



AWS/VMC에서 워크로드 보호

NetApp Solutions

NetApp
April 20, 2024

목차

AWS/VMC에서 워크로드 보호	1
TR-4931: Amazon Web Services 및 Guest Connect에서 VMware Cloud를 사용한 재해 복구.....	1
Amazon FSx for ONTAP를 사용한 VMware 클라우드에서 Veeam 백업 및 복원	70
TR-4955: ONTAP 및 VMC(AWS VMware Cloud)용 FSx를 통한 재해 복구	102
Veeam Replication 및 FSx for ONTAP를 사용하여 AWS 기반 VMware Cloud로 재해 복구	117

AWS/VMC에서 워크로드 보호

TR-4931: Amazon Web Services 및 Guest Connect에서 VMware Cloud를 사용한 재해 복구

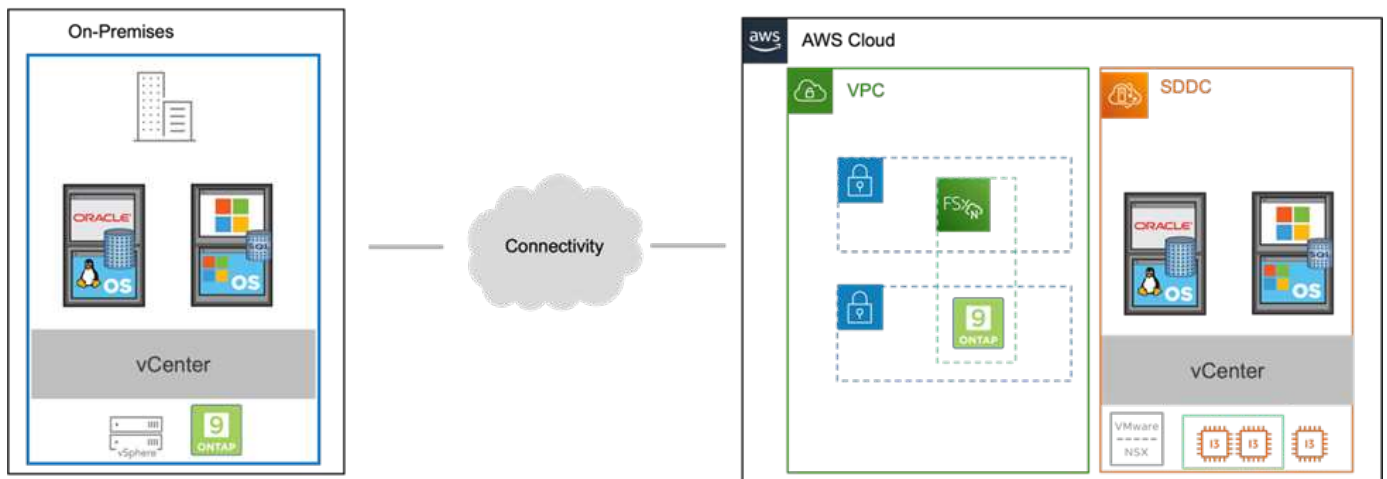
저자: Chris Reno, Josh Powell, Suesh Thoppay - NetApp 솔루션 엔지니어링

개요

조직에서는 중대한 운영 중단이 발생할 경우 비즈니스 크리티컬 애플리케이션을 신속하게 복구할 수 있도록 검증된 DR(재해 복구) 환경과 계획을 반드시 수립해야 합니다. 이 솔루션은 사내 및 AWS 기반의 VMware Cloud 모두에서 VMware 및 NetApp 기술을 중심으로 DR 사용 사례를 시연하는 데 초점을 맞춥니다.

NetApp은 오랫동안 VMware와 통합해왔습니다. 수만 명의 고객이 가상화 환경의 스토리지 파트너로 NetApp을 선택했다는 것이 증명되었습니다. 이러한 통합은 클라우드의 게스트 연결 옵션 및 최근 NFS 데이터 저장소와의 통합에서도 계속됩니다. 이 솔루션은 일반적으로 게스트 연결 스토리지라고 하는 사용 사례에 중점을 둡니다.

게스트 연결 스토리지에서 게스트 VMDK는 VMware 프로비저닝된 데이터 저장소에 구축되고 애플리케이션 데이터는 iSCSI 또는 NFS에 보관되며 VM에 직접 매핑됩니다. 다음 그림과 같이 Oracle 및 MS SQL 애플리케이션을 사용하여 DR 시나리오를 보여 줍니다.



가정, 전제 조건 및 구성 요소 개요

이 솔루션을 구축하기 전에 구성 요소 개요, 솔루션을 구축하는 데 필요한 전제 조건 및 이 솔루션을 문서화하는 데 필요한 가정을 검토하십시오.

"DR 솔루션 요구 사항, 사전 요청 및 계획"

SnapCenter를 사용하여 DR 수행

이 솔루션에서 SnapCenter는 SQL Server 및 Oracle 애플리케이션 데이터에 대해 애플리케이션 정합성이 보장되는 스냅샷을 제공합니다. 이 구성은 SnapMirror 기술과 함께 사내 AFF와 FSx ONTAP 클러스터 간에 고속 데이터 복제를 제공합니다. 또한 Veeam Backup & Replication은 가상 머신에 백업 및 복원 기능을 제공합니다.

이 섹션에서는 백업 및 복원을 위한 SnapCenter, SnapMirror 및 Veeam의 구성에 대해 살펴봅니다.

다음 섹션에서는 보조 사이트에서 페일오버를 완료하는 데 필요한 구성 및 단계에 대해 설명합니다.

SnapMirror 관계 및 보존 일정을 구성합니다

SnapCenter는 장기간 아카이브 및 보존을 위해 운영 스토리지 시스템(운영 > 미러) 및 보조 스토리지 시스템(운영 > 소산) 내의 SnapMirror 관계를 업데이트할 수 있습니다. 이렇게 하려면 SnapMirror를 사용하여 대상 볼륨과 소스 볼륨 간의 데이터 복제 관계를 설정하고 초기화해야 합니다.

소스 및 타겟 ONTAP 시스템은 Amazon VPC 피어링, 전송 게이트웨이, AWS Direct Connect 또는 AWS VPN을 사용하여 피어링된 네트워크에 있어야 합니다.

온프레미스 ONTAP 시스템과 FSx ONTAP 간에 SnapMirror 관계를 설정하려면 다음 단계가 필요합니다.



을 참조하십시오 ["ONTAP용 FSx – ONTAP 사용 설명서"](#) FSx를 사용하여 SnapMirror 관계를 만드는 방법에 대한 자세한 내용은 를 참조하십시오.

소스 및 대상 클러스터간 논리 인터페이스를 기록합니다

사내에 상주하는 소스 ONTAP 시스템의 경우 System Manager 또는 CLI에서 클러스터 간 LIF 정보를 검색할 수 있습니다.

1. ONTAP System Manager에서 네트워크 개요 페이지로 이동하여 FSx가 설치된 AWS VPC와 통신하도록 구성된 Type:Intercluster의 IP 주소를 검색합니다.

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
lif_ora_vsm_614	✓	ora_vsm	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL...	Data	0

2. FSx의 Intercluster IP 주소를 검색하려면 CLI에 로그인하여 다음 명령을 실행합니다.

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

```
FSxId0ae40e08acc0dea67::> network interface show -role intercluster
Vserver      Logical   Status   Network   Current   Current   Is
Interface    Admin/Oper Address/Mask Node       Port      Home
-----
FSxId0ae40e08acc0dea67
inter_1      up/up    172.30.15.42/25  FSxId0ae40e08acc0dea67-01
                                     e0e      true
inter_2      up/up    172.30.14.28/26  FSxId0ae40e08acc0dea67-02
                                     e0e      true
2 entries were displayed.
```

ONTAP와 FSx 간에 클러스터 피어링을 설정합니다

ONTAP 클러스터 간에 클러스터 피어링을 설정하려면 시작 ONTAP 클러스터에 입력된 고유한 암호가 다른 피어 클러스터에서 확인되어야 합니다.

1. 'cluster peer create' 명령을 사용하여 대상 FSx 클러스터에서 피어링을 설정합니다. 메시지가 표시되면 소스 클러스터에서 나중에 사용되는 고유한 암호를 입력하여 생성 프로세스를 마칩니다.

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

2. 소스 클러스터에서 ONTAP System Manager 또는 CLI를 사용하여 클러스터 피어 관계를 설정할 수 있습니다. ONTAP 시스템 관리자에서 보호 > 개요 로 이동하고 피어 클러스터 를 선택합니다.

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. 피어 클러스터 대화 상자에서 필요한 정보를 입력합니다.
 - a. 대상 FSx 클러스터에서 피어 클러스터 관계를 설정하는 데 사용된 암호를 입력합니다.
 - b. 암호화된 관계를 설정하려면 Yes를 선택합니다.

c. 대상 FSx 클러스터의 인터클러스터 LIF IP 주소를 입력합니다.

d. 클러스터 피어링 시작 을 클릭하여 프로세스를 마칩니다.

Peer Cluster

×

Local ————— Remote

STORAGE VM PERMISSIONS

All storage VMs (incl... X

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

1 PASSPHRASE ?

.....

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

2 Yes No

To generate passphrase, Launch Remote Cluster

3 Intercluster Network Interfaces IP Addresses

172.30.15.42

172.30.14.28

Cancel

+ Add

4 Initiate Cluster Peering Cancel

4. 다음 명령을 사용하여 FSx 클러스터에서 클러스터 피어 관계의 상태를 확인합니다.

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

```
FSxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability Authentication
-----
E13A300                1-80-000011      Available      ok
```

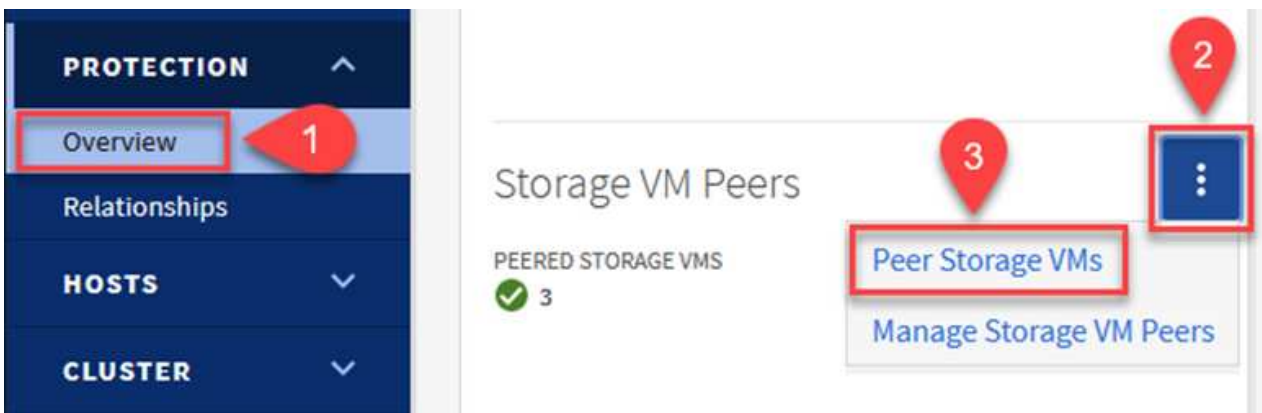
SVM 피어링 관계를 설정합니다

다음 단계는 SnapMirror 관계에 있는 볼륨을 포함하는 소스 스토리지 가상 시스템과 타겟 스토리지 가상 시스템 간에 SVM 관계를 설정하는 것입니다.

1. 소스 FSx 클러스터에서 CLI에서 다음 명령을 사용하여 SVM 피어 관계를 생성합니다.

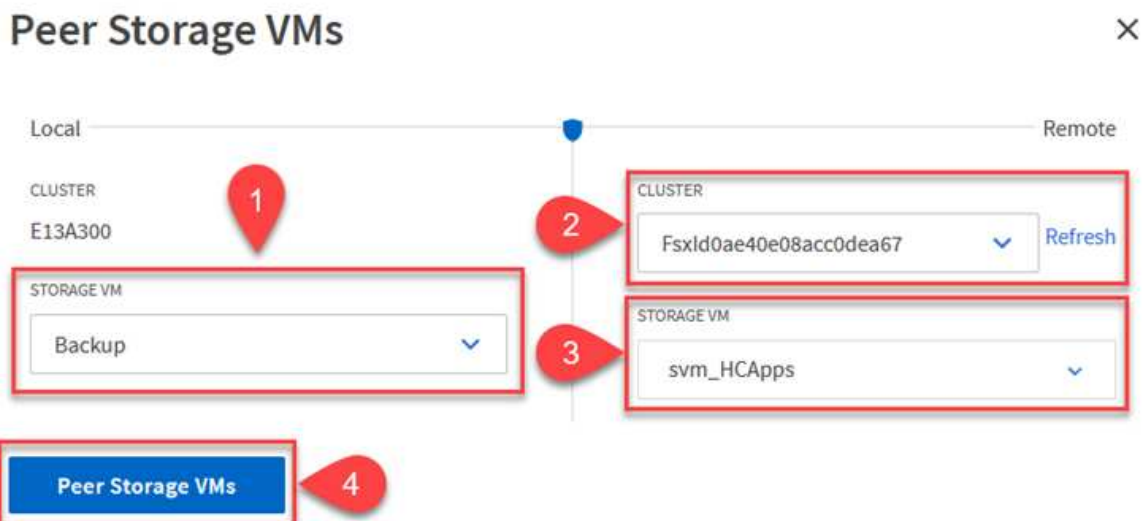
```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver  
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. 소스 ONTAP 클러스터에서 ONTAP System Manager 또는 CLI와 피어링 관계를 수락합니다.
3. ONTAP 시스템 관리자에서 보호 > 개요 로 이동하고 스토리지 VM 피어 아래에서 피어 스토리지 VM 을 선택합니다.



4. 피어 스토리지 VM 대화 상자에서 필수 필드를 입력합니다.

- 소스 스토리지 VM입니다
- 타겟 클러스터
- 대상 스토리지 VM입니다



5. 피어 스토리지 VM 을 클릭하여 SVM 피어링 프로세스를 완료합니다.

SnapCenter는 운영 스토리지 시스템에서 스냅샷 복사본으로 존재하는 백업의 보존 일정을 관리합니다. SnapCenter에서 정책을 생성할 때 설정됩니다. SnapCenter는 보조 스토리지 시스템에 보존되는 백업에 대한 보존 정책을 관리하지 않습니다. 이러한 정책은 보조 FSx 클러스터에서 생성되고 소스 볼륨과 SnapMirror 관계에 있는 대상 볼륨에 연결된 SnapMirror 정책을 통해 별도로 관리됩니다.

SnapCenter 정책을 생성할 때 SnapCenter 백업을 수행할 때 생성되는 각 스냅샷의 SnapMirror 레이블에 추가되는 2차 정책 레이블을 지정할 수 있습니다.



보조 스토리지에서 이러한 레이블은 스냅샷 보존을 적용하기 위해 대상 볼륨과 관련된 정책 규칙과 일치합니다.

다음 예제는 SQL Server 데이터베이스 및 로그 볼륨의 일일 백업에 사용되는 정책의 일부로 생성된 모든 스냅샷에 존재하는 SnapMirror 레이블을 보여줍니다.

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 데이터베이스에 대한 SnapCenter 정책을 만드는 방법에 대한 자세한 내용은 [을 참조하십시오 "SnapCenter 설명서"](#).

우선 유지할 스냅샷 복사본 수를 결정하는 규칙을 사용하여 SnapMirror 정책을 생성해야 합니다.

1. FSx 클러스터에서 SnapMirror 정책을 생성합니다.

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

2. SnapCenter 정책에 지정된 2차 정책 레이블과 일치하는 SnapMirror 레이블을 사용하여 정책에 규칙을 추가합니다.

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

다음 스크립트는 정책에 추가할 수 있는 규칙의 예를 제공합니다.

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



각 SnapMirror 레이블과 유지할 스냅샷 수(보존 기간)에 대한 추가 규칙을 생성합니다.

대상 볼륨을 생성합니다

소스 볼륨에서 스냅샷 복사본을 받을 FSx에 대상 볼륨을 생성하려면 FSx ONTAP에서 다음 명령을 실행합니다.

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

소스 볼륨과 타겟 볼륨 간의 **SnapMirror** 관계를 생성합니다

소스 볼륨과 타겟 볼륨 간에 SnapMirror 관계를 생성하려면 FSx ONTAP에서 다음 명령을 실행합니다.

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

SnapMirror 관계 초기화

SnapMirror 관계를 초기화합니다. 이 프로세스에서는 소스 볼륨에서 생성된 새 스냅샷을 시작하여 타겟 볼륨에 복사합니다.

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

온-프레미스에서 **Windows SnapCenter** 서버를 배포하고 구성합니다.

Windows SnapCenter Server를 사내에 배포합니다

이 솔루션은 NetApp SnapCenter를 사용하여 SQL Server 및 Oracle 데이터베이스의 애플리케이션 정합성이 보장되는 백업을 수행합니다. Veeam Backup & Replication을 사용하여 가상 머신의 VMDK를 백업하면 사내 및 클라우드 기반 데이터 센터를 위한 포괄적인 재해 복구 솔루션을 제공할 수 있습니다.

SnapCenter 소프트웨어는 NetApp Support 사이트에서 제공되며 도메인 또는 작업 그룹에 있는 Microsoft Windows 시스템에 설치할 수 있습니다. 자세한 계획 가이드 및 설치 지침은 에서 확인할 수 있습니다 "[NetApp 문서 센터](#)".

SnapCenter 소프트웨어는 에서 얻을 수 있습니다 "[이 링크](#)".

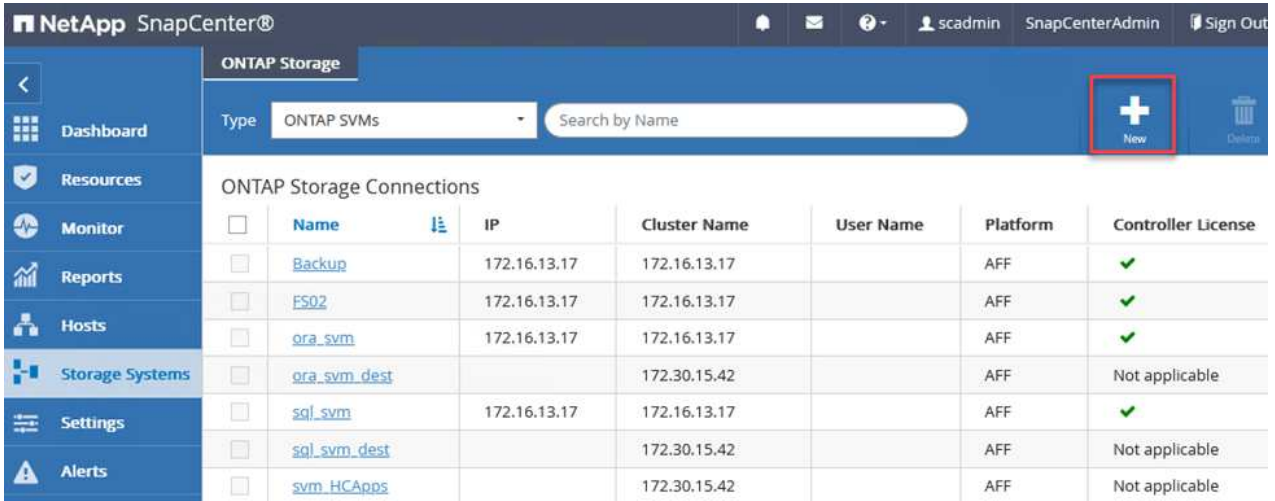
설치가 완료되면 `https://Virtual_Cluster_IP_or_FQDN:8146` 를 사용하여 웹 브라우저에서 SnapCenter 콘솔에 액세스할 수 있습니다.

콘솔에 로그인한 후 백업 SQL Server 및 Oracle 데이터베이스에 대해 SnapCenter를 구성해야 합니다.

SnapCenter에 스토리지 컨트롤러를 추가합니다

SnapCenter에 스토리지 컨트롤러를 추가하려면 다음 단계를 수행하십시오.

1. 왼쪽 메뉴에서 스토리지 시스템을 선택한 다음 새로 만들기 를 클릭하여 스토리지 컨트롤러를 SnapCenter에 추가하는 프로세스를 시작합니다.



The screenshot shows the NetApp SnapCenter web interface. The left sidebar contains navigation links: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems (highlighted), 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, a table titled 'ONTAP Storage Connections' displays a list of storage connections with columns for Name, IP, Cluster Name, User Name, Platform, and Controller License.

	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. 스토리지 시스템 추가 대화 상자에서 로컬 온-프레미스 ONTAP 클러스터의 관리 IP 주소와 사용자 이름 및 암호를 추가합니다. 그런 다음 제출 을 클릭하여 스토리지 시스템 검색을 시작합니다.

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..

- 이 과정을 반복하여 FSx ONTAP 시스템을 SnapCenter에 추가합니다. 이 경우 Add Storage System 창의 아래쪽에 있는 More Options 를 선택하고 Secondary 의 확인란을 클릭하여 FSx 시스템을 SnapMirror 복사본 또는 기본 백업 스냅샷으로 업데이트된 보조 스토리지 시스템으로 지정합니다.

More Options




Platform FAS

☒ Secondary 

Protocol HTTPS

Port 443

Timeout 60 seconds 

☐ Preferred IP 

Save

Cancel

SnapCenter에 스토리지 시스템을 추가하는 방법에 대한 자세한 내용은 [에서 설명서를 참조하십시오 "이 링크"](#).

SnapCenter에 호스트를 추가합니다

다음 단계는 SnapCenter에 호스트 애플리케이션 서버를 추가하는 것입니다. 이 프로세스는 SQL Server와 Oracle에서 모두 비슷합니다.

1. 왼쪽 메뉴에서 호스트를 선택한 다음 추가를 클릭하여 스토리지 컨트롤러를 SnapCenter에 추가하는 프로세스를 시작합니다.
2. 호스트 추가 창에서 호스트 유형, 호스트 이름 및 호스트 시스템 자격 증명을 추가합니다. 플러그인 유형을 선택합니다. SQL Server의 경우 Microsoft Windows 및 Microsoft SQL Server 플러그인을 선택합니다.

NetApp SnapCenter®

Managed Hosts

Search by Name

	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. Oracle의 경우 호스트 추가 대화 상자에서 필수 필드를 입력하고 Oracle Database 플러그인의 확인란을 선택합니다. 그런 다음 제출을 클릭하여 검색 프로세스를 시작하고 호스트를 SnapCenter에 추가합니다.

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...

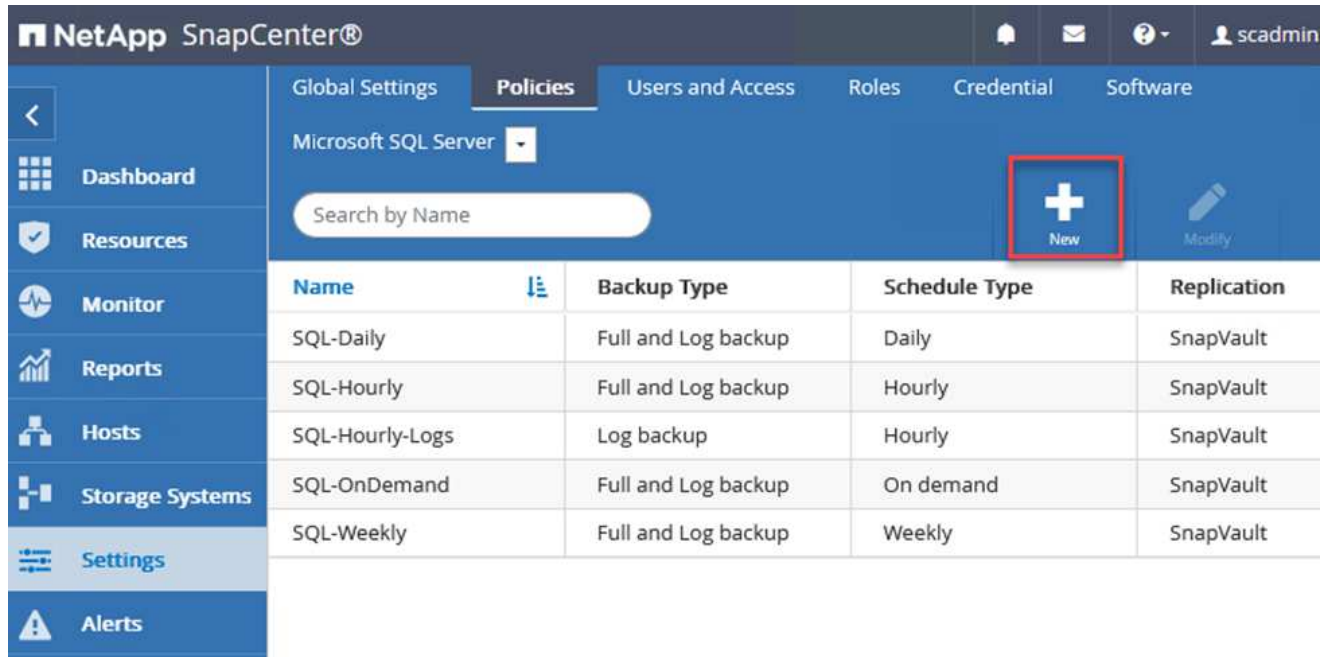
Submit

Cancel

SnapCenter 정책을 생성합니다

정책은 백업 작업에 대해 따라야 할 특정 규칙을 설정합니다. 여기에는 백업 일정, 복제 유형 및 SnapCenter에서 트랜잭션 로그 백업 및 잘라내기를 처리하는 방식이 포함되며 이에 국한되지 않습니다.

SnapCenter 웹 클라이언트의 설정 섹션에서 정책에 액세스할 수 있습니다.



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 백업에 대한 정책을 생성하는 방법에 대한 자세한 내용은 ["SnapCenter 설명서"](#)를 참조하십시오.

Oracle 백업에 대한 정책을 생성하는 방법에 대한 자세한 내용은 ["SnapCenter 설명서"](#)를 참조하십시오.

- 참고: *
- 정책 생성 마법사를 진행하는 동안 복제 섹션을 특별히 기록해 둡니다. 이 섹션에서는 백업 프로세스 중에 사용할 보조 SnapMirror 복사본의 유형을 설명합니다.
- “로컬 스냅샷 복사본을 생성한 후 SnapMirror 업데이트” 설정은 동일한 클러스터에 상주하는 두 스토리지 가상 시스템 사이에 SnapMirror 관계가 존재하는 경우 SnapMirror 관계를 업데이트하는 것을 의미합니다.
- “로컬 스냅샷 복사본을 만든 후 SnapVault 업데이트” 설정은 두 개의 개별 클러스터와 온-프레미스 ONTAP 시스템과 Cloud Volumes ONTAP 또는 FSxN 사이에 존재하는 SnapMirror 관계를 업데이트하는 데 사용됩니다.

다음 이미지는 이전 옵션과 백업 정책 마법사에서 이러한 옵션이 표시되는 방식을 보여 줍니다.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

Select secondary replication options i

☐ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label Choose i

Error retry count 3 i

SnapCenter 리소스 그룹을 생성합니다

리소스 그룹을 사용하면 백업에 포함할 데이터베이스 리소스와 해당 리소스에 대해 수행한 정책을 선택할 수 있습니다.

1. 왼쪽 메뉴의 리소스 섹션으로 이동합니다.
2. 창 위쪽에서 작업할 리소스 유형(이 경우 Microsoft SQL Server)을 선택한 다음 새 리소스 그룹을 클릭합니다.

NetApp SnapCenter®

Microsoft SQL Server 1

View Resource Group search by name 2 New Resource Group

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 설명서는 SQL Server 및 Oracle 데이터베이스 모두에 대한 리소스 그룹을 생성하는 단계별 세부 정보를 제공합니다.

SQL 리소스 백업의 경우 에 따릅니다 ["이 링크"](#).

Oracle 리소스 백업에 대해서는 을 참조하십시오 ["이 링크"](#).

Veeam Backup Server를 구축 및 구성합니다

Veeam 백업 및 복제 소프트웨어는 Veeam 스케일 아웃 백업 저장소(SOBR)를 사용하여 애플리케이션 가상 머신을 백업하고 백업 복사본을 Amazon S3 버킷에 아카이빙하는 데 사용됩니다. Veeam을 이 솔루션의 Windows 서버에 구축했습니다. Veeam 구축에 대한 자세한 지침은 ["Veeam Help Center 기술 문서"](#)를 참조하십시오.

Veeam 스케일아웃 백업 저장소를 구성합니다

소프트웨어를 배포하고 라이선스를 받은 후에는 백업 작업을 위한 타겟 스토리지로 SOBR(스케일 아웃 백업 저장소)을 생성할 수 있습니다. 재해 복구를 위해 VM 데이터를 오프 사이트로 백업하는 데에도 S3 버킷을 포함해야 합니다.

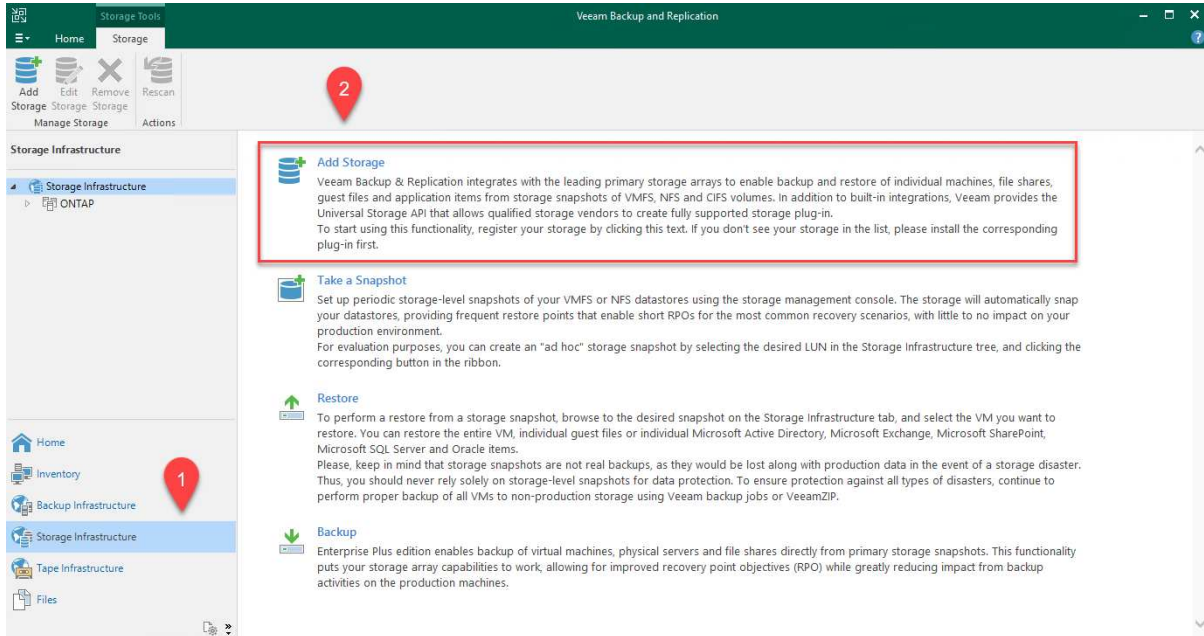
시작하기 전에 다음 필수 구성 요소를 참조하십시오.

1. 백업을 위한 타겟 스토리지로 사내 ONTAP 시스템에 SMB 파일 공유를 생성합니다.
2. SOBR에 포함할 Amazon S3 버킷을 생성합니다. 오프사이트 백업을 위한 저장소입니다.

Veeam에 ONTAP 스토리지를 추가합니다

먼저, Veeam에서 ONTAP 스토리지 클러스터와 관련 SMB/NFS 파일 시스템을 스토리지 인프라로 추가합니다.

1. Veeam 콘솔을 열고 로그인합니다. Storage Infrastructure로 이동한 다음 Add Storage를 선택합니다.



2. 스토리지 추가 마법사에서 NetApp을 스토리지 공급업체로 선택한 다음 Data ONTAP를 선택합니다.
3. 관리 IP 주소를 입력하고 NAS Fileer 상자를 선택합니다. 다음 을 클릭합니다.

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. 자격 증명을 추가하여 ONTAP 클러스터에 액세스합니다.

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 Filer 페이지에서 검사할 프로토콜을 선택하고 Next 를 선택합니다.

New NetApp Data ONTAP Storage ✕

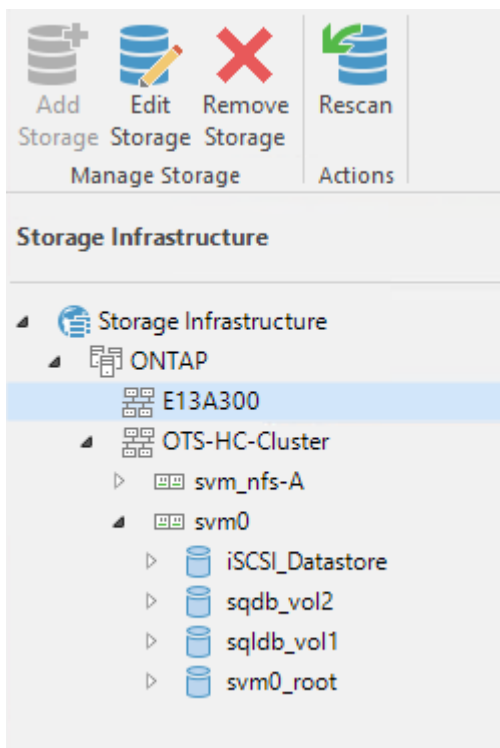
NAS Filer

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

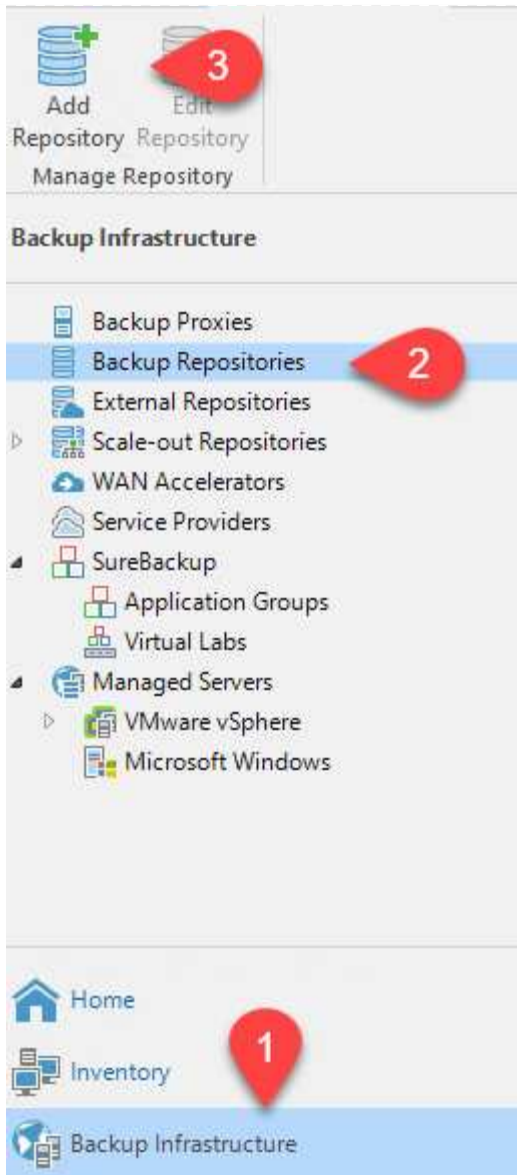
Name	Protocol to use:
Credentials	<input checked="" type="checkbox"/> SMB
NAS Filer	<input type="checkbox"/> NFS
Apply	<input checked="" type="checkbox"/> Create required export rules automatically
Summary	Volumes to scan:
	<input type="text" value="All volumes"/> Choose...
	Backup proxies to use:
	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

< Previous
Apply
Finish
Cancel

6. 마법사의 적용 및 요약 페이지를 완료하고 마침 을 클릭하여 스토리지 검색 프로세스를 시작합니다. 검사가 완료되면 ONTAP 클러스터가 NAS 파일러와 함께 사용 가능한 리소스로 추가됩니다.



7. 새로 검색된 NAS 공유를 사용하여 백업 리포지토리를 생성합니다. Backup Infrastructure에서 Backup Repositories를 선택하고 Add Repository 메뉴 항목을 클릭합니다.



8. 새 백업 저장소 마법사의 모든 단계를 수행하여 리포지토리를 생성합니다. Veeam Backup Repositories 생성에 대한 자세한 내용은 ["Veeam 문서를 참조하십시오"](#).

New Backup Repository

**Share**

Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.

Name

Share

Repository

Mount Server

Review

Apply

Summary

Shared folder:

Browse...

Use \\server\folder format

☒ This share requires access credentials:

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



Add...

[Manage accounts](#)

Gateway server:

☒ Automatic selection☐ The following server:

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

< Previous

Next >

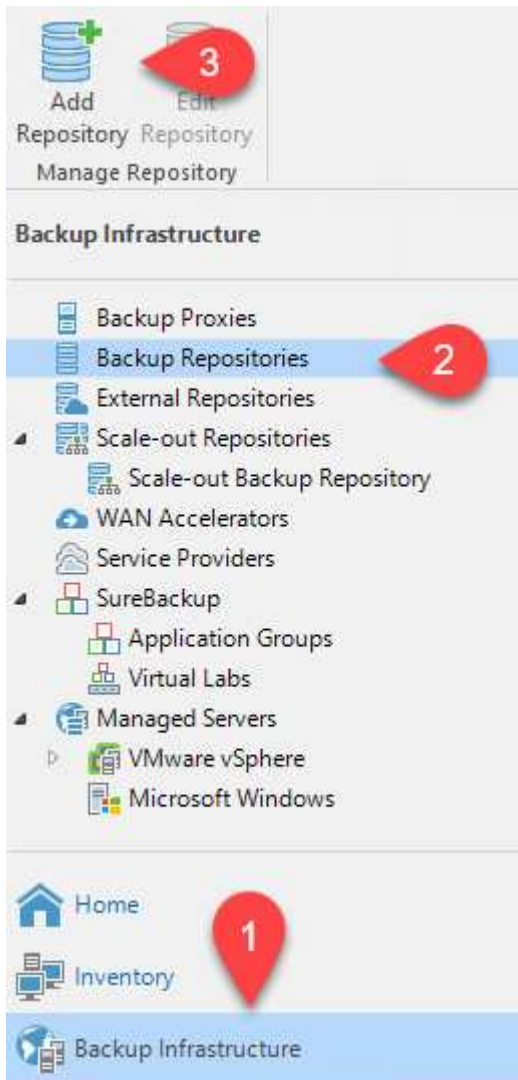
Finish

Cancel

Amazon S3 버킷을 백업 저장소로 추가합니다

다음 단계는 Amazon S3 스토리지를 백업 저장소로 추가하는 것입니다.

1. Backup Infrastructure > Backup Repositories 로 이동합니다. 리포지토리 추가 를 클릭합니다.



2. 백업 저장소 추가 마법사에서 오브젝트 스토리지를 선택한 다음 Amazon S3를 선택합니다. 그러면 New Object Storage Repository 마법사가 시작됩니다.

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.

3. 오브젝트 스토리지 저장소의 이름을 입력하고 Next를 클릭합니다.
4. 다음 섹션에서 자격 증명을 입력합니다. AWS 액세스 키와 비밀 키가 필요합니다.

New Object Storage Repository



Account

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

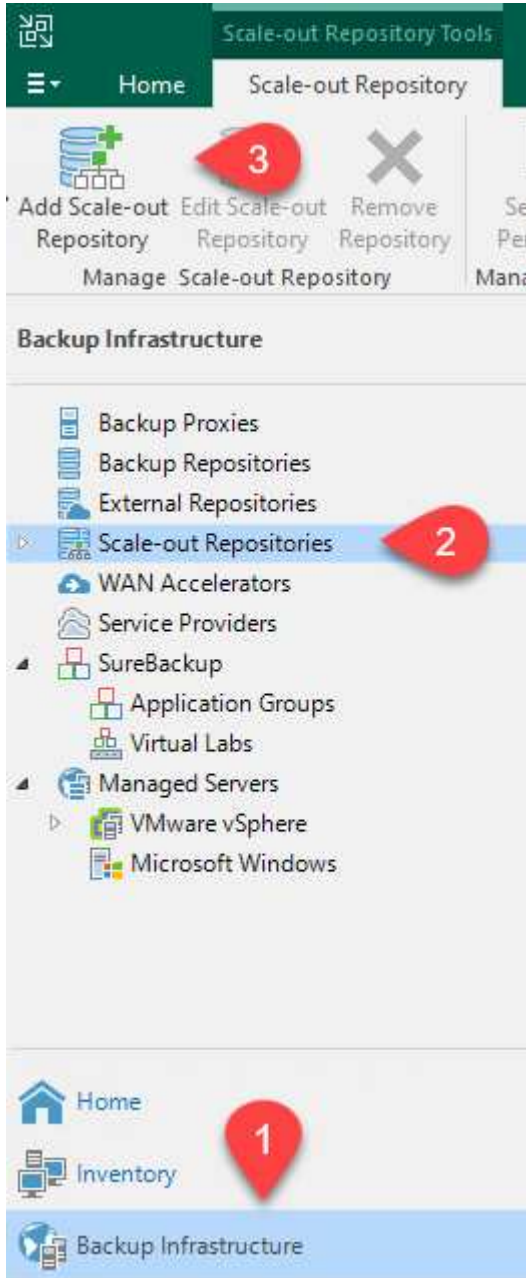
Name	Credentials:
Account	<input type="text" value="AKIAH4H43ZT557HXQT2W (last edited: 107 days ago)"/> Add... Manage cloud accounts
Bucket	AWS region:
Summary	<input type="text" value="Global"/>
<input type="checkbox"/> Use the following gateway server:	
<input type="text" value="veeam.sddc.netapp.com (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 "/>	

5. Amazon 구성이 로드되면 데이터 센터, 버킷 및 폴더를 선택하고 적용 을 클릭합니다. 마지막으로 마침을 클릭하여 마법사를 닫습니다.

스케일아웃 백업 저장소를 생성합니다

이제 Veeam에 스토리지 저장소를 추가했으므로 재해 복구를 위해 SOBR을 생성하여 백업 복사본을 외부 Amazon S3 오브젝트 스토리지에 자동으로 계층화할 수 있습니다.


1. 백업 인프라 에서 스케일 아웃 리포지토리 를 선택한 다음 스케일 아웃 리포지토리 추가 메뉴 항목을 클릭합니다.



2. 새 스케일 아웃 백업 리포지토리에서 SOBR의 이름을 제공하고 다음을 클릭합니다.
3. 성능 계층의 경우 로컬 ONTAP 클러스터에 상주하는 SMB 공유가 포함된 백업 저장소를 선택합니다.

New Scale-out Backup Repository X

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> </tr> </thead> <tbody> <tr> <td>VBRRepo2</td> </tr> </tbody> </table>	Name	VBRRepo2
Name			
VBRRepo2			
Placement Policy			

Add...
Remove

- 배치 정책의 경우 데이터 인접성 또는 요구 사항에 따른 성능 을 선택합니다. 다음을 선택합니다.
- 용량 계층의 경우 Amazon S3 오브젝트 스토리지로 SOBR을 확장합니다. 재해 복구를 위해, 2차 백업을 적시에 제공할 수 있도록 백업이 생성되는 즉시 Copy Backups to Object Storage 를 선택합니다.

New Scale-out Backup Repository X

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	Extents:
Performance Tier	
Placement Policy	
Capacity Tier	<input checked="" type="checkbox"/> Extend scale-out backup repository capacity with object storage: <div> Amazon S3 Repo ▼ Add... </div> <div> Define time windows when uploading to capacity tier is allowed Window... </div> <div> <input checked="" type="checkbox"/> 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. </div> <div> <input checked="" type="checkbox"/> 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... </div> <div> <input type="checkbox"/> Encrypt data uploaded to object storage Password: ▼ Add... Manage passwords </div>
Archive Tier	
Summary	

< Previous Next > Finish Cancel

- 마지막으로 적용 및 마침 을 선택하여 SOBR 생성을 마칩니다.

스케일아웃 백업 저장소 작업을 생성합니다

Veeam을 구성하는 마지막 단계는 새로 생성한 SOBR을 백업 대상으로 사용하여 백업 작업을 생성하는 것입니다. 백업 작업 생성은 스토리지 관리자의 일반적인 일부이며 여기서는 자세한 단계를 다루지 않습니다. Veeam에서 백업 작업 생성에 대한 자세한 내용은 ["Veeam Help Center 기술 문서"](#)를 참조하십시오.

BlueXP 백업 및 복구 톨 및 구성

애플리케이션 VM 및 데이터베이스 볼륨을 AWS에서 실행되는 VMware Cloud Volume 서비스로 페일오버하려면 SnapCenter Server와 Veeam Backup and Replication Server의 실행 중인 인스턴스를 설치 및 구성해야 합니다. 페일오버가 완료된 후 사내 데이터 센터에 대한 페일백이 계획 및 실행될 때까지 정상적인 백업 작업을 재개하도록 이러한 톨을 구성해야 합니다.

보조 Windows SnapCenter 서버를 배포합니다

SnapCenter 서버는 VMware 클라우드 SDDC에 구축하거나 VMware 클라우드 환경에 대한 네트워크 연결을 통해 VPC에 상주하는 EC2 인스턴스에 설치됩니다.

SnapCenter 소프트웨어는 NetApp Support 사이트에서 제공되며 도메인 또는 작업 그룹에 있는 Microsoft Windows 시스템에 설치할 수 있습니다. 자세한 계획 가이드 및 설치 지침은 에서 확인할 수 있습니다 ["NetApp 문서화 센터"](#).

SnapCenter 소프트웨어는 에서 찾을 수 있습니다 ["이 링크"](#).

보조 Windows SnapCenter 서버를 구성합니다

FSx ONTAP에 미러링된 애플리케이션 데이터를 복구하려면 먼저 온-프레미스 SnapCenter 데이터베이스의 전체 복원을 수행해야 합니다. 이 프로세스가 완료되면 VM과의 통신이 다시 설정되고 FSx ONTAP를 기본 스토리지로 사용하여 응용 프로그램 백업을 다시 시작할 수 있습니다.

이를 위해서는 SnapCenter 서버에서 다음 항목을 완료해야 합니다.

1. 원래 온-프레미스 SnapCenter 서버와 동일하게 컴퓨터 이름을 구성합니다.
2. VMware 클라우드 및 FSx ONTAP 인스턴스와 통신하도록 네트워킹을 구성합니다.
3. SnapCenter 데이터베이스를 복원하는 절차를 완료합니다.
4. SnapCenter가 재해 복구 모드에 있는지 확인하여 이제 FSx가 백업용 기본 스토리지인지 확인합니다.
5. 복구된 가상 머신과 통신이 다시 설정되었는지 확인합니다.

이러한 단계를 완료하는 방법에 대한 자세한 내용은 섹션을 참조하십시오 ["SnapCenter 데이터베이스 복원 프로세스"](#).

2차 Veeam Backup & Replication Server를 구축합니다

Veeam Backup & Replication 서버를 AWS의 VMware Cloud 또는 EC2 인스턴스에 설치할 수 있습니다. 자세한 구현 지침은 를 참조하십시오 ["Veeam Help Center 기술 문서"](#).

Secondary Veeam Backup & Replication Server를 구성합니다

Amazon S3 스토리지에 백업된 가상 머신의 복구를 수행하려면 Veeam Server를 Windows 서버에 설치하고 원래 백업 저장소가 포함된 VMware Cloud, FSx ONTAP 및 S3 버킷과 통신하도록 구성해야 합니다. 또한 VM이 복구된 후 새 백업을 수행하려면 FSx ONTAP에 새 백업 리포지토리가 구성되어 있어야 합니다.

이 프로세스를 수행하려면 다음 항목을 완료해야 합니다.

1. 네트워킹을 구성하여 원래 백업 저장소가 포함된 VMware Cloud, FSx ONTAP 및 S3 버킷과 통신합니다.
2. FSx ONTAP에서 SMB 공유를 새 백업 리포지토리로 구성합니다.
3. 사내에서 스케일아웃 백업 저장소의 일부로 사용된 원래 S3 버킷을 마운트합니다.
4. VM을 복구한 후 SQL 및 Oracle VM을 보호하기 위한 새로운 백업 작업을 설정합니다.

Veeam을 사용하여 VM을 복원하는 방법에 대한 자세한 내용은 섹션을 참조하십시오 ["Veeam Full Restore로 애플리케이션 VM을 복구합니다"](#).

재해 복구를 위한 SnapCenter 데이터베이스 백업

SnapCenter를 사용하면 재해 발생 시 SnapCenter 서버를 복구하기 위해 기본 MySQL 데이터베이스와 구성 데이터를 백업 및 복구할 수 있습니다. 이 솔루션을 위해 VPC에 상주하는 AWS EC2 인스턴스에서 SnapCenter 데이터베이스 및 구성을 복구했습니다. 이 단계에 대한 자세한 내용은 [이 링크](#)를 참조하십시오.

SnapCenter 백업 사전 요구 사항

SnapCenter 백업에 필요한 사전 요구 사항은 다음과 같습니다.

- 백업된 데이터베이스 및 구성 파일을 찾기 위해 사내 ONTAP 시스템에서 생성된 볼륨 및 SMB 공유입니다.
- 사내 ONTAP 시스템과 AWS 계정의 FSx 또는 CVO 간 SnapMirror 관계 이 관계는 백업된 SnapCenter 데이터베이스 및 구성 파일이 포함된 스냅샷을 전송하는 데 사용됩니다.
- EC2 인스턴스 또는 VMware Cloud SDDC의 VM에 클라우드 계정에 설치된 Windows Server
- VMware 클라우드의 Windows EC2 인스턴스 또는 VM에 설치된 SnapCenter

SnapCenter 백업 및 복원 프로세스 요약

- 백업 db 및 config 파일을 호스팅하기 위해 사내 ONTAP 시스템에 볼륨을 생성합니다.
- 온프레미스와 FSx/CVO 간에 SnapMirror 관계를 설정합니다.
- SMB 공유를 마운트합니다.
- API 작업을 수행하기 위한 Swagger 인증 토큰을 검색합니다.
- DB 복구 프로세스를 시작합니다.
- xcopy 유틸리티를 사용하여 db 및 config 파일 로컬 디렉토리를 SMB 공유에 복사합니다.
- FSx에서 ONTAP 볼륨의 클론을 생성합니다(사내에서 SnapMirror를 통해 복사됨).
- FSx에서 EC2/VMware Cloud로 SMB 공유를 마운트합니다.
- SMB 공유에서 로컬 디렉토리로 복구 디렉토리를 복사합니다.
- Swagger에서 SQL Server 복원 프로세스를 실행합니다.

SnapCenter 데이터베이스 및 구성을 백업합니다

SnapCenter는 REST API 명령을 실행하기 위한 웹 클라이언트 인터페이스를 제공합니다. Swagger를 통해 REST API에 액세스하는 방법에 대한 자세한 내용은 에서 SnapCenter 설명서를 참조하십시오 ["이 링크"](#).

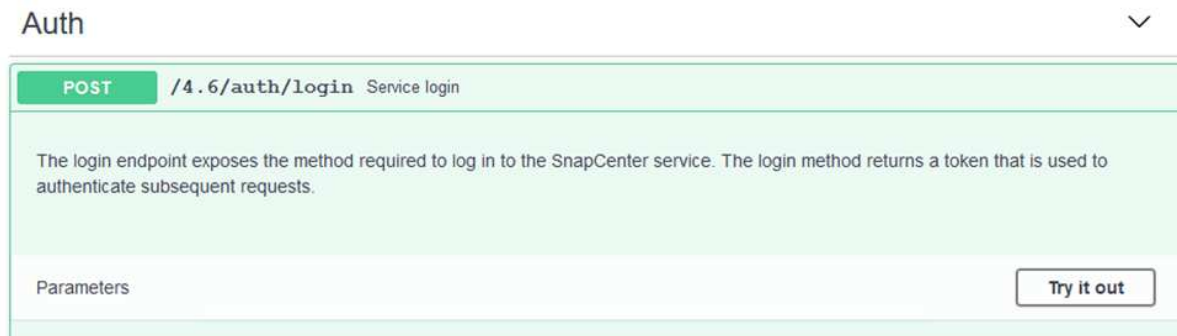
Swagger에 로그인하고 인증 토큰을 얻습니다

Swagger 페이지로 이동한 후 인증 토큰을 검색하여 데이터베이스 복원 프로세스를 시작해야 합니다.

1. <https://<SnapCenter 서버 IP>:8146/swagger/>에서 SnapCenter Swagger API 웹 페이지에 액세스합니다.



2. 인증 섹션을 확장하고 시험 사용 을 클릭합니다.



3. UserOperationContext 영역에서 SnapCenter 자격 증명 및 역할을 입력하고 실행 을 클릭합니다.

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

Execute

4. 아래의 응답 본문에서 토큰을 볼 수 있습니다. 백업 프로세스를 실행할 때 인증을 위해 토큰 텍스트를 복사합니다.

200

Response body


```
{
  "PluginName": null,
  "HostId": 0,
  "RoleId": null,
  "JobIds": null
},
{
  "User": {
    "Token": "K1YxOg==tsV6EOdtdAmAYpe8q5SG6wcoGaSjwME6jrNy5CsY63HQJ5LkoZLIESRNAhpGJJ0UQUynEHdgtVGDZnvx+I/ZJZIn5M1NZrj6CLfGTApplGmcagT08bqb5hM7x07EcdRAidzAXUDb3GyLOKtW0GdwKzSe0wKj3uVupnk1E31skK6PRBv9RS8j0qHQvo4v4RL0hhThhwPhV9/23nFeJVP/p1Ev4vrV/ze2VTUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjqQ==",
    "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 데이터베이스 백업을 수행합니다

그런 다음 Swagger 페이지의 Disaster Recovery 영역으로 이동하여 SnapCenter 백업 프로세스를 시작합니다.

1. 재해 복구 영역을 클릭하여 확장합니다.

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/server/backup' 섹션을 확장하고 try it을 클릭합니다.

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 섹션에서 올바른 로컬 대상 경로를 추가하고 Execute 를 선택하여 SnapCenter 데이터베이스 및 구성의 백업을 시작합니다.



백업 프로세스에서는 NFS 또는 CIFS 파일 공유에 직접 백업할 수 없습니다.

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

SnapCenter에서 백업 작업을 모니터링합니다

데이터베이스 복원 프로세스를 시작할 때 SnapCenter에 로그인하여 로그 파일을 검토합니다. 모니터 섹션에서 SnapCenter 서버 재해 복구 백업의 세부 정보를 볼 수 있습니다.

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'

i 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 유틸리티를 사용하여 SMB 공유에 데이터베이스 백업 파일을 복사합니다

그런 다음 SnapCenter 서버의 로컬 드라이브에서 데이터를 SnapMirror로 복제하는 데 사용되는 CIFS 공유로 AWS의 FSx 인스턴스에 있는 보조 위치로 백업을 이동해야 합니다. 파일 권한을 유지하는 특정 옵션과 함께 xcopy를 사용합니다.

관리자 권한으로 명령 프롬프트를 엽니다. 명령 프롬프트에서 다음 명령을 입력합니다.

```
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
```

페일오버

운영 사이트에서 재해가 발생합니다

운영 사내 데이터 센터에서 재해가 발생할 경우 당사의 시나리오에서는 AWS의 VMware Cloud를 사용하여 Amazon Web Services 인프라에 있는 2차 사이트로 페일오버합니다. 가상 시스템과 사내 ONTAP 클러스터에 더 이상 액세스할 수 없다고 가정합니다. 또한, SnapCenter 및 Veeam 가상 머신을 더 이상 액세스할 수 없으며 2차 사이트에서 다시 구축해야 합니다.

이 섹션에서는 클라우드 환경으로의 인프라 페일오버에 대해 다루며 다음 주제를 다룹니다.

- SnapCenter 데이터베이스 복원 새 SnapCenter 서버가 설정된 후, 보조 FSx 스토리지가 기본 스토리지 장치가 될 수 있도록 MySQL 데이터베이스 및 구성 파일을 복원하고 데이터베이스를 재해 복구 모드로 전환합니다.
- Veeam Backup & Replication을 사용하여 애플리케이션 가상 머신을 복구합니다. VM 백업이 포함된 S3 스토리지를 연결하고 백업을 가져온 다음 AWS의 VMware Cloud로 복원합니다.
- SnapCenter를 사용하여 SQL Server 응용 프로그램 데이터를 복원합니다.
- SnapCenter를 사용하여 Oracle 애플리케이션 데이터를 복구합니다.

SnapCenter는 MySQL 데이터베이스 및 구성 파일의 백업 및 복원을 허용하여 재해 복구 시나리오를 지원합니다. 이를 통해 관리자는 사내 데이터 센터에서 SnapCenter 데이터베이스의 정기적인 백업을 유지하고 나중에 해당 데이터베이스를 보조 SnapCenter 데이터베이스로 복원할 수 있습니다.

원격 SnapCenter 서버에서 SnapCenter 백업 파일에 액세스하려면 다음 단계를 수행하십시오.

1. FSx 클러스터에서 SnapMirror 관계를 중단하여 볼륨을 읽기/쓰기로 만듭니다.
2. 필요한 경우 CIFS 서버를 생성하고 복제된 볼륨의 연결 경로를 가리키는 CIFS 공유를 생성합니다.
3. xcopy를 사용하여 보조 SnapCenter 시스템의 로컬 디렉토리에 백업 파일을 복사합니다.
4. SnapCenter v4.6을 설치합니다.
5. SnapCenter 서버의 FQDN이 원래 서버와 동일한지 확인합니다. 이 작업은 DB 복원이 성공하려면 필요합니다.

복원 프로세스를 시작하려면 다음 단계를 수행하십시오.

1. 보조 SnapCenter 서버의 Swagger API 웹 페이지로 이동하고 이전 지침에 따라 인증 토큰을 얻습니다.
2. Swagger 페이지의 Disaster Recovery 섹션으로 이동하여 "/4.6/disasterrecovery/server/restore"를 선택하고 Try It Out을 클릭합니다.

POST /4.6/disasterrecovery/server/restore Starts SnapCenter Server Restore.

Starts SnapCenter Server Restore.

Parameters Try it out

3. 인증 토큰을 붙여 넣고 SmDRResterRequest 섹션에서 백업 이름과 보조 SnapCenter 서버의 로컬 디렉토리를 붙여 넣습니다.

Name	Description
Token * required string (header)	User authorization token
SmDRRestoreRequest * required object (body)	Parameters to take for Restore

Token value: KIYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQt

SmDRRestoreRequest value (JSON):

```
{
  "BackupName": "SnapCenter.sddc.netapp.com_03-23-2022_12.38.00.6713",
  "BackupPath": "C:\\SnapCenter\\"
}
```

4. 실행 버튼을 선택하여 복원 프로세스를 시작합니다.
5. SnapCenter에서 모니터 섹션으로 이동하여 복구 작업의 진행률을 확인합니다.

NetApp SnapCenter®

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. 보조 스토리지에서 SQL Server 복원을 사용하려면 SnapCenter 데이터베이스를 재해 복구 모드로 전환해야 합니다. 이 작업은 별도의 작업으로 수행되며 Swagger API 웹 페이지에서 시작됩니다.
 - a. Disaster Recovery(재해 복구) 섹션으로 이동하여 '/4.6/Disasterrecovery/storage(4.6/Disasterrecovery/storage)'를 클릭합니다.
 - b. 사용자 인증 토큰을 붙여 넣습니다.
 - c. SmSetDisasterRecoverySettingsRequest 섹션에서 EnableDisasterRecover 를 true 로 변경합니다.
 - d. 실행 을 클릭하여 SQL Server에 대한 재해 복구 모드를 활성화합니다.

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



추가 절차에 대한 설명을 참조하십시오.

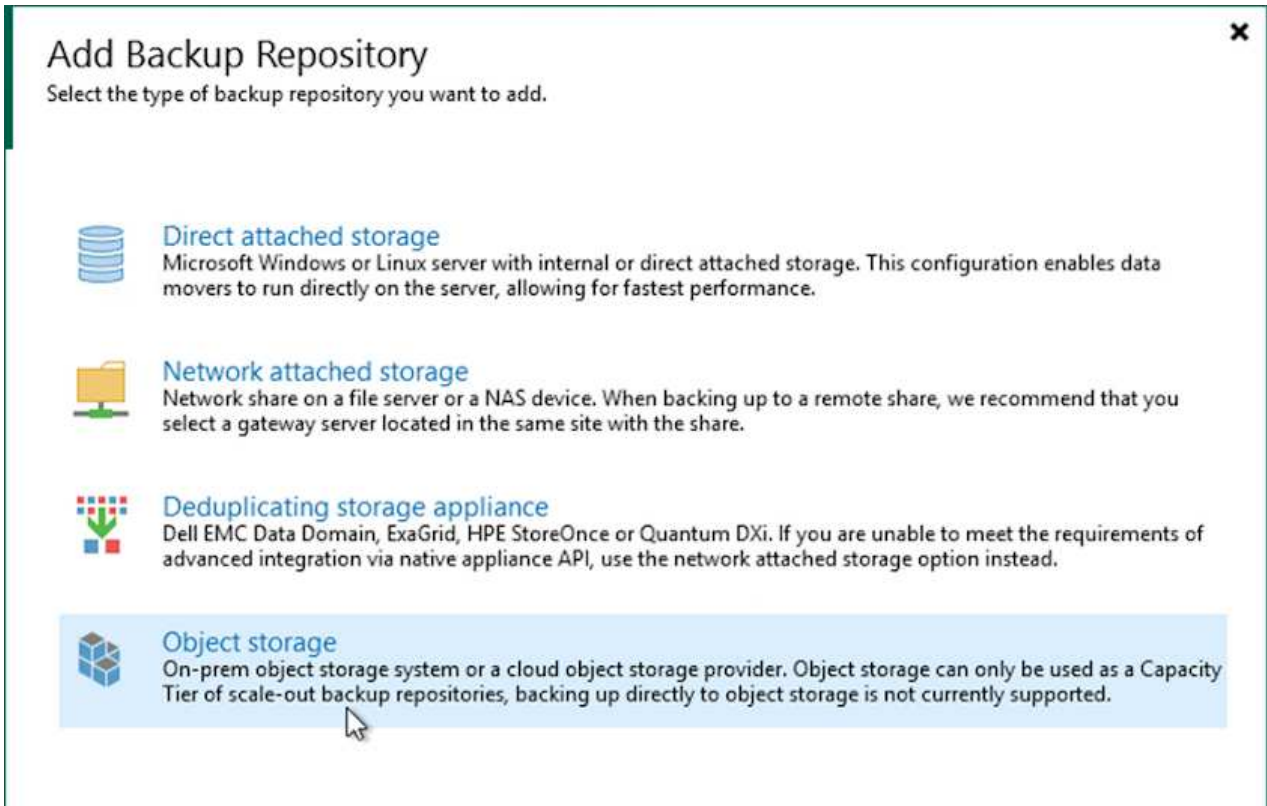
Veeam 전체 복원으로 애플리케이션 **VM**을 복원합니다

백업 리포지토리를 생성하고 S3에서 백업을 가져옵니다

2차 Veeam 서버에서 S3 스토리지의 백업을 가져오고 SQL Server 및 Oracle VM을 VMware Cloud 클러스터로 복원합니다.

사내 스케일아웃 백업 리포지토리에 속하는 S3 오브젝트에서 백업을 가져오려면 다음 단계를 완료합니다.

1. 백업 리포지토리 로 이동하고 상단 메뉴에서 리포지토리 추가 를 클릭하여 백업 리포지토리 추가 마법사를 시작합니다. 마법사의 첫 번째 페이지에서 백업 저장소 유형으로 오브젝트 스토리지 를 선택합니다.



2. 오브젝트 스토리지 유형으로 Amazon S3를 선택합니다.

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 목록에서 Amazon S3를 선택합니다.

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. 드롭다운 목록에서 미리 입력한 자격 증명을 선택하거나 클라우드 스토리지 리소스에 액세스하기 위한 새 자격 증명을 추가합니다. 다음을 클릭하여 계속합니다.

New Object Storage Repository ✕



Account

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

Name	Credentials:
Account	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 5px; background-color: #f0f0f0;">AKIA4H43ZT53YJXPY2Y (last edited: 33 days ago)</div> <div style="margin-left: 5px;">▼</div> <div style="margin-left: 10px; border: 1px solid #ccc; padding: 2px 5px;">Add...</div> </div> <div style="text-align: right; margin-top: 5px;">Manage cloud accounts</div>
Bucket	AWS region:
Summary	<div style="border: 1px solid #ccc; padding: 2px 5px; background-color: #f0f0f0;">Global</div> <div style="text-align: right; margin-top: 5px;">▼</div>

☐ Use the following gateway server:


EC2AMAZ-3POTKQV (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.

< Previous
Next >
Finish
Cancel

5. 버킷 페이지에서 데이터 센터, 버킷, 폴더 및 원하는 옵션을 입력합니다. 적용 을 클릭합니다.

New Object Storage Repository

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

Name	Data center: US East (N. Virginia)
Account	
Bucket	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.

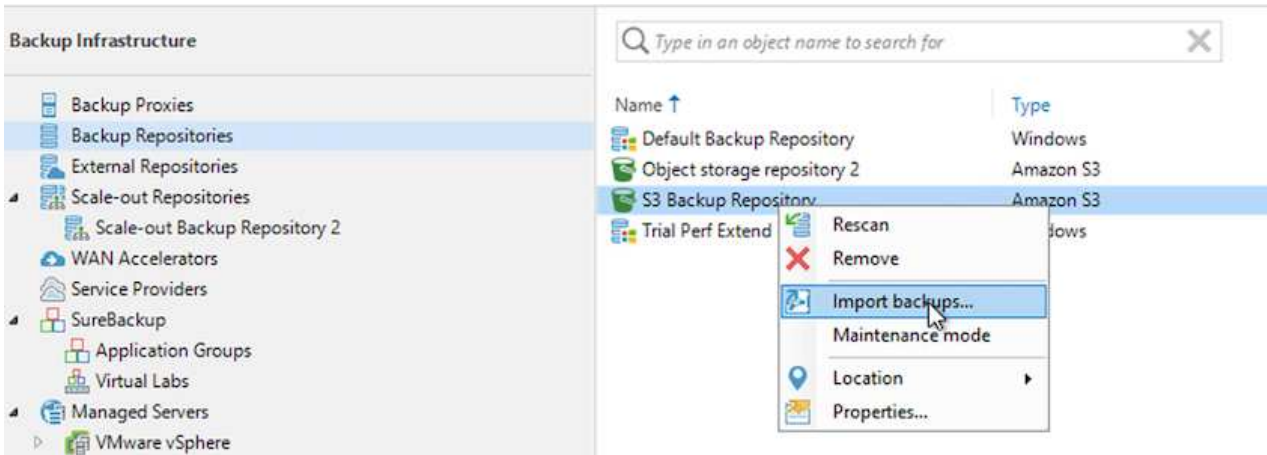
☐ Store backups in a single availability zone (even lower price per GB, reduced resilience)

< Previous **Apply** Finish Cancel

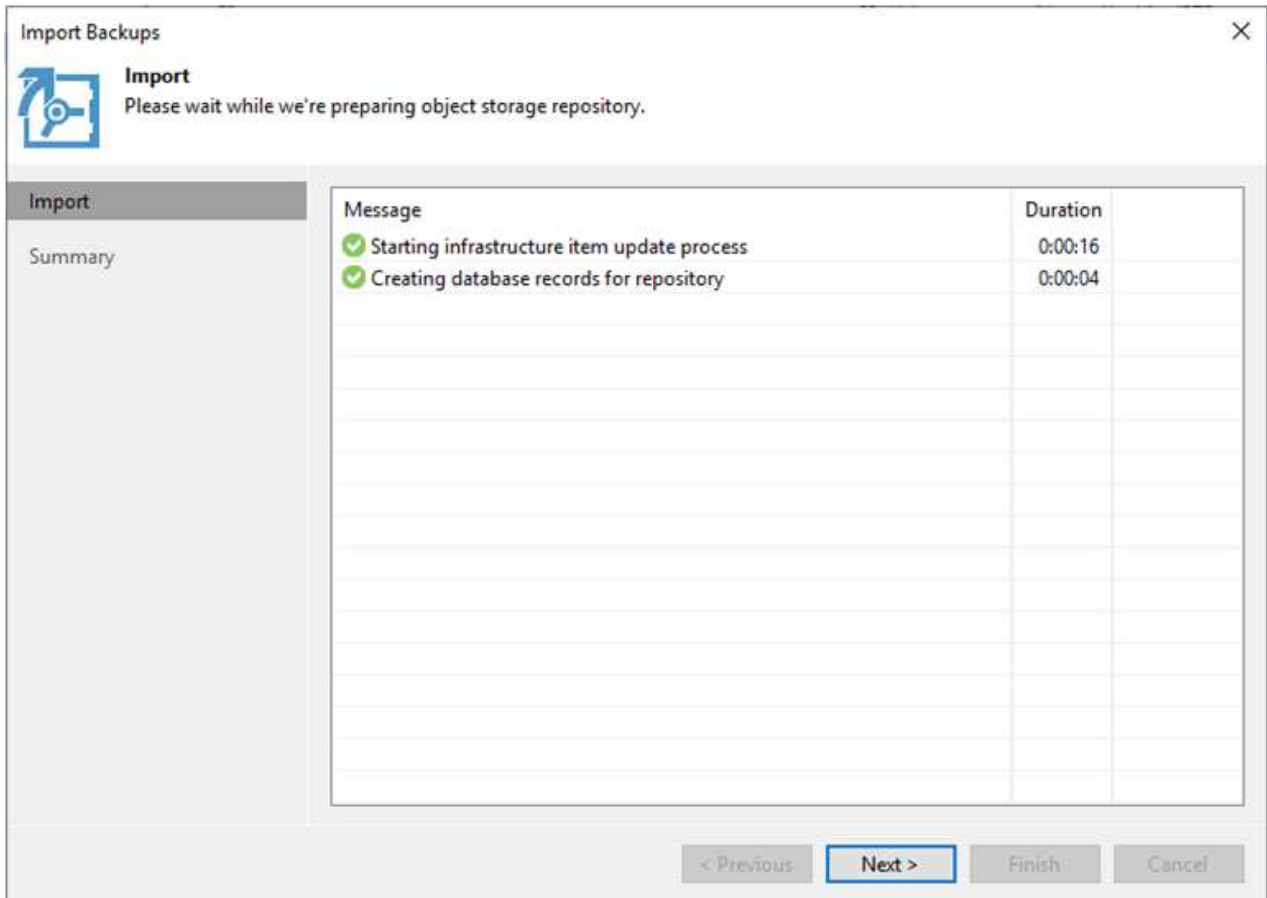
6. 마지막으로 마침 을 선택하여 프로세스를 완료하고 리포지토리를 추가합니다.

이전 섹션에 추가된 S3 리포지토리에서 백업을 가져오려면 다음 단계를 완료합니다.

1. S3 백업 리포지토리에서 백업 가져오기 를 선택하여 백업 가져오기 마법사를 시작합니다.



2. 가져오기에 대한 데이터베이스 레코드가 생성된 후 요약 화면에서 다음 을 선택한 다음 마침 을 선택하여 가져오기 프로세스를 시작합니다.



3. 가져오기가 완료되면 VM을 VMware Cloud 클러스터로 복구할 수 있습니다.

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

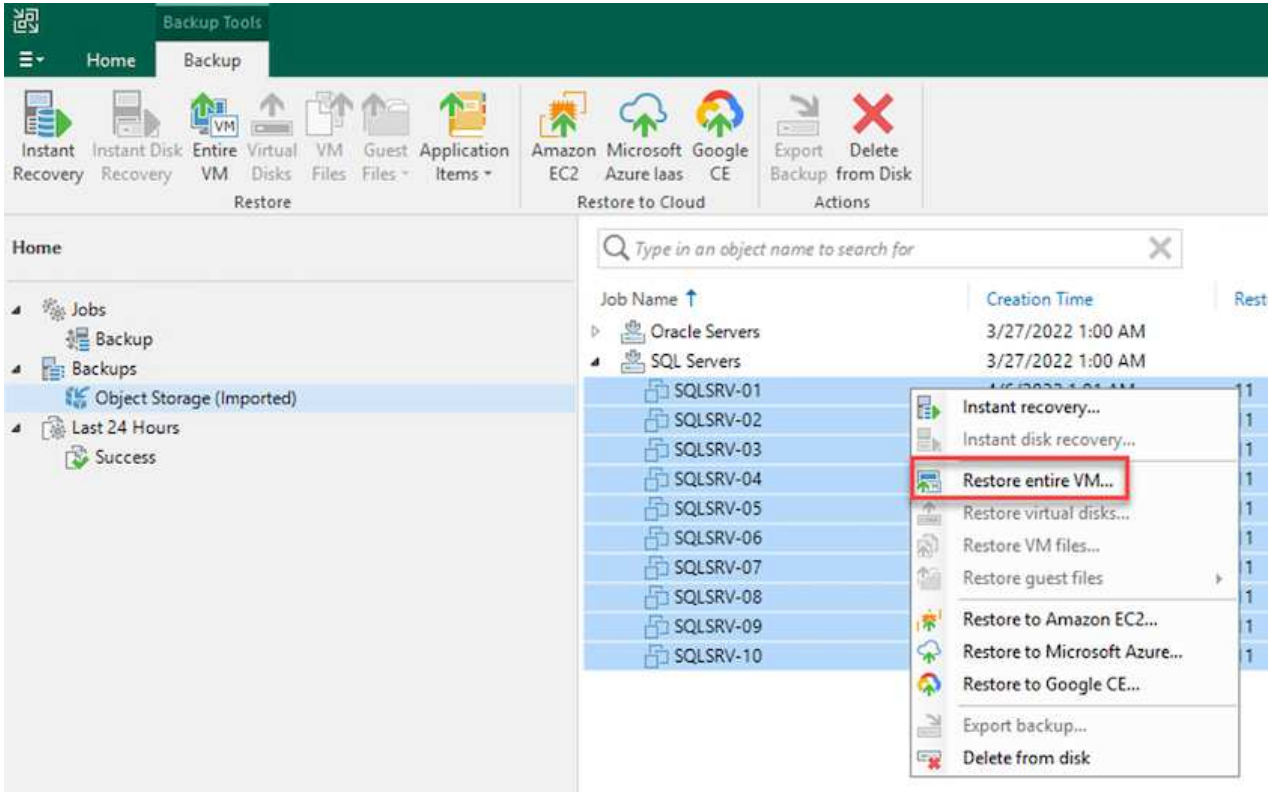
Message	Duration
✓ Starting backup repositories synchronization	
✓ Enumerating repositories	
✓ Found 1 repository	
✓ Processing capacity tier extent of S3 Backup Repository 2	0:03:23
✓ S3 Backup Repository: added 2 unencrypted	0:03:20
✓ Importing backup 2 out of 2	0:03:15
✓ Backup repositories synchronization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

Close

Veeam을 사용하여 애플리케이션 VM을 VMware Cloud로 완벽하게 복구합니다


SQL 및 Oracle 가상 머신을 AWS 워크로드 도메인/클러스터의 VMware Cloud로 복구하려면 다음 단계를 수행하십시오.

1. Veeam Home 페이지에서 가져온 백업이 포함된 객체 스토리지를 선택하고 복구할 VM을 선택한 다음 마우스 오른쪽 버튼을 클릭하고 Restore Entire VM을 선택합니다.



2. 전체 VM 복원 마법사의 첫 페이지에서 원하는 경우 백업할 VM을 수정하고 다음을 선택합니다.

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.

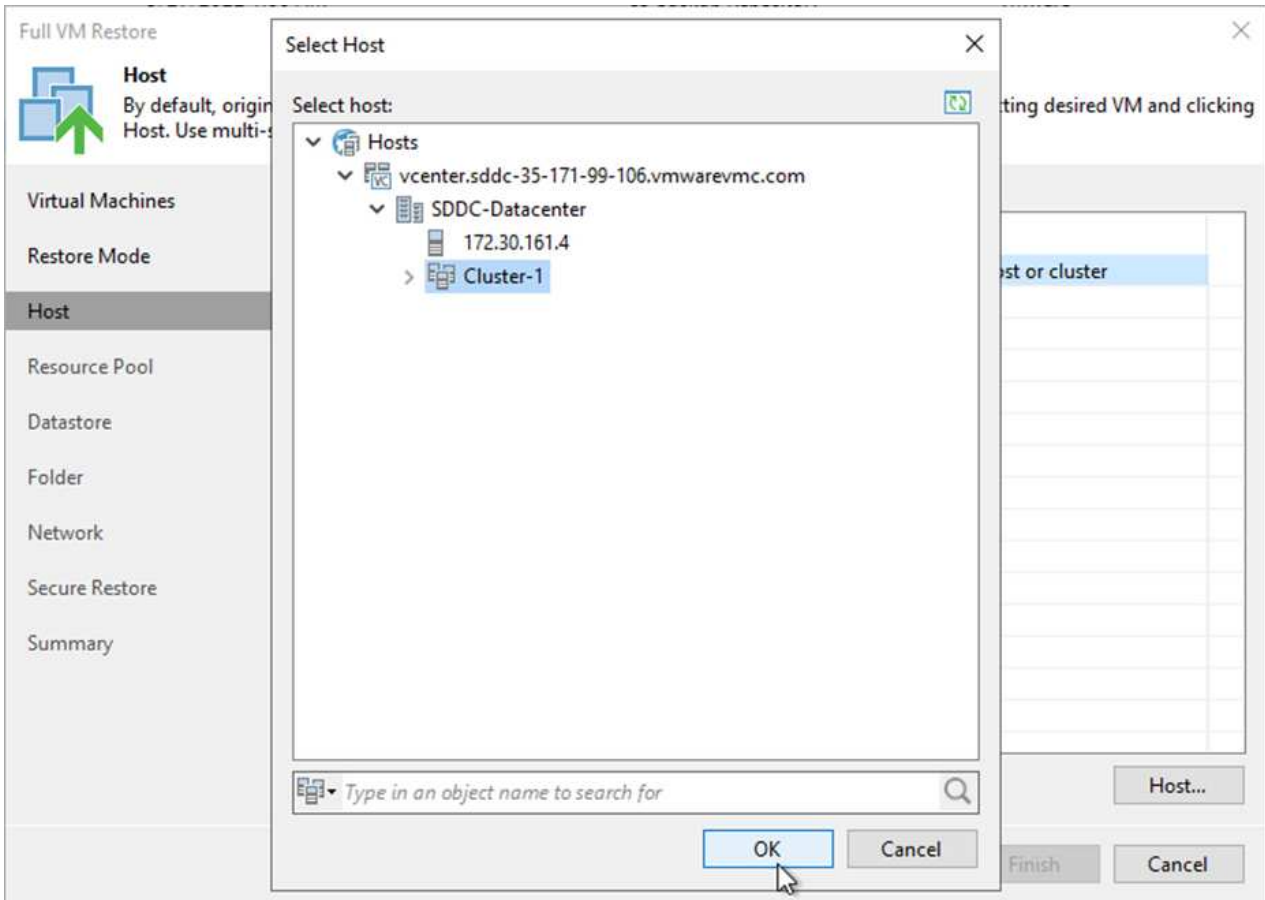
< Previous

Next >

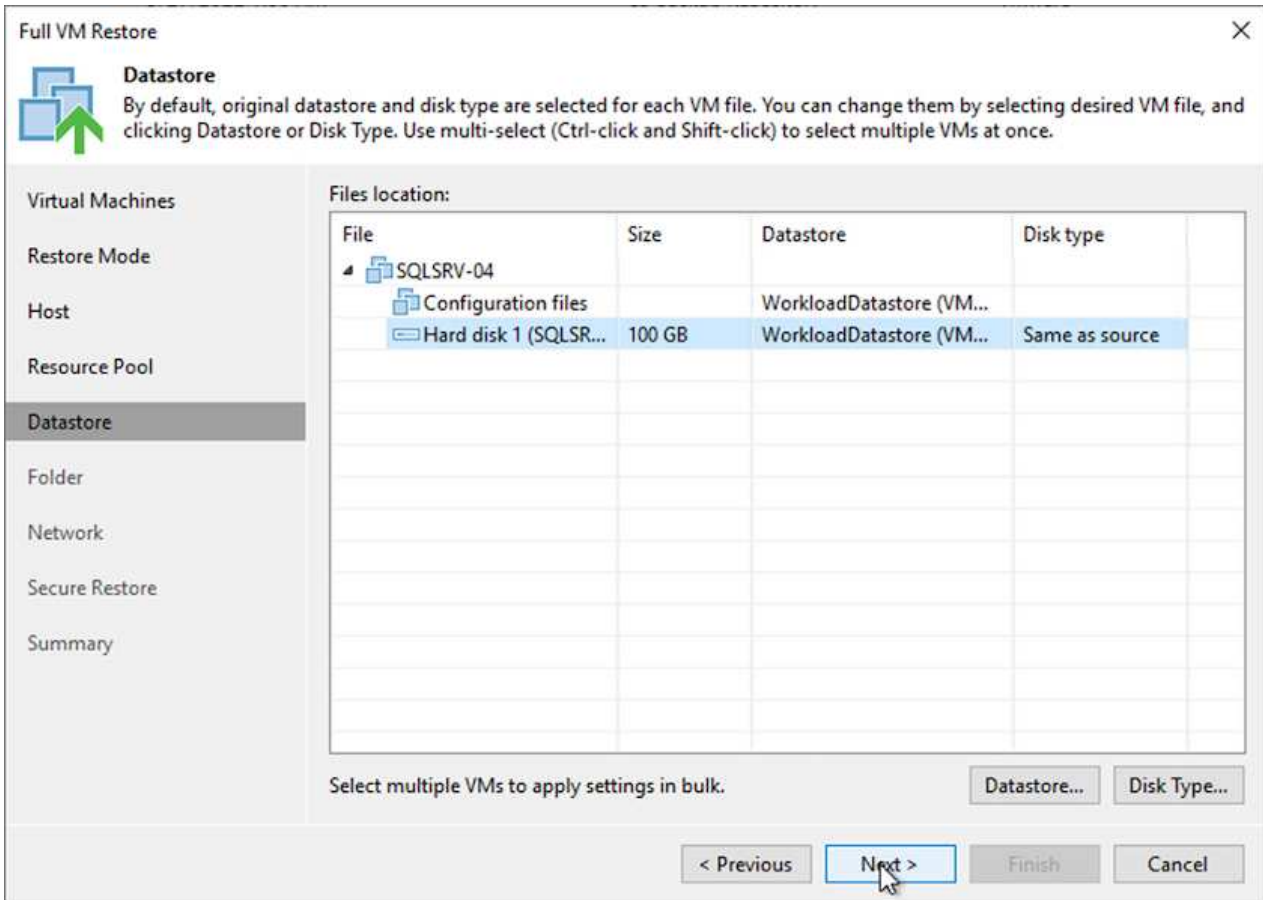
Finish

Cancel

4. 호스트 페이지에서 VM을 복구할 타겟 ESXi 호스트 또는 클러스터를 선택합니다.



5. Datastores 페이지에서 구성 파일과 하드 디스크 모두에 대한 타겟 데이터 저장소 위치를 선택합니다.



6. 네트워크 페이지에서 VM의 원래 네트워크를 새 대상 위치의 네트워크에 매핑합니다.

×

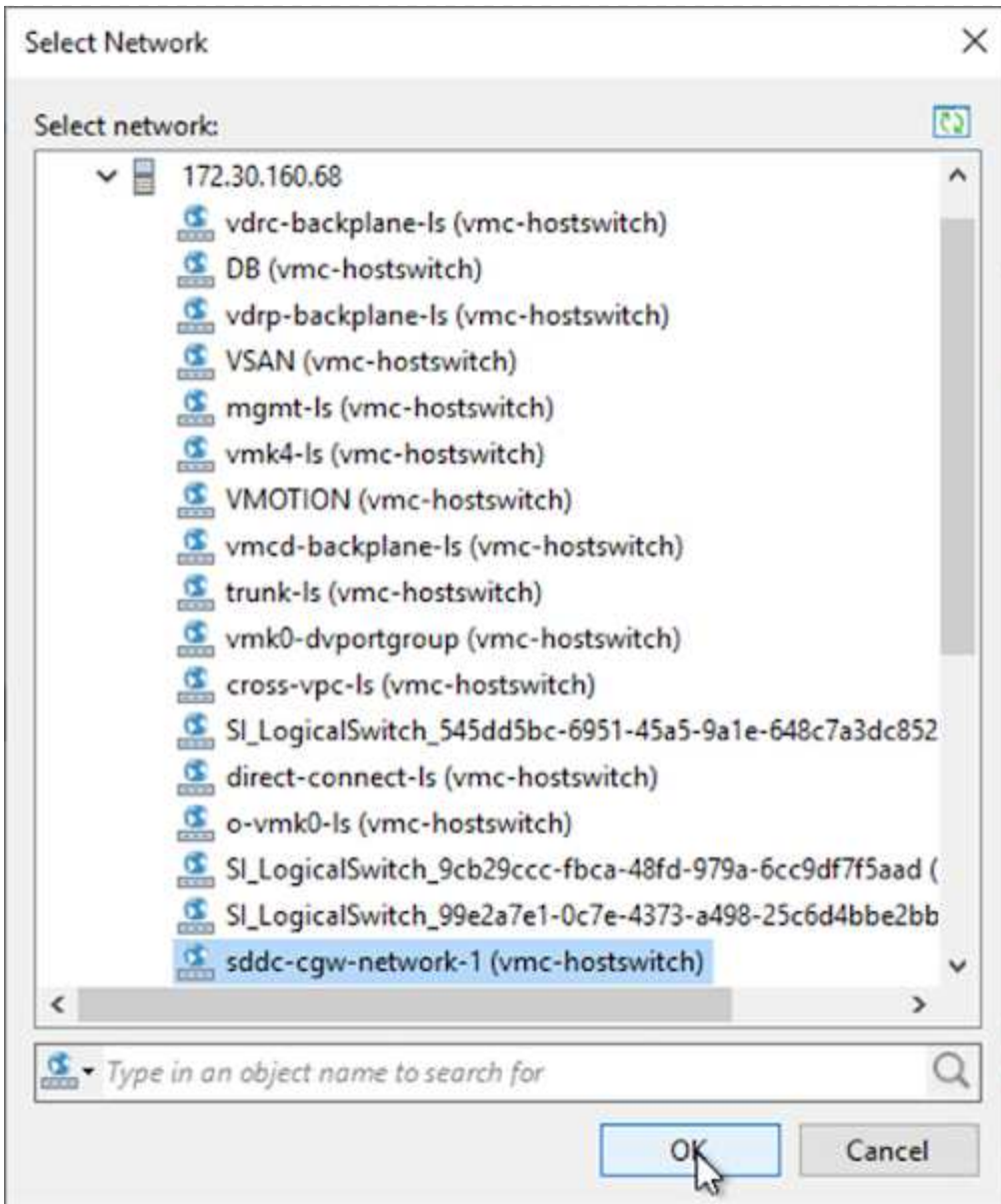


By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.

Summary

[illegible]

Cancel



7. 복원된 VM에서 맬웨어를 검사할지 여부를 선택하고 요약 페이지를 검토한 다음 마침 을 클릭하여 복원을 시작합니다.

SQL Server 응용 프로그램 데이터를 복원합니다

다음 프로세스에서는 사내 사이트가 작동 불능 상태가 되는 재해가 발생할 경우 AWS의 VMware Cloud Services에서 SQL Server를 복구하는 방법에 대한 지침을 제공합니다.

복구 단계를 계속 진행하려면 다음 필수 구성 요소가 완료된 것으로 가정합니다.

1. Veeam Full Restore를 사용하여 Windows Server VM을 VMware Cloud SDDC로 복구했습니다.
2. 보조 SnapCenter 서버가 설정되었고 섹션에 설명된 단계를 사용하여 SnapCenter 데이터베이스 복원 및 구성이 완료되었습니다 ["SnapCenter 백업 및 복원 프로세스 요약"](#)

VM: SQL Server VM에 대한 사후 복원 구성

VM 복원이 완료된 후 SnapCenter 내에서 호스트 VM을 재검색할 수 있도록 네트워킹 및 기타 항목을 구성해야 합니다.

1. 관리 및 iSCSI 또는 NFS에 새 IP 주소를 할당합니다.
2. Windows 도메인에 호스트를 연결합니다.
3. DNS 또는 SnapCenter 서버의 호스트 파일에 호스트 이름을 추가합니다.



SnapCenter 플러그인이 현재 도메인과 다른 도메인 자격 증명을 사용하여 배포된 경우 SQL Server VM의 Windows용 플러그인 서비스에 대한 로그인 계정을 변경해야 합니다. 로그인 계정을 변경한 후 SnapCenter SMCore, Windows용 플러그인 및 SQL Server 서비스용 플러그인을 다시 시작합니다.



SnapCenter에서 복원된 VM을 자동으로 다시 검색하려면 FQDN이 SnapCenter 온-프레미스에 원래 추가된 VM과 동일해야 합니다.

SQL Server 복구를 위한 FSx 스토리지를 구성합니다

SQL Server VM의 재해 복구 복원 프로세스를 수행하려면 FSx 클러스터에서 기존 SnapMirror 관계를 중단하고 볼륨에 대한 액세스를 부여해야 합니다. 이렇게 하려면 다음 단계를 완료하십시오.

1. SQL Server 데이터베이스 및 로그 볼륨에 대한 기존 SnapMirror 관계를 해제하려면 FSx CLI에서 다음 명령을 실행합니다.

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

2. SQL Server Windows VM의 iSCSI IQN이 포함된 이니시에이터 그룹을 생성하여 LUN에 대한 액세스 권한 부여:

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

3. 마지막으로 LUN을 방금 생성한 이니시에이터 그룹에 매핑합니다.

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

4. 경로 이름을 찾으려면 'lun show' 명령을 실행합니다.

iSCSI 액세스를 위해 **Windows VM**을 설정하고 파일 시스템을 검색합니다

1. SQL Server VM에서 iSCSI 네트워크 어댑터를 설정하여 FSx 인스턴스의 iSCSI 타겟 인터페이스에 대한 연결로 설정된 VMware 포트 그룹에서 통신합니다.
2. iSCSI 초기자 등록 정보 유틸리티를 열고 검색, 즐겨찾기 대상 및 대상 탭에서 이전 연결 설정을 지웁니다.
3. FSx 인스턴스/클러스터에서 iSCSI 논리 인터페이스에 액세스하기 위한 IP 주소를 찾습니다. AWS 콘솔의 Amazon FSx > ONTAP > Storage Virtual Machines에서 찾을 수 있습니다.

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

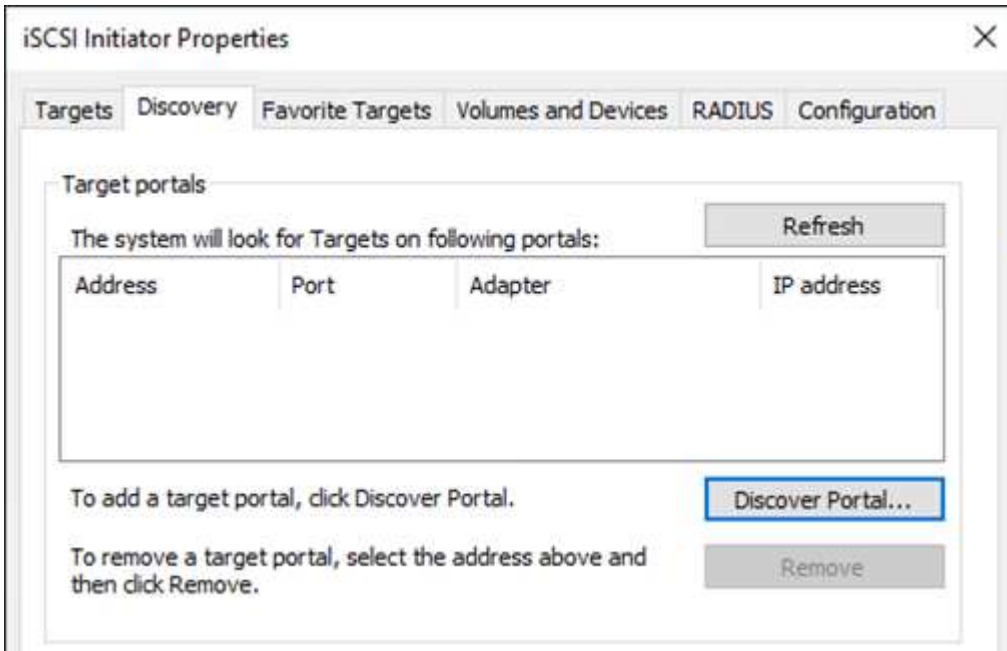
NFS IP address

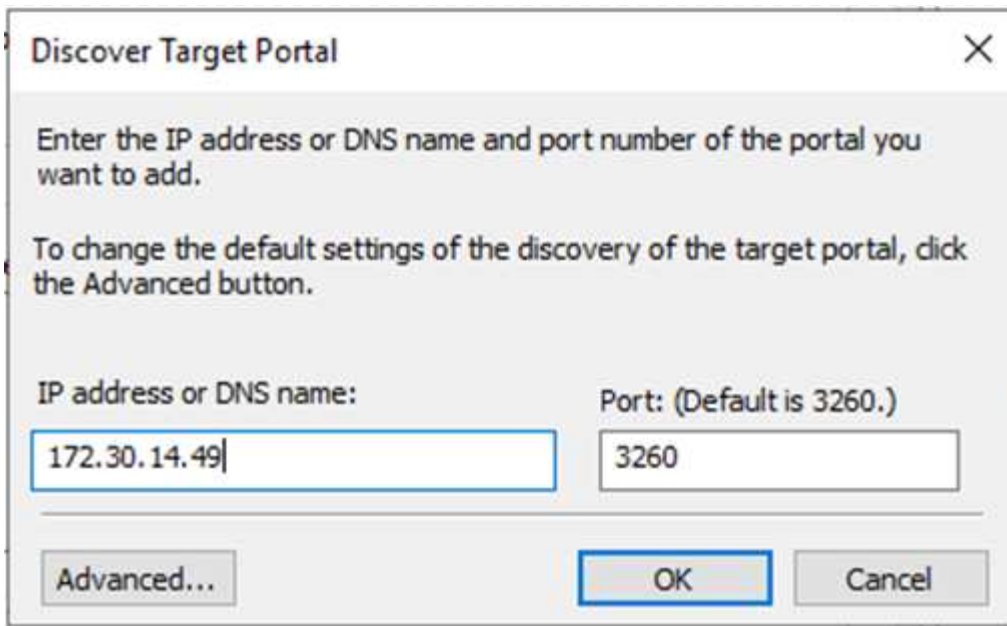
198.19.254.53

iSCSI IP addresses

172.30.15.101, 172.30.14.49

4. 검색 탭에서 포털 검색 을 클릭하고 FSx iSCSI 대상의 IP 주소를 입력합니다.





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.

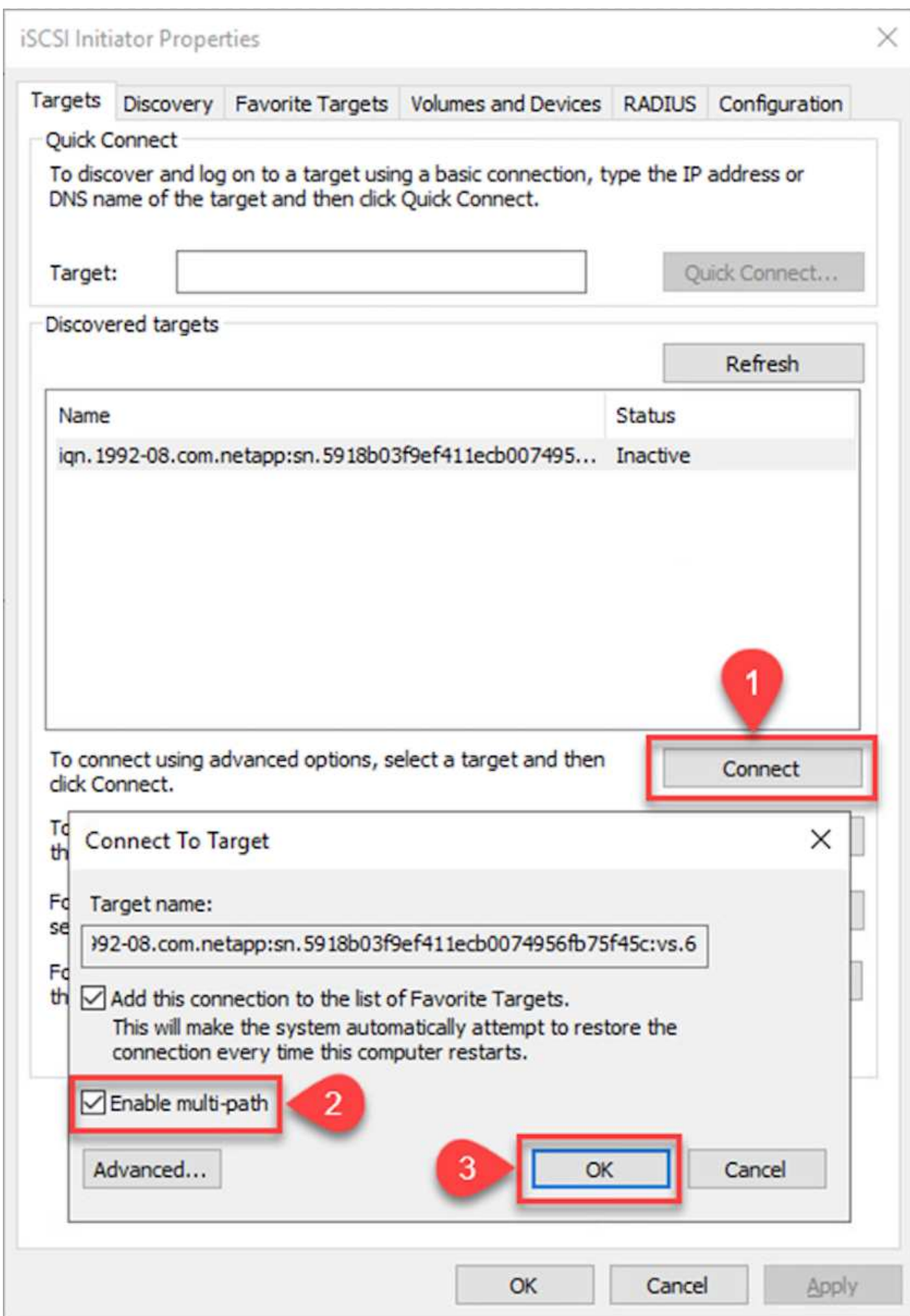
To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: 172.30.14.49

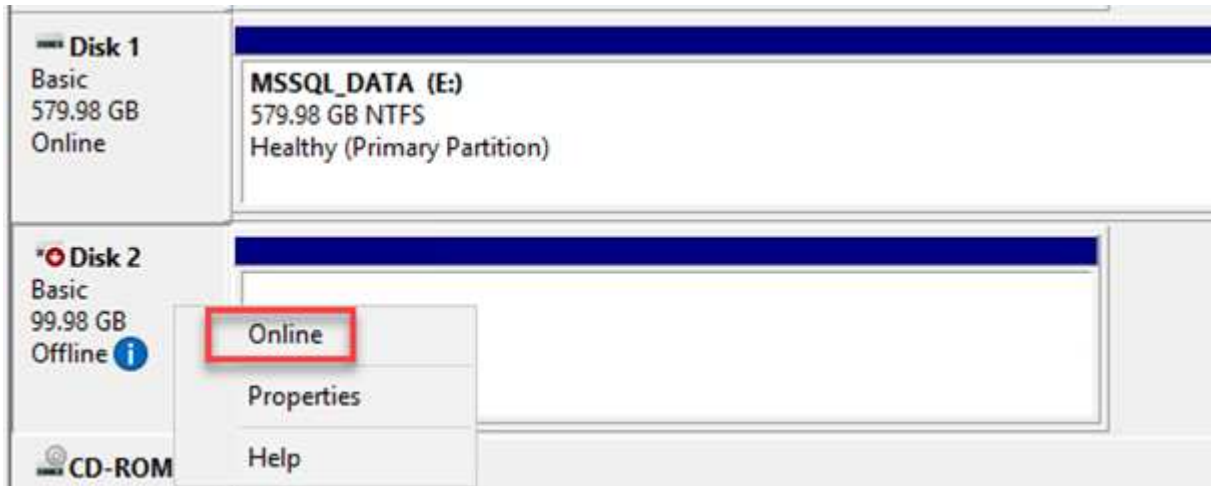
Port: (Default is 3260.) 3260

Advanced... OK Cancel

5. 대상 탭에서 연결을 클릭하고 구성에 적합한 경우 다중 경로 사용을 선택한 다음 확인을 클릭하여 대상에 연결합니다.

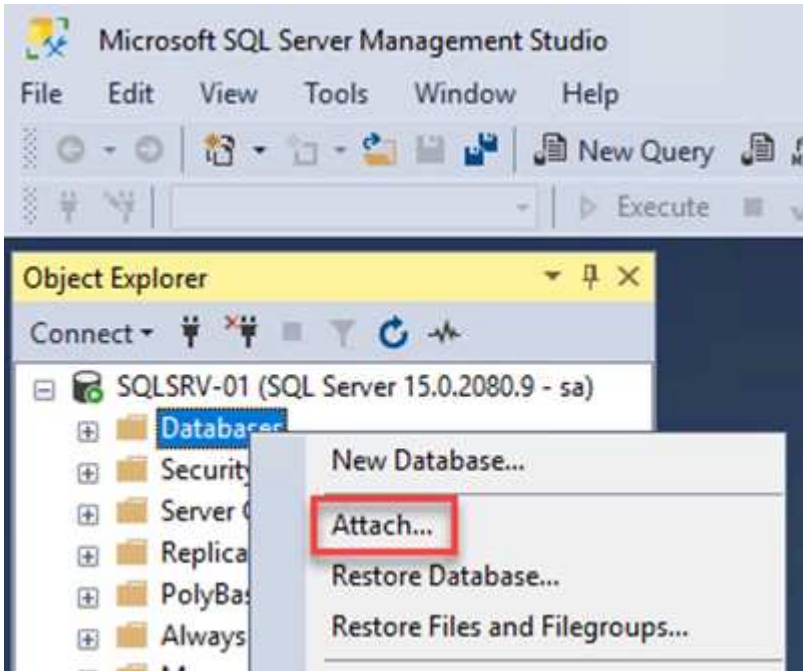


6. 컴퓨터 관리 유틸리티를 열고 디스크를 온라인 상태로 전환합니다. 이전에 사용했던 것과 동일한 드라이브 문자가 유지되는지 확인합니다.

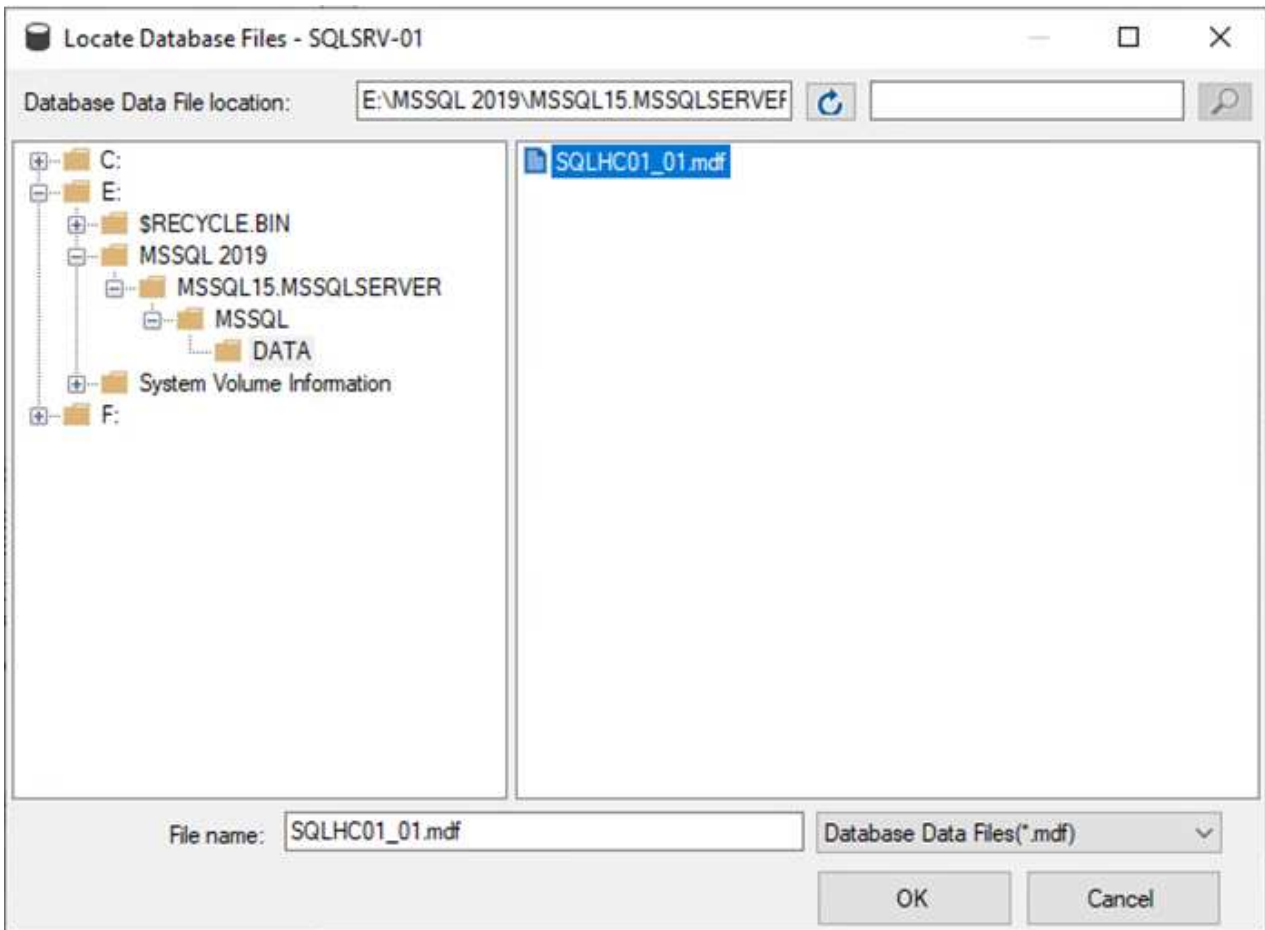


SQL Server 데이터베이스를 연결합니다

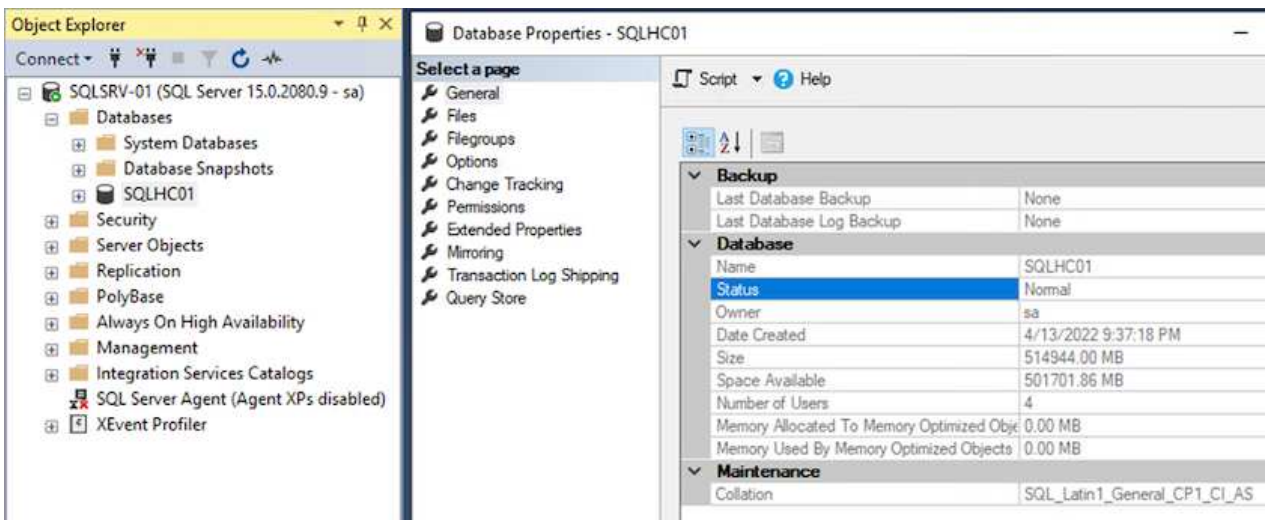
1. SQL Server VM에서 Microsoft SQL Server Management Studio를 열고 연결 을 선택하여 데이터베이스에 연결하는 프로세스를 시작합니다.



2. 추가 를 클릭하고 SQL Server 기본 데이터베이스 파일이 들어 있는 폴더로 이동한 다음 해당 파일을 선택하고 확인 을 클릭합니다.



3. 트랜잭션 로그가 별도의 드라이브에 있는 경우 트랜잭션 로그가 포함된 폴더를 선택합니다.
4. 완료되면 확인 을 클릭하여 데이터베이스를 연결합니다.

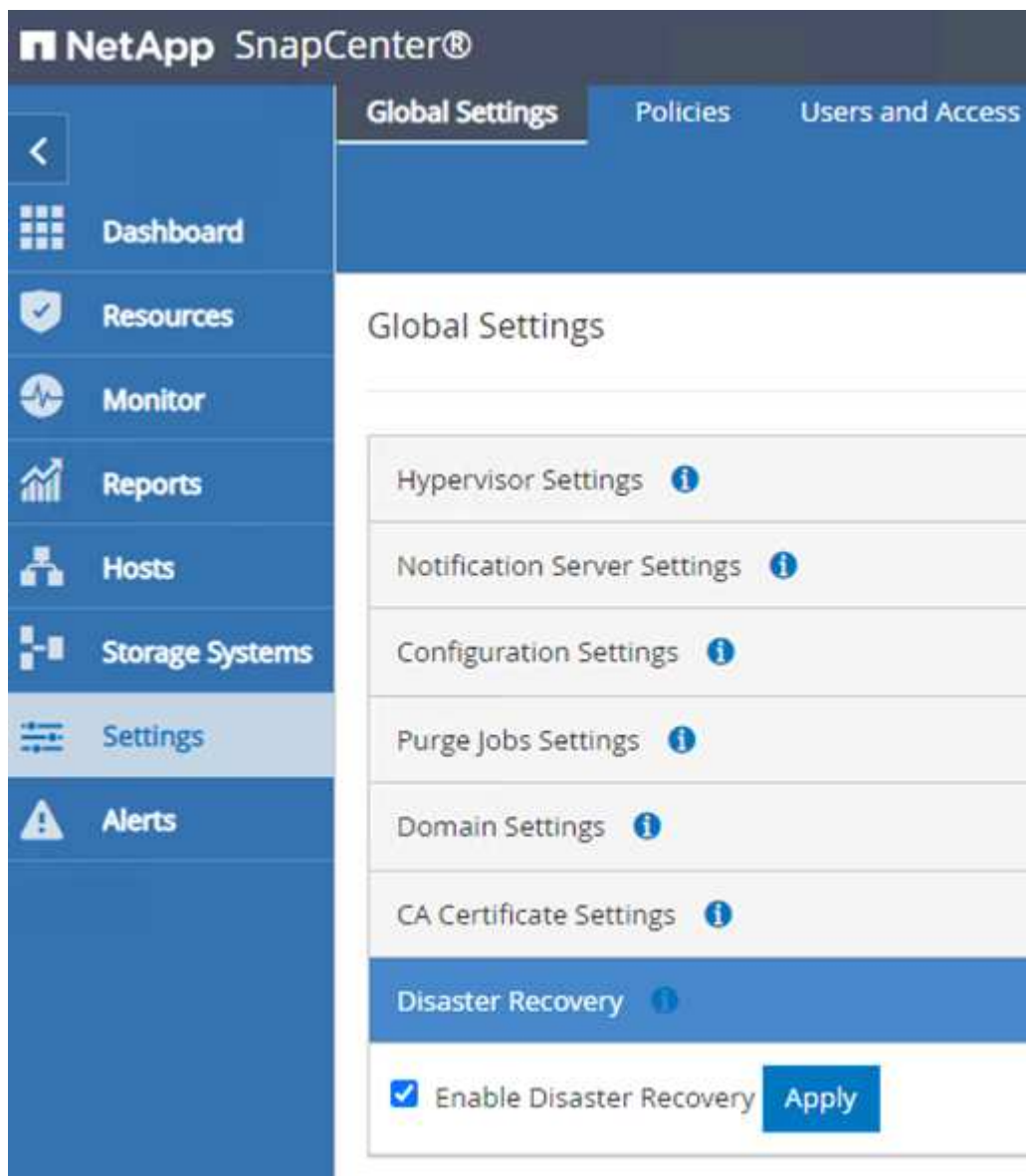


SQL Server 플러그인과 SnapCenter 통신을 확인합니다

SnapCenter 데이터베이스가 이전 상태로 복원되면 SQL Server 호스트가 자동으로 다시 검색됩니다. 이 작업이 올바르게 작동하려면 다음 필수 조건을 염두에 두십시오.

- SnapCenter를 재해 복구 모드로 전환해야 합니다. 이 작업은 Swagger API 또는 재해 복구의 글로벌 설정을 통해 수행할 수 있습니다.
- SQL Server의 FQDN은 온-프레미스 데이터 센터에서 실행 중인 인스턴스와 동일해야 합니다.
- 원래 SnapMirror 관계가 끊어야 합니다.
- 데이터베이스가 포함된 LUN은 SQL Server 인스턴스 및 연결된 데이터베이스에 마운트되어야 합니다.

SnapCenter가 재해 복구 모드에 있는지 확인하려면 SnapCenter 웹 클라이언트 내에서 설정 으로 이동합니다. 글로벌 설정 탭으로 이동한 다음 재해 복구 를 클릭합니다. 재해 복구 활성화 확인란이 활성화되어 있는지 확인합니다.



Oracle 애플리케이션 데이터를 복구합니다

다음 프로세스에서는 사내 사이트가 작동 불가능한 재해 발생 시 AWS의 VMware Cloud Services에서 Oracle 애플리케이션 데이터를 복구하는 방법에 대한 지침을 제공합니다.

복구 단계를 계속하려면 다음 필수 구성 요소를 완료하십시오.

1. Veeam Full Restore를 사용하여 Oracle Linux 서버 VM을 VMware Cloud SDDC로 복구했습니다.
2. 보조 SnapCenter 서버가 설정되었으며 이 섹션에 설명된 단계를 사용하여 SnapCenter 데이터베이스 및 구성 파일이 복원되었습니다 "[SnapCenter 백업 및 복원 프로세스 요약](#)"

Oracle 복원을 위해 FSx 구성 - SnapMirror 관계를 끊습니다

FSxN 인스턴스에서 호스팅되는 보조 스토리지 볼륨을 Oracle 서버에서 액세스할 수 있도록 하려면 먼저 기존 SnapMirror 관계를 해제해야 합니다.

1. FSx CLI에 로그인한 후 다음 명령을 실행하여 올바른 이름으로 필터링된 볼륨을 확인합니다.

```
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. 다음 명령을 실행하여 기존 SnapMirror 관계를 중단하십시오.

```
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 웹 클라이언트에서 junction-path를 업데이트합니다.

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. 접합 경로 이름을 추가하고 업데이트 를 클릭합니다. Oracle 서버에서 NFS 볼륨을 마운트할 때 이 연결 경로를 지정합니다.

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



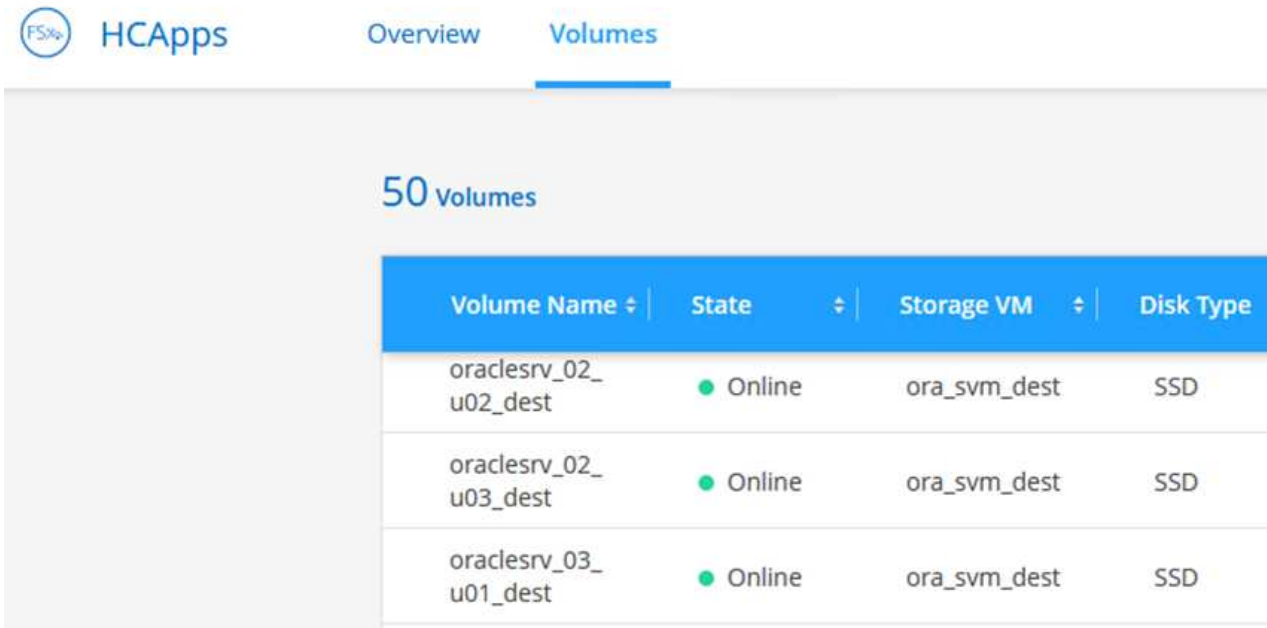
Cancel

Update

Oracle Server에서 NFS 볼륨을 마운트합니다

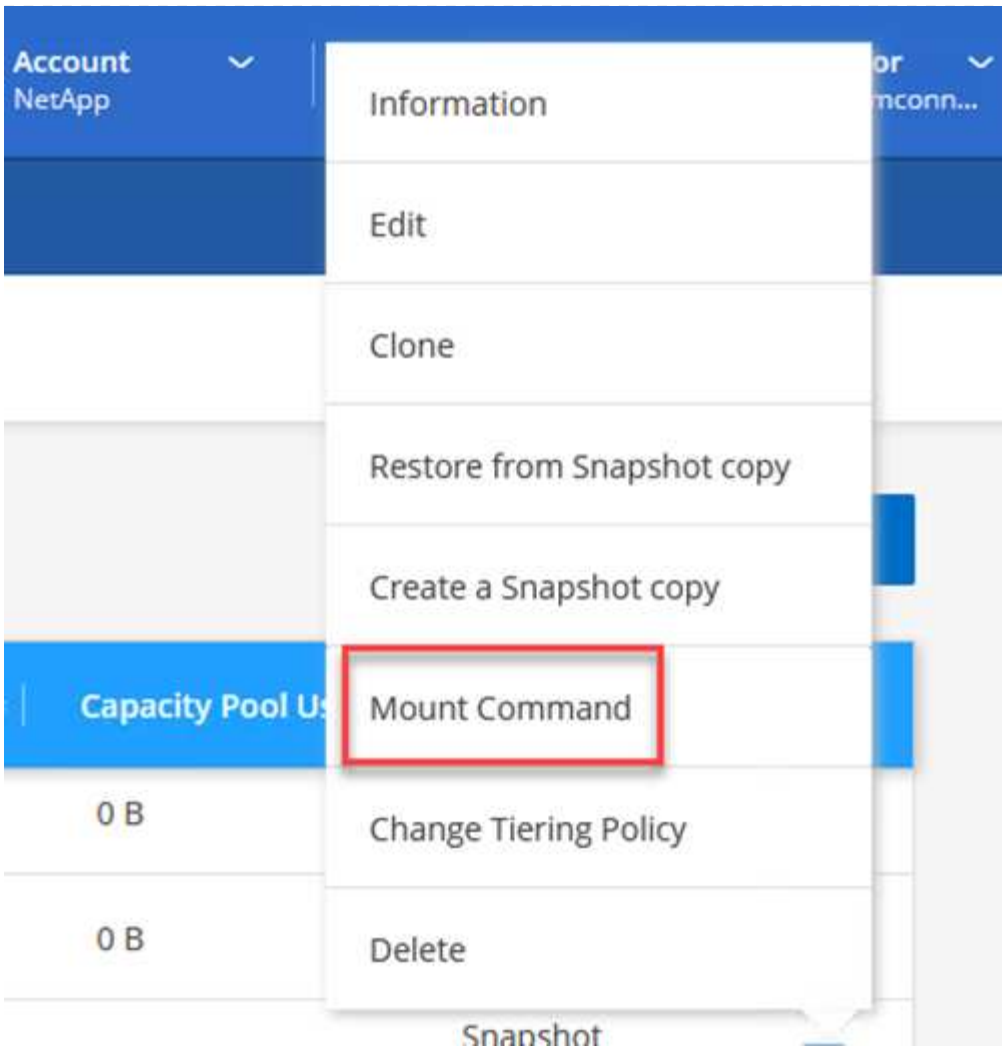
Cloud Manager에서 Oracle 데이터베이스 파일 및 로그가 포함된 NFS 볼륨을 마운트하기 위한 올바른 NFS LIF IP 주소를 사용하여 마운트 명령을 얻을 수 있습니다.

1. Cloud Manager에서 FSx 클러스터의 볼륨 목록에 액세스합니다.



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. 작업 메뉴에서 마운트 명령을 선택하여 Oracle Linux 서버에서 사용할 마운트 명령을 보고 복사합니다.



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. Oracle Linux Server에 NFS 파일 시스템을 마운트합니다. NFS 공유를 마운트하는 디렉토리가 Oracle Linux 호스트에 이미 있습니다.
4. Oracle Linux 서버에서 mount 명령을 사용하여 NFS 볼륨을 마운트합니다.

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

Oracle 데이터베이스와 연결된 각 볼륨에 대해 이 단계를 반복합니다.



재부팅 시 NFS 마운트를 영구적으로 만들려면 '/etc/fstab' 파일을 편집하여 마운트 명령을 포함합니다.

5. Oracle 서버를 재부팅합니다. Oracle 데이터베이스는 정상적으로 시작되어 사용할 수 있어야 합니다.

장애 복구

이 솔루션에 설명된 페일오버 프로세스가 성공적으로 완료되면 SnapCenter 및 Veeam이 AWS에서 백업 기능을 재개합니다. 이제 ONTAP용 FSx는 원래 사내 데이터 센터와 SnapMirror 관계가 없는 기본 스토리지로 지정됩니다. 정상적인 기능을 사내에서 다시 시작한 후 이 설명서에 나와 있는 것과 동일한 프로세스를 사용하여 데이터를 사내 ONTAP 스토리지 시스템에 다시 미러링할 수 있습니다.

또한 이 설명서에 나와 있는 것처럼 SnapCenter를 구성하여 ONTAP용 FSx에서 온프레미스에 있는 ONTAP 스토리지 시스템으로 애플리케이션 데이터 볼륨을 미러링할 수 있습니다. 마찬가지로, Veeam을 구성하여 스케일아웃 백업 저장소를 사용하여 Amazon S3에 백업 복사본을 복제함으로써 사내 데이터 센터에 상주하는 Veeam 백업 서버에 액세스할 수 있습니다.

페일백은 이 문서의 범위를 벗어나지만 장애 복구는 여기에 설명된 세부 프로세스와 거의 차이가 없습니다.

결론

이 문서에 제공된 사용 사례는 NetApp과 VMware의 통합을 강조하는 검증된 재해 복구 기술에 초점을 맞춥니다. NetApp ONTAP 스토리지 시스템은 검증된 데이터 미러링 기술을 제공하므로 조직이 주요 클라우드 공급자와 함께 상주하면서 사내 및 ONTAP 기술을 아우르는 재해 복구 솔루션을 설계할 수 있습니다.

AWS 기반 ONTAP용 FSX는 SnapCenter 및 SyncMirror와 원활하게 통합되어 애플리케이션 데이터를 클라우드로 복제할 수 있는 솔루션 중 하나입니다. Veeam 백업 및 복제는 NetApp ONTAP 스토리지 시스템과 긴밀하게 통합되며 vSphere 기본 스토리지에 대한 페일오버를 제공할 수 있는 또 다른 잘 알려진 기술입니다.

이 솔루션은 SQL Server 및 Oracle 애플리케이션 데이터를 호스팅하는 ONTAP 시스템의 게스트 연결 스토리지를 사용하는 재해 복구 솔루션을 제공합니다. SnapCenter with SnapMirror를 사용하면 ONTAP 시스템에서 애플리케이션 볼륨을 보호하고 클라우드에 있는 FSx 또는 CVO로 복제할 수 있는 관리가 쉬운 솔루션을 제공할 수 있습니다. SnapCenter는 모든 애플리케이션 데이터를 AWS의 VMware 클라우드로 페일오버하는 DR 지원 솔루션입니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- 솔루션 설명서 링크

["VMware 솔루션을 사용하는 NetApp 하이브리드 멀티 클라우드"](#)

["NetApp 솔루션"](#)

Amazon FSx for ONTAP를 사용한 VMware 클라우드에서 Veeam 백업 및 복원

저자: Josh Powell - NetApp 솔루션 엔지니어링

개요

Veeam Backup & Replication은 VMware Cloud의 데이터를 보호하는 효과적이고 안정적인 솔루션입니다. 이 솔루션은 Veeam 백업 및 복제를 사용하여 VMware 클라우드의 ONTAP NFS 데이터 저장소용 FSx에 상주하는 애플리케이션 VM을 백업 및 복원하기 위한 적절한 설정 및 구성을 보여 줍니다.

VMware Cloud(AWS의 경우)는 NFS 데이터 저장소를 보조 스토리지로 사용할 수 있도록 지원하며, FSx for NetApp ONTAP는 SDDC 클러스터의 ESXi 호스트 수에 관계없이 확장할 수 있는 클라우드 애플리케이션에 대량의 데이터를 저장해야 하는 고객을 위한 안전한 솔루션입니다. 이 통합 AWS 스토리지 서비스는 기존의 모든 NetApp ONTAP 기능을 갖춘 고효율 스토리지를 제공합니다.

사용 사례

이 솔루션은 다음과 같은 사용 사례를 해결합니다.

- NetApp ONTAP용 FSx를 백업 저장소로 사용하여 VMC에서 호스팅되는 Windows 및 Linux 가상 머신의 백업 및 복원
- NetApp ONTAP용 FSx를 백업 저장소로 사용하여 Microsoft SQL Server 애플리케이션 데이터를 백업 및 복원합니다.
- NetApp ONTAP용 FSx를 백업 저장소로 사용하여 Oracle 애플리케이션 데이터를 백업 및 복원합니다.

ONTAP용 Amazon FSx를 사용하는 NFS 데이터 저장소입니다

이 솔루션의 모든 가상 머신은 ONTAP 보조 NFS 데이터 저장소용 FSx에 상주합니다. ONTAP용 FSx를 보조 NFS 데이터 저장소로 사용하면 여러 가지 이점을 얻을 수 있습니다. 예를 들어, 다음을 수행할 수 있습니다.

- 복잡한 설정 및 관리 없이도 확장 가능하고 가용성이 높은 파일 시스템을 클라우드에서 생성할 수 있습니다.
- 기존 VMware 환경과 통합되므로 친숙한 툴 및 프로세스를 사용하여 클라우드 리소스를 관리할 수 있습니다.
- 스냅샷 및 복제와 같이 ONTAP에서 제공하는 고급 데이터 관리 기능을 활용하여 데이터를 보호하고 가용성을 보장합니다.

솔루션 구축 개요

이 목록에는 Veeam 백업 및 복제를 구성하고, ONTAP용 FSx를 백업 저장소로 사용하여 백업 및 복원 작업을 실행하고, SQL Server 및 Oracle VM 및 데이터베이스의 복원을 수행하는 데 필요한 높은 수준의 단계가 나와 있습니다.

1. Veeam 백업 및 복제를 위한 iSCSI 백업 저장소로 사용할 ONTAP 파일 시스템용 FSx를 생성합니다.
2. Veeam 프록시를 구축하여 백업 워크로드를 분산하고 ONTAP용 FSx에서 호스팅되는 iSCSI 백업 저장소를 마운트합니다.
3. SQL Server, Oracle, Linux 및 Windows 가상 머신을 백업하도록 Veeam 백업 작업을 구성합니다.
4. SQL Server 가상 머신 및 개별 데이터베이스를 복구합니다.
5. Oracle 가상 머신 및 개별 데이터베이스를 복원합니다.

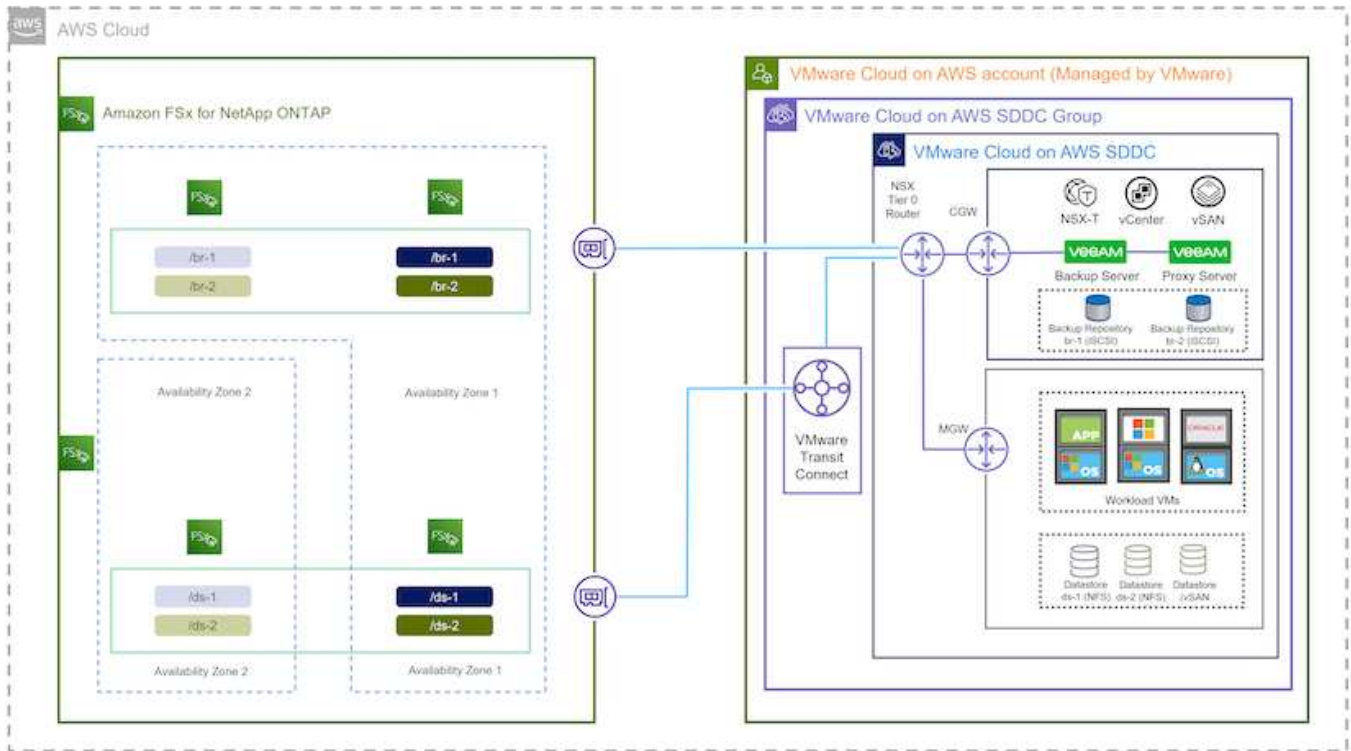
필수 구성 요소

이 솔루션의 목적은 VMware Cloud에서 실행되고 NetApp ONTAP용 FSx에서 호스팅하는 NFS 데이터 저장소에 있는 가상 머신의 데이터 보호를 시연하는 것입니다. 이 솔루션에서는 다음 구성 요소가 구성되어 사용할 준비가 되어 있다고 가정합니다.

1. VMware 클라우드에 연결된 NFS 데이터 저장소가 하나 이상 있는 ONTAP 파일 시스템용 FSX
2. Veeam Backup & Replication 소프트웨어가 설치된 Microsoft Windows Server VM
 - Veeam Backup & Replication 서버에서 IP 주소 또는 정규화된 도메인 이름을 사용하여 vCenter 서버를 검색했습니다.
3. 솔루션을 구축하는 동안 Veeam Backup Proxy 구성 요소와 함께 Microsoft Windows Server VM이 설치됩니다.
4. ONTAP NFS 데이터 저장소용 FSx에 상주하는 VMDK 및 애플리케이션 데이터가 있는 Microsoft SQL Server VM 이 솔루션에서는 두 개의 별도 VMDK에 두 개의 SQL 데이터베이스를 구축했습니다.
 - 참고: 최상의 데이터베이스 및 트랜잭션 로그 파일은 성능 및 안정성을 향상시키기 위해 별도의 드라이브에 배치됩니다. 이는 트랜잭션 로그가 순차적으로 작성되는 반면 데이터베이스 파일은 무작위로 작성되기 때문에 발생합니다.
5. ONTAP NFS 데이터 저장소용 FSx에 상주하는 VMDK 및 애플리케이션 데이터가 있는 Oracle 데이터베이스 VM
6. ONTAP NFS 데이터 저장소용 FSx에 상주하는 VMDK가 있는 Linux 및 Windows 파일 서버 VM
7. Veeam을 사용하려면 백업 환경의 서버와 구성 요소 간 통신에 특정 TCP 포트가 필요합니다. Veeam 백업 인프라 구성 요소에서 필요한 방화벽 규칙이 자동으로 생성됩니다. 네트워크 포트 요구 사항의 전체 목록은 의 포트 섹션을 참조하십시오 ["Veeam Backup and Replication User Guide for VMware vSphere를 참조하십시오"](#).

고급 아키텍처

이 솔루션의 테스트/검증은 최종 배포 환경과 일치하거나 일치하지 않을 수 있는 랩에서 수행되었습니다. 자세한 내용은 다음 섹션을 참조하십시오.



하드웨어/소프트웨어 구성 요소

이 솔루션의 목적은 VMware Cloud에서 실행되고 NetApp ONTAP용 FSx에서 호스팅하는 NFS 데이터 저장소에 있는 가상 머신의 데이터 보호를 시연하는 것입니다. 이 솔루션에서는 다음 구성 요소가 이미 구성되어 있고 사용할 준비가 되어 있다고 가정합니다.

- Microsoft Windows VM은 ONTAP NFS 데이터 저장소용 FSx에 있습니다
- Linux(CentOS) VM은 ONTAP NFS 데이터 저장소용 FSx에 있습니다
- Microsoft SQL Server VM은 ONTAP NFS 데이터 저장소용 FSx에 있습니다
 - 두 개의 데이터베이스가 별도의 VMDK에서 호스팅됩니다
- ONTAP NFS 데이터 저장소용 FSx에 있는 Oracle VM

솔루션 구축

이 솔루션에서는 Veeam Backup and Replication 소프트웨어를 사용하여 AWS 기반 VMware Cloud SDDC에서 SQL Server, Oracle, Windows 및 Linux 파일 서버 가상 시스템의 백업 및 복구를 수행하는 솔루션을 구축 및 검증하는 방법에 대한 자세한 지침을 제공합니다. 이 솔루션의 가상 머신은 FSx for ONTAP에서 호스팅하는 보조 NFS 데이터 저장소에 상주합니다. 또한 Veeam 백업 저장소에 사용할 iSCSI 볼륨을 호스팅하기 위해 ONTAP 파일 시스템용 별도의 FSx가 사용됩니다.

ONTAP 파일 시스템 생성을 위한 FSx, 백업 저장소로 사용할 iSCSI 볼륨 마운트, 백업 작업 생성 및 실행, VM 및 데이터베이스 복원 수행 등을 살펴보겠습니다.

NetApp ONTAP용 FSx에 대한 자세한 내용은 를 참조하십시오 ["ONTAP용 FSX 사용 설명서"](#).

Veeam Backup and Replication에 대한 자세한 내용은 을 참조하십시오 ["Veeam Help Center 기술 문서"](#) 사이트.

AWS에서 Veeam Backup and Replication을 VMware Cloud로 사용할 때의 고려 사항 및 제한 사항은 을 참조하십시오 ["AWS 기반 VMware 클라우드 및 Dell EMC 지원 기반 VMware 클라우드 고려 사항 및 제한 사항"](#).

Veeam 프록시 서버를 구축하십시오

Veeam 프록시 서버는 Veeam Backup & Replication 소프트웨어의 구성 요소로, 소스와 백업 또는 복제 타겟 간의 매개 역할을 합니다. 프록시 서버는 데이터를 로컬로 처리하여 백업 작업 중에 데이터 전송을 최적화하고 가속화할 수 있도록 지원하며, 서로 다른 전송 모드를 사용하여 VMware vStorage APIs for Data Protection 또는 직접 스토리지 액세스를 통해 데이터에 액세스할 수 있습니다.

Veeam 프록시 서버 설계를 선택할 때는 필요한 동시 작업 수와 전송 모드 또는 스토리지 액세스 유형을 고려해야 합니다.

프록시 서버의 수와 시스템 요구 사항에 대한 사이징은 를 참조하십시오 ["Veeam VMware vSphere 모범 사례 가이드"](#).

Veeam Data Mover는 Veeam Proxy Server의 구성 요소이며 소스에서 VM 데이터를 가져오고 타겟으로 전송하기 위한 수단으로 전송 모드를 사용합니다. 전송 모드는 백업 작업을 구성하는 동안 지정됩니다. 직접 스토리지 액세스를 사용하여 NFS 데이터 저장소에서 데이터 백업의 효율성을 높일 수 있습니다.

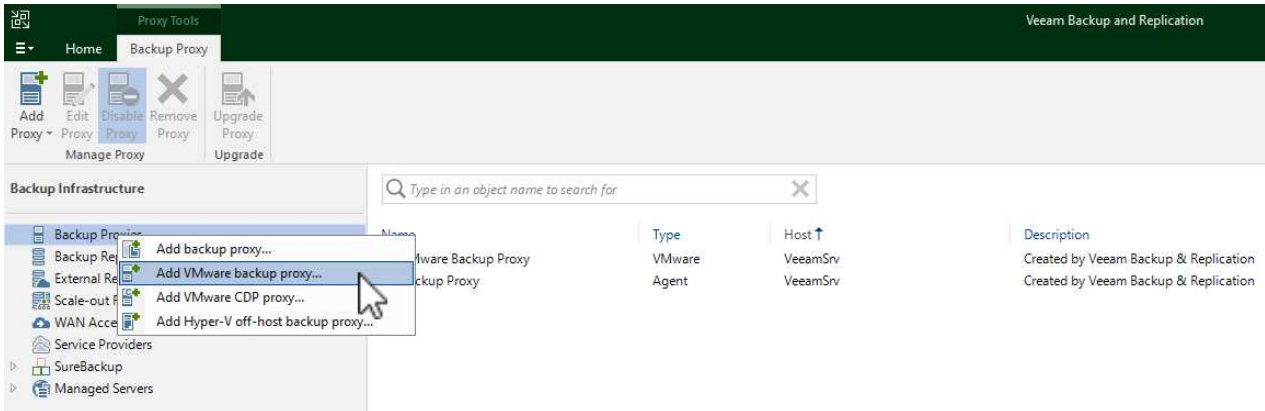
운송 모드에 대한 자세한 내용은 를 참조하십시오 ["Veeam Backup and Replication User Guide for VMware vSphere를 참조하십시오"](#).

다음 단계에서는 VMware Cloud SDDC의 Windows VM에 Veeam Proxy Server를 구축하는 방법을 살펴봅니다.

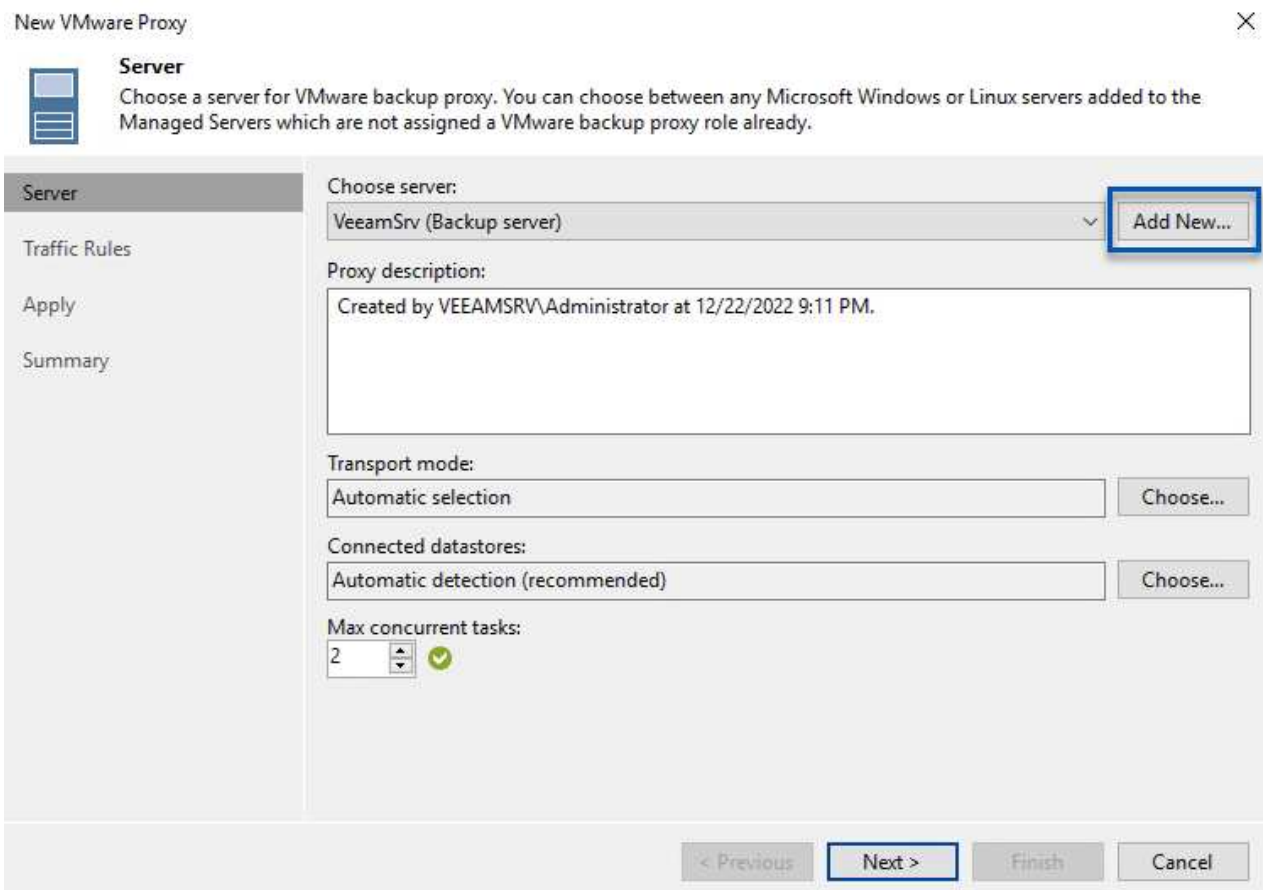
Veeam Proxy를 구축하여 백업 워크로드를 분산합니다

이 단계에서는 Veeam 프록시를 기존 Windows VM에 구축합니다. 따라서 운영 Veeam Backup Server와 Veeam Proxy 간에 백업 작업을 분산할 수 있습니다.

1. Veeam Backup and Replication 서버에서 관리 콘솔을 열고 왼쪽 하단 메뉴에서 * Backup Infrastructure * 를 선택합니다.
2. Backup Proxies * 를 마우스 오른쪽 버튼으로 클릭하고 * Add VMware backup proxy... * 를 클릭하여 마법사를 엽니다.

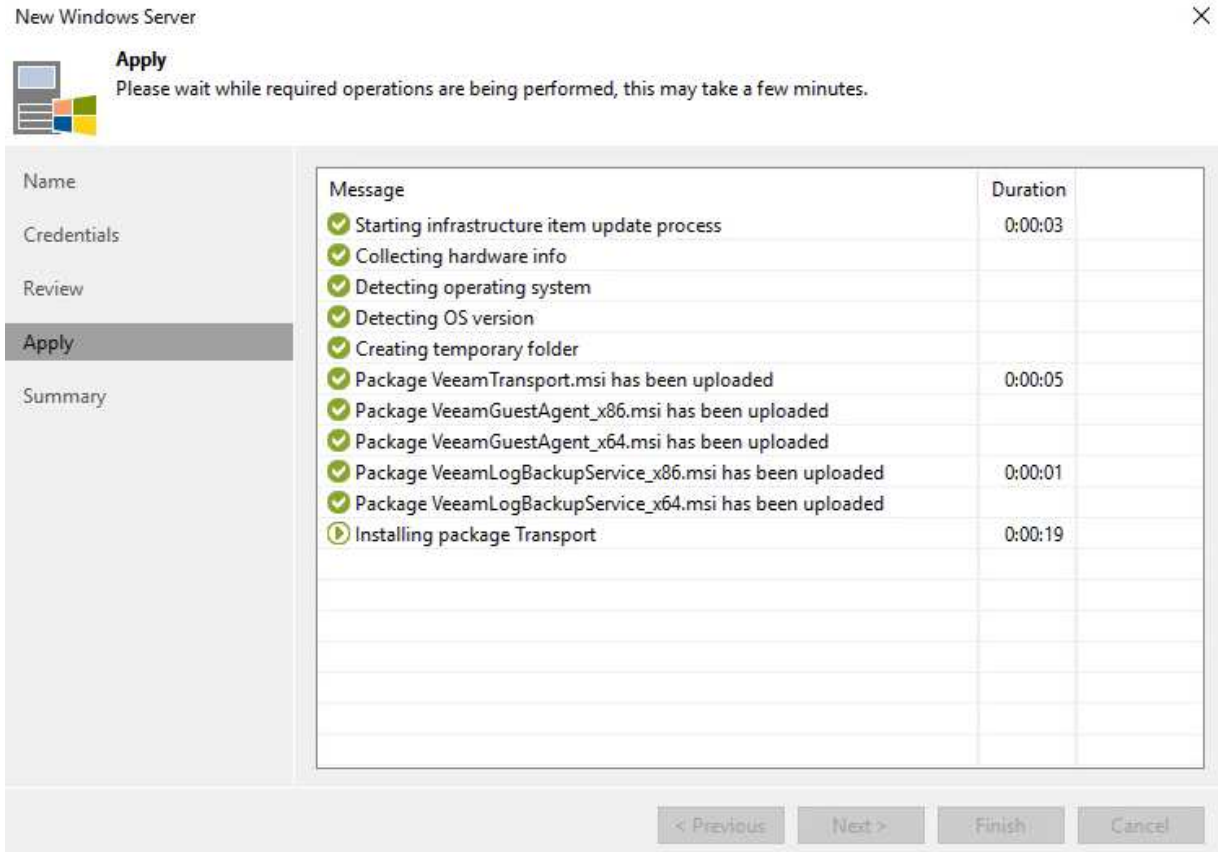


3. VMware 프록시 추가 * 마법사에서 * 새로 추가... * 버튼을 클릭하여 새 프록시 서버를 추가합니다.

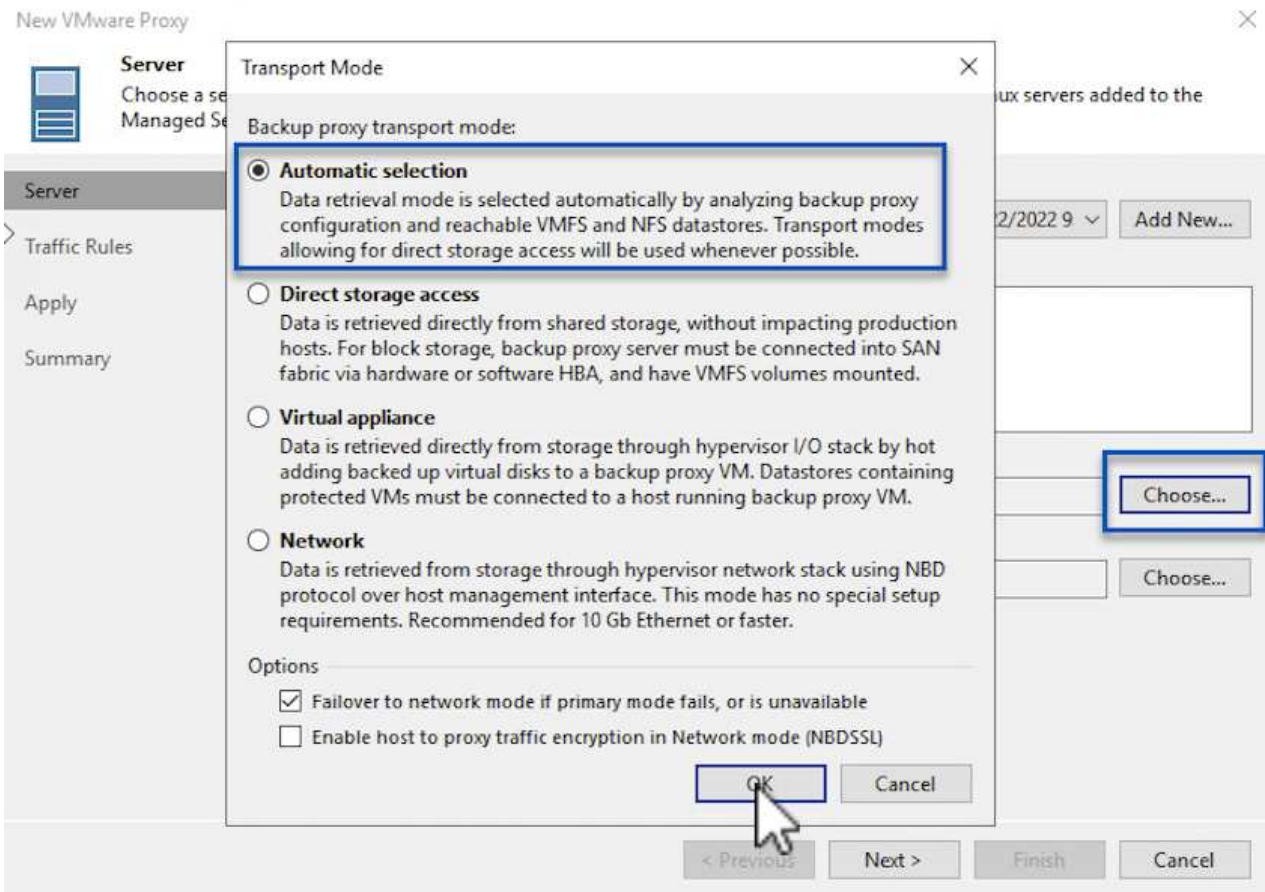


4. Microsoft Windows를 추가하려면 을 선택하고 프롬프트에 따라 서버를 추가합니다.

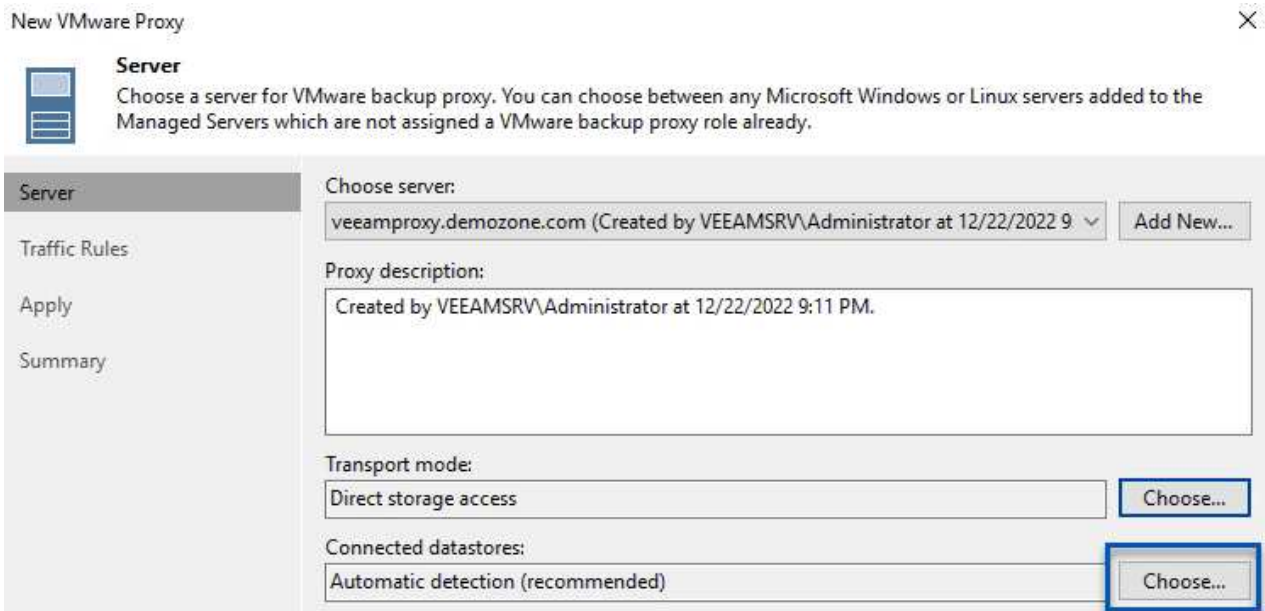
- DNS 이름 또는 IP 주소를 입력합니다
- 새 시스템의 자격 증명에 사용할 계정을 선택하거나 새 자격 증명을 추가합니다
- 설치할 구성 요소를 검토한 다음 * 적용 * 을 클릭하여 배포를 시작합니다

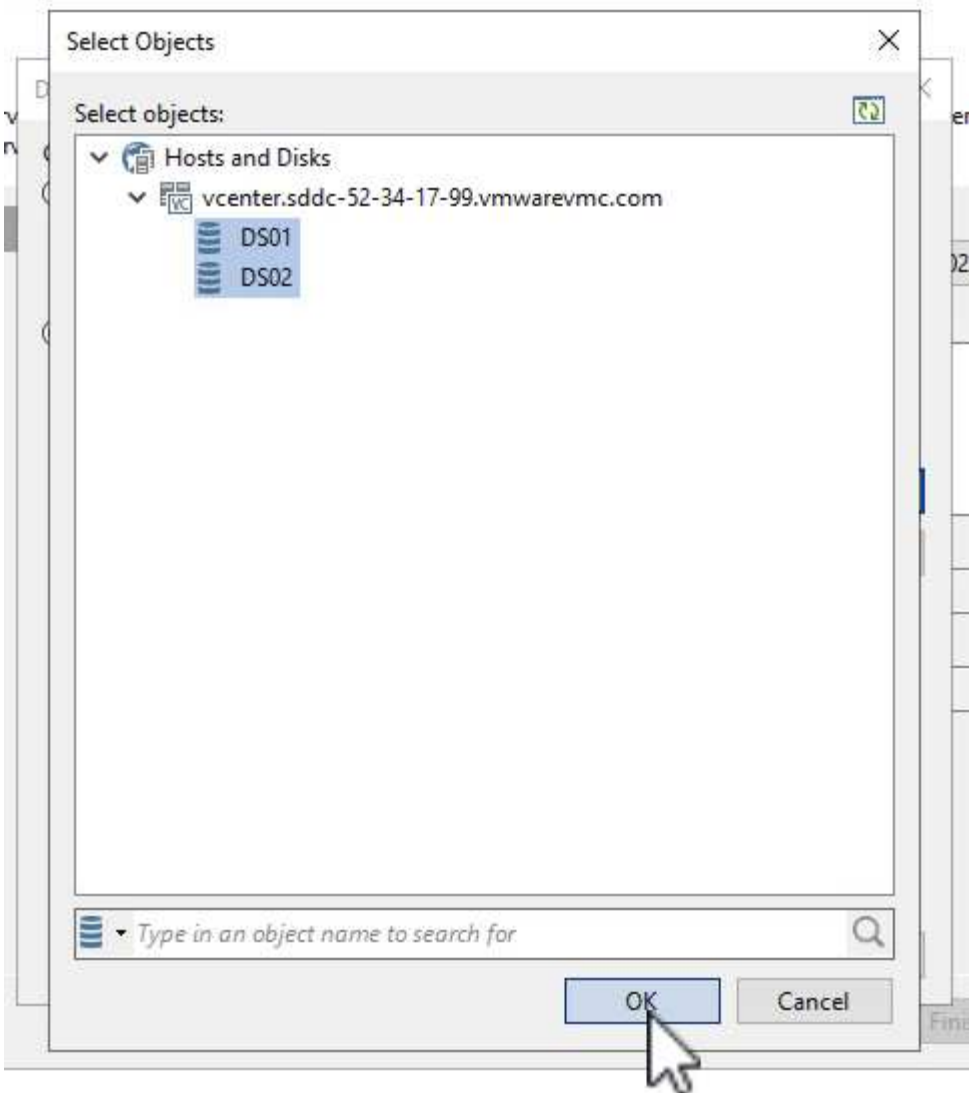


5. 새 VMware 프록시 * 마법사로 돌아가서 전송 모드를 선택합니다. 여기서는 * 자동 선택 * 을 선택했습니다.




6. VMware 프록시에서 직접 액세스할 수 있는 연결된 데이터 저장소를 선택합니다.





- 원하는 암호화 또는 임계치 조절과 같은 특정 네트워크 트래픽 규칙을 구성하고 적용합니다. 완료되면 * Apply * 버튼을 클릭하여 구축을 완료합니다.

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](#)

< Previous

Apply

Finish

Cancel

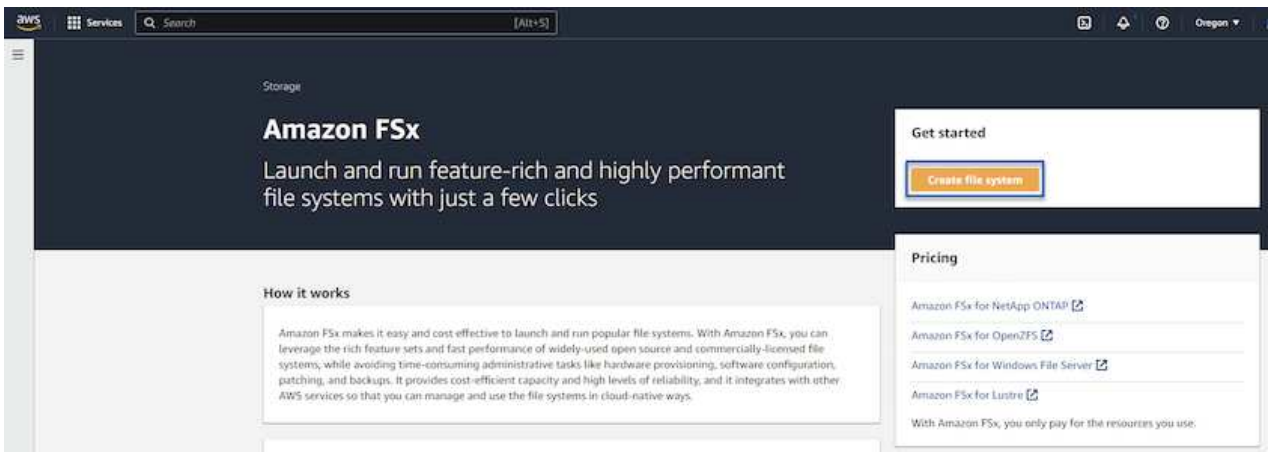
스토리지 및 백업 리포지토리를 구성합니다

Primary Veeam Backup 서버와 Veeam Proxy 서버는 직접 연결된 스토리지의 형태로 백업 저장소에 액세스할 수 있습니다. 이 섹션에서는 ONTAP 파일 시스템용 FSx 생성, Veeam 서버에 iSCSI LUN 마운트 및 백업 저장소 생성에 대해 설명합니다.

ONTAP 파일 시스템용 FSx를 생성합니다

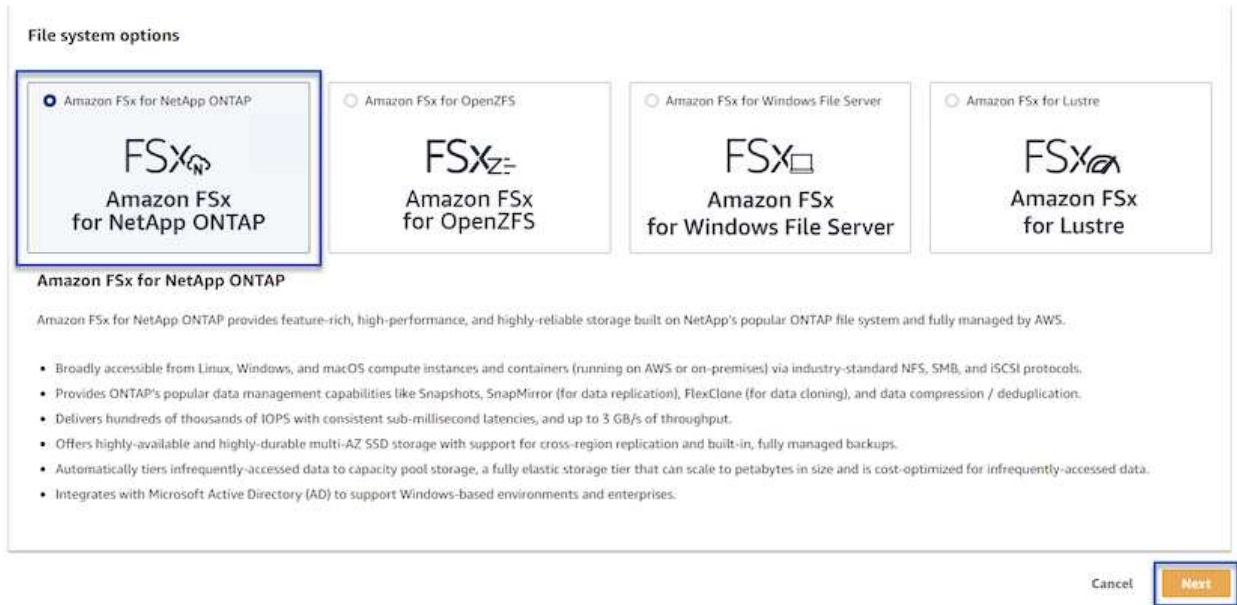
Veeam 백업 리포지토리를 위한 iSCSI 볼륨을 호스팅하는 데 사용할 ONTAP 파일 시스템용 FSx를 생성합니다.

1. AWS 콘솔에서 FSx로 이동한 다음 * 파일 시스템 생성 * 으로 이동합니다



2. 계속하려면 * Amazon FSx for NetApp ONTAP * 를 선택하고 * Next * 를 선택합니다.

Select file system type



3. ONTAP 클러스터용 FSx가 상주할 파일 시스템 이름, 구축 유형, SSD 스토리지 용량 및 VPC를 입력합니다. VMware Cloud에서 가상 머신 네트워크와 통신하도록 VPC를 구성해야 합니다. 다음 * 을 클릭합니다.

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. 배포 단계를 검토하고 * 파일 시스템 생성 * 을 클릭하여 파일 시스템 생성 프로세스를 시작합니다.

iSCSI LUN을 구성 및 마운트합니다

FSx for ONTAP에서 iSCSI LUN을 생성 및 구성하고 Veeam 백업 및 프록시 서버에 마운트합니다. 나중에 이러한 LUN을 사용하여 Veeam 백업 저장소를 생성할 수 있습니다.



ONTAP용 FSx에서 iSCSI LUN을 생성하는 과정은 여러 단계로 이루어집니다. 볼륨을 생성하는 첫 번째 단계는 Amazon FSx 콘솔 또는 NetApp ONTAP CLI에서 수행할 수 있습니다.



ONTAP용 FSx 사용에 대한 자세한 내용은 [참조하십시오 "ONTAP용 FSX 사용 설명서"](#).

1. NetApp ONTAP CLI에서 다음 명령을 사용하여 초기 볼륨을 생성합니다.

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

2. 이전 단계에서 생성한 볼륨을 사용하여 LUN 생성:

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

3. Veeam 백업 및 프록시 서버의 iSCSI IQN이 포함된 이니시에이터 그룹을 생성하여 LUN에 대한 액세스 권한을 부여합니다.

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



위의 단계를 완료하려면 먼저 Windows 서버의 iSCSI 이니시에이터 속성에서 IQN을 검색해야 합니다.

4. 마지막으로 LUN을 방금 생성한 이니시에이터 그룹에 매핑합니다.

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

5. iSCSI LUN을 마운트하려면 Veeam Backup & Replication Server에 로그인하고 iSCSI Initiator Properties를 엽니다. 검색 * 탭으로 이동하여 iSCSI 대상 IP 주소를 입력합니다.

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

- Targets * 탭에서 비활성 LUN을 강조 표시하고 * Connect * 를 클릭합니다. 다중 경로 사용 * 상자를 선택하고 * 확인 * 을 클릭하여 LUN에 연결합니다.

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.d9aad3cd818011edbfc87a...	Inactive

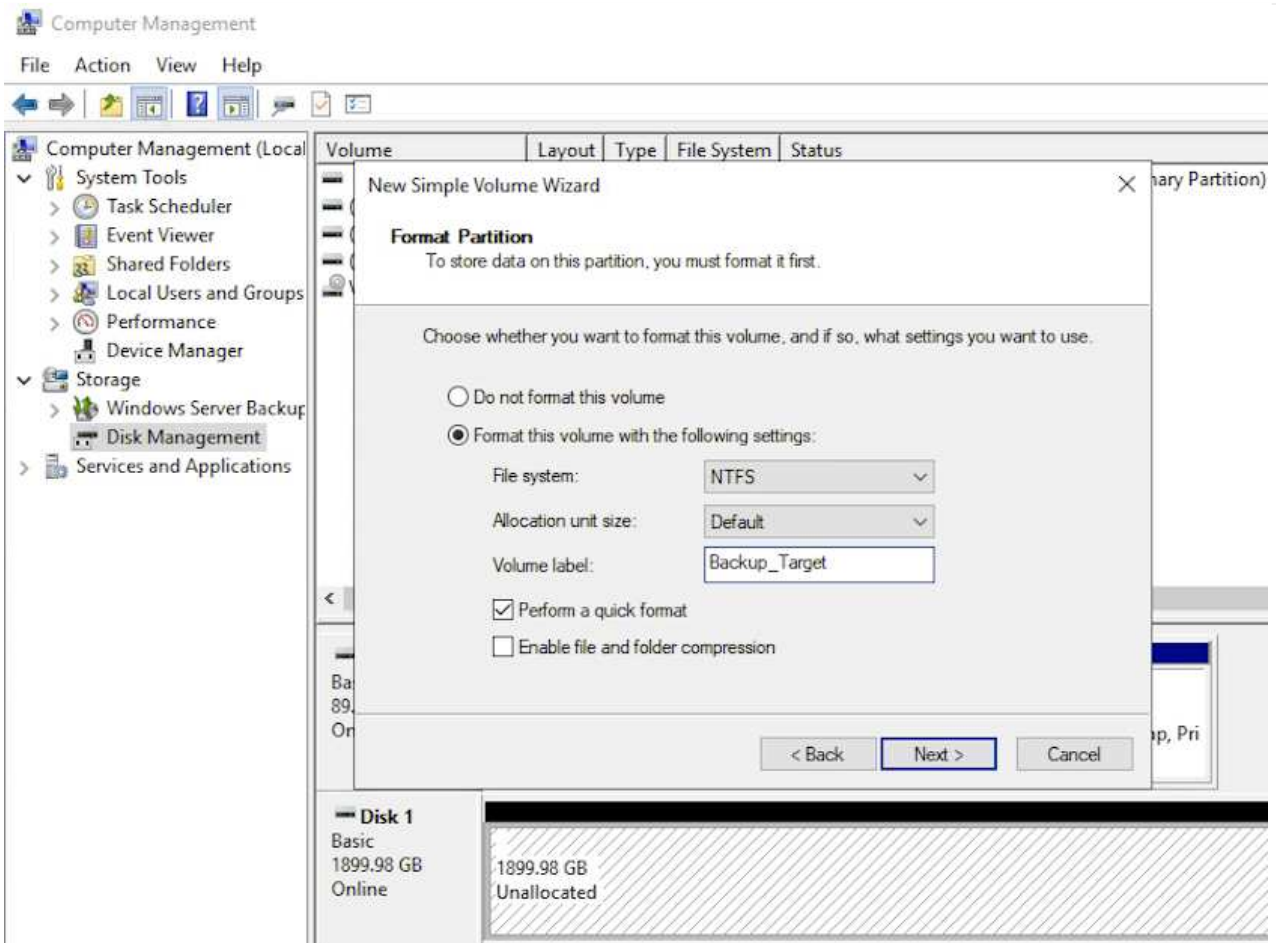
To connect using advanced options, select a target and then click Connect. Connect

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

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

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

7. 디스크 관리 유틸리티에서 새 LUN을 초기화하고 원하는 이름 및 드라이브 문자로 볼륨을 생성합니다. 다중 경로 사용 * 상자를 선택하고 * 확인 * 을 클릭하여 LUN에 연결합니다.

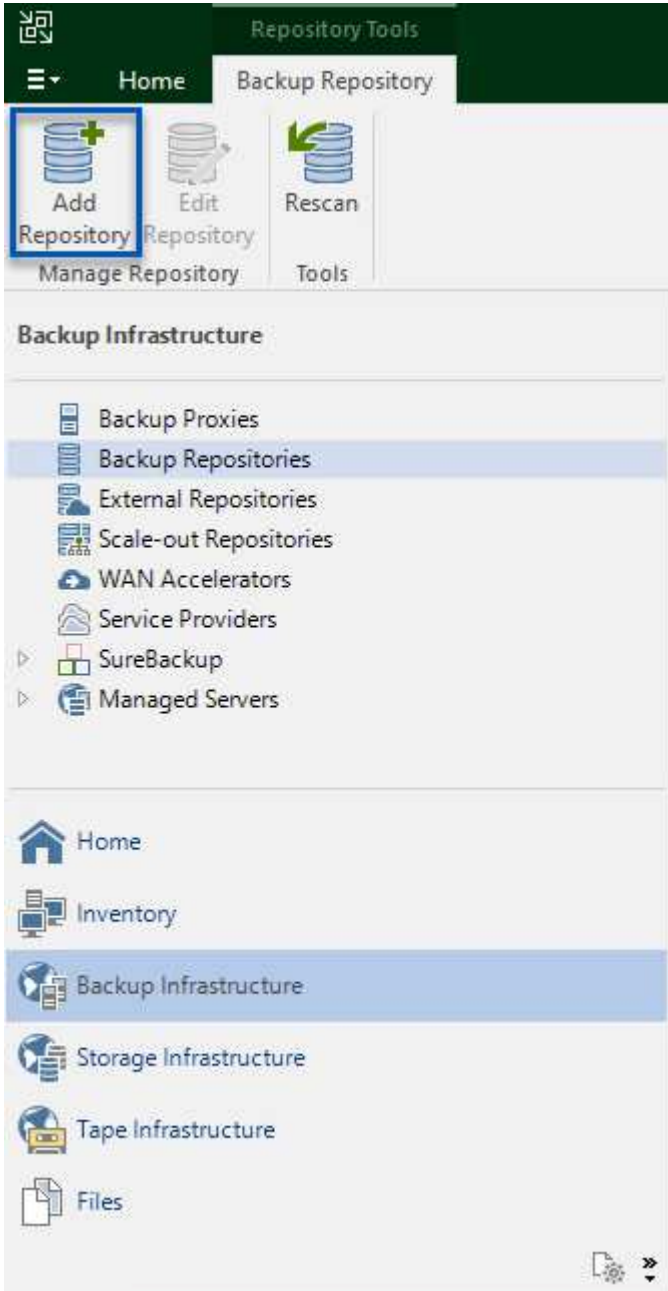


8. 이 단계를 반복하여 Veeam 프록시 서버에 iSCSI 볼륨을 마운트합니다.

Veeam 백업 리포지토리를 생성합니다

Veeam Backup and Replication 콘솔에서 Veeam Backup 및 Veeam Proxy 서버의 백업 저장소를 생성합니다. 이러한 저장소는 가상 머신 백업의 백업 타겟으로 사용됩니다.

1. Veeam Backup and Replication 콘솔의 왼쪽 아래에서 * Backup Infrastructure * 를 클릭한 다음 * Add Repository * 를 선택합니다



2. New Backup Repository(새 백업 리포지토리) 마법사에서 리포지토리 이름을 입력한 다음 드롭다운 목록에서 서버를 선택하고 * 채우기 * 버튼을 클릭하여 사용할 NTFS 볼륨을 선택합니다.

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. 추가 프록시 서버에 대해 이 단계를 반복합니다.

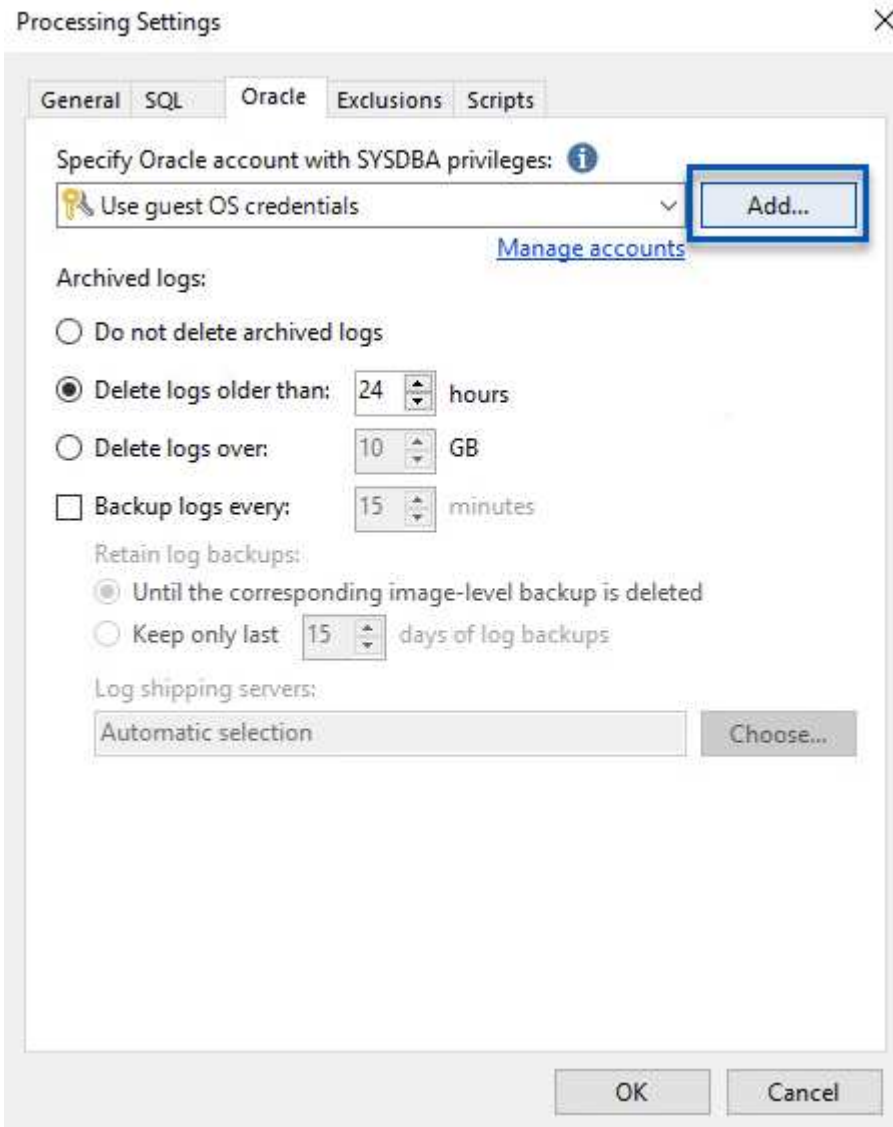
Veeam 백업 작업을 구성합니다

이전 섹션의 백업 리포지토리를 사용하여 백업 작업을 생성해야 합니다. 백업 작업 생성은 스토리지 관리자의 일반적인 일부이며 여기서는 모든 단계를 다루지 않습니다. Veeam에서 백업 작업 생성에 대한 자세한 내용은 ["Veeam Help Center 기술 문서"](#)를 참조하십시오.

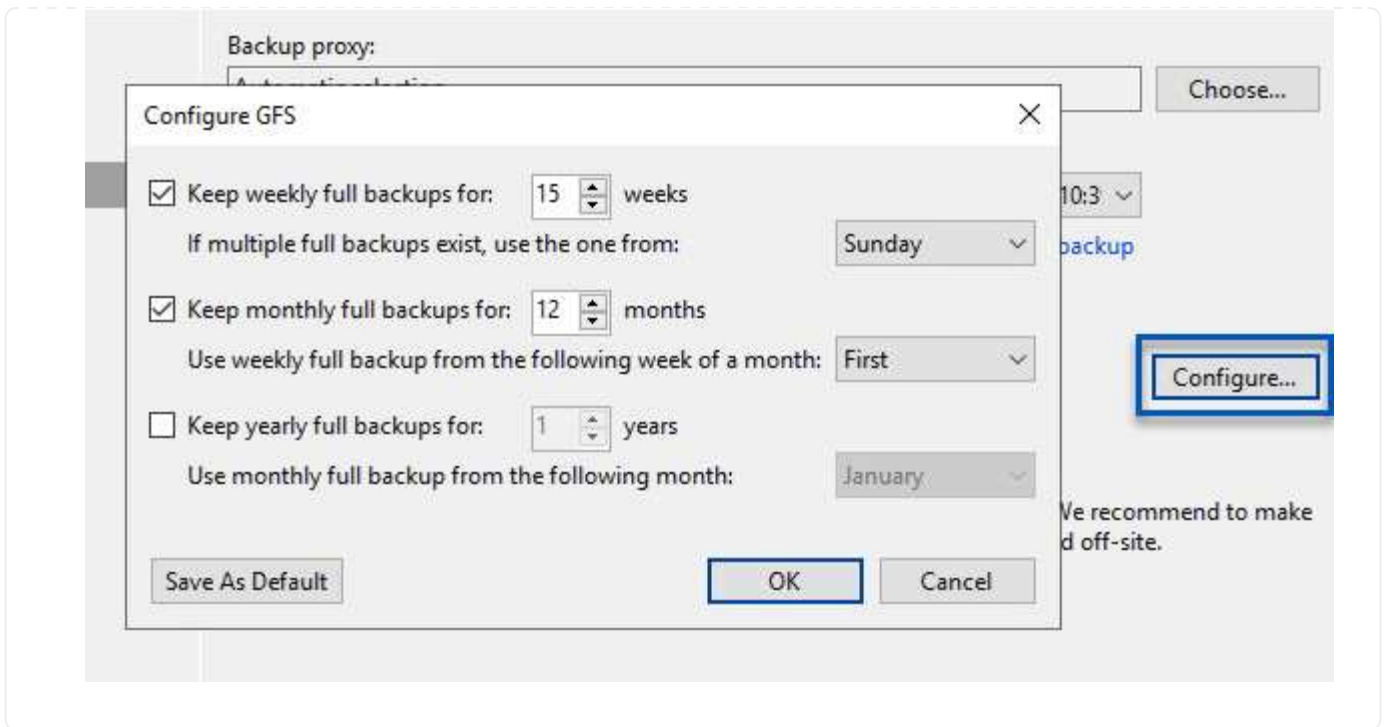
이 솔루션에서는 다음에 대해 별도의 백업 작업이 생성되었습니다.

- Microsoft Windows SQL Server를 참조하십시오
- Oracle 데이터베이스 서버
- Windows 파일 서버
- Linux 파일 서버

1. 애플리케이션 인식 처리를 통해 일관된 백업을 생성하고 트랜잭션 로그 처리를 수행할 수 있습니다.
2. 애플리케이션 인식 처리를 활성화한 후 게스트 OS 자격 증명과 다룰 수 있으므로 애플리케이션에 관리자 권한이 있는 올바른 자격 증명을 추가합니다.



3. 백업의 보존 정책을 관리하려면 * 보관용으로 특정 전체 백업을 더 오래 보존 * 을 선택하고 * 구성... * 버튼을 클릭하여 정책을 구성합니다.



Veeam 전체 복원으로 애플리케이션 VM을 복원합니다

Veeam을 사용하여 전체 복원을 수행하는 것은 애플리케이션 복원을 수행하는 첫 번째 단계입니다. VM의 전체 복원 전원이 켜져 있고 모든 서비스가 정상적으로 실행 중임을 확인했습니다.

서버 복원은 스토리지 관리자의 정상적인 일부이며 여기서는 모든 단계를 다루지 않습니다. Veeam에서 전체 복원을 수행하는 방법에 대한 자세한 내용은 [참조하십시오 "Veeam Help Center 기술 문서"](#).

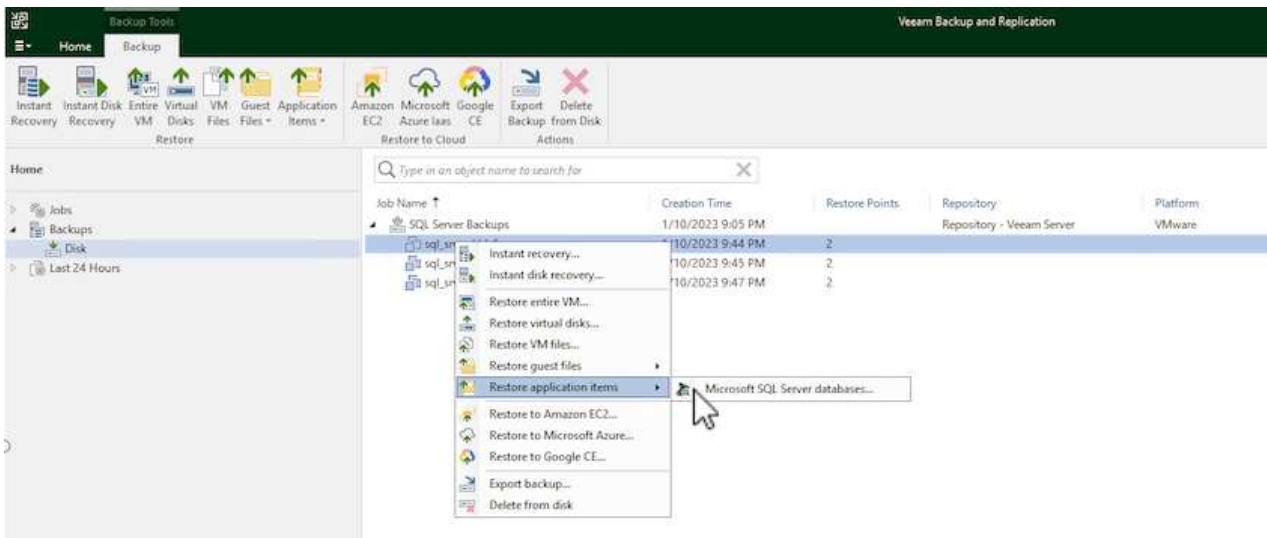
SQL Server 데이터베이스를 복구합니다

Veeam Backup & Replication은 SQL Server 데이터베이스를 복구하는 데 필요한 몇 가지 옵션을 제공합니다. 이 검증을 위해 Veeam Explorer for SQL Server with Instant Recovery를 사용하여 SQL Server 데이터베이스의 복원을 수행했습니다. SQL Server 인스턴트 복구는 전체 데이터베이스 복원을 기다리지 않고 SQL Server 데이터베이스를 신속하게 복원할 수 있는 기능입니다. 이러한 신속한 복구 프로세스는 다운타임을 최소화하고 비즈니스 연속성을 보장합니다. 작동 방식은 다음과 같습니다.

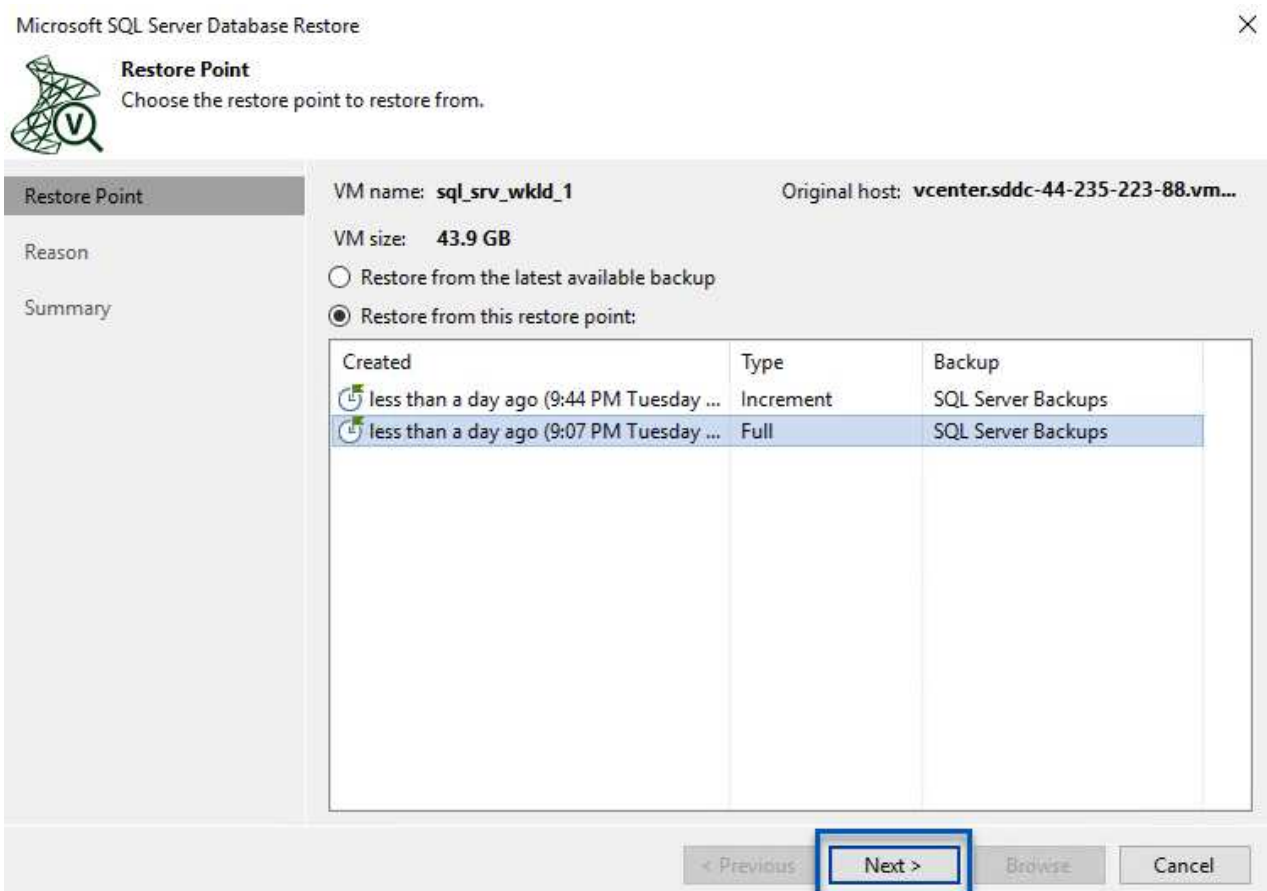
- Veeam Explorer * 는 복구할 SQL Server 데이터베이스가 포함된 백업 * 을 마운트합니다.
- 소프트웨어 * 는 마운트된 파일에서 직접 데이터베이스 * 를 게시하여 대상 SQL Server 인스턴스의 임시 데이터베이스로 액세스할 수 있도록 합니다.
- 임시 데이터베이스를 사용하는 동안 Veeam Explorer * 가 사용자 쿼리 * 를 이 데이터베이스로 리디렉션하여 사용자가 데이터에 계속 액세스하고 사용할 수 있도록 합니다.
- 배경에서 Veeam * 은 전체 데이터베이스 복원 * 을 수행하여 임시 데이터베이스에서 원래 데이터베이스 위치로 데이터를 전송합니다.
- 전체 데이터베이스 복원이 완료되면 Veeam Explorer * 가 사용자 쿼리를 원래 * 데이터베이스로 다시 전환하고 임시 데이터베이스를 제거합니다.

Veeam Explorer 인스턴트 복구를 사용하여 SQL Server 데이터베이스를 복원합니다

1. Veeam Backup and Replication 콘솔에서 SQL Server 백업 목록으로 이동하여 서버를 마우스 오른쪽 버튼으로 클릭하고 * Restore application items * 를 선택한 다음 * Microsoft SQL Server database... * 를 선택합니다.



2. Microsoft SQL Server 데이터베이스 복원 마법사의 목록에서 복원 지점을 선택하고 * 다음 * 을 클릭합니다.



3. 원하는 경우 * Restore Reason * 을 입력한 다음 Summary 페이지에서 * Browse * 버튼을 클릭하여 Veeam Explorer for Microsoft SQL Server를 시작합니다.

**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)

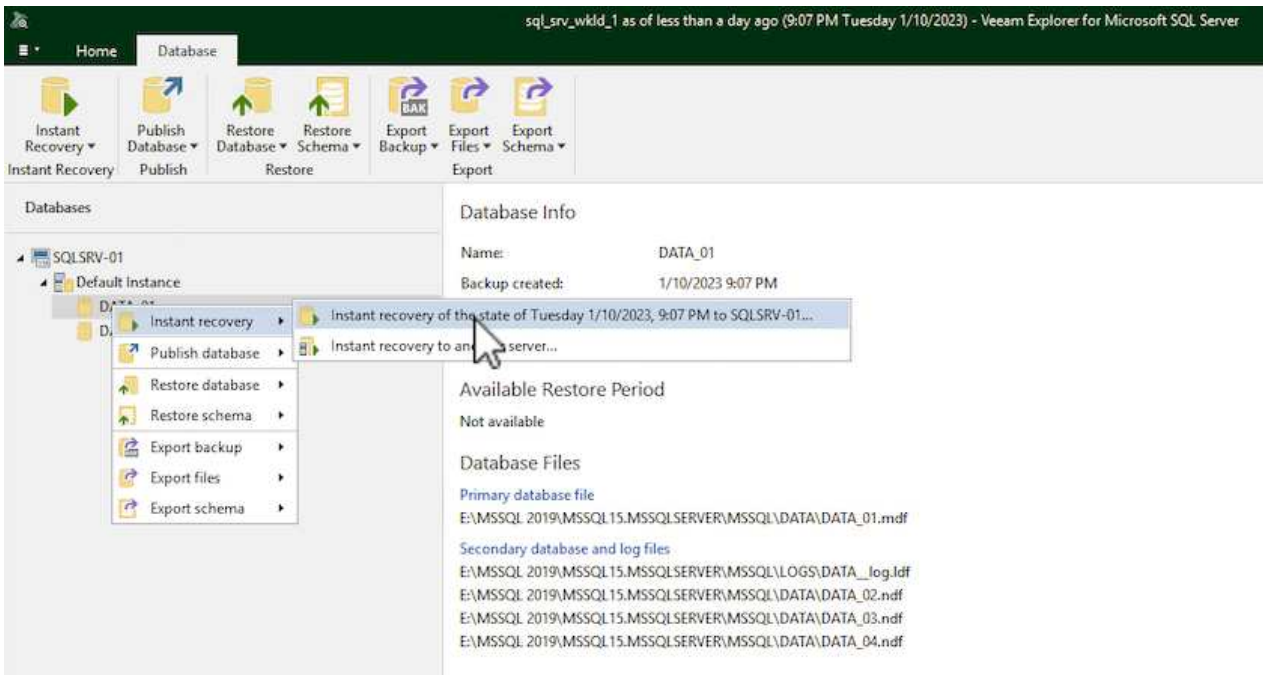
< Previous

Next >

Browse

Cancel

4. Veeam Explorer에서 데이터베이스 인스턴스 목록을 확장하고 * Instant recovery * 를 마우스 오른쪽 버튼으로 클릭한 다음 복구할 특정 복원 지점을 선택합니다.



5. 인스턴트 복구 마법사에서 전환 유형을 지정합니다. 이 작업은 최소한의 가동 중지 시간, 수동 또는 지정된 시간에 자동으로 수행할 수 있습니다. 그런 다음 * 복구 * 버튼을 클릭하여 복원 프로세스를 시작합니다.

Instant Recovery Wizard

Specify database switchover scheduling options

Specify switchover type:

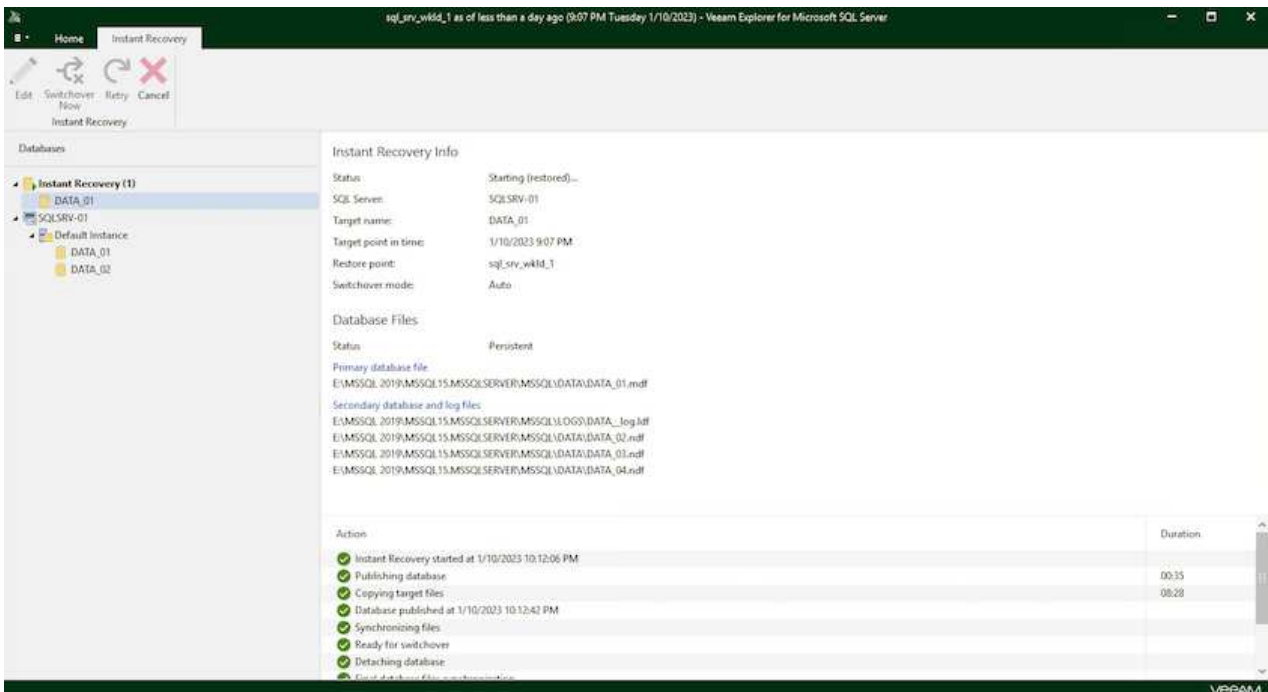
☒ Auto
Switchover will be performed automatically with minimal possible downtime once the database is ready.

☐ 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. 복구 프로세스는 Veeam Explorer에서 모니터링할 수 있습니다.



Veeam Explorer로 SQL Server 복원 작업을 수행하는 방법에 대한 자세한 내용은 [Microsoft SQL Server](#) 섹션을 참조하십시오 ["Veeam Explorers 사용자 가이드"](#).

Veeam Explorer로 Oracle 데이터베이스를 복구합니다

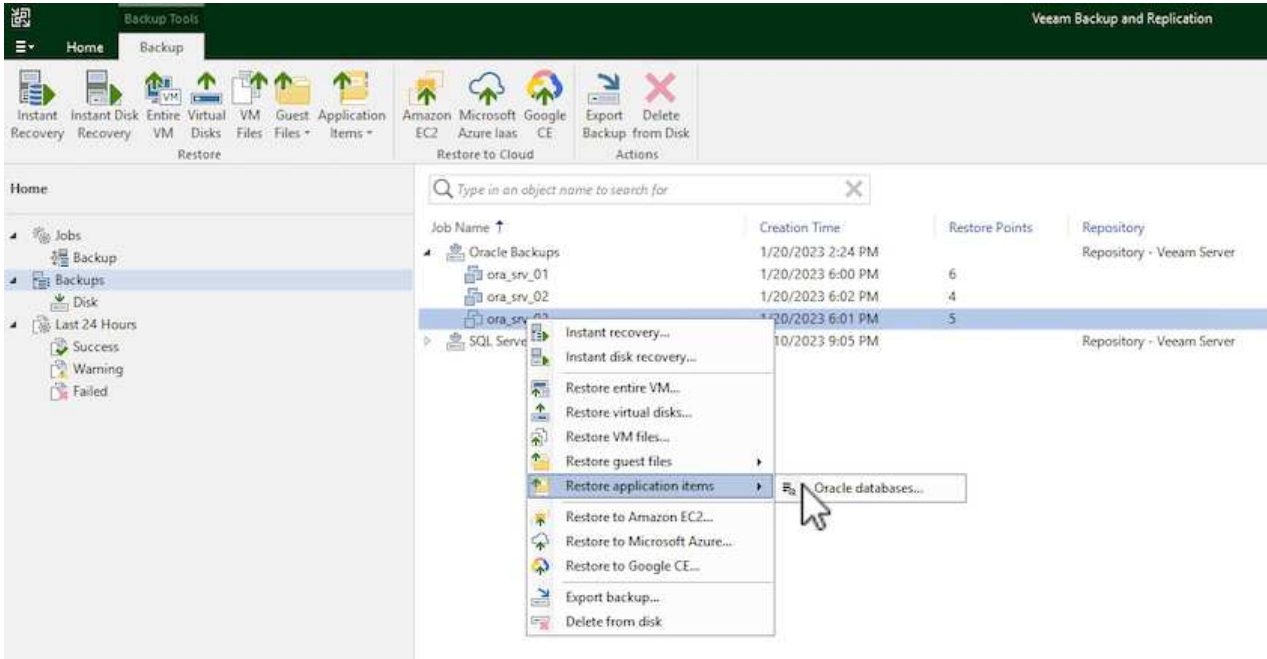
Oracle 데이터베이스용 Veeam Explorer를 사용하면 표준 Oracle 데이터베이스 복원 또는 즉각적인 복구를 통해 무중단 복원을 수행할 수 있습니다. 또한 빠른 액세스, Data Guard 데이터베이스 복구 및 RMAN 백업으로부터의 복구를 위해 데이터베이스를 게시하는 기능도 지원합니다.

Veeam Explorer로 Oracle 데이터베이스 복원 작업을 수행하는 방법에 대한 자세한 내용은 [의 Oracle 섹션](#)을 참조하십시오 "[Veeam Explorers 사용자 가이드](#)".

Veeam Explorer로 Oracle 데이터베이스를 복원합니다

이 섹션에서는 Veeam Explorer를 사용하여 다른 서버로 Oracle 데이터베이스를 복구하는 방법에 대해 설명합니다.

1. Veeam Backup and Replication 콘솔에서 Oracle 백업 목록으로 이동하여 서버를 마우스 오른쪽 버튼으로 클릭하고 * Restore application items * 를 선택한 다음 * oracle databases... * 를 선택합니다.



2. Oracle Database Restore Wizard의 목록에서 복원 지점을 선택하고 * Next * 를 클릭합니다.

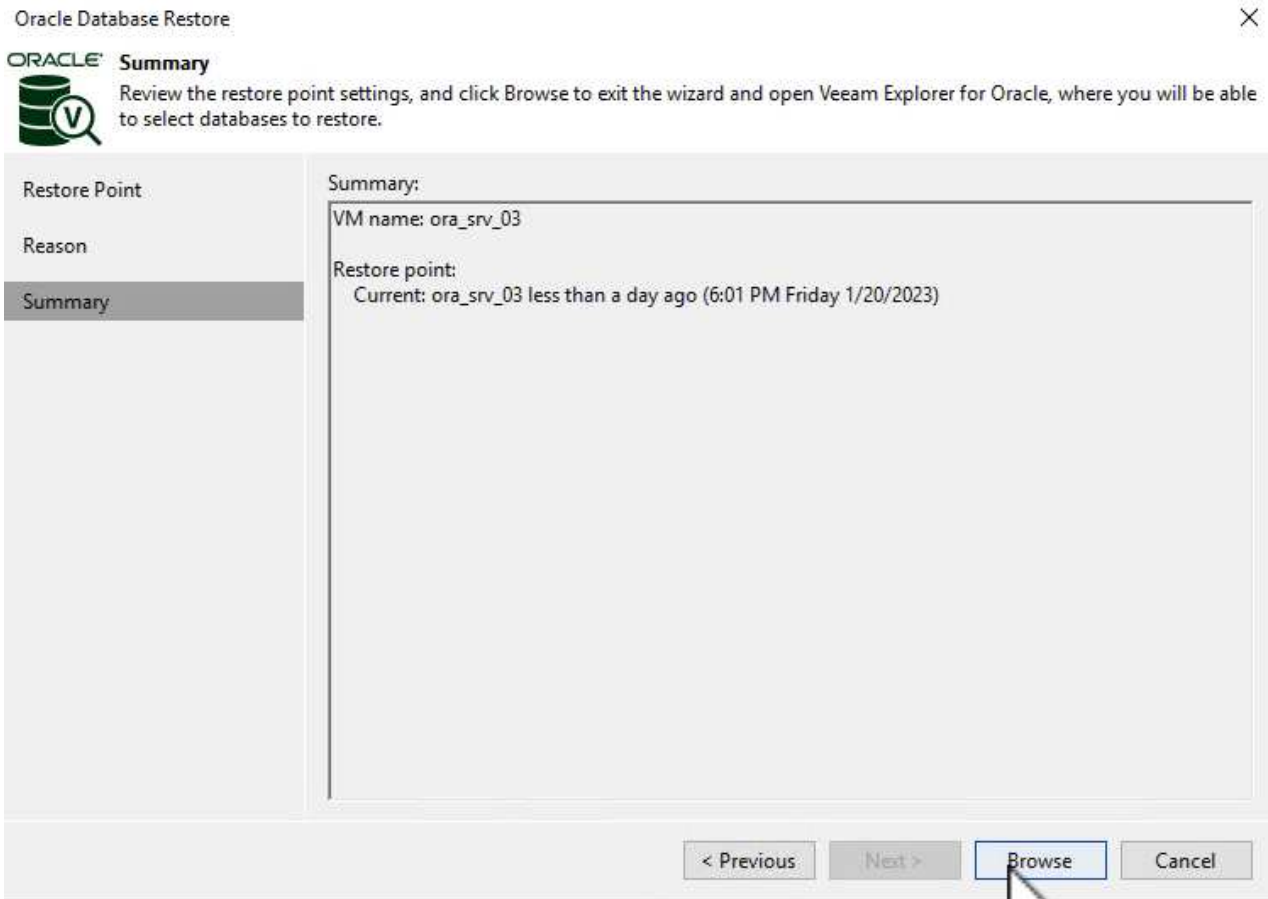


Restore Point

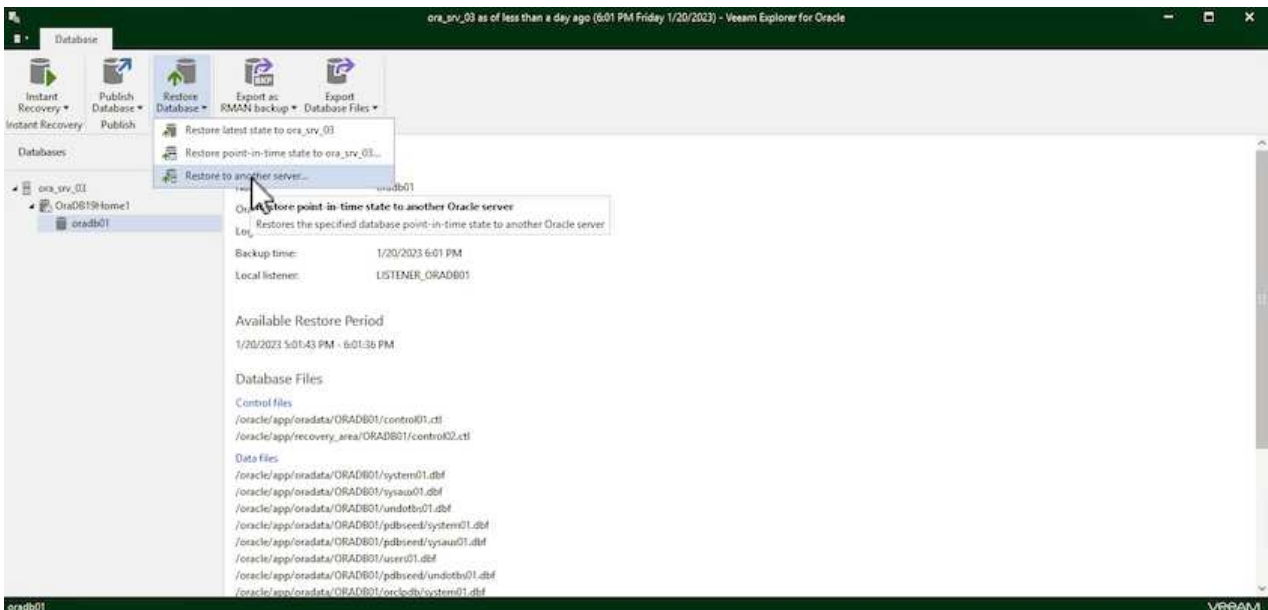
Choose the restore point to restore from.

Restore Point	VM name: ora_srv_03	Original host: vcenter.sddc-44-235-223-88.vm...																		
Reason	VM size: 38.5 GB																			
Summary	<input checked="" type="radio"/> Restore from the latest available backup <input type="radio"/> Restore from this restore point:																			
	<table><thead><tr><th>Created</th><th>Type</th><th>Backup</th></tr></thead><tbody><tr><td> less than a day ago (6:01 PM Friday 1/...</td><td>Increment</td><td>Oracle Backups</td></tr><tr><td> less than a day ago (5:01 PM Friday 1/...</td><td>Increment</td><td>Oracle Backups</td></tr><tr><td> less than a day ago (4:02 PM Friday 1/...</td><td>Increment</td><td>Oracle Backups</td></tr><tr><td> less than a day ago (3:47 PM Friday 1/...</td><td>Increment</td><td>Oracle Backups</td></tr><tr><td> less than a day ago (2:47 PM Friday 1/...</td><td>Full</td><td>Oracle Backups</td></tr></tbody></table>		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
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																		
<div>< Previous Next > Browse Cancel</div>																				

3. 원하는 경우 * Restore Reason * 을 입력한 다음 Summary 페이지에서 * Browse * 버튼을 클릭하여 Veeam Explorer for Oracle을 시작합니다.



4. Veeam Explorer에서 데이터베이스 인스턴스 목록을 확장하고 복원할 데이터베이스를 클릭한 다음 상단의 * Restore Database * 드롭다운 메뉴에서 * Restore to another server... * 를 선택합니다.



5. 복원 마법사에서 복원할 복원 지점을 지정하고 * 다음 * 을 클릭합니다.

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

6. 데이터베이스를 복원할 대상 서버와 계정 자격 증명을 지정하고 * 다음 * 을 클릭합니다.

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

7. 마지막으로 데이터베이스 파일 대상 위치를 지정하고 * 복원 * 버튼을 클릭하여 복원 프로세스를 시작합니다.

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

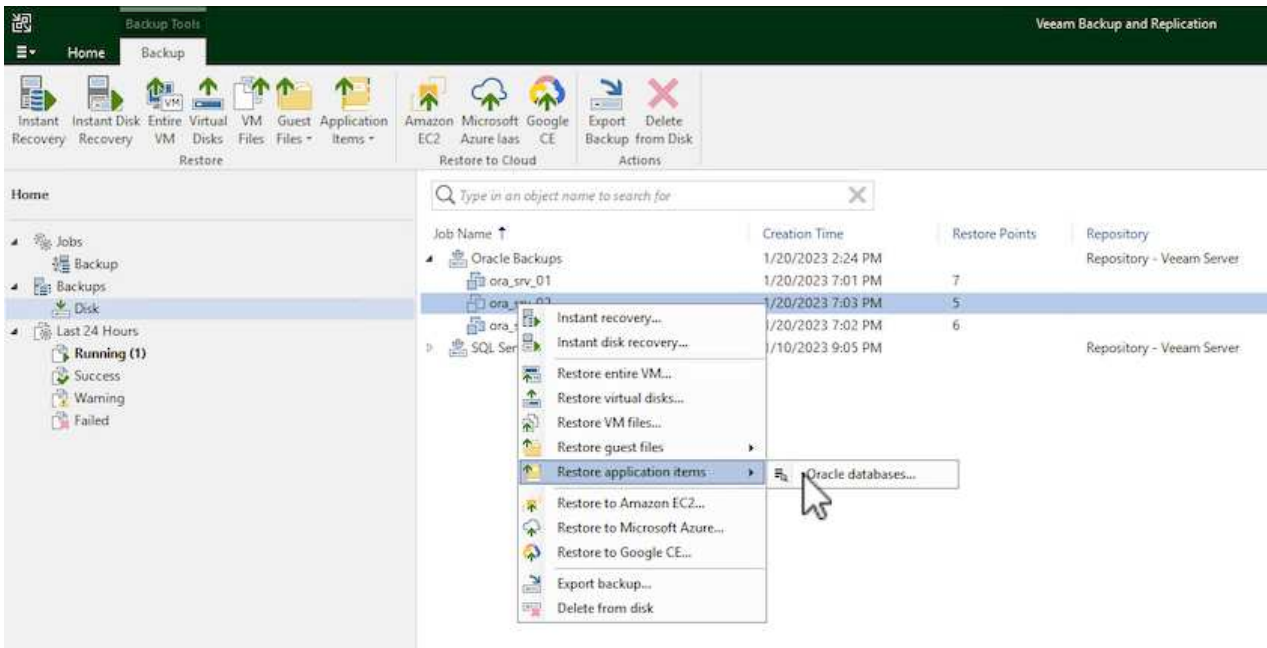
Cancel

8. 데이터베이스 복구가 완료되면 서버에서 Oracle 데이터베이스가 올바르게 시작되는지 확인합니다.

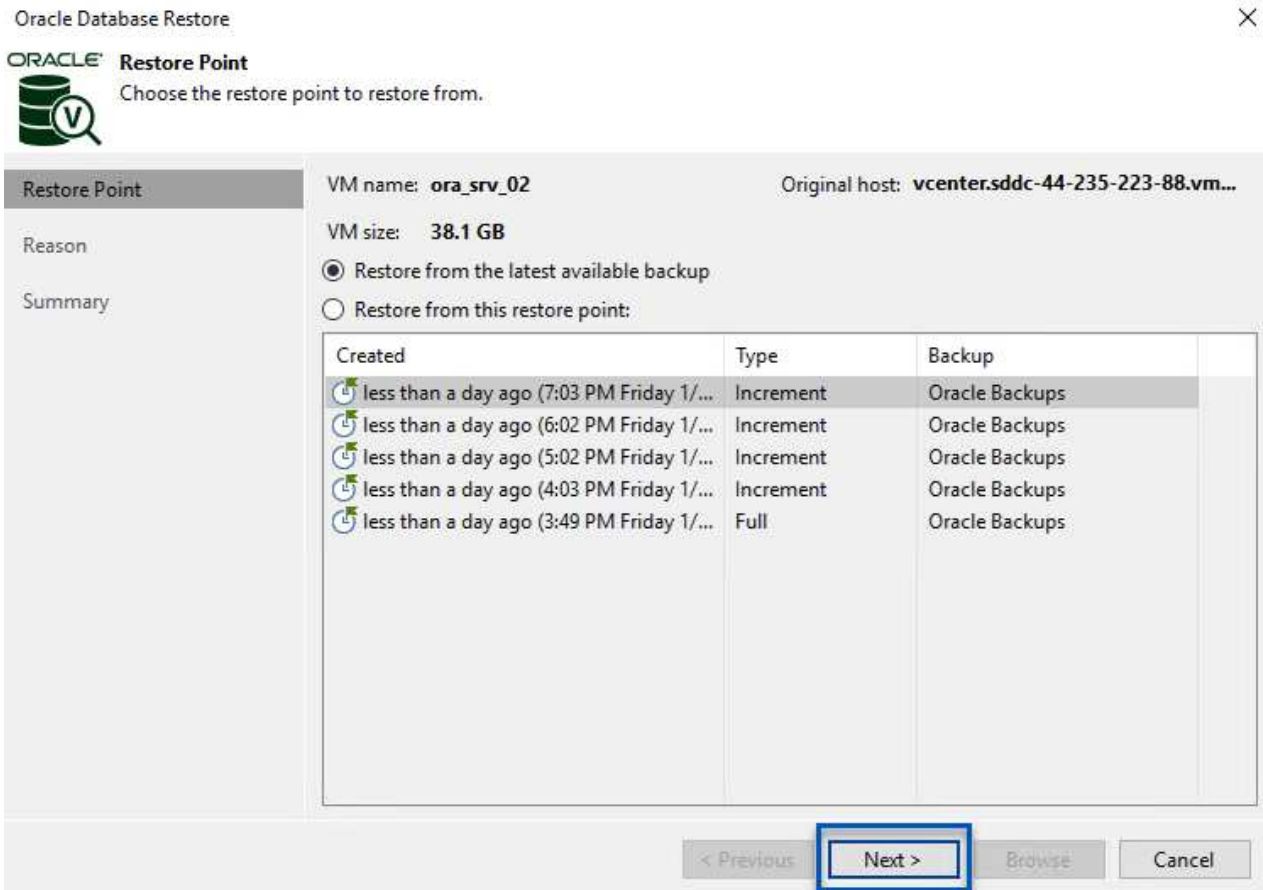
Oracle 데이터베이스를 대체 서버에 게시합니다

이 섹션에서는 전체 복원을 시작하지 않고 빠르게 액세스할 수 있도록 데이터베이스를 대체 서버에 게시합니다.

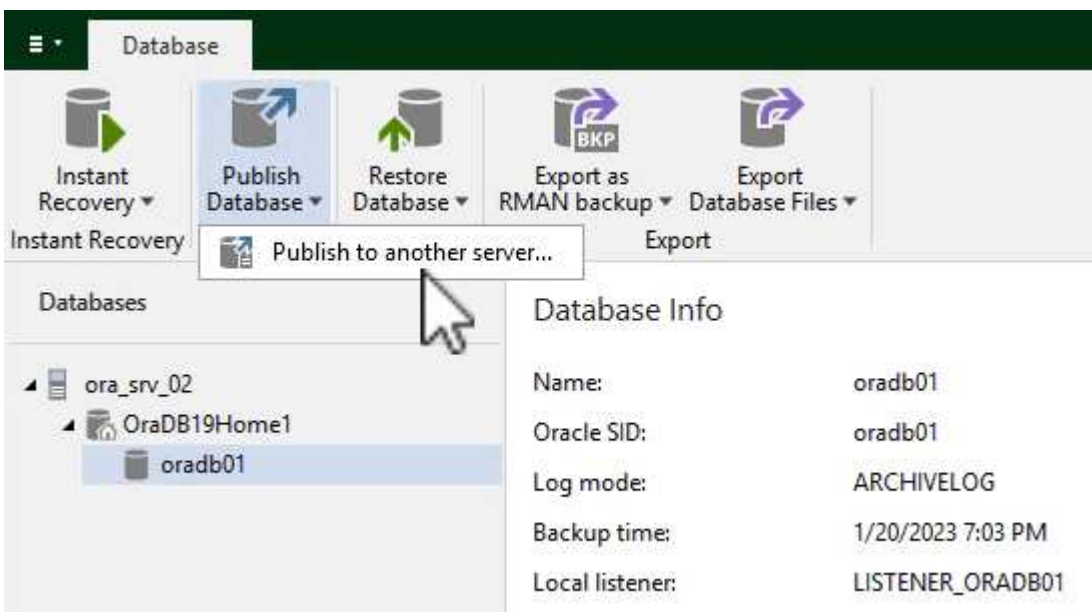
1. Veeam Backup and Replication 콘솔에서 Oracle 백업 목록으로 이동하여 서버를 마우스 오른쪽 버튼으로 클릭하고 * Restore application items * 를 선택한 다음 * oracle databases... * 를 선택합니다.



2. Oracle Database Restore Wizard의 목록에서 복원 지점을 선택하고 * Next * 를 클릭합니다.



- 원하는 경우 * Restore Reason * 을 입력한 다음 Summary 페이지에서 * Browse * 버튼을 클릭하여 Veeam Explorer for Oracle을 시작합니다.
- Veeam Explorer에서 데이터베이스 인스턴스 목록을 확장하고 복원할 데이터베이스를 클릭한 다음 상단의 * Publish Database * 드롭다운 메뉴에서 * Publish to another server... * 를 선택합니다.



- 게시 마법사에서 데이터베이스를 게시할 복원 지점을 지정하고 * 다음 * 을 클릭합니다.
- 마지막으로 대상 Linux 파일 시스템 위치를 지정하고 * 게시 * 를 클릭하여 복원 프로세스를 시작합니다.

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. 게시가 완료되면 대상 서버에 로그인하고 다음 명령을 실행하여 데이터베이스가 실행 중인지 확인합니다.

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

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

```
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 |


```

결론

VMware Cloud는 비즈니스 크리티컬 애플리케이션을 실행하고 중요한 데이터를 저장할 수 있는 강력한 플랫폼입니다. 비즈니스 연속성을 보장하고 사이버 위협 및 데이터 손실을 방지하기 위해 VMware Cloud를 사용하는 기업에게 보안 데이터 보호 솔루션은 필수적입니다. 안정적이고 강력한 데이터 보호 솔루션을 선택함으로써 기업은 중요한 데이터가 무엇에 관계없이 안전하고 안전하다는 확신을 가질 수 있습니다.

이 문서에 제공된 사용 사례는 NetApp, VMware, Veeam의 통합을 강조하는 검증된 데이터 보호 기술에 중점을 둡니다. ONTAP용 FSX는 AWS에서 VMware Cloud를 위한 보조 NFS 데이터 저장소로 지원되며 모든 가상 머신 및 애플리케이션 데이터에 사용됩니다. Veeam Backup & Replication은 기업이 백업 및 복구 프로세스를 개선, 자동화 및 간소화할 수 있도록 설계된 포괄적인 데이터 보호 솔루션입니다. Veeam을 ONTAP용 FSX에서 호스팅되는 iSCSI 백업 타겟 볼륨과 함께 사용하면 VMware Cloud에 상주하는 애플리케이션 데이터를 안전하고 쉽게 관리할 수 있는 데이터 보호 솔루션을 제공할 수 있습니다.

추가 정보

이 솔루션에 제공되는 기술에 대한 자세한 내용은 다음 추가 정보를 참조하십시오.

- ["ONTAP용 FSX 사용 설명서"](#)
- ["Veeam Help Center 기술 문서"](#)
- ["AWS의 VMware Cloud 지원: 고려 사항 및 제한 사항"](#)

TR-4955: ONTAP 및 VMC(AWS VMware Cloud)용 FSx를 통한 재해 복구

Niyaz Mohamed, NetApp

개요

클라우드 재해 복구는 사이트 운영 중단 및 데이터 손상 이벤트(예: 랜섬웨어)로부터 워크로드를 보호하는 복원력이 있고 비용 효율적인 방법입니다. NetApp SnapMirror 기술을 사용하면 사내 VMware 워크로드를 AWS에서 실행되는 ONTAP의 FSx에 복제할 수 있습니다.

DRO(재해 복구 오케스트레이터, UI를 포함한 스크립팅된 솔루션)를 사용하여 사내에서 ONTAP용 FSx로 복제된 워크로드를 원활하게 복구할 수 있습니다. DRO는 VM 등록을 통해 SnapMirror 레벨에서 VMC로 복구를 자동화하고 NSX-T에서 직접 네트워크 매핑을 수행합니다. 이 기능은 모든 VMC 환경에 포함되어 있습니다.

시작하기

AWS에서 VMware Cloud를 구축 및 구성합니다

"AWS 기반 VMware 클라우드" AWS 에코시스템의 VMware 기반 워크로드에 클라우드 네이티브 경험을 제공합니다. 각 VMware SDDC(소프트웨어 정의 데이터 센터)는 VPC(Amazon Virtual Private Cloud)에서 실행되며 전체 VMware 스택(vCenter Server 포함), NSX-T 소프트웨어 정의 네트워킹, vSAN 소프트웨어 정의 스토리지 및 워크로드에 컴퓨팅 및 스토리지 리소스를 제공하는 하나 이상의 ESXi 호스트를 제공합니다. AWS에서 VMC 환경을 구성하려면 다음 단계를 수행하십시오 ["링크"](#). DR 목적으로도 파일럿 라이트 클러스터를 사용할 수 있습니다.



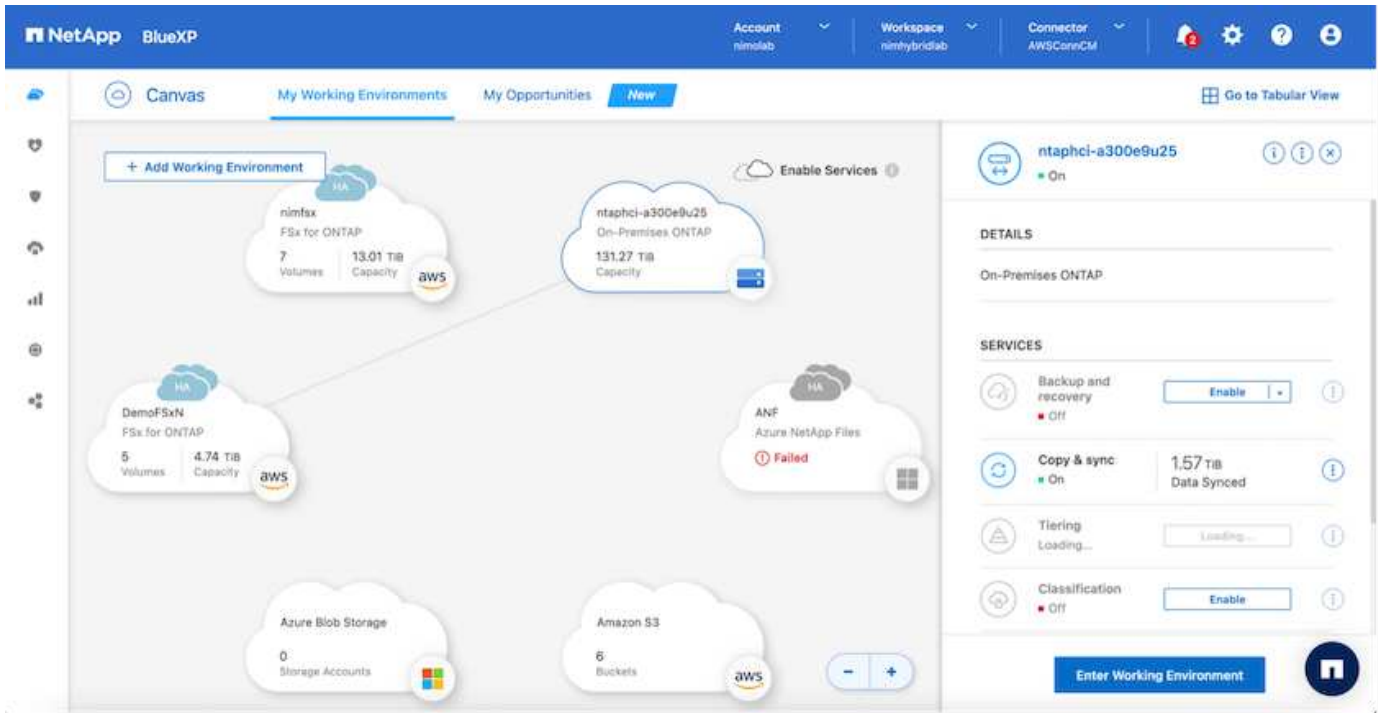
최초 릴리즈에서 DRO는 기존의 파일럿 라이트 클러스터를 지원합니다. 온디맨드 SDDC 작성은 향후 릴리스에서 제공될 예정입니다.

ONTAP용 FSx를 프로비저닝하고 구성합니다

NetApp ONTAP용 Amazon FSx는 널리 사용되는 NetApp ONTAP 파일 시스템에 구축된 매우 안정적이고 확장 가능하며 고성능의 풍부한 기능 파일 스토리지를 제공하는 완전 관리형 서비스입니다. 이 단계를 따릅니다 ["링크"](#) ONTAP용 FSx를 프로비저닝하고 구성하려면 다음을 수행합니다.

ONTAP용 FSx에 SnapMirror를 구축하고 구성합니다

다음 단계는 NetApp BlueXP를 사용하고 AWS에서 ONTAP용 프로비저닝된 FSx 인스턴스를 검색하고 적절한 빈도와 NetApp 스냅샷 복사본 보존을 사용하여 원하는 데이터 저장소 볼륨을 사내 환경에서 ONTAP용 FSx로 복제하는 것입니다.



이 링크의 단계에 따라 BlueXP를 구성합니다. NetApp ONTAP CLI를 사용하여 이 링크 이후의 복제를 예약할 수도 있습니다.



SnapMirror 관계는 전제 조건이며 미리 만들어야 합니다.

DRO 설치

DRO를 시작하려면 지정된 EC2 인스턴스 또는 가상 시스템에서 Ubuntu 운영 체제를 사용하여 필수 구성 요소를 충족하는지 확인합니다. 그런 다음 패키지를 설치합니다.

필수 구성 요소

- 소스 및 대상 vCenter 및 스토리지 시스템에 대한 접속이 있는지 확인합니다.
- DNS 이름을 사용하는 경우 DNS 확인이 필요합니다. 그렇지 않으면 vCenter 및 스토리지 시스템의 IP 주소를 사용해야 합니다.
- 루트 권한이 있는 사용자를 생성합니다. EC2 인스턴스에서 sudo를 사용할 수도 있습니다.

OS 요구 사항

- 최소 2GB 및 4개의 vCPU가 있는 Ubuntu 20.04(LTS)
- 지정된 에이전트 VM에 다음 패키지를 설치해야 합니다.
 - Docker 를 참조하십시오
 - Docker-Compose
 - JQ

의 사용 권한을 변경합니다 `docker.sock: sudo chmod 666 /var/run/docker.sock.`



를 클릭합니다 deploy.sh 스크립트는 필요한 모든 필수 구성 요소를 실행합니다.

패키지를 설치합니다

1. 지정된 가상 머신에 설치 패키지를 다운로드합니다.

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



이 에이전트는 사내에 설치하거나 AWS VPC 내에 설치할 수 있습니다.

2. 패키지의 압축을 풀고 배포 스크립트를 실행한 다음 호스트 IP(예: 10.10.10)를 입력합니다.

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

3. 디렉토리로 이동하고 다음과 같이 배포 스크립트를 실행합니다.

```
sudo sh deploy.sh
```

4. 다음을 사용하여 UI에 액세스합니다.

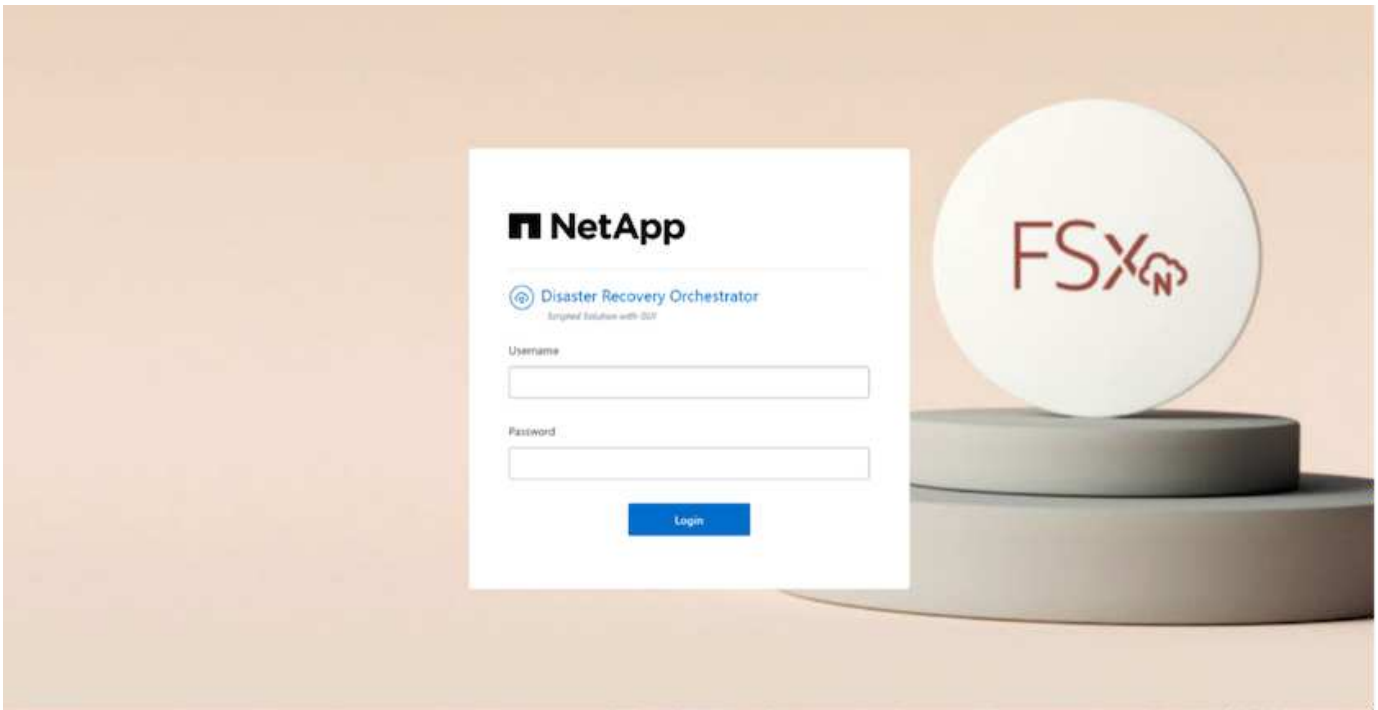
```
https://<host-ip-address>
```

다음 기본 자격 증명을 사용합니다.

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



암호는 "암호 변경" 옵션을 사용하여 변경할 수 있습니다.



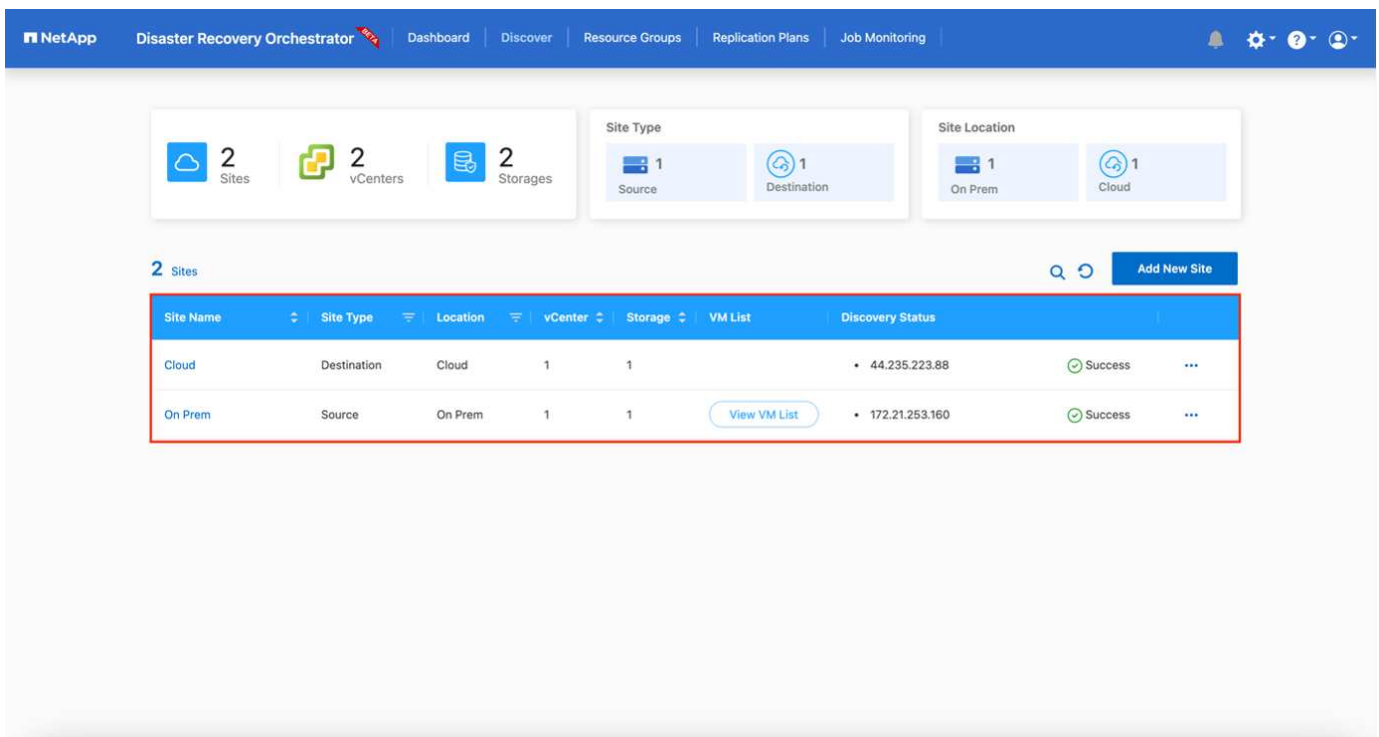
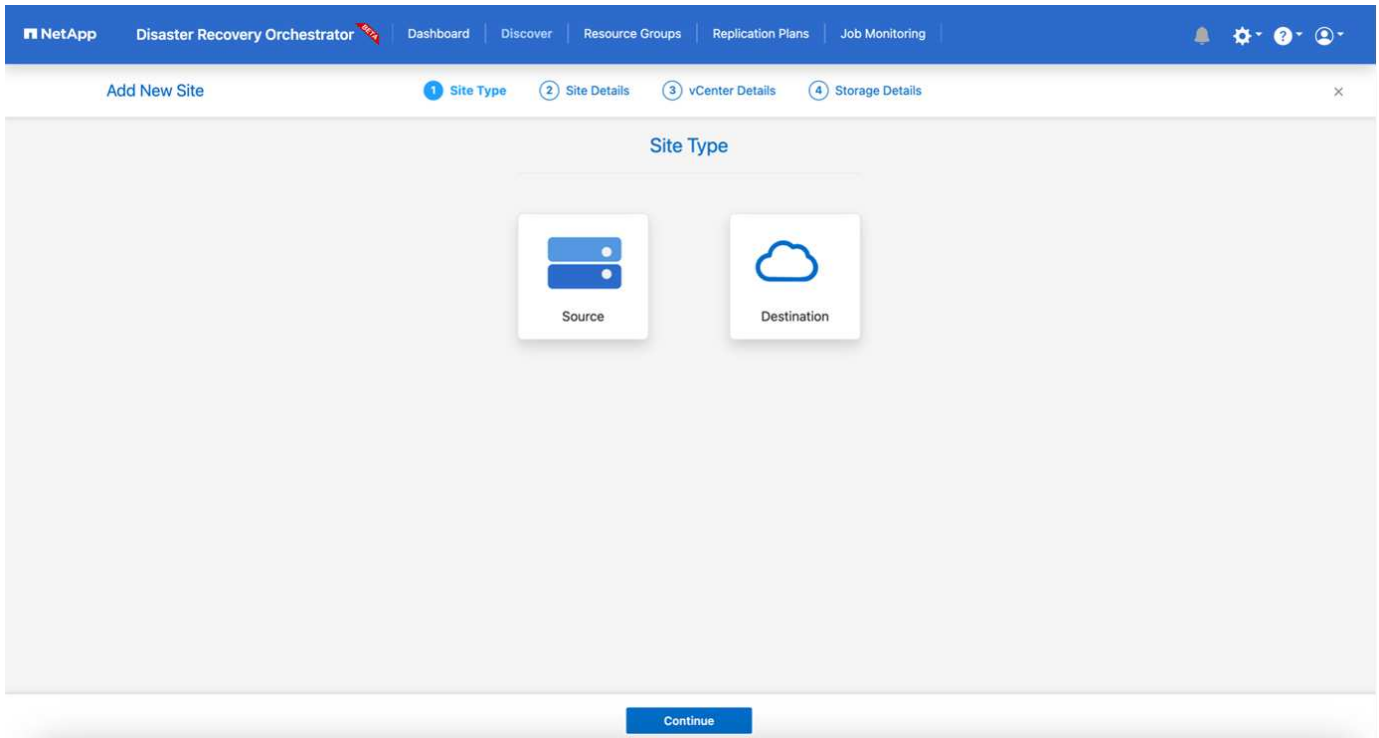
DRO 구성

ONTAP 및 VMC용 FSx가 올바르게 구성된 후에는 ONTAP용 FSx에서 읽기 전용 SnapMirror 복사본을 사용하여 VMC로 온-프레미스 워크로드의 복구를 자동화하도록 DRO를 구성할 수 있습니다.

ONTAP용 FSx가 구축된 AWS 및 동일한 VPC에 DRO 에이전트를 구축하는 것이 좋습니다(피어 연결도 가능). DRO 에이전트가 네트워크를 통해 온-프레미스 구성 요소와 ONTAP 및 VMC용 FSx 리소스와 통신할 수 있도록 합니다.

첫 번째 단계는 온프레미스 및 클라우드 리소스(vCenter 및 스토리지 모두)를 DRO에 검색하고 추가하는 것입니다. 지원되는 브라우저에서 DRO를 열고 기본 사용자 이름 및 암호(admin/admin)와 사이트 추가를 사용합니다. 검색 옵션을 사용하여 사이트를 추가할 수도 있습니다. 다음 플랫폼을 추가합니다.

- 온프레미스
 - 사내 vCenter
 - ONTAP 스토리지 시스템
- 클라우드
 - VMC vCenter
 - ONTAP용 FSX



추가된 DRO는 자동 검색을 수행하고 소스 스토리지에서 ONTAP용 FSx로 해당 SnapMirror 복제본이 있는 VM을 표시합니다. DRO는 VM에서 사용하는 네트워크 및 포트 그룹을 자동으로 감지하여 채웁니다.

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-vcsa02	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

다음 단계는 필요한 VM을 기능 그룹으로 그룹화하여 리소스 그룹 역할을 하는 것입니다.

리소스 그룹화

플랫폼을 추가한 후 복구할 VM을 리소스 그룹으로 그룹화할 수 있습니다. DRO 리소스 그룹을 사용하면 종속 VM 집합을 부팅 순서, 부팅 지연 및 복구 시 실행할 수 있는 선택적 응용 프로그램 유효성 검사가 포함된 논리 그룹으로 그룹화할 수 있습니다.

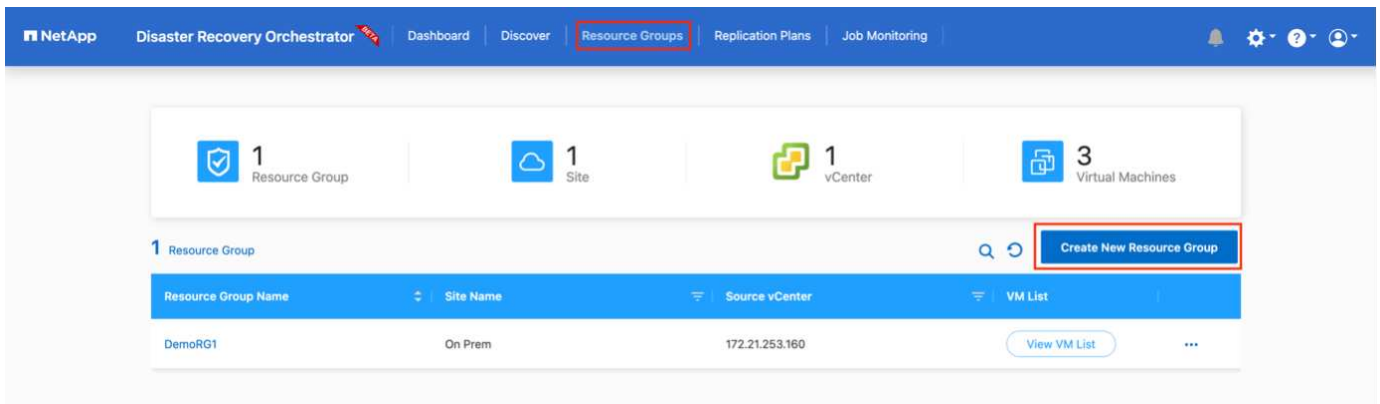
리소스 그룹 생성을 시작하려면 다음 단계를 수행하십시오.

1. 리소스 그룹 * 에 액세스하여 * 새 리소스 그룹 생성 * 을 클릭합니다.
2. 새 리소스 그룹 * 의 드롭다운에서 소스 사이트를 선택하고 * 만들기 * 를 클릭합니다.
3. 리소스 그룹 세부 정보 * 를 입력하고 * 계속 * 을 클릭합니다.
4. 검색 옵션을 사용하여 적절한 VM을 선택합니다.
5. 선택한 VM의 부팅 순서 및 부팅 지연(초)을 선택합니다. 각 VM을 선택하고 우선 순위를 설정하여 전원 켜기 순서의 순서를 설정합니다. 모든 VM의 기본값은 3입니다.

옵션은 다음과 같습니다.

1 – 전원을 켤 첫 번째 가상 머신 3 – 기본값 5 – 전원을 켤 마지막 가상 머신

6. 리소스 그룹 만들기 * 를 클릭합니다.

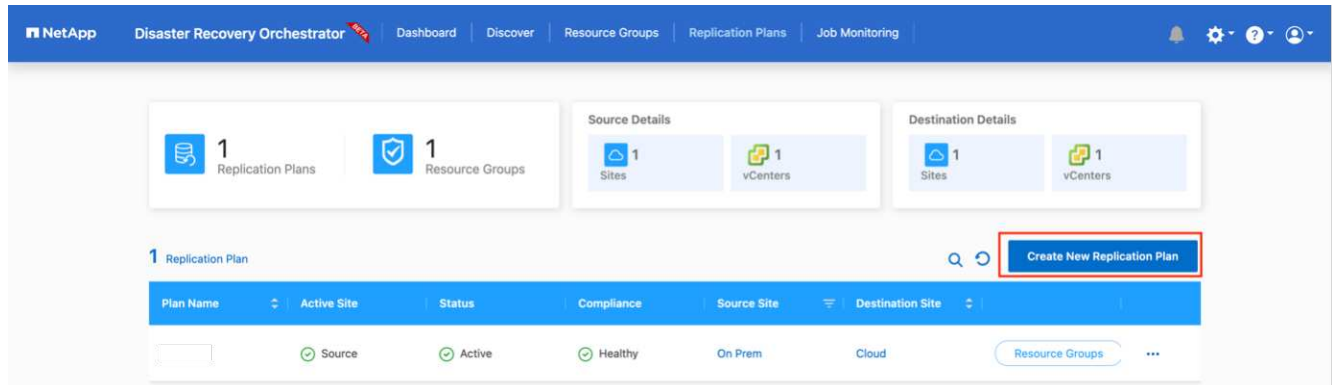


복제 계획

재해가 발생할 경우 애플리케이션을 복구할 계획이 필요합니다. 드롭다운에서 소스 및 대상 vCenter 플랫폼을 선택하고 이 계획에 포함할 리소스 그룹을 선택하고, 애플리케이션 복구 및 전원 켜기 방법(예: 도메인 컨트롤러, 계층 1, 계층 2 등)을 그룹화합니다. 이러한 계획을 청사진이라고도 합니다. 복구 계획을 정의하려면 * Replication Plan * 탭으로 이동하여 * New Replication Plan * 을 클릭합니다.

복제 계획 생성을 시작하려면 다음 단계를 수행하십시오.

1. Replication Plans * 에 액세스하여 * Create New Replication Plan * 을 클릭합니다.



2. 새 복제 계획 * 에서 소스 사이트, 연결된 vCenter, 대상 사이트 및 연결된 vCenter를 선택하여 계획 이름을 제공하고 복구 매핑을 추가합니다.

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: Select Source Site | Destination Site: Select Destination Site

Source vCenter: Select Source vCenter | Destination vCenter: Select Destination vCenter

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

Continue

3. 복구 매핑이 완료되면 클러스터 매핑을 선택합니다.

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: DemoRP

Recovery Mapping

Source Site: On Prem | Destination Site: Cloud

Source vCenter: 172.21.253.160 | Destination vCenter: 44.235.223.88

Cluster Mapping

Source Site Resource: TempCluster | Destination Site Resource: Cluster-1 | Add

Source Resource	Destination Resource
A300-Cluster01	Cluster-1 Delete

Continue

4. 리소스 그룹 세부 정보 * 를 선택하고 * 계속 * 을 클릭합니다.

5. 리소스 그룹의 실행 순서를 설정합니다. 이 옵션을 사용하면 여러 리소스 그룹이 있을 때 작업 순서를 선택할 수 있습니다.

6. 작업을 완료한 후 해당 세그먼트에 대한 네트워크 매핑을 선택합니다. 세그먼트는 VMC 내에서 이미 프로비저닝되어야 하므로 VM을 매핑할 적절한 세그먼트를 선택하십시오.

7. 선택한 VM에 따라 데이터 저장소 매핑이 자동으로 선택됩니다.



SnapMirror가 볼륨 레벨에 있습니다. 따라서 모든 VM이 복제 대상에 복제됩니다. 데이터 저장소에 속한 모든 VM을 선택해야 합니다. 이 옵션을 선택하지 않으면 복제 계획에 포함된 VM만 처리됩니다.

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 세부 정보 아래에서 VM의 CPU 및 RAM 매개 변수의 크기를 선택적으로 조정할 수 있습니다. 이는 대규모 환경을 소규모 타겟 클러스터로 복구하거나 일대일 물리적 VMware 인프라를 프로비저닝하지 않고도 DR 테스트를 수행할 때 매우 유용합니다. 또한 리소스 그룹에서 선택한 모든 VM에 대한 부팅 순서 및 부팅 지연(초)을 수정할 수 있습니다. 리소스 그룹 부팅 순서 선택 중에 선택한 변경 사항에서 필요한 변경 사항이 있는 경우 부팅 순서를 수정하는 추가 옵션이 있습니다. 기본적으로 리소스 그룹을 선택하는 동안 선택한 부팅 순서가 사용되지만 이 단계에서는 모든 수정 작업을 수행할 수 있습니다.

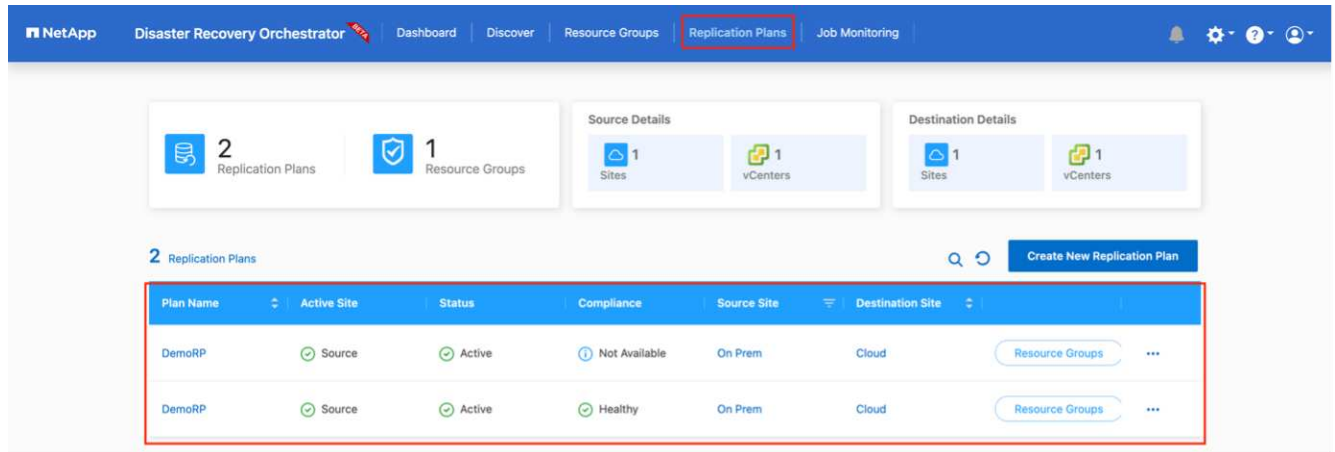
VM Details

3 VMs

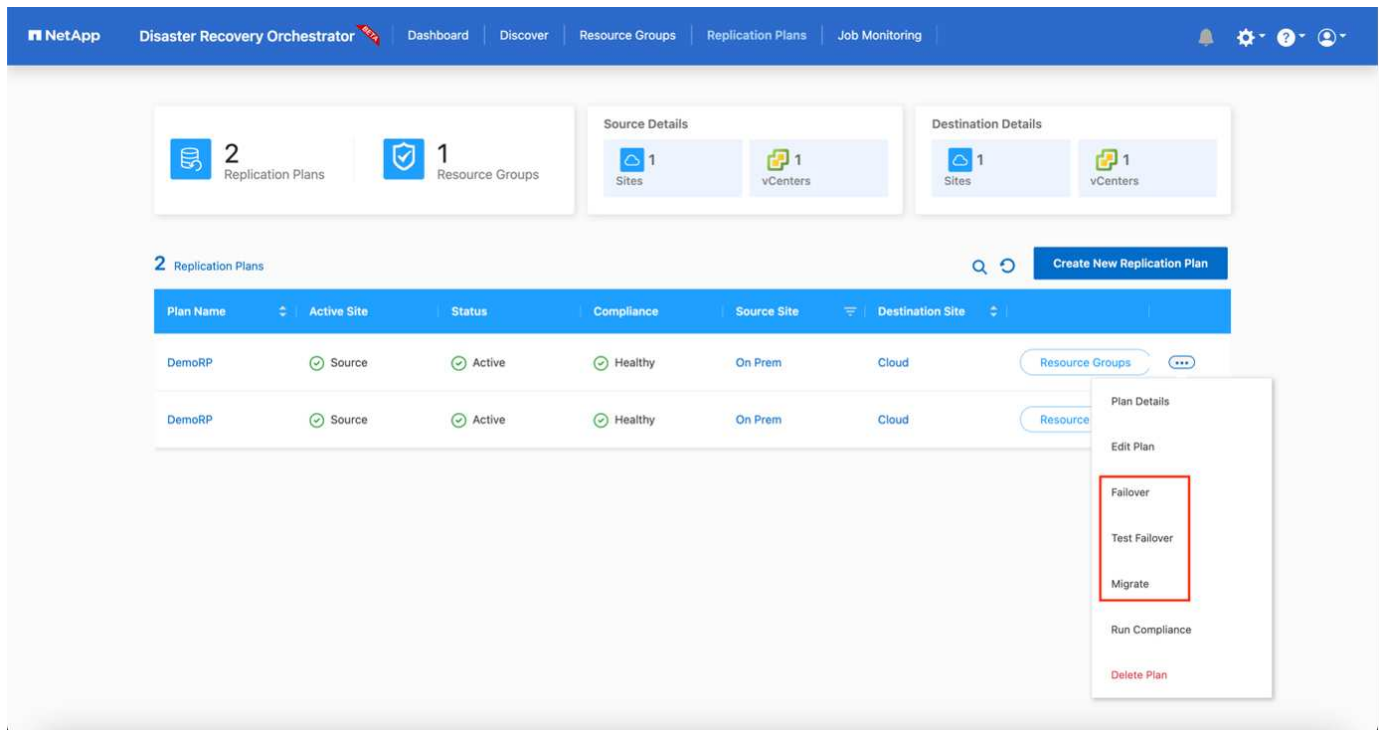
VM Name	No. of CPUs	Memory (MB)	NIC/IP	Boot Order	Override
Resource Group : DemoRG1					
Mini_Test01	1	2048	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic	3	
Mini_Test02	1	2048	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic	2	
Mini_Test03	1	2048	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic	1	

Previous Create Replication Plan

9. Create Replication Plan * 을 클릭합니다.



복제 계획이 생성되면 요구 사항에 따라 페일오버 옵션, 테스트 페일오버 옵션 또는 마이그레이션 옵션을 사용할 수 있습니다. 페일오버 및 테스트 페일오버 옵션 중에 최신 SnapMirror 스냅샷 복사본이 사용되거나, SnapMirror의 보존 정책에 따라 특정 시점의 Snapshot 복사본에서 특정 스냅샷 복사본을 선택할 수 있습니다. 가장 최근의 복제본이 이미 손상 또는 암호화된 상태에서 랜섬웨어와 같은 손상 이벤트가 발생할 경우 시점 옵션이 매우 유용할 수 있습니다. DRO는 사용 가능한 모든 시점을 표시합니다. 복제 계획에 지정된 구성으로 대체 작동을 트리거하거나 테스트 대체 작동을 트리거하려면 * 장애 조치 * 또는 * 테스트 대체 작동 * 을 클릭합니다.



Failover Details



Volume Snapshot Details

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

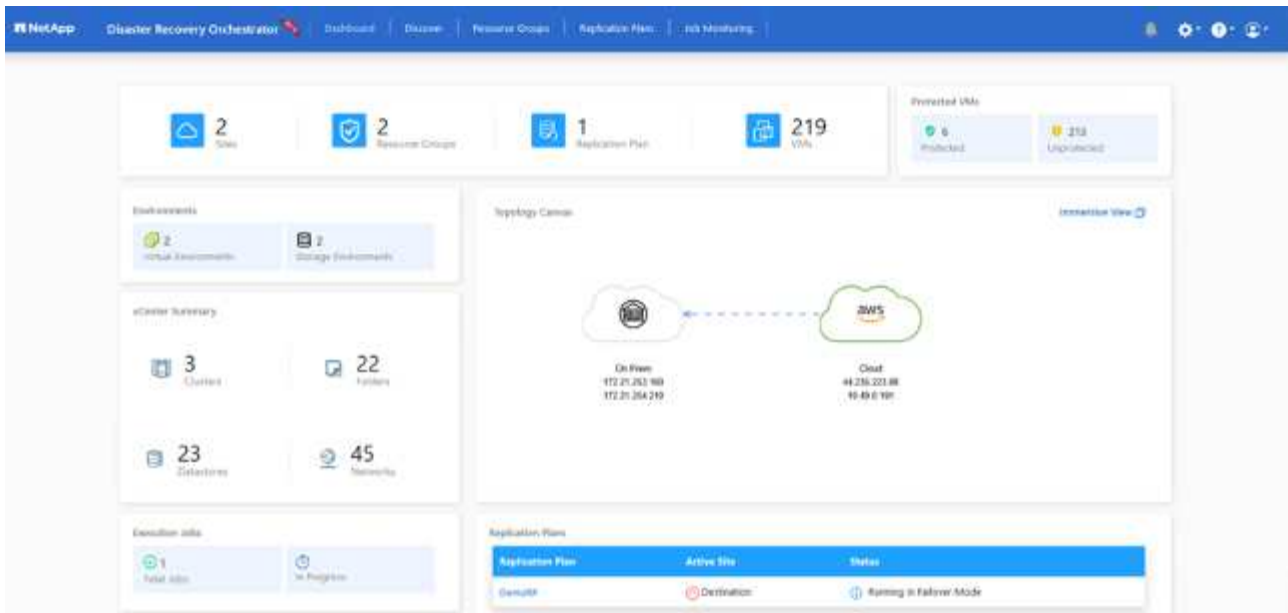
Start Failover

복제 계획은 작업 메뉴에서 모니터링할 수 있습니다.

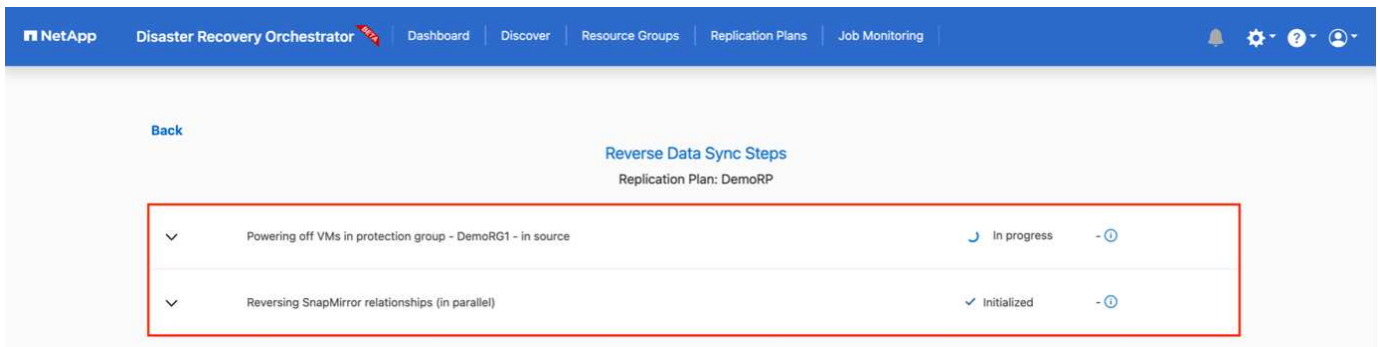
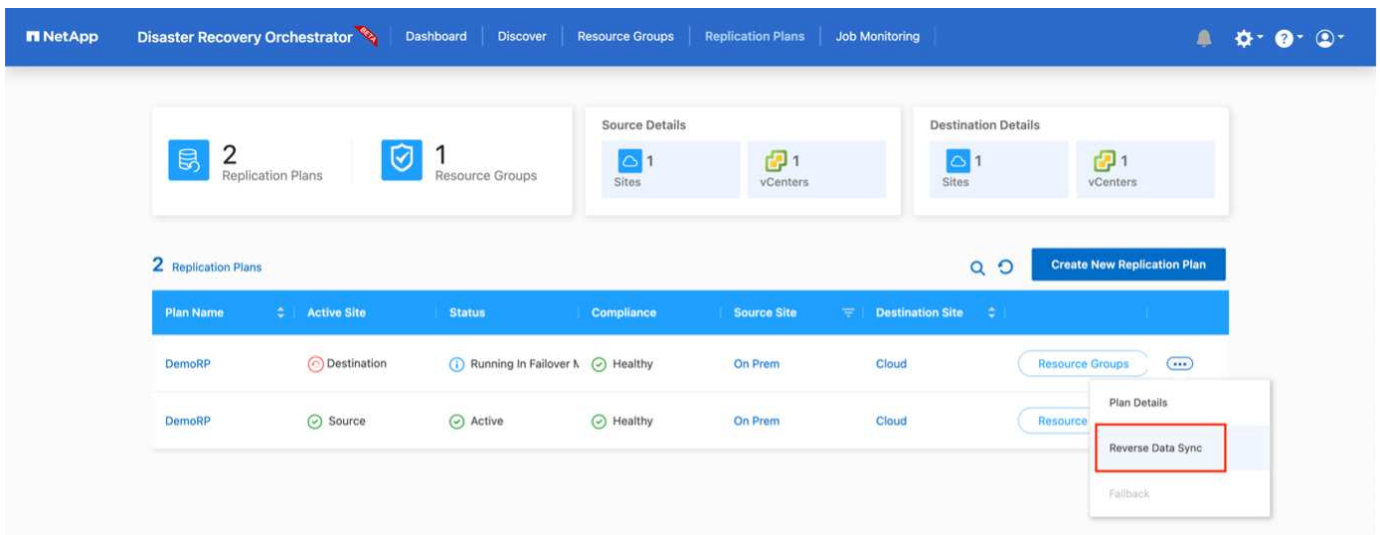
The screenshot shows the NetApp Disaster Recovery Orchestrator interface. The top navigation bar includes 'NetApp', 'Disaster Recovery Orchestrator', and several menu items: 'Dashboard', 'Discover', 'Resource Groups', 'Replication Plans', and 'Job Monitoring' (which is highlighted with a red box). On the right side of the navigation bar are icons for notifications, settings, help, and user profile. Below the navigation bar, the main content area has a 'Back' link on the left. In the center, there is a section titled 'Failover Steps' with a subtitle 'Replication Plan: DemoRP' (this section is also highlighted with a red box). Below this title is a table listing five steps of the failover process, each with a dropdown arrow, a description, a status, and a duration.

Step	Description	Status	Duration
1	Breaking SnapMirror relationships (in parallel)	Success	11.3 Seconds ⓘ
2	Mounting volumes and creating datastores (in parallel)	Success	34.7 Seconds ⓘ
3	Registering VMs (in parallel)	Success	13.2 Seconds ⓘ
4	Powering on VMs in protection group - DemoRG1 - in target	Success	95.8 Seconds ⓘ
5	Updating replication status	Success	0.5 Seconds ⓘ

페일오버가 트리거된 후 복구된 항목이 VMC vCenter(VM, 네트워크, 데이터 저장소)에서 표시될 수 있습니다. 기본적으로 VM은 Workload 폴더로 복구됩니다.



파일백은 복제 계획 레벨에서 트리거될 수 있습니다. 테스트 페일오버의 경우 최분해 옵션을 사용하여 변경 사항을 롤백하고 FlexClone 관계를 제거할 수 있습니다. 페일오버와 관련된 파일백은 2단계 프로세스입니다. 복제 계획을 선택하고 * Reverse data sync * 를 선택합니다.



완료되면 파일백을 트리거하여 원래 운영 사이트로 다시 이동할 수 있습니다.

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 [Create New Replication Plan](#)

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

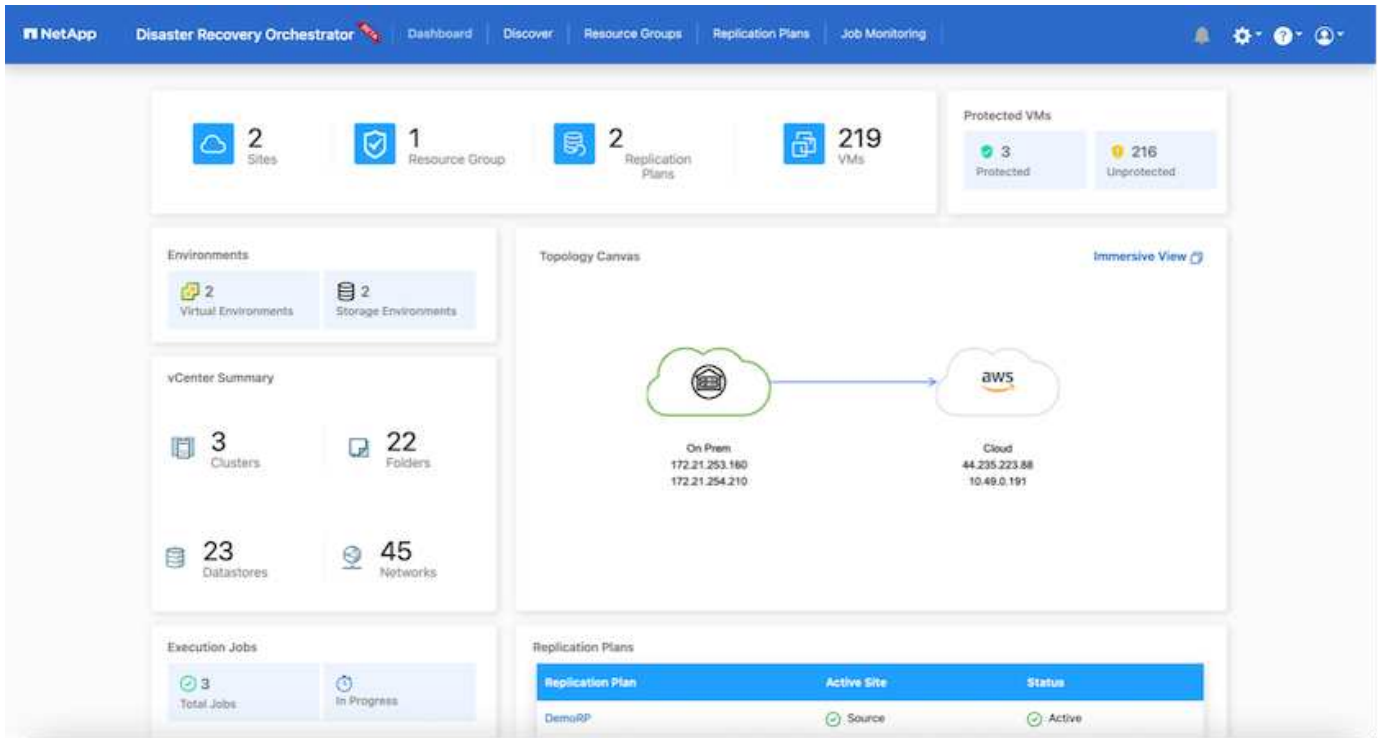
NetApp Disaster Recovery Orchestrator **NEW** Dashboard Discover Resource Groups Replication Plans Job Monitoring

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 BlueXP에서는 복제 상태가 적절한 볼륨(VMC에 읽기-쓰기 볼륨으로 매핑된 볼륨)에 대해 끊어지는 것을 볼 수 있습니다. 테스트 페일오버 중에 DRO는 대상 또는 복제본 볼륨을 매핑하지 않습니다. 대신 필요한 SnapMirror(또는 Snapshot) 인스턴스의 FlexClone 복사본을 만들고 FlexClone 인스턴스를 노출합니다. FlexClone 인스턴스는 ONTAP용 FSx의 추가 물리적 용량을 소비하지 않습니다. 이 프로세스를 통해 DR 테스트 또는 분류 워크플로우 중에도 볼륨을 수정하지 않고 복제 작업을 계속할 수 있습니다. 또한 이 프로세스를 통해 오류가 발생하거나 손상된 데이터가 복구되면 복제본을 제거할 위험 없이 복구를 정리할 수 있습니다.



랜섬웨어 복구

랜섬웨어에서 복구하는 것은 매우 힘든 작업이 될 수 있습니다. 특히, IT 조직은 안전한 반환 지점이 어디인지 정확히 파악하기가 어려우며, 일단 결정된 후에는 침낭성 맬웨어 또는 취약한 응용 프로그램 등의 재발생 공격으로부터 복구된 워크로드를 보호하기가 어려울 수 있습니다.

DRO는 사용 가능한 모든 시점에서 시스템을 복구할 수 있도록 함으로써 이러한 문제를 해결합니다. 또한 작업 부하를 기능적이면서도 격리된 네트워크로 복구할 수 있으므로 응용 프로그램이 남북 트래픽에 노출되지 않은 위치에서 상호 작동하고 통신할 수 있습니다. 이를 통해 보안 팀은 법의학 조사를 안전하게 수행할 수 있으며, 숨겨진 악성 코드나 잠자는 맬웨어가 없는지 확인할 수 있습니다.

이점

- 효율적이고 복원력이 뛰어난 SnapMirror 복제 사용:
- Snapshot 복사본 보존을 통해 사용 가능한 모든 시점으로 복구합니다.
- 스토리지, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계에서 수백 또는 수천 개의 VM을 복구하는 데 필요한 모든 단계를 완벽하게 자동화
- ONTAP FlexClone 기술을 사용하여 복제된 볼륨을 변경하지 않는 방법으로 워크로드 복구
 - 볼륨 또는 스냅샷 복사본에 대한 데이터 손상 위험을 방지합니다.
 - DR 테스트 워크플로우 중에 복제 중단 방지
 - DevTest, 보안 테스트, 패치 또는 업그레이드 테스트, 수정 테스트 등과 같은 DR 이외의 다른 워크플로우에 클라우드 컴퓨팅 리소스를 사용하여 DR 데이터를 사용할 수 있습니다.
- CPU 및 RAM 최적화를 통해 보다 작은 컴퓨팅 클러스터로 복구할 수 있으므로 클라우드 비용을 절감할 수 있습니다.

Veeam Replication 및 FSx for ONTAP를 사용하여 AWS 기반 VMware Cloud로 재해 복구

저자: Niyaz Mohamed-NetApp Solutions Engineering

개요

Amazon FSx for NetApp ONTAP와 AWS의 VMware Cloud의 통합은 SDDC의 클러스터에 연결할 수 있는 NetApp ONTAP 파일 시스템 기반의 AWS 관리형 외부 NFS 데이터 저장소입니다. 컴퓨팅 리소스와 독립적으로 확장이 가능한 유연한 고성능 가상화 스토리지 인프라를 고객에게 제공합니다.

AWS SDDC 기반 VMware Cloud를 재해 복구 타겟으로 사용하려는 고객은 VM 복제 기능을 제공하는 검증된 타사 솔루션을 사용하여 온프레미스에서 데이터를 복제하는 데 FSx for ONTAP 데이터 저장소를 사용할 수 있습니다. FSx for ONTAP 데이터 저장소를 추가하면 스토리지를 수용하기 위해 엄청난 양의 ESXi 호스트를 사용하여 AWS SDDC에 VMware 클라우드를 구축하는 것보다 비용 최적화된 배포를 실현할 수 있습니다.

또한 이 접근 방식은 고객이 VMC에서 FSx for ONTAP 데이터 저장소와 함께 파일럿 라이트 클러스터를 사용하여 VM 복제본을 호스팅할 수 있도록 지원합니다. 복제 계획을 정상적으로 페일오버하여 AWS 기반 VMware Cloud로의 마이그레이션 옵션으로 같은 프로세스를 확장할 수도 있습니다.

문제 설명

이 문서에서는 FSx for ONTAP 데이터 저장소와 Veeam 백업 및 복제를 사용하여 VM 복제 기능을 사용하여 온프레미스 VMware VM의 재해 복구를 AWS 기반의 VMware Cloud로 설정하는 방법을 설명합니다.

Veeam Backup & Replication을 사용하면 재해 복구(DR)를 위해 온사이트 및 원격 복제를 수행할 수 있습니다. 가상 머신을 복제할 때 Veeam Backup & Replication은 타겟 VMware Cloud on AWS SDDC 클러스터에 기본 VMware vSphere 형식으로 VM의 정확한 복제본을 생성하고 복제본을 원래 VM과 동기화된 상태로 유지합니다.

READY-TO-START 상태에 있는 VM의 복제본이 있기 때문에 복제는 최상의 RTO(Recovery Time Objective) 값을 제공합니다. 이 복제 메커니즘은 재해 발생 시 VMware Cloud on AWS SDDC에서 워크로드를 신속하게 시작할 수 있도록 보장합니다. Veeam Backup & Replication 소프트웨어는 또한 WAN을 통한 복제 및 느린 연결을 위해 트래픽 전송을 최적화합니다. 또한 중복 데이터 블록, 제로 데이터 블록, 스왑 파일 및 제외된 VM 게스트 OS 파일을 필터링하고 복제 트래픽을 압축합니다.

복제 작업이 전체 네트워크 대역폭을 소비하는 것을 방지하기 위해 WAN 가속기 및 네트워크 조절 규칙을 적용할 수 있습니다. Veeam Backup & Replication의 복제 프로세스는 작업 중심으로 수행되므로 복제 작업을 구성하여 복제가 수행됩니다. 재해가 발생할 경우 해당 복제본 복제본으로 장애 조치를 수행하여 VM을 복구하기 위해 장애 조치를 트리거할 수 있습니다.

페일오버가 수행되면 복제된 VM이 원래 VM의 역할을 대신합니다. 페일오버는 복제본의 최신 상태 또는 알려진 정상 복구 지점으로 수행할 수 있습니다. 따라서 필요에 따라 랜섬웨어 복구 또는 격리된 테스트가 가능합니다. Veeam Backup & Replication에서 페일오버와 페일백은 임시 중간 단계로, 이 단계는 추가로 완료해야 합니다. Veeam Backup & Replication은 다양한 재해 복구 시나리오를 처리할 수 있는 다양한 옵션을 제공합니다.

[Veeam Replication 및 FSx ONTAP for VMC를 사용하는 DR 시나리오의 다이어그램]

솔루션 구축

고급 단계

1. Veeam Backup and Replication 소프트웨어는 적절한 네트워크 연결을 통해 사내 환경에서 실행됩니다.
2. VMware Cloud on AWS 구성 에 대한 자세한 내용은 VMware Cloud Tech Zone 문서를 참조하십시오 "[AWS 기반 VMware Cloud와 Amazon FSx for NetApp ONTAP 구축 가이드 의 통합](#)" 구축하려면 AWS SDDC에 VMware Cloud를, FSx for ONTAP를 NFS 데이터 저장소로 구성합니다. (최소 구성으로 설정된 파일럿 라이트 환경을 DR 목적으로 사용할 수 있습니다. 장애 발생 시 VM이 이 클러스터로 페일오버되고 추가 노드를 추가할 수 있습니다.)
3. Veeam Backup and Replication을 사용하여 VM 복제본을 생성하도록 복제 작업을 설정합니다.
4. 페일오버 계획을 만들고 페일오버를 수행합니다.
5. 재해 이벤트가 완료되고 운영 사이트가 가동되면 운영 VM으로 다시 전환합니다.

Veeam VM을 VMC 및 FSx for ONTAP 데이터 저장소로 복제하기 위한 사전 요구 사항

1. Veeam Backup & Replication 백업 VM이 소스 vCenter와 AWS SDDC 클러스터의 타겟 VMware 클라우드에 연결되어 있는지 확인합니다.
2. 백업 서버는 짧은 이름을 확인하고 소스 및 타겟 vCenter에 연결할 수 있어야 합니다.
3. 대상 FSx for ONTAP 데이터 저장소에는 복제된 VM의 VMDK를 저장할 수 있는 충분한 여유 공간이 있어야 합니다

자세한 내용은 "고려 사항 및 제한 사항"을 참조하십시오 "[여기](#)".

배포 세부 정보

1단계: VM 복제

Veeam Backup & Replication은 VMware vSphere 스냅샷 기능을 활용하며, 복제하는 동안 Veeam Backup & Replication은 VMware vSphere에 VM 스냅샷을 생성하도록 요청합니다. VM 스냅샷은 가상 디스크, 시스템 상태, 구성 등을 포함하는 VM의 시점 복제본입니다. Veeam Backup & Replication은 이 스냅샷을 복제용 데이터 소스로 사용합니다.

VM을 복제하려면 다음 단계를 수행하십시오.

1. Veeam Backup & Replication Console을 엽니다.
2. 홈 보기에서 복제 작업 > 가상 머신 > VMware vSphere 를 선택합니다.
3. 작업 이름을 지정하고 해당 고급 제어 확인란을 선택합니다. 다음 을 클릭합니다.
 - 온-프레미스와 AWS 간의 접속 대역폭이 제한된 경우 복제 시드 확인란을 선택합니다.
 - VMware Cloud on AWS SDDC의 세그먼트가 사내 사이트 네트워크의 세그먼트와 일치하지 않으면 Network remapping (다른 네트워크를 가진 AWS VMC 사이트의 경우) 확인란을 선택합니다.
 - 온프레미스 운영 사이트의 IP 주소 지정 체계가 AWS VMC 사이트의 체계와 다른 경우 복제 Re-IP(IP 주소 지정 체계가 다른 DR 사이트의 경우) 확인란을 선택합니다.

[DR Veeam FSx 이미지 2] | *dr-veeam-fsx-image2.png*

4. AWS SDDC 기반 VMware Cloud에 연결된 FSx for ONTAP 데이터 저장소에 복제해야 하는 VM을 * 가상 머신 * 단계에서 선택합니다. vSAN에 가상 머신을 배치하여 사용 가능한 vSAN 데이터스토어 용량을 채울 수 있습니다. 파일럿 라이트 클러스터에서는 3노드 클러스터의 가용 용량이 제한됩니다. 나머지 데이터를 FSx for ONTAP 데이터 저장소에 복제할 수 있습니다. Add * 를 클릭한 다음 * Add Object * 창에서 필요한 VM 또는 VM 컨테이너를 선택하고 * Add * 를 클릭합니다. 다음 * 을 클릭합니다.

[DR Veeam FSx 이미지 3] | *dr-veeam-fsx-image3.png*

5. 그런 다음 대상을 AWS SDDC 클러스터/호스트의 VMware Cloud 및 VM 복제본용 적절한 리소스 풀, VM 폴더 및 FSx for ONTAP 데이터 저장소로 선택합니다. 그런 다음 * 다음 * 을 클릭합니다.

[DR Veeam FSx 이미지 4] | *dr-veeam-fsx-image4.png*

6. 다음 단계에서는 필요에 따라 소스 및 대상 가상 네트워크 간의 매핑을 생성합니다.

[DR Veeam FSx 이미지5] | *dr-veeam-fsx-image5.png*

7. 작업 설정 * 단계에서 VM 복제본, 보존 정책 등에 대한 메타데이터를 저장할 백업 리포지토리를 지정합니다.
8. 데이터 전송 * 단계에서 * 원본 * 및 * 대상 * 프록시 서버를 업데이트하고 * 자동 * 선택(기본값)을 그대로 두고 * 직접 * 옵션을 선택한 후 * 다음 * 을 클릭합니다.
9. Guest Processing * 단계에서 필요에 따라 * Enable application-aware processing * 옵션을 선택합니다. 다음 * 을 클릭합니다.

[DR Veeam FSx 이미지6] | *dr-veeam-fsx-image6.png*

10. 정기적으로 실행할 복제 작업을 실행할 복제 스케줄을 선택합니다.
11. 마법사의 * Summary * 단계에서 복제 작업의 세부 정보를 검토합니다. 마법사를 닫은 후 바로 작업을 시작하려면 * 마침을 클릭하면 작업 실행 * 확인란을 선택하고, 그렇지 않으면 확인란을 선택하지 않은 상태로 둡니다. 그런 다음 * 마침 * 을 클릭하여 마법사를 닫습니다.

[DR Veeam FSx 이미지7] | *dr-veeam-fsx-image7.png*

복제 작업이 시작되면 접미사가 지정된 VM이 대상 VMC SDDC 클러스터/호스트에 채워집니다.




[DR Veeam FSx 이미지8] | *dr-veeam-fsx-image8.png*

Veeam 복제에 대한 자세한 내용은 을 참조하십시오 ["복제 작동 방법"](#).

2단계: 장애 조치 계획을 만듭니다

초기 복제 또는 시드가 완료되면 페일오버 계획을 생성합니다. 페일오버 계획은 종속 VM에 대해 하나씩 또는 그룹으로 자동 페일오버를 수행하는 데 도움이 됩니다. 페일오버 계획은 부팅 지연을 포함하여 VM이 처리되는 순서에 대한 청사진입니다. 또한 페일오버 계획은 중요한 종속 VM이 이미 실행 중인지 확인하는 데 도움이 됩니다.

계획을 생성하려면 Replicas라는 새 하위 섹션으로 이동하고 Failover Plan을 선택합니다. 적절한 VM을 선택합니다. Veeam Backup & Replication은 이 시점에 가장 가까운 복원 지점을 찾아 VM 복제를 시작하는 데 사용합니다.

-  초기 복제가 완료되고 VM 복제본이 준비 상태가 된 후에만 페일오버 계획을 추가할 수 있습니다.
-  페일오버 계획을 실행할 때 동시에 시작할 수 있는 최대 VM 수는 10개입니다.
-  페일오버 프로세스 중에는 소스 VM의 전원이 꺼지지 않습니다.

장애 조치 계획 * 을 만들려면 다음을 수행합니다.

1. 홈 보기에서 * 페일오버 계획 > VMware vSphere * 를 선택합니다.
2. 그런 다음 계획에 이름과 설명을 입력합니다. 필요에 따라 사전 및 사후 페일오버 스크립트를 추가할 수 있습니다. 예를 들어 복제된 VM을 시작하기 전에 VM을 종료하는 스크립트를 실행합니다.

[DR Veeam FSx 이미지9] | *dr-veeam-fsx-image9.png*

3. VM을 계획에 추가하고 애플리케이션 종속성을 충족하도록 VM 부팅 순서 및 부팅 지연을 수정합니다.

[DR Veeam FSx 이미지 10] | *dr-veeam-fsx-image10.png*

복제 작업 생성에 대한 자세한 내용은 을 참조하십시오 ["복제 작업을 생성하는 중입니다"](#).

3단계: 페일오버 계획을 실행합니다

페일오버 중에 프로덕션 사이트의 소스 VM이 재해 복구 사이트의 해당 복제본으로 전환됩니다. 페일오버 프로세스의 일부로 Veeam Backup & Replication은 VM 복제본을 필요한 복구 지점으로 복구하고 소스 VM의 모든 입출력 작업을 해당 복제본으로 이동합니다. 복제본은 재해 발생 시에만 사용할 수 있으며 DR 드릴을 시뮬레이션하는 데도 사용할 수 있습니다. 페일오버 시뮬레이션 중에는 소스 VM이 계속 실행 중입니다. 필요한 모든 테스트가 수행되면 페일오버를 취소하고 정상 작업으로 돌아갈 수 있습니다.



DR 훈련 중에 IP 충돌을 피하기 위해 네트워크 분할이 제대로 수행되었는지 확인하십시오.

장애 조치 계획을 시작하려면 * 장애 조치 계획 * 탭을 클릭하고 장애 조치 계획을 마우스 오른쪽 버튼으로 클릭합니다. 시작 * 을 선택합니다. 이렇게 하면 VM 복제본의 최신 복구 지점을 사용하여 장애 조치가 수행됩니다. VM 복제본의 특정 복원 지점으로 페일오버하려면 * 시작 * 을 선택합니다.

[DR Veeam FSx 이미지 11] | *dr-veeam-fsx-image11.png*

[DR Veeam FSx 이미지12] | *dr-veeam-fsx-image12.png*

VM 복제본의 상태가 Ready에서 Failover로 변경되고 VM은 대상 VMware Cloud on AWS SDDC 클러스터 /호스트에서 시작됩니다.

[DR Veeam FSx 이미지 13] | *dr-veeam-fsx-image13.png*

페일오버가 완료되면 VM의 상태가 "페일오버"로 변경됩니다.

[DR Veeam FSx 이미지14] | *dr-veeam-fsx-image14.png*



Veeam Backup & Replication은 소스 VM의 복제본이 준비 상태로 돌아갈 때까지 소스 VM에 대한 모든 복제 작업을 중지합니다.

페일오버 계획에 대한 자세한 내용은 을 참조하십시오 ["페일오버 계획"](#).

4단계: 프로덕션 사이트로 페일백합니다

장애 조치 계획이 실행 중인 경우 중간 단계로 간주되며 요구 사항에 따라 확정되어야 합니다. 다음과 같은 옵션이 있습니다.

- * Failback to Production * - 원래 VM으로 다시 전환하고 VM 복제본이 실행되는 동안 발생한 모든 변경 사항을 원래 VM으로 전송합니다.



페일백을 수행하면 변경 내용이 전송되지만 게시되지는 않습니다. 원래 VM이 예상대로 작동하지 않는 경우 * 페일백 커밋 * (원래 VM이 예상대로 작동하는 것으로 확인된 경우) 또는 * 페일백 실행 취소 * 를 선택하여 VM 복제본으로 돌아갑니다.

- * 장애 조치 실행 취소 * - 원래 VM으로 다시 전환하고 실행 중에 VM 복제본의 모든 변경 사항을 취소합니다.
- * 영구 장애 조치 * - 원래 VM에서 VM 복제본으로 영구적으로 전환하고 이 복제본을 원래 VM으로 사용합니다.

이 데모에서는 Failback to Production을 선택했습니다. 마법사의 대상 단계에서 원래 VM으로 페일백이 선택되었고 "복원 후 VM 전원 켜기" 확인란이 활성화되었습니다.

[DR Veeam FSx 이미지 15] | *dr-veeam-fsx-image15.png*

[DR Veeam FSx 이미지 16] | *dr-veeam-fsx-image16.png*

페일백 커밋은 페일백 작업을 완료하는 방법 중 하나입니다. 페일백이 커밋되면 장애가 발생한 VM(운영 VM)에 전송된 변경 사항이 예상대로 작동하는지 확인합니다. 커밋 작업 후에 Veeam Backup & Replication은 운영 VM에 대한 복제 작업을 재개합니다.

페일백 프로세스에 대한 자세한 내용은 의 Veeam 문서를 참조하십시오 ["복제를 위한 페일오버 및 페일백"](#).

[DR Veeam FSx 이미지 17] | *dr-veeam-fsx-image17.png*

[DR Veeam FSx 이미지 18] | *dr-veeam-fsx-image18.png*

운영 환경으로 페일백이 성공한 후 VM이 모두 원래 운영 사이트로 복구됩니다.

[DR Veeam FSx 이미지 19] | *dr-veeam-fsx-image19.png*

결론

FSx for ONTAP 데이터 저장소 기능을 통해 Veeam 또는 검증된 타사 툴이 파일럿 라이트 클러스터를 사용하고, 클러스터에 VM 복제 복사본을 수용하기 위해 다수의 호스트를 보유하지 않고 경제적인 DR 솔루션을 제공할 수 있습니다. 이 제품은 맞춤형 재해 복구 계획을 처리할 수 있는 강력한 솔루션을 제공합니다. 또한 기존 백업 제품을 사내에서 재사용하여 DR 요구사항을 충족할 수 있으므로, 사내에서 DR 데이터 센터를 종료하여 클라우드 기반 재해 복구가 가능합니다. 재해가 발생한 경우 버튼 클릭 한 번으로 계획된 페일오버 또는 페일오버로 페일오버를 수행할 수 있으며 DR 사이트를 활성화하기로 결정합니다.

이 프로세스에 대해 자세히 알아보려면 자세한 단계별 안내 비디오를 참조하십시오.

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

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.