NetApp for GCP/GCVE

NetApp Solutions

NetApp
September 23, 2024

목차

NetApp for GCP/GCVE . . . 1
Google Cloud Platform GCVE를 위한 NetApp의 기능 . . . 1
GCP/GCVE에서 워크로드 보호 . . . 2
GCP/GCVE에서 워크로드를 마이그레이션하는 중입니다 . . . 38
지역 가용성 – Google Cloud Platform(GCP)용 보조 NFS 데이터 저장소 . . . 58
보안 개요 - Google Cloud의 NetApp CVS(Cloud Volumes Service . . . 60

NetApp for GCP/GCVE

Google Cloud Platform GCVE를 위한 NetApp의 기능

NetApp이 GCP(Google Cloud Platform) Google Cloud VMware Engine(GCVE)에 제공하는 기능에 대해 자세히 알아보십시오. NetApp(게스트 연결 스토리지 장치 또는 보조 NFS 데이터 저장소부터 마이그레이션, 클라우드로 확장/버스트, 재해 복구까지.

다음 옵션 중 하나를 선택하여 원하는 콘텐츠의 섹션으로 이동합니다.

- "GCP에서 GCVE 구성"
- "GCVE용 NetApp 스토리지 옵션"
- "NetApp/VMware 클라우드 솔루션"

GCP에서 GCVE 구성

온프레미스에서와 마찬가지로 클라우드 기반 가상화 환경을 계획하는 것은 VM 및 마이그레이션을 생성할 수 있는 성공적인 프로덕션 준비 환경에 매우 중요합니다.

이 섹션에서는 GCVE를 설정 및 관리하고 NetApp 스토리지를 연결하는 데 사용할 수 있는 옵션과 함께 사용하는 방법을 설명합니다.

> 게스트 내 저장소는 Cloud Volumes ONTAP 및 Cloud Volumes Services를 GCVE에 연결하는 유일한 지원 방법입니다.

설치 프로세스는 다음 단계로 나눌 수 있습니다.

- GCVE 배포 및 구성
- GCVE에 대한 개인 액세스를 활성화합니다

자세한 내용을 확인하십시오 "GCVE에 대한 구성 단계".

GCVE용 NetApp 스토리지 옵션

NetApp 스토리지는 GCP GCVE 내에서 guess Connected 또는 보충 NFS 데이터 저장소로 여러 가지 방법으로 활용할 수 있습니다.

를 방문하십시오 "지원되는 NetApp 스토리지 옵션" 를 참조하십시오.

Google Cloud는 다음과 같은 구성에서 NetApp 스토리지를 지원합니다.

- CVO(Cloud Volumes ONTAP)를 게스트 연결 스토리지로 사용합니다
- CVS(Cloud Volumes Service)를 게스트 연결 스토리지로 사용합니다
- CVS(Cloud Volumes Service)를 보조 NFS 데이터 저장소로 사용

자세한 내용을 확인하십시오 "GCVE에 대한 게스트 연결 저장소 옵션".

에 대해 자세히 알아보십시오 "Google Cloud VMware Engine에 대한 NetApp Cloud Volumes Service 데이터 저장소 지원(NetApp 블로그)" 또는 "NetApp CVS를 Google Cloud VMware Engine용 데이터 저장소로 사용하는 방법(Google 블로그)"

솔루션 사용 사례

NetApp 및 VMware 클라우드 솔루션을 사용하면 많은 사용 사례를 Azure AVS에서 간단하게 구축할 수 있습니다. SE 사례는 VMware에서 정의한 각 클라우드 영역에 대해 정의됩니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 확장
- 마이그레이션

"Google Cloud GCVE용 NetApp 솔루션을 찾아보십시오"

GCP/GCVE에서 워크로드 보호

NetApp SnapCenter 및 Veeam 복제를 통해 애플리케이션 정합성이 보장되는 재해 복구

클라우드로 재해 복구는 랜섬웨어 등 사이트 운영 중단 및 데이터 손상 이벤트로부터 워크로드를 보호하는 복원력이 있는 비용 효율적인 방법입니다. NetApp SnapMirror를 사용하면 게스트 연결 스토리지를 사용하는 사내 VMware 워크로드를 Google Cloud에서 실행 중인 NetApp Cloud Volumes ONTAP로 복제할 수 있습니다.

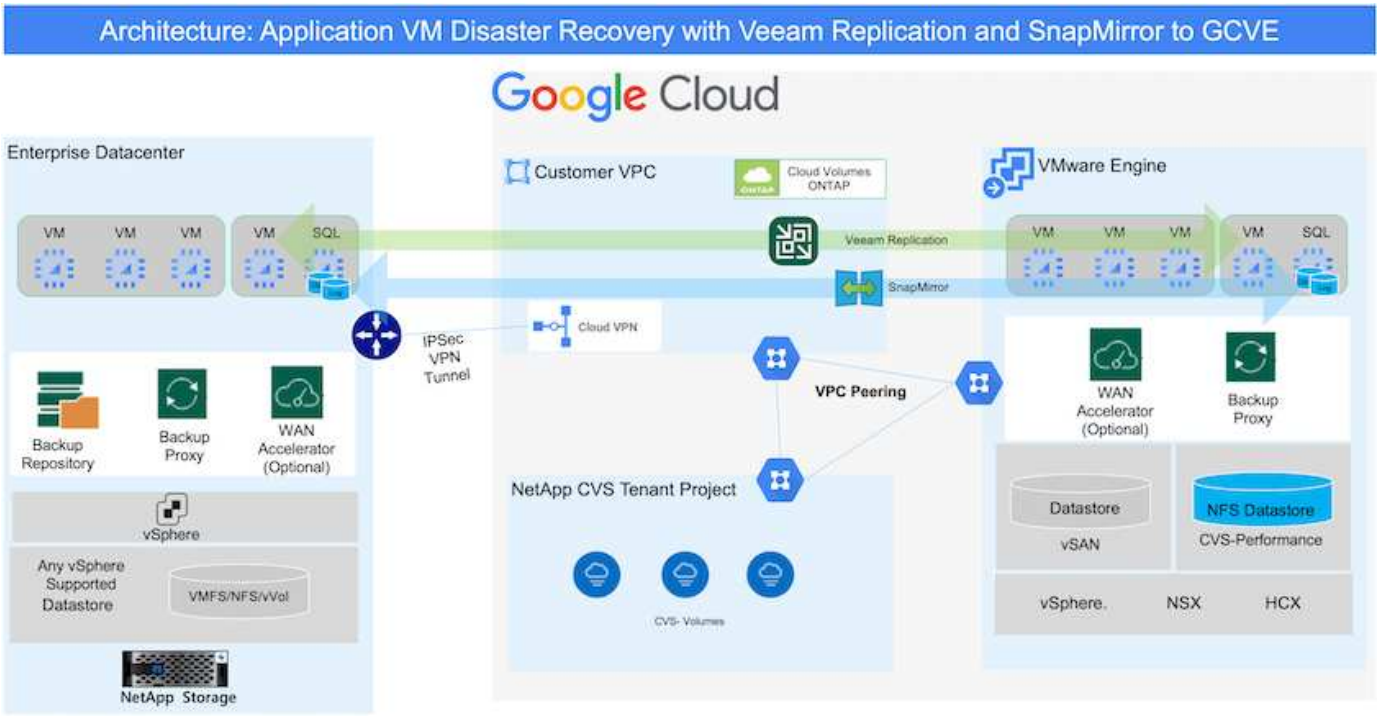
저자: NetApp Suesh Thoppay

개요

많은 고객이 VMware vSphere에서 호스팅되는 애플리케이션 VM을 위한 효율적인 재해 복구 솔루션을 찾고 있습니다. 이 중 다수는 기존 백업 솔루션을 사용하여 DIaster를 실행하는 동안 복구를 수행합니다.
이러한 솔루션은 RTO를 높여주고 기대에 미치지 못합니다. RPO 및 RTO를 줄이기 위해 적절한 권한이 있는 네트워크 연결 및 환경을 사용할 수 있는 한 Veeam VM 복제를 사내에서 GCVE로 활용할 수 있습니다.
참고: Veeam VM 복제는 게스트 VM 내부의 iSCSI 또는 NFS 마운트와 같은 VM 게스트에 연결된 스토리지 디바이스를 보호하지 않습니다. 별도로 보호해야 합니다.

SQL VM의 애플리케이션 정합성이 보장되는 복제 및 RTO를 줄이기 위해 SnapCenter을 사용하여 SQL 데이터베이스 및 로그 볼륨의 SnapMirror 작업을 오케스트레이션했습니다.

이 문서에서는 NetApp SnapMirror, Veeam 및 Google Cloud VMware Engine(GCVE)을 사용하는 재해 복구를 설정하고 수행하기 위한 단계별 접근 방식을 제공합니다.



가정

이 문서에서는 애플리케이션 데이터(게스트 연결)를 위한 게스트 내 스토리지에 초점을 두고 사내 환경에서 애플리케이션 정합성 보장 백업을 위해 SnapCenter를 사용하고 있다고 가정합니다.

> ⓘ 이 문서는 타사 백업 또는 복구 솔루션에 적용됩니다. 환경에 사용된 솔루션에 따라 Best Practice를 따라 조직 SLA를 충족하는 백업 정책을 생성합니다.

온프레미스 환경과 Google Cloud 네트워크 간의 연결을 위해 전용 상호 연결 또는 Cloud VPN과 같은 연결 옵션을 사용합니다. 세그먼트는 사내 VLAN 설계를 기반으로 생성해야 합니다.

> ⓘ 온프레미스 데이터 센터를 Google Cloud에 연결하는 옵션에는 여러 가지가 있으며, 이로 인해 NetApp에서 이 문서의 특정 워크플로우를 개괄적으로 설명하지 못하게 됩니다. 적절한 온프레미스 -Google 연결 방법은 Google Cloud 설명서를 참조하십시오.

DR 솔루션 구축

솔루션 구축 개요

1. 필요한 RPO 요구 사항에 따라 SnapCenter를 사용하여 애플리케이션 데이터를 백업했는지 확인합니다.
2. 적절한 가입 및 가상 네트워크 내에서 BlueXP를 사용하여 Cloud Volumes ONTAP의 인스턴스 크기를 올바르게 프로비저닝합니다.
    a. 관련 애플리케이션 볼륨에 대해 SnapMirror를 구성합니다.
    b. 예약된 작업 후 SnapMirror 업데이트를 트리거하도록 SnapCenter의 백업 정책을 업데이트합니다.
3. Veeam 소프트웨어를 설치하고 Google Cloud VMware Engine 인스턴스에 가상 머신 복제를 시작합니다.
4. 재해 발생 시 BlueXP를 사용하여 SnapMirror 관계를 중단시키고 Veeam으로 가상 시스템의 페일오버를 트리거하십시오.

a. 애플리케이션 VM에 대한 iSCSI LUN 및 NFS 마운트를 다시 연결합니다.

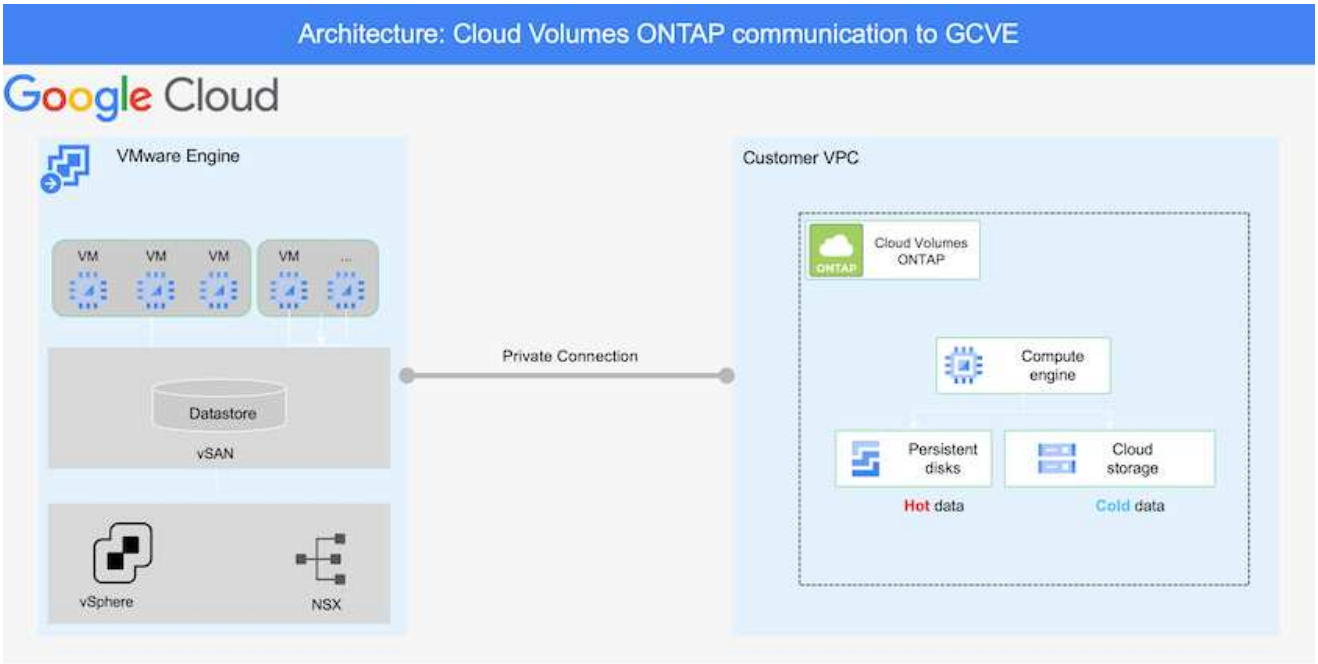
b. 애플리케이션을 온라인으로 전환합니다.

5. 운영 사이트가 복구된 후 SnapMirror를 다시 동기화하여 보호 사이트에 대한 페일백을 호출합니다.

배포 세부 정보

Google Cloud에서 **CVO**를 구성하고 볼륨을 **CVO**로 복제합니다

첫 번째 단계는 Cloud Volumes ONTAP Google Cloud("CVO")를 사용하여 원하는 볼륨을 Cloud Volumes ONTAP에 복제하고 원하는 빈도와 스냅샷 보존 기능을 사용할 수 있습니다.



SnapCenter 설정 및 데이터 복제에 대한 단계별 지침은 을 참조하십시오 "SnapCenter를 사용하여 복제를 설정합니다"

SnapCenter를 사용한 SQL VM 보호 검토

GCVE 호스트 및 **CVO** 데이터 액세스를 구성합니다

SDDC를 배포할 때 고려해야 할 두 가지 중요한 요소는 GCVE 솔루션의 SDDC 클러스터의 크기와 SDDC를 사용할 수 있는 기간 입니다. 재해 복구 솔루션의 두 가지 주요 고려 사항은 전체 운영 비용을 절감하는 데 도움이 됩니다. SDDC는 최대 3개의 호스트까지 구성할 수 있으며, 전체 구축 환경에서 다중 호스트 클러스터까지 가능합니다.

NFS 데이터 저장소용 NetApp Cloud Volume Service와 SQL 데이터베이스 및 로그용 Cloud Volumes ONTAP를 모든 VPC 및 GCVE에 구축할 수 있습니다. NFS 데이터 저장소를 마운트하고 VM을 iSCSI LUN에 연결하려면 해당 VPC에 대한 전용 연결이 있어야 합니다.

GCVE SDDC를 구성하려면 를 참조하십시오 "Google Cloud Platform(GCP)에서 가상화 환경 구축 및 구성". 먼저 GCVE 호스트에 상주하는 게스트 VM이 연결이 설정된 후 Cloud Volumes ONTAP의 데이터를 사용할 수 있는지 확인합니다.

Cloud Volumes ONTAP 및 GCVE가 올바르게 구성된 후에는 Veeam 복제 기능을 사용하고 Cloud Volumes ONTAP에 애플리케이션 볼륨 복사본에 SnapMirror를 활용하여 사내 워크로드(게스트 내 스토리지가 있는 애플리케이션 VMDK 및 VM이 있는 VM)를 GCVE로 자동 복구하도록 Veeam 구성을 시작하십시오.

Veeam 구성 요소를 설치합니다

Veeam 백업 서버, 백업 저장소 및 구축해야 하는 백업 프록시가 구축 시나리오에 기반을 두고 있습니다. 이 경우 Veeam 및 스케일아웃 저장소에도 오브젝트 저장소를 구축할 필요가 없습니다.
"설치 절차는 Veeam 설명서를 참조하십시오"
자세한 내용은 을 참조하십시오 "Veeam 복제를 사용한 마이그레이션"

Veeam으로 **VM** 복제를 설정합니다

사내 vCenter와 GCVE vCenter를 모두 Veeam에 등록해야 합니다. "vSphere VM 복제 작업을 설정합니다" 마법사의 게스트 처리 단계에서 애플리케이션 인식 백업 및 복구를 위해 SnapCenter를 활용할 예정이므로 애플리케이션 처리 비활성화 를 선택합니다.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Microsoft SQL Server VM의 페일오버

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

이 솔루션의 이점

- SnapMirror의 효율적이고 복원력이 뛰어난 복제를 사용합니다.
- ONTAP 스냅샷 보존을 사용하여 사용 가능한 모든 시점 복구
- 스토리지, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계에서 수백 또는 수천 개의 VM을 복구하는 데 필요한 모든 단계에서 완전한 자동화가 가능합니다.
- SnapCenter는 복제된 볼륨을 변경하지 않는 클론 생성 메커니즘을 사용합니다.

- 이렇게 하면 볼륨 및 스냅숏에 대한 데이터 손상 위험이 방지됩니다.
- DR 테스트 워크플로우 중에 복제 중단 방지
- 개발/테스트, 보안 테스트, 패치 및 업그레이드 테스트, 수정 테스트 등 DR 이외의 워크플로우에 DR 데이터를 활용합니다.

- Veeam Replication을 사용하면 DR 사이트에서 VM IP 주소를 변경할 수 있습니다.

SnapCenter, Cloud Volumes ONTAP, Veeam 복제를 통한 애플리케이션 재해 복구

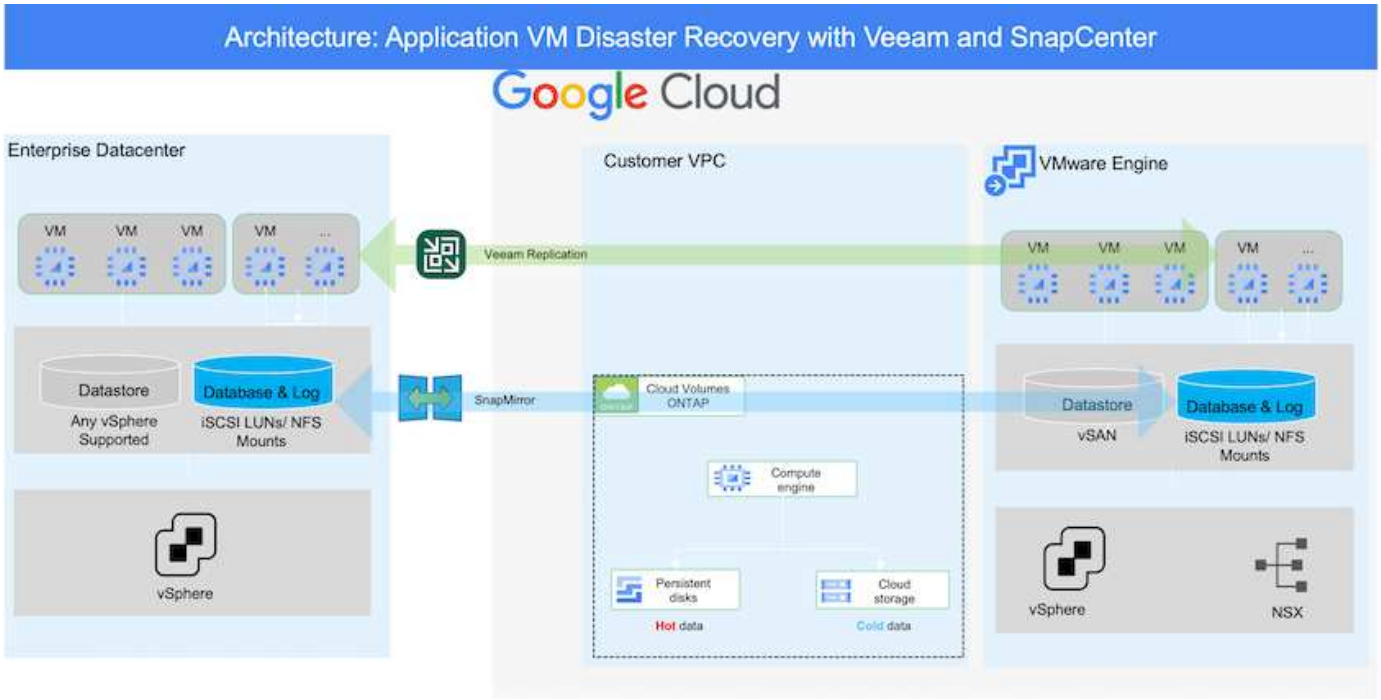
클라우드로 재해 복구는 랜섬웨어 등 사이트 운영 중단 및 데이터 손상 이벤트로부터 워크로드를 보호하는 복원력이 있는 비용 효율적인 방법입니다. NetApp SnapMirror를 사용하면 게스트 연결 스토리지를 사용하는 사내 VMware 워크로드를 Google Cloud에서 실행 중인 NetApp Cloud Volumes ONTAP로 복제할 수 있습니다.

저자: NetApp Suesh Thoppay

개요

여기에는 애플리케이션 데이터가 포함됩니다. 하지만 실제 VM 자체는 어떻습니까? 재해 복구는 가상 머신, VMDK, 애플리케이션 데이터 등을 비롯한 모든 종속 구성 요소를 포함해야 합니다. 이를 위해 Veeam과 함께 SnapMirror를 사용하여 VM VMDK에 vSAN 스토리지를 사용하면서 사내에서 Cloud Volumes ONTAP로 복제된 워크로드를 원활하게 복구할 수 있습니다.

이 문서에서는 NetApp SnapMirror, Veeam 및 Google Cloud VMware Engine(GCVE)을 사용하는 재해 복구를 설정하고 수행하기 위한 단계별 접근 방식을 제공합니다.



가정

이 문서에서는 애플리케이션 데이터(게스트 연결)를 위한 게스트 내 스토리지에 초점을 두고 사내 환경에서 애플리케이션 정합성 보장 백업을 위해 SnapCenter를 사용하고 있다고 가정합니다.

이 문서는 타사 백업 또는 복구 솔루션에 적용됩니다. 환경에 사용된 솔루션에 따라 Best Practice를 따라 조직 SLA를 충족하는 백업 정책을 생성합니다.

온프레미스 환경과 Google Cloud 네트워크 간의 연결을 위해 전용 상호 연결 또는 Cloud VPN과 같은 연결 옵션을 사용합니다. 세그먼트는 사내 VLAN 설계를 기반으로 생성해야 합니다.

온프레미스 데이터 센터를 Google Cloud에 연결하는 옵션에는 여러 가지가 있으며, 이로 인해 NetApp에서 이 문서의 특정 워크플로우를 개괄적으로 설명하지 못하게 됩니다. 적절한 온프레미스 -Google 연결 방법은 Google Cloud 설명서를 참조하십시오.

DR 솔루션 구축

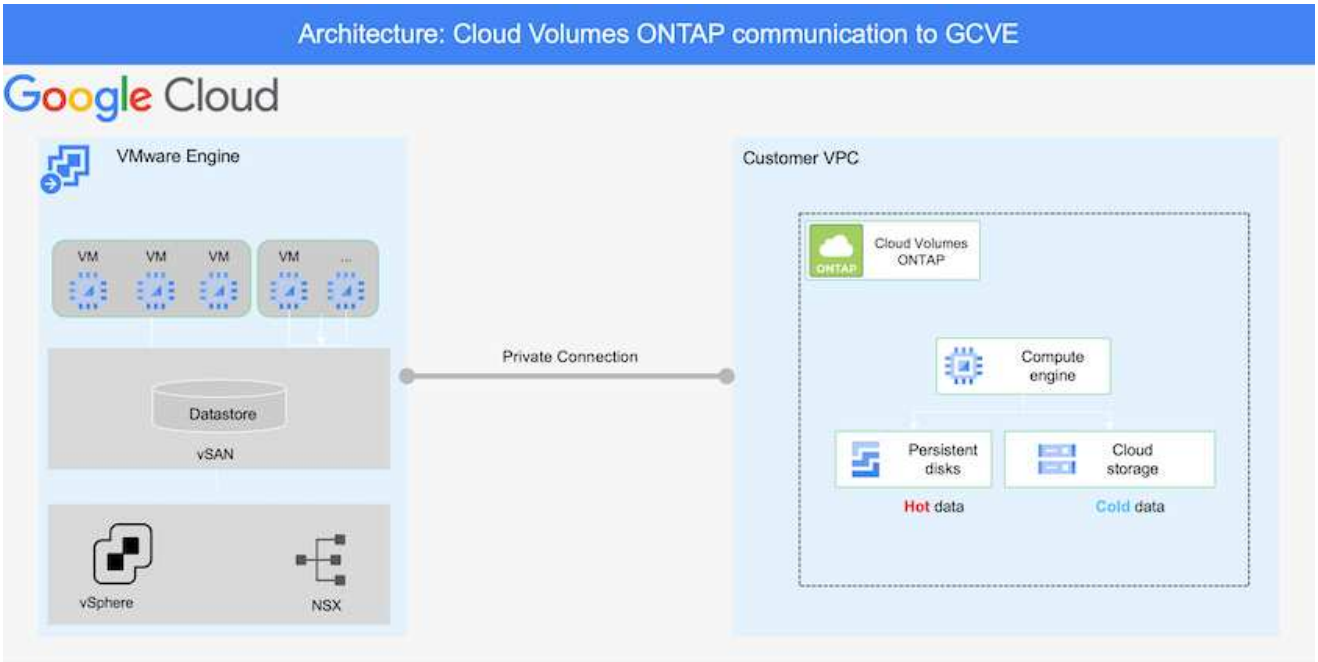
솔루션 구축 개요

1. 필요한 RPO 요구 사항에 따라 SnapCenter를 사용하여 애플리케이션 데이터를 백업했는지 확인합니다.
2. 적절한 서브스크립션 및 가상 네트워크 내에서 Cloud Manager를 사용하여 올바른 인스턴스 크기로 Cloud Volumes ONTAP를 프로비저닝합니다.
   a. 관련 애플리케이션 볼륨에 대해 SnapMirror를 구성합니다.
   b. 예약된 작업 후 SnapMirror 업데이트를 트리거하도록 SnapCenter의 백업 정책을 업데이트합니다.
3. Veeam 소프트웨어를 설치하고 Google Cloud VMware Engine 인스턴스에 가상 머신 복제를 시작합니다.
4. 재해 발생 시 Cloud Manager를 사용하여 SnapMirror 관계를 맺고 Veeam으로 가상 시스템의 페일오버를 트리거하십시오.
   a. 애플리케이션 VM에 대한 iSCSI LUN 및 NFS 마운트를 다시 연결합니다.
   b. 애플리케이션을 온라인으로 전환합니다.
5. 운영 사이트가 복구된 후 SnapMirror를 다시 동기화하여 보호 사이트에 대한 페일백을 호출합니다.

배포 세부 정보

Google Cloud에서 **CVO**를 구성하고 볼륨을 **CVO**로 복제합니다

첫 번째 단계는 Cloud Volumes ONTAP Google Cloud("CVO")를 사용하여 원하는 볼륨을 Cloud Volumes ONTAP에 복제하고 원하는 빈도와 스냅샷 보존 기능을 사용할 수 있습니다.



SnapCenter 설정 및 데이터 복제에 대한 단계별 지침은 을 참조하십시오 "SnapCenter를 사용하여 복제를 설정합니다"

SnapCenter를 사용하여 복제를 설정합니다

GCVE 호스트 및 **CVO** 데이터 액세스를 구성합니다

SDDC를 배포할 때 고려해야 할 두 가지 중요한 요소는 GCVE 솔루션의 SDDC 클러스터의 크기와 SDDC를 사용할 수 있는 기간 입니다. 재해 복구 솔루션의 두 가지 주요 고려 사항은 전체 운영 비용을 절감하는 데 도움이 됩니다. SDDC는 최대 3개의 호스트까지 구성할 수 있으며, 전체 구축 환경에서 다중 호스트 클러스터까지 가능합니다.

모든 VPC 및 GCVE에 Cloud Volumes ONTAP를 구축할 수 있습니다. VM이 iSCSI LUN에 접속하려면 해당 VPC에 대한 전용 연결이 있어야 합니다.

GCVE SDDC를 구성하려면 를 참조하십시오 "Google Cloud Platform(GCP)에서 가상화 환경 구축 및 구성". 먼저 GCVE 호스트에 상주하는 게스트 VM이 연결이 설정된 후 Cloud Volumes ONTAP의 데이터를 사용할 수 있는지 확인합니다.

Cloud Volumes ONTAP 및 GCVE가 올바르게 구성된 후에는 Veeam 복제 기능을 사용하고 Cloud Volumes ONTAP에 애플리케이션 볼륨 복사본에 SnapMirror를 활용하여 사내 워크로드(게스트 내 스토리지가 있는 애플리케이션 VMDK 및 VM이 있는 VM)를 GCVE로 자동 복구하도록 Veeam 구성을 시작하십시오.

Veeam 구성 요소를 설치합니다

Veeam 백업 서버, 백업 저장소 및 구축해야 하는 백업 프록시가 구축 시나리오에 기반을 두고 있습니다. 이 경우 Veeam 및 스케일아웃 저장소에도 오브젝트 저장소를 구축할 필요가 없습니다.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["설치 절차는 Veeam 설명서를 참조하십시오"]

Veeam으로 **VM** 복제를 설정합니다

사내 vCenter와 GCVE vCenter를 모두 Veeam에 등록해야 합니다. "vSphere VM 복제 작업을 설정합니다" 마법사의 게스트 처리 단계에서 애플리케이션 인식 백업 및 복구를 위해 SnapCenter를 활용할 예정이므로 애플리케이션 처리 비활성화 를 선택합니다.

vSphere VM 복제 작업을 설정합니다

Microsoft SQL Server VM의 페일오버

Microsoft SQL Server VM의 페일오버

이 솔루션의 이점

- SnapMirror의 효율적이고 복원력이 뛰어난 복제를 사용합니다.
- ONTAP 스냅샷 보존을 사용하여 사용 가능한 모든 시점 복구
- 스토리지, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계에서 수백 또는 수천 개의 VM을 복구하는 데 필요한 모든 단계에서 완전한 자동화가 가능합니다.
- SnapCenter는 복제된 볼륨을 변경하지 않는 클론 생성 메커니즘을 사용합니다.
  - 이렇게 하면 볼륨 및 스냅숏에 대한 데이터 손상 위험이 방지됩니다.
  - DR 테스트 워크플로우 중에 복제 중단 방지
  - 개발/테스트, 보안 테스트, 패치 및 업그레이드 테스트, 수정 테스트 등 DR 이외의 워크플로우에 DR 데이터를 활용합니다.
- Veeam Replication을 사용하면 DR 사이트에서 VM IP 주소를 변경할 수 있습니다.

Google Cloud VMware Engine으로 재해 복구를 위해 **Veeam Replication** 및 **Google Cloud NetApp Volumes** 데이터 저장소를 사용합니다

포괄적인 재해 복구 계획은 위기 상황에서 기업에 매우 중요합니다. 많은 조직이 일상적인 운영과 재해 복구에 클라우드 컴퓨팅을 활용합니다. 이 사전 예방적 접근 방식을 통해 값비싼 비즈니스 중단을 줄이거나 없앨 수 있습니다.

이 기사에서는 Veeam 백업 및 복제를 사용하여 Google Cloud NetApp 볼륨(NetApp Volumes)을 사용하여 온프레미스 VMware VM에 대한 재해 복구를 Google Cloud VMware Engine(GCVE)으로 설정하는 방법을 설명합니다.

개요

Google Cloud NetApp Volumes는 Google Cloud에 사용 가능한 Google 및 NetApp의 스토리지 서비스입니다. NetApp Volumes 서비스는 고성능 NFS/SMB 스토리지를 제공합니다. GCVE에서 VMware 인증 NetApp 볼륨 NFS 스토리지를 ESXi 호스트의 외부 데이터 저장소로 사용할 수 있습니다. 사용자는 GCVE 프라이빗 클라우드와 NetApp 볼륨 프로젝트 간의 피어링 연결을 설정해야 합니다. 한 지역 내의 스토리지 액세스로 인한 네트워크 요금은 없습니다. 사용자는 Google Cloud 콘솔에서 NetApp 볼륨 볼륨을 생성하고 삭제 보호를 활성화한 후 볼륨을 ESXi 호스트에 데이터 저장소로 마운트하기 전에 미리 설정할 수 있습니다.

NetApp 볼륨 기반 NFS 데이터 저장소를 사용하여 VM 복제 기능을 제공하는 검증된 타사 솔루션을 사용하여 사내에서 데이터를 복제할 수 있습니다. NetApp 볼륨 데이터 저장소를 추가하면 스토리지를 수용할 수 있는 다수의 ESXi 호스트와 함께 GCVE(Google Cloud VMware Engine) 기반 SDDC를 구축하는 대신 비용 최적화된 배포를 가능하게 합니다. 이러한 접근 방식을 "파일럿 라이트 클러스터"라고 합니다. 파일럿 라이트 클러스터는 용량 요구사항을 충족하도록 독립적으로 확장할 수 있도록 NetApp 볼륨 데이터 저장소 용량과 함께 최소 GCVE 호스트 구성(GCVE ESXi 호스트 3개)입니다.

핵심 구성 요소만 사용하여 비용 효율적인 인프라를 유지함으로써 페일오버를 관리하는 것이 목표입니다. 파일럿 라이트 클러스터는 장애 조치 시 GCVE 호스트를 확장하고 추가할 수 있습니다. 장애 조치가 해결되고 정상 작동이 재개되면 파일럿 라이트 클러스터가 저가의 운영 모드로 되돌아가 규모를 줄일 수 있습니다.

이 문서의 목적

이 기사에서는 Veeam 백업 및 복제와 함께 Google Cloud NetApp 볼륨 데이터 저장소를 사용하여 Veeam VM 복제 소프트웨어 기능을 사용하여 온프레미스 VMware VM의 재해 복구를 GCVE에 설정하는 방법을 설명합니다.

Veeam Backup & Replication은 가상 환경을 위한 백업 및 복제 애플리케이션입니다. 가상 머신이 복제되면 Veeam Backup & Replication은 타겟 GCVE SDDC 클러스터에 기본 VMware vSphere 형식으로 VM의 정확한 복제본을 생성합니다. Veeam Backup & Replication은 복제본을 원래 VM과 동기화된 상태로 유지합니다. 재해 복구 사이트에 시작 준비 상태의 VM 복제본이 마운트되어 있기 때문에 복제는 최상의 RTO(복구 시간 목표)를 제공합니다.

이 복제 메커니즘은 재해 발생 시 GCVE에서 워크로드를 빠르게 시작할 수 있도록 합니다. 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 파일"도 필터링합니다. 소프트웨어는 복제본 트래픽도 압축합니다. 복제 작업이 전체 네트워크 대역폭을 소비하는 것을 방지하기 위해 WAN 가속기 및 네트워크 조절 규칙을 활용할 수 있습니다.

Veeam Backup & Replication의 복제 프로세스는 작업 중심으로 수행되므로 복제 작업을 구성하여 복제가 수행됩니다. 재해 이벤트의 경우 해당 복제본 복제본으로 장애 조치를 수행하여 VM을 복구하기 위해 페일오버를 트리거할 수 있습니다. 페일오버가 수행되면 복제된 VM이 원래 VM의 역할을 대신합니다. 복제본의 최신 상태나 알려진 정상 복구 지점으로 페일오버를 수행할 수 있습니다. 따라서 필요에 따라 랜섬웨어 복구 또는 격리된 테스트가 가능합니다. Veeam Backup & Replication은 다양한 재해 복구 시나리오를 처리할 수 있는 다양한 옵션을 제공합니다.

솔루션 개요

이 솔루션은 다음과 같은 상위 단계를 다룹니다.

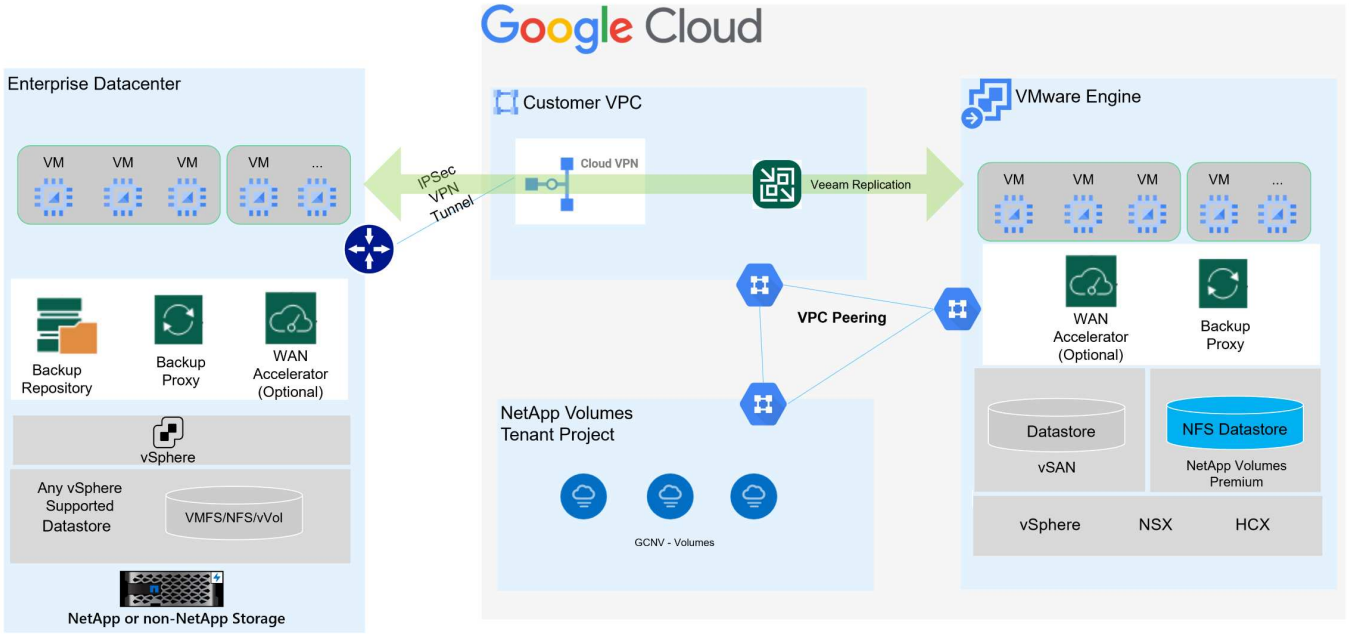
1. Google Cloud NetApp Volumes를 사용하여 NFS 볼륨을 생성한다
2. GCP 프로세스에 따라 NetApp Volumes NFS 볼륨에서 GCVE 데이터 저장소를 생성합니다.
3. Veeam Backup & Replication을 사용하여 VM 복제본을 생성하도록 복제 작업을 설정합니다.
4. 페일오버 계획을 만들고 페일오버를 수행합니다.
5. 재해 이벤트가 완료되고 운영 사이트가 가동되면 운영 VM으로 다시 전환합니다.

NetApp 볼륨에서 GCVE 데이터 저장소로 사용할 볼륨을 생성할 때 NFS v3만 지원됩니다.

NetApp 볼륨 NFS 볼륨을 GCVE용 데이터 저장소로 사용하는 방법에 대한 자세한 내용은 을 "NFS 볼륨을 Google Cloud NetApp 볼륨에서 호스팅하는 vSphere 데이터 저장소로 사용합니다" 참조하십시오.

있습니다

다음 다이어그램은 이 설명서에 제시된 솔루션의 아키텍처를 보여 줍니다. 사내 사이트와 GCVE SDDC 모두에 Veeam Backup & Replication Server를 배치하는 것이 좋습니다. 백업 및 복구는 Veeam 서버에서 온-프레미스로 수행 및 관리되며, 복제는 GCVE SDDC의 Veeam 서버에 의해 관리됩니다. 이 아키텍처는 운영 데이터 센터에서 장애가 발생할 경우 최고의 가용성을 제공합니다.



Veeam을 **GCVE** 및 **NetApp** 볼륨 데이터 저장소로 복제하기 위한 전제 조건입니다

이 솔루션에는 다음과 같은 구성 요소 및 구성이 필요합니다.

1. NetApp 볼륨에는 생성할 NFS 볼륨을 수용하기에 충분한 여유 용량과 함께 사용 가능한 스토리지 풀이 있습니다.
2. Veeam Backup and Replication 소프트웨어는 적절한 네트워크 연결을 갖춘 사내 환경에서 실행됩니다.
3. Veeam Backup & Replication 백업 VM이 소스 및 타겟 GCVE SDDC 클러스터에 연결되어 있는지 확인합니다.
4. Veeam Backup & Replication 백업 VM이 소스 및 타겟 GCVE 클러스터 모두에서 Veeam Proxy Server VM에 연결되어 있는지 확인합니다.
5. 백업 서버는 짧은 이름을 확인하고 소스 및 타겟 vCenter에 연결할 수 있어야 합니다.

사용자는 VMware Engine Cloud 콘솔 UI 내의 VPC 네트워크 피어링 또는 전용 연결 페이지를 사용하여 GCVE 프라이빗 클라우드와 NetApp Volumes 프로젝트 간에 피어링 연결을 설정해야 합니다.

Veeam을 사용하려면 Veeam Backup and Replication 인벤토리에 GCVE vCenter Server를 추가할 때 상승된 Privileges가 있는 GCVE 솔루션 사용자 계정이 필요합니다. 자세한 내용은 Google Cloud Platform (GCP) 설명서를 참조하십시오. "VMware Engine Privileges 상승"

자세한 내용은 "고려 사항 및 제한 사항" Veeam Backup & Replication 설명서의 을 참조하십시오.

배포 단계

다음 섹션에서는 Google Cloud NetApp 볼륨을 사용하여 NFS 데이터 저장소를 생성 및 마운트하고, Veeam 백업 및 복제를 사용하여 사내 데이터 센터와 Google Cloud VMware Engine 간에 전체 재해 복구 솔루션을 구현하는 구축 단계를 간략히 설명합니다.

GCVE용 **NetApp** 볼륨 **NFS** 볼륨 및 데이터 저장소를 생성합니다

`https://cloud.google.com/vmware-engine/docs/vmware-ecosystem/howto-cloud-volumes-datastores-gcve["NFS 볼륨을 Google Cloud NetApp 볼륨에서 호스팅하는 vSphere 데이터 저장소로 사용합니다"]GCVE용 데이터 저장소로 Google Cloud NetApp 볼륨을 사용하는 방법에 대한 개요는 를 참조하십시오.`

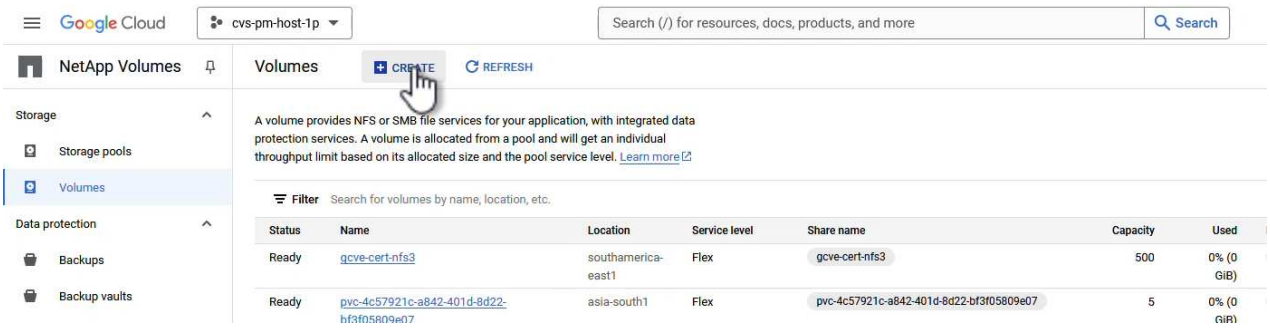
NetApp 볼륨을 사용하여 GCVE용 NFS 데이터 저장소를 만들고 사용하려면 다음 단계를 완료하십시오.

NetApp 볼륨 NFS 볼륨을 생성합니다

Google Cloud NetApp Volumes는 Google Cloud Platform(GCP) 콘솔에서 액세스할 수 있습니다.

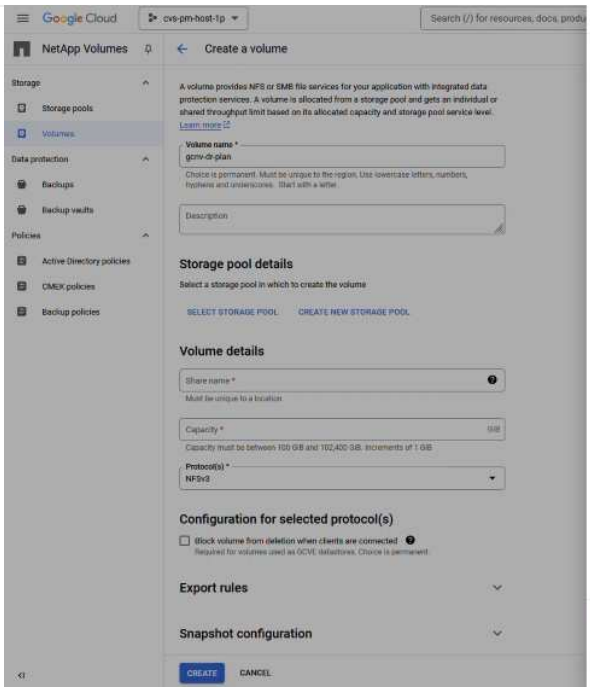
`https://cloud.google.com/netapp/volumes/docs/configure-and-use/volumes/create-volume["볼륨을 생성합니다"]이 단계에 대한 자세한 내용은 Google Cloud NetApp 볼륨 설명서의 을 참조하십시오.`

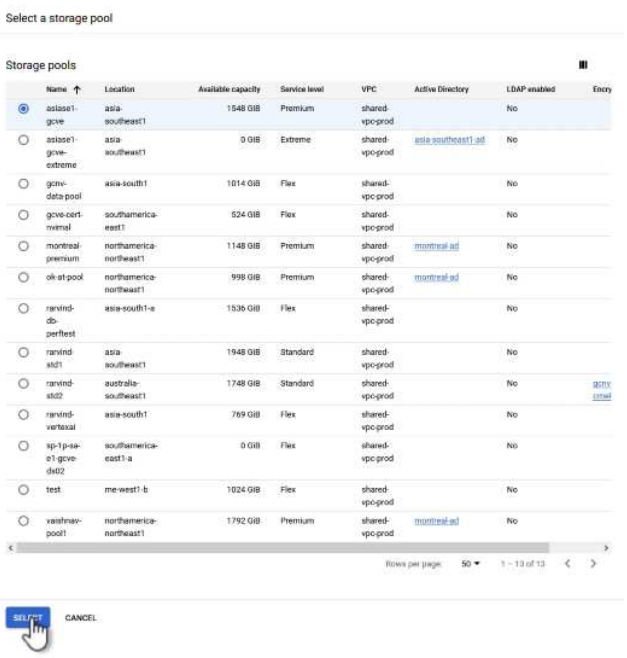
1. 웹 브라우저에서 https://console.cloud.google.com/ GCP 콘솔로 이동하여 로그인합니다. 시작하려면 * NetApp Volumes * 를 검색하십시오.
2. NetApp 볼륨 * 관리 인터페이스에서 * 생성 * 을 클릭하여 NFS 볼륨 생성을 시작합니다.

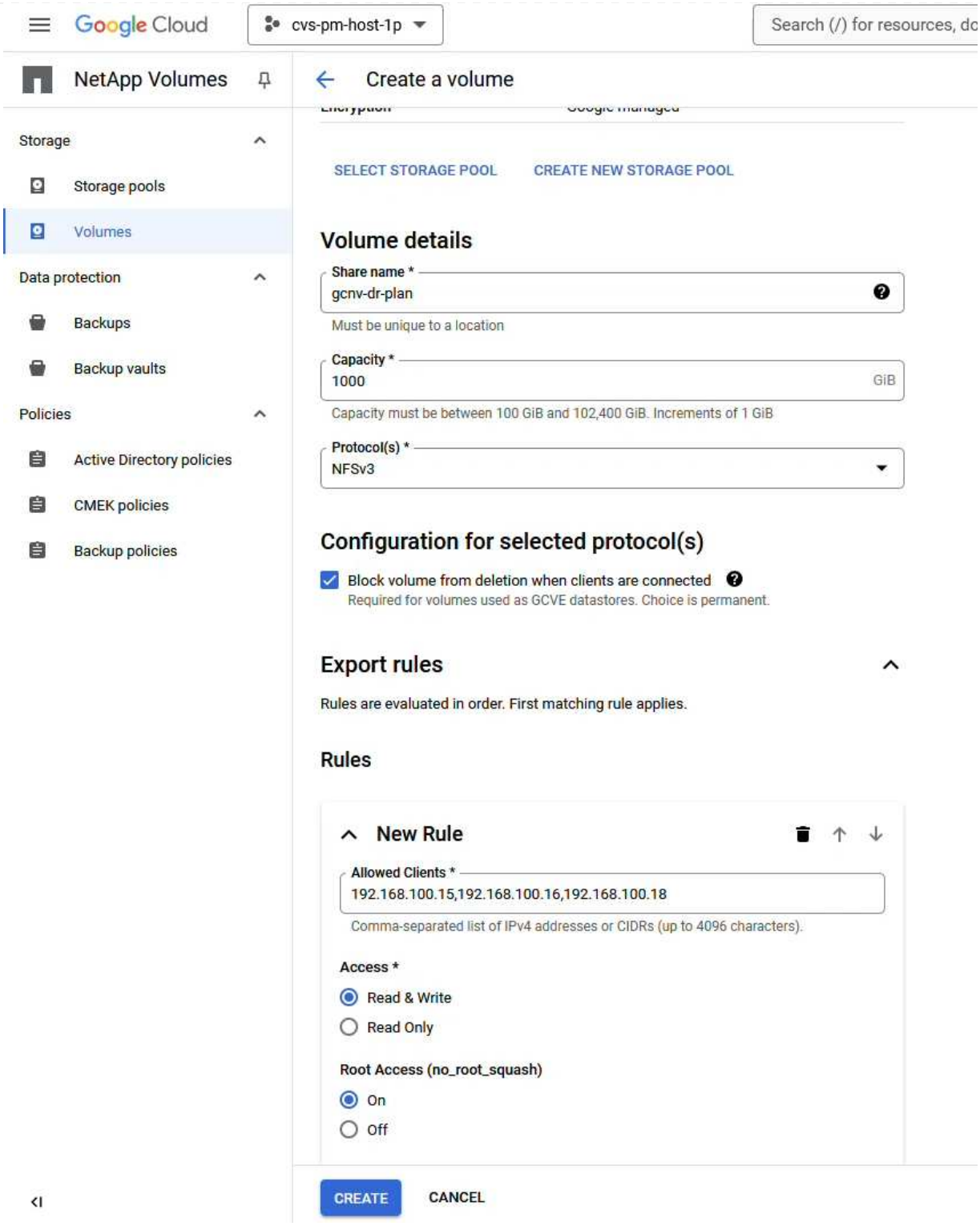


3. Create a volume * 마법사에서 필요한 모든 정보를 입력합니다.
   - 볼륨의 이름입니다.
   - 볼륨을 생성할 스토리지 풀입니다.
   - NFS 볼륨을 마운트할 때 사용되는 공유 이름입니다.
   - 볼륨의 용량(GiB)입니다.
   - 사용할 스토리지 프로토콜입니다.
   - 클라이언트가 연결된 경우 * 볼륨 삭제 차단 * (데이터 저장소로 마운트할 때 GCVE에 필요함) 확인란을 선택합니다.
   - 볼륨 액세스를 위한 내보내기 규칙. NFS 네트워크에 있는 ESXi 어댑터의 IP 주소입니다.
   - 로컬 스냅샷을 사용하여 볼륨을 보호하는 데 사용되는 스냅샷 스케줄입니다.
   - 선택적으로 볼륨을 백업하거나 볼륨에 대한 레이블을 만듭니다.

> NetApp 볼륨에서 GCVE 데이터 저장소로 사용할 볼륨을 생성할 때 NFS v3만 지원됩니다.

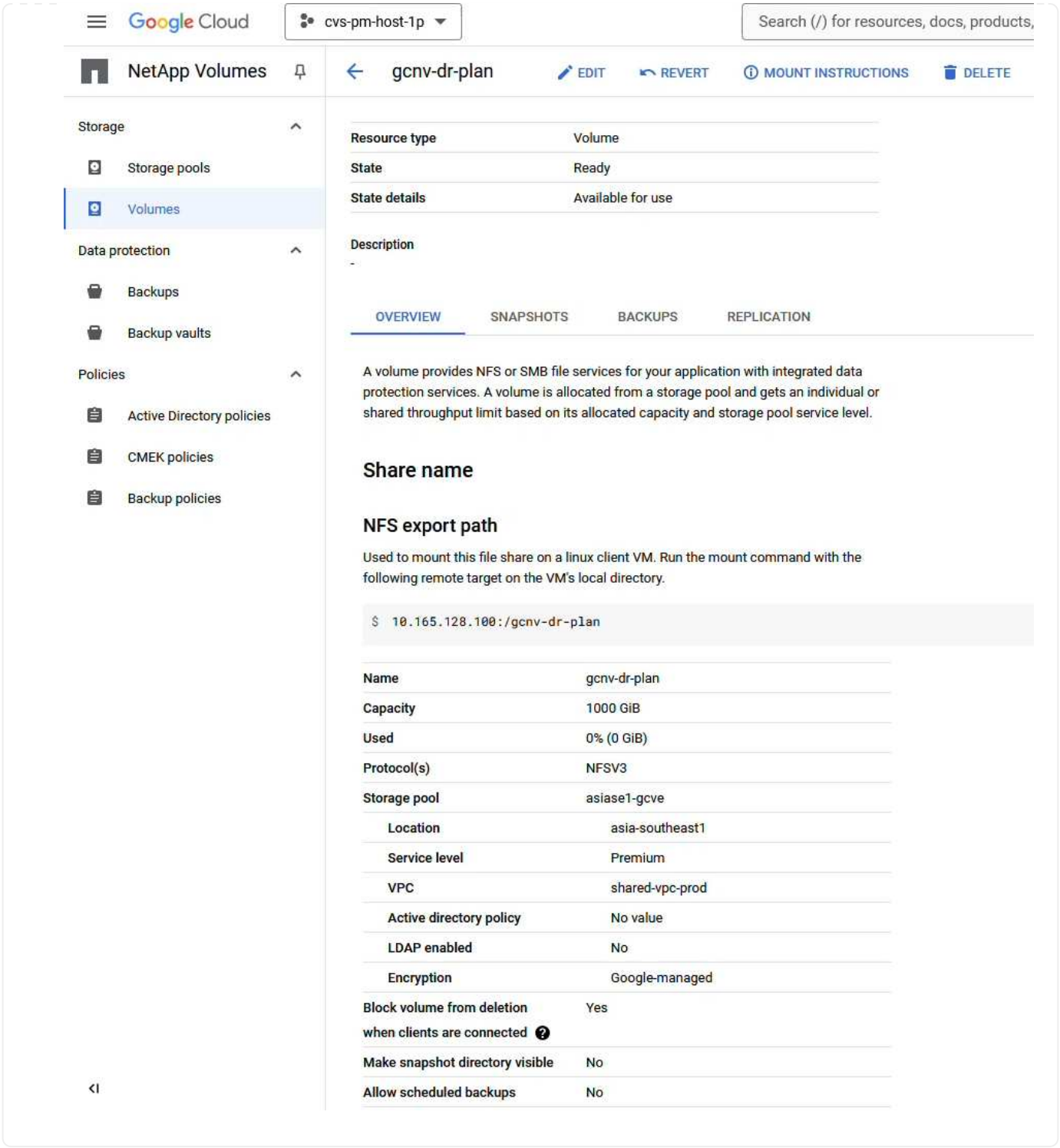

Google Cloud
cvs-pm-host-1p
Search (/) for resources, docs, produ
NetApp Volumes
Create a volume
Storage
Storage pools
Volumes
Data protection
Backups
Backup vaults
Policies
Active Directory policies
CMEK policies
Backup policies
A volume provides NFS or SMB file services for your application with integrated data protection services. A volume is allocated from a storage pool and gets an individual or shared throughput limit based on its allocated capacity and storage pool service level.
Learn more
Volume name *
gcnv-dr-plan
Choice is permanent. Must be unique to the region. Use lowercase letters, numbers, hyphens and underscores. Start with a letter.
Description
Storage pool details
Select a storage pool in which to create the volume
SELECT STORAGE POOL
CREATE NEW STORAGE POOL
Volume details
Share name *
Must be unique to a location
Capacity *
GiB
Capacity must be between 100 GiB and 102,400 GiB. Increments of 1 GiB
Protocol(s) *
NFSv3
Configuration for selected protocol(s)
Block volume from deletion when clients are connected
Required for volumes used as GCVE datastores. Choice is permanent.
Export rules
Snapshot configuration
CREATE
CANCEL


Select a storage pool
Storage pools
Name
Location
Available capacity
Service level
VPC
Active Directory
LDAP enabled
asiase1-gcve
asia-southeast1
1548 GiB
Premium
shared-vpc-prod
No
asiase1-gcve-extreme
0 GiB
Extreme
asia-southeast1-ad
gcnv-data-pool
asia-south1
1014 GiB
Flex
gcve-cert-nvimal
southamerica-east1
524 GiB
montreal-premium
northamerica-northeast1
1148 GiB
montreal-ad
ok-at-pool
998 GiB
ranvind-db-perftest
asia-south1-a
1536 GiB
ranvind-std1
1948 GiB
Standard
ranvind-std2
australia-southeast1
1748 GiB
ranvind-vertexai
769 GiB
sp-1p-se-e1-gcve-ds02
test
me-west1-b
1024 GiB
vaishnav-pool1
1792 GiB
Rows per page:
50
1 – 13 of 13
SELECT
CANCEL



Create * 를 클릭하여 볼륨 생성을 마칩니다.

4. 볼륨이 생성되면 볼륨을 마운트하는 데 필요한 NFS 내보내기 경로를 볼륨의 속성 페이지에서 볼 수 있습니다.



GCVE에서 **NFS** 데이터 저장소를 마운트합니다

이 쓰기 작업을 수행할 때 GCVE에서 데이터 저장소를 마운트하는 프로세스에서는 볼륨을 NFS 데이터 저장소로 마운트하기 위해 GCP 지원 티켓을 열어야 합니다.

자세한 내용은 을 "NFS 볼륨을 Google Cloud NetApp 볼륨에서 호스팅하는 vSphere 데이터 저장소로 사용합니다" 참조하십시오.

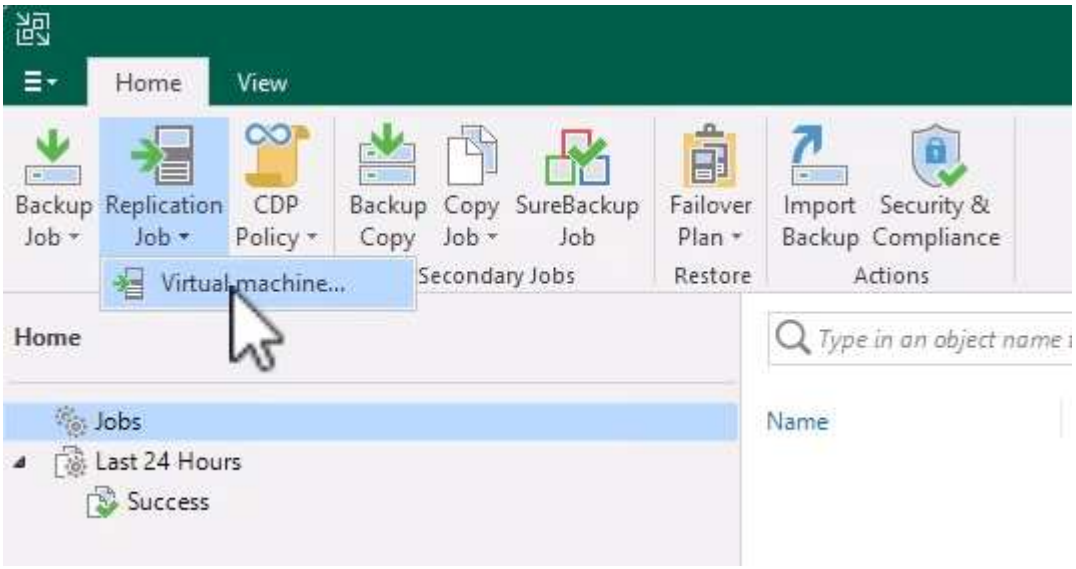
VM을 **GCVE**에 복제하고 페일오버 계획 및 페일백을 실행합니다

GCVE에서 **VM**을 **NFS** 데이터 저장소로 복제합니다

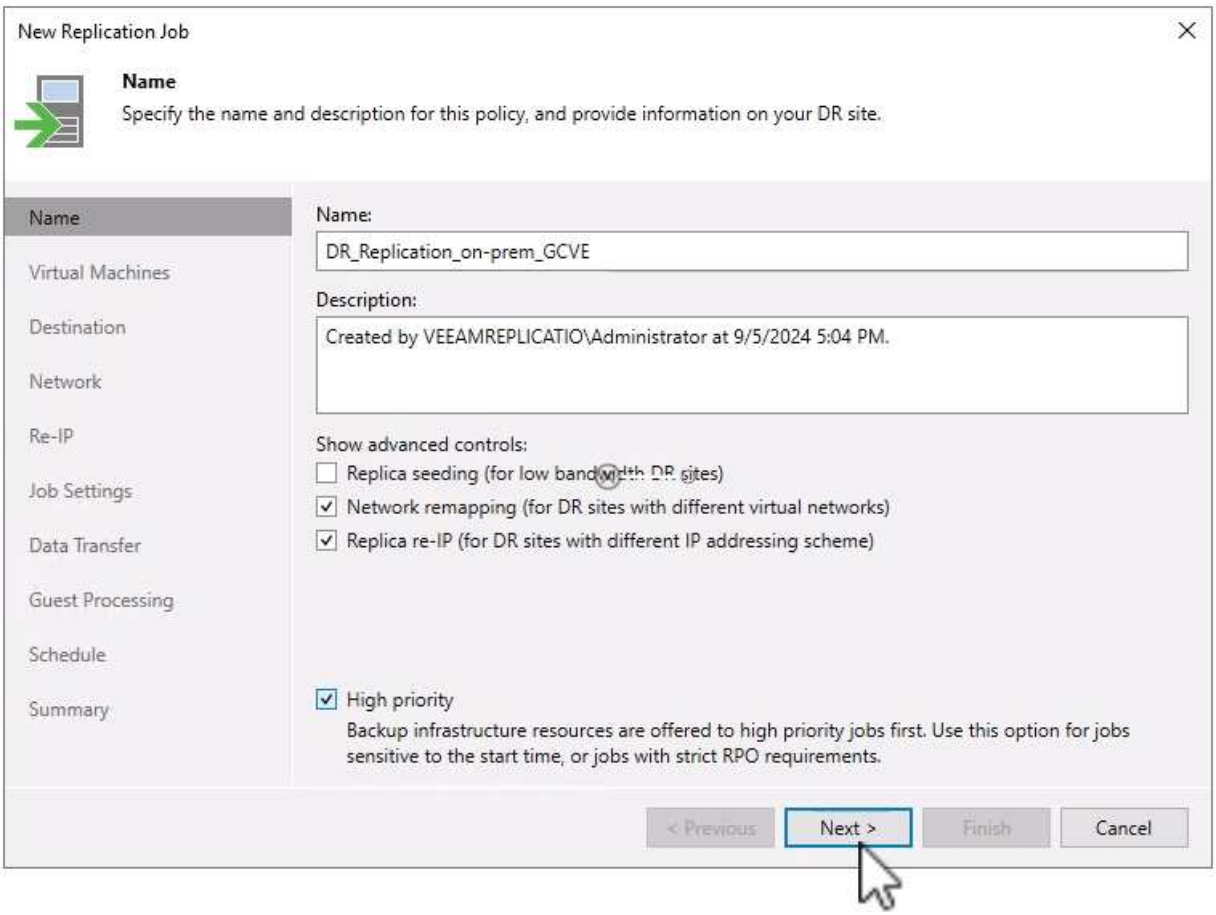
Veeam Backup & Replication은 VMware vSphere 스냅샷 기능을 활용합니다. 복제 중에 Veeam Backup & Replication은 VMware vSphere에 VM 스냅샷을 생성하도록 요청합니다. VM 스냅샷은 가상 디스크, 시스템 상태, 구성 및 메타데이터를 포함하는 VM의 시점 복제본입니다. Veeam Backup & Replication은 이 스냅샷을 복제용 데이터 소스로 사용합니다.

VM을 복제하려면 다음 단계를 완료합니다.

1. Veeam Backup & Replication Console을 엽니다.
2. 홈 * 탭에서 * 복제 작업 > 가상 머신… * 을 클릭합니다

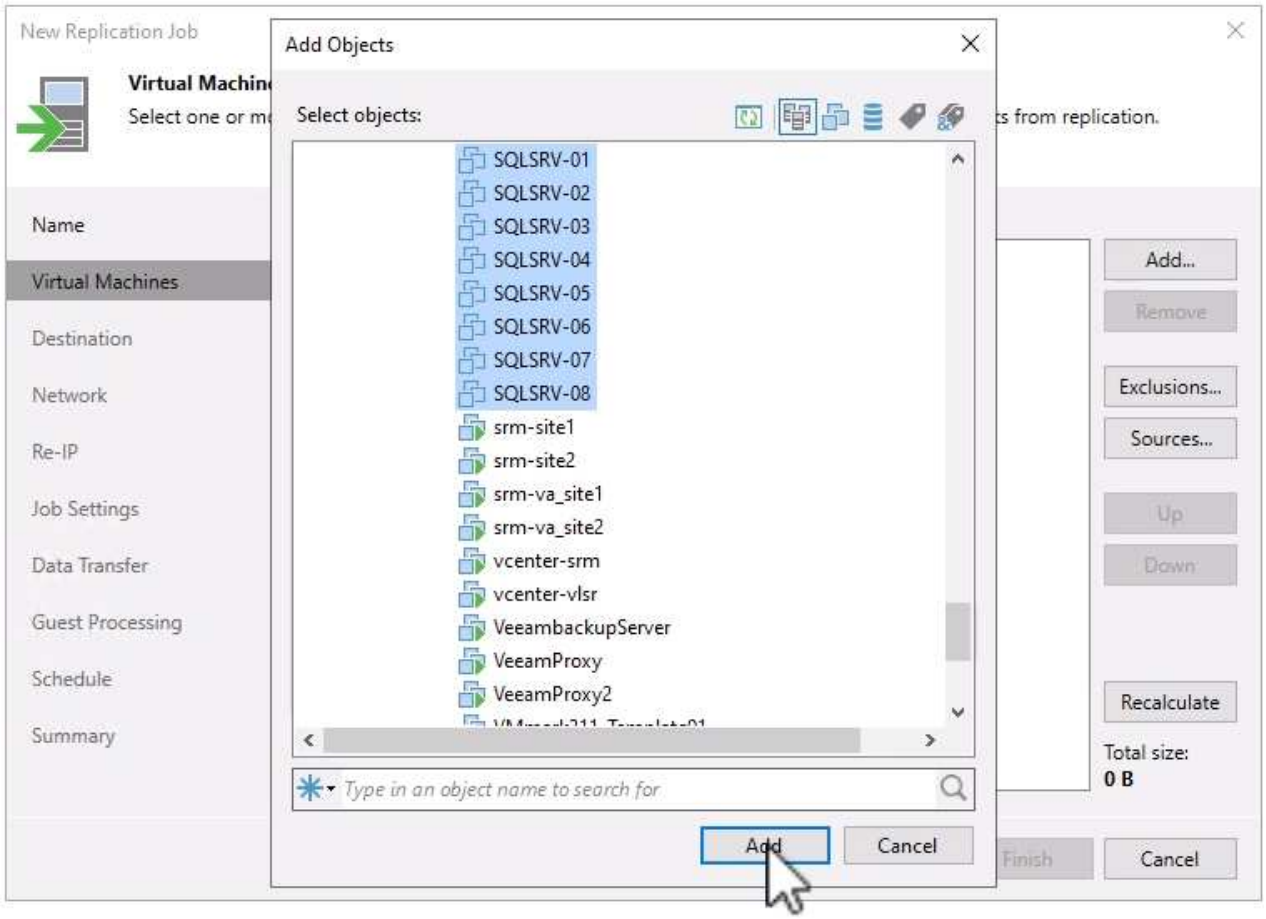


3. 새 복제 작업 * 마법사의 * 이름 * 페이지에서 작업 이름을 지정하고 해당 고급 제어 확인란을 선택합니다.
   - 온-프레미스와 GCP 간의 접속 대역폭이 제한된 경우 복제 시드 확인란을 선택합니다.
   - GCVE SDDC의 세그먼트가 온-프레미스 사이트 네트워크의 세그먼트와 일치하지 않으면 네트워크 재매핑(다른 네트워크를 가진 GCVE SDDC 사이트의 경우) 확인란을 선택합니다.
   - 온-프레미스 프로덕션 사이트의 IP 주소 지정 스키마가 대상 GCVE 사이트의 스키마와 다른 경우 복제 Re-IP(IP 주소 지정 스키마가 다른 DR 사이트의 경우) 확인란을 선택합니다.

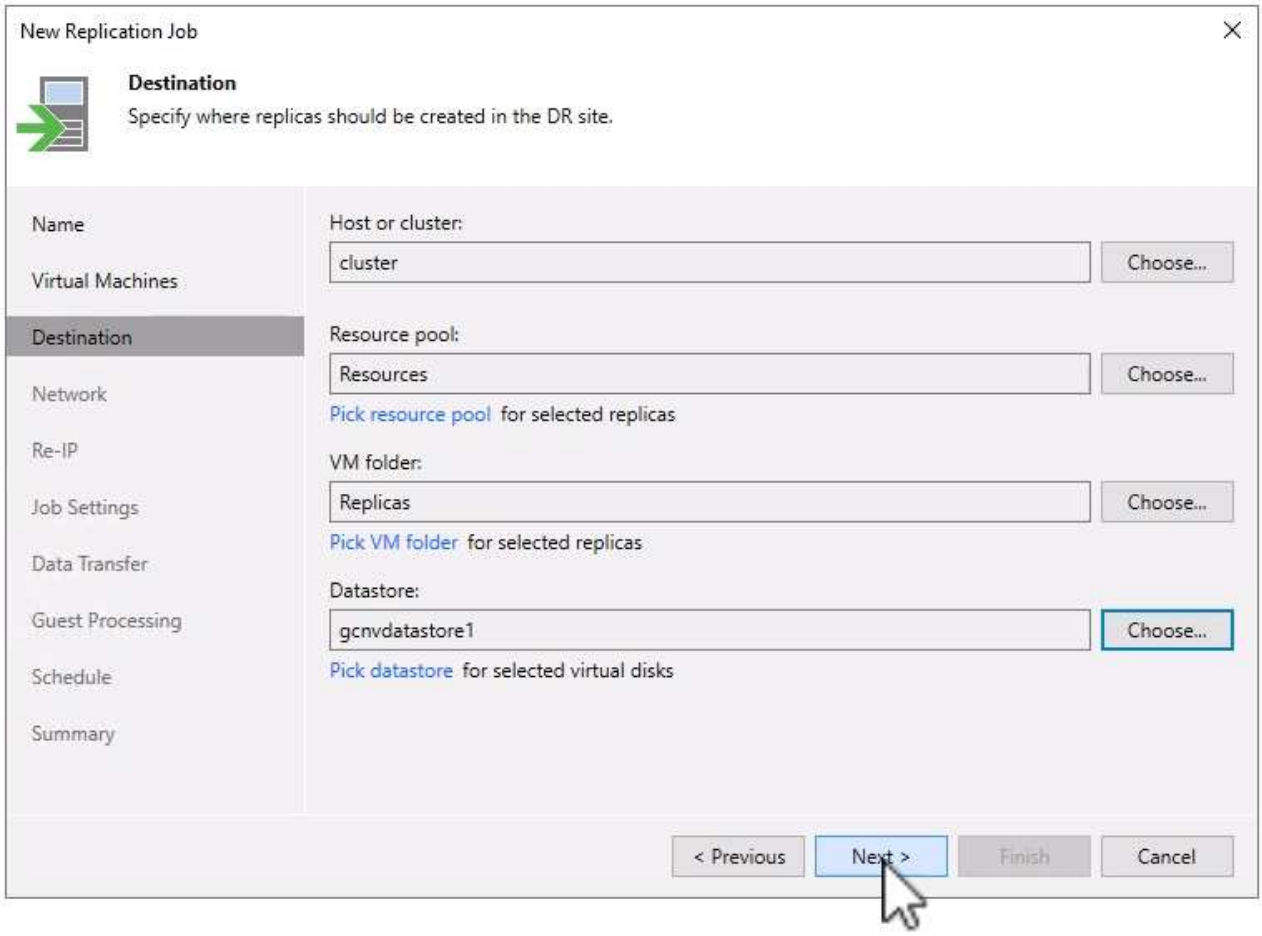


4. 가상 머신 * 페이지에서 GCVE SDDC에 연결된 NetApp 볼륨 데이터 저장소에 복제할 VM을 선택합니다. Add * 를 클릭한 다음 * Add Object * 창에서 필요한 VM 또는 VM 컨테이너를 선택하고 * Add * 를 클릭합니다. 다음 * 을 클릭합니다.

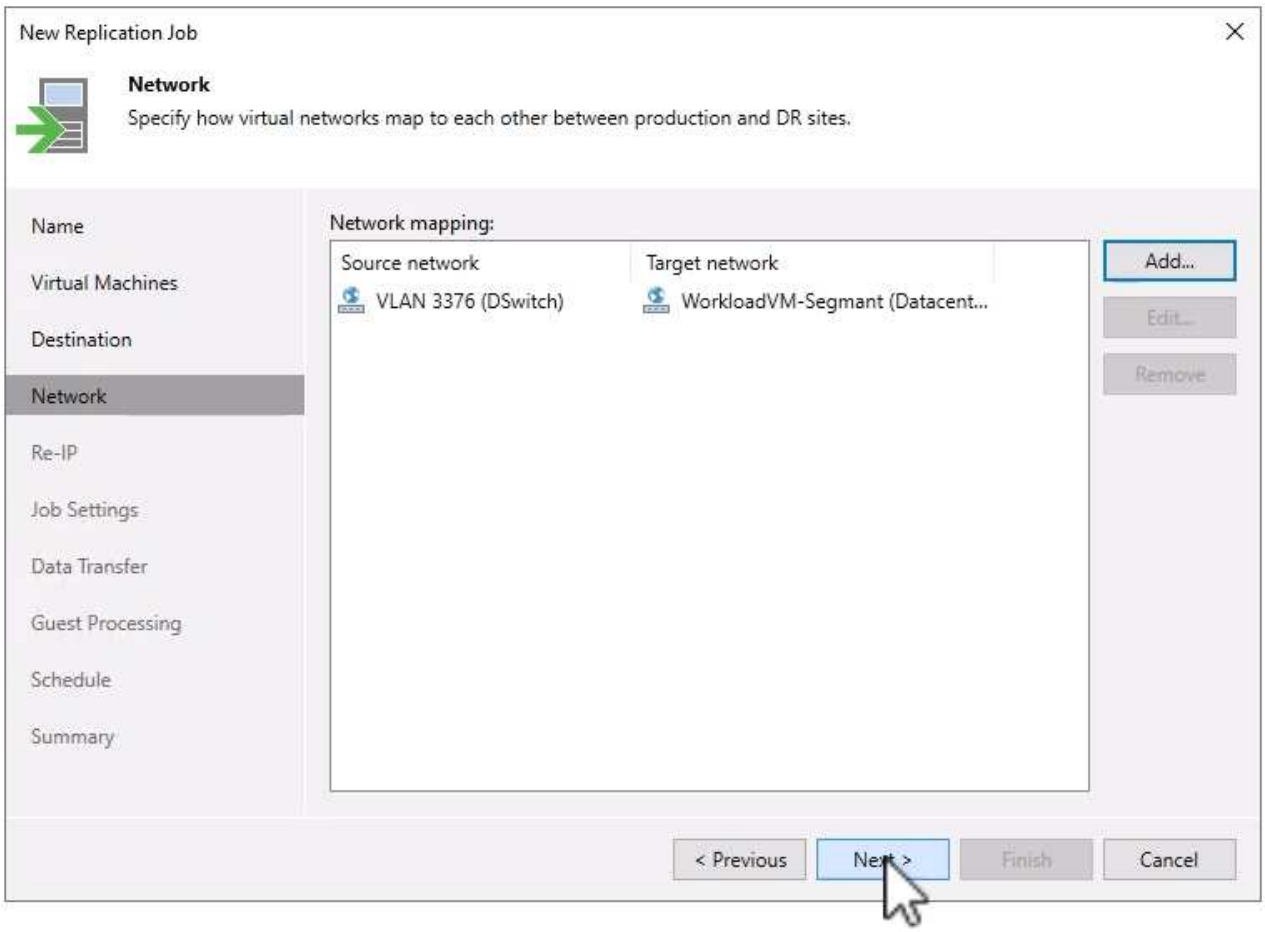
vSAN에 가상 머신을 배치하여 사용 가능한 vSAN 데이터스토어 용량을 채울 수 있습니다. 파일럿 라이트 클러스터에서는 3노드 vSAN 클러스터의 가용 용량이 제한됩니다. 나머지 데이터는 Google Cloud NetApp Volumes 데이터 저장소에 쉽게 배치하여 VM을 복구할 수 있으며, 나중에 CPU/메모리 요구사항을 충족하도록 클러스터를 확장할 수 있습니다.



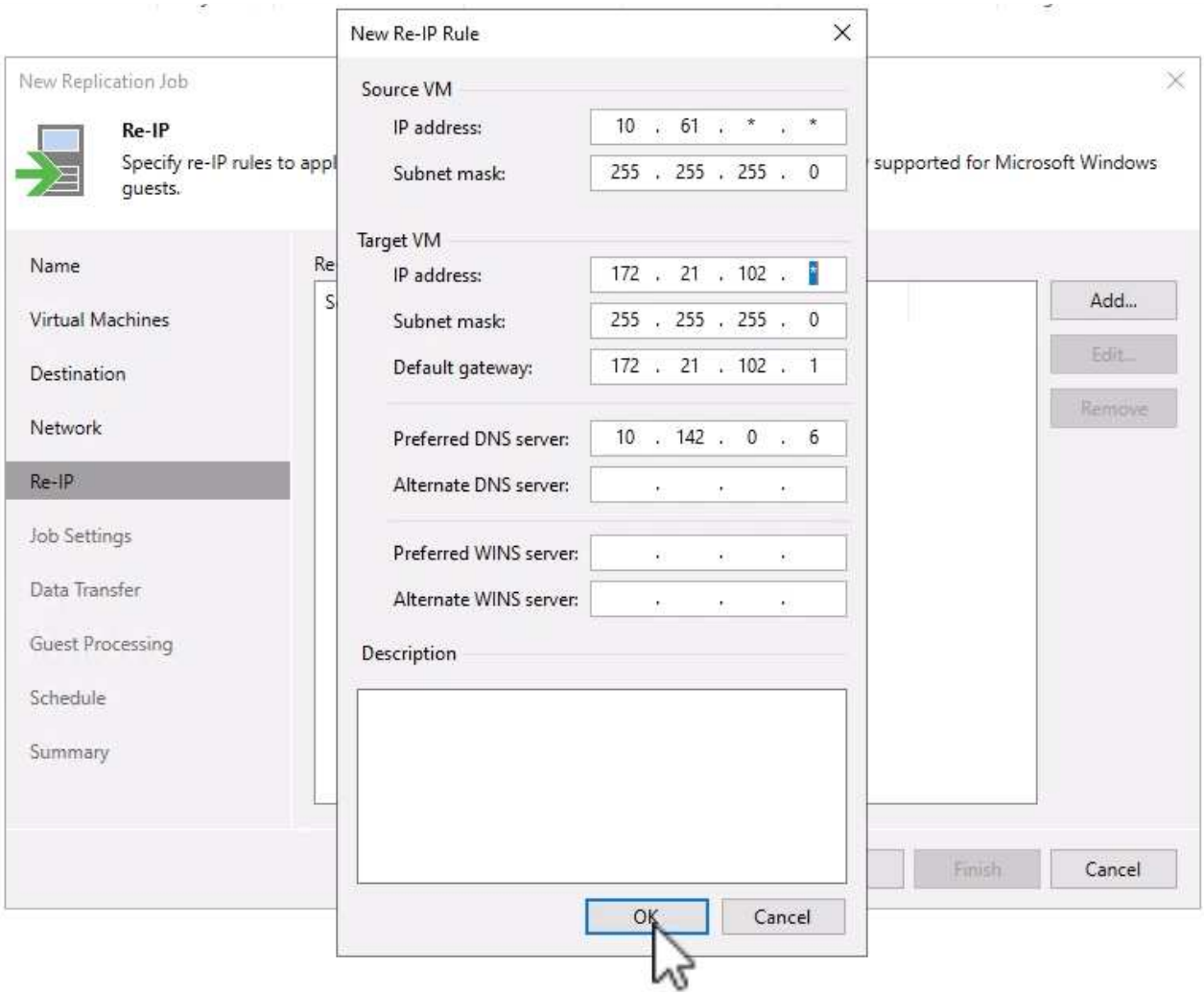
5. Destination * 페이지에서 대상을 GCVE SDDC 클러스터/호스트 및 VM 복제본에 대한 적절한 리소스 풀, VM 폴더 및 GCNV 데이터 저장소로 선택합니다. 계속하려면 * 다음 * 을 클릭합니다.



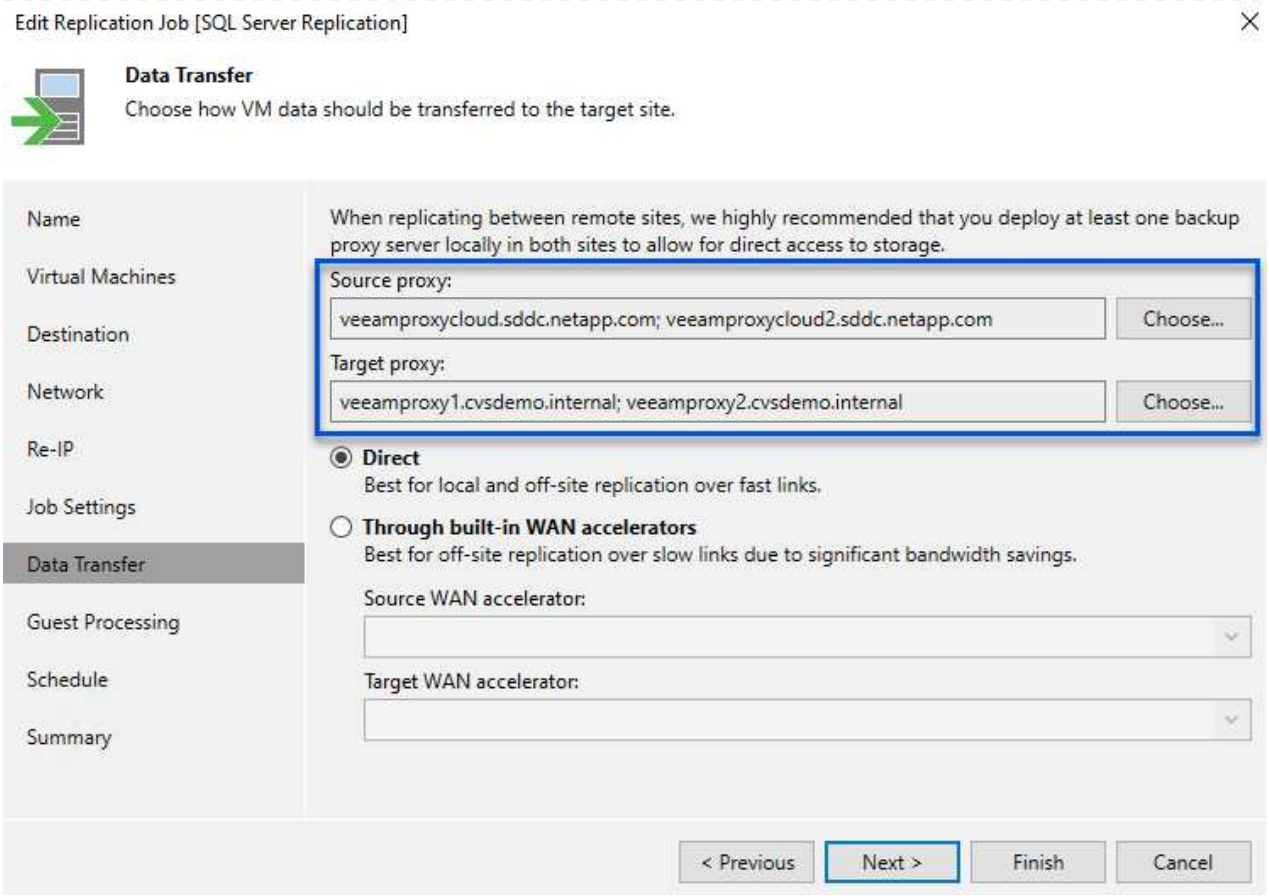
6. 네트워크 * 페이지에서 필요에 따라 소스 및 대상 가상 네트워크 간의 매핑을 생성합니다. 계속하려면 * 다음 * 을 클릭합니다.



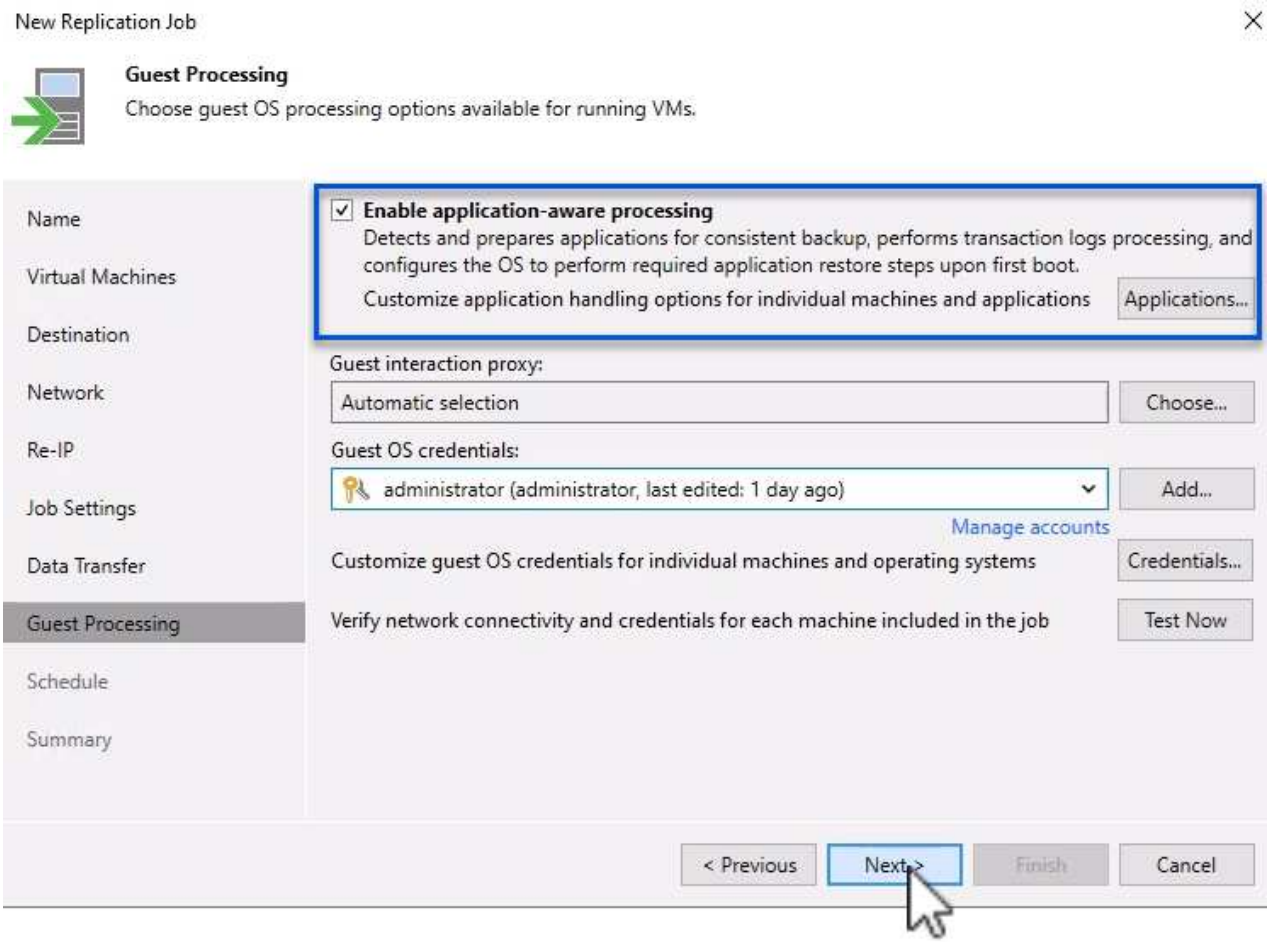
7. Re-IP * 페이지에서 * Add… * 버튼을 클릭하여 새 Re-IP 규칙을 추가합니다. 소스 및 타겟 VM IP 범위를 입력하여 페일오버 시 소스 VM에 적용할 네트워킹을 지정합니다. 별표를 사용하여 해당 옥텟에 대한 주소 범위를 지정합니다. 계속하려면 * 다음 * 을 클릭합니다.



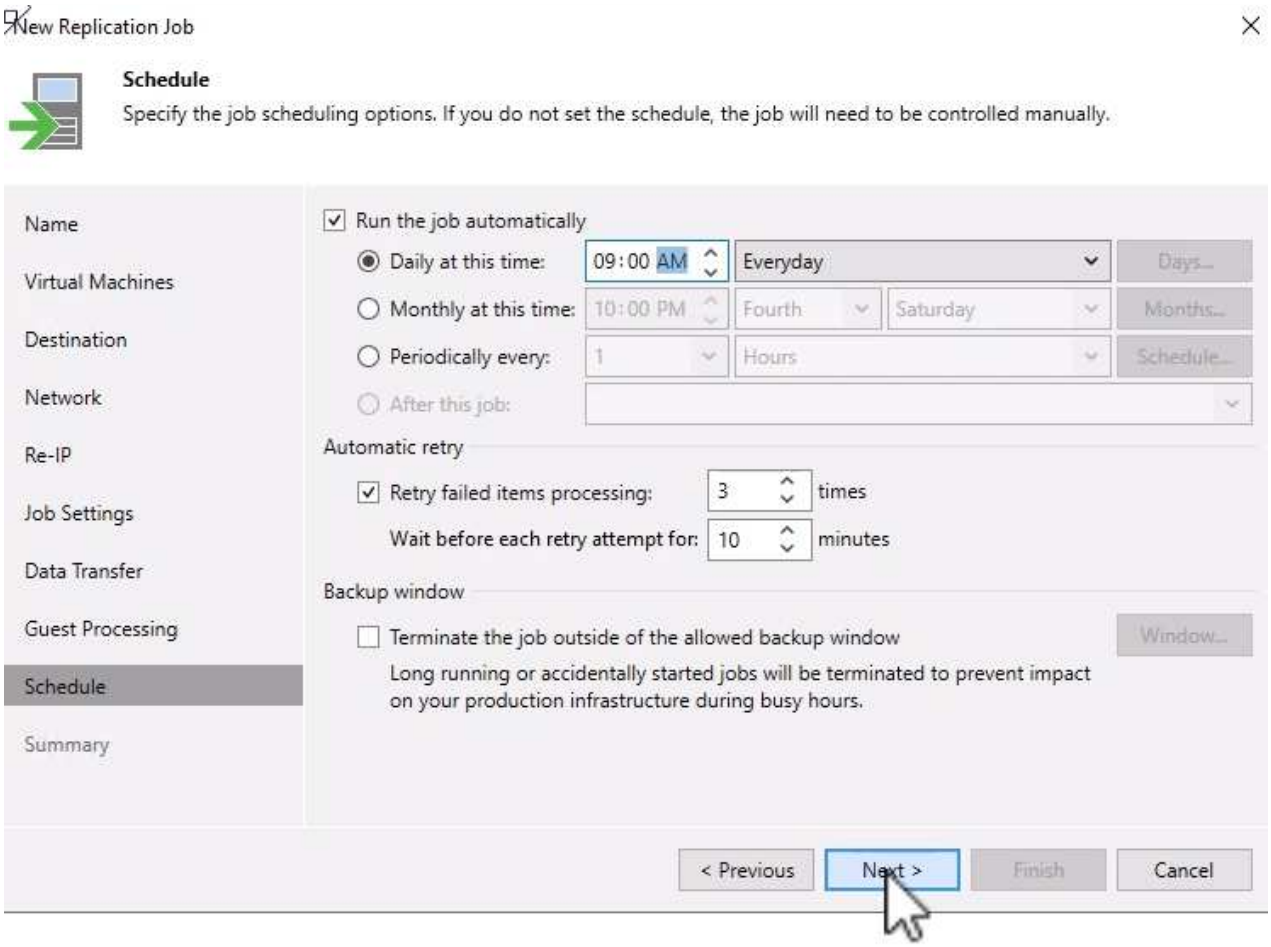
8. 작업 설정 * 페이지에서 VM 복제본에 대한 메타데이터를 저장할 백업 리포지토리 및 보존 정책을 지정하고 하단의 * 고급… * 버튼을 선택하여 추가 작업 설정을 확인합니다. 계속하려면 * 다음 * 을 클릭합니다.
9. 데이터 전송 * 에서 소스 및 대상 사이트에 상주하는 프록시 서버를 선택하고 직접 옵션을 선택한 상태로 유지합니다. WAN 가속기는 구성된 경우 여기에서 선택할 수도 있습니다. 계속하려면 * 다음 * 을 클릭합니다.



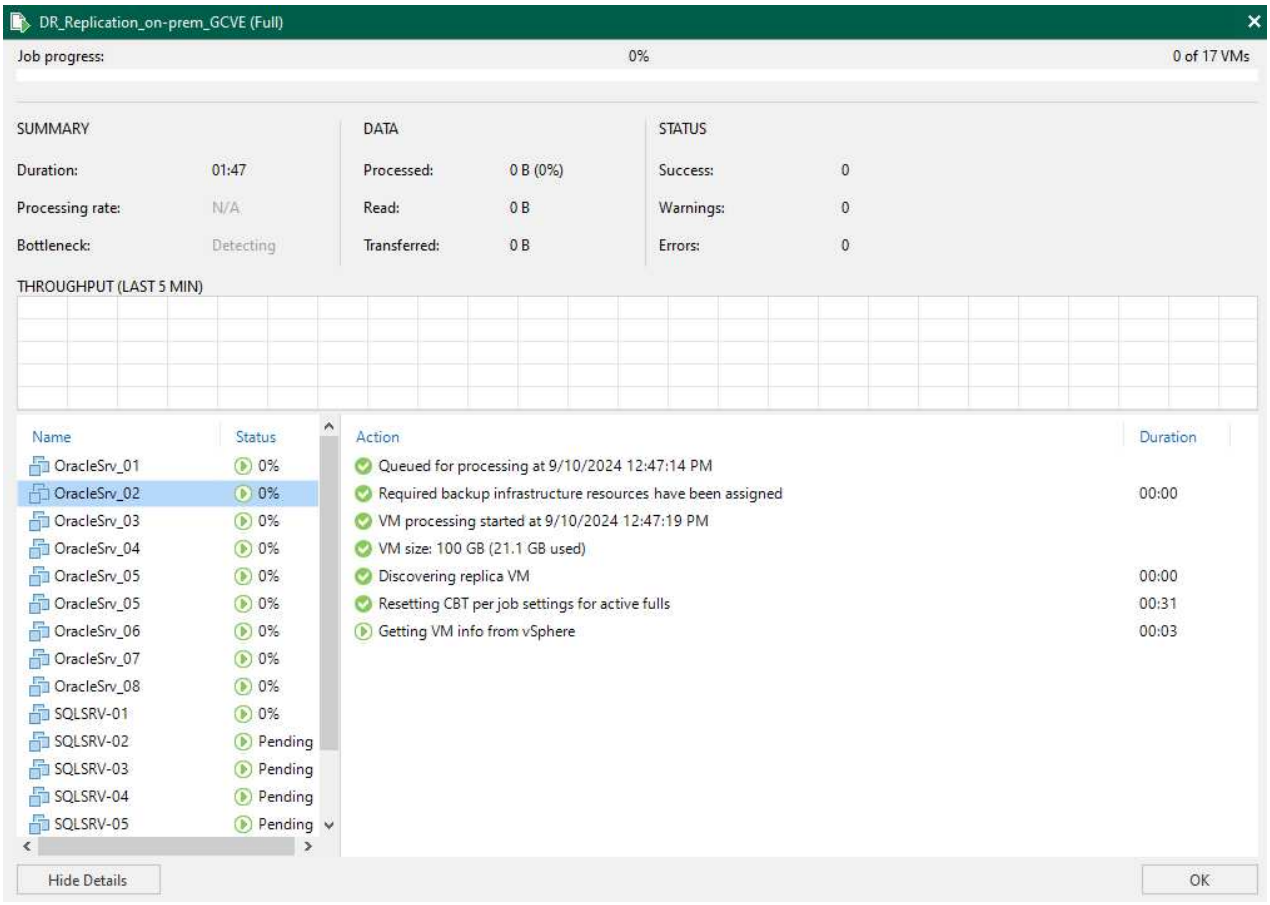
10. Guest Processing * 페이지에서 필요에 따라 * Enable application-aware processing * 확인란을 선택하고 * Guest OS credentials * 를 선택합니다. 계속하려면 * 다음 * 을 클릭합니다.



11. Schedule * 페이지에서 복제 작업이 실행되는 시간과 빈도를 정의합니다. 계속하려면 * 다음 * 을 클릭합니다.



12. 마지막으로 * 요약 * 페이지에서 작업 설정을 검토합니다. Finish * 를 클릭하면 작업 실행 확인란을 선택하고 * Finish * 를 클릭하여 복제 작업 생성을 완료합니다.
13. 복제 작업을 실행하면 작업 상태 창에서 복제 작업을 볼 수 있습니다.



Veeam 복제에 대한 자세한 내용은 을 참조하십시오 "복제 작동 방법"

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 장애 조치 계획을 통해 중요한 종속 VM이 이미 실행 중인지 확인할 수 있습니다.

초기 복제 또는 시드를 완료한 후 페일오버 계획을 생성합니다. 이 계획은 종속 VM의 장애 조치를 개별적으로 또는 그룹으로 조정하기 위한 전략적 청사진 역할을 합니다. VM의 처리 순서를 정의하고, 필요한 부팅 지연을 통합하고, 중요한 종속 VM이 다른 VM보다 먼저 작동하도록 보장합니다. 체계적인 장애 조치 계획을 구현함으로써 조직은 재해 복구 프로세스를 능률화하고, 장애 조치 이벤트 중에 상호 의존적인 시스템의 무결성을 유지할 수 있습니다.

계획을 생성할 때 Veeam Backup & Replication은 자동으로 최신 복구 지점을 식별하고 사용하여 VM 복제를 시작합니다.

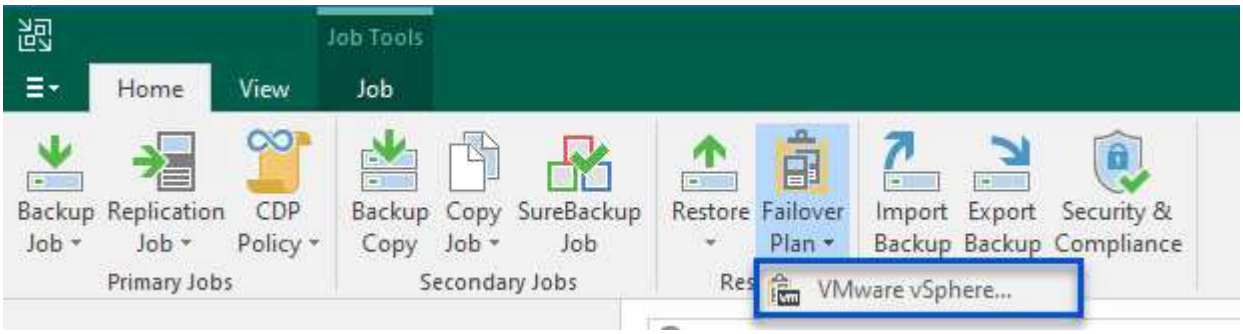
ⓘ 초기 복제가 완료되고 VM 복제본이 준비 상태가 된 후에만 페일오버 계획을 생성할 수 있습니다.

ⓘ 페일오버 계획을 실행할 때 동시에 시작할 수 있는 최대 VM 수는 10개입니다.

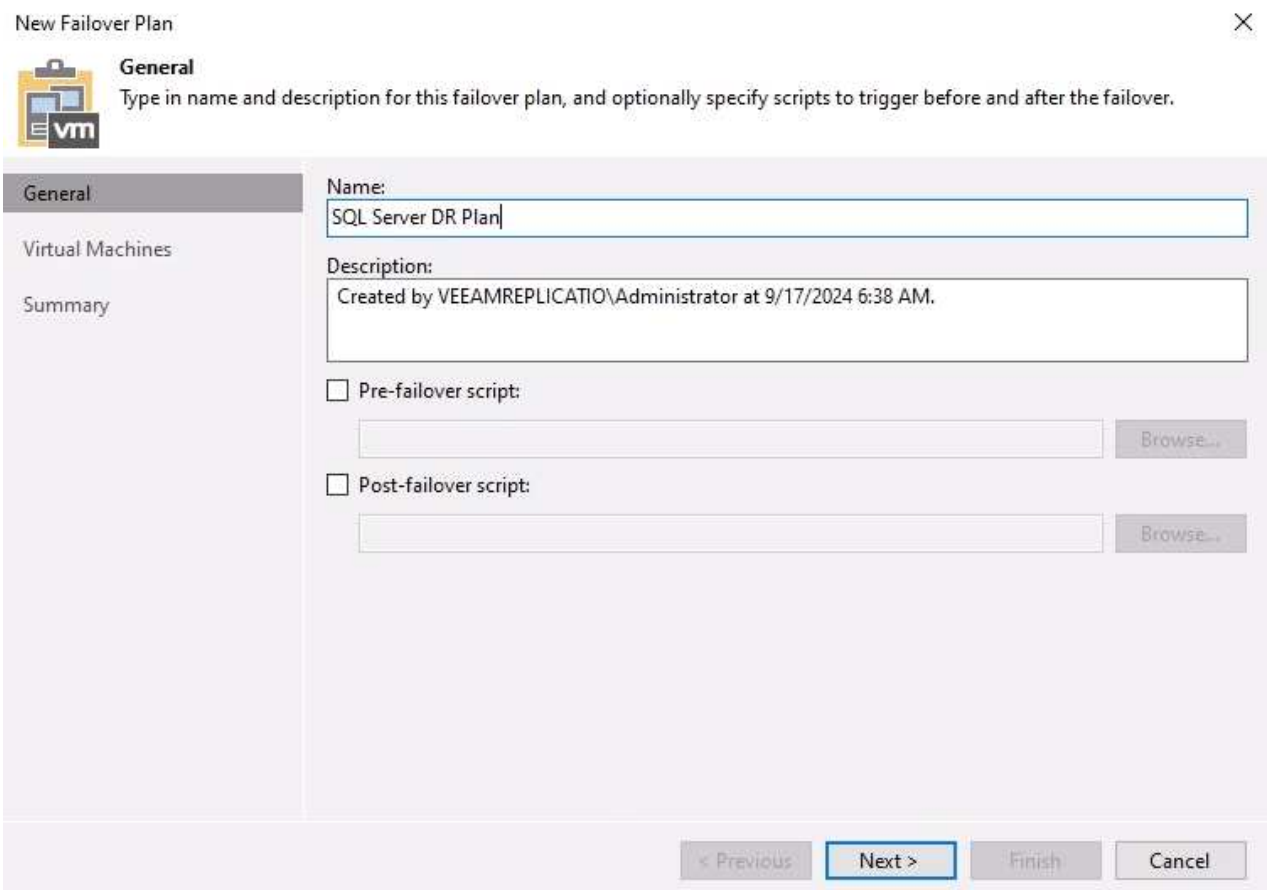
ⓘ 페일오버 프로세스 중에는 소스 VM의 전원이 꺼지지 않습니다.

장애 조치 계획 * 을 작성하려면 다음 단계를 수행하십시오.

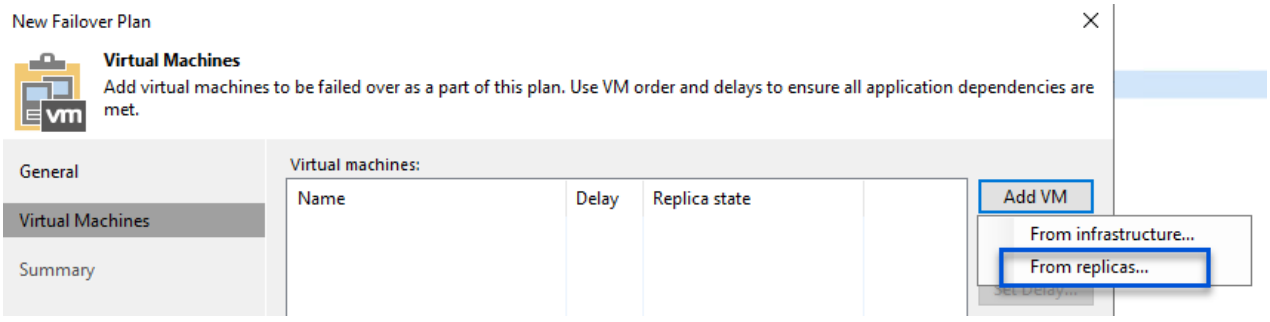
1. Home * 보기에서 * Restore * 섹션에 있는 * Failover Plan * 버튼을 클릭합니다. 드롭다운에서 * VMware vSphere… * 를 선택합니다

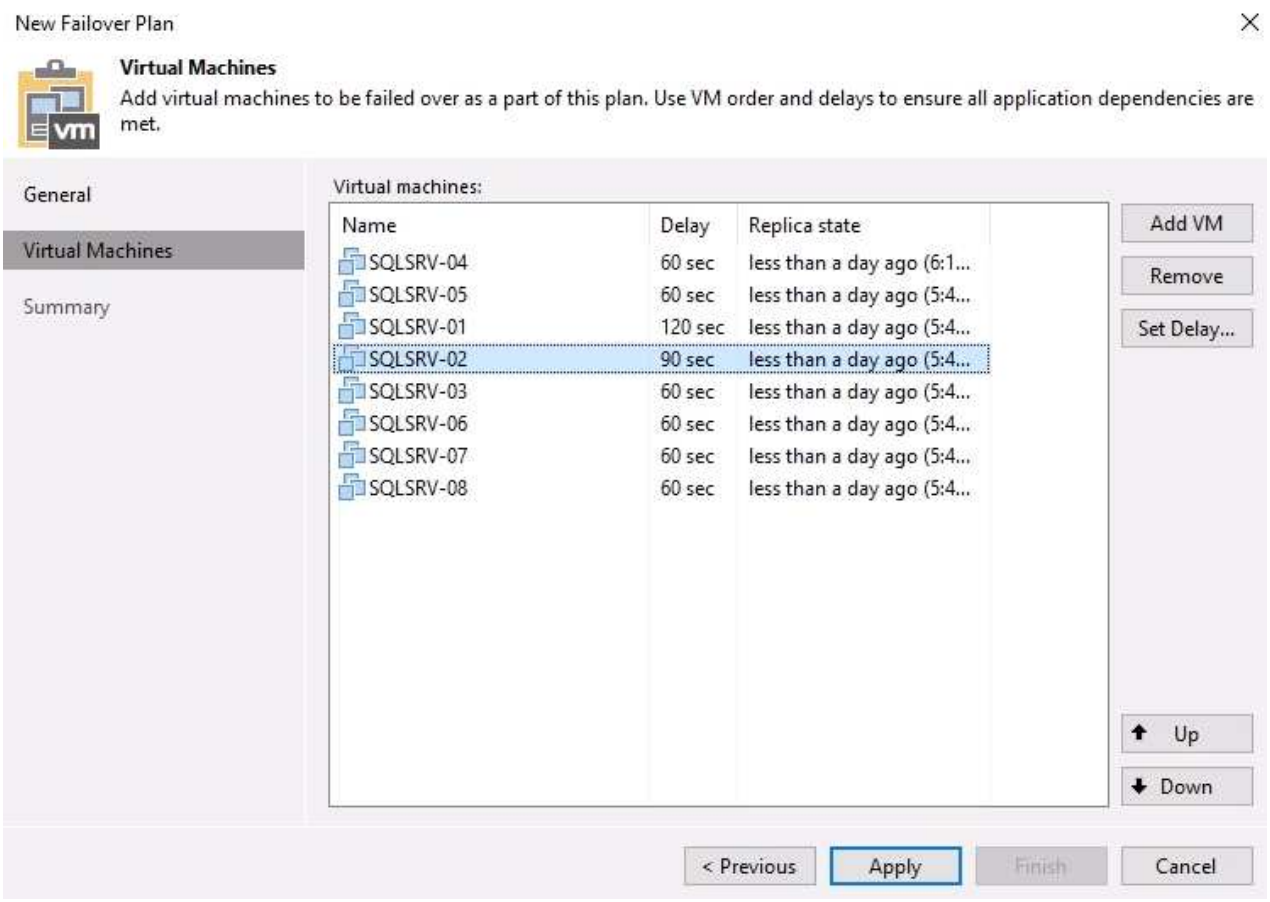


2. New Failover Plan * 마법사의 * General * 페이지에서 계획에 대한 이름과 설명을 입력합니다. 필요에 따라 사전 및 사후 페일오버 스크립트를 추가할 수 있습니다. 예를 들어 복제된 VM을 시작하기 전에 VM을 종료하는 스크립트를 실행합니다.



3. Virtual Machines * 페이지에서 * Add VM * 버튼을 클릭하고 * from Replicas… * 를 선택합니다. 페일오버 계획에 포함될 VM을 선택한 다음 애플리케이션 종속성을 충족하도록 VM 부팅 순서 및 필요한 부팅 지연을 수정합니다.





계속하려면 * 적용 * 을 클릭하십시오.

4. 마지막으로 모든 장애 조치 계획 설정을 검토하고 * Finish * 를 클릭하여 장애 조치 계획을 생성합니다.

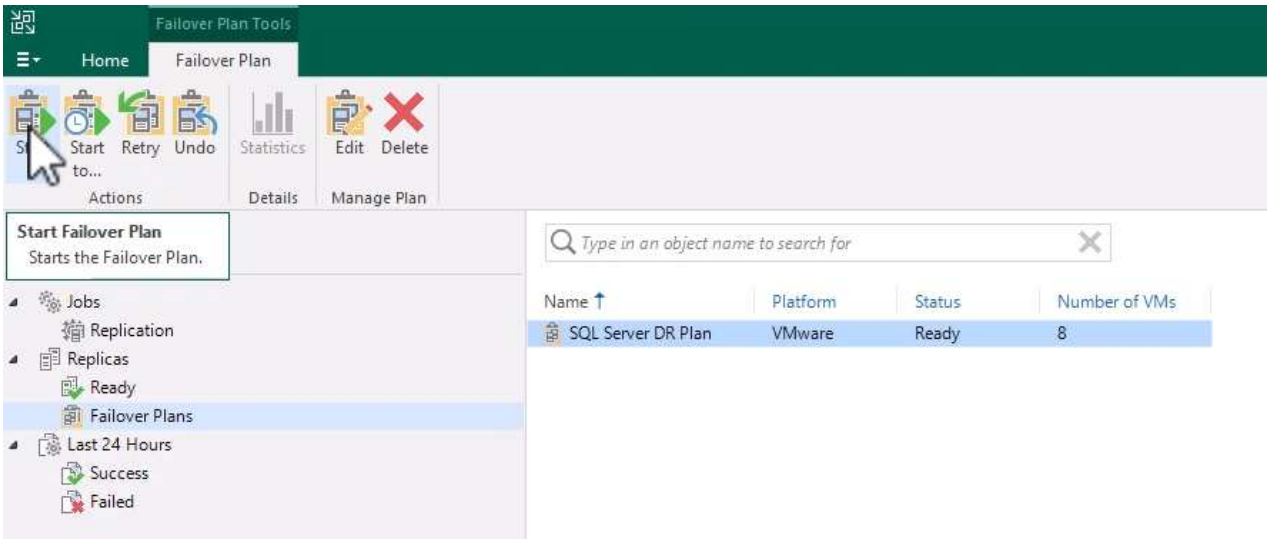
복제 작업 생성에 대한 자세한 내용은 을 "복제 작업을 생성하는 중입니다"참조하십시오.

페일오버 중에 프로덕션 사이트의 소스 VM이 재해 복구 사이트의 해당 복제본으로 전환됩니다. 프로세스의 일부로 Veeam Backup & Replication은 VM 복제본을 필요한 복구 지점으로 복구하고 소스 VM의 모든 입출력 작업을 해당 복제본으로 전송합니다. 복제본은 실제 재해뿐만 아니라 DR 드릴을 시뮬레이션하는 데도 사용됩니다. 장애 조치 시뮬레이션에서는 소스 VM이 계속 실행됩니다. 필요한 테스트가 완료되면 페일오버를 실행 취소하여 작업을 정상 상태로 되돌릴 수 있습니다.

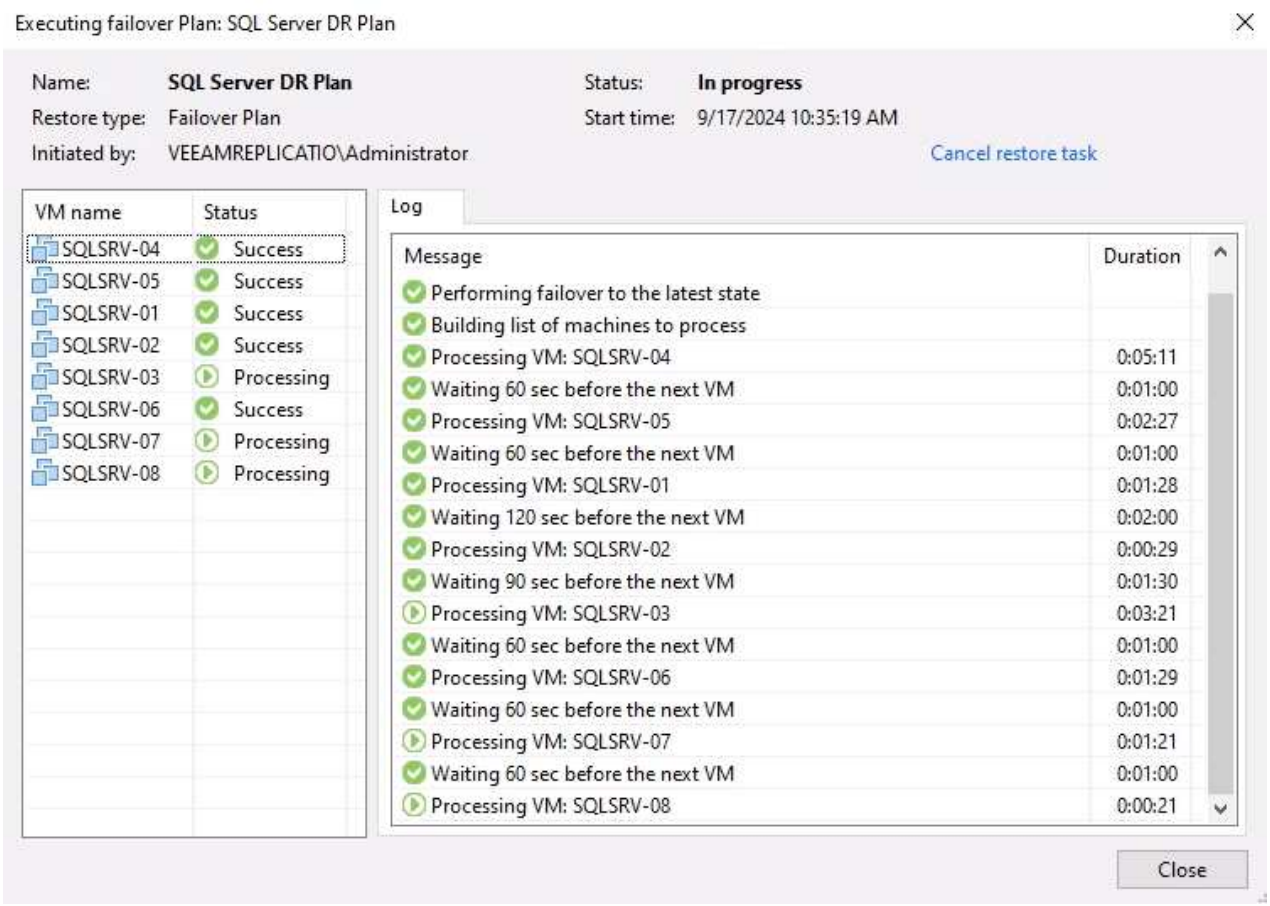
페일오버 중에 IP 충돌을 피하기 위해 네트워크 분할이 제대로 수행되었는지 확인하십시오.

다음 단계를 완료하여 페일오버 계획을 시작합니다.

1. 시작하려면 * Home * 보기에서 왼쪽 메뉴의 * Replicas > Failover Plans * 를 클릭한 다음 * Start * 버튼을 클릭합니다. 또는 * 시작… * 버튼을 사용하여 이전 복원 지점으로 페일오버할 수 있습니다.



2. 장애 조치 계획 실행 * 창에서 장애 조치 진행 상황을 모니터링합니다.



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".

장애 조치 수행은 중간 단계로 간주되며 요구 사항에 따라 완료되어야 합니다. 다음과 같은 옵션이 있습니다.

- * 프로덕션으로 페일백 * - 원래 VM으로 되돌리고 복제본의 활성 기간 동안 수행된 모든 수정 사항을 다시 소스 VM으로 동기화합니다.

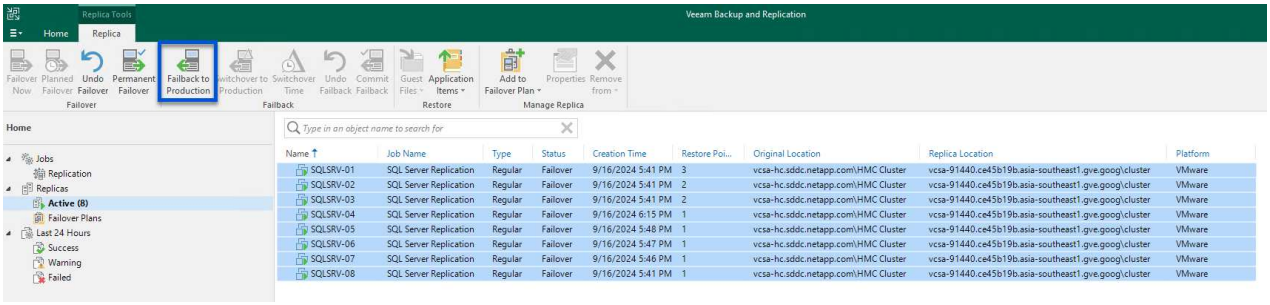
> 장애 복구 중에는 변경 사항이 전송되지만 즉시 적용되지는 않습니다. 원래 VM의 기능이 확인되면 * 페일백 커밋 * 을 선택합니다. 또는 원래 VM이 예상치 못한 동작을 보이는 경우 * 페일백 실행 취소 * 를 선택하여 VM 복제본으로 되돌립니다.

- * 장애 조치 실행 취소 * - 원래 VM으로 되돌리고 운영 기간 동안 VM 복제본의 모든 변경 사항을 취소합니다.
- * 영구 장애 조치 * - 원래 VM에서 해당 복제본으로 영구적으로 전환하여 지속적인 작업을 위해 복제본을 새 기본 VM으로 설정합니다.

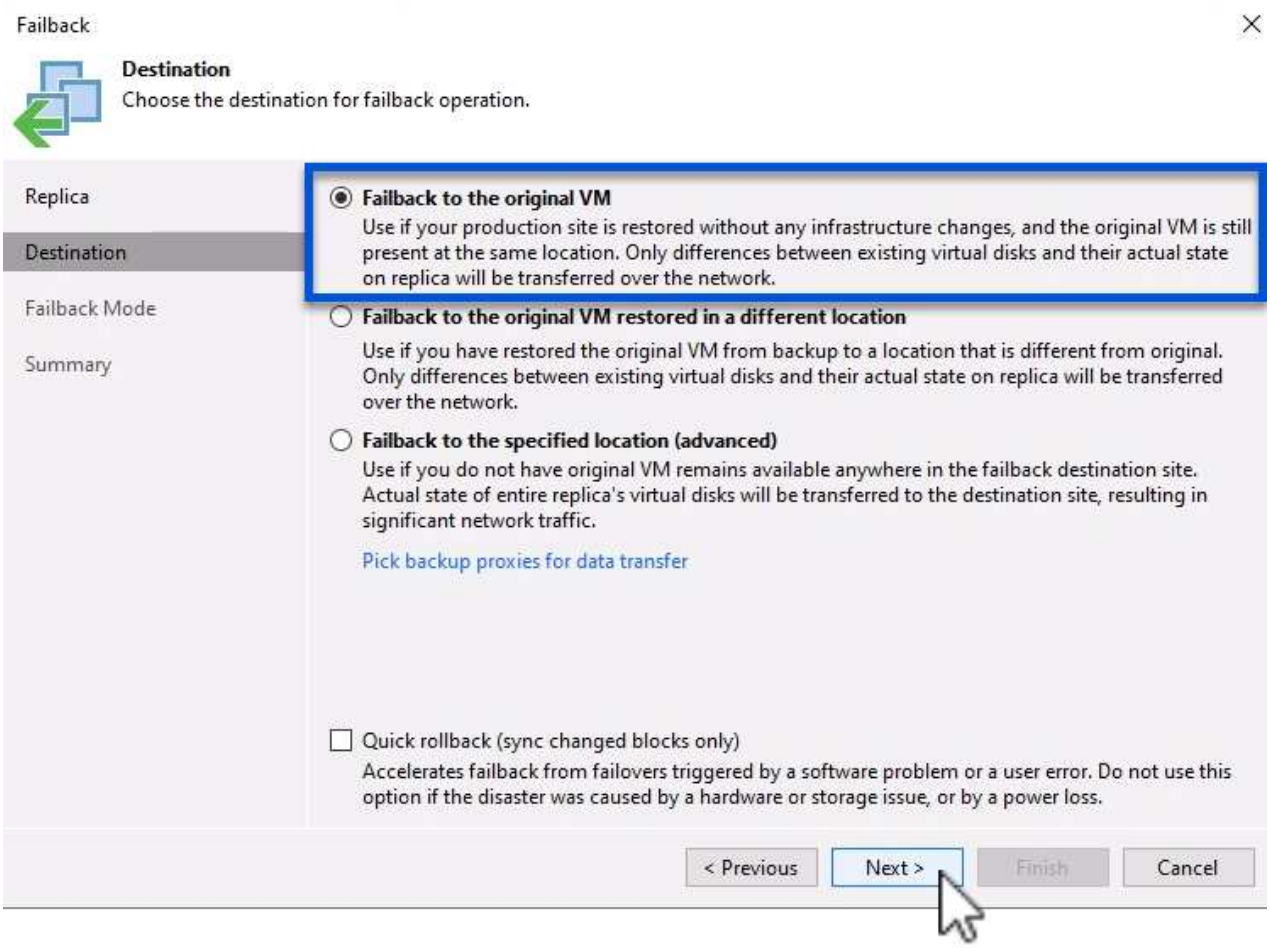
이 시나리오에서는 "Failback to production" 옵션이 선택되었습니다.

운영 사이트로 페일백을 수행하려면 다음 단계를 수행하십시오.

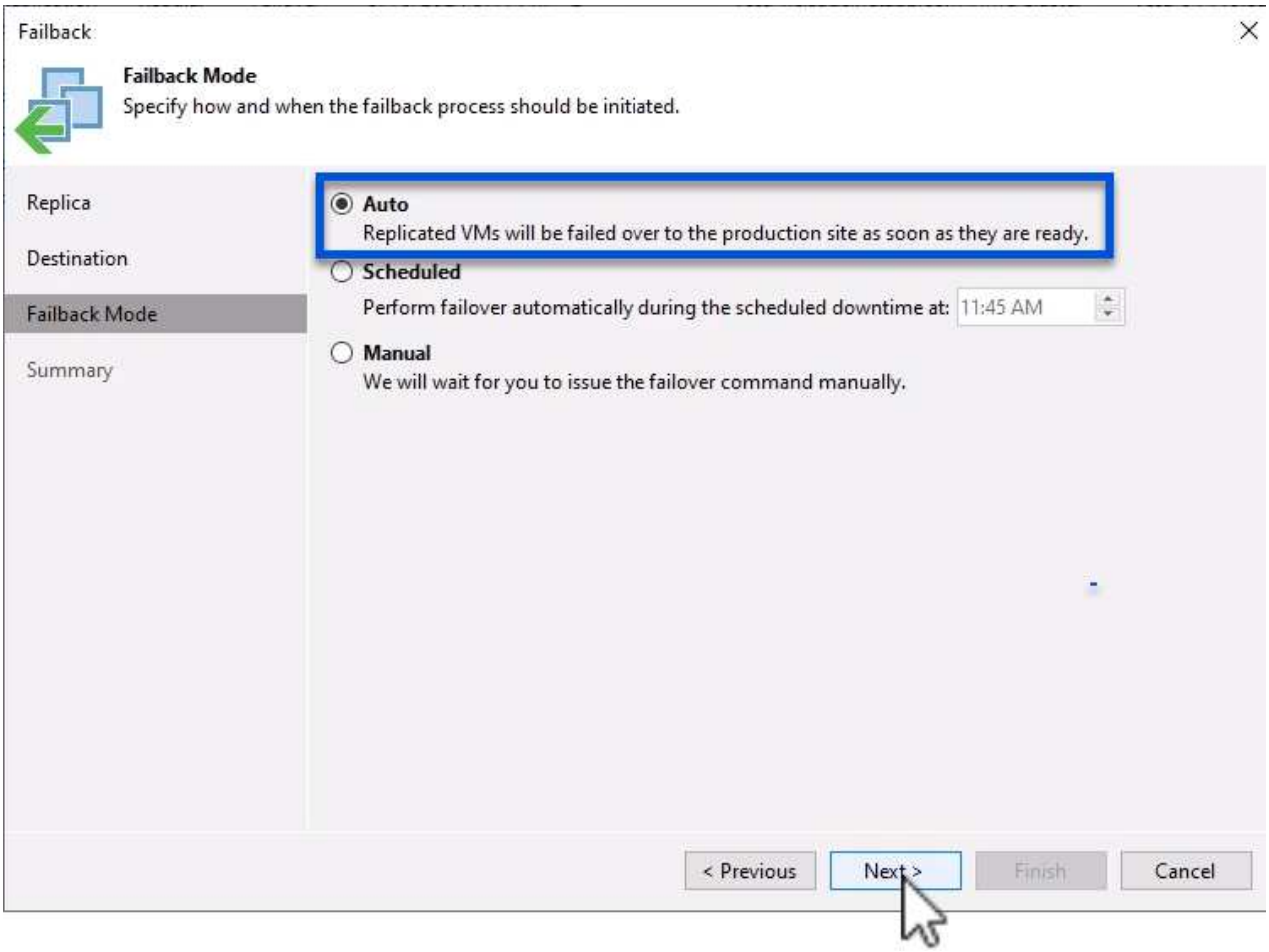
1. Home * 보기의 왼쪽 메뉴에서 * Replicas > Active * 를 클릭합니다. 포함할 VM을 선택하고 상단 메뉴에서 * Failback to Production * 버튼을 클릭합니다.



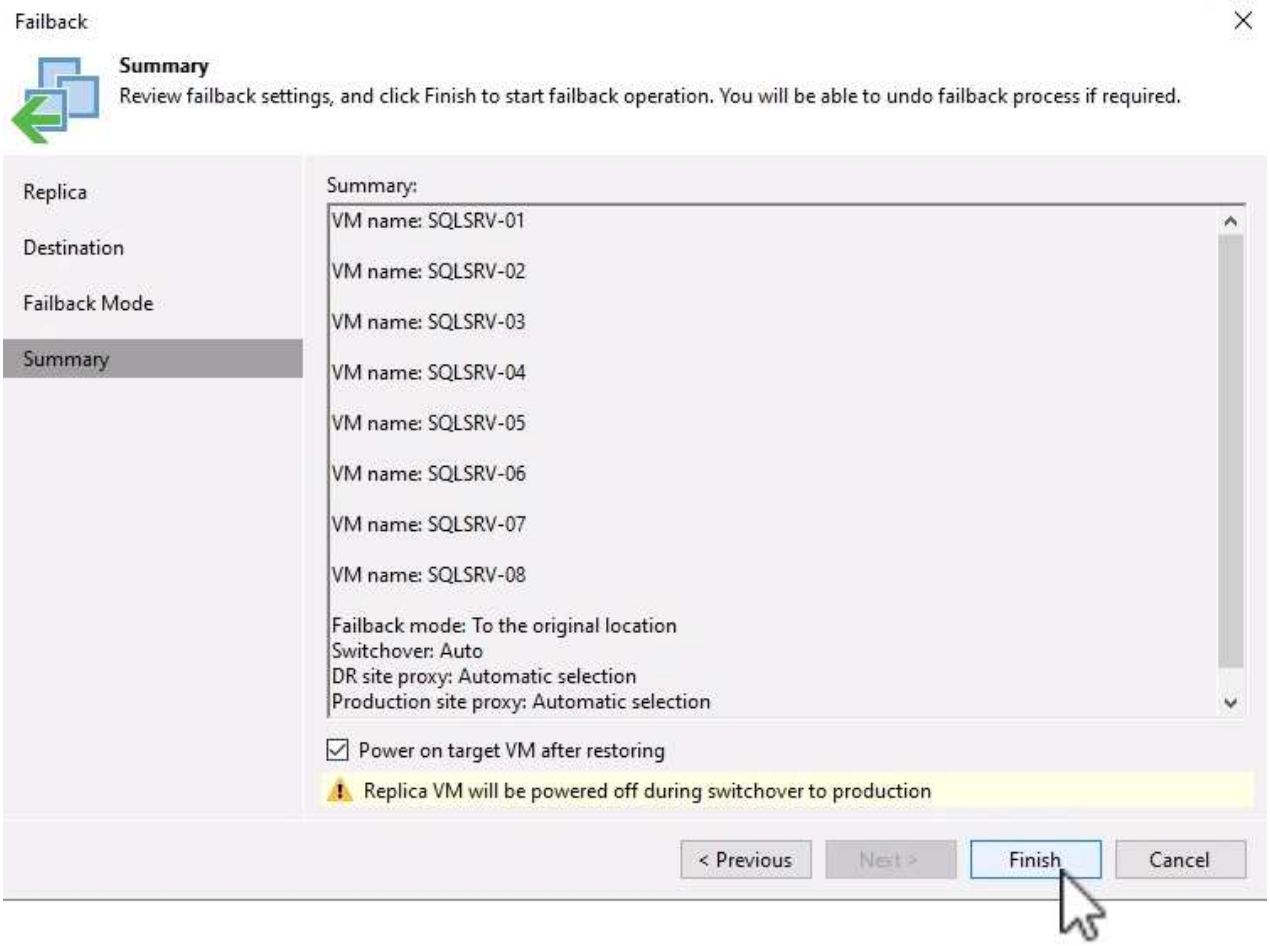
2. 장애 복구 * 마법사의 * 복제본 * 페이지에서 장애 복구 작업에 포함할 복제본을 선택합니다.
3. Destination * 페이지에서 * Failback to the original VM * 을 선택하고 * Next * 를 클릭하여 계속합니다.



4. 페일백 모드 * 페이지에서 * 자동 * 을 선택하여 가능한 한 빨리 페일백을 시작합니다.

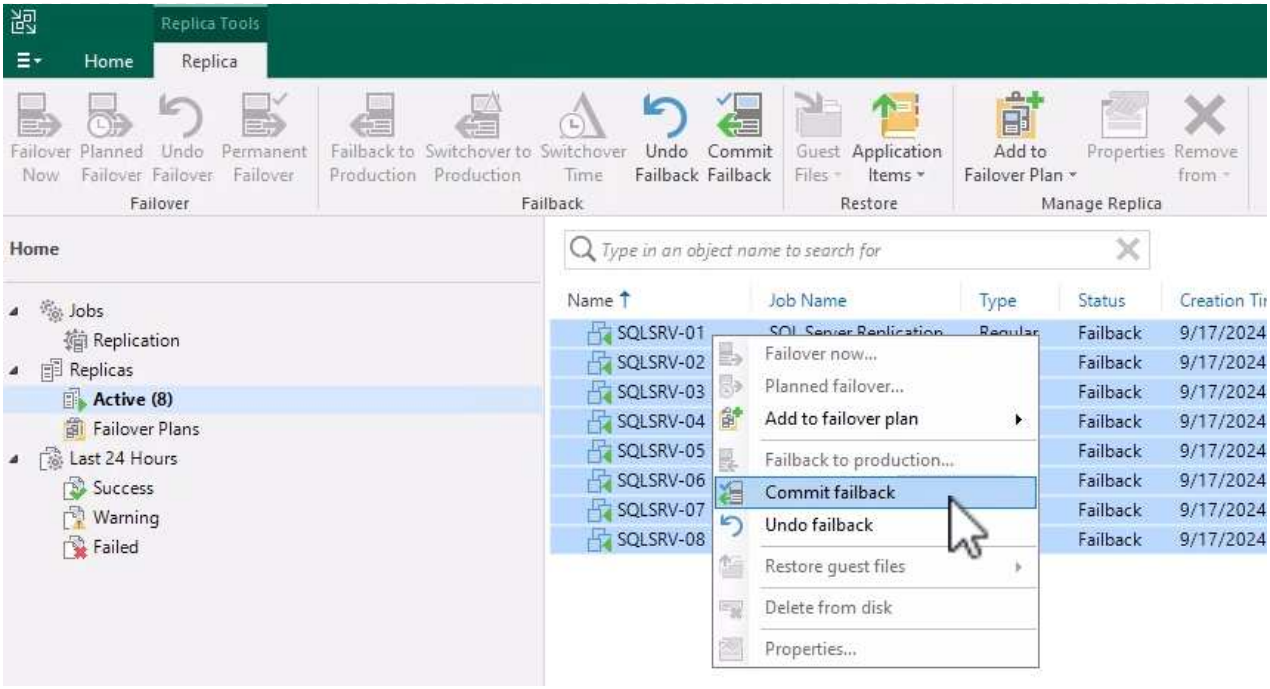


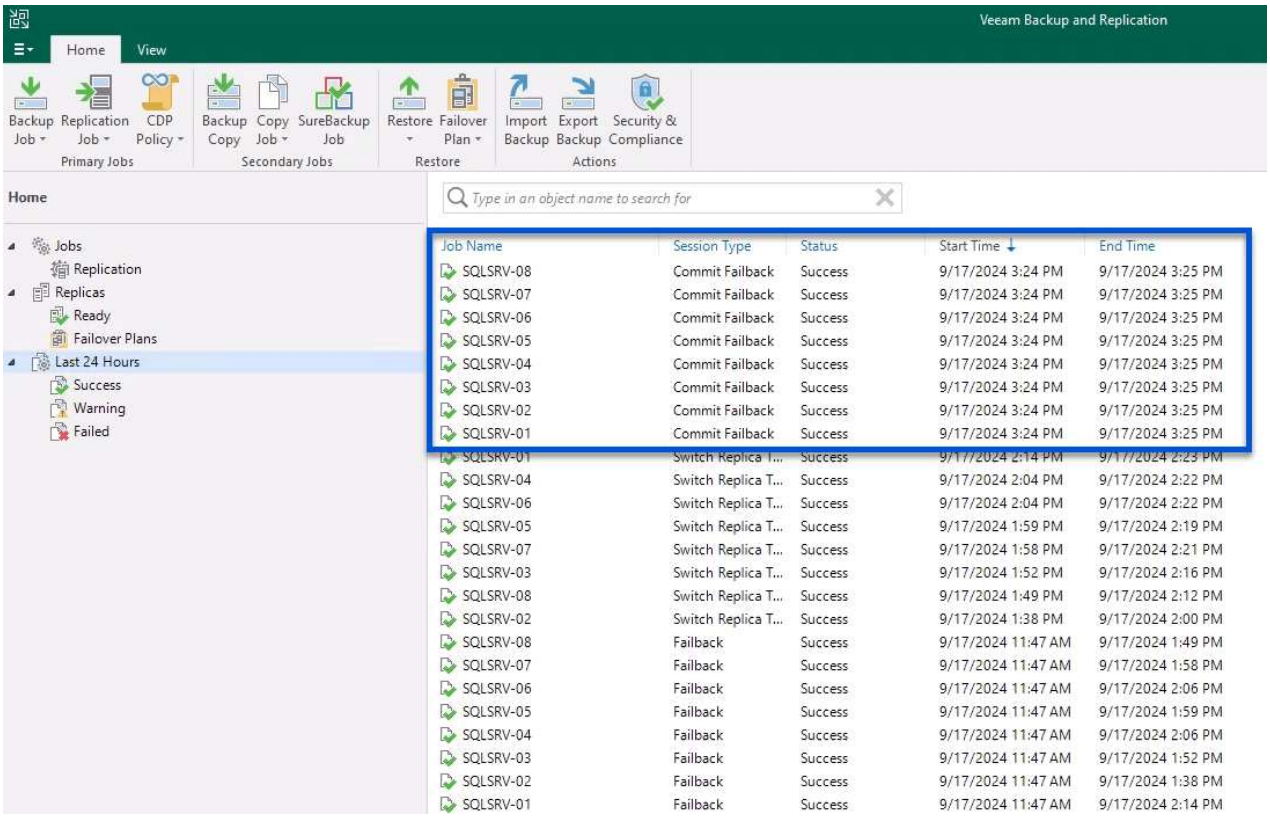
5. 요약 * 페이지에서 * 복원 후 대상 VM 전원 켜기 * 를 선택할지 여부를 선택한 다음 마침 을 클릭하여 장애 복구 작업을 시작합니다.



페일백 커밋은 페일백 작업을 종료하여 변경 사항이 프로덕션 VM에 성공적으로 통합되었는지 확인합니다. 커밋되면 Veeam Backup & Replication은 복구된 운영 VM에 대한 정기 복제 작업을 재개합니다. 이렇게 하면 복구된 복제본의 상태가 _Failback_에서 _Ready_로 변경됩니다.

1. 페일백을 커밋하려면 * Replicas > Active * 로 이동하여 커밋할 VM을 선택하고 마우스 오른쪽 버튼을 클릭한 후 * Commit failback * 을 선택합니다.





운영 환경으로 페일백이 성공하면 VM이 모두 원래 운영 사이트로 복구됩니다.

페일백 프로세스에 대한 자세한 내용은 의 Veeam 문서를 참조하십시오 "복제를 위한 페일오버 및 페일백".

결론

Google Cloud NetApp Volumes 데이터 저장소 기능은 Veeam 및 기타 검증된 타사 툴을 활용하여 비용 효율적인 DR(재해 복구) 솔루션을 제공할 수 있도록 합니다. 대규모 VM 복제본용 전용 클러스터 대신 파일럿 라이트 클러스터를 활용하면 조직에서 비용을 크게 절감할 수 있습니다. 이 접근 방식을 사용하면 기존 내부 백업 솔루션을 클라우드 기반 재해 복구에 활용하는 맞춤형 DR 전략을 수립할 수 있으므로 추가적인 사내 데이터 센터가 필요하지 않습니다. 재해가 발생할 경우 클릭 한 번으로 페일오버를 시작하거나 자동으로 실행되도록 구성할 수 있으므로 가동 중지 시간을 최소화하면서 비즈니스 연속성을 유지할 수 있습니다.

이 프로세스에 대해 자세히 알아보려면 자세한 단계별 안내 비디오를 참조하십시오.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=b2fb8597-c3fe-49e2-8a84-b1f10118db6d

GCP/GCVE에서 워크로드를 마이그레이션하는 중입니다

VMware HCX-Quickstart 가이드를 사용하여 **Google Cloud VMware Engine**에서 **NetApp Cloud Volume Service** 데이터 저장소로 워크로드를 마이그레이션합니다

Google Cloud VMware Engine 및 Cloud Volume Service 데이터 저장소의 가장 일반적인 사용 사례 중 하나는 VMware 워크로드 마이그레이션입니다. VMware HCX는 선호되는 옵션이며 사내 VM(가상 머신)과 데이터를 Cloud Volume Service NFS 데이터 저장소로 이동하는 다양한 마이그레이션 메커니즘을 제공합니다.

저자: NetApp 솔루션 엔지니어링

개요**: VMware HCX, NetApp Cloud Volume Service** 데이터 저장소 및 **Google Cloud VMware Engine(GCVE)**을 사용하여 가상 머신 마이그레이션

VMware HCX는 주로 클라우드 전반에서 애플리케이션 마이그레이션, 워크로드 재조정 및 비즈니스 연속성을 간소화하도록 설계된 마이그레이션 플랫폼입니다. 이 제품은 Google Cloud VMware Engine 프라이빗 클라우드의 일부로 포함되어 있으며 워크로드를 마이그레이션할 수 있는 다양한 방법을 제공하므로 재해 복구(DR) 작업에 사용할 수 있습니다.

이 문서에서는 Cloud Volume Service 데이터 저장소를 프로비저닝하기 위한 단계별 지침을 제공하고, 온프레미스 및 Google Cloud VMware Engine 측에 있는 모든 주요 구성 요소(상호 연결, 네트워크 확장, 다양한 VM 마이그레이션 메커니즘을 지원하기 위한 WAN 최적화 포함)를 포함하여 VMware HCX를 다운로드, 구축 및 구성하는 방법을 설명합니다.

VMware HCX는 마이그레이션이 VM 레벨에 있으므로 모든 데이터 저장소 유형과 함께 작동합니다. 따라서 이 문서는 비용 효율적인 VMware 클라우드 구축을 위해 Google Cloud VMware Engine과 함께 Cloud Volume Service를 구축하려는 기존 NetApp 고객 및 타사 고객에게 적용됩니다.

높은 수준의 단계

이 목록은 HCX Connector On-Premises에서 Google Cloud VMware Engine의 HCX Cloud Manager로 VM을 페어링 및 마이그레이션하는 데 필요한 고급 단계를 제공합니다.

1. Google VMware Engine 포털을 통해 HCX를 준비합니다.
2. 사내 VMware vCenter Server에서 HCX Connector OVA(Open Virtualization Appliance) 설치 프로그램을 다운로드하여 구축합니다.
3. 라이센스 키를 사용하여 HCX를 활성화합니다.
4. 온프레미스 VMware HCX Connector를 Google Cloud VMware Engine HCX Cloud Manager와 페어링합니다.
5. 네트워크 프로파일, 컴퓨팅 프로파일 및 서비스 메시를 구성합니다.
6. (선택 사항) 마이그레이션 중에 재IP를 방지하기 위해 네트워크 확장을 수행합니다.
7. 어플라이언스 상태를 확인하고 마이그레이션이 가능한지 확인합니다.
8. VM 워크로드를 마이그레이션합니다.

필수 구성 요소

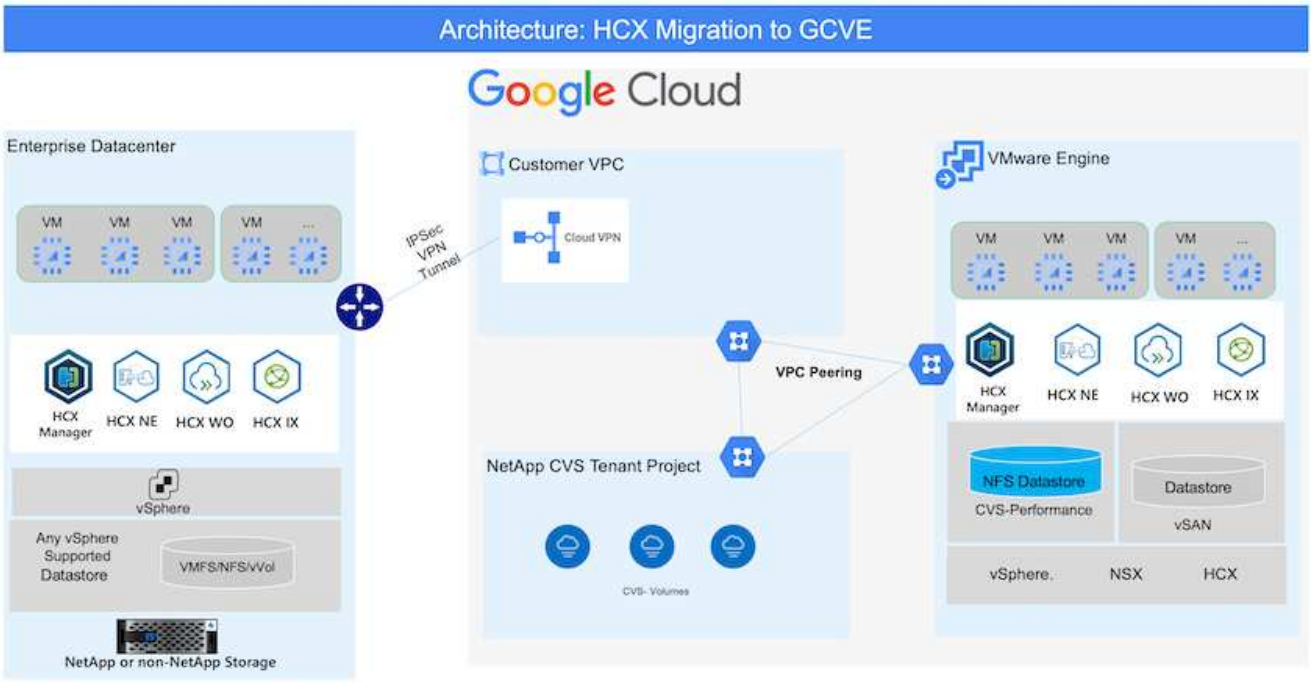
시작하기 전에 다음 필수 구성 요소가 충족되었는지 확인하십시오. 자세한 내용은 다음을 참조하십시오 "링크". 연결을 포함한 필수 구성 요소가 구축된 후에는 Google Cloud VMware Engine 포털에서 HCX 라이센스 키를 다운로드하십시오. OVA 설치 프로그램을 다운로드한 후 아래 설명된 대로 설치 프로세스를 진행합니다.

HCX Advanced가 기본 옵션이며 VMware HCX Enterprise Edition도 지원 티켓을 통해 제공되며 추가 비용 없이 지원됩니다. 을 참조하십시오 "이 링크"

- 기존 Google Cloud VMware Engine SDDC(소프트웨어 정의 데이터 센터)를 사용하거나 이를 사용하여 프라이빗 클라우드를 생성합니다 "NetApp 링크" 또는 이 "Google 링크".
- 사내 VMware vSphere 지원 데이터 센터에서 VM 및 관련 데이터를 마이그레이션하려면 데이터 센터에서 SDDC 환경으로 네트워크를 연결해야 합니다. 워크로드를 마이그레이션하기 전에 "Cloud VPN 또는 Cloud Interconnect 연결을 설정합니다" 데이터 관리 및 보호
- 사내 VMware vCenter Server 환경에서 Google Cloud로 연결되는 네트워크 경로 VMware Engine 프라이빗 클라우드는 vMotion을 사용하여 VM 마이그레이션을 지원해야 합니다.
- 필수 를 확인하십시오 "방화벽 규칙 및 포트" 온-프레미스 vCenter Server와 SDDC vCenter 간에 vMotion 트래픽이 허용됩니다.
- Cloud Volume Service NFS 볼륨은 Google Cloud VMware Engine에서 데이터 저장소로 마운트되어야 합니다. 이에 설명된 단계를 따릅니다 "링크" Google Cloud VMware Engine 호스트에 Cloud Volume Service 데이터 저장소를 연결하려면 다음을 수행합니다.

고급 아키텍처

테스트 목적으로, 이 검증에 사용된 온프레미스 연구소 환경이 Cloud VPN을 통해 연결되어 Google Cloud VPC에 사내 연결을 가능하게 했습니다.



HCX에 대한 자세한 다이어그램은 을 참조하십시오 "VMware 링크"

솔루션 구축

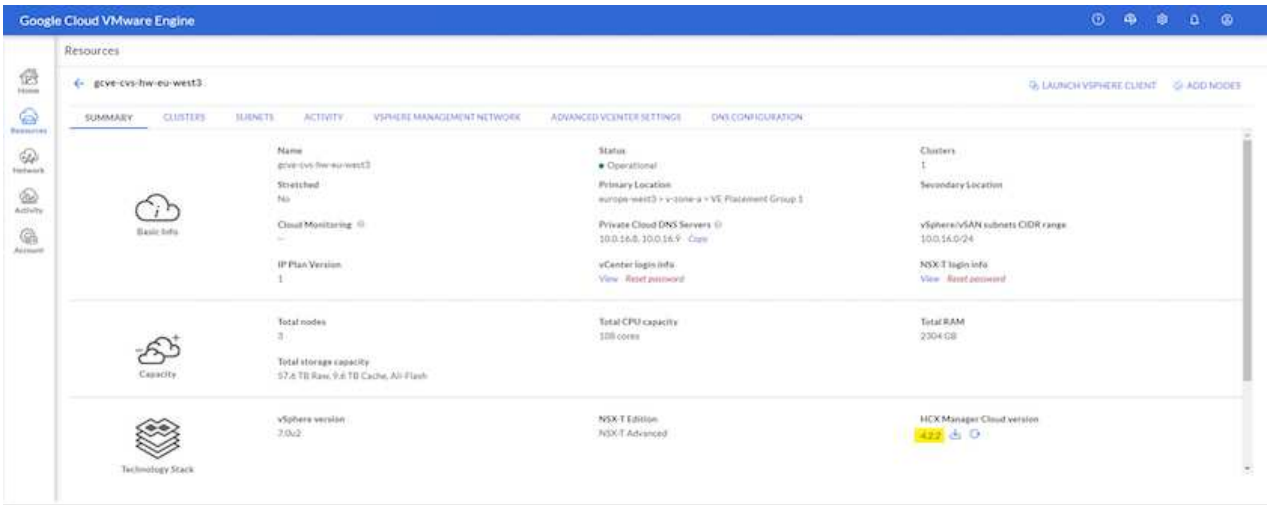
이 솔루션의 배포를 완료하려면 다음 단계를 따르십시오.

1단계**: Google VMware Engine Portal**을 통해 **HCX**를 준비합니다

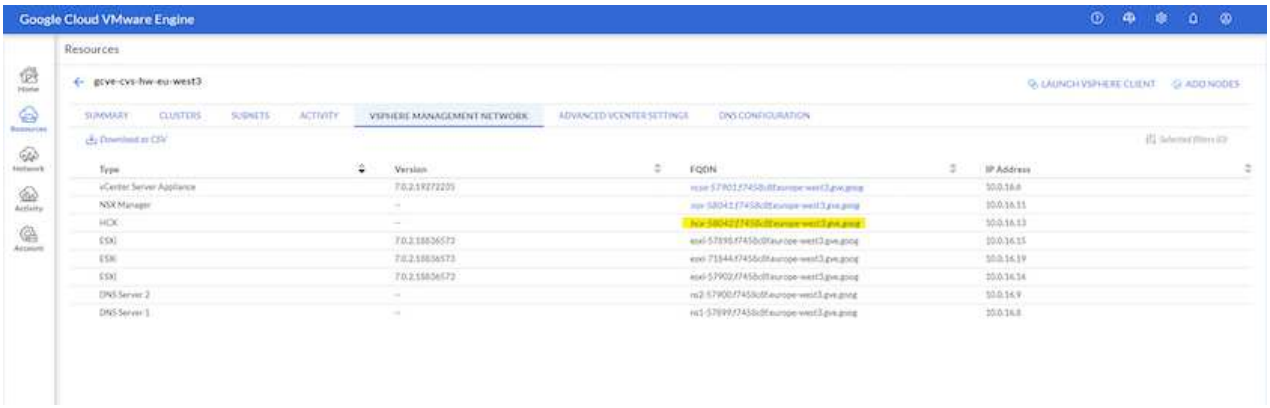
VMware Engine을 사용하여 프라이빗 클라우드를 프로비저닝할 때 HCX Cloud Manager 구성 요소가 자동으로 설치됩니다. 사이트 페어링을 준비하려면 다음 단계를 완료하십시오.

1. Google VMware Engine Portal에 로그인하고 HCX Cloud Manager에 로그인합니다.

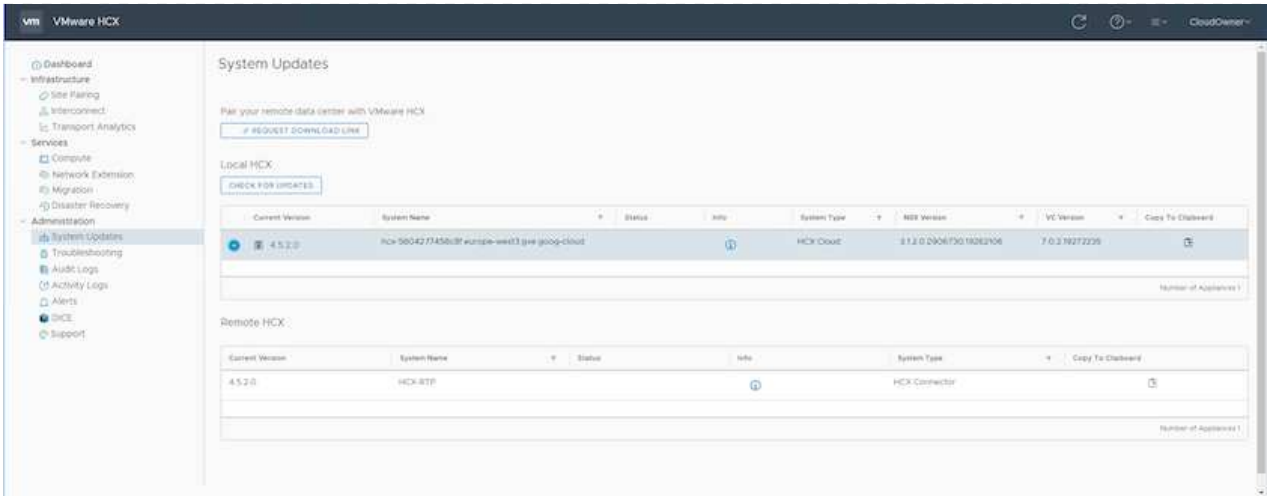
   HCX 버전 링크를



   클릭하거나 vSphere Management Network 탭에서 HCX FQDN을 클릭하여 HCX 콘솔에 로그인할 수 있습니다.



2. HCX Cloud Manager에서 * 관리 > 시스템 업데이트 * 로 이동합니다.
3. 다운로드 요청 링크 * 를 클릭하고 OVA 파일을 다운로드합니다.



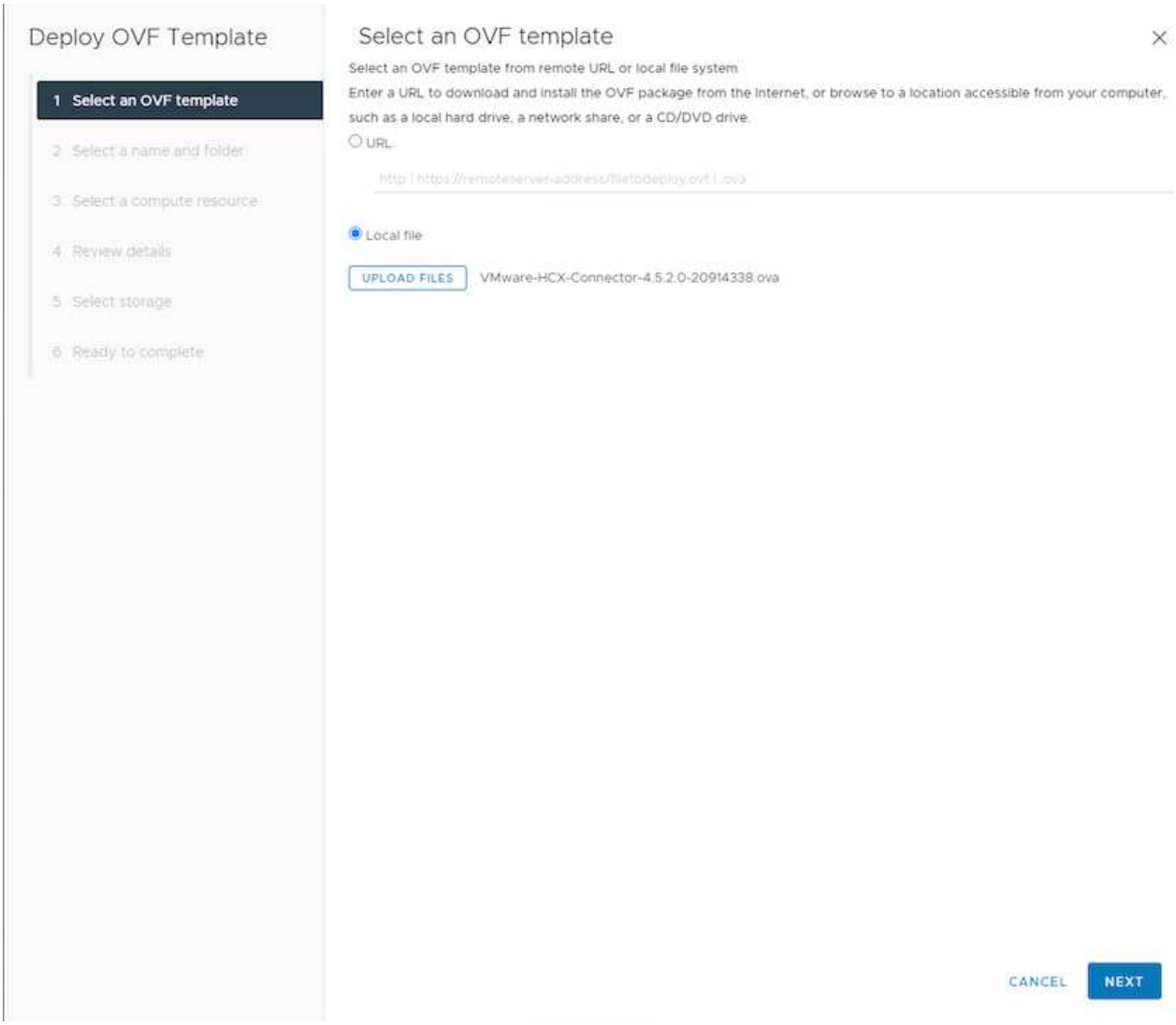
4. HCX Cloud Manager를 HCX Cloud Manager UI에서 사용 가능한 최신 버전으로 업데이트합니다.

2단계**:** 온**-**프레미스 **vCenter Server**에 설치 관리자 **OVA**를 구축합니다

온프레미스 커넥터가 Google Cloud VMware Engine의 HCX Manager에 연결하려면 적절한 방화벽 포트가 사내 환경에서 열려 있는지 확인합니다.

온-프레미스 vCenter Server에서 HCX Connector를 다운로드하여 설치하려면 다음 단계를 수행하십시오.

1. 이전 단계에서 설명한 대로 Google Cloud VMware Engine의 HCX 콘솔에서 OVA를 다운로드하도록 합니다.
2. OVA를 다운로드한 후 * Deploy OVF Template * 옵션을 사용하여 온프레미스 VMware vSphere 환경에 구축합니다.



3. OVA 배포에 필요한 모든 정보를 입력하고 * Next * 를 클릭한 다음 * Finish * 를 클릭하여 VMware HCX 커넥터 OVA를 배포합니다.

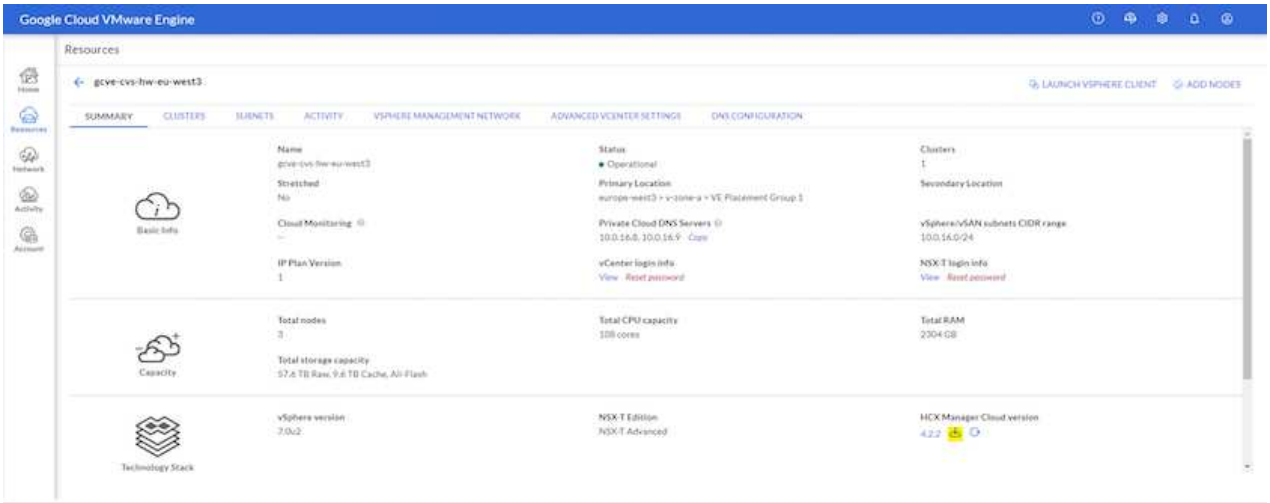
가상 어플라이언스의 전원을 수동으로 켭니다.

단계별 지침은 를 참조하십시오 "VMware HCX 사용자 가이드".

3단계**:** 라이센스 키로 **HCX** 커넥터를 활성화합니다

VMware HCX 커넥터 OVA를 온-프레미스로 배포하고 어플라이언스를 시작한 후 다음 단계를 수행하여 HCX 커넥터를 활성화하십시오. Google Cloud VMware Engine 포털에서 라이센스 키를 생성하고 VMware HCX Manager에서 활성화합니다.

1. VMware Engine 포털에서 리소스를 클릭하고 프라이빗 클라우드를 선택한 다음 * HCX Manager Cloud Version * 에서 다운로드 아이콘을 클릭합니다.



   다운로드한 파일을 열고 라이센스 키 문자열을 복사합니다.

2. 사내 VMware HCX Manager()에 로그인합니다 "`https://hcxmanagerIP:9443`" 관리자 자격 증명을 사용합니다.

   OVA 배포 중에 정의된 hcxmanageIP 및 암호를 사용합니다.

3. 라이센스에서 3단계에서 복사한 키를 입력하고 * Activate * 를 클릭합니다.

   온프레미스 HCX 커넥터는 인터넷에 연결되어 있어야 합니다.

4. 데이터 센터 위치 * 에서 VMware HCX Manager를 사내에 설치할 수 있는 가장 가까운 위치를 제공합니다. 계속 * 을 클릭합니다.
5. 시스템 이름 * 에서 이름을 업데이트하고 * 계속 * 을 클릭합니다.
6. 예, 계속 * 을 클릭합니다.
7. vCenter * 연결 아래에서 vCenter Server의 FQDN(정규화된 도메인 이름) 또는 IP 주소와 해당 자격 증명을 입력하고 * 계속 * 을 클릭합니다.

   나중에 연결 문제를 방지하려면 FQDN을 사용합니다.

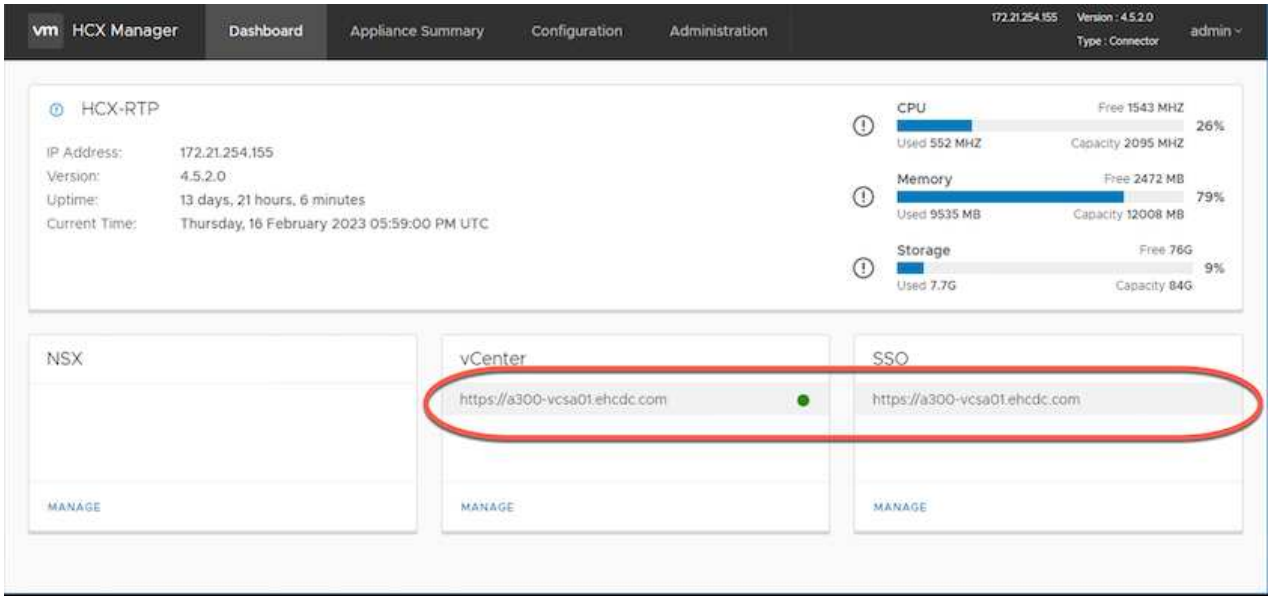
8. SSO/PSC * 구성 아래에서 플랫폼 서비스 컨트롤러(PSC) FQDN 또는 IP 주소를 제공하고 * 계속 * 을 클릭합니다.

   Embedded PSC의 경우 VMware vCenter Server FQDN 또는 IP 주소를 입력합니다.

9. 입력한 정보가 올바른지 확인하고 * Restart * (재시작 *)를 클릭합니다.

10. 서비스를 다시 시작하면 표시되는 페이지에 vCenter Server가 녹색으로 표시됩니다. vCenter Server와 SSO 모두 적절한 구성 매개 변수를 가져야 하며, 이는 이전 페이지와 동일해야 합니다.

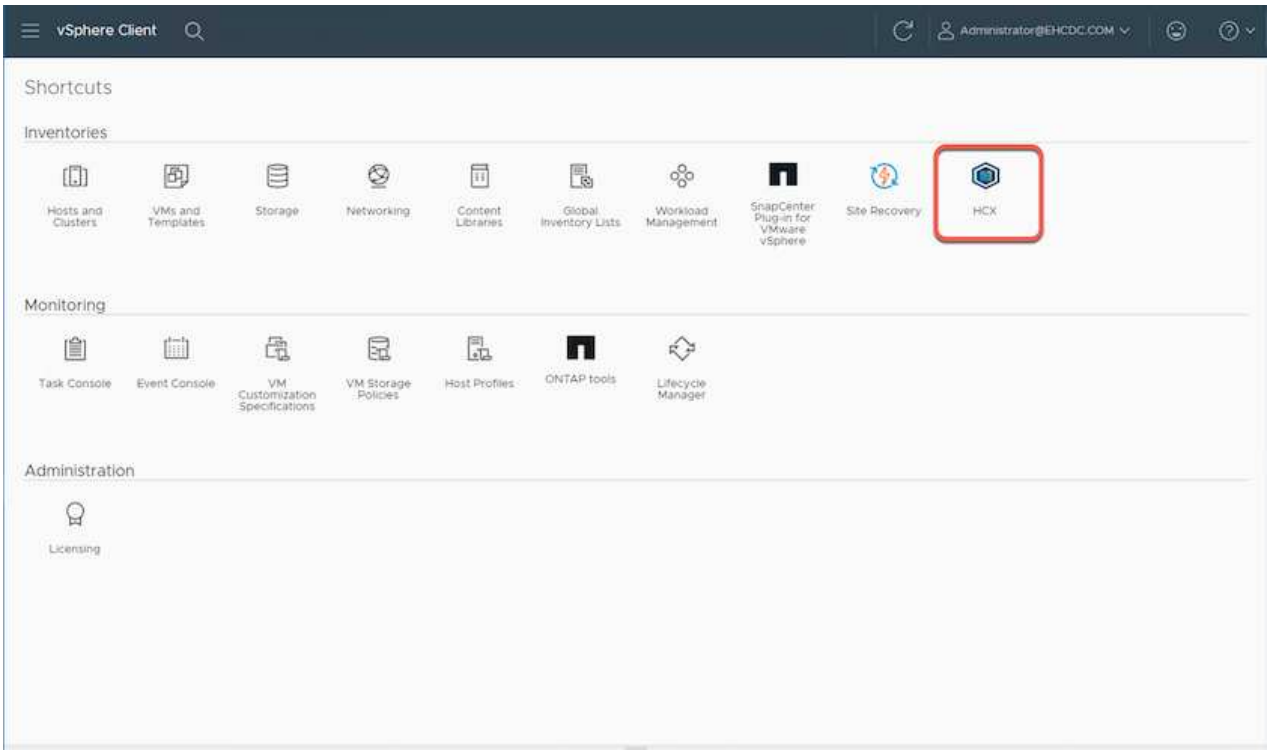
> 이 프로세스는 약 10~20분 정도 소요되며 플러그인이 vCenter Server에 추가되어야 합니다.



4단계: 온프레미스 **VMware HCX Connector**를 **Google Cloud VMware Engine HCX Cloud Manager**와 페어링합니다

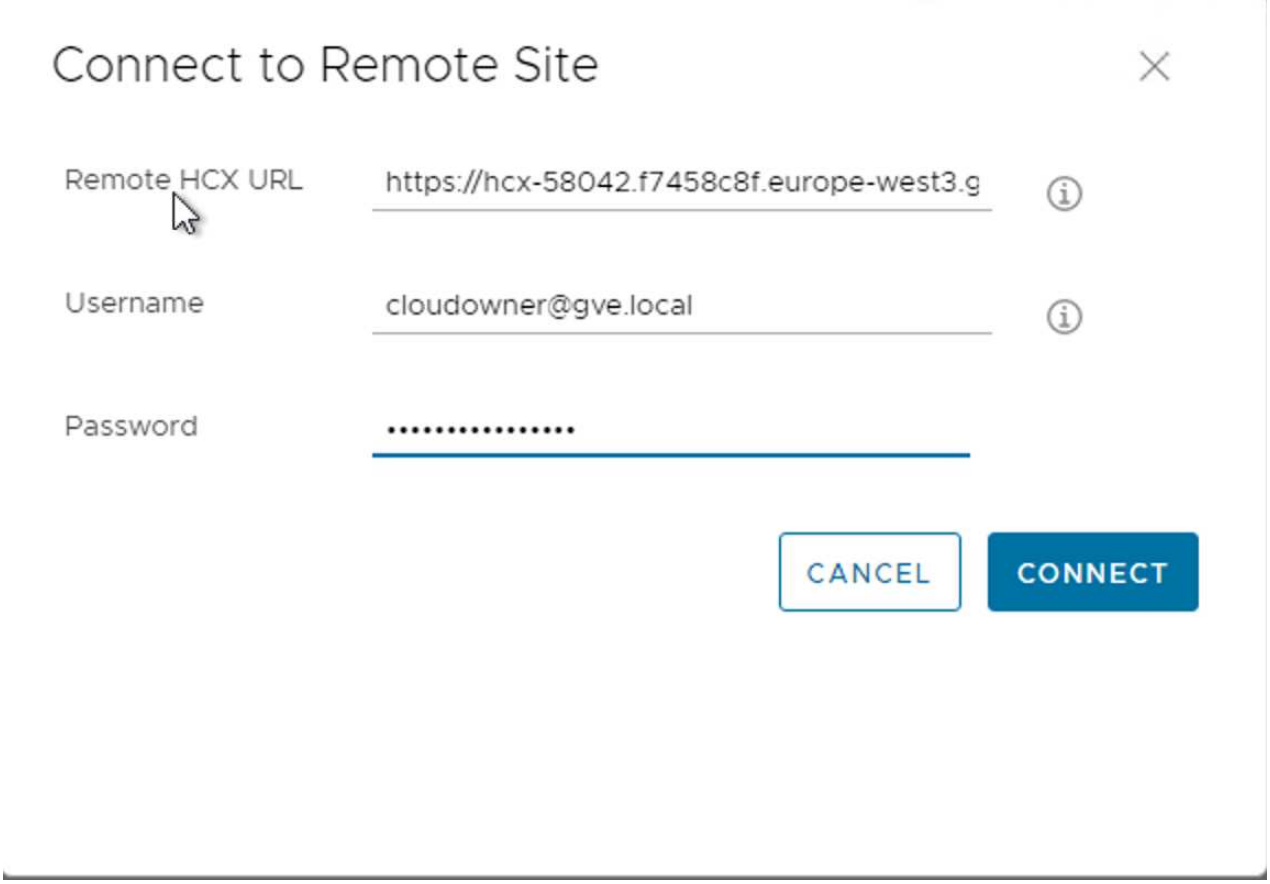
HCX Connector를 사내 vCenter에 구축 및 구성한 후 페어링을 추가하여 Cloud Manager에 연결합니다. 사이트 페어링을 구성하려면 다음 단계를 수행하십시오.

1. 온-프레미스 vCenter 환경과 Google Cloud VMware Engine SDDC 간에 사이트 쌍을 생성하려면 온-프레미스 vCenter Server에 로그인하고 새 HCX vSphere Web Client 플러그인에 액세스합니다.



2. 인프라 에서 * 사이트 페어링 추가 * 를 클릭합니다.

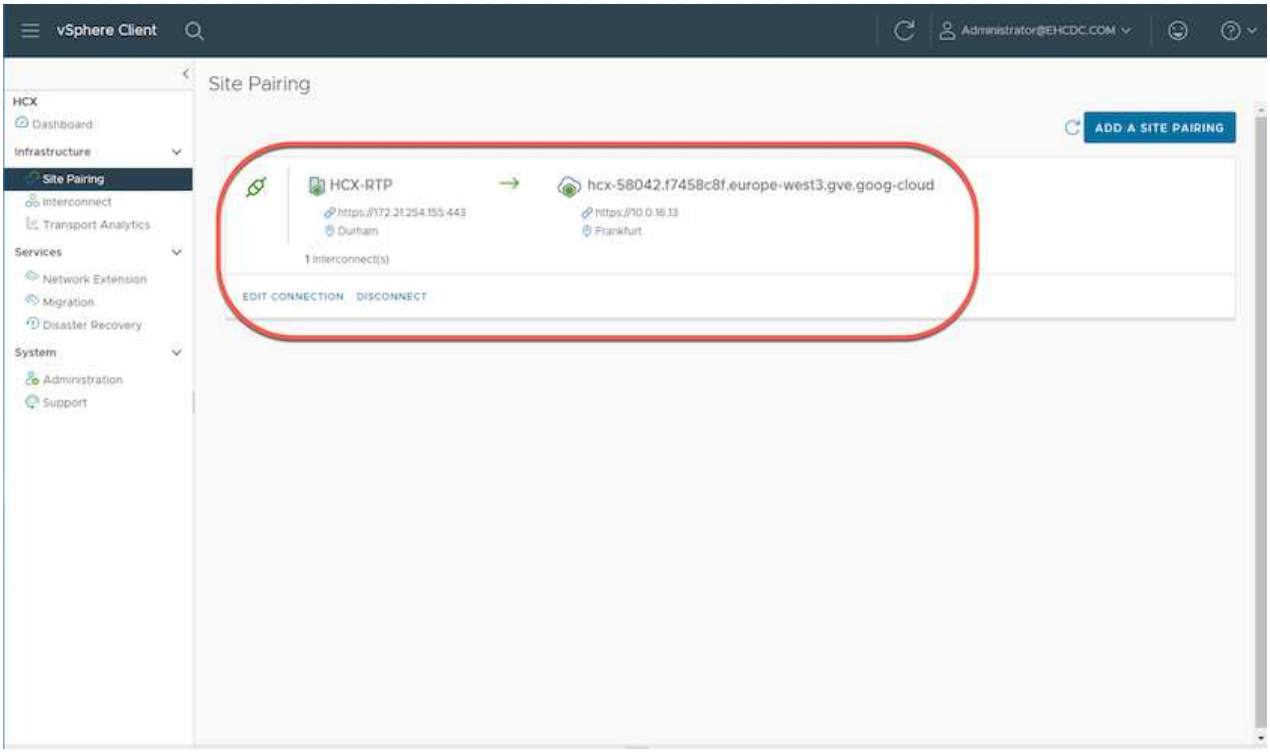
Google Cloud VMware Engine HCX Cloud Manager URL 또는 IP 주소와 Cloud-Owner-Role 권한이 있는 사용자의 자격 증명을 입력하여 프라이빗 클라우드에 액세스합니다.



3. 연결 * 을 클릭합니다.

VMware HCX Connector는 포트 443을 통해 HCX Cloud Manager IP로 라우팅할 수 있어야 합니다.

4. 페어링이 생성된 후에는 새로 구성된 사이트 페어링을 HCX 대시보드에서 사용할 수 있습니다.

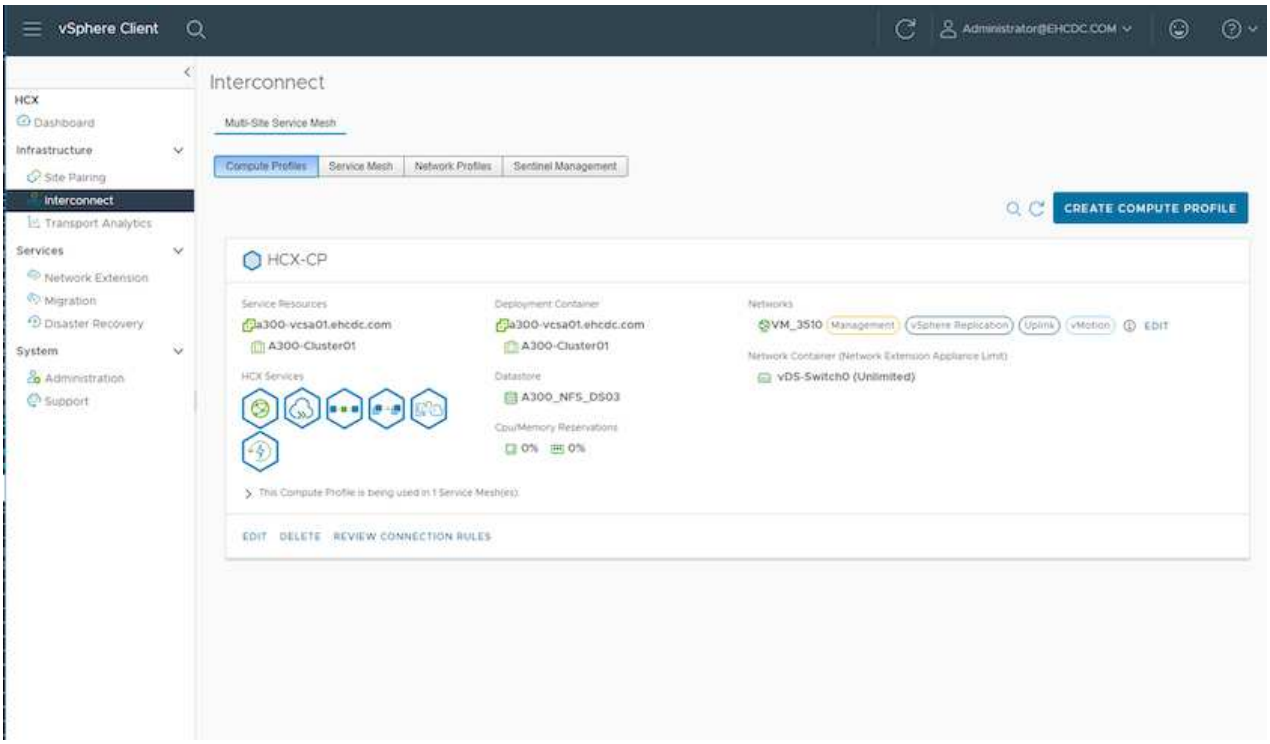

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud
https://10.0.16.13
Frankfurt
1 Interconnect(s)
EDIT CONNECTION
DISCONNECT

5단계**:** 네트워크 프로파일**,** 컴퓨팅 프로파일 및 서비스 메시를 구성합니다

VMware HCX Interconnect 서비스 어플라이언스는 인터넷을 통해 복제 및 vMotion 기반 마이그레이션 기능과 타겟 사이트에 대한 프라이빗 연결을 제공합니다. 상호 연결은 암호화, 트래픽 엔지니어링 및 VM 이동성을 제공합니다. 상호 연결 서비스 어플라이언스를 생성하려면 다음 단계를 수행하십시오.

1. 인프라 아래에서 * 상호 연결 > 멀티 사이트 서비스 메시 > 컴퓨팅 프로파일 > 컴퓨팅 프로파일 생성 * 을 선택합니다.

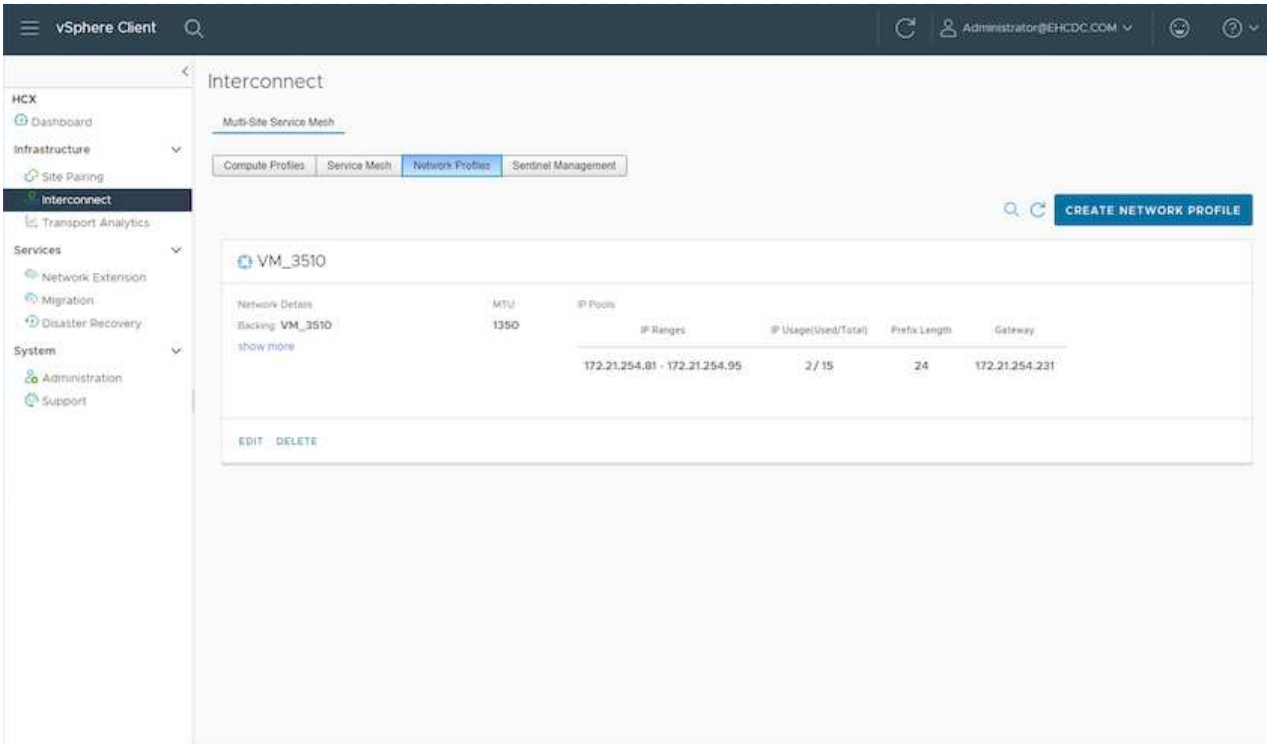
   컴퓨팅 프로필은 구축된 어플라이언스와 HCX 서비스에서 액세스할 수 있는 VMware 데이터 센터 부분을 포함하여 구축 매개 변수를 정의합니다.



2. 컴퓨팅 프로파일을 만든 후 * 다중 사이트 서비스 메시 > 네트워크 프로파일 > 네트워크 프로파일 만들기 * 를 선택하여 네트워크 프로파일을 만듭니다.

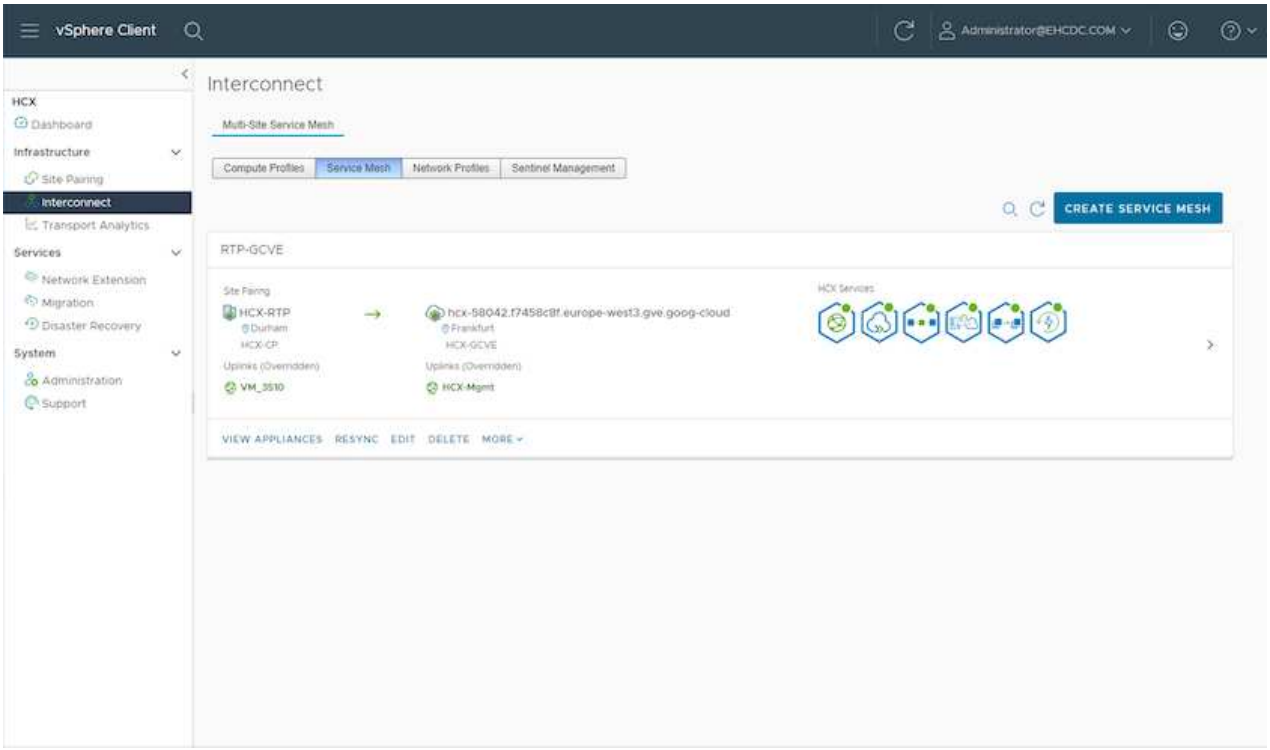
   네트워크 프로파일은 HCX가 가상 어플라이언스에 사용하는 IP 주소 및 네트워크의 범위를 정의합니다.

   이 단계에서는 두 개 이상의 IP 주소가 필요합니다. 이러한 IP 주소는 관리 네트워크에서 상호 연결 어플라이언스로 할당됩니다.

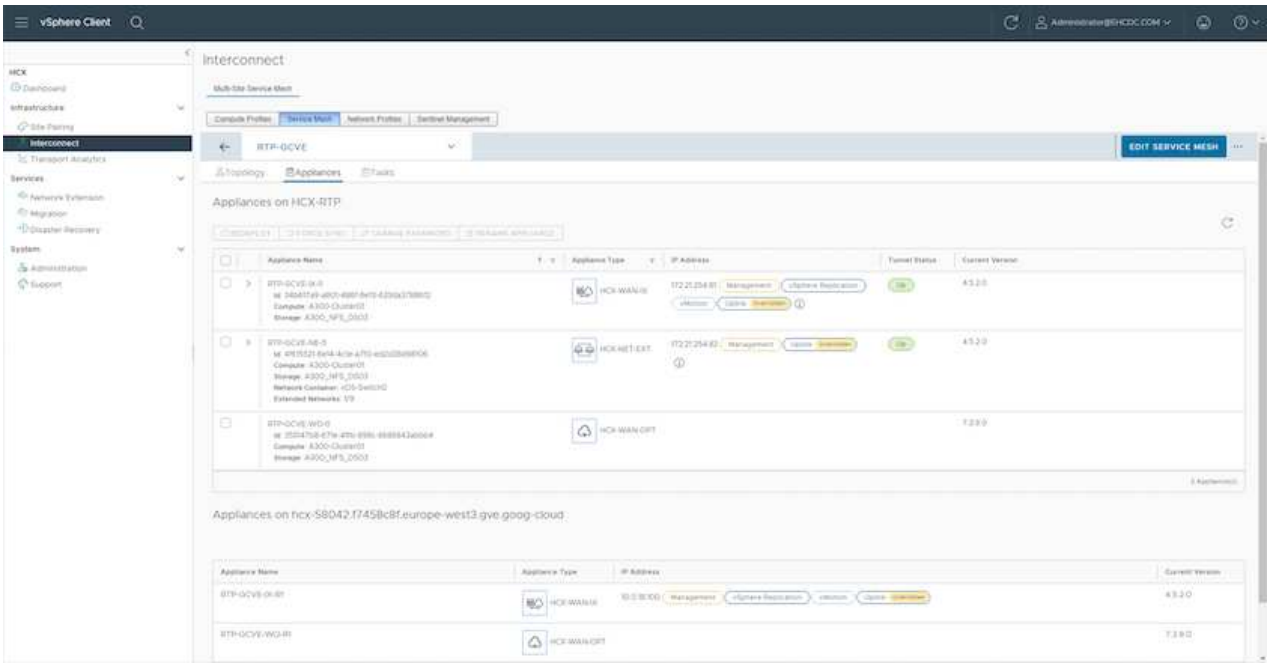


3. 현재 컴퓨팅 및 네트워크 프로파일이 성공적으로 생성되었습니다.
4. 상호 연결 * 옵션 내에서 * 서비스 메시 * 탭을 선택하고 온-프레미스 및 GCVE SDDC 사이트를 선택하여 서비스 메시를 생성합니다.
5. 서비스 메시는 로컬 및 원격 계산 및 네트워크 프로파일 쌍을 지정합니다.

이 프로세스의 일환으로 안전한 전송 패브릭을 생성하기 위해 소스 사이트와 타겟 사이트 모두에 HCX 어플라이언스를 구축하고 자동으로 구성합니다.



6. 이 단계는 구성의 마지막 단계입니다. 구축을 완료하는 데 약 30분이 소요됩니다. 서비스 메시가 구성된 후 작업 부하 VM을 마이그레이션하도록 IPsec 터널이 성공적으로 생성된 환경이 준비됩니다.



6단계**:** 워크로드 마이그레이션

다양한 VMware HCX 마이그레이션 기술을 사용하여 온프레미스 및 GCVE SDDC 간에 워크로드를 양방향으로 마이그레이션할 수 있습니다. VM은 HCX 대량 마이그레이션, HCX vMotion, HCX 콜드 마이그레이션, HCX Replication Assisted vMotion(HCX Enterprise Edition에서 사용 가능) 및 HCX OS 지원 마이그레이션(HCX Enterprise Edition에서 사용 가능)과 같은 여러 마이그레이션 기술을 사용하여 VMware HCX 활성 엔터티로 또는 VMware에서 이동할 수 있습니다.

다양한 HCX 마이그레이션 메커니즘에 대한 자세한 내용은 을 참조하십시오 "VMware HCX 마이그레이션 유형".

HCX-IX 어플라이언스는 Mobility Agent 서비스를 사용하여 vMotion, Cold 및 RAV(Replication Assisted vMotion) 마이그레이션을 수행합니다.

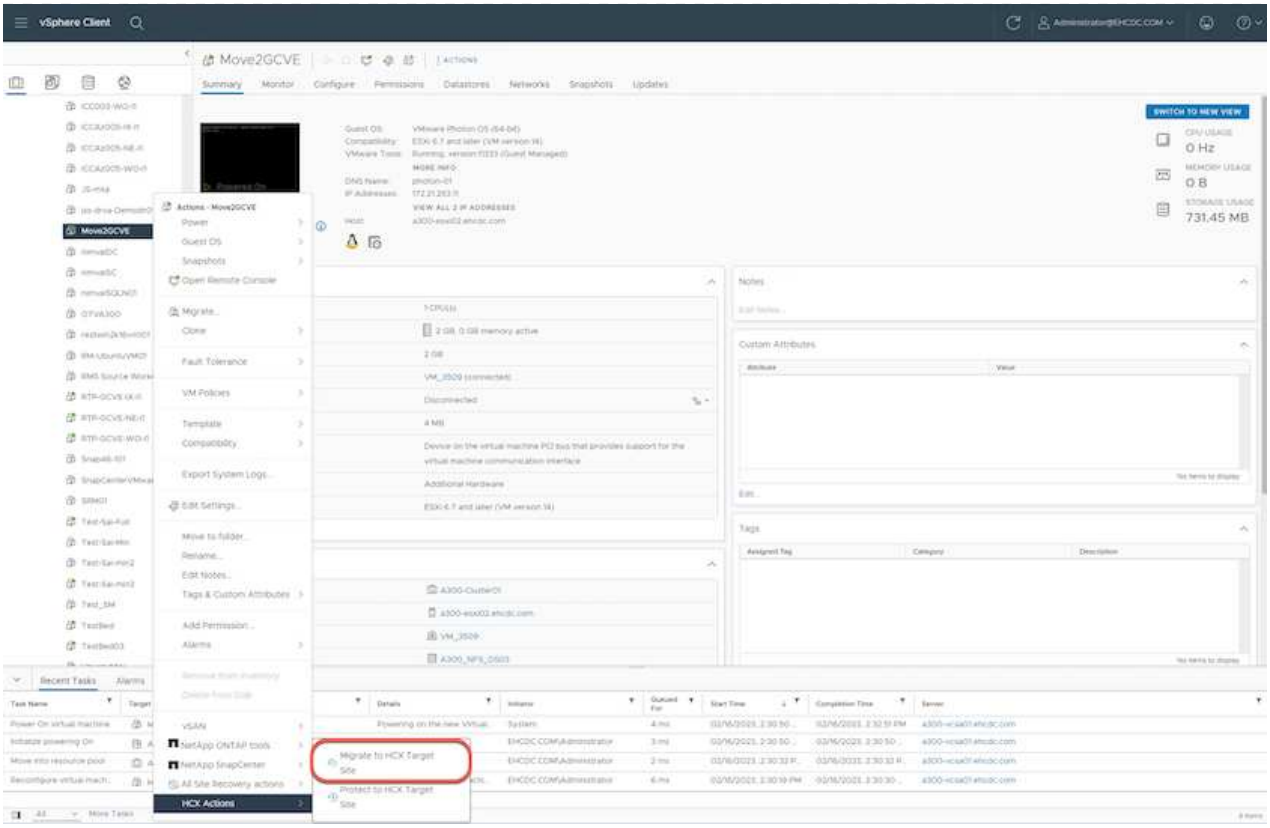
HCX-IX 어플라이언스는 vCenter Server에서 Mobility Agent 서비스를 호스트 개체로 추가합니다. 이 개체에 표시되는 프로세서, 메모리, 스토리지 및 네트워킹 리소스는 IX 어플라이언스를 호스팅하는 물리적 하이퍼바이저의 실제 소비량을 나타내지 않습니다.

- HCX vMotion *

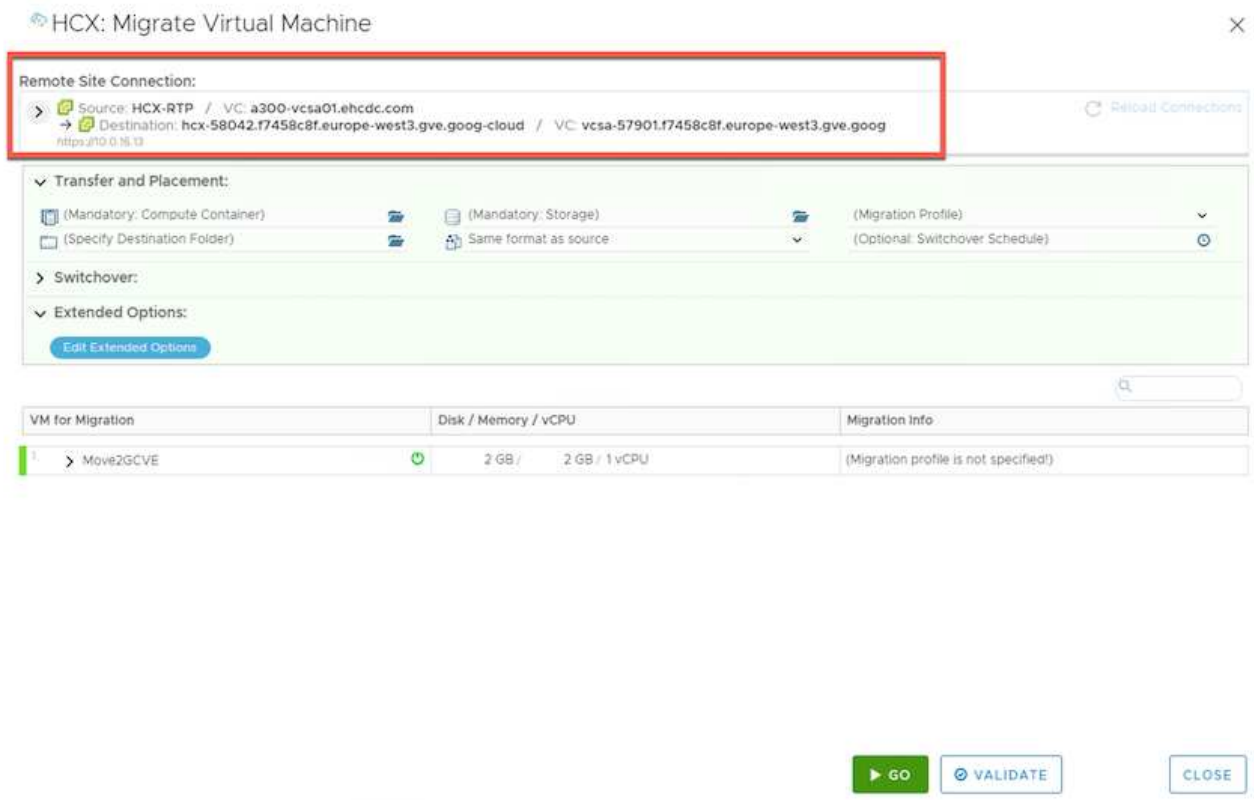
이 섹션에서는 HCX vMotion 메커니즘을 설명합니다. 이 마이그레이션 기술은 VMware vMotion 프로토콜을 사용하여 VM을 GCVE로 마이그레이션합니다. vMotion 마이그레이션 옵션은 한 번에 하나의 VM의 VM 상태를 마이그레이션하는 데 사용됩니다. 이 마이그레이션 방법 중에는 서비스가 중단되지 않습니다.

IP 주소를 변경할 필요 없이 VM을 마이그레이션하려면 네트워크 확장이 있어야 합니다(VM이 연결된 포트 그룹의 경우).

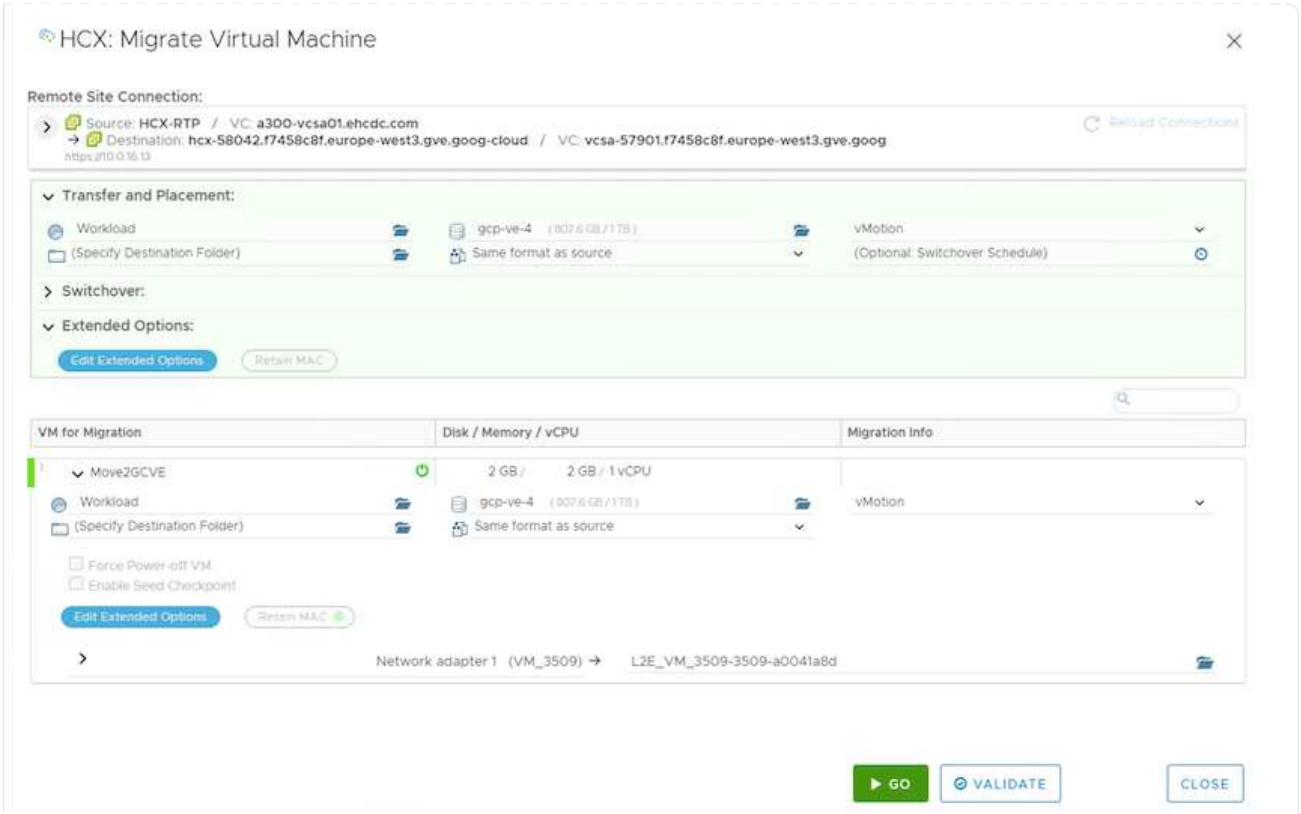
1. 온-프레미스 vSphere Client에서 Inventory로 이동하여 마이그레이션할 VM을 마우스 오른쪽 버튼으로 클릭하고 HCX Actions > Migrate to HCX Target Site를 선택합니다.



2. 가상 컴퓨터 마이그레이션 마법사에서 원격 사이트 연결(대상 GCVE)을 선택합니다.



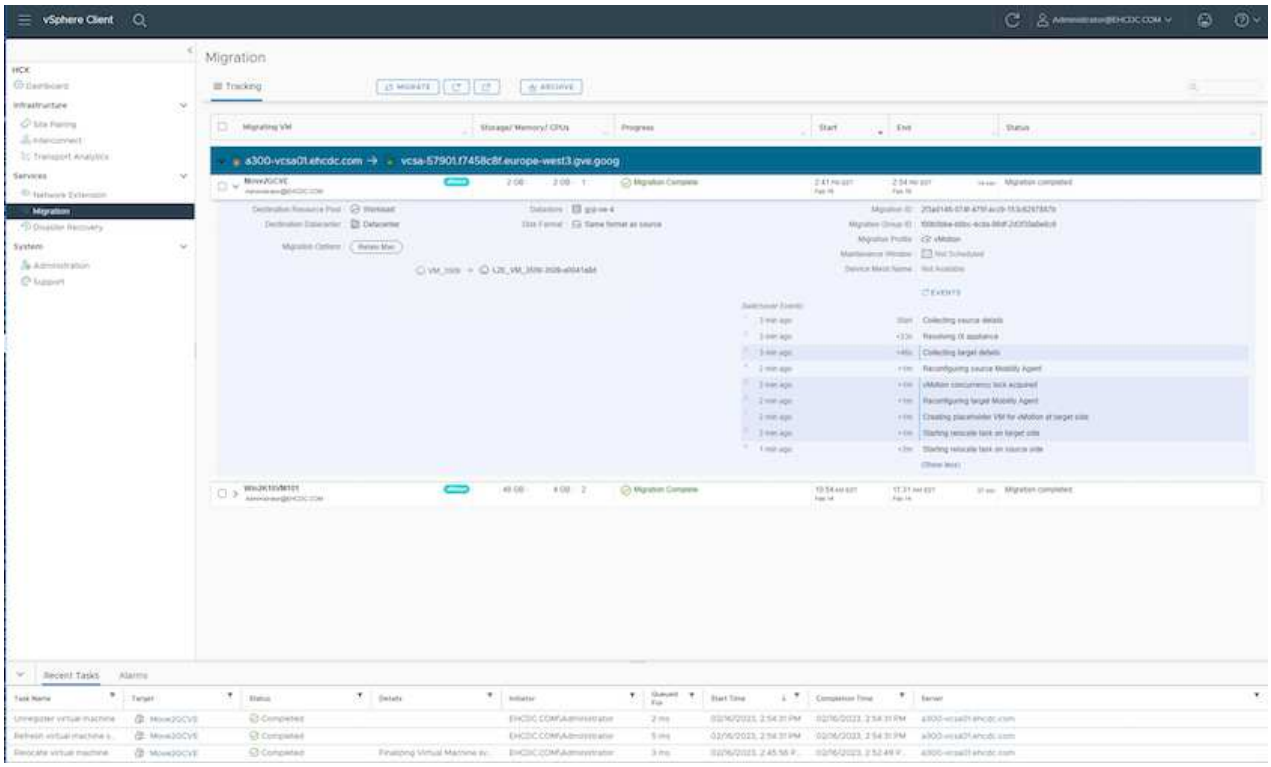
3. 필수 필드(클러스터, 스토리지 및 대상 네트워크)를 업데이트하고 검증 을 클릭합니다.



4. 유효성 검사가 완료된 후 이동을 클릭하여 마이그레이션을 시작합니다.

> vMotion 전송은 VM 활성 메모리, 실행 상태, IP 주소 및 MAC 주소를 캡처합니다. HCX vMotion의 요구 사항 및 제한 사항에 대한 자세한 내용은 을 참조하십시오 "VMware HCX vMotion 및 콜드 마이그레이션 이해".

5. HCX > 마이그레이션 대시보드에서 vMotion의 진행 상황과 완료 상태를 모니터링할 수 있습니다.



타겟 CVS NFS 데이터 저장소에 마이그레이션을 처리할 충분한 공간이 있어야 합니다.

결론

클라우드 볼륨 서비스 및 HCX는 온프레미스(On-Premises)의 모든 유형/공급업체 스토리지에 있는 모든 클라우드 또는 하이브리드 클라우드 및 데이터를 대상으로 하는 모든 환경에서 애플리케이션 워크로드를 배포 및 마이그레이션하는 동시에 데이터 요구 사항을 애플리케이션 계층으로 원활하게 만들어 TCO를 절감하는 탁월한 옵션을 제공합니다. 어떤 사용 사례에서든 Cloud Volume Service와 함께 Google Cloud VMware Engine을 사용하면 사내 및 멀티 클라우드 전체의 클라우드 이점, 일관된 인프라 및 운영을 신속하게 실현하고, 워크로드의 양방향 이동성을 제공하며, 엔터프라이즈급 용량과 성능을 실현할 수 있습니다. VMware vSphere Replication, VMware vMotion 또는 NFC(네트워크 파일 복사)를 사용하여 스토리지를 연결하고 VM을 마이그레이션하는 데 사용되는 익숙한 프로세스와 절차가 동일합니다.

이점

이 문서의 핵심 사항은 다음과 같습니다.

- 이제 Cloud Volume Service를 Google Cloud VMware Engine SDDC에서 데이터 저장소로 사용할 수 있습니다.
- 온프레미스에서 Cloud Volume Service 데이터 저장소로 데이터를 쉽게 마이그레이션할 수 있습니다.
- 마이그레이션 작업 중에 용량 및 성능 요구사항을 충족하기 위해 Cloud Volume Service 데이터 저장소를 쉽게 확장 및 축소할 수 있습니다.

Google 및 **VMware**의 비디오를 참조하십시오

Google에서

- "GCVE를 사용하여 HCX Connector를 배포합니다"
- "GCVE로 HCX ServiceMesh를 구성합니다"
- "HCX를 사용하는 VM을 GCVE로 마이그레이션합니다"

수 있습니다

- "GCVE에 대한 HCX Connector 배포"
- "GCVE에 대한 HCX ServiceMesh 구성"
- "GCVE로 HCX 워크로드 마이그레이션"

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 웹 사이트 링크를 참조하십시오.

- Google Cloud VMware Engine 설명서

  "https://cloud.google.com/vmware-engine/docs/overview"

- Cloud Volume Service 설명서

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes"

- VMware HCX 사용자 가이드

  "https://docs.vmware.com/en/VMware-HCX/index.html"

Veeam 복제 기능을 사용하여 **Google Cloud VMware Engine**에서 **NetApp Cloud Volume Service NFS** 데이터 저장소로 **VM** 마이그레이션

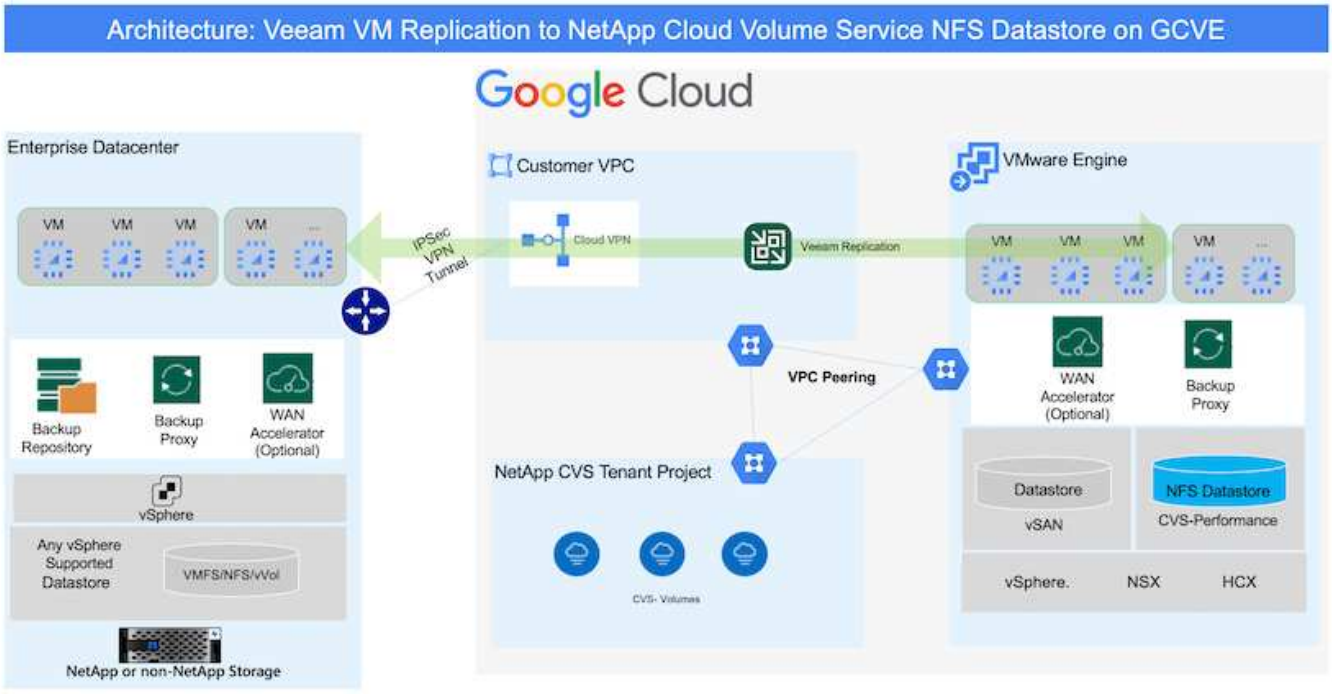
현재 데이터 보호 요구사항에 Veeam을 사용하는 고객은 이 솔루션을 사용하여 워크로드를 GCVE로 마이그레이션하고 NetApp Cloud Volume Service NFS 데이터 저장소의 이점을 계속 누릴 수 있습니다.

개요

저자: NetApp Suesh Thoppay

VMware vSphere에서 실행되는 VM 워크로드는 Veeam Replication 기능을 활용하여 Google Cloud VMware Engine(GCVE)으로 마이그레이션할 수 있습니다.

이 문서에서는 NetApp Cloud Volume Service, Veeam 및 Google Cloud VMware Engine(GCVE)을 사용하는 VM 마이그레이션을 설정하고 수행하기 위한 단계별 접근 방식을 제공합니다.



가정

이 문서에서는 기존 vSphere 서버에서 Google Cloud VMware Engine으로의 네트워크 연결을 설정할 수 있는 Google Cloud VPN 또는 Cloud Interconnect 또는 기타 네트워킹 옵션이 있다고 가정합니다.

온프레미스 데이터 센터를 Google Cloud에 연결하는 옵션에는 여러 가지가 있으며, 이로 인해 NetApp에서 이 문서의 특정 워크플로우를 개괄적으로 설명하지 못하게 됩니다.
을 참조하십시오 "Google Cloud 설명서" 을 참조하십시오.

마이그레이션 솔루션 배포

솔루션 구축 개요

1. NetApp 클라우드 볼륨 서비스의 NFS 데이터 저장소가 GCVE vCenter에 마운트되어 있는지 확인합니다.
2. Veeam Backup Recovery를 기존 VMware vSphere 환경에 구축했는지 확인합니다
3. 복제 작업을 생성하여 가상 시스템을 Google Cloud VMware Engine 인스턴스로 복제를 시작합니다.
4. Veeam 복제 작업의 페일오버를 수행합니다.
5. Veeam에서 영구 페일오버를 수행합니다.

배포 세부 정보

NetApp 클라우드 볼륨 서비스의 **NFS** 데이터 저장소가 **GCVE vCenter**에 마운트되어 있는지 확인합니다

GCVE vCenter에 로그인하고 공간이 충분한 NFS 데이터 저장소를 사용할 수 있는지 확인합니다.
그렇지 않은 경우 을 참조하십시오 "GCVE에서 NetApp CVS를 NFS 데이터 저장소로 마운트합니다"

Veeam Backup Recovery를 기존 **VMware vSphere** 환경에 구축했는지 확인합니다

을 참조하십시오 "Veeam 복제 구성 요소" 필요한 구성 요소 설치 설명서

복제 작업을 생성하여 가상 시스템을 **Google Cloud VMware Engine** 인스턴스로 복제를 시작합니다**.**

사내 vCenter와 GCVE vCenter를 모두 Veeam에 등록해야 합니다. "vSphere VM 복제 작업을 설정합니다"
다음은 방법을 설명하는 비디오입니다
"복제 작업을 구성합니다".

> 복제 VM은 소스 VM과 다른 IP를 가질 수 있으며 다른 포트 그룹에 연결할 수도 있습니다. 자세한 내용은 위의 동영상을 확인하십시오.

Veeam 복제 작업의 페일오버를 수행합니다

VM을 마이그레이션하려면 를 수행합니다 "페일오버를 수행합니다"

Veeam에서 영구 페일오버를 수행합니다**.**

GCVE를 새 소스 환경으로 처리하려면 를 수행합니다 "영구 페일오버"

이 솔루션의 이점

- 기존 Veeam 백업 인프라를 마이그레이션에 활용할 수 있습니다.
- Veeam Replication을 사용하면 타겟 사이트에서 VM IP 주소를 변경할 수 있습니다.
- Veeam 외부에서 복제된 기존 데이터를 재매핑할 수 있습니다(예: BlueXP의 복제된 데이터).
- 대상 사이트에 다른 네트워크 포트 그룹을 지정할 수 있습니다.
- VM의 전원 켜기 순서를 지정할 수 있습니다.
- VMware Change Block Tracking을 활용하여 WAN을 통해 전송할 데이터 양을 최소화합니다.
- 복제를 위해 사전/사후 스크립트를 실행할 수 있는 기능
- 스냅샷에 대한 사전/사후 스크립트를 실행할 수 있습니다.

지역 가용성 – Google Cloud Platform(GCP)용 보조 NFS 데이터 저장소

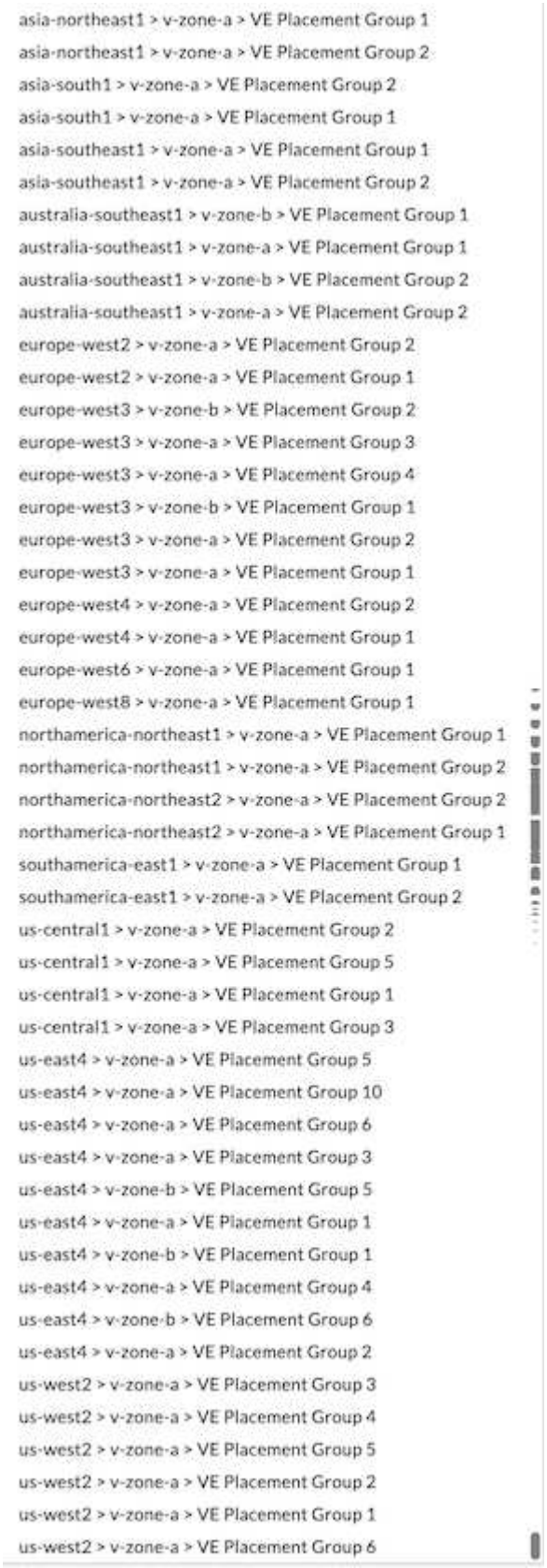
GCP, GCVE 및 CVS에 대한 글로벌 지역 지원에 대해 자세히 알아보십시오.

> NFS 데이터 저장소는 두 서비스(GCVE 및 CVS 성능)를 모두 사용할 수 있는 지역에서 사용할 수 있습니다.

GCVE용 보조 NFS 데이터 저장소는 NetApp 클라우드 볼륨 서비스에서 지원됩니다.

> CVS 전용 - GCVE NFS 데이터 저장소에는 성능 볼륨을 사용할 수 있습니다.
> 사용 가능한 위치는 을 참조하십시오 "글로벌 지역 지도"

Google Cloud VMware Engine은 다음 위치에서 제공됩니다.



지연 시간을 최소화하려면 볼륨을 마운트하려는 NetApp CVS 볼륨 및 GCVE가 동일한 가용성 영역에 있어야 합니다. Google 및 NetApp 솔루션 설계자와 협력하여 가용성 및 TCO 최적화

보안 개요 - Google Cloud의 NetApp CVS(Cloud Volumes Service

TR-4918: 보안 개요 - Google Cloud의 NetApp Cloud Volumes Service

Oliver Krause, Justin Parisi, NetApp

특히, 인프라가 스토리지 관리자의 제어 범위를 벗어난 클라우드의 경우 보안은 데이터를 클라우드 공급자가 제공하는 서비스 제공에 맡기는 것이 무엇보다 중요합니다. 이 문서는 NetApp의 보안 제품에 대한 개요입니다 "Cloud Volumes Service는 Google Cloud에서 제공합니다".

대상

이 문서의 대상 고객은 다음과 같은 역할을 포함하지만 이에 국한되지 않습니다.

- 설명합니다
- 스토리지 관리자
- 스토리지 설계자
- 현장 리소스
- 비즈니스 의사 결정자

이 기술 보고서의 내용에 대해 궁금한 점이 있으면 섹션을 참조하십시오 ""문의하기""

약어	정의
CVS-SW	Cloud Volumes Service, 서비스 유형 CVS
CVS - 성능	클라우드 볼륨 서비스, 서비스 유형 CVS - 성능
PSA	

Google Cloud의 Cloud Volumes Service로 데이터를 보호하는 방법

Google Cloud의 Cloud Volumes Service는 기본적으로 데이터를 보호할 수 있는 다양한 방법을 제공합니다.

안전한 아키텍처 및 테넌시 모델

Cloud Volumes Service는 서로 다른 엔드포인트에 걸쳐 서비스 관리(컨트롤 플레인)와 데이터 액세스(데이터 플레인)를 세분화하여 Google Cloud의 보안 아키텍처를 제공하므로 다른 엔드포인트에 영향을 미치지 않습니다(섹션 참조) ""Cloud Volumes Service 아키텍처"")를 클릭합니다. Google을 사용합니다 "프라이빗 서비스 액세스" (PSA) 프레임워크를 사용하여 서비스를 제공합니다. 이 프레임워크는 NetApp에서 제공하고 운영하는 서비스 생산자와 고객 프로젝트에서 VPC(가상 프라이빗 클라우드)인 서비스 소비자 간의 차이를 구별하며, Cloud Volumes Service 파일 공유에 액세스할 클라이언트를 호스팅합니다.

이 아키텍처에서 테넌트는 섹션을 참조하십시오 ""임차 모델"")는 사용자가 명시적으로 연결하지 않는 한 서로 완전히 격리된 Google Cloud 프로젝트로 정의됩니다. 테넌트를 통해 Cloud Volumes Service 볼륨 플랫폼을 사용하는 다른 테넌트에서 데이터 볼륨, 외부 이름 서비스 및 기타 필수 요소를 완벽하게 격리할 수 있습니다. Cloud Volumes Service

플랫폼은 VPC 피어링을 통해 연결되므로 이러한 격리가 적용됩니다. 공유 VPC를 사용하여 여러 프로젝트 간에 Cloud Volumes Service 볼륨을 공유할 수 있습니다(섹션 참조) ""공유 VPC"")를 클릭합니다. SMB 공유 및 NFS 내보내기에 액세스 제어를 적용하여 데이터 세트를 보거나 수정할 수 있는 사용자 또는 항목을 제한할 수 있습니다.

컨트롤 플레인을 위한 강력한 **ID** 관리

Cloud Volumes Service 구성이 수행되는 컨트롤 플레인에서 을 사용하여 ID 관리를 관리합니다 "IAM(Identity Access Management)". IAM은 Google Cloud 프로젝트 인스턴스에 대한 인증(로그인) 및 권한 부여(권한)를 제어할 수 있는 표준 서비스입니다. 모든 구성은 TLS 1.2 암호화를 사용하는 보안 HTTPS 전송을 통해 Cloud Volumes Service API로 수행되며, 보안을 강화하기 위해 JWT 토큰을 사용하여 인증이 수행됩니다. Cloud Volumes Service용 Google 콘솔 UI는 사용자 입력을 Cloud Volumes Service API 호출로 변환합니다.

보안 강화 **-** 공격 표면 제한

효과적인 보안 기능 중 일부는 서비스에서 사용할 수 있는 공격 표면의 수를 제한하고 있습니다. 공격 표면에는 유휴 데이터, 전송 중 데이터 전송, 로그인 및 데이터 세트 자체를 비롯한 다양한 사항이 포함될 수 있습니다.

관리되는 서비스는 기본적으로 설계의 일부 공격 표면을 제거합니다. 섹션에 설명된 대로 인프라스트럭처 관리 ""서비스 운영,"" 전담 팀에 의해 처리되고, 사람이 실제로 구성에 접촉하는 횟수를 줄이기 위해 자동화되어 의도적이거나 의도하지 않은 오류의 수를 줄입니다. 필요한 서비스만 서로 액세스할 수 있도록 네트워킹이 차단되었습니다. 암호화는 데이터 저장소에 저장되며 데이터 플레인에 대해서만 Cloud Volumes Service 관리자의 보안 주의가 필요합니다. API 인터페이스 뒤에 대부분의 관리 기능을 숨기면 공격 표면을 제한하여 보안을 달성할 수 있습니다.

제로 트러스트 모델

역사적으로 IT 보안 철학은 위협을 완화하기 위해 외부 메커니즘(예: 방화벽 및 침입 탐지 시스템)에만 의존하는 것으로 확인되고 검증해야 했습니다. 그러나 피싱, 사회 공학, 내부자 위협 및 네트워크에 침입하고 파괴를 초래할 수 있는 확인 기능을 제공하는 기타 방법을 통해 환경의 확인을 우회하기 위해 공격과 침해가 진화했습니다.

제로 트러스트는 "모든 것을 검증하면서 아무것도 신뢰하지 않는다"라는 현재의 원칙을 바탕으로 보안 측면에서 새로운 방식이 되었습니다. 따라서 기본적으로 액세스가 허용되지 않습니다. 표준 방화벽, 침입 탐지 시스템(IDS)을 비롯한 다양한 방법과 다음과 같은 방법을 바탕으로 이러한 원칙을 적용합니다.

- 강력한 인증 방법(예: AES 암호화 Kerberos 또는 JWT 토큰)
- 강력한 단일 ID 소스(예: Windows Active Directory, LDAP(Lightweight Directory Access Protocol) 및 Google IAM)
- 네트워크 세분화 및 보안 멀티 테넌시(테넌트만 기본적으로 액세스 허용)
- 최소 권한 액세스 정책을 통한 세분화된 액세스 제어
- 디지털 감사 및 종이 추적을 지원하는 신뢰할 수 있는 전담 관리자의 소규모 독점 목록

Google Cloud에서 실행되는 Cloud Volumes Service는 "신뢰, 모든 것을 확인"하는 입장을 구현하여 제로 트러스트 모델을 고수합니다.

암호화

유휴 데이터 암호화(섹션 참조 ""저장된 데이터 암호화"") XTS-AES-256 암호를 NetApp Volume Encryption(NVE)과 함께 사용하고 를 사용하여 전송 중입니다 ""SMB 암호화"" 또는 NFS Kerberos 5p를 지원합니다. 지역 간 복제 전송은 TLS 1.2 암호화로 보호됩니다(링크: ncvs-gc-security-considerations-and-attack-surface.html#랜섬웨어, 맬웨어 및 바이러스의 감지, 방지 및 완화 #지역 간 복제 ["지역 간 복제"] 참조). 또한 Google 네트워킹은 암호화된 통신도 제공합니다(섹션 참조) ""전송 중인 데이터 암호화"")를 사용하여 공격에 대한 보호 계층을 추가합니다. 전송 암호화에 대한 자세한 내용은 섹션을 참조하십시오 ""Google Cloud 네트워크"".

데이터 보호 및 백업

보안은 단순한 공격 방지에 관한 것이 아닙니다. 또한 공격이 발생할 경우 또는 발생할 때 공격을 어떻게 복구하는지도 다룹니다. 이 전략에는 데이터 보호 및 백업이 포함됩니다. Cloud Volumes Service는 정전 발생 시 다른 지역으로 복제할 수 있는 방법을 제공합니다(섹션 참조) ""지역 간 복제"") 또는 데이터 세트가 랜섬웨어 공격의 영향을 받는 경우 또한 을 사용하여 Cloud Volumes Service 인스턴스 외부의 위치에 데이터를 비동기식으로 백업할 수도 있습니다 "Cloud Volumes Service 백업". 정기적인 백업을 사용하면 보안 이벤트를 완화하는데 소요되는 시간을 줄이고 비용을 절감하고 관리자에게 불안감을 줄 수 있습니다.

업계 최고 수준의 **Snapshot** 복사본으로 랜섬웨어에 신속하게 대응

Cloud Volumes Service은 데이터 보호 및 백업 외에도 변경 불가능한 스냅샷 복사본에 대한 지원을 제공합니다(섹션 참조) ""변경 불가능한 Snapshot 복사본""랜섬웨어 공격으로부터 복구할 수 있는 볼륨(섹션 참조 ""서비스 운영"") 문제를 발견하는 후 몇 초 이내에 운영 중단을 최소화하십시오. 복구 시간과 효과는 스냅샷 일정에 따라 다르지만 랜섬웨어 공격의 경우 한 시간 차이만큼 작은 스냅샷 복사본을 생성할 수 있습니다. 스냅샷 복사본은 성능 및 용량 사용에 거의 영향을 주지 않고, 데이터 세트를 보호하는 데 있어 위험이 낮은 하이 보상 접근 방식입니다.

보안 고려 사항 및 공격 대상

데이터를 보호하는 방법을 이해하기 위한 첫 번째 단계는 위험 및 잠재적 공격 경로를 식별하는 것입니다.

여기에는 다음이 포함됩니다(이에 국한되지 않음).

- 관리 및 로그인
- 사용되지 않는 데이터
- 전송 중인 데이터
- 네트워크 및 방화벽
- 랜섬웨어, 맬웨어 및 바이러스

공격 경로를 이해하면 환경을 보다 안전하게 보호할 수 있습니다. Google Cloud의 Cloud Volumes Service는 이미 이러한 많은 항목을 고려하고 있으며 관리 개입 없이 기본적으로 보안 기능을 구현합니다.

보안 로그인 보장

중요 인프라 구성 요소를 보호할 때는 승인된 사용자만 환경에 로그인하여 관리할 수 있도록 해야 합니다. 공격자들이 관리 자격 증명을 위반하는 경우, 성을 위한 키가 있으며 구성 변경, 볼륨 및 백업 삭제, 백도어 생성, 스냅샷 스케줄 비활성화 등 원하는 모든 작업을 수행할 수 있습니다.

Cloud Volumes Service for Google Cloud는 StaaS(Storage as a Service)의 난독화 기능을 통해 무단 관리 로그인으로부터 보호합니다. Cloud Volumes Service은 외부에서 로그인할 수 없는 상태에서 클라우드 공급자가 완벽하게 유지합니다. 모든 설정 및 구성 작업이 완전히 자동화되므로 매우 드문 경우를 제외하고, 사용자 관리자는 시스템과 상호 작용할 필요가 없습니다.

로그인이 필요한 경우, Google Cloud의 Cloud Volumes Service는 시스템에 로그인할 수 있는 매우 간단한 신뢰할 수 있는 관리자 목록을 유지하여 로그인을 보호합니다. 이 가문부수는 액세스 권한이 있는 잠재적 불량 행위자의 수를 줄이는 데 도움이 됩니다. 또한 Google Cloud 네트워킹은 네트워크 보안 계층 뒤에서 시스템을 숨기고 외부 환경에 필요한 것만 노출합니다. Google Cloud, Cloud Volumes Service 아키텍처에 대한 자세한 내용은 섹션을 참조하십시오 ""Cloud Volumes Service 아키텍처.""

클러스터 관리 및 업그레이드

잠재적 보안 위험이 있는 두 가지 영역에는 클러스터 관리(잘못된 행위자가 관리자 액세스 권한을 가지고 있는 경우 발생하는 현상) 및 업그레이드(소프트웨어 이미지가 손상된 경우 발생하는 현상)가 포함됩니다.

스토리지 관리 보호

서비스형 스토리지를 사용하면 클라우드 데이터 센터 외부의 최종 사용자에 대한 액세스를 제거하여 관리자가 노출될 가능성을 최소화할 수 있습니다. 대신 고객이 데이터 액세스 플레인을 위해 설정하는 것이 유일한 구성입니다. 각 테넌트는 자체 볼륨을 관리하며 테넌트가 다른 Cloud Volumes Service 인스턴스에 연결할 수 없습니다. 이 서비스는 자동화를 통해 관리되며, 이 섹션에서 설명하는 프로세스를 통해 시스템에 액세스할 수 있는 신뢰할 수 있는 관리자의 목록은 매우 적습니다 ""서비스 운영""

CVS - 성능 서비스 유형은 지역 간 복제를 옵션으로 제공하여 지역 장애가 발생할 경우 다른 지역에 데이터를 보호합니다. 이 경우 Cloud Volumes Service를 영향을 받지 않는 영역으로 페일오버하여 데이터 액세스를 유지할 수 있습니다.

서비스 업그레이드

업데이트는 취약한 시스템을 보호하는 데 도움이 됩니다. 각 업데이트는 공격 경로를 최소화하는 보안 향상 기능 및 버그 수정을 제공합니다. 소프트웨어 업데이트는 중앙 저장소에서 다운로드되고 업데이트가 공식 이미지가 사용되고 잘못된 행위자에 의해 업그레이드에 영향을 받지 않는지 확인하기 전에 검증됩니다.

Cloud Volumes Service를 사용하면 클라우드 제공업체 팀이 업데이트를 처리하므로 관리자가 프로세스를 자동화하고 완벽하게 테스트한 구성 및 업그레이드에 정통하여 위험에 노출될 가능성을 줄일 수 있습니다. 업그레이드는 무중단으로 수행할 수 있으며 Cloud Volumes Service는 최신 업데이트를 유지하여 전체적인 결과를 최대한 제공합니다.

이러한 서비스 업그레이드를 수행하는 관리자 팀에 대한 자세한 내용은 섹션을 참조하십시오 ""서비스 운영""

사용되지 않는 데이터의 보안

유휴 데이터 암호화는 디스크 도난, 반환 또는 용도 변경이 발생할 경우 중요한 데이터를 보호하는 데 중요합니다. Cloud Volumes Service의 데이터는 소프트웨어 기반 암호화를 사용하여 유휴 상태에서 보호됩니다.

- Google에서 생성한 키는 CVS-SW에 사용됩니다.
- CVS - 성능의 경우 볼륨별 키는 Cloud Volumes Service에 내장된 키 관리자에 저장되며, NetApp ONTAP CryptoMod를 사용하여 AES-256 암호화 키를 생성합니다. CryptoMod는 CMVP FIPS 140-2 검증 모듈 목록에 나열되어 있습니다. 을 참조하십시오 "FIPS 140-2 인증 번호 4144".

2021년 11월부터 CVS-Performance에 CMEK(Customer-managed Encryption) 기능을 미리 볼 수 있습니다. 이 기능을 사용하면 Google KMS(Key Management Service)에서 호스팅되는 프로젝트별, 지역별 마스터 키를 사용하여 볼륨별 키를 암호화할 수 있습니다. KMS를 사용하면 외부 키 관리자를 연결할 수 있습니다.

CVS용 KMS 구성 방법에 대한 자세한 내용은 "Cloud Volumes Service 설명서를 참조하십시오".

아키텍처에 대한 자세한 내용은 섹션을 참조하십시오 ""Cloud Volumes Service 아키텍처.""

전송 중인 데이터 보안

유휴 데이터의 보안 외에도 Cloud Volumes Service 인스턴스와 클라이언트 또는 복제 타겟 간에 전송 중인 데이터를 안전하게 보호할 수 있어야 합니다. Cloud Volumes Service는 Kerberos를 사용한 SMB 암호화, 패킷의 서명/봉인 및 데이터 전송의 엔드 투 엔드 암호화를 위한 NFS Kerberos 5p 등의 암호화 방법을 사용하여 NAS 프로토콜을 통해 전송 중인 데이터에 대한 암호화를 제공합니다.

Cloud Volumes Service 볼륨의 복제는 TLS-GCM 암호화 방법을 활용하는 TLS 1.2를 사용합니다.

텔넷, NDMP 등과 같이 안전하지 않은 전송 중 프로토콜은 기본적으로 비활성화되어 있습니다. 그러나 DNS는 Cloud Volumes Service에 의해 암호화되지 않으며(DNS 초 지원 없음) 가능하면 외부 네트워크 암호화를 사용하여 암호화해야 합니다. 섹션을 참조하십시오 ""전송 중인 데이터 암호화"" 전송 중인 데이터 보안에 대한 자세한 내용은 를 참조하십시오.

NAS 프로토콜 암호화에 대한 자세한 내용은 섹션을 참조하십시오 ""NAS 프로토콜."""

NAS 권한에 대한 사용자 및 그룹

클라우드에서 데이터를 보호하기 위해서는 적절한 사용자 및 그룹 인증이 필요합니다. 여기서 데이터에 액세스하는 사용자는 해당 환경의 실제 사용자로서 확인되고 그룹에는 유효한 사용자가 포함됩니다. 이러한 사용자 및 그룹은 스토리지 시스템의 파일 및 폴더에 대한 권한 검증뿐만 아니라 초기 공유 및 내보내기 액세스를 제공합니다.

Cloud Volumes Service는 SMB 공유 및 Windows 스타일 권한에 표준 Active Directory 기반 Windows 사용자 및 그룹 인증을 사용합니다. 또한 UNIX용 LDAP 사용자 및 NFS 내보내기, NFSv4 ID 검증, Kerberos 인증 및 NFSv4 ACL을 위한 그룹 등의 UNIX ID 공급자를 활용할 수 있습니다.

현재 Active Directory LDAP만 Cloud Volumes Service for LDAP 기능에서 지원됩니다.

랜섬웨어, 맬웨어 및 바이러스의 감지, 방지 및 완화

랜섬웨어, 맬웨어 및 바이러스는 관리자에게 지속적인 위협이며 이러한 위협을 탐지, 예방 및 완화하는 것은 엔터프라이즈 조직의 최우선 고려입니다. 중요 데이터 세트에서 랜섬웨어 이벤트를 한 번 수행해도 수백만 달러의 비용이 발생할 수 있으므로 위험을 최소화하는 것이 좋습니다.

Cloud Volumes Service에는 현재 바이러스 백신 보호 또는 같은 기본 감지 또는 방지 조치가 포함되어 있지 않습니다 "자동 랜섬웨어 탐지"정기적인 Snapshot 일정을 활성화하여 랜섬웨어 이벤트에서 신속하게 복구할 수 있는 방법이 있습니다. 스냅샷 복사본은 변경할 수 없으며 파일 시스템의 변경된 블록에 대한 읽기 전용 포인터만 사용할 수 있으며, 거의 즉각적으로 성능에 미치는 영향이 최소화되고, 데이터가 변경 또는 삭제될 때만 공간을 사용합니다. 원하는 RPO(복구 시점 목표)/RTO(복구 시간 목표)에 맞게 Snapshot 복사본의 일정을 설정할 수 있으며 볼륨당 최대 1,024개의 Snapshot 복사본을 유지할 수 있습니다.

스냅샷 지원은 Cloud Volumes Service에서 추가 비용 없이(스냅샷 복사본에 의해 유지되는 변경된 블록/데이터에 대한 데이터 스토리지 비용 제외) 포함되며, 랜섬웨어 공격의 경우 공격이 발생하기 전에 스냅샷 복사본으로 롤백하는 데 사용할 수 있습니다. 스냅샷 복원을 완료하는 데 몇 초 밖에 걸리지 않습니다. 그런 다음 정상 데이터 상태로 되돌릴 수 있습니다. 자세한 내용은 을 참조하십시오 "랜섬웨어용 NetApp 솔루션".

랜섬웨어가 비즈니스에 영향을 주지 않도록 하려면 다음 중 하나 이상이 포함된 다계층 접근 방식이 필요합니다.

- 엔드포인트 보호
- 네트워크 방화벽을 통한 외부 위협으로부터 보호
- 데이터 이상 감지
- 중요 데이터 세트에 대한 다중 백업(온사이트 및 오프사이트
- 백업의 정기적인 복원 테스트
- 변경 불가능한 읽기 전용 NetApp Snapshot 복사본
- 중요 인프라를 위한 다단계 인증

- 시스템 로그인에 대한 보안 감사

이 목록은 전체적인 것으로부터 멀리 떨어져 있지만 랜섬웨어 공격의 가능성을 해결할 때 따라야 할 좋은 청사진입니다. Google Cloud의 Cloud Volumes Service는 랜섬웨어 이벤트를 방지하고 효과를 줄일 수 있는 여러 방법을 제공합니다.

변경 불가능한 스냅샷 복사본

Cloud Volumes Service은 데이터를 삭제하거나 랜섬웨어 공격으로 인해 전체 볼륨이 희생된 경우 사용자 지정이 가능한 일정에 따라 진행되는 변경 불가능한 읽기 전용 스냅샷 복사본을 기본적으로 제공합니다. 스냅샷 스케줄 및 RTO/RPO의 보존 기간을 기준으로 Snapshot을 이전 Snapshot 복제본으로 빠르게 복구하고 데이터 손실을 최소화합니다. 스냅샷 기술을 사용할 경우 성능 영향은 미미합니다.

Cloud Volumes Service의 스냅샷 복사본은 읽기 전용이므로 랜섬웨어가 데이터 세트에 확산되지 않고 Snapshot 복사본이 랜섬웨어에 의해 감염된 데이터를 가져가지 않는 한 랜섬웨어에 감염될 수 없습니다. 따라서 데이터 이상을 기반으로 랜섬웨어 탐지를 고려해야 하는 이유가 됩니다. Cloud Volumes Service는 현재 탐지 기능을 기본적으로 제공하지 않지만 외부 모니터링 소프트웨어를 사용할 수 있습니다.

백업 및 복원

Cloud Volumes Service는 표준 NAS 클라이언트 백업 기능(예: NFS 또는 SMB를 통한 백업)을 제공합니다.

- CVS - 성능은 다른 CVS - 성능 볼륨에 대한 교차 지역 볼륨 복제를 제공합니다. 자세한 내용은 을 참조하십시오 "볼륨 복제" Cloud Volumes Service 설명서를 참조하십시오.
- CVS-SW는 서비스 네이티브 볼륨 백업/복원 기능을 제공합니다. 자세한 내용은 을 참조하십시오 "클라우드 백업" Cloud Volumes Service 설명서를 참조하십시오.

볼륨 복제는 랜섬웨어 이벤트를 포함하여 재해 발생 시 신속한 페일오버를 위해 소스 볼륨의 정확한 복사본을 제공합니다.

지역 간 복제

CVS - 성능은 Google 네트워크에서 실행되는 복제에 사용되는 특정 인터페이스를 사용하여 NetApp이 제어하는 백엔드 서비스 네트워크에서 TLS1.2 AES 256 GCM 암호화를 사용하여 데이터 보호 및 아카이브 사용 사례를 위해 Google Cloud 지역 전반에 걸쳐 볼륨을 안전하게 복제할 수 있게 해줍니다. 운영(소스) 볼륨에는 활성 운영 데이터가 포함되어 있으며 보조(대상) 볼륨에 복제하여 운영 데이터 세트의 정확한 복제본을 제공합니다.

초기 복제는 모든 블록을 전송하지만 업데이트는 변경된 블록만 운영 볼륨에서 전송합니다. 예를 들어, 기본 볼륨에 상주하는 1TB 데이터베이스가 보조 볼륨으로 복제되면 1TB 공간이 초기 복제 시 전송됩니다. 해당 데이터베이스에 초기화와 다음 업데이트 간에 변경되는 수백 개의 행(몇 MB)이 있는 경우 변경된 행이 있는 블록만 보조 블록(몇 MB)으로 복제됩니다. 이렇게 하면 전송 시간이 낮게 유지되고 복제 비용이 계속 감소되도록 할 수 있습니다.

파일 및 폴더에 대한 모든 권한은 보조 볼륨으로 복제되지만 내보내기 정책 및 규칙, SMB 공유 및 ACL 공유 등의 공유 액세스 권한은 별도로 처리해야 합니다. 사이트 장애 조치의 경우 대상 사이트는 동일한 이름 서비스와 Active Directory 도메인 연결을 활용하여 사용자 및 그룹 ID와 사용 권한을 일관된 방식으로 처리해야 합니다. 재해 발생 시 보조 볼륨을 페일오버 타겟으로 사용할 수 있습니다. 즉, 2차 볼륨을 읽기-쓰기로 변환하는 복제 관계를 끊으면 됩니다.

볼륨 복사본은 읽기 전용이며, 바이러스가 감염된 데이터를 가지고 있거나 랜섬웨어가 기본 데이터 세트를 암호화한 경우 데이터를 빠르게 복구하기 위해 변경 불가능한 데이터 사본을 오프사이트에 제공합니다. 읽기 전용 데이터는 암호화되지 않지만 운영 볼륨이 영향을 받고 복제가 발생하는 경우 감염된 블록도 복제됩니다. 오래되고 영향을 받지 않는 Snapshot 복사본을 사용하여 복구할 수 있지만, 공격이 탐지되는 속도에 따라 SLA가 약속된 RTO/RPO의 범위를 벗어날 수 있습니다.

또한 Google Cloud에서 CRR(Cross-Region Replication) 관리를 통해 볼륨 삭제, 스냅샷 삭제 또는 스냅샷 스케줄 변경과 같은 악의적인 관리 작업을 방지할 수 있습니다. 이 작업은 볼륨 관리자를 분리하는 사용자 지정 역할을 생성하여 수행합니다. 볼륨 관리자는 소스 볼륨을 삭제할 수는 있지만 미러를 중단할 수는 없으므로 볼륨 작업을 수행할 수 없는 CRR 관리자로부터 대상 볼륨을 삭제할 수 없습니다. 을 참조하십시오 "보안 고려 사항" 각 관리자 그룹이 허용하는 권한에 대한 Cloud Volumes Service 문서

Cloud Volumes Service 백업

Cloud Volumes Service는 높은 데이터 내구성을 제공하지만 외부 이벤트는 데이터 손실을 일으킬 수 있습니다. 바이러스 또는 랜섬웨어와 같은 보안 이벤트가 발생할 경우, 백업 및 복원이 시기적절하게 데이터 액세스를 재개하는 데 중요한 역할을 합니다. 관리자가 실수로 Cloud Volumes Service 볼륨을 삭제할 수 있습니다. 또는 사용자가 단순히 데이터 백업 버전을 몇 개월 동안 유지하고 볼륨 내에 추가 Snapshot 복사본 공간을 유지하는 것은 비용 문제가 됩니다. Snapshot 복사본이 최근 몇 주 동안 손실된 데이터를 복원하는 백업 버전을 보관하는 기본 방법이어야 하지만, 볼륨 내에 있으며 볼륨이 없어지면 손실됩니다.

이러한 모든 이유로 NetApp Cloud Volumes Service은 를 통해 백업 서비스를 제공합니다 "Cloud Volumes Service 백업".

Cloud Volumes Service 백업은 GCS(Google Cloud Storage)에서 볼륨의 복사본을 생성합니다. 사용 가능한 공간이 아닌 볼륨 내에 저장된 실제 데이터만 백업합니다. 영구 증분 방식으로 작동하므로 볼륨 콘텐츠를 한 번 전송하고 변경된 데이터만 계속 백업합니다. 여러 개의 전체 백업을 사용하는 기존 백업 개념에 비해 많은 양의 백업 스토리지를 절약하여 비용을 절감합니다. 백업 공간의 월별 가격이 볼륨에 비해 낮기 때문에 백업 버전을 더 오래 유지하는 것이 좋습니다.

사용자는 Cloud Volumes Service 백업을 사용하여 모든 백업 버전을 동일한 지역 내의 동일한 볼륨 또는 다른 볼륨으로 복원할 수 있습니다. 소스 볼륨이 삭제되면 백업 데이터가 보존되므로 독립적으로 관리(예: 삭제)해야 합니다.

Cloud Volumes Service 백업은 Cloud Volumes Service에 옵션으로 내장되어 있습니다. 사용자는 볼륨별로 Cloud Volumes Service 백업을 활성화하여 보호할 볼륨을 결정할 수 있습니다. 를 참조하십시오 "Cloud Volumes Service 백업 설명서" 백업에 대한 자세한 내용은 를 참조하십시오 "지원되는 최대 백업 버전 수입니다", 스케줄링 및 을 참조하십시오 "가격".

프로젝트의 모든 백업 데이터는 GCS 버킷 내에 저장되며, 이 버킷은 서비스에서 관리되며 사용자에게 표시되지 않습니다. 프로젝트마다 다른 버킷을 사용합니다. 현재 버킷은 Cloud Volumes Service 볼륨과 동일한 영역에 있지만 더 많은 옵션에 대해 논의 중입니다. 최신 상태는 설명서를 참조하십시오.

Cloud Volumes Service 버킷에서 GCS로 데이터를 전송하는 경우 HTTPS 및 TLS1.2가 포함된 서비스 내부 Google 네트워크를 사용합니다. 데이터는 Google에서 관리하는 키로 유휴 상태로 암호화됩니다.

Cloud Volumes Service 백업(백업 생성, 삭제 및 복원)을 관리하려면 사용자에게 이 있어야 합니다 " 역할/netappcloudvolumes.admin" 역할.

있습니다

개요

클라우드 솔루션을 신뢰하는 것은 아키텍처와 보안 방식을 이해하는 것입니다. 이 섹션에서는 Google의 Cloud Volumes Service 아키텍처의 다양한 측면을 다루어 데이터 보안 방식에 대한 잠재적 우려를 완화하고 가장 안전한 배포를 위해 추가 구성 단계가 필요할 수 있는 영역을 설명합니다.

Cloud Volumes Service의 일반 아키텍처는 컨트롤 플레인과 데이터 플레인의 두 가지 주요 구성 요소로 나눌 수 있습니다.

컨트롤 플레인

Cloud Volumes Service의 제어 플레인은 Cloud Volumes Service 관리자와 NetApp 기본 자동화 소프트웨어가 관리하는 백엔드 인프라입니다. 이 방식은 최종 사용자에게 전혀 영향을 미치지 않으며 네트워킹, 스토리지 하드웨어, 소프트웨어 업데이트 등을 포함하여 Cloud Volumes Service와 같은 클라우드 상주 솔루션에 가치를 제공하는 데 도움을 줍니다.

데이터 플레인

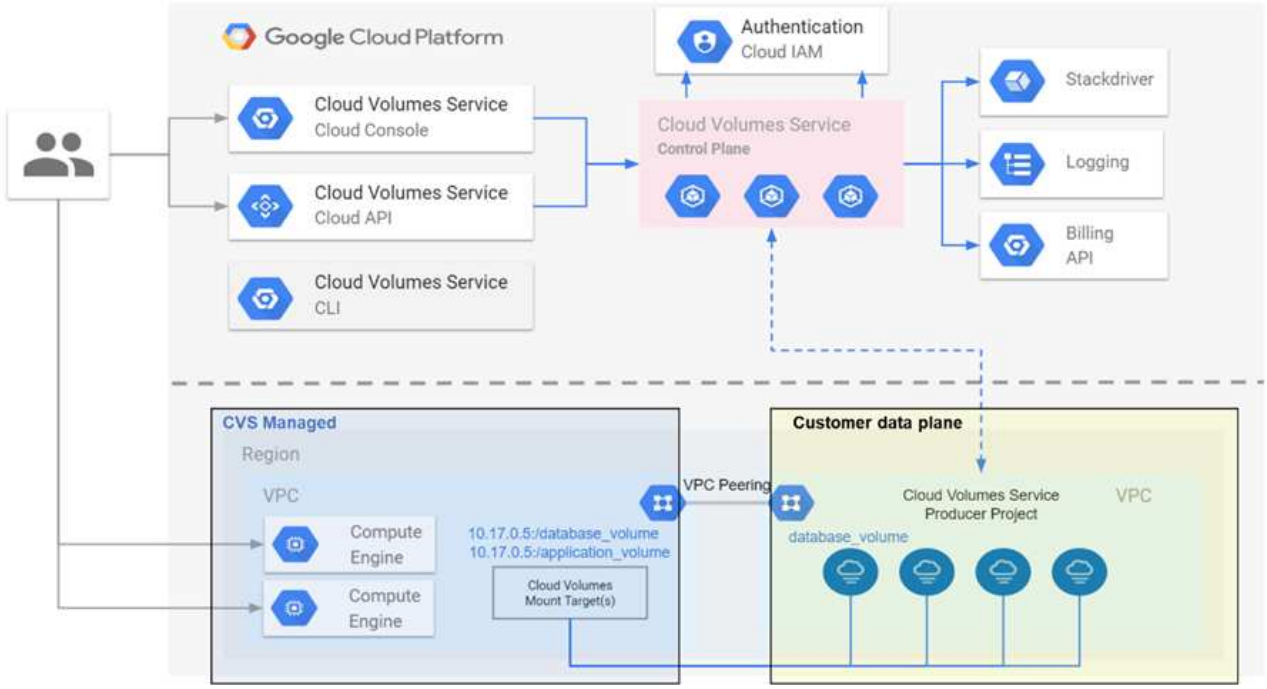
Cloud Volumes Service의 데이터 계층에는 실제 데이터 볼륨과 전체 Cloud Volumes Service 구성(액세스 제어, Kerberos 인증 등)이 포함됩니다. 데이터 플레인은 전적으로 최종 사용자와 Cloud Volumes Service 플랫폼 소비자를 제어하는 것입니다.

각 평면의 보안 및 관리 방법은 서로 다릅니다. 다음 섹션에서는 Cloud Volumes Service 아키텍처 개요부터 이러한 차이점에 대해 설명합니다.

Cloud Volumes Service 아키텍처

CloudSQL, GCVE(Google Cloud VMware Engine) 및 파일 저장소와 같은 다른 Google Cloud 네이티브 서비스와 유사한 방식으로 Cloud Volumes Service는 을 사용합니다 "Google PSA" 서비스를 제공합니다. PSA에서는 서비스를 사용하는 서비스 프로듀서 프로젝트에 내장하고 있습니다 "VPC 네트워크 피어링" 서비스 소비자에 연결합니다. 서비스 생산자는 NetApp에서 제공 및 운영하고, 서비스 소비자는 고객 프로젝트에서 VPC로, Cloud Volumes Service 파일 공유에 액세스하려는 클라이언트를 호스팅합니다.

에서 참조하는 다음 그림 "아키텍처 섹션을 참조하십시오" 에서는 Cloud Volumes Service 설명서의 개략적인 보기를 보여 줍니다.



점선 위의 파트는 볼륨 수명 주기를 제어하는 서비스의 컨트롤 평면을 보여줍니다. 점선 아래의 부분은 데이터 평면을 나타냅니다. 왼쪽 파란색 상자는 사용자 VPC(서비스 소비자)를 나타내고 오른쪽 파란색 상자는 NetApp에서 제공하는

서비스 생산업체입니다. 둘 다 VPC 피어링을 통해 연결됩니다.

테넌시 모델

Cloud Volumes Service에서 개별 프로젝트는 고유한 테넌트로 간주됩니다. 즉, 볼륨, 스냅샷 복사본 등을 프로젝트 단위로 조작할 수 있습니다. 즉, 모든 볼륨은 자신이 만든 프로젝트의 소유이며 해당 프로젝트에서만 기본적으로 해당 볼륨 내의 데이터를 관리하고 액세스할 수 있습니다. 이는 서비스의 컨트롤 플레인 뷰로 간주됩니다.

공유 **VPC**

데이터 평면 보기에서 Cloud Volumes Service는 공유 VPC에 연결할 수 있습니다. 호스팅 프로젝트 또는 공유 VPC에 연결된 서비스 프로젝트 중 하나에서 볼륨을 생성할 수 있습니다. 공유 VPC에 연결된 모든 프로젝트(호스트 또는 서비스)는 네트워크 계층(TCP/IP)에서 볼륨에 연결할 수 있습니다. 공유 VPC에서 네트워크 연결을 사용하는 모든 클라이언트는 NAS 프로토콜을 통해 데이터에 액세스할 수 있으므로 개별 볼륨의 액세스 제어(예: 사용자/그룹 ACL(액세스 제어 목록) 및 NFS 내보내기의 호스트 이름/IP 주소)를 사용하여 데이터에 액세스할 수 있는 사용자를 제어해야 합니다.

고객 프로젝트당 최대 5대의 VPC에 Cloud Volumes Service를 연결할 수 있습니다. 제어 플레인에서 프로젝트를 사용하면 연결된 VPC에 관계없이 생성된 모든 볼륨을 관리할 수 있습니다. 데이터 플레인에서 VPC는 서로 격리되며 각 볼륨은 하나의 VPC에만 연결할 수 있습니다.

개별 볼륨에 대한 액세스는 프로토콜별(NFS/SMB) 액세스 제어 메커니즘에 의해 제어됩니다.

즉, 네트워크 계층에서 공유 VPC에 연결된 모든 프로젝트가 볼륨을 볼 수 있는 반면 관리 측면에서는 소유자 프로젝트만 볼륨을 볼 수 있습니다.

VPC 서비스 제어

VPC 서비스 제어는 인터넷에 연결되어 있고 전 세계적으로 액세스할 수 있는 Google Cloud 서비스에 대한 액세스 제어 경계를 설정합니다. 이러한 서비스는 사용자 ID를 통해 액세스 제어를 제공하지만 어떤 네트워크 위치 요청이 시작되기까지의 지 제한할 수 없습니다. VPC 서비스는 정의된 네트워크에 대한 액세스를 제한하는 기능을 도입하여 이러한 격차를 해소합니다.

Cloud Volumes Service 데이터 플레인은 외부 인터넷에 연결되지 않고 잘 정의된 네트워크 경계(경계)가 있는 전용 VPC에 연결됩니다. 해당 네트워크 내에서 각 볼륨은 프로토콜별 액세스 제어를 사용합니다. 외부 네트워크 연결은 Google Cloud 프로젝트 관리자가 명시적으로 만듭니다. 그러나 컨트롤 플레인은 데이터 플레인과 동일한 보호 기능을 제공하지 않으며 모든 곳에서 유효한 자격 증명( )을 사용하여 액세스할 수 있습니다 "JWT 토큰")를 클릭합니다.

즉, Cloud Volumes Service 데이터 플레인은 VPC 서비스 제어를 지원할 필요 없이 VPC 서비스 제어를 명시적으로 사용하지 않고 네트워크 액세스 제어 기능을 제공합니다.

패킷 스니핑/추적 고려 사항

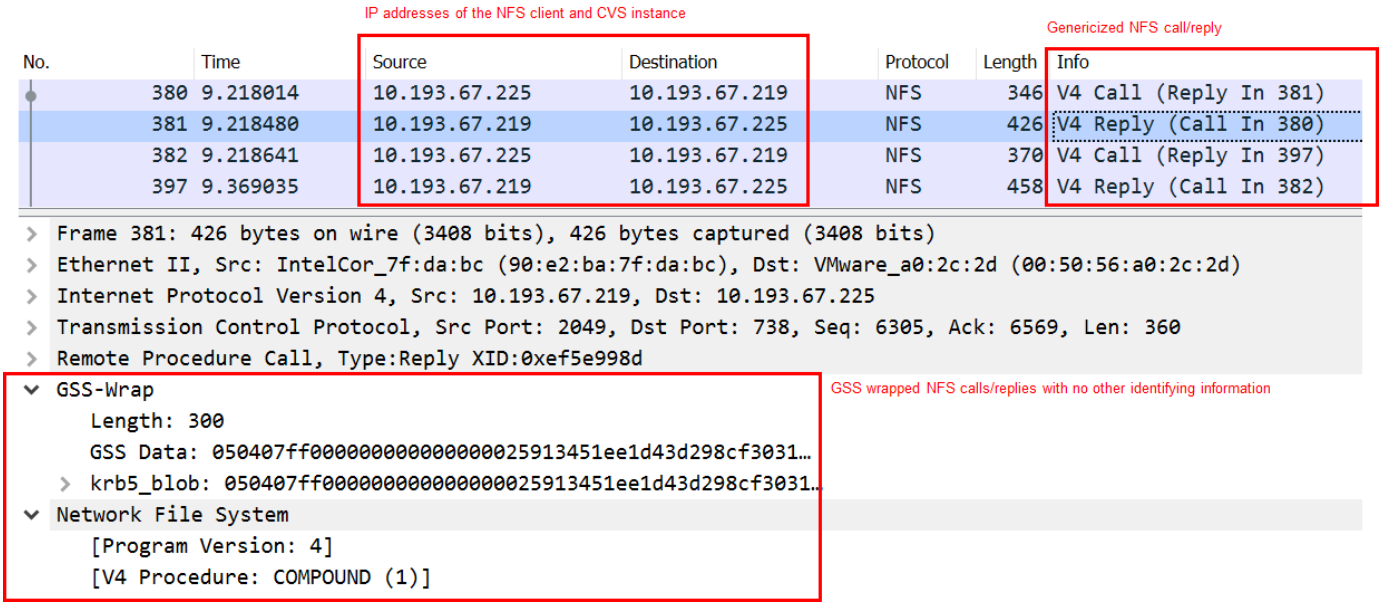
패킷 캡처는 네트워크 문제 또는 기타 문제(예: NAS 권한, LDAP 연결 등)를 해결하는 데 유용할 수 있지만 네트워크 IP 주소, MAC 주소, 사용자 및 그룹 이름 및 엔드포인트에서 사용되는 보안 수준에 대한 정보를 얻기 위해 악의적으로 사용할 수도 있습니다. Google Cloud 네트워킹, VPC 및 방화벽 규칙이 구성된 방식 때문에 사용자 로그인 자격 증명 또는 없이 네트워크 패킷에 대한 원치 않는 액세스를 얻기가 어렵습니다 "JWT 토큰" 클라우드로 인스턴스. 공유 VPC 및/또는 외부 네트워크 터널/IP 전달을 사용하여 엔드포인트에 대한 외부 트래픽을 명시적으로 허용하지 않는 한 패킷 캡처는 엔드포인트(예: 가상 머신(VM))에서만 가능하며 VPC 내부 엔드포인트에서만 가능합니다. 클라이언트 외부의 트래픽을 스니핑할 수 있는 방법은 없습니다.

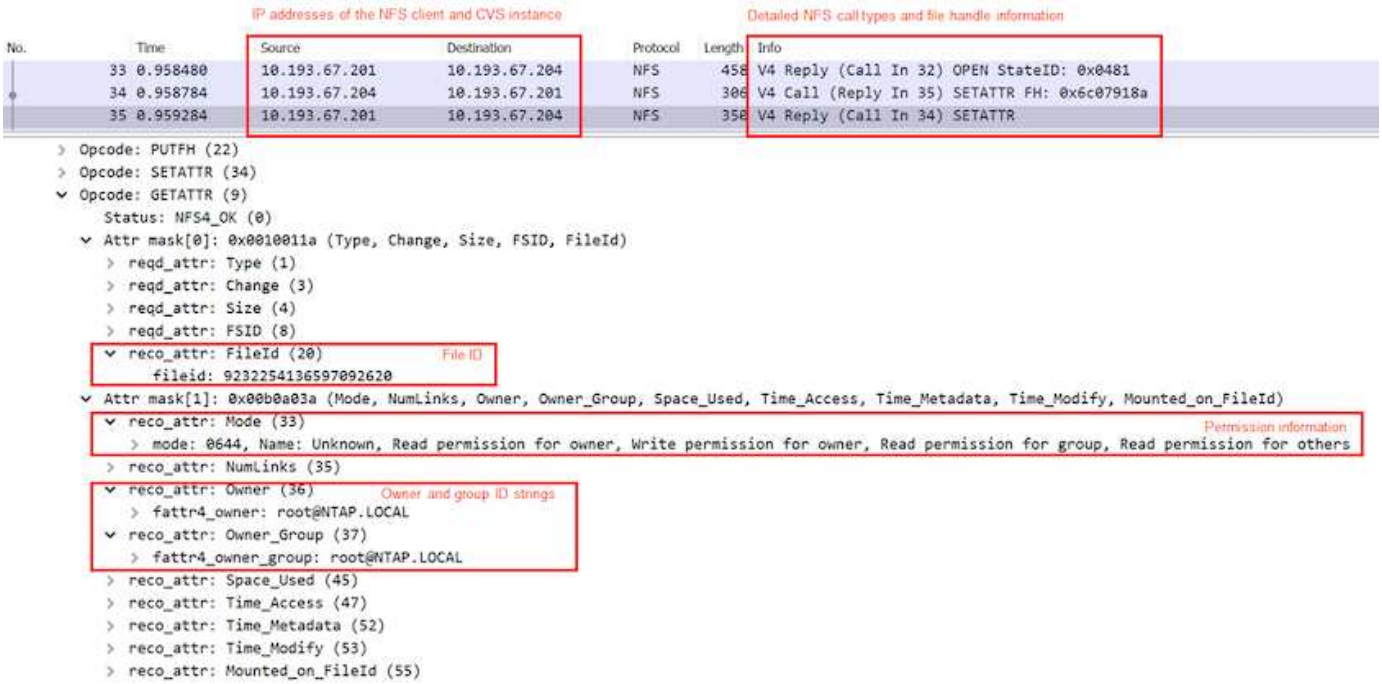
공유 VPC를 사용하는 경우 NFS Kerberos 및/또는 를 사용하여 전송 중 암호화 "SMB 암호화" 트레이스에서 얻은 정보의 대부분을 가릴 수 있습니다. 그러나 일부 트래픽은 과 같은 일반 텍스트로 계속 전송됩니다 "DNS" 및 "LDAP

쿼리입니다". 다음 그림에서는 Cloud Volumes Service에서 생성된 일반 텍스트 LDAP 쿼리 및 노출된 잠재적 식별 정보의 패킷 캡처를 보여 줍니다. Cloud Volumes Service의 LDAP 쿼리는 현재 SSL을 통한 암호화 또는 LDAP를 지원하지 않습니다. Active Directory에서 요청하는 경우 CVS - 성능은 LDAP 서명을 지원합니다. CVS-SW는 LDAP 서명을 지원하지 않습니다.

unixUserPassword는 LDAP에 의해 쿼리되며 일반 텍스트로 전송되지 않고 소염 해시로 보내집니다. 기본적으로 Windows LDAP는 unixUserPassword 필드를 채우지 않습니다. 이 필드는 LDAP를 통해 클라이언트에 대화형 로그인을 위해 Windows LDAP를 활용해야 하는 경우에만 필요합니다. Cloud Volumes Service는 인스턴스에 대한 대화형 LDAP 로그인을 지원하지 않습니다.

다음 그림에서는 AUTH_SYS를 통한 NFS 캡처 옆에 있는 NFS Kerberos 대화의 패킷 캡처를 보여 줍니다. 추적에서 사용할 수 있는 정보가 두 가지 간에 어떻게 다른지, 그리고 전송 중 암호화를 사용하여 NAS 트래픽에 대한 전반적인 보안을 강화하는 방법을 확인하십시오.





VM 네트워크 인터페이스

공격자는 의 VM에 새 NIC(네트워크 인터페이스 카드)를 추가하려고 시도할 수 있습니다 "무차별 모드" 모든 트래픽을 스니핑하기 위해 기존 NIC에서 Promiscuous 모드를 활성화(포트 미러링)하거나 활성화합니다. Google Cloud에서 새 NIC를 추가하려면 VM을 완전히 종료해야 하므로 경고가 생성되므로 공격자가 이를 놓치지 않고 확인할 수 없습니다.

또한 NIC를 무차별 모드로 설정할 수 없으며 Google Cloud에서 경고를 트리거합니다.

컨트롤 플레인 아키텍처

Cloud Volumes Service에 대한 모든 관리 작업은 API를 통해 수행됩니다. GCP 클라우드 콘솔에 통합된 Cloud Volumes Service 관리도 Cloud Volumes Service API를 사용합니다.

ID 및 액세스 관리

ID 및 액세스 관리 ("IAM")는 Google Cloud 프로젝트 인스턴스에 대한 인증(로그인) 및 권한 부여(권한)를 제어할 수 있는 표준 서비스입니다. Google IAM은 권한 승인 및 제거에 대한 전체 감사 추적을 제공합니다. 현재 Cloud Volumes Service는 제어 평면 감사를 제공하지 않습니다.

인증/권한 개요

IAM은 Cloud Volumes Service에 대한 세분화된 기본 권한을 제공합니다. 를 찾을 수 있습니다 "여기에서 세분화된 사용 권한의 전체 목록을 확인할 수 있습니다".

IAM은 또한 netapcloudvolumes.admin과 netapcloudvolumes.viewer라는 두 가지 사전 정의된 역할을 제공합니다. 이러한 역할은 특정 사용자 또는 서비스 계정에 할당할 수 있습니다.

IAM 사용자가 Cloud Volumes Service를 관리할 수 있도록 적절한 역할 및 권한을 할당합니다.

세분화된 사용 권한을 사용하는 예는 다음과 같습니다.

- 사용자가 볼륨을 삭제할 수 없도록 get/list/create/update 권한만 가진 사용자 지정 역할을 만듭니다.

- '스냅샷 *' 권한으로만 사용자 지정 역할을 사용하여 애플리케이션 정합성 보장 스냅샷 통합을 구축하는 데 사용되는 서비스 계정을 생성합니다.
- 특정 사용자에게 '볼륨 증가 *'를 위임하는 사용자 지정 역할을 만듭니다.

서비스 계정

또는 스크립트를 통해 Cloud Volumes Service API 호출을 수행하는 방법 "Terraform(Terraform" 역할/netapcloudvolumes.admin의 역할을 사용하여 서비스 계정을 생성해야 합니다. 이 서비스 계정을 사용하여 Cloud Volumes Service API 요청을 인증하는 데 필요한 JWT 토큰을 다음 두 가지 방법으로 생성할 수 있습니다.

- JSON 키를 생성하고 Google API를 사용하여 JWT 토큰을 파생시킵니다. 이 방법이 가장 간단한 방법이지만 수동 비밀(JSON 키) 관리와 관련이 있습니다.
- 사용 "서비스 계정 가장" 역할/iam.serviceAccountTokenCreator` 포함. 이 코드(스크립트, Terraform 등)는 에서 실행됩니다 "애플리케이션 기본 자격 증명" 서비스 계정을 가장하여 권한을 얻습니다. 이 접근 방식은 Google 보안 모범 사례를 반영합니다.

을 참조하십시오 "서비스 계정 및 개인 키 생성" 자세한 내용은 Google 클라우드 설명서를 참조하십시오.

Cloud Volumes Service API를 참조하십시오

Cloud Volumes Service API는 HTTPS(TLSv1.2)를 기본 네트워크 전송으로 사용하여 REST 기반 API를 사용합니다. 최신 API 정의를 찾을 수 있습니다 "여기" 및 에서 API 사용 방법에 대한 정보를 참조하십시오 "Google Cloud 설명서에서 Cloud Volumes API를 참조하십시오".

API 엔드포인트는 표준 HTTPS(TLSv1.2) 기능을 사용하여 NetApp에서 작동 및 보안됩니다.

JWT 토큰

API에 대한 인증은 JWT 베어러 토큰을 사용하여 수행됩니다 ("RFC-7519")를 클릭합니다. Google Cloud IAM 인증을 사용하여 유효한 JWT 토큰을 얻어야 합니다. 서비스 계정 JSON 키를 제공하여 IAM에서 토큰을 가져와 수행해야 합니다.

로깅 감사

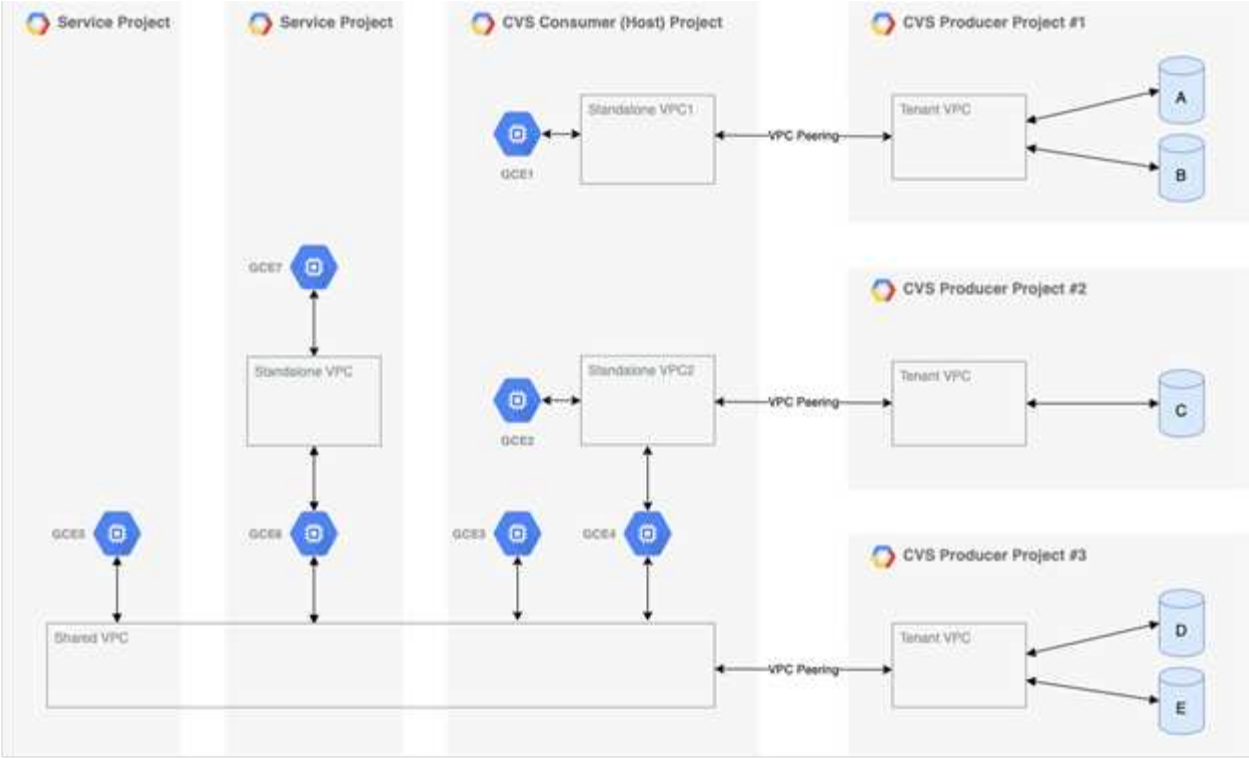
현재 사용자가 액세스할 수 있는 컨트롤 플레인 감사 로그를 사용할 수 없습니다.

데이터 플레인 아키텍처

Cloud Volumes Service for Google Cloud는 Google Cloud를 활용합니다 "프라이빗 서비스 액세스" 프레임워크: 이 프레임워크에서는 사용자가 Cloud Volumes Service에 연결할 수 있습니다. 이 프레임워크는 다른 Google Cloud 서비스와 같은 서비스 네트워킹 및 VPC 피어링 구조를 사용하여 테넌트 간의 완전한 격리를 보장합니다.

Google Cloud용 Cloud Volumes Service의 아키텍처 개요는 를 참조하십시오 "Cloud Volumes Service용 아키텍처".

사용자 VPC(독립 실행형 또는 공유)는 볼륨을 호스팅하는 Cloud Volumes Service 관리 테넌트 프로젝트 내의 VPC에 대해 자세히 살펴봅니다.



위 그림에서는 Cloud Volumes Service에 연결된 VPC 네트워크 3개와 볼륨을 공유하는 GCE1-7(다중 컴퓨팅 엔진 VM)이 포함된 프로젝트(중간 CVS 소비자 프로젝트)를 보여 줍니다.

- VPC1을 사용하면 GCE1이 볼륨 A와 B에 액세스할 수 있습니다
- VPC2는 GCE2와 GCE4가 볼륨 C에 액세스할 수 있도록 합니다
- 세 번째 VPC 네트워크는 공유 VPC로, 두 개의 서비스 프로젝트와 공유됩니다. GCE3, GCE4, GCE5 및 GCE6에서 D 및 E 볼륨에 액세스할 수 있습니다 공유 VPC 네트워크는 CVS 성능 서비스 유형의 볼륨에만 지원됩니다.

GCE7은 어떤 볼륨에도 액세스할 수 없습니다.

데이터는 전송 중(Kerberos 및/또는 SMB 암호화 사용) 및 Cloud Volumes Service에 저장된 데이터를 모두 암호화할 수 있습니다.

전송 중인 데이터 암호화

전송 중인 데이터는 NAS 프로토콜 계층에서 암호화할 수 있으며, Google Cloud 네트워크 자체는 다음 섹션에 설명된 대로 암호화됩니다.

Google Cloud 네트워크

Google Cloud는 에 설명된 대로 네트워크 수준의 트래픽을 암호화합니다 "전송 중인 암호화" Google 문서. “Cloud Volumes Services 아키텍처” 섹션에서 언급한 것처럼 Cloud Volumes Service는 NetApp이 제어하는 PSA 생산자 프로젝트를 통해 제공됩니다.

CVS-SW의 경우 프로듀서 테넌트는 Google VM을 실행하여 서비스를 제공합니다. 사용자 VM과 Cloud Volumes Service VM 간의 트래픽은 Google에서 자동으로 암호화됩니다.

CVS의 데이터 경로 - 성능은 네트워크 계층에서 완전히 암호화되지 않지만, NetApp과 Google은 이 조합을 사용합니다 "IEEE 802.1AE 암호화(MACSec)", "캡슐화" (데이터 암호화) 및 물리적으로 제한된 네트워크를 통해 Cloud Volumes Service CVS - 성능 서비스 유형과 Google 클라우드 간에 전송 중인 데이터를 보호합니다.

NAS 프로토콜

NFS 및 SMB NAS 프로토콜은 프로토콜 계층에서 선택적 전송 암호화를 제공합니다.

SMB 암호화

"SMB 암호화" SMB 데이터의 엔드 투 엔드 암호화를 제공하고 신뢰할 수 없는 네트워크에서 데이터를 도청하지 못하도록 보호합니다. 클라이언트/서버 데이터 연결(SMB3.x 가능 클라이언트에만 사용 가능)과 서버/도메인 컨트롤러 인증에 대해 암호화를 설정할 수 있습니다.

SMB 암호화가 활성화된 경우 암호화를 지원하지 않는 클라이언트는 공유에 액세스할 수 없습니다.

Cloud Volumes Service는 SMB 암호화를 위한 RC4-HMAC, AES-128-CTS-HMAC-SHA1 및 AES-256-CTS-HMAC-SHA1 보안 암호를 지원합니다. SMB는 서버에서 지원되는 가장 높은 암호화 유형으로 협상합니다.

NFSv4.1 Kerberos

NFSv4.1의 경우 CVS - 성능은 에서 설명한 대로 Kerberos 인증을 제공합니다 "RFC7530". 볼륨별로 Kerberos를 활성화할 수 있습니다.

Kerberos에서 현재 가장 강력한 암호화 유형은 AES-256-CTS-HMAC-SHA1입니다. NetApp Cloud Volumes Service는 NFS용 AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 및 DES를 지원합니다. 또한 CIFS/SMB 트래픽에 대해 ARCFOUR-HMAC(RC4)를 지원하지만 NFS에는 지원하지 않습니다.

Kerberos는 Kerberos 보안의 강화 방법을 선택할 수 있는 NFS 마운트에 대해 세 가지 서로 다른 보안 수준을 제공합니다.

RedHat에 따름 "일반 마운트 옵션" 설명서:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

일반적으로 Kerberos 보안 수준이 많을수록 클라이언트와 서버가 전송된 각 패킷의 NFS 작업을 암호화하고 해독하는 데 시간을 소비하므로 성능이 저하됩니다. 많은 클라이언트와 NFS 서버가 AES-NI 오프로딩을 CPU에 지원하므로 전반적인 환경이 개선되지만 Kerberos 5p(전체 엔드 투 엔드 암호화)의 성능 영향은 Kerberos 5(사용자 인증)의 영향보다 훨씬 큽니다.

다음 표에서는 보안 및 성능에 대한 각 수준의 차이점을 보여 줍니다.

보안 수준	보안	성능
NFSv3 - 시스템	• 최소 보안, 숫자 사용자 ID/그룹 ID가 있는 일반 텍스트 • UID, GID, 클라이언트 IP 주소, 내보내기 경로, 파일 이름, 패킷 캡처의 권한	• 대부분의 경우에 적합합니다
NFSv4.x - 시스템	• NFSv3(클라이언트 ID, 이름 문자열/도메인 문자열 일치)보다 더 안전하지만 여전히 일반 텍스트입니다 • UID, GID, 클라이언트 IP 주소, 이름 문자열, 도메인 ID를 볼 수 있습니다. 패킷 캡처의 내보내기 경로, 파일 이름, 권한	• 순차적 워크로드(예: VM, 데이터베이스, 대용량 파일)에 적합 • 파일 개수가 많음/메타데이터 많음(30~50% 악화)
NFS — krb5	• 모든 NFS 패킷의 자격 증명에 대한 Kerberos 암호화 - GSS 래퍼의 RPC 호출에서 사용자/그룹의 UID/GID를 래핑합니다 • 마운트 액세스를 요청하는 사용자는 유효한 Kerberos 티켓(사용자 이름/암호 또는 수동 키 탭 교환)이 필요합니다. 티켓은 지정된 기간 후에 만료되며 사용자는 액세스를 위해 다시 인증해야 합니다 • 마운트/portmapper/NLM 같은 NFS 작업 또는 보조 프로토콜에 대한 암호화 없음(내보내기 경로, IP 주소, 파일 핸들, 권한, 파일 이름 패킷 캡처의 atime/mtime)	• Kerberos의 경우 대부분 최상, AUTH_SYS보다 나쁨

보안 수준	보안	성능
NFS — krb5i	• 모든 NFS 패킷의 자격 증명에 대한 Kerberos 암호화 - GSS 래퍼의 RPC 호출에서 사용자 /그룹의 UID/GID를 래핑합니다 • 마운트 액세스를 요청하는 사용자는 유효한 Kerberos 티켓(사용자 이름/암호 또는 수동 키 탭 교환)이 필요합니다. 티켓은 지정된 기간 후에 만료되며 사용자는 액세스를 위해 다시 인증해야 합니다 • 마운트/portmapper/NLM 같은 NFS 작업 또는 보조 프로토콜에 대한 암호화 없음(내보내기 경로, IP 주소, 파일 핸들, 권한, 파일 이름 패킷 캡처의 atime/mtime) • Kerberos GSS 체크섬은 패킷을 가로챌 수 없도록 모든 패킷에 추가됩니다. 체크섬이 일치하면 대화가 허용됩니다.	• NFS 페이로드가 암호화되지 않기 때문에 krb5p보다 낫습니다. krb5와 비교하여 추가된 오버헤드만 무결성 체크섬입니다. krb5i의 성능은 krb5보다 훨씬 나쁘지는 않지만 약간의 성능 저하가 발생할 수 있습니다.
NFS – krb5p	• 모든 NFS 패킷의 자격 증명에 대한 Kerberos 암호화 - GSS 래퍼의 RPC 호출에서 사용자 /그룹의 UID/GID를 래핑합니다 • 마운트 액세스를 요청하는 사용자는 유효한 Kerberos 티켓(사용자 이름/암호 또는 수동 키 탭 교환)이 필요합니다. 티켓은 지정된 기간 이후에 만료되며 사용자는 액세스를 위해 다시 인증해야 합니다 • 모든 NFS 패킷 페이로드는 GSS 래퍼로 암호화됩니다(패킷 캡처에서 파일 핸들, 권한, 파일 이름, atime/mtime을 볼 수 없음). • 무결성 검사를 포함합니다. • NFS 작업 유형이 표시됩니다(FSINFO, ACCESS, GETATTR 등). • 보조 프로토콜(마운트, 포트 맵, NLM 등)이 암호화되지 않음 - (내보내기 경로, IP 주소 확인 가능)	• 보안 수준의 최악의 성능: krb5p는 더 많은 암호화/암호 해독을 해야 합니다. • 파일 개수가 많은 워크로드에 대해 NFSv4.x를 사용할 경우 krb5p보다 성능이 더 우수합니다.

Cloud Volumes Service에서 구성된 Active Directory 서버는 Kerberos 서버 및 LDAP 서버로 사용됩니다(RFC2307

호환 스키마에서 사용자 ID를 조회하기 위해). 다른 Kerberos 또는 LDAP 서버는 지원되지 않습니다. Cloud Volumes Service에서 ID 관리를 위해 LDAP를 사용하는 것이 좋습니다. 패킷 캡처에서 NFS Kerberos가 표시되는 방법에 대한 자세한 내용은 ncvs-gc-cloud-volumes-service-architecture 링크를 참조하십시오. html#패킷 스니핑/추적 고려 사항 ["패킷 스니핑/추적 고려 사항"]

유휴 데이터 암호화

Cloud Volumes Service의 모든 볼륨은 AES-256 암호화를 사용하여 유휴 상태로 암호화되므로 미디어에 기록된 모든 사용자 데이터가 암호화되며 볼륨당 키를 통해서만 해독할 수 있습니다.

- CVS-SW의 경우 Google에서 생성한 키가 사용됩니다.
- CVS - 성능의 경우 볼륨별 키는 Cloud Volumes Service에 내장된 키 관리자에 저장됩니다.

2021년 11월부터 CMEK(고객 관리 암호화 키) 기능을 미리 볼 수 있습니다. 이렇게 하면 에서 호스팅되는 프로젝트별, 지역별 마스터 키를 사용하여 볼륨별 키를 암호화할 수 있습니다 "Google KMS(키 관리 서비스)." KMS를 사용하면 외부 키 관리자를 연결할 수 있습니다.

CVS용 KMS 구성 - 성능에 대한 자세한 내용은 을 참조하십시오 "고객이 관리하는 암호화 키 설정".

방화벽

Cloud Volumes Service는 NFS 및 SMB 공유를 지원하기 위해 여러 TCP 포트를 노출합니다.

- "NFS 액세스에 필요한 포트 수"
- "SMB 액세스에 필요한 포트"

또한 Kerberos를 비롯한 LDAP를 지원하는 SMB, NFS 및 이중 프로토콜 구성을 사용하려면 Windows Active Directory 도메인에 대한 액세스가 필요합니다. Active Directory 연결은 이어야 합니다 "구성됨" 지역별로 제공됩니다. Active Directory 도메인 컨트롤러(DC)는 를 사용하여 식별합니다 "DNS 기반 DC 검색" 지정된 DNS 서버를 사용합니다. 반환된 DC 중 하나가 사용됩니다. Active Directory 사이트를 지정하면 자격 있는 DC 목록을 제한할 수 있습니다.

Cloud Volumes Service는 와 함께 할당된 CIDR 범위의 IP 주소를 사용하여 에 도달합니다 `gcloud compute address` 명령을 실행하는 동안 "Cloud Volumes Service에 대한 온보딩". 이 CIDR을 소스 주소로 사용하여 Active Directory 도메인 컨트롤러에 대한 인바운드 방화벽을 구성할 수 있습니다.

Active Directory 도메인 컨트롤러가 필요합니다 "여기에 설명된 대로 Cloud Volumes Service CIDR에 포트를 노출합니다".

NAS 프로토콜

NAS 프로토콜 개요

NAS 프로토콜에는 NFS(v3 및 v4.1) 및 SMB/CIFS(2.x 및 3.x)가 포함됩니다. 이러한 프로토콜은 CVS에서 여러 NAS 클라이언트 간에 데이터에 대한 공유 액세스를 허용하는 방법입니다. 또한 Cloud Volumes Service는 NFS 및 SMB/CIFS 클라이언트(이중 프로토콜)에 대한 액세스를 동시에 제공하는 동시에 NAS 공유의 파일 및 폴더에 대한 모든 ID 및 권한 설정을 존중할 수 있습니다. Cloud Volumes Service는 가장 높은 데이터 전송 보안을 유지하기 위해 SMB 암호화 및 NFS Kerberos 5p를 사용하여 전송 중인 프로토콜 암호화를 지원합니다.

이중 프로토콜은 CVS에서 사용할 수 있습니다. - 성능만 지원됩니다.

NAS 프로토콜의 기본 사항

NAS 프로토콜은 여러 클라이언트의 네트워크 상에서 Cloud Volumes Service on GCP와 같은 스토리지 시스템의 동일한 데이터에 액세스하는 방법입니다. NFS 및 SMB는 정의된 NAS 프로토콜로, Cloud Volumes Service이 서버 역할을 하는 클라이언트/서버 단위로 작동합니다. 클라이언트는 서버에 액세스, 읽기 및 쓰기 요청을 보내고, 서버는 파일에 대한 잠금 메커니즘을 조정하고, 사용 권한을 저장하고, ID 및 인증 요청을 처리할 책임이 있습니다.

예를 들어, NAS 클라이언트가 폴더에 새 파일을 생성하려는 경우 다음과 같은 일반 프로세스가 적용됩니다.

1. 클라이언트가 서버에 디렉터리(권한, 소유자, 그룹, 파일 ID, 사용 가능한 공간, 등). 서버는 요청한 클라이언트 및 사용자에게 상위 폴더에 대한 필요한 권한이 있는 경우 해당 정보로 응답합니다.
2. 디렉토리의 사용 권한이 액세스를 허용할 경우 클라이언트는 생성 중인 파일 이름이 파일 시스템에 이미 있는지 서버에 묻습니다. 파일 이름이 이미 사용 중인 경우 생성이 실패합니다. 파일 이름이 없는 경우 서버는 클라이언트가 계속 진행할 수 있음을 알려 줍니다.
3. 클라이언트는 디렉토리 핸들 및 파일 이름으로 파일을 만들기 위해 서버에 대한 호출을 수행하고 액세스 및 수정 시간을 설정합니다. 서버에서 파일에 고유한 파일 ID를 발급하여 동일한 파일 ID로 다른 파일이 생성되지 않도록 합니다.
4. 클라이언트는 쓰기 작업 전에 파일 특성을 확인하는 호출을 전송합니다. 권한이 허용하는 경우 클라이언트는 새 파일을 씁니다. 프로토콜/응용 프로그램에서 잠금을 사용하는 경우 클라이언트는 다른 클라이언트가 잠금 상태에서 파일에 액세스하지 못하도록 서버에 잠금을 요청합니다. 잠금 상태에서는 데이터 손상을 방지할 수 있습니다.

NFS 를 참조하십시오

NFS는 RFC(Request for Comments)에 정의된 공개 IETF 표준인 분산 파일 시스템 프로토콜로, 누구나 프로토콜을 구현할 수 있도록 합니다.

Cloud Volumes Service의 볼륨은 클라이언트 또는 클라이언트 세트에 액세스할 수 있는 경로를 내보내 NFS 클라이언트에 공유됩니다. 이러한 내보내기를 마운트할 수 있는 권한은 Cloud Volumes Service 관리자가 구성할 수 있는 내보내기 정책 및 규칙에 의해 정의됩니다.

NetApp NFS 구현은 프로토콜의 골드 표준으로 간주되며 수많은 엔터프라이즈 NAS 환경에서 사용됩니다. 다음 섹션에서는 NFS와 Cloud Volumes Service에서 사용할 수 있는 특정 보안 기능 및 구현 방법에 대해 설명합니다.

기본 로컬 UNIX 사용자 및 그룹

Cloud Volumes Service에는 다양한 기본 기능을 위한 여러 기본 UNIX 사용자 및 그룹이 포함되어 있습니다. 이러한 사용자 및 그룹은 현재 수정 또는 삭제할 수 없습니다. 현재 새 로컬 사용자 및 그룹을 Cloud Volumes Service에 추가할 수 없습니다. 기본 사용자 및 그룹 외부의 UNIX 사용자 및 그룹은 외부 LDAP 이름 서비스에서 제공해야 합니다.

다음 표에서는 기본 사용자 및 그룹과 해당 숫자 ID를 보여 줍니다. LDAP 또는 이러한 숫자 ID를 다시 사용하는 로컬 클라이언트에서는 새 사용자 또는 그룹을 생성하지 않는 것이 좋습니다.

기본 사용자: 숫자 ID	기본 그룹: 숫자 ID
• 루트: 0 • pcuser: 65534 • 아무도 없다: 65535	• 루트: 0 • 데몬: 1 • pcuser: 65534 • 아무도 없다: 65535

NFSv4.1을 사용하는 경우 NFS 클라이언트에서 디렉토리 목록 명령을 실행할 때 루트 사용자가 아무도 표시되지 않을 수 있습니다. 이는 클라이언트의 ID 도메인 매핑 구성 때문입니다. 의 섹션을 참조하십시오 NFSv4.1 및 그 누구도 사용자/그룹을 대상으로 하지 않습니다 이 문제에 대한 자세한 내용 및 해결 방법을 확인하십시오.

루트 사용자입니다

Linux에서 루트 계정은 Linux 기반 파일 시스템의 모든 명령, 파일 및 폴더에 액세스할 수 있습니다. 이 계정의 강력한 기능 때문에 보안 모범 사례에 따라 루트 사용자를 비활성화하거나 제한해야 하는 경우가 많습니다. NFS 내보내기에서 루트 사용자가 파일과 폴더에 가지고 있는 파워는 내보내기 정책과 규칙, 루트 스쿼시(root squash)라는 개념을 통해 Cloud Volumes Service에서 제어할 수 있습니다.

루트 스쿼싱 기능을 사용하면 NFS 마운트에 액세스하는 루트 사용자가 익명 숫자 사용자 65534에 스쿼트됩니다(“ 섹션 참조)익명 사용자") 및 은(는) 현재 CVS - Performance를 사용하는 경우에만 사용할 수 있습니다. 이 경우 내보내기 정책 규칙 생성 중 루트 액세스에 대해 Off를 선택합니다. 루트 사용자가 익명 사용자에게 스쿼트되면 chown 또는 을 실행할 수 있는 액세스 권한이 더 이상 없습니다 "setuid/setgid 명령(고정 비트)" NFS 마운트의 파일 또는 폴더와 루트 사용자가 생성한 파일 또는 폴더에 anon UID가 소유자/그룹으로 표시됩니다. 또한 루트 사용자가 NFSv4 ACL을 수정할 수 없습니다. 그러나 루트 사용자는 chmod 및 삭제된 파일에 대한 명시적 권한이 없는 액세스 권한을 계속 가집니다. 루트 사용자의 파일 및 폴더 권한에 대한 액세스를 제한하려면 NTFS ACL을 사용하여 볼륨을 사용하고, "root"라는 Windows 사용자를 생성하고, 파일 또는 폴더에 원하는 권한을 적용하는 것이 좋습니다.

익명 사용자

익명(anon) 사용자 ID는 유효한 NFS 자격 증명 없이 도착하는 클라이언트 요청에 매핑된 UNIX 사용자 ID 또는 사용자 이름을 지정합니다. 여기에는 루트 스쿼싱 사용 시 루트 사용자가 포함될 수 있습니다. Cloud Volumes Service의 anon 사용자는 65534입니다.

이 UID는 일반적으로 Linux 환경의 사용자 이름 'nobody' 또는 'nfsnobody’와 관련이 있습니다. Cloud Volumes Service는 로컬 UNIX 사용자 ' pcuser ' 로 65534도 사용합니다(“ 절 참조)기본 로컬 UNIX 사용자 및 그룹"). LDAP에서 일치하는 유효한 UNIX 사용자를 찾을 수 없는 경우 Windows에서 UNIX로의 이름 매핑의 기본 대체 사용자입니다.

Linux의 사용자 이름과 UID 65534의 Cloud Volumes Service 간 사용자 이름 차이로 인해 65534에 매핑된 사용자의 이름 문자열이 NFSv4.1을 사용할 때 일치하지 않을 수 있습니다. 따라서 일부 파일 및 폴더에 대해 사용자로 'nobody’가 표시될 수 있습니다. 자세한 내용은 " 단원을 참조하십시오NFSv4.1 및 그 누구도 사용자/그룹을 대상으로 하지 않습니다"를 참조하십시오.

액세스 제어/내보내기

NFS 마운트에 대한 초기 엑스포트/공유 액세스는 엑스포트 정책 내에 포함된 호스트 기반 엑스포트 정책 규칙을 통해 제어됩니다. 호스트 IP, 호스트 이름, 서브넷, 넷그룹 또는 도메인이 정의되어 NFS 공유를 마운트하는 액세스 권한과 호스트에 허용되는 액세스 수준을 허용합니다. 엑스포트 정책 규칙 구성 옵션은 Cloud Volumes Service 레벨에 따라 다릅니다.

CVS-SW의 경우 내보내기 정책 구성에 다음 옵션을 사용할 수 있습니다.

- * 클라이언트 일치. * 쉼표로 구분된 IP 주소 목록, 쉼표로 구분된 호스트 이름, 서브넷, 넷그룹, 도메인 이름 목록.
- * RO/RW 액세스 규칙 * 내보내기에 대한 액세스 수준을 제어하려면 읽기/쓰기 또는 읽기 전용 을 선택합니다. CVS - 성능은 다음 옵션을 제공합니다.
- * 클라이언트 일치. * 쉼표로 구분된 IP 주소 목록, 쉼표로 구분된 호스트 이름, 서브넷, 넷그룹, 도메인 이름 목록.
- * RO/RW 액세스 규칙. * 읽기/쓰기 또는 읽기 전용 을 선택하여 내보내기에 대한 액세스 수준을 제어합니다.
- * 루트 액세스(켜기/끄기). * 루트 스쿼시를 구성합니다(“ 절 참조)루트 사용자입니다"를 참조하십시오.)
- * Protocol type. * 이 옵션은 NFS 마운트에 대한 액세스를 특정 프로토콜 버전으로 제한합니다. 볼륨에 대해 NFSv3과 NFSv4.1을 모두 지정할 때 두 확인란을 모두 비워 두거나 두 확인란을 모두 선택합니다.
- * Kerberos 보안 수준(Kerberos 활성화 가 선택된 경우). * 읽기 전용 또는 읽기-쓰기 액세스에 대해 krb5, krb5i 및 /또는 krb5p의 옵션을 제공합니다.

변경 소유권**(chown)** 및 변경 그룹**(chgrp)**

Cloud Volumes Service의 NFS에서는 루트 사용자만 파일 및 폴더에 대해 chown/chgrp를 실행할 수 있습니다. 다른 사용자는 자신이 소유한 파일에서도 'Operation not mitted(작업이 허용되지 않음)' 오류를 볼 수 있습니다. 루트 스쿼시를 사용하는 경우(“ 섹션에서 다룹니다루트 사용자입니다”), 루트가 비루트 사용자에게 스쿼트되고 chown 및 chgrp에 대한 액세스가 허용되지 않습니다. 현재 Cloud Volumes Service에는 루트 이외의 사용자에 대한 chown 및 chgrp를 허용하는 대안이 없습니다. 소유권을 변경해야 하는 경우 이중 프로토콜 볼륨을 사용하고 보안 스타일을 NTFS로 설정하여 Windows 측의 권한을 제어할 수 있습니다.

권한 관리

Cloud Volumes Service는 모드 비트(예: rwx의 경우 644, 777 등)와 NFSv4.1 ACL을 모두 지원하여 UNIX 보안 스타일을 사용하는 볼륨의 NFS 클라이언트에 대한 사용 권한을 제어합니다. 이러한 사용자(chmod, chown 또는 nfs4_setfacl 등)에 대해 표준 권한 관리가 사용되며 이를 지원하는 모든 Linux 클라이언트와 함께 작동합니다.

또한 NTFS로 설정된 이중 프로토콜 볼륨을 사용하는 경우 NFS 클라이언트는 Windows 사용자에 대한 Cloud Volumes Service 이름 매핑을 활용할 수 있으며, 이 이름 매핑은 NTFS 권한을 확인하는 데 사용됩니다. Cloud Volumes Service를 Windows 사용자 이름에 올바르게 매핑하려면 유효한 UNIX 사용자 이름이 필요하기 때문에 이를 위해서는 Cloud Volumes Service에 대한 LDAP 연결이 필요합니다.

NFSv3에 대한 세부적인 **ACL** 제공

모드 비트 사용 권한은 소유자, 그룹 및 다른 모든 관련자만 사용할 수 있습니다. 즉, 기본 NFSv3에 대해 세부적인 사용자 액세스 제어를 사용할 수 없습니다. Cloud Volumes Service는 POSIX ACL 또는 확장된 특성(예: chattr)을 지원하지 않으므로 NFSv3을 사용하는 다음 시나리오에서만 세분화된 ACL을 사용할 수 있습니다.

- 유효한 UNIX와 Windows 사용자 간 매핑을 사용하는 NTFS 보안 스타일 볼륨(CIFS 서버 필요)
- NFSv4.1 ACL은 관리 클라이언트 마운트 NFSv4.1을 사용하여 ACL을 적용하여 적용됩니다.

두 방법 모두 UNIX ID 관리를 위한 LDAP 연결과 유효한 UNIX 사용자 및 그룹 정보를 채워야 합니다(섹션 참조) ""LDAP"") 및 은 CVS - 성능 인스턴스에서만 사용할 수 있습니다. NFS에서 NTFS 보안 스타일 볼륨을 사용하려면 SMB 연결이 구성되어 있지 않더라도 이중 프로토콜(SMB 및 NFSv3) 또는 이중 프로토콜(SMB 및 NFSv4.1)을 사용해야 합니다. NFSv3 마운트에서 NFSv4.1 ACL을 사용하려면 프로토콜 유형으로 'both(NFSv3/NFSv4.1)'를 선택해야 합니다.

일반 UNIX 모드 비트는 NTFS 또는 NFSv4.x ACL이 제공하는 사용 권한과 동일한 수준의 세분성을 제공하지

않습니다. 다음 표에서는 NFSv3 모드 비트와 NFSv4.1 ACL 간의 사용 권한 세분화를 비교합니다. NFSv4.1 ACL에 대한 자세한 내용은 을 참조하십시오 "NFS4_ACL-NFSv4 액세스 제어 목록".

NFSv3 모드 비트	**NFSv4.1 ACL**
• 실행 시 사용자 ID를 설정합니다 • 실행 시 그룹 ID를 설정합니다 • 바꾼 텍스트 저장(POSIX에 정의되지 않음) • 소유자에 대한 읽기 권한 • 소유자의 쓰기 권한 • 파일의 소유자에 대한 권한을 실행하거나 디렉터리에서 소유자를 찾기(검색) 권한을 실행합니다 • 그룹에 대한 읽기 권한 • 그룹에 대한 쓰기 권한 • 파일의 그룹에 대한 권한을 실행하거나 디렉터리의 그룹에 대한 검색 권한을 찾습니다 • 다른 사람의 읽기 권한 • 다른 사람에 대한 권한을 작성합니다 • 파일의 다른 사람에 대한 권한을 실행하거나 디렉터리에서 다른 사람에 대한 검색 권한을 찾습니다	ACE(액세스 제어 항목) 형식(허용/거부/감사) * 상속 플래그 * directory-inherit * file-inherit * no-propagate-inherit * inherit-only 권한 * 읽기-데이터(파일)/목록-디렉토리(디렉토리) * 쓰기-데이터(파일)/생성-파일(디렉토리) * 추가-데이터(파일)/생성-하위 디렉토리(디렉토리) * 실행(파일)/변경-디렉토리(디렉토리) * 삭제 * delete-child * read-attributes * write-named-attributes * write-named-acner-write-write-acl-write-write-write-write-acl-write-write-write-write-acl-write-write-write-write-

마지막으로, RPC 패킷 제한에 따라 NFS 그룹 멤버 자격(NFSv3 및 NFSv4.x에서 모두)은 AUTH_SYS에 대한 기본값 최대 16으로 제한됩니다. NFS Kerberos는 최대 32개의 그룹과 NFSv4 ACL을 제공하므로 사용자 및 그룹 ACL(ACE당 최대 1024개 항목)을 세부적으로 적용하여 제한을 제거할 수 있습니다.

또한 Cloud Volumes Service는 지원되는 최대 그룹을 32개까지 확장할 수 있도록 확장된 그룹 지원을 제공합니다. 이를 위해서는 유효한 UNIX 사용자 및 그룹 ID가 포함된 LDAP 서버에 대한 LDAP 연결이 필요합니다. 이 구성을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오 "NFS 볼륨 생성 및 관리" Google 문서.

NFSv3 사용자 및 그룹 **ID**

NFSv3 사용자 및 그룹 ID는 이름이 아닌 숫자 ID로 와이어를 통해 제공됩니다. Cloud Volumes Service는 NFSv3을 사용하는 이러한 숫자 ID에 대해 사용자 이름 확인을 수행하지 않으며 UNIX 보안 스타일 볼륨에서는 모드 비트만 사용합니다. NFSv4.1 ACL이 있으면 NFSv3을 사용하더라도 ACL을 제대로 해결하려면 숫자 ID 조회 및/또는 이름 문자열 조회가 필요합니다. NTFS 보안 스타일 볼륨에서 Cloud Volumes Service는 유효한 UNIX 사용자로 숫자 ID를 확인한 다음 유효한 Windows 사용자에게 매핑하여 액세스 권한을 협상해야 합니다.

NFSv3 사용자 및 그룹 **ID**의 보안 제한

NFSv3에서는 클라이언트와 서버가 숫자 ID로 읽기 또는 쓰기를 시도하는 사용자가 유효한 사용자인지 확인할 필요가 없으며 암시적으로 신뢰됩니다. 이렇게 하면 숫자 ID를 스푸핑하여 파일 시스템이 잠재적 위반으로 열립니다. 이와 같은 보안 문제를 방지하기 위해 Cloud Volumes Service에서 몇 가지 옵션을 사용할 수 있습니다.

- NFS용 Kerberos를 구현하면 사용자가 사용자 이름 및 암호 또는 keytab 파일로 인증하여 Kerberos 티켓을 받아 마운트에 액세스할 수 있도록 합니다. Kerberos는 CVS에서 사용 가능 - 성능 인스턴스와 NFSv4.1에서만 지원됩니다.

- 엑스포트 정책 규칙에 따라 호스트 목록을 제한하면 NFSv3 클라이언트가 Cloud Volumes Service 볼륨에 액세스할 수 있는 범위가 제한됩니다.
- 이중 프로토콜 볼륨을 사용하고 NTFS ACL을 볼륨에 적용하면 NFSv3 클라이언트가 숫자 ID를 유효한 UNIX 사용자 이름으로 확인하게 되어 액세스 마운트에 대한 올바른 인증이 필요합니다. 이를 위해서는 LDAP를 설정하고 UNIX 사용자 및 그룹 ID를 구성해야 합니다.
- 루트 사용자를 스쿼팅하면 루트 사용자가 NFS 마운트에 수행할 수 있는 손상을 제한하지만 위험을 완전히 제거할 수는 없습니다. 자세한 내용은 " 단원을 참조하십시오루트 사용자입니다."

궁극적으로 NFS 보안은 고객이 제공하는 프로토콜 버전으로 제한됩니다. NFSv3은 일반적으로 NFSv4.1보다 더 우수한 성능을 제공하지만, 같은 수준의 보안을 제공하지 않습니다.

NFSv4.1

NFSv4.1은 NFSv3과 비교할 때 다음과 같은 이유로 더욱 뛰어난 보안 및 안정성을 제공합니다.

- 임대 기반 메커니즘을 통한 통합 잠금
- 상태 저장 세션
- 단일 포트에서 모든 NFS 기능 지원(2049)
- TCP 전용
- ID 도메인 매핑
- Kerberos 통합(NFSv3은 Kerberos 사용 가능, NFS에만 해당, NLM 같은 보조 프로토콜에는 사용할 수 없음)

NFSv4.1 종속성

NFSv4.1의 추가 보안 기능 덕분에 NFSv3을 사용할 필요가 없는 몇 가지 외부 의존성이 발생했습니다(Active Directory와 같은 SMB의 의존도 필요 방식과 유사).

NFSv4.1 ACL

Cloud Volumes Service는 NFSv4.x ACL을 지원하므로 다음과 같은 일반적인 POSIX 스타일 사용 권한에 비해 뚜렷한 이점을 제공합니다.

- 파일 및 디렉토리에 대한 사용자 액세스를 세부적으로 제어
- NFS 보안 강화
- CIFS/SMB와의 상호 운용성 향상
- AUTH_SYS 보안을 사용하여 사용자당 16개 그룹의 NFS 제한을 제거합니다
- ACL은 GID(Group ID) 확인이 필요하지 않으므로 GID 리무진을 효과적으로 제거할 수 있습니다. 따라서 Cloud Volumes Service가 아닌 NFS 클라이언트에서 ACL을 제어할 수 있습니다. NFSv4.1 ACL을 사용하려면 클라이언트의 소프트웨어 버전이 이를 지원하고 적절한 NFS 유틸리티가 설치되어 있어야 합니다.

NFSv4.1 ACL과 **SMB** 클라이언트 간의 호환성

NFSv4 ACL은 Windows 파일 레벨 ACL(NTFS ACL)과 다르지만 유사한 기능을 제공합니다. 그러나 멀티 프로토콜 NAS 환경에서 NFSv4.1 ACL이 있고 동일한 데이터 세트의 NFS 및 SMB(이중 프로토콜 액세스)를 사용 중인 경우에는 SMB2.0 이상을 사용하는 클라이언트에서 Windows 보안 탭의 ACL을 보거나 관리할 수 없습니다.

NFSv4.1 ACL의 작동 방식

참고로 다음 용어가 정의되어 있습니다.

- * 액세스 제어 목록(ACL). * 권한 항목의 목록입니다.
- * ACE(액세스 제어 항목).* 목록에 있는 권한 항목.

SetAttr 작업 중에 클라이언트가 파일에서 NFSv4.1 ACL을 설정하면 Cloud Volumes Service는 개체에 해당 ACL을 설정하여 기존 ACL을 대체합니다. 파일에 ACL이 없으면 파일에 대한 모드 권한은 owner@, group@ 및 everyone@에서 계산됩니다. 파일에 기존 SUID/SGID/고정 비트가 있으면 영향을 받지 않습니다.

GETATTR 작업 중에 클라이언트가 파일에서 NFSv4.1 ACL을 받으면 Cloud Volumes Service는 오브젝트와 연결된 NFSv4.1 ACL을 읽고 ACE 목록을 생성하고 목록을 클라이언트에 반환합니다. 파일에 NT ACL 또는 모드 비트가 있는 경우 ACL은 모드 비트에서 구성되며 클라이언트로 반환됩니다.

ACL에 거부 ACE가 있는 경우 액세스가 거부되고 ACE 허용 이 있는 경우 액세스가 부여됩니다. 그러나 ACL에 ACE가 없는 경우에도 액세스가 거부됩니다.

보안 설명자는 SACL(보안 ACL) 및 DACL(임의 ACL)으로 구성됩니다. NFSv4.1이 CIFS/SMB와 상호 운용될 경우 DACL은 NFSv4와 CIFS에 매핑된 일대일 매핑입니다. DACL은 allow 및 deny ACE로 구성됩니다.

NFSv4.1 ACL이 설정된 파일 또는 폴더에서 기본적인 "chmod"를 실행하면 기존 사용자 및 그룹 ACL이 유지되지만 기본 소유자 @, group@, everyone@acls는 수정됩니다.

NFSv4.1 ACL을 사용하는 클라이언트는 시스템의 파일 및 디렉토리에 대한 ACL을 설정하고 볼 수 있습니다. ACL이 있는 디렉터리에 새 파일이나 하위 디렉터리가 만들어지면 해당 개체는 해당 ACL로 태그가 지정된 ACL의 모든 ACE를 상속합니다 "상속 플래그".

파일 또는 디렉토리에 NFSv4.1 ACL이 있으면 해당 ACL을 사용하여 파일 또는 디렉토리에 액세스하는 데 사용되는 프로토콜에 관계없이 액세스를 제어할 수 있습니다.

파일 및 디렉토리는 ACE에 올바른 상속 플래그가 지정된 경우 상위 디렉토리의 NFSv4 ACL에서 ACE를 상속합니다(적절한 수정 사항이 있을 수 있음).

NFSv4 요청의 결과로 파일 또는 디렉토리가 생성되면 결과 파일 또는 디렉토리의 ACL은 파일 생성 요청에 ACL이 포함되어 있는지 또는 표준 UNIX 파일 액세스 권한만 포함되는지에 따라 달라집니다. ACL은 상위 디렉토리에 ACL이 있는지 여부에도 따라 달라집니다.

- 요청에 ACL이 포함된 경우 해당 ACL이 사용됩니다.
- 요청에 표준 UNIX 파일 액세스 권한만 있고 상위 디렉토리에 ACL이 없는 경우 클라이언트 파일 모드를 사용하여 표준 UNIX 파일 액세스 권한을 설정합니다.
- 요청에 표준 UNIX 파일 액세스 권한만 있고 상위 디렉토리에 상속할 수 없는 ACL이 있는 경우, 요청에 전달된 모드 비트를 기반으로 하는 기본 ACL이 새 개체에 설정됩니다.
- 요청에 표준 UNIX 파일 액세스 권한만 포함되어 있지만 상위 디렉토리에 ACL이 있는 경우 ACE에 적절한 상속 플래그가 지정된 경우 상위 디렉토리의 ACL에 있는 ACE는 새 파일 또는 디렉토리에 의해 상속됩니다.

ACE 권한

NFSv4.1 ACL 사용 권한은 일련의 대문자 및 소문자 값('rxtncy' 등)을 사용하여 액세스를 제어합니다. 이러한 문자 값에 대한 자세한 내용은 을 참조하십시오 "방법: NFSv4 ACL 사용".

umask 및 ACL 상속을 사용하는 NFSv4.1 ACL 동작

"NFSv4 ACL을 사용하면 ACL 상속을 제공할 수 있습니다". ACL 상속은 NFSv4.1 ACL이 설정된 개체 아래에 생성된 파일 또는 폴더가 의 구성에 따라 ACL을 상속할 수 있음을 의미합니다 "ACL 상속 플래그입니다".

"umask(umask" 관리자 개입 없이 디렉터리에서 파일과 폴더를 만들 수 있는 권한 수준을 제어하는 데 사용됩니다. 기본적으로 Cloud Volumes Service에서는 umask 가 에 따라 예상되는 동작을 나타내는 상속된 ACL을 재정의할 수 있도록 합니다 "RFC 5661".

ACL 형식 지정

NFSv4.1 ACL에는 특정한 형식이 있습니다. 다음은 파일에 설정된 ACE 예제입니다.

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

앞의 예제는 의 ACL 형식 지침을 따릅니다.

```
type:flags:principal:permissions
```

A의 유형은 "허용"을 의미합니다. 이 경우 보안 주체가 그룹이 아니며 상속을 포함하지 않으므로 상속 플래그가 설정되지 않습니다. 또한 ACE는 감사 항목이 아니므로 감사 플래그를 설정할 필요가 없습니다. NFSv4.1 ACL에 대한 자세한 내용은 을 참조하십시오 "http://linux.die.net/man/5/nfs4_acl".

NFSv4.1 ACL이 제대로 설정되지 않았거나 클라이언트 및 서버에서 이름 문자열을 확인할 수 없는 경우 ACL이 예상대로 작동하지 않거나 ACL 변경이 적용되지 않고 오류가 발생할 수 있습니다.

샘플 오류에는 다음이 포함됩니다.

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

명시적 거부

NFSv4.1 권한에는 소유자, 그룹 및 모든 사용자에 대한 명시적 거부 특성이 포함될 수 있습니다. 따라서 NFSv4.1 ACL은 기본적으로 -deny를 사용하기 때문에 ACL이 명시적으로 ACE에 의해 부여되지 않으면 거부됩니다. 명시적 거부 특성은 액세스 ACE를 명시적 또는 명시적으로 재정의합니다.

거부 ACE는 Ddes 특성 태그로 설정됩니다.

아래 예에서 group@은 모든 읽기 및 실행 권한을 허용하지만 모든 쓰기 액세스는 거부됩니다.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

거부 ACE는 혼란스럽고 복잡할 수 있으므로 가능하면 피해야 합니다. 명시적으로 정의되지 않은 ACL 허용 은 암시적으로 거부됩니다. 거부 ACE가 설정되면 사용자에게 액세스 권한이 부여될 것으로 예상되는 경우 액세스가 거부될 수 있습니다.

앞의 ACE 집합은 모드 비트에서 755와 동일하며, 이는 다음을 의미합니다.

- 소유자에게는 모든 권한이 있습니다.
- 그룹은 읽기 전용입니다.
- 다른 사람들은 읽기 전용입니다.

그러나 사용 권한이 775 상응 권한으로 조정되더라도 모든 사용자에 대해 명시적 거부 설정이 설정되어 있으므로 액세스가 거부될 수 있습니다.

NFSv4.1 ID 도메인 매핑 종속성

NFSv4.1은 ID 도메인 매핑 논리를 보안 계층으로 활용하여 NFSv4.1 마운트에 액세스하려는 사용자가 실제로 자신들이 주장하는 사용자인지 확인합니다. 이 경우 NFSv4.1 클라이언트에서 들어오는 사용자 이름 및 그룹 이름에 이름 문자열이 추가되고 Cloud Volumes Service 인스턴스로 보내집니다. 사용자 이름/그룹 이름 및 ID 문자열 조합이 일치하지 않으면 사용자 및/또는 그룹이 클라이언트의 '/etc/idmapd.conf' 파일에 지정된 기본 nobody 사용자로 충돌합니다.

이 ID 문자열은 특히 NFSv4.1 ACL 및/또는 Kerberos를 사용하는 경우 적절한 권한 준수를 위한 요구 사항입니다. 따라서 적절한 사용자 및 그룹 이름 ID 확인을 위해 클라이언트와 Cloud Volumes Service 간에 일관성을 유지하기 위해 LDAP 서버와 같은 이름 서비스 서버 종속성이 필요합니다.

Cloud Volumes Service는 정적 기본 ID 도메인 이름 값인 ddefaultv4iddomain.com 를 사용합니다. NFS 클라이언트는 ID 도메인 이름 설정에 대해 DNS 도메인 이름으로 기본 설정되지만, '/etc/idmapd.conf'에서 ID 도메인 이름을 수동으로 조정할 수 있습니다.

Cloud Volumes Service에서 LDAP가 활성화된 경우 Cloud Volumes Service는 NFS ID 도메인을 자동화하여 DNS에서 검색 도메인에 대해 구성된 대로 변경할 수 있으며, 다른 DNS 도메인 검색 이름을 사용하지 않는 한 클라이언트를 수정할 필요가 없습니다.

Cloud Volumes Service가 로컬 파일 또는 LDAP에서 사용자 이름 또는 그룹 이름을 확인할 수 있는 경우 도메인 문자열이 사용되고 일치하지 않는 도메인 ID는 아무도 입력할 수 없습니다. Cloud Volumes Service가 로컬 파일 또는 LDAP에서 사용자 이름 또는 그룹 이름을 찾을 수 없는 경우 숫자 ID 값이 사용되며 NFS 클라이언트가 이름을 제대로 확인합니다(NFSv3 동작과 유사).

클라이언트의 NFSv4.1 ID 도메인을 Cloud Volumes Service 볼륨에서 사용 중인 도메인과 일치하도록 변경하지 않고도 다음과 같은 동작이 발생합니다.

- 로컬 UNIX 사용자 및 그룹에 정의된 루트와 같이 Cloud Volumes Service에 로컬 항목이 있는 UNIX 사용자 및 그룹이 nobody 값으로 스쿼트됩니다.
- LDAP에 항목이 있는 UNIX 사용자 및 그룹(Cloud Volumes Service가 LDAP를 사용하도록 구성된 경우)은 DNS 도메인이 NFS 클라이언트와 Cloud Volumes Service 간에 서로 다른 경우 아무도 사용하지 않습니다.
- 로컬 항목이나 LDAP 항목이 없는 UNIX 사용자 및 그룹은 숫자 ID 값을 사용하고 NFS 클라이언트에 지정된 이름으로 확인합니다. 클라이언트에 이름이 없으면 숫자 ID만 표시됩니다.

다음은 이전 시나리오의 결과입니다.

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

클라이언트 및 서버 ID 도메인이 일치하면 동일한 파일 목록이 표시됩니다.

```
# ls -la
total 8
drwxr-xr-x 2 root   root          4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root          4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835          9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

이 문제와 해결 방법에 대한 자세한 내용은 “ 절을 참조하십시오NFSv4.1 및 그 누구도 사용자/그룹을 대상으로 하지 않습니다.”

Kerberos 종속성

NFS에서 Kerberos를 사용하려면 Cloud Volumes Service에서 다음 권한이 있어야 합니다.

- Kerberos KDC(메일 센터 서비스)용 Active Directory 도메인
- LDAP 기능에 대한 UNIX 정보로 채워진 사용자 및 그룹 속성이 있는 Active Directory 도메인(Cloud Volumes Service의 NFS Kerberos에는 적절한 기능을 위해 사용자 SPN-UNIX 사용자 매핑이 필요합니다.)
- Cloud Volumes Service 인스턴스에 대해 LDAP가 설정되었습니다
- DNS 서비스에 대한 Active Directory 도메인입니다

NFSv4.1 및 그 누구도 사용자/그룹을 대상으로 하지 않습니다

NFSv4.1 구성에서 가장 흔히 발생하는 문제 중 하나는 'user:group’의 'nobody:nobody’의 조합으로 'ls’를 사용하여 파일 또는 폴더가 목록에 표시되는 것입니다.

예를 들면 다음과 같습니다.

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

숫자 ID는 99입니다.

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

경우에 따라 파일의 소유자가 올바르지만 '아무도'가 그룹에 표시되지 않을 수 있습니다.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

아무도 없나요?

NFSv4.1의 'nobody' 사용자는 nfsnobody 사용자와 다릅니다. "id" 명령을 실행하여 NFS 클라이언트가 각 사용자를 보는 방법을 볼 수 있습니다.

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

NFSv4.1에서는 'nobody' 사용자가 'idmapd.conf' 파일에 정의된 기본 사용자이며 사용할 모든 사용자로 정의할 수 있습니다.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

이 문제가 발생하는 이유는 무엇입니까?

이름 문자열 매핑을 통한 보안은 NFSv4.1 작업의 핵심 요소이므로 이름 문자열이 제대로 일치하지 않을 때 기본 동작은 일반적으로 사용자와 그룹이 소유한 파일 및 폴더에 액세스할 수 없는 사용자에게 스쿼시를 하는 것입니다.

파일 목록에서 사용자 및/또는 그룹에 대해 'nobody'가 표시되는 경우 이는 일반적으로 NFSv4.1에서 잘못 구성된 항목이 있음을 의미합니다. 케이스 민감도는 여기에서 확인할 수 있습니다.

예를 들어 user1@CVSDEMO.LOCA L(uid 1234, gid 1234)이 내보내기에 액세스하는 경우 Cloud Volumes Service에서 user1@CVSDEMO.LOCA L(uid 1234, gid 1234)을 찾을 수 있어야 합니다. Cloud Volumes Service의 사용자가 USER1@CVSDEMO.LOCA L인 경우 일치하지 않습니다(대문자 user1과 소문자 user1 비교). 대부분의

경우 클라이언트의 메시지 파일에서 다음을 볼 수 있습니다.

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

클라이언트와 서버는 모두 사용자가 실제로 자신이 주장하는 사람이라는 데 동의해야 합니다. 따라서 클라이언트가 보는 사용자에게 Cloud Volumes Service가 보는 사용자와 동일한 정보가 있는지 확인하려면 다음을 확인해야 합니다.

- * NFSv4.x ID domain. * Client:'idmapd.conf' file; Cloud Volumes Service는 defaultv4iddomain.com 파일을 사용하며 수동으로 변경할 수 없습니다. NFSv4.1과 함께 LDAP를 사용하는 경우 Cloud Volumes Service는 ID 도메인을 AD 도메인과 동일한 DNS 검색 도메인이 사용 중인 것으로 변경합니다.
- * 사용자 이름 및 숫자 ID. * 이 옵션은 클라이언트가 사용자 이름을 찾는 위치를 결정하고 이름 서비스 스위치 구성(client: ' nsswitch.conf' 및/또는 로컬 passwd 및 group 파일)을 활용합니다. Cloud Volumes Service는 이를 수정할 수 없지만 활성화된 경우 구성에 LDAP를 자동으로 추가합니다.
- * 그룹 이름 및 숫자 ID. * 이 옵션은 클라이언트가 그룹 이름을 찾는 위치를 결정하고 이름 서비스 스위치 구성(client: ' nsswitch.conf' 및/또는 로컬 passwd 및 group 파일)을 활용합니다. Cloud Volumes Service는 이를 수정할 수 없지만 활성화된 경우 구성에 LDAP를 자동으로 추가합니다.

거의 모든 경우에 클라이언트의 사용자 및 그룹 목록에 'nobody'가 표시되면 Cloud Volumes Service와 NFS 클라이언트 간의 사용자 또는 그룹 이름 도메인 ID 변환입니다. 이 시나리오를 방지하려면 LDAP를 사용하여 클라이언트와 Cloud Volumes Service 간의 사용자 및 그룹 정보를 확인합니다.

클라이언트의 **NFSv4.1**에 대한 이름 **ID** 문자열을 보는 중입니다

NFSv4.1을 사용하는 경우 앞서 설명한 대로 NFS 작업 중에 이름 문자열 매핑이 발생합니다.

NFSv4 ID에 대한 문제를 찾기 위해 '/var/log/messages'를 사용하는 것 외에도 을 사용할 수 있습니다 "nfsidmap -l" NFSv4 도메인에 올바르게 매핑된 사용자 이름을 보려면 NFS 클라이언트에서 명령을 실행하십시오.

예를 들어, 이 명령은 클라이언트에서 찾을 수 있는 사용자 및 Cloud Volumes Service가 NFSv4.x 마운트에 액세스하는 이후의 명령 출력입니다.

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

NFSv4.1 ID 도메인(이 경우, 즉 NetApp-user)에 제대로 매핑되지 않는 사용자가 동일한 마운트에 액세스하여 파일을 만지려고 하면 'nobody:nobody'가 예상한 대로 할당됩니다.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

nfsidmap-l 출력에서는 디스플레이에 사용자 pcuser가 표시되지만 NetApp-user는 표시되지 않습니다. 이는 엑스포트 정책 규칙('65534')의 익명 사용자입니다.

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

중소기업

"중소기업" 는 이더넷 네트워크를 통해 여러 SMB 클라이언트에 중앙 집중식 사용자/그룹 인증, 권한, 잠금 및 파일 공유를 제공하는 Microsoft에서 개발한 네트워크 파일 공유 프로토콜입니다. 파일 및 폴더는 다양한 공유 속성으로 구성할 수 있고 공유 수준 권한을 통해 액세스 제어를 제공하는 공유를 통해 클라이언트에 제공됩니다. SMB는 Windows, Apple 및 Linux 클라이언트를 비롯하여 프로토콜을 지원하는 모든 클라이언트에 제공될 수 있습니다.

Cloud Volumes Service는 SMB 2.1 및 3.x 버전의 프로토콜을 지원합니다.

액세스 제어/**SMB** 공유

- Windows 사용자 이름이 Cloud Volumes Service 볼륨에 대한 액세스를 요청하면 Cloud Volumes Service는 Cloud Volumes Service 관리자가 구성한 방법을 사용하여 UNIX 사용자 이름을 찾습니다.
- 외부 UNIX ID 공급자(LDAP)가 구성되어 있고 Windows/UNIX 사용자 이름이 동일한 경우 Windows 사용자 이름은 추가 구성 없이 1:1을 UNIX 사용자 이름으로 매핑합니다. LDAP가 설정되면 Active Directory를 사용하여 사용자 및 그룹 객체에 대한 UNIX 속성을 호스팅합니다.
- Windows 이름과 UNIX 이름이 동일하게 일치하지 않으면 Cloud Volumes Service에서 LDAP 이름 매핑 구성을

사용할 수 있도록 LDAP를 구성해야 합니다(섹션 참조) ""비대칭 이름 매핑에 LDAP 사용"")를 클릭합니다.

- LDAP를 사용하지 않는 경우 Windows SMB 사용자는 Cloud Volumes Service의 기본 로컬 UNIX 사용자 "pcuser"로 매핑됩니다. 즉, 멀티프로토콜 NAS 환경에서 pcuser로 매핑되는 사용자가 Windows에서 작성한 파일이 UNIX 소유권을 pcuser로 표시합니다. 여기에 있는 'pcuser'는 사실상 리눅스 환경(UID 65534)의 'nobody' 사용자입니다.

SMB만 사용하는 배포에서는 "pcuser" 매핑이 계속 발생하지만 Windows 사용자 및 그룹 소유권이 올바르게 표시되고 SMB 전용 볼륨에 대한 NFS 액세스가 허용되지 않으므로 문제가 되지 않습니다. 또한 SMB 전용 볼륨은 생성된 후 NFS 또는 이중 프로토콜 볼륨으로의 전환을 지원하지 않습니다.

Windows는 Active Directory 도메인 컨트롤러에서 사용자 이름 인증에 Kerberos를 사용합니다. 이 경우 AD DC와 사용자 이름/암호 교환이 필요하며 이는 Cloud Volumes Service 인스턴스 외부에 있습니다. Kerberos 인증은 SMB 클라이언트가 '\\서버 이름' UNC 경로를 사용하는 경우 사용되며 다음 조건이 적용됩니다.

- 서버 이름 에 대한 DNS A/AAAA 항목이 있습니다
- SMB/CIFS 액세스에 유효한 SPN이 SERVERNAME에 존재합니다

Cloud Volumes Service SMB 볼륨이 생성되면 섹션에 정의된 대로 시스템 계정 이름이 생성됩니다 ""Cloud Volumes Service가 Active Directory에 표시되는 방식"" Cloud Volumes Service는 DDNS(동적 DNS)를 활용하여 DNS에 필요한 A/AAAA 및 PTR 항목을 생성하고 시스템 계정 보안 주체에 필요한 SPN 항목을 생성하기 때문에 해당 시스템 계정 이름도 SMB 공유 액세스 경로가 됩니다.

PTR 항목을 작성하려면 Cloud Volumes Service 인스턴스 IP 주소에 대한 역방향 조회 영역이 DNS 서버에 있어야 합니다.

예를 들어, 이 Cloud Volumes Service 볼륨은 '\\cvs-east-433d.cvsdemo.local' UNC 공유 경로를 사용합니다.

Active Directory에서는 Cloud Volumes Service에서 생성한 SPN 항목이 다음과 같습니다.

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

DNS 정방향/역방향 조회 결과입니다.

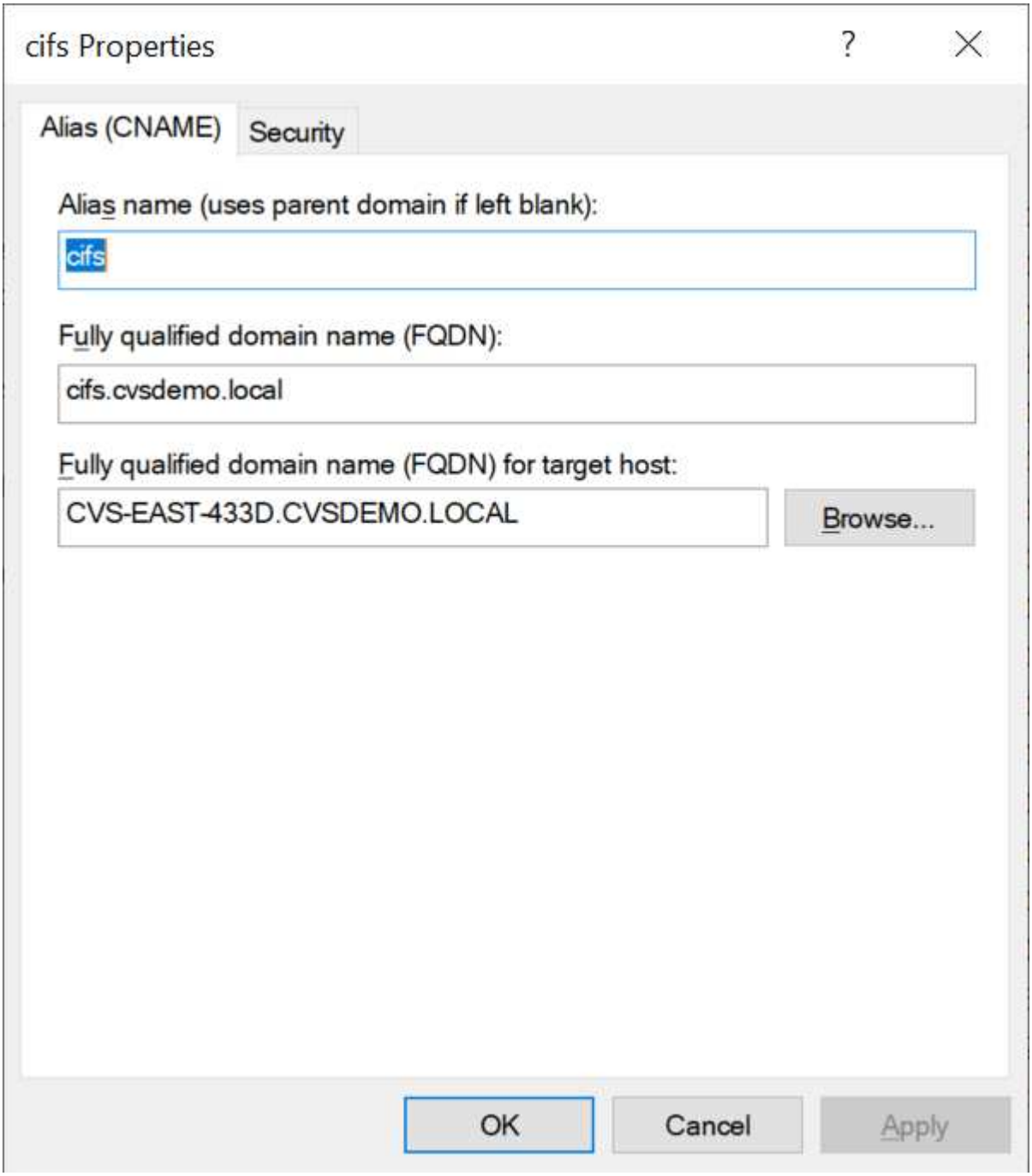
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

선택적으로 Cloud Volumes Service에서 SMB 공유에 대한 SMB 암호화를 설정/요구하여 더 많은 액세스 제어를 적용할 수 있습니다. 엔드포인트 중 하나가 SMB 암호화를 지원하지 않는 경우 액세스가 허용되지 않습니다.

SMB 이름 별칭 사용

경우에 따라 최종 사용자가 Cloud Volumes Service에 사용 중인 컴퓨터 계정 이름을 알아야 하는 보안 문제가 발생할 수 있습니다. 또는 최종 사용자에게 더 간단한 액세스 경로를 제공하려는 경우도 있습니다. 이 경우 SMB 별칭을 생성할 수 있습니다.

SMB 공유 경로에 대한 별칭을 만들려는 경우 DNS에서 CNAME 레코드로 알려진 별칭을 활용할 수 있습니다. 예를 들어 이름이 \\cvs-east-433d.cvssdemo.local이 아닌 공유에 액세스하기 위해 \\cifs"를 사용하되 Kerberos 인증을 계속 사용하려면 기존 A/AAAA 레코드를 가리키는 DNS의 CNAME과 기존 컴퓨터 계정에 추가된 추가 SPN이 Kerberos 액세스를 제공합니다.



CNAME을 추가한 후 생성되는 DNS 정방향 조회 결과입니다.

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

새 SPN을 추가한 후 생성되는 SPN 쿼리입니다.

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

패킷 캡처에서는 CNAME에 연결된 SPN을 사용하여 세션 설정 요청을 볼 수 있습니다.

```
431 4.156722                                    SMB2     308 Negotiate Protocol Response
432 4.156785                                    SMB2     232 Negotiate Protocol Request
434 4.158108                                    SMB2     374 Negotiate Protocol Response
435 4.160977                                    SMB2    1978 Session Setup Request
437 4.166224                                    SMB2     322 Session Setup Response
438 4.166891                                    SMB2     152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2     138 Tree Connect Response
```

```
realm: CVSDEMO.LOCAL
sname
    name-type: kRB5-NT-SRV-INST (2)
    sname-string: 2 items
        SNameString: cifs
        SNameString: cifs
enc-part
    etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB 인증 방언

Cloud Volumes Service는 다음을 지원합니다 "방언" SMB 인증의 경우:

- LM
- NTLM
- NTLMv2
- Kerberos

SMB 공유 액세스를 위한 Kerberos 인증은 사용할 수 있는 가장 안전한 인증 수준입니다. AES 및 SMB 암호화를 활성화하면 보안 수준이 더욱 높아집니다.

또한 Cloud Volumes Service는 LM 및 NTLM 인증에 대한 이전 버전과의 호환성을 지원합니다. Kerberos가 잘못 구성된 경우(예: SMB 별칭 생성 시), 공유 액세스는 NTLMv2와 같은 취약한 인증 방법으로 되돌아갑니다. 이러한 메커니즘은 보안성이 떨어지기 때문에 일부 Active Directory 환경에서는 비활성화됩니다. 취약한 인증 방법을 사용하지 않도록 설정하고 Kerberos를 제대로 구성하지 않으면 다시 사용할 유효한 인증 방법이 없기 때문에 공유 액세스가 실패합니다.

Active Directory에서 지원되는 인증 수준을 구성/보는 방법에 대한 자세한 내용은 을 참조하십시오 "네트워크 보안: LAN Manager 인증 레벨".

권한 모델

NTFS/파일 권한

NTFS 권한은 NTFS 로직을 따르는 파일 시스템의 파일 및 폴더에 적용되는 권한입니다. 기본 또는 고급 에서 NTFS 권한을 적용할 수 있으며 액세스 제어를 위해 허용 또는 거부 로 설정할 수 있습니다.

기본 사용 권한은 다음과 같습니다.

- 모든 권한
- 수정
- 읽기 및 실행
- 읽기
- 쓰기

ACE라고 하는 사용자 또는 그룹에 대한 사용 권한을 설정하면 ACL에 상주합니다. NTFS 권한은 UNIX 모드 비트와 동일한 읽기/쓰기/실행 기본 사항을 사용하지만 소유권 가져오기, 폴더 만들기/데이터 추가, 속성 쓰기 등과 같은 보다 세분화된 확장 액세스 제어(특수 권한이라고도 함)로 확장할 수도 있습니다.

표준 UNIX 모드 비트는 NTFS 권한과 동일한 수준의 세분화 수준을 제공하지 않습니다(예: ACL에서 개별 사용자 및 그룹 개체에 대한 권한을 설정하거나 확장 속성을 설정할 수 있음). 그러나 NFSv4.1 ACL은 NTFS ACL과 동일한 기능을 제공합니다.

NTFS 권한은 공유 권한보다 더 구체적이며 공유 권한과 함께 사용할 수 있습니다. NTFS 권한 구조에서는 가장 제한적인 권한이 적용됩니다. 따라서 사용자 또는 그룹에 대한 명시적 변명의 경우 액세스 권한을 정의할 때 전체 제어보다 우선합니다.

NTFS 권한은 Windows SMB 클라이언트에서 제어됩니다.

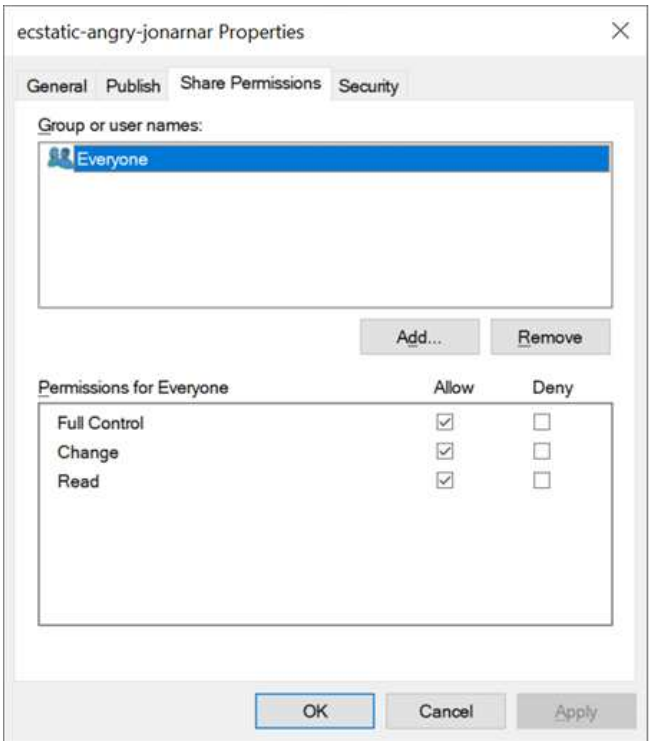
공유 권한

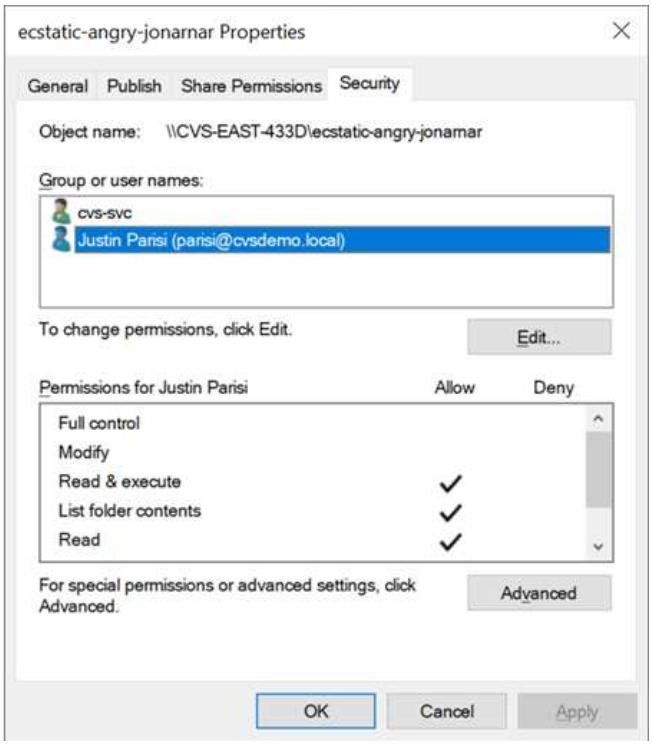
공유 권한은 NTFS 권한(읽기/변경/모든 제어만 해당)보다 더 일반적이며, SMB 공유의 초기 항목을 제어합니다. 이는 NFS 내보내기 정책 규칙의 작동 방식과 유사합니다.

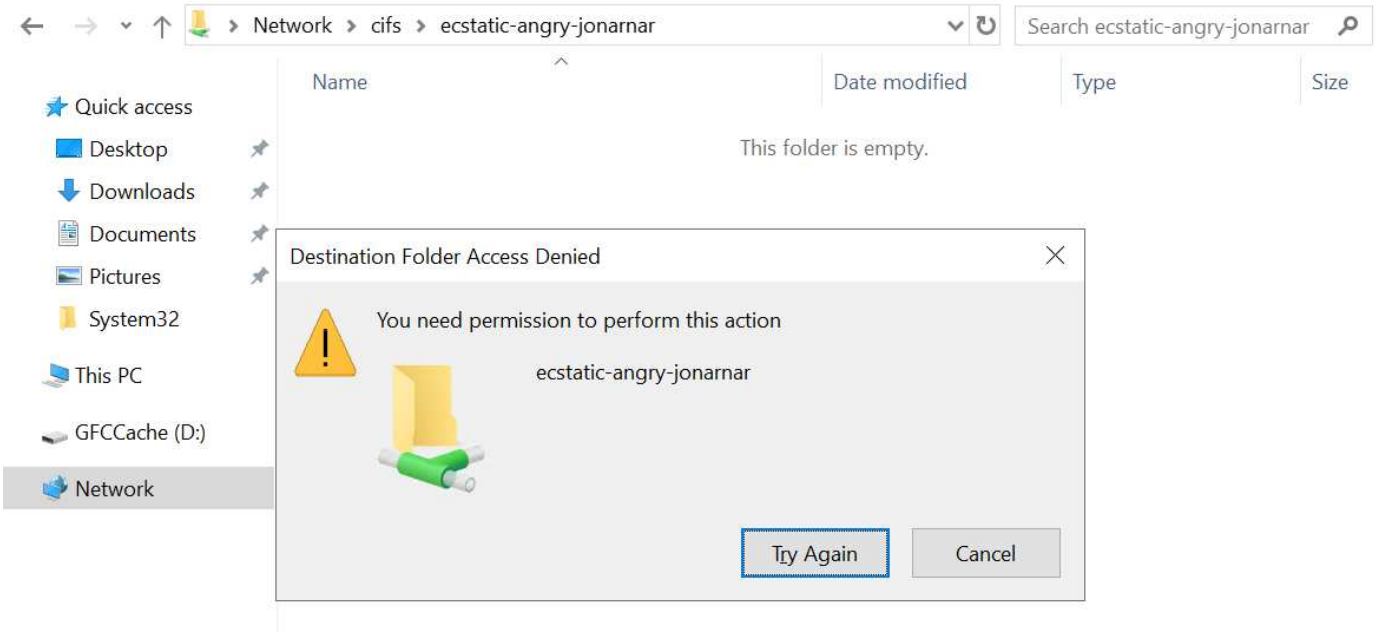
NFS 내보내기 정책 규칙은 IP 주소 또는 호스트 이름과 같은 호스트 기반 정보를 통해 액세스를 제어하지만 SMB 공유 권한은 공유 ACL에서 사용자 및 그룹 ACE를 사용하여 액세스를 제어할 수 있습니다. Windows 클라이언트 또는 Cloud Volumes Service 관리 UI에서 공유 ACL을 설정할 수 있습니다.

기본적으로 공유 ACL 및 초기 볼륨 ACL에는 모든 권한이 있는 모든 사용자가 포함됩니다. 파일 ACL은 변경되어야 하지만 공유 권한은 공유의 객체에 대한 파일 권한에 의해 무시됩니다.

예를 들어, 사용자가 Cloud Volumes Service 볼륨 파일 ACL에 대한 읽기 액세스만 허용되는 경우 다음 그림과 같이 공유 ACL이 모든 권한이 있는 사용자로 설정되어 있어도 파일 및 폴더 생성에 대한 액세스가 거부됩니다.







최상의 보안 결과를 얻으려면 다음을 수행하십시오.

- 공유 및 파일 ACL에서 모든 사용자를 제거하고 대신 사용자 또는 그룹에 대한 공유 액세스를 설정합니다.
- 개별 사용자 대신 그룹을 사용하여 액세스 제어를 수행할 수 있어 관리가 용이하고 그룹 관리를 통해 ACL을 공유할 사용자를 더 빠르게 제거/추가할 수 있습니다.
- 공유 권한에 있는 ACE에 대한 덜 제한적이고 보다 일반적인 공유 액세스를 허용하고 보다 세분화된 액세스 제어를 위한 파일 권한을 가진 사용자 및 그룹에 대한 액세스를 잠급니다.
- 명시적 거부 ACL은 ACL 허용 을 재정의하므로 일반적인 사용을 피합니다. 파일 시스템에 대한 액세스를 신속하게 제한해야 하는 사용자 또는 그룹의 명시적 거부 ACL 사용을 제한합니다.
- 에 주의를 기울이십시오 "ACL 상속" 사용 권한을 수정할 때 설정; 파일 수가 많은 디렉토리 또는 볼륨의 최상위

레벨에서 상속 플래그를 설정하면 해당 디렉토리 또는 볼륨 아래의 각 파일에 상속된 사용 권한이 추가되었음을 의미합니다. 의도하지 않은 액세스/거부 및 각 파일이 조정될 때 권한 수정 장기 이탈과 같은 원치 않는 동작이 발생할 수 있습니다.

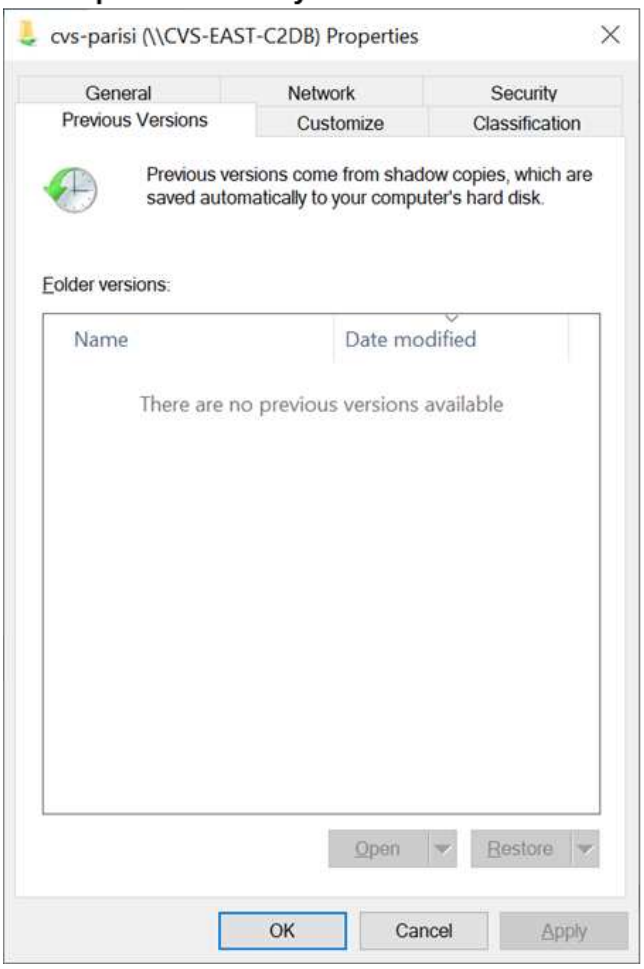
SMB는 보안 기능을 공유합니다

Cloud Volumes Service에서 SMB 액세스가 가능한 볼륨을 처음 생성하면 해당 볼륨을 보호하기 위한 일련의 선택 사항이 표시됩니다.

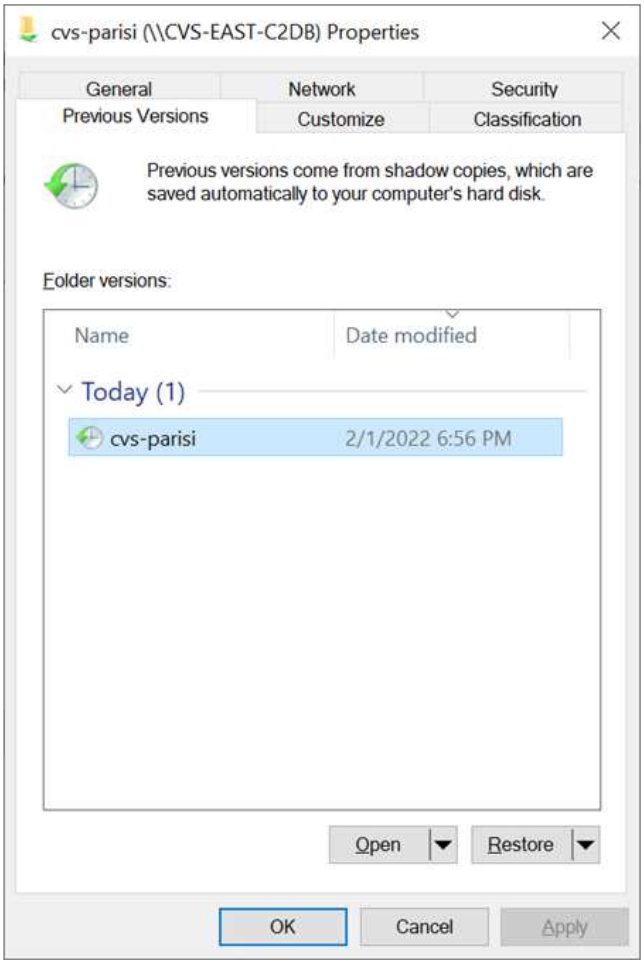
이러한 선택 사항 중 일부는 Cloud Volumes Service 레벨(성능 또는 소프트웨어)에 따라 달라지며 다음과 같은 옵션이 있습니다.

- * 스냅샷 디렉토리를 표시합니다(CVS - 성능 및 CVS - SW 모두에서 사용 가능). * 이 옵션은 SMB 클라이언트가 SMB 공유의 스냅샷 디렉토리에 액세스할 수 있는지 여부를 제어합니다('\\server\share\~snapshot' 및/또는 Previous Versions 탭). 기본 설정은 선택되지 않습니다. 즉, 볼륨이 기본적으로 `~snapshot' 디렉토리에 대한 액세스를 숨기거나 허용하지 않으며 볼륨의 이전 버전 탭에 스냅샷 복사본이 나타나지 않습니다.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



보안 상의 이유, 성능상의 이유(AV 스캔에서 이러한 폴더 숨기기) 또는 기본 설정을 위해 최종 사용자로부터 스냅샷 복사본을 숨기는 것이 좋습니다. Cloud Volumes Service 스냅샷은 읽기 전용이므로 이러한 스냅샷이 표시되는 경우에도 최종 사용자는 스냅샷 디렉토리의 파일을 삭제하거나 수정할 수 없습니다. 스냅샷 복사본이 생성된 시점의 파일 또는 폴더에 대한 파일 권한이 적용됩니다. 파일 또는 폴더의 사용 권한이 Snapshot 복사본 간에 변경되면 변경 내용이 Snapshot 디렉토리의 파일 또는 폴더에도 적용됩니다. 사용자 및 그룹은 권한에 따라 이러한 파일 또는 폴더에 액세스할 수 있습니다. 스냅샷 디렉토리에서 파일을 삭제하거나 수정할 수는 없지만 스냅샷 디렉토리에서 파일 또는 폴더를 복사할 수는 있습니다.

- * SMB 암호화 활성화(CVS - 성능 및 CVS - SW 모두에 사용 가능). * SMB 공유에서 SMB 암호화는 기본적으로 비활성화되어 있습니다(선택 취소됨). 이 확인란을 선택하면 SMB 암호화가 활성화됩니다. 즉, SMB 클라이언트와 서버 간의 트래픽은 협상된 가장 높은 암호화 수준으로 전송 중에 암호화됩니다. Cloud Volumes Service는 SMB에 대해 최대 AES-256 암호화를 지원합니다. SMB 암호화를 활성화하면 SMB 클라이언트에서 성능 저하가 발생할 수 있으며, 이는 대략 10~20% 범위에서 나타날 수도 있고 그렇지 않을 수도 있습니다. 테스트 결과, 성능 저하가 허용 가능한지 여부를 확인하는 것이 좋습니다.
- * SMB 공유 숨기기(CVS - 성능 및 CVS - SW 모두에 사용 가능) * 이 옵션을 설정하면 SMB 공유 경로가 일반 탐색에서 숨겨집니다. 즉, 공유 경로를 모르는 클라이언트는 기본 UNC 경로("\\CVS-SMB" 등)에 액세스할 때 공유를 볼 수 없습니다. 이 확인란을 선택하면 SMB 공유 경로를 명시적으로 알고 있거나 그룹 정책 개체에서 정의한 공유 경로를 가진 클라이언트만 액세스할 수 있습니다(난독 처리를 통한 보안).
- * ABE(액세스 기반 열거) 사용(CVS-SW만 해당). * SMB 공유를 숨기는 것과 비슷하지만, 공유 또는 파일이 개체에 액세스할 권한이 없는 사용자 또는 그룹에서만 숨겨지는 것을 제외하고는 차이가 있습니다. 예를 들어, Windows 사용자 'Joe'가 권한을 통한 읽기 액세스를 최소한 허용하지 않으면 Windows 사용자 'Joe'는 SMB 공유나 파일을 전혀 볼 수 없습니다. 이 기능은 기본적으로 비활성화되어 있으며 확인란을 선택하여 활성화할 수 있습니다. ABE에 대한 자세한 내용은 NetApp 기술 자료 문서를 참조하십시오 "ABE(Access Based Enumeration)는 어떻게 작동합니까?"
- * 지속적으로 사용 가능한(CA) 공유 지원 활성화(CVS - 성능만 해당) * "지속적으로 사용 가능한 SMB 공유" Cloud Volumes Service 백엔드 시스템의 노드 간에 잠금 상태를 복제하여 페일오버 이벤트 중에 애플리케이션 중단을 최소화할 수 있는 방법을 제공합니다. 이 기능은 보안 기능이 아니지만 전반적으로 더 뛰어난 복원력을 제공합니다. 현재 이 기능에는 SQL Server 및 FSLogix 애플리케이션만 지원됩니다.

숨겨진 기본 공유

SMB 서버가 Cloud Volumes Service에서 생성되면 서버가 생성됩니다 "숨겨진 관리 공유" ($ 명명 규칙 사용) - 데이터 볼륨 SMB 공유 이외에 생성됩니다. 여기에는 C$(네임스페이스 액세스) 및 IPC$(Microsoft Management Console(MMC) 액세스에 사용되는 RPC(원격 프로시저 호출)와 같은 프로그램 간 통신을 위한 명명된 파이프 공유)가 포함됩니다.

IPC$ 공유는 공유 ACL을 포함하지 않으며 수정할 수 없습니다. RPC 호출 및 에 엄격하게 사용됩니다 "Windows에서는 기본적으로 이러한 공유에 대한 익명 액세스를 허용하지 않습니다".

C$ 공유는 기본적으로 BUILTIN/Administrators 액세스를 허용하지만, Cloud Volumes Service 자동화는 공유 ACL을 제거하고, C$ 공유에 대한 액세스를 통해 Cloud Volumes Service 파일 시스템에 마운트된 모든 볼륨을 볼 수 있으므로 다른 사람에게 액세스를 허용하지 않습니다. 따라서 '\\server\C$'로 이동하려고 하면 실패합니다.

로컬/**BUILTIN** 관리자/백업 권한이 있는 계정

Cloud Volumes Service SMB 서버는 일부 도메인 사용자 및 그룹에 액세스 권한을 적용하는 로컬 그룹(예: BUILTIN\Administrators)이 있다는 점에서 일반 Windows SMB 서버와 유사한 기능을 유지합니다.

백업 사용자에 추가할 사용자를 지정하면 해당 Active Directory 연결을 사용하는 Cloud Volumes Service 인스턴스의 BUILTIN\Backup Operators 그룹에 사용자가 추가되고 이 그룹에 이 사용자가 추가됩니다 "SeBackupPrivilege 및 SeRestorePrivilege를 참조하십시오".

사용자를 보안 권한 사용자 에 추가하면 사용자에게 SeSecurityPrivilege 가 부여되며, 이 권한은 와 같은 일부 응용 프로그램 사용 사례에 유용합니다 "SMB 공유의 SQL Server".

Backup Users

Provide a comma separated list of domain users or a domain group name that require elevated privileges to access volumes created by Cloud Volumes Service.

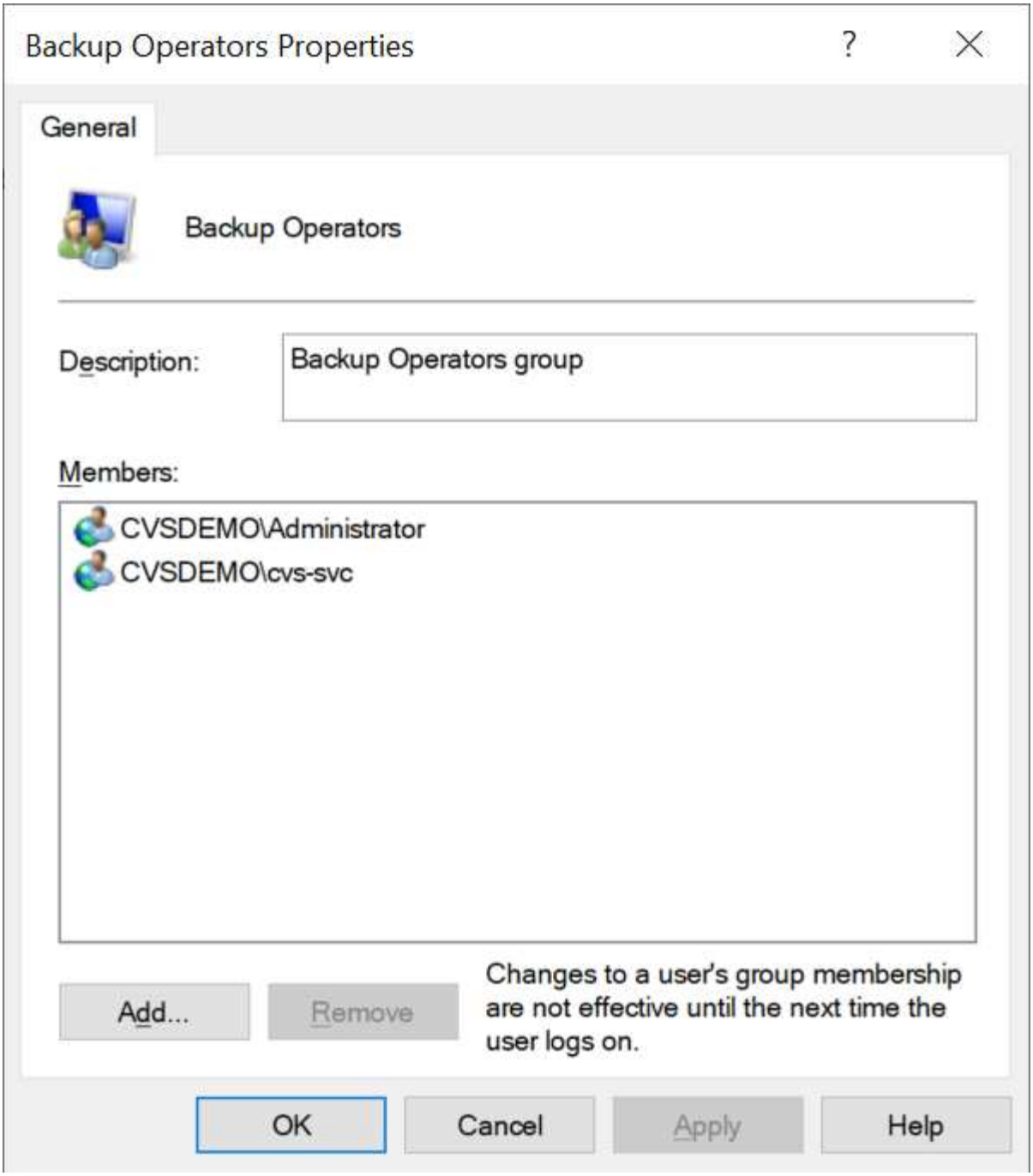
Accountnames
administrator,cvs-svc

Security Privilege Users

Provide a list of comma separated domain user accounts that require elevated privileges to manage security log for the Active Directory associated with Cloud Volumes Service.

Accountnames
administrator,cvs-svc

적절한 권한이 있는 MMC를 통해 Cloud Volumes Service 로컬 그룹 구성원 자격을 볼 수 있습니다. 다음 그림에서는 Cloud Volumes Service 콘솔을 사용하여 추가된 사용자를 보여 줍니다.

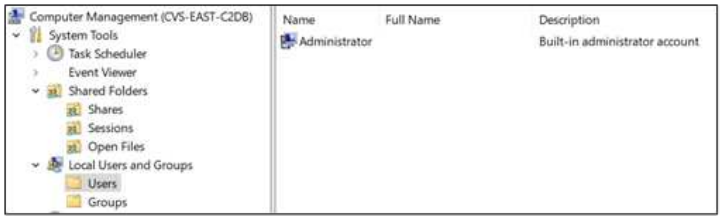


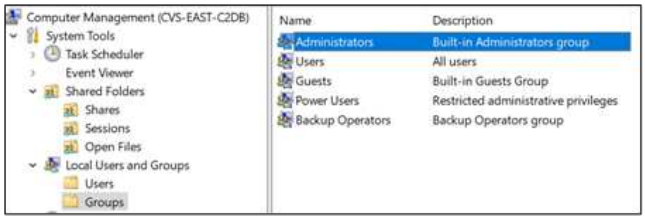
다음 표에서는 기본 BUILTIN 그룹 목록과 기본적으로 추가되는 사용자/그룹을 보여 줍니다.

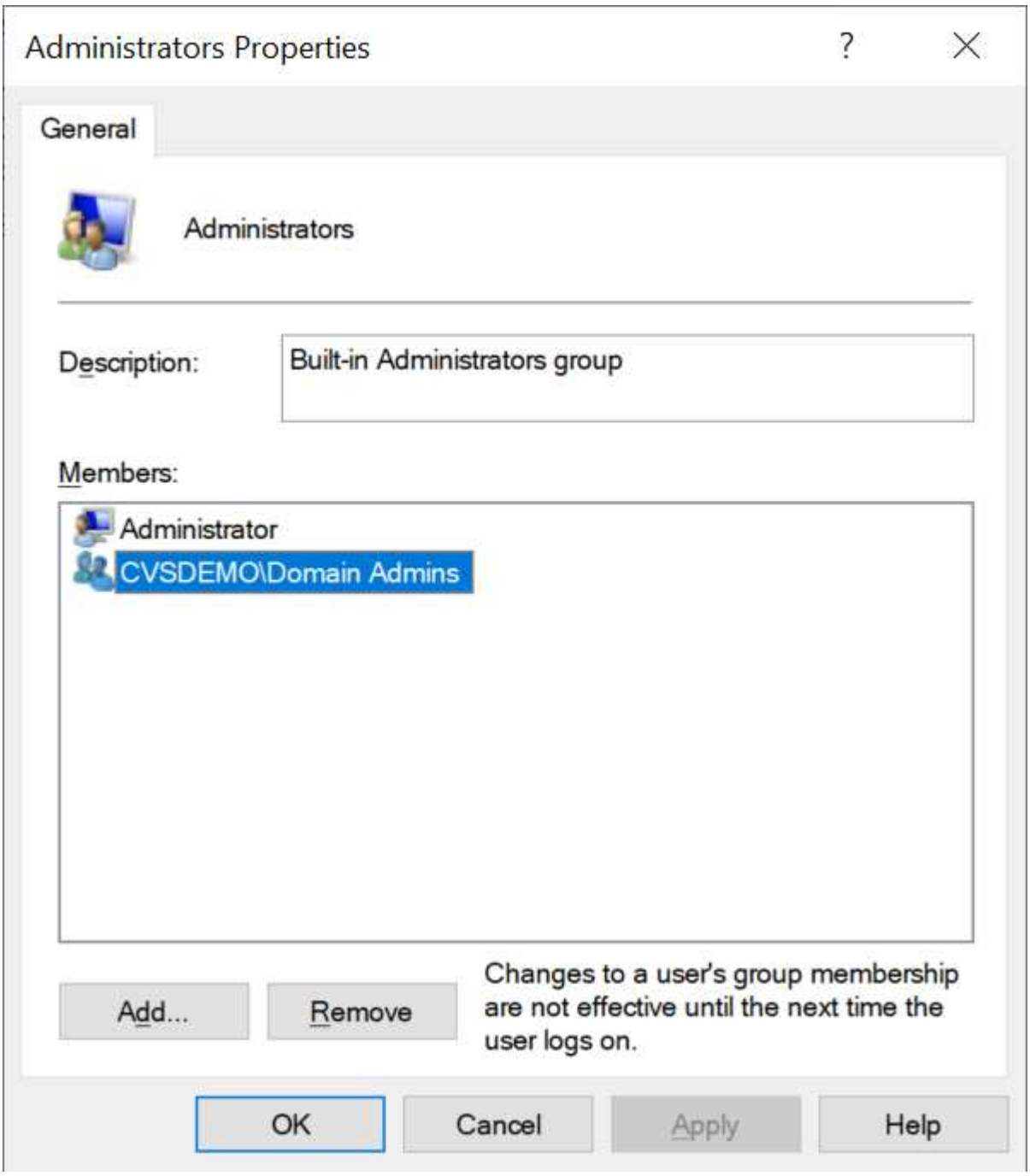
로컬/**BUILTIN** 그룹	기본 멤버
BUILTIN\Administrators *	Domain\Domain Admins입니다
BUILTIN\Backup Operators *	없음
BUILTIN\Guest입니다	도메인\도메인 게스트입니다
BUILTIN\고급 사용자	없음
BUILTIN\도메인 사용자	도메인\도메인 사용자

- Cloud Volumes Service Active Directory 연결 구성에서 그룹 멤버십이 제어됩니다.

MMC 창에서 로컬 사용자 및 그룹(및 그룹 구성원)을 볼 수 있지만 개체를 추가 또는 삭제하거나 이 콘솔에서 그룹 구성원을 변경할 수는 없습니다. 기본적으로 도메인 관리자 그룹 및 관리자만 Cloud Volumes Service의 BUILTIN\Administrators 그룹에 추가됩니다. 현재 수정할 수 없습니다.







MMC/컴퓨터 관리 액세스

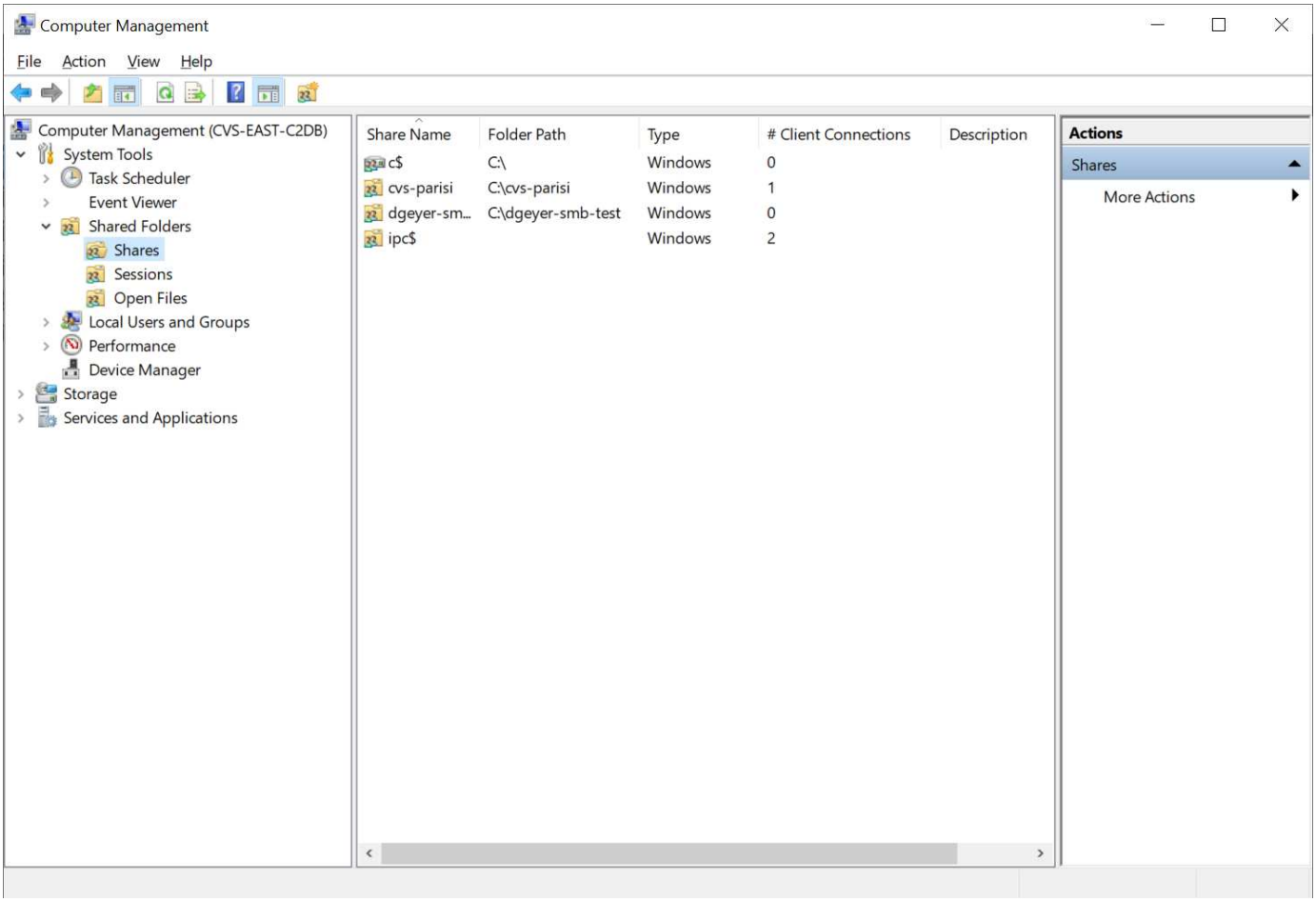
Cloud Volumes Service의 SMB 액세스는 공유를 보고, 공유 ACL을 관리하고, SMB 세션 및 열린 파일을 확인/관리할 수 있는 컴퓨터 관리 MMC에 대한 연결을 제공합니다.

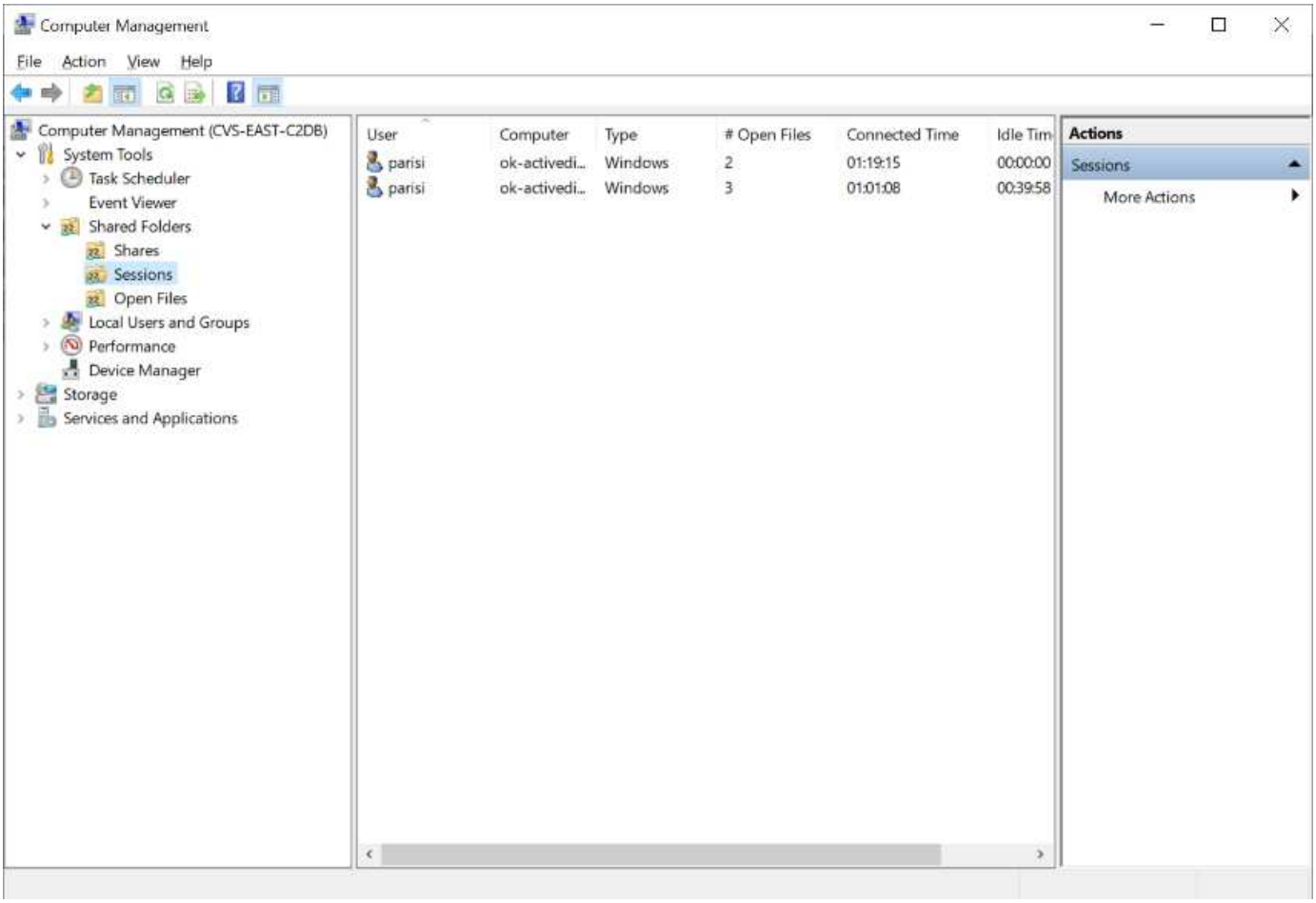
MMC를 사용하여 Cloud Volumes Service에서 SMB 공유 및 세션을 보려면 현재 로그인한 사용자가 도메인 관리자여야 합니다. 다른 사용자는 MMC에서 SMB 서버를 보거나 관리할 수 있으며 Cloud Volumes Service SMB 인스턴스에서 공유 또는 세션을 보려고 할 때 사용 권한 없음 대화 상자를 받을 수 있습니다.

SMB 서버에 연결하려면 컴퓨터 관리를 열고 컴퓨터 관리를 마우스 오른쪽 단추로 클릭한 다음 다른 컴퓨터에 연결을 선택합니다. 그러면 Cloud Volumes Service 볼륨 정보에 있는 SMB 서버 이름을 입력할 수 있는 컴퓨터 선택 대화 상자가 열립니다.

적절한 권한이 있는 SMB 공유를 보면 Active Directory 연결을 공유하는 Cloud Volumes Service 인스턴스에서 사용 가능한 모든 공유가 표시됩니다. 이 동작을 제어하려면 Cloud Volumes Service 볼륨 인스턴스에서 SMB 공유 숨기기 옵션을 설정합니다.

지역당 하나의 Active Directory 연결만 허용됩니다.





다음 표에는 MMC에서 지원/지원되지 않는 기능 목록이 나와 있습니다.

지원되는 함수	지원되지 않는 함수
• 공유 보기 • 활성 SMB 세션을 봅니다 • 열린 파일을 봅니다 • 로컬 사용자 및 그룹을 봅니다 • 로컬 그룹 구성원 자격을 봅니다 • 시스템의 세션, 파일 및 트리 연결 목록을 열거합니다 • 시스템에서 열려 있는 파일을 닫습니다 • 열려 있는 세션을 닫습니다 • 공유 생성/관리	• 새 로컬 사용자/그룹을 생성합니다 • 기존 로컬 사용자/그룹 관리/보기 • 이벤트 또는 성능 로그를 봅니다 • 스토리지 관리 • 서비스 및 애플리케이션 관리

SMB 서버 보안 정보

Cloud Volumes Service의 SMB 서버는 Kerberos 클록 편중, 티켓 사용 기간, 암호화 등 SMB 연결에 대한 보안 정책을 정의하는 일련의 옵션을 사용합니다.

다음 표에는 이러한 옵션, 기능, 기본 설정 및 Cloud Volumes Service를 사용하여 수정할 수 있는 경우 등이 나와

있습니다. 일부 옵션은 Cloud Volumes Service에는 적용되지 않습니다.

보안 옵션	기능	기본값	변경할 수 있습니까?
최대 Kerberos 클럭 비뚤어짐(분)	Cloud Volumes Service와 도메인 컨트롤러 간의 최대 시간 편중 시간 차이가 5분을 초과하면 Kerberos 인증이 실패합니다. 이 값은 Active Directory 기본값으로 설정됩니다.	5	아니요
Kerberos 티켓 수명(시간)	갱신이 요구되기 전에 Kerberos 티켓이 유효한 상태로 유지되는 최대 시간입니다. 10시간 전에 갱신이 발생하지 않으면 새 티켓을 받아야 합니다. Cloud Volumes Service는 이러한 갱신을 자동으로 수행합니다. Active Directory 기본값은 10시간입니다.	10	아니요
최대 Kerberos 티켓 갱신(일)	새 승인 요청이 필요해지기 전에 Kerberos 티켓을 갱신할 수 있는 최대 일 수입니다. Cloud Volumes Service는 SMB 연결에 대한 티켓을 자동으로 갱신합니다. 7일은 Active Directory 기본값입니다.	7	아니요
Kerberos KDC 연결 시간 초과(초)	KDC 연결이 시간 초과되기 전의 시간(초)입니다.	3	아니요
수신 SMB 트래픽에 서명 필요	SMB 트래픽에 서명 필요 로 설정합니다. true로 설정하면 서명을 지원하지 않는 클라이언트가 연결되지 않습니다.	거짓	
로컬 사용자 계정에 암호 복잡성 필요	로컬 SMB 사용자의 암호에 사용됩니다. Cloud Volumes Service는 로컬 사용자 생성을 지원하지 않으므로 이 옵션은 Cloud Volumes Service에는 적용되지 않습니다.	참	아니요
Active Directory LDAP 연결에 start_TLS를 사용합니다	Active Directory LDAP에 대한 TLS 연결 시작을 활성화하는 데 사용됩니다. Cloud Volumes Service에서는 현재 이 설정을 지원하지 않습니다.	거짓	아니요

보안 옵션	기능	기본값	변경할 수 있습니까?
Kerberos를 사용하도록 AES-128 및 AES-256 암호화를 사용합니다	Active Directory 연결에 AES 암호화를 사용할지 여부를 제어하고 Active Directory 연결을 생성/수정할 때 Active Directory 인증에 AES 암호화 사용 옵션을 사용하여 제어합니다.	거짓	예
LM 호환성 수준	Active Directory 연결에 대해 지원되는 인증 방언의 수준입니다. 자세한 내용은 " 단원을 참조하십시오SMB 인증 방언"를 참조하십시오.	NTLMv2 - KRB	아니요
수신 CIFS 트래픽에 SMB 암호화 필요	모든 공유에 SMB 암호화가 필요합니다. 이 기능은 Cloud Volumes Service에서 사용되지 않으며 대신 볼륨별로 암호화를 설정합니다(“ 절 참조)SMB는 보안 기능을 공유합니다").	거짓	아니요
클라이언트 세션 보안	LDAP 통신에 대한 서명 및/또는 봉인을 설정합니다. 이 설정은 현재 Cloud Volumes Service에 설정되어 있지 않지만 향후 릴리즈에서 필요할 수 있습니다. Windows 패치로 인한 LDAP 인증 문제에 대한 해결 방법은 섹션에서 설명합니다 ""LDAP 채널 바인딩.””.	없음	아니요
SMB2가 DC 연결에 대해 설정됩니다	DC 연결에 SMB2를 사용합니다. 기본적으로 사용됩니다.	System - 기본값입니다	아니요
LDAP 조회	여러 LDAP 서버를 사용하는 경우 조회 추적을 통해 첫 번째 서버에서 항목을 찾을 수 없을 때 클라이언트가 목록의 다른 LDAP 서버를 참조할 수 있습니다. 현재 Cloud Volumes Service에서는 지원되지 않습니다.	거짓	아니요
보안 Active Directory 연결에 LDAPS를 사용합니다	SSL을 통한 LDAP 사용을 활성화합니다. 현재 Cloud Volumes Service에서 지원되지 않습니다.	거짓	아니요

보안 옵션	기능	기본값	변경할 수 있습니까?
DC 연결에 암호화가 필요합니다	성공적인 DC 연결을 위해 암호화가 필요합니다. Cloud Volumes Service에서 기본적으로 비활성화되어 있습니다.	거짓	아니요

이중 프로토콜/멀티프로토콜

Cloud Volumes Service는 적절한 액세스 권한을 유지하면서 동일한 데이터 세트를 SMB 및 NFS 클라이언트 모두에 공유할 수 있는 기능을 제공합니다 ("이중 프로토콜")를 클릭합니다. 이는 프로토콜 간 ID 매핑을 조정하고 중앙 집중식 백엔드 LDAP 서버를 사용하여 Cloud Volumes Service에 UNIX ID를 제공하는 방식으로 수행됩니다. Windows Active Directory를 사용하여 Windows 및 UNIX 사용자를 모두 편리하게 제공할 수 있습니다.

액세스 제어

- * 공유 액세스 제어. * NAS 공유에 액세스할 수 있는 클라이언트 및/또는 사용자 및 그룹을 결정합니다. NFS의 경우 엑스포트 정책과 규칙을 사용하여 클라이언트 엑스포트 액세스를 제어합니다. NFS 내보내기는 Cloud Volumes Service 인스턴스에서 관리됩니다. SMB는 CIFS/SMB 공유를 사용하고 ACL을 공유하여 사용자 및 그룹 레벨에서 보다 세부적인 제어를 제공합니다. Cloud Volumes Service 인스턴스에 대한 관리자 권한이 있는 계정과 함께 https://library.netapp.com/ecmdocs/ECMP1401220/html/GUID-C1772CDF-8AEE-422B-AB87-CFCB7E50FF94.html[MMC/Computer 관리 를 사용하여 SMB 클라이언트에서 공유 수준 ACL을 구성할 수 있습니다(ncvs-gc-smb.html#로컬/BUILTIN 관리자/백업 권한이 있는 계정" 섹션 참조).
- * 파일 액세스 제어. * 파일 또는 폴더 수준에서 권한을 제어하고 항상 NAS 클라이언트에서 관리합니다. NFS 클라이언트는 기존 모드 비트(rwx) 또는 NFSv4 ACL을 사용할 수 있습니다. SMB 클라이언트는 NTFS 권한을 활용합니다.

NFS와 SMB 모두에 데이터를 제공하는 볼륨의 액세스 제어는 사용 중인 프로토콜에 따라 다릅니다. 이중 프로토콜의 사용 권한에 대한 자세한 내용은 “ 절을 참조하십시오권한 모델.”

사용자 매핑

클라이언트가 볼륨에 액세스하면 Cloud Volumes Service는 들어오는 사용자를 반대 방향으로 유효한 사용자에게 매핑하려고 시도합니다. 이는 프로토콜 간에 적절한 액세스를 결정하고 액세스를 요청하는 사용자가 실제로 자신이 주장하는 사용자인지 확인하기 위해 필요합니다.

예를 들어, "joe"라는 Windows 사용자가 SMB를 통해 UNIX 사용 권한이 있는 볼륨에 액세스하려고 하면 Cloud Volumes Service는 검색을 수행하여 "joe"라는 해당 UNIX 사용자를 찾습니다. 이 파일이 있으면 Windows 사용자 Joe로 SMB 공유에 기록되는 파일이 NFS 클라이언트의 UNIX 사용자 Joe로 나타납니다.

또는 UNIX 사용자인 "Joe"가 Windows 사용 권한이 있는 Cloud Volumes Service 볼륨에 대한 액세스를 시도할 경우 UNIX 사용자는 유효한 Windows 사용자에게 매핑할 수 있어야 합니다. 그렇지 않으면 볼륨에 대한 액세스가 거부됩니다.

현재 LDAP를 사용하는 외부 UNIX ID 관리에는 Active Directory만 지원됩니다. 이 서비스에 대한 액세스 구성에 대한 자세한 내용은 을 참조하십시오 "AD 연결을 생성하는 중입니다".

이중 프로토콜 설정을 사용하는 경우 Cloud Volumes Service는 볼륨에 대한 보안 스타일을 사용하여 ACL 유형을 결정합니다. 이러한 보안 스타일은 지정된 NAS 프로토콜을 기반으로 설정되거나, 이중 프로토콜의 경우 Cloud Volumes Service 볼륨 생성 시 선택하는 것입니다.

- NFS만 사용하는 경우 Cloud Volumes Service 볼륨은 UNIX 사용 권한을 사용합니다.
- SMB만 사용하는 경우 Cloud Volumes Service 볼륨은 NTFS 권한을 사용합니다.

이중 프로토콜 볼륨을 생성하는 경우 볼륨 생성 시 ACL 스타일을 선택할 수 있습니다. 이 결정은 원하는 권한 관리를 기반으로 해야 합니다. 사용자가 Windows/SMB 클라이언트의 권한을 관리하는 경우 NTFS 를 선택합니다. 사용자가 NFS 클라이언트 및 chmod/chown을 사용하려는 경우 UNIX 보안 스타일을 사용합니다.

Active Directory 연결을 생성할 때의 고려 사항

Cloud Volumes Service를 사용하면 Cloud Volumes Service 인스턴스를 외부 Active Directory 서버에 연결하여 SMB 및 UNIX 사용자 모두의 ID 관리를 수행할 수 있습니다. Cloud Volumes Service에서 SMB를 사용하려면 Active Directory 연결을 생성해야 합니다.

이 구성은 보안을 고려해야 하는 몇 가지 옵션을 제공합니다. 외부 Active Directory 서버는 온-프레미스 인스턴스 또는 클라우드 네이티브 서버가 될 수 있습니다. 온-프레미스 Active Directory 서버를 사용하는 경우, 도메인을 외부 네트워크(예: DMZ 또는 외부 IP 주소)에 노출하지 마십시오. 대신 을 사용하여 사내 네트워크에 대한 보안 전용 터널 또는 VPN, 단방향 포리스트 트러스트 또는 전용 네트워크 연결을 사용합니다 "개인 Google 액세스". 에 대한 자세한 내용은 Google Cloud 설명서를 참조하십시오 "Google Cloud에서 Active Directory를 사용하는 모범 사례".

> CVS-SW를 사용하려면 Active Directory 서버가 동일한 지역에 있어야 합니다. CVS-SW에서 다른 지역으로 DC 연결을 시도하면 시도가 실패합니다. CVS-SW를 사용할 때는 Active Directory DC를 포함하는 Active Directory 사이트를 생성한 다음 Cloud Volumes Service에서 사이트를 지정하여 교차 지역 DC 연결 시도를 방지해야 합니다.

Active Directory 자격 증명

NFS용 SMB 또는 LDAP가 활성화된 경우 Cloud Volumes Service는 Active Directory 컨트롤러와 상호 작용하여 인증에 사용할 컴퓨터 계정 개체를 생성합니다. 이는 Windows SMB 클라이언트가 도메인에 가입하는 방식과 다르지 않으며 Active Directory의 OU(조직 구성 단위)에 동일한 액세스 권한이 필요합니다.

대부분의 경우 보안 그룹은 Cloud Volumes Service와 같은 외부 서버에서 Windows 관리자 계정 사용을 허용하지 않습니다. 경우에 따라 Windows 관리자 사용자는 보안 모범 사례로 완전히 비활성화됩니다.

SMB 시스템 계정을 생성하는 데 필요한 권한입니다

Cloud Volumes Service 컴퓨터 개체를 Active Directory에 추가하려면 도메인에 대한 관리 권한이 있거나 있는 계정입니다 "컴퓨터 계정 객체를 생성 및 수정하는 위임된 권한" 지정된 OU에 대한 필수 구성 요소입니다. Active Directory의 제어 위임 마법사를 사용하여 다음과 같은 액세스 권한이 있는 컴퓨터 개체를 생성/삭제할 수 있는 사용자 지정 작업을 만들어 이 작업을 수행할 수 있습니다.

- 읽기/쓰기
- 모든 자식 개체를 생성/삭제합니다
- 모든 속성 읽기/쓰기
- 암호 변경/재설정

이렇게 하면 정의된 사용자에 대한 보안 ACL이 Active Directory의 OU에 자동으로 추가되고 Active Directory 환경에 대한 액세스가 최소화됩니다. 사용자가 위임된 후에는 이 창에서 해당 사용자 이름과 암호를 Active Directory 자격 증명으로 제공할 수 있습니다.

Active Directory 도메인에 전달되는 사용자 이름과 암호는 컴퓨터 계정 개체 쿼리 및 생성 중에 Kerberos 암호화를 사용하여 보안을 강화합니다.

Active Directory 연결 세부 정보입니다

를 클릭합니다 "Active Directory 연결 세부 정보" 다음과 같은 컴퓨터 계정 배치에 대한 특정 Active Directory 스키마 정보를 관리자에게 제공하는 필드를 제공합니다.

- * Active Directory 연결 유형. * Cloud Volumes Service 또는 CVS 성능 서비스 유형의 볼륨에 대해 영역의 Active Directory 연결이 사용되는지 여부를 지정하는 데 사용됩니다. 기존 연결에서 이 설정을 잘못 설정하면 사용하거나 편집할 때 제대로 작동하지 않을 수 있습니다.
- * 도메인. * Active Directory 도메인 이름입니다.
- * 사이트. * 보안 및 성능을 위해 Active Directory 서버를 특정 사이트로 제한합니다 "고려 사항". Cloud Volumes Service는 현재 Cloud Volumes Service 인스턴스가 아닌 다른 영역에 있는 Active Directory 서버에 대한 Active Directory 인증 요청을 허용하지 않으므로 여러 Active Directory 서버가 여러 지역에 걸쳐 있는 경우 이 작업이 필요합니다. 예를 들어, Active Directory 도메인 컨트롤러는 CVS-Performance만 지원하는 영역에 있지만 CVS-SW 인스턴스에서 SMB 공유를 원할 수 있습니다.
- DNS 서버 * 이름 조회에 사용할 DNS 서버.
- NetBIOS 이름(선택 사항).* 필요한 경우 서버의 NetBIOS 이름입니다. 이 기능은 Active Directory 연결을 사용하여 새 컴퓨터 계정을 만들 때 사용됩니다. 예를 들어 NetBIOS 이름이 CVS-East로 설정된 경우 컴퓨터 계정 이름은 CVS-East-{1234}가 됩니다. 섹션을 참조하십시오 "Active Directory에 Cloud Volumes Service가 표시되는 방식" 를 참조하십시오.
- * OU(조직 단위) * 컴퓨터 계정을 만들 특정 OU. 이 기능은 컴퓨터 계정에 대해 특정 OU에 제어를 위임하는 경우에 유용합니다.
- * AES 암호화. * AD 인증에 AES 암호화 사용 확인란을 선택하거나 선택 취소할 수도 있습니다. Active Directory 인증에 AES 암호화를 사용하면 사용자 및 그룹 조회 중에 Cloud Volumes Service에서 Active Directory로 통신하는 데 추가적인 보안을 제공할 수 있습니다. 이 옵션을 활성화하기 전에 도메인 관리자에게 문의하여 Active Directory 도메인 컨트롤러가 AES 인증을 지원하는지 확인하십시오.

기본적으로 대부분의 Windows 서버는 약한 암호(예: DES 또는 RC4-HMAC)를 비활성화하지 않지만 약한 암호를 비활성화하도록 선택하는 경우 Cloud Volumes Service Active Directory 연결이 AES를 사용하도록 구성되었는지 확인합니다. 그렇지 않으면 인증 실패가 발생합니다. AES 암호화를 사용하도록 설정하면 약한 암호가 비활성화되지 않고 대신 Cloud Volumes Service SMB 시스템 계정에 AES 암호화에 대한 지원이 추가됩니다.

Kerberos 영역 세부 정보

이 옵션은 SMB 서버에는 적용되지 않습니다. 대신, Cloud Volumes Service 시스템에 NFS Kerberos를 구성할 때 사용됩니다. 이러한 세부 정보가 채워지면 NFS Kerberos 영역이 구성되고(Linux의 krb5.conf 파일과 유사), Active Directory 연결이 NFS Kerberos 메일 센터(KDC) 역할을 하므로 Cloud Volumes Service 볼륨 생성에 NFS Kerberos가 지정될 때 사용됩니다.

Windows 이외의 KDC는 현재 Cloud Volumes Service에서 사용할 수 없습니다.

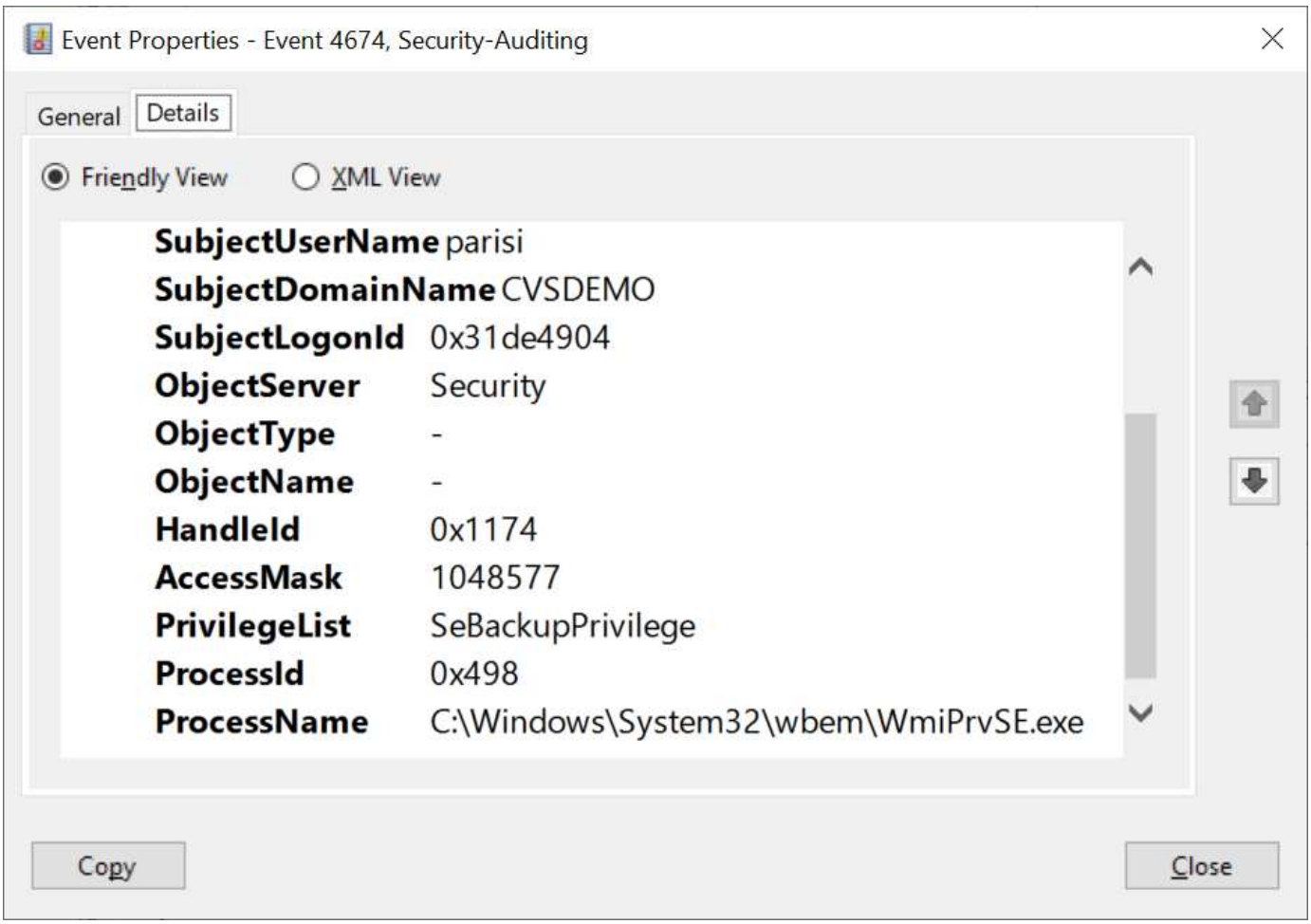
지역

영역을 사용하면 Active Directory 연결이 있는 위치를 지정할 수 있습니다. 이 영역은 Cloud Volumes Service 볼륨과 동일한 영역이어야 합니다.

- * LDAP를 사용하는 로컬 NFS 사용자 * 이 섹션에는 LDAP를 사용하는 로컬 NFS 사용자를 허용하는 옵션도 있습니다. UNIX 사용자 그룹 구성원 지원을 NFS(확장 그룹)의 16개 그룹 제한 이상으로 확장하려면 이 옵션을 선택하지 않아야 합니다. 그러나 확장된 그룹을 사용하려면 UNIX ID에 대해 구성된 LDAP 서버가 필요합니다. LDAP 서버가 없는 경우 이 옵션을 선택되지 않은 상태로 둡니다. LDAP 서버가 있고 로컬 UNIX 사용자(예: 루트)도 사용하려면 이 옵션을 선택합니다.

백업 사용자

이 옵션을 사용하면 Cloud Volumes Service 볼륨에 대한 백업 권한이 있는 Windows 사용자를 지정할 수 있습니다. NAS 볼륨의 데이터를 올바르게 백업 및 복원하려면 일부 애플리케이션에 백업 권한(SeBackupPrivilege)이 필요합니다. 이 사용자는 볼륨의 데이터에 대한 높은 수준의 액세스 권한을 가지고 있으므로 고려해야 합니다 "해당 사용자 액세스에 대한 감사를 설정합니다". 활성화된 감사 이벤트는 이벤트 뷰어 > Windows 로그 > 보안에 표시됩니다.



보안 권한 사용자

이 옵션을 사용하면 Cloud Volumes Service 볼륨에 대한 보안 수정 권한이 있는 Windows 사용자를 지정할 수 있습니다. 일부 응용 프로그램에는 보안 권한(SeSecurityPrivilege)이 필요합니다 ("SQL Server와 같은")를 클릭하여 설치 중에 권한을 적절하게 설정합니다. 이 권한은 보안 로그를 관리하는 데 필요합니다. 이 권한은 SeBackupPrivilege 권한만큼 강력하지는 않지만 NetApp이 권장합니다 "사용자의 사용자 액세스 감사" 필요한 경우 이 권한 수준을 사용합니다.

자세한 내용은 을 참조하십시오 "새 로그온에 할당된 특수 권한".

Active Directory에 **Cloud Volumes Service**가 표시되는 방식

Cloud Volumes Service는 Active Directory에 일반 컴퓨터 계정 개체로 표시됩니다. 명명 규칙은 다음과 같습니다.

- CIFS/SMB 및 NFS Kerberos는 별도의 시스템 계정 객체를 생성합니다.
- LDAP가 설정된 NFS는 Active Directory에서 Kerberos LDAP 바인드를 위한 컴퓨터 계정을 생성합니다.
- LDAP가 있는 이중 프로토콜 볼륨은 LDAP 및 SMB의 CIFS/SMB 시스템 계정을 공유합니다.
- CIFS/SMB 시스템 계정은 시스템 계정에 대해 이름-1234(10자 이름에 하이픈이 추가된 4자리 임의 ID)의 명명 규칙을 사용합니다. Active Directory 연결에서 NetBIOS 이름 설정을 사용하여 이름을 정의할 수 있습니다(“ 절 참조)Active Directory 연결 세부 정보입니다").
- NFS Kerberos에서는 nfs-name-1234를 명명 규칙(최대 15자)으로 사용합니다. 15자 이상을 사용하는 경우 이름은 nfs-duncated-name-1234입니다.
- NFS 전용 CVS - LDAP가 설정된 성능 인스턴스는 CIFS/SMB 인스턴스와 동일한 명명 규칙을 사용하여 LDAP 서버에 바인딩하기 위한 SMB 시스템 계정을 생성합니다.
- SMB 컴퓨터 계정이 생성되면 숨겨진 기본 관리자 공유가 생성됩니다(섹션 참조) ""숨겨진 기본 공유"")도 생성되지만(c$, admin$, ipc$) 해당 공유는 할당된 ACL이 없으며 액세스할 수 없습니다.
- 컴퓨터 계정 개체는 기본적으로 CN=Computers에 배치되지만 필요한 경우 다른 OU를 지정할 수 있습니다. 자세한 내용은 " 단원을 참조하십시오SMB 시스템 계정을 생성하는 데 필요한 권한입니다"Cloud Volumes Service에 대한 컴퓨터 계정 개체를 추가/제거하는 데 필요한 액세스 권한에 대한 정보를 제공합니다.

Cloud Volumes Service가 Active Directory에 SMB 컴퓨터 계정을 추가하면 다음 필드가 채워집니다.

- CN(지정된 SMB 서버 이름 포함)
- dNSHostName(SMBserver.domain.com 포함)
- msDS-SupportedEncryptionTypes (AES 암호화가 활성화되지 않은 경우 DES_CBC_MD5, RC4_HMAC_MD5 허용; AES 암호화가 활성화된 경우 DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96은 SMB용 시스템 계정과 티켓 교환에 허용됨)
- 이름(SMB 서버 이름 포함)
- sAMAccountName(SMBserver$ 사용)
- servicePrincipalName(호스트 /smbserver.domain.com 및 Kerberos에 대한 호스트/smbserver SPN 포함)

컴퓨터 계정에서 약한 Kerberos 암호화 유형(enctype)을 비활성화하려면 컴퓨터 계정의 MSDS-SupportedEncryptionTypes 값을 다음 표의 값 중 하나로 변경하여 AES만 허용할 수 있습니다.

MSDS - SupportedEncryptionTypes 값입니다	**Enctype**이 활성화되었습니다
2	DES_CBC_MD5
4	RC4_HMAC
8	AES128_CTS_HMAC_SHA1_96만 해당
16	AES256_CTS_HMAC_SHA1_96만 해당
24	AES128_CTS_HMAC_SHA1_96 및 AES256_CTS_HMAC_SHA1_96

MSDS - SupportedEncryptionTypes 값입니다	**Enctype**이 활성화되었습니다
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 및 AES256_CTS_HMAC_SHA1_96

SMB 시스템 계정에 대해 AES 암호화를 활성화하려면 Active Directory 연결을 생성할 때 AD 인증에 AES 암호화 사용을 클릭합니다.

NFS Kerberos에서 AES 암호화를 사용하도록 설정하려면 "Cloud Volumes Service 설명서를 참조하십시오".

기타 **NAS** 인프라스트럭처 서비스 종속성**(KDC, LDAP** 및 **DNS)**

NAS 공유에 Cloud Volumes Service를 사용하는 경우 적절한 기능을 위해 외부 종속성이 필요할 수 있습니다. 이러한 종속성은 특정 상황에서 적용됩니다. 다음 표에는 다양한 구성 옵션과 종속 항목이 필요한 항목이 나와 있습니다.

구성	종속성이 필요합니다
NFSv3만 해당	없음
NFSv3 Kerberos만 해당	Windows Active Directory: * KDC * DNS * LDAP
NFSv4.1만 해당	클라이언트 ID 매핑 구성(/etc/idmap.conf)
NFSv4.1 Kerberos만 해당	• 클라이언트 ID 매핑 구성(/etc/idmap.conf) • Windows Active Directory: KDC DNS LDAP
SMB만 해당	Active Directory: * KDC * DNS
멀티프로토콜 NAS(NFS 및 SMB)	• 클라이언트 ID 매핑 구성(NFSv4.1 전용; /etc/idmap.conf) • Windows Active Directory: KDC DNS LDAP

시스템 계정 개체에 대한 **Kerberos** 키 탭 회전/암호 재설정

SMB 시스템 계정의 경우 Cloud Volumes Service는 SMB 시스템 계정에 대한 주기적인 암호 재설정을 예약합니다. 이러한 암호 재설정은 Kerberos 암호화를 사용하여 발생하며, 오후 11시부터 오전 1시 사이에 임의 시간에 매주 일요일 일정에 따라 작동합니다. 이러한 암호 재설정은 Kerberos 키 버전을 변경하고, Cloud Volumes Service 시스템에 저장된 키 탭을 회전하며, Cloud Volumes Service에서 실행되는 SMB 서버의 보안을 더욱 강화할 수 있도록 도와줍니다. 시스템 계정 암호는 무작위배정되며 관리자에게 알려져 있지 않습니다.

NFS Kerberos 시스템 계정의 경우 KDC와 새 키 탭이 생성/교환될 때만 암호 재설정이 적용됩니다. 현재 Cloud Volumes Service에서는 이 작업을 수행할 수 없습니다.

LDAP 및 **Kerberos**와 함께 사용할 네트워크 포트

LDAP 및 Kerberos를 사용하는 경우 이러한 서비스에서 사용 중인 네트워크 포트를 확인해야 합니다. 에서 Cloud Volumes Service에서 사용 중인 포트의 전체 목록을 찾을 수 있습니다 "보안 고려 사항에 대한 Cloud Volumes Service 문서".

LDAP를 지원합니다

Cloud Volumes Service는 LDAP 클라이언트 역할을 하며 UNIX ID에 대한 사용자 및 그룹 조회를 위해 표준 LDAP 검색 쿼리를 사용합니다. Cloud Volumes Service에서 제공하는 표준 기본 사용자 이외의 사용자 및 그룹을 사용하려면 LDAP가 필요합니다. NFS Kerberos를 사용자 보안 주체(예: user1@domain.com 사용할 계획이라면 LDAP도 필요합니다. 현재 Microsoft Active Directory를 사용하는 LDAP만 지원됩니다.

Active Directory를 UNIX LDAP 서버로 사용하려면 UNIX ID에 사용할 사용자 및 그룹에 필요한 UNIX 속성을 채워야 합니다. Cloud Volumes Service에서는 에 따라 특성을 쿼리하는 기본 LDAP 스키마 템플릿을 사용합니다 "RFC-2307-bis". 따라서 다음 표에서는 사용자 및 그룹에 채울 최소 필수 Active Directory 속성과 각 속성이 사용되는 특성을 보여 줍니다.

Active Directory에서 LDAP 속성을 설정하는 방법에 대한 자세한 내용은 을 참조하십시오 "이중 프로토콜 액세스 관리."

속성	기능
UID *	UNIX 사용자 이름을 지정합니다
uidNumber *	UNIX 사용자의 숫자 ID를 지정합니다
gidNumber *	UNIX 사용자의 기본 그룹 숫자 ID를 지정합니다
objectClass *	사용 중인 개체 유형을 지정합니다. Cloud Volumes Service에서는 "사용자"를 개체 클래스 목록에 포함해야 합니다(기본적으로 대부분의 Active Directory 배포에는 포함됨).
이름	계정에 대한 일반 정보(실제 이름, 전화 번호 등, gecos라고도 함)
unixUserPassword	NAS 인증을 위한 UNIX ID 조회에 사용되지 않으므로 설정할 필요가 없습니다. 이렇게 설정하면 구성된 unixUserPassword 값이 일반 텍스트로 설정됩니다.
unixHomeDirectory	사용자가 Linux 클라이언트에서 LDAP에 대해 인증할 때 UNIX 홈 디렉토리의 경로를 정의합니다. UNIX 홈 디렉토리 기능에 LDAP를 사용하려면 이 옵션을 설정합니다.
LoginShell입니다	사용자가 LDAP에 대해 인증할 때 Linux 클라이언트의 bash/profile 셸에 대한 경로를 정의합니다.

- 는 Cloud Volumes Service의 적절한 기능을 위해 특성이 필요함을 나타냅니다. 나머지 속성은 클라이언트 측 전용입니다.

속성	기능
CN *	UNIX 그룹 이름을 지정합니다. LDAP에 Active Directory를 사용하는 경우 개체를 처음 만들 때 설정되지만 나중에 변경할 수 있습니다. 이 이름은 다른 개체와 같을 수 없습니다. 예를 들어, user1이라는 UNIX 사용자가 Linux 클라이언트의 user1이라는 그룹에 속해 있는 경우 Windows에서는 cn 특성이 같은 두 개체를 허용하지 않습니다. 이 문제를 해결하려면 Windows 사용자의 이름을 고유한 이름(예: user1-UNIX)으로 바꿉니다. Cloud Volumes Service의 LDAP는 UNIX 사용자 이름에 uid 속성을 사용합니다.
gidNumber *	UNIX 그룹 숫자 ID를 지정합니다.
objectClass *	사용 중인 개체 유형을 지정합니다. Cloud Volumes Service에서는 개체 클래스 목록에 그룹을 포함해야 합니다. 이 특성은 기본적으로 대부분의 Active Directory 배포에 포함됩니다.
memberUid	UNIX 그룹의 구성원인 UNIX 사용자를 지정합니다. Cloud Volumes Service에서 Active Directory LDAP를 사용할 경우 이 필드는 필요하지 않습니다. Cloud Volumes Service LDAP 스키마는 그룹 구성원 자격에 구성원 필드를 사용합니다.
구성원 *	그룹 구성원 자격/보조 UNIX 그룹에 필요합니다. 이 필드는 Windows 그룹에 Windows 사용자를 추가하여 채워집니다. 그러나 Windows 그룹에 채워진 UNIX 특성이 없는 경우 UNIX 사용자의 그룹 구성원 목록에는 포함되지 않습니다. NFS에서 사용할 수 있어야 하는 모든 그룹은 이 표에 나열된 필수 UNIX 그룹 속성을 채워야 합니다.

- 는 Cloud Volumes Service의 적절한 기능을 위해 특성이 필요함을 나타냅니다. 나머지 속성은 클라이언트 측 전용입니다.

LDAP 바인딩 정보

LDAP에서 사용자를 쿼리하려면 Cloud Volumes Service가 LDAP 서비스에 바인딩(로그인)해야 합니다. 이 로그인에는 읽기 전용 권한이 있으며 디렉토리 조회를 위해 LDAP UNIX 속성을 쿼리하는 데 사용됩니다. 현재 LDAP 바인딩은 SMB 컴퓨터 계정을 통해서만 가능합니다.

'CVS 성능' 인스턴스에만 LDAP를 사용하도록 설정하고 NFSv3, NFSv4.1 또는 이중 프로토콜 볼륨에는 LDAP를 사용할 수 있습니다. LDAP 지원 볼륨을 성공적으로 배포하려면 Cloud Volumes Service 볼륨과 동일한 영역에 Active Directory 연결을 설정해야 합니다.

LDAP가 활성화된 경우 특정 시나리오에서 다음이 발생합니다.

- Cloud Volumes Service 프로젝트에 NFSv3이나 NFSv4.1만 사용되는 경우 Active Directory 도메인 컨트롤러에서 새 컴퓨터 계정이 생성되고 Cloud Volumes Service의 LDAP 클라이언트는 시스템 계정 자격 증명을 사용하여 Active Directory에 바인딩됩니다. NFS 볼륨 및 숨겨진 기본 관리 공유에 대해 SMB 공유가 생성되지 않습니다(섹션 참조) ""숨겨진 기본 공유"")의 공유 ACL이 제거되었습니다.
- Cloud Volumes Service 프로젝트에 이중 프로토콜 볼륨을 사용하는 경우 SMB 액세스용으로 생성된 단일 컴퓨터 계정만 Cloud Volumes Service의 LDAP 클라이언트를 Active Directory에 바인딩하는 데 사용됩니다. 추가 컴퓨터 계정이 생성되지 않습니다.

- 전용 SMB 볼륨이 별도로 생성된 경우(LDAP가 설정된 NFS 볼륨 이전 또는 이후에) LDAP 바인딩의 컴퓨터 계정이 SMB 시스템 계정과 공유됩니다.
- NFS Kerberos도 사용하도록 설정된 경우 두 개의 시스템 계정이 생성됩니다. 하나는 SMB 공유 및/또는 LDAP 바인드이고 다른 하나는 NFS Kerberos 인증입니다.

LDAP 쿼리입니다

LDAP 바인딩은 암호화되지만 일반 LDAP 포트 389를 사용하여 LDAP 쿼리가 일반 텍스트로 회선을 통해 전달됩니다. 이 잘 알려진 포트는 현재 Cloud Volumes Service에서 변경할 수 없습니다. 따라서 네트워크에서 패킷 스니핑에 액세스할 수 있는 사용자는 사용자 및 그룹 이름, 숫자 ID 및 그룹 구성원 자격을 볼 수 있습니다.

그러나 Google Cloud VM은 다른 VM의 유니캐스트 트래픽을 스니프할 수 없습니다. LDAP 트래픽에 활성 중인 VM(즉, 바인딩 가능)만 LDAP 서버의 트래픽을 볼 수 있습니다. Cloud Volumes Service의 패킷 스니핑에 대한 자세한 내용은 섹션을 참조하십시오 ""패킷 감지/추적 고려 사항""

LDAP 클라이언트 구성 기본값

Cloud Volumes Service 인스턴스에서 LDAP가 활성화되면 기본적으로 특정 구성 세부 정보를 사용하여 LDAP 클라이언트 구성이 생성됩니다. 경우에 따라 옵션이 Cloud Volumes Service(지원되지 않음)에 적용되지 않거나 구성할 수 없습니다.

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까?
LDAP 서버 목록	쿼리에 사용할 LDAP 서버 이름 또는 IP 주소를 설정합니다. Cloud Volumes Service에는 사용되지 않습니다. 대신 Active Directory 도메인을 사용하여 LDAP 서버를 정의합니다.	설정되지 않았습니다	아니요
Active Directory 도메인	LDAP 쿼리에 사용할 Active Directory 도메인을 설정합니다. Cloud Volumes Service는 DNS의 LDAP에 대한 SRV 레코드를 활용하여 도메인에서 LDAP 서버를 찾습니다.	Active Directory 연결에 지정된 Active Directory 도메인으로 설정합니다.	아니요
기본 Active Directory 서버	LDAP에 사용할 기본 Active Directory 서버를 설정합니다. Cloud Volumes Service에서 지원되지 않습니다. 대신 Active Directory 사이트를 사용하여 LDAP 서버 선택을 제어할 수 있습니다.	설정되지 않았습니다.	아니요

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
SMB 서버 자격 증명을 사용하여 바인딩합니다	SMB 시스템 계정을 사용하여 LDAP에 바인딩합니다. 현재 Cloud Volumes Service에서 지원되는 유일한 LDAP 바인딩 방법입니다.	참	아니요
스키마 템플릿	LDAP 쿼리에 사용되는 스키마 템플릿입니다.	MS-AD-BIS	아니요
LDAP 서버 포트입니다	LDAP 쿼리에 사용되는 포트 번호입니다. Cloud Volumes Service는 현재 표준 LDAP 포트 389만 사용합니다. LDAPS/포트 636은 현재 지원되지 않습니다.	389	아니요
LDAPS가 활성화되어 있습니다	SSL(Secure Sockets Layer)을 통한 LDAP가 쿼리 및 바인딩에 사용되는지 여부를 제어합니다. 현재 Cloud Volumes Service에서 지원되지 않습니다.	거짓	아니요
쿼리 시간 제한(초)	쿼리 시간이 초과되었습니다. 쿼리가 지정된 값보다 오래 걸면 쿼리가 실패합니다.	3	아니요
최소 바인딩 인증 레벨	지원되는 최소 바인딩 레벨입니다. Cloud Volumes Service는 LDAP 바인딩에 컴퓨터 계정을 사용하고 Active Directory는 기본적으로 익명 바인딩을 지원하지 않으므로 이 옵션은 보안을 위해 사용되지 않습니다.	익명	아니요
DN 바인딩	단순 바인딩이 사용될 때 바인딩에 사용되는 사용자/고유 이름(DN)입니다. Cloud Volumes Service는 LDAP 바인딩에 시스템 계정을 사용하며 현재 단순 바인딩 인증을 지원하지 않습니다.	설정되지 않았습니다	아니요

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
기본 DN	LDAP 검색에 사용되는 기본 DN입니다.	Windows 도메인이 DN 형식(즉, DC=domain, DC=local)으로 Active Directory 연결에 사용됩니다.	아니요
기본 검색 범위	기본 DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service는 하위 트리 검색만 지원합니다.	하위 트리	아니요
사용자 DN	사용자가 LDAP 쿼리를 검색하는 DN을 정의합니다. 현재 Cloud Volumes Service에서는 지원되지 않으므로 모든 사용자 검색은 기본 DN에서 시작됩니다.	설정되지 않았습니다	아니요
사용자 검색 범위	사용자 DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service는 사용자 검색 범위 설정을 지원하지 않습니다.	하위 트리	아니요
그룹 DN	그룹 검색이 LDAP 쿼리를 시작하는 DN을 정의합니다. 현재 Cloud Volumes Service에 대해 지원되지 않으므로 모든 그룹 검색이 기본 DN에서 시작됩니다.	설정되지 않았습니다	아니요
그룹 검색 범위	그룹 DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service는 그룹 검색 범위 설정을 지원하지 않습니다.	하위 트리	아니요
넷그룹 DN입니다	넷그룹이 LDAP 쿼리를 검색하는 DN을 정의합니다. 현재 Cloud Volumes Service에 대해 지원되지 않으므로 모든 넷그룹 검색은 기본 DN에서 시작됩니다.	설정되지 않았습니다	아니요

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
넷그룹 검색 범위입니다	넷그룹 DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service에서는 넷그룹 검색 범위 설정을 지원하지 않습니다.	하위 트리	아니요
LDAP를 통해 start_tls를 사용합니다	포트 389를 통한 인증서 기반 LDAP 연결에 Start TLS를 활용합니다. 현재 Cloud Volumes Service에서 지원되지 않습니다.	거짓	아니요
Netgroup-by-host 조회를 설정합니다	넷그룹을 확장하여 모든 구성원을 나열하는 대신 호스트 이름별로 넷그룹 조회를 설정합니다. 현재 Cloud Volumes Service에서 지원되지 않습니다.	거짓	아니요
Netgroup-by-host DN입니다	넷그룹별 검색이 LDAP 쿼리를 시작하는 DN을 정의합니다. Cloud Volumes Service에 대해 현재 호스트별 넷그룹이 지원되지 않습니다.	설정되지 않았습니다	아니요
Netgroup-by-host 검색 범위입니다	Netgroup-by-host DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service에 대해 현재 호스트별 넷그룹이 지원되지 않습니다.	하위 트리	아니요
클라이언트 세션 보안	LDAP에서 사용하는 세션 보안 수준(서명, 봉인 또는 없음)을 정의합니다. LDAP 서명은 Active Directory에서 요청하는 경우 CVS - 성능에서 지원됩니다. CVS-SW는 LDAP 서명을 지원하지 않습니다. 두 서비스 유형 모두에서 봉인은 현재 지원되지 않습니다.	없음	아니요

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
LDAP 조회 추적	여러 LDAP 서버를 사용하는 경우 조회 추적을 통해 첫 번째 서버에서 항목을 찾을 수 없을 때 클라이언트가 목록의 다른 LDAP 서버를 참조할 수 있습니다. 현재 Cloud Volumes Service에서는 지원되지 않습니다.	거짓	아니요
그룹 구성원 필터	LDAP 서버에서 그룹 구성원을 검색할 때 사용할 사용자 지정 LDAP 검색 필터를 제공합니다. 현재 Cloud Volumes Service에서는 지원되지 않습니다.	설정되지 않았습니다	아니요

비대칭 이름 매핑에 **LDAP**를 사용합니다

Cloud Volumes Service는 기본적으로 특별한 구성 없이 양방향으로 동일한 사용자 이름을 가진 Windows 사용자와 UNIX 사용자를 매핑합니다. Cloud Volumes Service가 유효한 UNIX 사용자(LDAP 사용)를 찾을 수 있는 한 1:1 이름 매핑이 발생합니다. 예를 들어, 윈도우 사용자인 'johnsmith'를 사용하는 경우, Cloud Volumes Service가 LDAP에서 johnsmith라는 UNIX 사용자를 찾을 수 있다면, 해당 사용자에 대한 이름 매핑이 성공하면, johnsmith로 생성된 모든 파일/폴더에 올바른 사용자 소유권이 표시됩니다. 또한 사용 중인 NAS 프로토콜에 관계없이 "johnsmith"에 영향을 주는 모든 ACL이 적용됩니다. 이것을 대칭 이름 매핑이라고 합니다.

비대칭 이름 매핑은 Windows 사용자 및 UNIX 사용자 ID가 일치하지 않는 경우를 나타냅니다. 예를 들어, 윈도우 사용자인 주스미스(jsmith)가 유닉스의 ID를 갖고 있다면, Cloud Volumes Service는 그 변이에 대한 정보를 얻을 수 있는 방법이 필요합니다. Cloud Volumes Service는 현재 정적 이름 매핑 규칙 생성을 지원하지 않으므로, LDAP를 사용하여 Windows 및 UNIX ID 모두의 사용자 ID를 조회하여 파일 및 폴더의 올바른 소유권과 예상되는 권한을 확인해야 합니다.

기본적으로 Cloud Volumes Service는 이름 맵 데이터베이스 인스턴스의 ns-switch에 LDAP를 포함하므로 비대칭 이름에 LDAP를 사용하여 이름 매핑 기능을 제공하려면 Cloud Volumes Service의 모양을 반영하기 위해 일부 사용자/그룹 속성만 수정하면 됩니다.

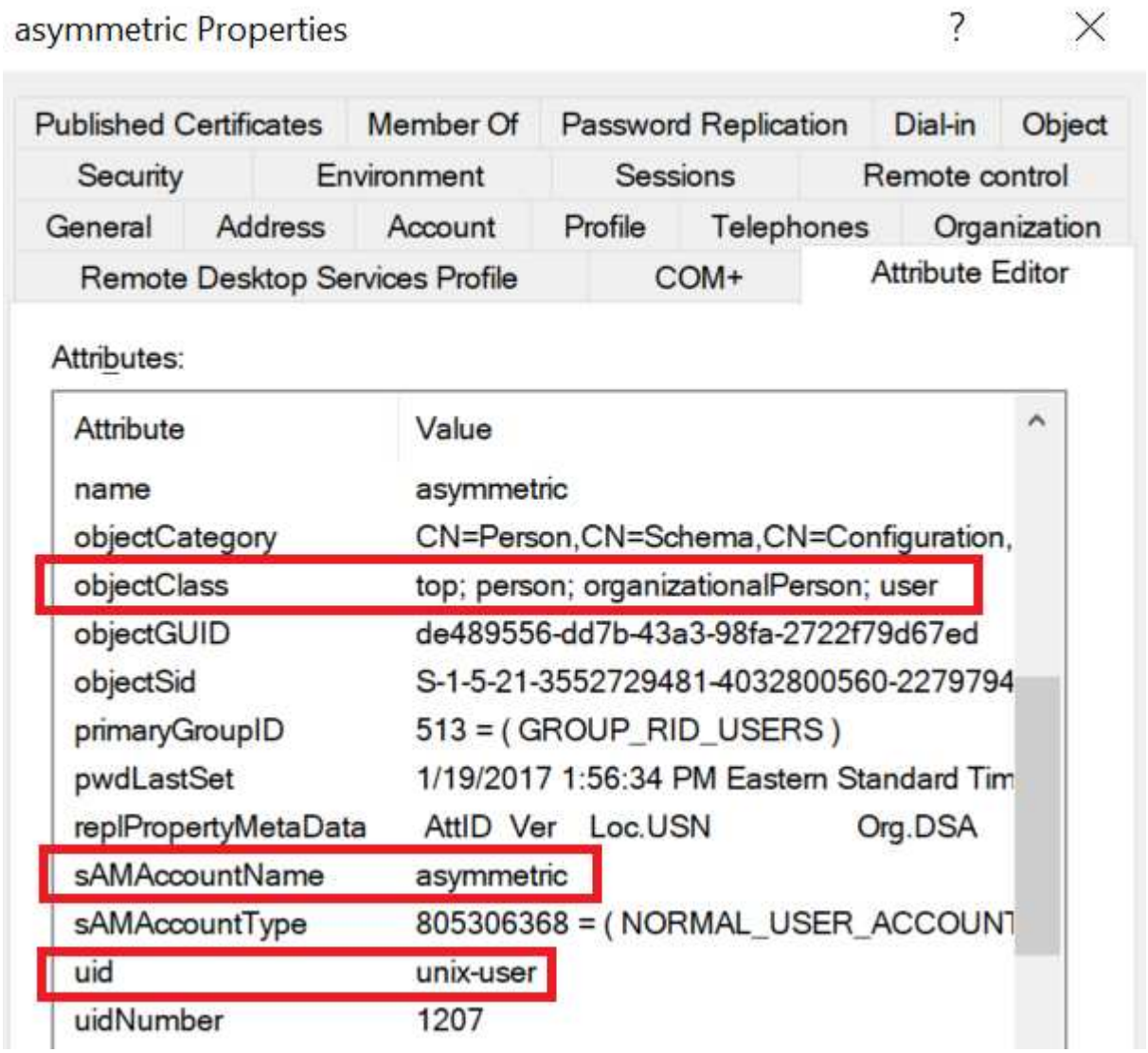
다음 표에서는 비대칭 이름 매핑 기능을 위해 LDAP에 채워야 하는 특성을 보여 줍니다. 대부분의 경우 Active Directory는 이미 이 작업을 수행하도록 구성되어 있습니다.

Cloud Volumes Service 특성입니다	기능	**Cloud Volumes Service**에서 이름 매핑에 사용하는 값입니다
Windows에서 UNIX로의 객체 클래스	사용 중인 개체의 형식을 지정합니다. (즉, 사용자, 그룹, posixAccount 등)	사용자를 포함해야 합니다(필요한 경우 다른 값을 여러 개 포함할 수 있음).
Windows에서 UNIX로의 속성	그러면 생성 시 Windows 사용자 이름이 정의됩니다. Cloud Volumes Service는 Windows에서 UNIX로의 조회에 이 기능을 사용합니다.	여기에서 변경할 필요가 없습니다. sAMAccountName은 Windows 로그인 이름과 동일합니다.
UID	UNIX 사용자 이름을 정의합니다.	원하는 UNIX 사용자 이름입니다.

Cloud Volumes Service는 현재 LDAP 조회에서 도메인 접두사를 사용하지 않으므로 LDAP 이름 맵 조회에서 여러 도메인 LDAP 환경이 제대로 작동하지 않습니다.

다음 예에서는 Windows 이름 "비대칭", UNIX 이름 "UNIX-user"를 가진 사용자와 SMB 및 NFS에서 파일을 쓸 때 나타나는 동작을 보여 줍니다.

다음 그림에서는 LDAP 특성이 Windows 서버에서 어떻게 표시되는지 보여 줍니다.



NFS 클라이언트에서 UNIX 이름을 쿼리할 수 있지만 Windows 이름은 쿼리할 수 없습니다.

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

NFS에서 UNIX-USER로 파일을 쓸 때 NFS 클라이언트의 결과는 다음과 같습니다.

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Windows 클라이언트에서 파일 소유자가 올바른 Windows 사용자로 설정되어 있는지 확인할 수 있습니다.

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

반대로, SMB 클라이언트에서 Windows 사용자 '비대칭'으로 생성된 파일은 다음 텍스트에서와 같이 적절한 UNIX 소유자를 표시합니다.

SMB:

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS:

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAP 채널 바인딩

Windows Active Directory 도메인 컨트롤러의 취약점으로 인해 "Microsoft 보안 권고 ADV190023" DC에서 LDAP 바인드를 허용하는 방법을 변경합니다.

Cloud Volumes Service에 미치는 영향은 모든 LDAP 클라이언트와 동일합니다. Cloud Volumes Service는 현재 채널 바인딩을 지원하지 않습니다. Cloud Volumes Service는 협상을 통해 기본적으로 LDAP 서명을 지원하므로 LDAP 채널 바인딩은 문제가 되지 않습니다. 채널 바인딩이 설정된 LDAP에 바인딩하는 데 문제가 있는 경우 ADV190023의 개선 단계를 수행하여 Cloud Volumes Service에서 LDAP 바인딩이 성공하도록 허용합니다.

DNS

Active Directory와 Kerberos 모두 호스트 이름 대 IP/IP 대 호스트 이름 확인에 대한 DNS에 대한 종속성을 가집니다. DNS를 열려면 포트 53이 열려 있어야 합니다. Cloud Volumes Service는 DNS 레코드를 수정하지 않으며 현재 의 사용을 지원하지 않습니다 "다이나믹 DNS" 네트워크 인터페이스.

DNS 레코드를 업데이트할 수 있는 서버를 제한하도록 Active Directory DNS를 구성할 수 있습니다. 자세한 내용은 을 참조하십시오 "Windows DNS 보안".

Google 프로젝트 내의 리소스는 기본적으로 Active Directory DNS와 연결되지 않은 Google Cloud DNS를 사용합니다. 클라우드 DNS를 사용하는 클라이언트는 Cloud Volumes Service에서 반환하는 UNC 경로를 확인할 수 없습니다. Active Directory 도메인에 참가한 Windows 클라이언트는 Active Directory DNS를 사용하도록 구성되어 있으며 이러한 UNC 경로를 확인할 수 있습니다.

Active Directory에 클라이언트를 연결하려면 Active Directory DNS를 사용하도록 해당 DNS 구성을 구성해야 합니다. 필요에 따라 Active Directory DNS로 요청을 전달하도록 Cloud DNS를 구성할 수 있습니다. 을 참조하십시오 "클라이언트가 SMB NetBIOS 이름을 확인할 수 없는 이유는 무엇입니까?"를 참조하십시오.

Cloud Volumes Service는 현재 DNSSEC를 지원하지 않으며 DNS 쿼리는 일반 텍스트로 수행됩니다.

파일 액세스 감사

현재 Cloud Volumes Service에서 지원되지 않습니다.

안티바이러스 보호

클라이언트의 Cloud Volumes Service에서 NAS 공유에 대한 바이러스 백신 검사를 수행해야 합니다. 현재 Cloud Volumes Service와 통합된 기본 바이러스 백신이 없습니다.

서비스 작업

Cloud Volumes Service 팀은 Google Cloud에서 백엔드 서비스를 관리하고 여러 전략을 사용하여 플랫폼을 보호하고 원치 않는 액세스를 방지합니다.

각 고객은 기본적으로 다른 고객으로부터 액세스 펜싱된 고유한 서브넷을 받게 되며, Cloud Volumes Service의 모든 테넌트는 전체 데이터 격리를 위한 고유한 네임스페이스와 VLAN을 갖게 됩니다. 사용자가 인증되면 SDE(Service Delivery Engine)는 해당 테넌트와 관련된 구성 데이터만 읽을 수 있습니다.

물리적 보안

적절한 사전 승인을 받은 경우, 현장 엔지니어와 NetApp 내부 현장 지원 엔지니어(FSE)만 물리적 작업을 위한 케이지 및 랙에 액세스할 수 있습니다. 스토리지 및 네트워크 관리는 허용되지 않습니다. 이러한 현장 리소스만 하드웨어 유지 관리 작업을 수행할 수 있습니다.

현장 엔지니어의 경우 랙 ID 및 장치 위치(RU)가 포함된 SOW(Statement of Work)에 대한 티켓이 발행되고 기타 모든 세부 정보가 티켓에 포함됩니다. NetApp FSE의 경우 COLO를 통해 사이트 방문 티켓을 제기해야 하며 티켓에는 감사 목적을 위한 방문자의 세부 정보, 날짜 및 시간이 포함됩니다. FSE용 SOW는 내부적으로 NetApp에 전달됩니다.

운영팀

Cloud Volumes Service의 운영 팀은 운영 엔지니어링과 SRE(Site Reliability Engineer)로 구성되며, 클라우드 볼륨 서비스를 위한 NetApp 현장 지원 엔지니어 및 파트너는 하드웨어에 대해 구성됩니다. 모든 운영 팀 구성원은 Google Cloud에서 작업할 수 있도록 인증되었으며, 제기된 모든 티켓에 대해 자세한 작업 기록이 유지됩니다. 또한 엄격한 변경 관리 및 승인 프로세스를 통해 각 결정이 적절하게 검토되는지 확인할 수 있습니다.

SRE 팀은 컨트롤 플레인을 관리하고 데이터가 UI 요청에서 백엔드 하드웨어 및 Cloud Volumes Service 소프트웨어로 라우팅되는 방식을 관리합니다. SRE 팀은 또한 볼륨 및 inode 최대값과 같은 시스템 리소스를 관리합니다. SRE는 고객 데이터와 상호 작용하거나 고객 데이터에 액세스할 수 없습니다. 또한 SRE는 백엔드 하드웨어에 대한 새 디스크 또는

메모리 교체 요청과 같은 RMA(Return Material Authorizations)와 함께 조정을 제공합니다.

고객의 책임

Cloud Volumes Service 고객은 조직의 Active Directory 및 사용자 역할 관리와 볼륨 및 데이터 작업을 관리합니다. 고객은 NetApp과 Google Cloud(관리자 및 뷰어)가 제공하는 두 가지 사전 정의된 역할을 사용하여 관리 역할을 수행하고 동일한 Google Cloud 프로젝트 내의 다른 최종 사용자에게 권한을 위임할 수 있습니다.

관리자는 고객 프로젝트 내의 모든 VPC를 고객이 적절하다고 판단한 Cloud Volumes Service에 연결할 수 있습니다. 고객은 Google Cloud Marketplace 구독에 대한 액세스를 관리하고 데이터 평면에 액세스할 수 있는 VPC를 관리해야 합니다.

악성 **SRE** 보호

악성 SRE가 있거나 SRE 자격 증명이 손상된 경우 Cloud Volumes Service가 이를 어떻게 보호합니까?

운영 환경에 대한 액세스는 제한된 수의 SRE 사용자만 가능합니다. 관리 권한은 소수의 숙련된 관리자에게만 더욱 제한됩니다. Cloud Volumes Service 운영 환경의 모든 작업이 기록되고 기준 또는 의심스러운 활동에 대한 모든 이상 사항은 SIEM(Security Information and Event Management) 위협 인텔리전스 플랫폼에서 탐지됩니다. 따라서 Cloud Volumes Service 백엔드에 너무 많은 손상이 발생하기 전에 악의적인 작업을 추적하고 완화할 수 있습니다.

볼륨 수명 주기

Cloud Volumes Service는 볼륨 내의 데이터가 아니라 서비스 내의 객체만 관리합니다. 볼륨에 액세스하는 클라이언트만 데이터, ACL, 파일 소유자 등을 관리할 수 있습니다. 이러한 볼륨의 데이터는 유휴 상태로 암호화되며 액세스는 Cloud Volumes Service 인스턴스 테넌트로 제한됩니다.

Cloud Volumes Service의 볼륨 라이프사이클은 create-update-delete입니다. 볼륨은 볼륨이 삭제될 때까지 볼륨의 스냅샷 복사본을 유지하며, 검증된 Cloud Volumes Service 관리자만 Cloud Volumes Service의 볼륨을 삭제할 수 있습니다. 관리자가 볼륨 삭제를 요청하는 경우 삭제를 확인하려면 볼륨 이름을 추가로 입력해야 합니다. 볼륨이 삭제된 후에는 볼륨이 사라지고 복구할 수 없습니다.

Cloud Volumes Service 계약이 종료된 경우 NetApp은 특정 기간 이후에 삭제할 볼륨을 표시합니다. 이 기간이 만료되기 전에 고객의 요청에 따라 볼륨을 복구할 수 있습니다.

인증

Cloud Volumes Services for Google Cloud는 현재 ISO/IEC 27001:2013 및 ISO/IEC 27018:2019 표준에 따라 인증되었습니다. 또한 이 서비스는 최근 SOC2 Type I Attestation 보고서를 받았습니다. 데이터 보안 및 개인 정보 보호에 대한 NetApp의 약속에 대한 자세한 내용은 을 참조하십시오 "규정 준수: 데이터 보안 및 데이터 개인 정보 보호".

GDPR을 참조하십시오

개인 정보 보호 및 GDPR 준수에 대한 NetApp의 약속은 당사의 다양한 규정으로 제공됩니다 "고객 계약"있습니다 "고객 데이터 처리 부록"를 포함합니다 "표준 계약 조항" 유럽 위원회에서 제공. 또한 NetApp은 개인 정보 보호 정책에 이러한 의무를 이행하며, 이는 기업 행동 강령에 명시된 핵심 가치를 기반으로 합니다.

추가 정보 및 연락처 정보

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

- Cloud Volumes Service용 Google Cloud 설명서

"https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Google 전용 서비스 액세스

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- NetApp 제품 설명서

  "https://www.netapp.com/support-and-training/documentation/"

- 암호화 검증 모듈 프로그램 — NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- 랜섬웨어용 NetApp 솔루션

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616: ONTAP에서 NFS Kerberos

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

문의하기

이 기술 보고서를 개선할 방법을 알려주십시오.

이메일: mailto:doccomments@netapp.com [doccomments@netapp.com^]로 연락해 주십시오. 제목 줄에 기술 보고서 4918 포함.