



AWS / VMCのワークロードを保護

NetApp Solutions

NetApp
April 10, 2024

目次

AWS / VMCのワークロードを保護	1
TR-4931 : 『Disaster Recovery with VMware Cloud on Amazon Web Services and Guest Connect』	1
Veeam Backup & Restore in VMware Cloud with Amazon FSx for ONTAP	71
TR-4955 : 『Disaster Recovery with FSX for ONTAP and VMC (AWS VMware Cloud) 』	103
Veeam ReplicationとFSx for ONTAPを使用したVMware Cloud on AWSへのディザスタリカバリ	118

AWS / VMCのワークロードを保護

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

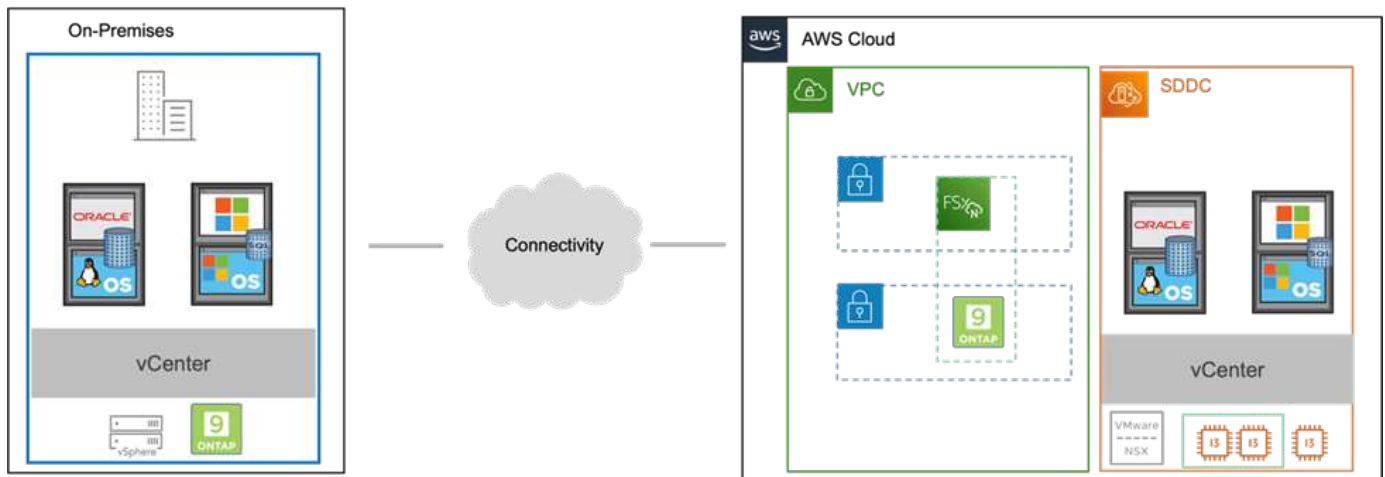
執筆者：Chris Reno、Josh Powell、Suresh Thoppay - NetApp Solutions Engineering

概要

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ーを中心にDRのユースケースを紹介します。

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テクノロジー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。

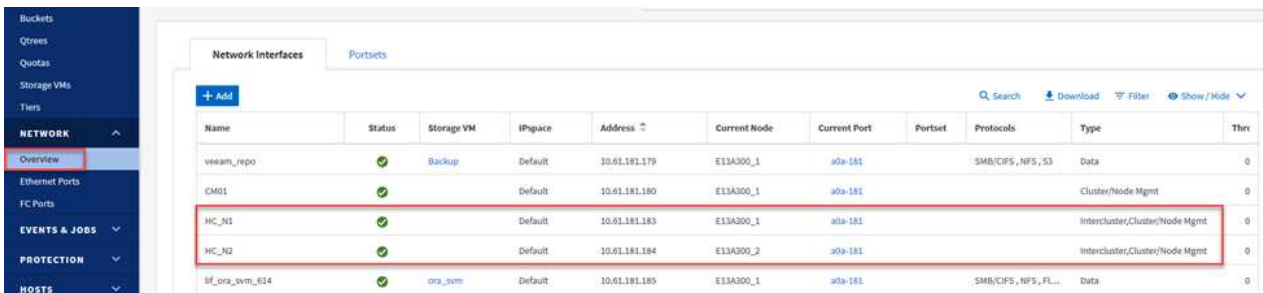


を参照してください "[FSX for ONTAP –ONTAP ユーザーガイド](#)" FSXを使用したSnapMirror関係の作成の詳細については、[を参照してください](#)。

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。



Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Portset	Protocols	Type	Thr
veeam_repo	✓	Backup	Default	10.61.181.179	E13A300_1	a0a-181		SMB/CIFS, NFS, S3	Data	0
CM01	✓		Default	10.61.181.180	E13A300_1	a0a-181			Cluster/Node Mgmt	0
HC_N1	✓		Default	10.61.181.183	E13A300_1	a0a-181			Intercluster/Cluster/Node Mgmt	0
HC_N2	✓		Default	10.61.181.184	E13A300_2	a0a-181			Intercluster/Cluster/Node Mgmt	0
lf_ora_vmm_814	✓	ora_vmm	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL...	Data	0

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
Vserver      Logical      Status      Network      Current      Current      Is
-----      -
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. デスティネーションFSXクラスタ上で' cluster peer create'コマンドを使用してピアリングを設定します。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-addr  
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。

ONTAP System Manager

DASHBOARD

STORAGE

- Overview
- Volumes
- LUNs
- Consistency Groups
- NVMe Namespaces
- Shares
- Buckets
- Qtrees
- Quotas
- Storage VMs
- Tiers

NETWORK

- Overview
- Ethernet Ports
- FC Ports

EVENTS & JOBS

PROTECTION

- Overview
- Relationships

HOSTS

Overview

< Intercluster Settings

Network Interfaces

IP ADDRESS

- ✓ 10.61.181.184
- ✓ 172.21.146.217
- ✓ 10.61.181.183
- ✓ 172.21.146.216

Cluster Peers

PEERED CLUSTER NAME

- ✓ FsxId0ae40e08acc0dea67
- ✓ OTS02

Peer Cluster

Generate Passphrase

Manage Cluster Peers

Mediator ?

Not configured.

Configure

Storage VM Peers

PEERED STORAGE VMS

- ✓ 3

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. [はい]を選択して'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。

Peer Cluster ×

Local
Remote

STORAGE VM PERMISSIONS

All storage VMs (incl... X

Storage VMs created in the future also will be given permissions.

PASSPHRASE ?
👁

●●●●●●●●

It cannot be determined from the passphrase whether this relationship was encrypted. Is the relationship encrypted?

Yes

No

To generate passphrase, Launch Remote Cluster

Intercluster Network Interfaces IP Addresses

172.30.15.42

172.30.14.28

Cancel

+ Add

Initiate Cluster Peering

Cancel

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
```

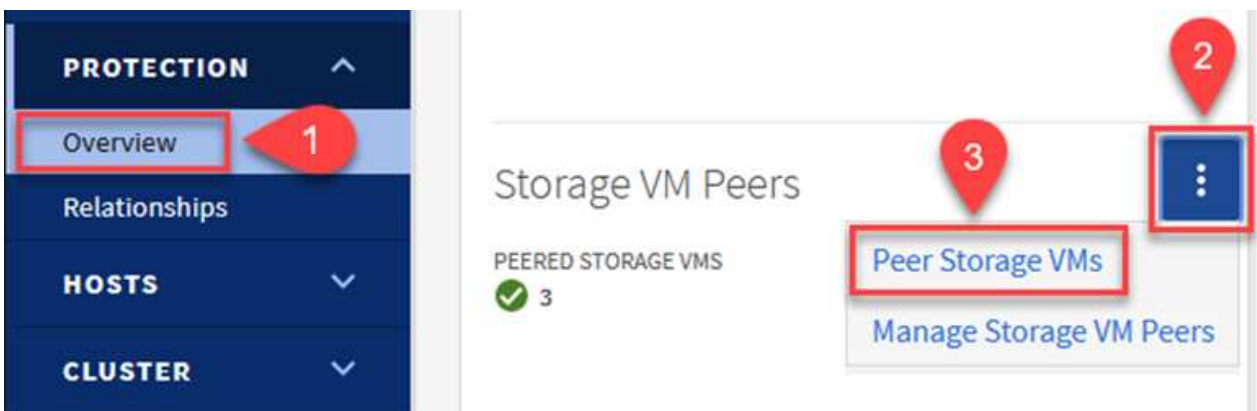

SVMピア関係を確立する

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

Peer Storage VMs



Local

Remote

CLUSTER
E13A300

CLUSTER
FsxId0ae40e08acc0dea67 Refresh

STORAGE VM
Backup

STORAGE VM
svm_HCApps

Peer Storage VMs

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クラスターで作成された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。

Select secondary replication options ⓘ

☐ Update SnapMirror after creating a local Snapshot copy.

☒ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Custom Label ⓘ

sql-daily

Error retry count

3 ⓘ

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クラスター上に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 ソフトウェアはネットアップサポートサイトから入手でき、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、を参照してください "[ネットアップドキュメントセンター](#)"。

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](#)"。

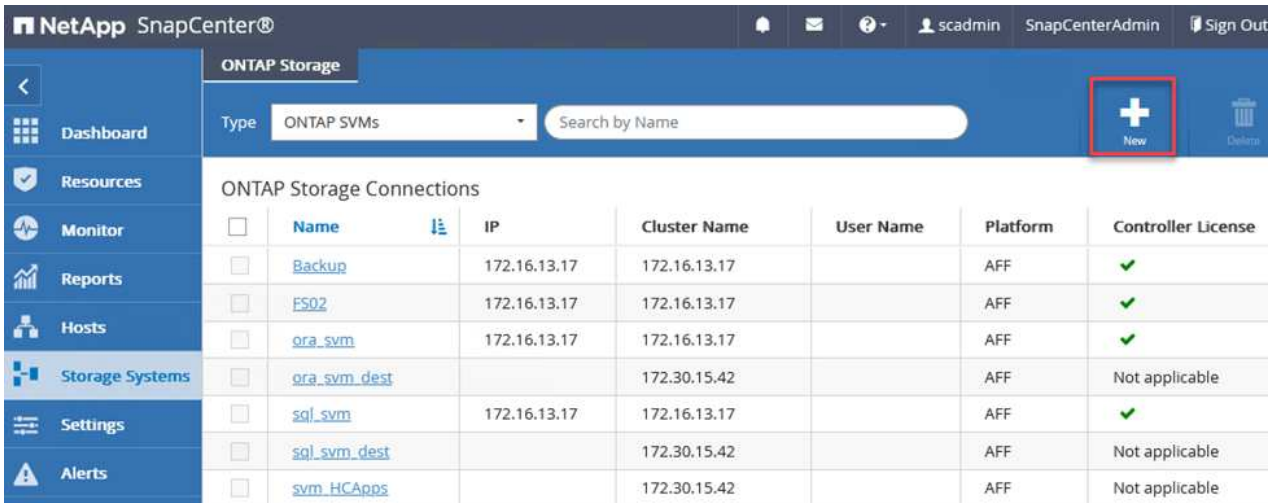
インストール後、\\ https://Virtual_Cluster_IP_or_FQDN:8146_を使用してWebブラウザからSnapCenter コンソールにアクセスできます。

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。



The screenshot shows the NetApp SnapCenter web interface. The left sidebar contains a menu with options: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area is titled 'ONTAP Storage' and includes a 'Type' dropdown set to 'ONTAP SVMs' and a 'Search by Name' input field. A red box highlights the '+ New' button in the top right corner. Below this, there is a table titled 'ONTAP Storage Connections' with columns: Name, IP, Cluster Name, User Name, Platform, and Controller License. The table lists several storage connections, including 'Backup', 'FS02', 'ora_svm', 'ora_svm_dest', 'sql_svm', 'sql_svm_dest', and 'svm_HCApps'.

	Name	IP	Cluster Name	User Name	Platform	Controller License
<input type="checkbox"/>	Backup	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	FS02	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	ora_svm	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	ora_svm_dest		172.30.15.42		AFF	Not applicable
<input type="checkbox"/>	sql_svm	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	sql_svm_dest		172.30.15.42		AFF	Not applicable
<input type="checkbox"/>	svm_HCApps		172.30.15.42		AFF	Not applicable


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 クラスターの管理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。

Add Storage System

Add Storage System

Storage System	<input type="text" value="10.61.181.180"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>

Event Management System (EMS) & AutoSupport Settings

- ☒ Send AutoSupport notification to storage system
- ☒ Log SnapCenter Server events to syslog
-  **More Options** : Platform, Protocol, Preferred IP etc..

- 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。

More Options




Platform FAS

☒ Secondary 

Protocol HTTPS

Port 443

Timeout 60 seconds 

☐ Preferred IP 

Save

Cancel

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"](#)。

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。

NetApp SnapCenter®

Managed Hosts

Search by Name

<input type="checkbox"/>	Name
<input type="checkbox"/>	oraclesrv_01.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_02.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_03.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_04.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_05.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_06.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_07.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_08.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_09.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_10.sddc.netapp.com

Add Host

Host Type: Windows

Host Name: sqlsrv-01.sddc.netapp.com

Credentials: sddc-jpowell

Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Windows

- ☒ Microsoft Windows
- ☒ Microsoft SQL Server
- ☐ Microsoft Exchange Server
- ☐ SAP HANA

[More Options](#) : Port, gMSA, Install Path, Custom Plug-Ins...

Submit **Cancel**

3. Oracleの場合は、[Add Host]ダイアログボックスの必須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オンにします。次に、Submit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...

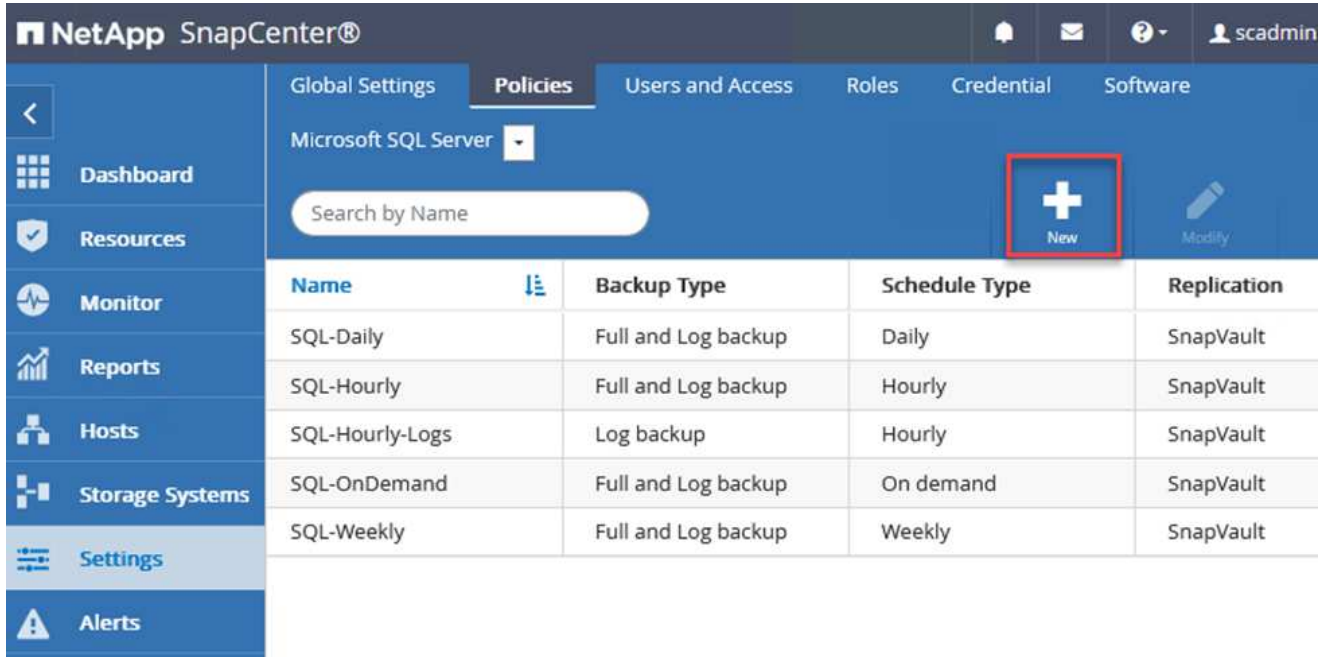
Submit

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。



Name	Backup Type	Schedule Type	Replication
SQL-Daily	Full and Log backup	Daily	SnapVault
SQL-Hourly	Full and Log backup	Hourly	SnapVault
SQL-Hourly-Logs	Log backup	Hourly	SnapVault
SQL-OnDemand	Full and Log backup	On demand	SnapVault
SQL-Weekly	Full and Log backup	Weekly	SnapVault

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

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

- 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。
- 「ローカルSnapshotコピーの作成後にSnapVault を更新」設定は、2つの別々のクラスタ間、およびオンプレミスのONTAP システムとCloud Volumes ONTAP またはFSxNとの間に存在する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。

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

Select secondary replication options ⓘ

☐ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Choose

Error retry count

3

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。

Name	Resource Count	Tags	Policies	Last Backup	Overall Status
SQLSRV-01	1		SQL-Daily SQL-Hourly SQL-OnDemand SQL-Weekly	05/11/2022 ...	Completed
SQLSRV-02	1		SQL-Daily SQL-Hourly SQL-OnDemand SQL-Weekly	03/28/2022 ...	Failed
SQLSRV-03	1		SQL-Daily SQL-Hourly	05/11/2022 ...	Completed

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、を参照してください ["リンクをクリックしてください"](#)。

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

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、を参照してください "[Veeamヘルプセンターのテクニカルドキュメント](#)"。

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。

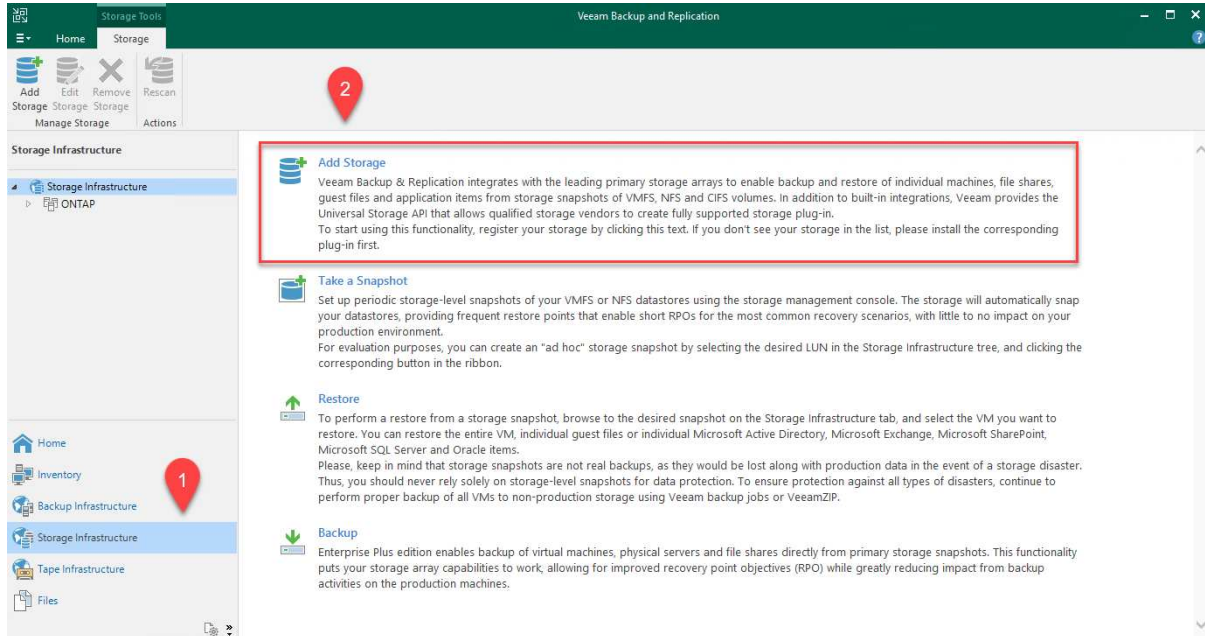
作業を開始する前に、次の前提条件を確認してください。

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。ストレージインフラに移動し、ストレージの追加を選択します。



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。次へをクリックします。

New NetApp Data ONTAP Storage



Name

Register NetApp Data ONTAP storage by specifying DNS name or IP address.

Name	Management server DNS name or IP address: <input type="text" value="10.61.181.180"/>
Credentials	Description: <input type="text" value="Created by SDDC\jpowell at 5/17/2022 10:34 AM."/>
NAS Filer	Role: <input type="checkbox"/> Block or file storage for VMware vSphere <input type="checkbox"/> Block storage for Microsoft Windows servers <input checked="" type="checkbox"/> NAS filer
Apply	
Summary	

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。

New NetApp Data ONTAP Storage



Credentials

Specify account with storage administrator privileges.

Name	Credentials: <input type="text" value="HCIEUC\Admin (HCIEUC\Admin, last edited: 98 days ago)"/>	<input type="button" value="Add..."/>
Credentials	Manage accounts	
NAS Filer	Protocol: <input type="text" value="HTTPS"/>	
Apply	Port: <input type="text" value="443"/>	
Summary		

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。

New NetApp Data ONTAP Storage ✕

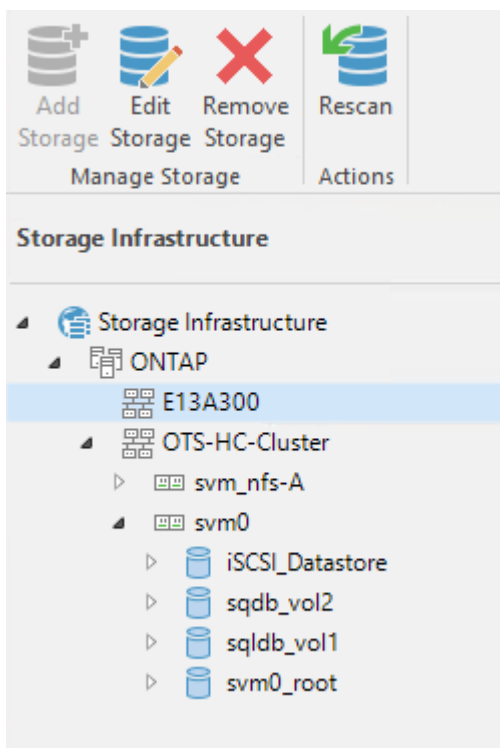
NAS Filer

Specify how this storage can be accessed by file backup jobs.

Name	Protocol to use:
Credentials	<input checked="" type="checkbox"/> SMB
NAS Filer	<input type="checkbox"/> NFS
Apply	<input checked="" type="checkbox"/> Create required export rules automatically
Summary	Volumes to scan:
	<input type="text" value="All volumes"/> Choose...
	Backup proxies to use:
	<input type="text" value="Automatic selection"/> Choose...

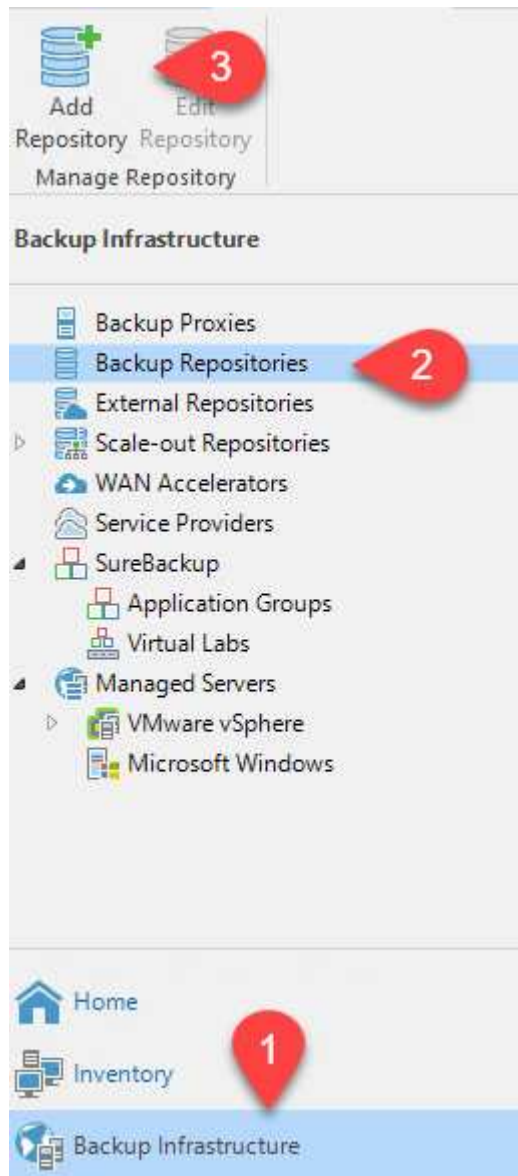
< Previous
Apply
Finish
Cancel

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

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バックアップリポジトリの作成の詳細については、を参照してください "[Veeamの製品ドキュメント](#)"。

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

Shared folder:

Share

Use \\server\folder format

Repository

☒ This share requires access credentials:

sddc\administrator (sddc\administrator, last edited: 85 days ago)



Mount Server

[Manage accounts](#)

Review

Gateway server:

☒ Automatic selection☐ The following server:

Apply

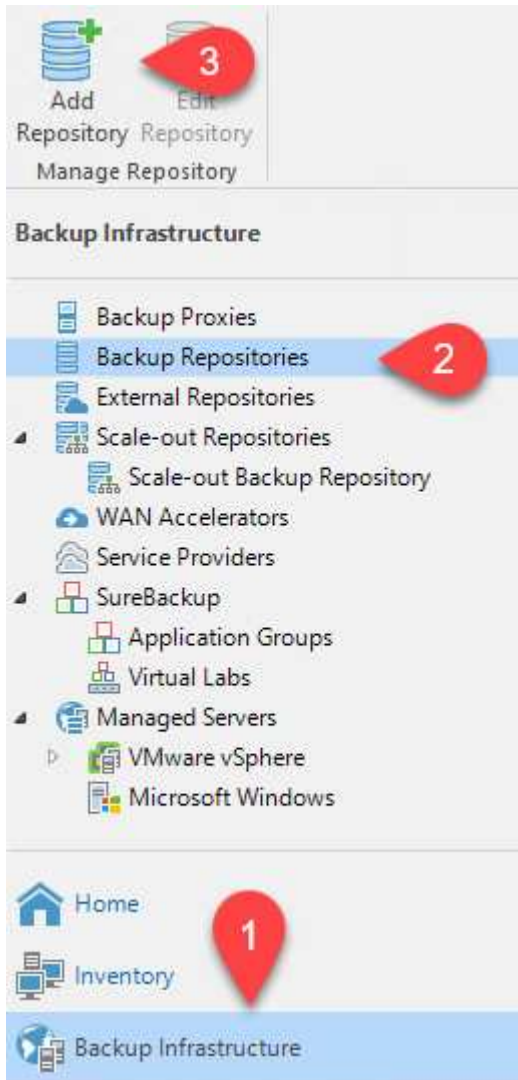
Use this option to improve performance and reliability of backup to a NAS located in a remote site.

Summary

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。

Add Backup Repository

Select the type of backup repository you want to add.



Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.



Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.



Deduplicating storage appliance

Dell EMC Data Domain, ExaGrid, HPE StoreOnce or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.



Object storage

On-prem object storage system or a cloud object storage provider. Object storage can only be used as a Capacity Tier of scale-out backup repositories, backing up directly to object storage is not currently supported.

- 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。
- 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。

New Object Storage Repository



Account

Specify AWS account to use for connecting to Amazon S3 storage bucket.

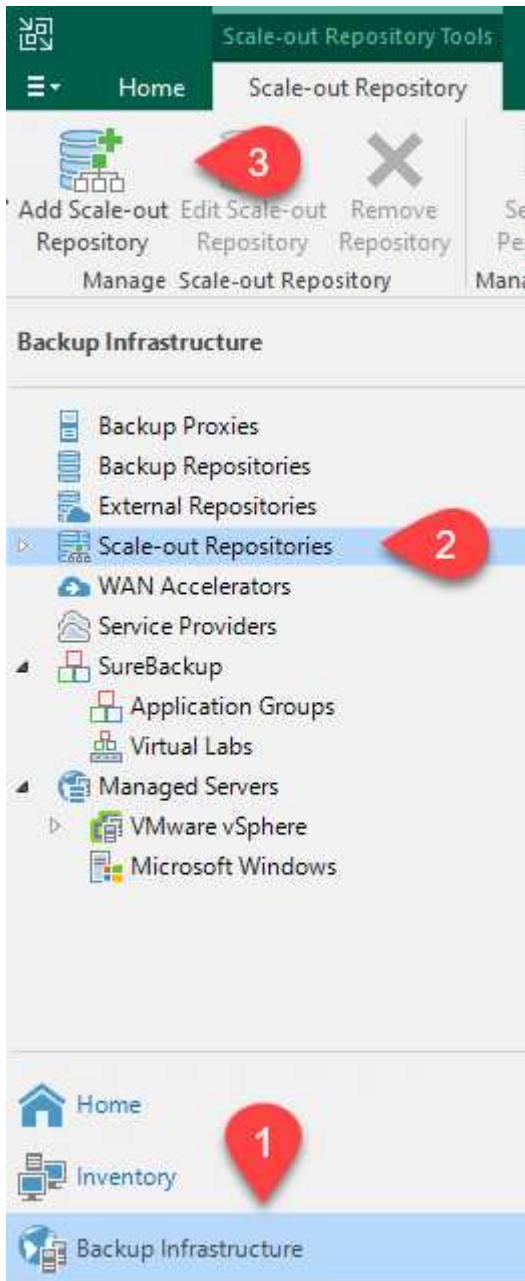
Name	Credentials:
Account	<input type="text" value="AKIAH4H43ZT557HXQT2W (last edited: 107 days ago)"/> Add...
Bucket	Manage cloud accounts
Summary	AWS region:
	<input type="text" value="Global"/>
	<input type="checkbox"/> Use the following gateway server:
	<input type="text" value="veeam.sddc.netapp.com (Backup server)"/>
	Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.
<input type="button" value=" < Previous"/> <input type="button" value=" Next > "/>	
<input type="button" value=" Finish "/>	
<input type="button" value=" Cancel "/>	

- 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。

New Scale-out Backup Repository ×

Performance Tier
Select backup repositories to use as the landing zone and for the short-term retention.




Name	Extents:				
Performance Tier	<table border="1"> <thead> <tr> <th>Name</th> <th></th> </tr> </thead> <tbody> <tr> <td>VBRRepo2</td> <td></td> </tr> </tbody> </table>	Name		VBRRepo2	
Name					
VBRRepo2					
Placement Policy					

Add...
Remove

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。

New Scale-out Backup Repository ×

Capacity Tier
Specify object storage to copy backups to for redundancy and DR purposes. Older backups can be moved to object storage completely to reduce long-term retention costs while preserving the ability to restore directly from offloaded backups.



Name	
Performance Tier	
Placement Policy	
Capacity Tier	<input checked="" type="checkbox"/> Extend scale-out backup repository capacity with object storage: <div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between;"> Amazon S3 Repo ▼ Add... </div> <div style="text-align: right; margin-top: 5px;">Window...</div>
Archive Tier	
Summary	

☒ Copy backups to object storage as soon as they are created
 Create additional copy of your backups for added redundancy by having all backups copied to the capacity tier as soon as they are created on the performance tier.

☒ Move backups to object storage as they age out of the operational restore window
 Reduce your long-term retention costs by moving older backups to object storage completely while preserving the ability to restore directly from offloaded backups.
 Move backup files older than 14 days (your operational restore window) Override...

☐ Encrypt data uploaded to object storage
 Password: Add...
Manage passwords

< Previous Next > Finish Cancel

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、を参照してください ["Veeam Help Centerテクニカルドキュメント"](#)。

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 ソフトウェアはネットアップサポートサイトから入手でき、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、を参照してください ["ネットアップドキュメントセンター"](#)。

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"](#)。

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。

これらの手順の実行方法の詳細については、「～」の項を参照してください ["SnapCenter データベースのリストアプロセス"](#)。

セカンダリVeeam Backup & Replicationサーバを導入します

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。実装の詳細なガイダンスについては、を参照してください ["Veeam Help Centerテクニカルドキュメント"](#)。

セカンダリVeeam Backup & Replicationサーバを設定します

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、を参照してください ["アプリケーションVMをVeeam Full Restoreでリストアします"](#)。

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。この手順の詳細については、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 経由での 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/](https://<SnapCenterサーバIP>:8146/swagger/)) にアクセスします。



SnapCenter API

[Base URL: /api]

<https://snapcenter.sddc.netapp.com:8146/Content/swagger/SnapCenter.yaml>

Manage your SnapCenter Server using the SnapCenter API.
To access the swagger documentation of "SnapCenter Plug-in for VMware vSphere" API's, please use
https://{SCV_hostname}:{SCV_host_port}/api/swagger-ui.html

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

Auth

POST

/4.6/auth/login Service login

The login endpoint exposes the method required to log in to the SnapCenter service. The login method returns a token that is used to authenticate subsequent requests.

Parameters

Try it out

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。

Name	Description
TokenNeverExpires	Token never expires
boolean (query)	<div>false</div>
UserOperationContext * required	User credentials
object (body)	<div>Edit Value Model</div> <pre>{ "UserOperationContext": { "User": { "Name": "localhost\\scadmin", "Passphrase": "NetApp321", "Rolename": "SnapCenterAdmin" } } }</pre> <div>Cancel</div> <div>Parameter content type</div> <div>application/json</div> <div>Execute</div>

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。

200

Response body


```
{
  "PluginName": null,
  "HostId": 0,
  "RoleId": null,
  "JobIds": null
},
{
  "User": {
    "Token":
    "KlYxOg==tsV6EOdttdAmAYpe8q5SG6wcoGaSjwME6jrNy5CsY63HQJ5LkoZLIESRNAhpGJJ0UQUynEHdgtVGDZnvx+I/ZJZIn5M1NZrj6
    CLfGTApplGmcagT08bqb5hMfx07EcdRAidzAXUDb3GyLOKtW0GdwKzSe0wKj3uVupnk1E31skK6PRBv9RS8j0qHQvo4v4RL0hhThhwPhV
    9/23nFeJVP/plEv4vrV/ze2VTUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjq=",
    "Name": "SCAdmin",
    "TokenBashed": null,
    "Type": "",
    "TokenTime": "2022-03-22T14:21:57.3665661-07:00",
    "Id": "1",
    "FullName": "SCAdmin",
    "Host": null,
    "Author": null,
    "UserName": "",
    "Domain": "",
    "Passphrase": ""
  }
}
```

Download

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。

Disaster Recovery 

GET

/4.6/disasterrecovery/server/backup

Fetch all the existing SnapCenter Server DR Backups.

POST

/4.6/disasterrecovery/server/backup

Starts the SnapCenter Server DR backup.

DELETE

/4.6/disasterrecovery/server/backup

Deletes the existing Snapcenter DR backup.

POST

/4.6/disasterrecovery/server/restore

Starts SnapCenter Server Restore.

POST

/4.6/disasterrecovery/storage

Enable or disable the storage disaster recovery.

2. 「/4.6/disasterrecovery/sa/backup」セクションを展開し、「試してみてください」をクリックします。

POST

/4.6/disasterrecovery/server/backup

Starts the SnapCenter Server DR backup.

Starts and creates a new SnapCenter Server DR backup.

Parameters

Try it out

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 <div>TUHFHUM069XRe5cuW9nwyj4b0l5Y5FN3XDkjQ==</div>
SmDRBackupRequest * required object (body)	Parameters to take Backup <div><div>Edit Value Model</div><div><pre>{ "TargetPath": "C:\\\\SnapCenter_Backups\\\\" }</pre></div></div> <div>Cancel</div> <div>Parameter content type application/json</div>

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ップ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。

Job Details

SnapCenter Server disaster recovery backup

- ✓ ▾ SnapCenter Server disaster recovery backup
 - ✓ ▶ Precheck validation
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_04.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of SnapCenter Server 'SnapCenter.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_02.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_03.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_05.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_07.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-02.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-03.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_10.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-04.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-01.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-05.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_09.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-06.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-07.sddc.netapp.com'

📌 Task Name: SnapCenter Server disaster recovery backup Start Time: 03/23/2022 10:27:11 AM End Time: 03/23/2022 10:27:47 AM

[View Logs](#)[Cancel Job](#)[Close](#)

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

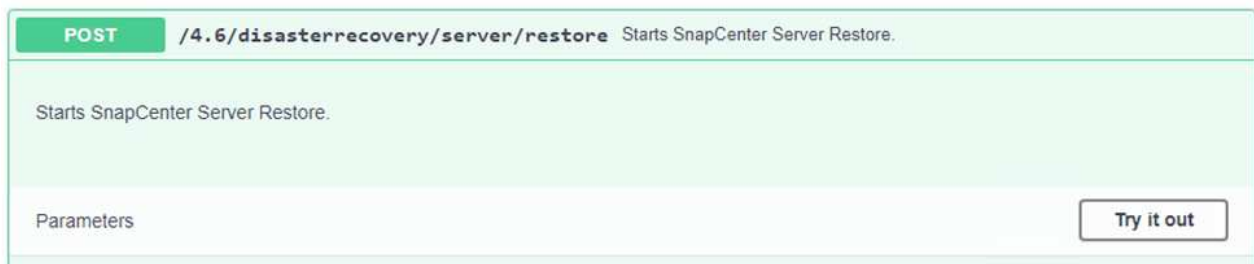
SnapCenter では、MySQLデータベースおよび構成ファイルのバックアップとリストアが可能なため、ディザスタリカバリのシナリオがサポートされます。これにより、管理者はSnapCenter データベースの定期的なバックアップをオンプレミスのデータセンターで保持し、そのデータベースをセカンダリSnapCenter データベースにリストアすることができます。

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、[0/4.6/disasterrecovery/sa/restore]を選択して、[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。

Name	Description
Token * required string (header)	User authorization token <div>KIYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQl</div>
SmDRRestoreRequest * required object (body)	Parameters to take for Restore <div> Edit Value Model <pre>{ "BackupName": "SnapCenter.sddc.netapp.com_03-23-2022_12.38.00.6713", "BackupPath": "C:\\\\SnapCenter\\" }</pre> </div>

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。

NetApp SnapCenter®			
<div><</div> <div>Dashboard</div> <div>Resources</div> <div>Monitor</div> <div>Reports</div> <div>Hosts</div> <div>Storage Systems</div> <div>Settings</div> <div>Alerts</div>	Jobs Schedules Events Logs		
	search by name		
	Jobs - Filter		
	ID	Status	Name
	20482	✓	SnapCenter Server Disaster Recovery
	20481	✓	SnapCenter Server disaster recovery backup
	20480	✗	SnapCenter Server disaster recovery backup
	20475	✓	Backup of Resource Group 'SQLSRV-09' with policy 'SQL-Hourly'
	20474	✓	Backup of Resource Group 'SQLSRV-05' with policy 'SQL-Hourly'
	20473	🔄	Backup of Resource Group 'OracleSrv_06' with policy 'Oracle-Hourly'
	20472	✗	SnapCenter Server disaster recovery backup

Job Details

SnapCenter Server Disaster Recovery

- ✓ ▼ SnapCenter Server Disaster Recovery
- ✓ ▼ Prepare for restore job
- ✓ ▼ Precheck validation
- ✓ ▼ Saving original server state
- ✓ ▼ Schedule restore
- ✓ ▼ Repository restore
- ✓ ▼ Config restore
- ✓ ▼ Reset MySQL password

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'[4.6/disasterrecovery/storage]'をクリックします
 - 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'EnableDisasterRecover'を'true'に変更します
 - 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

Name	Description
Token * required string (header)	User authorization token <div>KIYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQt</div>
SmSetDisasterRecoverySettingsRequest * required object (body)	Parameters to enable or disable the DR mode <div>Edit Value Model { "EnableDisasterRecovery": true }</div>



追加手順に関するコメントを参照してください。

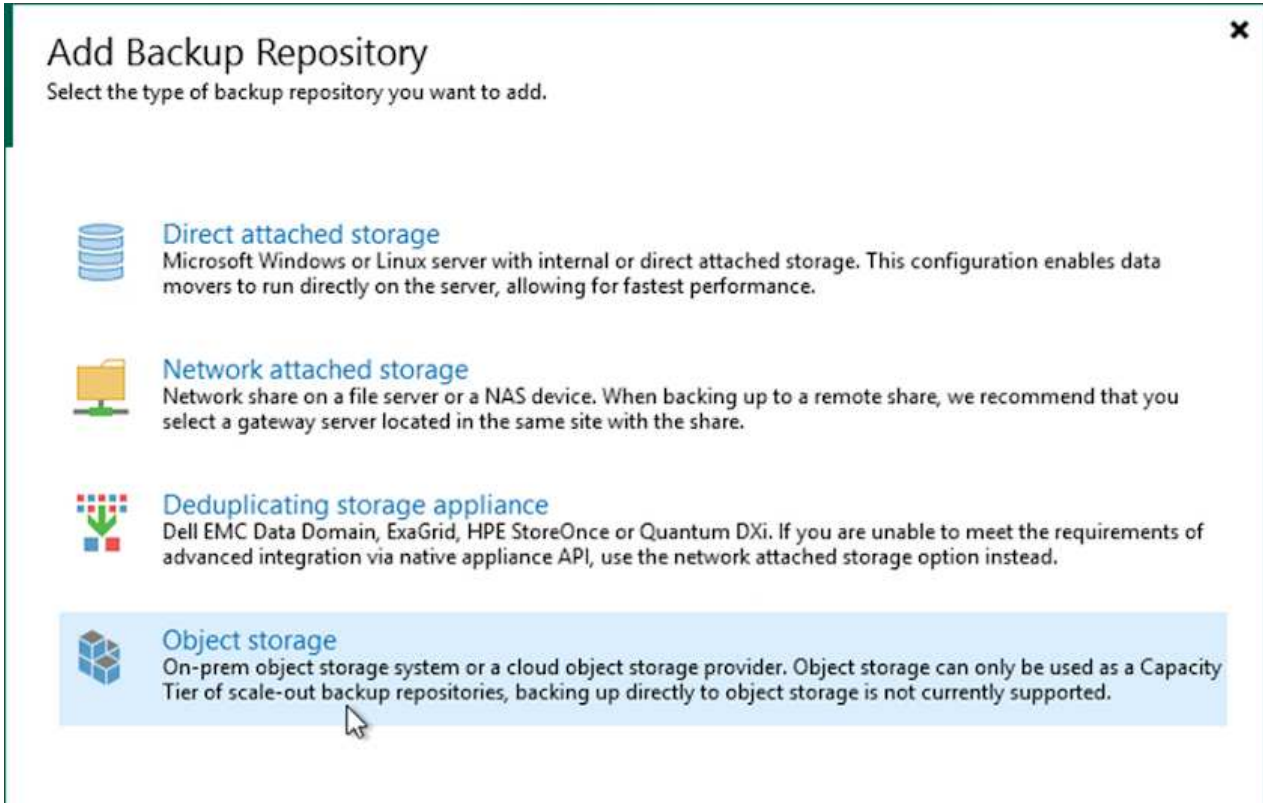
Veeamフルリストアを使用してアプリケーション**VM**をリストアする

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。





Object Storage


Select the type of object storage you want to use as a backup repository.

**S3 Compatible**
Adds an on-premises object storage system or a cloud object storage provider.


**Amazon S3**
Adds Amazon cloud object storage. Amazon S3, Amazon S3 Glacier (including Deep Archive) and Amazon Snowball Edge are supported.

**Google Cloud Storage**
Adds Google Cloud storage. Both Standard and Nearline storage classes are supported.

**IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.


**Microsoft Azure Storage**
Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage, Microsoft Azure Archive Storage and Microsoft Azure Data Box are supported.


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




Amazon Cloud Storage Services

Select the type of Amazon storage you want to use as a backup repository.


**Amazon S3**
Adds Amazon S3 storage. Both Standard and Infrequent Access (IA) storage classes are supported.


**Amazon S3 Glacier**
Adds Amazon S3 Glacier storage. Both Amazon S3 Glacier and Glacier Deep Archive are supported.

**AWS Snowball Edge**
Adds AWS Snowball Edge appliance to enable seeding of backups into Amazon S3 object storage.

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。

New Object Storage Repository ×


 **Account**
Specify AWS account to use for connecting to Amazon S3 storage bucket.

Name	Credentials:
Account	 AKIAH43ZT53YJXPY2Y (last edited: 33 days ago) ▼ Add...
Bucket	Manage cloud accounts
Summary	AWS region: Global ▼
	<input type="checkbox"/> Use the following gateway server: EC2AMAZ-3POTKQV (Backup server) ▼ <small>Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.</small>

< Previous Next > Finish Cancel

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。

New Object Storage Repository

 **Bucket**
Specify Amazon S3 bucket to use.

Name	Data center: US East (N. Virginia)
Account	
Bucket	ehcveeamrepo Browse...
Summary	Folder: RTP Browse...

☐ Limit object storage consumption to: 10 TB
This is a soft limit to help control your object storage spend. If the specified limit is exceeded, already running backup offload tasks will be allowed to complete, but no new tasks will be started.

☐ Make recent backups immutable for: 30 days
Protects backups from modification or deletion by ransomware, hackers or malicious insiders using native object storage capabilities.

☐ Use infrequent access storage class (may result in higher costs)
With lower price per GB but higher retrieval and early deletion fees, this storage class is best suited for long-term storage of GFS full backups. Avoid using it for short-term storage of recent backups.

☐ Store backups in a single availability zone (even lower price per GB, reduced resilience)

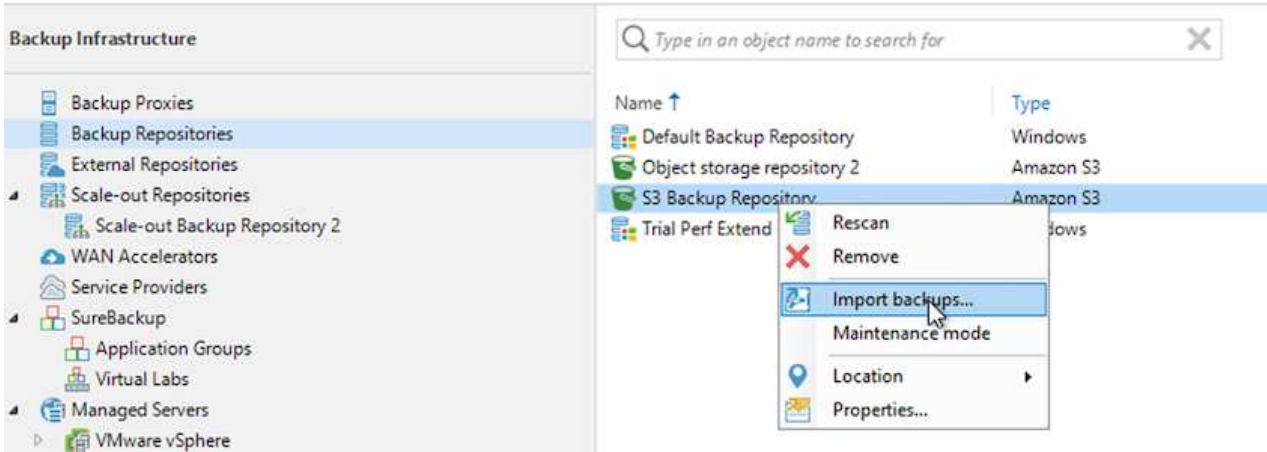
< Previous **Apply** Finish Cancel

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

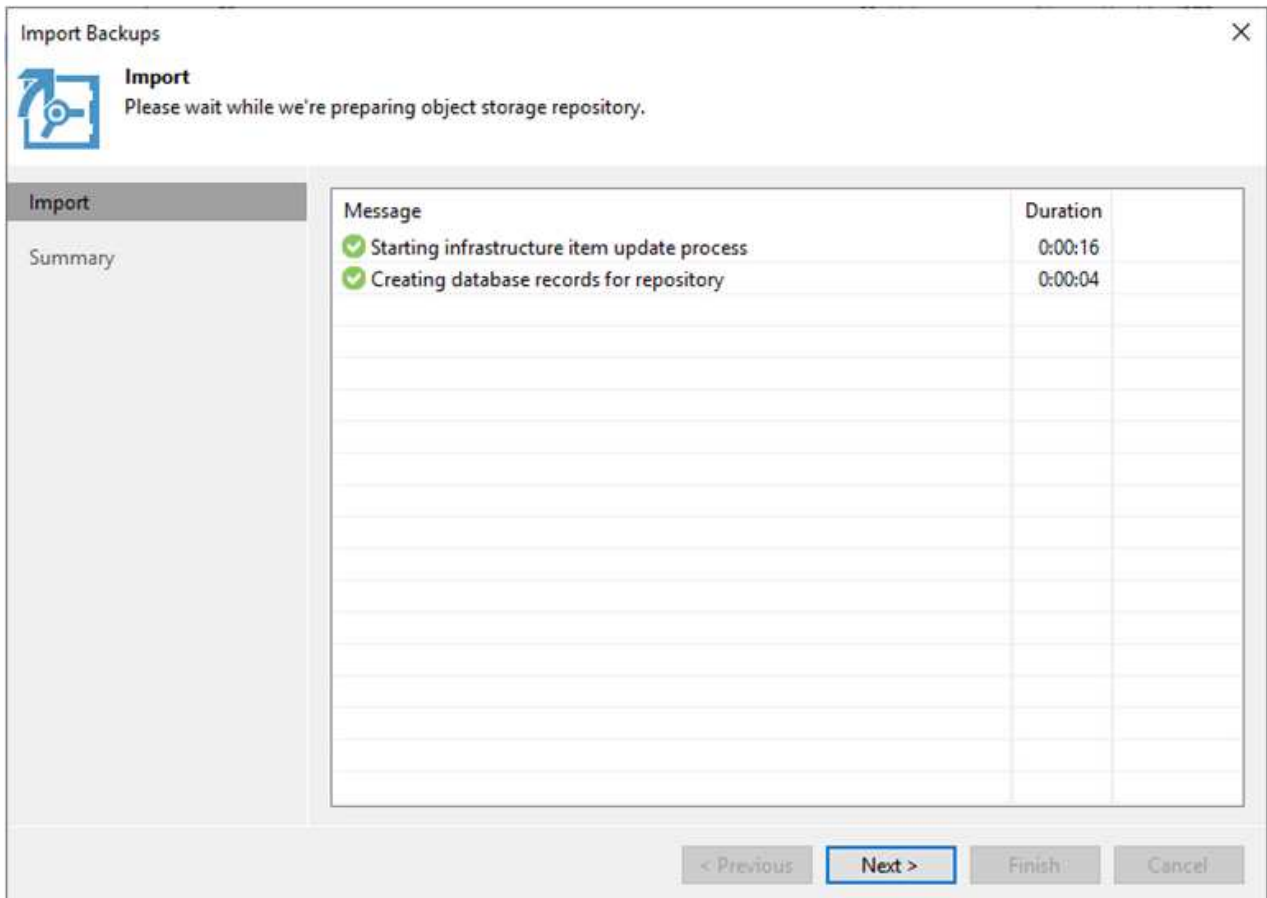
S3オブジェクトストレージからバックアップをインポートする

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\vdadmin End time: 4/6/2022 3:04:57 PM

Log

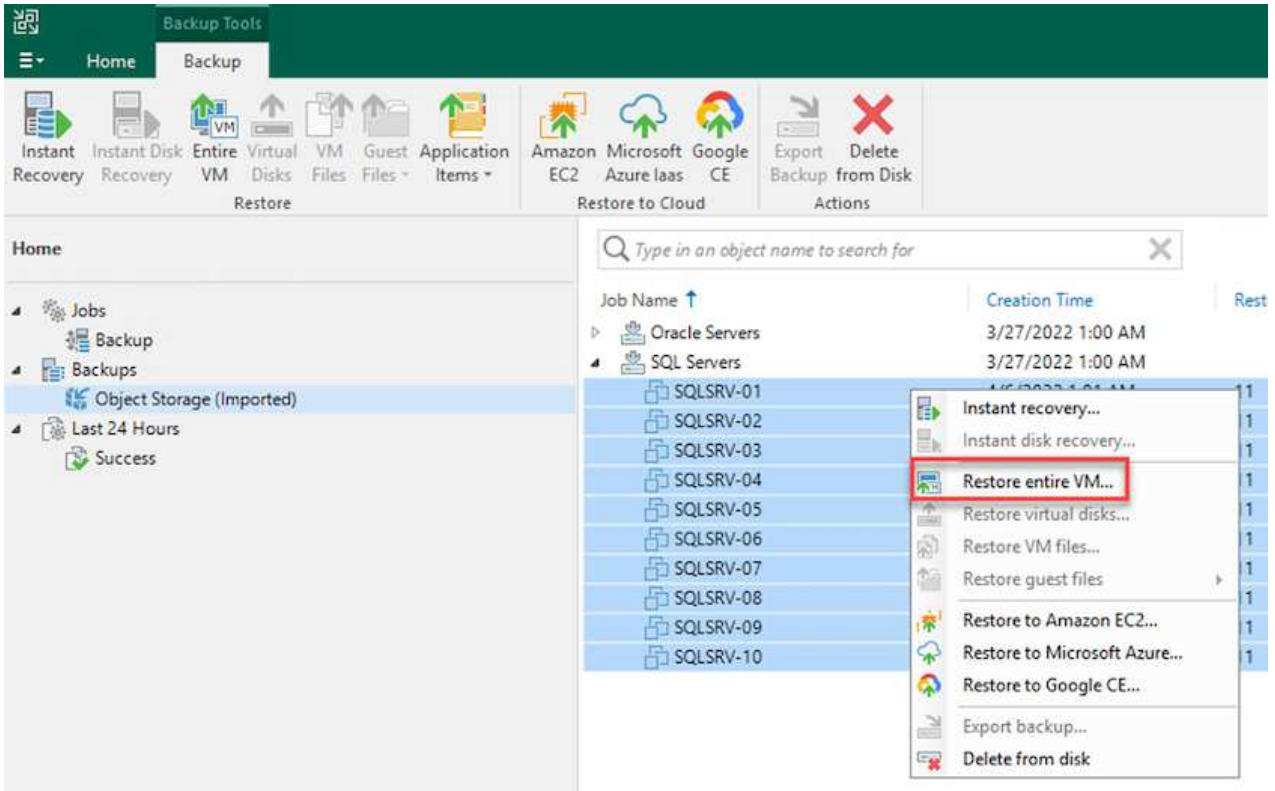
Message	Duration
✓ Starting backup repositories synchronization	
✓ Enumerating repositories	
✓ Found 1 repository	
✓ Processing capacity tier extent of S3 Backup Repository 2	0:03:23
✓ S3 Backup Repository: added 2 unencrypted	0:03:20
✓ Importing backup 2 out of 2	0:03:15
✓ Backup repositories synchronization completed successfully	

Close

Veeamを使用して、アプリケーションVMをVMware Cloudにリストアし

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。



Select virtual machines to be restored. You can add individual virtual machines from backup files, or containers from live environment (containers will be automatically expanded into plain VM list).

Summary

 Type in a VM name for instant lookup


[illegible]

Add...

Next >

Cancel

Full VM Restore

 **Restore Mode**
Specify whether selected VMs should be restored back to the original location, or to a new location or with different settings.

Virtual Machines

Restore Mode

Host

Resource Pool

Datastore

Folder

Network

Secure Restore

Summary

☐ **Restore to the original location**
Quickly initiate the restore of selected VM to its original location, with the original name and settings. This option minimizes the chance of user input error.

☒ **Restore to a new location, or with different settings**
Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults.

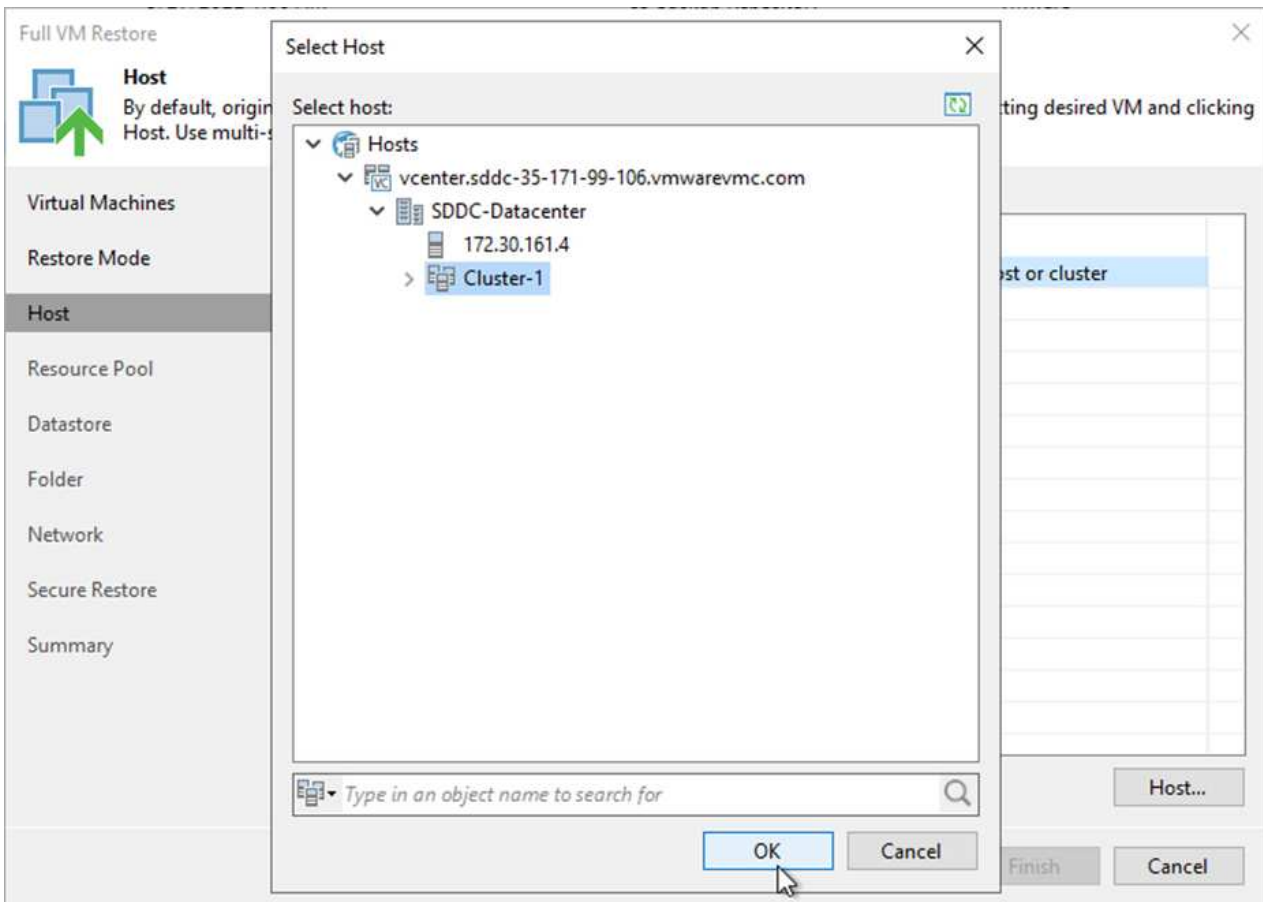
☐ **Staged restore**
Run the selected VM directly from backup files in the isolated DataLab to make changes to the guest OS or applications prior to placing the VM into production environment.

[Pick proxy to use](#)

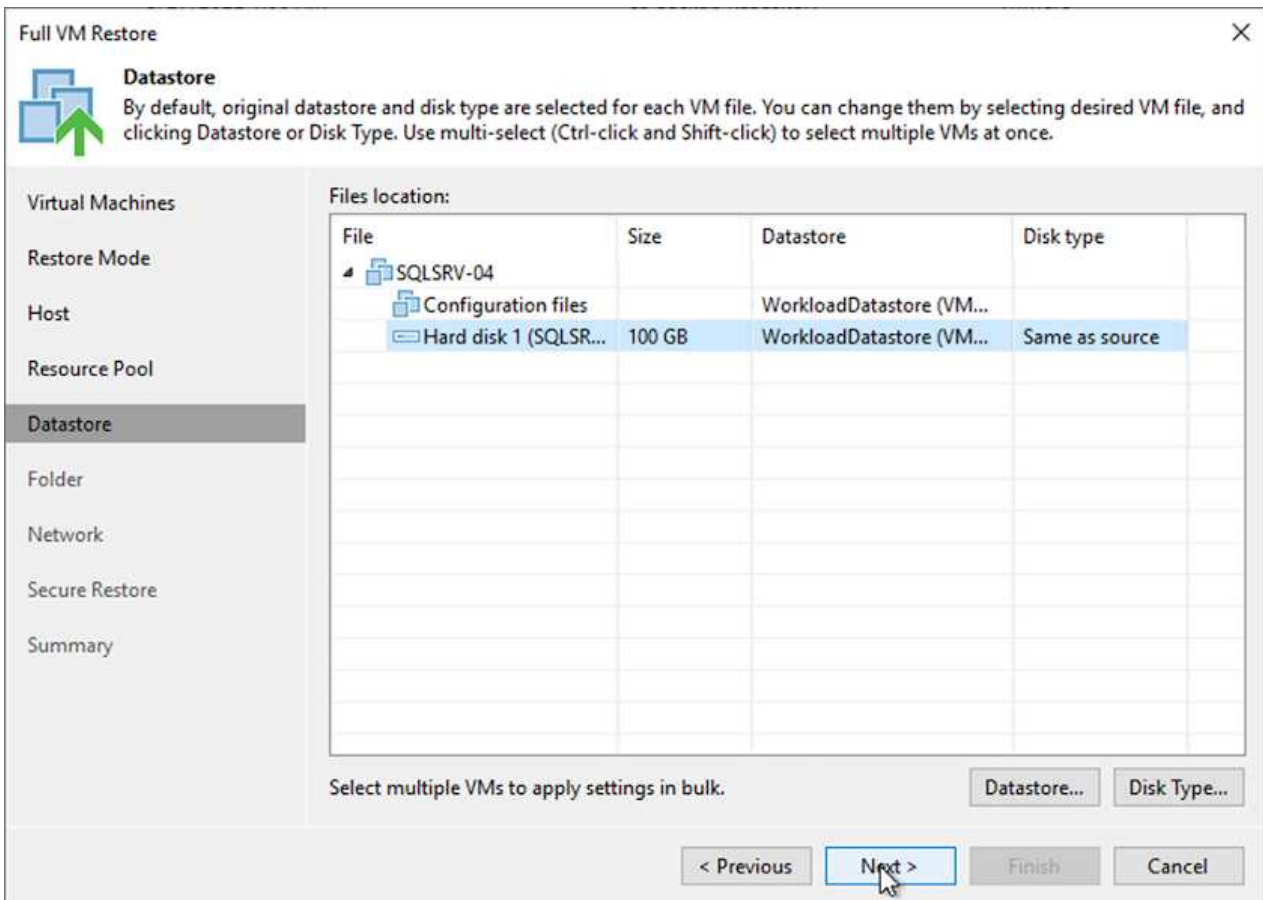
☐ **Quick rollback (restore changed blocks only)**
Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

< Previous **Next >** Finish Cancel

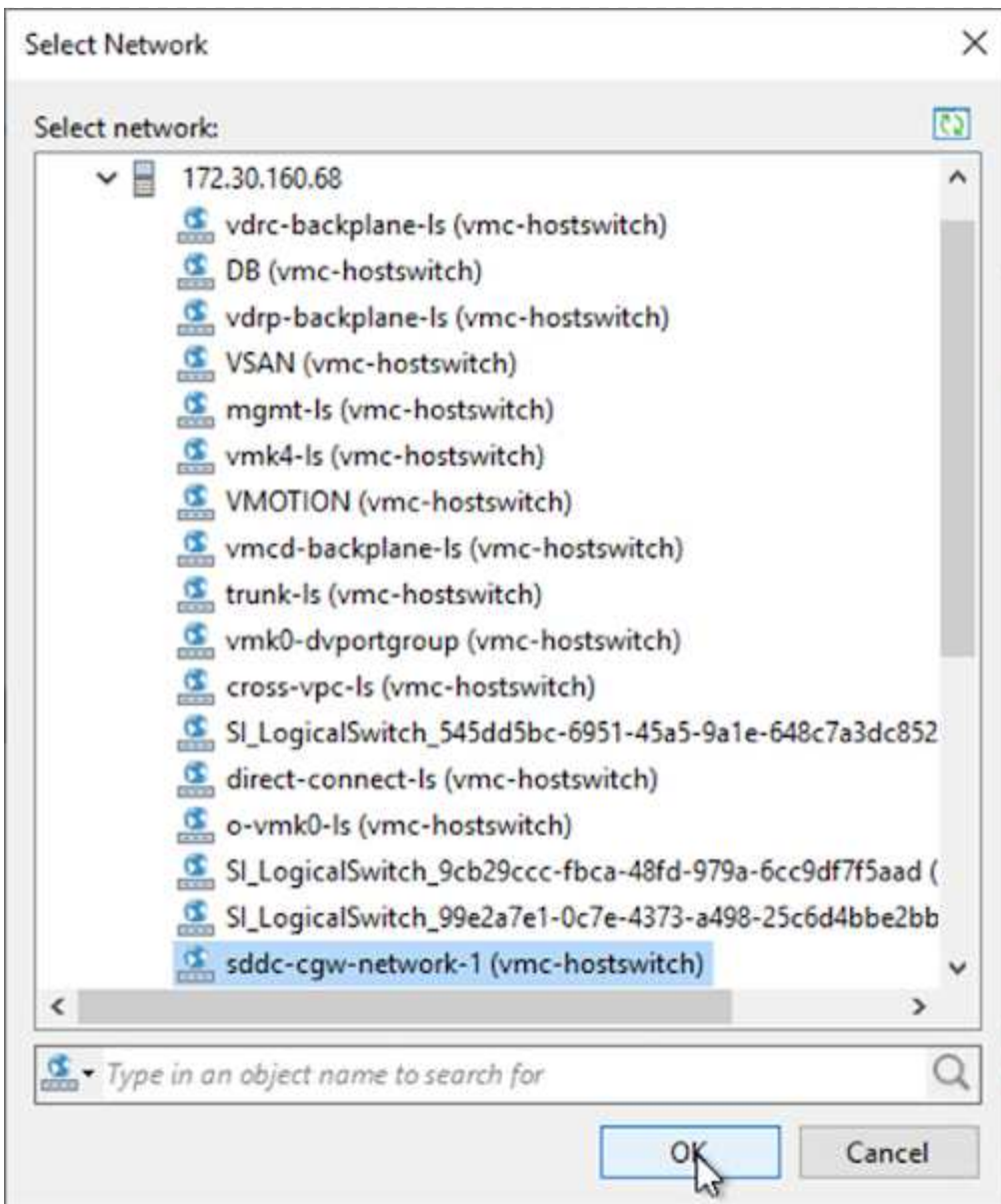
4. ホストページで、VMのリストア先となるターゲットESXiホストまたはクラスタを選択します。



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。



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. セカンダリSnapCenter サーバが確立され、セクションで説明する手順に従って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. パス名を検索するには'lun showコマンドを実行します

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。

Endpoints

Management DNS name

svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com

NFS DNS name

svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com

iSCSI DNS name

iscsi.svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com

Management IP address

198.19.254.53

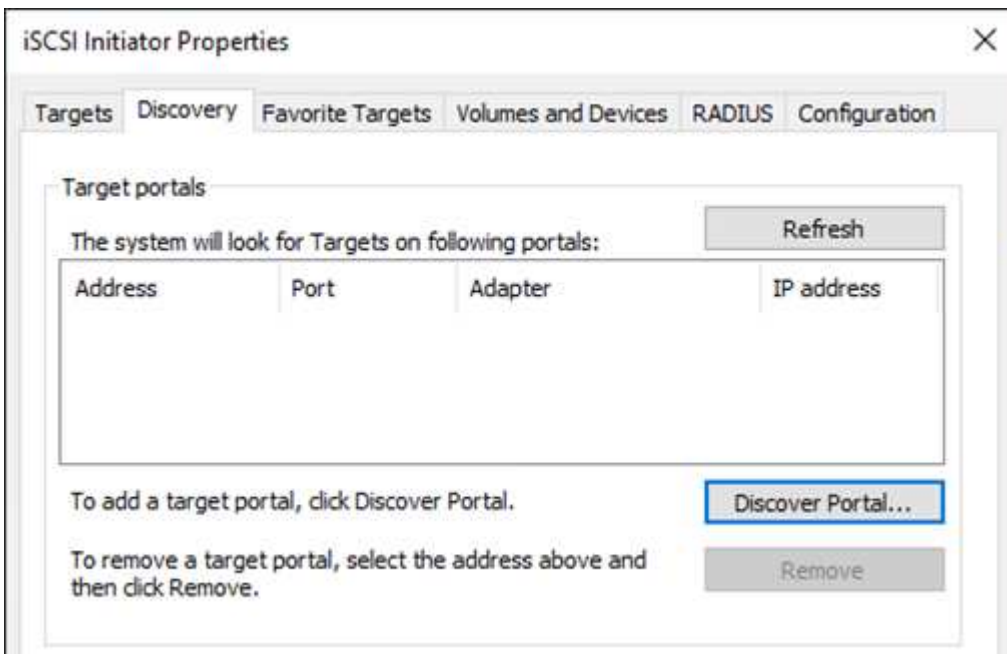
NFS IP address

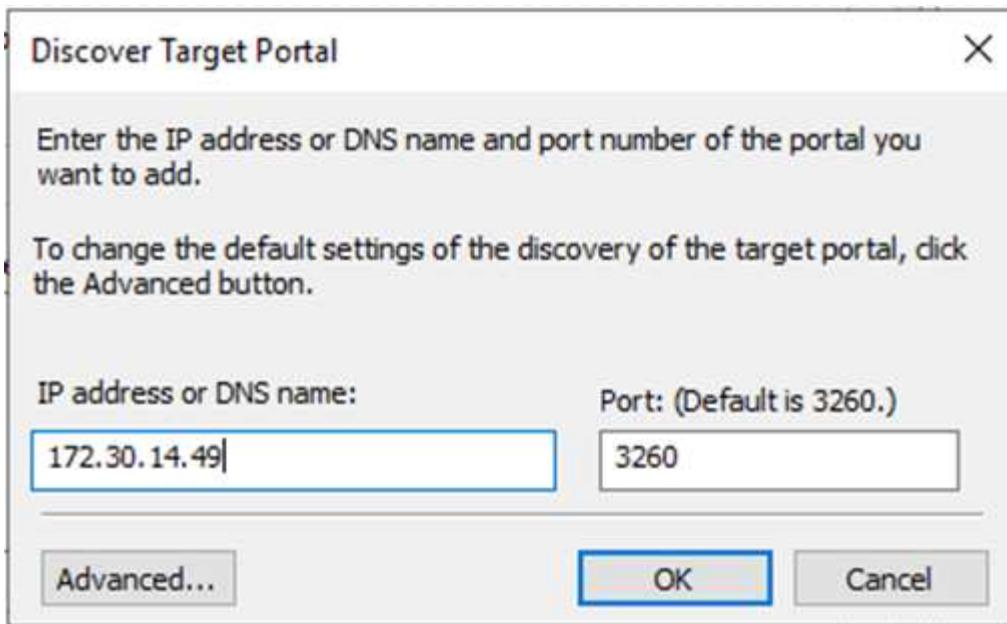
198.19.254.53

iSCSI IP addresses

172.30.15.101, 172.30.14.49

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。





The image shows a 'Discover Target Portal' dialog box. It has a title bar with a close button (X). The main area contains two paragraphs of text: 'Enter the IP address or DNS name and port number of the portal you want to add.' and 'To change the default settings of the discovery of the target portal, click the Advanced button.' Below the text are two input fields. The first is labeled 'IP address or DNS name:' and contains the text '172.30.14.49'. The second is labeled 'Port: (Default is 3260.)' and contains the text '3260'. At the bottom of the dialog are three buttons: 'Advanced...', 'OK', and 'Cancel'. The 'OK' button is highlighted with a blue border.

Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: 172.30.14.49

Port: (Default is 3260.) 3260

Advanced... OK Cancel

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。

iSCSI Initiator Properties

Targets Discovery Favorite Targets Volumes and Devices RADIUS Configuration

Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Quick Connect...

Discovered targets

Refresh

Name	Status
iqn.1992-08.com.netapp:sn.5918b03f9ef411ecb007495...	Inactive

To connect using advanced options, select a target and then click Connect.

Connect

Connect To Target

Target name:

iqn.1992-08.com.netapp:sn.5918b03f9ef411ecb0074956fb75f45c:vs.6

☒ Add this connection to the list of Favorite Targets.

This will make the system automatically attempt to restore the connection every time this computer restarts.

☒ Enable multi-path

Advanced...

OK

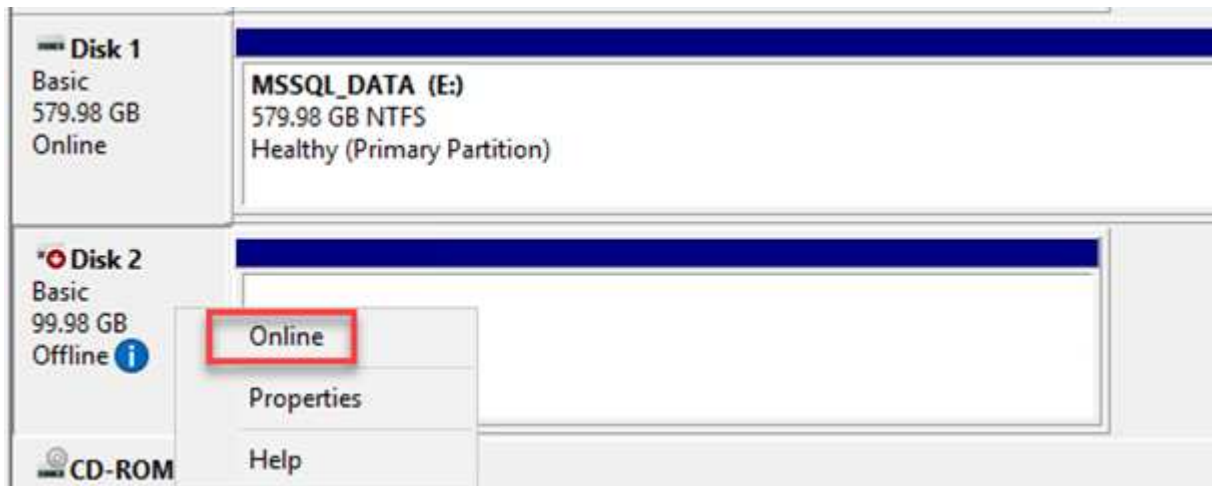
Cancel

OK

Cancel

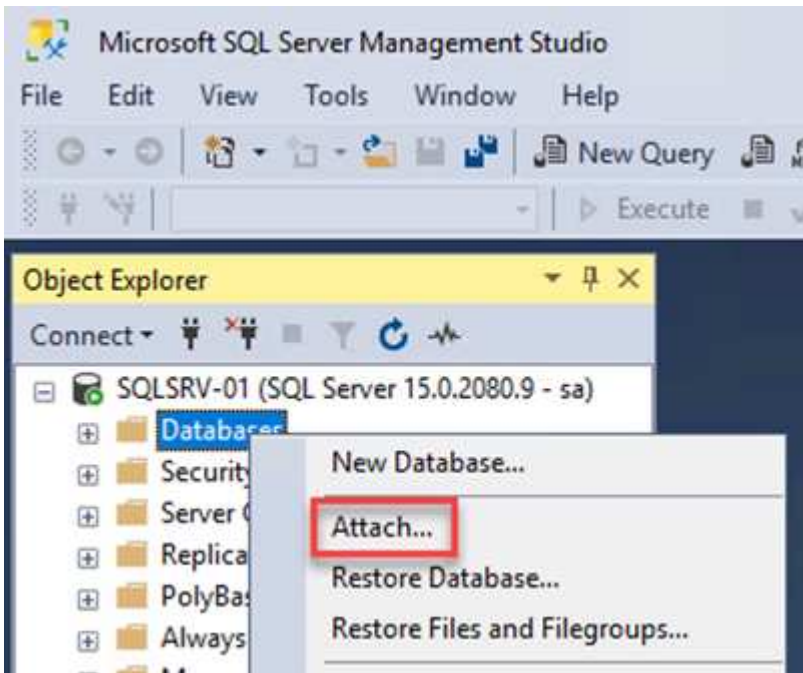
Apply

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。

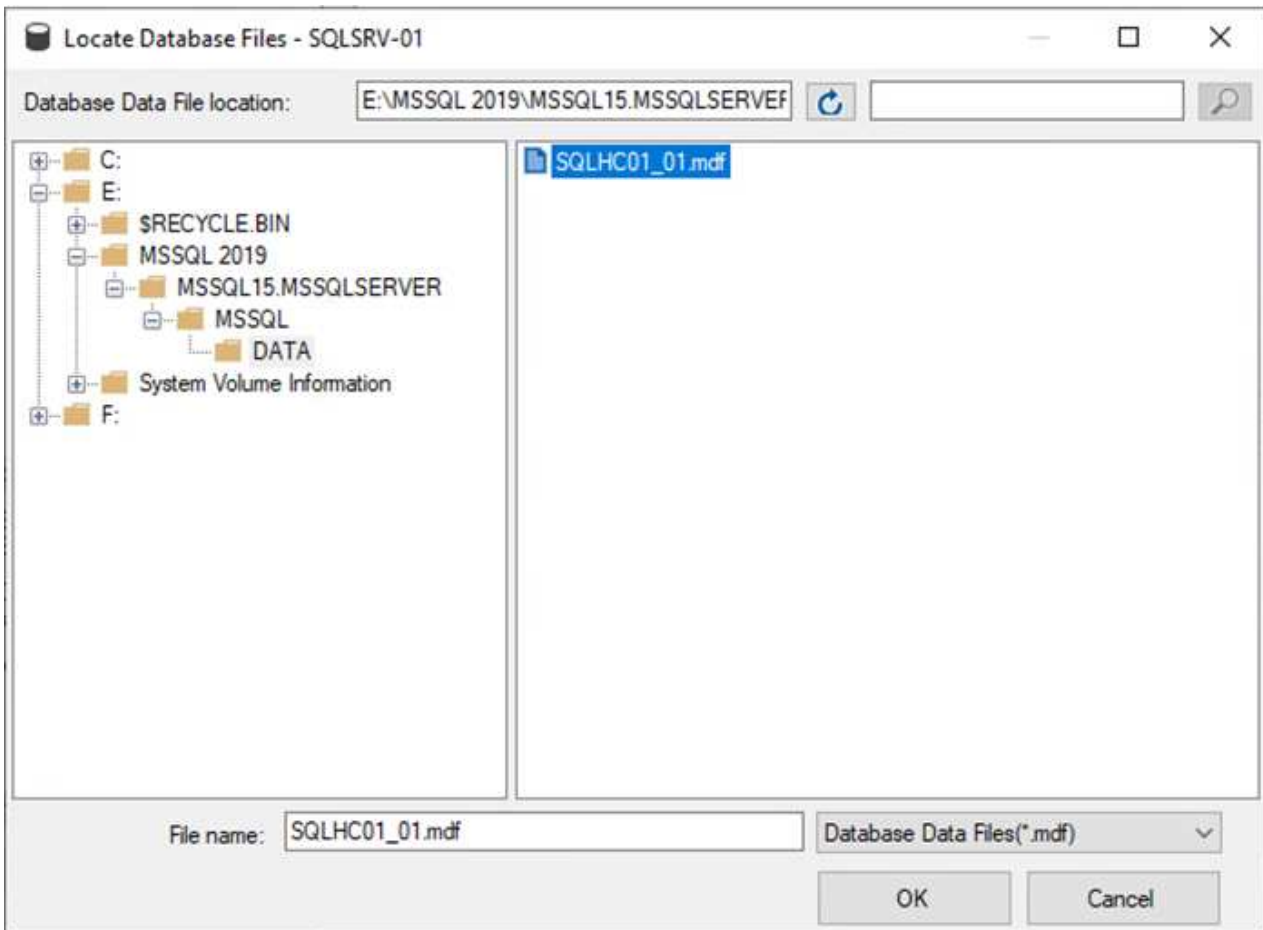


SQL Serverデータベースを接続します

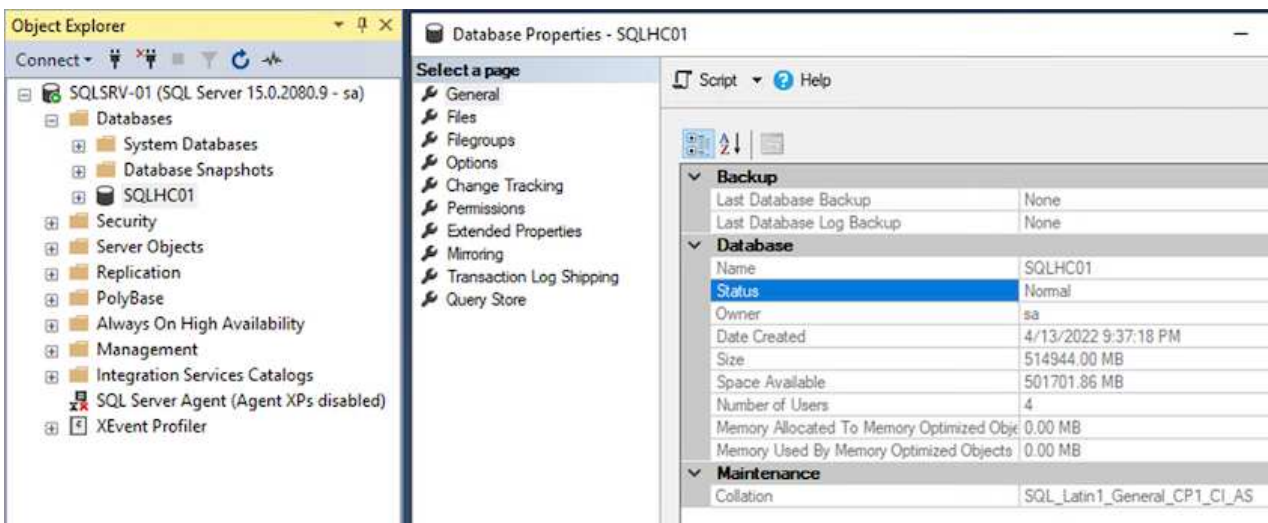
1. SQL Server VMで、Microsoft SQL Server Management Studioを開き、接続を選択してデータベースへの接続プロセスを開始します。



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。

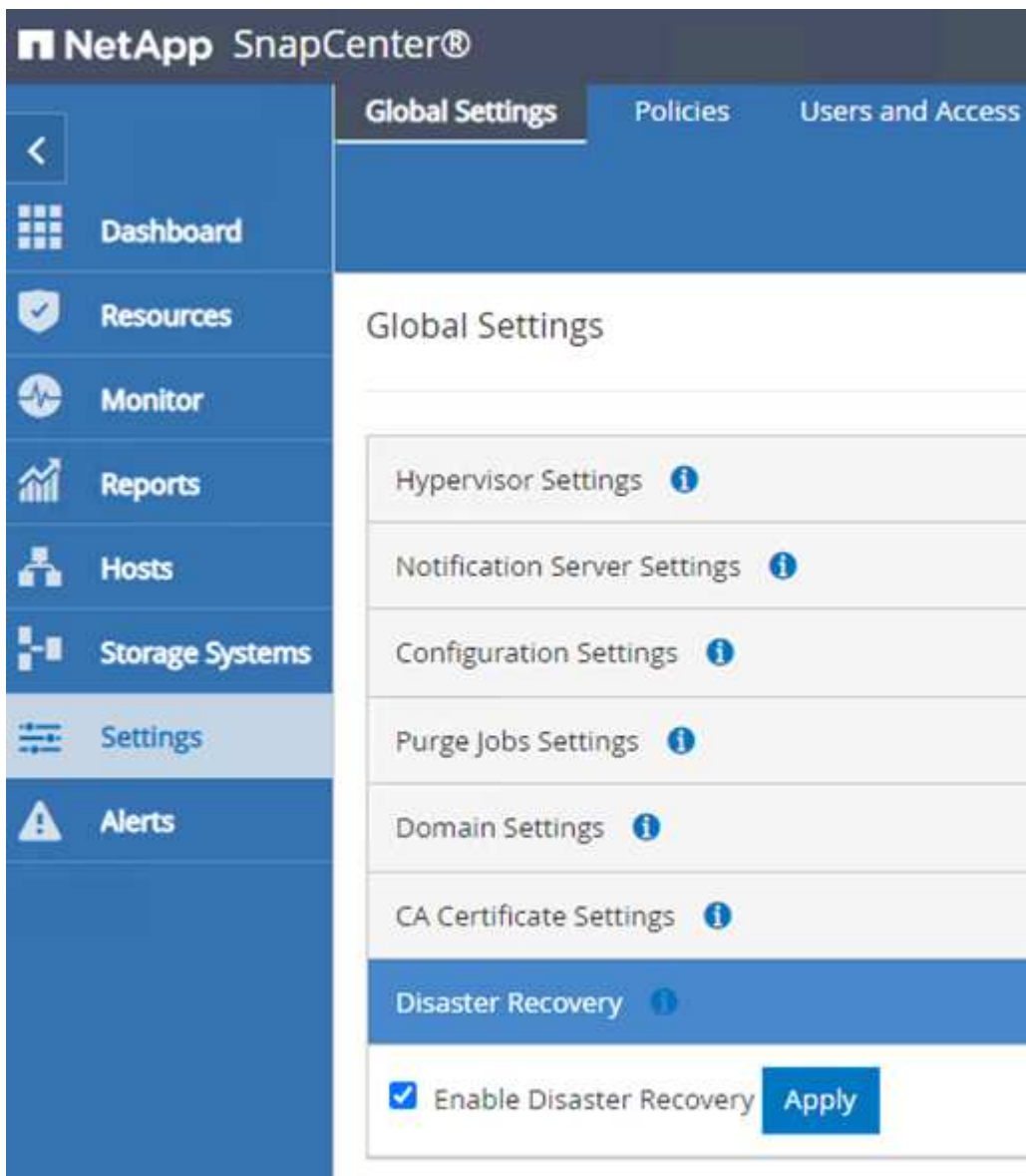


SQL Server Plug-inとのSnapCenter 通信を確認します

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. セカンダリSnapCenter サーバが確立され、このセクションで説明する手順でSnapCenter データベースおよび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

FSxN 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、正しい名前でも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。

oraclesrv_03_u01_dest (fsvol-01167370e9b7aefa0)

Attach

Actions ▲

Update volume

Create backup


Delete volume

Summary

Volume ID

fsvol-01167370e9b7aefa0 

Volume name

oraclesrv_03_u01_dest 


UUID

3d7338ce-9f19-11ec-
b007-4956fb75f45c

File system ID

fs-0ae40e08acc0dea67 

Resource ARN

arn:aws:fsx:us-
east-1:541696183547:volume/fs-
0ae40e08acc0dea67/fsvol-
01167370e9b7aefa0 

Creation time

2022-03-08T14:52:09-05:00

Lifecycle state

 Created

Volume type

ONTAP

Size

100.00 GB 

SVM ID

svm-02b2ad25c6b2e5bc2

Junction path

- 

Tiering policy name

SNAPSHOT_ONLY

Tiering policy cooling period (days)

2

Storage efficiency enabled

Disabled

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



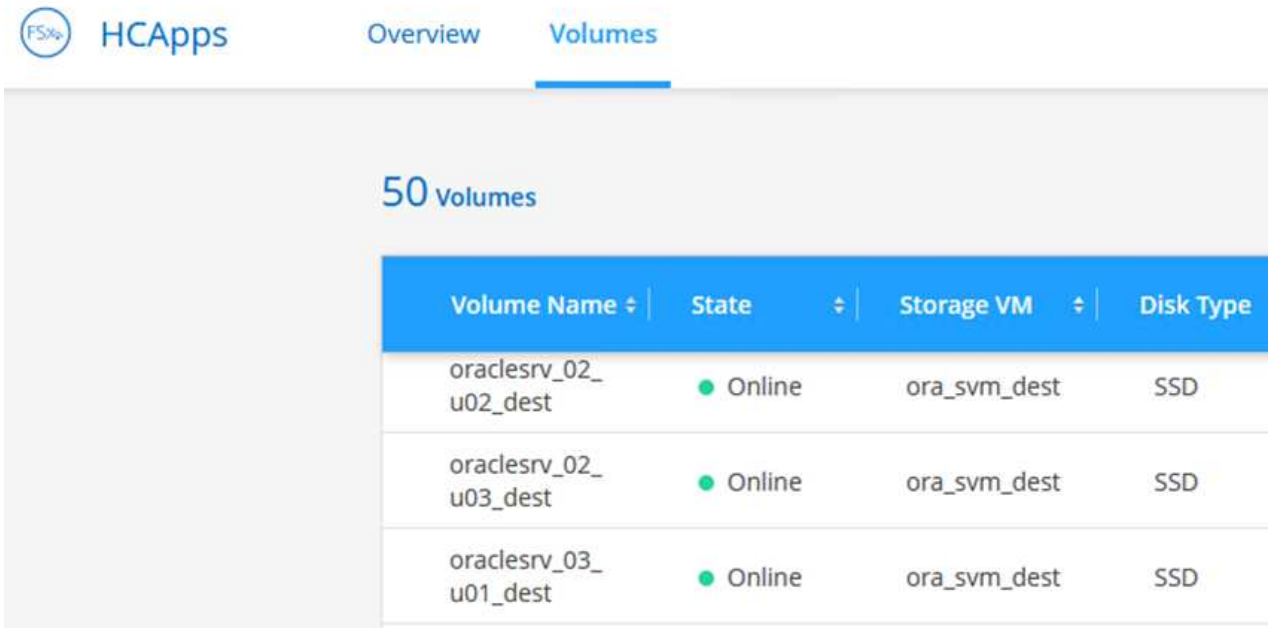
Cancel

Update

Oracle ServerにNFSボリュームをマウントします

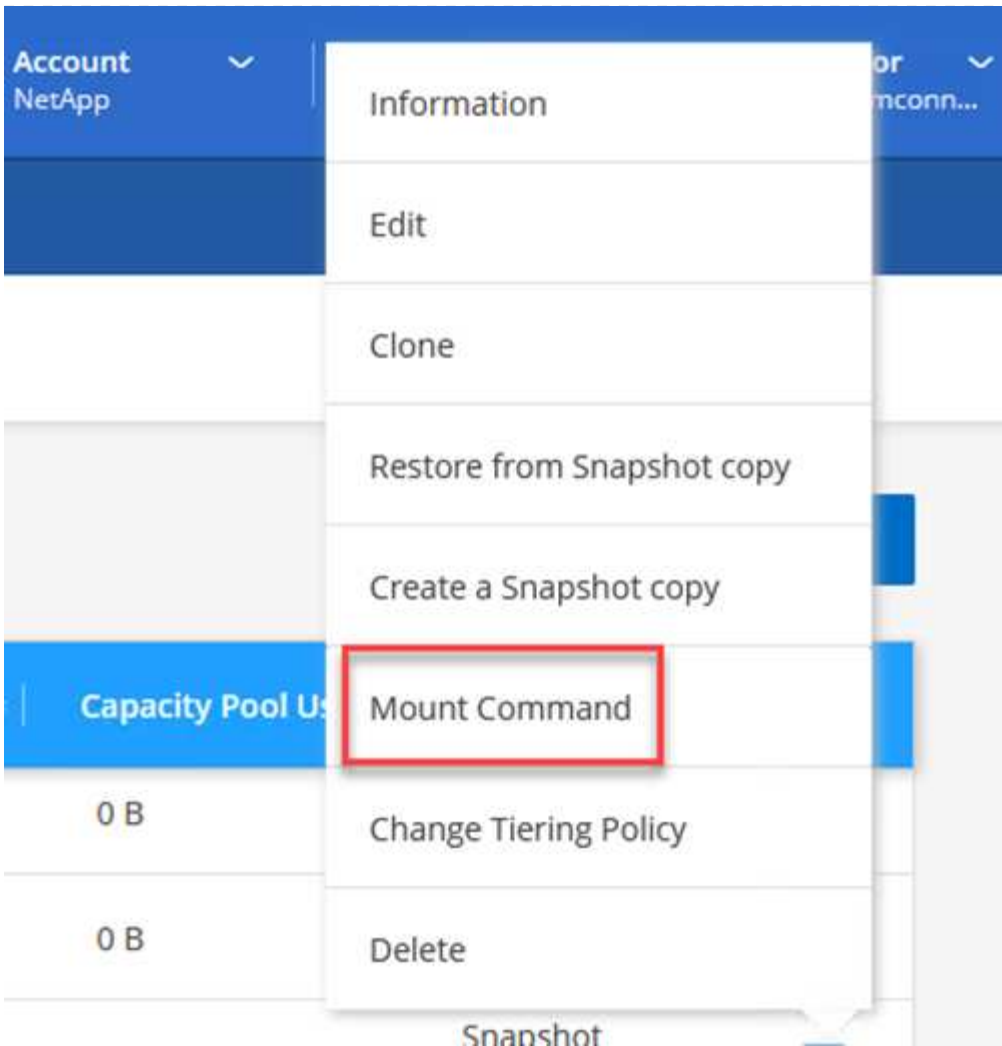
Cloud Managerでは、Oracleデータベースファイルとログを格納するNFSボリュームをマウントするための、正しいNFS LIFのIPアドレスを指定してmountコマンドを取得できます。

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。



50 volumes			
Volume Name ↕	State ↕	Storage VM ↕	Disk Type
oraclesrv_02_u02_dest	● Online	ora_svm_dest	SSD
oraclesrv_02_u03_dest	● Online	ora_svm_dest	SSD
oraclesrv_03_u01_dest	● Online	ora_svm_dest	SSD

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。




Mount Volume NFS

oraclesrv_03_u01_dest

Go to your linux machine and enter this mount command

Mount Command

```
mount 198.19.254.180:/oraclesrv_03_u01_dest <dest_d...
```

 Copy

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。



再起動時にNFSマウントを維持するには/etc/fstabファイルを編集してマウント・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

この解決策 で概説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がAWSで実行されるバックアップ機能を再開します。FSX for ONTAP は、元のオンプレミスデータセンターとの間にSnapMirror関係が確立されていないプライマリストレージとして指定されます。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。

また、このドキュメントで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 for 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 を設定することもできます。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ー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ーを提供します。このテクノロジーを使用すると、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ーとONTAP テクノロジー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。

ONTAP on AWSは、アプリケーションデータをクラウドにレプリケートするためにSnapCenter やSyncMirrorとシームレスに統合できる解決策 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ーです。

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。

追加情報の参照先

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"](#)

Veeam Backup & Restore in VMware Cloud with Amazon FSx for ONTAP

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

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。この解決策では、Veeam Backup and Replicationを使用して、FSx for ONTAP NFSデータストアにあるアプリケーションVMをVMware Cloudで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。

VMware Cloud (AWS) は、補完的ストレージとしてNFSデータストアの使用をサポートしています。FSx for NetApp 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解決策です。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。

- バックアップリポジトリとしてFSx for NetApp ONTAP を使用して、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できます。
- FSx for NetApp 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。
- バックアップリポジトリとしてFSx for NetApp ONTAP を使用した、Oracleアプリケーションデータのバックアップとリストア

Amazon FSx for ONTAP を使用したNFSデータストア

この解決策 内のすべての仮想マシンは、FSx for ONTAP の補完的NFSデータストア上に配置されます。FSx for 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。

以下のリストには、Veeam Backup & Replicationの設定、バックアップリポジトリとしてFSx for 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 for ONTAP ファイルシステムを作成します。
2. Veeamプロキシを導入して、バックアップワークロードを分散し、FSx for 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。

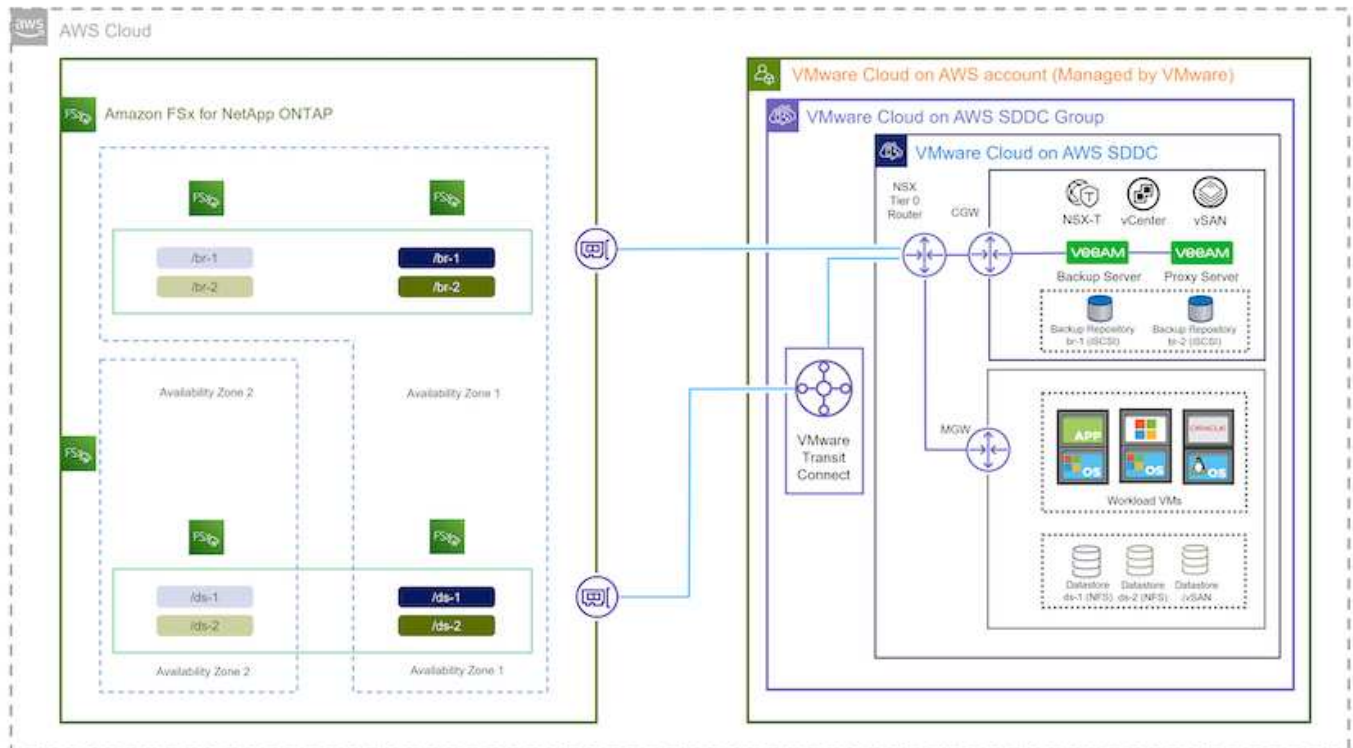
前提条件

この解決策 の目的は、VMware Cloudで実行され、FSx for NetApp 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について説明することです。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. FSx for ONTAP ファイルシステムで、VMware Cloudに接続された1つ以上のNFSデータストアを使用します。
2. Veeam Backup & ReplicationソフトウェアがインストールされたMicrosoft 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 for 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 for ONTAP NFSデータストアに格納されている。
6. FSx for 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ください ["Veeam Backup and Replication User Guide for VMware vSphereを参照してください"](#)。

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

この解決策 の目的は、VMware Cloudで実行され、FSx for NetApp 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について説明することです。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。

- Microsoft Windows VMはFSx for ONTAP NFSデータストアに配置されます
- FSx for ONTAP NFSデータストアにあるLinux (CentOS) VM
- FSx for 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
- Oracle VMはFSx for ONTAP NFSデータストアに配置されます

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。この解決策 の仮想マシンは、FSx for ONTAP で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するiSCSIボリュームのホストには、独立したFSx for ONTAP ファイルシステムが使用されます。

FSx for 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 for NetApp ONTAP の詳細については、を参照してください ["FSx for ONTAP ユーザガイド"](#)。

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

Veeam Backup and ReplicationをVMware Cloud on AWSで使用する場合は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。

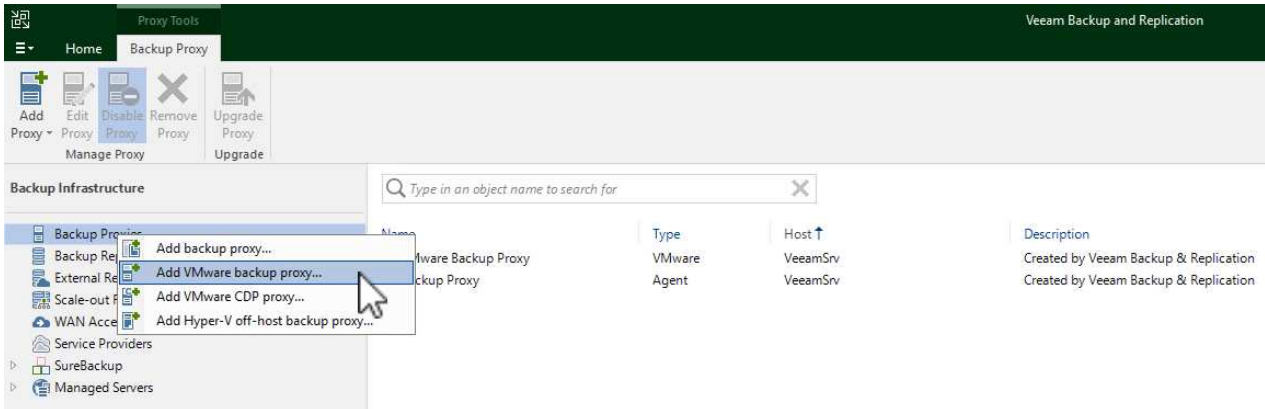
トランスポートモードの詳細については、を参照してください ["Veeam Backup and Replication User Guide for VMware vSphereを参照してください"](#)。

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の間に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。



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。

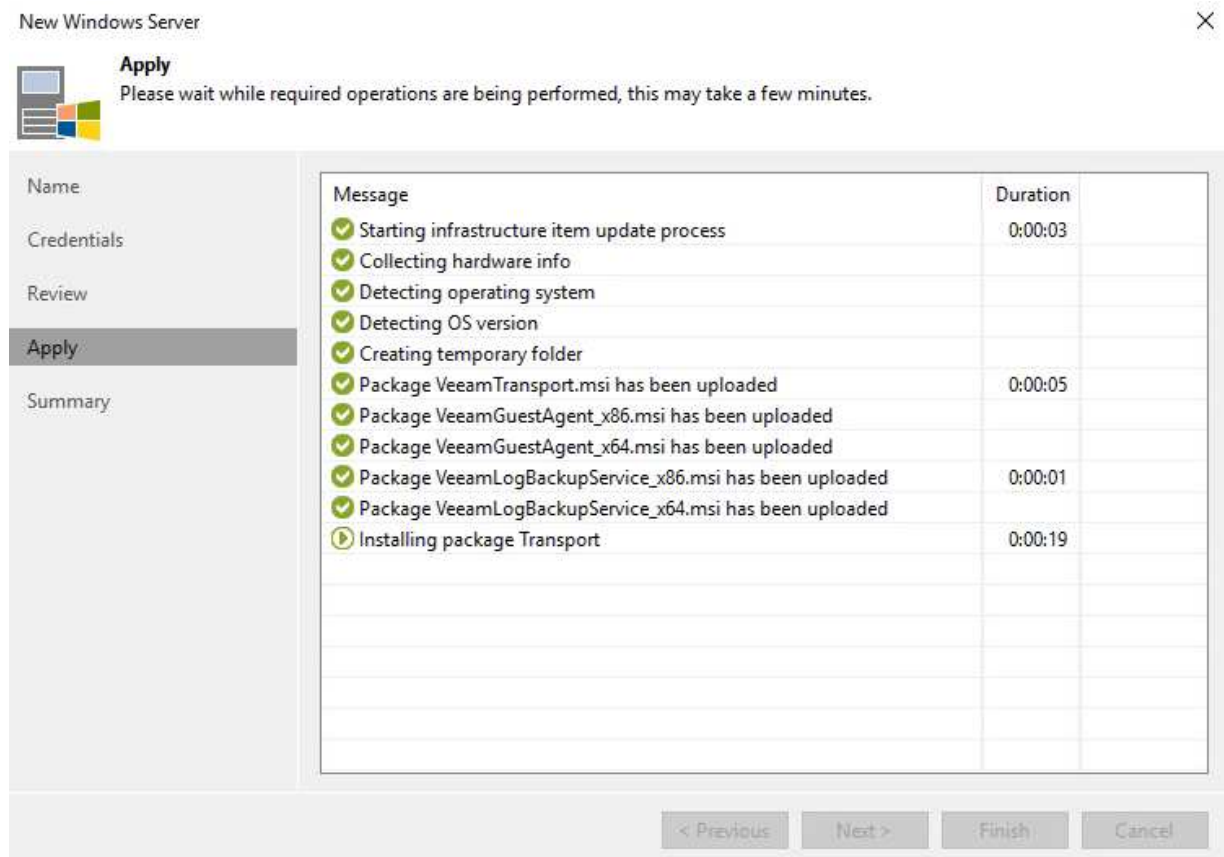
The screenshot shows the 'New VMware Proxy' wizard. The 'Server' step is selected in the left sidebar. The main area contains the following fields:

- Choose server:** A dropdown menu showing 'VeeamSrv (Backup server)' with an 'Add New...' button to its right.
- Proxy description:** A text box containing 'Created by VEEAMSRV\Administrator at 12/22/2022 9:11 PM.'
- Transport mode:** A dropdown menu set to 'Automatic selection' with a 'Choose...' button.
- Connected datastores:** A dropdown menu set to 'Automatic detection (recommended)' with a 'Choose...' button.
- Max concurrent tasks:** A numeric spinner set to '2' with a green checkmark icon.

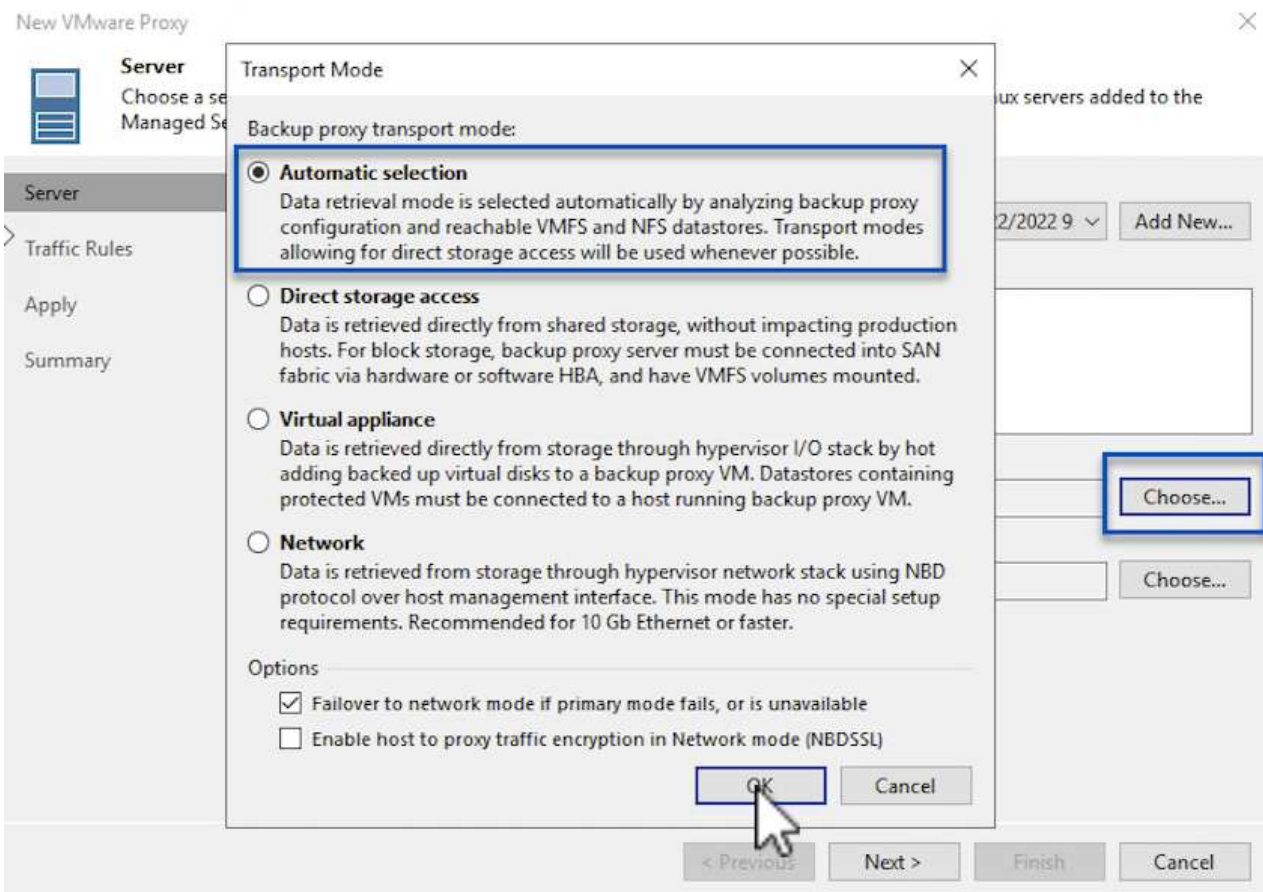
At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

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。

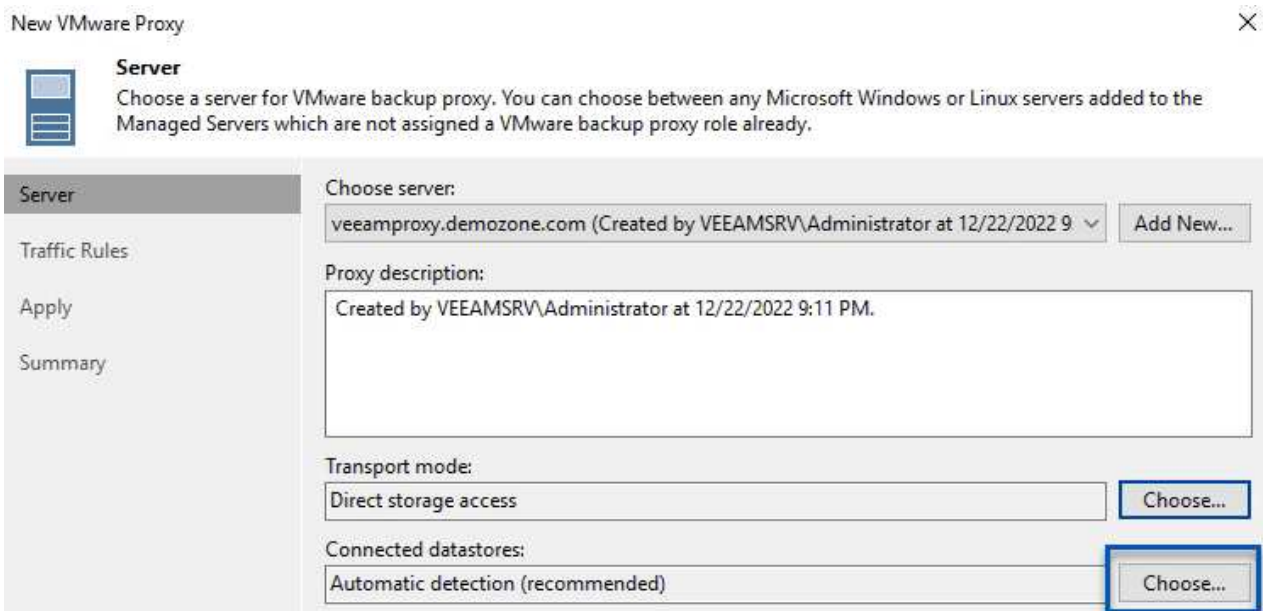
- DNS名またはIPアドレスを入力します
- 新しいシステムのクレデンシャルに使用するアカウントを選択するか、新しいクレデンシャルを追加します
- インストールするコンポーネントを確認し、*適用*をクリックして導入を開始します

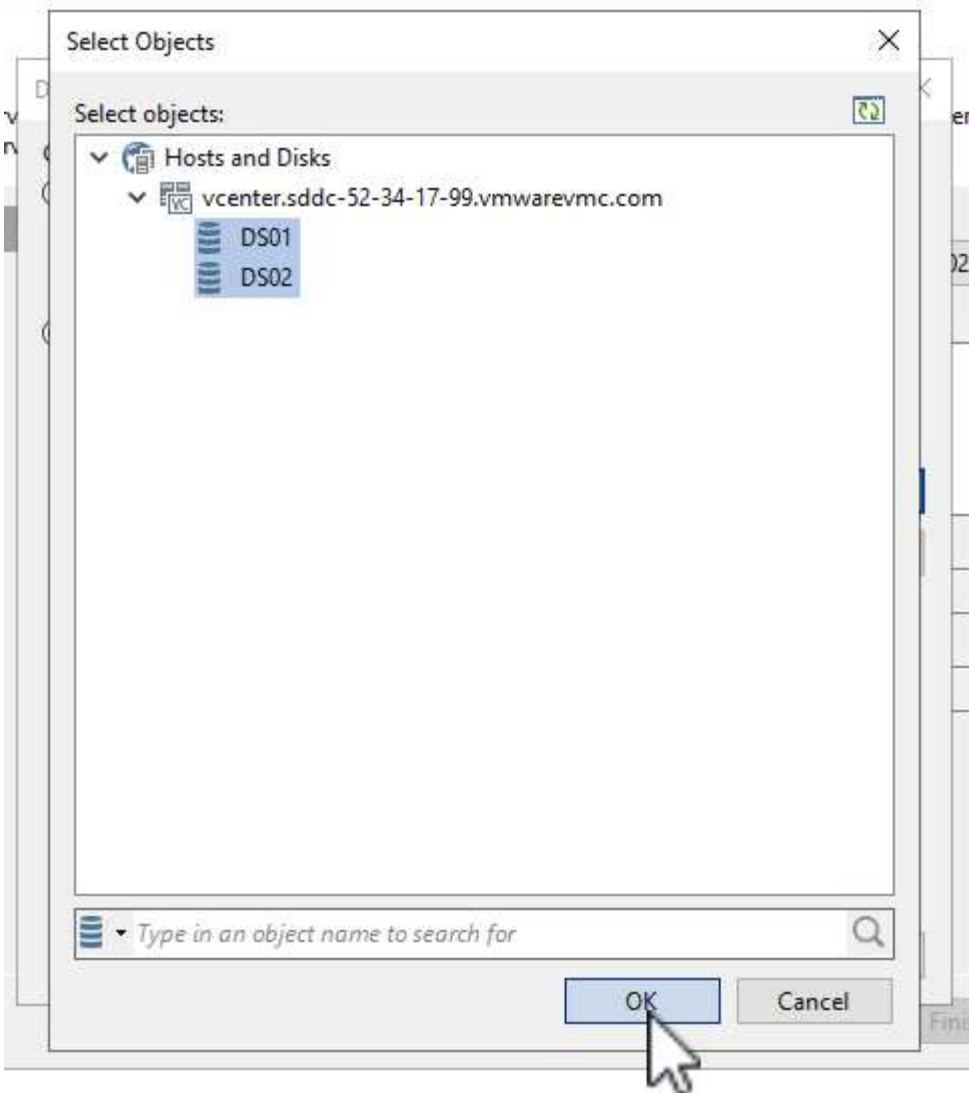


5. [New VMware Proxy]ウィザードに戻り、[Transport Mode]を選択します。ここでは、*自動選択*を選択しました。



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。

New VMware Proxy

Traffic Rules
Review network traffic encryption and throttling rules which apply to this backup proxy.

Server

Traffic Rules

Apply

Summary

Network traffic rules control encryption and throttling of network traffic based on the destination. Throttling is global, with set bandwidth split equally across all backup proxies falling into the rule.

The following network traffic rules apply to this proxy:

Name	Encryption	Throttling	Time period
Internet	Enabled	Disabled	

[Manage network traffic rules](#)

[View](#)

< Previous Apply Finish Cancel

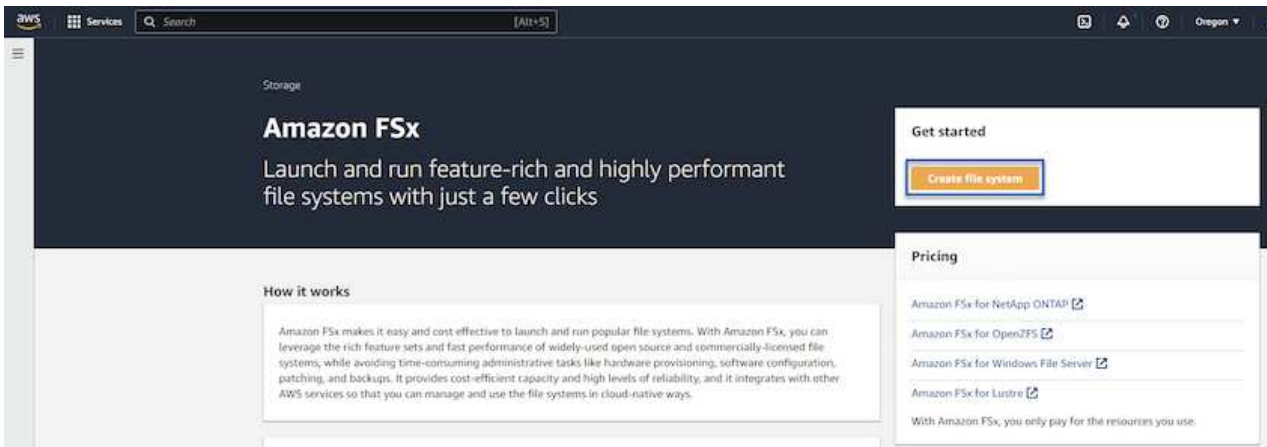
ストレージとバックアップリポジトリを設定します

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 for ONTAP ファイルシステムの作成、VeeamサーバへのiSCSI 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 for ONTAP ファイルシステムを作成

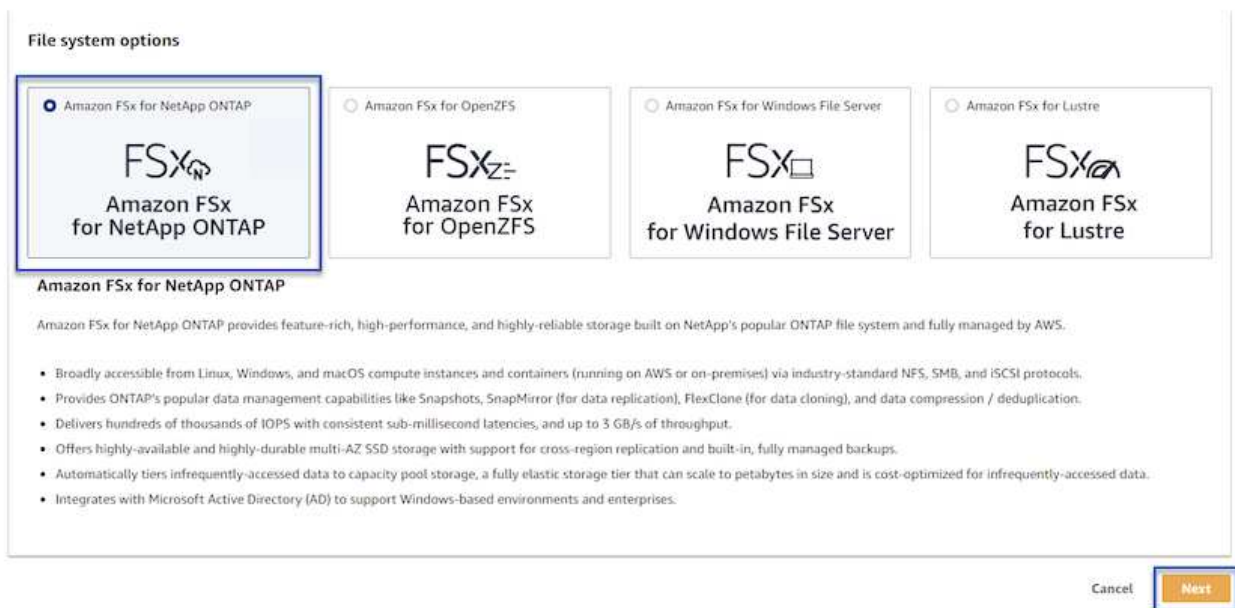
Veeamバックアップリポジトリ用のiSCSIボリュームのホストに使用するFSx for ONTAP ファイルシステムを作成します。

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 for NetApp ONTAP を選択し、Next *を選択して続行します。

Select file system type



3. ファイルシステム名、導入タイプ、SSDストレージ容量、FSx for 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。

Create file system

Creation method

☒ Quick create

Use recommended best-practice configurations. Most configuration options can be changed after the file system is created.

☐ Standard create

You set all of the configuration options, including specifying performance, networking, security, backups, and maintenance.

Quick configuration

File system name - optional info

BackupFSxN

1

Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = . _ : /

Deployment type info

☐ Multi-AZ

☒ Single-AZ

2

SSD storage capacity info

4096 GiB

3

Minimum 1024 GiB; Maximum 192 TiB

Virtual Private Cloud (VPC) info

Specify the VPC from which your file system is accessible.

Demo-FsxforONTAP-VPC | vpc-05596abe79cb653b7

4

Storage efficiency

Select whether you would like to enable ONTAP's storage efficiency features: deduplication, compression, and compaction

☒ Enabled (recommended)

☐ Disabled

Cancel

Back

Next

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

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。

Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: Port: (Default is 3260.)

Advanced... **OK** Cancel

To remove a target portal, select the address above and then click Remove.

iSNS servers

The system is registered on the following iSNS servers:

Name

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click Remove.

Refresh Add Server... Remove

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。

Targets Discovery Favorite Targets Volumes and Devices RADIUS Configuration

Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status
iqn.1992-08.com.netapp:sn.d9aad3cd818011edbfc87a...	Inactive

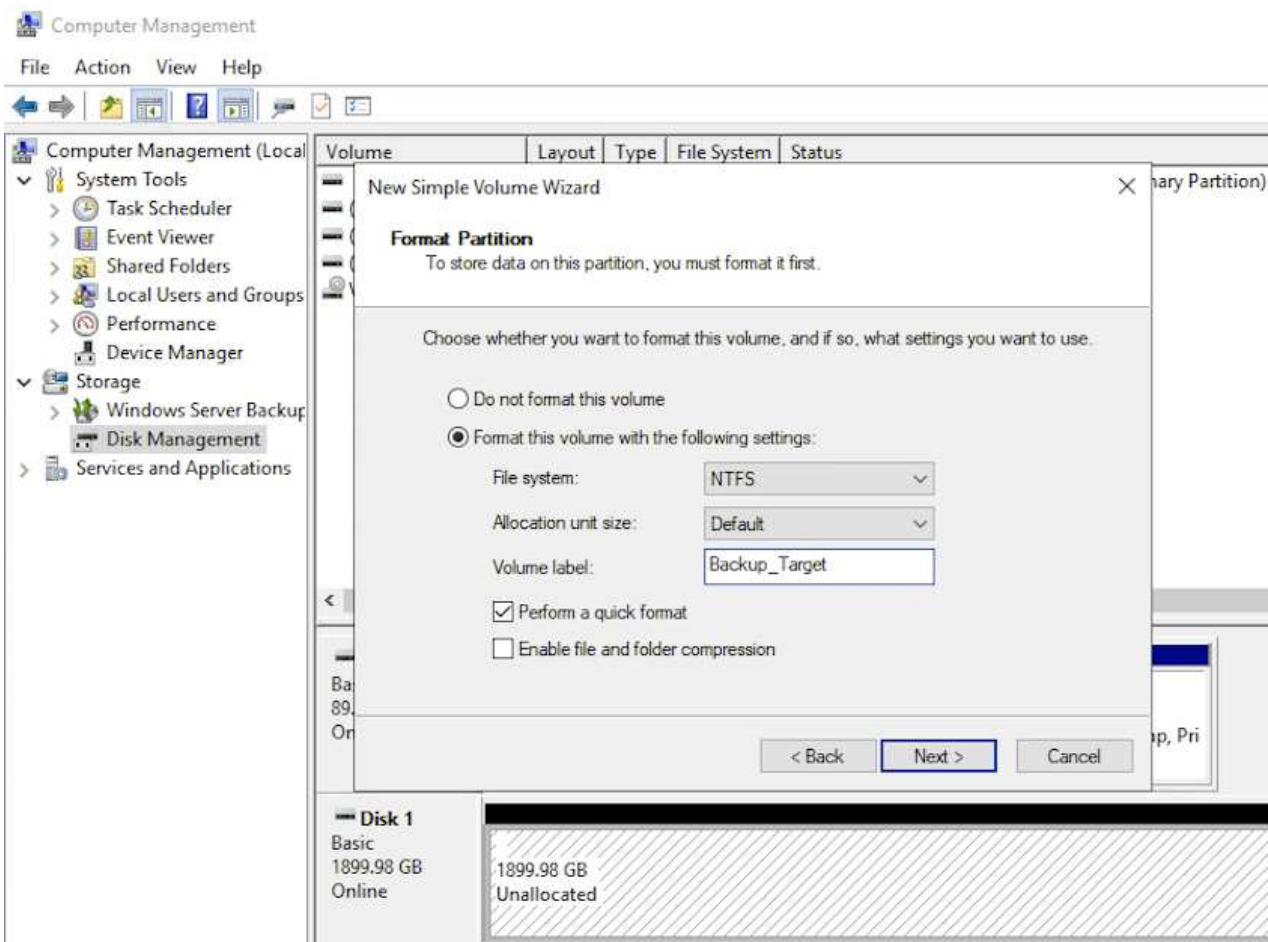
To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties...

For configuration of devices associated with a target, select the target and then click Devices...

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。

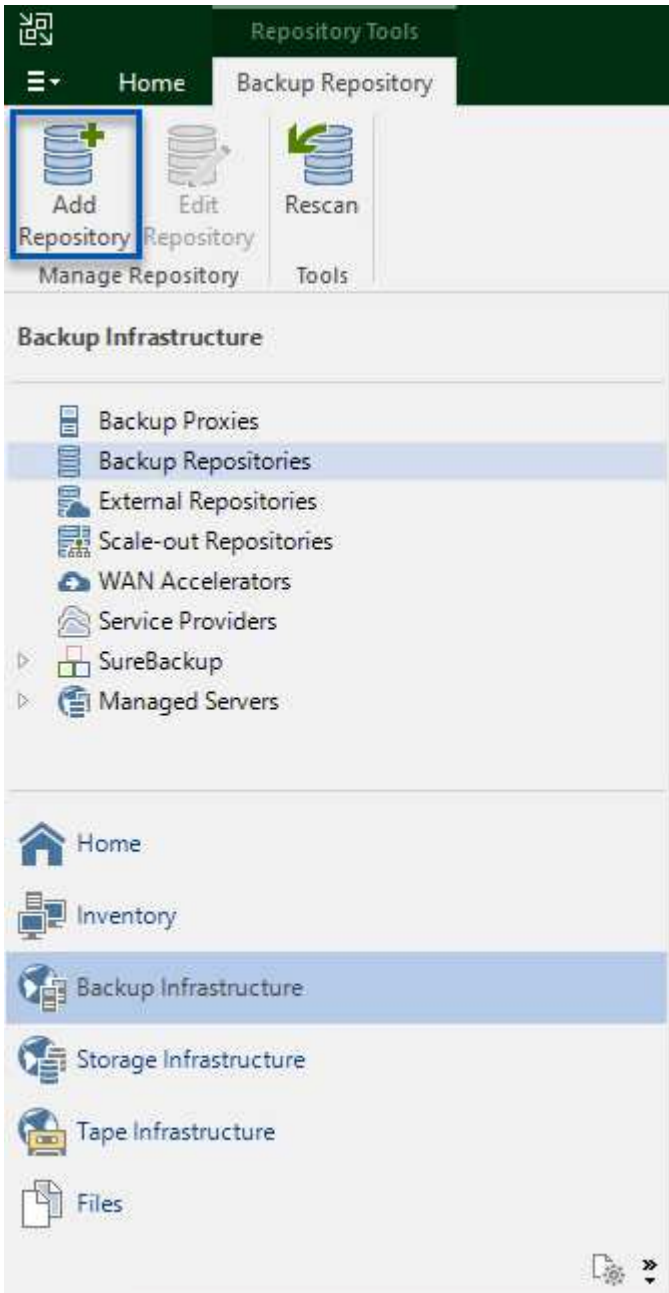


8. 同じ手順を繰り返して、iSCSIボリュームをVeeam Proxyサーバにマウントします。

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。



Name _____

Repository

Mount Server

Review

Apply

Summary

veeamproxy.demozone.com (Created by VEEAMSRV\Administrator at 12/22/2022 9:00 AM)

Add New...

Populate


[< Previous](#)

Next >

Cancel

- 87

New Backup Repository



Review
Please review the settings, and click Apply to continue.

Name

Server

Repository

Mount Server

Review

Apply

Summary

The following components will be processed on server veeamproxy.demozone.com:

Component name	Status
Transport	already exists
vPower NFS	will be installed
Mount Server	will be installed

☐ Search the repository for existing backups and import them automatically
☐ Import guest file system index data to the catalog

< Previous

Apply

Finish

Cancel

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

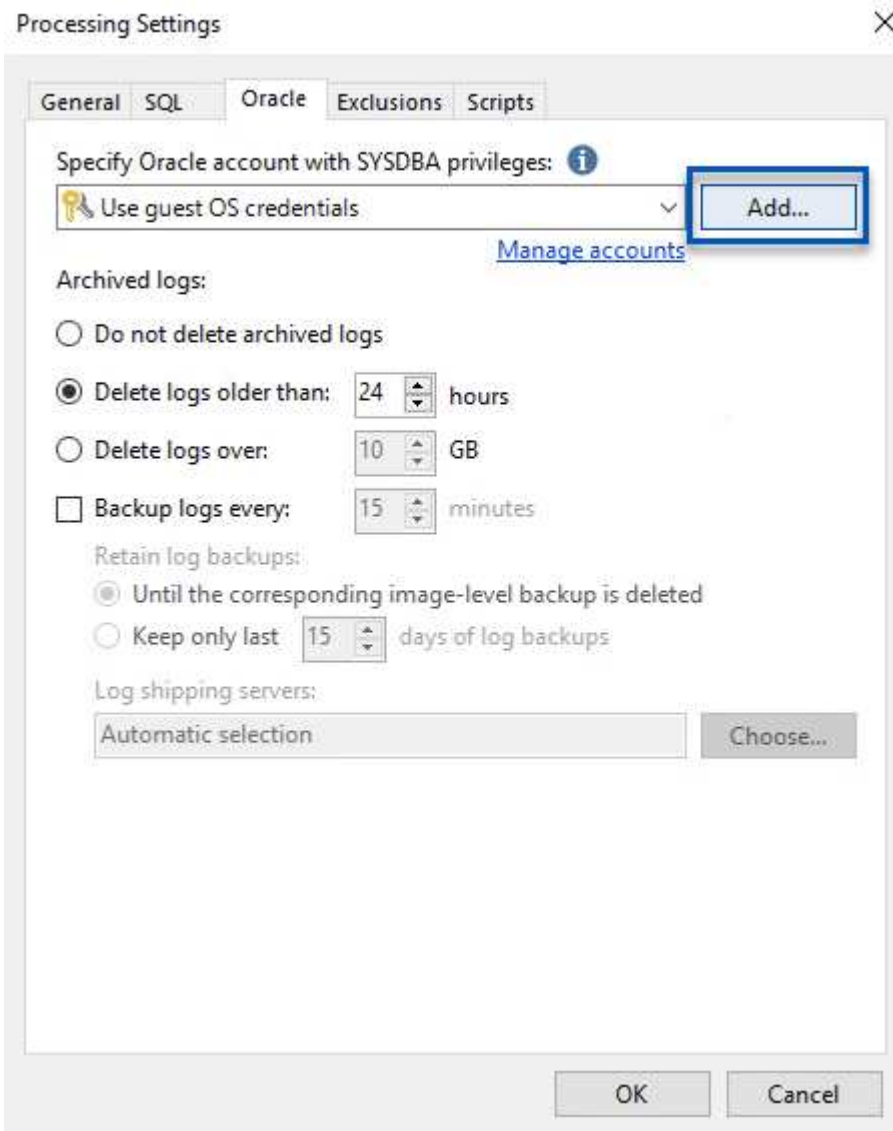
バックアップジョブは、前のセクションのバックアップリポジトリを使用して作成します。バックアップジョブの作成は、ストレージ管理者の業務の通常の一部であり、ここで紹介するすべての手順を網羅しているわけではありません。Veeamでのバックアップジョブの作成の詳細については、を参照してください "[Veeam Help Centerテクニカルドキュメント](#)"。

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。

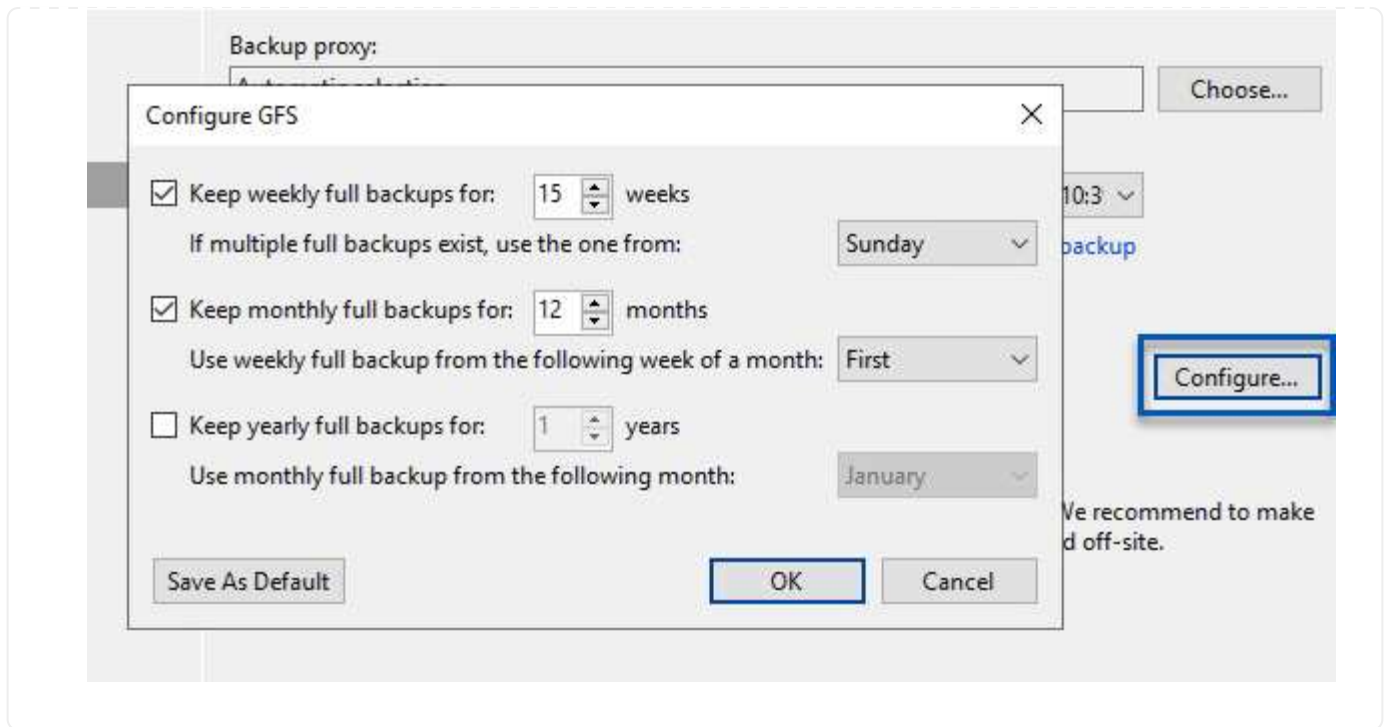
- Microsoft Windows SQL Serverの略
- Oracleデータベースサーバ
- Windowsファイルサーバ
- Linuxファイルサーバ

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、を参照してください ["Veeam Help Centerテクニカルドキュメント"](#)。

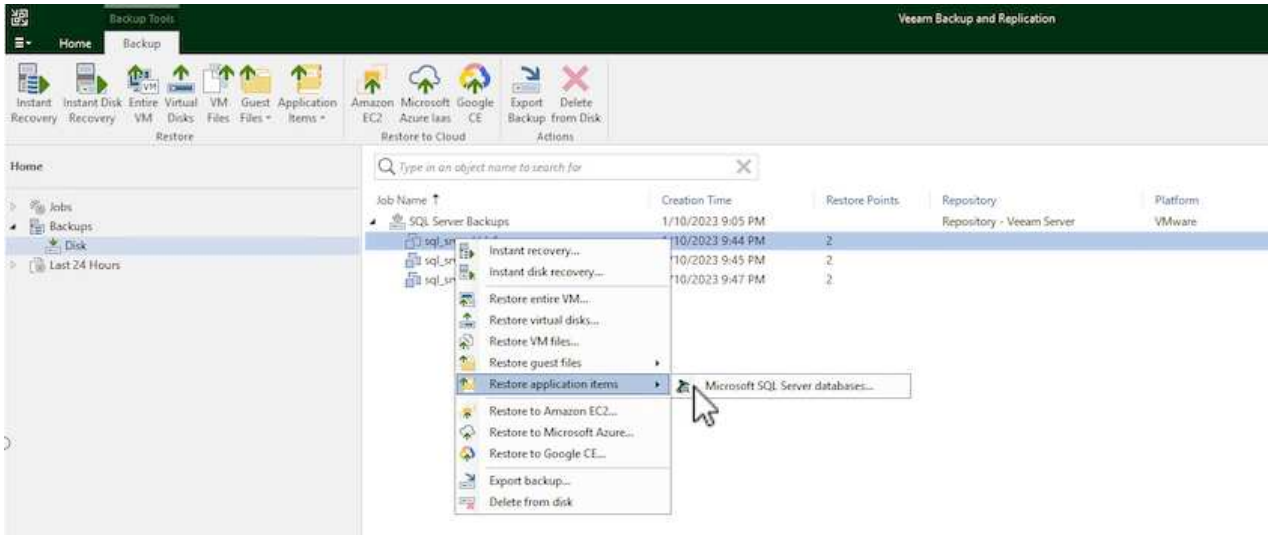
SQL Serverデータベースをリストアします

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。

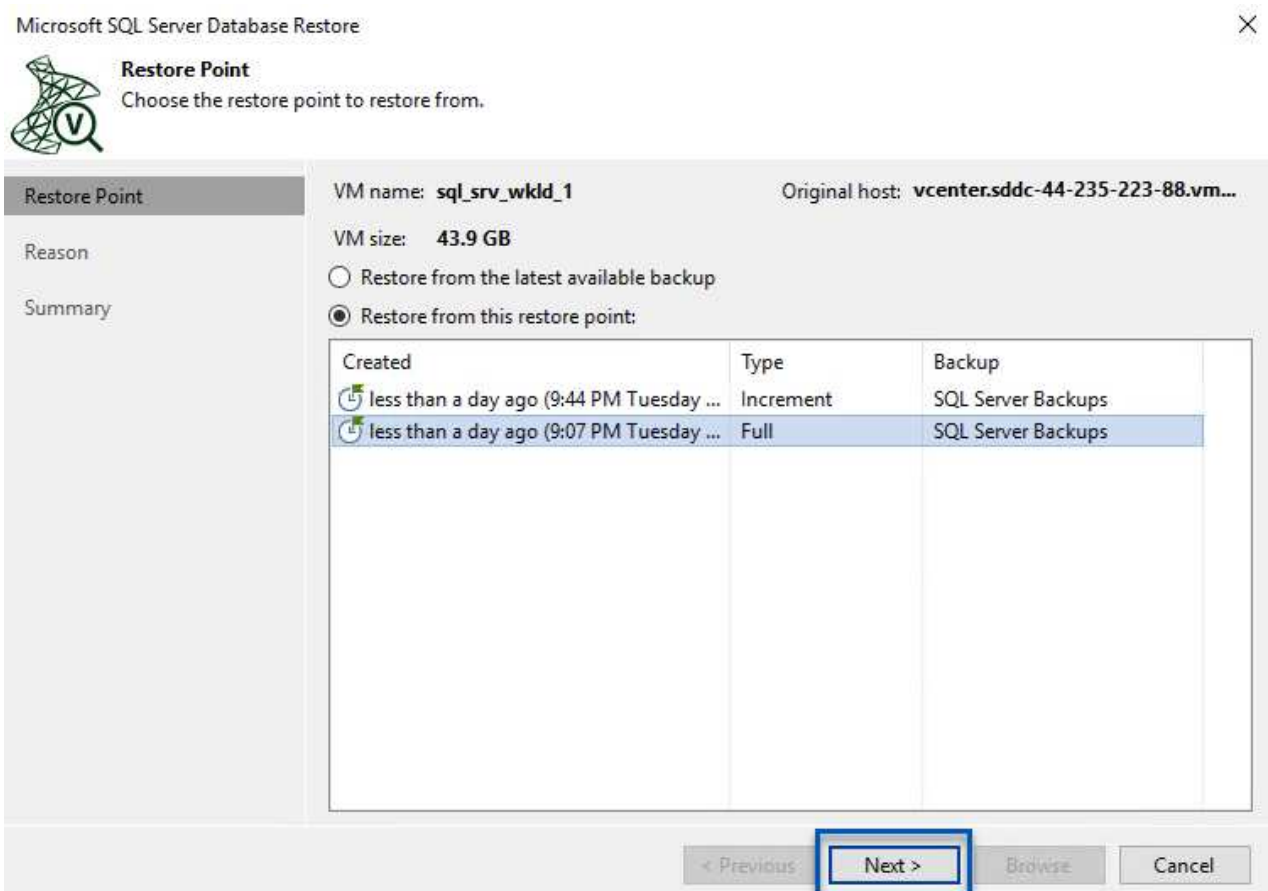
- Veeam Explorer *で、リストア対象のSQL Serverデータベースを含むバックアップ*をマウントします。
- ソフトウェア*は、マウントされたファイルからデータベース*を直接パブリッシュし、ターゲットSQL Serverインスタンス上の一時データベースとしてアクセスできるようにします。
- 一時データベースの使用、Veeam Explorer *はユーザークエリ*をこのデータベースにリダイレクトし、ユーザーが引き続きデータにアクセスして作業できるようにします。
- Veeam *はバックグラウンドでフルデータベースリストア*を実行し、一時データベースから元のデータベースの場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

**Summary**

Review the restore settings, and click Browse to exit the wizard and open Veeam Explorer for SQL Server, where you will select databases to restore.

Restore Point

Reason

Summary

Summary:

VM name: sql_srv_wkld_1

Restore point:

Current: sql_srv_wkld_1 less than a day ago (9:07 PM Tuesday 1/10/2023)

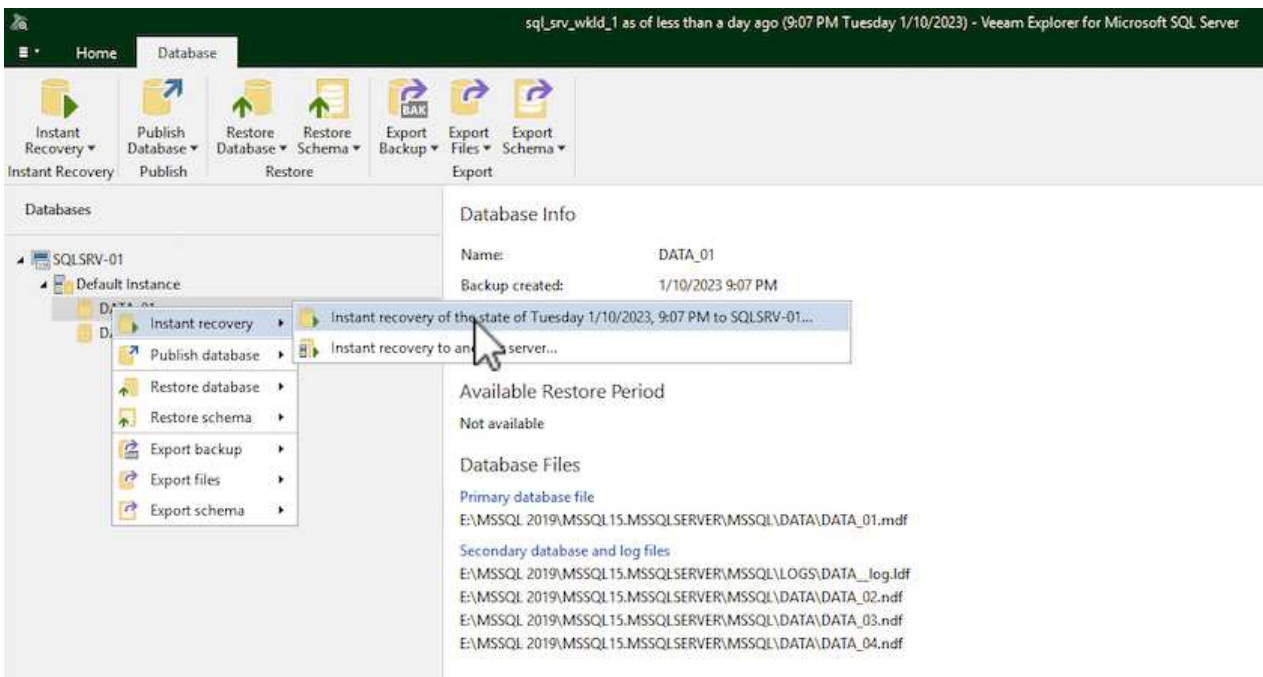
< Previous

Next >

Browse

Cancel

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。

Instant Recovery Wizard

×

Specify database switchover scheduling options

Specify switchover type:

☒ Auto

Switchover will be performed automatically with minimal possible downtime once the database is ready.

☐ Manual

Switchover can be performed manually at any point in time after the database is ready.

☐ Scheduled at:

1/10/2023 10:16 PM

▼

Back

Recover

Cancel

6. リカバリプロセスはVeeam Explorerから監視できます。

Home Instant Recovery

sql_srv_wkld_1 as of less than a day ago (0:07 PM Tuesday 1/10/2023) - Veeam Explorer for Microsoft SQL Server

✖

Instant Recovery

Instant Recovery

Databases

Instant Recovery (1)

DATA_01

SQLSRV-01

Default Instance

DATA_01

DATA_02

Instant Recovery Info

Status: Starting (restored)...

SQL Server: SQLSRV-01

Target name: DATA_01

Target point in time: 1/10/2023 9:07 PM

Restore point: sql_srv_wkld_1

Switchover mode: Auto

Database Files

Status: Persistent

Primary database file: E:\MSSQL 2019\MSSQL15.MSSQLSERVER\MSSQL\DATA\DATA_01.mdf

Secondary database and log files: E:\MSSQL 2019\MSSQL15.MSSQLSERVER\MSSQL\LOGS\DATA_log.ldf
E:\MSSQL 2019\MSSQL15.MSSQLSERVER\MSSQL\DATA\DATA_02.ndf
E:\MSSQL 2019\MSSQL15.MSSQLSERVER\MSSQL\DATA\DATA_03.ndf
E:\MSSQL 2019\MSSQL15.MSSQLSERVER\MSSQL\DATA\DATA_04.ndf

Action

Instant Recovery started at 1/10/2023 10:12:06 PM

Publishing database

Copying target files

Database published at 1/10/2023 10:12:42 PM

Synchronizing files

Ready for switchover

Detaching database

Completed database file synchronization

Duration

00:35

08:28

VEEAM

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の項を参照してください ["Veeam Explorers User Guideを参照してください"](#)。

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

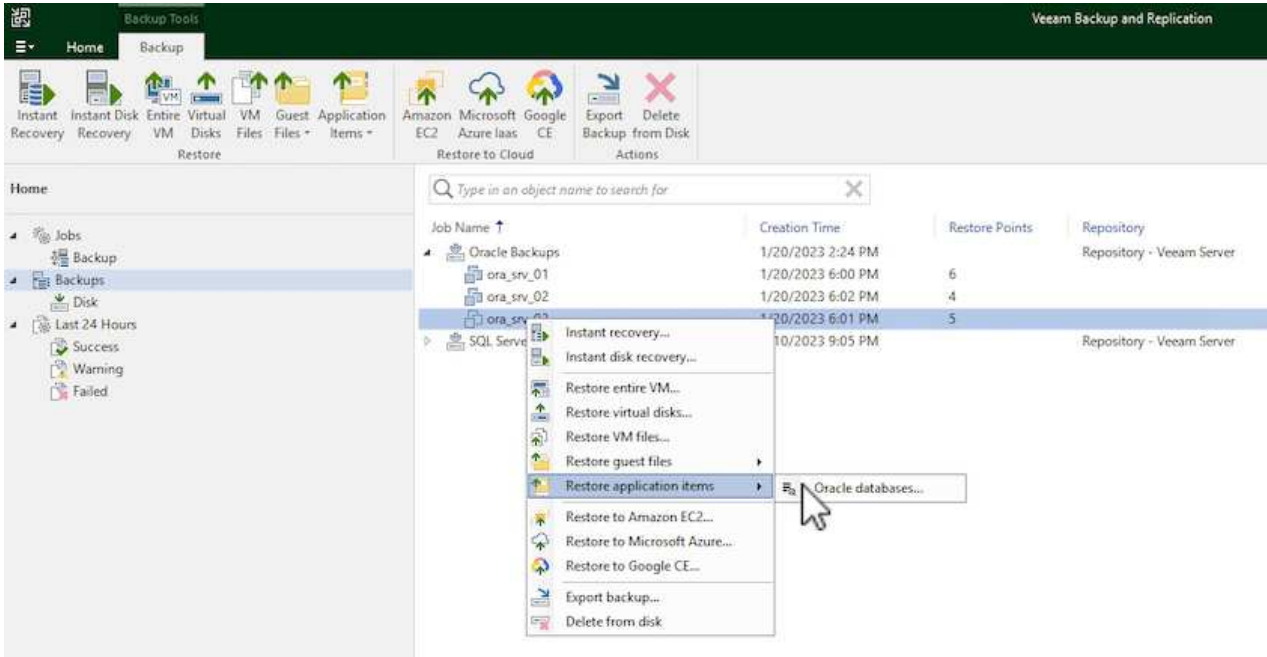
Veeam Explorer for Oracle databaseでは、Instant Recoveryを使用して、Oracleデータベースの標準リストアまたは中断のないリストアを実行できます。また、データベースのパブリッシュをサポートしているため、高速アクセス、Data Guardデータベースのリカバリ、RMANバックアップからのリストアが可能です。

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ください "[Veeam Explorers User Guideを参照してください](#)"。

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。

Oracle Database Restore

ORACLE® Restore Point
Choose the restore point to restore from.

Restore Point

Reason

Summary

VM name: **ora_srv_03** Original host: **vcenter.sddc-44-235-223-88.vm...**

VM size: **38.5 GB**

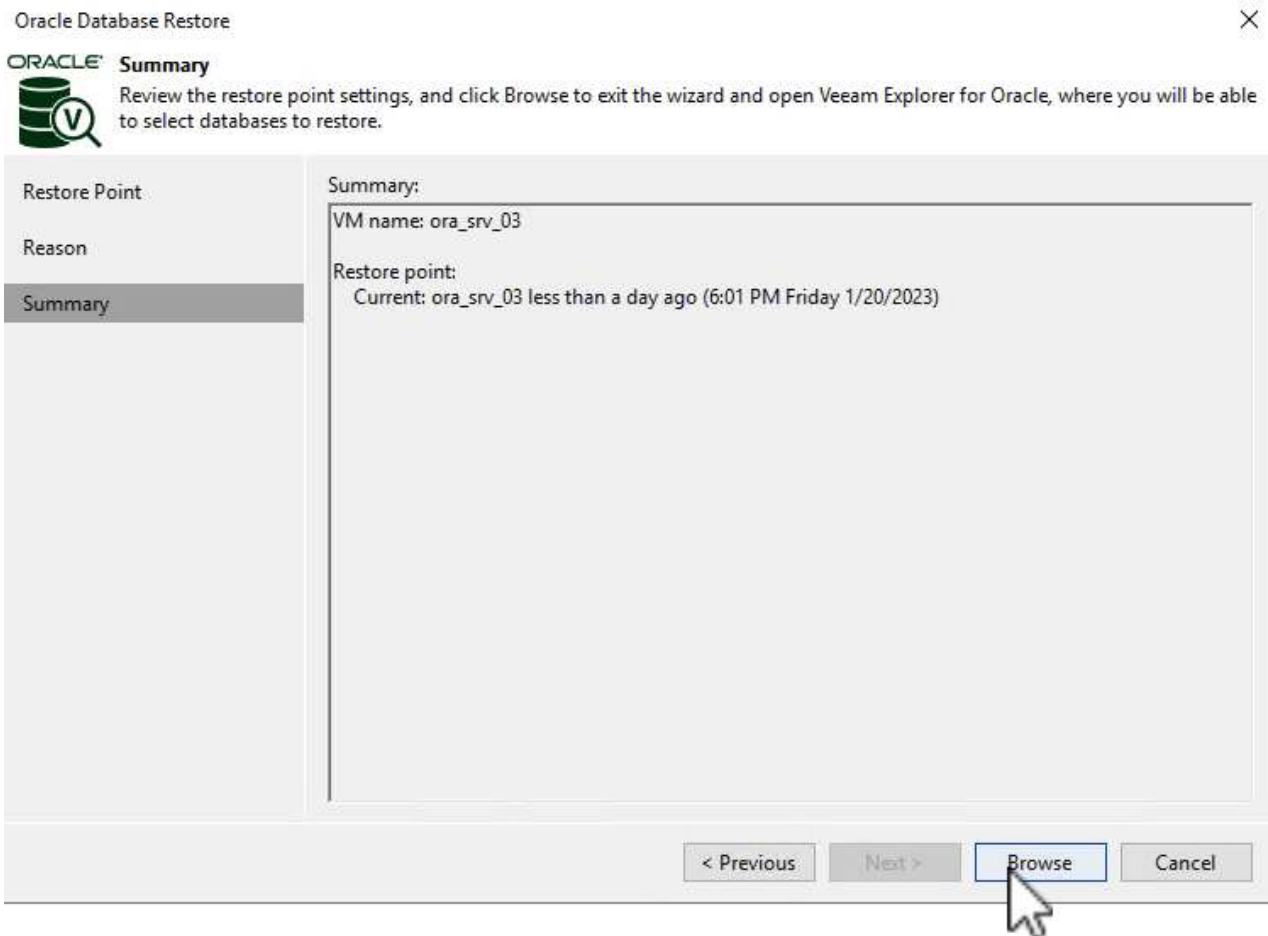
☒ Restore from the latest available backup

☐ Restore from this restore point:

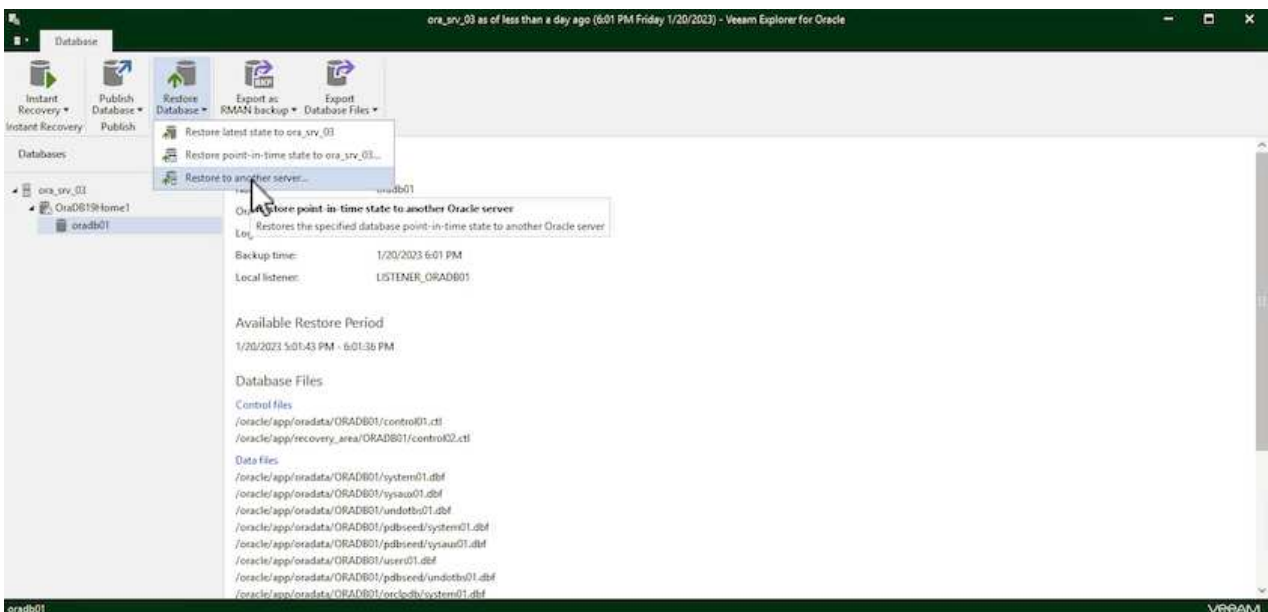
Created	Type	Backup
less than a day ago (6:01 PM Friday 1/...	Increment	Oracle Backups
less than a day ago (5:01 PM Friday 1/...	Increment	Oracle Backups
less than a day ago (4:02 PM Friday 1/...	Increment	Oracle Backups
less than a day ago (3:47 PM Friday 1/...	Increment	Oracle Backups
less than a day ago (2:47 PM Friday 1/...	Full	Oracle Backups

< Previous Next > Browse Cancel

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。



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。

Restore Wizard

Specify restore point

Specify point in time you want to restore the database to:

☒ Restore to the point in time of the selected image-level backup

☐ Restore to a specific point in time (requires redo log backups)

5:01 PM
1/20/2023

6:01 PM
1/20/2023

Friday, January 20, 2023 6:01 PM

☐ Perform restore to the specific transaction

Enables you to review major database transactions around the selected time, and restore the database to the moment in time right before the unwanted change.

⚠ To enable this functionality, specify the staging Oracle server under Menu > Options.

Back
Next
Cancel

- 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。

Restore Wizard

Specify target Linux server connection credentials

Server: ora_srv_01
SSH port: 22

Account: oracle
Advanced...

Password: [Click here to change the password]

☐ Private key is required for this connection

Private key:
Browse...

Passphrase:

Back
Next
Cancel

- 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。

Restore Wizard

×

Specify database files target location

Control files

/oracle/app/oradata/oradb01/control01.ctl
/oracle/app/recovery_area/oradb01/control02.ctl

Data files

/oracle/app/oradata/oradb01/system01.dbf
/oracle/app/oradata/oradb01/sysaux01.dbf
/oracle/app/oradata/oradb01/undotbs01.dbf
/oracle/app/oradata/oradb01/pdbseed/system01.dbf
/oracle/app/oradata/oradb01/pdbseed/sysaux01.dbf
/oracle/app/oradata/oradb01/users01.dbf

Back

Restore

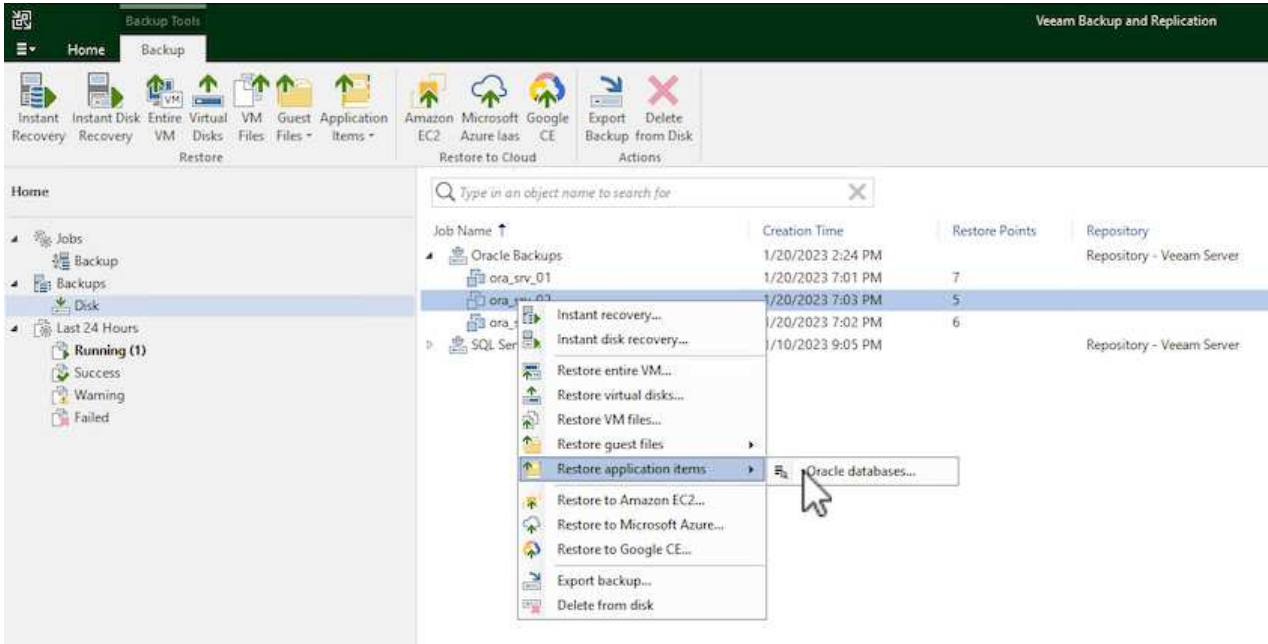
Cancel

- 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。

Oracle Database Restore

Restore Point
Choose the restore point to restore from.

VM name: **ora_srv_02** Original host: **vcenter.sddc-44-235-223-88.vm...**

VM size: **38.1 GB**

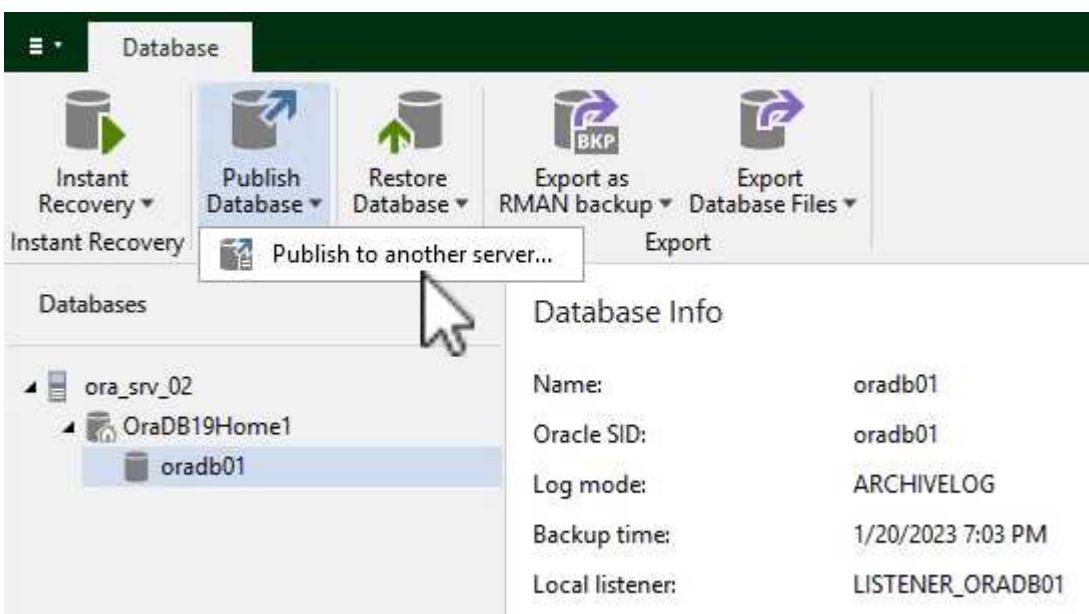
☒ Restore from the latest available backup

☐ Restore from this restore point:

Created	Type	Backup
less than a day ago (7:03 PM Friday 1/...	Increment	Oracle Backups
less than a day ago (6:02 PM Friday 1/...	Increment	Oracle Backups
less than a day ago (5:02 PM Friday 1/...	Increment	Oracle Backups
less than a day ago (4:03 PM Friday 1/...	Increment	Oracle Backups
less than a day ago (3:49 PM Friday 1/...	Full	Oracle Backups

< Previous **Next >** Browse Cancel

- 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。
- 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。



- 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。

Publish Wizard

Specify Oracle settings

☒ Restore to the original location

☐ Restore to a different location:

Oracle Home: /oracle/app/product/19c Browse...

Global Database Name: oradb01.demozone.com

Oracle SID: oradb01

Back Publish Cancel

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$databases;
```



```
oracle@ora_srv_01:~  
File Edit View Search Terminal Help  
[oracle@ora_srv_01 ~]$ sqlplus / as sysdba  
  
SQL*Plus: Release 19.0.0.0.0 - Production on Fri Jan 20 16:46:39 2023  
Version 19.3.0.0.0  
  
Copyright (c) 1982, 2019, Oracle. All rights reserved.  
  
Connected to:  
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production  
Version 19.3.0.0.0  
  
SQL> select name, open_mode from v$database;  


| NAME    | OPEN_MODE  |
|---------|------------|
| ORADB01 | READ WRITE |


```

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ーに焦点を当てています。FSx for 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をiSCSIバックアップターゲットボリューム（FSx for ONTAPでホスト）と組み合わせて使用すると、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解決策を提供できます。

追加情報

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

- ["FSx for 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"](#)

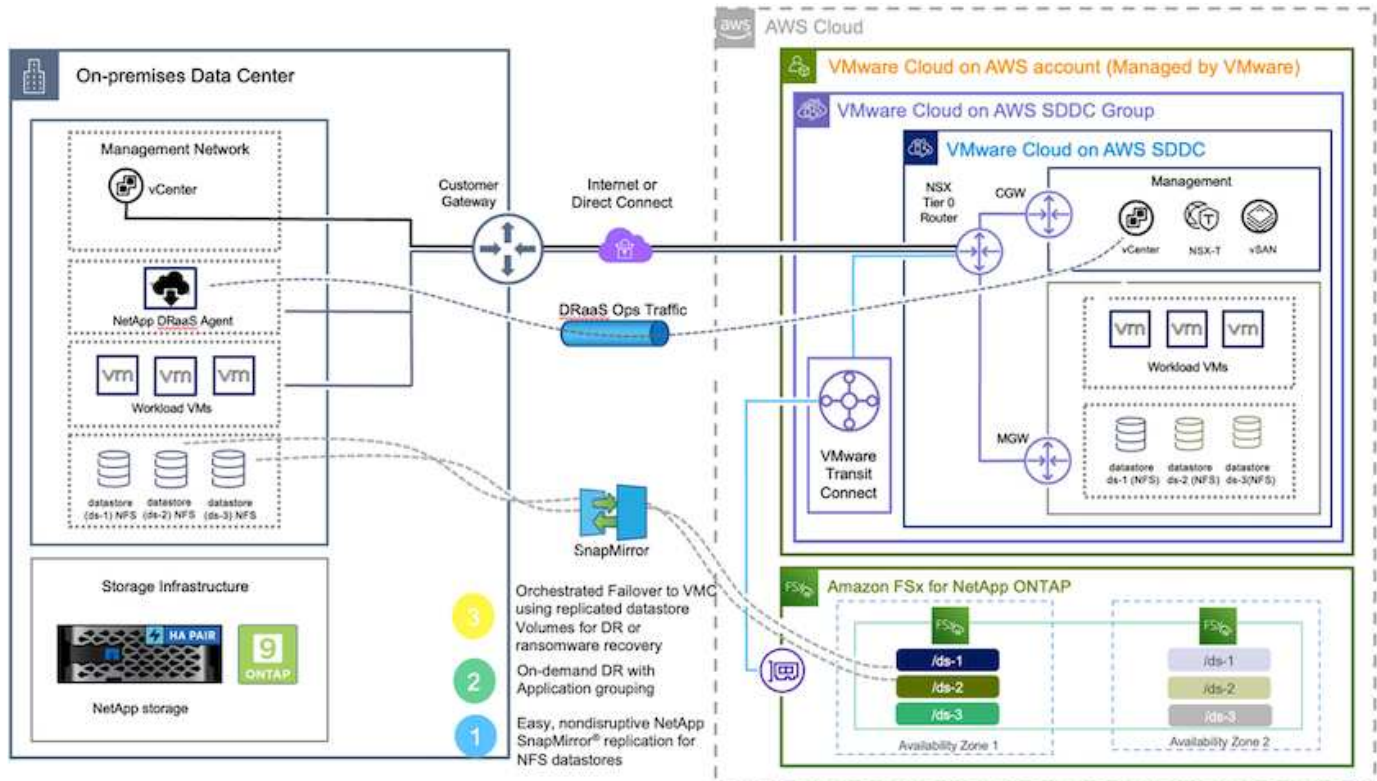
TR-4955：『Disaster Recovery with FSX for ONTAP and VMC（AWS VMware Cloud）』

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テクノロジーを使用すると、オンプレミスのVMwareワークロードをAWSで実行されるFSX for 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解決策）を使用すると、オンプレミスからFSX for 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VMの登録からVMCへのSnapMirrorレベルからNSXで直接ネットワーク・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エコシステム内の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、次の手順を実行します ["リンク"](#)。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。

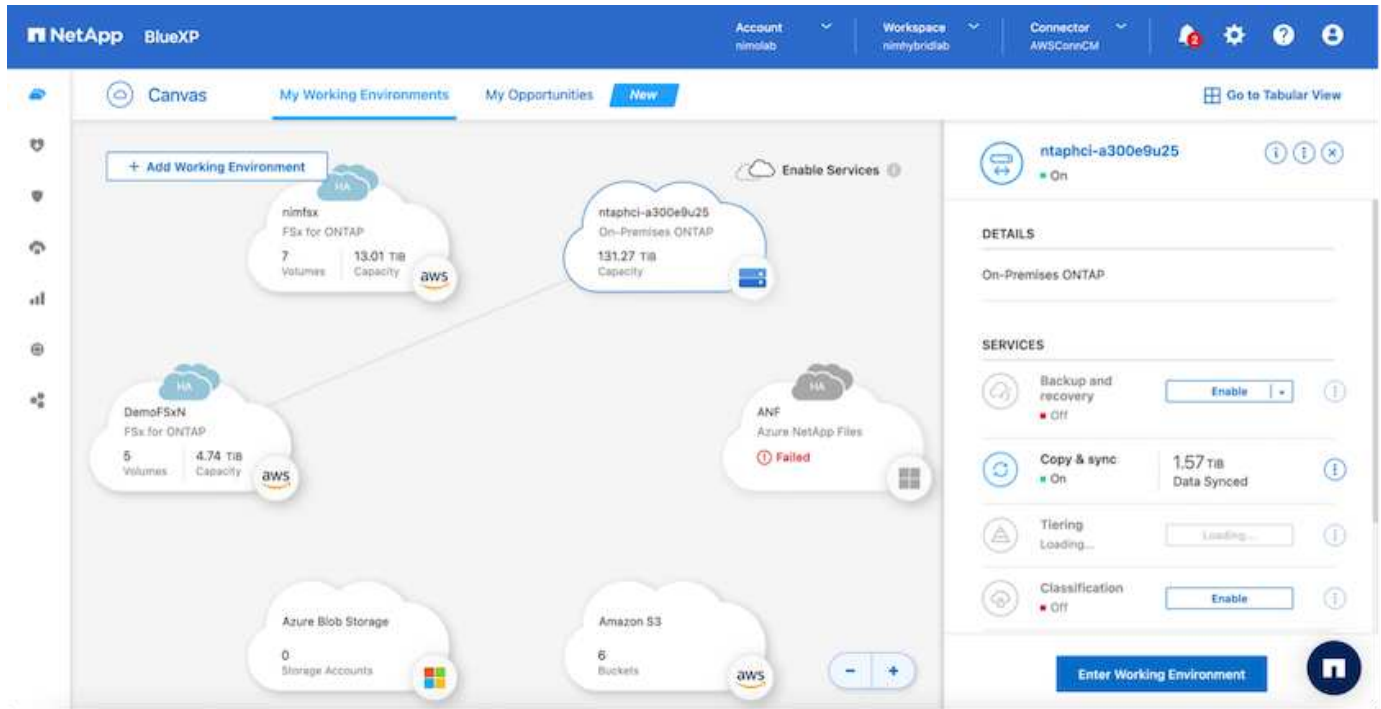
ONTAP のFSXをプロビジョニングして構成します

Amazon FSX for NetApp ONTAP はフルマネージドサービスで、広く普及しているNetApp ONTAP ファイルシステムを基盤に、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します。この手

順を実行します **"リンク"** ONTAP のFSXをプロビジョニングおよび構成するには、次の手順を実行します

SnapMirrorをONTAP 用にFSXに導入して設定する

次の手順では、NetApp BlueXPを使用して、AWSインスタンス上のONTAP 用にプロビジョニングされたFSX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適切な頻度でFSX for ONTAP にレプリケートし、ネットアップの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 です
 - docker -構成
 - Jq

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



◦ `deploy.sh` スクリプトは必要な前提条件をすべて実行します。

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。

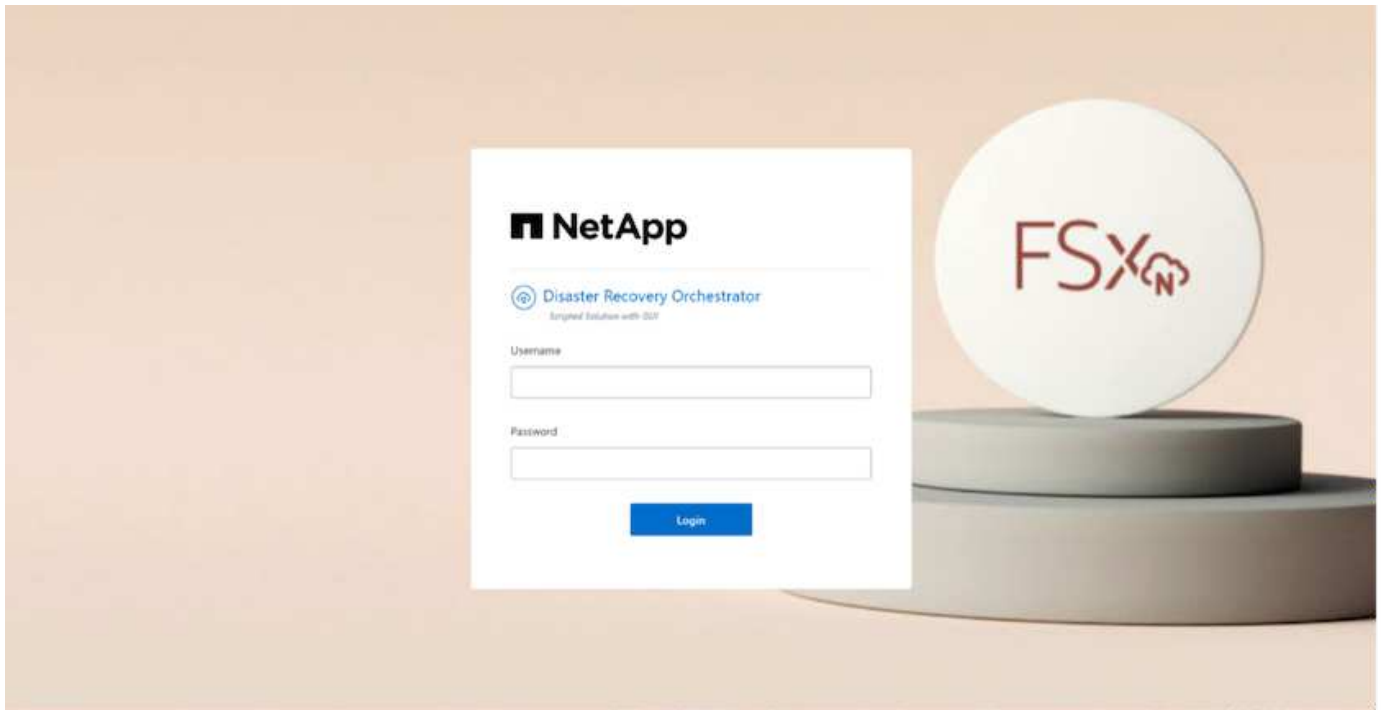
```
https://<host-ip-address>
```

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。



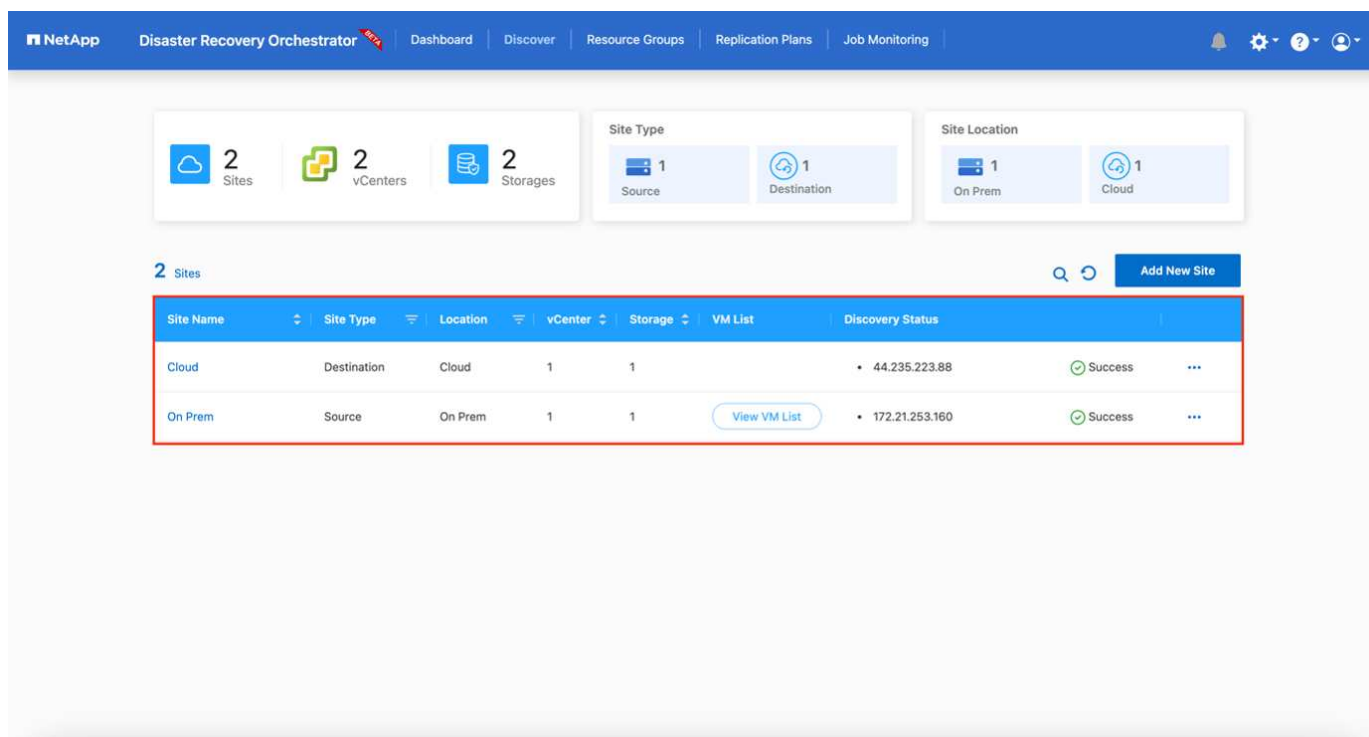
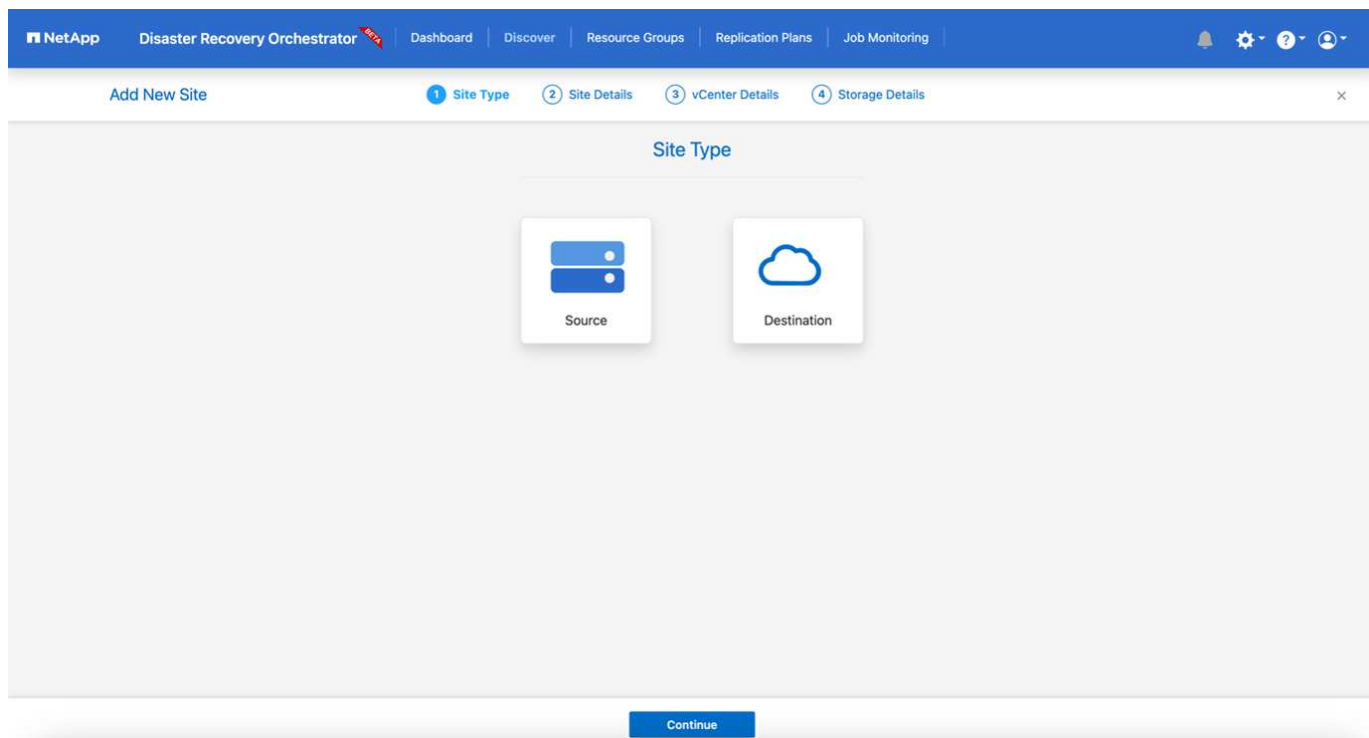
DRO構成

FSX for ONTAP およびVMCが適切に構成されると、FSX for ONTAP 上の読み取り専用SnapMirrorコピーを使用して、オンプレミスのワークロードをVMCに自動でリカバリするためのDROの設定を開始できます。

AWSでDROエージェントを導入し、FSX for ONTAP が導入されているVPCにも導入することを推奨します（ピア接続も可能です）。DROエージェントがネットワーク経由でオンプレミスコンポーネントおよびFSX for ONTAP およびVMCリソースと通信できるようにします。

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 for ONTAP の略



追加されると、DROは自動検出を実行し、対応するSnapMirrorレプリカがソースストレージからFSX for ONTAPにある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。

NetApp Disaster Recovery Orchestrator Dashboard Discover Resource Groups Replication Plans Job Monitoring

Back VM List Site: On Prem | vCenter: 172.21.253.160

10 Datastores 219 Virtual Machines

VM Protection 3 Protected 216 Unprotected

38 VMs Create Resource Group

VM Name	VM Status	VM State (1)	DataStore	CPU	Memory (MB)
a300-vcas02	Not Protected	Powered On	A300_NFS_DS04	16	65536
PFSense	Not Protected	Powered On	A300_NFS_DS04	4	8192
PFSense260	Not Protected	Powered On	A300_NFS_DS04	4	16384
NimDC02	Not Protected	Powered On	A300_NFS_DS04	4	8192
jRBhoja-187	Not Protected	Powered On	A300_NFS_DS04	4	16384
jNimo-187	Not Protected	Powered On	A300_NFS_DS04	4	16384
NimMSDesktop	Not Protected	Powered On	A300_NFS_DS04	8	12288

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。

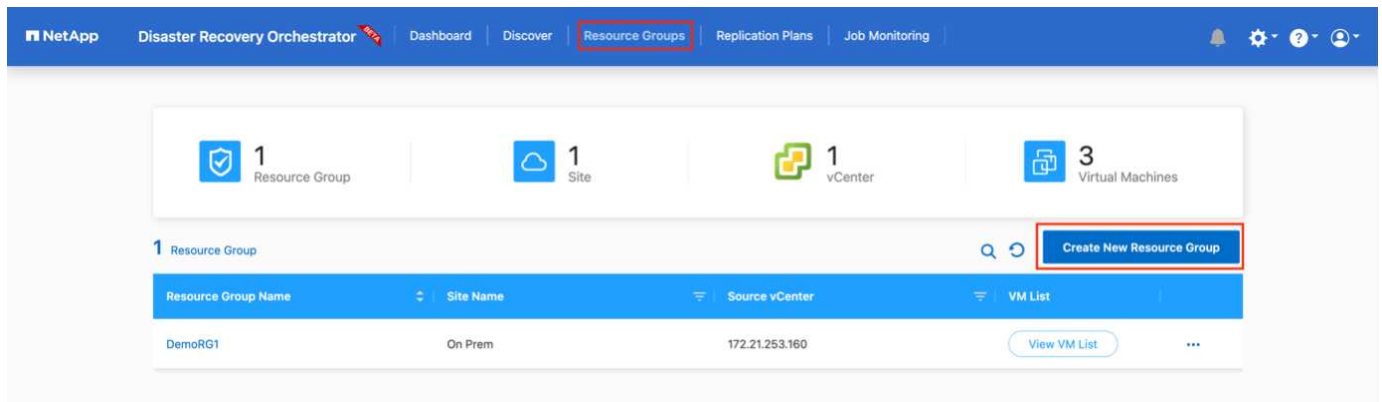
リソースグループの作成を開始するには、次の手順を実行します。

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。

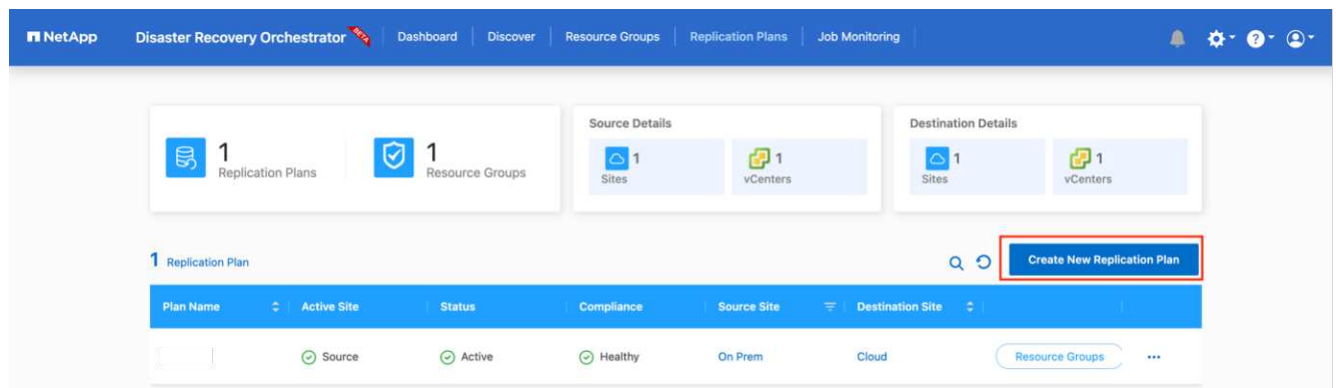


レプリケーションプラン

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。

NetApp Disaster Recovery Orchestrator | Dashboard | Discover | Resource Groups | **Replication Plans** | Job Monitoring

Create New Replication Plan | 1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

Replication Plan Details

Plan Name

Recovery Mapping

Source Site Destination Site

Source vCenter Destination vCenter

! Pre-requisite - You must configure SnapMirror relationships between the source site and target site to create successful replication plan

[Continue](#)

- 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。

NetApp Disaster Recovery Orchestrator | Dashboard | Discover | Resource Groups | **Replication Plans** | Job Monitoring

Create New Replication Plan | 1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

Replication Plan Details

Plan Name

Recovery Mapping

Source Site Destination Site

Source vCenter Destination vCenter

Cluster Mapping

Source Site Resource Destination Site Resource [Add](#)

Source Resource	Destination Resource
A300-Cluster01	Cluster-1 Delete

[Continue](#)

- [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。
- 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。
- 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。
- 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ィステ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。

NetApp Disaster Recovery Orchestrator

Create New Replication Plan

Replication Plan and Site Details | Select Resource Groups | **Set Execution Order** | Set VM Details

Replication Plan Details

Select Execution Order

Resource Group Name	Execution Order
DemoRG1	3

Network Mapping

No more Source/Destination network resources available for mapping

Source Resource	Destination Resource	
VLAN 3375	sddc-cgw-network-1	Delete

DataStore Mapping

Source DataStore	Destination Volume
DRO_Mini	DRO_Mini_copy

Previous Continue

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。

NetApp Disaster Recovery Orchestrator

Dashboard Discover Resource Groups Replication Plans Job Monitoring

Create New Replication Plan Replication Plan and Site Details Select Resource Groups Set Execution Order **Set VM Details**

VM Details

3 VMs

VM Name	No. of CPUs	Memory (MB)	NIC/IP	Boot Order
Resource Group : DemoRG1				
Mini_Test01	1	2048	Static Dynamic	3
Mini_Test02	1	2048	Static Dynamic	2
Mini_Test03	1	2048	Static Dynamic	1

Previous Create Replication Plan

9. レプリケーションプランの作成*をクリックします。

NetApp Disaster Recovery Orchestrator

Dashboard Discover Resource Groups **Replication Plans** Job Monitoring

2 Replication Plans

1 Resource Groups

Source Details

1 Sites 1 vCenters

Destination Details

1 Sites 1 vCenters

2 Replication Plans

Create New Replication Plan

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	
DemoRP	Source	Active	Not Available	On Prem	Cloud	Resource Groups ...
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups ...

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。

NetApp Disaster Recovery Orchestrator **NEW** | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

2 Replication Plans | 1 Resource Groups

Source Details: 1 Sites, 1 vCenters | Destination Details: 1 Sites, 1 vCenters

2 Replication Plans

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups

Plan Details
Edit Plan
Failover
Test Failover
Migrate
Run Compliance
Delete Plan

Failover Details

Volume Snapshot Details

- ☒ Use latest snapshot ⓘ
- ☐ Select specific snapshot ⓘ

Start Failover

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。

NetApp Disaster Recovery Orchestrator **NEW** | Dashboard | Discover | Resource Groups | Replication Plans | **Job Monitoring**

[Back](#)

Failover Steps
Replication Plan: DemoRP

✓	Breaking SnapMirror relationships (in parallel)	Success	11.3 Seconds ⓘ
✓	Mounting volumes and creating datastores (in parallel)	Success	34.7 Seconds ⓘ
✓	Registering VMs (in parallel)	Success	13.2 Seconds ⓘ
✓	Powering on VMs in protection group - DemoRG1 - in target	Success	95.8 Seconds ⓘ
✓	Updating replication status	Success	0.5 Seconds ⓘ

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。

NetApp Disaster Recovery Orchestrator **NEW** | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

2 Sites | 2 Replication Groups | 1 Replication Plan | 219 VMs

Protected VMs: 6 Protected | 213 Unprotected

Workloads
2 Virtual Workloads | 1 Storage Workloads

vCenter Subinventory
3 Clusters | 22 Pools
23 Datastores | 45 Networks

Topology Canvas
On Prem: 172.21.253.169 | 172.21.254.219
Cloud: 44.236.221.88 | 44.236.221.89

Execution Info
1 Total Jobs | 0 In Progress

Application Plans

Application Plan	Active Site	Status
DemoRP	Destination	Running in Failover Mode

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。

NetApp Disaster Recovery Orchestrator **NEW** | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

2 Replication Plans | 1 Resource Groups

Source Details: 1 Sites, 1 vCenters | Destination Details: 1 Sites, 1 vCenters

2 Replication Plans

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	
DemoRP	Destination	Running in Failover h	Healthy	On Prem	Cloud	Resource Groups
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups

Plan Details: Reverse Data Sync, Failback

NetApp Disaster Recovery Orchestrator **NEW** | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

Back

Reverse Data Sync Steps
Replication Plan: DemoRP

✓	Powering off VMs in protection group - DemoRG1 - in source	In progress	- ⓘ
✓	Reversing SnapMirror relationships (in parallel)	Initialized	- ⓘ

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。

NetApp Disaster Recovery Orchestrator **NEW** | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

2 Replication Plans | 1 Resource Groups

Source Details: 1 Sites, 1 vCenters | Destination Details: 1 Sites, 1 vCenters

2 Replication Plans

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	
DemoRP	Destination	Active	Healthy	On Prem	Cloud	Resource Groups
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups

Plan Details: Failback

NetApp Disaster Recovery Orchestrator **NEW** | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

Back

Failback Steps

Replication Plan: DemoRP

Powering off VMs in protection group - DemoRG1 - in target	In progress	- ①
Unregistering VMs in target (in parallel)	✓ Initialized	- ①
Unmounting volumes in target (in parallel)	✓ Initialized	- ①
Breaking reverse SnapMirror relationships (in parallel)	✓ Initialized	- ①
Updating VM networks (in parallel)	✓ Initialized	- ①
Powering on VMs in protection group - DemoRG1 - in source	✓ Initialized	- ①
Deleting reverse SnapMirror relationships (in parallel)	✓ Initialized	- ①
Resuming SnapMirror relationships to target (in parallel)	✓ Initialized	- ①

NetApp BlueXPでは、該当するボリリューム（読み書き可能ボリリュームとしてVMCにマッピングされているボリリューム）のレプリケーションの健全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リュームまたはレプリカボリ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コピーを作成し、FlexCloneインスタンスを公開します。FlexCloneインスタンスは、ONTAPのFSX用に追加の物理容量を消費す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

NetApp Disaster Recovery Orchestrator **NEW** | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

2 Sites

1 Resource Group

2 Replication Plans

219 VMs

Protected VMs

3 Protected

216 Unprotected

Environments

2 Virtual Environments

2 Storage Environments

vCenter Summary

3 Clusters

22 Folders

23 Datastores

45 Networks

Execution Jobs

3 Total Jobs

In Progress

Topology Canvas

Immersive View

Replication Plans

Replication Plan	Active Site	Status
DemoRP	Source	Active

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。

利点

- 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テクノロジー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 for ONTAPを使用したVMware Cloud on AWSへのディザスタリカバリ

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

概要

Amazon FSx for NetApp ONTAPとVMware Cloud on AWSの統合は、ネットアップの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。

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 for 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製解決策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 for 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。

また、このアプローチは、VMCのパイロットライトクラスタとFSx for 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 for 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。

[Veeam ReplicationとFSx ONTAP for VMCを使用したDRシナリオの図]

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の設定：VMware Cloud Tech Zoneに関する記事を参照 ["VMware Cloud on AWS integration with Amazon FSx for NetApp ONTAP導入ガイド"](#) 導入するには、VMware Cloud on AWS SDDCとFSx for ONTAPをNFSデータストアとして設定します。（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 for 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 for 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

追加情報については、「考慮事項と制限事項」を参照してください。 ["こちらをご覧ください"](#)。

展開の詳細

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。次へをクリックします。
 - 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。

[DR Veeam FSxイメージ2] | *dr-veeam-fsx-image2.png*

4. [仮想マシン]ステップで、VMware Cloud on AWS SDDCに接続されたFSx for 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 for 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。

[DR Veeam FSxイメージ3] | *dr-veeam-fsx-image3.png*

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 for 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。

[DR Veeam FSxイメージ4] | *dr-veeam-fsx-image4.png*

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。

[DR Veeam FSxイメージ5] | *dr-veeam-fsx-image5.png*

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。

[DR Veeam FSxイメージ6] | *dr-veeam-fsx-image6.png*

10. レプリケーションジョブを定期的に行う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。

[DR Veeam FSxイメージ7] | *dr-veeam-fsx-image7.png*

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。

[DR Veeam FSxイメージ8] | *dr-veeam-fsx-image8.png*

追加情報によるVeeamレプリケーションについては、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。

[DR Veeam FSxイメージ9] | *dr-veeam-fsx-image9.png*

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。

[DR Veeam FSxイメージ10] | *dr-veeam-fsx-image10.png*

レプリケーションジョブを作成するための追加情報については、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レプリカに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。

[DR Veeam FSxイメージ11] | *dr-veeam-fsx-image11.png*

[DR Veeam FSxイメージ12] | *dr-veeam-fsx-image12.png*

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。

[DR Veeam FSxイメージ13] | *dr-veeam-fsx-image13.png*

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。

[DR Veeam FSxイメージ14] | *dr-veeam-fsx-image14.png*



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。

[DR Veeam FSxイメージ15] | *dr-veeam-fsx-image15.png*

[DR Veeam FSxイメージ16] | *dr-veeam-fsx-image16.png*

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、次の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"](#)。

[DR Veeam FSxイメージ17] | *dr-veeam-fsx-image17.png*

[DR Veeam FSxイメージ18] | *dr-veeam-fsx-image18.png*

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。

[DR Veeam FSxイメージ19] | *dr-veeam-fsx-image19.png*

まとめ

FSx for ONTAPデータストア機能を使用すると、Veeamやその他の検証済みサードパーティ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、パイロットライトクラスタを使用して低コストのDR解決策を提供できます。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>

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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