AWS / VMCでのワークロードの保護

NetApp Solutions

NetApp
March 04, 2025

目次

AWS / VMCでのワークロードの保護

TR-4931：『Disaster Recovery with VMware Cloud on Amazon Web Services and Guest Connect』

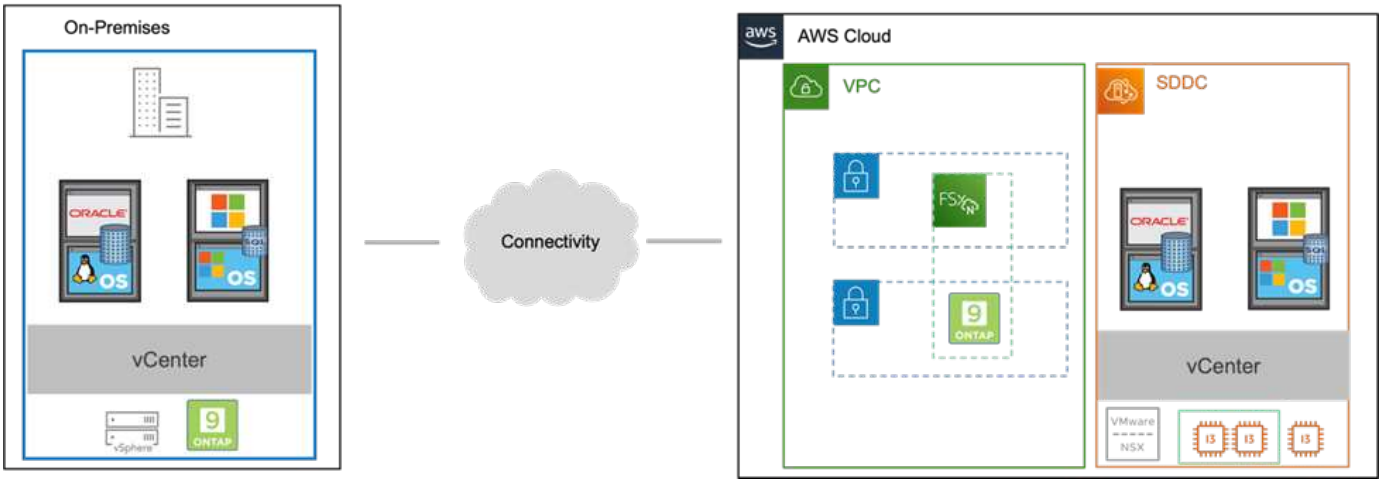
大規模な障害が発生した場合にビジネスクリティカルなアプリケーションを迅速にリストアできるようにするには、実績のあるディザスタリカバリ（DR）環境と計画が不可欠です。この解決策 では、オンプレミスとVMware Cloud on AWSの両方で、VMwareとネットアップのテクノロジを中心にDRのユースケースを紹介します。

執筆者：Chris Reno、Josh Powell、Suresh Thoppay - NetApp Solutions Engineering

概要

ネットアップはVMwareとの長年の統合を実現してきました。これは、仮想環境のストレージパートナーとしてネットアップを選んだ何万ものお客様から証明されています。この統合は、クラウドのゲスト接続オプションのほか、NFSデータストアとの最近の統合とも連動します。この解決策 では、一般にゲスト接続ストレージと呼ばれるユースケースを取り上げます。

ゲスト接続ストレージでは、ゲストVMDKはVMwareでプロビジョニングされたデータストアに導入され、アプリケーションデータはiSCSIまたはNFSに格納されてVMに直接マッピングされます。次の図に示すように、OracleおよびMS SQLアプリケーションを使用してDRシナリオを検証します。



前提条件、前提条件、コンポーネントの概要

この解決策 を導入する前に、コンポーネントの概要、解決策 を導入するための前提条件、およびこの解決策のドキュメント化に記載した前提条件を確認してください。

"DR解決策 の要件、事前要件、計画"

SnapCenter を使用してDRを実行する

この解決策 では、SnapCenter は、SQL ServerおよびOracleアプリケーションデータ用に、アプリケーションと整合性のあるSnapshotを提供します。この構成とSnapMirrorテクノロジを組み合わせることで、オンプレ

ミスのAFF とFSX ONTAP クラスタ間で高速なデータレプリケーションを実現できます。また、Veeam Backup & Replicationは、仮想マシンのバックアップとリストア機能も提供します。

ここでは、バックアップとリストアの両方について、SnapCenter 、SnapMirror、およびVeeamの構成について説明します。

次のセクションでは、セカンダリサイトでフェイルオーバーを完了するために必要な設定と手順について説明します。

SnapMirror関係と保持スケジュールを設定

SnapCenter では、長期のアーカイブと保持を目的として、プライマリストレージシステム（primary > mirror ）およびセカンダリストレージシステム（primary > vault）内のSnapMirror関係を更新できます。そのためには、SnapMirrorを使用して、デスティネーションボリュームとソースボリューム間のデータレプリケーション関係を確立して初期化する必要があります。

ソースとデスティネーションのONTAP システムが、Amazon VPCピアリング、トランジットゲートウェイ、AWS Direct Connect、またはAWS VPNを使用してピア関係にあるネットワークに配置されている必要があります。

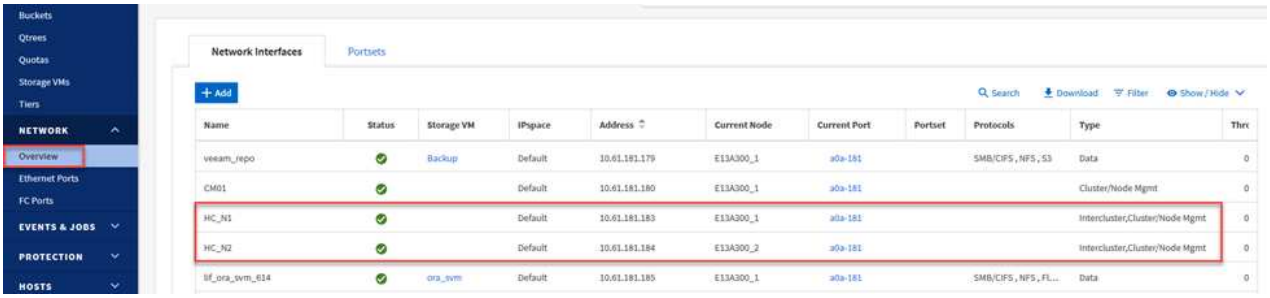
オンプレミスのONTAP システムとFSX ONTAP 間にSnapMirror関係を設定するには、次の手順を実行する必要があります。

FSxでSnapMirror関係を作成する方法の詳細については、を参照してください "FSx ONTAP–ONTAPユーザガイド"。

ソースとデスティネーションのクラスタ間論理インターフェイスを記録します

オンプレミスにあるソースONTAP システムの場合、クラスタ間LIFの情報をSystem ManagerまたはCLIから取得できます。

1. ONTAP System Managerで、ネットワークの概要ページに移動し、タイプ：クラスタ間のIPアドレスを取得します。このIPアドレスは、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ます。



2. FSXのクラスタ間IPアドレスを取得するには、CLIにログインして次のコマンドを実行します。

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

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
FsxId0ae40e08acc0dea67
            inter_1      up/up    172.30.15.42/25    FsxId0ae40e08acc0dea67-01
                                                                   e0e     true
            inter_2      up/up    172.30.14.28/26    FsxId0ae40e08acc0dea67-02
                                                                   e0e     true
2 entries were displayed.
```

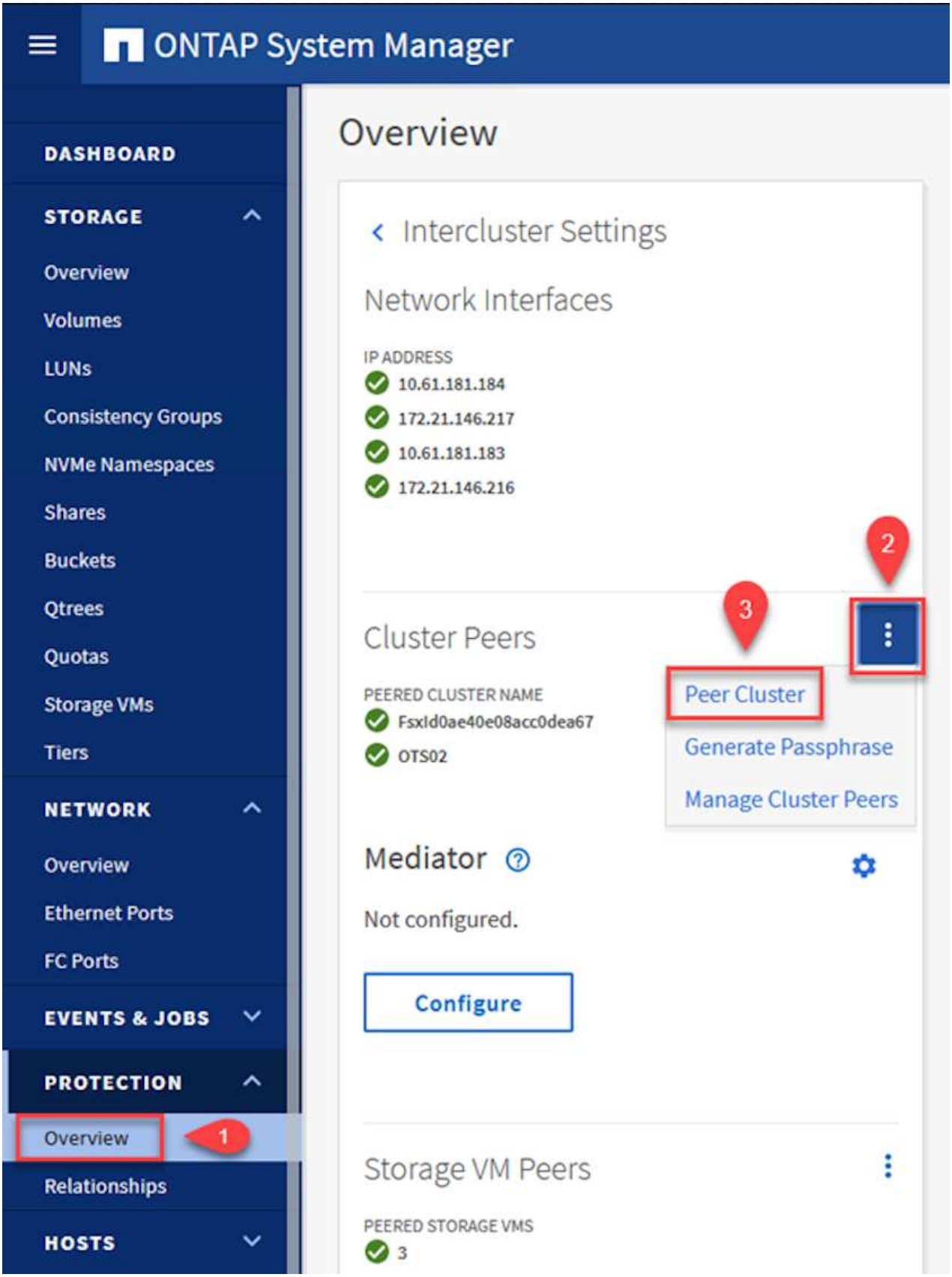
ONTAP と**FSX**の間にクラスタピアリングを確立します

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、もう一方のピアクラスタで確認する必要があります。

1. コマンドを使用して、デスティネーションFSxクラスタでピアリングを設定し `cluster peer create`ます。プロンプトが表示されたら、あとでソースクラスタで使用する一意のパスフレーズを入力して作成プロセスを完了します。

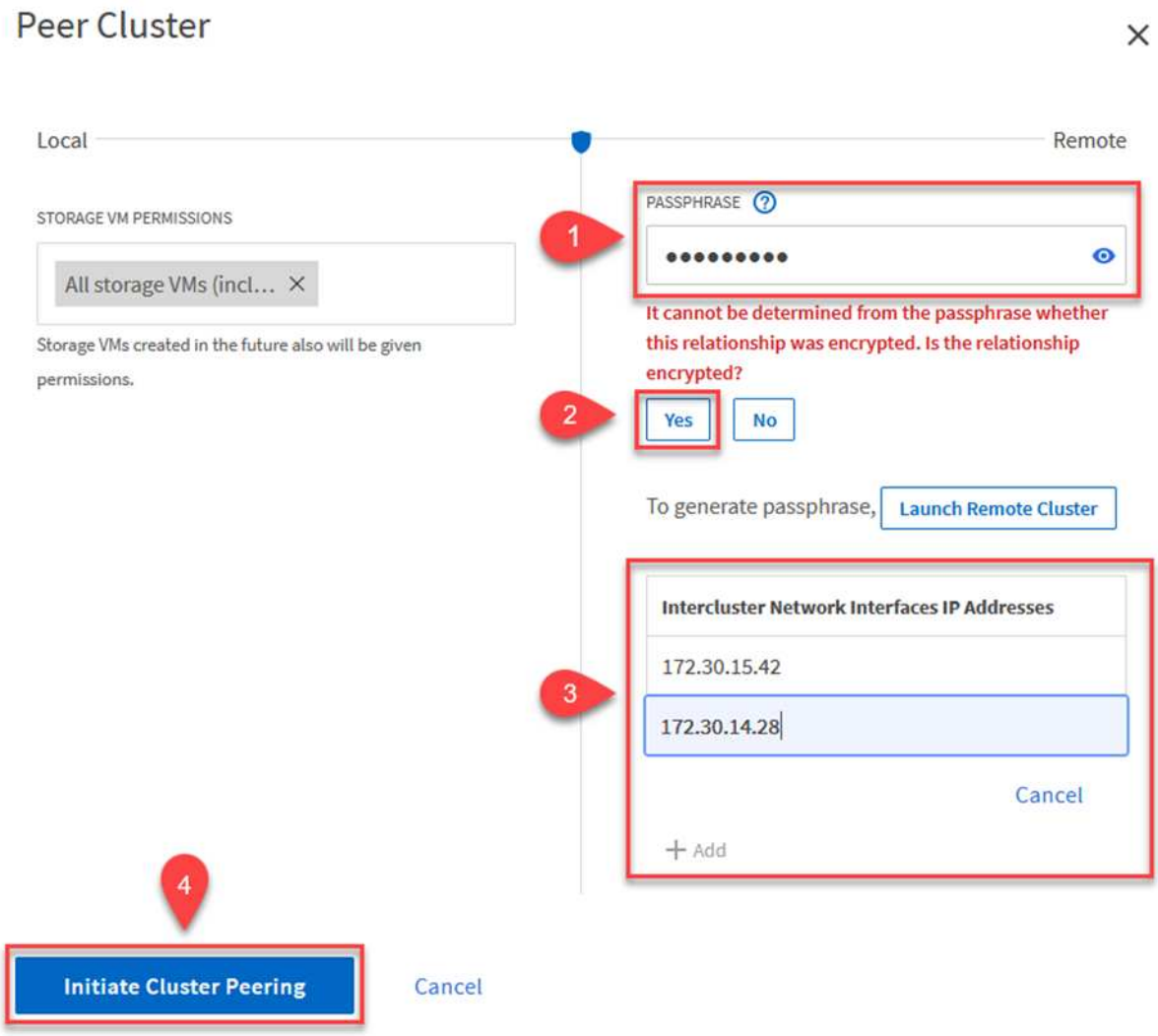
```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

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で、Protection > Overviewの順に選択し、Peer Clusterを選択します。



3. Peer Cluster（ピアクラスタ）ダイアログボックスで、必要な情報を入力します。
   a. デスティネーションFSXクラスタでピアクラスタ関係を確立するために使用したパスフレーズを入力します。

b. を選択し `Yes`て暗号化された関係を確立します。
c. デスティネーションFSXクラスタのクラスタ間LIFのIPアドレスを入力します。
d. クラスタピアリングの開始をクリックしてプロセスを完了します。



4. 次のコマンドを使用して、FSX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。

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

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

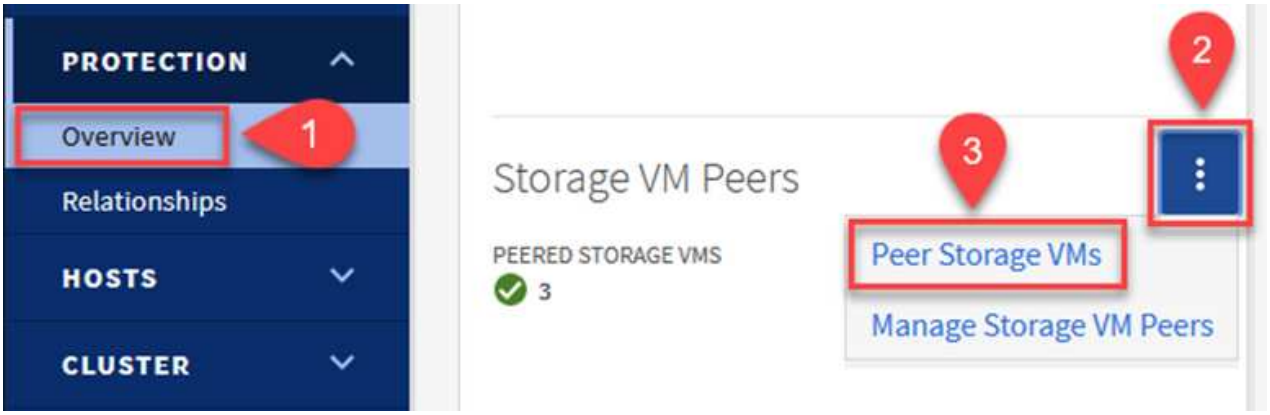
SVMピア関係を確立する

次の手順では、SnapMirror関係にあるボリュームを含むデスティネーションとソースのStorage Virtual Machineの間にSVM関係をセットアップします。

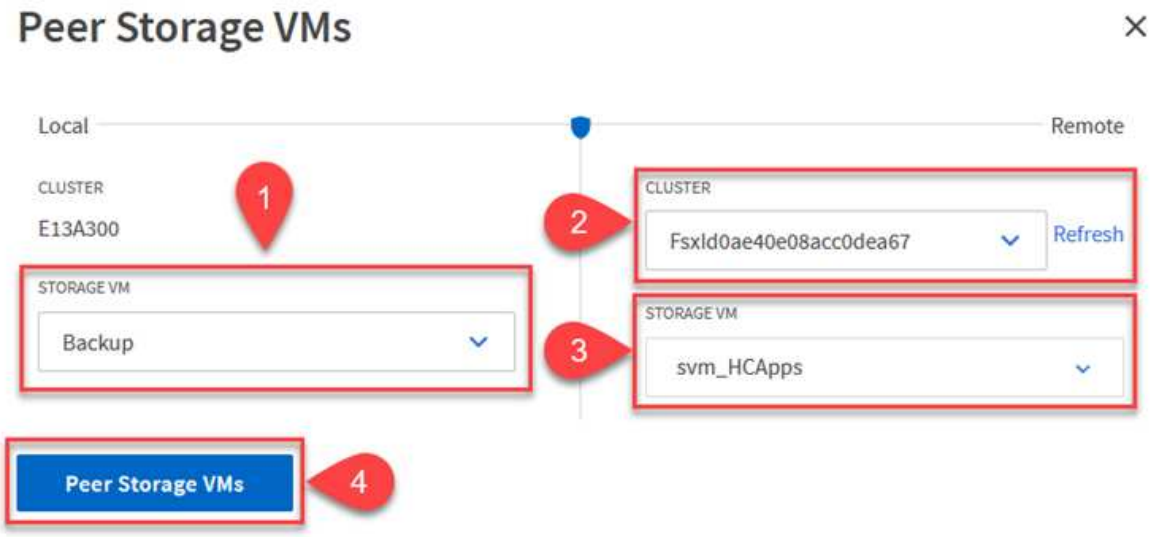
1. ソースFSXクラスタから、CLIから次のコマンドを使用して、SVMピア関係を作成します。

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

2. ソースONTAP クラスタで、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承認します。
3. ONTAP System Managerで、保護>概要に移動し、Storage VMピアの下にあるピアStorage VMを選択します。



4. Peer Storage VMダイアログボックスで、次のフィールドに入力します。
   - ソースStorage VM
   - デスティネーションクラスタ
   - デスティネーションStorage VM



5. [Peer Storage VMs]をクリックして、SVMピアリングプロセスを完了します。

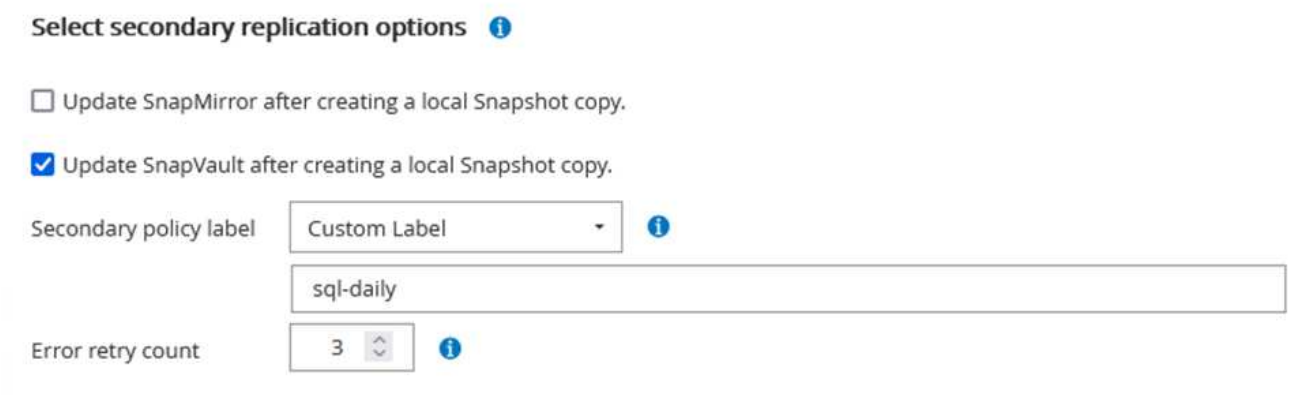
Snapshot保持ポリシーを作成します

SnapCenter は、プライマリストレージシステムにSnapshot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 では、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は管理されません。これらのポリシーは、セカンダリFSXクラスタで作成されたSnapMirrorポリシーを使用して個別に管理され、ソースボリュームとSnapMirror関係にあるデスティネーションボリュームに関連付けられます。

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SnapshotのSnapMirrorラベルに追加するセカンダリポリシーラベルを指定できます。

セカンダリストレージでは、Snapshotを保持するために、これらのラベルがデスティネーション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データベースおよびログボリュームの日次バックアップに使用するポリシーの一部として生成されたすべてのSnapshotに適用されるSnapMirrorラベルを示しています。



SQL ServerデータベースのSnapCenterポリシーの作成の詳細については、を参照してください "SnapCenter のドキュメント"。

まず、保持するSnapshotコピーの数にルールを指定してSnapMirrorポリシーを作成する必要があります。

1. FSXクラスタ上にSnapMirrorポリシーを作成します。

```
FSx-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ラベルを持つルールをポリシーに追加します。

```
FSx-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。

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

SnapMirrorラベルごとに追加のルールを作成し、保持するSnapshotの数（保持期間）を指定します。

デスティネーションボリュームを作成

ソースボリュームからSnapshotコピーの受信者となるデスティネーションボリュームをFSX上に作成するには、FSX ONTAP 上で次のコマンドを実行します。

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

ソースボリュームとデスティネーションボリューム間に**SnapMirror**関係を作成します

ソースボリュームとデスティネーションボリューム間のSnapMirror関係を作成するには、FSX ONTAP で次のコマンドを実行します。

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

SnapMirror関係を初期化

SnapMirror関係を初期化このプロセスにより、ソースボリュームから生成された新しいSnapshotが開始され、デスティネーションボリュームにコピーされます。

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

Windows SnapCenter サーバをオンプレミスに導入して設定

Windows SnapCenter Serverをオンプレミスに導入

この解決策 では、NetApp SnapCenter を使用して、アプリケーションと整合性のあるSQL Serverデータベースのバックアップを作成します。仮想マシンのVMDKをバックアップするVeeam Backup & Replicationと併用することで、オンプレミスのデータセンターとクラウドベースのデータセンター向けに包括的なディザスタリカバリ解決策 を実現できます。

SnapCenter ソフトウェアはNetApp Support Siteから入手でき、ドメインまたはワークグループ内にあるMicrosoft Windowsシステムにインストールできます。詳細な計画ガイドとインストール手順については、を参照し "ネットアップドキュメントセンター"てください。

SnapCenterソフトウェアは、から入手できます "リンクをクリックしてください"。

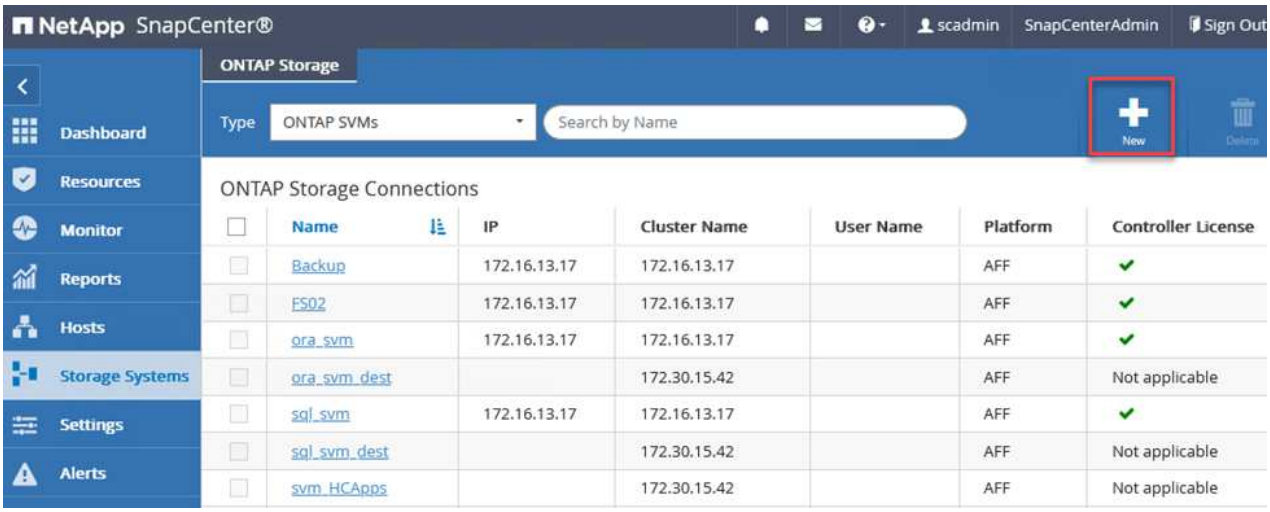
インストール後は、*https://Virtual_Cluster_IP_or_FQDN:8146*.を使用してWebブラウザからSnapCenterコンソールにアクセスできます。

コンソールにログインしたら、バックアップSQL ServerおよびOracleデータベース用にSnapCenter を設定する必要があります。

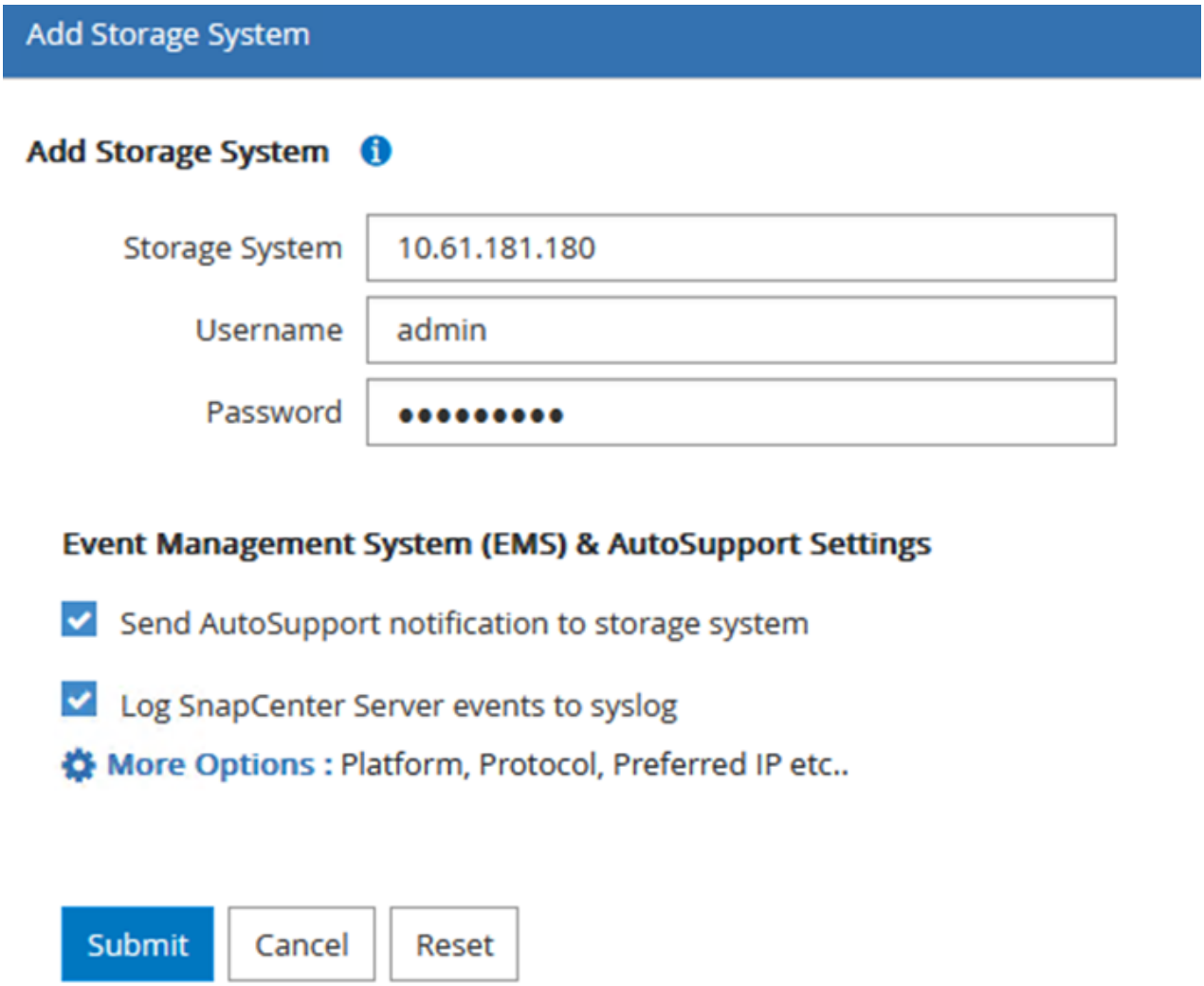
SnapCenter にストレージコントローラを追加

SnapCenter にストレージコントローラを追加するには、次の手順を実行します。

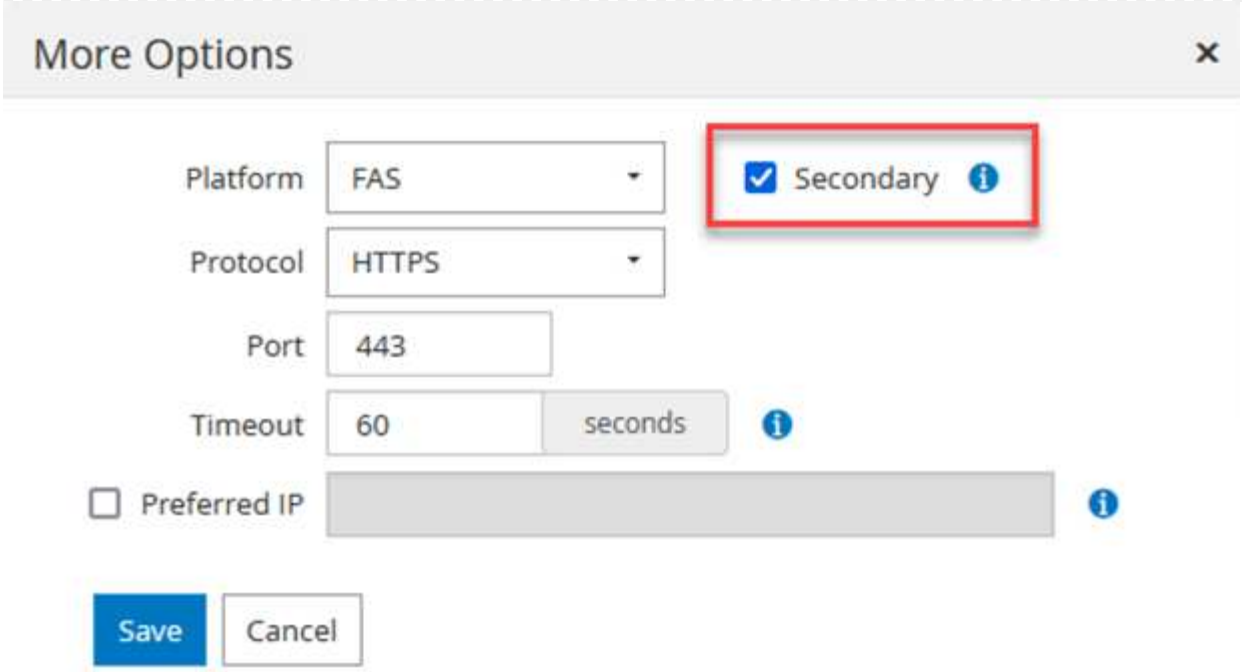
1. 左側のメニューから、ストレージシステムを選択し、新規をクリックして、ストレージコントローラをSnapCenter に追加するプロセスを開始します。



2. Add Storage System（ストレージシステムの追加）ダイアログボックスで、ローカルのオンプレミスONTAP クラスタの管理IPアドレス、およびユーザ名とパスワードを追加します。Submitをクリックして、ストレージ・システムの検出を開始します。



3. FSX ONTAP システムをSnapCenter に追加するには、この手順を繰り返します。この場合、Add Storage Systemウィンドウの下部にあるMore Optionsを選択し、Secondaryチェックボックスをオンにして、SnapMirrorコピーまたはプライマリバックアップスナップショットで更新されたセカンダリストレージシステムとしてFSXシステムを指定します。

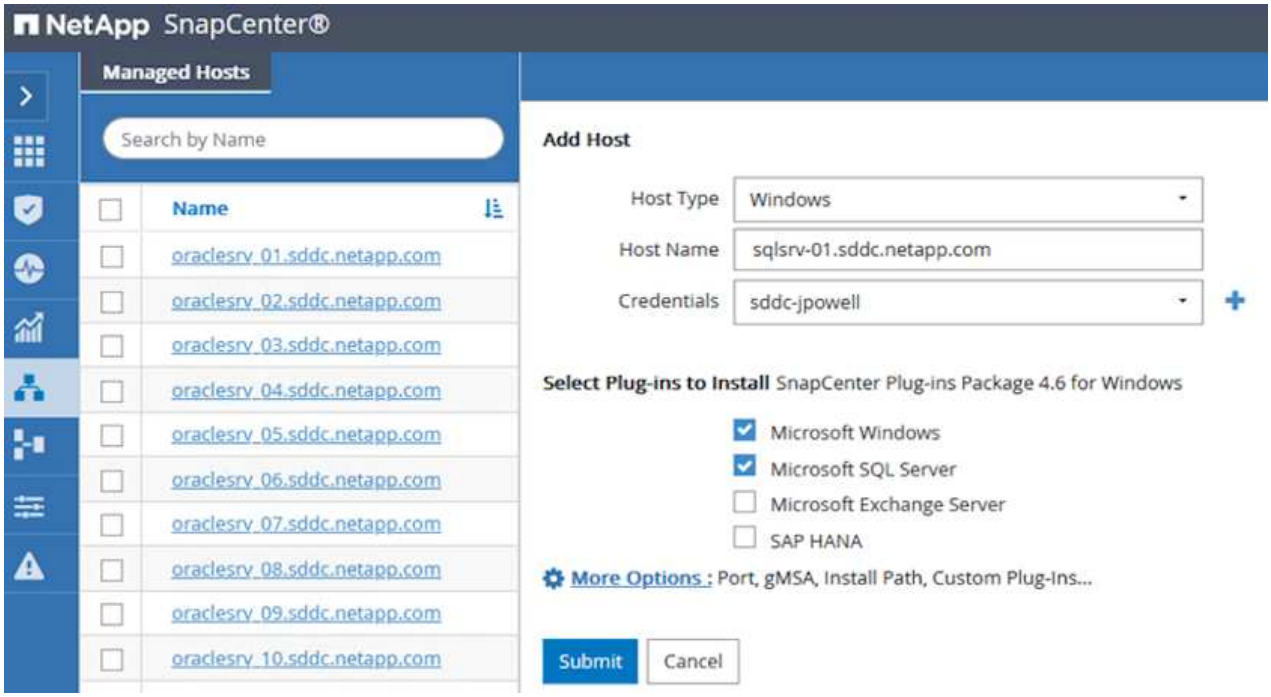


SnapCenterへのストレージシステムの追加に関する詳細については、のマニュアルを参照してください "リンクをクリックしてください"。

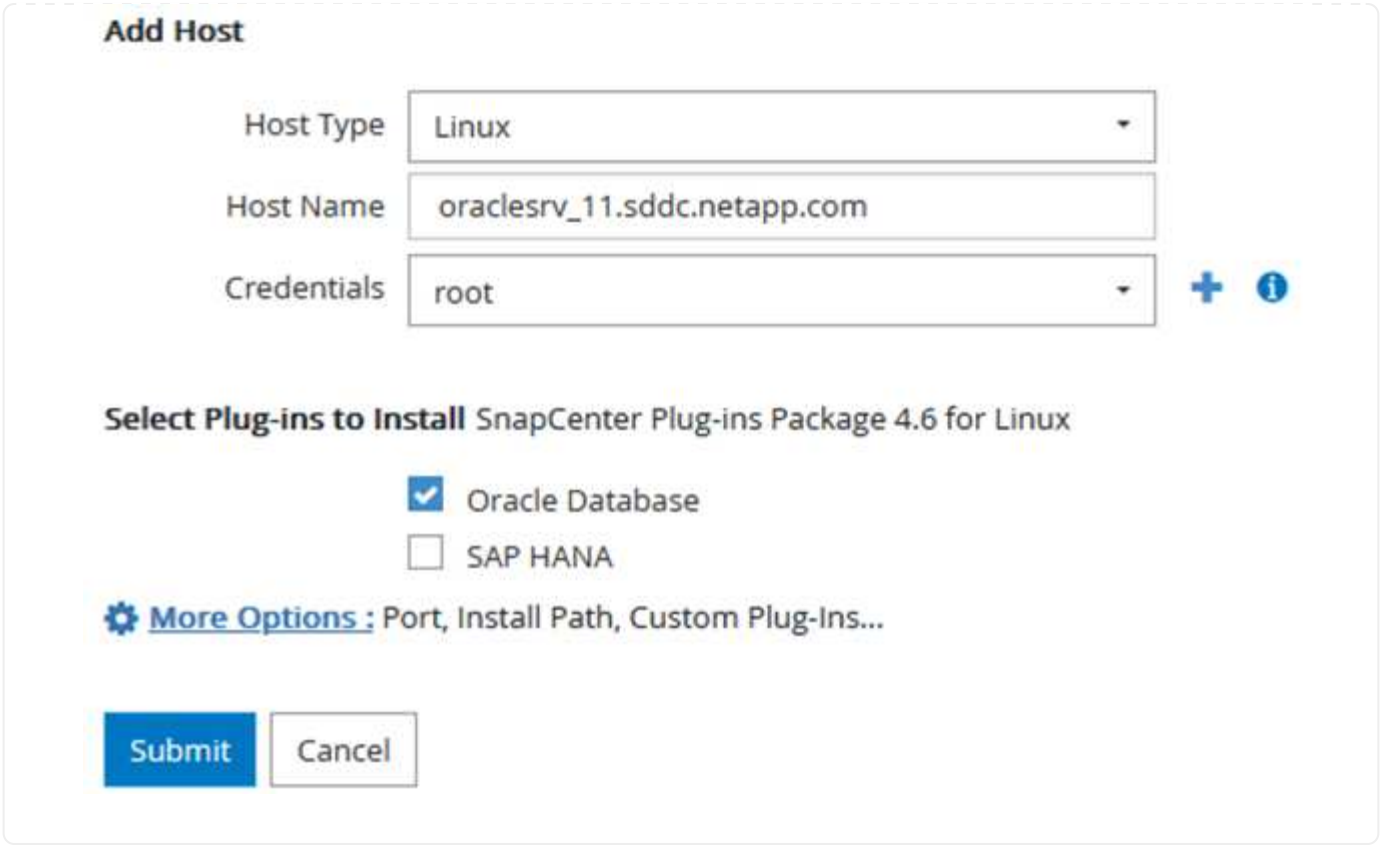
SnapCenter にホストを追加します

次の手順では、ホストアプリケーションサーバをSnapCenter に追加します。このプロセスは、SQL ServerとOracleのどちらでもほぼ同じです。

1. 左側のメニューから、Hostsを選択し、Addをクリックして、SnapCenter にストレージコントローラを追加する処理を開始します。
2. [Add Hosts]ウィンドウで、ホストタイプ、ホスト名、およびホストシステムの認証情報を追加します。プラグインタイプを選択します。SQL Serverの場合は、Microsoft WindowsとMicrosoft SQL Serverプラグインを選択します。



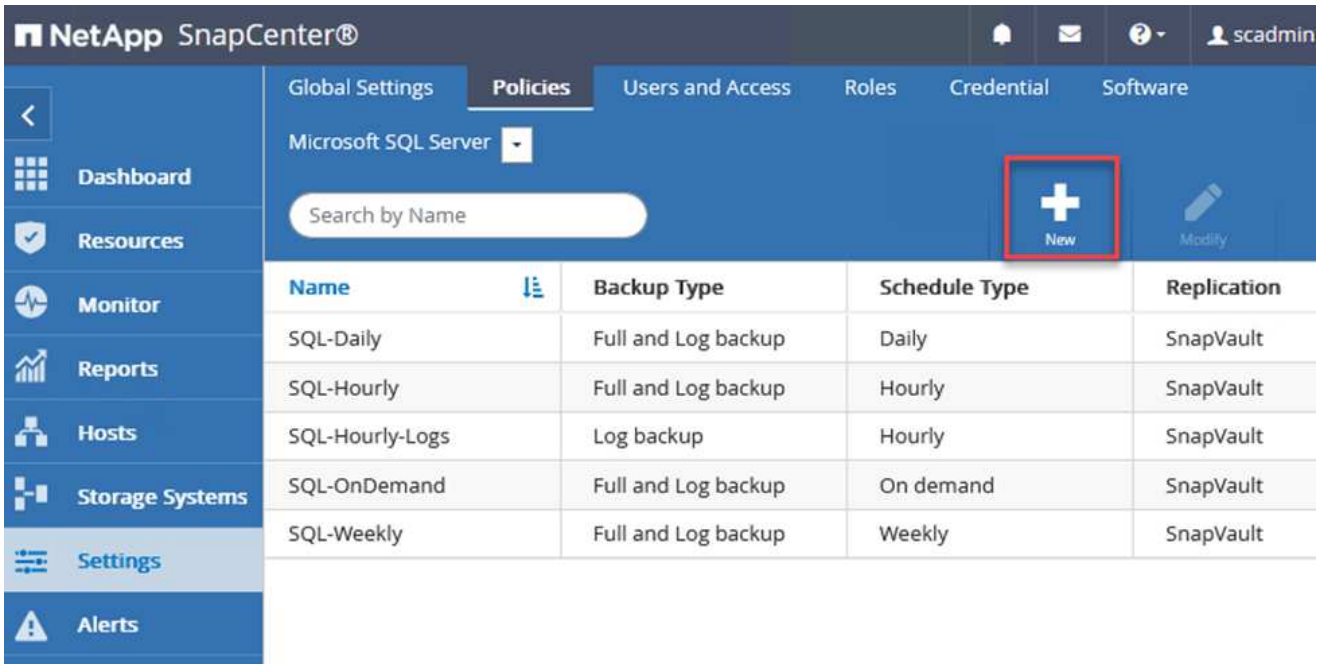
3. Oracleの場合、[ホストの追加]ダイアログボックスの必要なフィールドに入力し、Oracle Databaseプラグインのチェックボックスを選択します。次に、[送信]をクリックして検出プロセスを開始し、ホストをSnapCenterに追加します。


Add Host
Host Type
Linux
Host Name
oraclesrv_11.sddc.netapp.com
Credentials
root
Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux
Oracle Database
SAP HANA
More Options : Port, Install Path, Custom Plug-Ins...
Submit
Cancel

SnapCenter ポリシーを作成する

ポリシーを使用すると、バックアップジョブで使用する特定のルールを設定できます。バックアップスケジュール、レプリケーションタイプ、SnapCenter によるトランザクションログのバックアップと切り捨ての処理方法などが含まれますが、これらに限定されません。

ポリシーには、SnapCenter Webクライアントの設定セクションからアクセスできます。

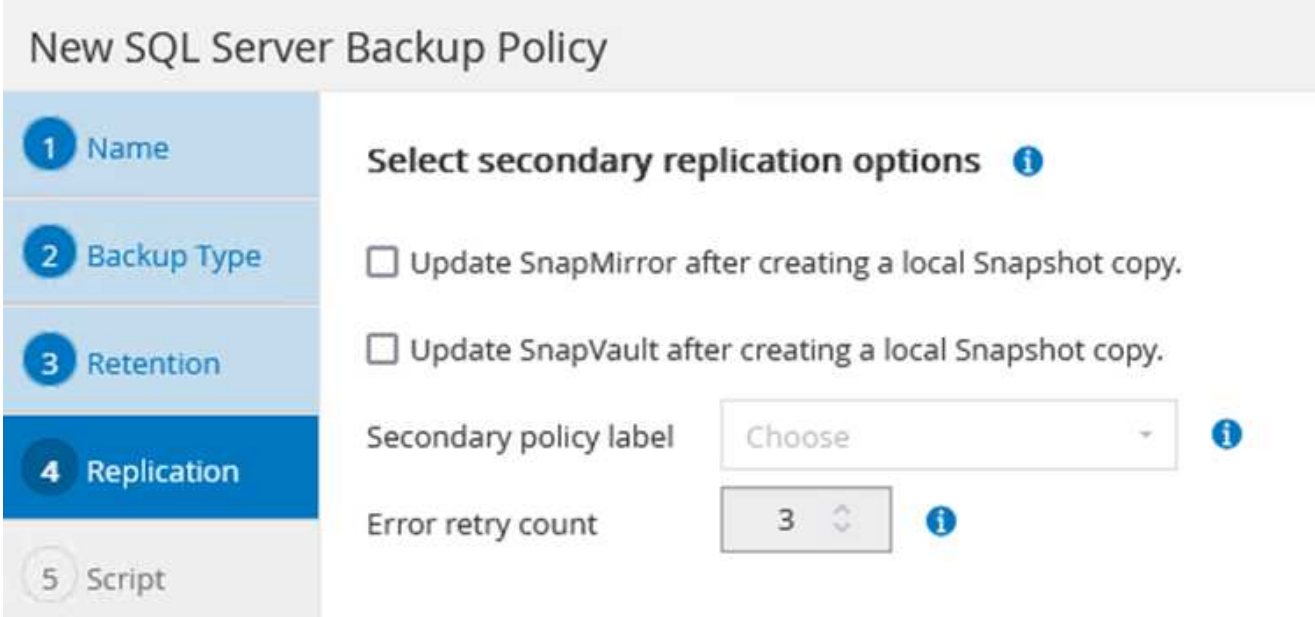


SQL Serverバックアップのポリシー作成の詳細については、を参照して "SnapCenter のドキュメント" ください。

Oracleバックアップのポリシー作成の詳細については、を参照して "SnapCenter のドキュメント"ください。

- 注：*
- ポリシー作成ウィザードの進行中は、Replicationセクションに特別な注意をしてください。このセクションでは、バックアッププロセスで作成するセカンダリSnapMirrorコピーのタイプを指定します。
- 「ローカルSnapshotコピー作成後にSnapMirrorを更新」設定とは、同じクラスタ上にある2台のSVM間にSnapMirror関係が存在する場合に、この関係を更新することを指します。
- [Update SnapVault after creating a local snapshot copy]設定は、2つの独立したクラスタ間、およびオンプレミスのONTAPシステムとCloud Volumes ONTAPまたはFSx ONTAPの間に存在するSnapMirror関係を更新する場合に使用します。

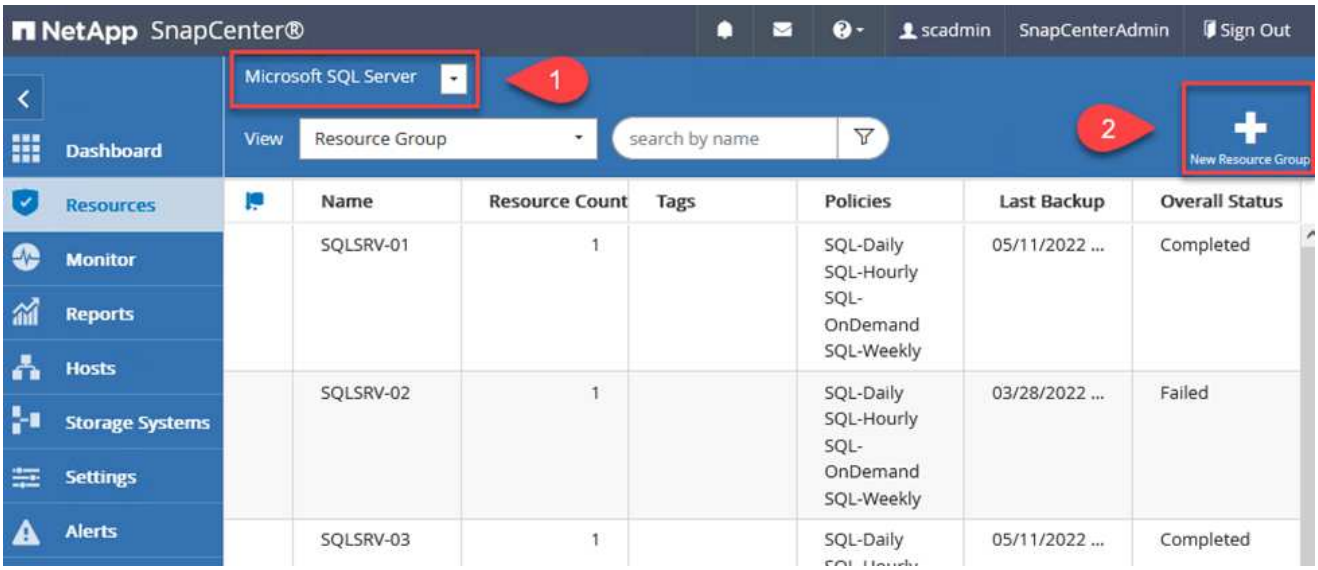
次の図は、この手順を示しており、バックアップポリシーウィザードでどのように表示されるかを示しています。



SnapCenter リソースグループを作成します

リソースグループを使用すると、バックアップに含めるデータベースリソースを選択できます。ポリシーは各リソースに適用されます。

1. 左側のメニューの[Resources]セクションに移動します。
2. ウィンドウの上部で、使用するリソースタイプ（この場合はMicrosoft SQL Server）を選択し、[新しいリソースグループ]をクリックします。



SnapCenter のドキュメントでは、SQL ServerデータベースとOracleデータベースの両方について、リソースグループを作成する手順を詳しく説明しています。

SQLリソースのバックアップについては、を参照して "リンクをクリックしてください"ください。

Oracleリソースのバックアップについては、を参照して "リンクをクリックしてください"ください。

Veeam Backup Serverを導入して設定します

Veeam Backup & Replicationソフトウェアは、解決策 で、アプリケーション仮想マシンのバックアップと、Veeamスケールアウトバックアップリポジトリ（SOBR）を使用したAmazon S3バケットへのバックアップのコピーのアーカイブを行うために使用します。Veeamは、この解決策 内のWindowsサーバに導入されます。Veeamの導入に関する具体的なガイダンスについては、を参照して "Veeamヘルプセンターのテクニカルドキュメント"ください。

Veeamスケールアウトバックアップリポジトリを設定

ソフトウェアを導入してライセンスを設定したら、バックアップジョブのターゲットストレージとしてスケールアウトバックアップリポジトリ（SOBR）を作成できます。また、ディザスタリカバリ用にVMデータのバックアップ用にS3バケットをオフサイトに配置することも必要です。

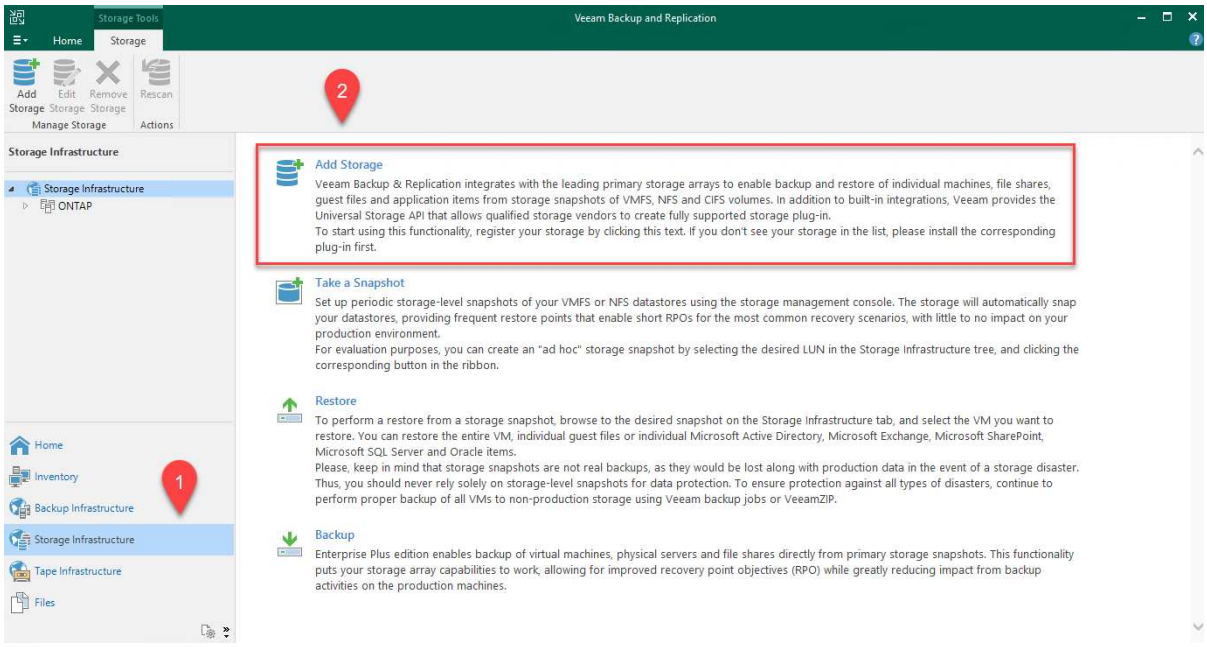
作業を開始する前に、次の前提条件を確認してください。

1. バックアップのターゲットストレージとして、オンプレミスのONTAP システム上にSMBファイル共有を作成します。
2. SOBRに含めるAmazon S3バケットを作成します。これは、オフサイトバックアップ用のリポジトリです。

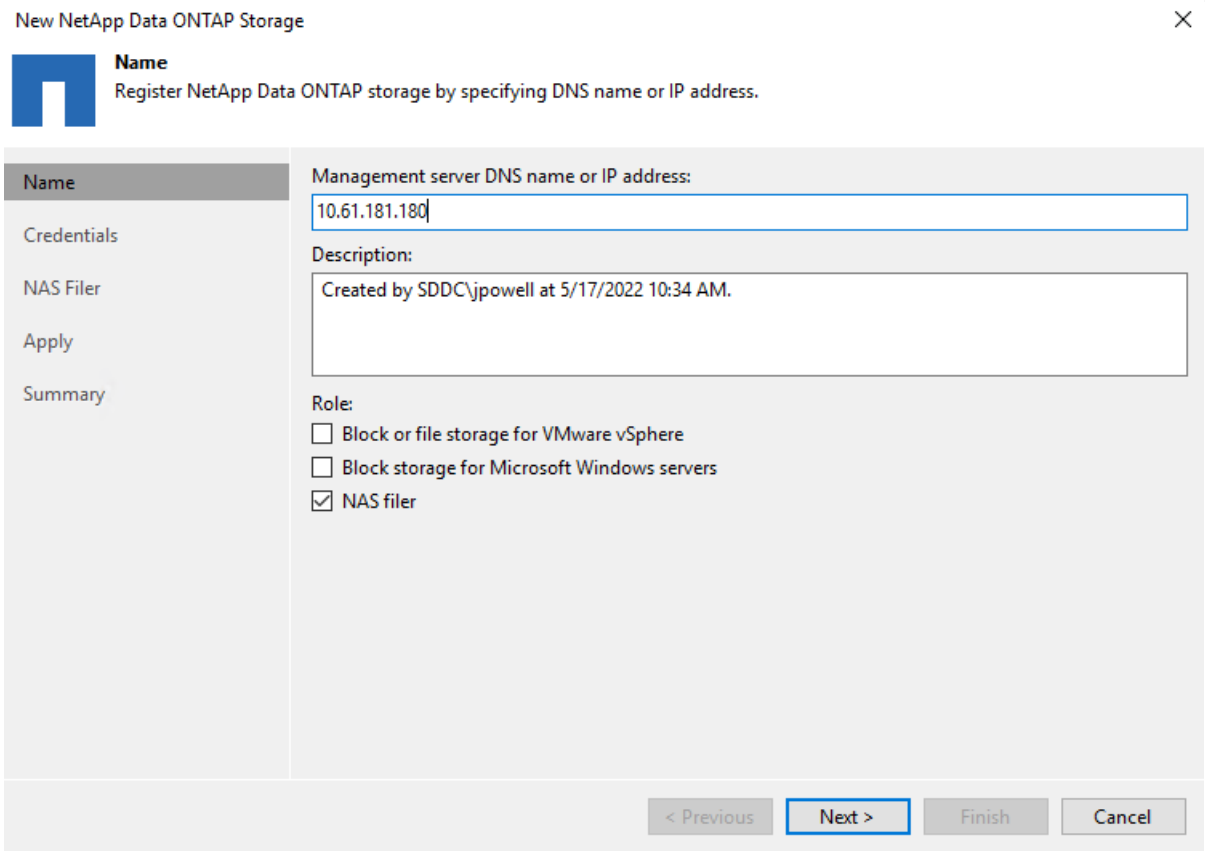
VeeamにONTAP ストレージを追加します

まず、ONTAP ストレージクラスタと関連するSMB / NFSファイルシステムをストレージインフラとしてVeeamに追加します。

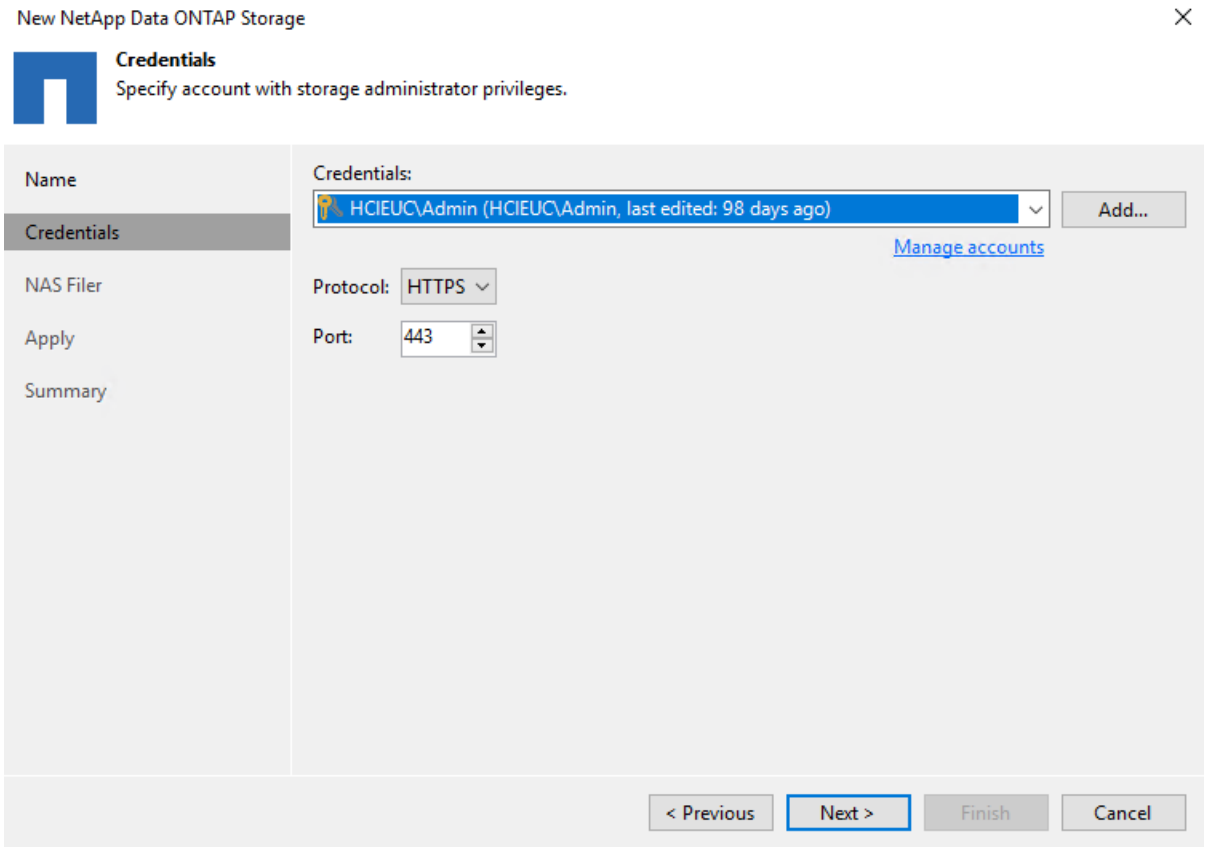
1. Veeamコンソールを開き、ログインします。[Storage Infrastructure]に移動し、[Add Storage]を選択します。



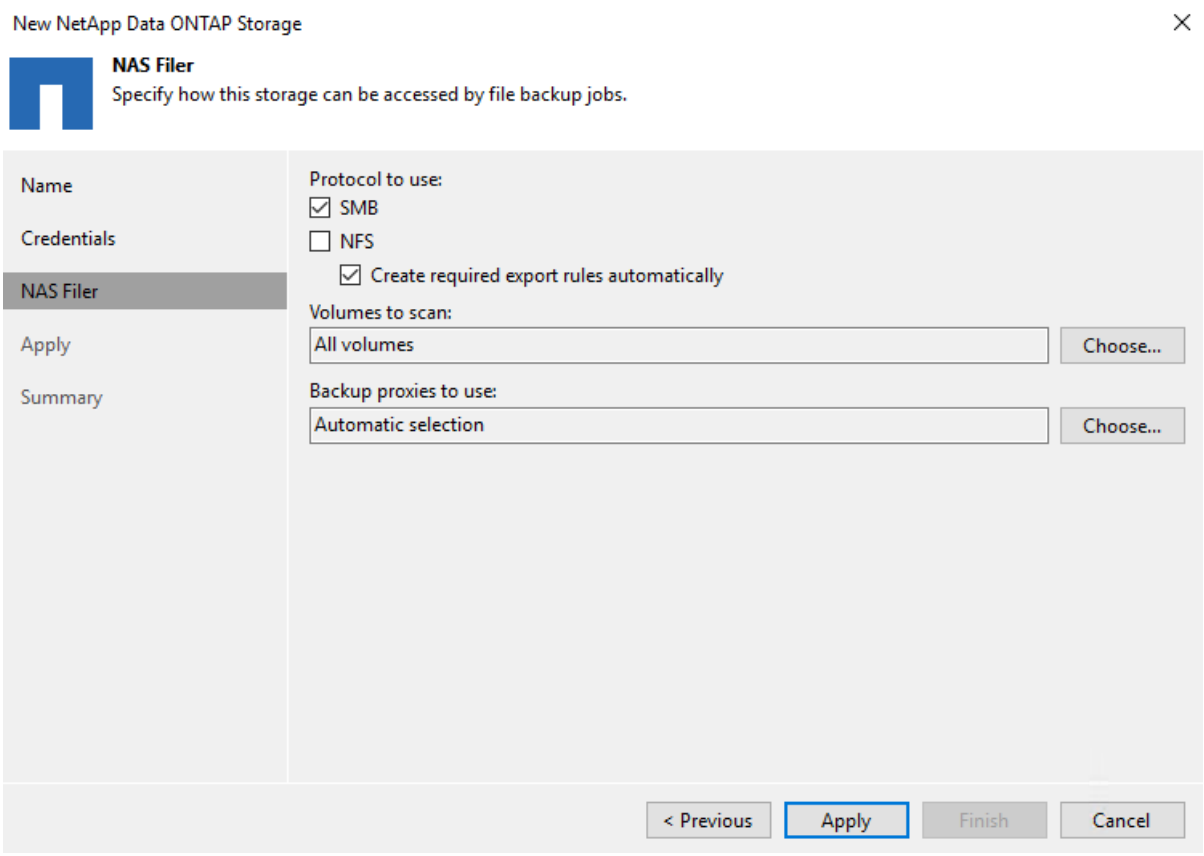
2. ストレージの追加ウィザードで、ストレージベンダーとしてネットアップを選択し、Data ONTAP を選択します。
3. 管理IPアドレスを入力し、NASファイラーボックスをオンにします。[Next]をクリックします。



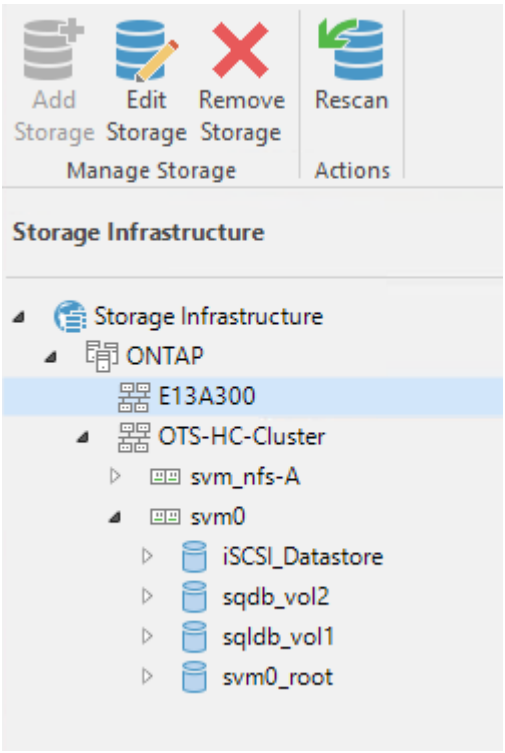
4. ONTAP クラスタにアクセスするためのクレデンシャルを追加してください。



5. NASファイラーページで、スキャンするプロトコルを選択し、次へを選択します。

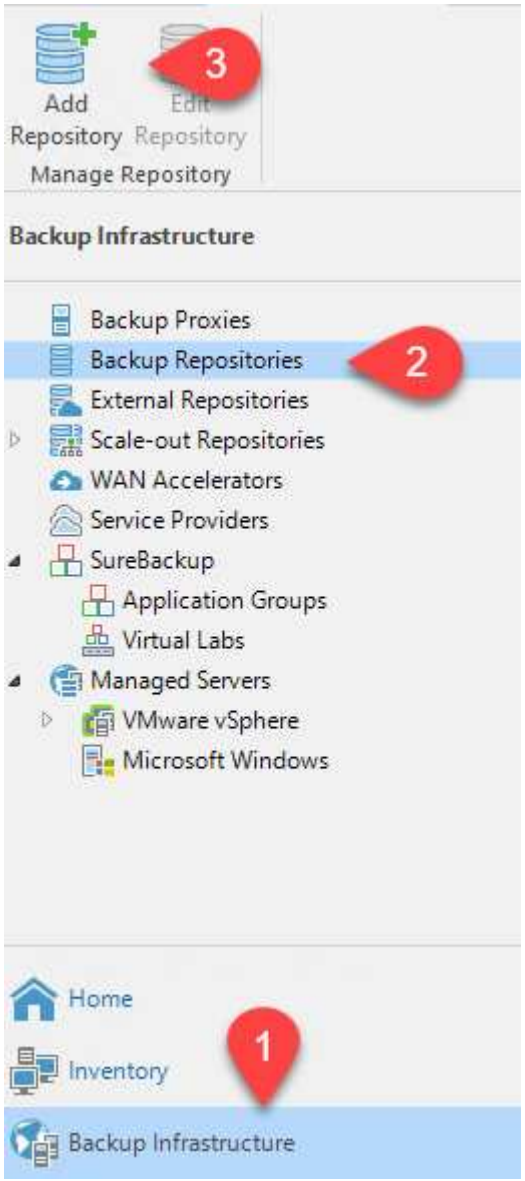


6. ウィザードのApplyページとSummaryページを設定し、Finishをクリックしてストレージ検出プロセスを開始します。スキャンが完了すると、ONTAP クラスタがNASファイラーとともに使用可能なリソースとして追加されます。

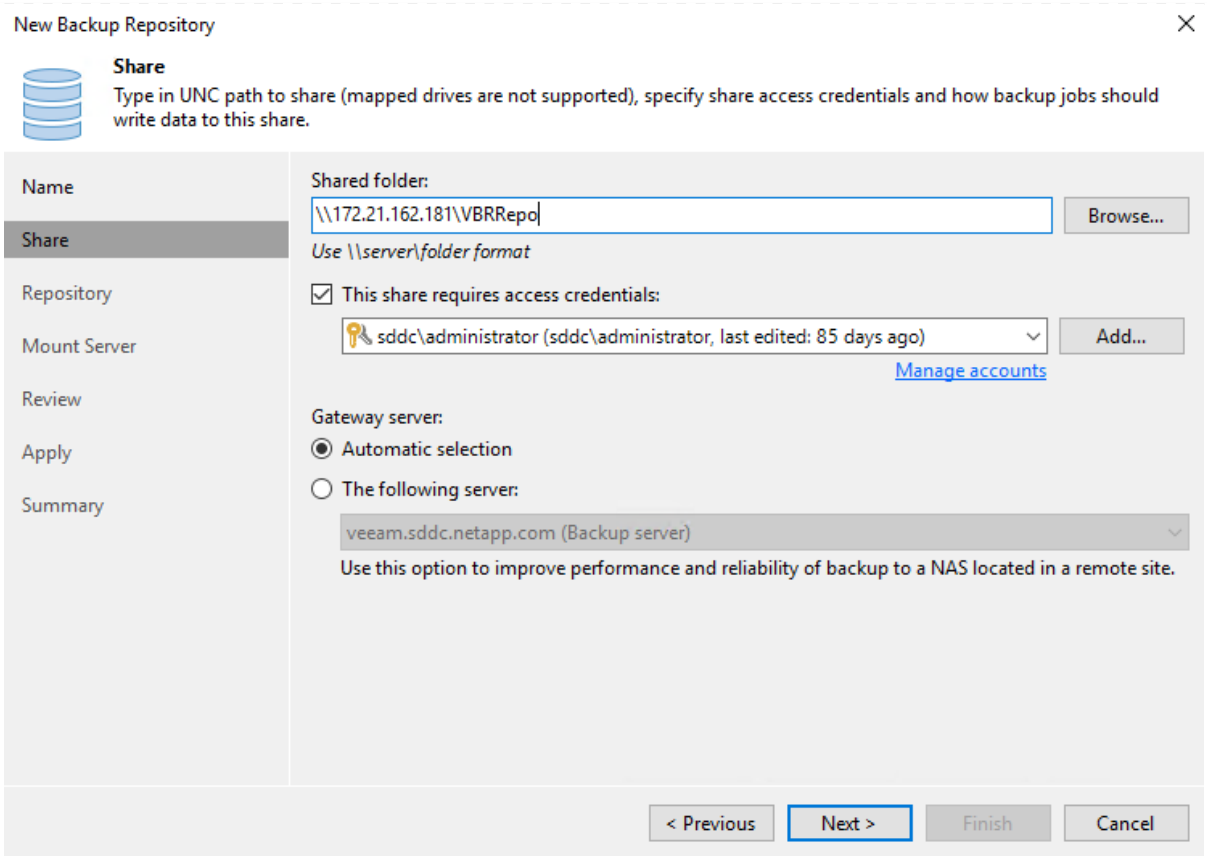


7. 新たに検出されたNAS共有を使用して、バックアップリポジトリを作成します。[バックアップインフラストラクチャ]で、[バックアップリポジトリ]を選択し、[リポジトリの追加]メニューア

イテムをクリックします。



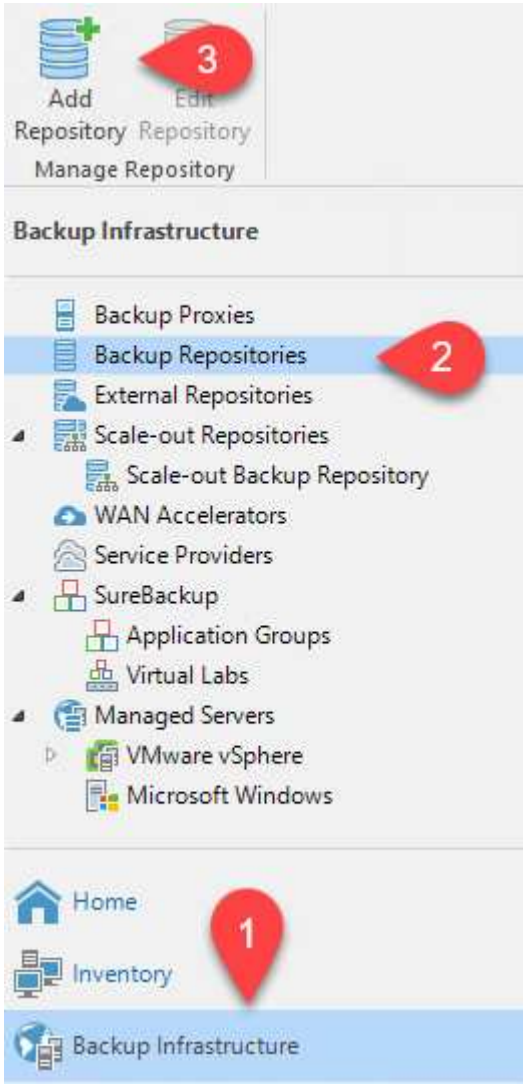
8. リポジトリを作成するには、[新規バックアップリポジトリ]ウィザードのすべての手順に従います。Veeam Backup Repositoriesの作成の詳細については、を参照して "Veeamの製品ドキュメント"ください。


New Backup Repository
Share
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Shared folder:
\\172.21.162.181\VBRRepo
Browse...
Use \\server\folder format
This share requires access credentials:
sddc\administrator (sddc\administrator, last edited: 85 days ago)
Add...
Manage accounts
Gateway server:
Automatic selection
The following server:
veeam.sddc.netapp.com (Backup server)
Use this option to improve performance and reliability of backup to a NAS located in a remote site.
< Previous
Next >
Finish
Cancel

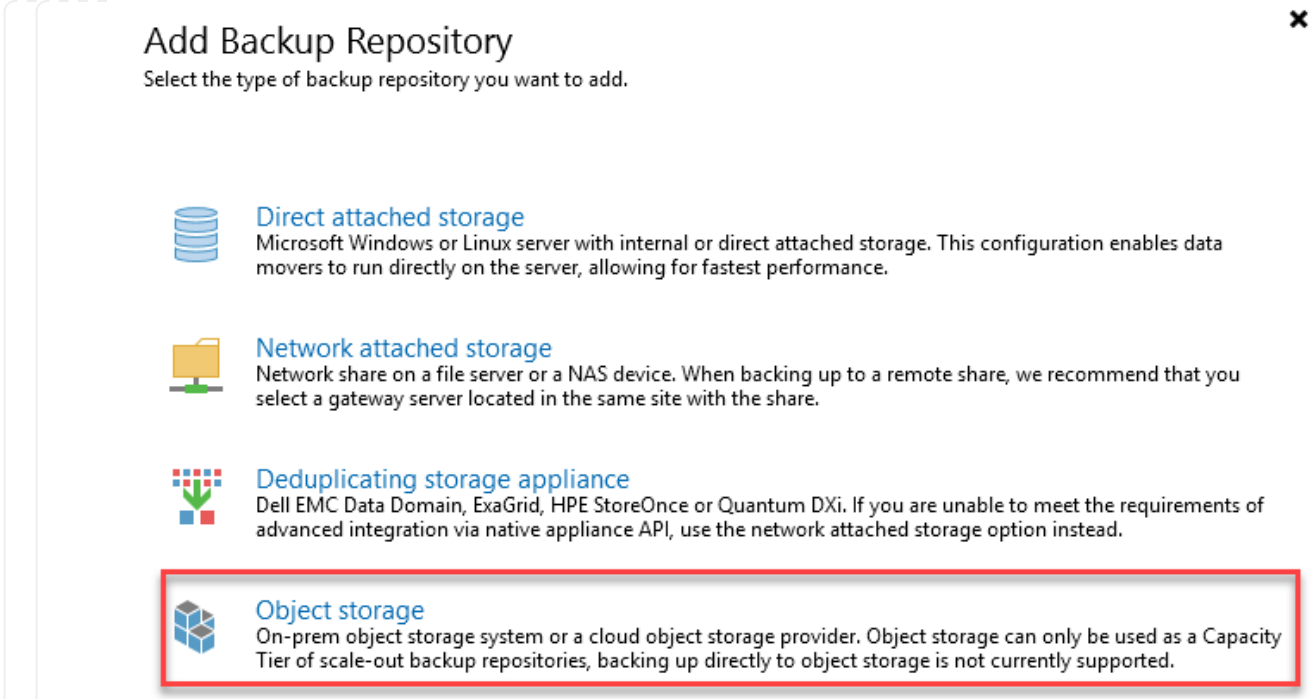
Amazon S3バケットをバックアップリポジトリとして追加します

次の手順では、Amazon S3ストレージをバックアップリポジトリとして追加します。

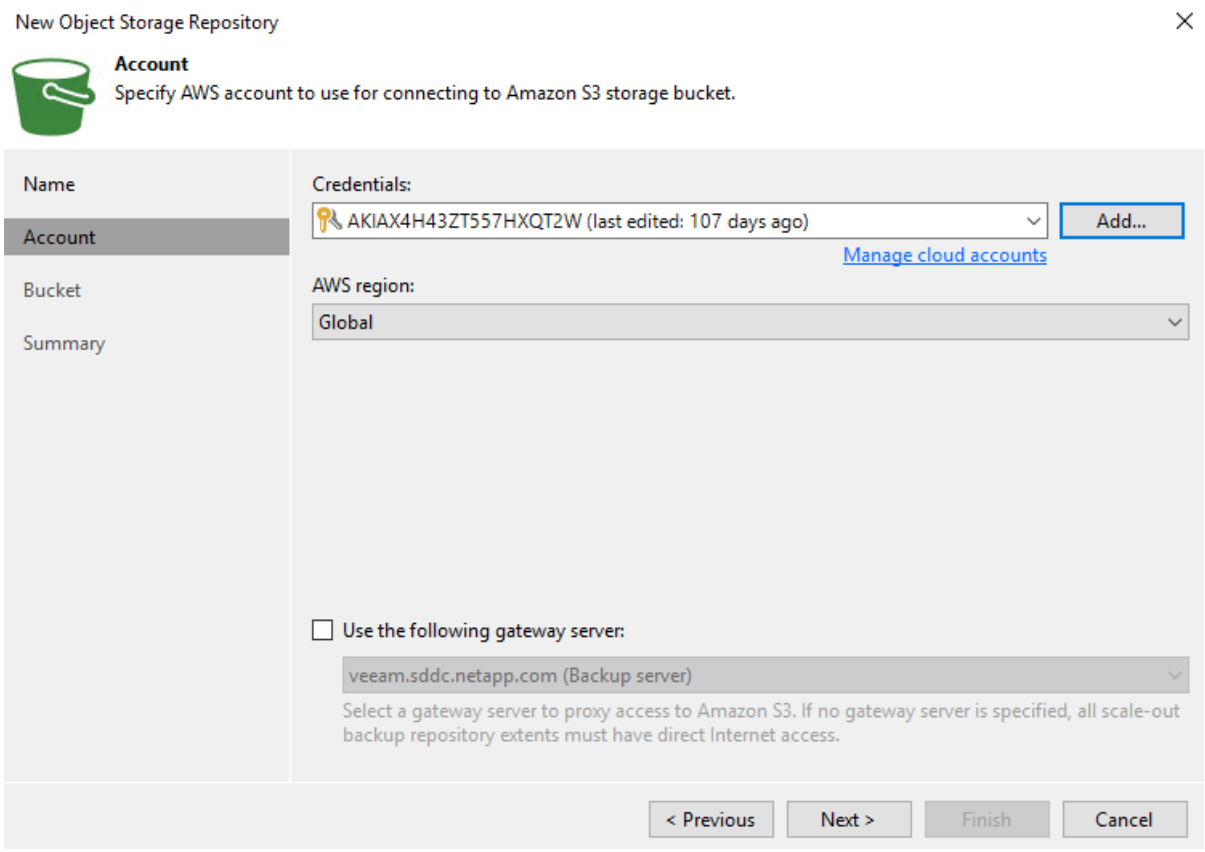
1. [バックアップインフラストラクチャ]>[バックアップリポジトリ]に移動します。[リポジトリの追加]をクリックします



2. バックアップリポジトリの追加ウィザードで、オブジェクトストレージ、Amazon S3の順に選択します。これにより、新規オブジェクトストレージリポジトリウィザードが起動します。



3. オブジェクトストレージリポジトリの名前を入力し、次へをクリックします。
4. 次のセクションで、クレデンシャルを入力します。AWSのアクセスキーとシークレットキーが必要です。

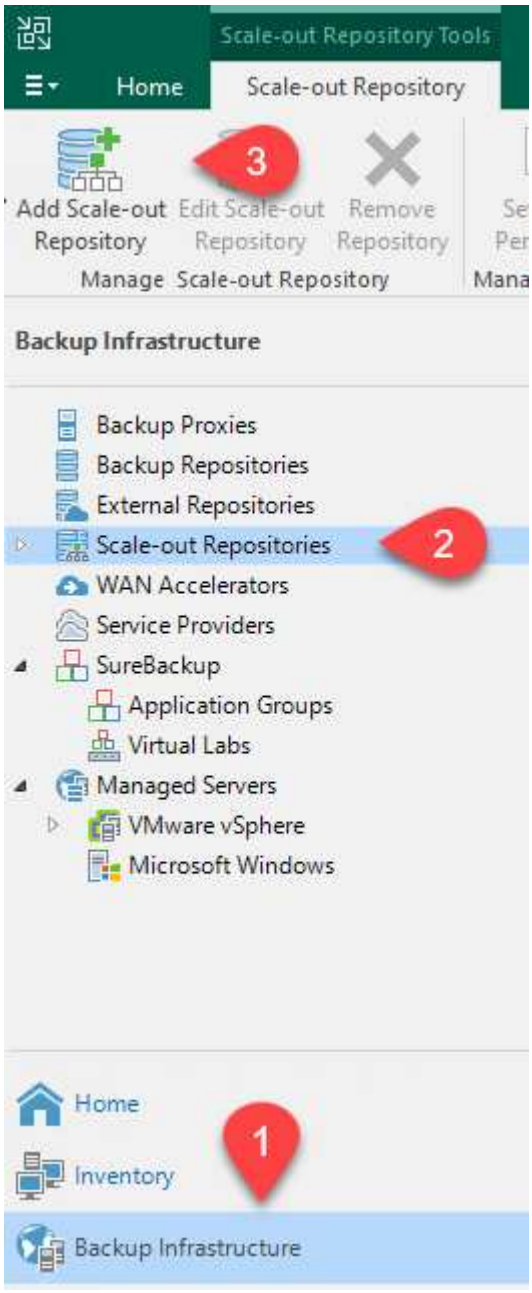


5. Amazon設定がロードされたら、データセンター、バケット、およびフォルダを選択し、適用をクリックします。最後に、[完了]をクリックしてウィザードを終了します。

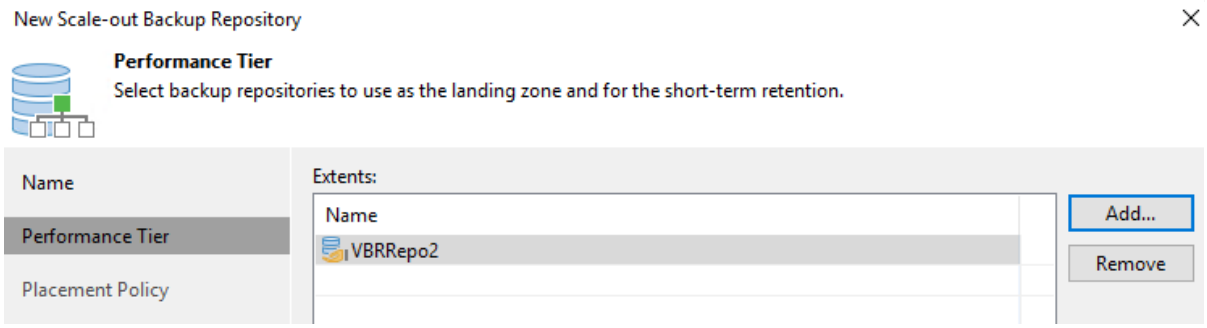
スケールアウトバックアップリポジトリの作成

これでVeeamにストレージリポジトリを追加したので、SOBRを作成して、ディザスタリカバリ用にオフサイトのAmazon S3オブジェクトストレージにバックアップコピーを自動的に階層化できます。

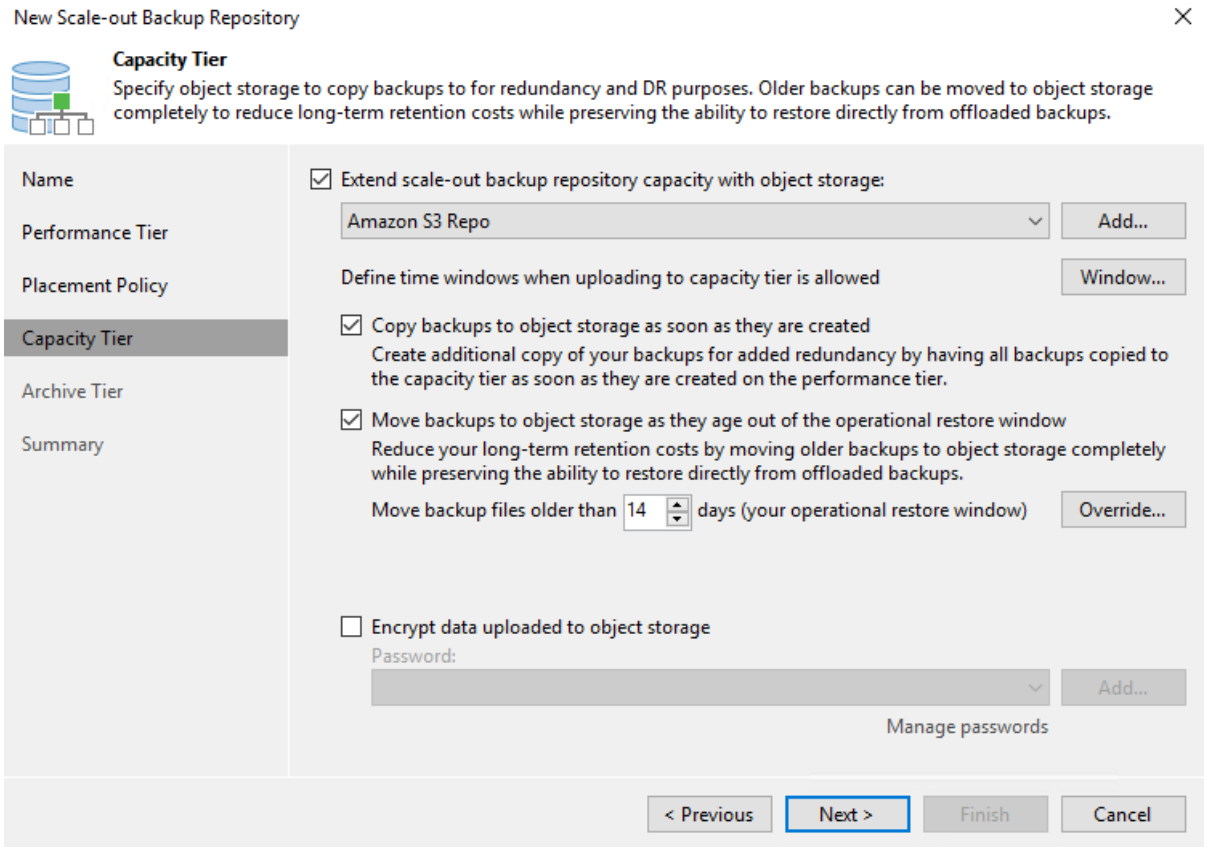
1. [バックアップインフラストラクチャ]で、[スケールアウトリポジトリ]を選択し、[スケールアウトリポジトリの追加]メニューアイテムをクリックします。



2. [新しいスケールアウトバックアップリポジトリ]で'SOBRの名前を指定し'[次へ]をクリックします
3. 階層のパフォーマンスについて、ローカルのONTAP クラスタにあるSMB共有を含むバックアップリポジトリを選択します。



4. 配置ポリシーで、要件に基づいて[データの局所性]または[パフォーマンス]を選択します。[次へ]を選択し
5. 大容量階層の場合は、SOBRとAmazon S3オブジェクトストレージを拡張します。ディザスタリカバリのために、セカンダリバックアップをタイムリーに提供できるように、バックアップを作成したらすぐにオブジェクトストレージにコピーするを選択します。



6. 最後に、[適用（Apply）]と[完了（Finish）]を選択してSOBRの作成を確定する。

スケールアウトバックアップリポジトリジョブを作成

Veeamを設定する最後の手順は、新しく作成したバックアップ先のSOBRを使用してバックアップジョブを作成することです。バックアップジョブの作成は、ストレージ管理者の作業内容に含まれる通常の作業であり、ここでは詳細な手順については説明しません。Veeamでのバックアップジョブの作成の詳細については、を参照して "Veeam Help Centerテクニカルドキュメント"ください。

BlueXPのバックアップとリカバリのツールと構成

アプリケーションVMおよびデータベースボリュームをAWSで実行されているVMware Cloud Volumeサービスにフェイルオーバーするには、SnapCenter サーバとVeeam Backup and Replication Serverの両方の実行中のインスタンスをインストールして設定する必要があります。フェイルオーバーが完了したら、オンプレミスのデータセンターへのフェイルバックが計画されて実行されるまで、通常のバックアップ処理を再開するようにこれらのツールも設定する必要があります。

セカンダリ**Windows SnapCenter** サーバを導入します

SnapCenter サーバは、VMware Cloud SDDCに導入するか、VPC内のEC2インスタンスにインストールし、VMware Cloud環境にネットワーク接続します。

SnapCenter ソフトウェアはNetApp Support Siteから入手でき、ドメインまたはワークグループ内にあるMicrosoft Windowsシステムにインストールできます。詳細な計画ガイドとインストール手順については、を参照し "ネットアップドキュメントセンター"てください。

SnapCenterソフトウェアは、から入手でき "リンクをクリックしてください"ます。

セカンダリ**Windows SnapCenter** サーバを設定します

FSX ONTAP にミラーリングされたアプリケーション・データのリストアを実行するには'まずオンプレミスのSnapCenter データベースのフル・リストアを実行する必要がありますこのプロセスが完了すると、VMとの通信が再確立され、プライマリストレージとしてFSX ONTAP を使用してアプリケーションのバックアップを再開できるようになります。

これを行うには、SnapCenter サーバで次の項目を完了する必要があります。

1. コンピュータ名を、元のオンプレミスSnapCenter サーバと同じ名前に設定します。
2. VMware CloudおよびFSX ONTAP インスタンスと通信するためのネットワークを設定します。
3. 手順 を完了してSnapCenter データベースをリストアします。
4. SnapCenter がディザスタリカバリモードになっていることを確認し、FSXがバックアップ用のプライマリストレージになったことを確認します。
5. リストアした仮想マシンとの通信が再確立されたことを確認します。

セカンダリ**Veeam Backup & Replication**サーバを導入

Veeam Backup & Replicationサーバは、AWS上のVMware CloudまたはEC2インスタンス上のWindowsサーバにインストールできます。実装に関する詳細なガイダンスについては、を参照して "Veeam Help Centerテクニカルドキュメント"ください。

セカンダリ**Veeam Backup & Replication**サーバの設定

Amazon S3ストレージにバックアップされた仮想マシンをリストアするには、WindowsサーバにVeeamサーバをインストールし、VMware Cloud、FSX ONTAP 、および元のバックアップリポジトリが格納されたS3バケットと通信するように設定する必要があります。また、リストア後にVMの新しいバックアップを実行するために、FSX ONTAP に新しいバックアップリポジトリが設定されている必要があります。

このプロセスを実行するには、次の項目を完了する必要があります。

1. VMware Cloud、FSX ONTAP 、および元のバックアップリポジトリを含むS3バケットと通信するためのネットワークを設定します。
2. FSX ONTAP 上のSMB共有を新しいバックアップリポジトリとして設定します。
3. スケールアウトバックアップリポジトリの一部として使用されていた元のS3バケットをオンプレミスにマウントします。
4. VMをリストアしたら、SQL VMとOracle VMを保護するための新しいバックアップジョブを確立します。

Veeamを使用したVMのリストアの詳細については、セクションを参照して"アプリケーションVMをVeeam Full Restoreでリストアします"ください。

ディザスタリカバリに備えた**SnapCenter** データベースバックアップ

SnapCenter を使用すると、災害発生時にSnapCenter サーバをリカバリできるように、基盤となるMySQLデータベースおよび設定データのバックアップとリカバリを行うことができます。解決策 では、VPC内のAWS EC2インスタンスでSnapCenter データベースと設定をリカバリしました。SnapCenterのディザスタリカバリの詳細については、を参照してください "リンクをクリックしてください"。

SnapCenter バックアップの前提条件

SnapCenter バックアップを実行するには、次の前提条件が必要です。

- オンプレミスのONTAP システムに作成されたボリュームとSMB共有。バックアップされたデータベースと構成ファイルを検索します。
- オンプレミスのONTAP システムと、AWSアカウントのFSXまたはCVOとの間のSnapMirror関係。この関係は、バックアップされたSnapCenter データベースおよび構成ファイルを含むSnapshotの転送に使用されます。
- EC2インスタンスまたはVMware Cloud SDDC内のVMに、クラウドアカウントにWindows Serverをインストールします。
- SnapCenter は、VMware CloudのWindows EC2インスタンスまたはVMにインストールします。

SnapCenter のバックアップとリストアのプロセスの概要

- バックアップのdbファイルと構成ファイルをホストするボリュームをオンプレミスのONTAP システムに作成します。
- オンプレミスとFSX/CVOの間にSnapMirror関係を設定
- SMB共有をマウント
- APIタスクを実行するためのSwagger承認トークンを取得します。
- dbのリストア・プロセスを開始します。
- xcopyユーティリティを使用して、dbおよびconfigファイルのローカルディレクトリをSMB共有にコピーします。
- FSXで、ONTAP ボリュームのクローンを作成する（オンプレミスからSnapMirror経由でコピーする）。
- FSXからEC2/VMware CloudにSMB共有をマウントします。
- SMB共有からローカルディレクトリにリストアディレクトリをコピーします。
- SwaggerからSQL Serverのリストアプロセスを実行します。

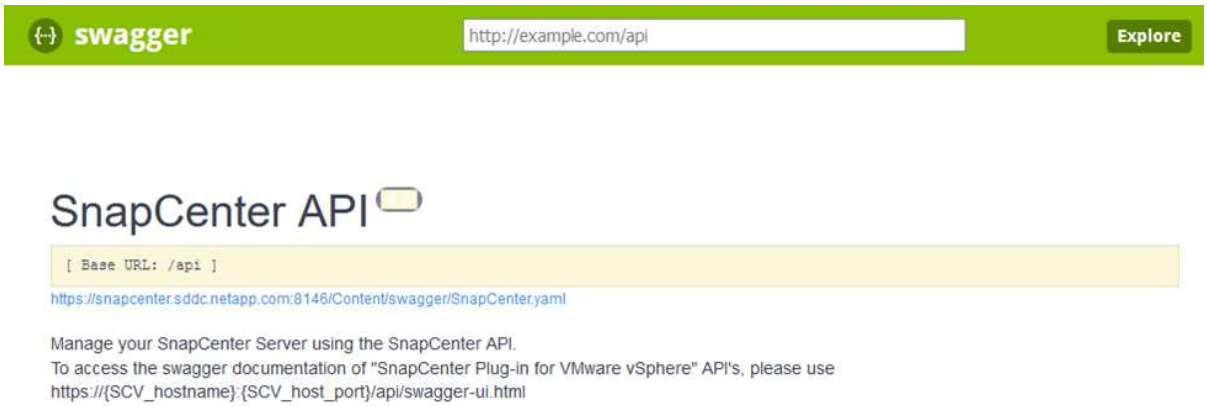
SnapCenter データベースと設定をバックアップします

SnapCenter は、REST APIコマンドを実行するためのWebクライアントインターフェイスを提供します。Swaggerを使用したREST APIへのアクセスについては、SnapCenterのドキュメントを参照してください "リンクをクリックしてください"。

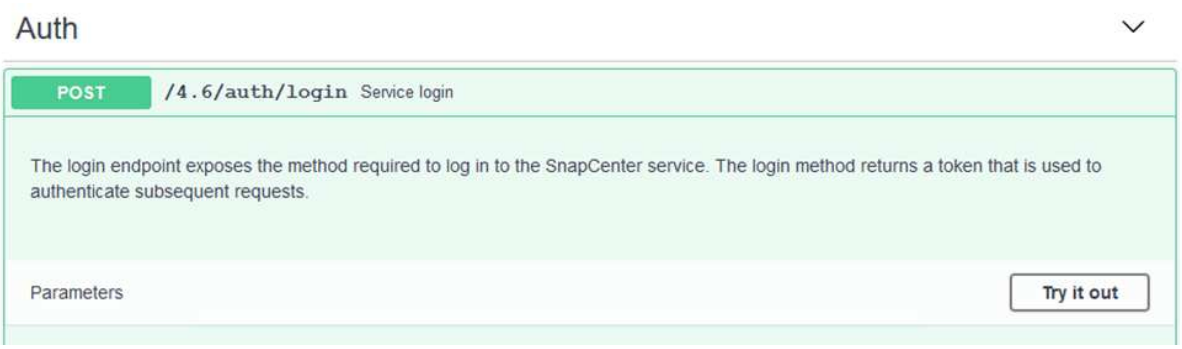
Swaggerにログインし、認証トークンを取得します

Swaggerページに移動したら、認証トークンを取得してデータベースリストアプロセスを開始する必要があります。

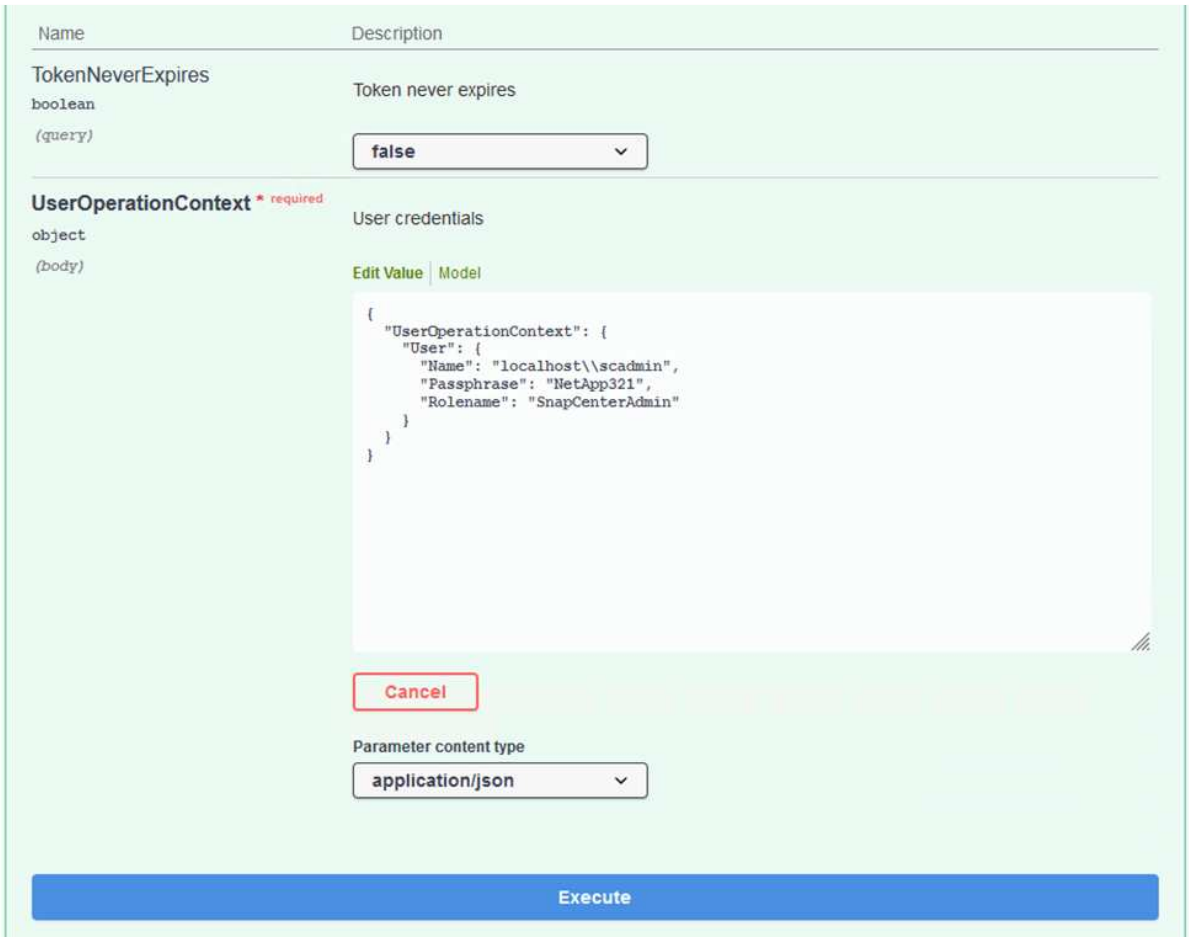
1. SnapCenter Swagger API Webページ（\ *https*：//< *SnapCenter*サーバ*IP*>：*8146/swagger/*）にアクセスします。



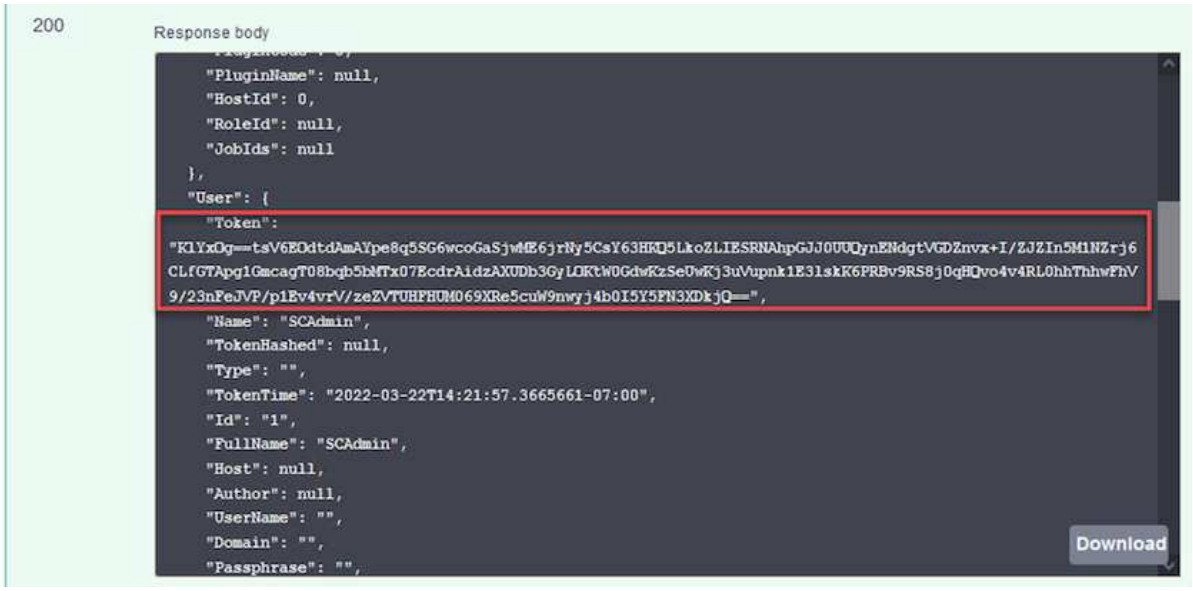
2. [Auth]セクションを展開し、[Try it Out]をクリックします。



3. UserOperationContext領域で、SnapCenter の資格情報と役割を入力し、Executeをクリックします。



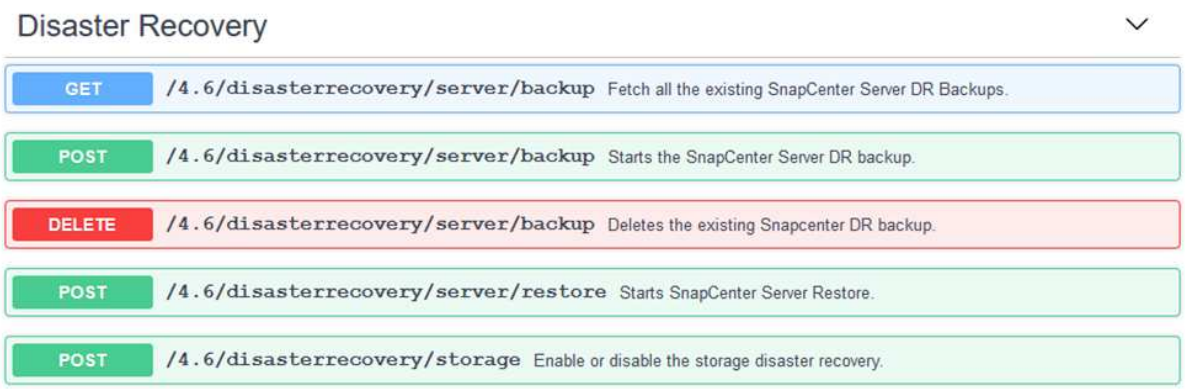
4. 以下の応答本文では、トークンを確認できます。バックアッププロセス実行時に、認証用のトークンテキストをコピーします。



SnapCenter データベースのバックアップを実行する

次に、Swaggerページのディザスタリカバリ領域に移動して、SnapCenter バックアッププロセスを開始します。

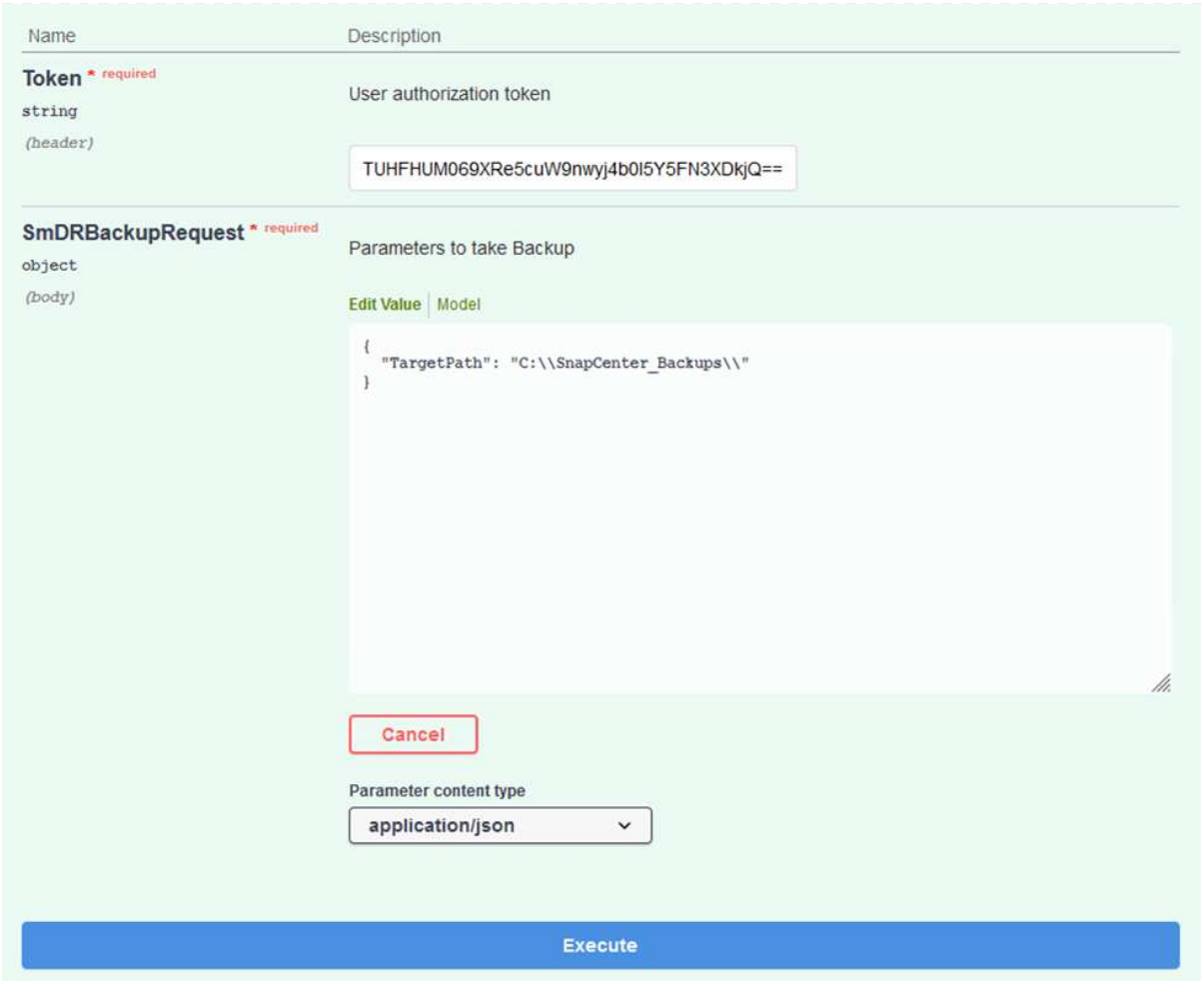
1. [Disaster Recovery]領域をクリックして展開します。



2. セクションを展開し `/4.6/disasterrecovery/server/backup`、[Try it out]をクリックします。

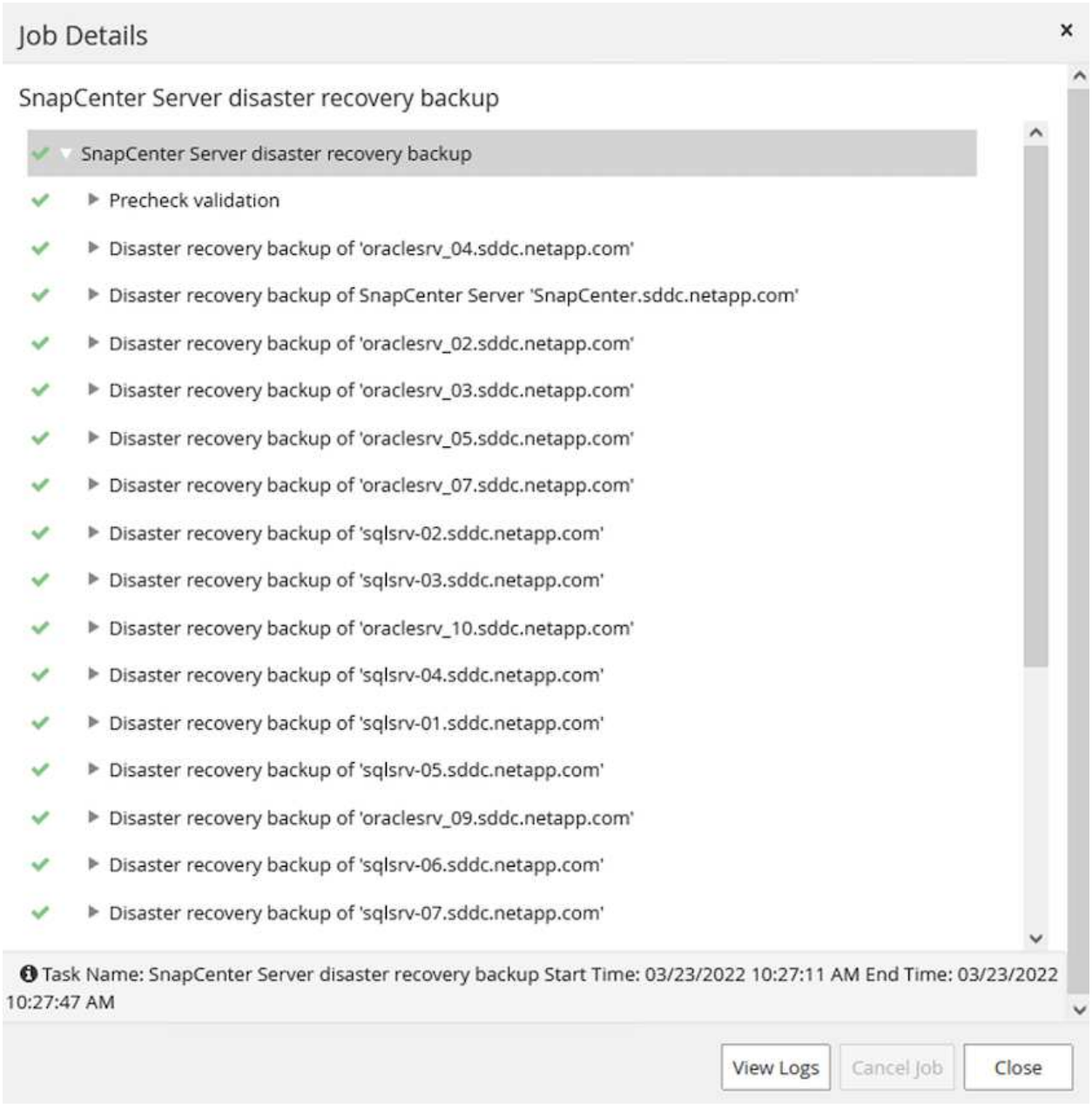
3. SmDRBackupRequestセクションで、正しいローカルターゲットパスを追加し、Executeを選択してSnapCenter データベースと設定のバックアップを開始します。

> バックアッププロセスでは、NFSまたはCIFSのファイル共有に直接バックアップすることはできません。


Name
Description
Token * required
string
(header)
User authorization token
TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==
SmDRBackupRequest * required
object
(body)
Parameters to take Backup
Edit Value
Model
{
"TargetPath": "C:\\SnapCenter_Backups\\"
}
Cancel
Parameter content type
application/json
Execute

SnapCenter からバックアップジョブを監視

データベースリストアプロセスを開始するときに、SnapCenter にログインしてログファイルを確認します。Monitorセクションでは、SnapCenter サーバのディザスタリカバリバックアップの詳細を表示できます。



XCOPYユーティリティを使用してデータベースバックアップファイルを**SMB**共有にコピーします

次に、SnapCenter サーバ上のローカルドライブから、SnapMirrorによってデータがAWSのFSXインスタンス上のセカンダリサイトにコピーされるCIFS共有にバックアップを移動する必要があります。ファイルのアクセス権を保持する特定のオプションを指定してxcopyを使用します

管理者としてコマンドプロンプトを開きます。コマンドプロンプトで、次のコマンドを入力します。

```
xcopy  <Source_Path>  \\<Destination_Server_IP>\<Folder_Path> /O /X
/E /H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O
/X /E /H /K
```

フェイルオーバー

災害はプライマリサイトで発生します

プライマリオンプレミスのデータセンターで災害が発生した場合のシナリオとして、AWSでVMware Cloudを使用して、Amazon Web Servicesインフラにあるセカンダリサイトへのフェイルオーバーがあります。仮想マシンとオンプレミスのONTAP クラスタにはアクセスできなくなると仮定しています。また、SnapCenter とVeeamの仮想マシンはどちらもアクセスできなくなり、2次サイトで再構築する必要があります。

このセクションでは、インフラからクラウドへのフェイルオーバーについて説明します。ここでは、次のトピックについて説明します。

- SnapCenter データベースのリストア：新しいSnapCenter サーバが確立されたら、MySQLデータベースと構成ファイルをリストアし、データベースをディザスタリカバリモードに切り替えて、セカンダリFSXストレージをプライマリストレージデバイスにします。
- Veeam Backup & Replicationを使用してアプリケーション仮想マシンをリストアします。VMバックアップを含むS3ストレージを接続し、バックアップをインポートして、AWS上のVMware Cloudにリストアします。
- SnapCenter を使用してSQL Serverアプリケーションデータをリストアします。
- SnapCenter を使用してOracleアプリケーションのデータをリストアします。

SnapCenter データベースのリストアプロセス

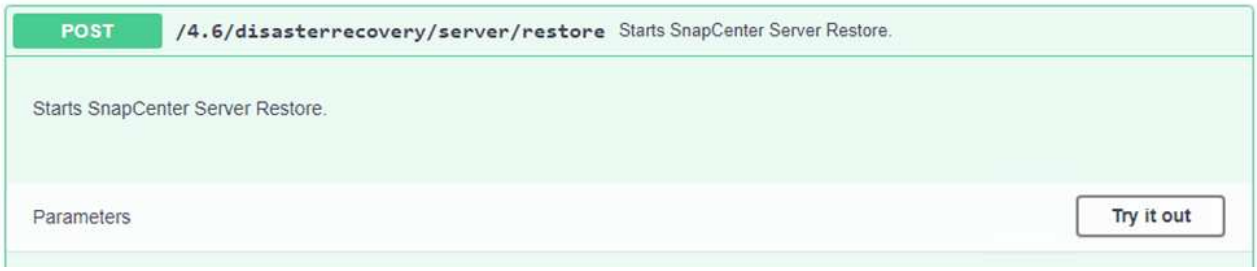
SnapCenter では、MySQLデータベースおよび構成ファイルのバックアップとリストアが可能なため、ディザスタリカバリのシナリオがサポートされます。これにより、管理者はSnapCenter データベースの定期的なバックアップをオンプレミスのデータセンターで保持し、そのデータベースをセカンダリSnapCenter データベースにリストアすることができます。

リモートSnapCenter サーバ上のSnapCenter バックアップファイルにアクセスするには、次の手順を実行します。

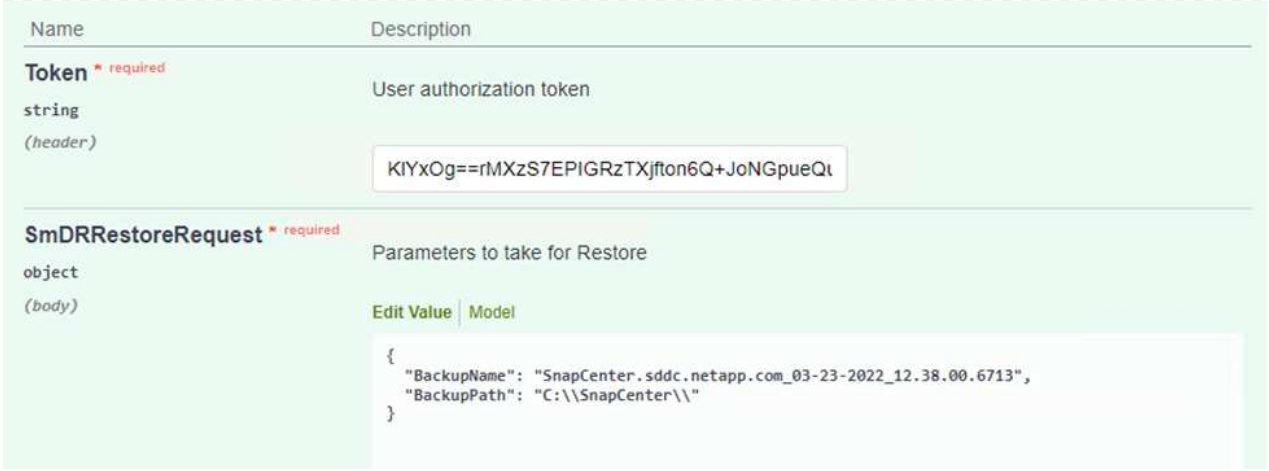
1. ボリュームを読み取り/書き込み可能にするFSXクラスタからSnapMirror関係を解除します。
2. 必要に応じてCIFSサーバを作成し、クローニングされたボリュームのジャンクションパスを参照するCIFS共有を作成します。
3. xcopyを使用して、セカンダリSnapCenter システムのローカルディレクトリにバックアップファイルをコピーします。
4. SnapCenter v4.6をインストールします。
5. SnapCenter サーバのFQDNが元のサーバと同じであることを確認します。これは、データベースのリストアを正常に実行するために必要です。

リストア・プロセスを開始するには、次の手順を実行します。

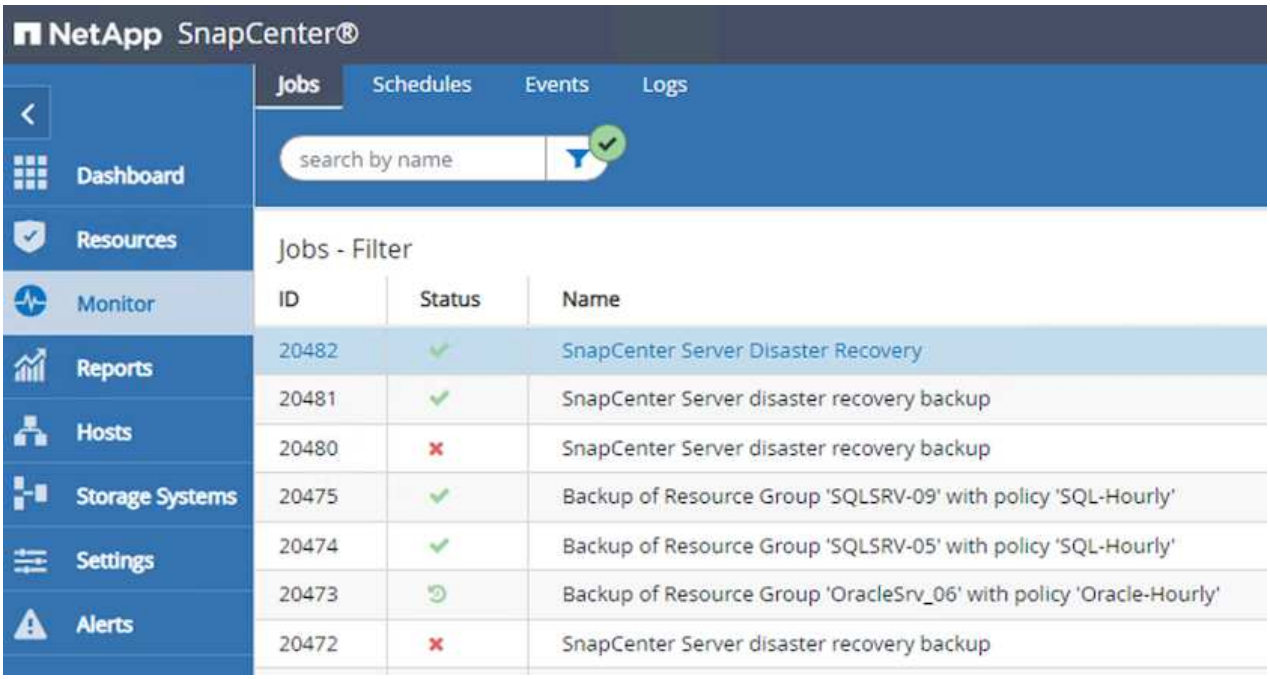
1. セカンダリSnapCenter サーバのSwagger API Webページに移動し、前述の手順に従って認証トークンを取得します。
2. Swaggerページの[Disaster Recovery]セクションに移動し、を選択して `/4.6/disasterrecovery/server/restore`[Try it out]をクリックします。

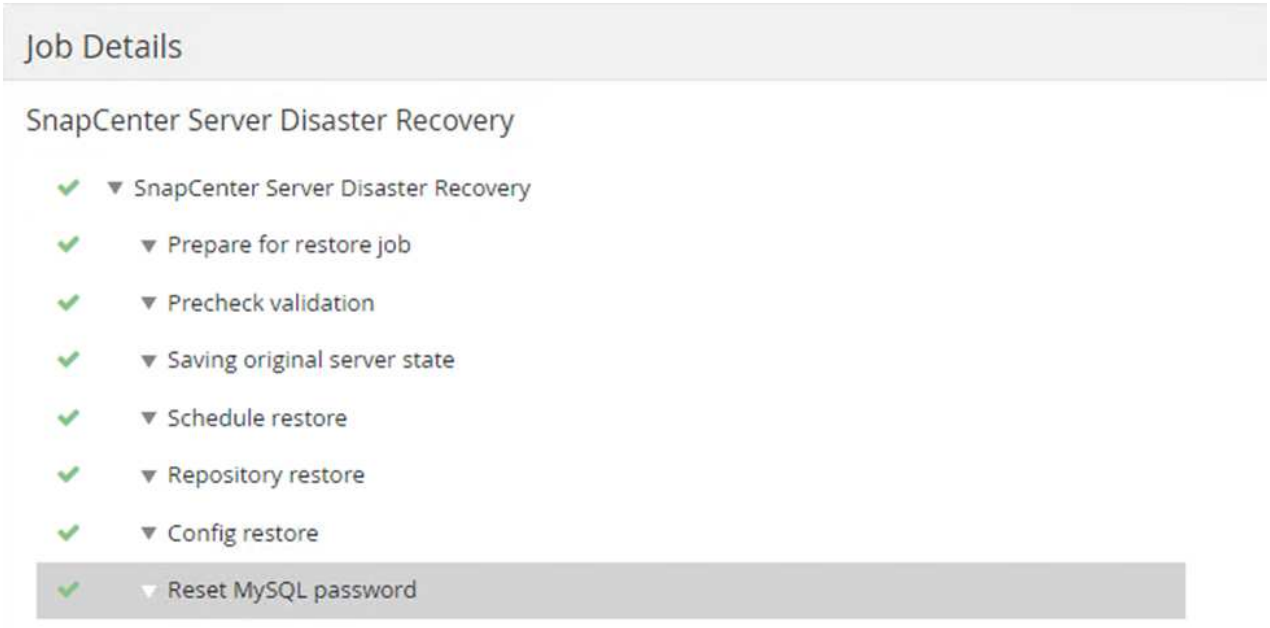


3. 認証トークンに貼り付けて、SmDRRestarterRequestセクションで、バックアップ名とセカンダリSnapCenter サーバのローカルディレクトリに貼り付けます。



4. Executeボタンを選択して'リストア・プロセスを開始します
5. SnapCenter で、監視セクションに移動してリストアジョブの進捗状況を確認します。





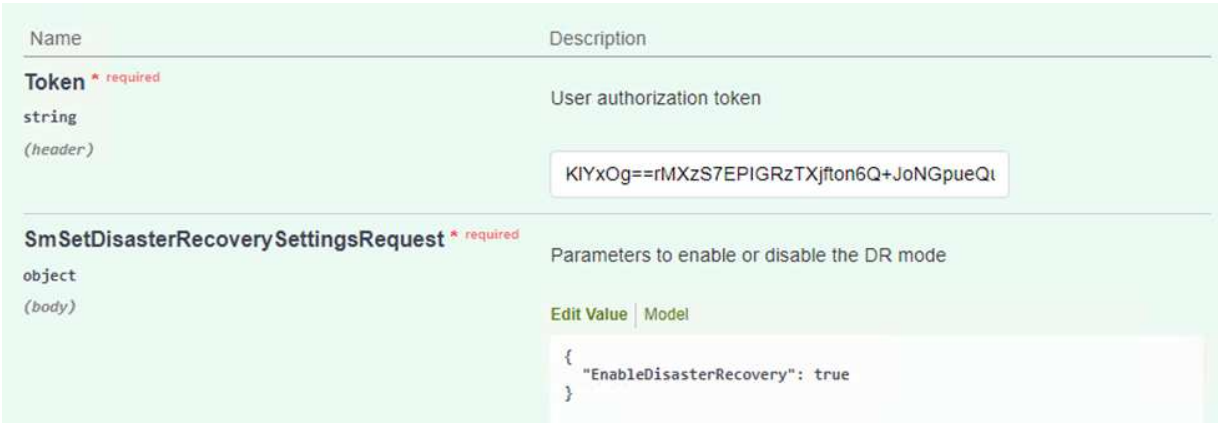
6. セカンダリストレージからのSQL Serverのリストアを有効にするには、SnapCenter データベースをディザスタリカバリモードに切り替える必要があります。この処理は、Swagger API Webページで個別の処理として開始されます。

   a. [Disaster Recovery]セクションに移動し、をクリックします `/4.6/disasterrecovery/storage`。

   b. ユーザー認証トークンに貼り付けます。

   c. [SmSetDisasterRecoverySettingsRequest]セクションで、をに `true`変更します `EnableDisasterRecover`。

   d. Executeをクリックして'SQL Serverの災害復旧モードを有効にします



追加手順に関するコメントを参照してください。

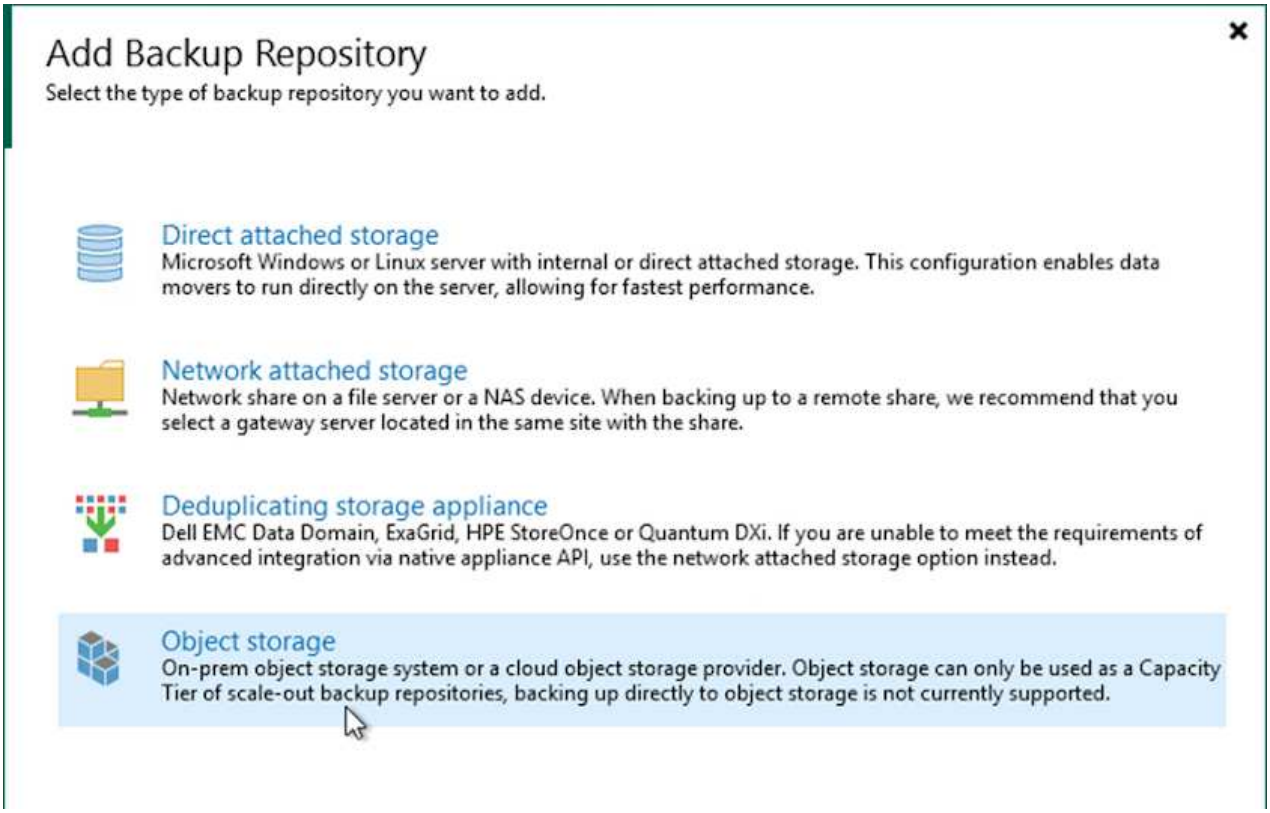
Veeamフルリストアを使用してアプリケーション**VM**をリストアする

バックアップリポジトリを作成し、S3からバックアップをインポートする

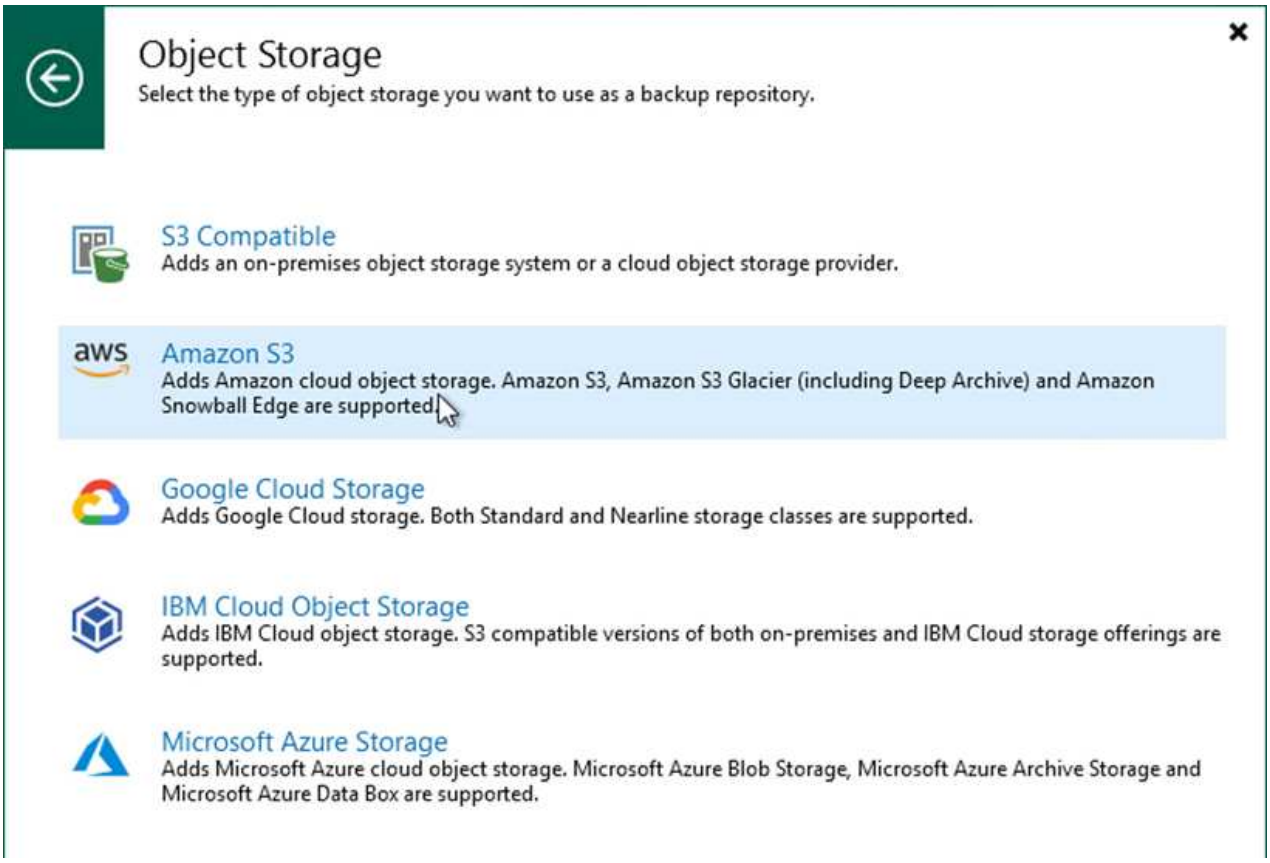
セカンダリVeeamサーバから、S3ストレージからバックアップをインポートし、SQL Server VMとOracle VMをVMware Cloudクラスタにリストアします。

オンプレミスのスケールアウトバックアップリポジトリに含まれていたS3オブジェクトからバックアップをインポートするには、次の手順を実行します。

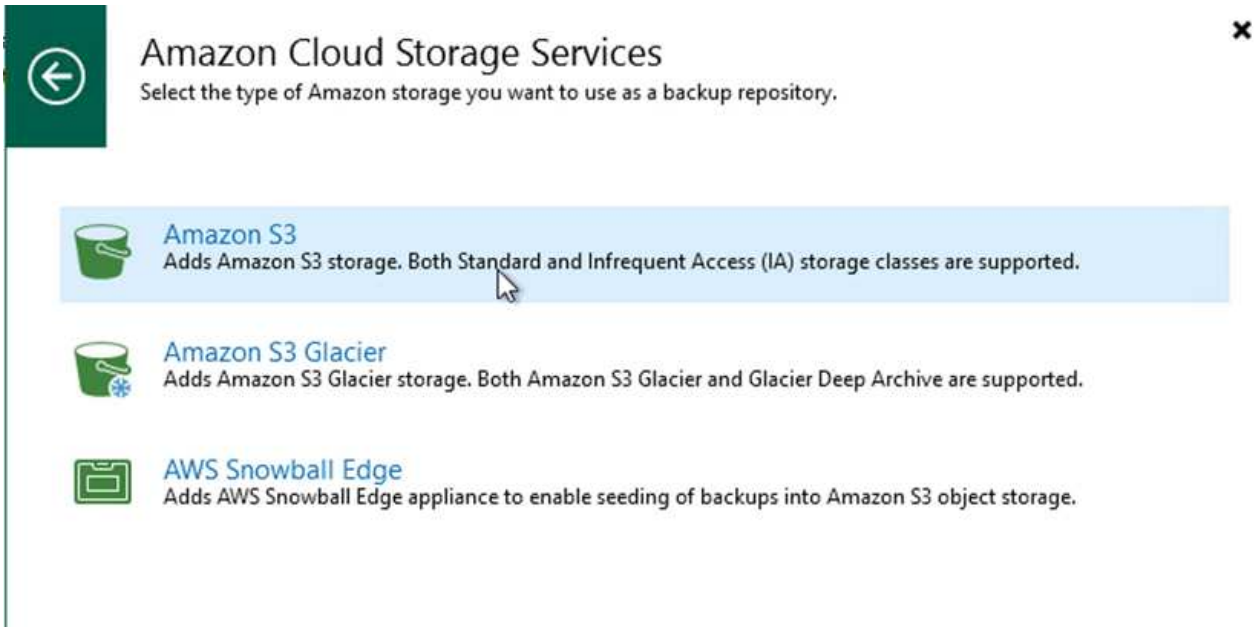
1. [バックアップリポジトリ]に移動し、上部のメニューで[リポジトリの追加]をクリックして、[バックアップリポジトリの追加]ウィザードを起動します。ウィザードの最初のページで、バックアップリポジトリタイプとしてObject Storageを選択します。



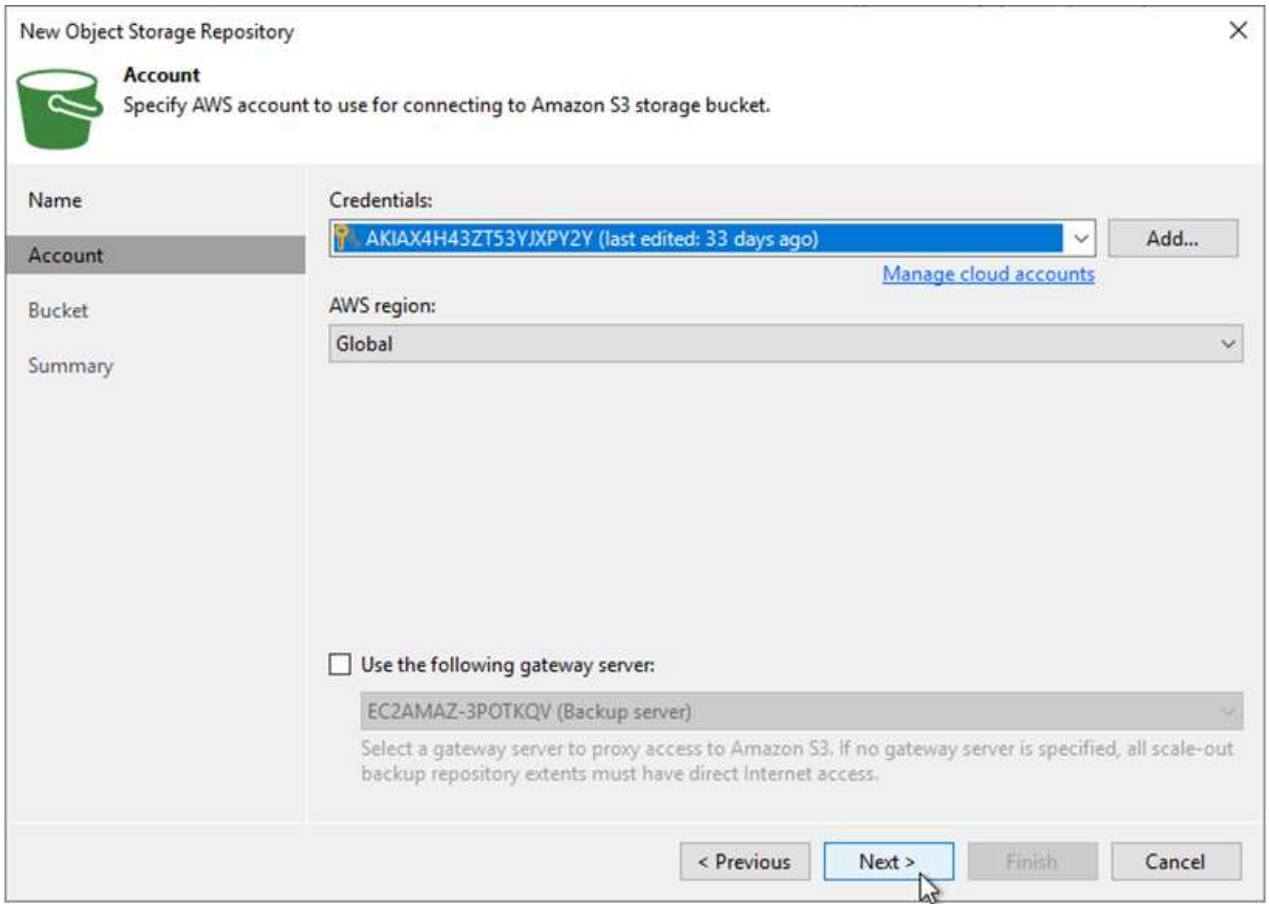
2. オブジェクトストレージタイプとしてAmazon S3を選択します。



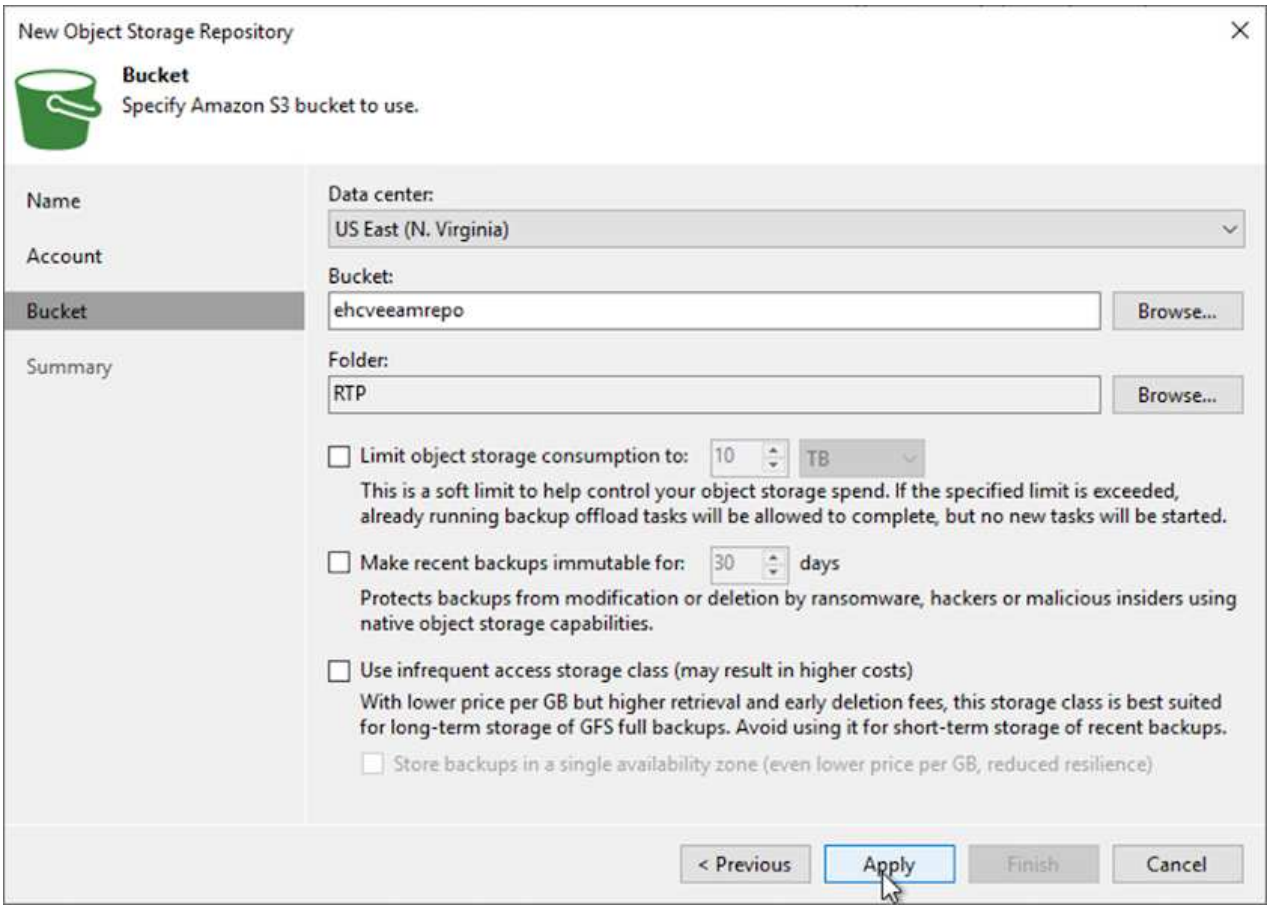
3. Amazon Cloud Storage ServicesのリストからAmazon S3を選択します。



4. ドロップダウンリストから事前に入力したクレデンシャルを選択するか、クラウドストレージリソースにアクセスするための新しいクレデンシャルを追加します。次へをクリックして続行します。



5. Bucketページで、データセンター、バケット、フォルダ、および必要なオプションを入力します。適用をクリックします。

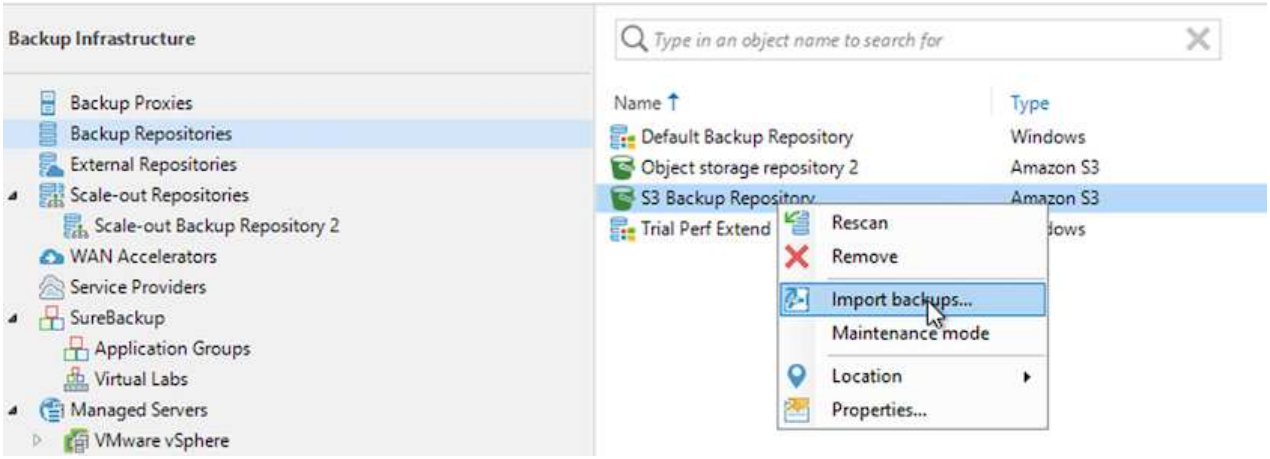


6. 最後に'完了を選択してプロセスを完了し'リポジトリを追加します

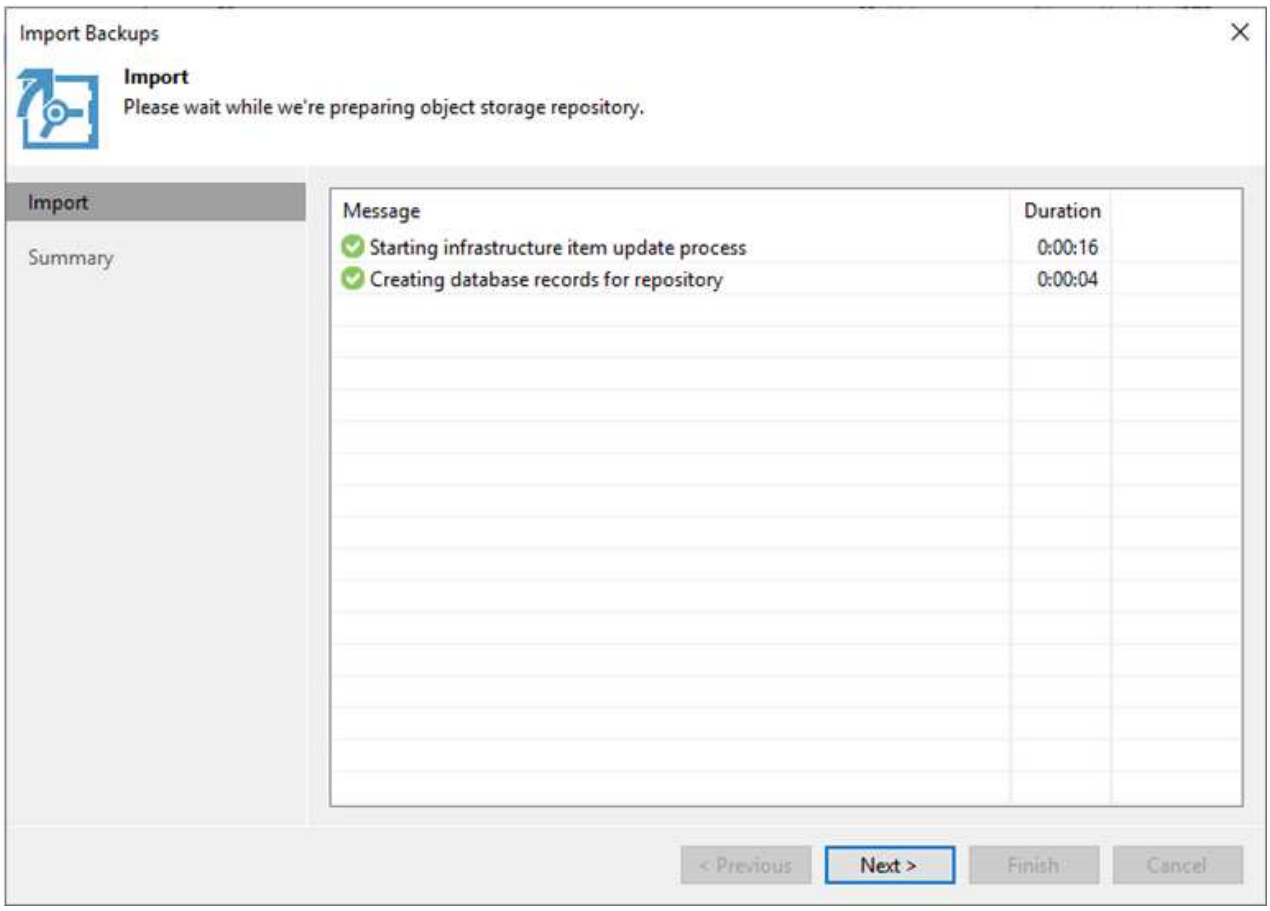
S3オブジェクトストレージからバックアップをインポートする

前のセクションで追加したS3リポジトリからバックアップをインポートするには、次の手順を実行します。

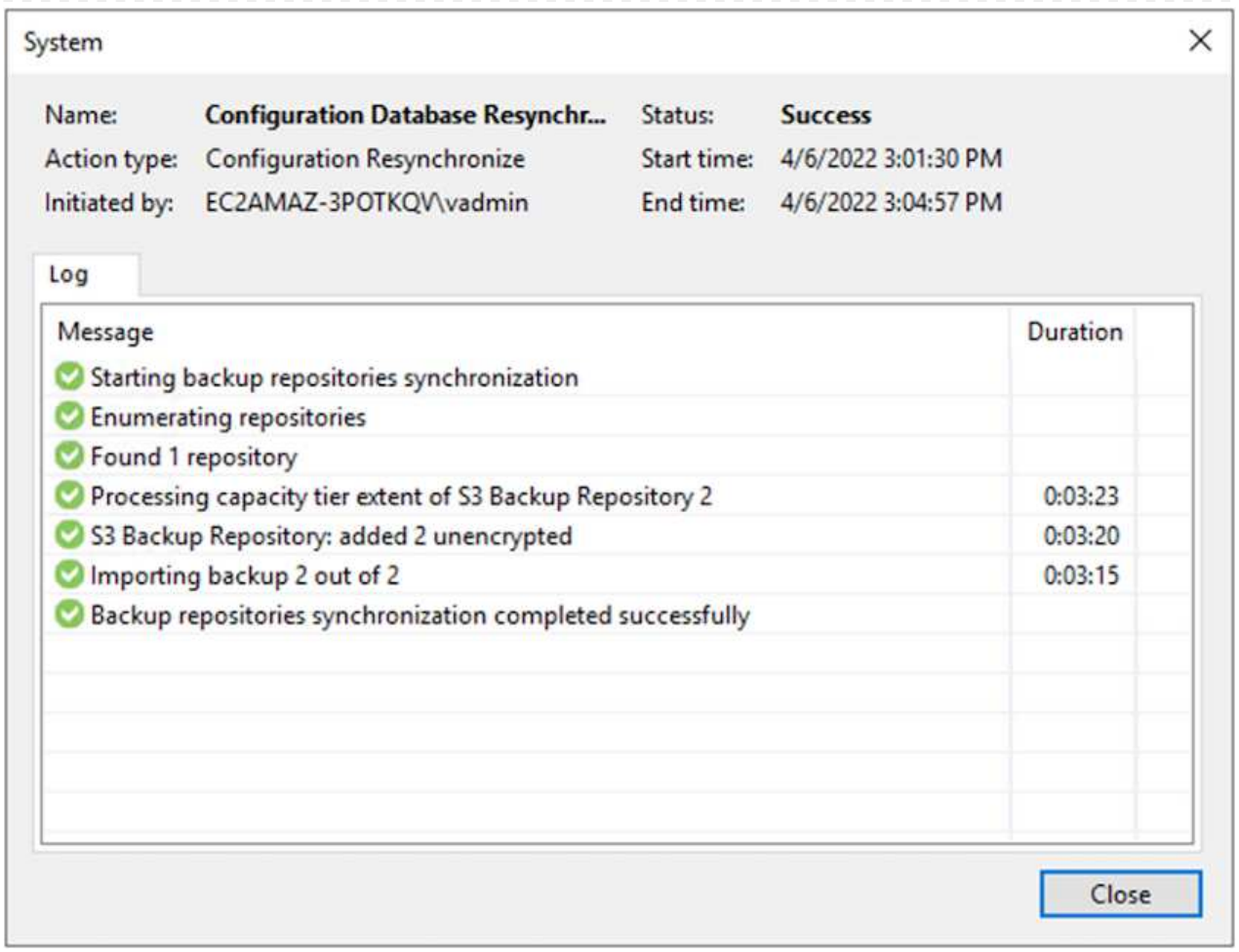
1. S3バックアップリポジトリで、バックアップのインポートを選択してバックアップのインポートウィザードを起動します。



2. インポート用のデータベースレコードが作成されたら、[次へ]を選択し、サマリー画面で[完了]を選択してインポートプロセスを開始します。

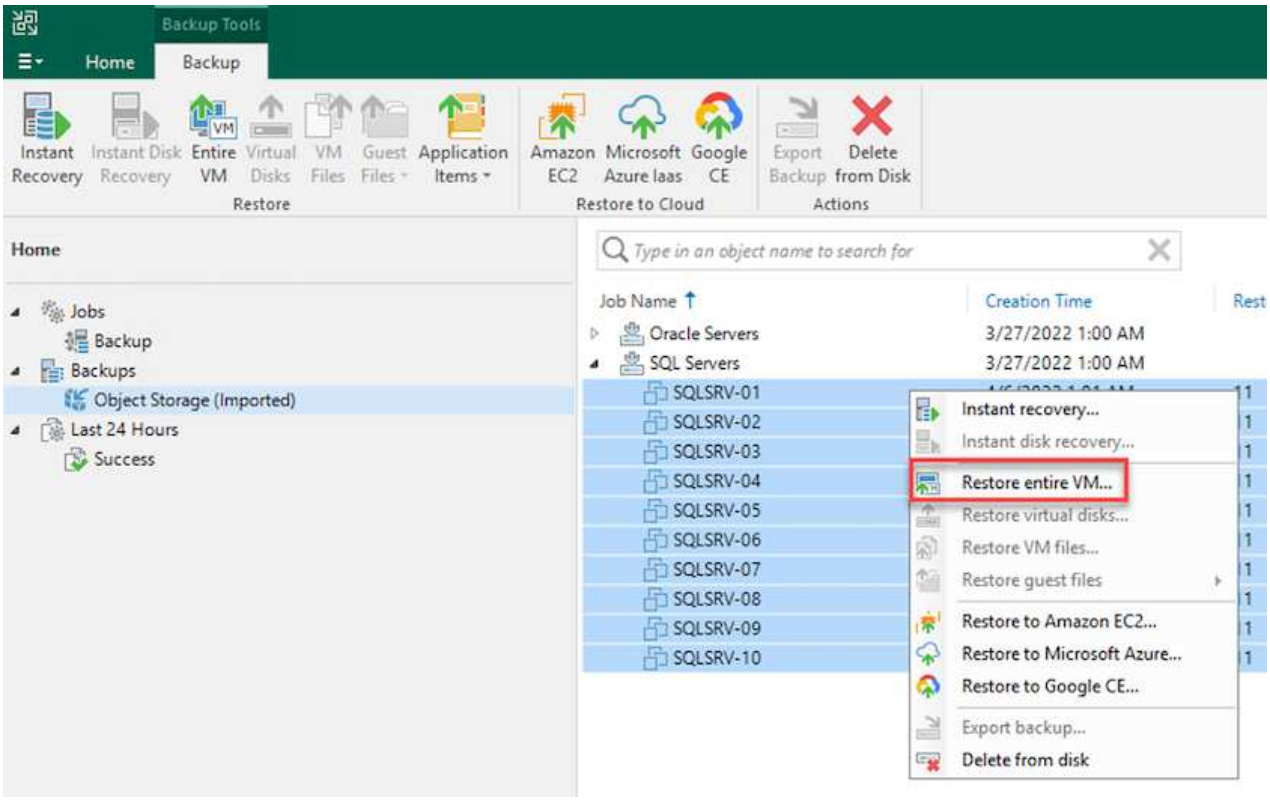


3. インポートが完了したら、VMware CloudクラスタにVMをリストアできます。

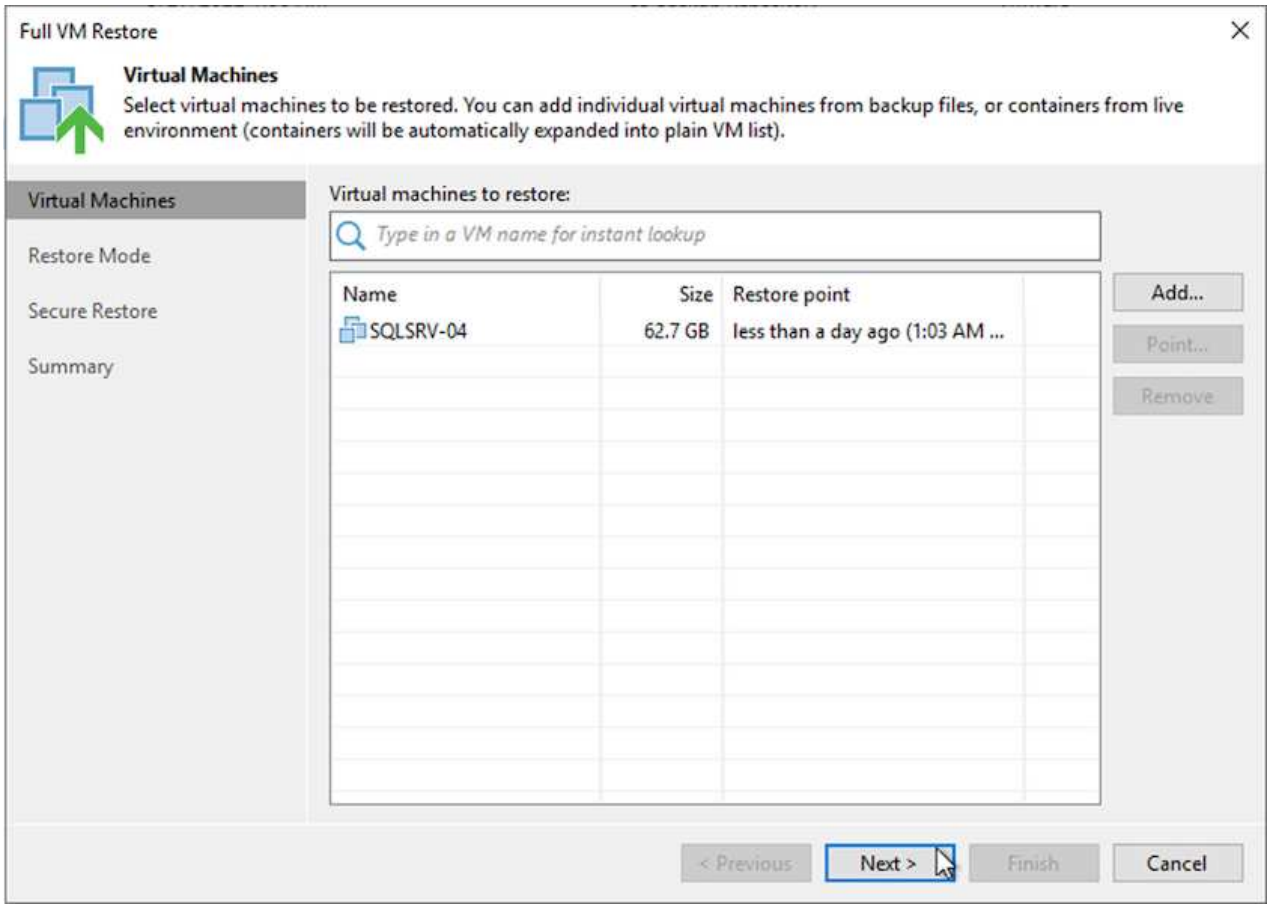

System
Name: Configuration Database Resynchr...
Status: Success
Action type: Configuration Resynchronize
Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vadmin
End time: 4/6/2022 3:04:57 PM
Log
Message
Duration
Starting backup repositories synchronization
Enumerating repositories
Found 1 repository
Processing capacity tier extent of S3 Backup Repository 2
0:03:23
S3 Backup Repository: added 2 unencrypted
0:03:20
Importing backup 2 out of 2
0:03:15
Backup repositories synchronization completed successfully
Close

SQLおよびOracle仮想マシンをAWSワークロードドメイン/クラスタ上のVMware Cloudにリストアするには、次の手順を実行します。

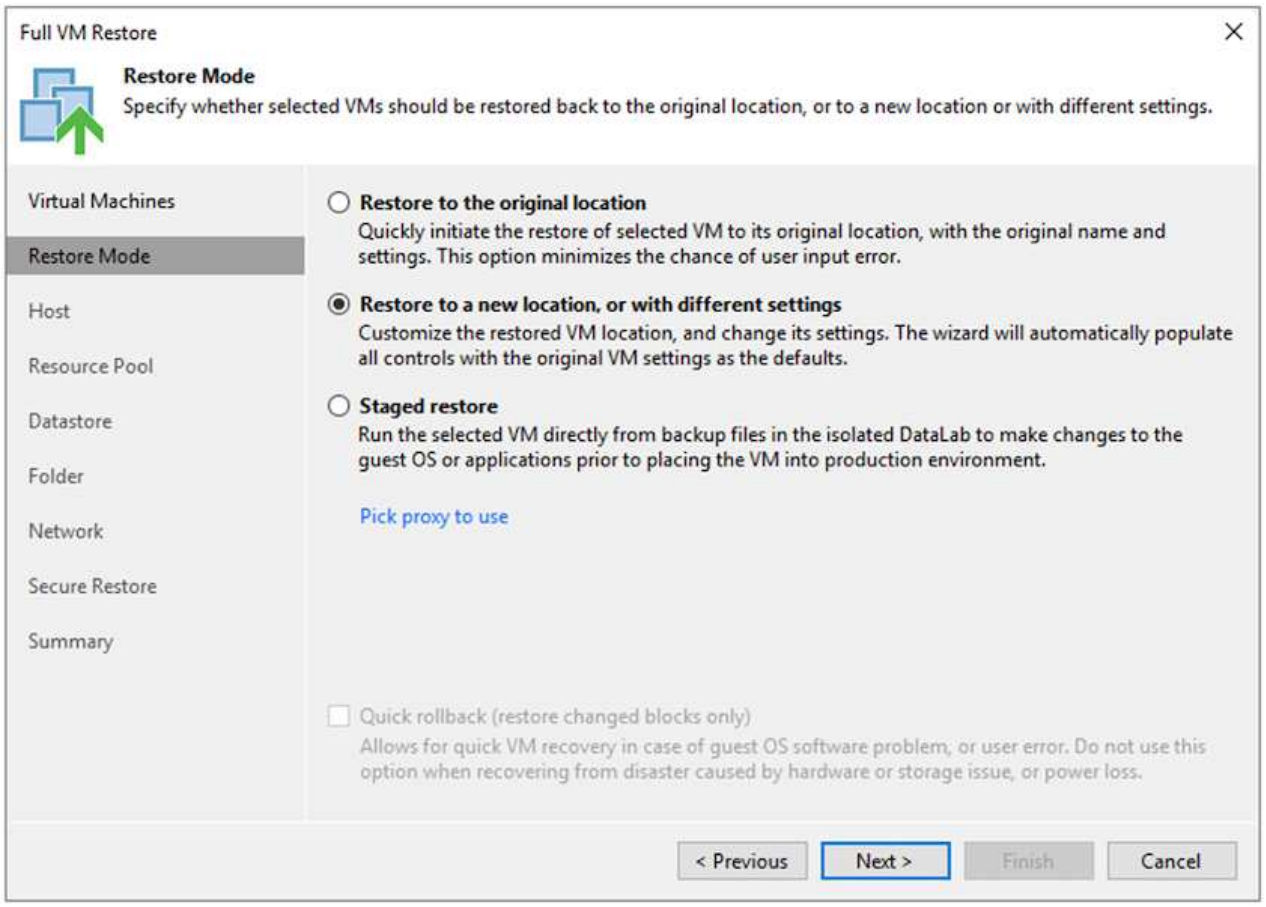
1. Veeamのホームページで、インポートしたバックアップを含むオブジェクトストレージを選択し、リストアするVMを選択して右クリックし、Restore Entire VM（VM全体のリストア）を選択します。



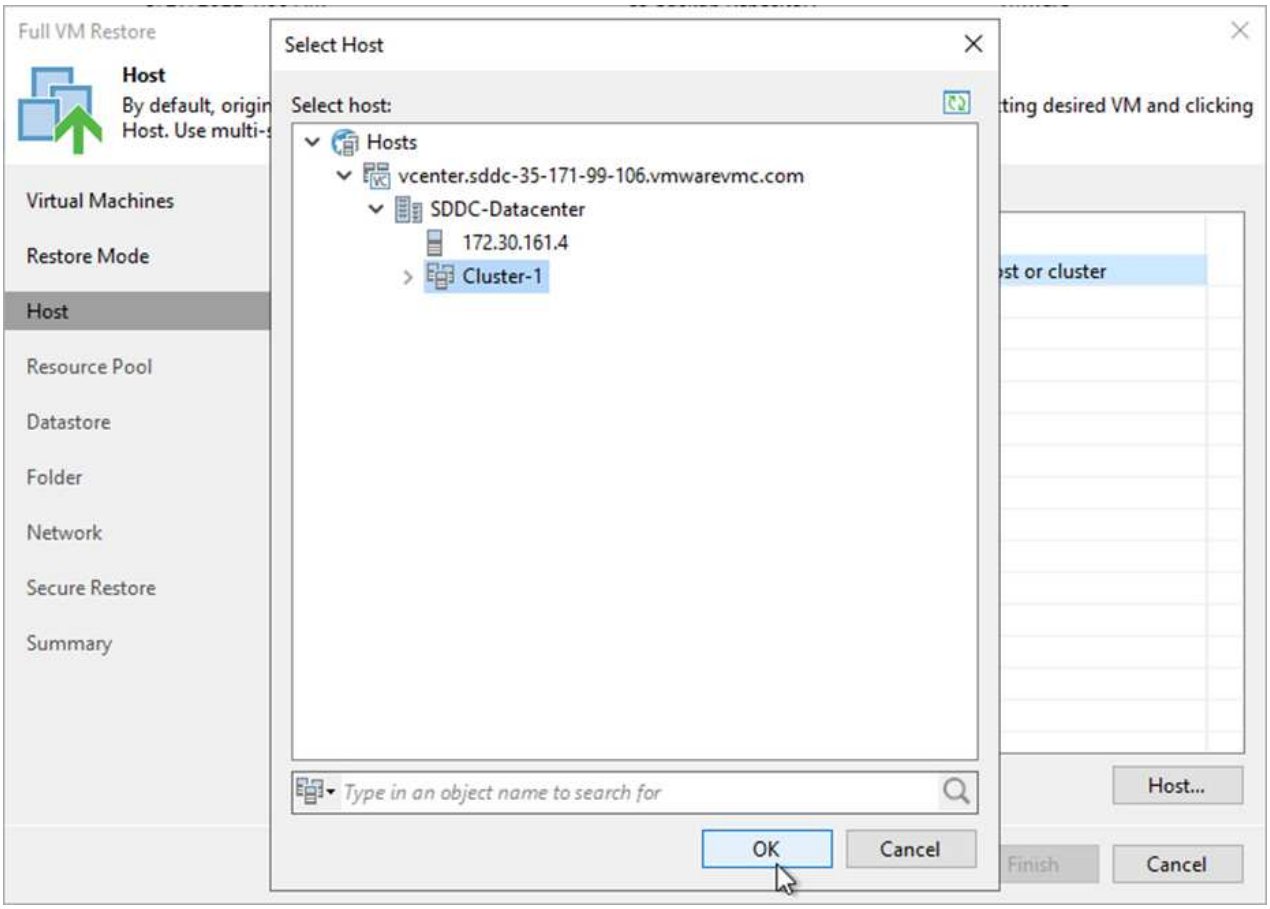
2. [Full VM Restore]ウィザードの最初のページで、必要に応じてVMをバックアップに変更し、[Next]を選択します。



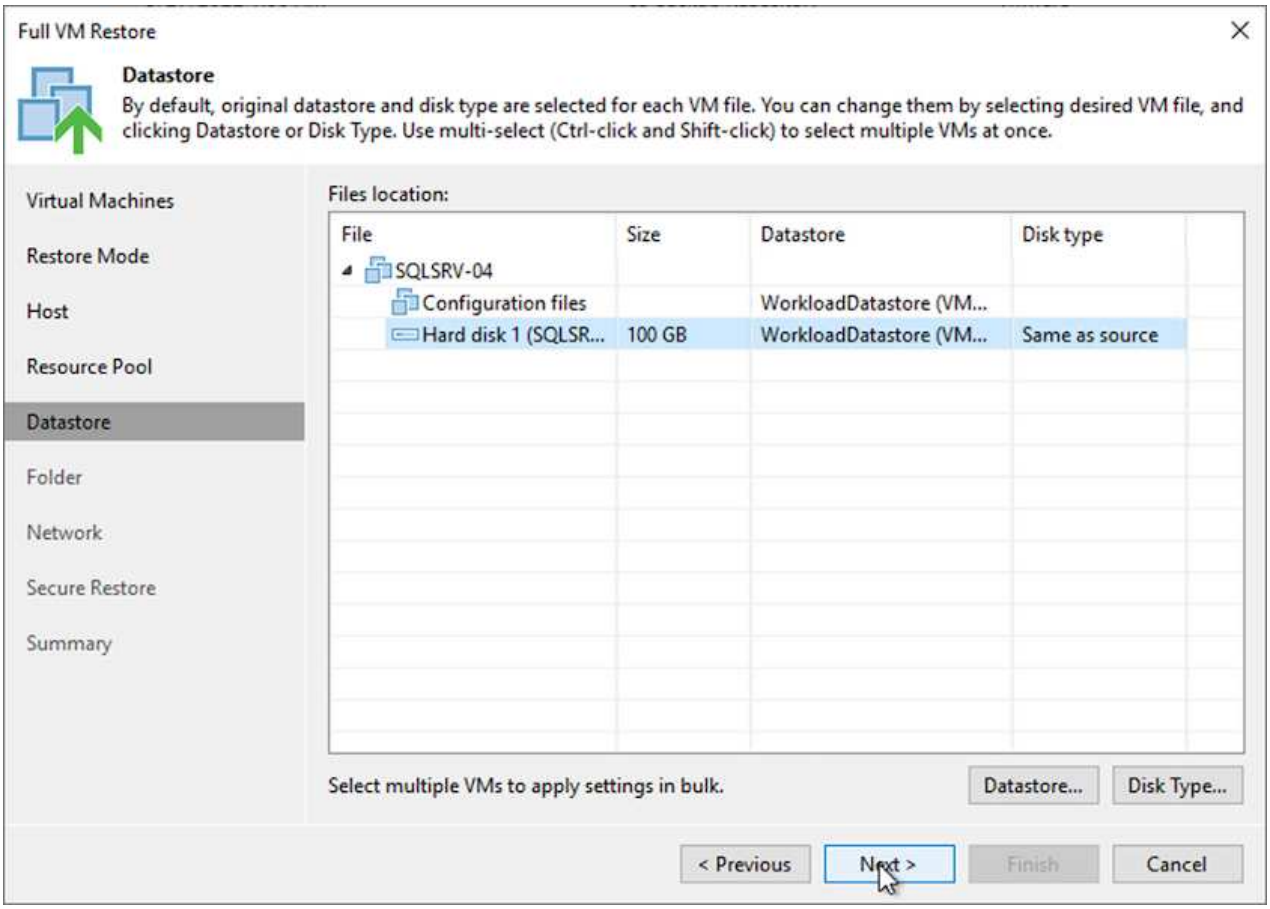
3. [復元モード]ページで、[新しい場所に復元]または[別の設定]を選択します。



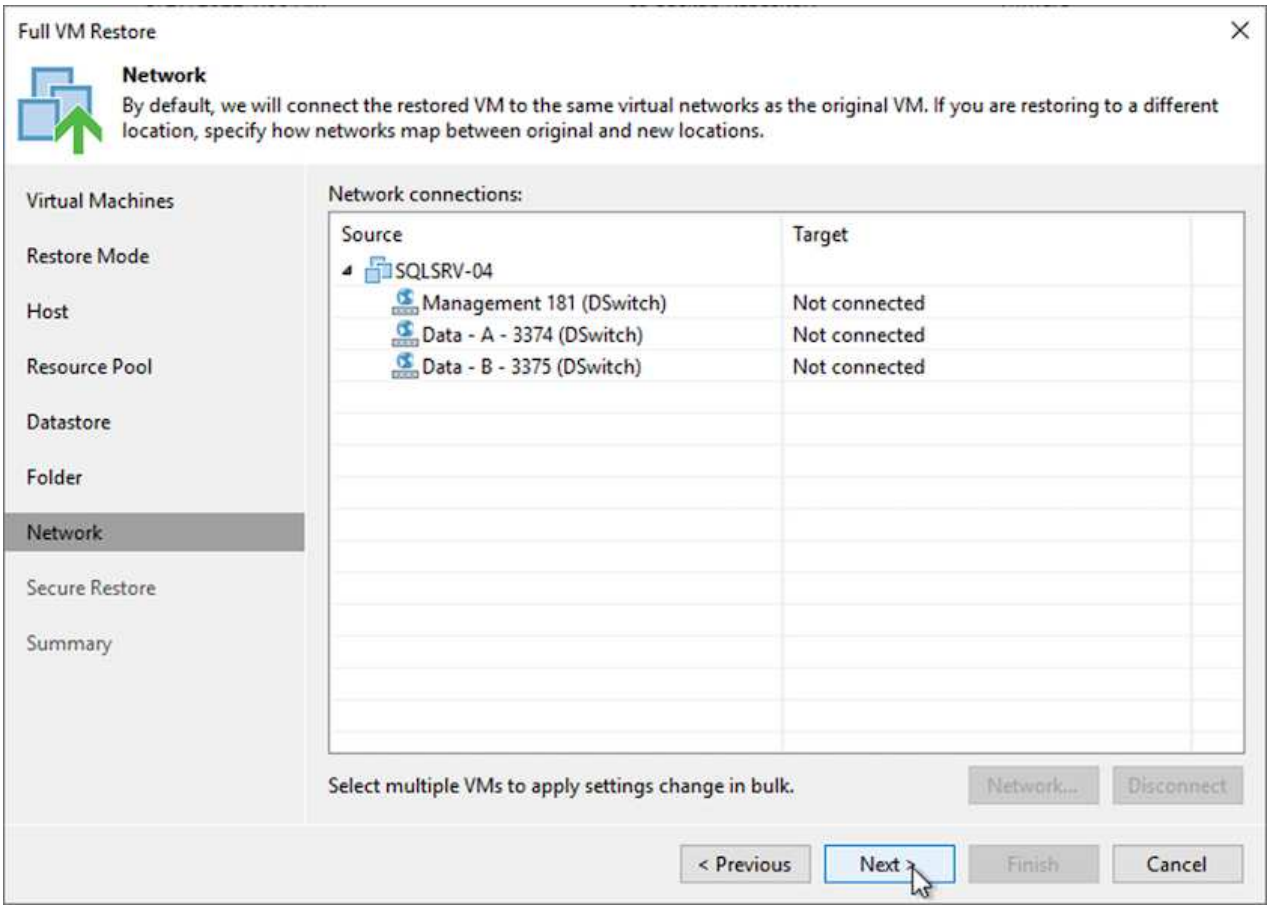
4. ホストページで、VMのリストア先となるターゲットESXiホストまたはクラスタを選択します。

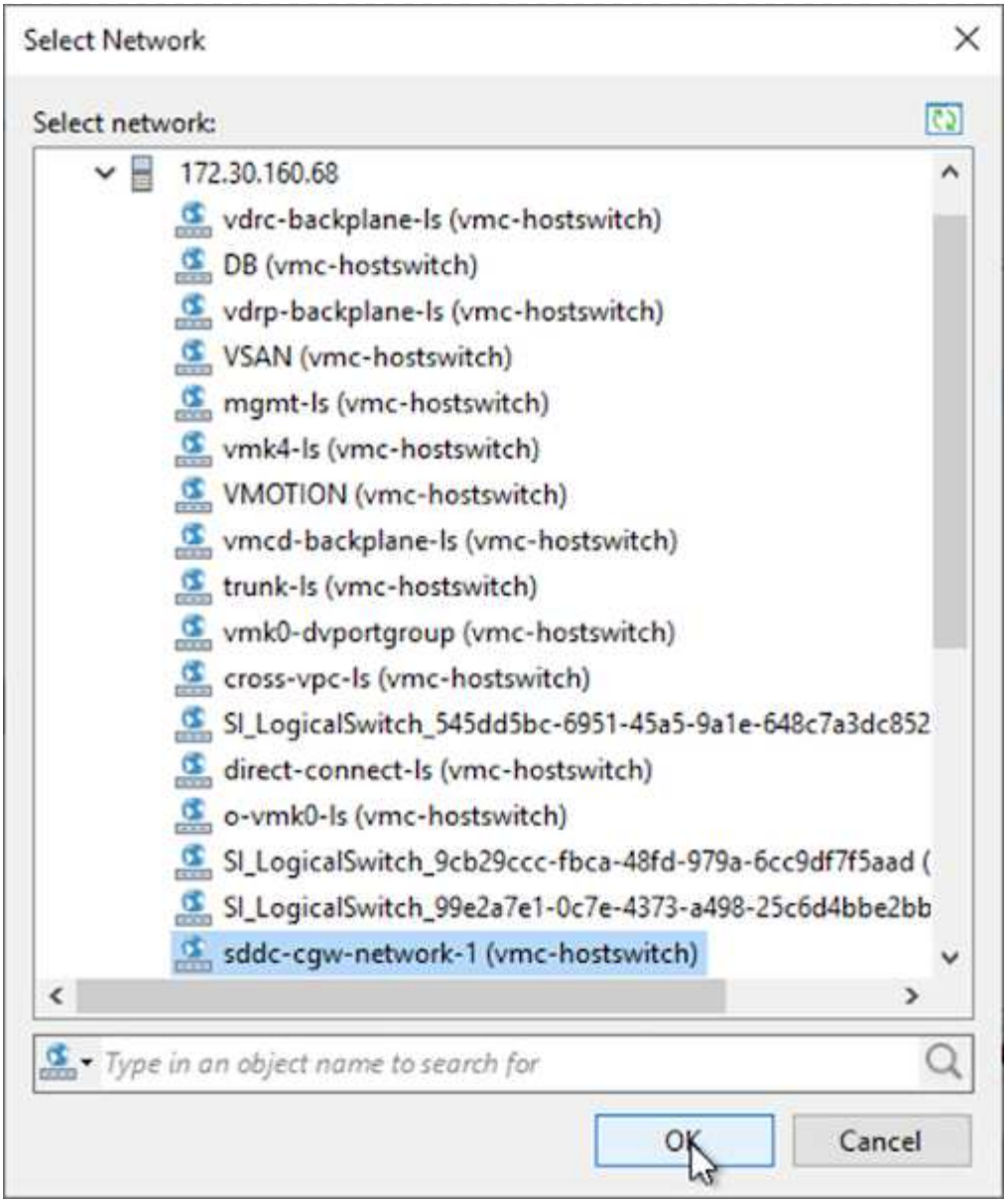


5. Datastores（データストア）ページで、構成ファイルとハードディスクの両方のターゲットデータストアの場所を選択します。



6. [ネットワーク]ページで、VM上の元のネットワークを新しいターゲットの場所にあるネットワークにマッピングします。


Full VM Restore
Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.
Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Summary
Network connections:
Source
Target
SQLSRV-04
Management 181 (DSwitch)
Not connected
Data - A - 3374 (DSwitch)
Not connected
Data - B - 3375 (DSwitch)
Not connected
Select multiple VMs to apply settings change in bulk.
Network...
Disconnect
< Previous
Next >
Finish
Cancel



7. 復元されたVMをスキャンしてマルウェアを検出するかどうかを選択し、概要ページを確認してから、完了をクリックして復元を開始します。

SQL Serverアプリケーションデータをリストアする

次のプロセスでは、オンプレミスサイトが動作不能になった場合に、VMwareクラウド サービス でAWS内のSQL Serverをリカバリする方法について説明します。

リカバリ手順を続行するには、次の前提条件を満たしている必要があります。

1. Windows Server VMがVeeam Full Restoreを使用してVMware Cloud SDDCにリストアされている。
2. セクションで説明した手順に従って、セカンダリSnapCenterサーバが確立され、SnapCenterデータベースのリストアと設定が完了している。"SnapCenter のバックアップとリストアのプロセスの概要"

VM：SQL Server VMのリストア後の設定

VMのリストアが完了したら、SnapCenter でホストVMを再検出するための準備として、ネットワークやその他の項目を設定する必要があります。

1. 管理およびiSCSIまたはNFS用に新しいIPアドレスを割り当てます。
2. ホストをWindowsドメインに追加します。
3. DNSにホスト名を追加するか、SnapCenter サーバのhostsファイルにホスト名を追加します。

SnapCenter プラグインが現在のドメインとは異なるドメインクレデンシャルを使用して導入されている場合は、SQL Server VMでPlug-in for Windowsサービスのログオンアカウントを変更する必要があります。ログオンアカウントを変更したら、SnapCenter SMCore、Plug-in for Windows、およびPlug-in for SQL Serverの各サービスを再起動します。

リストアされたVMをSnapCenter で自動的に再検出するには、FQDNをオンプレミスのSnapCenter に最初に追加されたVMと同じにする必要があります。

SQL Serverリストア用にFSXストレージを構成します

SQL Server VMのディザスタリカバリリストアプロセスを実行するには、既存のSnapMirror関係をFSXクラスタから解除し、ボリュームへのアクセスを許可する必要があります。これには、次の手順を実行します。

1. SQL Serverデータベースボリュームとログボリュームの既存のSnapMirror関係を解除するには、FSX CLIから次のコマンドを実行します。

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. SQL Server Windows VMのiSCSI IQNを含むイニシエータグループを作成して、LUNへのアクセスを許可します。

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN
```

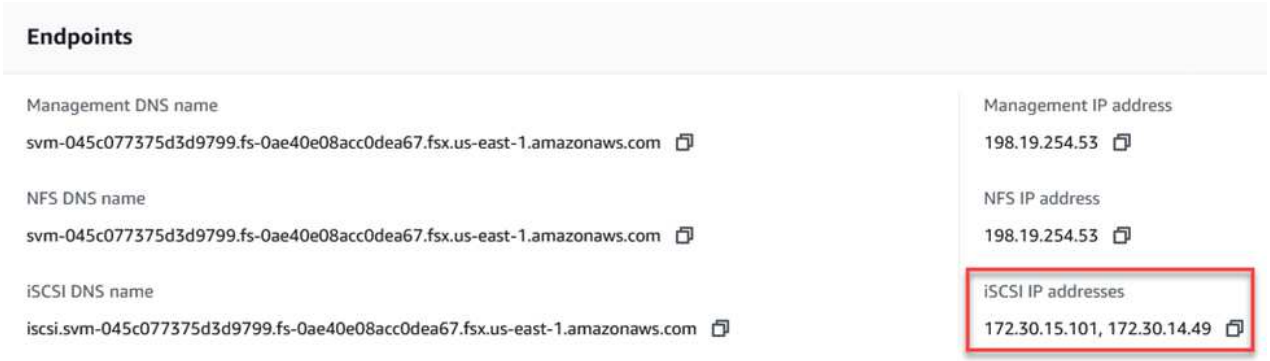
3. 最後に、作成したigroupにLUNをマッピングします。

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

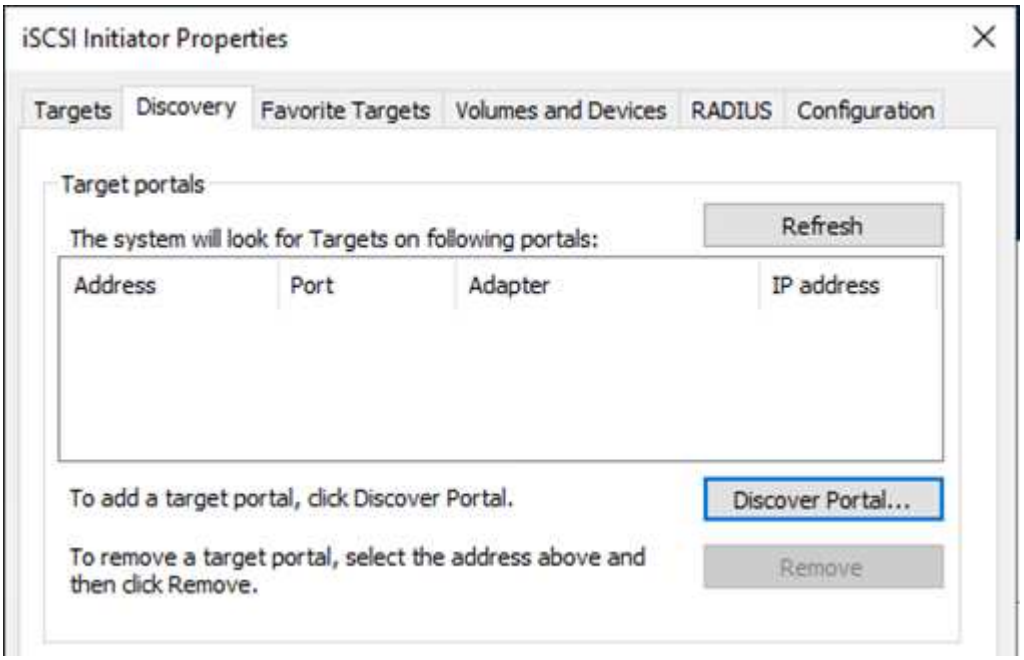
4. パス名を確認するには、コマンドを実行し `lun show`ます。

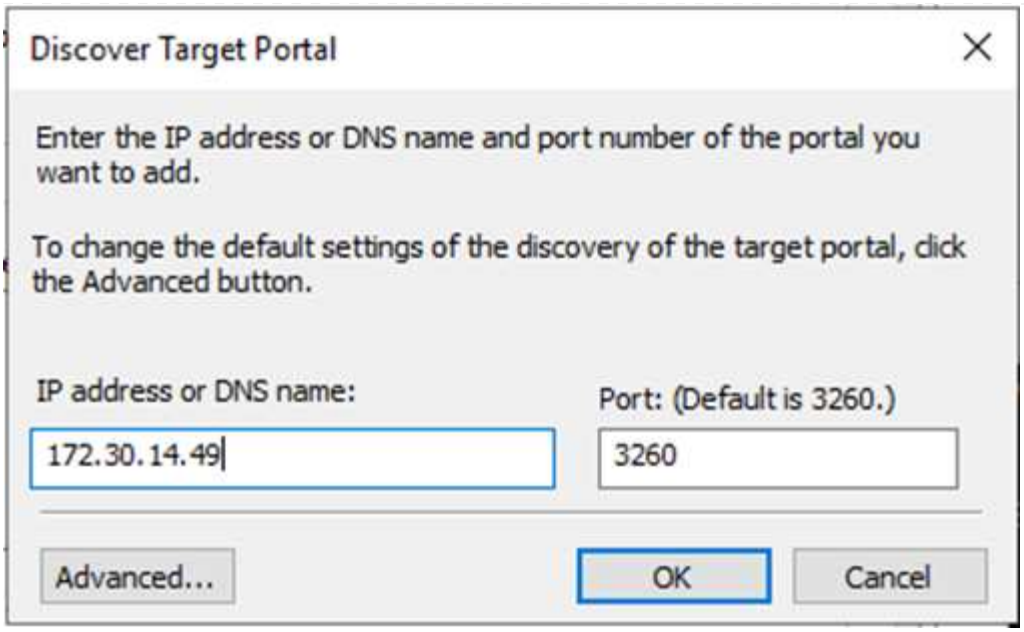
Windows VMでiSCSIアクセスを設定し、ファイルシステムを検出します

1. SQL Server VMからiSCSIネットワークアダプタをセットアップし、FSXインスタンス上のiSCSIターゲットインターフェイスへの接続が確立されたVMwareポートグループ上で通信します。
2. iSCSI Initiator Propertiesユーティリティを開き、Discovery、Favorite Targets、およびTargetsタブの古い接続設定を消去します。
3. FSXインスタンス/クラスタ上のiSCSI論理インターフェイスにアクセスするためのIPアドレスを特定します。これは、AWSコンソールのAmazon FSX > ONTAP > Storage Virtual Machinesの下にあります。

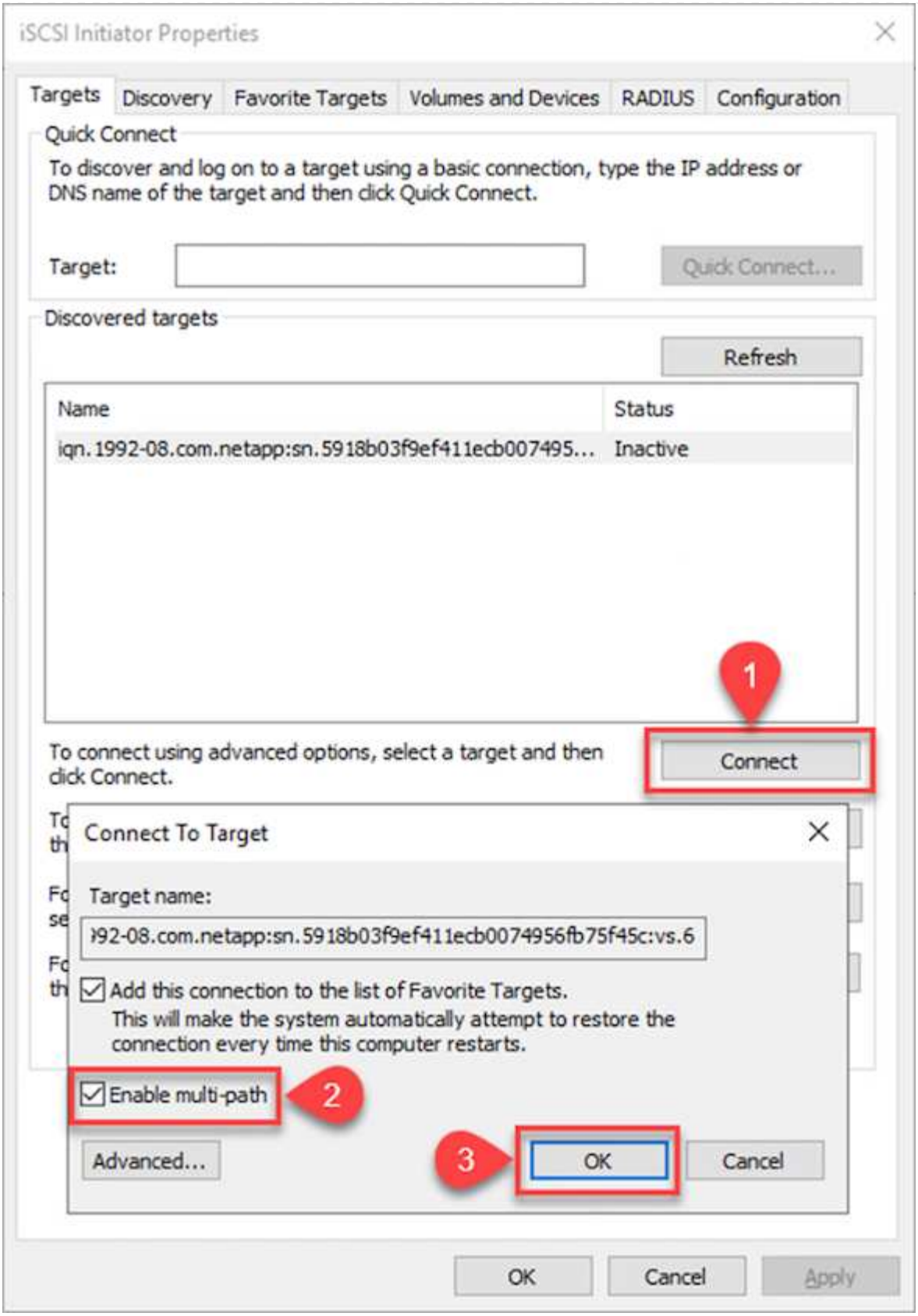


4. [Discovery]タブで[Discover Portal]をクリックし、FSX iSCSIターゲットのIPアドレスを入力します。

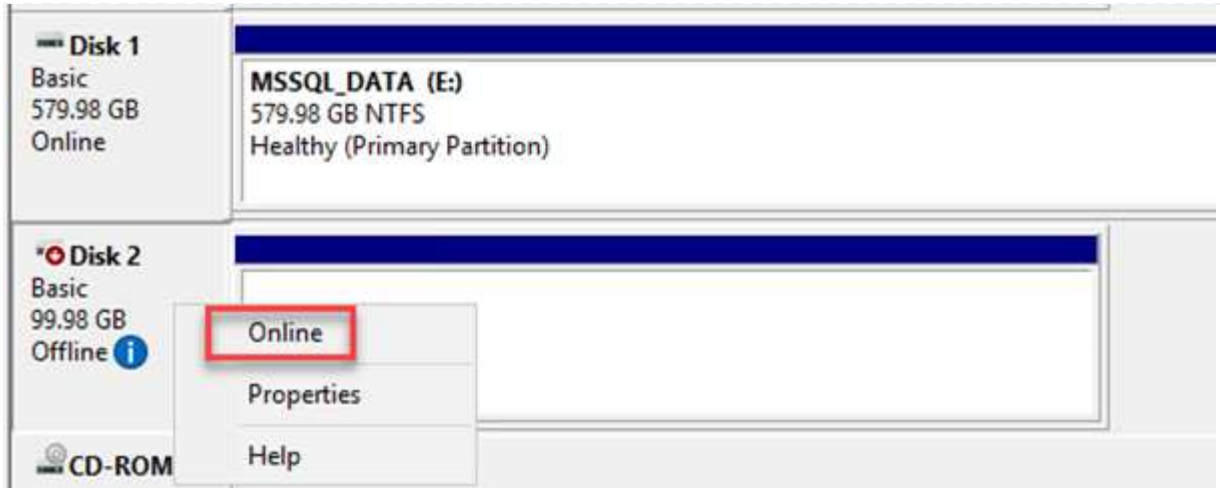




5. [ターゲット]タブで[接続]をクリックし、構成に応じて[マルチパスを有効にする]を選択し、[OK]をクリックしてターゲットに接続します。

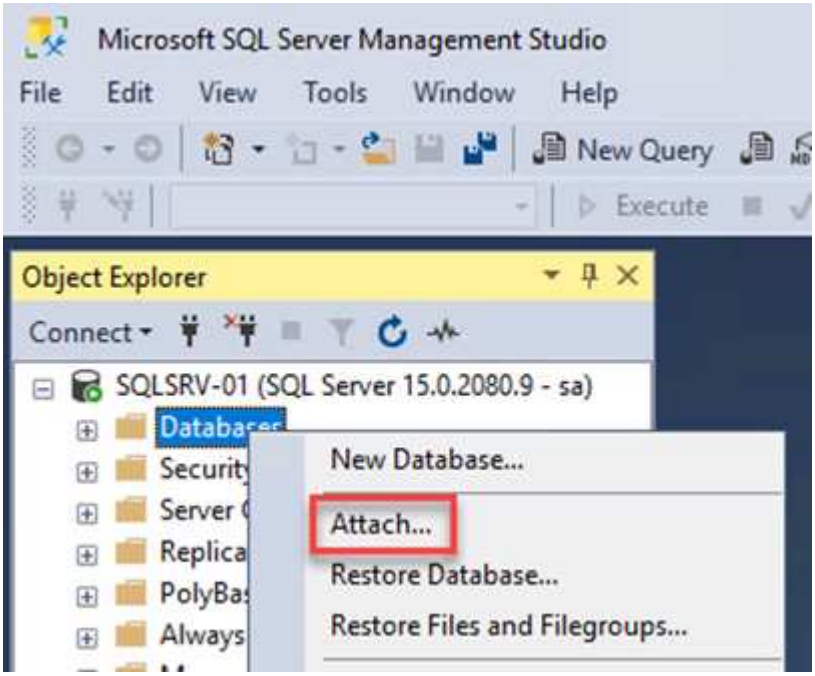


6. コンピュータの管理ユーティリティを開き、ディスクをオンラインにします。以前と同じドライブレターを保持していることを確認します。

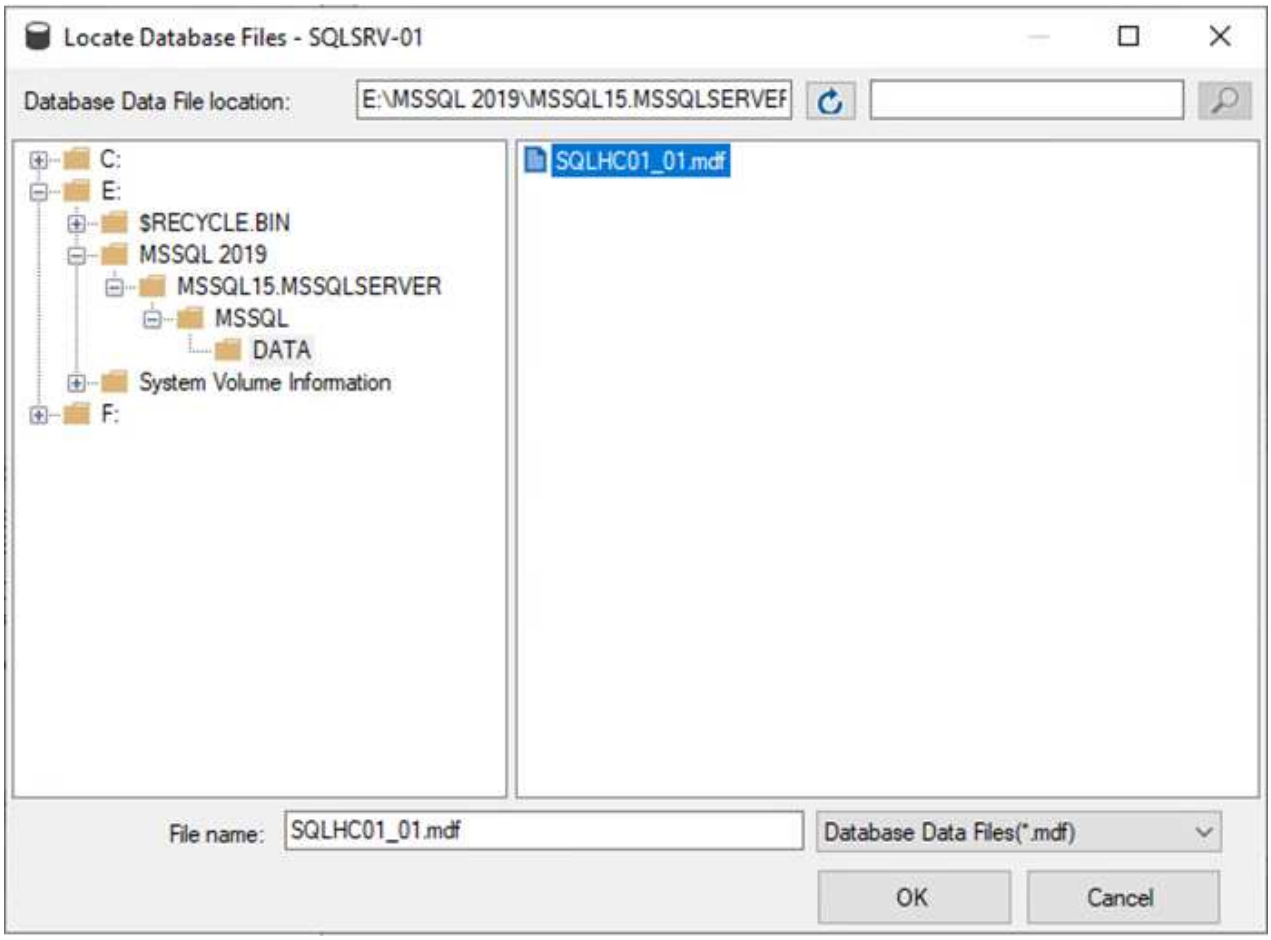

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

SQL Serverデータベースを接続します

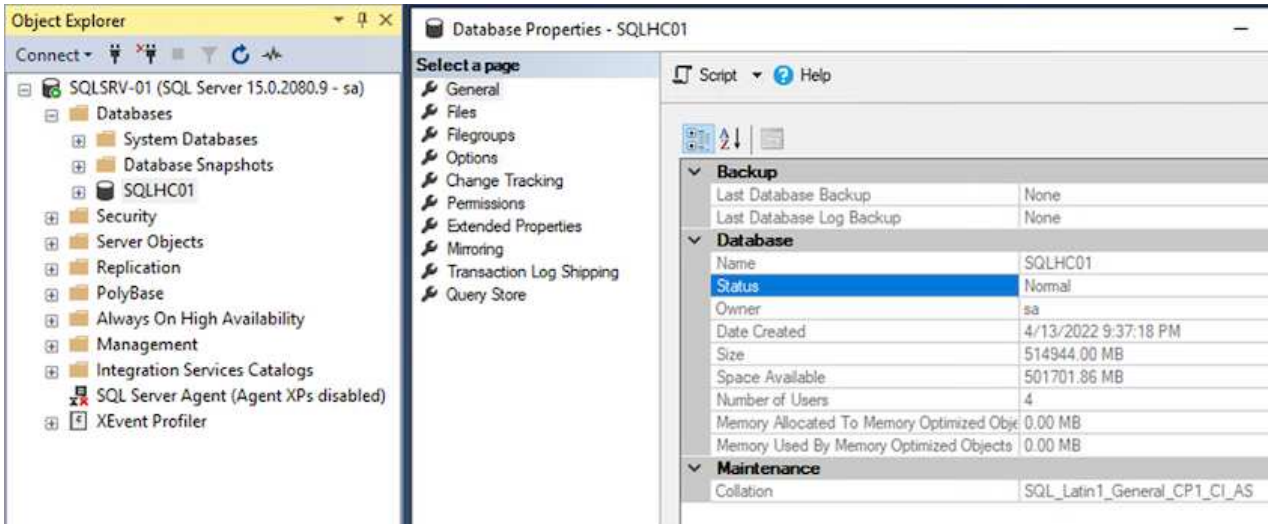
1. SQL Server VMで、Microsoft SQL Server Management Studioを開き、接続を選択してデータベースへの接続プロセスを開始します。



2. [追加]をクリックし、SQL Serverプライマリデータベースファイルが格納されているフォルダに移動して選択し、[OK]をクリックします。



3. トランザクションログが別のドライブにある場合は、トランザクションログが格納されているフォルダを選択します。
4. 終了したら、[OK]をクリックしてデータベースに接続します。

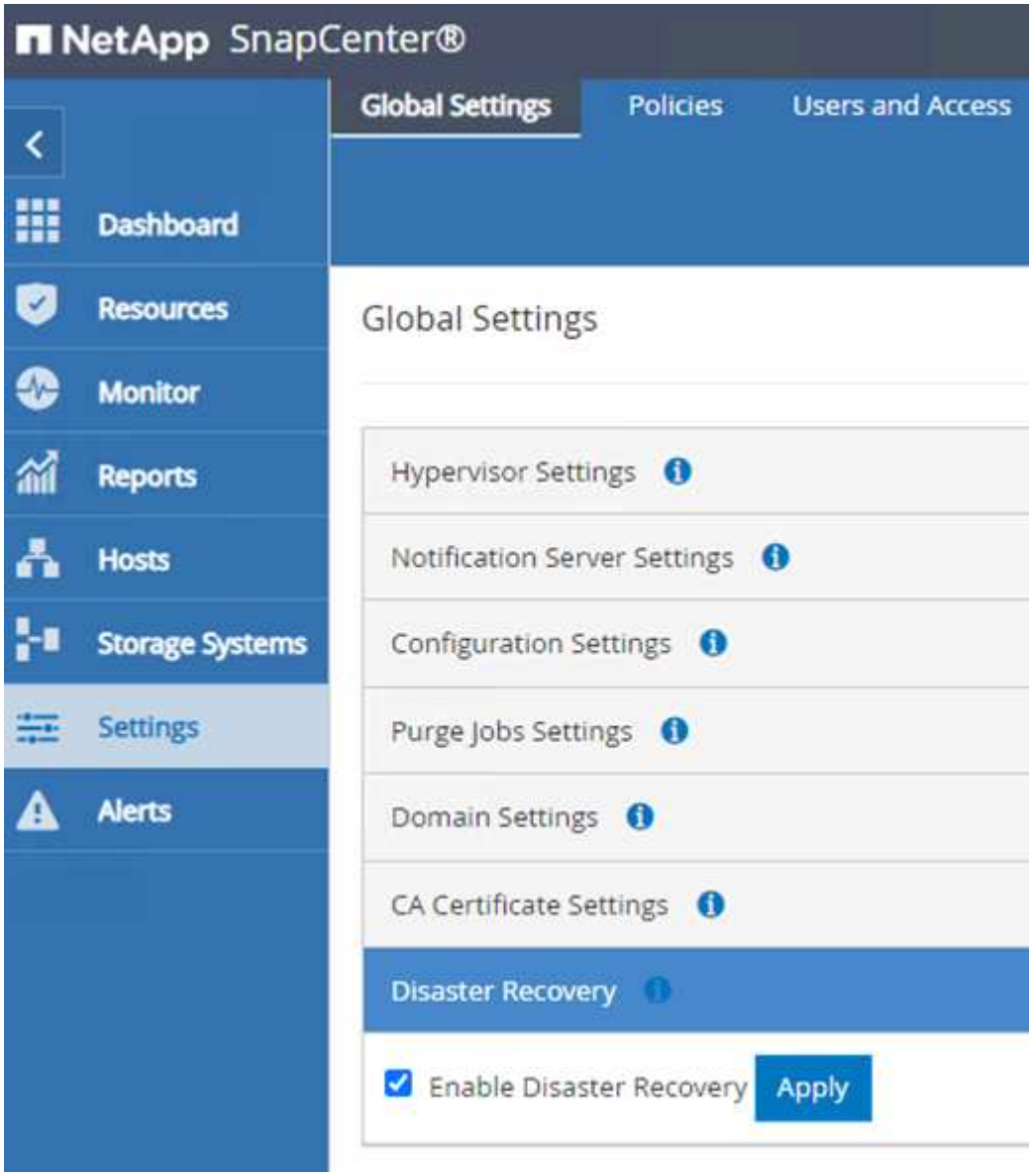


SQL Server Plug-inとの**SnapCenter** 通信を確認します

SnapCenter データベースを以前の状態にリストアすると、SQL Serverホストが自動的に再検出されます。これを正しく機能させるには、次の前提条件に注意してください。

- SnapCenter はディザスタリカバリモードにする必要があります。これは、Swagger APIまたはディザスタリカバリのグローバル設定で実行できます。
- SQL ServerのFQDNは、オンプレミスのデータセンターで実行されていたインスタンスと同じである必要があります。
- 元のSnapMirror関係が解除されている必要があります。
- データベースを含むLUNをSQL Serverインスタンスにマウントし、データベースを接続しておく必要があります。

SnapCenter がディザスタリカバリモードになっていることを確認するには、SnapCenter Webクライアントで設定に移動します。[グローバル設定]タブに移動し、[災害復旧]をクリックします。ディザスタリカバリを有効にするチェックボックスがオンになっていることを確認します。



Oracleアプリケーションデータをリストアします

次のプロセスでは、オンプレミスサイトが動作不能になった場合に、VMwareクラウド サービス でAWS でOracleアプリケーションデータをリカバリする方法について説明します。

リカバリ手順を続行するには、次の前提条件を満たしている必要があります。

1. Veeam Full Restoreを使用して、Oracle LinuxサーバVMがVMware Cloud SDDCにリストアされている。
2. このセクションで説明する手順を使用して、セカンダリSnapCenterサーバが確立され、SnapCenterデータベースと構成ファイルがリストアされている。"SnapCenter のバックアップとリストアのプロセスの概要"

Oracleリストア用にFSXを設定する–SnapMirror関係を解除します

FSx ONTAPインスタンスでホストされているセカンダリストレージボリュームにOracleサーバからアクセスできるようにするには、まず既存のSnapMirror関係を解除する必要があります。

1. FSX CLIにログインした後、次のコマンドを実行して、正しい名前でフィルタリングされたボリュームを表示します。

```
FSx-Dest::> volume show -volume VolumeName*
```

```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        online     DP        100GB    93.12GB    6%
ora_svm_dest
          oraclesrv_03_u02_dest
                       aggr1        online     DP        200GB    34.98GB   82%
ora_svm_dest
          oraclesrv_03_u03_dest
                       aggr1        online     DP        150GB    33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::>
```

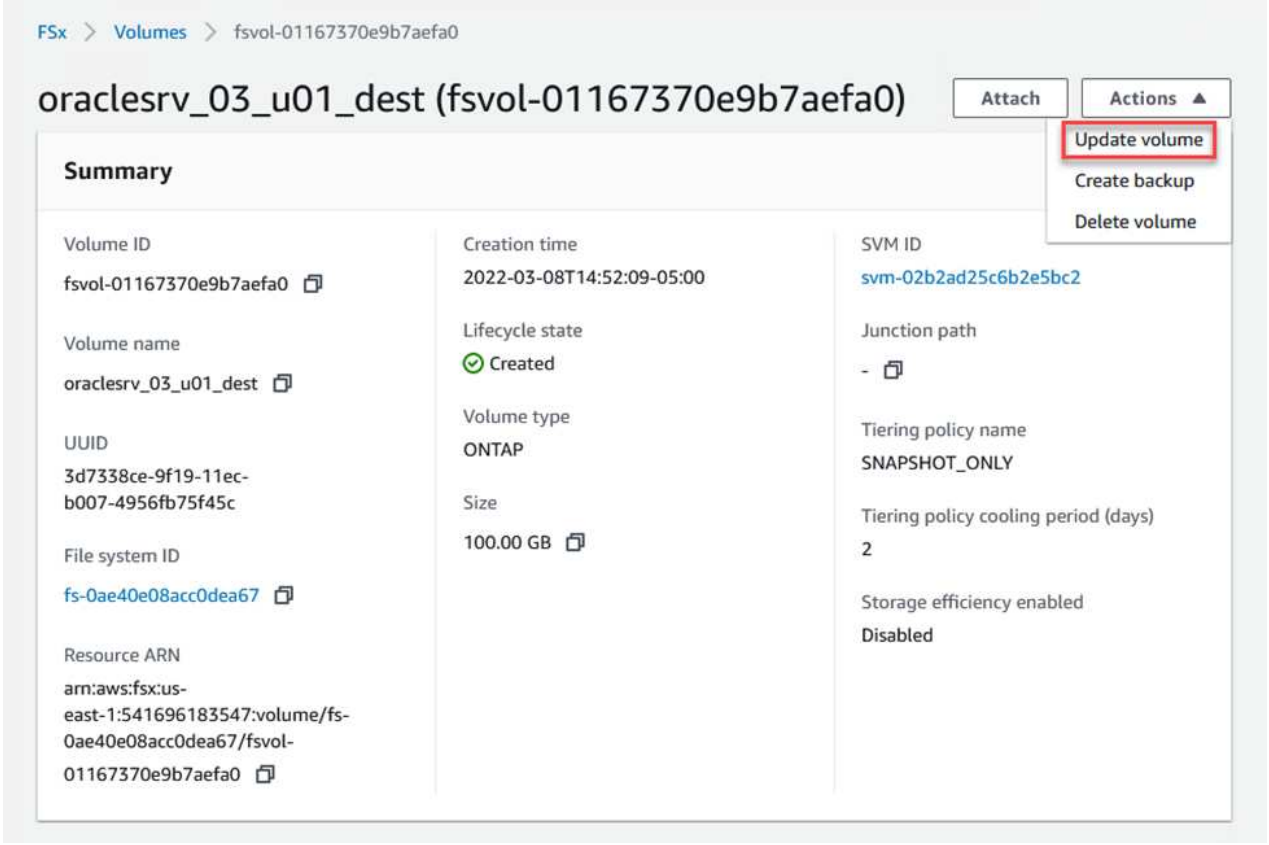
2. 次のコマンドを実行して、既存のSnapMirror関係を解除します。

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

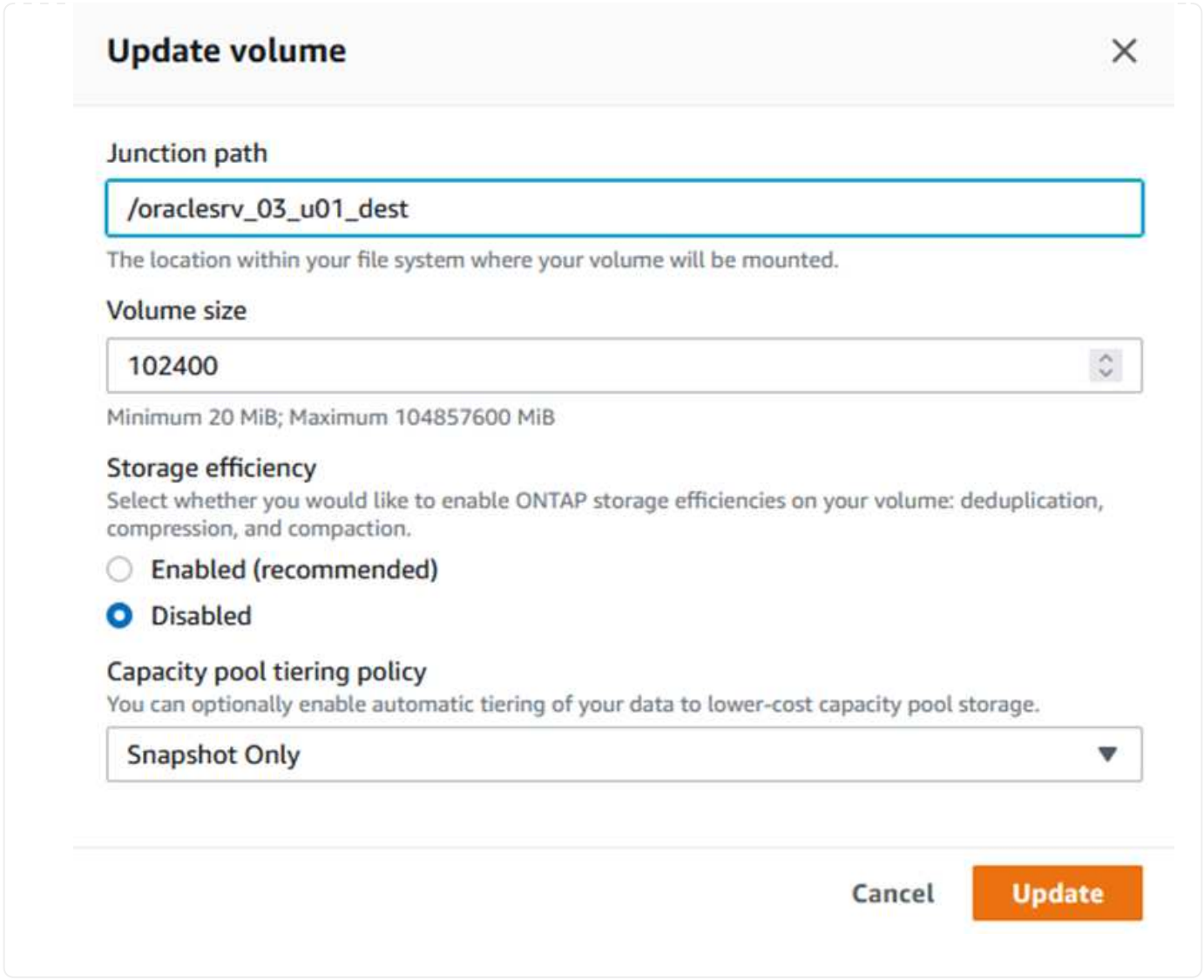
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Amazon FSX Web Clientでjunction-pathを更新します。



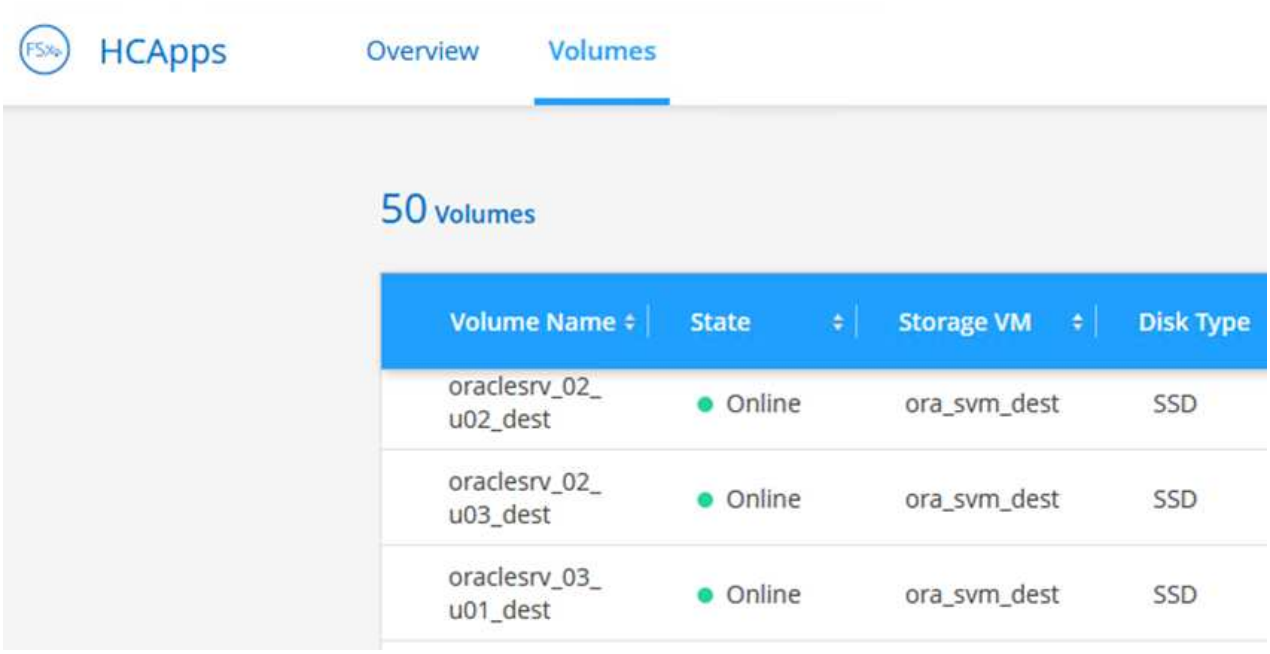
4. ジャンクションパス名を追加し、更新（Update）をクリックする。OracleサーバからNFSボリュームをマウントする際に、このジャンクションパスを指定します。


Update volume
Junction path
/oraclesrv_03_u01_dest
The location within your file system where your volume will be mounted.
Volume size
102400
Minimum 20 MiB; Maximum 104857600 MiB
Storage efficiency
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.
Enabled (recommended)
Disabled
Capacity pool tiering policy
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.
Snapshot Only
Cancel
Update

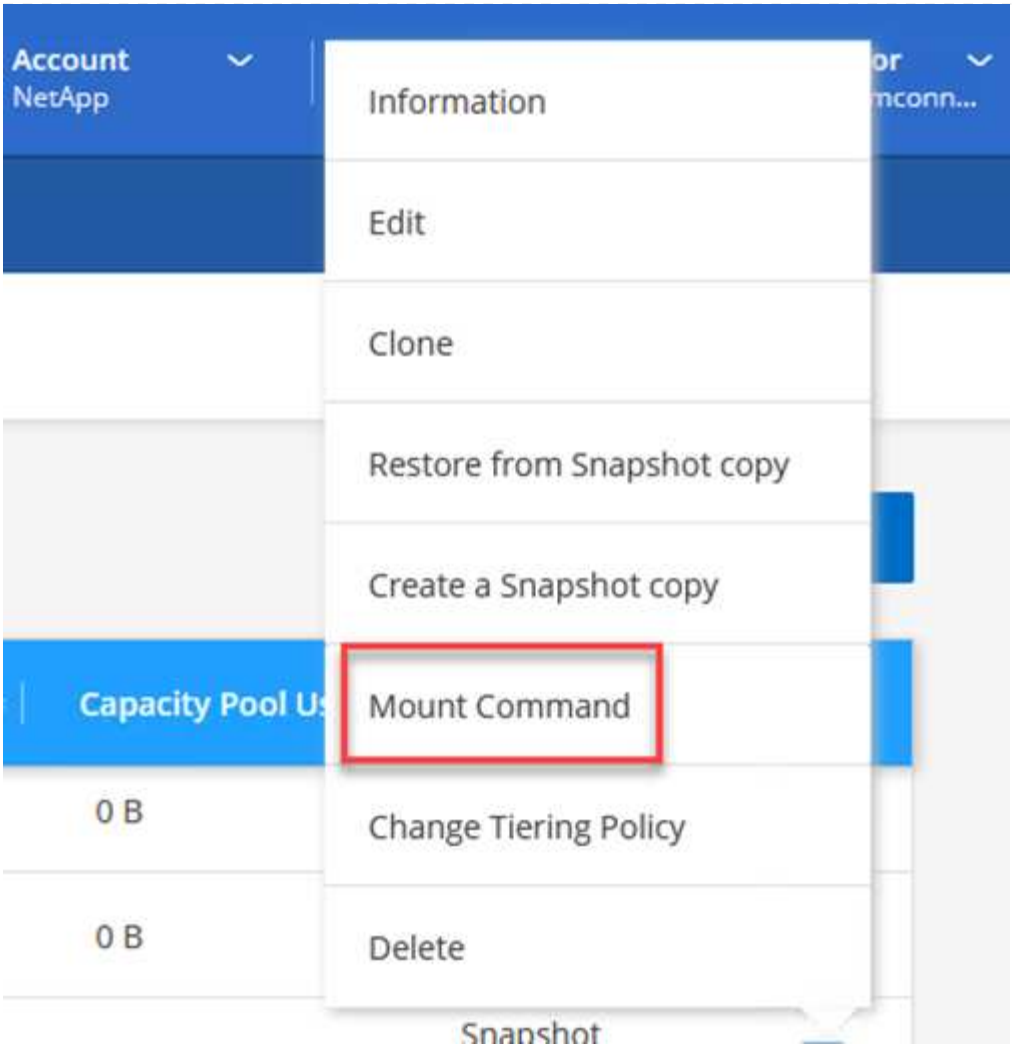
Oracle Serverに**NFS**ボリュームをマウントします

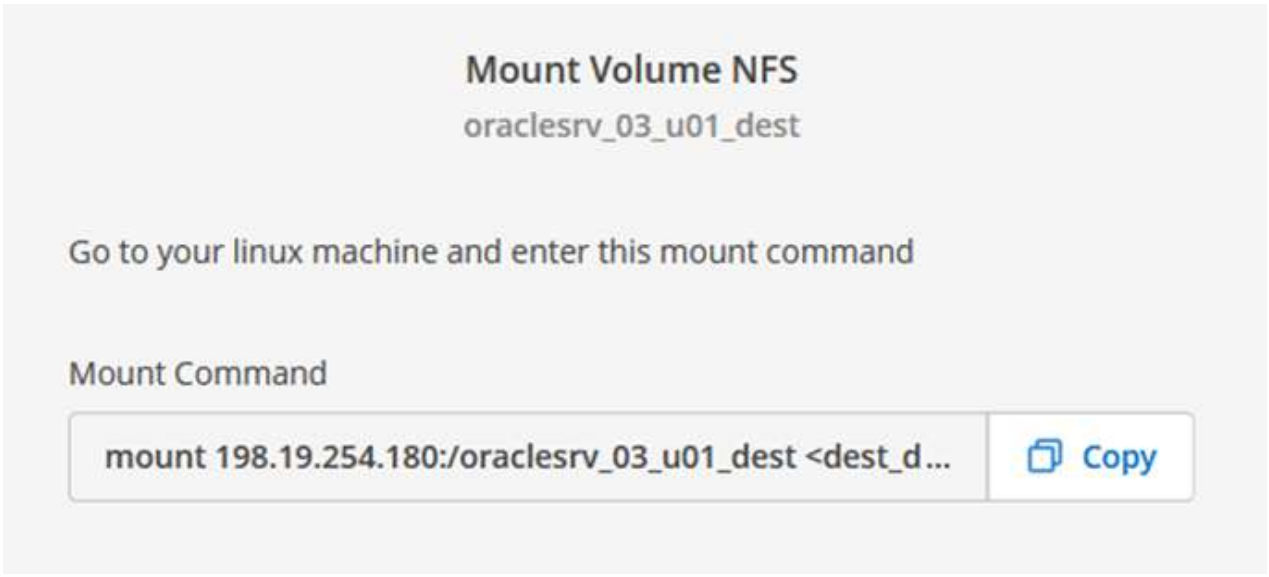
Cloud Managerでは、Oracleデータベースファイルとログを格納するNFSボリュームをマウントするための、正しいNFS LIFのIPアドレスを指定してmountコマンドを取得できます。

1. Cloud Managerで、FSXクラスタのボリュームのリストにアクセスします。



2. アクションメニューからマウントコマンドを選択し、Oracle Linuxサーバで使用するマウントコマンドを表示してコピーします。





3. NFSファイルシステムをOracle Linux Serverにマウントします。NFS共有をマウントするためのディレクトリがOracle Linuxホスト上にすでに存在している。
4. Oracle Linuxサーバから、mountコマンドを使用してNFSボリュームをマウントします。

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Oracleデータベースに関連付けられたボリュームごとに、この手順を繰り返します。

リブート時にNFSマウントを維持するには、ファイルを編集し `/etc/fstab`てmountコマンドを追加します。

5. Oracleサーバをリブートします。Oracleデータベースは正常に起動し、使用できるようになっている必要があります。

フェイルバック

このソリューションで説明しているフェイルオーバープロセスが正常に完了すると、SnapCenterとVeeamはAWSでのバックアップ機能を再開します。FSx ONTAPはプライマリストレージとして指定され、元のオンプレミスデータセンターとのSnapMirror関係は存在しません。オンプレミスで通常の機能が再開されたら、本ドキュメントに記載されているプロセスと同じ方法で、オンプレミスのONTAP ストレージシステムにデータをミラーリングできます。

このドキュメントでも説明しているように、アプリケーションデータボリュームをFSx ONTAPからオンプレミスのONTAPストレージシステムにミラーリングするようにSnapCenterを設定できます。同様に、スケールアウトバックアップリポジトリを使用してAmazon S3にバックアップコピーをレプリケートするようにVeeamを設定し、オンプレミスのデータセンターにあるVeeamバックアップサーバからこれらのバックアップにアクセスできるようにします。

フェイルバックについてはこのドキュメントでは説明していませんが、フェイルバックについてはここで説明する詳細なプロセスとはほとんど異なります。

まとめ

このドキュメントで紹介するユースケースでは、ネットアップとVMwareの統合に特化した、実績のあるディザスタリカバリテクノロジに焦点を当てています。ネットアップのONTAP ストレージシステムは、実績あるデータミラーリングテクノロジを提供します。このテクノロジを使用すると、業界をリードするクラウドプロバイダのオンプレミステクノロジとONTAP テクノロジにまたがるディザスタリカバリソリューションを設計できます。

FSx ONTAP on AWSは、SnapCenterやSyncMirrorとシームレスに統合してアプリケーションデータをクラウドにレプリケートできるソリューションの1つです。Veeam Backup & Replicationも、ネットアップのONTAPストレージシステムと緊密に統合され、vSphereネイティブストレージへのフェイルオーバーを可能にする、よく知られたテクノロジです。

この解決策 では、SQL ServerとOracleアプリケーションデータをホストしているONTAP システムから、ゲスト接続ストレージを使用してディザスタリカバリ解決策 を提供しています。SnapCenter とSnapMirrorを使用すると、ONTAP システム上のアプリケーションボリュームを保護し、それらをクラウド上のFSXまたはCVOにレプリケートするための管理しやすい解決策 が提供されます。SnapCenter は、DR対応の解決策 で、すべてのアプリケーションデータをAWS上のVMware Cloudにフェイルオーバーします。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

- 解決策 のドキュメントへのリンク

  "VMwareソリューションを使用したネットアップのハイブリッドマルチクラウド"

  "ネットアップのソリューション"

Amazon FSx ONTAPを使用したVMware CloudでのVeeamのバックアップとリストア

Veeam Backup & Replicationは、VMware Cloud内のデータを保護するための効果的で信頼性の高い解決策 です。このソリューションでは、Veeam Backup and Replicationを使用して、VMware CloudのFSx ONTAP NFSデータストアにあるアプリケーションVMをバックアップおよびリストアするための適切なセットアップと構成について説明します。

作成者：Josh Powell -ネットアップソリューションエンジニアリングチーム

概要

VMware Cloud（AWS）では、NFSデータストアを補助ストレージとして使用できます。FSx ONTAPは、SDDCクラスタ内のESXiホストの数に関係なく拡張できる、クラウドアプリケーション用の大量のデータを保存する必要があるお客様向けのセキュアなソリューションです。このAWS統合ストレージサービスは、従来のNetApp ONTAP の機能をすべて備えた、効率性に優れたストレージを提供します。

ユースケース

この解決策 は、次のユースケースに対応します。

- FSX ONTAPをバックアップリポジトリとして使用して、VMCでホストされているWindowsおよびLinux仮想マシンのバックアップとリストアを実行します。
- FSx ONTAPをバックアップリポジトリとして使用して、Microsoft SQL Serverアプリケーションデータをバックアップおよびリストアします。
- FSx ONTAPをバックアップリポジトリとして使用して、Oracleアプリケーションデータをバックアップおよびリストアします。

Amazon FSx ONTAPを使用したNFSデータストア

このソリューションのすべての仮想マシンは、FSx ONTAPの補完的NFSデータストア上に配置されます。FSx ONTAPを補完的NFSデータストアとして使用することには、いくつかのメリットがあります。たとえば、次のことが可能です。

- 複雑なセットアップと管理を必要とせずに、拡張性と可用性に優れたクラウドファイルシステムを構築できます。
- 既存のVMware環境との統合により、使い慣れたツールやプロセスを使用してクラウドリソースを管理できます。
- Snapshotやレプリケーションなど、ONTAP が提供する高度なデータ管理機能を活用して、データを保護し、データの可用性を確保できます。

解決策 の導入の概要

このリストには、Veeam Backup & Replicationの設定、バックアップリポジトリとしてFSx ONTAPを使用したバックアップジョブとリストアジョブの実行、SQL ServerとOracleのVMとデータベースのリストアに必要な手順の概要が記載されています。

1. Veeam Backup & ReplicationのiSCSIバックアップリポジトリとして使用するFSx ONTAPファイルシステムを作成します。
2. Veeam Proxyを導入して、バックアップワークロードを分散し、FSx ONTAPでホストされたiSCSIバックアップリポジトリをマウントします。
3. SQL Server、Oracle、Linux、Windowsの仮想マシンをバックアップするようにVeeam Backup Jobsを設定します。
4. SQL Server仮想マシンおよび個 々 のデータベースをリストアします。
5. Oracle仮想マシンおよび個 々 のデータベースをリストアします。

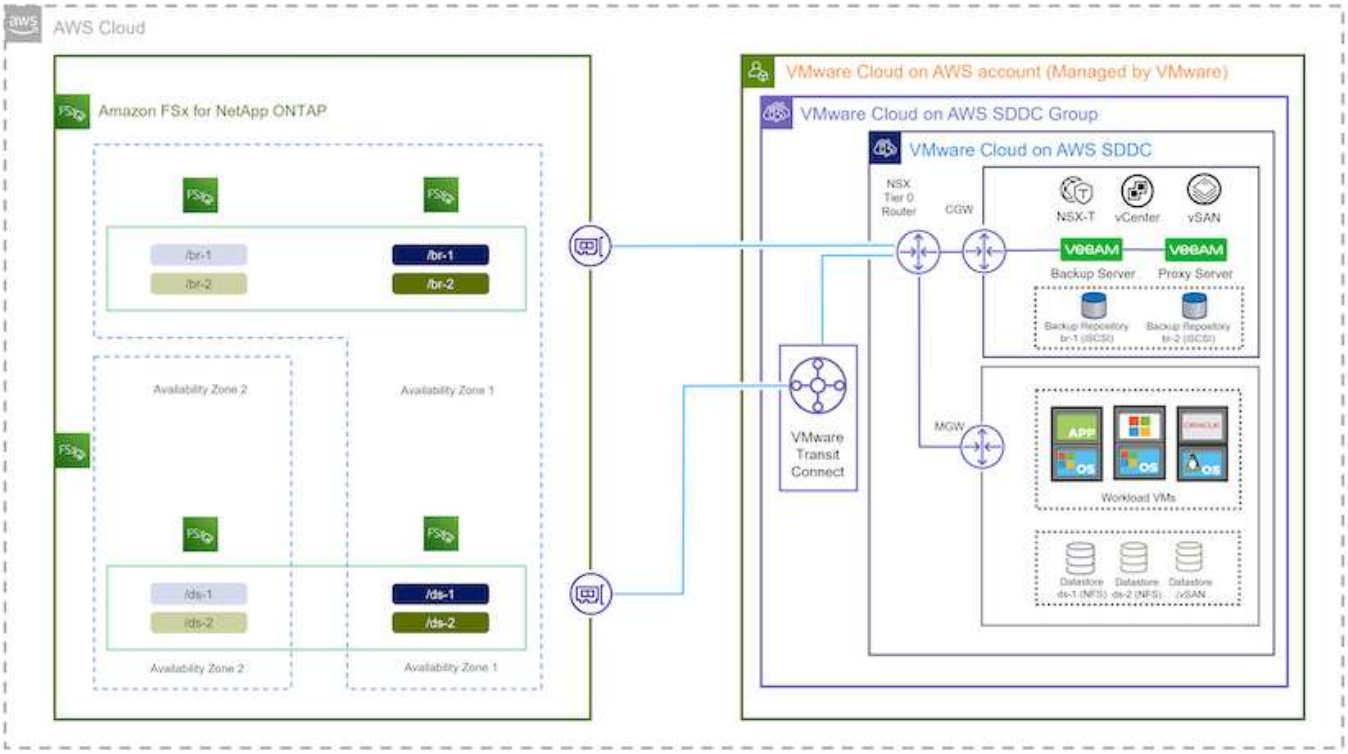
前提条件

このソリューションの目的は、VMware Cloudで実行され、FSx ONTAPでホストされるNFSデータストア上に配置された仮想マシンのデータ保護を実証することです。この解決策 は、次のコンポーネントが構成され、使用可能な状態にあることを前提としています。

1. VMware Cloudに接続された1つ以上のNFSデータストアで構成されるFSx ONTAPファイルシステム。
2. Veeam Backup & Replicationソフトウェアがインストールされたマイクロソフト Windows Server VM。
   - vCenter Serverが、IPアドレスまたは完全修飾ドメイン名を使用してVeeam Backup & Replicationサーバによって検出されている。
3. 解決策 の導入時にVeeamバックアッププロキシコンポーネントとともにインストールするMicrosoft Windows Server VM。
4. Microsoft SQL Server VMとVMDKおよびアプリケーションデータがFSx ONTAP NFSデータストアに格納されている。この解決策 では、2つのSQLデータベースを2つの独立したVMDKに格納しました。
   - 注：ベストプラクティスとして、データベースとトランザクションログファイルは別 々 のドライブに配置します。これにより、パフォーマンスと信頼性が向上します。これは、トランザクションログがシーケンシャルに書き込まれるのに対し、データベースファイルはランダムに書き込まれるためです。
5. OracleデータベースVMとVMDKおよびアプリケーションデータがFSx ONTAP NFSデータストアに格納されている。
6. FSx ONTAP NFSデータストア上に配置されたVMDKを使用したLinuxおよびWindowsのファイルサーバVM。
7. Veeamには、バックアップ環境のサーバとコンポーネント間の通信に特定のTCPポートが必要です。Veeamバックアップインフラコンポーネントでは、必要なファイアウォールルールが自動的に作成されます。ネットワークポート要件の詳細なリストについては、の「ポート」のセクションを参照して "Veeam Backup and Replication User Guide for VMware vSphereを参照してください"ください。

アーキテクチャの概要

この解決策 のテストと検証は、最終的な導入環境と異なる場合があるラボで実施しました。詳細については、次のセクションを参照してください。



ハードウェア/ソフトウェアコンポーネント

このソリューションの目的は、VMware Cloudで実行され、FSx ONTAPでホストされるNFSデータストア上に配置された仮想マシンのデータ保護を実証することです。この解決策 では、次のコンポーネントが設定済みで、使用可能な状態であることを前提としています。

- FSx ONTAP NFSデータストアに配置されたMicrosoft Windows VM
- FSx ONTAP NFSデータストア上のLinux（CentOS）VM
- FSx ONTAP NFSデータストアに配置されたMicrosoft SQL Server VM
  - 2つのデータベースが別 々 のVMDKにホストされている
- FSx ONTAP NFSデータストアにOracle VMを配置

解決策 の導入

この解決策 では、Veeam Backup & Replicationソフトウェアを使用して、AWS上のVMwareクラウドSDDC内のSQL Server、Oracle、WindowsおよびLinuxファイルサーバ仮想マシンのバックアップとリカバリを実行する解決策 の導入と検証の詳細な手順を説明します。このソリューションの仮想マシンは、FSx ONTAPによってホストされる補完的なNFSデータストアに配置されます。また、Veeamバックアップリポジトリに使用されるiSCSIボリュームのホストには、独立したFSx ONTAPファイルシステムが使用されます。

FSx ONTAPファイルシステムの作成、バックアップリポジトリとして使用するiSCSIボリュームのマウント、

バックアップジョブの作成と実行、VMとデータベースのリストアについて説明します。

FSx ONTAPの詳細については、を参照してください "FSx ONTAPユーザガイド"。

Veeam Backup and Replicationの詳細については、サイトを参照して "Veeam Help Centerテクニカルドキュメント"ください。

Veeam Backup and ReplicationをVMware Cloud on AWSで使用する場合の考慮事項と制限事項については、を参照してください "VMware Cloud on AWSおよびVMware Cloud on Dell EMCサポート考慮事項および制限事項"。

Veeam Proxyサーバを導入します

VeeamプロキシサーバはVeeam Backup & Replicationソフトウェアのコンポーネントで、ソースとバックアップまたはレプリケーションのターゲットを仲介します。プロキシサーバは、データをローカルで処理することで、バックアップジョブ中のデータ転送の最適化と高速化に役立ちます。また、さまざまな転送モードを使用して、VMware vStorage APIs for Data Protectionまたはダイレクトストレージアクセスを使用してデータにアクセスできます。

Veeamプロキシサーバの設計を選択する際には、同時に実行するタスクの数、転送モード、または必要なストレージアクセスの種類を考慮することが重要です。

プロキシサーバの数およびシステム要件については、を参照してください "Veeam VMware vSphere Best Practice Guideを参照してください"。

Veeam Data MoverはVeeam Proxy Serverのコンポーネントであり、ソースからVMデータを取得してターゲットに転送する方法としてトランスポートモードを使用します。転送モードは、バックアップジョブの設定時に指定します。ストレージへの直接アクセスを使用することで、NFSデータストアからのバックアップ効率を高めることができます。

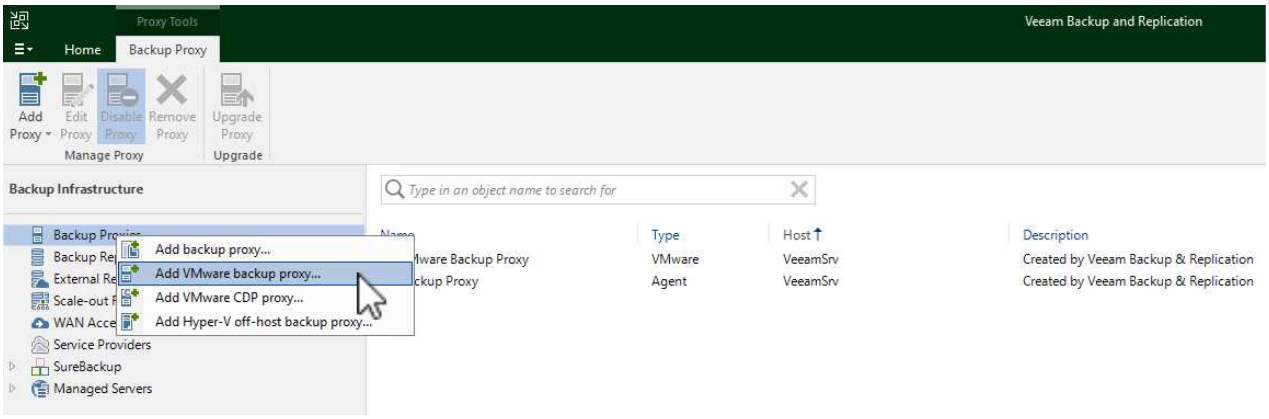
トランスポートモードの詳細については、を参照して "Veeam Backup and Replication User Guide for VMware vSphereを参照してください"ください。

次の手順では、VMware Cloud SDDC内のWindows VMにVeeam Proxy Serverを導入します。

Veeam Proxyを導入してバックアップワークロードを分散

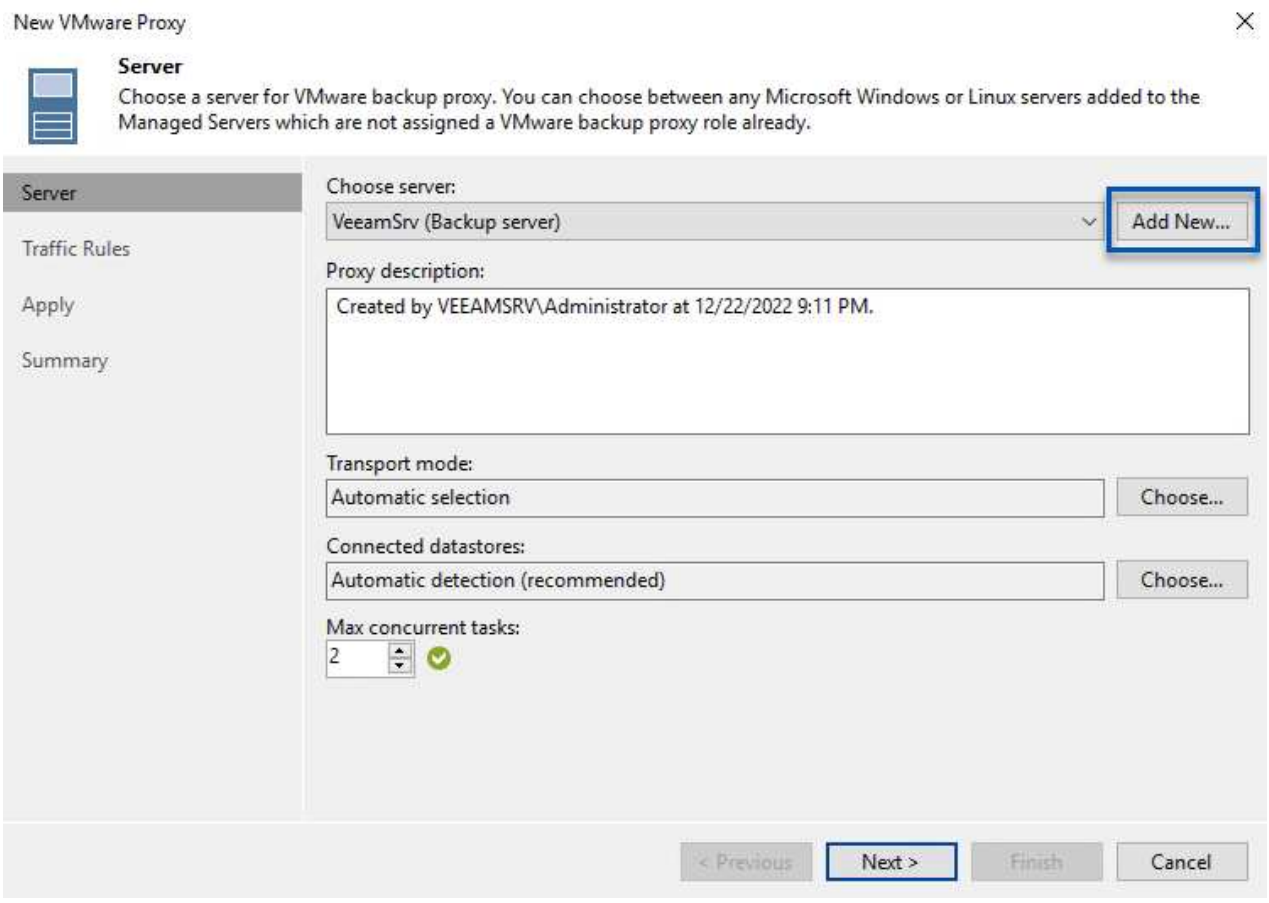
この手順では、Veeamプロキシを既存のWindows VMに導入します。これにより、プライマリVeeam Backup ServerとVeeam Proxyの間でバックアップジョブを分散させることができます。

1. Veeam Backup and Replicationサーバで、管理コンソールを開き、左下のメニューから*[バックアップインフラストラクチャ]*を選択します。
2. を右クリックし、[VMwareバックアッププロキシの追加…]*をクリックしてウィザードを開きます。

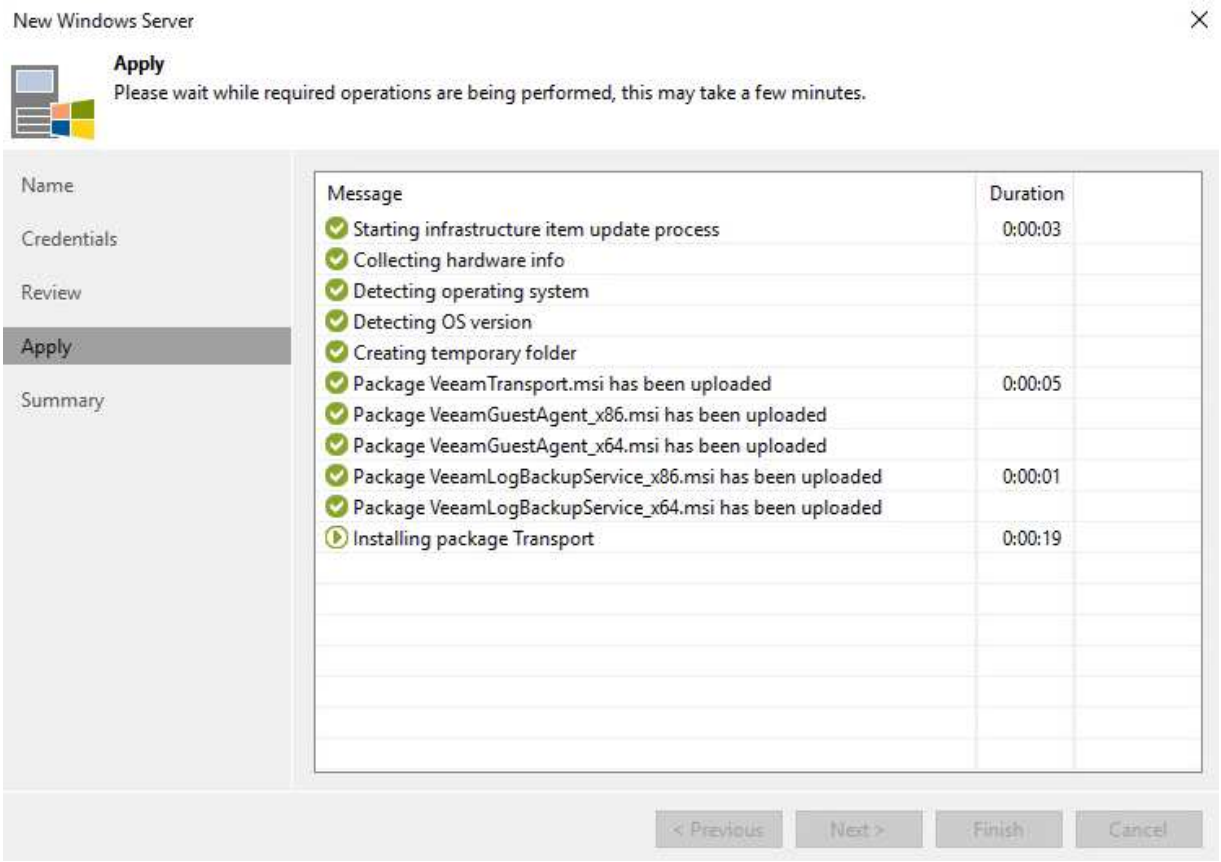


ウィザードを開きます"]

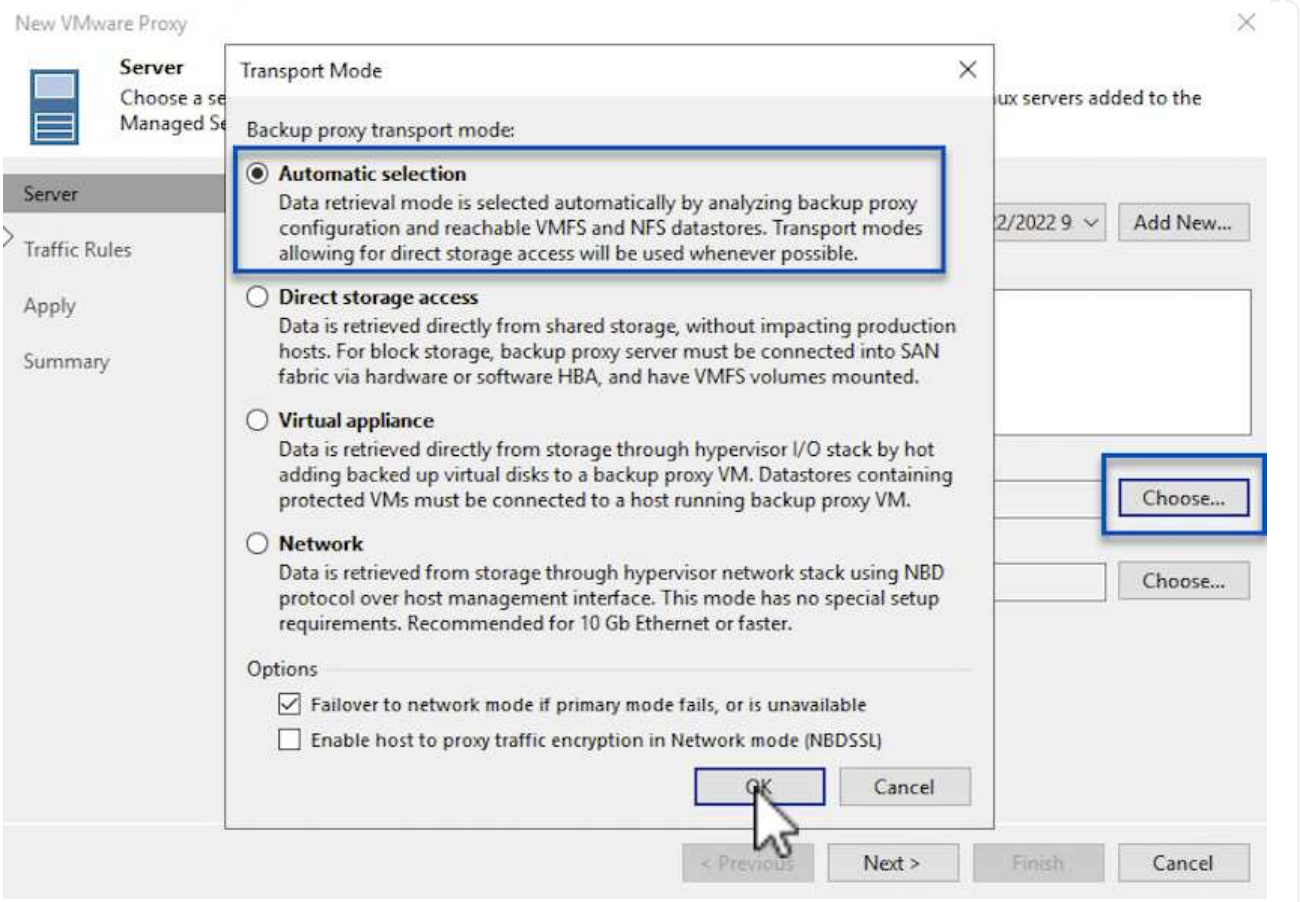
3. VMware Proxyの追加*ウィザードで*新規追加…*ボタンをクリックして、新しいプロキシサーバーを追加します。



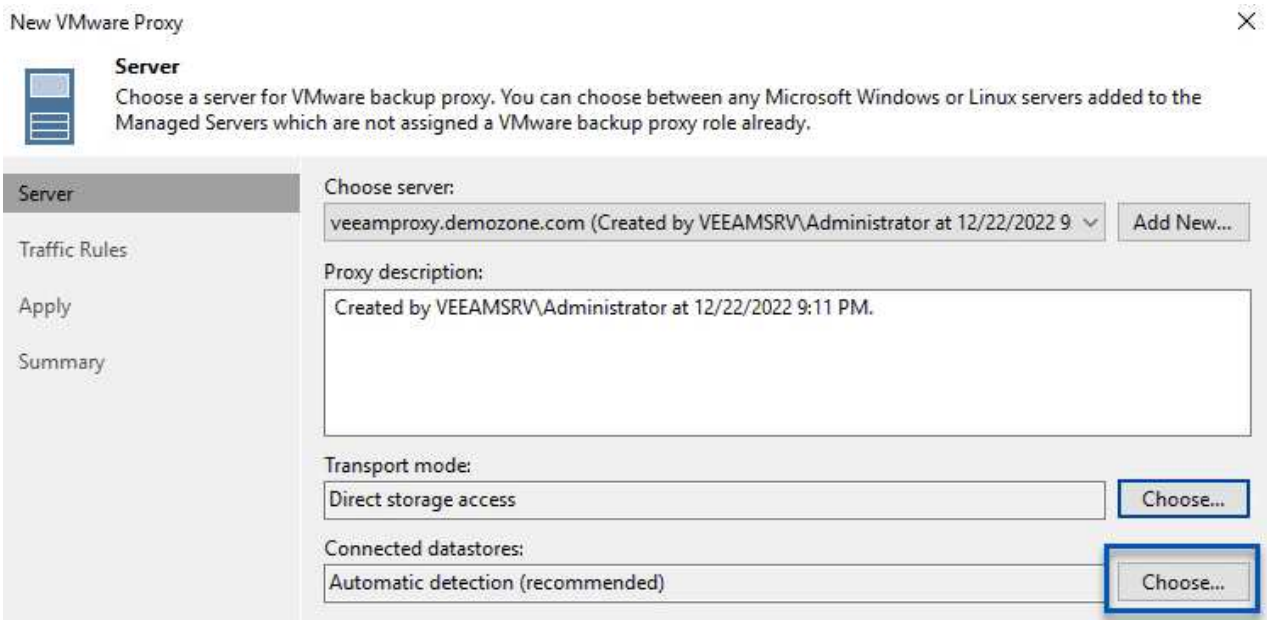
4. Microsoft Windowsを追加する場合に選択し、プロンプトに従ってサーバを追加します。
   - DNS名またはIPアドレスを入力します
   - 新しいシステムのクレデンシャルに使用するアカウントを選択するか、新しいクレデンシャルを追加します
   - インストールするコンポーネントを確認し、*適用*をクリックして導入を開始します

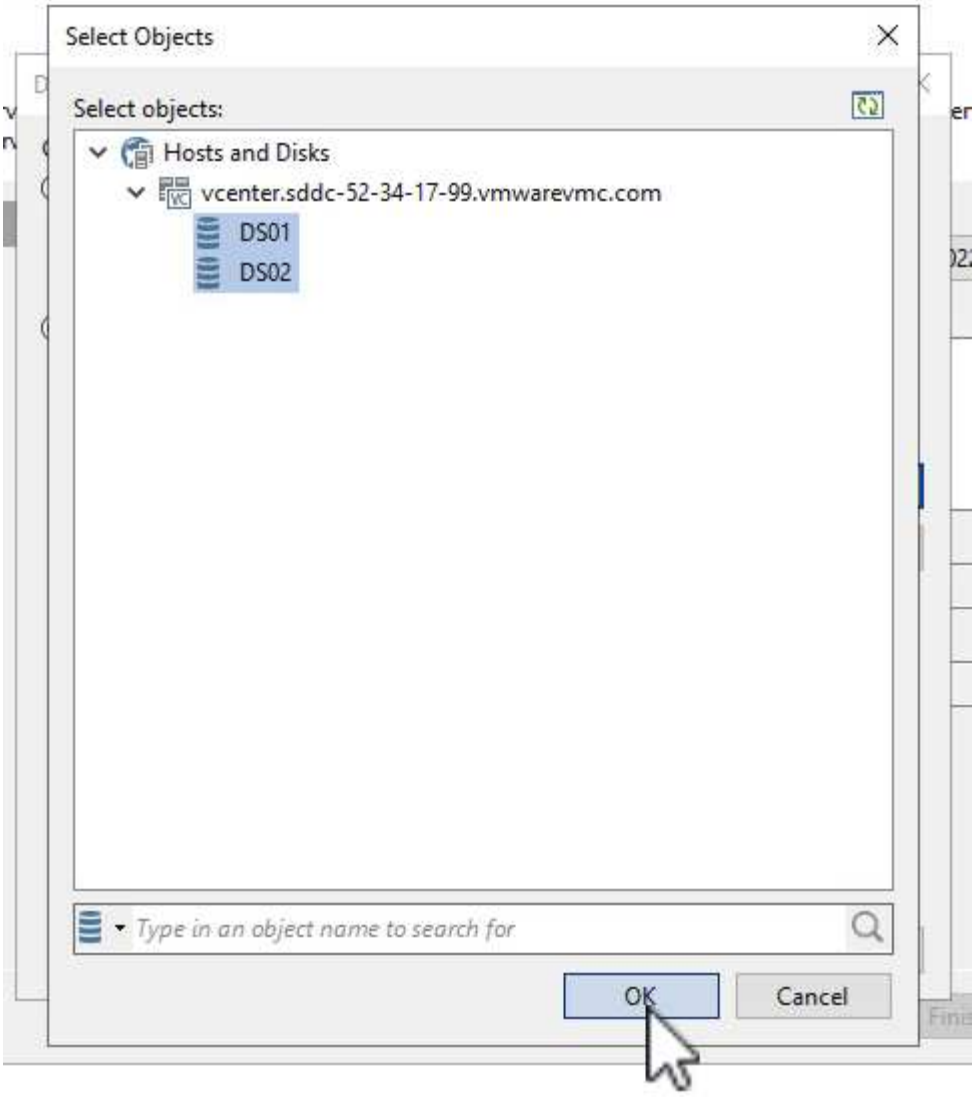


5. [New VMware Proxy]ウィザードに戻り、[Transport Mode]を選択します。ここでは、*自動選択*を選択しました。

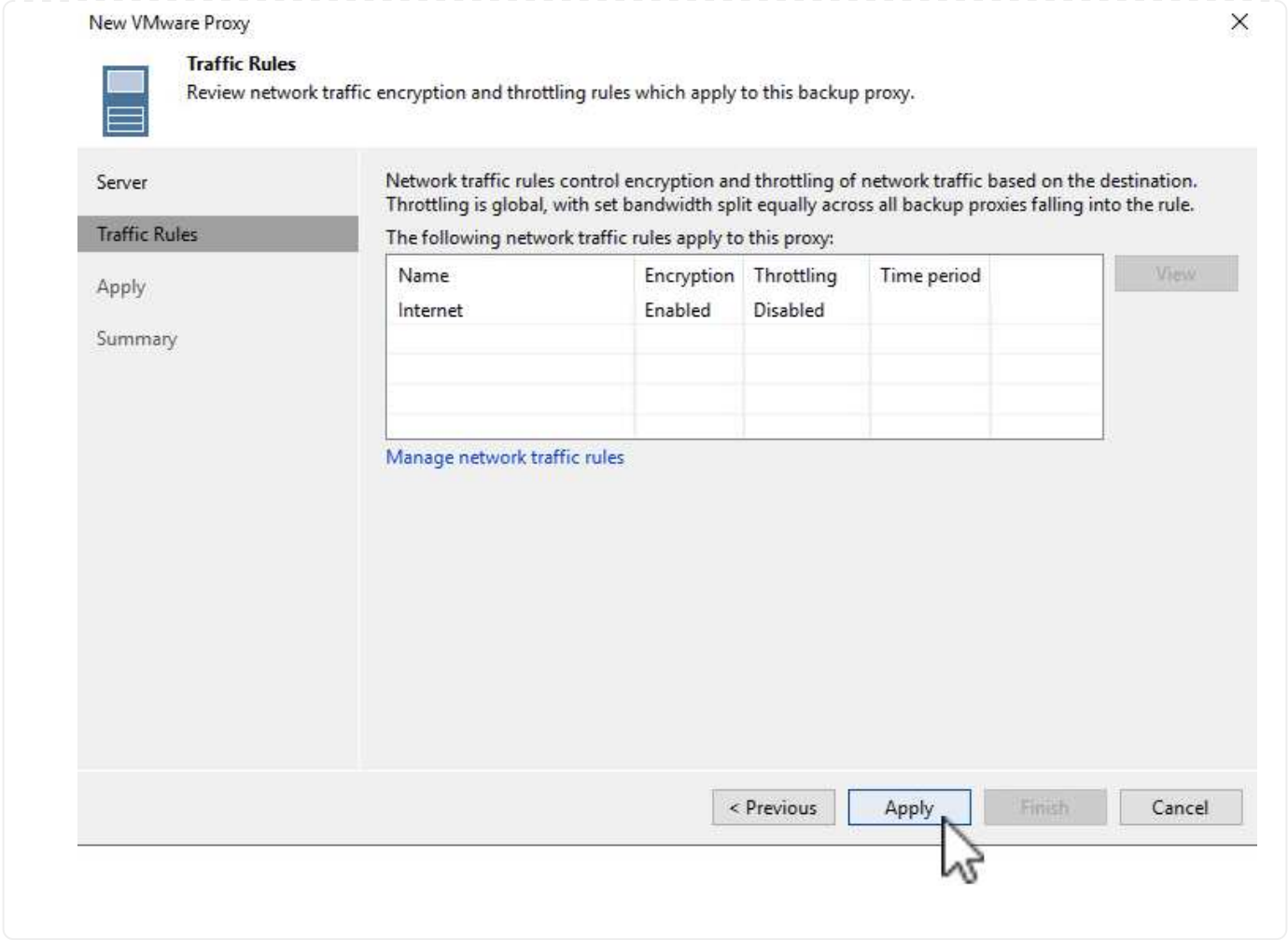


6. VMware Proxyから直接アクセスできるようにする、接続されているデータストアを選択します。





7. 暗号化やスロットリングなど、必要な特定のネットワークトラフィックルールを設定して適用します。完了したら、*[適用]*ボタンをクリックして導入を完了します。



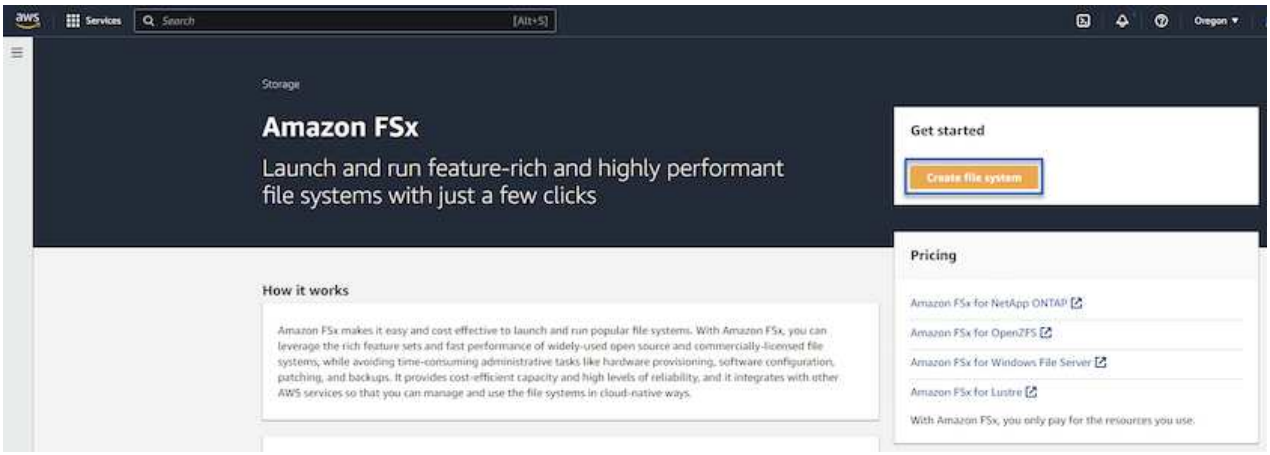
ストレージとバックアップリポジトリを設定します

プライマリVeeam BackupサーバとVeeam Proxyサーバは、直接接続されたストレージ形式のバックアップリポジトリにアクセスできます。このセクションでは、FSx ONTAPファイルシステムの作成、Veeamサーバへのi SCSI LUNのマウント、バックアップリポジトリの作成について説明します。

FSx ONTAPファイルシステムの作成

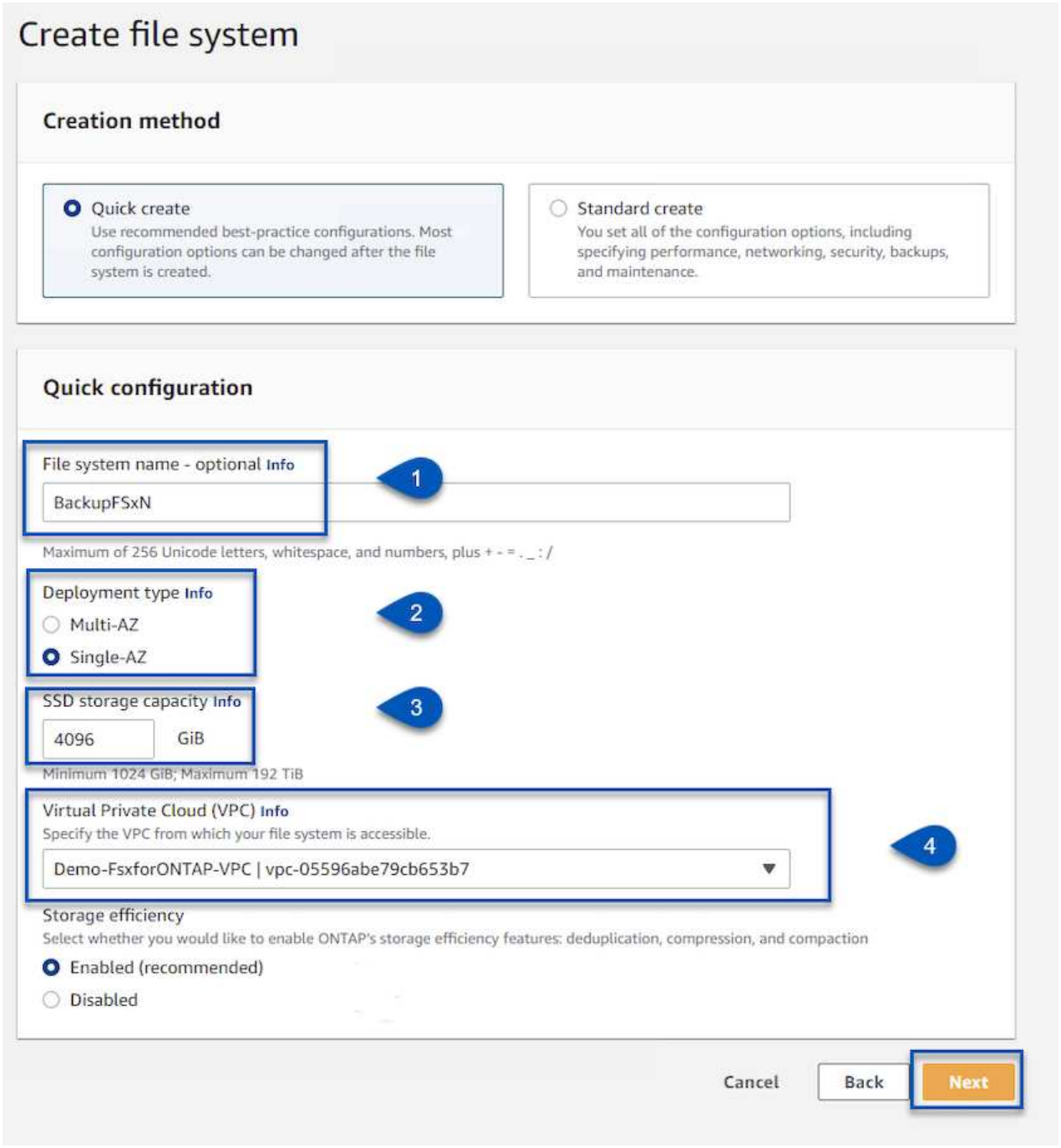
Veeamバックアップリポジトリ用のiSCSIボリュームのホストに使用するFSx ONTAPファイルシステムを作成します。

1. AWSコンソールで、FSxに移動し、*ファイルシステムの作成*をクリックします



2. Amazon FSx ONTAP を選択し、 Next *を選択して続行します。

3. ファイルシステム名、導入タイプ、SSDストレージ容量、FSx ONTAPクラスタを配置するVPCを入力します。これは、VMware Cloud内の仮想マシンネットワークと通信するように設定されたVPCである必要があります。[次へ]*をクリックします。



4. 導入手順を確認し、* Create File System *をクリックしてファイルシステムの作成プロセスを開始します。

iSCSI LUNを設定してマウントします

FSx ONTAPでiSCSI LUNを作成して設定し、Veeamバックアップサーバとプロキシサーバにマウントします。これらのLUNは、あとでVeeamバックアップリポジトリの作成に使用されます。

FSx ONTAPでiSCSI LUNを作成するプロセスは複数の手順で構成されます。ボリューム作成の最初のステップは、Amazon FSxコンソールまたはNetApp ONTAP CLIで実行できます。

FSx ONTAPの使用方法の詳細については、を参照して "FSx ONTAPユーザガイド"ください。

1. NetApp ONTAP CLIから次のコマンドを使用して初期ボリュームを作成します。

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. 前の手順で作成したボリュームを使用してLUNを作成します。

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. Veeamバックアップサーバとプロキシサーバのiscsi IQNを含むイニシエータグループを作成して、LUNへのアクセスを許可します。

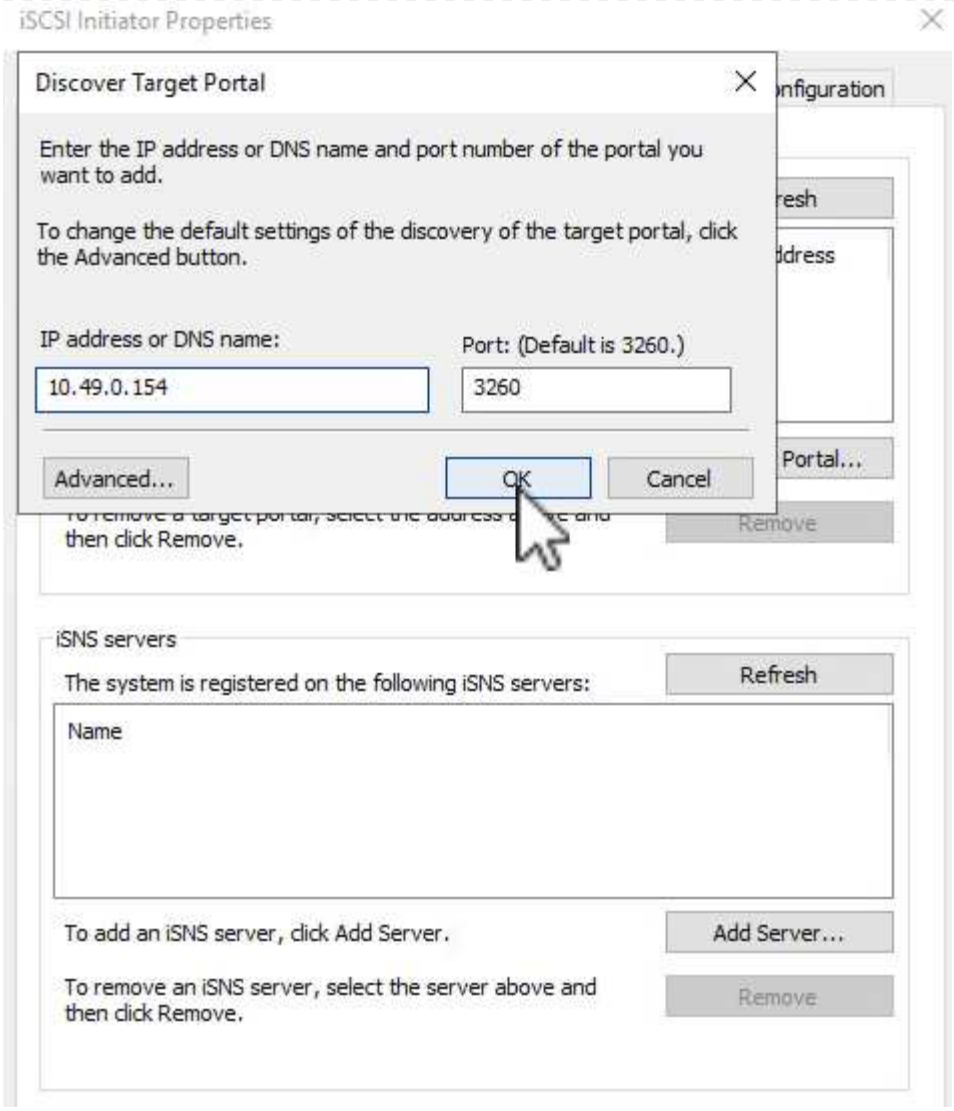
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

前の手順を完了するには、まずWindowsサーバのiSCSIイニシエータプロパティからIQNを取得する必要があります。

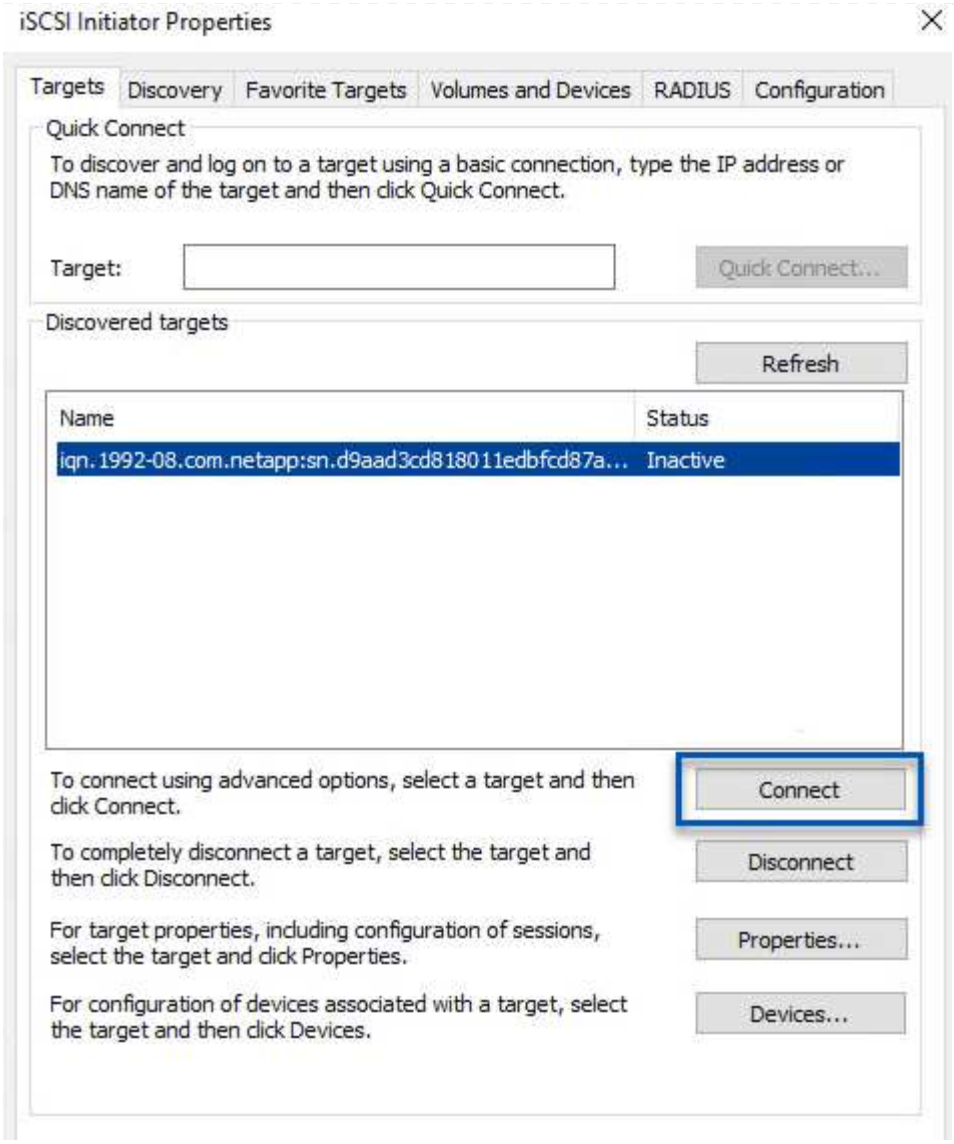
4. 最後に、作成したigroupにLUNをマッピングします。

```
FSx-Backup::> lun mapping create -vserver svm_name -path
/vol/vol_name/lun_name igroup igroup_name
```

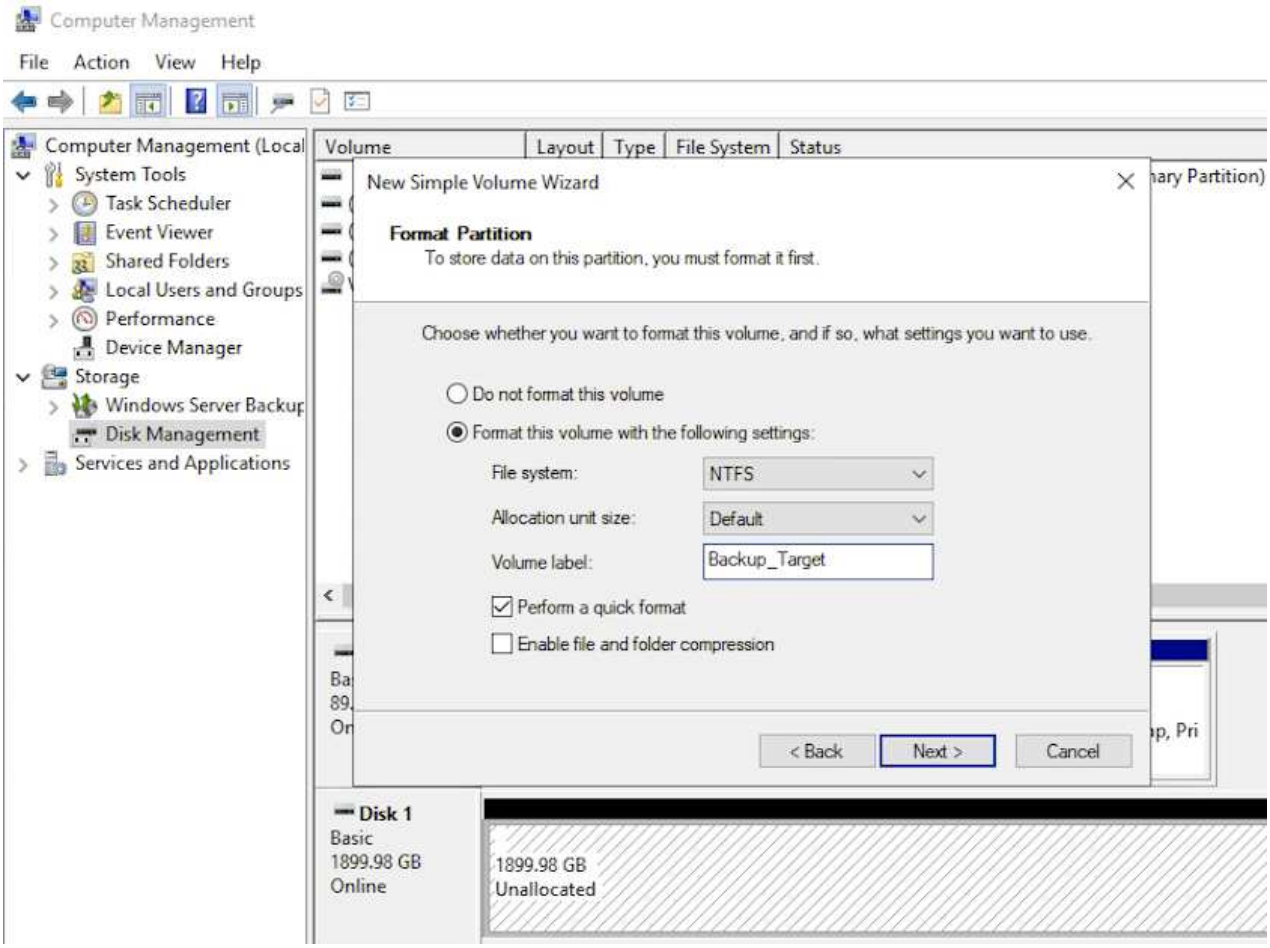
5. iSCSI LUNをマウントするには、Veeam Backup & Replication Serverにログインし、[iSCSI Initiator Properties]を開きます。[検出]タブに移動し、iSCSIターゲットのIPアドレスを入力します。



6. [ターゲット]タブで、非アクティブなLUNをハイライト表示し、**[接続]***をクリックします。**[Enable multi-path]***ボックスをオンにし、[OK]*をクリックしてLUNに接続します。



7. ディスクの管理ユーティリティで、新しいLUNを初期化し、必要な名前とドライブレターでボリュームを作成します。ボックスをオンにし、[OK]*をクリックしてLUNに接続します。

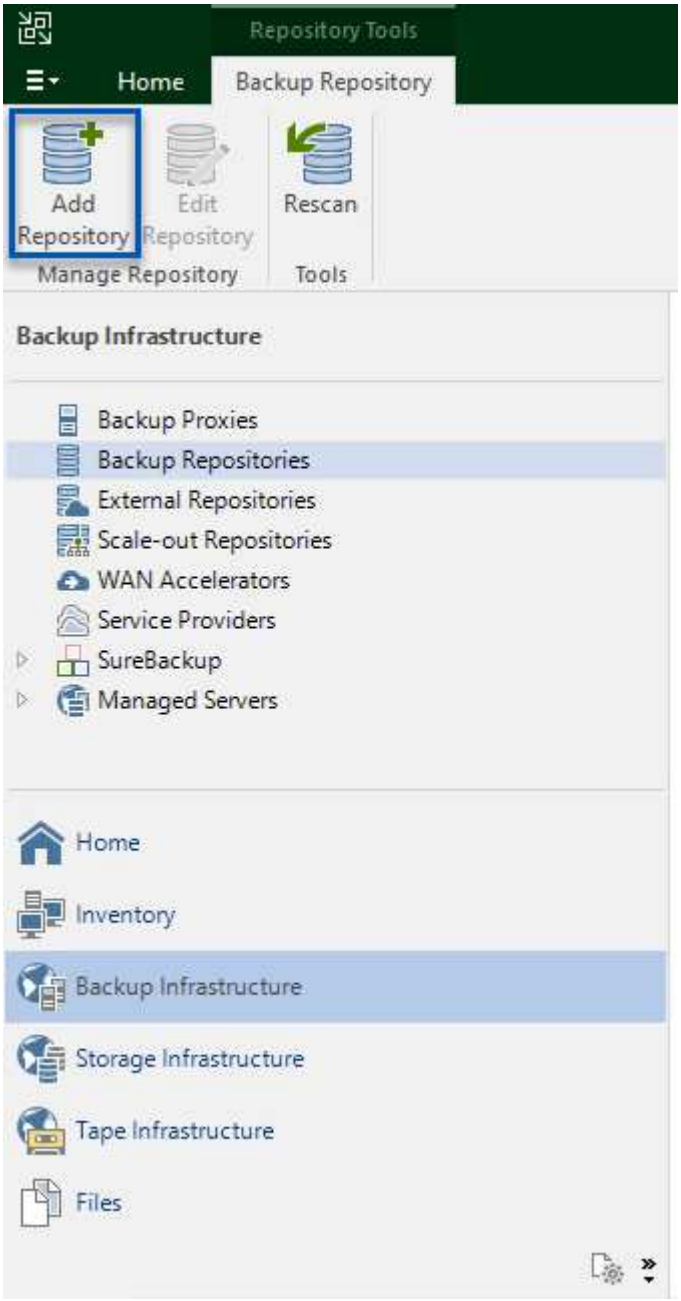


8. 同じ手順を繰り返して、iSCSIボリュームをVeeam Proxyサーバにマウントします。

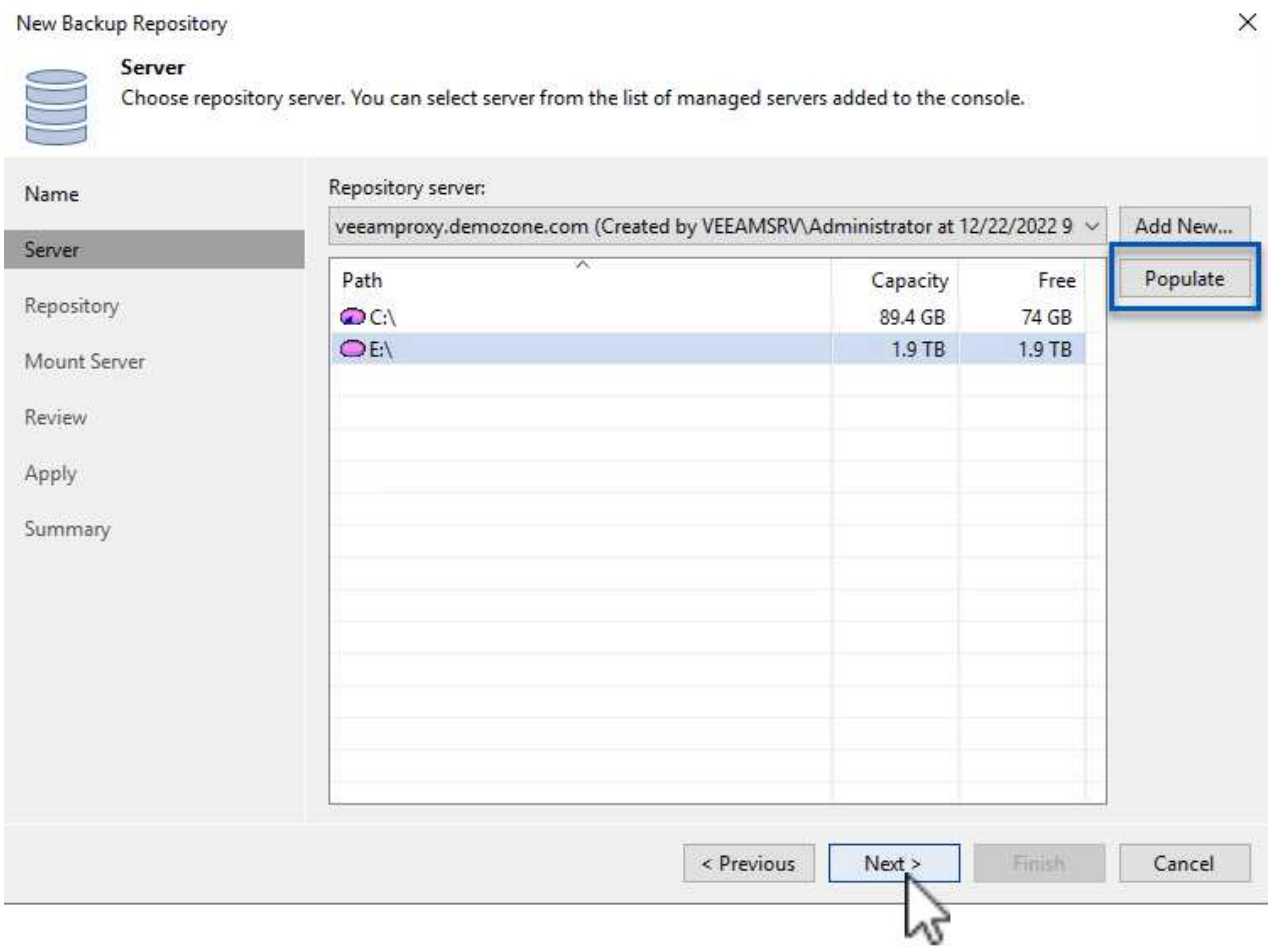
Veeamバックアップリポジトリを作成します

Veeam Backup and Replicationコンソールで、Veeam BackupサーバとVeeam Proxyサーバのバックアップリポジトリを作成します。これらのリポジトリは、仮想マシンのバックアップのバックアップターゲットとして使用されます。

1. Veeam Backup and Replicationコンソールで、左下の*をクリックし、[リポジトリの追加]*を選択します

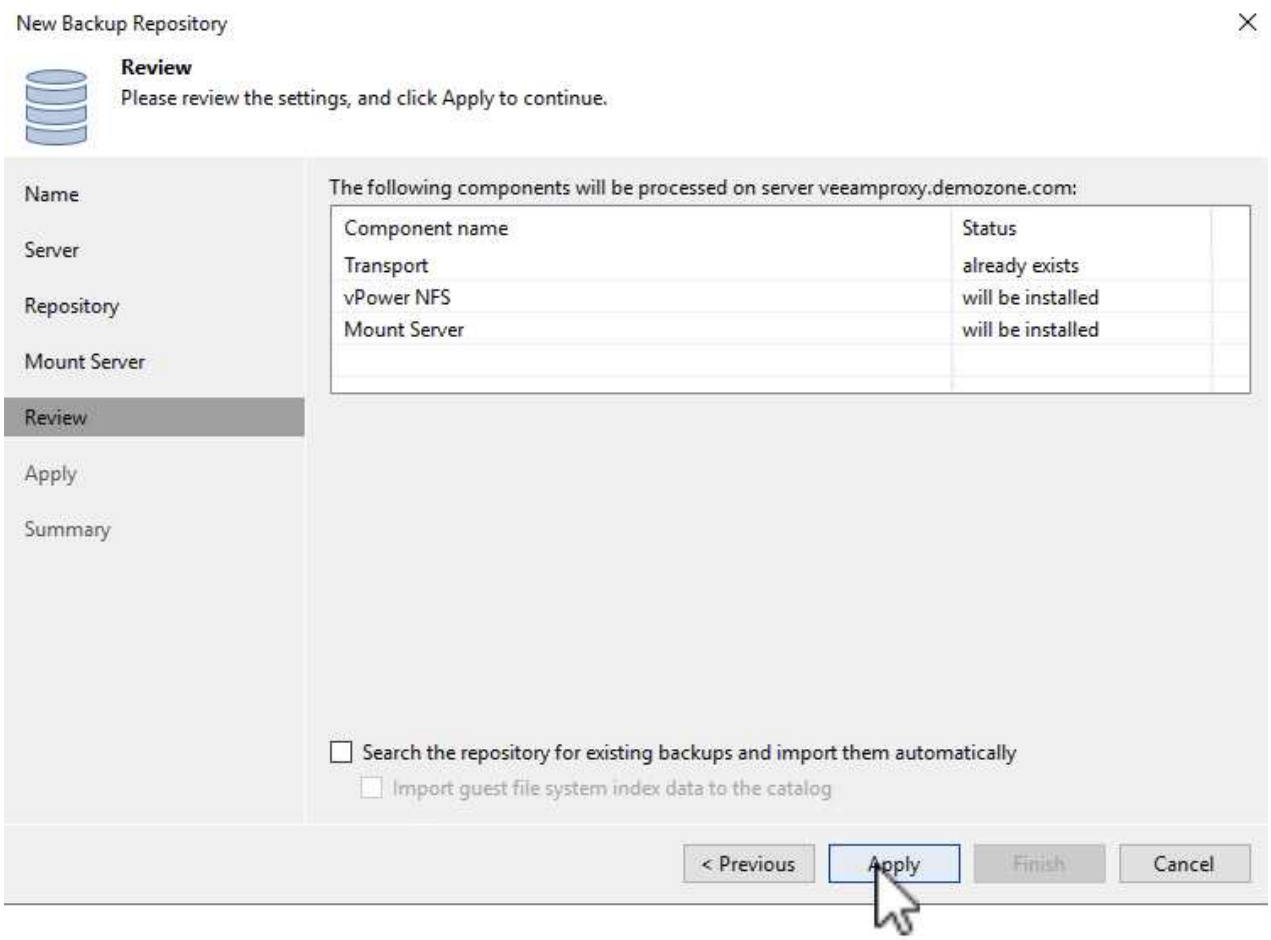


2. [New Backup Repository]ウィザードで、リポジトリの名前を入力し、ドロップダウンリストからサーバを選択して*[Populate]*ボタンをクリックし、使用するNTFSボリュームを選択します。



を選択します"]

3. 次のページで'高度なリストアを実行するときにバックアップのマウント先となるマウント・サーバを選択しますデフォルトでは、リポジトリストレージが接続されているサーバと同じです。
4. 選択内容を確認し、*[適用]*をクリックしてバックアップリポジトリの作成を開始します。



を選択します"]

5. 追加のプロキシサーバについて、上記の手順を繰り返します。

Veeamバックアップジョブを設定します

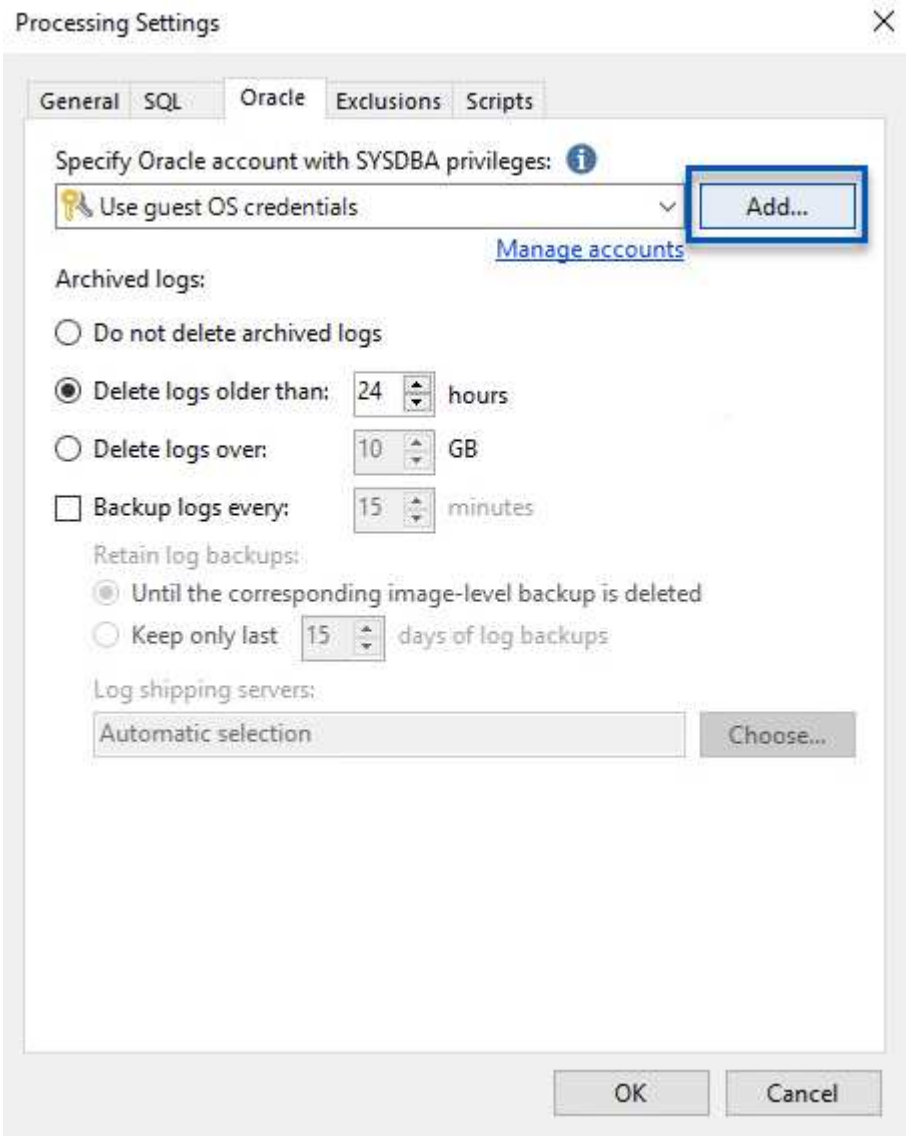
バックアップジョブは、前のセクションのバックアップリポジトリを使用して作成します。バックアップジョブの作成は、ストレージ管理者の業務の通常の一部であり、ここで紹介するすべての手順を網羅しているわけではありません。Veeamでのバックアップジョブの作成の詳細については、を参照して "Veeam Help Center テクニカルドキュメント"ください。

この解決策 では、次の項目に対して個別のバックアップジョブが作成されました。

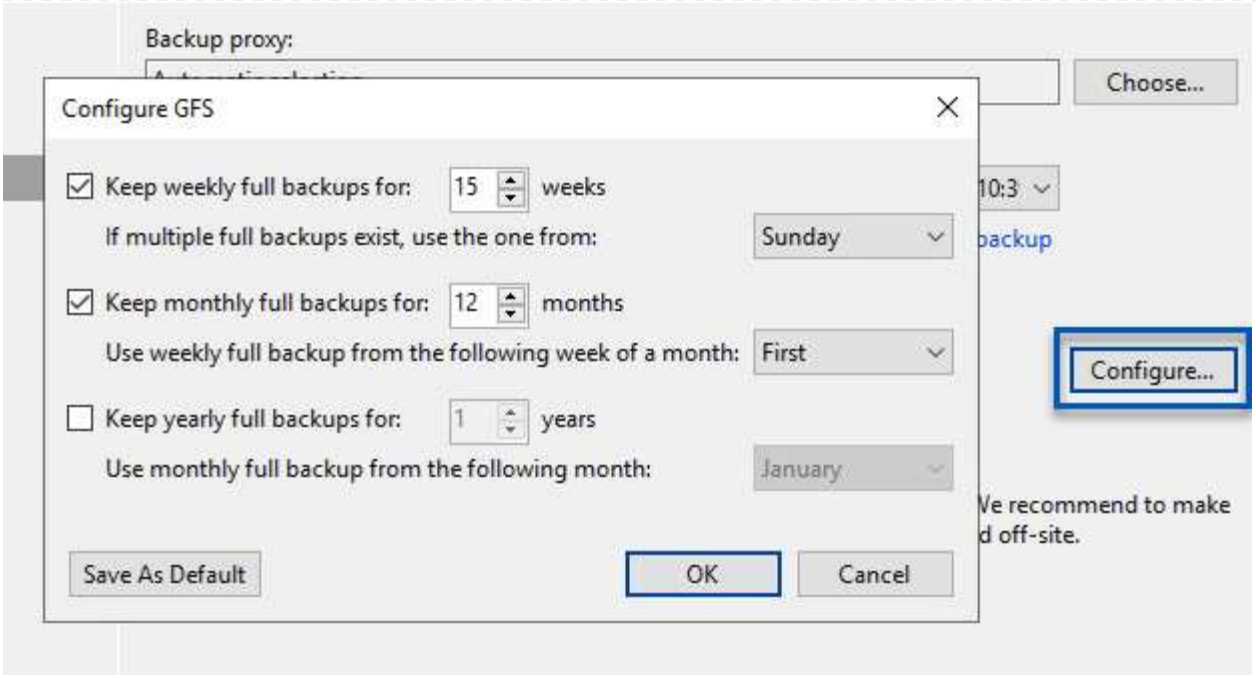
- Microsoft Windows SQL Serverの略
- Oracleデータベースサーバ
- Windowsファイルサーバ
- Linuxファイルサーバ

Veeamバックアップジョブを設定する際の一般的な考慮事項

1. アプリケーション対応の処理で整合性のあるバックアップを作成し、トランザクションログ処理を実行できます。
2. アプリケーション対応の処理を有効にした後、ゲストOSのクレデンシャルとは異なる可能性があるため、管理者権限を持つ正しいクレデンシャルをアプリケーションに追加します。



3. バックアップの保持ポリシーを管理するには、**[**アーカイブ用に特定のフルバックアップを長く保持する**]***をオンにし、[設定...]*ボタンをクリックしてポリシーを設定します。



Veeamのフルリストアによるアプリケーション**VM**のリストア

アプリケーションのリストアを実行する最初のステップは、Veeamを使用したフルリストアの実行です。VMのフルリストアの電源がオンになっており、すべてのサービスが正常に実行されていることを確認しました。

サーバのリストアは、ストレージ管理者の業務の通常の一部であり、ここで説明するすべての手順を説明するわけではありません。Veeamでのフルリストアの実行の詳細については、を参照して "Veeam Help Centerテクニカルドキュメント"ください。

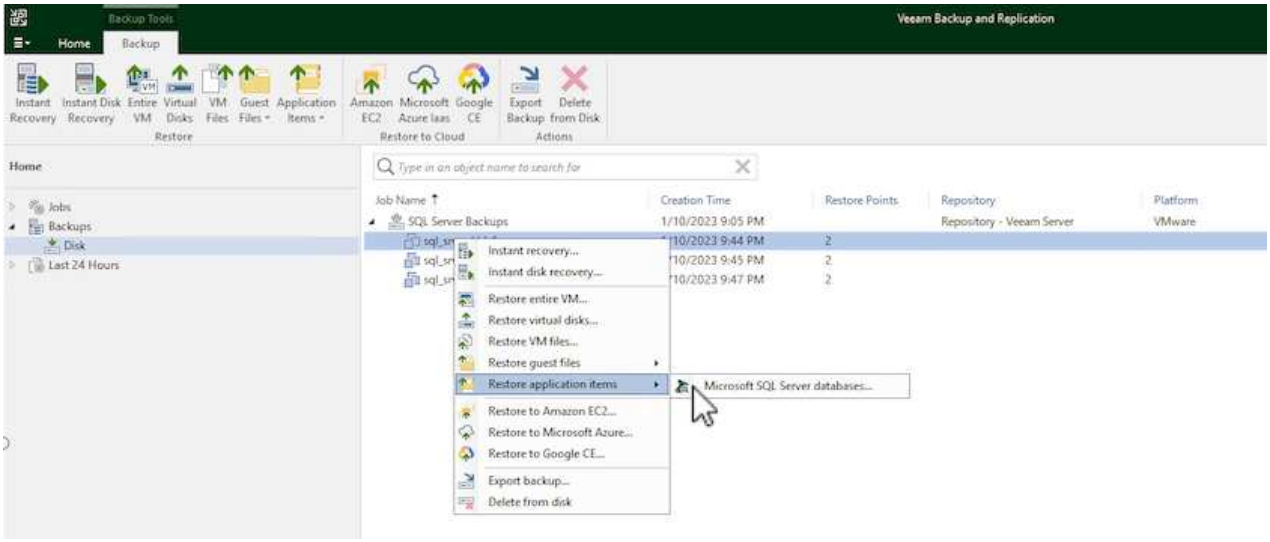
SQL Serverデータベースをリストアします

Veeam Backup & Replicationには、SQL Serverデータベースをリストアするためのオプションがいくつか用意されています。この検証では、Veeam Explorer for SQL ServerとInstant Recoveryを使用して、SQL Serverデータベースのリストアを実行しました。SQL Server Instant Recoveryは、データベースのフルリストアを待たずに、SQL Serverデータベースを迅速にリストアできる機能です。この迅速なリカバリプロセスにより、ダウンタイムが最小限に抑えられ、ビジネス継続性が確保されます。仕組みは次のとおりです。

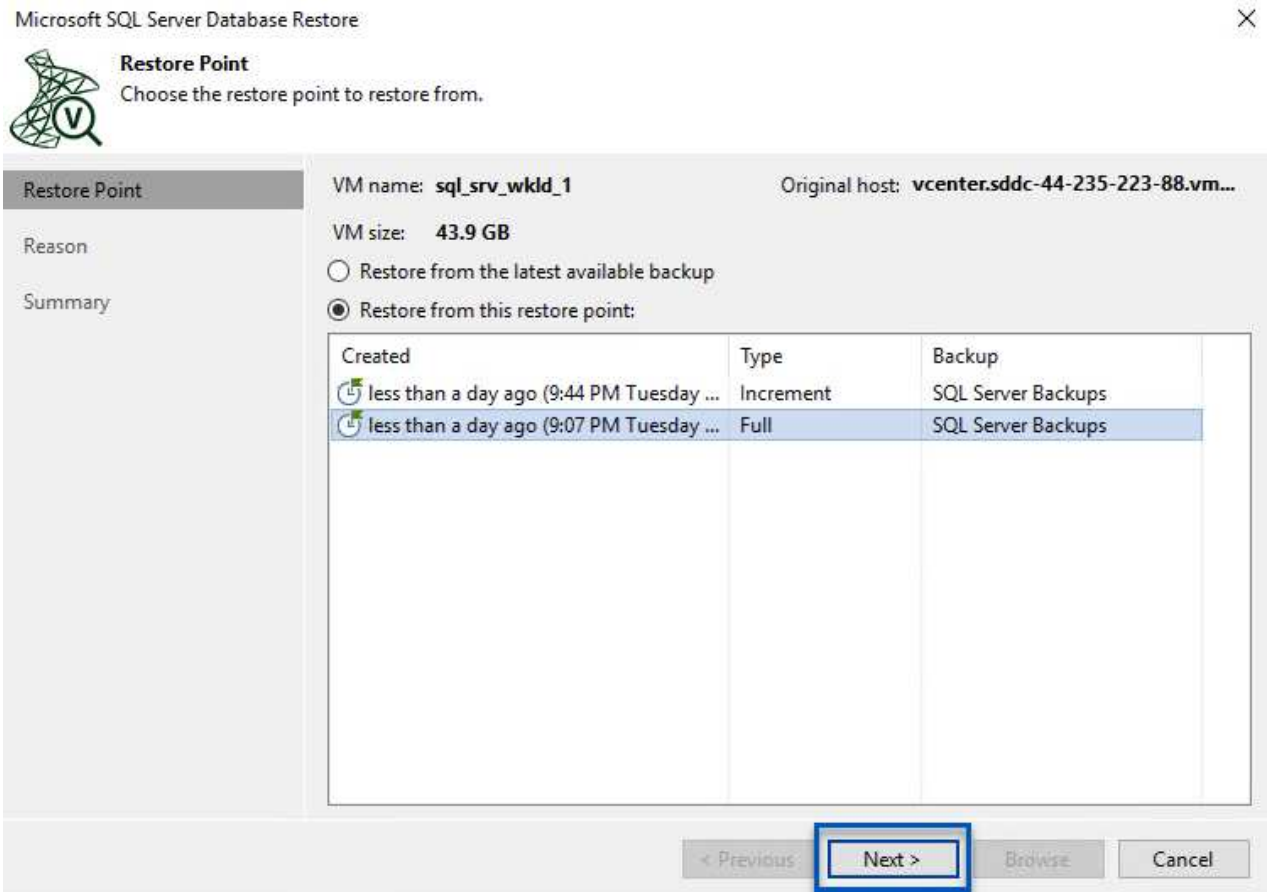
- Veeam Explorer *で、リストア対象のSQL Serverデータベースを含むバックアップ*をマウントします。
- ソフトウェア*は、マウントされたファイルからデータベース*を直接パブリッシュし、ターゲットSQL Serverインスタンス上の一時データベースとしてアクセスできるようにします。
- 一時データベースの使用中、Veeam Explorer *はユーザークエリ*をこのデータベースにリダイレクトし、ユーザーが引き続きデータにアクセスして作業できるようにします。
- Veeam *はバックグラウンドでフルデータベースリストア*を実行し、一時データベースから元のデータベースの場所にデータを転送します。
- フルデータベースのリストアが完了すると、Veeam Explorer *はユーザークエリを元の*データベースに戻し、一時データベースを削除します。

Veeam Explorer Instant Recoveryを使用して**SQL Server**データベースをリストアします

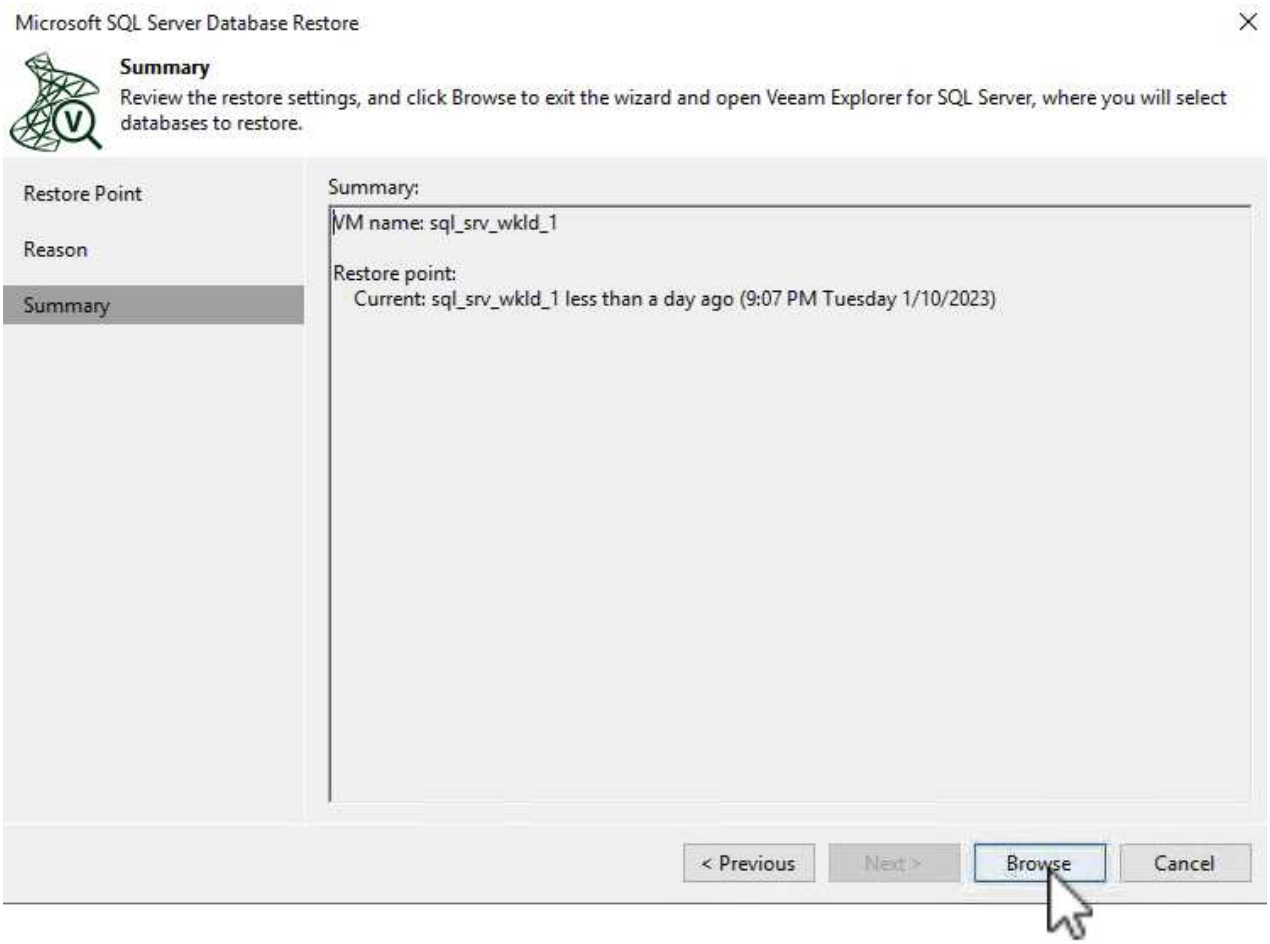
1. Veeam Backup & Replicationコンソールで、SQL Serverバックアップのリストに移動し、サーバを右クリックして*を選択し、[Microsoft SQL Serverデータベース…]*を選択します。



2. Microsoft SQL Serverデータベースのリストアウィザードで、リストからリストアポイントを選択し、*[次へ]*をクリックします。

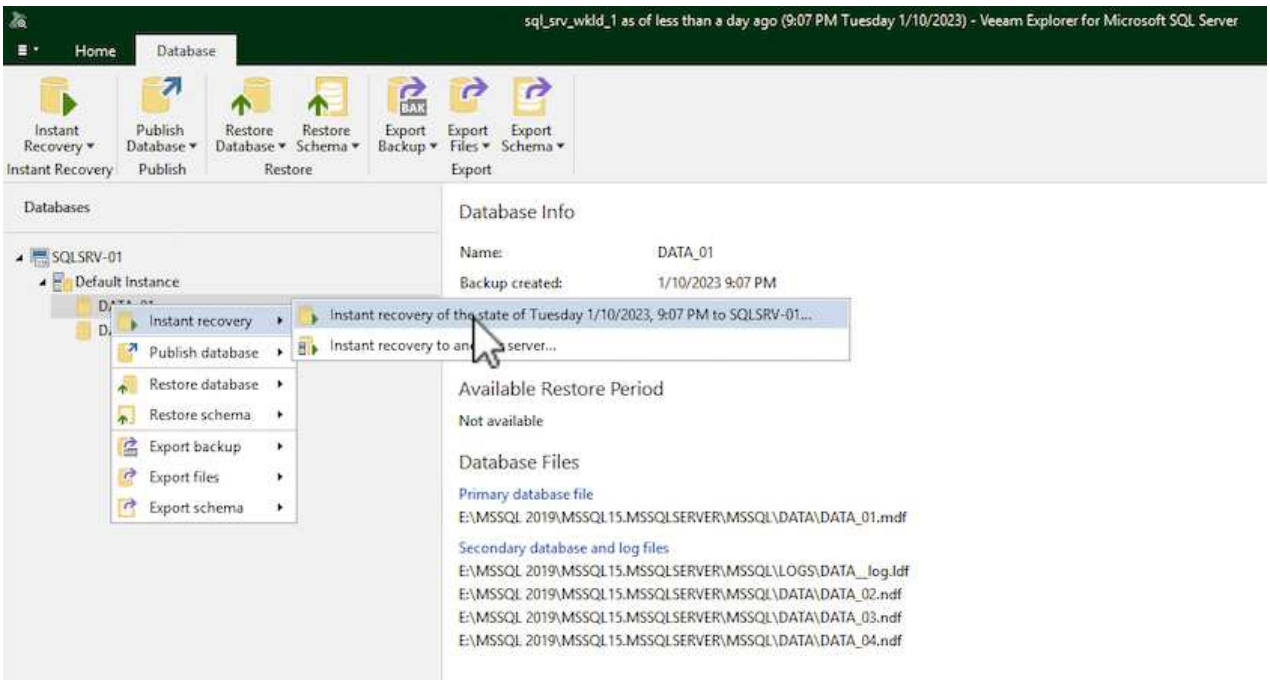


3. 必要に応じて*を入力し、**[**概要**]**ページで[参照]*ボタンをクリックしてVeeam Explorer for Microsoft SQL Serverを起動します。



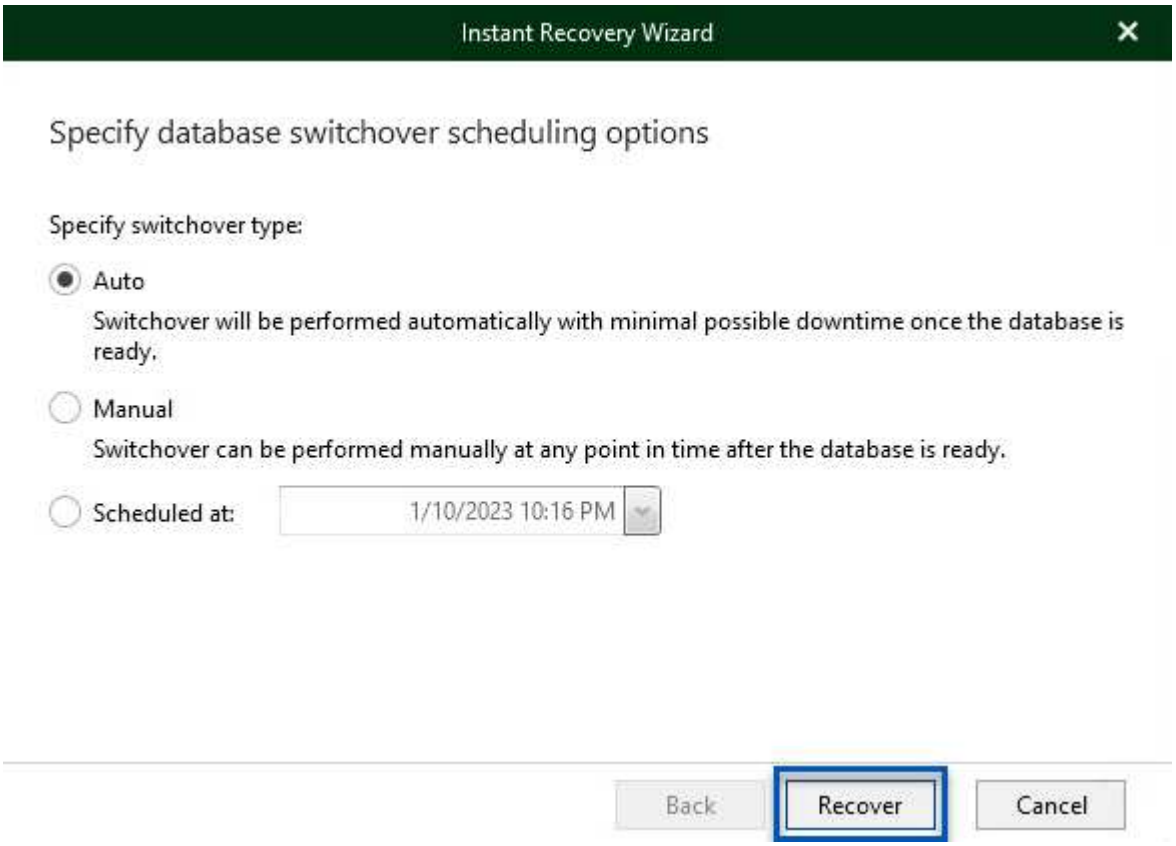
をクリックしてVeeam Explorerを起動します"]

4. Veeam Explorerでデータベースインスタンスのリストを展開し、右クリックして*[Instant recovery]*を選択し、リカバリ先のリストアポイントを指定します。

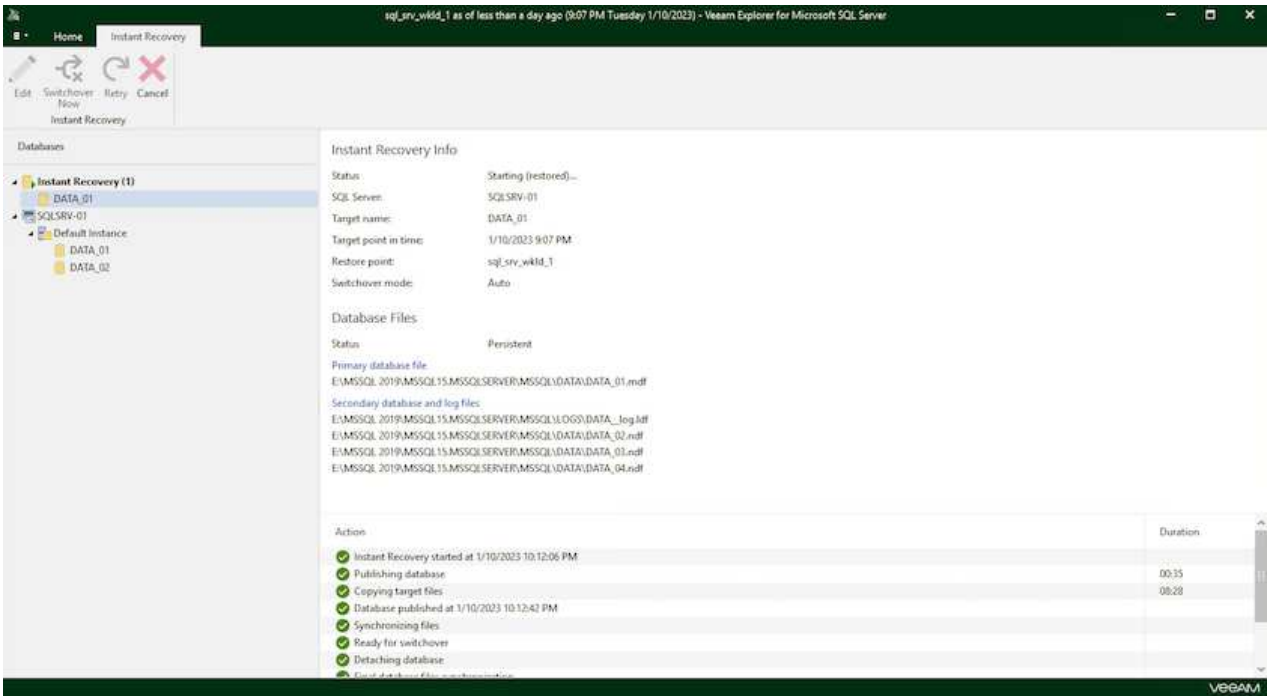


5. Instant Recovery Wizardで、スイッチオーバータイプを指定します。これは、最小限のダウンタイム

で自動的に行うことも、手動で行うことも、指定した時間に行うこともできます。次に、*回復*ボタンをクリックして、復元プロセスを開始します。



6. リカバリプロセスはVeeam Explorerから監視できます。



Veeam Explorerを使用してSQL Serverのリストア処理を実行する方法の詳細については、のMicrosoft SQL

Serverの項を参照して "Veeam Explorers User Guideを参照してください"ください。

Veeam Explorerを使用して**Oracle**データベースをリストアします

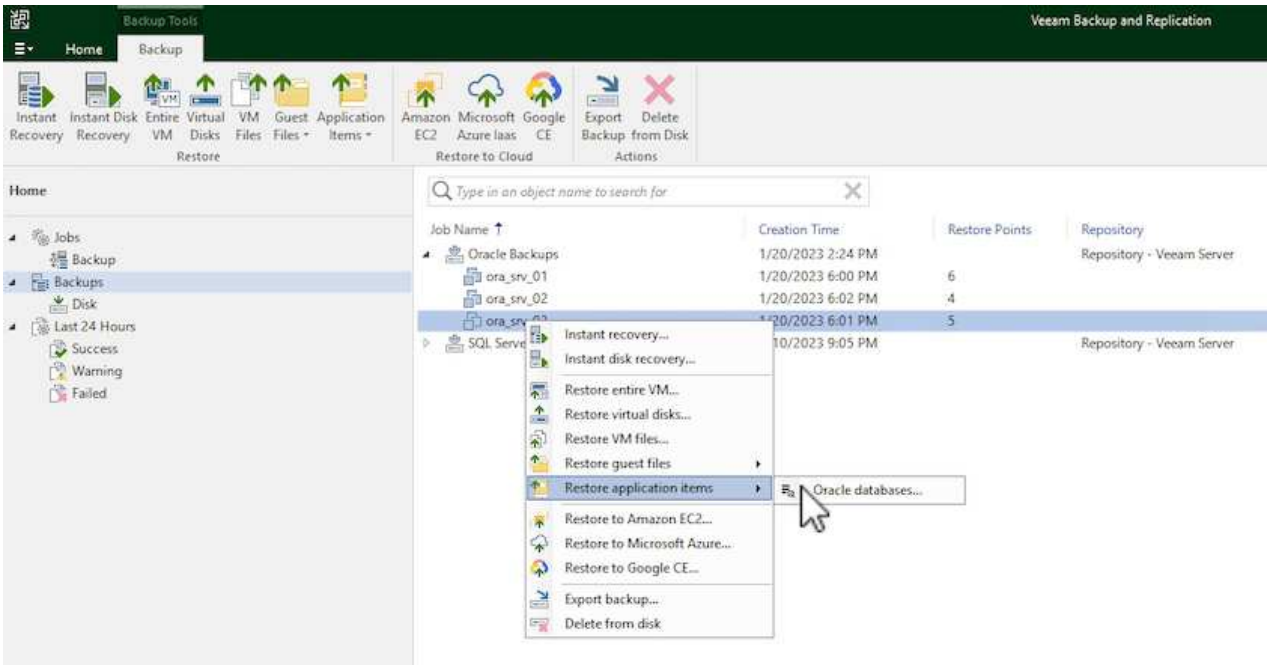
Veeam Explorer for Oracle databaseでは、Instant Recoveryを使用して、Oracleデータベースの標準リストアまたは中断のないリストアを実行できます。また、データベースのパブリッシュをサポートしているため、高速アクセス、Data Guardデータベースのリカバリ、RMANバックアップからのリストアが可能です。

Veeam Explorerを使用してOracleデータベースのリストア処理を実行する方法の詳細については、のOracleのセクションを参照して "Veeam Explorers User Guideを参照してください"ください。

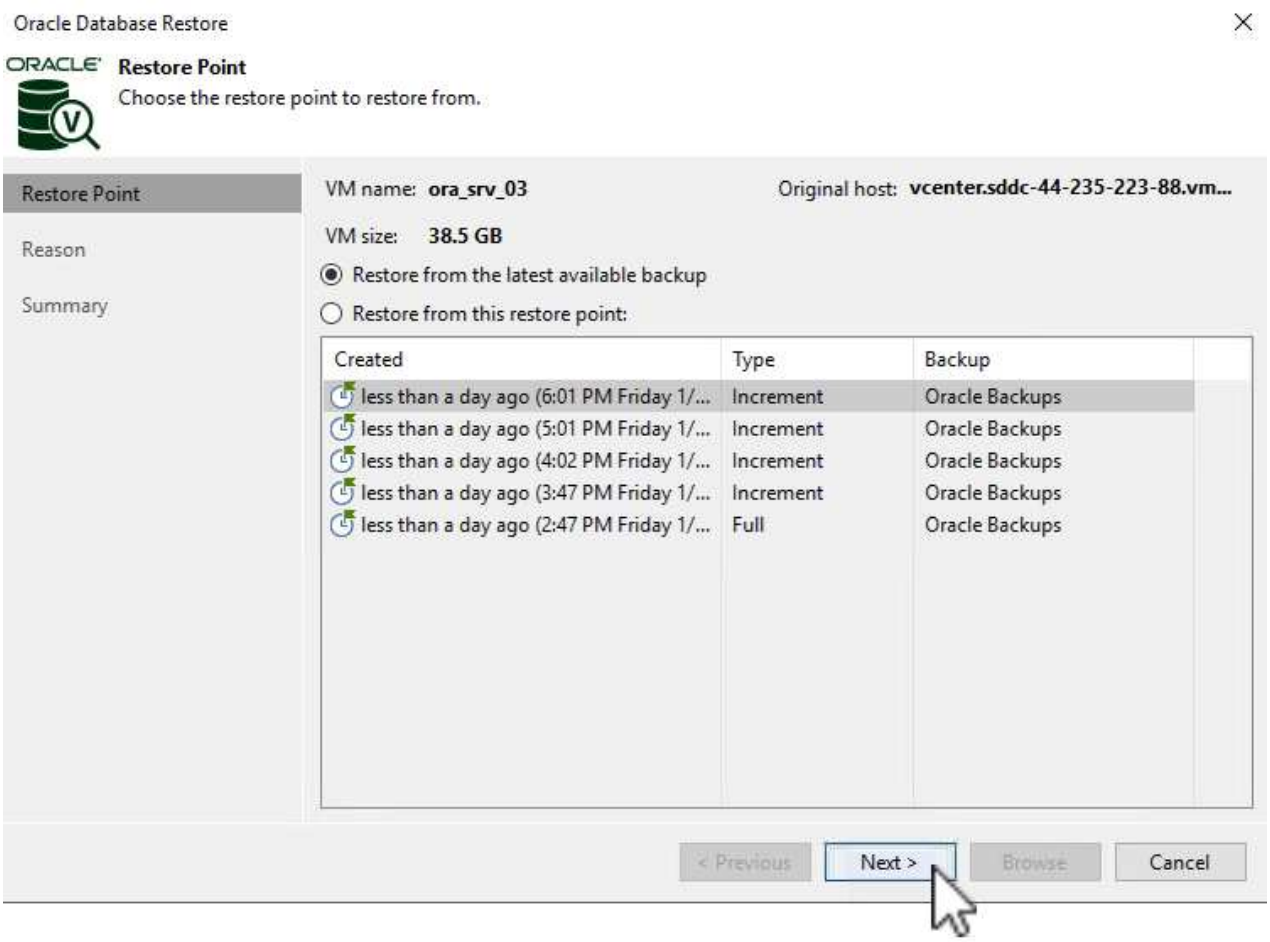
Veeam Explorerを使用してOracleデータベースをリストアします

このセクションでは、Veeam Explorerを使用して、別のサーバへのOracleデータベースのリストアについて説明します。

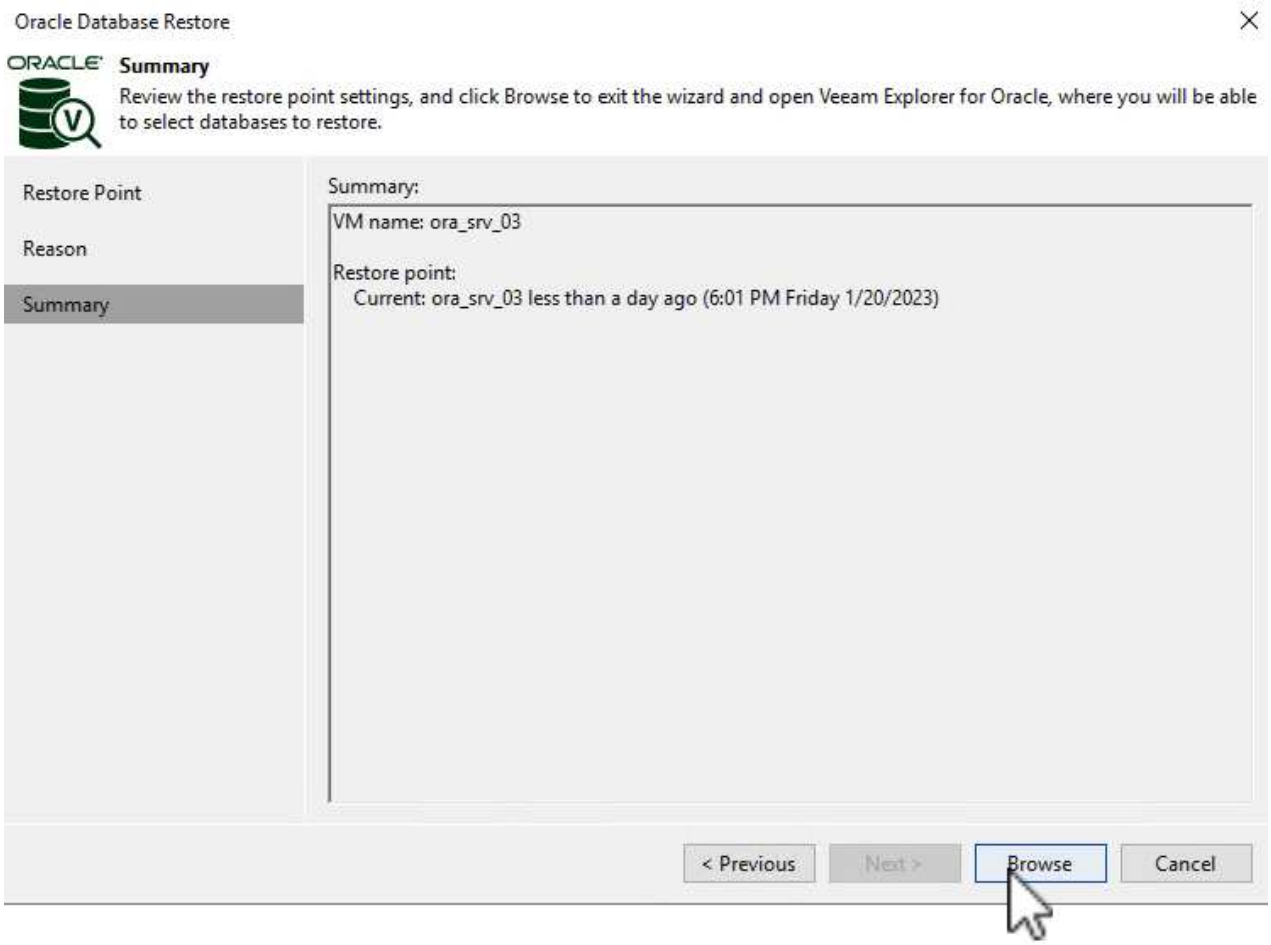
1. Veeam Backup & Replicationコンソールで、Oracleバックアップのリストに移動し、サーバを右クリックして*を選択し、[Oracleデータベース…]*を選択します。



2. Oracle Databaseリストア・ウィザードで、リストからリストア・ポイントを選択し、*[Next]*をクリックします。

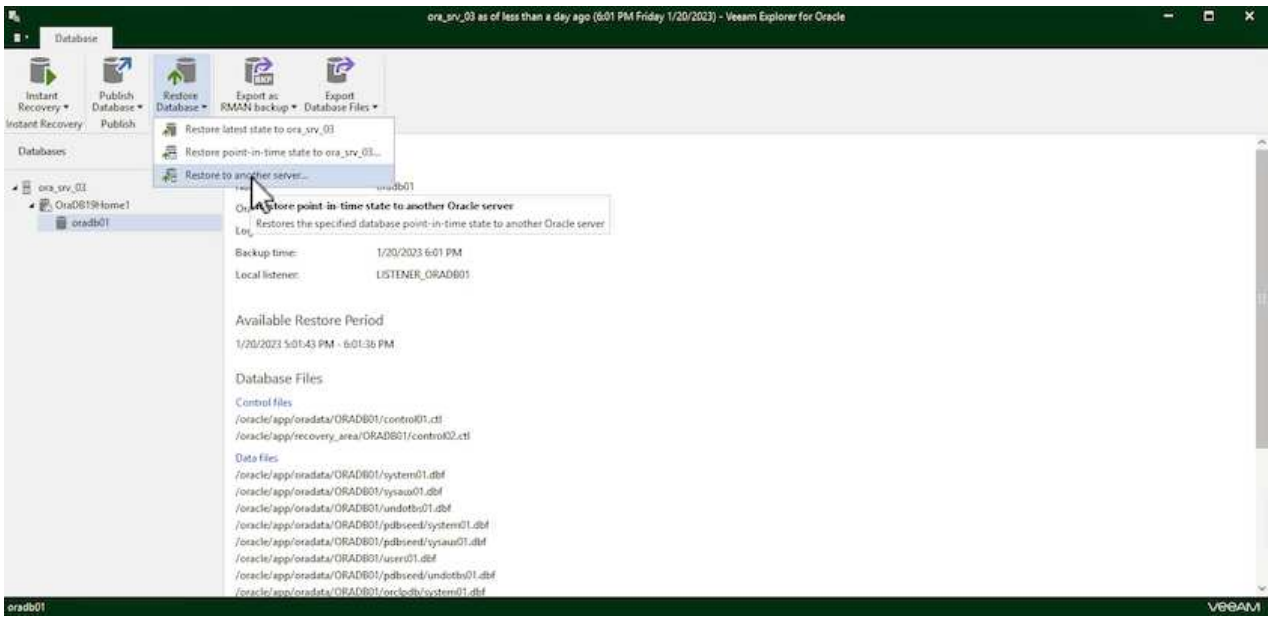


3. 必要に応じて*を入力し、**[**概要**]**ページで[参照]*ボタンをクリックしてVeeam Explorer for Oracleを起動します。



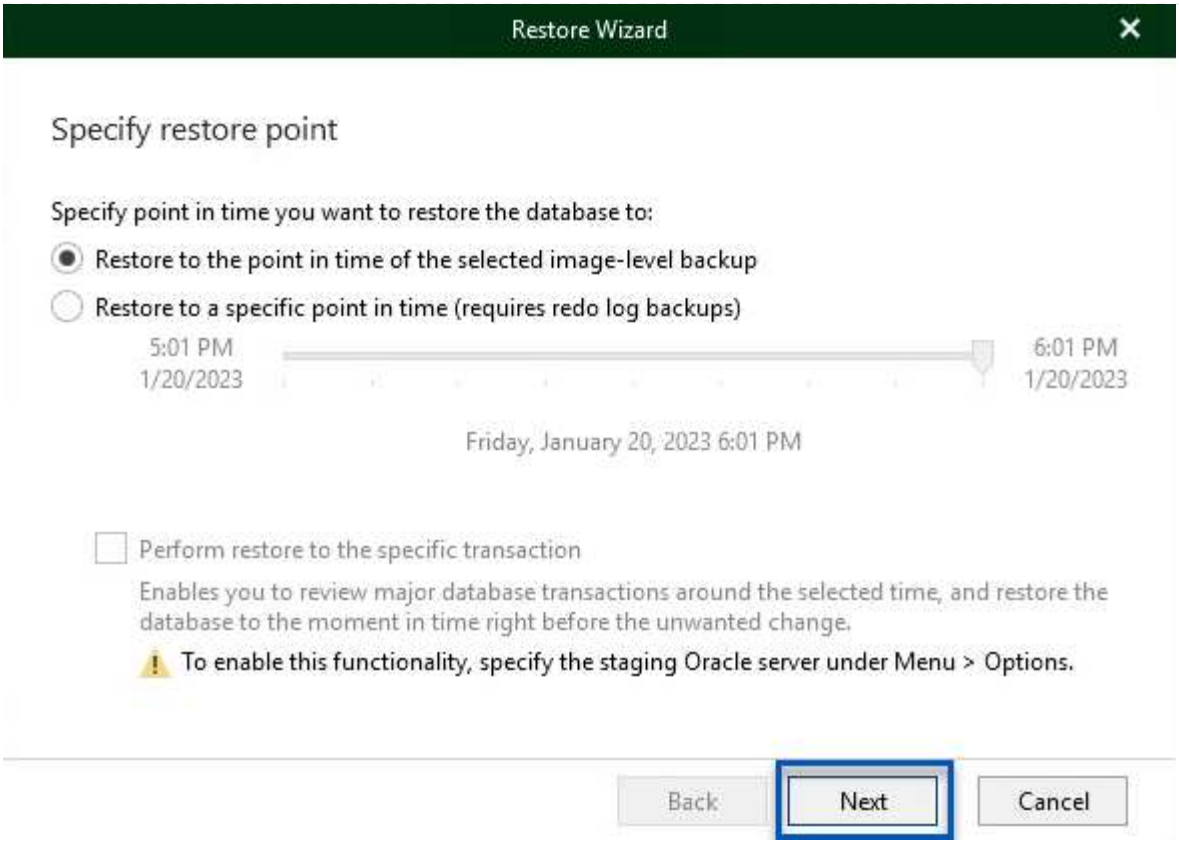
をクリックしてVeeam Explorerを起動します"]

4. Veeam Explorerでデータベースインスタンスのリストを展開表示し、リストアするデータベースをクリックしてから、上部の*ドロップダウンメニューから[別のサーバにリストア...]*を選択します。

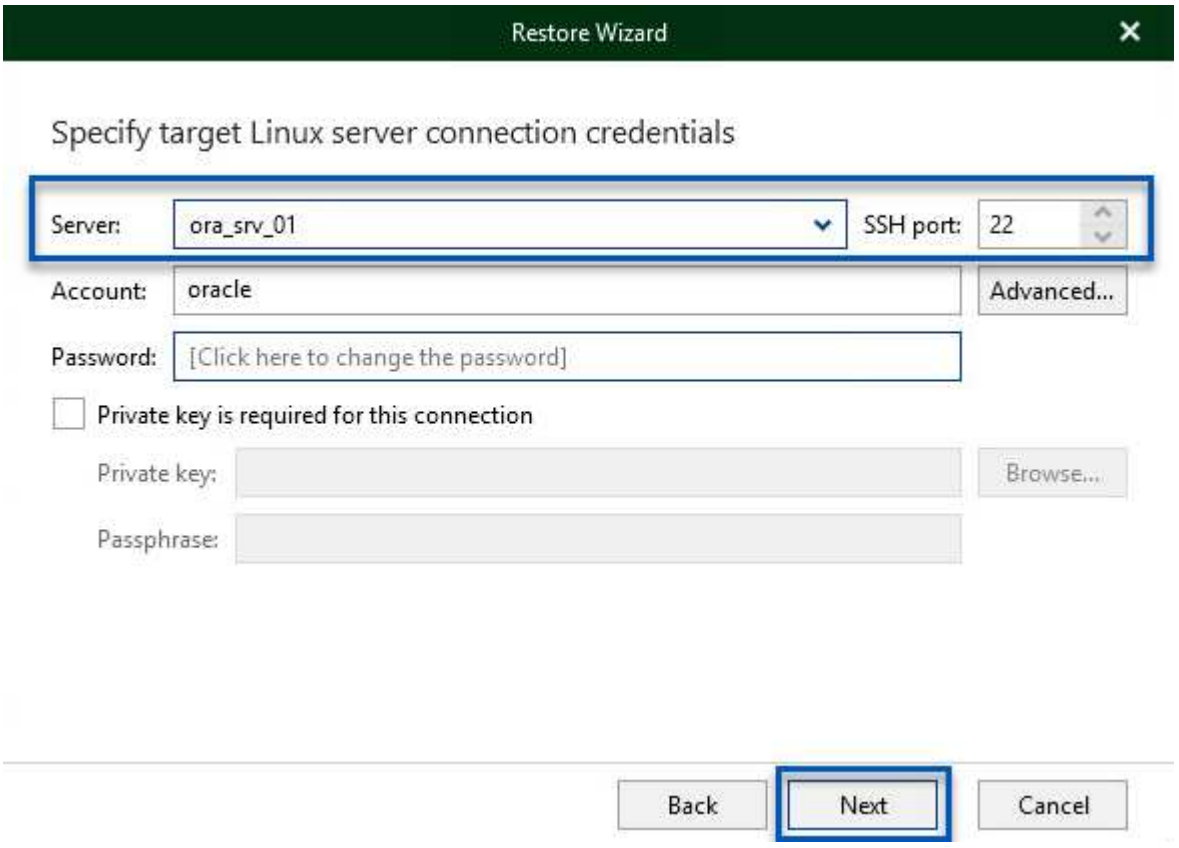


を選択します"]

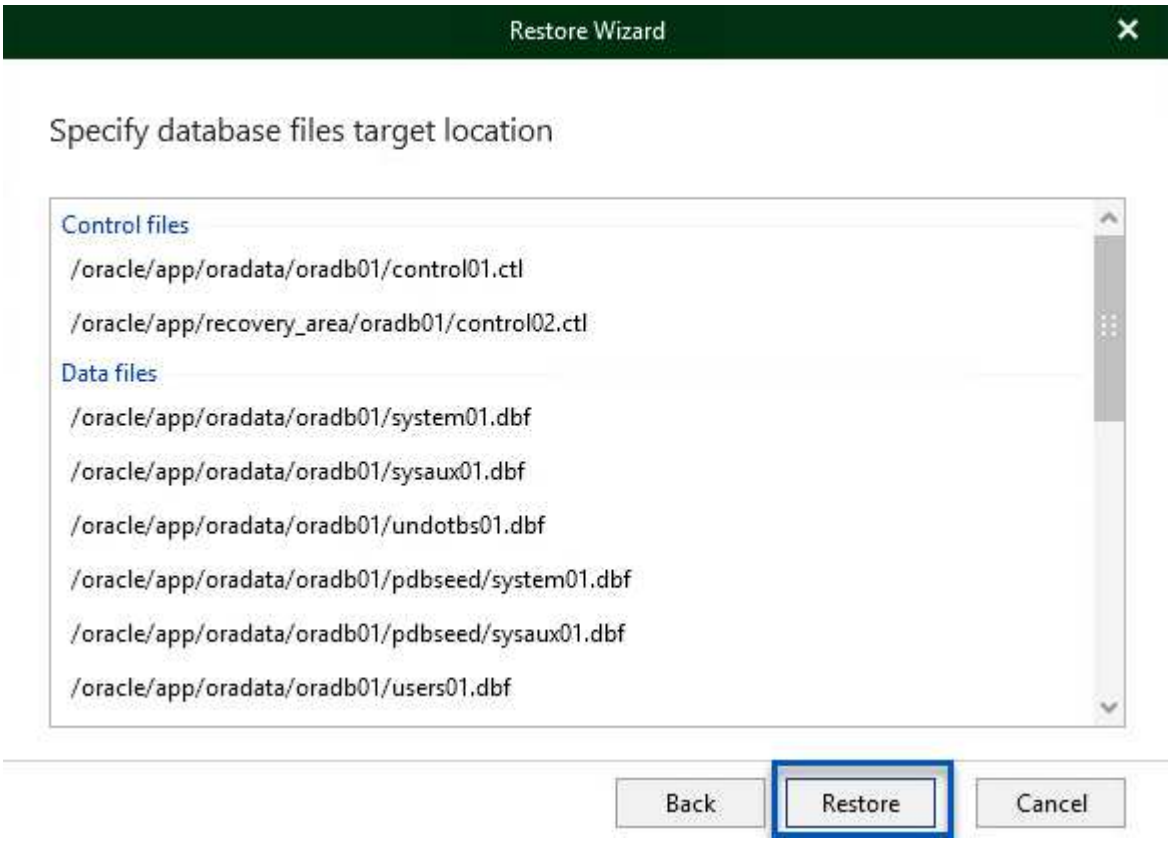
5. リストアウィザードで、リストア元のリストアポイントを指定し、*[次へ]*をクリックします。



6. データベースのリストア先となるターゲットサーバとアカウントのクレデンシャルを指定し、*[次へ]*をクリックします。



7. 最後に、データベースファイルのターゲットの場所を指定し、*[リストア]*ボタンをクリックしてリストアプロセスを開始します。

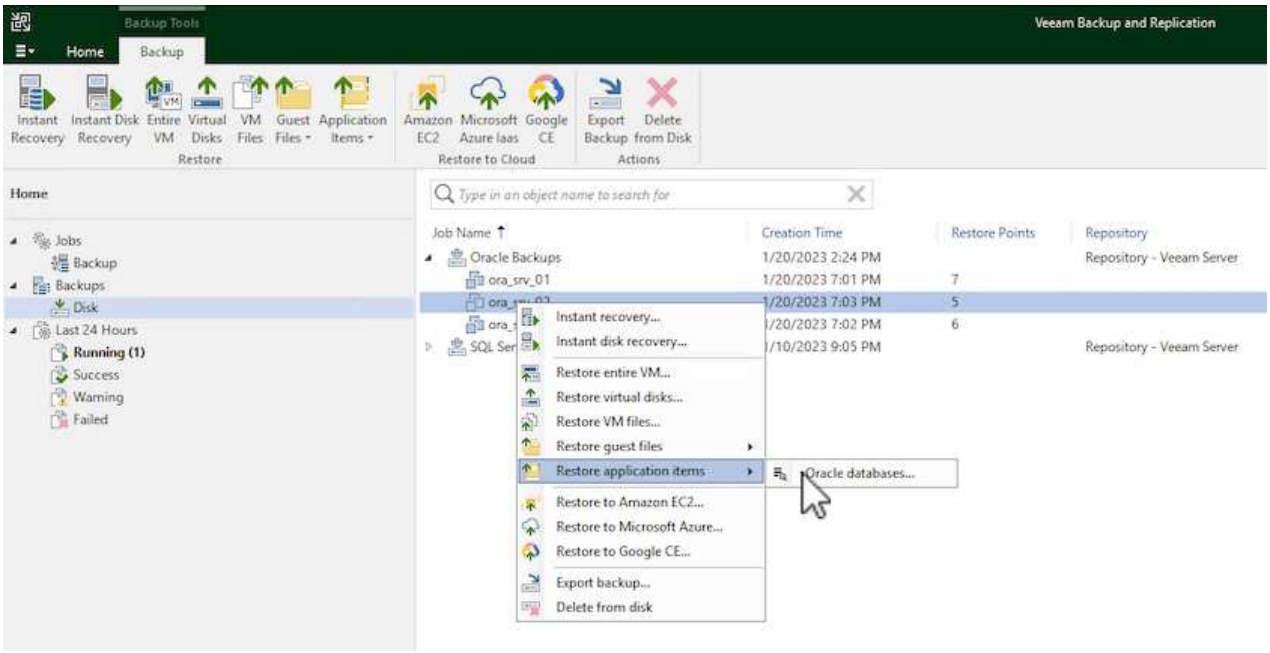


8. データベースのリカバリが完了したら、サーバ上でOracleデータベースが正常に起動していることを確認します。

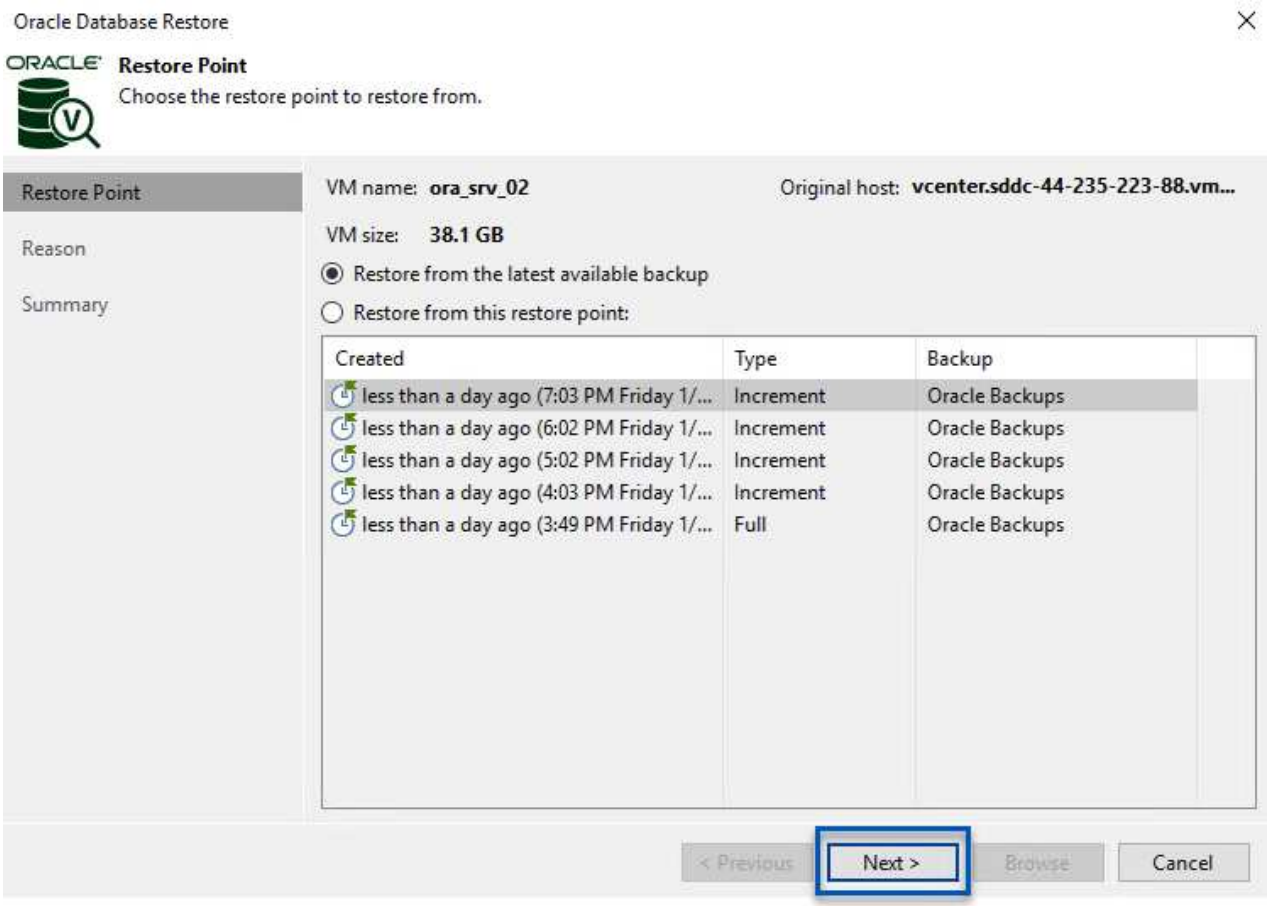
Oracleデータベースを代替サーバにパブリッシュします

このセクションでは、フルリストアを起動せずに高速アクセスできるように、データベースを代替サーバにパブリッシュします。

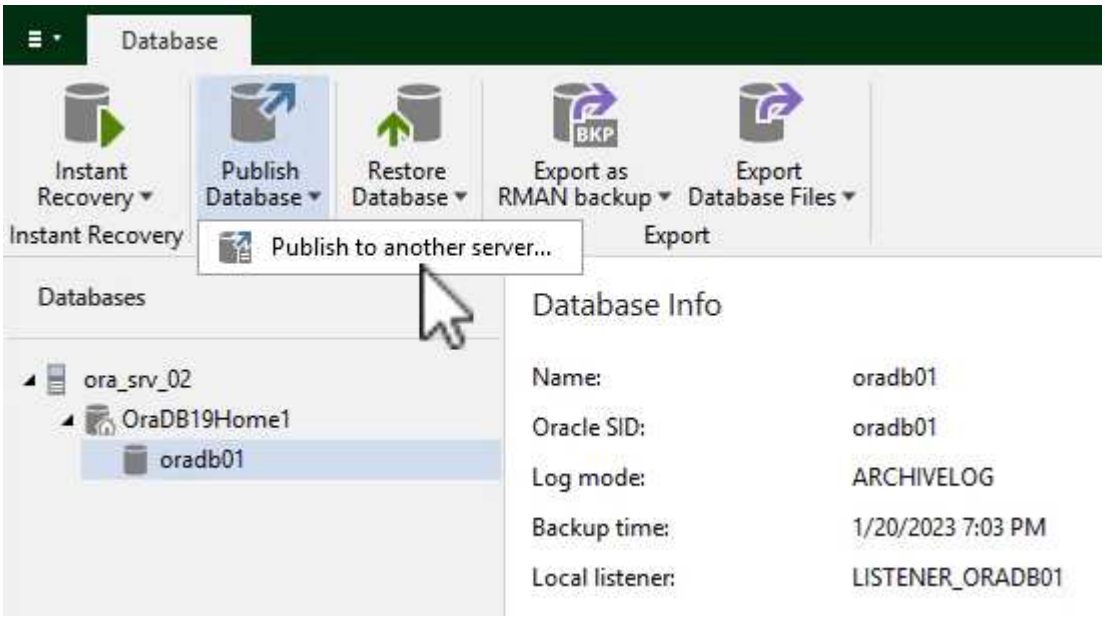
1. Veeam Backup & Replicationコンソールで、Oracleバックアップのリストに移動し、サーバを右クリックして*を選択し、[Oracleデータベース…]*を選択します。



2. Oracle Databaseリストア・ウィザードで、リストからリストア・ポイントを選択し、*[Next]*をクリックします。

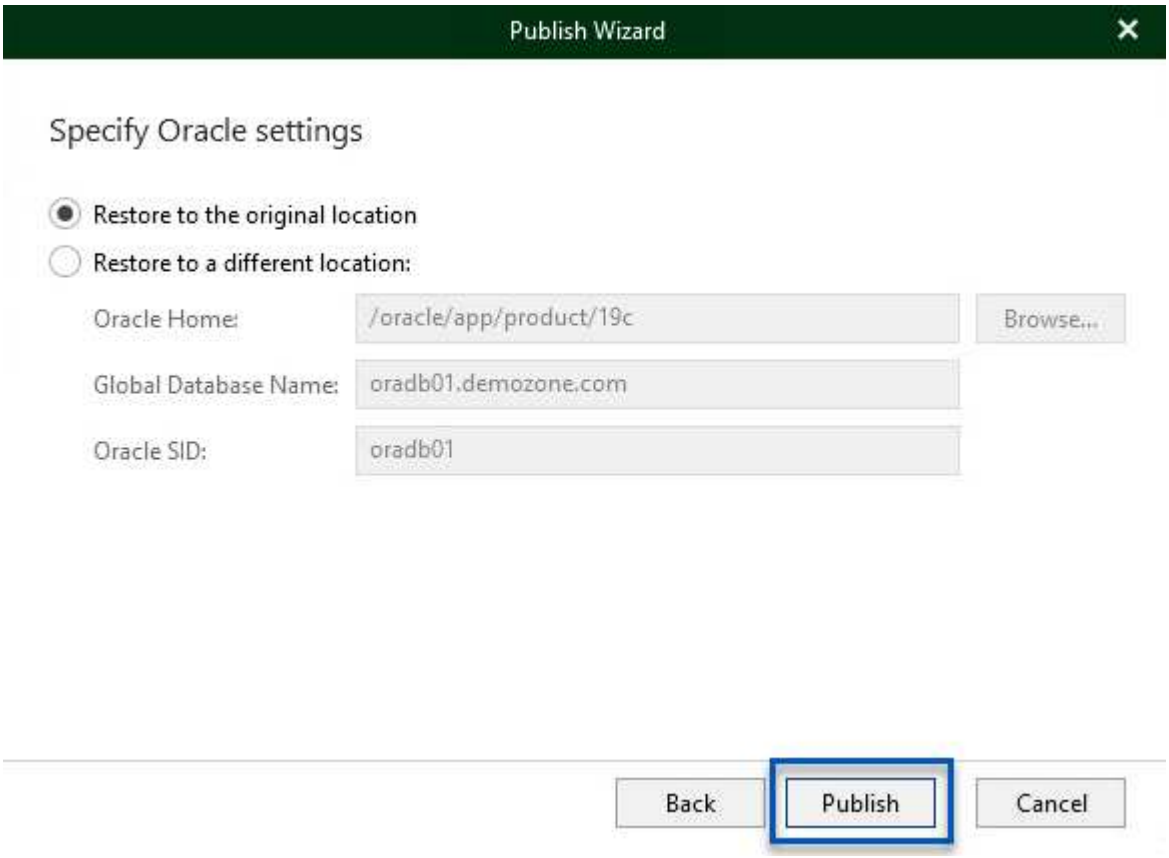


3. 必要に応じて*を入力し、**[概要]**ページで[参照]*ボタンをクリックしてVeeam Explorer for Oracleを起動します。
4. Veeam Explorerでデータベースインスタンスのリストを展開し、リストアするデータベースをクリックしてから、上部の*ドロップダウン・メニューから[Publish to another server…]*を選択します。



5. パブリッシュウィザードで、データベースのパブリッシュ元の復元ポイントを指定し、*次へ*をクリックします。

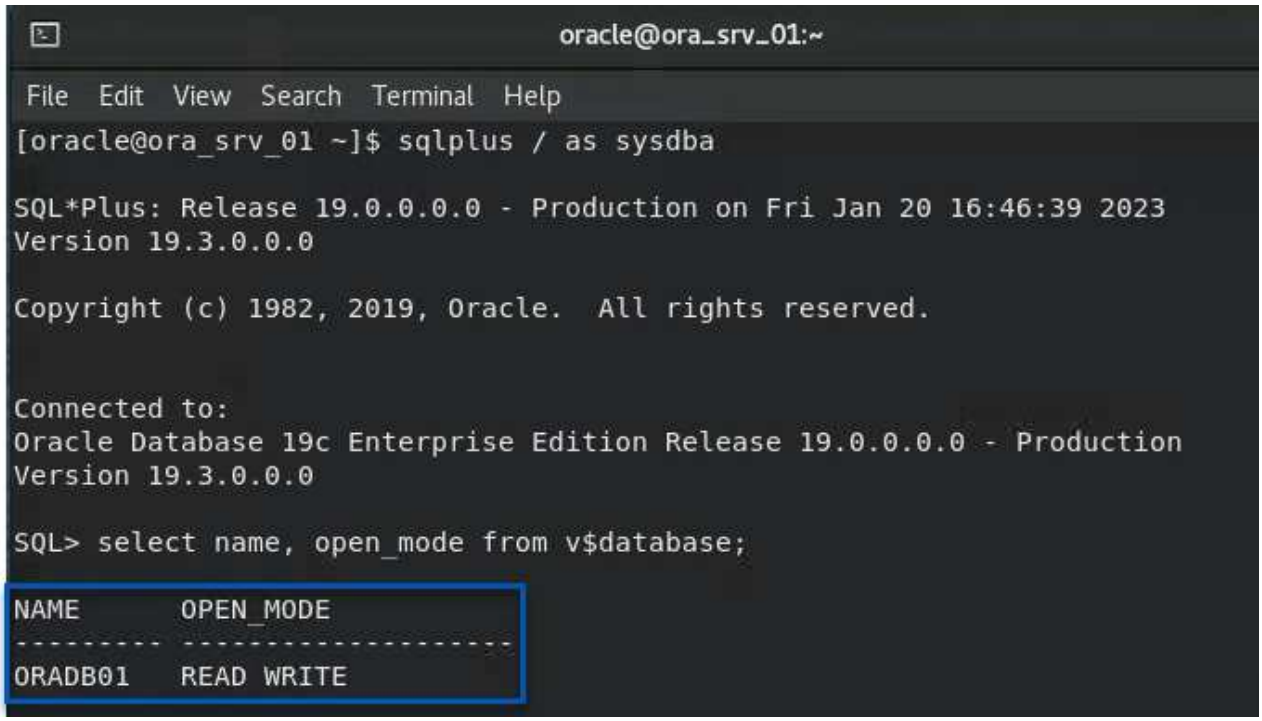
6. 最後に、ターゲットLinuxファイルシステムの場所を指定し、* Publish *をクリックしてリストアプロセスを開始します。



7. パブリッシュが完了したら、ターゲットサーバーにログインし、次のコマンドを実行してデータベースが実行されていることを確認します。

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```



まとめ

VMware Cloudは、ビジネスクリティカルなアプリケーションを実行し、機密データを保存するための強力なプラットフォームです。セキュアなデータ保護解決策 は、ビジネス継続性を確保し、サイバー脅威やデータ損失から保護するためにVMware Cloudを利用する企業にとって不可欠です。信頼性と堅牢性に優れたデータ保護解決策 を選択することで、企業は、重要なデータが何であっても安全であることを確信できます。

本ドキュメントで紹介するユースケースは、ネットアップ、VMware、Veeamの統合に焦点を当てた実績のあるデータ保護テクノロジに焦点を当てています。FSx ONTAPは、AWSのVMware Cloud向けの補完的NFSデータストアとしてサポートされており、すべての仮想マシンとアプリケーションデータに使用されます。Veeam Backup & Replicationは、バックアップ/リカバリプロセスの改善、自動化、合理化を支援するために設計された包括的なデータ保護解決策 です。Veeamは、FSx ONTAPでホストされるiSCSIバックアップターゲットボリュームと組み合わせて使用され、VMware Cloudに存在するアプリケーションデータに対して、安全で管理しやすいデータ保護ソリューションを提供します。

追加情報

この解決策 に記載されているテクノロジの詳細については、次の追加情報 を参照してください。

- "FSx ONTAPユーザガイド"
- "Veeam Help Centerテクニカルドキュメント"
- "VMware Cloud on AWSのサポート：考慮事項および制限事項"

TR-4955：『Disaster Recovery with FSx ONTAP and VMC（AWS VMware Cloud）』

ディザスタリカバリオーケストレーションツール（DRO、UIを備えたスクリプト化され

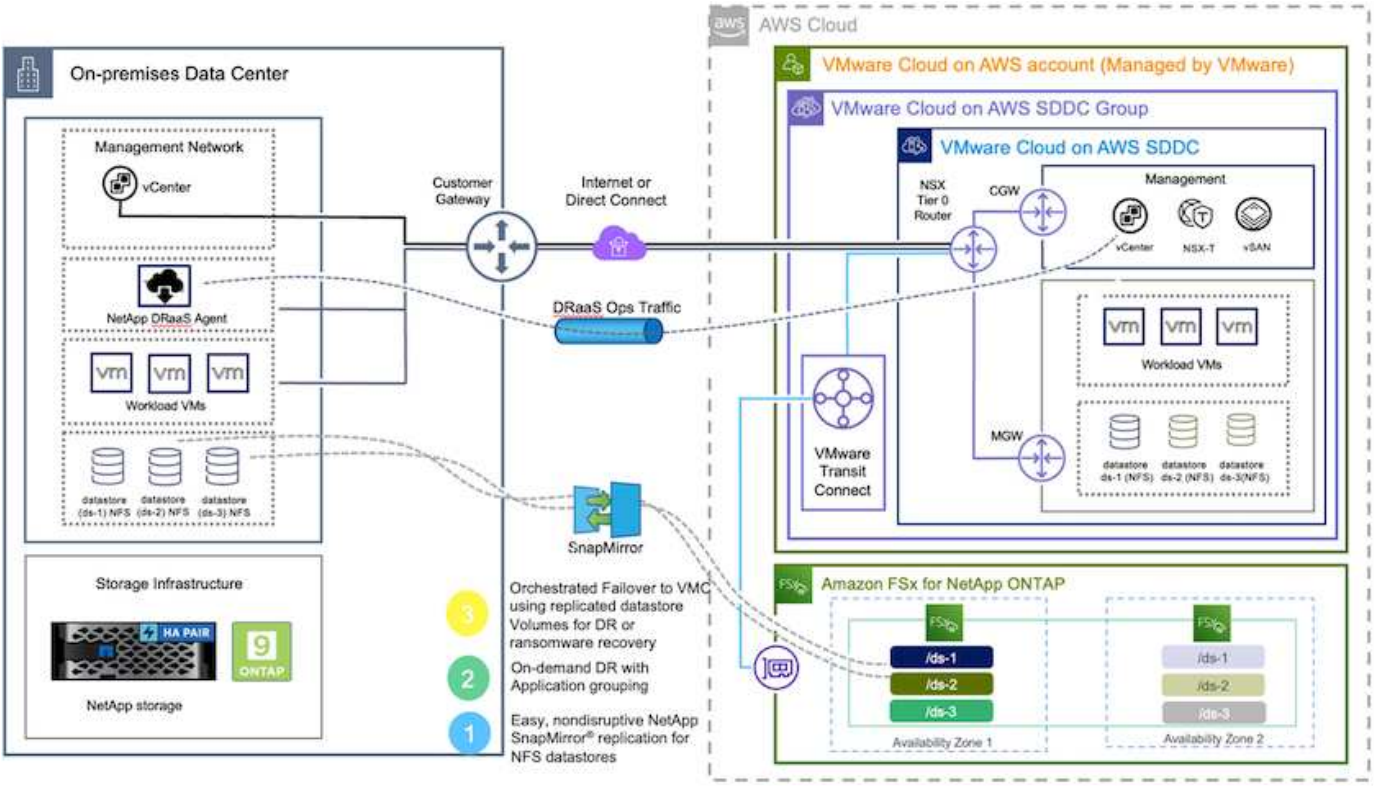
たソリューション）を使用すると、オンプレミスからFSx ONTAPにレプリケートされたワークロードをシームレスにリカバリできます。DROは、SnapMirrorレベルからVMCへのVM登録、NSX-T上のネットワークマッピングへのリカバリを自動化します。この機能は、すべてのVMC環境に含まれています。

ネットアップ、 Niyaz Mohamed

概要

クラウドへのディザスタリカバリは、耐障害性に優れた対費用効果の高い方法で、サイトの停止やデータ破損からワークロードを保護します（ランサムウェアなど）。NetApp SnapMirrorテクノロジを使用すると、オンプレミスのVMwareワークロードを、AWSで実行されるFSx ONTAPにレプリケートできます。

ディザスタリカバリオーケストレーションツール（DRO、UIを備えたスクリプト化されたソリューション）を使用すると、オンプレミスからFSx ONTAPにレプリケートされたワークロードをシームレスにリカバリできます。DROは、SnapMirrorレベルからVMCへのVM登録、NSX-T上のネットワークマッピングへのリカバリを自動化します。この機能は、すべてのVMC環境に含まれています。



はじめに

AWSにVMware Cloudを導入して設定

"AWS 上の VMware Cloud"AWSエコシステムでVMwareベースのワークロードにクラウドネイティブなエクスペリエンスを提供します。各VMware Software-Defined Data Center（SDDC）はAmazon Virtual Private Cloud（VPC）内で動作し、フルVMwareスタック（vCenter Serverを含む）、NSXベースのSoftware-Defined Networking、VSANソフトウェア定義ストレージ、およびワークロードにコンピューティングリソースとストレージリソースを提供する1つ以上のESXiホストを提供します。AWSでVMC環境を設定するには、次の手順を実行し"リンク"ます。パイロットライトクラスタはDRにも使用できます。

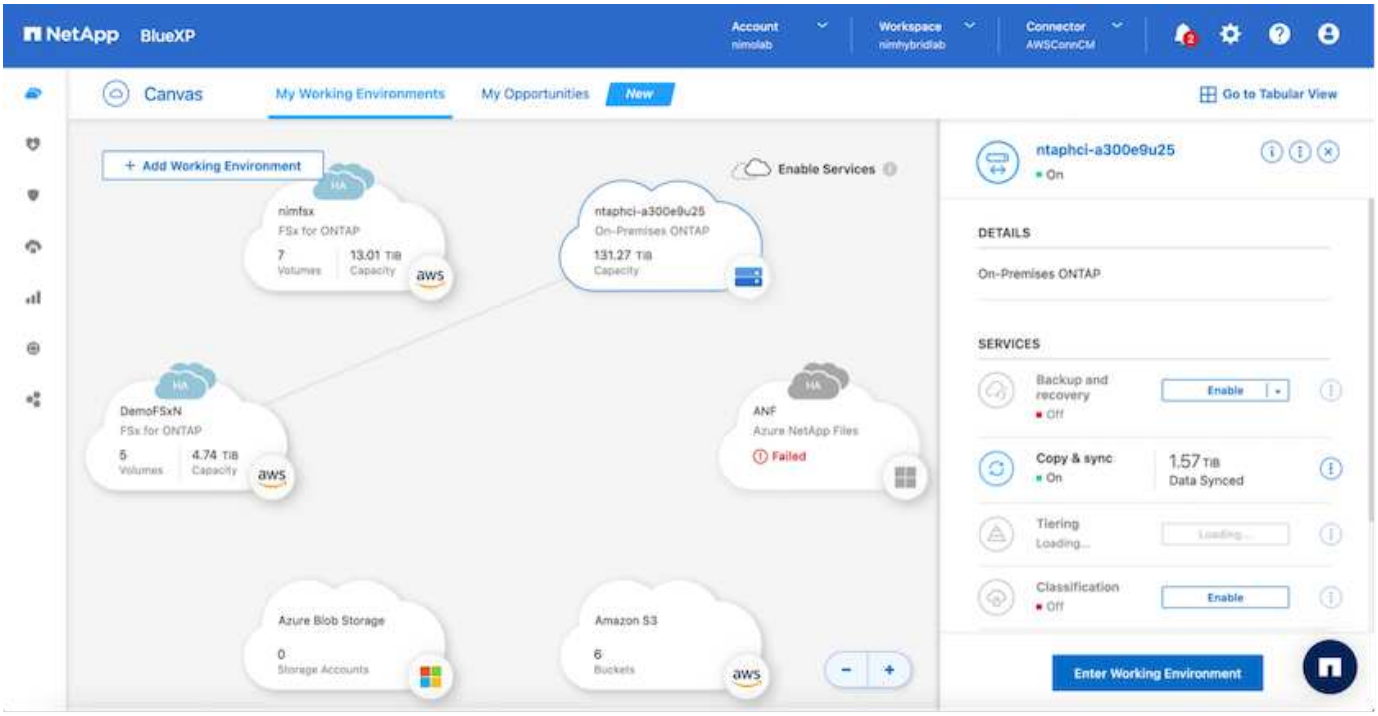
初期リリースでは、DROは既存のパイロットライトクラスタをサポートします。オンデマンドのSDDC作成は、今後のリリースで提供される予定です。

FSx ONTAPのプロビジョニングと設定

Amazon FSx ONTAPは、広く普及しているNetApp ONTAPファイルシステムを基盤に構築された、信頼性、拡張性、パフォーマンス、機能豊富なファイルストレージを提供するフルマネージドサービスです。以下の手順に従って、"リンク"FSx ONTAPのプロビジョニングと設定を行います。

FSx ONTAPへの**SnapMirror**の導入と設定

次のステップでは、NetApp BlueXP を使用して、プロビジョニングされたFSx ONTAP on AWSインスタンスを検出し、必要なデータストアボリュームをオンプレミス環境からFSx ONTAPにレプリケートします。その際、適切な頻度でNetApp Snapshotコピーを保持します。



BlueXPを設定するには、このリンクの手順に従います。NetApp ONTAP CLIを使用して、このリンクに続くレプリケーションをスケジュールすることもできます。

SnapMirror関係は前提条件であり、事前に作成しておく必要があります。

DROのインストール

DROを開始するには、指定されたEC2インスタンスまたは仮想マシン上のUbuntuオペレーティングシステムを使用して、前提条件を満たしていることを確認します。次に、パッケージをインストールします。

前提条件

- ソースおよびデスティネーションのvCenterおよびストレージシステムへの接続が存在することを確認してください。

- DNS名を使用する場合は、DNS解決を実施する必要があります。それ以外の場合は、vCenterとストレージシステムのIPアドレスを使用してください。
- root権限を持つユーザを作成します。EC2インスタンスではsudoも使用できます。

OSの要件

- Ubuntu 20.04（LTS）：2GB以上、vCPU×4
- 指定されたエージェントVMに次のパッケージがインストールされている必要があります。
  - Docker
  - docker -構成
  - Jq

次の `sudo chmod 666 /var/run/docker.sock`権限を変更し `docker.sock`ます。

`deploy.sh`スクリプトは、必要なすべての前提条件を実行します。

パッケージをインストールします

1. 指定した仮想マシンにインストールパッケージをダウンロードします。

```
git clone https://github.com/NetApp/DRO-AWS.git
```

このエージェントは、オンプレミスまたはAWS VPC内にインストールできます。

2. パッケージを解凍して導入スクリプトを実行し、ホストIP（10.10.10.10など）を入力します。

```
tar xvf DRO-prereq.tar
```

3. ディレクトリに移動し、次のように配置スクリプトを実行します。

```
sudo sh deploy.sh
```

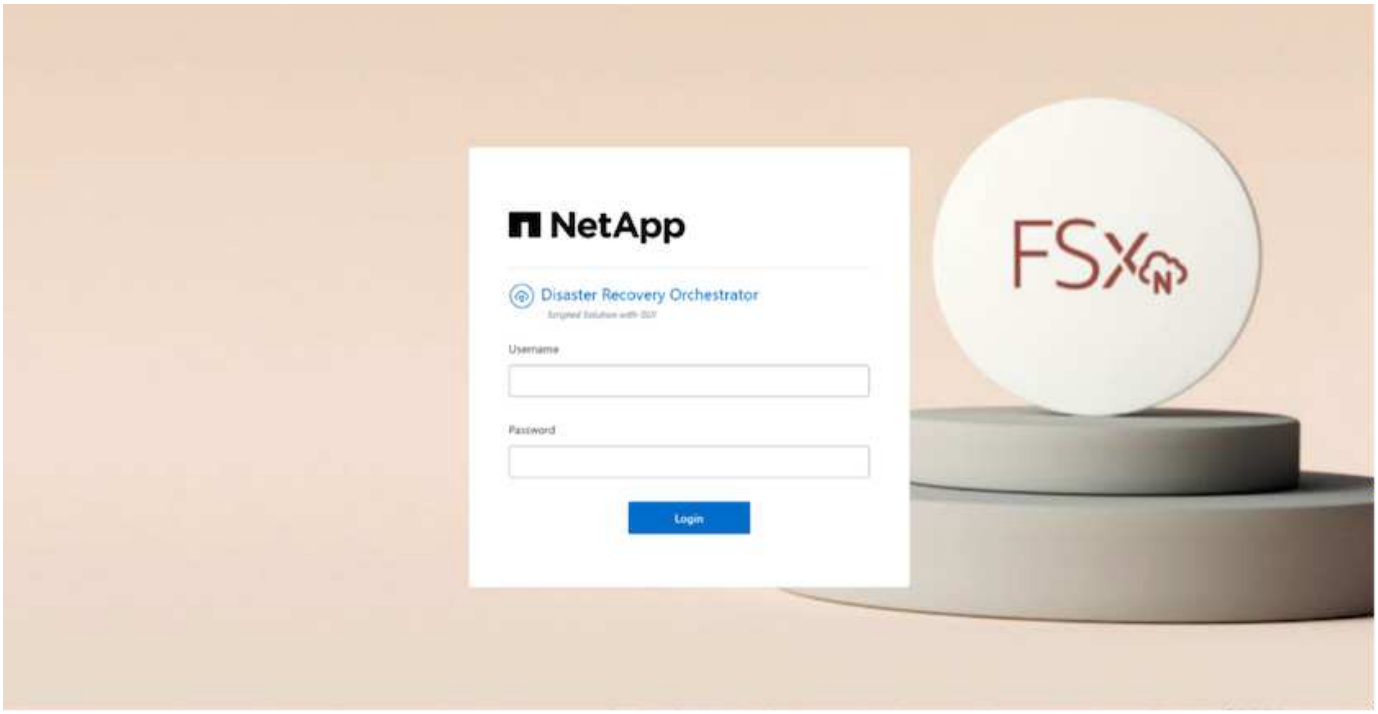
4. UIには次の方法でアクセスします。

```
https://<host-ip-address>
```

次のデフォルトクレデンシャルを使用：

```
Username: admin
Password: admin
```

パスワードは、Change Passwordオプションを使用して変更できます。



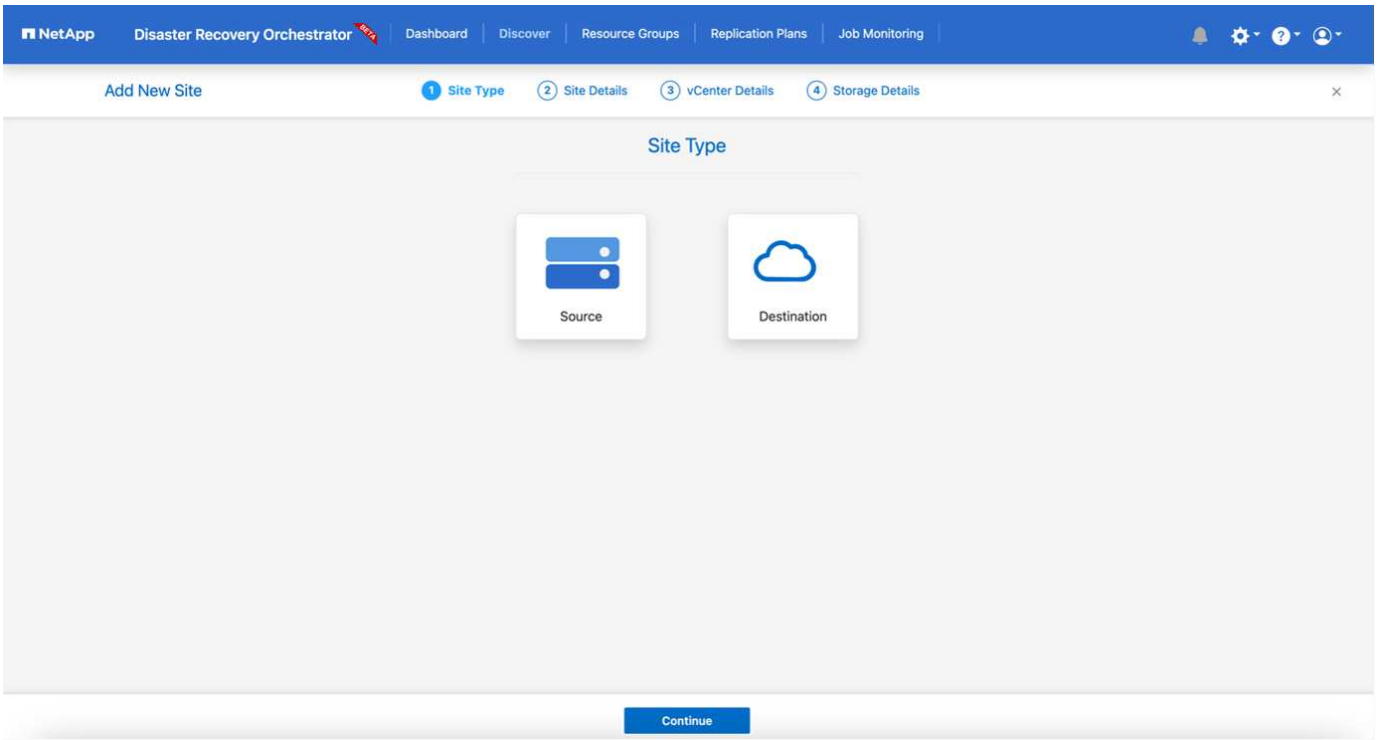
DRO構成

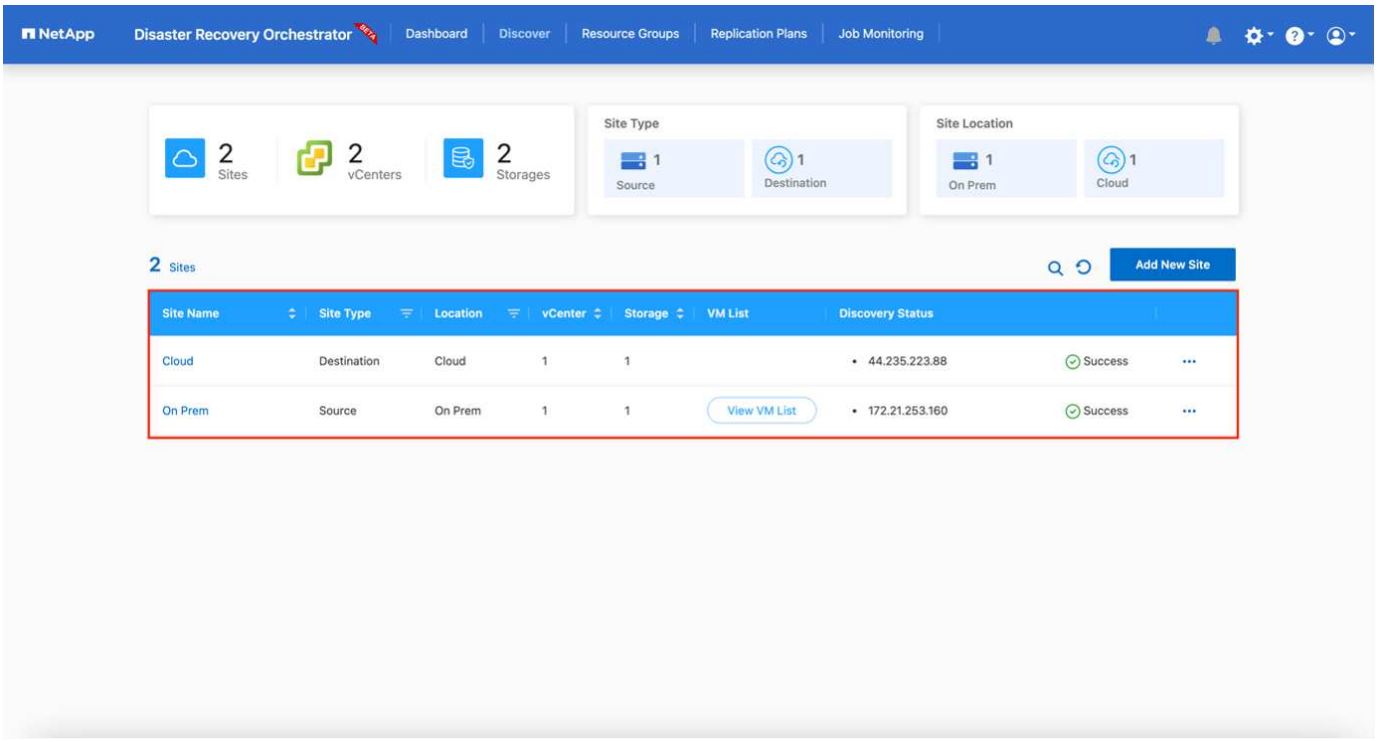
FSx ONTAPとVMCが適切に設定されたら、FSx ONTAPの読み取り専用SnapMirrorコピーを使用してオンプレミスのVMCへのワークロードのリカバリを自動化するDROの設定を開始できます。

NetAppでは、DROエージェントがオンプレミスのコンポーネントやFSx ONTAPおよびVMCリソースとネットワーク経由で通信できるように、AWSにDROエージェントを導入し、FSx ONTAPが導入されているVPCにもDROエージェントを導入することを推奨しています（ピア接続も可能です）。

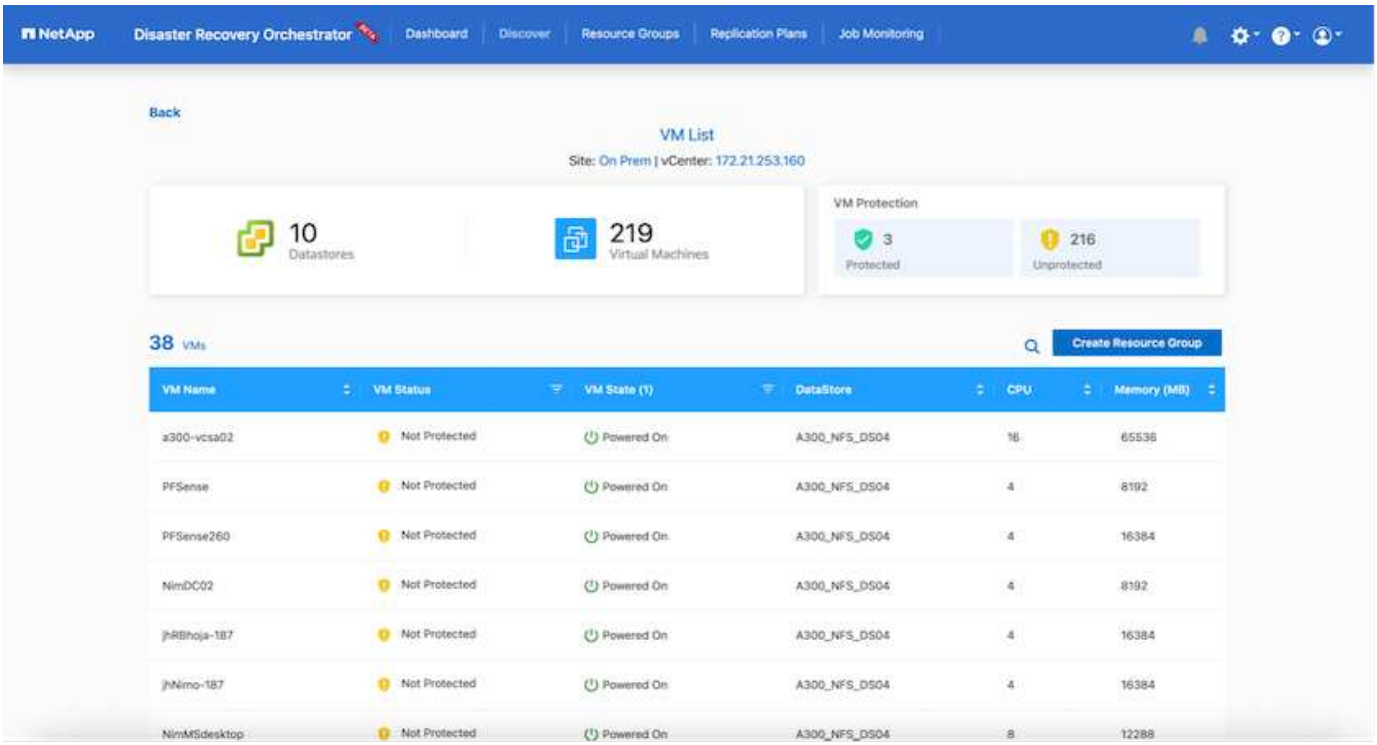
まず、オンプレミスリソースとクラウドリソース（vCenterとストレージの両方）を検出してDROに追加します。サポートされているブラウザでDROを開き、デフォルトのユーザー名とパスワード（admin/admin）およびサイトの追加を使用します。サイトは、Discoverオプションを使用して追加することもできます。次のプラットフォームを追加します。

- オンプレミス
  - オンプレミスのvCenter
  - ONTAP ストレージシステム
- クラウド
  - VMC vCenter
  - FSX ONTAP の略





追加されると、DROは自動検出を実行し、ソースストレージからFSx ONTAPに対応するSnapMirrorレプリカを持つVMを表示します。DROは、VMが使用するネットワークとポートグループを自動的に検出して、それらにデータを入力します。



次の手順では、必要なVMを、リソースグループとして機能するように機能グループにグループ化します。

リソースのグループ化

プラットフォームを追加したら、リカバリするVMをリソースグループにまとめることができます。DROリソースグループを使用すると、依存する一連のVMを論理グループにグループ化して、それらの起動順序、ブート遅延、およびリカバリ時に実行可能なオプションのアプリケーション検証を含めることができます。

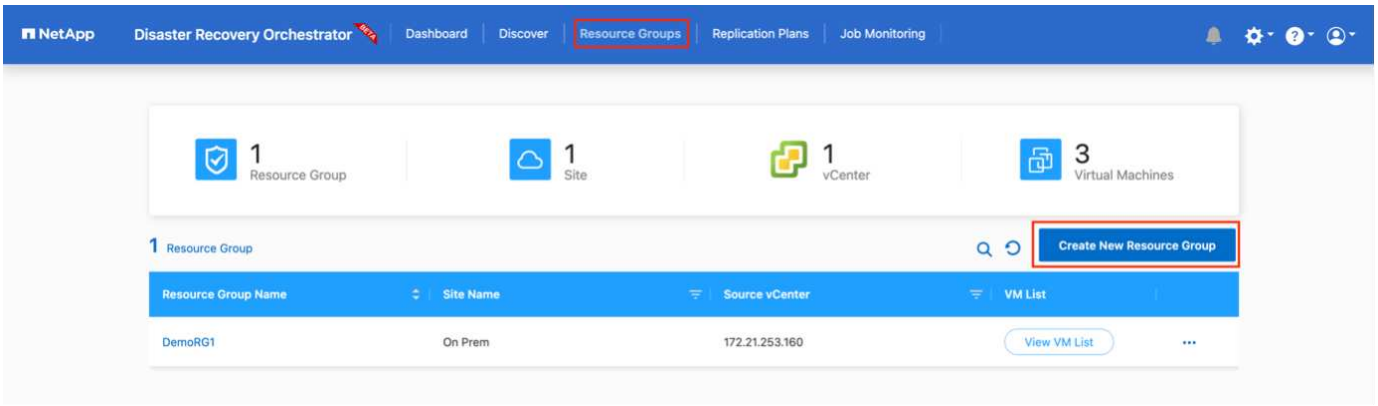
リソースグループの作成を開始するには、次の手順を実行します。

1. *リソースグループ*にアクセスし、*新しいリソースグループの作成*をクリックします。
2. [新しいリソースグループ*]で、ドロップダウンからソースサイトを選択し、[*Create]をクリックします。
3. リソースグループの詳細を入力し、*続行*をクリックします。
4. 検索オプションを使用して、適切なVMを選択します。
5. 選択したVMのブート順序とブート遅延（秒）を選択します。各VMを選択して優先順位を設定し、電源投入シーケンスの順序を設定します。3つはすべてのVMのデフォルト値です。

   オプションは次のとおりです。

   1–最初にパワーオンする仮想マシン3 -デフォルト5 -最後にパワーオンする仮想マシン

6. [リソースグループの作成]をクリックします。

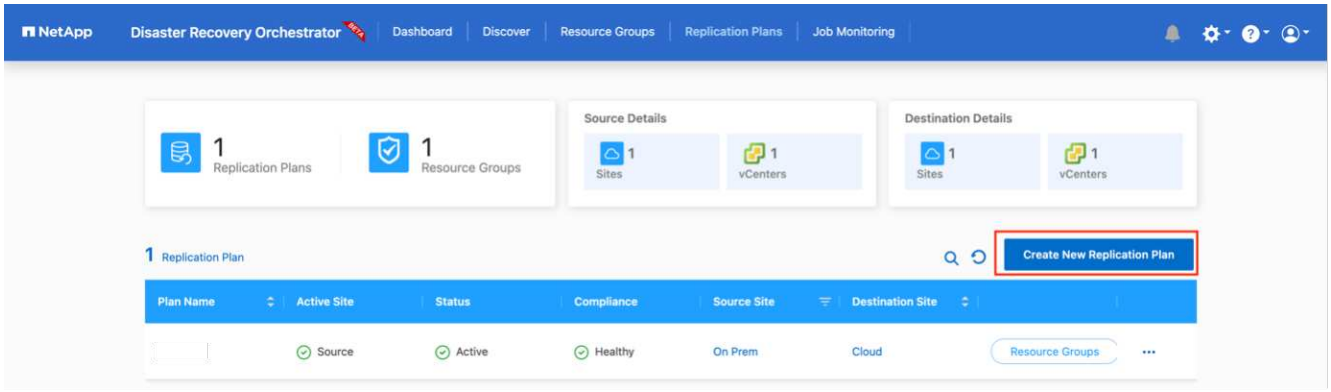


レプリケーションプラン

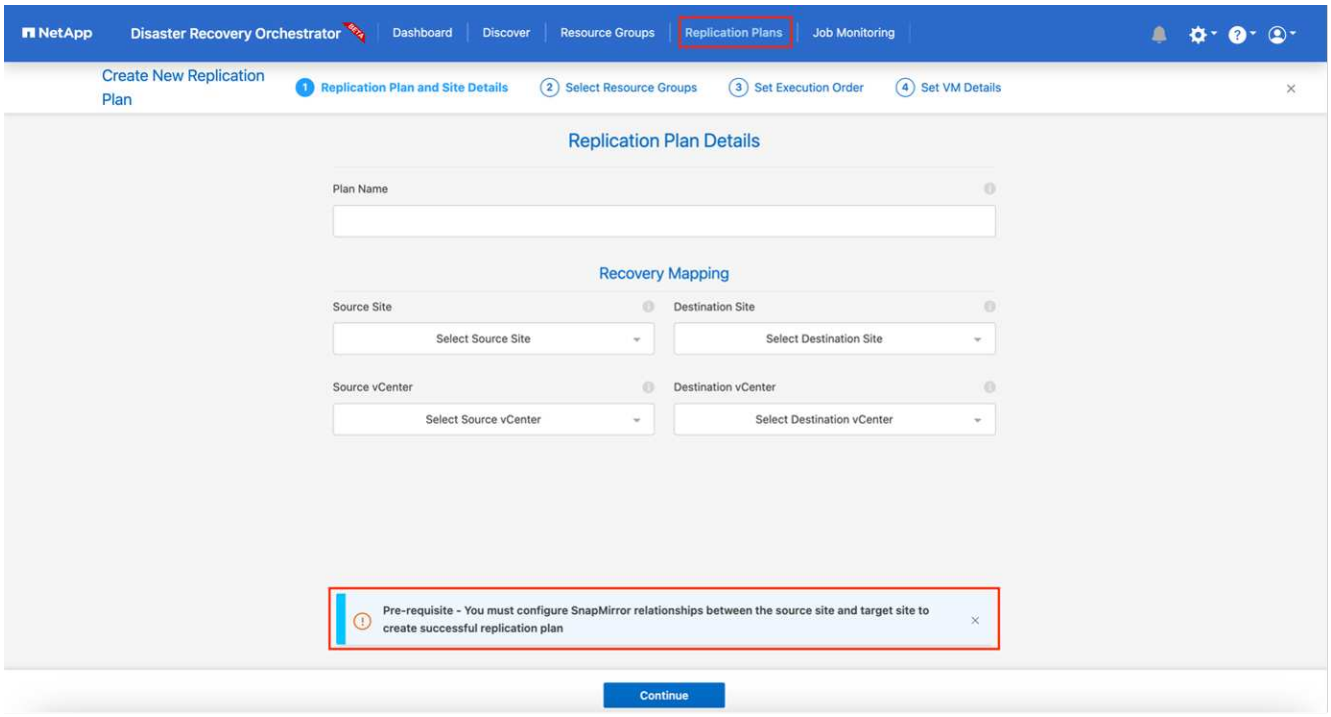
災害発生時にアプリケーションをリカバリするための計画が必要です。ドロップダウンからvCenterのソースプラットフォームとデスティネーションプラットフォームを選択し、このプランに含めるリソースグループと、アプリケーションのリストア方法と電源オン方法のグループを選択します（ドメインコントローラ、ティア1、ティア2など）。このような計画は、ブループリントとも呼ばれます。リカバリ・プランを定義するには'[レプリケーション・プラン]タブに移動し'[新しいレプリケーション・プラン]をクリックします

レプリケーションプランの作成を開始するには、次の手順を実行します。

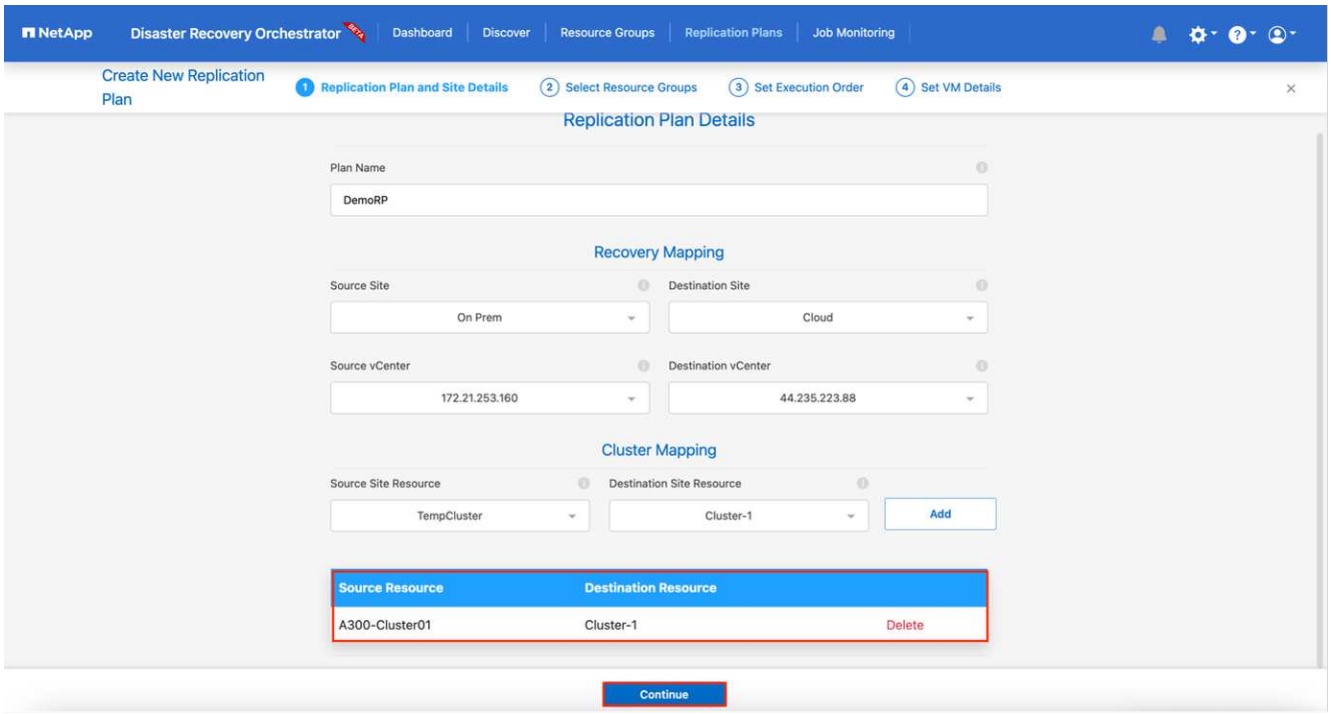
1. *レプリケーションプラン*にアクセスし、*新しいレプリケーションプランの作成*をクリックします。



2. [New Replication Plan]で、ソースサイト、関連するvCenter、デスティネーションサイト、および関連するvCenterを選択して、プランの名前を指定し、リカバリマッピングを追加します。

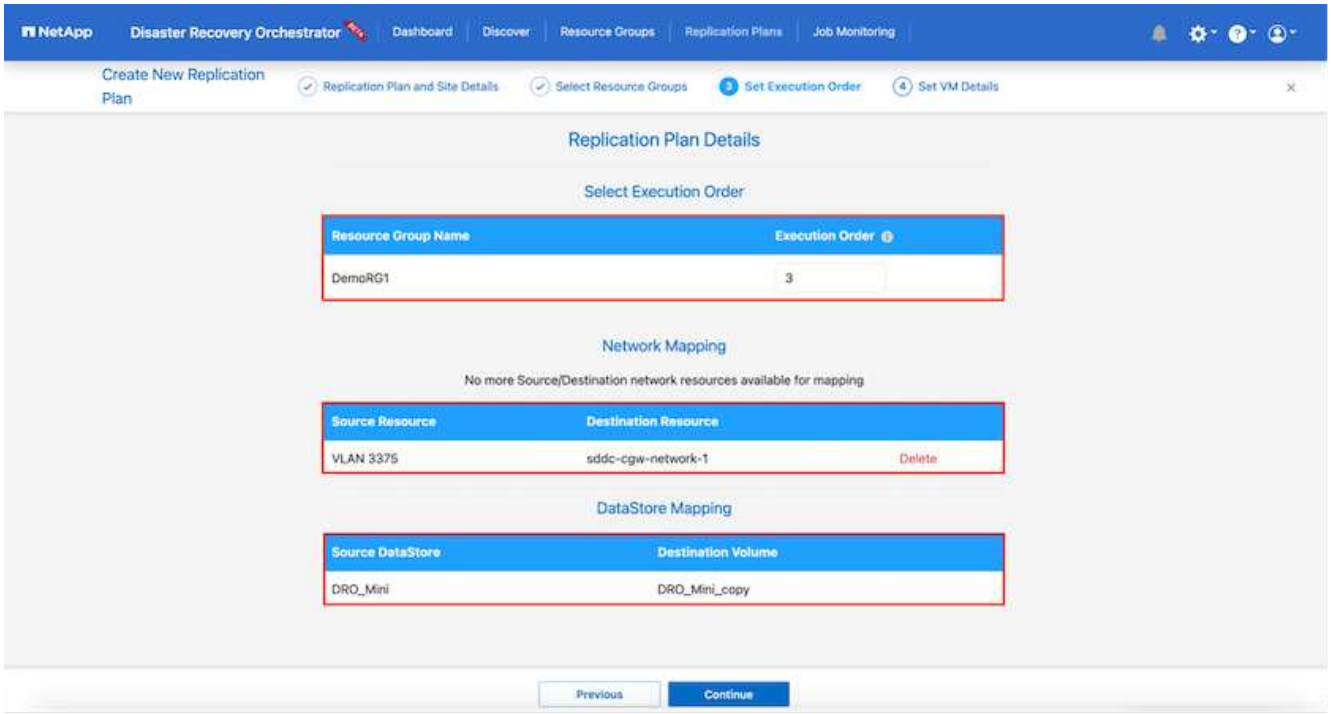


3. リカバリマッピングが完了したら、クラスタマッピングを選択します。

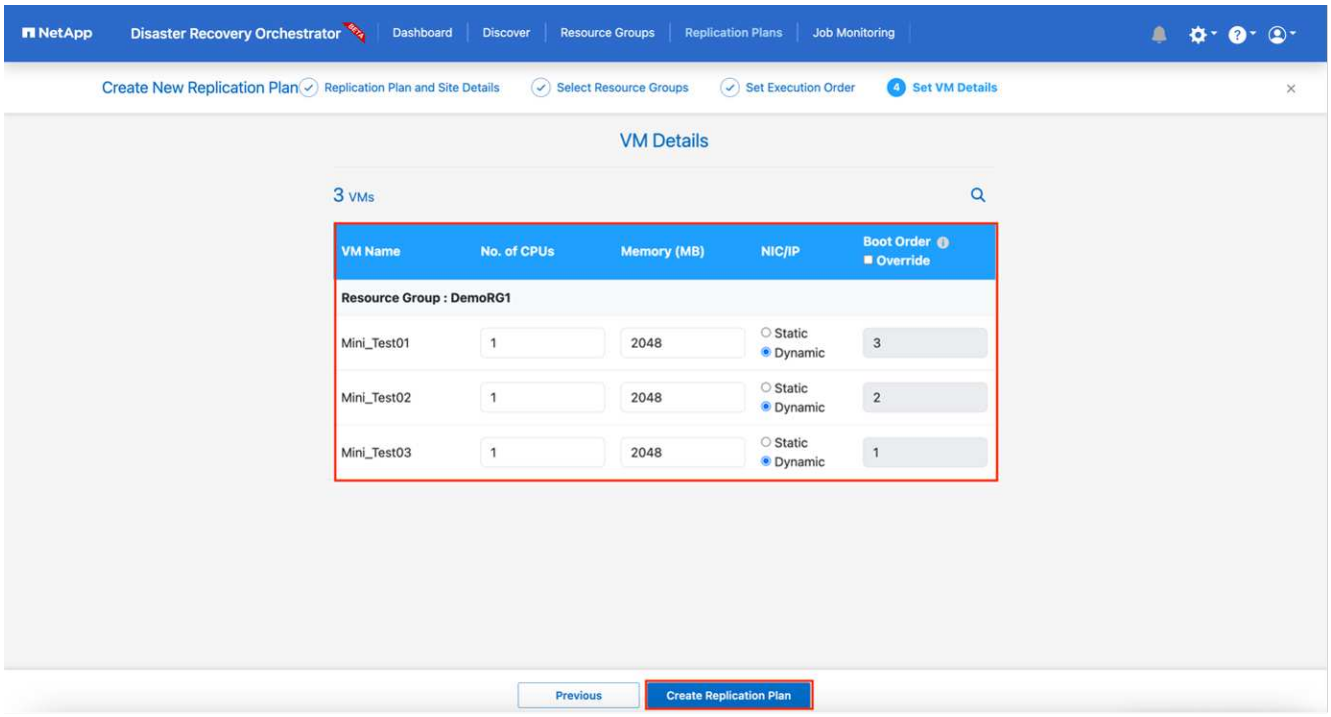


4. [リソースグループの詳細]を選択し、[*続行]をクリックします。
5. リソースグループの実行順序を設定します。このオプションを使用すると、複数のリソースグループが存在する場合の処理の順序を選択できます。
6. 完了したら、該当するセグメントへのネットワークマッピングを選択します。セグメントはVMC内でプロビジョニング済みである必要があるため、VMをマッピングする適切なセグメントを選択してください。
7. VMを選択すると、データストアマッピングが自動的に選択されます。

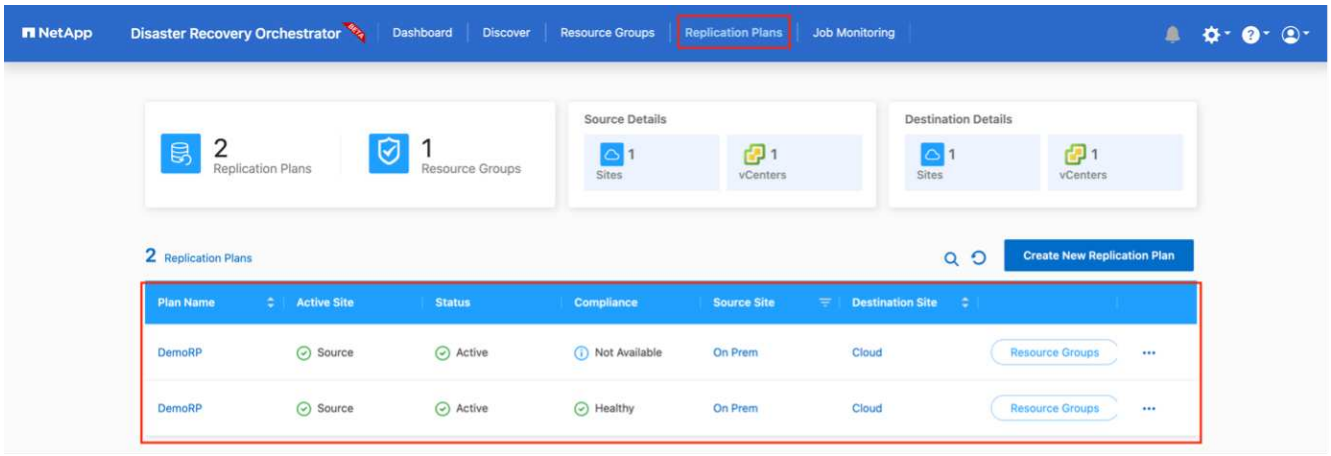
SnapMirrorはボリュームレベルです。したがって、すべてのVMがレプリケーションデスティネーションにレプリケートされます。必ずデータストアに含まれるすべてのVMを選択してください。選択しない場合は、レプリケーションプランの一部であるVMのみが処理されます。



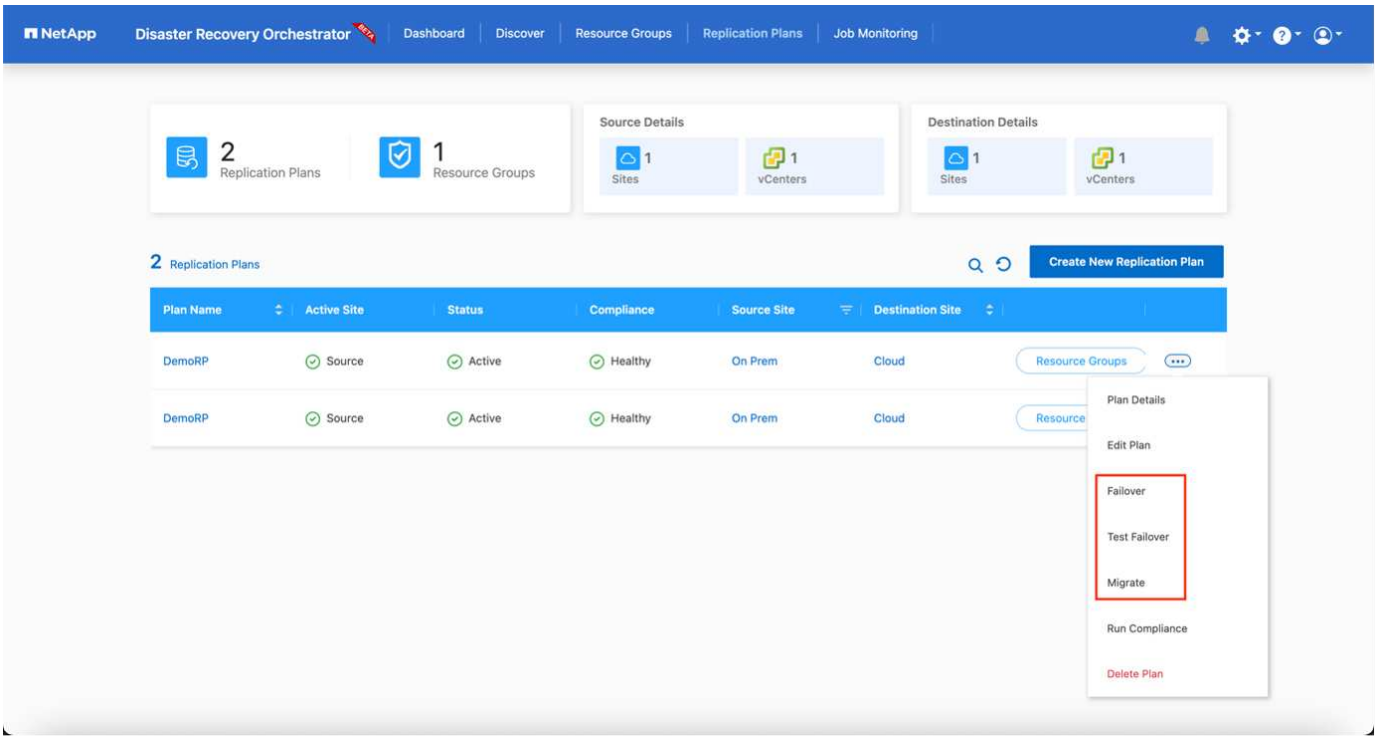
8. VMの詳細の下では、オプションでVMのCPUパラメータとRAMパラメータのサイズを変更できます。これは、大規模な環境を小規模なターゲットクラスタにリカバリする場合や、1対1の物理VMwareインフラをプロビジョニングしなくてもDRテストを実行する場合に非常に役立ちます。また、リソースグループ内の選択したすべてのVMのブート順序とブート遅延（秒）を変更することもできます。リソースグループのブート順序の選択時に選択したブート順序に変更が必要な場合は、追加のオプションを使用してブート順序を変更できます。デフォルトでは、リソースグループの選択時に選択したブート順序が使用されますが、この段階で変更を行うことができます。

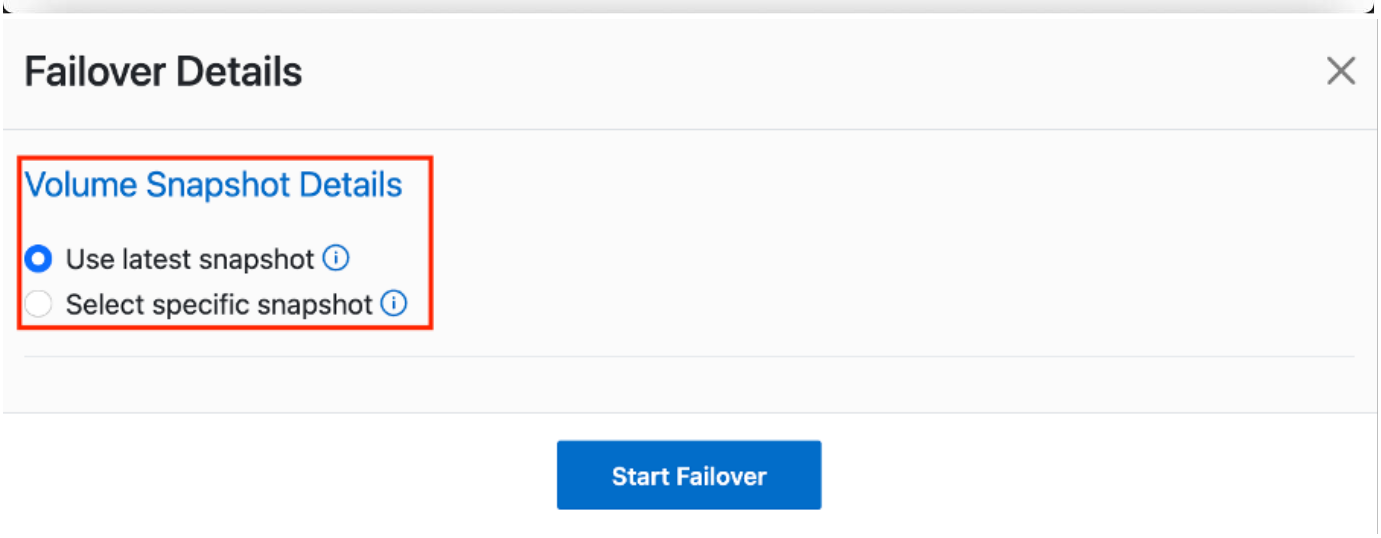


9. レプリケーションプランの作成*をクリックします。

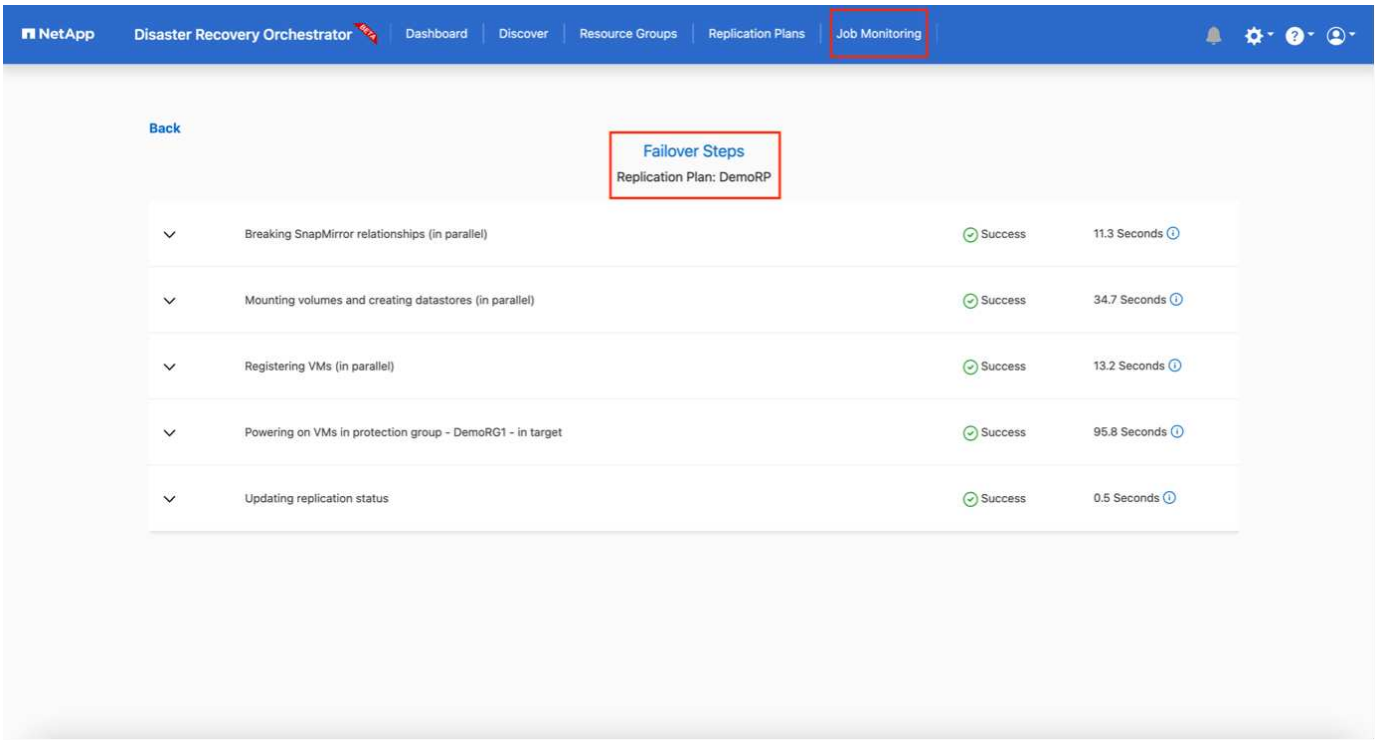


レプリケーションプランの作成後は、要件に応じて、フェイルオーバーオプション、テストフェイルオーバーオプション、または移行オプションを実行できます。フェイルオーバーおよびテストフェイルオーバーのオプションでは、最新のSnapMirror Snapshotコピーが使用されるほか、（SnapMirrorの保持ポリシーに基づいて）ポイントインタイムのSnapshotコピーから特定のSnapshotコピーを選択できます。ポイントインタイムオプションは、ランサムウェアなどの破損イベントに直面している場合に、最新のレプリカがすでに侵害されているか暗号化されていると非常に役立ちます。DROは、使用可能なすべてのポイントを時間単位で表示します。レプリケーションプランで指定された構成でフェイルオーバーまたはテストフェイルオーバーをトリガーするには、*フェイルオーバー*または*テストフェイルオーバー*をクリックします。

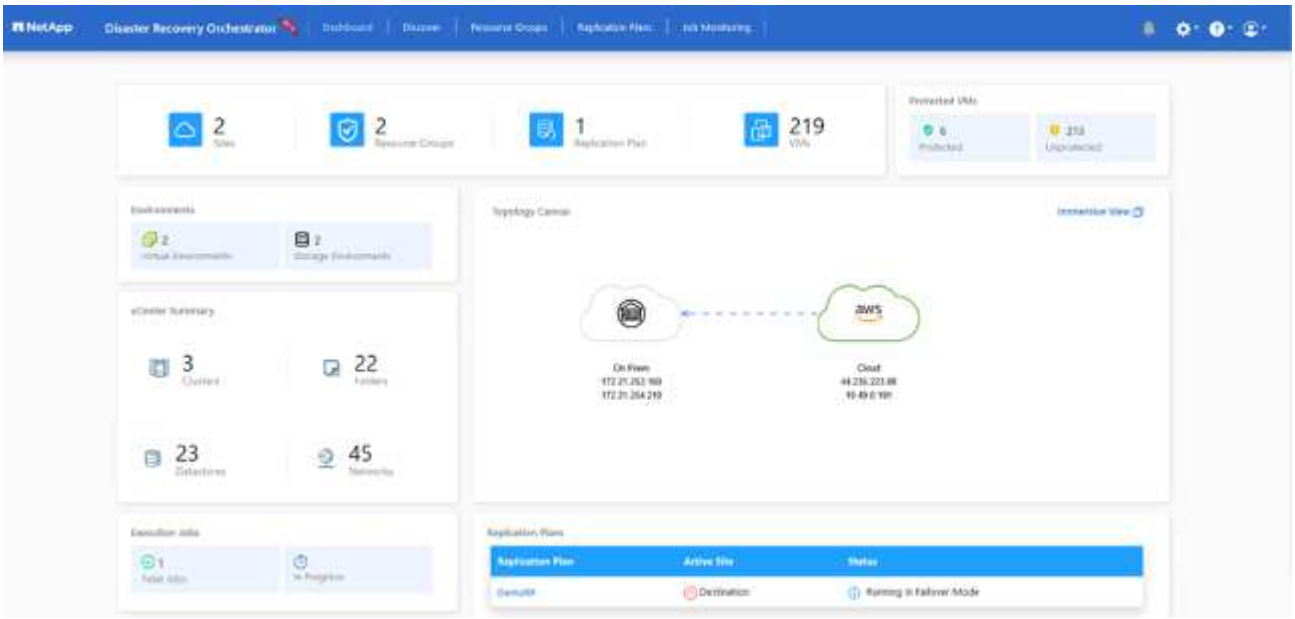




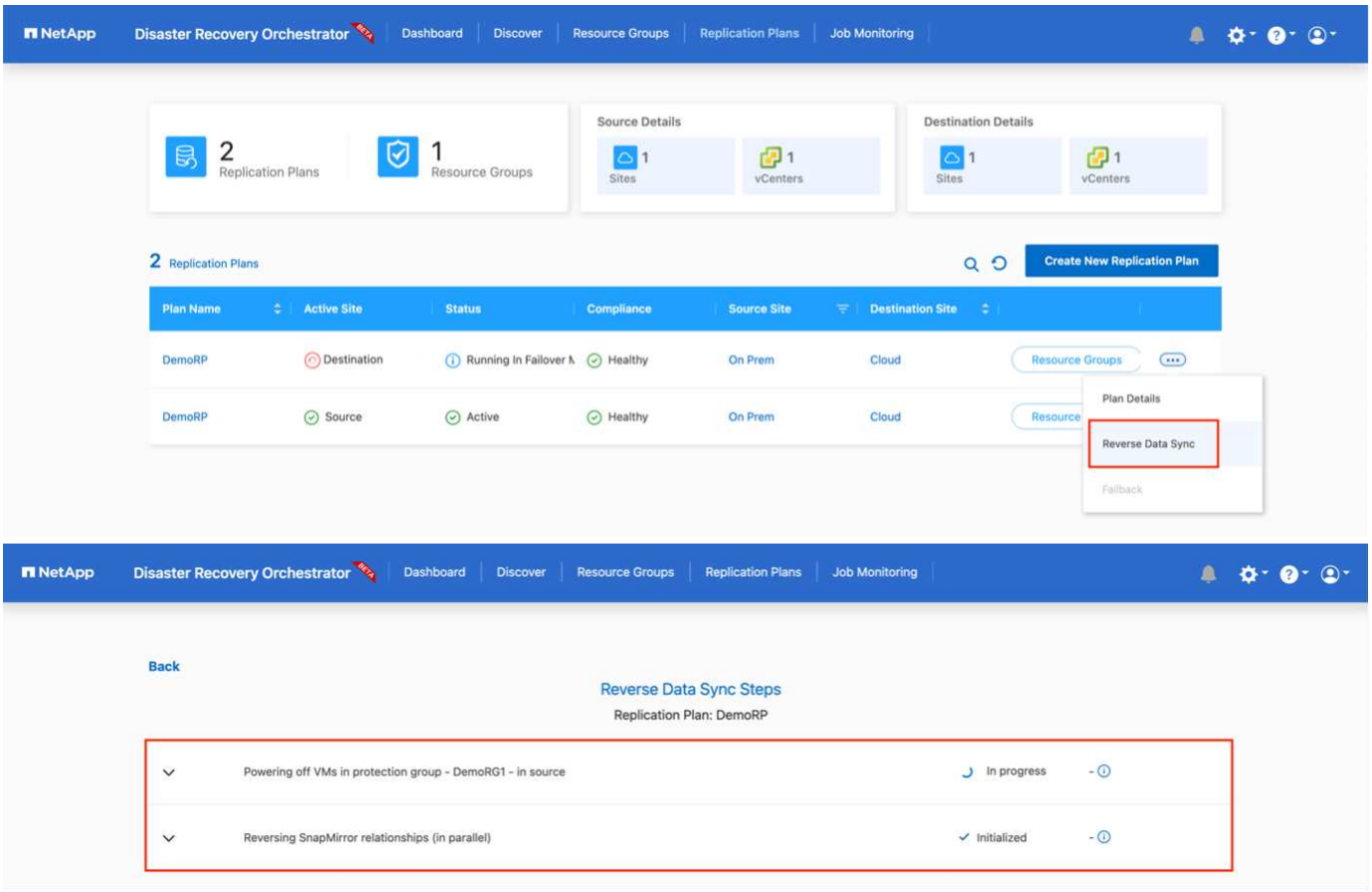
レプリケーションプランは、次のタスクメニューで監視できます。



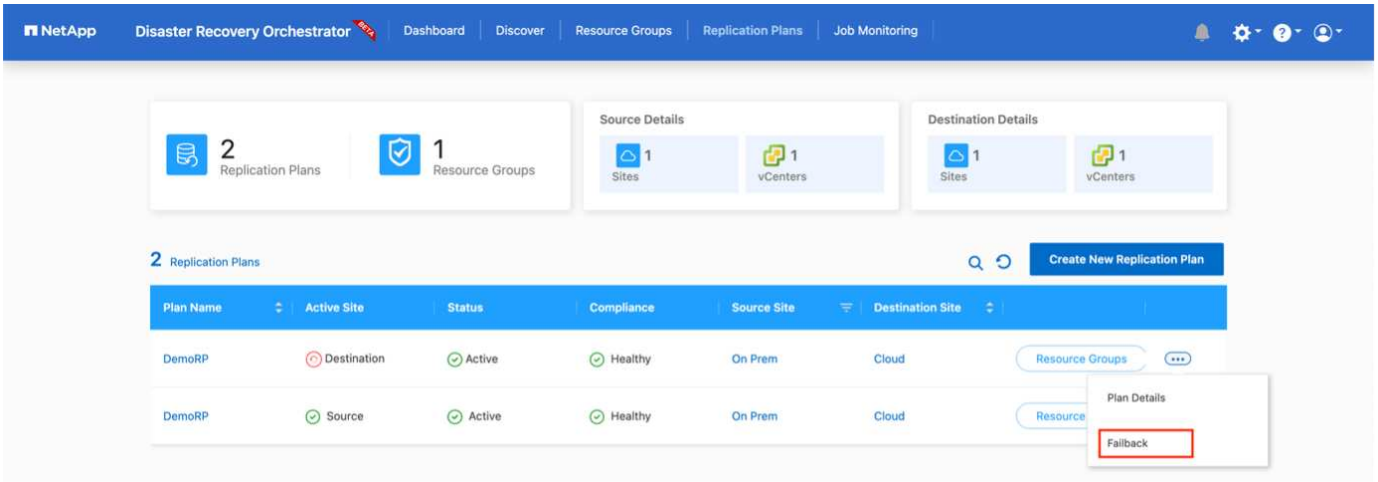
フェイルオーバーがトリガーされると、リカバリされた項目をVMC vCenter（VM、ネットワーク、データストア）で確認できます。デフォルトでは、VMはWorkloadフォルダにリカバリされます。



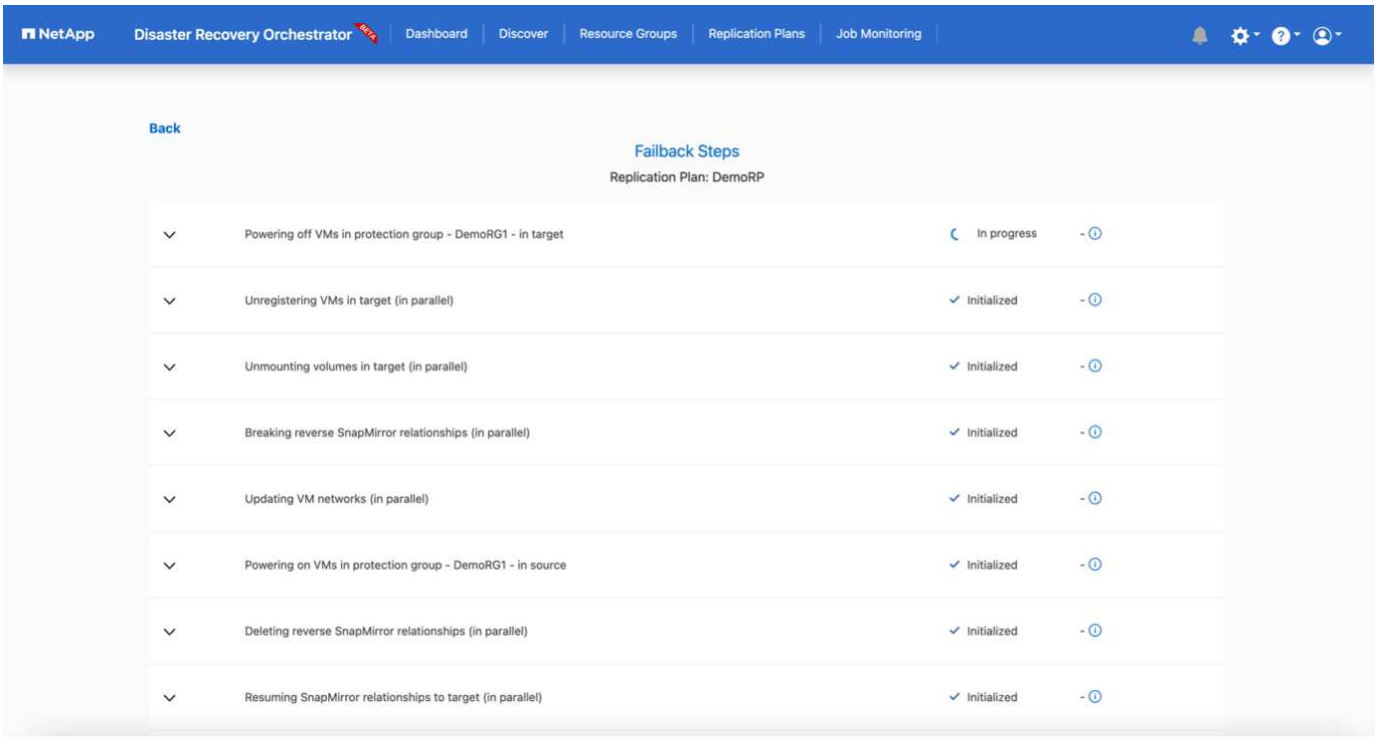
フェイルバックは、レプリケーションプランレベルで実行できます。テストフェイルオーバーでは、ティアダウンオプションを使用して変更をロールバックし、FlexClone関係を削除できます。フェイルオーバーに関連したフェイルバックは、2つのステップで行います。レプリケーションプランを選択し、*リバースデータ同期*を選択します。



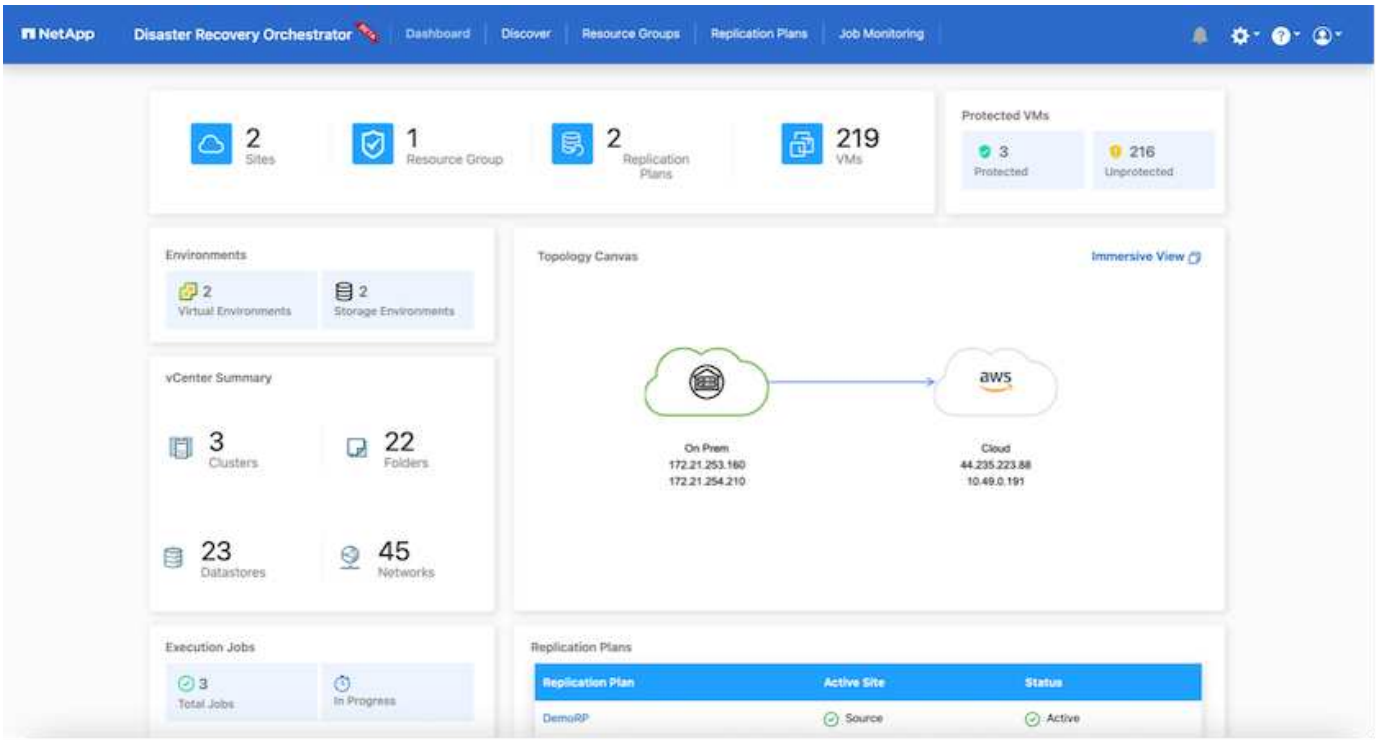
完了したら、フェイルバックを開始して元の本番サイトに戻すことができます。



オプションを含むドロップダウンを含むレプリケーションプランの概要のスクリーンショット"]



NetApp BlueXPでは、該当するボリューム（読み書き可能ボリュームとしてVMCにマッピングされているボリューム）のレプリケーションの健常性が遮断されていることがわかります。テストフェイルオーバー中、DROはデスティネーションボリュームまたはレプリカボリュームをマッピングしません。代わりに、必要なSnapMirror（またはSnapshot）インスタンスのFlexCloneコピーが作成され、FlexCloneインスタンスが公開されます。これにより、FSx ONTAPの物理容量が追加で消費されることはありません。このプロセスにより、DRのテストや優先度の異なるワークフローの実行中も、ボリュームが変更されず、レプリカジョブを続行できます。また'このプロセスにより'エラーが発生した場合や破損したデータがリカバリされた場合には'レプリカが破壊されるリスクを伴わずにリカバリをクリーンアップできます



ランサムウェアからのリカバリ

ランサムウェアからのリカバリは困難な作業です。具体的には、IT組織にとっては、安全な返品ポイントが特定され、復元されたワークロードを、睡眠中のマルウェアや脆弱なアプリケーションなどから再発生する攻撃から保護するために、ピンポイントを確立することは困難です。

DROは、利用可能な任意の時点からシステムを回復できるようにすることで、このような問題に対処します。また、機能的で分離されたネットワークにワークロードをリカバリして、南北トラフィックにさらされない場所でアプリケーションが機能し、相互に通信できるようにすることもできます。これにより、セキュリティチームはフォレンジックを実行する安全な場所を手に入れ、隠れているマルウェアや睡眠中のマルウェアが存在しないことを確認できます。

メリット

- 効率性と耐障害性に優れたSnapMirrorレプリケーションの使用：
- Snapshotコピーの保持により、任意の時点までのリカバリが可能
- ストレージ、コンピューティング、ネットワーク、アプリケーションの検証から、数百から数千のVMをリカバリするのに必要なすべての手順を完全に自動化します。
- ONTAP FlexCloneテクノロジを使用したワークロードのリカバリ：レプリケートされたボリュームを変更しない方法を使用します。
  - ボリュームやSnapshotコピーのデータが破損するリスクを回避します。
  - DRテストのワークフロー中にレプリケーションが中断されるのを回避します
  - DRデータとクラウドコンピューティングリソースを組み合わせたDRデータの使用は、DR以外のワークフロー（DevTest、セキュリティテスト、パッチテスト、アップグレードテスト、修復テストなど）にも適しています。
- CPUとRAMの最適化により、小規模なコンピューティングクラスタへのリカバリが可能になり、クラウドコストを削減

Veeam ReplicationとFSx ONTAPを使用したVMware Cloud on AWSへのディザスタリカバリ

Amazon FSx ONTAPとVMware Cloud on AWSの統合は、NetAppのONTAPファイルシステム上に構築されたAWS管理の外部NFSデータストアで、SDDC内のクラスタに接続できます。コンピューティングリソースとは別に拡張できる、柔軟性に優れたハイパフォーマンスな仮想ストレージインフラをお客様に提供します。

作成者：Niyaz Mohamed - NetAppソリューションエンジニアリング

概要

VMware Cloud on AWS SDDCをディザスタリカバリのターゲットとして使用することを検討しているお客様の場合、FSx ONTAPデータストアを使用して、VMレプリケーション機能を提供する検証済みのサードパーティソリューションを使用してオンプレミスからデータをレプリケートできます。FSx ONTAPデータストアを追加することで、ストレージに対応するためだけに大量のESXiホストを使用してAWS SDDC上にVMwareクラウドを構築するよりも、コストを最適化できます。

このアプローチは、VMCのパイロットライトクラスタとFSx ONTAPデータストアを使用してVMレプリカを

ホストするのにも役立ちます。レプリケーション計画を正常にフェイルオーバーすることで、VMware Cloud on AWSへの移行オプションとして同じプロセスを拡張することもできます。

問題点

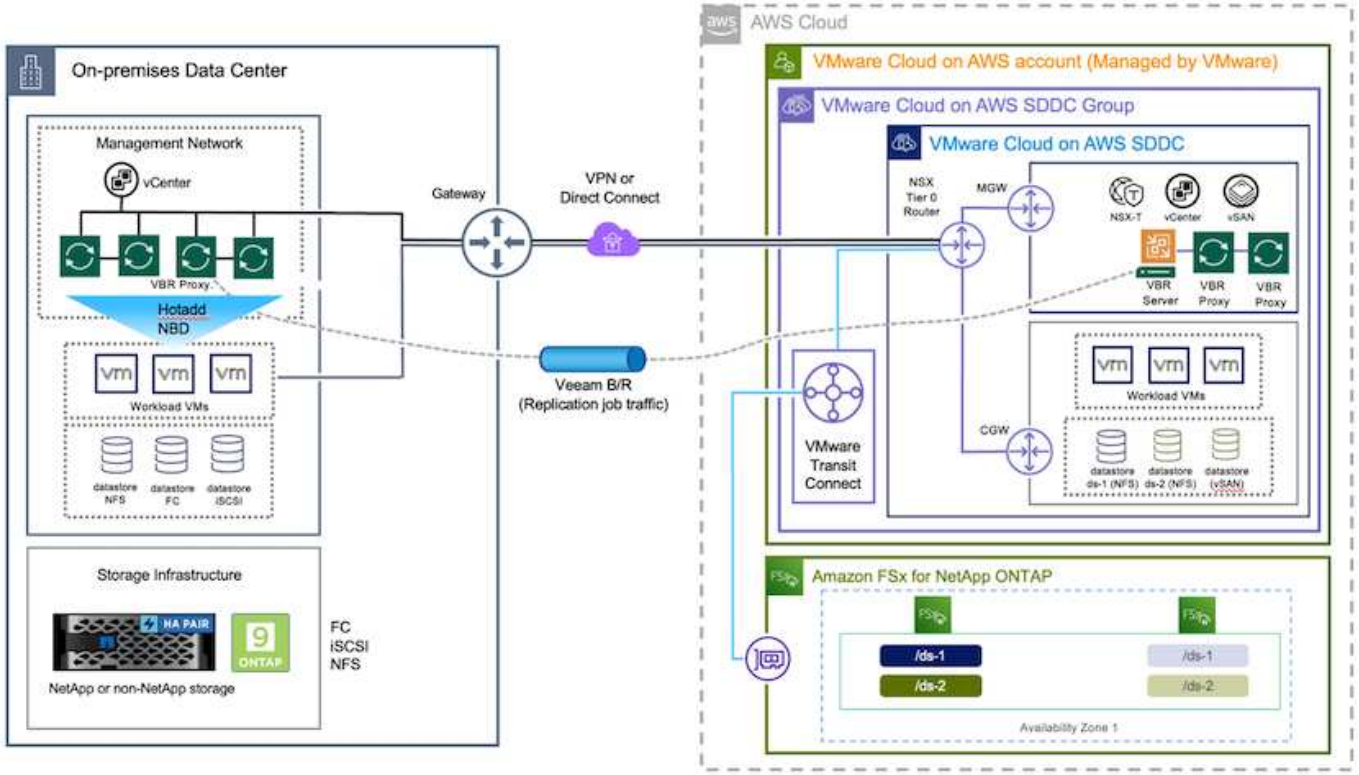
本ドキュメントでは、FSx ONTAPデータストアとVeeam Backup and Replicationを使用して、VMレプリケーション機能を使用してオンプレミスのVMware VMからVMware Cloud on AWSへのディザスタリカバリを設定する方法について説明します。

Veeam Backup & Replicationを使用すると、オンサイトとリモートのレプリケーションでディザスタリカバリ（DR）を実現できます。仮想マシンがレプリケートされると、Veeam Backup & Replicationは、ネイティブのVMware vSphere形式でターゲットのVMware Cloud on AWS SDDCクラスタにVMの正確なコピーを作成し、元のVMとの同期を維持します。

VMのコピーがすぐに開始できる状態にあるため、レプリケーションによって最適なRecovery Time Objective（RTO；目標復旧時間）値が得られます。このレプリケーションメカニズムにより、災害発生時にVMware Cloud on AWS SDDCでワークロードを迅速に開始できます。Veeam Backup & Replicationソフトウェアは、WAN経由のレプリケーションや低速接続のトラフィック転送も最適化します。さらに、重複データブロック、ゼロデータブロック、スワップファイル、除外VMゲストOSファイルを除外し、レプリカトラフィックを圧縮します。

レプリケーションジョブがネットワーク帯域幅全体を消費しないようにするには、WANアクセラレータとネットワークスロットリングルールを設定します。Veeam Backup & Replicationのレプリケーションプロセスはジョブベースです。つまり、レプリケーションはレプリケーションジョブを設定して実行されます。災害が発生した場合は、レプリカコピーにフェイルオーバーすることで、フェイルオーバーをトリガーしてVMをリカバリできます。

フェイルオーバーが実行されると、レプリケートされたVMが元のVMの役割を引き継ぎます。フェイルオーバーは、レプリカの最新の状態、または既知の任意のリストアポイントに対して実行できます。これにより、必要に応じてランサムウェアからのリカバリや個別のテストが可能Veeam Backup & Replicationでは、フェイルオーバーとフェイルバックは一時的な中間ステップであり、あとで完了する必要があります。Veeam Backup & Replicationには、さまざまなディザスタリカバリシナリオに対応するためのオプションが複数用意されています。



解決策 の導入

手順の概要

1. Veeam Backup & Replicationソフトウェアは、適切なネットワーク接続を備えたオンプレミス環境で実行されています。
2. VMware Cloud on AWSを設定します。VMware Cloud on AWS SDDCとFSx ONTAPをNFSデータストアとして導入、設定する方法については、VMware Cloud Tech Zoneの記事を参照して"VMware Cloud on AWS integration with Amazon FSx ONTAP導入ガイド"ください。（最小限の構成でセットアップされたパイロットライト環境は、DR目的で使用できます。インシデントが発生した場合、VMはこのクラスタにフェイルオーバーし、ノードを追加できます）。
3. Veeam Backup and Replicationを使用してVMレプリカを作成するためのレプリケーションジョブを設定します。
4. フェイルオーバープランを作成し、フェイルオーバーを実行
5. 災害が完了し、プライマリサイトが稼働したら、本番環境のVMにスイッチバックします。

VMCおよび**FSx ONTAP**データストアへの**Veeam VM**レプリケーションの前提条件

1. Veeam Backup & ReplicationのバックアップVMがソースvCenterと、AWS SDDCクラスタ上のターゲットVMwareクラウドに接続されていることを確認します。
2. バックアップサーバは、短縮名を解決し、ソースvCenterとターゲットvCenterに接続できる必要があります。
3. ターゲットのFSx ONTAPデータストアには、レプリケートされたVMのVMDKを格納できるだけの十分な空きスペースが必要

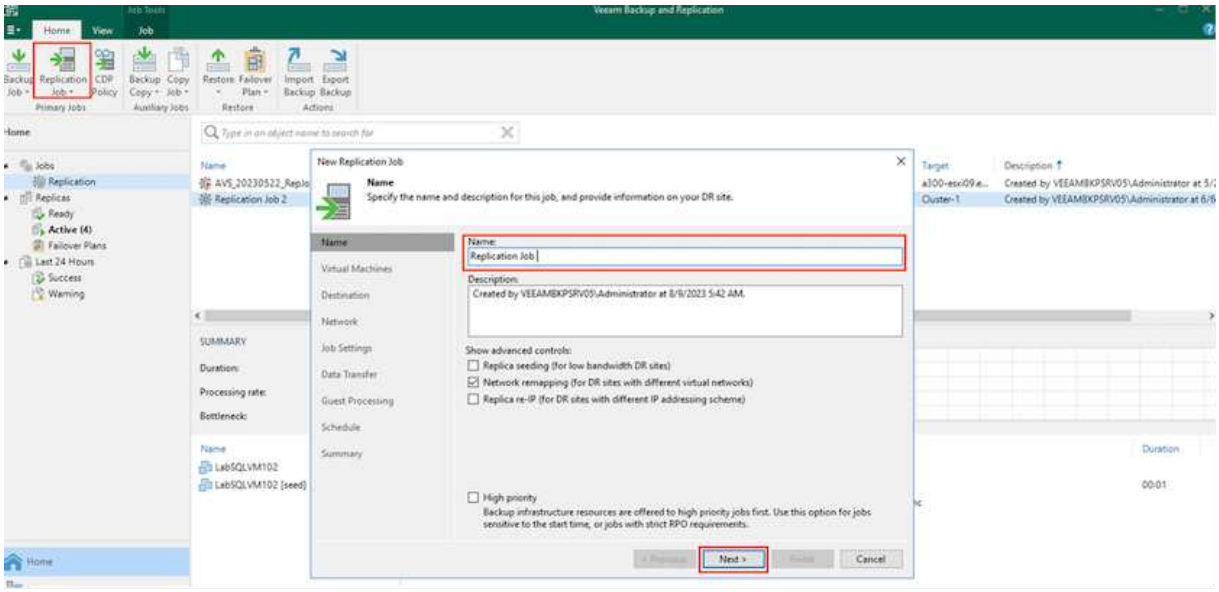
詳細については、「考慮事項と制限事項」を参照してください"ここをクリック"。

ステップ**1**：**VM**のレプリケート

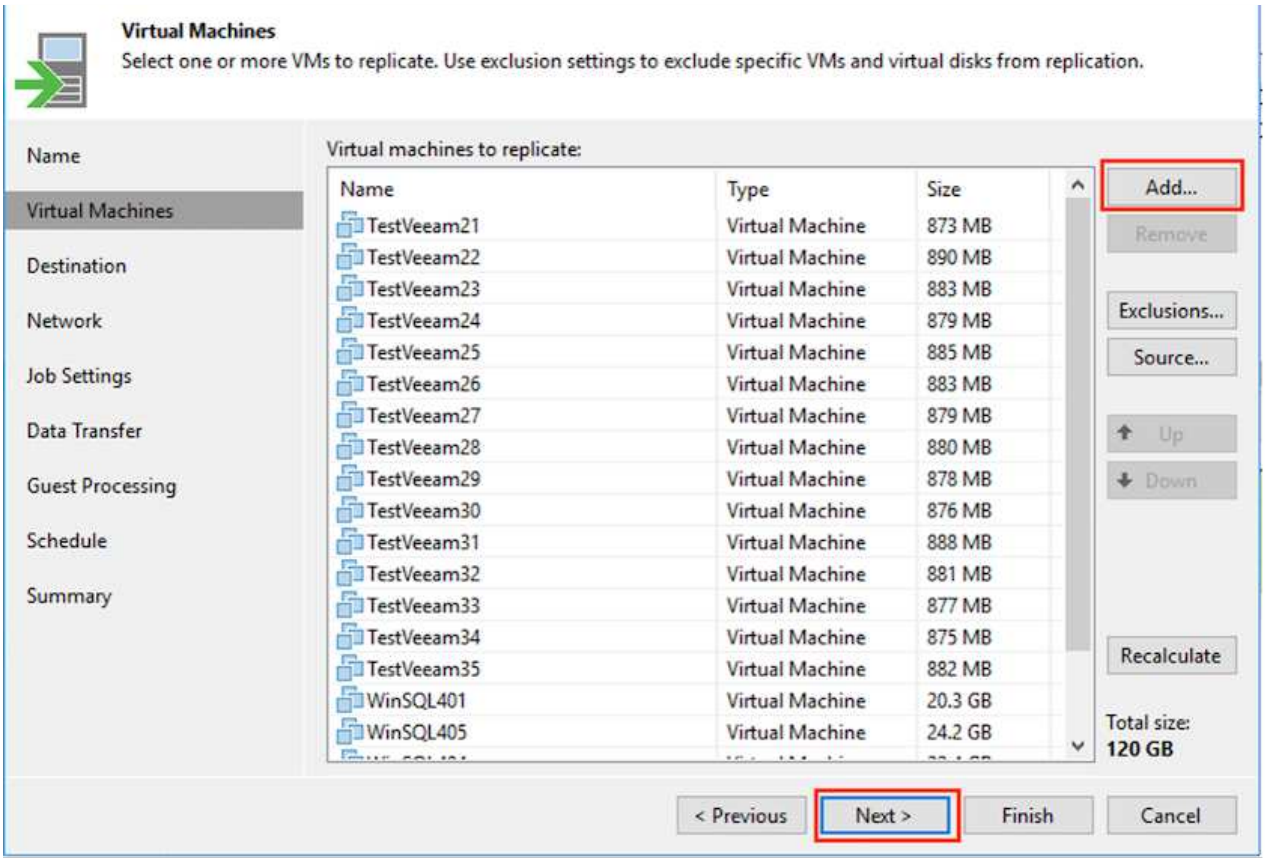
Veeam Backup & ReplicationはVMware vSphereスナップショット機能を活用し、レプリケーション中にVeeam Backup & ReplicationはVMware vSphereにVMスナップショットの作成を要求します。VMスナップショットは、仮想ディスク、システムの状態、構成などを含むVMのポイントインタイムコピーです。Veeam Backup & Replicationでは、Snapshotをレプリケーションのデータソースとして使用します。

VMをレプリケートするには、次の手順を実行します。

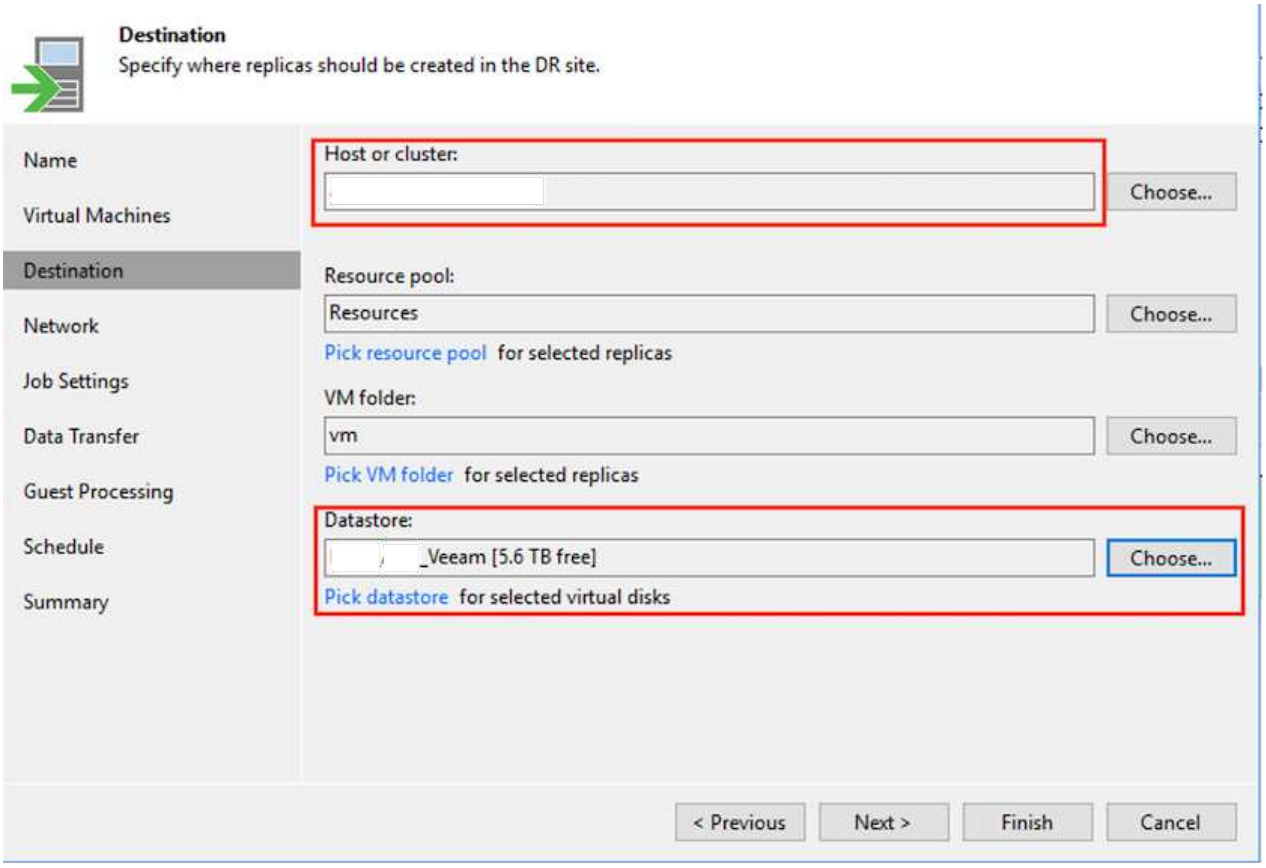
1. Veeam Backup & Replicationコンソールを開きます。
2. [Home]ビューで、[Replication Job]>[Virtual machine]>[VMware vSphere]を選択します。
3. ジョブ名を指定し、適切な詳細制御チェックボックスを選択します。[Next]をクリックします。
   - オンプレミスとAWS間の接続で帯域幅が制限されている場合は、[Replica seeding]チェックボックスをオンにします。
   - VMware Cloud on AWS SDDC上のセグメントがオンプレミスサイトネットワークのセグメントと一致しない場合は、[Network remapping（for AWS VMC sites with different networks）]チェックボックスをオンにします。
   - オンプレミスの本番用サイトのIPアドレス指定方式がAWS VMCサイトのIPアドレス指定方式と異なる場合は、Replica Re-IP（for DR sites with different IP addressing scheme）チェックボックスを選択します。



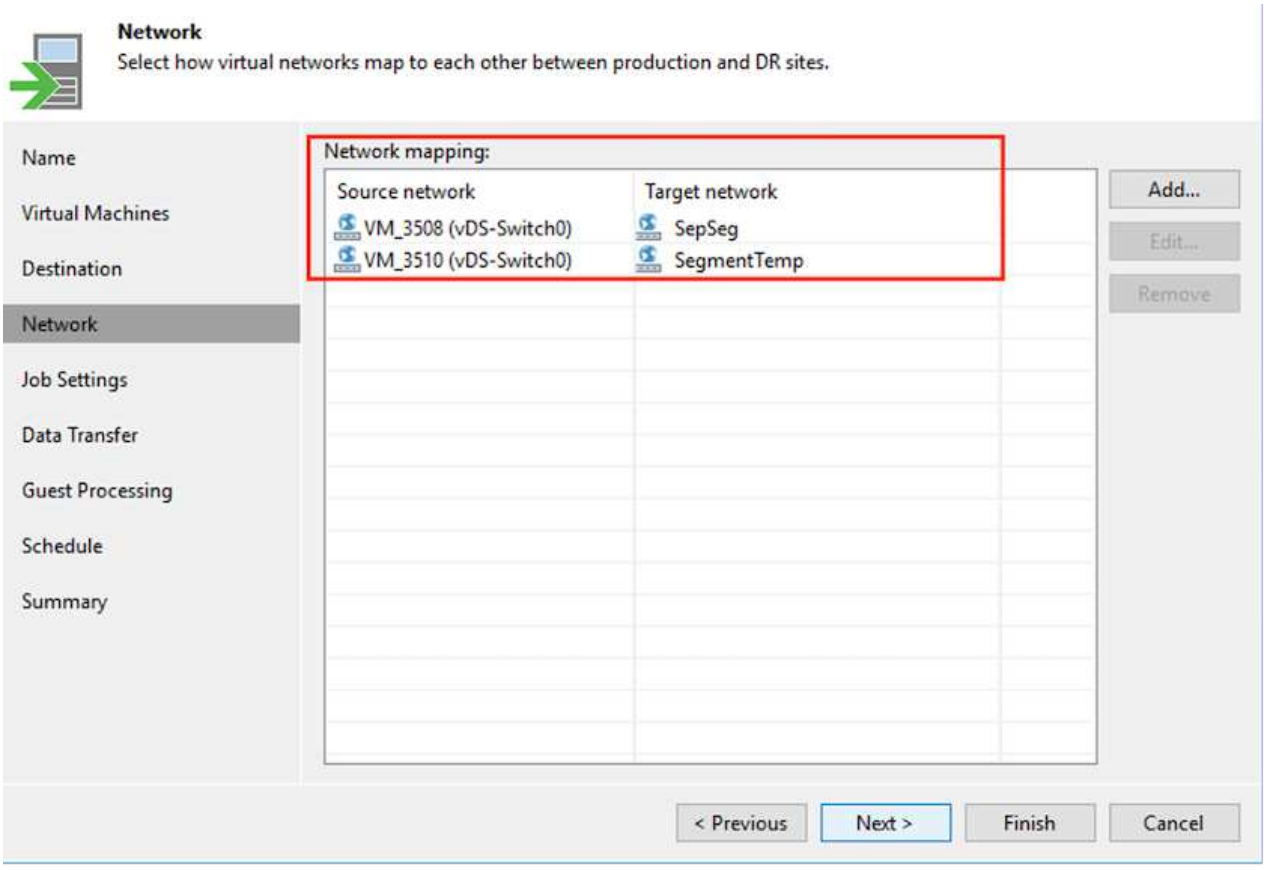
4. [Virtual Machines]手順で、VMware Cloud on AWS SDDCに接続されたFSx ONTAPデータストアにレプリケートする必要のあるVMを選択します。仮想マシンをVSANに配置して、使用可能なVSANデータストアの容量をいっぱいにすることができます。パイロットライトクラスタでは、3ノードクラスタの使用可能容量が制限されます。残りのデータはFSx ONTAPデータストアにレプリケートできます。をクリックし、[オブジェクトの追加]ウィンドウで必要な**VM**または**VM**コンテナを選択して[追加]*をクリックします。「 * 次へ * 」をクリックします。



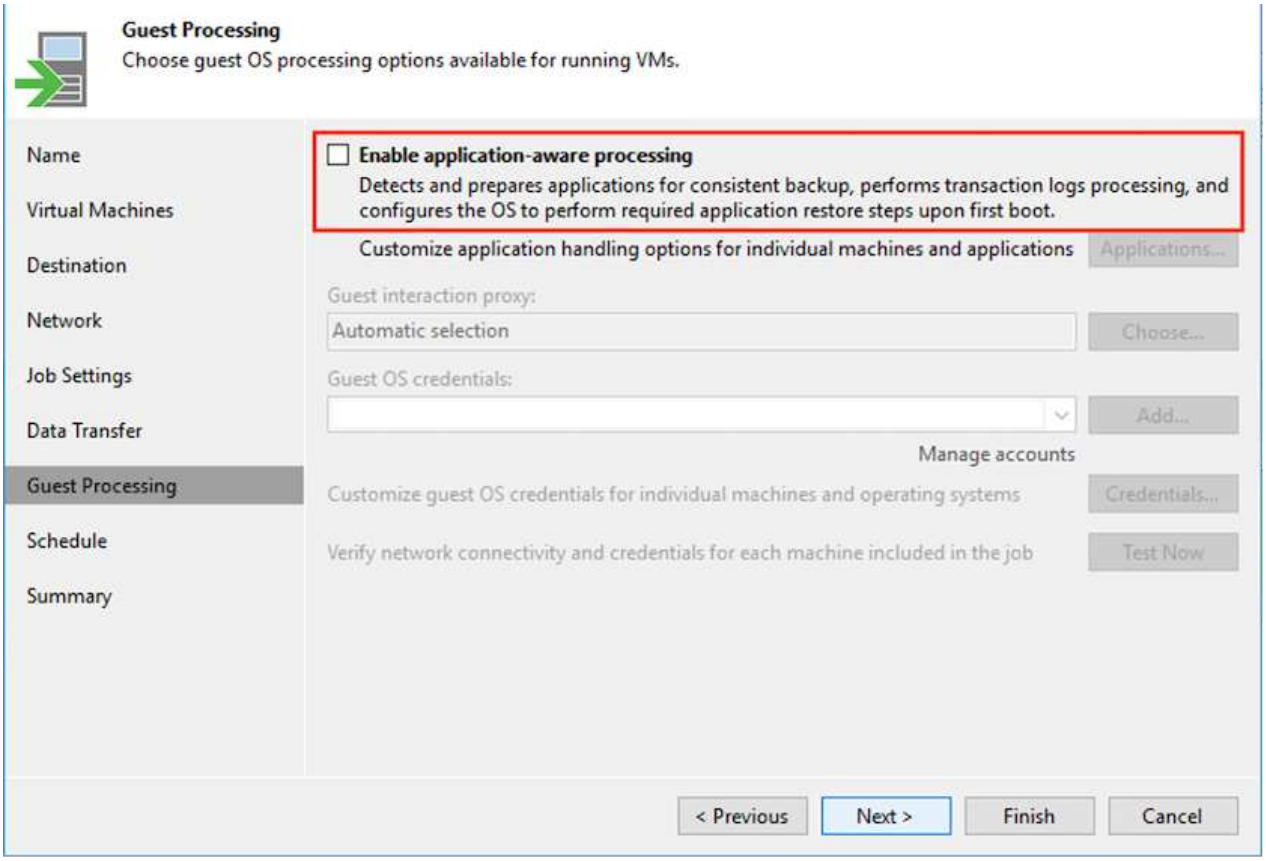
5. その後、デスティネーションをVMware Cloud on AWS SDDCクラスター/ホストとして選択し、VMレプリカ用の適切なリソースプール、VMフォルダ、FSx ONTAPデータストアを選択します。次に*[次へ]*をクリックします。



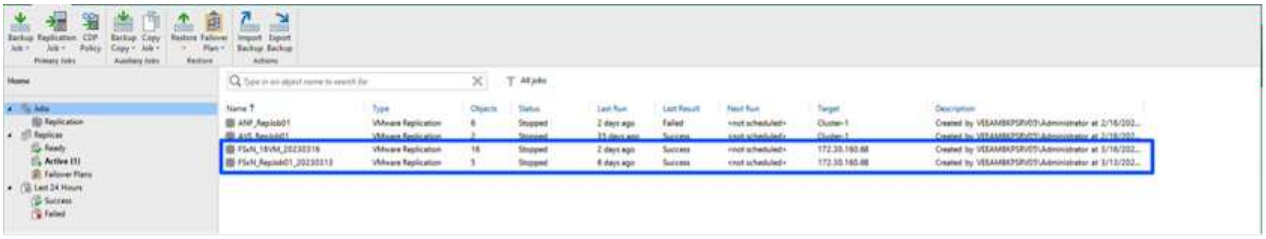
6. 次の手順では、必要に応じてソースとデスティネーションの仮想ネットワーク間のマッピングを作成します。



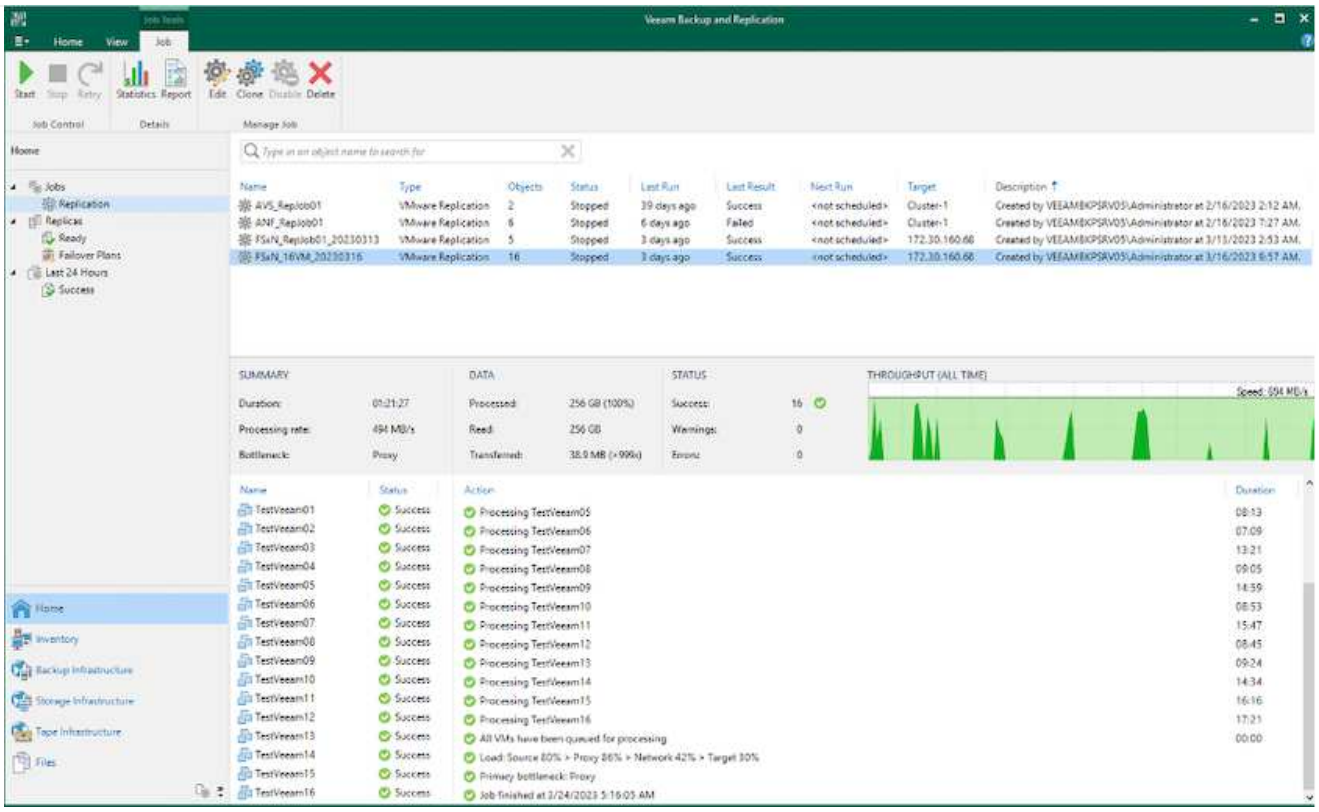
7. [ジョブ設定]ステップで、VMレプリカのメタデータや保持ポリシーなどを格納するバックアップリポジトリを指定します。
8. Data Transfer（データ転送）ステップで* Source（ソース）および Target（ターゲット）プロキシサーバーを更新し、 Automatic（自動）選択（デフォルト）のままにして Direct オプションを選択したままにして Next（次へ）*をクリックします。
9. [Guest Processing]ステップで、必要に応じて[Enable application-aware processing]オプションを選択します。「 * 次へ * 」をクリックします。



10. レプリケーションジョブを定期的に実行するレプリケーションスケジュールを選択します。
11. ウィザードの* Summary ステップで、レプリケーションジョブの詳細を確認します。ウィザードを終了した直後にジョブを開始するには、[完了]をクリックしたときにジョブを実行する*チェックボックスをオンにします。オンにしない場合は、チェックボックスをオフのままにします。次に、*[完了]*をクリックしてウィザードを閉じます。



レプリケーションジョブが開始されると、指定されたサフィックスのVMがデスティネーションVMC SDDCクラスタ/ホストに取り込まれます。



Veeamレプリケーションの詳細については、を参照してください"レプリケーションの仕組み"。

手順**2**：フェイルオーバープランを作成する

最初のレプリケーションまたはシードが完了したら、フェイルオーバープランを作成します。フェイルオーバープランは、依存するVMのフェイルオーバーを1つずつ、またはグループとして自動的に実行するのに役立ちます。フェイルオーバープランは、ブート遅延を含むVMの処理順序の青写真です。フェイルオーバープランは、重要な依存VMがすでに実行されていることを確認するのにも役立ちます。

プランを作成するには、レプリカという新しいサブセクションに移動し、フェイルオーバープランを選択します。適切なVMを選択します。Veeam Backup & Replicationは、この時点に最も近いリストアポイントを検索し、それらを使用してVMレプリカを開始します。

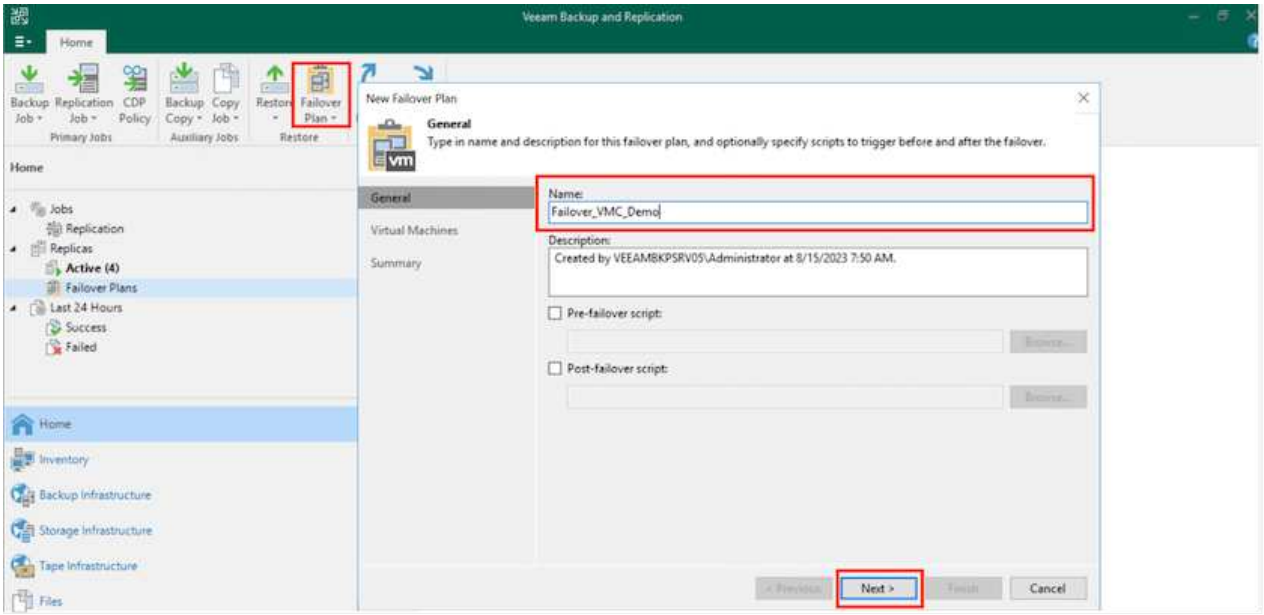
フェイルオーバープランを追加できるのは、初期レプリケーションが完了し、VMレプリカがReady状態になってからです。

フェイルオーバープランの実行時に同時に起動できるVMの最大数は10です。

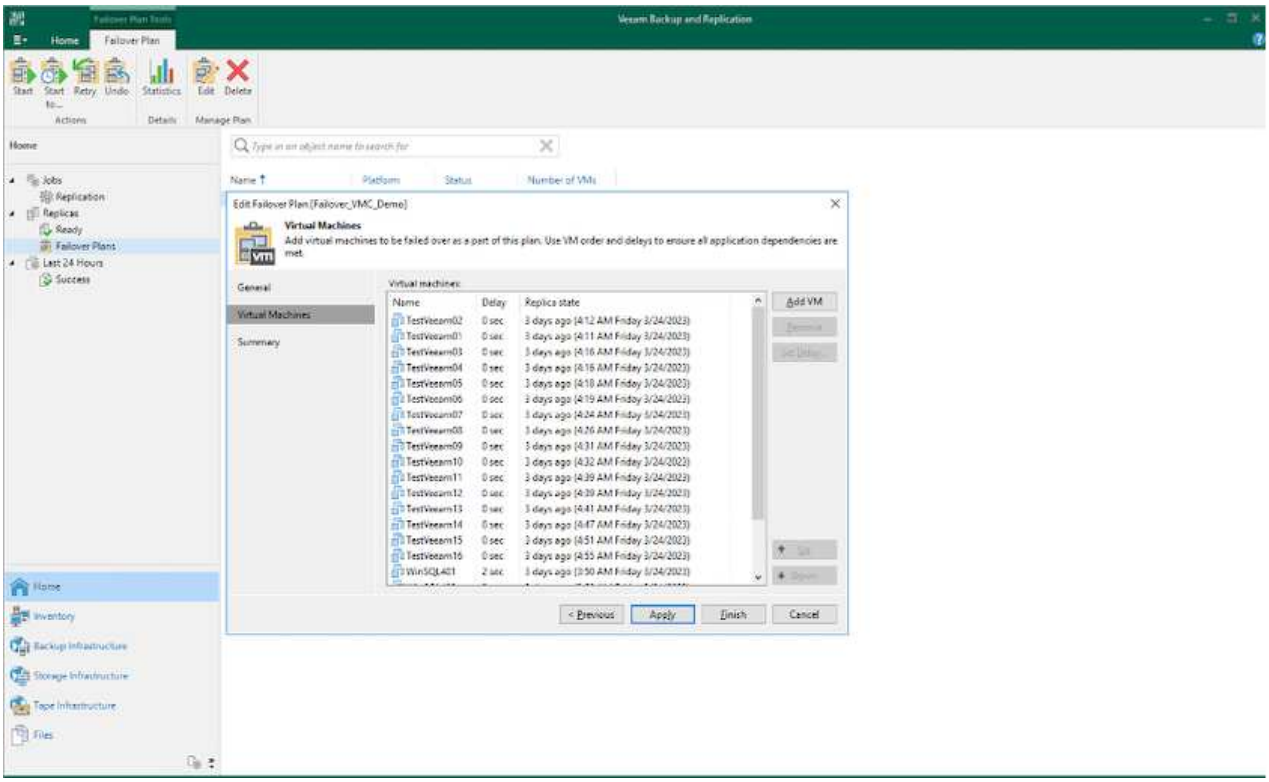
フェイルオーバープロセス中は、ソースVMの電源はオフになりません。

フェイルオーバープラン*を作成するには、次の手順を実行します。

1. [ホーム]ビューで、*[フェイルオーバープラン]>[VMware vSphere]*を選択します。
2. 次に、プランの名前と概要を入力します。必要に応じて、フェイルオーバー前およびフェイルオーバー後のスクリプトを追加できます。たとえば、スクリプトを実行して、レプリケートされたVMを起動する前にVMをシャットダウンします。



3. VMを計画に追加し、VMのブート順序とブート遅延を変更して、アプリケーションの依存関係を満たすようにします。



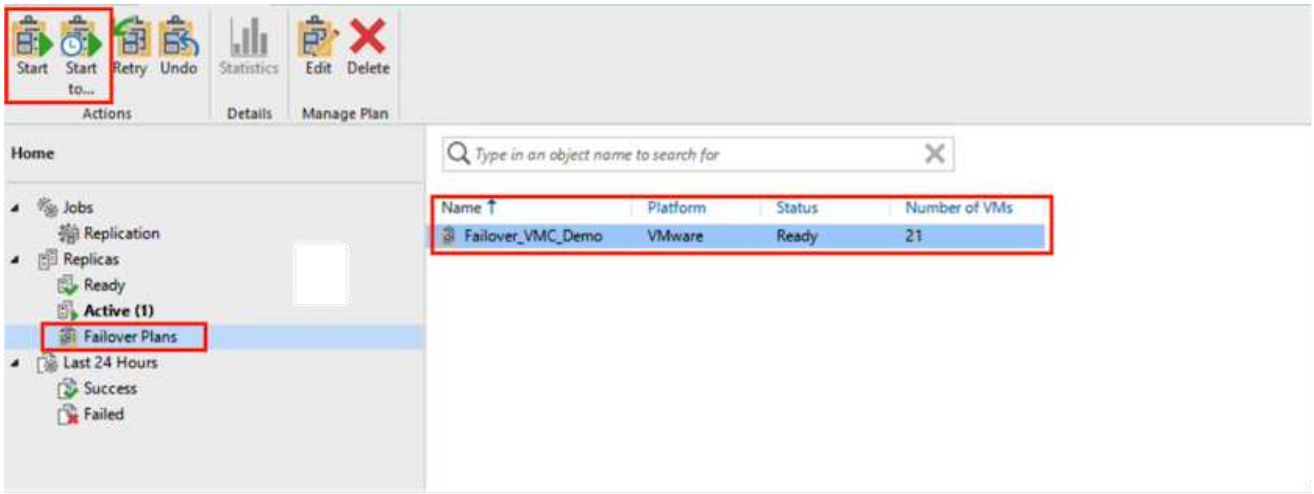
レプリケーションジョブの作成の詳細については、を参照してください"レプリケーションジョブの作成"。

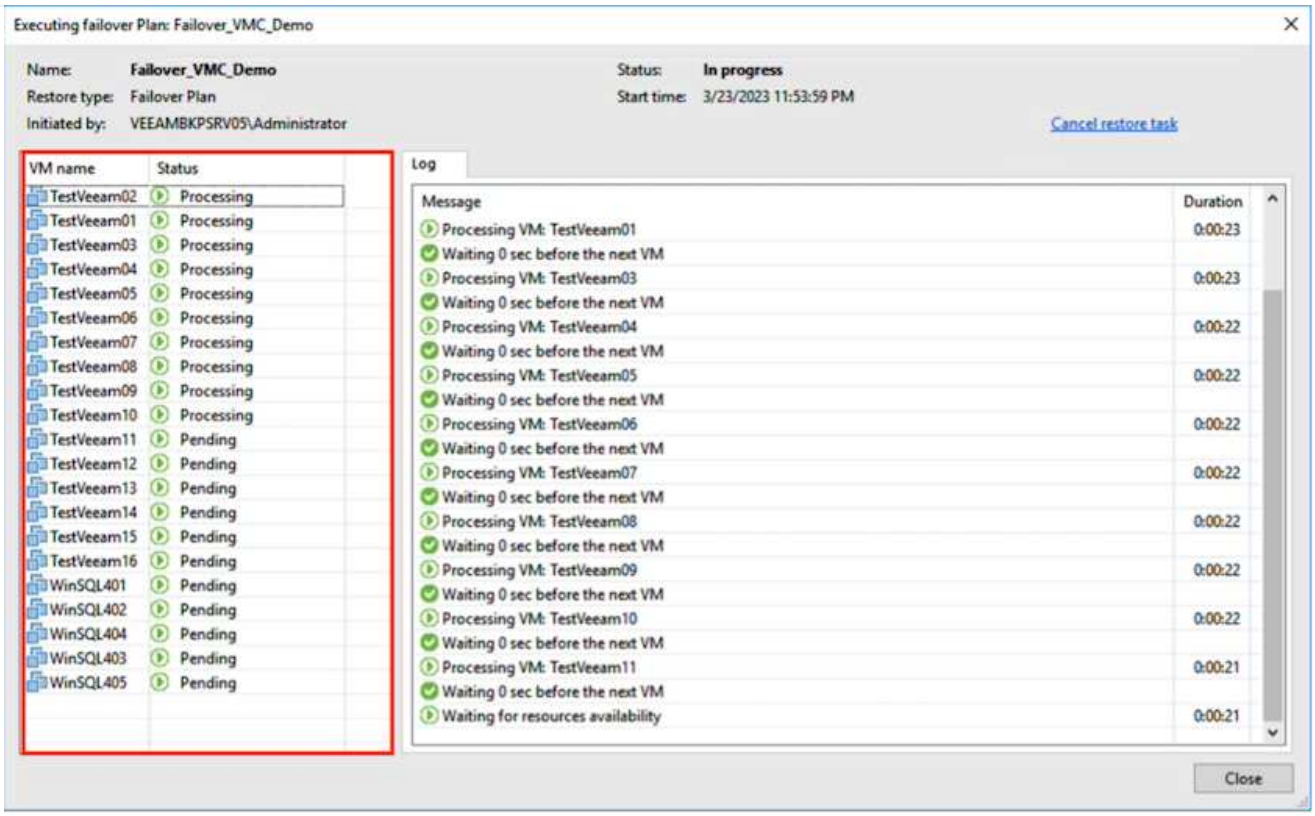
手順**3**：フェイルオーバープランを実行する

フェイルオーバー時には、本番サイトのソースVMがディザスタリカバリサイトのレプリカにスイッチオーバーされます。フェイルオーバープロセスの一環として、Veeam Backup & ReplicationはVMレプリカを必要なリストアポイントにリストアし、すべてのI/Oアクティビティをソース VMからそのレプリカに移動します。レプリカは、災害発生時だけでなく、DRドリルのシミュレーションにも使用できます。フェイルオーバーのシミュレーション中は、ソースVMは引き続き実行されます。必要なテストがすべて完了したら、フェイルオーバーを元に戻して通常の運用に戻すことができます。

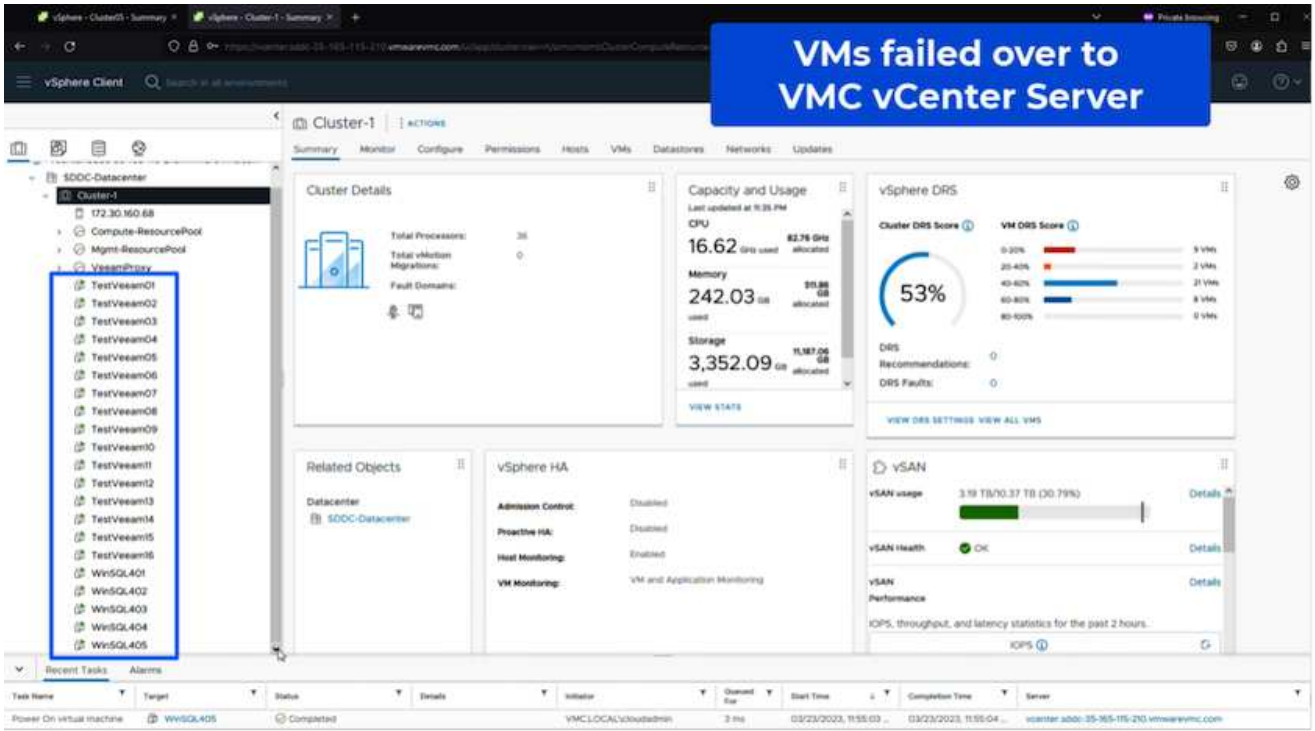
DRドリル中にIPの競合を回避するために、ネットワークのセグメント化が行われていることを確認します。

フェイルオーバープランを開始するには、* Failover Plans タブをクリックし、フェイルオーバープランを右クリックします。「 *** Start** （開始）」を選択しますこれにより、**VM**レプリカの最新のリストアポイントを使用してフェイルオーバーが実行されます。**VM**レプリカの特定のリストアポイントにフェイルオーバーするには、 Start to *を選択します。

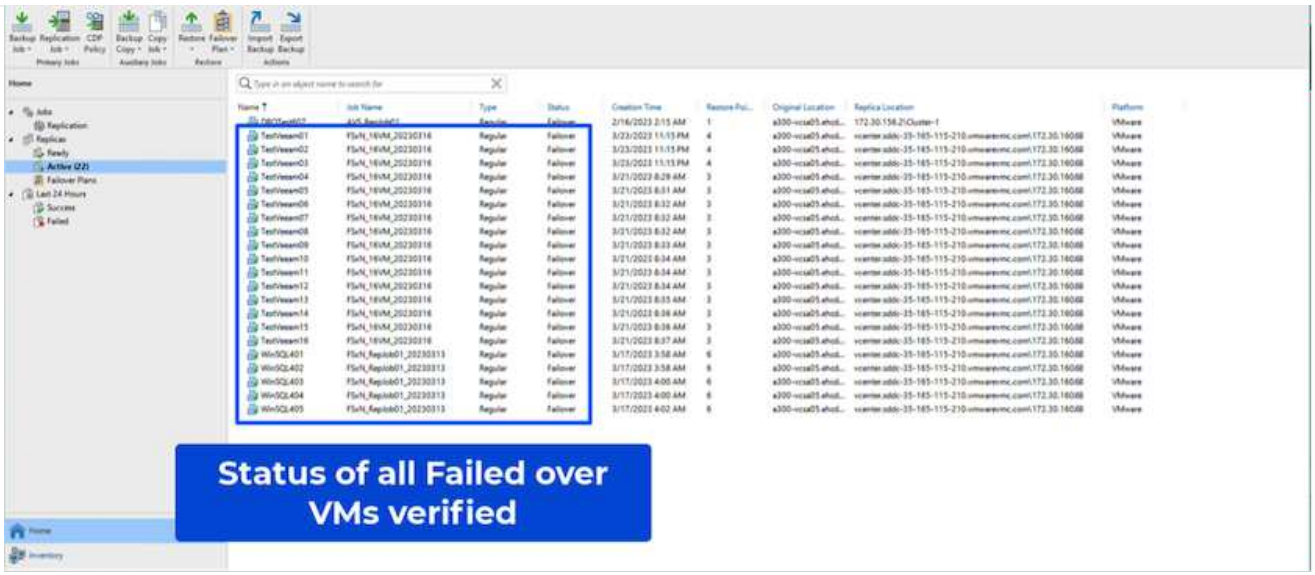




VMレプリカの状態がReadyからFailoverに変わり、VMはデスティネーションのVMware Cloud on AWS SDDCクラスタ/ホストで開始されます。



フェイルオーバーが完了すると、VMのステータスが「Failover」に変わります。



Veeam Backup & Replicationは、レプリカがReady状態に戻るまで、ソースVMのすべてのレプリケーションアクティビティを停止します。

フェイルオーバープランの詳細については、を参照してください"フェイルオーバープラン"。

手順**4**：本番サイトへのフェイルバック

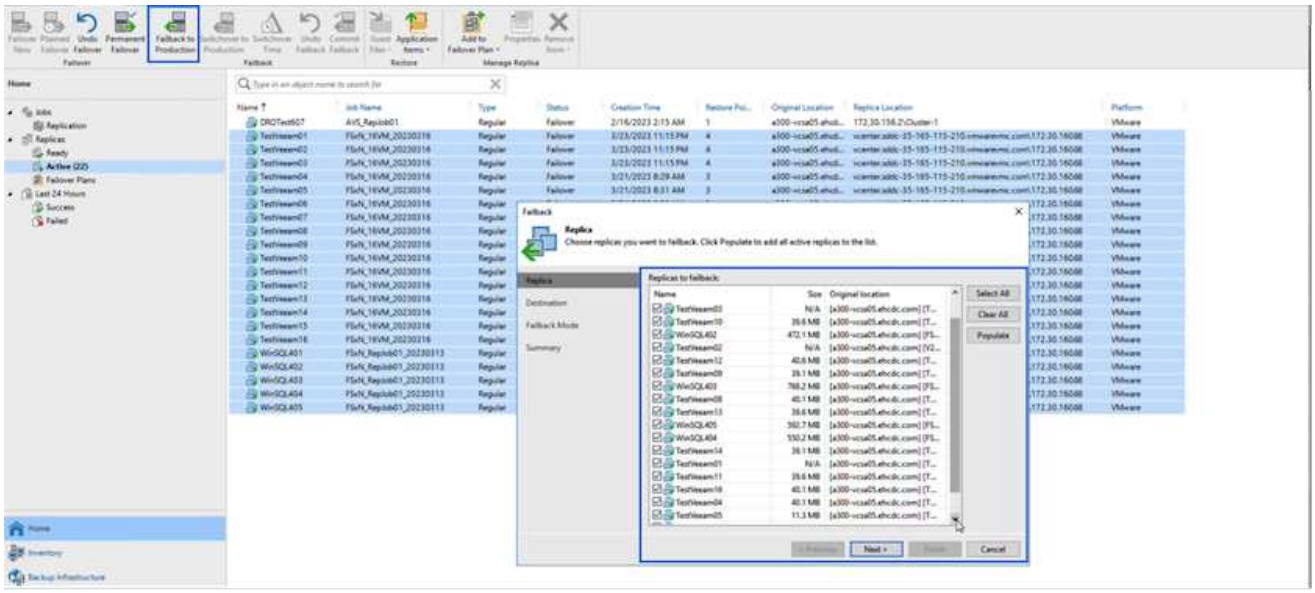
フェイルオーバープランの実行中は中間ステップとみなされ、要件に基づいて確定する必要があります。オプションには次のものがあります。

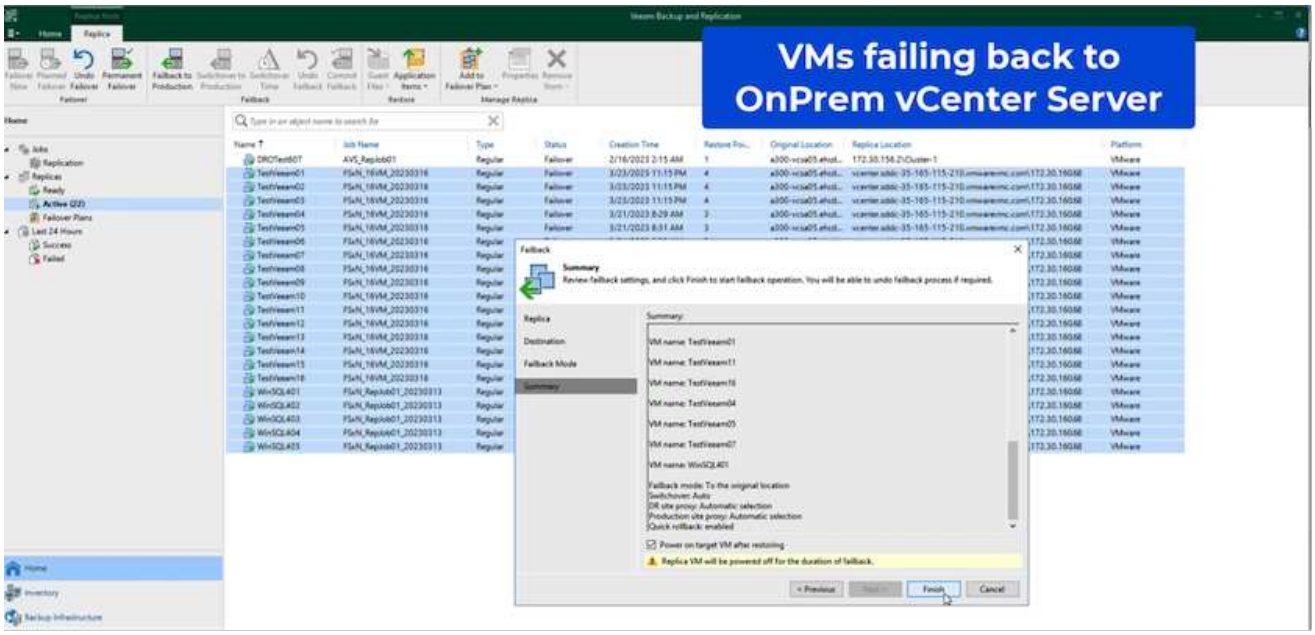
- 本番環境へのフェイルバック：元のVMに切り替えて、VMレプリカの実行中に発生したすべての変更を元のVMに転送します。

> フェイルバックを実行すると、変更は転送されますが、パブリッシュされません。[Commit failback]*（元のVMが期待どおりに動作することが確認されたら）または[Undo failback]*を選択して、元のVMが期待どおりに動作しない場合はVMレプリカに戻ります。

- フェイルオーバーを元に戻す-元のVMに切り替えて、VMレプリカの実行中に行った変更をすべて破棄します。
- 永続的フェイルオーバー-元のVMからVMレプリカに永続的に切り替え、このレプリカを元のVMとして使用します。

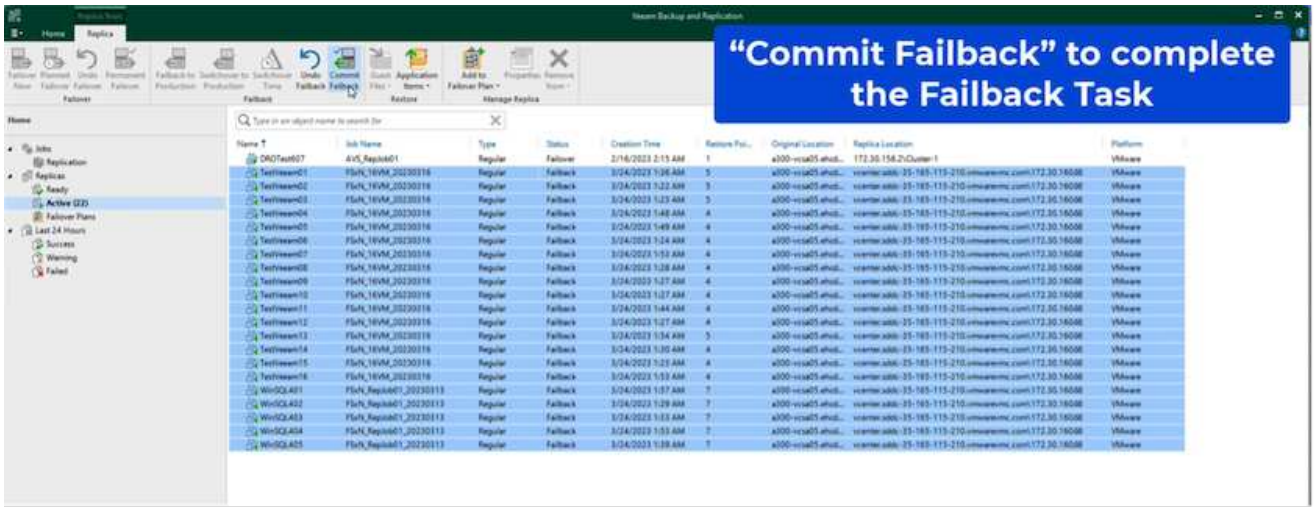
このデモでは、本番環境へのフェイルバックを選択しました。ウィザードの[Destination]ステップで[Failback to the original VM]が選択され、[Power on VM after restoring]チェックボックスが有効になっている。

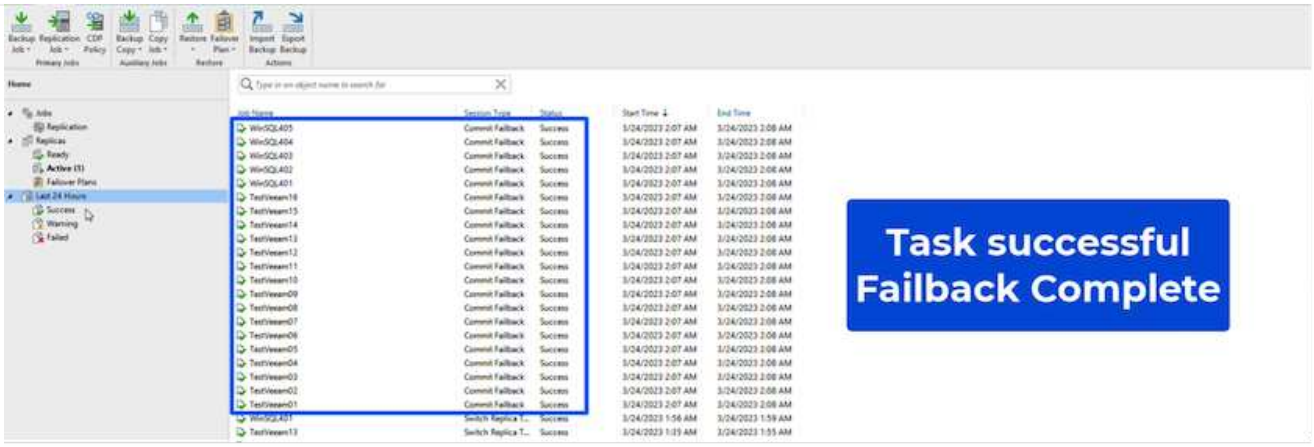




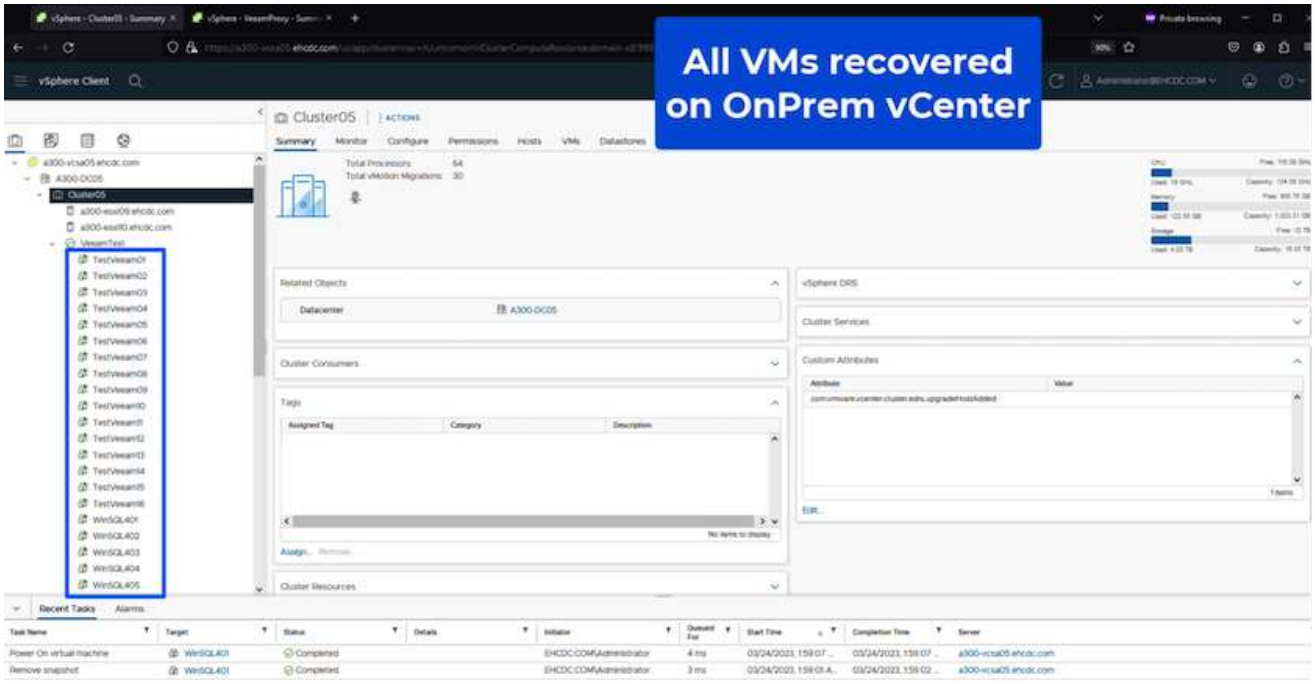
フェイルバックコミットは、フェイルバック操作を完了する方法の1つです。フェイルバックがコミットされると、フェイルバックされたVM（本番VM）に送信された変更が想定どおりに機能していることが確認されます。コミット処理が完了すると、Veeam Backup & Replicationは本番用VMのレプリケーションアクティビティを再開します。

フェイルバックプロセスの詳細については、Veeamのドキュメントを参照してください"レプリケーションのフェイルオーバーとフェイルバック"。





本番環境へのフェイルバックが成功すると、VMはすべて元の本番サイトにリストアされます。



まとめ

FSx ONTAPデータストア機能により、Veeamまたは検証済みの他社製ツールを使用して、VMのレプリカコピーに対応するためだけにクラスタ内の多数のホストを立ち上げることなく、Pilot Lightクラスタを使用して低コストのDRソリューションを提供できます。これにより、カスタマイズされたディザスタリカバリ計画を処理する強力な解決策が提供されます。また、既存のバックアップ製品を社内で再利用してDRのニーズを満たすことができるため、オンプレミスのDRデータセンターを終了することで、クラウドベースのディザスタリカバリを実現できます。フェイルオーバーは、計画的フェイルオーバーまたはフェイルオーバーとして実行でき、災害発生時にボタンをクリックするだけでDRサイトをアクティブ化できます。

このプロセスの詳細については、詳細なウォークスルービデオをご覧ください。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a