Cloud Volumes ONTAP 설명서

Cloud Volumes ONTAP

NetApp
February 26, 2026

목차

Cloud Volumes ONTAP 설명서

릴리스 노트

Cloud Volumes ONTAP 의 새로운 기능

NetApp Console 에서 Cloud Volumes ONTAP 관리의 새로운 기능을 알아보세요.

이 페이지에 설명된 개선 사항은 콘솔을 통해 Cloud Volumes ONTAP 관리하는 데 특화되어 있습니다. Cloud Volumes ONTAP 소프트웨어 자체의 새로운 기능을 알아보려면 "Cloud Volumes ONTAP 릴리스 노트로 이동" .

2026년 2월 26일

비공개 모드 배포를 위한 **Google Infrastructure Manager** 지원

Cloud Volumes ONTAP 9.16.1 이상에서는 이제 Google Cloud에서 새로운 프라이빗 모드 배포 시 "Google Cloud Infrastructure Manager" (IM)을 "Cloud Deployment Manager" (DM) 대신 지원합니다. Google은 더 발전된 Infrastructure Manager를 위해 가까운 시일 내에 Deployment Manager를 인프라 서비스에서 지원 중단할 예정입니다.

2026년 2월 25일부터 Cloud Volumes ONTAP는 신규 및 기존 프라이빗 모드 배포에 Infrastructure Manager를 사용합니다. 다음 표에서는 기본 워크플로를 설명합니다.

시나리오	행동	에이전트용 새 **API**	에이전트에 대한 새로운 권한	**Cloud Volumes ONTAP**용 새로운 **Google Cloud API**	문서 리소스
비공개 모드의 기존 에이전트 및 기존 배포	NetApp Support Site에서 설치 프로그램을 다운로드하여 호스트에 수동으로 에이전트를 설치함으로써 NetApp Console 에이전트를 최신 버전으로 업그레이드하십시오. 이렇게 하면 Infrastructure Manager API를 사용할 수 있습니다. 그 후 기존 Cloud Volumes ONTAP 시스템을 Infrastructure Manager를 사용하도록 변환하십시오.	• Cloud Infrastructure Manager API • 클라우드 할당량 API • Cloud Build API	콘솔 릴리스에 대해 나열된 모든 권한: • "2025년 12월 8일" • "2026년 2월 9일" • cloudbuild.workerpools.get • cloudbuild.workerpools.get	• https://cloudbuild.googleapis.com/v1 • https://www.googleapis.com/upload/storage/v1 • https://config.googleapis.com/v1	"기존 Cloud Volumes ONTAP 배포를 Google Cloud Infrastructure Manager에 맞게 구성합니다."
새 에이전트 및 새 배포	새 에이전트를 생성하고 프라이빗 모드로 새 Cloud Volumes ONTAP 시스템을 배포합니다.				• "Google Cloud에서 Console 에이전트를 생성합니다." • "프라이빗 모드 배포를 위한 빠른 시작"

프라이빗 모드 배포에서는 Cloud Volumes ONTAP가 Infrastructure Manager를 사용하기 시작하려면 몇 가지 구성

변경이 필요합니다. "프라이빗 모드 배포를 위한 Infrastructure Manager 구성"을 참조하십시오.

관련 링크

- "NetApp Console Agent 4.2.0 릴리스 노트"
- "Google Cloud Infrastructure Manager에 필요한 권한"

2026년 2월 19일

Azure에서 지원되는 새로운 지역

이제 다음 지역의 Azure에서 단일 및 여러 가용성 영역에 Cloud Volumes ONTAP 9.12.1 GA 이상을 배포할 수 있습니다. 여기에는 단일 노드와 고가용성(HA) 배포에 대한 지원이 포함됩니다.

- Japan West(japanwest)
- Indonesia Central (indonesiacentral)

모든 지역 목록은 다음을 참조하세요. "Azure의 글로벌 지역 맵" .

2026년 2월 17일

차세대 **Google Cloud VM**을 위한 **Cloud Volumes ONTAP** 지원

9.18.1에서 NetApp은 새로운 Cloud Volumes ONTAP 배포를 N2 VM에서 차세대 Google Cloud C3 시리즈 VM으로 전환하여 더욱 빠르고 확장 가능한 환경을 제공합니다. 이제 Google Cloud에서 Cloud Volumes ONTAP 9.18.1 이상 버전을 배포할 때 C3 시리즈 VM의 이점을 활용할 수 있습니다. C3 시리즈 머신은 Google Virtual NIC(gVNIC)와 Hyperdisk Balanced 디스크를 사용하여 향상된 성능과 더 높은 용량 제한을 제공하며, 집약적인 워크로드에 필요한 동적 성능을 보장합니다.

현재 Cloud Volumes ONTAP는 단일 노드 배포 환경에서만 C3 시리즈를 지원합니다.

Cloud Volumes ONTAP 시스템이 9.18.1 이상을 실행하는 경우 간편한 단일 노드 배포에 사용하는 사전 구성된 패키지는 자동으로 C3 VM을 사용하며 워크로드 요구 사항에 따라 IOPS 및 처리량 매개 변수를 사용자 지정할 수 있습니다. 마찬가지로 애그리게이트를 생성하는 동안 Hyperdisk Balanced 디스크를 추가하여 Google Cloud에서 더 나은 성능과 확장성을 달성할 수 있습니다. 또한 기본 Flash Cache 지원을 위해 C3 시리즈 머신의 LSSD 변형을 선택할 수 있습니다.

C3 VM은 Hyperdisk Balanced 디스크만 지원하기 때문에 애그리게이트에 볼륨을 추가할 때 디스크 유형을 변경할 수 없습니다. 마찬가지로 N2 VM 유형의 시스템을 C3 VM으로 복제할 때 디스크 유형은 기본적으로 Hyperdisk Balanced로 설정됩니다.

"Google Cloud에서 Cloud Volumes ONTAP에 대해 지원되는 구성"

"Google 문서: C3 머신 시리즈"

Azure의 **Cloud Volumes ONTAP**용 **VNet** 보안

Azure 단일 및 다중 가용성 영역에 배포된 Cloud Volumes ONTAP 9.18.1 이상 버전은 전송 중인 데이터를 보호하기 위한 계층형 보안 전략의 일환으로 Azure 가상 네트워크(VNet) 암호화를 지원합니다. Cloud Volumes ONTAP는 Azure의 기본 데이터그램 전송 계층 보안(DTLS) 프로토콜을 활용하여 ONTAP 노드, 관리 인터페이스 및 기타 Azure 서비스 간의 통신을 보호하고, 데이터 가로채기 및 무단 액세스를 방지합니다. 이러한 네트워크 수준 암호화는

ONTAP에 내장된 스토리지 및 저장 데이터 보호 기능을 보완하여 데이터에 대한 엔드 투 엔드 보안을 제공합니다.

"Azure VNet 암호화를 위한 네트워킹"

2026년 2월 12일

Azure에서 **Ebdsv5** 및 **E104ids_v5 VM** 지원

Cloud Volumes ONTAP 9.18.1부터 단일 노드 및 고가용성(HA) 배포 및 업그레이드를 위해 Ebdsv5 및 E104ids_v5 VM을 배포할 수 있습니다.

Azure 가상 머신 Eb 제품군의 Ebdsv5 VM은 더 높은 원격 스토리지 성능에 최적화되어 있습니다. 이러한 VM은 관계형 데이터베이스, 인메모리 분석 및 기타 까다로운 비즈니스 크리티컬 애플리케이션과 같이 메모리 집약적이고 I/O 작업이 많은 엔터프라이즈 워크로드에 사용할 수 있습니다.

E104ids_v5는 예약된 유지 관리 기간을 효율적으로 관리할 수 있도록 설계된 격리된 VM 인스턴스입니다. E80ids_v4와 비교했을 때 디스크 처리량과 IOPS가 훨씬 높으며, 전반적인 네트워크 성능 또한 향상되었습니다.

"Azure의 Cloud Volumes ONTAP 에 지원되는 구성"

"Azure 설명서: Edsv5 크기 시리즈"

2026년 2월 10일

Cloud Volumes ONTAP 9.18.1 GA

이제 NetApp Console을 사용하여 AWS, Azure 및 Google Cloud에서 Cloud Volumes ONTAP 9.18.1의 일반 출시(GA) 버전을 배포하고 관리할 수 있습니다.

"Cloud Volumes ONTAP 의 이 릴리스에 대해 자세히 알아보세요." .

2026년 2월 9일

Google Cloud Infrastructure Manager 지원

Cloud Volumes ONTAP 9.16.1 이상에서는 Google Cloud의 새 배포에 대해 "Cloud Deployment Manager" (DM) 대신 "Google Cloud Infrastructure Manager" (IM)을 지원합니다. Google은 더 고급 Infrastructure Manager를 위해 가까운 미래에 인프라 서비스로서 Deployment Manager를 더 이상 사용하지 않을 예정입니다.

2026년 2월 9일부터 Cloud Volumes ONTAP는 신규 및 기존 배포에 Infrastructure Manager를 사용합니다. 다음 표에서 몇 가지 워크플로를 설명합니다.

시나리오	행동	에이전트용 새 **API**	에이전트에 대한 새로운 권한	**Cloud Volumes ONTAP**용 새로운 **Google Cloud API**	문서 리소스
기존 에이전트 및 기존 Cloud Volumes ONTAP 배포	기존 에이전트에 새로운 API와 권한을 추가하고 기존 Cloud Volumes ONTAP 시스템을 변환합니다.	• Cloud Infrastructure Manager API • 클라우드 할당량 API	콘솔 릴리스에 대해 나열된 모든 권한: • "2025년 12월 8일" • "2026년 2월 9일"	https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1	"기존 Cloud Volumes ONTAP 배포를 Google Cloud Infrastructure Manager에 맞게 구성합니다."
기존 에이전트 및 새 Cloud Volumes ONTAP 배포	기존 에이전트에 새로운 API와 권한을 추가하고 새로운 Cloud Volumes ONTAP 시스템을 배포합니다.	• Cloud Infrastructure Manager API • 클라우드 할당량 API	콘솔 릴리스에 대해 나열된 모든 권한: • "2025년 12월 8일" • "2026년 2월 9일"	새로운 배포를 위한 모든 단계	"Google Cloud에서 Cloud Volumes ONTAP 시작하기"

시나리오	행동	에이전트용 새 **API**	에이전트에 대한 새로운 권한	**Cloud Volumes ONTAP**용 새로운 **Google Cloud API**	문서 리소스
새 에이전트 및 새 배포	새 에이전트를 생성하고 새 Cloud Volumes ONTAP 시스템을 구축합니다.				• "Google Cloud에서 Console 에이전트를 생성합니다." • "Google Cloud에서 Cloud Volumes ONTAP 시작하기"

이제 Cloud Volumes ONTAP을 배포하여 Infrastructure Manager를 자동으로 사용하거나 변환 도구를 실행하여 Deployment Manager의 기존 배포를 Infrastructure Manager로 전환하십시오. 변환은 일회성 프로세스이며, 변환 후 시스템에서 Infrastructure Manager를 사용하기 시작합니다. 변환 도구 실행에 대한 지침은 "기존 Cloud Volumes ONTAP 배포를 Google Cloud Infrastructure Manager에 맞게 구성합니다."을 참조하십시오.

Infrastructure Manager를 사용하는 Cloud Volumes ONTAP 시스템은 Google Cloud Storage 버킷을 사용하여 데이터를 저장하고 첫 번째 배포 영역에 배포 레코드를 저장하며, 이는 후속 배포에 재사용됩니다. 이러한 버킷에 대해 추가 비용이 발생할 수 있지만 버킷이나 해당 콘텐츠를 편집하거나 삭제하지 마십시오.

- `gs://netapp-cvo-infrastructure-manager-<project id>`: 새로운 Cloud Volumes ONTAP 배포에 사용되는 ONTAP 버전 및 SVM Terraform 템플릿용입니다. 이 안에 `dm-to-im-convert` 버킷에는 Cloud Volumes ONTAP Terraform 파일이 들어 있습니다.
- `<gcp project number>-<region>-blueprint-config`: Google Cloud Terraform 아티팩트를 저장하는 데 사용됩니다.

관련 링크

- "Google Cloud에서 Cloud Volumes ONTAP 시작하기"
- "NetApp Console Agent 4.2.0 릴리스 노트"
- "Google Cloud Infrastructure Manager에 필요한 권한"

2026년 1월 12일

Cloud Volumes ONTAP 에 선호하는 결제 옵션

이제 Cloud Volumes ONTAP 사용량 및 초과 사용량 계산에 사용할 원하는 청구 옵션을 선택할 수 있습니다. 2025년 6월 25일부터 BYOL(Bring Your Own Licenses) 라이선스 모델의 사용이 제한됨에 따라 NetApp NetApp Console 의 라이선스 및 구독 섹션에 선호하는 요금 청구 방식을 추가했습니다. 청구 및 초과 사용량 처리에는 연간 마켓플레이스 구독을 사용하거나 기존의 BYOL 모델을 사용하는 것이 좋습니다. BYOL 모델을 선호하는 옵션으로 선택할 수 있습니다. 이를 통해 조직의 재정 전략 및 사용 패턴에 가장 적합한 요금 청구 방식을 유연하게 선택할 수 있습니다.

"요금 설정 및 초과 사용 요금".

2025년 12월 10일

Azure에서 **Premium SSD v2** 디스크의 성능을 향상시킬 수 있는 기능

이제 Azure에서 Premium SSD v2 관리형 디스크의 성능을 IOPS 및 처리량 매개변수를 수정하여 향상시킬 수 있습니다. 이 기능을 사용하면 워크로드 요구 사항에 따라 시스템의 스토리지 성능을 최적화할 수 있습니다.

"Azure Cloud Volumes ONTAP 에서 Premium SSD v2 디스크 성능을 관리하세요.".

Essentials 라이선스 초과 사용 요금 청구 방식 간소화

Cloud Volumes ONTAP 마켓플레이스 연간 계약/프라이빗 오퍼의 경우, Essentials 라이선스 초과 사용량 계산 방식이 이제 BYOL(Bring Your Own License) 패키지와 동일하게 적용됩니다. 이전에는 초과 사용량에 대해 동일한 Essentials 패키지에 대한 시간당 시장 요율로 청구되었습니다. 만약 마켓플레이스 연간 계약에 여러 Essentials 패키지가 포함되어 있다면, NetApp Console 구독에 포함된 더 비싼 Essentials 패키지의 사용 가능한 용량을 기준으로 해당 Essentials 패키지의 초과 사용량을 청구합니다. 이를 통해 Essentials 패키지의 초과 사용량 계산이 간소화되고 BYOL 라이선스에서 구독 기반 모델로의 원활한 전환이 보장됩니다.

"Essentials 라이선스 초과 사용 요금 부과 방식"

Azure Edsv6 크기 시리즈 지원

Cloud Volumes ONTAP 9.17.1 버전부터 NetApp Console 통해 새로운 Cloud Volumes ONTAP 인스턴스에 Azure Edsv6 시리즈 VM을 배포할 수 있습니다. Cloud Volumes ONTAP 9.17.1 이상 버전에서는 신규 배포 시 2세대 VM만 지원합니다. 이러한 2세대 장비는 UEFI(Unified Extensible Firmware Interface), Azure Boost 시스템 및 NVMe와 같은 최신 기술과 호환됩니다. 이러한 스토리지 시스템은 데이터베이스 서버 및 분석 엔진과 같이 빠른 로컬 스토리지가 필요한 메모리 집약적인 시스템 및 애플리케이션에 이상적입니다.

"Azure의 Cloud Volumes ONTAP 에 지원되는 구성"

2025년 11월 10일

향상된 **NVMe-TCP** 지원

이전에는 NVMe-TCP를 통해 Cloud Volumes ONTAP 인스턴스를 배포할 때 배포 전에 NVMe 라이선스를 수동으로 획득하고 적용해야 했습니다. 이 업데이트를 통해 Cloud Volumes ONTAP 이제 배포 중에 필요한 NVMe 라이선스를 자동으로 설치하여 설정 프로세스를 간소화합니다.

라이선스가 없는 기존 NVMe-TCP 배포의 경우 Cloud Volumes ONTAP 라이선스를 자동으로 적용합니다. 라이센스를 적용하려면 시스템을 다시 시작해야 합니다.

자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 에 지원되는 클라이언트 프로토콜: NVMe-TCP" .

2025년 10월 17일

Azure의 Cloud Volumes ONTAP 이제 최신 지원 버전으로 제한됩니다**.**

NetApp Console 통한 Azure의 Cloud Volumes ONTAP 배포 및 업그레이드는 이제 최신 지원 버전으로 제한됩니다. 이를 통해 Microsoft에서 지원하는 최신 세대 하드웨어와의 호환성이 보장되고 최신 기능과 보안 강화 기능이 제공됩니다. 콘솔에서 지원되는 버전으로 업그레이드하라는 메시지가 표시됩니다.

자세한 내용은 다음을 참조하세요.

- 전개: "Cloud Volumes ONTAP 배포에 지원되는 ONTAP 버전"
- 치받이: "Azure에 지원되는 업그레이드 경로"

2025년 10월 6일

BlueXP 는 이제 **NetApp Console** 입니다**.**

강화되고 재구성된 BlueXP 기반을 기반으로 구축된 NetApp Console 엔터프라이즈급 온프레미스 및 클라우드 환경에서 NetApp 스토리지와 NetApp Data Services 중앙에서 관리하여 실시간 통찰력, 더 빠른 워크플로, 간소화된 관리를 제공하며, 높은 보안성과 규정 준수를 보장합니다.

변경된 사항에 대한 자세한 내용은 다음을 참조하세요. "NetApp Console 릴리스 노트" .

AWS에서 간소화된 **Cloud Volumes ONTAP** 배포

이제 단일 노드 및 고가용성(HA) 구성 모두에 대한 빠른 배포 방법을 사용하여 AWS에 Cloud Volumes ONTAP 배포할 수 있습니다. 이 간소화된 프로세스는 고급 방법에 비해 단계 수를 줄이고, 단일 페이지에 기본값을 자동으로 설정하고, 탐색을 최소화하여 배포를 더 빠르고 쉽게 만듭니다.

자세한 내용은 다음을 참조하세요. "빠른 배포를 사용하여 AWS에 Cloud Volumes ONTAP 배포" .

2025년 9월 4일

Cloud Volumes ONTAP 9.17.1 RC

이제 BlueXP 사용하여 Azure 및 Google Cloud에서 Cloud Volumes ONTAP 9.17.1 릴리스 후보 1을 배포하고 관리할 수 있습니다. 하지만 이 버전은 AWS에 배포하고 업그레이드할 수 없습니다.

"Cloud Volumes ONTAP 의 이 릴리스에 대해 자세히 알아보세요.".

2025년 8월 11일

최적화된 라이선스의 사용 가능 기간이 종료되었습니다**.**

2025년 8월 11일부터 Cloud Volumes ONTAP Optimized 라이선스는 더 이상 사용되지 않으며 Azure 및 Google Cloud 마켓플레이스에서 PAYGO(종량제) 구독을 구매하거나 갱신할 수 없습니다. 최적화된 라이선스에 대한 기존 연간 계약이 있는 경우, 계약 기간이 끝날 때까지 라이선스를 계속 사용할 수 있습니다. 최적화된 라이선스가 만료되면 BlueXP 에서 Cloud Volumes ONTAP Essentials 또는 Professional 라이선스를 선택할 수 있습니다.

하지만 최적화된 라이선스를 추가하거나 갱신하는 기능은 API를 통해 제공될 예정입니다.

라이센스 패키지에 대한 정보는 다음을 참조하세요. "Cloud Volumes ONTAP 라이선싱" .

다른 충전 방법으로 전환하는 방법에 대한 정보는 다음을 참조하세요. "용량 기반 라이선싱 관리" .

2025년 7월 14일

투명 프록시 지원

BlueXP 이제 기존의 명시적 프록시 연결 외에도 투명 프록시 서버를 지원합니다. BlueXP 커넥터를 만들거나 수정할 때 투명 프록시 서버를 구성하여 Cloud Volumes ONTAP 과의 네트워크 트래픽을 안전하게 관리할 수 있습니다.

Cloud Volumes ONTAP 에서 프록시 서버를 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요.

- "AWS에서 커넥터 프록시를 지원하는 네트워크 구성"
- "Azure에서 커넥터 프록시를 지원하는 네트워크 구성"
- "Google Cloud에서 커넥터 프록시를 지원하는 네트워크 구성"

Azure의 **Cloud Volumes ONTAP** 에 대해 지원되는 새로운 **VM** 유형

Cloud Volumes ONTAP 9.13.1부터 L8s_v3는 새 고가용성(HA) 쌍 배포와 기존 고가용성(HA) 쌍 배포 모두에 대해 Azure 단일 및 다중 가용성 영역에서 VM 유형으로 지원됩니다.

자세한 내용은 다음을 참조하세요. "Azure에서 지원되는 구성" .

2025년 6월 25일

Cloud Volumes ONTAP 에 대한 **BYOL** 라이선싱의 제한된 가용성

2025년 6월 25일부터 NetApp Cloud Volumes ONTAP 의 BYOL(Bring Your Own License) 라이선스 모델을 제한했습니다. 이 제한은 AWS, Azure, Google Cloud의 모든 고객 및 Cloud Volumes ONTAP 배포에 적용됩니다. 미국 공공 부문 고객과 중국 리전 배포는 예외입니다.

NetApp 지원 및 서비스는 BYOL 계약이 만료될 때까지 계속되지만, 만료된 라이선스는 갱신 또는 연장되지 않습니다. BYOL 라이선스가 만료되면 클라우드 마켓플레이스 구독을 통해 구매한 용량 기반 라이선스로 교체해야 합니다. 하이퍼스케일러 마켓플레이스를 통한 용량 기반 라이선스 모델은 라이선스 경험을 간소화하고 더 큰 비즈니스 이점을 제공합니다. 전환 옵션에 대해 논의하려면 NetApp 계정 팀 또는 고객 성공 담당자에게 문의하십시오.

자세한 내용은 다음 고객 공지문을 참조하세요. "CPC-00661: Cloud Volumes ONTAP BYOL 정책 변경" .

2025년 5월 29일

Cloud Volumes ONTAP 9.15.1에 대해 개인 모드 배포가 활성화되었습니다**.**

이제 AWS, Azure, Google Cloud에서 Cloud Volumes ONTAP 9.15.1을 프라이빗 모드로 배포할 수 있습니다. Cloud Volumes ONTAP 9.15.1의 단일 노드 및 고가용성(HA) 배포 모두에 대해 개인 모드가 활성화됩니다.

개인 모드 배포에 대한 자세한 내용은 다음을 참조하세요.https://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode["BlueXP 배포 모드에 대해 알아보세요"^] .

2025년 5월 12일

BlueXP 에서 **Azure Marketplace**를 통해 이루어진 배포 검색

이제 BlueXP Azure 마켓플레이스를 통해 직접 배포된 Cloud Volumes ONTAP 시스템을 검색할 수 있는 기능을 갖추게 되었습니다. 즉, 다른 Cloud Volumes ONTAP 시스템과 마찬가지로 이제 BlueXP 에서 이러한 시스템을 작업 환경으로 추가하고 관리할 수 있습니다.

"Azure Marketplace에서 Cloud Volumes ONTAP 배포"

2025년 4월 16일

Azure에서 지원되는 새로운 지역

이제 다음 지역의 Azure에서 단일 및 여러 가용성 영역에 Cloud Volumes ONTAP 9.12.1 GA 이상을 배포할 수 있습니다. 여기에는 단일 노드와 고가용성(HA) 배포에 대한 지원이 포함됩니다.

- 스페인 중부
- 멕시코 중부

모든 지역 목록은 다음을 참조하세요. "Azure의 글로벌 지역 맵" .

2025년 4월 14일

Google Cloud의 **API**를 통해 자동화된 스토리지 **VM** 생성

이제 BlueXP API를 사용하여 Google Cloud에서 스토리지 VM 생성을 자동화할 수 있습니다. 이 기능은 Cloud Volumes ONTAP 고가용성(HA) 구성에서 사용되었으며, 이제 단일 노드 배포에서도 사용할 수 있습니다. BlueXP API를 사용하면 필요한 네트워크 인터페이스, LIF 및 관리 LIF를 수동으로 구성할 필요 없이 Google Cloud 환경에서 추가 데이터 제공 스토리지 VM을 쉽게 만들고, 이름을 바꾸고, 삭제할 수 있습니다. 이러한 자동화를 통해 스토리지 VM을 관리하는 프로세스가 간소화됩니다.

"Google Cloud에서 Cloud Volumes ONTAP 위한 데이터 제공 스토리지 VM 관리"

2025년 4월 3일

AWS의 **Cloud Volumes ONTAP 9.13.1**에 대한 중국 지역 지원

이제 중국 지역의 AWS에 Cloud Volumes ONTAP 9.13.1을 배포할 수 있습니다. 여기에는 단일 노드와 고가용성(HA) 배포에 대한 지원이 포함됩니다. NetApp 에서 직접 구매한 라이선스만 지원됩니다.

지역별 가용성은 다음을 참조하세요. "Cloud Volumes ONTAP 위한 글로벌 지역 맵" .

2025년 3월 28일

Cloud Volumes ONTAP 9.14.1에 대해 개인 모드 배포가 활성화되었습니다**.**

이제 AWS, Azure, Google Cloud에서 Cloud Volumes ONTAP 9.14.1을 프라이빗 모드로 배포할 수 있습니다. Cloud Volumes ONTAP 9.14.1의 단일 노드 및 고가용성(HA) 배포 모두에 대해 개인 모드가 활성화됩니다.

개인 모드 배포에 대한 자세한 내용은 다음을 참조하세요.https://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode["BlueXP 배포 모드에 대해 알아보세요"^] .

2025년 3월 12일

Azure에서 여러 가용성 영역 배포를 지원하는 새로운 지역

다음 지역은 이제 Cloud Volumes ONTAP 9.12.1 GA 이상에 대해 Azure에서 HA 다중 가용성 영역 배포를 지원합니다.

- 미국 중부
- 미국 정부 버지니아(미국 정부 지역 - 버지니아)

모든 지역 목록은 다음을 참조하세요. "Azure의 글로벌 지역 맵" .

2025년 3월 10일

Azure의 **API**를 통해 스토리지 **VM** 생성 자동화

이제 BlueXP API를 사용하여 Azure에서 Cloud Volumes ONTAP 에 대한 추가 데이터 제공 스토리지 VM을 만들고, 이름을 바꾸고, 삭제할 수 있습니다. API를 사용하면 필요한 네트워크 인터페이스, LIF, 관리 LIF 구성을 포함하여 스토리지 VM 생성 프로세스가 자동화됩니다(관리 목적으로 스토리지 VM을 사용해야 하는 경우).

"Azure에서 Cloud Volumes ONTAP 대한 데이터 제공 스토리지 VM 관리"

2025년 3월 6일

Cloud Volumes ONTAP 9.16.1 GA

이제 BlueXP 사용하여 Azure와 Google Cloud에서 Cloud Volumes ONTAP 9.16.1 일반 공급 릴리스를 배포하고 관리할 수 있습니다. 하지만 이 버전은 AWS에 배포하고 업그레이드할 수 없습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

2025년 3월 3일

Azure에서 뉴질랜드 북부 지역 지원

뉴질랜드 북부 지역은 이제 Azure에서 Cloud Volumes ONTAP 9.12.1 GA 이상의 단일 노드 및 고가용성(HA) 구성이 지원됩니다. 이 지역에서는 Lsv3 인스턴스 유형이 지원되지 않습니다.

지원되는 모든 지역 목록은 다음을 참조하세요. "Azure의 글로벌 지역 맵" .

2025년 2월 18일

Azure Marketplace 직접 배포 소개

이제 Azure 마켓플레이스 직접 배포를 활용하여 Azure 마켓플레이스에서 직접 Cloud Volumes ONTAP 쉽고 빠르게 배포할 수 있습니다. 이 간소화된 방법을 사용하면 BlueXP 커넥터를 설정하거나 BlueXP 통해 Cloud Volumes ONTAP 배포하는 데 필요한 다른 온보딩 기준을 충족하지 않고도 사용자 환경에서 Cloud Volumes ONTAP 의 핵심

기능과 성능을 살펴볼 수 있습니다.

- "Azure에서 Cloud Volumes ONTAP 배포 옵션에 대해 알아보세요."
- "Azure Marketplace에서 Cloud Volumes ONTAP 배포"

2025년 2월 10일

BlueXP 에서 **System Manager**에 액세스하기 위해 사용자 인증이 활성화되었습니다**.**

BlueXP 관리자는 이제 BlueXP 에서 ONTAP System Manager에 액세스하는 ONTAP 사용자에 대한 인증을 활성화할 수 있습니다. BlueXP Connector 설정을 편집하면 이 옵션을 활성화할 수 있습니다. 이 옵션은 표준 모드와 개인 모드에서 사용할 수 있습니다.

"System Manager를 사용하여 Cloud Volumes ONTAP 관리" .

BlueXP Advanced View가 **System Manager**로 이름이 변경되었습니다**.**

ONTAP System Manager를 통한 BlueXP 의 Cloud Volumes ONTAP 고급 관리 옵션의 이름이 *고급 보기*에서 *시스템 관리자*로 변경되었습니다.

"System Manager를 사용하여 Cloud Volumes ONTAP 관리" .

BlueXP digital wallet 사용하여 라이선스를 관리하는 더 간단한 방법을 소개합니다**.**

이제 BlueXP digital wallet 내의 개선된 탐색 포인트를 사용하여 Cloud Volumes ONTAP 라이선스를 더욱 간편하게 관리할 수 있습니다.

- 관리 **> Licenses and subscriptions >** 개요/직접 라이선스 탭을 통해 Cloud Volumes ONTAP 라이선스 정보에 쉽게 액세스할 수 있습니다.
- 개요 탭의 Cloud Volume ONTAP 패널에서 *보기*를 클릭하면 용량 기반 라이선스에 대한 포괄적인 정보를 얻을 수 있습니다. 이 고급 보기는 라이선스와 구독에 대한 자세한 정보를 제공합니다.
- 이전 인터페이스를 선호하는 경우 레거시 보기로 전환 버튼을 클릭하면 라이선스 유형별 세부 정보를 보고 라이선스에 대한 청구 방법을 수정할 수 있습니다.

"용량 기반 라이선스 관리" .

2024년 12월 9일

Azure에서 지원되는 **VM** 목록이 모범 사례에 맞춰 업데이트되었습니다**.**

Azure에서 Cloud Volumes ONTAP 의 새 인스턴스를 배포할 때 BlueXP 에서 DS_v2 및 Es_v3 머신 제품군을 더 이상 선택할 수 없습니다. 이러한 가족은 기존의 오래된 시스템에서만 유지되고 지원됩니다. Cloud Volumes ONTAP 의 새로운 배포는 Azure 9.12.1 릴리스부터 지원됩니다. Cloud Volumes ONTAP 9.12.1 이상과 호환되는 Es_v4 또는 다른 시리즈로 전환하는 것이 좋습니다. 하지만 DS_v2 및 Es_v3 시리즈 머신은 API를 통해 이루어진 새로운 배포에 사용할 수 있습니다.

"Azure에서 지원되는 구성"

2024년 11월 11일

노드 기반 라이선스의 가용성 종료

NetApp Cloud Volumes ONTAP 노드 기반 라이선싱의 가용성 종료(EOA) 및 지원 종료(EOS)를 계획했습니다. 2024년 11월 11일부터 노드 기반 라이선스의 제한된 제공이 종료되었습니다. 노드 기반 라이선싱에 대한 지원은 2024년 12월 31일에 종료됩니다. 노드 기반 라이선스의 EOA가 만료된 후에는 BlueXP 라이선스 변환 도구를 사용하여 용량 기반 라이선스로 전환해야 합니다.

연간 또는 장기 약정의 경우 NetApp EOA 날짜 또는 라이선스 만료일 전에 NetApp 담당자에게 연락하여 전환에 필요한 전제 조건이 충족되었는지 확인할 것을 권장합니다. Cloud Volumes ONTAP 노드에 대한 장기 계약이 없고 온디맨드 PAYGO(Pay-as-you-go) 구독으로 시스템을 실행하는 경우 EOS 날짜 전에 전환을 계획하는 것이 중요합니다. 장기 계약과 PAYGO 구독 모두 BlueXP 라이선스 변환 도구를 사용하여 원활하게 변환할 수 있습니다.

"노드 기반 라이선스 제공 종료" "Cloud Volumes ONTAP 노드 기반 라이선스를 용량 기반 라이선스로 변환"

BlueXP 에서 노드 기반 배포 제거

BlueXP 에서는 노드 기반 라이선스를 사용하여 Cloud Volumes ONTAP 시스템을 배포하는 옵션이 더 이상 제공되지 않습니다. 몇 가지 특별한 경우를 제외하고, 어떤 클라우드 공급자의 Cloud Volumes ONTAP 배포에도 노드 기반 라이선스를 사용할 수 없습니다.

NetApp 계약 의무와 운영상의 필요 사항을 준수하기 위해 다음과 같은 고유한 라이선스 요구 사항을 인식하고 있으며, 이러한 상황에서 노드 기반 라이선스를 계속 지원할 것입니다.

- 미국 공공 부문 고객
- 개인 모드 배포
- AWS에서 Cloud Volumes ONTAP 의 중국 지역 배포
- 유효하고 만료되지 않은 노드별 BYOL 라이선스가 있는 경우

"노드 기반 라이선스 제공 종료"

Azure Blob 스토리지에 **Cloud Volumes ONTAP** 데이터를 위한 콜드 계층 추가

이제 BlueXP 사용하면 Azure Blob 저장소에 비활성 용량 계층 데이터를 저장할 콜드 계층을 선택할 수 있습니다. 기존의 따뜻하고 차가운 계층에 차가운 계층을 추가하면 보관 옵션을 더 저렴하게 제공하고 비용 효율성을 개선할 수 있습니다.

"Azure의 데이터 계층화"

Azure의 저장소 계정에 대한 공개 액세스를 제한하는 옵션

이제 Azure에서 Cloud Volumes ONTAP 시스템의 스토리지 계정에 대한 공개 액세스를 제한하는 옵션이 제공됩니다. 액세스를 비활성화하면 조직의 보안 정책을 준수해야 할 필요가 있는 경우 동일한 VNet 내에서도 개인 IP 주소가 노출되지 않도록 보호할 수 있습니다. 이 옵션은 Cloud Volumes ONTAP 시스템의 데이터 계층화를 비활성화하며, 단일 노드와 고가용성 쌍 모두에 적용할 수 있습니다.

"보안 그룹 규칙" .

Cloud Volumes ONTAP 배포 후 **WORM** 활성화

이제 BlueXP 사용하여 기존 Cloud Volumes ONTAP 시스템에서 WORM(Write Once, Read Many) 스토리지를 활성화할 수 있습니다. 이 기능을 사용하면 작업 환경을 생성할 때 WORM이 활성화되지 않았더라도 작업 환경에서 WORM을 활성화할 수 있는 유연성을 제공합니다. WORM을 활성화하면 비활성화할 수 없습니다.

"Cloud Volumes ONTAP 작업 환경에서 WORM 활성화"

2024년 10월 25일

Google Cloud에서 지원되는 **VM** 목록이 모범 사례에 맞춰 업데이트되었습니다**.**

Google Cloud에서 Cloud Volumes ONTAP 의 새로운 인스턴스를 배포할 때 BlueXP 에서 n1 시리즈 머신을 더 이상 선택할 수 없습니다. n1 시리즈 머신은 기존의 오래된 시스템에서만 유지 및 지원됩니다. Cloud Volumes ONTAP 의 새로운 배포는 Google Cloud 9.8 릴리스부터만 지원됩니다. Cloud Volumes ONTAP 9.8 이상과 호환되는 n2 시리즈 머신 유형으로 전환하는 것이 좋습니다. 하지만 n1 시리즈 머신은 API를 통해 수행되는 새로운 배포에 사용할 수 있습니다.

"Google Cloud에서 지원되는 구성" .

Amazon Web Services의 개인 모드에 대한 로컬 영역 지원

BlueXP 이제 프라이빗 모드에서 Cloud Volumes ONTAP 고가용성(HA) 배포를 위한 AWS 로컬 영역을 지원합니다. 이전에는 표준 모드로만 제한되었던 지원이 이제 개인 모드까지 포함하도록 확장되었습니다.

제한 모드에서 BlueXP 사용하는 경우 AWS 로컬 영역은 지원되지 않습니다.

HA 배포를 통한 AWS 로컬 영역에 대한 자세한 내용은 다음을 참조하세요."AWS 로컬 영역" .

2024년 10월 7일

업그레이드를 위한 버전 선택에서 향상된 사용자 경험

이 릴리스부터 BlueXP 알림을 사용하여 Cloud Volumes ONTAP 업그레이드하려고 하면 사용할 기본, 최신 및 호환 버전에 대한 안내를 받게 됩니다. 또한, 이제 Cloud Volumes ONTAP 인스턴스와 호환되는 최신 패치나 주요 버전을 선택하거나 업그레이드할 버전을 수동으로 입력할 수 있습니다.

"Cloud Volumes ONTAP 소프트웨어 업그레이드"

2024년 9월 9일

WORM 및 **ARP** 기능은 더 이상 유료화되지 않습니다**.**

WORM(Write Once Read Many) 및 ARP(Autonomous Ransomware Protection)의 내장된 데이터 보호 및 보안 기능은 추가 비용 없이 Cloud Volumes ONTAP 라이선스와 함께 제공됩니다. 새로운 가격 모델은 AWS, Azure, Google Cloud의 새 BYOL 및 PAYGO/마켓플레이스 구독과 기존 구독 모두에 적용됩니다. 용량 기반 라이선스와 노드 기반 라이선스 모두 단일 노드와 고가용성(HA) 쌍을 포함한 모든 구성에 대한 ARP와 WORM을 추가 비용 없이 포함합니다.

간소화된 가격 책정으로 다음과 같은 혜택을 누리실 수 있습니다.

- 현재 WORM 및 ARP가 포함된 계정에는 이러한 기능에 대한 요금이 더 이상 부과되지 않습니다. 앞으로는 이 변경 전과 마찬가지로 용량 사용에 대해서만 요금이 청구됩니다. WORM과 ARP는 더 이상 향후 청구서에 포함되지 않습니다.
- 현재 계정에 이러한 기능이 포함되어 있지 않은 경우 이제 추가 비용 없이 WORM 및 ARP를 선택할 수 있습니다.
- 모든 신규 계정에 대한 Cloud Volumes ONTAP 서비스에는 WORM 및 ARP 비용이 포함되지 않습니다.

이러한 기능에 대해 자세히 알아보세요.

- "Cloud Volumes ONTAP 에 NetApp 랜섬웨어 보호 솔루션 활성화"
- "WORM 스토리지"

2024년 8월 23일

캐나다 서부 지역이 이제 **AWS**에서 지원됩니다**.**

캐나다 서부 지역은 이제 AWS의 Cloud Volumes ONTAP 9.12.1 GA 이상에서 지원됩니다.

모든 지역 목록을 보려면 다음을 참조하세요. "AWS의 글로벌 지역 맵" .

2024년 8월 22일

Cloud Volumes ONTAP 9.15.1 GA

이제 BlueXP AWS, Azure 및 Google Cloud에서 Cloud Volumes ONTAP 9.15.1 일반 공급 릴리스를 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

2024년 8월 8일

Edge Cache 라이선싱 패키지가 더 이상 사용되지 않습니다**.**

Edge Cache 용량 기반 라이선싱 패키지는 향후 Cloud Volumes ONTAP 배포에 더 이상 제공되지 않습니다. 하지만 API를 사용하면 이 기능을 활용할 수 있습니다.

Azure의 **Flash Cache**에 대한 최소 버전 지원

Azure에서 Flash Cache를 구성하는 데 필요한 최소 Cloud Volumes ONTAP 버전은 9.13.1 GA입니다. Azure의 Cloud Volumes ONTAP 시스템에 Flash Cache를 배포하려면 ONTAP 9.13.1 GA 이상 버전만 사용할 수 있습니다.

지원되는 구성은 다음을 참조하세요. "Azure에서 지원되는 구성" .

마켓플레이스 구독에 대한 무료 평가판이 더 이상 제공되지 않습니다**.**

클라우드 공급업체 마켓플레이스의 사용량 기반 구독에 대한 30일 자동 무료 평가판 또는 평가 라이선스는 더 이상 Cloud Volumes ONTAP 에서 제공되지 않습니다. 모든 유형의 마켓플레이스 구독(PAYGO 또는 연간 계약)에 대한 요금은 무료 체험 기간 없이 처음 사용하는 순간부터 부과됩니다.

2024년 6월 10일

Cloud Volumes ONTAP 9.15.0

이제 BlueXP AWS, Azure, Google Cloud에서 Cloud Volumes ONTAP 9.15.0을 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

2024년 5월 17일

Amazon Web Services 로컬 영역 지원

이제 Cloud Volumes ONTAP HA 배포에 AWS 로컬 영역에 대한 지원이 제공됩니다. AWS 로컬 존은 스토리지, 컴퓨팅, 데이터베이스 및 기타 선택된 AWS 서비스가 대도시와 산업 지역 근처에 위치하는 인프라 배포입니다.

BlueXP 표준 모드로 사용하면 AWS 로컬 영역이 지원됩니다. 현재 제한 모드나 비공개 모드에서 BlueXP 사용하는 경우 AWS 로컬 영역은 지원되지 않습니다.

HA 배포를 통한 AWS 로컬 영역에 대한 자세한 내용은 다음을 참조하세요. "AWS 로컬 영역" .

2024년 4월 23일

Azure에서 여러 가용성 영역 배포를 지원하는 새로운 지역

다음 지역은 이제 Cloud Volumes ONTAP 9.12.1 GA 이상에 대해 Azure에서 HA 다중 가용성 영역 배포를 지원합니다.

- 독일 중서부
- 폴란드 중부
- 서부 미국 3
- 이스라엘 중앙
- 이탈리아 북부
- 캐나다 중부

모든 지역 목록은 다음을 참조하세요. "Azure의 글로벌 지역 맵" .

요하네스버그 지역이 이제 Google Cloud에서 지원됩니다.

요하네스버그 지역(`africa-south1` 지역)은 이제 Google Cloud for Cloud Volumes ONTAP 9.12.1 GA 이상에서 지원됩니다.

모든 지역 목록은 다음을 참조하세요. "Google Cloud의 글로벌 지역 맵" .

볼륨 템플릿 및 태그는 더 이상 지원되지 않습니다.

더 이상 템플릿에서 볼륨을 생성하거나 볼륨의 태그를 편집할 수 없습니다. 이러한 작업은 더 이상 제공되지 않는 BlueXP 복구 서비스와 관련이 있습니다.

2024년 3월 8일

Amazon Instant Metadata Service v2 지원

AWS에서 Cloud Volumes ONTAP, Mediator 및 Connector는 이제 모든 기능에 대해 Amazon Instant Metadata Service v2(IMDSv2)를 지원합니다. IMDSv2는 취약점에 대한 강화된 보호 기능을 제공합니다. 이전에는 IMDSv1만 지원되었습니다.

보안 정책에 따라 필요한 경우 EC2 인스턴스를 구성하여 IMDSv2를 사용할 수 있습니다. 지침은 다음을 참조하세요. "기존 커넥터 관리를 위한 BlueXP 설정 및 관리 문서" .

2024년 3월 5일

Cloud Volumes ONTAP 9.14.1 GA

이제 BlueXP AWS, Azure 및 Google Cloud에서 Cloud Volumes ONTAP 9.14.1 일반 공급 릴리스를 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

2024년 2월 2일

Azure에서 Edv5 시리즈 VM 지원

Cloud Volumes ONTAP 이제 9.14.1 릴리스부터 다음 Edv5 시리즈 VM을 지원합니다.

- E4ds_v5
- E8ds_v5
- E20s_v5
- E32ds_v5
- E48ds_v5
- E64ds_v5

"Azure에서 지원되는 구성"

2024년 1월 16일

BlueXP 의 패치 릴리스

패치 릴리스는 Cloud Volumes ONTAP 의 최신 3개 버전에 대해서만 BlueXP 에서 사용 가능합니다.

"Cloud Volumes ONTAP 업그레이드"

2024년 1월 8일

Azure 다중 가용성 영역을 위한 새로운 VM

Cloud Volumes ONTAP 9.13.1부터 다음 VM 유형은 새 고가용성 쌍 배포와 기존 고가용성 쌍 배포에 대해 Azure 다중 가용성 영역을 지원합니다.

- L16s_v3
- L32s_v3
- L48s_v3
- L64s_v3

"Azure에서 지원되는 구성"

2023년 12월 6일

Cloud Volumes ONTAP 9.14.1 RC1

이제 BlueXP AWS, Azure, Google Cloud에서 Cloud Volumes ONTAP 9.14.1을 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

300 TiB FlexVol volume 최대 한도

이제 Cloud Volumes ONTAP 9.12.1 P2 및 9.13.0 P2부터 System Manager와 ONTAP CLI를 사용하여 최대 300TiB 크기의 FlexVol volume 생성할 수 있으며, Cloud Volumes ONTAP 9.13.1부터 BlueXP 사용하여 생성할 수 있습니다.

- "AWS의 저장 한도"
- "Azure의 저장소 한도"
- "Google Cloud의 저장 용량 한도"

2023년 12월 5일

다음과 같은 변경 사항이 도입되었습니다.

Azure의 새로운 지역 지원

단일 가용성 영역 지역 지원

다음 지역은 이제 Azure에서 Cloud Volumes ONTAP 9.12.1 GA 이상에 대한 고가용성 단일 가용성 영역 배포를 지원합니다.

- 텔아비브
- 밀라노

다중 가용성 영역 지역 지원

다음 지역은 이제 Azure에서 Cloud Volumes ONTAP 9.12.1 GA 이상에 대해 고가용성 다중 가용성 영역 배포를 지원합니다.

- 중앙 인도
- 노르웨이 동부
- 스위스 북부
- 남아프리카 공화국 북부

- 아랍에미리트 북부

모든 지역 목록은 다음을 참조하세요. "Azure의 글로벌 지역 맵" .

2023년 11월 10일

다음 변경 사항은 Connector 3.9.35 릴리스와 함께 도입되었습니다.

베를린 지역이 이제 **Google Cloud**에서 지원됩니다**.**

베를린 지역은 이제 Google Cloud for Cloud Volumes ONTAP 9.12.1 GA 이상에서 지원됩니다.

모든 지역 목록은 다음을 참조하세요. "Google Cloud의 글로벌 지역 맵" .

2023년 11월 8일

다음 변경 사항은 Connector 3.9.35 릴리스와 함께 도입되었습니다.

텔아비브 지역이 이제 **AWS**에서 지원됩니다**.**

텔아비브 지역은 이제 AWS의 Cloud Volumes ONTAP 9.12.1 GA 이상에서 지원됩니다.

모든 지역 목록은 다음을 참조하세요. "AWS의 글로벌 지역 맵" .

2023년 11월 1일

다음 변경 사항은 Connector 3.9.34 릴리스와 함께 도입되었습니다.

사우디 아라비아 지역이 이제 **Google Cloud**에서 지원됩니다**.**

사우디아라비아 지역은 이제 Google Cloud for Cloud Volumes ONTAP 및 Connector for Cloud Volumes ONTAP 9.12.1 GA 이상에서 지원됩니다.

모든 지역 목록은 다음을 참조하세요. "Google Cloud의 글로벌 지역 맵" .

2023년 10월 23일

다음 변경 사항은 Connector 3.9.34 릴리스와 함께 도입되었습니다.

Azure에서 **HA** 다중 가용성 영역 배포를 지원하는 새로운 지역

Azure의 다음 지역은 이제 Cloud Volumes ONTAP 9.12.1 GA 이상에 대해 고가용성 다중 가용성 영역 배포를 지원합니다.

- 호주 동부
- 동아시아
- 프랑스 중부
- 북유럽

- 카타르 센트럴
- 스웨덴 중부
- 서유럽
- 서부 미국 2

여러 가용성 영역을 지원하는 모든 지역 목록은 다음을 참조하세요. "Azure의 글로벌 지역 맵" .

2023년 10월 6일

다음 변경 사항은 Connector 3.9.34 릴리스와 함께 도입되었습니다.

Cloud Volumes ONTAP 9.14.0

이제 BlueXP AWS, Azure 및 Google Cloud에서 Cloud Volumes ONTAP 9.14.0 일반 공급 릴리스를 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

2023년 9월 10일

다음 변경 사항은 Connector 3.9.33 릴리스와 함께 도입되었습니다.

Azure에서 Lsv3 시리즈 VM 지원

L48s_v3 및 L64s_v3 인스턴스 유형은 이제 Azure의 Cloud Volumes ONTAP 에서 지원되며, 단일 및 다중 가용성 영역에서 공유 관리 디스크를 사용하는 단일 노드 및 고가용성 쌍 배포가 가능합니다(9.13.1 릴리스부터). 이러한 인스턴스 유형은 Flash Cache를 지원합니다.

"Azure에서 Cloud Volumes ONTAP 에 지원되는 구성 보기" "Azure에서 Cloud Volumes ONTAP 의 저장소 한도 보기"

2023년 7월 30일

Connector 3.9.32 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Google Cloud의 Flash Cache 및 고속 쓰기 지원

Google Cloud의 Cloud Volumes ONTAP 9.13.1 이상에서는 Flash Cache와 고속 쓰기 속도를 별도로 활성화할 수 있습니다. 지원되는 모든 인스턴스 유형에서 높은 쓰기 속도를 사용할 수 있습니다. Flash Cache는 다음 인스턴스 유형에서 지원됩니다.

- n2-표준-16
- n2-표준-32
- n2-표준-48
- n2-표준-64

이러한 기능은 단일 노드와 고가용성 쌍 배포 모두에서 별도로 또는 함께 사용할 수 있습니다.

"Google Cloud에서 Cloud Volumes ONTAP 실행"

사용 보고서 개선

사용 보고서에 표시되는 정보에 다양한 개선 사항이 적용되었습니다. 사용 보고서의 개선 사항은 다음과 같습니다.

- 이제 TiB 단위가 열 이름에 포함됩니다.
- 이제 일련 번호에 대한 새로운 "노드" 필드가 포함되었습니다.
- 이제 스토리지 VM 사용 보고서에 새로운 "워크로드 유형" 열이 포함되었습니다.
- 이제 작업 환경 이름이 스토리지 VM 및 볼륨 사용 보고서에 포함됩니다.
- 볼륨 유형 "파일"이 이제 "기본(읽기/쓰기)"로 표시됩니다.
- 볼륨 유형 "보조"는 이제 "보조(DP)"로 표시됩니다.

사용 보고서에 대한 자세한 내용은 다음을 참조하세요. "사용 보고서 다운로드" .

2023년 7월 26일

Connector 3.9.31 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Cloud Volumes ONTAP 9.13.1 GA

이제 BlueXP AWS, Azure 및 Google Cloud에서 Cloud Volumes ONTAP 9.13.1 일반 공급 릴리스를 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

2023년 7월 2일

Connector 3.9.31 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Azure에서 **HA** 다중 가용성 영역 배포 지원

Azure의 일본 동부 및 한국 중부는 이제 Cloud Volumes ONTAP 9.12.1 GA 이상에 대해 HA 다중 가용성 영역 배포를 지원합니다.

여러 가용성 영역을 지원하는 모든 지역 목록은 다음을 참조하세요. "Azure의 글로벌 지역 맵" .

자율형 랜섬웨어 보호 지원

이제 Cloud Volumes ONTAP 에서 자율 랜섬웨어 보호(ARP)가 지원됩니다. ARP 지원은 Cloud Volumes ONTAP 버전 9.12.1 이상에서 사용할 수 있습니다.

Cloud Volumes ONTAP 사용한 ARP에 대해 자세히 알아보려면 다음을 참조하세요. "자율형 랜섬웨어 보호" .

2023년 6월 26일

다음 변경 사항은 Connector 3.9.30 릴리스와 함께 도입되었습니다.

Cloud Volumes ONTAP 9.13.1 RC1

이제 BlueXP AWS, Azure, Google Cloud에서 Cloud Volumes ONTAP 9.13.1을 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

2023년 6월 4일

다음 변경 사항은 Connector 3.9.30 릴리스와 함께 도입되었습니다.

Cloud Volumes ONTAP 업그레이드 버전 선택기 업데이트

Cloud Volumes ONTAP 업그레이드 페이지를 통해 이제 최신 버전의 Cloud Volumes ONTAP 또는 이전 버전으로 업그레이드할 수 있습니다.

BlueXP 통해 Cloud Volumes ONTAP 업그레이드하는 방법에 대해 자세히 알아보려면 다음을 참조하세요. "Cloud Volumes ONTAP 업그레이드" .

2023년 5월 7일

Connector 3.9.29 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

카타르 지역이 이제 Google Cloud에서 지원됩니다.

카타르 지역은 이제 Google Cloud for Cloud Volumes ONTAP 및 Connector for Cloud Volumes ONTAP 9.12.1 GA 이상에서 지원됩니다.

스웨덴 중부 지역이 이제 Azure에서 지원됩니다.

스웨덴 중부 지역은 이제 Azure에서 Cloud Volumes ONTAP 및 Connector for Cloud Volumes ONTAP 9.12.1 GA 이상에서 지원됩니다.

Azure Australia East에서 HA 다중 가용성 영역 배포 지원

Azure의 호주 동부 지역은 이제 Cloud Volumes ONTAP 9.12.1 GA 이상에 대해 HA 다중 가용성 영역 배포를 지원합니다.

충전 사용량 내역

이제 용량 기반 라이선스에 가입했을 때 요금이 얼마인지 알아볼 수 있습니다. 다음 유형의 사용 보고서는 BlueXP 의 디지털 지갑에서 다운로드할 수 있습니다. 사용 보고서는 구독의 용량 세부 정보를 제공하고 Cloud Volumes ONTAP 구독의 리소스에 대한 요금이 어떻게 청구되는지 알려줍니다. 다운로드 가능한 보고서는 다른 사람들과 쉽게 공유할 수 있습니다.

- Cloud Volumes ONTAP 패키지 사용
- 높은 수준의 사용법
- 스토리지 VM 사용량
- 볼륨 사용량

자세한 내용은 다음을 참조하세요. "용량 기반 라이선스 관리" .

이제 마켓플레이스 구독 없이 **BlueXP** 액세스할 때 알림이 표시됩니다**.**

이제 마켓플레이스 구독 없이 BlueXP 에서 Cloud Volumes ONTAP 액세스할 때마다 알림이 표시됩니다. 알림에는 "이 작업 환경에 대한 마켓플레이스 구독은 Cloud Volumes ONTAP 이용 약관을 준수해야 합니다."라고 명시되어 있습니다.

HA 미디에이터에 대한 **AWS IAM** 정책에 새로운 권한이 추가되었습니다**.**

이러한 새로운 AWS 권한이 Cloud Volumes ONTAP 고가용성(HA) 환경의 HA 미들웨어용 IAM 정책에 추가되었습니다.

- sts:역할 가정
- ec2:서브넷 설명

2023년 4월 4일

AWS 중국 지역 지원

Cloud Volumes ONTAP 9.12.1 GA부터 AWS에서 중국 지역이 다음과 같이 지원됩니다.

- 단일 노드 시스템이 지원됩니다.
- NetApp 에서 직접 구매한 라이선스가 지원됩니다.

지역별 가용성은 다음을 참조하세요. "Cloud Volumes ONTAP 위한 글로벌 지역 맵" .

2023년 4월 3일

Connector 3.9.28 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

이제 **Google Cloud**에서 토리노 지역이 지원됩니다**.**

이제 토리노 지역은 Google Cloud for Cloud Volumes ONTAP 및 Connector for Cloud Volumes ONTAP 9.12.1 GA 이상에서 지원됩니다.

BlueXP digital wallet 개선

이제 BlueXP digital wallet 마켓플레이스 비공개 제안으로 구매한 라이선스 용량이 표시됩니다.

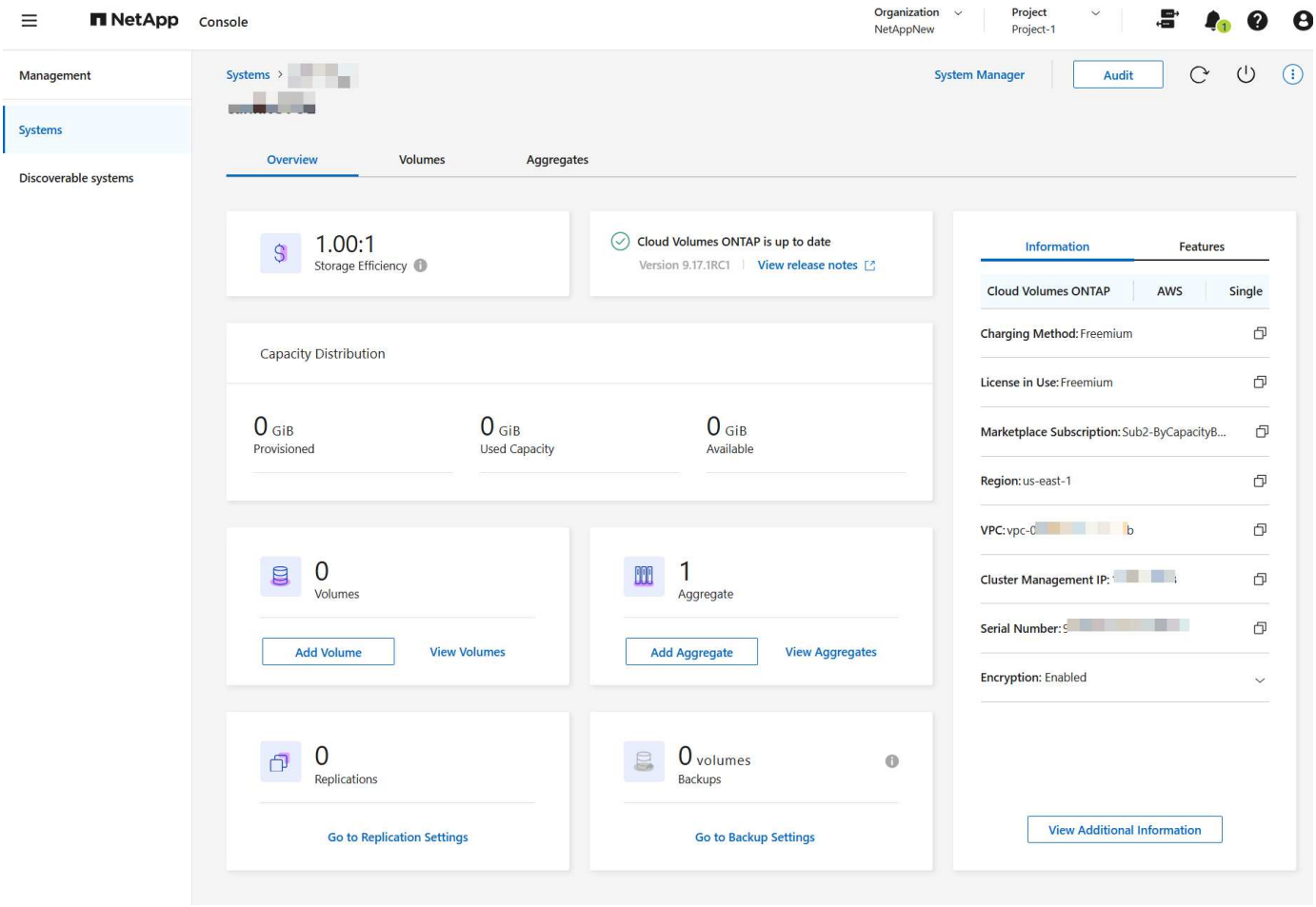
"계정에서 사용된 용량을 보는 방법을 알아보세요" .

볼륨 생성 중 주석 지원

이 릴리스에서는 API를 사용하여 Cloud Volumes ONTAP FlexGroup 볼륨이나 FlexVol volume 생성할 때 주석을 추가할 수 있습니다.

Cloud Volumes ONTAP 개요**,** 볼륨 및 집계 페이지에 대한 **BlueXP** 사용자 인터페이스 재설계

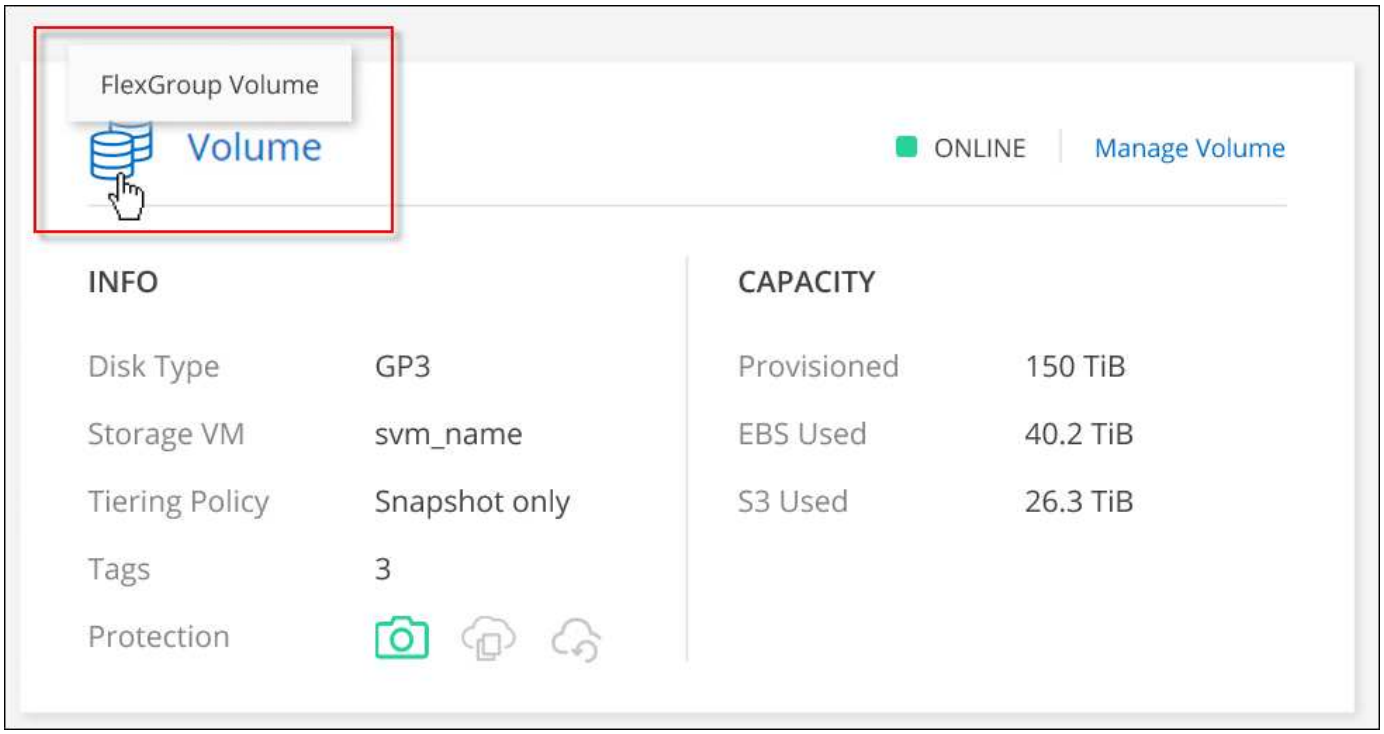
이제 BlueXP 에는 Cloud Volumes ONTAP 개요, 볼륨 및 집계 페이지에 대한 사용자 인터페이스가 재설계되었습니다. 타일 기반 디자인은 더 나은 사용자 경험을 위해 각 타일에 더욱 포괄적인 정보를 제공합니다.



Cloud Volumes ONTAP 을 통해 볼 수 있는 **FlexGroup** 볼륨

ONTAP 시스템 관리자나 ONTAP CLI를 통해 직접 생성된 FlexGroup 볼륨은 이제 BlueXP 의 재설계된 볼륨 타일을 통해 볼 수 있습니다. FlexVol 볼륨에 대해 제공되는 정보와 동일하게 BlueXP 전용 볼륨 타일을 통해 생성된 FlexGroup 볼륨에 대한 자세한 정보를 제공합니다.

현재는 BlueXP 에서만 기존 FlexGroup 볼륨을 볼 수 있습니다. BlueXP 에서 FlexGroup 볼륨을 생성하는 기능은 현재 제공되지 않지만 향후 릴리스에서 제공될 예정입니다.



"생성된 FlexGroup 볼륨을 보는 방법에 대해 자세히 알아보세요."

2023년 3월 13일

Azure에서 중국 지역 지원

이제 중국 북부 3 지역에서 Azure의 Cloud Volumes ONTAP 9.12.1 GA 및 9.13.0 GA의 단일 노드 배포가 지원됩니다. 이 지역에서는 NetApp 에서 직접 구매한 라이선스(BYOL 라이선스)만 지원됩니다.

중국 지역에서 Cloud Volumes ONTAP 새로 배포하는 것은 9.12.1 GA 및 9.13.0 GA에서만 지원됩니다. 이러한 버전을 Cloud Volumes ONTAP 의 최신 패치 및 릴리스로 업그레이드할 수 있습니다. 중국 지역에 이후 Cloud Volumes ONTAP 버전을 배포하려면 NetApp 지원팀에 문의하세요.

지역별 가용성은 다음을 참조하세요. "Cloud Volumes ONTAP 위한 글로벌 지역 맵" .

2023년 3월 5일

Connector 3.9.27 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Cloud Volumes ONTAP 9.13.0

이제 BlueXP AWS, Azure, Google Cloud에서 Cloud Volumes ONTAP 9.13.0을 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

Azure에서 **16TiB** 및 **32TiB** 지원

Cloud Volumes ONTAP 이제 Azure의 관리형 디스크에서 실행되는 고가용성 배포를 위해 16TiB 및 32TiB 디스크 크기를 지원합니다.

자세히 알아보세요 "Azure에서 지원되는 디스크 크기" .

MTEKM 라이센스

다중 테넌트 암호화 키 관리(MTEKM) 라이선스는 이제 버전 9.12.1 GA 이상을 실행하는 새 Cloud Volumes ONTAP 시스템과 기존 Cloud Volumes ONTAP 시스템에 포함됩니다.

다중 테넌트 외부 키 관리를 통해 NetApp 볼륨 암호화를 사용할 때 개별 스토리지 VM(SVM)이 KMIP 서버를 통해 자체 키를 유지 관리할 수 있습니다.

"NetApp 암호화 솔루션으로 볼륨을 암호화하는 방법을 알아보세요" .

인터넷이 없는 환경 지원

Cloud Volumes ONTAP 은 이제 인터넷에서 완전히 격리된 모든 클라우드 환경에서 지원됩니다. 이러한 환경에서는 노드 기반 라이선싱(BYOL)만 지원됩니다. 용량 기반 라이선싱은 지원되지 않습니다. 시작하려면 Connector 소프트웨어를 수동으로 설치하고, Connector에서 실행 중인 BlueXP 콘솔에 로그인하고, BYOL 라이선스를 BlueXP digital wallet 에 추가한 다음 Cloud Volumes ONTAP 배포합니다.

- "인터넷 접속이 불가능한 위치에 커넥터를 설치하세요"
- "커넥터에서 BlueXP 콘솔에 액세스하세요"
- "할당되지 않은 라이선스 추가"

Google Cloud의 플래시 캐시와 빠른 쓰기 속도

Cloud Volumes ONTAP 9.13.0 릴리스를 통해 일부 인스턴스에서 Flash Cache, 빠른 쓰기 속도, 8,896바이트의 높은 최대 전송 단위(MTU)에 대한 지원이 제공됩니다.

자세히 알아보세요 "Google Cloud 라이선스에 따라 지원되는 구성" .

2023년 2월 5일

Connector 3.9.26 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

AWS에서 배치 그룹 생성

AWS HA 단일 가용성 영역(AZ) 배포를 통해 배치 그룹을 생성할 때 새로운 구성 설정을 사용할 수 있습니다. 이제 실패한 배치 그룹 생성을 우회하고 AWS HA 단일 AZ 배포를 성공적으로 완료할 수 있습니다.

배치 그룹 생성 설정을 구성하는 방법에 대한 자세한 내용은 다음을 참조하세요. "AWS HA 단일 AZ에 대한 배치 그룹 생성 구성" .

개인 **DNS** 영역 구성 업데이트

Azure Private Links를 사용할 때 개인 DNS 영역과 가상 네트워크 간에 링크를 만들지 않도록 하는 새로운 구성 설정이 추가되었습니다. 생성은 기본적으로 활성화되어 있습니다.

"Azure Private DNS에 대한 세부 정보를 BlueXP 에 제공하세요."

WORM 스토리지 및 데이터 계층화

이제 Cloud Volumes ONTAP 9.8 시스템 이상을 만들 때 데이터 계층화와 WORM 스토리지를 함께 활성화할 수 있습니다. WORM 스토리지를 사용하여 데이터 계층화를 활성화하면 클라우드의 개체 저장소에 데이터를 계층화할 수 있습니다.

"WORM 저장소에 대해 알아보세요."

2023년 1월 1일

Connector 3.9.25 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Google Cloud에서 사용 가능한 라이선스 패키지

Google Cloud Marketplace에서 Cloud Volumes ONTAP 에 대한 최적화된 캐시 및 에지 캐시 용량 기반 라이선싱 패키지를 사용량 기반 지불 방식이나 연간 계약으로 이용할 수 있습니다.

참조하다 "Cloud Volumes ONTAP 라이선싱" .

Cloud Volumes ONTAP 의 기본 구성

다중 테넌트 암호화 키 관리(MTEKM) 라이선스는 더 이상 새로운 Cloud Volumes ONTAP 배포에 포함되지 않습니다.

Cloud Volumes ONTAP 과 함께 자동으로 설치되는 ONTAP 기능 라이선스에 대한 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 의 기본 구성" .

2022년 12월 15일

Cloud Volumes ONTAP 9.12.0

이제 BlueXP AWS와 Google Cloud에서 Cloud Volumes ONTAP 9.12.0을 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

2022년 12월 8일

Cloud Volumes ONTAP 9.12.1

BlueXP 이제 새로운 기능과 추가 클라우드 공급자 지역에 대한 지원을 포함하는 Cloud Volumes ONTAP 9.12.1을 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요."

2022년 12월 4일

Connector 3.9.24 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

이제 **Cloud Volumes ONTAP** 생성 중에 **WORM +** 클라우드 백업을 사용할 수 있습니다**.**

이제 Cloud Volumes ONTAP 생성 프로세스 중에 WORM(Write Once, Read Many) 및 클라우드 백업 기능을 모두 활성화할 수 있습니다.

이스라엘 지역이 이제 **Google Cloud**에서 지원됩니다**.**

이스라엘 지역은 이제 Google Cloud for Cloud Volumes ONTAP 및 Connector for Cloud Volumes ONTAP 9.11.1 P3 이상에서 지원됩니다.

2022년 11월 15일

Connector 3.9.23 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Google Cloud의 **ONTAP S3** 라이선스

이제 Google Cloud Platform에서 버전 9.12.1 이상을 실행하는 새 Cloud Volumes ONTAP 시스템과 기존 Cloud Volumes ONTAP 시스템에 ONTAP S3 라이선스가 포함됩니다.

"ONTAP 설명서: S3 개체 스토리지 서비스를 구성하고 관리하는 방법을 알아보세요."

2022년 11월 6일

Connector 3.9.23 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Azure에서 리소스 그룹 이동

이제 동일한 Azure 구독 내에서 Azure의 한 리소스 그룹에서 다른 리소스 그룹으로 작업 환경을 이동할 수 있습니다.

자세한 내용은 다음을 참조하세요. "리소스 그룹 이동" .

NDMP-복사 인증

NDMP-copy는 이제 Cloud Volume ONTAP 과 함께 사용하도록 인증되었습니다.

NDMP를 구성하고 사용하는 방법에 대한 정보는 다음을 참조하십시오. "ONTAP 설명서: NDMP 구성 개요" .

Azure에 대한 관리 디스크 암호화 지원

관리되는 모든 디스크를 생성 시 암호화할 수 있는 새로운 Azure 권한이 추가되었습니다.

이 새로운 기능에 대한 자세한 내용은 다음을 참조하세요. "Azure에서 고객 관리 키를 사용하도록 Cloud Volumes ONTAP 설정" .

2022년 9월 18일

Connector 3.9.22 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

디지털 지갑 개선

- 이제 디지털 지갑에는 계정 전체의 Cloud Volumes ONTAP 시스템에 대한 최적화된 I/O 라이선싱 패키지와 프로비저닝된 WORM 용량에 대한 요약이 표시됩니다.

  이러한 세부 정보는 요금이 어떻게 청구되는지, 추가 용량을 구매해야 하는지 여부를 더 잘 이해하는 데 도움이 될 수 있습니다.

"계정에서 사용된 용량을 보는 방법을 알아보세요" .

- 이제 하나의 충전 방법에서 최적화된 충전 방법으로 변경할 수 있습니다.

  "충전 방법을 변경하는 방법을 알아보세요" .

비용과 성능을 최적화하세요

이제 Canvas에서 바로 Cloud Volumes ONTAP 시스템의 비용과 성능을 최적화할 수 있습니다.

작업 환경을 선택한 후 비용 및 성능 최적화 옵션을 선택하여 Cloud Volumes ONTAP 의 인스턴스 유형을 변경할 수 있습니다. 더 작은 크기의 인스턴스를 선택하면 비용을 줄이는 데 도움이 되고, 더 큰 크기의 인스턴스로 변경하면 성능을 최적화하는 데 도움이 됩니다.

[Cloud Volumes ONTAP 시스템을 선택한 후 Canvas에서 사용할 수 있는 Optimize Cost Performance 옵션의 스크린샷입니다.]

AutoSupport 알림

이제 BlueXP Cloud Volumes ONTAP 시스템이 AutoSupport 메시지를 보낼 수 없는 경우 알림을 생성합니다. 알림에는 네트워크 문제를 해결하는 데 사용할 수 있는 지침에 대한 링크가 포함되어 있습니다.

2022년 7월 31일

Connector 3.9.21 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

MTEKM 라이센스

다중 테넌트 암호화 키 관리(MTEKM) 라이선스는 이제 버전 9.11.1 이상을 실행하는 새 Cloud Volumes ONTAP 시스템과 기존 Cloud Volumes ONTAP 시스템에 포함됩니다.

다중 테넌트 외부 키 관리를 통해 NetApp 볼륨 암호화를 사용할 때 개별 스토리지 VM(SVM)이 KMIP 서버를 통해 자체 키를 유지 관리할 수 있습니다.

"NetApp 암호화 솔루션으로 볼륨을 암호화하는 방법을 알아보세요" .

프록시 서버

이제 BlueXP 아웃바운드 인터넷 연결을 통해 AutoSupport 메시지를 보낼 수 없는 경우 커넥터를 프록시 서버로 사용하도록 Cloud Volumes ONTAP 시스템을 자동으로 구성합니다.

AutoSupport 시스템 상태를 사전에 모니터링하고 NetApp 기술 지원팀에 메시지를 전송합니다.

유일한 요구 사항은 커넥터의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 커넥터를 배포한 후 이 포트를 열어야 합니다.

충전 방식 변경

이제 용량 기반 라이선싱을 사용하는 Cloud Volumes ONTAP 시스템의 요금 청구 방법을 변경할 수 있습니다. 예를 들어, Essentials 패키지로 Cloud Volumes ONTAP 시스템을 배포한 경우 비즈니스 요구 사항이 변경되면 Professional 패키지로 변경할 수 있습니다. 이 기능은 디지털 지갑에서 사용할 수 있습니다.

"충전 방법을 변경하는 방법을 알아보세요" .

보안 그룹 강화

Cloud Volumes ONTAP 작업 환경을 만들 때 이제 사용자 인터페이스에서 미리 정의된 보안 그룹이 선택한 네트워크 내에서만 트래픽을 허용할지(권장) 또는 모든 네트워크에서 트래픽을 허용할지 선택할 수 있습니다.

[보안 그룹을 선택할 때 작업 환경 마법사에서 사용할 수 있는 '트래픽 허용' 옵션을 보여주는 스크린샷입니다.]

2022년 7월 18일

Azure의 새로운 라이선스 패키지

Azure Marketplace 구독을 통해 결제하는 경우 Azure의 Cloud Volumes ONTAP 에 대해 두 가지 새로운 용량 기반 라이선싱 패키지를 사용할 수 있습니다.

- 최적화: 프로비저닝된 용량과 I/O 작업에 대해 별도로 지불합니다.
- **Edge Cache**: 라이선스 "클라우드 볼륨 에지 캐시"

"이러한 라이선스 패키지에 대해 자세히 알아보세요" .

2022년 7월 3일

Connector 3.9.20 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

디지털 지갑

이제 디지털 지갑에서 계정의 총 소비 용량과 라이선스 패키지별 소비 용량을 확인할 수 있습니다. 이를 통해 요금이 어떻게 청구되는지, 추가 용량을 구매해야 하는지 파악하는 데 도움이 됩니다.

[용량 기반 라이선스에 대한 디지털 지갑 페이지를 보여주는 스크린샷입니다. 이 페이지에서는 계정에서 사용된 용량에 대한 개요를 제공하고, 라이선스 패키지별로 사용된 용량을 세부적으로 보여줍니다.]

탄력 볼륨 향상

이제 BlueXP 사용자 인터페이스에서 Cloud Volumes ONTAP 작업 환경을 생성할 때 Amazon EBS Elastic Volumes 기능을 지원합니다. gp3 또는 io1 디스크를 사용하면 Elastic Volumes 기능이 기본적으로 활성화됩니다. 스토리지 요구 사항에 따라 초기 용량을 선택하고 Cloud Volumes ONTAP 배포한 후 수정할 수 있습니다.

"AWS에서 Elastic Volumes 지원에 대해 자세히 알아보세요" .

AWS의 **ONTAP S3** 라이선스

ONTAP S3 라이선스는 이제 AWS에서 버전 9.11.0 이상을 실행하는 새 Cloud Volumes ONTAP 시스템과 기존 Cloud Volumes ONTAP 시스템에 포함됩니다.

"ONTAP 설명서: S3 개체 스토리지 서비스를 구성하고 관리하는 방법을 알아보세요."

새로운 **Azure Cloud** 지역 지원

9.10.1 릴리스부터 Cloud Volumes ONTAP 이 이제 Azure West US 3 지역에서 지원됩니다.

"Cloud Volumes ONTAP 에 지원되는 지역의 전체 목록을 확인하세요."

Azure의 **ONTAP S3** 라이선스

이제 Azure에서 버전 9.9.1 이상을 실행하는 새 Cloud Volumes ONTAP 시스템과 기존 Cloud Volumes ONTAP 시스템에 ONTAP S3 라이선스가 포함됩니다.

"ONTAP 설명서: S3 개체 스토리지 서비스를 구성하고 관리하는 방법을 알아보세요."

2022년 6월 7일

Connector 3.9.19 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Cloud Volumes ONTAP 9.11.1

BlueXP 이제 새로운 기능과 추가 클라우드 공급자 지역에 대한 지원을 포함하는 Cloud Volumes ONTAP 9.11.1을 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요."

새로운 고급 보기

Cloud Volumes ONTAP 의 고급 관리를 수행해야 하는 경우 ONTAP 시스템과 함께 제공되는 관리 인터페이스인 ONTAP System Manager를 사용하여 해당 작업을 수행할 수 있습니다. 고급 관리를 위해 BlueXP 벗어날 필요가 없도록 BlueXP 내부에 시스템 관리자 인터페이스를 포함시켰습니다.

이 고급 보기는 Cloud Volumes ONTAP 9.10.0 이상에서 미리 보기로 제공됩니다. 우리는 이 경험을 더욱 개선하고 향후 릴리스에서 향상된 기능을 추가할 계획입니다. 제품 내 채팅을 이용해 피드백을 보내주세요.

"고급 보기에 대해 자세히 알아보세요" .

Amazon EBS 탄력적 볼륨 지원

Cloud Volumes ONTAP 집계를 통한 Amazon EBS Elastic Volumes 기능을 지원하면 더 나은 성능과 추가 용량을 제공하는 동시에 BlueXP 필요에 따라 기본 디스크 용량을 자동으로 늘릴 수 있습니다.

Elastic Volumes에 대한 지원은 새로운 Cloud Volumes ONTAP 9.11.0 시스템과 gp3 및 io1 EBS 디스크 유형부터 사용할 수 있습니다.

"Elastic Volumes 지원에 대해 자세히 알아보세요" .

Elastic Volumes를 지원하려면 커넥터에 대한 새로운 AWS 권한이 필요합니다.

```
"ec2:DescribeVolumesModifications",
"ec2:ModifyVolume",
```

BlueXP 에 추가한 각 AWS 자격 증명 세트에 이러한 권한을 제공해야 합니다. "AWS의 최신 커넥터 정책 보기" .

공유 **AWS** 서브넷에 **HA** 쌍 배포 지원

Cloud Volumes ONTAP 9.11.1에는 AWS VPC 공유에 대한 지원이 포함되어 있습니다. 이 커넥터 릴리스를 사용하면 API를 사용할 때 AWS 공유 서브넷에 HA 쌍을 배포할 수 있습니다.

"공유 서브넷에 HA 쌍을 배포하는 방법을 알아보세요." .

서비스 엔드포인트를 사용할 때 네트워크 액세스가 제한됨

이제 BlueXP Cloud Volumes ONTAP 과 스토리지 계정 간 연결에 VNet 서비스 엔드포인트를 사용할 때 네트워크 액세스를 제한합니다. Azure Private Link 연결을 비활성화하면 BlueXP 서비스 엔드포인트를 사용합니다.

"Cloud Volumes ONTAP 사용한 Azure Private Link 연결에 대해 자세히 알아보세요." .

Google Cloud에서 스토리지 **VM** 생성 지원

Google Cloud의 Cloud Volumes ONTAP 9.11.1 릴리스부터 여러 스토리지 VM을 지원합니다. 이 커넥터 릴리스부터 BlueXP 사용하면 API를 사용하여 Google Cloud의 Cloud Volumes ONTAP HA 쌍에서 스토리지 VM을 생성할 수 있습니다.

스토리지 VM 생성을 지원하려면 커넥터에 대한 새로운 Google Cloud 권한이 필요합니다.

```
- compute.instanceGroups.get
- compute.addresses.get
```

단일 노드 시스템에서 스토리지 VM을 생성하려면 ONTAP CLI 또는 System Manager를 사용해야 합니다.

- "Google Cloud의 스토리지 VM 제한에 대해 자세히 알아보세요."
- "Google Cloud에서 Cloud Volumes ONTAP 위한 데이터 제공 스토리지 VM을 만드는 방법을 알아보세요."

2022년 5월 2일

Connector 3.9.18 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Cloud Volumes ONTAP 9.11.0

이제 BlueXP Cloud Volumes ONTAP 9.11.0을 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

중재자 업그레이드 개선

BlueXP HA 쌍의 중재자를 업그레이드할 때 이제 부팅 디스크를 삭제하기 전에 새로운 중재자 이미지를 사용할 수 있는지 확인합니다. 이러한 변경을 통해 업그레이드 프로세스가 실패하더라도 중재자가 계속해서 성공적으로 운영될 수 있습니다.

K8s 탭이 제거되었습니다

K8s 탭은 이전 릴리스에서 더 이상 지원되지 않았으며, 현재는 제거되었습니다.

Azure의 연간 계약

Essentials 및 Professional 패키지는 이제 연간 계약을 통해 Azure에서 사용할 수 있습니다. 연간 계약을 구매하려면 NetApp 영업 담당자에게 문의하세요. 해당 계약은 Azure Marketplace에서 비공개 제안으로 제공됩니다.

NetApp 에서 비공개 제안을 공유한 후 작업 환경을 만드는 동안 Azure Marketplace에서 구독할 때 연간 요금제를 선택할 수 있습니다.

"라이선싱에 대해 자세히 알아보세요" .

S3 Glacier 즉시 검색

이제 계층형 데이터를 Amazon Simple Storage Service(Amazon S3) Glacier Instant Retrieval 스토리지 클래스에 저장할 수 있습니다.

"계층화된 데이터의 스토리지 클래스를 변경하는 방법을 알아보세요." .

커넥터에 필요한 새로운 AWS 권한

이제 단일 가용성 영역(AZ)에 HA 쌍을 배포할 때 AWS 스프레드 배치 그룹을 생성하려면 다음 권한이 필요합니다.

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

이제 BlueXP 배치 그룹을 생성하는 방식을 최적화하려면 이러한 권한이 필요합니다.

BlueXP 에 추가한 각 AWS 자격 증명 세트에 이러한 권한을 제공해야 합니다. "AWS의 최신 커넥터 정책 보기" .

새로운 Google Cloud 지역 지원

Cloud Volumes ONTAP 이제 9.10.1 릴리스부터 다음 Google Cloud 지역에서 지원됩니다.

- 델리(asia-south2)
- 멜버른(호주-사우스이스트2)
- 밀라노(europe-west8) - 단일 노드만
- 산티아고(southamerica-west1) - 단일 노드만

"Cloud Volumes ONTAP 에 지원되는 지역의 전체 목록을 확인하세요."

Google Cloud에서 n2-standard-16 지원

n2-standard-16 머신 유형은 이제 Google Cloud의 Cloud Volumes ONTAP 9.10.1 릴리스부터 지원됩니다.

"Google Cloud에서 Cloud Volumes ONTAP 에 지원되는 구성 보기"

Google Cloud 방화벽 정책 개선

- Google Cloud에서 Cloud Volumes ONTAP HA 쌍을 생성하면 이제 BlueXP 가 VPC에 있는 모든 기존 방화벽 정책을 표시합니다.

이전에는 BlueXP 대상 태그가 없는 VPC-1, VPC-2 또는 VPC-3의 정책을 표시하지 않았습니다.

- Google Cloud에서 Cloud Volumes ONTAP 단일 노드 시스템을 생성할 때 사전 정의된 방화벽 정책이 선택한 VPC 내의 트래픽만 허용하도록 할지(권장) 아니면 모든 VPC를 허용하도록 할지 선택할 수 있습니다.

Google Cloud 서비스 계정 개선

Cloud Volumes ONTAP 과 함께 사용할 Google Cloud 서비스 계정을 선택하면 이제 BlueXP 각 서비스 계정과 연결된 이메일 주소가 표시됩니다. 이메일 주소를 보면 같은 이름을 공유하는 서비스 계정을 더 쉽게 구별할 수 있습니다.

[서비스 계정 필드의 스크린샷]

2022년 4월 3일

시스템 관리자 링크가 제거되었습니다.

이전에 Cloud Volumes ONTAP 작업 환경에서 사용할 수 있었던 시스템 관리자 링크를 제거했습니다.

Cloud Volumes ONTAP 시스템에 연결된 웹 브라우저에 클러스터 관리 IP 주소를 입력하면 System Manager에 연결할 수 있습니다. "시스템 관리자에 연결하는 방법에 대해 자세히 알아보세요." .

WORM 저장에 대한 요금 청구

이제 소개 특별 요금이 만료되었으므로 WORM 스토리지 사용에 대한 요금이 청구됩니다. 요금은 WORM 볼륨의 총 프로비저닝 용량에 따라 시간당으로 부과됩니다. 이는 새로운 Cloud Volumes ONTAP 시스템에 모두 적용됩니다.

"WORM 스토리지 가격에 대해 알아보세요" .

2022년 2월 27일

Connector 3.9.16 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

재설계된 볼륨 마법사

최근 도입한 새 볼륨 생성 마법사는 이제 고급 할당 옵션에서 특정 집계에 볼륨을 생성할 때 사용할 수 있습니다.

"특정 집계에 볼륨을 생성하는 방법을 알아보세요." .

2022년 2월 9일

마켓플레이스 업데이트

- Essentials 패키지와 Professional 패키지는 이제 모든 클라우드 공급업체 마켓플레이스에서 이용할 수 있습니다.

  이러한 용량별 요금 청구 방식을 사용하면 시간당 요금을 지불하거나 클라우드 공급업체로부터 직접 연간 계약을 구매할 수 있습니다. NetApp 에서 직접 용량별 라이선스를 구매할 수도 있습니다.

  클라우드 마켓플레이스에서 기존 구독이 있는 경우 이러한 새로운 서비스도 자동으로 구독됩니다. 새로운 Cloud Volumes ONTAP 작업 환경을 배포할 때 용량별 요금 청구를 선택할 수 있습니다.

신규 고객인 경우, 새로운 작업 환경을 만들 때 BlueXP 구독하라는 메시지가 표시됩니다.

- 모든 클라우드 공급업체 마켓플레이스의 노드별 라이선싱은 더 이상 제공되지 않으며, 신규 구독자에게는 더 이상 제공되지 않습니다. 여기에는 연간 계약과 시간당 구독(Explore, Standard, Premium)이 포함됩니다.

  이 청구 방법은 활성 구독이 있는 기존 고객에게는 계속 제공됩니다.

"Cloud Volumes ONTAP 의 라이선싱 옵션에 대해 자세히 알아보세요." .

2022년 2월 6일

할당되지 않은 라이센스 교환

사용하지 않은 Cloud Volumes ONTAP 용 노드 기반 라이선스가 할당되지 않은 경우 이제 해당 라이선스를 Cloud Backup 라이선스, Cloud Data Sense 라이선스 또는 Cloud Tiering 라이선스로 변환하여 교환할 수 있습니다.

이 작업을 수행하면 Cloud Volumes ONTAP 라이선스가 취소되고 동일한 만료 날짜를 가진 서비스에 대한 달러 상당의 라이선스가 생성됩니다.

"할당되지 않은 노드 기반 라이선스를 교환하는 방법을 알아보세요." .

2022년 1월 30일

Connector 3.9.15 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

재설계된 라이센스 선택

새로운 Cloud Volumes ONTAP 작업 환경을 만들 때 라이선스 선택 화면을 재설계했습니다. 이러한 변경 사항은 2021년 7월에 도입된 용량별 요금 청구 방식을 강조하고 클라우드 공급업체 마켓플레이스를 통해 향후 제공될 서비스를 지원합니다.

디지털 지갑 업데이트

Cloud Volumes ONTAP 라이선스를 단일 탭으로 통합하여 *디지털 지갑*을 업데이트했습니다.

2022년 1월 2일

Connector 3.9.14 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

추가 **Azure VM** 유형 지원

Cloud Volumes ONTAP 은 이제 Microsoft Azure 9.10.1 릴리스부터 다음 VM 유형에서 지원됩니다.

- E4ds_v4
- E8ds_v4
- E32ds_v4
- E48ds_v4

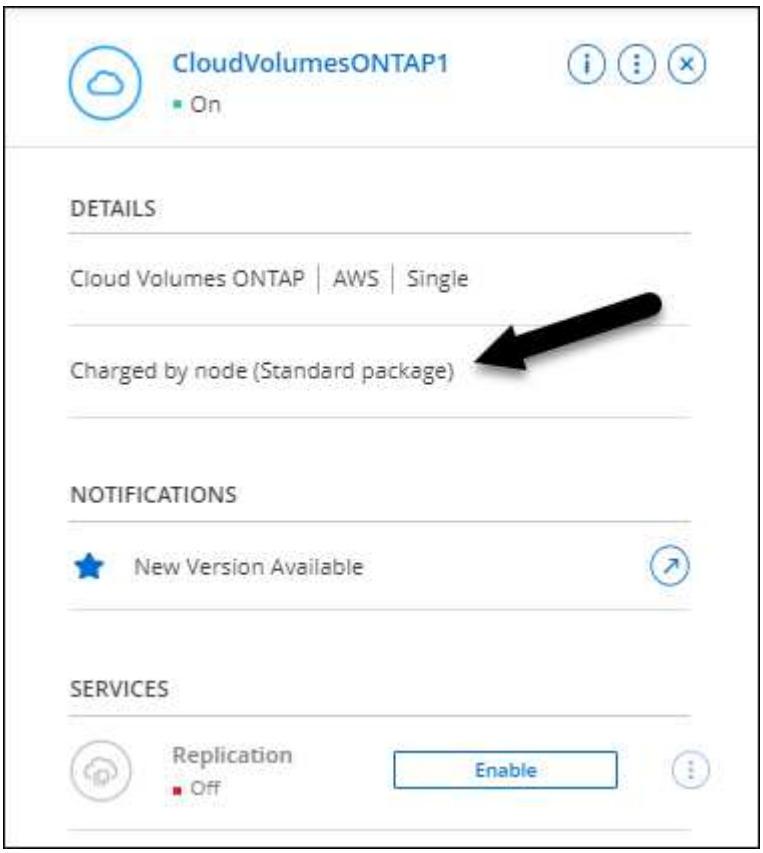
로 가다 "Cloud Volumes ONTAP 릴리스 노트" 지원되는 구성에 대한 자세한 내용은 다음을 참조하세요.

FlexClone 충전 업데이트

만약 당신이 사용한다면 "용량 기반 라이센스" Cloud Volumes ONTAP 의 경우 FlexClone 볼륨에서 사용하는 용량에 대해 더 이상 요금이 청구되지 않습니다.

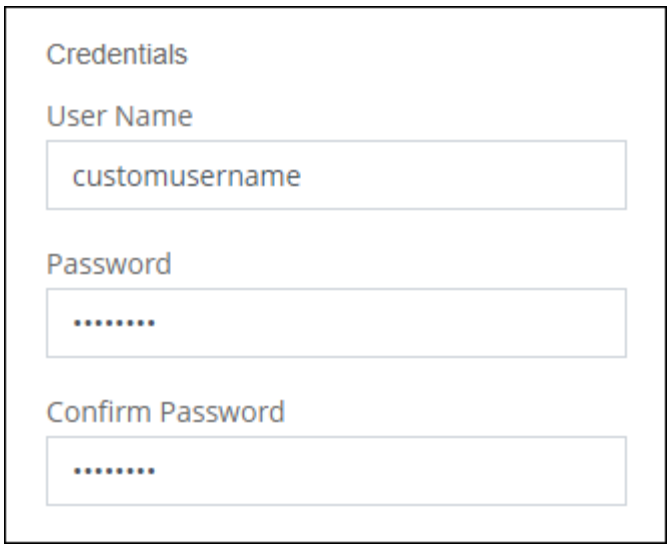
충전 방법이 표시됩니다.

이제 BlueXP Canvas의 오른쪽 패널에 각 Cloud Volumes ONTAP 작업 환경에 대한 요금 청구 방법을 표시합니다.



사용자 이름을 선택하세요

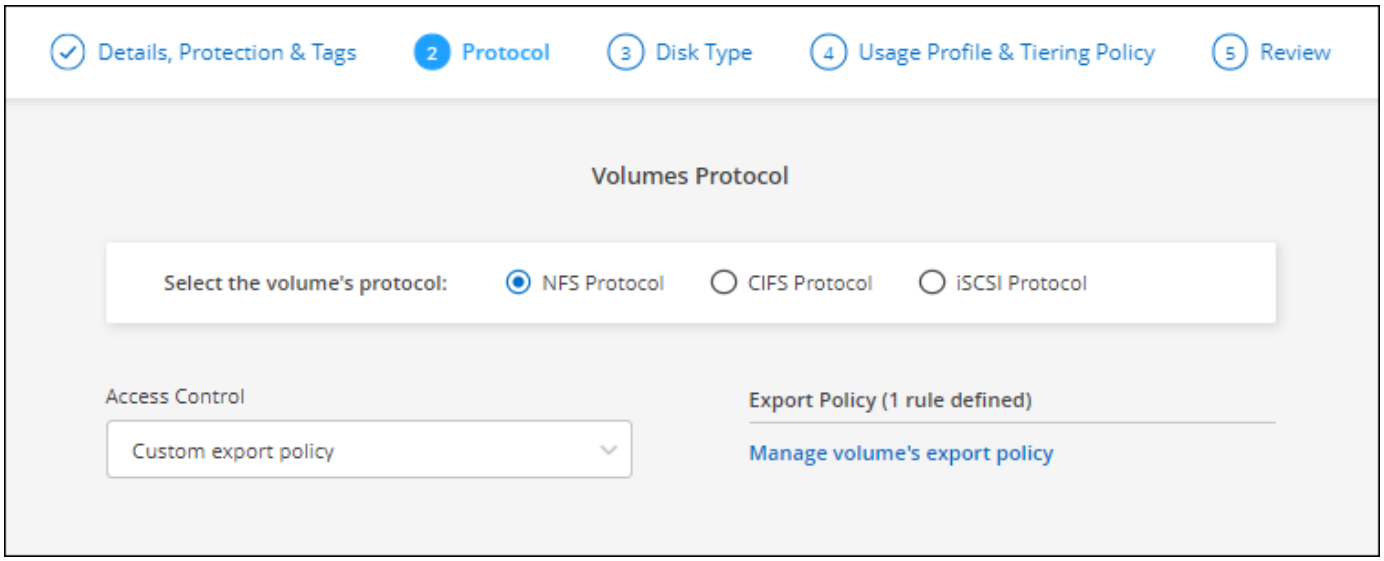
Cloud Volumes ONTAP 작업 환경을 만들 때 이제 기본 관리자 사용자 이름 대신 원하는 사용자 이름을 입력할 수 있습니다.



볼륨 생성 향상

볼륨 생성에 몇 가지 개선 사항을 적용했습니다.

- 사용 편의성을 높이기 위해 볼륨 생성 마법사를 재설계했습니다.
- 이제 NFS에 대한 사용자 정의 내보내기 정책을 선택할 수 있습니다.



2021년 11월 28일

Connector 3.9.13 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Cloud Volumes ONTAP 9.10.1

이제 BlueXP Cloud Volumes ONTAP 9.10.1을 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

NetApp Keystone 구독

이제 Keystone 구독을 사용하여 Cloud Volumes ONTAP HA 쌍에 대한 비용을 지불할 수 있습니다.

Keystone 구독은 선불 CapEx나 리스보다 OpEx 소비 모델을 선호하는 사람들에게 원활한 하이브리드 클라우드 환경을 제공하는, 성장에 따라 비용을 지불하는 구독 기반 서비스입니다.

Keystone 구독은 BlueXP 에서 배포할 수 있는 모든 새로운 버전의 Cloud Volumes ONTAP 에서 지원됩니다.

- "NetApp Keystone 구독에 대해 자세히 알아보세요" .
- "BlueXP 에서 Keystone 구독을 시작하는 방법을 알아보세요" .

새로운 AWS 지역 지원

Cloud Volumes ONTAP 이제 AWS 아시아 태평양(오사카) 지역(ap-northeast-3)에서 지원됩니다.

포트 감소

Azure의 Cloud Volumes ONTAP 시스템에서 단일 노드 시스템과 HA 쌍 모두에 대해 포트 8023 및 49000이 더 이상 열려 있지 않습니다.

이 변경 사항은 Connector 3.9.13 릴리스부터 시작되는 새로운 Cloud Volumes ONTAP 시스템에 적용됩니다.

2021년 10월 4일

Connector 3.9.11 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Cloud Volumes ONTAP 9.10.0

이제 BlueXP Cloud Volumes ONTAP 9.10.0을 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

배포 시간 단축

일반 쓰기 속도가 활성화된 경우 Microsoft Azure 또는 Google Cloud에서 Cloud Volumes ONTAP 작업 환경을 배포하는 데 걸리는 시간을 줄였습니다. 이제 배포 시간은 평균 3~4분 단축되었습니다.

2021년 9월 2일

Connector 3.9.10 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Azure의 고객 관리 암호화 키

Azure의 Cloud Volumes ONTAP 에서 데이터는 자동으로 암호화됩니다. "Azure Storage 서비스 암호화" Microsoft에서 관리하는 키를 사용합니다. 하지만 이제 다음 단계를 완료하면 고객이 관리하는 암호화 키를 사용할 수 있습니다.

1. Azure에서 키 자격 증명 모음을 만든 다음 해당 자격 증명 모음에서 키를 생성합니다.
2. BlueXP 에서 API를 사용하여 키를 사용하는 Cloud Volumes ONTAP 작업 환경을 만듭니다.

"이 단계에 대해 자세히 알아보세요" .

2021년 7월 7일

Connector 3.9.8 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

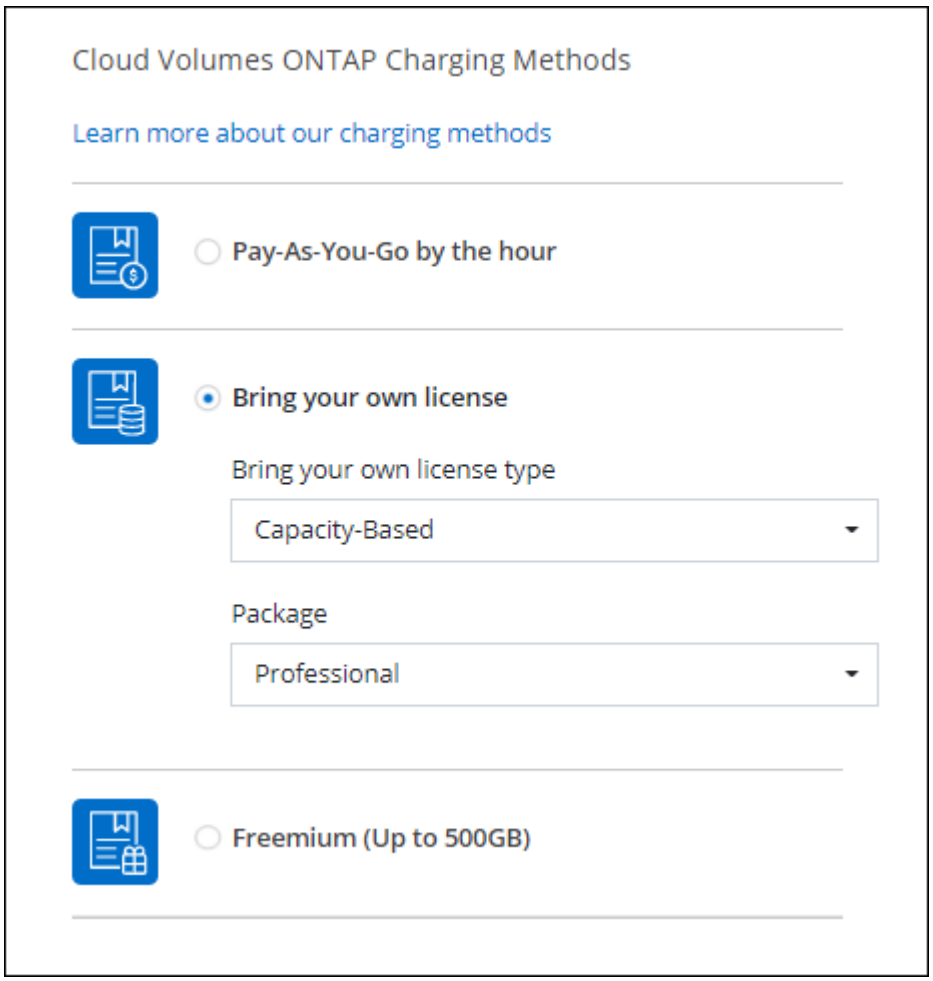
새로운 충전 방법

Cloud Volumes ONTAP 에 대한 새로운 요금 청구 방법을 사용할 수 있습니다.

- 용량 기반 **BYOL**: 용량 기반 라이선스를 사용하면 TiB 용량당 Cloud Volumes ONTAP 에 대한 비용을 지불할 수 있습니다. 라이선스는 NetApp 계정과 연결되며 라이선스를 통해 충분한 용량을 사용할 수 있는 한 여러 개의 Cloud Volumes ONTAP 시스템을 만들 수 있습니다. 용량 기반 라이선싱은 *Essentials* 또는 *Professional* 패키지 형태로 제공됩니다.
- 프리미엄 제공: 프리미엄을 이용하면 NetApp 에서 모든 Cloud Volumes ONTAP 기능을 무료로 사용할 수 있습니다(클라우드 공급자 요금은 여전히 적용됩니다). 시스템당 프로비저닝 용량은 500GiB로 제한되며 지원 계약은 없습니다. 최대 10개의 프리미엄 시스템을 가질 수 있습니다.

  "이러한 라이선싱 옵션에 대해 자세히 알아보세요" .

  선택할 수 있는 충전 방법의 예는 다음과 같습니다.



일반 용도로 사용 가능한 **WORM** 스토리지

한 번 쓰고 여러 번 읽는(WORM) 스토리지는 더 이상 미리 보기에 없으며 이제 Cloud Volumes ONTAP 과 함께 일반적으로 사용할 수 있습니다. "WORM 스토리지에 대해 자세히 알아보세요" .

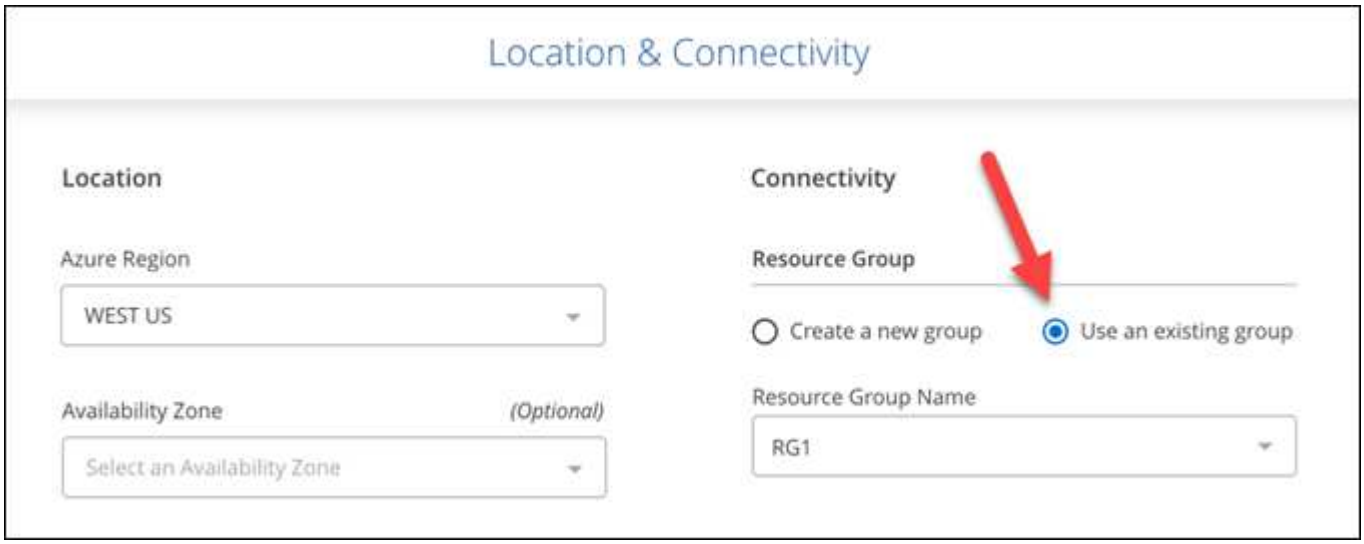
AWS에서 **m5dn.24xlarge** 지원

9.9.1 릴리스부터 Cloud Volumes ONTAP 이제 PAYGO Premium, BYOL(Bring Your Own License), Freemium 등의 요금 청구 방식으로 m5dn.24xlarge 인스턴스 유형을 지원합니다.

"AWS에서 Cloud Volumes ONTAP 에 지원되는 구성 보기" .

기존 **Azure** 리소스 그룹 선택

Azure에서 Cloud Volumes ONTAP 시스템을 만들 때 이제 VM 및 관련 리소스에 대한 기존 리소스 그룹을 선택할 수 있는 옵션이 제공됩니다.



다음 권한을 통해 BlueXP 배포 실패 또는 삭제 시 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거할 수 있습니다.

```
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Compute/availabilitySets/delete",
```

BlueXP 에 추가한 각 Azure 자격 증명 세트에 이러한 권한을 제공해야 합니다. "Azure에 대한 최신 커넥터 정책 보기" .

Azure에서 **Blob** 공용 액세스가 이제 비활성화되었습니다**.**

보안 강화를 위해 BlueXP 이제 Cloud Volumes ONTAP 에 대한 스토리지 계정을 생성할 때 *Blob 공용 액세스*를 비활성화합니다.

Azure Private Link 향상

기본적으로 BlueXP 이제 새로운 Cloud Volumes ONTAP 시스템의 부트 진단 스토리지 계정에서 Azure Private Link 연결을 활성화합니다.

즉, Cloud Volumes ONTAP 의 모든 스토리지 계정은 이제 개인 링크를 사용하게 됩니다.

"Cloud Volumes ONTAP 에서 Azure Private Link를 사용하는 방법에 대해 자세히 알아보세요." .

Google Cloud의 균형 잡힌 영구 디스크

9.9.1 릴리스부터 Cloud Volumes ONTAP 이제 균형 잡힌 영구 디스크(pd-balanced)를 지원합니다.

이러한 SSD는 GiB당 더 낮은 IOPS를 제공하여 성능과 비용의 균형을 맞춥니다.

custom-4-16384는 더 이상 **Google Cloud**에서 지원되지 않습니다**.**

custom-4-16384 머신 유형은 더 이상 새로운 Cloud Volumes ONTAP 시스템에서 지원되지 않습니다.

이 머신 유형에서 기존 시스템을 실행 중인 경우 계속 사용할 수 있지만 n2-standard-4 머신 유형으로 전환하는 것이 좋습니다.

"Google Cloud에서 Cloud Volumes ONTAP 에 지원되는 구성 보기".

2021년 5월 30일

Connector 3.9.7 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

AWS의 새로운 프로페셔널 패키지

새로운 Professional 패키지를 이용하면 AWS Marketplace에서 연간 계약을 통해 Cloud Volumes ONTAP 과 Cloud Backup Service 번들로 구매할 수 있습니다. 결제는 TiB 단위로 이루어집니다. 이 구독에서는 온프레미스 데이터를 백업할 수 없습니다.

이 결제 옵션을 선택하면 EBS 디스크를 통해 Cloud Volumes ONTAP 시스템당 최대 2PiB를 프로비저닝하고 S3 개체 스토리지(단일 노드 또는 HA)로 계층화할 수 있습니다.

로 가다 "AWS Marketplace 페이지" 가격 세부 정보를 보고 이동하려면 "Cloud Volumes ONTAP 릴리스 노트" 이 라이선싱 옵션에 대해 자세히 알아보세요.

AWS의 **EBS** 볼륨에 대한 태그

이제 BlueXP 새로운 Cloud Volumes ONTAP 작업 환경을 생성할 때 EBS 볼륨에 태그를 추가합니다. 태그는 Cloud Volumes ONTAP 배포된 후에 생성되었습니다.

조직에서 SCP(서비스 제어 정책)를 사용하여 권한을 관리하는 경우 이러한 변경 사항이 도움이 될 수 있습니다.

자동 티어링 정책에 대한 최소 냉각 기간

자동 계층화 정책을 사용하여 볼륨에서 데이터 계층화를 활성화한 경우 이제 API를 사용하여 최소 냉각 기간을 조정할 수 있습니다.

"최소 냉각 기간을 조정하는 방법을 알아보세요."

사용자 정의 수출 정책 향상

새로운 NFS 볼륨을 생성할 때 BlueXP 이제 사용자 정의 내보내기 정책을 오름차순으로 표시하여 필요한 내보내기 정책을 더 쉽게 찾을 수 있게 되었습니다.

이전 클라우드 스냅샷 삭제

이제 BlueXP Cloud Volumes ONTAP 시스템이 배포될 때와 전원이 꺼질 때마다 생성되는 루트 및 부팅 디스크의 이전 클라우드 스냅샷을 삭제합니다. 루트 볼륨과 부트 볼륨 모두에 대해 가장 최근의 스냅샷 두 개만 보존됩니다.

이 향상된 기능은 더 이상 필요하지 않은 스냅샷을 제거하여 클라우드 공급자 비용을 줄이는 데 도움이 됩니다.

커넥터에는 Azure 스냅샷을 삭제하기 위한 새로운 권한이 필요합니다. "Azure에 대한 최신 커넥터 정책 보기" .

```
"Microsoft.Compute/snapshots/delete"
```

2021년 5월 24일

Cloud Volumes ONTAP 9.9.1

이제 BlueXP Cloud Volumes ONTAP 9.9.1을 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

2021년 4월 11일

Connector 3.9.5 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

논리적 공간 보고

이제 BlueXP Cloud Volumes ONTAP 에 대해 생성하는 초기 스토리지 VM에 대한 논리적 공간 보고를 활성화합니다.

공간이 논리적으로 보고되는 경우 ONTAP 저장 효율성 기능으로 절약된 모든 물리적 공간도 사용된 것으로 보고되도록 볼륨 공간을 보고합니다.

AWS에서 **gp3** 디스크 지원

Cloud Volumes ONTAP 이제 9.7 릴리스부터 일반 용도 *SSD(gp3)* 디스크를 지원합니다. gp3 디스크는 광범위한 작업 부하에 대해 비용과 성능의 균형을 맞춘 가장 저렴한 SSD입니다.

"AWS에서 시스템 크기 조정" .

AWS에서는 콜드 **HDD** 디스크가 더 이상 지원되지 않습니다**.**

Cloud Volumes ONTAP 더 이상 Cold HDD(sc1) 디스크를 지원하지 않습니다.

Azure 스토리지 계정용 **TLS 1.2**

BlueXP Azure에서 Cloud Volumes ONTAP 용 스토리지 계정을 생성할 때 스토리지 계정의 TLS 버전은 이제 1.2입니다.

2021년 3월 8일

Connector 3.9.4 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Cloud Volumes ONTAP 9.9.0

이제 BlueXP Cloud Volumes ONTAP 9.9.0을 배포하고 관리할 수 있습니다.

"이번 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 알아보세요." .

AWS C2S 환경 지원

이제 AWS Commercial Cloud Services(C2S) 환경에 Cloud Volumes ONTAP 9.8을 배포할 수 있습니다.

"AWS Secret Cloud 또는 AWS Top Secret Cloud에 Cloud Volumes ONTAP 배포" .

고객 관리 CMK를 사용한 AWS 암호화

BlueXP 사용하면 AWS Key Management Service(KMS)를 사용하여 Cloud Volumes ONTAP 데이터를 암호화할 수 있습니다. Cloud Volumes ONTAP 9.9.0부터 고객 관리 CMK를 선택하면 EBS 디스크의 데이터와 S3에 계층화된 데이터가 암호화됩니다. 이전에는 EBS 데이터만 암호화되었습니다.

CMK를 사용하려면 Cloud Volumes ONTAP IAM 역할에 액세스 권한을 제공해야 합니다.

"Cloud Volumes ONTAP 사용하여 AWS KMS를 설정하는 방법에 대해 자세히 알아보세요." .

Azure DoD 지원

이제 Azure 국방부(DoD) 영향 수준 6(IL6)에 Cloud Volumes ONTAP 9.8을 배포할 수 있습니다.

Google Cloud의 IP 주소 감소

Google Cloud에서 Cloud Volumes ONTAP 9.8 이상에 필요한 IP 주소 수가 줄었습니다. 기본적으로 필요한 IP 주소가 하나 줄었습니다(클러스터 간 LIF를 노드 관리 LIF와 통합했습니다). API를 사용할 때 SVM 관리 LIF 생성을 건너뛸 수 있는 옵션도 있는데, 이를 통해 추가 IP 주소의 필요성을 줄일 수 있습니다.

"Google Cloud의 IP 주소 요구 사항에 대해 자세히 알아보세요." .

Google Cloud의 공유 VPC 지원

Google Cloud에 Cloud Volumes ONTAP HA 쌍을 배포할 때 이제 VPC-1, VPC-2, VPC-3에 대한 공유 VPC를 선택할 수 있습니다. 이전에는 VPC-0만 공유 VPC가 될 수 있었습니다. 이 변경 사항은 Cloud Volumes ONTAP 9.8 이상에서 지원됩니다.

"Google Cloud 네트워킹 요구 사항에 대해 자세히 알아보세요" .

2021년 1월 4일

Connector 3.9.2 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

AWS 아웃포스트

몇 달 전, 우리는 Cloud Volumes ONTAP 이 Amazon Web Services(AWS) Outposts Ready 지정을 달성했다고 발표했습니다. 오늘, AWS Outposts에서 BlueXP 와 Cloud Volumes ONTAP 유효성을 검증했다는 소식을 전해드리게 되어 기쁩니다.

AWS Outpost가 있는 경우 작업 환경 마법사에서 Outpost VPC를 선택하여 해당 Outpost에 Cloud Volumes ONTAP 배포할 수 있습니다. 경험은 AWS에 있는 다른 VPC와 동일합니다. 먼저 AWS Outpost에 커넥터를 배포해야 합니다.

지적해야 할 몇 가지 제한 사항이 있습니다.

- 현재 단일 노드 Cloud Volumes ONTAP 시스템만 지원됩니다.
- Cloud Volumes ONTAP 과 함께 사용할 수 있는 EC2 인스턴스는 Outpost에서 사용 가능한 인스턴스로 제한됩니다.
- 현재는 일반용 SSD(gp2)만 지원됩니다.

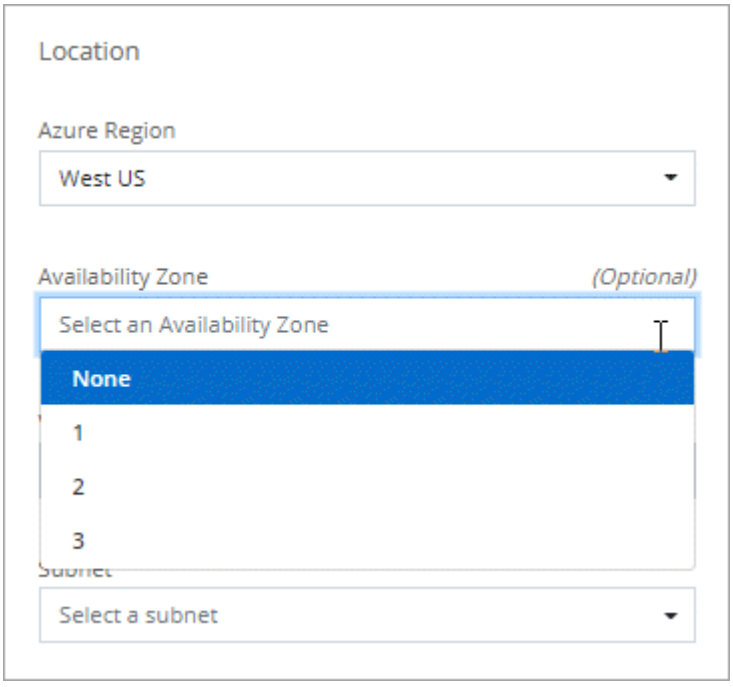
지원되는 Azure 지역의 Ultra SSD VNVRAM

Cloud Volumes ONTAP는 이제 단일 노드 시스템과 함께 E32s_v3 VM 유형을 사용할 때 Ultra SSD를 VNVRAM으로 사용할 수 있습니다 "지원되는 모든 Azure 지역에서".

VNVRAM은 더 나은 쓰기 성능을 제공합니다.

Azure에서 가용성 영역 선택

이제 단일 노드 Cloud Volumes ONTAP 시스템을 배포할 가용성 영역을 선택할 수 있습니다. AZ를 선택하지 않으면 BlueXP 대신 AZ를 선택해 드립니다.



Google Cloud의 더 큰 디스크

Cloud Volumes ONTAP는 이제 Google Cloud에서 64TB 디스크를 지원합니다.

Google Cloud 제한으로 인해 디스크만으로 구성된 최대 시스템 용량은 256TB입니다.

Google Cloud의 새로운 머신 유형

Cloud Volumes ONTAP 이제 다음과 같은 머신 유형을 지원합니다.

- Explore 라이선스와 BYOL을 사용하는 n2-standard-4
- Standard 라이선스와 BYOL을 갖춘 n2-standard-8
- 프리미엄 라이선스와 BYOL을 갖춘 n2-standard-32

2020년 11월 3일

Connector 3.9.0 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

Cloud Volumes ONTAP 용 Azure Private Link

기본적으로 BlueXP 이제 Cloud Volumes ONTAP 과 연결된 스토리지 계정 간에 Azure Private Link 연결을 활성화합니다. 개인 링크는 Azure의 엔드포인트 간 연결을 보호합니다.

- "Azure Private Links에 대해 자세히 알아보세요"
- "Cloud Volumes ONTAP 에서 Azure Private Link를 사용하는 방법에 대해 자세히 알아보세요."

알려진 제한 사항

알려진 제한 사항은 이 제품 릴리스에서 지원하지 않거나 올바르게 상호 운용되지 않는 플랫폼, 장치 또는 기능을 나타냅니다. 이러한 제한 사항을 주의 깊게 검토하세요.

이러한 제한 사항은 NetApp Console 의 Cloud Volumes ONTAP 관리에만 적용됩니다. Cloud Volumes ONTAP 소프트웨어 자체의 제한 사항을 보려면 "Cloud Volumes ONTAP 릴리스 노트로 이동" .

콘솔은 **FlexGroup** 볼륨 생성을 지원하지 않습니다.

Cloud Volumes ONTAP FlexGroup 볼륨을 지원하지만 콘솔은 현재 FlexGroup 볼륨 생성을 지원하지 않습니다. ONTAP System Manager 또는 ONTAP CLI에서 FlexGroup 볼륨을 생성하는 경우 콘솔에서 용량 관리 모드를 설정해야 합니다. `Manual` . `Automatic` FlexGroup 볼륨에서는 모드가 제대로 작동하지 않을 수 있습니다.

콘솔에서 FlexGroup 볼륨을 생성하는 기능은 향후 릴리스에서 제공될 예정입니다.

콘솔은 **Cloud Volumes ONTAP** 사용하는 **S3**를 지원하지 않습니다.

Cloud Volumes ONTAP는 스케일아웃 스토리지 옵션으로 S3를 지원하지만 Console에서는 이 기능에 대한 관리 기능을 제공하지 않습니다. 명령줄을 사용하는 것이 Cloud Volumes ONTAP에서 S3 클라이언트 액세스를 구성하는 모범 사례입니다. 자세한 내용은 "ONTAP S3 구성 파워 가이드"을 참조하십시오.

"Cloud Volumes ONTAP의 ONTAP S3 및 기타 클라이언트 프로토콜 지원에 대해 자세히 알아보십시오".

콘솔은 스토리지 **VM**에 대한 재해 복구를 지원하지 않습니다**.**

콘솔은 스토리지 VM(SVM) 재해 복구에 대한 설정이나 오케스트레이션 지원을 제공하지 않습니다. ONTAP 시스템 관리자나 ONTAP CLI를 사용해야 합니다.

"SVM 재해 복구에 대해 자세히 알아보세요" .

Cloud Volumes ONTAP 릴리스 노트

Cloud Volumes ONTAP 릴리스 노트는 릴리스별 정보를 제공합니다. 이번 릴리스의 새로운 기능, 지원되는 구성, 저장 용량 한도, 그리고 제품 기능에 영향을 미칠 수 있는 알려진 제한 사항이나 문제점에 대한 설명입니다.

"Cloud Volumes ONTAP 릴리스 노트로 이동"

시작하기

Cloud Volumes ONTAP 에 대해 알아보세요

Cloud Volumes ONTAP 사용하면 데이터 보호, 보안 및 규정 준수를 강화하는 동시에 클라우드 스토리지 비용과 성능을 최적화할 수 있습니다.

Cloud Volumes ONTAP 클라우드에서 ONTAP 데이터 관리 소프트웨어를 실행하는 소프트웨어 전용 스토리지 어플라이언스입니다. 다음과 같은 주요 기능을 갖춘 엔터프라이즈급 스토리지를 제공합니다.

- 저장 효율성

  내장된 데이터 중복 제거, 데이터 압축, 씬 프로비저닝, 복제 기능을 활용하여 스토리지 비용을 최소화합니다.

- 고가용성

  클라우드 환경에서 장애가 발생하더라도 기업의 안정성과 지속적인 운영을 보장하세요.

- 데이터 보호

  Cloud Volumes ONTAP NetApp의 업계 최고 복제 기술인 SnapMirror 활용하여 온프레미스 데이터를 클라우드에 복제하므로 여러 사용 사례에 사용할 수 있는 보조 사본을 쉽게 확보할 수 있습니다.

  Cloud Volumes ONTAP NetApp Backup and Recovery 와 통합되어 클라우드 데이터의 보호 및 장기 보관을 위한 백업 및 복원 기능을 제공합니다.

  "백업 및 복구에 대해 자세히 알아보세요"

- 데이터 계층화

  애플리케이션을 오프라인으로 전환하지 않고도 필요에 따라 고성능 및 저성능 스토리지 풀을 전환할 수 있습니다.

- 애플리케이션 일관성

  NetApp SnapCenter 사용하여 NetApp Snapshot 복사본의 일관성을 보장합니다.

  "SnapCenter 에 대해 자세히 알아보세요"

- 데이터 보안

  Cloud Volumes ONTAP 데이터 암호화를 지원하고 바이러스 및 랜섬웨어로부터 보호합니다.

- 개인정보 보호 규정 준수 제어

  NetApp Data Classification 와의 통합을 통해 데이터 컨텍스트를 이해하고 중요한 데이터를 식별하는 데 도움이 됩니다.

  "데이터 분류에 대해 자세히 알아보세요"

ONTAP 기능 라이선스는 Cloud Volumes ONTAP 에 포함되어 있습니다.

"지원되는 Cloud Volumes ONTAP 구성 보기"

"Cloud Volumes ONTAP 에 대해 자세히 알아보세요"

Cloud Volumes ONTAP 배포에 지원되는 ONTAP 버전

NetApp Console 사용하면 Cloud Volumes ONTAP 시스템을 추가할 때 여러 가지 ONTAP 버전 중에서 선택할 수 있습니다.

여기에 나열된 버전 이외의 Cloud Volumes ONTAP 버전은 신규 배포에 사용할 수 없습니다. 릴리스에 표시된 패치 버전 또는 일반(General Availability) 버전은 배포에 사용할 수 있는 기본 버전을 나타냅니다. 사용 가능한 패치에 대한 자세한 내용은 각 릴리스의 "버전별 릴리스 노트"를 참조하십시오.

업그레이드에 대한 자세한 내용은 "지원되는 업그레이드 경로"을(를) 참조하십시오.

AWS

단일 노드

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

HA 쌍

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1

- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

하늘빛

단일 노드

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

HA 쌍

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

구글 클라우드

단일 노드

- 9.18.1
- 9.17.1 P1

- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HA 쌍

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

Amazon Web Services에서 시작하세요

AWS에서 Cloud Volumes ONTAP 빠르게 시작하세요

몇 단계만 거치면 AWS에서 Cloud Volumes ONTAP 시작할 수 있습니다.

1 콘솔 에이전트 만들기

만약 당신이 없다면 "콘솔 에이전트" 하지만, 하나는 만들어야 합니다. "AWS에서 콘솔 에이전트를 만드는 방법을 알아보세요" .

인터넷 접속이 불가능한 서브넷에 Cloud Volumes ONTAP 배포하려면 콘솔 에이전트를 수동으로 설치하고 해당 콘솔 에이전트에서 실행되는 NetApp Console 사용자 인터페이스에 액세스해야 합니다. "인터넷 접속이 불가능한 위치에 콘솔 에이전트를 수동으로 설치하는 방법을 알아보세요." .

2 구성을 계획하세요

콘솔은 사용자의 작업 부하 요구 사항에 맞는 미리 구성된 패키지를 제공하거나 사용자가 직접 구성을 만들 수도 있습니다. 원하는 구성을 선택하는 경우, 사용 가능한 옵션을 이해해야 합니다. "자세히 알아보기" .

3 네트워킹을 설정하세요

1. VPC와 서브넷이 콘솔 에이전트와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인하세요.
2. NetApp AutoSupport 에 대해 대상 VPC에서 아웃바운드 인터넷 액세스를 활성화합니다.

   인터넷 접속이 불가능한 위치에 Cloud Volumes ONTAP 배포하는 경우 이 단계는 필요하지 않습니다.

3. Amazon Simple Storage Service(Amazon S3) 서비스에 대한 VPC 엔드포인트를 설정합니다.

   Cloud Volumes ONTAP 에서 저비용 개체 스토리지로 콜드 데이터를 계층화하려면 VPC 엔드포인트가 필요합니다.

"네트워킹 요구 사항에 대해 자세히 알아보세요" .

4 **AWS KMS** 설정

Cloud Volumes ONTAP 과 함께 Amazon 암호화를 사용하려면 활성 고객 마스터 키(CMK)가 있는지 확인해야 합니다. 또한 콘솔 에이전트에 대한 권한을 제공하는 IAM 역할을 _키 사용자_로 추가하여 각 CMK에 대한 키 정책을 수정해야 합니다. "자세히 알아보기" .

5 콘솔을 사용하여 **Cloud Volumes ONTAP** 실행

*시스템 추가*를 클릭하고 배포하려는 시스템 유형을 선택한 다음 마법사의 단계를 완료합니다. "단계별 지침을 읽어보세요" .

관련 링크

- "AWS용 콘솔 에이전트 만들기"
- "AWS Marketplace에서 콘솔 에이전트 만들기"
- "온프레미스에 콘솔 에이전트 설치 및 설정"
- "콘솔 에이전트에 대한 AWS 권한"

AWS에서 Cloud Volumes ONTAP 구성을 계획하세요

AWS에 Cloud Volumes ONTAP 배포하는 경우 워크로드 요구 사항에 맞는 미리 구성된 시스템을 선택하거나 고유한 구성을 만들 수 있습니다. 원하는 구성을 선택하는 경우, 사용 가능한 옵션을 이해해야 합니다.

Cloud Volumes ONTAP 라이선스를 선택하세요

Cloud Volumes ONTAP 에는 여러 가지 라이선싱 옵션이 제공됩니다. 각 옵션을 통해 귀하의 필요에 맞는 소비 모델을 선택할 수 있습니다.

- "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요"
- "라이선싱 설정 방법 알아보기"

지원되는 지역을 선택하세요

Cloud Volumes ONTAP 대부분의 AWS 지역에서 지원됩니다. "지원되는 지역의 전체 목록 보기" .

새로운 AWS 지역은 해당 지역에서 리소스를 생성하고 관리하기 전에 활성화해야 합니다. "AWS 설명서: 리전을 활성화하는 방법 알아보기" .

지원되는 로컬 영역을 선택하세요

로컬 존을 선택하는 것은 선택 사항입니다. Cloud Volumes ONTAP 싱가포르를 포함한 일부 AWS 로컬 영역에서 지원됩니다. AWS의 Cloud Volumes ONTAP 단일 가용성 영역에서만 고가용성(HA) 모드를 지원합니다. 단일 노드 배포는 지원되지 않습니다.

> Cloud Volumes ONTAP AWS 로컬 영역에서 데이터 계층화 및 클라우드 계층화를 지원하지 않습니다. 또한, Cloud Volumes ONTAP 에 적합하지 않은 인스턴스가 있는 로컬 영역은 지원되지 않습니다. 이에 대한 예는 마이애미인데, 지원되지 않고 적격하지 않은 Gen6 인스턴스만 있기 때문에 로컬 영역으로 사용할 수 없습니다.

"AWS 문서: 로컬 영역 전체 목록 보기" . 로컬 영역을 활성화해야만 해당 영역에서 리소스를 만들고 관리할 수 있습니다.

"AWS 설명서: AWS 로컬 영역 시작하기" .

지원되는 인스턴스를 선택하세요

Cloud Volumes ONTAP 선택한 라이선스 유형에 따라 여러 인스턴스 유형을 지원합니다.

"AWS의 Cloud Volumes ONTAP 에 지원되는 구성"

저장 한도 이해하기

Cloud Volumes ONTAP 시스템의 원시 용량 제한은 라이선스에 따라 결정됩니다. 추가적인 제한은 골재와 부피의 크기에 영향을 미칩니다. 구성을 계획할 때 이러한 제한 사항을 알고 있어야 합니다.

"AWS의 Cloud Volumes ONTAP 대한 스토리지 한도"

AWS에서 시스템 크기 조정

Cloud Volumes ONTAP 시스템의 크기를 조정하면 성능 및 용량 요구 사항을 충족하는 데 도움이 될 수 있습니다. 인스턴스 유형, 디스크 유형 및 디스크 크기를 선택할 때 몇 가지 핵심 사항을 알아야 합니다.

인스턴스 유형

- 각 EC2 인스턴스 유형에 대한 최대 처리량 및 IOPS에 맞게 워크로드 요구 사항을 조정하세요.
- 여러 사용자가 동시에 시스템에 쓰는 경우 요청을 관리할 수 있는 충분한 CPU가 있는 인스턴스 유형을 선택하세요.
- 주로 읽기 작업을 하는 애플리케이션을 사용하는 경우, 충분한 RAM을 갖춘 시스템을 선택하세요.
  - "AWS 설명서: Amazon EC2 인스턴스 유형"
  - "AWS 설명서: Amazon EBS 최적화 인스턴스"

EBS 디스크 유형

높은 수준에서 EBS 디스크 유형 간의 차이점은 다음과 같습니다. EBS 디스크의 사용 사례에 대해 자세히 알아보려면 다음을 참조하세요. "AWS 문서: EBS 볼륨 유형" .

- 일반 용도 *SSD(gp3)* 디스크는 광범위한 작업 부하에 대해 비용과 성능의 균형을 맞춘 가장 저렴한 SSD입니다. 성능은 IOPS와 처리량으로 정의됩니다. gp3 디스크는 Cloud Volumes ONTAP 9.7 이상에서 지원됩니다.

  gp3 디스크를 선택하면 NetApp Console 선택한 디스크 크기를 기준으로 gp2 디스크와 동등한 성능을 제공하는 기본 IOPS 및 처리량 값을 입력합니다. 더 높은 비용으로 더 나은 성능을 얻으려면 값을 늘릴 수 있지만, 낮은 값은 성능이 저하될 수 있으므로 지원하지 않습니다. 간단히 말해, 기본값을 고수하거나 기본값을 늘리세요. 낮추지 마세요. "AWS 문서: gp3 디스크와 성능에 대해 자세히 알아보세요" .

  Cloud Volumes ONTAP gp3 디스크를 사용하는 Amazon EBS Elastic Volumes 기능을 지원합니다. "Elastic Volumes 지원에 대해 자세히 알아보세요" .

- 일반 용도 *SSD(gp2)* 디스크는 광범위한 작업 부하에 대해 비용과 성능의 균형을 맞춥니다. 성능은 IOPS로 정의됩니다.
- 프로비저닝된 *IOPS SSD(io1)* 디스크는 더 높은 비용으로 최고의 성능을 필요로 하는 중요한 애플리케이션을 위한 것입니다.

  Cloud Volumes ONTAP io1 디스크를 사용하여 Amazon EBS Elastic Volumes 기능을 지원합니다. "Elastic Volumes 지원에 대해 자세히 알아보세요" .

- 처리량 최적화 *HDD(st1)* 디스크는 저렴한 가격으로 빠르고 일관된 처리량이 필요한 자주 액세스되는 워크로드에 적합합니다.

> ⓘ Cloud Volumes ONTAP 시스템이 AWS Local Zone에 있는 경우 Amazon Simple Storage Service(Amazon S3)로의 데이터 계층화는 지원되지 않습니다. Local Zone 외부의 Amazon S3 버킷에 액세스하면 지연 시간이 길어지고 Cloud Volumes ONTAP 활동에 영향을 미치기 때문입니다.

EBS 디스크 크기

지원하지 않는 구성을 선택하는 경우"Amazon EBS Elastic Volumes 기능" , Cloud Volumes ONTAP 시스템을 시작할 때 초기 디스크 크기를 선택해야 합니다. 그 후에는 할 수 있습니다"콘솔이 시스템 용량을 관리하도록 하세요" , 하지만 당신이 원한다면"직접 집계를 생성하세요" 다음 사항을 주의하세요.

- 집계된 모든 디스크의 크기는 동일해야 합니다.
- EBS 디스크의 성능은 디스크 크기에 따라 달라집니다. 크기는 SSD 디스크의 기준 IOPS와 최대 버스트 지속 시간을 결정하고, HDD 디스크의 기준 및 버스트 처리량을 결정합니다.
- 궁극적으로, 필요한 _지속적인 성능_을 제공하는 디스크 크기를 선택해야 합니다.
- 더 큰 디스크(예: 4TiB 디스크 6개)를 선택하더라도 EC2 인스턴스가 대역폭 제한에 도달할 수 있으므로 모든 IOPS를 얻지 못할 수 있습니다.

  EBS 디스크 성능에 대한 자세한 내용은 다음을 참조하세요. "AWS 문서: EBS 볼륨 유형" .

  위에서 언급한 대로 Amazon EBS Elastic Volumes 기능을 지원하는 Cloud Volumes ONTAP 구성에서는 디스크 크기를 선택할 수 없습니다. "Elastic Volumes 지원에 대해 자세히 알아보세요" .

기본 시스템 디스크 보기

사용자 데이터 저장 외에도 콘솔은 Cloud Volumes ONTAP 시스템 데이터(부팅 데이터, 루트 데이터, 코어 데이터 및 NVRAM)를 위한 클라우드 스토리지도 구매합니다. 계획을 세우려면 Cloud Volumes ONTAP 배포하기 전에 이러한 세부 정보를 검토하는 것이 도움이 될 수 있습니다.

"AWS에서 Cloud Volumes ONTAP 시스템 데이터의 기본 디스크 보기" .

콘솔 에이전트에도 시스템 디스크가 필요합니다. "콘솔 에이전트의 기본 구성에 대한 세부 정보 보기" .

AWS Outpost에 **Cloud Volumes ONTAP** 배포 준비

AWS Outpost가 있는 경우 배포 프로세스 중에 Outpost VPC를 선택하여 해당 Outpost에 Cloud Volumes ONTAP 배포할 수 있습니다. 경험은 AWS에 있는 다른 VPC와 동일합니다. 먼저 AWS Outpost에 콘솔 에이전트를 배포해야 합니다.

지적해야 할 몇 가지 제한 사항이 있습니다.

- 현재 단일 노드 Cloud Volumes ONTAP 시스템만 지원됩니다.
- Cloud Volumes ONTAP 과 함께 사용할 수 있는 EC2 인스턴스는 Outpost에서 사용 가능한 인스턴스로 제한됩니다.
- 현재는 일반용 SSD(gp2)만 지원됩니다.

네트워킹 정보 수집

AWS에서 Cloud Volumes ONTAP 시작할 때 VPC 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

단일 **AZ**의 단일 노드 또는 **HA** 쌍

AWS 정보	당신의 가치
지역	
VPC	
서브넷	

AWS 정보	당신의 가치
보안 그룹(자체 보안 그룹을 사용하는 경우)	

여러 AZ의 HA 쌍

AWS 정보	당신의 가치
지역	
VPC	
보안 그룹(자체 보안 그룹을 사용하는 경우)	
노드 1 가용성 영역	
노드 1 서브넷	
노드 2 가용성 영역	
노드 2 서브넷	
중재자 가용성 영역	
중재자 서브넷	
중재자를 위한 키 쌍	
클러스터 관리 포트에 대한 유동 IP 주소	
노드 1의 데이터에 대한 유동 IP 주소	
노드 2의 데이터에 대한 플로팅 IP 주소	
플로팅 IP 주소에 대한 경로 테이블	

쓰기 속도를 선택하세요

콘솔을 사용하면 Cloud Volumes ONTAP 에 대한 쓰기 속도 설정을 선택할 수 있습니다. 쓰기 속도를 선택하기 전에 일반 설정과 높은 설정의 차이점, 높은 쓰기 속도를 사용할 때의 위험과 권장 사항을 이해해야 합니다. "쓰기 속도에 대해 자세히 알아보세요" .

볼륨 사용 프로필을 선택하세요

ONTAP 에는 필요한 총 저장 용량을 줄일 수 있는 여러 가지 저장 효율성 기능이 포함되어 있습니다. 콘솔에서 볼륨을 생성할 때 이러한 기능을 활성화하는 프로필이나 비활성화하는 프로필을 선택할 수 있습니다. 어떤 프로필을 사용할지 결정하는 데 도움이 되도록 이러한 기능에 대해 자세히 알아보세요.

NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

씬 프로비저닝

실제 물리적 스토리지 풀에 있는 것보다 더 많은 논리적 스토리지를 호스트나 사용자에게 제공합니다. 저장 공간을 미리 할당하는 대신, 데이터가 기록됨에 따라 각 볼륨에 저장 공간이 동적으로 할당됩니다.

중복제거

동일한 데이터 블록을 찾아 단일 공유 블록에 대한 참조로 대체하여 효율성을 향상시킵니다. 이 기술은 동일한 볼륨에 있는 중복된 데이터 블록을 제거하여 저장 용량 요구 사항을 줄입니다.

압축

1차, 2차, 보관 저장소의 볼륨 내 데이터를 압축하여 데이터를 저장하는 데 필요한 물리적 용량을 줄입니다.

네트워킹을 설정하세요

Cloud Volumes ONTAP 에 대한 **AWS** 네트워킹 설정

NetApp Console IP 주소, 넷마스크, 경로 등 Cloud Volumes ONTAP 의 네트워킹 구성 요소를 설정합니다. 아웃바운드 인터넷 접속이 가능한지, 충분한 개인 IP 주소가 사용 가능한지, 올바른 연결이 설정되어 있는지 등을 확인해야 합니다.

일반 요구 사항

AWS에서 다음 요구 사항을 충족했는지 확인하세요.

Cloud Volumes ONTAP 노드에 대한 아웃바운드 인터넷 액세스

Cloud Volumes ONTAP 시스템은 다양한 기능을 위해 외부 엔드포인트에 액세스하기 위해 아웃바운드 인터넷 액세스가 필요합니다. 엄격한 보안 요구 사항이 있는 환경에서 이러한 엔드포인트가 차단되면 Cloud Volumes ONTAP 제대로 작동할 수 없습니다.

콘솔 에이전트는 일상 업무를 위해 여러 엔드포인트에 연결합니다. 사용된 엔드포인트에 대한 정보는 다음을 참조하세요. "콘솔 에이전트에서 연결된 엔드포인트 보기" 그리고 "콘솔 사용을 위한 네트워킹 준비" .

Cloud Volumes ONTAP 엔드포인트

Cloud Volumes ONTAP 이러한 엔드포인트를 사용하여 다양한 서비스와 통신합니다.

엔드포인트	적용 가능	목적	배포 모드	엔드포인트를 사용할 수 없는 경우의 영향
\ https://netapp-cloud-account.auth0.com	입증	콘솔에서 인증에 사용됩니다.	표준 모드와 제한 모드.	사용자 인증에 실패하고 다음 서비스를 계속 사용할 수 없습니다. • Cloud Volumes ONTAP 서비스 • ONTAP 서비스 • 프로토콜 및 프록시 서비스

엔드포인트	적용 가능	목적	배포 모드	엔드포인트를 사용할 수 없는 경우의 영향
\ https://api.bluexp.netapp.com/tenancy	차용	콘솔에서 Cloud Volumes ONTAP 리소스를 검색하여 리소스와 사용자에게 권한을 부여하는 데 사용됩니다.	표준 모드와 제한 모드.	Cloud Volumes ONTAP 리소스와 사용자는 권한이 없습니다.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	AutoSupport 원격 측정 데이터를 NetApp 지원팀으로 전송하는 데 사용됩니다.	표준 모드와 제한 모드.	AutoSupport 정보가 전달되지 않았습니다.
AWS 서비스의 정확한 상업적 종점(접미사 포함) `amazonaws.com`)는 사용하는 AWS 지역에 따라 다릅니다. 를 참조하세요 "자세한 내용은 AWS 설명서를 참조하세요." .	• 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • Amazon Simple Storage Service(S3)	AWS 서비스와의 통신.	표준 모드와 개인 모드.	Cloud Volumes ONTAP AWS 서비스와 통신하여 AWS에서 특정 작업을 수행할 수 없습니다.
AWS 서비스에 대한 정확한 정부 엔드포인트는 사용 중인 AWS 지역에 따라 달라집니다. 끝점에는 접미사가 붙습니다. `amazonaws.com` 그리고 `c2s.ic.gov` . 참조하다 "AWS SDK" 그리고 "AWS 문서" 자세한 내용은.	• 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 서비스와의 통신.	제한 모드.	Cloud Volumes ONTAP AWS 서비스와 통신하여 AWS에서 특정 작업을 수행할 수 없습니다.

HA 중재자를 위한 아웃바운드 인터넷 액세스

HA 중재자 인스턴스는 스토리지 장애 조치를 지원할 수 있도록 AWS EC2 서비스에 대한 아웃바운드 연결이 있어야 합니다. 연결을 제공하려면 공용 IP 주소를 추가하거나, 프록시 서버를 지정하거나, 수동 옵션을 사용할 수 있습니다.

수동 옵션은 대상 서브넷에서 AWS EC2 서비스로 연결되는 NAT 게이트웨이 또는 인터페이스 VPC 엔드포인트가 될 수 있습니다. VPC 엔드포인트에 대한 자세한 내용은 다음을 참조하세요. "AWS 설명서: VPC 엔드포인트 인터페이스(AWS PrivateLink)" .

NetApp Console 에이전트의 네트워크 프록시 구성

NetApp Console 에이전트의 프록시 서버 구성을 사용하여 Cloud Volumes ONTAP 에서 아웃바운드 인터넷 액세스를 활성화할 수 있습니다. 콘솔은 두 가지 유형의 프록시를 지원합니다.

- 명시적 프록시: Cloud Volumes ONTAP 의 아웃바운드 트래픽은 콘솔 에이전트의 프록시 구성 중에 지정된 프록시 서버의 HTTP 주소를 사용합니다. 관리자는 추가 인증을 위해 사용자 자격 증명과 루트 CA 인증서를 구성했을 수도 있습니다. 명시적 프록시에 대해 루트 CA 인증서를 사용할 수 있는 경우 다음을 사용하여 동일한 인증서를 Cloud Volumes ONTAP 시스템에 가져와 업로드해야 합니다. "ONTAP CLI: 보안 인증서 설치" 명령.
- 투명 프록시: 네트워크는 콘솔 에이전트의 프록시를 통해 Cloud Volumes ONTAP 에서 아웃바운드 트래픽을 자동으로 라우팅하도록 구성됩니다. 투명 프록시를 설정할 때 관리자는 프록시 서버의 HTTP 주소가 아닌 Cloud Volumes ONTAP 에서의 연결을 위한 루트 CA 인증서만 제공하면 됩니다. 다음을 사용하여 Cloud Volumes ONTAP 시스템에 동일한 루트 CA 인증서를 가져와 업로드해야 합니다. "ONTAP CLI: 보안 인증서 설치" 명령.

프록시 서버 구성에 대한 정보는 다음을 참조하세요. "프록시 서버를 사용하도록 콘솔 에이전트 구성" .

개인 IP 주소

콘솔은 필요한 수의 개인 IP 주소를 Cloud Volumes ONTAP 에 자동으로 할당합니다. 네트워크에 사용 가능한 개인 IP 주소가 충분한지 확인해야 합니다.

Console에서 Cloud Volumes ONTAP에 할당하는 LIF 수는 단일 노드 시스템을 배포하는지 또는 HA 쌍을 배포하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다.

단일 노드 시스템의 IP 주소

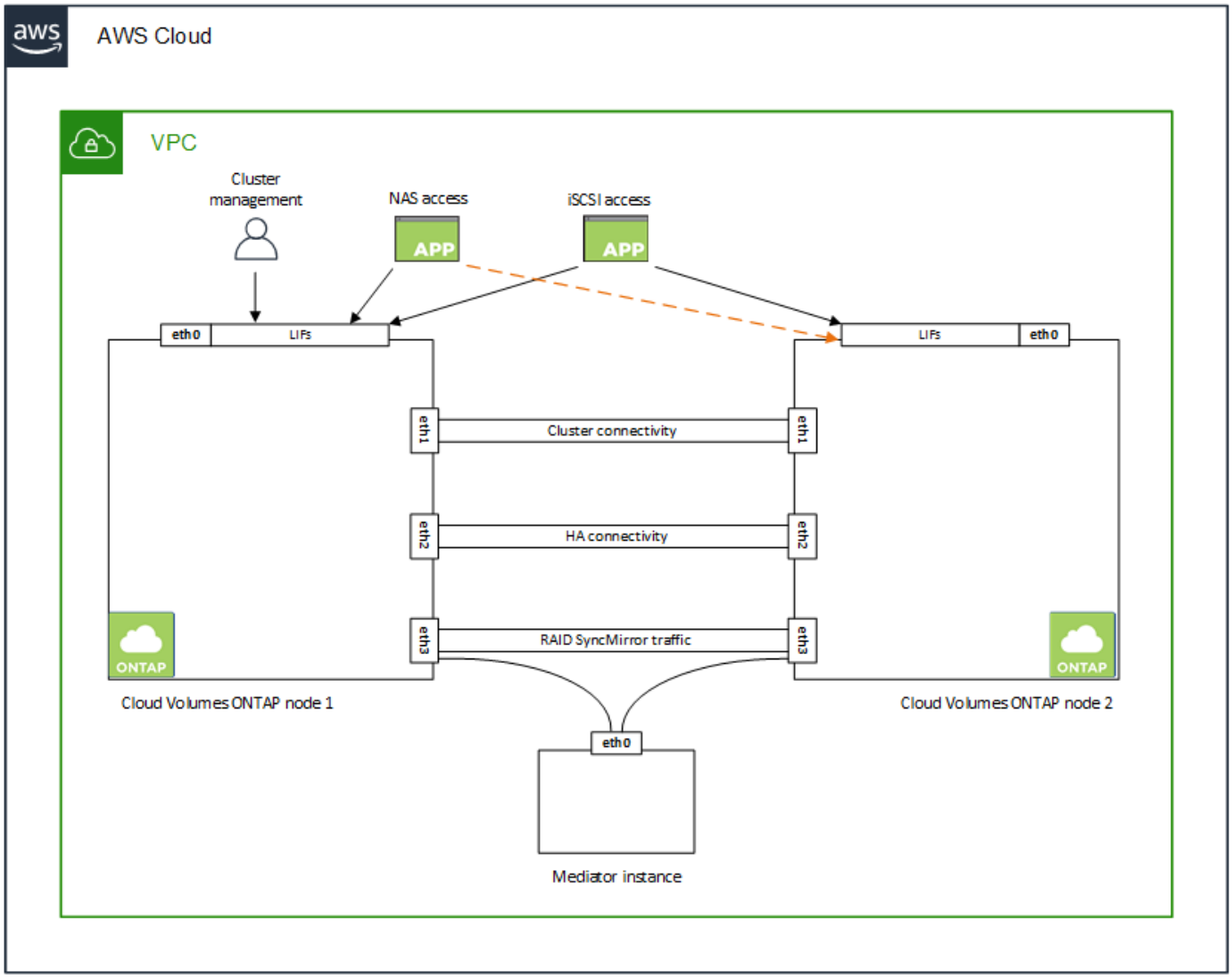
NetApp Console은 단일 노드 시스템에 6개의 IP 주소를 할당합니다.

다음 표는 각 개인 IP 주소와 연결된 LIF에 대한 세부 정보를 제공합니다.

라이프	목적
클러스터 관리	전체 클러스터(HA 쌍)의 관리.
노드 관리	노드의 관리.
클러스터 간	클러스터 간 통신, 백업 및 복제.
NAS 데이터	NAS 프로토콜을 통한 클라이언트 접근.
iSCSI 데이터	iSCSI 프로토콜을 통한 클라이언트 액세스. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에도 사용됩니다. 이 LIF는 필수이므로 삭제하면 안 됩니다.
스토리지 VM 관리	스토리지 VM 관리 LIF는 SnapCenter 와 같은 관리 도구와 함께 사용됩니다.

HA 쌍의 IP 주소

HA 쌍은 단일 노드 시스템보다 더 많은 IP 주소가 필요합니다. 이러한 IP 주소는 다음 이미지에 표시된 것처럼 여러 이더넷 인터페이스에 분산됩니다.



HA 쌍에 필요한 개인 IP 주소 수는 선택한 배포 모델에 따라 달라집니다. 단일 AWS 가용성 영역(AZ)에 배포된 HA 쌍에는 15개의 개인 IP 주소가 필요하고, 여러 AZ에 배포된 HA 쌍에는 13개의 개인 IP 주소가 필요합니다.

다음 표에서는 각 개인 IP 주소와 연결된 LIF에 대한 세부 정보를 제공합니다.

라이프	인터페이스	마디	목적
클러스터 관리	eth0	노드 1	전체 클러스터(HA 쌍)의 관리.
노드 관리	eth0	노드 1과 노드 2	노드의 관리.
클러스터 간	eth0	노드 1과 노드 2	클러스터 간 통신, 백업 및 복제.
NAS 데이터	eth0	노드 1	NAS 프로토콜을 통한 클라이언트 접근.
iSCSI 데이터	eth0	노드 1과 노드 2	iSCSI 프로토콜을 통한 클라이언트 액세스. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에도 사용됩니다. 이러한 LIF는 필수이므로 삭제하면 안 됩니다.
클러스터 연결성	eth1	노드 1과 노드 2	클러스터 내에서 노드가 서로 통신하고 데이터를 이동할 수 있도록 합니다.
HA 연결	eth2	노드 1과 노드 2	장애 조치 시 두 노드 간의 통신.

라이프	인터페이스	마디	목적
RSM iSCSI 트래픽	eth3	노드 1과 노드 2	RAID SyncMirror iSCSI 트래픽과 두 Cloud Volumes ONTAP 노드와 중재자 간의 통신입니다.
중재인	eth0	중재인	저장소 인수 및 반환 프로세스를 지원하기 위한 노드와 중재자 간의 통신 채널입니다.

라이프	인터페이스	마디	목적
노드 관리	eth0	노드 1과 노드 2	노드의 관리.
클러스터 간	eth0	노드 1과 노드 2	클러스터 간 통신, 백업 및 복제.
iSCSI 데이터	eth0	노드 1과 노드 2	iSCSI 프로토콜을 통한 클라이언트 액세스. 이러한 LIF는 노드 간의 플로팅 IP 주소 마이그레이션도 관리합니다. 이러한 LIF는 필수이므로 삭제하면 안 됩니다.
클러스터 연결성	eth1	노드 1과 노드 2	클러스터 내에서 노드가 서로 통신하고 데이터를 이동할 수 있도록 합니다.
HA 연결	eth2	노드 1과 노드 2	장애 조치 시 두 노드 간의 통신.
RSM iSCSI 트래픽	eth3	노드 1과 노드 2	RAID SyncMirror iSCSI 트래픽과 두 Cloud Volumes ONTAP 노드와 중재자 간의 통신입니다.
중재인	eth0	중재인	저장소 인수 및 반환 프로세스를 지원하기 위한 노드와 중재자 간의 통신 채널입니다.

여러 가용성 영역에 배포되는 경우 여러 LIF가 연결됩니다."유동 IP 주소" AWS 개인 IP 제한에 포함되지 않습니다.

보안 그룹

콘솔이 보안 그룹을 자동으로 생성하므로 직접 보안 그룹을 만들 필요가 없습니다. 자신의 것을 사용해야 하는 경우 다음을 참조하세요."보안 그룹 규칙" .

콘솔 에이전트에 대한 정보를 찾고 계신가요? "콘솔 에이전트에 대한 보안 그룹 규칙 보기"

데이터 계층화를 위한 연결

EBS를 성능 계층으로, Amazon S3를 용량 계층으로 사용하려면 Cloud Volumes ONTAP이 S3에 연결되어 있어야 합니다. 이 연결을 제공하는 가장 좋은 방법은 S3 서비스에 대한 VPC 엔드포인트를 생성하는 것입니다. 지침은 "AWS 설명서: 게이트웨이 엔드포인트 생성"을 참조하십시오.

VPC 엔드포인트를 생성할 때 Cloud Volumes ONTAP 인스턴스에 해당하는 지역, VPC 및 경로 테이블을 선택해야 합니다. 또한 S3 엔드포인트로의 트래픽을 활성화하는 아웃바운드 HTTPS 규칙을 추가하려면 보안 그룹을 수정해야 합니다. 그렇지 않으면 Cloud Volumes ONTAP 이 S3 서비스에 연결할 수 없습니다.

문제가 발생하면 다음을 참조하세요. "AWS 지원 지식 센터: 게이트웨이 VPC 엔드포인트를 사용하여 S3 버킷에 연결할 수 없는 이유는 무엇입니까?"

ONTAP 시스템에 대한 연결

AWS의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 AWS VPC와 다른 네트워크(예: 회사 네트워크) 간에 VPN 연결이 필요합니다. 지침은 다음을 참조하세요. "AWS 설명서: AWS VPN 연결 설정" .

CIFS용 **DNS** 및 **Active Directory**

CIFS 스토리지를 프로비저닝하려면 AWS에서 DNS와 Active Directory를 설정하거나 온프레미스 설정을 AWS로 확장해야 합니다.

DNS 서버는 Active Directory 환경에 대한 이름 확인 서비스를 제공해야 합니다. Active Directory 환경에서 사용되는 DNS 서버가 아닌 기본 EC2 DNS 서버를 사용하도록 DHCP 옵션 세트를 구성할 수 있습니다.

지침은 다음을 참조하세요. "AWS 설명서: AWS 클라우드의 Active Directory 도메인 서비스: 빠른 시작 참조 배포" .

VPC 공유

9.11.1 릴리스부터 VPC 공유를 통해 AWS에서 Cloud Volumes ONTAP HA 쌍이 지원됩니다. VPC 공유를 사용하면 조직에서 다른 AWS 계정과 서브넷을 공유할 수 있습니다. 이 구성을 사용하려면 AWS 환경을 설정한 다음 API를 사용하여 HA 쌍을 배포해야 합니다.

"공유 서브넷에 HA 쌍을 배포하는 방법을 알아보세요." .

여러 **AZ**의 **HA** 쌍에 대한 요구 사항

여러 가용성 영역(AZ)을 사용하는 Cloud Volumes ONTAP HA 구성에는 추가 AWS 네트워킹 요구 사항이 적용됩니다. Cloud Volumes ONTAP 시스템을 추가할 때 콘솔에 네트워킹 세부 정보를 입력해야 하므로 HA 쌍을 시작하기 전에 이러한 요구 사항을 검토해야 합니다.

HA 쌍이 어떻게 작동하는지 이해하려면 다음을 참조하세요."고가용성 쌍" .

가용성 영역

이 HA 배포 모델은 여러 AZ를 사용하여 데이터의 높은 가용성을 보장합니다. HA 쌍 간의 통신 채널을 제공하는 각 Cloud Volumes ONTAP 인스턴스와 중재자 인스턴스에 대해 전용 AZ를 사용해야 합니다.

각 가용성 영역에서 서브넷을 사용할 수 있어야 합니다.

NAS 데이터 및 클러스터**/SVM** 관리를 위한 유동 **IP** 주소

여러 AZ의 HA 구성은 장애가 발생할 경우 노드 간에 마이그레이션되는 부동 IP 주소를 사용합니다. VPC 외부에서는 기본적으로 액세스할 수 없습니다."AWS 전송 게이트웨이 설정" .

하나의 부동 IP 주소는 클러스터 관리용이고, 하나는 노드 1의 NFS/CIFS 데이터용이고, 다른 하나는 노드 2의 NFS/CIFS 데이터용입니다. SVM 관리를 위한 네 번째 유동 IP 주소는 선택 사항입니다.

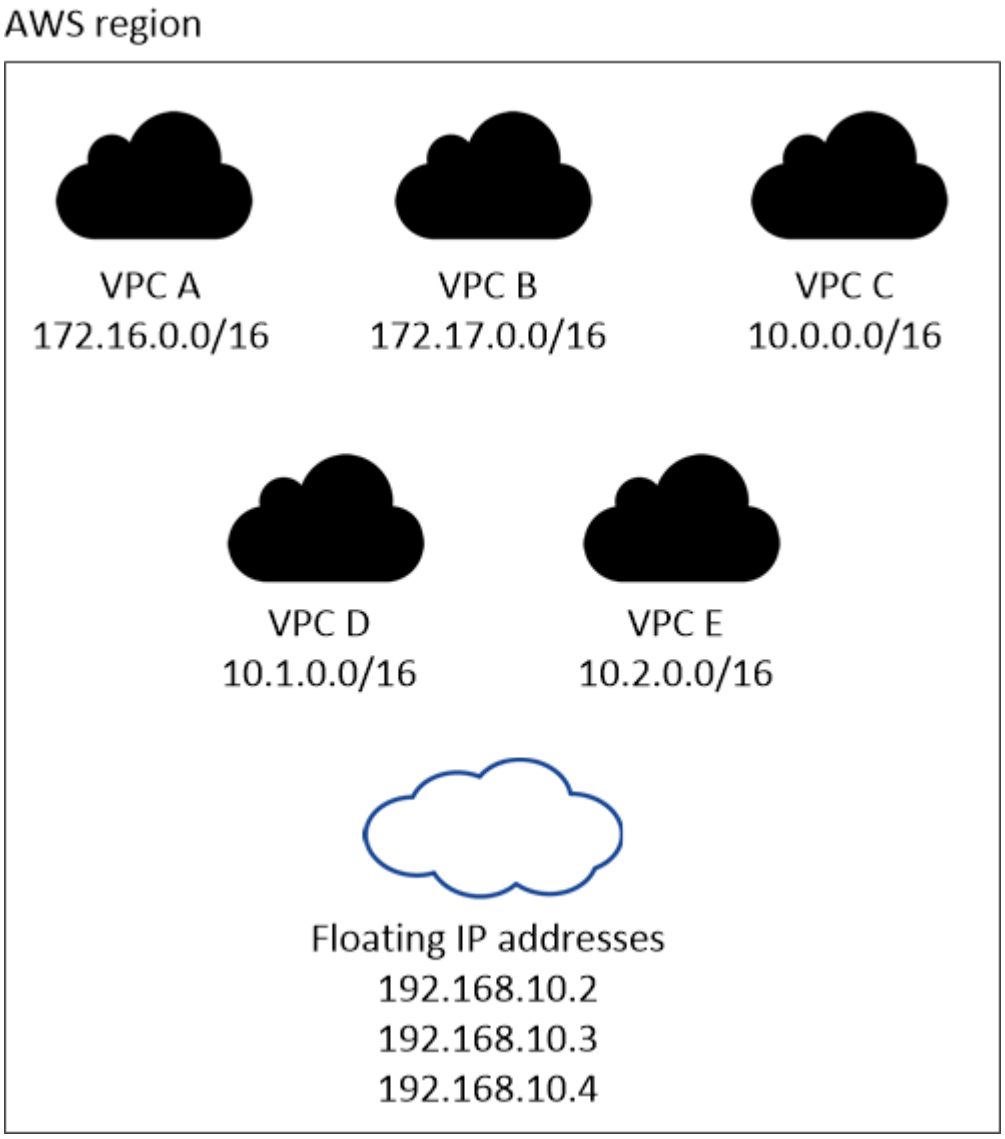
HA 쌍과 함께 Windows용 SnapDrive 또는 SnapCenter 사용하는 경우 SVM 관리 LIF에 부동 IP 주소가 필요합니다.

Cloud Volumes ONTAP HA 시스템을 추가하는 경우 유동 IP 주소를 입력해야 합니다. 콘솔은 시스템을 시작할 때 HA 쌍에 IP 주소를 할당합니다.

HA 구성을 배포하는 AWS 지역의 모든 VPC에 대한 CIDR 블록 외부에 부동 IP 주소가 있어야 합니다. 유동 IP

주소를 해당 지역의 VPC 외부에 있는 논리적 서브넷으로 생각해 보세요.

다음 예에서는 AWS 지역의 VPC와 플로팅 IP 주소 간의 관계를 보여줍니다. 플로팅 IP 주소는 모든 VPC의 CIDR 블록 외부에 있지만, 경로 테이블을 통해 서브넷으로 라우팅할 수 있습니다.



콘솔은 VPC 외부의 클라이언트에서 iSCSI 액세스와 NAS 액세스를 위해 정적 IP 주소를 자동으로 생성합니다. 이러한 유형의 IP 주소에 대해서는 어떠한 요구 사항도 충족할 필요가 없습니다.

VPC 외부에서 플로팅 **IP** 액세스를 가능하게 하는 트랜짓 게이트웨이

필요한 경우,"AWS 전송 게이트웨이 설정" HA 쌍이 있는 VPC 외부에서 HA 쌍의 부동 IP 주소에 액세스할 수 있도록 합니다.

경로 테이블

유동 IP 주소를 지정한 후에는 유동 IP 주소에 대한 경로를 포함할 경로 테이블을 선택하라는 메시지가 표시됩니다. 이를 통해 클라이언트가 HA 쌍에 액세스할 수 있습니다.

VPC의 서브넷에 대한 경로 테이블이 하나뿐인 경우(기본 경로 테이블), 콘솔은 자동으로 해당 경로 테이블에 플로팅 IP 주소를 추가합니다. 두 개 이상의 경로 테이블이 있는 경우 HA 쌍을 시작할 때 올바른 경로 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP 에 액세스하지 못할 수도

있습니다.

예를 들어, 서로 다른 경로 테이블과 연결된 두 개의 서브넷이 있을 수 있습니다. 경로 테이블 A를 선택했지만 경로 테이블 B는 선택하지 않은 경우, 경로 테이블 A에 연결된 서브넷의 클라이언트는 HA 쌍에 액세스할 수 있지만 경로 테이블 B에 연결된 서브넷의 클라이언트는 액세스할 수 없습니다.

경로 테이블에 대한 자세한 내용은 다음을 참조하세요. "AWS 문서: 라우팅 테이블" .

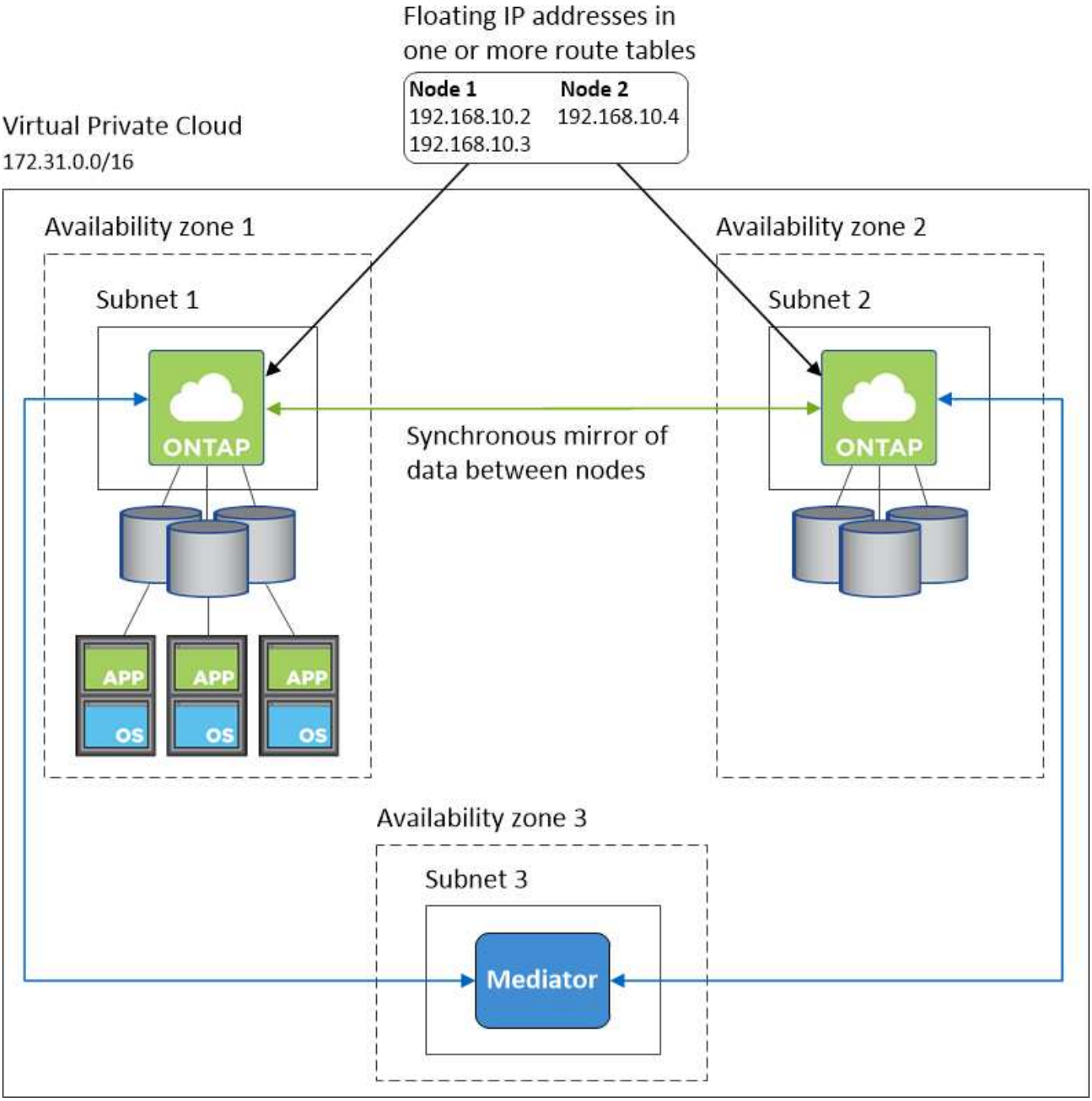
NetApp 관리 도구에 연결

여러 AZ에 있는 HA 구성에서 NetApp 관리 도구를 사용하려면 두 가지 연결 옵션이 있습니다.

1. 다른 VPC에 NetApp 관리 도구를 배포합니다."AWS 전송 게이트웨이 설정" . 게이트웨이를 사용하면 VPC 외부에서 클러스터 관리 인터페이스의 플로팅 IP 주소에 액세스할 수 있습니다.
2. NAS 클라이언트와 유사한 라우팅 구성을 사용하여 동일한 VPC에 NetApp 관리 도구를 배포합니다.

HA 구성 예시

다음 이미지는 여러 AZ의 HA 쌍에 특정한 네트워킹 구성 요소를 보여줍니다. 즉, 3개의 가용성 영역, 3개의 서브넷, 부동 IP 주소 및 경로 테이블입니다.



콘솔 에이전트에 대한 요구 사항

아직 콘솔 에이전트를 만들지 않았다면 네트워킹 요구 사항을 검토해야 합니다.

- "콘솔 에이전트에 대한 네트워킹 요구 사항 보기"
- "AWS의 보안 그룹 규칙"

관련 주제

- "Cloud Volumes ONTAP 에 대한 AutoSupport 설정 확인"
- "ONTAP 내부 포트에 대해 알아보세요" .

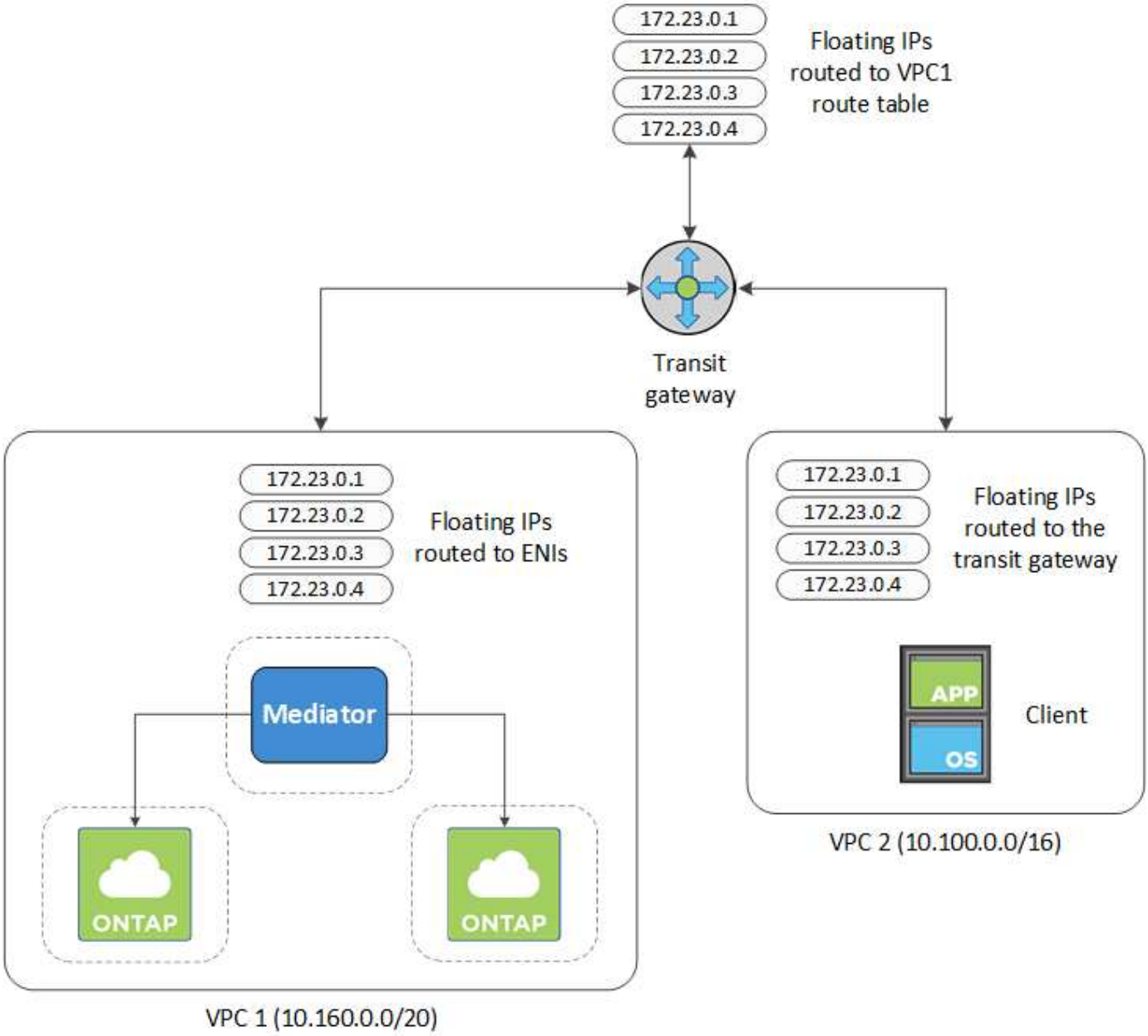
HA 쌍에 대한 액세스를 활성화하기 위해 AWS 전송 게이트웨이를 설정합니다."유동 IP 주소" HA 쌍이 있는 VPC 외부에서.

Cloud Volumes ONTAP HA 구성이 여러 AWS 가용성 영역에 걸쳐 분산된 경우 VPC 내에서 NAS 데이터에 액세스하려면 플로팅 IP 주소가 필요합니다. 이러한 유동 IP 주소는 장애 발생 시 노드 간에 마이그레이션될 수 있지만 기본적으로 VPC 외부에서 액세스할 수는 없습니다. 별도의 개인 IP 주소는 VPC 외부에서 데이터에 액세스할 수 있도록 하지만 자동 장애 조치는 제공하지 않습니다.

클러스터 관리 인터페이스와 선택적 SVM 관리 LIF에도 부동 IP 주소가 필요합니다.

AWS 전송 게이트웨이를 설정하면 HA 쌍이 있는 VPC 외부에서 플로팅 IP 주소에 액세스할 수 있습니다. 즉, VPC 외부의 NAS 클라이언트와 NetApp 관리 도구가 플로팅 IP에 액세스할 수 있습니다.

다음은 두 개의 VPC가 트랜짓 게이트웨이로 연결된 것을 보여주는 예입니다. HA 시스템은 한 VPC에 있고, 클라이언트는 다른 VPC에 있습니다. 그런 다음 부동 IP 주소를 사용하여 클라이언트에 NAS 볼륨을 마운트할 수 있습니다.

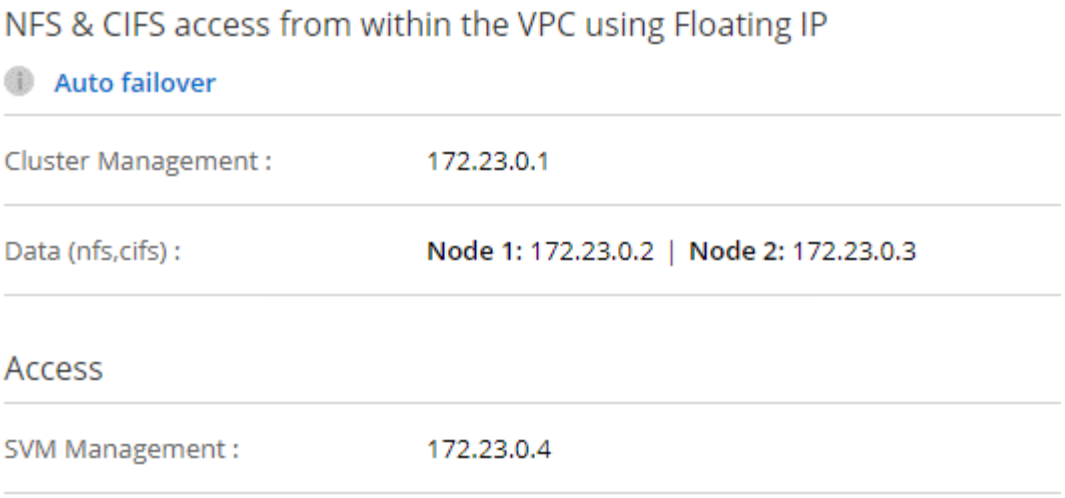


다음 단계에서는 비슷한 구성을 설정하는 방법을 보여줍니다.

단계

1. "트랜짓 게이트웨이를 생성하고 VPC를 게이트웨이에 연결합니다." .
2. VPC를 전송 게이트웨이 경로 테이블과 연결합니다.
   a. **VPC** 서비스에서 *전송 게이트웨이 경로 테이블*을 클릭합니다.
   b. 경로 테이블을 선택하세요.
   c. *협회*를 클릭한 다음 *협회 만들기*를 선택합니다.
   d. 연결할 첨부 파일(VPC)을 선택한 다음 *연결 만들기*를 클릭합니다.
3. HA 쌍의 플로팅 IP 주소를 지정하여 트랜짓 게이트웨이의 경로 테이블에 경로를 생성합니다.

   NetApp Console 의 시스템 정보 페이지에서 부동 IP 주소를 찾을 수 있습니다. 예를 들면 다음과 같습니다.



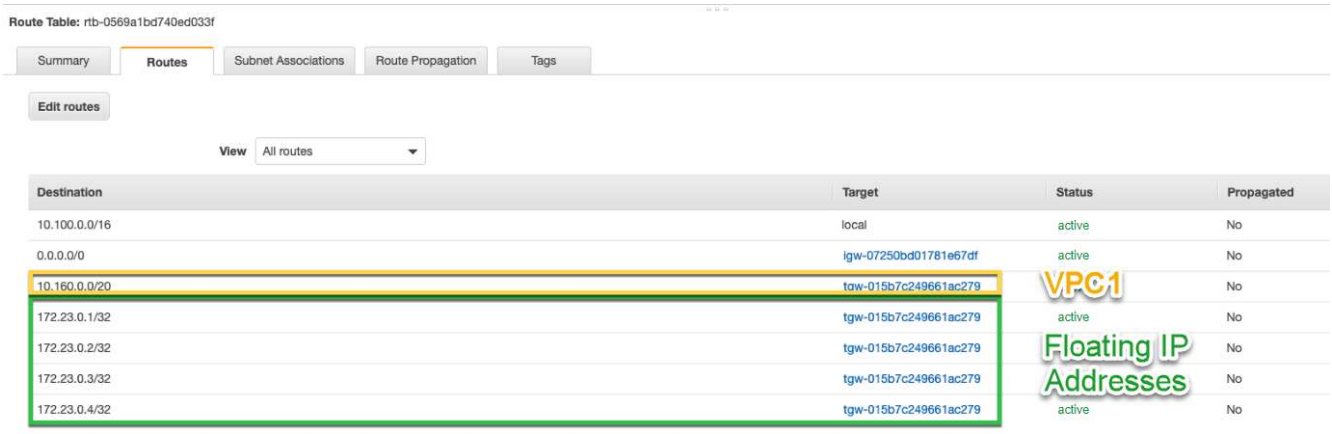
다음 샘플 이미지는 트랜짓 게이트웨이의 경로 테이블을 보여줍니다. 여기에는 Cloud Volumes ONTAP 에서 사용하는 두 개의 VPC의 CIDR 블록에 대한 경로와 4개의 플로팅 IP 주소가 포함됩니다.

4. 플로팅 IP 주소에 액세스해야 하는 VPC의 경로 테이블을 수정합니다.

   a. 플로팅 IP 주소에 경로 항목을 추가합니다.

   b. HA 쌍이 있는 VPC의 CIDR 블록에 경로 항목을 추가합니다.

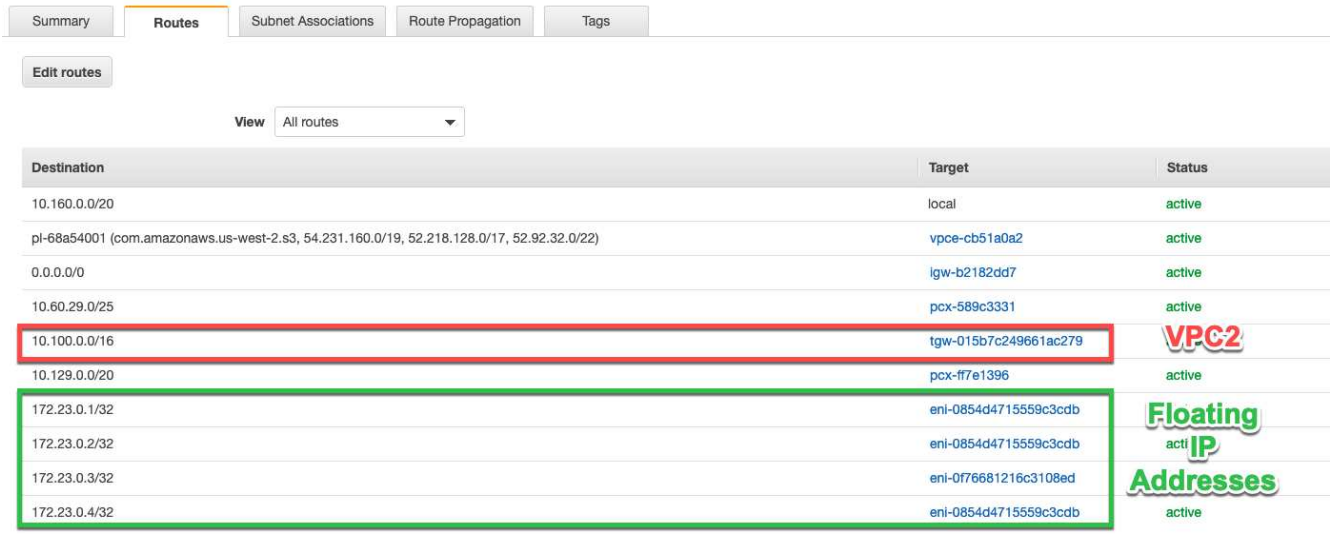
      다음 샘플 이미지는 VPC 1에 대한 경로와 플로팅 IP 주소를 포함하는 VPC 2의 경로 테이블을 보여줍니다.



5. 부동 IP 주소에 액세스해야 하는 VPC에 경로를 추가하여 HA 쌍의 VPC에 대한 경로 테이블을 수정합니다.

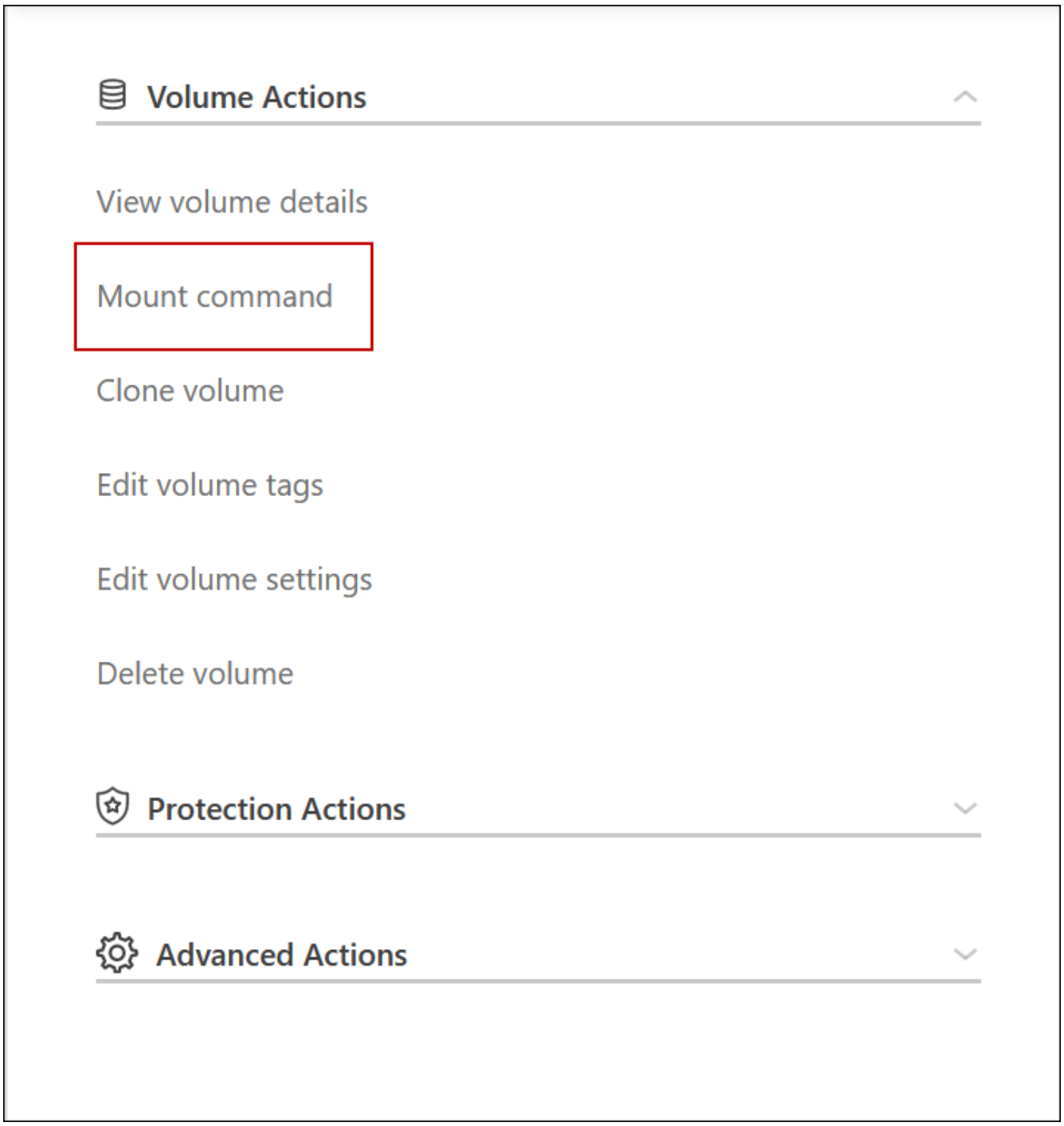
   이 단계는 VPC 간 라우팅을 완료하기 때문에 중요합니다.

   다음 샘플 이미지는 VPC 1의 경로 테이블을 보여줍니다. 여기에는 부동 IP 주소와 클라이언트가 있는 VPC 2에 대한 경로가 포함됩니다. 콘솔은 HA 쌍을 배포할 때 자동으로 플로팅 IP를 경로 테이블에 추가했습니다.



6. VPC에 대한 모든 트래픽에 대한 보안 그룹 설정을 업데이트합니다.
   a. 가상 사설 클라우드에서 *서브넷*을 클릭합니다.
   b. 경로 테이블 탭을 클릭하고 HA 쌍의 부동 IP 주소 중 하나에 대한 원하는 환경을 선택합니다.
   c. *보안 그룹*을 클릭하세요.
   d. *인바운드 규칙 편집*을 선택합니다.
   e. *규칙 추가*를 클릭합니다.
   f. 유형에서 *모든 트래픽*을 선택한 다음 VPC IP 주소를 선택합니다.
   g. 변경 사항을 적용하려면 *규칙 저장*을 클릭하세요.
7. 플로팅 IP 주소를 사용하여 클라이언트에 볼륨을 마운트합니다.

   콘솔의 볼륨 관리 패널에서 마운트 명령 옵션을 통해 콘솔에서 올바른 IP 주소를 찾을 수 있습니다.



8. NFS 볼륨을 마운트하는 경우 클라이언트 VPC의 서브넷과 일치하도록 내보내기 정책을 구성합니다.

   "볼륨을 편집하는 방법을 알아보세요" .

관련 링크

- "AWS의 고가용성 쌍"
- "AWS의 Cloud Volumes ONTAP 에 대한 네트워킹 요구 사항"

AWS 공유 서브넷에 **Cloud Volumes ONTAP HA** 쌍 배포

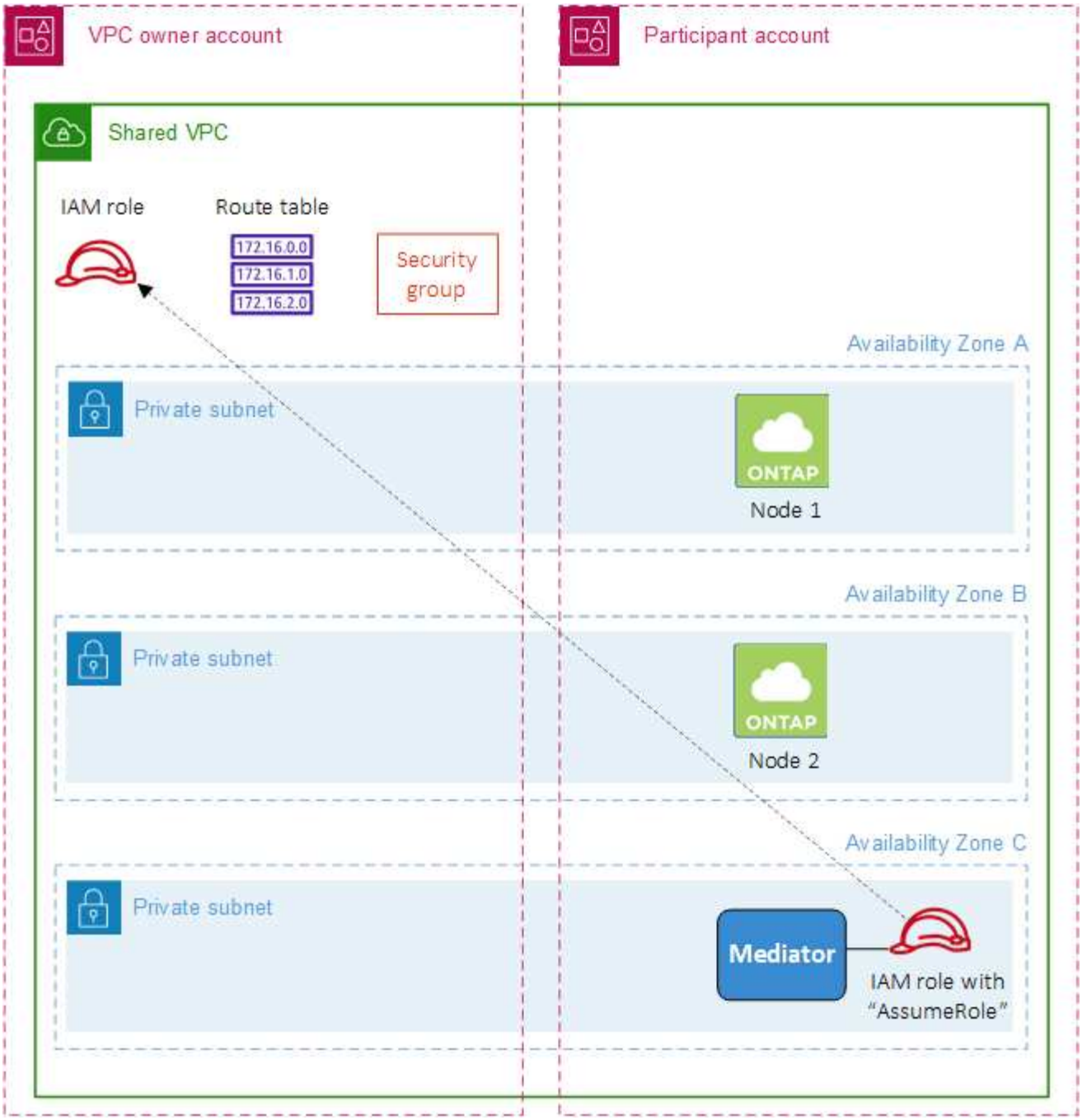
9.11.1 릴리스부터 VPC 공유를 통해 AWS에서 Cloud Volumes ONTAP HA 쌍이 지원됩니다. VPC 공유를 사용하면 조직에서 다른 AWS 계정과 서브넷을 공유할 수 있습니다. 이 구성을 사용하려면 AWS 환경을 설정한 다음 API를 사용하여 HA 쌍을 배포해야 합니다.

와 함께 "VPC 공유" Cloud Volumes ONTAP HA 구성은 두 계정에 분산됩니다.

- 네트워킹(VPC, 서브넷, 경로 테이블 및 Cloud Volumes ONTAP 보안 그룹)을 소유한 VPC 소유자 계정
- EC2 인스턴스가 공유 서브넷에 배포되는 참여자 계정(여기에는 두 개의 HA 노드와 중재자가 포함됨)

여러 가용성 영역에 배포된 Cloud Volumes ONTAP HA 구성의 경우, HA 중재자에게 VPC 소유자 계정의 경로 테이블에 쓰기 위한 특정 권한이 필요합니다. 중재자가 맡을 수 있는 IAM 역할을 설정하여 해당 권한을 제공해야 합니다.

다음 이미지는 이 배포에 포함된 구성 요소를 보여줍니다.



아래 단계에 설명된 대로 참여자 계정과 서브넷을 공유한 다음 VPC 소유자 계정에서 IAM 역할과 보안 그룹을 만들어야 합니다.

Cloud Volumes ONTAP 시스템을 생성하면 NetApp Console 자동으로 IAM 역할을 생성하여 중재자에 연결합니다. 이 역할은 HA 쌍과 관련된 경로 테이블을 변경하기 위해 VPC 소유자 계정에서 생성한 IAM 역할을 수행합니다.

단계

1. VPC 소유자 계정의 서브넷을 참여자 계정과 공유합니다.

   이 단계는 공유 서브넷에 HA 쌍을 배포하는 데 필요합니다.

   "AWS 설명서: 서브넷 공유"

2. VPC 소유자 계정에서 Cloud Volumes ONTAP 에 대한 보안 그룹을 만듭니다.

   "Cloud Volumes ONTAP 에 대한 보안 그룹 규칙을 참조하세요." . HA 중재자에 대한 보안 그룹을 만들 필요는 없습니다. 콘솔이 그 일을 대신해 줍니다.

3. VPC 소유자 계정에서 다음 권한이 포함된 IAM 역할을 만듭니다.

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. API를 사용하여 새로운 Cloud Volumes ONTAP 시스템을 만듭니다.

   다음 필드를 지정해야 합니다.

   - "보안그룹ID"

     "securityGroupId" 필드는 VPC 소유자 계정에서 생성한 보안 그룹을 지정해야 합니다(위의 2단계 참조).

   - "haParams" 객체의 "assumeRoleArn"

     "assumeRoleArn" 필드에는 VPC 소유자 계정에서 생성한 IAM 역할의 ARN이 포함되어야 합니다(위의 3단계 참조).

     예를 들어:

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

   +
   "Cloud Volumes ONTAP API에 대해 알아보세요"

AWS 단일 **AZ**에서 **Cloud Volumes ONTAP HA** 쌍에 대한 배치 그룹 생성 구성

AWS 단일 가용성 영역(AZ)에 있는 Cloud Volumes ONTAP 고가용성(HA) 배포는 배치 그룹 생성에 실패하면 실패하고 롤백될 수 있습니다. Cloud Volumes ONTAP 노드와 중재자 인스턴스를 사용할 수 없는 경우 배치 그룹 생성도 실패하고 배포가 롤백됩니다. 이를 방지하려면 배치 그룹 생성에 실패하더라도 배포가 완료되도록 구성을 수정할 수 있습니다.

롤백 프로세스를 우회하면 Cloud Volumes ONTAP 배포 프로세스가 성공적으로 완료되고 배치 그룹 생성이 완료되지 않았음을 알립니다.

단계

1. SSH를 사용하여 NetApp Console 에이전트 호스트에 연결하고 로그인합니다.
2. 로 이동 `/opt/application/netapp/cloudmanager/docker_occm/data` .
3. 편집하다 `app.conf` 값을 변경하여 `rollback-on-placement-group-failure` 매개변수 `false` . 이 매개변수의 기본값은 다음과 같습니다. `true` .

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. 파일을 저장하고 콘솔 에이전트에서 로그오프합니다. 콘솔 에이전트를 다시 시작할 필요가 없습니다.

Cloud Volumes ONTAP 에 대한 **AWS** 보안 그룹 인바운드 및 아웃바운드 규칙

NetApp Console Cloud Volumes ONTAP 성공적으로 작동하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함하는 AWS 보안 그룹을 생성합니다. 테스트 목적으로 포트를 참조하거나 자체 보안 그룹을 사용하려는 경우 포트를 참조할 수 있습니다.

Cloud Volumes ONTAP 규칙

Cloud Volumes ONTAP 의 보안 그룹에는 인바운드 규칙과 아웃바운드 규칙이 모두 필요합니다.

인바운드 규칙

Cloud Volumes ONTAP 시스템을 추가하고 미리 정의된 보안 그룹을 선택하면 다음 중 하나 내에서 트래픽을 허용하도록 선택할 수 있습니다.

- 선택된 **VPC**만 해당: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템의 VPC 서브넷 범위와 콘솔 에이전트가 있는 VPC의 서브넷 범위입니다. 이것은 권장되는 옵션입니다.
- 모든 **VPC**: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.

규약	포트	목적
모든 ICMP	모두	인스턴스에 ping을 보냅니다.
HTTP	80	클러스터 관리 LIF의 IP 주소를 사용하여 ONTAP System Manager 웹 콘솔에 대한 HTTP 액세스
HTTPS	443	클러스터 관리 LIF의 IP 주소를 사용하여 콘솔 에이전트와 ONTAP System Manager 웹 콘솔에 대한 HTTPS 액세스 연결

규약	포트	목적
SSH	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 대한 SSH 액세스
TCP	111	NFS에 대한 원격 프로시저 호출
TCP	139	CIFS용 NetBIOS 서비스 세션
TCP	161-162	간단한 네트워크 관리 프로토콜
TCP	445	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
TCP	635	NFS 마운트
TCP	749	케르베로스
TCP	2049	NFS 서버 데몬
TCP	3260	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045	NFS 잠금 데몬
TCP	4046	NFS용 네트워크 상태 모니터
TCP	10000	NDMP를 사용한 백업
TCP	11104	SnapMirror 위한 클러스터 간 통신 세션 관리
TCP	11105	클러스터 간 LIF를 사용한 SnapMirror 데이터 전송
UDP	111	NFS에 대한 원격 프로시저 호출
UDP	161-162	간단한 네트워크 관리 프로토콜
UDP	635	NFS 마운트
UDP	2049	NFS 서버 데몬
UDP	4045	NFS 잠금 데몬
UDP	4046	NFS용 네트워크 상태 모니터
UDP	4049	NFS rquotad 프로토콜

아웃바운드 규칙

Cloud Volumes ONTAP 의 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 개방합니다. 이것이 허용된다면, 기본적인 아웃바운드 규칙을 따르세요. 더욱 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

Cloud Volumes ONTAP 의 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함되어 있습니다.

규약	포트	목적
모든 ICMP	모두	모든 아웃바운드 트래픽
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Cloud Volumes ONTAP 의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

소스는 Cloud Volumes ONTAP 시스템의 인터페이스(IP 주소)입니다.

서비스	규약	포트	원천	목적지	목적
액티브 디렉토리	TCP	88	노드 관리 LIF	Active Directory 포리스트	Kerberos V 인증
	UDP	137	노드 관리 LIF	Active Directory 포리스트	NetBIOS 이름 서비스
	UDP	138	노드 관리 LIF	Active Directory 포리스트	NetBIOS 데이터그램 서비스
	TCP	139	노드 관리 LIF	Active Directory 포리스트	NetBIOS 서비스 세션
	TCP 및 UDP	389	노드 관리 LIF	Active Directory 포리스트	LDAP
	TCP	445	노드 관리 LIF	Active Directory 포리스트	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
	TCP	464	노드 관리 LIF	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(SET_CHANGE)
	UDP	464	노드 관리 LIF	Active Directory 포리스트	Kerberos 키 관리
	TCP	749	노드 관리 LIF	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(RPCSEC_GSS)
	TCP	88	데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트	Kerberos V 인증
	UDP	137	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 이름 서비스
	UDP	138	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 데이터그램 서비스
	TCP	139	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 서비스 세션
	TCP 및 UDP	389	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	LDAP
	TCP	445	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
	TCP	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(SET_CHANGE)
	UDP	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos 키 관리
	TCP	749	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(RPCSEC_GSS)

서비스	규약	포트	원천	목적지	목적
AutoSupport	HTTPS	443	노드 관리 LIF	mysupport.netapp.com	AutoSupport (HTTPS가 기본값)
	HTTP	80	노드 관리 LIF	mysupport.netapp.com	AutoSupport (전송 프로토콜이 HTTPS에서 HTTP로 변경된 경우에만)
	TCP	3128	노드 관리 LIF	콘솔 에이전트	아웃바운드 인터넷 연결이 불가능한 경우 콘솔 에이전트의 프록시 서버를 통해 AutoSupport 메시지 보내기
S3에 백업	TCP	5010	클러스터 간 LIF	백업 엔드포인트 또는 복원 엔드포인트	S3 백업 기능에 대한 백업 및 복원 작업
무리	모든 트래픽	모든 트래픽	한 노드의 모든 LIF	다른 노드의 모든 LIF	클러스터 간 통신(Cloud Volumes ONTAP HA만 해당)
	TCP	3000	노드 관리 LIF	HA 중재자	ZAPI 호출(Cloud Volumes ONTAP HA만 해당)
	ICMP	1	노드 관리 LIF	HA 중재자	유지(Cloud Volumes ONTAP HA만 해당)
구성 백업	HTTP	80	노드 관리 LIF	http://<콘솔 에이전트 IP 주소>/occm/offboxconfig	구성 백업을 콘솔 에이전트로 보냅니다 ."ONTAP 문서"
DHCP	UDP	68	노드 관리 LIF	DHCP	최초 설정을 위한 DHCP 클라이언트
DHCPS	UDP	67	노드 관리 LIF	DHCP	DHCP 서버
DNS	UDP	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	TCP	18600년–18699년	노드 관리 LIF	대상 서버	NDMP 사본
SMTP	TCP	25	노드 관리 LIF	메일 서버	SMTP 알림은 AutoSupport 에 사용할 수 있습니다.
SNMP	TCP	161	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	UDP	161	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	TCP	162	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	UDP	162	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
SnapMirror	TCP	11104	클러스터 간 LIF	ONTAP 클러스터 간 LIF	SnapMirror 위한 클러스터 간 통신 세션 관리
	TCP	11105	클러스터 간 LIF	ONTAP 클러스터 간 LIF	SnapMirror 데이터 전송

서비스	규약	포트	원천	목적지	목적
시스템 로그	UDP	514	노드 관리 LIF	시스템 로그 서버	Syslog 전달 메시지

HA 중재자 외부 보안 그룹에 대한 규칙

Cloud Volumes ONTAP HA 중재자의 미리 정의된 외부 보안 그룹에는 다음과 같은 인바운드 및 아웃바운드 규칙이 포함됩니다.

인바운드 규칙

HA 중재자에 대한 미리 정의된 보안 그룹에는 다음과 같은 인바운드 규칙이 포함됩니다.

규약	포트	원천	목적
TCP	3000	콘솔 에이전트의 CIDR	콘솔 에이전트에서 RESTful API 액세스

아웃바운드 규칙

HA 중재자에 대한 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 개방합니다. 이것이 허용된다면, 기본적인 아웃바운드 규칙을 따르세요. 더욱 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

HA 중재자에 대한 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

규약	포트	목적
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 HA 중재자의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

규약	포트	목적지	목적
HTTP	80	AWS EC2 인스턴스의 콘솔 에이전트의 IP 주소	중재자용 업그레이드 다운로드
HTTPS	443	ec2.amazonaws.com	스토리지 장애 조치 지원
UDP	53	ec2.amazonaws.com	스토리지 장애 조치 지원

포트 443과 53을 여는 대신 대상 서브넷에서 AWS EC2 서비스로 인터페이스 VPC 엔드포인트를 만들 수 있습니다.

HA 구성 내부 보안 그룹에 대한 규칙

Cloud Volumes ONTAP HA 구성을 위한 미리 정의된 내부 보안 그룹에는 다음 규칙이 포함됩니다. 이 보안 그룹은 HA 노드 간, 중재자와 노드 간 통신을 가능하게 합니다.

콘솔은 항상 이 보안 그룹을 생성합니다. 귀하 자신의 것을 사용할 수 있는 옵션이 없습니다.

인바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 인바운드 규칙이 포함됩니다.

규약	포트	목적
모든 트래픽	모두	HA 중재자와 HA 노드 간 통신

아웃바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

규약	포트	목적
모든 트래픽	모두	HA 중재자와 HA 노드 간 통신

콘솔 에이전트에 대한 규칙

"콘솔 에이전트에 대한 보안 그룹 규칙 보기"

AWS에서 고객 관리 키를 사용하도록 Cloud Volumes ONTAP 설정

Cloud Volumes ONTAP 과 함께 Amazon 암호화를 사용하려면 AWS Key Management Service(KMS)를 설정해야 합니다.

단계

1. 활성 고객 마스터 키(CMK)가 있는지 확인하세요.

   CMK는 AWS 관리형 CMK이거나 고객 관리형 CMK일 수 있습니다. NetApp Console 및 Cloud Volumes ONTAP 과 동일한 AWS 계정에 있을 수도 있고 다른 AWS 계정에 있을 수도 있습니다.

   "AWS 문서: 고객 마스터 키(CMK)"

2. 콘솔에 대한 권한을 제공하는 IAM 역할을 _키 사용자_로 추가하여 각 CMK에 대한 키 정책을 수정합니다.

   IAM(Identity and Access Management) 역할을 주요 사용자로 추가하면 콘솔에서 Cloud Volumes ONTAP 과 함께 CMK를 사용할 수 있는 권한이 부여됩니다.

   "AWS 문서: 키 편집"

3. CMK가 다른 AWS 계정에 있는 경우 다음 단계를 완료하세요.

   a. CMK가 있는 계정에서 KMS 콘솔로 이동합니다.

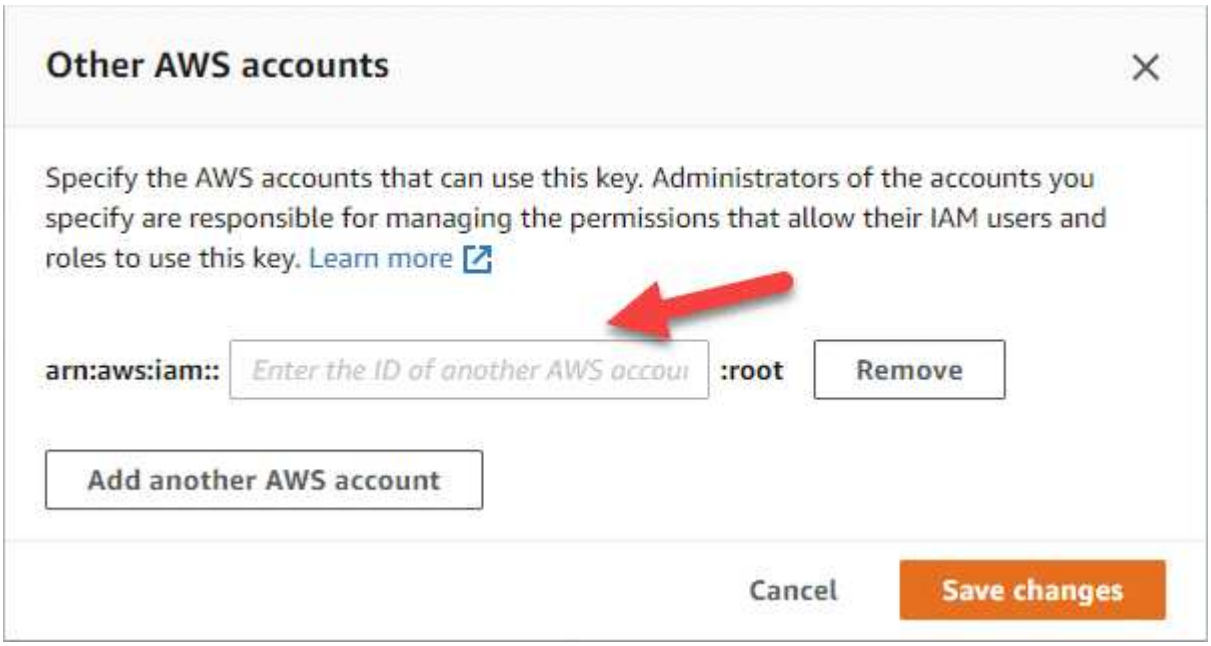
   b. 키를 선택하세요.

c. 일반 구성 창에서 키의 ARN을 복사합니다.

Cloud Volumes ONTAP 시스템을 생성할 때 콘솔에 ARN을 제공해야 합니다.

d. 다른 **AWS** 계정 창에서 콘솔에 권한을 제공하는 AWS 계정을 추가합니다.

일반적으로 이 계정에는 콘솔이 배포됩니다. AWS에 콘솔이 설치되어 있지 않은 경우 콘솔에 대한 AWS 액세스 키를 제공한 계정을 사용하세요.



e. 이제 콘솔에 권한을 제공하는 AWS 계정으로 전환하고 IAM 콘솔을 엽니다.

f. 아래 나열된 권한을 포함하는 IAM 정책을 만듭니다.

g. 콘솔에 대한 권한을 제공하는 IAM 역할이나 IAM 사용자에게 정책을 연결합니다.

다음 정책은 콘솔이 외부 AWS 계정에서 CMK를 사용하는 데 필요한 권한을 제공합니다. "리소스" 섹션에서 지역 및 계정 ID를 수정하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
이 프로세스에 대한 추가 세부 사항은 다음을 참조하세요. "AWS 문서: 다른 계정의 사용자가 KMS 키를 사용하도록 허용" .

4. 고객 관리 CMK를 사용하는 경우 Cloud Volumes ONTAP IAM 역할을 _키 사용자_로 추가하여 CMK에 대한 키 정책을 수정합니다.

이 단계는 Cloud Volumes ONTAP에서 데이터 계층화를 활성화했으며 Amazon Simple Storage Service(Amazon S3) 버킷에 저장된 데이터를 암호화하려는 경우에 필요합니다.

Cloud Volumes ONTAP 시스템을 생성할 때 IAM 역할이 생성되므로 Cloud Volumes ONTAP 배포한 후에 이 단계를 수행해야 합니다. (물론, 기존 Cloud Volumes ONTAP IAM 역할을 사용할 수도 있으므로 이 단계를 미리 수행할 수 있습니다.)

"AWS 문서: 키 편집"

Cloud Volumes ONTAP 노드에 대한 AWS IAM 역할 설정

필요한 권한이 있는 AWS Identity and Access Management(IAM) 역할은 각 Cloud Volumes ONTAP 노드에 연결되어야 합니다. HA 중재자의 경우도 마찬가지입니다. NetApp Console IAM 역할을 자동으로 생성하도록 하는 것이 가장 쉽지만, 사용자가 직접 역할을 지정할 수도 있습니다.

이 작업은 선택 사항입니다. Cloud Volumes ONTAP 시스템을 생성할 때 기본 옵션은 콘솔에서 IAM 역할을 생성하도록 하는 것입니다. 회사의 보안 정책에 따라 IAM 역할을 직접 만들어야 하는 경우 아래 단계를 따르세요.

AWS Secret Cloud에서는 고유한 IAM 역할을 제공해야 합니다. "C2S에 Cloud Volumes ONTAP 배포하는 방법을 알아보세요" .

단계

1. AWS IAM 콘솔로 이동합니다.
2. 다음 권한을 포함하는 IAM 정책을 만듭니다.
    - Cloud Volumes ONTAP 노드에 대한 기본 정책

표준 지역

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud(미국) 지역

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

극비 지역

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

비밀 지역

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Cloud Volumes ONTAP 노드에 대한 백업 정책

  Cloud Volumes ONTAP 시스템과 함께 NetApp Backup and Recovery 사용하려는 경우 노드의 IAM 역할에 아래에 표시된 두 번째 정책이 포함되어야 합니다.

표준 지역

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud(미국) 지역

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

극비 지역

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

비밀 지역

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA 중재자

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. IAM 역할을 만들고 해당 역할에 만든 정책을 연결합니다.

결과

이제 새로운 Cloud Volumes ONTAP 시스템을 생성할 때 선택할 수 있는 IAM 역할이 생겼습니다.

더 많은 정보

- "AWS 설명서: IAM 정책 생성"
- "AWS 설명서: IAM 역할 생성"

AWS에서 Cloud Volumes ONTAP 에 대한 라이선싱 설정

Cloud Volumes ONTAP 에서 사용할 라이선싱 옵션을 결정한 후에는 새 시스템을 만들 때 해당 라이선싱 옵션을 선택하기 전에 몇 가지 단계를 거쳐야 합니다.

프리미엄

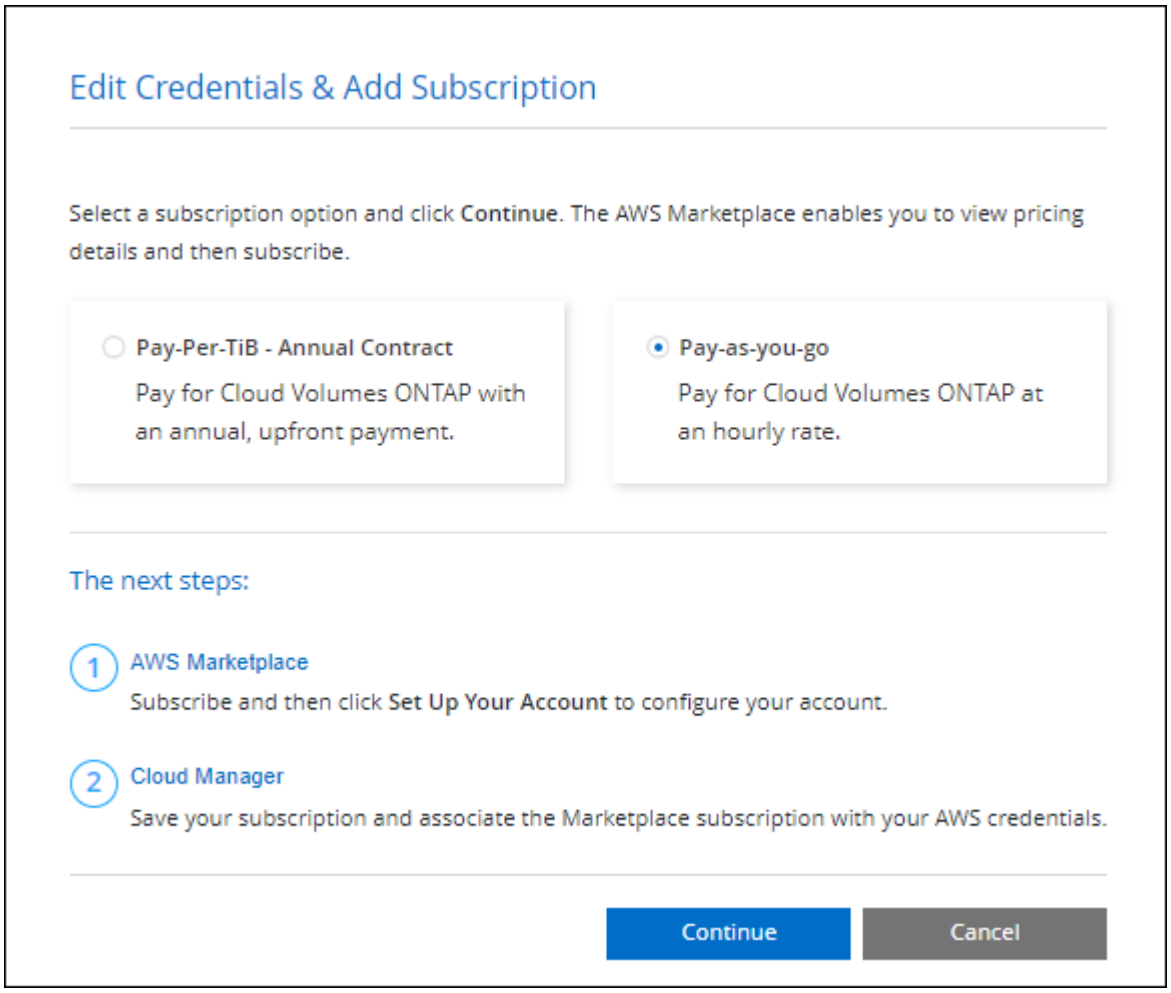
최대 500GiB의 프로비저닝 용량을 제공하는 Cloud Volumes ONTAP 무료로 사용하려면 Freemium 옵션을 선택하세요. "Freemium 제공에 대해 자세히 알아보세요" .

단계

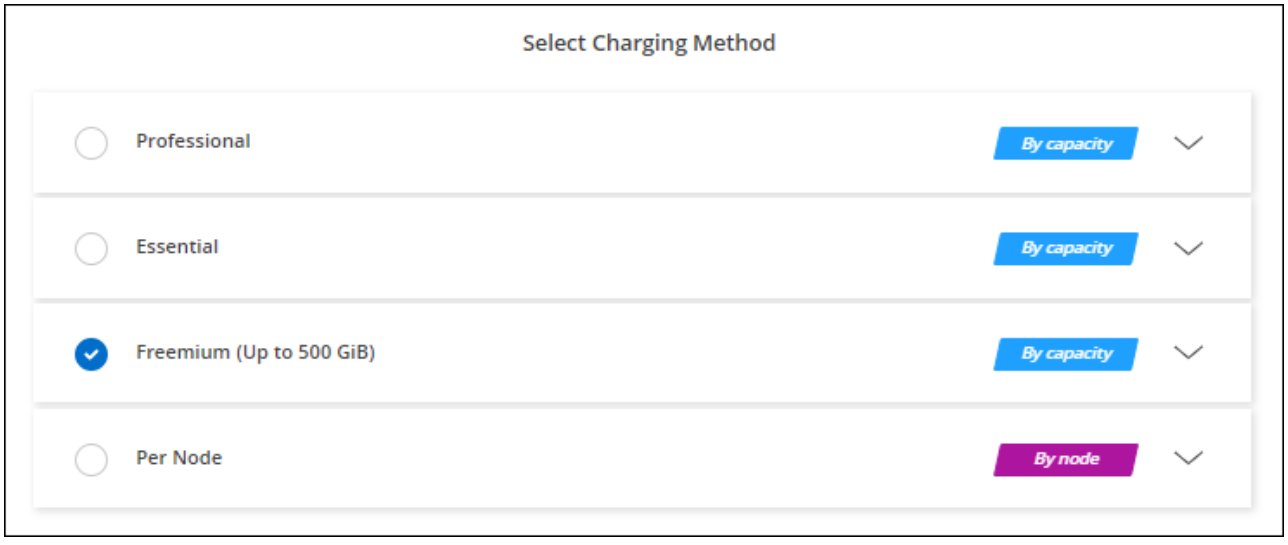
1. NetApp Console 의 왼쪽 탐색 메뉴에서 *스토리지 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
    a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 메시지에 따라 AWS

Marketplace에서 사용량에 따라 지불하는 서비스를 구독하세요.

프로비저닝된 용량이 500GiB를 초과하지 않는 한 마켓플레이스 구독을 통해 요금이 청구되지 않습니다. 초과 시 시스템은 자동으로 다음 용량으로 변환됩니다."필수 패키지" .



a. 콘솔로 돌아와서 요금 청구 방법 페이지에서 *프리미엄*을 선택하세요.



"AWS에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

용량 기반 라이센스

용량 기반 라이선싱을 사용하면 TiB 용량당 Cloud Volumes ONTAP 비용을 지불할 수 있습니다. 용량 기반 라이선싱은 패키지 형태로 제공됩니다. 패키지에는 Essentials 패키지와 Professional 패키지가 있습니다.

Essentials 및 Professional 패키지는 다음과 같은 소비 모델 또는 구매 옵션으로 이용 가능합니다.

- NetApp 에서 구매한 라이선스(BYOL(Bring Your Own License))
- AWS Marketplace의 시간당 결제(PAYGO) 구독
- AWS Marketplace의 연간 계약

"용량 기반 라이선싱에 대해 자세히 알아보세요" .

다음 섹션에서는 각 소비 모델을 시작하는 방법을 설명합니다.

바이올

NetApp 에서 라이선스(BYOL)를 구매하여 선불로 지불하면 모든 클라우드 공급자에 Cloud Volumes ONTAP 시스템을 배포할 수 있습니다.

NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 에 대한 BYOL 라이선싱의 제한된 가용성" .

단계

1. "라이센스를 얻으려면 NetApp Sales에 문의하세요."
2. "콘솔에 NetApp 지원 사이트 계정 추가"

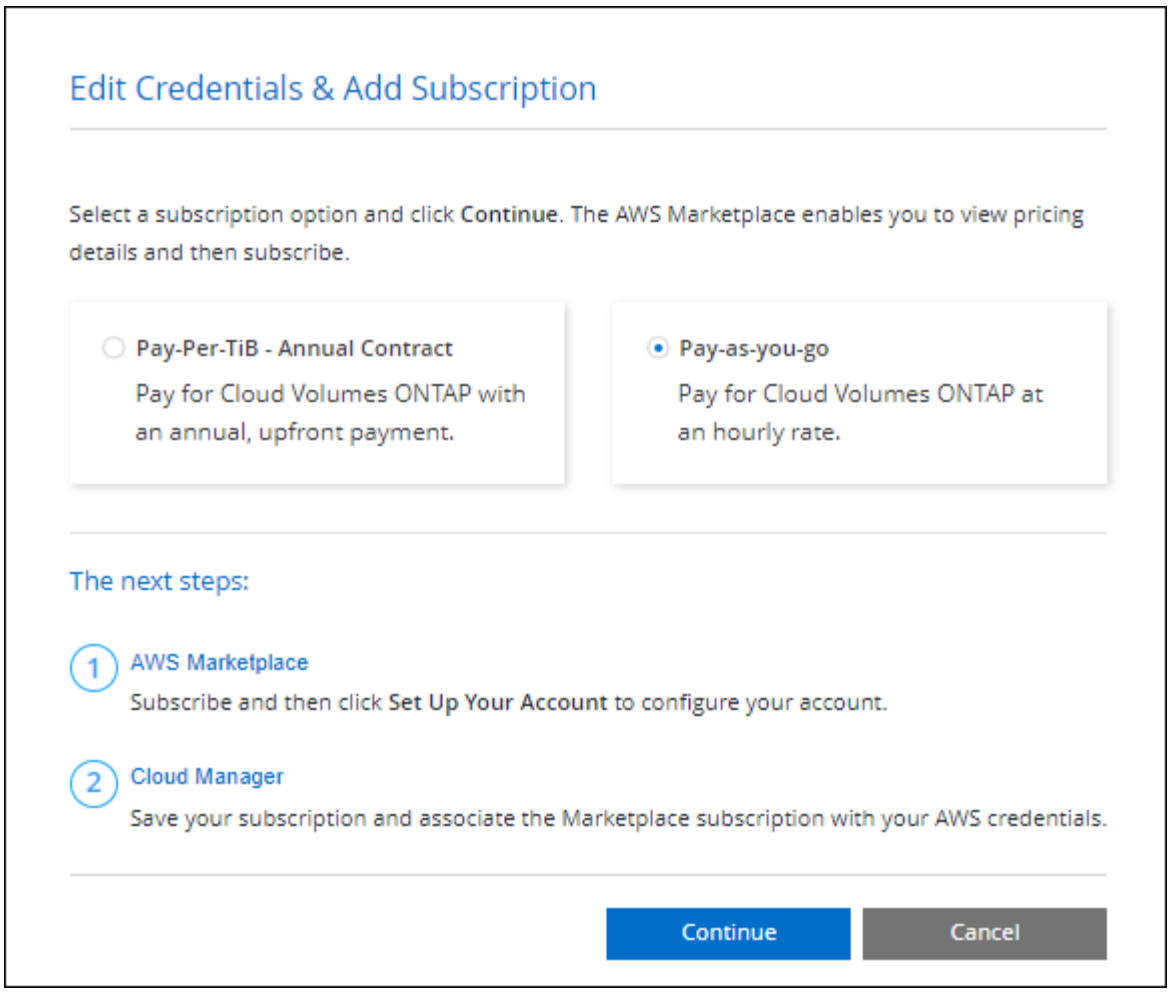
   콘솔은 NetApp 지원 사이트 계정과 연결된 라이선스에 대한 세부 정보를 얻기 위해 NetApp 라이선스 서비스에 자동으로 쿼리를 보냅니다. 오류가 없으면 콘솔이 자동으로 라이선스를 콘솔에 추가합니다.

   Cloud Volumes ONTAP 에서 라이선스를 사용하려면 먼저 콘솔에서 라이선스를 사용할 수 있어야 합니다. 필요한 경우 다음을 수행할 수 있습니다."콘솔에 라이센스를 수동으로 추가합니다." .

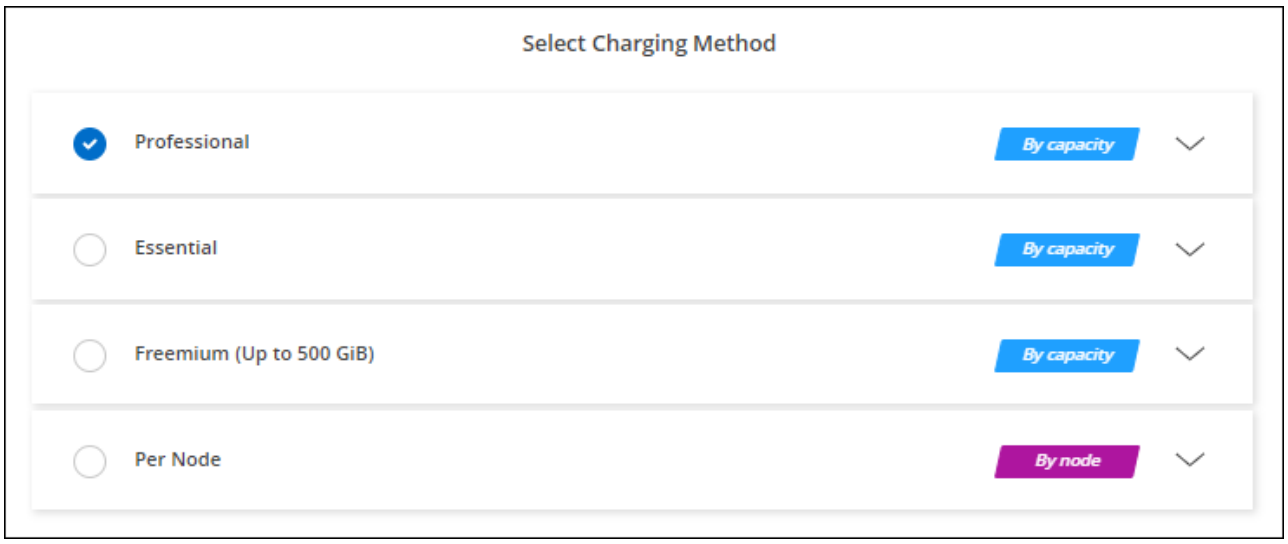
3. 콘솔의 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 메시지에 따라 AWS Marketplace에서 사용량에 따라 지불하는 서비스를 구독하세요.

      NetApp 에서 구매한 라이선스는 항상 먼저 청구되지만, 라이선스 용량을 초과하거나 라이선스 기간이 만료되면 마켓플레이스의 시간당 요금으로 청구됩니다.



a. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"AWS에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

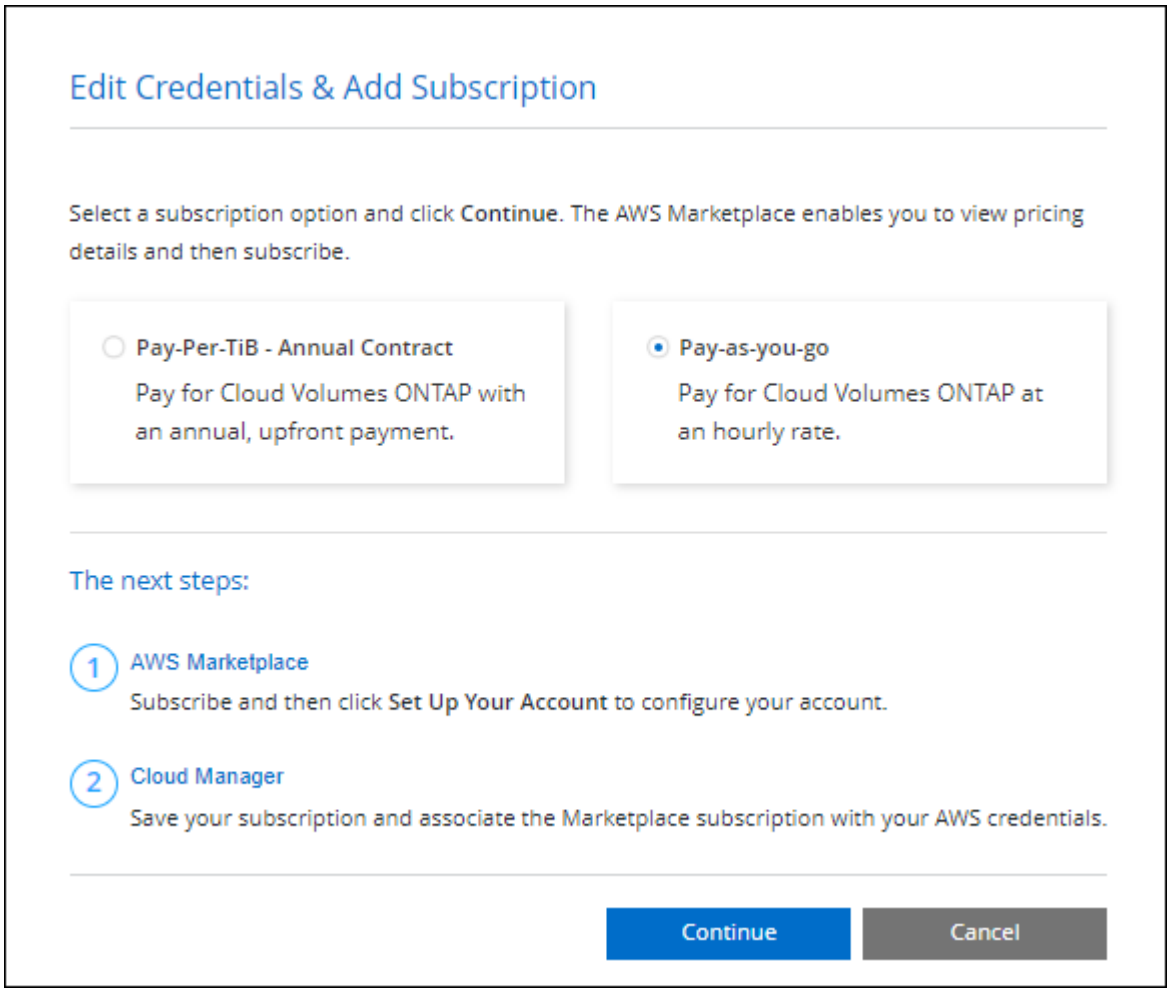
PAYGO 구독

클라우드 공급업체의 마켓플레이스에서 제공하는 혜택을 구독하여 시간당 요금을 지불하세요.

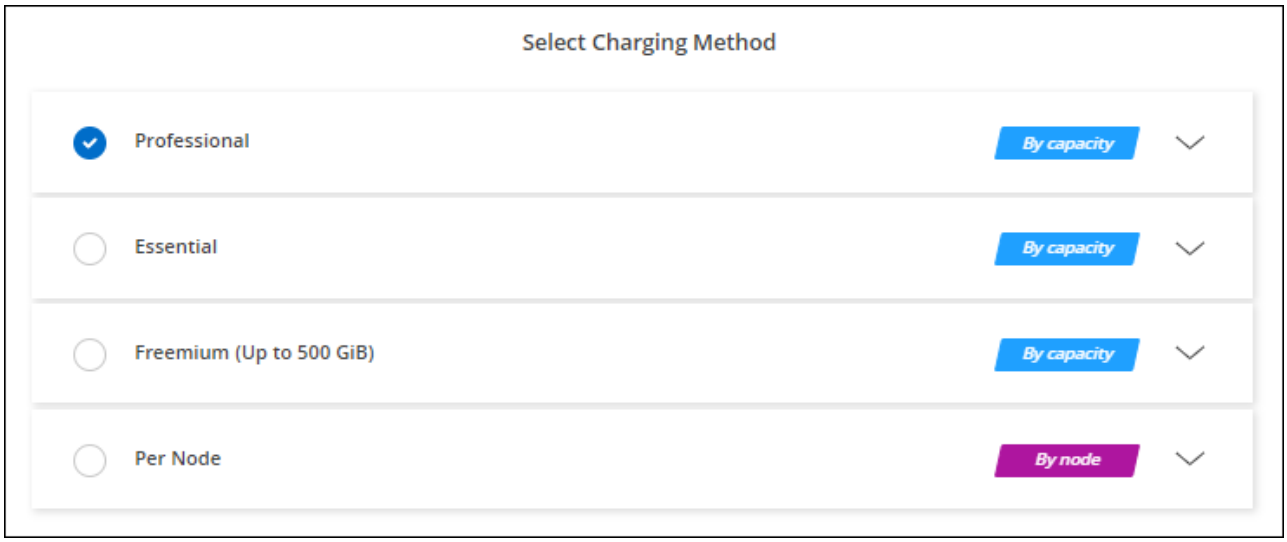
Cloud Volumes ONTAP 시스템을 생성하면 콘솔에서 AWS Marketplace에서 제공되는 계약에 가입하라는 메시지가 표시됩니다. 해당 구독은 요금 청구를 위해 시스템에 연결됩니다. 동일한 구독을 추가 Cloud Volumes ONTAP 시스템에도 사용할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음 프롬프트에 따라 AWS Marketplace에서 사용량에 따라 지불하는 서비스를 구독합니다.



   b. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"AWS에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

설정 > 자격 증명 페이지에서 AWS 계정과 연결된 AWS Marketplace 구독을 관리할 수 있습니다. "AWS 계정 및 구독을 관리하는 방법을 알아보세요"

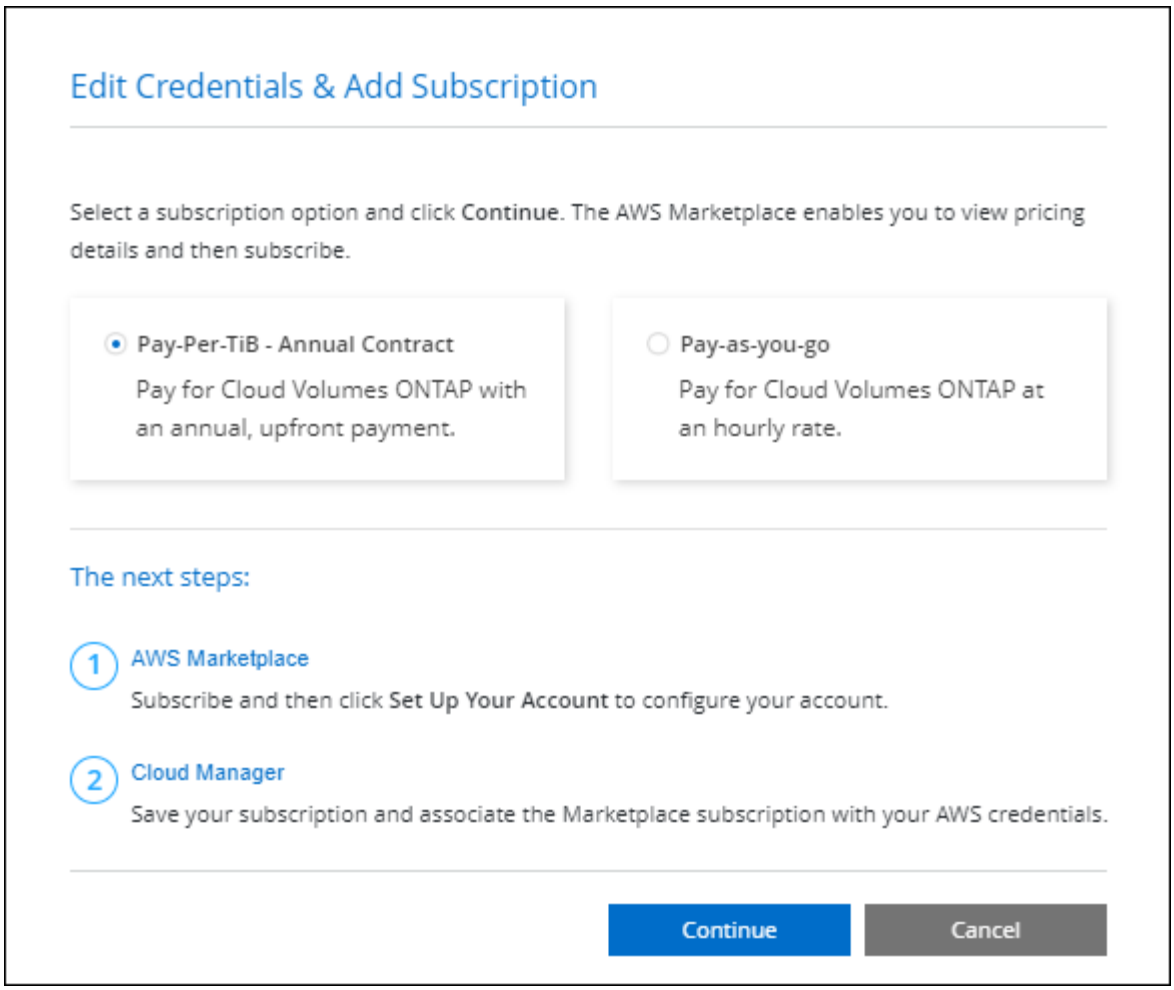
연간 계약

클라우드 공급업체의 마켓플레이스에서 연간 계약을 구매하여 연간으로 지불하세요.

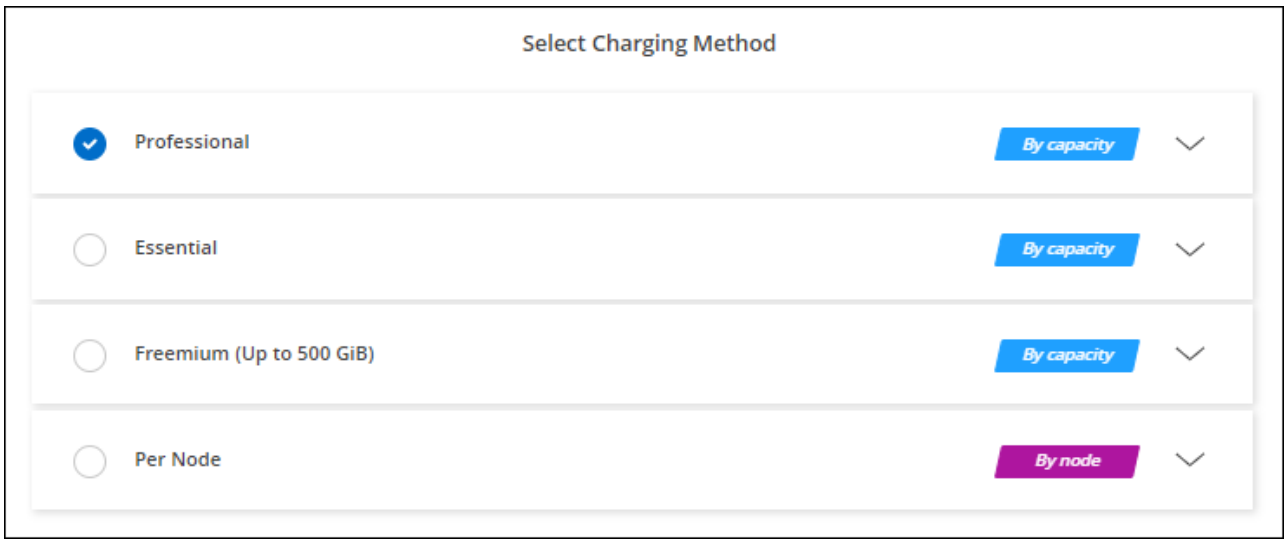
시간당 구독과 비슷하게, 콘솔에서는 AWS Marketplace에서 제공되는 연간 계약을 구독하라는 메시지가 표시됩니다.

단계

1. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 메시지에 따라 AWS Marketplace에서 연간 계약을 구독하세요.



b. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"AWS에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

Keystone 구독

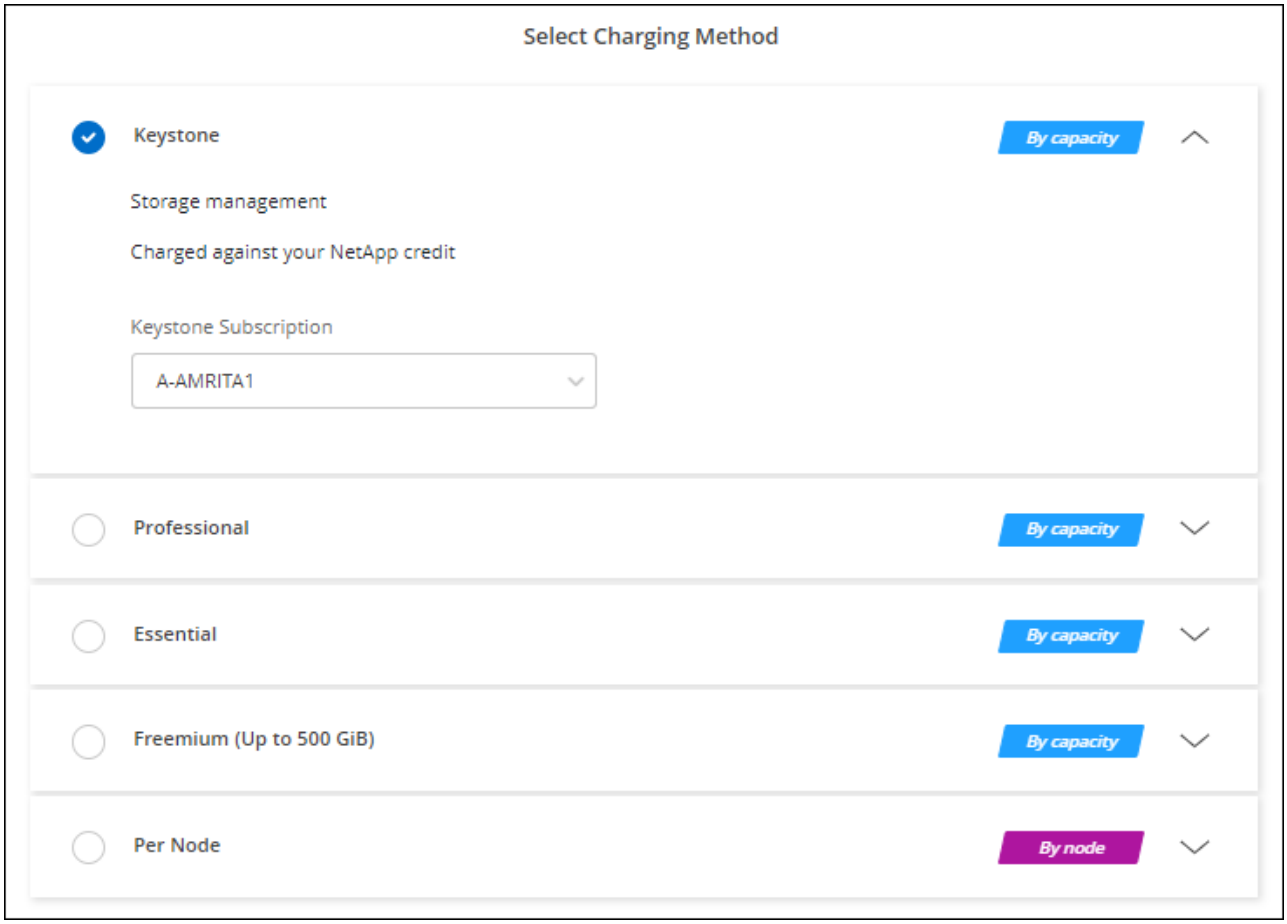
Keystone 구독은 사용량에 따라 비용을 지불하는 구독 기반 서비스입니다. "NetApp Keystone 구독에 대해 자세히

알아보세요" .

단계

1. 아직 구독이 없으신 경우, "NetApp 에 문의하세요"
2. 사용자 계정에 하나 이상의 Keystone 구독을 승인하려면 NetApp 에 문의으로 이메일을 보내주세요.
3. NetApp 귀하의 계정을 승인한 후,"Cloud Volumes ONTAP 과 함께 사용할 구독을 연결하세요" .
4. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

    a. 청구 방법을 선택하라는 메시지가 표시되면 Keystone 구독 청구 방법을 선택하세요.



"AWS에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

노드 기반 라이센스

노드 기반 라이선스는 Cloud Volumes ONTAP 의 이전 세대 라이선스입니다. 노드 기반 라이선스는 NetApp (BYOL)에서 구매할 수 있으며, 특정 경우에만 라이선스를 갱신할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- "노드 기반 라이선스의 가용성 종료"
- "노드 기반 라이선스 제공 종료"
- "노드 기반 라이선스를 용량 기반 라이선스로 변환"

빠른 배포를 사용하여 **AWS**에 **Cloud Volumes ONTAP** 배포

단일 노드와 고가용성(HA) 구성 모두에 대해 빠른 배포 방법을 사용하여 AWS에 Cloud Volumes ONTAP 배포할 수 있습니다. 이 간소화된 프로세스는 고급 방법에 비해 배포 단계를 줄여줍니다. 또한 단일 페이지에 기본값을 자동으로 설정하고 탐색을 최소화하여 작업 흐름을 더 명확하게 해줍니다.

시작하기 전에

NetApp Console 에서 AWS에 Cloud Volumes ONTAP 시스템을 추가하려면 다음이 필요합니다.

- 이미 실행 중인 콘솔 에이전트입니다.
  - 당신은 ~을 가져야합니다 "프로젝트 또는 작업 공간과 연결된 콘솔 에이전트" .
  - "항상 콘솔 에이전트를 실행 상태로 두어야 합니다." .
- 사용하려는 구성에 대한 이해.

  구성을 선택하고 관리자로부터 AWS 네트워킹 정보를 얻어서 준비했어야 합니다. 자세한 내용은 다음을 참조하세요."Cloud Volumes ONTAP 구성 계획" .
- Cloud Volumes ONTAP 에 대한 라이선싱을 설정하는 데 필요한 사항에 대한 이해.

  "라이선싱 설정 방법 알아보기" .
- CIFS 구성을 위한 DNS 및 Active Directory.

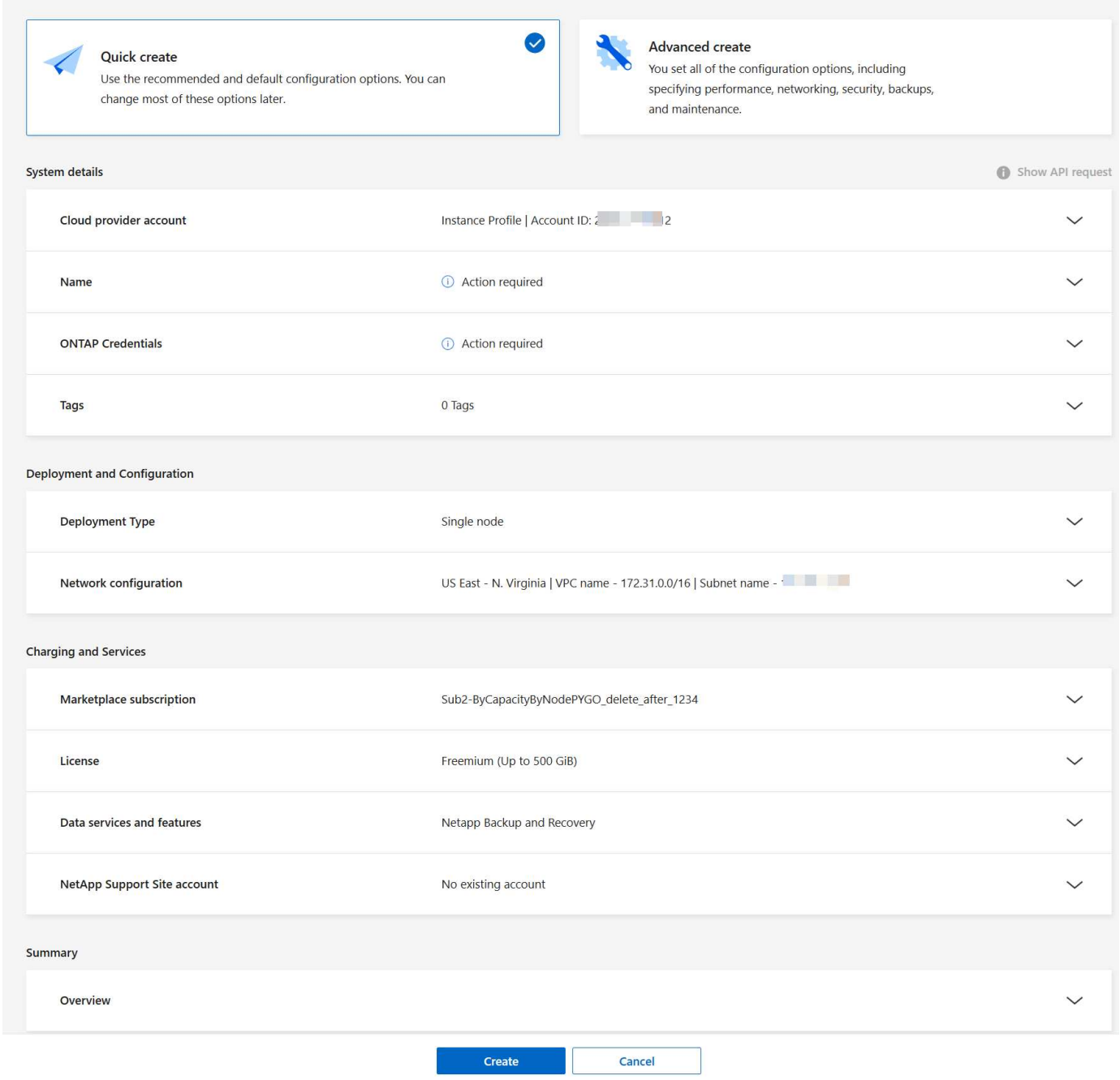
  자세한 내용은 다음을 참조하세요."AWS의 Cloud Volumes ONTAP 에 대한 네트워킹 요구 사항" .

이 작업에 관하여

Cloud Volumes ONTAP 시스템을 생성한 직후, NetApp Console 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 콘솔은 즉시 인스턴스를 종료한 다음 시스템 배포를 시작합니다. 콘솔에서 연결을 확인할 수 없는 경우 시스템 생성이 실패합니다. 테스트 인스턴스는 다음 중 하나입니다. `t2.nano` (기본 VPC 테넌시의 경우) 또는 `m3.medium` (전용 VPC 테넌시용).

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 캔버스 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. **Amazon Web Services** > * Cloud Volumes ONTAP* > 새로 추가*를 선택합니다. 기본적으로 *빠른 생성 옵션이 선택되어 있습니다.



시스템 세부 정보

1. 클라우드 공급자 계정: 선택한 콘솔 에이전트에 따라 계정 세부 정보가 자동으로 채워집니다. 여러 계정이 있는 경우 사용할 계정을 선택하세요. 콘솔 에이전트를 사용할 수 없는 경우 다음 메시지가 표시됩니다. "콘솔 에이전트 생성" .
2. 이름: 시스템 이름입니다. 콘솔은 시스템(클러스터) 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
3. * ONTAP 자격 증명* 이는 Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하면 ONTAP System Manager나 ONTAP CLI를 통해 Cloud Volumes ONTAP 에 연결할 수 있습니다. 기본 *admin* 사용자 이름을 유지하거나 사용자 지정 사용자 이름으로 변경할 수 있습니다.
4. 태그 AWS 태그는 AWS 리소스에 대한 메타데이터입니다. 콘솔은 Cloud Volumes ONTAP 인스턴스와 인스턴스에 연결된 각 AWS 리소스에 태그를 추가합니다. Cloud Volumes ONTAP 시스템을 생성할 때 사용자 인터페이스에서 최대 15개의 태그를 추가할 수 있으며, 시스템을 생성한 후에 태그를 더 추가할 수 있습니다. API는 시스템을 생성할

때 태그를 4개로 제한하지 않습니다. 태그에 대한 정보는 다음을 참조하세요. "AWS 설명서: Amazon EC2 리소스 태그 지정" .

배포 및 구성

1. 배포 유형: 사용할 배포 유형을 선택합니다. 단일 노드, 단일 가용성 영역(AZ)의 고가용성(HA), 여러 AZ의 HA입니다.
2. 네트워크 구성 : 기록해 두신 네트워크 정보를 입력하세요. "AWS 워크시트" .
   a. **AWS** 지역: 기본적으로 서브넷 리소스가 있는 VPC가 있는 연결된 클라우드 계정의 지역이 선택됩니다.
   b. **VPC**: 서브넷이 있는 AWS 지역의 VPC를 입력하세요. 서브넷이 없으면 VPC의 기본값이 선택됩니다.
   c. 서브넷: 단일 노드 배포 또는 단일 AZ의 HA 배포에 대해서만 VPC에 대한 서브넷을 선택할 수 있습니다.

고가용성

HA 구성을 선택한 경우 다음 정보를 입력하세요.

단일 **AZ**의 **HA**

1. 중재자 접근: 중재자 접근 정보를 지정합니다. 중재자는 HA 쌍의 상태를 모니터링하고 장애 발생 시 쿼럼을 제공하는 별도의 인스턴스입니다. AWS EC2 서비스에 연결할 수 있도록 중재자 인스턴스에 키 쌍 이름을 제공하고 연결 방법을 선택합니다.

여러 **AZ**의 **HA**

1. 가용성 영역 및 중재자: 각 노드와 중재자에 대한 가용성 영역(AZ)과 Cloud Volumes ONTAP HA 쌍을 배포하려는 해당 서브넷을 선택합니다.
2. 유동 **IP**: 여러 AZ를 선택한 경우 NFS 및 CIFS 서비스와 클러스터 및 SVM 관리를 위한 유동 IP 주소를 지정합니다. IP 주소는 해당 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 추가 세부 사항은 다음을 참조하세요."여러 AZ에서 Cloud Volumes ONTAP HA에 대한 AWS 네트워킹 요구 사항" .
3. 중재자 접근: 중재자 접근 정보를 지정합니다. 중재자는 HA 쌍의 상태를 모니터링하고 장애 발생 시 쿼럼을 제공하는 별도의 인스턴스입니다. AWS EC2 서비스에 연결할 수 있도록 중재자 인스턴스에 키 쌍 이름을 제공하고 연결 방법을 선택합니다.
4. 경로 테이블: 여러 AZ를 선택한 경우, 플로팅 IP 주소에 대한 경로가 포함된 경로 테이블을 선택합니다. 두 개 이상의 경로 테이블이 있는 경우 올바른 경로 테이블을 선택하는 것이 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP HA 쌍에 액세스하지 못할 수도 있습니다. 경로 테이블에 대한 자세한 내용은 다음을 참조하세요. "AWS 문서: 라우팅 테이블" .

충전 및 서비스

1. 마켓플레이스 구독: 이 Cloud Volumes ONTAP 시스템과 함께 사용할 AWS 마켓플레이스 구독을 선택하세요.
2. 라이선스: 이 Cloud Volumes ONTAP 시스템에 사용할 라이선스 유형을 선택하세요. Professional, Essential, Premium 라이선스 중에서 선택할 수 있습니다. 다양한 라이센스에 대한 정보는 다음을 참조하세요."Cloud Volumes ONTAP 라이선스에 대해 알아보세요" .
3. 데이터 서비스 및 기능: Cloud Volumes ONTAP 에서 사용하지 않으려는 서비스를 활성화 상태로 유지하거나 비활성화합니다.
   - "NetApp 분류에 대해 자세히 알아보세요"
   - "NetApp Backup and Recovery 에 대해 자세히 알아보세요"
   - "Cloud Volumes ONTAP 의 WORM 스토리지에 대해 알아보세요"

WORM 및 데이터 계층화를 활용하려면 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 시스템을 배포해야 합니다.

- * NetApp 지원 사이트 계정*: 계정이 여러 개인 경우 사용할 계정을 선택하세요.

요약

입력한 세부 정보를 확인하거나 편집한 다음 *만들기*를 클릭하세요.

배포 프로세스가 완료된 후에는 AWS 클라우드 포털에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

관련 링크

- "Cloud Volumes ONTAP 구성 계획"
- "고급 배포를 사용하여 AWS에 Cloud Volumes ONTAP 배포"

AWS에서 Cloud Volumes ONTAP 실행

AWS에서 단일 시스템 구성이나 HA 쌍으로 Cloud Volumes ONTAP 시작할 수 있습니다. 이 방법은 빠른 배포 방법보다 더 많은 구성 옵션과 유연성을 제공하는 고급 배포 환경을 제공합니다.

시작하기 전에

시작하기 전에 다음 사항이 필요합니다.

- 이미 실행 중인 콘솔 에이전트입니다.
  - 당신은 ~을 가져야합니다 "시스템과 연결된 콘솔 에이전트" .
  - "항상 콘솔 에이전트를 실행 상태로 두어야 합니다." .
- 사용하려는 구성에 대한 이해.

  구성을 선택하고 관리자로부터 AWS 네트워킹 정보를 얻어서 준비했어야 합니다. 자세한 내용은 다음을 참조하세요."Cloud Volumes ONTAP 구성 계획" .

- Cloud Volumes ONTAP 에 대한 라이선싱을 설정하는 데 필요한 사항에 대한 이해.

  "라이선싱 설정 방법 알아보기" .

- CIFS 구성을 위한 DNS 및 Active Directory.

  자세한 내용은 다음을 참조하세요."AWS의 Cloud Volumes ONTAP 에 대한 네트워킹 요구 사항" .

AWS에서 단일 노드 Cloud Volumes ONTAP 시스템 실행

AWS에서 Cloud Volumes ONTAP 시작하려면 NetApp Console 에서 새 시스템을 만들어야 합니다.

이 작업에 관하여

시스템을 생성한 직후, 콘솔은 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 콘솔은 즉시 인스턴스를 종료한 다음 Cloud Volumes ONTAP 시스템 배포를 시작합니다. 연결성을 검증할 수 없으면 시스템 생성이 실패합니다. 테스트 인스턴스는 다음 중 하나입니다. `t2.nano` (기본 VPC 테넌시의 경우) 또는 `m3.medium` (전용 VPC 테넌시용).

단계

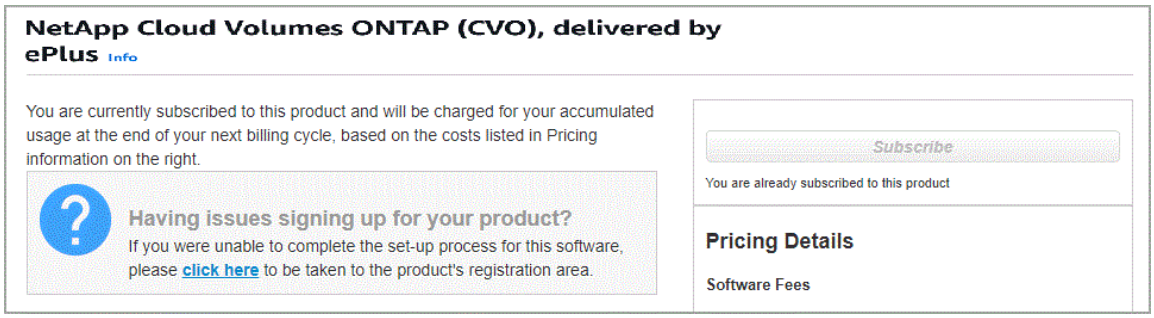
1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. *Amazon Web Services*와 * Cloud Volumes ONTAP Single Node*를 선택하세요.
4. 고급 만들기*를 선택하세요. 기본적으로 *빠른 생성 모드가 선택되어 있으므로 기본값에 대한 메시지가 표시될 수 있습니다. *계속*을 클릭하세요.
5. 메시지가 표시되면 "콘솔 에이전트 생성" .
6. 세부 정보 및 자격 증명: 선택적으로 AWS 자격 증명과 구독을 변경하고, 시스템 이름을 입력하고, 필요한 경우 태그를 추가한 다음 비밀번호를 입력합니다.

   이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
태그 추가	AWS 태그는 AWS 리소스에 대한 메타데이터입니다. 콘솔은 Cloud Volumes ONTAP 인스턴스와 인스턴스에 연결된 각 AWS 리소스에 태그를 추가합니다. 시스템을 생성할 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 시스템을 생성한 후에 태그를 더 추가할 수 있습니다. API는 시스템을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 정보는 다음을 참조하세요. "AWS 설명서: Amazon EC2 리소스 태그 지정" .
사용자 이름과 비밀번호	이는 Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하면 ONTAP System Manager나 ONTAP CLI를 통해 Cloud Volumes ONTAP 에 연결할 수 있습니다. 기본 *admin* 사용자 이름을 유지하거나 사용자 지정 사용자 이름으로 변경하세요.
자격 증명 편집	이 시스템을 배포하려는 계정과 연결된 AWS 자격 증명을 선택하세요. AWS 마켓플레이스 구독을 연결하여 이 Cloud Volumes ONTAP 시스템과 함께 사용할 수도 있습니다. 선택한 자격 증명을 새 AWS 마켓플레이스 구독과 연결하려면 *구독 추가*를 클릭하세요. 구독은 연간 계약 또는 시간당 요금으로 Cloud Volumes ONTAP 결제할 수 있습니다. "NetApp Console 에 추가 AWS 자격 증명을 추가하는 방법을 알아보세요." .

여러 IAM 사용자가 동일한 AWS 계정에서 작업하는 경우 각 사용자는 구독해야 합니다. 첫 번째 사용자가 구독한 후, AWS 마켓플레이스는 다음 사용자에게 이미 구독되었음을 알립니다(아래 이미지 참조). AWS 계정에 대한 구독이 있는 동안 각 IAM 사용자는 해당 구독에 자신을 연결해야 합니다. 아래에 표시된 메시지가 나타나면 여기를 클릭 링크를 클릭하여 콘솔 웹사이트로 이동하여 프로세스를 완료하세요

.



7. 서비스: Cloud Volumes ONTAP 에서 사용하지 않으려는 서비스를 활성화 상태로 유지하거나 개별 서비스를 비활성화합니다.
   - "NetApp Data Classification 에 대해 자세히 알아보세요"
   - "NetApp Backup and Recovery 에 대해 자세히 알아보세요"

   WORM 및 데이터 계층화를 활용하려면 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 시스템을 배포해야 합니다.

8. 위치 및 연결: 기록한 네트워크 정보를 입력하세요. "AWS 워크시트" .

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
VPC	AWS Outpost가 있는 경우 Outpost VPC를 선택하여 해당 Outpost에 단일 노드 Cloud Volumes ONTAP 시스템을 배포할 수 있습니다. 경험은 AWS에 있는 다른 VPC와 동일합니다.
생성된 보안 그룹	콘솔에서 보안 그룹을 생성하도록 허용하는 경우 트래픽 허용 방법을 선택해야 합니다. • *선택한 VPC만*을 선택하는 경우 인바운드 트래픽의 소스는 선택한 VPC의 서브넷 범위와 콘솔 에이전트가 있는 VPC의 서브넷 범위입니다. 이것은 권장되는 옵션입니다. • *모든 VPC*를 선택하면 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 보안 그룹 사용	기존 방화벽 정책을 사용하는 경우 필요한 규칙이 포함되어 있는지 확인하세요. "Cloud Volumes ONTAP 의 방화벽 규칙에 대해 알아보세요" .

9. 데이터 암호화: 데이터 암호화를 사용하지 않거나 AWS에서 관리하는 암호화를 선택합니다.

   AWS 관리 암호화의 경우, 귀하의 계정이나 다른 AWS 계정에서 다른 고객 마스터 키(CMK)를 선택할 수 있습니다.

   Cloud Volumes ONTAP 시스템을 생성한 후에는 AWS 데이터 암호화 방법을 변경할 수 없습니다.

"Cloud Volumes ONTAP 에 AWS KMS를 설정하는 방법을 알아보세요." .

"지원되는 암호화 기술에 대해 자세히 알아보세요" .

10. 청구 방법 및 **NSS** 계정: 이 시스템에서 사용할 청구 옵션을 지정한 다음 NetApp 지원 사이트 계정을 지정하세요.
    - "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요" .
    - "라이선싱 설정 방법 알아보기" .
11. * Cloud Volumes ONTAP 구성* (연간 AWS 마켓플레이스 계약에만 해당): 기본 구성을 검토하고 *계속*을 클릭하거나 *구성 변경*을 클릭하여 원하는 구성을 선택합니다.

    기본 구성을 유지하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.

12. 사전 구성된 패키지: Cloud Volumes ONTAP 빠르게 시작하려면 패키지 중 하나를 선택하거나, *구성 변경*을 클릭하여 원하는 구성을 선택하세요.

    패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.

13. **IAM** 역할: 콘솔에서 역할을 자동으로 생성하도록 기본 옵션을 유지하는 것이 가장 좋습니다.

    자체 정책을 사용하려면 다음 사항을 충족해야 합니다."Cloud Volumes ONTAP 노드에 대한 정책 요구 사항" .

14. 라이선스: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 인스턴스 유형과 인스턴스 테넌시를 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 공급 또는 패치 릴리스가 제공되는 경우 콘솔은 시스템을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.13.1을 선택하고 9.13.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리스에서 다른 릴리스로 전달되지 않습니다(예: 9.13에서 9.14로 전달).

15. 기본 스토리지 리소스: 디스크 유형을 선택하고, 기본 스토리지를 구성하고, 데이터 계층화를 계속 사용할지 여부를 선택합니다.

    다음 사항에 유의하세요.

    - 디스크 유형은 초기 볼륨(및 집계)을 위한 것입니다. 이후 볼륨(및 집계)에 대해 다른 디스크 유형을 선택할 수 있습니다.
    - gp3 또는 io1 디스크를 선택하면 콘솔은 AWS의 Elastic Volumes 기능을 사용하여 필요에 따라 기본 스토리지 디스크 용량을 자동으로 늘립니다. 스토리지 요구 사항에 따라 초기 용량을 선택하고 Cloud Volumes ONTAP 배포한 후 수정할 수 있습니다. "AWS에서 Elastic Volumes 지원에 대해 자세히 알아보세요" .
    - gp2 또는 st1 디스크를 선택하는 경우 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔에서 생성하는 추가 집계에 대한 디스크 크기를 선택할 수 있습니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.
    - 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
    - 데이터 계층화를 비활성화하면 이후 집계에서 활성화할 수 있습니다.

      "데이터 계층화 작동 방식 알아보기" .

16. 쓰기 속도 및 **WORM**:

    a. 원하는 경우 보통 또는 높음 쓰기 속도를 선택하세요.

"쓰기 속도에 대해 자세히 알아보세요" .

b. 원하는 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

Cloud Volumes ONTAP 버전 9.7 이하에서 데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로 되돌리거나 다운그레이드하는 것이 차단됩니다.

"WORM 스토리지에 대해 자세히 알아보세요" .

a. WORM 저장소를 활성화하는 경우 보존 기간을 선택하세요.

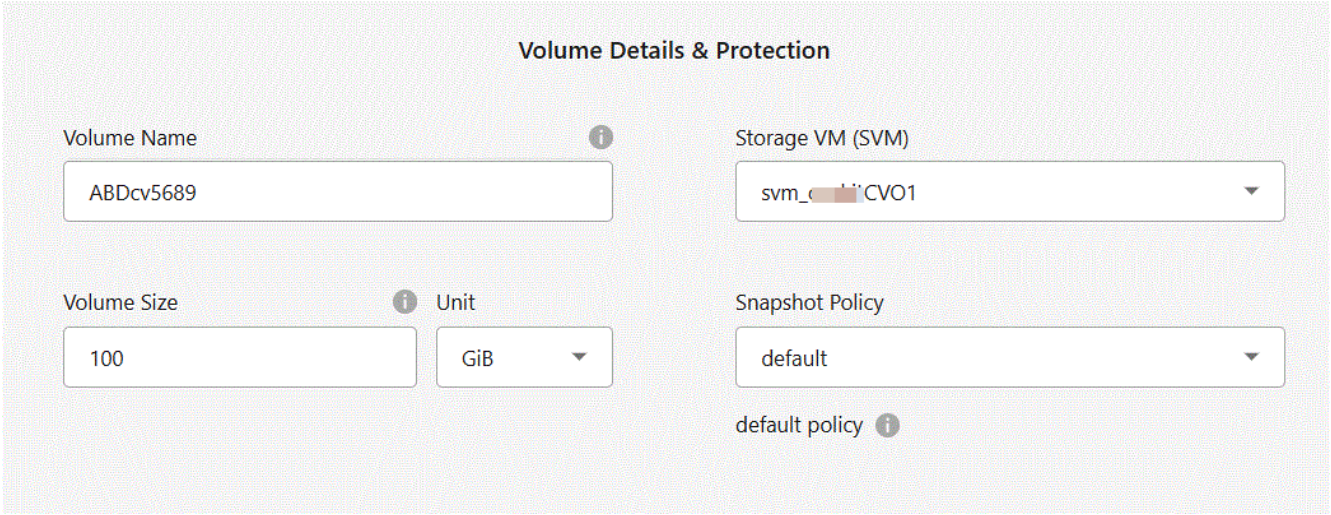
17. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

"지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝을 활성화하는지 여부에 따라 크게 달라집니다. 씬 프로비저닝을 활성화하면 현재 사용 가능한 물리적 저장소보다 큰 볼륨을 만들 수 있습니다.
액세스 제어(NFS에만 해당)	내보내기 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 콘솔은 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS에만 해당)	이러한 필드를 사용하면 사용자 및 그룹의 공유 액세스 수준(액세스 제어 목록 또는 ACL이라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자나 그룹, 또는 UNIX 사용자나 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사 정책은 NetApp 스냅샷 복사본이 자동으로 생성되는 빈도와 수를 지정합니다. NetApp 스냅샷 복사본은 성능에 영향을 미치지 않고 최소한의 저장 공간만 필요한 특정 시점의 파일 시스템 이미지입니다. 기본 정책을 선택하거나 아무것도 선택하지 않을 수 있습니다. 일시적인 데이터의 경우 '없음'을 선택할 수 있습니다. 예를 들어 Microsoft SQL Server의 경우 tempdb를 선택합니다.
고급 옵션(NFS에만 해당)	볼륨에 대한 NFS 버전을 선택합니다: NFSv3 또는 NFSv4.
이니시에이터 그룹 및 IQN(iSCSI에만 해당)	iSCSI 스토리지 대상은 LUN(논리 단위)이라고 하며 호스트에 표준 블록 장치로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름 테이블이며, 어떤 이니시에이터가 어떤 LUN에 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 컨버지드 네트워크 어댑터(CNA) 또는 전용 호스트 버스 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 정규화된 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후, "IQN을 사용하여 호스트에서 LUN에 연결합니다." .

다음 이미지는 볼륨 생성 마법사의 첫 번째 페이지를 보여줍니다.



18. **CIFS** 설정: CIFS 프로토콜을 선택한 경우 CIFS 서버를 설정합니다.

필드	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인의 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.
도메인에 가입할 수 있는 권한이 있는 자격 증명	AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.
CIFS 서버 NetBIOS 이름	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Cloud Volumes ONTAP 의 AD 서버로 AWS Managed Microsoft AD를 구성하는 경우 이 필드에 *OU=Computers,OU=corp*를 입력해야 합니다.
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 대부분의 경우 도메인은 AD 도메인과 동일합니다.
NTP 서버	Active Directory DNS를 사용하여 NTP 서버를 구성하려면 *Active Directory 도메인 사용*을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 를 참조하세요 "NetApp Console 자동화 문서" 자세한 내용은. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

19. 사용 프로필, 디스크 유형 및 계층화 정책: 스토리지 효율성 기능을 활성화할지 여부를 선택하고 필요한 경우 볼륨 계층화 정책을 편집합니다.

    자세한 내용은 다음을 참조하세요."볼륨 사용 프로필 이해" ,"데이터 계층화 개요" , 그리고 "KB: CVO에서는 어떤 인라인 스토리지 효율성 기능이 지원되나요?"

20. 검토 및 승인: 선택 사항을 검토하고 확인합니다.

    a. 구성에 대한 세부 정보를 검토하세요.

    b. *자세한 정보*를 클릭하면 콘솔에서 구매할 지원 및 AWS 리소스에 대한 세부 정보를 검토할 수 있습니다.

c. 이해합니다... 확인란을 선택하세요.

d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 인스턴스를 시작합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 인스턴스를 시작하는 데 문제가 있는 경우 실패 메시지를 검토하세요. 시스템을 선택하고 *환경 다시 만들기*를 클릭할 수도 있습니다.

추가 도움말을 보려면 다음으로 이동하세요. "NetApp Cloud Volumes ONTAP 지원" .

배포 프로세스가 완료된 후에는 AWS 클라우드 포털에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

당신이 완료한 후

- CIFS 공유를 프로비저닝한 경우 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 ONTAP 시스템 관리자나 ONTAP CLI를 사용하세요.

  할당량을 사용하면 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적할 수 있습니다.

AWS에서 Cloud Volumes ONTAP HA 쌍 실행

AWS에서 Cloud Volumes ONTAP HA 쌍을 시작하려면 콘솔에서 HA 시스템을 만들어야 합니다.

한정

현재 AWS Outposts에서는 HA 쌍이 지원되지 않습니다.

이 작업에 관하여

Cloud Volumes ONTAP 시스템을 생성한 직후, 콘솔은 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 콘솔은 즉시 인스턴스를 종료한 다음 Cloud Volumes ONTAP 시스템 배포를 시작합니다. 연결성을 검증할 수 없으면 시스템 생성이 실패합니다. 테스트 인스턴스는 다음 중 하나입니다. `t2.nano` (기본 VPC 테넌시의 경우) 또는 `m3.medium` (전용 VPC 테넌시용).

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 화면의 지시를 따르세요.
3. *Amazon Web Services*와 * Cloud Volumes ONTAP HA*를 선택하세요.

   일부 AWS 로컬 영역을 사용할 수 있습니다.

   AWS 로컬 영역을 사용하려면 먼저 로컬 영역을 활성화하고 AWS 계정의 로컬 영역에 서브넷을 생성해야 합니다. AWS 로컬 영역에 가입하기* 및 Amazon VPC를 로컬 영역으로 확장하기* 단계를 따르세요."AWS 튜토리얼 "AWS 로컬 영역을 사용하여 저지연 애플리케이션 배포 시작하기"" .

   콘솔 에이전트 3.9.36 이하를 실행 중인 경우 다음을 추가해야 합니다. `DescribeAvailabilityZones` AWS

EC2 콘솔에서 AWS 역할에 대한 권한.

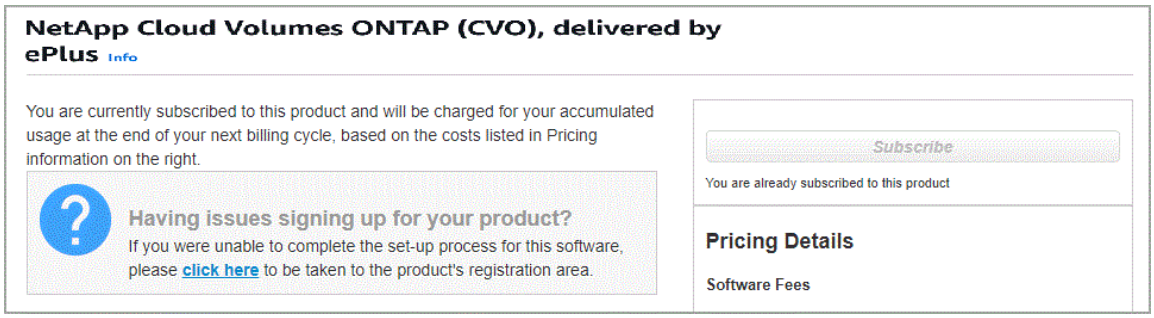
4. 세부 정보 및 자격 증명: 선택적으로 AWS 자격 증명과 구독을 변경하고, 시스템 이름을 입력하고, 필요한 경우 태그를 추가한 다음 비밀번호를 입력합니다.

   이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
태그 추가	AWS 태그는 AWS 리소스에 대한 메타데이터입니다. 콘솔은 Cloud Volumes ONTAP 인스턴스와 인스턴스에 연결된 각 AWS 리소스에 태그를 추가합니다. 시스템을 생성할 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 시스템을 생성한 후에 태그를 더 추가할 수 있습니다. API는 시스템을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 정보는 다음을 참조하세요. "AWS 설명서: Amazon EC2 리소스 태그 지정" .
사용자 이름과 비밀번호	이는 Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하면 ONTAP System Manager나 ONTAP CLI를 통해 Cloud Volumes ONTAP 에 연결할 수 있습니다. 기본 *admin* 사용자 이름을 유지하거나 사용자 지정 사용자 이름으로 변경하세요.
자격 증명 편집	이 Cloud Volumes ONTAP 시스템에 사용할 AWS 자격 증명과 마켓플레이스 구독을 선택하세요. 선택한 자격 증명을 새 AWS 마켓플레이스 구독과 연결하려면 *구독 추가*를 클릭하세요. 구독은 연간 계약 또는 시간당 요금으로 Cloud Volumes ONTAP 결제할 수 있습니다. NetApp 에서 직접 라이선스를 구매한 경우(BYOL(Bring Your Own License)), AWS 구독은 필요하지 않습니다. NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 에 대한 BYOL 라이선싱의 제한된 가용성" . "콘솔에 추가 AWS 자격 증명을 추가하는 방법을 알아보세요." .

여러 IAM 사용자가 동일한 AWS 계정에서 작업하는 경우 각 사용자는 구독해야 합니다. 첫 번째 사용자가 구독한 후, AWS 마켓플레이스는 아래 이미지에서 볼 수 있듯이 후속 사용자에게 이미 구독되었음을 알립니다. AWS 계정에 대한 구독이 있는 동안 각 IAM 사용자는 해당 구독에 자신을 연결해야 합니다. 아래에 표시된 메시지가 나타나면 여기를 클릭 링크를 클릭하여 콘솔 웹사이트로 이동하여 프로세스를 완료하세요

.



5. 서비스: 해당 Cloud Volumes ONTAP 시스템에서 사용하지 않으려는 서비스를 활성화 상태로 유지하거나 개별 서비스를 비활성화합니다.

   - "NetApp Data Classification 에 대해 자세히 알아보세요"

◦ "백업 및 복구에 대해 자세히 알아보세요"

WORM 및 데이터 계층화를 활용하려면 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 시스템을 배포해야 합니다.

6. **HA** 배포 모델: HA 구성을 선택하세요.

   배포 모델 개요는 다음을 참조하세요."AWS용 Cloud Volumes ONTAP HA" .

7. 위치 및 연결(단일 가용성 영역(AZ)) 또는 지역 및 **VPC**(여러 AZ): AWS 워크시트에 기록한 네트워크 정보를 입력합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
생성된 보안 그룹	콘솔에서 보안 그룹을 생성하도록 허용하는 경우 트래픽 허용 방법을 선택해야 합니다. • *선택한 VPC만*을 선택하는 경우 인바운드 트래픽의 소스는 선택한 VPC의 서브넷 범위와 콘솔 에이전트가 있는 VPC의 서브넷 범위입니다. 이것은 권장되는 옵션입니다. • *모든 VPC*를 선택하면 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 보안 그룹 사용	기존 방화벽 정책을 사용하는 경우 필요한 규칙이 포함되어 있는지 확인하세요. "Cloud Volumes ONTAP 의 방화벽 규칙에 대해 알아보세요" .

8. 연결 및 **SSH** 인증: HA 쌍과 중재자에 대한 연결 방법을 선택합니다.
9. 유동 **IP**: 여러 AZ를 선택한 경우 유동 IP 주소를 지정하세요.

   IP 주소는 해당 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 추가 세부 사항은 다음을 참조하세요. "여러 AZ에서 Cloud Volumes ONTAP HA에 대한 AWS 네트워킹 요구 사항" .

10. 경로 테이블: 여러 AZ를 선택한 경우, 플로팅 IP 주소에 대한 경로를 포함해야 하는 경로 테이블을 선택합니다.

    두 개 이상의 경로 테이블이 있는 경우 올바른 경로 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP HA 쌍에 액세스하지 못할 수도 있습니다. 경로 테이블에 대한 자세한 내용은 다음을 참조하세요. "AWS 문서: 라우팅 테이블" .

11. 데이터 암호화: 데이터 암호화를 사용하지 않거나 AWS에서 관리하는 암호화를 선택합니다.

    AWS 관리 암호화의 경우, 귀하의 계정이나 다른 AWS 계정에서 다른 고객 마스터 키(CMK)를 선택할 수 있습니다.

    Cloud Volumes ONTAP 시스템을 생성한 후에는 AWS 데이터 암호화 방법을 변경할 수 없습니다.

    "Cloud Volumes ONTAP 에 AWS KMS를 설정하는 방법을 알아보세요." .

    "지원되는 암호화 기술에 대해 자세히 알아보세요" .

12. 청구 방법 및 **NSS** 계정: 이 시스템에서 사용할 청구 옵션을 지정한 다음 NetApp 지원 사이트 계정을 지정하세요.

- "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요" .
- "라이선싱 설정 방법 알아보기" .

13. * Cloud Volumes ONTAP 구성* (연간 AWS Marketplace 계약에만 해당): 기본 구성을 검토하고 *계속*을 클릭하거나 *구성 변경*을 클릭하여 원하는 구성을 선택합니다.

    기본 구성을 유지하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.

14. 사전 구성된 패키지(시간별 또는 BYOL만 해당): Cloud Volumes ONTAP 빠르게 시작하려면 패키지 중 하나를 선택하거나, *구성 변경*을 클릭하여 원하는 구성을 선택하세요.

    패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.

15. **IAM** 역할: 콘솔에서 역할을 자동으로 생성하도록 기본 옵션을 유지하는 것이 가장 좋습니다.

    자체 정책을 사용하려면 다음 사항을 충족해야 합니다."Cloud Volumes ONTAP 노드 및 HA 중재자에 대한 정책 요구 사항" .

16. 라이선스: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 인스턴스 유형과 인스턴스 테넌시를 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 공급 또는 패치 릴리스가 제공되는 경우 콘솔은 시스템을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.13.1을 선택하고 9.13.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리스에서 다른 릴리스로 전달되지 않습니다(예: 9.13에서 9.14로 전달).

17. 기본 스토리지 리소스: 디스크 유형을 선택하고, 기본 스토리지를 구성하고, 데이터 계층화를 계속 사용할지 여부를 선택합니다.

    다음 사항에 유의하세요.

    - 디스크 유형은 초기 볼륨(및 집계)을 위한 것입니다. 이후 볼륨(및 집계)에 대해 다른 디스크 유형을 선택할 수 있습니다.
    - gp3 또는 io1 디스크를 선택하면 콘솔은 AWS의 Elastic Volumes 기능을 사용하여 필요에 따라 기본 스토리지 디스크 용량을 자동으로 늘립니다. 스토리지 요구 사항에 따라 초기 용량을 선택하고 Cloud Volumes ONTAP 배포한 후 수정할 수 있습니다. "AWS에서 Elastic Volumes 지원에 대해 자세히 알아보세요" .
    - gp2 또는 st1 디스크를 선택하는 경우 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔에서 생성하는 추가 집계에 대한 디스크 크기를 선택할 수 있습니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.
    - 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
    - 데이터 계층화를 비활성화하면 이후 집계에서 활성화할 수 있습니다.

      "데이터 계층화 작동 방식 알아보기" .

18. 쓰기 속도 및 **WORM**:

    a. 원하는 경우 보통 또는 높음 쓰기 속도를 선택하세요.

       "쓰기 속도에 대해 자세히 알아보세요" .

    b. 원하는 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

Cloud Volumes ONTAP 버전 9.7 이하에서 데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로 되돌리거나 다운그레이드하는 것이 차단됩니다.

"WORM 스토리지에 대해 자세히 알아보세요" .

a. WORM 저장소를 활성화하는 경우 보존 기간을 선택하세요.

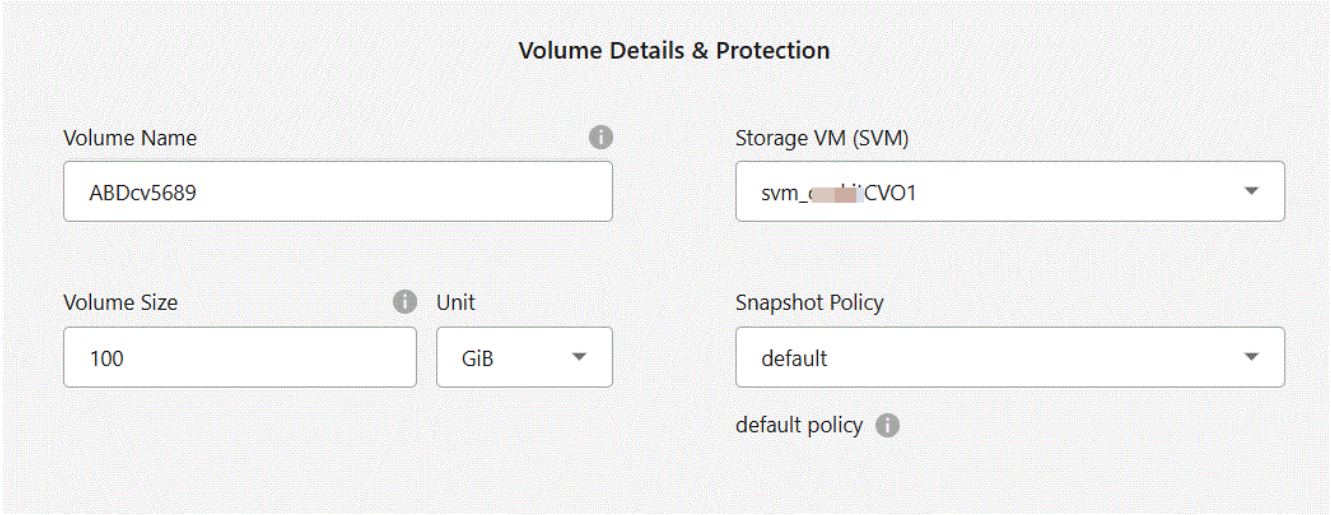
19. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

"지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝을 활성화하는지 여부에 따라 크게 달라집니다. 씬 프로비저닝을 활성화하면 현재 사용 가능한 물리적 저장소보다 큰 볼륨을 만들 수 있습니다.
액세스 제어(NFS에만 해당)	내보내기 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 콘솔은 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS에만 해당)	이러한 필드를 사용하면 사용자 및 그룹의 공유 액세스 수준(액세스 제어 목록 또는 ACL이라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자나 그룹, 또는 UNIX 사용자나 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사 정책은 NetApp 스냅샷 복사본이 자동으로 생성되는 빈도와 수를 지정합니다. NetApp 스냅샷 복사본은 성능에 영향을 미치지 않고 최소한의 저장 공간만 필요한 특정 시점의 파일 시스템 이미지입니다. 기본 정책을 선택하거나 아무것도 선택하지 않을 수 있습니다. 일시적인 데이터의 경우 '없음'을 선택할 수 있습니다. 예를 들어 Microsoft SQL Server의 경우 tempdb를 선택합니다.
고급 옵션(NFS에만 해당)	볼륨에 대한 NFS 버전을 선택합니다: NFSv3 또는 NFSv4.
이니시에이터 그룹 및 IQN(iSCSI에만 해당)	iSCSI 스토리지 대상은 LUN(논리 단위)이라고 하며 호스트에 표준 블록 장치로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름 테이블이며, 어떤 이니시에이터가 어떤 LUN에 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 컨버지드 네트워크 어댑터(CNA) 또는 전용 호스트 버스 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 정규화된 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후, "IQN을 사용하여 호스트에서 LUN에 연결합니다." .

다음 이미지는 볼륨 생성 마법사의 첫 번째 페이지를 보여줍니다.



20. **CIFS** 설정: CIFS 프로토콜을 선택한 경우 CIFS 서버를 설정합니다.

필드	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인의 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.
도메인에 가입할 수 있는 권한이 있는 자격 증명	AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.
CIFS 서버 NetBIOS 이름	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Cloud Volumes ONTAP 의 AD 서버로 AWS Managed Microsoft AD를 구성하는 경우 이 필드에 *OU=Computers,OU=corp*를 입력해야 합니다.
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 대부분의 경우 도메인은 AD 도메인과 동일합니다.
NTP 서버	Active Directory DNS를 사용하여 NTP 서버를 구성하려면 *Active Directory 도메인 사용*을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 를 참조하세요 "NetApp Console 자동화 문서" 자세한 내용은. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

21. 사용 프로필, 디스크 유형 및 계층화 정책: 스토리지 효율성 기능을 활성화할지 여부를 선택하고 필요한 경우 볼륨 계층화 정책을 편집합니다.

    자세한 내용은 다음을 참조하세요."볼륨 사용 프로필을 선택하세요" 그리고"데이터 계층화 개요" .

22. 검토 및 승인: 선택 사항을 검토하고 확인합니다.
    a. 구성에 대한 세부 정보를 검토하세요.
    b. *자세한 정보*를 클릭하면 콘솔에서 구매할 지원 및 AWS 리소스에 대한 세부 정보를 검토할 수 있습니다.
    c. 이해합니다... 확인란을 선택하세요.

d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP HA 쌍을 시작합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

HA 쌍을 시작하는 데 문제가 발생하면 실패 메시지를 검토하세요. 시스템을 선택하고 '환경 다시 만들기'를 클릭할 수도 있습니다.

추가 도움말을 보려면 다음으로 이동하세요. "NetApp Cloud Volumes ONTAP 지원" .

당신이 완료한 후

- CIFS 공유를 프로비저닝한 경우 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 ONTAP 시스템 관리자나 ONTAP CLI를 사용하세요.

  할당량을 사용하면 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적할 수 있습니다.

> 배포 프로세스가 완료된 후에는 AWS 클라우드 포털에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

관련 링크

- "Cloud Volumes ONTAP 구성 계획"
- "빠른 배포를 사용하여 AWS에 Cloud Volumes ONTAP 배포"

AWS Secret Cloud 또는 AWS Top Secret Cloud에 Cloud Volumes ONTAP 배포

표준 AWS 지역과 유사하게 NetApp Console 사용할 수 있습니다."AWS 시크릿 클라우드" 그리고"AWS 최고 비밀 클라우드" 클라우드 스토리지에 엔터프라이즈급 기능을 제공하는 Cloud Volumes ONTAP 구축하세요. AWS Secret Cloud와 Top Secret Cloud는 미국 정보 커뮤니티에 한정된 폐쇄된 지역입니다. 이 페이지의 지침은 AWS Secret Cloud와 Top Secret Cloud 지역 사용자에게만 적용됩니다.

시작하기 전에

시작하기 전에 AWS Secret Cloud와 Top Secret Cloud에서 지원되는 버전을 검토하고 콘솔에서 비공개 모드에 대해 알아보세요.

- AWS Secret Cloud 및 Top Secret Cloud에서 지원되는 다음 버전을 검토하세요.
  - Cloud Volumes ONTAP 9.12.1 P2
  - 콘솔 에이전트 버전 3.9.32

    AWS에서 Cloud Volumes ONTAP 배포하고 관리하려면 콘솔 에이전트가 필요합니다. 콘솔 에이전트 인스턴스에 설치된 소프트웨어에서 콘솔에 로그인합니다. AWS Secret Cloud 및 Top Secret Cloud에서는 콘솔용 SaaS 웹사이트가 지원되지 않습니다.
- 개인 모드에 대해 알아보세요

AWS Secret Cloud와 Top Secret Cloud에서는 콘솔이 _비공개 모드_로 작동합니다. 개인 모드에서는 콘솔에서 SaaS 계층에 연결할 수 없습니다. 콘솔 에이전트에 액세스할 수 있는 로컬 웹 기반 애플리케이션을 통해 콘솔에 액세스할 수 있습니다.

개인 모드의 작동 방식에 대해 자세히 알아보려면 다음을 참조하세요."콘솔의 개인 배포 모드" .

1단계**:** 네트워킹 설정

Cloud Volumes ONTAP 제대로 작동할 수 있도록 AWS 네트워킹을 설정하세요.

단계

1. 콘솔 에이전트와 Cloud Volumes ONTAP 인스턴스의 인스턴스를 시작할 VPC와 서브넷을 선택합니다.
2. VPC와 서브넷이 콘솔 에이전트와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인하세요.
3. Amazon Simple Storage Service(Amazon S3) 서비스에 대한 VPC 엔드포인트를 설정합니다.

   Cloud Volumes ONTAP 에서 저비용 개체 스토리지로 콜드 데이터를 계층화하려면 VPC 엔드포인트가 필요합니다.

2단계**:** 권한 설정

AWS Secret Cloud 또는 Top Secret Cloud에서 작업을 수행하는 데 필요한 권한을 Console 에이전트와 Cloud Volumes ONTAP 에 제공하는 IAM 정책과 역할을 설정합니다.

다음 각각에 대해 IAM 정책과 IAM 역할이 필요합니다.

- 콘솔 에이전트의 인스턴스
- Cloud Volumes ONTAP 인스턴스
- HA 쌍의 경우 Cloud Volumes ONTAP HA 중재자 인스턴스(HA 쌍을 배포하려는 경우)

단계

1. AWS IAM 콘솔로 가서 *정책*을 클릭합니다.
2. 콘솔 에이전트 인스턴스에 대한 정책을 만듭니다.

AWS 환경에서 S3 버킷을 지원하기 위해 이러한 정책을 생성합니다. 나중에 버킷을 생성할 때 버킷 이름 앞에 접두사가 있는지 확인하십시오. `fabric-pool-` . 이 요구 사항은 AWS Secret Cloud 및 Top Secret Cloud 지역 모두에 적용됩니다.

비밀 지역

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

극비 지역

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
```

```
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
```

```
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
```

```
        ]
}
```

3. Cloud Volumes ONTAP 에 대한 정책을 만듭니다.

비밀 지역

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

극비 지역

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

HA 쌍의 경우 Cloud Volumes ONTAP HA 쌍을 배포할 계획이라면 HA 중재자에 대한 정책을 만듭니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. 역할 유형이 Amazon EC2인 IAM 역할을 만들고 이전 단계에서 만든 정책을 연결합니다.

   역할을 만듭니다.

   정책과 마찬가지로 콘솔 에이전트에 대한 IAM 역할 하나와 Cloud Volumes ONTAP 노드에 대한 IAM 역할 하나가 있어야 합니다. HA 쌍의 경우: 정책과 마찬가지로 콘솔 에이전트에 대한 IAM 역할 하나, Cloud Volumes ONTAP 노드에 대한 IAM 역할 하나, HA 중재자(HA 쌍을 배포하려는 경우)에 대한 IAM 역할 하나가 있어야 합니다.

   역할을 선택하세요:

   콘솔 에이전트 인스턴스를 시작할 때 콘솔 에이전트 IAM 역할을 선택해야 합니다. 콘솔에서 Cloud Volumes ONTAP 시스템을 생성할 때 Cloud Volumes ONTAP 에 대한 IAM 역할을 선택할 수 있습니다. HA 쌍의 경우 Cloud Volumes ONTAP 시스템을 생성할 때 Cloud Volumes ONTAP 및 HA 중재자에 대한 IAM 역할을 선택할 수 있습니다.

3단계: AWS KMS 설정

Cloud Volumes ONTAP 과 함께 Amazon 암호화를 사용하려면 AWS Key Management Service(KMS)에 대한 요구 사항이 충족되는지 확인하세요.

단계

1. 귀하의 계정이나 다른 AWS 계정에 활성 고객 마스터 키(CMK)가 있는지 확인하세요.

   CMK는 AWS 관리형 CMK이거나 고객 관리형 CMK일 수 있습니다.

2. CMK가 Cloud Volumes ONTAP 배포하려는 계정과 별도의 AWS 계정에 있는 경우 해당 키의 ARN을 얻어야 합니다.

   Cloud Volumes ONTAP 시스템을 생성할 때 콘솔에 ARN을 제공해야 합니다.

3. CMK의 주요 사용자 목록에 인스턴스의 IAM 역할을 추가합니다.

   이렇게 하면 콘솔에서 Cloud Volumes ONTAP 과 함께 CMK를 사용할 수 있는 권한이 부여됩니다.

4단계**:** 콘솔 에이전트 설치 및 콘솔 설정

AWS에서 Cloud Volumes ONTAP 배포하기 위해 콘솔을 사용하려면 먼저 콘솔 에이전트를 설치하고 설정해야 합니다. 콘솔을 통해 퍼블릭 클라우드 환경(여기에는 Cloud Volumes ONTAP 포함됨) 내의 리소스와 프로세스를 관리할 수 있습니다.

단계

1. 인증 기관(CA)에서 서명한 루트 인증서를 PEM(Privacy Enhanced Mail) Base-64 인코딩된 X.509 형식으로 얻습니다. 인증서를 취득하기 위해서는 귀하의 조직의 정책과 절차를 참조하세요.

   AWS Secret Cloud 지역의 경우 다음을 업로드해야 합니다. `NSS Root CA 2` 인증서 및 Top Secret Cloud의 경우 `Amazon Root CA 4` 자격증. 전체 체인이 아닌 해당 인증서만 업로드해야 합니다. 인증서 체인 파일이 커서 업로드가 실패할 수 있습니다. 추가 인증서가 있는 경우 다음 단계에 설명된 대로 나중에 업로드할 수 있습니다.

   설정 과정에서 인증서를 업로드해야 합니다. 콘솔은 HTTPS를 통해 AWS에 요청을 보낼 때 신뢰할 수 있는 인증서를 사용합니다.

2. 콘솔 에이전트 인스턴스를 시작합니다.
   a. 콘솔의 AWS Intelligence Community Marketplace 페이지로 이동합니다.
   b. 사용자 지정 시작 탭에서 EC2 콘솔에서 인스턴스를 시작하는 옵션을 선택합니다.
   c. 프롬프트에 따라 인스턴스를 구성합니다.

      인스턴스를 구성할 때 다음 사항에 유의하세요.

      - t3.xlarge을 권장합니다.
      - 권한을 설정할 때 생성한 IAM 역할을 선택해야 합니다.
      - 기본 저장 옵션을 유지해야 합니다.
      - 콘솔 에이전트에 필요한 연결 방법은 다음과 같습니다: SSH, HTTP, HTTPS.
3. 인스턴스에 연결된 호스트에서 콘솔을 설정합니다.
   a. 웹 브라우저를 열고 입력하세요 https://ipaddress 여기서 _ipaddress_는 콘솔 에이전트를 설치한 Linux 호스트의 IP 주소입니다.
   b. AWS 서비스에 연결하기 위한 프록시 서버를 지정합니다.
   c. 1단계에서 얻은 인증서를 업로드하세요.
   d. 화면의 지시에 따라 새로운 시스템을 설정하세요.
      - 시스템 세부 정보: 콘솔 에이전트의 이름과 회사 이름을 입력하세요.
      - 관리자 사용자 만들기: 시스템의 관리자 사용자를 만듭니다.

        이 사용자 계정은 시스템에서 로컬로 실행됩니다. 콘솔을 통해 auth0 서비스에 연결할 수 없습니다.

- 검토: 세부 정보를 검토하고, 라이선스 계약에 동의한 후 *설정*을 선택합니다.

e. CA 서명 인증서 설치를 완료하려면 EC2 콘솔에서 콘솔 에이전트 인스턴스를 다시 시작합니다.

4. 콘솔 에이전트가 다시 시작된 후 설치 마법사에서 만든 관리자 사용자 계정을 사용하여 로그인합니다.

5단계**: (**선택 사항**)** 개인 모드 인증서 설치

이 단계는 AWS Secret Cloud 및 Top Secret Cloud 지역의 경우 선택 사항이며, 이전 단계에서 설치한 루트 인증서 외에 추가 인증서가 있는 경우에만 필요합니다.

단계

1. 기존에 설치된 인증서를 나열합니다.

a. occm 컨테이너 docker ID(식별된 이름 "ds-occm-1")를 수집하려면 다음 명령을 실행하세요.

```
docker ps
```

b. occm 컨테이너 안으로 들어가려면 다음 명령을 실행하세요.

```
docker exec -it <docker-id> /bin/sh
```

c. "TRUST_STORE_PASSWORD" 환경 변수에서 비밀번호를 수집하려면 다음 명령을 실행하세요.

```
env
```

d. 신뢰 저장소에 설치된 모든 인증서를 나열하려면 다음 명령을 실행하고 이전 단계에서 수집한 비밀번호를 사용하세요.

```
keytool -list -v -keystore occm.truststore
```

2. 인증서를 추가합니다.

a. occm 컨테이너 docker ID(식별된 이름 "ds-occm-1")를 수집하려면 다음 명령을 실행하세요.

```
docker ps
```

b. occm 컨테이너 안으로 들어가려면 다음 명령을 실행하세요.

```
docker exec -it <docker-id> /bin/sh
```

새로운 인증서 파일을 내부에 저장합니다.

c. "TRUST_STORE_PASSWORD" 환경 변수에서 비밀번호를 수집하려면 다음 명령을 실행하세요.

```
env
```

d. 인증서를 신뢰 저장소에 추가하려면 다음 명령을 실행하고 이전 단계의 비밀번호를 사용하세요.

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. 인증서가 설치되었는지 확인하려면 다음 명령을 실행하세요.

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. occm 컨테이너를 종료하려면 다음 명령을 실행하세요.

```
exit
```

g. occm 컨테이너를 재설정하려면 다음 명령을 실행하세요.

```
docker restart <docker-id>
```

6단계**:** 콘솔에 라이선스 추가

NetApp 에서 라이선스를 구매한 경우 콘솔에 라이선스를 추가해야 새 Cloud Volumes ONTAP 시스템을 생성할 때 라이선스를 선택할 수 있습니다. 이러한 라이선스는 새 Cloud Volumes ONTAP 시스템과 연결할 때까지 할당되지 않은 상태로 유지됩니다.

단계

1. 왼쪽 탐색 메뉴에서 * Licenses and subscriptions*을 선택하세요.
2. * Cloud Volumes ONTAP* 패널에서 *보기*를 선택합니다.
3. * Cloud Volumes ONTAP* 탭에서 *라이선스 > 노드 기반 라이선스*를 선택합니다.
4. *할당되지 않음*을 클릭합니다.
5. *할당되지 않은 라이선스 추가*를 클릭합니다.
6. 라이선스의 일련번호를 입력하거나 라이선스 파일을 업로드하세요.
7. 아직 라이선스 파일이 없으면 netapp.com에서 라이선스 파일을 수동으로 업로드해야 합니다.
   a. 로 가다"NetApp 라이선스 파일 생성기" NetApp 지원 사이트 자격 증명을 사용하여 로그인하세요.
   b. 비밀번호를 입력하고, 제품을 선택하고, 일련번호를 입력하고, 개인정보 보호정책을 읽고 동의함을 확인한 후 *제출*을 클릭하세요.
   c. serialnumber.NLF JSON 파일을 이메일로 받을지, 아니면 직접 다운로드할지 선택하세요.
8. *라이선스 추가*를 클릭하세요.

결과

콘솔은 새 Cloud Volumes ONTAP 시스템과 연결할 때까지 라이선스를 미할당으로 추가합니다. 라이선스는 왼쪽 탐색 메뉴의 * Licenses and subscriptions > Cloud Volumes ONTAP > 보기 > 라이선스*에서 확인할 수 있습니다.

7단계: 콘솔에서 **Cloud Volumes ONTAP** 실행

콘솔에서 새로운 시스템을 생성하여 AWS Secret Cloud 및 Top Secret Cloud에서 Cloud Volumes ONTAP 인스턴스를 시작할 수 있습니다.

시작하기 전에

HA 쌍의 경우 HA 중재자에 대한 키 기반 SSH 인증을 활성화하려면 키 쌍이 필요합니다.

단계

1. 시스템 페이지에서 *시스템 추가*를 클릭합니다.
2. *만들기*에서 Cloud Volumes ONTAP 선택합니다.

   HA의 경우: *만들기*에서 Cloud Volumes ONTAP 또는 Cloud Volumes ONTAP HA를 선택합니다.

3. 마법사의 단계를 완료하여 Cloud Volumes ONTAP 시스템을 시작합니다.

> 마법사를 통해 선택하는 동안 *서비스*에서 *데이터 감지 및 규정 준수*와 *클라우드에 백업*을 선택하지 마세요. *사전 구성된 패키지*에서 *구성 변경*만 선택하고 다른 옵션은 선택하지 않았는지 확인하세요. 사전 구성된 패키지는 AWS Secret Cloud 및 Top Secret Cloud 지역에서는 지원되지 않으며, 이를 선택하면 배포가 실패합니다.

여러 가용성 영역에 **Cloud Volumes ONTAP HA**를 배포하기 위한 참고 사항

HA 쌍에 대한 마법사를 완료할 때 다음 사항에 유의하세요.

- 여러 가용성 영역(AZ)에 Cloud Volumes ONTAP HA를 배포하는 경우 전송 게이트웨이를 구성해야 합니다. 지침은 다음을 참조하세요."AWS 전송 게이트웨이 설정" .
- AWS Top Secret Cloud가 게시될 당시에는 사용 가능한 AZ가 두 개뿐이었으므로 다음과 같이 구성을 배포합니다.
  - 노드 1: 가용성 영역 A
  - 노드 2: 가용성 영역 B
  - 중재자: 가용성 영역 A 또는 B

단일 및 **HA** 노드 모두에 **Cloud Volumes ONTAP** 배포하기 위한 참고 사항

마법사를 완료할 때 다음 사항에 유의하세요.

- 생성된 보안 그룹을 사용하려면 기본 옵션을 그대로 두어야 합니다.

  미리 정의된 보안 그룹에는 Cloud Volumes ONTAP 성공적으로 작동하는 데 필요한 규칙이 포함되어 있습니다. 자체 보안 그룹이 필요한 경우 아래 보안 그룹 섹션을 참조하세요.

- AWS 환경을 준비할 때 생성한 IAM 역할을 선택해야 합니다.
- 기본 AWS 디스크 유형은 초기 Cloud Volumes ONTAP 볼륨을 위한 것입니다.

  이후 볼륨에는 다른 디스크 유형을 선택할 수 있습니다.

- AWS 디스크의 성능은 디스크 크기에 따라 달라집니다.

  지속적으로 필요한 성능을 제공하는 디스크 크기를 선택해야 합니다. EBS 성능에 대한 자세한 내용은 AWS 설명서를 참조하세요.

- 디스크 크기는 시스템의 모든 디스크에 대한 기본 크기입니다.

  나중에 다른 크기가 필요한 경우 고급 할당 옵션을 사용하여 특정 크기의 디스크를 사용하는 집계를 만들 수 있습니다.

결과

Cloud Volumes ONTAP 인스턴스가 시작됩니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

8단계**:** 데이터 계층화를 위한 보안 인증서 설치

AWS Secret Cloud 및 Top Secret Cloud 지역에서 데이터 계층화를 활성화하려면 보안 인증서를 수동으로 설치해야 합니다.

시작하기 전에

1. S3 버킷을 생성합니다.

   버킷 이름 앞에 접두사가 있는지 확인하십시오. `fabric-pool-`. 예를 들어 `fabric-pool-testbucket` .

2. 설치한 루트 인증서를 유지하세요. `step 4` 능숙한.

단계

1. 설치한 루트 인증서에서 텍스트를 복사하세요. `step 4` .
2. CLI를 사용하여 Cloud Volumes ONTAP 시스템에 안전하게 연결합니다.
3. 루트 인증서를 설치합니다. 당신은 눌러야 할 수도 있습니다 `ENTER` 키를 여러 번 누르세요:

   ```
   security certificate install -type server-ca -cert-name <certificate-name>
   ```

4. 메시지가 표시되면 다음을 포함하여 복사된 전체 텍스트를 입력하십시오. `----- BEGIN CERTIFICATE -----` 에게 `----- END CERTIFICATE -----` .
5. 나중에 참조할 수 있도록 CA 서명 디지털 인증서 사본을 보관하세요.
6. CA 이름과 인증서 일련번호를 보관하세요.
7. AWS Secret Cloud 및 Top Secret Cloud 지역에 대한 개체 저장소를 구성합니다. `set -privilege advanced -confirmations off`
8. 이 명령을 실행하여 개체 저장소를 구성합니다.

모든 Amazon 리소스 이름(ARN)에는 다음 접미사가 붙어야 합니다. `-iso-b` , 와 같은 `arn:aws-iso-b` . 예를 들어 리소스에 지역이 포함된 ARN이 필요한 경우 Top Secret Cloud의 경우 다음과 같은 명명 규칙을 사용합니다. `us-iso-b` 를 위해 `-server` 깃발. AWS Secret Cloud의 경우 다음을 사용하세요. `us-iso-b-1` .

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. 개체 저장소가 성공적으로 생성되었는지 확인하세요. `storage aggregate object-store show -instance`
10. 개체 저장소를 집계에 연결합니다. 이것은 모든 새로운 집계에 대해 반복되어야 합니다. `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

Microsoft Azure에서 시작하기

Azure에서 Cloud Volumes ONTAP 배포 옵션에 대해 알아보세요.

NetApp Azure에 Cloud Volumes ONTAP 배포하기 위한 두 가지 옵션을 제공합니다. Cloud Volumes ONTAP 전통적으로 배포 및 오케스트레이션을 위해 NetApp Console 사용합니다. Cloud Volumes ONTAP 9.16.1부터 Azure 마켓플레이스 직접 배포를 활용할 수 있습니다. 이는 제한적이지만 여전히 강력한 Cloud Volumes ONTAP 기능과 옵션에 대한 액세스를 제공하는 간소화된 프로세스입니다.

Azure Marketplace에서 직접 Cloud Volumes ONTAP 배포하는 경우 콘솔 에이전트를 설정하거나 콘솔을 통해 Cloud Volumes ONTAP 배포하는 데 필요한 다른 보안 및 온보딩 기준을 충족할 필요가 없습니다. Azure 마켓플레이스에서 몇 번의 클릭만으로 Cloud Volumes ONTAP 빠르게 배포하고 사용자 환경에서 핵심 기능과 성능을 살펴볼 수 있습니다.

Azure Marketplace에서 배포를 완료하면 콘솔에서 이러한 시스템을 검색할 수 있습니다. 발견 후에는 이를 Cloud Volumes ONTAP 시스템으로 관리하고 모든 콘솔 기능을 활용할 수 있습니다. "콘솔에서 배포된 시스템을 검색하세요" .

두 옵션의 기능을 비교한 내용은 다음과 같습니다. Azure 마켓플레이스를 통해 배포된 독립 실행형 인스턴스의 기능은 콘솔에서 검색될 때 변경됩니다.

	Azure 마켓플레이스	**NetApp Console**
온보딩	직접 배치에 필요한 준비가 최소화되어 더 짧고 쉽습니다.	콘솔 에이전트 설치를 포함한 더 긴 온보딩 프로세스
지원되는 가상 머신**(VM)** 유형	Eds_v5 및 Ls_v3 인스턴스 유형	다양한 VM 유형.https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Azure에서 지원되는 구성"^]

	Azure 마켓플레이스	NetApp Console
특허	무료 라이센스	모든 용량 기반 라이센스."Cloud Volumes ONTAP 라이선싱"
* NetApp 지원*	포함되지 않음	라이센스 유형에 따라 사용 가능
용량	최대 500GiB	구성에 따라 확장 가능
배포 모델	단일 가용성 영역(AZ)에 고가용성(HA) 모드 배포	단일 노드 및 HA 모드, 단일 및 다중 AZ 배포를 포함한 모든 지원 구성
지원되는 디스크 유형	프리미엄 SSD v2 관리 디스크	더 폭넓은 지원."Cloud Volumes ONTAP 의 기본 구성"
쓰기 속도(빠른 쓰기 모드)	지원되지 않음	구성에 따라 지원됩니다. "Cloud Volumes ONTAP 의 쓰기 속도에 대해 알아보세요" .
오케스트레이션 기능	사용할 수 없음	라이센스 유형에 따라 NetApp Console 통해 사용 가능
지원되는 스토리지 VM 수	배포당 하나	구성에 따라 여러 개의 스토리지 VM이 제공됩니다."지원되는 스토리지 VM 수"
인스턴스 유형 변경	지원되지 않음	지원됨
* FabricPool 계층화*	지원되지 않음	지원됨

관련 링크

- Azure 마켓플레이스 직접 배포:"Azure Marketplace에서 Cloud Volumes ONTAP 배포"
- 콘솔을 통한 배포:"Azure에서 Cloud Volumes ONTAP 대한 빠른 시작"
- "NetApp Console 설명서"

NetApp Console 에서 시작하기

Azure에서 **Cloud Volumes ONTAP** 대한 빠른 시작

몇 단계만 거치면 Azure용 Cloud Volumes ONTAP 시작할 수 있습니다.

콘솔 에이전트 만들기

만약 당신이 없다면 "콘솔 에이전트" 하지만, 하나는 만들어야 합니다. "Azure에서 콘솔 에이전트를 만드는 방법을 알아보세요."

인터넷 접속이 불가능한 서브넷에 Cloud Volumes ONTAP 배포하려면 콘솔 에이전트를 수동으로 설치하고 해당 콘솔 에이전트에서 실행 중인 NetApp Console 에 액세스해야 합니다. "인터넷 접속이 불가능한 위치에 콘솔 에이전트를 수동으로 설치하는 방법을 알아보세요."

구성을 계획하세요

콘솔은 사용자의 작업 부하 요구 사항에 맞는 미리 구성된 패키지를 제공하거나 사용자가 직접 구성을 만들 수도

있습니다. 원하는 구성을 선택하는 경우, 사용 가능한 옵션을 이해해야 합니다. 자세한 내용은 다음을 참조하세요. "Azure에서 Cloud Volumes ONTAP 구성 계획" .

3 네트워킹을 설정하세요

1. VNet과 서브넷이 콘솔 에이전트와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인하세요.
2. NetApp AutoSupport 에 대해 대상 VPC에서 아웃바운드 인터넷 액세스를 활성화합니다.

   인터넷 접속이 불가능한 위치에 Cloud Volumes ONTAP 배포하는 경우 이 단계는 필요하지 않습니다.

"네트워킹 요구 사항에 대해 자세히 알아보세요" .

4 **Cloud Volumes ONTAP** 출시

*시스템 추가*를 클릭하고 배포하려는 시스템 유형을 선택한 다음 마법사의 단계를 완료합니다. "단계별 지침을 읽어보세요" .

관련 링크

- "콘솔에서 콘솔 에이전트 만들기"
- "Azure Marketplace에서 콘솔 에이전트 만들기"
- "Linux 호스트에 콘솔 에이전트 소프트웨어 설치"
- "콘솔이 권한으로 수행하는 작업"

Azure에서 **Cloud Volumes ONTAP** 구성 계획

Azure에 Cloud Volumes ONTAP 배포할 때 워크로드 요구 사항에 맞는 미리 구성된 시스템을 선택하거나 고유한 구성을 만들 수 있습니다. 원하는 구성을 선택하는 경우, 사용 가능한 옵션을 이해해야 합니다.

Cloud Volumes ONTAP 라이선스를 선택하세요

Cloud Volumes ONTAP 에는 여러 가지 라이선싱 옵션이 제공됩니다. 각 옵션을 통해 귀하의 필요에 맞는 소비 모델을 선택할 수 있습니다.

- "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요"
- "라이선싱 설정 방법 알아보기"

지원되는 지역을 선택하세요

Cloud Volumes ONTAP 대부분의 Microsoft Azure 지역에서 지원됩니다. "지원되는 지역의 전체 목록 보기" .

지원되는 **VM** 유형을 선택하세요

Cloud Volumes ONTAP 선택한 라이선스 유형에 따라 여러 VM 유형을 지원합니다.

"Azure의 Cloud Volumes ONTAP 에 지원되는 구성"

Cloud Volumes ONTAP 시스템의 원시 용량 제한은 라이선스에 따라 결정됩니다. 추가적인 제한은 골재와 부피의 크기에 영향을 미칩니다. 구성을 계획할 때 이러한 제한 사항을 알고 있어야 합니다.

"Azure의 Cloud Volumes ONTAP 에 대한 저장소 한도"

Azure에서 시스템 크기 조정

Cloud Volumes ONTAP 시스템의 크기를 조정하면 성능 및 용량 요구 사항을 충족하는 데 도움이 될 수 있습니다. VM 유형, 디스크 유형 및 디스크 크기를 선택할 때 몇 가지 핵심 사항을 알아야 합니다.

가상 머신 유형

지원되는 가상 머신 유형을 살펴보세요. "Cloud Volumes ONTAP 릴리스 노트" 그런 다음 지원되는 각 VM 유형에 대한 세부 정보를 검토합니다. 각 VM 유형은 특정 수의 데이터 디스크를 지원한다는 점을 알아두세요.

- "Azure 설명서: 범용 가상 머신 크기"
- "Azure 설명서: 메모리 최적화된 가상 머신 크기"

단일 노드 시스템의 **Azure** 디스크 유형

Cloud Volumes ONTAP 에 대한 볼륨을 생성할 때 Cloud Volumes ONTAP 디스크로 사용하는 기본 클라우드 스토리지를 선택해야 합니다.

단일 노드 시스템에서는 다음과 같은 유형의 Azure 관리 디스크를 사용할 수 있습니다.

- _프리미엄 SSD 관리 디스크_는 비용이 더 많이 들더라도 I/O 집약적 워크로드에 대해 높은 성능을 제공합니다.
- _프리미엄 SSD v2 관리형 디스크_는 프리미엄 SSD 관리형 디스크에 비해 더 낮은 비용으로 더 높은 성능과 더 낮은 지연 시간을 제공합니다.
- _표준 SSD 관리 디스크_는 낮은 IOPS가 필요한 작업 부하에 대해 일관된 성능을 제공합니다.
- _표준 HDD 관리 디스크_는 높은 IOPS가 필요하지 않고 비용을 절감하고 싶은 경우에 좋은 선택입니다.

이러한 디스크의 사용 사례에 대한 추가 세부 정보는 다음을 참조하세요. "Microsoft Azure 설명서: Azure에서 사용할 수 있는 디스크 유형은 무엇인가요?" .

HA 쌍이 있는 **Azure** 디스크 유형

HA 시스템은 비용이 더 많이 들더라도 I/O 집약적 워크로드에 대해 높은 성능을 제공하는 프리미엄 SSD 공유 관리 디스크를 사용합니다. 9.12.1 릴리스 이전에 생성된 HA 배포는 프리미엄 페이지 Blob을 사용합니다.

Azure 디스크 크기

Cloud Volumes ONTAP 인스턴스를 시작할 때 집계에 대한 기본 디스크 크기를 선택해야 합니다. NetApp Console 초기 집계에 이 디스크 크기를 사용하고, 간단한 프로비저닝 옵션을 사용할 때 생성하는 추가 집계에도 이 디스크 크기를 사용합니다. 기본값과 다른 디스크 크기를 사용하는 집계를 생성할 수 있습니다."고급 할당 옵션 사용" .

집계된 모든 디스크의 크기는 동일해야 합니다.

디스크 크기를 선택할 때는 여러 가지 요소를 고려해야 합니다. 디스크 크기는 스토리지 비용, 집계하여 생성할 수 있는 볼륨 크기, Cloud Volumes ONTAP 에서 사용할 수 있는 총 용량, 스토리지 성능에 영향을 미칩니다.

Azure Premium Storage의 성능은 디스크 크기에 따라 달라집니다. 더 큰 디스크는 더 높은 IOPS와 처리량을

제공합니다. 예를 들어, 1TiB 디스크를 선택하면 500GiB 디스크보다 비용이 더 많이 들더라도 더 나은 성능을 제공할 수 있습니다.

표준 저장소의 디스크 크기에는 성능 차이가 없습니다. 필요한 용량에 따라 디스크 크기를 선택해야 합니다.

디스크 크기별 IOPS 및 처리량은 Azure를 참조하세요.

- "Microsoft Azure: 관리 디스크 가격"
- "Microsoft Azure: 페이지 Blob 가격 책정"

기본 시스템 디스크 보기

사용자 데이터 저장 외에도 콘솔은 Cloud Volumes ONTAP 시스템 데이터(부팅 데이터, 루트 데이터, 코어 데이터 및 NVRAM)를 위한 클라우드 스토리지도 구매합니다. 계획을 세우려면 Cloud Volumes ONTAP 배포하기 전에 이러한 세부 정보를 검토하는 것이 도움이 될 수 있습니다.

"Azure에서 Cloud Volumes ONTAP 시스템 데이터의 기본 디스크 보기" .

콘솔 에이전트에도 시스템 디스크가 필요합니다. "콘솔 에이전트의 기본 구성에 대한 세부 정보 보기" .

네트워킹 정보 수집

Azure에 Cloud Volumes ONTAP 배포하는 경우 가상 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

Azure 정보	당신의 가치
지역	
가상 네트워크(VNet)	
서브넷	
네트워크 보안 그룹(자체 그룹 사용 시)	

쓰기 속도를 선택하세요

콘솔을 사용하면 Cloud Volumes ONTAP 에 대한 쓰기 속도 설정을 선택할 수 있습니다. 쓰기 속도를 선택하기 전에 일반 설정과 높은 설정의 차이점, 높은 쓰기 속도를 사용할 때의 위험과 권장 사항을 이해해야 합니다. "쓰기 속도에 대해 자세히 알아보세요" .

볼륨 사용 프로필을 선택하세요

ONTAP 에는 필요한 총 저장 용량을 줄일 수 있는 여러 가지 저장 효율성 기능이 포함되어 있습니다. 콘솔에서 볼륨을 생성할 때 이러한 기능을 활성화하는 프로필이나 비활성화하는 프로필을 선택할 수 있습니다. 어떤 프로필을 사용할지 결정하는 데 도움이 되도록 이러한 기능에 대해 자세히 알아보세요.

NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

씬 프로비저닝

실제 물리적 스토리지 풀에 있는 것보다 더 많은 논리적 스토리지를 호스트나 사용자에게 제공합니다. 저장 공간을 미리 할당하는 대신, 데이터가 기록됨에 따라 각 볼륨에 저장 공간이 동적으로 할당됩니다.

중복제거

동일한 데이터 블록을 찾아 단일 공유 블록에 대한 참조로 대체하여 효율성을 향상시킵니다. 이 기술은 동일한 볼륨에 있는 중복된 데이터 블록을 제거하여 저장 용량 요구 사항을 줄입니다.

압축

1차, 2차, 보관 저장소의 볼륨 내 데이터를 압축하여 데이터를 저장하는 데 필요한 물리적 용량을 줄입니다.

Cloud Volumes ONTAP 에 대한 **Azure** 네트워킹 설정

NetApp Console IP 주소, 넷마스크, 경로 등 Cloud Volumes ONTAP 의 네트워킹 구성 요소를 설정합니다. 아웃바운드 인터넷 접속이 가능한지, 충분한 개인 IP 주소가 사용 가능한지, 올바른 연결이 설정되어 있는지 등을 확인해야 합니다.

Cloud Volumes ONTAP 요구 사항

Azure에서는 다음과 같은 네트워킹 요구 사항을 충족해야 합니다.

아웃바운드 인터넷 접속

Cloud Volumes ONTAP 시스템은 다양한 기능을 위해 외부 엔드포인트에 액세스하기 위해 아웃바운드 인터넷 액세스가 필요합니다. 엄격한 보안 요구 사항이 있는 환경에서 이러한 엔드포인트가 차단되면 Cloud Volumes ONTAP 제대로 작동할 수 없습니다.

콘솔 에이전트는 일상 업무를 위해 여러 엔드포인트에 연결합니다. 엔드포인트에 대한 정보는 다음을 참조하세요. "콘솔 에이전트에서 연결된 엔드포인트 보기" 그리고 "콘솔 사용을 위한 네트워킹 준비" .

Cloud Volumes ONTAP 엔드포인트

Cloud Volumes ONTAP 이러한 엔드포인트를 사용하여 다양한 서비스와 통신합니다.

엔드포인트	적용 가능	목적	배포 모드	사용할 수 없는 경우 영향
\ https://netapp-cloud-account.auth0.com	입증	콘솔에서 인증에 사용됩니다.	표준 모드와 제한 모드.	사용자 인증에 실패하고 다음 서비스를 계속 사용할 수 없습니다. • Cloud Volumes ONTAP 서비스 • ONTAP 서비스 • 프로토콜 및 프록시 서비스
https://vault.azure.net	키 볼트	고객 관리 키(CMK)를 사용할 때 Azure Key Vault에서 클라이언트 비밀 키를 검색하는 데 사용됩니다.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP 서비스를 사용할 수 없습니다.

엔드포인트	적용 가능	목적	배포 모드	사용할 수 없는 경우 영향
\ https://api.bluexp.netapp.com/tenancy	차용	콘솔에서 Cloud Volumes ONTAP 리소스를 검색하여 리소스와 사용자에게 권한을 부여하는 데 사용됩니다.	표준 모드와 제한 모드.	Cloud Volumes ONTAP 리소스와 사용자는 권한이 없습니다.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	AutoSupport 원격 측정 데이터를 NetApp 지원팀으로 전송하는 데 사용됩니다.	표준 모드와 제한 모드.	AutoSupport 정보가 전달되지 않았습니다.
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://core.windows.net	공공 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	중국 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	독일 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.

엔드포인트	적용 가능	목적	배포 모드	사용할 수 없는 경우 영향
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	정부 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.
\ https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	정부 DoD 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.

NetApp Console 에이전트의 네트워크 프록시 구성

NetApp Console 에이전트의 프록시 서버 구성을 사용하여 Cloud Volumes ONTAP 에서 아웃바운드 인터넷 액세스를 활성화할 수 있습니다. 콘솔은 두 가지 유형의 프록시를 지원합니다.

- 명시적 프록시: Cloud Volumes ONTAP 의 아웃바운드 트래픽은 콘솔 에이전트의 프록시 구성 중에 지정된 프록시 서버의 HTTP 주소를 사용합니다. 관리자는 추가 인증을 위해 사용자 자격 증명과 루트 CA 인증서를 구성했을 수도 있습니다. 명시적 프록시에 대해 루트 CA 인증서를 사용할 수 있는 경우 다음을 사용하여 동일한 인증서를 Cloud Volumes ONTAP 시스템에 가져와 업로드해야 합니다. "ONTAP CLI: 보안 인증서 설치" 명령.
- 투명 프록시: 네트워크는 콘솔 에이전트의 프록시를 통해 Cloud Volumes ONTAP 에서 아웃바운드 트래픽을 자동으로 라우팅하도록 구성됩니다. 투명 프록시를 설정할 때 관리자는 프록시 서버의 HTTP 주소가 아닌 Cloud Volumes ONTAP 에서의 연결을 위한 루트 CA 인증서만 제공하면 됩니다. 다음을 사용하여 Cloud Volumes ONTAP 시스템에 동일한 루트 CA 인증서를 가져와 업로드해야 합니다. "ONTAP CLI: 보안 인증서 설치" 명령.

프록시 서버 구성에 대한 정보는 다음을 참조하세요. "프록시 서버를 사용하도록 콘솔 에이전트 구성" .

IP 주소

콘솔은 Azure의 Cloud Volumes ONTAP 에 필요한 수의 개인 IP 주소를 자동으로 할당합니다. 네트워크에 사용 가능한 개인 IP 주소가 충분한지 확인해야 합니다.

Cloud Volumes ONTAP에 할당된 LIF 수는 단일 노드 시스템을 배포하는지 또는 HA 쌍을 배포하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다. SVM 관리 LIF는 SnapCenter와 같은 관리 툴에 필요합니다.

iSCSI LIF는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공하며 시스템에서 다른 중요한 네트워킹 워크플로에 사용됩니다. 이러한 LIF는 필수이므로 삭제하면 안 됩니다.

단일 노드 시스템의 **IP** 주소

NetApp Console은 단일 노드 시스템에 5개 또는 6개의 IP 주소를 할당합니다.

- 클러스터 관리 IP
- 노드 관리 IP
- SnapMirror 용 클러스터 간 IP
- NFS/CIFS IP
- iSCSI IP

> iSCSI IP는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공합니다. 또한 시스템에서 다른 중요한 네트워킹 워크플로에도 사용됩니다. 이 LIF는 필수이므로 삭제하면 안 됩니다.

- SVM 관리(선택 사항 - 기본적으로 구성되지 않음)

HA 쌍의 **IP** 주소

콘솔은 배포 중에 노드당 4개의 NIC에 IP 주소를 할당합니다.

참고로 Console은 HA 쌍에 대해서는 SVM 관리 LIF를 생성하지만, Azure의 단일 노드 시스템에 대해서는 생성하지 않습니다.

NIC0

- 노드 관리 IP
- 클러스터 간 IP
- iSCSI IP

> iSCSI IP는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공합니다. 또한 시스템에서 다른 중요한 네트워킹 워크플로에도 사용됩니다. 이 LIF는 필수이므로 삭제하면 안 됩니다.

NIC1

- 클러스터 네트워크 IP

NIC2

- 클러스터 상호 연결 IP(HA IC)

NIC3

- Pageblob NIC IP(디스크 액세스)

> NIC3는 페이지 Blob 스토리지를 사용하는 HA 배포에만 적용할 수 있습니다.

위의 IP 주소는 장애 조치 이벤트 시 마이그레이션되지 않습니다.

또한 4개의 프런트엔드 IP(FIP)가 장애 조치 이벤트 시 마이그레이션되도록 구성됩니다. 이러한 프런트엔드 IP는 로드

밸런서에 있습니다.

- 클러스터 관리 IP
- NodeA 데이터 IP(NFS/CIFS)
- NodeB 데이터 IP(NFS/CIFS)
- SVM 관리 IP

Azure 서비스에 대한 보안 연결

기본적으로 콘솔은 Cloud Volumes ONTAP 과 Azure 페이지 Blob 스토리지 계정 간의 연결을 위해 Azure Private Link를 활성화합니다.

대부분의 경우 사용자가 해야 할 일은 없습니다. 콘솔이 사용자를 대신하여 Azure Private Link를 관리해 줍니다. 하지만 Azure Private DNS를 사용하는 경우 구성 파일을 편집해야 합니다. Azure에서 콘솔 에이전트의 위치에 대한 요구 사항도 알고 있어야 합니다.

비즈니스 요구 사항에 따라 Private Link 연결을 비활성화할 수도 있습니다. 링크를 비활성화하면 콘솔은 Cloud Volumes ONTAP 대신 서비스 엔드포인트를 사용하도록 구성합니다.

"Cloud Volumes ONTAP 에서 Azure Private Links 또는 서비스 엔드포인트를 사용하는 방법에 대해 자세히 알아보세요." .

Azure VNet 암호화를 위한 네트워킹

Cloud Volumes ONTAP는 VNet 내부 또는 피어링된 VNet 간의 VM 간 트래픽 "Azure Virtual Network(VNet) 암호화"을 지원합니다. 이 기능은 Azure VNet 계층에서 구성되며 Cloud Volumes ONTAP 토폴로지(단일 노드 또는 HA)와는 무관합니다.

VM의 NIC에서 가속 네트워킹이 활성화되어 있는지 확인하고 Azure VNet 암호화 요구 사항 및 제한 사항을 검토한 후 해당 기능을 활성화하면 됩니다. NetApp 관리형 로드 밸런서 개체는 수정해서는 안 됩니다.

"Azure 설명서: VNet 암호화 및 가속 네트워킹".

다른 **ONTAP** 시스템에 대한 연결

Azure의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 Azure VNet과 다른 네트워크(예: 회사 네트워크) 간에 VPN 연결이 필요합니다.

지침은 다음을 참조하세요. "Microsoft Azure 설명서: Azure Portal에서 사이트 간 연결 만들기" .

HA 상호 연결을 위한 포트

Cloud Volumes ONTAP HA 쌍에는 HA 상호 연결이 포함되어 있어 각 노드가 파트너가 제대로 작동하는지 지속적으로 확인하고 다른 노드의 비휘발성 메모리에 대한 로그 데이터를 미러링할 수 있습니다. HA 상호 연결은 통신을 위해 TCP 포트 10006을 사용합니다.

기본적으로 HA 상호 연결 LIF 간 통신은 열려 있으며 이 포트에 대한 보안 그룹 규칙은 없습니다. 하지만 HA 상호 연결 LIF 사이에 방화벽을 만드는 경우 HA 쌍이 제대로 작동할 수 있도록 포트 10006에 대한 TCP 트래픽이 열려 있는지 확인해야 합니다.

Azure 리소스 그룹에는 **HA** 쌍이 하나만 있습니다**.**

Azure에 배포하는 각 Cloud Volumes ONTAP HA 쌍에 대해 전용 리소스 그룹을 사용해야 합니다. 리소스 그룹에서는 HA 쌍을 하나만 지원합니다.

Azure 리소스 그룹에 두 번째 Cloud Volumes ONTAP HA 쌍을 배포하려고 하면 콘솔에서 연결 문제가 발생합니다.

보안 그룹 규칙

콘솔은 Cloud Volumes ONTAP 성공적으로 작동할 수 있도록 인바운드 및 아웃바운드 규칙을 포함하는 Azure 보안 그룹을 만듭니다. "콘솔 에이전트에 대한 보안 그룹 규칙 보기" .

Cloud Volumes ONTAP 용 Azure 보안 그룹에는 노드 간 내부 통신을 위해 적절한 포트가 열려 있어야 합니다. "ONTAP 내부 포트에 대해 알아보세요" .

미리 정의된 보안 그룹을 수정하거나 사용자 지정 보안 그룹을 사용하는 것은 권장하지 않습니다. 하지만 반드시 그렇게 해야 하는 경우 배포 프로세스에서 Cloud Volumes ONTAP 시스템이 자체 서브넷 내에서 전체 액세스 권한을 가져야 한다는 점에 유의하세요. 배포가 완료된 후 네트워크 보안 그룹을 수정하기로 결정한 경우 클러스터 포트와 HA 네트워크 포트를 열어 두세요. 이를 통해 Cloud Volumes ONTAP 클러스터 내에서 원활한 통신(노드 간 모든 통신)이 보장됩니다.

단일 노드 시스템에 대한 인바운드 규칙

Cloud Volumes ONTAP 시스템을 추가하고 미리 정의된 보안 그룹을 선택하면 다음 중 하나 내에서 트래픽을 허용하도록 선택할 수 있습니다.

- 선택된 **VNet**만 해당: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템의 VNet 서브넷 범위와 콘솔 에이전트가 있는 VNet의 서브넷 범위입니다. 이것은 권장되는 옵션입니다.
- 모든 **VNet**: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
- 비활성화: 이 옵션은 스토리지 계정에 대한 공용 네트워크 액세스를 제한하고 Cloud Volumes ONTAP 시스템의 데이터 계층화를 비활성화합니다. 보안 규정 및 정책으로 인해 동일한 VNet 내에서도 개인 IP 주소가 노출되어서는 안 되는 경우 이 옵션을 사용하는 것이 좋습니다.

우선순위와 이름	포트 및 프로토콜	출발지와 목적지	설명
1000 인바운드_ssh	22 TCP	어떤 것으로든	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 대한 SSH 액세스
1001 인바운드_http	80 TCP	어떤 것으로든	클러스터 관리 LIF의 IP 주소를 사용하여 ONTAP System Manager 웹 콘솔에 대한 HTTP 액세스
1002 inbound_111_tcp	111 TCP	어떤 것으로든	NFS에 대한 원격 프로시저 호출
1003 inbound_111_udp	111 UDP	어떤 것으로든	NFS에 대한 원격 프로시저 호출
1004 inbound_139	139 TCP	어떤 것으로든	CIFS용 NetBIOS 서비스 세션
1005 인바운드_161-162_tcp	161-162 TCP	어떤 것으로든	간단한 네트워크 관리 프로토콜

우선순위와 이름	포트 및 프로토콜	출발지와 목적지	설명
1006 인바운드_161-162_udp	161-162 UDP	어떤 것으로든	간단한 네트워크 관리 프로토콜
1007 inbound_443	443 TCP	어떤 것으로든	클러스터 관리 LIF의 IP 주소를 사용하여 콘솔 에이전트와 ONTAP System Manager 웹 콘솔에 대한 HTTPS 액세스 연결
1008 inbound_445	445 TCP	어떤 것으로든	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
1009 inbound_635_tcp	635 TCP	어떤 것으로든	NFS 마운트
1010 inbound_635_udp	635 UDP	어떤 것으로든	NFS 마운트
1011 inbound_749	749 TCP	어떤 것으로든	케르베로스
1012 inbound_2049_tcp	2049 TCP	어떤 것으로든	NFS 서버 데몬
1013 inbound_2049_udp	2049 UDP	어떤 것으로든	NFS 서버 데몬
1014 inbound_3260	3260 TCP	어떤 것으로든	iSCSI 데이터 LIF를 통한 iSCSI 액세스
1015 인바운드_4045-4046_tcp	4045-4046 TCP	어떤 것으로든	NFS 잠금 데몬 및 네트워크 상태 모니터
1016 인바운드_4045-4046_udp	4045-4046 UDP	어떤 것으로든	NFS 잠금 데몬 및 네트워크 상태 모니터
1017 inbound_10000	10000 TCP	어떤 것으로든	NDMP를 사용한 백업
1018 인바운드_11104-11105	11104-11105 TCP	어떤 것으로든	SnapMirror 데이터 전송
3000 인바운드_거부_모든_tcp	모든 포트 TCP	어떤 것으로든	다른 모든 TCP 인바운드 트래픽 차단
3001 인바운드_거부_모든_udp	모든 포트 UDP	어떤 것으로든	다른 모든 UDP 인바운드 트래픽 차단
65000 AllowVnetInBound	모든 포트 모든 프로토콜	VirtualNetwork에서 VirtualNetwork로	VNet 내부에서 들어오는 트래픽
65001 AllowAzureLoadBalancerInBound	모든 포트 모든 프로토콜	AzureLoadBalancer를 Any로	Azure Standard Load Balancer의 데이터 트래픽
65500 DenyAllInBound	모든 포트 모든 프로토콜	어떤 것으로든	다른 모든 인바운드 트래픽 차단

HA 시스템에 대한 인바운드 규칙

Cloud Volumes ONTAP 시스템을 추가하고 미리 정의된 보안 그룹을 선택하면 다음 중 하나 내에서 트래픽을 허용하도록 선택할 수 있습니다.

- 선택된 **VNet**만 해당: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템의 VNet 서브넷 범위와 콘솔

에이전트가 있는 VNet의 서브넷 범위입니다. 이것은 권장되는 옵션입니다.

- 모든 **VNet**: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.

> HA 시스템은 인바운드 데이터 트래픽이 Azure Standard Load Balancer를 통과하기 때문에 단일 노드 시스템보다 인바운드 규칙이 적습니다. 따라서 "AllowAzureLoadBalancerInBound" 규칙에 표시된 것처럼 Load Balancer에서 들어오는 트래픽은 허용되어야 합니다.

- 비활성화: 이 옵션은 스토리지 계정에 대한 공용 네트워크 액세스를 제한하고 Cloud Volumes ONTAP 시스템의 데이터 계층화를 비활성화합니다. 보안 규정 및 정책으로 인해 동일한 VNet 내에서도 개인 IP 주소가 노출되어서는 안 되는 경우 이 옵션을 사용하는 것이 좋습니다.

우선순위와 이름	포트 및 프로토콜	출발지와 목적지	설명
100 inbound_443	443 모든 프로토콜	어떤 것으로든	클러스터 관리 LIF의 IP 주소를 사용하여 콘솔 에이전트와 ONTAP System Manager 웹 콘솔에 대한 HTTPS 액세스 연결
101 inbound_111_tcp	111 모든 프로토콜	어떤 것으로든	NFS에 대한 원격 프로시저 호출
102 inbound_2049_tcp	2049 모든 프로토콜	어떤 것으로든	NFS 서버 데몬
111 인바운드_ssh	22 모든 프로토콜	어떤 것으로든	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 대한 SSH 액세스
121 inbound_53	53 모든 프로토콜	어떤 것으로든	DNS와 CIFS
65000 AllowVnetInBound	모든 포트 모든 프로토콜	VirtualNetwork에서 VirtualNetwork로	VNet 내부에서 들어오는 트래픽
65001 AllowAzureLoad BalancerInBound	모든 포트 모든 프로토콜	AzureLoadBalancer를 Any로	Azure Standard Load Balancer의 데이터 트래픽
65500 DenyAllInBound	모든 포트 모든 프로토콜	어떤 것으로든	다른 모든 인바운드 트래픽 차단

아웃바운드 규칙

Cloud Volumes ONTAP 의 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 개방합니다. 이것이 허용된다면, 기본적인 아웃바운드 규칙을 따르세요. 더욱 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

Cloud Volumes ONTAP 의 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함되어 있습니다.

포트	규약	목적
모두	모든 TCP	모든 아웃바운드 트래픽
모두	모든 UDP	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Cloud Volumes ONTAP 의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

소스는 Cloud Volumes ONTAP 시스템의 인터페이스(IP 주소)입니다.

서비스	포트	규약	원천	목적지	목적
액티브 디렉토리	88	TCP	노드 관리 LIF	Active Directory 포리스트	Kerberos V 인증
	137	UDP	노드 관리 LIF	Active Directory 포리스트	NetBIOS 이름 서비스
	138	UDP	노드 관리 LIF	Active Directory 포리스트	NetBIOS 데이터그램 서비스
	139	TCP	노드 관리 LIF	Active Directory 포리스트	NetBIOS 서비스 세션
	389	TCP 및 UDP	노드 관리 LIF	Active Directory 포리스트	LDAP
	445	TCP	노드 관리 LIF	Active Directory 포리스트	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
	464	TCP	노드 관리 LIF	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(SET_CHANGE)
	464	UDP	노드 관리 LIF	Active Directory 포리스트	Kerberos 키 관리
	749	TCP	노드 관리 LIF	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(RPCSEC_GSS)
	88	TCP	데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트	Kerberos V 인증
	137	UDP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 이름 서비스
	138	UDP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 데이터그램 서비스
	139	TCP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 서비스 세션
	389	TCP 및 UDP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	LDAP
	445	TCP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
	464	TCP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(SET_CHANGE)
	464	UDP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos 키 관리
	749	TCP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(RPCSEC_GSS)

서비스	포트	규약	원천	목적지	목적
AutoSupport	HTTPS	443	노드 관리 LIF	mysupport.netapp.com	AutoSupport (HTTPS가 기본값)
	HTTP	80	노드 관리 LIF	mysupport.netapp.com	AutoSupport (전송 프로토콜이 HTTPS에서 HTTP로 변경된 경우에만)
	TCP	3128	노드 관리 LIF	콘솔 에이전트	아웃바운드 인터넷 연결이 불가능한 경우 콘솔 에이전트의 프록시 서버를 통해 AutoSupport 메시지 보내기
구성 백업	HTTP	80	노드 관리 LIF	http://<콘솔 에이전트 IP 주소>/occm/offboxconfig	구성 백업을 콘솔 에이전트로 보냅니다. "ONTAP 문서" .
DHCP	68	UDP	노드 관리 LIF	DHCP	최초 설정을 위한 DHCP 클라이언트
DHCPS	67	UDP	노드 관리 LIF	DHCP	DHCP 서버
DNS	53	UDP	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	18600년–18699년	TCP	노드 관리 LIF	대상 서버	NDMP 사본
SMTP	25	TCP	노드 관리 LIF	메일 서버	SMTP 알림은 AutoSupport 에 사용할 수 있습니다.
SNMP	161	TCP	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	161	UDP	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	162	TCP	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	162	UDP	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
SnapMirror	11104	TCP	클러스터 간 LIF	ONTAP 클러스터 간 LIF	SnapMirror 위한 클러스터 간 통신 세션 관리
	11105	TCP	클러스터 간 LIF	ONTAP 클러스터 간 LIF	SnapMirror 데이터 전송
시스템 로그	514	UDP	노드 관리 LIF	시스템 로그 서버	Syslog 전달 메시지

콘솔 에이전트에 대한 요구 사항

아직 콘솔 에이전트를 만들지 않았다면 콘솔 에이전트에 대한 네트워킹 요구 사항도 검토해야 합니다.

- "콘솔 에이전트에 대한 네트워킹 요구 사항 보기"
- "Azure의 보안 그룹 규칙"

관련 주제

- "Cloud Volumes ONTAP 에 대한 AutoSupport 설정 확인"

- "ONTAP 내부 포트에 대해 알아보세요" .

Azure에서 고객 관리 키를 사용하도록 **Cloud Volumes ONTAP** 설정

Azure의 Cloud Volumes ONTAP 에서는 Microsoft에서 관리하는 키를 사용하여 Azure Storage Service Encryption을 사용하여 데이터가 자동으로 암호화됩니다. 하지만 이 페이지의 단계에 따라 자신의 암호화 키를 대신 사용할 수 있습니다.

데이터 암호화 개요

Cloud Volumes ONTAP 데이터는 Azure에서 자동으로 암호화됩니다. "Azure Storage 서비스 암호화" . 기본 구현에서는 Microsoft에서 관리하는 키를 사용합니다. 설정이 필요하지 않습니다.

Cloud Volumes ONTAP 에서 고객 관리 키를 사용하려면 다음 단계를 완료해야 합니다.

1. Azure에서 키 자격 증명 모음을 만든 다음 해당 자격 증명 모음에서 키를 생성합니다.
2. NetApp Console 에서 API를 사용하여 키를 사용하는 Cloud Volumes ONTAP 시스템을 만듭니다.

데이터 암호화 방법

콘솔은 디스크 암호화 세트를 사용하는데, 이를 통해 페이지 블롭이 아닌 관리형 디스크에서 암호화 키를 관리할 수 있습니다. 새로운 데이터 디스크도 동일한 디스크 암호화 세트를 사용합니다. 하위 버전에서는 고객 관리 키 대신 Microsoft 관리 키를 사용합니다.

고객 관리 키를 사용하도록 구성된 Cloud Volumes ONTAP 시스템을 생성한 후 Cloud Volumes ONTAP 데이터는 다음과 같이 암호화됩니다.

Cloud Volumes ONTAP 구성	키 암호화에 사용되는 시스템 디스크	키 암호화에 사용되는 데이터 디스크
단일 노드	• 부팅 • 핵심 • NVRAM	• 뿌리 • 데이터
페이지 Blob이 있는 Azure HA 단일 가용성 영역	• 부팅 • 핵심 • NVRAM	None
공유 관리 디스크가 있는 Azure HA 단일 가용성 영역	• 부팅 • 핵심 • NVRAM	• 뿌리 • 데이터
공유 관리 디스크를 사용한 Azure HA 다중 가용성 영역	• 부팅 • 핵심 • NVRAM	• 뿌리 • 데이터

Cloud Volumes ONTAP 의 모든 Azure 스토리지 계정은 고객 관리 키를 사용하여 암호화됩니다. 스토리지 계정을 생성하는 동안 암호화하려면 Cloud Volumes ONTAP 생성 요청에서 리소스 ID를 생성하고 제공해야 합니다. 이는 모든 유형의 배포에 적용됩니다. 해당 정보를 제공하지 않으면 저장소 계정은 여전히 암호화되지만 콘솔은 먼저 Microsoft에서 관리하는 키 암호화를 사용하여 저장소 계정을 만든 다음, 저장소 계정을 업데이트하여 고객이 관리하는 키를 사용합니다.

Cloud Volumes ONTAP 의 키 회전

암호화 키를 구성할 때 Azure Portal을 사용하여 자동 키 순환을 설정하고 활성화해야 합니다. 암호화 키의 새로운 버전을 만들고 활성화하면 Cloud Volumes ONTAP 암호화에 최신 키 버전을 자동으로 감지하고 사용할 수 있으므로 수동 개입 없이도 데이터가 안전하게 유지됩니다.

키 구성 및 키 순환 설정에 대한 자세한 내용은 다음 Microsoft Azure 설명서 항목을 참조하세요.

- "Azure Key Vault에서 암호화 키 자동 순환 구성"
- "Azure PowerShell - 고객 관리 키 사용"

> ⓘ 키를 구성한 후 다음을 선택했는지 확인하십시오. "자동 회전 활성화" 이를 통해 Cloud Volumes ONTAP 이전 키가 만료되면 새 키를 사용할 수 있습니다. Azure Portal에서 이 옵션을 활성화하지 않으면 Cloud Volumes ONTAP 새 키를 자동으로 감지하지 못하여 스토리지 프로비저닝에 문제가 발생할 수 있습니다.

사용자가 할당한 관리 ID 만들기

사용자 지정 관리 ID라는 리소스를 만들 수 있는 옵션이 있습니다. 이렇게 하면 Cloud Volumes ONTAP 시스템을 생성할 때 스토리지 계정을 암호화할 수 있습니다. 키 보관소를 만들고 키를 생성하기 전에 이 리소스를 만드는 것이 좋습니다.

리소스의 ID는 다음과 같습니다. `userassignedidentity` .

단계

1. Azure에서 Azure 서비스로 이동하여 *관리 ID*를 선택합니다.
2. *만들기*를 클릭하세요.
3. 다음 세부 정보를 제공하세요.
    - 구독: 구독을 선택하세요. 콘솔 에이전트 구독과 동일한 구독을 선택하는 것이 좋습니다.
    - 리소스 그룹: 기존 리소스 그룹을 사용하거나 새 리소스 그룹을 만듭니다.
    - 지역: 선택적으로 콘솔 에이전트와 동일한 지역을 선택합니다.
    - 이름: 리소스의 이름을 입력하세요.
4. 선택적으로 태그를 추가합니다.
5. *만들기*를 클릭하세요.

키 볼트를 생성하고 키를 생성합니다.

키 보관소는 Cloud Volumes ONTAP 시스템을 만들려는 동일한 Azure 구독 및 지역에 있어야 합니다.

만약 당신이라면사용자가 할당한 관리 ID를 생성했습니다. 키 보관소를 생성하는 동안 키 보관소에 대한 액세스 정책도 생성해야 합니다.

단계

1. "Azure 구독에서 키 자격 증명 모음 만들기" .

   키 보관소에 대한 다음 요구 사항을 참고하세요.

   - 키 볼트는 Cloud Volumes ONTAP 시스템과 동일한 지역에 있어야 합니다.
   - 다음 옵션을 활성화해야 합니다.
     - 소프트 삭제 (이 옵션은 기본적으로 활성화되어 있지만 비활성화해서는 안 됩니다)
     - 퍼지 보호
     - 볼륨 암호화를 위한 **Azure Disk Encryption** (단일 노드 시스템, 여러 영역의 HA 쌍 및 HA 단일 AZ 배포용)

       Azure 고객 관리 암호화 키를 사용하려면 키 자격 증명 모음에 Azure Disk 암호화가 활성화되어 있어야 합니다.

   - 사용자가 할당한 관리 ID를 생성한 경우 다음 옵션을 활성화해야 합니다.
     - 금고 접근 정책
2. Vault 액세스 정책을 선택한 경우 만들기를 클릭하여 키 볼트에 대한 액세스 정책을 만듭니다. 그렇지 않은 경우 3단계로 넘어가세요.
   a. 다음 권한을 선택하세요.
      - 얻다
      - 목록
      - 해독하다
      - 암호화하다
      - 열쇠를 풀다
      - 랩 키
      - 확인하다
      - 징후
   b. 사용자가 할당한 관리 ID(리소스)를 주체로 선택합니다.
   c. 액세스 정책을 검토하고 생성합니다.
3. "키 보관소에서 키 생성" .

   키에 대한 다음 요구 사항을 참고하세요.

   - 키 유형은 *RSA*여야 합니다.
   - 권장되는 RSA 키 크기는 *2048*이지만 다른 크기도 지원됩니다.

암호화 키를 사용하는 시스템을 만듭니다.

키 볼트를 만들고 암호화 키를 생성한 후에는 해당 키를 사용하도록 구성된 새 Cloud Volumes ONTAP 시스템을 만들 수 있습니다. 이러한 단계는 API를 사용하여 지원됩니다.

필요한 권한

단일 노드 Cloud Volumes ONTAP 시스템에서 고객 관리 키를 사용하려면 콘솔 에이전트에 다음 권한이 있는지 확인하세요.

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"최신 권한 목록 보기"

단계

1. 다음 API 호출을 사용하여 Azure 구독의 주요 자격 증명 모음 목록을 가져옵니다.

   HA 쌍의 경우: `GET /azure/ha/metadata/vaults`

   단일 노드의 경우: `GET /azure/vsa/metadata/vaults`

   *이름*과 *리소스그룹*을 기록해 두세요. 다음 단계에서 해당 값을 지정해야 합니다.

   "이 API 호출에 대해 자세히 알아보세요" .

2. 다음 API 호출을 사용하여 볼트 내의 키 목록을 가져옵니다.

   HA 쌍의 경우: `GET /azure/ha/metadata/keys-vault`

   단일 노드의 경우: `GET /azure/vsa/metadata/keys-vault`

   *keyName*을 기록해 두세요. 다음 단계에서는 해당 값(볼트 이름과 함께)을 지정해야 합니다.

   "이 API 호출에 대해 자세히 알아보세요" .

3. 다음 API 호출을 사용하여 Cloud Volumes ONTAP 시스템을 만듭니다.

   a. HA 쌍의 경우:

      `POST /azure/ha/working-environments`

      요청 본문에는 다음 필드가 포함되어야 합니다.

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

포함하다 "userAssignedIdentity": " userAssignedIdentityId" 저장소 계정 암호화에 사용할 리소스를 만든 경우 필드입니다.

"이 API 호출에 대해 자세히 알아보세요" .

b. 단일 노드 시스템의 경우:

`POST /azure/vsa/working-environments`

요청 본문에는 다음 필드가 포함되어야 합니다.

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

포함하다 "userAssignedIdentity": " userAssignedIdentityId" 저장소 계정 암호화에 사용할 리소스를 만든 경우 필드입니다.

"이 API 호출에 대해 자세히 알아보세요" .

결과

데이터 암호화를 위해 고객 관리 키를 사용하도록 구성된 새로운 Cloud Volumes ONTAP 시스템이 있습니다.

Azure에서 **Cloud Volumes ONTAP** 에 대한 라이선싱 설정

Cloud Volumes ONTAP 에서 사용할 라이선싱 옵션을 결정한 후에는 새 시스템을 만들 때 해당 라이선싱 옵션을 선택하기 전에 몇 가지 단계를 거쳐야 합니다.

프리미엄

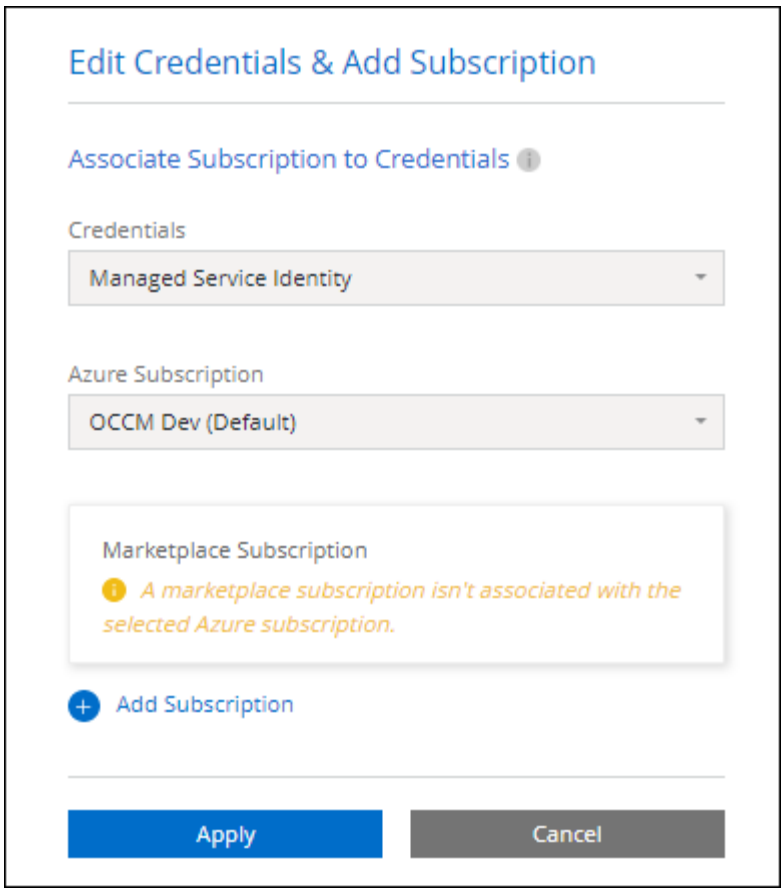
최대 500GiB의 프로비저닝 용량을 제공하는 Cloud Volumes ONTAP 무료로 사용하려면 Freemium 옵션을 선택하세요. "Freemium 제공에 대해 자세히 알아보세요" .

단계

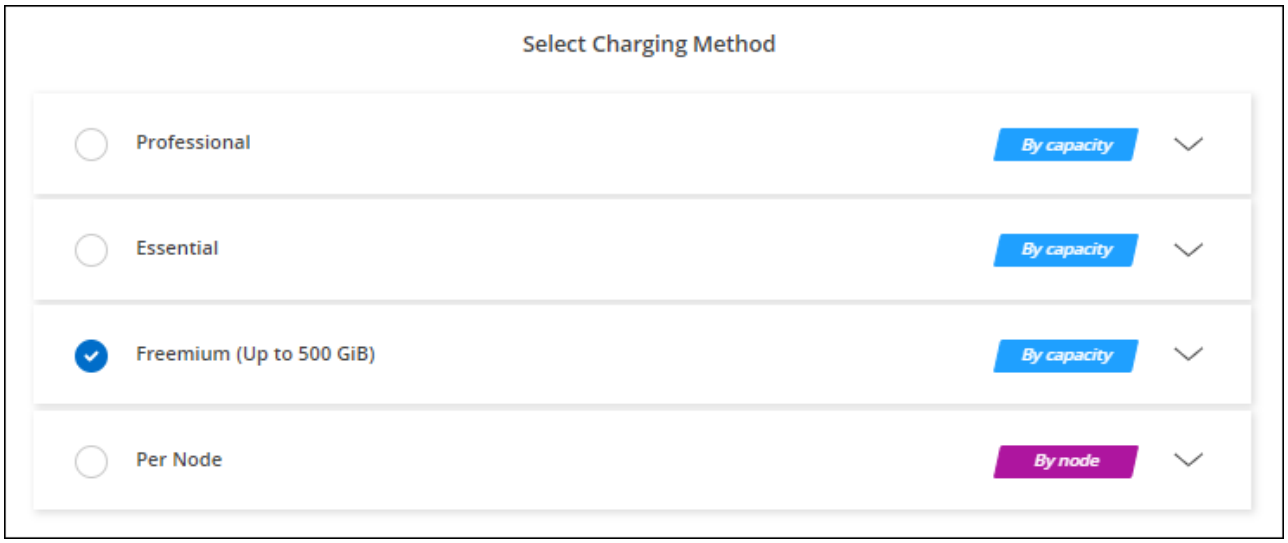
1. NetApp Console 의 왼쪽 탐색 메뉴에서 *스토리지 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 화면의 지시에 따라 Azure Marketplace에서 종량제 상품을 구독하세요.

   프로비저닝된 용량이 500GiB를 초과하지 않는 한 마켓플레이스 구독을 통해 요금이 청구되지 않습니다. 초과 시 시스템은 자동으로 다음 용량으로 변환됩니다."필수 패키지" .



a. 콘솔로 돌아와서 요금 청구 방법 페이지에서 *프리미엄*을 선택하세요.



"Azure에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

용량 기반 라이센스

용량 기반 라이선싱을 사용하면 TiB 용량당 Cloud Volumes ONTAP 비용을 지불할 수 있습니다. 용량 기반 라이선싱은 패키지 형태로 제공됩니다. 패키지에는 Essentials 패키지와 Professional 패키지가 있습니다.

Essentials 및 Professional 패키지는 다음과 같은 소비 모델 또는 구매 옵션으로 이용 가능합니다.

- NetApp 에서 구매한 라이선스(BYOL(Bring Your Own License))
- Azure Marketplace의 시간당, 사용량에 따라 지불(PAYGO) 구독
- 연간 계약

"용량 기반 라이선싱에 대해 자세히 알아보세요" .

다음 섹션에서는 각 소비 모델을 시작하는 방법을 설명합니다.

바이올

NetApp 에서 라이선스(BYOL)를 구매하여 선불로 지불하면 모든 클라우드 공급자에 Cloud Volumes ONTAP 시스템을 배포할 수 있습니다.

NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 에 대한 BYOL 라이선싱의 제한된 가용성" .

단계

1. "라이센스를 얻으려면 NetApp Sales에 문의하세요."
2. "콘솔에 NetApp 지원 사이트 계정 추가"

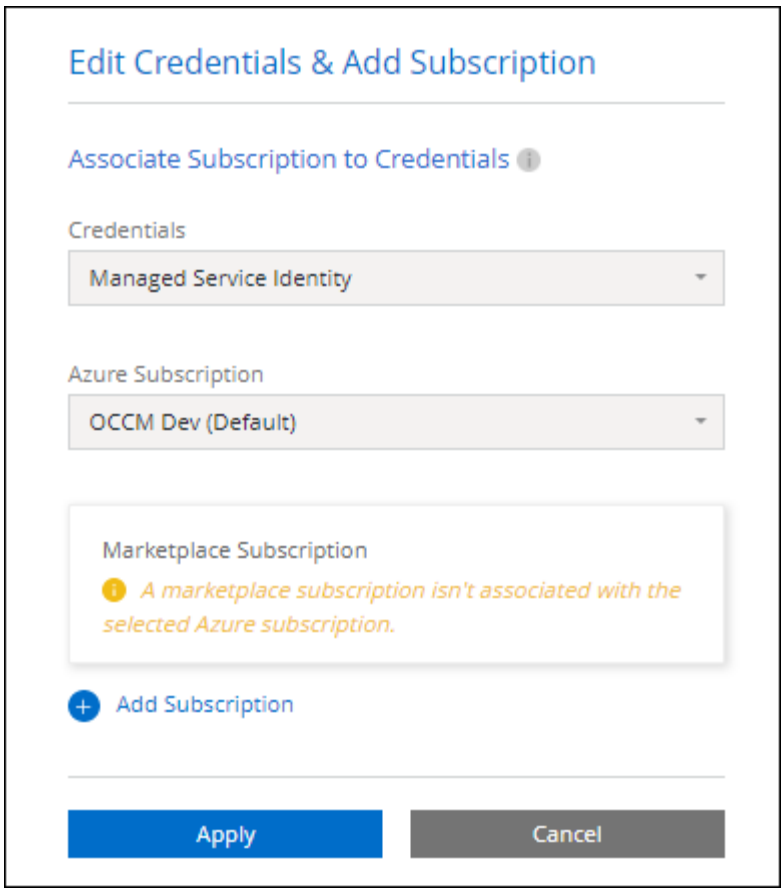
   콘솔은 NetApp 지원 사이트 계정과 연결된 라이선스에 대한 세부 정보를 얻기 위해 NetApp 라이선스 서비스에 자동으로 쿼리를 보냅니다. 오류가 없으면 콘솔이 자동으로 라이선스를 콘솔에 추가합니다.

   Cloud Volumes ONTAP 에서 라이선스를 사용하려면 먼저 콘솔에서 라이선스를 사용할 수 있어야 합니다. 필요한 경우 다음을 수행할 수 있습니다."콘솔에 라이센스를 수동으로 추가합니다." .

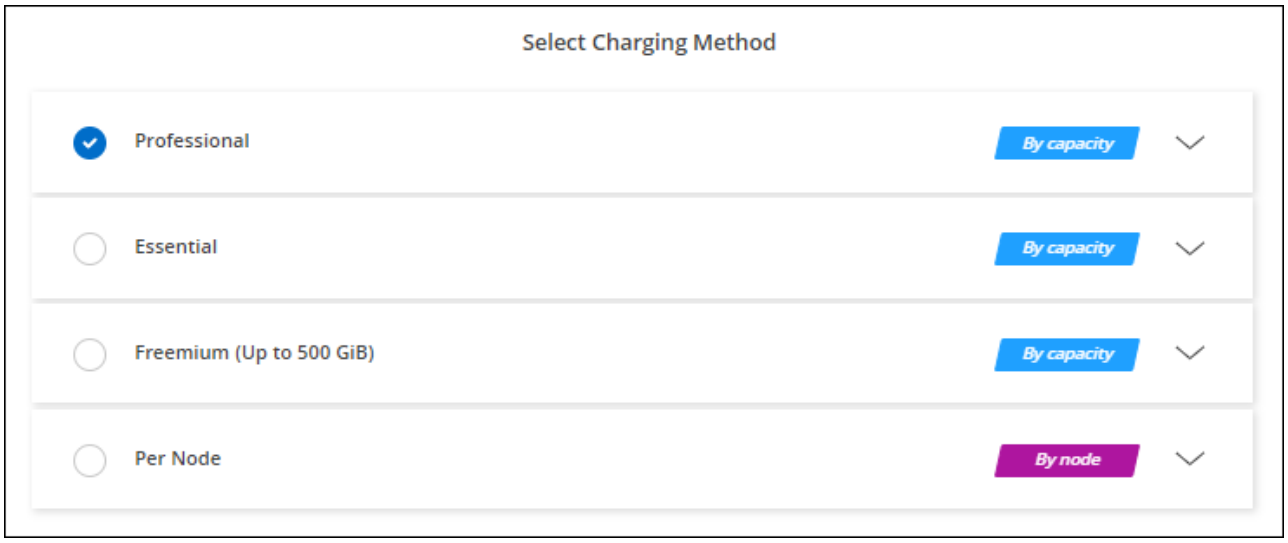
3. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 화면의 지시에 따라 Azure Marketplace에서 종량제 상품을 구독하세요.

      NetApp 에서 구매한 라이선스는 항상 먼저 청구되지만, 라이선스 용량을 초과하거나 라이선스 기간이 만료되면 마켓플레이스의 시간당 요금으로 청구됩니다.



a. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"Azure에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

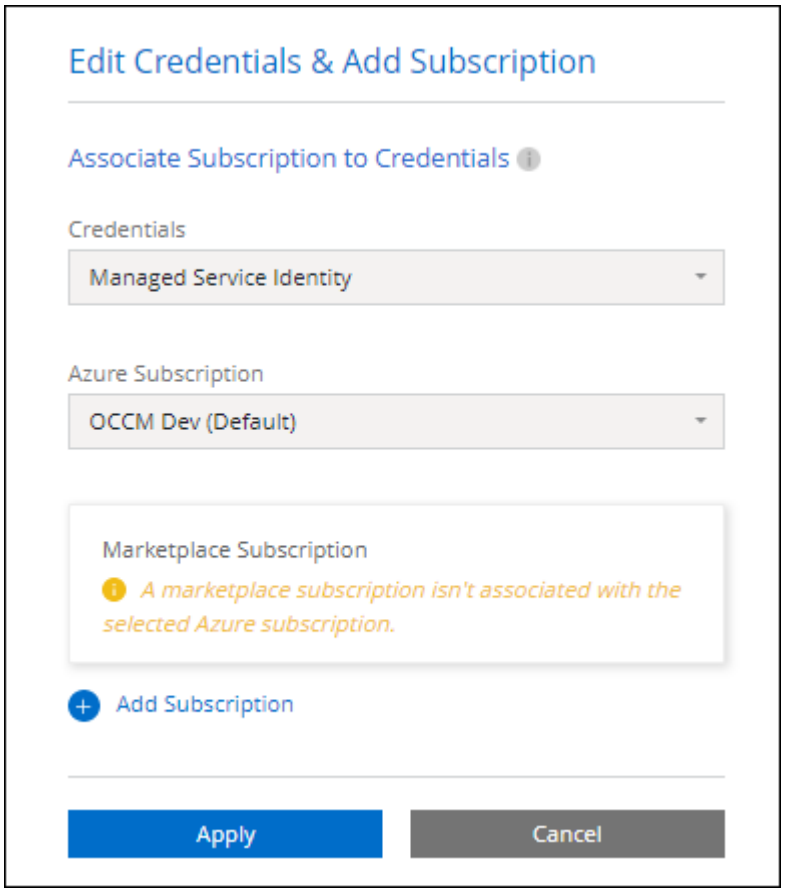
PAYGO 구독

클라우드 공급업체의 마켓플레이스에서 제공하는 혜택을 구독하여 시간당 요금을 지불하세요.

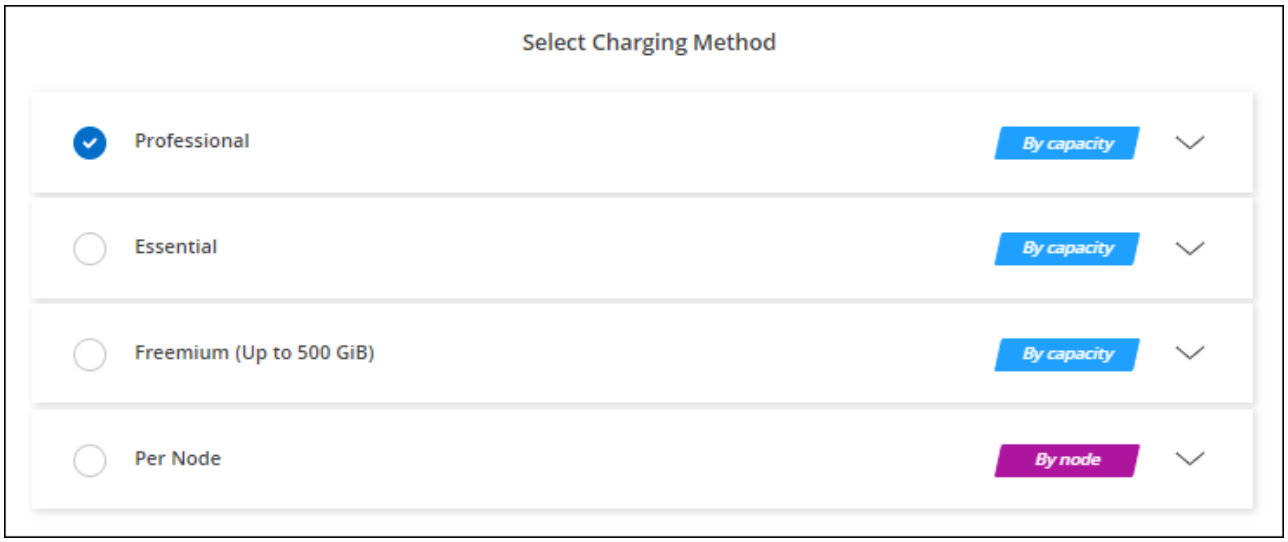
Cloud Volumes ONTAP 시스템을 만들면 콘솔에서 Azure Marketplace에서 제공되는 계약에 가입하라는 메시지가 표시됩니다. 해당 구독은 요금 청구를 위해 시스템에 연결됩니다. 동일한 구독을 추가 시스템에도 사용할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 화면의 지시에 따라 Azure Marketplace에서 종량제 상품을 구독하세요.



   b. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"Azure에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

설정 > 자격 증명 페이지에서 Azure 계정과 연결된 Azure Marketplace 구독을 관리할 수 있습니다. "Azure 계정 및 구독을 관리하는 방법을 알아보세요."

연간 계약

연간 계약을 구매하여 매년 Cloud Volumes ONTAP 에 대한 비용을 지불하세요.

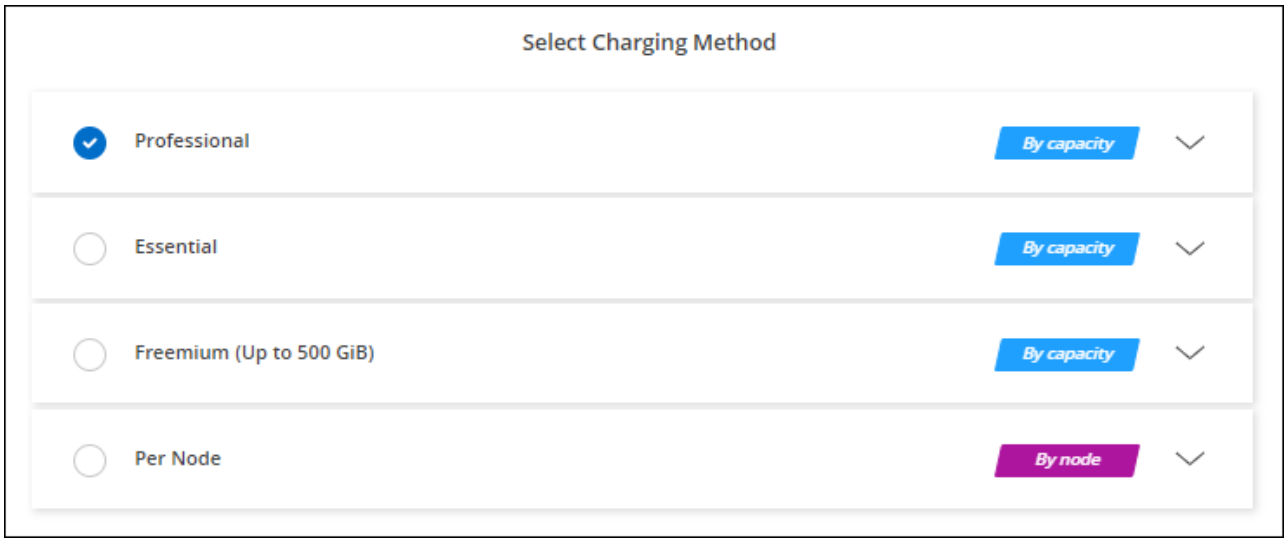
단계

1. 연간 계약을 구매하려면 NetApp 영업 담당자에게 문의하세요.

   해당 계약은 Azure Marketplace에서 비공개 제안으로 제공됩니다.

   NetApp 에서 비공개 제안을 공유한 후, 시스템을 만드는 동안 Azure Marketplace에서 구독할 때 연간 요금제를 선택할 수 있습니다.

2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가 > 계속*을 클릭합니다.
   b. Azure Portal에서 Azure 계정과 공유된 연간 플랜을 선택한 다음 *구독*을 클릭합니다.
   c. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"Azure에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

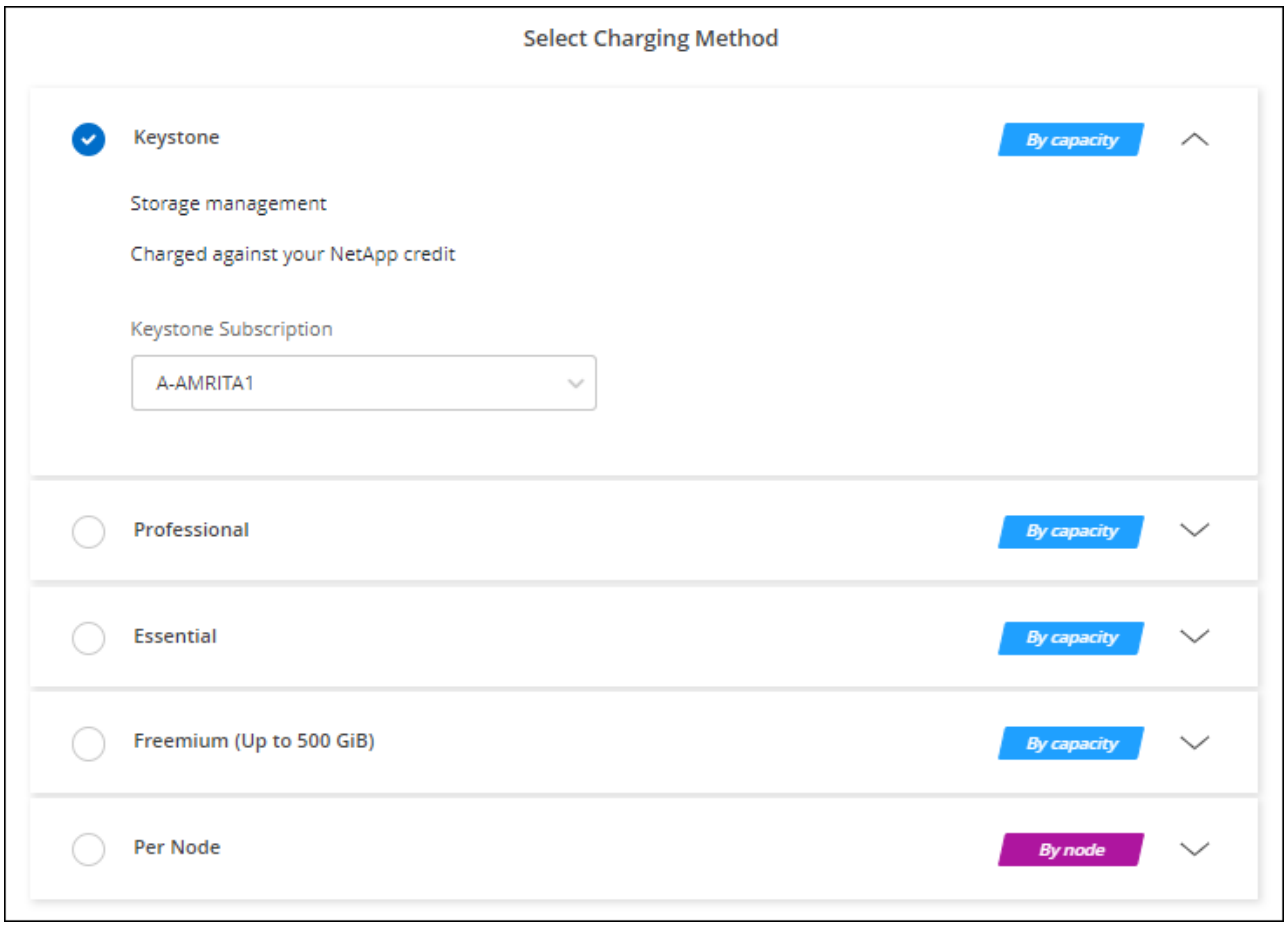
Keystone 구독

Keystone 구독은 사용량에 따라 비용을 지불하는 구독 기반 서비스입니다. "NetApp Keystone 구독에 대해 자세히 알아보세요" .

단계

1. 아직 구독이 없으신 경우, "NetApp 에 문의하세요"
2. 콘솔에서 하나 이상의 Keystone 구독으로 사용자 계정을 인증하려면 NetApp 에 문의으로 이메일을 보내주세요.
3. NetApp 귀하의 계정을 승인한 후,"Cloud Volumes ONTAP 과 함께 사용할 구독을 연결하세요" .

4. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
   a. 청구 방법을 선택하라는 메시지가 표시되면 Keystone 구독 청구 방법을 선택하세요.



"Azure에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

노드 기반 라이센스

노드 기반 라이선스는 Cloud Volumes ONTAP 의 이전 세대 라이선스입니다. 노드 기반 라이선스는 NetApp (BYOL)에서 구매할 수 있으며, 특정 경우에만 라이선스를 갱신할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- "노드 기반 라이선스의 가용성 종료"
- "노드 기반 라이선스 제공 종료"
- "노드 기반 라이선스를 용량 기반 라이선스로 변환"

Azure에서 **Cloud Volumes ONTAP** 에 대해 고가용성 모드 활성화

예기치 않은 장애 조치 시간을 줄이고 Cloud Volumes ONTAP에 대한 NFSv4 지원을 활성화하려면 Microsoft Azure의 고가용성(HA) 모드를 활성화해야 합니다. 이 모드를 활성화하면 Cloud Volumes ONTAP HA 노드는 CIFS 및 NFSv4 클라이언트에 대한 예기치 않은 장애 조치 시 낮은(60초) 복구 시간 목표(RTO)를 달성할 수 있습니다.

Cloud Volumes ONTAP 9.10.1부터 Microsoft Azure에서 실행되는 Cloud Volumes ONTAP HA 쌍에 대한 계획되지 않은 장애 조치 시간을 줄이고 NFSv4에 대한 지원을 추가했습니다. 이러한 향상된 기능을 Cloud Volumes ONTAP 에

적용하려면 Azure 구독에서 고가용성 기능을 활성화해야 합니다.

이 작업에 관하여

NetApp Console은 Azure 구독에서 해당 기능을 활성화해야 할 때 다음과 같은 세부 정보를 표시합니다. 다음 사항에 유의하십시오.

- Cloud Volumes ONTAP HA 쌍의 고가용성에는 문제가 없습니다. 이 Azure 기능은 ONTAP 과 함께 작동하여 계획되지 않은 장애 조치 이벤트로 인해 NFS 프로토콜에 대한 클라이언트 관찰 애플리케이션 중단 시간을 줄입니다.
- 이 기능을 활성화해도 Cloud Volumes ONTAP HA 쌍은 중단되지 않습니다.
- Azure 구독에서 이 기능을 활성화해도 다른 VM에는 문제가 발생하지 않습니다.
- Cloud Volumes ONTAP CIFS 및 NFS 클라이언트에서 클러스터 및 SVM 관리 LIF의 장애 조치 중에 내부 Azure Load Balancer를 사용합니다.
- HA 모드가 활성화되면 콘솔은 12시간마다 시스템을 검사하여 내부 Azure Load Balancer 규칙을 업데이트합니다.

단계

소유자 권한이 있는 Azure 사용자는 Azure CLI에서 해당 기능을 활성화할 수 있습니다.

1. "Azure Portal에서 Azure Cloud Shell에 액세스"
2. 고가용성 모드 기능을 등록하세요:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. 선택적으로 해당 기능이 등록되었는지 확인하세요.

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure CLI는 다음과 유사한 결과를 반환해야 합니다.

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

관련 링크

1. "Microsoft Azure 설명서: 고가용성 포트 개요"
2. "Microsoft Azure 설명서: Azure CLI 시작하기"

Azure에서 **Cloud Volumes ONTAP** 에 **VMOrchestratorZonalMultiFD** 사용

로컬 중복 스토리지(LRS) 단일 가용성 영역(AZ)에 VM 인스턴스를 배포하려면 Microsoft를 활성화해야 합니다. `Microsoft.Compute/VMOrchestratorZonalMultiFD` 귀하의 구독에 대한 기능입니다. 고가용성(HA) 모드에서 이 기능은 동일한 가용성 영역 내의 별도의 장애 도메인에 노드를 배포하는 것을 용이하게 합니다.

이 기능을 활성화하지 않으면 영역별 배포가 발생하지 않으며, 이전 LRS 비영역별 배포가 적용됩니다.

단일 가용성 영역에 VM을 배포하는 방법에 대한 자세한 내용은 다음을 참조하세요."Azure의 고가용성 쌍" .

"소유자" 권한이 있는 사용자로 다음 단계를 수행하세요.

단계

1. Azure Portal에서 Azure Cloud Shell에 액세스합니다. 자세한 내용은 다음을 참조하세요. "Microsoft Azure 설명서: Azure Cloud Shell 시작하기" .
2. 등록하세요 `Microsoft.Compute/VMOrchestratorZonalMultiFD` 다음 명령을 실행하여 기능을 추가하세요.

   az 계정 설정 -s <*Azure_subscription_name_or_ID*> az 기능 등록 --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute

3. 등록 상태와 출력 샘플을 확인하세요.

   az 기능 표시 -n VMOrchestratorZonalMultiFD --네임스페이스 Microsoft.Compute { "id": "/subscriptions/<*ID*>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "state": "등록됨" }, "type": "Microsoft.Features/providers/features" }

Azure에서 **Cloud Volumes ONTAP** 실행

NetApp Console에서 Cloud Volumes ONTAP 시스템을 생성하여 Azure에서 단일 노드 시스템 또는 HA 쌍을 시작할 수 있습니다.

시작하기 전에

시작하기 전에 다음 사항이 필요합니다.

- 이미 실행 중인 콘솔 에이전트입니다.
  - 당신은 ~을 가져야합니다 "시스템과 연결된 콘솔 에이전트" .
  - "항상 콘솔 에이전트를 실행 상태로 두어야 합니다." .

- 사용하려는 구성에 대한 이해.

  구성을 계획해야 하며, 관리자로부터 필요한 Azure 네트워킹 세부 정보를 받아야 합니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 구성 계획" .

- Cloud Volumes ONTAP 에 대한 라이선싱을 설정하는 데 필요한 사항에 대한 이해.

  "라이선싱 설정 방법 알아보기" .

이 작업에 관하여

콘솔이 Azure에 Cloud Volumes ONTAP 시스템을 만들면 리소스 그룹, 네트워크 인터페이스, 스토리지 계정 등 여러 Azure 개체가 만들어집니다. 마법사가 끝나면 리소스 요약을 검토할 수 있습니다.

> 데이터 손실 가능성
>
> 가장 좋은 방법은 각 Cloud Volumes ONTAP 시스템에 대해 새로운 전용 리소스 그룹을 사용하는 것입니다.
>
> 데이터 손실 위험 때문에 기존의 공유 리소스 그룹에 Cloud Volumes ONTAP 배포하는 것은 권장되지 않습니다. 배포 실패 또는 삭제 시 콘솔에서 공유 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거할 수 있지만, Azure 사용자가 실수로 공유 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 삭제할 수도 있습니다.

Azure에서 단일 노드 **Cloud Volumes ONTAP** 시스템 실행

Azure에서 단일 노드 Cloud Volumes ONTAP 시스템을 시작하려면 Console에서 단일 노드 시스템을 생성해야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. 위치 선택: *Microsoft Azure*와 * Cloud Volumes ONTAP 단일 노드*를 선택하세요.
4. 메시지가 표시되면 "콘솔 에이전트 생성" .
5. 세부 정보 및 자격 증명: 필요에 따라 Azure 자격 증명과 구독을 변경하고, 클러스터 이름을 지정하고, 필요한 경우 태그를 추가한 다음 자격 증명을 지정합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Azure 가상 머신의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
리소스 그룹 태그	태그는 Azure 리소스에 대한 메타데이터입니다. 이 필드에 태그를 입력하면 콘솔이 Cloud Volumes ONTAP 시스템과 연결된 리소스 그룹에 태그를 추가합니다. 시스템을 생성할 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 시스템을 생성한 후에 태그를 더 추가할 수 있습니다. API는 시스템을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 정보는 다음을 참조하세요. "Microsoft Azure 설명서: 태그를 사용하여 Azure 리소스 구성" .

필드	설명
사용자 이름과 비밀번호	이는 Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하면 ONTAP System Manager나 ONTAP CLI를 통해 Cloud Volumes ONTAP 에 연결할 수 있습니다. 기본 *admin* 사용자 이름을 유지하거나 사용자 지정 사용자 이름으로 변경하세요.
자격 증명 편집	이 Cloud Volumes ONTAP 시스템에서는 다양한 Azure 자격 증명과 Azure 구독을 선택하여 사용할 수 있습니다. 사용량에 따라 지불하는 Cloud Volumes ONTAP 시스템을 배포하려면 선택한 Azure 구독과 Azure Marketplace 구독을 연결해야 합니다. "자격 증명을 추가하는 방법을 알아보세요" .

6. 서비스: Cloud Volumes ONTAP 과 함께 사용하거나 사용하지 않을 개별 서비스를 활성화하거나 비활성화합니다.
   - "NetApp Data Classification 에 대해 자세히 알아보세요"
   - "NetApp Backup and Recovery 에 대해 자세히 알아보세요"

   WORM 및 데이터 계층화를 활용하려면 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 시스템을 배포해야 합니다.

7. 위치: 지역, 가용성 영역, VNet 및 서브넷을 선택한 다음 확인란을 선택하여 콘솔 에이전트와 대상 위치 간의 네트워크 연결을 확인합니다.

   중국 지역의 경우 단일 노드 배포는 Cloud Volumes ONTAP 9.12.1 GA 및 9.13.0 GA에서만 지원됩니다. 이러한 버전을 Cloud Volumes ONTAP 의 최신 패치 및 릴리스로 업그레이드할 수 있습니다."Azure에서 지원됨" . 중국 지역에 이후 Cloud Volumes ONTAP 버전을 배포하려면 NetApp 지원팀에 문의하세요. 중국 지역에서는 NetApp 에서 직접 구매한 라이선스만 지원되며, 마켓플레이스 구독은 이용할 수 없습니다.

8. 연결성: 새 리소스 그룹이나 기존 리소스 그룹을 선택한 다음, 미리 정의된 보안 그룹을 사용할지 아니면 사용자 고유의 보안 그룹을 사용할지 선택합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
리소스 그룹	Cloud Volumes ONTAP 에 대한 새 리소스 그룹을 만들거나 기존 리소스 그룹을 사용하세요. 가장 좋은 방법은 Cloud Volumes ONTAP 에 대해 새로운 전용 리소스 그룹을 사용하는 것입니다. 기존의 공유 리소스 그룹에 Cloud Volumes ONTAP 배포하는 것은 가능하지만 데이터 손실 위험 때문에 권장하지는 않습니다. 자세한 내용은 위의 경고를 참조하세요. 사용 중인 Azure 계정에 다음이 있는 경우 "필요한 권한" 배포 실패 또는 삭제 시 콘솔은 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거합니다.

필드	설명
생성된 보안 그룹	콘솔에서 보안 그룹을 생성하도록 허용하는 경우 트래픽 허용 방법을 선택해야 합니다. • *선택한 VNet만*을 선택하는 경우 인바운드 트래픽의 소스는 선택한 VNet의 서브넷 범위와 콘솔 에이전트가 있는 VNet의 서브넷 범위입니다. 이것은 권장되는 옵션입니다. • *모든 VNet*을 선택하면 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 사용	기존 보안 그룹을 선택하는 경우 Cloud Volumes ONTAP 요구 사항을 충족해야 합니다. "기본 보안 그룹 보기" .

9. 청구 방법 및 **NSS** 계정: 이 시스템에서 사용할 청구 옵션을 지정한 다음 NetApp 지원 사이트 계정을 지정하세요.
   - "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요" .
   - "라이선싱 설정 방법 알아보기" .
10. 사전 구성된 패키지: Cloud Volumes ONTAP 시스템을 빠르게 배포하려면 패키지 중 하나를 선택하거나 *내 구성 만들기*를 클릭하세요.

    패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.
11. 라이선스: 필요한 경우 Cloud Volumes ONTAP 버전을 변경하고 가상 머신 유형을 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 출시 버전 또는 패치 릴리스가 제공되는 경우 BlueXP 작업 환경을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.16.1 P3를 선택하고 9.16.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리스에서 다른 릴리스로 전달되지 않습니다(예: 9.15에서 9.16로 전달).
12. **Azure Marketplace**에서 구독: 콘솔에서 Cloud Volumes ONTAP 의 프로그래밍 방식 배포를 활성화할 수 없는 경우 이 페이지가 표시됩니다. 화면에 나열된 단계를 따르세요. "마켓플레이스 제품의 프로그래밍 방식 배포" 자세한 내용은.
13. 기본 스토리지 리소스: 초기 집계에 대한 설정을 선택합니다. 디스크 유형, 각 디스크의 크기, Blob 스토리지에 대한 데이터 계층화를 활성화할지 여부입니다.

    다음 사항에 유의하세요.
    - VNet 내에서 스토리지 계정에 대한 공용 액세스가 비활성화된 경우 Cloud Volumes ONTAP 시스템에서 데이터 계층화를 활성화할 수 없습니다. 자세한 내용은 다음을 참조하세요."보안 그룹 규칙" .
    - 디스크 유형은 초기 볼륨을 위한 것입니다. 이후 볼륨에는 다른 디스크 유형을 선택할 수 있습니다.
    - 디스크 크기는 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔이 생성하는 모든 추가 집계에 적용됩니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.

      디스크 유형 및 크기 선택에 대한 도움말은 다음을 참조하세요."Azure에서 시스템 크기 조정" .
    - 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
    - 데이터 계층화를 비활성화하면 이후 집계에서 활성화할 수 있습니다.

      "데이터 계층화에 대해 자세히 알아보세요" .

14. 쓰기 속도 및 **WORM**:

    a. 원하는 경우 보통 또는 높음 쓰기 속도를 선택하세요.

       "쓰기 속도에 대해 자세히 알아보세요" .

    b. 원하는 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

       이 옵션은 특정 VM 유형에만 사용할 수 있습니다. 지원되는 VM 유형을 알아보려면 다음을 참조하세요."HA 쌍에 대한 라이선스별 지원 구성" .

       Cloud Volumes ONTAP 버전 9.7 이하에서 데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로 되돌리거나 다운그레이드하는 것이 차단됩니다.

    "WORM 스토리지에 대해 자세히 알아보세요" .

    a. WORM 저장소를 활성화하는 경우 보존 기간을 선택하세요.

15. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

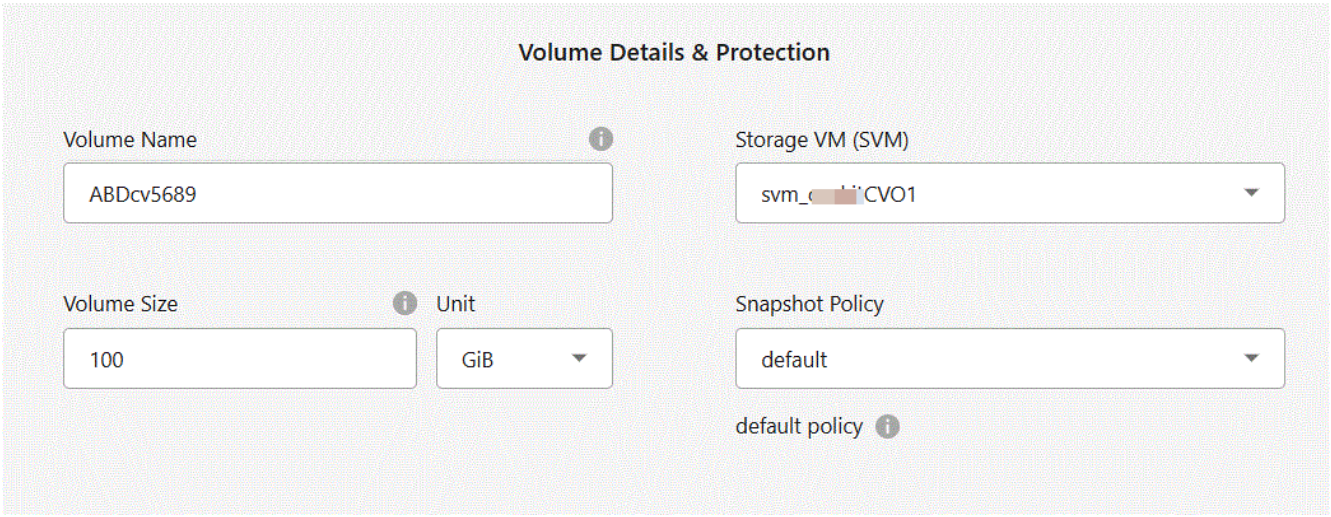
    "지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

    이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝을 활성화하는지 여부에 따라 크게 달라집니다. 씬 프로비저닝을 활성화하면 현재 사용 가능한 물리적 저장소보다 큰 볼륨을 만들 수 있습니다.
액세스 제어(NFS에만 해당)	내보내기 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 콘솔은 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS에만 해당)	이러한 필드를 사용하면 사용자 및 그룹의 공유 액세스 수준(액세스 제어 목록 또는 ACL이라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자나 그룹, 또는 UNIX 사용자나 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사 정책은 NetApp 스냅샷 복사본이 자동으로 생성되는 빈도와 수를 지정합니다. NetApp 스냅샷 복사본은 성능에 영향을 미치지 않고 최소한의 저장 공간만 필요한 특정 시점의 파일 시스템 이미지입니다. 기본 정책을 선택하거나 아무것도 선택하지 않을 수 있습니다. 일시적인 데이터의 경우 '없음'을 선택할 수 있습니다. 예를 들어 Microsoft SQL Server의 경우 tempdb를 선택합니다.
고급 옵션(NFS에만 해당)	볼륨에 대한 NFS 버전을 선택합니다: NFSv3 또는 NFSv4.

필드	설명
이니시에이터 그룹 및 IQN(iSCSI에만 해당)	iSCSI 스토리지 대상은 LUN(논리 단위)이라고 하며 호스트에 표준 블록 장치로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름 테이블이며, 어떤 이니시에이터가 어떤 LUN에 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 컨버지드 네트워크 어댑터(CNA) 또는 전용 호스트 버스 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 정규화된 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후, "IQN을 사용하여 호스트에서 LUN에 연결합니다." .

다음 이미지는 볼륨 생성 마법사의 첫 번째 페이지를 보여줍니다.



16. **CIFS** 설정: CIFS 프로토콜을 선택한 경우 CIFS 서버를 설정합니다.

필드	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인의 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.
도메인에 가입할 수 있는 권한이 있는 자격 증명	AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.
CIFS 서버 NetBIOS 이름	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Cloud Volumes ONTAP 의 AD 서버로 Azure AD Domain Services를 구성하려면 이 필드에 **OU=AADDC Computers** 또는 *OU=AADDC Users*를 입력해야 합니다.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 설명서: Azure AD Domain Services 관리 도메인에서 OU(조직 단위) 만들기"^]
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 대부분의 경우 도메인은 AD 도메인과 동일합니다.

필드	설명
NTP 서버	Active Directory DNS를 사용하여 NTP 서버를 구성하려면 *Active Directory 도메인 사용*을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 를 참조하세요 "NetApp Console 자동화 문서" 자세한 내용은. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

17. 사용 프로필, 디스크 유형 및 계층화 정책: 필요한 경우 스토리지 효율성 기능을 활성화할지 여부를 선택하고 볼륨 계층화 정책을 변경합니다.

    자세한 내용은 다음을 참조하세요."볼륨 사용 프로필 이해" 그리고"데이터 계층화 개요" .

18. 검토 및 승인: 선택 사항을 검토하고 확인합니다.
    a. 구성에 대한 세부 정보를 검토하세요.
    b. *자세한 정보*를 클릭하여 콘솔에서 구매할 지원 및 Azure 리소스에 대한 세부 정보를 검토하세요.
    c. 이해합니다... 확인란을 선택하세요.
    d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 시스템을 배포합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템 배포 중 문제가 발생하면 실패 메시지를 검토하세요. 시스템을 선택하고 *환경 다시 만들기*를 클릭할 수도 있습니다.

추가 도움말을 보려면 다음으로 이동하세요. "NetApp Cloud Volumes ONTAP 지원" .

> 배포 프로세스가 완료된 후에는 Azure Portal에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

당신이 완료한 후

- CIFS 공유를 프로비저닝한 경우 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 ONTAP 시스템 관리자나 ONTAP CLI를 사용하세요.

  할당량을 사용하면 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적할 수 있습니다.

Azure에서 Cloud Volumes ONTAP HA 쌍 시작

Azure에서 Cloud Volumes ONTAP HA 쌍을 시작하려면 콘솔에서 HA 시스템을 만들어야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. 메시지가 표시되면 "콘솔 에이전트 생성" .

4. 세부 정보 및 자격 증명: 필요에 따라 Azure 자격 증명과 구독을 변경하고, 클러스터 이름을 지정하고, 필요한 경우 태그를 추가한 다음 자격 증명을 지정합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Azure 가상 머신의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
리소스 그룹 태그	태그는 Azure 리소스에 대한 메타데이터입니다. 이 필드에 태그를 입력하면 콘솔이 Cloud Volumes ONTAP 시스템과 연결된 리소스 그룹에 태그를 추가합니다. 시스템을 생성할 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 시스템을 생성한 후에 태그를 더 추가할 수 있습니다. API는 시스템을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 정보는 다음을 참조하세요. "Microsoft Azure 설명서: 태그를 사용하여 Azure 리소스 구성" .
사용자 이름과 비밀번호	이는 Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하면 ONTAP System Manager나 ONTAP CLI를 통해 Cloud Volumes ONTAP 에 연결할 수 있습니다. 기본 *admin* 사용자 이름을 유지하거나 사용자 지정 사용자 이름으로 변경하세요.
자격 증명 편집	이 Cloud Volumes ONTAP 시스템에서는 다양한 Azure 자격 증명과 Azure 구독을 선택하여 사용할 수 있습니다. 사용량에 따라 지불하는 Cloud Volumes ONTAP 시스템을 배포하려면 선택한 Azure 구독과 Azure Marketplace 구독을 연결해야 합니다. "자격 증명을 추가하는 방법을 알아보세요" .

5. 서비스: Cloud Volumes ONTAP 과 함께 사용할지 여부에 따라 개별 서비스를 활성화하거나 비활성화합니다.
   - "NetApp Data Classification 에 대해 자세히 알아보세요"
   - "NetApp Backup and Recovery 에 대해 자세히 알아보세요"

   WORM 및 데이터 계층화를 활용하려면 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 시스템을 배포해야 합니다.

6. **HA** 배포 모델:
   a. 단일 가용 영역 또는 *다중 가용 영역*을 선택하세요.
      - 단일 가용성 영역의 경우 Azure 지역, 가용성 영역, VNet 및 서브넷을 선택합니다.

        Cloud Volumes ONTAP 9.15.1부터 Azure의 단일 가용성 영역(AZ)에 HA 모드로 가상 머신(VM) 인스턴스를 배포할 수 있습니다. 이 배포를 지원하는 영역과 지역을 선택해야 합니다. 해당 영역이나 지역이 영역별 배포를 지원하지 않는 경우 LRS에 대한 이전 비영역별 배포 모드가 따릅니다. 공유 관리 디스크에 대해 지원되는 구성을 이해하려면 다음을 참조하세요."공유 관리 디스크를 사용한 HA 단일 가용성 영역 구성" .

      - 여러 가용성 영역의 경우 노드 1에 대한 지역, VNet, 서브넷, 영역, 노드 2에 대한 영역을 선택합니다.

   b. 네트워크 연결을 확인했습니다... 확인란을 선택하세요.

7. 연결성: 새 리소스 그룹이나 기존 리소스 그룹을 선택한 다음, 미리 정의된 보안 그룹을 사용할지 아니면 사용자 고유의 보안 그룹을 사용할지 선택합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
리소스 그룹	Cloud Volumes ONTAP 에 대한 새 리소스 그룹을 만들거나 기존 리소스 그룹을 사용하세요. 가장 좋은 방법은 Cloud Volumes ONTAP 에 대해 새로운 전용 리소스 그룹을 사용하는 것입니다. 기존의 공유 리소스 그룹에 Cloud Volumes ONTAP 배포하는 것은 가능하지만 데이터 손실 위험 때문에 권장하지는 않습니다. 자세한 내용은 위의 경고를 참조하세요. Azure에 배포하는 각 Cloud Volumes ONTAP HA 쌍에 대해 전용 리소스 그룹을 사용해야 합니다. 리소스 그룹에서는 HA 쌍을 하나만 지원합니다. Azure 리소스 그룹에서 두 번째 Cloud Volumes ONTAP HA 쌍을 배포하려고 하면 콘솔에서 연결 문제가 발생합니다. 사용 중인 Azure 계정에 다음이 있는 경우 "필요한 권한" 배포 실패 또는 삭제 시 콘솔은 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거합니다.
생성된 보안 그룹	콘솔에서 보안 그룹을 생성하도록 허용하는 경우 트래픽 허용 방법을 선택해야 합니다. • *선택한 VNet만*을 선택하는 경우 인바운드 트래픽의 소스는 선택한 VNet의 서브넷 범위와 콘솔 에이전트가 있는 VNet의 서브넷 범위입니다. 이것은 권장되는 옵션입니다. • *모든 VNet*을 선택하면 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 사용	기존 보안 그룹을 선택하는 경우 Cloud Volumes ONTAP 요구 사항을 충족해야 합니다. "기본 보안 그룹 보기" .

8. 청구 방법 및 **NSS** 계정: 이 시스템에서 사용할 청구 옵션을 지정한 다음 NetApp 지원 사이트 계정을 지정하세요.
   - "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요" .
   - "라이선싱 설정 방법 알아보기" .
9. 사전 구성된 패키지: Cloud Volumes ONTAP 시스템을 빠르게 배포하려면 패키지 중 하나를 선택하거나 *구성 변경*을 클릭하세요.

   패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.
10. 라이선스: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 가상 머신 유형을 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 공급 또는 패치 릴리스가 제공되는 경우 콘솔은 버전을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.13.1을 선택하고 9.13.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리스에서 다른 릴리스로 전달되지 않습니다. 예를 들어, 9.13에서 9.14로 전달되지 않습니다.
11. **Azure Marketplace**에서 구독: 콘솔에서 Cloud Volumes ONTAP 의 프로그래밍 방식 배포를 활성화할 수 없는 경우 다음 단계를 따르세요.
12. 기본 스토리지 리소스: 초기 집계에 대한 설정을 선택합니다. 디스크 유형, 각 디스크의 크기, Blob 스토리지에 대한 데이터 계층화를 활성화할지 여부입니다.

    다음 사항에 유의하세요.

- 디스크 크기는 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔이 생성하는 모든 추가 집계에 적용됩니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.

  디스크 크기 선택에 대한 도움말은 다음을 참조하세요."Azure에서 시스템 크기 조정" .

- VNet 내에서 스토리지 계정에 대한 공용 액세스가 비활성화된 경우 Cloud Volumes ONTAP 시스템에서 데이터 계층화를 활성화할 수 없습니다. 자세한 내용은 다음을 참조하세요."보안 그룹 규칙" .
- 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
- 데이터 계층화를 비활성화하면 이후 집계에서 활성화할 수 있습니다.

  "데이터 계층화에 대해 자세히 알아보세요" .

- Cloud Volumes ONTAP 9.15.0P1부터 새로운 고가용성 쌍 배포에 대해 Azure 페이지 Blob이 더 이상 지원되지 않습니다. 현재 기존 고가용성 쌍 배포에서 Azure 페이지 Blob을 사용하는 경우 Edsv4 시리즈 VM 및 Edsv5 시리즈 VM에서 최신 VM 인스턴스 유형으로 마이그레이션할 수 있습니다.

  "Azure에서 지원되는 구성에 대해 자세히 알아보세요." .

13. 쓰기 속도 및 **WORM**:

    a. 원하는 경우 보통 또는 높음 쓰기 속도를 선택하세요.

       "쓰기 속도에 대해 자세히 알아보세요" .

    b. 원하는 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

       이 옵션은 특정 VM 유형에만 사용할 수 있습니다. 지원되는 VM 유형을 알아보려면 다음을 참조하세요."HA 쌍에 대한 라이선스별 지원 구성" .

       Cloud Volumes ONTAP 버전 9.7 이하에서 데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로 되돌리거나 다운그레이드하는 것이 차단됩니다.

    "WORM 스토리지에 대해 자세히 알아보세요" .

    a. WORM 저장소를 활성화하는 경우 보존 기간을 선택하세요.

14. 저장소 및 **WORM**에 대한 보안 통신: Azure 저장소 계정에 HTTPS 연결을 사용할지 여부를 선택하고, 필요한 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

    HTTPS 연결은 Cloud Volumes ONTAP 9.7 HA 쌍에서 Azure 페이지 Blob 스토리지 계정으로 이루어집니다. 이 옵션을 활성화하면 쓰기 성능에 영향을 줄 수 있습니다. 시스템을 만든 후에는 설정을 변경할 수 없습니다.

    "WORM 스토리지에 대해 자세히 알아보세요" .

    데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다.

    "WORM 스토리지에 대해 자세히 알아보세요" .

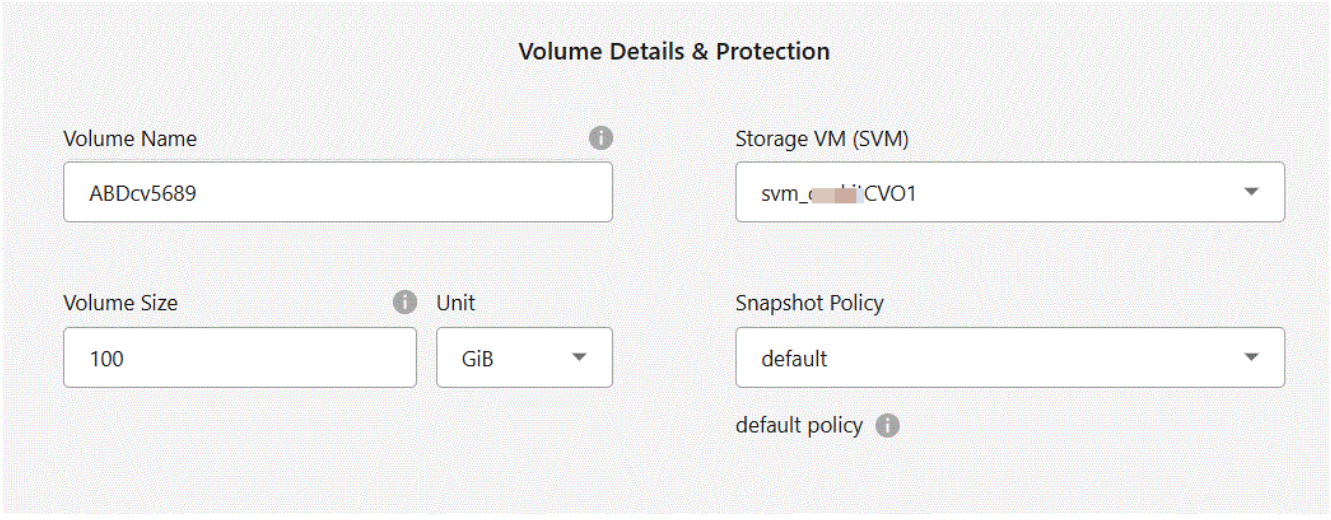
15. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

    "지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝을 활성화하는지 여부에 따라 크게 달라집니다. 씬 프로비저닝을 활성화하면 현재 사용 가능한 물리적 저장소보다 큰 볼륨을 만들 수 있습니다.
액세스 제어(NFS에만 해당)	내보내기 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 콘솔은 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS에만 해당)	이러한 필드를 사용하면 사용자 및 그룹의 공유 액세스 수준(액세스 제어 목록 또는 ACL이라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자나 그룹, 또는 UNIX 사용자나 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사 정책은 NetApp 스냅샷 복사본이 자동으로 생성되는 빈도와 수를 지정합니다. NetApp 스냅샷 복사본은 성능에 영향을 미치지 않고 최소한의 저장 공간만 필요한 특정 시점의 파일 시스템 이미지입니다. 기본 정책을 선택하거나 아무것도 선택하지 않을 수 있습니다. 일시적인 데이터의 경우 '없음'을 선택할 수 있습니다. 예를 들어 Microsoft SQL Server의 경우 tempdb를 선택합니다.
고급 옵션(NFS에만 해당)	볼륨에 대한 NFS 버전을 선택합니다: NFSv3 또는 NFSv4.
이니시에이터 그룹 및 IQN(iSCSI에만 해당)	iSCSI 스토리지 대상은 LUN(논리 단위)이라고 하며 호스트에 표준 블록 장치로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름 테이블이며, 어떤 이니시에이터가 어떤 LUN에 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 컨버지드 네트워크 어댑터(CNA) 또는 전용 호스트 버스 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 정규화된 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후, "IQN을 사용하여 호스트에서 LUN에 연결합니다." .

다음 이미지는 볼륨 생성 마법사의 첫 번째 페이지를 보여줍니다.



16. **CIFS** 설정: CIFS 프로토콜을 선택한 경우 CIFS 서버를 설정합니다.

필드	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인의 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.
도메인에 가입할 수 있는 권한이 있는 자격 증명	AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.
CIFS 서버 NetBIOS 이름	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Cloud Volumes ONTAP 의 AD 서버로 Azure AD Domain Services를 구성하려면 이 필드에 **OU=AADDC Computers** 또는 *OU=AADDC Users*를 입력해야 합니다.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 설명서: Azure AD Domain Services 관리 도메인에서 OU(조직 단위) 만들기"^]
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 대부분의 경우 도메인은 AD 도메인과 동일합니다.
NTP 서버	Active Directory DNS를 사용하여 NTP 서버를 구성하려면 *Active Directory 도메인 사용*을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 를 참조하세요 "NetApp Console 자동화 문서" 자세한 내용은. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

17. 사용 프로필, 디스크 유형 및 계층화 정책: 필요한 경우 스토리지 효율성 기능을 활성화할지 여부를 선택하고 볼륨 계층화 정책을 변경합니다.

    자세한 내용은 다음을 참조하세요."볼륨 사용 프로필을 선택하세요" ,"데이터 계층화 개요" , 그리고 "KB: CVO에서는 어떤 인라인 스토리지 효율성 기능이 지원되나요?"

18. 검토 및 승인: 선택 사항을 검토하고 확인합니다.
    a. 구성에 대한 세부 정보를 검토하세요.
    b. *자세한 정보*를 클릭하여 콘솔에서 구매할 지원 및 Azure 리소스에 대한 세부 정보를 검토하세요.
    c. 이해합니다... 확인란을 선택하세요.
    d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 시스템을 배포합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템 배포 중 문제가 발생하면 실패 메시지를 검토하세요. 시스템을 선택하고 *환경 다시 만들기*를 클릭할 수도 있습니다.

추가 도움말을 보려면 다음으로 이동하세요. "NetApp Cloud Volumes ONTAP 지원" .

당신이 완료한 후

- CIFS 공유를 프로비저닝한 경우 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인합니다.

- 볼륨에 할당량을 적용하려면 ONTAP 시스템 관리자나 ONTAP CLI를 사용하세요.

  할당량을 사용하면 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적할 수 있습니다.

> 배포 프로세스가 완료된 후에는 Azure Portal에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

관련 링크

*"Azure에서 Cloud Volumes ONTAP 구성 계획" *"Azure Marketplace에서 Azure에 Cloud Volumes ONTAP 배포"

Azure 플랫폼 이미지 확인

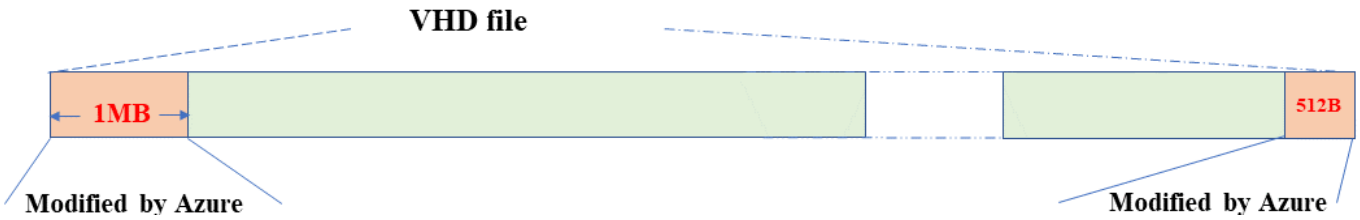
Cloud Volumes ONTAP 에 대한 Azure 마켓플레이스 이미지 검증

Azure 이미지 검증은 향상된 NetApp 보안 요구 사항을 준수합니다. 이미지 파일을 검증하는 것은 간단한 과정입니다. 그러나 Azure 이미지 서명 검증에는 Azure VHD 이미지 파일에 대한 특정 고려 사항이 필요합니다. Azure VHD 이미지 파일은 Azure Marketplace에서 변경되기 때문입니다.

> Azure 이미지 검증은 Cloud Volumes ONTAP 9.15.0 이상에서 지원됩니다.

Azure에서 게시된 VHD 파일 변경

VHD 파일의 시작 부분인 1MB(1048576바이트)와 끝 부분인 512바이트는 Azure에 의해 수정됩니다. NetApp 나머지 VHD 파일에 서명합니다.



이 예에서 VHD 파일의 크기는 10GB입니다. NetApp 에서 서명한 부분은 녹색으로 표시되어 있습니다(10GB - 1MB - 512바이트).

관련 링크

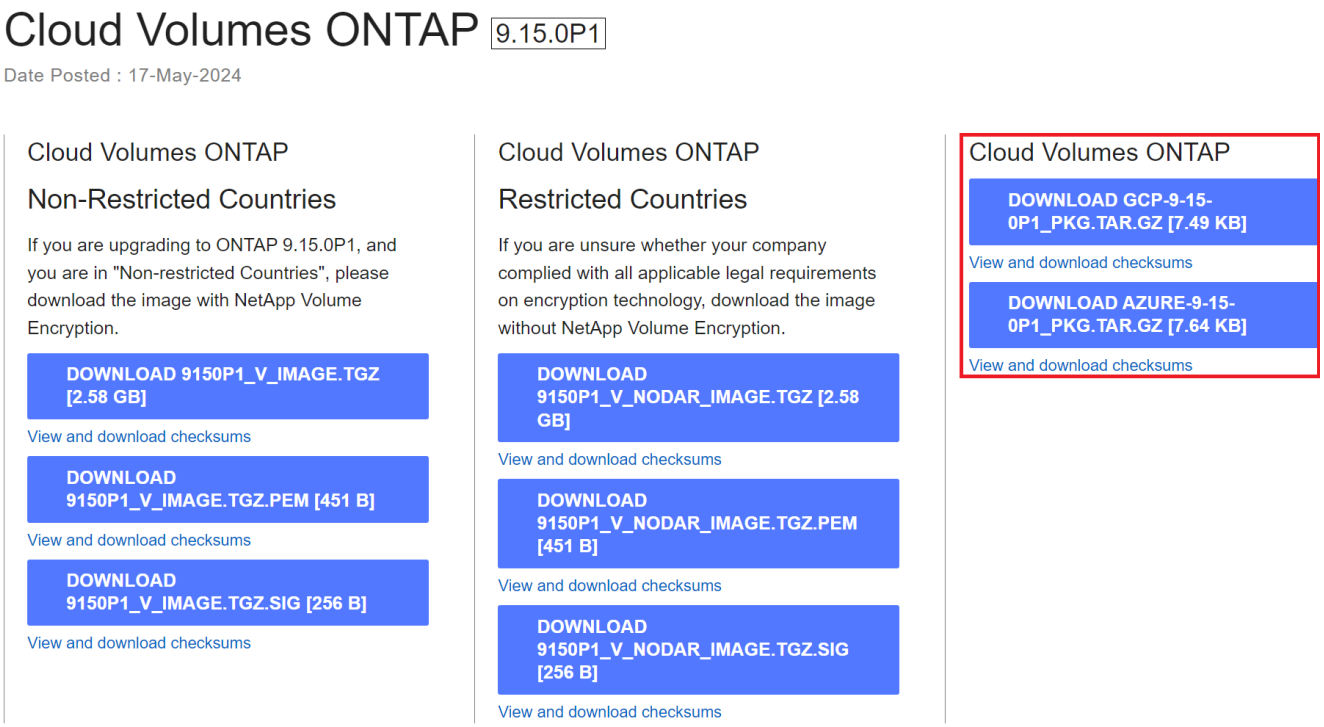
- "페이지 폴트 블로그: OpenSSL을 사용하여 서명하고 확인하는 방법"
- "Azure Marketplace 이미지를 사용하여 Azure Stack Edge Pro GPU용 VM 이미지 만들기 | Microsoft Learn"
- "Azure CLI를 사용하여 관리 디스크를 저장소 계정으로 내보내기/복사 | Microsoft Learn"
- "Azure Cloud Shell 빠른 시작 - Bash | Microsoft Learn"
- "Azure CLI 설치 방법 | Microsoft Learn"
- "az 스토리지 BLOB 복사 | Microsoft Learn"
- "Azure CLI로 Sign in - 로그인 및 인증 | Microsoft Learn"

Azure 이미지 파일은 다음에서 다운로드할 수 있습니다. "NetApp 지원 사이트" .

tar.gz 파일에는 이미지 서명 검증에 필요한 파일이 포함되어 있습니다. *tar.gz* 파일과 함께 이미지에 대한 *checksum* 파일도 다운로드해야 합니다. 체크섬 파일에는 다음이 포함됩니다. `md5` 그리고 `sha256` *tar.gz* 파일의 체크섬.

단계

1. 로 가다 "NetApp 지원 사이트의 Cloud Volumes ONTAP 제품 페이지" 다운로드 섹션에서 필요한 소프트웨어 버전을 다운로드하세요.
2. Cloud Volumes ONTAP 다운로드 페이지에서 Azure 이미지에 대한 다운로드 가능한 파일을 클릭하고 *tar.gz* 파일을 다운로드합니다.



3. Linux에서 실행 `md5sum AZURE-<version>_PKG.TAR.GZ` .

   macOS에서는 다음을 실행합니다. `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. 다음을 확인하십시오. `md5sum` 그리고 `sha256sum` 값이 다운로드한 Azure 이미지의 값과 일치합니다.
5. Linux 및 macOS에서는 다음을 사용하여 *tar.gz* 파일을 추출합니다. `tar -xzf` 명령.

   추출된 *tar.gz* 파일에는 다이제스트(*.sig*) 파일, 공개 키 인증서(*.pem*) 파일, 체인 인증서(*.pem*) 파일이 포함되어 있습니다.

   tar.gz 파일을 추출한 후의 출력 예**:**

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Azure Marketplace에서 Cloud Volumes ONTAP 용 VHD 이미지 내보내기

VHD 이미지가 Azure 클라우드에 게시되면 더 이상 NetApp 에서 관리되지 않습니다. 대신, 게시된 이미지는 Azure Marketplace에 배치됩니다. 이미지가 Azure 마켓플레이스에 스테이징되어 게시되면 Azure는 VHD의 시작 부분에서 1MB, 끝 부분에서 512바이트를 수정합니다. VHD 파일의 서명을 확인하려면 Azure 마켓플레이스에서 Azure가 수정한 VHD 이미지를 내보내야 합니다.

시작하기 전에

시스템에 Azure CLI가 설치되어 있는지, 아니면 Azure Portal을 통해 Azure Cloud Shell을 사용할 수 있는지 확인하세요. Azure CLI를 설치하는 방법에 대한 자세한 내용은 다음을 참조하세요. "Microsoft 설명서: Azure CLI 설치 방법" .

단계

1. *version_readme* 파일의 내용을 사용하여 시스템의 Cloud Volumes ONTAP 버전을 Azure Marketplace 이미지 버전에 매핑합니다. Cloud Volumes ONTAP 버전은 다음과 같이 표현됩니다. `buildname` Azure Marketplace 이미지 버전은 다음과 같이 표현됩니다. `version` 버전 매핑에서.

   다음 예에서는 Cloud Volumes ONTAP 버전 `9.15.0P1` Azure Marketplace 이미지 버전에 매핑됨 `9150.01000024.05090105` . 이 Azure 마켓플레이스 이미지 버전은 나중에 이미지 URN을 설정하는 데 사용됩니다.

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. VM을 만들려는 지역을 식별합니다. 지역 이름은 값으로 사용됩니다. `locName` 마켓플레이스 이미지의 URN을 설정할 때 변수입니다. 사용 가능한 지역을 나열하려면 다음 명령을 실행하세요.

   ```
   az account list-locations -o table
   ```

   이 표에서는 지역 이름이 다음과 같이 나타납니다. `Name` 필드.

```
$ az account list-locations -o table
DisplayName               Name                 RegionalDisplayName
------------------------  -------------------
-------------------------------------
East US                   eastus               (US) East US
East US 2                 eastus2              (US) East US 2
South Central US          southcentralus       (US) South Central US
...
```

3. 아래 표에서 해당 Cloud Volumes ONTAP 버전과 VM 배포 유형에 대한 SKU 이름을 검토하세요. SKU 이름은 값으로 사용됩니다. `skuName` 마켓플레이스 이미지의 URN을 설정할 때 변수입니다.

   예를 들어, Cloud Volumes ONTAP 9.15.0을 사용한 모든 단일 노드 배포는 다음을 사용해야 합니다. `ontap_cloud_byol` SKU 이름으로.

* Cloud Volumes ONTAP 버전*	**VM** 배포를 통해	**SKU** 이름
9.17.1 이상	Azure 마켓플레이스	ontap_cloud_direct_gen2
9.17.1 이상	NetApp Console	ontap_cloud_gen2
9.16.1	Azure 마켓플레이스	온탭_클라우드_다이렉트
9.16.1	콘솔	온탭_클라우드
9.15.1	콘솔	온탭_클라우드
9.15.0	콘솔, 단일 노드 배포	온탭_클라우드_바이올
9.15.0	콘솔, 고가용성(HA) 배포	온탑_클라우드_비올_하

4. ONTAP 버전과 Azure 마켓플레이스 이미지를 매핑한 후 Azure Cloud Shell 또는 Azure CLI를 사용하여 Azure 마켓플레이스에서 VHD 파일을 내보냅니다.

Linux에서 **Azure Cloud Shell**을 사용하여 **VHD** 파일 내보내기

Azure Cloud Shell에서 마켓플레이스 이미지를 VHD 파일(예: *9150.01000024.05090105.vhd*)로 내보내고 로컬 Linux 시스템에 다운로드합니다. Azure Marketplace에서 VHD 이미지를 가져오려면 다음 단계를 수행하세요.

단계

1. 마켓플레이스 이미지의 URN 및 기타 매개변수를 설정합니다. URN 형식은 다음과 같습니다. `<publisher>:<offer>:<sku>:<version>` . 선택적으로 NetApp 마켓플레이스 이미지를 나열하여 올바른 이미지 버전을 확인할 수 있습니다.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. 일치하는 이미지 버전으로 마켓플레이스 이미지에서 새 관리 디스크를 만듭니다.

```
PS /home/user1> $diskName = “9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = “fnf1”
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. 관리 디스크에서 Azure Storage로 VHD 파일을 내보냅니다. 적절한 액세스 수준으로 컨테이너를 만듭니다. 이 예에서 우리는 다음과 같은 이름의 컨테이너를 사용했습니다. `vm-images` ~와 함께 `Container` 접근 수준. Azure Portal에서 저장소 계정 액세스 키를 가져옵니다. 저장소 계정 **> *examplesaname* >** 액세스 키 **> *key1* > *key* >** 표시 **> <복사>**

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. 생성된 이미지를 Linux 시스템에 다운로드합니다. 사용하다 `wget` VHD 파일을 다운로드하는 명령:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

URL은 표준 형식을 따릅니다. 자동화를 위해 아래와 같이 URL 문자열을 파생시킬 수 있습니다. 또는 Azure CLI를 사용할 수 있습니다. `az` URL을 가져오는 명령입니다. URL 예시:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. 관리되는 디스크 정리

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Linux에서 **Azure CLI**를 사용하여 **VHD** 파일 내보내기

로컬 Linux 시스템에서 Azure CLI를 사용하여 마켓플레이스 이미지를 VHD 파일로 내보냅니다.

단계

1. Azure CLI에 로그인하고 마켓플레이스 이미지를 나열합니다.

```
% az login --use-device-code
```

2. 로그인하려면 웹 브라우저를 사용하여 페이지를 엽니다. https://microsoft.com/devicelogin 인증코드를 입력하세요.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. 마켓플레이스 이미지에서 일치하는 이미지 버전으로 새로운 관리 디스크를 만듭니다.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
```

프로세스를 자동화하려면 표준 출력에서 SAS를 추출해야 합니다. 자세한 내용은 해당 문서를 참조하세요.

4. 관리 디스크에서 VHD 파일을 내보냅니다.

   a. 적절한 액세스 수준으로 컨테이너를 만듭니다. 이 예에서는 컨테이너라는 이름이 있습니다. `vm-images` ~와 함께 `Container` 접근 수준이 사용됩니다.

   b. Azure Portal에서 저장소 계정 액세스 키를 가져옵니다. 저장소 계정 **> *examplesaname* >** 액세스 키 **> *key1* > *key* >** 표시 **> <복사>**

      또한 다음을 사용할 수도 있습니다. `az` 이 단계에 대한 명령입니다.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Blob 복사본의 상태를 확인하세요.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. 생성된 이미지를 Linux 서버로 다운로드합니다.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

URL은 표준 형식을 따릅니다. 자동화를 위해 아래와 같이 URL 문자열을 파생시킬 수 있습니다. 또는 Azure CLI를 사용할 수 있습니다. `az` URL을 가져오는 명령입니다. URL 예시:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. 관리되는 디스크 정리

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

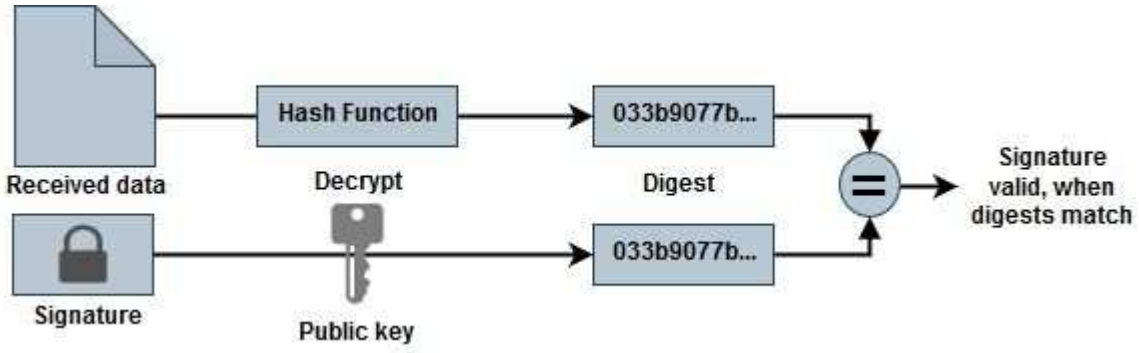
파일 서명 확인

Cloud Volumes ONTAP 에 대한 **Azure** 마켓플레이스 이미지 서명 확인

Azure 이미지 검증 프로세스는 VHD 파일의 시작 부분에서 1MB, 끝 부분에서 512바이트를 제거한 다음 해시 함수를 적용하여 다이제스트 파일을 생성합니다. 서명 절차를 일치시키기 위해 해싱에는 _sha256_이 사용됩니다.

파일 서명 검증 워크플로 요약

다음은 파일 서명 검증 워크플로 프로세스에 대한 개요입니다.



- Azure 이미지를 다운로드합니다. "NetApp 지원 사이트" 그리고 다이제스트(.sig) 파일, 공개 키 인증서(.pem) 파일, 체인 인증서(.pem) 파일을 추출합니다. . "Azure 이미지 다이제스트 파일 다운로드" 자세한 내용은.
- 신뢰 사슬의 검증.
- 공개 키 인증서(.pem)에서 공개 키(.pub)를 추출합니다.
- 추출된 공개 키를 사용하여 다이제스트 파일을 해독합니다.
- 이미지 파일에서 시작 부분 1MB와 끝 부분 512바이트를 제거한 후 생성된 임시 파일의 새로 생성된 다이제스트와 결과를 비교합니다. 이 단계는 OpenSSL 명령줄 도구를 사용하여 수행됩니다. OpenSSL CLI 도구는 파일 일치에 성공하거나 실패할 경우 적절한 메시지를 표시합니다.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Linux에서 **Cloud Volumes ONTAP** 에 대한 **Azure** 마켓플레이스 이미지 서명 확인

Linux에서 내보낸 VHD 파일 서명을 검증하는 작업에는 신뢰 체인 검증, 파일 편집, 서명 검증이 포함됩니다.

단계

1. Azure 이미지 파일을 다운로드하세요. "NetApp 지원 사이트" 그리고 다이제스트(.sig) 파일, 공개 키 인증서(.pem) 파일, 체인 인증서(.pem) 파일을 추출합니다.

   참조하다 "Azure 이미지 다이제스트 파일 다운로드" 자세한 내용은.

2. 신뢰 사슬을 확인하세요.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. VHD 파일의 시작 부분에서 1MB(1,048,576바이트)를 제거하고 끝 부분에서 512바이트를 제거합니다. 사용시 `tail` , 그 `-c +K` 이 옵션은 파일의 K번째 바이트에서 바이트를 생성합니다. 따라서 1048577을 전달합니다. `tail -c` .

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. OpenSSL을 사용하여 인증서에서 공개 키를 추출하고, 스트립된 파일(sign.tmp)을 서명 파일과 공개 키로 검증합니다.

   명령 프롬프트는 검증 결과에 따라 성공 또는 실패를 나타내는 메시지를 표시합니다.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 작업 공간을 정리하세요.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

macOS에서 **Cloud Volumes ONTAP** 대한 **Azure** 마켓플레이스 이미지 서명 확인

Linux에서 내보낸 VHD 파일 서명을 검증하는 작업에는 신뢰 체인 검증, 파일 편집, 서명 검증이 포함됩니다.

단계

1. Azure 이미지 파일을 다운로드하세요. "NetApp 지원 사이트" 그리고 다이제스트(.sig) 파일, 공개 키 인증서(.pem) 파일, 체인 인증서(.pem) 파일을 추출합니다.

   참조하다 "Azure 이미지 다이제스트 파일 다운로드" 자세한 내용은.

2. 신뢰 사슬을 확인하세요.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. VHD 파일의 시작 부분에서 1MB(1,048,576바이트)를 제거하고 끝 부분에서 512바이트를 제거합니다. 사용시 `tail` , 그 `-c +K` 이 옵션은 파일의 K번째 바이트에서 바이트를 생성합니다. 따라서 1048577을 전달합니다. `tail -c` . macOS에서는 tail 명령을 완료하는 데 약 10분이 걸릴 수 있습니다.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. OpenSSL을 사용하여 인증서에서 공개 키를 추출하고, 스트립된 파일(sign.tmp)을 서명 파일과 공개 키로 검증합니다. 명령 프롬프트는 검증 결과에 따라 성공 또는 실패를 나타내는 메시지를 표시합니다.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 작업 공간을 정리하세요.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Azure Marketplace에서 Cloud Volumes ONTAP 배포

Azure Marketplace 직접 배포를 사용하면 Cloud Volumes ONTAP 빠르고 쉽게 배포할 수 있습니다. Azure 마켓플레이스에서 몇 번의 클릭만으로 Cloud Volumes ONTAP 빠르게 배포하고 사용자 환경에서 핵심 기능과 성능을 살펴볼 수 있습니다.

이 제안에 대한 자세한 내용은 다음을 참조하세요."NetApp Console 과 마켓플레이스에서 Cloud Volumes ONTAP 제품에 대해 알아보세요." .

이 작업에 관하여

Azure Marketplace 직접 배포를 사용하여 배포된 Cloud Volumes ONTAP 시스템은 다음과 같은 속성을 갖습니다. Azure 마켓플레이스를 통해 배포된 독립 실행형 인스턴스의 기능은 NetApp Console 에서 검색될 때 변경됩니다.

- 최신 Cloud Volumes ONTAP 버전(9.16.1 이상).
- 프로비저닝 용량이 500GiB로 제한된 Cloud Volumes ONTAP 의 무료 라이선스입니다. 이 라이선스에는 NetApp 지원이 포함되지 않으며 만료 날짜도 없습니다.
- 단일 가용성 영역(AZ)에서 고가용성(HA) 모드로 구성된 두 개의 노드는 기본 일련 번호로 제공됩니다. 스토리지 가상 머신(스토리지 VM)은 다음에 배포됩니다."유연한 오케스트레이션 모드" .
- 기본적으로 생성된 인스턴스에 대한 집계입니다.
- 500GiB 프로비저닝 용량의 프리미엄 SSD v2 관리 디스크와 루트 디스크, 데이터 디스크.
- NFS, CIFS, iSCSI 및 NVMe/TCP 데이터 서비스를 갖춘 하나의 데이터 저장 VM이 배포되었습니다. 추가 데이터 저장소 VM을 추가할 수 없습니다.
- NFS, CIFS(SMB), iSCSI, Autonomous Ransomware Protection(ARP), SnapLock 및 SnapMirror 대한 라이센스가 설치되었습니다.
- "ONTAP 온도 민감 저장 효율성(TSSE)", 볼륨 암호화 및 외부 키 관리가 기본적으로 활성화되어 있습니다.
- 다음 기능은 지원되지 않습니다.

- FabricPool 계층화
- 스토리지 VM 유형 변경
- 빠른 쓰기 모드

시작하기 전에

- 유효한 Azure Marketplace 구독이 있는지 확인하세요.
- 네트워킹 요구 사항을 충족하는지 확인하세요."단일 AZ에 HA 배포" Azure에서. "Cloud Volumes ONTAP 에 대한 Azure 네트워킹 설정" .
- Cloud Volumes ONTAP 배포하려면 다음 Azure 역할 중 하나가 할당되어야 합니다.
  - 그만큼 `contributor` 기본 권한이 있는 역할입니다. 자세한 내용은 다음을 참조하세요. "Microsoft Azure 설명서: Azure 기본 제공 역할" .
  - 다음 권한이 있는 사용자 지정 RBAC 역할입니다. 자세한 내용은 다음을 참조하세요. "Azure 설명서: Azure 사용자 지정 역할" .

```
"사용 권한": [ { "작업": [ "Microsoft.AAD/등록/작업", "Microsoft.Resources/구독/리소스그룹/쓰기",
"Microsoft.Network/로드밸런서/쓰기", "Microsoft.ClassicCompute/virtualMachines/쓰기",
"Microsoft.Compute/capacityReservationGroups/배포/작업",
"Microsoft.ClassicCompute/virtualMachines/네트워크인터페이스/연관된네트워크보안그룹/쓰기",
"Microsoft.Network/네트워크인터페이스/쓰기", "Microsoft.Compute/virtualMachines/쓰기",
"Microsoft.Compute/virtualMachines/확장/쓰기", "Microsoft.Resources/배포/검증/작업",
"Microsoft.Resources/구독/리소스그룹/읽기", "Microsoft.Network/virtualNetworks/쓰기",
"Microsoft.Network/virtualNetworks/read", "Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Compute/disks/write",
"Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Resources/deployments/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write" ], "notActions": [], "dataActions": [],
"notDataActions": [] } ]
```

> 구독에 리소스 공급자 "Microsoft.storage"를 등록한 경우에는 필요하지 않습니다. `Microsoft.AAD/register/action` 허가. 자세한 내용은 다음을 참조하세요. "Azure 설명서: 저장소에 대한 Azure 권한" .

단계

1. Azure Marketplace 사이트에서 NetApp 제품을 검색합니다.
2. * NetApp Cloud Volumes ONTAP 직접*을 선택하세요.
3. *만들기*를 클릭하여 배포 마법사를 시작합니다.
4. 플랜을 선택하세요. 계획 목록에는 일반적으로 Cloud Volumes ONTAP 의 최신 릴리스가 표시됩니다.
5. 기본 탭에서 다음 세부 정보를 제공합니다.
   - 구독: 구독을 선택하세요. 배포는 구독 번호에 연결됩니다.
   - 리소스 그룹: 기존 리소스 그룹을 사용하거나 새 리소스 그룹을 만듭니다. 리소스 그룹은 Cloud Volumes ONTAP 시스템의 단일 그룹 내에서 디스크 및 스토리지 VM과 같은 모든 리소스를 할당하는 데 도움이 됩니다.
   - 지역: 단일 AZ에서 Azure HA 배포를 지원하는 지역을 선택하세요. 목록에서는 사용 가능한 지역만 볼 수 있습니다.

- 크기: 지원되는 Premium SSD v2 관리 디스크에 대한 스토리지 VM 크기를 선택하세요.
- 지역: 선택한 지역의 지역을 선택하세요.
- 관리자 비밀번호: 비밀번호를 설정하세요. 배포 후 이 관리자 비밀번호를 사용하여 시스템에 로그인합니다.
- 비밀번호 확인: 확인을 위해 동일한 비밀번호를 다시 입력하세요.
  - 네트워크 탭에서 가상 네트워크와 서브넷을 추가하거나 목록에서 선택합니다.

    Microsoft Azure 제한 사항을 준수하려면 새 가상 네트워크를 설정할 때 새 서브넷을 만들어야 합니다. 마찬가지로, 기존 네트워크를 선택하는 경우 기존 서브넷을 선택해야 합니다.

  - 미리 정의된 네트워크 보안 그룹을 선택하려면 *예*를 선택하세요. 미리 정의된 Azure 네트워크 보안 그룹에 필요한 트래픽 규칙을 할당하려면 *아니요*를 선택합니다. 자세한 내용은 다음을 참조하세요. "Azure에 대한 보안 그룹 규칙" .
  - 고급 탭에서 이 배포에 필요한 두 가지 Azure 기능이 설정되었는지 확인합니다. 참조하다"Cloud Volumes ONTAP 단일 AZ 배포를 위한 Azure 기능 활성화" 그리고"Azure에서 Cloud Volumes ONTAP 에 대해 고가용성 모드 활성화" .
  - 태그 탭에서 리소스 또는 리소스 그룹에 대한 이름과 값 쌍을 정의할 수 있습니다.
  - 검토 + 생성 탭에서 세부 정보를 검토하고 배포를 시작합니다.

당신이 완료한 후

배포 진행 상황을 보려면 알림 아이콘을 선택하세요. Cloud Volumes ONTAP 이 배포되면 작업을 위해 나열된 스토리지 VM을 볼 수 있습니다.

접근이 가능해지면 ONTAP System Manager나 ONTAP CLI를 사용하여 설정한 관리자 자격 증명으로 스토리지 VM에 로그인합니다. 그 후에는 볼륨, LUN 또는 공유를 생성하고 Cloud Volumes ONTAP 의 스토리지 기능을 활용할 수 있습니다.

배포 문제 해결

Azure 마켓플레이스를 통해 직접 배포된 Cloud Volumes ONTAP 시스템에는 NetApp 의 지원이 포함되지 않습니다. 배포 중에 문제가 발생하면 독립적으로 문제를 해결하고 해결할 수 있습니다.

단계

1. Azure Marketplace 사이트에서 *부팅 진단 > 직렬 로그*로 이동합니다.
2. 직렬 로그를 다운로드하고 조사하세요.
3. 문제 해결을 위해서는 제품 설명서와 지식 기반(KB) 문서를 참조하세요.
   - "Azure 마켓플레이스 문서"
   - "NetApp 문서"
   - "NetApp KB 문서"

콘솔에서 배포된 시스템을 찾아보세요

Azure Marketplace 직접 배포를 사용하여 배포한 Cloud Volumes ONTAP 시스템을 검색하고 콘솔의 시스템 페이지에서 관리할 수 있습니다. 콘솔 에이전트는 시스템을 검색하고, 시스템을 추가하고, 필요한 라이선스를 적용하고, 이러한 시스템에 대해 콘솔의 모든 기능을 잠금 해제합니다. PSSD v2 관리형 디스크가 있는 단일 AZ의 원래 HA

구성은 유지되며, 시스템은 원래 배포와 동일한 Azure 구독 및 리소스 그룹에 등록됩니다.

이 작업에 관하여

Azure Marketplace 직접 배포를 사용하여 배포된 Cloud Volumes ONTAP 시스템을 검색하면 콘솔 에이전트는 다음 작업을 수행합니다.

- 발견된 시스템의 무료 라이센스를 일반적인 용량 기반으로 대체합니다."프리미엄 라이선스" .
- 배포된 시스템의 기존 기능을 유지하고, 데이터 보호, 데이터 관리, 보안 기능 등 콘솔의 추가 기능을 추가합니다.
- 노드에 설치된 라이선스를 NFS, CIFS(SMB), iSCSI, ARP, SnapLock 및 SnapMirror 에 대한 새로운 ONTAP 라이선스로 교체합니다.
- 일반 노드 일련 번호를 고유한 일련 번호로 변환합니다.
- 필요에 따라 리소스에 새로운 시스템 태그를 할당합니다.
- 인스턴스의 동적 IP 주소를 정적 IP 주소로 변환합니다.
- 기능을 활성화합니다"FabricPool 계층화" ,"AutoSupport" , 그리고"한 번 쓰고 여러 번 읽기" 배포된 시스템에 (WORM) 저장소를 설치합니다. 필요할 때 콘솔에서 이러한 기능을 활성화할 수 있습니다.
- 인스턴스를 검색하는 데 사용된 NSS 계정에 인스턴스를 등록합니다.
- 용량 관리 기능을 활성화합니다."자동 및 수동 모드" 발견된 시스템에 대해서.

시작하기 전에

Azure Marketplace에서 배포가 완료되었는지 확인하세요. 콘솔 에이전트는 배포가 완료되고 검색이 가능한 경우에만 시스템을 검색할 수 있습니다.

단계

콘솔에서는 기존 시스템을 검색하기 위한 표준 절차를 따릅니다. "콘솔에 기존 Cloud Volumes ONTAP 시스템 추가" .

검색하는 동안 실패 메시지가 표시될 수 있지만 검색 프로세스가 완료될 때까지 무시할 수 있습니다. 검색 중에는 Azure Marketplace 포털에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예상치 못한 시스템 동작이 발생할 수 있습니다.

당신이 완료한 후

검색이 완료되면 콘솔의 시스템 페이지에 나열된 시스템을 볼 수 있습니다. 다음과 같은 다양한 관리 작업을 수행할 수 있습니다."집계 확장" ,"볼륨 추가" ,"추가 스토리지 VM 프로비저닝" , 그리고"인스턴스 유형 변경" .

관련 링크

저장소 생성에 대한 자세한 내용은 ONTAP 설명서를 참조하세요.

- "NFS용 볼륨 생성"
- "iSCSI에 대한 LUN 생성"
- "CIFS에 대한 공유 생성"

Google Cloud에서 시작하기

Google Cloud에서 Cloud Volumes ONTAP 빠르게 시작하세요

몇 단계만 거치면 Google Cloud에서 Cloud Volumes ONTAP 시작할 수 있습니다.

콘솔 에이전트 만들기

만약 당신이 없다면 "콘솔 에이전트" 하지만, 하나는 만들어야 합니다. "Google Cloud에서 콘솔 에이전트를 만드는 방법을 알아보세요."

인터넷 접속이 불가능한 서브넷에 Cloud Volumes ONTAP 배포하려면 콘솔 에이전트를 수동으로 설치하고 해당 콘솔 에이전트에서 실행 중인 NetApp Console 에 액세스해야 합니다. "인터넷 접속이 불가능한 위치에 콘솔 에이전트를 수동으로 설치하는 방법을 알아보세요."

구성을 계획하세요

콘솔은 사용자의 작업 부하 요구 사항에 맞는 미리 구성된 패키지를 제공하거나 사용자가 직접 구성을 만들 수도 있습니다. 원하는 구성을 선택하는 경우, 사용 가능한 옵션을 이해해야 합니다.

"구성 계획에 대해 자세히 알아보세요" .

네트워킹을 설정하세요

1. VPC와 서브넷이 콘솔 에이전트와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인하세요.
2. 데이터 계층화를 활성화하려는 경우 "Private Google Access를 위해 Cloud Volumes ONTAP 서브넷을 구성합니다." .
3. HA 쌍을 배포하는 경우 각각 자체 서브넷이 있는 4개의 VPC가 있는지 확인하세요.
4. 공유 VPC를 사용하는 경우 콘솔 에이전트 서비스 계정에 *Compute Network User* 역할을 제공합니다.
5. NetApp AutoSupport 에 대해 대상 VPC에서 아웃바운드 인터넷 액세스를 활성화합니다.

   인터넷 접속이 불가능한 위치에 Cloud Volumes ONTAP 배포하는 경우 이 단계는 필요하지 않습니다.

"네트워킹 요구 사항에 대해 자세히 알아보세요" .

서비스 계정 설정

Cloud Volumes ONTAP 두 가지 목적으로 Google Cloud 서비스 계정이 필요합니다. 첫 번째는 활성화할 때입니다. "데이터 계층화" Google Cloud의 저렴한 객체 스토리지에 콜드 데이터를 계층화합니다. 두 번째는 다음을 활성화할 때입니다. "NetApp Backup and Recovery" 저렴한 개체 스토리지에 볼륨을 백업합니다.

하나의 서비스 계정을 설정하여 두 가지 목적으로 모두 사용할 수 있습니다. 서비스 계정에는 저장소 관리자 역할이 있어야 합니다.

"단계별 지침을 읽어보세요" .

Google Cloud API 활성화

"프로젝트에서 Google Cloud API 활성화". "이러한 API"콘솔 에이전트를 생성하는 과정에서 이미 활성화했을 수도 있는 이러한 기능은 Google Cloud에 Cloud Volumes ONTAP을 배포하는 데 필요합니다.

6 콘솔을 사용하여 **Cloud Volumes ONTAP** 실행

*시스템 추가*를 클릭하고 배포하려는 시스템 유형을 선택한 다음 마법사의 단계를 완료합니다. "단계별 지침을 읽어보세요" .

관련 링크

- "콘솔 에이전트 생성"
- "Linux 호스트에 콘솔 에이전트 소프트웨어 설치"
- "콘솔 에이전트에 대한 Google Cloud 권한"

Google Cloud에서 **Cloud Volumes ONTAP** 구성을 계획하세요.

Google Cloud에 Cloud Volumes ONTAP 배포하는 경우 워크로드 요구 사항에 맞는 미리 구성된 시스템을 선택하거나 고유한 구성을 만들 수 있습니다. 원하는 구성을 선택하는 경우, 사용 가능한 옵션을 이해해야 합니다.

Cloud Volumes ONTAP 라이선스를 선택하세요

Cloud Volumes ONTAP 에는 여러 가지 라이선싱 옵션이 제공됩니다. 각 옵션을 통해 귀하의 필요에 맞는 소비 모델을 선택할 수 있습니다.

- "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요"
- "라이선싱 설정 방법 알아보기"

지원되는 지역을 선택하세요

Cloud Volumes ONTAP 대부분의 Google Cloud 지역에서 지원됩니다. "지원되는 지역의 전체 목록 보기" .

지원되는 머신 유형을 선택하세요

Cloud Volumes ONTAP 선택한 라이선스 유형에 따라 여러 가지 머신 유형을 지원합니다.

"Google Cloud에서 Cloud Volumes ONTAP에 대해 지원되는 구성"

저장 한도 이해하기

Cloud Volumes ONTAP 시스템의 원시 용량 제한은 라이선스에 따라 결정됩니다. 추가적인 제한은 골재와 부피의 크기에 영향을 미칩니다. 구성을 계획할 때 이러한 제한 사항을 알고 있어야 합니다.

"Google Cloud의 Cloud Volumes ONTAP 스토리지 제한 사항"

Google Cloud에서 시스템 크기 조정

Cloud Volumes ONTAP 시스템의 크기를 조정하면 성능 및 용량 요구 사항을 충족하는 데 도움이 될 수 있습니다. 머신 유형, 디스크 유형 및 디스크 크기를 선택할 때 몇 가지 핵심 사항을 알아야 합니다.

기계 유형

지원되는 기계 유형을 확인하세요. "Cloud Volumes ONTAP 릴리스 노트" 그런 다음 Google에서 지원되는 각 기기 유형에 대한 세부 정보를 검토합니다. 머신 유형에 맞는 vCPU 수와 메모리에 맞게 워크로드 요구 사항을 조정하세요. 각 CPU 코어가 네트워킹 성능을 향상시킨다는 점에 유의하세요.

자세한 내용은 다음을 참조하세요.

- "Google Cloud 문서: N1 표준 머신 유형"
- "Google Cloud 문서: 성능"

디스크 유형

Cloud Volumes ONTAP 에 대한 볼륨을 생성할 때 Cloud Volumes ONTAP 디스크에 사용하는 기본 클라우드 스토리지를 선택해야 합니다. 디스크 유형은 다음 중 하나일 수 있습니다.

- 영역별 *SSD* 영구 디스크: SSD 영구 디스크는 높은 속도의 무작위 IOPS가 필요한 워크로드에 가장 적합합니다.
- 영역별 균형 지속 디스크: 이러한 SSD는 GB당 더 낮은 IOPS를 제공하여 성능과 비용의 균형을 맞춥니다.
- 영역별 표준 영구 디스크 : 표준 영구 디스크는 경제적이며 순차적 읽기/쓰기 작업을 처리할 수 있습니다.

  자세한 내용은 다음을 참조하세요. "Google Cloud 문서: 영역별 영구 디스크(표준 및 SSD)" .

디스크 크기

Cloud Volumes ONTAP 시스템을 배포할 때 초기 디스크 크기를 선택해야 합니다. 그 후에는 NetApp Console 사용하여 시스템 용량을 관리할 수 있지만 직접 집계를 구축하려는 경우 다음 사항에 유의하세요.

- 집계된 모든 디스크의 크기는 동일해야 합니다.
- 성능을 고려하면서 필요한 공간을 결정하세요.
- 영구 디스크의 성능은 디스크 크기와 시스템에서 사용 가능한 vCPU 수에 따라 자동으로 확장됩니다.

  자세한 내용은 다음을 참조하세요.

  - "Google Cloud 문서: 영역별 영구 디스크(표준 및 SSD)"
  - "Google Cloud 설명서: 영구 디스크 및 로컬 SSD 성능 최적화"

기본 시스템 디스크 보기

사용자 데이터 저장 외에도 콘솔은 Cloud Volumes ONTAP 시스템 데이터(부팅 데이터, 루트 데이터, 코어 데이터 및 NVRAM)를 위한 클라우드 스토리지도 구매합니다. 계획을 세우려면 Cloud Volumes ONTAP 배포하기 전에 이러한 세부 정보를 검토하는 것이 도움이 될 수 있습니다.

- "Google Cloud에서 Cloud Volumes ONTAP 시스템 데이터의 기본 디스크 보기" .
- "Google Cloud 문서: Cloud Quotas 개요"

  Google Cloud Compute Engine은 리소스 사용에 할당량을 적용하므로 Cloud Volumes ONTAP 배포하기 전에 한도에 도달하지 않았는지 확인해야 합니다.

콘솔 에이전트에도 시스템 디스크가 필요합니다. "콘솔 에이전트의 기본 구성에 대한 세부 정보 보기" .

네트워킹 정보 수집

Google Cloud에 Cloud Volumes ONTAP을 배포할 때 가상 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

단일 노드 시스템에 대한 네트워크 정보

Google Cloud 정보	당신의 가치
지역	
존	
VPC 네트워크	
서브넷	
방화벽 정책(자체 방화벽 정책을 사용하는 경우)	

여러 영역의 **HA** 쌍에 대한 네트워크 정보

Google Cloud 정보	당신의 가치
지역	
노드 1의 영역	
노드 2의 영역	
중재자를 위한 구역	
VPC-0 및 서브넷	
VPC-1 및 서브넷	
VPC-2 및 서브넷	
VPC-3 및 서브넷	
방화벽 정책(자체 방화벽 정책을 사용하는 경우)	

단일 존의 **HA** 쌍에 대한 네트워크 정보

Google Cloud 정보	당신의 가치
지역	
존	
VPC-0 및 서브넷	
VPC-1 및 서브넷	
VPC-2 및 서브넷	
VPC-3 및 서브넷	
방화벽 정책(자체 방화벽 정책을 사용하는 경우)	

쓰기 속도를 선택하세요

콘솔을 사용하면 Google Cloud의 고가용성(HA) 쌍을 제외하고 Cloud Volumes ONTAP 에 대한 쓰기 속도 설정을 선택할 수 있습니다. 쓰기 속도를 선택하기 전에 일반 설정과 높은 설정의 차이점, 높은 쓰기 속도를 사용할 때의 위험과 권장 사항을 이해해야 합니다. "쓰기 속도에 대해 자세히 알아보세요" .

볼륨 사용 프로필을 선택하세요

ONTAP 에는 필요한 총 저장 용량을 줄일 수 있는 여러 가지 저장 효율성 기능이 포함되어 있습니다. 콘솔에서 볼륨을 생성할 때 이러한 기능을 활성화하는 프로필이나 비활성화하는 프로필을 선택할 수 있습니다. 어떤 프로필을 사용할지 결정하는 데 도움이 되도록 이러한 기능에 대해 자세히 알아보세요.

NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

씬 프로비저닝

실제 물리적 스토리지 풀에 있는 것보다 더 많은 논리적 스토리지를 호스트나 사용자에게 제공합니다. 저장 공간을 미리 할당하는 대신, 데이터가 기록됨에 따라 각 볼륨에 저장 공간이 동적으로 할당됩니다.

중복제거

동일한 데이터 블록을 찾아 단일 공유 블록에 대한 참조로 대체하여 효율성을 향상시킵니다. 이 기술은 동일한 볼륨에 있는 중복된 데이터 블록을 제거하여 저장 용량 요구 사항을 줄입니다.

압축

1차, 2차, 보관 저장소의 볼륨 내 데이터를 압축하여 데이터를 저장하는 데 필요한 물리적 용량을 줄입니다.

Cloud Volumes ONTAP 에 대한 Google Cloud 네트워킹 설정

NetApp Console IP 주소, 넷마스크, 경로 등 Cloud Volumes ONTAP 의 네트워킹 구성 요소를 설정합니다. 아웃바운드 인터넷 접속이 가능한지, 충분한 개인 IP 주소가 사용 가능한지, 올바른 연결이 설정되어 있는지 등을 확인해야 합니다.

HA 쌍을 배포하려면 다음을 수행해야 합니다."Google Cloud에서 HA 쌍이 작동하는 방식 알아보기" .

Cloud Volumes ONTAP 요구 사항

Google Cloud에서는 다음 요구 사항을 충족해야 합니다.

단일 노드 시스템에 대한 요구 사항

단일 노드 시스템을 구축하려면 네트워킹이 다음 요구 사항을 충족하는지 확인하십시오.

하나의 VPC

단일 노드 시스템에는 하나의 Virtual Private Cloud(VPC)가 필요합니다.

개인 IP 주소

Google Cloud의 단일 노드 시스템의 경우 Console은 다음에 프라이빗 IP 주소를 할당합니다.

- 마디

- 무리
- 스토리지 VM
- 데이터 NAS LIF
- 데이터 iSCSI LIF

API를 사용하여 Cloud Volumes ONTAP 배포하고 다음 플래그를 지정하면 스토리지 VM(SVM) 관리 LIF 생성을 건너뛸 수 있습니다.

```
skipSvmManagementLif: true
```

LIF는 물리적 포트와 연결된 IP 주소입니다. SnapCenter 와 같은 관리 도구에는 스토리지 VM(SVM) 관리 LIF가 필요합니다.

HA 쌍에 대한 특정 요구 사항

HA 쌍을 배포하려면 네트워킹이 다음 요구 사항을 충족하는지 확인하세요.

하나 또는 여러 개의 구역

여러 영역이나 단일 영역에 HA 구성을 배포하면 데이터의 높은 가용성을 보장할 수 있습니다. HA 쌍을 생성할 때 콘솔에서는 여러 영역이나 단일 영역을 선택하라는 메시지가 표시됩니다.

- 여러 구역(권장)

  3개 영역에 걸쳐 HA 구성을 배포하면 영역 내에서 장애가 발생하더라도 지속적인 데이터 가용성이 보장됩니다. 단일 영역을 사용하는 것에 비해 쓰기 성능은 약간 낮지만 최소한입니다.

- 단일 구역

  단일 영역에 배포되는 경우 Cloud Volumes ONTAP HA 구성은 확산 배치 정책을 사용합니다. 이 정책은 오류 격리를 위해 별도의 영역을 사용하지 않고도 영역 내의 단일 장애 지점으로부터 HA 구성이 보호되도록 보장합니다.

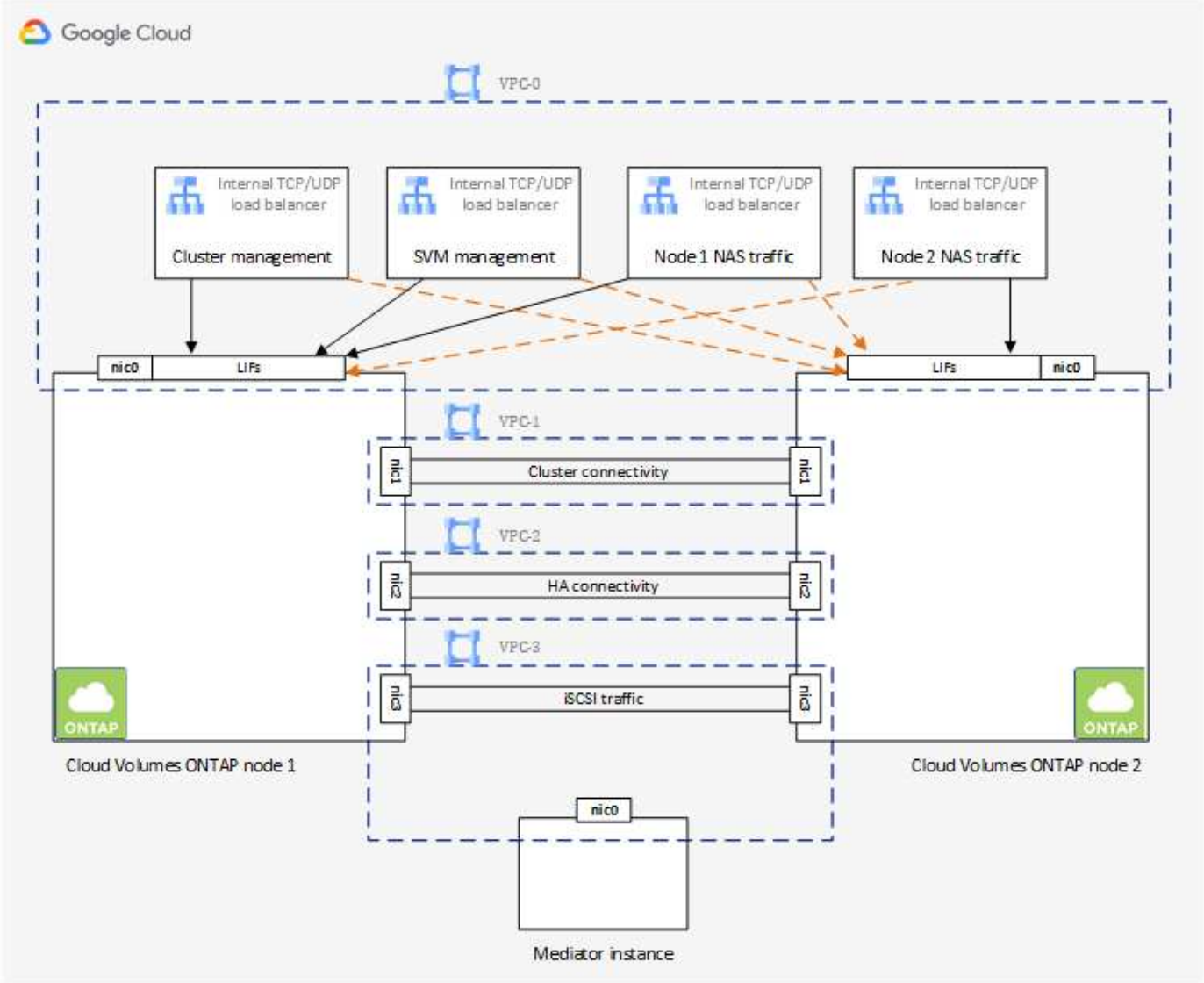
  이 배포 모델을 사용하면 영역 간에 데이터 유출 요금이 발생하지 않으므로 비용이 절감됩니다.

4개의 가상 사설 클라우드

HA 구성에는 4개의 가상 사설 클라우드(VPC)가 필요합니다. Google Cloud에서는 각 네트워크 인터페이스가 별도의 VPC 네트워크에 있어야 하므로 4개의 VPC가 필요합니다.

HA 쌍을 생성할 때 콘솔에서는 4개의 VPC를 선택하라는 메시지가 표시됩니다.

- 데이터 및 노드에 대한 인바운드 연결을 위한 VPC-0
- 노드와 HA 중재자 간 내부 통신을 위한 VPC-1, VPC-2 및 VPC-3



서브넷

각 VPC에는 개인 서브넷이 필요합니다.

VPC-0에 콘솔 에이전트를 배치하는 경우 API에 액세스하고 데이터 계층화를 활성화하려면 서브넷에서 Private Google Access를 활성화해야 합니다.

이러한 VPC의 서브넷에는 서로 다른 CIDR 범위가 있어야 합니다. CIDR 범위가 겹칠 수 없습니다.

개인 **IP** 주소

콘솔은 Google Cloud의 Cloud Volumes ONTAP 에 필요한 수의 개인 IP 주소를 자동으로 할당합니다. 네트워크에 사용 가능한 개인 주소가 충분한지 확인해야 합니다.

Cloud Volumes ONTAP에 할당된 LIF 수는 단일 노드 시스템을 배포하는지 또는 HA 쌍을 배포하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다. SVM 관리 LIF는 SnapCenter와 같은 관리 툴에 필요합니다.

- 단일 노드 NetApp Console은 단일 노드 시스템에 4개의 IP 주소를 할당합니다.
  - 노드 관리 LIF

- 클러스터 관리 LIF
- iSCSI 데이터 LIF

  iSCSI LIF는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공하며 시스템에서 다른 중요한 네트워킹 워크플로에 사용됩니다. 이러한 LIF는 필수이므로 삭제하면 안 됩니다.

- 나스 라이프

  API를 사용하여 Cloud Volumes ONTAP 배포하고 다음 플래그를 지정하면 스토리지 VM(SVM) 관리 LIF 생성을 건너뛸 수 있습니다.

```
skipSvmManagementLif: true
```

- **HA** 쌍 콘솔은 HA 쌍에 12-13개의 IP 주소를 할당합니다.
  - 2개의 노드 관리 LIF(e0a)
  - 1 클러스터 관리 LIF(e0a)
  - 2개의 iSCSI LIF(e0a)

    iSCSI LIF는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공하며 시스템에서 다른 중요한 네트워킹 워크플로에 사용됩니다. 이러한 LIF는 필수이므로 삭제하면 안 됩니다.

  - 1개 또는 2개의 NAS LIF(e0a)
  - 2개의 클러스터 LIF(e0b)
  - 2개의 HA 상호 연결 IP 주소(e0c)
  - 2개의 RSM iSCSI IP 주소(e0d)

    API를 사용하여 Cloud Volumes ONTAP 배포하고 다음 플래그를 지정하면 스토리지 VM(SVM) 관리 LIF 생성을 건너뛸 수 있습니다.

```
skipSvmManagementLif: true
```

내부 로드 밸런서

콘솔은 Cloud Volumes ONTAP HA 쌍으로 들어오는 트래픽을 관리하는 4개의 Google Cloud 내부 부하 분산 장치(TCP/UDP)를 생성합니다. 귀하 측에서는 아무런 설정이 필요하지 않습니다. 우리는 네트워크 트래픽에 대해 알려드리고 보안 문제를 완화하기 위해 이를 필수 사항으로 나열했습니다.

한 로드 밸런서는 클러스터 관리용이고, 다른 하나는 스토리지 VM(SVM) 관리용이며, 다른 하나는 노드 1로의 NAS 트래픽용이고, 마지막 하나는 노드 2로의 NAS 트래픽용입니다.

각 로드 밸런서의 설정은 다음과 같습니다.

- 공유된 개인 IP 주소 하나
- 글로벌 건강 검진 한 번

  기본적으로 상태 점검에 사용되는 포트는 63001, 63002, 63003입니다.

- 하나의 지역 TCP 백엔드 서비스
- 하나의 지역 UDP 백엔드 서비스
- 하나의 TCP 전달 규칙
- UDP 전달 규칙 1개
- 글로벌 접근이 비활성화되었습니다

  기본적으로 글로벌 액세스는 비활성화되어 있지만 배포 후에 활성화하는 것이 지원됩니다. 지역 간 트래픽의 지연 시간이 상당히 길어지기 때문에 이 기능을 비활성화했습니다. 우리는 여러분이 우연히 다른 지역의 탈것을 타고 부정적인 경험을 하지 않도록 하려고 했습니다. 이 옵션을 활성화하는 것은 귀하의 비즈니스 요구 사항에 맞게 결정됩니다.

공유 **VPC**

Cloud Volumes ONTAP 과 콘솔 에이전트는 Google Cloud 공유 VPC와 독립형 VPC에서 지원됩니다.

단일 노드 시스템의 경우 VPC는 공유 VPC 또는 독립형 VPC일 수 있습니다.

HA 쌍의 경우 4개의 VPC가 필요합니다. 각 VPC는 공유형이거나 독립형일 수 있습니다. 예를 들어, VPC-0은 공유 VPC가 될 수 있고, VPC-1, VPC-2, VPC-3은 독립형 VPC가 될 수 있습니다.

공유 VPC를 사용하면 여러 프로젝트에서 가상 네트워크를 구성하고 중앙에서 관리할 수 있습니다. _호스트 프로젝트 _에서 공유 VPC 네트워크를 설정하고 _서비스 프로젝트_에서 콘솔 에이전트와 Cloud Volumes ONTAP 가상 머신 인스턴스를 배포할 수 있습니다.

"Google Cloud 문서: 공유 VPC 개요" .

"콘솔 에이전트 배포에서 다루는 필수 공유 VPC 권한을 검토하세요."

VPC에서의 패킷 미러링

"패킷 미러링"Cloud Volumes ONTAP 배포하는 Google Cloud 서브넷에서 비활성화해야 합니다.

아웃바운드 인터넷 접속

Cloud Volumes ONTAP 시스템은 다양한 기능을 위해 외부 엔드포인트에 액세스하기 위해 아웃바운드 인터넷 액세스가 필요합니다. 엄격한 보안 요구 사항이 있는 환경에서 이러한 엔드포인트가 차단되면 Cloud Volumes ONTAP 제대로 작동할 수 없습니다.

콘솔 에이전트는 일상 업무를 위해 여러 엔드포인트에 연결합니다. 엔드포인트에 대한 정보는 다음을 참조하세요. "콘솔 에이전트에서 연결된 엔드포인트 보기" 그리고 "콘솔 사용을 위한 네트워킹 준비" .

Cloud Volumes ONTAP 엔드포인트

Cloud Volumes ONTAP 이러한 엔드포인트를 사용하여 다양한 서비스와 통신합니다.

엔드포인트	적용 가능	목적	배포 모드	엔드포인트를 사용할 수 없는 경우의 영향
\ https://netapp-cloud-account.auth0.com	입증	콘솔에서 인증에 사용됩니다.	표준 모드와 제한 모드.	사용자 인증에 실패하고 다음 서비스를 계속 사용할 수 없습니다. • Cloud Volumes ONTAP 서비스 • ONTAP 서비스 • 프로토콜 및 프록시 서비스
\ https://api.bluexp.netapp.com/tenancy	차용	콘솔에서 Cloud Volumes ONTAP 리소스를 검색하여 리소스와 사용자에게 권한을 부여하는 데 사용됩니다.	표준 모드와 제한 모드.	Cloud Volumes ONTAP 리소스와 사용자는 권한이 없습니다.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	AutoSupport 원격 측정 데이터를 NetApp 지원팀으로 전송하는 데 사용됩니다.	표준 모드와 제한 모드.	AutoSupport 정보가 전달되지 않았습니다.

엔드포인트	적용 가능	목적	배포 모드	엔드포인트를 사용할 수 없는 경우의 영향
https://cloudbuild.googleapis.com/v1 (개인 모드 배포 전용) https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud(상업적 사용).	Google Cloud 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Google Cloud 서비스와 통신하여 Google Cloud의 콘솔에 대한 특정 작업을 수행할 수 없습니다.

다른 네트워크의 **ONTAP** 시스템에 대한 연결

Google Cloud의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 VPC와 다른 네트워크(예: 회사 네트워크) 간에 VPN 연결이 필요합니다.

"Google Cloud 문서: Cloud VPN 개요" .

방화벽 규칙

콘솔은 Cloud Volumes ONTAP 성공적으로 작동하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함하는 Google Cloud 방화벽 규칙을 생성합니다. 테스트 목적으로 포트를 참조하거나 자체 방화벽 규칙을 사용하려는 경우 포트를 참조할 수 있습니다.

Cloud Volumes ONTAP 의 방화벽 규칙에는 인바운드 규칙과 아웃바운드 규칙이 모두 필요합니다. HA 구성을 배포하는 경우 VPC-0의 Cloud Volumes ONTAP 에 대한 방화벽 규칙은 다음과 같습니다.

HA 구성에는 두 세트의 방화벽 규칙이 필요합니다.

- VPC-0의 HA 구성 요소에 대한 한 세트의 규칙입니다. 이러한 규칙은 Cloud Volumes ONTAP 에 대한 데이터 액세스를 가능하게 합니다.
- VPC-1, VPC-2, VPC-3의 HA 구성 요소에 대한 또 다른 규칙 세트입니다. 이러한 규칙은 HA 구성 요소 간의 인바운드 및 아웃바운드 통신에 적용됩니다. 자세히 알아보기 .

콘솔 에이전트에 대한 정보를 찾고 계신가요? "콘솔 에이전트에 대한 방화벽 규칙 보기"

인바운드 규칙

Cloud Volumes ONTAP 시스템을 추가하면 배포 중에 미리 정의된 방화벽 정책에 대한 소스 필터를 선택할 수 있습니다.

- 선택된 **VPC**만 해당: 인바운드 트래픽의 소스 필터는 Cloud Volumes ONTAP 시스템의 VPC 서브넷 범위와 콘솔 에이전트가 있는 VPC의 서브넷 범위입니다. 이것은 권장되는 옵션입니다.
- 모든 **VPC**: 인바운드 트래픽의 소스 필터는 0.0.0.0/0 IP 범위입니다.

자체 방화벽 정책을 사용하는 경우 Cloud Volumes ONTAP 과 통신해야 하는 모든 네트워크를 추가해야 하지만, 내부 Google Load Balancer가 올바르게 작동할 수 있도록 두 주소 범위도 추가해야 합니다. 이 주소는 130.211.0.0/22와 35.191.0.0/16입니다. 자세한 내용은 다음을 참조하세요. "Google Cloud 문서: 로드 밸런서 방화벽 규칙" .

규약	포트	목적
모든 ICMP	모두	인스턴스에 ping을 보냅니다.
HTTP	80	클러스터 관리 LIF의 IP 주소를 사용하여 ONTAP System Manager 웹 콘솔에 대한 HTTP 액세스
HTTPS	443	클러스터 관리 LIF의 IP 주소를 사용하여 콘솔 에이전트와 ONTAP System Manager 웹 콘솔에 대한 HTTPS 액세스 연결
SSH	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 대한 SSH 액세스
TCP	111	NFS에 대한 원격 프로시저 호출
TCP	139	CIFS용 NetBIOS 서비스 세션
TCP	161-162	간단한 네트워크 관리 프로토콜
TCP	445	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
TCP	635	NFS 마운트
TCP	749	케르베로스
TCP	2049	NFS 서버 데몬
TCP	3260	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045	NFS 잠금 데몬
TCP	4046	NFS용 네트워크 상태 모니터
TCP	10000	NDMP를 사용한 백업
TCP	11104	SnapMirror 위한 클러스터 간 통신 세션 관리
TCP	11105	클러스터 간 LIF를 사용한 SnapMirror 데이터 전송

규약	포트	목적
TCP	63001-63050	어느 노드가 정상인지 확인하기 위한 로드 밸런싱 프로브 포트(HA 쌍에만 필요)
UDP	111	NFS에 대한 원격 프로시저 호출
UDP	161-162	간단한 네트워크 관리 프로토콜
UDP	635	NFS 마운트
UDP	2049	NFS 서버 데몬
UDP	4045	NFS 잠금 데몬
UDP	4046	NFS용 네트워크 상태 모니터
UDP	4049	NFS rquotad 프로토콜

아웃바운드 규칙

Cloud Volumes ONTAP 의 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 개방합니다. 이것이 허용된다면, 기본적인 아웃바운드 규칙을 따르세요. 더욱 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

Cloud Volumes ONTAP 의 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함되어 있습니다.

규약	포트	목적
모든 ICMP	모두	모든 아웃바운드 트래픽
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Cloud Volumes ONTAP 의 아웃바운드 통신에 필요한 포트만 열 수 있습니다. Cloud Volumes ONTAP 클러스터는 노드 트래픽을 조절하기 위해 다음 포트를 사용합니다.

소스는 Cloud Volumes ONTAP 시스템의 인터페이스(IP 주소)입니다.

서비스	규약	포트	원천	목적지	목적
액티브 디렉토리	TCP	88	노드 관리 LIF	Active Directory 포리스트	Kerberos V 인증
	UDP	137	노드 관리 LIF	Active Directory 포리스트	NetBIOS 이름 서비스
	UDP	138	노드 관리 LIF	Active Directory 포리스트	NetBIOS 데이터그램 서비스
	TCP	139	노드 관리 LIF	Active Directory 포리스트	NetBIOS 서비스 세션
	TCP 및 UDP	389	노드 관리 LIF	Active Directory 포리스트	LDAP
	TCP	445	노드 관리 LIF	Active Directory 포리스트	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
	TCP	464	노드 관리 LIF	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(SET_CHANGE)
	UDP	464	노드 관리 LIF	Active Directory 포리스트	Kerberos 키 관리
	TCP	749	노드 관리 LIF	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(RPCSEC_GSS)
	TCP	88	데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트	Kerberos V 인증
	UDP	137	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 이름 서비스
	UDP	138	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 데이터그램 서비스
	TCP	139	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 서비스 세션
	TCP 및 UDP	389	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	LDAP
	TCP	445	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
	TCP	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(SET_CHANGE)
	UDP	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos 키 관리
	TCP	749	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(RPCSEC_GSS)

서비스	규약	포트	원천	목적지	목적
AutoSupport	HTTPS	443	노드 관리 LIF	mysupport.netapp.com	AutoSupport (HTTPS가 기본값)
	HTTP	80	노드 관리 LIF	mysupport.netapp.com	AutoSupport (전송 프로토콜이 HTTPS에서 HTTP로 변경된 경우에만)
	TCP	3128	노드 관리 LIF	콘솔 에이전트	아웃바운드 인터넷 연결이 불가능한 경우 콘솔 에이전트의 프록시 서버를 통해 AutoSupport 메시지 보내기
구성 백업	HTTP	80	노드 관리 LIF	http://<콘솔 에이전트 IP 주소>/occm/offboxconfig	구성 백업을 콘솔 에이전트로 보냅니다 ."ONTAP 문서"
DHCP	UDP	68	노드 관리 LIF	DHCP	최초 설정을 위한 DHCP 클라이언트
DHCPS	UDP	67	노드 관리 LIF	DHCP	DHCP 서버
DNS	UDP	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	TCP	18600년–18699년	노드 관리 LIF	대상 서버	NDMP 사본
SMTP	TCP	25	노드 관리 LIF	메일 서버	SMTP 알림은 AutoSupport 에 사용할 수 있습니다.
SNMP	TCP	161	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	UDP	161	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	TCP	162	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	UDP	162	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
SnapMirror	TCP	11104	클러스터 간 LIF	ONTAP 클러스터 간 LIF	SnapMirror 위한 클러스터 간 통신 세션 관리
	TCP	11105	클러스터 간 LIF	ONTAP 클러스터 간 LIF	SnapMirror 데이터 전송
시스템 로그	UDP	514	노드 관리 LIF	시스템 로그 서버	Syslog 전달 메시지

VPC-1, VPC-2 및 **VPC-3**에 대한 규칙

Google Cloud에서는 HA 구성이 4개의 VPC에 배포됩니다. VPC-0의 HA 구성에 필요한 방화벽 규칙은 다음과 같습니다.위에 나열된 Cloud Volumes ONTAP .

한편, VPC-1, VPC-2, VPC-3의 인스턴스에 대해 미리 정의된 방화벽 규칙은 모든 프로토콜과 포트를 통한 수신 통신을 활성화합니다. 이러한 규칙은 HA 노드 간의 통신을 가능하게 합니다.

HA 노드에서 HA 중재자로의 통신은 포트 3260(iSCSI)을 통해 이루어집니다.

새로운 Google Cloud HA 쌍 배포에 대해 높은 쓰기 속도를 구현하려면 VPC-1, VPC-2, VPC-3에 최소 8,896바이트의 최대 전송 단위(MTU)가 필요합니다. 기존 VPC-1, VPC-2, VPC-3을 8,896바이트의 MTU로 업그레이드하기로 선택한 경우 구성 프로세스 중에 이러한 VPC를 사용하는 모든 기존 HA 시스템을 종료해야 합니다.

프라이빗 모드 배포를 위한 **Infrastructure Manager** 구성

Cloud Volumes ONTAP 9.16.1 이상 버전을 프라이빗 모드로 배포하려면 Google에서 향후 지원을 중단할 예정인 Deployment Manager 대신 Cloud Volumes ONTAP가 Google Cloud Infrastructure Manager를 배포 서비스로 사용하도록 몇 가지 구성을 변경해야 합니다.

시작하기 전에

- Cloud Volumes ONTAP 시스템이 9.16.1 이상인지 확인하십시오. 그렇지 않은 경우 시스템을 업그레이드하십시오. 지침은 "Cloud Volumes ONTAP 업그레이드"을 참조하십시오.
- Google Cloud API가 사용 설정되어 있는지 확인하세요. "Google Cloud API 활성화"를 참조하십시오.
- Cloud Build API가 활성화되어 있는지 확인하십시오. "여기에서 Cloud Build API를 활성화하세요"을(를) 참조하십시오.
- Console 에이전트의 서비스 계정에 모든 표준 권한이 있는지 확인하십시오. 또한 서비스 계정에 `cloudbuild.workerpools.get` 및 `cloudbuild.workerpools.list` 권한이 있는지 확인하십시오. "콘솔 에이전트에 대한 Google Cloud 권한"을 참조하십시오.

단계

1. Cloud Volumes ONTAP 배포와 동일한 리전에 이 구성을 사용하여 프라이빗 워커 풀을 생성합니다. 프라이빗 워커 풀 생성에 대한 자세한 내용은 "Google Cloud 문서: 프라이빗 풀 생성 및 관리" 및 "Google Cloud Build 가격 책정"을 참조하십시오.

   워커 풀은 다음 구성을 가져야 합니다.

   - 시스템 유형: e2-medium
   - 디스크 크기: 100 GB
   - 외부 IP 할당: False
   - 네트워크: 기본 또는 프라이빗.
   - "Google API"에 액세스하도록 구성된 서브넷. 서브넷이 Google API에 액세스할 수 있도록 하려면 다음 단계를 수행하십시오.
     i. 서브넷에 대해 "Private Google Access"가 켜져 있는지 확인하십시오.
     ii. *VPC Network 레벨 > Private Service Access 탭 > 서비스에 할당된 IP 범위*로 이동하십시오.
     iii. *IP 범위 할당*을 선택하고 Google Compute Service에 대한 프라이빗 연결의 내부 IP 범위를 할당합니다.
     iv. *서비스에 대한 프라이빗 연결*에서 *연결 생성*을 선택합니다.
     v. *연결된 서비스 공급자 = Google Cloud Platform*을 선택합니다.
     vi. 이전 단계에서 생성한 프라이빗 연결 IP 범위에 대한 할당을 지정합니다.
2. 이 워커 풀을 배포하고 Cloud Volumes ONTAP 관리를 위해 계속 실행 상태로 유지하세요. Google Cloud는 이 워커 풀을 사용하여 모든 Terraform 작업을 격리된 환경에서 실행합니다.
3. 프라이빗 모드에서 Cloud Volumes ONTAP을 배포할 때 **GCP Worker Pool** 필드에서 이 워커 풀의 이름을 선택하십시오. 지침은 "Google Cloud에서 Cloud Volumes ONTAP 실행"을 참조하십시오.

콘솔 에이전트에 대한 요구 사항

아직 콘솔 에이전트를 만들지 않았다면 네트워킹 요구 사항을 검토해야 합니다.

- "콘솔 에이전트에 대한 네트워킹 요구 사항 보기"
- "Google Cloud의 방화벽 규칙"

콘솔 에이전트 프록시를 지원하는 네트워크 구성

콘솔 에이전트에 구성된 프록시 서버를 사용하여 Cloud Volumes ONTAP 에서 아웃바운드 인터넷 액세스를 활성화할 수 있습니다. 콘솔은 두 가지 유형의 프록시를 지원합니다.

- 명시적 프록시: Cloud Volumes ONTAP 의 아웃바운드 트래픽은 콘솔 에이전트 프록시 구성 중에 지정된 프록시 서버의 HTTP 주소를 사용합니다. 콘솔 에이전트 관리자는 추가 인증을 위해 사용자 자격 증명과 루트 CA 인증서를 구성했을 수도 있습니다. 명시적 프록시에 대해 루트 CA 인증서를 사용할 수 있는 경우 다음을 사용하여 동일한 인증서를 Cloud Volumes ONTAP 시스템에 가져와 업로드해야 합니다. "ONTAP CLI: 보안 인증서 설치" 명령.
- 투명 프록시: 네트워크는 콘솔 에이전트 프록시를 통해 Cloud Volumes ONTAP 에서 아웃바운드 트래픽을 자동으로 라우팅하도록 구성됩니다. 투명 프록시를 설정할 때 콘솔 에이전트 관리자는 프록시 서버의 HTTP 주소가 아닌 Cloud Volumes ONTAP 에서의 연결을 위한 루트 CA 인증서만 제공하면 됩니다. 다음을 사용하여 Cloud Volumes ONTAP 시스템에 동일한 루트 CA 인증서를 가져와 업로드해야 합니다. "ONTAP CLI: 보안 인증서 설치" 명령.

콘솔 에이전트에 대한 프록시 서버 구성에 대한 정보는 다음을 참조하십시오. "프록시 서버를 사용하도록 콘솔 에이전트 구성" .

Google Cloud에서 **Cloud Volumes ONTAP** 에 대한 네트워크 태그 구성

콘솔 에이전트의 투명 프록시 구성 중에 관리자는 Google Cloud에 대한 네트워크 태그를 추가합니다. Cloud Volumes ONTAP 구성에 대해 동일한 네트워크 태그를 얻어 수동으로 추가해야 합니다. 이 태그는 프록시 서버가 올바르게 작동하는 데 필요합니다.

1. Google Cloud Console에서 Cloud Volumes ONTAP 시스템을 찾습니다.
2. *세부정보 > 네트워킹 > 네트워크 태그*로 이동합니다.
3. 콘솔 에이전트에 사용된 태그를 추가하고 구성을 저장합니다.

관련 주제

- "Cloud Volumes ONTAP 에 대한 AutoSupport 설정 확인"
- "ONTAP 내부 포트에 대해 알아보세요" .

Google Cloud에 **Cloud Volumes ONTAP** 배포하기 위한 **VPC** 서비스 제어 설정

VPC 서비스 제어를 사용하여 Google Cloud 환경을 잠그기로 선택하는 경우 NetApp Console 과 Cloud Volumes ONTAP Google Cloud API와 상호 작용하는 방식과 Console과 Cloud Volumes ONTAP 배포하기 위해 서비스 경계를 구성하는 방법을 이해해야 합니다.

VPC 서비스 제어를 사용하면 신뢰할 수 있는 경계 외부에서 Google 관리 서비스에 대한 액세스를 제어하고, 신뢰할 수 없는 위치에서의 데이터 액세스를 차단하고, 승인되지 않은 데이터 전송 위험을 완화할 수 있습니다. "Google Cloud VPC 서비스 제어에 대해 자세히 알아보세요" .

NetApp 서비스가 VPC 서비스 제어와 통신하는 방법

콘솔은 Google Cloud API와 직접 통신합니다. 이는 Google Cloud 외부의 외부 IP 주소(예: api.services.cloud.netapp.com)에서 트리거되거나, Google Cloud 내에서 Console 에이전트에 할당된 내부 주소에서 트리거됩니다.

콘솔 에이전트의 배포 스타일에 따라 서비스 경계에 대한 특정 예외를 만들어야 할 수도 있습니다.

이미지

Cloud Volumes ONTAP과 Console은 모두 NetApp에서 관리하는 Google Cloud 내 프로젝트의 이미지를 사용합니다. 조직에서 조직 내에 호스팅되지 않은 이미지 사용을 차단하는 정책이 있는 경우 Console 에이전트 및 Cloud Volumes ONTAP 배포에 영향을 미칠 수 있습니다.

수동 설치 방법을 사용하여 콘솔 에이전트를 수동으로 배포할 수 있지만 Cloud Volumes ONTAP 도 NetApp 프로젝트에서 이미지를 가져와야 합니다. 콘솔 에이전트와 Cloud Volumes ONTAP 배포하려면 허용 목록을 제공해야 합니다.

콘솔 에이전트 배포

콘솔 에이전트를 배포하는 사용자는 프로젝트 ID _netapp-cloudmanager_와 프로젝트 번호 _14190056516_에 호스팅된 이미지를 참조할 수 있어야 합니다.

Cloud Volumes ONTAP 배포

- 콘솔 서비스 계정은 서비스 프로젝트의 프로젝트 ID _netapp-cloudmanager_와 프로젝트 번호 _14190056516_에 호스팅된 이미지를 참조해야 합니다.
- 기본 Google API 서비스 에이전트의 서비스 계정은 서비스 프로젝트의 프로젝트 ID _netapp-cloudmanager_와 프로젝트 번호 _14190056516_에 호스팅된 이미지를 참조해야 합니다.

VPC 서비스 제어를 사용하여 이러한 이미지를 가져오는 데 필요한 규칙의 예는 아래와 같습니다.

VPC 서비스 제어 경계 정책

정책을 사용하면 VPC Service Controls 규칙 집합에 대한 예외를 허용할 수 있습니다. 정책에 대한 자세한 내용은 해당 페이지를 참조하십시오 "Google Cloud VPC Service Controls 정책 설명서".

콘솔에 필요한 정책을 설정하려면 조직 내의 VPC 서비스 제어 경계로 이동하여 다음 정책을 추가하세요. 필드는 VPC 서비스 제어 정책 페이지에 제공된 옵션과 일치해야 합니다. 또한 모든 규칙이 필수이며 규칙 세트에서는 **OR** 매개변수를 사용해야 합니다.

Ingress 규칙

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

또는

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

또는

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

탈출 규칙

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

위에 설명된 프로젝트 번호는 NetApp 에서 콘솔 에이전트와 Cloud Volumes ONTAP 의 이미지를 저장하는 데 사용되는 프로젝트 _netapp-cloudmanager_입니다.

Cloud Volumes ONTAP 에 대한 Google Cloud 서비스 계정을 만듭니다.

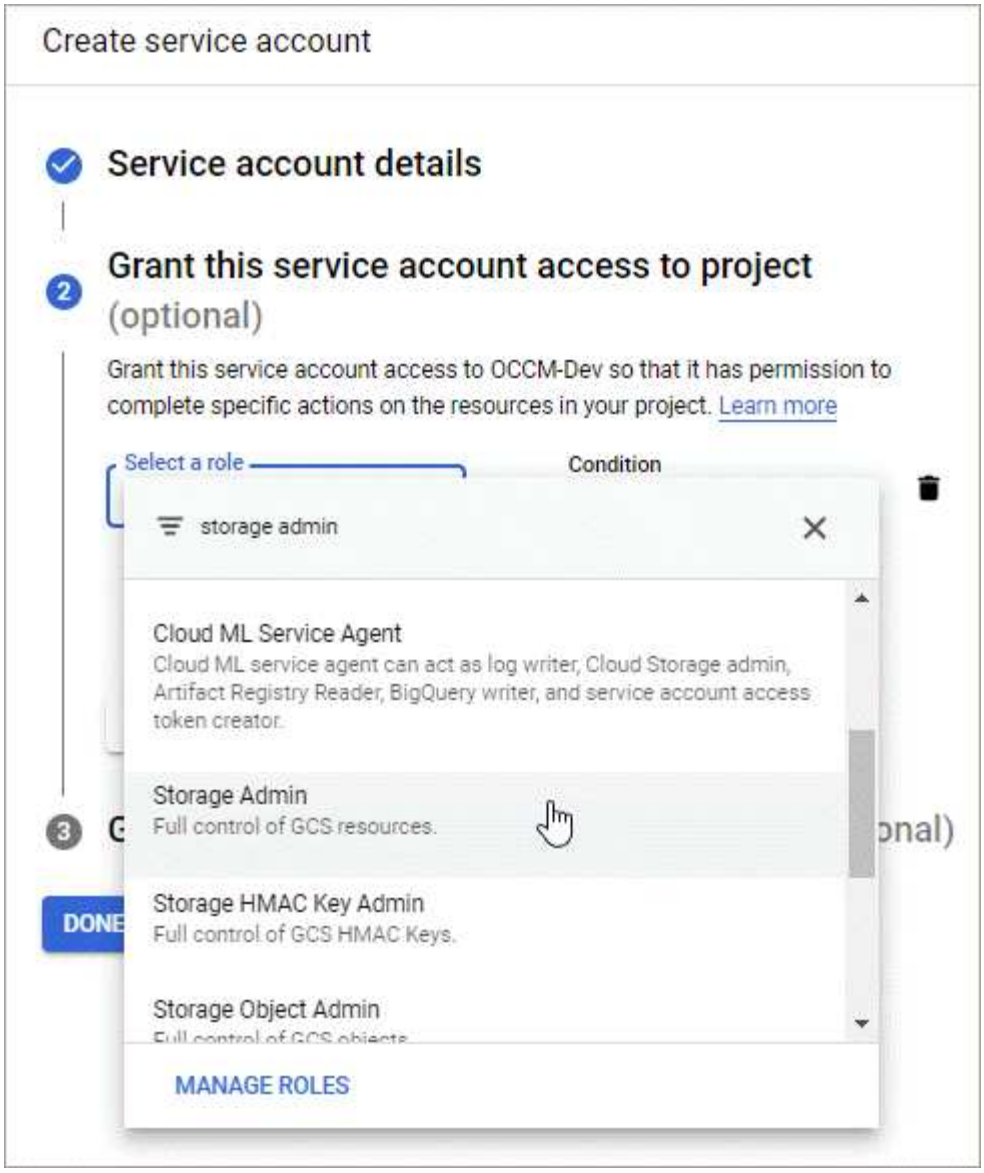
Cloud Volumes ONTAP 두 가지 목적으로 Google Cloud 서비스 계정이 필요합니다. 첫 번째는 활성화할 때입니다."데이터 계층화" Google Cloud의 저렴한 객체 스토리지에 콜드 데이터를 계층화합니다. 두 번째는 다음을 활성화할 때입니다. "NetApp Backup and Recovery" 저렴한 개체 스토리지에 볼륨을 백업합니다.

Cloud Volumes ONTAP 서비스 계정을 사용하여 계층화된 데이터용 버킷 하나와 백업용 버킷 하나에 액세스하고 관리합니다.

하나의 서비스 계정을 설정하여 두 가지 목적으로 모두 사용할 수 있습니다. 서비스 계정에는 저장소 관리자 역할이 있어야 합니다.

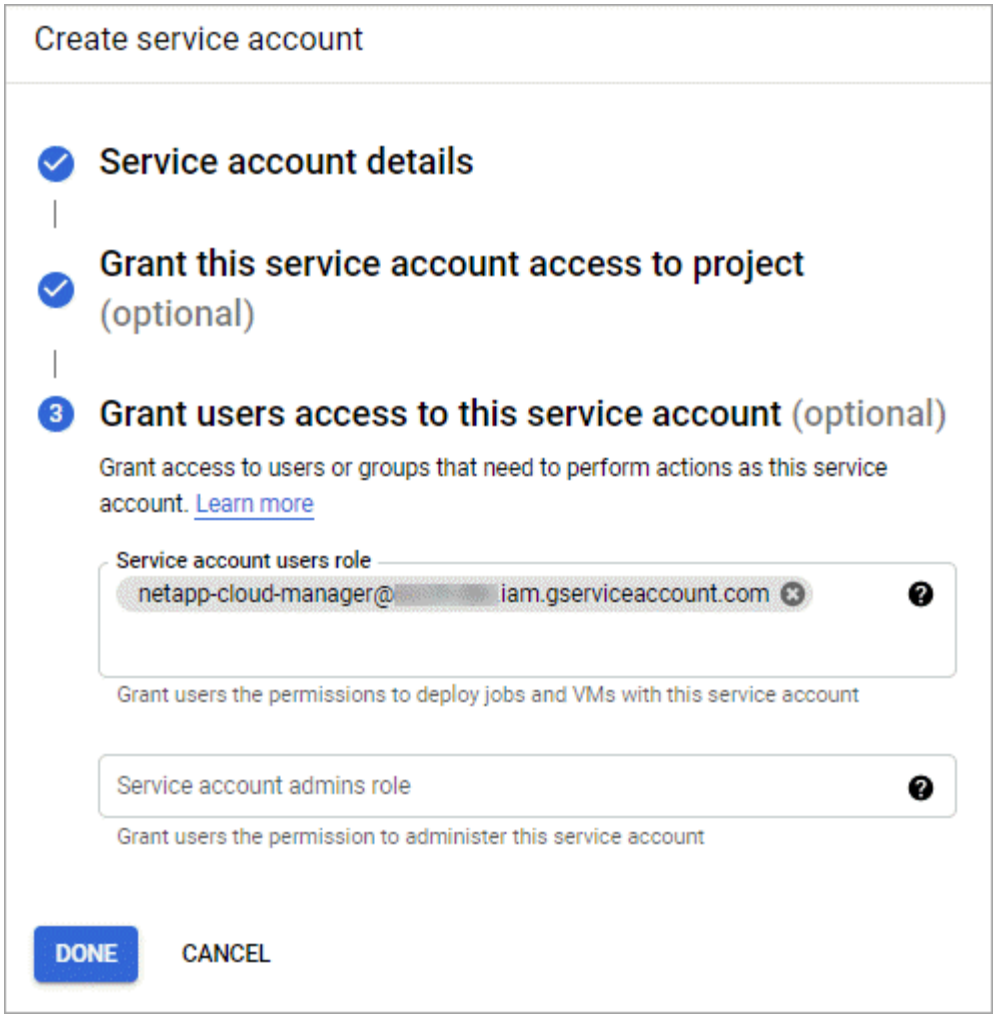
단계

1. Google Cloud 콘솔에서 "서비스 계정 페이지로 이동".
2. 프로젝트를 선택하세요.
3. *서비스 계정 만들기*를 클릭하고 필요한 정보를 입력하세요.
    a. 서비스 계정 세부 정보: 이름과 설명을 입력하세요.
    b. 이 서비스 계정에 프로젝트에 대한 액세스 권한 부여: 저장소 관리자 역할을 선택합니다.



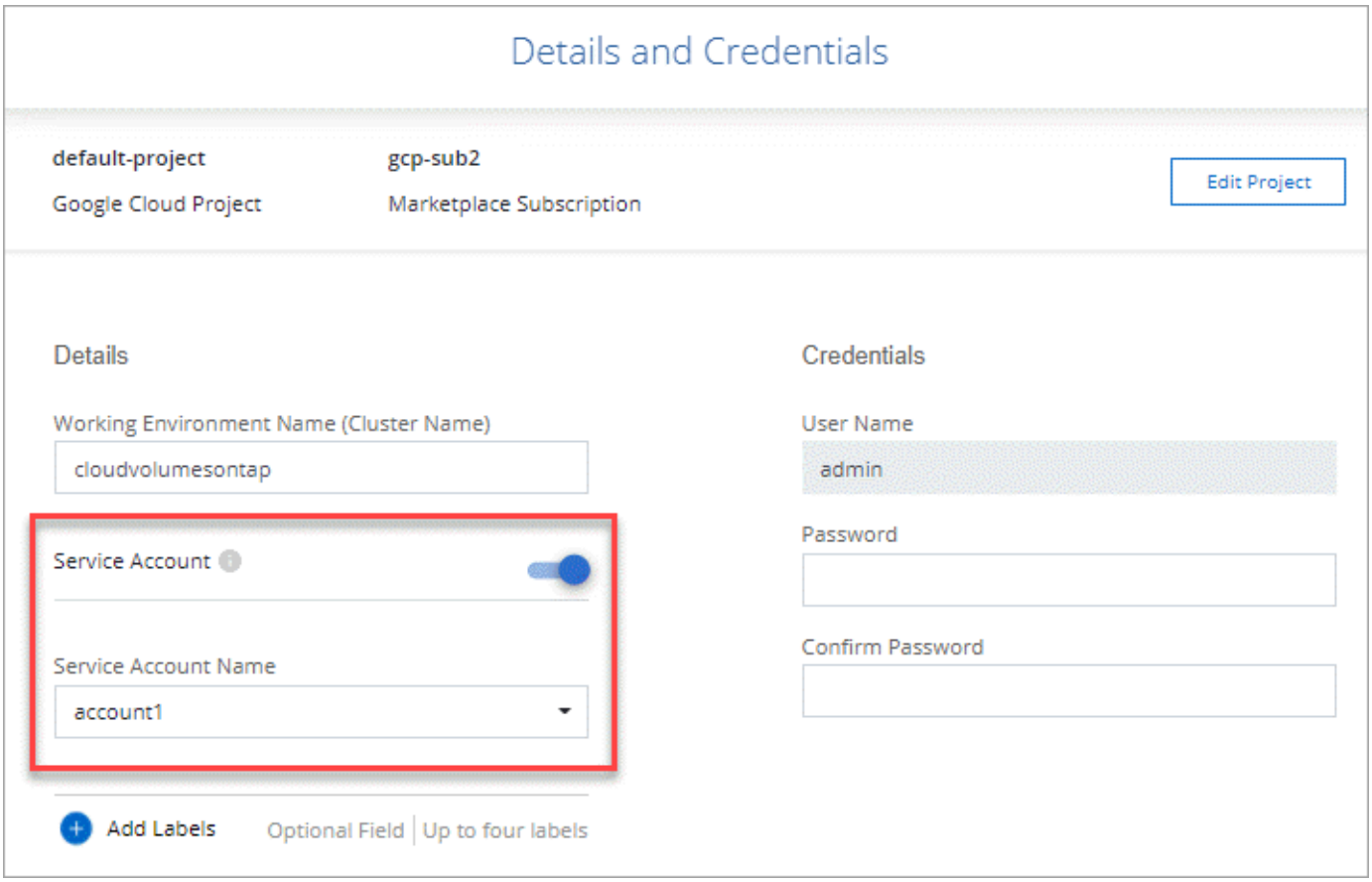
c. 사용자에게 이 서비스 계정에 대한 액세스 권한 부여: 이 새로운 서비스 계정에 콘솔 에이전트 서비스 계정을 _서비스 계정 사용자_로 추가합니다.

   이 단계는 데이터 계층화에만 필요합니다. 백업 및 복구에는 필요하지 않습니다.



다음은 무엇인가요?

나중에 Cloud Volumes ONTAP 시스템을 생성할 때 서비스 계정을 선택해야 합니다.



Cloud Volumes ONTAP 에서 고객 관리 암호화 키 사용

Google Cloud Storage는 디스크에 쓰기 전에 항상 데이터를 암호화하지만, API를 사용하면 _고객 관리 암호화 키_를 사용하는 Cloud Volumes ONTAP 시스템을 만들 수 있습니다. 이러한 키는 Cloud Key Management Service를 사용하여 GCP에서 생성하고 관리하는 키입니다.

단계

1. 키가 저장된 프로젝트에서 콘솔 에이전트 서비스 계정에 프로젝트 수준에서 올바른 권한이 있는지 확인하세요.

   권한은 다음에서 제공됩니다. "기본적으로 서비스 계정 권한" 하지만 Cloud Key Management Service에 대한 대체 프로젝트를 사용하는 경우에는 적용되지 않을 수 있습니다.

   권한은 다음과 같습니다.

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. 서비스 계정이 다음인지 확인하세요. "Google Compute Engine 서비스 에이전트" 키에 Cloud KMS 암호화/복호화 권한이 있습니다.

   서비스 계정의 이름은 "service-[service_project_number]@compute-system.iam.gserviceaccount.com" 형식을 사용합니다.

"Google Cloud 문서: Cloud KMS와 함께 IAM 사용 - 리소스에 대한 역할 부여"

3. get 명령을 호출하여 키의 "id"를 얻으십시오. `/gcp/vsa/metadata/gcp-encryption-keys` API 호출 또는 GCP 콘솔의 키에서 "리소스 이름 복사"를 선택합니다.
4. 고객 관리 암호화 키를 사용하고 데이터를 개체 스토리지로 계층화하는 경우 NetApp Console 영구 디스크를 암호화하는 데 사용되는 것과 동일한 키를 활용하려고 시도합니다. 하지만 먼저 Google Cloud Storage 버킷을 활성화하여 키를 사용해야 합니다.

   a. 다음을 따라 Google Cloud Storage 서비스 에이전트를 찾으세요. "Google Cloud 문서: Cloud Storage 서비스 에이전트 가져오기" .

   b. 암호화 키로 이동하여 Google Cloud Storage 서비스 에이전트에 Cloud KMS 암호화/복호화 권한을 할당합니다.

   자세한 내용은 다음을 참조하세요. "Google Cloud 문서: 고객 관리 암호화 키 사용"

5. 시스템을 생성할 때 API 요청에 "gcpEncryption" 매개변수를 사용하십시오.

   예

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-
1/cryptoKeys/generatedkey1"
  }
```

를 참조하세요 "NetApp Console 자동화 문서" "GcpEncryption" 매개변수 사용에 대한 자세한 내용은 다음을 참조하세요.

Google Cloud에서 Cloud Volumes ONTAP 에 대한 라이선싱 설정

Cloud Volumes ONTAP 에서 사용할 라이선싱 옵션을 결정한 후에는 새 시스템을 만들 때 해당 라이선싱 옵션을 선택하기 전에 몇 가지 단계를 거쳐야 합니다.

프리미엄

최대 500GiB의 프로비저닝 용량을 제공하는 Cloud Volumes ONTAP 무료로 사용하려면 Freemium 옵션을 선택하세요. "Freemium 제공에 대해 자세히 알아보세요" .

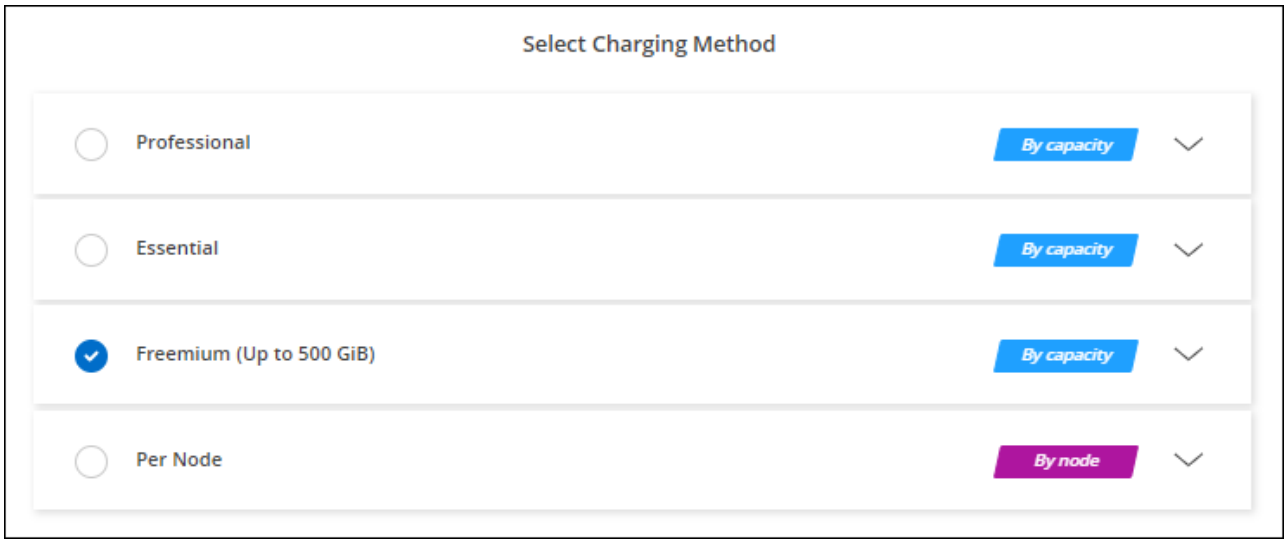
단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 NetApp Console 의 단계를 따릅니다.

   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 메시지에 따라 Google Cloud Marketplace에서 사용량에 따라 지불하는 서비스를 구독하세요.

   프로비저닝된 용량이 500GiB를 초과하지 않는 한 마켓플레이스 구독을 통해 요금이 청구되지 않습니다. 초과 시 시스템은 자동으로 다음 용량으로 변환됩니다."필수 패키지" .

   b. 콘솔로 돌아와서 요금 청구 방법 페이지에서 *프리미엄*을 선택하세요.



"Google Cloud에서 Cloud Volumes ONTAP 시작하는 단계별 지침을 확인하세요." .

용량 기반 라이센스

용량 기반 라이선싱을 사용하면 TiB 용량당 Cloud Volumes ONTAP 비용을 지불할 수 있습니다. 용량 기반 라이선싱은 패키지(Essentials 또는 Professional 패키지) 형태로 제공됩니다.

Essentials 및 Professional 패키지는 다음과 같은 소비 모델 또는 구매 옵션으로 이용 가능합니다.

- NetApp 에서 구매한 라이선스(BYOL(Bring Your Own License))
- Google Cloud Marketplace의 시간당 결제(PAYGO) 구독
- 연간 계약

"용량 기반 라이선싱에 대해 자세히 알아보세요" .

다음 섹션에서는 각 소비 모델을 시작하는 방법을 설명합니다.

바이올

NetApp 에서 라이선스(BYOL)를 구매하여 선불로 지불하면 모든 클라우드 공급자에 Cloud Volumes ONTAP 시스템을 배포할 수 있습니다.

NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 에 대한 BYOL 라이선싱의 제한된 가용성" .

단계

1. "라이센스를 얻으려면 NetApp Sales에 문의하세요."
2. "NetApp Console 에 NetApp 지원 사이트 계정 추가"

   콘솔은 NetApp 지원 사이트 계정과 연결된 라이선스에 대한 세부 정보를 얻기 위해 NetApp 라이선스 서비스에 자동으로 쿼리를 보냅니다. 오류가 없으면 콘솔이 라이선스를 추가합니다.

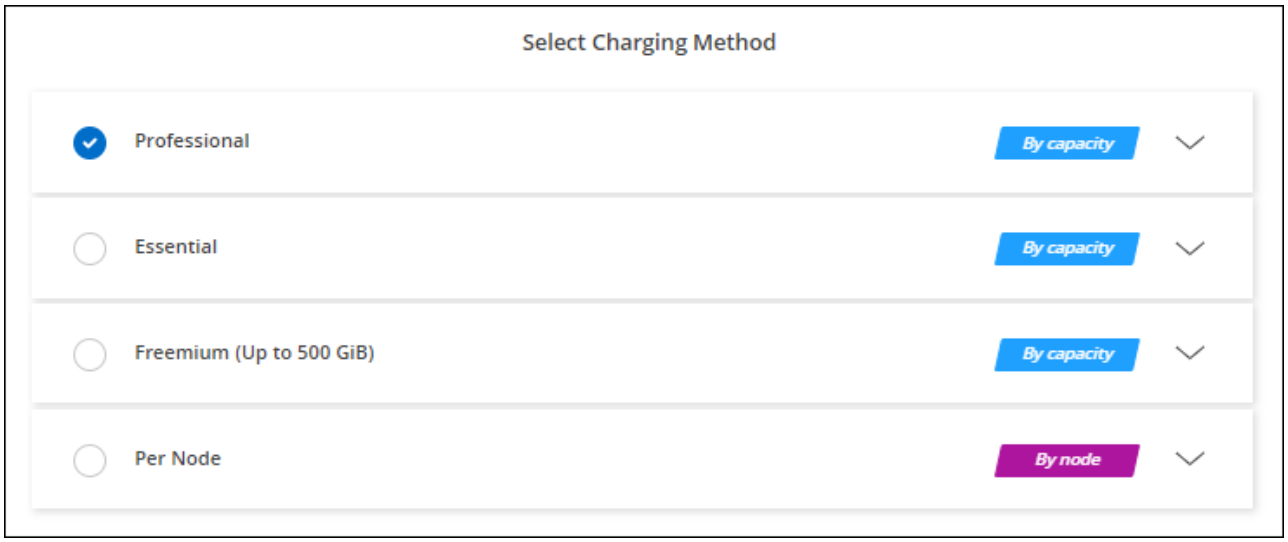
   Cloud Volumes ONTAP 에서 라이선스를 사용하려면 먼저 콘솔에서 라이선스를 사용할 수 있어야 합니다. 필요한 경우 다음을 수행할 수 있습니다."콘솔에 라이센스를 수동으로 추가합니다." .

3. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 메시지에 따라 Google Cloud Marketplace에서 사용량에 따라 지불하는 서비스를 구독하세요.

      NetApp 에서 구매한 라이선스는 항상 먼저 청구되지만, 라이선스 용량을 초과하거나 라이선스 기간이 만료되면 마켓플레이스의 시간당 요금으로 청구됩니다.

   b. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"Google Cloud에서 Cloud Volumes ONTAP 시작하는 단계별 지침을 확인하세요." .

PAYGO 구독

클라우드 공급업체의 마켓플레이스에서 제공하는 혜택을 구독하여 시간당 요금을 지불하세요.

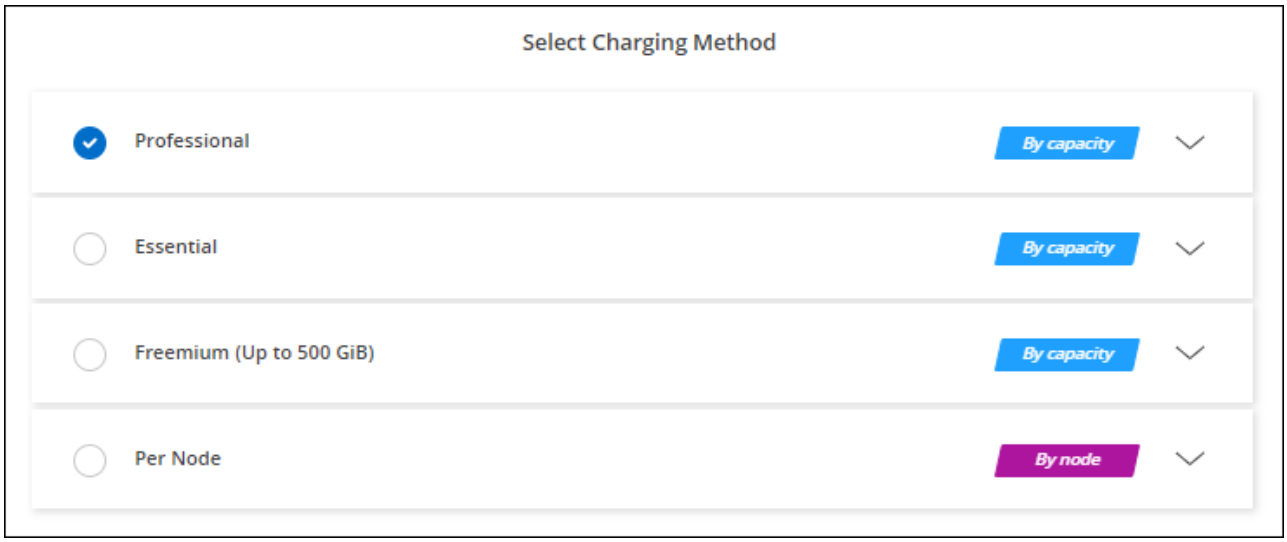
Cloud Volumes ONTAP 시스템을 만들면 콘솔에서 Google Cloud Marketplace에서 제공되는 계약에 가입하라는 메시지가 표시됩니다. 해당 구독은 요금 청구를 위해 시스템에 연결됩니다. 동일한 구독을 추가 시스템에도 사용할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 메시지에 따라 Google Cloud Marketplace에서 사용량에 따라 지불하는 서비스를 구독하세요.

   b. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"Google Cloud에서 Cloud Volumes ONTAP 시작하는 단계별 지침을 확인하세요." .

설정 > 사용자 인증 정보 페이지에서 계정과 연결된 Google Cloud Marketplace 구독을 관리할 수 있습니다. "Google Cloud 자격 증명 및 구독을 관리하는 방법을 알아보세요."

연간 계약

연간 계약을 구매하여 매년 Cloud Volumes ONTAP 에 대한 비용을 지불하세요.

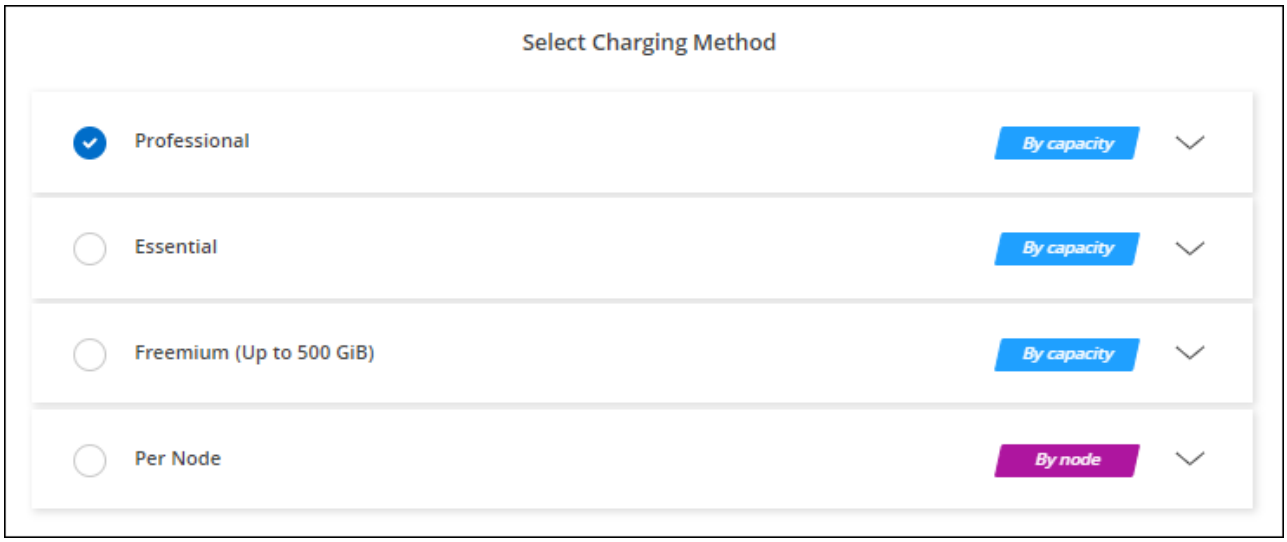
단계

1. 연간 계약을 구매하려면 NetApp 영업 담당자에게 문의하세요.

   해당 계약은 Google Cloud Marketplace에서 비공개 제안으로 제공됩니다.

   NetApp 에서 비공개 제안을 공유한 후, 시스템을 생성하는 동안 Google Cloud Marketplace에서 구독할 때 연간 요금제를 선택할 수 있습니다.

2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 메시지에 따라 Google Cloud Marketplace에서 연간 요금제를 구독하세요.
   b. Google Cloud에서 계정과 공유된 연간 요금제를 선택한 다음 *구독*을 클릭합니다.
   c. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"Google Cloud에서 Cloud Volumes ONTAP 시작하는 단계별 지침을 확인하세요." .

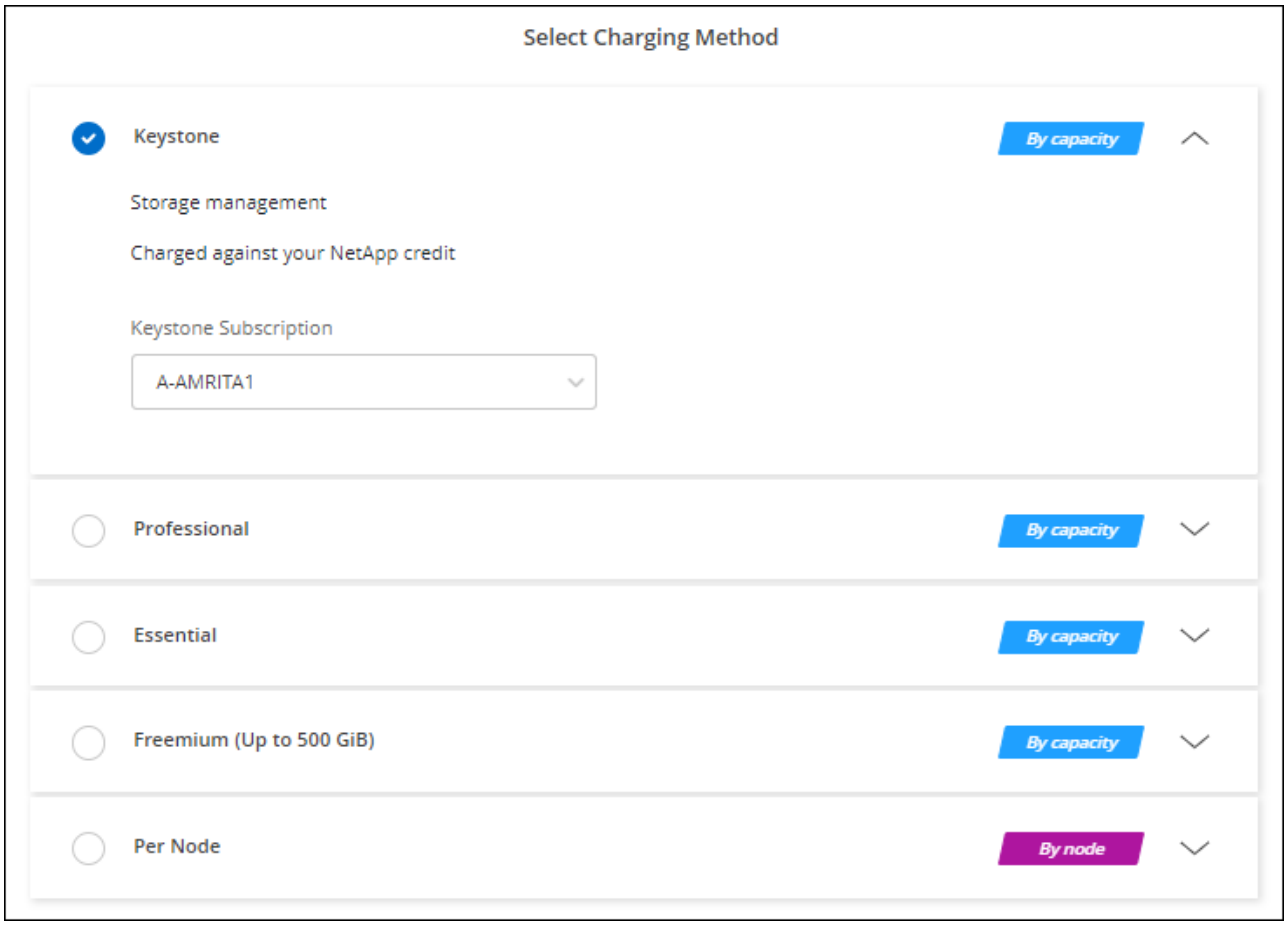
Keystone 구독

Keystone 구독은 사용량에 따라 비용을 지불하는 구독 기반 서비스입니다. "NetApp Keystone 구독에 대해 자세히 알아보세요" .

단계

1. 아직 구독이 없으신 경우, "NetApp 에 문의하세요"
2. 콘솔 사용자 계정에 하나 이상의 Keystone 구독을 승인하려면 NetApp 에 문의으로 이메일을 보내주세요.
3. NetApp 귀하의 계정을 승인한 후,"Cloud Volumes ONTAP 과 함께 사용할 구독을 연결하세요" .
4. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

    a. 청구 방법을 선택하라는 메시지가 표시되면 Keystone 구독 청구 방법을 선택하세요.



"Google Cloud에서 Cloud Volumes ONTAP 시작하는 단계별 지침을 확인하세요." .

노드 기반 라이센스

노드 기반 라이선스는 Cloud Volumes ONTAP 의 이전 세대 라이선스입니다. 노드 기반 라이선스는 NetApp (BYOL)에서 구매할 수 있으며, 특정 경우에만 라이선스를 갱신할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- "노드 기반 라이선스의 가용성 종료"
- "노드 기반 라이선스 제공 종료"
- "노드 기반 라이선스를 용량 기반 라이선스로 변환"

Google Cloud에서 Cloud Volumes ONTAP 실행

Google Cloud에서 단일 노드 구성이나 HA 쌍으로 Cloud Volumes ONTAP 실행할 수 있습니다.

시작하기 전에

시작하기 전에 다음 사항이 필요합니다.

- 정상적으로 실행 중인 NetApp Console 에이전트입니다.
  - 당신은 ~을 가져야합니다 "시스템과 연결된 콘솔 에이전트" .

- "항상 콘솔 에이전트를 실행 상태로 두어야 합니다." .
- 콘솔 에이전트와 연결된 서비스 계정 "필요한 권한이 있어야 합니다"

- 사용하려는 구성에 대한 이해.

  구성을 선택하고 관리자로부터 Google Cloud 네트워킹 정보를 얻어서 준비해야 합니다. 자세한 내용은 다음을 참조하세요."Cloud Volumes ONTAP 구성 계획" .

- Cloud Volumes ONTAP 에 대한 라이선싱을 설정하는 데 필요한 사항에 대한 이해.

  "라이선싱 설정 방법 알아보기" .

- Google Cloud API는 다음과 같아야 합니다. "프로젝트에서 활성화됨" :
  - 클라우드 배포 관리자 V2 API
  - 클라우드 로깅 API
  - 클라우드 리소스 관리자 API
  - 컴퓨트 엔진 API
  - ID 및 액세스 관리(IAM) API

Google Cloud에서 단일 노드 시스템 출시

NetApp Console 에서 시스템을 만들어 Google Cloud에서 Cloud Volumes ONTAP 시작합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. 위치 선택: *Google Cloud*와 * Cloud Volumes ONTAP*을 선택하세요.
4. 메시지가 표시되면 "콘솔 에이전트 생성" .
5. 세부 정보 및 자격 증명: 프로젝트를 선택하고, 클러스터 이름을 지정하고, 선택적으로 서비스 계정을 선택하고, 선택적으로 레이블을 추가한 다음 자격 증명을 지정합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Google Cloud VM 인스턴스의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
서비스 계정 이름	사용할 계획이라면"데이터 계층화" 또는 "NetApp Backup and Recovery" Cloud Volumes ONTAP 사용하는 경우 *서비스 계정*을 활성화하고 사전 정의된 스토리지 관리자 역할이 있는 서비스 계정을 선택해야 합니다. "서비스 계정을 만드는 방법을 알아보세요" .

필드	설명
라벨 추가	라벨은 Google Cloud 리소스에 대한 메타데이터입니다. 콘솔은 Cloud Volumes ONTAP 시스템 및 해당 시스템과 연결된 Google Cloud 리소스에 레이블을 추가합니다. 시스템을 생성할 때 사용자 인터페이스에서 최대 4개의 라벨을 추가할 수 있으며, 시스템을 생성한 후에 라벨을 더 추가할 수 있습니다. API는 시스템을 생성할 때 레이블을 4개로 제한하지 않습니다. 라벨에 대한 정보는 다음을 참조하세요. "Google Cloud 문서: 리소스 레이블 지정" .
사용자 이름과 비밀번호	이는 Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하면 ONTAP System Manager나 ONTAP CLI를 통해 Cloud Volumes ONTAP 에 연결할 수 있습니다. 기본 *admin* 사용자 이름을 유지하거나 사용자 지정 사용자 이름으로 변경하세요.
프로젝트 편집	Cloud Volumes ONTAP 저장할 프로젝트를 선택하세요. 기본 프로젝트는 콘솔의 프로젝트입니다. 드롭다운 목록에 추가 프로젝트가 표시되지 않으면 아직 서비스 계정을 다른 프로젝트와 연결하지 않은 것입니다. Google Cloud Console로 이동하여 IAM 서비스를 열고 해당 프로젝트를 선택하세요. Console에서 사용하는 역할로 서비스 계정을 해당 프로젝트에 추가합니다. 각 프로젝트에 대해 이 단계를 반복해야 합니다. 이는 콘솔에 대해 설정한 서비스 계정입니다."이 페이지에 설명된 대로" . *구독 추가*를 클릭하여 선택한 자격 증명을 구독과 연결합니다. 사용량에 따라 요금을 지불하는 Cloud Volumes ONTAP 시스템을 만들려면 Google Cloud 마켓플레이스에서 Cloud Volumes ONTAP 구독과 연결된 Google Cloud 프로젝트를 선택해야 합니다. 참조하다 "Google Cloud 자격 증명과 마켓플레이스 구독 연결" .

6. 서비스: 이 시스템에서 사용할 서비스를 선택하세요. 백업 및 복구를 선택하거나 NetApp Cloud Tiering 사용하려면 3단계에서 서비스 계정을 지정해야 합니다.

   WORM 및 데이터 계층화를 활용하려면 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 시스템을 배포해야 합니다.

7. 위치 및 연결: 시스템에 사용할 Google Cloud 지역 및 영역을 선택하고, 방화벽 정책을 선택한 다음, 데이터 계층화를 위해 Google Cloud 스토리지에 대한 네트워크 연결을 확인하십시오.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
연결성 검증	콜드 데이터를 Google Cloud Storage 버킷에 계층화하려면 Cloud Volumes ONTAP 이 있는 서브넷을 비공개 Google 액세스로 구성해야 합니다. 지침은 다음을 참조하세요. "Google Cloud 문서: 비공개 Google 액세스 구성" .

필드	설명
생성된 방화벽 정책	콘솔에서 방화벽 정책을 생성하도록 하는 경우 트래픽 허용 방법을 선택해야 합니다. • *선택한 VPC만*을 선택하는 경우 인바운드 트래픽의 소스 필터는 선택한 VPC의 서브넷 범위와 콘솔 에이전트가 있는 VPC의 서브넷 범위입니다. 이것은 권장되는 옵션입니다. • *모든 VPC*를 선택하는 경우 인바운드 트래픽의 소스 필터는 0.0.0.0/0 IP 범위입니다.
기존 방화벽 정책 사용	기존 방화벽 정책을 사용하는 경우 필수 규칙이 포함되어 있는지 확인하세요."Cloud Volumes ONTAP 의 방화벽 규칙에 대해 알아보세요"

8. 청구 방법 및 **NSS** 계정: 이 시스템에서 사용할 청구 옵션을 지정한 다음 NetApp 지원 사이트 계정을 지정하세요.
   - "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요"
   - "라이선싱 설정 방법 알아보기"
9. 사전 구성된 패키지: 패키지 중 하나를 선택하여 Cloud Volumes ONTAP 시스템을 빠르게 배포하거나 *나만의 구성 생성*을 클릭하십시오. 사전 구성된 패키지는 선택한 Cloud Volumes ONTAP 버전에 따라 다릅니다. 예를 들어 Cloud Volumes ONTAP 9.18.1 이상 버전의 경우 NetApp Console에 Hyperdisk Balanced 디스크를 포함한 C3 VM이 포함된 패키지가 표시됩니다. 워크로드 요구 사항에 따라 IOPS 및 처리량 매개변수와 같은 구성을 수정할 수 있습니다.

   패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.
10. 라이선스: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 머신 유형을 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 공급 또는 패치 릴리스가 제공되는 경우 콘솔은 버전을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.13.1을 선택하고 9.13.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리스에서 다른 릴리스로 전달되지 않습니다. 예를 들어, 9.13에서 9.14로 전달되지 않습니다.
11. 기본 스토리지 리소스: 초기 집계에 대한 설정을 선택합니다. 디스크 유형과 각 디스크의 크기입니다.

    디스크 유형은 초기 볼륨을 위한 것입니다. 이후 볼륨에는 다른 디스크 유형을 선택할 수 있습니다.

    디스크 크기는 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔이 생성하는 모든 추가 집계에 적용됩니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.

    디스크 유형 및 크기 선택에 대한 도움말은 다음을 참조하세요."Google Cloud에서 시스템 크기 조정" .
12. 플래시 캐시, 쓰기 속도 및 **WORM**:
    a. 필요한 경우 **Flash Cache***를 활성화하거나 ***Normal** 또는 **High** 쓰기 속도를 선택하십시오.

    ```
    https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-gcp.html#flash-cache-support["Flash Cache"^]와 xref:{relative_path}concept-write-speed.html["쓰기 속도"]에 대해 자세히 알아보세요.
    ```

높은 쓰기 속도 옵션을 통해 높은 쓰기 속도와 8,896바이트의 더 높은 최대 전송 단위(MTU)를 사용할 수 있습니다. 또한, 8,896의 더 높은 MTU는 배포를 위해 VPC-1, VPC-2, VPC-3을 선택해야 합니다. VPC-1, VPC-2 및 VPC-3에 대한 자세한 내용은 다음을 참조하세요. "VPC-1, VPC-2 및 VPC-3에 대한 규칙" .

b. 원하는 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

Cloud Volumes ONTAP 버전 9.7 이하에서 데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로 되돌리거나 다운그레이드하는 것이 차단됩니다.

"WORM 스토리지에 대해 자세히 알아보세요" .

a. WORM 저장소를 활성화하는 경우 보존 기간을 선택하세요.

13. **Google Cloud Platform**의 데이터 계층화: 초기 집계에서 데이터 계층화를 활성화할지 여부를 선택하고, 계층화된 데이터에 대한 스토리지 클래스를 선택한 다음, 사전 정의된 스토리지 관리자 역할(Cloud Volumes ONTAP 9.7 이상에 필요)이 있는 서비스 계정을 선택하거나, Google Cloud 계정(Cloud Volumes ONTAP 9.6에 필요)을 선택합니다.

다음 사항에 유의하세요.

- 콘솔은 Cloud Volumes ONTAP 인스턴스에 서비스 계정을 설정합니다. 이 서비스 계정은 Google Cloud Storage 버킷에 대한 데이터 계층화 권한을 제공합니다. 계층화 서비스 계정의 사용자로 콘솔 에이전트 서비스 계정을 반드시 추가해야 합니다. 그렇지 않으면 콘솔에서 해당 계정을 선택할 수 없습니다.
- Google Cloud 계정 추가에 대한 도움말은 다음을 참조하세요. "9.6을 사용하여 데이터 계층화를 위한 Google Cloud 계정 설정 및 추가" .
- 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
- 데이터 계층화를 비활성화한 경우 후속 애그리게이트에서 다시 활성화할 수 있지만, 시스템을 종료하고 Google Cloud Console에서 서비스 계정을 추가해야 합니다.

"데이터 계층화에 대해 자세히 알아보세요" .

14. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

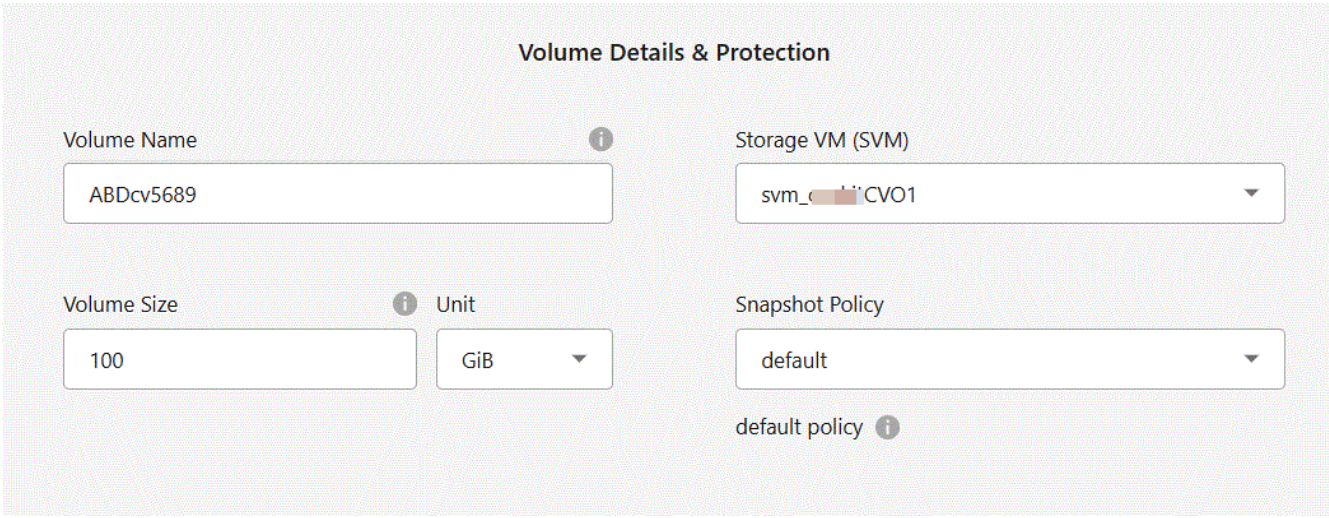
"지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝을 활성화하는지 여부에 따라 크게 달라집니다. 씬 프로비저닝을 활성화하면 현재 사용 가능한 물리적 저장소보다 큰 볼륨을 만들 수 있습니다.
액세스 제어(NFS에만 해당)	내보내기 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 콘솔은 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.

필드	설명
권한 및 사용자/그룹(CIFS에만 해당)	이러한 필드를 사용하면 사용자 및 그룹의 공유 액세스 수준(액세스 제어 목록 또는 ACL이라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자나 그룹, 또는 UNIX 사용자나 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사 정책은 NetApp 스냅샷 복사본이 자동으로 생성되는 빈도와 수를 지정합니다. NetApp 스냅샷 복사본은 성능에 영향을 미치지 않고 최소한의 저장 공간만 필요한 특정 시점의 파일 시스템 이미지입니다. 기본 정책을 선택하거나 아무것도 선택하지 않을 수 있습니다. 일시적인 데이터의 경우 '없음'을 선택할 수 있습니다. 예를 들어 Microsoft SQL Server의 경우 tempdb를 선택합니다.
고급 옵션(NFS에만 해당)	볼륨에 대한 NFS 버전을 선택합니다: NFSv3 또는 NFSv4.
이니시에이터 그룹 및 IQN(iSCSI에만 해당)	iSCSI 스토리지 대상은 LUN(논리 단위)이라고 하며 호스트에 표준 블록 장치로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름 테이블이며, 어떤 이니시에이터가 어떤 LUN에 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 컨버지드 네트워크 어댑터(CNA) 또는 전용 호스트 버스 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 정규화된 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후, "IQN을 사용하여 호스트에서 LUN에 연결합니다." .

다음 이미지는 볼륨 생성 마법사의 첫 번째 페이지를 보여줍니다.



15. **CIFS** 설정: CIFS 프로토콜을 선택한 경우 CIFS 서버를 설정합니다.

필드	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인의 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다. Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.

필드	설명
도메인에 가입할 수 있는 권한이 있는 자격 증명	AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.
CIFS 서버 NetBIOS 이름	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Cloud Volumes ONTAP 의 AD 서버로 Google Managed Microsoft AD를 구성하려면 이 필드에 *OU=Computers,OU=Cloud*를 입력합니다.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 문서: Google Managed Microsoft AD의 조직 단위"^]
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 대부분의 경우 도메인은 AD 도메인과 동일합니다.
NTP 서버	Active Directory DNS를 사용하여 NTP 서버를 구성하려면 *Active Directory 도메인 사용*을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 자세한 내용은 다음을 참조하세요. "NetApp Console 자동화 문서" 자세한 내용은. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

16. 사용 프로필, 디스크 유형 및 계층화 정책: 필요한 경우 스토리지 효율성 기능을 활성화할지 여부를 선택하고 볼륨 계층화 정책을 변경합니다.

    자세한 내용은 다음을 참조하세요."볼륨 사용 프로필을 선택하세요" ,"데이터 계층화 개요" , 그리고 "KB: CVO에서는 어떤 인라인 스토리지 효율성 기능이 지원되나요?"

17. 검토 및 승인: 선택 사항을 검토하고 확인합니다.

    a. 구성에 대한 세부 정보를 검토하세요.

    b. *자세한 정보*를 클릭하면 콘솔에서 구매할 지원 및 Google Cloud 리소스에 대한 세부 정보를 검토할 수 있습니다.

    c. 이해합니다... 확인란을 선택하세요.

    d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 시스템을 배포합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템 배포 중 문제가 발생하면 실패 메시지를 검토하세요. 시스템을 선택하고 *환경 다시 만들기*를 클릭할 수도 있습니다.

추가 도움말을 보려면 다음으로 이동하세요. "NetApp Cloud Volumes ONTAP 지원" .

당신이 완료한 후

- CIFS 공유를 프로비저닝한 경우 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 ONTAP 시스템 관리자나 ONTAP CLI를 사용하세요.

  할당량을 사용하면 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적할 수 있습니다.

배포 프로세스가 완료된 후에는 Google Cloud 포털에서 시스템에서 생성된 Cloud Volumes ONTAP 구성(예: 시스템 태그 및 Google Cloud 리소스에 설정된 레이블)을 수정하지 마십시오. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

Google Cloud에서 HA 쌍 시작

Google Cloud에서 Cloud Volumes ONTAP 시작하기 위한 시스템을 콘솔에서 만듭니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *저장소 > 시스템*을 클릭하고 화면의 지시를 따르세요.
3. 위치 선택: *Google Cloud*와 * Cloud Volumes ONTAP HA*를 선택합니다.
4. 세부 정보 및 자격 증명: 프로젝트를 선택하고, 클러스터 이름을 지정하고, 선택적으로 서비스 계정을 선택하고, 선택적으로 레이블을 추가한 다음 자격 증명을 지정합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Google Cloud VM 인스턴스의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
서비스 계정 이름	사용할 계획이라면"NetApp Cloud Tiering" 또는 "백업 및 복구" 서비스를 사용하려면 서비스 계정 스위치를 활성화한 다음 미리 정의된 스토리지 관리자 역할이 있는 서비스 계정을 선택해야 합니다.
라벨 추가	라벨은 Google Cloud 리소스에 대한 메타데이터입니다. 콘솔은 Cloud Volumes ONTAP 시스템 및 해당 시스템과 연결된 Google Cloud 리소스에 레이블을 추가합니다. 시스템을 생성할 때 사용자 인터페이스에서 최대 4개의 라벨을 추가할 수 있으며, 시스템을 생성한 후에 라벨을 더 추가할 수 있습니다. API는 시스템을 생성할 때 레이블을 4개로 제한하지 않습니다. 라벨에 대한 정보는 다음을 참조하세요. "Google Cloud 문서: 리소스 레이블 지정" .
사용자 이름과 비밀번호	이는 Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하면 ONTAP System Manager나 ONTAP CLI를 통해 Cloud Volumes ONTAP 에 연결할 수 있습니다. 기본 *admin* 사용자 이름을 유지하거나 사용자 지정 사용자 이름으로 변경하세요.

필드	설명
프로젝트 편집	Cloud Volumes ONTAP를 배치할 프로젝트를 선택하십시오. 드롭다운 목록에 추가 프로젝트가 표시되지 않으면 아직 서비스 계정을 다른 프로젝트와 연결하지 않은 것입니다. Google Cloud Console로 이동하여 IAM 서비스를 열고 해당 프로젝트를 선택하세요. Console에서 사용하는 역할로 서비스 계정을 해당 프로젝트에 추가합니다. 각 프로젝트에 대해 이 단계를 반복해야 합니다. 이는 콘솔에 대해 설정한 서비스 계정입니다."이 페이지에 설명된 대로" . *구독 추가*를 클릭하여 선택한 자격 증명을 구독과 연결합니다. 사용량에 따라 요금을 지불하는 Cloud Volumes ONTAP 시스템을 만들려면 Google Cloud Marketplace에서 Cloud Volumes ONTAP 구독과 연결된 Google Cloud 프로젝트를 선택해야 합니다. 참조하다 "Google Cloud 자격 증명과 마켓플레이스 구독 연결" .

5. 서비스: 이 시스템에서 사용할 서비스를 선택하세요. 백업 및 복구를 선택하거나 NetApp Cloud Tiering 사용하려면 3단계에서 서비스 계정을 지정해야 합니다.

   WORM 및 데이터 계층화를 활용하려면 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 시스템을 배포해야 합니다.

6. **HA** 배포 모델: HA 구성에 대해 여러 영역(권장) 또는 단일 영역을 선택합니다. 그런 다음 지역과 영역을 선택합니다.

   "HA 배포 모델에 대해 자세히 알아보세요" .

7. 연결성: HA 구성을 위해 4개의 다른 VPC를 선택하고, 각 VPC에 서브넷을 선택한 다음 방화벽 정책을 선택합니다.

   "네트워킹 요구 사항에 대해 자세히 알아보세요" .

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
생성된 정책	콘솔에서 방화벽 정책을 생성하도록 하는 경우 트래픽 허용 방법을 선택해야 합니다. • *선택한 VPC만*을 선택하는 경우 인바운드 트래픽의 소스 필터는 선택한 VPC의 서브넷 범위와 콘솔 에이전트가 있는 VPC의 서브넷 범위입니다. 이것은 권장되는 옵션입니다. • *모든 VPC*를 선택하는 경우 인바운드 트래픽의 소스 필터는 0.0.0.0/0 IP 범위입니다.
기존 사용	기존 방화벽 정책을 사용하는 경우 필요한 규칙이 포함되어 있는지 확인하세요. "Cloud Volumes ONTAP 의 방화벽 규칙에 대해 알아보세요" .

8. 청구 방법 및 **NSS** 계정: 이 시스템에서 사용할 청구 옵션을 지정한 다음 NetApp 지원 사이트 계정을 지정하세요.

- "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요" .
- "라이선싱 설정 방법 알아보기" .

9. 사전 구성된 패키지: Cloud Volumes ONTAP 시스템을 빠르게 배포하려면 패키지 중 하나를 선택하거나 *내 구성 만들기*를 클릭하세요.

   패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.

10. 라이선스: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 머신 유형을 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 공급 또는 패치 릴리스가 제공되는 경우 콘솔은 버전을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.13.1을 선택하고 9.13.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리스에서 다른 릴리스로 전달되지 않습니다(예: 9.13에서 9.14로 전달).

11. 기본 스토리지 리소스: 초기 집계에 대한 설정을 선택합니다. 디스크 유형과 각 디스크의 크기입니다.

    디스크 유형은 초기 볼륨을 위한 것입니다. 이후 볼륨에는 다른 디스크 유형을 선택할 수 있습니다.

    디스크 크기는 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔이 생성하는 모든 추가 집계에 적용됩니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.

    디스크 유형 및 크기 선택에 대한 도움말은 다음을 참조하세요."Google Cloud에서 시스템 크기 조정" .

12. 플래시 캐시, 쓰기 속도 및 **WORM**:

    a. 필요한 경우 **Flash Cache***를 활성화하거나 ***Normal** 또는 **High** 쓰기 속도를 선택하십시오.

    ```
    https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-gcp.html#flash-cache-support["Flash Cache"^]와 xref:{relative_path}concept-write-speed.html["쓰기 속도"]에 대해 자세히 알아보세요.
    ```

    높음 쓰기 속도 옵션을 사용하면 n2-standard-16, n2-standard-32, n2-standard-48 및 n2-standard-64 인스턴스 유형에서 높은 쓰기 속도와 8,896바이트의 더 높은 최대 전송 단위(MTU)를 사용할 수 있습니다. 또한, 8,896의 더 높은 MTU는 배포를 위해 VPC-1, VPC-2, VPC-3을 선택해야 합니다. 높은 쓰기 속도와 8,896의 MTU는 기능에 따라 달라지며 구성된 인스턴스 내에서 개별적으로 비활성화할 수 없습니다. VPC-1, VPC-2 및 VPC-3에 대한 자세한 내용은 다음을 참조하세요. "VPC-1, VPC-2 및 VPC-3에 대한 규칙" .

    b. 원하는 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

    Cloud Volumes ONTAP 버전 9.7 이하에서 데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로 되돌리거나 다운그레이드하는 것이 차단됩니다.

    "WORM 스토리지에 대해 자세히 알아보세요" .

    a. WORM 저장소를 활성화하는 경우 보존 기간을 선택하세요.

13. **Google Cloud**의 데이터 계층화: 초기 집계에서 데이터 계층화를 활성화할지 여부를 선택하고, 계층화된 데이터에 대한 스토리지 클래스를 선택한 다음, 사전 정의된 스토리지 관리자 역할이 있는 서비스 계정을 선택합니다.

    다음 사항에 유의하세요.

    - 콘솔은 Cloud Volumes ONTAP 인스턴스에 서비스 계정을 설정합니다. 이 서비스 계정은 Google Cloud Storage 버킷에 대한 데이터 계층화 권한을 제공합니다. 계층화 서비스 계정의 사용자로 콘솔 에이전트 서비스 계정을 반드시 추가해야 합니다. 그렇지 않으면 콘솔에서 해당 계정을 선택할 수 없습니다.
    - 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
    - 데이터 계층화를 비활성화한 경우 후속 애그리게이트에서 다시 활성화할 수 있지만, 시스템을 종료하고 Google Cloud Console에서 서비스 계정을 추가해야 합니다.

      "데이터 계층화에 대해 자세히 알아보세요" .

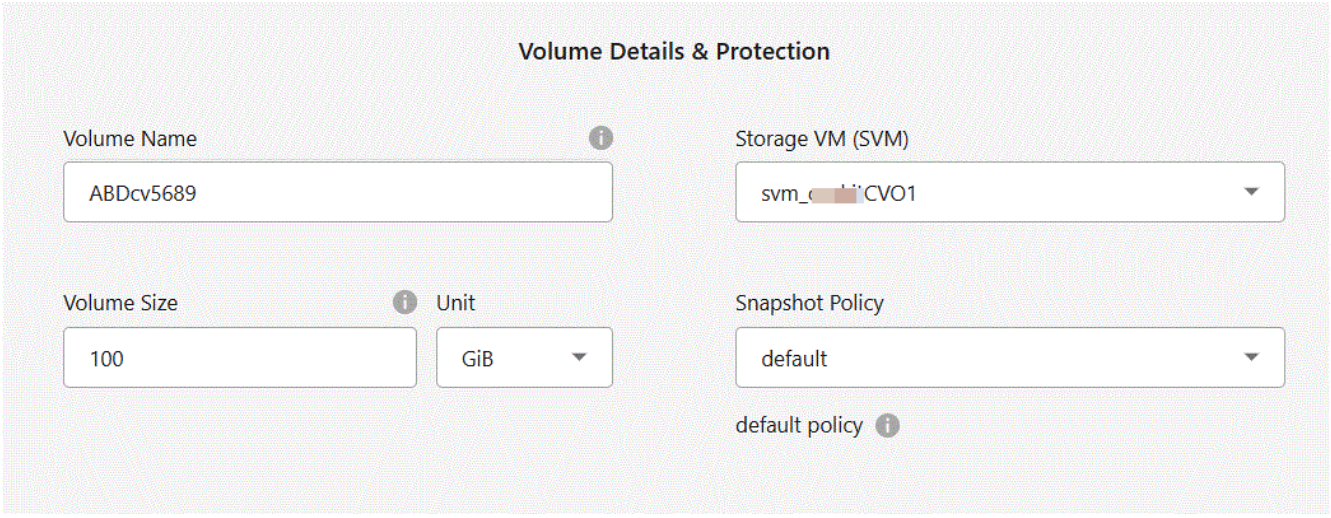
14. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

    "지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

    이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝을 활성화하는지 여부에 따라 크게 달라집니다. 씬 프로비저닝을 활성화하면 현재 사용 가능한 물리적 저장소보다 큰 볼륨을 만들 수 있습니다.
액세스 제어(NFS에만 해당)	내보내기 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 콘솔은 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS에만 해당)	이러한 필드를 사용하면 사용자 및 그룹의 공유 액세스 수준(액세스 제어 목록 또는 ACL이라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자나 그룹, 또는 UNIX 사용자나 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사 정책은 NetApp 스냅샷 복사본이 자동으로 생성되는 빈도와 수를 지정합니다. NetApp 스냅샷 복사본은 성능에 영향을 미치지 않고 최소한의 저장 공간만 필요한 특정 시점의 파일 시스템 이미지입니다. 기본 정책을 선택하거나 아무것도 선택하지 않을 수 있습니다. 일시적인 데이터의 경우 '없음'을 선택할 수 있습니다. 예를 들어 Microsoft SQL Server의 경우 tempdb를 선택합니다.
고급 옵션(NFS에만 해당)	볼륨에 대한 NFS 버전을 선택합니다: NFSv3 또는 NFSv4.
이니시에이터 그룹 및 IQN(iSCSI에만 해당)	iSCSI 스토리지 대상은 LUN(논리 단위)이라고 하며 호스트에 표준 블록 장치로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름 테이블이며, 어떤 이니시에이터가 어떤 LUN에 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 컨버지드 네트워크 어댑터(CNA) 또는 전용 호스트 버스 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 정규화된 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후, "IQN을 사용하여 호스트에서 LUN에 연결합니다." .

    다음 이미지는 볼륨 생성 마법사의 첫 번째 페이지를 보여줍니다.



15. **CIFS** 설정: CIFS 프로토콜을 선택한 경우 CIFS 서버를 설정합니다.

필드	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인의 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다. Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.
도메인에 가입할 수 있는 권한이 있는 자격 증명	AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.
CIFS 서버 NetBIOS 이름	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Cloud Volumes ONTAP 의 AD 서버로 Google Managed Microsoft AD를 구성하려면 이 필드에 *OU=Computers,OU=Cloud*를 입력합니다.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 문서: Google Managed Microsoft AD의 조직 단위"^]
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 대부분의 경우 도메인은 AD 도메인과 동일합니다.
NTP 서버	Active Directory DNS를 사용하여 NTP 서버를 구성하려면 *Active Directory 도메인 사용*을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 를 참조하세요 "NetApp Console 자동화 문서" 자세한 내용은. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

16. 사용 프로필, 디스크 유형 및 계층화 정책: 필요한 경우 스토리지 효율성 기능을 활성화할지 여부를 선택하고 볼륨 계층화 정책을 변경합니다.

    자세한 내용은 다음을 참조하세요."볼륨 사용 프로필을 선택하세요" ,"데이터 계층화 개요" , 그리고 "KB: CVO에서는 어떤 인라인 스토리지 효율성 기능이 지원되나요?"

17. 검토 및 승인: 선택 사항을 검토하고 확인합니다.

    a. 구성에 대한 세부 정보를 검토하세요.

    b. *자세한 정보*를 클릭하면 콘솔에서 구매할 지원 및 Google Cloud 리소스에 대한 세부 정보를 검토할 수 있습니다.

    c. 이해합니다... 확인란을 선택하세요.

    d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 시스템을 배포합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템 배포 중 문제가 발생하면 실패 메시지를 검토하세요. 시스템을 선택하고 *환경 다시 만들기*를 클릭할 수도 있습니다.

추가 도움말을 보려면 다음으로 이동하세요. "NetApp Cloud Volumes ONTAP 지원" .

당신이 완료한 후

- CIFS 공유를 프로비저닝한 경우 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 ONTAP 시스템 관리자나 ONTAP CLI를 사용하세요.

  할당량을 사용하면 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적할 수 있습니다.

> 배포 프로세스가 완료된 후에는 Google Cloud 포털에서 시스템에서 생성된 Cloud Volumes ONTAP 구성(예: 시스템 태그 및 Google Cloud 리소스에 설정된 레이블)을 수정하지 마십시오. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

관련 링크

- "Google Cloud에서 Cloud Volumes ONTAP 구성 계획"

Google Cloud Platform 이미지 검증

Cloud Volumes ONTAP 에서 **Google Cloud** 이미지가 검증되는 방식을 알아보세요**.**

Google Cloud 이미지 검증은 향상된 NetApp 보안 요구 사항을 준수합니다. 이 작업을 위해 특별히 생성된 개인 키를 사용하여 이미지에 서명하는 방식으로 이미지를 생성하는 스크립트가 변경되었습니다. Google Cloud 이미지의 무결성은 다음을 통해 다운로드할 수 있는 서명된 다이제스트 및 Google Cloud 공개 인증서를 사용하여 확인할 수 있습니다. "NSS" 특정 릴리스에 대한.

> Google Cloud 이미지 검증은 Cloud Volumes ONTAP 소프트웨어 버전 9.13.0 이상에서 지원됩니다.

Google Cloud 이미지를 **Cloud Volumes ONTAP** 용 **RAW** 포맷으로 변환

새로운 인스턴스, 업그레이드를 배포하는 데 사용되는 이미지 또는 기존 이미지에서 사용되는

이미지는 다음을 통해 클라이언트와 공유됩니다. "NetApp 지원 사이트(NSS)" . 서명된 다이제스트와 인증서는 NSS 포털을 통해 다운로드할 수 있습니다. NetApp 지원팀에서 공유한 이미지에 해당하는 올바른 릴리스에 대한 다이제스트와 인증서를 다운로드하고 있는지 확인하세요. 예를 들어, 9.13.0 이미지에는 9.13.0 서명된 다이제스트와 NSS에서 사용할 수 있는 인증서가 포함됩니다.

왜 이 단계가 필요한가요?

Google Cloud의 이미지는 직접 다운로드할 수 없습니다. 서명된 다이제스트와 인증서에 대해 이미지를 검증하려면 두 파일을 비교하고 이미지를 다운로드할 수 있는 메커니즘이 필요합니다. 이를 위해서는 이미지를 disk.raw 형식으로 내보내거나 변환하고 그 결과를 Google Cloud의 스토리지 버킷에 저장해야 합니다. disk.raw 파일은 이 과정에서 tar와 gzip으로 압축됩니다.

사용자/서비스 계정에는 다음을 수행할 수 있는 권한이 필요합니다.

- Google 스토리지 버킷에 액세스
- Google Storage 버킷에 쓰기
- 클라우드 빌드 작업 생성(내보내기 프로세스 중 사용)
- 원하는 이미지에 접근
- 이미지 내보내기 작업 만들기

이미지를 확인하려면 disk.raw 형식으로 변환한 다음 다운로드해야 합니다.

Google Cloud 명령줄을 사용하여 **Google Cloud** 이미지를 내보냅니다.

이미지를 Cloud Storage로 내보내는 가장 좋은 방법은 다음을 사용하는 것입니다. "gcloud compute 이미지 내보내기 명령" . 이 명령은 제공된 이미지를 가져와서 tar와 gzip으로 압축된 disk.raw 파일로 변환합니다. 생성된 파일은 대상 URL에 저장되며, 확인을 위해 다운로드할 수 있습니다.

이 작업을 실행하려면 사용자/계정에 원하는 버킷에 액세스하고 쓰기 권한이 있어야 하며, 이미지를 내보내고, 클라우드 빌드(Google에서 이미지를 내보내는 데 사용)에 대한 권한이 있어야 합니다.

gcloud를 사용하여 **Google Cloud** 이미지 내보내기

클릭하여 표시

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

압축 파일 추출

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

Google Cloud를 통해 이미지를 내보내는 방법에 대한 자세한 내용은 다음을 참조하세요. "이미지 내보내기에 대한 Google Cloud 문서" .

이미지 서명 검증

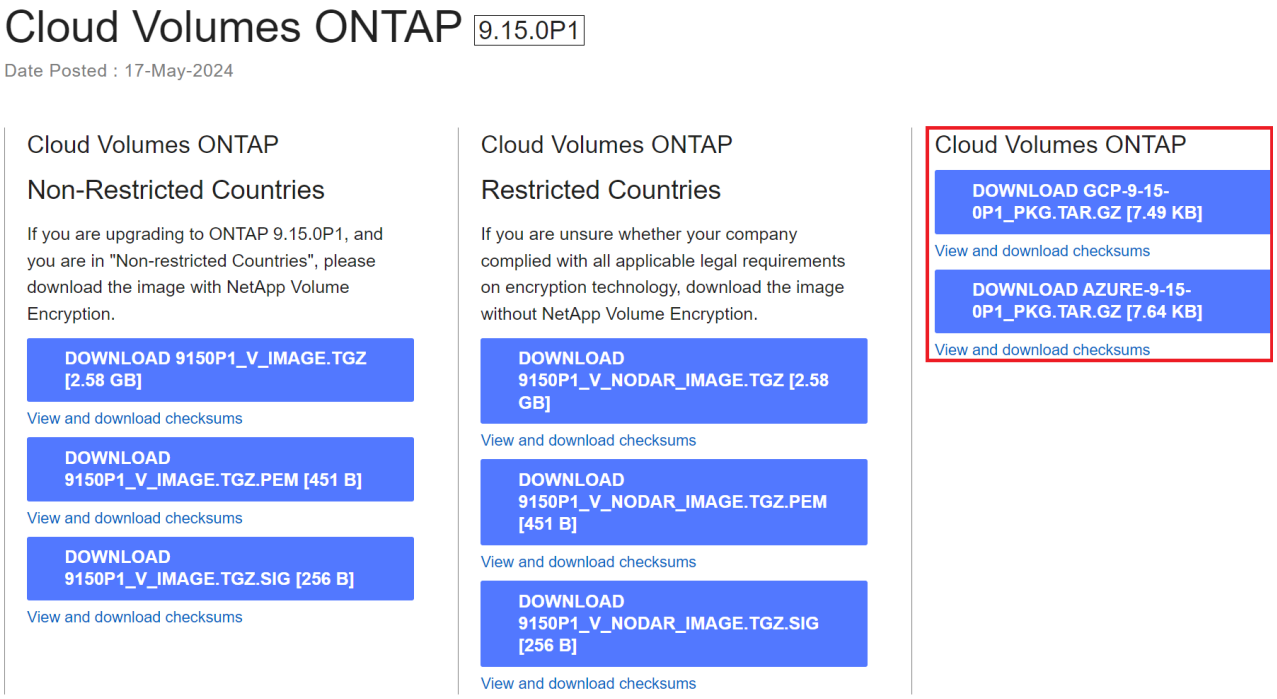
Cloud Volumes ONTAP 에 대한 **Google Cloud** 이미지 서명 확인

내보낸 Google Cloud 서명 이미지를 확인하려면 NSS에서 이미지 다이제스트 파일을 다운로드하여 disk.raw 파일과 다이제스트 파일 내용을 검증해야 합니다.

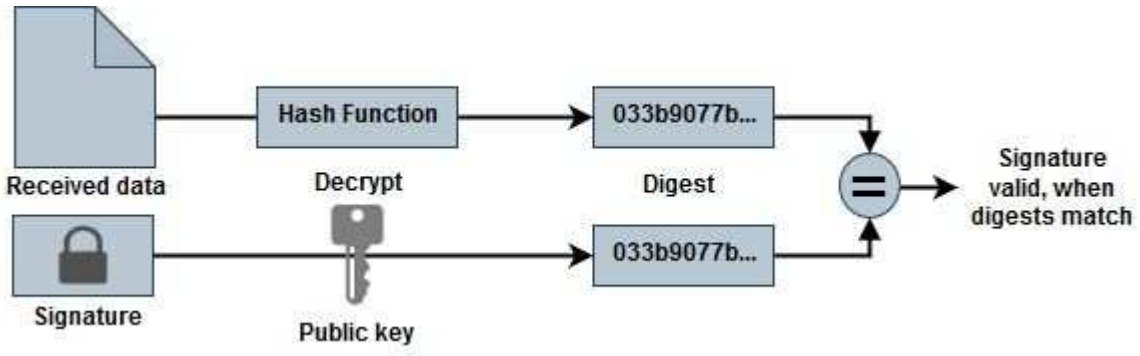
서명된 이미지 검증 워크플로 요약

다음은 Google Cloud 서명 이미지 검증 워크플로 프로세스에 대한 개요입니다.

- 에서 "NSS" 다음 파일이 포함된 Google Cloud 보관 파일을 다운로드하세요.
  - 서명된 다이제스트(.sig)
  - 공개 키(.pem)를 포함하는 인증서
  - 인증서 체인(.pem)



- 변환된 disk.raw 파일을 다운로드하세요
- 인증서 체인을 사용하여 인증서 검증
- 공개 키가 포함된 인증서를 사용하여 서명된 다이제스트를 검증합니다.
  - 공개 키를 사용하여 서명된 다이제스트를 복호화하여 이미지 파일의 다이제스트를 추출합니다.
  - 다운로드한 disk.raw 파일의 다이제스트를 만듭니다.
  - 검증을 위해 두 개의 다이제스트 파일을 비교합니다.



OpenSSL을 사용하여 **Cloud Volumes ONTAP** 에 대한 **Google Cloud** 이미지 **disk.raw** 파일을 확인합니다**.**

Google Cloud에서 다운로드한 disk.raw 파일을 다이제스트 파일 콘텐츠와 비교하여 확인할 수 있습니다. "NSS" OpenSSL을 사용합니다.

이미지를 검증하는 OpenSSL 명령은 Linux, macOS, Windows 시스템과 호환됩니다.

단계

1. OpenSSL을 사용하여 인증서를 확인합니다.

클릭하여 표시

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
          e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
          22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
          38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
          fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
          bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. 다운로드한 disk.raw 파일, 서명, 인증서를 디렉토리에 넣습니다.
3. OpenSSL을 사용하여 인증서에서 공개 키를 추출합니다.
4. 추출된 공개 키를 사용하여 서명을 복호화하고 다운로드한 disk.raw 파일의 내용을 확인합니다.

클릭하여 표시

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Cloud Volumes ONTAP 사용

라이선스 관리

Cloud Volumes ONTAP 에 대한 용량 기반 라이선싱 관리

NetApp Console 에서 용량 기반 라이선스를 관리하여 NetApp 계정에 Cloud Volumes ONTAP 시스템에 필요한 용량이 충분한지 확인하세요.

_용량 기반 라이선스_를 사용하면 TiB 용량당 Cloud Volumes ONTAP 비용을 지불할 수 있습니다.

NetApp Console 에서 용량 기반 Cloud Volumes ONTAP 라이선스를 관리할 수 있습니다.

콘솔에서 관리되는 제품과 서비스의 실제 사용량과 측정은 항상 GiB와 TiB로 계산되지만, GB/GiB와 TB/TiB라는 용어도 서로 바꿔 사용됩니다. 이는 Cloud Marketplace 목록, 가격 견적, 목록 설명 및 기타 지원 문서에 반영됩니다.

"Cloud Volumes ONTAP 라이선스에 대해 자세히 알아보세요" .

NetApp Console 에 라이센스가 추가되는 방식

NetApp 영업 담당자로부터 라이선스를 구매하면 NetApp 일련 번호와 추가 라이선스 세부 정보가 포함된 이메일을 보내드립니다.

그 사이에 콘솔은 NetApp 지원 사이트 계정과 연결된 라이선스에 대한 세부 정보를 얻기 위해 NetApp 라이선스 서비스에 자동으로 쿼리를 보냅니다. 오류가 없으면 라이센스를 추가합니다.

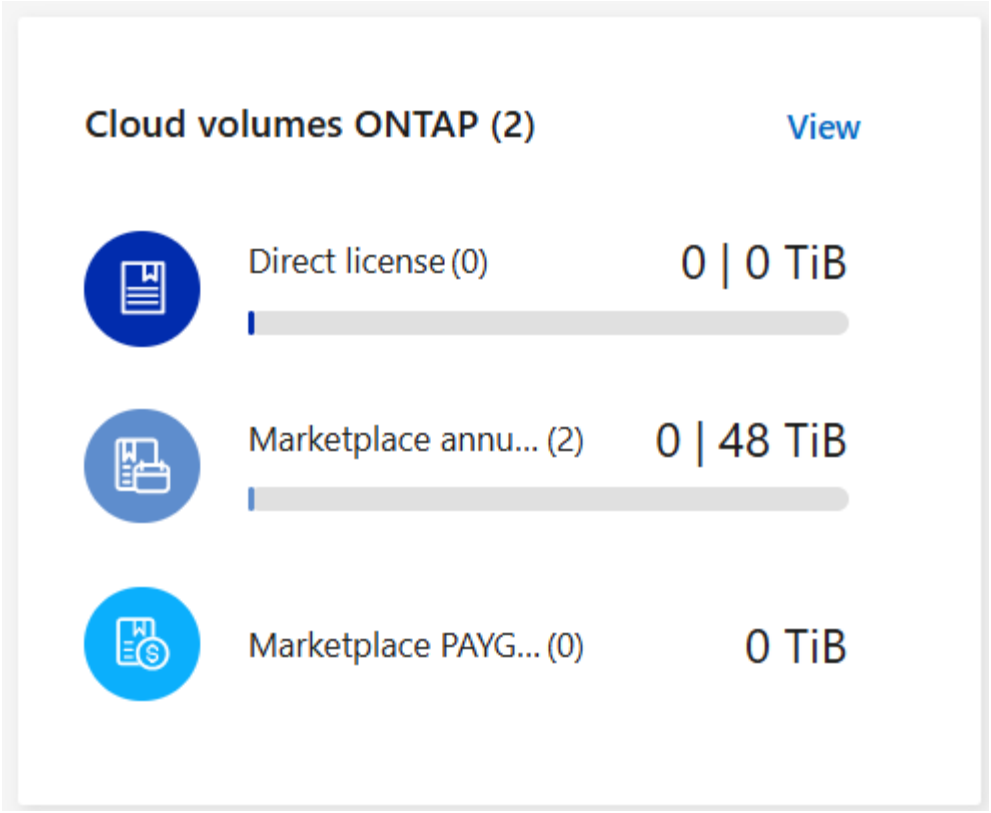
콘솔에서 라이선스를 추가할 수 없는 경우 수동으로 추가해야 합니다. 예를 들어, 콘솔 에이전트가 인터넷 접속이 불가능한 위치에 설치된 경우 라이선스를 직접 추가해야 합니다. "구매한 라이선스를 계정에 추가하는 방법을 알아보세요." .

계정에서 사용된 용량을 확인하세요

콘솔은 계정에서 사용된 총 용량과 라이선스 패키지별로 사용된 용량을 보여줍니다. 이를 통해 요금이 어떻게 청구되는지, 추가 용량을 구매해야 하는지 파악하는 데 도움이 될 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭에서 Cloud Volumes ONTAP 타일은 계정에 대해 현재 프로비저닝된 용량을 표시합니다.



- _직접 라이선스_는 NetApp 계정의 모든 Cloud Volumes ONTAP 시스템에 프로비저닝된 총 용량입니다. 요금은 볼륨 내의 로컬, 사용, 저장 또는 유효 공간에 관계없이 각 볼륨의 프로비저닝된 크기를 기준으로 부과됩니다.
- _연간 계약_은 NetApp 에서 구매한 총 라이선스 용량(BYOL(자체 라이선스 사용) 또는 마켓플레이스 계약)입니다.
- _PAYGO_는 클라우드 마켓플레이스 구독을 사용하여 프로비저닝된 총 용량입니다. PAYGO를 통한 요금 청구는 사용된 용량이 라이선스 용량보다 높거나 콘솔에서 사용 가능한 BYOL 라이선스가 없는 경우에만 사용됩니다.

3. *보기*를 선택하면 각 라이선스 패키지의 사용된 용량을 확인할 수 있습니다.
4. 구매한 각 패키지 라이선스에 대한 세부 정보를 보려면 라이선스 탭을 선택하세요.

   Essentials 패키지에 표시되는 용량을 더 잘 이해하려면 충전 방식을 알아야 합니다. "Essentials 패키지 요금 청구에 대해 알아보세요" .

5. 라이선스 소비 모델에 따른 소비 용량을 확인하려면 구독 탭을 선택하세요. 이 탭에는 PAYGO 및 연간 계약 라이선스가 모두 포함되어 있습니다.

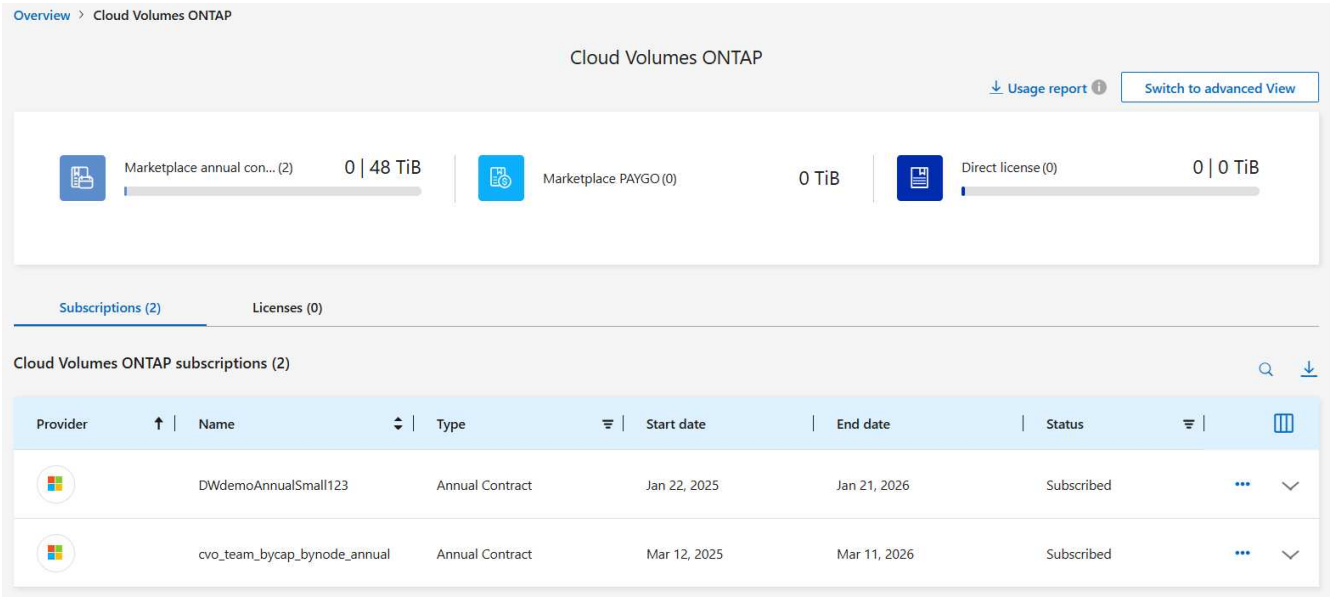
   현재 보고 있는 조직과 연관된 구독만 볼 수 있습니다.

6. 구독에 대한 정보를 볼 때 표에 있는 세부 정보와 상호 작용할 수 있습니다. 더 자세한 내용을 보려면 행을 확장하세요.
   - 선택하다 표에 어떤 열을 표시할지 선택합니다. 기본적으로 기간 및 자동 갱신 열은 나타나지 않습니다. 자동 갱신 열에는 Azure 계약에 대한 갱신 정보만 표시됩니다.

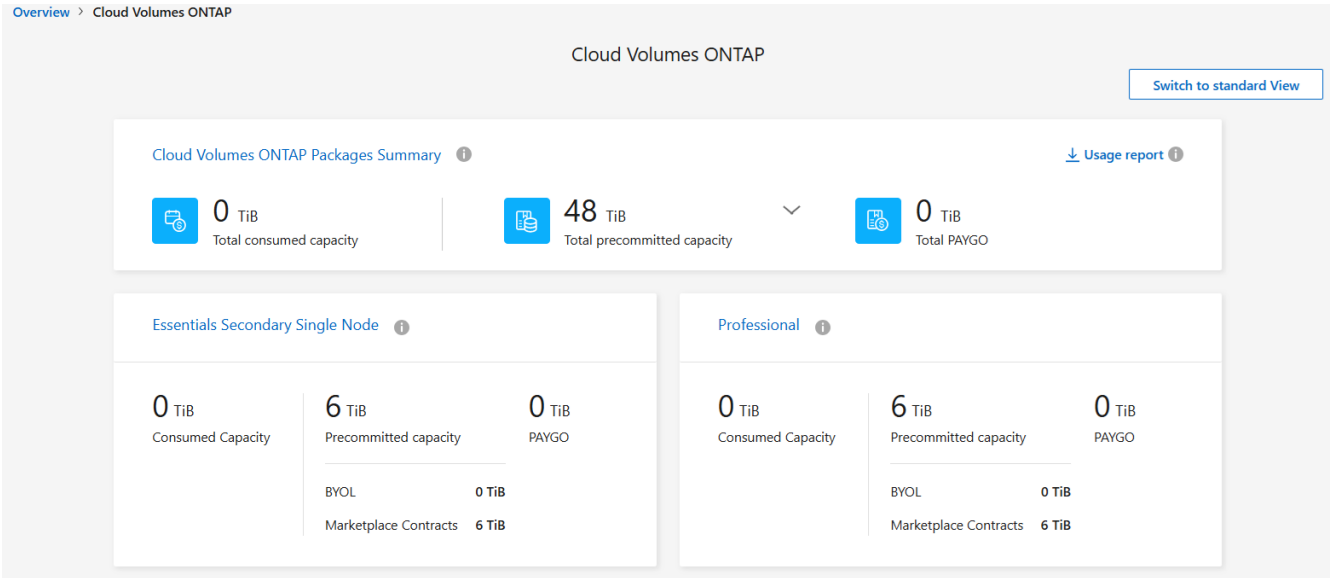
패키지 세부 정보 보기

Cloud Volumes ONTAP 페이지에서 레거시 모드로 전환하면 패키지별로 사용된 용량에 대한 세부 정보를 볼 수 있습니다.

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭에서 Cloud Volumes ONTAP 타일은 계정에 대해 현재 프로비저닝된 용량을 표시합니다.
3. *보기*를 선택하여 각 라이선스 패키지에 대해 제공된 용량을 확인하세요.
4. *고급 보기로 전환*을 선택하세요.



5. 원하는 패키지의 세부 정보를 확인하세요.



충전 방법 변경

용량 기반 라이선싱은 패키지 형태로 제공됩니다. Cloud Volumes ONTAP 시스템을 만들면 비즈니스 요구 사항에 따라 여러 가지 라이선스 패키지 중에서 선택할 수 있습니다. 시스템을 만든 후에 요구 사항이 변경되면 언제든지 패키지를

변경할 수 있습니다. 예를 들어, Essentials 패키지에서 Professional 패키지로 변경할 수 있습니다.

"용량 기반 라이선싱 패키지에 대해 자세히 알아보세요" .

이 작업에 관하여

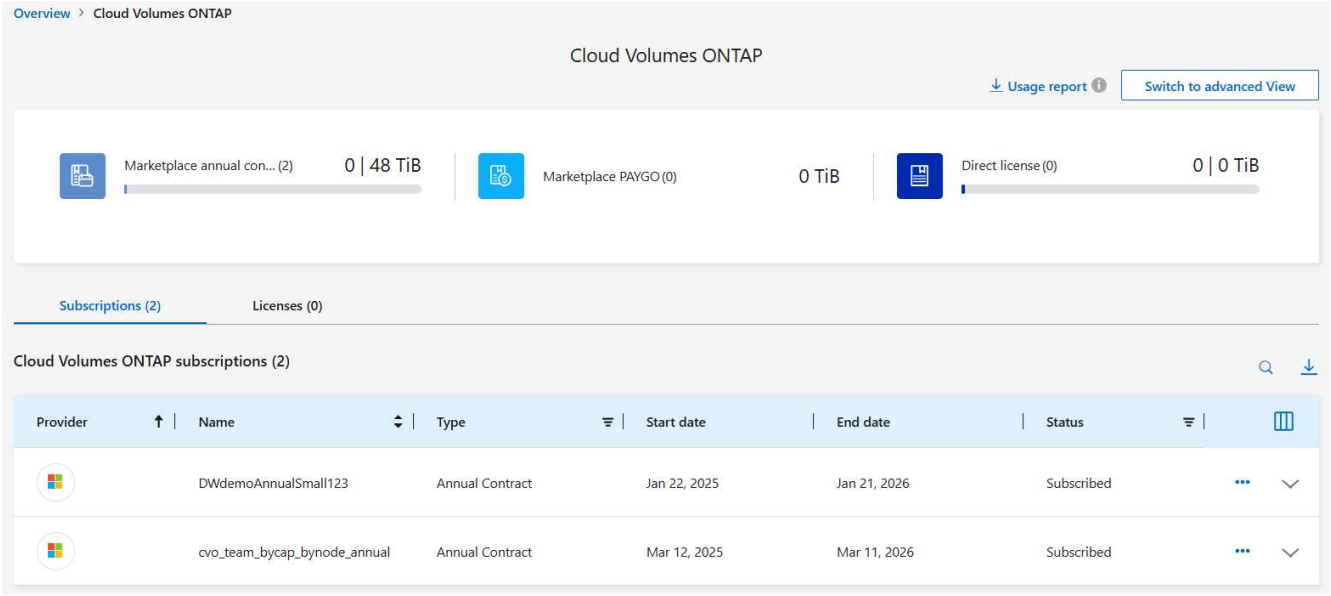
- 요금 청구 방식을 변경해 NetApp (BYOL)에서 구매한 라이선스를 통해 요금이 청구되는지, 아니면 클라우드 공급업체의 마켓플레이스에서 사용량에 따라 지불하는(PAYGO) 구독을 통해 요금이 청구되는지에는 영향을 미치지 않습니다.

  콘솔은 항상 라이선스에 대해 먼저 요금을 청구하려고 시도합니다. 라이선스를 사용할 수 없는 경우 마켓플레이스 구독료에 대한 요금이 부과됩니다. BYOL 구독을 마켓플레이스 구독으로 전환할 필요는 없으며, 그 반대의 경우도 마찬가지입니다.

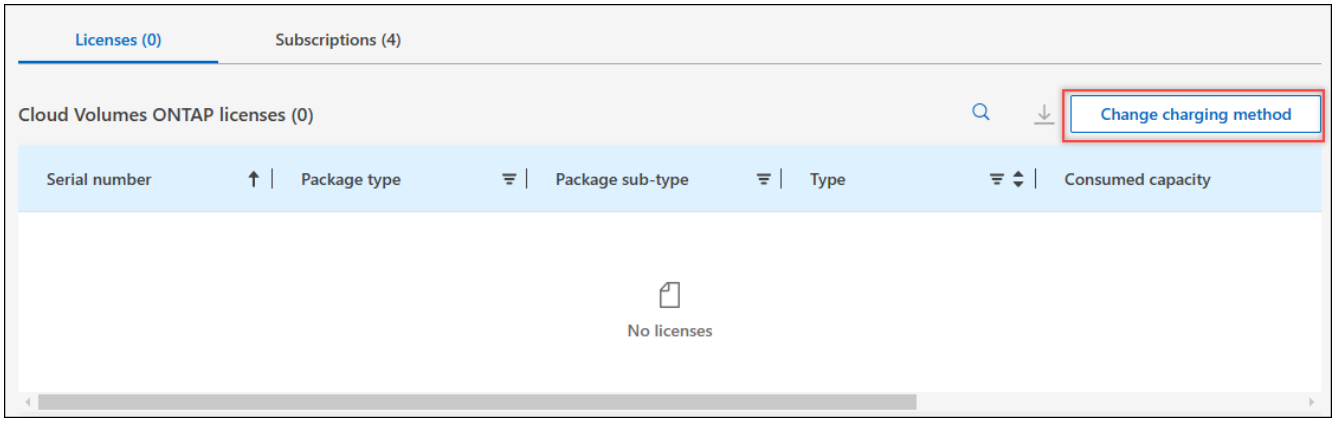
- 클라우드 공급업체의 마켓플레이스에서 개인 제안이나 계약을 체결한 경우, 계약에 포함되지 않은 청구 방식으로 변경하면 BYOL(NetApp 에서 라이선스를 구매한 경우) 또는 PAYGO로 요금이 청구됩니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. *고급 보기로 전환*을 선택하세요.



5. 용량 기반 라이선스 표까지 아래로 스크롤하여 *청구 방법 변경*을 선택하세요.



6. 청구 방법 변경 팝업에서 Cloud Volumes ONTAP 시스템을 선택하고 새로운 청구 방법을 선택한 다음, 패키지 유형을 변경하면 서비스 요금이 변경된다는 사실을 이해했는지 확인하세요.
7. *충전 방법 변경*을 선택하세요.

사용 보고서 다운로드

콘솔에서 4개의 사용 보고서를 다운로드할 수 있습니다. 이러한 사용 보고서는 구독의 용량 세부 정보를 제공하고 Cloud Volumes ONTAP 구독의 리소스에 대한 요금이 어떻게 청구되는지 알려줍니다. 다운로드 가능한 보고서는 특정 시점의 데이터를 수집하여 다른 사람들과 쉽게 공유할 수 있습니다.

다음 보고서를 다운로드할 수 있습니다. 표시된 용량 값은 TiB 단위입니다.

- 높은 수준의 사용: 이 보고서에는 다음 정보가 포함되어 있습니다.
  - 총 소비 용량
  - 총 사전 약속 용량
  - 총 BYOL 용량
  - 총 마켓플레이스 계약 용량
  - 총 PAYGO 용량
- * Cloud Volumes ONTAP 패키지 사용*: 이 보고서에는 각 패키지에 대한 다음 정보가 포함되어 있습니다.
  - 총 소비 용량
  - 총 사전 약속 용량
  - 총 BYOL 용량
  - 총 마켓플레이스 계약 용량
  - 총 PAYGO 용량
- 스토리지 **VM** 사용량: 이 보고서는 Cloud Volumes ONTAP 시스템과 스토리지 가상 머신(SVM)에서 청구된 용량이 어떻게 세분화되는지 보여줍니다. 이 정보는 보고서에서만 제공됩니다. 여기에는 다음 정보가 포함되어

있습니다.

- 시스템 ID 및 이름(UUID로 표시됨)
- 클라우드
- NetApp 계정 ID
- 시스템 구성
- SVM 이름
- 프로비저닝된 용량
- 충전 용량 반올림
- 마켓플레이스 청구 기간
- Cloud Volumes ONTAP 패키지 또는 기능
- SaaS Marketplace 구독 이름 청구
- SaaS 마켓플레이스 구독 ID 청구
- 작업 유형

- 볼륨 사용량: 이 보고서는 Cloud Volumes ONTAP 시스템에서 볼륨별로 청구된 용량을 어떻게 세분화하는지 보여줍니다. 이 정보는 콘솔의 어떤 화면에서도 사용할 수 없습니다. 여기에는 다음 정보가 포함됩니다.
  - 시스템 ID 및 이름(UUID로 표시됨)
  - SVN 이름
  - 볼륨 ID
  - 볼륨 유형
  - 볼륨 프로비저닝 용량

> FlexClone 볼륨은 이 보고서에 포함되지 않습니다. 이러한 유형의 볼륨에는 요금이 부과되지 않기 때문입니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭에서 Cloud Volumes ONTAP 타일의 *보기*를 선택합니다.
3. *사용 보고서*를 선택하세요.

   사용 보고서를 다운로드합니다.

4. 다운로드한 파일을 열어 보고서에 접근하세요.

NetApp Console 통해 Cloud Volumes ONTAP 대한 Keystone 구독 관리

NetApp Console 에서 Cloud Volumes ONTAP 과 함께 사용할 구독을 활성화하고 구독 서비스 수준에 대한 커밋된 용량 변경을 요청하여 Keystone 구독을 관리합니다. 서비스 수준에 대한 추가 용량을 요청하면 Cloud Volumes ONTAP 시스템에 더 많은 스토리지가 제공됩니다.

NetApp Keystone CapEx나 리스보다 OpEx를 선호하는 고객에게 하이브리드 클라우드 환경을 제공하는 유연한

종량제 구독 기반 서비스입니다.

"Keystone 에 대해 자세히 알아보세요"

계정 승인

콘솔에서 Keystone 구독을 사용하고 관리하려면 먼저 NetApp 에 문의하여 Keystone 구독으로 콘솔 계정을 인증해야 합니다.

단계

1. NetApp Console 메뉴에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. * Keystone 구독*을 선택하세요.
3. * NetApp Keystone 에 오신 것을 환영합니다* 페이지가 보이면 페이지에 나열된 주소로 이메일을 보내주세요.

   NetApp 담당자가 귀하의 계정에 구독에 대한 액세스를 승인하여 귀하의 요청을 처리합니다.

4. 구독 내역을 보려면 * Keystone 구독* 탭으로 돌아가세요.

구독 연결

NetApp 계정을 승인한 후 Keystone 구독을 연결하여 Cloud Volumes ONTAP 과 함께 사용할 수 있습니다. 이 작업을 통해 사용자는 새로운 Cloud Volumes ONTAP 시스템에 대한 요금 청구 방법으로 구독을 선택할 수 있습니다.

단계

1. NetApp Console 메뉴에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. * Keystone 구독*을 선택하세요.
3. 연결하려는 구독의 경우 클릭하세요. ••• 그리고 *링크*를 선택하세요.

결과

이제 구독이 콘솔 조직이나 계정에 연결되었으며 Cloud Volumes ONTAP 작업 환경을 만들 때 선택할 수 있습니다.

더 많거나 적은 용량을 요청하세요

구독 서비스 수준에 대한 약정 용량을 변경하려면 콘솔에서 직접 NetApp 에 요청을 보낼 수 있습니다. 서비스 수준에 대한 추가 용량을 요청하면 Cloud Volumes ONTAP 시스템에 더 많은 스토리지가 제공됩니다.

단계

1. NetApp Console 메뉴에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. * Keystone 구독*을 선택하세요.
3. 용량을 조정하려는 구독의 경우 클릭하세요. ••• *자세히 보기 및 편집*을 선택하세요.
4. 하나 이상의 구독에 대해 요청된 약정 용량을 입력하세요.
5. 아래로 스크롤하여 요청에 대한 추가 세부 정보를 입력한 다음 *제출*을 클릭합니다.

결과

귀하의 요청은 NetApp 시스템에 처리를 위한 티켓을 생성합니다.

모니터 사용

Digital Advisor 대시보드를 사용하면 Keystone 구독 사용량을 모니터링하고 보고서를 생성할 수 있습니다.

"구독 사용량 모니터링에 대해 자세히 알아보세요"

구독 연결 해제

콘솔에서 Keystone 구독을 더 이상 사용하지 않으려면 구독 연결을 해제할 수 있습니다. 기존 Cloud Volumes ONTAP 구독에 연결되지 않은 구독만 연결 해제할 수 있습니다.

단계

1. NetApp Console 메뉴에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. * Keystone*을 선택하세요.
3. 연결을 해제하려는 구독의 경우 다음을 클릭하세요. ••• *연결 해제*를 선택하세요.

결과

구독이 콘솔 조직 또는 계정에서 연결 해제되어 Cloud Volumes ONTAP 작업 환경을 생성할 때 더 이상 선택할 수 없습니다.

Cloud Volumes ONTAP 에 대한 노드 기반 라이선싱 관리

NetApp Console 에서 노드 기반 라이선스를 관리하여 각 Cloud Volumes ONTAP 시스템에 필요한 용량을 갖춘 유효한 라이선스가 있는지 확인하세요.

_노드 기반 라이선스_는 이전 세대 라이선스 모델입니다(신규 고객은 사용할 수 없습니다).

- NetApp 에서 구매한 BYOL(Bring Your Own License) 라이선스
- 클라우드 제공업체의 마켓플레이스에서 시간당 결제(PAYGO) 구독

NetApp Console 에서 노드 기반 Cloud Volumes ONTAP 라이선스를 관리할 수 있습니다.

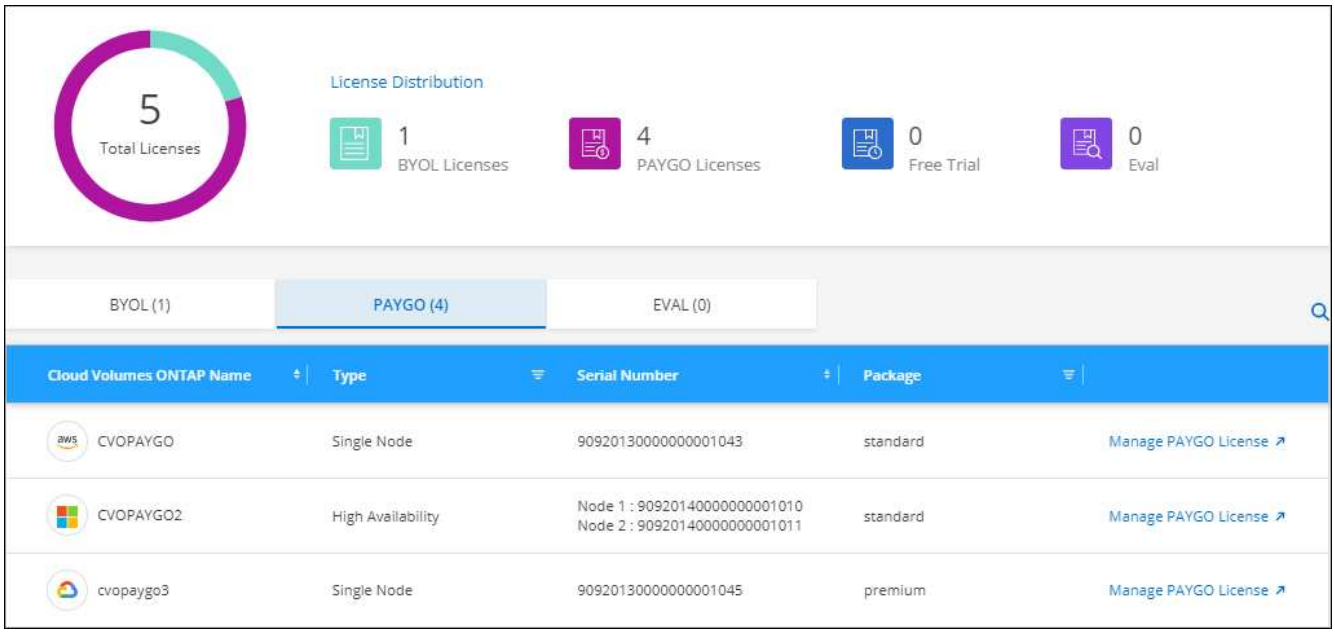
"Cloud Volumes ONTAP 라이선스에 대해 자세히 알아보세요" .

PAYGO 라이선스 관리

Licenses and subscriptions 메뉴를 사용하면 일련 번호와 PAYGO 라이선스 유형을 포함하여 각 PAYGO Cloud Volumes ONTAP 시스템에 대한 세부 정보를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. *PAYGO*를 클릭하세요.
6. 각 PAYGO 라이선스에 대한 세부 정보를 표에서 확인하세요.



7. 필요한 경우 *PAYGO 라이선스 관리*를 클릭하여 PAYGO 라이선스를 변경하거나 인스턴스 유형을 변경합니다.

BYOL 라이선스 관리

NetApp 에서 직접 구매한 라이선스를 관리하려면 시스템 라이선스와 추가 용량 라이선스를 추가하거나 제거하세요.

NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 에 대한 BYOL 라이선싱의 제한된 가용성" .

할당되지 않은 라이선스 추가

새로운 Cloud Volumes ONTAP 시스템을 생성할 때 라이선스를 선택할 수 있도록 콘솔에 노드 기반 라이선스를 추가합니다. 콘솔에서는 이러한 라이선스를 _할당되지 않음_으로 식별합니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. *할당되지 않음*을 클릭합니다.
6. *할당되지 않은 라이선스 추가*를 클릭합니다.
7. 라이선스의 일련번호를 입력하거나 라이선스 파일을 업로드하세요.

   아직 라이센스 파일이 없다면 아래 섹션을 참조하세요.

8. *라이선스 추가*를 클릭하세요.

결과

콘솔은 라이센스를 추가합니다. 라이선스는 새로운 Cloud Volumes ONTAP 시스템과 연결할 때까지 할당되지 않은 것으로 표시됩니다. 그런 다음 라이선스는 * Licenses and subscriptions*의 **BYOL** 탭으로 이동합니다.

할당되지 않은 노드 기반 라이선스 교환

사용하지 않은 Cloud Volumes ONTAP 용 노드 기반 라이선스가 할당되지 않은 경우, 해당 라이선스를 NetApp Backup and Recovery 라이선스, NetApp Data Classification 라이선스 또는 NetApp Cloud Tiering 라이선스로 변환하여 라이선스를 교환할 수 있습니다.

라이선스를 교환하면 Cloud Volumes ONTAP 라이선스가 취소되고 서비스에 대한 달러 상당의 라이선스가 생성됩니다.

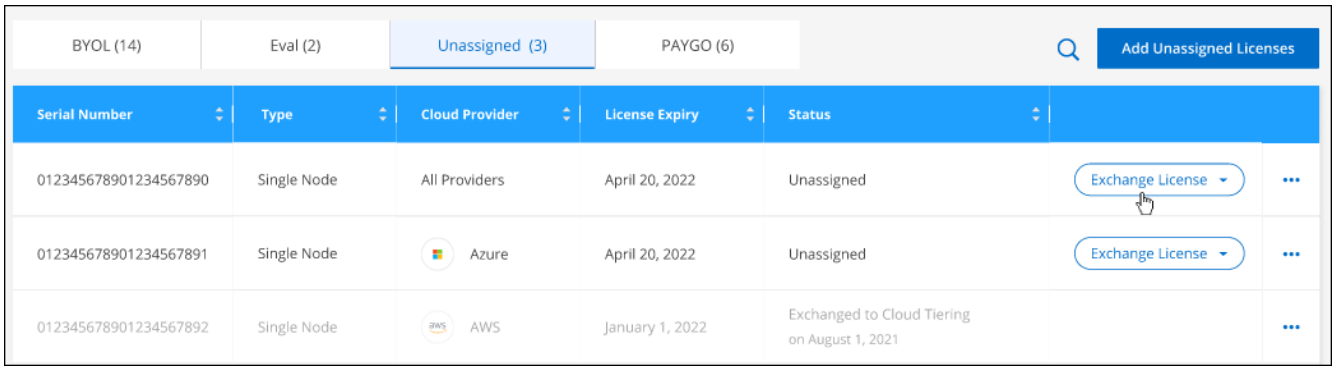
- Cloud Volumes ONTAP HA 쌍에 대한 라이선싱은 51TiB 직접 라이선스로 변환됩니다.
- Cloud Volumes ONTAP 단일 노드에 대한 라이선싱은 32TiB 직접 라이선스로 변환됩니다.

변환된 라이선스의 만료일은 Cloud Volumes ONTAP 라이선스와 동일합니다.

"노드 기반 라이선스를 교환하는 방법에 대한 연습을 확인하세요."

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. *할당되지 않음*을 클릭합니다.
6. *라이선스 교환*을 클릭하세요.



7. 라이센스를 교환할 서비스를 선택하세요.
8. 메시지가 표시되면 HA 쌍에 대한 추가 라이선스를 선택하세요.
9. 법적 동의서를 읽고 *동의*를 클릭하세요.

결과

콘솔은 할당되지 않은 라이선스를 선택한 서비스로 변환합니다. 데이터 서비스 라이선스 탭에서 새 라이선스를 볼 수 있습니다.

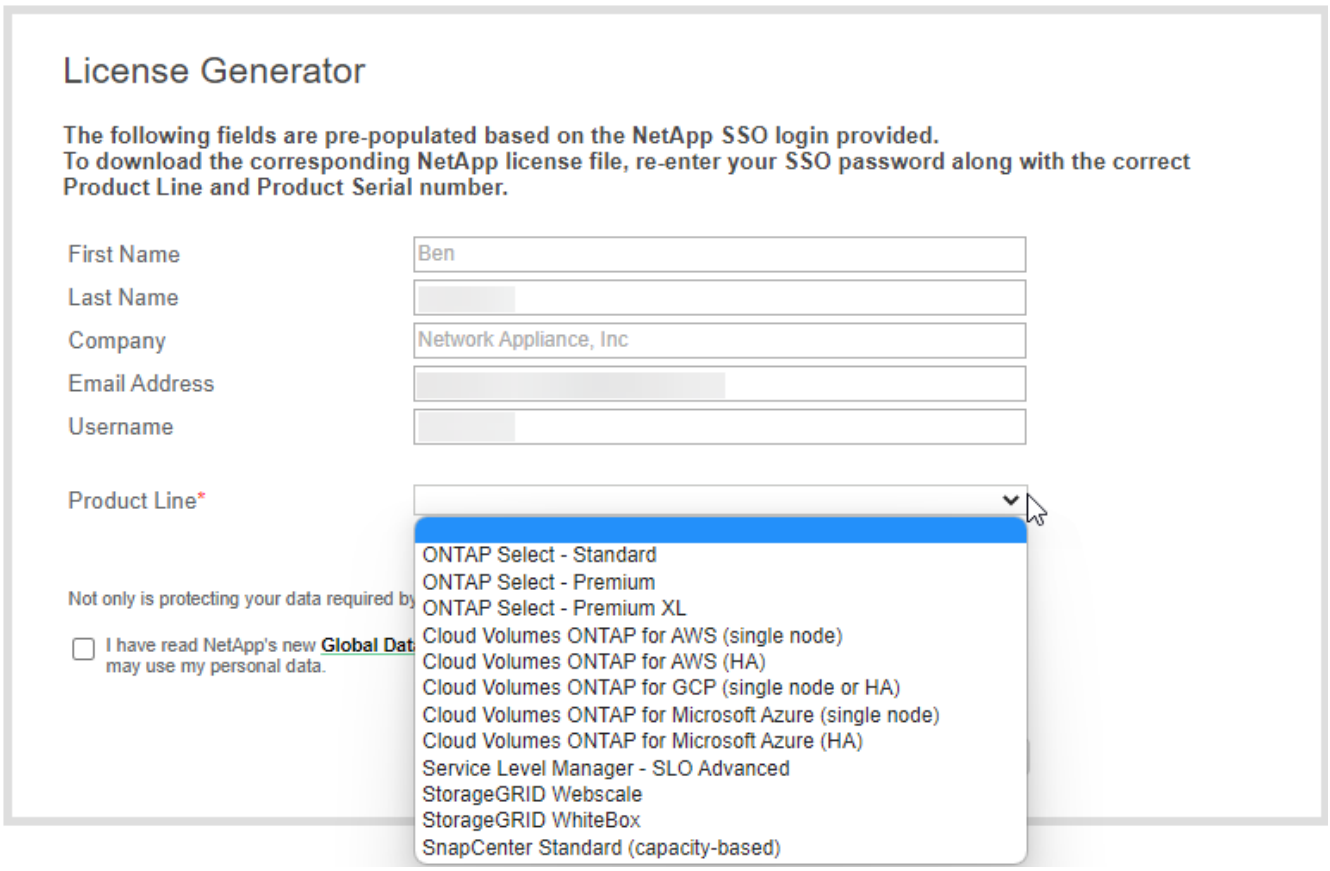
시스템 라이센스 파일을 얻으세요

대부분의 경우 콘솔은 NetApp 지원 사이트 계정을 사용하여 자동으로 라이선스 파일을 가져올 수 있습니다. 하지만 그렇지 않은 경우에는 라이선스 파일을 수동으로 업로드해야 합니다. 라이센스 파일이 없으면 netapp.com에서 받을 수 있습니다.

단계

1. 로 가다 "NetApp 라이선스 파일 생성기" NetApp 지원 사이트 자격 증명을 사용하여 로그인하세요.
2. 비밀번호를 입력하고, 제품을 선택하고, 일련번호를 입력하고, 개인정보 보호정책을 읽고 동의함을 확인한 후 *제출*을 클릭하세요.

   예



3. serialnumber.NLF JSON 파일을 이메일로 받을지, 아니면 직접 다운로드할지 선택하세요.

시스템 라이선스 업데이트

NetApp 담당자에게 연락하여 BYOL 구독을 갱신하면 콘솔이 자동으로 NetApp 에서 새 라이선스를 받아 Cloud Volumes ONTAP 시스템에 설치합니다. 콘솔이 보안 인터넷 연결을 통해 라이선스 파일에 액세스할 수 없는 경우 직접 파일을 얻은 다음 수동으로 파일을 업로드할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. **BYOL** 탭에서 Cloud Volumes ONTAP 시스템에 대한 세부 정보를 확장합니다.
6. 시스템 라이선스 옆에 있는 작업 메뉴를 클릭하고 *라이선스 업데이트*를 선택하세요.
7. 라이선스 파일(HA 쌍이 있는 경우 여러 개)을 업로드합니다.

8. *라이선스 업데이트*를 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 시스템의 라이선스를 업데이트합니다.

추가 용량 라이선스 관리

BYOL 시스템 라이선스로 제공되는 368TiB의 용량보다 더 많은 용량을 할당하려면 Cloud Volumes ONTAP BYOL 시스템에 대한 추가 용량 라이선스를 구매할 수 있습니다. 예를 들어, Cloud Volumes ONTAP 에 최대 736TiB의 용량을 할당하기 위해 추가 라이선스 용량 하나를 구매할 수 있습니다. 또는 추가 용량 라이선스 3개를 구매하여 최대 1.4 PiB까지 확보할 수 있습니다.

단일 노드 시스템 또는 HA 쌍에 대해 구매할 수 있는 라이센스 수는 무제한입니다.

용량 라이선스 추가

콘솔 오른쪽 하단에 있는 채팅 아이콘을 통해 문의하여 추가 용량 라이선스를 구매하세요. 라이선스를 구매한 후에는 Cloud Volumes ONTAP 시스템에 적용할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. **BYOL** 탭에서 Cloud Volumes ONTAP 시스템에 대한 세부 정보를 확장합니다.
6. *용량 라이선스 추가*를 클릭하세요.
7. 일련 번호를 입력하거나 라이선스 파일(HA 쌍이 있는 경우 여러 파일)을 업로드합니다.
8. *용량 라이선스 추가*를 클릭하세요.

용량 라이선스 업데이트

추가 용량 라이선스 기간을 연장한 경우 콘솔에서 라이선스를 업데이트해야 합니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. **BYOL** 탭에서 Cloud Volumes ONTAP 시스템에 대한 세부 정보를 확장합니다.
6. 용량 라이선스 옆에 있는 작업 메뉴를 클릭하고 *라이선스 업데이트*를 선택합니다.
7. 라이선스 파일(HA 쌍이 있는 경우 여러 개)을 업로드합니다.
8. *라이선스 업데이트*를 클릭하세요.

용량 라이센스 제거

추가 용량 라이선스가 만료되어 더 이상 사용하지 않는 경우 언제든지 제거할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. **BYOL** 탭에서 Cloud Volumes ONTAP 시스템에 대한 세부 정보를 확장합니다.
6. 용량 라이선스 옆에 있는 작업 메뉴를 클릭하고 *라이선스 제거*를 선택합니다.
7. *제거*를 클릭하세요.

PAYGO와 **BYOL** 간 변경

PAYGO 노드별 라이선싱에서 BYOL 노드별 라이선싱으로 시스템을 변환하는 것(또는 그 반대)은 지원되지 않습니다. 사용량에 따른 요금제 구독과 BYOL 구독 간에 전환하려면 새로운 시스템을 배포하고 기존 시스템의 데이터를 새로운 시스템으로 복제해야 합니다.

단계

1. 새로운 Cloud Volumes ONTAP 시스템을 만듭니다.
2. 복제해야 하는 각 볼륨에 대해 시스템 간에 일회성 데이터 복제를 설정합니다.

   "시스템 간에 데이터를 복제하는 방법을 알아보세요"

3. 더 이상 필요하지 않은 Cloud Volumes ONTAP 시스템을 종료하려면 원래 시스템을 삭제합니다.

   "Cloud Volumes ONTAP 시스템을 삭제하는 방법을 알아보세요" .

관련 링크

링크:"노드 기반 라이선스 제공 종료" "노드 기반 라이센스를 용량 기반으로 변환"

볼륨 및 LUN 관리

Cloud Volumes ONTAP 시스템에서 FlexVol volume 생성

초기 Cloud Volumes ONTAP 시스템을 시작한 후 더 많은 스토리지가 필요한 경우 NetApp Console 에서 NFS, CIFS 또는 iSCSI에 대한 새로운 FlexVol 볼륨을 생성할 수 있습니다.

새 볼륨을 생성하는 방법은 여러 가지가 있습니다.

- 새 볼륨에 대한 세부 정보를 지정하고 콘솔에서 기본 데이터 집계를 처리하도록 하세요.자세히 알아보기
- 원하는 데이터 집계에 볼륨을 생성합니다.자세히 알아보기
- HA 구성의 두 번째 노드에 볼륨을 생성합니다.자세히 알아보기

시작하기 전에

볼륨 프로비저닝에 대한 몇 가지 참고 사항:

- iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후,"IQN을 사용하여 호스트에서 LUN에 연결합니다." .
- ONTAP 시스템 관리자나 ONTAP CLI에서 추가 LUN을 생성할 수 있습니다.
- AWS에서 CIFS를 사용하려면 DNS와 Active Directory를 설정해야 합니다. 자세한 내용은 다음을 참조하세요 ."AWS용 Cloud Volumes ONTAP 에 대한 네트워킹 요구 사항" .
- Cloud Volumes ONTAP 구성이 Amazon EBS Elastic Volumes 기능을 지원하는 경우 다음을 수행할 수 있습니다."볼륨을 생성하면 어떤 일이 발생하는지 자세히 알아보세요." .

볼륨을 생성합니다

볼륨을 생성하는 가장 일반적인 방법은 필요한 볼륨 유형을 지정한 다음 콘솔에서 디스크 할당을 처리하도록 하는 것입니다. 하지만 볼륨을 생성할 특정 집계를 선택할 수도 있습니다.

단계

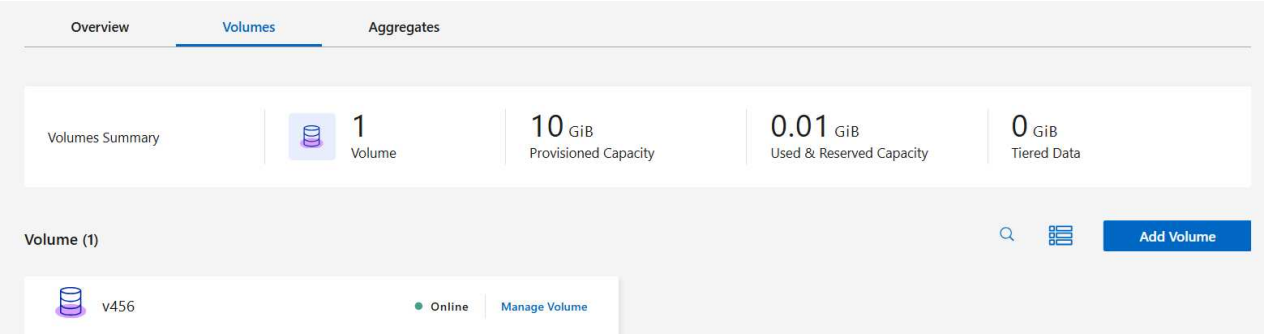
1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 FlexVol volume 프로비저닝하려는 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.

   콘솔에서 디스크 할당을 처리하도록 하여 볼륨을 만들거나 볼륨에 대한 특정 집계를 선택할 수 있습니다. Cloud Volumes ONTAP 시스템의 데이터 집계에 대해 잘 이해하고 있는 경우에만 특정 집계를 선택하는 것이 좋습니다.

모든 집계

볼륨 탭을 선택하고 *볼륨 추가*를 클릭합니다

.

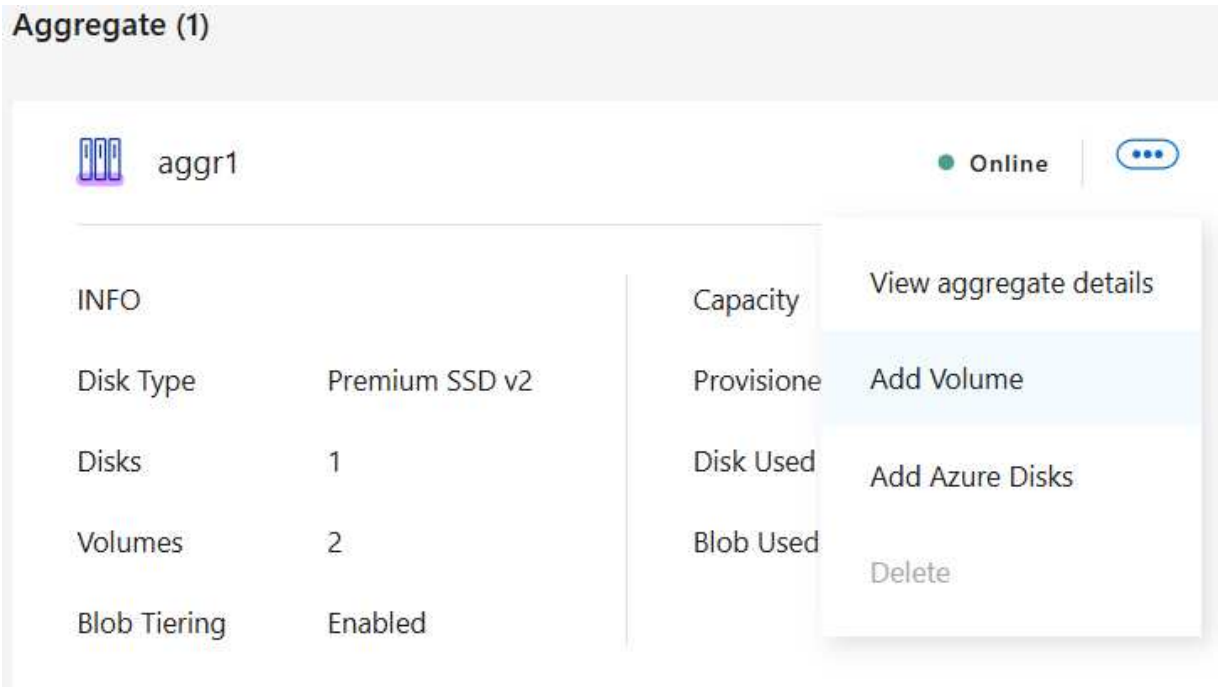


특정 집계

a. 집계 탭에서 필요한 집계로 이동하여 클릭하십시오. ••• 상.

b. *볼륨 추가*를 선택하세요

.



3. 마법사의 단계에 따라 볼륨을 생성합니다.

a. 세부 정보, 보호 및 태그: 볼륨에 대한 기본 세부 정보를 입력하고 스냅샷 정책을 선택합니다.

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 목록은 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
볼륨 이름	새 볼륨에 입력할 수 있는 식별 가능한 이름입니다.

필드	설명
볼륨 크기	입력할 수 있는 최대 크기는 씬 프로비저닝을 활성화하는지 여부에 따라 크게 달라집니다. 씬 프로비저닝을 활성화하면 현재 사용 가능한 물리적 저장소보다 큰 볼륨을 만들 수 있습니다.
스토리지 VM(SVM)	스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에게 스토리지 및 데이터 서비스를 제공합니다. 이것을 SVM이나 vserver라고 알고 있을 수도 있습니다. Cloud Volumes ONTAP 은 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다. 새 볼륨에 대한 스토리지 VM을 지정할 수 있습니다.
스냅샷 정책	스냅샷 복사 정책은 NetApp 스냅샷 복사본이 자동으로 생성되는 빈도와 수를 지정합니다. NetApp 스냅샷 복사본은 성능에 영향을 미치지 않고 최소한의 저장 공간만 필요한 특정 시점의 파일 시스템 이미지입니다. 기본 정책을 선택하거나 아무것도 선택하지 않을 수 있습니다. 일시적인 데이터의 경우 '없음'을 선택할 수 있습니다. 예를 들어 Microsoft SQL Server의 경우 tempdb를 선택합니다.

b. 프로토콜: 볼륨에 대한 프로토콜(NFS, CIFS 또는 iSCSI)을 선택한 다음 필요한 정보를 제공합니다.

   CIFS를 선택하고 서버가 설정되지 않은 경우, *다음*을 클릭하면 콘솔에서 CIFS 연결을 설정하라는 메시지가 표시됩니다.

   "지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

   다음 섹션에서는 지침이 필요할 수 있는 분야에 대해 설명합니다. 설명은 프로토콜별로 구성되어 있습니다.

NFS

접근 제어

볼륨을 클라이언트가 사용할 수 있도록 사용자 지정 내보내기 정책을 선택합니다.

수출 정책

볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 콘솔은 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.

CIFS

권한 및 사용자/그룹

사용자 및 그룹의 SMB 공유에 대한 액세스 수준을 제어할 수 있습니다(액세스 제어 목록 또는 ACL이라고도 함). 로컬 또는 도메인 Windows 사용자나 그룹, 또는 UNIX 사용자나 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자 도메인을 포함해야 합니다.

DNS 기본 및 보조 **IP** 주소

CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인의 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.

Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.

가입할 **Active Directory** 도메인

CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.

도메인에 가입할 수 있는 권한이 있는 자격 증명

AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.

CIFS 서버 **NetBIOS** 이름

AD 도메인에서 고유한 CIFS 서버 이름입니다.

조직 단위

CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.

- Cloud Volumes ONTAP 의 AD 서버로 AWS Managed Microsoft AD를 구성하려면 이 필드에 *OU=Computers,OU=corp*를 입력합니다.
- Cloud Volumes ONTAP 의 AD 서버로 Azure AD Domain Services를 구성하려면 이 필드에 **OU=AADDC Computers** 또는 *OU=AADDC Users*를 입력합니다.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 설명서: Azure AD Domain Services 관리 도메인에서 OU(조직 단위) 만들기"^]
- Cloud Volumes ONTAP 의 AD 서버로 Google Managed Microsoft AD를 구성하려면 이 필드에 *OU=Computers,OU=Cloud*를 입력합니다.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 문서: Google Managed Microsoft AD의 조직 단위"^]

DNS 도메인

Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 대부분의 경우 도메인은 AD 도메인과 동일합니다.

NTP 서버

Active Directory DNS를 사용하여 NTP 서버를 구성하려면 *Active Directory 도메인 사용*을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 자세한 내용은 다음을 참조하세요. "NetApp Console 자동화 문서" .

CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

iSCSI

LUN

iSCSI 스토리지 대상은 LUN(논리 단위)이라고 하며 호스트에 표준 블록 장치로 표시됩니다. iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후,"IQN을 사용하여 호스트에서 LUN에 연결합니다." .

개시자 그룹

이니시에이터 그룹(igroup)은 스토리지 시스템의 지정된 LUN에 액세스할 수 있는 호스트를 지정합니다.

호스트 개시자**(IQN)**

iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 컨버지드 네트워크 어댑터(CNA) 또는 전용 호스트 버스트 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 정규 이름(IQN)으로 식별됩니다.

a. 디스크 유형: 성능 요구 사항과 비용 요구 사항에 따라 볼륨의 기본 디스크 유형을 선택합니다.
   - "AWS에서 시스템 크기 조정"
   - "Azure에서 시스템 크기 조정"
   - "Google Cloud에서 시스템 크기 조정"

4. 사용 프로필 및 계층화 정책: 볼륨에서 스토리지 효율성 기능을 활성화할지 비활성화할지 선택한 다음 다음을 선택합니다."볼륨 티어링 정책" .

   ONTAP 에는 필요한 총 저장 용량을 줄일 수 있는 여러 가지 저장 효율성 기능이 포함되어 있습니다. NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

   씬 프로비저닝

   실제 물리적 스토리지 풀에 있는 것보다 더 많은 논리적 스토리지를 호스트나 사용자에게 제공합니다. 저장 공간을 미리 할당하는 대신, 데이터가 기록됨에 따라 각 볼륨에 저장 공간이 동적으로 할당됩니다.

   중복제거

   동일한 데이터 블록을 찾아 단일 공유 블록에 대한 참조로 대체하여 효율성을 향상시킵니다. 이 기술은 동일한 볼륨에 있는 중복된 데이터 블록을 제거하여 저장 용량 요구 사항을 줄입니다.

   압축

   1차, 2차, 보관 저장소의 볼륨 내 데이터를 압축하여 데이터를 저장하는 데 필요한 물리적 용량을 줄입니다.

5. 검토: 볼륨에 대한 세부 정보를 검토한 후 *추가*를 클릭합니다.

결과

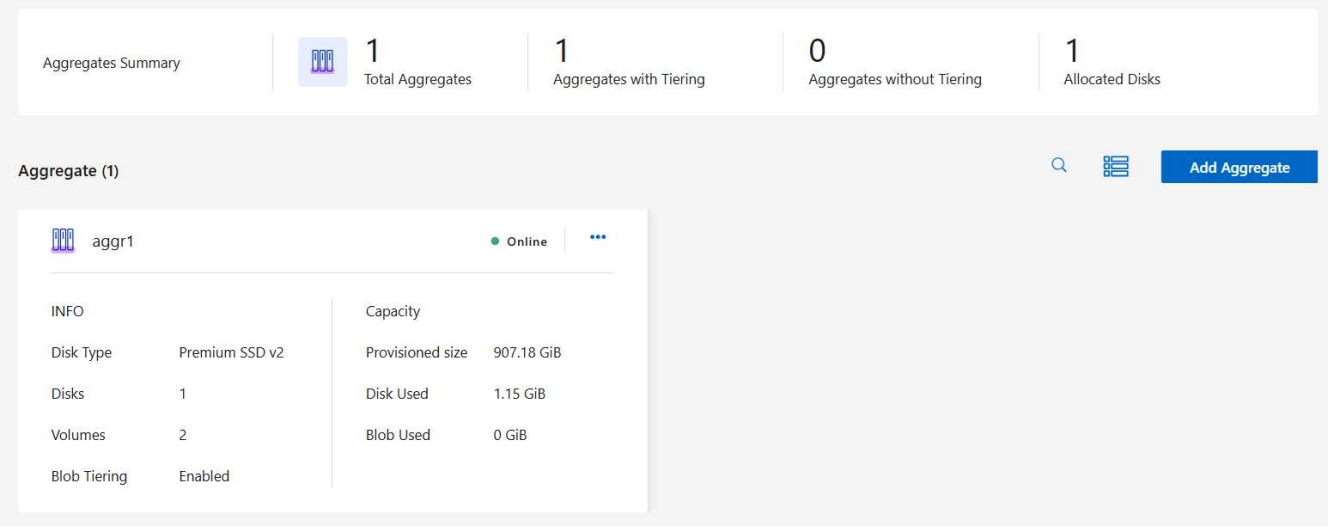
콘솔은 Cloud Volumes ONTAP 시스템에 볼륨을 생성합니다.

HA 구성의 두 번째 노드에 볼륨을 생성합니다.

기본적으로 콘솔은 HA 구성의 첫 번째 노드에 볼륨을 생성합니다. 두 노드 모두 클라이언트에 데이터를 제공하는 액티브-액티브 구성이 필요한 경우 두 번째 노드에서 집계와 볼륨을 만들어야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 집계를 관리하려는 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
3. 집계 탭에서 *집계 추가*를 클릭하고 집계를 만듭니다.



4. 홈 노드의 경우 HA 쌍에서 두 번째 노드를 선택합니다.
5. 콘솔에서 집계를 생성한 후, 해당 집계를 선택한 다음 *볼륨 생성*을 클릭합니다.
6. 새 볼륨에 대한 세부 정보를 입력한 다음 *만들기*를 클릭합니다.

결과

콘솔은 HA 쌍의 두 번째 노드에 볼륨을 생성합니다.

여러 AWS 가용성 영역에 배포된 HA 쌍의 경우 볼륨이 있는 노드의 부동 IP 주소를 사용하여 볼륨을 클라이언트에 마운트해야 합니다.

볼륨을 생성한 후

CIFS 공유를 프로비저닝한 경우 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인합니다.

볼륨에 할당량을 적용하려면 ONTAP System Manager나 ONTAP CLI를 사용해야 합니다. 할당량을 사용하면 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템에서 볼륨 관리

NetApp Console 에서 볼륨과 CIFS 서버를 관리할 수 있습니다. 용량 문제를 피하기 위해 볼륨을 이동할 수도 있습니다.

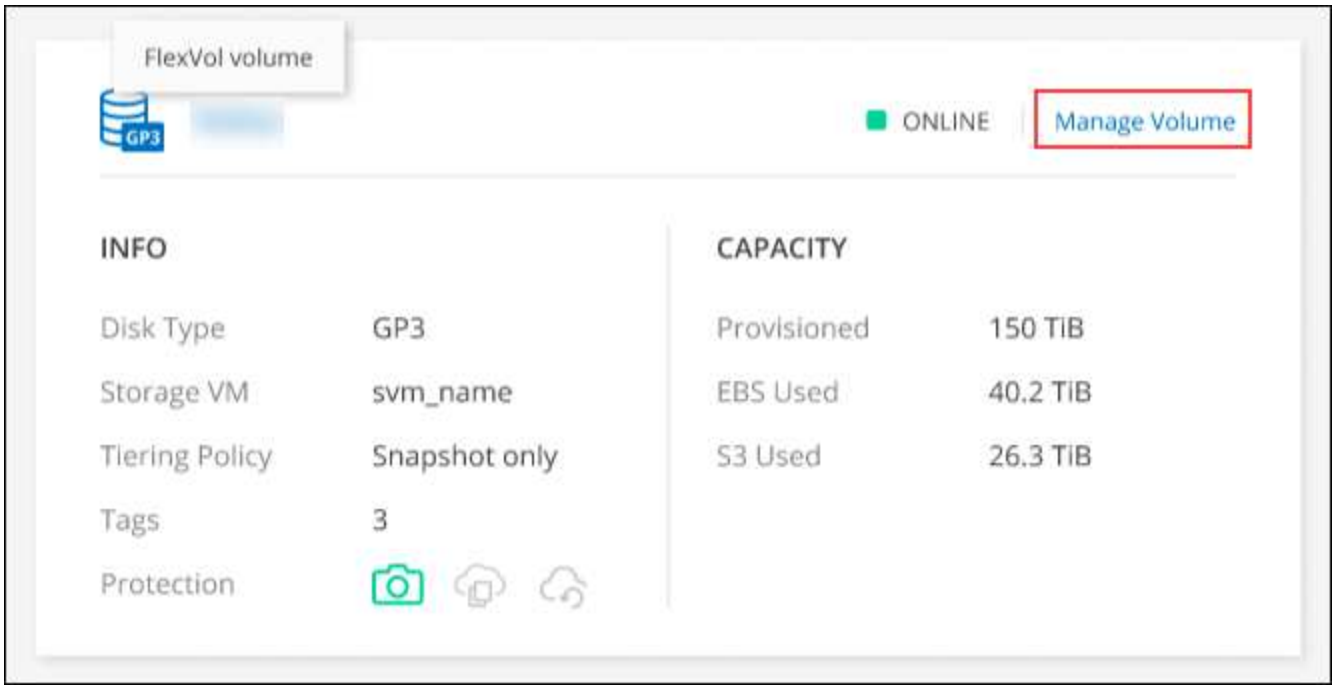
NetApp Console 표준 보기에서 볼륨을 관리하거나 고급 볼륨 관리를 위해 콘솔에 포함된 ONTAP 시스템 관리자를 통해 볼륨을 관리할 수 있습니다. 표준 보기는 볼륨을 수정하기 위한 제한된 옵션 세트를 제공합니다. System Manager는 복제, 크기 조정, 랜섬웨어 방지 설정 변경, 분석, 보호 및 활동 추적, 계층 간 볼륨 이동 등 고급 수준의 관리 기능을 제공합니다. 자세한 내용은 다음을 참조하세요."System Manager를 사용하여 Cloud Volumes ONTAP 관리" .

볼륨 관리

콘솔의 표준 보기를 사용하면 스토리지 요구 사항에 따라 볼륨을 관리할 수 있습니다. 볼륨을 보고, 편집하고, 복제하고, 복원하고, 삭제할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 볼륨을 관리할 Cloud Volumes ONTAP 시스템을 두 번 클릭합니다.
3. 볼륨 탭을 선택하세요.



4. 필요한 볼륨 타일에서 *볼륨 관리*를 클릭합니다.

일	행동
볼륨에 대한 정보 보기	볼륨 관리 패널의 볼륨 작업에서 *볼륨 세부 정보 보기*를 클릭합니다.
NFS 마운트 명령 받기	a. 볼륨 관리 패널의 볼륨 작업에서 *마운트 명령*을 클릭합니다. b. *복사*를 클릭하세요.

일	행동
볼륨 복제	a. 볼륨 관리 패널의 볼륨 작업에서 *볼륨 복제*를 클릭합니다. b. 필요에 따라 복제 이름을 수정한 다음 *복제*를 클릭합니다. 이 프로세스는 FlexClone 볼륨을 생성합니다. FlexClone 볼륨은 메타데이터에 소량의 공간을 사용하고 데이터가 변경되거나 추가될 때만 추가 공간을 사용하기 때문에 공간 효율적인 쓰기 가능한 지정 시간 복사본입니다. FlexClone 볼륨에 대해 자세히 알아보려면 다음을 참조하세요. "ONTAP 9 논리 스토리지 관리 가이드" .
볼륨 편집(읽기-쓰기 볼륨만 해당)	a. 볼륨 관리 패널의 볼륨 작업에서 *볼륨 설정 편집*을 클릭합니다. b. 볼륨의 스냅샷 정책, NFS 프로토콜 버전, NFS 액세스 제어 목록(내보내기 정책) 또는 공유 권한을 수정한 다음 *적용*을 클릭합니다. 사용자 정의 스냅샷 정책이 필요한 경우 ONTAP System Manager를 사용하여 만들 수 있습니다.
볼륨 삭제	a. 볼륨 관리 패널의 볼륨 작업에서 *볼륨 삭제*를 클릭합니다. b. 볼륨 삭제 창에서 삭제하려는 볼륨의 이름을 입력합니다. c. 다시 한번 *삭제*를 클릭하여 확인하세요.
필요에 따라 스냅샷 사본을 만듭니다.	a. 볼륨 관리 패널의 보호 작업에서 *스냅샷 복사본 만들기*를 클릭합니다. b. 필요한 경우 이름을 변경한 다음 *만들기*를 클릭합니다.
스냅샷 복사본에서 새 볼륨으로 데이터 복원	a. 볼륨 관리 패널의 보호 작업에서 *스냅샷 복사본에서 복원*을 클릭합니다. b. 스냅샷 복사본을 선택하고 새 볼륨의 이름을 입력한 다음 *복원*을 클릭합니다.
기본 디스크 유형 변경	a. 볼륨 관리 패널의 고급 작업에서 *디스크 유형 변경*을 클릭합니다. b. 디스크 유형을 선택한 다음 *변경*을 클릭합니다. 콘솔은 선택한 디스크 유형을 사용하는 기존 집계로 볼륨을 이동하거나 볼륨에 대한 새 집계를 만듭니다.
티어링 정책 변경	a. 볼륨 관리 패널의 고급 작업에서 *계층화 정책 변경*을 클릭합니다. b. 다른 정책을 선택하고 *변경*을 클릭하세요. 콘솔은 계층화를 통해 선택한 디스크 유형을 사용하는 기존 집계로 볼륨을 이동하거나 볼륨에 대한 새 집계를 만듭니다.

일	행동
볼륨 삭제	a. 볼륨을 선택한 다음 *삭제*를 클릭합니다. b. 대화 상자에 볼륨 이름을 입력합니다. c. 다시 한번 *삭제*를 클릭하여 확인하세요.

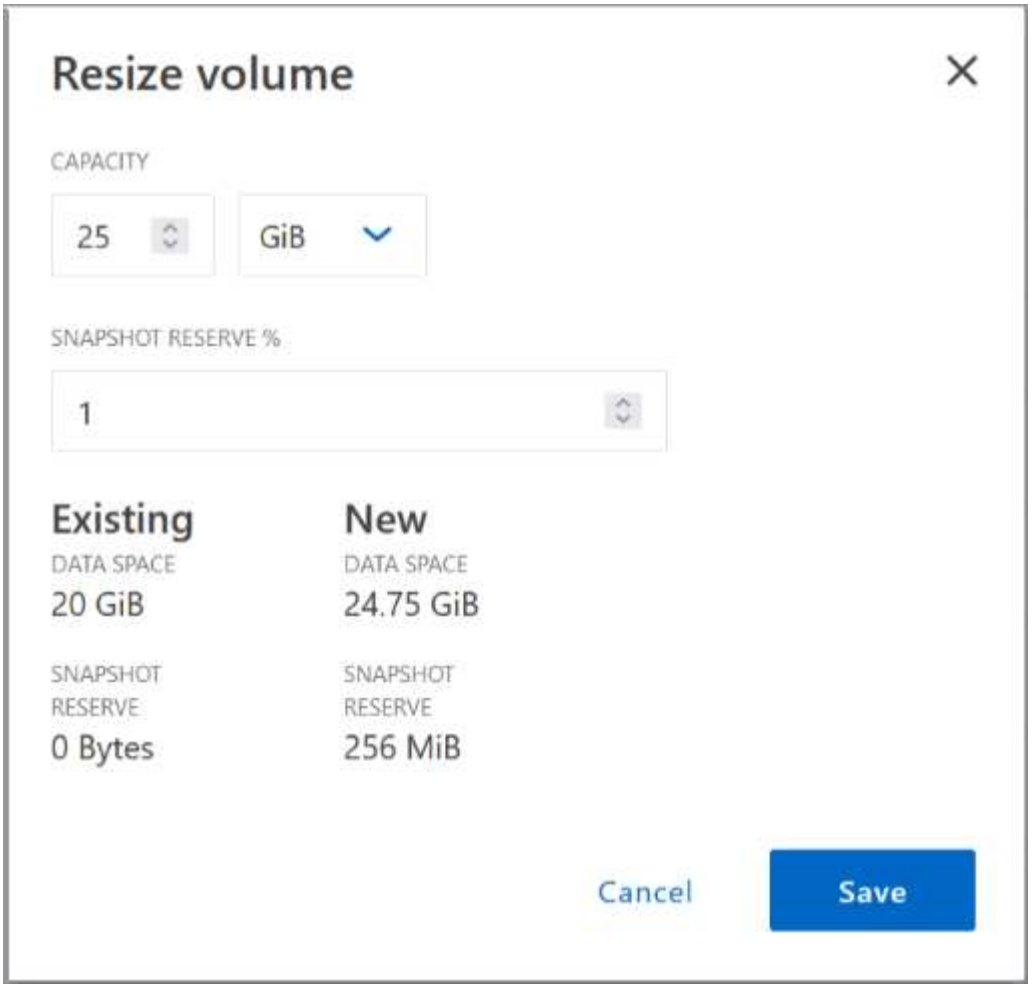
볼륨 크기 조정

기본적으로 볼륨은 공간이 부족하면 자동으로 최대 크기로 커집니다. 기본값은 1,000이며, 이는 볼륨이 원래 크기의 11배까지 커질 수 있음을 의미합니다. 이 값은 콘솔 에이전트 설정에서 구성할 수 있습니다.

볼륨 크기를 조정해야 하는 경우 콘솔의 ONTAP 시스템 관리자에서 조정할 수 있습니다.

단계

1. ONTAP 시스템 관리자를 통해 볼륨 크기를 조정하려면 시스템 관리자 보기를 클릭합니다. "시작하는 방법" .
2. 왼쪽 탐색 메뉴에서 *저장소 > 볼륨*을 선택합니다.
3. 볼륨 목록에서 크기를 조절해야 하는 볼륨을 식별합니다.
4. 옵션 아이콘을 클릭하세요 .
5. *크기 조정*을 선택하세요.
6. 볼륨 크기 조정 화면에서 필요에 따라 용량과 스냅샷 예약 비율을 편집합니다. 기존의 사용 가능한 공간과 수정된 용량을 비교할 수 있습니다.
7. *저장*을 클릭하세요.



볼륨 크기를 조정할 때는 시스템의 용량 제한을 고려해야 합니다. 로 가다 "Cloud Volumes ONTAP 릴리스 노트" 자세한 내용은.

CIFS 서버 수정

DNS 서버나 Active Directory 도메인을 변경하는 경우 Cloud Volumes ONTAP 의 CIFS 서버를 수정해야 클라이언트에 계속해서 스토리지를 제공할 수 있습니다.

단계

1. Cloud Volumes ONTAP 시스템의 개요 탭에서 오른쪽 패널 아래에 있는 기능 탭을 클릭합니다.
2. CIFS 설정 필드에서 *연필 아이콘*을 클릭하여 CIFS 설정 창을 표시합니다.
3. CIFS 서버에 대한 설정을 지정합니다.

일	행동
스토리지 VM(SVM) 선택	Cloud Volume ONTAP 스토리지 가상 머신(SVM)을 선택하면 구성된 CIFS 정보가 표시됩니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.
도메인에 가입할 수 있는 권한이 있는 자격 증명	AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.

일	행동
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인에 대한 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 SRV(서비스 위치 레코드)가 포함되어야 합니다. ifdef::gcp[] Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다. endif::gcp[]
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 대부분의 경우 도메인은 AD 도메인과 동일합니다.
CIFS 서버 NetBIOS 이름	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. • Cloud Volumes ONTAP 의 AD 서버로 AWS Managed Microsoft AD를 구성하려면 이 필드에 *OU=Computers,OU=corp*를 입력합니다. • Cloud Volumes ONTAP 의 AD 서버로 Azure AD Domain Services를 구성하려면 이 필드에 **OU=AADDC Computers** 또는 *OU=AADDC Users*를 입력합니다."Azure 설명서: Azure AD Domain Services 관리 도메인에서 OU(조직 단위) 만들기" • Cloud Volumes ONTAP 의 AD 서버로 Google Managed Microsoft AD를 구성하려면 이 필드에 *OU=Computers,OU=Cloud*를 입력합니다 ."Google Cloud 문서: Google Managed Microsoft AD의 조직 단위"

4. *설정*을 클릭하세요.

결과

Cloud Volumes ONTAP CIFS 서버에 변경 사항을 업데이트합니다.

볼륨 이동

용량 활용도, 성능 향상, 서비스 수준 계약 충족을 위해 볼륨을 이동합니다.

ONTAP 시스템 관리자에서 볼륨과 대상 집계를 선택하고, 볼륨 이동 작업을 시작하고, 선택적으로 볼륨 이동 작업을 모니터링하여 볼륨을 이동할 수 있습니다. 시스템 관리자를 사용하면 볼륨 이동 작업이 자동으로 완료됩니다.

단계

1. ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 볼륨을 집계로 이동합니다.

   대부분의 경우 시스템 관리자를 사용하여 볼륨을 이동할 수 있습니다.

   지침은 다음을 참조하세요."ONTAP 9 볼륨 이동 익스프레스 가이드" .

콘솔에 작업 필요 메시지가 표시되면 볼륨을 이동합니다.

콘솔에 볼륨을 이동하면 용량 문제를 방지할 수 있지만, 문제를 직접 해결해야 한다는 내용의 '조치 필요' 메시지가 표시될 수 있습니다. 이런 일이 발생하면 문제를 해결하는 방법을 파악한 다음 하나 이상의 볼륨을 이동해야 합니다.

집계된 용량이 90% 사용률에 도달하면 콘솔에 다음과 같은 조치 필요 메시지가 표시됩니다. 데이터 계층화가 활성화된 경우 집계가 사용 용량의 80%에 도달하면 메시지가 표시됩니다. 기본적으로 10%의 여유 공간이 데이터 계층화를 위해 예약되어 있습니다. "데이터 계층화를 위한 여유 공간 비율에 대해 자세히 알아보세요" .

단계

1. 용량 문제를 해결하는 방법을 식별합니다. .
2. 분석에 따라 용량 문제를 방지하기 위해 볼륨을 이동합니다.
   - 용량 문제를 피하기 위해 볼륨을 다른 시스템으로 이동합니다. .
   - 용량 문제를 방지하기 위해 볼륨을 다른 집계로 이동합니다. .

용량 문제를 해결하는 방법을 식별합니다.

콘솔에서 용량 문제를 방지하기 위한 볼륨 이동에 대한 권장 사항을 제공할 수 없는 경우 이동해야 할 볼륨을 식별하고 동일한 시스템의 다른 집계로 이동해야 할지 아니면 다른 시스템으로 이동해야 할지 결정해야 합니다.

단계

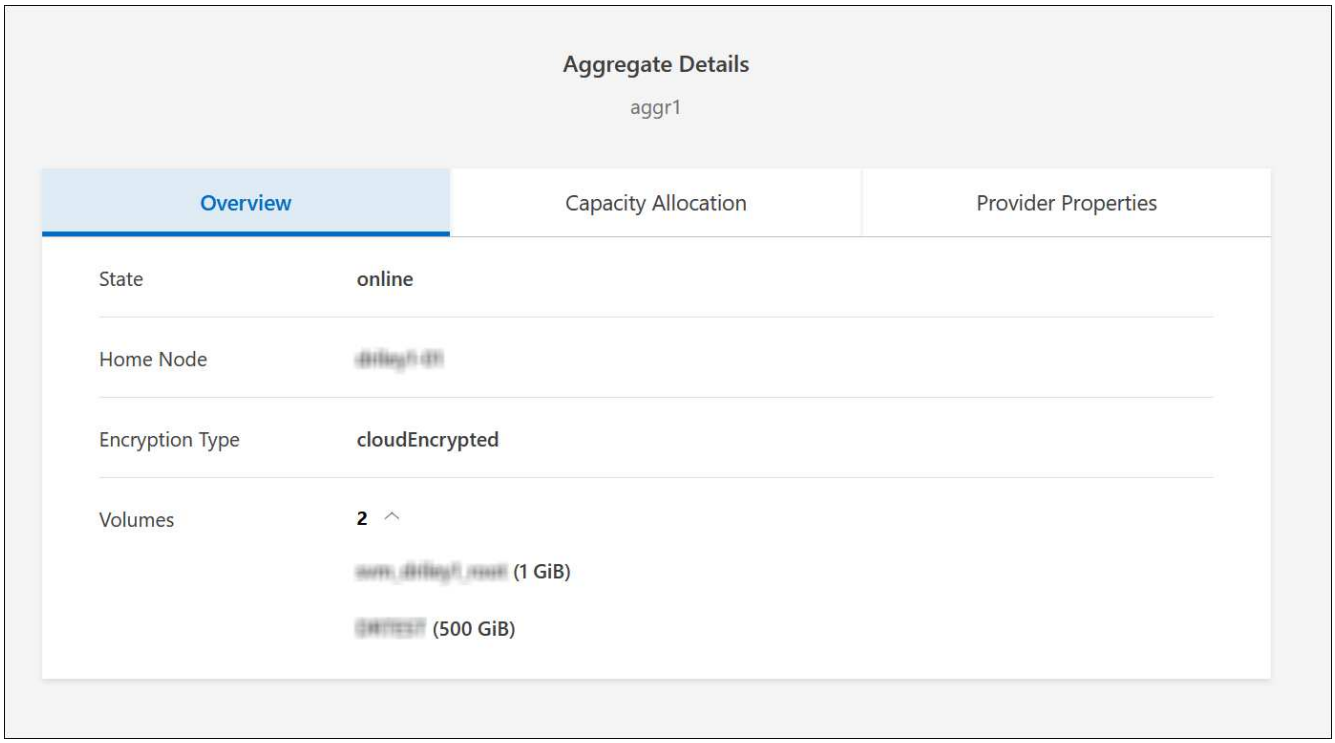
1. 집계가 용량 한도에 도달한 것을 식별하려면 작업 필요 메시지의 고급 정보를 확인하세요.

   예를 들어, 고급 정보에는 다음과 비슷한 내용이 나와 있어야 합니다. 집계 aggr1이 용량 한도에 도달했습니다.

2. 집계에서 이동할 하나 이상의 볼륨을 식별합니다.

   a. Cloud Volumes ONTAP 시스템에서 *집계 탭*을 클릭합니다.
   b. 집계 타일에서 다음을 클릭합니다. ••• 아이콘을 클릭한 다음 *집계 세부 정보 보기*를 클릭하세요.
   c. 집계 세부 정보 화면의 개요 탭에서 각 볼륨의 크기를 검토하고 집계에서 이동할 볼륨을 하나 이상 선택합니다.

      나중에 추가 용량 문제가 발생하지 않도록 전체적으로 여유 공간을 확보할 수 있을 만큼 큰 볼륨을 선택해야 합니다.



3. 시스템이 디스크 한도에 도달하지 않은 경우 볼륨을 동일한 시스템의 기존 집계나 새 집계로 이동해야 합니다.

   자세한 내용은 다음을 참조하세요.용량 문제를 방지하기 위해 볼륨을 다른 집계로 이동합니다. .

4. 시스템이 디스크 한도에 도달한 경우 다음 중 하나를 수행하세요.
   a. 사용하지 않는 볼륨을 삭제합니다.
   b. 집계된 공간을 확보하기 위해 볼륨을 재배열합니다.

      자세한 내용은 다음을 참조하세요.용량 문제를 방지하기 위해 볼륨을 다른 집계로 이동합니다. .

   c. 두 개 이상의 볼륨을 공간이 있는 다른 시스템으로 이동합니다.

      자세한 내용은 다음을 참조하세요.용량 문제를 방지하기 위해 볼륨을 다른 집계로 이동합니다. .

용량 문제를 피하기 위해 볼륨을 다른 시스템으로 이동합니다.

용량 문제를 방지하기 위해 하나 이상의 볼륨을 다른 Cloud Volumes ONTAP 시스템으로 이동할 수 있습니다. 시스템이 디스크 한도에 도달한 경우 이 작업이 필요할 수 있습니다.

이 작업에 관하여

이 작업의 단계에 따라 다음과 같은 작업 필요 메시지를 수정할 수 있습니다.

> 볼륨을 이동하는 것은 용량 문제를 방지하기 위해 필요합니다. 하지만 시스템이 디스크 한도에 도달했기 때문에 콘솔에서 이 작업을 수행할 수 없습니다.

단계

1. 사용 가능한 용량이 있는 Cloud Volumes ONTAP 시스템을 확인하거나 새로운 시스템을 배포합니다.

2. 볼륨의 일회성 데이터 복제를 수행하려면 소스 시스템을 대상 시스템으로 끌어서 놓습니다.

   자세한 내용은 다음을 참조하세요."시스템 간 데이터 복제" .

3. 복제 상태 페이지로 이동한 다음 SnapMirror 관계를 해제하여 복제된 볼륨을 데이터 보호 볼륨에서 읽기/쓰기 볼륨으로 변환합니다.

   자세한 내용은 다음을 참조하세요."데이터 복제 일정 및 관계 관리" .

4. 데이터 액세스를 위한 볼륨을 구성합니다.

   데이터 액세스를 위한 대상 볼륨 구성에 대한 정보는 다음을 참조하십시오."ONTAP 9권 재해 복구 익스프레스 가이드" .

5. 원본 볼륨을 삭제합니다.

   자세한 내용은 다음을 참조하세요."볼륨 관리" .

용량 문제를 방지하기 위해 볼륨을 다른 집계로 이동합니다.

용량 문제를 방지하기 위해 하나 이상의 볼륨을 다른 집계로 이동할 수 있습니다.

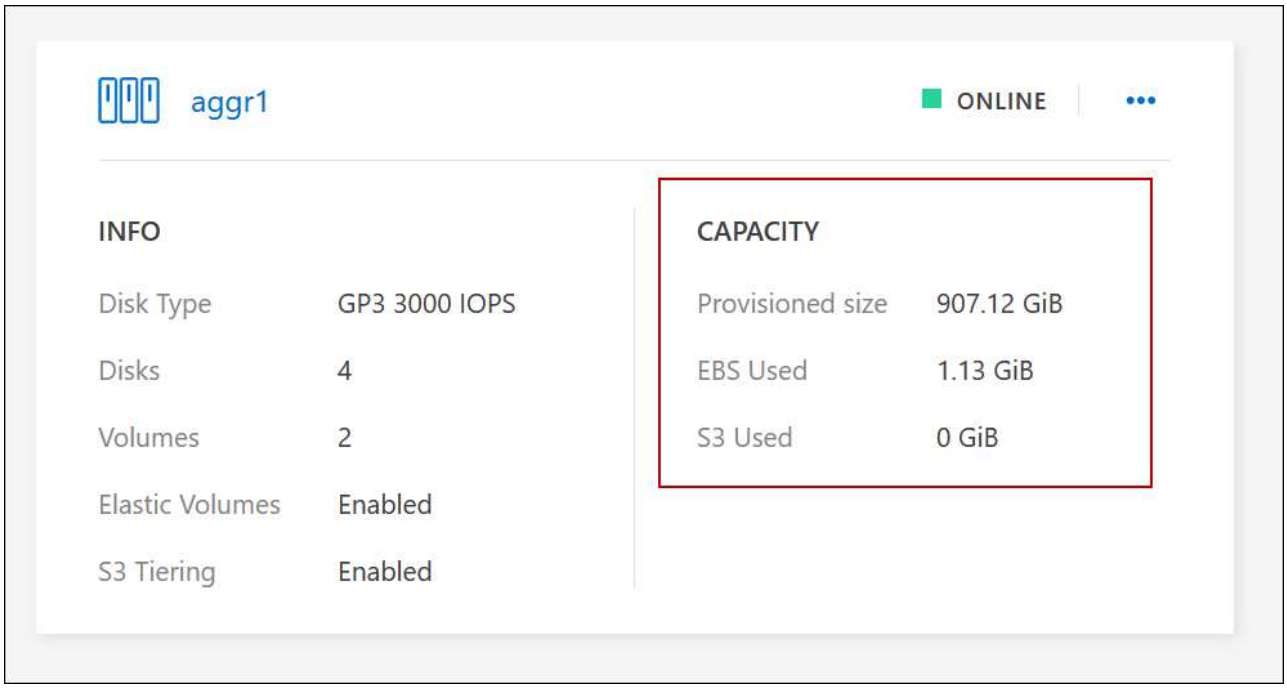
이 작업에 관하여

이 작업의 단계에 따라 다음과 같은 작업 필요 메시지를 수정할 수 있습니다.

> 용량 문제를 방지하려면 두 개 이상의 볼륨을 이동하는 것이 필요합니다. 하지만 콘솔에서는 이 작업을 대신 수행할 수 없습니다.

단계

1. 이동해야 하는 볼륨에 대한 사용 가능한 용량이 기존 집계에 있는지 확인하세요.
   a. Cloud Volumes ONTAP 시스템에서 *집계 탭*을 클릭합니다.
   b. 필요한 집계 타일에서 다음을 클릭합니다. ••• 아이콘을 클릭한 다음 *집계 세부 정보 보기*를 클릭하면 사용 가능한 용량(프로비저닝된 크기에서 사용된 집계 용량을 뺀 값)을 볼 수 있습니다.



2. 필요한 경우 기존 집계에 디스크를 추가합니다.
   a. 집계를 선택한 다음 클릭하세요. ••• 아이콘 > 디스크 추가.
   b. 추가할 디스크 수를 선택한 다음 *추가*를 클릭합니다.
3. 사용 가능한 용량이 있는 집계가 없으면 새 집계를 만듭니다.

   자세한 내용은 다음을 참조하세요."집계 생성" .
4. ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 볼륨을 집계로 이동합니다.
5. 대부분의 경우 시스템 관리자를 사용하여 볼륨을 이동할 수 있습니다.

   지침은 다음을 참조하세요."ONTAP 9 볼륨 이동 익스프레스 가이드" .

볼륨 이동이 느리게 수행되는 이유

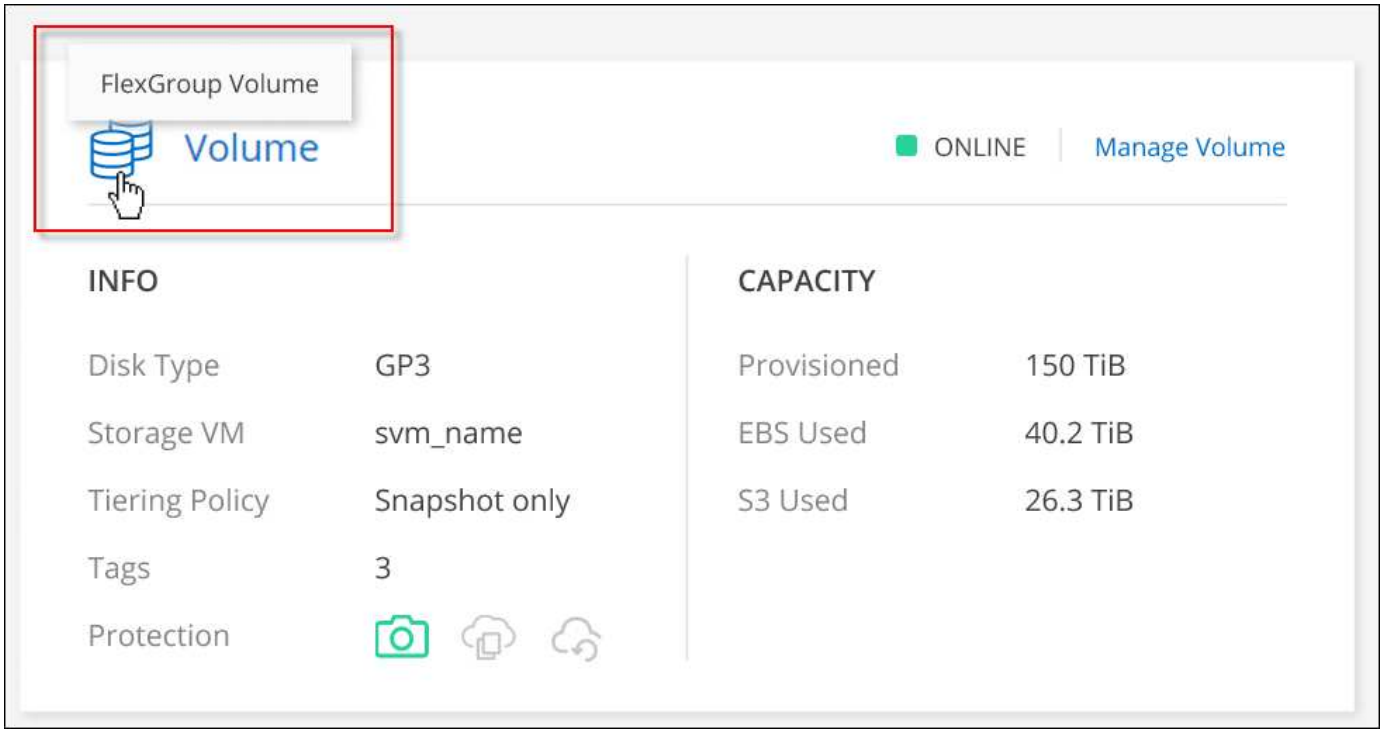
다음 조건 중 하나라도 Cloud Volumes ONTAP 에 해당하는 경우 볼륨을 이동하는 데 예상보다 시간이 더 오래 걸릴 수 있습니다.

- 볼륨은 복제본입니다.
- 볼륨은 클론의 부모입니다.
- 소스 또는 대상 집계에는 단일 처리량 최적화 HDD(st1) 디스크가 있습니다.
- 집계 중 하나는 객체에 대해 이전의 명명 체계를 사용합니다. 두 집계 모두 동일한 이름 형식을 사용해야 합니다.

  9.4 릴리스 또는 이전 릴리스에서 집계에 대한 데이터 계층화가 활성화된 경우 이전 명명 체계가 사용됩니다.
- 소스 및 대상 집계의 암호화 설정이 일치하지 않거나 키 재지정이 진행 중입니다.
- 볼륨 이동 시 계층화 정책을 변경하기 위해 *-tiering-policy* 옵션이 지정되었습니다.
- 볼륨 이동 시 *-generate-destination-key* 옵션이 지정되었습니다.

FlexGroup 볼륨 보기

ONTAP 시스템 관리자나 ONTAP CLI를 통해 생성된 FlexGroup 볼륨은 콘솔의 볼륨 탭을 통해 직접 볼 수 있습니다. 전용 볼륨 타일을 통해 FIeGroup 볼륨에 대한 자세한 정보를 볼 수 있으며, 아이콘에 마우스를 올려 놓으면 각 FlexGroup 볼륨 그룹이 식별됩니다. 또한 볼륨 목록 보기에서 볼륨 스타일 열을 통해 FlexGroup 볼륨을 식별하고 정렬할 수 있습니다.



현재는 콘솔에서만 기존 FlexGroup 볼륨을 볼 수 있습니다. 콘솔에서 FlexGroup 볼륨을 생성할 수 없습니다.

비활성 **Cloud Volumes ONTAP** 데이터를 저렴한 개체 스토리지로 계층화합니다.

자주 사용되는 데이터의 경우 SSD 또는 HDD 성능 계층을 사용하고, 비활성 데이터의 경우 객체 스토리지 용량 계층을 사용하면 Cloud Volumes ONTAP 의 스토리지 비용을 줄일 수 있습니다. 데이터 계층화는 FabricPool 기술을 기반으로 합니다. 상위 수준 개요는 다음을 참조하세요. "데이터 계층화 개요" .

데이터 계층화를 설정하려면 다음을 수행해야 합니다.

1 지원되는 구성을 선택하세요

대부분의 구성이 지원됩니다. 최신 버전을 실행하는 Cloud Volumes ONTAP 시스템이 있다면 문제없이 사용할 수 있습니다. "자세히 알아보기" .

2 **Cloud Volumes ONTAP** 과 개체 스토리지 간 연결을 보장합니다.

- AWS의 경우, Amazon Simple Storage Service(Amazon S3)에 대한 VPC 엔드포인트가 필요합니다. 자세히 알아보기.

- Azure의 경우 NetApp Console 필요한 권한이 있는 한 아무것도 할 필요가 없습니다. 자세히 알아보기 .
- Google Cloud의 경우 Private Google Access에 대한 서브넷을 구성하고 서비스 계정을 설정해야 합니다. 자세히 알아보기 .

3 계층화가 활성화된 집계가 있는지 확인하세요.

볼륨에서 데이터 계층화를 활성화하려면 집계에서 데이터 계층화를 활성화해야 합니다. 새로운 볼륨과 기존 볼륨에 대한 요구 사항을 알고 있어야 합니다. 자세히 알아보기 .

4 볼륨을 생성, 수정 또는 복제할 때 계층화 정책을 선택하세요.

NetApp Console 볼륨을 생성, 수정 또는 복제할 때 계층화 정책을 선택하라는 메시지를 표시합니다.

- "읽기-쓰기 볼륨의 계층 데이터"
- "데이터 보호 볼륨의 계층 데이터"

데이터 계층화에 필요하지 않은 것은 무엇입니까?

- 데이터 계층화를 활성화하기 위해 기능 라이선스를 설치할 필요는 없습니다.
- 용량 계층에 대한 객체 저장소를 만들 필요가 없습니다. 콘솔이 그 일을 대신해 줍니다.
- 시스템 수준에서 데이터 계층화를 활성화할 필요는 없습니다.

콘솔은 시스템을 생성할 때 콜드 데이터에 대한 객체 저장소를 생성합니다.연결이나 권한 문제가 없는 한 . 그 후에는 볼륨에서 데이터 계층화를 활성화하기만 하면 됩니다(어떤 경우에는집계에 대하여).

데이터 계층화를 지원하는 구성

특정 구성 및 기능을 사용할 때 데이터 계층화를 활성화할 수 있습니다.

AWS 지원

- AWS에서는 Cloud Volumes ONTAP 9.2부터 데이터 계층화가 지원됩니다.
- 성능 계층은 일반 용도 SSD(gp3 또는 gp2) 또는 프로비저닝된 IOPS SSD(io1)가 될 수 있습니다.

처리량 최적화 HDD(st1)를 사용할 때 개체 스토리지에 데이터를 계층화하는 것은 권장하지 않습니다.

- 비활성 데이터는 Amazon S3 버킷에 계층화됩니다. 다른 공급자로의 계층화는 지원되지 않습니다.

Azure 지원

- Azure에서는 데이터 계층화가 다음과 같이 지원됩니다.
  - 단일 노드 시스템의 버전 9.4
  - HA 쌍이 포함된 버전 9.6

- 성능 계층은 프리미엄 SSD 관리 디스크, 표준 SSD 관리 디스크 또는 표준 HDD 관리 디스크가 될 수 있습니다.
- 비활성 데이터는 Microsoft Azure Blob에 계층화됩니다. 다른 공급자로의 계층화는 지원되지 않습니다.

Google Cloud 지원

- Google Cloud에서는 Cloud Volumes ONTAP 9.6부터 데이터 계층화가 지원됩니다.
- 성능 계층은 SSD 영구 디스크, 균형 영구 디스크 또는 표준 영구 디스크가 될 수 있습니다.
- 비활성 데이터는 Google Cloud Storage에 저장됩니다. 다른 공급자로의 계층화는 지원되지 않습니다.

기능 상호 운용성

- 데이터 계층화는 암호화 기술을 통해 지원됩니다.
- 볼륨에서 씬 프로비저닝을 활성화해야 합니다.

요구 사항

클라우드 제공업체에 따라 Cloud Volumes ONTAP 콜드 데이터를 개체 스토리지로 계층화할 수 있도록 특정 연결 및 권한을 설정해야 합니다.

콜드 데이터를 **Amazon S3**로 계층화하기 위한 요구 사항

Cloud Volumes ONTAP이 Amazon S3에 연결되어 있는지 확인하십시오. 가장 좋은 연결 방법은 S3 서비스에 대한 VPC 엔드포인트를 생성하는 것입니다. 자세한 지침은 "AWS 설명서: 게이트웨이 엔드포인트 생성"을 참조하십시오.

VPC 엔드포인트를 생성할 때 Cloud Volumes ONTAP 인스턴스에 해당하는 지역, VPC 및 경로 테이블을 선택해야 합니다. 또한 S3 엔드포인트로의 트래픽을 활성화하는 아웃바운드 HTTPS 규칙을 추가하려면 보안 그룹을 수정해야 합니다. 그렇지 않으면 Cloud Volumes ONTAP 이 S3 서비스에 연결할 수 없습니다.

문제가 발생하면 다음을 참조하세요. "AWS 지원 지식 센터: 게이트웨이 VPC 엔드포인트를 사용하여 S3 버킷에 연결할 수 없는 이유는 무엇입니까?" .

Azure Blob 스토리지에 콜드 데이터를 계층화하기 위한 요구 사항

콘솔에 필요한 권한이 있는 한 성능 계층과 용량 계층 간에 연결을 설정할 필요가 없습니다. 콘솔 에이전트의 사용자 지정 역할에 다음 권한이 있는 경우 콘솔에서 VNet 서비스 엔드포인트를 사용할 수 있습니다.

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

사용자 정의 역할에는 기본적으로 권한이 포함됩니다. "콘솔 에이전트에 대한 Azure 권한 보기"

Google Cloud Storage 버킷에 콜드 데이터를 계층화하기 위한 요구 사항

- Cloud Volumes ONTAP 이 있는 서브넷은 비공개 Google 액세스로 구성되어야 합니다. 지침은 다음을 참조하세요. "Google Cloud 문서: 비공개 Google 액세스 구성" .
- 서비스 계정은 Cloud Volumes ONTAP 에 연결되어야 합니다.

  "이 서비스 계정을 설정하는 방법을 알아보세요" .

Cloud Volumes ONTAP 시스템을 생성할 때 이 서비스 계정을 선택하라는 메시지가 표시됩니다.

배포 중에 서비스 계정을 선택하지 않은 경우 Cloud Volumes ONTAP를 종료하고 Google Cloud 콘솔로 이동하여 Cloud Volumes ONTAP 인스턴스에 서비스 계정을 연결해야 합니다. 그런 다음 다음 섹션에 설명된 대로 데이터 계층화를 활성화할 수 있습니다.

- 고객 관리 암호화 키로 버킷을 암호화하려면 Google Cloud Storage 버킷에서 해당 키를 사용하도록 설정합니다.

  "Cloud Volumes ONTAP 에서 고객 관리 암호화 키를 사용하는 방법을 알아보세요." .

요구 사항 구현 후 데이터 계층화 활성화

콘솔은 연결이나 권한 문제가 없는 한 시스템이 생성될 때 콜드 데이터에 대한 개체 저장소를 생성합니다. 시스템을 생성한 후에 위에 나열된 요구 사항을 구현하지 않은 경우, 객체 저장소를 생성하는 API나 ONTAP 시스템 관리자를 통해 수동으로 계층화를 활성화해야 합니다.

콘솔을 통해 계층화를 활성화하는 기능은 향후 Cloud Volumes ONTAP 릴리스에서 제공될 예정입니다.

집계에서 계층화가 활성화되었는지 확인하세요.

볼륨에서 데이터 계층화를 활성화하려면 집계에서 데이터 계층화를 활성화해야 합니다. 새로운 볼륨과 기존 볼륨에 대한 요구 사항을 알고 있어야 합니다.

- 새로운 권

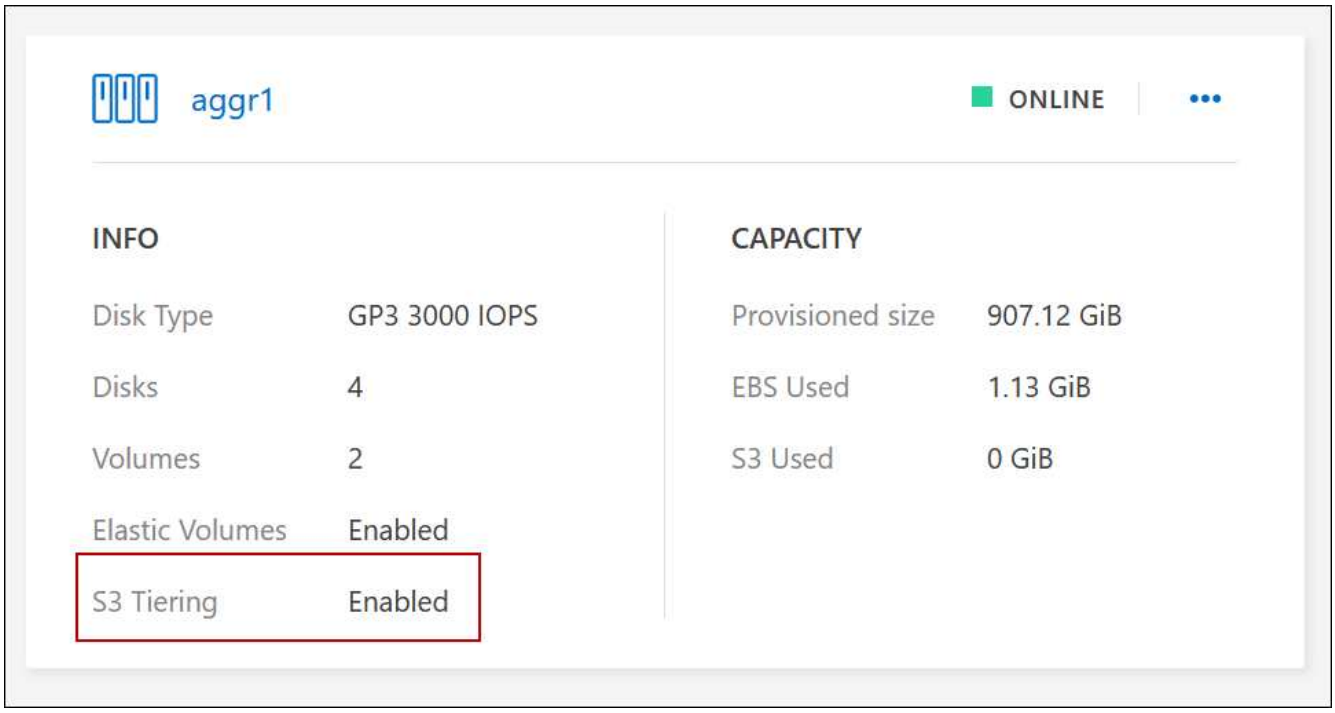
  새 볼륨에서 데이터 계층화를 활성화하는 경우 집계에서 데이터 계층화를 활성화하는 것에 대해 걱정할 필요가 없습니다. 콘솔은 계층화가 활성화된 기존 집계에 볼륨을 생성하거나, 데이터 계층화가 활성화된 집계가 아직 없는 경우 볼륨에 대한 새 집계를 생성합니다.

- 기존 볼륨

  기존 볼륨에서 데이터 계층화를 활성화하려면 기본 집계에서도 활성화되어 있는지 확인하세요. 기존 집계에서 데이터 계층화가 활성화되어 있지 않으면 ONTAP System Manager를 사용하여 기존 집계를 개체 저장소에 연결해야 합니다.

집계에서 계층화가 활성화되었는지 확인하는 단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. Cloud Volumes ONTAP 시스템을 엽니다.
3. 집계 탭을 선택하고 집계에서 계층화가 활성화되어 있는지 비활성화되어 있는지 확인합니다.



집계에서 계층화를 활성화하는 단계

1. ONTAP 시스템 관리자에서 *스토리지 > 계층*을 클릭합니다.
2. 집계에 대한 작업 메뉴를 클릭하고 *클라우드 계층 연결*을 선택합니다.
3. 연결할 클라우드 계층을 선택하고 *저장*을 클릭합니다.

다음은 무엇인가요?

다음 섹션에서 설명하는 대로 이제 새 볼륨과 기존 볼륨에서 데이터 계층화를 활성화할 수 있습니다.

읽기-쓰기 볼륨의 계층 데이터

Cloud Volumes ONTAP 읽기-쓰기 볼륨의 비활성 데이터를 비용 효율적인 개체 스토리지로 계층화하여 성능 계층을 핫 데이터에 사용할 수 있도록 확보합니다.

단계

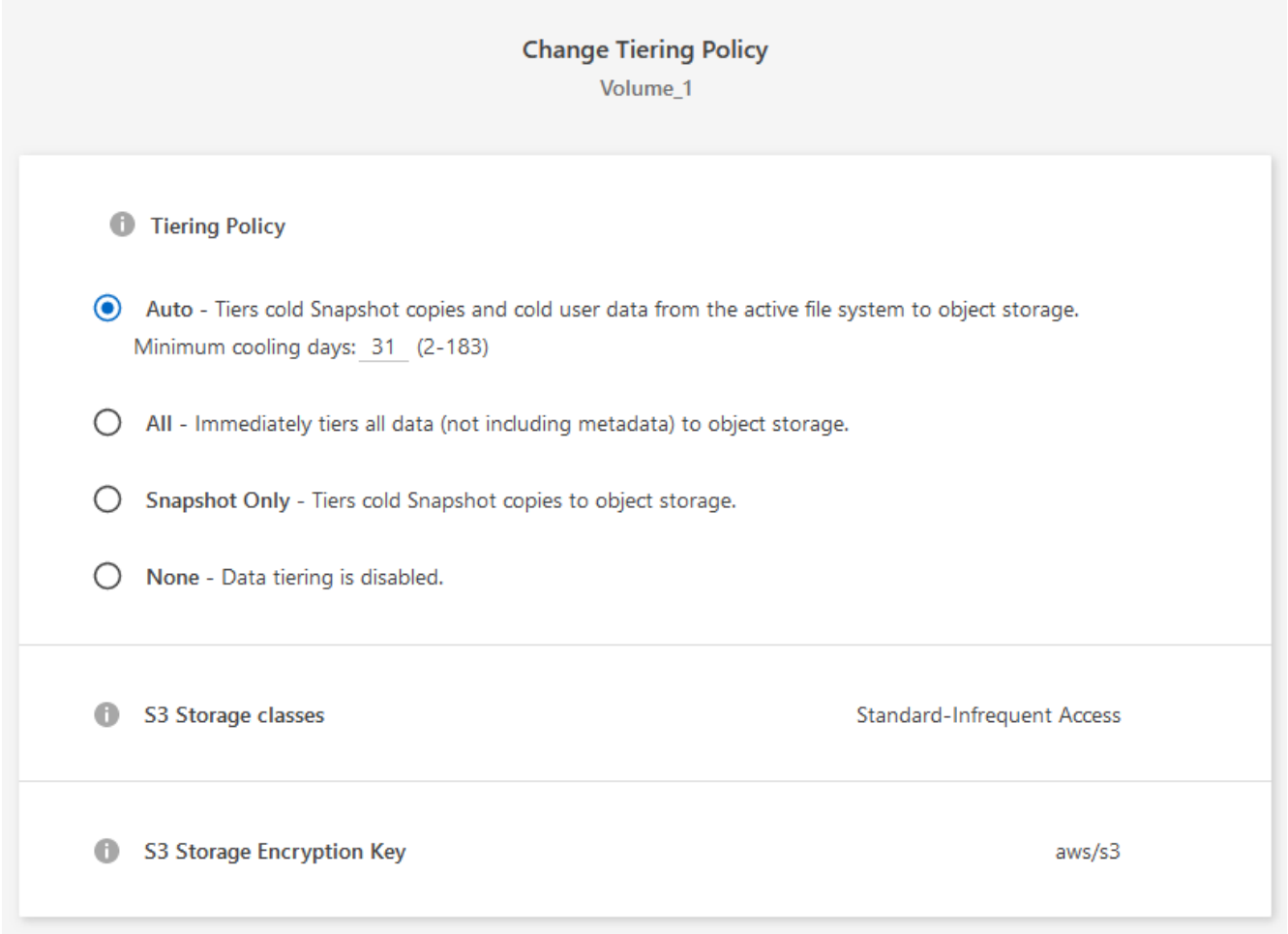
1. 시스템 아래의 볼륨 탭에서 새 볼륨을 생성하거나 기존 볼륨의 계층을 변경합니다.

일	행동
새 볼륨을 만듭니다	*새 볼륨 추가*를 클릭합니다.
기존 볼륨 수정	원하는 볼륨 타일을 선택하고 *볼륨 관리*를 클릭하여 오른쪽 패널의 볼륨 관리에 액세스한 다음 오른쪽 패널 아래에서 *고급 작업*과 *계층화 정책 변경*을 클릭합니다.

2. 계층화 정책을 선택하세요.

   이러한 정책에 대한 설명은 다음을 참조하세요."데이터 계층화 개요" .

   예



데이터 계층화가 가능한 집계가 아직 없는 경우 콘솔은 볼륨에 대한 새로운 집계를 생성합니다.

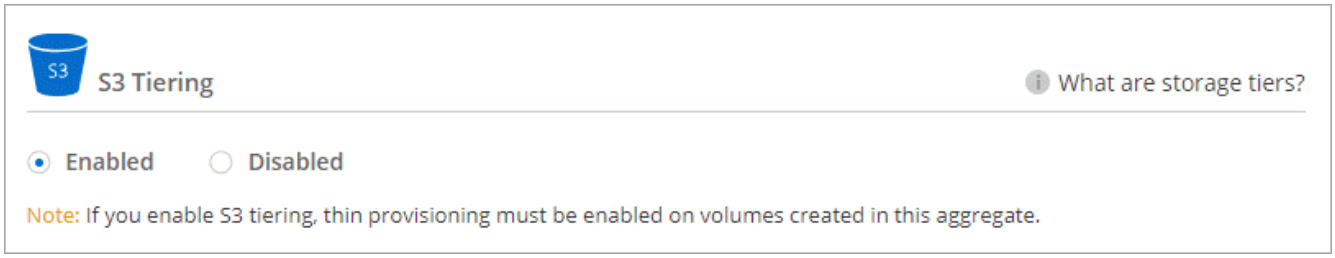
데이터 보호 볼륨의 계층 데이터

Cloud Volumes ONTAP 데이터 보호 볼륨에서 용량 계층으로 데이터를 계층화할 수 있습니다. 대상 볼륨을 활성화하면 데이터는 읽혀지면서 점차 성능 계층으로 이동합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 소스 볼륨이 포함된 Cloud Volumes ONTAP 시스템을 선택한 다음 볼륨을 복제하려는 시스템으로 끌어다 놓습니다.
3. 계층화 페이지에 도달할 때까지 안내를 따르고 개체 스토리지에 대한 데이터 계층화를 활성화합니다.

   예



데이터 복제에 대한 도움말은 다음을 참조하세요. "클라우드에서 데이터 복제 및 클라우드로 데이터 복제" .

계층화된 데이터의 스토리지 클래스 변경

Cloud Volumes ONTAP 배포한 후 30일 동안 액세스되지 않은 비활성 데이터의 스토리지 클래스를 변경하여 스토리지 비용을 줄일 수 있습니다. 데이터에 액세스하는 경우 액세스 비용이 더 높아지므로 스토리지 클래스를 변경하기 전에 이 점을 고려해야 합니다.

계층형 데이터의 저장 클래스는 볼륨별이 아닌 시스템 전체에 적용됩니다.

지원되는 스토리지 클래스에 대한 정보는 다음을 참조하세요."데이터 계층화 개요" .

단계

1. Cloud Volumes ONTAP 시스템에서 메뉴 아이콘을 클릭한 다음 스토리지 클래스 또는 *Blob 스토리지 계층화*를 클릭합니다.
2. 저장 클래스를 선택한 다음 *저장*을 클릭합니다.

데이터 계층화를 위한 여유 공간 비율 변경

데이터 계층화를 위한 여유 공간 비율은 데이터를 개체 스토리지에 계층화할 때 Cloud Volumes ONTAP SSD/HDD에 필요한 여유 공간의 양을 정의합니다. 기본 설정은 10%의 여유 공간이지만, 요구 사항에 맞게 설정을 조정할 수 있습니다.

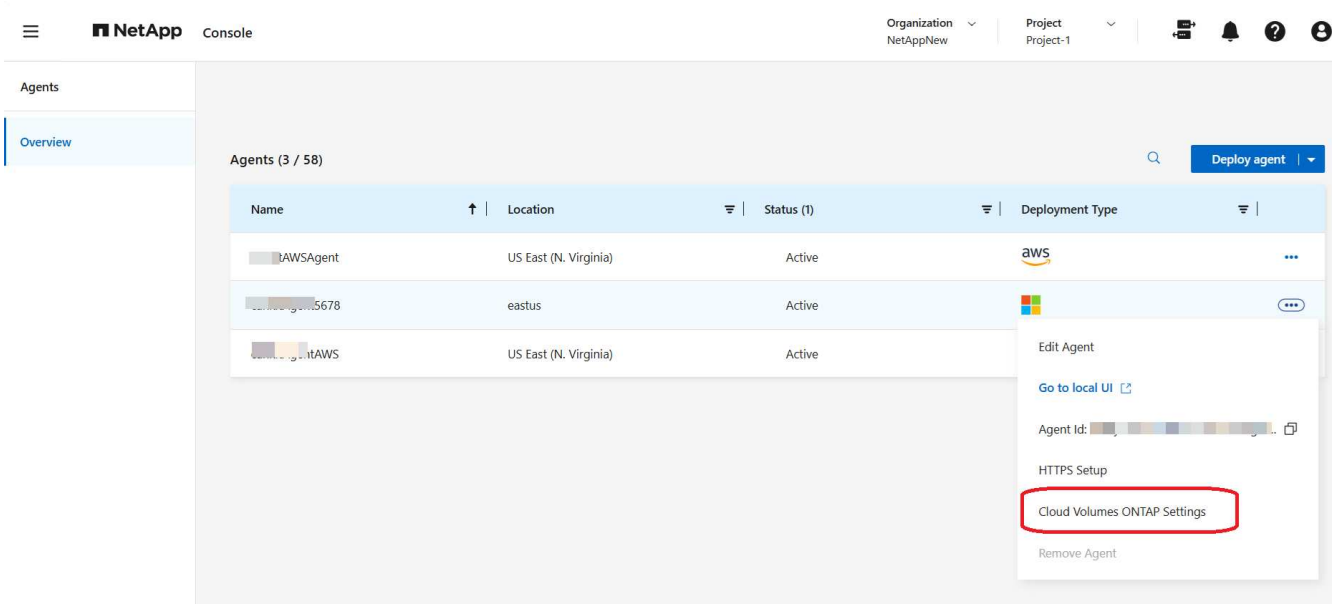
예를 들어, 구매한 용량을 충분히 활용하려면 10% 미만의 여유 공간을 선택하는 것이 좋습니다. 콘솔은 추가 용량이 필요할 때(전체 디스크 한도에 도달할 때까지) 추가 디스크를 구매할 수 있습니다.

충분한 공간이 없으면 Cloud Volumes ONTAP 이 데이터를 이동할 수 없으며 성능 저하가 발생할 수 있습니다. 모든 변경은 신중하게 이루어져야 합니다. 확실하지 않은 경우 NetApp 지원팀에 문의하여 안내를 받으세요.

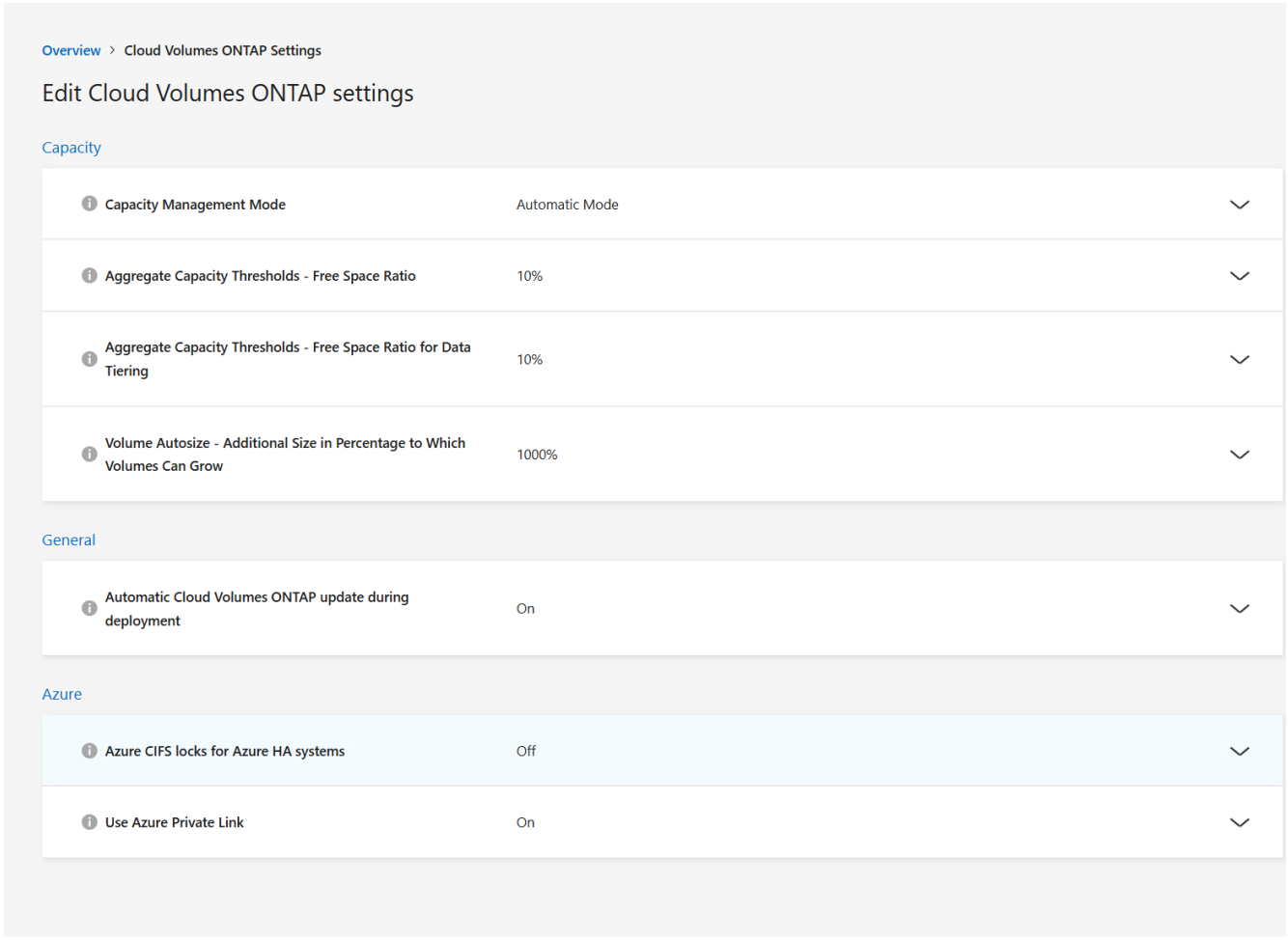
재해 복구 시나리오에서는 이 비율이 중요합니다. 왜냐하면 개체 저장소에서 데이터를 읽을 때 Cloud Volumes ONTAP 해당 데이터를 SSD/HDD로 옮겨 더 나은 성능을 제공하기 때문입니다. 충분한 공간이 없으면 Cloud Volumes ONTAP 이 데이터를 이동할 수 없습니다. 비즈니스 요구 사항을 충족할 수 있도록 비율을 변경할 때 이 점을 고려하세요.

단계

1. 왼쪽 탐색 창에서 *관리 > 에이전트*로 이동합니다.
2. 클릭 Cloud Volumes ONTAP 시스템을 관리하는 콘솔 에이전트의 아이콘입니다.
3. * Cloud Volumes ONTAP 설정*을 선택합니다.



4. *용량*에서 *데이터 계층화를 위한 집계 용량 임계값 - 여유 공간 비율*을 클릭합니다.



5. 요구 사항에 맞게 여유 공간 비율을 변경하고 *저장*을 클릭하세요.

자동 티어링 정책의 냉각 기간 변경

자동 계층화 정책을 사용하여 Cloud Volumes ONTAP 볼륨에서 데이터 계층화를 활성화한 경우 비즈니스 요구 사항에 따라 기본 냉각 기간을 조정할 수 있습니다. 이 작업은 ONTAP CLI 및 API를 사용해서만 지원됩니다.

쿨링 기간이란 볼륨의 사용자 데이터가 "콜드" 상태로 간주되어 개체 스토리지로 이동되기 전에 비활성 상태를 유지해야 하는 일 수입니다.

자동 티어링 정책의 기본 냉각 기간은 31일입니다. 냉각 기간은 다음과 같이 변경할 수 있습니다.

- 9.8 이상: 2일 ~ 183일
- 9.7 이하: 2일 ~ 63일

단계

1. 볼륨을 생성하거나 기존 볼륨을 수정할 때 API 요청과 함께 *minimumCoolingDays* 매개변수를 사용하세요.

시스템 해체 시 **S3** 버킷 제거

환경을 해제할 때 Cloud Volumes ONTAP 시스템에서 계층화된 데이터가 있는 S3 버킷을 삭제할 수 있습니다.

다음과 같은 경우에만 S3 버킷을 삭제할 수 있습니다.

- Cloud Volume ONTAP 시스템이 콘솔에서 삭제됩니다.
- 버킷에서 모든 객체가 삭제되고 S3 버킷이 비어 있습니다.

Cloud Volumes ONTAP 시스템을 해제해도 해당 환경을 위해 생성된 S3 버킷은 자동으로 삭제되지 않습니다. 대신 실수로 데이터가 손실되는 것을 방지하기 위해 고아 상태로 유지됩니다. 버킷에 있는 객체를 삭제한 다음 S3 버킷 자체를 제거하거나 나중에 사용하기 위해 보관할 수 있습니다. 참조하다 "ONTAP CLI: vserver 객체-저장소-서버 버킷 삭제" .

호스트 시스템에서 **Cloud Volumes ONTAP** 의 **LUN**에 연결합니다.

iSCSI 볼륨을 생성하면 NetApp Console 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후 IQN을 사용하여 호스트에서 LUN에 연결합니다.

다음 사항에 유의하세요.

- 콘솔의 자동 용량 관리 기능은 LUN에 적용되지 않습니다. LUN을 생성하면 자동 증가 기능이 비활성화됩니다.
- ONTAP 시스템 관리자나 ONTAP CLI에서 추가 LUN을 생성할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 볼륨을 관리할 Cloud Volumes ONTAP 시스템을 두 번 클릭합니다.
3. 시스템에서 볼륨 탭을 선택합니다.
4. 필요한 볼륨 타일로 이동한 다음 *볼륨 관리*를 선택하여 오른쪽의 볼륨 관리 패널에 액세스합니다.
5. *대상 iQN*을 클릭합니다.

6. *복사*를 클릭하여 iQN 이름을 복사합니다.
7. 호스트에서 LUN으로 iSCSI 연결을 설정합니다.
    - "Red Hat Enterprise Linux를 위한 ONTAP 9 iSCSI express 구성: 대상에서 iSCSI 세션 시작"
    - "Windows용 ONTAP 9 iSCSI express 구성: 대상과 iSCSI 세션 시작"
    - "ONTAP SAN 호스트 구성"

Cloud Volumes ONTAP 시스템에서 FlexCache 볼륨을 사용하여 데이터 액세스 가속화

FlexCache 볼륨은 원본(또는 소스) 볼륨에서 SMB 및 NFS 읽기 데이터를 캐시하는 스토리지 볼륨입니다. 캐시된 데이터를 이어서 읽으면 해당 데이터에 더 빨리 액세스할 수 있습니다.

FlexCache 볼륨을 사용하면 데이터 액세스 속도를 높이거나 액세스 빈도가 높은 볼륨의 트래픽을 오프로드할 수 있습니다. FlexCache 볼륨은 특히 클라이언트가 동일한 데이터에 반복적으로 액세스해야 할 때 성능을 개선하는 데 도움이 됩니다. 원본 볼륨에 액세스하지 않고도 데이터를 직접 제공할 수 있기 때문입니다. FlexCache 볼륨은 읽기 작업이 많은 시스템 작업 부하에 적합합니다.

NetApp Console FlexCache 볼륨 관리를 제공합니다."NetApp Volume Caching" .

ONTAP CLI 또는 ONTAP 시스템 관리자를 사용하여 FlexCache 볼륨을 생성하고 관리할 수도 있습니다.

- "더 빠른 데이터 액세스를 위한 FlexCache 볼륨 전원 가이드"
- "System Manager에서 FlexCache 볼륨 생성"

원본이 암호화된 경우 **FlexCache** 와 함께 작업합니다.

원본 볼륨이 암호화된 Cloud Volumes ONTAP 시스템에서 FlexCache 구성하는 경우 FlexCache 볼륨이 암호화된

데이터에 적절하게 액세스하고 캐싱할 수 있도록 추가 단계가 필요합니다.

시작하기 전에

1. 암호화 설정: 소스 볼륨이 완전히 암호화되어 작동 가능한지 확인합니다. Cloud Volumes ONTAP 시스템의 경우 클라우드별 키 관리 서비스와의 통합이 필요합니다.

AWS의 경우 일반적으로 AWS Key Management Service(KMS)를 사용하는 것을 의미합니다. 자세한 내용은 다음을 참조하세요."AWS Key Management Service로 키 관리" .

Azure의 경우 NetApp 볼륨 암호화(NVE)를 위해 Azure Key Vault를 설정해야 합니다. 자세한 내용은 다음을 참조하세요."Azure Key Vault를 사용하여 키 관리" .

Google Cloud의 경우 Google Cloud Key Management Service입니다. 자세한 내용은 다음을 참조하세요."Google의 Cloud Key Management Service로 키 관리" .

1. 키 관리 서비스: FlexCache 볼륨을 생성하기 전에 Cloud Volumes ONTAP 시스템에서 키 관리 서비스가 올바르게 구성되었는지 확인하세요. 이 구성은 FlexCache 볼륨이 원본 볼륨의 데이터를 암호 해독하는 데 필수적입니다.
2. 라이선스: 유효한 FlexCache 라이선스가 Cloud Volumes ONTAP 시스템에서 사용 가능하고 활성화되었는지 확인합니다.
3. * ONTAP 버전*: Cloud Volumes ONTAP 시스템의 ONTAP 버전이 암호화된 볼륨이 있는 FlexCache 지원하는지 확인하세요. 최신 내용을 참조하세요 "ONTAP 릴리스 노트" 자세한 내용은 호환성 매트릭스를 참조하세요.
4. 네트워크 구성: 네트워크 구성이 원본 볼륨과 FlexCache 볼륨 간의 원활한 통신을 허용하는지 확인하세요. 여기에는 클라우드 환경에서의 적절한 라우팅과 DNS 확인이 포함됩니다.

단계

암호화된 소스 볼륨을 사용하여 Cloud Volumes ONTAP 시스템에 FlexCache 볼륨을 만듭니다. 자세한 단계와 추가 고려 사항은 다음 섹션을 참조하세요.

- "더 빠른 데이터 액세스를 위한 FlexCache 볼륨 전원 가이드"
- "System Manager에서 FlexCache 볼륨 생성"

집계 관리

Cloud Volumes ONTAP 시스템에 대한 집계를 만듭니다.

직접 집계를 만들 수도 있고 NetApp Console 볼륨을 생성할 때 집계를 대신 만들어 줄 수도 있습니다. 집계를 직접 만드는 이점은 기본 디스크 크기를 선택할 수 있다는 점입니다. 즉, 필요한 용량이나 성능에 맞게 집계 크기를 조정할 수 있습니다.

모든 디스크와 집계는 콘솔에서 직접 만들고 삭제해야 합니다. 다른 관리 도구에서는 이러한 작업을 수행해서는 안 됩니다. 그렇게 하면 시스템 안정성에 영향을 미치고, 나중에 디스크를 추가하는 기능을 방해할 수 있으며, 잠재적으로 중복된 클라우드 공급자 수수료가 발생할 수 있습니다.

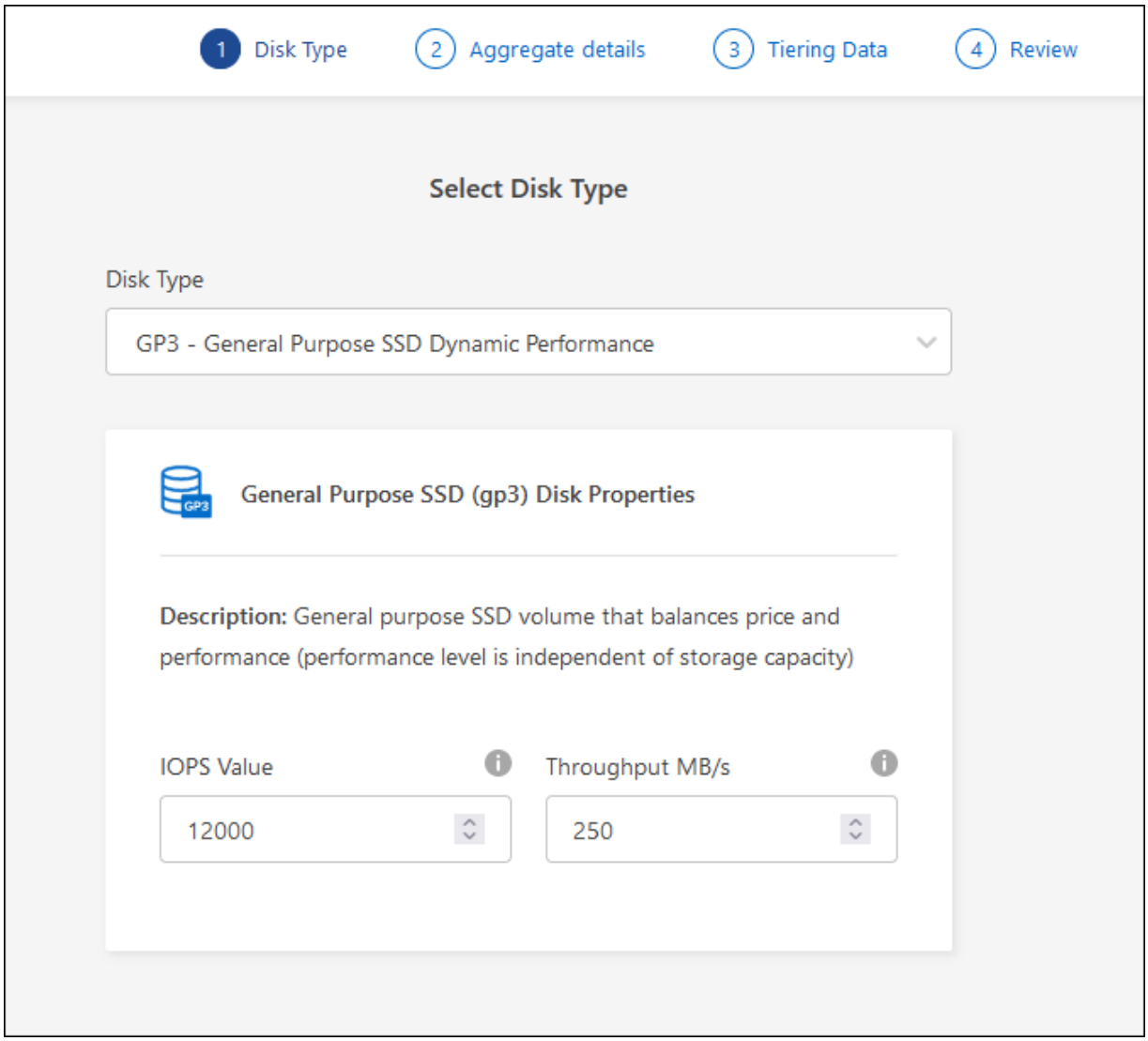
단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 집계를 관리하려는 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.

3. 집계 탭에서 *집계 추가*를 클릭한 다음 집계에 대한 세부 정보를 지정합니다.

AWS

- 디스크 유형 및 디스크 크기를 선택하라는 메시지가 표시되면 다음을 참조하세요."AWS에서 Cloud Volumes ONTAP 구성을 계획하세요" .
- 집계의 용량 크기를 입력하라는 메시지가 표시되면 Amazon EBS Elastic Volumes 기능을 지원하는 구성에서 집계를 생성하고 있는 것입니다. 다음 스크린샷은 gp3 디스크로 구성된 새로운 집계의 예를 보여줍니다.



"Elastic Volumes 지원에 대해 자세히 알아보세요" .

하늘빛

디스크 유형 및 디스크 크기에 대한 도움말은 다음을 참조하세요."Azure에서 Cloud Volumes ONTAP 구성 계획" .

구글 클라우드

디스크 유형 및 디스크 크기에 대한 도움말은 다음을 참조하세요."Google Cloud에서 Cloud Volumes ONTAP 구성을 계획하세요." .

4. *추가*를 클릭한 다음 *승인 및 구매*를 클릭합니다.

Cloud Volumes ONTAP 클러스터에 대한 집계 관리

디스크를 추가하고, 집계에 대한 정보를 보고, 삭제하여 집계를 직접 관리합니다.

> 모든 디스크와 집계는 NetApp Console 에서 직접 만들고 삭제해야 합니다. 다른 관리 도구에서는 이러한 작업을 수행해서는 안 됩니다. 그렇게 하면 시스템 안정성에 영향을 미치고, 나중에 디스크를 추가하는 기능을 방해할 수 있으며, 잠재적으로 중복된 클라우드 공급자 수수료가 발생할 수 있습니다.

시작하기 전에

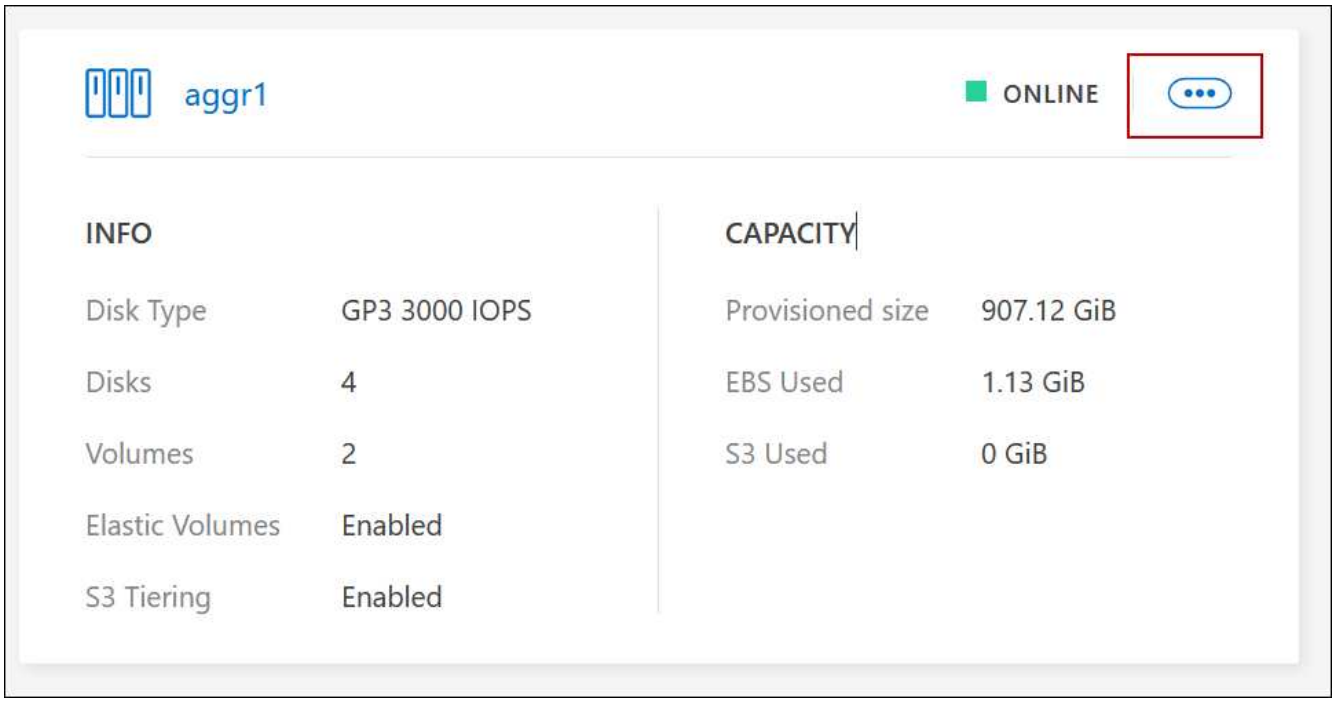
집계를 삭제하려면 먼저 집계에서 볼륨을 삭제해야 합니다.

이 작업에 관하여

집계된 공간이 부족한 경우 ONTAP System Manager를 사용하여 볼륨을 다른 집계로 이동할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 집계를 관리할 Cloud Volumes ONTAP 시스템을 두 번 클릭합니다.
3. 시스템 세부 정보에서 집계 탭을 클릭합니다.
4. 필요한 집계를 위해 다음을 클릭하세요. ••• 관리 작업에 대한 아이콘입니다.



5. 사용 가능한 옵션에서 집계를 관리하세요. ••• 메뉴.

> 집계에 디스크를 추가하려면 집계에 있는 모든 디스크의 크기가 동일해야 합니다.

AWS의 경우 Amazon EBS Elastic Volumes를 지원하는 집계의 용량을 늘릴 수 있습니다.

1. 아래에 ••• 메뉴에서 *용량 늘리기*를 클릭하세요.
2. 추가하려는 용량을 입력한 다음 *증가*를 클릭하세요.

집계 용량을 최소 256GiB 또는 집계 크기의 10%만큼 늘려야 합니다. 예를 들어, 1.77TiB 집계가 있는 경우 10%는 181GiB입니다. 이는 256GiB보다 작으므로 집계 크기도 최소 256GiB만큼 늘어나야 합니다.

콘솔 에이전트에서 **Cloud Volumes ONTAP** 집계 용량 관리

각 콘솔 에이전트에는 Cloud Volumes ONTAP 의 집계 용량을 관리하는 방법을 결정하는 설정이 있습니다.

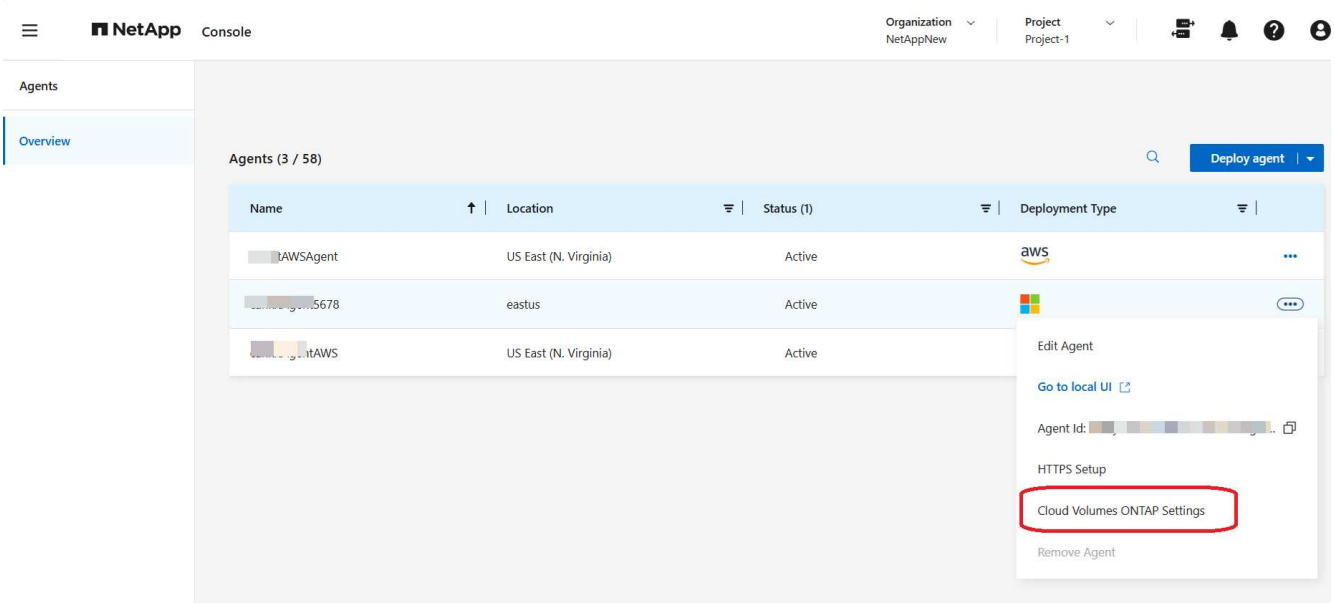
이러한 설정은 콘솔 에이전트에서 관리하는 모든 Cloud Volumes ONTAP 시스템에 영향을 미칩니다. 다른 콘솔 에이전트가 있는 경우 다르게 구성할 수 있습니다.

필요한 권한

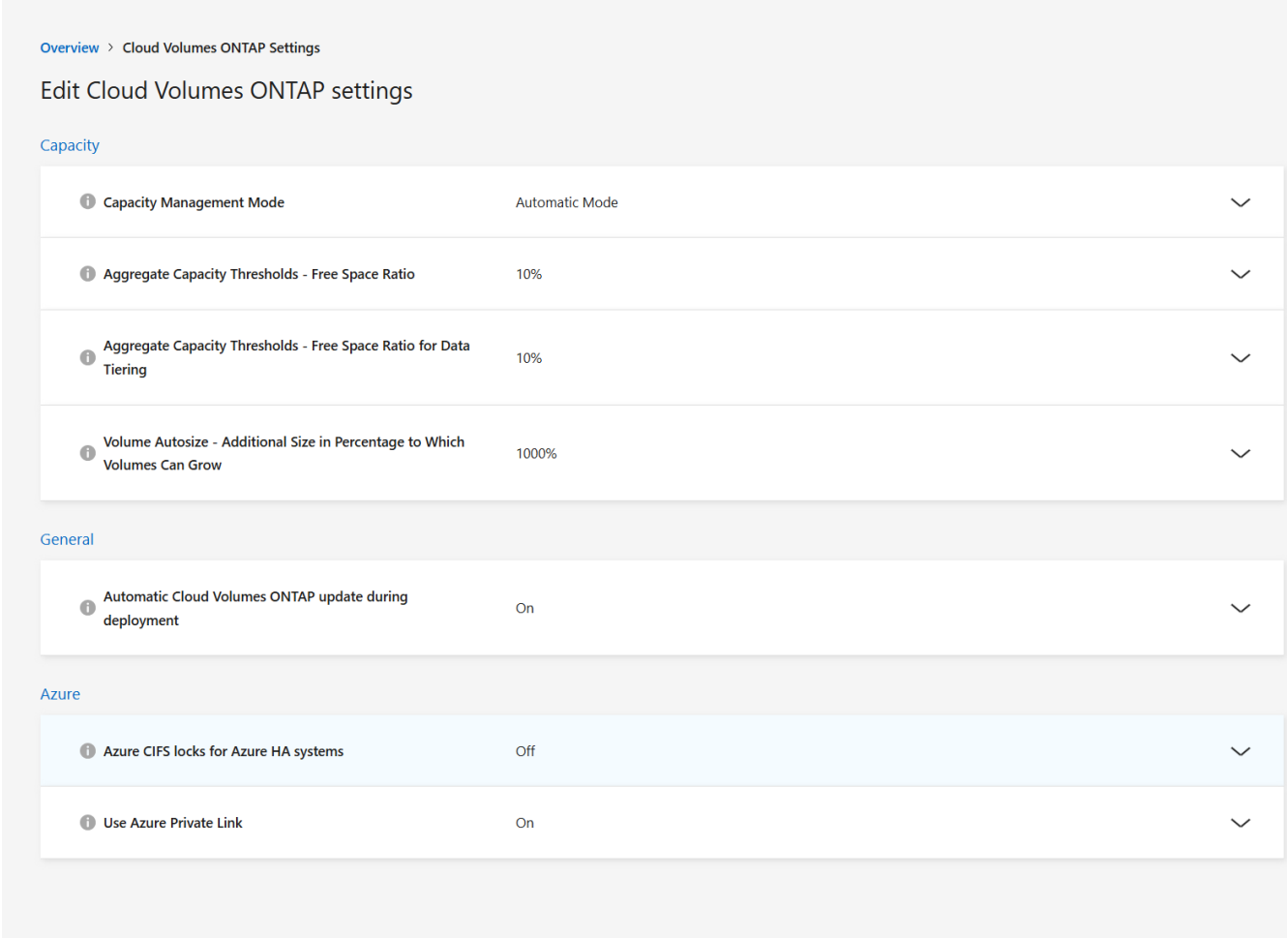
Cloud Volumes ONTAP 설정을 수정하려면 NetApp Console 의 조직 또는 계정 관리자 권한이 필요합니다.

단계

1. 왼쪽 탐색 창에서 *관리 > 에이전트*로 이동합니다.
2. 클릭 ••• Cloud Volumes ONTAP 시스템을 관리하는 콘솔 에이전트의 아이콘입니다.
3. * Cloud Volumes ONTAP 설정*을 선택합니다.



4. *용량*에서 다음 설정을 수정하세요.



용량 관리 모드

콘솔에서 저장 용량 결정 사항을 알려야 하는지, 아니면 자동으로 용량 요구 사항을 관리해야 하는지 선택하세요.

"용량 관리 모드의 작동 방식 알아보기" .

총 용량 임계값 - 여유 공간 비율

이 비율은 용량 관리 결정에 있어 핵심 매개변수이며, 용량 관리 모드가 자동이든 수동이든 관계없이 이 비율의 영향을 이해하는 것이 필수적입니다. 리소스 활용도와 비용 간의 균형을 유지하려면 특정 저장 요구 사항과 예상되는 성장 상황을 고려하여 이 임계값을 설정하는 것이 좋습니다.

수동 모드에서 집계의 여유 공간 비율이 지정된 임계값 아래로 떨어지면 알림이 트리거되어 여유 공간 비율이 낮은 문제를 해결하기 위한 조치를 취해야 함을 알려줍니다. 서비스 중단을 방지하고 최적의 성능을 보장하려면 이러한 알림을 모니터링하고 집계 용량을 수동으로 관리하는 것이 중요합니다.

여유 공간 비율은 다음과 같이 계산됩니다. (집계 용량 - 집계에서 사용된 총 용량) / 집계 용량

참조하다"자동 용량 관리" 이제 Cloud Volumes ONTAP 에서 용량이 자동으로 관리됩니다.

집계 용량 임계값 - 데이터 계층화를 위한 여유 공간 비율

데이터를 용량 계층(개체 스토리지)으로 계층화할 때 성능 계층(디스크)에 얼마나 많은 여유 공간이 필요한지 정의합니다.

이 비율은 재해 복구 시나리오에서 중요합니다. 데이터가 용량 계층에서 읽히면 Cloud Volumes ONTAP 더 나은 성능을 제공하기 위해 데이터를 성능 계층으로 이동합니다. 충분한 공간이 없으면 Cloud Volumes ONTAP

이 데이터를 이동할 수 없습니다.

5. *저장*을 클릭하세요.

Azure에서 디스크 성능 관리

Azure Cloud Volumes ONTAP 에서 **Premium SSD v2** 디스크 성능을 관리하세요**.**

Azure에서 Cloud Volumes ONTAP 성능을 최적화하려면 Premium SSD v2 디스크의 IOPS 및 처리량 매개변수를 구성하면 됩니다. 이 기능은 Cloud Volumes ONTAP Azure Premium SSD v2 디스크 유형으로 이미 배포된 경우에만 사용할 수 있으며, 초기 배포 시에는 사용할 수 없습니다. 성능을 향상시키면 Azure Premium SSD v2 디스크의 모든 유연성과 고성능 기능을 활용할 수 있습니다.

프리미엄 SSD v2 디스크는 낮은 지연 시간, 높은 IOPS 및 높은 처리량을 통해 빠르고 안정적인 성능이 필요한 워크로드를 지원합니다. IOPS 및 처리량 설정을 조정하여 배포 환경에서 집계 도구의 성능을 맞춤 설정할 수 있습니다. Premium SSD v2 디스크에 대한 자세한 내용은 다음을 참조하십시오. "Premium SSD v2 디스크를 배포하세요" .

API를 사용하여 Premium SSD v2 디스크 설정 수정 프로세스를 자동화하세요. Cloud Volumes ONTAP API 호출 실행에 대한 자세한 내용은 다음을 참조하십시오. "첫 번째 API 호출" .

이 작업에 관하여

- 이 기능은 Azure 단일 가용성 영역의 Cloud Volumes ONTAP 배포에 적용됩니다.
- 디스크 설정을 변경하면 RAID 그룹 또는 집합체의 성능이 일괄적으로 변경됩니다. 집합체 내 모든 디스크의 성능은 집합체 전체에서 일관된 성능을 보장하기 위해 동일한 수준으로 조정됩니다.
- 이러한 변화는 단일 집합체에만 영향을 미치며 그룹 내의 다른 집합체에는 영향을 미치지 않습니다.
- NetApp Console 에서 Cloud Volumes ONTAP 배포 또는 용량 최적화 중에 자동으로 프로비저닝되거나 API를 통해 추가된 Premium SSD v2 디스크는 모두 수정 가능합니다.
- 디스크 크기 조정(디스크 용량 변경)은 지원되지 않습니다.

시작하기 전에

Premium SSD v2 디스크의 IOPS 및 처리량 매개변수를 구성하기 전에 다음 사항에 유의하십시오.

- 프리미엄 SSD v2 데이터 디스크만 선택했는지 확인하십시오. 프리미엄 SSD v1 디스크 또는 루트 및 부팅 디스크는 이 변경 사항의 적용 대상이 아닙니다.
- 배포 중에 Cloud Volumes ONTAP 에서 설정한 사전 구성된 기준 설정을 해당 디스크 크기에 대한 최소 IOPS 및 처리량 값으로 사용하십시오. 이러한 기본 설정은 Premium SSD v1의 성능 특성과 일치합니다.
- 디스크 크기에 맞는 최소 기준선 이상으로 IOPS 및 처리량 값을 설정하십시오. 예를 들어, 1TB 디스크 크기의 경우 최소 IOPS 값을 5,000으로, 최소 처리량 값을 200MBps로 설정하십시오. 이 최소값보다 높은 값은 설정할 수 있지만 낮은 값은 설정할 수 없습니다.
- 지원되는 Premium SSD v2 범위 내에서 값을 구성하십시오. IOPS는 3000~80000, 처리량은 125~1200MBps입니다.
- Azure의 Cloud Volumes ONTAP 에서 지원되는 범위인 500GB~32TB 내에 Premium SSD v2 디스크 크기가 있는지 확인하십시오. 참고로 이러한 크기 제한은 Azure에서 Premium SSD v2 디스크에 대해 제공하는 최소 및 최대 값과 다릅니다.

단계

- 다음 API 호출을 사용하여 IOPS 및 처리량 속성 값을 변경하십시오.

  이 API는 24시간 내에 최대 4회까지 호출할 수 있습니다.

  `PUT /azure/vsa/aggregates/{workingEnvironmentId}/{aggregateName}`

  요청 본문에 다음 매개변수를 포함합니다.

```
{
  "aggregateName": "aggr_name",
  "iops": "modified_iops_value",
  "throughput": "modified_throughput_value",
  "workingEnvironmentId": "we_id"
}
```

당신이 완료한 후

API에서 작업이 성공했다는 응답이 반환되면 Azure 포털에서 Cloud Volumes ONTAP 시스템의 디스크 세부 정보를 확인하여 수정된 매개변수를 검증하십시오.

관련 정보

- "API 사용을 준비하세요"
- "Cloud Volumes ONTAP 워크플로"
- "필수 식별자 가져오기"
- "Cloud Volumes ONTAP 용 REST API 사용"
- "가용성 세트의 VM에서 Premium SSD v2를 사용하세요."

Azure Cloud Volumes ONTAP 에서 프리미엄 **SSD** 디스크의 성능 계층을 변경합니다**.**

Azure 포털을 사용하여 Azure의 Cloud Volumes ONTAP 에서 프리미엄 SSD 관리 디스크의 성능 등급을 업그레이드할 수 있습니다. 이는 각 프리미엄 SSD 디스크의 디스크 티어를 더 높은 성능 티어로 변경하는 수동 프로세스입니다. NVRAM 디스크의 성능 등급을 변경하면 더 높은 IOPS 및 처리량 기능을 제공하여 성능 병목 현상을 완화하고 Cloud Volumes ONTAP 시스템의 효율성을 향상시킬 수 있습니다.

NetApp 지원팀과 협력하여 환경에서 발생하는 병목 현상이 NVRAM 디스크 때문인지 확인하고, 티어 업그레이드를 통해 문제가 해결되는지 확인하십시오.

이 작업에 관하여

- Azure의 Cloud Volumes ONTAP 기본적으로 P20 계층에 NVRAM 용으로 프리미엄 SSD 디스크를 배포합니다. P20 등급은 대부분의 작업 부하에 적합한 균형 잡힌 성능을 제공합니다. 하지만 작업 부하에 더 높은 성능이 요구되는 경우 NVRAM 디스크를 P30과 같은 상위 등급으로 업그레이드할 수 있습니다.

  현재로서는 Azure 포털을 통해서만 NVRAM 디스크를 P20 티어에서 P30 티어로 업그레이드할 수 있습니다.

- 디스크 크기는 변경하지 않습니다. 용량은 여전히 512GB입니다. 이 절차는 디스크의 성능 등급만 변경합니다.

시작하기 전에

- NVRAM 디스크를 더 높은 성능 등급으로 업그레이드하면 추가 비용이 발생하므로 이러한 변경의 필요성을 신중하게 평가하십시오.
- Cloud Volumes ONTAP 버전은 9.11.1 이상이어야 합니다. 하위 버전의 경우 9.11.1 이상 버전으로 업그레이드하거나 NetApp 지원팀에 기능 정책 변경 요청(FPVR)을 제출할 수 있습니다.

단계

이 시나리오는 노드가 두 개 있다고 가정합니다. `node01` 그리고 `node02` Cloud Volumes ONTAP 고가용성(HA) 배포에서. Azure 포털을 사용하여 티어를 업그레이드하세요.

1. 만들기 위해 이 명령어를 실행하세요 `node1` 활성 노드. 수동 페일오버 `node02`.

   ```
   storage failover takeover -ofnode <Node02>
   ```

2. Azure Portal에 Sign in .
3. 인수 작업이 완료되면 VM 인스턴스로 이동하세요. `node02`그리고 정지 버튼을 클릭하여 전원을 끄세요.
4. 해당 리소스 그룹으로 이동하세요. `node02` 디스크 목록에서 티어를 변경할 NVRAM 디스크를 선택합니다.
5. 크기와 성능을 모두 고려하여 선택하세요.
6. 성능 등급 드롭다운 메뉴에서 선택하세요. `P30 - 5000 IOPS, 200MB/s`.
7. *크기 조정*을 선택하세요.
8. 스위치를 켜세요 `node02` 사례.
9. Azure 시리얼 콘솔에서 메시지가 표시될 때까지 확인하세요. `waiting for giveback`.
10. 이 명령어를 실행하여 돌려주세요 `node02`:

    ```
    storage failover giveback -ofnode <Node02>
    ```

11. 다음 단계를 반복하세요. `node01` 만들다 `node02` 인수하다 `node01`이를 통해 NVRAM 디스크 계층을 업그레이드할 수 있습니다. `node01`.

당신이 완료한 후

두 노드를 모두 켠 후에는 Azure 포털에서 Cloud Volumes ONTAP 시스템의 디스크 세부 정보를 확인하여 수정된 매개변수를 검증하십시오.

관련 정보

- Azure 설명서: "다운타임 없이 성능 등급을 변경하세요"
- 지원팀을 위한 지식 기반: "Azure CVO에서 NVRAM 디스크의 성능 계층을 업그레이드하는 방법"
- "Cloud Volumes ONTAP 소프트웨어 버전 업그레이드"

스토리지 VM 관리

Cloud Volumes ONTAP 의 스토리지 VM 관리

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에게 스토리지 및 데이터 서비스를 제공합니다. 이것을 *SVM* 또는 _vserver_라고 알고 있을 수도 있습니다. Cloud Volumes ONTAP 은 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다.

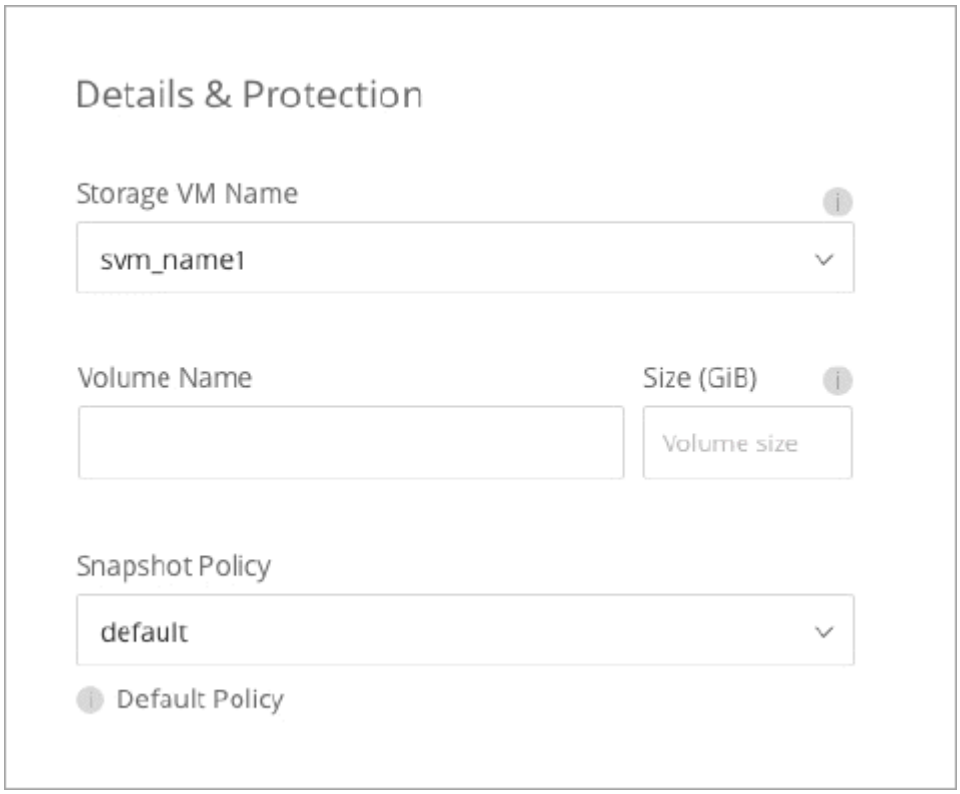
지원되는 스토리지 VM 수

특정 구성에서는 여러 개의 스토리지 VM이 지원됩니다. 로 가다 "Cloud Volumes ONTAP 릴리스 노트" Cloud Volumes ONTAP 버전에 지원되는 스토리지 VM 수를 확인하세요.

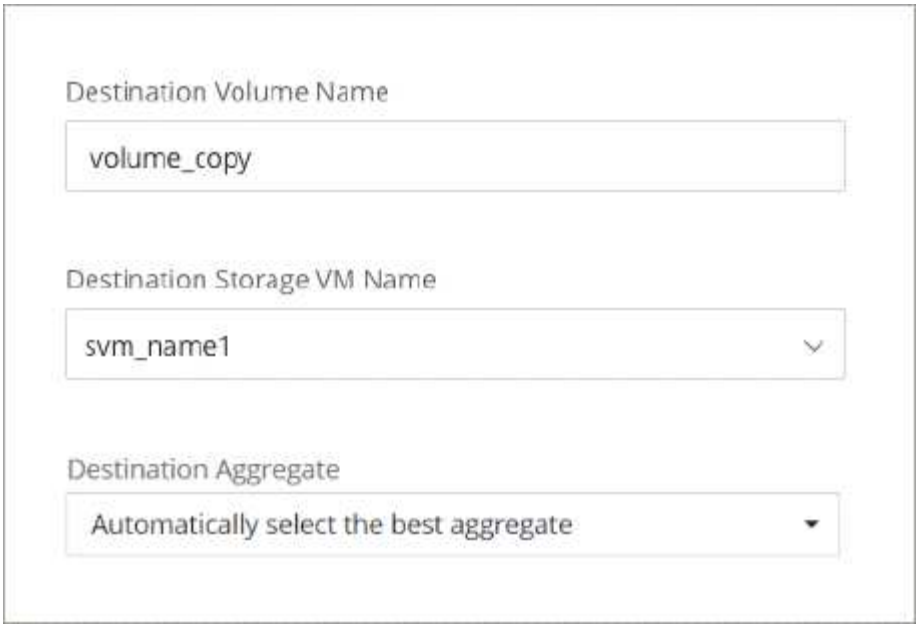
여러 스토리지 VM으로 작업

NetApp Console ONTAP System Manager나 ONTAP CLI에서 생성하는 모든 추가 스토리지 VM을 지원합니다.

예를 들어, 다음 이미지는 볼륨을 생성할 때 스토리지 VM을 선택하는 방법을 보여줍니다.



다음 이미지는 볼륨을 다른 시스템에 복제할 때 스토리지 VM을 선택하는 방법을 보여줍니다.



기본 스토리지 **VM**의 이름을 수정합니다**.**

콘솔은 Cloud Volumes ONTAP 에 대해 생성하는 단일 스토리지 VM의 이름을 자동으로 지정합니다. 엄격한 명명 기준이 있는 경우 ONTAP 시스템 관리자, ONTAP CLI 또는 API를 사용하여 스토리지 VM의 이름을 수정할 수 있습니다. 예를 들어, ONTAP 클러스터의 스토리지 VM에 지정한 이름과 일치하도록 이름을 지정할 수 있습니다.

AWS에서 Cloud Volumes ONTAP 위한 데이터 제공 스토리지 VM 관리

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에게 스토리지 및 데이터 서비스를 제공합니다. 이것을 *SVM* 또는 _vserver_라고 알고 있을 수도 있습니다. Cloud Volumes ONTAP 은 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다.

추가 데이터 제공 스토리지 VM을 생성하려면 AWS에서 IP 주소를 할당한 다음 Cloud Volumes ONTAP 구성에 따라 ONTAP 명령을 실행해야 합니다.

지원되는 스토리지 VM 수

9.7 릴리스부터 특정 Cloud Volumes ONTAP 구성에서 여러 스토리지 VM이 지원됩니다. 로 가다 "Cloud Volumes ONTAP 릴리스 노트" Cloud Volumes ONTAP 버전에 지원되는 스토리지 VM 수를 확인하세요.

다른 모든 Cloud Volumes ONTAP 구성은 재해 복구에 사용되는 하나의 데이터 제공 스토리지 VM과 하나의 대상 스토리지 VM을 지원합니다. 소스 스토리지 VM에 장애가 발생하는 경우 데이터 액세스를 위해 대상 스토리지 VM을 활성화할 수 있습니다.

구성에 대한 제한 사항을 확인하세요

각 EC2 인스턴스는 네트워크 인터페이스당 최대 개수의 개인 IPv4 주소를 지원합니다. AWS에서 새로운 스토리지 VM에 IP 주소를 할당하기 전에 제한을 확인해야 합니다.

단계

1. 가다 "Cloud Volumes ONTAP 릴리스 노트의 스토리지 한도 섹션" .

2. 인스턴스 유형에 대한 인터페이스당 최대 IP 주소 수를 식별합니다.
3. 다음 섹션에서 AWS에서 IP 주소를 할당할 때 필요하므로 이 번호를 기록해 두세요.

AWS에서 **IP** 주소 할당

새 스토리지 VM에 대한 LIF를 생성하기 전에 AWS의 포트 e0a에 개인 IPv4 주소를 할당해야 합니다.

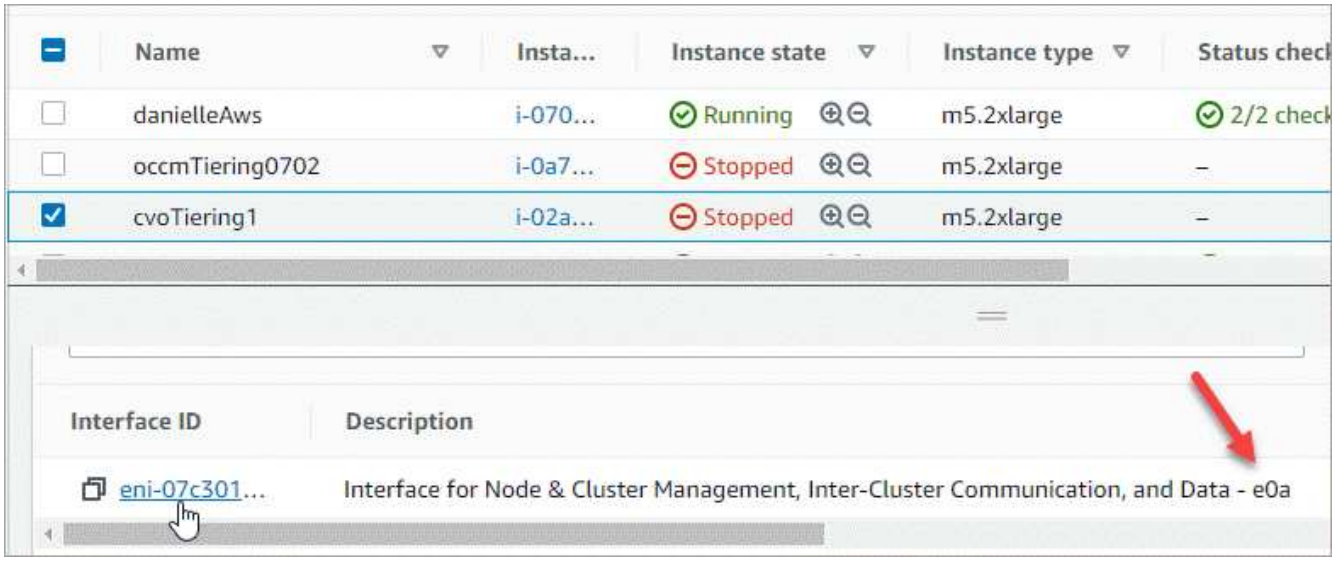
스토리지 VM용 선택적 관리 LIF에는 단일 노드 시스템과 단일 AZ의 HA 쌍에서 프라이빗 IP 주소가 필요합니다. 이 관리 LIF는 SnapCenter와 같은 관리 툴에 대한 연결을 제공합니다.

단계

1. AWS에 로그인하고 EC2 서비스를 엽니다.
2. Cloud Volumes ONTAP 인스턴스를 선택하고 *네트워킹*을 클릭합니다.

   HA 쌍에 스토리지 VM을 생성하는 경우 노드 1을 선택합니다.

3. *네트워크 인터페이스*로 스크롤하여 포트 e0a의 *인터페이스 ID*를 클릭합니다.



4. 네트워크 인터페이스를 선택하고 *작업 > IP 주소 관리*를 클릭합니다.
5. e0a의 IP 주소 목록을 확장합니다.
6. IP 주소를 확인하세요:
   a. 할당된 IP 주소의 수를 세어 포트에 추가 IP를 위한 공간이 있는지 확인하세요.

      이 페이지의 이전 섹션에서 인터페이스당 지원되는 IP 주소의 최대 개수를 확인했어야 합니다.

   b. 선택 사항: Cloud Volumes ONTAP 의 ONTAP CLI로 이동하여 *network interface show*를 실행하여 각 IP 주소가 사용 중인지 확인합니다.

      IP 주소가 사용되지 않으면 새 스토리지 VM에서 해당 IP 주소를 사용할 수 있습니다.

7. AWS 콘솔로 돌아와서 *새 IP 주소 할당*을 클릭하여 새 스토리지 VM에 필요한 양에 따라 추가 IP 주소를 할당합니다.

- 단일 노드 시스템: 사용하지 않는 보조 프라이빗 IP 1개가 필요합니다.

  스토리지 VM에 관리 LIF를 생성하려면 선택적 보조 개인 IP가 필요합니다.

- 단일 AZ의 HA 쌍: 노드 1에 사용되지 않는 보조 개인 IP가 하나 필요합니다.

  스토리지 VM에 관리 LIF를 생성하려면 선택적 보조 개인 IP가 필요합니다.

- 여러 AZ의 HA 쌍: 각 노드에 사용되지 않는 보조 개인 IP가 하나씩 필요합니다.

8. 단일 AZ의 HA 쌍에 IP 주소를 할당하는 경우 *보조 개인 IPv4 주소 재할당 허용*을 활성화합니다.
9. *저장*을 클릭하세요.
10. 여러 AZ에 HA 쌍이 있는 경우 노드 2에 대해 이 단계를 반복해야 합니다.

단일 노드 시스템에서 스토리지 **VM** 생성

이 단계는 단일 노드 시스템에 새 스토리지 VM을 생성합니다. NAS LIF를 생성하려면 프라이빗 IP 주소 하나가 필요하며, 관리 LIF를 생성하려면 선택적으로 프라이빗 IP 주소 하나가 더 필요합니다.

단계

1. 스토리지 VM과 스토리지 VM으로의 경로를 만듭니다.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. NAS LIF를 생성합니다.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node
```

   여기서 _private_ip_x_는 e0a의 사용되지 않는 보조 개인 IP입니다.

3. 선택 사항: 스토리지 VM 관리 LIF를 만듭니다.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

   여기서 _private_ip_y_는 e0a의 사용되지 않는 또 다른 보조 개인 IP입니다.

4. 스토리지 VM에 하나 이상의 집계를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

이 단계는 새 스토리지 VM이 볼륨을 생성하기 전에 최소한 하나의 집계에 액세스해야 하기 때문에 필요합니다.

단일 **AZ**의 **HA** 쌍에 스토리지 **VM** 생성

이 단계에서는 단일 AZ의 HA 쌍에 새로운 스토리지 VM을 만듭니다. NAS LIF를 생성하려면 개인 IP 주소 하나가 필요하고, 관리 LIF를 생성하려면 선택적으로 개인 IP 주소가 하나 더 필요합니다.

두 LIF는 모두 노드 1에 할당됩니다. 장애가 발생하면 개인 IP 주소가 노드 간에 이동할 수 있습니다.

단계

1. 스토리지 VM과 스토리지 VM으로의 경로를 만듭니다.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. 노드 1에 NAS LIF를 생성합니다.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

여기서 _private_ip_x_는 cvo-node1의 e0a에 있는 사용되지 않는 보조 개인 IP입니다. 서비스 정책 default-data-files는 IP가 파트너 노드로 마이그레이션될 수 있음을 나타내므로 인수 시 이 IP 주소는 cvo-node2의 e0a로 이전될 수 있습니다.

3. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 만듭니다.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

여기서 _private_ip_y_는 e0a의 사용되지 않는 또 다른 보조 개인 IP입니다.

4. 스토리지 VM에 하나 이상의 집계를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

이 단계는 새 스토리지 VM이 볼륨을 생성하기 전에 최소한 하나의 집계에 액세스해야 하기 때문에 필요합니다.

5. Cloud Volumes ONTAP 9.11.1 이상을 실행하는 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정하세요.

   Cloud Volumes ONTAP 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하려면 서비스를 수정해야 합니다.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

여러 **AZ**의 **HA** 쌍에 스토리지 **VM** 생성

이 단계에서는 여러 AZ의 HA 쌍에 새로운 스토리지 VM을 만듭니다.

NAS LIF에는 유동 IP 주소가 필요하지만 관리 LIF에는 선택 사항입니다. 이러한 유동 IP 주소를 사용하면 AWS에서

개인 IP를 할당할 필요가 없습니다. 대신, AWS 라우팅 테이블에서 플로팅 IP가 자동으로 구성되어 동일한 VPC에 있는 특정 노드의 ENI를 가리킵니다.

ONTAP 에서 플로팅 IP를 사용하려면 각 노드의 모든 스토리지 VM에 개인 IP 주소를 구성해야 합니다. 이는 노드 1과 노드 2에서 iSCSI LIF가 생성되는 아래 단계에 반영됩니다.

단계

1. 스토리지 VM과 스토리지 VM으로의 경로를 만듭니다.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. 노드 1에 NAS LIF를 생성합니다.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

   - HA 구성을 배포하는 AWS 지역의 모든 VPC에 대한 CIDR 블록 외부에 부동 IP 주소가 있어야 합니다. 192.168.209.27은 유동 IP 주소의 예입니다. "플로팅 IP 주소 선택에 대해 자세히 알아보세요" .
   - `-service-policy default-data-files`IP가 파트너 노드로 마이그레이션될 수 있음을 나타냅니다.

3. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 만듭니다.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. 노드 1에 iSCSI LIF를 생성합니다.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

   - 이 iSCSI LIF는 스토리지 VM의 플로팅 IP의 LIF 마이그레이션을 지원하는 데 필요합니다. iSCSI LIF일 필요는 없지만 노드 간 마이그레이션을 위해 구성할 수는 없습니다.
   - `-service-policy default-data-block`IP 주소가 노드 간에 마이그레이션되지 않음을 나타냅니다.
   - _private_ip_는 cvo_node1의 eth0(e0a)에 있는 사용되지 않는 보조 개인 IP 주소입니다.

5. 노드 2에 iSCSI LIF를 생성합니다.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

   - 이 iSCSI LIF는 스토리지 VM의 플로팅 IP의 LIF 마이그레이션을 지원하는 데 필요합니다. iSCSI LIF일 필요는 없지만 노드 간 마이그레이션을 위해 구성할 수는 없습니다.
   - `-service-policy default-data-block`IP 주소가 노드 간에 마이그레이션되지 않음을 나타냅니다.
   - _private_ip_는 cvo_node2의 eth0(e0a)에 있는 사용되지 않는 보조 개인 IP 주소입니다.

6. 스토리지 VM에 하나 이상의 집계를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

   이 단계는 새 스토리지 VM이 볼륨을 생성하기 전에 최소한 하나의 집계에 액세스해야 하기 때문에 필요합니다.

7. Cloud Volumes ONTAP 9.11.1 이상을 실행하는 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정하세요.

   Cloud Volumes ONTAP 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하려면 서비스를 수정해야 합니다.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Azure에서 Cloud Volumes ONTAP 대한 데이터 제공 스토리지 VM 관리

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에게 스토리지 및 데이터 서비스를 제공합니다. 이것을 *SVM* 또는 _vserver_라고 알고 있을 수도 있습니다. Cloud Volumes ONTAP 기본적으로 하나의 스토리지 VM으로 구성되지만 Azure에서 Cloud Volumes ONTAP 실행할 때 추가 스토리지 VM을 만들 수 있습니다.

Azure에서 추가 데이터 제공 스토리지 VM을 만들고 관리하려면 API를 사용해야 합니다. API는 스토리지 VM을 생성하고 필요한 네트워크 인터페이스를 구성하는 프로세스를 자동화하기 때문입니다. 스토리지 VM을 생성할 때 NetApp Console 필수 LIF 서비스와 스토리지 VM에서 아웃바운드 SMB/CIFS 통신에 필요한 iSCSI LIF를 구성합니다.

Cloud Volumes ONTAP API 호출 실행에 대한 정보는 다음을 참조하세요. "첫 번째 API 호출" .

지원되는 스토리지 VM 수

Cloud Volumes ONTAP 9.9.0부터 라이선스에 따라 특정 구성으로 여러 스토리지 VM이 지원됩니다. 를 참조하세요 "Cloud Volumes ONTAP 릴리스 노트" Cloud Volumes ONTAP 버전에 지원되는 스토리지 VM 수를 확인하세요.

9.9.0 이전의 모든 Cloud Volumes ONTAP 버전은 재해 복구에 사용되는 하나의 데이터 제공 스토리지 VM과 하나의 대상 스토리지 VM을 지원합니다. 소스 스토리지 VM에 장애가 발생하는 경우 데이터 액세스를 위해 대상 스토리지 VM을 활성화할 수 있습니다.

스토리지 VM 생성

구성 및 라이센스 유형에 따라 NetApp Console용 API를 사용하여 단일 노드 시스템 또는 고가용성(HA) 구성에서 여러 스토리지 VM을 생성할 수 있습니다.

이 작업에 관하여

API를 사용하여 스토리지 VM을 생성하고 필요한 네트워크 인터페이스를 구성하는 경우 콘솔도 다음을 수정합니다. `default-data-files` 다음 서비스를 NAS 데이터 LIF에서 제거하고 아웃바운드 관리 연결에 사용되는 iSCSI 데이터 LIF에 추가하여 데이터 스토리지 VM에 대한 정책을 적용합니다.

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

시작하기 전에

콘솔 에이전트에는 Cloud Volumes ONTAP 에 대한 스토리지 VM을 생성하기 위한 특정 권한이 필요합니다. 필요한 권한이 포함되어 있습니다. "NetApp 에서 제공하는 정책" .

단일 노드 시스템

단일 노드 시스템에 스토리지 VM을 생성하려면 다음 API 호출을 사용하십시오.

```
POST /azure/vsa/working-environments/{workingEnvironmentId}/svm
```

요청 본문에 다음 매개변수를 포함합니다.

```
{ "svmName": "myNewSvm1"
   "svmPassword": "optional, the API takes the cluster password if not
provided"
   "mgmtLif": "optional, to create an additional management LIF, if you
want to use the storage VM for management purposes"}
```

HA 쌍

다음 API 호출을 사용하여 HA 쌍에 스토리지 VM을 만듭니다.

```
POST /azure/ha/working-environments/{workingEnvironmentId}/svm
```

요청 본문에 다음 매개변수를 포함합니다.

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

단일 노드 시스템 및 HA 쌍에서 스토리지 VM 관리

API를 사용하면 단일 노드와 HA 구성 모두에서 스토리지 VM의 이름을 바꾸고 삭제할 수 있습니다.

시작하기 전에

콘솔 에이전트에는 Cloud Volumes ONTAP 의 스토리지 VM을 관리하기 위한 특정 권한이 필요합니다. 필요한 권한이 포함되어 있습니다. "NetApp 에서 제공하는 정책" .

스토리지 VM 이름 바꾸기

스토리지 VM의 이름을 바꾸려면 기존 스토리지 VM과 새 스토리지 VM의 이름을 매개변수로 제공해야 합니다.

단계

- 단일 노드 시스템에서 스토리지 VM의 이름을 변경하려면 다음 API 호출을 사용하십시오.

  `PUT /azure/vsa/working-environments/{workingEnvironmentId}/svm`

  요청 본문에 다음 매개변수를 포함합니다.

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- 다음 API 호출을 사용하여 HA 쌍의 스토리지 VM 이름을 바꾸세요.

  `PUT /azure/ha/working-environments/{workingEnvironmentId}/svm`

  요청 본문에 다음 매개변수를 포함합니다.

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

스토리지 VM 삭제

단일 노드 또는 HA 구성에서는 활성 볼륨이 없는 스토리지 VM을 제거할 수 있습니다.

단계

- 단일 노드 시스템에서 스토리지 VM을 삭제하려면 다음 API 호출을 사용하십시오.

```
DELETE /azure/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- HA 쌍에서 스토리지 VM을 삭제하려면 다음 API 호출을 사용하세요.

```
DELETE /azure/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

관련 정보

- "API 사용을 준비하세요"
- "Cloud Volumes ONTAP 워크플로"
- "필수 식별자 가져오기"
- "NetApp Console 에 REST API 사용"

Google Cloud에서 Cloud Volumes ONTAP 위한 데이터 제공 스토리지 VM 관리

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에게 스토리지 및 데이터 서비스를 제공합니다. 이것을 *SVM* 또는 _vserver_라고 알고 있을 수도 있습니다. Cloud Volumes ONTAP 은 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다.

Google Cloud에서 추가 데이터 제공 스토리지 VM을 만들고 관리하려면 API를 사용해야 합니다. API는 스토리지 VM을 생성하고 필요한 네트워크 인터페이스를 구성하는 프로세스를 자동화하기 때문입니다. 스토리지 VM을 생성할 때 NetApp Console 필수 LIF 서비스와 스토리지 VM에서 아웃바운드 SMB/CIFS 통신에 필요한 iSCSI LIF를 구성합니다.

Cloud Volumes ONTAP API 호출 실행에 대한 정보는 다음을 참조하세요. "첫 번째 API 호출" .

지원되는 스토리지 VM 수

Cloud Volumes ONTAP 9.11.1부터 라이선스에 따라 특정 구성으로 여러 스토리지 VM이 지원됩니다. 를 참조하세요 "Cloud Volumes ONTAP 릴리스 노트" Cloud Volumes ONTAP 버전에 지원되는 스토리지 VM 수를 확인하세요.

9.11.1 이전의 모든 Cloud Volumes ONTAP 버전은 재해 복구에 사용되는 하나의 데이터 제공 스토리지 VM과 하나의 대상 스토리지 VM을 지원합니다. 소스 스토리지 VM에 장애가 발생하는 경우 데이터 액세스를 위해 대상 스토리지 VM을 활성화할 수 있습니다.

스토리지 VM 생성

구성 및 라이센스 유형에 따라 API를 사용하여 단일 노드 시스템 또는 고가용성(HA) 구성에서 여러 스토리지 VM을 생성할 수 있습니다.

이 작업에 관하여

API를 사용하여 스토리지 VM을 생성하고 필요한 네트워크 인터페이스를 구성하는 경우 콘솔도 다음을 수정합니다.

`default-data-files` 다음 서비스를 NAS 데이터 LIF에서 제거하고 아웃바운드 관리 연결에 사용되는 iSCSI 데이터 LIF에 추가하여 데이터 스토리지 VM에 대한 정책을 적용합니다.

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

시작하기 전에

콘솔 에이전트에는 Cloud Volumes ONTAP HA 쌍에 대한 스토리지 VM을 생성하기 위한 특정 권한이 필요합니다. 필요한 권한이 포함되어 있습니다. "NetApp 에서 제공하는 정책" .

단일 노드 시스템

단일 노드 시스템에 스토리지 VM을 생성하려면 다음 API 호출을 사용하십시오.

```
POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

요청 본문에 다음 매개변수를 포함합니다.

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

HA 쌍

다음 API 호출을 사용하여 HA 쌍에 스토리지 VM을 만듭니다.

```
POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/
```

요청 본문에 다음 매개변수를 포함합니다.

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
}
```

스토리지 **VM** 관리

API를 사용하면 단일 노드와 HA 구성 모두에서 스토리지 VM의 이름을 바꾸고 삭제할 수 있습니다.

시작하기 전에

콘솔 에이전트에는 Cloud Volumes ONTAP HA 쌍의 스토리지 VM을 관리하기 위한 특정 권한이 필요합니다. 필요한 권한이 포함되어 있습니다. "NetApp 에서 제공하는 정책" .

스토리지 VM 이름 바꾸기

스토리지 VM의 이름을 바꾸려면 기존 스토리지 VM과 새 스토리지 VM의 이름을 매개변수로 제공해야 합니다.

단계

- 단일 노드 시스템에서 스토리지 VM의 이름을 변경하려면 다음 API 호출을 사용하십시오.

  ```
  PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm
  ```

  요청 본문에 다음 매개변수를 포함합니다.

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- 다음 API 호출을 사용하여 HA 쌍의 스토리지 VM 이름을 바꾸세요.

  ```
  PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm
  ```

  요청 본문에 다음 매개변수를 포함합니다.

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

스토리지 VM 삭제

단일 노드 또는 HA 구성에서는 활성 볼륨이 없는 스토리지 VM을 제거할 수 있습니다.

단계

- 단일 노드 시스템에서 스토리지 VM을 삭제하려면 다음 API 호출을 사용하십시오.

  ```
  DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

- HA 쌍에서 스토리지 VM을 삭제하려면 다음 API 호출을 사용하세요.

  ```
  DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

관련 정보

- "API 사용을 준비하세요"
- "Cloud Volumes ONTAP 워크플로"

- "필수 식별자 가져오기"
- "NetApp Console 에 REST API 사용"

Cloud Volumes ONTAP 에 대한 스토리지 VM 재해 복구 설정

NetApp Console 스토리지 VM(SVM) 재해 복구에 대한 설정이나 오케스트레이션 지원을 제공하지 않습니다. 이러한 작업을 수행하려면 ONTAP 시스템 관리자나 ONTAP CLI를 사용하세요.

두 Cloud Volumes ONTAP 시스템 간에 SnapMirror SVM 복제를 설정하는 경우, 복제는 두 개의 HA 쌍 시스템 또는 두 개의 단일 노드 시스템 간에만 가능합니다. HA 쌍 시스템과 단일 노드 시스템 간에는 SnapMirror SVM 복제를 설정할 수 없습니다.

ONTAP CLI 지침은 다음 문서를 참조하세요.

- "SVM 재해 복구 준비 익스프레스 가이드"
- "SVM 재해 복구 익스프레스 가이드"

보안 및 데이터 암호화

NetApp 암호화 솔루션을 사용하여 Cloud Volumes ONTAP 에서 볼륨 암호화

Cloud Volumes ONTAP NetApp Volume Encryption(NVE)과 NetApp Aggregate Encryption(NAE)을 지원합니다. NVE와 NAE는 볼륨의 FIPS 140-2 호환 저장 데이터 암호화를 지원하는 소프트웨어 기반 솔루션입니다. "이러한 암호화 솔루션에 대해 자세히 알아보세요" .

NVE와 NAE는 모두 외부 키 관리자를 통해 지원됩니다.

] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[] ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[

AWS Key Management Service를 사용하여 Cloud Volumes ONTAP 암호화 키 관리

사용할 수 있습니다"AWS의 키 관리 서비스(KMS)" AWS에 배포된 애플리케이션에서 ONTAP 암호화 키를 보호합니다.

AWS KMS를 통한 키 관리 기능은 CLI 또는 ONTAP REST API를 통해 활성화할 수 있습니다.

KMS를 사용할 때 기본적으로 데이터 SVM의 LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용된다는 점에 유의하세요. 노드 관리 네트워크는 AWS 인증 서비스와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않으면 클러스터가 키 관리 서비스를 제대로 활용하지 못합니다.

시작하기 전에

- Cloud Volumes ONTAP 버전 9.12.0 이상을 실행해야 합니다.
- 볼륨 암호화(VE) 라이선스를 설치해야 합니다.
- MTEKM(Multi-tenant Encryption Key Management) 라이선스가 설치되어 있어야 합니다.

- 클러스터 또는 SVM 관리자여야 합니다.
- 활성 AWS 구독이 있어야 합니다.

데이터 SVM에 대해서만 키를 구성할 수 있습니다.

구성

AWS

1. 당신은 만들어야합니다"승인하다" 암호화를 관리하는 IAM 역할에서 사용될 AWS KMS 키에 대한 것입니다. IAM 역할에는 다음 작업을 허용하는 정책이 포함되어야 합니다.
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`보조금을 생성하려면 다음을 참조하세요."AWS 문서" .
2. "적절한 IAM 역할에 정책을 추가합니다."정책은 다음을 지원해야 합니다. `DescribeKey` , `Encrypt` , 그리고 `Decrypt` 운영.

Cloud Volumes ONTAP

1. Cloud Volumes ONTAP 환경으로 전환하세요.
2. 고급 권한 수준으로 전환:
   `set -privilege advanced`
3. AWS 키 관리자를 활성화합니다.
   `security key-manager external aws enable -vserver` *`data_svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. 메시지가 표시되면 비밀 키를 입력하세요.
5. AWS KMS가 올바르게 구성되었는지 확인하세요.
   `security key-manager external aws show -vserver` *`svm_name`*

Azure Key Vault를 사용하여 Cloud Volumes ONTAP 암호화 키 관리

Azure Key Vault(AKV)를 사용하면 Azure에 배포된 애플리케이션에서 ONTAP 암호화 키를 보호할 수 있습니다. 를 참조하세요"Microsoft 설명서" .

AKV는 데이터 SVM에 대해서만 NetApp 볼륨 암호화(NVE) 키를 보호하는 데 사용할 수 있습니다. 자세한 내용은 다음을 참조하세요. "ONTAP 문서" .

AKV를 사용한 키 관리 기능은 CLI 또는 ONTAP REST API를 통해 활성화할 수 있습니다.

AKV를 사용할 때 기본적으로 데이터 SVM LIF를 사용하여 클라우드 키 관리 엔드포인트와 통신한다는 점에 유의하세요. 노드 관리 네트워크는 클라우드 공급자의 인증 서비스(login.microsoftonline.com)와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않으면 클러스터가 키 관리 서비스를 제대로 활용하지 못합니다.

시작하기 전에

- Cloud Volumes ONTAP 버전 9.10.1 이상을 실행해야 합니다.
- 볼륨 암호화(VE) 라이선스가 설치됨(NetApp 볼륨 암호화 라이선스는 NetApp 지원에 등록된 각 Cloud Volumes ONTAP 시스템에 자동으로 설치됨)

- 다중 테넌트 암호화 키 관리(MT_EK_MGMT) 라이선스가 있어야 합니다.
- 클러스터 또는 SVM 관리자여야 합니다.
- 활성 Azure 구독

제한 사항

- AKV는 데이터 SVM에서만 구성될 수 있습니다.
- NAE는 AKV와 함께 사용할 수 없습니다. NAE에는 외부 지원 KMIP 서버가 필요합니다.
- Cloud Volumes ONTAP 노드는 15분마다 AKV를 폴링하여 접근성과 키 가용성을 확인합니다. 이 폴링 기간은 구성할 수 없으며, 폴링 시도에서 4번 연속 실패하면(총 1시간) 볼륨이 오프라인으로 전환됩니다.

구성 프로세스

설명된 단계에서는 Cloud Volumes ONTAP 구성을 Azure에 등록하는 방법과 Azure Key Vault 및 키를 만드는 방법을 설명합니다. 이미 이러한 단계를 완료한 경우 특히 올바른 구성 설정이 있는지 확인하십시오.Azure Key Vault 만들기 , 그리고 다음으로 진행합니다Cloud Volumes ONTAP 구성 .

- Azure 애플리케이션 등록
- Azure 클라이언트 비밀 만들기
- Azure Key Vault 만들기
- 암호화 키 생성
- Azure Active Directory 엔드포인트 만들기(HA 전용)
- Cloud Volumes ONTAP 구성

Azure 애플리케이션 등록

1. 먼저 Cloud Volumes ONTAP Azure Key Vault에 액세스하는 데 사용할 Azure 구독에 애플리케이션을 등록해야 합니다. Azure Portal에서 앱 등록을 선택합니다.
2. 신규 등록을 선택하세요.
3. 애플리케이션 이름을 입력하고 지원되는 애플리케이션 유형을 선택하세요. Azure Key Vault를 사용하려면 기본 단일 테넌트로 충분합니다. 등록을 선택하세요.
4. Azure 개요 창에서 등록한 애플리케이션을 선택합니다. 애플리케이션**(**클라이언트**) ID**와 디렉토리**(**테넌트**) ID**를 안전한 위치에 복사합니다. 이는 나중에 등록 과정에서 필요합니다.

Azure 클라이언트 비밀 만들기

1. Azure Key Vault 앱 등록을 위한 Azure Portal에서 인증서 및 비밀 창을 선택합니다.
2. 새로운 클라이언트 비밀번호를 선택하세요. 클라이언트 비밀번호에 의미 있는 이름을 입력하세요. NetApp 24개월 만료 기간을 권장하지만, 특정 클라우드 거버넌스 정책에는 다른 설정이 필요할 수 있습니다.
3. 추가를 클릭하여 클라이언트 비밀번호를 생성합니다. 값 열에 나열된 비밀 문자열을 복사하여 나중에 사용할 수 있도록 안전한 위치에 저장하세요.Cloud Volumes ONTAP 구성 . 해당 페이지에서 벗어나면 비밀번호 값은 다시 표시되지 않습니다.

Azure Key Vault 만들기

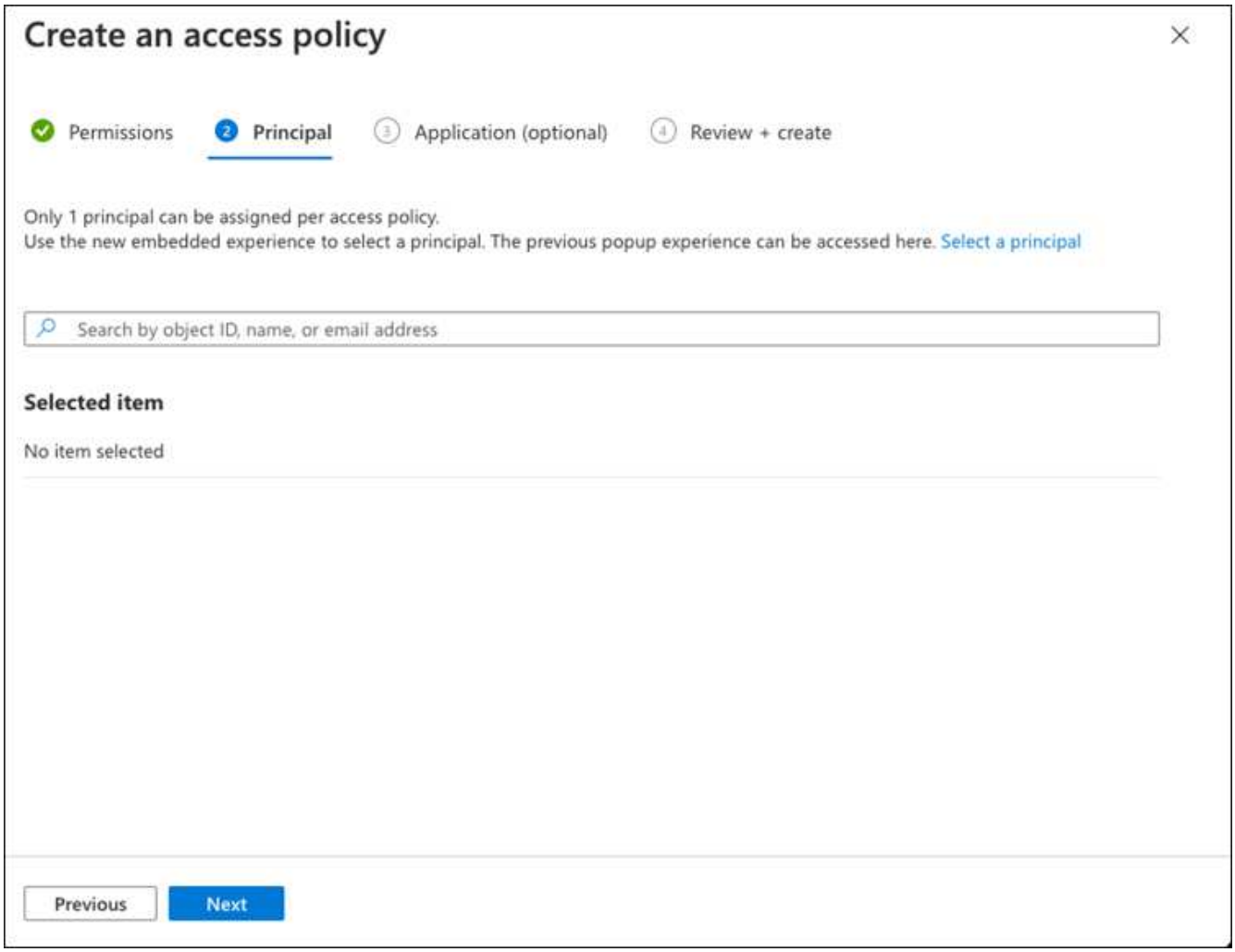
1. 기존 Azure Key Vault가 있는 경우 Cloud Volumes ONTAP 구성에 연결할 수 있습니다. 하지만 이 프로세스에서는 설정에 맞게 액세스 정책을 조정해야 합니다.

2. Azure Portal에서 키 자격 증명 모음 섹션으로 이동합니다.
3. **+**만들기를 클릭하고 리소스 그룹, 지역, 가격 책정 계층을 포함한 필수 정보를 입력합니다. 또한 삭제된 볼트를 보관할 일수를 입력하고 키 볼트에서 퍼지 보호 사용을 선택합니다.
4. 다음을 선택하여 액세스 정책을 선택하세요.
5. 다음 옵션을 선택하세요:
   a. 액세스 구성에서 **Vault** 액세스 정책을 선택합니다.
   b. 리소스 액세스에서 볼륨 암호화를 위해 **Azure Disk Encryption**을 선택합니다.
6. **+**만들기를 선택하여 액세스 정책을 추가합니다.
7. 템플릿에서 구성에서 드롭다운 메뉴를 클릭한 다음 키**,** 비밀번호 및 인증서 관리 템플릿을 선택합니다.
8. 각 드롭다운 권한 메뉴(키, 비밀, 인증서)를 선택한 다음 메뉴 목록 상단에서 모두 선택을 클릭하여 사용 가능한 모든 권한을 선택합니다. 다음이 있어야 합니다.
   - 주요 권한: 20개 선택됨
   - 비밀 권한: 8개 선택됨
   - 인증서 권한: 16개 선택됨


Create an access policy
1 Permissions
2 Principal
3 Application (optional)
4 Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
Purge
Previous
Next

9. 다음을 클릭하여 주 Azure 등록 애플리케이션을 선택하십시오.Azure 애플리케이션 등록 . 다음을 선택하세요.

   정책당 한 명의 주체만 할당할 수 있습니다.



10. 다음을 두 번 클릭하여 검토 및 생성에 도달합니다. 그런 다음 만들기를 클릭합니다.
11. 다음을 선택하여 네트워킹 옵션으로 넘어갑니다.
12. 적절한 네트워크 액세스 방법을 선택하거나 모든 네트워크와 검토 + 생성을 선택하여 키 보관소를 만듭니다. (네트워크 액세스 방법은 거버넌스 정책이나 회사 클라우드 보안 팀에서 규정할 수 있습니다.)
13. 키 보관소 URI를 기록합니다. 생성한 키 보관소에서 개요 메뉴로 이동하여 오른쪽 열에서 보관소 **URI**를 복사합니다. 이것은 나중의 단계에서 필요합니다.

암호화 키 생성

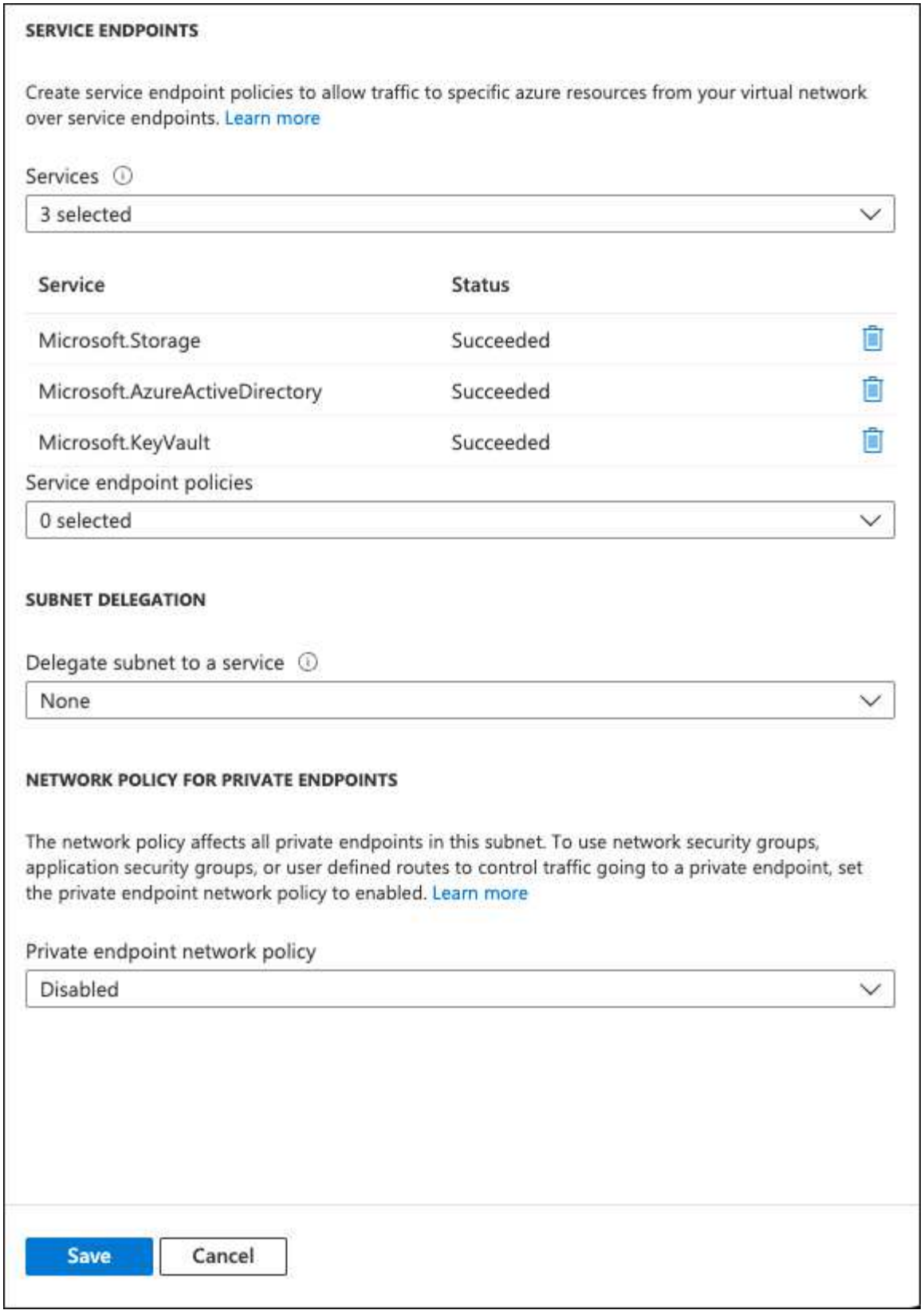
1. Cloud Volumes ONTAP 에 대해 생성한 Key Vault 메뉴에서 키 옵션으로 이동합니다.
2. 생성/가져오기를 선택하여 새 키를 만듭니다.
3. 기본 옵션을 생성으로 설정된 상태로 둡니다.
4. 다음 정보를 제공하세요.
   - 암호화 키 이름

- 키 유형: RSA
- RSA 키 크기: 2048
- 활성화됨: 예

5. 암호화 키를 생성하려면 생성을 선택하세요.
6. 키 메뉴로 돌아가서 방금 만든 키를 선택하세요.
7. 현재 버전에서 키 ID를 선택하여 키 속성을 확인하세요.
8. 키 식별자 필드를 찾으세요. 16진수 문자열을 제외하고 URI를 해당 문자열까지 복사합니다.

Azure Active Directory 엔드포인트 만들기**(HA** 전용**)**

1. 이 프로세스는 HA Cloud Volumes ONTAP 시스템에 대해 Azure Key Vault를 구성하는 경우에만 필요합니다.
2. Azure Portal에서 가상 네트워크로 이동합니다.
3. Cloud Volumes ONTAP 시스템을 배포한 가상 네트워크를 선택하고 페이지 왼쪽에 있는 서브넷 메뉴를 선택합니다.
4. 목록에서 Cloud Volumes ONTAP 배포에 대한 서브넷 이름을 선택합니다.
5. 서비스 엔드포인트 제목으로 이동합니다. 드롭다운 메뉴에서 다음을 선택하세요.
   - **Microsoft.AzureActiveDirectory**
   - 마이크로소프트 키볼트
   - **Microsoft.Storage** (선택 사항)



6. 저장을 선택하여 설정을 적용합니다.

Cloud Volumes ONTAP 구성

1. 원하는 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.
2. ONTAP 에서 고급 권한 모드로 들어가세요:

```
set advanced -con off
```

3. 원하는 데이터 SVM을 식별하고 DNS 구성을 확인합니다.
`vserver services name-service dns show`

   a. 원하는 데이터 SVM에 대한 DNS 항목이 있고 Azure DNS에 대한 항목이 포함되어 있는 경우 아무 작업도 필요하지 않습니다. 그렇지 않은 경우 Azure DNS, 개인 DNS 또는 온-프레미스 서버를 가리키는 데이터 SVM에 대한 DNS 서버 항목을 추가합니다. 이는 클러스터 관리 SVM 항목과 일치해야 합니다.
   `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. 데이터 SVM에 대한 DNS 서비스가 생성되었는지 확인하세요.
   `vserver services name-service dns show`

4. 애플리케이션 등록 후 저장된 클라이언트 ID와 테넌트 ID를 사용하여 Azure Key Vault를 활성화합니다.
`security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI`

   > 그만큼 `_full_key_URI` 가치는 활용되어야 합니다 `<https:// <key vault host name>/keys/<key label>` 체재.

5. Azure Key Vault를 성공적으로 활성화한 후 다음을 입력하십시오. `client secret value` 메시지가 표시되면.

6. 키 관리자의 상태를 확인하세요.
`security key-manager external azure check` 출력은 다음과 같습니다.

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_server
    Status: OK

Category: kms_wrapped_key_status
    Status: UNKNOWN
    Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

만약 `service_reachability` 상태가 아닙니다 `OK` SVM은 필요한 모든 연결 및 권한을 통해 Azure Key Vault 서비스에 연결할 수 없습니다. Azure 네트워크 정책과 라우팅이 개인 vNet이 Azure Key Vault 공용 엔드포인트에 도달하는 것을 차단하지 않는지 확인하세요. 그렇다면 vNet 내에서 Key Vault에 액세스하기 위해 Azure Private 엔드포인트를 사용하는 것을 고려하세요. 엔드포인트의 개인 IP 주소를 확인하려면 SVM에 정적 호스트 항목을 추가해야 할 수도 있습니다.

그만큼 `kms_wrapped_key_status` 보고할 것이다 `UNKNOWN` 초기 구성에서. 상태가 다음으로 변경됩니다. `OK` 첫 번째 볼륨이 암호화된 후.

7. 선택 사항: NVE의 기능을 확인하기 위해 테스트 볼륨을 만듭니다.

   ```
   vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
   -state online -policy default
   ```

   올바르게 구성된 경우 Cloud Volumes ONTAP 자동으로 볼륨을 생성하고 볼륨 암호화를 활성화합니다.

8. 볼륨이 올바르게 생성되고 암호화되었는지 확인하세요. 그렇다면, `-is-encrypted` 매개변수는 다음과 같이 표시됩니다. `true` .
   ```
   vol show -vserver SVM_name -fields is-encrypted
   ```
9. 선택 사항: Azure Key Vault 인증 인증서의 자격 증명을 업데이트하려면 다음 명령을 사용하세요.
   ```
   security key-manager external azure update-credentials -vserver v1
   -authentication-method certificate
   ```

관련 링크

- "Azure에서 고객 관리 키를 사용하도록 Cloud Volumes ONTAP 설정"
- "Microsoft Azure 설명서: Azure Key Vault 정보"
- "ONTAP 명령 참조 가이드"

Google Cloud KMS를 사용하여 Cloud Volumes ONTAP 암호화 키 관리

사용할 수 있습니다"Google Cloud Platform의 키 관리 서비스(Cloud KMS)" Google Cloud Platform에 배포된 애플리케이션에서 Cloud Volumes ONTAP 암호화 키를 보호합니다.

Cloud KMS를 사용한 키 관리 기능은 ONTAP CLI 또는 ONTAP REST API를 통해 활성화할 수 있습니다.

Cloud KMS를 사용할 때 기본적으로 데이터 SVM의 LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용된다는 점에 유의하세요. 노드 관리 네트워크는 클라우드 제공자의 인증 서비스(oauth2.googleapis.com)와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않으면 클러스터가 키 관리 서비스를 제대로 활용하지 못합니다.

시작하기 전에

- 시스템에서는 Cloud Volumes ONTAP 9.10.1 이상을 실행해야 합니다.
- 데이터 SVM을 사용해야 합니다. Cloud KMS는 데이터 SVM에서만 구성할 수 있습니다.
- 클러스터 또는 SVM 관리자여야 합니다.
- SVM에 볼륨 암호화(VE) 라이선스를 설치해야 합니다.
- Cloud Volumes ONTAP 9.12.1 GA부터 다중 테넌트 암호화 키 관리(MTEKM) 라이선스도 설치해야 합니다.
- 활성화된 Google Cloud Platform 구독이 필요합니다.

구성

구글 클라우드

1. Google Cloud 환경에서"대칭 GCP 키 링과 키를 생성합니다." .
2. Cloud KMS 키와 Cloud Volumes ONTAP 서비스 계정에 사용자 지정 역할을 할당합니다.

a. 사용자 정의 역할을 만듭니다.

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

b. 생성한 사용자 지정 역할을 할당합니다.
`gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name --location key_location --member serviceAccount:_service_account_Name_ --role projects/customer_project_id/roles/kmsCustomRole`

> Cloud Volumes ONTAP 9.13.0 이상을 사용하는 경우 사용자 지정 역할을 만들 필요가 없습니다. 미리 정의된 것을 할당할 수 있습니다 [`cloudkms.cryptoKeyEncrypterDecrypter` ^] 역할.

3. 서비스 계정 JSON 키 다운로드:
`gcloud iam service-accounts keys create key-file --iam-account=sa-name @project-id.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. 원하는 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.
2. 고급 권한 수준으로 전환:
`set -privilege advanced`
3. 데이터 SVM에 대한 DNS를 생성합니다.
`dns create -domains c.<project>.internal -name-servers server_address -vserver SVM_name`
4. CMEK 항목 생성:
`security key-manager external gcp enable -vserver SVM_name -project-id project -key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
5. 메시지가 표시되면 GCP 계정의 서비스 계정 JSON 키를 입력합니다.
6. 활성화된 프로세스가 성공했는지 확인하세요.
`security key-manager external gcp check -vserver svm_name`
7. 선택 사항: 암호화를 테스트하기 위한 볼륨 생성 `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

문제 해결

문제 해결이 필요한 경우 위의 마지막 두 단계에서 원시 REST API 로그를 추적할 수 있습니다.

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Cloud Volumes ONTAP 에 NetApp 랜섬웨어 보호 솔루션 활성화

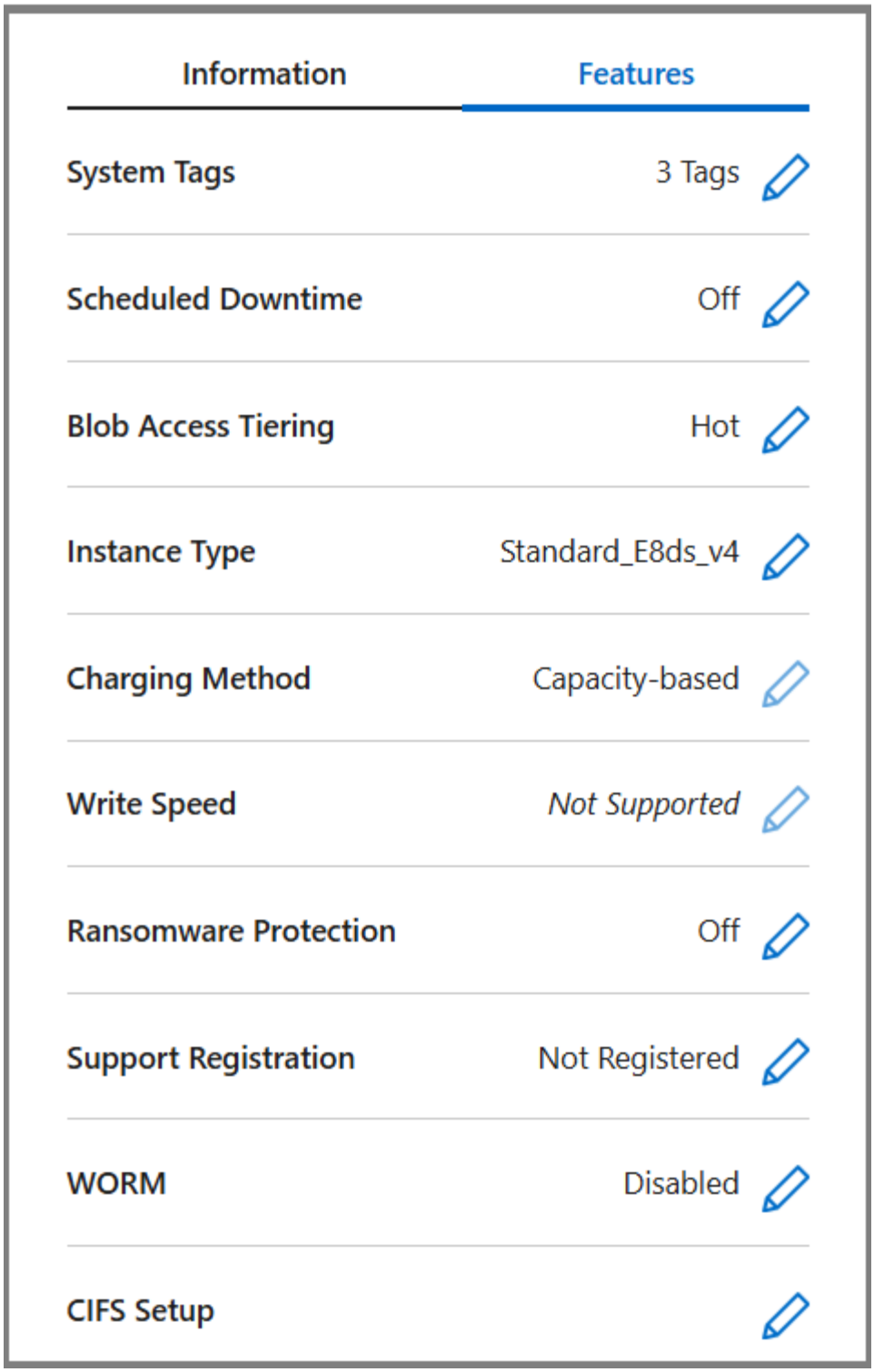
랜섬웨어 공격은 기업의 시간, 자원, 평판을 앗아갈 수 있습니다. NetApp Console 사용하면 랜섬웨어에 대한 두 가지 NetApp 솔루션, 즉 일반적인 랜섬웨어 파일 확장자로부터의 보호 및 자율 랜섬웨어 보호(ARP)를 구현할 수 있습니다. 이러한 솔루션은 가시성, 탐지 및 복구를 위한 효과적인 도구를 제공합니다.

일반적인 랜섬웨어 파일 확장자로부터 보호

콘솔에서 사용할 수 있는 랜섬웨어 보호 설정을 사용하면 ONTAP FPolicy 기능을 활용하여 일반적인 랜섬웨어 파일 확장자 유형으로부터 보호할 수 있습니다.

단계

1. 시스템 페이지에서 랜섬웨어 보호를 사용하도록 구성한 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 랜섬웨어 보호 옆에 있는 연필 아이콘을 클릭합니다.



3. 랜섬웨어에 대한 NetApp 솔루션 구현:

   a. 스냅샷 정책이 활성화되지 않은 볼륨이 있는 경우 *스냅샷 정책 활성화*를 클릭합니다.

      NetApp Snapshot 기술은 랜섬웨어 치료를 위한 업계 최고의 솔루션을 제공합니다. 성공적인 복구의 핵심은 감염되지 않은 백업에서 복원하는 것입니다. 스냅샷 사본은 읽기 전용이므로 랜섬웨어로 인한 손상을 방지할 수 있습니다. 또한 단일 파일 사본이나 완벽한 재해 복구 솔루션의 이미지를 만드는 세분성을 제공할 수도 있습니다.

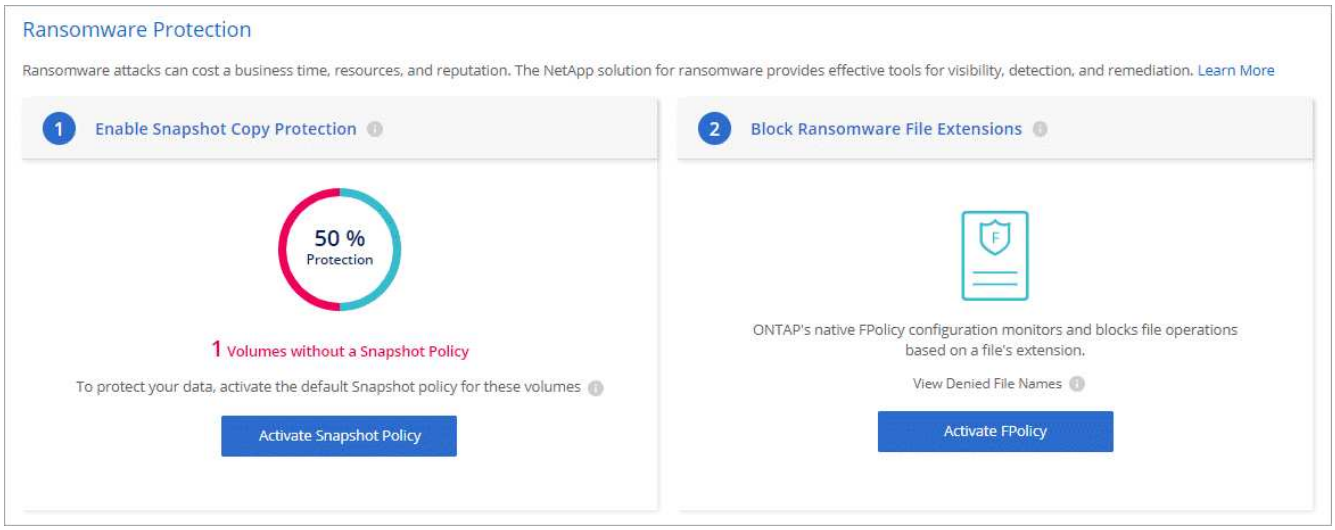
b. ONTAP의 FPolicy 솔루션을 활성화하려면 *FPolicy 활성화*를 클릭하세요. 이 솔루션은 파일 확장자를 기준으로 파일 작업을 차단할 수 있습니다.

   이 예방 솔루션은 일반적인 랜섬웨어 파일 유형을 차단하여 랜섬웨어 공격으로부터의 보호 기능을 강화합니다.

   기본 FPolicy 범위는 다음 확장자를 가진 파일을 차단합니다.

   마이크로, 암호화된, 잠긴, 크립토, 크립토, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, 좋은, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre

   이 범위는 Cloud Volumes ONTAP 에서 FPolicy를 활성화할 때 생성됩니다. 이 목록은 일반적인 랜섬웨어 파일 유형을 기반으로 작성되었습니다. Cloud Volumes ONTAP CLI의 *vserver fpolicy policy scope* 명령을 사용하여 차단된 파일 확장자를 사용자 정의할 수 있습니다.



자율형 랜섬웨어 보호

Cloud Volumes ONTAP 랜섬웨어 공격을 나타낼 수 있는 비정상적인 활동을 사전에 감지하고 경고하기 위해 워크로드에 대한 분석을 수행하는 ARP(Autonomous Ransomware Protection) 기능을 지원합니다.

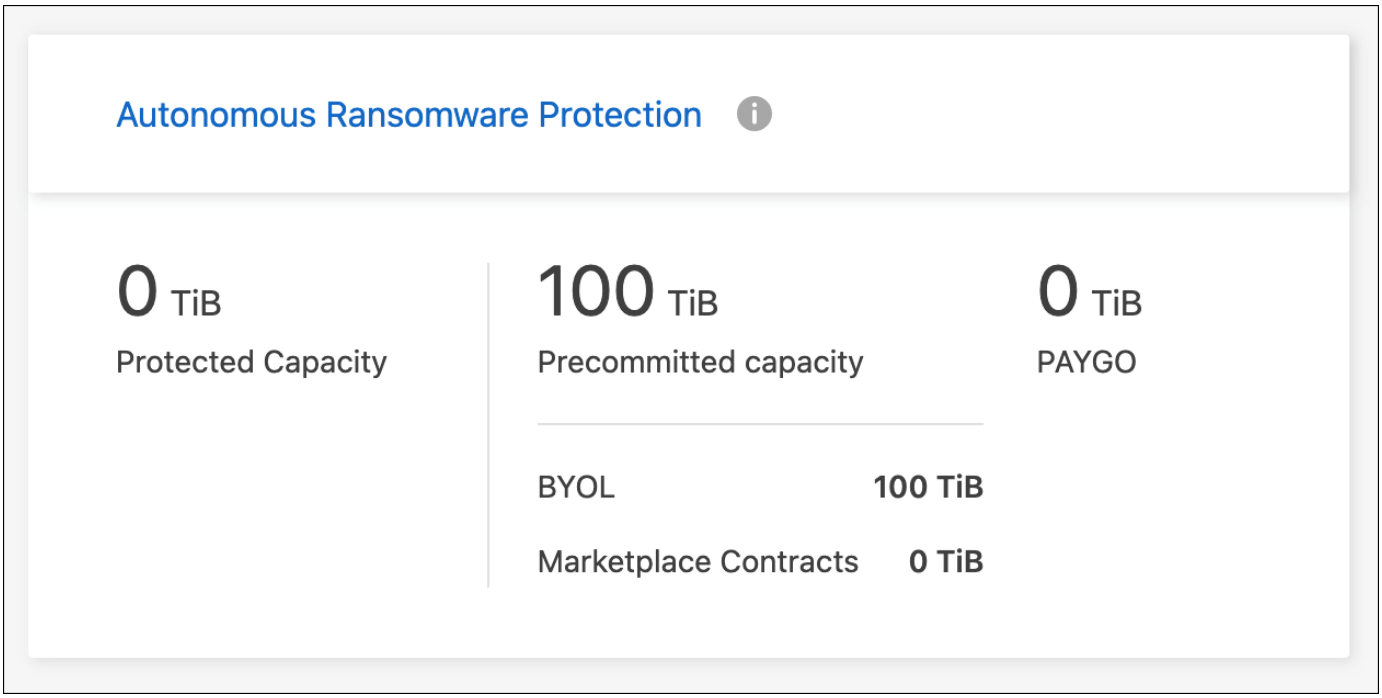
다음을 통해 제공되는 파일 확장자 보호와 별도로 "랜섬웨어 보호 설정" ARP 기능은 작업 부하 분석을 사용하여 감지된 "비정상적인 활동"을 기반으로 잠재적인 공격에 대해 사용자에게 경고합니다. 랜섬웨어 보호 설정과 ARP 기능은 모두 종합적인 랜섬웨어 보호를 위해 함께 사용할 수 있습니다.

ARP 기능은 추가 비용 없이 BYOL(Bring Your Own License) 및 마켓플레이스 구독을 통해 라이선스를 사용할 수 있습니다.

ARP 지원 볼륨에는 "학습 모드" 또는 "활성" 상태가 지정됩니다.

볼륨에 대한 ARP 구성은 ONTAP 시스템 관리자와 ONTAP CLI를 통해 수행됩니다.

ONTAP System Manager 및 ONTAP CLI를 사용하여 ARP를 활성화하는 방법에 대한 자세한 내용은 다음을 참조하십시오. "ONTAP 설명서: 자율 랜섬웨어 보호 활성화" .



Cloud Volumes ONTAP 에서 WORM 파일의 변조 방지 스냅샷 복사본을 만듭니다.

Cloud Volumes ONTAP 시스템에서 한 번 쓰고 여러 번 읽을 수 있는(WORM) 파일의 변조 방지 스냅샷 사본을 만들고 특정 보존 기간 동안 수정되지 않은 형태로 스냅샷을 보관할 수 있습니다. 이 기능은 SnapLock 기술을 기반으로 하며, 데이터 보호 및 규정 준수를 한층 더 강화합니다.

시작하기 전에

스냅샷 복사본을 만드는 데 사용하는 볼륨이 SnapLock 볼륨인지 확인하세요. 볼륨에서 SnapLock 보호를 활성화하는 방법에 대한 자세한 내용은 다음을 참조하십시오. "ONTAP 설명서: SnapLock 구성" .

단계

1. SnapLock 볼륨에서 스냅샷 복사본을 만듭니다. CLI 또는 시스템 관리자를 사용하여 스냅샷 복사본을 만드는 방법에 대한 자세한 내용은 다음을 참조하십시오. "ONTAP 설명서: 로컬 스냅샷 복사본 관리 개요" .

   스냅샷 복사본은 볼륨의 WORM 속성을 상속하므로 변조가 불가능합니다. 기본 SnapLock 기술은 지정된 보존 기간이 경과할 때까지 스냅샷이 편집 및 삭제되지 않도록 보호합니다.

2. 스냅샷을 편집해야 하는 경우 보존 기간을 수정할 수 있습니다. 자세한 내용은 다음을 참조하세요. "ONTAP 문서: 보존 시간 설정" .

> ⓘ 스냅샷 사본은 특정 보존 기간 동안 보호되지만, Cloud Volumes ONTAP 의 WORM 스토리지는 "신뢰할 수 있는 스토리지 관리자" 모델에서 작동하므로 클러스터 관리자가 소스 볼륨을 삭제할 수 있습니다. 또한 신뢰할 수 있는 클라우드 관리자는 클라우드 스토리지 리소스를 조작하여 WORM 데이터를 삭제할 수 있습니다.

관련 링크

- WORM에 대한 자세한 내용은 다음을 참조하세요."Cloud Volumes ONTAP 의 WORM 스토리지에 대해 알아보세요" .

- SnapLock 볼륨 충전에 대한 정보는 다음을 참조하세요."Cloud Volumes ONTAP 의 라이선싱 및 요금 청구" .

시스템 관리

Cloud Volumes ONTAP 업그레이드

NetApp Console 에서 Cloud Volumes ONTAP 업그레이드하여 최신 새 기능과 향상된 기능을 활용하세요. 소프트웨어를 업그레이드하기 전에 Cloud Volumes ONTAP 시스템을 준비해야 합니다.

업그레이드 개요

Cloud Volumes ONTAP 업그레이드 프로세스를 시작하기 전에 다음 사항을 알고 있어야 합니다.

콘솔에서만 업그레이드

ONTAP System Manager나 ONTAP CLI를 사용해서는 안 되며, 오직 콘솔을 사용해서만 Cloud Volumes ONTAP 업그레이드해야 합니다. 그렇지 않으면 시스템 안정성에 영향을 미칠 수 있습니다.

콘솔은 Cloud Volumes ONTAP 을 업그레이드하는 두 가지 방법을 제공합니다.

- 시스템에 표시되는 업그레이드 알림을 따르십시오
- HTTPS 위치에 업그레이드 이미지를 배치한 다음 콘솔에 URL을 제공합니다.

지원되는 업그레이드 경로

업그레이드할 수 있는 Cloud Volumes ONTAP 버전은 현재 실행 중인 버전에 따라 다릅니다. 다음 표의 각 릴리스에 있는 일반 버전 또는 패치 버전은 업그레이드 가능한 기본 버전을 나타냅니다. 사용 가능한 패치에 대한 자세한 내용은 각 릴리스의 "버전별 릴리스 노트"를 참조하십시오.

AWS에서 지원되는 업그레이드 경로

현재 버전	직접 업그레이드할 수 있는 버전
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1

현재 버전	직접 업그레이드할 수 있는 버전
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

Azure에 지원되는 업그레이드 경로

현재 버전	직접 업그레이드할 수 있는 버전
9.17.1 P1	9.18.1
9.16.1 P3	9.17.1 P1
9.15.1 P10	9.16.1 P3
9.14.1 P13	9.15.1 P10
9.13.1 P16	9.14.1 P13
9.12.1 P18	9.13.1 P16
9.11.1 P20	9.12.1 P18

Azure에 이전 버전의 Cloud Volumes ONTAP 있는 경우 먼저 다음 버전으로 업그레이드한 후 지원되는 업그레이드

경로를 따라 대상 버전에 도달해야 합니다. 예를 들어 Cloud Volumes ONTAP 9.7 P7이 있는 경우 다음 업그레이드 경로를 따르세요.

- 9.7 P7 → 9.8 P18
- 9.8 P18 → 9.9.1 P15
- 9.9.1 P15 → 9.10.1 P12
- 9.10.1 P12 → 9.11.1 P20

Google Cloud에 대해 지원되는 업그레이드 경로

현재 버전	직접 업그레이드할 수 있는 버전
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6

현재 버전	직접 업그레이드할 수 있는 버전
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

다음 사항에 유의하세요.

- Cloud Volumes ONTAP 에 지원되는 업그레이드 경로는 온프레미스 ONTAP 클러스터와 다릅니다.
- 시스템에 나타나는 알림에 따라 업그레이드하는 경우, 콘솔에서 지원되는 업그레이드 경로를 따르는 릴리스로 업그레이드하라는 메시지가 표시됩니다.
- HTTPS 위치에 업그레이드 이미지를 배치하여 업그레이드하는 경우, 지원되는 다음 업그레이드 경로를 따라야 합니다.
- 어떤 경우에는 대상 릴리스에 도달하기 위해 여러 번 업그레이드해야 할 수도 있습니다.

  예를 들어, 버전 9.8을 사용 중이고 9.10.1로 업그레이드하려는 경우 먼저 버전 9.9.1로 업그레이드한 다음 9.10.1로 업그레이드해야 합니다.

패치 릴리스

2024년 1월부터 Cloud Volumes ONTAP 의 최신 버전 3개에 대한 패치 릴리스가 있는 경우에만 패치 업그레이드가 가능합니다. RC 또는 GA 버전을 배포할 수 없을 때 패치 버전을 배포할 수 있는 경우가 있습니다.

콘솔에 표시할 최신 버전 3개를 결정하기 위해 최신 GA 릴리스를 사용합니다. 예를 들어, 현재 GA 릴리스가 9.13.1이면 9.11.1-9.13.1에 대한 패치가 콘솔에 나타납니다.

패치 버전 9.11.1 이하의 경우 수동 업그레이드 절차를 사용해야 합니다.ONTAP 이미지 다운로드 .

패치 릴리스에 대한 일반적인 규칙에 따라 동일하거나 다음 Cloud Volumes ONTAP 릴리스에서 낮은 패치 버전에서 더 높은 패치 버전으로 업그레이드할 수 있습니다.

다음은 몇 가지 예입니다.

- 9.13.0 → 9.13.1 P15
- 9.12.1 → 9.13.1 P2

되돌리기 또는 다운그레이드

Cloud Volumes ONTAP 이전 릴리스로 되돌리거나 다운그레이드하는 것은 지원되지 않습니다.

지원 등록

이 페이지에 설명된 방법을 사용하여 소프트웨어를 업그레이드하려면 Cloud Volumes ONTAP NetApp 지원팀에 등록해야 합니다. 이는 종량제(PAYGO)와 자체 라이선스 사용(BYOL) 모두에 적용됩니다. 당신은 필요합니다"PAYGO 시스템 수동 등록" BYOL 시스템은 기본적으로 등록됩니다.

지원에 등록되지 않은 시스템도 새 버전이 출시되면 콘솔에 표시되는 소프트웨어 업데이트 알림을 받게 됩니다. 하지만 소프트웨어를 업그레이드하려면 먼저 시스템을 등록해야 합니다.

HA 중재자의 업그레이드

콘솔은 Cloud Volumes ONTAP 업그레이드 프로세스 중에 필요에 따라 중재자 인스턴스도 업데이트합니다.

c4, m4 및 r4 EC2 인스턴스 유형을 사용한 AWS 업그레이드

Cloud Volumes ONTAP 더 이상 c4, m4, r4 EC2 인스턴스 유형을 지원하지 않습니다. 다음 인스턴스 유형을 사용하면 기존 배포를 Cloud Volumes ONTAP 버전 9.8-9.12.1로 업그레이드할 수 있습니다. 업그레이드하기 전에 다음을 권장합니다.인스턴스 유형을 변경합니다 . 인스턴스 유형을 변경할 수 없는 경우 다음을 수행해야 합니다.향상된 네트워킹을 활성화하세요 업그레이드하기 전에. 인스턴스 유형을 변경하고 향상된 네트워킹을 활성화하는 방법에 대해 자세히 알아보려면 다음 섹션을 읽어보세요.

9.13.0 이상 버전을 실행하는 Cloud Volumes ONTAP 에서는 c4, m4, r4 EC2 인스턴스 유형으로 업그레이드할 수 없습니다. 이 경우에는 디스크 개수를 줄여야 합니다.인스턴스 유형을 변경합니다 또는 c5, m5, r5 EC2 인스턴스 유형을 사용하여 새로운 HA 쌍 구성을 배포하고 데이터를 마이그레이션합니다.

인스턴스 유형 변경

c4, m4 및 r4 EC2 인스턴스 유형은 c5, m5 및 r5 EC2 인스턴스 유형보다 노드당 더 많은 디스크를 허용합니다. 실행 중인 c4, m4 또는 r4 EC2 인스턴스의 노드당 디스크 수가 c5, m5 및 r5 인스턴스의 노드당 최대 디스크 허용량보다 낮은 경우 EC2 인스턴스 유형을 c5, m5 또는 r5로 변경할 수 있습니다.

"EC2 인스턴스별 디스크 및 계층화 제한 확인" "Cloud Volumes ONTAP 의 EC2 인스턴스 유형 변경"

인스턴스 유형을 변경할 수 없는 경우 다음 단계를 따르세요.향상된 네트워킹 활성화 .

향상된 네트워킹 활성화

Cloud Volumes ONTAP 버전 9.8 이상으로 업그레이드하려면 c4, m4 또는 r4 인스턴스 유형을 실행하는 클러스터에서 _향상된 네트워킹_을 활성화해야 합니다. ENA를 활성화하려면 기술 자료 문서를 참조하세요."AWS Cloud Volumes ONTAP 인스턴스에서 SR-IOV 또는 ENA와 같은 향상된 네트워킹을 활성화하는 방법" .

업그레이드 준비

업그레이드를 수행하기 전에 시스템이 준비되었는지 확인하고 필요한 구성을 변경해야 합니다.

- 가동 중지 시간을 계획하세요
- 자동 환불이 여전히 활성화되어 있는지 확인하세요.
- SnapMirror 전송 일시 중단
- 집계가 온라인인지 확인하세요
- 모든 LIF가 홈 포트에 있는지 확인하세요.

가동 중지 시간을 계획하세요

단일 노드 시스템을 업그레이드하면 업그레이드 프로세스로 인해 시스템이 최대 25분 동안 오프라인 상태가 되며, 이 기간 동안 I/O가 중단됩니다.

많은 경우 HA 쌍을 업그레이드하는 작업은 중단 없이 진행되며 I/O도 중단되지 않습니다. 이러한 중단 없는 업그레이드 프로세스 동안 각 노드는 클라이언트에 I/O를 계속 제공하기 위해 동시에 업그레이드됩니다.

세션 지향 프로토콜은 업그레이드 중 특정 영역의 클라이언트와 애플리케이션에 부정적인 영향을 미칠 수 있습니다. 자세한 내용은 다음을 참조하세요. "ONTAP 문서"

자동 환불이 여전히 활성화되어 있는지 확인하세요.

Cloud Volumes ONTAP HA 쌍에서 자동 반환 기능을 활성화해야 합니다(이는 기본 설정입니다). 그렇지 않으면 작업이 실패합니다.

"ONTAP 설명서: 자동 반환 구성을 위한 명령"

SnapMirror 전송 일시 중단

Cloud Volumes ONTAP 시스템에 활성 SnapMirror 관계가 있는 경우 Cloud Volumes ONTAP 소프트웨어를 업데이트하기 전에 전송을 일시 중단하는 것이 가장 좋습니다. 전송을 일시 중단하면 SnapMirror 오류가 방지됩니다. 대상 시스템에서 전송을 중단해야 합니다.

NetApp Backup and Recovery SnapMirror 구현(SnapMirror Cloud라고 함)을 사용하여 백업 파일을 생성하지만, 시스템을 업그레이드할 때 백업을 중단할 필요는 없습니다.

이 작업에 관하여

이 단계에서는 ONTAP System Manager 9.3 이상을 사용하는 방법을 설명합니다.

단계

1. 대상 시스템에서 시스템 관리자에 로그인합니다.

   웹 브라우저에서 클러스터 관리 LIF의 IP 주소를 입력하면 System Manager에 로그인할 수 있습니다. IP 주소는 Cloud Volumes ONTAP 시스템에서 찾을 수 있습니다.

   콘솔에 액세스하는 컴퓨터는 Cloud Volumes ONTAP 에 네트워크로 연결되어 있어야 합니다. 예를 들어, 클라우드 공급자 네트워크에 있는 점프 호스트에서 콘솔에 로그인해야 할 수도 있습니다.

2. *보호 > 관계*를 클릭합니다.
3. 관계를 선택하고 *작업 > 정지*를 클릭합니다.

집계가 온라인인지 확인하세요

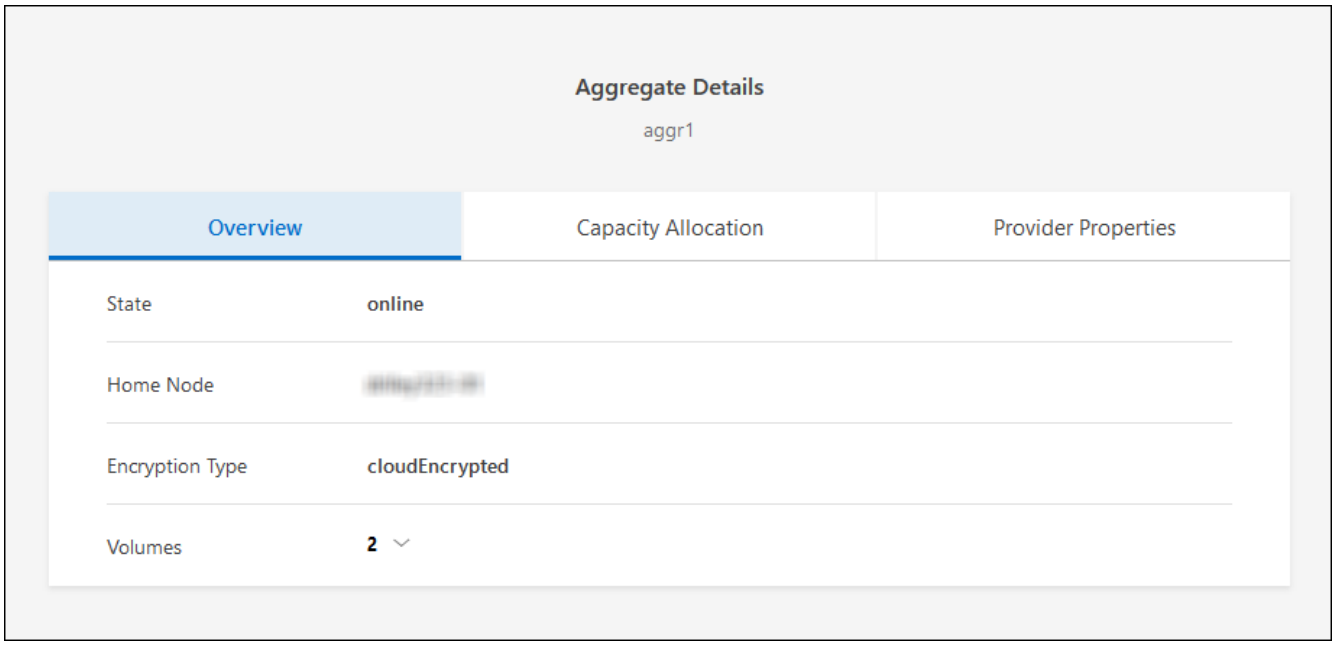
소프트웨어를 업데이트하기 전에 Cloud Volumes ONTAP 의 집계가 온라인 상태여야 합니다. 대부분의 구성에서 집계는 온라인 상태여야 하지만, 그렇지 않은 경우 온라인으로 전환해야 합니다.

이 작업에 관하여

이 단계에서는 ONTAP System Manager 9.3 이상을 사용하는 방법을 설명합니다.

단계

1. Cloud Volumes ONTAP 시스템에서 집계 탭을 클릭합니다.
2. 필요한 집계 타일에서 다음을 클릭합니다. ••• 아이콘을 클릭한 다음 *집계 세부 정보 보기*를 선택하세요.



3. 집계가 오프라인인 경우 ONTAP 시스템 관리자를 사용하여 집계를 온라인으로 전환합니다.
   a. *저장소 > 집계 및 디스크 > 집계*를 클릭합니다.
   b. 집계를 선택한 다음 *추가 작업 > 상태 > 온라인*을 클릭합니다.

모든 **LIF**가 홈 포트에 있는지 확인하세요.

업그레이드하기 전에 모든 LIF가 홈 포트에 있어야 합니다. ONTAP 설명서를 참조하세요."모든 LIF가 홈 포트에 있는지 확인하세요" .

업그레이드 실패 오류가 발생하면 기술 자료(KB) 문서를 참조하세요."Cloud Volumes ONTAP 업그레이드 실패" .

Cloud Volumes ONTAP 업그레이드

콘솔은 업그레이드할 수 있는 새로운 버전이 있을 때 알려줍니다. 이 알림에서 업그레이드 프로세스를 시작할 수 있습니다. 자세한 내용은 다음을 참조하세요. 콘솔 알림에서 업그레이드 .

외부 URL의 이미지를 사용하여 소프트웨어 업그레이드를 수행하는 또 다른 방법입니다. 이 옵션은 콘솔이 S3 버킷에 액세스하여 소프트웨어를 업그레이드할 수 없거나 패치가 제공된 경우에 유용합니다. 자세한 내용은 다음을 참조하세요. URL에서 사용 가능한 이미지에서 업그레이드 .

콘솔 알림에서 업그레이드

Cloud Volumes ONTAP Cloud Volumes ONTAP ONTAP 작업 환경에 알림을 표시합니다.

알림을 통해 Cloud Volumes ONTAP 업그레이드하려면 NetApp 지원 사이트 계정이 있어야 합니다.

이 알림을 통해 업그레이드 프로세스를 시작할 수 있습니다. 이 알림은 S3 버킷에서 소프트웨어 이미지를 얻고, 이미지를 설치한 다음 시스템을 다시 시작하여 프로세스를 자동화합니다.

시작하기 전에

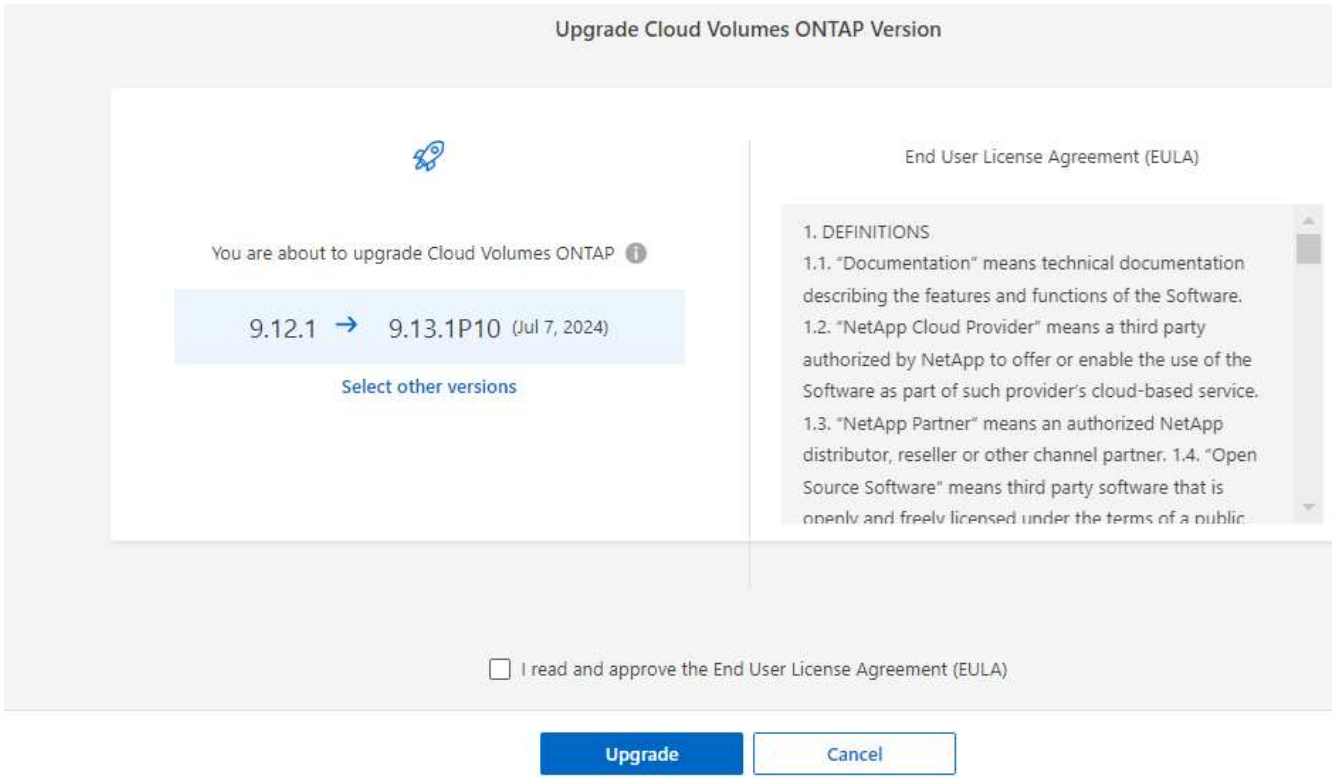
볼륨이나 집계 생성과 같은 작업은 Cloud Volumes ONTAP 시스템에서 진행 중이어서는 안 됩니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. Cloud Volumes ONTAP 시스템을 선택하세요.

   새 버전이 출시되면 개요 탭에 알림이 표시됩니다.

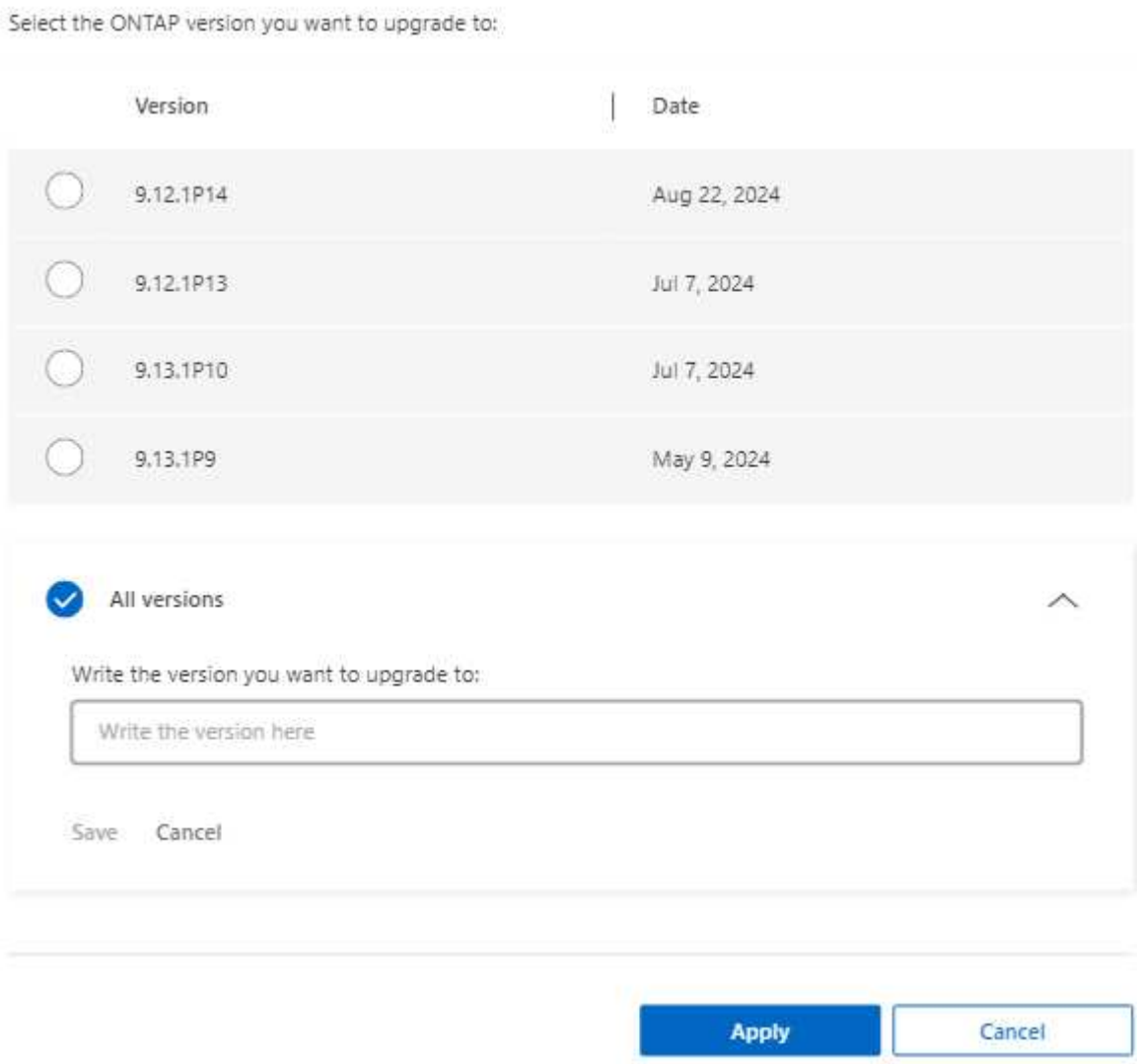
3. 설치된 Cloud Volumes ONTAP 버전을 업그레이드하려면 *지금 업그레이드!*를 클릭하세요. 기본적으로 업그레이드할 수 있는 최신 호환 버전이 표시됩니다.



다른 버전으로 업그레이드하려면 *다른 버전 선택*을 클릭하세요. 시스템에 설치된 버전과 호환되는 최신 Cloud Volumes ONTAP 버전이 나열되어 있습니다. 예를 들어, 시스템에 설치된 버전이 9.12.1P3이고, 다음과 같은 호환 버전을 사용할 수 있습니다.

- 9.12.1P4부터 9.12.1P14까지
- 9.13.1 및 9.13.1P1 업그레이드를 위한 기본 버전으로 9.13.1P1이 표시되고, 다른 사용 가능한 버전으로 9.12.1P13, 9.13.1P14, 9.13.1 및 9.13.1P1이 표시됩니다.

4. 선택적으로, *모든 버전*을 클릭하여 업그레이드하려는 다른 버전(예: 설치된 버전의 다음 패치)을 입력할 수 있습니다. 현재 Cloud Volumes ONTAP 버전의 호환 업그레이드 경로는 다음을 참조하세요."지원되는 업그레이드 경로" .
5. *저장*을 클릭한 다음 *적용*을 클릭합니다



.

6. 업그레이드 Cloud Volumes ONTAP 페이지에서 EULA를 읽은 다음 *EULA를 읽고 승인합니다*를 선택합니다.
7. *업그레이드*를 선택하세요.
8. 진행 상황을 보려면 Cloud Volumes ONTAP 시스템에서 *감사*를 선택하세요.

결과

콘솔에서 소프트웨어 업그레이드가 시작됩니다. 소프트웨어 업데이트가 완료되면 시스템에서 작업을 수행할 수 있습니다.

당신이 완료한 후

SnapMirror 전송을 중단한 경우 시스템 관리자를 사용하여 전송을 재개하세요.

URL에서 사용 가능한 이미지에서 업그레이드

Cloud Volumes ONTAP 소프트웨어 이미지를 콘솔 에이전트나 HTTP 서버에 배치한 다음 콘솔에서 소프트웨어 업그레이드를 시작할 수 있습니다. 콘솔이 S3 버킷에 액세스하여 소프트웨어를 업그레이드할 수 없는 경우 이 옵션을

사용할 수 있습니다.

시작하기 전에

- 볼륨이나 집계 생성과 같은 작업은 Cloud Volumes ONTAP 시스템에서 진행 중이어서는 안 됩니다.
- ONTAP 이미지를 호스팅하기 위해 HTTPS를 사용하는 경우 인증서 누락으로 인해 SSL 인증 문제가 발생하여 업그레이드가 실패할 수 있습니다. 해결 방법은 ONTAP 과 콘솔 간 인증에 사용할 CA 서명 인증서를 생성하고 설치하는 것입니다.

  NetApp 기술 자료로 이동하여 단계별 지침을 확인하세요.

  "NetApp KB: 업그레이드 이미지를 호스팅하기 위해 콘솔을 HTTPS 서버로 구성하는 방법"

단계

1. 선택 사항: Cloud Volumes ONTAP 소프트웨어 이미지를 호스팅할 수 있는 HTTP 서버를 설정합니다.

   가상 네트워크에 VPN 연결이 있는 경우 Cloud Volumes ONTAP 소프트웨어 이미지를 자체 네트워크의 HTTP 서버에 배치할 수 있습니다. 그렇지 않은 경우 클라우드의 HTTP 서버에 파일을 저장해야 합니다.

2. Cloud Volumes ONTAP 에 자체 보안 그룹을 사용하는 경우 아웃바운드 규칙에서 HTTP 연결을 허용하여 Cloud Volumes ONTAP 이 소프트웨어 이미지에 액세스할 수 있는지 확인하세요.

   미리 정의된 Cloud Volumes ONTAP 보안 그룹은 기본적으로 아웃바운드 HTTP 연결을 허용합니다.

3. 소프트웨어 이미지를 얻으세요 "NetApp 지원 사이트" .
4. 소프트웨어 이미지를 콘솔 에이전트나 파일이 제공될 HTTP 서버의 디렉토리에 복사합니다.

   두 가지 경로가 있습니다. 올바른 경로는 콘솔 에이전트 버전에 따라 다릅니다.

   - `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
   - `/opt/application/netapp/cloudmanager/ontap/images/`

5. 시스템에서 다음을 클릭합니다. ••• 아이콘을 클릭한 다음 * Cloud Volumes ONTAP 업데이트*를 클릭합니다.
6. Cloud Volumes ONTAP 버전 업데이트 페이지에서 URL을 입력한 다음 *이미지 변경*을 클릭합니다.

   위에 표시된 경로의 콘솔 에이전트에 소프트웨어 이미지를 복사한 경우 다음 URL을 입력합니다.

   http://<콘솔_에이전트_개인-IP-주소>/ontap/images/<이미지-파일-이름>

   URL에서 *이미지 파일 이름*은 "cot.image.9.13.1P2.tgz" 형식을 따라야 합니다.

7. 확인하려면 *계속*을 클릭하세요.

결과

콘솔에서 소프트웨어 업데이트가 시작됩니다. 소프트웨어 업데이트가 완료되면 시스템에서 작업을 수행할 수 있습니다.

당신이 완료한 후

SnapMirror 전송을 중단한 경우 시스템 관리자를 사용하여 전송을 재개하세요.

Google Cloud NAT 게이트웨이 사용 시 다운로드 실패 문제 해결

콘솔 에이전트는 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 자동으로 다운로드합니다. 구성에서 Google Cloud NAT 게이트웨이를 사용하는 경우 다운로드가 실패할 수 있습니다. 이 문제는 소프트웨어 이미지가 나누어지는 부분의 수를 제한하면 해결할 수 있습니다. 이 단계를 완료하려면 API를 사용해야 합니다.

단계

1. 다음 JSON을 본문으로 하여 `/occm/`config에 PUT 요청을 제출합니다.

```
{
  "maxDownloadSessions": 32
}
```

_maxDownloadSessions_의 값은 1이거나 1보다 큰 정수일 수 있습니다. 값이 1이면 다운로드한 이미지는 분할되지 않습니다.

32는 예시 값입니다. 사용해야 하는 값은 NAT 구성과 동시에 가질 수 있는 세션 수에 따라 달라집니다.

"/occm/config API 호출에 대해 자세히 알아보세요" .

Cloud Volumes ONTAP 종량제 시스템 등록

NetApp 의 지원은 Cloud Volumes ONTAP PAYGO(Pay-as-you-go) 시스템에 포함되어 있지만, 먼저 NetApp 에 시스템을 등록하여 지원을 활성화해야 합니다.

ONTAP 소프트웨어를 업그레이드하려면 NetApp 에 PAYGO 시스템을 등록해야 합니다."이 페이지에 설명되어 있습니다" .

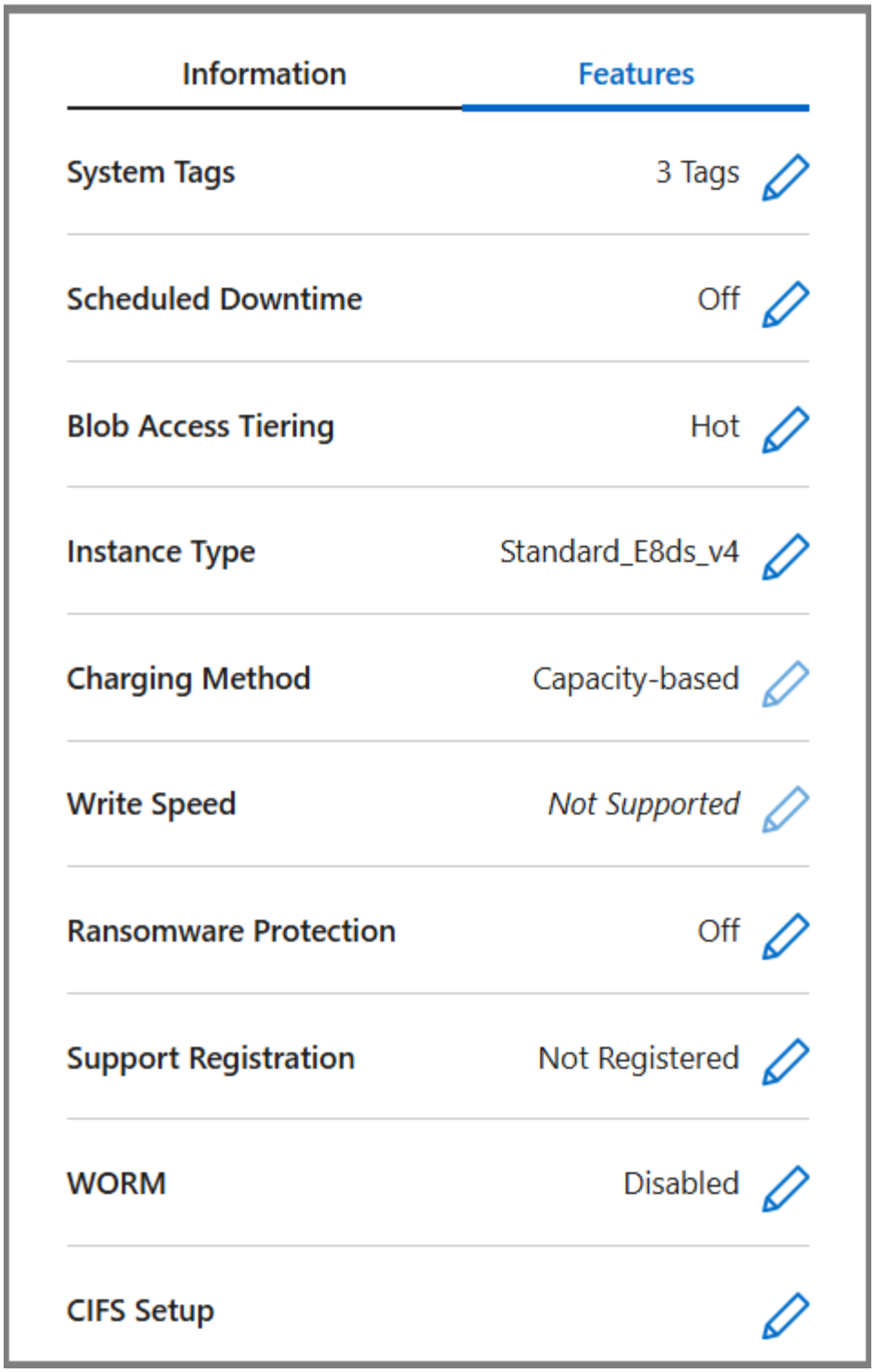
지원에 등록되지 않은 시스템에서도 새로운 버전이 출시되면 NetApp Console 에 표시되는 소프트웨어 업데이트 알림을 받게 됩니다. 하지만 소프트웨어를 업그레이드하려면 먼저 시스템을 등록해야 합니다.

단계

1. 아직 NetApp 지원 사이트 계정을 콘솔에 추가하지 않았다면 *계정 설정*으로 이동하여 지금 추가하세요.

   "NetApp 지원 사이트 계정을 추가하는 방법을 알아보세요" .

2. 시스템 페이지에서 등록하려는 시스템 이름을 두 번 클릭합니다.
3. 개요 탭에서 기능 패널을 클릭한 다음 지원 등록 옆에 있는 연필 아이콘을 클릭합니다.



4. NetApp 지원 사이트 계정을 선택하고 *등록*을 클릭하세요.

결과

해당 시스템은 NetApp 에 등록되어 있습니다.

Cloud Volumes ONTAP 노드 기반 라이선스를 용량 기반 라이선스로 변환

노드 기반 라이선스의 사용 가능 기간 종료(EOA) 후에는 NetApp Console 의 라이선스 변환

도구를 사용하여 용량 기반 라이선스로 전환해야 합니다.

연간 또는 장기 약정의 경우 NetApp EOA 날짜(2024년 11월 11일) 또는 라이선스 만료일 전에 NetApp 담당자에게 연락하여 전환에 필요한 전제 조건이 충족되었는지 확인하는 것을 권장합니다. Cloud Volumes ONTAP 노드에 대한 장기 계약이 없고 온디맨드 종량제(PAYGO) 구독으로 시스템을 실행하는 경우 2024년 12월 31일 지원 종료(EOS) 전에 전환을 계획하는 것이 중요합니다. 두 경우 모두 NetApp Console 의 라이선스 변환 도구를 사용하여 원활하게 전환하기 전에 시스템이 요구 사항을 충족하는지 확인해야 합니다.

EOA 및 EOS에 대한 정보는 다음을 참조하세요."노드 기반 라이선스 제공 종료" .

이 작업에 관하여

- 라이선스 변환 도구를 사용하면 노드 기반에서 용량 기반 라이선스 모델로의 전환이 현장에서 온라인에서 수행되므로 데이터 마이그레이션이나 추가 클라우드 리소스 프로비저닝이 필요 없습니다.
- 이는 중단 없는 작업이므로 서비스 중단이나 애플리케이션 가동 중지가 발생하지 않습니다.
- Cloud Volumes ONTAP 시스템의 계정 및 애플리케이션 데이터는 그대로 유지됩니다.
- 기본 클라우드 리소스는 변환 후에도 영향을 받지 않습니다.
- 라이선스 변환 도구는 단일 노드, 단일 가용성 영역(AZ)의 고가용성(HA), 여러 AZ의 HA, 자체 라이선스 사용(BYOL), PAYGO 등 모든 배포 유형을 지원합니다.
- 이 도구는 모든 노드 기반 라이선스를 소스로, 모든 용량 기반 라이선스를 대상으로 지원합니다. 예를 들어 PAYGO Standard 노드 기반 라이선스가 있는 경우 마켓플레이스를 통해 구매한 모든 용량 기반 라이선스로 변환할 수 있습니다. NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 에 대한 BYOL 라이선싱의 제한된 가용성" .
- 이러한 변환은 AWS, Azure, Google Cloud 등 모든 클라우드 제공업체에서 지원됩니다.
- 변환 후 노드 기반 라이센스의 일련 번호는 용량 기반 형식으로 대체됩니다. 이 작업은 변환의 일부로 수행되며 NetApp 지원 사이트(NSS) 계정에 반영됩니다.
- 용량 기반 모델로 전환하면 데이터는 노드 기반 라이선싱과 동일한 위치에 계속 보관됩니다. 이러한 접근 방식은 데이터 배치에 어떠한 중단도 발생하지 않도록 보장하며, 전환 과정 전반에 걸쳐 데이터 주권 원칙을 지지합니다.

시작하기 전에

- 고객 액세스 또는 관리자 액세스 권한이 있는 NSS 계정이 있어야 합니다.
- 귀하의 NSS 계정은 콘솔에 액세스하는 데 사용한 사용자 자격 증명으로 등록되어야 합니다.
- Cloud Volumes ONTAP 시스템은 고객 액세스 또는 관리자 액세스 권한이 있는 NSS 계정에 연결되어야 합니다.
- BYOL 라이선스 또는 마켓플레이스 구독 등 유효한 용량 기반 라이선스가 있어야 합니다.
- 귀하의 계정에는 용량 기반 라이선스가 사용 가능해야 합니다. 이 라이선스는 콘솔의 * Licenses and subscriptions*에서 사용할 수 있는 마켓플레이스 구독 또는 BYOL/개인 제공 패키지일 수 있습니다.
- 목적지 패키지를 선택하기 전에 다음 기준을 이해하세요.
  - 계정에 용량 기반 BYOL 라이선스가 있는 경우 선택한 대상 패키지는 계정의 BYOL 용량 기반 라이선스와 일치해야 합니다.
    - 언제 `Professional` 대상 패키지로 선택된 경우 계정에 Professional 패키지가 포함된 BYOL 라이선스가 있어야 합니다.
    - 언제 `Essentials` 대상 패키지로 선택된 경우, 계정에 Essentials 패키지가 포함된 BYOL 라이선스가 있어야 합니다.
  - 대상 패키지가 계정의 BYOL 라이선스 가용성과 일치하지 않으면 용량 기반 라이선스에 선택한 패키지가

포함되지 않을 수 있습니다. 이 경우 마켓플레이스 구독을 통해 요금이 청구됩니다.

- 용량 기반 BYOL 라이선스가 없고 마켓플레이스 구독만 있는 경우, 선택한 패키지가 용량 기반 마켓플레이스 구독에 포함되어 있는지 확인해야 합니다.
- 기존 용량 기반 라이선스에 충분한 용량이 없고, 추가 용량 사용에 대해 요금을 청구하는 마켓플레이스 구독이 있는 경우, 마켓플레이스 구독을 통해 추가 용량에 대한 요금이 청구됩니다.
- 기존 용량 기반 라이선스에 충분한 용량이 없고, 추가 용량 사용에 대한 요금을 청구할 마켓플레이스 구독이 없으면 변환이 이루어질 수 없습니다. 추가 용량에 대한 요금을 청구하거나 현재 라이선스의 사용 가능한 용량을 확장하려면 마켓플레이스 구독을 추가해야 합니다.
- 대상 패키지가 계정의 BYOL 라이선스 가용성과 맞지 않고 기존 용량 기반 라이선스에 충분한 용량이 없는 경우 마켓플레이스 구독을 통해 요금이 청구됩니다.

이러한 요구 사항 중 하나라도 충족되지 않으면 라이센스 전환이 이루어지지 않습니다. 특정한 경우 라이센스는 변환되지만 사용할 수 없을 수도 있습니다. 정보 아이콘을 클릭하여 문제를 파악하고 시정 조치를 취하세요.

단계

1. 시스템 페이지에서 라이선스 유형을 수정하려는 시스템의 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭합니다.
3. 충전 방법 옆에 있는 연필 아이콘을 확인하세요. 시스템의 충전 방법이 다음과 같은 경우 `Node Based` , 용량별 요금으로 변환할 수 있습니다.

   Cloud Volumes ONTAP 시스템이 이미 용량에 따라 요금이 청구되었거나 요구 사항 중 하나라도 충족되지 않으면 아이콘이 비활성화됩니다.

4. 노드 기반 라이선스를 용량 기반으로 변환 화면에서 시스템 이름과 소스 라이선스 세부 정보를 확인합니다.
5. 기존 라이선스를 변환할 대상 패키지를 선택하세요.
   - 골자. 기본값은 `Essentials` .
   - 전문적인
6. BYOL 라이선스가 있는 경우 변환이 완료된 후 콘솔에서 노드 기반 라이선스를 삭제하기 위한 확인란을 선택할 수 있습니다. 변환이 진행 중이면 이 확인란을 선택해도 콘솔에서 라이센스가 제거되지 않습니다. 이 옵션은 마켓플레이스 구독에는 사용할 수 없습니다.
7. 변경 사항의 의미를 이해했음을 확인하려면 확인란을 선택한 다음 *계속*을 클릭합니다.

당신이 완료한 후

새로운 라이선스 일련 번호를 보고 콘솔의 * Licenses and subscriptions* 메뉴에서 변경 사항을 확인하세요.

다양한 하이퍼스칼라 가격 책정

가격에 대한 자세한 내용은 다음을 참조하세요. "NetApp Console 웹사이트" .

특정 하이퍼스칼라에 대한 개인 제안에 대한 자세한 내용은 다음 주소로 문의하세요.

- AWS - awspo@netapp.com
- Azure - azurepo@netapp.com

- 구글 클라우드 - gcppo@netapp.com

Cloud Volumes ONTAP 시스템 시작 및 중지

NetApp Console 에서 Cloud Volumes ONTAP 중지하고 시작하여 클라우드 컴퓨팅 비용을 관리할 수 있습니다.

Cloud Volumes ONTAP 자동 종료 예약

컴퓨팅 비용을 낮추려면 특정 시간 간격으로 Cloud Volumes ONTAP 종료해야 할 수도 있습니다. 이 작업을 수동으로 수행하는 대신, 콘솔을 구성하여 특정 시간에 시스템을 자동으로 종료한 다음 다시 시작할 수 있습니다.

이 작업에 관하여

- Cloud Volumes ONTAP 시스템의 자동 종료를 예약하는 경우, 활성 데이터 전송이 진행 중이면 콘솔에서 종료를 연기합니다.

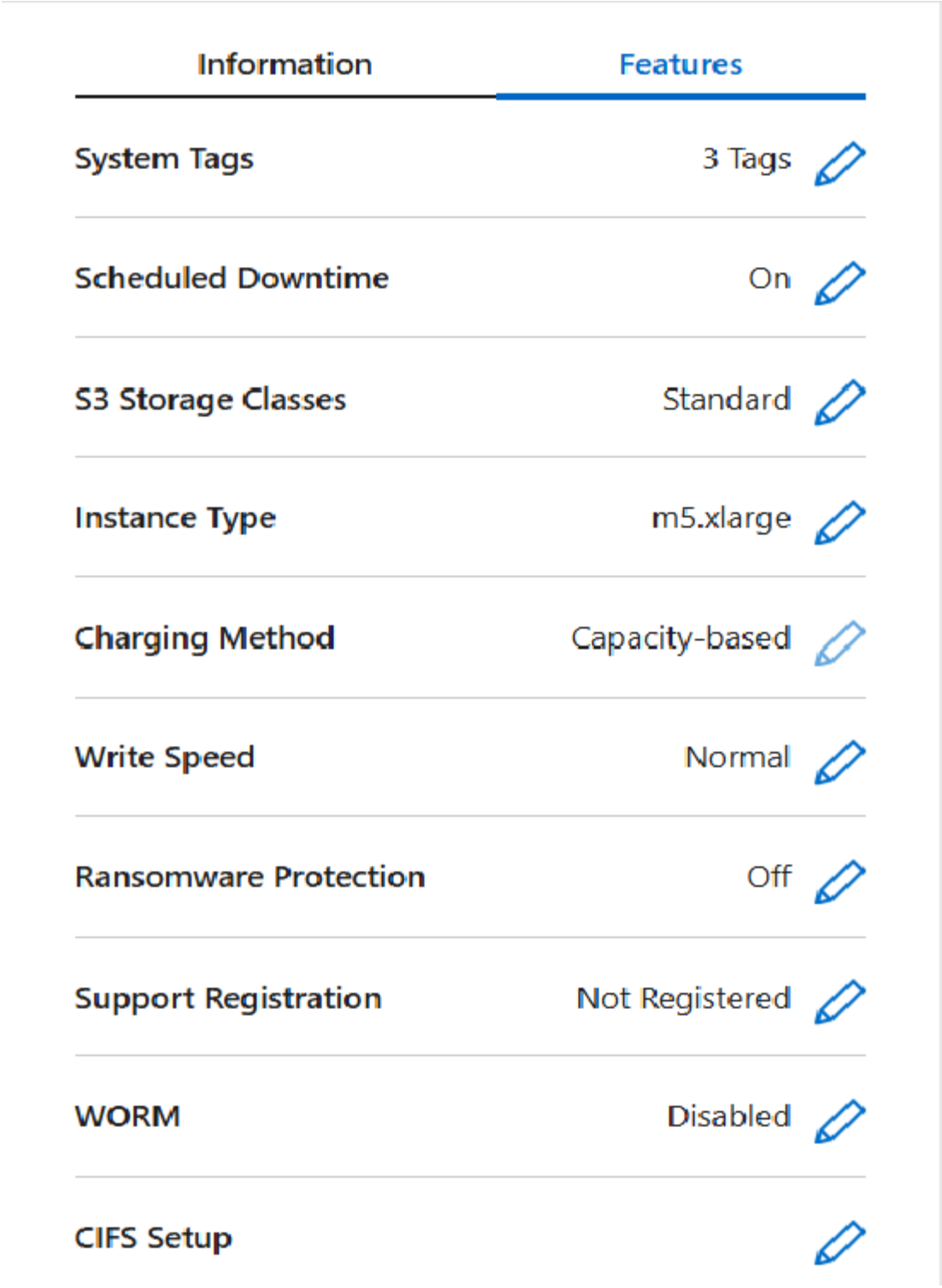
  전송이 완료되면 시스템이 종료됩니다.

- 이 작업은 HA 쌍의 두 노드를 자동으로 종료하도록 예약합니다.
- 예약된 종료를 통해 Cloud Volumes ONTAP 끄면 부팅 및 루트 디스크의 스냅샷이 생성되지 않습니다.

  다음 섹션에서 설명하는 대로, 스냅샷은 수동 종료를 수행할 때만 자동으로 생성됩니다.

단계

1. 시스템 페이지에서 Cloud Volumes ONTAP 시스템을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 예약된 가동 중지 시간 옆에 있는 연필 아이콘을 클릭합니다.



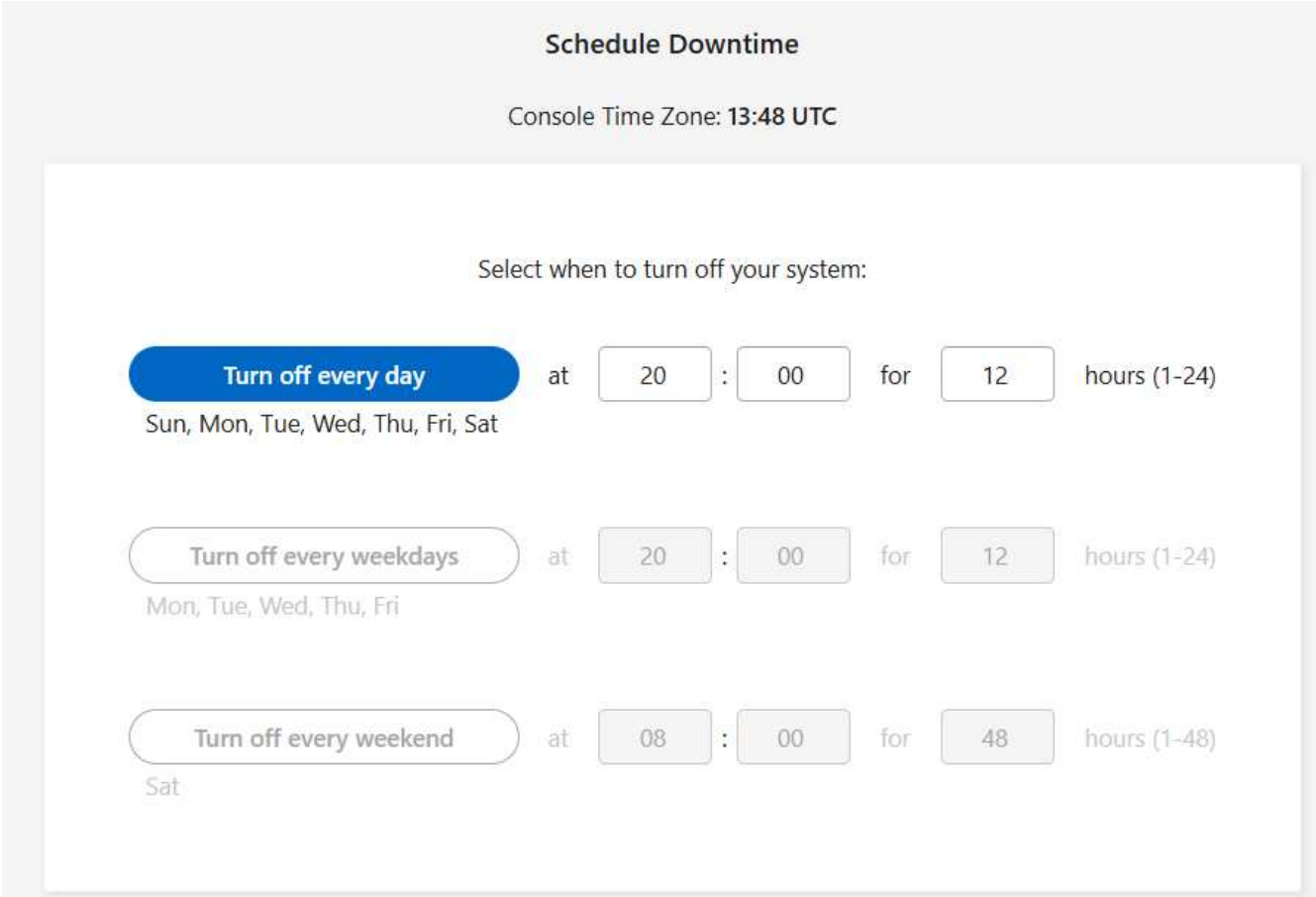
3. 종료 일정을 지정하세요:

   a. 매일, 주중마다, 주말마다 시스템을 종료할지 또는 이 세 가지 옵션을 조합하여 종료할지 선택하세요.

   b. 시스템을 끄고 싶은 시점과 끄고 싶은 시간을 지정하세요.

      예

      다음 이미지는 콘솔에 매주 토요일 오후 8시(오후 8시)에 12시간 동안 시스템을 종료하도록 지시하는 일정을 보여줍니다. 콘솔은 매주 월요일 오전 12시에 시스템을 다시 시작합니다.



4. *저장*을 클릭하세요.

결과

일정이 저장되었습니다. 기능 패널 아래의 해당 예약된 가동 중지 시간 항목에 '켜짐'이 표시됩니다.

Cloud Volumes ONTAP 중지

Cloud Volumes ONTAP 중지하면 컴퓨팅 비용이 발생하지 않고 루트 및 부팅 디스크의 스냅샷이 생성되므로 문제 해결에 도움이 될 수 있습니다.

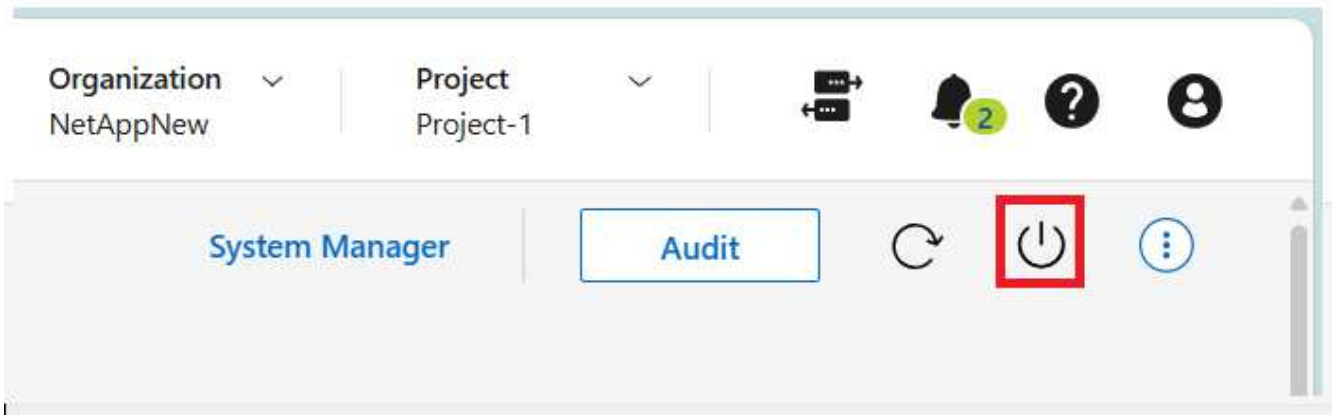
비용을 줄이기 위해 콘솔은 루트 및 부팅 디스크의 오래된 스냅샷을 주기적으로 삭제합니다. 루트 디스크와 부팅 디스크 모두에 가장 최근의 스냅샷 두 개만 보존됩니다.

이 작업에 관하여

HA 쌍을 중지하면 콘솔은 두 노드를 모두 종료합니다.

단계

1. 시스템에서 끄기 아이콘을 클릭합니다.



2. 스냅샷을 생성하면 시스템 복구가 가능하므로 스냅샷 생성 옵션을 활성화해 두세요.
3. *끄기*를 클릭하세요.

   시스템을 중지하는 데 최대 몇 분이 걸릴 수 있습니다. 나중에 시스템 페이지에서 시스템을 다시 시작할 수 있습니다.

재부팅 시 스냅샷이 자동으로 생성됩니다.

NTP 서버를 사용하여 Cloud Volumes ONTAP 시스템 시간 동기화

정확한 시간 동기화를 위해서는 Cloud Volumes ONTAP 시스템에 네트워크 시간 프로토콜(NTP) 서버를 설정해야 합니다. Cloud Volumes ONTAP 시스템의 네트워크 내 시간 동기화를 일관되게 유지하려면 모든 클라우드 공급자에 NTP 서버를 구성해야 합니다.

NTP 서버를 구성하지 않으면 서비스 중단 및 시간 동기화 오류가 발생할 수 있습니다.

다음과 같이 NTP 서버를 지정할 수 있습니다.

- "NetApp Console API".
- ONTAP CLI 명령 "클러스터 시간 서비스 NTP 서버 생성".

관련 링크

- 기술 자료(KB) 문서: "CVO 클러스터는 NTP를 어떻게 사용합니까?"
- "API 사용을 준비하세요"
- "Cloud Volumes ONTAP 워크플로"
- "필수 식별자 가져오기"
- "NetApp Console 에 REST API 사용"

시스템 쓰기 속도 수정

NetApp Console 에서 Cloud Volumes ONTAP 에 대한 일반 쓰기 속도 또는 높은 쓰기 속도를 선택할 수 있습니다. 기본 쓰기 속도는 보통입니다. 작업 부하에 빠른 쓰기 성능이 필요한 경우 높은 쓰기 속도로 변경할 수 있습니다.

고속 쓰기 기능은 모든 유형의 단일 노드 시스템과 일부 HA 쌍 구성에서 지원됩니다. 지원되는 구성은 다음에서 확인하세요 "Cloud Volumes ONTAP 릴리스 노트"

쓰기 속도를 변경하기 전에 다음을 수행해야 합니다."일반 설정과 높은 설정의 차이점을 이해하세요" .

이 작업에 관하여

- 볼륨이나 집계 생성과 같은 작업이 진행 중이 아닌지 확인하세요.
- 이 변경으로 인해 Cloud Volumes ONTAP 시스템이 다시 시작된다는 점에 유의하세요. 이는 전체 시스템의 가동 중지를 필요로 하는 파괴적인 프로세스입니다.

단계

1. 시스템 페이지에서 쓰기 속도를 구성할 시스템 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 쓰기 속도 옆에 있는 연필 아이콘을 클릭합니다.
3. 보통 또는 *높음*을 선택하세요.

   높음을 선택한 경우, "이해합니다..."라는 문장을 읽고 상자를 체크하여 확인해야 합니다.

   높음 쓰기 속도 옵션은 Google Cloud의 Cloud Volumes ONTAP HA 쌍에서 버전 9.13.0부터 지원됩니다.

4. *저장*을 클릭하고 확인 메시지를 검토한 다음 *승인*을 클릭합니다.

Cloud Volumes ONTAP 클러스터 관리자 비밀번호 변경

Cloud Volumes ONTAP 클러스터 관리자 계정이 포함되어 있습니다. 필요한 경우 NetApp Console 에서 이 계정의 비밀번호를 변경할 수 있습니다.

ONTAP 시스템 관리자나 ONTAP CLI를 통해 관리자 계정의 비밀번호를 변경해서는 안 됩니다. 비밀번호는 콘솔에 반영되지 않습니다. 결과적으로 콘솔에서 인스턴스를 제대로 모니터링할 수 없습니다.

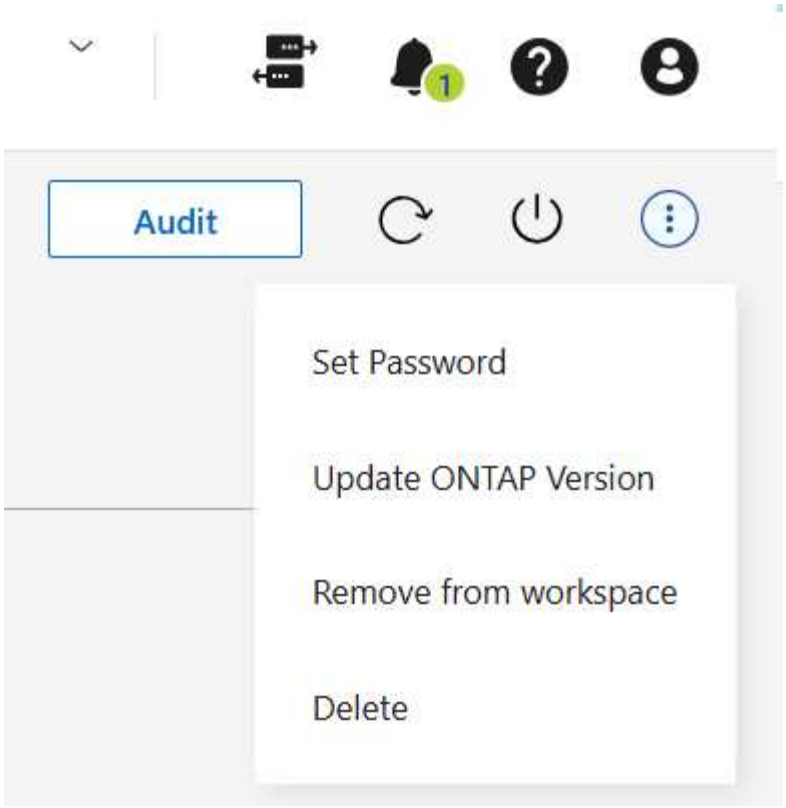
이 작업에 관하여

비밀번호는 몇 가지 규칙을 따라야 합니다. 새로운 비밀번호:

- 단어를 포함해서는 안 됩니다 `admin`
- 길이는 8~50자 사이여야 합니다.
- 영어 문자 1개와 숫자 1개 이상을 포함해야 합니다.
- 다음 특수문자는 포함할 수 없습니다: `/ ( ) { } [ ] # : % " ? \`

단계

1. 시스템 페이지에서 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
2. 콘솔의 오른쪽 상단에서 다음을 클릭하세요. ••• 아이콘을 클릭하고 *비밀번호 설정*을 선택하세요.



시스템 추가, 제거 또는 삭제

NetApp Console 에 기존 **Cloud Volumes ONTAP** 시스템 추가

기존 Cloud Volumes ONTAP 시스템을 검색하고 NetApp Console에 추가하여 중앙 집중식으로 관리할 수 있습니다. 계정을 사용하여 시스템을 온보딩하면 해당 시스템이 해당 계정에 등록됩니다. 여러 계정 또는 조직이 있는 환경에서는 Console 로그인 계정에 등록된 시스템만 검색하고 관리할 수 있습니다.

시스템 등록 작업을 수행할 때는 모든 작업이 시스템이 처음 등록된 동일한 조직 및 계정 내에서 수행되도록 해야 합니다. 예를 들어, Cloud Volumes ONTAP 시스템을 새 NetApp Console 에이전트로 이동할 때 마이그레이션이 동일한 조직 내에서 이루어져야 합니다.

다른 계정이나 조직에 등록된 시스템은 검색, 보기 또는 관리할 수 없습니다.

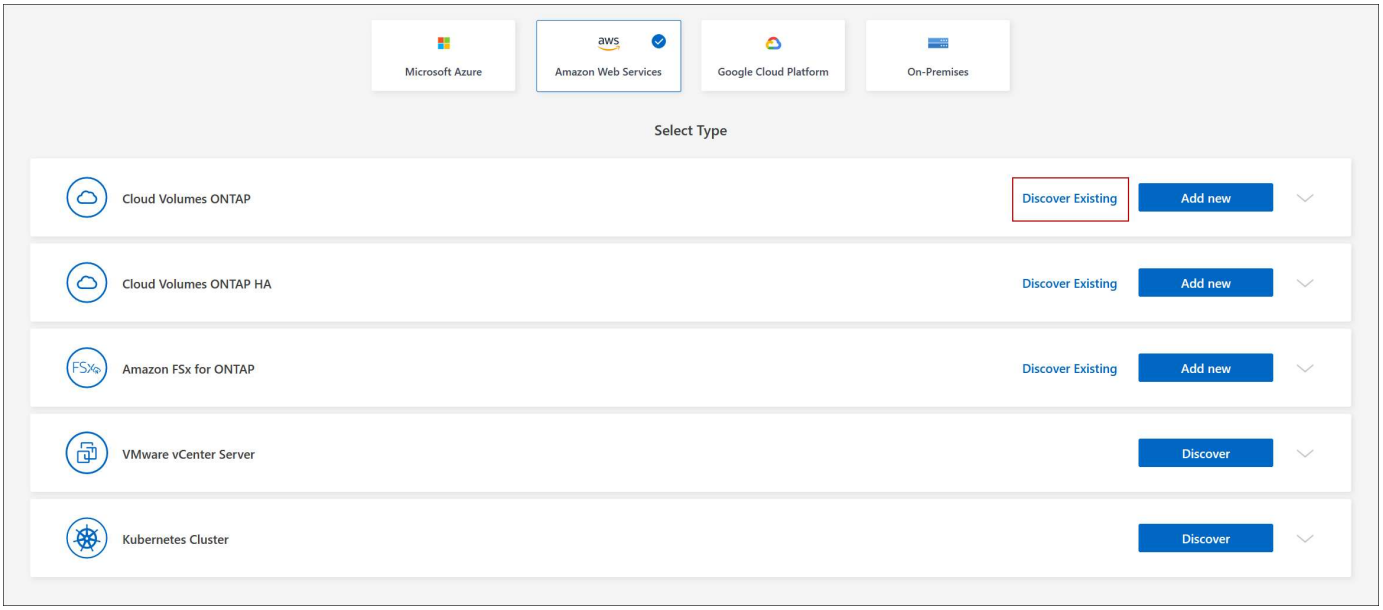
시작하기 전에

Cloud Volumes ONTAP 관리자 사용자 계정의 비밀번호를 알아야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭합니다.
3. 시스템이 있는 클라우드 공급자를 선택하세요.
4. 추가할 Cloud Volumes ONTAP 시스템 유형을 선택하세요.
5. 링크를 클릭하여 기존 시스템을 알아보세요.

+



1. 지역 페이지에서 지역을 선택하세요. 선택한 지역에서 실행 중인 시스템을 볼 수 있습니다.

   이 페이지에서는 Cloud Volumes ONTAP 시스템이 인스턴스로 표시됩니다. 목록에서 현재 계정에 등록된 인스턴스만 선택할 수 있습니다.

2. 자격 증명 페이지에서 Cloud Volumes ONTAP 관리자의 비밀번호를 입력한 다음 *시작*을 선택합니다.

결과

콘솔은 Cloud Volumes ONTAP 시스템을 시스템 페이지에 추가합니다.

NetApp Console 에서 Cloud Volumes ONTAP 시스템 제거

Cloud Volumes ONTAP 시스템을 제거하여 다른 시스템으로 이동하거나 검색 문제를 해결할 수 있습니다.

이 작업에 관하여

Cloud Volumes ONTAP 시스템을 제거하면 NetApp Console 에서도 제거됩니다. Cloud Volumes ONTAP 시스템은 삭제되지 않습니다. 나중에 필요할 경우 시스템을 다시 검색할 수 있습니다.

단계

1. 시스템 페이지에서 제거하려는 시스템을 두 번 클릭합니다.
2. 콘솔의 오른쪽 상단에서 다음을 클릭합니다. ••• 아이콘을 클릭하고 *작업 공간에서 제거*를 선택합니다.
3. 작업 공간에서 제거 창에서 *제거*를 클릭합니다.

결과

콘솔은 시스템을 제거합니다. 사용자는 언제든지 시스템 페이지에서 삭제된 시스템을 다시 찾을 수 있습니다.

NetApp Console 에서 Cloud Volumes ONTAP 시스템 삭제

클라우드 공급업체의 애플리케이션이 아닌 NetApp Console 에서 Cloud Volumes ONTAP

시스템을 항상 삭제해야 합니다. 예를 들어, 클라우드 공급자로부터 라이선스가 부여된 Cloud Volumes ONTAP 인스턴스를 종료하는 경우 다른 인스턴스에 해당 라이선스 키를 사용할 수 없습니다. 라이선스를 해제하려면 콘솔에서 Cloud Volumes ONTAP 시스템을 삭제해야 합니다.

시스템을 삭제하면 콘솔에서 Cloud Volumes ONTAP 인스턴스를 종료하고 디스크와 스냅샷을 삭제합니다.

NetApp Backup and Recovery 에서 관리하는 백업과 NetApp Data Classification 의 인스턴스와 같은 기타 리소스는 시스템을 삭제해도 삭제되지 않습니다. 수동으로 삭제해야 합니다. 그렇지 않으면 이러한 리소스에 대한 요금이 계속 부과됩니다.

콘솔이 클라우드 공급자에 Cloud Volumes ONTAP 배포하면 인스턴스에 대한 종료 보호가 활성화됩니다. 이 옵션은 실수로 종료되는 것을 방지하는 데 도움이 됩니다.

단계

1. 시스템에서 백업 및 복구를 활성화한 경우 백업된 데이터가 여전히 필요한지 확인한 다음 "필요한 경우 백업을 삭제하세요" .

   백업 및 복구는 설계상 Cloud Volumes ONTAP 과 독립적입니다. 백업 및 복구 기능은 Cloud Volumes ONTAP 시스템을 삭제할 때 자동으로 백업을 삭제하지 않으며, 시스템이 삭제된 후 백업을 삭제하는 UI 지원도 현재 제공되지 않습니다.

2. 이 시스템에서 데이터 분류를 활성화했고 다른 시스템에서 이 서비스를 사용하지 않는 경우 해당 서비스의 인스턴스를 삭제해야 합니다.

   "데이터 분류 인스턴스에 대해 자세히 알아보세요" .

3. Cloud Volumes ONTAP 시스템을 삭제합니다.
   a. 시스템 페이지에서 삭제하려는 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
   b. 콘솔의 오른쪽 상단에서 다음을 클릭하세요. ••• 아이콘을 클릭하고 *삭제*를 선택하세요.
   c. 삭제하려는 시스템 이름을 입력한 다음 *삭제*를 클릭합니다. 시스템을 삭제하는 데 최대 5분이 걸릴 수 있습니다.

백업 및 복구는 Cloud Volumes ONTAP Professional 라이선스에 대해서만 무료입니다. 이 무료 혜택은 삭제된 환경에는 적용되지 않습니다. Cloud Volumes ONTAP 환경의 백업된 사본이 백업 및 복구 인스턴스에 보관되는 경우, 해당 사본이 삭제될 때까지 백업된 사본에 대한 요금이 청구됩니다.

AWS 관리

AWS에서 Cloud Volumes ONTAP 시스템에 대한 EC2 인스턴스 유형 수정

AWS에서 Cloud Volumes ONTAP 시작하면 여러 인스턴스나 유형 중에서 선택할 수 있습니다. 필요에 따라 인스턴스 유형이 너무 크거나 작다고 판단되면 언제든지 인스턴스 유형을 변경할 수 있습니다.

이 작업에 관하여

- Cloud Volumes ONTAP HA 쌍에서 자동 반환 기능을 활성화해야 합니다(이는 기본 설정입니다). 그렇지 않으면 작업이 실패합니다.

"ONTAP 9 설명서: 자동 반환 구성을 위한 명령"

- 인스턴스 유형을 변경하면 AWS 서비스 요금에 영향을 미칠 수 있습니다.
- 이 작업은 Cloud Volumes ONTAP 다시 시작합니다.

  단일 노드 시스템의 경우 I/O가 중단됩니다.

  HA 쌍의 경우 변경은 중단되지 않습니다. HA 쌍은 계속해서 데이터를 제공합니다.

NetApp Console 인수를 시작하고 반환을 기다리는 방식으로 한 번에 한 노드씩 변경합니다. NetApp의 품질 보증 팀은 이 프로세스 동안 파일 쓰기와 읽기를 모두 테스트했으며 클라이언트 측에서 아무런 문제도 발견하지 못했습니다. 연결이 변경됨에 따라 I/O 수준에서 일부 재시도가 관찰되었지만 애플리케이션 계층은 NFS/CIFS 연결의 재배선을 극복했습니다.

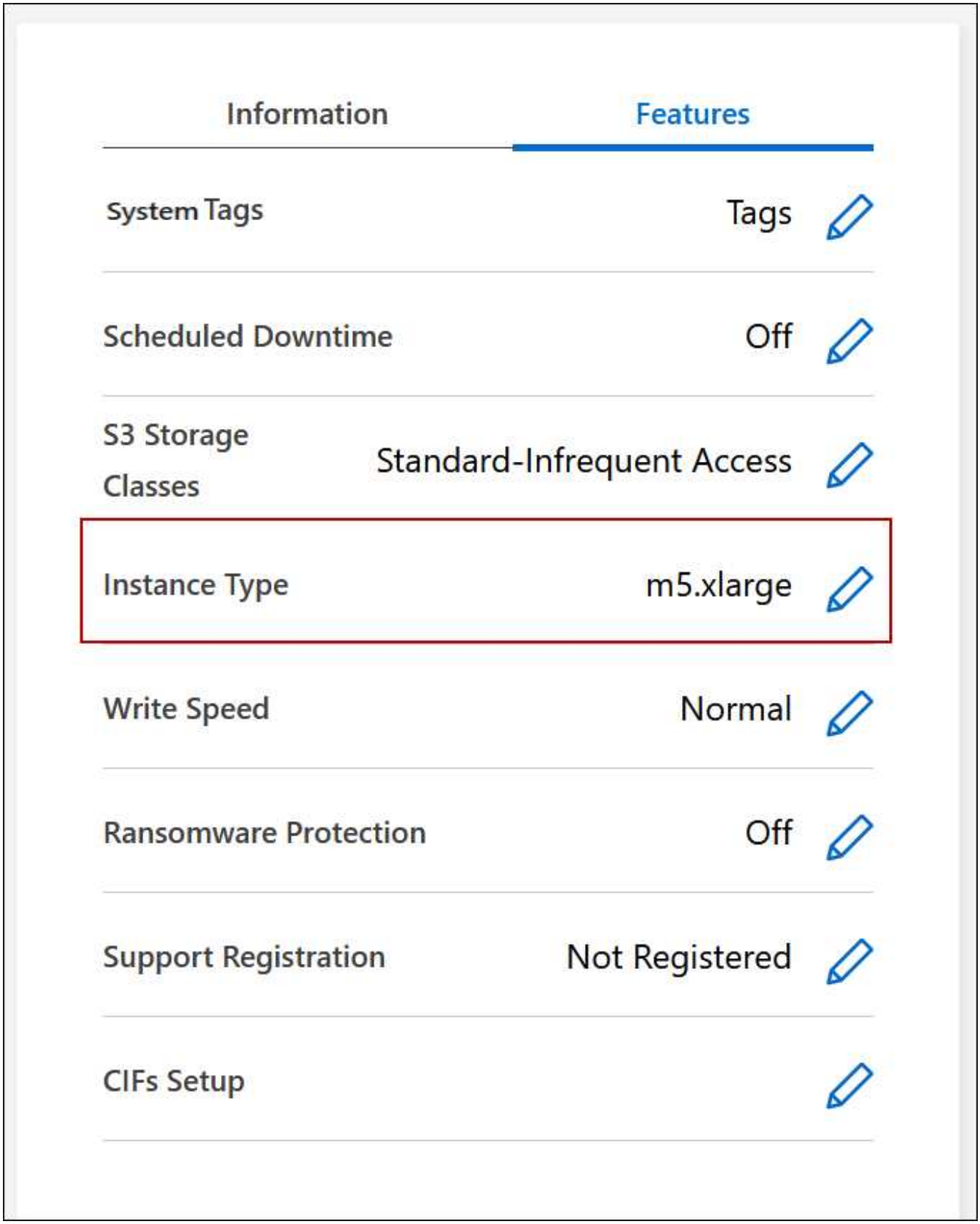
참조

AWS에서 지원되는 인스턴스 유형 목록은 다음을 참조하세요."지원되는 EC2 인스턴스" .

c4, m4 또는 r4 인스턴스에서 인스턴스 유형을 변경할 수 없는 경우 KB 문서를 참조하세요."AWS Xen CVO 인스턴스를 Nitro(KVM)로 변환" .

단계

1. 시스템 페이지에서 시스템을 선택하세요.
2. 개요 탭에서 기능 패널을 클릭한 다음 인스턴스 유형 옆에 있는 연필 아이콘을 클릭합니다.



노드 기반 사용량 기반(PAYGO) 라이선스를 사용하는 경우, 라이선스 유형 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스와 인스턴스 유형을 선택할 수 있습니다.

3. 인스턴스 유형을 선택하고, 변경 사항의 의미를 이해했음을 확인하는 확인란을 선택한 다음 *변경*을 클릭합니다.

결과

Cloud Volumes ONTAP 새로운 구성으로 재부팅됩니다.

여러 **AWS AZ**에서 **Cloud Volumes ONTAP HA** 쌍에 대한 경로 테이블 수정

여러 AWS 가용성 영역(AZ)에 배포된 HA 쌍에 대한 플로팅 IP 주소에 대한 경로를 포함하는 AWS 경로 테이블을 수정할 수 있습니다. AWS에서 새로운 NFS 또는 CIFS 클라이언트가 HA 쌍에 액세스해야 하는 경우 이 작업을 수행할 수 있습니다.

단계

1. 시스템 페이지에서 시스템을 선택하세요.
2. 개요 탭에서 기능 패널을 클릭한 다음 경로 테이블 옆에 있는 연필 아이콘을 클릭합니다.
3. 선택한 경로 테이블 목록을 수정한 다음 *저장*을 클릭합니다.

결과

NetApp Console AWS 요청을 보내 경로 테이블을 수정합니다.

Azure 관리

Cloud Volumes ONTAP 에 대한 **Azure VM** 유형 변경

Microsoft Azure에서 Cloud Volumes ONTAP 시작하면 여러 VM 유형 중에서 선택할 수 있습니다. 필요에 따라 VM 유형이 너무 크거나 작다고 판단되면 언제든지 VM 유형을 변경할 수 있습니다.

이 작업에 관하여

- Cloud Volumes ONTAP HA 쌍에서 자동 반환 기능을 활성화해야 합니다(이는 기본 설정입니다). 그렇지 않으면 작업이 실패합니다.

  "ONTAP 9 설명서: 자동 반환 구성을 위한 명령"

- VM 유형을 변경하면 Microsoft Azure 서비스 요금에 영향을 미칠 수 있습니다.
- 이 작업은 Cloud Volumes ONTAP 다시 시작합니다.

  단일 노드 시스템의 경우 I/O가 중단됩니다.

  HA 쌍의 경우 변경은 중단되지 않습니다. HA 쌍은 계속해서 데이터를 제공합니다.

  NetApp Console 인수를 시작하고 반환을 기다리는 방식으로 한 번에 한 노드씩 변경합니다. NetApp의 품질 보증 팀은 이 프로세스 동안 파일 쓰기와 읽기를 모두 테스트했으며 클라이언트 측에서 아무런 문제도 발견하지 못했습니다. 연결이 변경됨에 따라 I/O 수준에서 일부 재시도가 관찰되었지만 애플리케이션 계층은 NFS/CIFS 연결의 재배선을 극복했습니다.

단계

1. 시스템 페이지에서 시스템을 선택하세요.
2. 개요 탭에서 기능 패널을 클릭한 다음 **VM** 유형 옆에 있는 연필 아이콘을 클릭합니다.

노드 기반 사용량 기반(PAYGO) 라이선스를 사용하는 경우, 라이선스 유형 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스와 VM 유형을 선택할 수 있습니다.

3. VM 유형을 선택하고, 변경 사항의 의미를 이해했음을 확인하는 확인란을 선택한 다음 *변경*을 클릭합니다.

결과

Cloud Volumes ONTAP 새로운 구성으로 재부팅됩니다.

Azure에서 Cloud Volumes ONTAP HA 쌍에 대한 CIFS 잠금 재정의

조직 또는 계정 관리자는 NetApp Console 에서 Azure 유지 관리 이벤트 중에 Cloud Volumes ONTAP 저장소 반환 문제를 방지하는 설정을 활성화할 수 있습니다. 이 설정을 활성화하면 Cloud Volumes ONTAP CIFS 잠금을 거부하고 활성 CIFS 세션을 재설정합니다.

이 작업에 관하여

Microsoft Azure는 가상 머신에 대한 정기적인 유지 관리 이벤트를 예약합니다. Cloud Volumes ONTAP HA 쌍에서 유지 관리 이벤트가 발생하면 HA 쌍이 스토리지 인수를 시작합니다. 이 유지 관리 이벤트 중에 활성 CIFS 세션이 있는 경우 CIFS 파일에 대한 잠금으로 인해 저장소 반환이 방해받을 수 있습니다.

이 설정을 활성화하면 Cloud Volumes ONTAP 이 잠금을 거부하고 활성 CIFS 세션을 재설정합니다. 결과적으로 HA 쌍은 이러한 유지 관리 이벤트 중에 스토리지 반환을 완료할 수 있습니다.

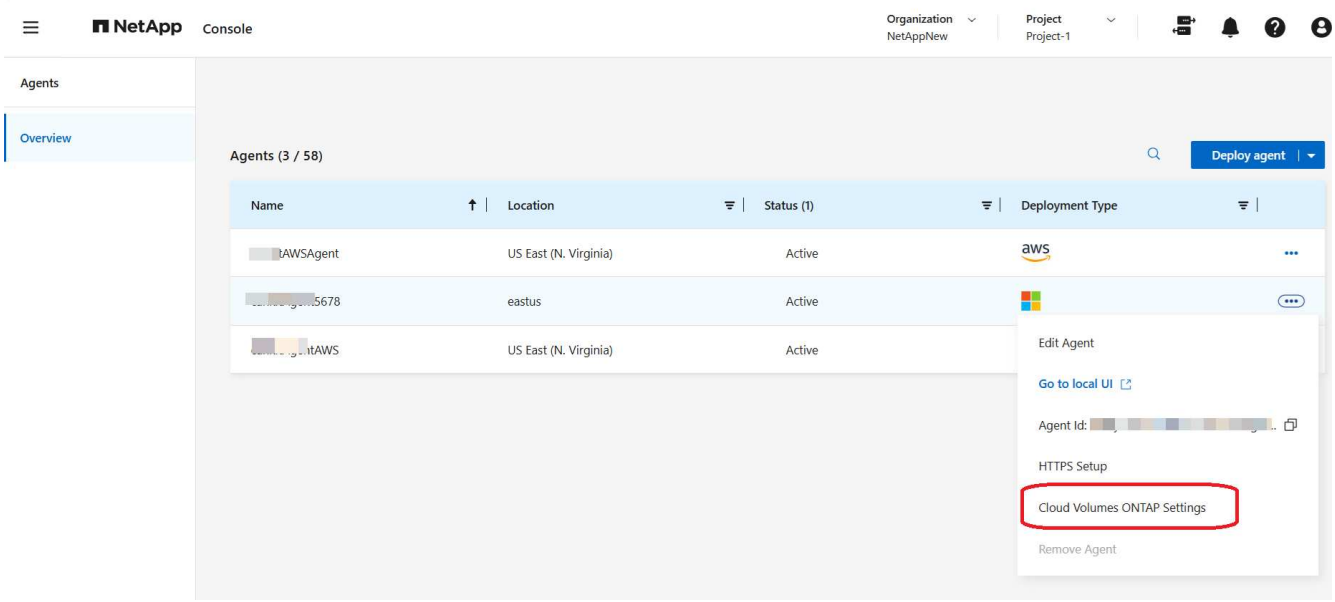
이 프로세스는 CIFS 클라이언트에 방해가 될 수 있습니다. CIFS 클라이언트에서 커밋되지 않은 데이터는 손실될 수 있습니다.

시작하기 전에

콘솔 설정을 변경하려면 먼저 콘솔 에이전트를 만들어야 합니다. "방법을 알아보세요" .

단계

1. 왼쪽 탐색 창에서 *관리 > 에이전트*로 이동합니다.
2. 클릭 ••• Cloud Volumes ONTAP 시스템을 관리하는 콘솔 에이전트의 아이콘입니다.
3. * Cloud Volumes ONTAP 설정*을 선택합니다.



4. *Azure*에서 *Azure HA 시스템에 대한 Azure CIFS 잠금*을 클릭합니다.
5. 해당 기능을 활성화하려면 확인란을 클릭한 다음 *저장*을 클릭하세요.

Cloud Volumes ONTAP 시스템에 **Azure Private Link** 또는 서비스 엔드포인트 사용

Cloud Volumes ONTAP 연결된 스토리지 계정에 연결하기 위해 Azure Private Link를 사용합니다. 필요한 경우 Azure Private Links를 비활성화하고 대신 서비스 엔드포인트를 사용할 수 있습니다.

개요

기본적으로 NetApp Console Cloud Volumes ONTAP 과 연결된 스토리지 계정 간의 연결을 위해 Azure Private Link를 활성화합니다. Azure Private Link는 Azure의 엔드포인트 간 연결을 보호하고 성능 이점을 제공합니다.

필요한 경우 Azure Private Link 대신 서비스 엔드포인트를 사용하도록 Cloud Volumes ONTAP 구성할 수 있습니다.

두 구성 모두에서 콘솔은 항상 Cloud Volumes ONTAP 과 스토리지 계정 간 연결에 대한 네트워크 액세스를 제한합니다. 네트워크 액세스는 Cloud Volumes ONTAP 배포된 VNet과 콘솔 에이전트가 배포된 VNet으로 제한됩니다.

Azure Private Links를 비활성화하고 대신 서비스 엔드포인트를 사용하세요.

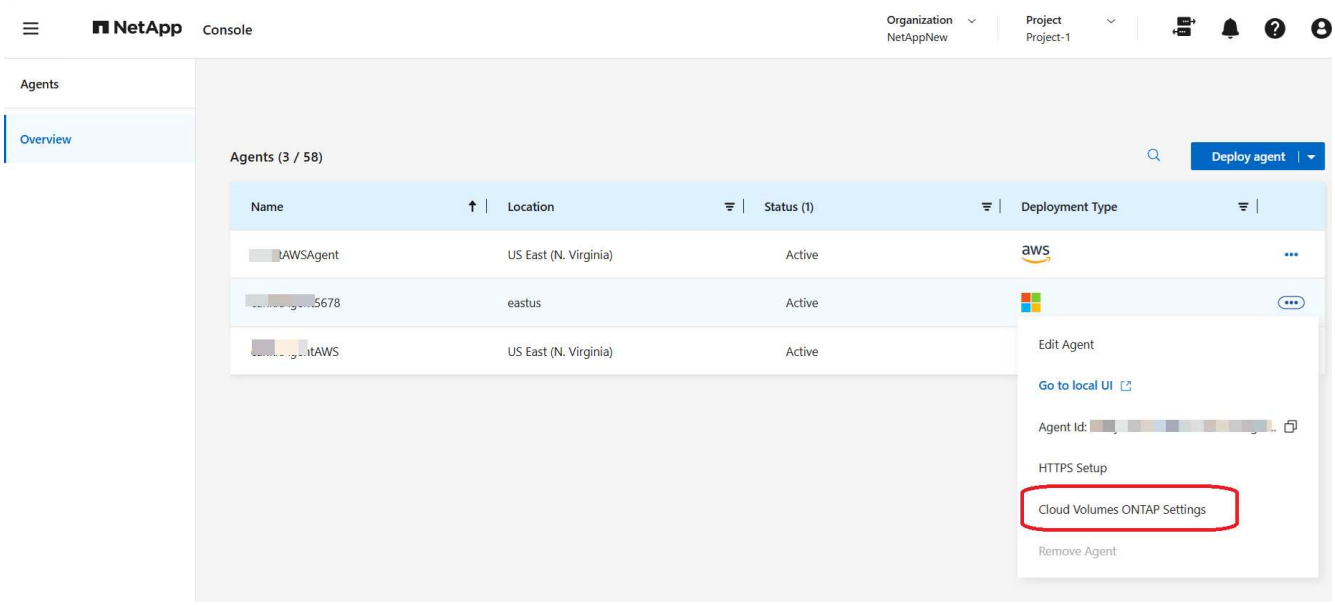
비즈니스에 필요한 경우 콘솔에서 설정을 변경하여 Azure Private Link 대신 서비스 엔드포인트를 사용하도록 Cloud Volumes ONTAP 구성할 수 있습니다. 이 설정을 변경하면 새로 만든 Cloud Volumes ONTAP 시스템에 적용됩니다. 서비스 엔드포인트는 다음에서만 지원됩니다."Azure 지역 쌍" 콘솔 에이전트와 Cloud Volumes ONTAP VNet 사이.

콘솔 에이전트는 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 지역이나 "Azure 지역 쌍" Cloud Volumes ONTAP 시스템용.

단계

1. 왼쪽 탐색 창에서 *관리 > 에이전트*로 이동합니다.
2. 클릭 ••• Cloud Volumes ONTAP 시스템을 관리하는 콘솔 에이전트의 아이콘입니다.

3. * Cloud Volumes ONTAP 설정*을 선택합니다.



4. *Azure*에서 *Azure Private Link 사용*을 클릭합니다.
5. Cloud Volumes ONTAP 과 스토리지 계정 간의 개인 링크 연결을 선택 해제합니다.
6. *저장*을 클릭하세요.

당신이 완료한 후

Azure Private Links를 비활성화하고 콘솔 에이전트가 프록시 서버를 사용하는 경우 직접 API 트래픽을 활성화해야 합니다.

"콘솔 에이전트에서 직접 API 트래픽을 활성화하는 방법을 알아보세요."

Azure Private Links로 작업

대부분의 경우 Cloud Volumes ONTAP 사용하여 Azure Private Link를 설정하는 데 필요한 작업은 없습니다. 콘솔은 Azure Private Links를 관리합니다. 하지만 기존 Azure Private DNS 영역을 사용하는 경우 구성 파일을 편집해야 합니다.

사용자 정의 **DNS**에 대한 요구 사항

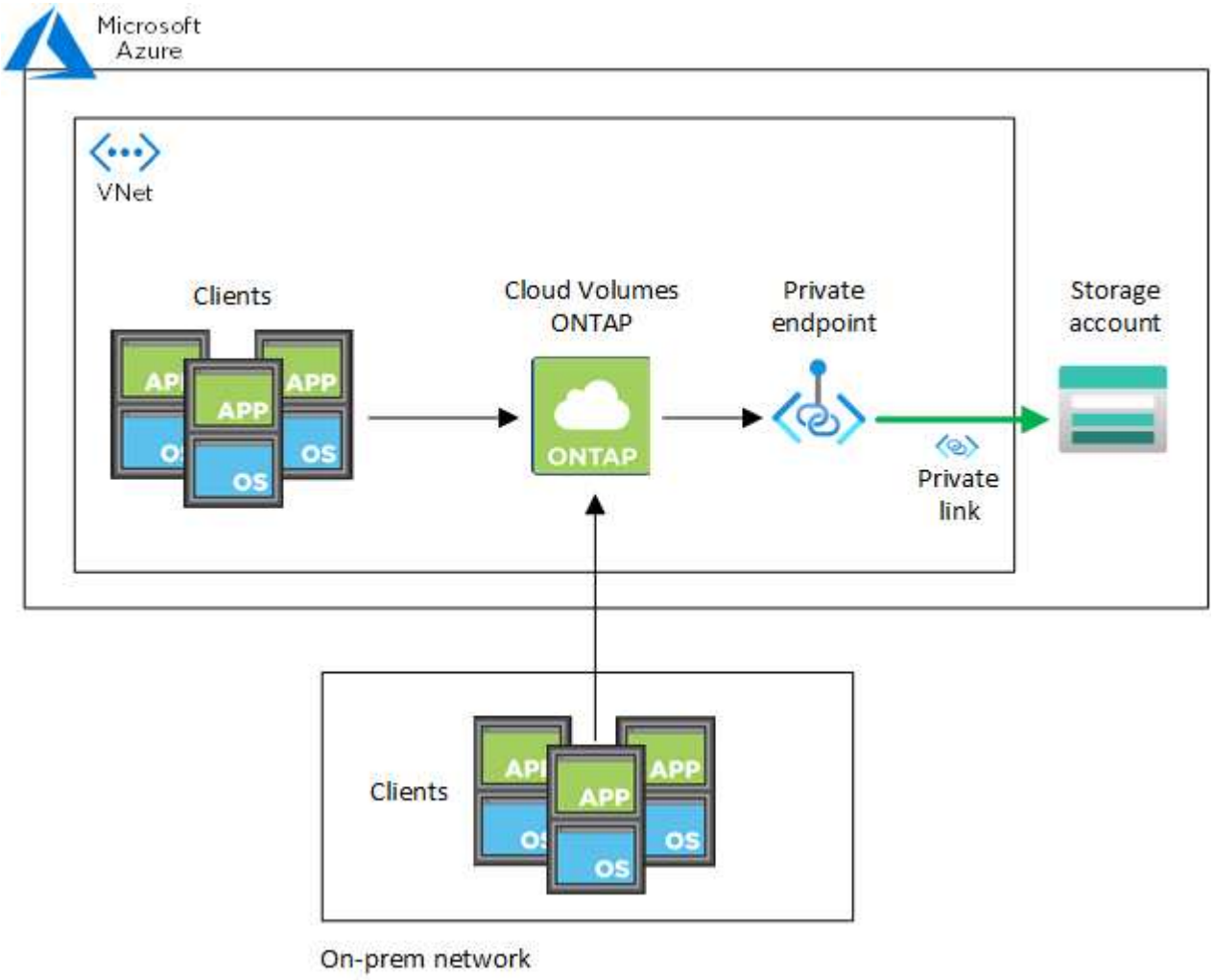
선택적으로 사용자 지정 DNS를 사용하는 경우 사용자 지정 DNS 서버에서 Azure 개인 DNS 영역에 대한 조건부 전달자를 만들어야 합니다. 자세한 내용은 다음을 참조하세요."DNS 전달자 사용에 대한 Azure 설명서" .

Private Link 연결 작동 방식

콘솔이 Azure에 Cloud Volumes ONTAP 배포하면 리소스 그룹에 개인 엔드포인트가 생성됩니다. 개인 엔드포인트는 Cloud Volumes ONTAP 의 스토리지 계정과 연결됩니다. 결과적으로 Cloud Volumes ONTAP 스토리지에 대한 액세스는 Microsoft 백본 네트워크를 통해 이루어집니다.

클라이언트가 Cloud Volumes ONTAP 과 동일한 VNet에 있거나, 피어링된 VNet에 있거나, VNet에 대한 개인 VPN이나 ExpressRoute 연결을 사용할 때 온프레미스 네트워크에 있는 경우 클라이언트 액세스는 개인 링크를 통해 이루어집니다.

다음은 동일한 VNet 내부와 개인 VPN 또는 ExpressRoute 연결이 있는 온프레미스 네트워크에서 개인 링크를 통해 클라이언트 액세스를 보여주는 예입니다.



콘솔 에이전트와 Cloud Volumes ONTAP 시스템이 서로 다른 VNet에 배포된 경우 콘솔 에이전트가 배포된 VNet과 Cloud Volumes ONTAP 시스템이 배포된 VNet 간에 VNet 피어링을 설정해야 합니다.

Azure Private DNS에 대한 세부 정보를 제공하세요.

당신이 사용하는 경우 "Azure 프라이빗 DNS" 그러면 각 콘솔 에이전트에서 구성 파일을 수정해야 합니다. 그렇지 않으면 콘솔은 Cloud Volumes ONTAP 과 연결된 스토리지 계정 간에 Azure Private Link 연결을 설정할 수 없습니다.

DNS 이름은 Azure DNS 명명 요구 사항과 일치해야 합니다. "Azure 설명서에 표시된 대로" .

단계

1. 콘솔 에이전트 호스트에 SSH를 실행하고 로그인합니다.
2. 로 이동합니다 `/opt/application/netapp/cloudmanager/docker_occm/data` 예배 규칙서.
3. 편집하다 `app.conf` 추가하여 `user-private-dns-zone-settings` 다음 키워드-값 쌍을 포함하는 매개변수:

```
"user-private-dns-zone-settings" : {
   "resource-group" : "<resource group name of the DNS zone>",
   "subscription" : "<subscription ID>",
   "use-existing" : true,
   "create-private-dns-zone-link" : true
}
```

그만큼 `subscription` 키워드는 개인 DNS 영역이 콘솔 에이전트와 다른 구독에 있는 경우에만 필요합니다.

4. 파일을 저장하고 콘솔 에이전트에서 로그오프합니다.

   재부팅이 필요하지 않습니다.

실패 시 롤백 활성화

콘솔이 특정 작업의 일부로 Azure Private Link를 만들지 못하면 Azure Private Link 연결 없이 작업을 완료합니다. 이는 새로운 시스템(단일 노드 또는 HA 쌍)을 생성할 때 또는 HA 쌍에서 다음 작업이 발생할 때 발생할 수 있습니다. 새로운 집계 생성, 기존 집계에 디스크 추가 또는 32TiB를 초과할 때 새로운 스토리지 계정 생성.

콘솔에서 Azure Private Link를 만들지 못하는 경우 롤백을 활성화하여 이 기본 동작을 변경할 수 있습니다. 이를 통해 회사의 보안 규정을 완벽하게 준수하는 데 도움이 될 수 있습니다.

롤백을 활성화하면 콘솔에서 작업이 중지되고 작업의 일부로 생성된 모든 리소스가 롤백됩니다.

API를 통해 롤백을 활성화하거나 app.conf 파일을 업데이트할 수 있습니다.

API를 통한 롤백 활성화

단계

1. 사용하다 `PUT /occm/config` 다음 요청 본문을 포함하는 API 호출:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

app.conf를 업데이트하여 롤백을 활성화합니다

단계

1. 콘솔 에이전트 호스트에 SSH를 실행하고 로그인합니다.
2. 다음 디렉토리로 이동합니다: /opt/application/netapp/cloudmanager/docker_occm/data
3. 다음 매개변수와 값을 추가하여 app.conf를 편집합니다.

```
 "rollback-on-private-link-failure": true
. 파일을 저장하고 콘솔 에이전트에서 로그오프합니다.
```

재부팅이 필요하지 않습니다.

Azure 콘솔에서 Cloud Volumes ONTAP 대한 Azure 리소스 그룹 이동

Cloud Volumes ONTAP Azure 리소스 그룹 이동을 지원하지만 워크플로는 Azure 콘솔에서만 발생합니다.

동일한 Azure 구독 내에서 Azure의 한 리소스 그룹에서 다른 리소스 그룹으로 Cloud Volumes ONTAP 시스템을 이동할 수 있습니다. 서로 다른 Azure 구독 간에 리소스 그룹을 이동하는 것은 지원되지 않습니다.

단계

1. Cloud Volumes ONTAP 시스템을 제거합니다. "Cloud Volumes ONTAP 시스템 제거" .
2. Azure 콘솔에서 리소스 그룹 이동을 실행합니다.

   이동을 완료하려면 다음을 참조하세요."Microsoft Azure 설명서에서 리소스를 새 리소스 그룹 또는 구독으로 이동" .
3. 시스템 페이지에서 시스템을 알아보세요.
4. 시스템 정보에서 새로운 리소스 그룹을 찾으세요.

결과

시스템과 해당 리소스(VM, 디스크, 스토리지 계정, 네트워크 인터페이스, 스냅샷)는 새 리소스 그룹에 있습니다.

Azure에서 SnapMirror 트래픽 분리

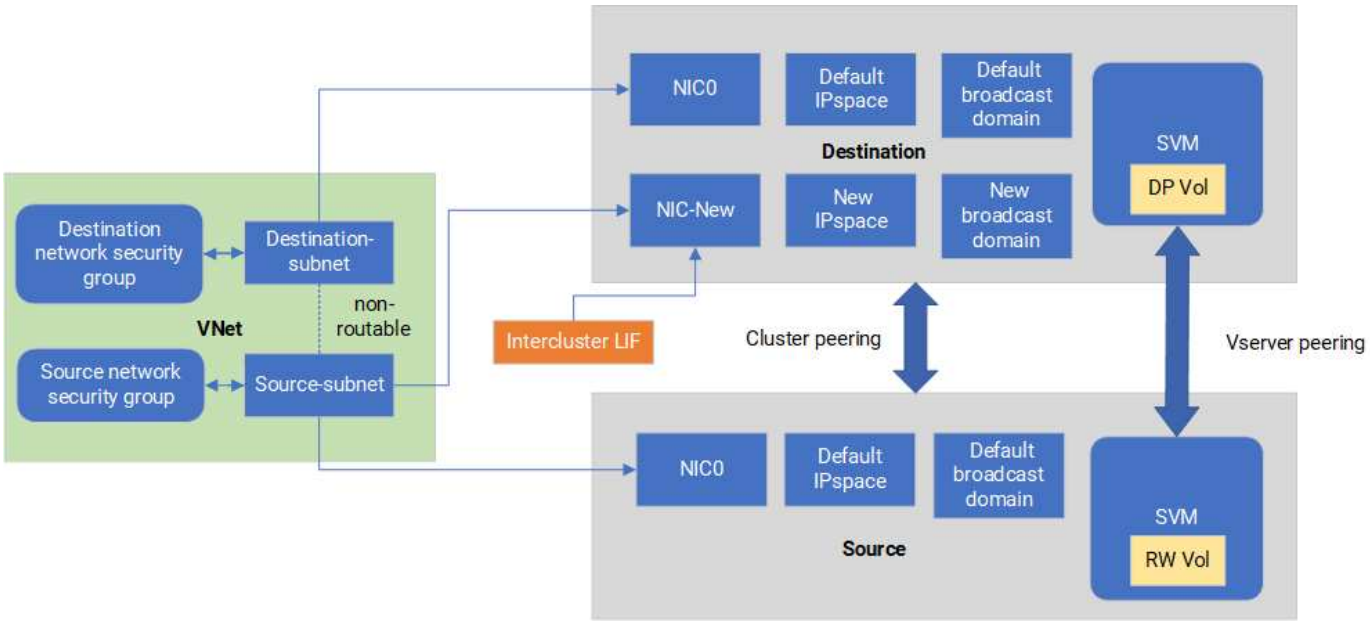
Azure의 Cloud Volumes ONTAP 사용하면 SnapMirror 복제 트래픽을 데이터 및 관리 트래픽에서 분리할 수 있습니다. SnapMirror 복제 트래픽을 데이터 트래픽에서 분리하려면 새 네트워크 인터페이스 카드(NIC), 연관된 클러스터 간 LIF 및 라우팅이 불가능한 서브넷을 추가합니다.

Azure의 SnapMirror 트래픽 분리에 관하여

기본적으로 NetApp Console 동일한 서브넷의 Cloud Volumes ONTAP 배포에 있는 모든 NIC와 LIF를 구성합니다. 이러한 구성에서는 SnapMirror 복제 트래픽과 데이터 및 관리 트래픽이 동일한 서브넷을 사용합니다. SnapMirror 트래픽을 분리하면 데이터 및 관리 트래픽에 사용되는 기존 서브넷으로 라우팅할 수 없는 추가 서브넷을 활용할 수 있습니다.

그림 **1**

다음 다이어그램은 단일 노드 배포에서 추가 NIC, 연관된 클러스터 간 LIF 및 라우팅 불가능한 서브넷을 사용하여 SnapMirror 복제 트래픽을 분리하는 방식을 보여줍니다. HA 쌍 배포는 약간 다릅니다.



시작하기 전에

다음 고려 사항을 검토하세요.

- SnapMirror 트래픽 분리를 위해 Cloud Volumes ONTAP 단일 노드 또는 HA 쌍 배포(VM 인스턴스)에 단일 NIC만 추가할 수 있습니다.
- 새로운 NIC를 추가하려면 배포하는 VM 인스턴스 유형에 사용되지 않는 NIC가 있어야 합니다.
- 소스 및 대상 클러스터는 동일한 가상 네트워크(VNet)에 액세스할 수 있어야 합니다. 대상 클러스터는 Azure의 Cloud Volumes ONTAP 시스템입니다. 소스 클러스터는 Azure의 Cloud Volumes ONTAP 시스템이나 ONTAP 시스템이 될 수 있습니다.

1단계**:** 추가 **NIC**를 생성하고 대상 **VM**에 연결합니다**.**

이 섹션에서는 추가 NIC를 생성하고 대상 VM에 연결하는 방법에 대한 지침을 제공합니다. 대상 VM은 Azure의 Cloud Volumes ONTAP 에 있는 단일 노드 또는 HA 쌍 시스템으로, 여기에 추가 NIC를 설정하려는 것입니다.

단계

1. ONTAP CLI에서 노드를 중지합니다.

```
dest::> halt -node <dest_node-vm>
```

2. Azure Portal에서 VM(노드) 상태가 중지되었는지 확인하세요.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Azure Cloud Shell의 Bash 환경을 사용하여 노드를 중지합니다.
   a. 노드를 중지합니다.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. 노드의 할당을 해제합니다.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. 두 서브넷(소스 클러스터 서브넷과 대상 클러스터 서브넷)이 서로 라우팅되지 않도록 네트워크 보안 그룹 규칙을 구성합니다.

a. 대상 VM에 새 NIC를 만듭니다.

b. 소스 클러스터 서브넷의 서브넷 ID를 찾습니다.

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet -name <vnet> --query id
```

c. 소스 클러스터 서브넷의 서브넷 ID를 사용하여 대상 VM에 새 NIC를 만듭니다. 여기에 새 NIC의 이름을 입력합니다.

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

d. 개인IP주소를 저장합니다. 이 IP 주소 <new_added_nic_primary_addr>는 클러스터 간 LIF를 생성하는 데 사용됩니다.브로드캐스트 도메인, 새 NIC에 대한 클러스터 간 LIF .

5. 새 NIC를 VM에 연결합니다.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. VM(노드)을 시작합니다.

```
az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
```

7. Azure Portal에서 *네트워킹*으로 이동하여 새 NIC(예: nic-new)가 있는지, 가속 네트워킹이 활성화되어 있는지 확인합니다.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

HA 쌍 배포의 경우 파트너 노드에 대해 단계를 반복합니다.

2단계: 새 NIC에 대한 새 IP 공간, 브로드캐스트 도메인 및 클러스터 간 LIF 만들기

클러스터 간 LIF를 위한 별도의 IP 공간은 클러스터 간 복제를 위한 네트워킹 기능 간의 논리적 분리를 제공합니다.

다음 단계에서는 ONTAP CLI를 사용하세요.

단계

1. 새로운 IPspace(new_ipspace)를 생성합니다.

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. 새로운 IPspace(new_ipspace)에 브로드캐스트 도메인을 만들고 nic-new 포트를 추가합니다.

```
dest::> network port show
```

3. 단일 노드 시스템의 경우 새로 추가된 포트는 _e0b_입니다. 관리형 디스크를 사용하는 HA 페어 배포의 경우 새로 추가된 포트는 _e0d_입니다. 페이지 블롭을 사용하는 HA 페어 배포의 경우 새로 추가된 포트는 _e0e_입니다. VM 이름이 아닌 노드 이름을 사용하십시오. `node show`을 실행하여 노드 이름을 확인할 수 있습니다.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. 새로운 브로드캐스트 도메인(new_bd)과 새로운 NIC(nic-new)에 클러스터 간 LIF를 만듭니다.

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. 새로운 클러스터 간 LIF 생성을 확인합니다.

```
dest::> net int show
```

HA 쌍 배포의 경우 파트너 노드에 대해 단계를 반복합니다.

3단계: 소스 시스템과 대상 시스템 간 클러스터 피어링 확인

이 섹션에서는 소스 시스템과 대상 시스템 간의 피어링을 확인하는 방법에 대한 지침을 제공합니다.

다음 단계에서는 ONTAP CLI를 사용하세요.

단계

1. 대상 클러스터의 클러스터 간 LIF가 소스 클러스터의 클러스터 간 LIF를 ping할 수 있는지 확인합니다. 대상 클러스터가 이 명령을 실행하므로 대상 IP 주소는 소스의 클러스터 간 LIF IP 주소입니다.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. 소스 클러스터의 클러스터 간 LIF가 대상 클러스터의 클러스터 간 LIF를 ping할 수 있는지 확인합니다. 목적지는 목적지에 생성된 새로운 NIC의 IP 주소입니다.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

HA 쌍 배포의 경우 파트너 노드에 대해 단계를 반복합니다.

4단계: 소스 시스템과 대상 시스템 간 SVM 피어링 생성

이 섹션에서는 소스 시스템과 대상 시스템 간에 SVM 피어링을 생성하는 방법에 대한 지침을 제공합니다.

다음 단계에서는 ONTAP CLI를 사용하세요.

단계

1. 소스 클러스터 간 LIF IP 주소를 사용하여 대상에서 클러스터 피어링을 생성합니다. `-peer-addrs` . HA 쌍의 경우 두 노드의 소스 클러스터 간 LIF IP 주소를 다음과 같이 나열합니다. `-peer-addrs` .

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. 암호를 입력하고 확인하세요.
3. 대상 클러스터 LIF IP 주소를 사용하여 소스에서 클러스터 피어링을 생성합니다. `peer-addrs` . HA 쌍의 경우 두 노드 모두에 대한 대상 클러스터 간 LIF IP 주소를 다음과 같이 나열합니다. `-peer-addrs` .

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. 암호를 입력하고 확인하세요.
5. 클러스터가 피어링되었는지 확인하세요.

```
src::> cluster peer show
```

   피어링이 성공하면 가용성 필드에 *사용 가능*이 표시됩니다.

6. 목적지에 SVM 피어링을 생성합니다. 소스 SVM과 대상 SVM은 모두 데이터 SVM이어야 합니다.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. SVM 피어링을 허용합니다.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. SVM이 피어링되었는지 확인하세요.

```
dest::> vserver peer show
```

피어 스테이트 쇼*`peered` * 및 피어링 애플리케이션이 표시됩니다.*`snapmirror` *.

5단계: 소스 시스템과 대상 시스템 간에 SnapMirror 복제 관계 생성

이 섹션에서는 소스 시스템과 대상 시스템 간에 SnapMirror 복제 관계를 만드는 방법에 대한 지침을 제공합니다.

기존 SnapMirror 복제 관계를 이동하려면 새 SnapMirror 복제 관계를 만들기 전에 먼저 기존 SnapMirror 복제 관계를 해제해야 합니다.

다음 단계에서는 ONTAP CLI를 사용하세요.

단계

1. 대상 SVM에 데이터 보호 볼륨을 만듭니다.

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. SnapMirror 정책과 복제 일정을 포함하는 대상에 SnapMirror 복제 관계를 만듭니다.

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. 대상에서 SnapMirror 복제 관계를 초기화합니다.

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. ONTAP CLI에서 다음 명령을 실행하여 SnapMirror 관계 상태를 확인합니다.

```
dest::> snapmirror show
```

관계 상태는 다음과 같습니다. `Snapmirrored` 그리고 관계의 건강은 `true` .

5. 선택 사항: ONTAP CLI에서 다음 명령을 실행하여 SnapMirror 관계에 대한 작업 기록을 확인합니다.

```
dest::> snapmirror show-history
```

선택적으로 소스 및 대상 볼륨을 마운트하고, 소스에 파일을 쓰고, 볼륨이 대상에 복제되는지 확인할 수 있습니다.

Google Cloud 관리

Cloud Volumes ONTAP 에 대한 Google Cloud 머신 유형 변경

Google Cloud에서 Cloud Volumes ONTAP 실행하면 여러 가지 머신 유형 중에서 선택할 수 있습니다. 필요에 따라 인스턴스나 머신 유형이 너무 크거나 작다고 판단되면 언제든지 변경할 수 있습니다.

이 작업에 관하여

- Cloud Volumes ONTAP HA 쌍에서 자동 반환 기능을 활성화해야 합니다(이는 기본 설정입니다). 그렇지 않으면 작업이 실패합니다.

  "ONTAP 9 설명서: 자동 반환 구성을 위한 명령"

- 머신 유형을 변경하면 Google Cloud 서비스 요금에 영향을 미칠 수 있습니다.
- 이 작업은 Cloud Volumes ONTAP 다시 시작합니다.

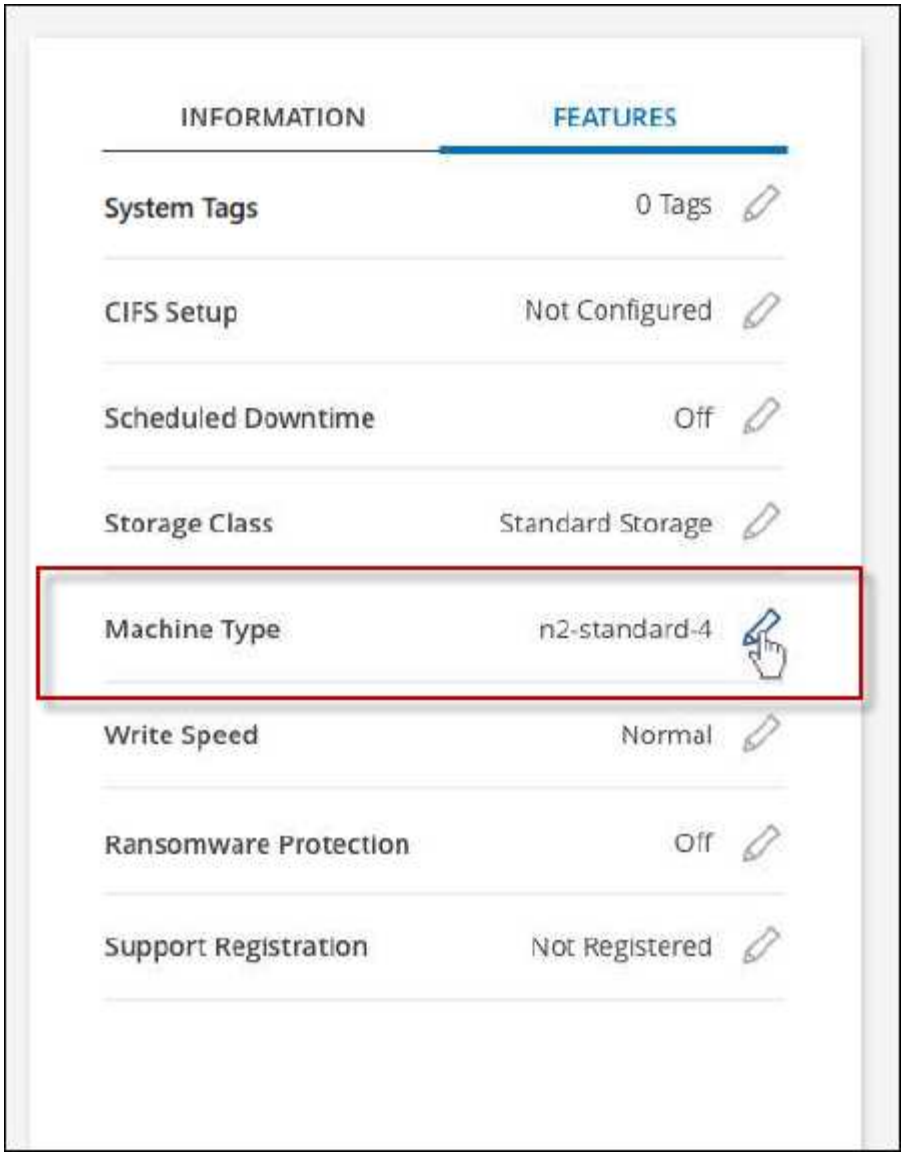
  단일 노드 시스템의 경우 I/O가 중단됩니다.

  HA 쌍의 경우 변경은 중단되지 않습니다. HA 쌍은 계속해서 데이터를 제공합니다.

NetApp Console 인수를 시작하고 반환을 기다리는 방식으로 한 번에 한 노드씩 변경합니다. NetApp의 품질 보증 팀은 이 프로세스 동안 파일 쓰기와 읽기를 모두 테스트했으며 클라이언트 측에서 아무런 문제도 발견하지 못했습니다. 연결이 변경됨에 따라 I/O 수준에서 일부 재시도가 관찰되었지만 애플리케이션 계층은 NFS/CIFS 연결의 재배선을 극복했습니다.

단계

1. 시스템 페이지에서 시스템을 선택하세요.
2. 개요 탭에서 기능 패널을 클릭한 다음 머신 유형 옆에 있는 연필 아이콘을 클릭합니다.



노드 기반 사용량 기반(PAYGO) 라이선스를 사용하는 경우, 라이선스 유형 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스와 머신 유형을 선택할 수 있습니다.

1. 머신 유형을 선택하고, 변경 사항의 의미를 이해했음을 확인하는 확인란을 선택한 다음 *변경*을 클릭합니다.

결과

Cloud Volumes ONTAP 새로운 구성으로 재부팅됩니다.

기존 **Cloud Volumes ONTAP** 배포를 **Infrastructure Manager**로 전환합니다**.**

2026년 2월 9일부터 Google Cloud에서 새로 배포하는 Cloud Volumes ONTAP은 Google Cloud Infrastructure Manager를 사용할 수 있습니다. Google은 Google Cloud Deployment Manager를 Infrastructure Manager로 대체할 예정입니다. 따라서 기존 Cloud Volumes ONTAP 배포를 Deployment Manager에서 Infrastructure Manager로 전환하려면 전환 도구를 수동으로 실행해야 합니다. 이 과정은 한 번만 수행하면 되며, 전환 후에는 시스템이 자동으로 Infrastructure Manager를 사용하게 됩니다.

이 작업에 관하여

전환 도구는 "NetApp 지원 사이트"에서 사용할 수 있으며 다음과 같은 산출물을 생성합니다.

- `conversion_output/deployment_name`에 저장된 Terraform 아티팩트.
- 변환 요약, 다음에 저장됨 `conversion_output/batch_summary_<deployment_name>_<timestamp>.json`.
- 디버그 로그는 `<gcp project number>-<region>-blueprint-config/<cvo name>` 디렉터리에 저장됩니다. 문제 해결을 위해 이 로그가 필요합니다. `<gcp project number>-<region>-blueprint-config` 버킷에는 Terraform 로그가 저장됩니다.

Infrastructure Manager를 사용하는 Cloud Volumes ONTAP 시스템은 데이터와 레코드를 Google Cloud Storage 버킷에 저장합니다. 이러한 버킷에 대해 추가 비용이 발생할 수 있지만 버킷이나 해당 콘텐츠를 편집하거나 삭제하지 마십시오.

- `gs://netapp-cvo-infrastructure-manager-<project id>`: 새로운 Cloud Volumes ONTAP 배포에 사용되는 ONTAP 버전 및 SVM Terraform 템플릿용입니다. 이 안에 `dm-to-im-convert` 버킷에는 Cloud Volumes ONTAP Terraform 파일이 들어 있습니다.
- `<gcp project number>-<region>-blueprint-config`: Google Cloud Terraform 아티팩트를 저장하는 데 사용됩니다.

시작하기 전에

- Cloud Volumes ONTAP 시스템이 9.16.1 이상인지 확인하십시오.
- Google Cloud Console에서 Cloud Volumes ONTAP 리소스 또는 해당 속성이 수동으로 편집되지 않았는지 확인하십시오.
- Google Cloud API가 사용 설정되어 있는지 확인하세요. "Google Cloud API 활성화"를 참조하십시오. 다른 API와 함께 Google Cloud Quotas API도 사용 설정해야 합니다.
- NetApp Console 에이전트의 서비스 계정에 필요한 모든 권한이 있는지 확인하십시오. 을 참조하십시오 "콘솔 에이전트에 대한 Google Cloud 권한".

  비공개 모드 배포의 경우 다음 추가 필수 조건을 충족해야 합니다.

  - 최신 Console 에이전트 버전을 사용하고 있는지 확인하십시오. NetApp Support Site에서 제품 설치 프로그램을 다운로드한 다음 호스트에 에이전트를 수동으로 설치하여 에이전트가 Infrastructure Manager API를 사용할 수 있도록 하십시오.
  - 도구를 비공개 모드로 실행하는 경우 다른 API와 함께 Cloud Build API도 활성화했는지 확인하십시오 "Google Cloud API 활성화".
  - 개인 모드 배포를 위해 네트워크 구성을 완료하고 작업자 풀을 생성했는지 확인하십시오. "프라이빗 모드 배포를 위한 Infrastructure Manager 구성"을(를) 참조하십시오.

- 변환 도구는 다음 도메인을 사용합니다. 네트워크에서 포트 443에서 활성화하십시오.

도메인	포트	규약	방향	목적
cloudresourcemanager.googleapis.com	443	TCP	EGRESS	프로젝트 검증

도메인	포트	규약	방향	목적
deploymentmanager.googleapis.com	443	TCP	EGRESS	배포 검색
config.googleapis.com	443	TCP	EGRESS	Infrastructure Manager API
storage.googleapis.com	443	TCP	EGRESS	GCS 버킷 작업
iam.googleapis.com	443	TCP	EGRESS	서비스 계정 검증
compute.googleapis.com	443	TCP	EGRESS	Google Cloud 및 Terraform Import 및 Plan에서 사용되는 Compute API 호출
cloudbuild.googleapis.com	443	TCP	EGRESS	비공개 모드에만 필요한 빌드 작업
openidconnect.googleapis.com	443	TCP	EGRESS	입증
oauth2.googleapis.com	443	TCP	EGRESS	OAuth2 토큰 교환
registry.terraform.io	443	TCP	EGRESS	Terraform 공급자 레지스트리
releases.hashicorp.com	443	TCP	EGRESS	Terraform 바이너리 다운로드
apt.releases.hashicorp.com	443	TCP	EGRESS	HashiCorp APT 저장소
us-central1-docker.pkg.dev	443	TCP	EGRESS	GCP Artifact Registry
metadata.google.internal	80	HTTP	내부	VM metadata 및 인증 토큰
pypi.org	443	TCP	EGRESS	Python 패키지 인덱스
files.pythonhosted.org	443	TCP	EGRESS	Python 패키지 다운로드
checkpoint-api.hashicorp.com	443	TCP	EGRESS	Terraform 버전 확인
download.docker.com	443	TCP	EGRESS	Docker APT 저장소
security.ubuntu.com	80/443	TCP	EGRESS	Ubuntu 보안 업데이트
*.gce.archive.ubuntu.com	80	TCP	EGRESS	Ubuntu 패키지 미러

도구를 실행하기 전에 다음 단계를 실행하십시오.

단계

1. 역할을 생성하고 서비스 계정에 연결합니다.
   a. 다음 권한을 가진 YAML 파일을 생성하십시오.

```
title: NetApp Dm TO IM Convert Solution
description: Permissions for the service account associated with the
VM where the tool will run.
stage: GA
includedPermissions:
- compute.addresses.get
- compute.disks.get
- compute.forwardingRules.get
- compute.healthChecks.get
- compute.instanceGroups.get
- compute.instances.get
- compute.regionBackendServices.get
- config.deployments.create
- config.deployments.get
- config.deployments.getLock
- config.deployments.lock
- config.deployments.unlock
- config.deployments.update
- config.deployments.delete
- config.deployments.updateState
- config.operations.get
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- iam.serviceAccounts.get
- storage.buckets.create
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.list
```

프라이빗 모드 배포에 대한 추가 권한 포함

도구를 비공개 모드로 실행하는 경우 YAML 파일에 `cloudbuild.workerpools.get` 권한도 추가해야 합니다.

   b. YAML 파일에 정의된 권한으로 Google Cloud에서 사용자 지정 역할을 생성합니다.

`gcloud iam roles create dmtoim_convert_tool_role --project=PROJECT_ID \ --file=YAML_FILE_PATH` 자세한 내용은 "사용자 지정 역할 생성 및 관리"를 참조하십시오.

c. VM을 생성하는 데 사용할 서비스 계정에 사용자 지정 역할을 연결합니다.

d. 이 서비스 계정에 `roles/iam.serviceAccountUser` 역할을 추가하세요. "서비스 계정 개요"을(를) 참조하십시오.

2. 다음 구성으로 VM을 생성합니다. 이 VM에서 도구를 실행합니다.
   - 머신 유형: Google Compute Engine 머신 유형 e2-medium
   - OS: 요구 사항에 따라 다음 이미지 중 하나를 선택합니다.
     - Ubuntu 25.10 AMD64 Minimal (이미지: ubuntu-minimal-2510-amd64)
     - SUSE Linux Enterprise Server 15 SP7 x86_64
   - 네트워킹: HTTP 및 HTTPS를 허용하는 방화벽
   - 디스크 크기: 20GB
   - 보안: 서비스 계정: 생성한 서비스 계정
   - 보안: 액세스 범위 - 각 API에 대해 설정된 액세스:
     - 클라우드 플랫폼: 활성화됨
     - Compute Engine: 읽기 전용
     - 스토리지: 읽기 전용(기본값)
     - Google Cloud Logging(이전 Stackdriver Logging) API: 쓰기 전용(기본값)
     - Stackdriver Monitoring(현재 Google Cloud Operations의 일부) API: 쓰기 전용(기본값)
     - 서비스 관리: 읽기 전용(기본값)
     - 서비스 제어: 활성화됨(기본값)
     - Google Cloud Trace(이전 Stackdriver Trace): 쓰기 전용(기본값)
3. SSH를 사용하여 새로 생성된 VM에 연결합니다: `gcloud compute ssh dmtoim-convert-executor-vm --zone <region where VM is deployed>`
4. NSS 자격 증명을 사용하여 "NetApp 지원 사이트"에서 변환 도구를 다운로드하십시오. `wget <download link from NetApp Support site>`
5. 다운로드한 TAR 파일의 압축을 풉니다. `unzip <downloaded file name>`

Ubuntu

1. 다음 필수 패키지를 다운로드하고 설치하십시오:
   - Docker: 28.2.2 build 28.2.2-0ubuntu1 이상
   - Terraform: 1.14.1 이상
   - Python: 3.13.7, python3-pip, python3 venv

   ```
   sudo apt-get update
   sudo apt-get install python3-pip python3-venv -y
   wget -O - https://apt.releases.hashicorp.com/gpg | sudo gpg
   --dearmor -o /usr/share/keyrings/hashicorp-archive-keyring.gpg
   echo "deb [arch=$(dpkg --print-architecture) signed-
   by=/usr/share/keyrings/hashicorp-archive-keyring.gpg]
   https://apt.releases.hashicorp.com noble main" | sudo tee
   /etc/apt/sources.list.d/hashicorp.list
   sudo apt update && sudo apt install terraform
   sudo apt-get install -y docker.io
   sudo systemctl start docker
   ```

   Google Cloud CLI `gcloud`가 VM에 사전 설치되어 있습니다.

SUSE Linux Enterprise Server

1. Python 설정: `sudo update-alternatives --install /usr/bin/python3 python3 /usr/bin/python3.11 2`
2. 패키지 설치를 위해 pip3를 설치하세요. `python3.11 -m ensurepip --upgrade`
3. Terraform 설치:

   ```
   wget
   https://releases.hashicorp.com/terraform/1.7.4/terraform_1.7.4_linux
   _amd64.zip
   unzip terraform_1.7.4_linux_amd64.zip
   sudo mv terraform /usr/local/bin/
   rm terraform_1.7.4_linux_amd64.zip
   ```

4. Google Cloud SDK(gcloud) 설치

   ```
   curl https://sdk.cloud.google.com | bash
   exec -l $SHELL
   ```

이 단계는 Ubuntu 및 SUSE Linux Enterprise Server 모두에서 변환 도구를 실행하는 데 적용됩니다.

단계

1. 현재 사용자를 Docker 그룹에 추가하여 해당 도구가 `sudo` 권한 없이 Docker를 사용할 수 있도록 합니다.

```
sudo usermod -aG docker $USER
newgrp docker
```

2. 변환 도구를 설치합니다.

```
cd <folder where you extracted the tool>
 ./install.sh
```

이렇게 하면 도구가 격리된 환경에 설치되고 `dmconvert-venv` 필요한 모든 소프트웨어 패키지가 설치되었는지 확인합니다.

3. 도구가 설치된 환경을 입력합니다. `source dmconvert-venv/bin/activate`
4. 변환 도구를 `non-sudo` 사용자로 실행합니다. Console 에이전트의 서비스 계정과 동일한 서비스 계정을 사용하고 서비스 계정에 모든 "Google Cloud Infrastructure Manager에 필요한 권한"이 있는지 확인합니다.

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent>
```

프라이빗 모드 배포에서 도구 실행

`--worker-pool` 매개변수를 지정하여 개인 모드 배포에서 도구를 실행하십시오. 작업자 풀 구성에 대해서는 xref:{relative_path}reference-networking-gcp.html#infrastructure-manager-configuration-for-private-mode-deployments["프라이빗 모드 배포를 위한 Infrastructure Manager 구성"]을 참조하십시오.

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent> \
--worker-pool=<worker pool name>
```

당신이 완료한 후

이 도구는 모든 Cloud Volumes ONTAP 시스템 및 SVM 세부 정보 목록을 표시합니다. 실행이 완료되면 변환된 모든 시스템의 상태를 확인할 수 있습니다. 변환된 각 시스템은 Google Console의 Infrastructure Manager에서 *<system-name-imdeploy>* 형식으로 표시되며, 이는 Console에서 이제 해당 Cloud Volumes ONTAP 시스템을 관리하기 위해 Infrastructure Manager API를 사용한다는 것을 나타냅니다.

변환 후 Google Cloud 콘솔에서 Deployment Manager의 배포 객체를 삭제하지 마세요. 이 배포 객체에는 변환된 시스템을 롤백하는 데 필요한 정보가 포함되어 있습니다.

변환을 되돌려야 하는 경우 동일한 VM을 사용해야 합니다. 모든 시스템을 변환했고 Deployment Manager로 되돌릴 필요가 없는 경우 VM을 삭제할 수 있습니다.

변환 롤백

변환을 계속 진행하지 않으려면 다음 단계를 따라 Deployment Manager로 되돌릴 수 있습니다.

단계

1. 동일한 도구를 실행하기 위해 생성한 VM에서 다음 명령을 실행합니다.

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent> \
--rollback
```

2. 롤백이 완료될 때까지 기다리세요.

관련 링크

- "NetApp Console Agent 4.2.0 릴리스 노트"
- "Google Cloud Infrastructure Manager에 필요한 권한"

System Manager를 사용하여 Cloud Volumes ONTAP 관리

Cloud Volumes ONTAP 의 고급 스토리지 관리 기능은 ONTAP 시스템과 함께 제공되는 관리 인터페이스인 ONTAP System Manager를 통해 제공됩니다. NetApp Console 에서 직접 System Manager에 액세스할 수 있습니다.

특징

콘솔에서 ONTAP 시스템 관리자를 사용하여 다양한 스토리지 관리 기능을 수행할 수 있습니다. 다음 목록에는 일부 기능이 포함되어 있지만, 전체 목록은 아닙니다.

- 고급 스토리지 관리: 일관성 그룹, 공유, Q트리, 할당량 및 스토리지 VM을 관리합니다.
- 볼륨 이동: "볼륨을 다른 집계로 이동합니다."
- 네트워킹 관리: IP 공간, 네트워크 인터페이스, 포트셋, 이더넷 포트를 관리합니다.
- FlexGroup 볼륨 관리: FlexGroup 볼륨은 System Manager를 통해서만 생성하고 관리할 수 있습니다. 콘솔은 FlexGroup 볼륨 생성을 지원하지 않습니다.
- 이벤트 및 작업: 이벤트 로그, 시스템 알림, 작업 및 감사 로그를 확인합니다.
- 고급 데이터 보호: 스토리지 VM, LUN 및 일관성 그룹을 보호합니다.
- 호스트 관리: SAN 이니시에이터 그룹과 NFS 클라이언트를 설정합니다.
- ONTAP S3 객체 스토리지 관리: Cloud Volumes ONTAP의 ONTAP S3 스토리지 관리 기능은 System Manager에서만 사용할 수 있으며 Console에서는 사용할 수 없습니다.

지원되는 구성

- ONTAP System Manager를 통한 고급 스토리지 관리 기능은 표준 클라우드 지역에서 Cloud Volumes ONTAP 9.10.0 이상에서 사용할 수 있습니다.
- GovCloud 지역이나 아웃바운드 인터넷 액세스가 없는 지역에서는 System Manager 통합이 지원되지 않습니다.

제한 사항

System Manager 인터페이스에 나타나는 몇 가지 기능은 Cloud Volumes ONTAP 에서 지원되지 않습니다.

- NetApp Cloud Tiering: Cloud Volumes ONTAP 클라우드 계층화를 지원하지 않습니다. 볼륨을 생성할 때 표준 보기에서 직접 개체 스토리지에 대한 데이터 계층화를 설정해야 합니다.
- 계층: System Manager에서는 집계 관리(로컬 계층 및 클라우드 계층 포함)가 지원되지 않습니다. 표준 보기에서 직접 집계를 관리해야 합니다.
- 펌웨어 업그레이드: Cloud Volumes ONTAP 시스템 관리자의 클러스터 **>** 설정 페이지에서 자동 펌웨어 업데이트를 지원하지 않습니다.
- 역할 기반 액세스 제어: System Manager의 역할 기반 액세스 제어는 지원되지 않습니다.

- SMB 지속적 가용성(CA): Cloud Volumes ONTAP 지원하지 않습니다. "지속적으로 이용 가능한 SMB 주식" 중단 없는 운영을 위해.

시스템 관리자에 액세스하기 위한 인증 구성

관리자는 콘솔에서 ONTAP System Manager에 액세스하는 사용자에 대한 인증을 활성화할 수 있습니다. ONTAP 사용자 역할에 따라 적절한 수준의 액세스 권한을 결정하고 필요에 따라 인증을 활성화하거나 비활성화할 수 있습니다. 인증을 활성화하면 사용자는 콘솔에서 System Manager에 액세스할 때마다 또는 페이지를 다시 로드할 때마다 ONTAP 사용자 자격 증명을 입력해야 합니다. 콘솔은 자격 증명을 내부적으로 저장하지 않기 때문입니다. 인증을 비활성화하면 사용자는 관리자 자격 증명을 사용하여 시스템 관리자에 액세스할 수 있습니다.

이 설정은 Cloud Volumes ONTAP 시스템과 관계없이 조직 또는 계정의 ONTAP 사용자에 대한 각 콘솔 에이전트에 적용됩니다.

필요한 권한

Cloud Volumes ONTAP 사용자 인증을 위한 콘솔 에이전트 설정을 수정하려면 조직 또는 계정 관리자 권한이 지정되어야 합니다.

단계

1. 왼쪽 탐색 창에서 *관리 > 에이전트*로 이동합니다.
2. 클릭 ••• 필요한 콘솔 에이전트의 아이콘을 클릭하고 *콘솔 에이전트 편집*을 선택합니다.
3. 사용자 자격 증명 강제 적용*에서 *활성화/비활성화 확인란을 선택합니다. 기본적으로 인증은 비활성화되어 있습니다.

   이 값을 *사용*으로 설정하면 인증이 재설정되고 이 변경 사항을 수용하기 위해 기존 워크플로를 수정해야 합니다.

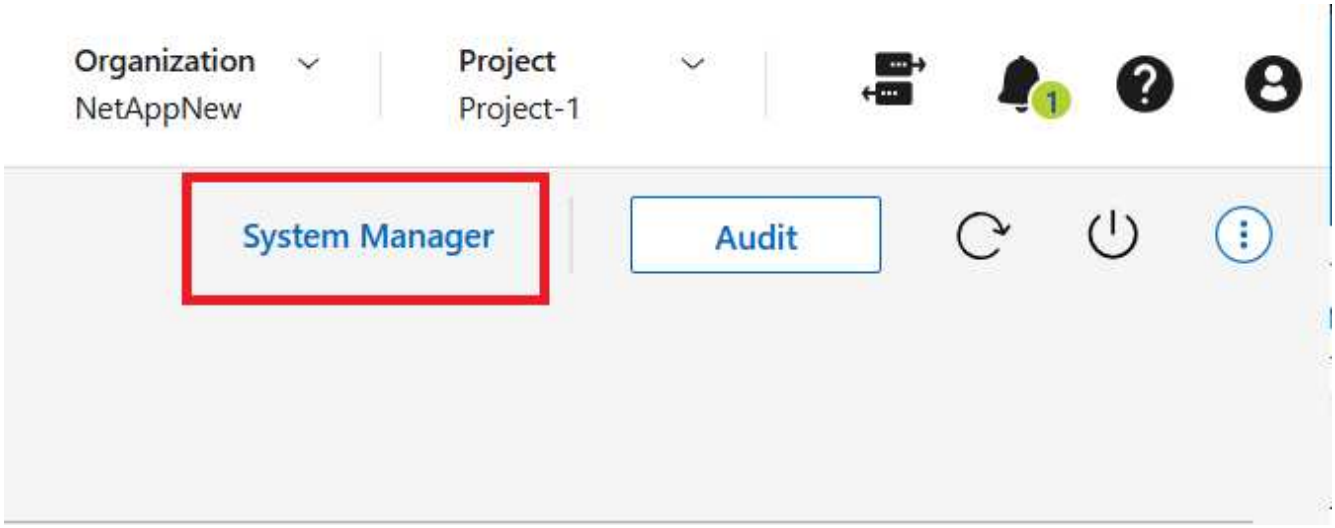
4. *저장*을 클릭하세요.

시스템 관리자 시작하기

Cloud Volumes ONTAP 시스템에서 ONTAP System Manager에 액세스할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 필요한 Cloud Volumes ONTAP 시스템을 두 번 클릭합니다.
3. *시스템 관리자*를 클릭하세요.



4. 메시지가 표시되면 ONTAP 사용자 자격 증명을 입력하고 *로그인*을 클릭합니다.
5. 확인 메시지가 나타나면, 내용을 읽고 *닫기*를 클릭하세요.

System Manager를 사용하여 Cloud Volumes ONTAP 시스템을 관리하세요. *돌아가기*를 클릭하면 콘솔로 돌아갈 수 있습니다.

시스템 관리자 사용에 대한 도움말

Cloud Volumes ONTAP 과 함께 System Manager를 사용하는 데 도움이 필요한 경우 다음을 참조할 수 있습니다. "ONTAP 문서" 단계별 지침을 확인하세요. 도움이 될 만한 몇 가지 ONTAP 문서 링크는 다음과 같습니다.

- "ONTAP 역할, 애플리케이션 및 인증"
- "시스템 관리자를 사용하여 클러스터에 액세스합니다." .
- "볼륨 및 LUN 관리"
- "네트워크 관리"
- "데이터 보호"
- "지속적으로 사용 가능한 SMB 공유 생성"

CLI에서 Cloud Volumes ONTAP 관리

Cloud Volumes ONTAP CLI를 사용하면 모든 관리 명령을 실행할 수 있으며 고급 작업을 수행하거나 CLI를 사용하는 것이 더 편리한 경우에 좋은 선택입니다. SSH(Secure Shell)를 사용하여 CLI에 연결할 수 있습니다.

시작하기 전에

SSH를 사용하여 Cloud Volumes ONTAP 에 연결하는 호스트에는 Cloud Volumes ONTAP 에 대한 네트워크 연결이 있어야 합니다. 예를 들어, 클라우드 공급자 네트워크에 있는 점프 호스트에서 SSH를 수행해야 할 수도 있습니다.

여러 AZ에 배포하는 경우 Cloud Volumes ONTAP HA 구성은 클러스터 관리 인터페이스에 부동 IP 주소를 사용하므로 외부 라우팅을 사용할 수 없습니다. 동일한 라우팅 도메인에 속한 호스트에서 연결해야 합니다.

단계

1. NetApp Console 에서 클러스터 관리 인터페이스의 IP 주소를 식별합니다.
   a. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
   b. 시스템 페이지에서 Cloud Volumes ONTAP 시스템을 선택합니다.
   c. 오른쪽 창에 나타나는 클러스터 관리 IP 주소를 복사합니다.
2. 관리자 계정을 사용하여 SSH를 사용하여 클러스터 관리 인터페이스 IP 주소에 연결합니다.

   예

   다음 이미지는 PuTTY를 사용하는 예를 보여줍니다.

3. 로그인 프롬프트에서 관리자 계정의 비밀번호를 입력하세요.

   예

```
Password: ********
COT2::>
```

시스템 상태 및 이벤트

Cloud Volumes ONTAP 에 대한 **AutoSupport** 설정 확인

AutoSupport 시스템 상태를 사전에 모니터링하고 NetApp 기술 지원팀에 메시지를 전송합니다. 기본적으로 AutoSupport 각 노드에서 HTTPS 전송 프로토콜을 사용하여 기술 지원팀에 메시지를 보낼 수 있도록 활성화되어 있습니다. AutoSupport 이러한 메시지를 보낼 수 있는지 확인하는 것이 가장 좋습니다.

유일하게 필요한 구성 단계는 Cloud Volumes ONTAP 아웃바운드 인터넷 연결이 있는지 확인하는 것입니다. 자세한 내용은 클라우드 제공업체의 네트워킹 요구 사항을 참조하세요.

AutoSupport 요구 사항

Cloud Volumes ONTAP 노드에는 NetApp AutoSupport 에 대한 아웃바운드 인터넷 액세스가 필요합니다. NetApp AutoSupport는 시스템 상태를 사전에 모니터링하고 NetApp 기술 지원팀에 메시지를 전송합니다.

라우팅 및 방화벽 정책은 Cloud Volumes ONTAP AutoSupport 메시지를 보낼 수 있도록 다음 엔드포인트에 대한 HTTPS 트래픽을 허용해야 합니다.

- \ https://mysupport.netapp.com/aods/asupmessage
- \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup

AutoSupport 메시지를 보내기 위한 아웃바운드 인터넷 연결이 불가능한 경우 NetApp Console Cloud Volumes ONTAP 시스템이 콘솔 에이전트를 프록시 서버로 사용하도록 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

Cloud Volumes ONTAP 에 대해 엄격한 아웃바운드 규칙을 정의한 경우 Cloud Volumes ONTAP 보안 그룹이 포트 3128을 통한 아웃바운드 연결을 허용하는지 확인해야 합니다.

HA 쌍을 사용하는 경우 HA 중재자는 아웃바운드 인터넷 액세스가 필요하지 않습니다.

아웃바운드 인터넷 접속이 가능한지 확인한 후 AutoSupport 메시지를 보낼 수 있는지 테스트할 수 있습니다. 지침은 다음을 참조하세요. "ONTAP 설명서: AutoSupport 설정" .

AutoSupport 구성 문제 해결

외부 연결이 불가능하고 콘솔에서 Cloud Volumes ONTAP 시스템을 콘솔 에이전트를 프록시 서버로 사용하도록 구성할 수 없는 경우, 시스템에서 AutoSupport 메시지를 보낼 수 없다는 알림이 콘솔에서 표시됩니다. 이 문제를 해결하려면 다음 단계를 따르십시오.

단계

1. ONTAP CLI를 사용하려면 SSH를 사용하여 Cloud Volumes ONTAP 시스템에 안전하게 연결하십시오.

   "Cloud Volumes ONTAP 에 SSH하는 방법 알아보기" .

2. AutoSupport 하위 시스템의 자세한 상태를 확인하십시오.

   ```
   autosupport check show-details
   ```

   응답은 다음과 같습니다.

```
    Category: smtp
          Component: mail-server
             Status: failed
             Detail: SMTP connectivity check failed for destination:
                     mailhost. Error: Could not resolve host -
'mailhost'
            Corrective Action: Check the hostname of the SMTP server

    Category: http-https
        Component: http-put-destination
            Status: ok
            Detail: Successfully connected to:
                    <https://support.netapp.com/put/AsupPut/>.

          Component: http-post-destination
             Status: ok
             Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

    Category: on-demand
          Component: ondemand-server
             Status: ok
             Detail: Successfully connected to:
                     https://support.netapp.com/aods/asupmessage.

    Category: configuration
            Component: configuration
                Status: ok
                Detail: No configuration issues found.
    5 entries were displayed.
```

http-https 카테고리의 상태가 다음과 같으면 `OK` 이는 AutoSupport 제대로 구성되어 메시지를 보낼 수 있음을 의미합니다.

3. 그렇지 않다면 각 Cloud Volumes ONTAP 노드의 프록시 URL을 확인하십시오.

   ```
   autosupport show -fields proxy-url
   ```

4. 프록시 URL 매개변수가 비어 있으면 Cloud Volumes ONTAP 구성하여 콘솔 에이전트를 프록시로 사용합니다.

   ```
   autosupport modify -proxy-url http://<console agent private ip>:3128
   ```

5. AutoSupport 상태를 다시 확인하십시오.

   ```
   autosupport check show-details
   ```

6. 상태가 여전히 실패로 표시되는 경우, Cloud Volumes ONTAP 과 콘솔 에이전트 간에 포트를 통해 연결이 제대로 되어 있는지 확인하십시오. `3128`.
7. 확인 후에도 상태가 여전히 실패로 표시되면 콘솔 에이전트에 SSH로 접속하십시오.

   "콘솔 에이전트를 위한 Linux VM 연결에 대해 자세히 알아보세요."

8. 가다 `/opt/application/netapp/cloudmanager/docker_occm/data/`.
9. 프록시 구성 파일을 엽니다. `squid.conf`. 파일의 구조는 다음과 같습니다.

```
        http_port 3128
        acl netapp_support dst support.netapp.com
        http_access allow netapp_support
        request_header_max_size 21 KB
        reply_header_max_size 21 KB
        http_access deny all
        httpd_suppress_version_string on
```

10. 파일에 Cloud Volumes ONTAP 시스템의 CIDR 블록에 대한 항목이 없는 경우 새 항목을 추가하고 액세스를 허용하십시오.

    `acl cvonet src <cidr>`

    `http_access allow cvonet`

    예를 들면 다음과 같습니다.

```
        http_port 3128
        acl netapp_support dst support.netapp.com
        acl cvonet src <cidr>
        http_access allow netapp_support
        http_access allow cvonet
        request_header_max_size 21 KB
        reply_header_max_size 21 KB
        http_access deny all
        httpd_suppress_version_string on
```

11. 설정 파일을 편집한 후 프록시 컨테이너를 다시 시작하십시오. `sudo`. 그런 다음 Docker 또는 Podman을 사용하는지에 따라 다음 명령을 실행하세요.

    Docker의 경우, 다음 명령을 실행하세요. `docker restart squid`.

    Podman을 사용 중이라면 다음 명령을 실행하세요. `podman restart squid`.

12. ONTAP CLI로 돌아가서 Cloud Volumes ONTAP AutoSupport 메시지를 보낼 수 있는지 확인하십시오.

    `autosupport check show-details`

관련 링크

- "AWS의 Cloud Volumes ONTAP 에 대한 네트워킹 요구 사항"
- "Azure에서 Cloud Volumes ONTAP 의 네트워킹 요구 사항"
- "Google Cloud에서 Cloud Volumes ONTAP 사용하기 위한 네트워킹 요구 사항"

Cloud Volumes ONTAP 시스템에 대한 EMS 구성

이벤트 관리 시스템(EMS)은 ONTAP 시스템에서 발생하는 이벤트에 대한 정보를 수집하고 표시합니다. 이벤트 알림을 받으려면 특정 이벤트 심각도에 대한 이벤트 대상(이메일 주소, SNMP 트랩 호스트 또는 시스템 로그 서버)과 이벤트 경로를 설정할 수 있습니다.

CLI를 사용하여 EMS를 구성할 수 있습니다. 지침은 다음을 참조하세요. "ONTAP 문서: EMS 구성 개요" .

개념

라이센스

Cloud Volumes ONTAP 라이선싱

Cloud Volumes ONTAP 에는 여러 가지 라이선싱 옵션이 제공됩니다. 각 옵션을 통해 귀하의 필요에 맞는 소비 모델을 선택할 수 있습니다.

라이센스 개요

신규 고객에게는 다음과 같은 라이선스 옵션이 제공됩니다.

용량 기반 라이선싱

NetApp 계정에서 여러 Cloud Volumes ONTAP 시스템에 대한 비용을 프로비저닝된 용량에 따라 지불합니다. 추가 클라우드 데이터 서비스를 구매할 수 있는 기능이 포함되어 있습니다. 용량 기반 라이선스의 소비 모델 또는 구매 옵션에 대한 자세한 내용은 다음을 참조하십시오."용량 기반 라이선스에 대해 자세히 알아보세요" .

Keystone 구독

고가용성(HA) 쌍에 대한 원활한 하이브리드 클라우드 환경을 제공하는, 사용량에 따라 비용을 지불하는 구독 기반 서비스입니다.

다음 섹션에서는 각 옵션에 대한 자세한 내용을 설명합니다.

라이선스가 없으면 라이선스 기능을 사용할 수 없습니다.

용량 기반 라이선싱

용량 기반 라이선싱 패키지를 사용하면 TiB 용량당 Cloud Volumes ONTAP 비용을 지불할 수 있습니다. 라이선스는 NetApp 계정과 연결되며, 라이선스를 통해 충분한 용량을 사용할 수 있는 한 라이선스에 따라 여러 시스템에 요금을 청구할 수 있습니다.

예를 들어, 20TiB 라이선스 하나를 구매하고, Cloud Volumes ONTAP 시스템 4개를 배포한 다음, 각 시스템에 5TiB 볼륨을 할당하여 총 20TiB를 확보할 수 있습니다. 해당 계정에 배포된 각 Cloud Volumes ONTAP 시스템의 볼륨에서 용량을 사용할 수 있습니다.

용량 기반 라이선싱은 패키지 형태로 제공됩니다. Cloud Volumes ONTAP 시스템을 배포하면 비즈니스 요구 사항에 따라 여러 가지 라이선스 패키지 중에서 선택할 수 있습니다.

NetApp Console 에서 관리되는 제품과 서비스의 실제 사용량과 측정은 항상 GiB와 TiB로 계산되지만, GB/GiB와 TB/TiB라는 용어는 서로 바꿔 사용됩니다. 이는 클라우드 마켓플레이스 목록, 가격 견적, 목록 설명 및 기타 지원 문서에 반영되어 있습니다.

패키지

다음과 같은 용량 기반 패키지는 Cloud Volumes ONTAP 에서 사용할 수 있습니다. 용량 기반 라이센스 패키지에 대한 자세한 내용은 다음을 참조하세요."용량 기반 라이선스에 대해 자세히 알아보세요" .

다음 용량 기반 패키지가 포함된 지원되는 VM 유형 목록은 다음을 참조하세요.

- "Azure에서 지원되는 구성"
- "Google Cloud에서 지원되는 구성"

프리미엄

NetApp 에서 모든 Cloud Volumes ONTAP 기능을 무료로 제공합니다(클라우드 공급자 요금은 여전히 적용됩니다). 프리미엄 패키지에는 다음과 같은 특징이 있습니다.

- 라이센스나 계약이 필요하지 않습니다.
- NetApp 의 지원은 포함되지 않습니다.
- Cloud Volumes ONTAP 시스템당 프로비저닝 용량은 500GiB로 제한됩니다.
- NetApp 계정당 최대 10개의 Cloud Volumes ONTAP 시스템을 Freemium으로 모든 클라우드 공급자와 함께 사용할 수 있습니다.
- Cloud Volumes ONTAP 시스템의 프로비저닝된 용량이 500GiB를 초과하면 콘솔은 시스템을 Essentials 패키지로 전환합니다.

  시스템이 Essentials 패키지로 변환되면"최소 충전" 이에 적용됩니다.

  Essentials 패키지로 전환된 Cloud Volumes ONTAP 시스템은 프로비저닝된 용량이 500GiB 미만으로 줄어들더라도 Freemium으로 다시 전환할 수 없습니다. 프로비저닝된 용량이 500GiB 미만인 다른 시스템은 Freemium을 유지합니다(Freemium 제공을 사용하여 배포된 경우).

골자

다양한 구성으로 용량별로 요금을 지불할 수 있습니다.

- Cloud Volumes ONTAP 구성을 선택하세요.
  - 단일 노드 또는 HA 시스템
  - 재해 복구(DR)를 위한 파일 및 블록 스토리지 또는 보조 데이터
- 추가 비용으로 NetApp의 클라우드 데이터 서비스를 추가하세요

전문적인

무제한 백업이 가능한 모든 유형의 Cloud Volumes ONTAP 구성에 대해 용량별로 요금을 지불하세요.

- 모든 Cloud Volumes ONTAP 구성에 대한 라이선싱을 제공합니다.

  1차 및 2차 볼륨에 대해 동일한 요금으로 용량 요금을 청구하는 단일 노드 또는 HA

- NetApp Backup and Recovery 사용한 무제한 볼륨 백업이 포함되지만 Professional 패키지를 사용하는 Cloud Volumes ONTAP 시스템에만 해당됩니다.

  백업 및 복구에는 사용량에 따른 요금(PAYGO) 구독이 필요하지만, 이 서비스 사용에는 요금이 부과되지 않습니다. 백업 및 복구에 대한 라이센싱 설정에 대한 자세한 내용은 다음을 참조하세요. "백업 및 복구에 대한 라이선싱 설정" .

- 추가 비용으로 NetApp의 클라우드 데이터 서비스를 추가하세요

용량 기반 라이선스의 가용성

Cloud Volumes ONTAP 시스템에 대한 PAYGO 및 BYOL 라이선스를 사용하려면 콘솔 에이전트가 작동 중이어야 합니다.

"콘솔 에이전트에 대해 알아보세요" .

NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAPP 에 대한 BYOL 라이선싱의 제한된 가용성" .

시작하는 방법

용량 기반 라이선싱을 시작하는 방법을 알아보세요.

- "AWS에서 Cloud Volumes ONTAP 에 대한 라이선싱 설정"
- "Azure에서 Cloud Volumes ONTAP 에 대한 라이선싱 설정"
- "Google Cloud에서 Cloud Volumes ONTAP 에 대한 라이선싱 설정"

Keystone 구독

선불 CapEx 또는 임대보다 OpEx 소비 모델을 선호하는 고객을 위해 원활한 하이브리드 클라우드 환경을 제공하는, 사용량에 따라 비용을 지불하는 구독 기반 서비스입니다.

요금은 Keystone 구독에서 하나 이상의 Cloud Volumes ONTAP HA 쌍에 대해 약속한 용량 크기에 따라 부과됩니다.

각 볼륨에 대해 제공된 용량은 집계되어 Keystone 구독에 약정된 용량과 주기적으로 비교되며, 초과분은 Keystone 구독에 버스트로 청구됩니다.

"NetApp Keystone 에 대해 자세히 알아보세요" .

지원되는 구성

Keystone 구독은 HA 쌍에서 지원됩니다. 현재 이 라이센스 옵션은 단일 노드 시스템에서는 지원되지 않습니다.

용량 제한

용량 기반 라이선싱 모델에서 각 Cloud Volumes ONTAP 시스템은 개체 스토리지에 대한 계층화를 지원하며, 전체 계층화 용량은 클라우드 공급자의 버킷 한도까지 확장될 수 있습니다. 라이센스에는 용량 제한이 부과되지 않지만 다음을 따르십시오. "FabricPool 모범 사례" 계층화를 구성하고 관리할 때 최적의 성능, 안정성 및 비용 효율성을 보장합니다.

각 클라우드 공급자의 용량 제한에 대한 자세한 내용은 해당 문서를 참조하세요.

- "AWS 문서"
- "관리 디스크에 대한 Azure 설명서"그리고 "Blob 저장소에 대한 Azure 설명서"
- "Google Cloud 문서"

시작하는 방법

Keystone 구독을 시작하는 방법을 알아보세요.

- "AWS에서 Cloud Volumes ONTAP 에 대한 라이선싱 설정"
- "Azure에서 Cloud Volumes ONTAP 에 대한 라이선싱 설정"
- "Google Cloud에서 Cloud Volumes ONTAP 에 대한 라이선싱 설정"

노드 기반 라이선싱

노드 기반 라이선싱은 노드별로 Cloud Volumes ONTAP 대한 라이선스를 부여할 수 있는 이전 세대 라이선스 모델입니다. 이 라이선스 모델은 신규 고객에게는 제공되지 않습니다. 노드별 요금 청구는 위에 설명된 용량별 요금 청구 방식으로 대체되었습니다.

NetApp 노드 기반 라이선싱의 가용성 종료(EOA) 및 지원 종료(EOS)를 계획했습니다. EOA 및 EOS 이후에는 노드 기반 라이선스를 용량 기반 라이선스로 전환해야 합니다.

자세한 내용은 다음을 참조하세요. "고객 공지: CPC-00589" .

노드 기반 라이선스 제공 종료

2024년 11월 11일부터 노드 기반 라이선스의 제한된 제공이 종료되었습니다. 노드 기반 라이선싱에 대한 지원은 2024년 12월 31일에 종료됩니다.

EOA 날짜를 넘어서도 유효한 노드 기반 계약이 있는 경우, 계약이 만료될 때까지 라이선스를 계속 사용할 수 있습니다. 계약이 만료되면 용량 기반 라이선스 모델로 전환해야 합니다. Cloud Volumes ONTAP 노드에 대한 장기 계약이 없는 경우 EOS 날짜 전에 전환을 계획하는 것이 중요합니다.

다음 표를 통해 각 라이선스 유형과 EOA가 라이선스 유형에 미치는 영향에 대해 자세히 알아보세요.

라이센스 유형	**EOA** 이후의 영향
BYOL(Bring Your Own License)을 통해 구매한 유효한 노드 기반 라이선스	라이센스는 만료일까지 유효합니다. 기존에 사용되지 않은 노드 기반 라이선스는 새로운 Cloud Volumes ONTAP 시스템을 배포하는 데 사용할 수 있습니다.
BYOL을 통해 구매한 노드 기반 라이센스가 만료되었습니다.	이 라이선스를 사용하여 새로운 Cloud Volumes ONTAP 시스템을 배포할 수 없습니다. 기존 시스템은 계속 작동할 수 있지만 EOS 날짜 이후에는 시스템에 대한 지원이나 업데이트를 받을 수 없습니다.
PAYGO 구독이 포함된 유효한 노드 기반 라이센스	EOS 날짜 이후에는 용량 기반 라이선스로 전환할 때까지 NetApp 지원을 받을 수 없습니다.

제외 사항

NetApp 특정 상황에서는 특별한 고려가 필요하다는 점을 인식하고 있으며, 노드 기반 라이선싱의 EOA 및 EOS는 다음과 같은 경우에는 적용되지 않습니다.

- 미국 공공 부문 고객
- 개인 모드 배포
- AWS에서 Cloud Volumes ONTAP 의 중국 지역 배포

이러한 특정 시나리오에서 NetApp 계약 의무와 운영적 요구 사항을 준수하면서 고유한 라이선스 요구 사항을 해결하기

위한 지원을 제공합니다.

> 이러한 시나리오에서도 새로운 노드 기반 라이선스와 라이선스 갱신은 승인일로부터 최대 1년 동안 유효합니다.

라이센스 변환

콘솔을 사용하면 라이선스 변환 도구를 통해 노드 기반 라이선스를 용량 기반으로 원활하게 변환할 수 있습니다. 노드 기반 라이센싱의 EOA에 대한 정보는 다음을 참조하세요."노드 기반 라이선스 제공 종료" .

전환하기 전에 두 라이선스 모델의 차이점을 숙지하는 것이 좋습니다. 노드 기반 라이선싱에는 각 ONTAP 인스턴스에 대한 고정 용량이 포함되어 있어 유연성이 제한될 수 있습니다. 반면, 용량 기반 라이선싱은 여러 인스턴스에서 공유 스토리지 풀을 허용하여 유연성을 높이고 리소스 활용도를 최적화하며 작업 부하를 재분배할 때 발생할 수 있는 재정적 불이익 가능성을 줄입니다. 용량 기반 요금 청구는 변화하는 저장 요구 사항에 맞게 원활하게 조정됩니다.

이 변환을 수행하는 방법을 알아보려면 다음을 참조하세요."Cloud Volumes ONTAP 노드 기반 라이선스를 용량 기반 라이선스로 변환" .

> 용량 기반 라이선싱에서 노드 기반 라이선싱으로 시스템을 전환하는 것은 지원되지 않습니다.

Cloud Volumes ONTAP 의 용량 기반 라이선스에 대해 자세히 알아보세요.

용량 기반 라이선스의 요금 및 용량 사용량에 대해 잘 알고 있어야 합니다.

소비 모델 또는 라이선스 구매 옵션

용량 기반 라이선스 패키지는 다음과 같은 소비 모델 또는 구매 옵션으로 제공됩니다.

- **BYOL**: 자체 라이선스 지참(BYOL) 모든 클라우드 공급자에 Cloud Volumes ONTAP 배포하는 데 사용할 수 있는 NetApp 에서 구매한 라이선스입니다.

  > NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 에 대한 BYOL 라이선싱의 제한된 가용성" .

- **PAYGO**: 사용량에 따른 요금 지불(PAYGO) 구독은 클라우드 공급업체의 마켓플레이스에서 제공하는 시간당 구독입니다.
- 연간: 클라우드 공급업체의 마켓플레이스와 맺은 연간 계약입니다.

다음 사항에 유의하세요.

- NetApp (BYOL)에서 라이선스를 구매하는 경우, 클라우드 제공업체의 마켓플레이스에서 PAYGO 상품도 구독해야 합니다. NetApp BYOL 라이선스를 제한적으로 제공합니다. BYOL 라이선스가 만료되면 클라우드 마켓플레이스 구독으로 교체해야 합니다.

  귀하의 라이선스 요금이 항상 먼저 청구되지만, 다음의 경우에는 마켓플레이스의 시간당 요금으로 청구됩니다.

  - 허가된 용량을 초과하는 경우
  - 면허 기간이 만료되면
- 마켓플레이스와 연간 계약을 맺은 경우 배포하는 모든 Cloud Volumes ONTAP 시스템에 대해 해당 계약 요금이

청구됩니다. 연간 마켓플레이스 계약과 BYOL을 섞어서 사용할 수는 없습니다.

- 중국 지역에서는 BYOL을 지원하는 단일 노드 시스템만 지원됩니다. 중국 지역 배포는 BYOL 라이선스 제한에서 제외됩니다.

라이선스 패키지 변경

배포 후에는 용량 기반 라이선싱을 사용하는 Cloud Volumes ONTAP 시스템의 패키지를 변경할 수 있습니다. 예를 들어, Essentials 패키지로 Cloud Volumes ONTAP 시스템을 배포한 경우 비즈니스 요구 사항이 변경되면 Professional 패키지로 변경할 수 있습니다.

"충전 방법을 변경하는 방법을 알아보세요" .

노드 기반 라이센스를 용량 기반으로 변환하는 방법에 대한 자세한 내용은 다음을 참조하세요.

지원되는 스토리지 유형 및 패키지에 대한 요금 청구 방식

Cloud Volumes ONTAP 의 요금은 패키지 및 볼륨 유형 등 여러 요인에 따라 결정됩니다. 용량 기반 라이선싱 패키지는 Cloud Volumes ONTAP 9.7 이상에서 사용할 수 있습니다.

가격에 대한 자세한 내용은 다음을 참조하세요. "NetApp Console 웹사이트" .

스토리지 **VM**

- 추가 데이터 제공 스토리지 VM(SVM)에는 추가 라이선스 비용이 없지만 데이터 제공 SVM당 최소 4TiB 용량 요금이 부과됩니다.
- 재해 복구 SVM은 제공된 용량에 따라 요금이 부과됩니다.

HA 쌍

HA 쌍의 경우 노드에 프로비저닝된 용량에 대해서만 요금이 청구됩니다. 파트너 노드에 동기적으로 미러링된 데이터에는 요금이 부과되지 않습니다.

FlexClone 및 **FlexCache** 볼륨

- FlexClone 볼륨에서 사용된 용량에 대해서는 요금이 청구되지 않습니다.
- 소스 및 대상 FlexCache 볼륨은 기본 데이터로 간주되며 프로비저닝된 공간에 따라 요금이 부과됩니다.

읽기/쓰기 볼륨

쓰기 가능한(읽기/쓰기) 볼륨을 생성하거나 사용하는 경우 해당 볼륨은 기본 볼륨으로 간주되며 스토리지 VM(SVM)당 최소 요금을 기준으로 프로비저닝된 용량에 대한 요금이 청구됩니다. 예로는 FlexVol 읽기/쓰기 볼륨, SnapLock 감사 볼륨, CIFS/NFS 감사 볼륨이 있습니다. 사용자가 생성한 모든 데이터 볼륨은 구독 및 패키지 유형에 따라 요금이 청구됩니다. SVM 루트 볼륨과 같이 자동으로 생성되어 데이터를 저장할 수 없는 ONTAP 내부 볼륨에는 요금이 부과되지 않습니다.

필수 패키지

Essentials 패키지를 사용하면 배포 유형(HA 또는 단일 노드)과 볼륨 유형(기본 또는 보조)에 따라 요금이 청구됩니다. 높은 가격부터 낮은 가격 순으로 가격은 다음과 같습니다: *Essentials Primary HA*, *Essentials Primary Single Node*, *Essentials Secondary HA*, *Essentials Secondary Single Node*. 또는 마켓플레이스 계약을 구매하거나 개인 제안을 수락하는 경우 모든 배포 또는 볼륨 유형에 대해 용량 요금이 동일합니다.

라이선싱은 Cloud Volumes ONTAP 시스템 내에서 생성된 볼륨 유형에 따라 전적으로 결정됩니다.

- 필수 단일 노드: 단 하나의 ONTAP 노드를 사용하여 Cloud Volumes ONTAP 시스템에서 생성된 읽기/쓰기 볼륨입니다.
- 필수 HA: 중단 없는 데이터 액세스를 위해 서로 장애 조치를 취할 수 있는 두 개의 ONTAP 노드를 사용하여 볼륨을 읽고 씁니다.
- 필수 보조 단일 노드: Cloud Volumes ONTAP 시스템에서 하나의 ONTAP 노드만 사용하여 생성된 데이터 보호(DP) 유형 볼륨(일반적으로 읽기 전용인 SnapMirror 또는 SnapVault 대상 볼륨)입니다.

  읽기 전용/DP 볼륨이 기본 볼륨이 되면 콘솔은 이를 기본 데이터로 간주하고 볼륨이 읽기/쓰기 모드였던 시간을 기준으로 요금을 계산합니다. 볼륨이 다시 읽기 전용/DP로 바뀌면 해당 볼륨을 다시 보조 데이터로 간주하고 콘솔에서 가장 잘 일치하는 라이선스를 사용하여 요금을 청구합니다.

- 필수 보조 HA: 두 개의 ONTAP 노드를 사용하여 Cloud Volumes ONTAP 시스템에서 생성된 데이터 보호(DP) 유형 볼륨(일반적으로 읽기 전용인 SnapMirror 또는 SnapVault 대상 볼륨)으로, 중단 없는 데이터 액세스를 위해 서로 장애 조치할 수 있습니다.

용량 제한

용량 기반 라이선싱 모델에서 각 Cloud Volumes ONTAP 시스템은 개체 스토리지에 대한 계층화를 지원하며, 전체 계층화 용량은 클라우드 공급자의 버킷 한도까지 확장될 수 있습니다. 라이센스에는 용량 제한이 부과되지 않지만 다음을 따르십시오. "FabricPool 모범 사례" 계층화를 구성하고 관리할 때 최적의 성능, 안정성 및 비용 효율성을 보장합니다.

각 클라우드 공급자의 용량 제한에 대한 자세한 내용은 해당 문서를 참조하세요.

- "AWS 문서"
- "관리 디스크에 대한 Azure 설명서"그리고 "Blob 저장소에 대한 Azure 설명서"
- "Google Cloud 문서"

최대 시스템 수

용량 기반 라이선스를 사용하는 경우, Cloud Volumes ONTAP 시스템의 최대 개수는 NetApp Console 조직당 24개로 제한됩니다. _시스템_은 Cloud Volumes ONTAP HA 쌍, Cloud Volumes ONTAP 단일 노드 시스템 또는 사용자가 생성하는 추가 스토리지 VM을 의미합니다. 기본 스토리지 VM은 이 제한에 포함되지 않습니다. 이 제한은 모든 라이선스 모델에 적용됩니다.

예를 들어, 세 가지 시스템이 있다고 가정해 보겠습니다.

- 하나의 스토리지 VM이 있는 단일 노드 Cloud Volumes ONTAP 시스템(이것은 Cloud Volumes ONTAP 배포할 때 생성되는 기본 스토리지 VM입니다)

  이 시스템은 하나의 시스템으로 간주됩니다.

- 두 개의 스토리지 VM(기본 스토리지 VM과 사용자가 생성한 추가 스토리지 VM 하나)이 있는 단일 노드 Cloud Volumes ONTAP 시스템

  이 시스템은 단일 노드 시스템용 하나와 추가 스토리지 VM용 하나, 이렇게 두 개의 시스템으로 간주됩니다.

- 3개의 스토리지 VM(기본 스토리지 VM과 사용자가 생성한 추가 스토리지 VM 2개)이 있는 Cloud Volumes

ONTAP HA 쌍

이 시스템은 HA 쌍용 시스템 1개, 추가 스토리지 VM용 시스템 2개, 총 3개로 계산됩니다.

총 6개의 시스템이 있습니다. 그러면 조직 내에 14개의 시스템을 추가로 수용할 수 있는 여유가 생깁니다.

24개 이상의 시스템이 필요한 대규모 배포의 경우, 고객 담당자나 영업팀에 문의하세요.

"AWS, Azure 및 Google Cloud의 저장 용량 한도에 대해 알아보세요." .

최소 요금

최소한 하나의 기본(읽기-쓰기) 볼륨이 있는 각 데이터 제공 스토리지 VM에 대해 최소 4TiB의 요금이 부과됩니다. 기본 볼륨의 합계가 4TiB 미만이면 콘솔은 해당 스토리지 VM에 최소 4TiB 요금을 적용합니다.

아직 볼륨을 프로비저닝하지 않은 경우 최소 요금이 적용되지 않습니다.

Essentials 패키지의 경우, 최소 4TiB 용량 요금은 보조(데이터 보호) 볼륨만 포함된 스토리지 VM에는 적용되지 않습니다. 예를 들어, 1TiB의 보조 데이터가 있는 스토리지 VM이 있는 경우 해당 1TiB의 데이터에 대해서만 요금이 청구됩니다. Professional 패키지 유형의 경우 볼륨 유형에 관계없이 최소 4TiB 용량 충전이 적용됩니다.

요금 설정 및 초과 사용 요금

콘솔의 * Licenses and subscriptions* 섹션에서 원하는 요금 청구 방식을 선택할 수 있습니다. 사용량 초과는 라이선스 패키지 또는 연간 구독에 명시된 용량을 초과할 때 발생합니다.

- * NetApp 라이선스 우선 적용*: 이 모델에서는 사용자의 사용량이 먼저 보유 라이선스 패키지(BYOL)의 용량에 따라 청구됩니다. 라이선스 용량을 초과하는 경우, 초과 사용량은 연간 마켓플레이스 구독료 또는 마켓플레이스 온디맨드 시간당 요금(PAYGO)을 기준으로 부과됩니다. BYOL 라이선스가 만료되면 클라우드 마켓플레이스를 통해 용량 기반 라이선스 모델로 전환해야 합니다. 자세한 내용은 다음을 참조하십시오. "Cloud Volumes ONTAP 노드 기반 라이선스를 용량 기반 라이선스로 변환".
- 마켓플레이스 구독에만 해당: 이 모델에서는 사용량에 따라 연간 마켓플레이스 구독료가 먼저 차감됩니다. 추가 사용량은 시장 상황에 따라 시간당 요금(PAYGO)으로 청구됩니다. 사용하지 않은 라이선스 용량은 요금 청구 시 고려되지 않습니다.

결제 방식에 대한 자세한 내용은 다음을 참조하십시오. "라이선스 및 구독에 대한 청구 기본 설정에 대해 알아보세요".

Essentials 라이선스 초과 사용 요금 부과 방식

NetApp 에서 Essentials 라이선스를 구매(BYOL)하고 특정 Essentials 패키지의 라이선스 용량을 초과하는 경우, 콘솔은 초과 사용량에 대해 더 높은 가격의 Essentials 라이선스(사용 가능한 용량이 있는 경우)에 대해 요금을 청구합니다. 콘솔은 먼저 사용자가 비용을 지불한 사용 가능한 용량을 사용한 후 마켓플레이스에 요금을 청구합니다. BYOL 라이선스로 이용 가능한 용량이 없을 경우, 초과 용량에 대해서는 마켓플레이스 시간당 요금(PAYGO)이 부과되어 월 청구서에 추가됩니다.

마찬가지로, 연간 마켓플레이스 계약이나 여러 Essentials 패키지가 포함된 비공개 오퍼를 체결한 경우, 사용량이 특정 패키지의 배포 및 볼륨 유형에 대해 약정된 용량을 초과하면 콘솔은 사용 가능한 용량을 기준으로 더 높은 가격의 Essentials 패키지에 초과 사용량에 대한 요금을 부과합니다. 해당 용량이 소진된 후 남은 초과 사용량은 시장 수요 기반(PAYGO) 시간당 요금으로 청구되어 월 청구서에 추가됩니다.

Essentials 라이선스 요금에 대한 자세한 내용은 다음을 참조하십시오."필수 패키지" .

예를 들어 보겠습니다. Essentials 패키지에 대해 다음과 같은 라이선스가 있다고 가정해 보겠습니다.

- 500TiB의 커밋 용량을 갖는 500TiB *Essentials Secondary HA* 라이선스
- 100TiB의 커밋 용량만 있는 500TiB *Essentials Single Node* 라이선스

보조 볼륨이 있는 HA 쌍에 추가로 50TiB가 프로비저닝됩니다. 50TiB를 PAYGO에 청구하는 대신, 콘솔은 *Essentials Single Node* 라이선스에 대해 50TiB 초과 요금을 청구합니다. 해당 라이선스의 가격은 _Essentials Secondary HA_보다 높지만, 이미 구매한 라이선스를 활용하고 있으므로 월별 청구서에 비용이 추가되지 않습니다.

*관리 > Licenses and subscriptions*에서 *Essentials Single Node* 라이선스에 대해 50TiB가 청구된 것을 확인할 수 있습니다.

또 다른 예를 들어보겠습니다. Essentials 패키지에 대해 다음과 같은 라이선스가 있다고 가정해 보겠습니다.

- 500TiB의 커밋 용량을 갖는 500TiB *Essentials Secondary HA* 라이선스
- 100TiB의 커밋 용량만 있는 500TiB *Essentials Single Node* 라이선스

기본 볼륨이 있는 HA 쌍에 추가로 100TiB가 프로비저닝됩니다. 구매하신 라이선스에는 *Essentials Primary HA* 용량이 할당되어 있지 않습니다. *Essentials Primary HA* 라이선스의 가격은 *Essentials Primary Single Node*_와 _*Essentials Secondary HA* 라이선스보다 높습니다.

이 예에서 콘솔은 추가 100TiB에 대해 시장 가격으로 초과 요금을 청구합니다. 초과 요금은 월별 청구서에 표시됩니다.

스토리지

Cloud Volumes ONTAP 에 지원되는 클라이언트 프로토콜

Cloud Volumes ONTAP iSCSI, NFS, SMB, NVMe-TCP 및 S3 클라이언트 프로토콜을 지원합니다.

iSCSI

iSCSI는 표준 이더넷 네트워크에서 실행될 수 있는 블록 프로토콜입니다. 대부분의 클라이언트 운영 체제는 표준 이더넷 포트를 통해 실행되는 소프트웨어 개시 프로그램을 제공합니다.

NFS

NFS는 UNIX와 LINUX 시스템을 위한 전통적인 파일 접근 프로토콜입니다. 클라이언트는 NFSv3, NFSv4 및 NFSv4.1 프로토콜을 사용하여 ONTAP 볼륨의 파일에 액세스할 수 있습니다. UNIX 스타일 권한, NTFS 스타일 권한 또는 두 가지를 혼합하여 파일 액세스를 제어할 수 있습니다.

클라이언트는 NFS와 SMB 프로토콜을 모두 사용하여 동일한 파일에 액세스할 수 있습니다.

중소기업

SMB는 Windows 시스템을 위한 전통적인 파일 접근 프로토콜입니다. 클라이언트는 SMB 2.0, SMB 2.1, SMB 3.0 및 SMB 3.1.1 프로토콜을 사용하여 ONTAP 볼륨의 파일에 액세스할 수 있습니다. NFS와 마찬가지로 다양한 권한 스타일이 지원됩니다.

S3

Cloud Volumes ONTAP 확장형 스토리지 옵션으로 S3를 지원합니다. S3 프로토콜 지원을 통해 스토리지 VM(SVM)의 버킷에 포함된 개체에 대한 S3 클라이언트 액세스를 구성할 수 있습니다.

"ONTAP 문서: S3 멀티프로토콜 작동 방식 알아보기" . "ONTAP 설명서: ONTAP 에서 S3 개체 스토리지 서비스를 구성하고 관리하는 방법을 알아보세요." .

NVMe-TCP

ONTAP 버전 9.12.1부터 모든 클라우드 공급자에서 NVMe-TCP가 지원됩니다. Cloud Volumes ONTAP 배포 중에 스토리지 VM(SVM)에 대한 블록 프로토콜로 NVMe-TCP를 지원하고 필요한 NVMe 라이선스를 자동으로 설치합니다.

NetApp Console NVMe-TCP에 대한 관리 기능을 제공하지 않습니다.

ONTAP 통한 NVMe 구성에 대한 자세한 내용은 다음을 참조하세요. "ONTAP 설명서: NVMe를 위한 스토리지 VM 구성" .

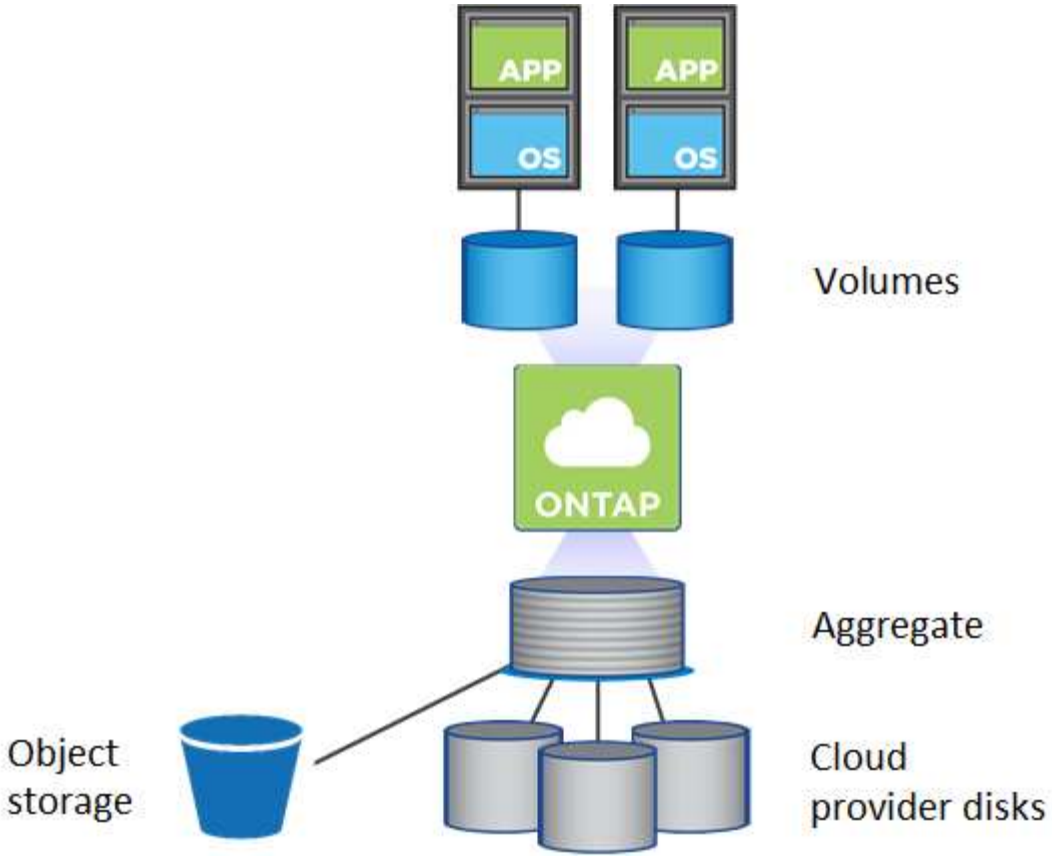
Cloud Volumes ONTAP 클러스터에 사용되는 디스크 및 집계

Cloud Volumes ONTAP 클라우드 스토리지를 어떻게 사용하는지 이해하면 스토리지 비용을 이해하는 데 도움이 될 수 있습니다.

> NetApp Console 에서 모든 디스크와 집계를 만들고 삭제해야 합니다. 다른 관리 도구에서는 이러한 작업을 수행해서는 안 됩니다. 그렇게 하면 시스템 안정성에 영향을 미치고, 나중에 디스크를 추가하는 기능을 방해할 수 있으며, 잠재적으로 중복된 클라우드 공급자 수수료가 발생할 수 있습니다.

개요

Cloud Volumes ONTAP 클라우드 공급자 스토리지를 디스크로 사용하고 이를 하나 이상의 집계로 그룹화합니다. 집계는 하나 이상의 볼륨에 대한 저장소를 제공합니다.



여러 유형의 클라우드 디스크가 지원됩니다. 볼륨을 생성할 때 디스크 유형을 선택하고 Cloud Volumes ONTAP 배포할 때 기본 디스크 크기를 선택합니다.

클라우드 공급업체로부터 구매한 총 저장 용량을 _원시 용량_이라고 합니다. 사용 가능한 용량은 약 12~14%가 Cloud Volumes ONTAP 사용을 위해 예약된 오버헤드이기 때문에 적습니다. 예를 들어, 콘솔이 500GiB 집계를 생성하는 경우 사용 가능한 용량은 442.94GiB입니다.

AWS 스토리지

AWS에서 Cloud Volumes ONTAP 사용자 데이터에 EBS 스토리지를 사용하고 일부 EC2 인스턴스 유형에서는 로컬 NVMe 스토리지를 Flash Cache로 사용합니다.

EBS 스토리지

AWS에서는 집계에 크기가 모두 같은 디스크를 최대 6개까지 포함할 수 있습니다. 하지만 Amazon EBS Elastic Volumes 기능을 지원하는 구성이 있는 경우 집계에는 최대 8개의 디스크가 포함될 수 있습니다. "Elastic Volumes 지원에 대해 자세히 알아보세요" .

최대 디스크 크기는 16TiB입니다.

기본 EBS 디스크 유형은 범용 SSD(gp3 또는 gp2), 프로비저닝된 IOPS SSD(io1) 또는 처리량 최적화 HDD(st1)일 수 있습니다. EBS 디스크를 Amazon Simple Storage Service(Amazon S3)와 연결하여 "저렴한 객체 스토리지"할 수 있습니다.

처리량 최적화 HDD(st1)를 사용하는 경우 개체 스토리지에 데이터를 계층화하는 것은 권장되지 않습니다.

로컬 **NVMe** 스토리지

일부 EC2 인스턴스 유형에는 로컬 NVMe 스토리지가 포함되어 있으며 이를 Cloud Volumes ONTAP 에서 사용합니다."Flash Cache" .

관련 링크

- "AWS 설명서: EBS 볼륨 유형"
- "AWS에서 시스템에 맞는 디스크 유형과 디스크 크기를 선택하는 방법을 알아보세요."
- "AWS에서 Cloud Volumes ONTAP 의 스토리지 한도 검토"
- "AWS에서 Cloud Volumes ONTAP 에 지원되는 구성을 검토하세요."

Azure 스토리지

Azure에서 애그리게이트는 최대 12개의 동일한 크기의 디스크를 포함할 수 있습니다. 디스크 유형과 최대 디스크 크기는 단일 노드 시스템을 사용하는지 또는 HA 쌍을 사용하는지에 따라 달라집니다.

단일 노드 시스템

단일 노드 시스템에서는 다음과 같은 유형의 Azure 관리 디스크를 사용할 수 있습니다.

- _프리미엄 SSD 관리 디스크_는 비용이 더 많이 들더라도 I/O 집약적 워크로드에 대해 높은 성능을 제공합니다.
- _프리미엄 SSD v2 관리형 디스크_는 단일 노드와 HA 쌍 모두에 대해 프리미엄 SSD 관리형 디스크에 비해 더 낮은 비용으로 더 높은 성능과 더 낮은 지연 시간을 제공합니다.
- _표준 SSD 관리 디스크_는 낮은 IOPS가 필요한 작업 부하에 대해 일관된 성능을 제공합니다.
- _표준 HDD 관리 디스크_는 높은 IOPS가 필요하지 않고 비용을 절감하고 싶은 경우에 좋은 선택입니다.

  각 관리 디스크 유형의 최대 디스크 크기는 32TiB입니다.

  관리형 디스크를 Azure Blob 저장소와 페어링할 수 있습니다."저렴한 객체 스토리지" .

HA 쌍

HA 쌍은 비용이 더 많이 들더라도 I/O 집약적 워크로드에 대해 높은 성능을 제공하는 두 가지 유형의 디스크를 사용합니다.

- 최대 8TiB 디스크 크기를 갖는 프리미엄 페이지 블롭
- 최대 32TiB 디스크 크기를 갖는 관리 디스크

관련 링크

- "Azure에서 시스템에 맞는 디스크 유형과 디스크 크기를 선택하는 방법을 알아보세요."
- "Azure에서 Cloud Volumes ONTAP HA 쌍 시작"
- "Microsoft Azure 설명서: Azure 관리 디스크 유형"
- "Microsoft Azure 설명서: Azure 페이지 Blob 개요"
- "Azure에서 Cloud Volumes ONTAP 의 저장소 한도 검토"

구글 클라우드 스토리지

Google Cloud에서는 집계에 크기가 모두 같은 디스크를 최대 6개까지 포함할 수 있습니다. 최대 디스크 크기는 64TiB입니다.

디스크 유형은 영역 *SSD* 영구 디스크, 영역 균형 영구 디스크 또는 _영역 표준 영구 디스크_가 될 수 있습니다. Google Storage 버킷과 영구 디스크를 페어링할 수 있습니다."저렴한 객체 스토리지" .

관련 링크

- "Google Cloud 문서: 스토리지 옵션"
- "Google Cloud에서 Cloud Volumes ONTAP 의 저장 한도 검토"

RAID 유형

각 Cloud Volumes ONTAP 집계의 RAID 유형은 RAID0(스트라이핑)입니다. Cloud Volumes ONTAP 디스크 가용성과 내구성을 위해 클라우드 공급자를 활용합니다. 다른 RAID 유형은 지원되지 않습니다.

핫 스페어

RAID0은 중복성을 위한 핫 스페어 사용을 지원하지 않습니다.

Cloud Volumes ONTAP 인스턴스에 연결된 사용하지 않는 디스크(핫 스페어)를 만드는 것은 불필요한 비용이며, 필요에 따라 추가 공간을 프로비저닝하지 못할 수 있습니다. 그러므로 권장하지 않습니다.

Cloud Volumes ONTAP 통한 AWS Elastic Volumes 지원에 대해 알아보세요.

Cloud Volumes ONTAP 집계를 통한 Amazon EBS Elastic Volumes 기능에 대한 지원은 더 나은 성능과 추가 용량을 제공하는 동시에 NetApp Console 필요에 따라 기본 디스크 용량을 자동으로 늘릴 수 있도록 합니다.

이익

- 동적 디스크 성장

  콘솔은 Cloud Volumes ONTAP 실행 중이고 디스크가 연결되어 있는 동안 디스크 크기를 동적으로 늘릴 수 있습니다.

- 더 나은 성능

  Elastic Volumes가 활성화된 집계에는 최대 8개의 디스크가 두 개의 RAID 그룹에서 동일하게 활용될 수 있습니다. 이 구성은 더 많은 처리량과 일관된 성능을 제공합니다.

- 더 큰 골재

  8개의 디스크를 지원하므로 최대 128TiB의 총 용량을 제공합니다. 이러한 제한은 Elastic Volumes 기능이 활성화되지 않은 집계에 대한 6개 디스크 제한 및 96TiB 제한보다 높습니다.

  전체 시스템 용량 제한은 동일하게 유지됩니다.

"AWS 설명서: AWS의 탄력적 볼륨에 대해 자세히 알아보세요"

지원되는 구성

Amazon EBS Elastic Volumes 기능은 특정 Cloud Volumes ONTAP 버전과 특정 EBS 디스크 유형에서 지원됩니다.

Cloud Volumes ONTAP 버전

Elastic Volumes 기능은 버전 9.11.0 이상에서 생성된 새로운 Cloud Volumes ONTAP 시스템에서 지원됩니다. 이 기능은 9.11.0 이전에 배포된 기존 Cloud Volumes ONTAP 시스템에서는 지원되지 않습니다.

예를 들어, Cloud Volumes ONTAP 9.9.0 시스템을 만든 다음 나중에 해당 시스템을 9.11.0 버전으로 업그레이드한 경우 Elastic Volumes 기능이 지원되지 않습니다. 버전 9.11.0 이상을 사용하여 배포된 새로운 시스템이어야 합니다.

EBS 디스크 유형

일반 용도 SSD(gp3) 또는 프로비저닝된 IOPS SSD(io1)를 사용하는 경우 Elastic Volumes 기능이 집계 수준에서 자동으로 활성화됩니다. Elastic Volumes 기능은 다른 디스크 유형을 사용하는 집계에서는 지원되지 않습니다.

필수 AWS 권한

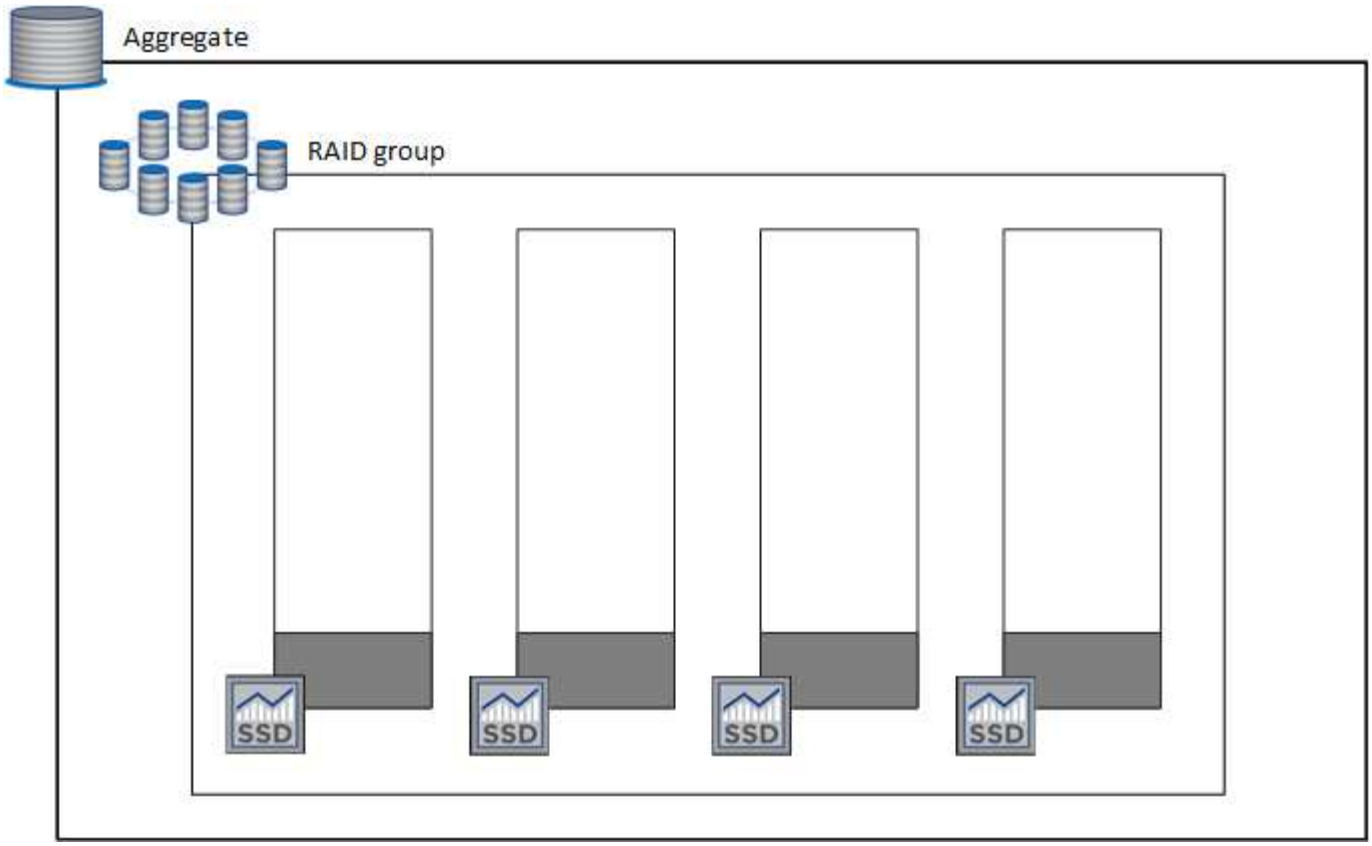
3.9.19 릴리스부터 콘솔 에이전트에는 Cloud Volumes ONTAP 집계에서 Elastic Volumes 기능을 활성화하고 관리하기 위해 다음 권한이 필요합니다.

- ec2:볼륨 수정 설명
- ec2:볼륨 수정

이러한 권한은 다음에 포함됩니다. "NetApp 에서 제공하는 정책"

Elastic Volumes 지원 작동 방식

Elastic Volumes 기능이 활성화된 집계는 하나 또는 두 개의 RAID 그룹으로 구성됩니다. 각 RAID 그룹에는 동일한 용량을 가진 4개의 동일한 디스크가 있습니다. 각각 2.5TiB인 디스크 4개가 있는 10TiB 집계의 예는 다음과 같습니다.



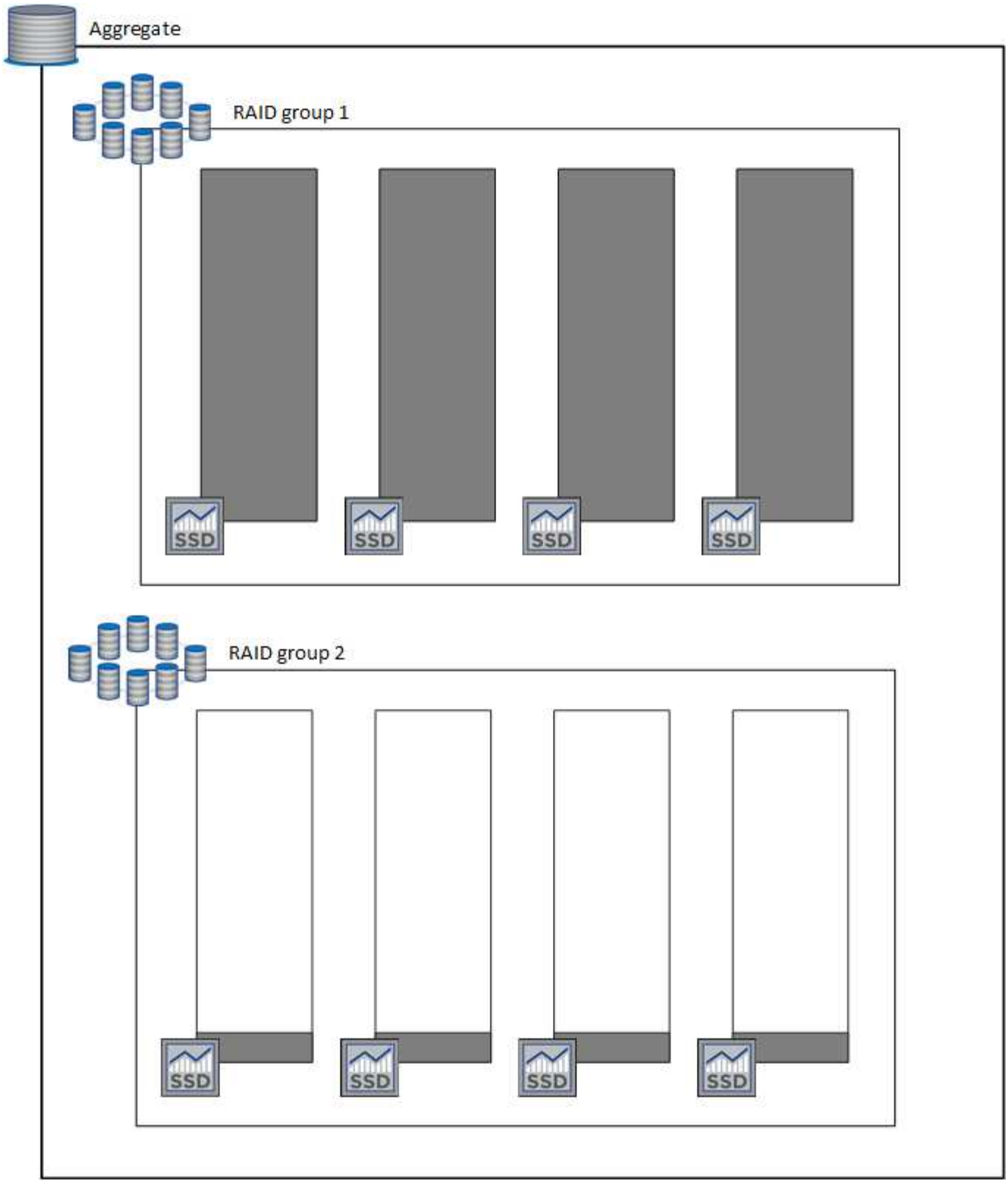
콘솔이 집계를 생성할 때는 하나의 RAID 그룹으로 시작합니다. 추가 용량이 필요한 경우 RAID 그룹에 있는 모든 디스크의 용량을 같은 양만큼 늘려서 집계를 늘립니다. 용량 증가는 최소 256GiB 또는 전체 크기의 10%입니다.

예를 들어, 1TiB 집계가 있는 경우 각 디스크는 250GiB입니다. 전체 용량의 10%는 100GiB입니다. 이는 256GiB보다 작으므로 집계 크기는 최소 256GiB(또는 디스크당 64GiB)만큼 증가합니다.

콘솔은 Cloud Volumes ONTAP 시스템이 실행 중이고 디스크가 연결되어 있는 동안 디스크 크기를 늘립니다. 변화는 방해가 되지 않습니다.

집계가 64TiB(또는 디스크당 16TiB)에 도달하면 콘솔은 추가 용량을 위해 두 번째 RAID 그룹을 생성합니다. 두 번째 RAID 그룹은 첫 번째 RAID 그룹과 동일하게 작동합니다. 정확히 동일한 용량을 가진 디스크가 4개 있으며 최대 64TiB까지 확장할 수 있습니다. 즉, 집계된 데이터의 최대 용량은 128TiB입니다.

다음은 두 개의 RAID 그룹이 있는 집계의 예입니다. 첫 번째 RAID 그룹에서는 용량 한도에 도달했지만 두 번째 RAID 그룹의 디스크에는 충분한 여유 공간이 있습니다.



볼륨을 생성하면 어떻게 되나요**?**

gp3 또는 io1 디스크를 사용하는 볼륨을 생성하는 경우 콘솔은 다음과 같이 집계에 볼륨을 생성합니다.

- Elastic Volumes가 활성화된 기존 gp3 또는 io1 집계가 있는 경우 콘솔은 해당 집계에 볼륨을 생성합니다.
- Elastic Volumes가 활성화된 gp3 또는 io1 집계가 여러 개 있는 경우 콘솔은 리소스가 가장 적게 필요한 집계에

볼륨을 생성합니다.

- 시스템에 Elastic Volumes에 대해 활성화되지 않은 gp3 또는 io1 집계만 있는 경우 볼륨은 해당 집계에 따라 생성됩니다.

> 이런 시나리오가 발생할 가능성은 낮지만 두 가지 경우에는 가능합니다.
>
> - API에서 집계를 생성할 때 Elastic Volumes 기능을 명시적으로 비활성화했습니다.
> - 사용자 인터페이스에서 새로운 Cloud Volumes ONTAP 시스템을 생성한 경우 초기 집계에서는 Elastic Volumes 기능이 비활성화됩니다. 검토제한 사항 자세한 내용은 아래를 참조하세요.

- 기존 집계에 충분한 용량이 없으면 콘솔은 Elastic Volumes가 활성화된 집계를 만든 다음 해당 새 집계에 볼륨을 만듭니다.

  집계 크기는 요청된 볼륨 크기에 추가 10% 용량을 더한 값을 기준으로 합니다.

용량 관리 모드

콘솔 에이전트의 용량 관리 모드는 다른 유형의 집계와 유사한 방식으로 Elastic Volumes에서 작동합니다.

- 자동 모드가 활성화된 경우(기본 설정), 추가 용량이 필요한 경우 콘솔이 자동으로 집계 크기를 늘립니다.
- 용량 관리 모드를 수동으로 변경하면 콘솔에서 추가 용량 구매에 대한 승인을 요청합니다.

"용량 관리 모드에 대해 자세히 알아보세요" .

제한 사항

집계 크기를 늘리는 데 최대 6시간이 걸릴 수 있습니다. 그 시간 동안 콘솔은 해당 집계에 대한 추가 용량을 요청할 수 없습니다.

Elastic Volumes를 사용하는 방법

Elastic Volumes를 사용하여 다음 작업을 수행할 수 있습니다.

- gp3 또는 io1 디스크를 사용할 때 초기 집계에서 탄력적 볼륨이 활성화된 새 시스템을 만듭니다.

  "Cloud Volumes ONTAP 시스템을 만드는 방법을 알아보세요"

- Elastic Volumes가 활성화된 집계에 새 볼륨을 만듭니다.

  gp3 또는 io1 디스크를 사용하는 볼륨을 생성하는 경우 콘솔은 Elastic Volumes가 활성화된 집계에 볼륨을 자동으로 생성합니다. 자세한 내용은 다음을 참조하세요.볼륨을 생성하면 어떻게 되나요? .

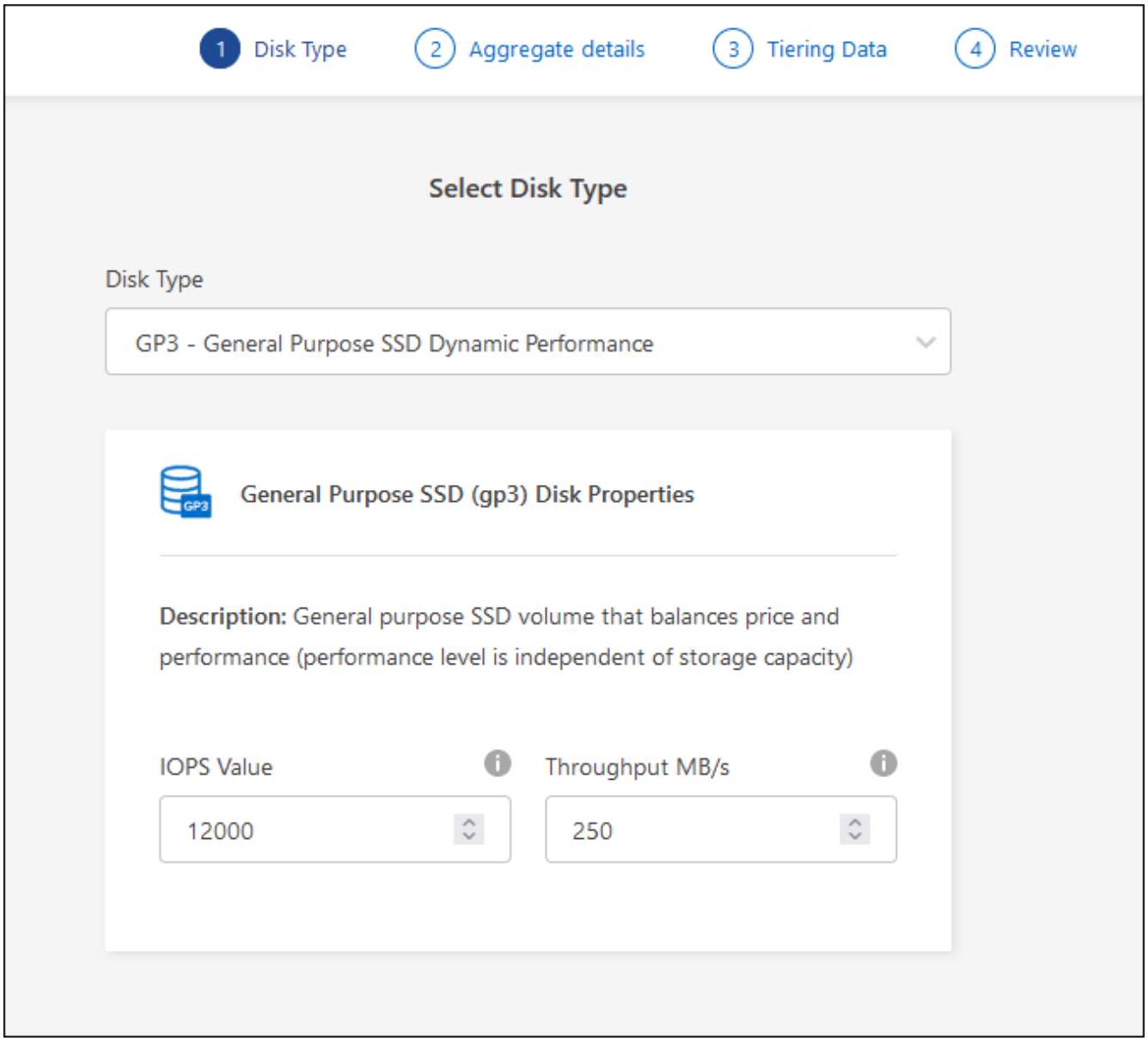
  "볼륨을 만드는 방법을 알아보세요" .

- Elastic Volumes가 활성화된 새 집계를 만듭니다.

  Cloud Volumes ONTAP 시스템이 9.11.0 이상 버전에서 생성된 경우, gp3 또는 io1 디스크를 사용하는 새 집계에서 Elastic Volumes가 자동으로 활성화됩니다.

집계를 만들 때 콘솔에서 집계의 용량 크기를 입력하라는 메시지가 표시됩니다. 이는 디스크 크기와 디스크 개수를 선택하는 다른 구성과는 다릅니다.

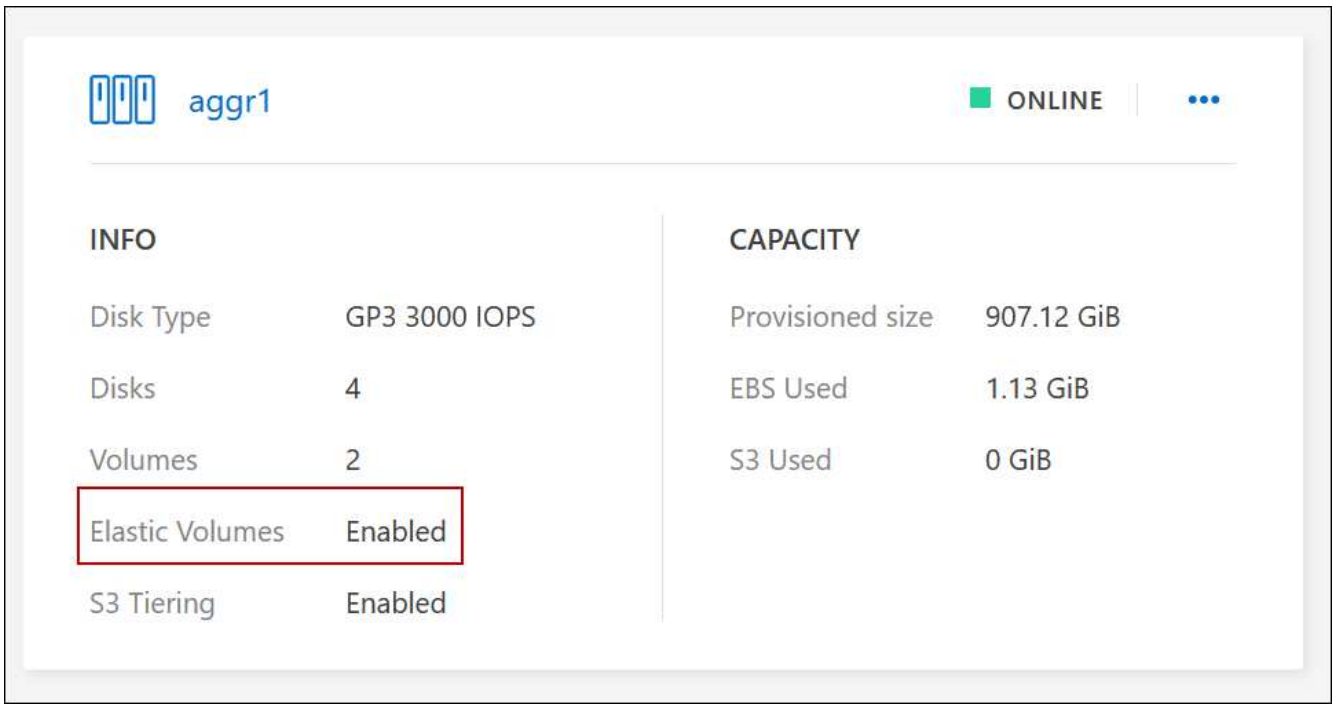
다음 스크린샷은 gp3 디스크로 구성된 새로운 집계의 예를 보여줍니다.



"집계를 만드는 방법을 알아보세요" .

- Elastic Volumes가 활성화된 집계를 식별합니다.

  고급 할당 페이지로 이동하면 집계에서 탄력적 볼륨 기능이 활성화되어 있는지 확인할 수 있습니다. 다음 예에서 aggr1에는 Elastic Volumes가 활성화되어 있습니다.



- 집계에 용량 추가

  콘솔은 필요에 따라 자동으로 집계에 용량을 추가하지만, 직접 수동으로 용량을 늘릴 수 있습니다.

  "집계 용량을 늘리는 방법을 알아보세요" .

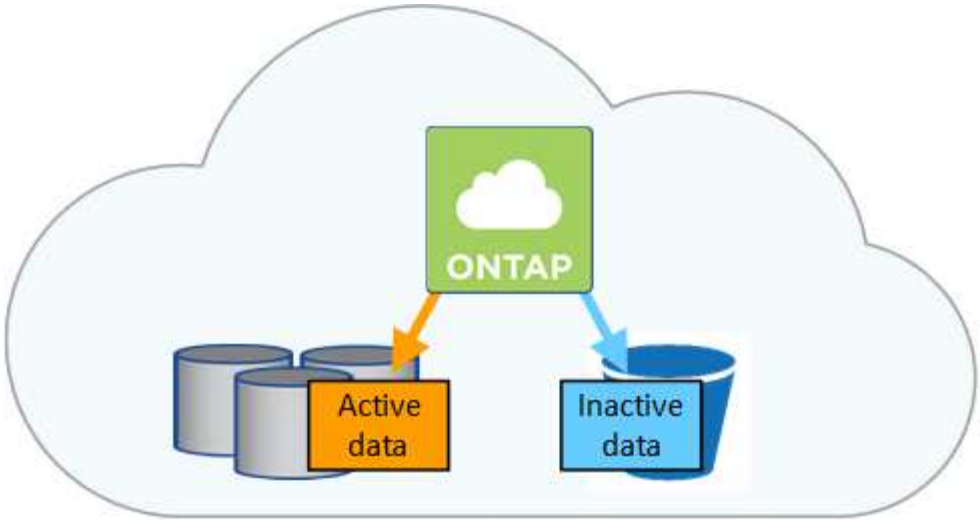
- Elastic Volumes가 활성화된 집계에 데이터 복제

  대상 Cloud Volumes ONTAP 시스템이 Elastic Volumes를 지원하는 경우 대상 볼륨은 Elastic Volumes가 활성화된 집계에 배치됩니다(gp3 또는 io1 디스크를 선택하는 경우).

  "데이터 복제를 설정하는 방법을 알아보세요"

AWS, Azure 또는 Google Cloud에서 Cloud Volumes ONTAP 사용한 데이터 계층화에 대해 알아보세요.

비활성 데이터를 저비용 객체 스토리지로 자동 계층화하여 스토리지 비용을 절감하세요. 활성 데이터는 고성능 SSD 또는 HDD에 보관되고, 비활성 데이터는 저비용 개체 스토리지에 계층화됩니다. 이를 통해 기본 저장소의 공간을 확보하고 보조 저장소의 크기를 줄일 수 있습니다.



데이터 계층화는 FabricPool 기술을 기반으로 합니다. Cloud Volumes ONTAP 추가 라이선스 없이 모든 Cloud Volumes ONTAP 클러스터에 대한 데이터 계층화를 제공합니다. 데이터 계층화를 활성화하면 개체 스토리지에 계층화된 데이터에 요금이 부과됩니다. 개체 스토리지 비용에 대한 자세한 내용은 클라우드 제공업체의 설명서를 참조하세요.

AWS의 데이터 계층화

AWS에서 데이터 계층화를 활성화하면 Cloud Volumes ONTAP는 자주 사용되는 데이터에 대해 EBS를 성능 계층으로 사용하고, 사용되지 않는 데이터에 대해 Amazon Simple Storage Service(Amazon S3)를 용량 계층으로 사용합니다.

성능 계층

성능 계층은 일반 용도 SSD(gp3 또는 gp2) 또는 프로비저닝된 IOPS SSD(io1)가 될 수 있습니다.

처리량 최적화 HDD(st1)를 사용하는 경우 개체 스토리지에 데이터를 계층화하는 것은 권장되지 않습니다.

용량 계층

Cloud Volumes ONTAP 시스템은 비활성 데이터를 단일 S3 버킷에 계층화합니다.

NetApp Console 각 시스템에 대해 단일 S3 버킷을 생성하고 이를 fabric-pool-_cluster unique identifier_로 명명합니다. 각 볼륨에 대해 다른 S3 버킷이 생성되지 않습니다.

콘솔이 S3 버킷을 생성할 때 다음과 같은 기본 설정을 사용합니다.

- 저장 등급: 표준
- 기본 암호화: 비활성화됨
- 공개 접근 차단: 모든 공개 접근 차단
- 개체 소유권: ACL 활성화됨
- 버킷 버전 관리: 비활성화됨
- 객체 잠금: 비활성화됨

스토리지 클래스

AWS의 계층형 데이터에 대한 기본 스토리지 클래스는 _Standard_입니다. Standard는 여러 가용성 영역에 저장된 자주 액세스되는 데이터에 이상적입니다.

비활성 데이터에 액세스할 계획이 없다면 스토리지 클래스를 다음 중 하나로 변경하여 스토리지 비용을 줄일 수 있습니다. 지능형 계층화, 단일 영역 드물게 액세스, 표준 드물게 액세스 또는 *S3 Glacier* 즉시 검색. 저장 클래스를 변경하면 비활성 데이터는 표준 저장 클래스에서 시작되고 30일 동안 데이터에 액세스하지 않으면 선택한 저장 클래스로 전환됩니다.

데이터에 액세스하는 경우 액세스 비용이 더 높아지므로 스토리지 클래스를 변경하기 전에 이 점을 고려하세요. "Amazon S3 설명서: Amazon S3 스토리지 클래스에 대해 자세히 알아보세요" .

시스템을 생성할 때 저장 클래스를 선택할 수 있으며, 나중에 언제든지 변경할 수 있습니다. 저장 클래스 변경에 대한 지침은 다음을 참조하세요."비활성 데이터를 저비용 객체 스토리지로 계층화" .

데이터 계층화를 위한 스토리지 클래스는 볼륨별이 아닌 시스템 전체에 적용됩니다.

Azure의 데이터 계층화

Azure에서 데이터 계층화를 활성화하면 Cloud Volumes ONTAP 핫 데이터에 대한 성능 계층으로 Azure 관리 디스크를 사용하고 비활성 데이터에 대한 용량 계층으로 Azure Blob Storage를 사용합니다.

성능 계층

성능 계층은 SSD 또는 HDD가 될 수 있습니다.

용량 계층

Cloud Volumes ONTAP 시스템은 비활성 데이터를 단일 Blob 컨테이너에 계층화합니다.

콘솔은 각 Cloud Volumes ONTAP 시스템에 대한 컨테이너가 있는 새로운 스토리지 계정을 생성합니다. 저장 계정의 이름은 무작위입니다. 각 볼륨에 대해 다른 컨테이너가 생성되지 않습니다.

콘솔은 다음 설정으로 저장소 계정을 생성합니다.

- 액세스 계층: 핫
- 성능: 표준
- 중복성: Cloud Volume ONTAP 배포에 따라
  - 단일 가용성 영역: 로컬 중복 스토리지(LRS)
  - 다중 가용성 영역: 영역 중복 스토리지(ZRS)
- 계정: StorageV2(일반 용도 v2)
- REST API 작업에 대한 보안 전송 필요: 활성화됨
- 저장소 계정 키 액세스: 활성화됨
- 최소 TLS 버전: 버전 1.2
- 인프라 암호화: 비활성화됨

스토리지 액세스 계층

Azure의 계층화된 데이터에 대한 기본 저장소 액세스 계층은 핫 계층입니다. 핫 티어는 용량 티어에서 자주 액세스되는 데이터에 이상적입니다.

용량 계층에서 비활성 데이터에 액세스할 계획이 없다면 비활성 데이터가 최소 30일 동안 보관되는 쿨 스토리지 계층을 선택할 수 있습니다. 최소 90일 동안 비활성 데이터를 저장하는 콜드 계층을 선택할 수도 있습니다. 보관 요구 사항과 비용 고려 사항에 따라 필요에 가장 적합한 계층을 선택할 수 있습니다. 스토리지 계층을 *cool* 또는 _cold_로

변경하면 비활성 용량 계층 데이터가 쿨 또는 콜드 스토리지 계층으로 직접 이동합니다. 쿨 티어와 콜드 티어는 핫 티어에 비해 보관 비용이 낮지만, 액세스 비용이 더 높으므로 보관 티어를 변경하기 전에 이 점을 고려하세요. 참조하다 "Microsoft Azure 설명서: Azure Blob 저장소 액세스 계층에 대해 자세히 알아보기" .

Cloud Volumes ONTAP 시스템을 추가할 때 스토리지 계층을 선택할 수 있으며, 나중에 언제든지 변경할 수 있습니다. 저장 계층 변경에 대한 자세한 내용은 다음을 참조하세요."비활성 데이터를 저비용 객체 스토리지로 계층화" .

데이터 계층화를 위한 스토리지 액세스 계층은 볼륨별이 아닌 시스템 전체에 적용됩니다.

Google Cloud의 데이터 계층화

Google Cloud에서 데이터 계층화를 활성화하면 Cloud Volumes ONTAP 핫 데이터의 성능 계층으로 영구 디스크를 사용하고 비활성 데이터의 용량 계층으로 Google Cloud Storage 버킷을 사용합니다.

성능 계층

성능 계층은 SSD 영구 디스크, 균형 영구 디스크 또는 표준 영구 디스크가 될 수 있습니다.

용량 계층

Cloud Volumes ONTAP 시스템은 비활성 데이터를 단일 Google Cloud Storage 버킷에 계층화합니다.

콘솔은 각 시스템에 대한 버킷을 생성하고 이를 fabric-pool-_cluster unique identifier_로 명명합니다. 각 볼륨마다 다른 버킷이 생성되지 않습니다.

콘솔에서 버킷을 생성할 때 다음과 같은 기본 설정을 사용합니다.

- 위치 유형: 지역
- 저장 등급: 표준
- 공개 액세스: 객체 ACL에 따름
- 접근 제어: 세분화됨
- 보호: 없음
- 데이터 암호화: Google 관리 키

스토리지 클래스

계층형 데이터의 기본 저장 클래스는 표준 저장 클래스입니다. 데이터에 자주 접근하지 않는다면 *Nearline Storage* 또는 _Coldline Storage_로 변경하여 저장 비용을 줄일 수 있습니다. 저장 클래스를 변경하면 이후의 비활성 데이터는 선택한 클래스로 직접 이동됩니다.

> ⓘ 저장 클래스를 변경해도 기존의 비활성 데이터는 기본 저장 클래스를 유지합니다. 기존 비활성 데이터의 저장 클래스를 변경하려면 수동으로 지정해야 합니다.

데이터에 액세스하는 경우 액세스 비용이 더 높아지므로 스토리지 클래스를 변경하기 전에 이 점을 고려하세요. 자세한 내용은 다음을 참조하세요. "Google Cloud 문서: 스토리지 클래스" .

시스템을 생성할 때 저장 계층을 선택할 수 있으며, 나중에 언제든지 변경할 수 있습니다. 저장 클래스 변경에 대한 자세한 내용은 다음을 참조하세요."비활성 데이터를 저비용 객체 스토리지로 계층화" .

데이터 계층화를 위한 스토리지 클래스는 볼륨별이 아닌 시스템 전체에 적용됩니다.

데이터 계층화 및 용량 제한

데이터 계층화를 활성화하면 시스템 용량 제한이 동일하게 유지됩니다. 제한은 성능 계층과 용량 계층에 걸쳐 분산됩니다.

볼륨 티어링 정책

데이터 계층화를 활성화하려면 볼륨을 생성, 수정 또는 복제할 때 볼륨 계층화 정책을 선택해야 합니다. 각 볼륨마다 다른 정책을 선택할 수 있습니다.

일부 계층화 정책에는 연관된 최소 냉각 기간이 있는데, 이는 볼륨의 사용자 데이터가 "콜드"로 간주되어 용량 계층으로 이동되기 위해 비활성 상태를 유지해야 하는 시간을 설정합니다. 냉각 기간은 데이터가 집계에 기록될 때부터 시작됩니다.

최소 냉각 기간과 기본 집계 임계값인 50%를 변경할 수 있습니다(자세한 내용은 아래 참조). "냉각 기간을 변경하는 방법을 알아보세요" 그리고 "임계값을 변경하는 방법을 알아보세요" .

콘솔을 사용하면 볼륨을 생성하거나 수정할 때 다음 볼륨 계층화 정책 중에서 선택할 수 있습니다.

스냅샷만
: 집계가 용량의 50%에 도달하면 Cloud Volumes ONTAP 활성 파일 시스템과 연결되지 않은 스냅샷 복사본의 콜드 사용자 데이터를 용량 계층으로 계층화합니다. 냉각 기간은 약 2일입니다.

  읽을 경우, 용량 계층의 콜드 데이터 블록이 핫이 되어 성능 계층으로 이동됩니다.

모두
: 모든 데이터(메타데이터 제외)는 즉시 콜드 데이터로 표시되고 가능한 한 빨리 개체 스토리지에 계층화됩니다. 볼륨의 새로운 블록이 차가워질 때까지 48시간을 기다릴 필요가 없습니다. 모든 정책이 설정되기 전에 볼륨에 위치한 블록은 차가워지려면 48시간이 필요합니다.

  읽을 경우, 클라우드 계층의 콜드 데이터 블록은 콜드 상태로 유지되며 성능 계층에 다시 기록되지 않습니다. 이 정책은 ONTAP 9.6부터 사용할 수 있습니다.

자동
: 집계가 용량의 50%에 도달하면 Cloud Volumes ONTAP 은 볼륨의 콜드 데이터 블록을 용량 계층으로 계층화합니다. 콜드 데이터에는 스냅샷 사본뿐만 아니라 활성 파일 시스템의 콜드 사용자 데이터도 포함됩니다. 냉각 기간은 약 31일입니다.

  이 정책은 Cloud Volumes ONTAP 9.4부터 지원됩니다.

  무작위 읽기로 읽는 경우 용량 계층의 콜드 데이터 블록이 핫해지고 성능 계층으로 이동합니다. 인덱스 및 바이러스 백신 검사와 관련된 순차적 읽기로 읽는 경우, 콜드 데이터 블록은 콜드 상태로 유지되고 성능 계층으로 이동하지 않습니다.

None
: 볼륨의 데이터를 성능 계층에 보관하여 용량 계층으로 이동되는 것을 방지합니다.

복제
: 볼륨을 복제할 때 데이터를 개체 스토리지에 계층화할지 여부를 선택할 수 있습니다. 그러면 콘솔은 데이터 보호 볼륨에 백업 정책을 적용합니다. Cloud Volumes ONTAP 9.6부터 모든 계층화 정책이 백업 정책을 대체합니다. 복제 관계가 삭제되면 대상 볼륨은 복제 중에 적용되었던 계층화 정책을 유지합니다.

Cloud Volumes ONTAP 끄면 냉각 기간에 영향을 미칩니다**.**

데이터 블록은 냉각 스캔을 통해 냉각됩니다. 이 과정에서 사용되지 않은 블록의 블록 온도는 다음으로 낮은 값으로 이동(냉각)됩니다. 기본 냉각 시간은 볼륨 계층화 정책에 따라 달라집니다.

- 자동: 31일
- 스냅샷만: 2일

냉각 스캔이 작동하려면 Cloud Volumes ONTAP 실행 중이어야 합니다. Cloud Volumes ONTAP 이 꺼져 있으면 냉각도 중지됩니다. 결과적으로 더 오랜 시간 동안 시원함을 느낄 수 있습니다.

Cloud Volumes ONTAP 끄면 시스템을 다시 시작할 때까지 각 블록의 온도가 유지됩니다. 예를 들어, 시스템을 끌 때 블록의 온도가 5라면, 시스템을 다시 켜도 온도는 여전히 5입니다.

데이터 계층화 설정

지침 및 지원되는 구성 목록은 다음을 참조하세요."비활성 데이터를 저비용 객체 스토리지로 계층화" .

Cloud Volumes ONTAP 스토리지 관리

NetApp Console Cloud Volumes ONTAP 스토리지에 대한 간편하고 고급 관리 기능을 제공합니다.

모든 디스크와 집계는 콘솔에서 직접 만들고 삭제해야 합니다. 다른 관리 도구에서는 이러한 작업을 수행해서는 안 됩니다. 그렇게 하면 시스템 안정성에 영향을 미치고, 나중에 디스크를 추가하는 기능을 방해할 수 있으며, 잠재적으로 중복된 클라우드 공급자 수수료가 발생할 수 있습니다.

스토리지 프로비저닝

콘솔을 사용하면 디스크를 구매하고 집계를 관리하여 Cloud Volumes ONTAP 에 대한 스토리지 프로비저닝이 쉬워집니다. 볼륨만 생성하면 됩니다. 원하는 경우 고급 할당 옵션을 사용하여 직접 집계를 프로비저닝할 수 있습니다.

간소화된 프로비저닝

집계는 볼륨에 클라우드 스토리지를 제공합니다. 콘솔은 인스턴스를 시작할 때와 추가 볼륨을 프로비저닝할 때 집계를 생성합니다.

볼륨을 생성하면 콘솔은 다음 세 가지 작업 중 하나를 수행합니다.

- 충분한 여유 공간이 있는 기존 집합체에 볼륨을 배치합니다.
- 해당 집계에 대해 추가 디스크를 구매하여 볼륨을 기존 집계에 배치합니다.

+ Elastic Volumes를 지원하는 AWS의 집계의 경우 RAID 그룹의 디스크 크기도 늘어납니다. "Elastic Volumes 지원에 대해 자세히 알아보세요" .

- 새로운 집계를 위해 디스크를 구매하고 해당 집계에 볼륨을 배치합니다.

콘솔은 집계의 최대 크기, 씬 프로비저닝이 활성화되어 있는지 여부, 집계의 여유 공간 임계값 등 여러 요소를 고려하여 새 볼륨을 배치할 위치를 결정합니다.

AWS의 집계를 위한 디스크 크기 선택

콘솔이 AWS에서 Cloud Volumes ONTAP 에 대한 새로운 집계를 생성할 때 집계 수가 증가함에 따라 디스크 크기를 점차 늘려 AWS 데이터 디스크 제한에 도달하기 전에 시스템 용량을 극대화합니다.

예를 들어, 콘솔은 다음과 같은 디스크 크기를 선택할 수 있습니다.

집계 번호	디스크 크기	최대 집계 용량
1	500기가바이트	3티비
4	1티비	6티비
6	2티비	12티비

이 동작은 Amazon EBS Elastic Volumes 기능을 지원하는 집계에는 적용되지 않습니다. 탄력적 볼륨이 활성화된 집계는 하나 또는 두 개의 RAID 그룹으로 구성됩니다. 각 RAID 그룹에는 동일한 용량을 가진 4개의 동일한 디스크가 있습니다. "Elastic Volumes 지원에 대해 자세히 알아보세요" .

고급 할당 옵션을 사용하면 디스크 크기를 직접 선택할 수 있습니다.

고급 할당

집계도 관리할 수 있습니다. "고급 할당 페이지에서" , 특정 수의 디스크를 포함하는 새로운 집계를 만들고, 기존 집계에 디스크를 추가하고, 특정 집계에 볼륨을 만들 수 있습니다.

용량 관리

조직 또는 계정 관리자는 콘솔을 구성하여 저장 용량 결정 사항을 알리거나 자동으로 용량 요구 사항을 관리할지 여부를 결정할 수 있습니다.

이 동작은 콘솔 에이전트의 _용량 관리 모드_에 의해 결정됩니다. 용량 관리 모드는 해당 콘솔 에이전트가 관리하는 모든 Cloud Volumes ONTAP 시스템에 영향을 미칩니다. 다른 콘솔 에이전트가 있는 경우 다르게 구성할 수 있습니다.

자동 용량 관리

용량 관리 모드는 기본적으로 자동으로 설정되어 있습니다. 이 모드에서는 콘솔이 15분마다 여유 공간 비율을 확인하여 여유 공간 비율이 지정된 임계값 아래로 떨어지는지 확인합니다. 더 많은 용량이 필요한 경우 새 디스크를 구매하고, 사용하지 않는 디스크 컬렉션(집계)을 삭제하고, 필요에 따라 집계 간에 볼륨을 이동하고, 디스크 오류를 방지하려고 시도합니다.

다음 예에서는 이 모드가 작동하는 방식을 보여줍니다.

- 집계가 용량 임계값에 도달하고 디스크를 더 추가할 공간이 있는 경우 콘솔은 자동으로 해당 집계에 대한 새 디스크를 구매하여 볼륨이 계속 증가할 수 있도록 합니다.

Elastic Volumes를 지원하는 AWS의 집계의 경우 RAID 그룹의 디스크 크기도 늘어납니다. "Elastic Volumes 지원에 대해 자세히 알아보세요" .

+ * 집계가 용량 임계값에 도달하여 추가 디스크를 지원할 수 없는 경우 콘솔은 자동으로 해당 집계의 볼륨을 사용 가능한 용량이 있는 집계나 새 집계로 이동합니다.

+ 콘솔이 볼륨에 대한 새로운 집계를 생성하는 경우 해당 볼륨의 크기에 맞는 디스크 크기를 선택합니다.

+ 원래 집계에서 이제 사용 가능한 공간이 생겼다는 점에 유의하세요. 기존 볼륨이나 새로운 볼륨이 해당 공간을 사용할 수 있습니다. 이 시나리오에서는 해당 공간을 클라우드 제공자에게 반환할 수 없습니다.

- 집계에 12시간 이상 볼륨이 없으면 콘솔에서 해당 집계를 삭제합니다.

자동 용량 관리를 통한 **LUN** 관리

콘솔의 자동 용량 관리 기능은 LUN에 적용되지 않습니다. LUN을 생성하면 자동 증가 기능이 비활성화됩니다.

수동 용량 관리

조직 또는 계정 관리자가 *용량 관리 모드*를 수동으로 설정하면 콘솔에서 용량 결정에 대한 적절한 조치를 취하라는 메시지가 표시됩니다. 자동 모드에서 설명한 것과 동일한 예가 수동 모드에도 적용되지만, 작업을 수락하는 것은 사용자의 책임입니다.

자세히 알아보기

"용량 관리 모드를 수정하는 방법을 알아보세요" .

쓰기 속도

NetApp Console 사용하면 대부분의 Cloud Volumes ONTAP 구성에 대해 일반 또는 높은 쓰기 속도를 선택할 수 있습니다. 쓰기 속도를 선택하기 전에 일반 설정과 높은 설정의 차이점, 높은 쓰기 속도를 사용할 때의 위험과 권장 사항을 이해해야 합니다.

일반 쓰기 속도

일반 쓰기 속도를 선택하면 데이터가 디스크에 직접 기록됩니다. 데이터가 디스크에 직접 기록되면 계획되지 않은 시스템 중단이나 계획되지 않은 시스템 중단을 수반하는 연쇄적 장애가 발생할 경우 데이터 손실 가능성이 줄어듭니다(HA 쌍에만 해당).

기본 옵션은 일반 쓰기 속도입니다.

높은 쓰기 속도

높은 쓰기 속도를 선택하면 데이터는 디스크에 쓰기 전에 메모리에 버퍼링되므로 쓰기 성능이 더 빨라집니다. 이러한 캐싱으로 인해 계획되지 않은 시스템 중단이 발생하면 데이터가 손실될 가능성이 있습니다.

계획되지 않은 시스템 중단이 발생할 경우 손실될 수 있는 데이터 양은 마지막 두 일관성 지점의 범위입니다. 일관성 지점은 버퍼링된 데이터를 디스크에 쓰는 행위입니다. 일관성 지점은 쓰기 로그가 가득 차거나 10초가 지난 후(먼저 발생하는 경우)에 발생합니다. 하지만 클라우드 공급업체가 제공하는 스토리지의 성능은 일관성 지점 처리 시간에 영향을 미칠 수 있습니다.

높은 쓰기 속도를 사용해야 하는 경우

워크로드에 빠른 쓰기 성능이 필요하고 계획되지 않은 시스템 중단이나 계획되지 않은 시스템 중단을 수반하는 연쇄적 오류(HA 쌍에만 해당) 발생 시 데이터 손실 위험을 견딜 수 있는 경우 높은 쓰기 속도가 좋은 선택입니다.

고속 쓰기 속도 사용 시 권장 사항

높은 쓰기 속도를 활성화하는 경우 애플리케이션 계층에서 쓰기 보호를 보장하거나 데이터 손실이 발생할 경우 애플리케이션이 이를 허용할 수 있도록 해야 합니다.

AWS에서 HA 쌍을 사용한 높은 쓰기 속도

AWS에서 HA 쌍에 높은 쓰기 속도를 활성화하려는 경우 여러 가용 영역(AZ) 배포와 단일 AZ 배포 간의 보호 수준 차이를 이해해야 합니다. 여러 AZ에 HA 쌍을 배포하면 복원력이 높아지고 데이터 손실 가능성을 줄이는 데 도움이 될 수 있습니다.

"AWS의 HA 쌍에 대해 자세히 알아보세요" .

높은 쓰기 속도를 지원하는 구성

모든 Cloud Volumes ONTAP 구성이 높은 쓰기 속도를 지원하는 것은 아닙니다. 이러한 구성에서는 기본적으로 일반 쓰기 속도가 사용됩니다.

AWS

단일 노드 시스템을 사용하는 경우 Cloud Volumes ONTAP는 모든 인스턴스 유형에서 높은 쓰기 속도를 지원합니다.

9.8 릴리스부터 Cloud Volumes ONTAP m5.xlarge 및 r5.xlarge를 제외한 거의 모든 지원되는 EC2 인스턴스 유형을 사용할 때 HA 쌍으로 높은 쓰기 속도를 지원합니다.

"Cloud Volumes ONTAP 지원하는 Amazon EC2 인스턴스에 대해 자세히 알아보세요." .

하늘빛

단일 노드 시스템을 사용하는 경우 Cloud Volumes ONTAP는 모든 VM 유형에서 높은 쓰기 속도를 지원합니다.

HA 쌍을 사용하는 경우 Cloud Volumes ONTAP 9.8 릴리스부터 여러 VM 유형에서 높은 쓰기 속도를 지원합니다. 로 가다 "Cloud Volumes ONTAP 릴리스 노트" 높은 쓰기 속도를 지원하는 VM 유형을 확인하세요.

구글 클라우드

단일 노드 시스템을 사용하는 경우 Cloud Volumes ONTAP는 모든 머신 유형에서 높은 쓰기 속도를 지원합니다.

HA 쌍을 사용하는 경우 Cloud Volumes ONTAP 9.13.0 릴리스부터 여러 VM 유형에서 높은 쓰기 속도를 지원합니다. 로 가다 "Cloud Volumes ONTAP 릴리스 노트" 높은 쓰기 속도를 지원하는 VM 유형을 확인하세요.

"Cloud Volumes ONTAP 지원하는 Google Cloud 머신 유형에 대해 자세히 알아보세요." .

쓰기 속도를 선택하는 방법

새로운 Cloud Volumes ONTAP 시스템을 추가할 때 쓰기 속도를 선택할 수 있습니다."기존 시스템의 쓰기 속도 변경" .

데이터 손실이 발생할 경우 예상되는 상황

빠른 쓰기 속도로 인해 데이터 손실이 발생하면 이벤트 관리 시스템(EMS)은 다음 두 가지 이벤트를 보고합니다.

- Cloud Volumes ONTAP 9.12.1 이상

```
 NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* Cloud Volumes ONTAP 9.11.0~9.11.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
 ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect..
* Cloud Volumes ONTAP 9.8~9.10.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect.
```

이런 일이 발생하면 Cloud Volumes ONTAP 부팅되어 사용자 개입 없이도 데이터를 계속 제공할 수 있어야 합니다.

데이터 손실이 발생한 경우 데이터 액세스를 중지하는 방법

데이터 손실이 우려되는 경우, 데이터 손실 시 애플리케이션 실행을 중지하고 데이터 손실 문제가 적절히 해결된 후 데이터 액세스를 재개하려는 경우, CLI에서 NVFAIL 옵션을 사용하여 해당 목표를 달성할 수 있습니다.

NVFAIL 옵션을 활성화하려면

```
vol modify -volume <vol-name> -nvfail on
```

NVFAIL 설정을 확인하려면

```
vol show -volume <vol-name> -fields nvfail
```

NVFAIL 옵션을 비활성화하려면

```
vol modify -volume <vol-name> -nvfail off
```

데이터 손실이 발생하면 NVFAIL이 활성화된 NFS 또는 iSCSI 볼륨은 데이터 제공을 중단해야 합니다(상태 비저장 프로토콜인 CIFS에는 영향을 미치지 않습니다). 자세한 내용은 다음을 참조하세요. "NVFAIL이 NFS 볼륨 또는 LUN에 대한 액세스에 미치는 영향" .

NVFAIL 상태를 확인하려면

```
vol show -fields in-nvfailed-state
```

데이터 손실 문제가 적절히 해결되면 NVFAIL 상태를 지울 수 있으며 볼륨을 데이터 액세스에 사용할 수 있습니다.

NVFAIL 상태를 지우려면

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

Flash Cache

일부 Cloud Volumes ONTAP 구성에는 로컬 NVMe 스토리지가 포함되어 있으며, Cloud Volumes ONTAP 더 나은 성능을 위해 이를 _Flash Cache_로 사용합니다.

플래시 캐시란 무엇인가요?

Flash Cache는 최근 읽은 사용자 데이터와 NetApp 메타데이터를 실시간으로 지능적으로 캐싱하여 데이터 액세스 속도를 높입니다. 데이터베이스, 이메일, 파일 서비스 등 무작위 읽기 작업이 많은 작업에 효과적입니다.

지원되는 구성

Flash Cache는 특정 Cloud Volumes ONTAP 구성에서 지원됩니다. 지원되는 구성을 보려면 "Cloud Volumes ONTAP 릴리스 노트"

제한 사항

- AWS에서 Cloud Volumes ONTAP 9.12.0 이하 버전에 대해 Flash Cache를 구성하는 경우 Flash Cache 성능 향상을 활용하려면 모든 볼륨에서 압축을 비활성화해야 합니다. Cloud Volumes ONTAP 9.12.1 이상을 배포하거나 업그레이드하는 경우 압축을 비활성화할 필요가 없습니다.

  NetApp Console 에서 볼륨을 생성할 때 스토리지 효율성 설정 선택을 건너뛰거나 볼륨을 생성한 다음 "CLI를 사용하여 데이터 압축을 비활성화합니다." .

- Cloud Volumes ONTAP 에서는 재부팅 후 캐시 재가동이 지원되지 않습니다.

관련 주제

- "AWS의 Cloud Volumes ONTAP 에 지원되는 구성"
- "Azure의 Cloud Volumes ONTAP 에 지원되는 구성"
- "Google Cloud에서 Cloud Volumes ONTAP에 대해 지원되는 구성"

Cloud Volumes ONTAP 의 WORM 스토리지에 대해 알아보세요

Cloud Volumes ONTAP 시스템에서 WORM(Write Once, Read Many) 스토리지를 활성화하여 지정된 보존 기간 동안 수정되지 않은 형태로 파일을 보존할 수 있습니다. 클라우드 WORM 스토리지는 SnapLock 기술을 기반으로 하며, 이는 WORM 파일이 파일 수준에서 보호된다는 것을 의미합니다.

WORM 기능은 추가 비용 없이 BYOL(Bring Your Own License) 및 마켓플레이스 구독을 통해 라이선스를 구매할 때 사용할 수 있습니다. 현재 라이선스에 WORM을 추가하려면 NetApp 영업 담당자에게 문의하세요.

WORM 스토리지 작동 방식

파일이 WORM 저장소에 커밋되면 보존 기간이 만료된 후에도 해당 파일을 수정할 수 없습니다. 변조 방지 시계는 WORM 파일의 보존 기간이 경과한 시점을 판별합니다.

보관 기간이 경과한 후에는 더 이상 필요하지 않은 파일을 삭제해야 합니다.

WORM 스토리지 활성화

WORM 스토리지를 활성화하는 방법은 사용 중인 Cloud Volumes ONTAP 버전에 따라 달라집니다.

버전 9.10.1 이상

Cloud Volumes ONTAP 9.10.1부터 볼륨 수준에서 WORM을 활성화하거나 비활성화하는 옵션이 제공됩니다.

Cloud Volumes ONTAP 시스템을 추가하면 WORM 스토리지를 활성화하거나 비활성화하라는 메시지가 표시됩니다.

- 시스템을 추가할 때 WORM 스토리지를 활성화하면 NetApp Console 에서 생성하는 모든 볼륨에 WORM이 활성화됩니다. 하지만 ONTAP 시스템 관리자나 ONTAP CLI를 사용하면 WORM이 비활성화된 볼륨을 생성할 수 있습니다.
- 시스템을 추가할 때 WORM 저장소를 비활성화하면 콘솔, ONTAP 시스템 관리자 또는 ONTAP CLI에서 생성하는 모든 볼륨에서 WORM이 비활성화됩니다.

버전 9.10.0 및 이전 버전

새로운 시스템을 추가할 때 Cloud Volumes ONTAP 시스템에서 WORM 스토리지를 활성화할 수 있습니다. 콘솔에서 생성하는 모든 볼륨에는 WORM이 활성화되어 있습니다. 개별 볼륨에서 WORM 저장소를 비활성화할 수 없습니다.

WORM에 파일 커밋

NFS 또는 CIFS를 통해 WORM에 파일을 커밋하려면 애플리케이션을 사용하거나 ONTAP CLI를 사용하여 자동으로 파일을 WORM에 커밋할 수 있습니다. 또한 WORM 추가 가능 파일을 사용하여 로그 정보와 같이 증분적으로 기록되는 데이터를 보관할 수 있습니다.

Cloud Volumes ONTAP 시스템에서 WORM 스토리지를 활성화한 후에는 WORM 스토리지의 모든 관리에 ONTAP CLI를 사용해야 합니다. 지침은 다음을 참조하세요. "SnapLock 에 대한 ONTAP 문서" .

Cloud Volumes ONTAP 시스템에서 WORM 활성화

콘솔에서 Cloud Volumes ONTAP 시스템을 생성할 때 WORM 스토리지를 활성화할 수 있습니다. 생성 중에 WORM이 활성화되지 않은 경우에도 시스템에서 WORM을 활성화할 수 있습니다. WORM을 활성화한 후에는 비활성화할 수 없습니다.

이 작업에 관하여

- WORM은 ONTAP 9.10.1 이상에서 지원됩니다.
- 백업 기능이 있는 WORM은 ONTAP 9.11.1 이상에서 지원됩니다.

단계

1. 시스템 페이지에서 WORM을 활성화하려는 시스템의 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 **WORM** 옆에 있는 연필 아이콘을 클릭합니다.

   시스템에서 WORM이 이미 활성화된 경우 연필 아이콘은 비활성화됩니다.

3. **WORM** 페이지에서 클러스터 규정 준수 시계의 보존 기간을 설정합니다.

   자세한 내용은 다음을 참조하세요. "ONTAP 설명서: 규정 준수 시계 초기화" .

4. *설정*을 클릭하세요.

당신이 완료한 후

*WORM*의 상태는 기능 패널에서 확인할 수 있습니다. WORM이 활성화되면 SnapLock 라이선스가 클러스터에 자동으로 설치됩니다. ONTAP System Manager에서 SnapLock 라이선스를 볼 수 있습니다.

WORM 파일 삭제

권한 있는 삭제 기능을 사용하여 보존 기간 동안 WORM 파일을 삭제할 수 있습니다.

지침은 다음을 참조하세요. "ONTAP 문서" .

WORM 및 데이터 계층화

새로운 Cloud Volumes ONTAP 9.8 시스템 이상을 만들면 데이터 계층화와 WORM 스토리지를 함께 활성화할 수 있습니다. WORM 스토리지를 사용하여 데이터 계층화를 활성화하면 클라우드의 개체 저장소에 데이터를 계층화할 수 있습니다.

데이터 계층화와 WORM 스토리지를 모두 활성화하는 데 필요한 다음 사항을 이해해야 합니다.

- 개체 스토리지에 계층화된 데이터에는 ONTAP WORM 기능이 포함되지 않습니다. 엔드투엔드 WORM 기능을 보장하려면 버킷 권한을 올바르게 설정해야 합니다.
- 개체 스토리지에 계층화된 데이터에는 WORM 기능이 없으므로, 기술적으로 버킷과 컨테이너에 대한 전체 액세스 권한이 있는 사람은 누구나 ONTAP 에 의해 계층화된 개체를 삭제할 수 있습니다.
- WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로 되돌리거나 다운그레이드하는 것이 차단됩니다.

제한 사항

- Cloud Volumes ONTAP 의 WORM 스토리지는 "신뢰할 수 있는 스토리지 관리자" 모델에 따라 작동합니다. WORM 파일은 변경이나 수정으로부터 보호되지만, 볼륨에 만료되지 않은 WORM 데이터가 포함되어 있더라도 클러스터 관리자가 볼륨을 삭제할 수 있습니다.
- 신뢰할 수 있는 스토리지 관리자 모델 외에도 Cloud Volumes ONTAP 의 WORM 스토리지는 암묵적으로 "신뢰할 수 있는 클라우드 관리자" 모델에 따라 작동합니다. 클라우드 관리자는 클라우드 제공자로부터 직접 클라우드 스토리지를 제거하거나 편집하여 만료일 전에 WORM 데이터를 삭제할 수 있습니다.

관련 링크

- "WORM 스토리지를 위한 변조 방지 스냅샷 복사본 생성"
- "Cloud Volumes ONTAP 의 라이선싱 및 요금 청구"

고가용성 쌍

AWS의 **Cloud Volumes ONTAP HA** 쌍에 대해 알아보세요

Cloud Volumes ONTAP 고가용성(HA) 구성은 중단 없는 운영과 내결함성을 제공합니다. AWS에서는 데이터가 두 노드 간에 동기적으로 미러링됩니다.

HA 구성 요소

AWS에서 Cloud Volumes ONTAP HA 구성에는 다음 구성 요소가 포함됩니다.

- 두 개의 Cloud Volumes ONTAP 노드의 데이터가 서로 동기적으로 미러링됩니다.
- 저장소 인수 및 반환 프로세스를 지원하기 위해 노드 간 통신 채널을 제공하는 중재자 인스턴스입니다.

중재인

AWS의 중재자 인스턴스에 대한 몇 가지 주요 세부 정보는 다음과 같습니다.

인스턴스 유형
: t3-마이크로

디스크
: 8GiB와 4GiB의 두 개의 st1 디스크

운영 체제
: 데비안 11

Cloud Volumes ONTAP 9.10.0 및 이전 버전의 경우, Debian 10이 메디에이터에 설치되었습니다.

업그레이드
: Cloud Volumes ONTAP 업그레이드하면 NetApp Console 도 필요에 따라 중재자 인스턴스를 업데이트합니다.

인스턴스에 대한 액세스
: 콘솔에서 Cloud Volumes ONTAP HA 쌍을 생성하면 중재자 인스턴스에 대한 키 쌍을 제공하라는 메시지가 표시됩니다. SSH 액세스를 위해 해당 키 쌍을 사용할 수 있습니다. `admin` 사용자.

제3자 에이전트
: 중재자 인스턴스에서는 타사 에이전트나 VM 확장이 지원되지 않습니다.

저장소 인수 및 반환

노드 하나가 다운되더라도 다른 노드는 파트너에게 데이터를 제공하여 지속적인 데이터 서비스를 제공할 수 있습니다. 데이터가 파트너에 동기적으로 미러링되었기 때문에 클라이언트는 파트너 노드에서 동일한 데이터에 액세스할 수 있습니다.

노드가 재부팅된 후 파트너는 저장소를 반환하기 전에 데이터를 다시 동기화해야 합니다. 데이터를 다시 동기화하는 데 걸리는 시간은 노드가 다운된 동안 얼마나 많은 데이터가 변경되었는지에 따라 달라집니다.

저장소 인수, 재동기화 및 반환은 모두 기본적으로 자동으로 수행됩니다. 사용자 작업이 필요하지 않습니다.

RPO와 RTO

HA 구성은 다음과 같이 데이터의 고가용성을 유지합니다.

- 복구 지점 목표(RPO)는 0초입니다. 귀하의 데이터는 데이터 손실 없이 거래적으로 일관성을 유지합니다.
- 복구 시간 목표(RTO)는 120초입니다. 정전이 발생하더라도 120초 이내에 데이터를 사용할 수 있어야 합니다.

HA 배포 모델

여러 가용성 영역(AZ) 또는 단일 가용성 영역(AZ)에 HA 구성을 배포하여 데이터의 높은 가용성을 보장할 수 있습니다. 각 구성에 대한 자세한 내용을 검토하여 귀하의 요구 사항에 가장 적합한 구성을 선택하시기 바랍니다.

여러 가용성 영역

여러 가용성 영역(AZ)에 HA 구성을 배포하면 Cloud Volumes ONTAP 노드를 실행하는 AZ 또는 인스턴스에 장애가 발생하더라도 데이터의 고가용성이 보장됩니다. NAS IP 주소가 데이터 액세스와 스토리지 장애 조치에 어떤 영향을 미치는지 이해해야 합니다.

NFS 및 CIFS 데이터 액세스

HA 구성이 여러 가용성 영역에 걸쳐 분산되어 있는 경우 _유동 IP 주소_를 사용하면 NAS 클라이언트 액세스가 가능합니다. 해당 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 하는 유동 IP 주소는 장애가 발생하면 노드 간에 마이그레이션될 수 있습니다. VPC 외부에 있는 클라이언트는 기본적으로 액세스할 수 없습니다."AWS 전송 게이트웨이 설정" .

트랜짓 게이트웨이를 설정할 수 없는 경우 VPC 외부에 있는 NAS 클라이언트에서 개인 IP 주소를 사용할 수 있습니다. 하지만 이러한 IP 주소는 정적이므로 노드 간에 장애 조치를 취할 수 없습니다.

여러 가용성 영역에 HA 구성을 배포하기 전에 부동 IP 주소와 경로 테이블에 대한 요구 사항을 검토해야 합니다. 구성을 배포할 때 부동 IP 주소를 지정해야 합니다. 개인 IP 주소는 자동으로 생성됩니다.

자세한 내용은 다음을 참조하세요. "여러 AZ에서 Cloud Volumes ONTAP HA에 대한 AWS 네트워킹 요구 사항" .

iSCSI 데이터 액세스

iSCSI는 유동 IP 주소를 사용하지 않으므로 VPC 간 데이터 통신은 문제가 되지 않습니다.

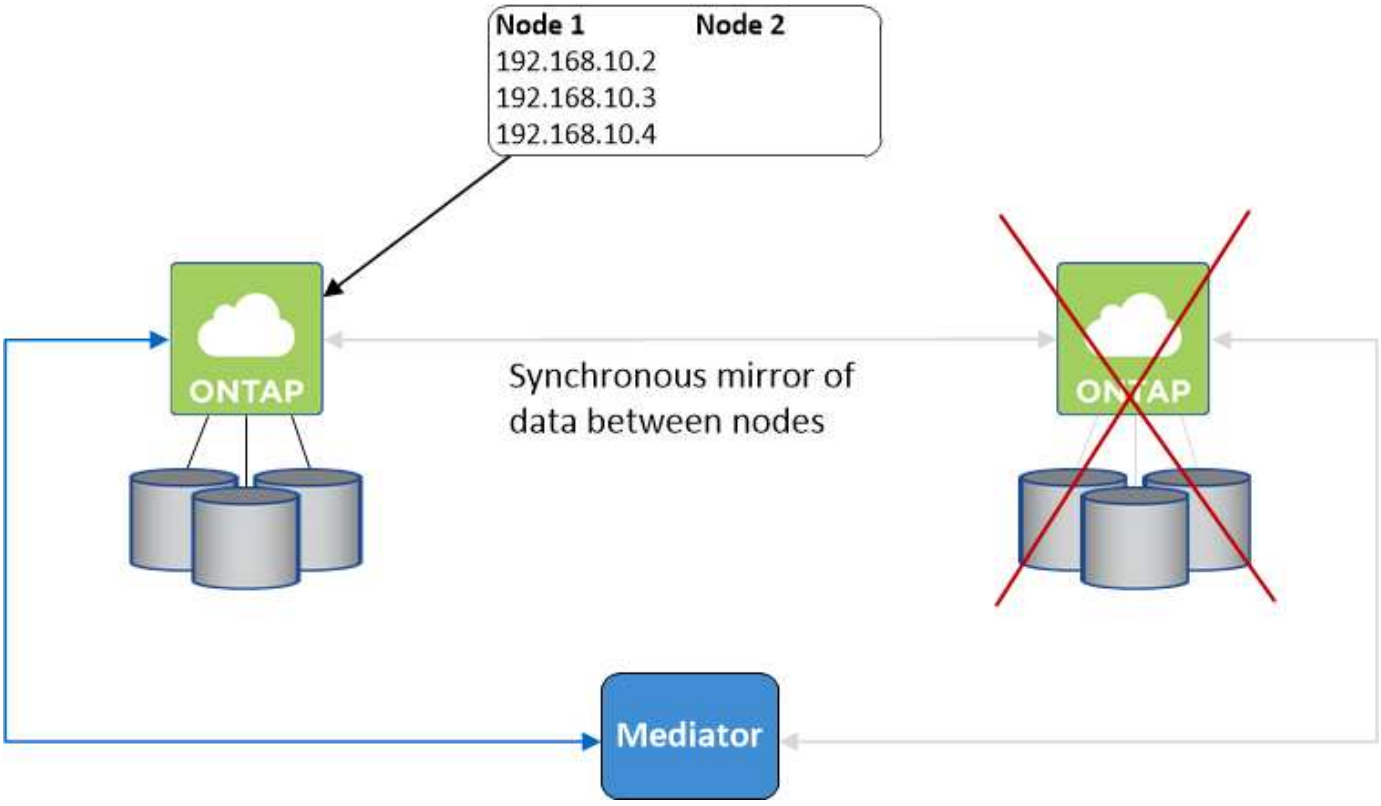
iSCSI 인수 및 환원

iSCSI의 경우 Cloud Volumes ONTAP 다중 경로 I/O(MPIO) 및 비대칭 논리 단위 액세스(ALUA)를 사용하여 활성 최적화 경로와 최적화되지 않은 경로 간의 경로 장애 조치를 관리합니다.

ALUA를 지원하는 특정 호스트 구성에 대한 정보는 다음을 참조하십시오. "NetApp 상호 운용성 매트릭스 도구" 그리고 "SAN 호스트 및 클라우드 클라이언트 가이드" 호스트 운영 체제에 맞게.

NAS 인수 및 환원

유동 IP를 사용하는 NAS 구성에서 인수가 발생하면 클라이언트가 데이터에 액세스하는 데 사용하는 노드의 유동 IP 주소가 다른 노드로 이동합니다. 다음 이미지는 플로팅 IP를 사용한 NAS 구성에서의 스토리지 인수를 보여줍니다. 노드 2가 다운되면 노드 2의 플로팅 IP 주소가 노드 1로 이동합니다.



장애가 발생하면 외부 VPC 액세스에 사용되는 NAS 데이터 IP는 노드 간에 마이그레이션할 수 없습니다. 노드가 오프라인 상태가 되면 다른 노드의 IP 주소를 사용하여 VPC 외부의 클라이언트에 볼륨을 수동으로 다시 마운트해야 합니다.

실패한 노드가 다시 온라인 상태가 되면 원래 IP 주소를 사용하여 클라이언트를 볼륨에 다시 마운트합니다. 이 단계는 두 HA 노드 간에 불필요한 데이터 전송을 방지하기 위해 필요합니다. 불필요한 데이터 전송은 성능과 안정성에 상당한 영향을 미칠 수 있습니다.

볼륨을 선택하고 *마운트 명령*을 클릭하면 콘솔에서 올바른 IP 주소를 찾을 수 있습니다.

단일 가용성 영역

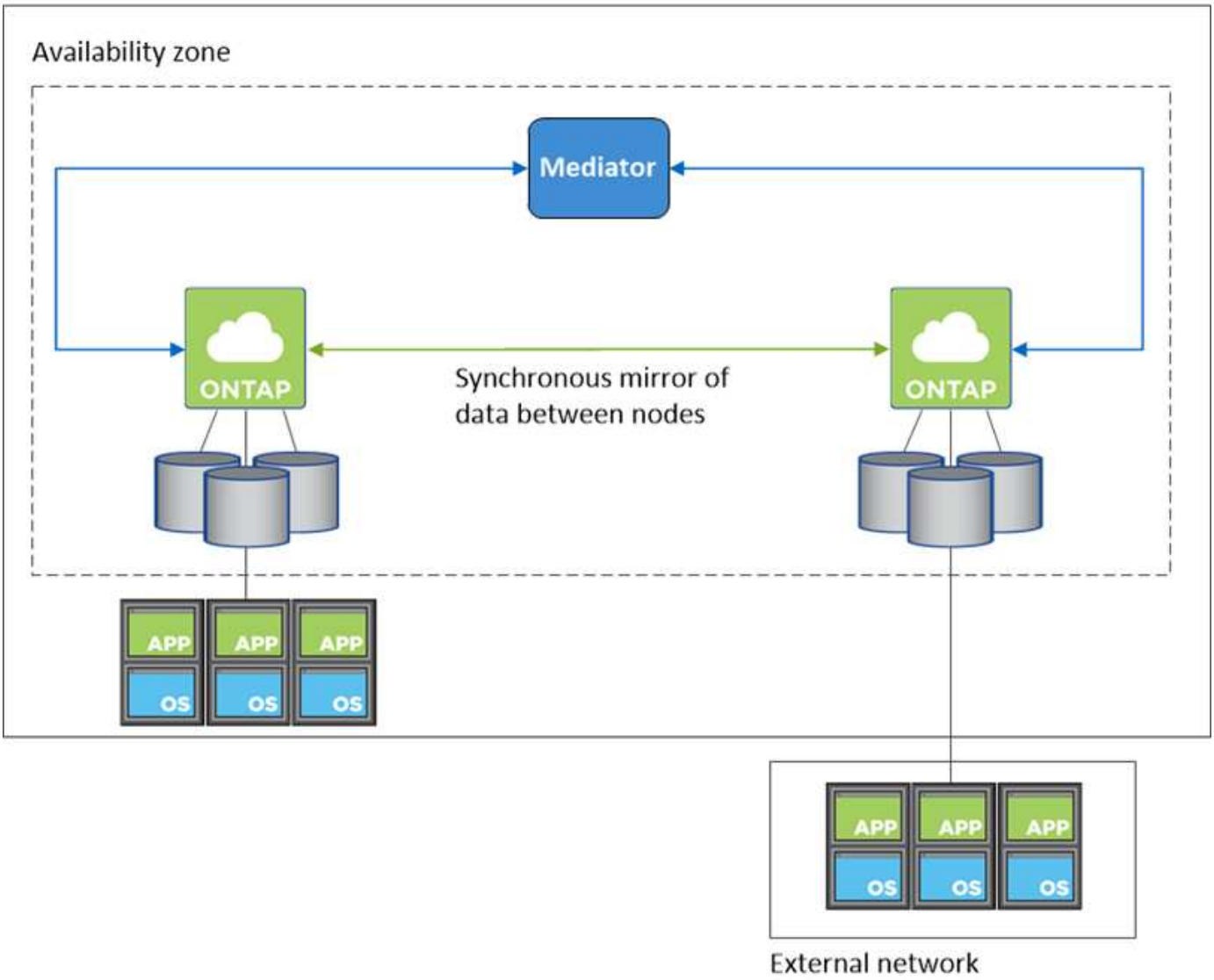
단일 가용성 영역(AZ)에 HA 구성을 배포하면 Cloud Volumes ONTAP 노드를 실행하는 인스턴스에 장애가 발생하더라도 데이터의 고가용성을 보장할 수 있습니다. 모든 데이터는 기본적으로 VPC 외부에서 접근할 수 있습니다.

콘솔은 다음을 생성합니다. "AWS 문서: AWS 스프레드 배치 그룹" 그리고 해당 배치 그룹에서 두 개의 HA 노드를 시작합니다. 배치 그룹은 인스턴스를 여러 기본 하드웨어에 분산하여 동시 장애가 발생할 위험을 줄입니다. 이 기능은 디스크 오류 관점이 아닌 컴퓨팅 관점에서 중복성을 향상시킵니다.

데이터 접근

이 구성은 단일 AZ에 있으므로 유동 IP 주소가 필요하지 않습니다. VPC 내부와 외부에서 데이터에 액세스하는 데 동일한 IP 주소를 사용할 수 있습니다.

다음 이미지는 단일 AZ의 HA 구성을 보여줍니다. VPC 내부와 외부에서 데이터에 접근할 수 있습니다.



인수와 환원

iSCSI의 경우 Cloud Volumes ONTAP 다중 경로 I/O(MPIO) 및 비대칭 논리 단위 액세스(ALUA)를 사용하여 활성 최적화 경로와 최적화되지 않은 경로 간의 경로 장애 조치를 관리합니다.

ALUA를 지원하는 특정 호스트 구성에 대한 정보는 다음을 참조하십시오. "NetApp 상호 운용성 매트릭스 도구" 그리고 "SAN 호스트 및 클라우드 클라이언트 가이드" 호스트 운영 체제에 맞게.

NAS 구성의 경우 장애가 발생하면 데이터 IP 주소가 HA 노드 간에 마이그레이션될 수 있습니다. 이를 통해 클라이언트가 저장소에 액세스할 수 있습니다.

AWS 로컬 영역

AWS 로컬 존은 스토리지, 컴퓨팅, 데이터베이스 및 기타 선택된 AWS 서비스가 대도시와 산업 지역 근처에 위치하는 인프라 배포입니다. AWS 로컬 존을 사용하면 AWS 서비스를 사용자에게 더 가깝게 제공하여 워크로드의 지연 시간을 개선하고 데이터베이스를 로컬로 유지 관리할 수 있습니다. Cloud Volumes ONTAP 에서

AWS 로컬 영역에는 단일 AZ 또는 여러 AZ 구성을 배포할 수 있습니다.

AWS 로컬 영역은 표준 모드와 프라이빗 모드에서 콘솔을 사용할 때 지원됩니다. 현재 AWS 로컬 영역은 제한 모드에서 지원되지 않습니다.

AWS 로컬 영역 구성 예

AWS의 Cloud Volumes ONTAP 단일 가용성 영역에서만 고가용성(HA) 모드를 지원합니다. 단일 노드 배포는 지원되지 않습니다.

Cloud Volumes ONTAP AWS 로컬 영역에서 데이터 계층화, 클라우드 계층화 및 비적격 인스턴스를 지원하지 않습니다.

다음은 구성의 예입니다.

- 단일 가용성 영역: 클러스터 노드와 중재자가 모두 동일한 로컬 영역에 있습니다.
- 여러 가용성 영역 여러 가용성 영역 구성에는 인스턴스 3개, 노드 2개, 중재자 1개가 있습니다. 세 개의 인스턴스 중 하나는 별도의 영역에 있어야 합니다. 설정 방법은 사용자가 선택할 수 있습니다.

  다음은 세 가지 구성 예입니다.

  - 각 클러스터 노드는 다른 로컬 영역에 있고 중재자는 공용 가용성 영역에 있습니다.
  - 로컬 영역에 있는 한 클러스터 노드, 로컬 영역에 있는 중재자, 그리고 가용성 영역에 있는 두 번째 클러스터 노드.
  - 각 클러스터 노드와 중재자는 별도의 로컬 영역에 있습니다.

지원되는 디스크 및 인스턴스 유형

지원되는 디스크 유형은 GP2뿐입니다. 현재 지원되는 EC2 인스턴스 유형 패밀리는 xlarge에서 4xlarge까지입니다.

- M5
- C5
- C5d
- R5
- R5d

Cloud Volumes ONTAP는 이러한 구성만 지원합니다. AWS Local Zone 구성에서 지원되지 않는 디스크 유형 또는 부적격 인스턴스를 선택하면 배포가 실패할 수 있습니다. Cloud Volumes ONTAP 시스템이 AWS Local Zone에 있는 경우 Amazon Simple Storage Service(Amazon S3)로의 데이터 계층화는 지원되지 않습니다. Local Zone 외부의 Amazon S3 버킷에 액세스하면 지연 시간이 증가하고 Cloud Volumes ONTAP 활동에 영향을 미치기 때문입니다.

"AWS 설명서: 로컬 영역의 EC2 인스턴스 유형" .

HA 쌍에서 스토리지가 작동하는 방식

ONTAP 클러스터와 달리 Cloud Volumes ONTAP HA 쌍의 스토리지는 노드 간에 공유되지 않습니다. 대신, 데이터는 노드 간에 동기적으로 미러링되므로 장애가 발생하더라도 데이터를 사용할 수 있습니다.

저장 공간 할당

새 볼륨을 생성하고 추가 디스크가 필요한 경우 콘솔은 두 노드에 동일한 수의 디스크를 할당하고 미러링된 집계를 만든 다음 새 볼륨을 생성합니다. 예를 들어, 볼륨에 두 개의 디스크가 필요한 경우 콘솔은 노드당 두 개의 디스크를 할당하여 총 4개의 디스크를 할당합니다.

스토리지 구성

HA 쌍을 액티브-액티브 구성으로 사용할 수 있습니다. 이 경우 두 노드 모두 클라이언트에 데이터를 제공하고, 액티브-패시브 구성으로 사용할 경우 패시브 노드는 액티브 노드의 스토리지를 인수한 경우에만 데이터 요청에 응답합니다.

스토리지 시스템 뷰에서 콘솔을 사용할 때만 액티브-액티브 구성을 설정할 수 있습니다.

성과 기대치

Cloud Volumes ONTAP HA 구성은 노드 간에 데이터를 동기적으로 복제하므로 네트워크 대역폭을 소모합니다. 결과적으로 단일 노드 Cloud Volumes ONTAP 구성과 비교했을 때 다음과 같은 성능을 기대할 수 있습니다.

- 단일 노드에서만 데이터를 제공하는 HA 구성의 경우, 읽기 성능은 단일 노드 구성의 읽기 성능과 비슷하지만 쓰기 성능은 낮습니다.
- 두 노드 모두에서 데이터를 제공하는 HA 구성의 경우, 읽기 성능은 단일 노드 구성의 읽기 성능보다 높고, 쓰기 성능은 동일하거나 더 높습니다.

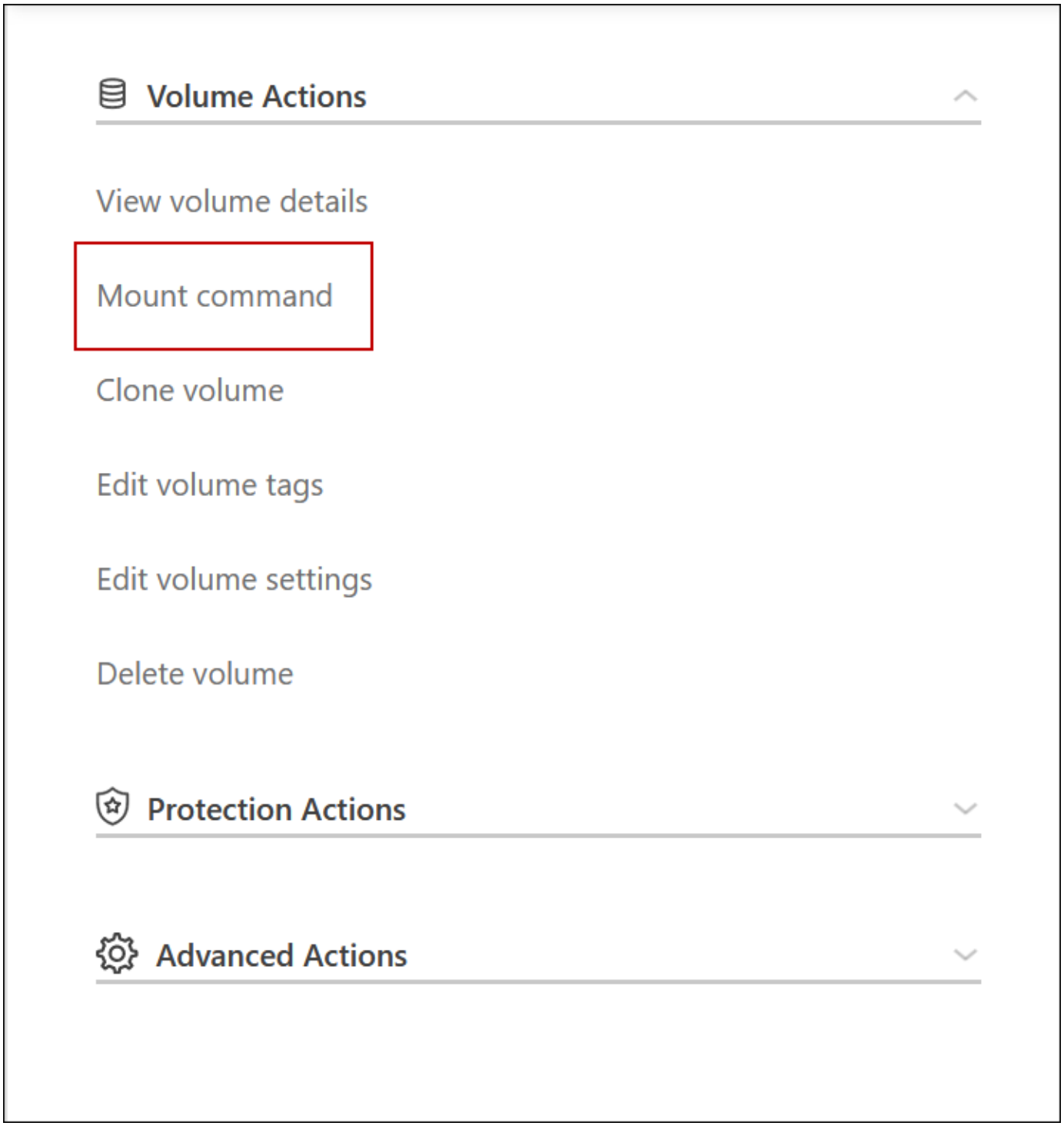
Cloud Volumes ONTAP 성능에 대한 자세한 내용은 다음을 참조하세요."성능" .

저장소에 대한 클라이언트 액세스

클라이언트는 볼륨이 있는 노드의 데이터 IP 주소를 사용하여 NFS 및 CIFS 볼륨에 액세스해야 합니다. NAS 클라이언트가 파트너 노드의 IP 주소를 사용하여 볼륨에 액세스하는 경우 트래픽이 두 노드 사이를 이동하게 되어 성능이 저하됩니다.

HA 쌍의 노드 간에 볼륨을 이동하는 경우 다른 노드의 IP 주소를 사용하여 볼륨을 다시 마운트해야 합니다. 그렇지 않으면 성능이 저하될 수 있습니다. 클라이언트가 CIFS에 대한 NFSv4 참조 또는 폴더 리디렉션을 지원하는 경우 Cloud Volumes ONTAP 시스템에서 해당 기능을 활성화하여 볼륨을 다시 마운트하지 않아도 됩니다. 자세한 내용은 ONTAP 문서를 참조하세요.

볼륨 관리 패널의 마운트 명령 옵션을 통해 올바른 IP 주소를 쉽게 식별할 수 있습니다.

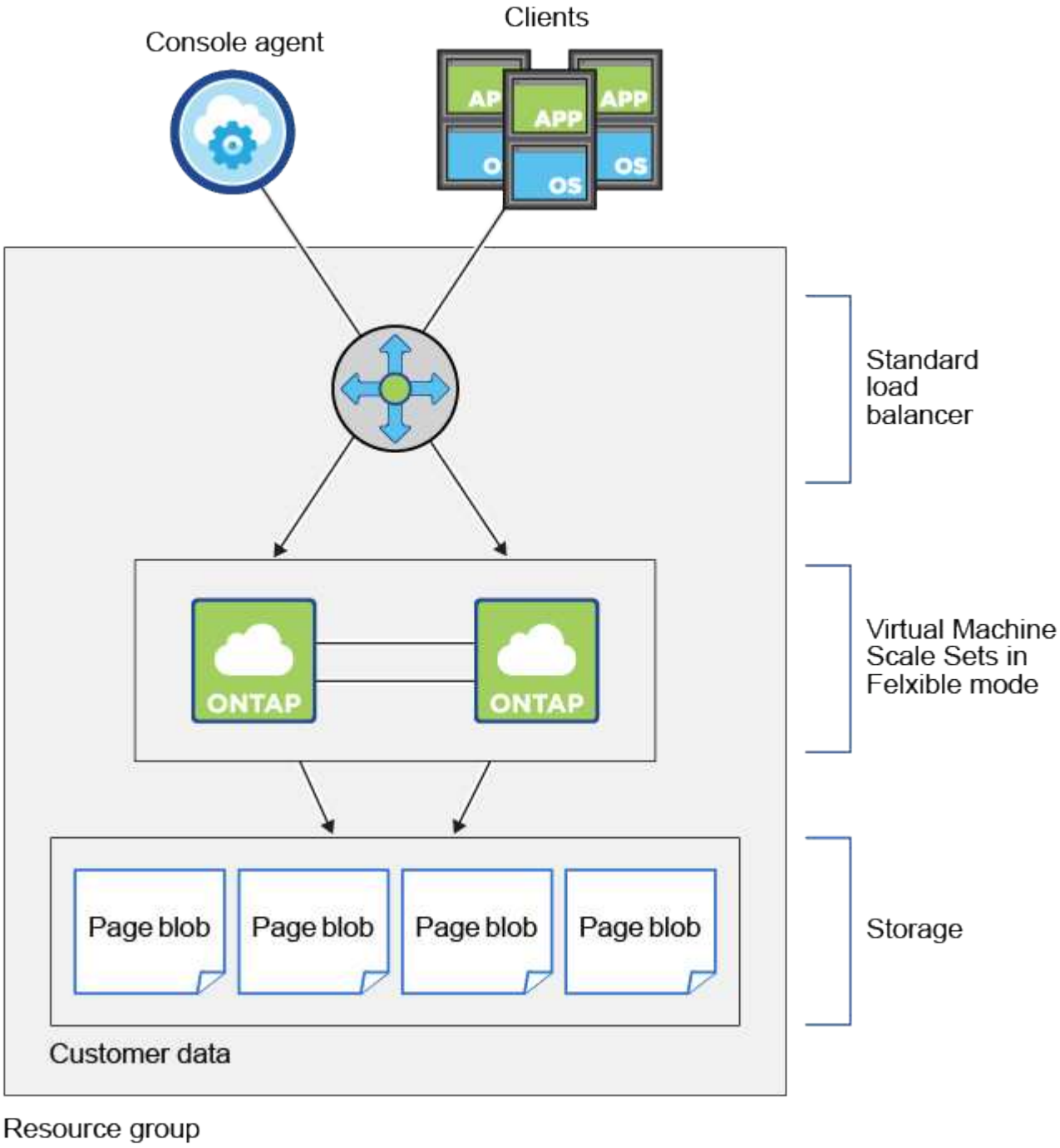


Azure의 Cloud Volumes ONTAP HA 쌍에 대해 알아보세요

Cloud Volumes ONTAP 고가용성(HA) 쌍은 클라우드 환경에서 장애가 발생하더라도 기업의 안정성과 지속적인 운영을 제공합니다. Azure에서는 두 노드 간에 저장소가 공유됩니다.

HA 구성 요소

Azure의 Cloud Volumes ONTAP HA 페이지 Blob 구성에는 다음 구성 요소가 포함됩니다.



NetApp Console 배포하는 Azure 구성 요소에 대해 다음 사항을 참고하세요.

Azure 표준 부하 분산 장치

로드 밸런서는 Cloud Volumes ONTAP HA 쌍으로 들어오는 트래픽을 관리합니다.

단일 가용성 영역의 **VM**

Cloud Volumes ONTAP 9.15.1부터 단일 가용성 영역(AZ)에서 이기종 가상 머신(VM)을 만들고 관리할 수 있습니다. 동일한 AZ 내의 별도의 장애 도메인에 고가용성(HA) 노드를 배포하여 최적의 가용성을 보장할 수

있습니다. 이 기능을 활성화하는 유연한 오케스트레이션 모드에 대해 자세히 알아보려면 다음을 참조하세요. "Microsoft Azure 설명서: 가상 머신 확장 집합" .

디스크

고객 데이터는 프리미엄 스토리지 페이지 블롭에 저장됩니다. 각 노드는 다른 노드의 저장소에 접근할 수 있습니다. 추가 저장 공간도 필요합니다."부트, 루트 및 코어 데이터" .

저장 계정

- 관리 디스크에는 하나의 스토리지 계정이 필요합니다.
- 스토리지 계정당 디스크 용량 한도에 도달했으므로 프리미엄 스토리지 페이지 Blob에 하나 이상의 스토리지 계정이 필요합니다.

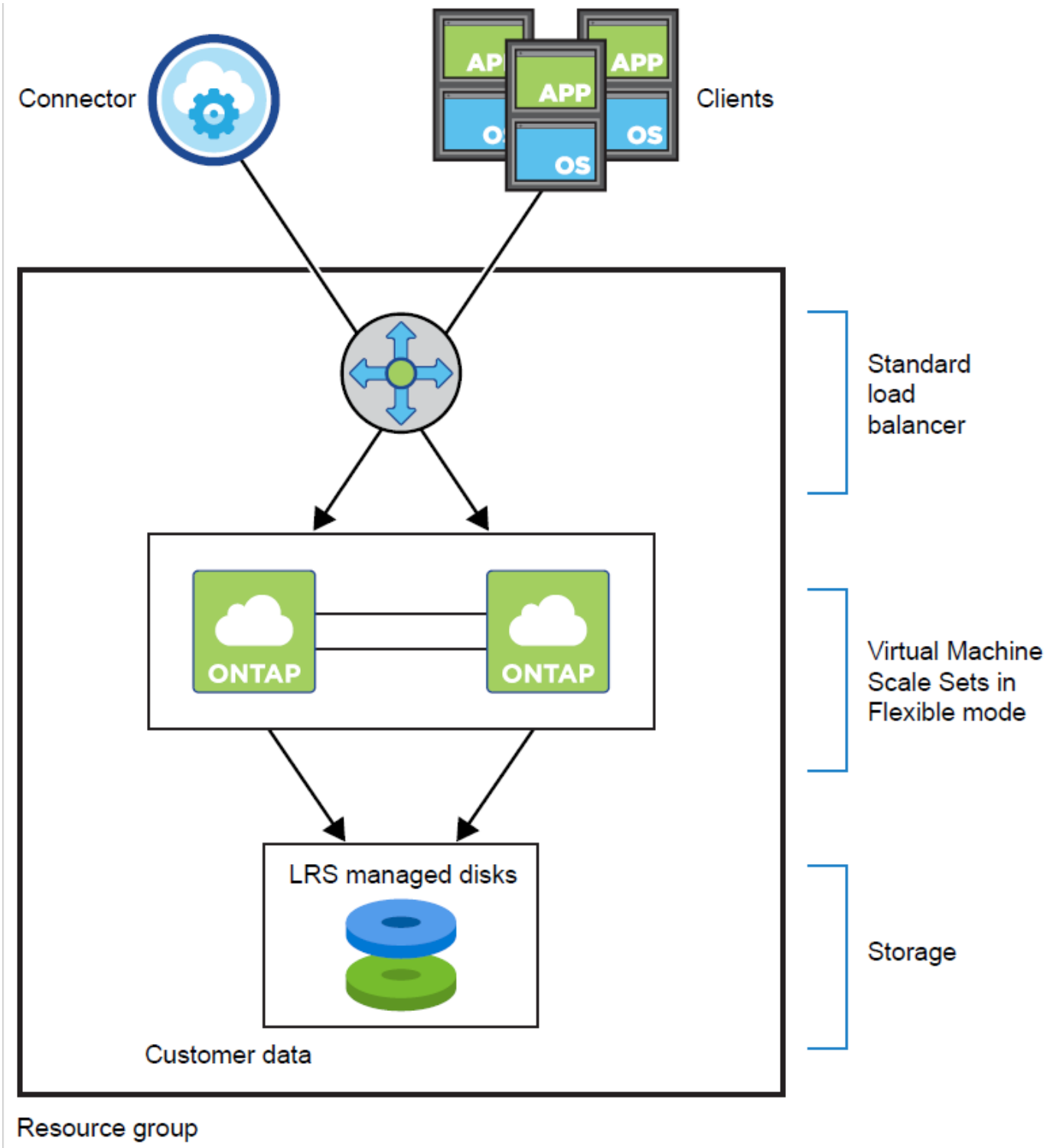
  "Microsoft Azure 설명서: 저장소 계정에 대한 Azure Storage 확장성 및 성능 목표" .

- Azure Blob Storage에 데이터를 계층화하려면 하나의 스토리지 계정이 필요합니다.
- Cloud Volumes ONTAP 9.7부터 콘솔이 HA 쌍에 대해 생성하는 스토리지 계정은 일반 용도의 v2 스토리지 계정입니다.
- Cloud Volumes ONTAP 시스템을 추가할 때 Cloud Volumes ONTAP 9.7 HA 쌍에서 Azure 스토리지 계정으로 HTTPS 연결을 활성화할 수 있습니다. 이 옵션을 활성화하면 쓰기 성능에 영향을 줄 수 있습니다. 시스템을 만든 후에는 설정을 변경할 수 없습니다.

Cloud Volumes ONTAP 9.15.0P1부터 새로운 고가용성 쌍 배포에 대해 Azure 페이지 Blob이 더 이상 지원되지 않습니다. 현재 기존 고가용성 쌍 배포에서 Azure 페이지 Blob을 사용하는 경우 Edsv4 시리즈 VM 및 Edsv5 시리즈 VM에서 최신 VM 인스턴스 유형으로 마이그레이션할 수 있습니다. "Azure에서 지원되는 구성에 대해 자세히 알아보세요." .

공유 관리 디스크를 사용한 **HA** 단일 가용성 영역 구성

공유 관리 디스크 위에서 실행되는 Cloud Volumes ONTAP HA 단일 가용성 영역 구성에는 다음 구성 요소가 포함됩니다.



콘솔에서 배포하는 Azure 구성 요소에 대해 다음 사항을 참고하세요.

Azure 표준 부하 분산 장치

로드 밸런서는 Cloud Volumes ONTAP HA 쌍으로 들어오는 트래픽을 관리합니다.

단일 가용성 영역의 **VM**

Cloud Volumes ONTAP 9.15.1부터 단일 가용성 영역(AZ)에서 이기종 가상 머신(VM)을 만들고 관리할 수 있습니다. 동일한 AZ 내의 별도의 장애 도메인에 고가용성(HA) 노드를 배포하여 최적의 가용성을 보장할 수 있습니다. 이 기능을 활성화하는 유연한 오케스트레이션 모드에 대해 자세히 알아보려면 다음을 참조하세요.

"Microsoft Azure 설명서: 가상 머신 확장 집합" .

다음 조건이 충족되면 영역 배포에서는 프리미엄 SSD v2 관리 디스크를 사용합니다.

- Cloud Volumes ONTAP 버전은 9.15.1 이상입니다.
- 선택한 지역 및 영역은 Premium SSD v2 Managed Disks를 지원합니다. 지원되는 지역에 대한 정보는 다음을 참조하세요. "Microsoft Azure 웹사이트: 지역별 사용 가능한 제품" .
- 구독은 Microsoft에 등록되었습니다."Microsoft.Compute/VMOrchestratorZonalMultiFD 기능" .

위의 기준을 충족하는 환경에 대해 프리미엄 SSD 관리형 디스크를 선택하면 콘솔에서 프리미엄 SSD v2 관리형 디스크를 자동으로 배포합니다. Premium SSD v1 Managed Disks로 전환할 수 없습니다.

디스크

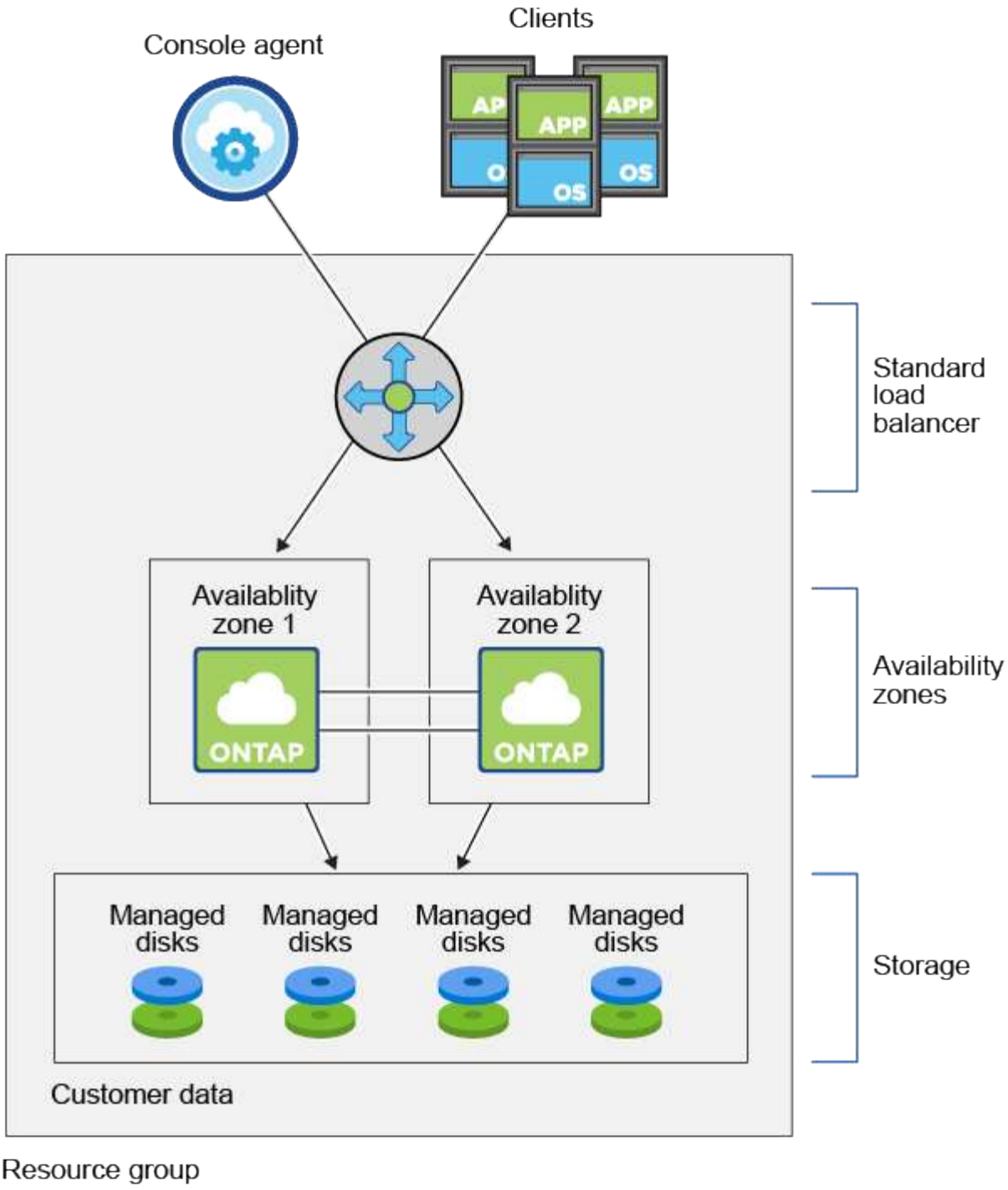
고객 데이터는 로컬 중복 스토리지(LRS) 관리 디스크에 저장됩니다. 각 노드는 다른 노드의 저장소에 접근할 수 있습니다. 추가 저장 공간도 필요합니다."부팅, 루트, 파트너 루트, 코어 및 NVRAM 데이터" .

저장 계정

스토리지 계정은 진단 로그를 처리하고 Blob 스토리지로 계층화하기 위해 관리형 디스크 기반 배포에 사용됩니다.

HA 다중 가용성 영역 구성

Azure의 Cloud Volumes ONTAP HA 다중 가용성 영역 구성에는 다음 구성 요소가 포함됩니다.



콘솔에서 배포하는 Azure 구성 요소에 대해 다음 사항을 참고하세요.

Azure 표준 부하 분산 장치

로드 밸런서는 Cloud Volumes ONTAP HA 쌍으로 들어오는 트래픽을 관리합니다.

가용성 영역

HA 다중 가용성 영역 구성은 두 개의 Cloud Volumes ONTAP 노드를 서로 다른 가용성 영역에 배포하는 배포 모델을 활용하여 노드가 서로 다른 장애 도메인에 위치하도록 하여 중복성과 가용성을 제공합니다. 유연한 오케스트레이션 모드에서 Virtual Machine Scale Sets가 Azure의 가용성 영역을 사용하는 방법을 알아보려면 다음을 참조하세요. "Microsoft Azure 설명서: 가용성 영역을 사용하는 가상 머신 확장 집합 만들기" .

디스크

고객 데이터는 ZRS(Zone-Redundant Storage) 관리 디스크에 저장됩니다. 각 노드는 다른 노드의 저장소에 접근할 수 있습니다. 추가 저장 공간도 필요합니다."부트, 루트, 파트너 루트 및 코어 데이터" .

저장 계정

스토리지 계정은 진단 로그를 처리하고 Blob 스토리지로 계층화하기 위해 관리형 디스크 기반 배포에 사용됩니다.

RPO와 **RTO**

HA 구성은 다음과 같이 데이터의 높은 가용성을 유지합니다.

- 복구 지점 목표(RPO)는 0초입니다. 귀하의 데이터는 데이터 손실 없이 거래적으로 일관성을 유지합니다.
- 복구 시간 목표(RTO)는 120초입니다. 정전이 발생하더라도 120초 이내에 데이터를 사용할 수 있어야 합니다.

저장소 인수 및 반환

물리적 ONTAP 클러스터와 유사하게 Azure HA 쌍의 저장소는 노드 간에 공유됩니다. 파트너의 저장소에 연결하면 _인수_가 발생할 경우 각 노드가 다른 노드의 저장소에 액세스할 수 있습니다. 네트워크 경로 장애 조치 메커니즘은 클라이언트와 호스트가 생존 노드와 계속 통신할 수 있도록 보장합니다. 노드가 다시 온라인 상태가 되면 파트너는 저장소를 _반환_합니다.

NAS 구성의 경우 장애가 발생하면 데이터 IP 주소가 HA 노드 간에 자동으로 마이그레이션됩니다.

iSCSI의 경우 Cloud Volumes ONTAP 다중 경로 I/O(MPIO) 및 비대칭 논리 단위 액세스(ALUA)를 사용하여 활성 최적화 경로와 최적화되지 않은 경로 간의 경로 장애 조치를 관리합니다.

ALUA를 지원하는 특정 호스트 구성에 대한 정보는 다음을 참조하십시오. "NetApp 상호 운용성 매트릭스 도구" 그리고 "SAN 호스트 및 클라우드 클라이언트 가이드" 호스트 운영 체제에 맞게.

저장소 인수, 재동기화 및 반환은 모두 기본적으로 자동으로 수행됩니다. 사용자 작업이 필요하지 않습니다.

스토리지 구성

HA 쌍을 액티브-액티브 구성으로 사용할 수 있습니다. 이 경우 두 노드 모두 클라이언트에 데이터를 제공하고, 액티브-패시브 구성으로 사용할 경우 패시브 노드는 액티브 노드의 스토리지를 인수한 경우에만 데이터 요청에 응답합니다.

Google Cloud의 Cloud Volumes ONTAP HA 쌍에 대해 알아보세요

Cloud Volumes ONTAP 고가용성(HA) 구성은 중단 없는 운영과 내결함성을 제공합니다. Google Cloud에서는 데이터가 두 노드 간에 동기적으로 미러링됩니다.

HA 구성 요소

Google Cloud의 Cloud Volumes ONTAP HA 구성에는 다음 구성 요소가 포함됩니다.

- 두 개의 Cloud Volumes ONTAP 노드의 데이터가 서로 동기적으로 미러링됩니다.
- 저장소 인수 및 반환 프로세스를 지원하기 위해 노드 간 통신 채널을 제공하는 중재자 인스턴스입니다.
- 1개 구역 또는 3개 구역(권장).

3개의 영역을 선택하면 두 노드와 중재자가 별도의 Google Cloud 영역에 위치합니다.

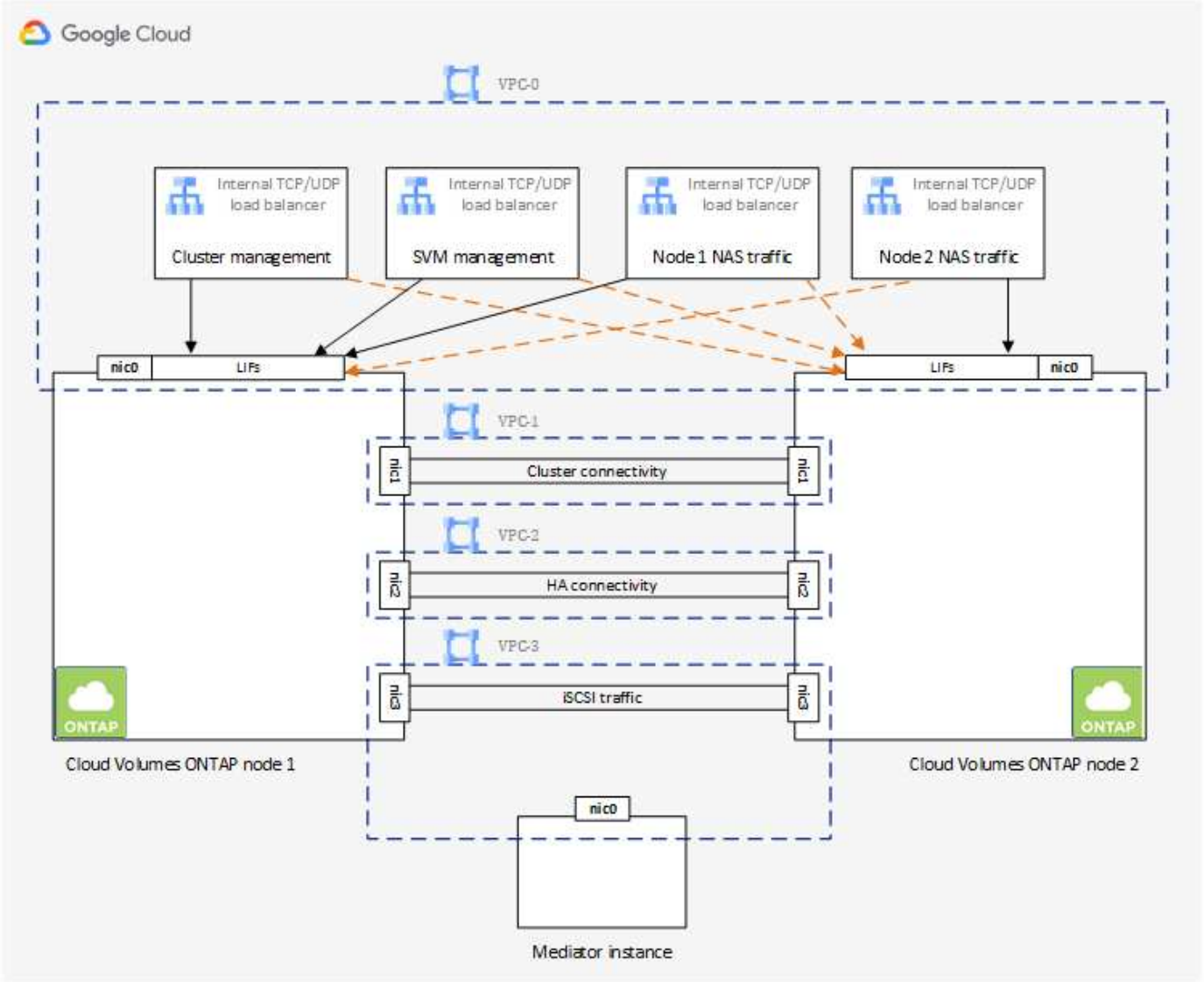
- 4개의 가상 사설 클라우드(VPC).

  GCP에서는 각 네트워크 인터페이스가 별도의 VPC 네트워크에 있어야 하므로 이 구성에서는 4개의 VPC를 사용합니다.

- Cloud Volumes ONTAP HA 쌍으로 들어오는 트래픽을 관리하는 4개의 Google Cloud 내부 부하 분산 장치(TCP/UDP).

"네트워킹 요구 사항에 대해 알아보세요"여기에는 로드 밸런서, VPC, 내부 IP 주소, 서브넷 등에 대한 자세한 내용이 포함됩니다.

다음 개념적 이미지는 Cloud Volumes ONTAP HA 쌍과 해당 구성 요소를 보여줍니다.



중재인

Google Cloud의 중재자 인스턴스에 대한 주요 세부 정보는 다음과 같습니다.

인스턴스 유형

e2-micro(이전에 f1-micro 인스턴스가 사용됨)

디스크

각각 10GiB인 두 개의 표준 영구 디스크

운영 체제

데비안 11

Cloud Volumes ONTAP 9.10.0 및 이전 버전의 경우, Debian 10이 메디에이터에 설치되었습니다.

업그레이드

Cloud Volumes ONTAP 업그레이드하면 NetApp Console 도 필요에 따라 중재자 인스턴스를 업데이트합니다.

인스턴스에 대한 액세스

Debian의 경우 기본 클라우드 사용자는 `admin`입니다. Google Cloud는 Google Cloud Console 또는 gcloud 명령줄을 통해 SSH 액세스가 요청되면 `admin 사용자에 대한 인증서를 생성하고 추가합니다. `sudo`을 지정하여 루트 권한을 얻을 수 있습니다.

제3자 에이전트

중재자 인스턴스에서는 타사 에이전트나 VM 확장이 지원되지 않습니다.

저장소 인수 및 반환

노드 하나가 다운되더라도 다른 노드는 파트너에게 데이터를 제공하여 지속적인 데이터 서비스를 제공할 수 있습니다. 데이터가 파트너에 동기적으로 미러링되었기 때문에 클라이언트는 파트너 노드에서 동일한 데이터에 액세스할 수 있습니다.

노드가 재부팅된 후 파트너는 저장소를 반환하기 전에 데이터를 다시 동기화해야 합니다. 데이터를 다시 동기화하는 데 걸리는 시간은 노드가 다운된 동안 얼마나 많은 데이터가 변경되었는지에 따라 달라집니다.

저장소 인수, 재동기화 및 반환은 모두 기본적으로 자동으로 수행됩니다. 사용자 작업이 필요하지 않습니다.

RPO와 RTO

HA 구성은 다음과 같이 데이터의 높은 가용성을 유지합니다.

- 복구 지점 목표(RPO)는 0초입니다.

  귀하의 데이터는 데이터 손실 없이 거래적으로 일관성을 유지합니다.

- 복구 시간 목표(RTO)는 120초입니다.

  정전이 발생하더라도 120초 이내에 데이터를 사용할 수 있어야 합니다.

HA 배포 모델

여러 영역이나 단일 영역에 HA 구성을 배포하면 데이터의 높은 가용성을 보장할 수 있습니다.

여러 구역(권장)

3개 영역에 걸쳐 HA 구성을 배포하면 영역 내에서 장애가 발생하더라도 지속적인 데이터 가용성이 보장됩니다. 단일 영역을 사용하는 것에 비해 쓰기 성능은 약간 낮지만 최소한입니다.

단일 구역

단일 영역에 배포되는 경우 Cloud Volumes ONTAP HA 구성은 확산 배치 정책을 사용합니다. 이 정책은 오류 격리를 위해 별도의 영역을 사용하지 않고도 영역 내의 단일 장애 지점으로부터 HA 구성이 보호되도록 보장합니다.

이 배포 모델을 사용하면 영역 간에 데이터 유출 요금이 발생하지 않으므로 비용이 절감됩니다.

HA 쌍에서 스토리지가 작동하는 방식

ONTAP 클러스터와 달리 GCP의 Cloud Volumes ONTAP HA 쌍의 스토리지는 노드 간에 공유되지 않습니다. 대신, 데이터는 노드 간에 동기적으로 미러링되므로 장애가 발생하더라도 데이터를 사용할 수 있습니다.

저장 공간 할당

새 볼륨을 생성하고 추가 디스크가 필요한 경우 콘솔은 두 노드에 동일한 수의 디스크를 할당하고 미러링된 집계를 만든 다음 새 볼륨을 생성합니다. 예를 들어, 볼륨에 두 개의 디스크가 필요한 경우 콘솔은 노드당 두 개의 디스크를 할당하여 총 4개의 디스크를 할당합니다.

스토리지 구성

HA 쌍을 액티브-액티브 구성으로 사용할 수 있습니다. 이 경우 두 노드 모두 클라이언트에 데이터를 제공하고, 액티브-패시브 구성으로 사용할 경우 패시브 노드는 액티브 노드의 스토리지를 인수한 경우에만 데이터 요청에 응답합니다.

HA 구성에 대한 성능 기대치

Cloud Volumes ONTAP HA 구성은 노드 간에 데이터를 동기적으로 복제하므로 네트워크 대역폭을 소모합니다. 결과적으로 단일 노드 Cloud Volumes ONTAP 구성과 비교했을 때 다음과 같은 성능을 기대할 수 있습니다.

- 단일 노드에서만 데이터를 제공하는 HA 구성의 경우, 읽기 성능은 단일 노드 구성의 읽기 성능과 비슷하지만 쓰기 성능은 낮습니다.
- 두 노드 모두에서 데이터를 제공하는 HA 구성의 경우, 읽기 성능은 단일 노드 구성의 읽기 성능보다 높고, 쓰기 성능은 동일하거나 더 높습니다.

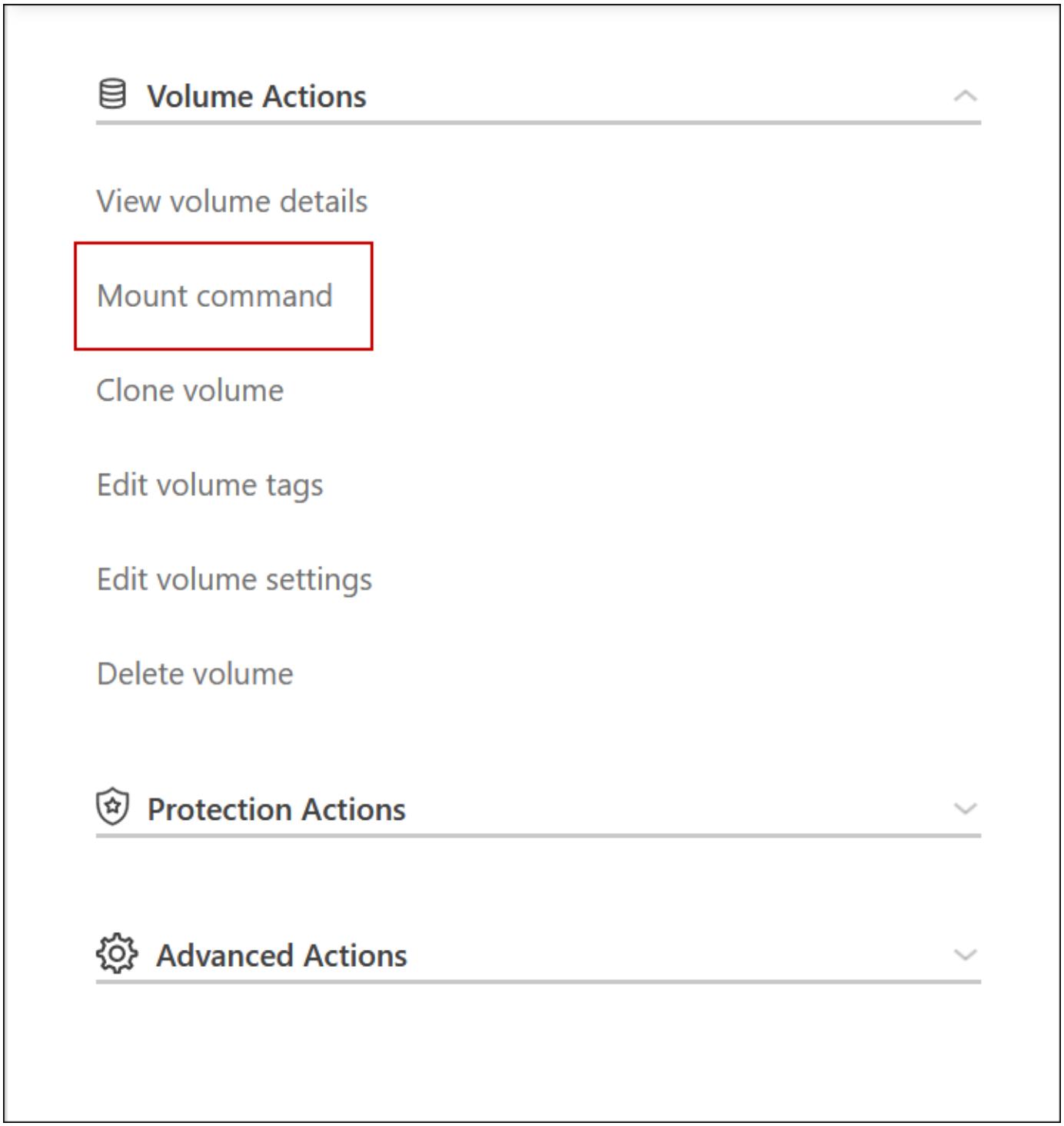
Cloud Volumes ONTAP 성능에 대한 자세한 내용은 다음을 참조하세요."성능" .

저장소에 대한 클라이언트 액세스

클라이언트는 볼륨이 있는 노드의 데이터 IP 주소를 사용하여 NFS 및 CIFS 볼륨에 액세스해야 합니다. NAS 클라이언트가 파트너 노드의 IP 주소를 사용하여 볼륨에 액세스하는 경우 트래픽이 두 노드 사이를 이동하게 되어 성능이 저하됩니다.

HA 쌍의 노드 간에 볼륨을 이동하는 경우 다른 노드의 IP 주소를 사용하여 볼륨을 다시 마운트해야 합니다. 그렇지 않으면 성능이 저하될 수 있습니다. 클라이언트가 CIFS에 대한 NFSv4 참조 또는 폴더 리디렉션을 지원하는 경우 Cloud Volumes ONTAP 시스템에서 해당 기능을 활성화하여 볼륨을 다시 마운트하지 않아도 됩니다. 자세한 내용은 ONTAP 문서를 참조하세요.

볼륨을 선택하고 *마운트 명령*을 클릭하면 콘솔에서 올바른 IP 주소를 찾을 수 있습니다.



관련 링크

- "네트워킹 요구 사항에 대해 알아보세요"
- "GCP를 시작하는 방법을 알아보세요"

Cloud Volumes ONTAP HA 쌍의 노드가 오프라인일 때 작업을 사용할 수 없음

HA 쌍의 노드를 사용할 수 없는 경우 다른 노드가 파트너에게 데이터를 제공하여 지속적인 데이터 서비스를 제공합니다. 이것을 _스토리지 인수_라고 합니다. 보관된 물품을 반환하는

작업이 완료될 때까지 여러 작업을 수행할 수 없습니다.

HA 쌍의 노드를 사용할 수 없는 경우 NetApp Console 의 시스템 상태는 _저하_됩니다.

저장소 인수에서는 다음 작업을 수행할 수 없습니다.

- 지원 등록
- 라이센스 변경
- 인스턴스 또는 VM 유형 변경
- 쓰기 속도 변경
- CIFS 설정
- 구성 백업 위치 변경
- 클러스터 비밀번호 설정
- 디스크 및 집계 관리(고급 할당)

이러한 작업은 저장 공간 반환이 완료되고 시스템 상태가 정상으로 돌아온 후에 다시 사용할 수 있습니다.

Cloud Volumes ONTAP 데이터 암호화 및 랜섬웨어 보호에 대해 알아보세요

Cloud Volumes ONTAP 데이터 암호화를 지원하고 바이러스 및 랜섬웨어로부터 보호합니다.

저장 중인 데이터의 암호화

Cloud Volumes ONTAP 다음과 같은 암호화 기술을 지원합니다.

- NetApp 암호화 솔루션(NVE 및 NAE)
- AWS 키 관리 서비스
- Azure Storage 서비스 암호화
- Google Cloud Platform 기본 암호화

클라우드 공급업체의 기본 암호화와 함께 NetApp 암호화 솔루션을 사용하면 하이퍼바이저 수준에서 데이터를 암호화할 수 있습니다. 그렇게 하면 매우 민감한 데이터의 경우 바람직할 수 있는 이중 암호화가 제공됩니다. 암호화된 데이터에 액세스하면 두 번 암호화가 해제됩니다. 한 번은 하이퍼바이저 수준에서(클라우드 공급업체의 키를 사용하여) 해제되고, 두 번째는 NetApp 암호화 솔루션을 사용하여(외부 키 관리자의 키를 사용하여) 해제됩니다.

NetApp 암호화 솔루션(NVE 및 NAE)

Cloud Volumes ONTAP 지원 "NetApp 볼륨 암호화(NVE) 및 NetApp 집계 암호화(NAE)" . NVE와 NAE는 볼륨의 (FIPS) 140-2 규격에 따른 저장 데이터 암호화를 지원하는 소프트웨어 기반 솔루션입니다. NVE와 NAE는 모두 AES 256비트 암호화를 사용합니다.

- NVE는 저장 중인 데이터를 한 번에 한 볼륨씩 암호화합니다. 각 데이터 볼륨에는 고유한 암호화 키가 있습니다.
- NAE는 NVE의 확장 버전으로, 각 볼륨의 데이터를 암호화하고 볼륨은 전체 집계에서 키를 공유합니다. NAE를

사용하면 집계된 모든 볼륨의 공통 블록을 중복 제거할 수도 있습니다.

Cloud Volumes ONTAP Fortanix와 같은 타사 솔루션을 포함하여 AWS, Azure, Google Cloud에서 제공하는 외부 키 관리 서비스(EKM)를 통해 NVE와 NAE를 모두 지원합니다. ONTAP 과 달리 Cloud Volumes ONTAP 의 경우 암호화 키는 ONTAP 아닌 클라우드 공급자 측에서 생성됩니다. Cloud Volumes ONTAP 지원하지 않습니다. "온보드 키 관리자".

Cloud Volumes ONTAP ONTAP 사용하는 표준 KMIP(Key Management Interoperability Protocol) 서비스를 사용합니다. 지원되는 서비스에 대한 자세한 내용은 다음을 참조하세요. "상호 운용성 매트릭스 도구" .

NVE를 사용하는 경우 클라우드 공급자의 키 보관소를 사용하여 ONTAP 암호화 키를 보호하는 옵션이 있습니다.

- AWS 키 관리 서비스(KMS)
- Azure 키 보관소(AKV)
- Google Cloud 키 관리 서비스

외부 키 관리자를 설정한 후에는 새로운 집계에서 기본적으로 NetApp 집계 암호화(NAE)가 활성화됩니다. NAE 집계에 포함되지 않은 새 볼륨에는 기본적으로 NVE가 활성화되어 있습니다(예: 외부 키 관리자를 설정하기 전에 생성된 기존 집계가 있는 경우).

지원되는 키 관리자를 설정하는 것이 유일하게 필요한 단계입니다. 설정 지침은 다음을 참조하세요."NetApp 암호화 솔루션으로 볼륨 암호화" .

AWS 키 관리 서비스

AWS에서 Cloud Volumes ONTAP 시스템을 시작하면 다음을 사용하여 데이터 암호화를 활성화할 수 있습니다. "AWS 키 관리 서비스(KMS)" . NetApp Console 고객 마스터 키(CMK)를 사용하여 데이터 키를 요청합니다.

Cloud Volumes ONTAP 시스템을 생성한 후에는 AWS 데이터 암호화 방법을 변경할 수 없습니다.

이 암호화 옵션을 사용하려면 AWS KMS가 적절하게 설정되어 있는지 확인해야 합니다. 자세한 내용은 다음을 참조하세요."AWS KMS 설정" .

Azure Storage 서비스 암호화

Azure의 Cloud Volumes ONTAP 에서 데이터는 자동으로 암호화됩니다. "Azure Storage 서비스 암호화" Microsoft에서 관리하는 키를 사용합니다.

원하시면 자체 암호화 키를 사용하실 수 있습니다. "Azure에서 고객 관리 키를 사용하도록 Cloud Volumes ONTAP 설정하는 방법을 알아보세요." .

Google Cloud Platform 기본 암호화

"Google Cloud Platform 저장 데이터 암호화"Cloud Volumes ONTAP 에서는 기본적으로 활성화되어 있습니다. 설정이 필요하지 않습니다.

Google Cloud Storage는 디스크에 쓰기 전에 항상 데이터를 암호화하지만, Console API를 사용하면 _고객 관리 암호화 키_를 사용하는 Cloud Volumes ONTAP 시스템을 만들 수 있습니다. 이러한 키는 Cloud Key Management Service를 사용하여 GCP에서 생성하고 관리하는 키입니다. "자세히 알아보기" .

ONTAP 바이러스 검사

ONTAP 시스템에서 통합된 바이러스 백신 기능을 사용하면 바이러스나 기타 악성 코드로 인해 데이터가 손상되는 것을 방지할 수 있습니다.

ONTAP 바이러스 검사(_Vscan_이라고 함)는 동급 최고의 타사 바이러스 백신 소프트웨어와 ONTAP 기능을 결합하여 어떤 파일을 언제 검사할지 제어하는 데 필요한 유연성을 제공합니다.

Vscan에서 지원하는 공급업체, 소프트웨어 및 버전에 대한 정보는 다음을 참조하십시오. "NetApp 상호 운용성 매트릭스" .

ONTAP 시스템에서 바이러스 백신 기능을 구성하고 관리하는 방법에 대한 정보는 다음을 참조하십시오. "ONTAP 9 바이러스 백신 구성 가이드" .

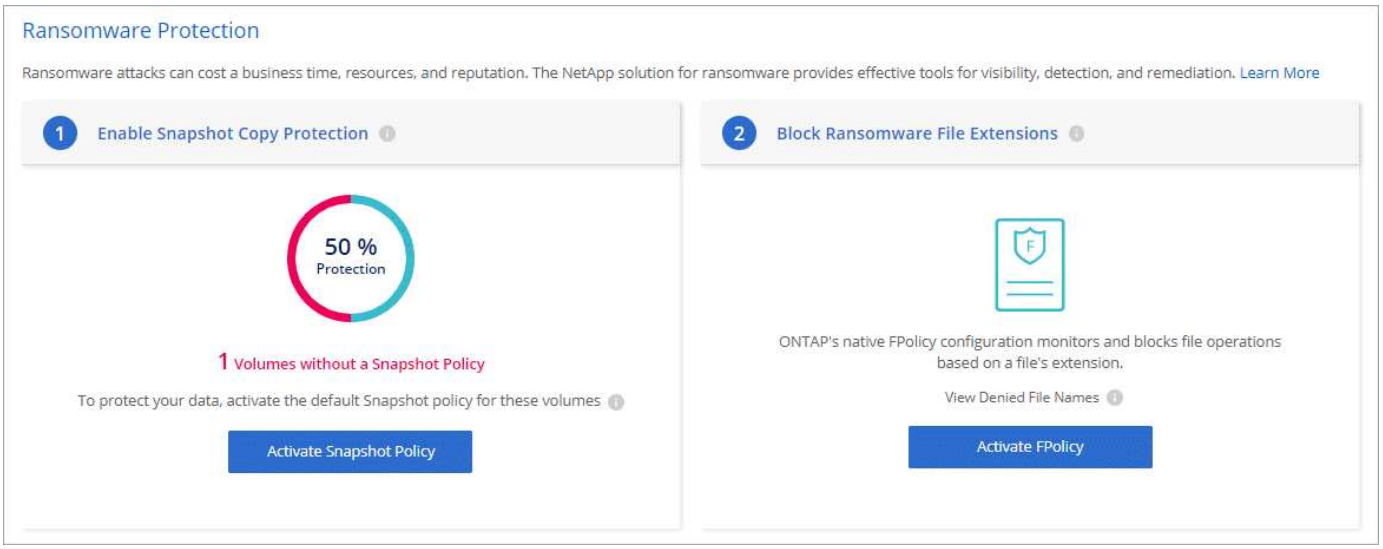
랜섬웨어 보호

랜섬웨어 공격은 기업의 시간, 자원, 평판을 앗아갈 수 있습니다. 콘솔을 사용하면 가시성, 탐지 및 치료를 위한 효과적인 도구를 제공하는 랜섬웨어에 대한 NetApp 솔루션을 구현할 수 있습니다.

- 콘솔은 스냅샷 정책으로 보호되지 않는 볼륨을 식별하고 해당 볼륨에서 기본 스냅샷 정책을 활성화할 수 있도록 합니다.

  스냅샷 사본은 읽기 전용이므로 랜섬웨어로 인한 손상을 방지할 수 있습니다. 또한 단일 파일 사본이나 완전한 재해 복구 솔루션의 이미지를 만드는 세분성을 제공할 수도 있습니다.

- 콘솔을 사용하면 ONTAP의 FPolicy 솔루션을 활성화하여 일반적인 랜섬웨어 파일 확장자를 차단할 수도 있습니다.



"랜섬웨어에 대한 NetApp 솔루션을 구현하는 방법을 알아보세요" .

Cloud Volumes ONTAP 워크로드에 대한 성능 모니터링에 대해 알아보세요.

Cloud Volumes ONTAP 에 적합한 워크로드가 무엇인지 결정하는 데 도움이 되도록 성능 결과를 검토할 수 있습니다.

성능 기술 보고서

- AWS용 Cloud Volumes ONTAP

  "NetApp 기술 보고서 4383: 애플리케이션 워크로드를 포함한 Amazon Web Services의 Cloud Volumes ONTAP 성능 특성 분석"

- Microsoft Azure용 Cloud Volumes ONTAP

  "NetApp 기술 보고서 4671: 애플리케이션 워크로드를 포함한 Azure의 Cloud Volumes ONTAP 성능 특성 분석"

- Google Cloud용 Cloud Volumes ONTAP

  "NetApp 기술 보고서 4816: Google Cloud용 Cloud Volumes ONTAP 의 성능 특성 분석"

CPU 성능

클라우드 공급업체의 모니터링 도구에 따르면 Cloud Volumes ONTAP 노드는 높은 활용도(90% 이상)를 보입니다. ONTAP 가상 머신에 제공된 모든 vCPU를 예약해 두어 필요할 때 사용할 수 있도록 하기 때문입니다.

자세한 내용은 다음을 참조하세요. "CLI를 사용하여 ONTAP CPU 사용률을 모니터링하는 방법에 대한 NetApp 기술 자료 문서"

노드 기반 BYOL에 대한 라이선스 관리

노드 기반 BYOL(Bring Your Own License)이 있는 각 Cloud Volumes ONTAP 시스템에는 활성 구독과 함께 설치된 시스템 라이선스가 있어야 합니다. NetApp Console 라이선스를 관리하고 라이선스가 만료되기 전에 경고를 표시하여 프로세스를 간소화합니다.

노드 기반 라이선스는 Cloud Volumes ONTAP 의 이전 세대 라이선스입니다. 노드 기반 라이선스는 NetApp (BYOL)에서 구매할 수 있으며, 특정 경우에만 라이선스를 갱신할 수 있습니다.

"Cloud Volumes ONTAP 라이선싱 옵션에 대해 자세히 알아보세요" .

"노드 기반 라이선스를 관리하는 방법에 대해 자세히 알아보세요." .

BYOL 시스템 라이선스

노드 기반 라이선스는 NetApp에서 구매할 수 있습니다. 단일 노드 시스템 또는 HA 쌍에 대해 구매할 수 있는 라이선스 수는 무제한입니다.

NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAPP 에 대한 BYOL 라이선싱의 제한된 가용성" .

노드 기반 라이선스는 단일 노드 또는 HA 쌍에 최대 368TiB의 용량을 제공합니다. Cloud Volumes ONTAP BYOL 시스템에 368TiB 이상의 용량을 할당하기 위해 여러 라이선스를 구매했을 수 있습니다. 예를 들어, Cloud Volumes ONTAP 에 최대 736TiB의 용량을 할당하기 위해 두 개의 라이선스를 구매할 수 있습니다. 또는 최대 1.4PiB의 용량을 확보하기 위해 네 개의 라이선스를 구매할 수도 있습니다.

디스크 제한으로 인해 디스크만 사용하여 용량 제한에 도달하지 못할 수도 있습니다. 디스크 한도를 초과할 수 있습니다 ."비활성 데이터를 개체 스토리지로 계층화" . 디스크 제한에 대한 정보는 다음을 참조하세요. "Cloud Volumes ONTAP 릴리스 노트의 저장 한도" .

새 시스템에 대한 라이선스 관리

노드 기반 BYOL 시스템을 만들면 콘솔에서 라이선스의 일련 번호와 NetApp 지원 사이트 계정을 입력하라는 메시지가 표시됩니다. 콘솔은 계정을 사용하여 NetApp 에서 라이선스 파일을 다운로드하고 이를 Cloud Volumes ONTAP 시스템에 설치합니다.

"콘솔에 NetApp 지원 사이트 계정을 추가하는 방법을 알아보세요." .

콘솔이 보안 인터넷 연결을 통해 라이센스 파일에 액세스할 수 없는 경우 다음을 수행할 수 있습니다."직접 파일을 얻은 다음 콘솔에 수동으로 파일을 업로드합니다." .

라이센스 만료

콘솔은 노드 기반 라이선스가 만료되기 30일 전에 경고를 표시하고, 라이선스가 만료될 때 다시 경고를 표시합니다. 다음 이미지는 사용자 인터페이스에 나타나는 30일 만료 경고를 보여줍니다.

메시지를 검토할 시스템을 선택할 수 있습니다.

조직 또는 계정 관리자가 해당 옵션을 활성화한 경우 콘솔에는 이메일로 전송되는 Cloud Volumes ONTAP 보고서에 라이선스 만료 경고가 포함되어 있습니다. 이메일 보고서에는 2주마다 라이선스 만료 경고가 포함되어 있습니다.

정해진 기간 내에 라이센스를 갱신하지 않으면 Cloud Volumes ONTAP 시스템이 자동으로 종료됩니다. 다시 시작하면 다시 꺼집니다.

면허 갱신

NetApp 담당자에게 연락하여 노드 기반 BYOL 구독을 갱신하는 경우 콘솔은 자동으로 NetApp 에서 새 라이선스를 받아 Cloud Volumes ONTAP 시스템에 설치합니다.

콘솔이 보안 인터넷 연결을 통해 라이센스 파일에 액세스할 수 없는 경우 다음을 수행할 수 있습니다."직접 파일을 얻은 다음 콘솔에 수동으로 파일을 업로드합니다." .

새로운 시스템으로 라이센스 이전

노드 기반 BYOL 라이선스는 기존 시스템을 삭제한 다음 동일한 라이선스를 사용하여 새 시스템을 만들 때 Cloud Volumes ONTAP 시스템 간에 전송할 수 있습니다.

예를 들어, 기존 라이선스 시스템을 삭제한 다음 다른 VPC/VNet 또는 클라우드 공급자의 새로운 BYOL 시스템에서 라이선스를 사용할 수 있습니다. 모든 클라우드 공급자에서는 클라우드 독립적 일련 번호만 작동합니다. 클라우드에 독립적인 일련 번호는 *908xxxx* 접두사로 시작합니다.

BYOL 라이선스는 회사와 특정 NetApp 지원 사이트 자격 증명에 연결되어 있다는 점을 알아두는 것이 중요합니다.

AutoSupport 와 Digital Advisor Cloud Volumes ONTAP 에 어떻게 사용되는지 알아보세요.

ONTAP 의 AutoSupport 구성 요소는 원격 측정 데이터를 수집하여 분석을 위해 전송합니다. Active IQ Digital Advisor (Digital Advisor 라고도 함)는 AutoSupport 의 데이터를 분석하고 사전 예방적 관리와 최적화를 제공합니다. Digital Advisor 인공지능을 사용하여 잠재적인 문제를 파악하고 그러한 문제가 비즈니스에 영향을 미치기 전에 해결하는 데 도움을 줍니다.

Digital Advisor 사용하면 클라우드 기반 포털과 모바일 앱을 통해 실행 가능한 예측 분석과 사전 예방적 지원을 제공하여 글로벌 하이브리드 클라우드에서 데이터 인프라를 최적화할 수 있습니다. Digital Advisor 의 데이터 기반 통찰력과 권장 사항은 활성 SupportEdge 계약이 있는 모든 NetApp 고객에게 제공됩니다(기능은 제품 및 지원 계층에 따라 다름).

Digital Advisor 사용하면 다음과 같은 작업을 수행할 수 있습니다.

- 업그레이드를 계획하세요.

  Digital Advisor ONTAP 의 최신 버전으로 업그레이드하여 해결할 수 있는 환경의 문제를 식별하고, Upgrade Advisor 구성 요소는 성공적인 업그레이드를 계획하는 데 도움을 줍니다.

- 시스템 상태를 확인하세요.

  Digital Advisor 대시보드는 건강 관련 문제를 보고하고 해당 문제를 해결하는 데 도움을 줍니다. 저장 공간이 부족해지지 않도록 시스템 용량을 모니터링하세요. 시스템에 대한 지원 사례를 확인하세요.

- 성과를 관리합니다.

  Digital Advisor ONTAP System Manager에서 볼 수 있는 것보다 더 긴 기간 동안의 시스템 성능을 보여줍니다. 성능에 영향을 미치는 구성 및 시스템 문제를 파악합니다. 효율성을 극대화하세요. 저장 효율성 지표를 보고 더 적은 공간에 더 많은 데이터를 저장하는 방법을 파악하세요.

- 인벤토리와 구성을 확인하세요.

  Digital Advisor 전체 재고와 소프트웨어 및 하드웨어 구성 정보를 표시합니다. 서비스 계약이 만료되는 시점을 확인하고 갱신하여 지원을 계속 받으세요.

관련 링크

- "NetApp 문서: Digital Advisor"
- "Digital Advisor 출시"
- "SupportEdge 서비스"

Cloud Volumes ONTAP 에 지원되는 기본 구성

Cloud Volumes ONTAP 기본적으로 어떻게 구성되는지 이해하면 시스템을 설정하고 관리하는 데 도움이 될 수 있습니다. 특히 ONTAP 에 익숙하다면 더욱 그렇습니다 . Cloud Volumes

ONTAP 의 기본 설정은 ONTAP 과 다르기 때문입니다.

기본 설정

- NetApp Console Cloud Volumes ONTAP 배포할 때 하나의 데이터 제공 스토리지 VM을 생성합니다. 일부 구성에서는 추가 스토리지 VM을 지원합니다. "스토리지 VM 관리에 대해 자세히 알아보세요" .

  3.9.5 릴리스부터 초기 스토리지 VM에서 논리적 공간 보고가 활성화됩니다. 공간이 논리적으로 보고되는 경우 ONTAP 저장 효율성 기능으로 절약된 모든 물리적 공간도 사용된 것으로 보고되도록 볼륨 공간을 보고합니다. 인라인 스토리지 효율성 기능에 대한 정보는 지식 기반 문서를 참조하세요. "KB: CVO에서는 어떤 인라인 스토리지 효율성 기능이 지원되나요?"

- 콘솔은 Cloud Volumes ONTAP 에 다음 ONTAP 기능 라이선스를 자동으로 설치합니다.
  - CIFS
  - FlexCache
  - FlexClone
  - iSCSI
  - Cloud Volumes ONTAP 9.12.1 GA부터 시작하는 다중 테넌트 암호화 키 관리(MTEKM)
  - NetApp 볼륨 암호화(BYOL(Bring Your Own License) 또는 PAYGO(Registered Pay-as-You-Go) 시스템에만 해당)
  - NFS ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[]
  - SnapMirror
  - SnapRestore
  - SnapVault
- 기본적으로 여러 네트워크 인터페이스가 생성됩니다.
  - 클러스터 관리 LIF
  - 클러스터 간 LIF
- Azure의 HA 시스템에 대한 SVM 관리 LIF
- Google Cloud의 HA 시스템에 대한 SVM 관리 LIF
- AWS의 단일 노드 시스템에서 SVM 관리 LIF
- 노드 관리 LIF

+ Google Cloud에서 이 LIF는 클러스터 간 LIF와 결합됩니다.

- iSCSI 데이터 LIF
- CIFS 및 NFS 데이터 LIF

  클라우드 공급자 요구 사항으로 인해 Cloud Volumes ONTAP 의 경우 LIF 장애 조치는 기본적으로 비활성화되어 있습니다. LIF를 다른 포트로 마이그레이션하면 인스턴스의 IP 주소와 네트워크 인터페이스 간의 외부 매핑이 끊어져 LIF에 액세스할 수 없게 됩니다.

  - Cloud Volumes ONTAP HTTP를 사용하여 구성 백업을 콘솔 에이전트로 보냅니다.

백업은 http://ipaddress/occm/offboxconfig/에서 접근할 수 있습니다. 여기서 _ipaddress_는 콘솔 에이전트 호스트의 IP 주소입니다.

백업을 사용하여 Cloud Volumes ONTAP 시스템을 재구성할 수 있습니다. 구성 백업에 대한 자세한 내용은 다음을 참조하세요. "ONTAP 문서" .

- 콘솔은 다른 관리 도구(예: ONTAP System Manager 또는 ONTAP CLI)와 다르게 몇 가지 볼륨 속성을 설정합니다.

  다음 표는 기본값과 다르게 설정된 볼륨 속성을 나열합니다.

기인하다	콘솔이 구성하는 값
자동 크기 조정 모드	자라다
최대 자동 크기	1,000퍼센트 조직 또는 계정 관리자는 설정 페이지에서 이 값을 수정할 수 있습니다.
보안 스타일	CIFS 볼륨의 경우 NTFS, NFS 볼륨의 경우 UNIX
공간 보장 스타일	없음
UNIX 권한(NFS 전용)	777

+
이러한 속성에 대한 정보는 다음을 참조하세요."ONTAP 볼륨 생성 매뉴얼 페이지" .

시스템 데이터용 내부 디스크

콘솔은 사용자 데이터를 저장하는 것 외에도 시스템 데이터를 위한 클라우드 스토리지도 구매합니다.

AWS

- 부트, 루트, 코어 데이터를 위한 노드당 3개의 디스크:
  - 부팅 데이터용 47GiB io1 디스크
  - 루트 데이터용 140GiB gp3 디스크
  - 코어 데이터용 540GiB gp2 디스크
- HA 쌍의 경우:
  - 중재자 인스턴스용 st1 EBS 볼륨 2개, 루트 디스크로 약 8GiB 중 하나, 데이터 디스크로 4GiB 중 하나
  - 각 노드에 140GiB gp3 디스크 1개, 다른 노드의 루트 데이터 사본 포함

    일부 영역에서는 사용 가능한 EBS 디스크 유형이 gp2만 가능합니다.
- 각 부팅 디스크와 루트 디스크에 대한 하나의 EBS 스냅샷

재부팅 시 스냅샷이 자동으로 생성됩니다.

- AWS에서 키 관리 서비스(KMS)를 사용하여 데이터 암호화를 활성화하면 Cloud Volumes ONTAP 의 부팅 및 루트 디스크도 암호화됩니다. 여기에는 HA 쌍의 중재자 인스턴스에 대한 부팅 디스크가 포함됩니다. 디스크는 Cloud Volumes ONTAP 시스템을 추가할 때 선택하는 CMK를 사용하여 암호화됩니다.

AWS에서는 NVRAM 이 부팅 디스크에 있습니다.

Azure(단일 노드)

- 프리미엄 SSD 디스크 3개:
  - 부팅 데이터용 10GiB 디스크 1개
  - 루트 데이터용 140GiB 디스크 1개
  - NVRAM 용 512GiB 디스크 1개

    Cloud Volumes ONTAP 에 대해 선택한 가상 머신이 Ultra SSD를 지원하는 경우 시스템은 Premium SSD가 아닌 NVRAM 에 32GiB Ultra SSD를 사용합니다.
- 코어 저장을 위한 1024GiB 표준 HDD 디스크 1개
- 각 부팅 디스크와 루트 디스크에 대한 하나의 Azure 스냅샷
- Azure의 모든 디스크는 기본적으로 저장 시 암호화됩니다.

  Cloud Volumes ONTAP 에 대해 선택한 가상 머신이 데이터 디스크로 Premium SSD v2 관리 디스크를 지원하는 경우, 시스템은 NVRAM 에 32GiB Premium SSD v2 관리 디스크를 사용하고, 다른 디스크를 루트 디스크로 사용합니다.

Azure(HA 쌍)

페이지 블롭이 있는 **HA** 쌍

- 부팅 볼륨을 위한 2개의 10GiB 프리미엄 SSD 디스크(노드당 1개)
- 루트 볼륨에 대한 2개의 140GiB 프리미엄 스토리지 페이지 Blob(노드당 하나)
- 코어 저장을 위한 2개의 1024GiB 표준 HDD 디스크(노드당 1개)
- NVRAM 용 512GiB 프리미엄 SSD 디스크 2개(노드당 1개)
- 각 부팅 디스크와 루트 디스크에 대한 하나의 Azure 스냅샷

재부팅 시 스냅샷이 자동으로 생성됩니다.

- Azure의 모든 디스크는 기본적으로 저장 시 암호화됩니다.

여러 가용성 영역에 있는 공유 관리 디스크와 **HA** 쌍

- 부팅 볼륨을 위한 2개의 10GiB 프리미엄 SSD 디스크(노드당 1개)
- 루트 볼륨을 위한 512GiB 프리미엄 SSD 디스크 2개(노드당 1개)
- 코어 저장을 위한 2개의 1024GiB 표준 HDD 디스크(노드당 1개)

- NVRAM 용 512GiB 프리미엄 SSD 디스크 2개(노드당 1개)
- 각 부팅 디스크와 루트 디스크에 대한 하나의 Azure 스냅샷

  재부팅 시 스냅샷이 자동으로 생성됩니다.

- Azure의 모든 디스크는 기본적으로 저장 시 암호화됩니다.

단일 가용성 영역에서 공유 관리 디스크와 **HA** 쌍

- 부팅 볼륨을 위한 2개의 10GiB 프리미엄 SSD 디스크(노드당 1개)
- 루트 볼륨을 위한 2개의 512GiB 프리미엄 SSD 공유 관리 디스크(노드당 1개)
- 코어 저장을 위한 2개의 1024GiB 표준 HDD 디스크(노드당 1개)
- NVRAM 용 512GiB 프리미엄 SSD 관리 디스크 2개(노드당 1개)

가상 머신이 데이터 디스크로 Premium SSD v2 관리형 디스크를 지원하는 경우 NVRAM 에는 32GiB Premium SSD v2 관리형 디스크를 사용하고 루트 볼륨에는 512GiB Premium SSD v2 공유 관리형 디스크를 사용합니다.

다음 조건이 충족되면 단일 가용성 영역에 HA 쌍을 배포하고 프리미엄 SSD v2 관리형 디스크를 사용할 수 있습니다.

- Cloud Volumes ONTAP 버전은 9.15.1 이상입니다.
- 선택한 지역 및 영역은 Premium SSD v2 Managed Disks를 지원합니다. 지원되는 지역에 대한 정보는 다음을 참조하세요. "Microsoft Azure 웹사이트: 지역별 사용 가능한 제품" .
- 구독은 Microsoft에 등록되었습니다."Microsoft.Compute/VMOrchestratorZonalMultiFD 기능" .

Google Cloud(단일 노드)

- 부팅 데이터용 10GiB SSD 영구 디스크 1개
- 루트 데이터용 64GiB SSD 영구 디스크 1개
- NVRAM 용 500GiB SSD 영구 디스크 1개
- 코어 저장을 위한 315GiB 표준 영구 디스크 1개
- 부팅 및 루트 데이터에 대한 스냅샷

  재부팅 시 스냅샷이 자동으로 생성됩니다.

- 부팅 디스크와 루트 디스크는 기본적으로 암호화됩니다.

Google Cloud(HA 쌍)

- 부팅 데이터용 10GiB SSD 영구 디스크 2개
- 루트 데이터용 64GiB SSD 영구 디스크 4개
- NVRAM 용 500GiB SSD 영구 디스크 2개
- 코어 저장을 위한 2개의 315GiB 표준 영구 디스크
- 중재자 데이터용 10GiB 표준 영구 디스크 1개
- 중재자 부팅 데이터를 위한 10GiB 표준 영구 디스크 1개

- 부팅 및 루트 데이터에 대한 스냅샷

  재부팅 시 스냅샷이 자동으로 생성됩니다.

- 부팅 디스크와 루트 디스크는 기본적으로 암호화됩니다.

디스크가 있는 위치

보관 레이아웃:

- 부팅 데이터는 인스턴스 또는 가상 머신에 연결된 디스크에 저장됩니다.

  부팅 이미지가 포함된 이 디스크는 Cloud Volumes ONTAP 에서 사용할 수 없습니다.

- 시스템 구성과 로그를 포함하는 루트 데이터는 aggr0에 있습니다.
- 스토리지 가상 머신(SVM) 루트 볼륨은 aggr1에 있습니다.
- 데이터 볼륨은 aggr1에도 있습니다.

지식과 지원

지원 등록

NetApp Console 과 해당 스토리지 솔루션, 데이터 서비스에 대한 기술 지원을 받으려면 지원 등록이 필요합니다. Cloud Volumes ONTAP 시스템의 주요 워크플로를 활성화하려면 지원 등록도 필요합니다.

지원에 등록해도 클라우드 공급자 파일 서비스에 대한 NetApp 지원은 제공되지 않습니다. 클라우드 공급자 파일 서비스, 해당 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원에 대해서는 해당 제품 설명서의 "도움말 받기 "를 참조하세요.

- "ONTAP 용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

지원 등록 개요

지원 자격을 활성화하기 위한 등록 방법은 두 가지가 있습니다.

- NetApp Console 계정 일련 번호를 등록합니다(콘솔의 지원 리소스 페이지에 있는 20자리 960xxxxxxxxx 일련 번호).

  이는 콘솔 내의 모든 서비스에 대한 단일 지원 구독 ID 역할을 합니다. 각 콘솔 계정을 등록해야 합니다.

- 클라우드 공급업체의 마켓플레이스에서 구독과 관련된 Cloud Volumes ONTAP 일련 번호를 등록합니다(20자리 909201xxxxxxxx 일련 번호).

  이러한 일련 번호는 일반적으로 _PAYGO 일련 번호_라고 하며 Cloud Volumes ONTAP 배포 시 NetApp Console 에서 생성됩니다.

두 가지 유형의 일련 번호를 모두 등록하면 지원 티켓 개설 및 자동 사례 생성과 같은 기능을 사용할 수 있습니다. 아래 설명된 대로 콘솔에 NetApp 지원 사이트(NSS) 계정을 추가하여 등록을 완료합니다.

NetApp 지원을 위해 **NetApp Console** 등록

지원을 등록하고 지원 자격을 활성화하려면 NetApp Console 계정의 한 사용자가 NetApp 지원 사이트 계정을 콘솔 로그인과 연결해야 합니다. NetApp 지원에 등록하는 방법은 NetApp 지원 사이트(NSS) 계정이 있는지 여부에 따라 달라집니다.

NSS 계정이 있는 기존 고객

NSS 계정이 있는 NetApp 고객이라면 콘솔을 통해 지원을 등록하기만 하면 됩니다.

단계

1. 관리 > *자격 증명*을 선택합니다.
2. *사용자 자격 증명*을 선택하세요.

3. *NSS 자격 증명 추가*를 선택하고 NetApp 지원 사이트(NSS) 인증 프롬프트를 따릅니다.
4. 등록 과정이 성공적으로 완료되었는지 확인하려면 도움말 아이콘을 선택하고 *지원*을 선택하세요.

   리소스 페이지에는 귀하의 콘솔 계정이 지원을 위해 등록되어 있다는 내용이 표시됩니다.

   다른 콘솔 사용자는 NetApp 지원 사이트 계정을 로그인과 연결하지 않은 경우 동일한 지원 등록 상태를 볼 수 없습니다. 하지만 그렇다고 해서 귀하의 계정이 지원을 위해 등록되지 않았다는 의미는 아닙니다. 조직 내 한 명의 사용자가 이러한 단계를 따랐다면 귀하의 계정은 등록되었습니다.

기존 고객이지만 **NSS** 계정이 없습니다.

기존 라이선스와 일련 번호는 있지만 NSS 계정이 없는 기존 NetApp 고객인 경우 NSS 계정을 만들고 콘솔 로그인과 연결해야 합니다.

단계

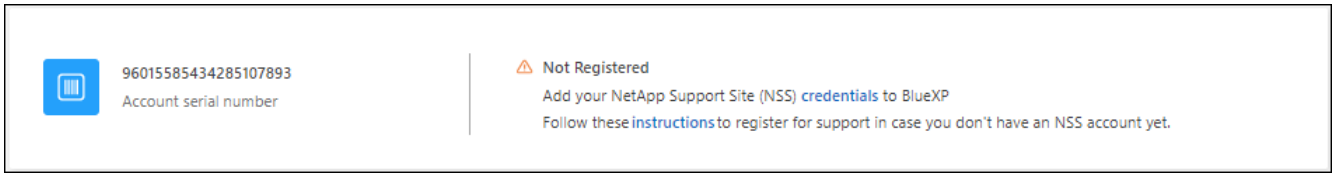
1. 다음을 완료하여 NetApp 지원 사이트 계정을 만드십시오. "NetApp 지원 사이트 사용자 등록 양식"
   a. 일반적으로 * NetApp 고객/최종 사용자*인 적절한 사용자 수준을 선택하세요.
   b. 위에 사용된 콘솔 계정 일련번호(960xxxx)를 일련번호 필드에 꼭 복사해 두세요. 이렇게 하면 계정 처리가 빨라집니다.
2. 다음 단계를 완료하여 새 NSS 계정을 콘솔 로그인과 연결하세요.NSS 계정이 있는 기존 고객 .

NetApp 의 새로운 기능

NetApp 처음 사용하시고 NSS 계정이 없으신 경우 아래의 각 단계를 따르세요.

단계

1. 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 *지원*을 선택하세요.
2. 지원 등록 페이지에서 계정 ID 일련 번호를 찾으세요.



3. 로 이동 "NetApp 지원 등록 사이트" *저는 등록된 NetApp 고객이 아닙니다*를 선택하세요.
4. 필수 입력란(빨간색 별표가 있는 항목)을 작성해 주세요.
5. 제품군 필드에서 *클라우드 관리자*를 선택한 다음 해당 청구 제공자를 선택하세요.
6. 위의 2단계에서 계정 일련번호를 복사하고 보안 검사를 완료한 다음 NetApp의 글로벌 데이터 개인정보 보호정책을 읽었는지 확인하세요.

   이 안전한 거래를 마무리하기 위해 제공된 사서함으로 이메일이 즉시 전송됩니다. 몇 분 안에 인증 이메일이 도착하지 않으면 스팸 폴더를 확인하세요.

7. 이메일 내에서 작업을 확인하세요.

   확인을 클릭하면 귀하의 요청이 NetApp 에 제출되고 NetApp 지원 사이트 계정을 만드는 것이 좋습니다.

8. 다음을 완료하여 NetApp 지원 사이트 계정을 만드십시오. "NetApp 지원 사이트 사용자 등록 양식"
    a. 일반적으로 * NetApp 고객/최종 사용자*인 적절한 사용자 수준을 선택하세요.
    b. 위에 사용된 계정 일련번호(960xxxx)를 일련번호 필드에 꼭 복사해 두세요. 이렇게 하면 처리 속도가 빨라집니다.

당신이 완료한 후

이 과정에서 NetApp 귀하에게 연락을 드릴 것입니다. 이는 신규 사용자를 대상으로 한 일회성 온보딩 과정입니다.

NetApp 지원 사이트 계정이 있으면 아래 단계를 완료하여 계정을 콘솔 로그인과 연결하세요.NSS 계정이 있는 기존 고객 .

Cloud Volumes ONTAP 지원을 위한 NSS 자격 증명 연결

Cloud Volumes ONTAP 에 대한 다음 주요 워크플로를 활성화하려면 NetApp 지원 사이트 자격 증명을 콘솔 계정과 연결해야 합니다.

- 지원을 위해 Pay-as-you-go Cloud Volumes ONTAP 시스템 등록

  시스템 지원을 활성화하고 NetApp 기술 지원 리소스에 액세스하려면 NSS 계정을 제공해야 합니다.

- BYOL(Bring Your Own License)을 사용할 때 Cloud Volumes ONTAP 배포

  콘솔에서 라이선스 키를 업로드하고 구매한 기간 동안 구독을 활성화하려면 NSS 계정을 제공해야 합니다. 여기에는 기간 갱신을 위한 자동 업데이트가 포함됩니다.

- Cloud Volumes ONTAP 소프트웨어를 최신 릴리스로 업그레이드

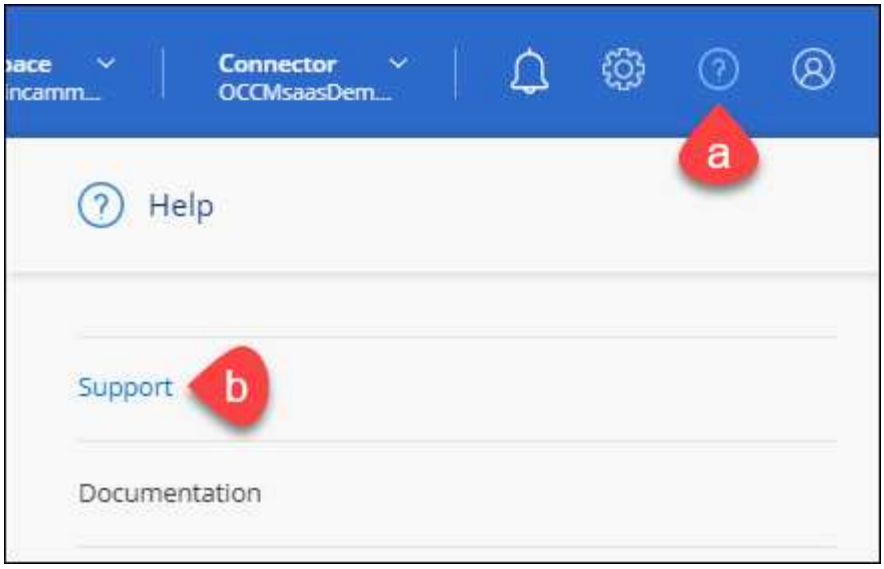
NSS 자격 증명을 NetApp Console 계정과 연결하는 것은 콘솔 사용자 로그인과 연결된 NSS 계정과 다릅니다.

이러한 NSS 자격 증명은 특정 콘솔 계정 ID와 연결됩니다. 콘솔 조직에 속한 사용자는 *지원 > NSS 관리*에서 이러한 자격 증명에 액세스할 수 있습니다.

- 고객 수준 계정이 있는 경우 하나 이상의 NSS 계정을 추가할 수 있습니다.
- 파트너 또는 리셀러 계정이 있는 경우 하나 이상의 NSS 계정을 추가할 수 있지만 고객 수준 계정과 함께 추가할 수는 없습니다.

단계

1. 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 *지원*을 선택하세요.



2. *NSS 관리 > NSS 계정 추가*를 선택하세요.
3. 메시지가 표시되면 *계속*을 선택하여 Microsoft 로그인 페이지로 이동합니다.

   NetApp 지원 및 라이선싱에 특화된 인증 서비스를 위한 ID 공급자로 Microsoft Entra ID를 사용합니다.

4. 로그인 페이지에서 NetApp 지원 사이트에 등록된 이메일 주소와 비밀번호를 입력하여 인증 과정을 진행합니다.

   이러한 작업을 통해 콘솔은 라이선스 다운로드, 소프트웨어 업그레이드 확인, 향후 지원 등록과 같은 작업에 NSS 계정을 사용할 수 있습니다.

   다음 사항에 유의하세요.

   - NSS 계정은 고객 수준 계정이어야 합니다(게스트나 임시 계정이어서는 안 됩니다). 여러 개의 고객 수준 NSS 계정을 가질 수 있습니다.
   - 해당 계정이 파트너 수준 계정인 경우 NSS 계정은 하나만 있을 수 있습니다. 고객 수준 NSS 계정을 추가하려고 하는데 파트너 수준 계정이 이미 있는 경우 다음과 같은 오류 메시지가 표시됩니다.

     "이 계정에는 다른 유형의 NSS 사용자가 이미 있으므로 NSS 고객 유형이 허용되지 않습니다."

   기존 고객 수준 NSS 계정이 있고 파트너 수준 계정을 추가하려는 경우에도 마찬가지입니다.

   - 로그인에 성공하면 NetApp NSS 사용자 이름을 저장합니다.

     이는 귀하의 이메일에 매핑되는 시스템 생성 ID입니다. **NSS** 관리 페이지에서 이메일을 표시할 수 있습니다. ••• 메뉴.

   - 로그인 자격 증명 토큰을 새로 고쳐야 하는 경우 자격 증명 업데이트 옵션도 있습니다. ••• 메뉴.

     이 옵션을 사용하면 다시 로그인하라는 메시지가 표시됩니다. 이 계정의 토큰은 90일 후에 만료됩니다. 이에 대한 알림이 게시됩니다.

도움을 받으세요

NetApp 다양한 방법으로 NetApp Console 과 클라우드 서비스에 대한 지원을 제공합니다. 지식 기반(KB) 문서와 커뮤니티 포럼 등 광범위한 무료 셀프 지원 옵션을 24시간 연중무휴로 이용할 수 있습니다. 지원 등록 시 웹 티켓팅을 통한 원격 기술 지원이 제공됩니다.

클라우드 공급자 파일 서비스에 대한 지원을 받으세요

클라우드 공급자 파일 서비스, 해당 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원에 대해서는 해당 제품의 설명서를 참조하세요.

- "ONTAP 용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

NetApp 과 해당 스토리지 솔루션, 데이터 서비스에 대한 특정 기술 지원을 받으려면 아래에 설명된 지원 옵션을 사용하세요.

셀프 지원 옵션 사용

다음 옵션은 주 7일, 하루 24시간 무료로 이용 가능합니다.

- 설명서

  현재 보고 있는 NetApp Console 문서입니다.

- "지식 기반"

  NetApp 지식 기반을 검색하여 문제 해결에 도움이 되는 문서를 찾아보세요.

- "커뮤니티"

  NetApp Console 커뮤니티에 가입하여 진행 중인 토론을 팔로우하거나 새로운 토론을 만들어 보세요.

NetApp 지원을 통해 사례 만들기

위에 나열된 셀프 지원 옵션 외에도, 지원을 활성화한 후 NetApp 지원 전문가와 협력하여 문제를 해결할 수 있습니다.

시작하기 전에

- 사례 만들기 기능을 사용하려면 먼저 NetApp 지원 사이트 자격 증명을 콘솔 로그인과 연결해야 합니다. "콘솔 로그인과 관련된 자격 증명을 관리하는 방법을 알아보세요." .
- 일련 번호가 있는 ONTAP 시스템에 대한 사례를 개설하는 경우 NSS 계정은 해당 시스템의 일련 번호와 연결되어야 합니다.

단계

1. NetApp Console 에서 *도움말 > 지원*을 선택합니다.
2. 리소스 페이지에서 기술 지원 아래에 있는 사용 가능한 옵션 중 하나를 선택하세요.

a. 전화로 상담원과 통화하고 싶으시면 *전화하기*를 선택하세요. netapp.com에서 전화할 수 있는 전화번호가 나열된 페이지로 이동하게 됩니다.

b. NetApp 지원 전문가에게 티켓을 열려면 *사례 만들기*를 선택하세요.

   - 서비스: 문제와 관련된 서비스를 선택하세요. 예를 들어, * NetApp Console*은 콘솔 내 워크플로 또는 기능과 관련된 기술 지원 문제에 대한 구체적인 내용입니다.
   - 시스템: 스토리지에 해당되는 경우 * Cloud Volumes ONTAP* 또는 *온프레미스*를 선택한 다음 연관된 작업 환경을 선택합니다.

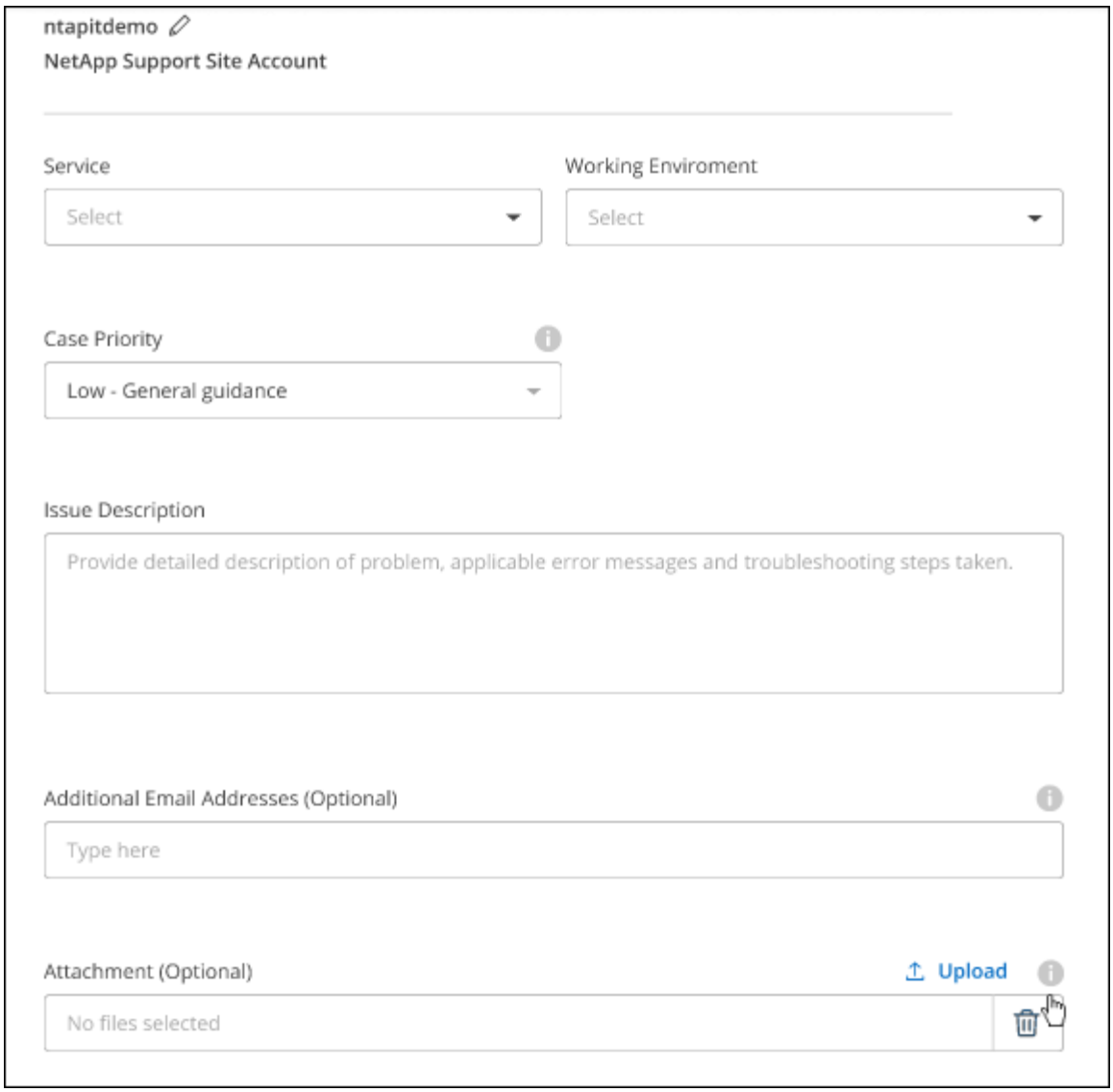
     시스템 목록은 콘솔 조직 범위 내에 있으며, 상단 배너에서 선택한 콘솔 에이전트입니다.

   - 사례 우선순위: 낮음, 보통, 높음 또는 중요로 사례의 우선순위를 선택합니다.

     이러한 우선순위에 대한 자세한 내용을 알아보려면 필드 이름 옆에 있는 정보 아이콘 위에 마우스를 올려놓으세요.

   - 문제 설명: 해당 오류 메시지나 수행한 문제 해결 단계를 포함하여 문제에 대한 자세한 설명을 제공하세요.
   - 추가 이메일 주소: 이 문제를 다른 사람에게 알리려면 추가 이메일 주소를 입력하세요.
   - 첨부파일(선택사항): 최대 5개의 첨부파일을 한 번에 하나씩 업로드하세요.

     첨부파일은 파일당 25MB로 제한됩니다. 다음 파일 확장자가 지원됩니다: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, csv.



당신이 완료한 후

지원 사례 번호가 포함된 팝업이 나타납니다. NetApp 지원 전문가가 귀하의 사례를 검토하고 곧 연락드릴 것입니다.

지원 사례 기록을 보려면 *설정 > 타임라인*을 선택하고 "지원 사례 만들기"라는 이름의 작업을 찾으세요. 가장 오른쪽에 있는 버튼을 누르면 동작을 확장하여 자세한 내용을 볼 수 있습니다.

사례를 생성하려고 할 때 다음과 같은 오류 메시지가 나타날 수 있습니다.

"선택한 서비스에 대해 사례를 생성할 권한이 없습니다."

이 오류는 NSS 계정과 해당 계정과 연결된 기록상 회사가 NetApp Console 계정 일련 번호에 대한 기록상 회사와 동일하지 않다는 것을 의미할 수 있습니다(예: 960xxxx) 또는 작업 환경 일련 번호. 다음 옵션 중 하나를 사용하여 도움을 요청할 수 있습니다.

- 비기술적 사례를 제출하세요 https://mysupport.netapp.com/site/help

지원 사례 관리

콘솔에서 직접 활성화된 지원 사례와 해결된 지원 사례를 보고 관리할 수 있습니다. 귀하의 NSS 계정 및 회사와 관련된

사례를 관리할 수 있습니다.

다음 사항에 유의하세요.

- 페이지 상단의 사례 관리 대시보드는 두 가지 보기를 제공합니다.
  - 왼쪽 보기는 귀하가 제공한 NSS 계정 사용자에 의해 지난 3개월 동안 열린 총 사례를 보여줍니다.
  - 오른쪽 보기는 사용자 NSS 계정을 기준으로 지난 3개월 동안 회사 수준에서 열린 총 사례를 보여줍니다.

  표의 결과는 귀하가 선택한 보기와 관련된 사례를 반영합니다.
- 관심 있는 열을 추가하거나 제거할 수 있으며, 우선순위 및 상태와 같은 열의 내용을 필터링할 수 있습니다. 다른 열은 정렬 기능만 제공합니다.

  자세한 내용은 아래 단계를 참조하세요.
- 사례별로 사례 메모를 업데이트하거나 아직 닫힘 또는 닫힘 보류 상태가 아닌 사례를 닫는 기능을 제공합니다.

단계

1. NetApp Console 에서 *도움말 > 지원*을 선택합니다.
2. *사례 관리*를 선택하고 메시지가 표시되면 콘솔에 NSS 계정을 추가합니다.

   사례 관리 페이지는 콘솔 사용자 계정과 연결된 NSS 계정과 관련된 미해결 사례를 표시합니다. 이는 **NSS** 관리 페이지 상단에 표시되는 NSS 계정과 동일합니다.
3. 필요에 따라 표에 표시되는 정보를 수정합니다.
   - *조직 사례*에서 *보기*를 선택하면 회사와 관련된 모든 사례를 볼 수 있습니다.
   - 정확한 날짜 범위를 선택하거나 다른 기간을 선택하여 날짜 범위를 수정하세요.
   - 열의 내용을 필터링합니다.
   - 표에 나타나는 열을 변경하려면 다음을 선택하세요. 그런 다음 표시하려는 열을 선택합니다.
4. 기존 사례를 관리하려면 다음을 선택하세요. 그리고 사용 가능한 옵션 중 하나를 선택하세요:
   - 사례 보기: 특정 사례에 대한 전체 세부 정보를 확인하세요.
   - 사례 메모 업데이트: 문제에 대한 추가 세부 정보를 제공하거나 *파일 업로드*를 선택하여 최대 5개의 파일을 첨부하세요.

     첨부파일은 파일당 25MB로 제한됩니다. 다음 파일 확장자가 지원됩니다: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, csv.
   - 사건 종결: 사건을 종결하는 이유를 자세히 입력하고 *사건 종결*을 선택하세요.

법적 고지 사항

법적 고지사항은 저작권 표시, 상표, 특허 등에 대한 정보를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NETAPP, NETAPP 로고 및 NetApp 상표 페이지에 나열된 마크는 NetApp, Inc.의 상표입니다. 다른 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 이 소유한 현재 특허 목록은 다음에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인정보 보호정책

"https://www.netapp.com/company/legal/privacy-policy/"

오픈소스

공지 파일은 NetApp 소프트웨어에서 사용되는 타사 저작권 및 라이선스에 대한 정보를 제공합니다.

- "NetApp Console 에 대한 알림"
- "Cloud Volumes ONTAP 에 대한 공지"
- "ONTAP 에 대한 공지"