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

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

목차

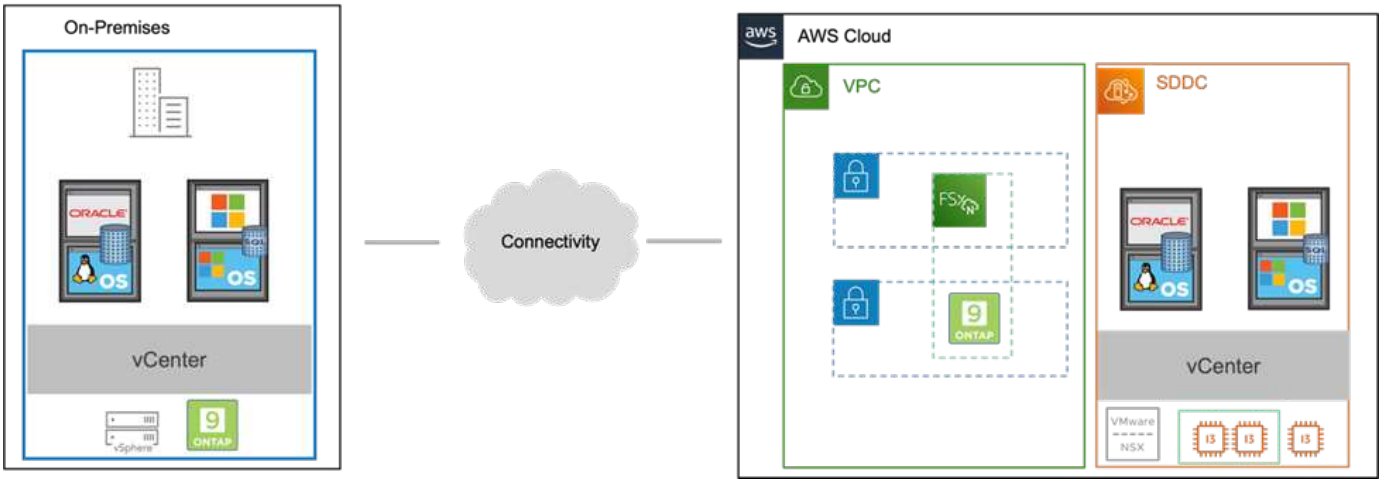
TR-4931: Amazon Web Services 및 Guest Connect에서 VMware Cloud를 사용한 재해 복구

검증된 재해 복구(DR) 환경과 계획은 조직이 주요 비즈니스 중단 발생 시에도 비즈니스에 중요한 애플리케이션을 신속하게 복구할 수 있도록 하는 데 필수적입니다. 이 솔루션은 온프레미스와 AWS의 VMware Cloud를 모두 활용한 VMware 및 NetApp 기술에 초점을 맞춰 DR 사용 사례를 보여주는 데 중점을 둡니다.

개요

NetApp VMware와 오랫동안 통합을 이루어 왔으며, 이는 수만 명의 고객이 가상화 환경을 위한 스토리지 파트너로 NetApp 선택한 것에서 입증됩니다. 이러한 통합은 클라우드의 게스트 연결 옵션과 최근 NFS 데이터 저장소와의 통합에서도 계속됩니다. 이 솔루션은 일반적으로 게스트 연결 스토리지라고 하는 사용 사례에 초점을 맞춥니다.

게스트 연결 스토리지에서는 게스트 VMDK가 VMware에서 제공하는 데이터 저장소에 배포되고, 애플리케이션 데이터는 iSCSI 또는 NFS에 저장되어 VM에 직접 매핑됩니다. 다음 그림에서 볼 수 있듯이 Oracle 및 MS SQL 애플리케이션은 DR 시나리오를 설명하는 데 사용됩니다.



가정, 전제 조건 및 구성 요소 개요

이 솔루션을 배포하기 전에 구성 요소 개요, 솔루션을 배포하는 데 필요한 사전 요구 사항, 이 솔루션을 문서화하는 데 필요한 가정 사항을 검토하세요.

"DR 솔루션 요구 사항, 사전 요구 사항 및 계획"

SnapCenter 사용하여 DR 수행

이 솔루션에서 SnapCenter SQL Server 및 Oracle 애플리케이션 데이터에 대한 애플리케이션 일관성 스냅샷을 제공합니다. 이 구성은 SnapMirror 기술과 함께 온프레미스 AFF 와 FSx ONTAP 클러스터 간에 고속 데이터 복제를 제공합니다. 또한, Veeam Backup & Replication은 가상 머신에 대한 백업 및 복원 기능을 제공합니다.

이 섹션에서는 백업과 복원을 위한 SnapCenter, SnapMirror 및 Veeam의 구성에 대해 다룹니다.

다음 섹션에서는 보조 사이트에서 장애 조치를 완료하는 데 필요한 구성과 단계를 다룹니다.

SnapMirror 관계 및 보존 일정 구성

SnapCenter 장기 보관 및 보존 목적으로 기본 스토리지 시스템(기본 > 미러) 및 보조 스토리지 시스템(기본 > 볼트) 내의 SnapMirror 관계를 업데이트할 수 있습니다. 이를 위해 SnapMirror 사용하여 대상 볼륨과 소스 볼륨 간의 데이터 복제 관계를 설정하고 초기화해야 합니다.

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

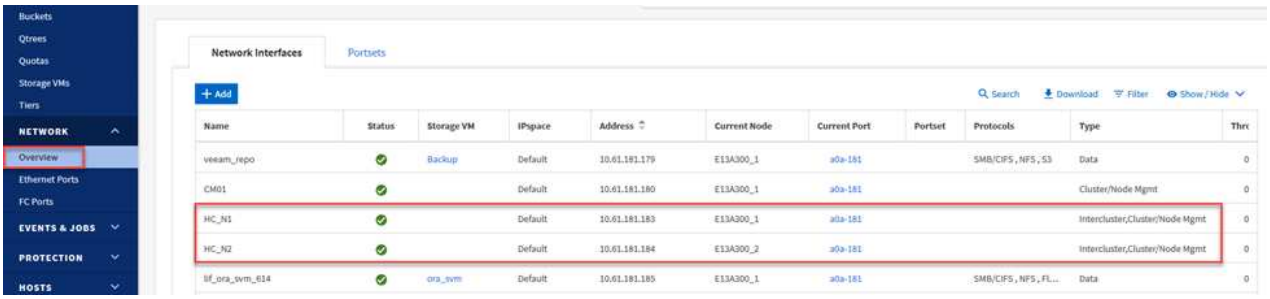
온프레미스 ONTAP 시스템과 FSx ONTAP 간의 SnapMirror 관계를 설정하려면 다음 단계가 필요합니다.

를 참조하세요 "FSx ONTAP – ONTAP 사용자 가이드" FSx를 사용하여 SnapMirror 관계를 만드는 방법에 대한 자세한 내용은 다음을 참조하세요.

소스 및 대상 **Intercluster** 논리 인터페이스를 기록합니다**.**

온프레미스에 있는 소스 ONTAP 시스템의 경우 시스템 관리자나 CLI에서 클러스터 간 LIF 정보를 검색할 수 있습니다.

1. ONTAP System Manager에서 네트워크 개요 페이지로 이동하여 FSx가 설치된 AWS VPC와 통신하도록 구성된 유형: 클러스터 간 IP 주소를 검색합니다.



2. FSx의 Intercluster IP 주소를 검색하려면 CLI에 로그인하고 다음 명령을 실행하세요.

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

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

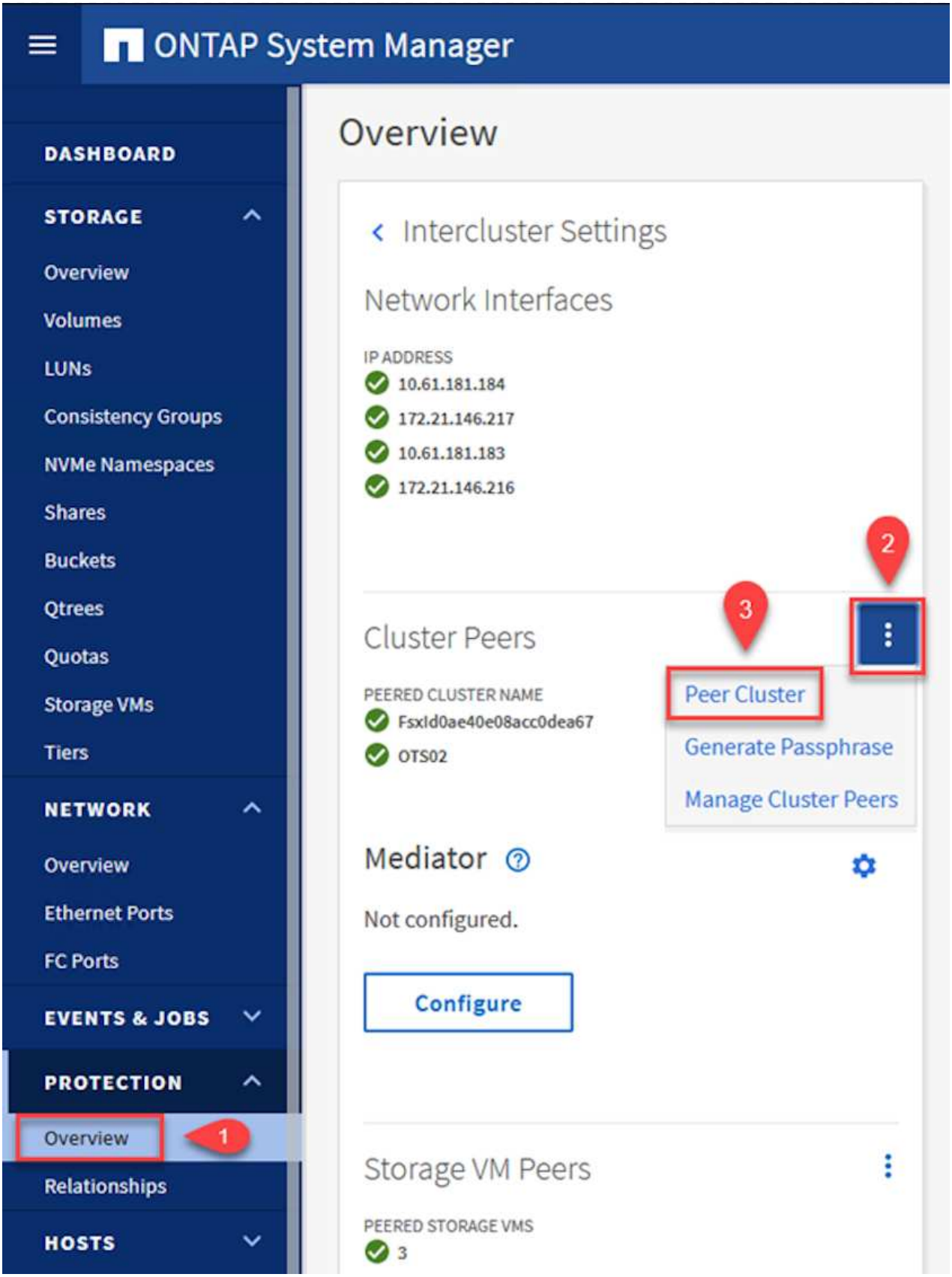
ONTAP 과 **FSx** 간 클러스터 피어링 설정

ONTAP 클러스터 간에 클러스터 피어링을 설정하려면 시작 ONTAP 클러스터에서 입력한 고유한 암호문구를 다른 피어 클러스터에서 확인해야 합니다.

1. 다음을 사용하여 대상 FSx 클러스터에서 피어링을 설정합니다. `cluster peer create` 명령. 메시지가 표시되면 나중에 소스 클러스터에서 생성 프로세스를 마무리하는 데 사용되는 고유한 암호구를 입력합니다.

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

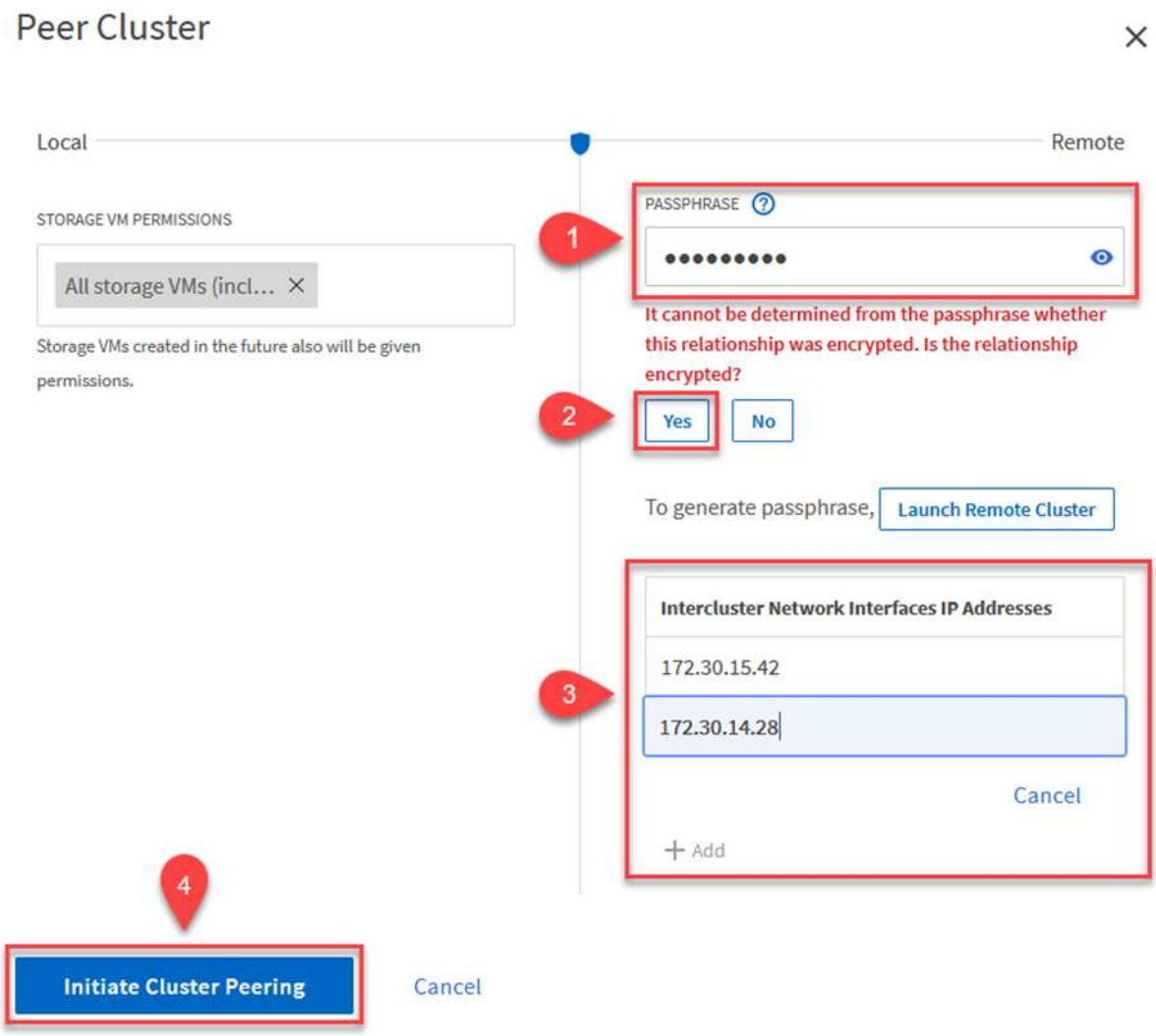
2. 소스 클러스터에서 ONTAP 시스템 관리자나 CLI를 사용하여 클러스터 피어 관계를 설정할 수 있습니다. ONTAP 시스템 관리자에서 보호 > 개요로 이동하여 피어 클러스터를 선택합니다.



3. 피어 클러스터 대화 상자에서 필요한 정보를 입력합니다.
   a. 대상 FSx 클러스터에서 피어 클러스터 관계를 설정하는 데 사용된 암호를 입력하세요.
   b. 선택하다 `Yes` 암호화된 관계를 구축합니다.

c. 대상 FSx 클러스터의 클러스터 간 LIF IP 주소를 입력하세요.

d. 클러스터 피어링 시작을 클릭하여 프로세스를 마무리합니다.



4. 다음 명령을 사용하여 FSx 클러스터에서 클러스터 피어 관계 상태를 확인하세요.

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

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

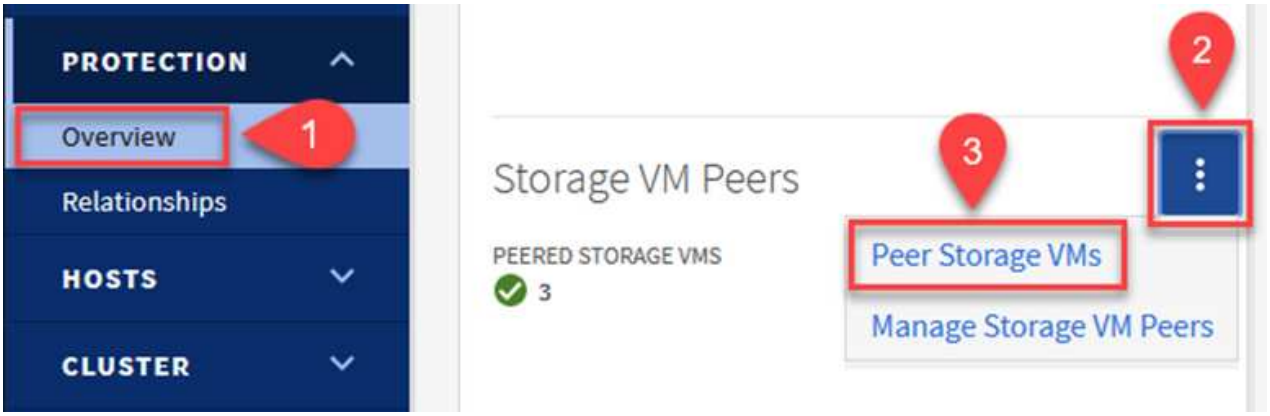
SVM 피어링 관계 설정

다음 단계는 SnapMirror 관계에 포함될 볼륨을 포함하는 대상 및 소스 스토리지 가상 머신 간에 SVM 관계를 설정하는 것입니다.

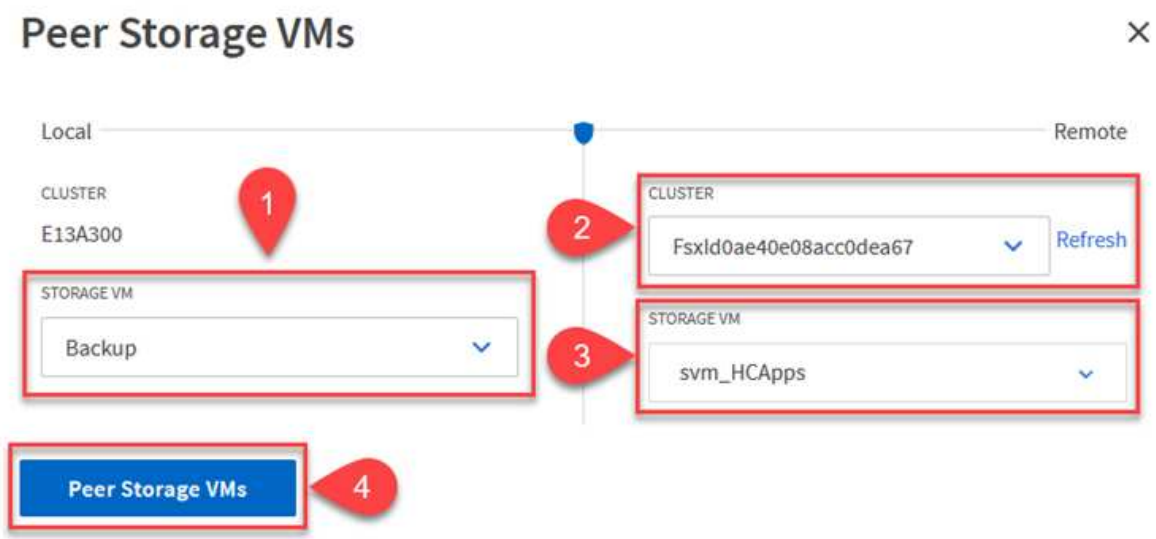
1. 소스 FSx 클러스터에서 CLI에서 다음 명령을 사용하여 SVM 피어 관계를 만듭니다.

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

2. 소스 ONTAP 클러스터에서 ONTAP 시스템 관리자나 CLI를 사용하여 피어링 관계를 수락합니다.
3. ONTAP 시스템 관리자에서 보호 > 개요로 이동하여 스토리지 VM 피어 아래에서 피어 스토리지 VM을 선택합니다.



4. Peer Storage VM 대화 상자에서 필수 필드를 작성합니다.
   - 소스 스토리지 VM
   - 대상 클러스터
   - 대상 저장소 VM



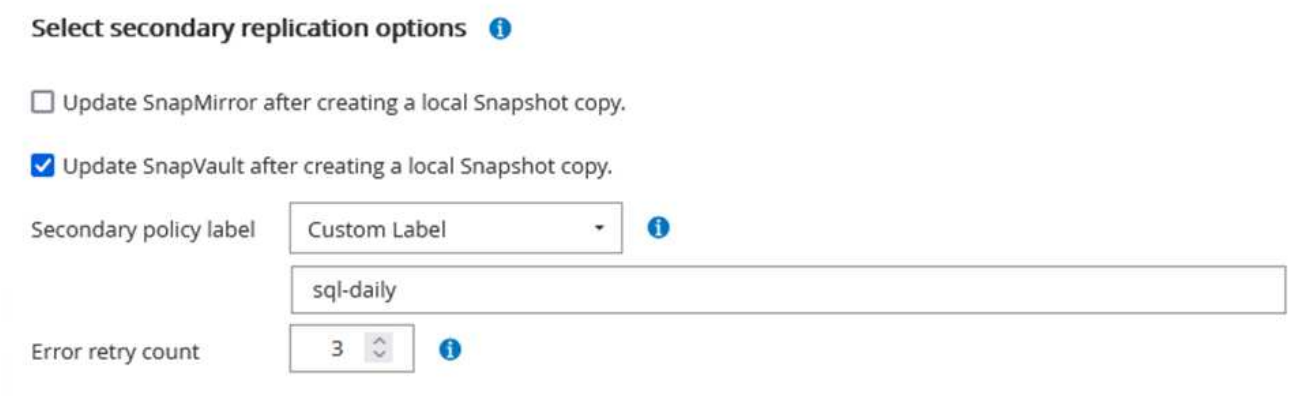
5. SVM 피어링 프로세스를 완료하려면 Peer Storage VMs를 클릭하세요.

SnapCenter 기본 스토리지 시스템에 스냅샷 복사본으로 존재하는 백업의 보존 일정을 관리합니다. 이는 SnapCenter 에서 정책을 생성할 때 설정됩니다. SnapCenter 보조 스토리지 시스템에 보관된 백업에 대한 보존 정책을 관리하지 않습니다. 이러한 정책은 보조 FSx 클러스터에서 생성되고 소스 볼륨과 SnapMirror 관계에 있는 대상 볼륨과 연관된 SnapMirror 정책을 통해 별도로 관리됩니다.

SnapCenter 정책을 생성할 때 SnapCenter 백업이 수행될 때 생성되는 각 스냅샷의 SnapMirror 레이블에 추가되는 보조 정책 레이블을 지정하는 옵션이 있습니다.

ⓘ 보조 저장소에서 이러한 레이블은 스냅샷 보존을 강제하기 위해 대상 볼륨과 연관된 정책 규칙과 일치합니다.

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



SQL Server 데이터베이스에 대한 SnapCenter 정책을 만드는 방법에 대한 자세한 내용은 다음을 참조하세요. "SnapCenter 문서" .

먼저 보존할 스냅샷 복사본의 수를 결정하는 규칙이 포함된 SnapMirror 정책을 만들어야 합니다.

1. FSx 클러스터에서 SnapMirror 정책을 만듭니다.

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

2. SnapCenter 정책에 지정된 보조 정책 레이블과 일치하는 SnapMirror 레이블이 있는 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 보관할 스냅샷 수(보관 기간)에 대한 추가 규칙을 만듭니다.

대상 볼륨 생성

소스 볼륨의 스냅샷 복사본을 수신할 FSx에 대상 볼륨을 생성하려면 FSx ONTAP 에서 다음 명령을 실행합니다.

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

소스 볼륨과 대상 볼륨 간의 **SnapMirror** 관계 생성

소스 볼륨과 대상 볼륨 사이에 SnapMirror 관계를 생성하려면 FSx ONTAP 에서 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 프로세스는 소스 볼륨에서 생성된 새로운 스냅샷을 시작하고 대상 볼륨에 복사합니다.

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

온프레미스에 **Windows SnapCenter** 서버를 배포하고 구성합니다.

온프레미스에 **Windows SnapCenter** 서버 배포

이 솔루션은 NetApp SnapCenter 사용하여 SQL Server 및 Oracle 데이터베이스의 애플리케이션 일관성 백업을 수행합니다. 가상 머신 VMDK를 백업하기 위한 Veeam Backup & Replication과 함께 사용하면 온프레미스 및 클라우드 기반 데이터 센터를 위한 포괄적인 재해 복구 솔루션을 제공합니다.

SnapCenter software NetApp 지원 사이트에서 구할 수 있으며 도메인이나 작업 그룹에 있는 Microsoft Windows 시스템에 설치할 수 있습니다. 자세한 계획 가이드와 설치 지침은 다음에서 확인할 수 있습니다. "NetApp 문서 센터" .

SnapCenter software 다음에서 구할 수 있습니다. "이 링크" .

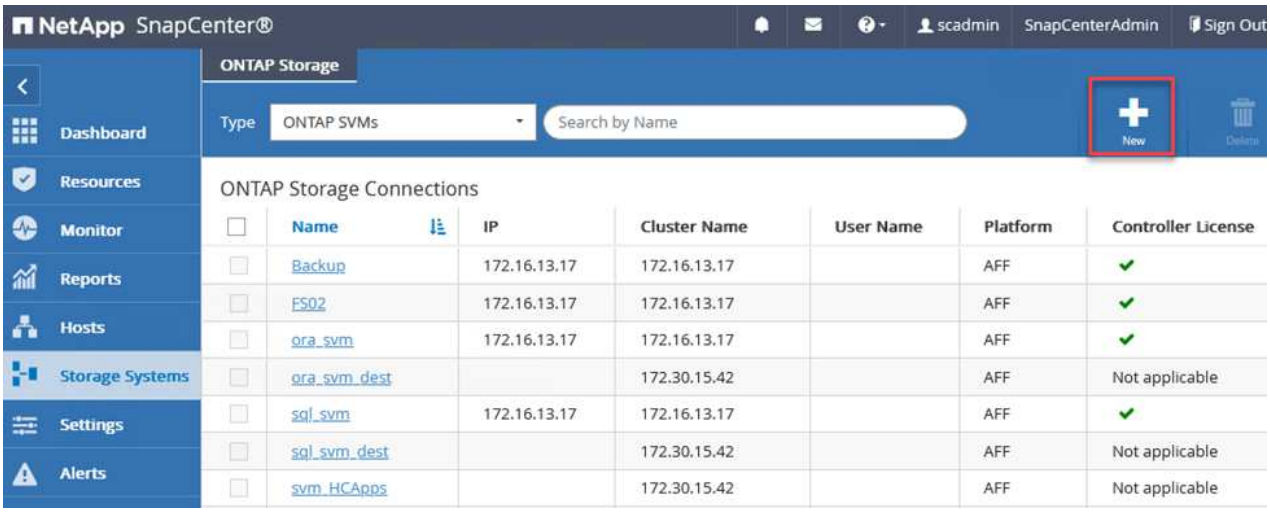
설치가 완료되면 웹 브라우저에서 _\https://Virtual_Cluster_IP_or_FQDN:8146_을 사용하여 SnapCenter 콘솔에 액세스할 수 있습니다.

콘솔에 로그인한 후 SQL Server 및 Oracle 데이터베이스를 백업하기 위해 SnapCenter 구성해야 합니다.

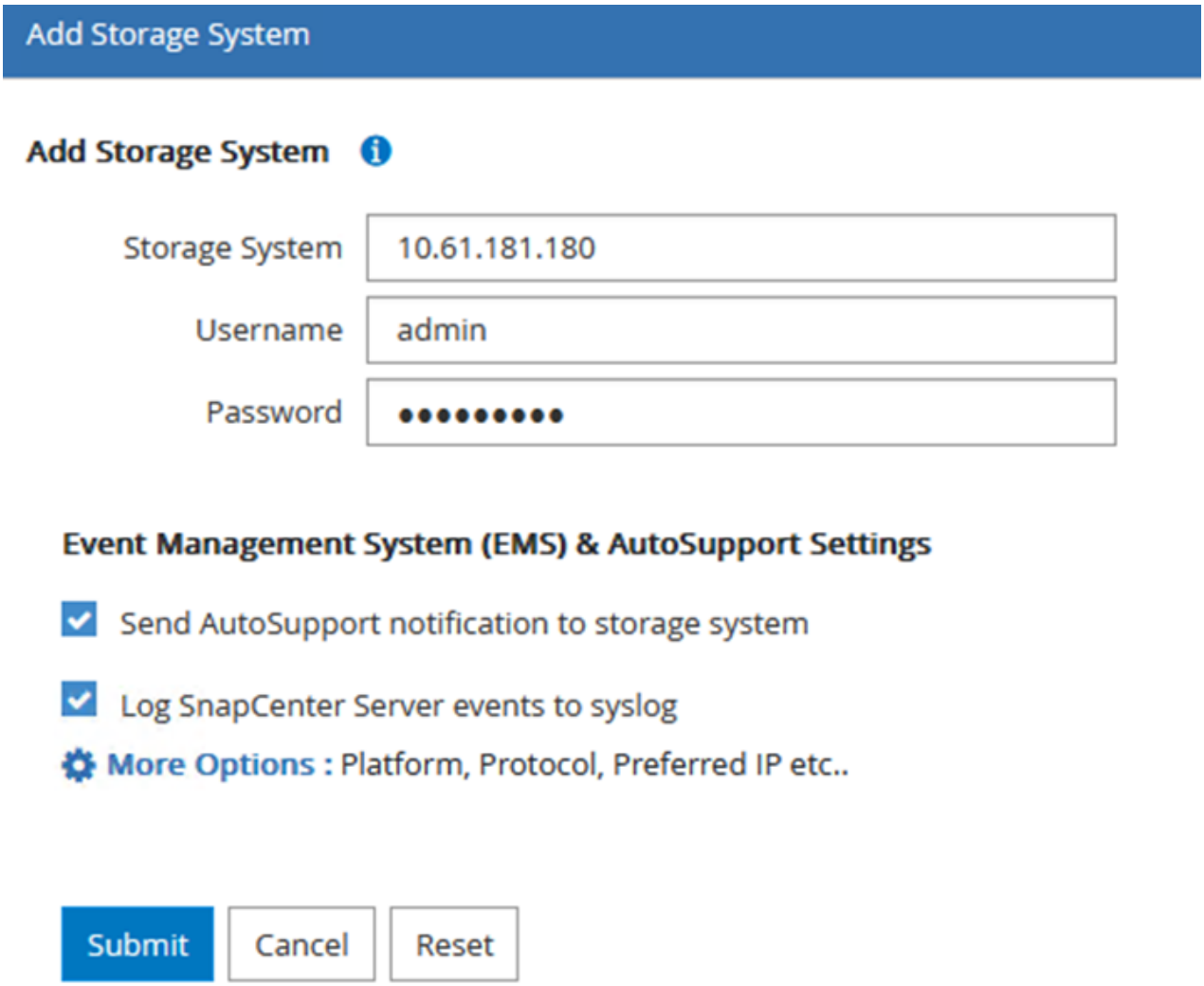
SnapCenter 에 스토리지 컨트롤러 추가

SnapCenter 에 스토리지 컨트롤러를 추가하려면 다음 단계를 완료하세요.

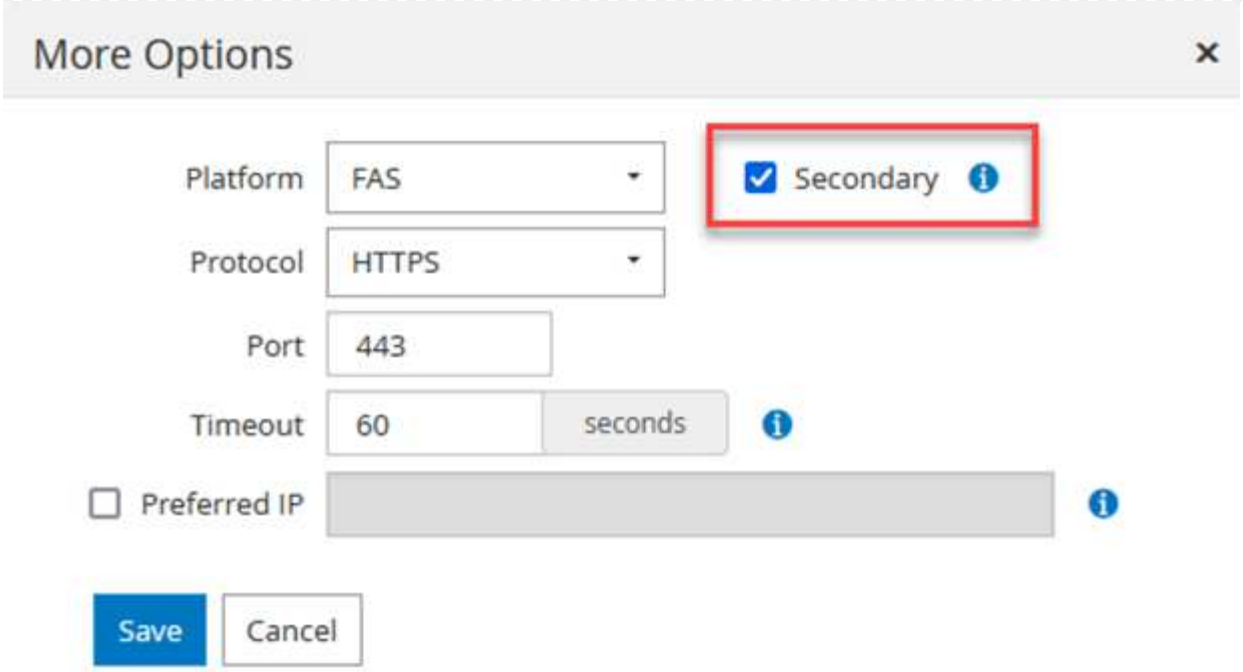
1. 왼쪽 메뉴에서 스토리지 시스템을 선택한 다음 새로 만들기를 클릭하여 SnapCenter 에 스토리지 컨트롤러를 추가하는 프로세스를 시작합니다.



2. 스토리지 시스템 추가 대화 상자에서 로컬 온프레미스 ONTAP 클러스터의 관리 IP 주소와 사용자 이름 및 비밀번호를 추가합니다. 그런 다음 제출을 클릭하여 스토리지 시스템 검색을 시작하세요.



3. SnapCenter 에 FSx ONTAP 시스템을 추가하려면 이 프로세스를 반복합니다. 이 경우, 스토리지 시스템 추가 창 하단에서 추가 옵션을 선택하고 보조 스토리지 시스템의 확인란을 클릭하여 FSx 시스템을 SnapMirror 복사본이나 기본 백업 스냅샷으로 업데이트된 보조 스토리지 시스템으로 지정합니다.

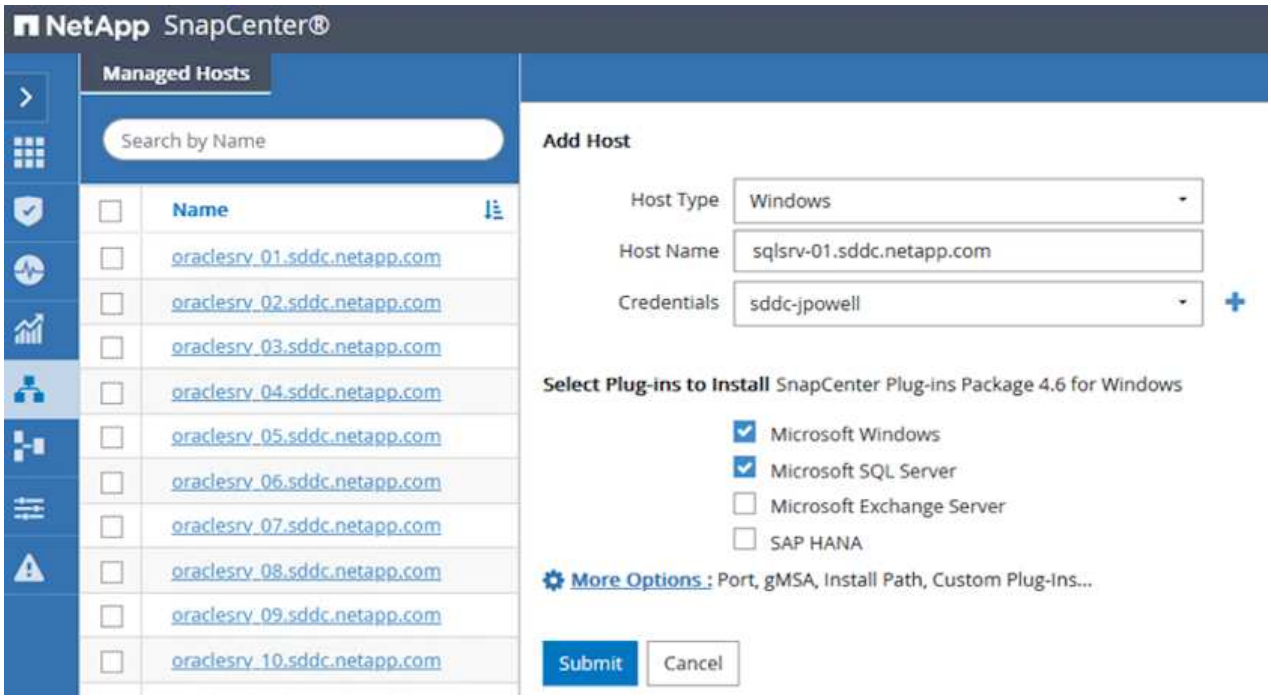


SnapCenter 에 스토리지 시스템을 추가하는 것과 관련된 자세한 내용은 다음 설명서를 참조하세요. "이 링크" .

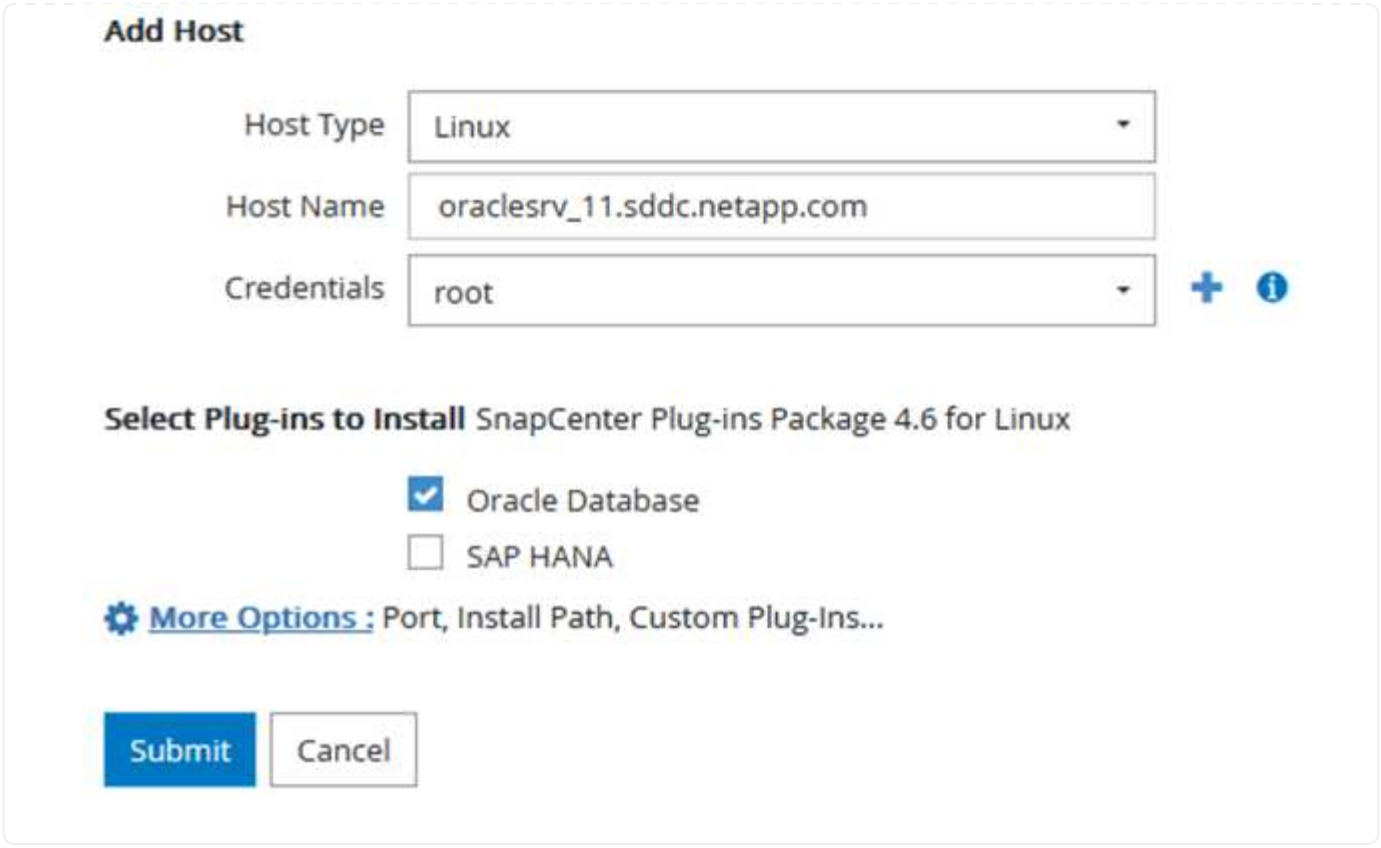
SnapCenter 에 호스트 추가

다음 단계는 SnapCenter 에 호스트 애플리케이션 서버를 추가하는 것입니다. SQL Server와 Oracle의 프로세스는 비슷합니다.

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



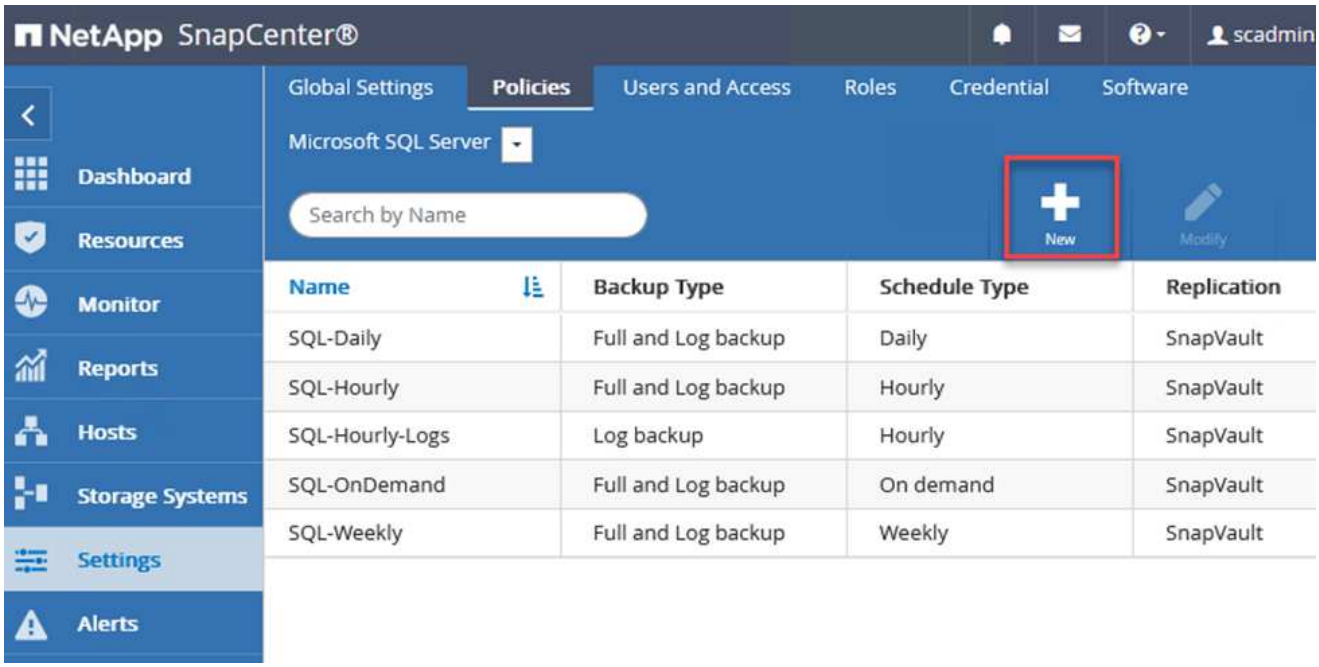
3. Oracle의 경우, "호스트 추가" 대화 상자에서 필수 필드를 입력하고 Oracle 데이터베이스 플러그인 확인란을 선택합니다. 그런 다음 "제출"을 클릭하여 검색 프로세스를 시작하고 SnapCenter 에 호스트를 추가합니다.


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 정책 만들기

정책은 백업 작업에 따라야 할 구체적인 규칙을 설정합니다. 여기에는 백업 일정, 복제 유형, SnapCenter 트랜잭션 로그 백업 및 잘라내기를 처리하는 방법 등이 포함되지만 이에 국한되지는 않습니다.

SnapCenter 웹 클라이언트의 설정 섹션에서 정책에 액세스할 수 있습니다.



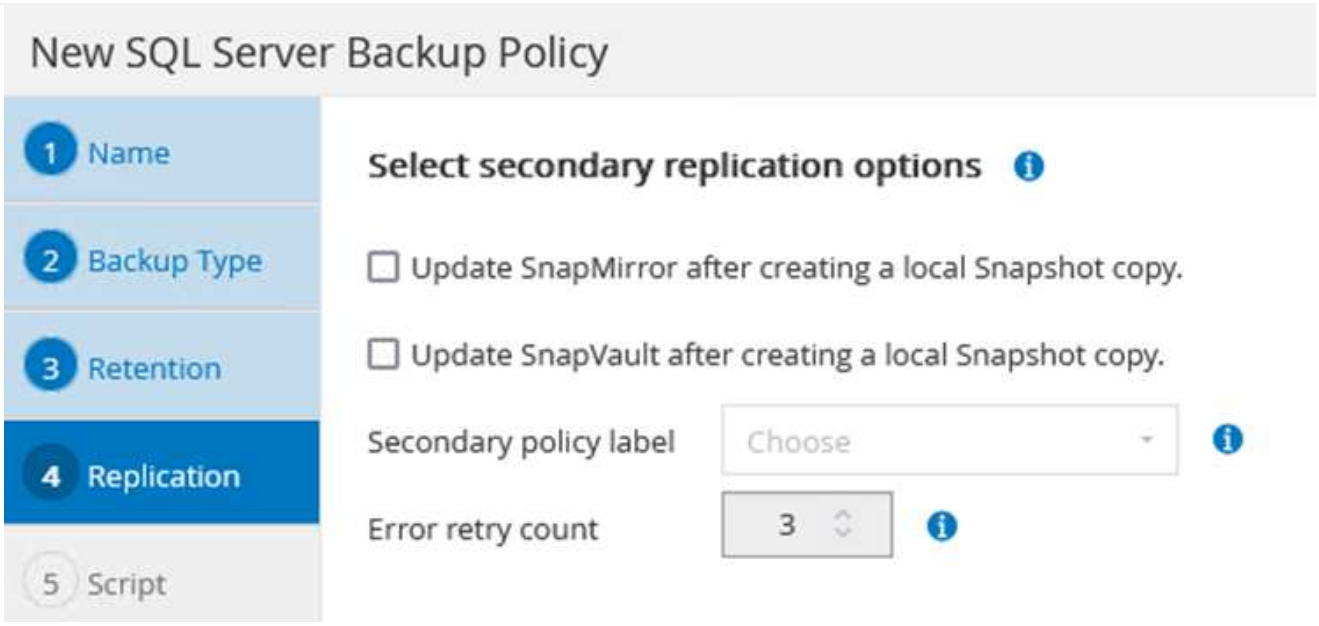
SQL Server 백업에 대한 정책 생성에 대한 전체 정보는 다음을 참조하세요. "SnapCenter 문서" .

Oracle 백업에 대한 정책 생성에 대한 전체 정보는 다음을 참조하세요. "SnapCenter 문서" .

참고사항**:**

- 정책 생성 마법사를 진행하면서 복제 섹션을 특별히 주의하세요. 이 섹션에서는 백업 프로세스 중에 생성할 보조 SnapMirror 복사본 유형을 지정합니다.
- "로컬 스냅샷 복사본을 만든 후 SnapMirror 업데이트" 설정은 동일한 클러스터에 있는 두 스토리지 가상 머신 간에 SnapMirror 관계가 있는 경우 해당 관계를 업데이트하는 것을 의미합니다.
- "로컬 SnapShot 복사본을 만든 후 SnapVault 업데이트" 설정은 두 개의 별도 클러스터와 온프레미스 ONTAP 시스템과 Cloud Volumes ONTAP 또는 FSx ONTAP 사이에 존재하는 SnapMirror 관계를 업데이트하는 데 사용됩니다.

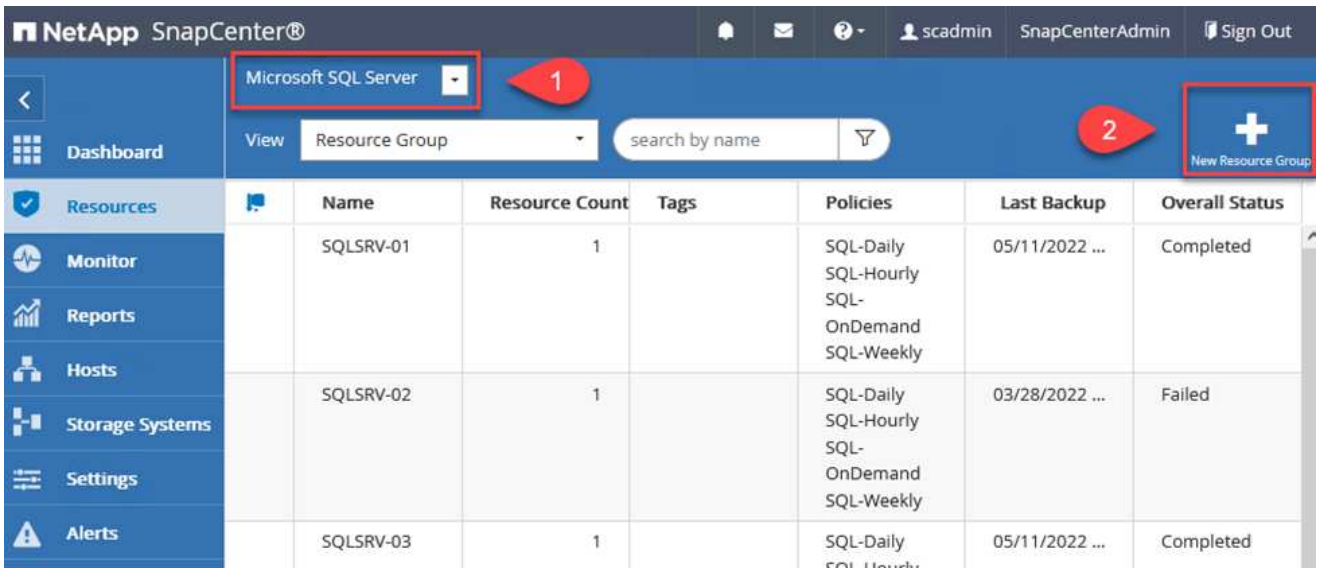
다음 이미지는 이전 옵션과 백업 정책 마법사에서 이 옵션이 어떻게 나타나는지 보여줍니다.



SnapCenter 리소스 그룹 만들기

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

1. 왼쪽 메뉴의 리소스 섹션으로 이동하세요.
2. 창 상단에서 작업할 리소스 유형을 선택합니다(이 경우 Microsoft SQL Server). 그런 다음 새 리소스 그룹을 클릭합니다.



SnapCenter 설명서에서는 SQL Server와 Oracle 데이터베이스 모두에 대한 리소스 그룹을 만드는 방법에 대한 단계별 세부 정보를 다룹니다.

SQL 리소스를 백업하려면 다음을 따르세요. "이 링크" .

Oracle 리소스를 백업하려면 다음을 따르세요. "이 링크" .

Veeam 백업 서버 배포 및 구성

Veeam Backup & Replication 소프트웨어는 Veeam 스케일아웃 백업 저장소(SOBR)를 사용하여 애플리케이션 가상 머신을 백업하고 백업 사본을 Amazon S3 버킷에 보관하는 솔루션에 사용됩니다. 이 솔루션에서는 Veeam이 Windows 서버에 배포됩니다. Veeam 배포에 대한 구체적인 지침은 다음을 참조하세요. "Veeam 도움말 센터 기술 문서" .

Veeam 스케일아웃 백업 저장소 구성

소프트웨어를 배포하고 라이선스를 취득한 후 백업 작업의 대상 저장소로 SOBR(스케일아웃 백업 저장소)을 생성할 수 있습니다. 재해 복구를 위해 VM 데이터의 백업으로 S3 버킷도 포함해야 합니다.

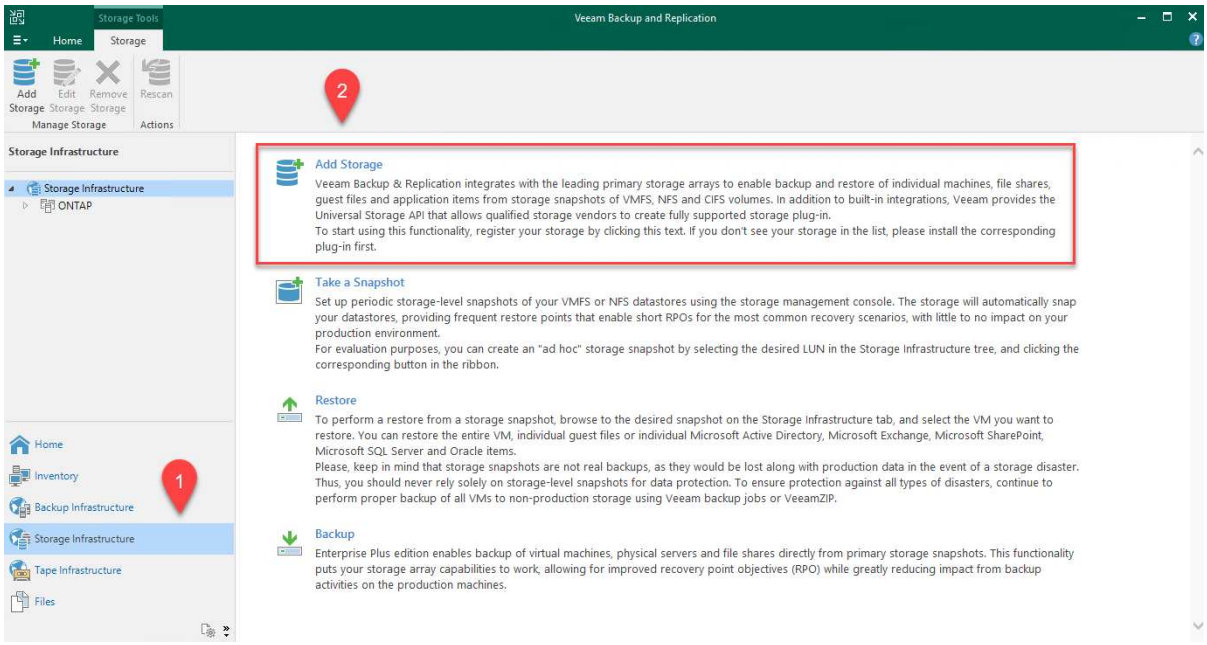
시작하기 전에 다음 전제 조건을 확인하세요.

1. 온프레미스 ONTAP 시스템에 백업 대상 저장소로 SMB 파일 공유를 만듭니다.
2. SOBR에 포함할 Amazon S3 버킷을 만듭니다. 이는 오프사이트 백업을 위한 저장소입니다.

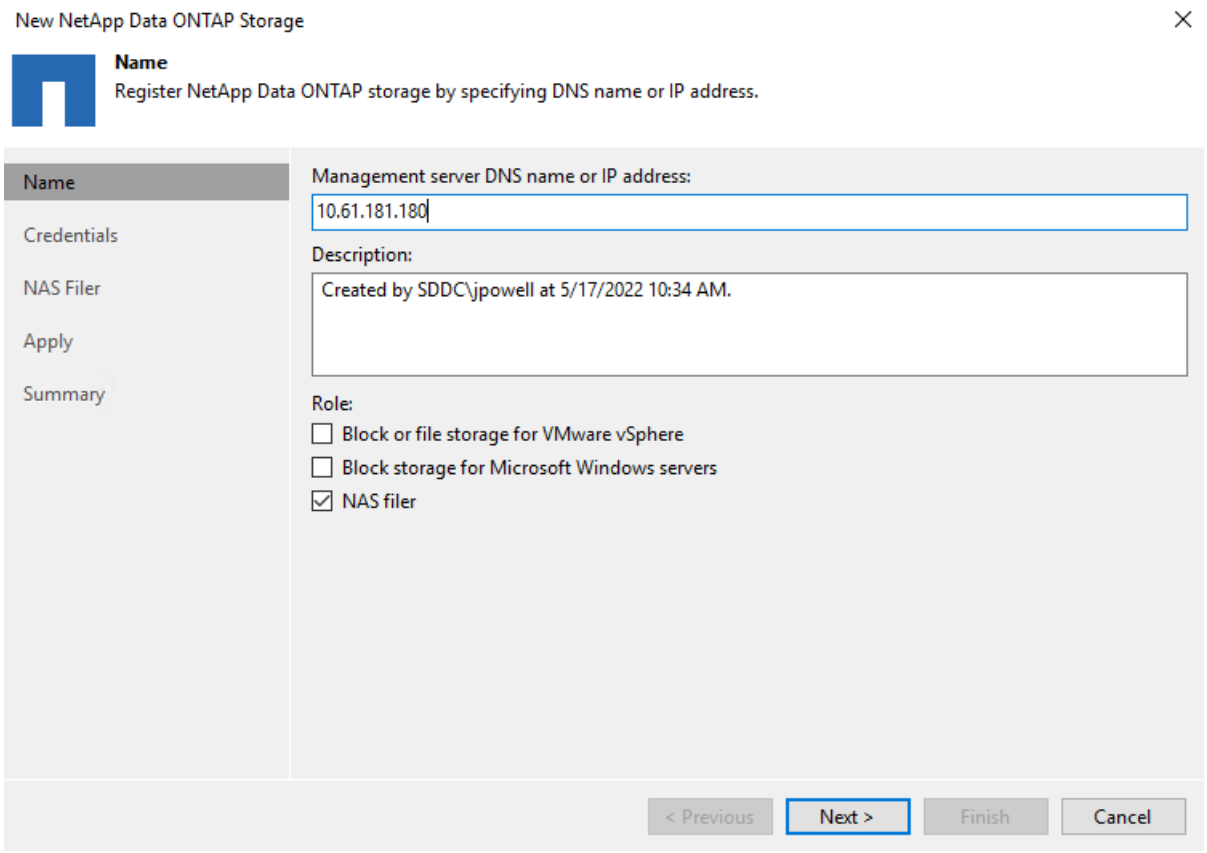
Veeam에 ONTAP 스토리지 추가

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

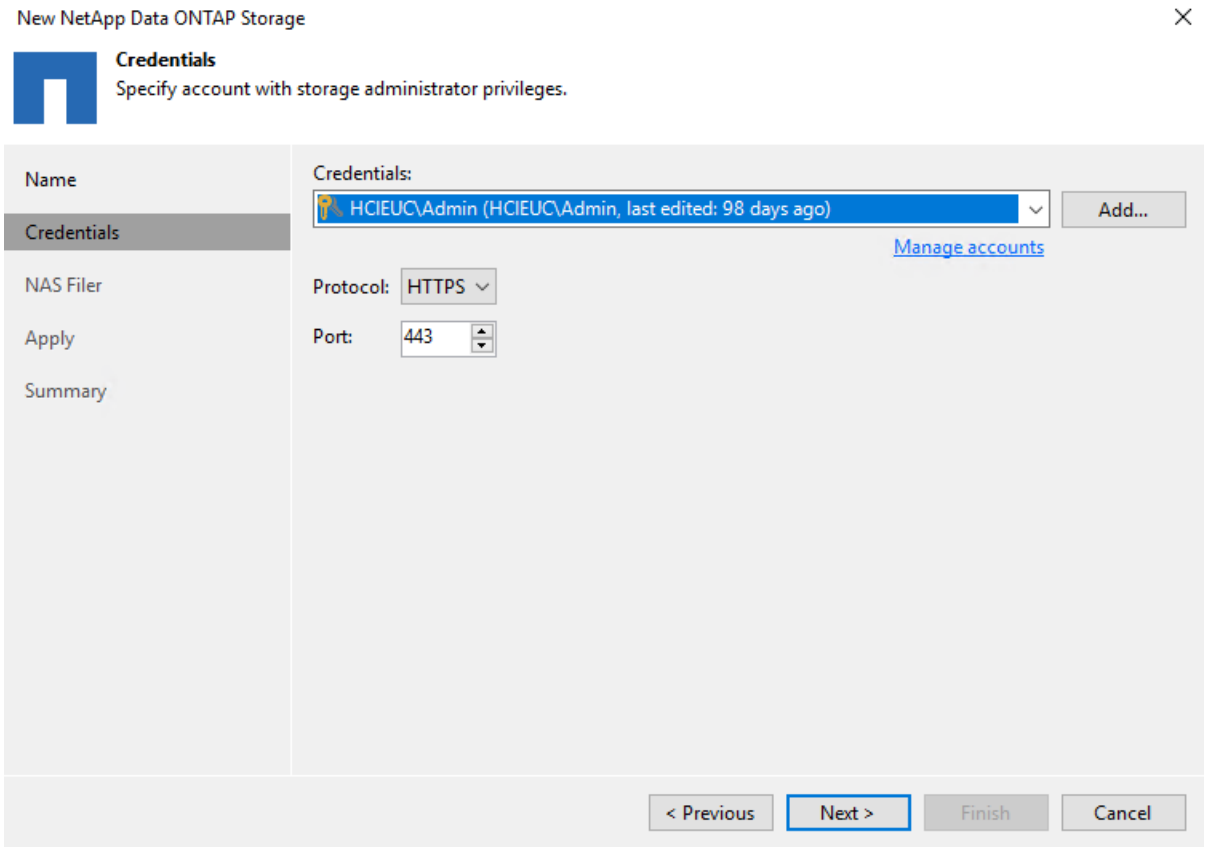
1. Veeam 콘솔을 열고 로그인합니다. 스토리지 인프라로 이동한 다음 스토리지 추가를 선택합니다.



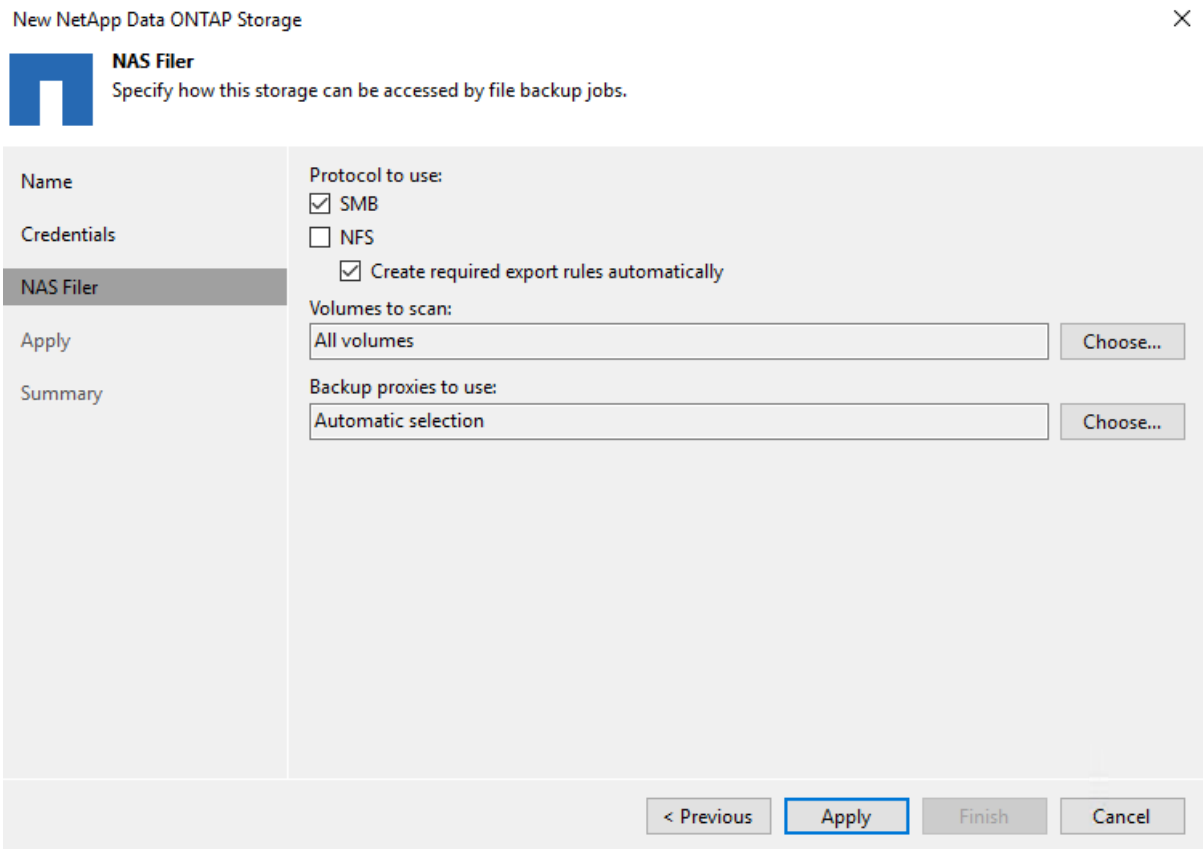
2. 스토리지 추가 마법사에서 스토리지 공급업체로 NetApp 선택한 다음 Data ONTAP 선택합니다.
3. 관리 IP 주소를 입력하고 NAS Filer 상자를 선택하세요. 다음을 클릭하세요.



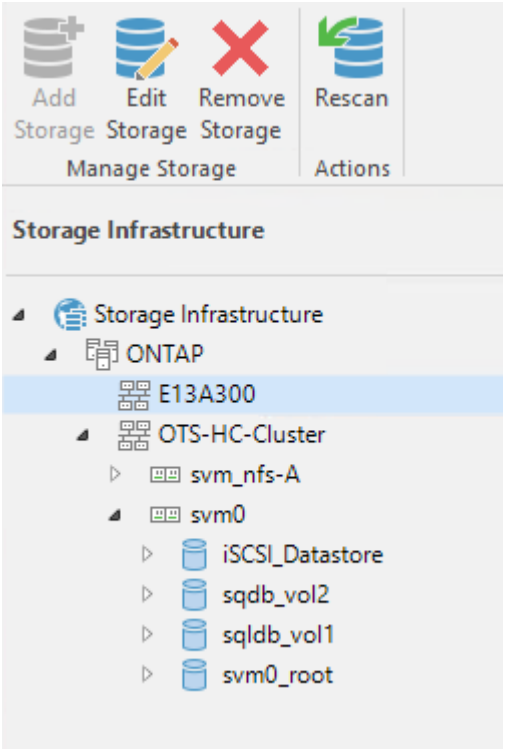
4. ONTAP 클러스터에 액세스하려면 자격 증명을 추가하세요.



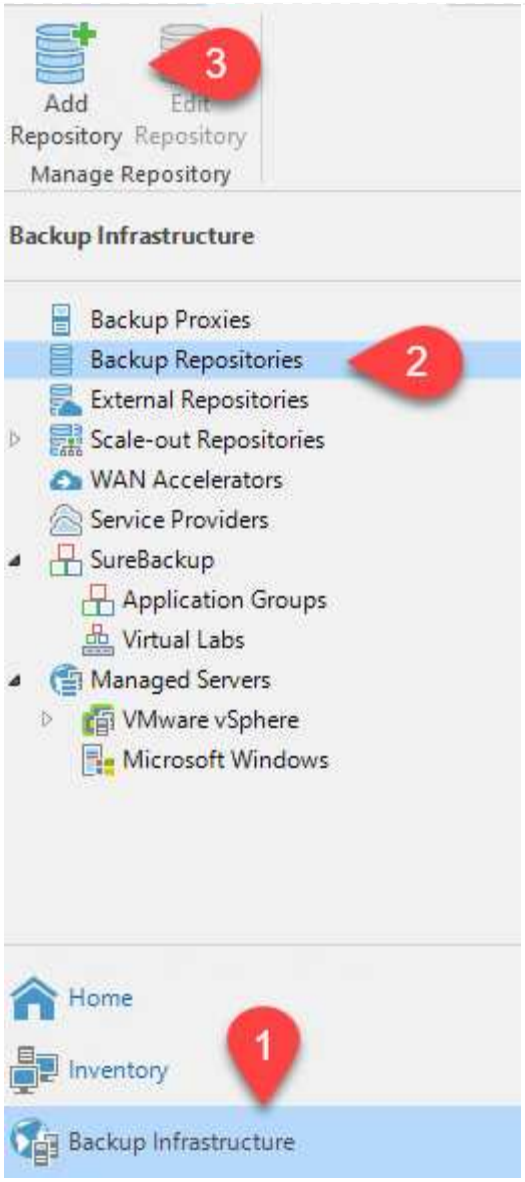
5. NAS Filer 페이지에서 스캔할 원하는 프로토콜을 선택하고 다음을 선택합니다.



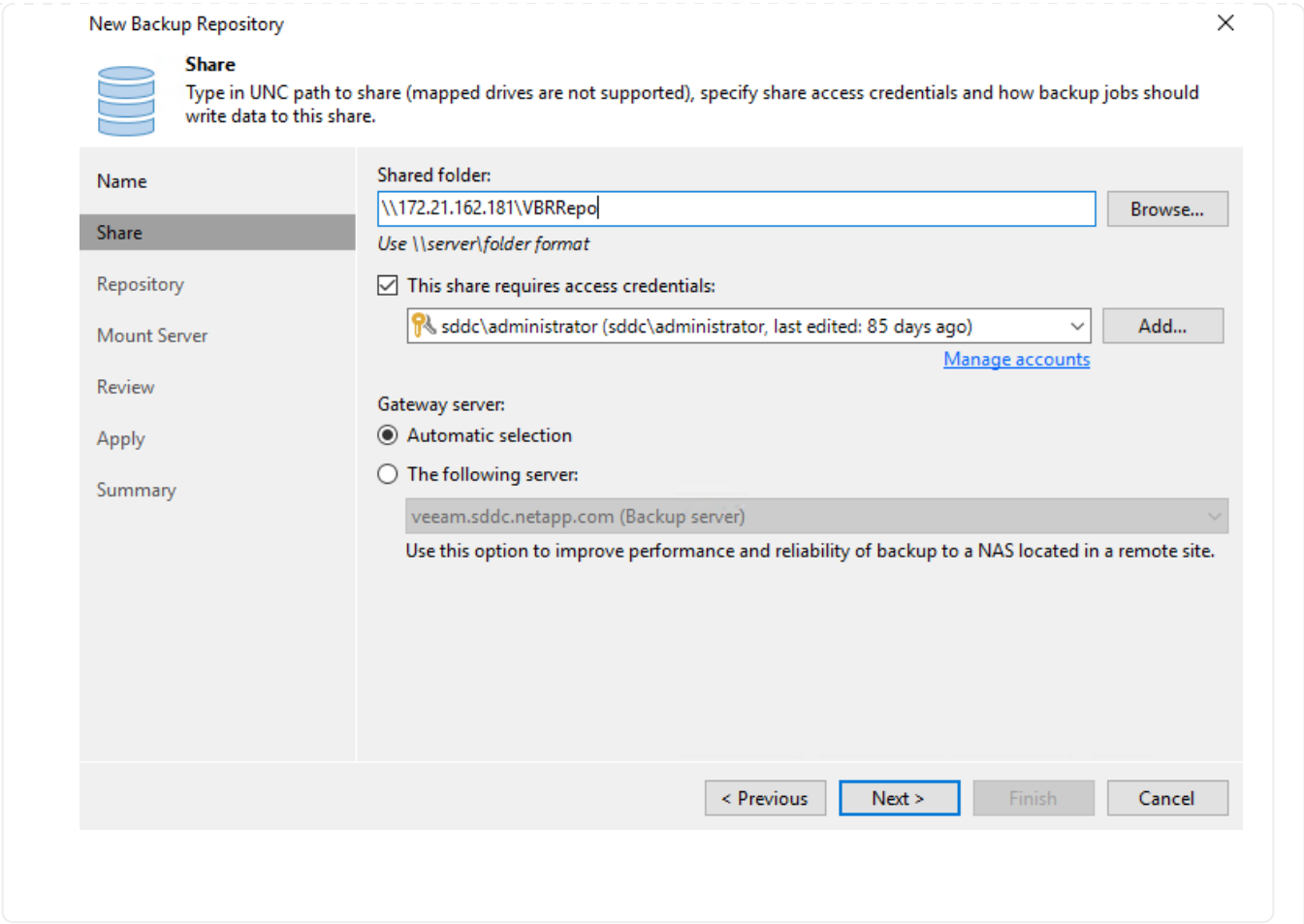
6. 마법사의 적용 및 요약 페이지를 완료하고 마침을 클릭하여 저장소 검색 프로세스를 시작합니다. 검사가 완료되면 ONTAP 클러스터가 NAS 파일러와 함께 사용 가능한 리소스로 추가됩니다.



7. 새로 검색된 NAS 공유를 사용하여 백업 저장소를 만듭니다. 백업 인프라에서 백업 저장소를 선택하고 저장소 추가 메뉴 항목을 클릭합니다.



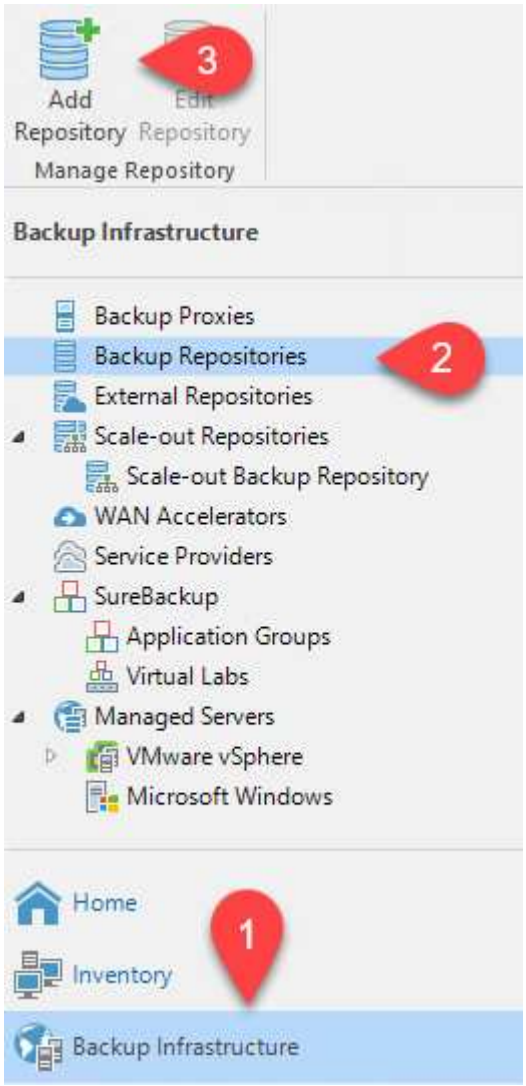
8. 새 백업 저장소 마법사의 모든 단계를 따라 저장소를 만듭니다. Veeam 백업 저장소 생성에 대한 자세한 내용은 다음을 참조하세요. "Veeam 문서" .


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

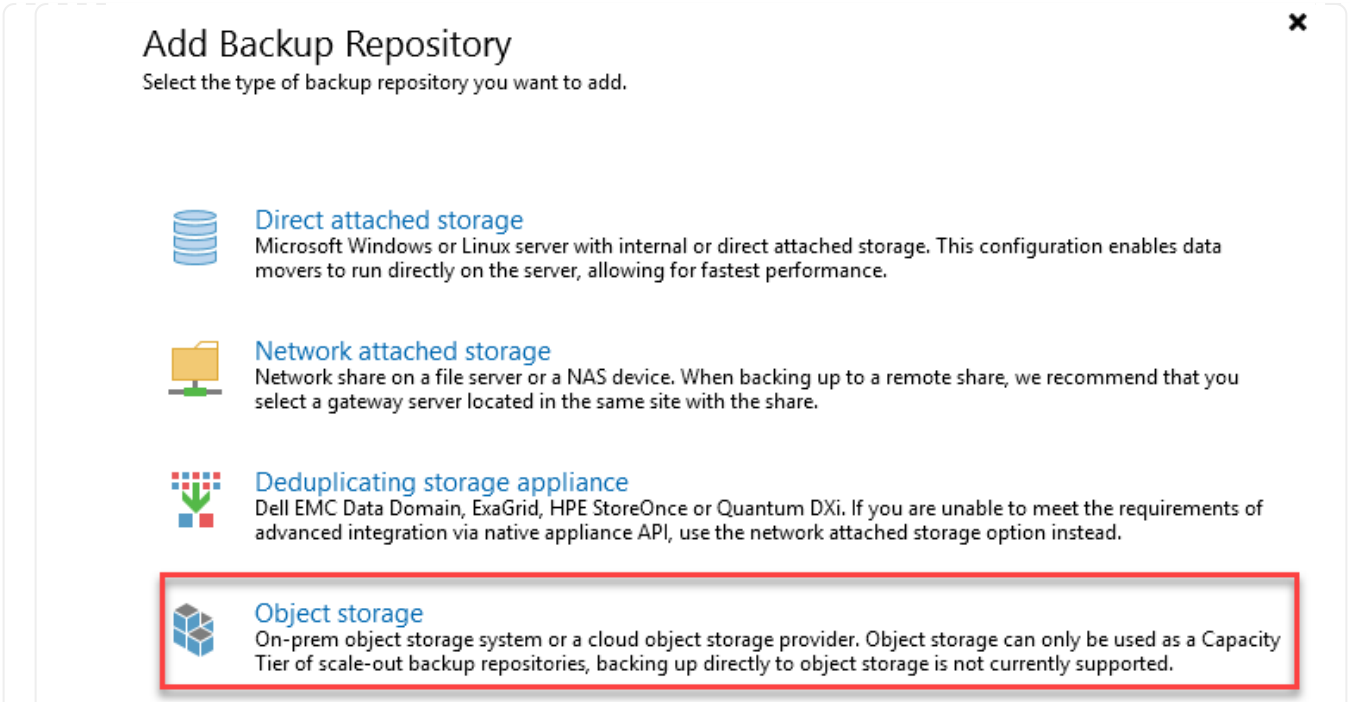
Amazon S3 버킷을 백업 저장소로 추가합니다.

다음 단계는 Amazon S3 스토리지를 백업 저장소로 추가하는 것입니다.

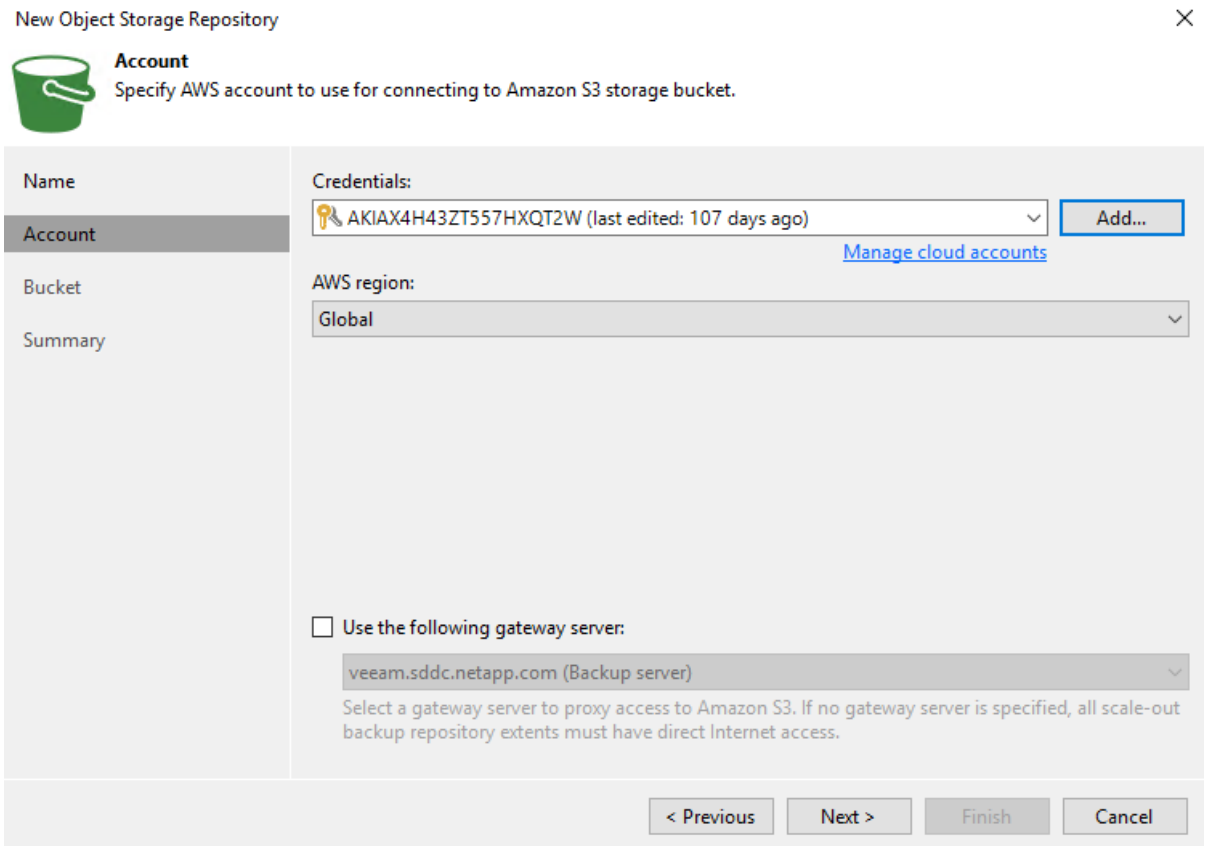
1. 백업 인프라 > 백업 저장소로 이동합니다. 저장소 추가를 클릭합니다.



2. 백업 저장소 추가 마법사에서 개체 스토리지를 선택한 다음 Amazon S3를 선택합니다. 그러면 새 개체 스토리지 리포지토리 마법사가 시작됩니다.



3. 개체 스토리지 저장소의 이름을 입력하고 다음을 클릭합니다.
4. 다음 섹션에서는 신임장을 입력하세요. AWS 액세스 키와 비밀 키가 필요합니다.

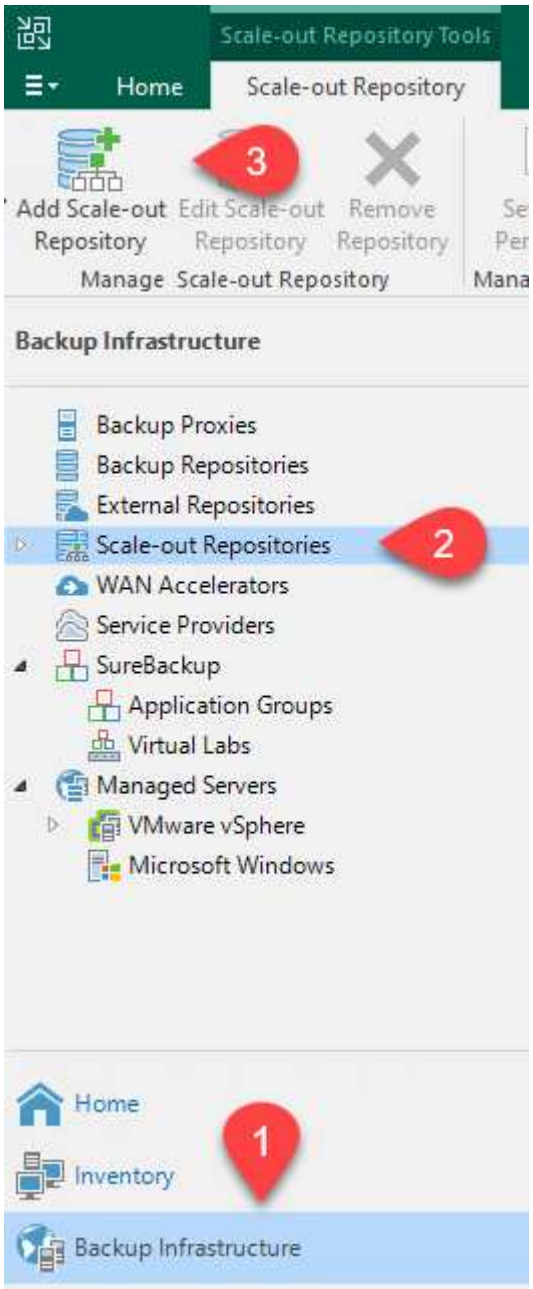


5. Amazon 구성이 로드되면 데이터 센터, 버킷, 폴더를 선택하고 적용을 클릭합니다. 마지막으로 마침을 클릭하여 마법사를 닫습니다.

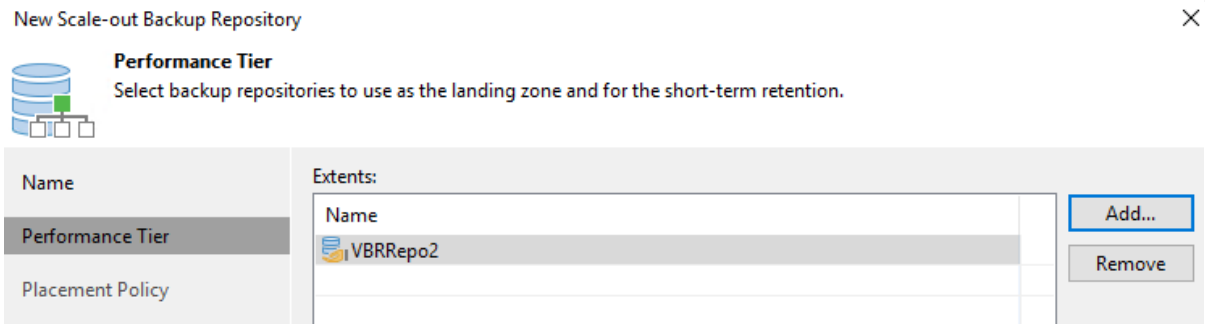
스케일아웃 백업 저장소 생성

이제 Veeam에 스토리지 저장소를 추가했으므로 재해 복구를 위해 오프사이트 Amazon S3 개체 스토리지에 백업 사본을 자동으로 계층화하는 SOBR을 만들 수 있습니다.

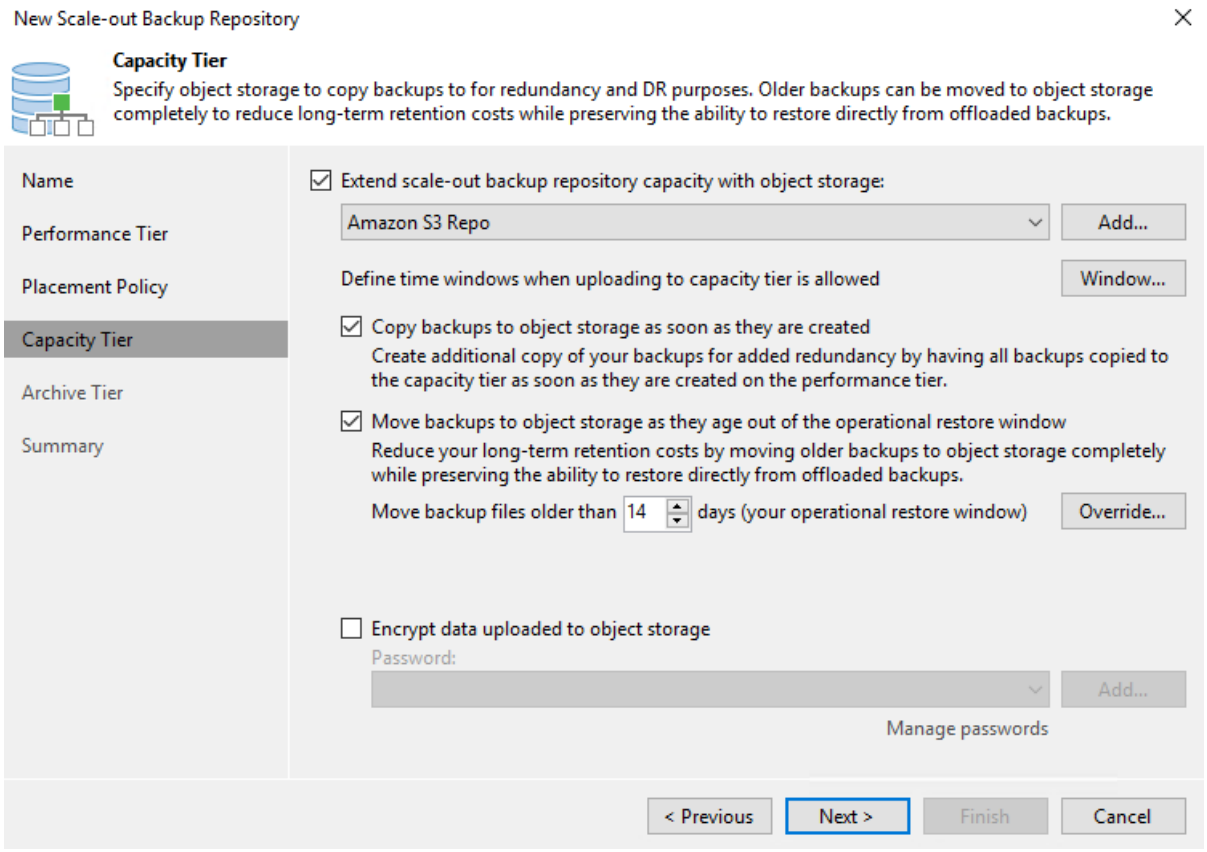
1. 백업 인프라에서 스케일아웃 리포지토리를 선택한 다음 스케일아웃 리포지토리 추가 메뉴 항목을 클릭합니다.



2. 새로운 확장형 백업 저장소에서 SOBR의 이름을 입력하고 다음을 클릭합니다.
3. 성능 계층의 경우 로컬 ONTAP 클러스터에 있는 SMB 공유가 포함된 백업 저장소를 선택합니다.



4. 배치 정책의 경우 요구 사항에 따라 데이터 지역성이나 성능을 선택하세요. 다음을 선택하세요.
5. 용량 계층의 경우 Amazon S3 객체 스토리지로 SOBR을 확장합니다. 재해 복구를 위해 보조 백업을 적시에 전달하려면 백업이 생성되는 즉시 개체 스토리지에 복사를 선택하세요.



6. 마지막으로 '적용' 및 '마침'을 선택하여 SOBR 생성을 완료합니다.

스케일아웃 백업 저장소 작업 생성

Veeam을 구성하는 마지막 단계는 새로 만든 SOBR을 백업 대상으로 사용하여 백업 작업을 만드는 것입니다. 백업 작업을 만드는 것은 모든 스토리지 관리자의 일반적인 업무이므로 여기서는 자세한 단계를 다루지 않습니다. Veeam에서 백업 작업을 만드는 방법에 대한 자세한 내용은 다음을 참조하세요. "Veeam 도움말 센터 기술 문서" .

BlueXP backup and recovery 도구와 구성

AWS에서 실행되는 VMware Cloud Volume 서비스로 애플리케이션 VM 및 데이터베이스 볼륨의 장애 조치를 수행하려면 SnapCenter Server와 Veeam Backup and Replication Server의 실행 인스턴스를 설치하고 구성해야 합니다. 장애 조치가 완료된 후에는 온프레미스 데이터 센터로의 장애 복구를 계획하고 실행할 때까지 정상적인 백업 작업을 재개하도록 이러한 도구를 구성해야 합니다.

보조 **Windows SnapCenter** 서버 배포

SnapCenter 서버는 VMware Cloud SDDC에 배포되거나 VMware Cloud 환경에 네트워크로 연결된 VPC에 있는 EC2 인스턴스에 설치됩니다.

SnapCenter software NetApp 지원 사이트에서 구할 수 있으며 도메인이나 작업 그룹에 있는 Microsoft Windows 시스템에 설치할 수 있습니다. 자세한 계획 가이드와 설치 지침은 다음에서 확인할 수 있습니다. "NetApp 문서 센터" .

SnapCenter software 다음에서 찾을 수 있습니다. "이 링크" .

보조 **Windows SnapCenter** 서버 구성

FSx ONTAP 에 미러링된 애플리케이션 데이터를 복원하려면 먼저 온프레미스 SnapCenter 데이터베이스를 전체 복원해야 합니다. 이 프로세스가 완료되면 VM과의 통신이 재설정되고 이제 FSx ONTAP 기본 스토리지로 사용하여 애플리케이션 백업을 재개할 수 있습니다.

이를 달성하려면 SnapCenter 서버에서 다음 항목을 완료해야 합니다.

1. 컴퓨터 이름을 원래 온프레미스 SnapCenter 서버와 동일하게 구성합니다.
2. VMware Cloud 및 FSx ONTAP 인스턴스와 통신하도록 네트워킹을 구성합니다.
3. SnapCenter 데이터베이스를 복원하는 절차를 완료하세요.
4. SnapCenter 재해 복구 모드에 있는지 확인하여 FSx가 이제 백업을 위한 기본 저장소인지 확인하세요.
5. 복구된 가상 머신과 통신이 다시 설정되었는지 확인합니다.

보조 **Veeam** 백업 및 복제 서버 배포

AWS의 VMware Cloud에 있는 Windows 서버나 EC2 인스턴스에 Veeam Backup & Replication 서버를 설치할 수 있습니다. 자세한 구현 지침은 다음을 참조하세요. "Veeam 도움말 센터 기술 문서" .

보조 **Veeam** 백업 및 복제 서버 구성

Amazon S3 스토리지에 백업된 가상 머신을 복원하려면 Windows 서버에 Veeam Server를 설치하고 VMware Cloud, FSx ONTAP 및 원본 백업 저장소가 포함된 S3 버킷과 통신하도록 구성해야 합니다. VM이 복원된 후 새로운 백업을 수행하려면 FSx ONTAP 에 새로운 백업 저장소를 구성해야 합니다.

이 프로세스를 수행하려면 다음 항목을 완료해야 합니다.

1. VMware Cloud, FSx ONTAP 및 원본 백업 저장소가 포함된 S3 버킷과 통신하도록 네트워킹을 구성합니다.
2. FSx ONTAP 에서 SMB 공유를 새로운 백업 저장소로 구성합니다.
3. 온프레미스에서 확장형 백업 저장소의 일부로 사용된 원래 S3 버킷을 마운트합니다.
4. VM을 복원한 후 SQL 및 Oracle VM을 보호하기 위해 새로운 백업 작업을 설정합니다.

Veeam을 사용하여 VM을 복원하는 방법에 대한 자세한 내용은 섹션을 참조하세요."Veeam Full Restore를 사용하여 애플리케이션 VM 복원" .

재해 복구를 위한 **SnapCenter** 데이터베이스 백업

SnapCenter 사용하면 재해 발생 시 SnapCenter 서버를 복구할 목적으로 기본 MySQL 데이터베이스와 구성 데이터를 백업하고 복구할 수 있습니다. 우리 솔루션의 경우, VPC에 있는 AWS EC2 인스턴스에서 SnapCenter 데이터베이스와 구성을 복구했습니다. SnapCenter 의 재해 복구에 대한 자세한 내용은 다음을 참조하세요. "이 링크" .

SnapCenter 백업 필수 구성 요소

SnapCenter 백업에는 다음과 같은 필수 구성 요소가 필요합니다.

- 백업된 데이터베이스와 구성 파일을 찾기 위해 온프레미스 ONTAP 시스템에 볼륨과 SMB 공유를 생성했습니다.
- 온프레미스 ONTAP 시스템과 AWS 계정의 FSx 또는 CVO 간의 SnapMirror 관계입니다. 이 관계는 백업된 SnapCenter 데이터베이스와 구성 파일이 포함된 스냅샷을 전송하는 데 사용됩니다.
- EC2 인스턴스나 VMware Cloud SDDC의 VM에 있는 클라우드 계정에 Windows Server가 설치되어 있습니다.
- VMware Cloud의 Windows EC2 인스턴스 또는 VM에 SnapCenter 설치되었습니다.

SnapCenter 백업 및 복원 프로세스 요약

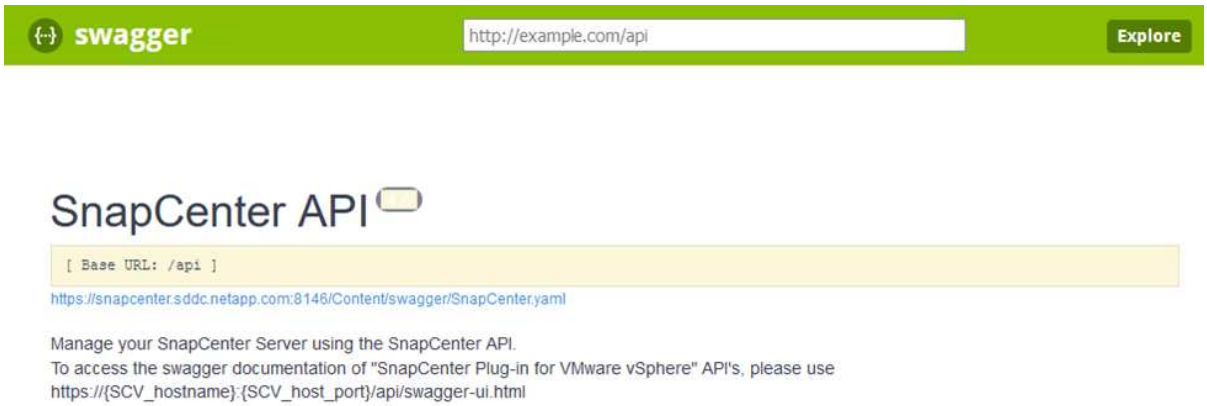
- 백업 DB 및 구성 파일을 호스팅하기 위해 온프레미스 ONTAP 시스템에 볼륨을 생성합니다.
- 온프레미스와 FSx/CVO 간에 SnapMirror 관계를 설정합니다.
- SMB 공유를 마운트합니다.
- API 작업을 수행하기 위한 Swagger 인증 토큰을 검색합니다.
- DB 복원 프로세스를 시작합니다.
- xcopy 유틸리티를 사용하여 db 및 config 파일 로컬 디렉토리를 SMB 공유로 복사합니다.
- FSx에서 ONTAP 볼륨의 복제본을 만듭니다(온프레미스에서 SnapMirror 통해 복사).
- FSx에서 EC2/VMware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

SnapCenter REST API 명령을 실행하기 위한 웹 클라이언트 인터페이스를 제공합니다. Swagger를 통해 REST API에 액세스하는 방법에 대한 정보는 SnapCenter 설명서를 참조하세요. "이 링크" .

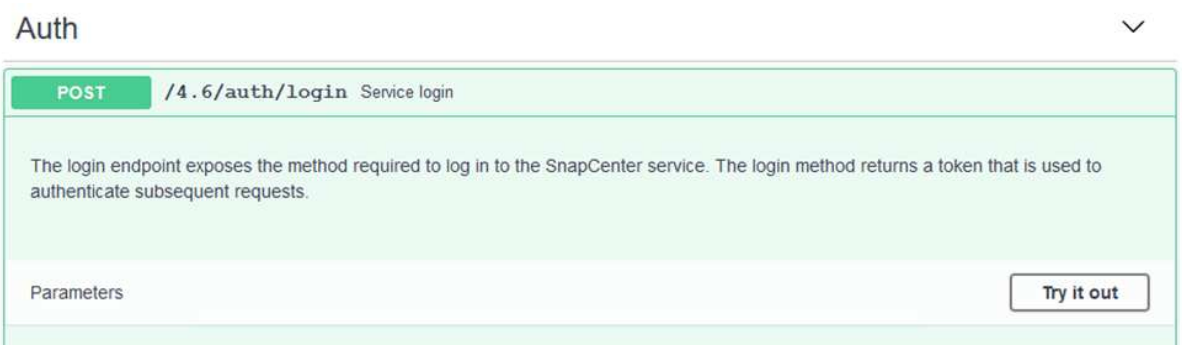
Swagger에 로그인하여 승인 토큰을 받으세요

Swagger 페이지로 이동한 후에는 데이터베이스 복원 프로세스를 시작하기 위해 권한 부여 토큰을 검색해야 합니다.

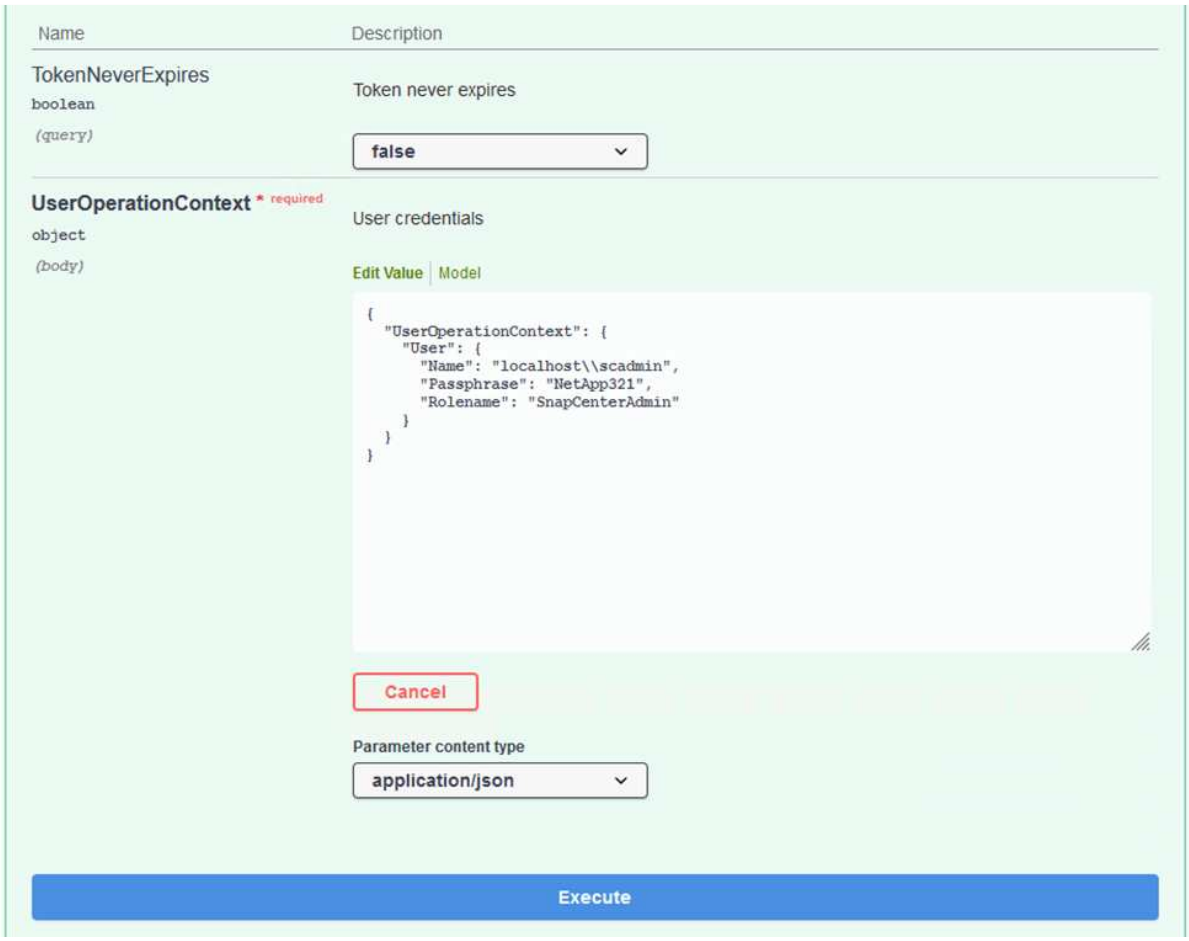
1. _\https://< SnapCenter 서버 IP>:8146/swagger/_에서 SnapCenter Swagger API 웹 페이지에 접속하세요.



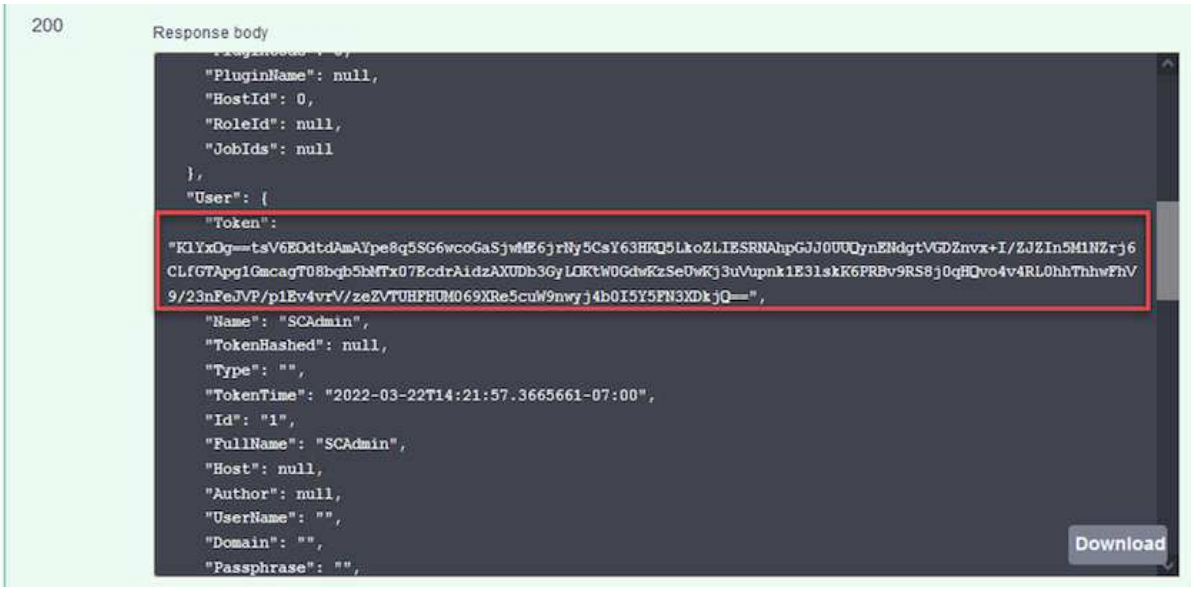
2. 인증 섹션을 확장하고 사용해보기를 클릭하세요.



3. UserOperationContext 영역에서 SnapCenter 자격 증명과 역할을 입력하고 실행을 클릭합니다.



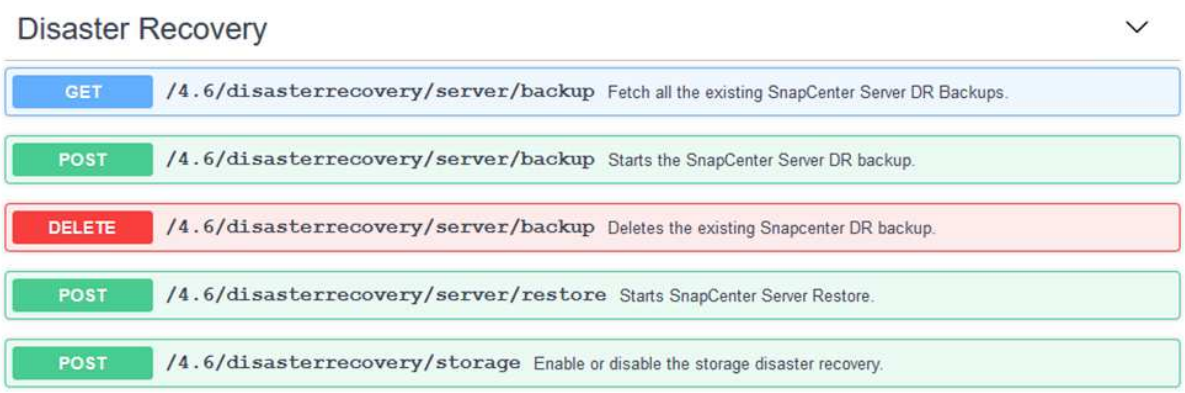
4. 아래의 응답 본문에서 토큰을 확인할 수 있습니다. 백업 프로세스를 실행할 때 인증을 위해 토큰 텍스트를 복사합니다.



SnapCenter 데이터베이스 백업 수행

다음으로 Swagger 페이지의 재해 복구 영역으로 이동하여 SnapCenter 백업 프로세스를 시작합니다.

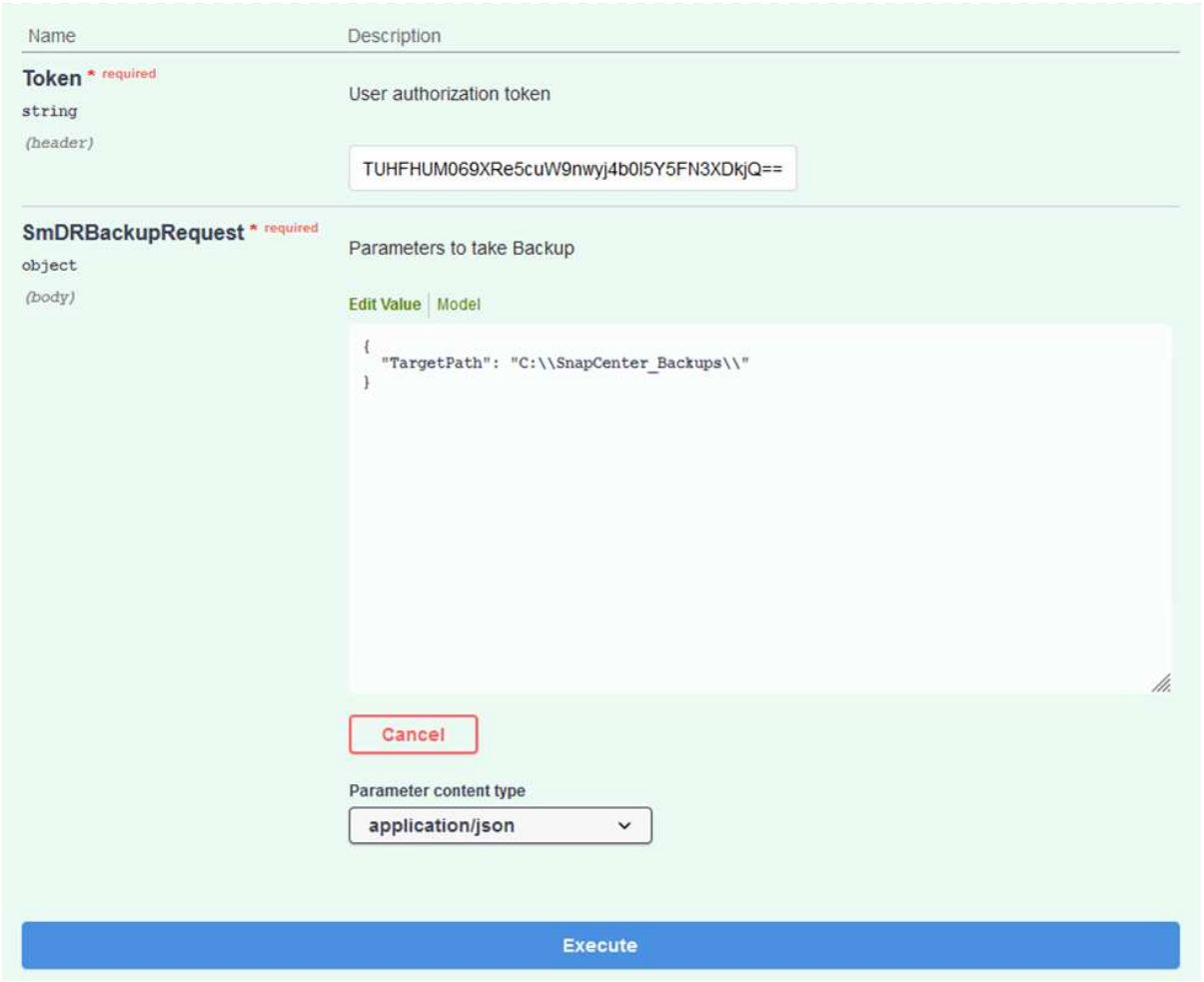
1. 재해 복구 영역을 클릭하여 확장합니다.



2. 확장하다 `/4.6/disasterrecovery/server/backup` 섹션으로 가서 '시도해보기'를 클릭하세요.

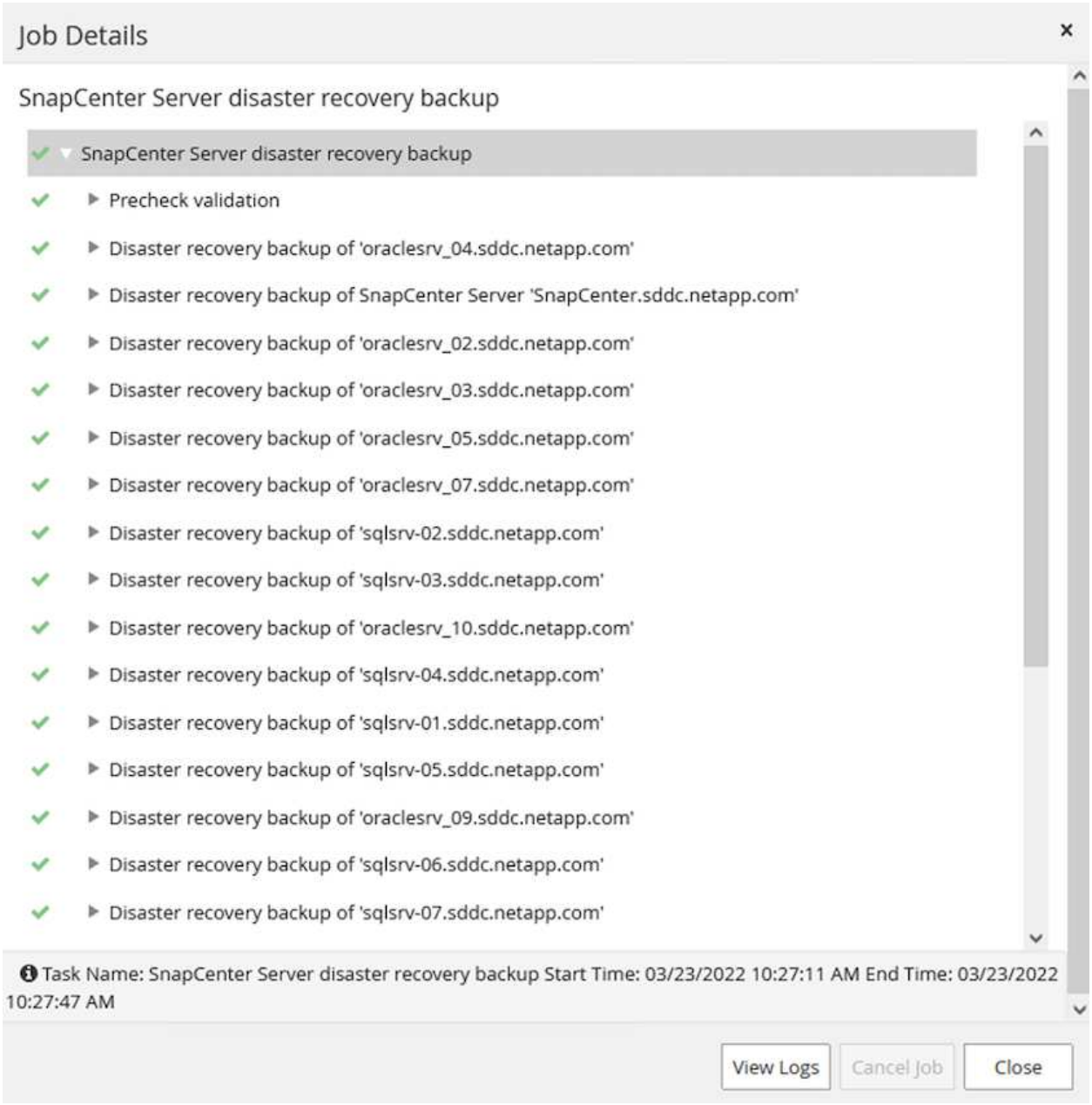
3. SmDRBackupRequest 섹션에서 올바른 로컬 대상 경로를 추가하고 실행을 선택하여 SnapCenter 데이터베이스 및 구성의 백업을 시작합니다.

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


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

SnapCenter 에서 백업 작업 모니터링

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



XCOPY 유틸리티를 사용하여 데이터베이스 백업 파일을 **SMB** 공유로 복사합니다**.**

다음으로 SnapCenter 서버의 로컬 드라이브에서 CIFS 공유로 백업을 옮겨야 합니다. 이 공유는 SnapMirror 사용하여 AWS의 FSx 인스턴스에 있는 보조 위치로 데이터를 복사하는 데 사용됩니다. 특정 옵션과 함께 xcopy를 사용하여 파일의 권한을 유지합니다.

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
```

장애 조치

재해는 **1**차 현장에서 발생합니다**.**

온프레미스 기본 데이터 센터에서 재해가 발생하는 경우, 당사 시나리오에는 AWS의 VMware Cloud를 사용하여 Amazon Web Services 인프라에 있는 보조 사이트로 장애 조치를 취하는 것이 포함됩니다. 가상 머신과 온프레미스 ONTAP 클러스터에 더 이상 액세스할 수 없다고 가정합니다. 또한 SnapCenter 와 Veeam 가상 머신에 더 이상 액세스할 수 없으므로 보조 사이트에서 다시 구축해야 합니다.

이 섹션에서는 인프라를 클라우드로 장애 조치하는 방법을 다루며, 다음과 같은 주제를 다룹니다.

- SnapCenter 데이터베이스를 복구합니다. 새로운 SnapCenter 서버가 구축된 후 MySQL 데이터베이스와 구성 파일을 복원하고 데이터베이스를 재해 복구 모드로 전환하여 보조 FSx 스토리지가 기본 스토리지 장치가 되도록 합니다.
- Veeam Backup & Replication을 사용하여 애플리케이션 가상 머신을 복원합니다. VM 백업이 포함된 S3 스토리지를 연결하고 백업을 가져온 다음 AWS의 VMware Cloud에 복원합니다.
- SnapCenter 사용하여 SQL Server 애플리케이션 데이터를 복원합니다.
- SnapCenter 사용하여 Oracle 애플리케이션 데이터를 복원합니다.

SnapCenter 데이터베이스 복원 프로세스

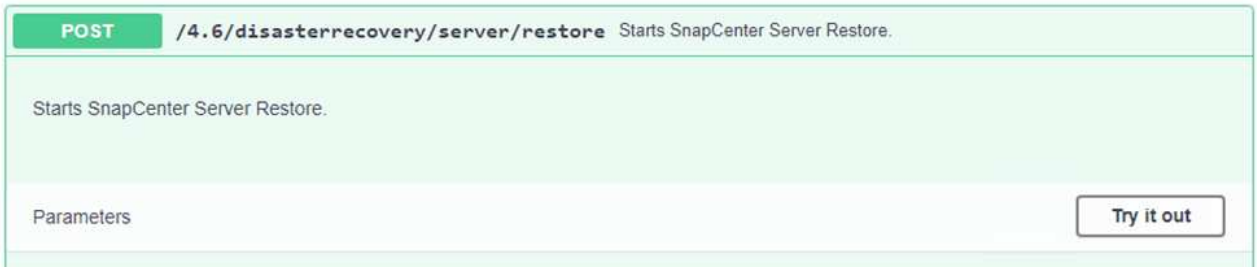
SnapCenter MySQL 데이터베이스와 구성 파일의 백업 및 복원을 허용하여 재해 복구 시나리오를 지원합니다. 이를 통해 관리자는 온프레미스 데이터 센터에서 SnapCenter 데이터베이스를 정기적으로 백업하고 나중에 해당 데이터베이스를 보조 SnapCenter 데이터베이스로 복원할 수 있습니다.

원격 SnapCenter 서버에서 SnapCenter 백업 파일에 액세스하려면 다음 단계를 완료하세요.

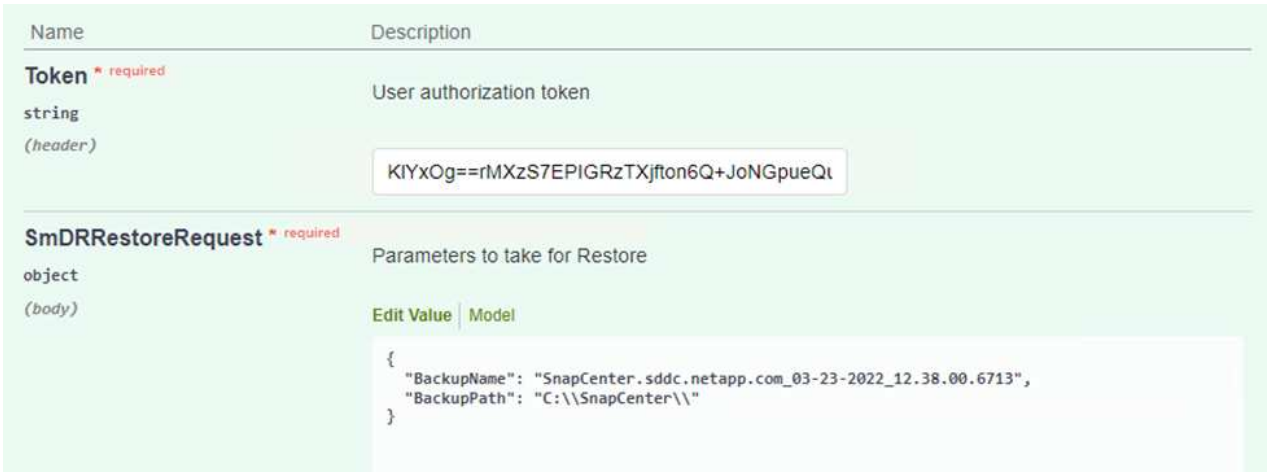
1. FSx 클러스터에서 SnapMirror 관계를 끊어 볼륨을 읽기/쓰기로 설정합니다.
2. 필요한 경우 CIFS 서버를 생성하고 복제된 볼륨의 연결 경로를 가리키는 CIFS 공유를 생성합니다.
3. xcopy를 사용하여 백업 파일을 보조 SnapCenter 시스템의 로컬 디렉토리에 복사합니다.
4. SnapCenter v4.6을 설치하세요.
5. SnapCenter 서버의 FQDN이 원본 서버와 동일한지 확인하세요. 이는 DB 복원이 성공하는 데 필요합니다.

복원 프로세스를 시작하려면 다음 단계를 완료하세요.

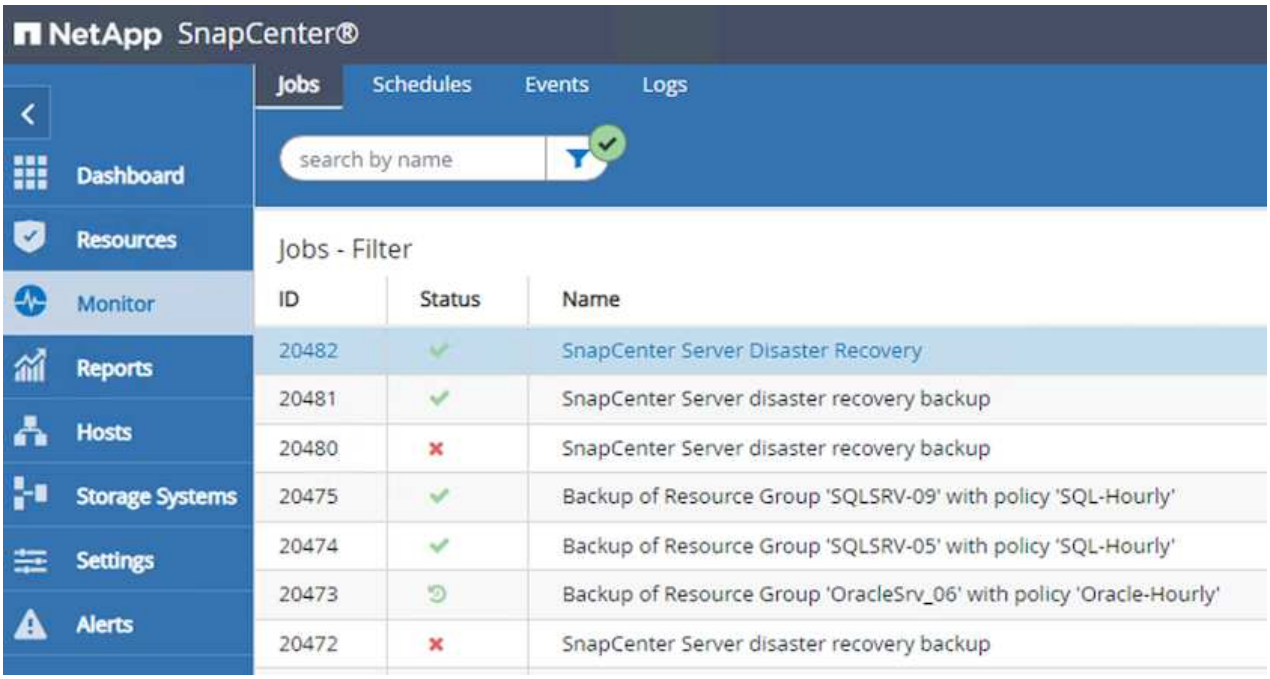
1. 보조 SnapCenter 서버의 Swagger API 웹 페이지로 이동하여 이전 지침에 따라 승인 토큰을 얻습니다.
2. Swagger 페이지의 재해 복구 섹션으로 이동하여 다음을 선택합니다. `/4.6/disasterrecovery/server/restore` 를 클릭하고 '시도해보기'를 클릭하세요.

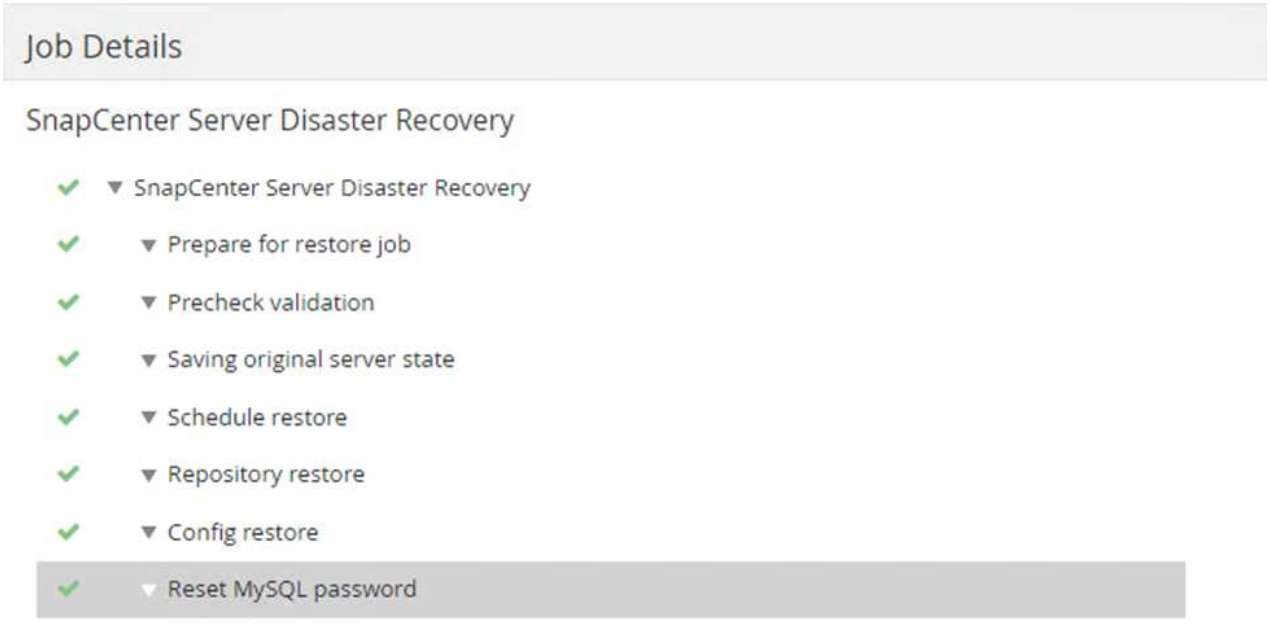


3. 권한 토큰을 붙여넣고, SmDRResterRequest 섹션에 백업 이름과 보조 SnapCenter 서버의 로컬 디렉토리 이름을 붙여넣습니다.



4. 복원 프로세스를 시작하려면 실행 버튼을 선택하세요.
5. SnapCenter 에서 모니터 섹션으로 이동하여 복원 작업의 진행 상황을 확인합니다.





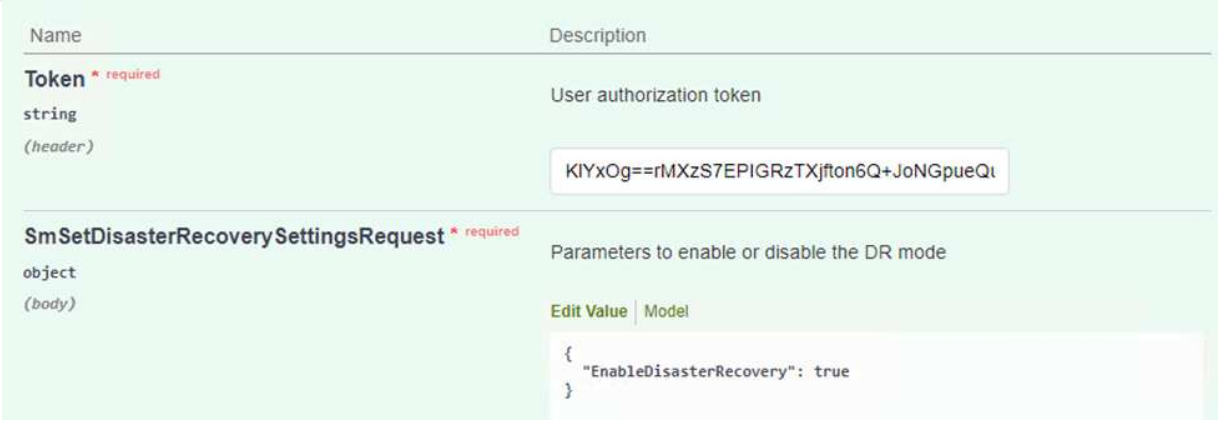
6. 보조 저장소에서 SQL Server 복원을 활성화하려면 SnapCenter 데이터베이스를 재해 복구 모드로 전환해야 합니다. 이 작업은 별도의 작업으로 수행되며 Swagger API 웹 페이지에서 시작됩니다.

   a. 재해 복구 섹션으로 이동하여 클릭하십시오. `/4.6/disasterrecovery/storage` .

   b. 사용자 인증 토큰을 붙여넣습니다.

   c. SmSetDisasterRecoverySettingsRequest 섹션에서 변경하세요. `EnableDisasterRecover` 에게 `true` .

   d. SQL Server에 대한 재해 복구 모드를 활성화하려면 실행을 클릭합니다.



추가 절차에 대한 의견을 참조하세요.

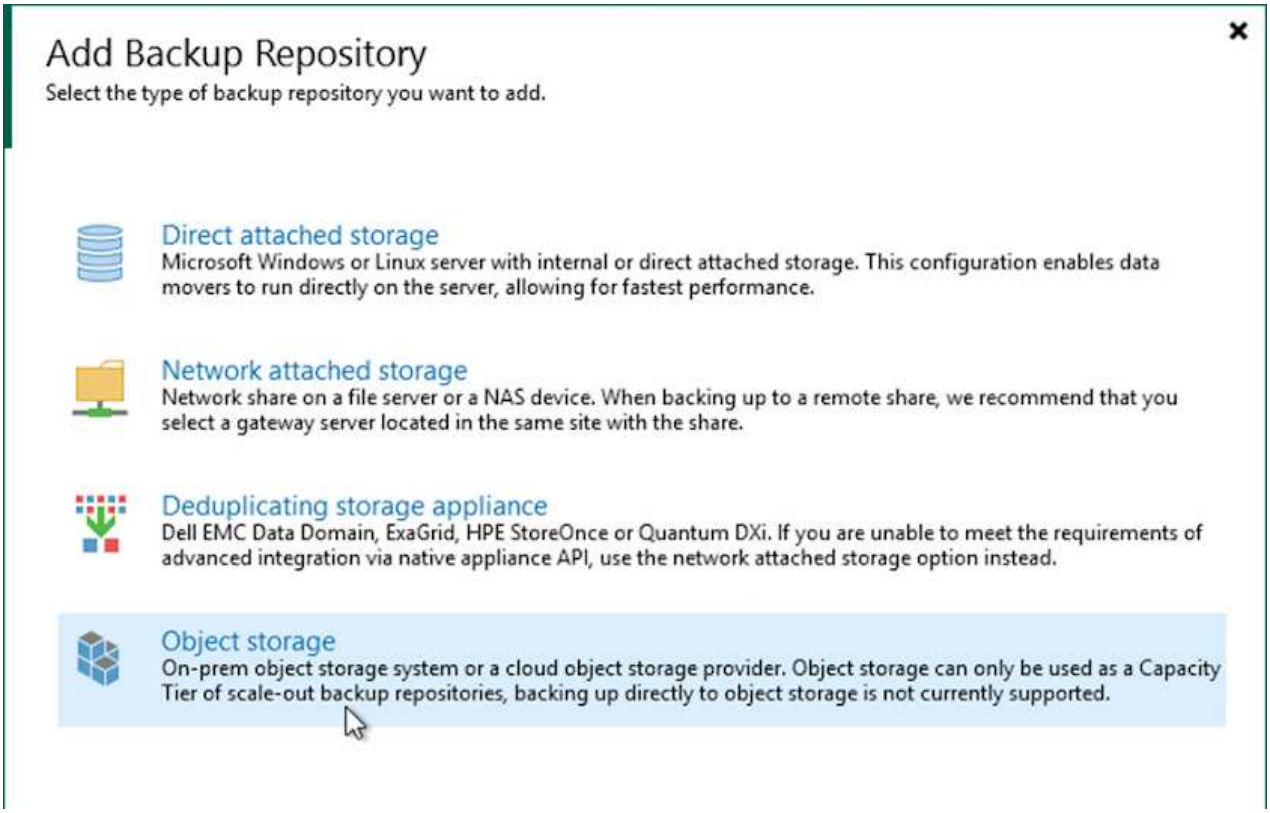
Veeam 전체 복원을 사용하여 애플리케이션 VM 복원

백업 저장소를 만들고 **S3**에서 백업을 가져옵니다.

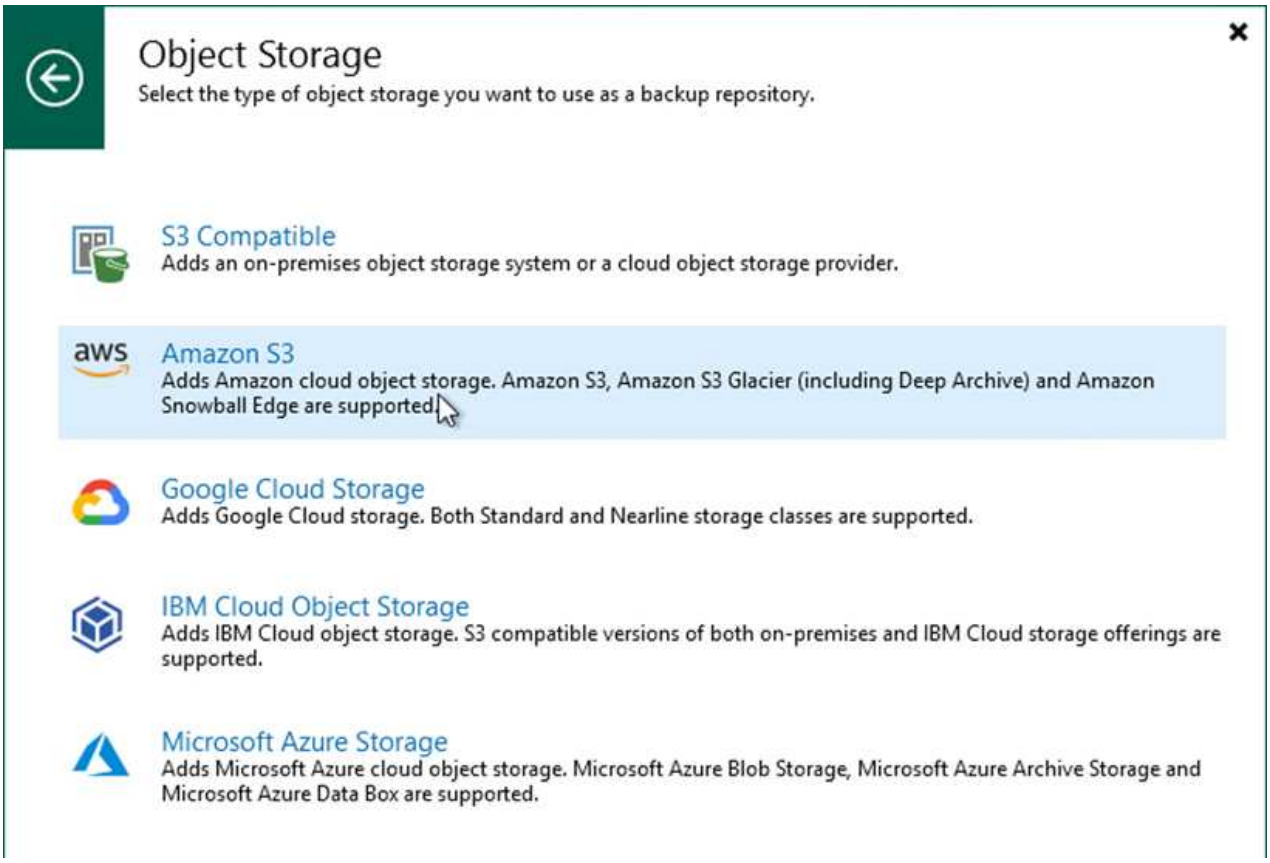
보조 Veeam 서버에서 S3 스토리지의 백업을 가져와 SQL Server 및 Oracle VM을 VMware Cloud 클러스터로 복원합니다.

온프레미스 확장형 백업 저장소에 속한 S3 개체에서 백업을 가져오려면 다음 단계를 완료하세요.

1. 백업 저장소로 가서 상단 메뉴에서 저장소 추가를 클릭하여 백업 저장소 추가 마법사를 시작합니다. 마법사의 첫 번째 페이지에서 백업 저장소 유형으로 개체 스토리지를 선택합니다.

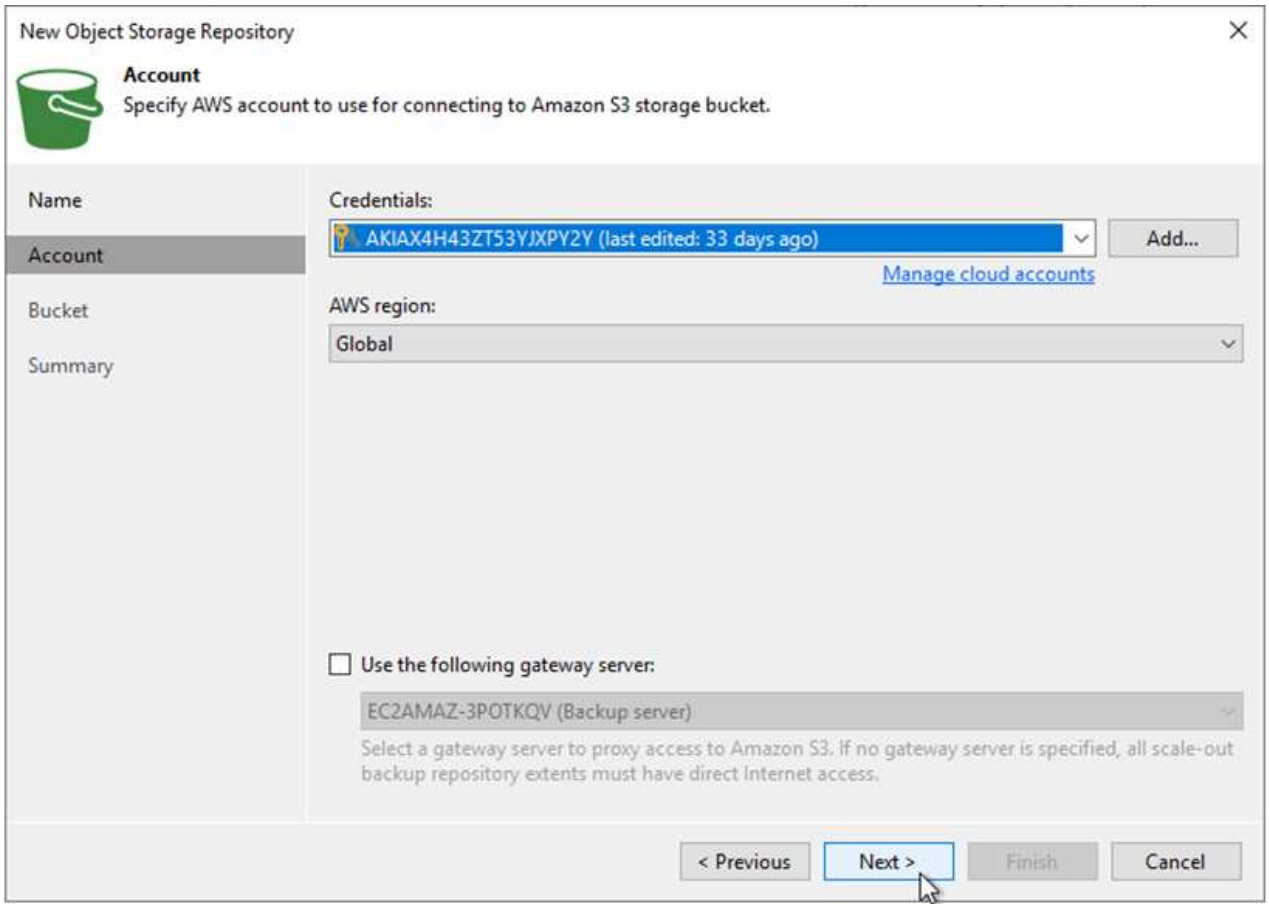


2. 개체 스토리지 유형으로 Amazon S3를 선택합니다.

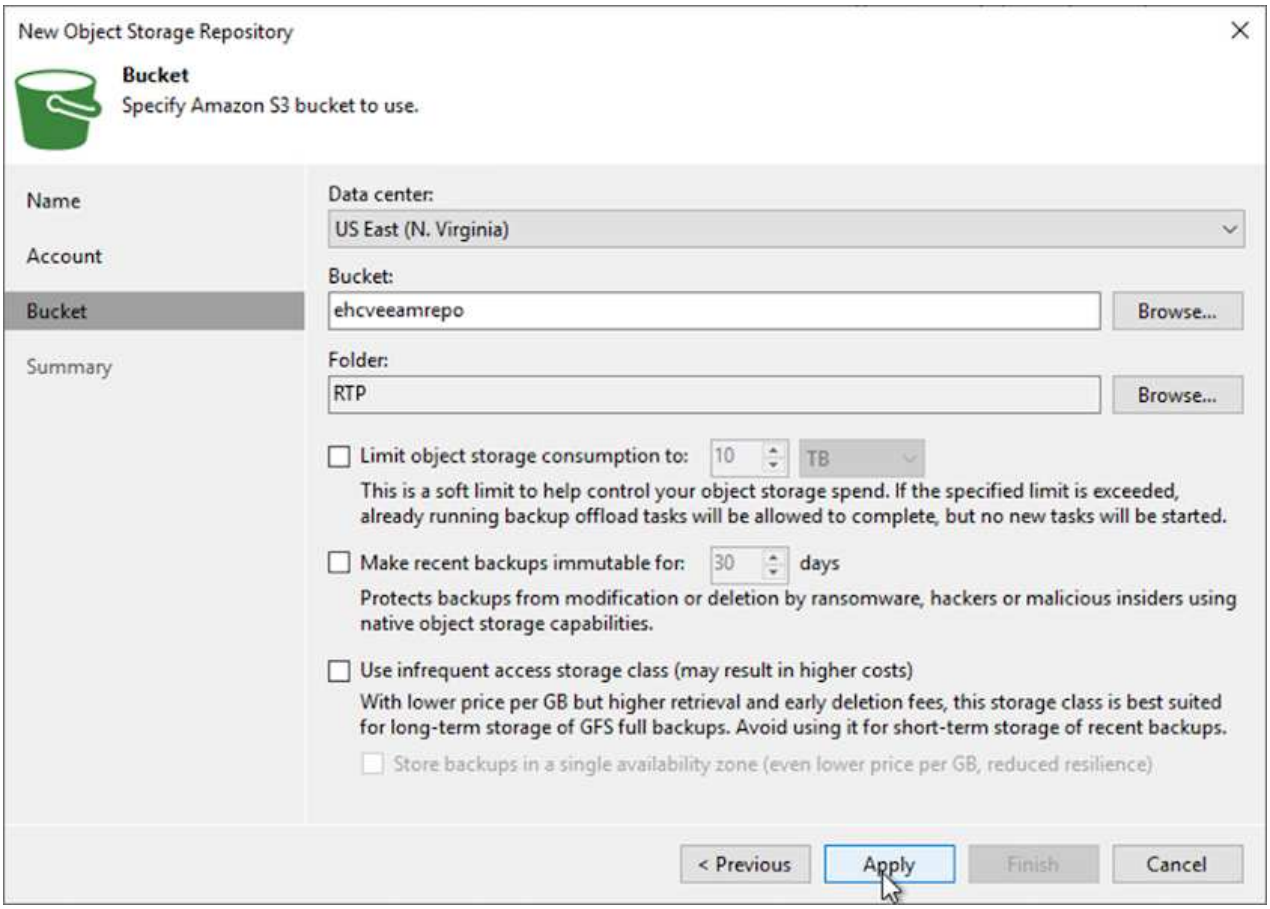


3. Amazon Cloud Storage Services 목록에서 Amazon S3를 선택합니다.

4. 드롭다운 목록에서 미리 입력한 자격 증명을 선택하거나 클라우드 스토리지 리소스에 액세스하기 위한 새 자격 증명을 추가하세요. 계속하려면 '다음'을 클릭하세요.



5. 버킷 페이지에서 데이터 센터, 버킷, 폴더 및 원하는 옵션을 입력합니다. 적용을 클릭하세요.

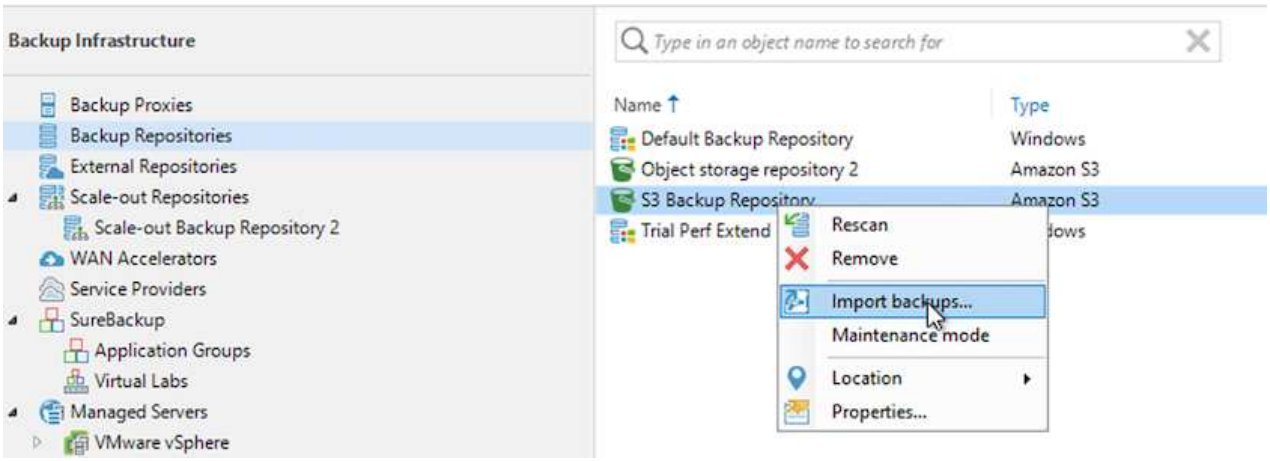


6. 마지막으로, 마침을 선택하여 프로세스를 완료하고 저장소를 추가합니다.

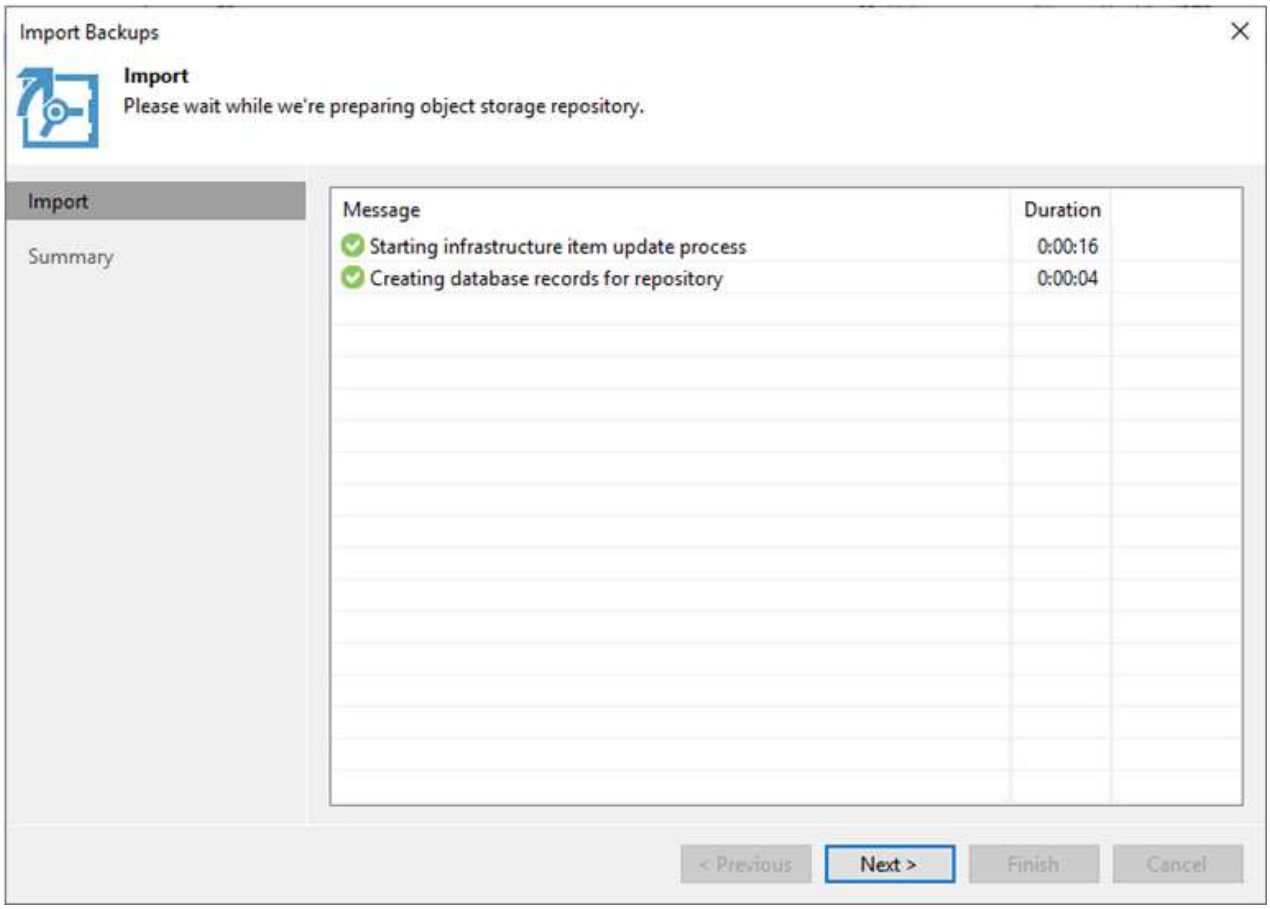
S3 개체 스토리지에서 백업 가져오기

이전 섹션에서 추가한 S3 저장소에서 백업을 가져오려면 다음 단계를 완료하세요.

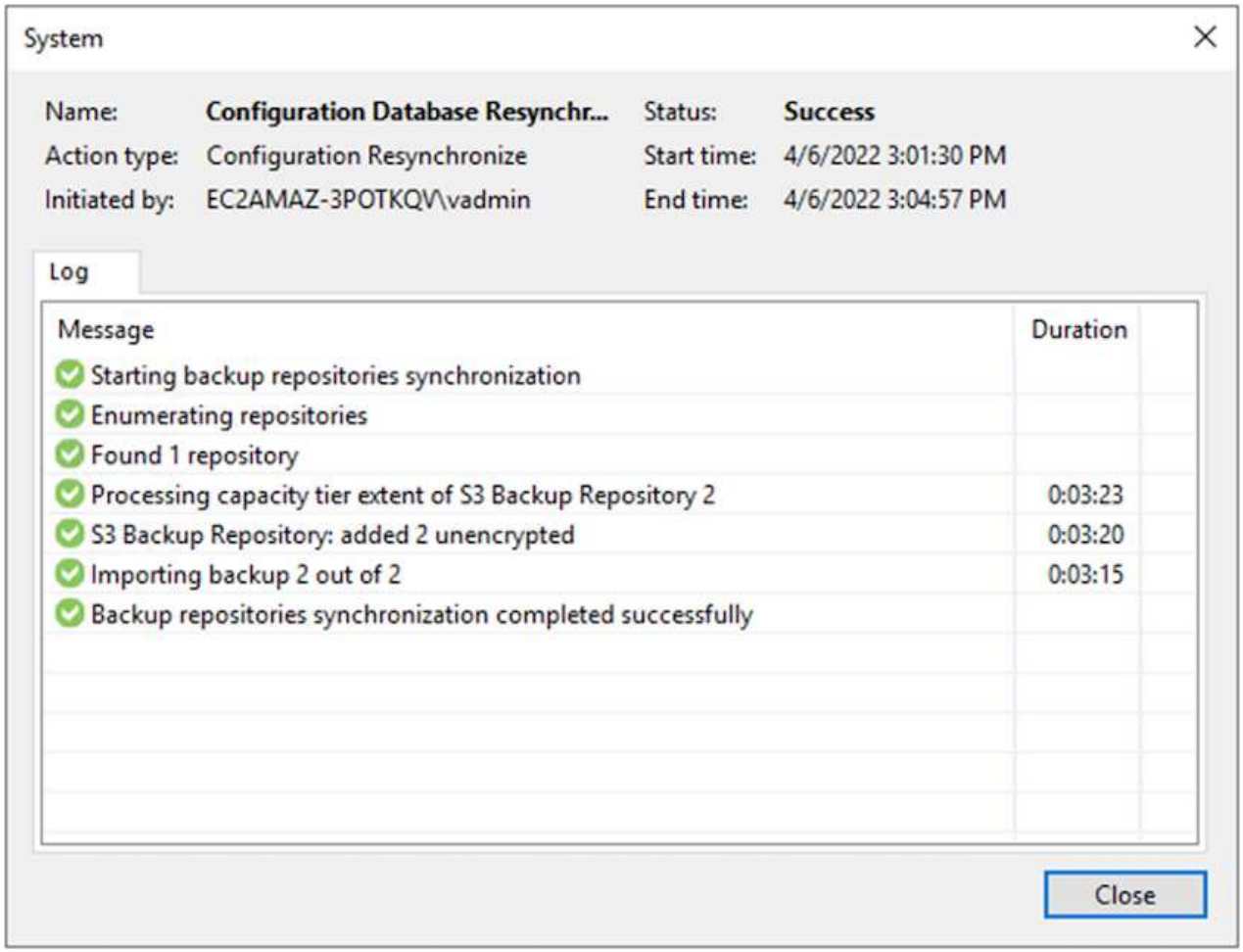
1. S3 백업 저장소에서 백업 가져오기를 선택하여 백업 가져오기 마법사를 시작합니다.



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

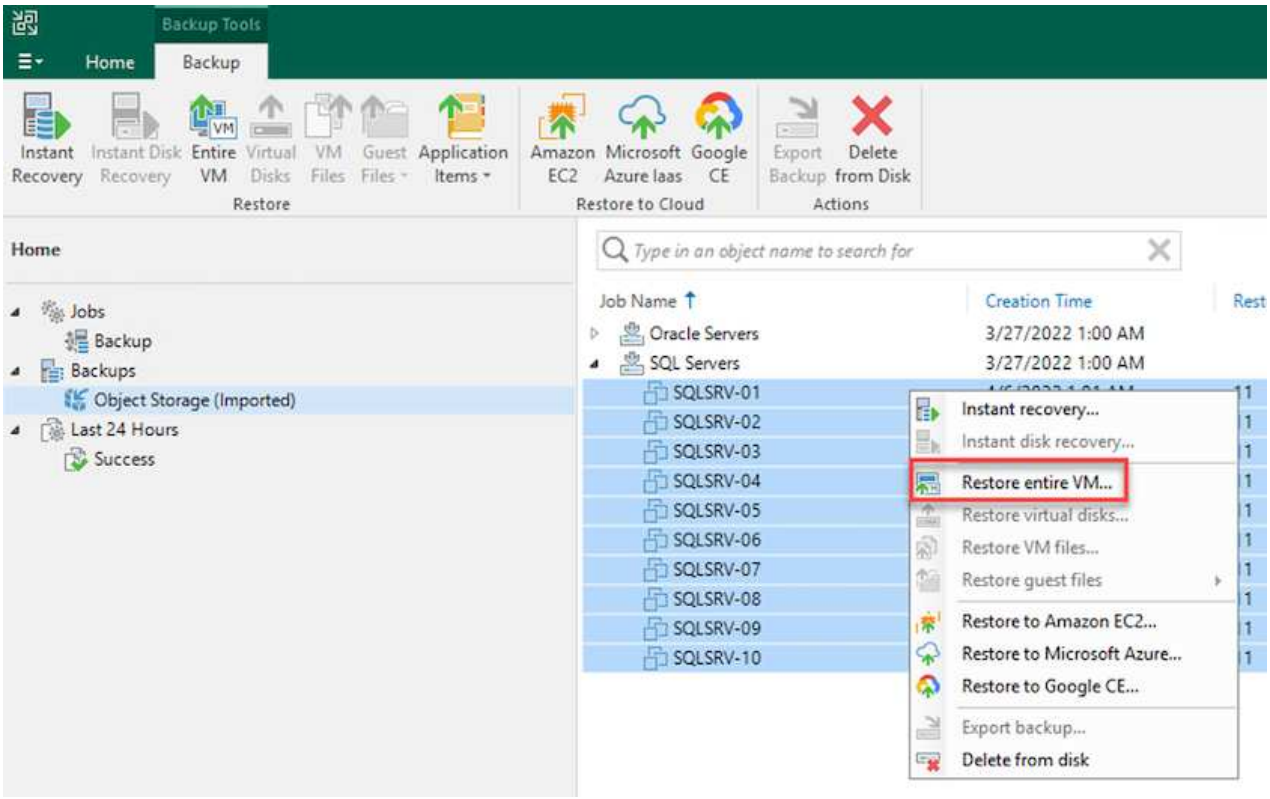


3. 가져오기가 완료되면 VM을 VMware Cloud 클러스터로 복원할 수 있습니다.

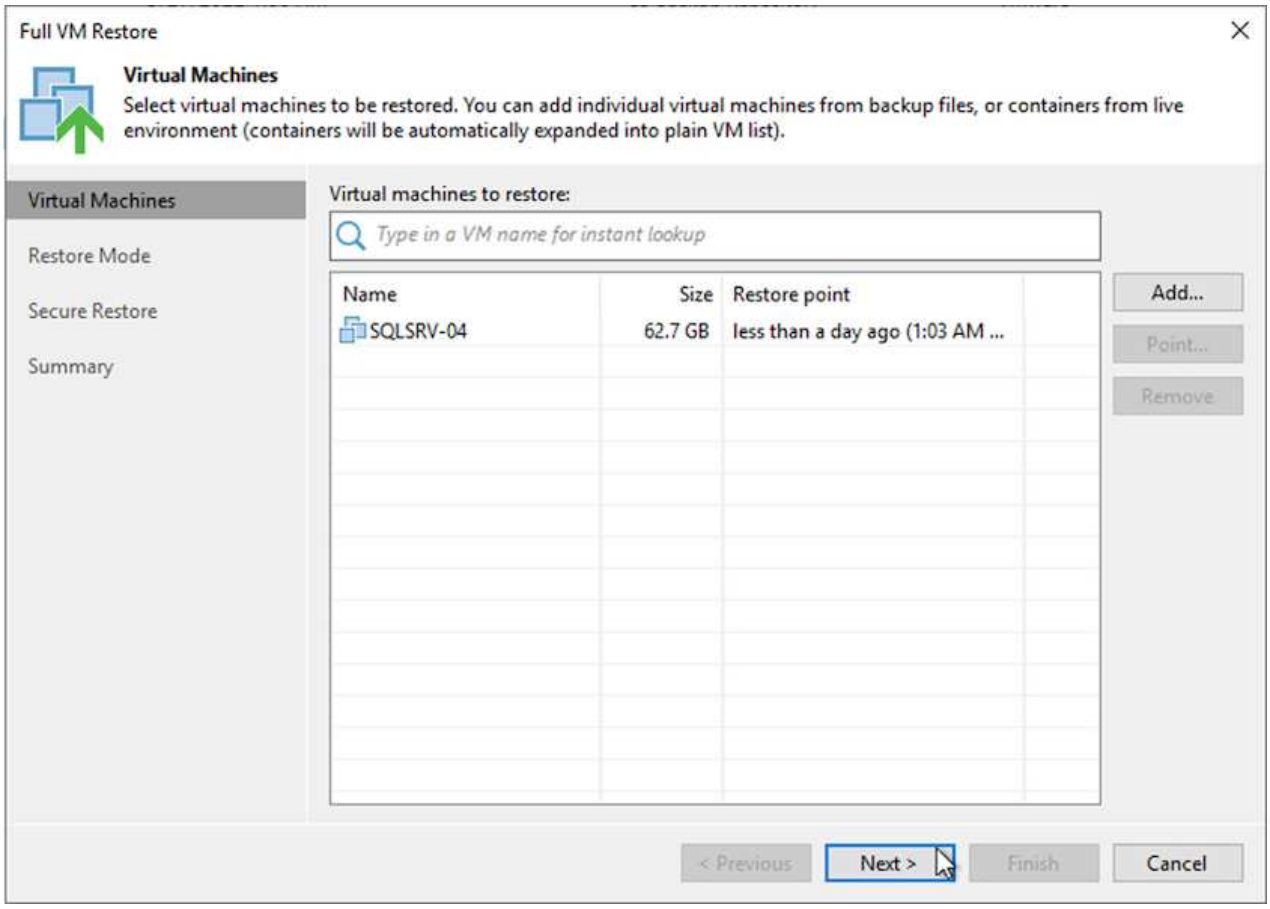

System
Name: Configuration Database Resynchr...
Status: Success
Action type: Configuration Resynchronize
Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vadmin
End time: 4/6/2022 3:04:57 PM
Log
Message
Duration
Starting backup repositories synchronization
Enumerating repositories
Found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

VMware Cloud on AWS 워크로드 도메인/클러스터에 SQL 및 Oracle 가상 머신을 복원하려면 다음 단계를 완료하세요.

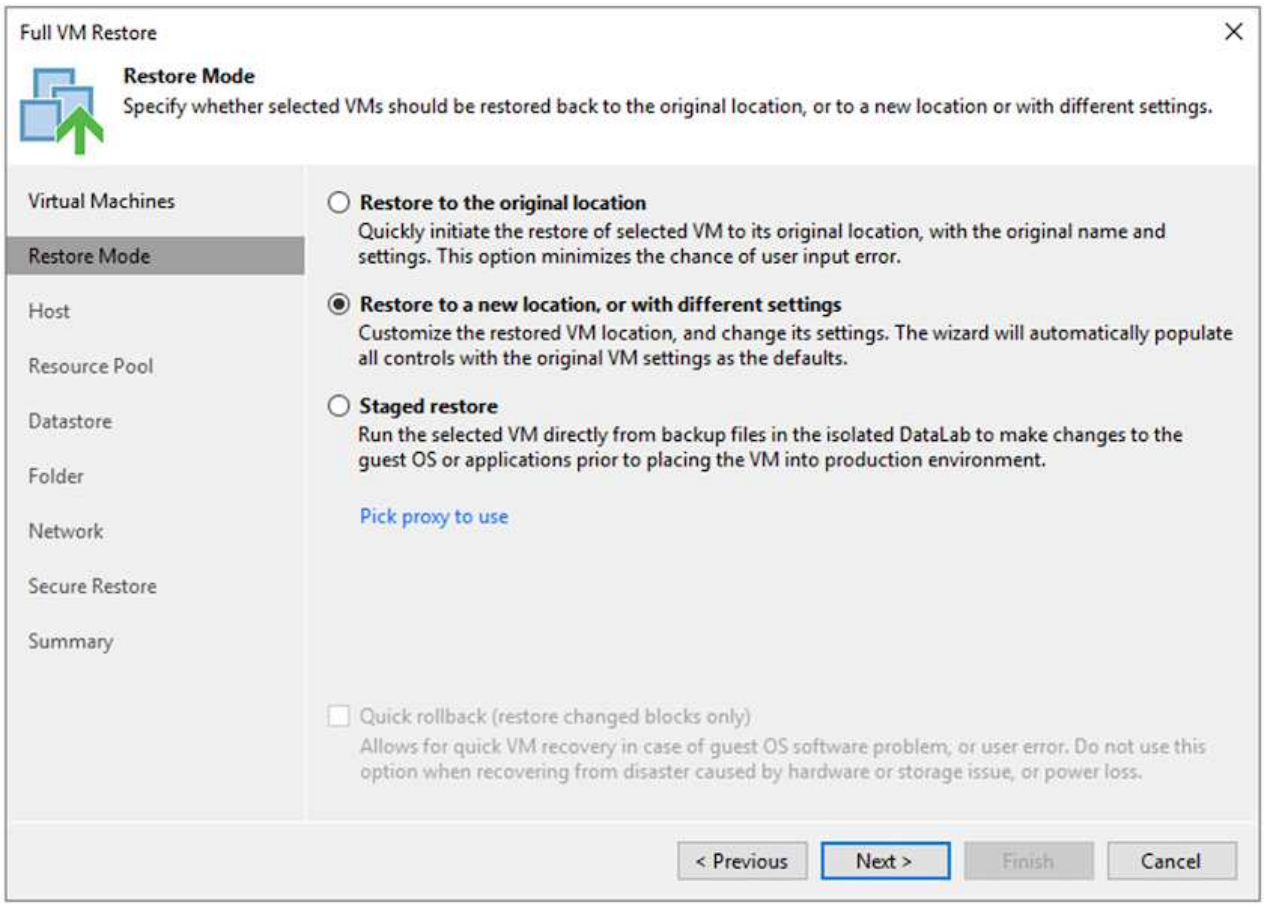
1. Veeam 홈페이지에서 가져온 백업이 포함된 개체 스토리지를 선택하고 복원할 VM을 선택한 다음 마우스 오른쪽 버튼을 클릭하고 전체 VM 복원을 선택합니다.



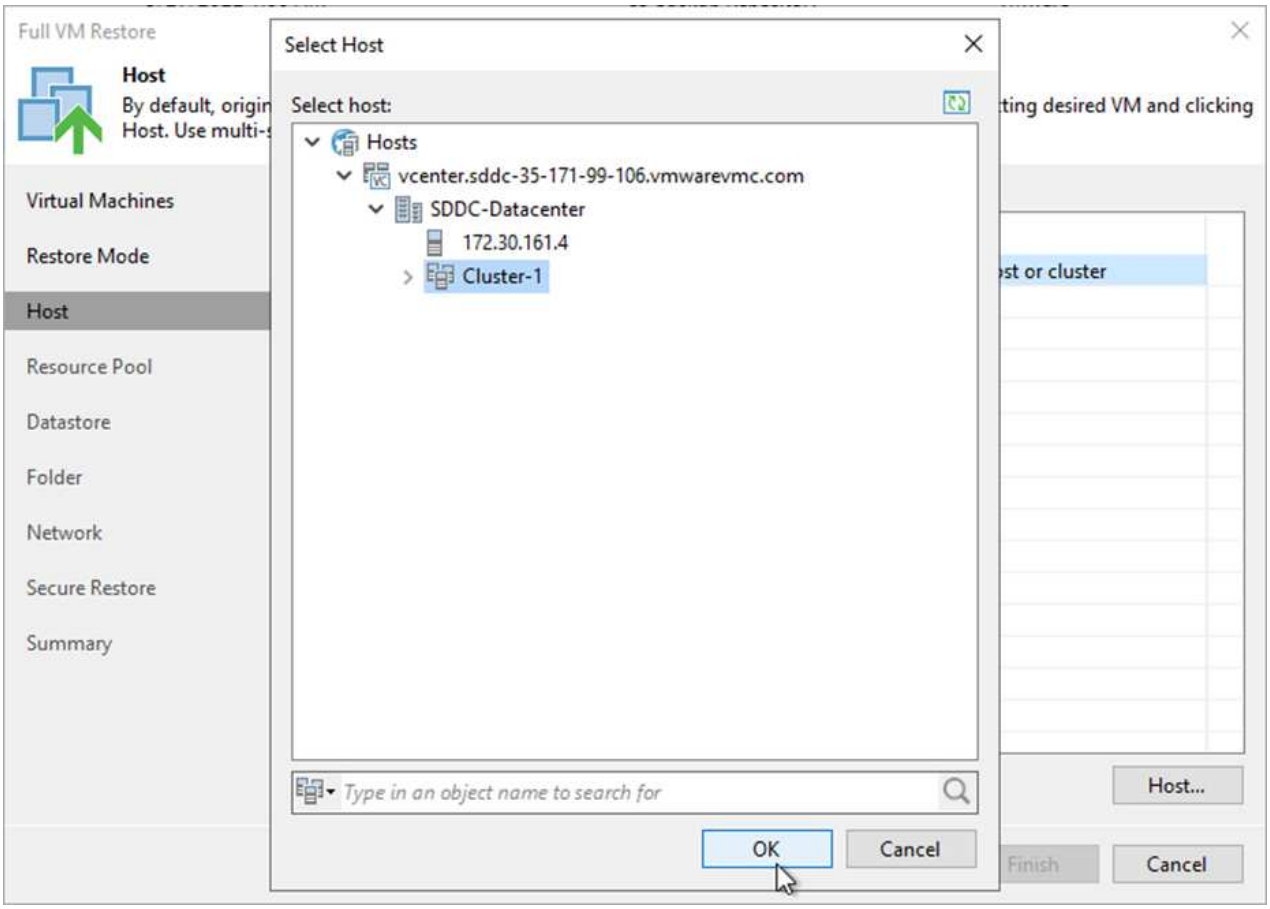
2. 전체 VM 복원 마법사의 첫 번째 페이지에서 원하는 경우 백업할 VM을 수정하고 다음을 선택합니다.



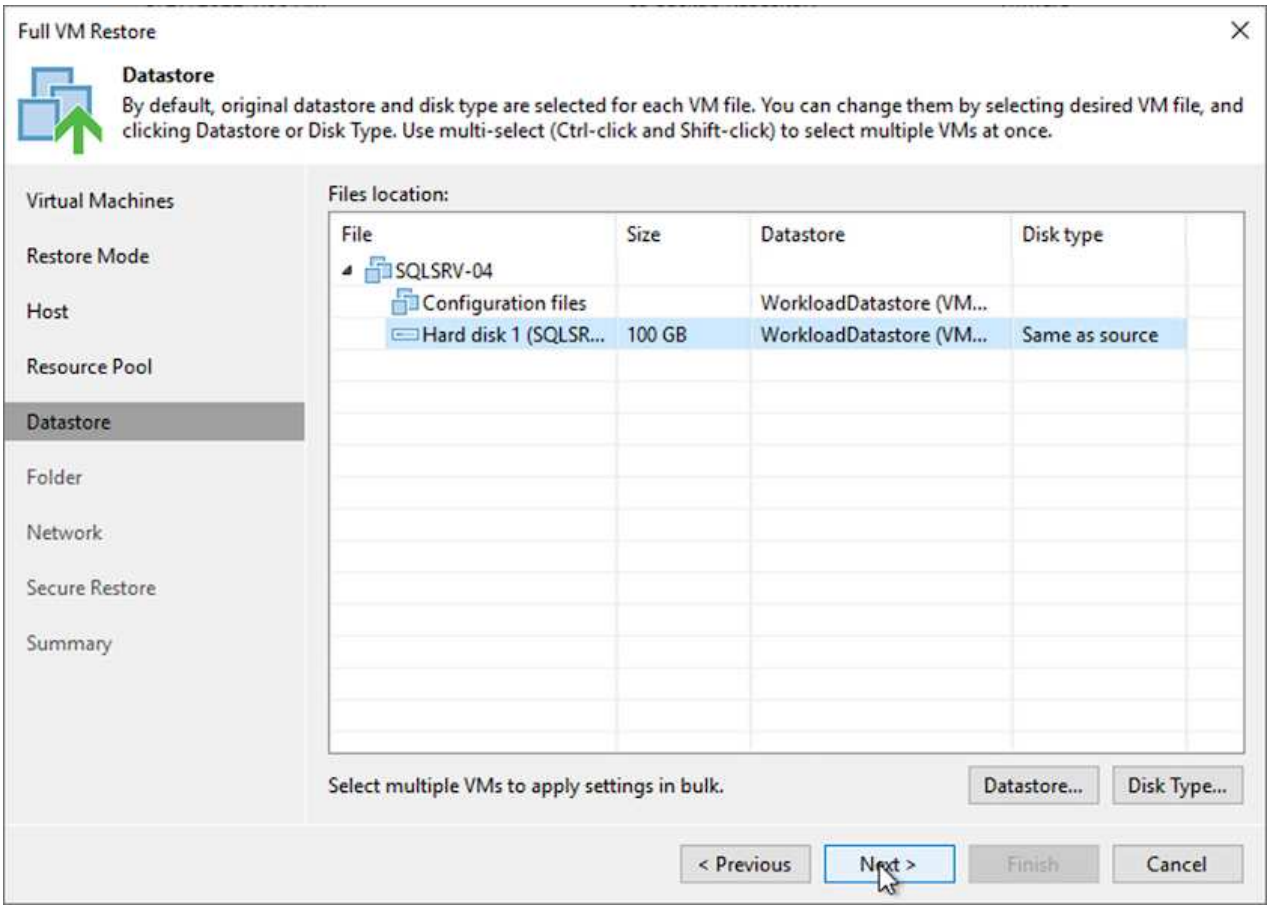
3. 복원 모드 페이지에서 새 위치로 복원 또는 다른 설정으로 복원을 선택합니다.



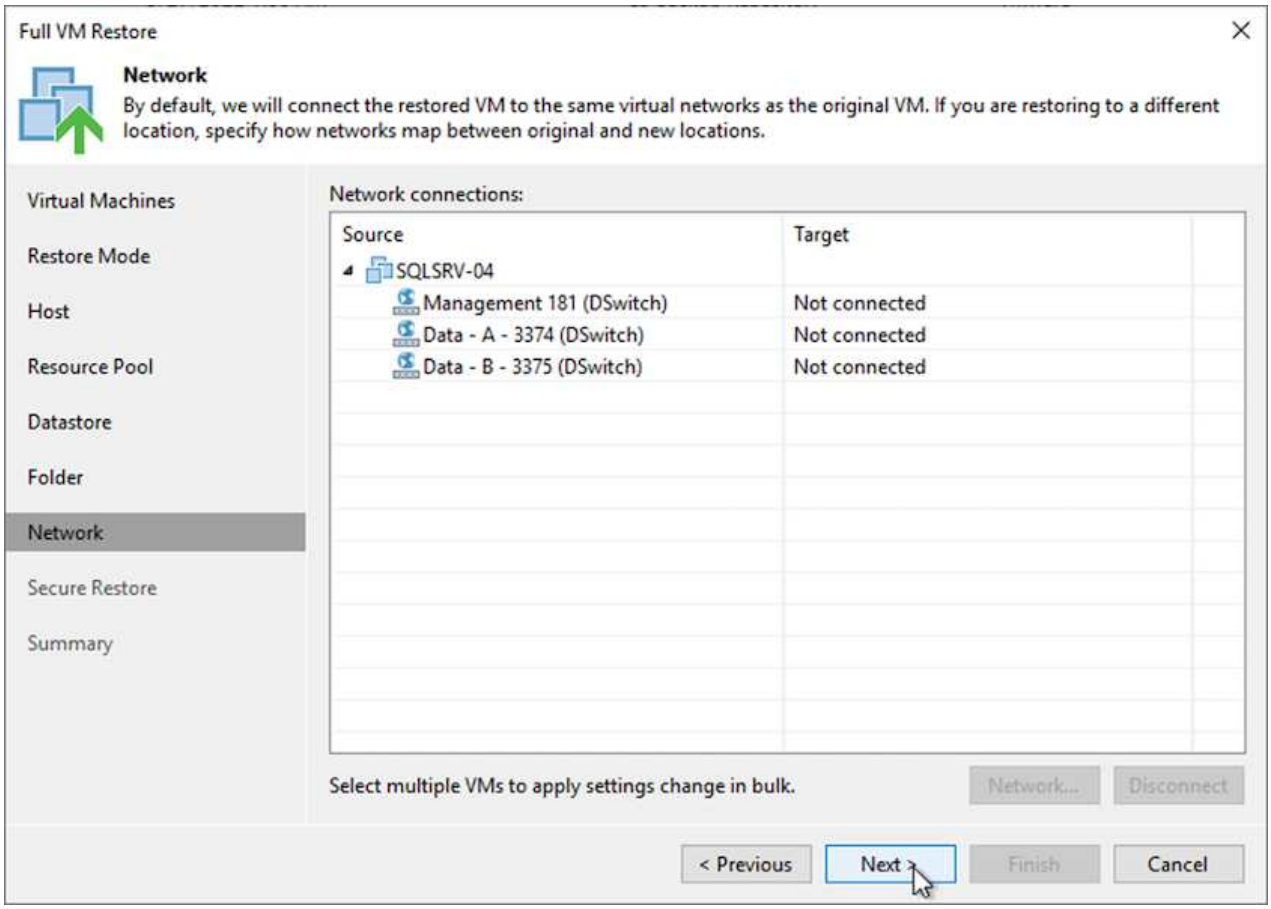
4. 호스트 페이지에서 VM을 복원할 대상 ESXi 호스트 또는 클러스터를 선택합니다.

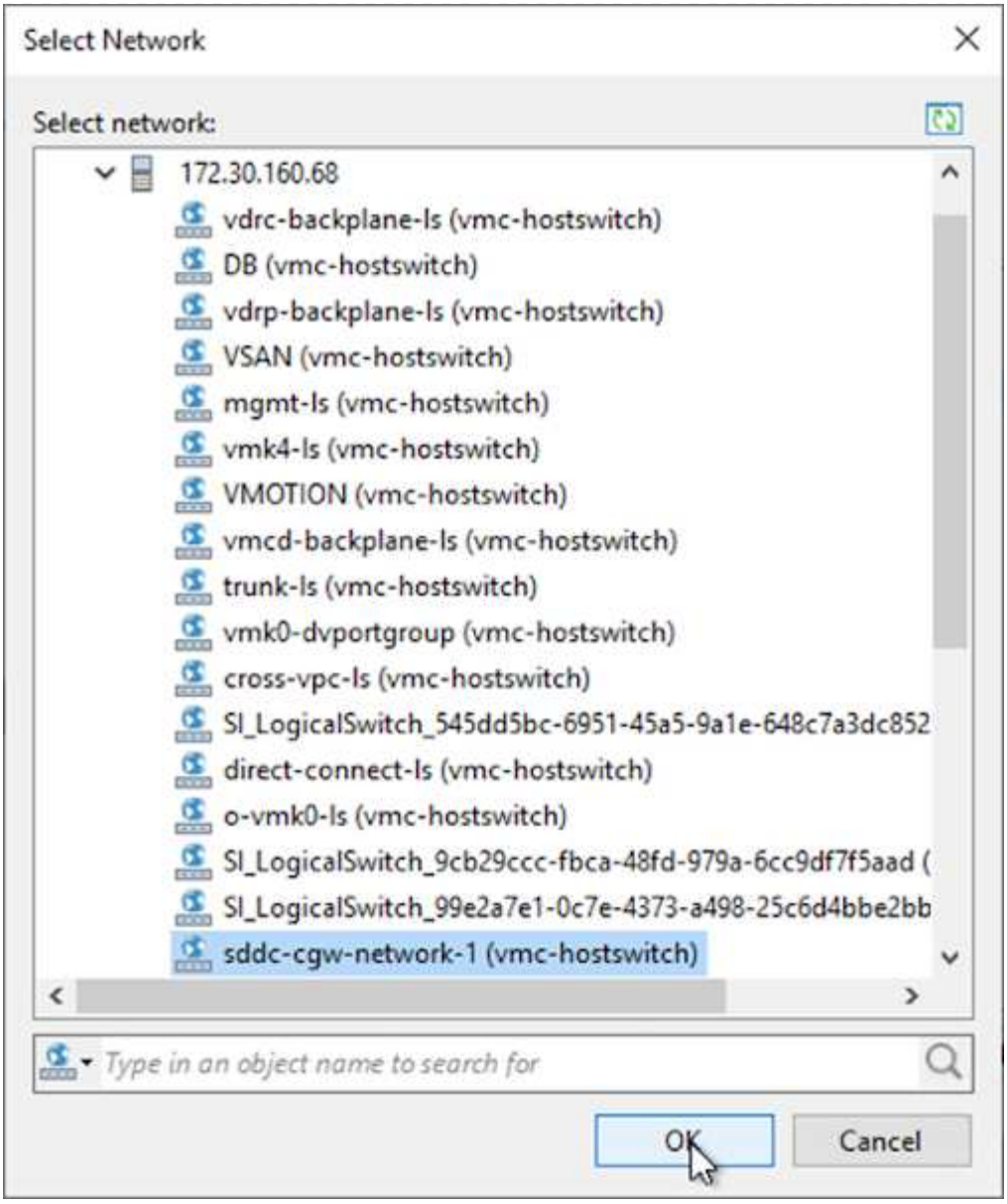


5. 데이터 저장소 페이지에서 구성 파일과 하드 디스크 모두에 대한 대상 데이터 저장소 위치를 선택합니다.



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


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



7. 복구된 VM에서 맬웨어를 검사할지 여부를 선택하고 요약 페이지를 검토한 후 마침을 클릭하여 복원을 시작합니다.

SQL Server 애플리케이션 데이터 복원

다음 프로세스에서는 온프레미스 사이트를 작동 불가능하게 만드는 재해가 발생한 경우 AWS의 VMware Cloud Services에서 SQL Server를 복구하는 방법에 대한 지침을 제공합니다.

복구 단계를 계속 진행하려면 다음 전제 조건이 모두 충족된 것으로 가정합니다.

1. Veeam Full Restore를 사용하여 Windows Server VM이 VMware Cloud SDDC로 복원되었습니다.
2. 보조 SnapCenter 서버가 설정되었고 SnapCenter 데이터베이스 복원 및 구성이 섹션에 설명된 단계를 사용하여 완료되었습니다."SnapCenter 백업 및 복원 프로세스 요약."

VM: SQL Server VM에 대한 복원 후 구성

VM 복원이 완료되면 SnapCenter 내에서 호스트 VM을 다시 검색하기 위해 네트워킹 및 기타 항목을 구성해야 합니다.

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

SnapCenter 플러그인이 현재 도메인과 다른 도메인 자격 증명을 사용하여 배포된 경우 SQL Server VM에서 Windows 서비스용 플러그인에 대한 로그온 계정을 변경해야 합니다. 로그온 계정을 변경한 후 SnapCenter SMCore, Windows용 플러그인, SQL Server용 플러그인 서비스를 다시 시작합니다.

SnapCenter 에서 복구된 VM을 자동으로 다시 검색하려면 FQDN이 온프레미스 SnapCenter 에 원래 추가된 VM과 동일해야 합니다.

SQL Server 복원을 위한 **FSx** 저장소 구성

SQL Server VM에 대한 재해 복구 복원 프로세스를 완료하려면 FSx 클러스터에서 기존 SnapMirror 관계를 해제하고 볼륨에 대한 액세스 권한을 부여해야 합니다. 그렇게 하려면 다음 단계를 완료하세요.

1. SQL Server 데이터베이스와 로그 볼륨에 대한 기존 SnapMirror 관계를 끊으려면 FSx CLI에서 다음 명령을 실행합니다.

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

2. SQL Server Windows VM의 iSCSI IQN을 포함하는 이니시에이터 그룹을 만들어 LUN에 대한 액세스 권한을 부여합니다.

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

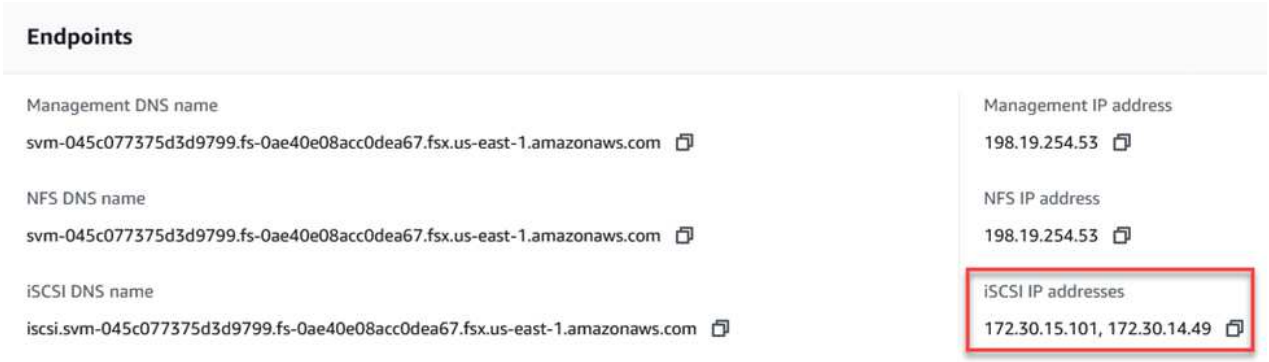
3. 마지막으로 방금 생성한 이니시에이터 그룹에 LUN을 매핑합니다.

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

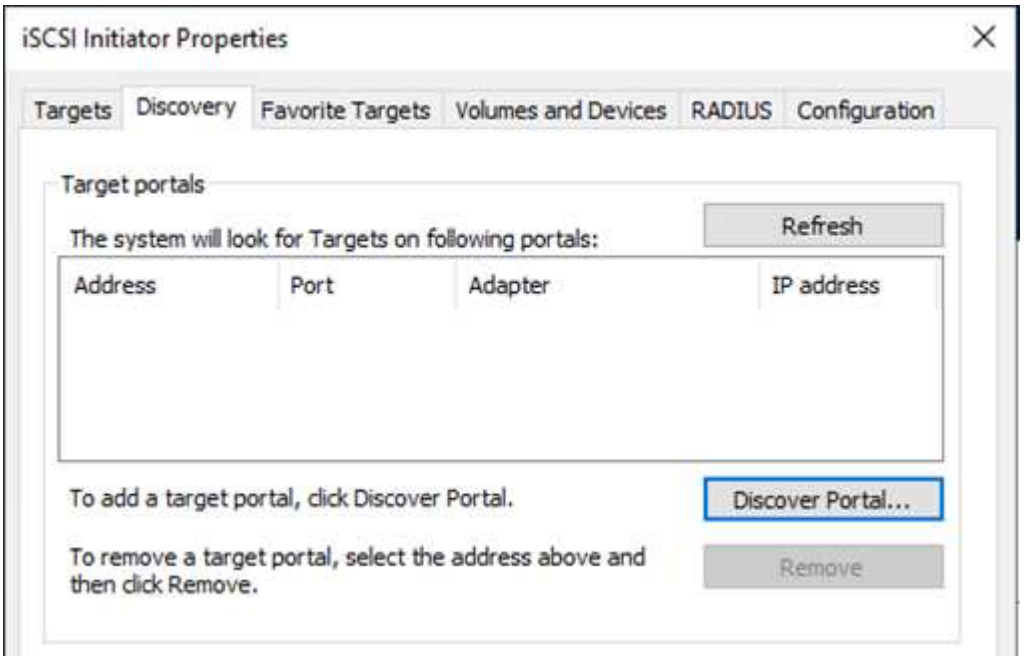
4. 경로 이름을 찾으려면 다음을 실행하세요. `lun show` 명령.

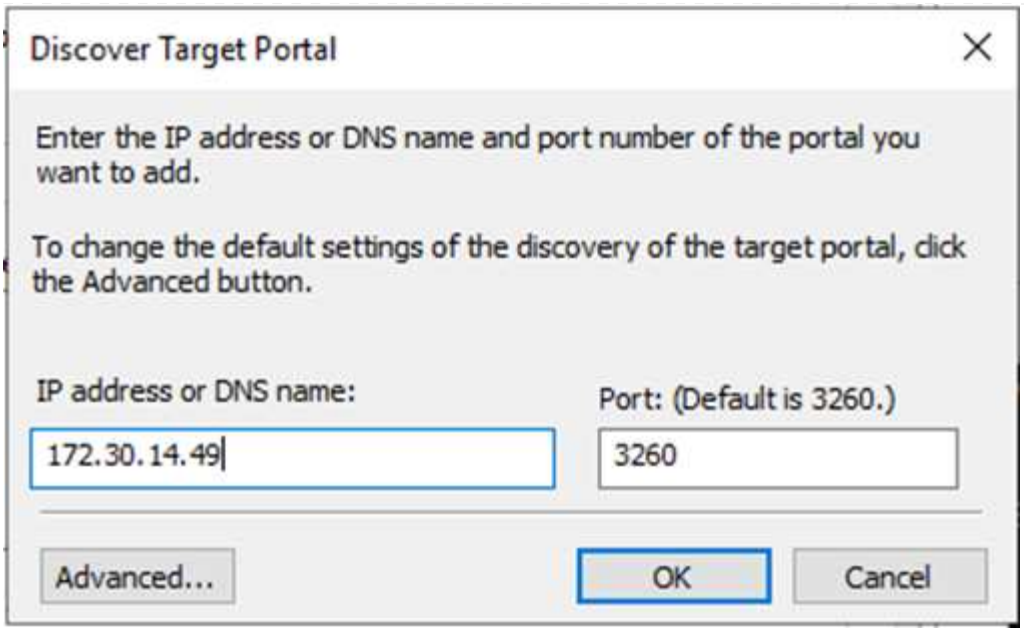
iSCSI 액세스를 위해 **Windows VM**을 설정하고 파일 시스템을 검색합니다**.**

1. SQL Server VM에서 FSx 인스턴스의 iSCSI 대상 인터페이스에 대한 연결이 설정된 VMware 포트 그룹에서 통신하도록 iSCSI 네트워크 어댑터를 설정합니다.
2. iSCSI 초기자 속성 유틸리티를 열고 검색, 즐겨찾는 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 해당 내용을 확인할 수 있습니다.

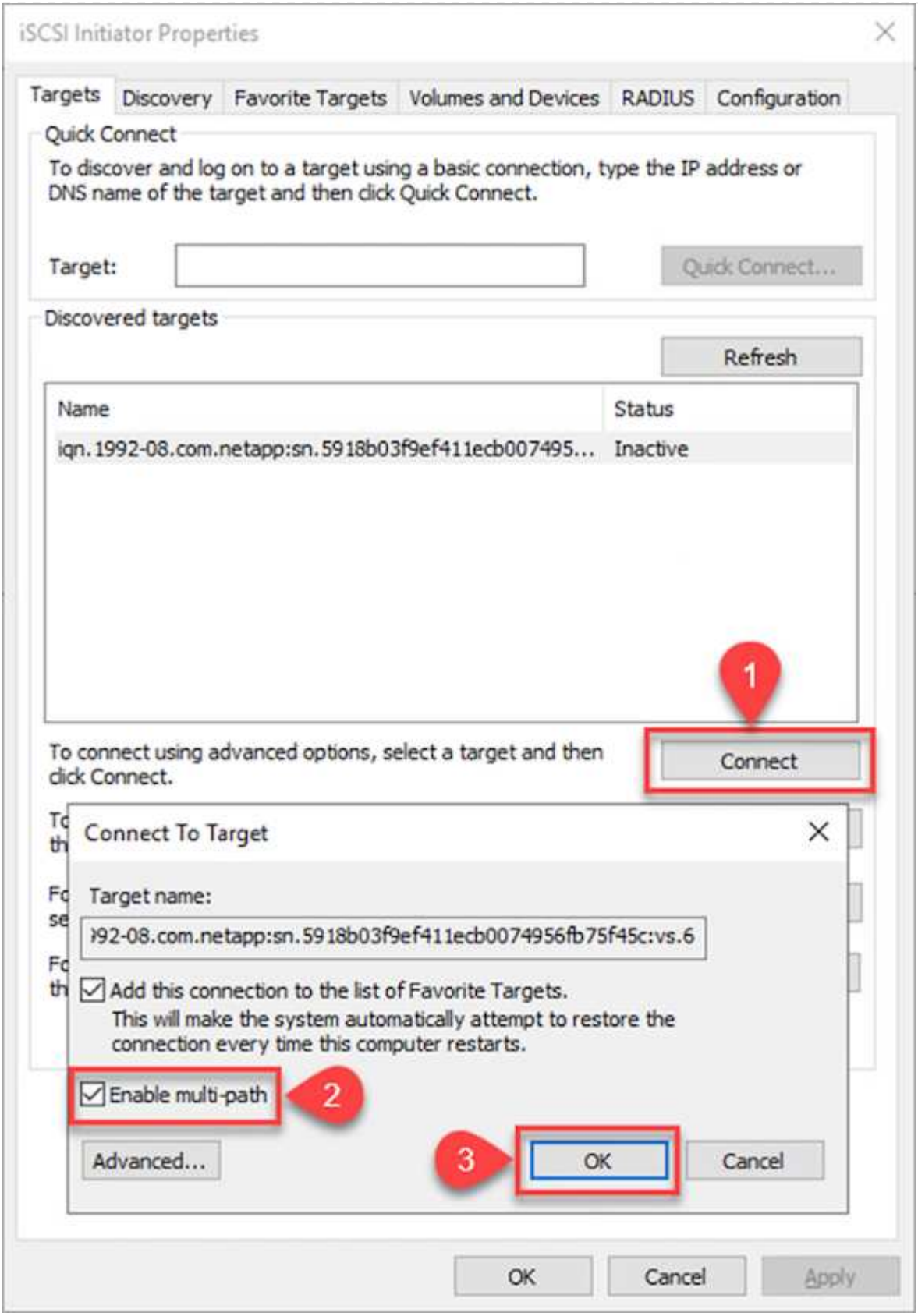


4. 검색 탭에서 검색 포털을 클릭하고 FSx iSCSI 대상의 IP 주소를 입력합니다.

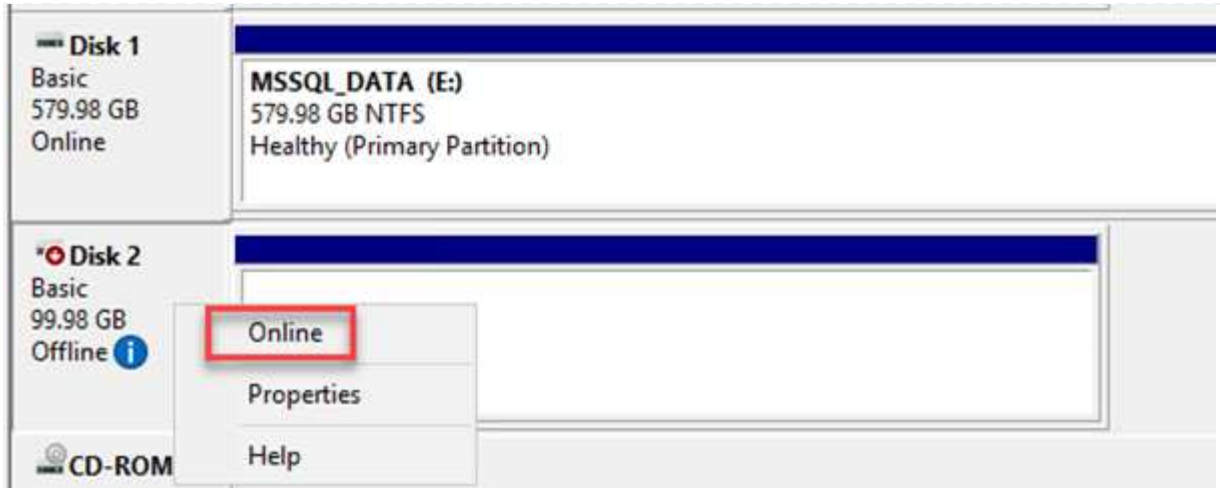




5. 대상 탭에서 연결을 클릭하고 구성에 적합한 경우 다중 경로 사용을 선택한 다음 확인을 클릭하여 대상에 연결합니다.

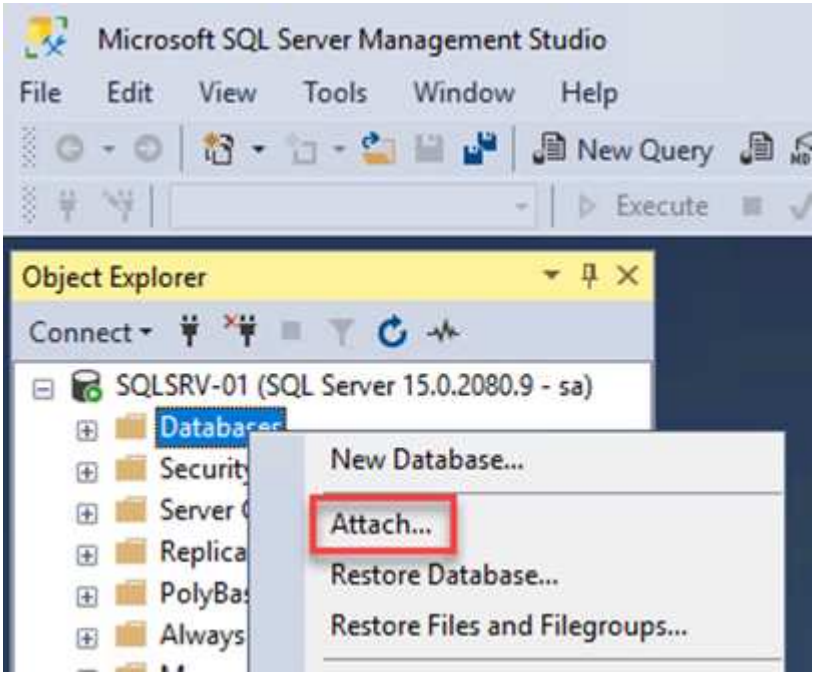


6. 컴퓨터 관리 유틸리티를 열고 디스크를 온라인으로 전환합니다. 이전에 사용하던 것과 동일한 드라이브 문자가 유지되는지 확인하세요.

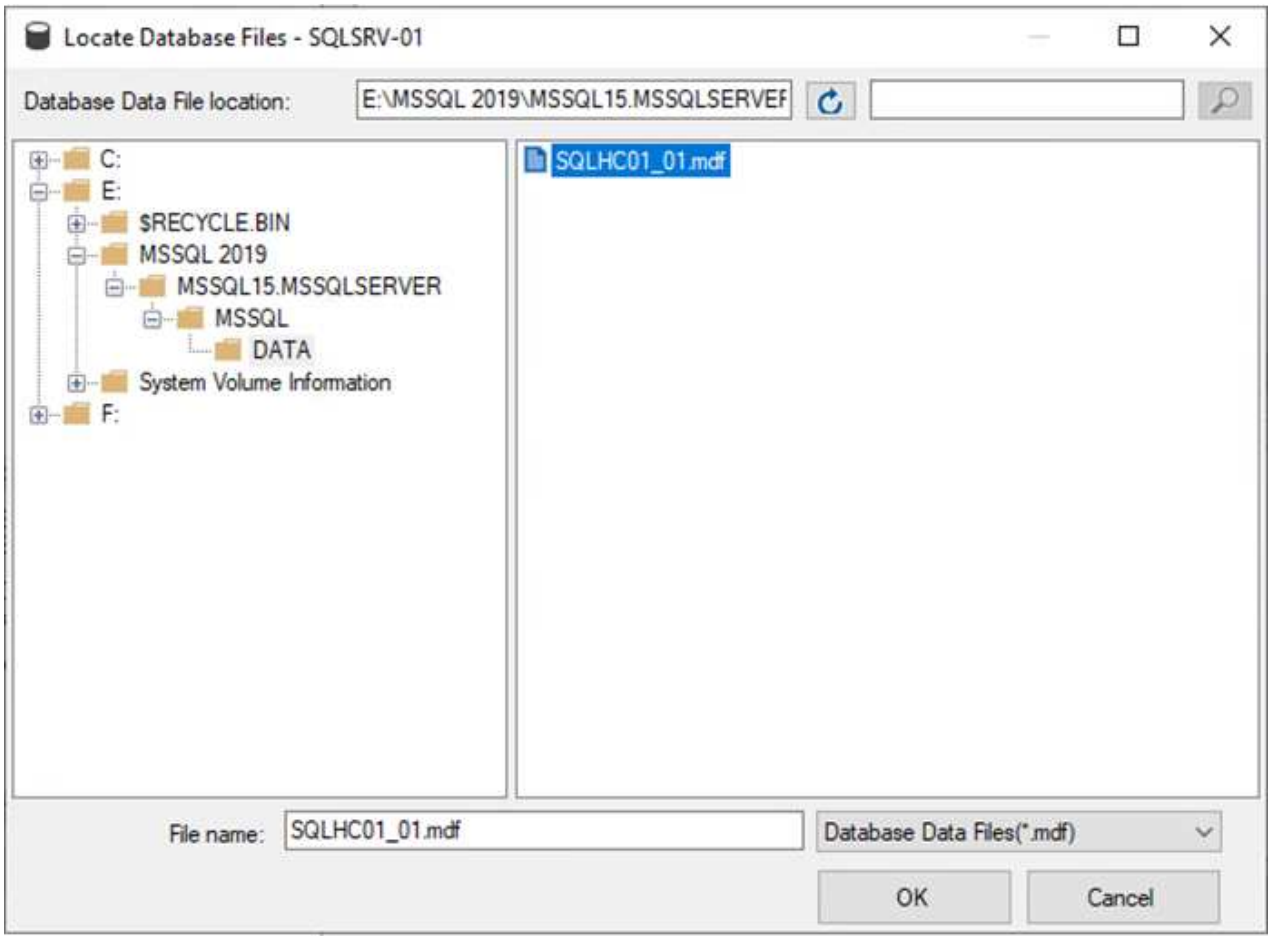

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

SQL Server 데이터베이스 연결

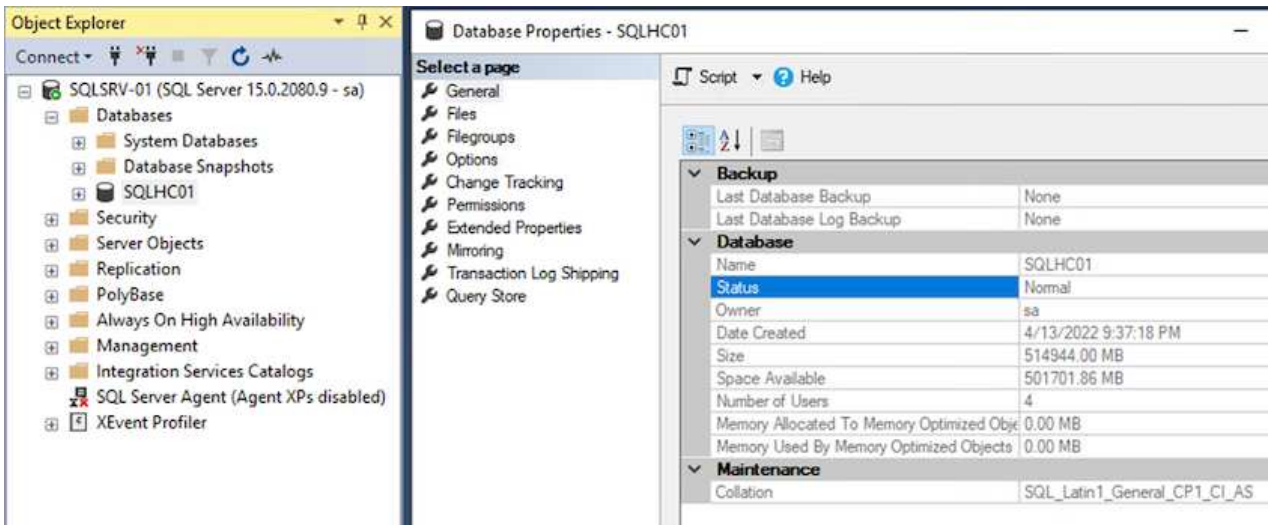
1. SQL Server VM에서 Microsoft SQL Server Management Studio를 열고 연결을 선택하여 데이터베이스에 연결하는 프로세스를 시작합니다.



2. 추가를 클릭하고 SQL Server 기본 데이터베이스 파일이 있는 폴더로 이동하여 해당 파일을 선택한 다음 확인을 클릭합니다.



3. 거래 로그가 별도 드라이브에 있는 경우 거래 로그가 포함된 폴더를 선택하세요.
4. 완료되면 확인을 클릭하여 데이터베이스를 연결합니다.

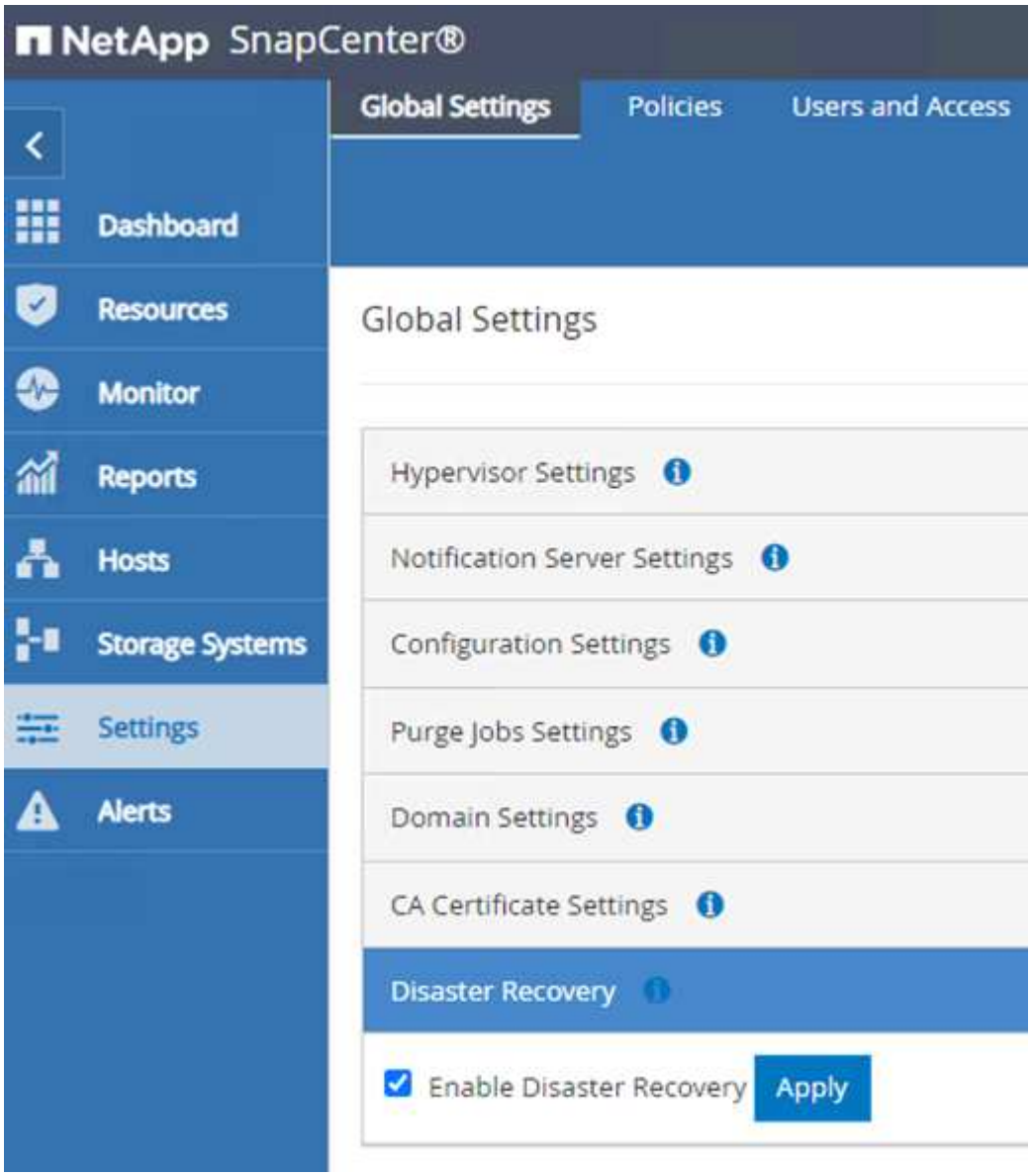


SQL Server 플러그인과 **SnapCenter** 통신 확인

SnapCenter 데이터베이스가 이전 상태로 복원되면 SQL Server 호스트를 자동으로 다시 검색합니다. 이것이 제대로 작동하려면 다음 전제 조건을 염두에 두십시오.

- SnapCenter 재해 복구 모드로 전환해야 합니다. 이 작업은 Swagger API를 통해 수행하거나 재해 복구 아래의 글로벌 설정을 통해 수행할 수 있습니다.
- SQL Server의 FQDN은 온프레미스 데이터 센터에서 실행 중인 인스턴스와 동일해야 합니다.
- 원래의 SnapMirror 관계는 끊어져야 합니다.
- 데이터베이스가 포함된 LUN을 SQL Server 인스턴스에 마운트하고 데이터베이스를 연결해야 합니다.

SnapCenter 재해 복구 모드에 있는지 확인하려면 SnapCenter 웹 클라이언트에서 설정으로 이동하세요. 글로벌 설정 탭으로 이동한 다음 재해 복구를 클릭합니다. 재해 복구 사용 확인란이 활성화되어 있는지 확인하세요.



Oracle 애플리케이션 데이터 복원

다음 프로세스에서는 온프레미스 사이트를 작동 불가능하게 만드는 재해가 발생한 경우 AWS의 VMware Cloud Services에서 Oracle 애플리케이션 데이터를 복구하는 방법에 대한 지침을 제공합니다.

복구 단계를 계속하려면 다음 전제 조건을 완료하세요.

1. Oracle Linux 서버 VM은 Veeam Full Restore를 사용하여 VMware Cloud SDDC로 복원되었습니다.
2. 보조 SnapCenter 서버가 설정되었고 SnapCenter 데이터베이스와 구성 파일이 이 섹션에 설명된 단계를 사용하여 복원되었습니다."SnapCenter 백업 및 복원 프로세스 요약."

Oracle 복원을 위한 FSx 구성 – SnapMirror 관계 끊기

FSx ONTAP 인스턴스에 호스팅된 보조 스토리지 볼륨을 Oracle 서버에서 액세스할 수 있게 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::>
```

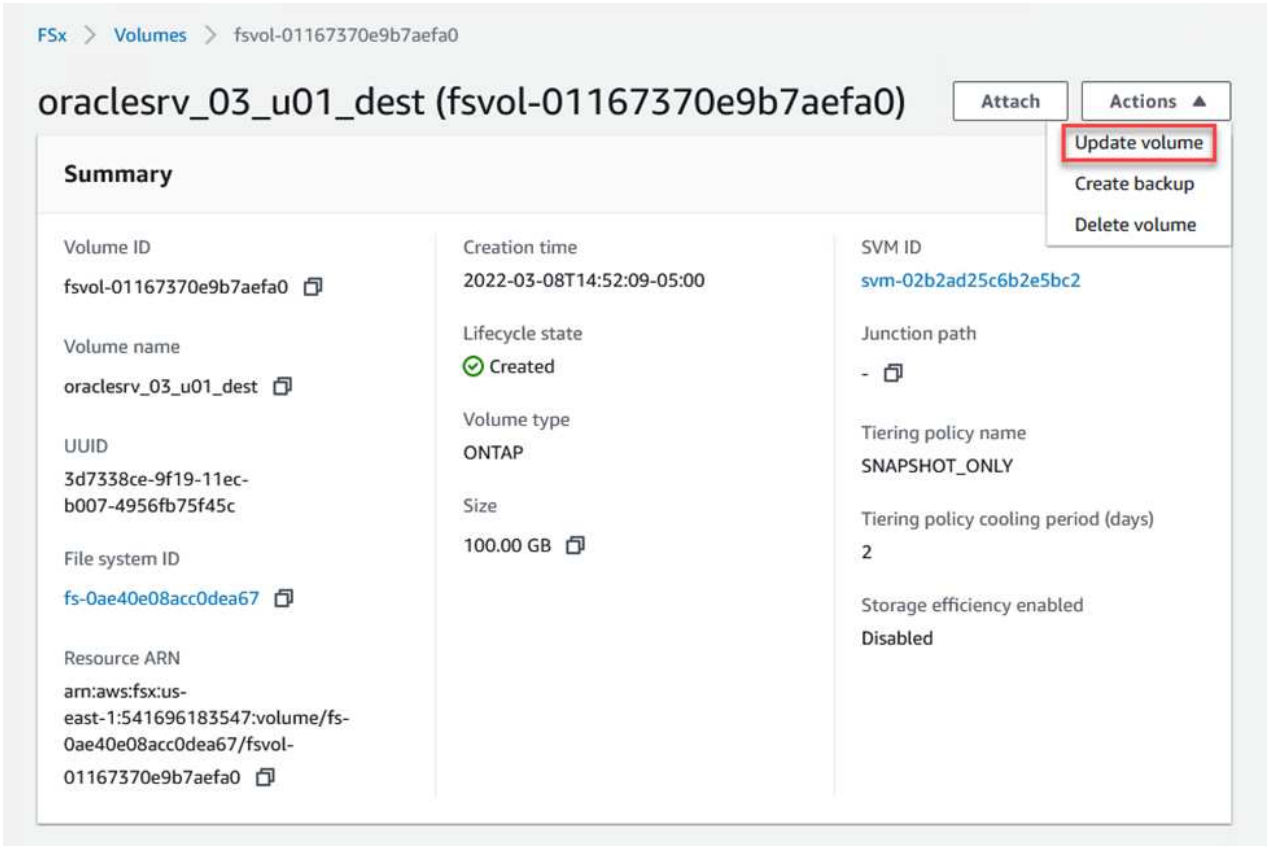
2. 다음 명령을 실행하여 기존 SnapMirror 관계를 해제합니다.

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

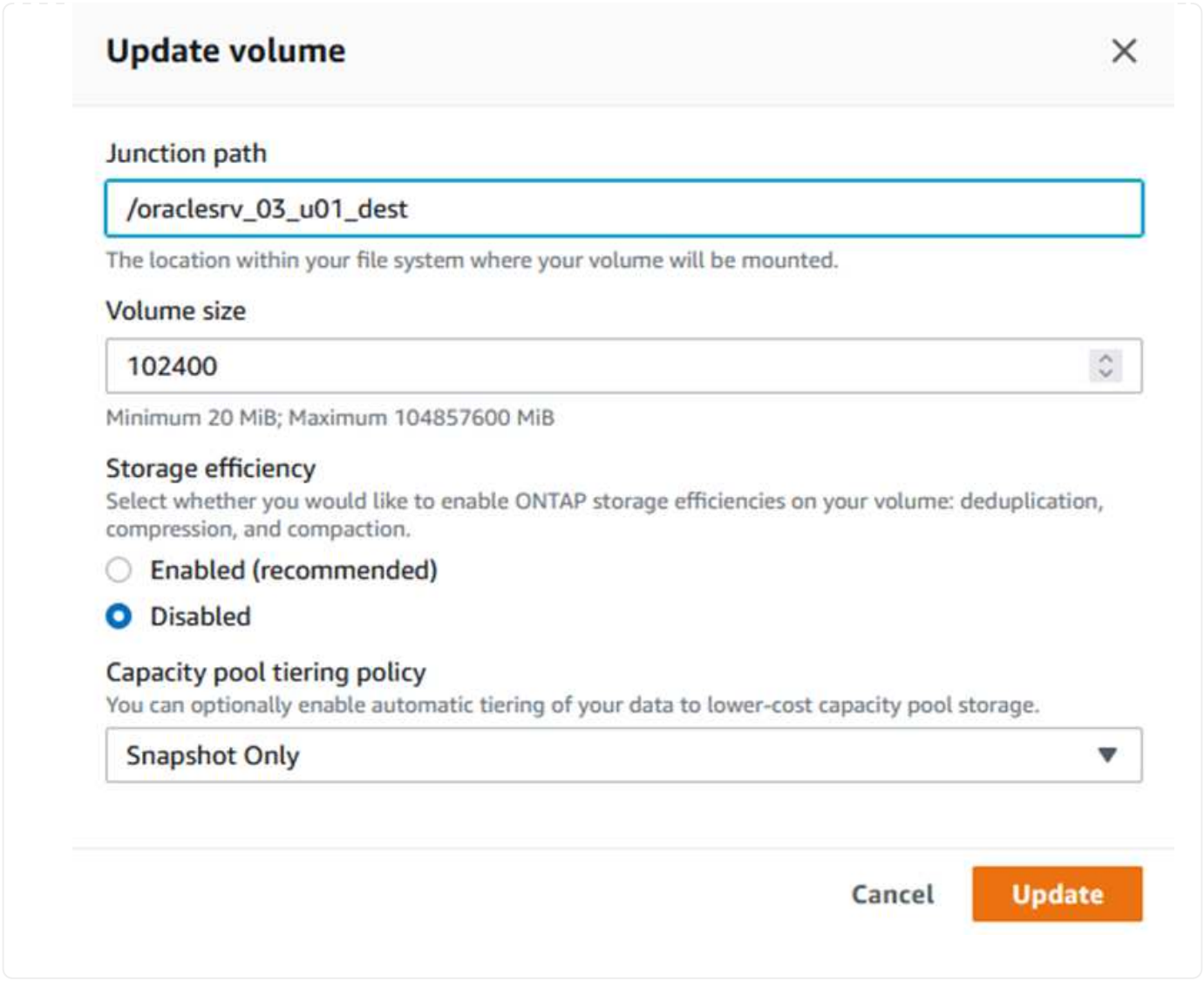
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

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.



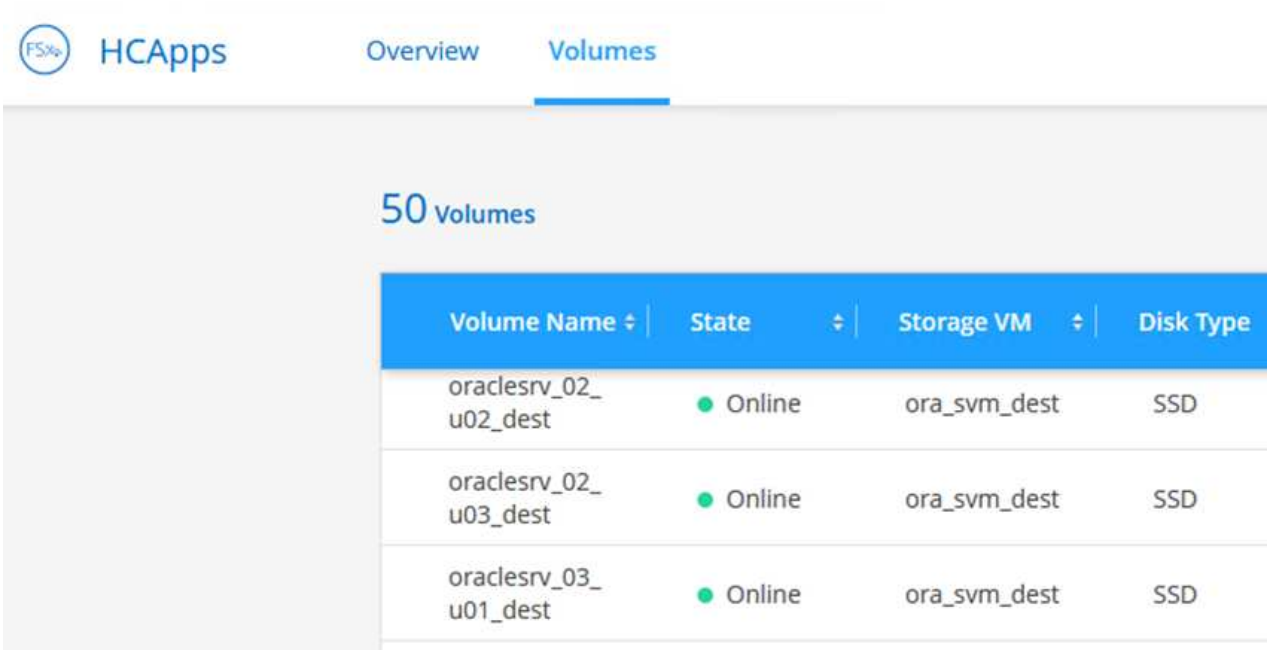
4. 교차로 경로 이름을 추가하고 업데이트를 클릭합니다. Oracle 서버에서 NFS 볼륨을 마운트할 때 이 연결 경로를 지정하세요.


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

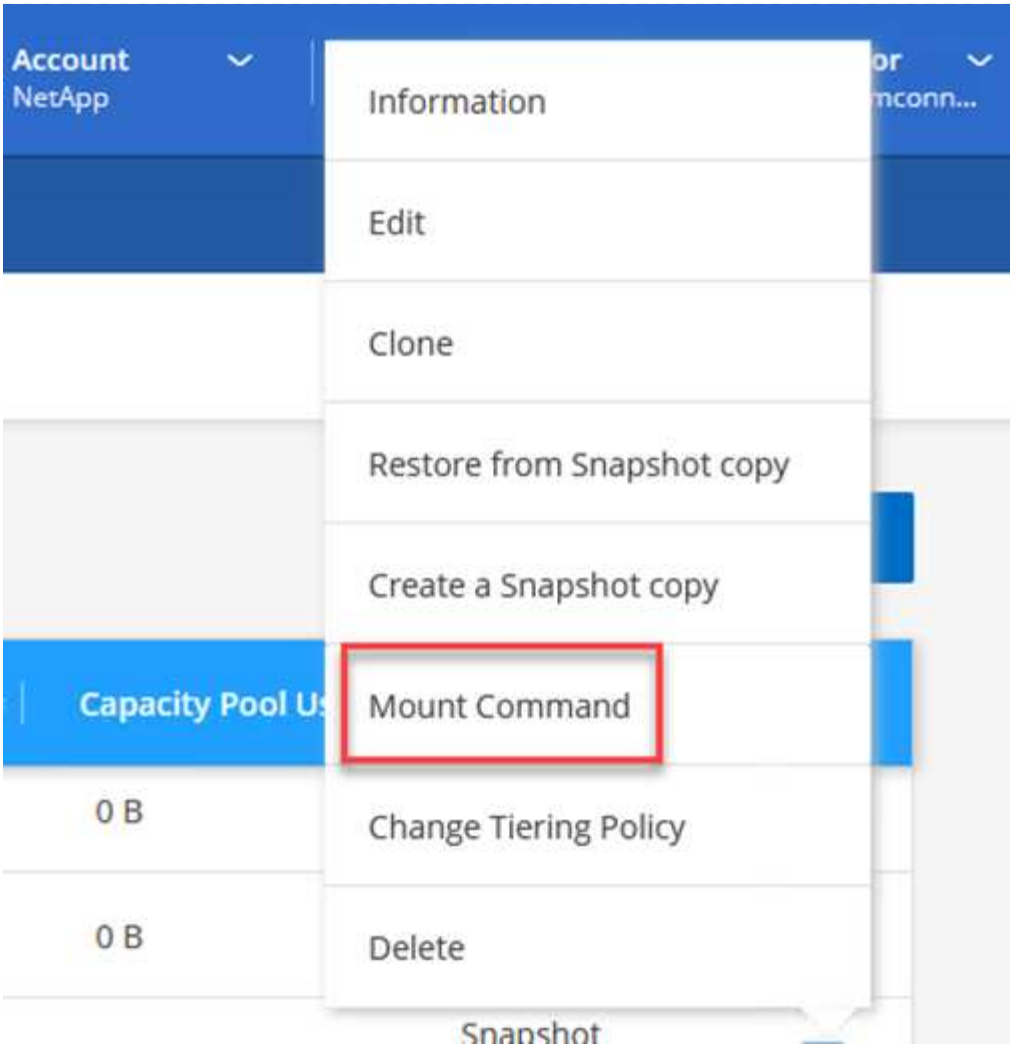
Oracle Server에 **NFS** 볼륨 마운트

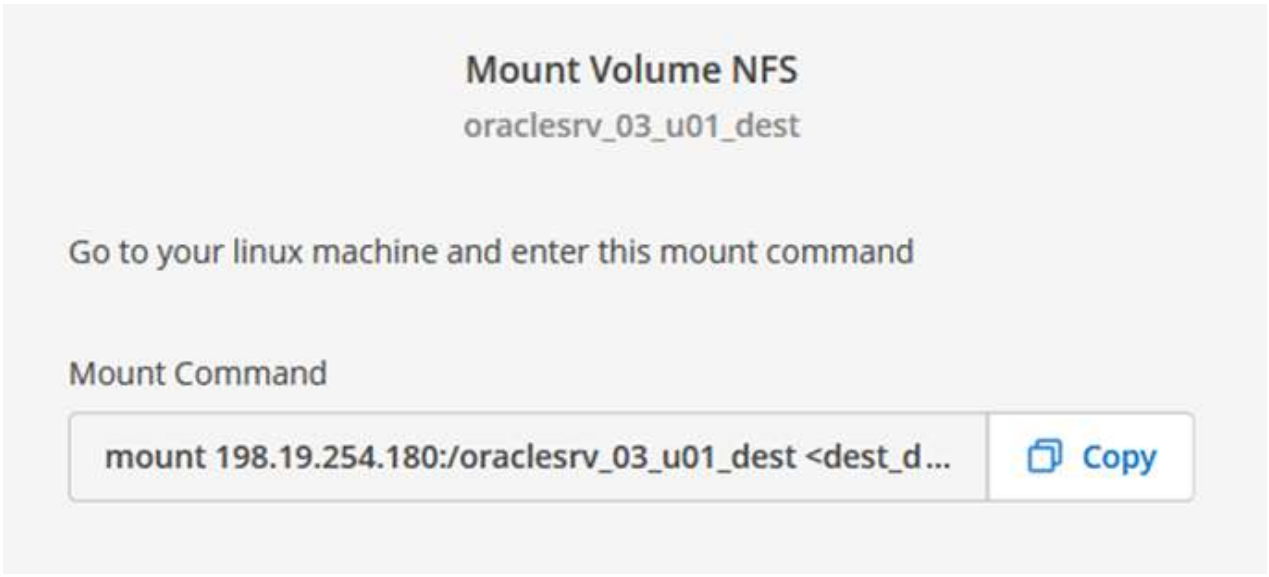
Cloud Manager에서는 Oracle 데이터베이스 파일과 로그가 포함된 NFS 볼륨을 마운트하기 위한 올바른 NFS LIF IP 주소를 사용하여 mount 명령을 얻을 수 있습니다.

1. Cloud Manager에서 FSx 클러스터의 볼륨 목록에 액세스합니다.



2. 작업 메뉴에서 Mount Command를 선택하여 Oracle Linux 서버에서 사용할 mount 명령을 보고 복사합니다.





3. Oracle Linux 서버에 NFS 파일 시스템을 마운트합니다. NFS 공유를 마운트하기 위한 디렉토리가 이미 Oracle Linux 호스트에 있습니다.
4. Oracle Linux 서버에서 mount 명령을 사용하여 NFS 볼륨을 마운트합니다.

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

Oracle 데이터베이스와 연관된 각 볼륨에 대해 이 단계를 반복합니다.

재부팅 시에도 NFS 마운트를 유지하려면 다음을 편집하세요. `/etc/fstab` 마운트 명령을 포함할 파일입니다.

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

장애 복구

이 솔루션에 설명된 장애 조치 프로세스를 성공적으로 완료하면 SnapCenter 와 Veeam은 AWS에서 실행되는 백업 기능을 재개하고 FSx ONTAP 이제 원래 온프레미스 데이터 센터와 기존 SnapMirror 관계가 없는 기본 스토리지로 지정됩니다. 온프레미스에서 정상 기능이 재개된 후에는 이 문서에 설명된 것과 동일한 프로세스를 사용하여 데이터를 온프레미스 ONTAP 스토리지 시스템으로 다시 미러링할 수 있습니다.

이 문서에도 설명되어 있듯이 SnapCenter 구성하여 FSx ONTAP 의 애플리케이션 데이터 볼륨을 온프레미스에 있는 ONTAP 스토리지 시스템으로 미러링할 수 있습니다. 마찬가지로, 스케일아웃 백업 저장소를 사용하여 Veeam이 백업 사본을 Amazon S3에 복제하도록 구성하면 온프레미스 데이터 센터에 있는 Veeam 백업 서버에서 해당 백업에 액세스할 수 있습니다.

이 문서에서는 장애 복구에 대해 다루지 않지만, 장애 복구는 여기에 설명된 자세한 프로세스와 크게 다르지 않습니다.

결론

이 문서에 제시된 사용 사례는 NetApp 과 VMware 간의 통합을 강조하는 검증된 재해 복구 기술에 초점을 맞춥니다. NetApp ONTAP 스토리지 시스템은 검증된 데이터 미러링 기술을 제공하여 조직이 온프레미스와 주요 클라우드 공급업체가 제공하는 ONTAP 기술을 아우르는 재해 복구 솔루션을 설계할 수 있도록 지원합니다.

AWS의 FSx ONTAP SnapCenter 및 SyncMirror 와 원활하게 통합되어 애플리케이션 데이터를 클라우드로 복제할 수 있는 솔루션 중 하나입니다. Veeam Backup & Replication은 NetApp ONTAP 스토리지 시스템과 잘 통합되는 또 다른 잘 알려진 기술이며 vSphere 기본 스토리지로의 장애 조치를 제공할 수 있습니다.

이 솔루션은 SQL Server와 Oracle 애플리케이션 데이터를 호스팅하는 ONTAP 시스템의 게스트 연결 스토리지를 사용하는 재해 복구 솔루션을 제공합니다. SnapMirror 탑재된 SnapCenter ONTAP 시스템의 애플리케이션 볼륨을 보호하고 이를 클라우드에 있는 FSx 또는 CVO로 복제하기 위한 관리하기 쉬운 솔루션을 제공합니다. SnapCenter 모든 애플리케이션 데이터를 AWS의 VMware Cloud로 장애 조치하기 위한 DR 지원 솔루션입니다.