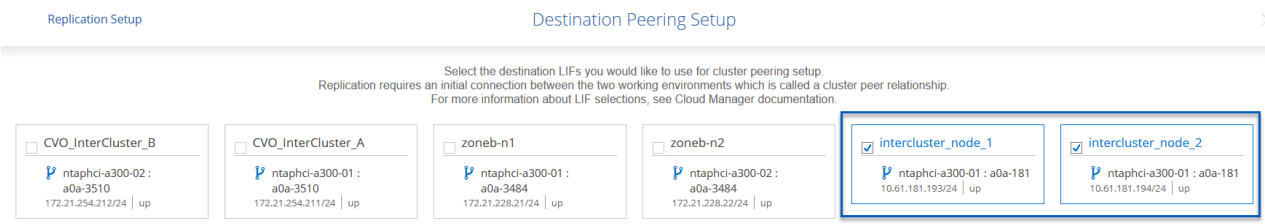
1. ソース (プライマリ) ONTAPストレージ システムを、宛先 (セカンダリ) ONTAPストレージ システムにドラッグ アンド ドロップします。



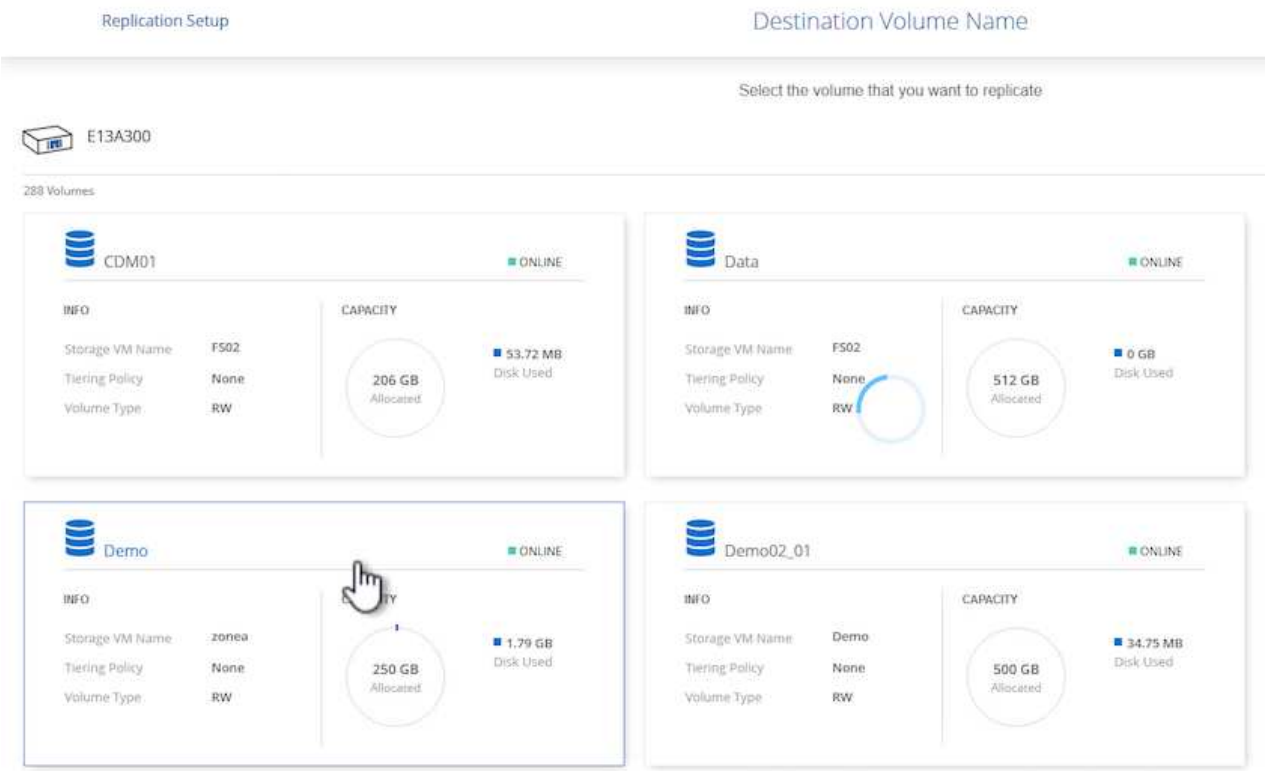
2. 表示されるメニューから*レプリケーション*を選択します。



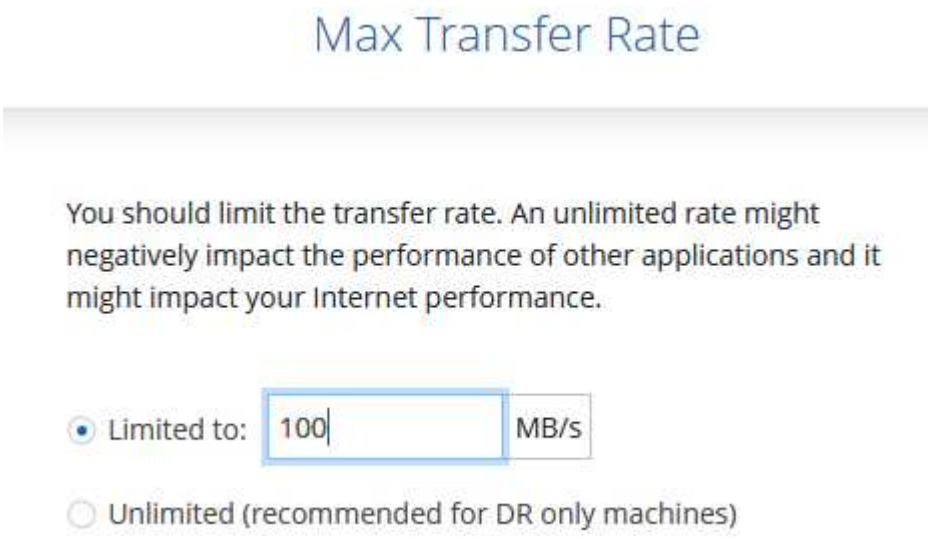
3. 宛先ピアリング設定 ページで、ストレージ システム間の接続に使用する宛先クラスタ間 LIF を選択します。



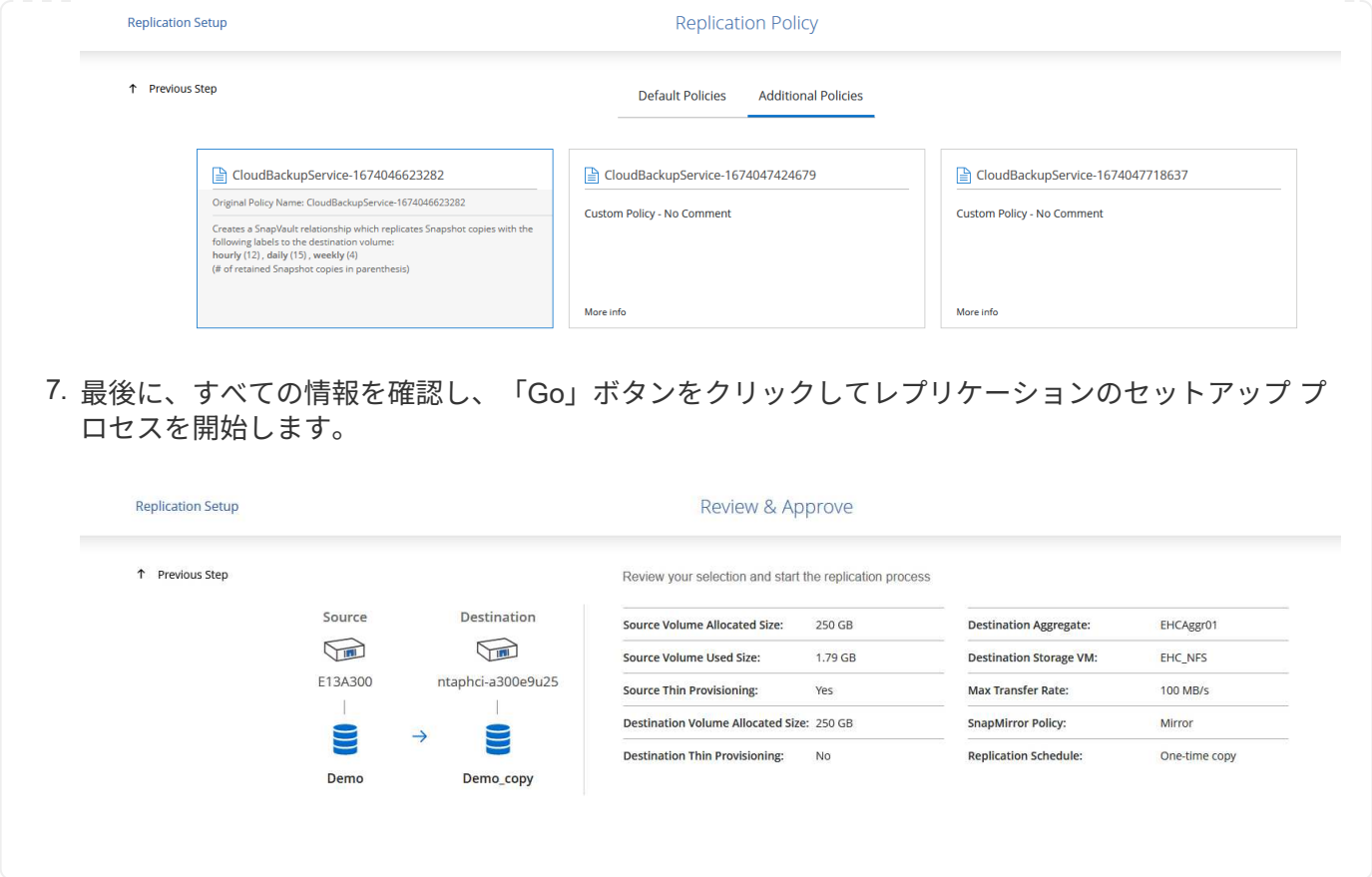
4. 宛先ボリューム名 ページで、最初にソース ボリュームを選択し、次に宛先ボリューム名を入力して、宛先 SVM とアグリゲートを選択します。続行するには、[次へ] をクリックします。



5. レプリケーションを実行するための最大転送速度を選択します。



6. セカンダリ バックアップの保持スケジュールを決定するポリシーを選択します。このポリシーは事前に作成することも (以下の「スナップショット保持ポリシーの作成」手順の手動プロセスを参照)、必要に応じて事後に変更することもできます。



7. 最後に、すべての情報を確認し、「Go」ボタンをクリックしてレプリケーションのセットアップ プロセスを開始します。

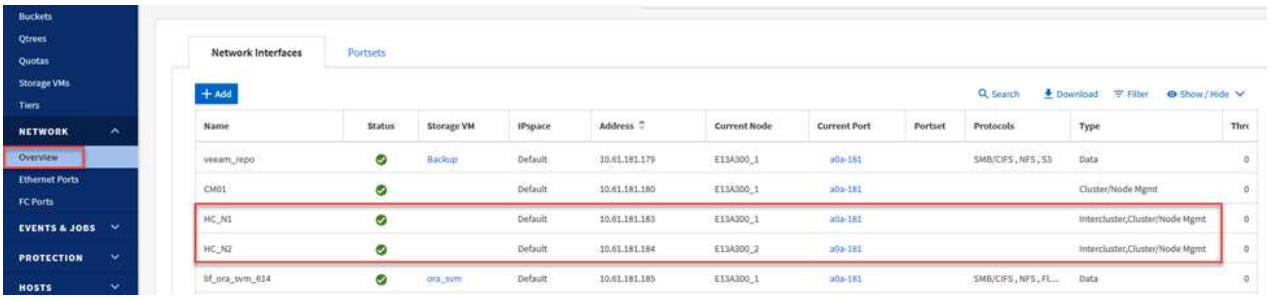
System ManagerとONTAP CLIを使用してSnapMirror関係を確立する

SnapMirror関係を確立するために必要なすべての手順は、System Manager またはONTAP CLI を使用して実行できます。次のセクションでは、両方の方法について詳細な情報を提供します。

送信元と宛先のクラスタ間論理インターフェースを記録する

ソースおよびデスティネーションのONTAPクラスタについては、System Manager または CLI からクラスタ間 LIF 情報を取得できます。

1. ONTAP System Manager で、[ネットワークの概要] ページに移動し、FSx がインストールされている AWS VPC と通信するように設定されているタイプ: クラスタ間の IP アドレスを取得します。



2. CLI を使用してクラスタ間 IP アドレスを取得するには、次のコマンドを実行します。

```
ONTAP-Dest::> network interface show -role intercluster
```

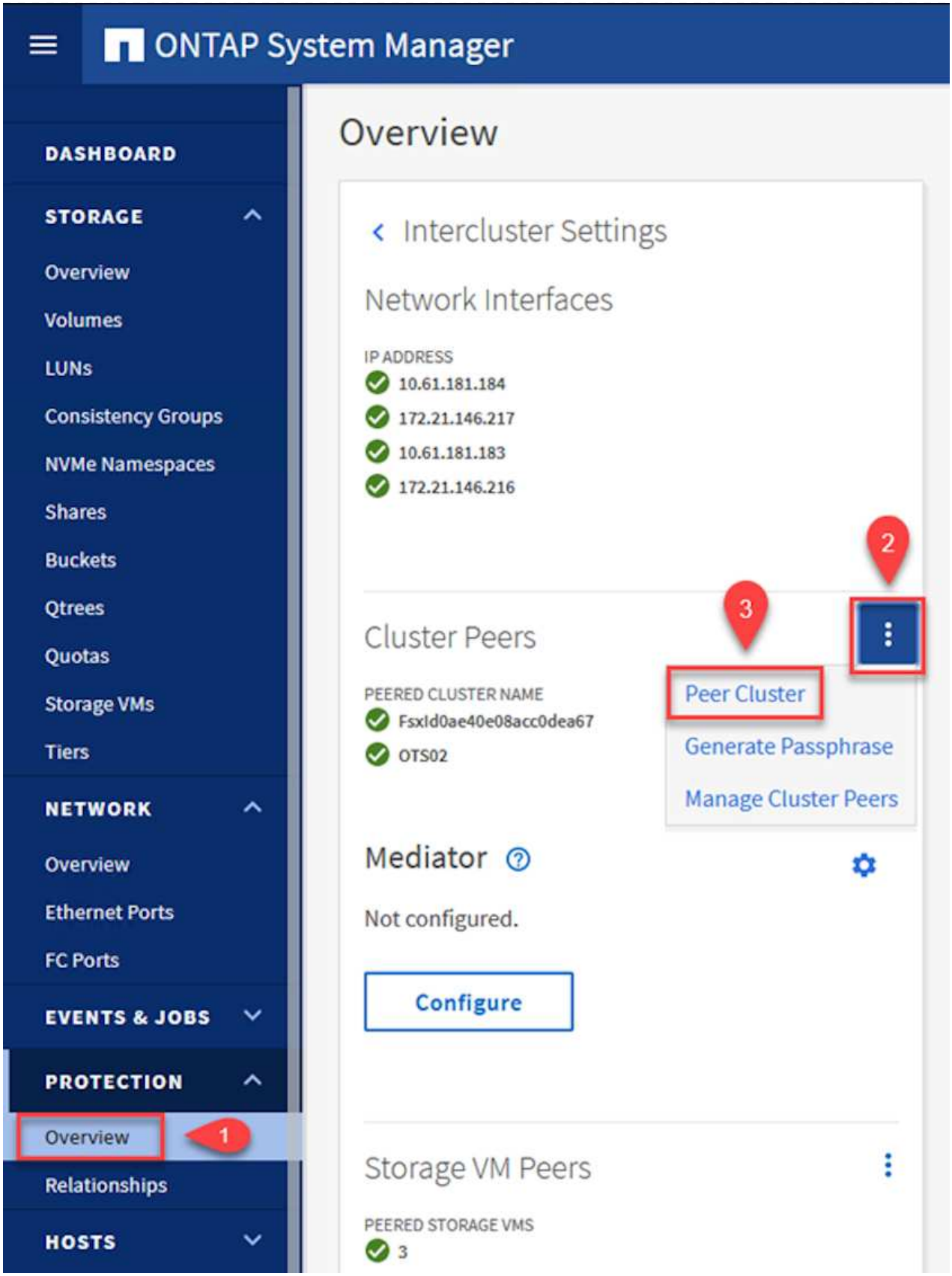
ONTAPクラスタ間のクラスタピアリングを確立する

ONTAPクラスタ間のクラスタ ピアリングを確立するには、開始側のONTAPクラスタで入力した一意のパスフレーズを、他のピア クラスタで確認する必要があります。

1. 宛先ONTAPクラスタでピアリングを設定するには、 `cluster peer create`指示。プロンプトが表示されたら、後でソース クラスターで作成プロセスを完了するために使用する一意のパスフレーズを入力します。

```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. ソース クラスタでは、 ONTAP System Manager または CLI を使用してクラスタ ピア関係を確立できます。 ONTAP System Manager から、[Protection] > [Overview] に移動し、[Peer Cluster] を選択します。

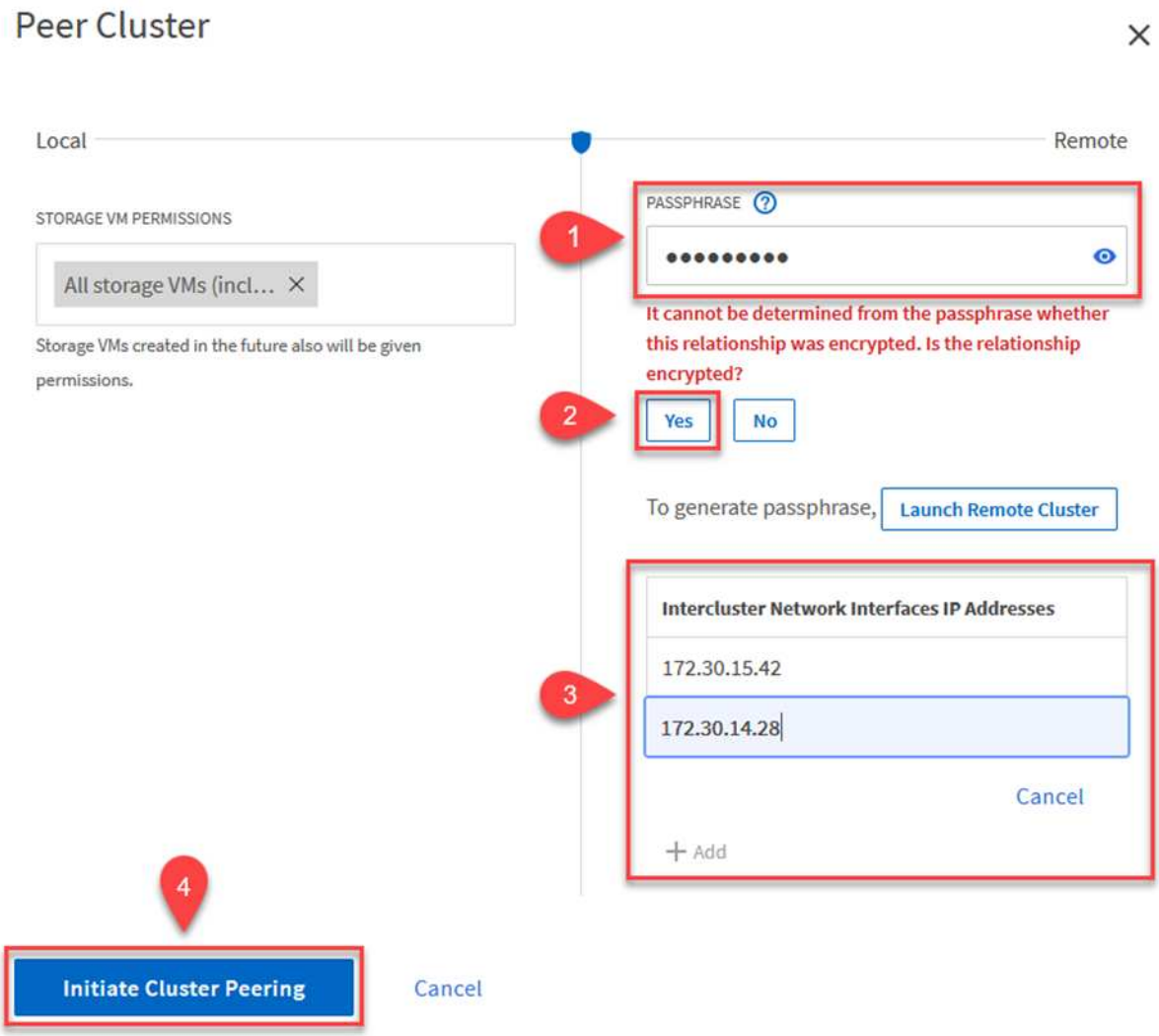


3. [ピア クラスター] ダイアログ ボックスで、必要な情報を入力します。
   a. 宛先ONTAPクラスタでピア クラスタ関係を確立するために使用されたパスフレーズを入力します。

b. 選択 `Yes`暗号化された関係を確立します。

c. 宛先ONTAPクラスタのクラスタ間 LIF IP アドレスを入力します。

d. プロセスを終了するには、「クラスター ピアリングの開始」をクリックします。



4. 次のコマンドを使用して、宛先ONTAPクラスタからクラスタ ピア関係のステータスを確認します。

```
ONTAP-Dest::> cluster peer show
```

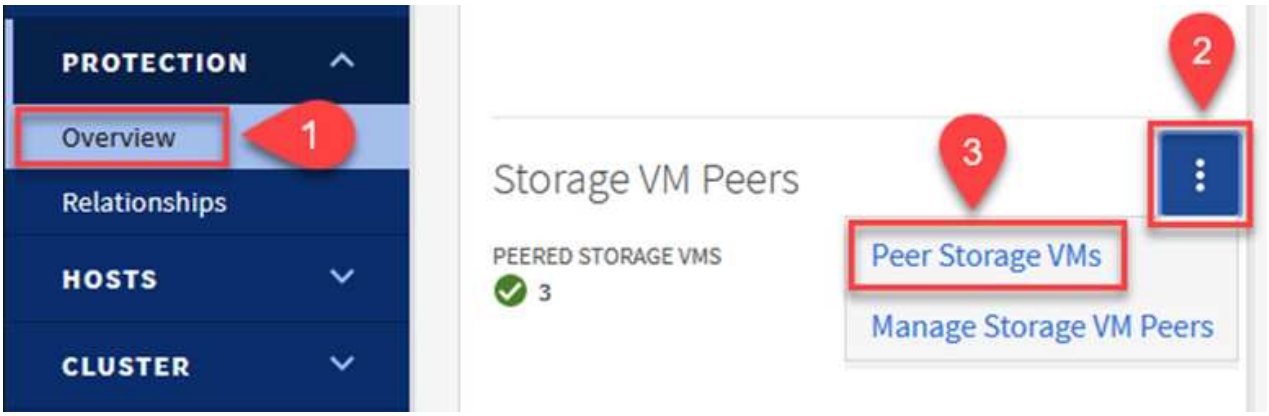
SVMピアリング関係を確立する

次の手順では、 SnapMirror関係になるボリュームを含む宛先ストレージ仮想マシンとソース ストレージ仮想マシン間の SVM 関係を設定します。

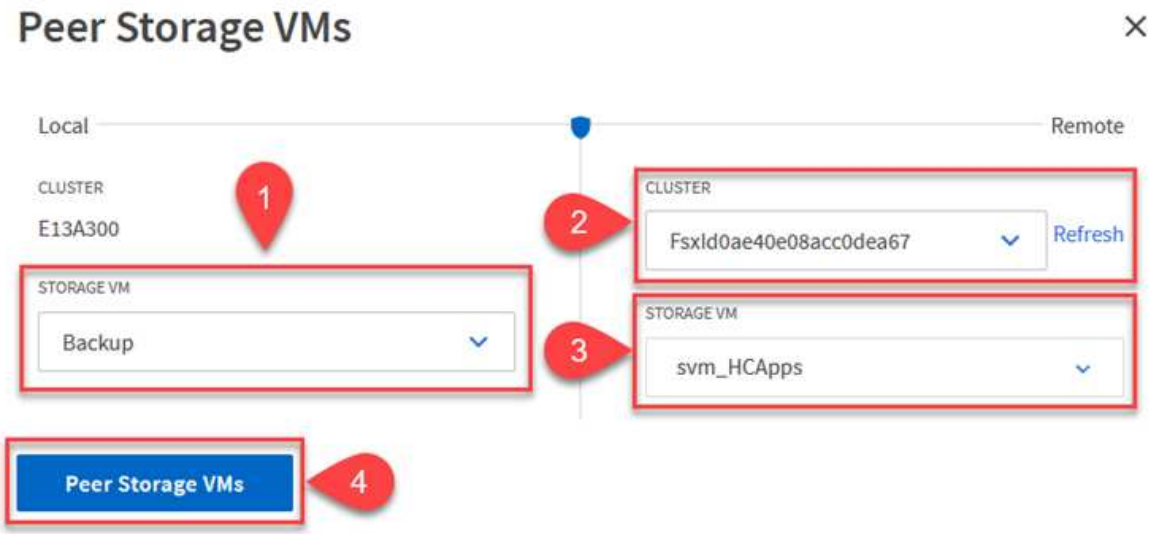
1. 宛先ONTAPクラスタから、CLI から次のコマンドを使用して SVM ピア関係を作成します。

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. ソースONTAPクラスタから、 ONTAP System Manager または CLI のいずれかを使用してピアリング関係を受け入れます。
3. ONTAP System Manager から、[Protection] > [Overview] に移動し、[Storage VM Peers] の下の [Peer Storage VMs] を選択します。



4. ピア ストレージ VM のダイアログ ボックスで、必須フィールドに入力します。
   - ソースストレージVM
   - 宛先クラスター
   - 宛先ストレージVM



5. SVM ピアリング プロセスを完了するには、[ピア ストレージ VM] をクリックします。

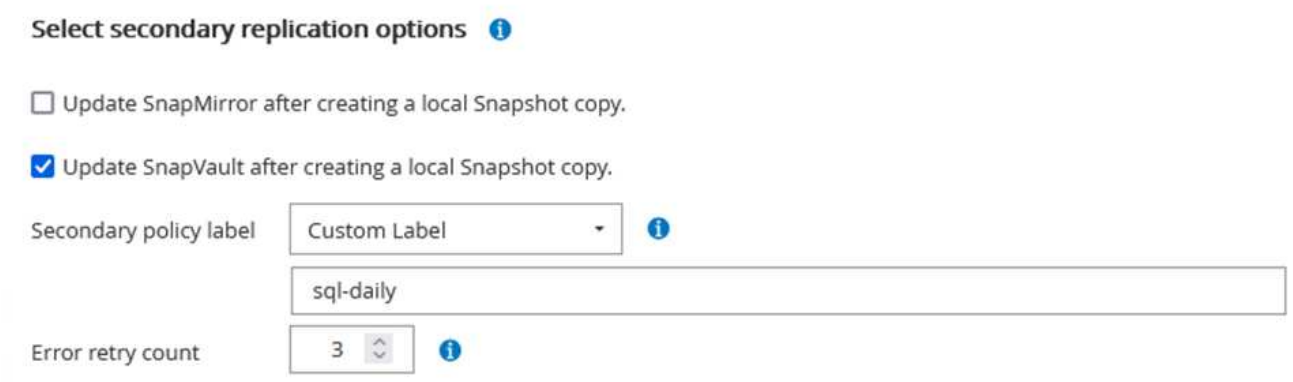
スナップショット保持ポリシーを作成する

SnapCenter は、プライマリ ストレージ システム上にスナップショット コピーとして存在するバックアップの保持スケジュールを管理します。これは、 SnapCenterでポリシーを作成するときに確立されます。 SnapCenter は、セカンダリ ストレージ システムに保持されるバックアップの保持ポリシーを管理しません。これらのポリシーは、セカンダリ FSx クラスター上に作成され、ソース ボリュームとSnapMirror関係にある宛先ボリュームに関連付けられたSnapMirrorポリシーを通じて個別に管理されます。

SnapCenterポリシーを作成するときに、 SnapCenterバックアップの作成時に生成される各スナップショットのSnapMirrorラベルに追加されるセカンダリ ポリシー ラベルを指定するオプションがあります。

> セカンダリ ストレージでは、これらのラベルは、スナップショットの保持を強制する目的で、宛先ボリュームに関連付けられたポリシー ルールと照合されます。

次の例は、SQL Server データベースとログ ボリュームの毎日のバックアップに使用されるポリシーの一部として生成されたすべてのスナップショットに存在するSnapMirrorラベルを示しています。



SQL Serverデータベース用のSnapCenterポリシーの作成の詳細については、 "SnapCenterのドキュメント" 。

まず、保持するスナップショット コピーの数を指定するルールを含むSnapMirrorポリシーを作成する必要があります。

1. FSx クラスターにSnapMirrorポリシーを作成します。

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. SnapCenterポリシーで指定されたセカンダリ ポリシー ラベルと一致するSnapMirrorラベルを使用して、ポリシーにルールを追加します。

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

次のスクリプトは、ポリシーに追加できるルールの例を示しています。

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest
-policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

各SnapMirrorラベルと保持するスナップショットの数 (保持期間) に対して追加のルールを作成します。

宛先ボリュームを作成する

ソース ボリュームからのスナップショット コピーの受信者となる宛先ボリュームをONTAP上に作成するには、宛先ONTAPクラスターで次のコマンドを実行します。

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

ソースボリュームと宛先ボリューム間の**SnapMirror**関係を作成する

ソース ボリュームと宛先ボリュームの間にSnapMirror関係を作成するには、宛先ONTAPクラスタで次のコマンドを実行します。

```
ONTAP-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

SnapMirror関係を初期化する

SnapMirror関係を初期化します。このプロセスは、ソース ボリュームから生成された新しいスナップショットを開始し、それを宛先ボリュームにコピーします。

ボリュームを作成するには、宛先のONTAPクラスターで次のコマンドを実行します。

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

SnapCenter Plug-in for VMware vSphereを構成する

インストールが完了すると、vCenter Server Appliance 管理インターフェイスからSnapCenter Plug-in for VMware vSphereにアクセスできるようになります。 SCV は、ESXi ホストにマウントされ、Windows および Linux VM を含む NFS データストアのバックアップを管理します。

レビュー "データ保護のワークフロー"バックアップの構成手順の詳細については、SCV ドキュメントのセクションを参照してください。

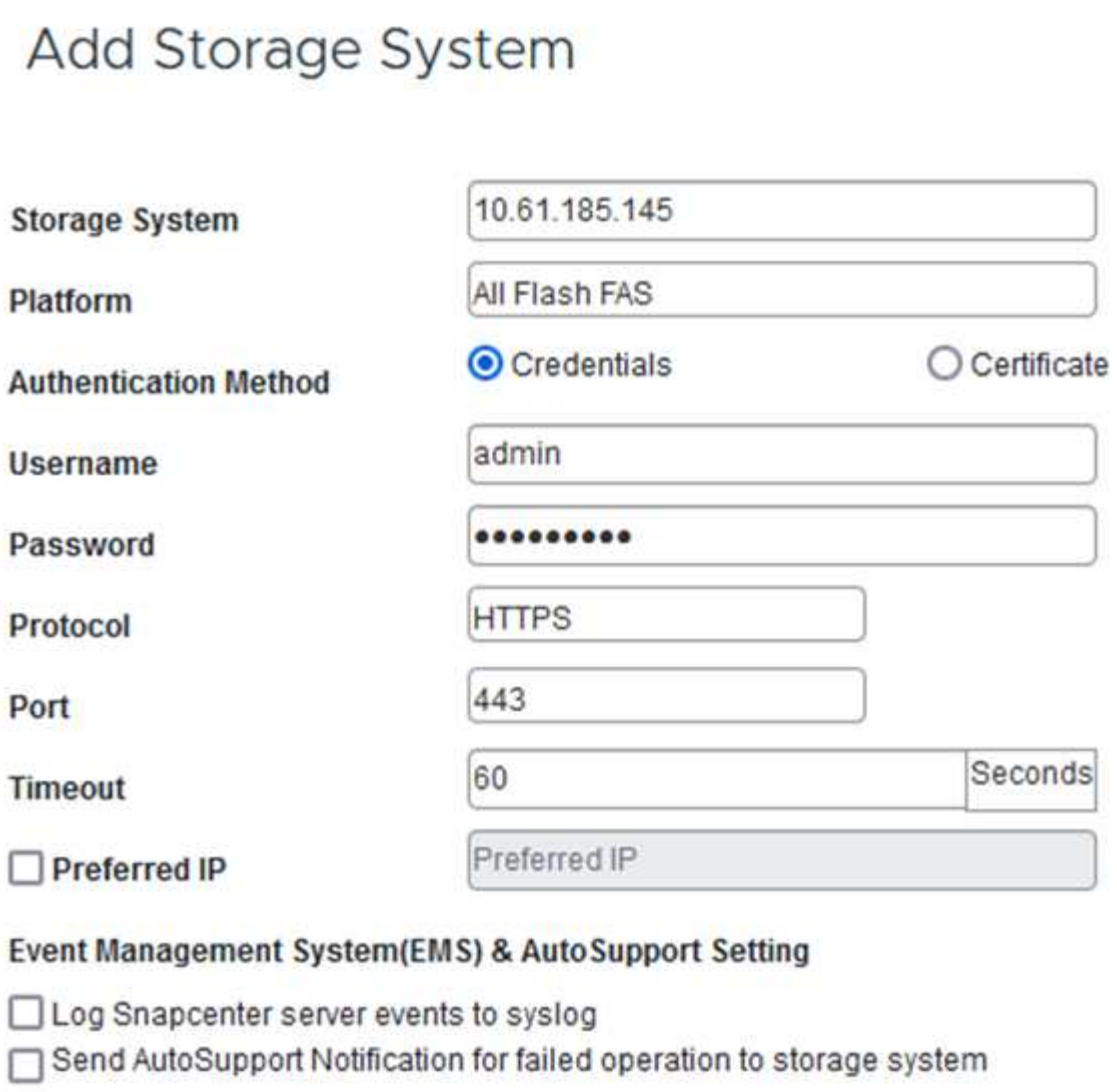
仮想マシンとデータストアのバックアップを構成するには、プラグイン インターフェイスから次の手順を完了する必要があります。

Discovery ONTAPストレージシステム

プライマリ バックアップとセカンダリ バックアップの両方に使用されるONTAPストレージ クラスターを検出します。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの ストレージ システム に移動し、追加ボタンをクリックします。

2. プライマリONTAPストレージ システムの資格情報とプラットフォーム タイプを入力し、[追加] をクリックします。



3. セカンダリONTAPストレージ システムに対してこの手順を繰り返します。

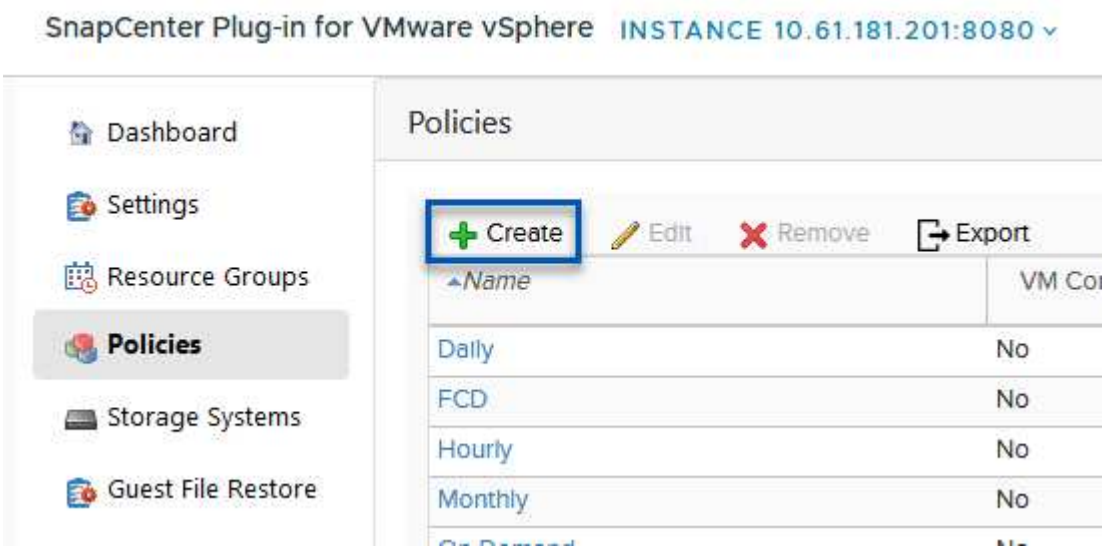
SCVバックアップポリシーを作成する

ポリシーは、SCV によって管理されるバックアップの保持期間、頻度、およびレプリケーション オプションを指定します。

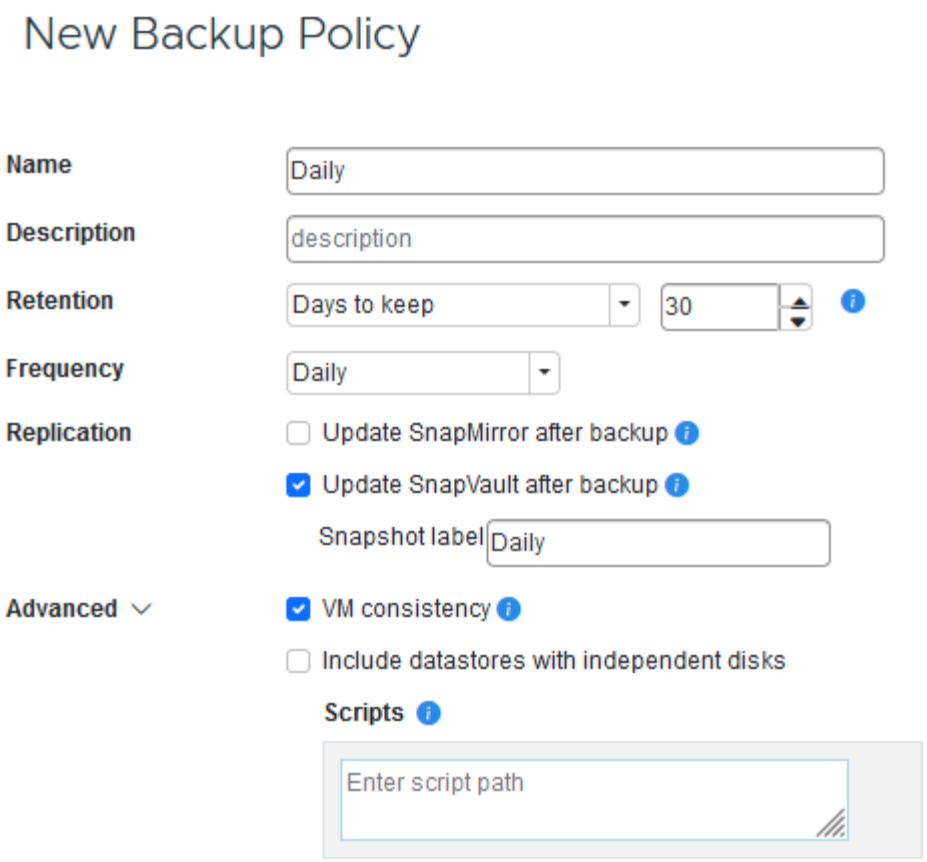
レビュー "VMとデータストアのバックアップ ポリシーの作成"詳細については、ドキュメントのセクションを参照してください。

バックアップ ポリシーを作成するには、次の手順を実行します。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの ポリシー に移動し、作成 ボタンをクリックします。



2. ポリシーの名前、保持期間、頻度とレプリケーションのオプション、スナップショット ラベルを指定します。



SnapCenterプラグインでポリシーを作成すると、 SnapMirrorとSnapVaultのオプションが表示されます。 SnapMirrorを選択した場合、ポリシーで指定された保持スケジュールはプライマリ スナップショットとセカンダリ スナップショットの両方で同じになります。 SnapVaultを選択した場合、セカンダリ スナップショットの保持スケジュールは、 SnapMirror関係で実装された別のスケジュールに基づいて決定されます。これは、セカンダリ バックアップの保持期間を長くしたい場合に便利です。

スナップショット ラベルは、セカンダリONTAPクラスタに複製されたSnapVaultコピーに対して特定の保持期間を設定したポリシーを適用するために使用できるため便利です。 SCV をBlueXPバックアップおよびリストアで使用する場合、スナップショット ラベル フィールドは空白にするか、 BlueXPバックアップ ポリシーで指定されたラベルと 一致 する必要があります。

3. 必要なポリシーごとにこの手順を繰り返します。たとえば、毎日、毎週、毎月のバックアップに個別のポリシーを設定します。

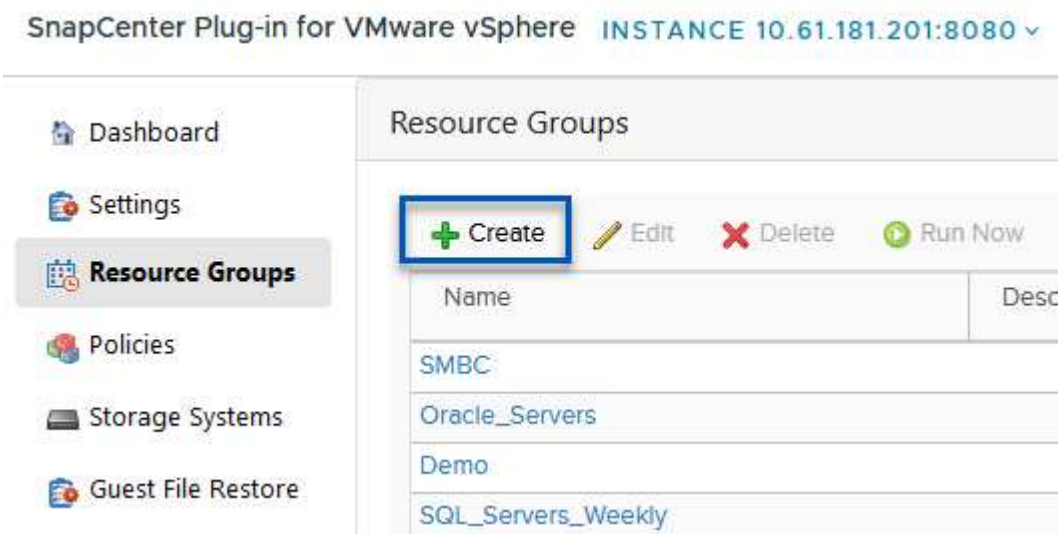
リソース グループの作成

リソース グループには、バックアップ ジョブに含めるデータストアと仮想マシン、および関連するポリシーとバックアップ スケジュールが含まれます。

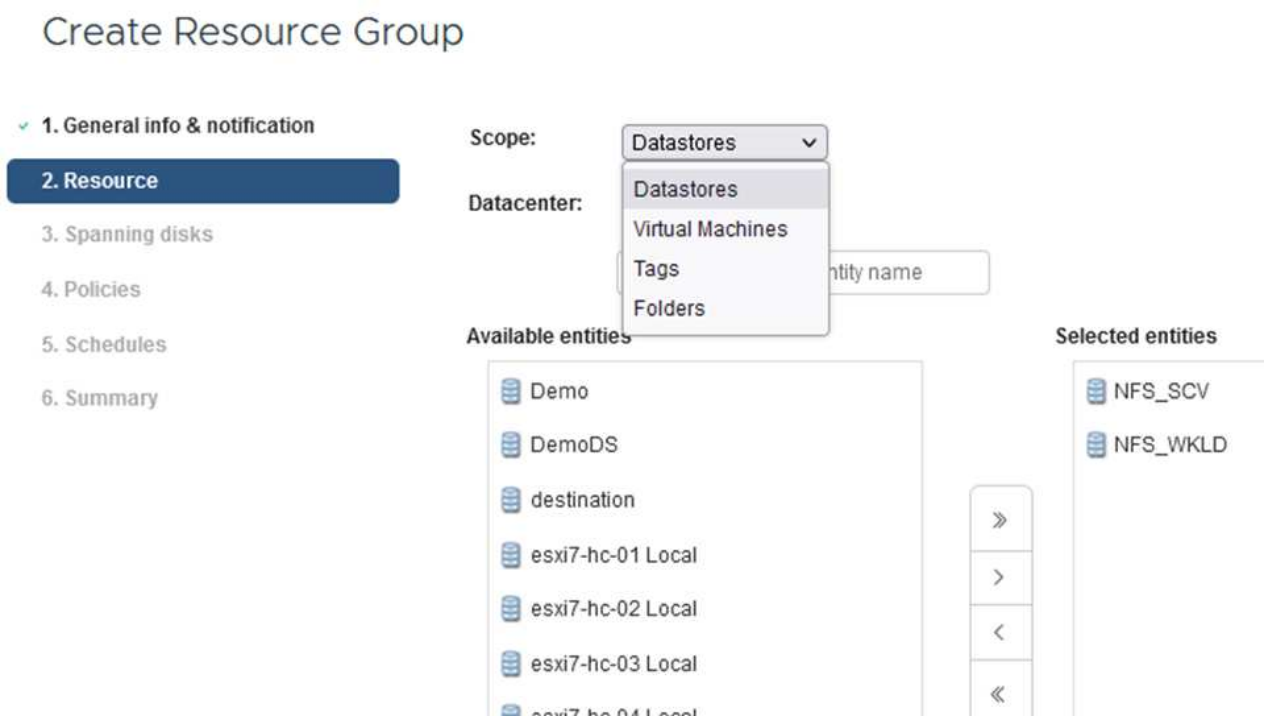
レビュー "リソース グループの作成"詳細については、ドキュメントのセクションを参照してください。

リソース グループを作成するには、次の手順を実行します。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの リソース グループ に移動し、作成ボタンをクリックします。

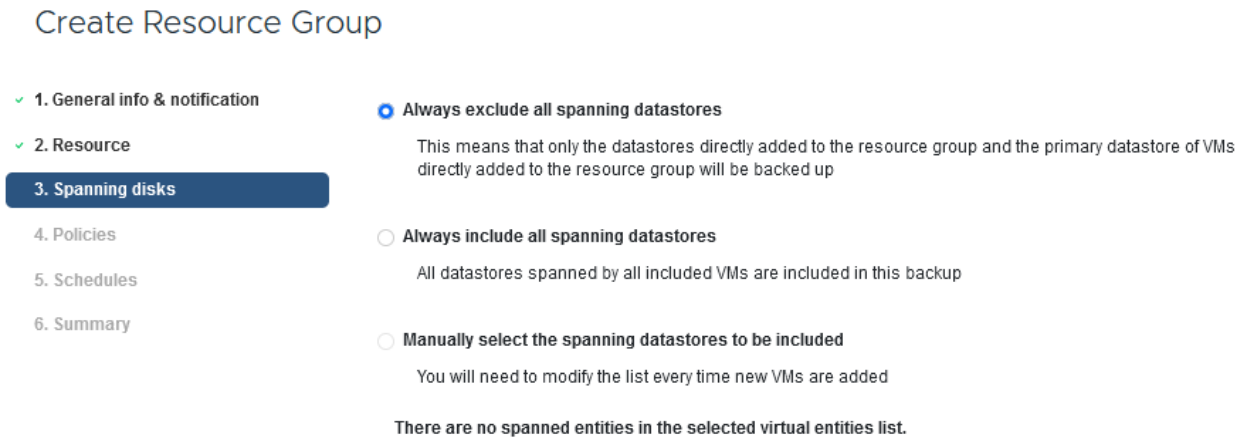


2. リソース グループの作成ウィザードで、グループの名前と説明、および通知を受信するために必要な情報を入力します。 「次へ」をクリックします
3. 次のページで、バックアップ ジョブに含めるデータストアと仮想マシンを選択し、[次へ] をクリックします。



特定の VM またはデータストア全体を選択するオプションがあります。どちらを選択した場合でも、バックアップは基礎となるボリュームのスナップショットを取得した結果であるため、ボリューム全体 (およびデータストア) がバックアップされます。ほとんどの場合、データストア全体を選択するのが最も簡単です。ただし、復元時に使用可能な VM のリストを制限する場合は、バックアップ対象として VM のサブセットのみを選択できます。

4. 複数のデータストアに存在する VMDK を持つ VM のデータストアをまたぐためのオプションを選択し、[次へ] をクリックします。

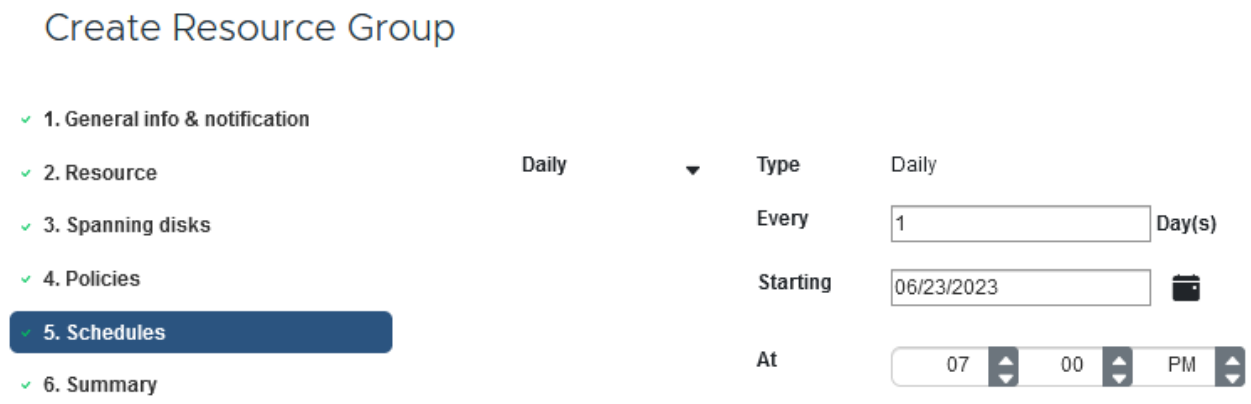


BlueXP backup and recoveryでは、現在、複数のデータストアにまたがる VMDK を持つ VM のバックアップはサポートされていません。

5. 次のページで、リソース グループに関連付けるポリシーを選択し、[次へ] をクリックします。

BlueXP backup and recoveryを使用して SCV 管理スナップショットをオブジェクトストレージにバックアップする場合、各リソース グループは 1 つのポリシーにのみ関連付けることができます。

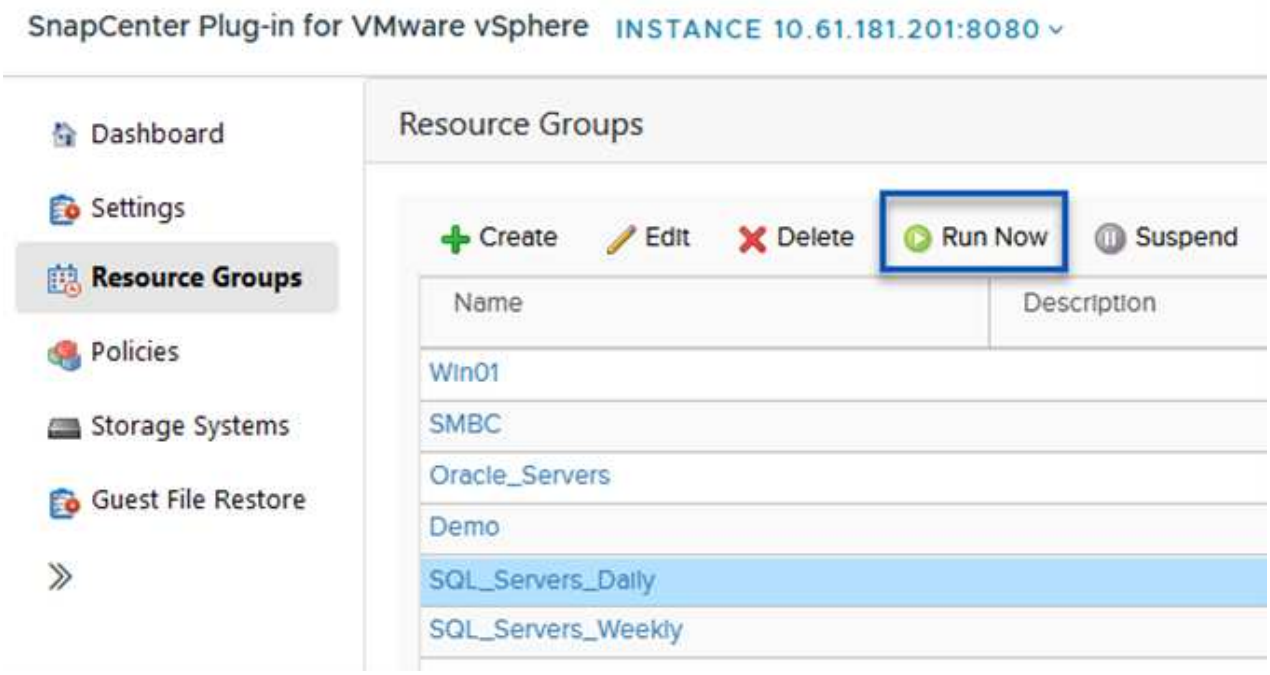
6. バックアップが実行される時刻を決定するスケジュールを選択します。 *次へ*をクリックします。



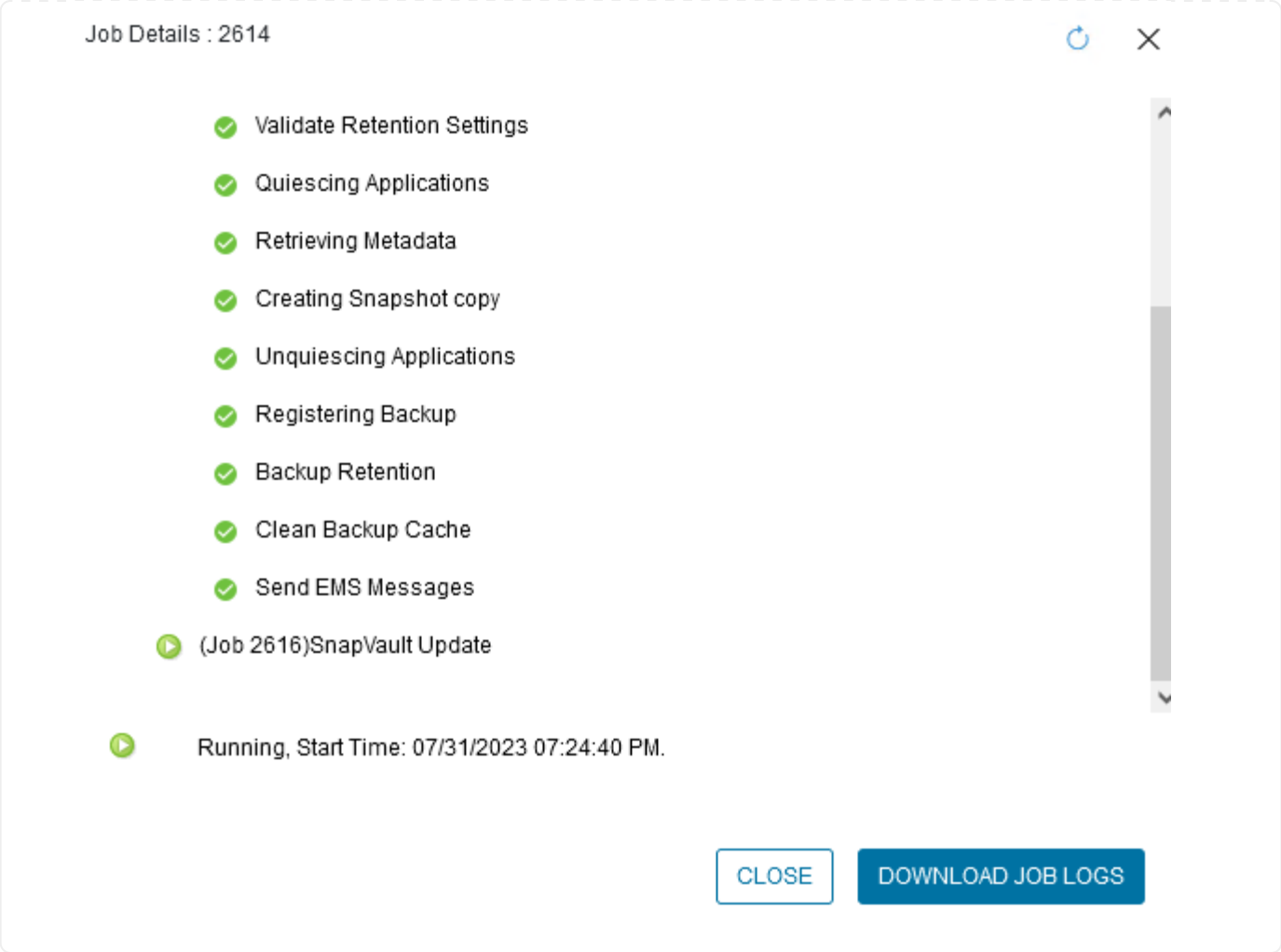
7. 最後に、概要ページを確認し、[完了] をクリックしてリソース グループの作成を完了します。

この最後のステップでは、バックアップ ジョブを実行し、その進行状況を監視します。 BlueXP backup and recoveryからリソースを検出する前に、SCV で少なくとも 1 つのバックアップ ジョブが正常に完了している必要があります。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの リソース グループ に移動します。
2. バックアップ ジョブを開始するには、目的のリソース グループを選択し、[今すぐ実行] ボタンをクリックします。



3. バックアップ ジョブを監視するには、左側のメニューの ダッシュボード に移動します。 最近のジョブアクティビティ の下でジョブ ID 番号をクリックして、ジョブの進行状況を監視します。



BlueXP backup and recoveryでオブジェクト ストレージへのバックアップを構成する

BlueXPがデータ インフラストラクチャを効果的に管理するには、事前にコネクタをインストールする必要があります。コネクタは、リソースの検出とデータ操作の管理に関連するアクションを実行します。

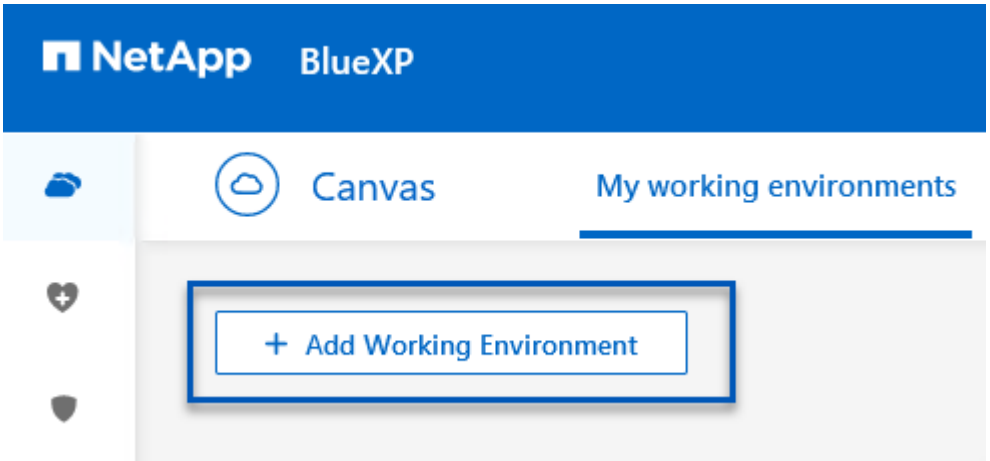
BlueXPコネクタの詳細については、以下を参照してください。 "コネクタについて学ぶ" BlueXPドキュメント内。

利用しているクラウド プロバイダーのコネクタがインストールされると、オブジェクト ストレージのグラフィック表現がキャンバスから表示できるようになります。

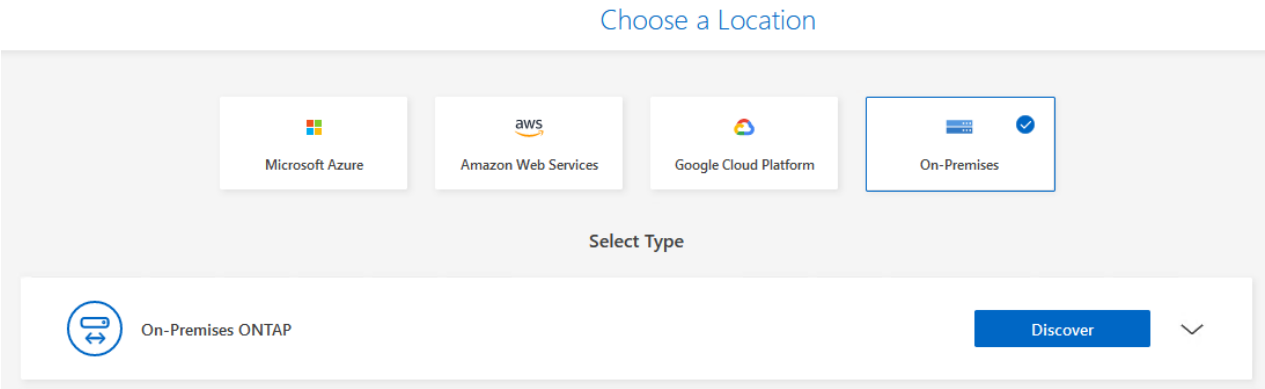
SCV オンプレミスで管理されるデータをバックアップするようにBlueXP backup and recoveryを構成するには、次の手順を実行します。

最初のステップは、オンプレミスのONTAPストレージシステムをBlueXPに追加することです。

1. キャンバスから「作業環境の追加」を選択して開始します。



2. 場所の選択肢から「オンプレミス」を選択し、「検出」ボタンをクリックします。



3. ONTAPストレージ システムの資格情報を入力し、[検出] ボタンをクリックして作業環境を追加します。

ONTAP Cluster IP

10.61.181.180

User Name

admin

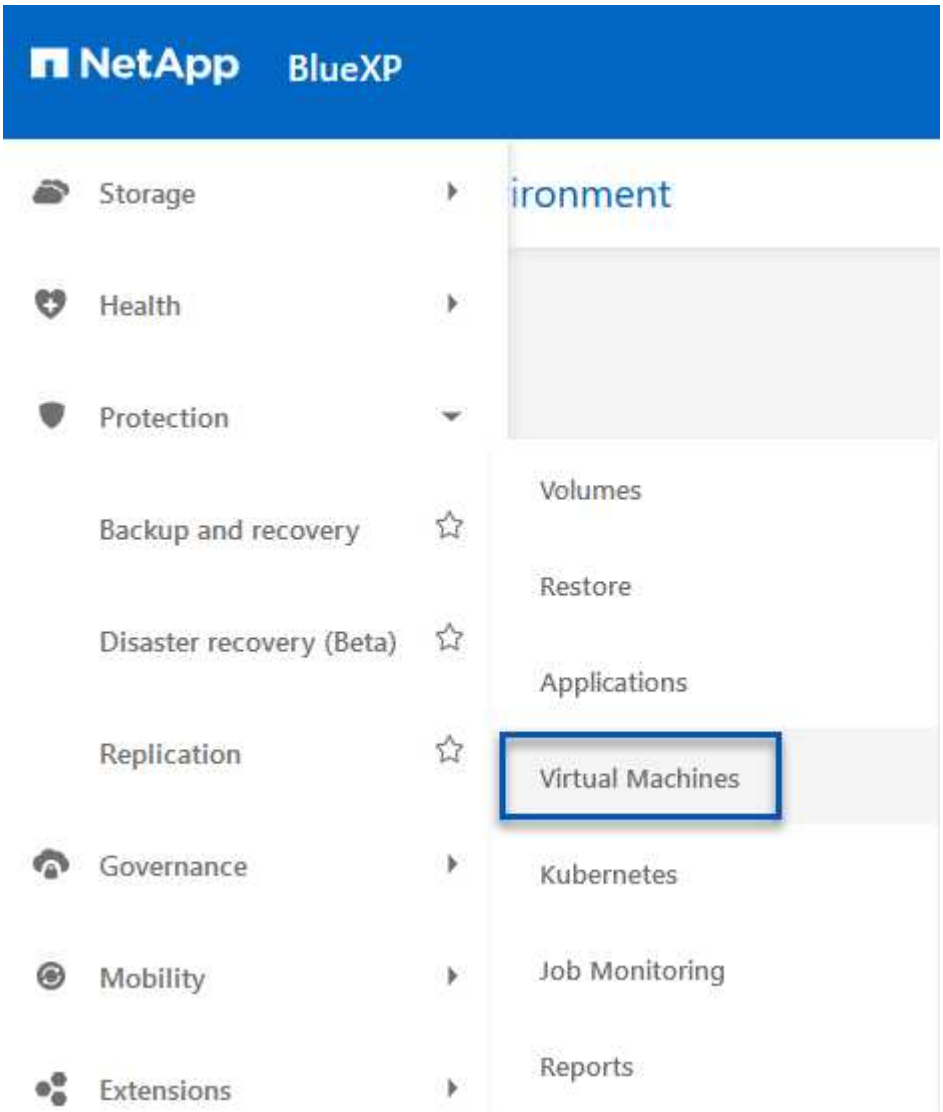
Password

••••••••••

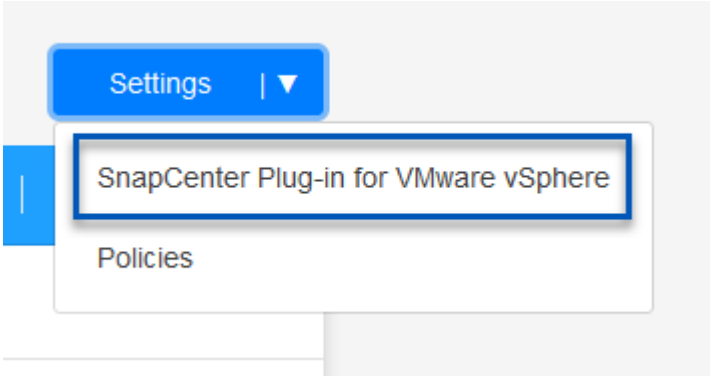
オンプレミスの **SCV** アプライアンスと **vCenter** の検出

オンプレミスのデータストアと仮想マシンのリソースを検出するには、SCV データ ブローカーの情報と vCenter 管理アプライアンスの資格情報を追加します。

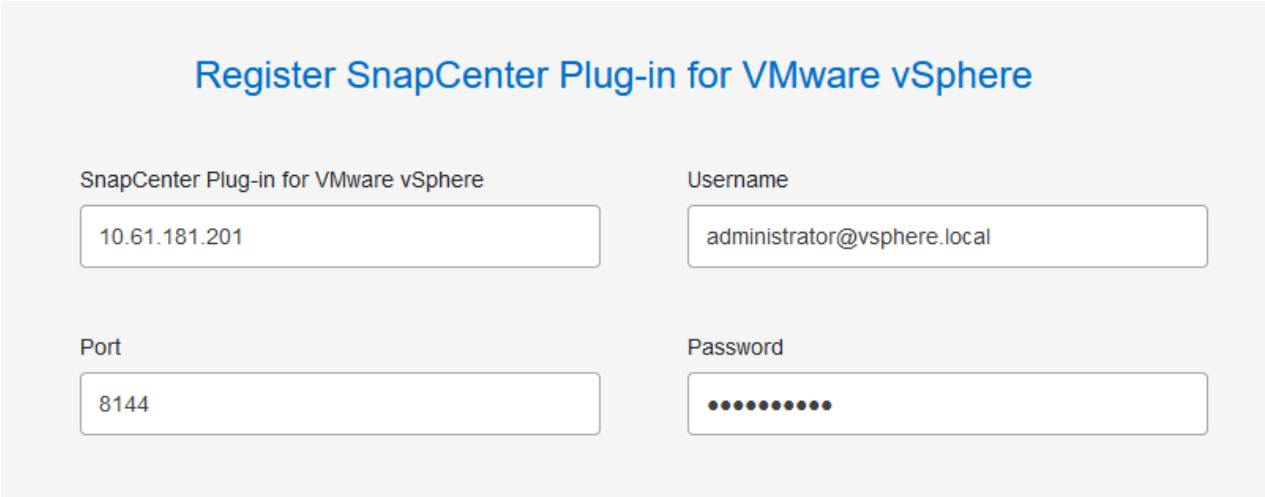
1. BlueXPの左側のメニューから*保護 > バックアップとリカバリ > 仮想マシン*を選択します。



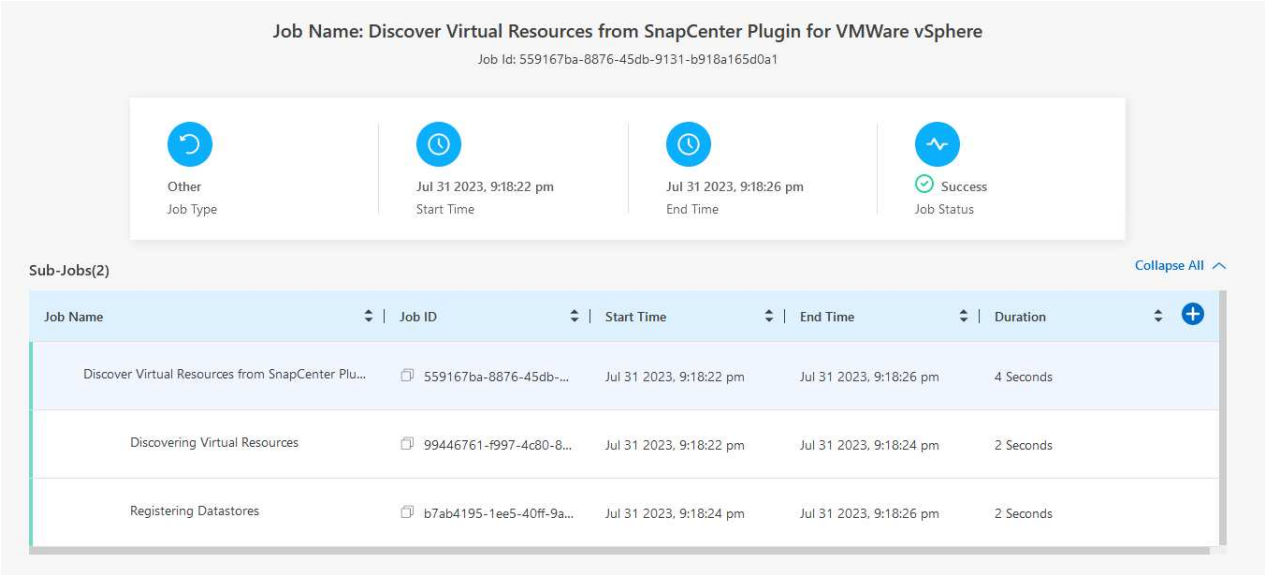
2. 仮想マシンのメイン画面から [設定] ドロップダウン メニューにアクセスし、[SnapCenter Plug-in for VMware vSphere] を選択します。



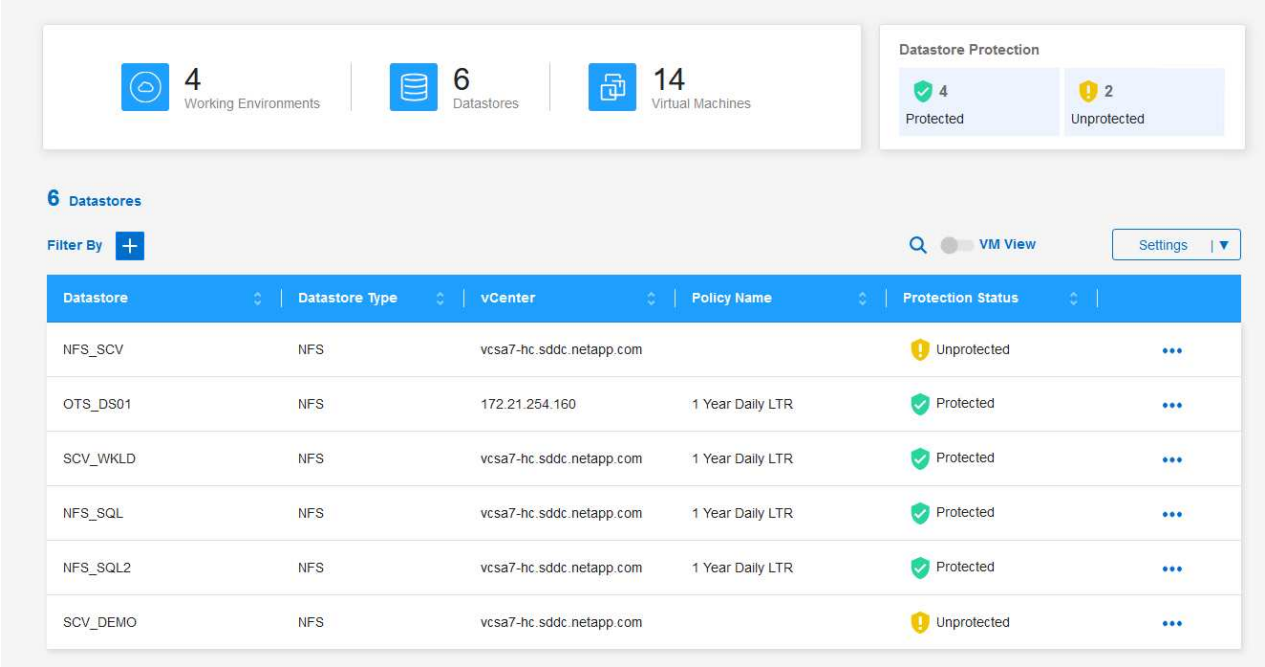
3. 登録 ボタンをクリックし、 SnapCenterプラグイン アプライアンスの IP アドレスとポート番号、および vCenter 管理アプライアンスのユーザー名とパスワードを入力します。検出プロセスを開始するには、[登録] ボタンをクリックします。



4. ジョブの進行状況は、「ジョブ監視」タブから監視できます。



5. 検出が完了すると、検出されたすべての SCV アプライアンスのデータストアと仮想マシンを表示できるようになります。

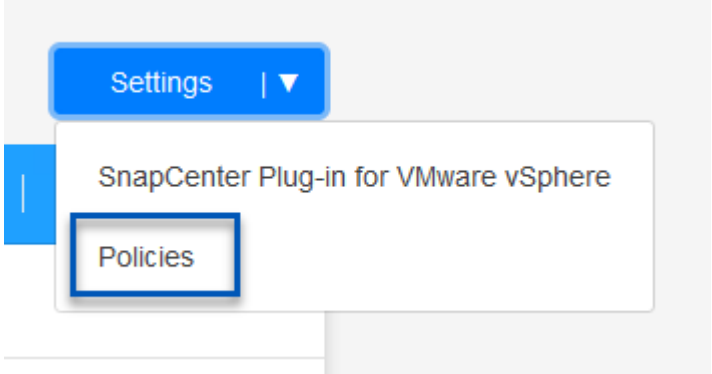

4
Working Environments
6
Datastores
14
Virtual Machines
Datastore Protection
4
Protected
2
Unprotected
6 Datastores
Filter By
VM View
Settings
Datastore
Datastore Type
vCenter
Policy Name
Protection Status
NFS_SCV NFS vcsa7-hc.sddc.netapp.com Unprotected
OTS_DS01 NFS 172.21.254.160 1 Year Daily LTR Protected
SCV_WKLD NFS vcsa7-hc.sddc.netapp.com 1 Year Daily LTR Protected
NFS_SQL NFS vcsa7-hc.sddc.netapp.com 1 Year Daily LTR Protected
NFS_SQL2 NFS vcsa7-hc.sddc.netapp.com 1 Year Daily LTR Protected
SCV_DEMO NFS vcsa7-hc.sddc.netapp.com Unprotected

BlueXPバックアップポリシーを作成する

仮想マシンのBlueXP backup and recoveryでは、保持期間、バックアップ ソース、アーカイブ ポリシーを指定するポリシーを作成します。

ポリシー作成の詳細については、以下を参照してください。 "データストアをバックアップするポリシーを作成する" 。

1. BlueXP backup and recoveryのメイン ページで、[設定] ドロップダウン メニューにアクセスし、[ポリシー] を選択します。



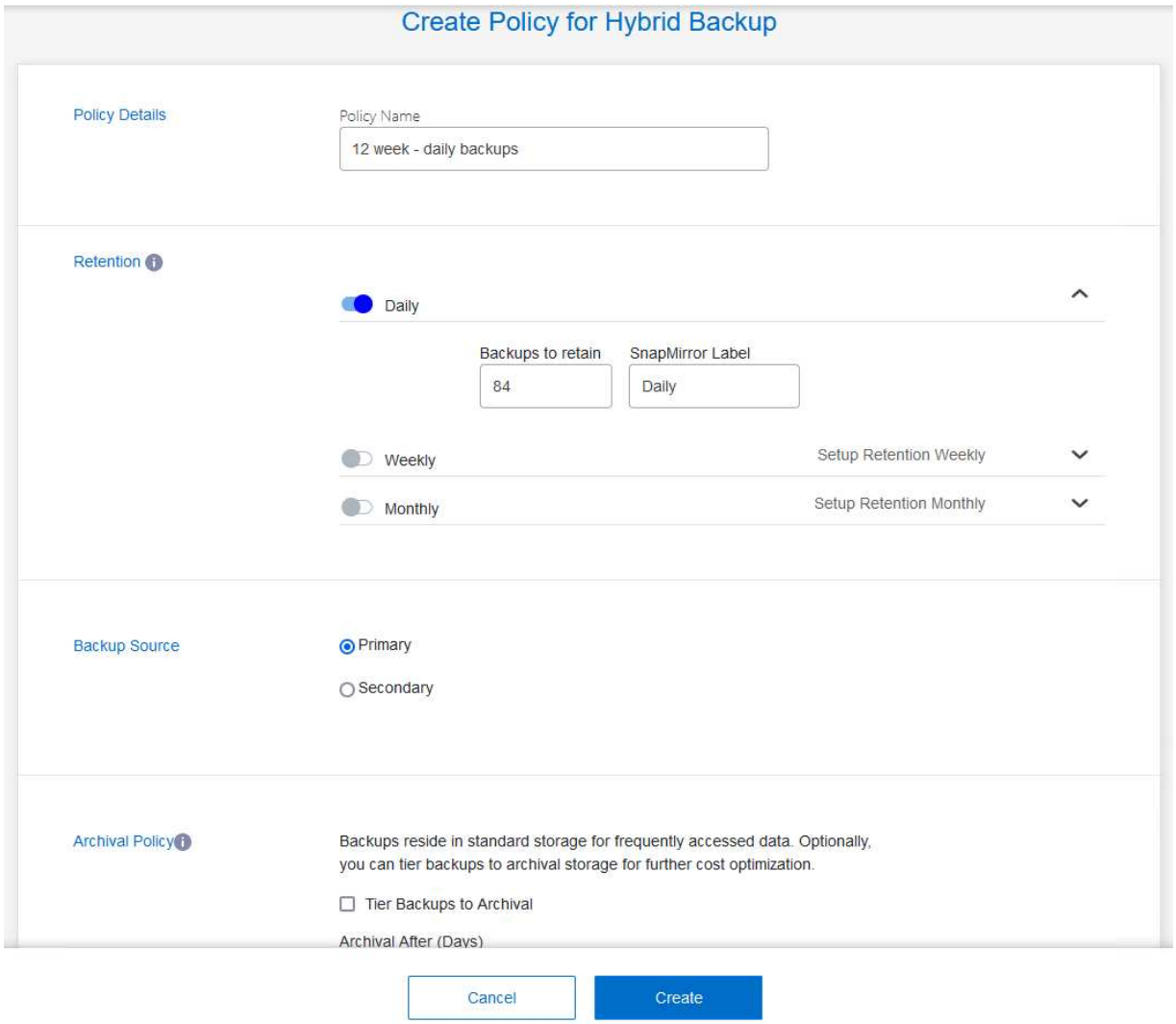
2. ポリシーの作成 をクリックして、ハイブリッド バックアップのポリシーの作成 ウィンドウにアクセスします。

   a. ポリシーの名前を追加する

   b. 希望する保存期間を選択してください

   c. バックアップをプライマリまたはセカンダリのオンプレミスONTAPストレージ システムから取得するかどうかを選択します。

   d. オプションで、追加のコスト削減のために、どのくらいの期間後にバックアップがアーカイブ ストレージに階層化されるかを指定します。



ここで入力したSnapMirrorラベルは、ポリシーを適用するバックアップを識別するために使用されます。ラベル名は、対応するオンプレミスの SCV ポリシーのラベル名と一致する必要があります。

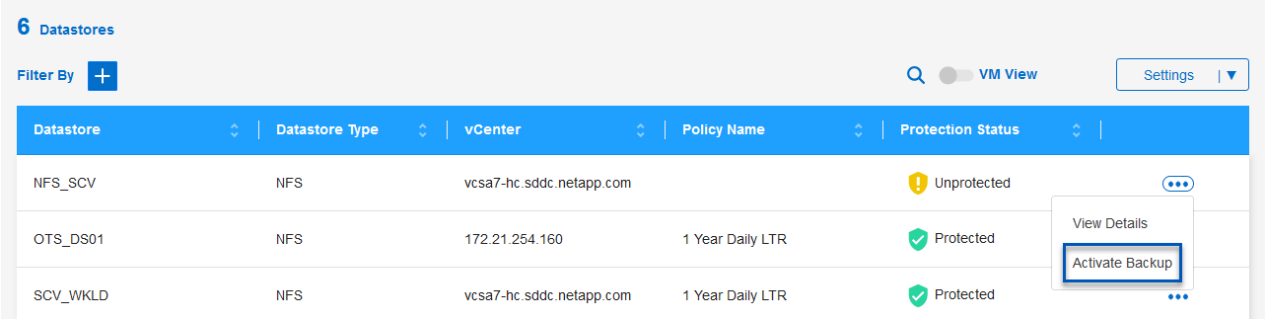
3. *作成*をクリックしてポリシーの作成を完了します。

Amazon Web Services へのデータストアのバックアップ

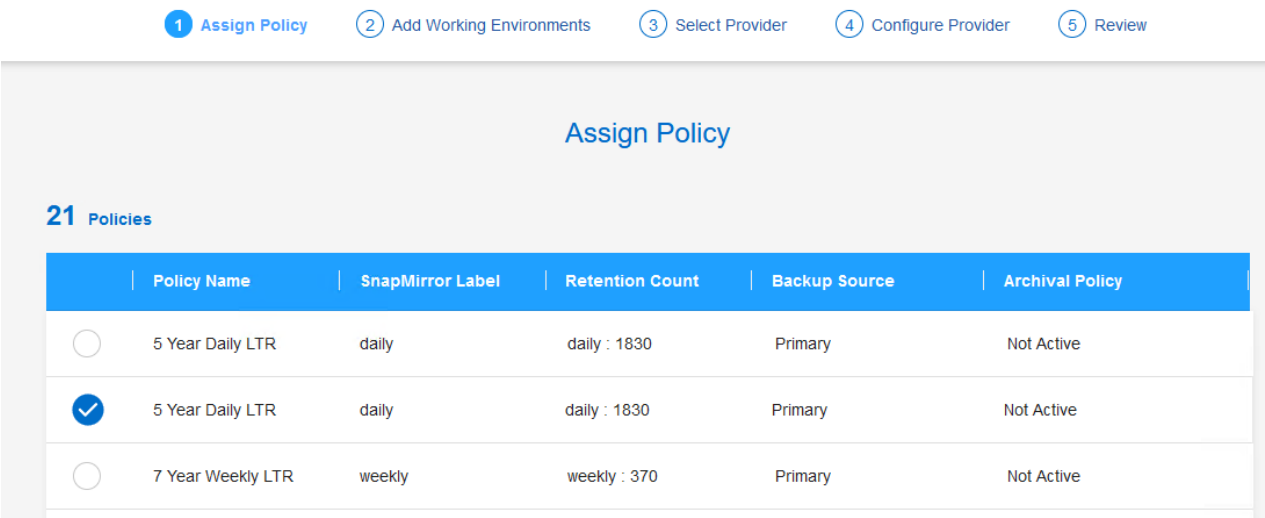
最後のステップは、個々のデータストアと仮想マシンのデータ保護を有効にすることです。次の手順では、AWS へのバックアップをアクティブ化する方法を説明します。

詳細については、 "データストアを Amazon Web Services にバックアップする" 。

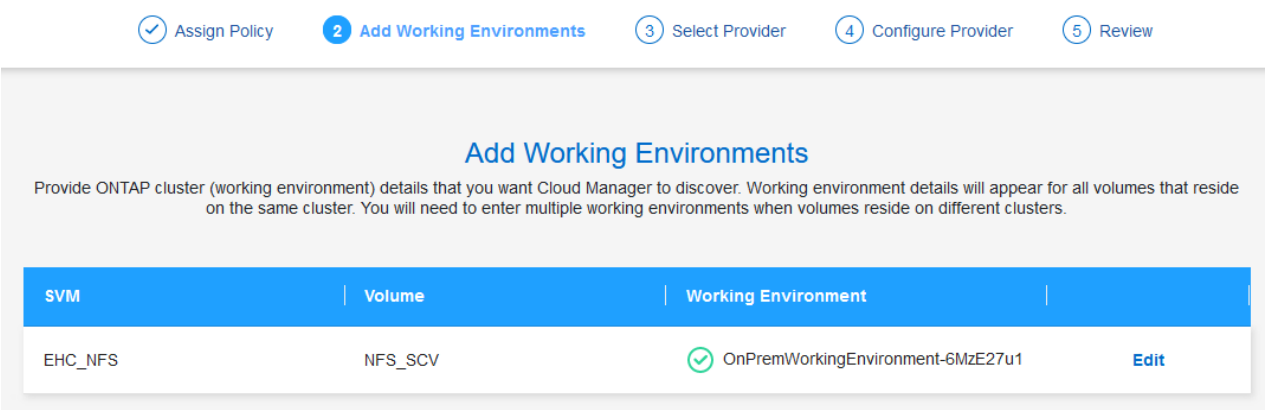
1. BlueXP backup and recoveryのメイン ページから、バックアップするデータストアの設定ドロップダウンにアクセスし、[バックアップのアクティブ化] を選択します。



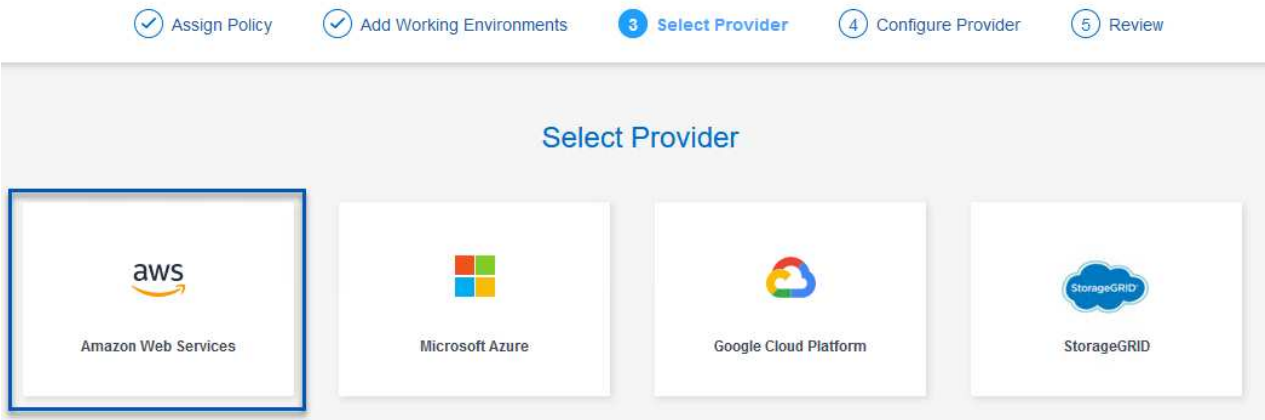
2. データ保護操作に使用するポリシーを割り当て、[次へ] をクリックします。



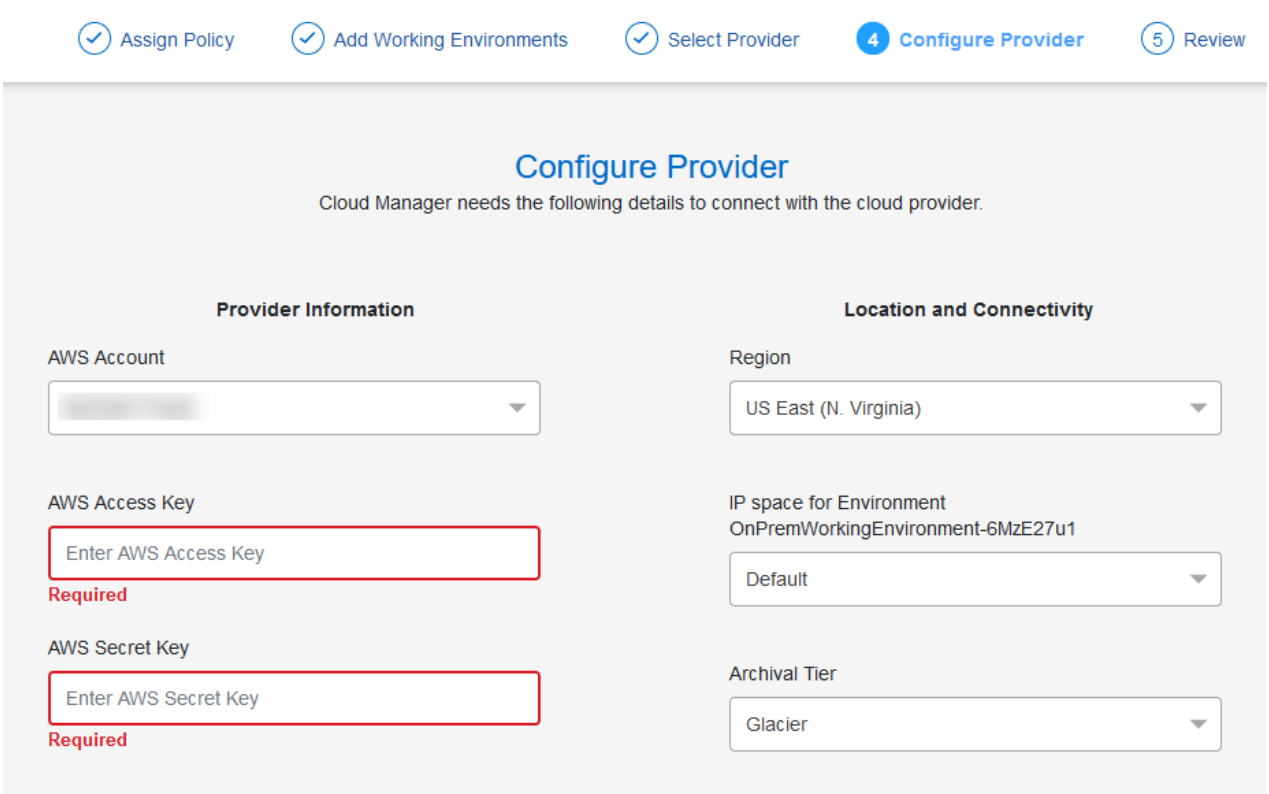
3. 作業環境が以前に検出されている場合は、「作業環境の追加」ページに、チェックマークが付いたデータストアと作業環境が表示されます。作業環境が以前に検出されていない場合は、ここで追加できます。続行するには、[次へ] をクリックします。



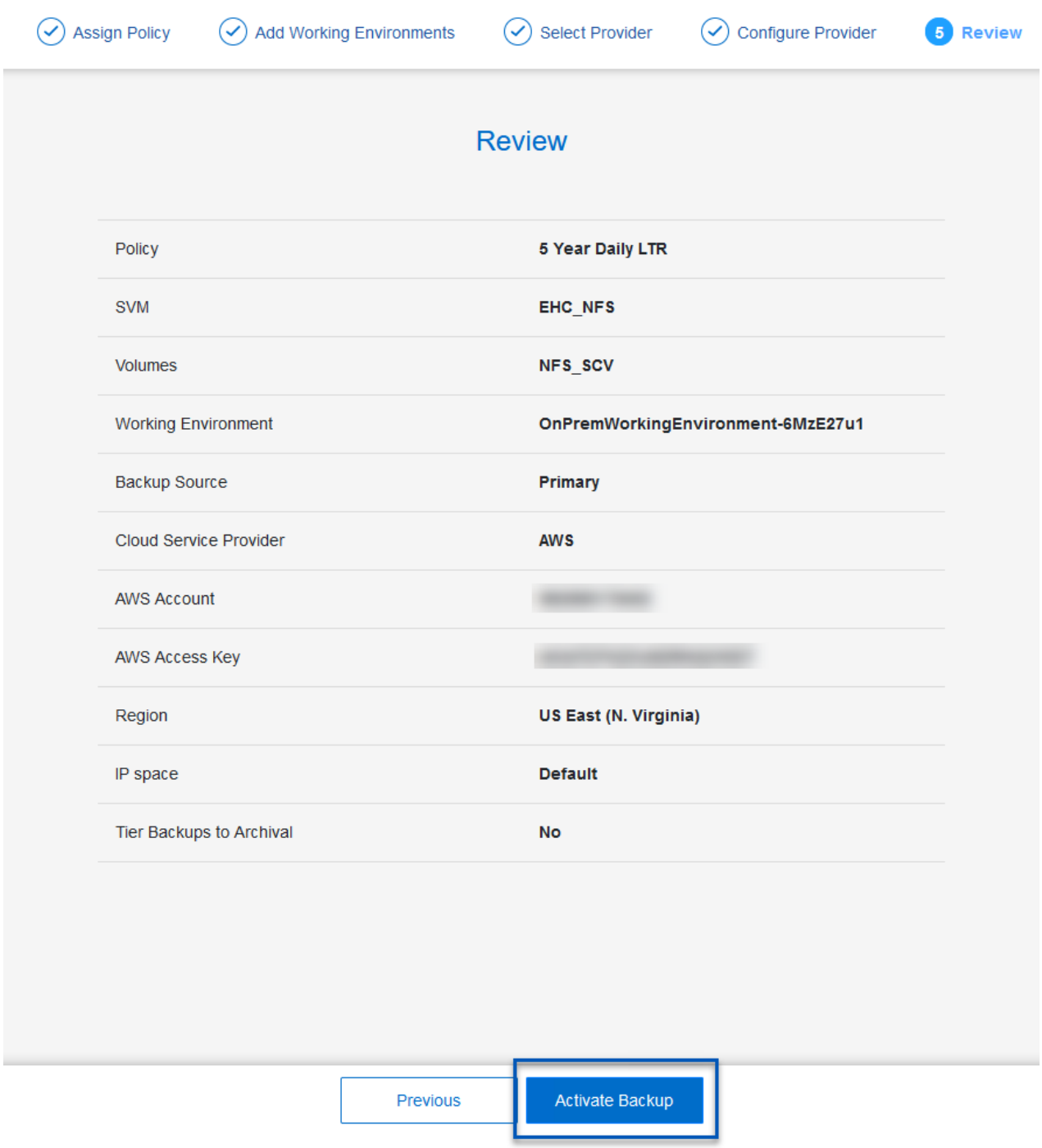
4. *プロバイダーの選択*ページでAWSをクリックし、*次へ*ボタンをクリックして続行します。



5. 使用する AWS アクセスキーとシークレットキー、リージョン、アーカイブ層など、AWS のプロバイダー固有の認証情報を入力します。また、オンプレミスのONTAPストレージ システムのONTAP IP スペースを選択します。 *次へ*をクリックします。



6. 最後に、バックアップ ジョブの詳細を確認し、[バックアップのアクティブ化] ボタンをクリックして、データストアのデータ保護を開始します。



この時点ではデータ転送がすぐに開始されない場合があります。 BlueXP backup and recoveryは、未処理のスナップショットを 1 時間ごとにスキャンし、それらをオブジェクト ストレージに転送します。

データ損失の場合の仮想マシンの復元

データの安全を確保することは、包括的なデータ保護の 1 つの側面にすぎません。同様に重要なのは、データの損失やランサムウェア攻撃が発生した場合に、どこからでも迅速にデータを復元できる機能です。この機能は、シームレスなビジネス運用を維持し、リカバリポイント目標を達成するために不可欠です。

NetApp は、適応性に優れた 3-2-1 戦略を提供し、プライマリ、セカンダリ、およびオブジェクト ストレージの場所で保持スケジュールをカスタマイズして制御できます。この戦略により、データ保護のアプローチを特定のニーズに合わせて柔軟にカスタマイズできるようになります。

このセクションでは、SnapCenter Plug-in for VMware vSphereと仮想マシンのBlueXP backup and recoveryの両方からのデータ復元プロセスの概要を説明します。

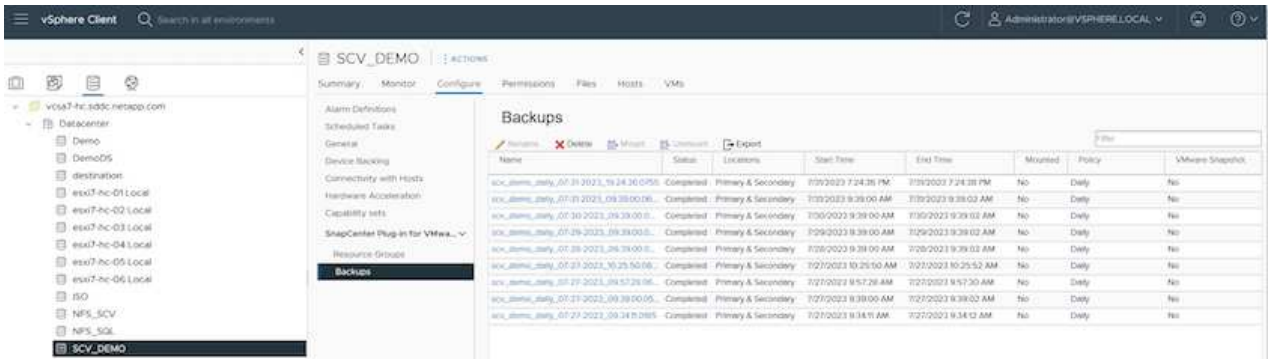
SnapCenter Plug-in for VMware vSphereからの仮想マシンの復元

このソリューションでは、仮想マシンが元の場所と別の場所に復元されました。このソリューションでは、SCV のデータ復元機能のすべての側面がカバーされるわけではありません。 SCVが提供するすべての詳細情報については、 "バックアップからのVMのリストア"製品ドキュメントに記載されています。

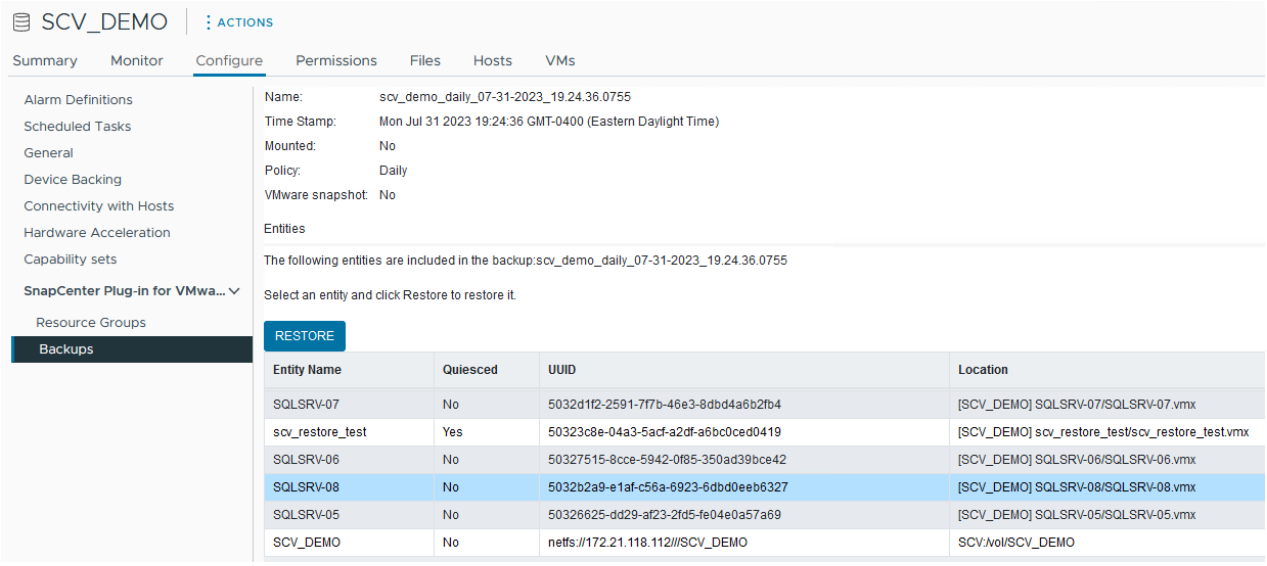
SCVから仮想マシンを復元する

プライマリ ストレージまたはセカンダリ ストレージから仮想マシンを復元するには、次の手順を実行します。

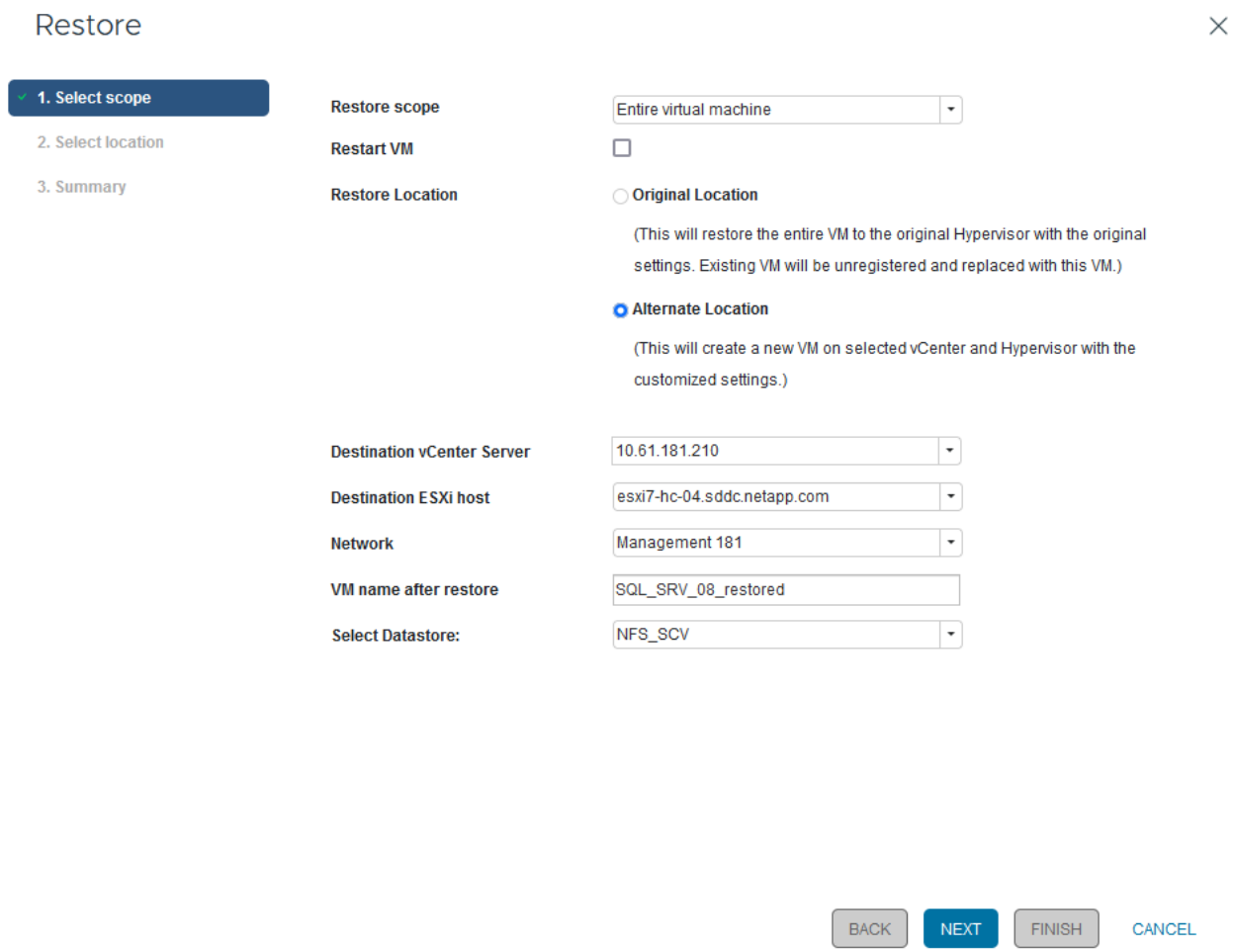
1. vCenter クライアントから インベントリ > ストレージ に移動し、復元する仮想マシンが含まれているデータストアをクリックします。
2. 構成 タブから バックアップ をクリックして、利用可能なバックアップのリストにアクセスします。



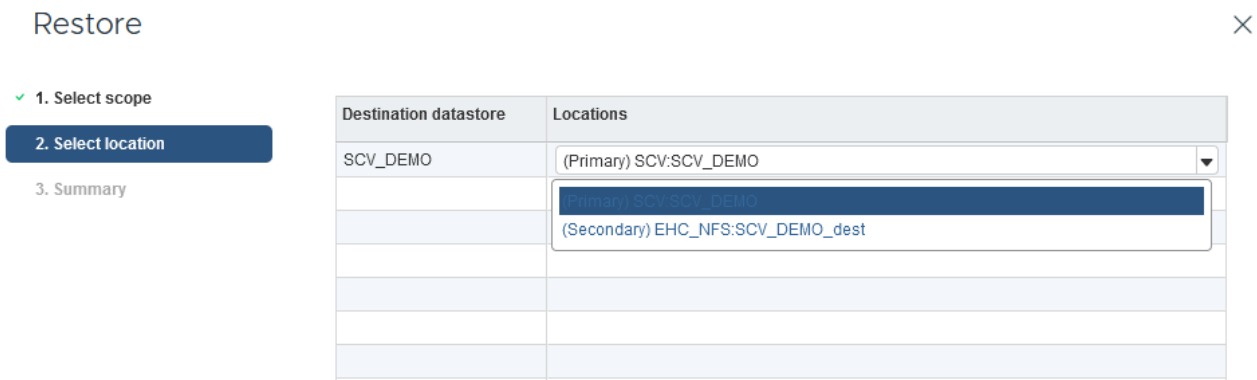
3. バックアップをクリックして VM のリストにアクセスし、復元する VM を選択します。 *復元*をクリックします。



4. 復元ウィザードから、仮想マシン全体を復元するか、特定の VMDK を復元するかを選択します。元の場所または別の場所にインストールすることを選択し、復元後の VM 名と宛先データストアを指定します。*次へ*をクリックします。



5. プライマリまたはセカンダリのストレージ場所からバックアップすることを選択します。



6. 最後に、バックアップ ジョブの概要を確認し、「完了」をクリックして復元プロセスを開始します。

BlueXP backup and recoveryから仮想マシンを復元する

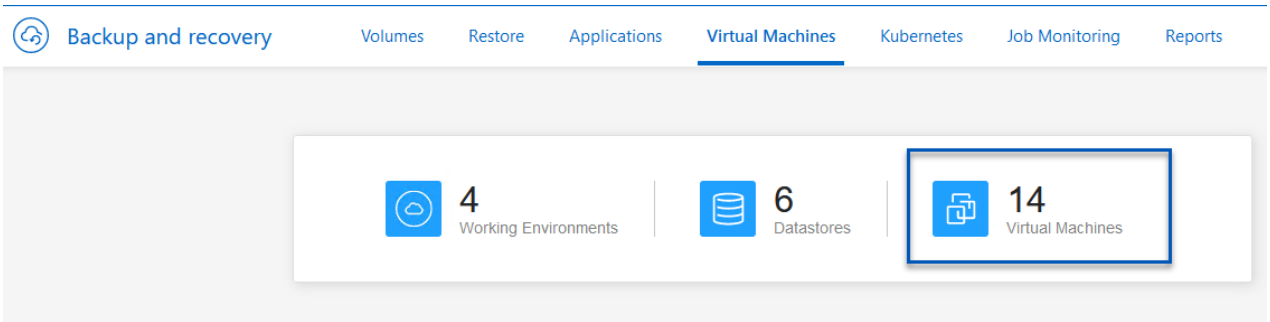
仮想マシン用のBlueXP backup and recoveryを使用すると、仮想マシンを元の場所に復元できます。復元機能には、 BlueXP Web コンソールからアクセスします。

詳細については、 "クラウドから仮想マシンのデータを復元する" 。

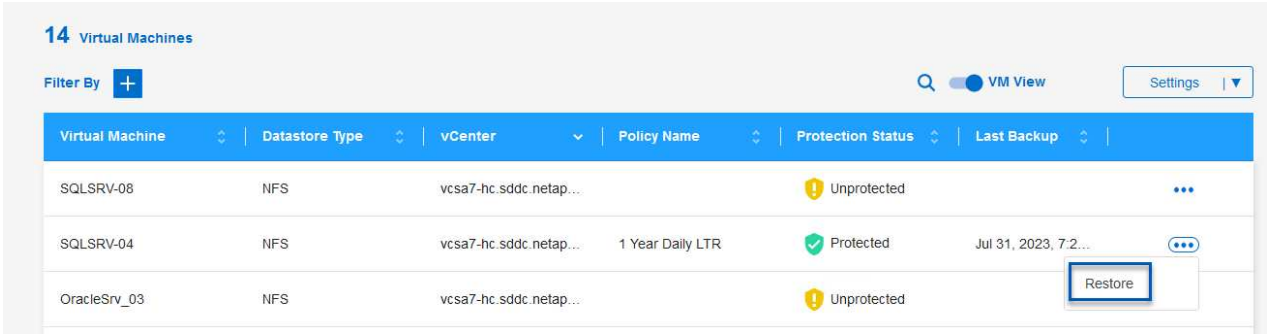
BlueXP backup and recoveryから仮想マシンを復元する

BlueXP backup and recoveryから仮想マシンを復元するには、次の手順を実行します。

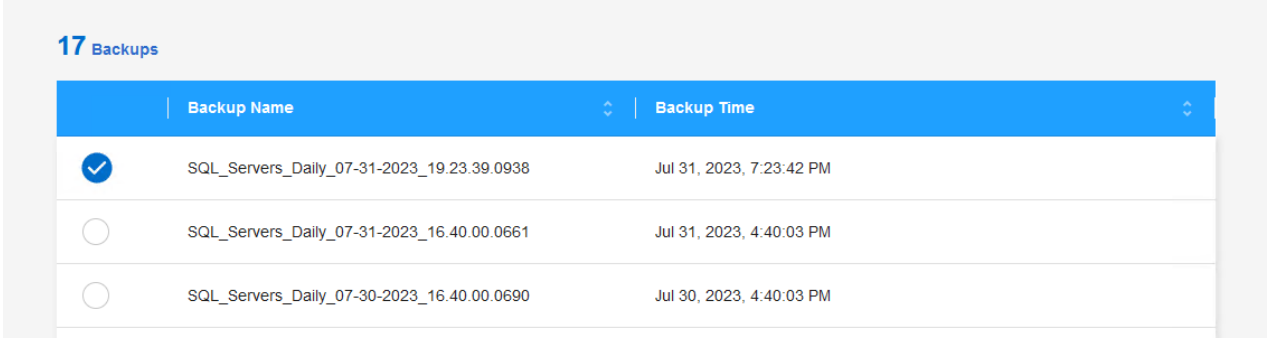
1. 保護 > バックアップとリカバリ > 仮想マシン に移動し、仮想マシンをクリックして、復元可能な仮想マシンのリストを表示します。



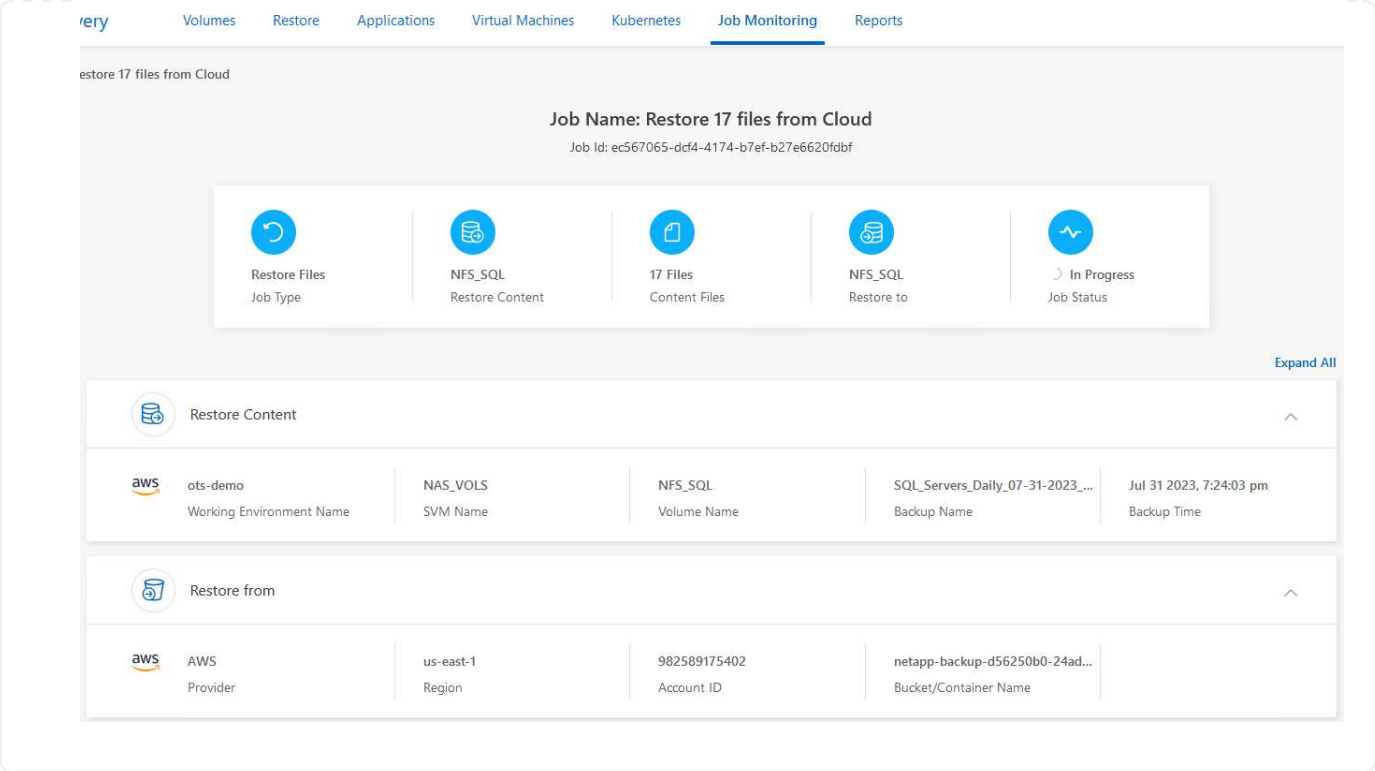
2. 復元するVMの設定ドロップダウンメニューにアクセスし、



3. 復元するバックアップを選択し、「次へ」をクリックします。



4. バックアップ ジョブの概要を確認し、[復元] をクリックして復元プロセスを開始します。
5. *ジョブ監視*タブから復元ジョブの進行状況を監視します。



まとめ

3-2-1 バックアップ戦略は、 SnapCenter Plug-in for VMware vSphereと仮想マシン用のBlueXP backup and recoveryを使用して実装すると、データ保護のための堅牢で信頼性が高く、コスト効率に優れたソリューションを提供します。この戦略は、データの冗長性とアクセス性を保証するだけでなく、オンプレミスのONTAP ストレージ システムとクラウドベースのオブジェクト ストレージの両方から、任意の場所からデータを復元できる柔軟性も提供します。

このドキュメントで紹介するユースケースは、 NetApp、VMware、および主要なクラウド プロバイダー間の統合を強調する実証済みのデータ保護テクノロジに重点を置いています。 SnapCenter Plug-in for VMware vSphere は、VMware vSphere とのシームレスな統合を提供し、データ保護操作の効率的かつ集中的な管理を可能にします。この統合により、仮想マシンのバックアップおよびリカバリ プロセスが合理化され、VMware エコシステム内でのスケジュール設定、監視、および柔軟な復元操作が容易になります。 BlueXP backup and recoveryは、仮想マシン データの安全なエアギャップ バックアップをクラウド ベースのオブジェクト ストレージに提供することで、3-2-1 の 1 つを実現します。直感的なインターフェースと論理的なワークフローにより、重要なデータを長期にわたってアーカイブするための安全なプラットフォームが提供されます。

追加情報

このソリューションで紹介されているテクノロジーの詳細については、次の追加情報を参照してください。

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

著作権に関する情報

Copyright © 2025 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権を有し、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権については、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。