Cloud Manager 및 Cloud Volumes ONTAP 설명서

Cloud Manager 3.6

NetApp
March 25, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/occm36/index.html on March 25, 2024.
Always check docs.netapp.com for the latest.

목차

Cloud Manager 및 Cloud Volumes ONTAP 설명서 . . . 1
BlueXP . . . 1
새로운 기능 알아보기 . . . 1
시작하십시오 . . . 1
API를 통한 자동화 . . . 1
동료와 연결하고 도움을 받고 더 많은 정보를 찾을 수 있습니다 . . . 1
릴리스 정보 . . . 2
클라우드 관리자 . . . 2
개념 . . . 17
Cloud Manager 및 Cloud Volumes ONTAP 개요 . . . 17
NetApp Cloud Central에서 . . . 18
클라우드 공급자 계정 및 권한 . . . 19
스토리지 . . . 23
고가용성 쌍 . . . 36
평가 중 . . . 44
라이센싱 . . . 44
보안 . . . 45
성능 . . . 47
시작하기 . . . 48
구축 개요 . . . 48
AWS에서 Cloud Volumes ONTAP 시작하기 . . . 49
Azure에서 Cloud Volumes ONTAP 시작하기 . . . 50
Cloud Manager 설정 . . . 51
네트워킹 요구 사항 . . . 67
추가 구축 옵션 . . . 82
Cloud Volumes ONTAP 배포 . . . 91
Cloud Volumes ONTAP 시스템을 생성하기 전에 . . . 91
Cloud Manager에 로그인 . . . 91
Cloud Volumes ONTAP 구성 계획 . . . 92
AWS의 Cloud Volumes ONTAP에서 Flash Cache 활성화 . . . 96
AWS에서 Cloud Volumes ONTAP 실행 . . . 97
Azure에서 Cloud Volumes ONTAP 실행 . . . 106
선불 종량제 시스템을 등록하는 중입니다 . . . 110
Cloud Volumes ONTAP 설정 . . . 111
스토리지 프로비저닝 . . . 113
스토리지 프로비저닝 . . . 113
비활성 데이터를 저비용 오브젝트 스토리지로 계층화 . . . 116
Kubernetes용 영구 스토리지로 Cloud Volumes ONTAP 사용 . . . 119
NetApp 볼륨 암호화로 볼륨 암호화 . . . 122

기존 스토리지 관리 123
볼륨 보기에서 NFS 볼륨 프로비저닝 129
하이브리드 클라우드에서 데이터 관리 134
ONTAP 클러스터 검색 및 관리 134
클라우드 간 데이터 복제 136
데이터를 AWS S3에 동기화 중입니다 143
Cloud Volumes ONTAP 관리 145
Cloud Volumes ONTAP에 연결 중입니다 145
Cloud Volumes ONTAP 소프트웨어를 업데이트하는 중입니다 146
Cloud Volumes ONTAP 시스템 수정 152
Cloud Volumes ONTAP의 상태 관리 156
AWS 리소스 비용 모니터링 157
랜섬웨어에 대한 보호 개선 158
Cloud Manager에 기존 Cloud Volumes ONTAP 시스템 추가 160
Cloud Volumes ONTAP 작업 환경 삭제 160
Cloud Manager 관리 162
Cloud Manager 업데이트 중 162
Cloud Manager 백업 및 복원 163
Cloud Volumes ONTAP 작업 환경 제거 164
사용자 계정 편집 165
프록시 서버를 사용하도록 Cloud Manager 구성 165
Cloud Manager HTTPS 인증서를 갱신하는 중입니다 166
Cloud Manager 제거 중 166
API 및 자동화 167
코드로서 인프라를 위한 자동화 샘플 167
참조하십시오 168
질문과 대답: Cloud Manager와 NetApp Cloud Central의 통합 168
AWS의 보안 그룹 규칙 169
Azure의 보안 그룹 규칙 177
Cloud Manager에 대한 AWS 및 Azure 권한 183
기본 설정 187
사용자 역할 190
도움을 받을 수 있는 곳 및 자세한 정보를 얻을 수 있는 곳 190
법적 고지 192
저작권 192
상표 192
특허 192
개인 정보 보호 정책 192
오픈 소스 192

Cloud Manager 및 Cloud Volumes ONTAP 설명서

OnCommand Cloud Manager를 사용하면 클라우드 기반 워크로드를 보호, 가시성, 제어하는 데이터 관리 솔루션인 NetApp Cloud Volumes ONTAP를 구축 및 관리할 수 있습니다.

BlueXP

NetApp BlueXP는 Cloud Manager를 통해 제공되는 기능을 확장하고 개선합니다.

"BlueXP 문서로 이동합니다"

새로운 기능 알아보기

- "Cloud Manager의 새로운 기능"
- "Cloud Volumes ONTAP의 새로운 기능"

시작하십시오

- "AWS에서 시작하십시오"
- "Azure에서 시작하십시오"
- "Cloud Volumes ONTAP에 지원되는 구성을 찾습니다"
- "Cloud Manager에 대한 자세한 네트워킹 요구사항을 검토합니다"
- "Cloud Volumes ONTAP for AWS에 대한 자세한 네트워킹 요구사항을 검토하십시오"
- "Cloud Volumes ONTAP for Azure에 대한 자세한 네트워킹 요구사항을 검토하십시오"
- "Cloud Volumes ONTAP 구성 계획"

API를 통한 자동화

- "API 개발자 가이드 를 참조하십시오"
- "자동화 샘플"

동료와 연결하고 도움을 받고 더 많은 정보를 찾을 수 있습니다

- "NetApp 커뮤니티: 클라우드 데이터 서비스"
- "NetApp Cloud Volumes ONTAP 지원"
- "도움을 받을 수 있는 곳 및 자세한 정보를 얻을 수 있는 곳"

릴리스 정보

클라우드 관리자

Cloud Manager 3.6의 새로운 기능

OnCommand Cloud Manager에는 일반적으로 새로운 기능, 향상 기능 및 버그 수정을 제공하기 위해 매월 새로운 릴리즈가 도입되었습니다.

이전 릴리스를 찾으십니까?"3.5의 새로운 기능"
"3.4의 새로운 기능"

AWS C2S 환경 지원(2019년 5월 2일)

Cloud Volumes ONTAP 9.5 및 Cloud Manager 3.6.4는 현재 미국에서 사용할 수 있습니다 C2S(AWS Commercial Cloud Services) 환경을 통한 IC(Intelligence Community) C2S에 HA 쌍 및 단일 노드 시스템을 구축할 수 있습니다.

"AWS 상용 클라우드 서비스 환경을 위한 빠른 시작 가이드"

Cloud Manager 3.6.6(2019년 5월 1일)

- AWS에서 6TB 디스크 지원
- Azure에서 단일 노드 시스템으로 새로운 디스크 크기 지원
- Azure에서 단일 노드 시스템으로 표준 SSD 지원
- NetApp Kubernetes Service를 통해 생성된 Kubernetes 클러스터의 자동 검색
- NTP 서버를 구성하는 기능입니다

AWS에서 6TB 디스크 지원

이제 Cloud Volumes ONTAP for AWS로 EBS 디스크 크기를 6TB로 선택할 수 있습니다. 최근 을 클릭합니다 "범용 SSD의 향상된 성능"이제 최대 성능을 위해 6TB 디스크가 가장 적합합니다.

이 변경 사항은 Cloud Volumes ONTAP 9.5, 9.4 및 9.3에서 지원됩니다.

Azure에서 단일 노드 시스템으로 새로운 디스크 크기 지원

이제 Azure의 단일 노드 시스템에서 8TB, 16TB 및 32TB 디스크를 사용할 수 있습니다. 디스크 크기가 커지면 Premium 또는 BYOL 라이센스를 사용할 때 디스크만으로 최대 368TB의 시스템 용량을 달성할 수 있습니다.

이 변경 사항은 Cloud Volumes ONTAP 9.5, 9.4 및 9.3에서 지원됩니다.

Azure에서 단일 노드 시스템으로 표준 SSD 지원

표준 SSD 관리 디스크는 이제 Azure의 단일 노드 시스템에서 지원됩니다. 이러한 디스크는 프리미엄 SSD와 표준 HDD 간에 높은 수준의 성능을 제공합니다.

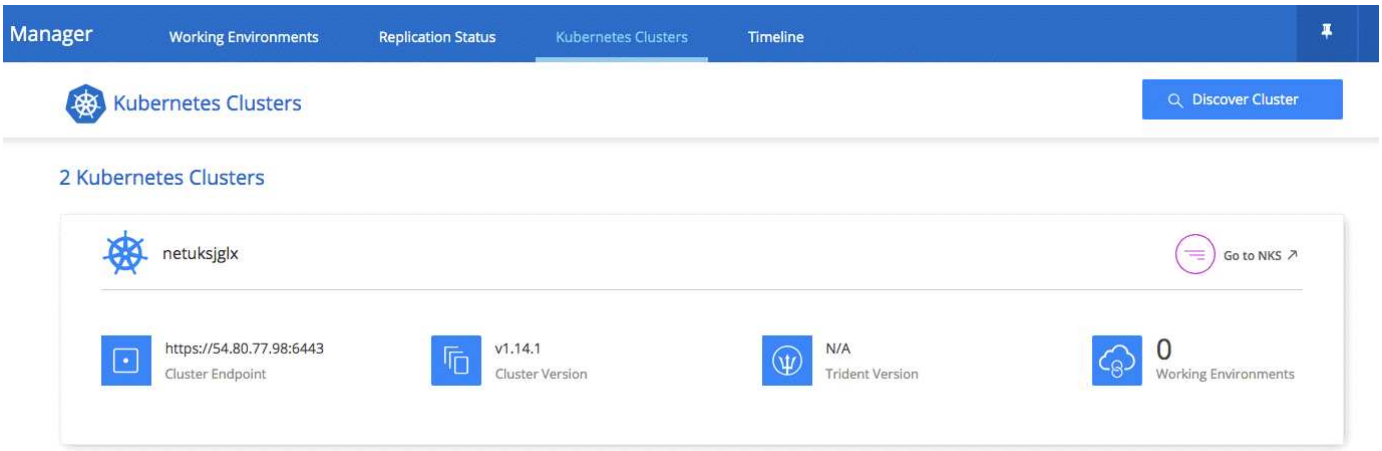
이 변경 사항은 Cloud Volumes ONTAP 9.5, 9.4 및 9.3에서 지원됩니다.

"표준 SSD에 대해 자세히 알아보십시오".

NetApp Kubernetes Service를 통해 생성된 **Kubernetes** 클러스터의 자동 검색

Cloud Manager는 이제 NetApp Kubernetes Service를 사용하여 구축하는 Kubernetes 클러스터를 자동으로 검색할 수 있습니다. 이를 통해 Kubernetes 클러스터를 Cloud Volumes ONTAP 시스템에 연결하여 컨테이너에 영구 스토리지로 사용할 수 있습니다.

다음 이미지는 자동으로 검색된 Kubernetes 클러스터를 보여줍니다. "NKS로 이동" 링크를 통해 NetApp Kubernetes Service에 직접 연락할 수 있습니다.



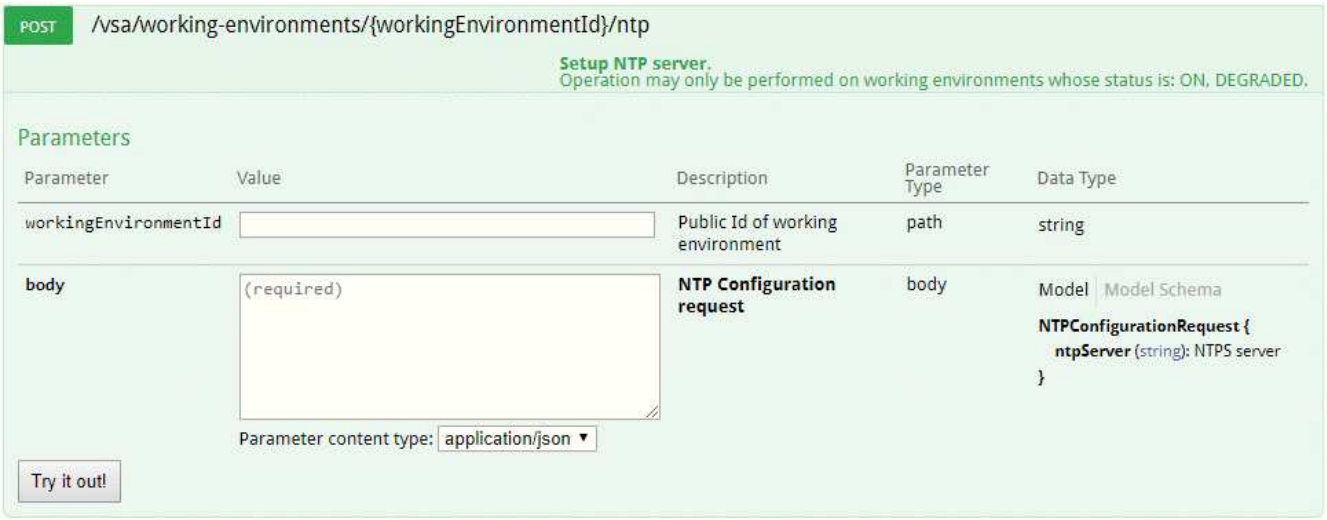
"작업 환경을 Kubernetes 클러스터에 연결하는 방법을 알아보십시오".

NTP 서버를 구성하는 기능입니다

이제 NTP(네트워크 시간 프로토콜) 서버를 사용하도록 Cloud Volumes ONTAP를 구성할 수 있습니다. NTP 서버를 지정하면 네트워크 시스템 간의 시간이 동기화되어 시간 차이로 인한 문제를 방지할 수 있습니다.

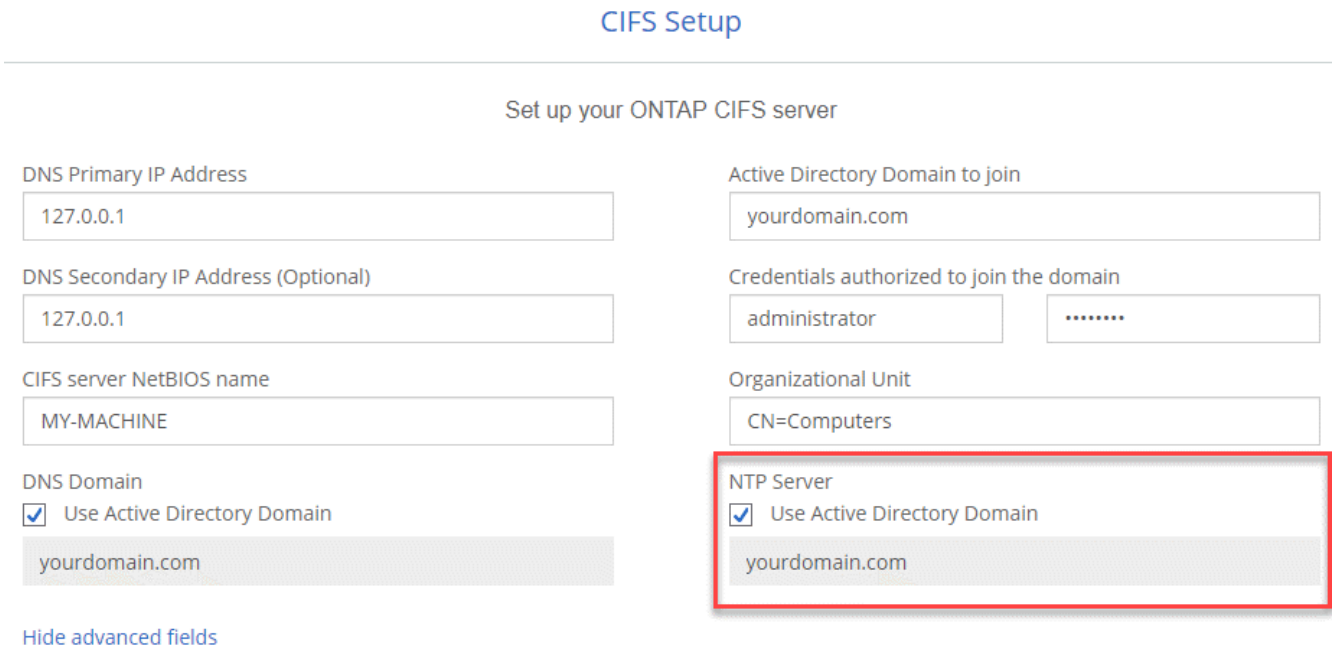
CIFS 서버를 설정할 때 Cloud Manager API를 사용하거나 사용자 인터페이스에서 NTP 서버를 지정합니다.

- 를 클릭합니다 "Cloud Manager API" NTP 서버의 주소를 지정할 수 있습니다. 다음은 AWS의 단일 노드 시스템용 API입니다.



- CIFS 서버를 구성할 때 Cloud Manager 사용자 인터페이스를 통해 Active Directory 도메인을 사용하는 NTP 서버를 지정할 수 있습니다. 다른 주소를 사용해야 하는 경우 API를 사용해야 합니다.

  다음 이미지는 CIFS 설정 시 사용할 수 있는 NTP 서버 필드를 보여 줍니다.



Cloud Manager 3.6.5(2019년 4월 2일)

Cloud Manager 3.6.5에는 다음과 같은 향상된 기능이 포함되어 있습니다.

- Kubernetes의 향상된 기능
- NetApp Support 사이트 계정은 이제 시스템 수준에서 관리됩니다
- AWS 전송 게이트웨이는 부동 IP 주소에 액세스할 수 있습니다
- Azure 리소스 그룹이 잠겼습니다
- 이제 NFS 4 및 NFS 4.1이 기본적으로 사용하도록 설정됩니다
- 새로운 API를 사용하여 ONTAP 스냅샷 복사본을 삭제할 수 있습니다

Kubernetes의 향상된 기능

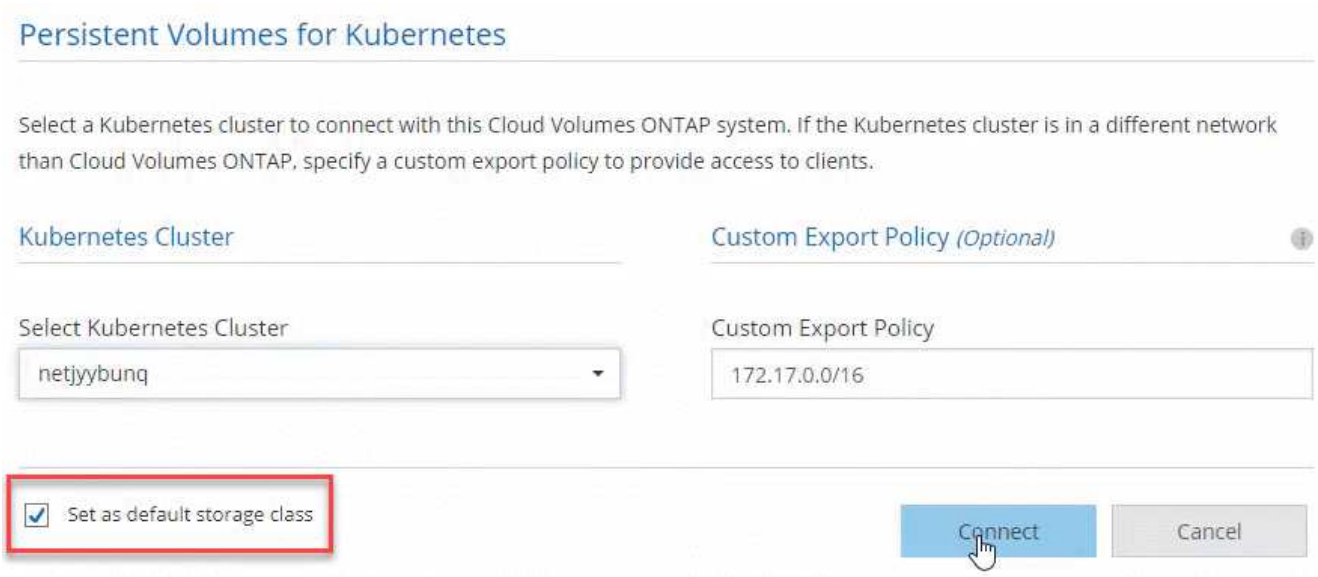
컨테이너용 영구 스토리지로 Cloud Volumes ONTAP를 더 쉽게 사용할 수 있도록 몇 가지 기능이 향상되었습니다.

- 이제 여러 Kubernetes 클러스터를 Cloud Manager에 추가할 수 있습니다.

  따라서 여러 클러스터를 서로 다른 Cloud Volumes ONTAP 시스템에 연결하고 여러 클러스터를 동일한 Cloud Volumes ONTAP 시스템에 연결할 수 있습니다.

- 클러스터를 연결하면 이제 Cloud Volumes ONTAP를 Kubernetes 클러스터의 기본 스토리지 클래스로 설정할 수 있습니다.

  사용자가 영구 볼륨을 생성할 때 Kubernetes 클러스터는 기본적으로 Cloud Volumes ONTAP를 백엔드 스토리지로 사용할 수 있습니다.



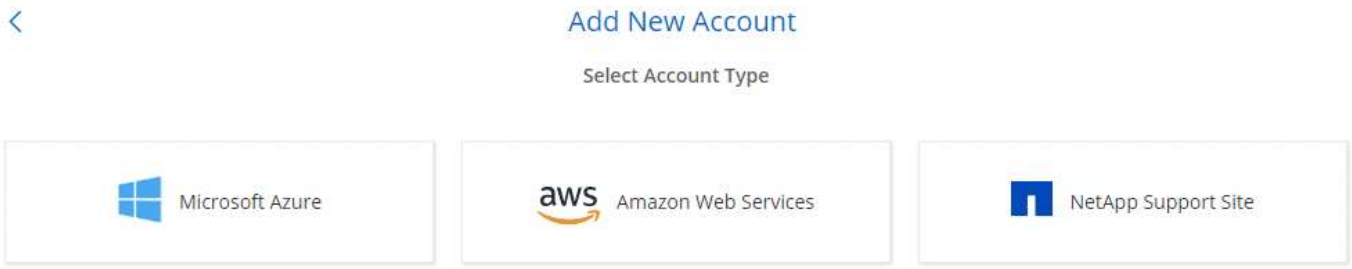
- Cloud Manager에서 Kubernetes 스토리지 클래스를 더 쉽게 식별할 수 있도록 이름 지정하는 방법을 변경했습니다.
  - * NetApp-파일 *: 단일 노드 Cloud Volumes ONTAP 시스템에 영구 볼륨을 바인딩하는 데 사용됩니다
  - * NetApp-파일-중복 *: 영구 볼륨을 Cloud Volumes ONTAP HA 쌍에 바인딩하는 데 사용됩니다
- Cloud Manager가 설치한 NetApp Trident의 버전이 최신 버전으로 업데이트되었습니다.

"Kubernetes의 영구 스토리지로 Cloud Volumes ONTAP를 사용하는 방법에 대해 알아보십시오".

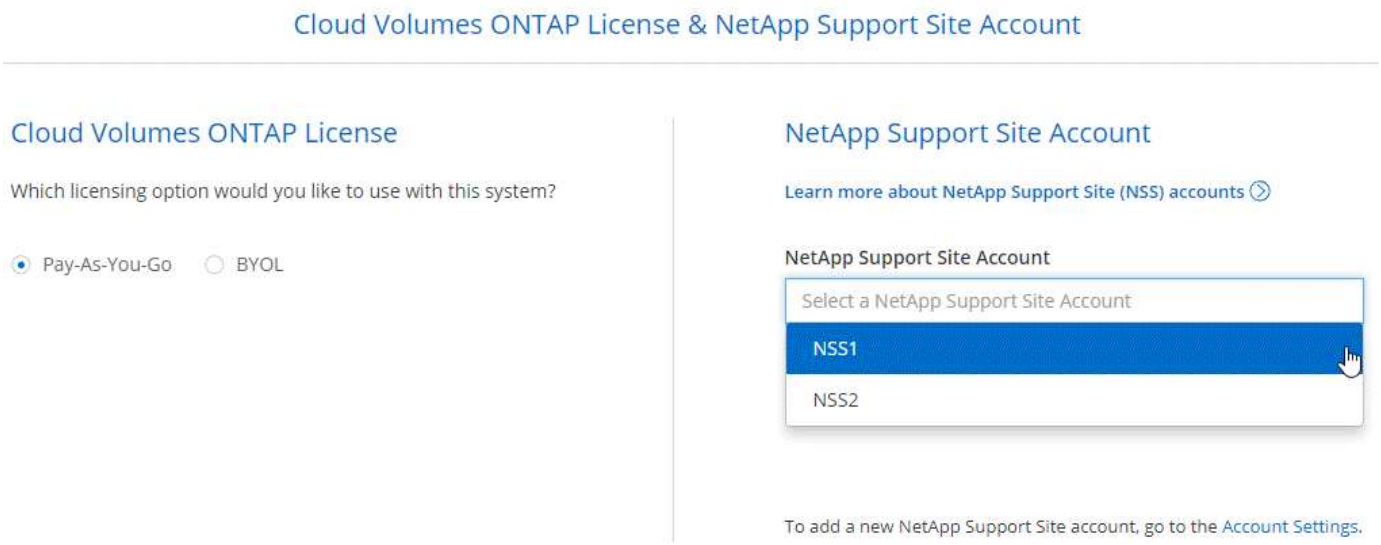
NetApp Support 사이트 계정은 이제 시스템 수준에서 관리됩니다

이제 Cloud Manager에서 NetApp Support 사이트 계정을 더 쉽게 관리할 수 있습니다.

이전 릴리스에서는 NetApp Support 사이트 계정을 특정 테넌트에 연결해야 했습니다. 이제 클라우드 공급자 계정을 관리하는 것과 동일한 위치에서 Cloud Manager 시스템 수준에서 계정이 관리됩니다. 이러한 변경 사항을 통해 Cloud Volumes ONTAP 시스템을 등록할 때 여러 NetApp Support 사이트 계정 중에서 원하는 계정을 유연하게 선택할 수 있습니다.



새로운 작업 환경을 생성하는 경우 NetApp Support 사이트 계정을 선택하여 Cloud Volumes ONTAP 시스템을 다음 사이트에 등록하기만 하면 됩니다.



Cloud Manager를 3.6.5로 업데이트하면, 이전에 테넌트를 계정에 연결했던 경우 NetApp Support 사이트 계정이 자동으로 추가됩니다.

"NetApp Support 사이트 계정을 Cloud Manager에 추가하는 방법을 알아보십시오".

AWS 전송 게이트웨이는 부동 **IP** 주소에 액세스할 수 있습니다

여러 AWS Availability Zone의 HA 쌍에서는 NAS 데이터 액세스 및 관리 인터페이스에 _floating IP address_를 사용합니다. 지금까지는 HA 쌍이 상주하는 VPC 외부에서 해당 부동 IP 주소에 액세스할 수 없었습니다.

을(를) 사용할 수 있는지 확인했습니다 "AWS 전송 게이트웨이" VPC 외부에서 부동 IP 주소에 액세스할 수 있도록 합니다. 즉, VPC 외부에 있는 NetApp 관리 툴 및 NAS 클라이언트가 유동 IP에 액세스하고 자동 페일오버를 활용할 수 있습니다.

"여러 AZs에서 HA 쌍에 대한 AWS 전송 게이트웨이를 설정하는 방법에 대해 알아보십시오".

Azure 리소스 그룹이 잠겼습니다

이제 Cloud Manager에서 Azure 리소스 그룹을 생성할 때 Cloud Volumes ONTAP 리소스 그룹을 잠급니다. 리소스 그룹을 잠그면 사용자가 실수로 중요한 리소스를 삭제하거나 수정할 수 없습니다.

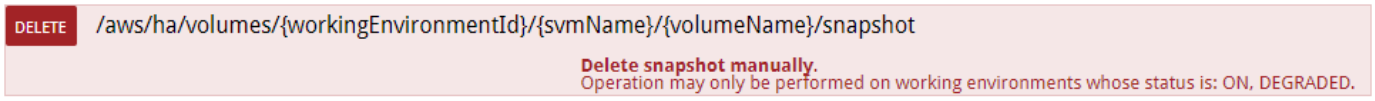
이제 **NFS 4** 및 **NFS 4.1**이 기본적으로 사용하도록 설정됩니다

이제 Cloud Manager에서 제공하는 새로운 모든 Cloud Volumes ONTAP 시스템에서 NFS 4 및 NFS 4.1 프로토콜을 사용할 수 있습니다. 이 변경 사항은 더 이상 수동으로 프로토콜을 활성화할 필요가 없기 때문에 시간을 절약할 수 있습니다.

새로운 **API**를 사용하여 **ONTAP** 스냅샷 복사본을 삭제할 수 있습니다

이제 Cloud Manager API 호출을 사용하여 읽기-쓰기 볼륨의 스냅샷 복사본을 삭제할 수 있습니다.

다음은 AWS의 HA 시스템에 대한 API 호출의 예입니다.



AWS의 단일 노드 시스템과 Azure의 단일 노드 및 HA 시스템에 유사한 API 호출을 사용할 수 있습니다.

"OnCommand Cloud Manager API 개발자 가이드 를 참조하십시오"

Cloud Manager 3.6.4 업데이트**(2019**년 **3**월 **18**일**)**

Cloud Volumes ONTAP용 9.5 P1 패치 릴리스를 지원하도록 Cloud Manager가 업데이트되었습니다. 이 패치 릴리즈를 사용하면 Azure의 HA 쌍이 이제 GA(GA)로 제공됩니다.

를 참조하십시오 "Cloud Volumes ONTAP 9.5 릴리스 정보" HA 쌍에 대한 Azure 지역 지원에 대한 중요한 정보를 포함하여 자세한 내용은 을 참조하십시오.

Cloud Manager 3.6.4(2019년 **3**월 **3**일**)**

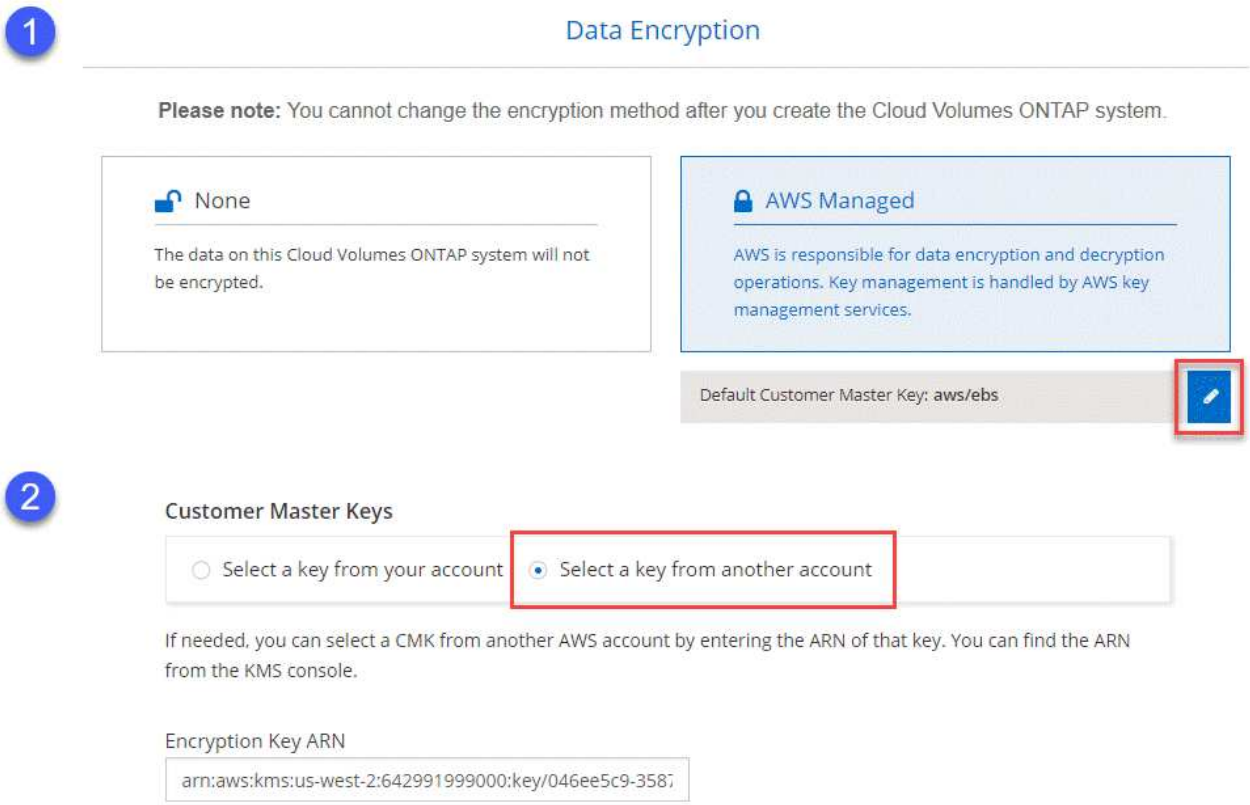
Cloud Manager 3.6.4에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 다른 계정의 키로 AWS 관리 암호화
- 오류가 발생한 디스크 복구
- Blob 컨테이너에 데이터를 계층화할 때 HTTPS에 대해 Azure 스토리지 계정이 활성화됩니다

다른 계정의 키로 **AWS** 관리 암호화

AWS에서 Cloud Volumes ONTAP 시스템을 시작하면 이제 를 사용하도록 설정할 수 있습니다 "AWS로 관리하는 이기종 암호화" 다른 AWS 사용자 계정의 CMK(Customer Master Key) 사용

다음 이미지는 새 작업 환경을 만들 때 옵션을 선택하는 방법을 보여줍니다.



"지원되는 암호화 기술에 대해 자세히 알아보십시오".

오류가 발생한 디스크 복구

Cloud Manager는 이제 Cloud Volumes ONTAP 시스템에서 장애가 발생한 디스크를 복구하려고 시도합니다. 성공한 시도는 이메일 알림 보고서에 기록됩니다. 다음은 샘플 알림입니다.

사용자 계정을 편집하여 알림 보고서를 활성화할 수 있습니다.

Blob 컨테이너에 데이터를 계층화할 때 HTTPS에 대해 Azure 스토리지 계정이 활성화됩니다

비활성 데이터를 Azure Blob 컨테이너에 계층화하도록 Cloud Volumes ONTAP 시스템을 설정하면 Cloud Manager에서 해당 컨테이너에 대한 Azure 저장소 계정을 만듭니다. 이 릴리스부터 Cloud Manager는 이제 보안 전송(HTTPS)을 통해 새 저장소 계정을 활성화합니다. 기존 스토리지 계정은 계속해서 HTTP를 사용합니다.

Cloud Manager 3.6.3(2019년 2월 4일)

Cloud Manager 3.6.3에는 다음과 같은 개선 사항이 포함되어 있습니다.

- Cloud Volumes ONTAP 9.5 GA에 대한 지원
- 모든 프리미엄 및 BYOL 구성에 368TB 용량 제한
- 새로운 AWS 지역 지원
- S3 지능형 계층화 지원
- 초기 애그리게이트에서 데이터 계층화를 사용하지 않도록 설정하는 기능
- Cloud Manager에 권장되는 EC2 인스턴스 유형은 현재 T3.MEDIUM입니다
- 데이터 전송 중 예정된 종료 연기

Cloud Volumes ONTAP 9.5 GA에 대한 지원

Cloud Manager는 이제 Cloud Volumes ONTAP 9.5의 GA(General Availability) 릴리즈를 지원합니다. 여기에는 AWS의 M5 및 R5 인스턴스에 대한 지원이 포함됩니다. 9.5 릴리스에 대한 자세한 내용은 를 참조하십시오 "Cloud Volumes ONTAP 9.5 릴리스 정보".

모든 프리미엄 및 BYOL 구성에 368TB 용량 제한

Cloud Volumes ONTAP Premium 및 BYOL의 시스템 용량 제한은 이제 모든 구성(AWS 및 Azure의 단일 노드 및 HA)에서 368TB입니다. 이 변경 사항은 Cloud Volumes ONTAP 9.5, 9.4 및 9.3(9.3을 포함한 AWS에만 해당)에 적용됩니다.

일부 구성에서는 디스크 제한만으로 368TB의 용량 제한에 도달하지 못합니다. 이 경우 의 용량 제한에 도달할 수 있습니다 "비활성 데이터를 오브젝트 스토리지로 계층화". 예를 들어, Azure의 단일 노드 시스템은 252TB의 디스크

기반 용량을 가질 수 있으며 Azure Blob 스토리지에서 최대 116TB의 비활성 데이터를 허용합니다.

디스크 제한에 대한 자세한 내용은 의 스토리지 제한을 참조하십시오 "Cloud Volumes ONTAP 릴리즈 노트".

새로운 **AWS** 지역 지원

Cloud Manager 및 Cloud Volumes ONTAP는 현재 다음 AWS 지역에서 지원됩니다.

- 유럽(스톡홀름)

  단일 노드 시스템만 해당합니다. 현재 HA 쌍은 지원되지 않습니다.

- GovCloud(미국 - 동부)

  또한, AWS GovCloud(미국-서부) 지역을 지원할 수 있습니다.

"지원되는 지역의 전체 목록을 참조하십시오".

S3 지능형 계층화 지원

AWS에서 데이터 계층화를 활성화하면 Cloud Volumes ONTAP은 기본적으로 비활성 데이터를 S3 표준 스토리지 클래스로 계층화합니다. 이제 계층화 레벨을 _Intelligent Tiering_storage 클래스로 변경할 수 있습니다. 이 스토리지 클래스는 데이터 액세스 패턴이 변경될 때 두 계층 간에 데이터를 이동하여 스토리지 비용을 최적화합니다. 한 계층은 잦은 액세스를 위한 반면 다른 계층은 낮은 액세스 빈도로 사용됩니다.

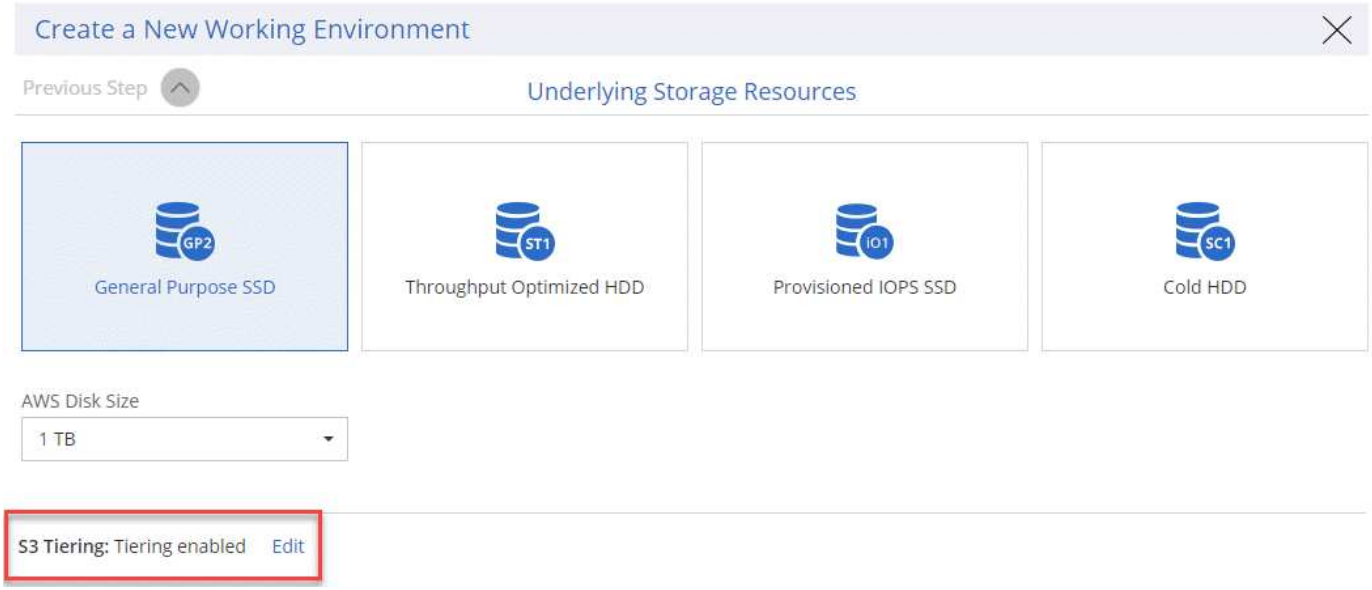
이전 릴리즈에서와 마찬가지로 Standard - Infrequent Access 계층과 One Zone - Infrequent Access 계층도 사용할 수 있습니다.

"데이터 계층화에 대해 자세히 알아보십시오" 및 "스토리지 클래스를 변경하는 방법에 대해 알아보십시오".

초기 애그리게이트에서 데이터 계층화를 사용하지 않도록 설정하는 기능

이전 릴리즈에서는 Cloud Manager가 초기 Cloud Volumes ONTAP 애그리게이트에서 데이터 계층화를 자동으로 사용하도록 설정되었습니다. 이제 이 초기 애그리게이트에서 데이터 계층화를 사용하지 않도록 선택할 수 있습니다. 후속 애그리게이트에서도 데이터 계층화를 설정하거나 해제할 수 있습니다.

이 새로운 옵션은 기본 스토리지 리소스를 선택할 때 사용할 수 있습니다. 다음 이미지는 AWS에서 시스템을 시작할 때의 예를 보여줍니다.



Cloud Manager에 권장되는 **EC2** 인스턴스 유형은 현재 **T3.MEDIUM**입니다

Cloud Manager의 인스턴스 유형은 이제 T3.MEDIUM으로 NetApp Cloud Central에서 AWS에 Cloud Manager를 구축할 수 있습니다. 또한 AWS Marketplace에서 권장되는 인스턴스 유형이기도 합니다. 이러한 변경을 통해 최신 AWS 지역에서 지원을 제공하고 인스턴스 비용을 줄일 수 있습니다. 권장 인스턴스 유형은 이전에 T2.medium로, 여전히 지원됩니다.

데이터 전송 중 예정된 종료 연기

Cloud Volumes ONTAP 시스템의 자동 종료를 예약한 경우, Cloud Manager는 활성 데이터 전송이 진행 중인 경우 종료를 연기합니다. 전송이 완료된 후 Cloud Manager가 시스템을 종료합니다.

Cloud Manager 3.6.2(2019년 1월 2일)

Cloud Manager 3.6.2에는 새로운 기능과 개선 사항이 포함되어 있습니다.

- Cloud Volumes ONTAP HA를 위한 AWS의 배치 그룹이 단일 AZ에 분산되어 있습니다
- 랜섬웨어 보호
- 새로운 데이터 복제 정책
- Kubernetes의 볼륨 액세스 제어

Cloud Volumes ONTAP HA를 위한 **AWS**의 배치 그룹이 단일 **AZ**에 분산되어 있습니다

단일 AWS 가용성 영역에 Cloud Volumes ONTAP HA를 구축하면 Cloud Manager에서 을 생성할 수 있습니다 "AWS 배치 그룹 분산" 그런 다음 해당 배치 그룹에서 2개의 HA 노드를 시작합니다. 배치 그룹은 서로 다른 기본 하드웨어에 인스턴스를 분산하여 동시 오류 위험을 줄입니다.

이 기능은 디스크 장애 관점이 아니라 컴퓨팅 측면에서 중복성을 향상시킵니다.

Cloud Manager에는 이 기능에 대한 새로운 권한이 필요합니다. Cloud Manager에 권한을 제공하는 IAM 정책에 다음 작업이 포함되어 있는지 확인합니다.

```
"ec2:CreatePlacementGroup",
"ec2:DeletePlacementGroup"
```

에서 필요한 사용 권한의 전체 목록을 찾을 수 있습니다 "Cloud Manager의 최신 AWS 정책".

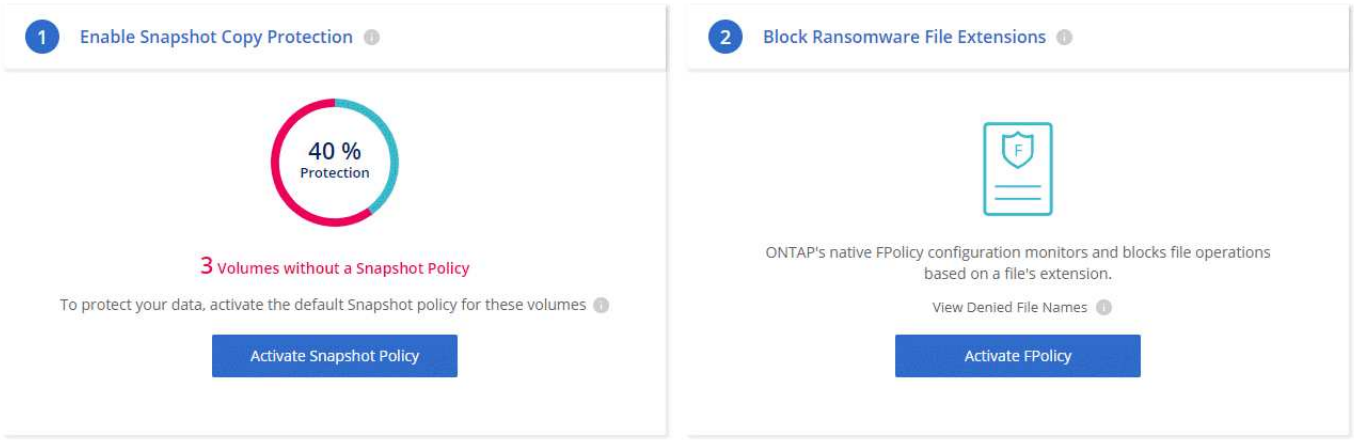
랜섬웨어 보호

랜섬웨어 공격은 비즈니스 시간, 리소스 및 평판에 악영향을 줄 수 있습니다. Cloud Manager에서 이제 랜섬웨어에 대한 NetApp 솔루션을 구현할 수 있으며, 이 솔루션은 가시성, 탐지, 문제 해결을 위한 효율적인 툴을 제공합니다.

- Cloud Manager는 스냅샷 정책에 의해 보호되지 않는 볼륨을 식별하고 이러한 볼륨에서 기본 스냅샷 정책을 활성화할 수 있도록 지원합니다.

  Snapshot 복사본은 읽기 전용이므로 랜섬웨어 손상을 방지합니다. 또한 세분화하여 단일 파일 복사본 또는 전체 재해 복구 솔루션의 이미지를 생성할 수도 있습니다.

- Cloud Manager를 사용하면 ONTAP의 FPolicy 솔루션을 활성화하여 일반적인 랜섬웨어 파일 확장을 차단할 수도 있습니다.



"랜섬웨어에 대한 NetApp 솔루션을 구축하는 방법을 알아보십시오".

새로운 데이터 복제 정책

Cloud Manager에는 데이터 보호에 사용할 수 있는 5가지 새로운 데이터 복제 정책이 있습니다.

세 가지 정책은 동일한 대상 볼륨에 재해 복구 및 백업의 장기 보존을 구성합니다. 각 정책은 서로 다른 백업 보존 기간을 제공합니다.

- 미러링 및 백업(7년 보존)
- 미러링 및 백업(7년 보존, 더 많은 주별 백업 포함)
- 미러 및 백업(1년 보존, 매월)

나머지 정책은 백업을 장기간 보존할 수 있는 더 많은 옵션을 제공합니다.

- 백업(1개월 보존)

- 백업(1주 보존)

작업 환경을 끌어다 놓기만 하면 새 정책 중 하나를 선택할 수 있습니다.

Kubernetes의 볼륨 액세스 제어

이제 Kubernetes 영구 볼륨의 엑스포트 정책을 구성할 수 있습니다. Kubernetes 클러스터가 Cloud Volumes ONTAP 시스템과 다른 네트워크에 있는 경우, 엑스포트 정책을 통해 클라이언트에 액세스할 수 있습니다.

작업 환경을 Kubernetes 클러스터에 연결할 때와 기존 볼륨을 편집하여 엑스포트 정책을 구성할 수 있습니다.

Cloud Manager 3.6.1(2018년 12월 4일)

Cloud Manager 3.6.1에는 새로운 기능과 개선 사항이 포함되어 있습니다.

- Azure에서 Cloud Volumes ONTAP 9.5를 지원합니다
- 클라우드 공급자 계정
- AWS 비용 보고서의 향상된 기능
- 새로운 Azure 지역 지원

Azure에서 Cloud Volumes ONTAP 9.5를 지원합니다

Cloud Manager는 이제 Microsoft Azure에서 Cloud Volumes ONTAP 9.5 릴리즈를 지원하며, 이 릴리스에는 고가용성(HA) 쌍의 미리 보기가 포함되어 있습니다. Azure HA 쌍에 대한 미리 보기 라이센스를 요청하려면 ng-Cloud-Volume-ONTAP-preview@netapp.com 으로 문의하십시오.

9.5 릴리스에 대한 자세한 내용은 를 참조하십시오 "Cloud Volumes ONTAP 9.5 릴리스 정보".

Cloud Volumes ONTAP 9.5에 필요한 새 Azure 사용 권한

Cloud Manager를 사용하려면 Cloud Volumes ONTAP 9.5 릴리스의 주요 기능에 대한 새로운 Azure 권한이 필요합니다. Cloud Manager에서 Cloud Volumes ONTAP 9.5 시스템을 배포 및 관리할 수 있도록 다음 권한을 추가하여 Cloud Manager 정책을 업데이트해야 합니다.

```
"Microsoft.Network/loadBalancers/read",
"Microsoft.Network/loadBalancers/write",
"Microsoft.Network/loadBalancers/delete",
"Microsoft.Network/loadBalancers/backendAddressPools/read",
"Microsoft.Network/loadBalancers/backendAddressPools/join/action",
"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
"Microsoft.Network/loadBalancers/loadBalancingRules/read",
"Microsoft.Network/loadBalancers/probes/read",
"Microsoft.Network/loadBalancers/probes/join/action",
"Microsoft.Network/routeTables/join/action"
"Microsoft.Authorization/roleDefinitions/write",
"Microsoft.Authorization/roleAssignments/write",
"Microsoft.Web/sites/*"
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/usages/read",
```

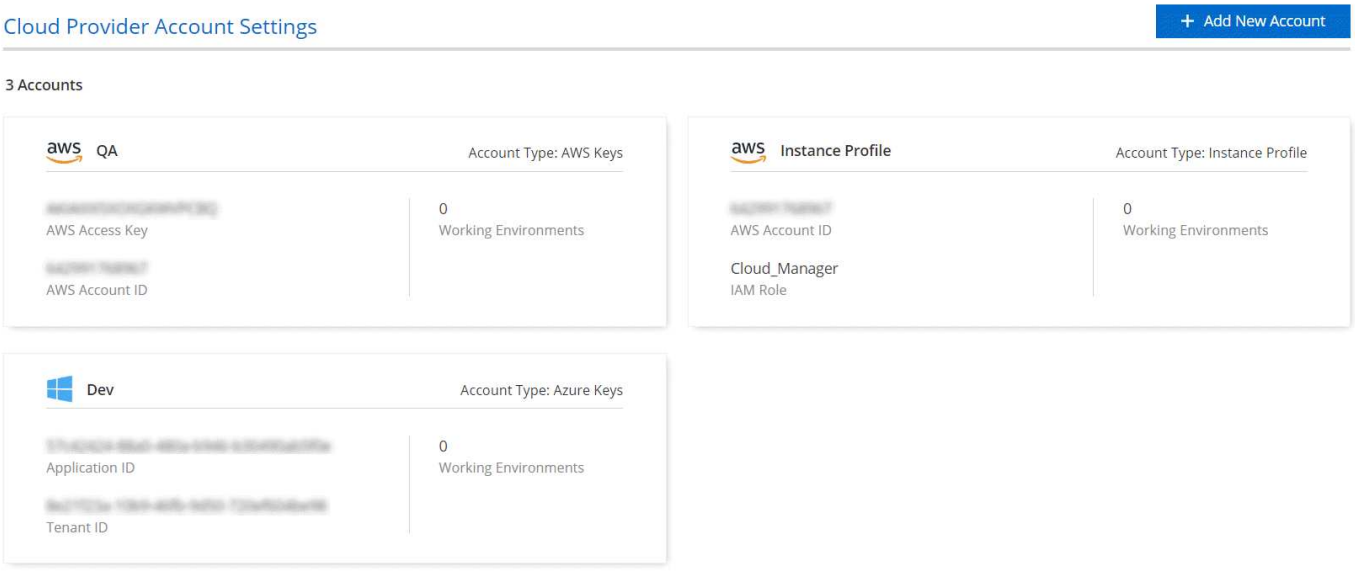
에서 필요한 사용 권한의 전체 목록을 찾을 수 있습니다 "Cloud Manager에 대한 최신 Azure 정책".

"Cloud Manager에서 이러한 권한을 사용하는 방법에 대해 알아봅니다".

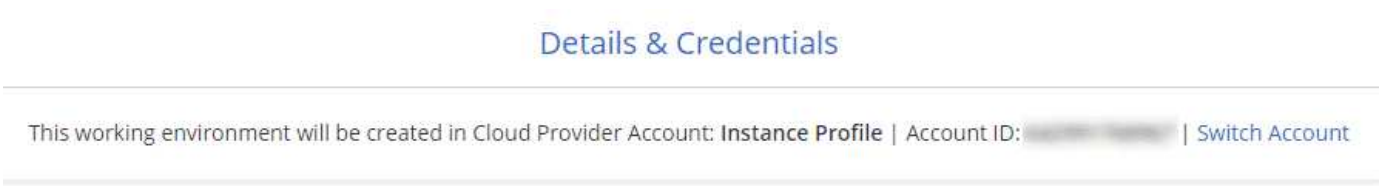
클라우드 공급자 계정

이제 Cloud Provider 계정을 사용하여 Cloud Manager에서 여러 AWS 및 Azure 계정을 더 쉽게 관리할 수 있습니다.

이전 릴리즈에서는 각 Cloud Manager 사용자 계정에 대한 클라우드 공급자 권한을 지정해야 했습니다. 이제 클라우드 공급자 계정을 사용하여 Cloud Manager 시스템 수준에서 사용 권한이 관리됩니다.



새 작업 환경을 만들 때 Cloud Volumes ONTAP 시스템을 배포할 계정을 선택하기만 하면 됩니다.



3.6.1로 업그레이드하면 Cloud Manager는 현재 구성을 기반으로 자동으로 클라우드 공급자 계정을 만듭니다. 스크립트가 있는 경우 이전 버전과의 호환성이 제공되므로 문제가 없습니다.

- "클라우드 공급자 계정 및 사용 권한 작동 방식에 대해 알아보십시오"
- "Cloud Manager에 클라우드 공급자 계정을 설정 및 추가하는 방법에 대해 알아보십시오"

AWS 비용 보고서의 향상된 기능

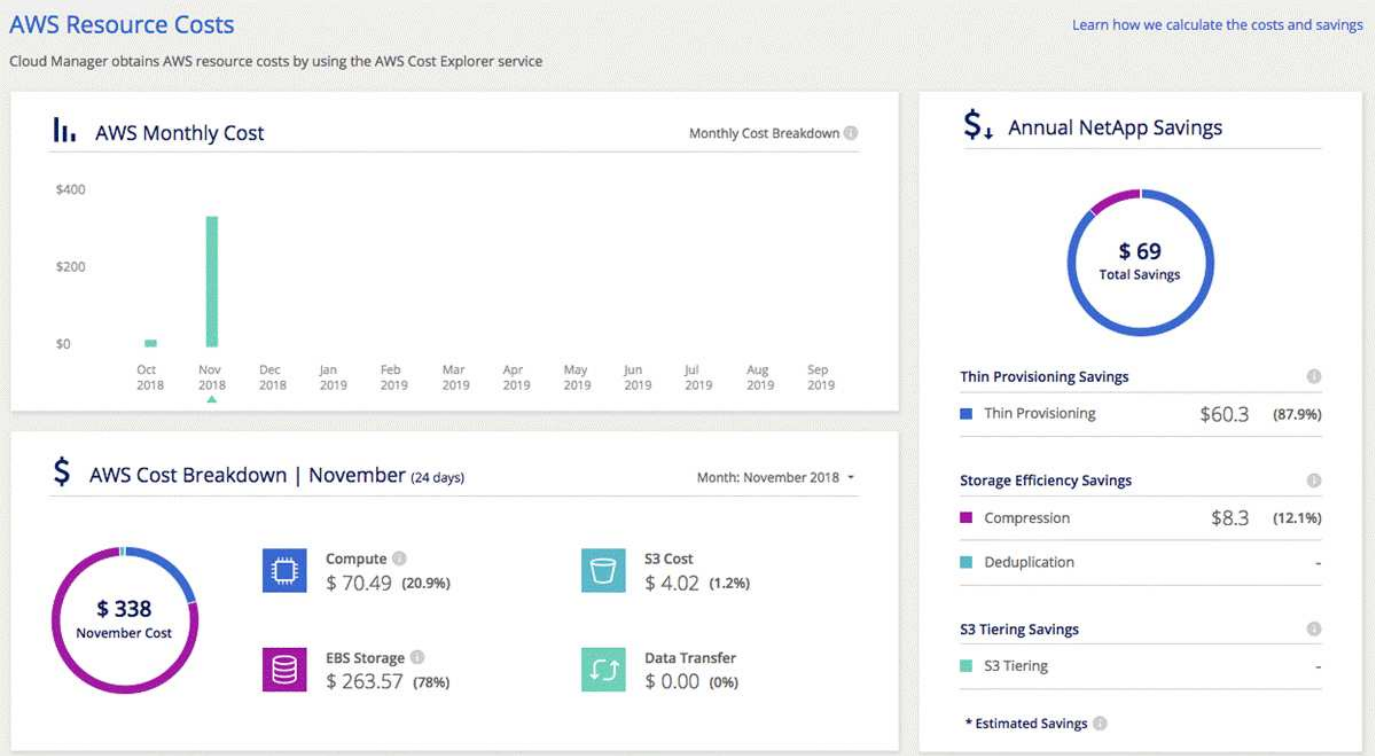
이제 AWS 비용 보고서에 더 많은 정보가 제공되며 설정이 더 쉽습니다.

- 이 보고서에서는 AWS에서 Cloud Volumes ONTAP를 실행하는 것과 관련된 월간 리소스 비용을 줄일 수 있습니다. 컴퓨팅, EBS 스토리지(EBS 스냅샷 포함), S3 스토리지 및 데이터 전송에 대한 월별 비용을 확인할 수 있습니다.
- 비활성 데이터를 S3로 계층화할 때 보고서에 비용 절감이 표시됩니다.
- 또한, Cloud Manager가 AWS에서 비용 데이터를 가져오는 방법도 단순화했습니다.

  Cloud Manager에서는 S3 버킷에 저장된 청구 보고서에 더 이상 액세스할 필요가 없습니다. 대신 Cloud Manager에서는 Cost Explorer API를 사용합니다. Cloud Manager에 권한을 제공하는 IAM 정책에는 다음 작업이 포함되는지 확인해야 합니다.

```
"ce:GetReservationUtilization",
"ce:GetDimensionValues",
"ce:GetCostAndUsage",
"ce:GetTags"
```

  이러한 작업은 최신 에 포함되어 있습니다 "NetApp 제공 정책". NetApp Cloud Central에서 구축한 새 시스템에 이러한 사용 권한이 자동으로 포함됩니다.



새로운 **Azure** 지역 지원

이제 프랑스 중부 지역에 Cloud Manager 및 Cloud Volumes ONTAP를 구축할 수 있습니다.

Cloud Manager 3.6(2018년 11월 4일)

Cloud Manager 3.6에는 새로운 기능이 포함되어 있습니다.

Kubernetes 클러스터의 영구 스토리지로 Cloud Volumes ONTAP 사용

Cloud Manager는 이제 구축을 자동화할 수 있습니다 "NetApp 트라이던트" 단일 Kubernetes 클러스터에서 Cloud Volumes ONTAP를 컨테이너용 영구 스토리지로 사용할 수 있습니다. 그런 다음, 사용자는 네이티브 Kubernetes 인터페이스 및 구조를 사용하여 영구 볼륨을 요청 및 관리하는 동시에 ONTAP의 고급 데이터 관리 기능을 활용할 수 있습니다.

"Cloud Volumes ONTAP 시스템을 Kubernetes 클러스터에 연결하는 방법에 대해 알아보십시오"

알려진 문제

알려진 문제점은 이 제품 릴리스를 성공적으로 사용하지 못하게 만들 수 있는 문제를 식별합니다.

이번 Cloud Manager 릴리즈에는 알려진 문제가 없습니다.

에서 Cloud Volumes ONTAP에 대해 알려진 문제를 찾을 수 있습니다 "Cloud Volumes ONTAP 릴리즈 노트" 및 ONTAP 소프트웨어의 일반 "ONTAP 릴리즈 노트".

알려진 제한 사항

알려진 제한 사항은 이 제품 릴리스에서 지원하지 않거나 올바르게 상호 운용되지 않는 플랫폼,

장치 또는 기능을 식별합니다. 이러한 제한 사항을 주의 깊게 검토하십시오.

Cloud Manager는 **FlexGroup** 볼륨을 지원하지 않습니다

Cloud Volumes ONTAP는 FlexGroup 볼륨을 지원하지만 Cloud Manager는 지원하지 않습니다. System Manager 또는 CLI에서 FlexGroup 볼륨을 생성하는 경우 Cloud Manager의 용량 관리 모드를 수동으로 설정해야 합니다. FlexGroup 볼륨에서 자동 모드가 제대로 작동하지 않을 수 있습니다.

새로 설치된 **Cloud Manager**에서는 **Active Directory**가 기본적으로 지원되지 않습니다

버전 3.4부터 새로 설치된 Cloud Manager는 사용자 관리를 위한 조직의 Active Directory 인증 사용을 지원하지 않습니다. 필요한 경우 NetApp을 통해 Cloud Manager로 Active Directory를 설정할 수 있습니다. Cloud Manager의 오른쪽 아래에 있는 채팅 아이콘을 클릭하여 지원을 받으십시오.

AWS GovCloud(US) 지역 제한사항

- AWS GovCloud(US) 지역에서 Cloud Volumes ONTAP 인스턴스를 실행하려면 Cloud Manager를 AWS GovCloud(US) 지역에 구축해야 합니다.
- AWS GovCloud(US) 지역에 구축한 경우 Cloud Manager는 Microsoft Azure용 NetApp 프라이빗 스토리지 구성 또는 SoftLayer 구성을 위한 NetApp 프라이빗 스토리지에서 ONTAP 클러스터를 검색할 수 없습니다.

볼륨 보기 제한 사항

- 볼륨 뷰는 AWS GovCloud(US) 지역, AWS 상용 클라우드 서비스 환경 및 Microsoft Azure에서 지원되지 않습니다.
- 볼륨 보기를 사용하면 NFS 볼륨만 생성할 수 있습니다.
- Cloud Manager는 볼륨 뷰에서 Cloud Volumes ONTAP BYOL 인스턴스를 시작하지 않습니다.

Cloud Manager는 **iSCSI** 볼륨을 설정하지 않습니다

Storage System View를 사용하여 Cloud Manager에서 볼륨을 생성할 때 NFS 또는 CIFS 프로토콜을 선택할 수 있습니다. OnCommand 시스템 관리자를 사용하여 iSCSI용 볼륨을 생성해야 합니다.

SVM(Storage Virtual Machine) 제한

Cloud Volumes ONTAP는 재해 복구에 사용되는 1개 이상의 SVM과 1개 이상의 SVM을 지원합니다.

Cloud Manager는 SVM 재해 복구에 대한 설정 또는 오케스트레이션 지원을 제공하지 않습니다. 또한 추가 SVM에서 스토리지 관련 작업도 지원하지 않습니다. SVM 재해 복구에 System Manager 또는 CLI를 사용해야 합니다.

개념

Cloud Manager 및 Cloud Volumes ONTAP 개요

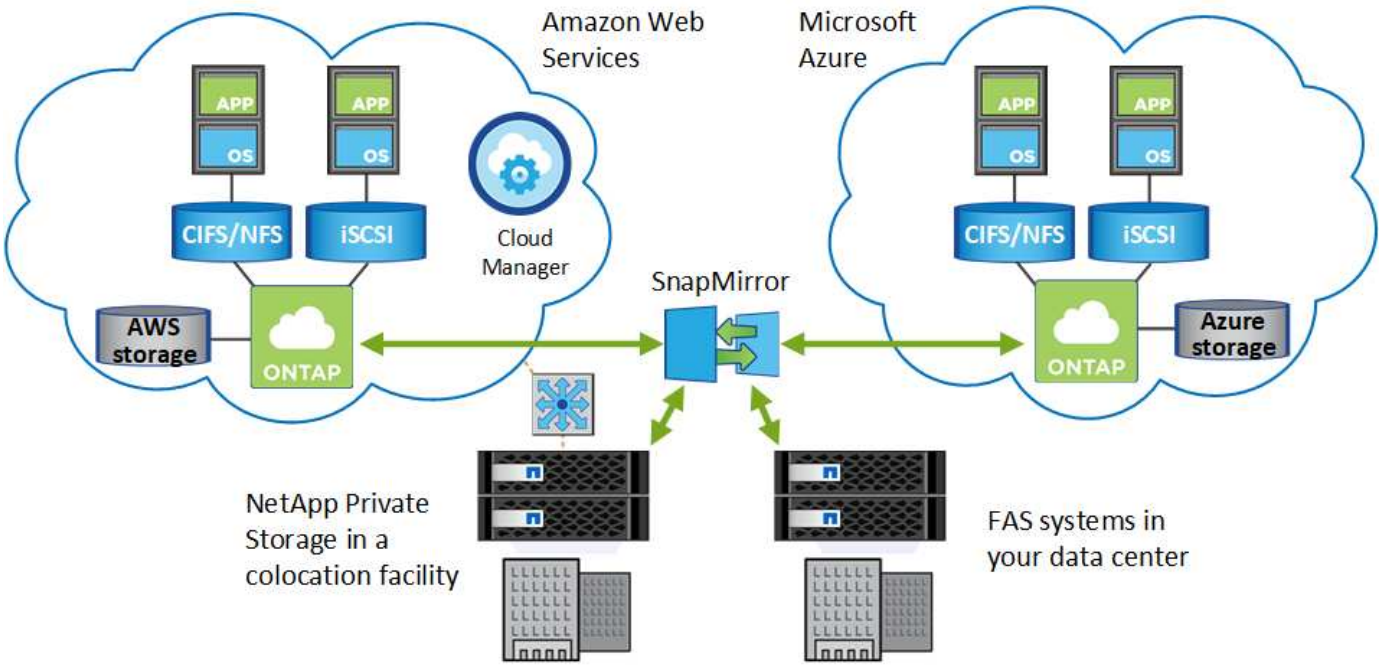
OnCommand Cloud Manager를 사용하면 Cloud Volumes ONTAP를 구축하여 클라우드 스토리지에 엔터프라이즈급 기능을 제공하고 NetApp 기반의 하이브리드 클라우드 전체에서 데이터를 쉽게 복제할 수 있습니다.

클라우드 관리자

Cloud Manager는 단순성을 염두에 두고 설계되었습니다. 이 가이드는 몇 단계로 Cloud Volumes ONTAP 설정을 안내하며, 스토리지 프로비저닝을 단순화하고 용량 관리를 자동화하여 데이터 관리를 용이하게 하며, 하이브리드 클라우드 전반에서 끌어서 놓기 데이터 복제를 지원합니다.

Cloud Volumes ONTAP를 구축 및 관리하려면 Cloud Manager가 필요하지만, 사내 ONTAP 클러스터를 위한 스토리지를 검색하고 프로비저닝할 수도 있습니다. 클라우드 및 사내 스토리지 인프라를 중앙에서 제어할 수 있습니다.

클라우드 또는 네트워크에서 Cloud Manager를 실행할 수 있으며, Cloud Volumes ONTAP를 구축하려는 네트워크에 연결만 있으면 됩니다. 다음 그림은 AWS에서 실행되는 Cloud Manager와 AWS 및 Azure에서 Cloud Volumes ONTAP 시스템을 관리하는 모습을 보여줍니다. 또한 하이브리드 클라우드 전반의 데이터 복제도 보여 줍니다.



"Cloud Manager에 대해 자세히 알아보십시오"

Cloud Volumes ONTAP

Cloud Volumes ONTAP은 클라우드에서 ONTAP 데이터 관리 소프트웨어를 실행하는 소프트웨어 전용 스토리지 어플라이언스입니다. Cloud Volumes ONTAP를 운영 워크로드, 재해 복구, DevOps, 파일 공유 및 데이터베이스 관리에 사용할 수 있습니다.

Cloud Volumes ONTAP은 다음과 같은 주요 기능을 통해 엔터프라이즈 스토리지를 클라우드로 확장합니다.

- 스토리지 효율성 기능은 내장된 데이터 중복제거, 데이터 압축, 씬 프로비저닝 및 복제를 활용하여 스토리지 비용을

최소화합니다.

- 고가용성은 클라우드 환경에서 장애가 발생할 경우 엔터프라이즈급 안정성과 지속적인 운영을 보장합니다.
- 데이터 복제 Cloud Volumes ONTAP는 NetApp의 업계 최고 복제 기술인 SnapMirror를 활용하여 사내 데이터를 클라우드로 복제하므로 여러 사용 사례에서 보조 복사본을 쉽게 사용할 수 있습니다.
- 데이터 계층화 애플리케이션을 오프라인으로 전환하지 않고도 필요에 따라 고성능 스토리지 풀과 고성능 스토리지 풀 간에 전환할 수 있습니다.
- 애플리케이션 정합성을 보장하는 NetApp SnapCenter은 NetApp Snapshot 복사본의 일관성을 보장합니다.

Cloud Volumes ONTAP 기능에 대한 라이센스는 NetApp 볼륨 암호화를 제외하고 ONTAP에 포함되어 있습니다.

"지원되는 Cloud Volumes ONTAP 구성을 봅니다"

"Cloud Volumes ONTAP에 대해 자세히 알아보십시오"

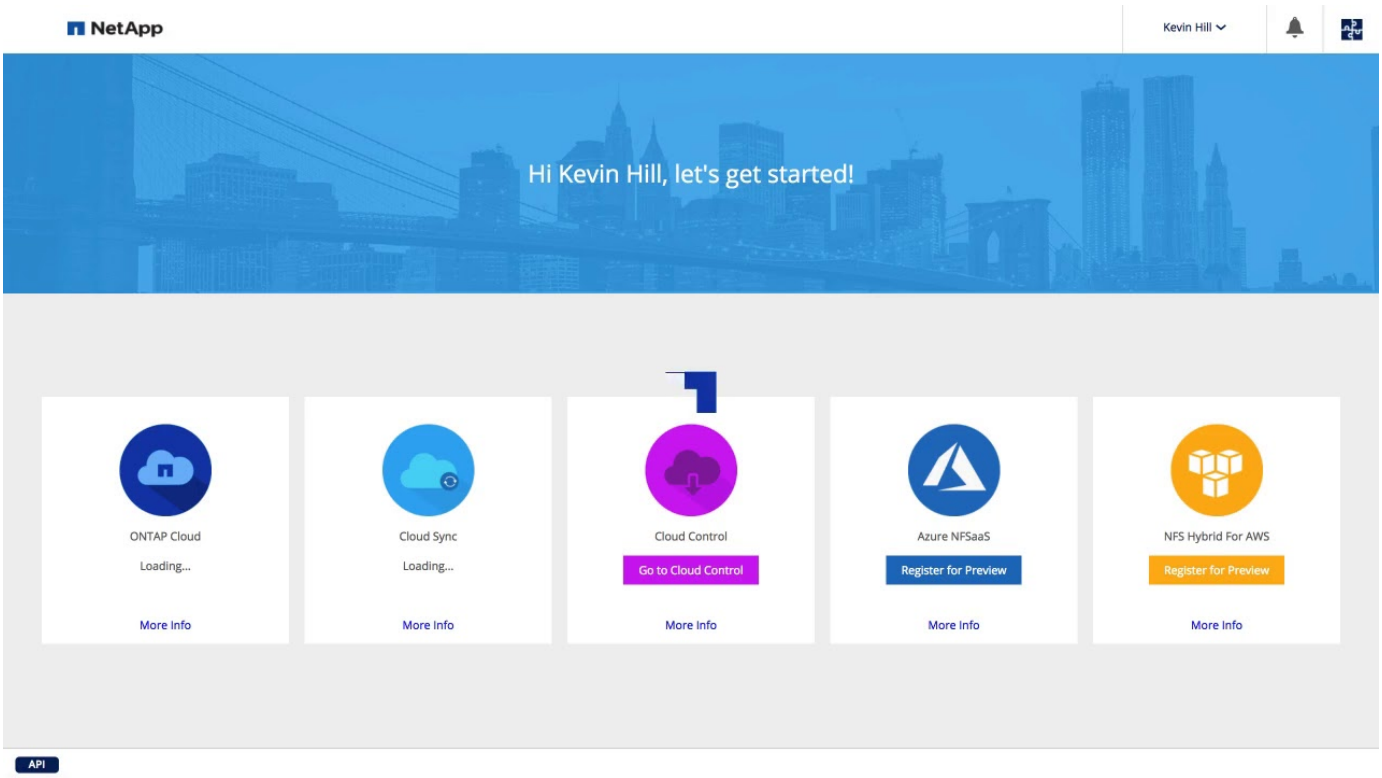
NetApp Cloud Central에서

"NetApp Cloud Central에서" NetApp 클라우드 데이터 서비스에 액세스하고 관리할 수 있는 중앙 위치 제공 이러한 서비스를 사용하여 클라우드에서 중요한 애플리케이션을 실행하고, 자동화된 DR 사이트를 생성하고, SaaS 데이터를 백업하고, 여러 클라우드 간에 데이터를 효과적으로 마이그레이션 및 제어할 수 있습니다.

Cloud Manager와 NetApp Cloud Central의 통합은 간소화된 배포 경험, 여러 Cloud Manager 시스템을 보고 관리할 수 있는 단일 위치, 중앙 집중식 사용자 인증 등 여러 가지 이점을 제공합니다.

중앙 집중식 사용자 인증을 통해 Cloud Manager 시스템과 Cloud Manager와 Cloud Sync 같은 다른 데이터 서비스 간에 동일한 자격 증명 세트를 사용할 수 있습니다. 또한 암호를 잊은 경우에도 암호를 쉽게 재설정할 수 있습니다.

다음 비디오에서 NetApp Cloud Central에 대해 알아보십시오.



클라우드 공급자 계정 및 권한

Cloud Manager를 사용하면 Cloud Volumes ONTAP 시스템을 구축할 _ 클라우드 공급자 계정 _ 을(를) 선택할 수 있습니다. Cloud Manager에 계정을 추가하기 전에 권한 요구 사항을 이해해야 합니다.

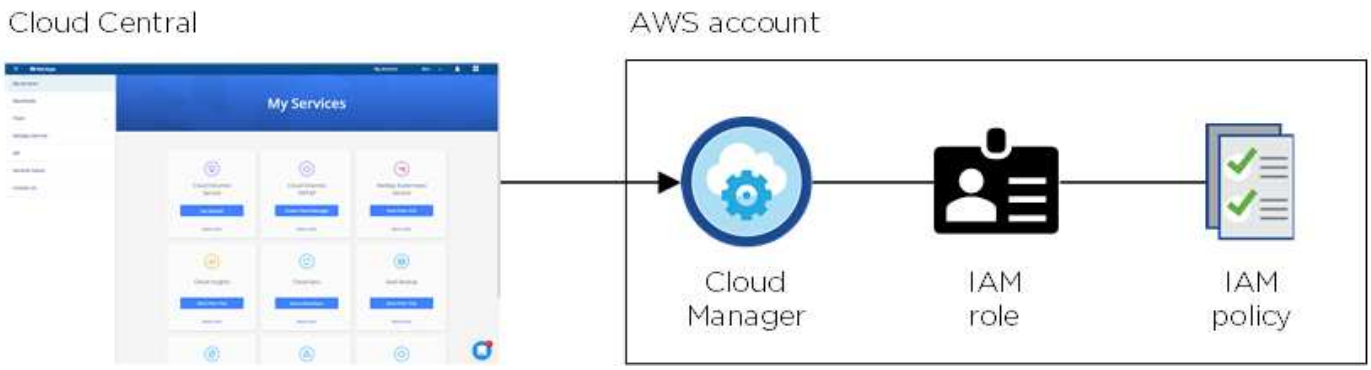
AWS 계정 및 권한

모든 Cloud Volumes ONTAP 시스템을 초기 AWS 계정에 구축하거나 추가 계정을 설정할 수 있습니다.

초기 AWS 계정

NetApp Cloud Central에서 Cloud Manager를 구축할 때 Cloud Manager 인스턴스를 시작할 수 있는 권한이 있는 AWS 계정을 사용해야 합니다. 필요한 권한이 에 나열됩니다 "AWS를 위한 NetApp Cloud Central 정책".

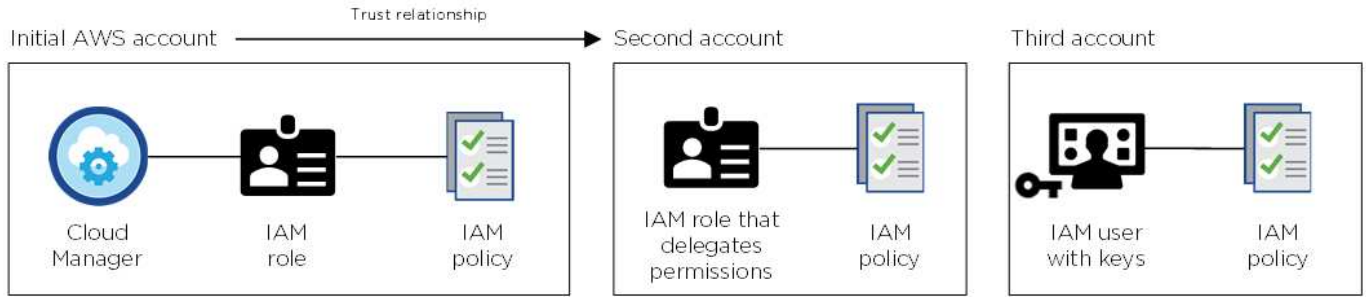
Cloud Central이 AWS에서 Cloud Manager 인스턴스를 시작하면 IAM 역할과 인스턴스에 대한 인스턴스 프로필이 생성됩니다. 또한, Cloud Manager에 해당 AWS 계정에 Cloud Volumes ONTAP를 구축 및 관리할 수 있는 권한을 제공하는 정책을 연결합니다. "Cloud Manager에서 사용 권한을 사용하는 방법을 검토합니다".



새 작업 환경을 생성할 때 Cloud Manager는 기본적으로 이 클라우드 공급자 계정을 선택합니다.

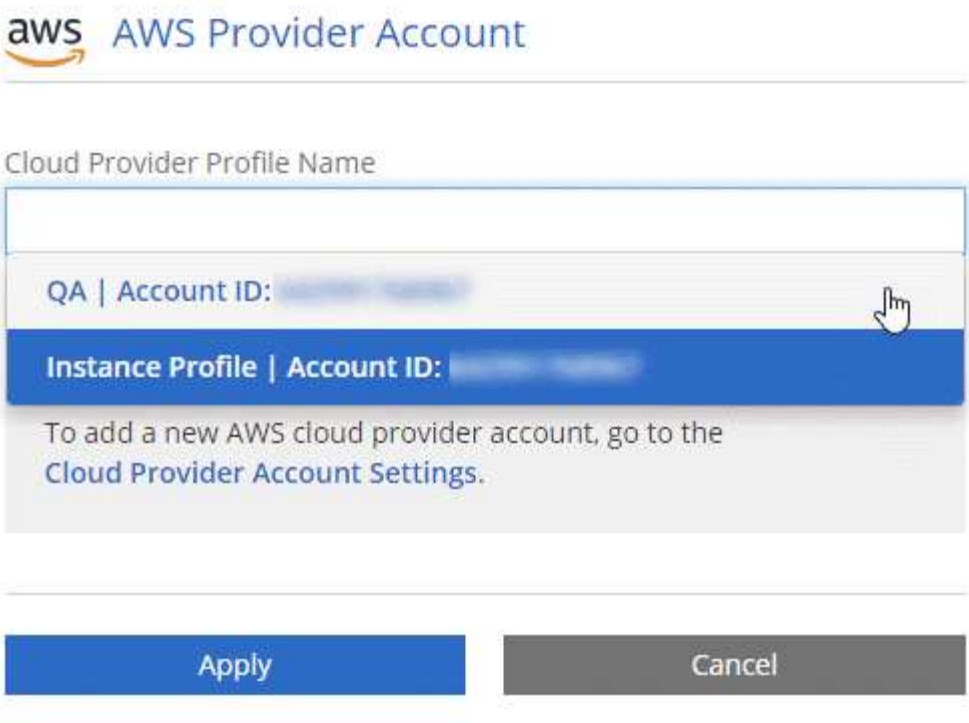
추가 **AWS** 계정

다른 AWS 계정에서 Cloud Volumes ONTAP를 실행하려면 다음 중 하나를 수행합니다 "IAM 사용자 또는 신뢰할 수 있는 계정에서 역할의 ARN에 AWS 키를 제공합니다". 다음 이미지는 두 개의 추가 계정을 보여 줍니다. 하나는 신뢰할 수 있는 계정에서 IAM 역할을 통해 권한을 제공하고 다른 하나는 IAM 사용자의 AWS 키를 통해 권한을 제공합니다.



그러면 됩니다 "Cloud Manager에 클라우드 공급자 계정을 추가합니다" IAM 역할의 ARN(Amazon Resource Name) 또는 IAM 사용자의 AWS 키를 지정합니다.

다른 계정을 추가한 후 새 작업 환경을 만들 때 다른 계정으로 전환할 수 있습니다.



Azure 계정 및 권한

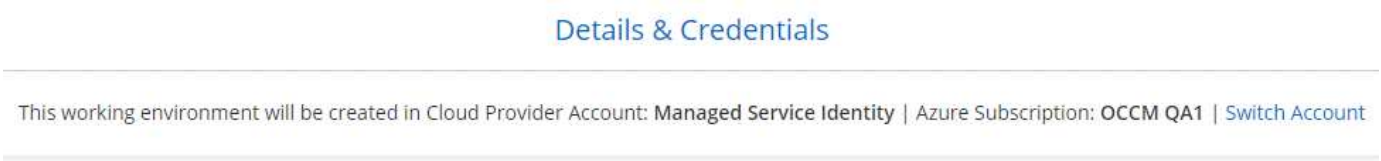
모든 Cloud Volumes ONTAP 시스템을 초기 Azure 계정에 배포하거나 추가 계정을 설정할 수 있습니다.

초기 Azure 계정입니다

NetApp Cloud Central에서 Cloud Manager를 구축할 때 Cloud Manager 가상 머신을 구축할 권한이 있는 Azure 계정을 사용해야 합니다. 필요한 권한이 에 나열됩니다 "Azure를 위한 NetApp Cloud Central 정책".

Cloud Central은 Azure에 Cloud Manager 가상 머신을 구축할 때 가 가능합니다 "시스템에서 할당한 관리 ID입니다" Cloud Manager 가상 머신에서 사용자 지정 역할을 생성하고 가상 머신에 할당합니다. 이 역할은 Cloud Manager에 Azure 구독에서 Cloud Volumes ONTAP를 배포하고 관리할 수 있는 권한을 제공합니다. "Cloud Manager에서 사용 권한을 사용하는 방법을 검토합니다".

새 작업 환경을 생성할 때 Cloud Manager는 기본적으로 이 클라우드 공급자 계정을 선택합니다.

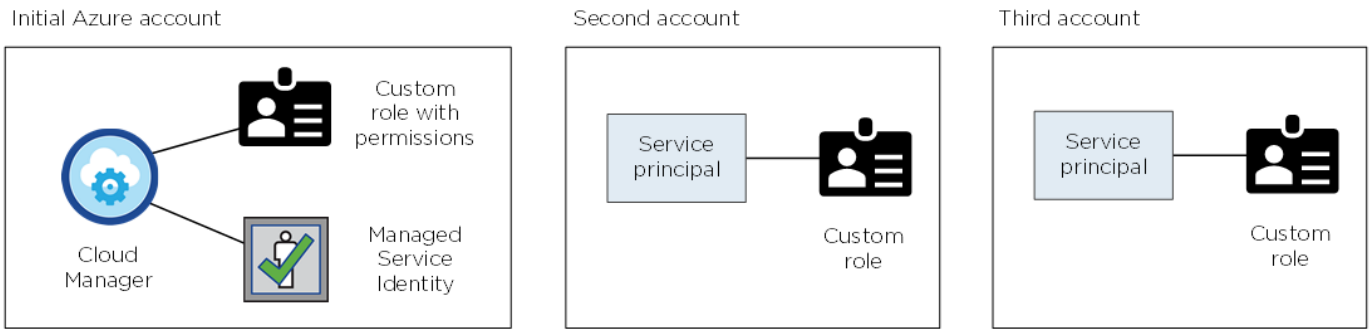


초기 계정에 대한 추가 **Azure** 구독

관리 ID는 Cloud Manager를 시작한 구독과 연결됩니다. 다른 Azure 구독을 선택하려면 를 수행해야 합니다 "관리되는 ID를 해당 구독과 연결합니다".

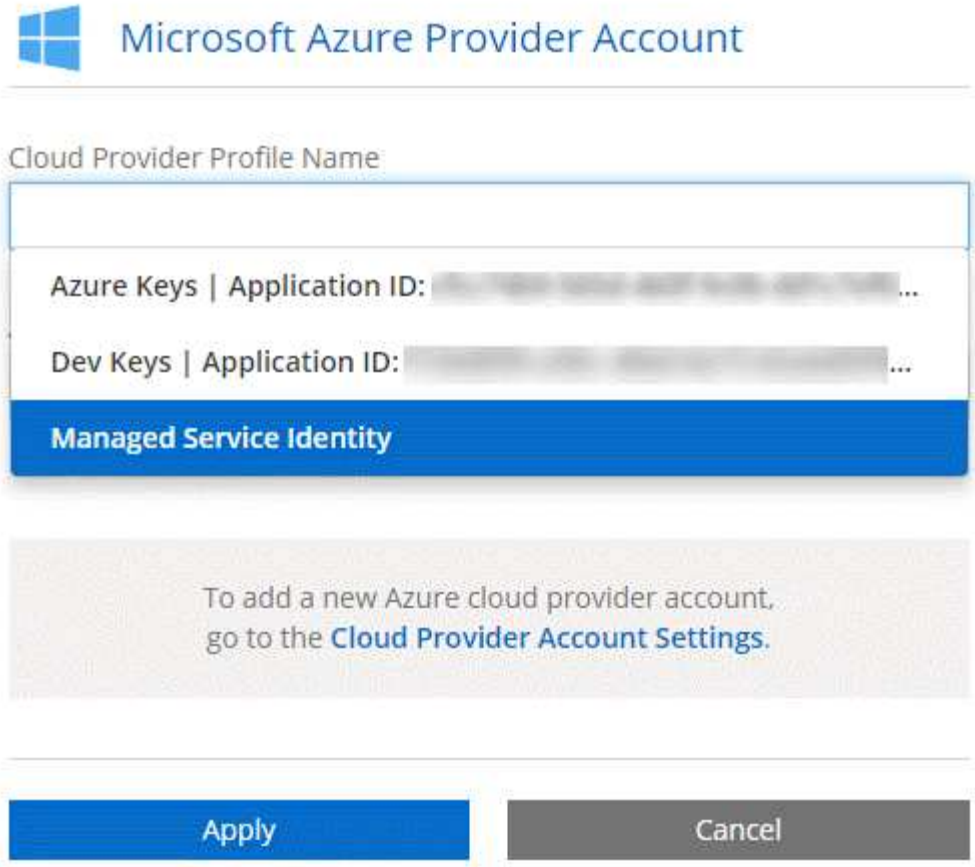
추가 **Azure** 계정

다른 Azure 계정에 Cloud Volumes ONTAP를 배포하려면 에서 필요한 권한을 부여해야 합니다 "Azure Active Directory에서 서비스 보안 주체 만들기 및 설정" 각 Azure 계정에 대해. 다음 그림에서는 두 개의 추가 계정을 보여 줍니다. 각 계정에는 권한을 제공하는 서비스 보안 주체와 사용자 지정 역할이 설정되어 있습니다.



그러면 됩니다 "Cloud Manager에 클라우드 공급자 계정을 추가합니다" AD 서비스 보안 주체에 대한 세부 정보를 제공합니다.

다른 계정을 추가한 후 새 작업 환경을 만들 때 다른 계정으로 전환할 수 있습니다.



Marketplace 구축 및 온프레미스 배포는 어떻습니까?

위 섹션에서는 NetApp Cloud Central에서 권장하는 구축 방법을 설명합니다. 에서 Cloud Manager를 구축할 수도 있습니다 "AWS 마켓플레이스 를 참조하십시오", "Azure 마켓플레이스 를 참조하십시오", 그리고 당신은 할 수 있다 "Cloud Manager를 사내에 설치합니다".

두 마켓플레이스 중 하나를 사용하는 경우 사용 권한이 동일한 방식으로 제공됩니다. Cloud Manager에 대해 IAM 역할 또는 관리 ID를 수동으로 생성 및 설정한 다음 추가 계정에 대한 권한을 제공하면 됩니다.

온-프레미스 배포의 경우 Cloud Manager 시스템에 대해 IAM 역할 또는 관리 ID를 설정할 수 없지만 추가 계정에 대한 것과 같은 권한을 제공할 수 있습니다.

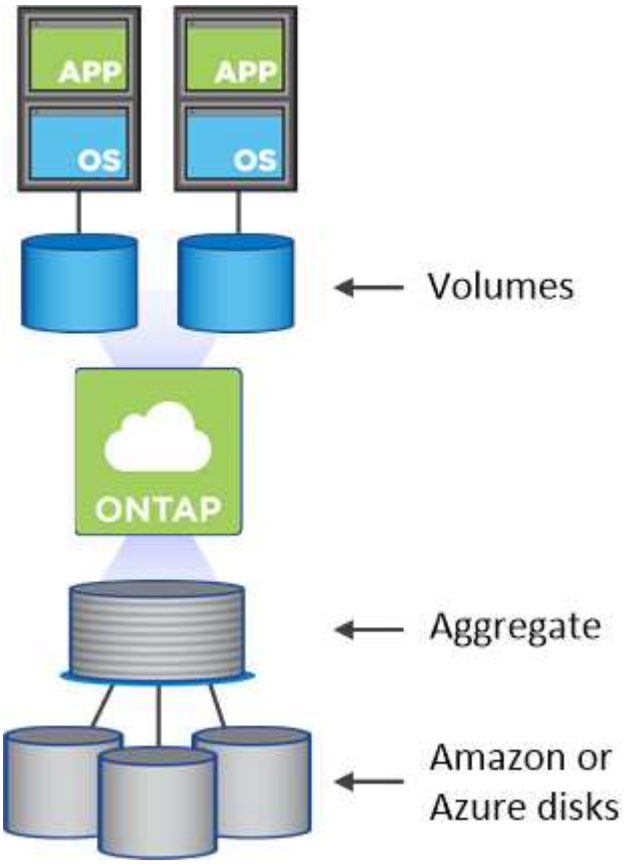
스토리지

Cloud Volumes ONTAP이 클라우드 스토리지를 사용하는 방법

Cloud Volumes ONTAP에서 클라우드 스토리지를 사용하는 방법을 이해하면 스토리지 비용을 이해하는 데 도움이 됩니다.

개요

Cloud Volumes ONTAP는 AWS 및 Azure 볼륨을 백엔드 스토리지로 사용합니다. 볼륨을 디스크로 보고 하나 이상의 애그리게이트로 그룹화합니다. 애그리게이트는 하나 이상의 볼륨에 스토리지를 제공합니다.



여러 유형의 클라우드 디스크가 지원됩니다. Cloud Volumes ONTAP를 배포할 때 볼륨을 생성할 때 디스크 유형을 선택하고 기본 디스크 크기를 선택합니다.

AWS 또는 Azure에서 구입한 총 스토리지 양은 _ 물리적 용량 _ 입니다. 가용 용량은 약 12~14%가 Cloud Volumes ONTAP용으로 예약된 오버헤드이므로 _ 이(가) 적습니다. 예를 들어, Cloud Manager에서 500GB 애그리게이트를 생성할 경우 사용 가능한 용량은 442.94GB입니다.

설치하고

AWS에서는 aggregate에 동일한 크기의 디스크를 최대 6개까지 포함할 수 있습니다. 최대 디스크 크기는 16TB입니다.

기본 EBS 디스크 유형은 범용 SSD, 프로비저닝된 IOPS SSD, 처리량 최적화 HDD 또는 콜드 HDD가 될 수 있습니다. 용 Amazon S3와 EBS 디스크를 페어링할 수도 있습니다 "데이터 계층화".

EBS 디스크 유형의 차이점은 다음과 같습니다.

- _범용 SSD_디스크는 광범위한 워크로드에 맞는 비용과 성능의 균형을 제공합니다. 성능은 IOPS 측면에서 정의됩니다.
- _프로비저닝된 IOPS SSD_디스크는 높은 비용으로 최고의 성능을 요구하는 중요한 애플리케이션을 위한 것입니다.
- _Throughput Optimized HDD_disks는 액세스 빈도가 높은 워크로드에 적합합니다. 이 워크로드는 저렴한 가격으로 빠르고 일관된 처리량을 요구합니다.
- _Cold HDD_디스크는 성능이 매우 낮기 때문에 백업 또는 자주 액세스하지 않는 데이터용으로 사용됩니다. 처리량이 최적화된 HDD 디스크와 마찬가지로 성능은 처리량 측면에서 정의됩니다.

콜드 HDD 디스크는 HA 구성 및 데이터 계층화에서 지원되지 않습니다.

이러한 디스크의 사용 사례에 대한 자세한 내용은 를 참조하십시오 "AWS 설명서:EBS 볼륨 유형".

"AWS에서 시스템의 디스크 유형 및 디스크 크기를 선택하는 방법에 대해 알아보십시오".

"Cloud Volumes ONTAP에 대한 스토리지 제한값을 검토합니다".

Azure 스토리지

Azure에서는 aggregate가 동일한 크기의 디스크를 최대 12개까지 포함할 수 있습니다. 디스크 유형과 최대 디스크 크기는 단일 노드 시스템을 사용하는지 HA 쌍을 사용하는지에 따라 달라집니다.

단일 노드 시스템

단일 노드 시스템에서는 세 가지 유형의 Azure 관리 디스크를 사용할 수 있습니다.

- *Premium SSD* 관리 디스크 높은 비용으로 I/O 집약적인 작업 부하에 높은 성능을 제공합니다.
- _Standard SSD Managed Disks_는 낮은 IOPS가 필요한 워크로드에 일관된 성능을 제공합니다.
- _표준 HDD 관리 디스크 _ 는 높은 IOPS가 필요하지 않고 비용을 절감하려는 경우에 적합합니다.

관리되는 각 디스크 유형의 최대 디스크 크기는 32TB입니다.

에 Azure Blob 저장소와 관리 디스크를 페어링할 수 있습니다 "데이터 계층화".

HA 쌍

HA 쌍에서는 최대 디스크 크기가 8TB인 프리미엄 페이지 Blob을 사용합니다.

이러한 디스크의 사용 사례에 대한 자세한 내용은 를 참조하십시오 "Microsoft Azure 설명서: Microsoft Azure 스토리지 소개".

"Azure에서 시스템의 디스크 유형 및 디스크 크기를 선택하는 방법에 대해 알아보십시오".

"Cloud Volumes ONTAP에 대한 스토리지 제한값을 검토합니다".

데이터 계층화 개요

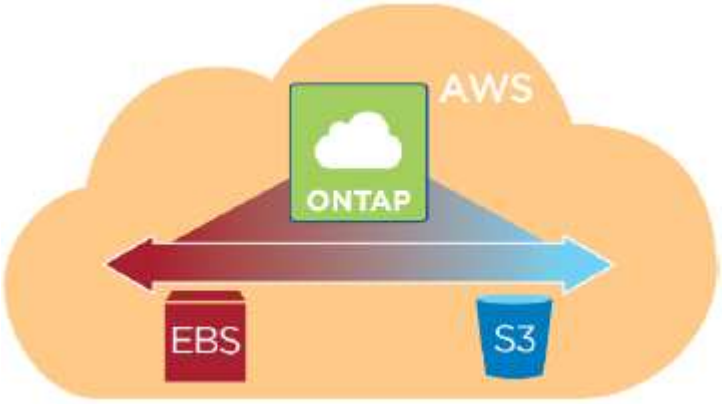
비활성 데이터를 저비용 오브젝트 스토리지로 자동 계층화하여 스토리지 비용을 절감할 수 있습니다. 활성 데이터는 고성능 SSD 또는 HDD(성능 계층)에 유지되고 비활성 데이터는 저비용 오브젝트 스토리지(용량 계층)로 계층화합니다. 따라서 운영 스토리지의 공간을 재확보하고 2차 스토리지를 축소할 수 있습니다.

Cloud Volumes ONTAP는 AWS 및 Microsoft Azure에서 데이터 계층화를 지원합니다. 데이터 계층화는 FabricPool 기술을 기반으로 합니다.

데이터 계층화를 사용하기 위해 기능 라이센스를 설치할 필요는 없습니다.

AWS에서 데이터 계층화의 작동 원리

AWS에서 데이터 계층화를 활성화하면 Cloud Volumes ONTAP은 EBS를 핫 데이터의 성능 계층으로, AWS S3를 비활성 데이터의 용량 계층으로 사용합니다.



AWS의 성능 계층

성능 계층은 범용 SSD, 프로비저닝된 IOPS SSD 또는 처리량 최적화 HDD가 될 수 있습니다.

AWS의 용량 계층

기본적으로 Cloud Volumes ONTAP는 비활성 데이터를 S3_Standard_Storage 클래스에 계층화합니다. 표준은 여러 가용성 영역에 걸쳐 자주 액세스하는 데이터에 적합합니다.

비활성 데이터에 액세스할 계획이 없는 경우 Cloud Volumes ONTAP를 구축한 후 시스템의 계층화 수준을 다음 중 하나로 변경하여 스토리지 비용을 절감할 수 있습니다.

지능형 계층화
: 데이터 액세스 패턴이 변경될 경우 두 계층 간에 데이터를 이동하여 스토리지 비용을 최적화합니다. 한 계층은 잦은 액세스를 위한 반면 다른 계층은 낮은 액세스 빈도로 사용됩니다.

단일 영역 - 낮은 액세스 빈도
: 자주 액세스하지 않는 데이터는 단일 가용성 영역에 저장됩니다.

표준 - 낮은 액세스 빈도
: 자주 액세스하지 않는 데이터는 여러 가용성 영역에 저장됩니다.

데이터에 액세스하는 경우 액세스 비용이 더 높아지므로 계층화 수준을 변경하기 전에 이 점을 고려해야 합니다. S3 스토리지 클래스에 대한 자세한 내용은 를 참조하십시오 "AWS 문서".

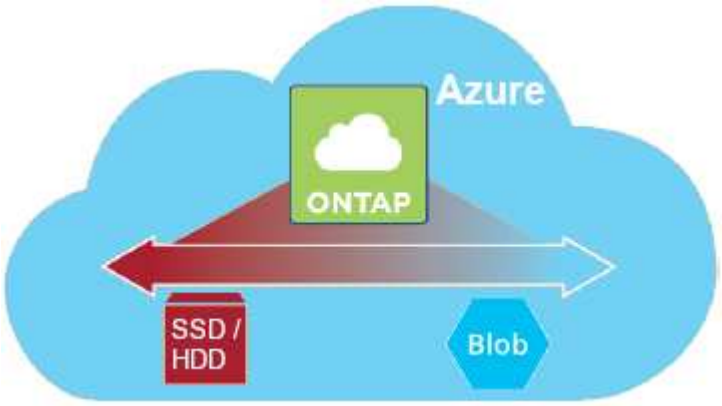
계층화 레벨을 변경하면 비활성 데이터가 표준 스토리지 클래스에서 시작되어 30일 후에 액세스하지 않는 경우 선택한 스토리지 클래스로 이동합니다. 계층화 수준 변경에 대한 자세한 내용은 을 참조하십시오 "비활성 데이터를 저비용 오브젝트 스토리지로 계층화".

계층화 레벨은 시스템 전체에 있으며, 볼륨별로 없습니다.

Cloud Volumes ONTAP 작업 환경에서는 시스템의 모든 계층화된 데이터에 S3 버킷을 사용합니다. 각 볼륨에 다른 S3 버킷이 사용되지 않습니다. 여기에는 HA 작업 환경이 포함됩니다. Cloud Manager에서 S3 버킷을 생성하고 이를 Fabric-pool-_cluster unique identifier_로 지정합니다.

Microsoft Azure에서 데이터 계층화의 작동 원리

Azure에서 데이터 계층화를 활성화하면 Cloud Volumes ONTAP는 Azure 관리 디스크를 핫 데이터용 성능 계층으로 사용하고 Azure Blob 스토리지를 비활성 데이터의 용량 계층으로 사용합니다.



Azure의 성능 계층

성능 계층은 프리미엄 스토리지(SSD) 또는 표준 스토리지(HDD)일 수 있습니다.

Azure의 용량 계층

기본적으로 Cloud Volumes ONTAP는 자주 액세스하는 데이터에 적합한 Azure_hot_storage 계층에 비활성 데이터를 계층화합니다.

비활성 데이터에 액세스할 계획이 없는 경우 Cloud Volumes ONTAP를 배포한 후 시스템의 계층화 수준을 Azure_Cool_storage 계층으로 변경하여 스토리지 비용을 절감할 수 있습니다. 계층 냉각 계층은 계층 내에 최소 30일 동안 자주 액세스하지 않는 데이터에 적합합니다.

데이터에 액세스하는 경우 액세스 비용이 더 높아지므로 계층화 수준을 변경하기 전에 이 점을 고려해야 합니다. Azure Blob 스토리지 계층에 대한 자세한 내용은 를 참조하십시오 "Azure 문서".

계층화 레벨을 변경하면 비활성 데이터가 핫 스토리지 계층에서 시작되어 30일 후에 액세스하지 않는 경우 스토리지 계층으로 이동합니다. 계층화 수준 변경에 대한 자세한 내용은 을 참조하십시오 "비활성 데이터를 저비용 오브젝트 스토리지로 계층화".

계층화 레벨은 시스템 전체에 있으며, 볼륨별로 없습니다.

Cloud Volumes ONTAP 작업 환경에서는 시스템의 모든 계층화된 데이터에 Azure Blob 컨테이너를 사용합니다. 각 볼륨에 다른 컨테이너가 사용되지 않습니다. Cloud Manager에서 각 Cloud Volumes ONTAP 시스템의 컨테이너로 새 스토리지 계정을 생성할 수 있습니다. 스토리지 계정의 이름은 임의로 지정됩니다.

데이터 계층화가 용량 제한에 미치는 영향

데이터 계층화를 사용하는 경우 시스템의 용량 제한은 동일하게 유지됩니다. 이 제한은 성능 계층과 용량 계층 전체에 분산됩니다.

볼륨 계층화 정책

데이터 계층화를 사용하려면 볼륨을 생성, 수정 또는 복제할 때 볼륨 계층화 정책을 선택해야 합니다. 각 볼륨에 대해 다른 정책을 선택할 수 있습니다.

일부 계층화 정책에는 연결된 최소 냉각 기간이 있습니다. 이 기간은 볼륨의 사용자 데이터가 "콜드"로 간주되어 용량 계층으로 이동되기 위해 비활성 상태로 유지되어야 하는 시간을 설정합니다.

Cloud Volumes ONTAP는 다음과 같은 계층화 정책을 지원합니다.

스냅샷만

Aggregate가 50% 용량에 도달하면 Cloud Volumes ONTAP는 활성 파일 시스템과 연결되지 않은 스냅샷 복사본의 콜드 사용자 데이터를 용량 계층으로 이동합니다. 냉각 기간은 약 2일입니다.

읽으면 용량 계층의 콜드 데이터 블록이 핫 상태가 되고 성능 계층으로 이동합니다.

자동

Aggregate가 50% 용량에 도달하면 Cloud Volumes ONTAP는 볼륨의 콜드 데이터 블록을 용량 계층에 계층화합니다. 콜드 데이터에는 스냅샷 복사본뿐만 아니라 액티브 파일 시스템의 콜드 사용자 데이터도 포함됩니다. 냉각 기간은 약 31일입니다.

이 정책은 Cloud Volumes ONTAP 9.4부터 지원됩니다.

랜덤 읽기로 읽는 경우 용량 계층의 콜드 데이터 블록이 핫 상태가 되어 성능 계층으로 이동합니다. 인덱스 및 바이러스 백신 검사와 관련된 읽기 작업을 순차적으로 수행할 경우 콜드 데이터 블록이 콜드 상태를 유지하고 성능 계층으로 이동하지 않습니다.

백업

재해 복구 또는 장기 보존을 위해 볼륨을 복제할 경우 대상 볼륨의 데이터는 용량 계층에서 시작됩니다. 대상 볼륨을 활성화하면 데이터가 읽혀지면서 성능 계층으로 서서히 이동합니다.

없음

볼륨의 데이터를 성능 계층에 유지하여 용량 계층으로 이동하지 않도록 합니다.

데이터 계층화 설정

지원되는 구성의 지침과 목록은 를 참조하십시오 "비활성 데이터를 저비용 오브젝트 스토리지로 계층화".

스토리지 관리

Cloud Manager는 Cloud Volumes ONTAP 스토리지를 간편하고 효율적으로 관리합니다.

모든 디스크와 애그리게이트는 Cloud Manager에서 직접 생성 및 삭제해야 합니다. 다른 관리 도구에서 이러한 작업을 수행해서는 안 됩니다. 이렇게 하면 시스템 안정성에 영향을 주고 향후 디스크를 추가할 수 없도록 하며 중복 클라우드 공급자 비용을 생성할 수 있습니다.

스토리지 프로비저닝

Cloud Manager를 사용하면 디스크를 구매하고 애그리게이트를 관리하여 Cloud Volumes ONTAP를 위한 스토리지 프로비저닝을 간편하게 수행할 수 있습니다. 볼륨을 생성하기만 하면 됩니다. 필요한 경우 고급 할당 옵션을 사용하여 애그리게이트를 직접 프로비저닝할 수 있습니다.

간소화된 프로비저닝

애그리게이트는 볼륨에 클라우드 스토리지를 제공합니다. 인스턴스를 시작할 때와 추가 볼륨을 프로비저닝할 때 Cloud Manager에서 애그리게이트를 생성합니다.

볼륨을 생성할 때 Cloud Manager는 다음 세 가지 중 하나를 수행합니다.

- 여유 공간이 충분한 기존 애그리게이트에 볼륨을 배치합니다.
- 이 Aggregate에 사용할 디스크를 더 많이 구입하여 기존 Aggregate에 볼륨을 배치합니다.
- 새로운 애그리게이트를 위해 디스크를 구매하고 애그리게이트에 볼륨을 배치했습니다.

Cloud Manager에서는 애그리게이트의 최대 크기, 씬 프로비저닝 활성화 여부 및 애그리게이트의 여유 공간 임계값 등 여러 요소를 확인하여 새 볼륨을 배치할 위치를 결정합니다.

Cloud Manager 관리자는 * 설정 * 페이지에서 여유 공간 임계값을 수정할 수 있습니다.

AWS에서 **Aggregate**를 위한 디스크 크기 선택

Cloud Manager에서 AWS에 Cloud Volumes ONTAP용 새 애그리게이트를 생성할 경우, 시스템 내 애그리게이트 수가 증가함에 따라 애그리게이트의 디스크 크기가 점차적으로 증가합니다. Cloud Manager를 사용하면 AWS에서 허용하는 최대 데이터 디스크 수에 도달하기 전에 시스템의 최대 용량을 활용할 수 있습니다.

예를 들어, Cloud Manager는 Cloud Volumes ONTAP 프리미엄 또는 BYOL 시스템에서 다음의 애그리게이트 디스크 크기를 선택할 수 있습니다.

집계 번호	디스크 크기입니다	최대 애그리게이트 용량입니다
1	500MB	3TB
4	1TB	6TB
6	2TB입니다	12TB

고급 할당 옵션을 사용하여 디스크 크기를 직접 선택할 수 있습니다.

고급 할당

Cloud Manager로 애그리게이트를 관리할 수 있다는 것이 아니라, 자신이 직접 애그리게이트를 관리할 수 있습니다. "고급 할당 * 페이지에서 선택합니다"특정 수의 디스크를 포함하는 새 애그리게이트를 생성하고, 기존 애그리게이트에 디스크를 추가하고, 특정 애그리게이트에서 볼륨을 생성할 수 있습니다.

용량 관리

Cloud Manager 관리자는 Cloud Manager에서 스토리지 용량 결정을 내리거나 Cloud Manager에서 자동으로 용량 요구사항을 관리하는지 여부를 선택할 수 있습니다. 이러한 모드의 작동 방식을 이해하는 데 도움이 될 수 있습니다.

자동 용량 관리

Cloud Manager 관리자가 용량 관리 모드를 자동으로 설정하면 Cloud Manager는 더 많은 용량이 필요할 때 Cloud Volumes ONTAP 인스턴스에 대해 새 디스크를 자동으로 구매하고, 사용되지 않는 디스크 컬렉션(애그리게이트)을 삭제하고, 필요할 때 애그리게이트 간에 볼륨을 이동하며, 디스크 장애를 제거합니다.

다음 예제에서는 이 모드가 작동하는 방식을 보여 줍니다.

- EBS 디스크가 5개 이하인 aggregate가 용량 임계값에 도달하면 Cloud Manager가 자동으로 해당 aggregate에 대한 새 디스크를 구매하여 볼륨을 계속 확장할 수 있습니다.
- 12개의 Azure 디스크가 있는 애그리게이트는 용량 임계값에 도달하면 Cloud Manager가 자동으로 볼륨을 해당 애그리게이트의 볼륨을 가용 용량이 있는 애그리게이트로 이동하거나 새 애그리게이트로 이동합니다.

  Cloud Manager가 볼륨에 대한 새 애그리게이트를 만들 경우, 해당 볼륨의 크기를 수용하는 디스크 크기를 선택합니다.

  이제 원래 aggregate에서 여유 공간을 사용할 수 있습니다. 기존 볼륨 또는 새 볼륨에서 해당 공간을 사용할 수 있습니다. 이 시나리오에서는 공간을 AWS 또는 Azure로 반환할 수 없습니다.

- Aggregate에 12시간 이상 볼륨이 포함되어 있지 않으면 Cloud Manager에서 해당 볼륨을 삭제합니다.

수동 용량 관리

Cloud Manager 관리자가 용량 관리 모드를 수동으로 설정한 경우, 용량 결정을 내려야 할 때 Cloud Manager에 작업 필요 메시지가 표시됩니다. 자동 모드에서 설명한 것과 동일한 예가 수동 모드에 적용되지만 사용자는 이 작업을 수락할 수 있습니다.

테넌트를 사용하여 스토리지 격리

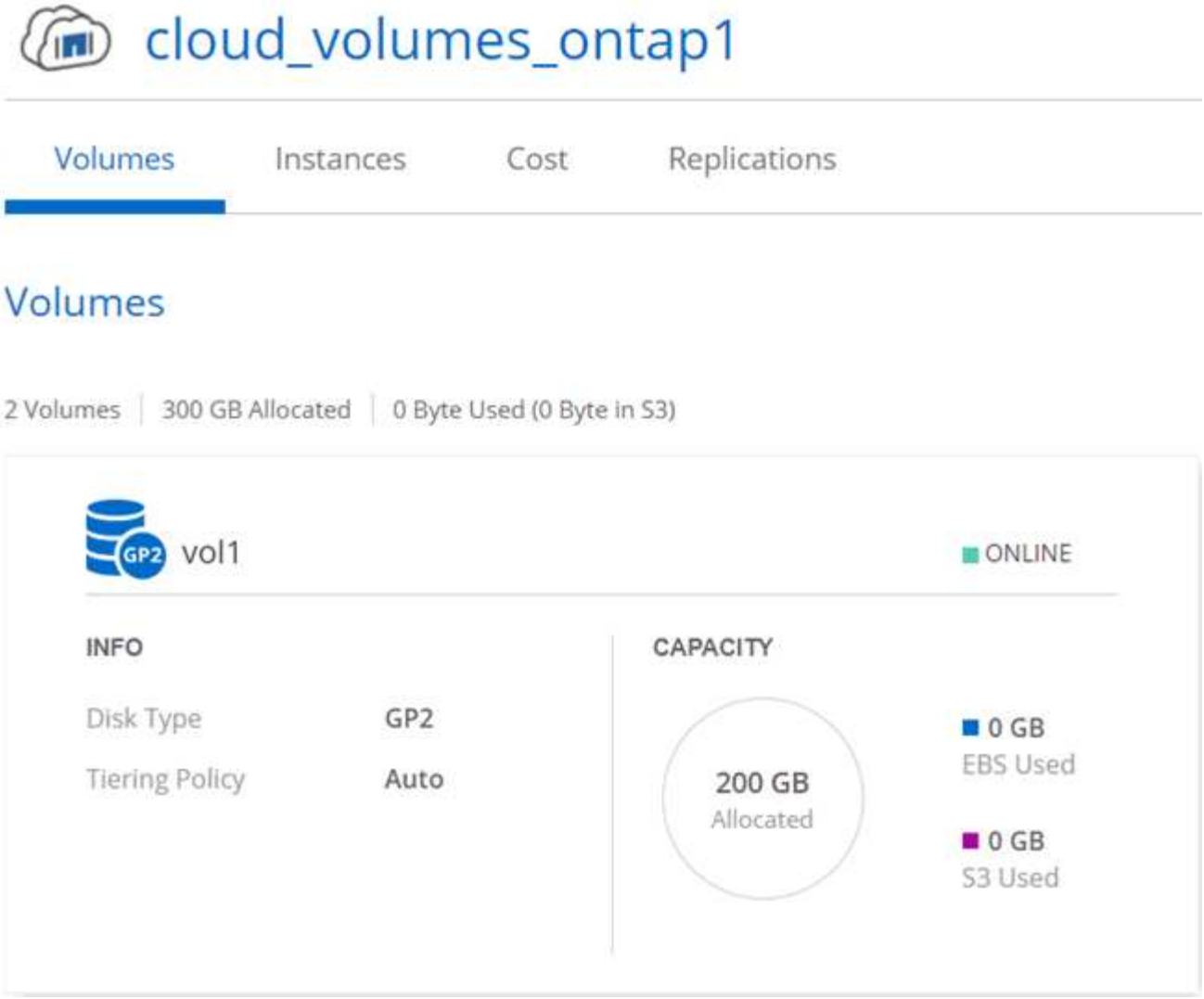
Cloud Manager를 사용하면 테넌트라고 하는 격리된 그룹에서 스토리지를 프로비저닝하고 관리할 수 있습니다. 테넌트 전체에서 Cloud Manager 사용자와 사용자의 작업 환경을 구성하는 방법을 결정해야 합니다.

작업 환경

Cloud Manager는 스토리지 시스템을 _ 작업 환경 _ 으로 나타냅니다. 작업 환경은 다음 중 하나일 수 있습니다.

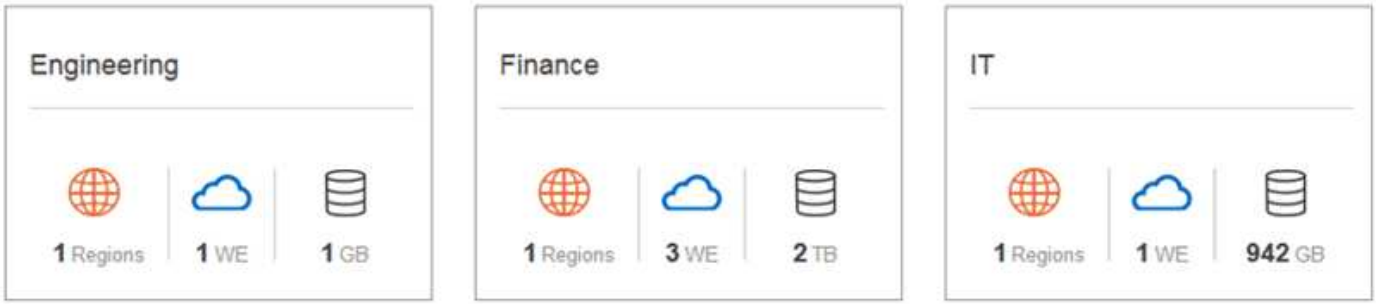
- 단일 Cloud Volumes ONTAP 시스템 또는 HA 쌍
- 네트워크의 온-프레미스 ONTAP 클러스터
- NetApp 프라이빗 스토리지 구성의 ONTAP 클러스터

다음 그림은 Cloud Volumes ONTAP 작업 환경을 보여 줍니다.



테넌트

a_tenant_는 그룹의 작업 환경을 격리합니다. 테넌트 내에서 하나 이상의 작업 환경을 생성합니다. 다음 이미지에는 Cloud Manager에 정의된 세 가지 테넌트가 나와 있습니다.



테넌트 및 작업 환경의 사용자 관리

Cloud Manager 사용자가 관리할 수 있는 테넌트 및 작업 환경은 사용자 역할 및 할당에 따라 달라집니다. 세 가지 사용자 역할은 다음과 같습니다.

Cloud Manager 관리자

제품을 관리하고 모든 테넌트 및 작업 환경에 액세스할 수 있습니다.

테넌트 관리자

단일 테넌트를 관리합니다. 테넌트에서 모든 작업 환경 및 사용자를 생성하고 관리할 수 있습니다.

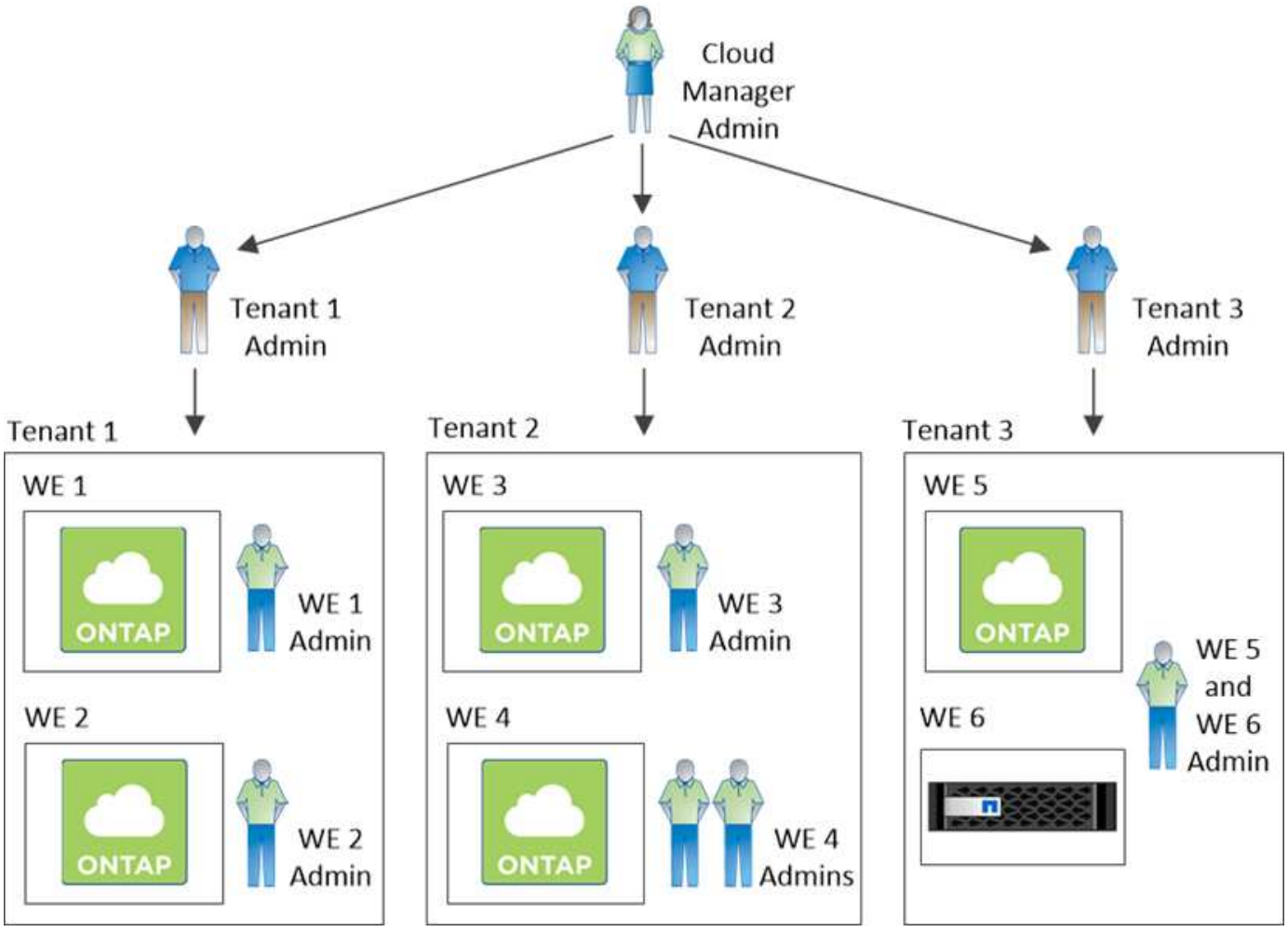
작업 환경 관리자

테넌트에서 하나 이상의 작업 환경을 생성하고 관리할 수 있습니다.

테넌트 및 사용자를 생성하는 방법의 예

조직에 독립적으로 운영되는 부서가 있는 경우 각 부서에 테넌트를 제공하는 것이 좋습니다.

예를 들어, 세 개의 개별 부서에 대해 세 개의 테넌트를 생성할 수 있습니다. 그런 다음 각 테넌트에 대한 테넌트 관리자를 생성합니다. 각 테넌트 내에는 작업 환경을 관리하는 하나 이상의 작업 환경 관리자가 있습니다. 다음 이미지는 이 시나리오를 보여 줍니다.



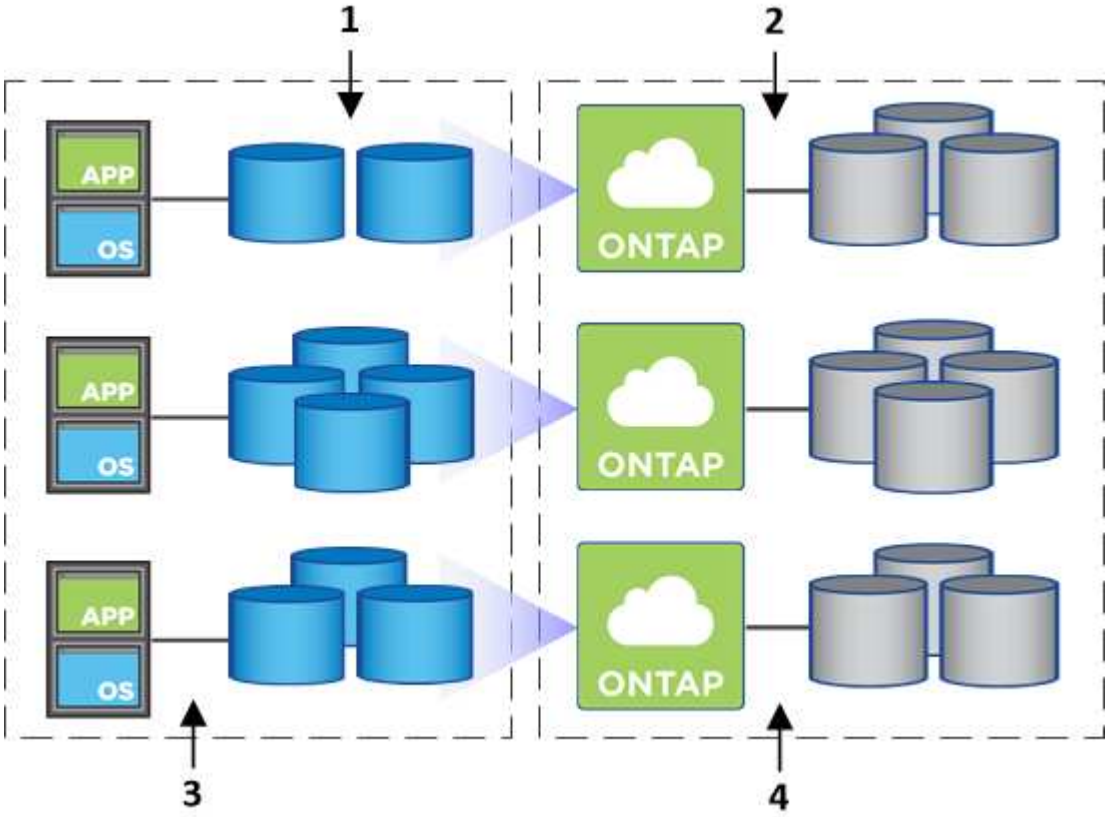
볼륨 보기를 사용하여 스토리지 관리를 간소화했습니다

Cloud Manager에서 제공하는 _Volume View_라는 별도의 관리 뷰를 사용하면 AWS에서 스토리지 관리를 더욱 간소화할 수 있습니다.

볼륨 보기를 사용하면 AWS에 필요한 NFS 볼륨을 지정한 다음, Cloud Manager에서 나머지 볼륨을 처리합니다. 즉,

필요에 따라 Cloud Volumes ONTAP 시스템을 구축하고 볼륨이 커짐에 따라 용량 할당 결정을 내릴 수 있습니다. 이러한 관점의 이점은 스토리지 관리 기능이 거의 없는 클라우드상의 엔터프라이즈급 스토리지의 이점을 제공합니다.

다음 이미지는 볼륨 뷰에서 Cloud Manager와 상호 작용하는 방법을 보여줍니다.

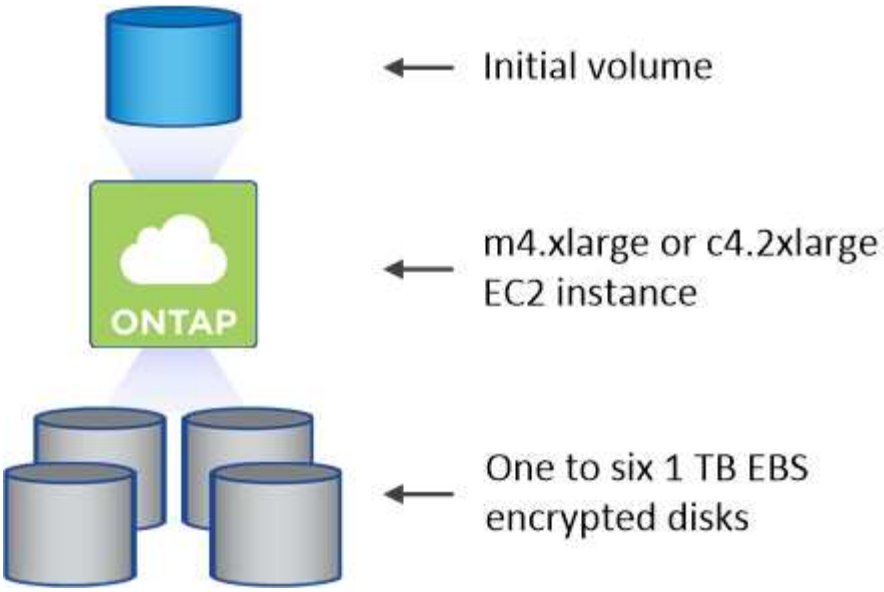


1. NFS 볼륨을 생성합니다.
2. Cloud Manager는 AWS에서 새로운 볼륨에 대한 Cloud Volumes ONTAP 인스턴스를 시작하거나 기존 인스턴스에 볼륨을 생성합니다. 볼륨에 물리적 EBS 스토리지도 구매합니다.
3. 호스트 및 애플리케이션에서 볼륨을 사용할 수 있도록 설정합니다.
4. Cloud Manager는 볼륨이 커짐에 따라 용량 할당 결정을 내립니다.

   즉, 볼륨(왼쪽 이미지)과 상호 작용하기만 하면 Cloud Manager가 스토리지 시스템 및 기본 스토리지(오른쪽 이미지)와 상호 작용합니다.

초기 볼륨에 대한 클라우드 리소스 할당

첫 번째 볼륨을 생성할 때 Cloud Manager가 AWS에서 Cloud Volumes ONTAP 인스턴스 또는 Cloud Volumes ONTAP HA 쌍을 시작하고 해당 볼륨에 대한 Amazon EBS 스토리지를 구매합니다.



초기 볼륨의 크기에 따라 EC2 인스턴스 유형과 EBS 디스크 수가 결정됩니다.

Cloud Manager는 초기 볼륨 크기에 따라 Cloud Volumes ONTAP Explore 또는 Standard 인스턴스를 시작합니다. 볼륨이 증가하면 Cloud Manager에서 AWS 인스턴스를 변경하라는 메시지가 표시될 수 있습니다. 즉, 인스턴스의 라이센스를 Standard 또는 Premium으로 업그레이드해야 합니다. 업그레이드를 하면 EBS 물리적 용량 제한이 증가하므로 볼륨을 늘릴 수 있습니다.

Cloud Manager는 볼륨 뷰에서 Cloud Volumes ONTAP BYOL 인스턴스를 시작하지 않습니다. Cloud Volumes ONTAP 라이센스를 구입한 경우 스토리지 시스템 보기에서 Cloud Manager를 사용해야 합니다.

추가 볼륨에 클라우드 리소스 할당

볼륨을 더 생성할 때 Cloud Manager는 기존 Cloud Volumes ONTAP 인스턴스 또는 새 Cloud Volumes ONTAP 인스턴스에 볼륨을 생성합니다. 인스턴스의 AWS 위치와 디스크 유형이 요청된 볼륨과 일치하고 충분한 공간이 있는 경우 Cloud Manager가 기존 인스턴스에 볼륨을 생성할 수 있습니다.

NetApp 스토리지 효율성 기능 및 스토리지 비용

Cloud Manager를 사용하면 모든 볼륨에서 NetApp 스토리지 효율성 기능을 자동으로 사용할 수 있습니다. 이러한 효율성은 필요한 총 스토리지 양을 줄일 수 있습니다. 할당된 용량과 구입한 AWS 용량 간에 차이가 있을 수 있으므로 스토리지 비용을 절감할 수 있습니다.

Cloud Manager에서 자동으로 처리하는 용량 할당 결정

- Cloud Manager는 용량 임계값이 초과되면 추가 EBS 디스크를 구매합니다. 볼륨이 커짐에 따라 이러한 현상이 발생합니다.
- 디스크에 12시간 동안 볼륨이 없는 경우 Cloud Manager는 사용하지 않는 EBS 디스크 세트를 삭제합니다.
- Cloud Manager는 용량 문제를 방지하기 위해 디스크 세트 간에 볼륨을 이동합니다.

  경우에 따라 추가 EBS 디스크를 구입해야 합니다. 또한 원본 디스크 세트의 공간을 새 볼륨과 기존 볼륨에 사용할 수 있습니다.

WORM 스토리지

Cloud Volumes ONTAP 시스템에서 WORM(Write Once, Read Many) 스토리지를 활성화하여 지정된 보존 기간 동안 수정되지 않은 형식으로 파일을 보존할 수 있습니다. WORM 스토리지는 엔터프라이즈 모드에서 SnapLock 기술을 기반으로 하며, 이는 WORM 파일이 파일 레벨에서 보호됨을 의미합니다.

파일이 WORM 스토리지에 커밋된 후에는 보존 기간이 만료된 후에도 수정할 수 없습니다. 변조 방지 시계는 WORM 파일의 보존 기간이 경과된 시점을 결정합니다.

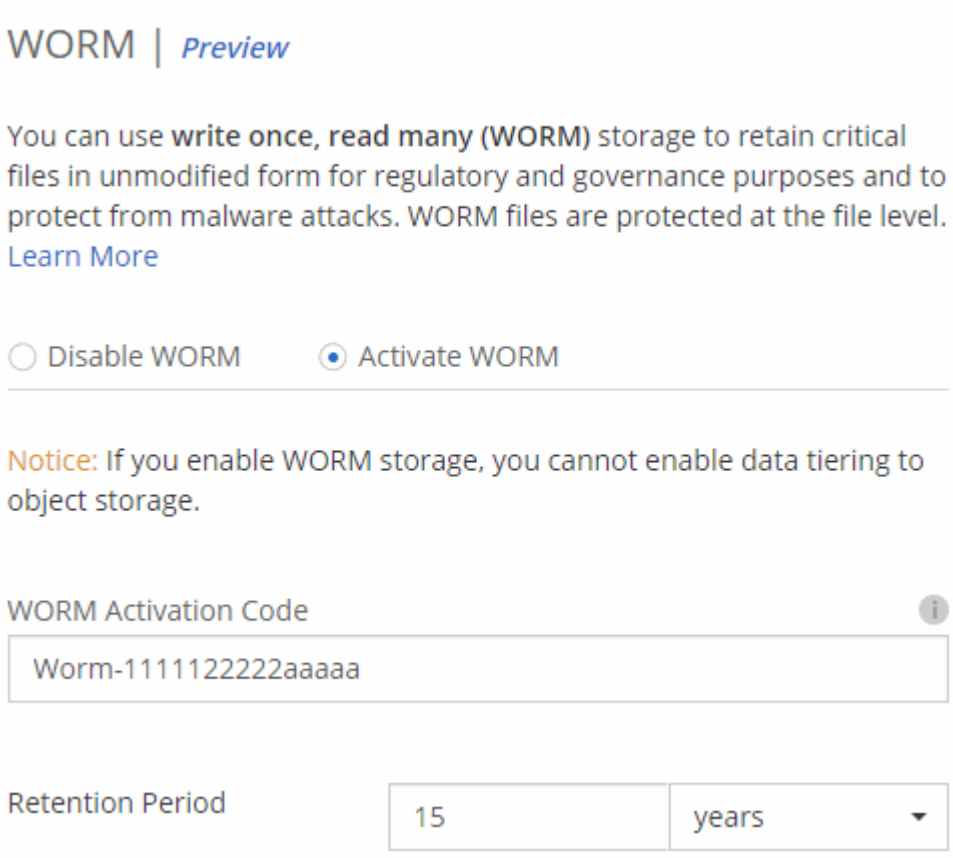
보존 기간이 경과한 후에는 더 이상 필요하지 않은 파일을 삭제해야 합니다.

WORM 스토리지를 활성화하는 중입니다

새로운 작업 환경을 생성할 때 Cloud Volumes ONTAP 시스템에서 WORM 스토리지를 활성화할 수 있습니다. 여기에는 활성화 코드 지정 및 파일의 기본 보존 기간 설정이 포함됩니다. Cloud Manager 인터페이스의 오른쪽 아래에 있는 채팅 아이콘을 사용하여 활성화 코드를 얻을 수 있습니다.

개별 볼륨에서 WORM 스토리지를 활성화할 수 없음 — WORM은 시스템 레벨에서 활성화해야 합니다.

다음 이미지는 작업 환경을 생성할 때 WORM 스토리지를 활성화하는 방법을 보여줍니다.



WORM에 파일 커밋 중

애플리케이션을 사용하여 NFS 또는 CIFS를 통해 WORM에 파일을 커밋하거나 ONTAP CLI를 사용하여 파일을 WORM에 자동으로 커밋할 수 있습니다. 또한 WORM 추가 가능 파일을 사용하여 로그 정보와 같이 점증적으로 기록된

데이터를 보존할 수 있습니다.

Cloud Volumes ONTAP 시스템에서 WORM 스토리지를 활성화한 후에는 모든 WORM 스토리지 관리에 ONTAP CLI를 사용해야 합니다. 자세한 지침은 을 참조하십시오 "ONTAP 설명서".

> WORM 스토리지에 대한 Cloud Volumes ONTAP 지원은 SnapLock 엔터프라이즈 모드와 동일합니다.

제한 사항

- AWS 또는 Azure에서 직접 디스크를 삭제하거나 이동하는 경우, 만료 날짜 전에 볼륨을 삭제할 수 있습니다.
- WORM 스토리지가 활성화된 경우 오브젝트 스토리지에 대한 데이터 계층화를 설정할 수 없습니다.

고가용성 쌍

AWS의 고가용성 쌍

Cloud Volumes ONTAP HA(고가용성) 구성은 무중단 운영 및 내결함성을 제공합니다. AWS에서는 데이터가 두 노드 간에 동기식으로 미러링됩니다.

개요

AWS에서 Cloud Volumes ONTAP HA 구성에는 다음과 같은 구성요소가 포함됩니다.

- 데이터가 서로 동기식으로 미러링되는 2개의 Cloud Volumes ONTAP 노드
- 스토리지 테이크오버 및 반환 프로세스를 지원하는 노드 간 통신 채널을 제공하는 중재자 인스턴스

> 중재자 인스턴스는 T2.micro 인스턴스에서 Linux 운영 체제를 실행하고 약 8GB의 EBS 마그네틱 디스크 하나를 사용합니다.

스토리지 테이크오버 및 반환

노드가 중단되면 다른 노드가 파트너에게 데이터를 제공하여 지속적인 데이터 서비스를 제공할 수 있습니다. 데이터는 파트너에게 동기식으로 미러링되므로 클라이언트가 파트너 노드에서 동일한 데이터에 액세스할 수 있습니다.

노드가 재부팅된 후 파트너가 스토리지를 반환하기 전에 데이터를 다시 동기화해야 합니다. 데이터를 재동기화하는 데 걸리는 시간은 노드가 다운된 동안 변경된 데이터의 양에 따라 달라집니다.

RPO 및 RTO

HA 구성을 사용하면 다음과 같이 데이터의 고가용성을 유지할 수 있습니다.

- 복구 지점 목표(RPO)는 0초입니다. 데이터는 데이터 손실 없이 트랜잭션 측면에서 일관적입니다.
- 복구 시간 목표(RTO)는 60초입니다. 정전이 발생할 경우 60초 이내에 데이터를 사용할 수 있어야 합니다.

HA 구축 모델

여러 AZs(Availability Zone) 또는 단일 AZ에 HA 구성을 배포하여 데이터의 고가용성을 보장할 수 있습니다. 각 구성에

대한 자세한 내용을 검토하여 요구 사항에 가장 적합한 구성을 선택해야 합니다.

여러 가용성 영역의 **Cloud Volumes ONTAP HA**

AZ(Multiple Availability Zones)에 HA 구성을 구축하면 AZ 또는 Cloud Volumes ONTAP 노드를 실행하는 인스턴스에서 장애가 발생할 경우 데이터의 고가용성을 보장할 수 있습니다. NAS IP 주소가 데이터 액세스 및 스토리지 페일오버에 미치는 영향을 이해해야 합니다.

NFS 및 **CIFS** 데이터 액세스

HA 구성이 여러 가용성 영역 간에 분산되면 _floating IP addresses_enable NAS 클라이언트 액세스를 사용합니다. 해당 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 하는 부동 IP 주소는 장애가 발생할 경우 노드 간에 마이그레이션할 수 있습니다. 고객이 아닌 한 VPC 외부에 있는 클라이언트에서 기본적으로 액세스할 수 없습니다 "AWS 전송 게이트웨이를 설정합니다".

전송 게이트웨이를 설정할 수 없는 경우 VPC 외부에 있는 NAS 클라이언트에서 전용 IP 주소를 사용할 수 있습니다. 그러나 이러한 IP 주소는 정적이며 노드 간에 페일오버할 수 없습니다.

여러 가용성 영역에 HA 구성을 배포하기 전에 부동 IP 주소 및 라우팅 테이블에 대한 요구 사항을 검토해야 합니다. 구성을 배포할 때 부동 IP 주소를 지정해야 합니다. 프라이빗 IP 주소는 Cloud Manager에서 자동으로 생성합니다.

자세한 내용은 을 참조하십시오 "여러 AZs에서 Cloud Volumes ONTAP HA를 위한 AWS 네트워킹 요구사항".

iSCSI 데이터 액세스

iSCSI는 부동 IP 주소를 사용하지 않으므로 Cross-VPC 데이터 통신은 문제가 되지 않습니다.

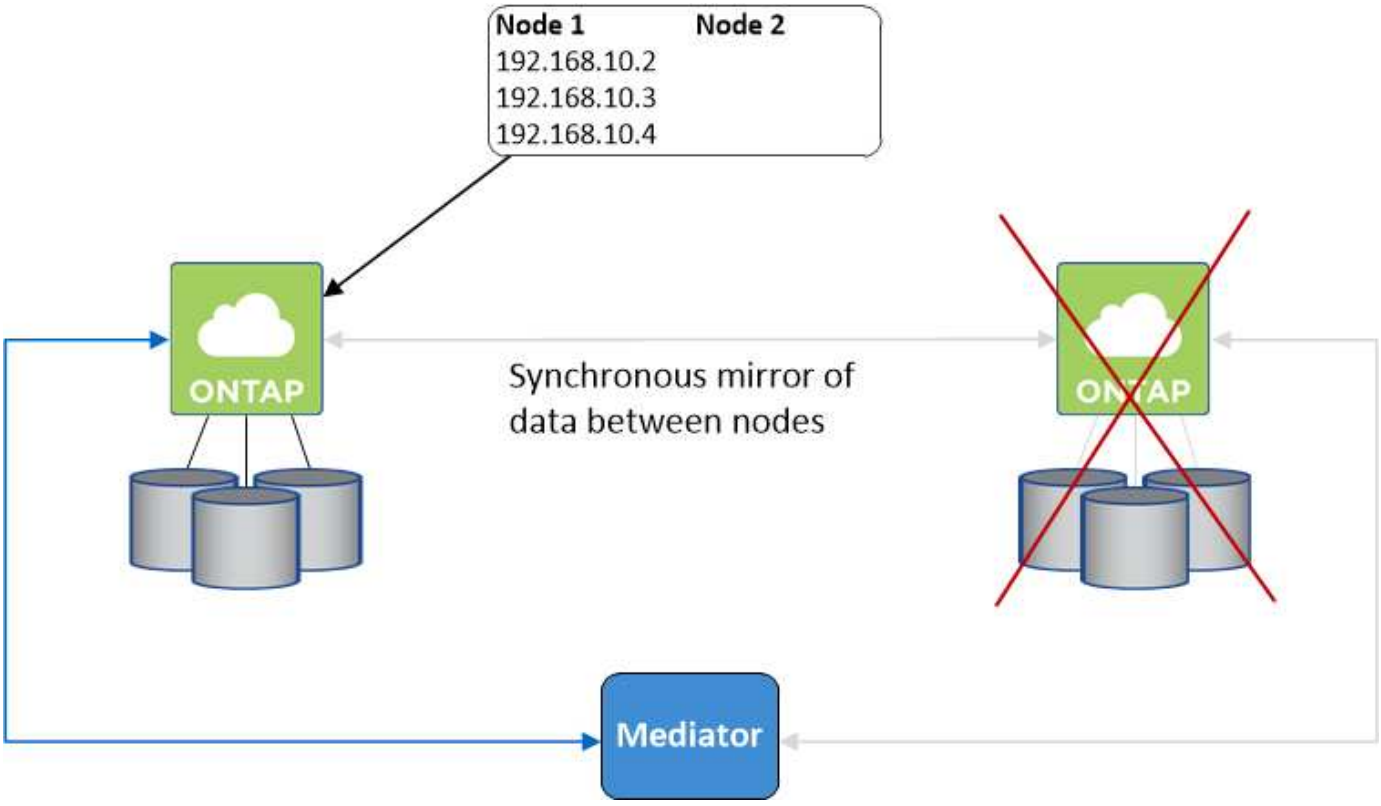
iSCSI의 스토리지 테이크오버 및 반환

iSCSI의 경우 Cloud Volumes ONTAP는 다중 경로 I/O(MPIO) 및 ALUA(Asymmetric Logical Unit Access)를 사용하여 능동 최적화 경로와 최적화되지 않은 경로 간의 경로 페일오버를 관리합니다.

ALUA를 지원하는 특정 호스트 구성에 대한 자세한 내용은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴" 및 호스트 운영 체제용 Host Utilities 설치 및 설정 설명서를 참조하십시오.

NAS의 스토리지 테이크오버 및 반환

유동 IP를 사용하는 NAS 구성에서 테이크오버가 발생하면 클라이언트가 데이터에 액세스하는 데 사용하는 노드의 부동 IP 주소가 다른 노드로 이동합니다. 다음 이미지는 유동 IP를 사용하는 NAS 구성의 스토리지 테이크오버를 보여 줍니다. 노드 2가 다운되면 노드 2의 부동 IP 주소가 노드 1로 이동합니다.



외부 VPC 액세스에 사용되는 NAS 데이터 IP는 장애가 발생할 경우 노드 간에 마이그레이션할 수 없습니다. 노드가 오프라인이 되면 다른 노드의 IP 주소를 사용하여 VPC 외부의 클라이언트에 볼륨을 수동으로 다시 마운트해야 합니다.

장애가 발생한 노드가 다시 온라인 상태가 되면 원래 IP 주소를 사용하여 클라이언트를 볼륨에 다시 마운트합니다. 이 단계는 두 HA 노드 간에 불필요한 데이터를 전송하지 않아야 하므로 성능에 중대한 영향을 미칠 수 있습니다.

볼륨을 선택하고 * 탑재 명령 * 을 클릭하여 Cloud Manager에서 올바른 IP 주소를 쉽게 식별할 수 있습니다.

단일 가용성 영역의 **Cloud Volumes ONTAP HA**

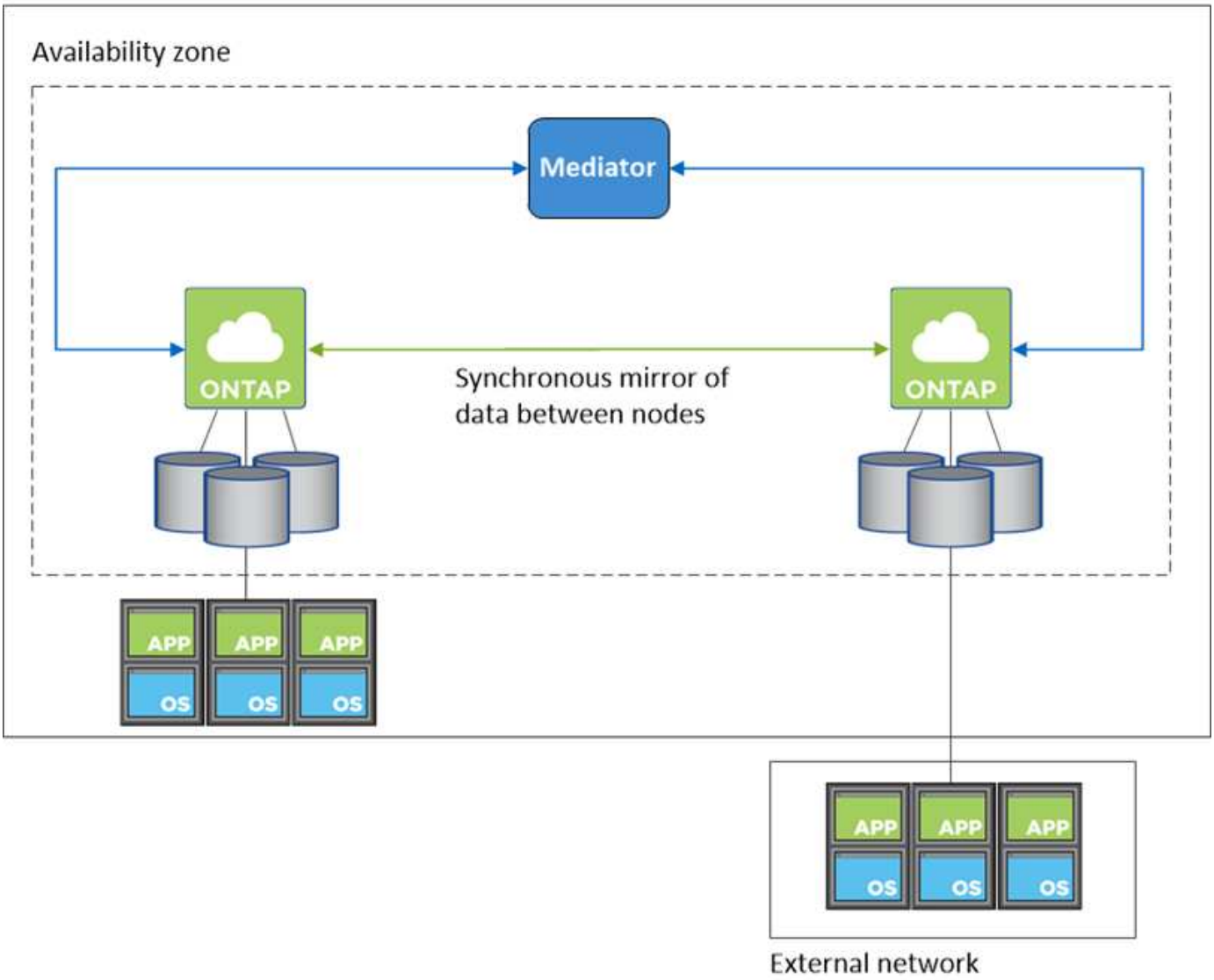
AZ(단일 가용성 영역)에 HA 구성을 구축하면 Cloud Volumes ONTAP 노드를 실행하는 인스턴스에 장애가 발생할 경우 데이터의 고가용성을 보장할 수 있습니다. 모든 데이터는 VPC 외부에서 기본적으로 액세스할 수 있습니다.

Cloud Manager에서 을 생성합니다 "AWS 배치 그룹 분산" 그런 다음 해당 배치 그룹에서 2개의 HA 노드를 시작합니다. 배치 그룹은 서로 다른 기본 하드웨어에 인스턴스를 분산하여 동시 오류 위험을 줄입니다. 이 기능은 디스크 장애 관점이 아니라 컴퓨팅 측면에서 중복성을 향상시킵니다.

데이터 액세스

이 구성은 단일 AZ에 있으므로 부동 IP 주소가 필요하지 않습니다. VPC 내부 및 VPC 외부에서 동일한 IP 주소를 사용하여 데이터에 액세스할 수 있습니다.

다음 이미지는 단일 AZ의 HA 구성을 보여줍니다. VPC 내부 및 VPC 외부에서 데이터에 액세스할 수 있습니다.



스토리지 테이크오버 및 반환

iSCSI의 경우 Cloud Volumes ONTAP는 다중 경로 I/O(MPIO) 및 ALUA(Asymmetric Logical Unit Access)를 사용하여 능동 최적화 경로와 최적화되지 않은 경로 간의 경로 페일오버를 관리합니다.

ALUA를 지원하는 특정 호스트 구성에 대한 자세한 내용은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴" 및 호스트 운영 체제용 Host Utilities 설치 및 설정 설명서를 참조하십시오.

NAS 구성의 경우 장애가 발생할 경우 데이터 IP 주소를 HA 노드 간에 마이그레이션할 수 있습니다. 이렇게 하면 클라이언트가 스토리지에 액세스할 수 있습니다.

HA Pair의 스토리지 작동 방식

ONTAP 클러스터와 달리 Cloud Volumes ONTAP HA 쌍의 스토리지는 노드 간에 공유되지 않습니다. 대신 데이터가 노드 간에 동기식으로 미러링되므로 장애 발생 시 데이터를 사용할 수 있습니다.

스토리지 할당

새 볼륨을 생성하고 추가 디스크가 필요하면 Cloud Manager에서 두 노드에 동일한 수의 디스크를 할당하고 미러링된 애그리게이트를 생성한 다음 새 볼륨을 생성합니다. 예를 들어, 볼륨에 2개의 디스크가 필요한 경우 Cloud Manager는 노드당 총 4개의 디스크에 2개의 디스크를 할당합니다.

구성의 스토리지

HA 쌍을 액티브-액티브 구성으로 사용할 수 있으며, 두 노드에서 클라이언트에 데이터를 제공하거나 액티브-패시브 구성으로 사용할 수 있습니다. 이 구성에서는 패시브 노드가 액티브 노드의 스토리지를 인계받은 경우에만 데이터 요청에 응답합니다.

스토리지 시스템 보기에서 Cloud Manager를 사용하는 경우에만 액티브-액티브 구성을 설정할 수 있습니다.

HA 구성에 대한 성능 기대치

Cloud Volumes ONTAP HA 구성은 노드 간에 데이터를 동기식으로 복제하여 네트워크 대역폭을 사용합니다. 따라서 단일 노드 Cloud Volumes ONTAP 구성과 비교하여 다음과 같은 성능을 기대할 수 있습니다.

- 한 노드의 데이터만 제공하는 HA 구성의 경우 읽기 성능은 단일 노드 구성의 읽기 성능과 비슷하며 쓰기 성능은 낮습니다.
- 두 노드의 데이터를 제공하는 HA 구성의 경우 읽기 성능은 단일 노드 구성의 읽기 성능보다 높고 쓰기 성능은 동일하거나 더 높습니다.

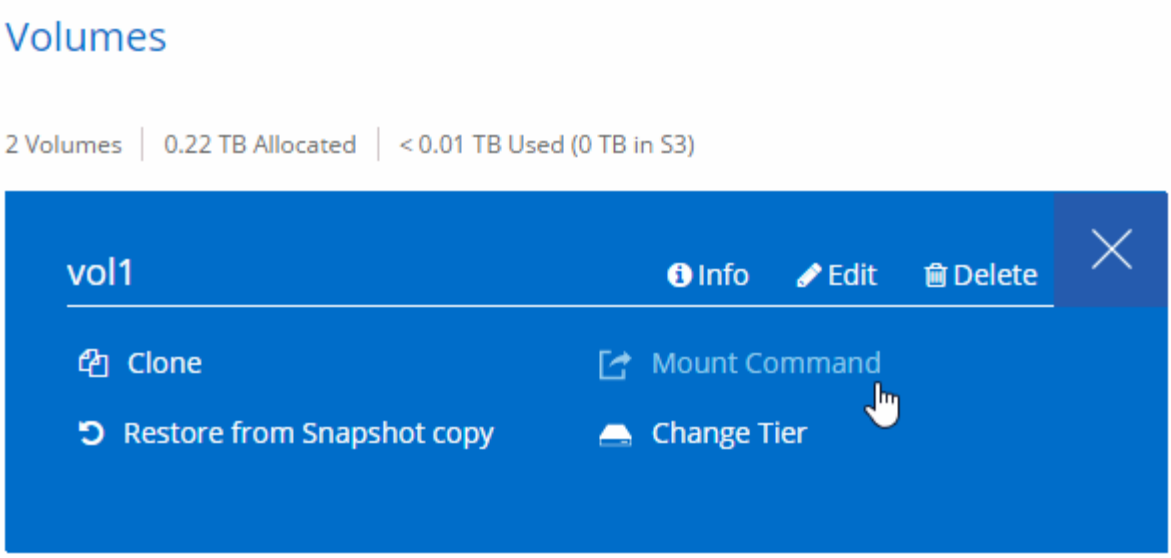
Cloud Volumes ONTAP 성능에 대한 자세한 내용은 를 참조하십시오 "성능".

스토리지에 대한 클라이언트 액세스

클라이언트는 볼륨이 상주하는 노드의 데이터 IP 주소를 사용하여 NFS 및 CIFS 볼륨을 액세스해야 합니다. NAS 클라이언트가 파트너 노드의 IP 주소를 사용하여 볼륨에 액세스하는 경우 트래픽이 두 노드 간에 이동하므로 성능이 저하됩니다.

HA 쌍에서 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 이러한 기능을 설정하여 볼륨을 다시 마운트하지 않도록 할 수 있습니다. 자세한 내용은 ONTAP 설명서를 참조하십시오.

Cloud Manager에서 올바른 IP 주소를 쉽게 식별할 수 있습니다. 다음 이미지는 스토리지 시스템 보기를 보여 줍니다.



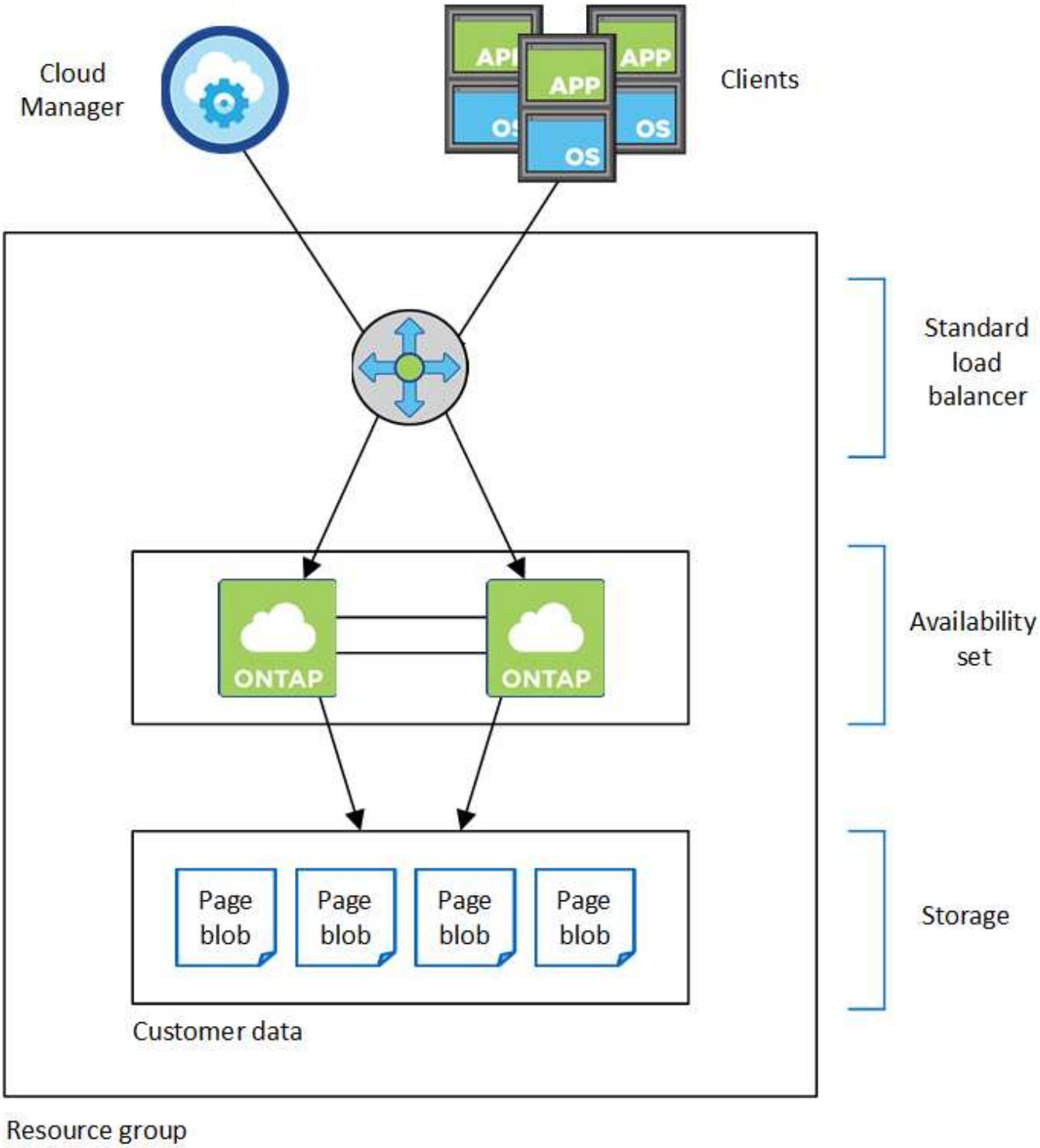
다음 이미지는 볼륨 보기를 보여줍니다.

Azure의 고가용성 쌍

Cloud Volumes ONTAP HA(고가용성) 쌍은 클라우드 환경에서 장애가 발생할 경우 엔터프라이즈급 안정성과 지속적인 운영을 제공합니다. Azure에서 스토리지는 두 노드 간에 공유됩니다.

HA 구성 요소

Azure의 Cloud Volumes ONTAP HA 구성에는 다음과 같은 구성요소가 포함됩니다.



Cloud Manager가 사용자를 위해 배포하는 Azure 구성요소에 대한 다음 정보를 확인하십시오.

Azure 표준 로드 밸런서

로드 밸런서는 Cloud Volumes ONTAP HA 쌍에 대한 들어오는 트래픽을 관리합니다.

가용성 설정

가용성 집합은 노드가 서로 다른 장애 및 업데이트 도메인에 있는지 확인합니다.

스토리지

고객 데이터는 프리미엄 스토리지 페이지 Blob에 있습니다. 각 노드는 다른 노드의 스토리지에 액세스할 수 있습니다. 부팅 및 루트 데이터에는 추가 스토리지가 필요합니다.

- 노드의 부팅 데이터는 프리미엄 SSD 관리 디스크에 있습니다.
- 노드의 루트 데이터는 프리미엄 스토리지 페이지 blob에 상주합니다.

RPO 및 RTO

HA 구성을 사용하면 다음과 같이 데이터의 고가용성을 유지할 수 있습니다.

- 복구 지점 목표(RPO)는 0초입니다. 데이터는 데이터 손실 없이 트랜잭션 측면에서 일관적입니다.
- 복구 시간 목표(RTO)는 60초입니다. 정전이 발생할 경우 60초 이내에 데이터를 사용할 수 있어야 합니다.

스토리지 테이크오버 및 반환

물리적 ONTAP 클러스터와 마찬가지로 Azure HA 쌍의 스토리지가 노드 간에 공유됩니다. 파트너의 스토리지에 연결하면 각 노드가 _Takeover_가 발생한 경우 다른 노드의 스토리지에 액세스할 수 있습니다. 네트워크 경로 페일오버 메커니즘을 통해 클라이언트 및 호스트가 정상 작동하는 노드와 계속 통신할 수 있습니다. 노드가 다시 온라인 상태가 되면 PARTNER_에서 BACK_STORAGE를 제공합니다.

NAS 구성의 경우 장애가 발생할 경우 데이터 IP 주소가 HA 노드 간에 자동으로 마이그레이션됩니다.

iSCSI의 경우 Cloud Volumes ONTAP는 다중 경로 I/O(MPIO) 및 ALUA(Asymmetric Logical Unit Access)를 사용하여 능동 최적화 경로와 최적화되지 않은 경로 간의 경로 페일오버를 관리합니다.

ALUA를 지원하는 특정 호스트 구성에 대한 자세한 내용은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴" 및 호스트 운영 체제용 Host Utilities 설치 및 설정 설명서를 참조하십시오.

구성의 스토리지

HA 쌍을 액티브-액티브 구성으로 사용할 수 있으며, 두 노드에서 클라이언트에 데이터를 제공하거나 액티브-패시브 구성으로 사용할 수 있습니다. 이 구성에서는 패시브 노드가 액티브 노드의 스토리지를 인계받은 경우에만 데이터 요청에 응답합니다.

HA 제한 사항

Azure의 Cloud Volumes ONTAP HA 쌍에는 다음과 같은 제한이 있습니다.

- HA 쌍은 Cloud Volumes ONTAP Standard, Premium 및 BYOL에서 지원됩니다. 탐색이 지원되지 않습니다.
- 데이터 계층화는 지원되지 않습니다.
- NFSv4는 지원되지 않습니다. NFSv3이 지원됩니다.
- 일부 지역에서는 HA 쌍이 지원되지 않습니다.

  "지원되는 Azure 지역 목록을 참조하십시오".

"Azure에서 HA 시스템을 구축하는 방법을 알아보십시오".

평가 중

소프트웨어 비용을 지불하기 전에 Cloud Volumes ONTAP를 평가할 수 있습니다.

단일 노드 Cloud Volumes ONTAP 시스템의 30일 무료 평가판을 에서 사용할 수 있습니다 "NetApp Cloud Central에서". 시간당 소프트웨어 비용은 없지만 인프라 비용은 여전히 적용됩니다. 무료 평가판은 만료 시 유료 시간별 구독으로 자동 변환됩니다.

개념 증명에 대한 도움이 필요한 경우 에 문의하십시오 "영업 팀" 또는 에서 사용할 수 있는 채팅 옵션을 통해 에 연락할 수 있습니다 "NetApp Cloud Central에서" 그리고 Cloud Manager 내에서.

라이센싱

각 Cloud Volumes ONTAP BYOL 시스템에는 활성 서브스크립션이 설치된 라이센스가 있어야 합니다. 활성 라이센스가 설치되지 않은 경우 Cloud Volumes ONTAP 시스템은 30일 후에 자동으로 종료됩니다. Cloud Manager는 라이센스를 관리하고 만료되기 전에 사용자에게 알려 프로세스를 간소화합니다.

새 시스템의 라이센스 관리

BYOL 시스템을 생성하는 경우 Cloud Manager에서는 NetApp Support 사이트 계정을 묻는 메시지를 표시합니다. Cloud Manager는 이 계정을 사용하여 NetApp에서 라이센스 파일을 다운로드하고 Cloud Volumes ONTAP 시스템에 설치합니다.

"NetApp Support 사이트 계정을 Cloud Manager에 추가하는 방법을 알아보십시오".

Cloud Manager가 보안 인터넷 연결을 통해 라이센스 파일에 액세스할 수 없는 경우 직접 파일을 얻은 다음 파일을 Cloud Manager에 수동으로 업로드할 수 있습니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP BYOL 시스템에 라이센스 파일 설치".

라이센스 만료

Cloud Manager는 라이센스가 만료되기 30일 전과 라이센스가 만료되면 경고를 보냅니다. 다음 이미지는 30일 만료 경고를 보여줍니다.

작업 환경을 선택하여 메시지를 검토할 수 있습니다.

라이센스를 제때 갱신하지 않으면 Cloud Volumes ONTAP 시스템이 자동으로 종료됩니다. 다시 시작하면 자동으로 종료됩니다.

Cloud Volumes ONTAP는 EMS(이벤트 관리 시스템) 이벤트 알림을 사용하여 이메일, SNMP traaphost 또는 syslog 서버를 통해 사용자에게 알릴 수도 있습니다. 자세한 내용은 를 참조하십시오 "ONTAP 9 EMS 구성 익스프레스 가이드".

라이센스 갱신

NetApp 담당자에게 연락하여 BYOL 구독을 갱신하면 Cloud Manager는 NetApp에서 새 라이센스를 자동으로 얻어 Cloud Volumes ONTAP 시스템에 설치합니다.

Cloud Manager가 보안 인터넷 연결을 통해 라이센스 파일에 액세스할 수 없는 경우 직접 파일을 얻은 다음 파일을 Cloud Manager에 수동으로 업로드할 수 있습니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP BYOL 시스템에 라이센스 파일 설치".

보안

Cloud Volumes ONTAP는 데이터 암호화를 지원하고 바이러스 및 랜섬웨어에 대한 보호를 제공합니다.

유휴 데이터의 암호화

Cloud Volumes ONTAP는 다음과 같은 암호화 기술을 지원합니다.

- NetApp 볼륨 암호화(Cloud Volumes ONTAP 9.5부터)
- AWS 키 관리 서비스
- Azure 스토리지 서비스 암호화

네이티브 AWS 및 Azure 암호화와 NetApp 볼륨 암호화를 사용하여 하이퍼바이저 레벨에서 데이터를 암호화할 수 있습니다.

NetApp 볼륨 암호화

NetApp Volume Encryption(NVE)은 유휴 데이터를 한 번에 하나의 볼륨으로 암호화하는 소프트웨어 기반 기술입니다. 데이터, 스냅샷 복사본 및 메타데이터가 암호화됩니다. 데이터에 대한 액세스는 볼륨별로 고유한 XTS-AES-256 키를 통해 제공됩니다.

Cloud Volumes ONTAP은 외부 키 관리 서버에서 NetApp 볼륨 암호화를 지원합니다. Onboard Key Manager는 지원되지 않습니다. 에서 지원되는 주요 관리자를 찾을 수 있습니다 "NetApp 상호 운용성 매트릭스 툴" 주요 관리자 * 솔루션 아래.

CLI 또는 System Manager를 사용하여 새 볼륨이나 기존 볼륨에서 NetApp 볼륨 암호화를 활성화할 수 있습니다. Cloud Manager는 NetApp Volume Encryption을 지원하지 않습니다. 자세한 내용은 을 참조하십시오 "NetApp 볼륨 암호화로 볼륨 암호화".

AWS 키 관리 서비스

AWS에서 Cloud Volumes ONTAP 시스템을 시작하면 를 사용하여 데이터 암호화를 설정할 수 있습니다 "AWS KMS(키 관리 서비스)". Cloud Manager는 CMK(Customer Master Key)를 사용하여 데이터 키를 요청합니다.

이 암호화 옵션을 사용하려면 AWS KMS가 적절하게 설정되어 있는지 확인해야 합니다. 자세한 내용은 을 참조하십시오

"AWS KMS 설정".

Azure 스토리지 서비스 암호화

"Azure 스토리지 서비스 암호화" 저장된 데이터의 경우 Azure의 Cloud Volumes ONTAP 데이터에 대해 기본적으로 활성화됩니다. 설정이 필요하지 않습니다.

Cloud Volumes ONTAP에서는 고객이 관리하는 키가 지원되지 않습니다.

ONTAP 바이러스 검사

ONTAP 시스템에서 통합 바이러스 백신 기능을 사용하여 바이러스나 기타 악성 코드에 의해 데이터가 손상되는 것을 방지할 수 있습니다.

ONTAP 바이러스 검사(*Vscan*)는 동급 최강의 타사 바이러스 백신 소프트웨어와 ONTAP 기능을 결합하여 언제 어떤 파일을 스캔할지 제어하는 데 필요한 유연성을 제공합니다.

Vscan에서 지원하는 공급업체, 소프트웨어 및 버전에 대한 자세한 내용은 를 참조하십시오 "NetApp 상호 운용성 매트릭스".

ONTAP 시스템에서 바이러스 백신 기능을 구성 및 관리하는 방법에 대한 자세한 내용은 을 참조하십시오 "ONTAP 9 안티바이러스 구성 가이드".

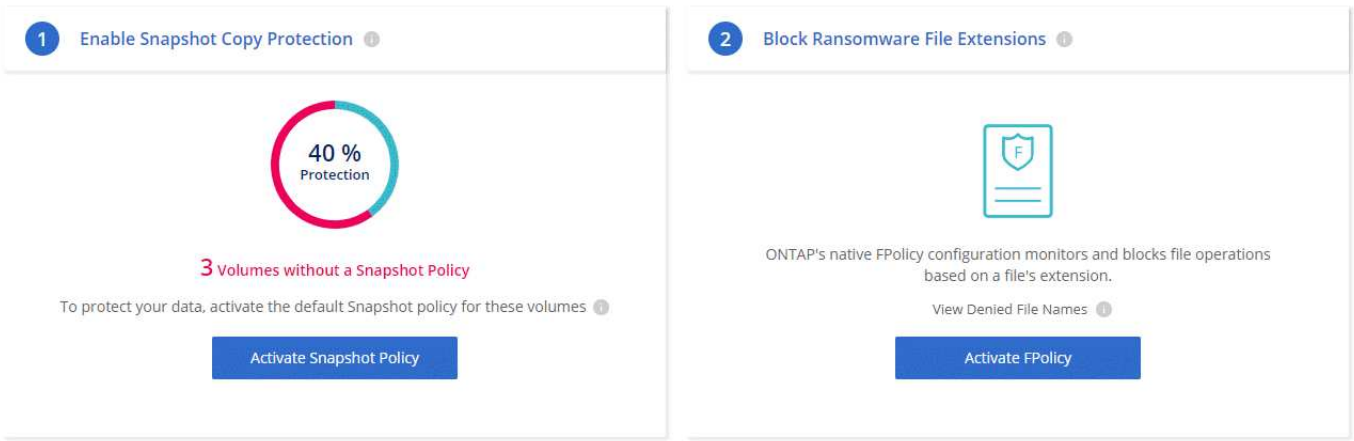
랜섬웨어 보호

랜섬웨어 공격은 비즈니스 시간, 리소스 및 평판에 악영향을 줄 수 있습니다. Cloud Manager를 사용하면 랜섬웨어에 대한 NetApp 솔루션을 구축하고 가시성, 감지, 문제 해결을 위한 효율적인 툴을 제공할 수 있습니다.

- Cloud Manager는 스냅샷 정책에 의해 보호되지 않는 볼륨을 식별하고 이러한 볼륨에서 기본 스냅샷 정책을 활성화할 수 있도록 지원합니다.

  Snapshot 복사본은 읽기 전용이므로 랜섬웨어 손상을 방지합니다. 또한 세분화하여 단일 파일 복사본 또는 전체 재해 복구 솔루션의 이미지를 생성할 수도 있습니다.

- Cloud Manager를 사용하면 ONTAP의 FPolicy 솔루션을 활성화하여 일반적인 랜섬웨어 파일 확장을 차단할 수도 있습니다.



"랜섬웨어에 대한 NetApp 솔루션을 구축하는 방법을 알아보십시오".

성능

성능 결과를 검토하여 Cloud Volumes ONTAP에 적합한 워크로드를 결정할 수 있습니다.

AWS용 Cloud Volumes ONTAP의 경우 를 참조하십시오 "NetApp 기술 보고서 4383: 애플리케이션 워크로드를 포함한 Amazon Web Services의 Cloud Volumes ONTAP 성능 특성".

Microsoft Azure용 Cloud Volumes ONTAP의 경우 를 참조하십시오 "NetApp 기술 보고서 4671: 애플리케이션 워크로드를 포함한 Azure의 Cloud Volumes ONTAP 성능 특성".

시작하기

구축 개요

시작하기 전에 OnCommand Cloud Manager 및 Cloud Volumes ONTAP 구축 옵션에 대해 잘 알고 싶을 수 있습니다.

Cloud Manager 설치

Cloud Volumes ONTAP를 구축 및 관리하려면 Cloud Manager 소프트웨어가 필요합니다. Cloud Manager는 다음 위치 중 원하는 곳에 구축할 수 있습니다.

- AWS(Amazon Web Services)
- Microsoft Azure를 참조하십시오
- IBM 클라우드
- 직접 네트워크를 통해

Cloud Manager의 구축 방법은 선택한 위치에 따라 다릅니다.

위치	**Cloud Manager** 구축 방법
설치하고	"NetApp Cloud Central에서 Cloud Manager 구축"
AWS C2S	"AWS Intelligence Community Marketplace에서 Cloud Manager 구축"
Azure는 일반적으로 사용 가능한 지역입니다	"NetApp Cloud Central에서 Cloud Manager 구축"
Azure 정부	"Azure US Government Marketplace에서 Cloud Manager를 구현합니다"
Azure 독일	"Linux 호스트에 소프트웨어를 다운로드하고 설치합니다"
IBM 클라우드	"Linux 호스트에 소프트웨어를 다운로드하고 설치합니다"
온프레미스 네트워크	"Linux 호스트에 소프트웨어를 다운로드하고 설치합니다"

Cloud Manager 설정

클라우드 공급자 계정 추가, HTTPS 인증서 설치 등과 같은 Cloud Manager를 설치한 후 추가 설정을 수행할 수 있습니다.

- "Cloud Manager에 클라우드 공급자 계정 추가"
- "HTTPS 인증서 설치"
- "사용자 및 테넌트 설정"
- "AWS KMS 설정"

Cloud Volumes ONTAP 구축

Cloud Manager를 시작 및 실행한 후 AWS 및 Microsoft Azure에서 Cloud Volumes ONTAP 구축을 시작할 수

있습니다.

"AWS 시작하기" 및 "Azure에서 시작하기" Cloud Volumes ONTAP를 빠르게 시작하고 실행하기 위한 지침을 제공합니다. 추가 도움말은 다음을 참조하십시오.

- "Cloud Volumes ONTAP 9.5에 지원되는 구성입니다"
- "구성 계획"
- "AWS에서 Cloud Volumes ONTAP 실행"
- "Azure에서 Cloud Volumes ONTAP 실행"

AWS에서 Cloud Volumes ONTAP 시작하기

NetApp Cloud Central에서 AWS의 Cloud Volumes ONTAP를 시작할 수 있습니다.

네트워크 설정

1. Cloud Manager 및 Cloud Volumes ONTAP가 여러 엔드포인트에 연결할 수 있도록 타겟 VPC에서 아웃바운드 인터넷 액세스를 지원합니다.

   이 단계는 Cloud Manager가 아웃바운드 인터넷 액세스 없이 Cloud Volumes ONTAP를 구축할 수 없기 때문에 중요합니다. 아웃바운드 연결을 제한해야 하는 경우 의 끝점 목록을 참조하십시오 "클라우드 관리자" 및 "Cloud Volumes ONTAP".

2. VPC 엔드포인트를 S3 서비스로 설정합니다.

   Cloud Volumes ONTAP의 콜드 데이터를 저비용 오브젝트 스토리지로 계층화하려는 경우 VPC 엔드포인트가 필요합니다.

AWS Marketplace에서 **Cloud Volumes ONTAP**를 구독하십시오

가입 "AWS 마켓플레이스" 소프트웨어 약관에 동의해야 합니다. 마켓플레이스에서만 구독해야 합니다. 어디서나 Cloud Volumes ONTAP를 시작할 수는 있지만 Cloud Manager는 지원되지 않습니다.

필요한 **AWS** 권한을 제공합니다

NetApp Cloud Central에서 Cloud Manager를 구축할 때 인스턴스를 배포할 수 있는 권한이 있는 AWS 계정을 사용해야 합니다.

1. AWS IAM 콘솔로 이동하여 의 내용을 복사하여 붙여 넣어 정책을 생성합니다 "AWS를 위한 NetApp Cloud Central 정책".
2. 정책을 IAM 사용자에게 연결합니다.

NetApp Cloud Central에서 **Cloud Manager**를 실행합니다

Cloud Volumes ONTAP를 구축 및 관리하려면 Cloud Manager 소프트웨어가 필요합니다. Cloud Manager 인스턴스를 시작하는 데는 몇 분 밖에 걸리지 않습니다 "Cloud Central을 참조하십시오".

Cloud Manager를 사용하여 **Cloud Volumes ONTAP**를 실행합니다

Cloud Manager가 준비되면 생성 을 클릭하고 시작할 시스템 유형을 선택한 다음 마법사의 단계를 완료합니다. 25분 후 첫 번째 Cloud Volumes ONTAP 시스템이 가동되어 실행 중이어야 합니다.

관련 링크

- "평가 중"
- "Cloud Manager의 네트워킹 요구사항"
- "AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항"
- "AWS의 보안 그룹 규칙"
- "Cloud Manager에 클라우드 공급자 계정 추가"
- "Cloud Manager에서 AWS 권한을 통해 수행하는 것"
- "AWS에서 Cloud Volumes ONTAP 실행"
- "AWS Marketplace에서 Cloud Manager 시작"

Azure에서 Cloud Volumes ONTAP 시작하기

NetApp Cloud Central에서 Azure의 Cloud Volumes ONTAP를 시작할 수 있습니다. Cloud Manager를 구축할 수 있는 별도의 지침이 제공됩니다 "Azure 미국 정부 지역" 및 IN "Azure 독일 지역".

네트워크 설정

클라우드 관리자 및 Cloud Volumes ONTAP가 여러 엔드포인트에 연결할 수 있도록 대상 VNET에서 아웃바운드 인터넷 액세스를 활성화합니다.

이 단계는 Cloud Manager가 아웃바운드 인터넷 액세스 없이 Cloud Volumes ONTAP를 구축할 수 없기 때문에 중요합니다. 아웃바운드 연결을 제한해야 하는 경우 의 끝점 목록을 참조하십시오 "클라우드 관리자" 및 "Cloud Volumes ONTAP".

필요한 **Azure** 권한을 제공합니다

NetApp Cloud Central에서 Cloud Manager를 구축할 때 Cloud Manager 가상 머신을 구축할 권한이 있는 Azure 계정을 사용해야 합니다.

1. 를 다운로드합니다 "Azure를 위한 NetApp Cloud Central 정책".

2. Azure 구독 ID를 "AssignableScopes" 필드에 추가하여 JSON 파일을 수정합니다.
3. JSON 파일을 사용하여 이름이 _Azure SetupAsService_인 Azure에서 사용자 지정 역할을 생성합니다.

   예: * az 역할 정의 create — role-definition C:\Policy_for_Setup_as_Service_Azure.json *

4. Azure 포털에서 Cloud Central에서 Cloud Manager를 배포할 사용자에게 사용자 지정 역할을 할당합니다.

NetApp Cloud Central에서 **Cloud Manager**를 실행합니다

Cloud Volumes ONTAP를 구축 및 관리하려면 Cloud Manager 소프트웨어가 필요합니다. Cloud Manager 인스턴스를 시작하는 데는 몇 분 밖에 걸리지 않습니다 "Cloud Central을 참조하십시오".

Cloud Manager를 사용하여 **Cloud Volumes ONTAP**를 실행합니다

Cloud Manager가 준비되면 생성 을 클릭하고 구축할 시스템 유형을 선택한 다음 마법사의 단계를 완료합니다. 25분 후 첫 번째 Cloud Volumes ONTAP 시스템이 가동되어 실행 중이어야 합니다.

관련 링크

- "평가 중"
- "Cloud Manager의 네트워킹 요구사항"
- "Azure의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항"
- "Azure의 보안 그룹 규칙"
- "Cloud Manager에 클라우드 공급자 계정 추가"
- "Cloud Manager가 Azure 권한으로 수행하는 기능"
- "Azure에서 Cloud Volumes ONTAP 실행"
- "Azure 마켓플레이스에서 Cloud Manager 시작"

Cloud Manager 설정

Cloud Manager에 클라우드 공급자 계정 추가

다른 클라우드 계정에 Cloud Volumes ONTAP를 배포하려면 해당 계정에 필요한 권한을 제공한 다음 세부 정보를 Cloud Manager에 추가해야 합니다.

Cloud Central에서 Cloud Manager를 구축하면 Cloud Manager가 자동으로 을 추가합니다 "클라우드 공급자 계정입니다" Cloud Manager를 구축한 계정의 경우 기존 시스템에 Cloud Manager 소프트웨어를 수동으로 설치한 경우 초기 클라우드 공급자 계정이 추가되지 않습니다.

Cloud Manager에 AWS 계정 설정 및 추가

다른 AWS 계정에 Cloud Volumes ONTAP를 구축하려는 경우 해당 계정에 필요한 권한을 제공한 다음 세부 정보를 Cloud Manager에 추가해야 합니다. 사용 권한을 제공하는 방법은 Cloud Manager에 AWS 키를 제공할지, 아니면 신뢰할 수 있는 계정에서 역할의 ARN을 제공하는지에 따라 달라집니다.

- AWS 키를 제공할 때 사용 권한 부여
- 다른 계정에서 IAM 역할을 가정하여 권한 부여

AWS 키를 제공할 때 사용 권한 부여

Cloud Manager에 IAM 사용자를 위한 AWS 키를 제공하려면 해당 사용자에게 필요한 권한을 부여해야 합니다. Cloud Manager IAM 정책은 Cloud Manager에서 사용할 수 있는 AWS 작업 및 리소스를 정의합니다.

단계

1. 에서 Cloud Manager IAM 정책을 다운로드합니다 "Cloud Manager 정책 페이지".
2. IAM 콘솔에서 Cloud Manager IAM 정책의 텍스트를 복사하여 붙여넣어 고유한 정책을 생성합니다.

   "AWS 설명서: IAM 정책 생성"

3. IAM 역할 또는 IAM 사용자에 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"

결과

이제 계정에 필요한 권한이 있습니다. 이제 Cloud Manager에 추가할 수 있습니다.

다른 계정에서 IAM 역할을 가정하여 권한 부여

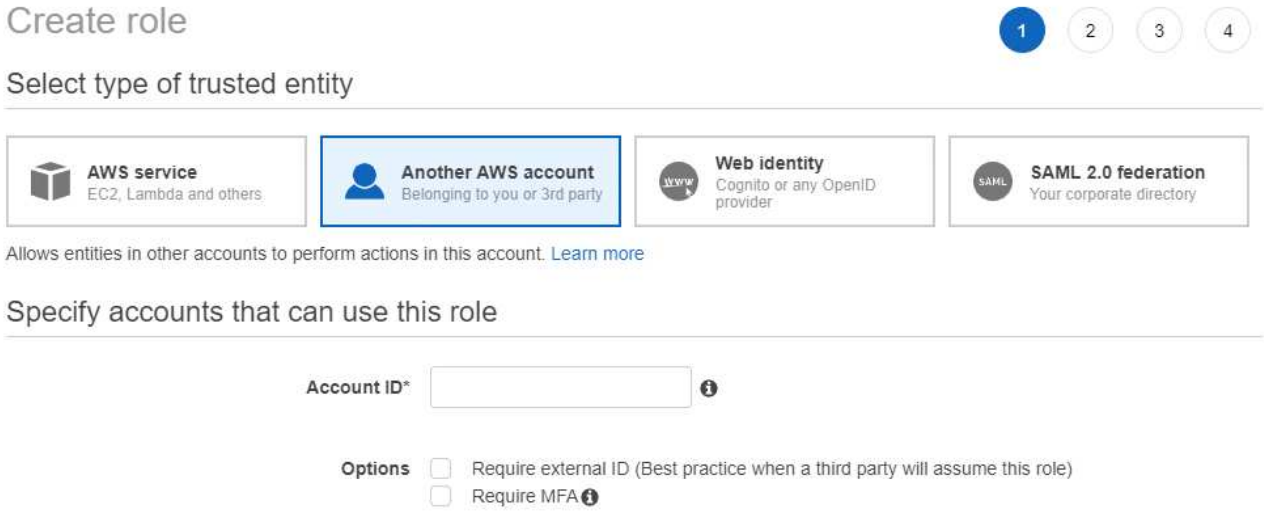
IAM 역할을 사용하여 Cloud Manager 인스턴스와 다른 AWS 계정을 구축한 소스 AWS 계정과 신뢰 관계를 설정할 수 있습니다. 그런 다음 Cloud Manager에 신뢰할 수 있는 계정의 IAM 역할 ARN을 제공합니다.

단계

1. Cloud Volumes ONTAP를 배포하려는 대상 계정으로 이동하여 * 다른 AWS 계정 * 을 선택하여 IAM 역할을 생성합니다.

   다음을 수행하십시오.

   - Cloud Manager 인스턴스가 있는 계정의 ID를 입력합니다.
   - 에서 사용할 수 있는 Cloud Manager IAM 정책을 연결합니다 "Cloud Manager 정책 페이지".



2. Cloud Manager 인스턴스가 있는 소스 계정으로 이동하여 인스턴스에 연결된 IAM 역할을 선택합니다.

   a. 신뢰 관계 > 신뢰 관계 편집 * 을 클릭합니다.

   b. "STS:AssumRole" 작업과 대상 계정에서 생성한 역할의 ARN을 추가합니다.

      ▪ 예 *

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

결과

이제 계정에 필요한 권한이 있습니다. 이제 Cloud Manager에 추가할 수 있습니다.

Cloud Manager에 AWS 계정 추가

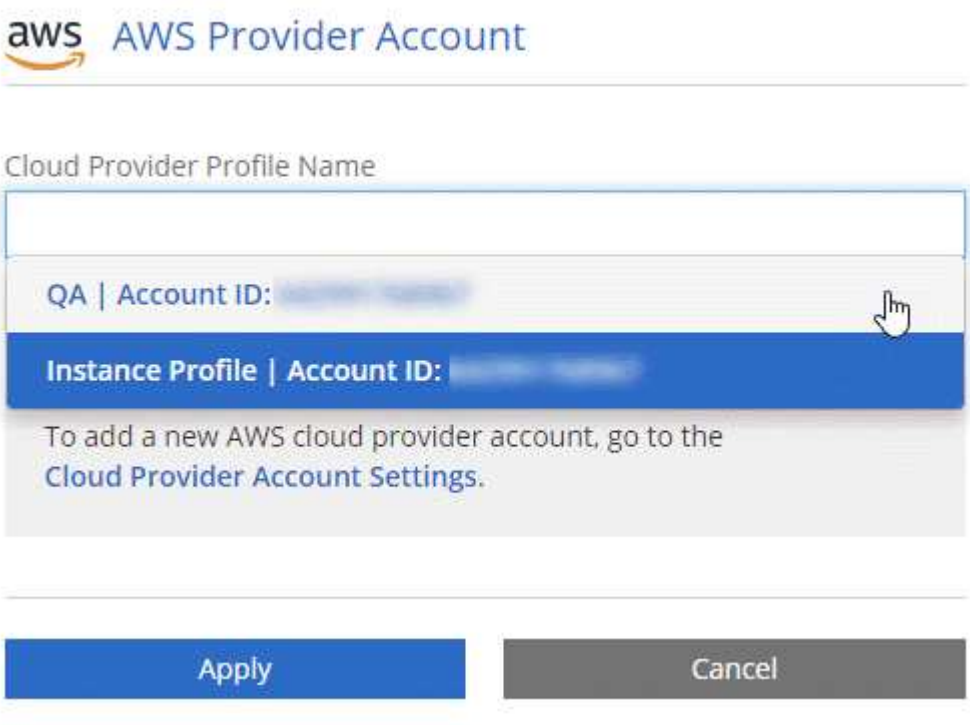
필요한 권한이 있는 AWS 계정을 제공한 후 Cloud Manager에 계정을 추가할 수 있습니다. 그러면 해당 계정에서 Cloud Volumes ONTAP 시스템을 시작할 수 있습니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 작업 드롭다운 목록을 클릭한 다음 * 계정 설정 * 을 선택합니다.
2. 새 계정 추가 * 를 클릭하고 * AWS * 를 선택합니다.
3. AWS 키를 제공할지 또는 신뢰할 수 있는 IAM 역할의 ARN을 제공할지 여부를 선택합니다.
4. 정책 요구 사항이 충족되었는지 확인한 다음 * 계정 생성 * 을 클릭합니다.

결과

이제 새 작업 환경을 생성할 때 세부 정보 및 자격 증명 페이지에서 다른 계정으로 전환할 수 있습니다.



Cloud Manager에 **Azure** 계정 설정 및 추가

다른 Azure 계정에 Cloud Volumes ONTAP를 배포하려는 경우 해당 계정에 필요한 권한을 제공한 다음 Cloud Manager에 계정에 대한 세부 정보를 추가해야 합니다.

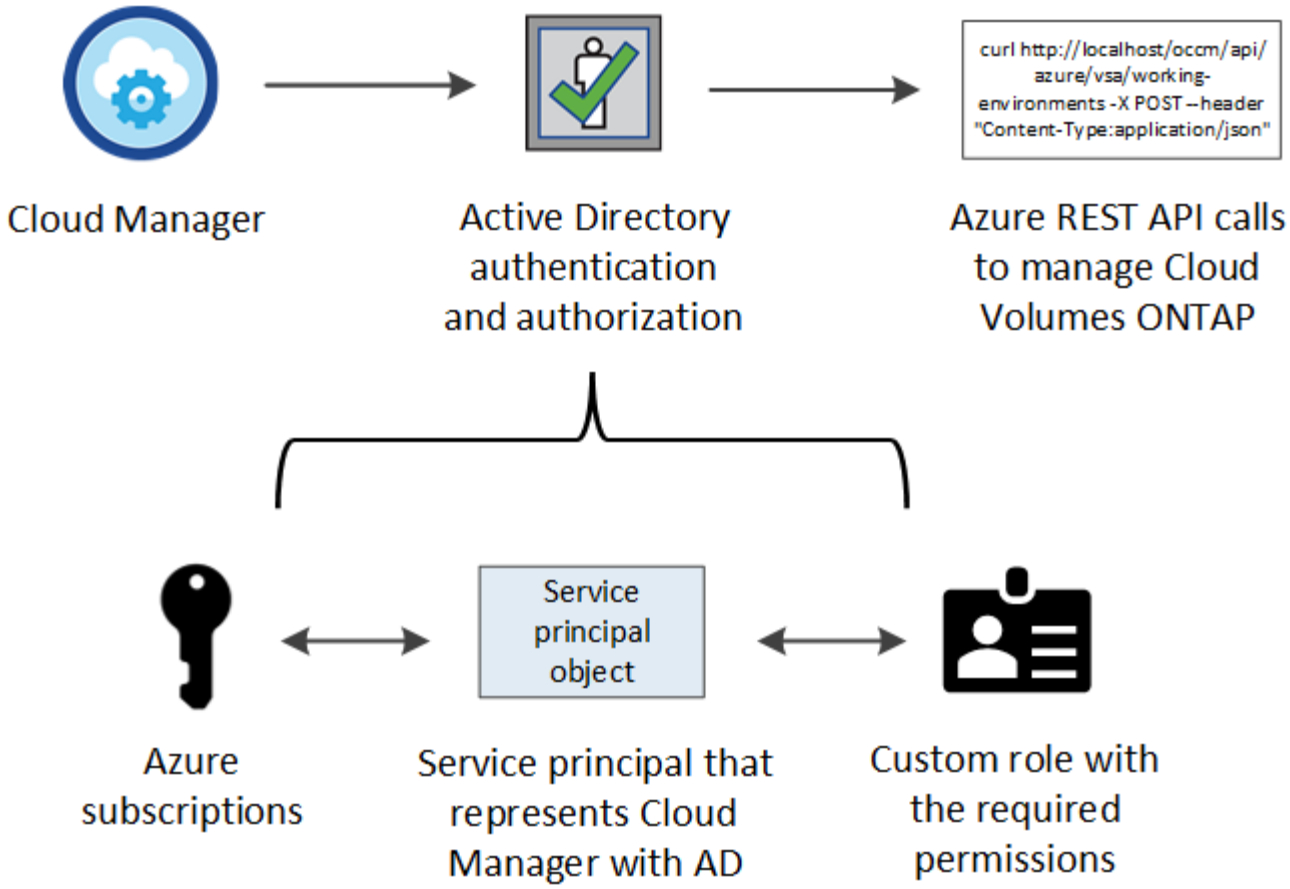
- 서비스 보안 주체를 사용하여 Azure 사용 권한 부여
- Cloud Manager에 Azure 계정 추가

서비스 보안 주체를 사용하여 **Azure** 사용 권한 부여

Cloud Manager는 Azure에서 작업을 수행할 수 있는 권한이 필요합니다. Azure Active Directory에서 서비스 보안 주체를 생성 및 설정하고 Cloud Manager에 필요한 Azure 자격 증명을 획득하여 Azure 계정에 필요한 권한을 부여할 수 있습니다.

이 작업에 대해

다음 그림에서는 Cloud Manager가 Azure에서 작업을 수행할 수 있는 권한을 얻는 방법을 보여 줍니다. 하나 이상의 Azure 구독에 연결된 서비스 보안 주체 개체는 Azure Active Directory의 Cloud Manager를 나타내며 필요한 권한을 허용하는 사용자 지정 역할에 할당됩니다.



다음 단계에서는 새로운 Azure 포털을 사용합니다. 문제가 발생하는 경우 Azure Classic 포털을 사용해야 합니다.

단계

1. 필요한 Cloud Manager 권한으로 사용자 지정 역할을 생성합니다.
2. Active Directory 서비스 보안 사용자를 생성합니다.
3. 사용자 지정 Cloud Manager 운영자 역할을 서비스 보안 주체에 할당합니다.

필요한 **Cloud Manager** 권한으로 사용자 지정 역할 생성

Azure에서 Cloud Volumes ONTAP를 시작 및 관리하는 데 필요한 권한을 클라우드 관리자에게 제공하려면 사용자 지정 역할이 필요합니다.

단계

1. 를 다운로드합니다 "Cloud Manager Azure 정책".
2. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

   사용자가 Cloud Volumes ONTAP 시스템을 생성할 각 Azure 구독에 대한 ID를 추가해야 합니다.

   ◦ 예 *

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

3. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 생성합니다.

   다음 예에서는 Azure CLI 2.0을 사용하여 사용자 지정 역할을 생성하는 방법을 보여 줍니다.

   ◦ az 역할 정의 create — 역할 정의 C:\Policy_for_cloud_Manager_Azure_3.6.1.json *

결과

이제 OnCommand 클라우드 관리자 운영자 라는 사용자 지정 역할을 갖게 됩니다.

Active Directory 서비스 보안 주체 만들기

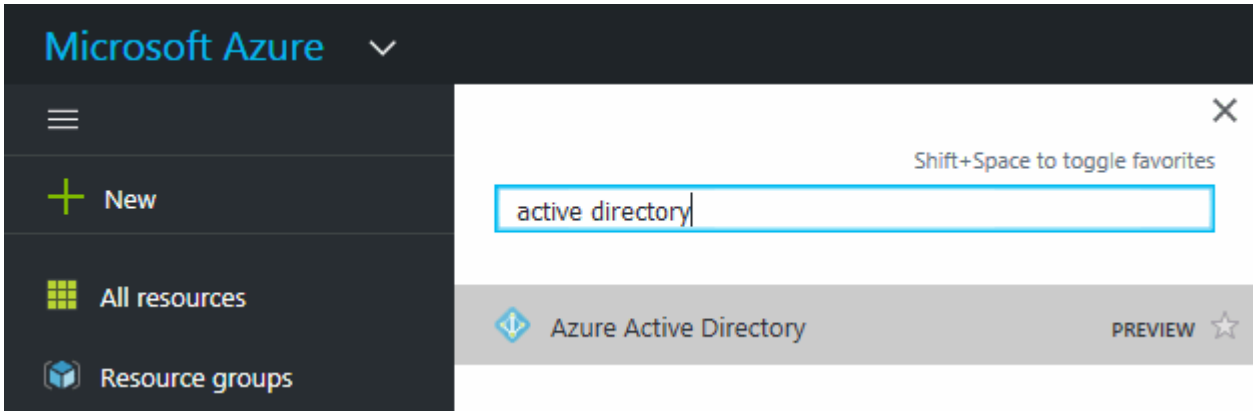
Cloud Manager가 Azure Active Directory로 인증할 수 있도록 Active Directory 서비스 보안 주체를 만들어야 합니다.

시작하기 전에

Active Directory 응용 프로그램을 만들고 응용 프로그램을 역할에 할당하려면 Azure에 적절한 권한이 있어야 합니다. 자세한 내용은 을 참조하십시오 "Microsoft Azure 설명서: 포털을 사용하여 리소스에 액세스할 수 있는 Active Directory 응용 프로그램 및 서비스 보안 주체를 만듭니다".

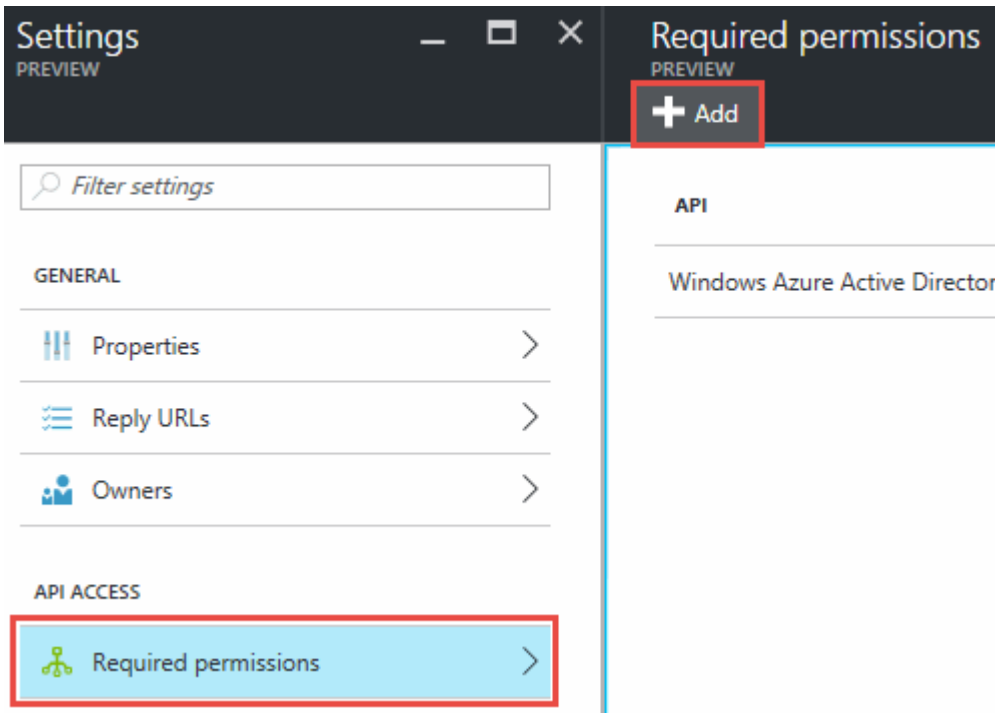
단계

1. Azure 포털에서 * Azure Active Directory * 서비스를 엽니다.

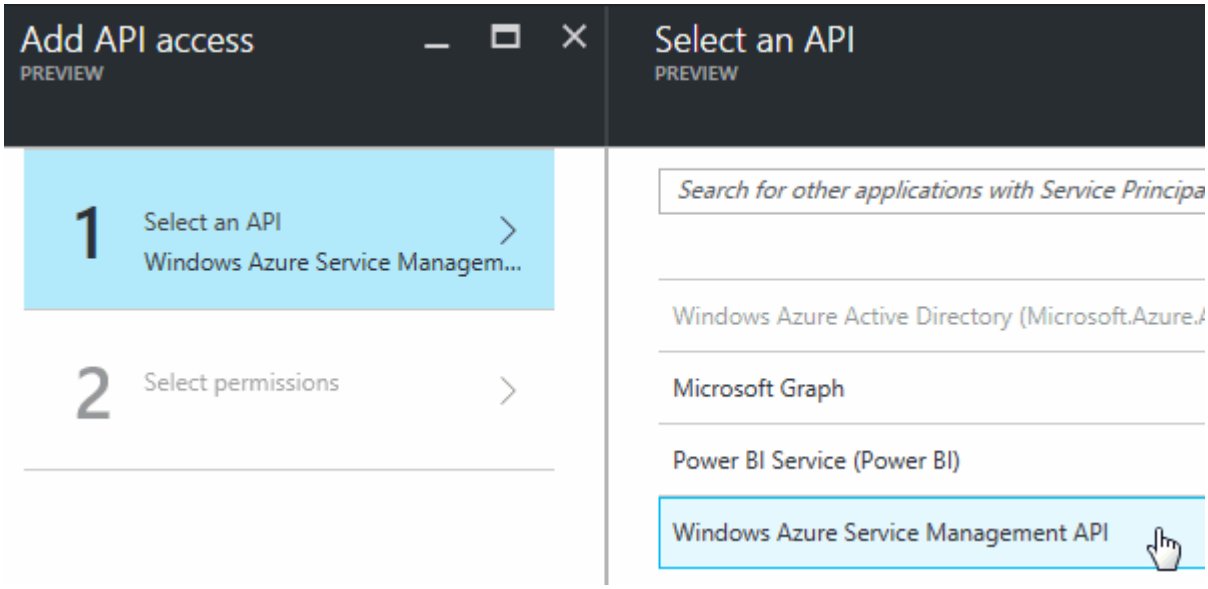


2. 메뉴에서 * 앱 등록(레거시) * 을 클릭합니다.
3. 서비스 보안 주체 만들기:
   a. 새 응용 프로그램 등록 * 을 클릭합니다.
   b. 응용 프로그램 이름을 입력하고 * Web App/API * 를 선택한 상태로 URL을 입력합니다(예: http://url
   c. Create * 를 클릭합니다.
4. 응용 프로그램을 수정하여 필요한 권한을 추가합니다.
   a. 생성된 애플리케이션을 선택합니다.

b. 설정에서 * 필요한 권한 * 을 클릭한 다음 * 추가 * 를 클릭합니다.



c. Select an API * 를 클릭하고 * Windows Azure Service Management API * 를 선택한 다음 * Select * 를 클릭합니다.



d. 조직 사용자로 Azure 서비스 관리 액세스 * 를 클릭하고 * 선택 * 을 클릭한 다음 * 완료 * 를 클릭합니다.

5. 서비스 보안 주체에 대한 키를 생성합니다.

a. 설정에서 * 키 * 를 클릭합니다.

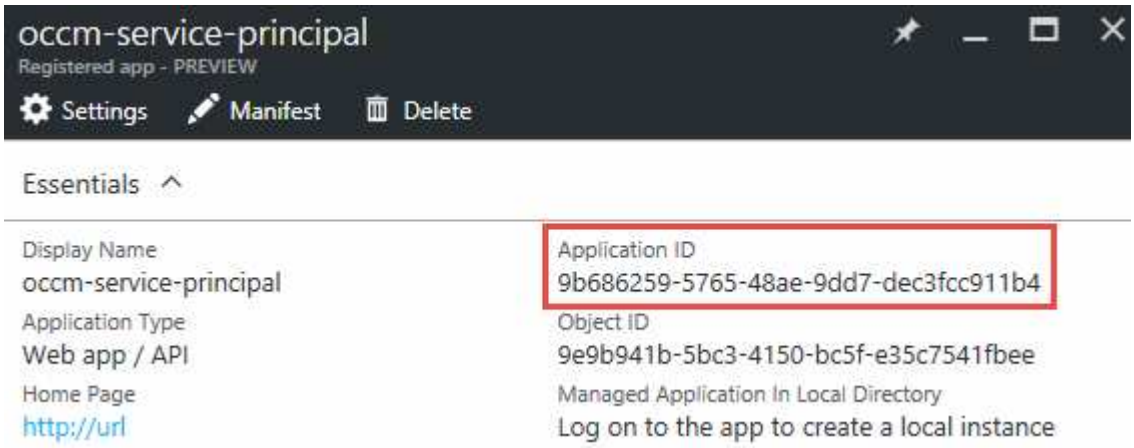
b. 설명을 입력하고 기간을 선택한 다음 * 저장 * 을 클릭합니다.

c. 키 값을 복사합니다.

클라우드 공급자 계정을 Cloud Manager에 추가할 때 키 값을 입력해야 합니다.

d. 속성 * 을 클릭한 다음 서비스 보안 주체에 대한 응용 프로그램 ID를 복사합니다.

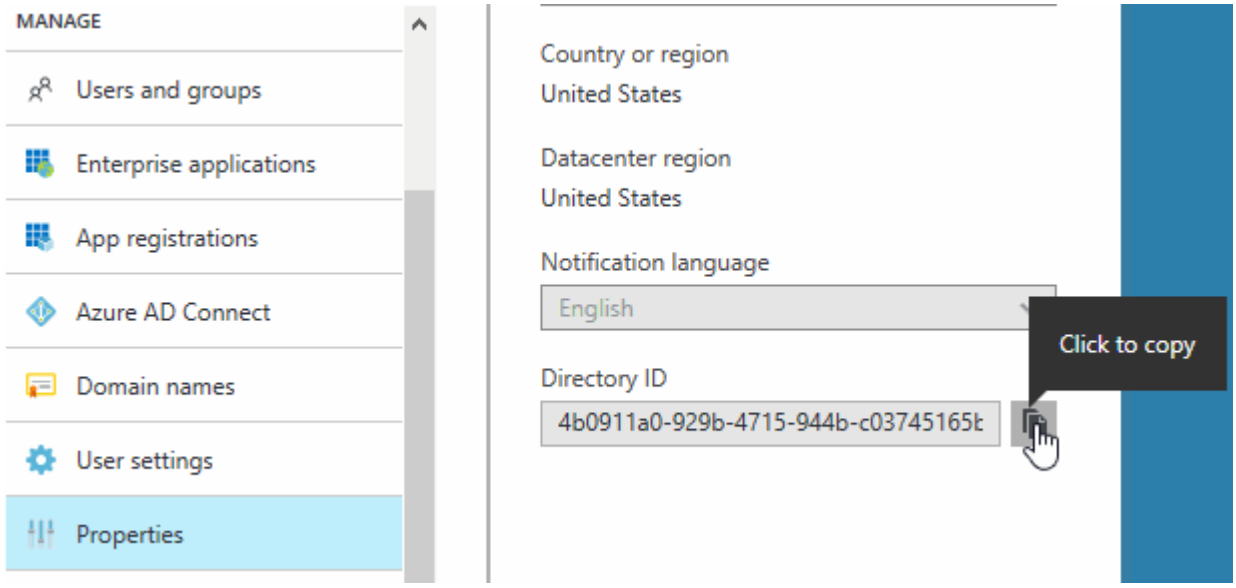
키 값과 마찬가지로, Cloud Manager에 클라우드 공급자 계정을 추가할 때 Cloud Manager에 애플리케이션 ID를 입력해야 합니다.



6. 조직의 Active Directory 테넌트 ID를 가져옵니다.

a. Active Directory 메뉴에서 * 속성 * 을 클릭합니다.

b. 디렉터리 ID를 복사합니다.



애플리케이션 ID 및 애플리케이션 키와 마찬가지로 클라우드 공급자 계정을 Cloud Manager에 추가할 때 Active Directory 테넌트 ID를 입력해야 합니다.

결과

이제 Active Directory 서비스 보안 주체가 있어야 하며 응용 프로그램 ID, 응용 프로그램 키 및 Active Directory 테넌트 ID를 복사해야 합니다. 클라우드 공급자 계정을 추가할 때는 Cloud Manager에 이 정보를 입력해야 합니다.

서비스 보안 주체에 **Cloud Manager** 운영자 역할 할당

서비스 보안 주체를 하나 이상의 Azure 구독에 바인딩하고 Cloud Manager 운영자 역할을 할당해야만 Cloud

Manager가 Azure에서 권한을 갖게 됩니다.

이 작업에 대해

여러 Azure 구독에서 Cloud Volumes ONTAP를 배포하려면 서비스 보안 주체를 해당 구독 각각에 바인딩해야 합니다. Cloud Manager를 사용하면 Cloud Volumes ONTAP를 구축할 때 사용할 구독을 선택할 수 있습니다.

단계

1. Azure 포털의 왼쪽 창에서 * 구독 * 을 선택합니다.
2. 구독을 선택합니다.
3. IAM(Access Control) * 을 클릭한 다음 * 추가 * 를 클릭합니다.
4. OnCommand 클라우드 관리자 운영자 * 역할을 선택하십시오.
5. 응용 프로그램의 이름을 검색합니다(스크롤하면 목록에서 찾을 수 없음).
6. 응용 프로그램을 선택하고 * 선택 * 을 클릭한 다음 * 확인 * 을 클릭합니다.

결과

이제 Cloud Manager의 서비스 보안 주체에 필요한 Azure 권한이 있습니다.

Cloud Manager에 **Azure** 계정 추가

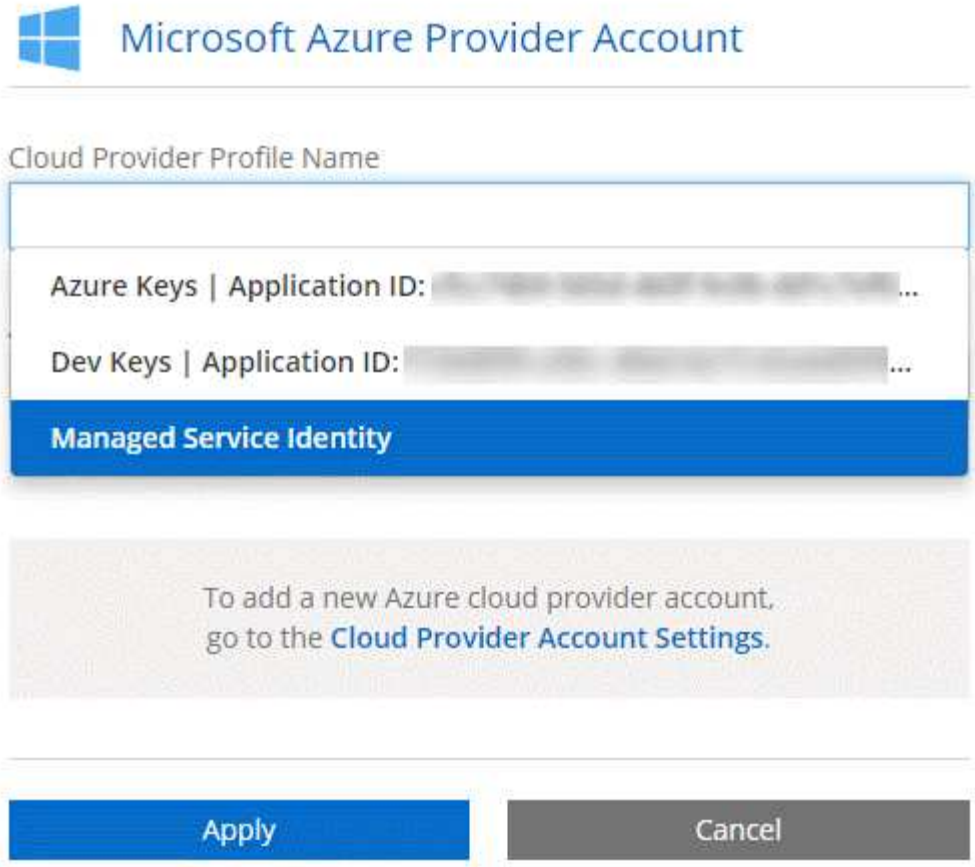
필요한 권한이 있는 Azure 계정을 제공한 후 Cloud Manager에 계정을 추가할 수 있습니다. 그러면 해당 계정에서 Cloud Volumes ONTAP 시스템을 시작할 수 있습니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 작업 드롭다운 목록을 클릭한 다음 * 계정 설정 * 을 선택합니다.
2. 새 계정 추가 * 를 클릭하고 * Microsoft Azure * 를 선택합니다.
3. 필요한 권한을 부여하는 Azure Active Directory 서비스 보안 주체에 대한 정보를 입력합니다.
4. 정책 요구 사항이 충족되었는지 확인한 다음 * 계정 생성 * 을 클릭합니다.

결과

이제 새 작업 환경을 생성할 때 세부 정보 및 자격 증명 페이지에서 다른 계정으로 전환할 수 있습니다.



관리되는 **ID**와 추가 **Azure** 구독을 연결합니다

Cloud Manager를 사용하면 Cloud Volumes ONTAP를 배포할 Azure 계정 및 구독을 선택할 수 있습니다. 를 연결하지 않으면 관리 ID 프로필에 대해 다른 Azure 구독을 선택할 수 없습니다 "관리 ID" 있습니다.

이 작업에 대해

관리 ID가 초기 ID입니다 "클라우드 공급자 계정입니다" NetApp Cloud Central에서 Cloud Manager를 구축할 때 Cloud Manager를 구축하면 Cloud Central에서 OnCommand Cloud Manager 운영자 역할을 생성하여 Cloud Manager 가상 머신에 할당합니다.

단계

1. Azure 포털에 로그인합니다.
2. Subscriptions * 서비스를 연 다음 Cloud Volumes ONTAP 시스템을 배포할 구독을 선택합니다.
3. IAM(액세스 제어) * 을 클릭합니다.
   a. Add * > * Add role assignment * 를 클릭한 후 권한을 추가합니다.
      - OnCommand 클라우드 관리자 운영자 * 역할을 선택하십시오.

        OnCommand Cloud Manager Operator는 에 제공되는 기본 이름입니다 "Cloud Manager 정책". 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

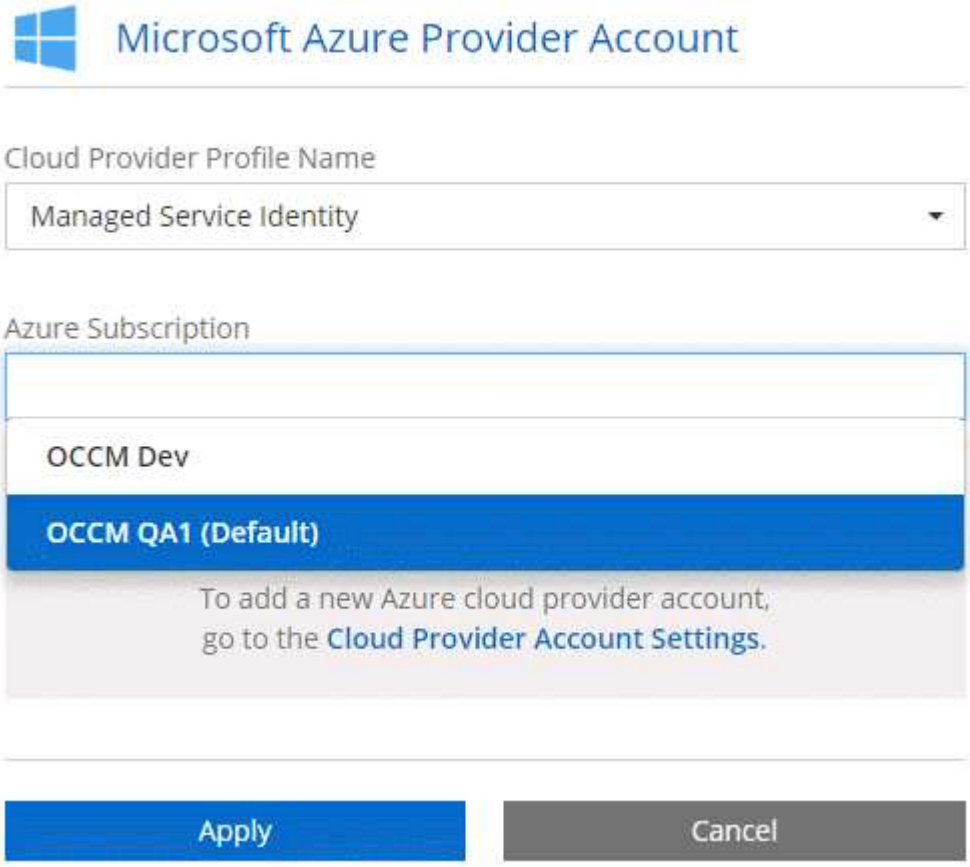
      - Virtual Machine * 에 대한 액세스 권한을 할당합니다.
      - Cloud Manager 가상 머신이 생성된 서브스크립션을 선택합니다.

- Cloud Manager 가상 머신을 선택합니다.
- 저장 * 을 클릭합니다.

4. 추가 구독에 대해 이 단계를 반복합니다.

결과

새 작업 환경을 만들 때 이제 관리되는 ID 프로필에 대해 여러 Azure 구독에서 선택할 수 있습니다.



Cloud Manager에 NetApp Support 사이트 계정 추가

BYOL 시스템을 구축하려면 NetApp Support 사이트 계정을 Cloud Manager에 추가해야 합니다. 또한 종량제 시스템을 등록하고 ONTAP 소프트웨어를 업그레이드해야 합니다.

다음 비디오에서 Cloud Manager에 NetApp Support 사이트 계정을 추가하는 방법을 알아보십시오. 또는 아래로 스크롤하여 단계를 읽습니다.

[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

단계

1. 아직 NetApp Support 사이트 계정이 없는 경우 "1인 등록".
2. Cloud Manager 콘솔의 오른쪽 위에서 작업 드롭다운 목록을 클릭한 다음 * 계정 설정 * 을 선택합니다.
3. 새 계정 추가 * 를 클릭하고 * NetApp Support 사이트 * 를 선택합니다.

4. 계정의 이름을 지정한 다음 사용자 이름과 암호를 입력합니다.
   - 계정은 고객 수준 계정이어야 합니다(게스트 또는 임시 계정이 아님).
   - BYOL 시스템을 구축하려는 경우:
     - 이 계정은 BYOL 시스템의 일련 번호에 액세스할 수 있는 권한이 있어야 합니다.
     - 안전한 BYOL 구독을 구입한 경우 보안 NSS 계정이 필요합니다.
5. 계정 만들기 * 를 클릭합니다

다음 단계

이제 사용자는 새 Cloud Volumes ONTAP 시스템을 생성할 때와 기존 시스템을 등록할 때 계정을 선택할 수 있습니다.

- "AWS에서 Cloud Volumes ONTAP 실행"
- "Azure에서 Cloud Volumes ONTAP 실행"
- "선불 종량제 시스템을 등록하는 중입니다"
- "Cloud Manager로 라이센스 파일을 관리하는 방법에 대해 알아보십시오"

보안 액세스를 위해 **HTTPS** 인증서 설치

기본적으로 Cloud Manager는 웹 콘솔에 대한 HTTPS 액세스를 위해 자체 서명된 인증서를 사용합니다. CA(인증 기관)에서 서명한 인증서를 설치하면 자체 서명된 인증서보다 보안 보호가 향상됩니다.

단계

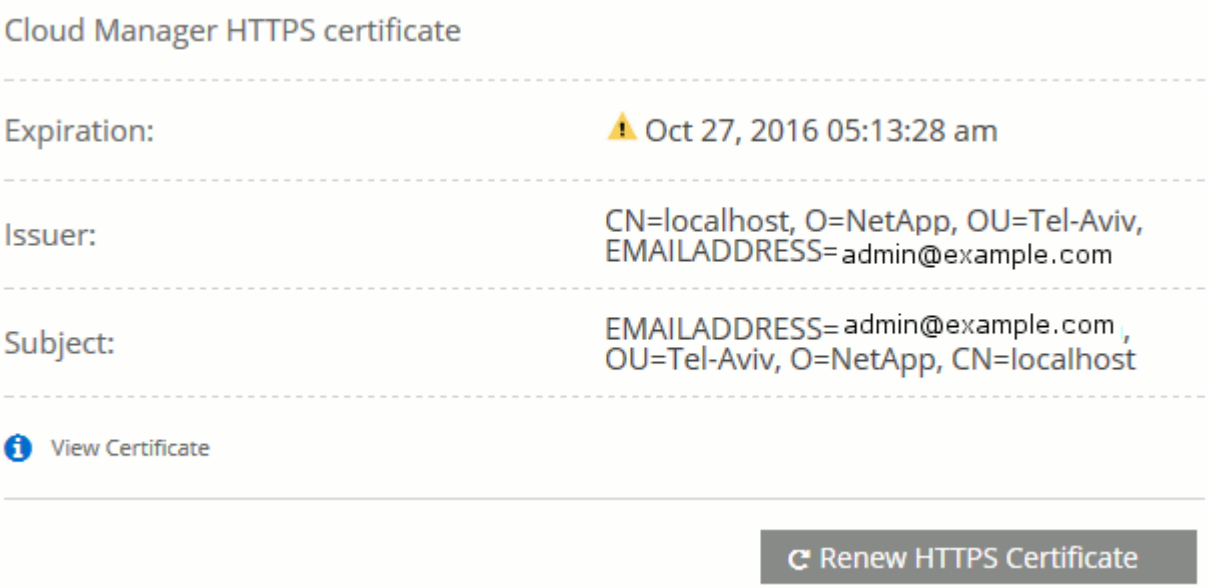
1. Cloud Manager 콘솔의 오른쪽 위에서 작업 드롭다운 목록을 클릭한 다음 * HTTPS 설정 * 을 선택합니다.
2. HTTPS 설정 페이지에서 인증서 서명 요청(CSR)을 생성하거나 고유한 CA 서명 인증서를 설치하여 인증서를 설치합니다.

옵션을 선택합니다	설명
CSR을 생성합니다	a. Cloud Manager 호스트(공통 이름)의 호스트 이름 또는 DNS를 입력한 다음 * CSR 생성 * 을 클릭합니다. Cloud Manager는 인증서 서명 요청을 표시합니다. b. CSR을 사용하여 CA에 SSL 인증서 요청을 제출합니다. 인증서는 PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식을 사용해야 합니다. c. 서명된 인증서의 내용을 복사하여 인증서 필드에 붙여 넣은 다음 * 설치 * 를 클릭합니다.

옵션을 선택합니다	설명
고유한 CA 서명 인증서를 설치합니다	a. CA 서명 인증서 설치 * 를 선택합니다. b. 인증서 파일과 개인 키를 모두 로드한 다음 * 설치 * 를 클릭합니다. 인증서는 PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식을 사용해야 합니다.

결과

Cloud Manager는 이제 CA 서명 인증서를 사용하여 보안 HTTPS 액세스를 제공합니다. 다음 이미지는 보안 액세스를 위해 구성된 Cloud Manager 시스템을 보여줍니다.



사용자 및 테넌트 설정

Cloud Manager를 사용하면 Cloud Manager에 Cloud Central 사용자를 추가하고 테넌트를 사용하여 작업 환경을 격리할 수 있습니다.

Cloud Manager에 사용자 추가

추가 사용자가 Cloud Manager 시스템을 사용해야 하는 경우 NetApp Cloud Central에서 계정을 등록해야 합니다. 그런 다음 Cloud Manager에 사용자를 추가할 수 있습니다.

단계

1. 아직 NetApp Cloud Central에 계정이 없는 경우 Cloud Manager 시스템에 대한 링크를 보내 등록하도록 하십시오.

   사용자가 계정 등록을 확인할 때까지 기다립니다.

2. Cloud Manager에서 사용자 아이콘을 클릭한 다음 * 사용자 보기 * 를 클릭합니다.
3. 새 사용자 * 를 클릭합니다.

4. 사용자 계정과 연결된 이메일 주소를 입력하고 역할을 선택한 다음 * 추가 * 를 클릭합니다.

다음 단계

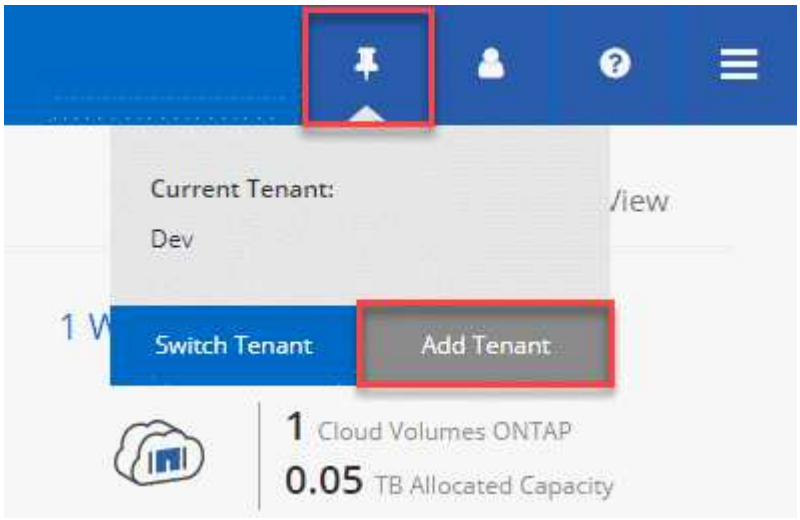
이제 Cloud Manager 시스템에 로그인할 수 있다고 알려줍니다.

테넌트 생성

테넌트를 사용하면 작업 환경을 별도의 그룹으로 격리할 수 있습니다. 테넌트 내에서 하나 이상의 작업 환경을 생성합니다. "테넌트에 대해 자세히 알아보십시오".

단계

1. 테넌트 아이콘을 클릭한 다음 * 테넌트 추가 * 를 클릭합니다.



2. 필요한 경우 이름, 설명 및 비용 센터를 입력합니다.
3. 저장 * 을 클릭합니다.

다음 단계

이제 이 새 테넌트로 전환하고 테넌트 관리자 및 작업 환경 관리자를 이 테넌트에 추가할 수 있습니다.

AWS KMS 설정

Cloud Volumes ONTAP에서 Amazon 암호화를 사용하려면 AWS KMS(키 관리 서비스)를 설정해야 합니다.

단계

1. 활성 CMK(Customer Master Key)가 있는지 확인합니다.

   CMK는 AWS로 관리되는 CMK 또는 고객이 관리하는 CMK가 될 수 있습니다. Cloud Manager 및 Cloud Volumes ONTAP와 동일한 AWS 계정 또는 다른 AWS 계정에 있을 수 있습니다.

   "AWS 설명서:CMK(Customer Master Key)"

2. Cloud Manager에 권한을 제공하는 IAM 역할을 _KEY USER_로 추가하여 각 CMK에 대한 키 정책을 수정합니다.

IAM 역할을 주요 사용자로 추가하면 Cloud Manager에서 Cloud Volumes ONTAP와 함께 CMK를 사용할 수 있는 권한이 부여됩니다.

"AWS 설명서:키 편집"

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

   a. CMK가 상주하는 계정에서 KMS 콘솔로 이동합니다.

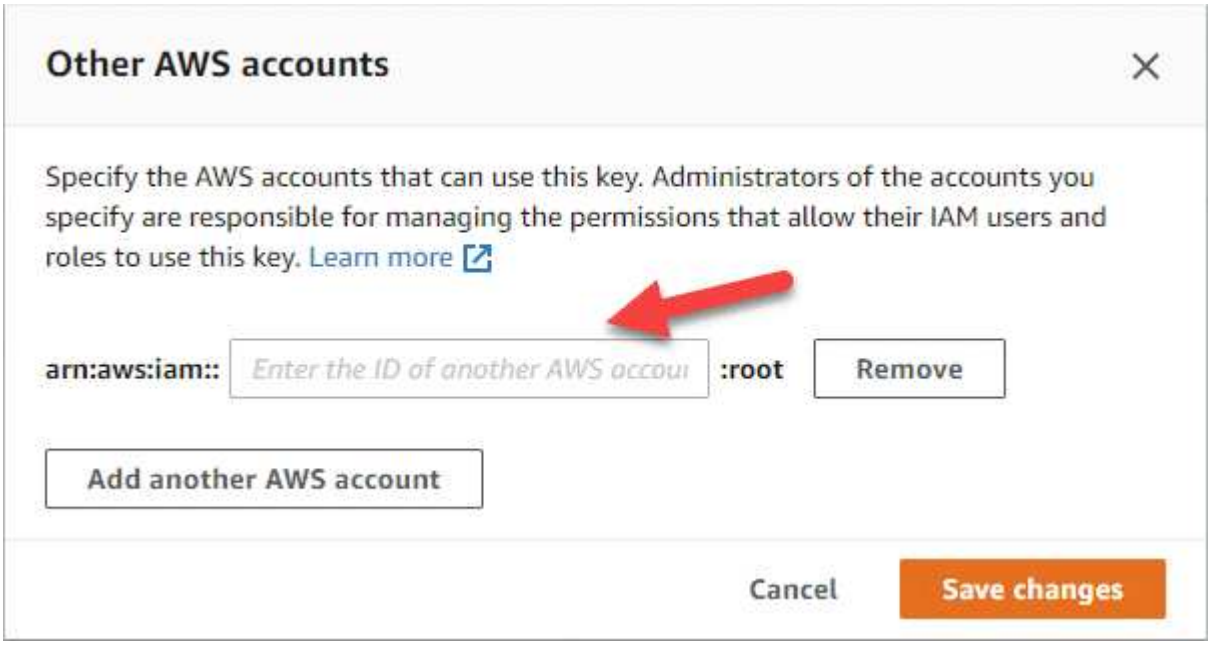
   b. 키를 선택합니다.

   c. General configuration * 창에서 키의 ARN을 복사합니다.

      Cloud Volumes ONTAP 시스템을 생성할 때 클라우드 관리자에게 ARN을 제공해야 합니다.

   d. 다른 AWS 계정 * 창에서 Cloud Manager에 사용 권한을 제공하는 AWS 계정을 추가합니다.

      대부분의 경우 Cloud Manager가 상주하는 계정입니다. Cloud Manager가 AWS에 설치되어 있지 않으면, Cloud Manager에 AWS 액세스 키를 제공한 계정이 될 수 있습니다.



   e. 이제 Cloud Manager에 사용 권한을 제공하는 AWS 계정으로 전환하고 IAM 콘솔을 엽니다.

   f. 아래에 나열된 권한을 포함하는 IAM 정책을 생성합니다.

   g. Cloud Manager에 권한을 제공하는 IAM 역할 또는 IAM 사용자에 정책을 연결합니다.

      다음 정책은 Cloud Manager가 외부 AWS 계정에서 CMK를 사용하는 데 필요한 권한을 제공합니다. "리소스"

섹션에서 지역 및 계정 ID를 수정해야 합니다.

```
{
    "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 자세한 내용은 을 참조하십시오 "AWS 설명서: CMK에 외부 AWS 계정 액세스 허용".

네트워킹 요구 사항

Cloud Manager의 네트워킹 요구사항

Cloud Manager가 AWS 또는 Microsoft Azure에 Cloud Volumes ONTAP 시스템을 구축할 수 있도록 네트워킹을 설정해야 합니다. 가장 중요한 단계는 다양한 엔드포인트에 대한 아웃바운드 인터넷 액세스를 보장하는 것입니다.

네트워크에서 인터넷에 대한 모든 통신에 프록시 서버를 사용하는 경우 Cloud Manager에서 설정 중에 프록시를 지정하라는 메시지를 표시합니다. 설정 페이지에서 프록시 서버를 지정할 수도 있습니다. 을 참조하십시오 "프록시 서버를 사용하도록 Cloud Manager 구성".

대상 네트워크에 연결

Cloud Manager를 사용하려면 Cloud Volumes ONTAP를 구축할 AWS VPC 및 Azure VNets에 대한 네트워크 연결이 필요합니다.

예를 들어, 회사 네트워크에 Cloud Manager를 설치하는 경우 Cloud Volumes ONTAP를 실행하는 AWS VPC 또는 Azure VNET에 대한 VPN 연결을 설정해야 합니다.

아웃바운드 인터넷 액세스

Cloud Manager는 Cloud Volumes ONTAP를 배포 및 관리하기 위해 아웃바운드 인터넷 액세스를 필요로 합니다. 웹 브라우저에서 Cloud Manager에 액세스하고 Linux 호스트에서 Cloud Manager 설치 프로그램을 실행할 때도 아웃바운드 인터넷 액세스가 필요합니다.

다음 섹션에서는 특정 끝점을 식별합니다.

AWS에서 Cloud Volumes ONTAP를 관리하기 위한 아웃바운드 인터넷 액세스

AWS에서 Cloud Volumes ONTAP를 구축 및 관리할 때 Cloud Manager에서 다음 엔드포인트에 액세스하려면 아웃바운드 인터넷 액세스가 필요합니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • CloudFormation 을 참조하십시오 • EC2(탄력적인 컴퓨팅 클라우드) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • S3(Simple Storage Service) 정확한 끝점은 Cloud Volumes ONTAP를 배포하는 지역에 따라 다릅니다. "자세한 내용은 AWS 설명서를 참조하십시오."	Cloud Manager를 사용하여 AWS에서 Cloud Volumes ONTAP를 구축 및 관리할 수 있습니다.
https://api.services.cloud.netapp.com:443 으로 문의하십시오	NetApp Cloud Central에 API 요청

엔드포인트	목적
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com 으로 문의하십시오	소프트웨어 이미지, 매니페스트 및 템플릿에 대한 액세스를 제공합니다.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com 으로 문의하십시오	Cloud Manager에서 매니페스트, 템플릿 및 Cloud Volumes ONTAP 업그레이드 이미지에 액세스하고 다운로드할 수 있습니다.
https://kinesis.us-east-1.amazonaws.com 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.
https://cloudmanager.cloud.netapp.com 으로 문의하십시오	Cloud Central 계정을 포함한 Cloud Manager 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com 으로 문의하십시오	NetApp Cloud Central과 통신하여 중앙 집중식 사용자 인증 제공
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup 으로 문의하십시오	NetApp AutoSupport과 커뮤니케이션:
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement 으로 문의하십시오	라이센싱 및 지원 등록에 대해 NetApp과 커뮤니케이션
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ 으로 문의하십시오	Cloud Volumes ONTAP 시스템을 Kubernetes 클러스터에 연결하는 데 필요합니다. 엔드포인트를 통해 NetApp Trident를 설치할 수 있습니다.
다음과 같은 다양한 타사 위치: • https://repo1.maven.org/maven2 으로 문의하십시오 • https://oss.sonatype.org/content/repositories 으로 문의하십시오 • https://repo.typesafe.org 으로 문의하십시오 타사 위치는 변경될 수 있습니다.	업그레이드하는 동안 Cloud Manager는 타사 종속성을 위한 최신 패키지를 다운로드합니다.

Azure에서 **Cloud Volumes ONTAP**를 관리하기 위한 아웃바운드 인터넷 액세스

Microsoft Azure에서 Cloud Volumes ONTAP를 배포 및 관리할 때 Cloud Manager는 다음 엔드포인트에 연락할 수 있는 아웃바운드 인터넷 액세스를 필요로 합니다.

엔드포인트	목적
https://management.azure.com https://login.microsoftonline.com 으로 문의하십시오	Cloud Manager를 사용하면 대부분의 Azure 지역에서 Cloud Volumes ONTAP를 구축 및 관리할 수 있습니다.
https://management.microsoftazure.de https://login.microsoftonline.de 으로 문의하십시오	Cloud Manager를 사용하여 Azure 독일 지역에서 Cloud Volumes ONTAP를 구축 및 관리할 수 있습니다.

엔드포인트	목적
https://management.usgovcloudapi.net https://login.microsoftonline.com 으로 문의하십시오	Cloud Manager를 사용하여 Azure US Gov 지역에 Cloud Volumes ONTAP를 배포하고 관리할 수 있습니다.
https://api.services.cloud.netapp.com:443 으로 문의하십시오	NetApp Cloud Central에 API 요청
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com 으로 문의하십시오	소프트웨어 이미지, 매니페스트 및 템플릿에 대한 액세스를 제공합니다.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com 를 참조하십시오	Cloud Manager에서 매니페스트, 템플릿 및 Cloud Volumes ONTAP 업그레이드 이미지에 액세스하고 다운로드할 수 있습니다.
https://kinesis.us-east-1.amazonaws.com 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.
https://netapp-cloud-account.auth0.com 으로 문의하십시오	NetApp Cloud Central과 통신하여 중앙 집중식 사용자 인증 제공
https://mysupport.netapp.com 으로 문의하십시오	NetApp AutoSupport과 커뮤니케이션:
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement 으로 문의하십시오	라이센싱 및 지원 등록에 대해 NetApp과 커뮤니케이션
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ 으로 문의하십시오	Cloud Volumes ONTAP 시스템을 Kubernetes 클러스터에 연결하는 데 필요합니다. 엔드포인트를 통해 NetApp Trident를 설치할 수 있습니다.
다음과 같은 다양한 타사 위치: • https://repo1.maven.org/maven2 으로 문의하십시오 • https://oss.sonatype.org/content/repositories 으로 문의하십시오 • https://repo.typesafe.org 으로 문의하십시오 타사 위치는 변경될 수 있습니다.	업그레이드하는 동안 Cloud Manager는 타사 종속성을 위한 최신 패키지를 다운로드합니다.

웹 브라우저에서 아웃바운드 인터넷 액세스

사용자는 웹 브라우저에서 Cloud Manager에 액세스해야 합니다. 웹 브라우저를 실행하는 컴퓨터는 다음 끝점에 연결되어 있어야 합니다.

엔드포인트	목적
Cloud Manager 호스트	Cloud Manager 콘솔을 로드하려면 웹 브라우저에서 호스트의 IP 주소를 입력해야 합니다. 클라우드 공급자에 대한 연결에 따라 호스트에 할당된 프라이빗 IP 또는 공용 IP를 사용할 수 있습니다. • 개인 IP는 VPN이 있고 가상 네트워크에 직접 연결할 수 있는 경우 작동합니다 • 공용 IP는 모든 네트워킹 시나리오에서 작동합니다 어떤 경우든 보안 그룹 규칙이 승인된 IP 또는 서브넷에서의 액세스만 허용하도록 하여 네트워크 액세스를 보호해야 합니다.
https://auth0.com\https://cdn.auth0.com\https://netapp-cloud-account.auth0.com\https://services.cloud.netapp.com	웹 브라우저는 NetApp Cloud Central을 통해 중앙 집중식 사용자 인증을 위해 이러한 엔드포인트에 연결됩니다.
https://widget.intercom.io 으로 문의하십시오	제품 내에서 NetApp 클라우드 전문가와 상담할 수 있는 채팅을 제공합니다.

Linux 호스트에 **Cloud Manager**를 설치하기 위한 아웃바운드 인터넷 액세스

설치 프로세스 중에 Cloud Manager 설치 관리자가 다음 URL에 액세스해야 합니다.

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm 으로 문의하십시오
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm 으로 문의하십시오
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip 으로 문의하십시오

포트 및 보안 그룹

- Cloud Central 또는 마켓플레이스 이미지에서 Cloud Manager를 배포하는 경우 다음을 참조하십시오.
  - "AWS의 Cloud Manager에 대한 보안 그룹 규칙"
  - "Azure의 Cloud Manager에 대한 보안 그룹 규칙"
- 기존 Linux 호스트에 Cloud Manager를 설치하는 경우 를 참조하십시오 "Cloud Manager 호스트 요구사항".

AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항

Cloud Volumes ONTAP 시스템이 올바르게 작동할 수 있도록 AWS 네트워킹을 설정합니다.

Cloud Manager에 액세스해야 하는 엔드포인트 목록을 찾고 계십니까? 이제 단일 위치에서 유지 관리됩니다. "자세한 내용을 보려면 여기를 클릭하십시오".

Cloud Volumes ONTAP의 일반적인 AWS 네트워킹 요구사항

AWS에서 다음 요구사항을 충족해야 합니다.

Cloud Volumes ONTAP 노드에 대한 아웃바운드 인터넷 액세스

Cloud Volumes ONTAP 노드를 사용하려면 스토리지 상태를 사전에 모니터링하는 NetApp AutoSupport에 메시지를 보내기 위해 아웃바운드 인터넷 액세스가 필요합니다.

라우팅 및 방화벽 정책은 Cloud Volumes ONTAP가 AutoSupport 메시지를 전송할 수 있도록 다음 엔드포인트로 AWS HTTP/HTTPS 트래픽을 허용해야 합니다.

- https://support.netapp.com/aods/asupmessage 으로 문의하십시오
- https://support.netapp.com/asupprod/post/1.0/postAsup 으로 문의하십시오

NAT 인스턴스가 있는 경우 개인 서브넷에서 인터넷으로 HTTPS 트래픽을 허용하는 인바운드 보안 그룹 규칙을 정의해야 합니다.

HA 중재자를 위한 아웃바운드 인터넷 액세스

HA 중재자 인스턴스는 스토리지 페일오버를 지원할 수 있도록 AWS EC2 서비스에 대한 아웃바운드 연결이 있어야 합니다. 연결을 제공하기 위해 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 엔드포인트일 수 있습니다. VPC 엔드포인트에 대한 자세한 내용은 을 참조하십시오 "AWS 문서:인터페이스 VPC 엔드포인트(AWS PrivateLink)".

보안 그룹

Cloud Manager에서 보안 그룹을 생성할 수 있으므로 보안 그룹을 생성할 필요가 없습니다. 직접 사용해야 하는 경우 을 참조하십시오 "보안 그룹 규칙".

데이터 계층화를 위해 Cloud Volumes ONTAP에서 AWS S3로 연결

EBS를 성능 계층으로 사용하고 AWS S3를 용량 계층으로 사용하려면 Cloud Volumes ONTAP이 S3에 연결되어 있는지 확인해야 합니다. 이 연결을 제공하는 가장 좋은 방법은 S3 서비스에 VPC 엔드포인트를 생성하는 것입니다. 자세한 내용은 을 참조하십시오 "AWS 설명서: 게이트웨이 엔드포인트 생성".

VPC 끝점을 만들 때 Cloud Volumes ONTAP 인스턴스에 해당하는 영역, VPC 및 라우팅 테이블을 선택해야 합니다. 또한 S3 엔드포인트에 대한 트래픽을 활성화하는 아웃바운드 HTTPS 규칙을 추가하려면 보안 그룹을 수정해야 합니다. 그렇지 않으면 Cloud Volumes ONTAP에서 S3 서비스에 연결할 수 없습니다.

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

다른 네트워크의 ONTAP 시스템에 대한 연결

AWS의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 AWS VPC와 다른 네트워크(예: Azure VNET 또는 회사 네트워크) 간에 VPN 연결이 있어야 합니다. 자세한 내용은 을 참조하십시오 "AWS 설명서: AWS VPN 연결 설정".

CIFS용 DNS 및 Active Directory

CIFS 스토리지를 프로비저닝하려면 AWS에서 DNS 및 Active Directory를 설정하거나 사내 설정을 AWS로 확장해야 합니다.

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

자세한 지침은 을 참조하십시오 "AWS 설명서: AWS 클라우드의 Active Directory 도메인 서비스 빠른 시작 참조 구축".

여러 **AZs**에서 **Cloud Volumes ONTAP HA**를 위한 **AWS** 네트워킹 요구사항

추가 AWS 네트워킹 요구사항은 ZS(Multiple Availability Zones)를 사용하는 Cloud Volumes ONTAP HA 구성에 적용됩니다. Cloud Manager에 네트워킹 세부 정보를 입력해야 하므로 HA 쌍을 실행하기 전에 이러한 요구사항을 검토해야 합니다.

HA 쌍의 작동 방식을 이해하려면 를 참조하십시오 "고가용성 쌍".

가용성 영역

이 HA 구축 모델은 여러 대의 AZs를 사용하여 데이터의 고가용성을 보장합니다. 각 Cloud Volumes ONTAP 인스턴스와 중재자 인스턴스에 전용 AZ를 사용해야 하며 HA 쌍 간의 통신 채널을 제공합니다.

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

여러 AZs의 HA 구성에서는 장애가 발생할 경우 노드 간에 이동하는 부동 IP 주소를 사용합니다. 고객이 아니라면 VPC 외부에서 기본적으로 액세스할 수 없습니다 "AWS 전송 게이트웨이를 설정합니다".

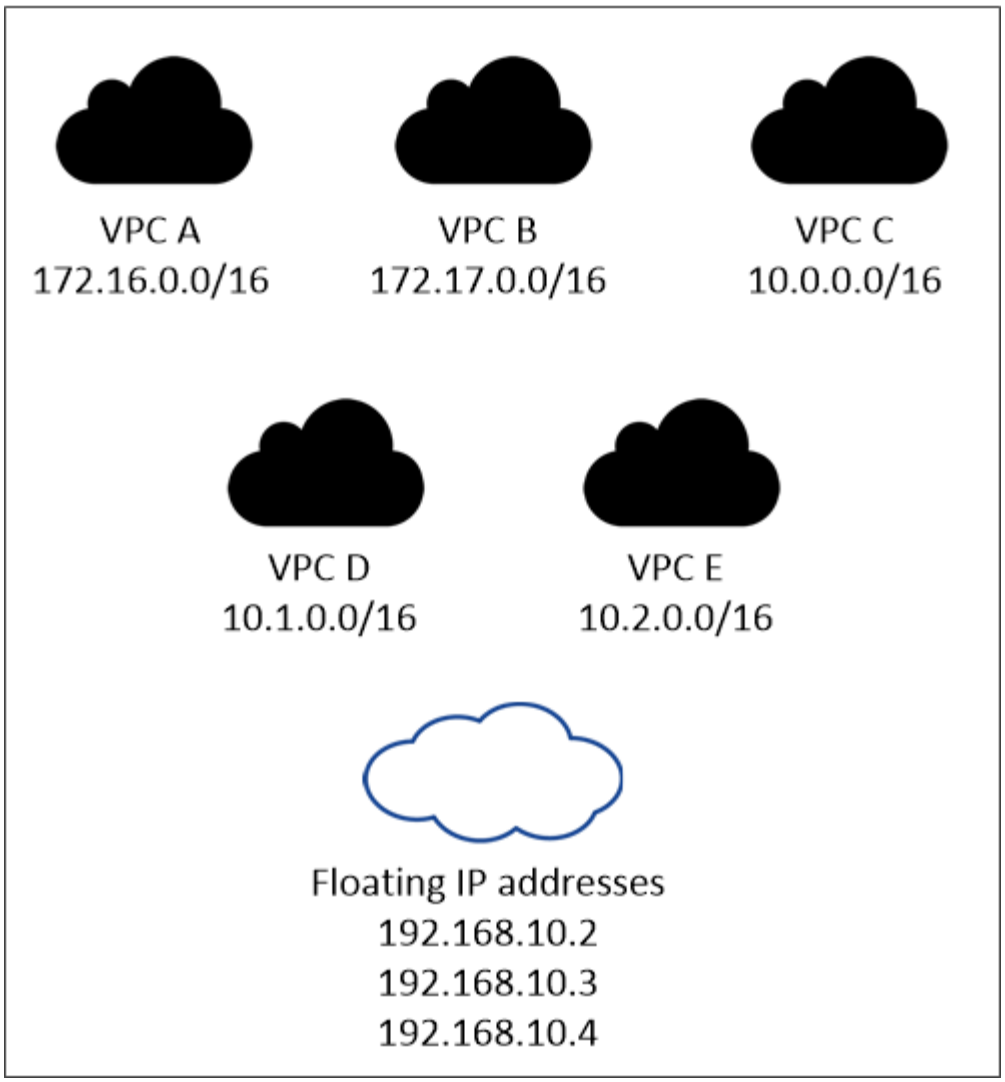
하나의 부동 IP 주소는 클러스터 관리용, 하나는 노드 1의 NFS/CIFS 데이터용으로, 다른 하나는 노드 2의 NFS/CIFS 데이터용으로 사용됩니다. SVM 관리를 위한 네 번째 유동 IP 주소는 선택 사항입니다.

Windows용 SnapDrive 또는 HA 쌍을 지원하는 SnapCenter를 사용하는 경우 SVM 관리 LIF에는 부동 IP 주소가 필요합니다. 시스템을 구축할 때 IP 주소를 지정하지 않으면 나중에 LIF를 생성할 수 있습니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP 설정".

Cloud Volumes ONTAP HA 작업 환경을 생성할 때 Cloud Manager에 부동 IP 주소를 입력해야 합니다. Cloud Manager는 시스템을 시작할 때 HA 쌍에 IP 주소를 할당합니다.

부동 IP 주소는 HA 구성을 배포하는 AWS 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 유동 IP 주소를 해당 지역의 VPC 외부에 있는 논리적 서브넷으로 생각해 보십시오.

다음 예에서는 AWS 영역에 있는 VPC와 유동 IP 주소 간의 관계를 보여 줍니다. 부동 IP 주소는 모든 VPC에 대한 CIDR 블록 외부에 있지만 라우팅 테이블을 통해 서브넷으로 라우팅할 수 있습니다.



Cloud Manager는 VPC 외부의 클라이언트에서 iSCSI 액세스 및 NAS 액세스를 위한 정적 IP 주소를 자동으로 생성합니다. 이러한 유형의 IP 주소에 대한 요구 사항을 충족할 필요는 없습니다.

VPC 외부에서 유동 **IP** 액세스를 지원하는 전송 게이트웨이

"AWS 전송 게이트웨이를 설정합니다" HA 쌍이 상주하는 VPC 외부에서 HA 쌍의 부동 IP 주소에 액세스할 수 있도록 합니다.

배관 테이블

Cloud Manager에서 부동 IP 주소를 지정한 후 부동 IP 주소에 대한 라우트를 포함해야 하는 라우팅 테이블을 선택해야 합니다. 이렇게 하면 클라이언트가 HA 쌍에 액세스할 수 있습니다.

VPC(기본 경로 테이블)에 있는 서브넷에 대해 하나의 라우팅 테이블만 있는 경우 Cloud Manager는 해당 라우팅 테이블에 부동 IP 주소를 자동으로 추가합니다. 둘 이상의 라우트 테이블이 있는 경우 HA 쌍을 시작할 때 올바른 라우트 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP에 액세스하지 못할 수 있습니다.

예를 들어, 서로 다른 라우팅 테이블에 연결된 두 개의 서브넷이 있을 수 있습니다. 라우트 테이블 A를 선택했지만 라우트 테이블 B는 선택하지 않은 경우, 라우트 테이블 A와 연결된 서브넷에 있는 클라이언트는 HA 쌍에 액세스할 수 있지만, 라우트 테이블 B와 연결된 서브넷에 있는 클라이언트는 액세스할 수 없습니다.

라우팅 테이블에 대한 자세한 내용은 을 참조하십시오 "AWS 설명서: 경로 테이블".

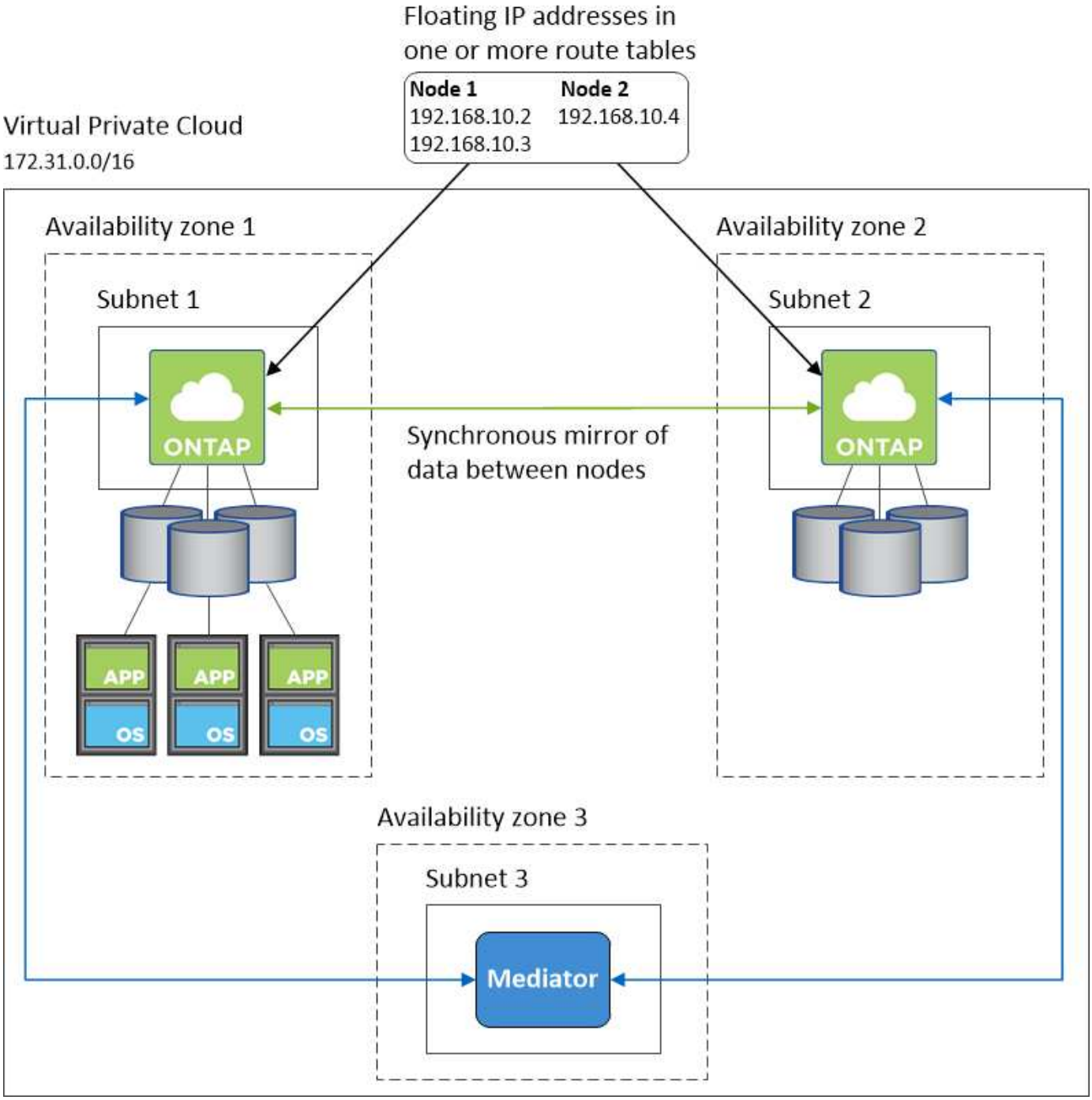
NetApp 관리 툴에 연결

여러 AZs에 있는 HA 구성에서 NetApp 관리 툴을 사용하려면 다음 두 가지 연결 옵션을 사용할 수 있습니다.

1. NetApp 관리 툴을 다른 VPC 및 에 구축할 수 있습니다 "AWS 전송 게이트웨이를 설정합니다". 게이트웨이를 사용하면 VPC 외부에서 클러스터 관리 인터페이스의 부동 IP 주소에 액세스할 수 있습니다.
2. NAS 클라이언트와 비슷한 라우팅 구성을 사용하여 동일한 VPC에 NetApp 관리 툴을 구축합니다.

구성의 예

다음 이미지는 액티브-패시브 구성으로 작동하는 AWS의 최적의 HA 구성을 보여줍니다.



VPC 구성의 예

AWS에서 Cloud Manager 및 Cloud Volumes ONTAP를 구축하는 방법을 자세히 알아보려면 가장 일반적인 VPC 구성을 검토해야 합니다.

- 공용 및 전용 서브넷과 NAT 장치가 있는 VPC입니다
- 개인 서브넷과 네트워크에 대한 VPN 연결을 지원하는 VPC입니다

공용 및 전용 서브넷과 **NAT** 장치가 있는 **VPC**입니다

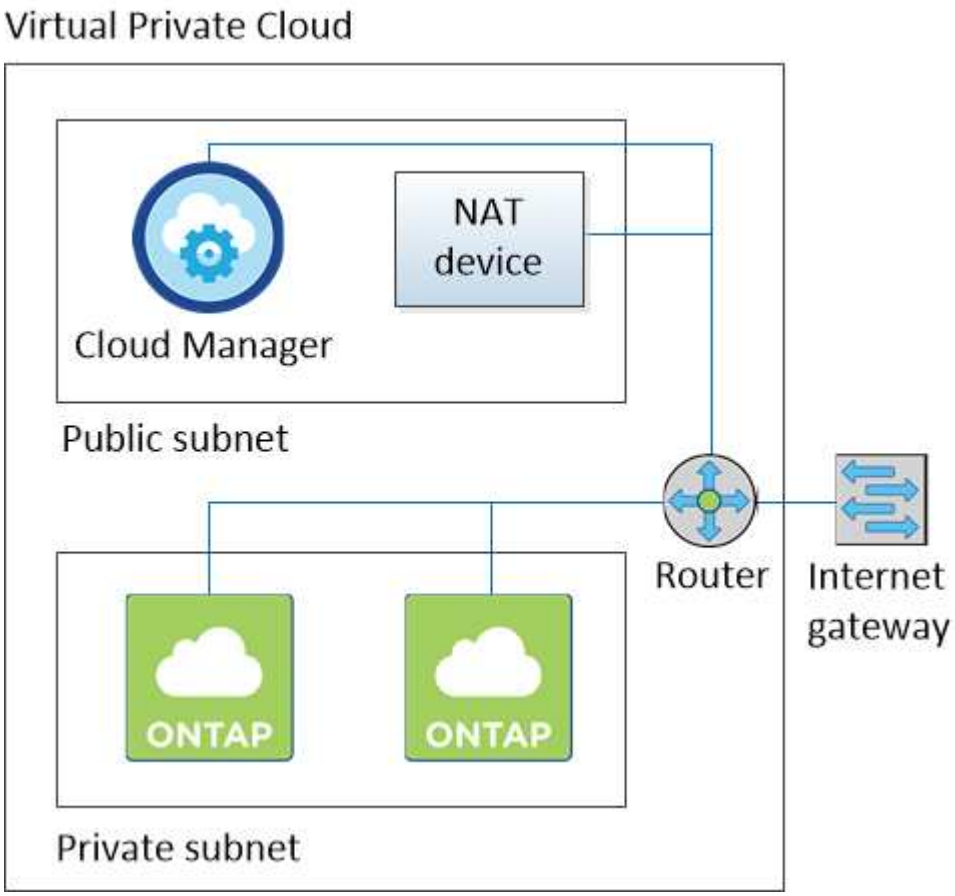
이 VPC 구성에는 공용 및 전용 서브넷, VPC를 인터넷에 연결하는 인터넷 게이트웨이, 사설 서브넷의 아웃바운드 인터넷 트래픽을 지원하는 공용 서브넷의 NAT 게이트웨이 또는 NAT 인스턴스가 포함됩니다. 이 구성에서는 퍼블릭

서브넷 또는 프라이빗 서브넷에서 Cloud Manager를 실행할 수 있지만, VPC 외부의 호스트에서 액세스할 수 있기 때문에 퍼블릭 서브넷을 사용하는 것이 좋습니다. 그런 다음 전용 서브넷에서 Cloud Volumes ONTAP 인스턴스를 시작할 수 있습니다.

NAT 장치 대신 HTTP 프록시를 사용하여 인터넷 연결을 제공할 수 있습니다.

이 시나리오에 대한 자세한 내용은 을 참조하십시오 "AWS 문서:시나리오 2: 공용 및 사설 서브넷(NAT)이 있는 VPC".

다음 그림에서는 공용 서브넷에서 실행되는 Cloud Manager와 프라이빗 서브넷에서 실행되는 단일 노드 시스템을 보여 줍니다.



개인 서브넷과 네트워크에 대한 **VPN** 연결을 지원하는 **VPC**입니다

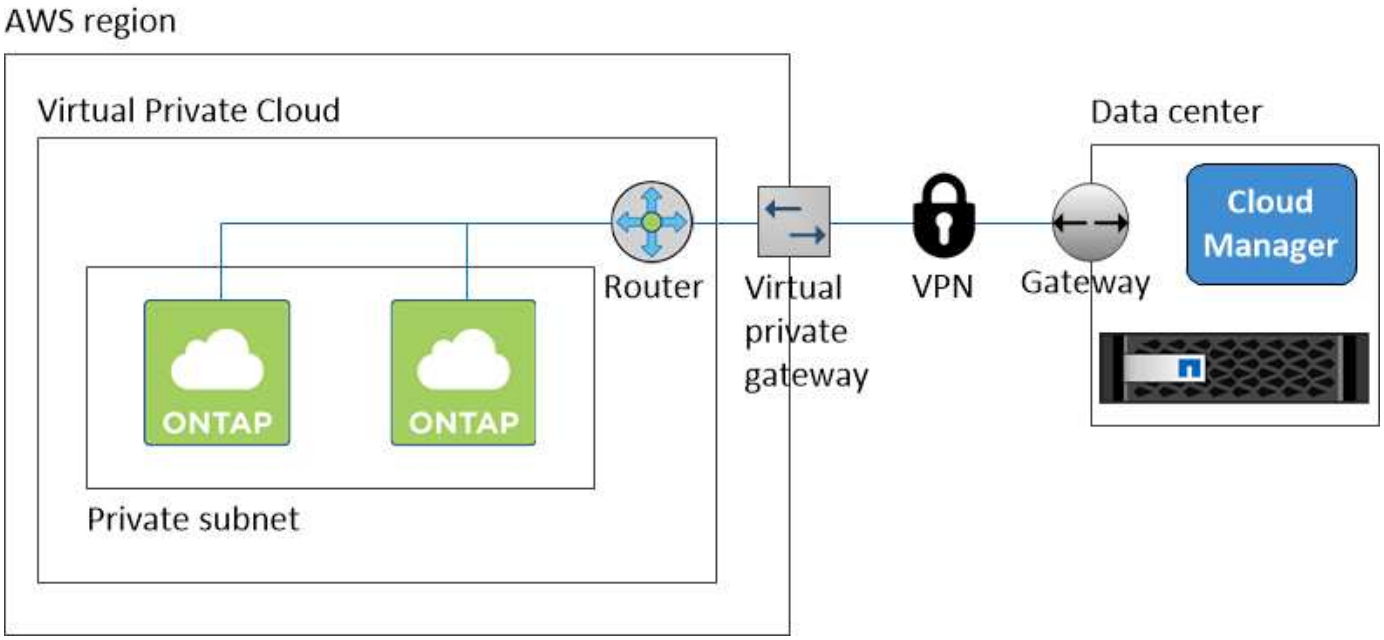
이 VPC 구성은 Cloud Volumes ONTAP가 프라이빗 환경의 확장이 되는 하이브리드 클라우드 구성입니다. 이 구성에는 네트워크에 대한 VPN 연결이 있는 전용 서브넷 및 가상 전용 게이트웨이가 포함됩니다. VPN 터널을 통해 라우팅하면 EC2 인스턴스가 네트워크 및 방화벽을 통해 인터넷에 액세스할 수 있습니다. 프라이빗 서브넷 또는 데이터 센터에서 Cloud Manager를 실행할 수 있습니다. 그런 다음 개인 서브넷에서 Cloud Volumes ONTAP를 실행합니다.

이 구성에서 프록시 서버를 사용하여 인터넷 액세스를 허용할 수도 있습니다. 프록시 서버는 데이터 센터 또는 AWS에 있을 수 있습니다.

데이터 센터의 FAS 시스템과 AWS의 Cloud Volumes ONTAP 시스템 간에 데이터를 복제하려면 링크가 안전하도록 VPN 연결을 사용해야 합니다.

이 시나리오에 대한 자세한 내용은 을 참조하십시오 "AWS 문서: 시나리오 4: 전용 서브넷만 있는 VPC 및 AWS 관리형 VPN 액세스".

다음 그래픽은 데이터 센터에서 실행되는 Cloud Manager와 프라이빗 서브넷에서 실행되는 단일 노드 시스템을 보여 줍니다.



여러 **AZs**에서 **HA** 쌍에 대한 **AWS** 전송 게이트웨이 설정

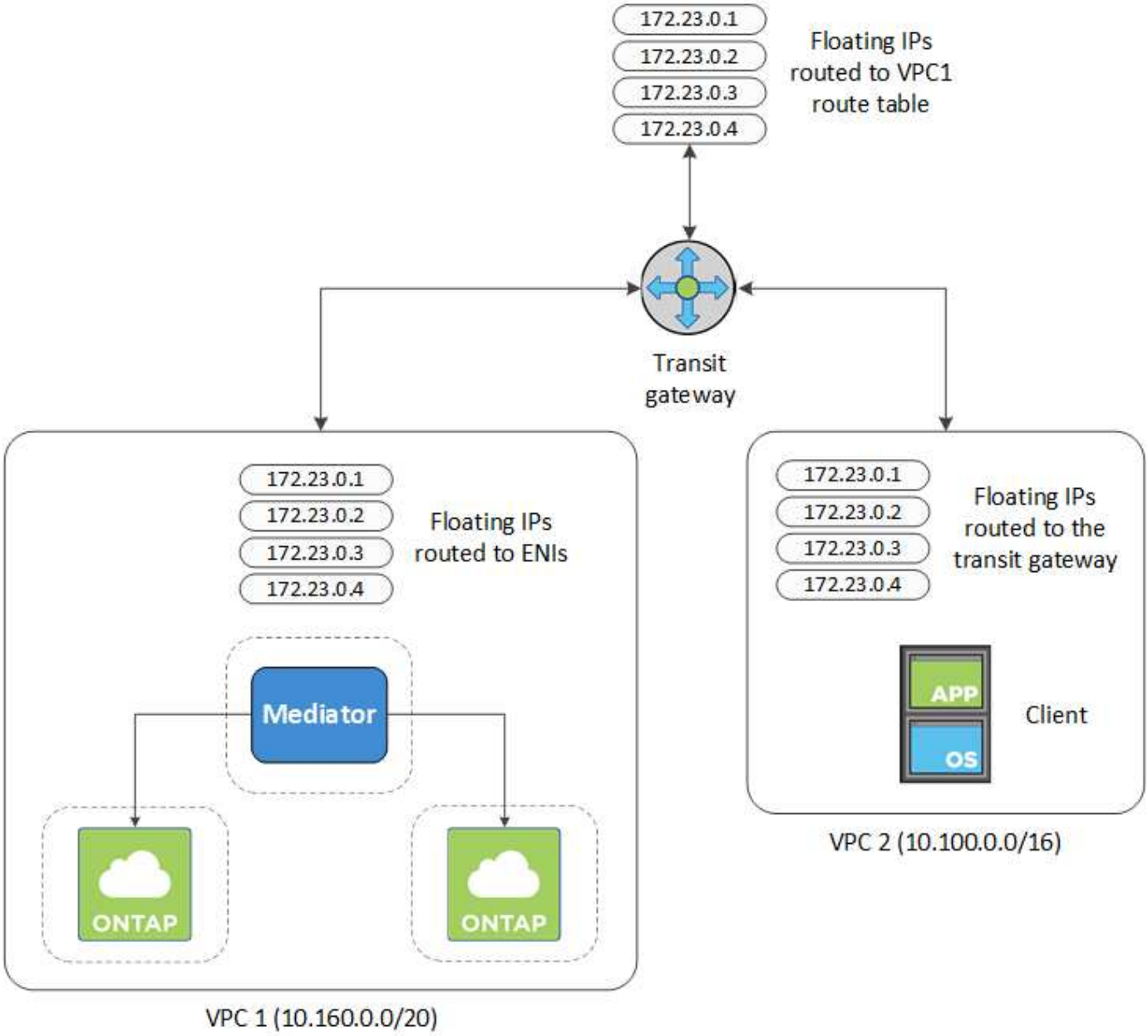
HA 쌍이 상주하는 VPC 외부에서 HA 쌍의 부동 IP 주소에 액세스할 수 있도록 AWS 전송 게이트웨이를 설정합니다.

Cloud Volumes ONTAP HA 구성이 여러 AWS 가용성 영역에 분산되면 VPC 내에서 NAS 데이터 액세스에 유동 IP 주소가 필요합니다. 이러한 부동 IP 주소는 장애가 발생할 때 노드 간에 마이그레이션할 수 있지만 VPC 외부에서 기본적으로 액세스할 수 없습니다. 별도의 프라이빗 IP 주소를 통해 VPC 외부에서 데이터에 액세스할 수 있지만 자동 페일오버를 제공하지 않습니다.

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

AWS 전송 게이트웨이를 설정한 경우 HA 쌍이 상주하는 VPC 외부의 유동 IP 주소에 액세스할 수 있습니다. 즉, VPC 외부에 있는 NAS 클라이언트와 NetApp 관리 툴이 유동 IP에 액세스할 수 있습니다.

다음은 전송 게이트웨이에 의해 연결된 두 대의 VPC를 보여 주는 예입니다. HA 시스템은 VPC 하나에 상주하고 클라이언트는 다른 VPC에 상주합니다. 그런 다음 부동 IP 주소를 사용하여 클라이언트에 NAS 볼륨을 마운트할 수 있습니다.

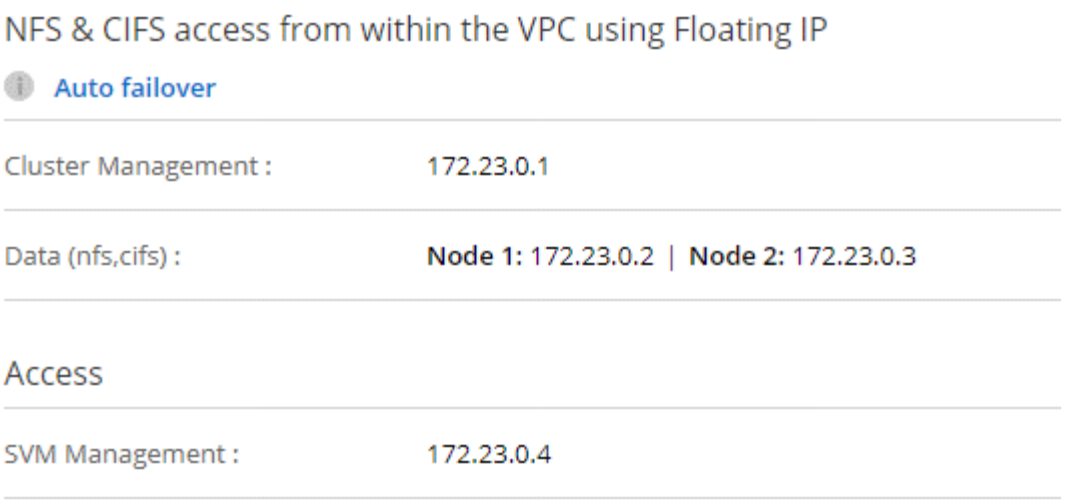


다음 단계에서는 유사한 구성을 설정하는 방법을 보여 줍니다.

단계

1. "전송 게이트웨이를 만들고 VPC를 게이트웨이에 연결합니다".
2. HA 쌍의 부동 IP 주소를 지정하여 전송 게이트웨이의 라우팅 테이블에서 경로를 만듭니다.

   Cloud Manager의 작업 환경 정보 페이지에서 부동 IP 주소를 찾을 수 있습니다. 예를 들면 다음과 같습니다.



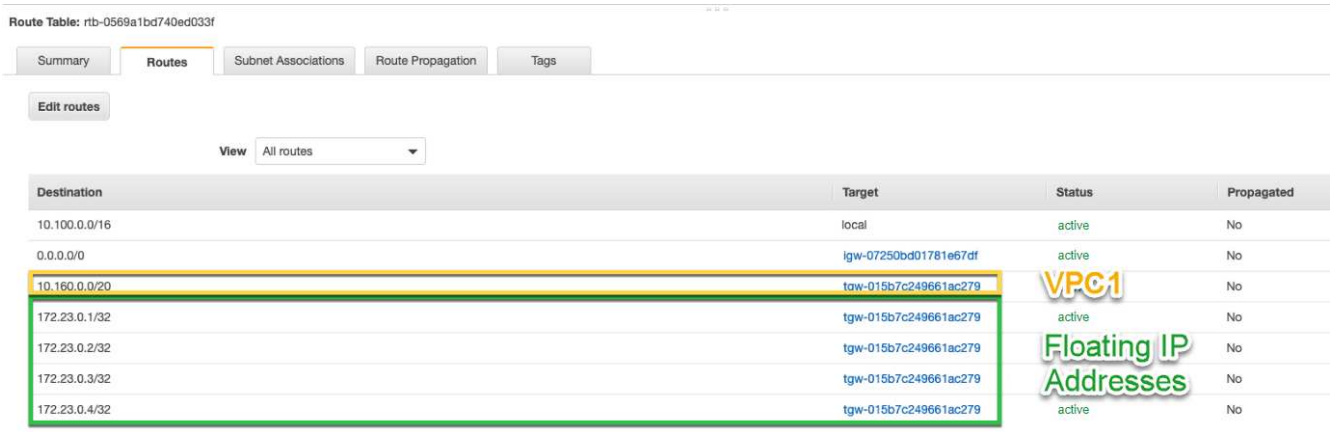
다음 샘플 이미지는 전송 게이트웨이의 라우트 테이블을 보여 줍니다. 여기에는 2개의 VPC의 CIDR 블록에 대한 경로와 Cloud Volumes ONTAP에서 사용하는 4개의 부동 IP 주소가 포함됩니다.

3. 부동 IP 주소에 액세스해야 하는 VPC의 라우팅 테이블을 수정합니다.

   a. 부동 IP 주소에 라우트 항목을 추가합니다.

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

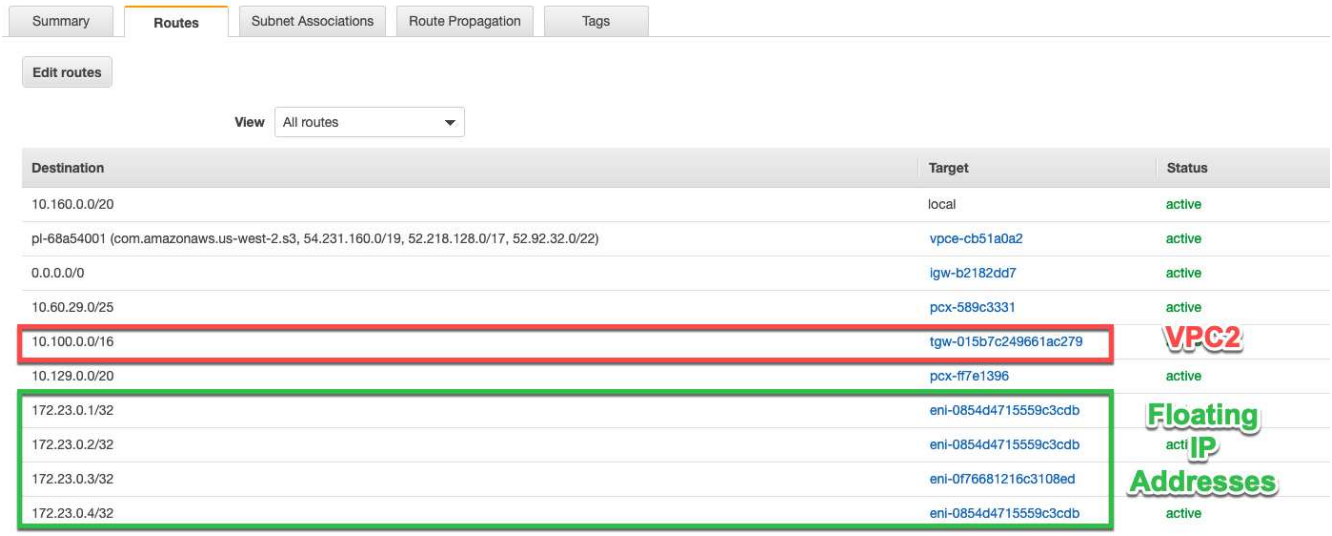
      다음 샘플 이미지는 VPC 1에 대한 라우트 및 부동 IP 주소를 포함하는 VPC 2용 라우팅 테이블을 보여 줍니다.



4. 유동 IP 주소에 액세스해야 하는 VPC에 경로를 추가하여 HA 쌍 VPC의 경로 테이블을 수정합니다.

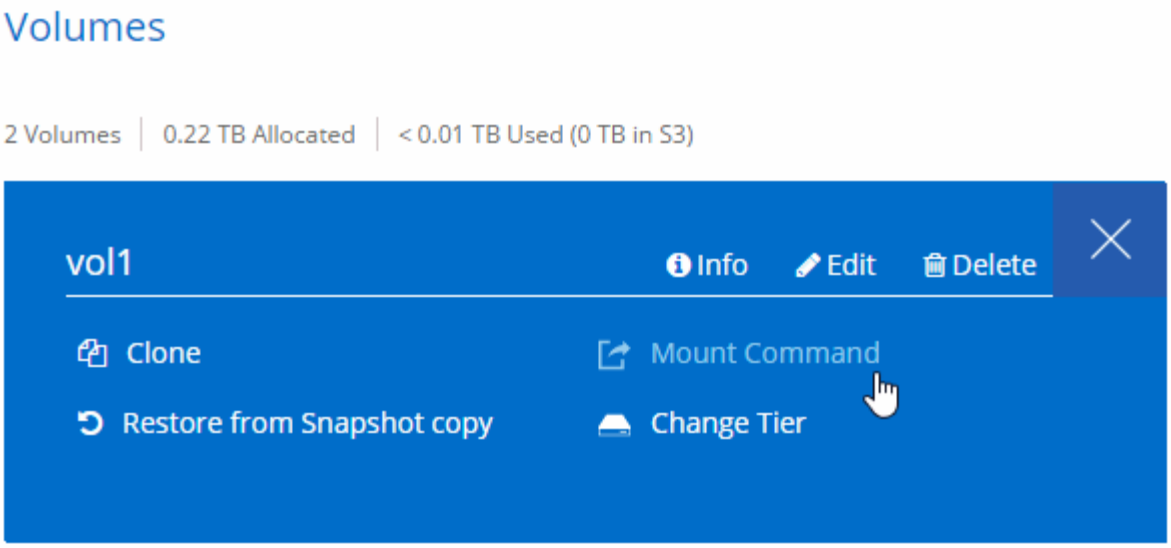
   이 단계는 VPC 간 라우팅을 완료하기 때문에 중요합니다.

   다음 샘플 이미지는 VPC 1의 라우트 테이블을 보여 줍니다. 여기에는 부동 IP 주소 및 클라이언트가 있는 VPC 2로의 라우트가 포함됩니다. Cloud Manager에서 HA 쌍을 구축하면 라우팅 테이블에 유동 IP가 자동으로 추가됩니다.



5. 부동 IP 주소를 사용하여 클라이언트에 볼륨을 마운트합니다.

   볼륨을 선택하고 * 탑재 명령 * 을 클릭하여 Cloud Manager에서 올바른 IP 주소를 찾을 수 있습니다.



◦ 관련 링크 *

◦ "AWS의 고가용성 쌍"

◦ "AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항"

Azure의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항

Cloud Volumes ONTAP 시스템이 올바르게 작동할 수 있도록 Azure 네트워킹을 설정해야 합니다.

Cloud Manager에 액세스해야 하는 엔드포인트 목록을 찾고 계십니까? 이제 단일 위치에서 유지 관리됩니다. "자세한 내용을 보려면 여기를 클릭하십시오".

Cloud Volumes ONTAP에 대한 아웃바운드 인터넷 액세스

Cloud Volumes ONTAP에서 스토리지 상태를 능동적으로 모니터링하는 NetApp AutoSupport에 메시지를 보내려면 아웃바운드 인터넷 액세스가 필요합니다.

라우팅 및 방화벽 정책은 Cloud Volumes ONTAP가 AutoSupport 메시지를 전송할 수 있도록 다음 엔드포인트로 AWS HTTP/HTTPS 트래픽을 허용해야 합니다.

- https://support.netapp.com/aods/asupmessage 으로 문의하십시오
- https://support.netapp.com/asupprod/post/1.0/postAsup 으로 문의하십시오

보안 그룹

Cloud Manager에서 보안 그룹을 생성할 수 있으므로 보안 그룹을 생성할 필요가 없습니다. 직접 사용해야 하는 경우 을 참조하십시오 "보안 그룹 규칙".

데이터 계층화를 위해 **Cloud Volumes ONTAP**에서 **Azure Blob** 저장소로 연결

콜드 데이터를 Azure Blob 저장소에 계층화하려는 경우 Cloud Manager에 필요한 권한이 있는 한 VNET 서비스 엔드포인트를 설정할 필요가 없습니다.

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

이러한 권한은 최신 에 포함되어 있습니다 "Cloud Manager 정책".

데이터 계층화 설정에 대한 자세한 내용은 을 참조하십시오 "콜드 데이터를 저비용 오브젝트 스토리지로 계층화".

다른 네트워크의 **ONTAP** 시스템에 대한 연결

Azure의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 Azure VNET와 다른 네트워크(예: AWS VPC 또는 기업 네트워크) 간에 VPN 연결이 있어야 합니다.

자세한 지침은 을 참조하십시오 "Microsoft Azure 문서: Azure 포털에서 사이트 간 연결을 만듭니다".

추가 구축 옵션

Cloud Manager 호스트 요구사항

자체 호스트에 Cloud Manager를 설치하는 경우 운영 체제 요구사항, 포트 요구사항 등이 포함된 구성에 대한 지원을 확인해야 합니다.

지원되는 **AWS EC2** 인스턴스 유형

T3.MEDIUM(권장), T2.MEDIUM 및 M4.Large

지원되는 **Azure VM** 크기입니다

A2, D2 v2 또는 D2 v3(가용성 기준)

지원되는 운영 체제

- CentOS 7.2
- CentOS 7.3
- CentOS 7.4
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4

  Red Hat Enterprise Linux 시스템은 Red Hat 서브스크립션 관리 에 등록되어 있어야 합니다. 등록되지 않은 경우 시스템은 Cloud Manager 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.

  Cloud Manager는 이러한 운영 체제의 영어 버전에서 지원됩니다.

하이퍼바이저

CentOS 또는 Red Hat Enterprise Linux 실행 인증을 받은 베어 메탈 또는 호스팅된 하이퍼바이저https://access.redhat.com/certified-hypervisors["Red Hat 솔루션: Red Hat Enterprise Linux 실행 인증을 받은 하이퍼바이저는 무엇입니까?"^]

CPU

코어 2개가 있는 경우 2.27GHz 이상

RAM

4GB

사용 가능한 디스크 공간

50GB

아웃바운드 인터넷 액세스

Cloud Manager를 설치할 때와 Cloud Manager를 사용하여 Cloud Volumes ONTAP를 구축할 때는 아웃바운드 인터넷 액세스가 필요합니다. 끝점 목록은 을 참조하십시오 "Cloud Manager의 네트워킹 요구사항".

포트

다음 포트를 사용할 수 있어야 합니다.

- HTTP 액세스용 80
- HTTPS 액세스용 443
- Cloud Manager 데이터베이스용 3306
- Cloud Manager API 프록시의 경우 8080

다른 서비스에서 이러한 포트를 사용하는 경우 Cloud Manager 설치가 실패합니다.

포트 3306과 충돌할 가능성이 있습니다. MySQL의 다른 인스턴스가 호스트에서 실행 중인 경우 기본적으로 포트 3306을 사용합니다. 기존 MySQL 인스턴스가 사용하는 포트를 변경해야 합니다.

Cloud Manager를 설치할 때 기본 HTTP 및 HTTPS 포트를 변경할 수 있습니다. MySQL 데이터베이스의 기본 포트는 변경할 수 없습니다. HTTP 및 HTTPS 포트를 변경하는 경우 사용자가 원격 호스트에서 Cloud Manager 웹 콘솔에 액세스할 수 있는지 확인해야 합니다.

- 포트를 통한 인바운드 연결을 허용하도록 보안 그룹을 수정합니다.
- Cloud Manager 웹 콘솔에 대한 URL을 입력할 때 포트를 지정합니다.

기존 **Linux** 호스트에 **Cloud Manager** 설치

Cloud Manager를 구축하는 가장 일반적인 방법은 Cloud Central 또는 클라우드 공급자의 마켓플레이스에서 구축하는 것입니다. 네트워크 또는 클라우드의 기존 Linux 호스트에 Cloud Manager 소프트웨어를 다운로드하고 설치할 수 있습니다.

시작하기 전에

- Red Hat Enterprise Linux 시스템은 Red Hat 서브스크립션 관리 에 등록되어 있어야 합니다. 등록되지 않은 경우 시스템은 Cloud Manager 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.
- Cloud Manager 설치 프로그램은 설치 프로세스 중에 여러 URL에 액세스합니다. 이러한 엔드포인트에 아웃바운드 인터넷 액세스가 허용되는지 확인해야 합니다. 을 참조하십시오 "Cloud Manager의 네트워킹 요구사항".

이 작업에 대해

- Cloud Manager를 설치하는 데 루트 권한이 필요하지 않습니다.
- Cloud Manager는 AWS 명령줄 툴(awscli)을 설치하여 NetApp 지원으로부터 복구 절차를 지원합니다.

  awscli 설치에 실패했다는 메시지가 표시되면 메시지를 무시해도 됩니다. Cloud Manager는 툴 없이 성공적으로 운영될 수 있습니다.

- NetApp Support 사이트에서 제공되는 설치 프로그램은 이전 버전일 수 있습니다. 새 버전을 사용할 수 있는 경우 설치 후 Cloud Manager가 자동으로 업데이트됩니다.

단계

1. 네트워킹 요구 사항 검토:
   - "Cloud Manager의 네트워킹 요구사항"
   - "Cloud Volumes ONTAP for AWS의 네트워킹 요구사항"
   - "Azure용 Cloud Volumes ONTAP의 네트워킹 요구사항"
2. 검토 "Cloud Manager 호스트 요구사항".
3. 에서 소프트웨어를 다운로드합니다 "NetApp Support 사이트"를 선택한 다음 Linux 호스트에 복사합니다.

   AWS에서 EC2 인스턴스에 파일을 연결하고 복사하는 방법은 를 참조하십시오 "AWS 설명서: SSH를 사용하여 Linux 인스턴스에 연결".

4. 스크립트를 실행할 권한을 할당합니다.
   - 예 *

   ```
   chmod +x OnCommandCloudManager-V3.6.3.sh
   . 설치 스크립트를 실행합니다.
   ```

   ```
   ./OnCommandCloudManager-V3.6.3.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   _silent_는 정보를 묻지 않고 설치를 실행합니다.

   Cloud Manager 호스트가 프록시 서버 뒤에 있으면 _proxy_가 필요합니다.

   _proxyPort_는 프록시 서버의 포트입니다.

   _proxyuser_는 기본 인증이 필요한 경우 프록시 서버의 사용자 이름입니다.

   _proxypwd_는 지정한 사용자 이름의 암호입니다.

5. silent 매개 변수를 지정하지 않은 경우 스크립트를 계속하려면 * Y * 를 입력하고 메시지가 표시되면 HTTP 및 HTTPS 포트를 입력합니다.

   HTTP 및 HTTPS 포트를 변경하는 경우 사용자가 원격 호스트에서 Cloud Manager 웹 콘솔에 액세스할 수 있는지 확인해야 합니다.

◦ 포트를 통한 인바운드 연결을 허용하도록 보안 그룹을 수정합니다.

◦ Cloud Manager 웹 콘솔에 대한 URL을 입력할 때 포트를 지정합니다.

이제 Cloud Manager가 설치되었습니다. 설치가 끝나면 프록시 서버를 지정한 경우 occm(Cloud Manager) 서비스가 두 번 다시 시작됩니다.

6. 웹 브라우저를 열고 다음 URL을 입력합니다.

https://ipaddress:port

_ipaddress_는 Cloud Manager 호스트 구성에 따라 localhost, 전용 IP 주소 또는 공용 IP 주소일 수 있습니다. 예를 들어, Cloud Manager가 퍼블릭 IP 주소 없이 퍼블릭 클라우드에 있는 경우 Cloud Manager 호스트에 대한 연결이 있는 호스트의 프라이빗 IP 주소를 입력해야 합니다.

기본 HTTP(80) 또는 HTTPS(443) 포트를 변경한 경우 port_가 필요합니다. 예를 들어, HTTPS 포트가 8443으로 변경된 경우 를 입력합니다 https://_ipaddress:8443

7. NetApp Cloud Central 계정에 가입하거나 이미 가지고 있는 경우 로그인하십시오.
8. 등록 또는 로그인하면 Cloud Manager에서 자동으로 사용자 계정을 이 시스템의 관리자로 추가합니다.
9. 로그인한 후 이 Cloud Manager 시스템의 이름을 입력합니다.

작업을 마친 후

Cloud Manager에서 Cloud Volumes ONTAP를 구축할 수 있도록 AWS 및 Azure 계정에 대한 권한 설정:

- AWS에 Cloud Volumes ONTAP를 구축하려는 경우, "AWS 계정을 설정한 다음 Cloud Manager에 추가합니다".
- Azure에서 Cloud Volumes ONTAP를 배포하려는 경우 "Azure 계정을 설정한 다음 Cloud Manager에 추가합니다".

AWS Marketplace에서 Cloud Manager 시작

AWS에서 Cloud Manager를 시작하는 것이 가장 좋습니다 "NetApp Cloud Central에서"하지만 필요한 경우 AWS Marketplace에서 시작할 수 있습니다.

AWS 마켓플레이스에서 Cloud Manager를 시작하면 Cloud Manager가 NetApp Cloud Central과 통합됩니다. "통합에 대해 자세히 알아보십시오".

이 작업에 대해

다음 단계에서는 콘솔에서 IAM 역할을 Cloud Manager 인스턴스에 연결할 수 있으므로 EC2 콘솔에서 인스턴스를 시작하는 방법을 설명합니다. 1-클릭 옵션은 사용할 수 없습니다.

단계

1. EC2 인스턴스에 대해 IAM 정책 및 역할을 생성합니다.
   a. 다음 위치에서 Cloud Manager IAM 정책을 다운로드합니다.

      "NetApp OnCommand 클라우드 관리자: AWS 및 Azure 정책"

b. IAM 콘솔에서 Cloud Manager IAM 정책의 텍스트를 복사하여 붙여넣어 고유한 정책을 생성합니다.

c. Amazon EC2 역할 유형으로 IAM 역할을 생성하고 이전 단계에서 생성한 정책을 역할에 연결합니다.

2. 로 이동합니다 "Cloud Manager 페이지로 이동하여 AWS 마켓플레이스를 확인하십시오".
3. 계속 * 을 클릭합니다.
4. 사용자 지정 시작 탭에서 해당 지역의 * EC2 콘솔 * 로 시작 을 클릭한 후 다음을 선택합니다.

a. 지역 사용 가능 여부에 따라 T3.MEDIUM(권장), T2.MEDIUM 또는 M4.Large instance type을 선택합니다.

b. 요구 사항을 충족하는 VPC, 서브넷, IAM 역할 및 기타 구성 옵션을 선택합니다.

c. 기본 스토리지 옵션을 유지합니다.

d. 필요한 경우 인스턴스에 대한 태그를 입력합니다.

e. Cloud Manager 인스턴스에 필요한 SSH, HTTP 및 HTTPS 연결 방법을 지정합니다.

f. 시작 * 을 클릭합니다.

결과

AWS가 지정된 설정으로 소프트웨어를 시작합니다. Cloud Manager 인스턴스와 소프트웨어는 약 5분 내에 실행되어야 합니다.

작업을 마친 후

웹 브라우저에 공용 IP 주소 또는 전용 IP 주소를 입력하여 Cloud Manager에 로그인한 다음 설정 마법사를 완료합니다.

Azure 마켓플레이스에서 Cloud Manager 구축

Azure에서 Cloud Manager를 구축하는 것이 가장 좋습니다 "NetApp Cloud Central에서 "필요한 경우 Azure 마켓플레이스에서 구축할 수 있습니다.

Cloud Manager를 구축할 수 있는 별도의 지침이 제공됩니다 "Azure 미국 정부 지역" 및 IN "Azure 독일 지역".

Azure Marketplace에서 Cloud Manager를 구축한 경우에도 Cloud Manager는 NetApp Cloud Central과 통합됩니다. "통합에 대해 자세히 알아보십시오".

Azure에 Cloud Manager 배포

Azure에서 Cloud Volumes ONTAP를 시작하는 데 사용할 수 있도록 Cloud Manager를 설치 및 설정해야 합니다.

단계

1. "Cloud Manager의 Azure 마켓플레이스 페이지로 이동합니다".
2. 지금 받기 * 를 클릭한 다음 * 계속 * 을 클릭합니다.
3. Azure 포털에서 * Create * 를 클릭하고 다음 단계에 따라 가상 시스템을 구성합니다.

   VM을 구성할 때 다음 사항에 유의하십시오.

   - Cloud Manager는 HDD 또는 SSD 디스크를 최적의 상태로 사용할 수 있습니다.
   - A2, D2 v2 또는 D2 v3(사용 가능 여부에 따라)의 권장 가상 머신 크기 중 하나를 선택합니다.

◦ 네트워크 보안 그룹의 경우 Cloud Manager에는 SSH, HTTP 및 HTTPS를 사용한 인바운드 연결이 필요합니다.

"Cloud Manager의 보안 그룹 규칙에 대해 자세히 알아보십시오".

◦ 관리 * 에서 * 켜기 * 를 선택하여 클라우드 관리자에 대해 * 시스템 할당 관리 ID * 를 활성화합니다.

이 설정은 Cloud Manager 가상 머신이 자격 증명을 제공하지 않고 Azure Active Directory에 자신을 식별할 수 있도록 관리되는 ID를 허용하므로 중요합니다. "Azure 리소스의 관리 ID에 대해 자세히 알아보십시오".

4. Review + create * 페이지에서 선택 사항을 검토하고 * Create * 를 클릭하여 배포를 시작합니다.

Azure는 지정된 설정으로 가상 머신을 구축합니다. 가상 머신과 Cloud Manager 소프트웨어가 약 5분 이내에 실행되어야 합니다.

5. Cloud Manager 가상 머신에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

http://ipaddress:80

로그인하면 Cloud Manager에서 자동으로 사용자 계정을 이 시스템의 관리자로 추가합니다.

6. 로그인한 후 Cloud Manager 시스템의 이름을 입력합니다.

결과

이제 Cloud Manager가 설치되고 설정되었습니다. Azure에서 Cloud Volumes ONTAP를 배포하기 전에 Azure 사용 권한을 부여해야 합니다.

Cloud Manager에 **Azure** 사용 권한 부여

Azure에 Cloud Manager를 구축한 경우 를 활성화해야 합니다 "시스템에서 할당한 관리 ID입니다". 이제 사용자 지정 역할을 만든 다음 하나 이상의 구독에 대해 Cloud Manager 가상 머신에 역할을 할당하여 필요한 Azure 권한을 부여해야 합니다.

단계

1. Cloud Manager 정책을 사용하여 사용자 지정 역할 생성:

a. 를 다운로드합니다 "Cloud Manager Azure 정책".

b. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

사용자가 Cloud Volumes ONTAP 시스템을 생성할 각 Azure 구독에 대한 ID를 추가해야 합니다.

▪ 예 *

"AssignableScopes":["/Subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzzz","/Subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz","/Subscripts/398e471c-3bzzzzzzzzzzz-4bzbzz-4bzbzbzz-4959-4bzz

c. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 생성합니다.

다음 예에서는 Azure CLI 2.0을 사용하여 사용자 지정 역할을 생성하는 방법을 보여 줍니다.

▪ az 역할 정의 create — 역할 정의 C:\Policy_for_cloud_Manager_Azure_3.6.1.json *

이제 OnCommand Cloud Manager 운영이라는 사용자 지정 역할을 갖게 됩니다. 이 역할은 Cloud Manager 가상 머신에 할당할 수 있습니다.

2. 하나 이상의 구독에 대해 Cloud Manager 가상 머신에 역할을 할당합니다.
   a. Subscriptions * 서비스를 연 다음 Cloud Volumes ONTAP 시스템을 배포할 구독을 선택합니다.
   b. IAM(액세스 제어) * 을 클릭합니다.
   c. Add * > * Add role assignment * 를 클릭한 후 권한을 추가합니다.
      - OnCommand 클라우드 관리자 운영자 * 역할을 선택하십시오.

        OnCommand Cloud Manager Operator는 에 제공되는 기본 이름입니다 "Cloud Manager 정책". 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

      - Virtual Machine * 에 대한 액세스 권한을 할당합니다.
      - Cloud Manager 가상 머신이 생성된 서브스크립션을 선택합니다.
      - Cloud Manager 가상 머신을 선택합니다.
      - 저장 * 을 클릭합니다.
   d. 추가 구독에서 Cloud Volumes ONTAP를 배포하려면 해당 구독으로 전환한 다음 이 단계를 반복합니다.

결과

이제 Cloud Manager에 Azure에서 Cloud Volumes ONTAP를 배포하고 관리하는 데 필요한 권한이 있습니다.

Azure 미국 정부 지역에서 Cloud Manager 구축

미국 정부 지역에서 Cloud Manager를 시작 및 실행하려면 먼저 Azure Government Marketplace에서 Cloud Manager를 구축해야 합니다. 그런 다음, Cloud Manager에서 Cloud Volumes ONTAP 시스템을 구축하고 관리하는 데 필요한 권한을 제공합니다.

지원되는 Azure 미국 정부 지역 목록은 를 참조하십시오 "Cloud Volumes 글로벌 지역".

Azure US Government Marketplace에서 Cloud Manager 구축

Cloud Manager는 Azure US Government Marketplace에서 이미지로 사용할 수 있습니다.

단계

1. Azure US Government 포털에서 OnCommand Cloud Manager를 검색하십시오.
2. Create * 를 클릭하고 다음 단계에 따라 가상 머신을 구성합니다.

   가상 머신을 구성할 때 다음 사항에 유의하십시오.

   - Cloud Manager는 HDD 또는 SSD 디스크를 최적의 상태로 사용할 수 있습니다.
   - A2, D2 v2 또는 D2 v3(사용 가능 여부에 따라)의 권장 가상 머신 크기 중 하나를 선택해야 합니다.
   - 네트워크 보안 그룹의 경우 * 고급 * 을 선택하는 것이 가장 좋습니다.

     고급 * 옵션은 Cloud Manager에 필요한 인바운드 규칙을 포함하는 새 보안 그룹을 만듭니다. 기본 을 선택한 경우 을 참조하십시오 "보안 그룹 규칙" 필수 규칙 목록을 참조하십시오.

3. 요약 페이지에서 선택 사항을 검토하고 * 생성 * 을 클릭하여 배포를 시작합니다.

   Azure는 지정된 설정으로 가상 머신을 구축합니다. 가상 머신과 Cloud Manager 소프트웨어가 약 5분 이내에 실행되어야 합니다.

4. Cloud Manager 가상 머신에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

   http://ipaddress:80

   로그인하면 Cloud Manager에서 자동으로 사용자 계정을 이 시스템의 관리자로 추가합니다.

5. 로그인한 후 Cloud Manager 시스템의 이름을 입력합니다.

결과

이제 Cloud Manager가 설치되고 설정되었습니다. Azure에서 Cloud Volumes ONTAP를 배포하기 전에 Azure 사용 권한을 부여해야 합니다.

관리되는 **ID**를 사용하여 **Cloud Manager**에 **Azure** 사용 권한 부여

사용 권한을 제공하는 가장 쉬운 방법은 을 사용하는 것입니다 "관리 ID" Cloud Manager 가상 머신에서 가상 머신에 필요한 사용 권한을 할당합니다. 원하는 경우, 다른 방법은 입니다 "서비스 보안 주체를 사용하여 Azure 사용 권한을 부여합니다".

단계

1. Cloud Manager 가상 시스템에서 관리 ID 사용:
   a. Cloud Manager 가상 머신으로 이동하여 * Identity * 를 선택합니다.
   b. System Assigned * 에서 * On * 을 클릭한 다음 * Save * 를 클릭합니다.
2. Cloud Manager 정책을 사용하여 사용자 지정 역할 생성:
   a. 를 다운로드합니다 "Cloud Manager Azure 정책".
   b. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

      사용자가 Cloud Volumes ONTAP 시스템을 생성할 각 Azure 구독에 대한 ID를 추가해야 합니다.

      - 예 *

      "AssignableScopes":["/Subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzzz","/Subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz","/Subscripts/398e471c-3bzzzzzzzzzzz-4bzbzz-4bzbzbzz-4959-4bzz

   c. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 생성합니다.

      다음 예에서는 Azure CLI 2.0을 사용하여 사용자 지정 역할을 생성하는 방법을 보여 줍니다.

      - az 역할 정의 create — 역할 정의 C:\Policy_for_cloud_Manager_Azure_3.6.1.json *

   이제 OnCommand Cloud Manager 운영이라는 사용자 지정 역할을 갖게 됩니다. 이 역할은 Cloud Manager 가상 머신에 할당할 수 있습니다.

3. 하나 이상의 구독에 대해 Cloud Manager 가상 머신에 역할을 할당합니다.

a. Subscriptions * 서비스를 연 다음 Cloud Volumes ONTAP 시스템을 배포할 구독을 선택합니다.

b. IAM(액세스 제어) * 을 클릭합니다.

c. 추가 * 를 클릭하고 * 역할 할당 추가 * 를 클릭한 다음 권한을 추가합니다.

- OnCommand 클라우드 관리자 운영자 * 역할을 선택하십시오.

  OnCommand Cloud Manager Operator는 에 제공되는 기본 이름입니다 "Cloud Manager 정책". 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

- Virtual Machine * 에 대한 액세스 권한을 할당합니다.
- Cloud Manager 가상 머신이 생성된 서브스크립션을 선택합니다.
- 가상 머신의 이름을 입력한 다음 선택합니다.
- 저장 * 을 클릭합니다.

d. 추가 구독에서 Cloud Volumes ONTAP를 배포하려면 해당 구독으로 전환한 다음 이 단계를 반복합니다.

결과

이제 Cloud Manager에 Azure에서 Cloud Volumes ONTAP를 배포하고 관리하는 데 필요한 권한이 있습니다.

Azure 독일 지역에 Cloud Manager 설치

Azure 마켓플레이스는 Azure 독일 지역에서 사용할 수 없으므로 NetApp Support 사이트에서 Cloud Manager 설치 프로그램을 다운로드하고 이 지역의 기존 Linux 호스트에 설치해야 합니다.

단계

1. "Azure의 네트워킹 요구 사항을 검토합니다".
2. "Cloud Manager 호스트 요구사항을 검토합니다".
3. "Cloud Manager를 다운로드하고 설치합니다".
4. "서비스 보안 주체를 사용하여 Cloud Manager에 Azure 권한을 부여합니다".

작업을 마친 후

Cloud Manager는 이제 다른 지역과 마찬가지로 Azure 독일 지역에 Cloud Volumes ONTAP를 구축할 준비가 되었습니다. 그러나 먼저 추가 설정을 수행할 수 있습니다.

Cloud Volumes ONTAP 배포

Cloud Volumes ONTAP 시스템을 생성하기 전에

Cloud Manager를 사용하여 Cloud Volumes ONTAP 시스템을 생성하고 관리하기 전에 먼저 Cloud Manager에서 네트워킹을 준비하고 Cloud Manager를 설치 및 설정해야 합니다.

관리자가 지침을 따라 설치하고 실행해야 합니다 "AWS에서" 또는 "Azure에서", 및 옵션 "Cloud Manager 설정".

Cloud Volumes ONTAP 배포를 시작하기 전에 다음 조건이 충족되어야 합니다.

- Cloud Manager 및 Cloud Volumes ONTAP에 대한 AWS 및 Azure 네트워킹 요구사항이 충족되었습니다.
- Cloud Manager에는 사용자 대신 AWS 및 Azure에서 작업을 수행할 수 있는 권한이 있습니다.
- 사용자가 구축할 각 Cloud Volumes ONTAP 제품이 AWS 마켓플레이스를 통해 구독되었습니다.
- Cloud Manager가 설치되었습니다.
- (선택 사항) 추가 테넌트가 정의되었습니다.
- (선택 사항) 테넌트 관리자 및 작업 환경 관리자를 포함할 수 있는 추가 사용자 계정이 생성되었습니다.

Cloud Manager에 로그인

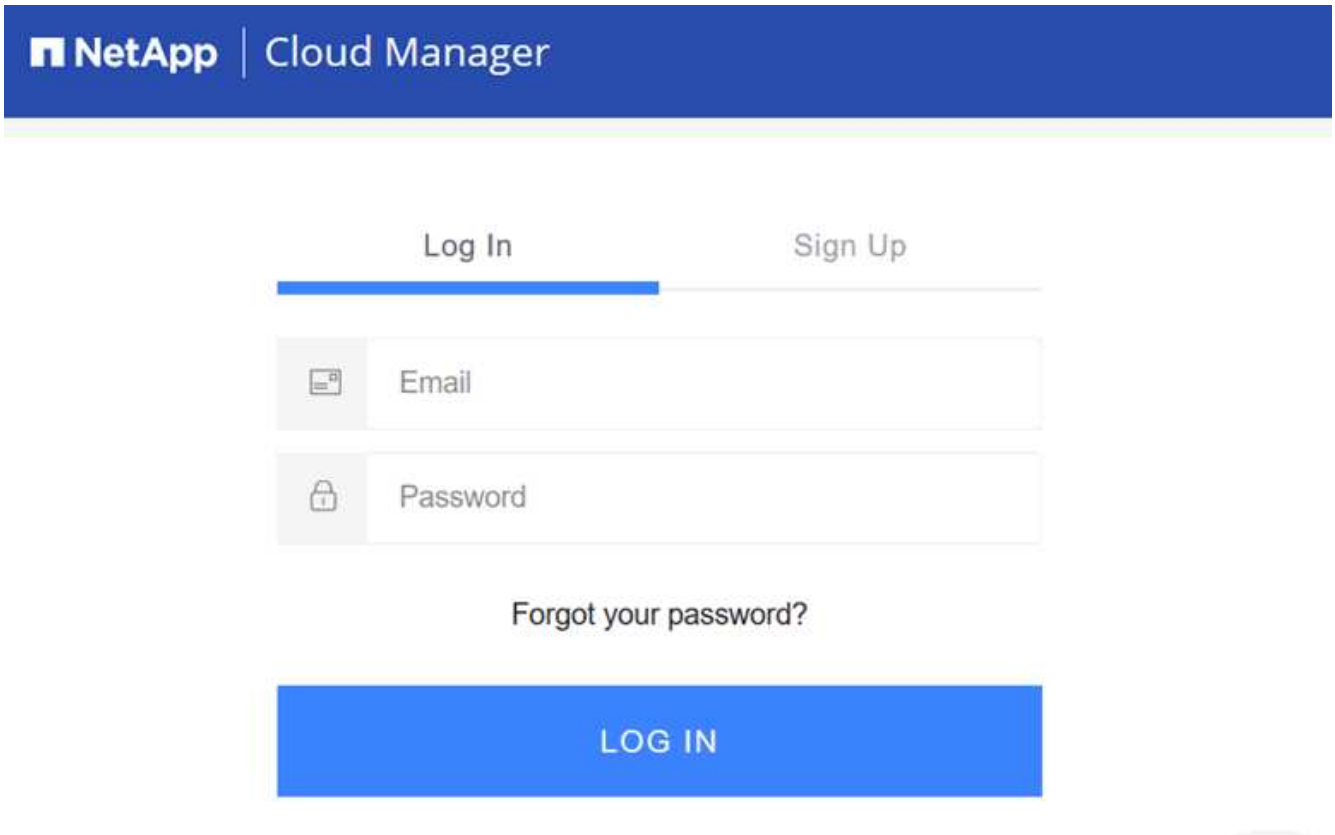
Cloud Manager 시스템에 연결된 모든 웹 브라우저에서 Cloud Manager에 로그인할 수 있습니다. 를 사용하여 로그인해야 합니다 "NetApp Cloud Central에서" 사용자 계정.

단계

1. 웹 브라우저를 열고 에 로그인합니다 "NetApp Cloud Central에서".
2. 클라우드 데이터 서비스로 이동 * 을 클릭하고 * Cloud Volumes ONTAP * 를 선택합니다.
3. 액세스하려는 Cloud Manager 시스템에 대해 * Cloud Manager로 이동 * 을 클릭합니다.

나열된 시스템이 표시되지 않으면 Cloud Manager 관리자가 NetApp Cloud Central 계정을 시스템에 추가했는지 확인하십시오.

4. NetApp Cloud Central 계정을 사용하여 Cloud Manager에 로그인합니다.



Cloud Volumes ONTAP 구성 계획

Cloud Volumes ONTAP를 구축하면 워크로드 요구사항에 맞게 사전 구성된 시스템을 선택하거나 고유한 구성을 생성할 수 있습니다. 자신의 구성을 선택하는 경우 사용 가능한 옵션을 이해해야 합니다.

라이센스 유형을 선택합니다

Cloud Volumes ONTAP는 AWS 및 Azure에서 BYOL(Pay-as-you-go and Bring Your Own License)의 두 가지 가격 옵션으로 제공됩니다. 선불 종량제 의 경우 Explore, Standard 또는 Premium의 세 가지 라이센스 중에서 선택할 수 있습니다. 각 라이센스는 용량과 컴퓨팅 옵션을 다르게 제공합니다.

- "Cloud Volumes ONTAP 9.5에 지원되는 구성입니다"
- "Cloud Volumes ONTAP 9.4에 지원되는 구성"
- "ONTAP 클라우드 9.3에서 지원되는 구성"

스토리지 제한 이해

Cloud Volumes ONTAP 시스템의 물리적 용량 제한은 라이센스에 연결되어 있습니다. 추가 제한은 애그리게이트 및 볼륨 크기에 영향을 줍니다. 구성을 계획할 때 이러한 제한 사항을 숙지해야 합니다.

- "Cloud Volumes ONTAP 9.5의 보관 제한"
- "Cloud Volumes ONTAP 9.4의 스토리지 제한"

- "ONTAP 클라우드 9.3의 스토리지 제한"

AWS에서 시스템 사이징

Cloud Volumes ONTAP 시스템을 사이징하면 성능 및 용량 요구사항을 충족하는 데 도움이 될 수 있습니다. 인스턴스 유형, 디스크 유형 및 디스크 크기를 선택할 때 몇 가지 주요 사항을 알고 있어야 합니다.

인스턴스 유형

- 각 EC2 인스턴스 유형별 최대 처리량과 IOPS에 맞춰 워크로드 요구사항을 충족합니다.
- 여러 사용자가 동시에 시스템에 쓸 경우 요청을 관리할 CPU가 충분한 인스턴스 유형을 선택합니다.
- 대부분 읽혀지는 응용 프로그램이 있는 경우 충분한 RAM이 있는 시스템을 선택합니다.

  "AWS 문서: Amazon EC2 인스턴스 유형"
  "AWS 문서: Amazon EBS – 최적화된 인스턴스"

EBS 디스크 유형입니다

범용 SSD는 Cloud Volumes ONTAP의 가장 일반적인 디스크 유형입니다. EBS 디스크의 사용 사례를 보려면 을 참조하십시오 "AWS 설명서:EBS 볼륨 유형".

EBS 디스크 크기입니다

Cloud Volumes ONTAP 시스템을 시작할 때 초기 디스크 크기를 선택해야 합니다. 그 이후에는 가능합니다 "Cloud Manager로 시스템 용량을 관리할 수 있습니다"하지만 원하는 경우 "스스로 애그리게이트를 빌드하십시오"다음 사항에 유의하십시오.

- Aggregate의 모든 디스크는 동일한 크기여야 합니다.
- EBS 디스크의 성능은 디스크 크기와 관련이 있습니다. 이 크기는 SSD 디스크의 기준 IOPS 및 최대 버스트 지속 시간과 HDD 디스크의 기준 및 버스트 처리량을 결정합니다.
- 궁극적으로 필요한 _ 지속적인 성능 _ 을(를) 제공하는 디스크 크기를 선택해야 합니다.
- 4TB 디스크 6개와 같이 더 큰 디스크를 선택하는 경우에도 EC2 인스턴스가 대역폭 제한에 도달할 수 있으므로 모든 IOPS를 가져오지 못할 수 있습니다.

  EBS 디스크 성능에 대한 자세한 내용은 을 참조하십시오 "AWS 설명서:EBS 볼륨 유형".

AWS에서 Cloud Volumes ONTAP 시스템 사이징에 대한 자세한 내용은 다음 비디오에서 확인하십시오.

[] | *https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg*

Azure에서 시스템 사이징

Cloud Volumes ONTAP 시스템을 사이징하면 성능 및 용량 요구사항을 충족하는 데 도움이 될 수 있습니다. VM 유형, 디스크 유형 및 디스크 크기를 선택할 때 고려해야 할 몇 가지 주요 사항은 다음과 같습니다.

가상 머신 유형입니다

에서 지원되는 가상 머신 유형을 확인합니다 "Cloud Volumes ONTAP 릴리즈 노트" 지원되는 각 VM 유형에 대한 세부 정보를 검토합니다. 각 VM 유형은 특정 수의 데이터 디스크를 지원합니다.

- "Azure 설명서: 범용 가상 머신 크기"

- "Azure 설명서: 메모리에 최적화된 가상 머신 크기"

Azure 디스크 유형입니다

Cloud Volumes ONTAP용 볼륨을 생성할 때 Cloud Volumes ONTAP가 디스크로 사용하는 기본 클라우드 스토리지를 선택해야 합니다.

HA 시스템은 프리미엄 페이지 Blob을 사용합니다. 한편, 단일 노드 시스템에서는 두 가지 유형의 Azure 관리 디스크를 사용할 수 있습니다.

- *Premium SSD* 관리 디스크 높은 비용으로 I/O 집약적인 작업 부하에 높은 성능을 제공합니다.
- _Standard SSD Managed Disks_는 낮은 IOPS가 필요한 워크로드에 일관된 성능을 제공합니다.
- _표준 HDD 관리 디스크 _ 는 높은 IOPS가 필요하지 않고 비용을 절감하려는 경우에 적합합니다.

  이러한 디스크의 사용 사례에 대한 자세한 내용은 를 참조하십시오 "Microsoft Azure 설명서: Microsoft Azure 스토리지 소개".

Azure 디스크 크기입니다

Cloud Volumes ONTAP 인스턴스를 시작할 때 Aggregate의 기본 디스크 크기를 선택해야 합니다. Cloud Manager에서는 이 디스크 크기를 초기 aggregate와 단순 프로비저닝 옵션을 사용할 때 생성되는 추가 애그리게이트에 사용합니다. 에서는 기본적으로 와는 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다 "고급 할당 옵션을 사용합니다".

Aggregate의 모든 디스크는 동일한 크기여야 합니다.

디스크 크기를 선택할 때는 몇 가지 요소를 고려해야 합니다. 디스크 크기는 스토리지에 대한 비용 지불, 애그리게이트에서 생성할 수 있는 볼륨 크기, Cloud Volumes ONTAP에 사용할 수 있는 총 용량 및 스토리지 성능에 영향을 줍니다.

Azure 프리미엄 스토리지의 성능은 디스크 크기와 관련이 있습니다. 디스크가 클수록 IOPS와 처리량이 높아집니다. 예를 들어 1TB 디스크를 선택하면 500GB 디스크보다 더 높은 성능을 얻을 수 있습니다.

표준 스토리지의 디스크 크기 간에는 성능 차이가 없습니다. 필요한 용량에 따라 디스크 크기를 선택해야 합니다.

IOPS 및 디스크 크기별 처리량은 Azure를 참조하십시오.

- "Microsoft Azure: 관리형 디스크 가격"
- "Microsoft Azure: 페이지 Blob 가격 책정"

쓰기 속도 선택

Cloud Manager를 사용하면 단일 노드 Cloud Volumes ONTAP 시스템에 대해 쓰기 속도 설정을 선택할 수 있습니다. 쓰기 속도를 선택하기 전에 고속 쓰기 속도를 사용할 때 정상 및 높음 설정의 차이점과 위험 및 권장 사항을 이해해야 합니다.

일반 쓰기 속도와 높은 쓰기 속도 간의 차이

정상적인 쓰기 속도를 선택하면 데이터가 디스크에 직접 기록되므로 계획되지 않은 시스템 중단 시 데이터 손실 가능성이 줄어듭니다.

빠른 쓰기 속도를 선택하면 데이터가 디스크에 쓰기 전에 메모리에 버퍼링되어 쓰기 성능이 향상됩니다. 이 캐싱으로 인해 계획되지 않은 시스템 중단이 발생할 경우 데이터 손실이 발생할 수 있습니다.

계획되지 않은 시스템 중단 시 손실될 수 있는 데이터 양은 마지막 두 정합성 보장 지점의 스팬입니다. 정합성 보장 지점은 버퍼링된 데이터를 디스크에 쓰는 작업을 가리킵니다. 정합성 보장 지점은 쓰기 로그가 꽉 찼거나 10초 후에(둘 중 먼저 도래하는 시점)에 발생합니다. 그러나 AWS EBS 볼륨 성능은 정합성 보장 지점 처리 시간에 영향을 미칠 수 있습니다.

빠른 쓰기 속도 사용 시기

워크로드에 빠른 쓰기 성능이 필요하고 계획되지 않은 시스템 운영 중단 시 데이터 손실 위험을 감수할 수 있는 경우 빠른 쓰기 속도가 가장 좋습니다.

빠른 쓰기 속도 사용 시 권장 사항

빠른 쓰기 속도를 설정하는 경우 애플리케이션 계층에서 쓰기 보호가 보장되어야 합니다.

볼륨 사용 프로필 선택

ONTAP에는 필요한 총 스토리지 양을 줄일 수 있는 몇 가지 스토리지 효율성 기능이 포함되어 있습니다. Cloud Manager에서 볼륨을 생성할 때 이러한 기능을 사용하도록 설정하는 프로필이나 기능을 사용하지 않도록 설정하는 프로필을 선택할 수 있습니다. 사용할 프로파일을 결정하는 데 도움이 되도록 이러한 기능에 대해 자세히 알아 두어야 합니다.

NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

씬 프로비저닝

에서는 실제 스토리지 풀에 있는 것보다 더 많은 논리적 스토리지를 호스트 또는 사용자에게 제공합니다. 스토리지 공간을 사전에 할당하는 대신 데이터가 기록될 때 스토리지 공간을 각 볼륨에 동적으로 할당합니다.

중복 제거

동일한 데이터 블록을 찾아 단일 공유 블록에 대한 참조로 대체하여 효율성을 향상시킵니다. 이 기술은 동일한 볼륨에 상주하는 중복된 데이터 블록을 제거하여 스토리지 용량 요구 사항을 줄여줍니다.

압축

1차, 2차 및 아카이브 스토리지의 볼륨 내에서 데이터를 압축하여 데이터를 저장하는 데 필요한 물리적 용량을 줄입니다.

AWS 네트워크 정보 워크시트

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

Cloud Volumes ONTAP에 대한 네트워크 정보입니다

확인하십시오	귀사의 가치
지역	
VPC	
서브넷	

확인하십시오	귀사의 가치
보안 그룹(자체 보안 그룹 사용 시)	

여러 **AZs**의 **HA** 쌍에 대한 네트워크 정보

확인하십시오	귀사의 가치
지역	
VPC	
보안 그룹(자체 보안 그룹 사용 시)	
노드 1 가용성 영역	
노드 1 서브넷	
노드 2 가용성 영역	
노드 2 서브넷	
중재자 가용성 영역	
중재자 서브넷	
중재자를 위한 키 쌍입니다	
클러스터 관리 포트의 부동 IP 주소입니다	
노드 1의 데이터에 대한 유동 IP 주소입니다	
노드 2의 데이터에 대한 유동 IP 주소입니다	
부동 IP 주소에 대한 라우팅 테이블	

Azure 네트워크 정보 워크시트

Azure에서 Cloud Volumes ONTAP를 구축할 때는 가상 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

Azure 정보	귀사의 가치
지역	
VNet(가상 네트워크)	
서브넷	
네트워크 보안 그룹(자체 사용 시)	

AWS의 Cloud Volumes ONTAP에서 Flash Cache 활성화

일부 EC2 인스턴스 유형에는 Cloud Volumes ONTAP가 _Flash Cache_로 사용하는 로컬 NVMe 스토리지가 있습니다. Flash Cache는 최근에 읽은 사용자 데이터와 NetApp

메타데이터의 실시간 지능형 캐싱을 통해 데이터 액세스 속도를 높입니다. 데이터베이스, 이메일, 파일 서비스를 비롯한 랜덤 읽기 집약적인 워크로드에 효과적입니다.

재부팅 후 캐시 재가기는 Cloud Volumes ONTAP에서 지원되지 않습니다.

단계

1. Premium 및 BYOL 라이센스로 제공되는 다음 EC2 인스턴스 유형 중 하나를 선택합니다.
   - c5d.4xLarge
   - c5d.9xLarge
   - r5d.2xLarge
2. 모든 볼륨에서 압축을 해제합니다.

   Flash Cache의 성능 향상 기능을 활용하려면 모든 볼륨에서 압축을 해제해야 합니다. Cloud Manager에서 볼륨을 생성할 때 스토리지 효율성을 선택하지 않거나, 볼륨을 생성한 후 생성할 수 있습니다 "CLI를 사용하여 데이터 압축을 비활성화합니다".

AWS에서 Cloud Volumes ONTAP 실행

Cloud Volumes ONTAP는 단일 시스템 구성에서 실행하거나 AWS에서 HA 쌍으로 실행할 수 있습니다.

AWS에서 단일 Cloud Volumes ONTAP 시스템 시작

AWS에서 Cloud Volumes ONTAP를 시작하려면 Cloud Manager에서 새로운 작업 환경을 만들어야 합니다.

시작하기 전에

- 구성을 선택하고 관리자로부터 AWS 네트워킹 정보를 받아 준비해야 합니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP 구성 계획".
- BYOL 시스템을 시작하려면 20자리의 일련 번호(라이센스 키)가 있어야 합니다.
- CIFS를 사용하려면 DNS와 Active Directory를 설정해야 합니다. 자세한 내용은 을 참조하십시오 "AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항".

이 작업에 대해

작업 환경을 생성한 직후 Cloud Manager는 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 Cloud Manager가 즉시 인스턴스를 종료한 다음 Cloud Volumes ONTAP 시스템 구축을 시작합니다. Cloud Manager에서 연결을 확인할 수 없는 경우 작업 환경을 생성하지 못합니다. 테스트 인스턴스는 T2.nano(기본 VPC 테넌시의 경우) 또는 m3.medium(전용 VPC 테넌시의 경우)입니다.

단계

1. 작업 환경 페이지에서 * 작업 환경 추가 * 를 클릭합니다.
2. 생성 아래에서 * Cloud Volumes ONTAP * 를 선택합니다.
3. 세부 정보 및 자격 증명 페이지에서 AWS 계정을 변경하고, 작업 환경 이름을 입력하고, 필요한 경우 태그를 추가한 다음 암호를 입력합니다.

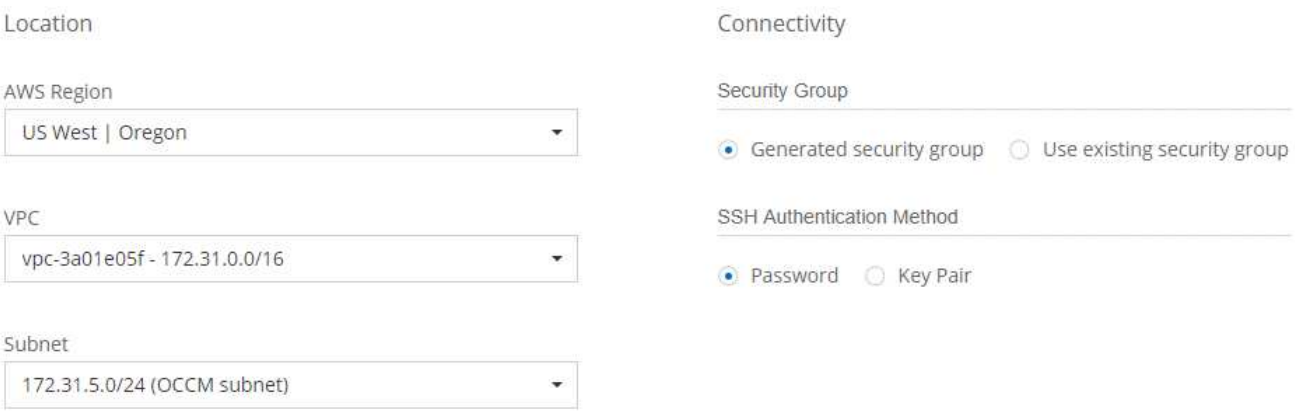
   이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
계정 전환	클라우드 제공업체 계정을 추가한 경우 다른 계정을 선택할 수 있습니다. 자세한 내용은 을 참조하십시오 "Cloud Manager에 클라우드 공급자 계정 추가".
작업 환경 이름	Cloud Manager에서는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
태그 추가	AWS 태그는 AWS 리소스에 대한 메타데이터입니다. Cloud Manager에서 Cloud Volumes ONTAP 인스턴스와 해당 인스턴스에 연결된 각 AWS 리소스에 태그를 추가합니다. 작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 생성된 후에는 더 많은 태그를 추가할 수 있습니다. API는 작업 환경을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 자세한 내용은 을 참조하십시오 "AWS 문서: Amazon EC2 리소스에 태그 달기".
자격 증명	Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 OnCommand 시스템 관리자 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다.

Cloud Manager 계정에 AWS 키가 지정되지 않은 경우 계속 을 클릭하면 키를 입력하라는 메시지가 표시됩니다. 계속 진행하려면 먼저 입력해야 합니다.

4. 위치 및 연결 페이지에서 AWS 워크시트에 기록한 네트워크 정보를 입력한 다음 * 계속 * 을 클릭합니다.

   다음 이미지는 위치 및 연결 페이지가 채워진 상태를 보여줍니다.



5. 데이터 암호화 페이지에서 데이터 암호화 또는 AWS로 관리되는 암호화 없음을 선택합니다.

   AWS로 관리되는 암호화의 경우 사용자 계정 또는 다른 AWS 계정에서 다른 CMK(Customer Master Key)를 선택할 수 있습니다.

   "Cloud Volumes ONTAP용 AWS KMS를 설정하는 방법에 대해 알아보십시오".

   "지원되는 암호화 기술에 대해 자세히 알아보십시오".

6. 라이센스 및 지원 사이트 계정 페이지에서 용량제 또는 BYOL 중 무엇을 사용할지 지정한 다음 NetApp Support 사이트 계정을 지정합니다.

   라이센스 작동 방식을 이해하려면 를 참조하십시오 "라이센싱".

NetApp Support 사이트 계정은 사용한 만큼만 지불하는 데 선택 사항이지만 BYOL 시스템에는 필요합니다. "NetApp Support 사이트 계정을 추가하는 방법을 알아보십시오".

7. 사전 구성된 패키지 페이지에서 패키지 중 하나를 선택하여 Cloud Volumes ONTAP를 빠르게 시작하거나 * 고유한 구성 만들기 * 를 클릭합니다.

   패키지 중 하나를 선택하는 경우 볼륨을 지정한 다음 구성을 검토 및 승인하기만 하면 됩니다.

8. IAM 역할 페이지에서 Cloud Manager가 역할을 생성할 수 있도록 기본 옵션을 유지해야 합니다.

   자체 정책을 사용하려면 이 정책이 충족해야 합니다 "Cloud Volumes ONTAP 노드의 정책 요구사항".

9. 라이센스 페이지에서 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 라이센스, 인스턴스 유형, 인스턴스 테넌시를 선택한 다음 * 계속 * 을 클릭합니다.

   인스턴스를 시작한 후 필요한 사항이 변경되면 나중에 라이센스 또는 인스턴스 유형을 수정할 수 있습니다.

   선택한 버전에 대해 새로운 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우, Cloud Manager는 작업 환경을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.4 RC1 및 9.4 GA를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리즈에서 다른 릴리즈로 발생하지 않습니다(예: 9.3에서 9.4).

10. 기본 스토리지 리소스 페이지에서 초기 애그리게이트의 설정, 디스크 유형, 각 디스크의 크기, S3 계층화 활성화 여부를 선택합니다.

    디스크 유형은 초기 볼륨입니다. 이후 볼륨에 대해 다른 디스크 유형을 선택할 수 있습니다.

    디스크 크기는 초기 애그리게이트의 모든 디스크와 단순 프로비저닝 옵션을 사용할 때 Cloud Manager가 생성하는 추가 애그리게이트의 경우 모두 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

    디스크 유형과 크기를 선택하는 방법은 을 참조하십시오 "AWS에서 시스템 사이징".

11. 쓰기 속도 및 WORM 페이지에서 * 일반 * 또는 * 고속 * 쓰기 속도를 선택하고 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

    "쓰기 속도에 대해 자세히 알아보십시오".

    "WORM 스토리지에 대해 자세히 알아보십시오".

12. 볼륨 생성 페이지에서 새 볼륨에 대한 세부 정보를 입력한 다음 * 계속 * 을 클릭합니다.

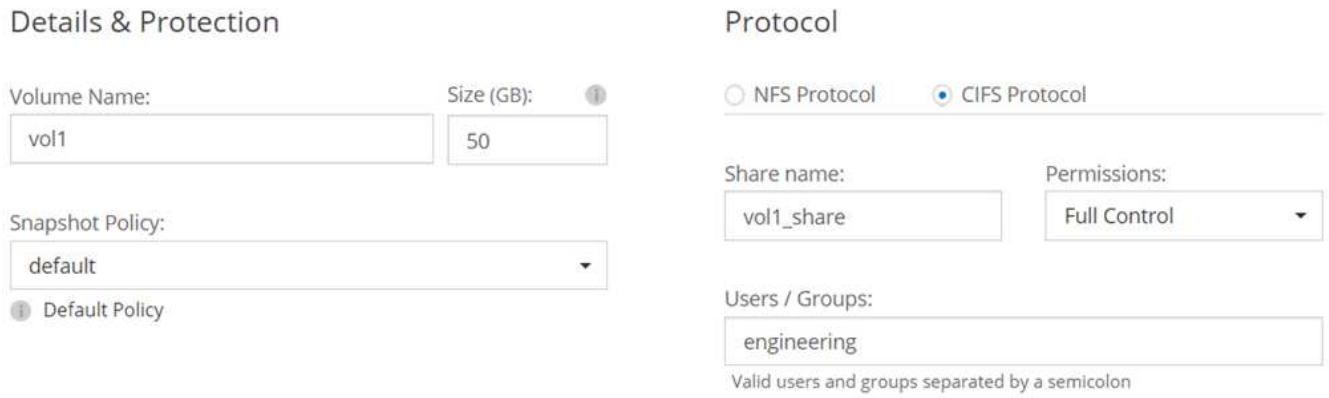
    iSCSI에 대한 볼륨을 생성하려면 이 단계를 건너뛸 수 있습니다. Cloud Manager는 NFS 및 CIFS에 대해서만 볼륨을 설정합니다.

    이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝의 사용 여부에 따라 크게 달라집니다. 이를 통해 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다.

필드에 입력합니다	설명
액세스 제어(NFS에만 해당)	엑스포트 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 Cloud Manager는 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS 전용)	이러한 필드를 사용하면 사용자 및 그룹의 공유에 대한 액세스 수준(액세스 제어 목록 또는 ACL라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자 또는 그룹, UNIX 사용자 또는 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자의 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사본 정책은 자동으로 생성되는 NetApp 스냅샷 복사본의 수와 빈도를 지정합니다. NetApp 스냅샷 복사본은 성능 영향이 없고 최소한의 스토리지가 필요한 시점 파일 시스템 이미지입니다. 기본 정책을 선택하거나 선택하지 않을 수 있습니다. Microsoft SQL Server의 tempdb와 같이 임시 데이터에 대해 없음을 선택할 수 있습니다.

다음 이미지는 CIFS 프로토콜에 대해 작성된 볼륨 페이지를 보여 줍니다.



13. CIFS 프로토콜을 선택한 경우 CIFS 설정 페이지에서 CIFS 서버를 설정합니다.

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.
도메인에 가입하도록 승인된 자격 증명입니다	AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.
DNS 도메인	SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 대부분의 경우 도메인은 AD 도메인과 동일합니다.

필드에 입력합니다	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 참조하십시오 "Cloud Manager API 개발자 가이드 를 참조하십시오" 를 참조하십시오.

14. 필요한 경우 Usage Profile, Disk Type 및 Tiering Policy 페이지에서 스토리지 효율성 기능을 사용하도록 설정하고 S3 계층화 정책을 편집할지 여부를 선택합니다.

    자세한 내용은 을 참조하십시오 "볼륨 사용 프로필 이해" 및 "데이터 계층화 개요".

15. 검토 및 승인 페이지에서 선택 항목을 검토하고 확인합니다.
    a. 구성에 대한 세부 정보를 검토합니다.
    b. Cloud Manager가 구매할 지원 및 AWS 리소스에 대한 세부 정보를 검토하려면 * 자세한 정보 * 를 클릭합니다.
    c. 이해함… * 확인란을 선택합니다.
    d. Go * 를 클릭합니다.

결과

Cloud Manager가 Cloud Volumes ONTAP 인스턴스를 시작합니다. 타임라인에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 인스턴스를 시작하는 데 문제가 있는 경우 실패 메시지를 검토합니다. 작업 환경을 선택하고 환경 다시 생성 을 클릭할 수도 있습니다.

자세한 내용은 를 참조하십시오 "NetApp Cloud Volumes ONTAP 지원".

작업을 마친 후

- CIFS 공유를 프로비저닝한 경우 파일 및 폴더에 대한 사용자 또는 그룹 권한을 제공하고 해당 사용자가 공유를 액세스하고 파일을 생성할 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 System Manager 또는 CLI를 사용하십시오.

  할당량을 사용하면 사용자, 그룹 또는 qtree가 사용하는 파일 수와 디스크 공간을 제한하거나 추적할 수 있습니다.

AWS에서 Cloud Volumes ONTAP HA 쌍 시작

AWS에서 Cloud Volumes ONTAP HA 쌍을 실행하려면 Cloud Manager에서 HA 작업 환경을 만들어야 합니다.

시작하기 전에

- 구성을 선택하고 관리자로부터 AWS 네트워킹 정보를 받아 준비해야 합니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP 구성 계획".
- BYOL 라이센스를 구입한 경우 각 노드에 대해 20자리의 일련 번호(라이센스 키)가 있어야 합니다.
- CIFS를 사용하려면 DNS와 Active Directory를 설정해야 합니다. 자세한 내용은 을 참조하십시오 "AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항".

이 작업에 대해

작업 환경을 생성한 직후 Cloud Manager는 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 Cloud Manager가 즉시 인스턴스를 종료한 다음 Cloud Volumes ONTAP 시스템 구축을 시작합니다. Cloud

Manager에서 연결을 확인할 수 없는 경우 작업 환경을 생성하지 못합니다. 테스트 인스턴스는 T2.nano(기본 VPC 테넌시의 경우) 또는 m3.medium(전용 VPC 테넌시의 경우)입니다.

단계

1. 작업 환경 페이지에서 * 작업 환경 추가 * 를 클릭합니다.
2. 생성 아래에서 * Cloud Volumes ONTAP HA * 를 선택합니다.
3. 세부 정보 및 자격 증명 페이지에서 AWS 계정을 변경하고, 작업 환경 이름을 입력하고, 필요한 경우 태그를 추가한 다음 암호를 입력합니다.

   이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
계정 전환	클라우드 제공업체 계정을 추가한 경우 다른 계정을 선택할 수 있습니다. 자세한 내용은 을 참조하십시오 "Cloud Manager에 클라우드 공급자 계정 추가".
작업 환경 이름	Cloud Manager에서는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
태그 추가	AWS 태그는 AWS 리소스에 대한 메타데이터입니다. Cloud Manager에서 Cloud Volumes ONTAP 인스턴스와 해당 인스턴스에 연결된 각 AWS 리소스에 태그를 추가합니다. 태그에 대한 자세한 내용은 을 참조하십시오 "AWS 문서: Amazon EC2 리소스에 태그 달기".
자격 증명	Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 OnCommand 시스템 관리자 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다.

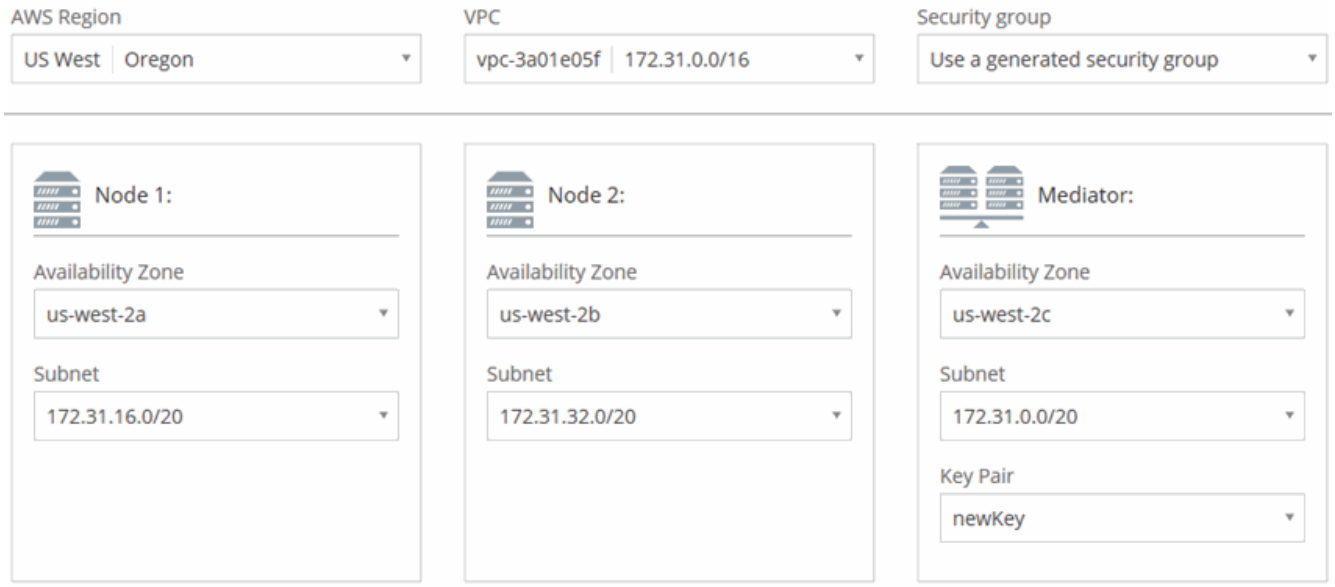
   Cloud Manager 계정에 AWS 키가 지정되지 않은 경우 계속 을 클릭하면 키를 입력하라는 메시지가 표시됩니다. 계속하기 전에 AWS 키를 입력해야 합니다.

4. HA 구축 모델 페이지에서 HA 구성을 선택합니다.

   배포 모델에 대한 개요는 을 참조하십시오 "AWS용 Cloud Volumes ONTAP HA".

5. 지역 및 VPC 페이지에서 AWS 워크시트에 기록한 네트워크 정보를 입력한 다음 * 계속 * 을 클릭합니다.

   다음 이미지는 다중 AZ 구성에 대해 작성된 위치 페이지를 보여줍니다.



6. 연결 및 SSH 인증 페이지에서 HA 쌍의 연결 방법과 중재자를 선택합니다.
7. 여러 AZs를 선택한 경우 부동 IP 주소를 지정한 다음 * 계속 * 을 클릭합니다.

   IP 주소는 해당 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 자세한 내용은 을 참조하십시오 "여러 AZs에서 Cloud Volumes ONTAP HA를 위한 AWS 네트워킹 요구사항".

8. 여러 AZs를 선택한 경우 부동 IP 주소에 대한 라우트가 포함되어야 하는 라우트 테이블을 선택한 다음 * 계속 * 을 클릭합니다.

   둘 이상의 라우팅 테이블이 있는 경우 올바른 라우팅 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP HA 쌍에 액세스하지 못할 수 있습니다. 라우팅 테이블에 대한 자세한 내용은 을 참조하십시오 "AWS 설명서: 경로 테이블".

9. 데이터 암호화 페이지에서 데이터 암호화 또는 AWS로 관리되는 암호화 없음을 선택합니다.

   AWS로 관리되는 암호화의 경우 사용자 계정 또는 다른 AWS 계정에서 다른 CMK(Customer Master Key)를 선택할 수 있습니다.

   "Cloud Volumes ONTAP용 AWS KMS를 설정하는 방법에 대해 알아보십시오".

   "지원되는 암호화 기술에 대해 자세히 알아보십시오".

10. 라이센스 및 지원 사이트 계정 페이지에서 용량제 또는 BYOL 중 무엇을 사용할지 지정한 다음 NetApp Support 사이트 계정을 지정합니다.

    라이센스 작동 방식을 이해하려면 를 참조하십시오 "라이센싱".

    NetApp Support 사이트 계정은 사용한 만큼만 지불하는 데 선택 사항이지만 BYOL 시스템에는 필요합니다. "NetApp Support 사이트 계정을 추가하는 방법을 알아보십시오".

11. 사전 구성된 패키지 페이지에서 패키지 중 하나를 선택하여 Cloud Volumes ONTAP 시스템을 빠르게 시작하거나 * 고유한 구성 만들기 * 를 클릭합니다.

    패키지 중 하나를 선택하는 경우 볼륨을 지정한 다음 구성을 검토 및 승인하기만 하면 됩니다.

12. IAM 역할 페이지에서 Cloud Manager가 역할을 생성할 수 있도록 기본 옵션을 유지해야 합니다.

    자체 정책을 사용하려면 이 정책이 충족해야 합니다 "Cloud Volumes ONTAP 노드 및 HA 중재자의 정책 요구사항".

13. 라이센스 페이지에서 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 라이센스, 인스턴스 유형, 인스턴스 테넌시를 선택한 다음 * 계속 * 을 클릭합니다.

    인스턴스를 시작한 후 요구 사항이 변경되는 경우 나중에 라이센스 또는 인스턴스 유형을 수정할 수 있습니다.

    선택한 버전에 대해 새로운 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우, Cloud Manager는 작업 환경을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.4 RC1 및 9.4 GA를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리즈에서 다른 릴리즈로 발생하지 않습니다(예: 9.3에서 9.4).

14. 기본 스토리지 리소스 페이지에서 초기 애그리게이트의 설정, 디스크 유형, 각 디스크의 크기, S3 계층화 활성화 여부를 선택합니다.

    디스크 유형은 초기 볼륨입니다. 이후 볼륨에 대해 다른 디스크 유형을 선택할 수 있습니다.

    디스크 크기는 초기 애그리게이트의 모든 디스크와 단순 프로비저닝 옵션을 사용할 때 Cloud Manager가 생성하는 추가 애그리게이트의 경우 모두 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

    디스크 유형과 크기를 선택하는 방법은 을 참조하십시오 "AWS에서 시스템 사이징".

15. 필요한 경우 WORM 페이지에서 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

    "WORM 스토리지에 대해 자세히 알아보십시오".

16. 볼륨 생성 페이지에서 새 볼륨에 대한 세부 정보를 입력한 다음 * 계속 * 을 클릭합니다.

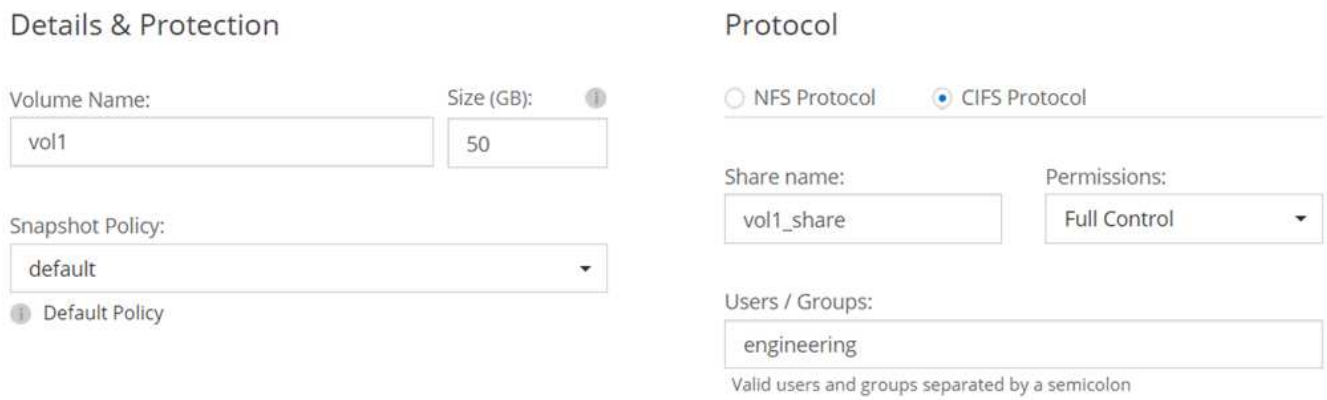
    iSCSI에 대한 볼륨을 생성하려면 이 단계를 건너뛸 수 있습니다. Cloud Manager는 NFS 및 CIFS에 대해서만 볼륨을 설정합니다.

    이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝의 사용 여부에 따라 크게 달라집니다. 이를 통해 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다.
액세스 제어(NFS에만 해당)	엑스포트 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 Cloud Manager는 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS 전용)	이러한 필드를 사용하면 사용자 및 그룹의 공유에 대한 액세스 수준(액세스 제어 목록 또는 ACL라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자 또는 그룹, UNIX 사용자 또는 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자의 도메인을 포함해야 합니다.

필드에 입력합니다	설명
스냅샷 정책	스냅샷 복사본 정책은 자동으로 생성되는 NetApp 스냅샷 복사본의 수와 빈도를 지정합니다. NetApp 스냅샷 복사본은 성능 영향이 없고 최소한의 스토리지가 필요한 시점 파일 시스템 이미지입니다. 기본 정책을 선택하거나 선택하지 않을 수 있습니다. Microsoft SQL Server의 tempdb와 같이 임시 데이터에 대해 없음을 선택할 수 있습니다.

다음 이미지는 CIFS 프로토콜에 대해 작성된 볼륨 페이지를 보여 줍니다.



17. CIFS 프로토콜을 선택한 경우 CIFS 설정 페이지에서 CIFS 서버를 설정합니다.

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.
도메인에 가입하도록 승인된 자격 증명입니다	AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.
DNS 도메인	SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 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 참조하십시오 "Cloud Manager API 개발자 가이드 를 참조하십시오" 를 참조하십시오.

18. 필요한 경우 Usage Profile, Disk Type 및 Tiering Policy 페이지에서 스토리지 효율성 기능을 사용하도록 설정하고 S3 계층화 정책을 편집할지 여부를 선택합니다.

자세한 내용은 을 참조하십시오 "볼륨 사용 프로필 이해" 및 "데이터 계층화 개요".

19. 검토 및 승인 페이지에서 선택 항목을 검토하고 확인합니다.
    a. 구성에 대한 세부 정보를 검토합니다.
    b. Cloud Manager가 구매할 지원 및 AWS 리소스에 대한 세부 정보를 검토하려면 * 자세한 정보 * 를 클릭합니다.
    c. 이해함… * 확인란을 선택합니다.
    d. Go * 를 클릭합니다.

결과

Cloud Manager가 Cloud Volumes ONTAP HA 쌍을 시작합니다. 타임라인에서 진행 상황을 추적할 수 있습니다.

HA 쌍 실행에 문제가 있는 경우 장애 메시지를 검토하십시오. 작업 환경을 선택하고 환경 다시 생성 을 클릭할 수도 있습니다.

자세한 내용은 를 참조하십시오 "NetApp Cloud Volumes ONTAP 지원".

작업을 마친 후

- CIFS 공유를 프로비저닝한 경우 파일 및 폴더에 대한 사용자 또는 그룹 권한을 제공하고 해당 사용자가 공유를 액세스하고 파일을 생성할 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 System Manager 또는 CLI를 사용하십시오.

  할당량을 사용하면 사용자, 그룹 또는 qtree가 사용하는 파일 수와 디스크 공간을 제한하거나 추적할 수 있습니다.

Azure에서 Cloud Volumes ONTAP 실행

Cloud Manager에서 Cloud Volumes ONTAP 작업 환경을 생성하여 Azure에서 단일 노드 시스템 또는 HA 쌍을 시작할 수 있습니다.

시작하기 전에

- Azure 계정에 필요한 권한이 있는지 확인하십시오. 특히 이전 릴리즈에서 업그레이드하고 처음으로 HA 시스템을 배포하는 경우 더욱 그렇습니다.

  "HA 시스템을 배포하는 데 필요한 새로운 권한을 확인하십시오".

- 구성을 선택하고 관리자로부터 Azure 네트워킹 정보를 받아야 합니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP 구성 계획".
- BYOL 시스템을 구축하려면 각 노드에 대해 20자리의 일련 번호(라이센스 키)가 필요합니다.

이 작업에 대해

Cloud Manager는 Azure에서 Cloud Volumes ONTAP 시스템을 생성할 때 리소스 그룹, 네트워크 인터페이스, 스토리지 계정 등과 같은 여러 Azure 개체를 생성합니다. 마법사 마지막에서 리소스 요약을 검토할 수 있습니다.

단계

1. 작업 환경 페이지에서 * 작업 환경 추가 * 를 클릭합니다
2. 생성 아래에서 Azure의 단일 노드 시스템 또는 Azure의 HA 쌍을 선택합니다.
3. 세부 정보 및 자격 증명 페이지에서 필요에 따라 Azure 계정 또는 구독을 변경하고, 클러스터 이름 및 리소스 그룹 이름을 지정하고, 필요한 경우 태그를 추가한 다음 자격 증명을 지정합니다.

다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
계정 전환	다른 계정 또는 구독을 선택할 수 있습니다 "추가 클라우드 공급자 계정이 추가되었습니다".
작업 환경 이름	Cloud Manager에서는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Azure 가상 머신 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
리소스 그룹 이름	기본값 사용 * 의 선택을 취소하면 새 자원 그룹의 이름을 입력할 수 있습니다. 기존 리소스 그룹을 사용하려면 API를 사용해야 합니다.
태그	태그는 Azure 리소스에 대한 메타데이터입니다. Cloud Manager는 Cloud Volumes ONTAP 시스템과 시스템에 연결된 각 Azure 리소스에 태그를 추가합니다. 작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 생성된 후에는 더 많은 태그를 추가할 수 있습니다. API는 작업 환경을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 자세한 내용은 을 참조하십시오 "Microsoft Azure 문서: 태그를 사용하여 Azure 리소스를 구성합니다".
자격 증명	Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 OnCommand 시스템 관리자 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다.

4. 위치 페이지에서 위치 및 보안 그룹을 선택하고 확인란을 선택하여 네트워크 연결을 확인한 다음 * 계속 * 을 클릭합니다.
5. 라이센스 및 지원 사이트 계정 페이지에서 용량제 또는 BYOL 중 무엇을 사용할지 지정한 다음 NetApp Support 사이트 계정을 지정합니다.

   라이센스 작동 방식을 이해하려면 를 참조하십시오 "라이센싱".

   NetApp Support 사이트 계정은 사용한 만큼만 지불하는 데 선택 사항이지만 BYOL 시스템에는 필요합니다. "NetApp Support 사이트 계정을 추가하는 방법을 알아보십시오".

6. 사전 구성된 패키지 페이지에서 패키지 중 하나를 선택하여 Cloud Volumes ONTAP 시스템을 신속하게 배포하거나 * 고유한 구성 만들기 * 를 클릭합니다.

   패키지 중 하나를 선택하는 경우 볼륨을 지정한 다음 구성을 검토 및 승인하기만 하면 됩니다.

7. 라이센스 페이지에서 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 라이센스 및 가상 시스템 유형을 선택한 다음 * 계속 * 을 클릭합니다.

   시스템을 시작한 후 요구 사항이 변경되는 경우 나중에 라이센스 또는 가상 시스템 유형을 수정할 수 있습니다.

   선택한 버전에 대해 새로운 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우, Cloud Manager는 작업 환경을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.5 RC1 및 9.5 GA를 사용할 수 있는 경우 업데이트가 발생합니다. 9.4에서 9.5와 같이 릴리스 간에 업데이트가 발생하지 않습니다.

8. Azure 마켓플레이스 페이지에서 Cloud Manager가 Cloud Volumes ONTAP의 프로그래밍 방식 배포를 활성화할 수 없는 경우 단계를 따릅니다.
9. 기본 스토리지 리소스 페이지에서 초기 애그리게이트의 설정, 디스크 유형, 각 디스크의 크기, 데이터 계층화 활성화 여부를 선택합니다.

디스크 유형은 초기 볼륨입니다. 이후 볼륨에 대해 다른 디스크 유형을 선택할 수 있습니다.

디스크 크기는 초기 애그리게이트의 모든 디스크와 단순 프로비저닝 옵션을 사용할 때 Cloud Manager가 생성하는 추가 애그리게이트의 경우 모두 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

디스크 유형과 크기를 선택하는 방법은 을 참조하십시오 "Azure에서 시스템 사이징".

10. 쓰기 속도 및 WORM 페이지에서 * 일반 * 또는 * 고속 * 쓰기 속도를 선택하고 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

    ⓘ 쓰기 속도 선택은 단일 노드 시스템에서만 지원됩니다.

    "쓰기 속도에 대해 자세히 알아보십시오".

    "WORM 스토리지에 대해 자세히 알아보십시오".

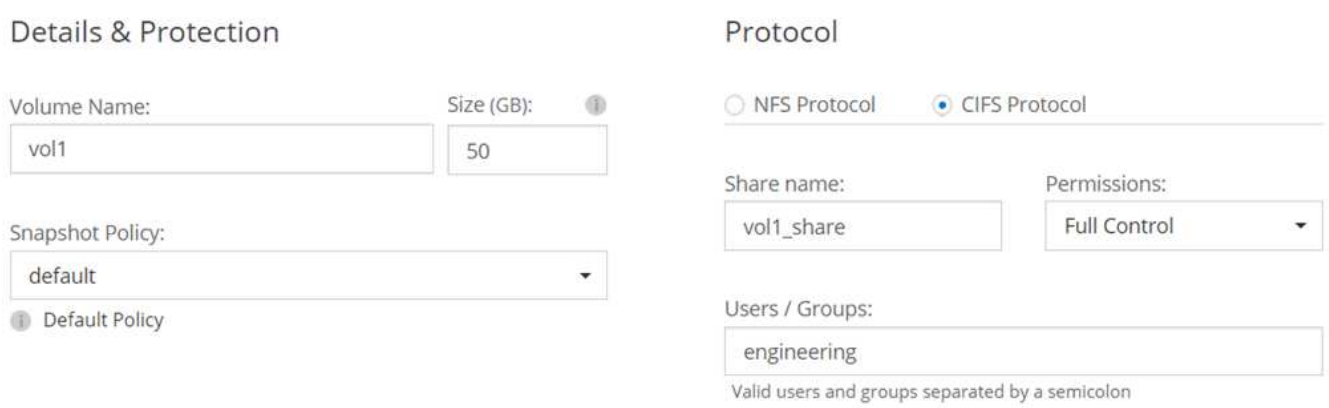
11. 볼륨 생성 페이지에서 새 볼륨에 대한 세부 정보를 입력한 다음 * 계속 * 을 클릭합니다.

    iSCSI를 사용하려면 이 단계를 건너뛰어야 합니다. Cloud Manager를 사용하면 NFS 및 CIFS에 대해서만 볼륨을 생성할 수 있습니다.

    이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝의 사용 여부에 따라 크게 달라집니다. 이를 통해 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다.
액세스 제어(NFS에만 해당)	엑스포트 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 Cloud Manager는 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS 전용)	이러한 필드를 사용하면 사용자 및 그룹의 공유에 대한 액세스 수준(액세스 제어 목록 또는 ACL라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자 또는 그룹, UNIX 사용자 또는 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자의 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사본 정책은 자동으로 생성되는 NetApp 스냅샷 복사본의 수와 빈도를 지정합니다. NetApp 스냅샷 복사본은 성능 영향이 없고 최소한의 스토리지가 필요한 시점 파일 시스템 이미지입니다. 기본 정책을 선택하거나 선택하지 않을 수 있습니다. Microsoft SQL Server의 tempdb와 같이 임시 데이터에 대해 없음을 선택할 수 있습니다.

    다음 이미지는 CIFS 프로토콜에 대해 작성된 볼륨 페이지를 보여 줍니다.



12. CIFS 프로토콜을 선택한 경우 CIFS 설정 페이지에서 CIFS 서버를 설정합니다.

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.
도메인에 가입하도록 승인된 자격 증명입니다	AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.
DNS 도메인	SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 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 참조하십시오 "Cloud Manager API 개발자 가이드 를 참조하십시오" 를 참조하십시오.

13. Usage Profile, Disk Type 및 Tiering Policy 페이지에서 스토리지 효율성 기능을 사용할지 여부를 선택하고 필요한 경우 계층화 정책을 변경합니다.

ⓘ 스토리지 계층화는 단일 노드 시스템에서만 지원됩니다.

자세한 내용은 을 참조하십시오 "볼륨 사용 프로필 이해" 및 "데이터 계층화 개요".

14. 검토 및 승인 페이지에서 선택 항목을 검토하고 확인합니다.
    a. 구성에 대한 세부 정보를 검토합니다.
    b. Cloud Manager가 구매할 지원 및 Azure 리소스에 대한 세부 정보를 검토하려면 * 추가 정보 * 를 클릭합니다.
    c. 이해함… * 확인란을 선택합니다.

d. Go * 를 클릭합니다.

결과

Cloud Manager는 Cloud Volumes ONTAP 시스템을 구축합니다. 타임라인에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템을 배포하는 데 문제가 있으면 오류 메시지를 검토합니다. 작업 환경을 선택하고 * 환경 다시 작성 * 을 클릭할 수도 있습니다.

자세한 내용은 를 참조하십시오 "NetApp Cloud Volumes ONTAP 지원".

작업을 마친 후

- CIFS 공유를 프로비저닝한 경우 파일 및 폴더에 대한 사용자 또는 그룹 권한을 제공하고 해당 사용자가 공유를 액세스하고 파일을 생성할 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 System Manager 또는 CLI를 사용하십시오.

  할당량을 사용하면 사용자, 그룹 또는 qtree가 사용하는 파일 수와 디스크 공간을 제한하거나 추적할 수 있습니다.

선불 종량제 시스템을 등록하는 중입니다

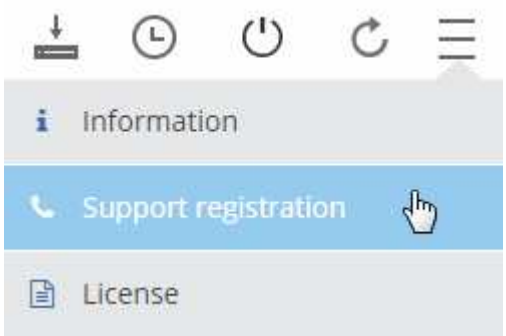
NetApp의 지원은 Cloud Volumes ONTAP Explore, Standard 및 Premium 시스템에 포함되어 있지만, 먼저 NetApp에 시스템을 등록하여 지원을 활성화해야 합니다.

단계

1. NetApp Support 사이트 계정을 Cloud Manager에 아직 추가하지 않은 경우 * 계정 설정 * 으로 이동하여 지금 추가하십시오.

   "NetApp Support 사이트 계정을 추가하는 방법을 알아보십시오".

2. 작업 환경 페이지에서 등록할 시스템의 이름을 두 번 클릭합니다.
3. 메뉴 아이콘을 클릭한 다음 * 지원 등록 * 을 클릭합니다.



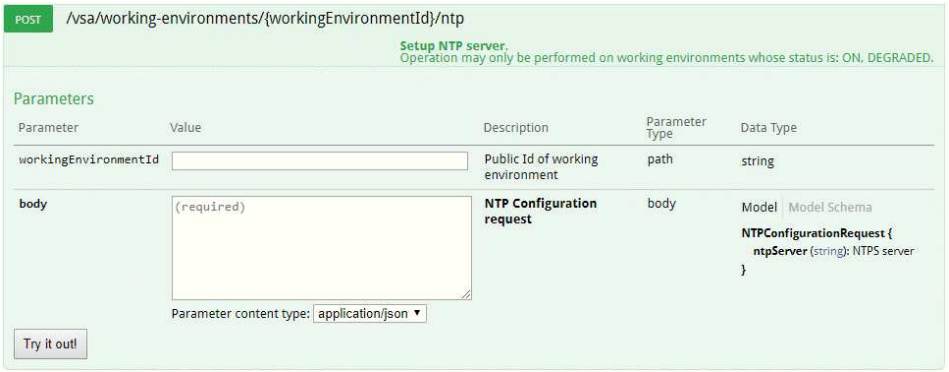
4. NetApp Support 사이트 계정을 선택하고 * Register * 를 클릭합니다.

결과

Cloud Manager가 시스템을 NetApp에 등록합니다.

Cloud Volumes ONTAP 설정

Cloud Volumes ONTAP를 구축한 후에는 NTP를 사용하여 시스템 시간을 동기화하고 System Manager 또는 CLI에서 몇 가지 선택적 작업을 수행하여 시스템 시간을 설정할 수 있습니다.

작업	설명
NTP를 사용하여 시스템 시간을 동기화합니다	NTP 서버를 지정하면 네트워크 시스템 간의 시간이 동기화되어 시간 차이로 인한 문제를 방지할 수 있습니다. CIFS 서버를 설정할 때 Cloud Manager API를 사용하거나 사용자 인터페이스에서 NTP 서버를 지정합니다. • "CIFS 서버 수정" • "Cloud Manager API 개발자 가이드 를 참조하십시오" 예를 들어, AWS의 단일 노드 시스템에 대한 API는 다음과 같습니다. 
선택 사항: AutoSupport를 구성합니다	AutoSupport은 시스템의 상태를 능동적으로 모니터링하고 기본적으로 NetApp 기술 지원 팀에 메시지를 자동으로 보냅니다. 인스턴스를 시작하기 전에 Cloud Manager 관리자가 프록시 서버를 Cloud Manager에 추가한 경우 Cloud Volumes ONTAP은 해당 프록시 서버를 AutoSupport 메시지에 사용하도록 구성됩니다. AutoSupport를 테스트하여 메시지를 보낼 수 있는지 확인해야 합니다. 자세한 내용은 System Manager 도움말 또는 을 참조하십시오 "ONTAP 9 시스템 관리 참조".
선택 사항: EMS를 구성합니다	EMS(이벤트 관리 시스템)는 Cloud Volumes ONTAP 시스템에서 발생하는 이벤트에 대한 정보를 수집하고 표시합니다. 이벤트 알림을 수신하려면 이벤트 대상(이메일 주소, SNMP 트랩 호스트 또는 syslog 서버)과 이벤트 경로를 특정 이벤트 심각도에 대해 설정할 수 있습니다. CLI를 이용하여 EMS를 구성할 수 있다. 자세한 내용은 를 참조하십시오 "ONTAP 9 EMS 구성 익스프레스 가이드".

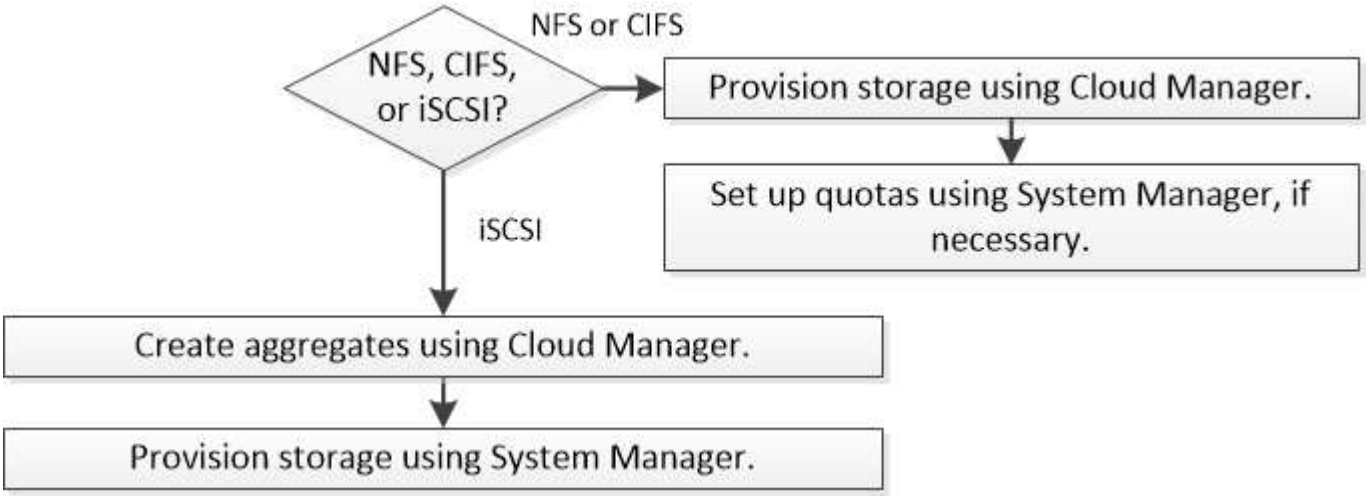
작업	설명
선택 사항: 여러 AWS 가용성 영역의 HA 시스템을 위한 SVM 관리 네트워크 인터페이스(LIF)를 생성합니다	Windows용 SnapCenter 또는 SnapDrive를 HA 쌍으로 사용하려면 스토리지 가상 시스템(SVM) 관리 네트워크 인터페이스(LIF)가 필요합니다. 여러 AWS 가용성 영역에서 HA 쌍을 사용할 때는 SVM 관리 LIF에서 _floating_IP 주소를 사용해야 합니다. HA 쌍을 시작할 때 Cloud Manager에서 부동 IP 주소를 지정하라는 메시지를 표시합니다. IP 주소를 지정하지 않은 경우 System Manager 또는 CLI에서 직접 SVM 관리 LIF를 생성할 수 있습니다. 다음 예에서는 CLI에서 LIF를 생성하는 방법을 보여줍니다. `network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt`
선택 사항: 구성 파일의 백업 위치를 변경합니다	Cloud Volumes ONTAP는 올바르게 작동하는 데 필요한 구성 가능한 옵션에 대한 정보가 포함된 구성 백업 파일을 자동으로 생성합니다. 기본적으로 Cloud Volumes ONTAP는 8시간마다 파일을 Cloud Manager 호스트에 백업합니다. 백업을 대체 위치로 전송하려면 데이터 센터 또는 AWS에서 위치를 FTP 또는 HTTP 서버로 변경할 수 있습니다. 예를 들어, FAS 스토리지 시스템의 백업 위치가 이미 있을 수 있습니다. CLI를 사용하여 백업 위치를 변경할 수 있습니다. 를 참조하십시오 "ONTAP 9 시스템 관리 참조".

스토리지 프로비저닝

스토리지 프로비저닝

볼륨 및 애그리게이트를 관리하여 Cloud Manager에서 Cloud Volumes ONTAP 시스템에 추가 NFS 및 CIFS 스토리지를 프로비저닝할 수 있습니다. iSCSI 스토리지를 생성해야 하는 경우 System Manager에서 생성해야 합니다.

모든 디스크와 애그리게이트는 Cloud Manager에서 직접 생성 및 삭제해야 합니다. 다른 관리 도구에서 이러한 작업을 수행해서는 안 됩니다. 이렇게 하면 시스템 안정성에 영향을 주고 향후 디스크를 추가할 수 없도록 하며 중복 클라우드 공급자 비용을 생성할 수 있습니다.



볼륨 프로비저닝

Cloud Volumes ONTAP 시스템을 시작한 후 더 많은 스토리지가 필요한 경우 Cloud Manager에서 새 NFS 및 CIFS 볼륨을 프로비저닝할 수 있습니다.

시작하기 전에

AWS에서 CIFS를 사용하려면 DNS와 Active Directory를 설정해야 합니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP for AWS의 네트워킹 요구사항".

단계

1. 작업 환경 페이지에서 볼륨을 프로비저닝할 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
2. Aggregate 또는 특정 Aggregate에 새 볼륨을 생성합니다.

조치	단계
새 볼륨을 생성하고 Cloud Manager가 포함된 애그리게이트를 선택하도록 합니다	새 볼륨 추가 * 를 클릭합니다.

조치	단계
특정 애그리게이트에 새 볼륨을 생성합니다	a. 메뉴 아이콘을 클릭한 다음 * 고급 > 고급 할당 * 을 클릭합니다. b. 집계 메뉴를 클릭합니다. c. 볼륨 생성 * 을 클릭합니다.

3. 새 볼륨에 대한 세부 정보를 입력한 다음 * 계속 * 을 클릭합니다.

   이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝의 사용 여부에 따라 크게 달라집니다. 이를 통해 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다.
액세스 제어(NFS에만 해당)	엑스포트 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 Cloud Manager는 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS 전용)	이러한 필드를 사용하면 사용자 및 그룹의 공유에 대한 액세스 수준(액세스 제어 목록 또는 ACL라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자 또는 그룹, UNIX 사용자 또는 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자의 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사본 정책은 자동으로 생성되는 NetApp 스냅샷 복사본의 수와 빈도를 지정합니다. NetApp 스냅샷 복사본은 성능 영향이 없고 최소한의 스토리지가 필요한 시점 파일 시스템 이미지입니다. 기본 정책을 선택하거나 선택하지 않을 수 있습니다. Microsoft SQL Server의 tempdb와 같이 임시 데이터에 대해 없음을 선택할 수 있습니다.

4. CIFS 프로토콜을 선택하고 CIFS 서버가 설정되지 않은 경우 CIFS 서버 생성 대화 상자에서 서버에 대한 세부 정보를 지정한 다음 * 저장 후 계속 * 을 클릭합니다.

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.
도메인에 가입하도록 승인된 자격 증명입니다	AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.
DNS 도메인	SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 대부분의 경우 도메인은 AD 도메인과 동일합니다.

필드에 입력합니다	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 참조하십시오 "Cloud Manager API 개발자 가이드 를 참조하십시오" 를 참조하십시오.

5. 필요한 경우 Usage Profile, Disk Type 및 Tiering Policy 페이지에서 스토리지 효율성 기능을 사용하도록 설정하고 디스크 유형을 선택한 다음 S3 계층화 정책을 편집할지 여부를 선택합니다.

   자세한 내용은 다음을 참조하십시오.

   - "볼륨 사용 프로필 이해"
   - "AWS에서 시스템 사이징"
   - "Azure에서 시스템 사이징"
   - "데이터 계층화 개요"

6. Go * 를 클릭합니다.

결과

Cloud Volumes ONTAP가 볼륨을 프로비저닝합니다.

작업을 마친 후

CIFS 공유를 프로비저닝한 경우 파일 및 폴더에 대한 사용자 또는 그룹 권한을 제공하고 해당 사용자가 공유를 액세스하고 파일을 생성할 수 있는지 확인합니다.

볼륨에 할당량을 적용하려면 System Manager 또는 CLI를 사용해야 합니다. 할당량을 사용하면 사용자, 그룹 또는 qtree가 사용하는 파일 수와 디스크 공간을 제한하거나 추적할 수 있습니다.

HA 구성에서 두 번째 노드의 볼륨 프로비저닝

기본적으로 Cloud Manager는 HA 구성의 첫 번째 노드에 볼륨을 생성합니다. 두 노드에서 모두 클라이언트에 데이터를 제공하는 액티브-액티브 구성이 필요한 경우 두 번째 노드에서 애그리게이트와 볼륨을 생성해야 합니다.

단계

1. 작업 환경 페이지에서 애그리게이트를 관리할 Cloud Volumes ONTAP 작업 환경의 이름을 두 번 클릭합니다.
2. 메뉴 아이콘을 클릭한 다음 * 고급 > 고급 할당 * 을 클릭합니다.
3. Add Aggregate * 를 클릭한 다음 Aggregate를 생성합니다.
4. 홈 노드의 경우 HA 쌍의 두 번째 노드를 선택합니다.
5. Cloud Manager에서 애그리게이트를 생성한 후, 애그리게이트를 선택하고 * 볼륨 생성 * 을 클릭합니다.
6. 새 볼륨에 대한 세부 정보를 입력한 다음 * Create * 를 클릭합니다.

작업을 마친 후

필요한 경우 이 애그리게이트에 볼륨을 추가로 생성할 수 있습니다.

여러 AWS Availability Zone에 구축된 HA 쌍의 경우 볼륨이 상주하는 노드의 부동 IP 주소를 사용하여 볼륨을 클라이언트에 마운트해야 합니다.

애그리게이트 생성

볼륨을 직접 생성하거나 Cloud Manager에서 볼륨을 생성할 때 자동으로 애그리게이트를 생성할 수 있습니다. 애그리게이트를 직접 생성할 때의 이점은 기본 디스크 크기를 선택할 수 있다는 것입니다. 이를 통해 필요한 용량 또는 성능에 맞게 애그리게이트를 크기를 조정할 수 있습니다.

단계

1. 작업 환경 페이지에서 애그리게이트를 관리할 Cloud Volumes ONTAP 인스턴스의 이름을 두 번 클릭합니다.
2. 메뉴 아이콘을 클릭한 다음 * 고급 > 고급 할당 * 을 클릭합니다.
3. Add Aggregate * 를 클릭한 다음 Aggregate에 대한 세부 정보를 지정합니다.

   디스크 유형 및 디스크 크기에 대한 도움말은 를 참조하십시오 "구성 계획".

4. Go * 를 클릭한 다음 * Approve and Purchase * 를 클릭합니다.

iSCSI LUN 프로비저닝

iSCSI LUN을 생성하려면 System Manager에서 생성해야 합니다.

시작하기 전에

- LUN에 접속할 호스트에 Host Utilities를 설치하고 설정해야 합니다.
- 호스트에서 iSCSI 이니시에이터 이름을 기록해야 합니다. LUN에 대한 igroup을 생성할 때 이 이름을 제공해야 합니다.
- System Manager에서 볼륨을 생성하기 전에 충분한 공간이 있는 Aggregate가 있어야 합니다. Cloud Manager에서 애그리게이트를 생성해야 합니다. 자세한 내용은 을 참조하십시오 "애그리게이트 생성".

이 작업에 대해

다음 단계에서는 버전 9.3 이상에서 System Manager를 사용하는 방법을 설명합니다.

단계

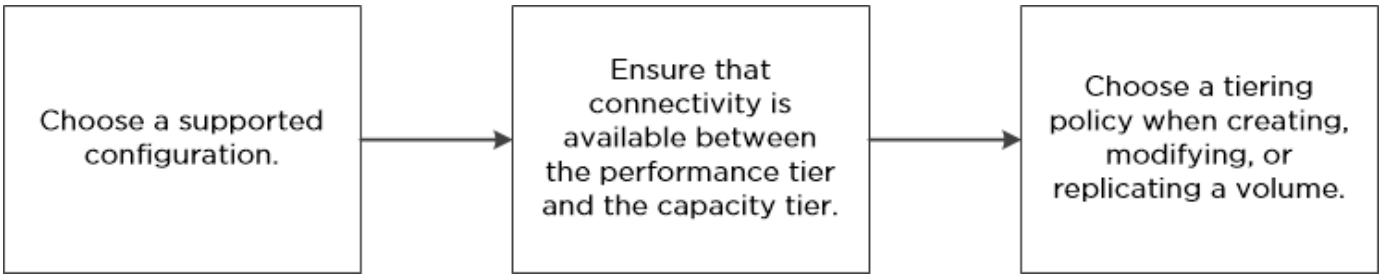
1. "System Manager에 로그인합니다".
2. 스토리지 > LUN * 을 클릭합니다.
3. Create * 를 클릭하고 표시되는 메시지에 따라 LUN을 생성합니다.
4. 호스트에서 LUN에 접속합니다.

   자세한 내용은 를 참조하십시오 "Host Utilities 설명서" 를 참조하십시오.

비활성 데이터를 저비용 오브젝트 스토리지로 계층화

사용 빈도가 높은 데이터를 위한 SSD 또는 HDD 성능 계층과 비활성 데이터를 위한 오브젝트 스토리지 용량 계층을 결합하여 AWS 및 Azure에서 스토리지 비용을 절감할 수 있습니다. 개괄적인 개요는 을 참조하십시오 "데이터 계층화 개요".

데이터 계층화를 설정하려면 다음을 수행하기만 하면 됩니다.



어떤'은 데이터 계층화에 필요하지 않습니다

- 데이터 계층화를 사용하기 위해 기능 라이센스를 설치할 필요는 없습니다.
- 용량 계층(S3 버킷 또는 Azure Blob 컨테이너)을 생성할 필요가 없습니다. Cloud Manager가 이 작업을 수행합니다.

데이터 계층화를 지원하는 구성

특정 구성 및 기능을 사용할 때 데이터 계층화를 설정할 수 있습니다.

- 데이터 계층화는 Cloud Volumes ONTAP Standard, Premium 및 BYOL에서 지원되며, AWS 버전 9.2 및 Microsoft Azure 버전 9.4부터 가능합니다.
  - Microsoft Azure의 HA 쌍에서는 데이터 계층화가 지원되지 않습니다.
  - 데이터 계층화는 DS3_v2 가상 머신 유형의 Azure에서 지원되지 않습니다.
- AWS에서 성능 계층은 범용 SSD, 프로비저닝된 IOPS SSD 또는 처리량 최적화 HDD가 될 수 있습니다.
- Azure에서 성능 계층은 프리미엄 SSD 관리 디스크, 표준 SSD 관리 디스크 또는 표준 HDD 관리 디스크일 수 있습니다.
- 데이터 계층화는 암호화 기술을 통해 지원됩니다.
- 볼륨에 씬 프로비저닝이 설정되어 있어야 합니다.

AWS의 데이터 계층화 요구사항

Cloud Volumes ONTAP가 S3에 연결되어 있는지 확인해야 합니다. 이 연결을 제공하는 가장 좋은 방법은 S3 서비스에 VPC 엔드포인트를 생성하는 것입니다. 자세한 내용은 을 참조하십시오 "AWS 설명서: 게이트웨이 엔드포인트 생성".

VPC 끝점을 만들 때 Cloud Volumes ONTAP 인스턴스에 해당하는 영역, VPC 및 라우팅 테이블을 선택해야 합니다. 또한 S3 엔드포인트에 대한 트래픽을 활성화하는 아웃바운드 HTTPS 규칙을 추가하려면 보안 그룹을 수정해야 합니다. 그렇지 않으면 Cloud Volumes ONTAP에서 S3 서비스에 연결할 수 없습니다.

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

Microsoft Azure의 데이터 계층화 요구사항

Cloud Manager에 필요한 권한이 있는 경우 성능 계층과 용량 계층 간의 연결을 설정할 필요가 없습니다. Cloud Manager 정책에 적절한 권한이 있는 경우 Cloud Manager를 통해 VNET 서비스 엔드포인트를 사용할 수 있습니다.

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

이러한 권한은 최신 에 포함되어 있습니다 "Cloud Manager 정책".

읽기-쓰기 볼륨의 데이터 계층화

Cloud Volumes ONTAP는 읽기-쓰기 볼륨의 비활성 데이터를 비용 효율적인 오브젝트 스토리지에 계층화하여 핫 데이터에 대한 성능 계층을 확보할 수 있습니다.

단계

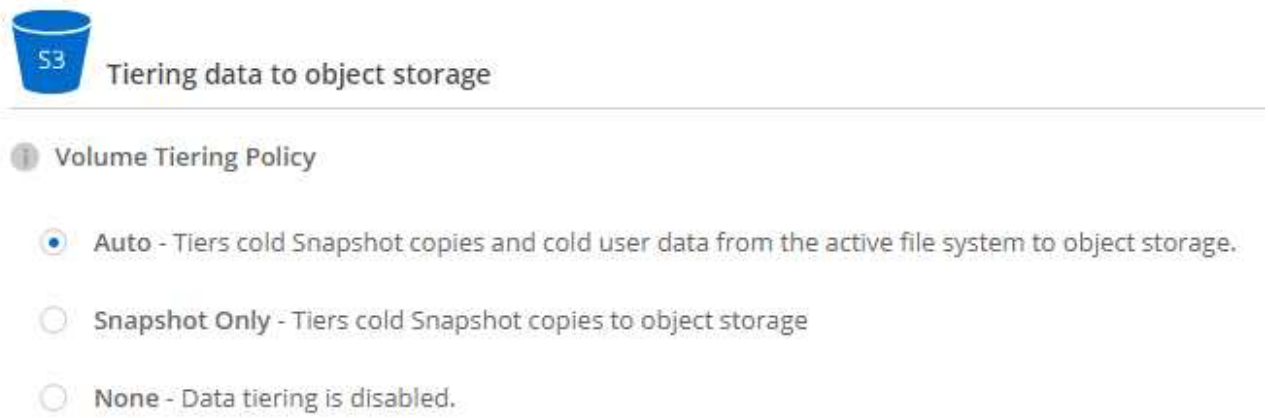
1. 작업 환경에서 새 볼륨을 생성하거나 기존 볼륨의 계층을 변경합니다.

작업	조치
새 볼륨을 생성합니다	새 볼륨 추가 * 를 클릭합니다.
기존 볼륨을 수정합니다	볼륨을 선택하고 * 디스크 유형 및 계층화 정책 변경 * 을 클릭합니다.

2. 스냅샷 전용 정책 또는 자동 정책을 선택합니다.

   이러한 정책에 대한 설명은 를 참조하십시오 "데이터 계층화 개요".

   ◦ 예 *



   데이터 계층화를 지원하는 애그리게이트가 아직 존재하지 않는 경우 Cloud Manager는 볼륨에 대한 새로운 애그리게이트를 생성합니다.

   애그리게이트를 직접 생성하려는 경우, 애그리게이트를 만들 때 애그리게이트에서 데이터 계층화를 설정할 수 있습니다.

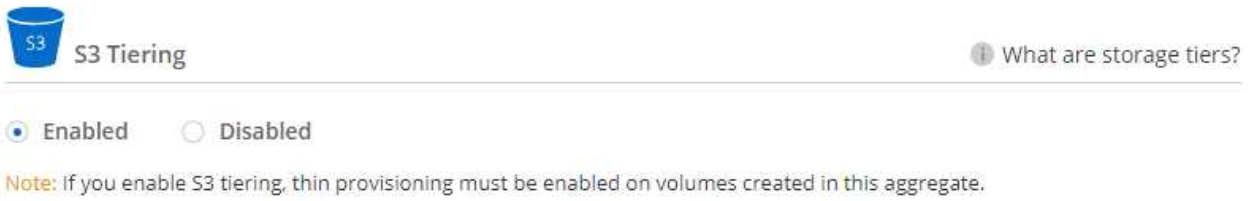
데이터 보호 볼륨의 데이터 계층화

Cloud Volumes ONTAP는 데이터 보호 볼륨의 데이터를 용량 계층으로 계층화할 수 있습니다. 대상 볼륨을 활성화하면 데이터가 읽혀지면서 성능 계층으로 서서히 이동합니다.

단계

1. 작업 환경 페이지에서 소스 볼륨이 포함된 작업 환경을 선택한 다음 볼륨을 복제할 작업 환경으로 끌어다 놓습니다.
2. 표시되는 메시지에 따라 계층화 페이지로 이동한 다음 오브젝트 스토리지에 데이터 계층화를 설정합니다.

    ◦ 예 *



데이터 복제에 대한 도움말은 을 참조하십시오 "클라우드 간 데이터 복제".

계층화 레벨 변경

데이터 계층화를 활성화하면 Cloud Volumes ONTAP은 비활성 데이터를 AWS의 S3_Standard_Storage 클래스 또는 Azure의 _hot_storage 계층에 계층화합니다. Cloud Volumes ONTAP를 구축한 후 30일 동안 액세스하지 않은 비활성 데이터의 계층화 레벨을 변경하여 스토리지 비용을 절감할 수 있습니다. 데이터에 액세스하는 경우 액세스 비용이 더 높아지므로 계층화 수준을 변경하기 전에 이 점을 고려해야 합니다.

이 작업에 대해

계층화 레벨은 볼륨 기준으로 하지 않는 시스템 전체에 적용됩니다.

AWS에서는 30일 동안 사용하지 않을 경우 비활성 데이터가 다음 스토리지 클래스 중 하나로 이동하도록 계층화 레벨을 변경할 수 있습니다.

- 지능형 계층화
- 표준 - 낮은 액세스 빈도
- 단일 영역 - 낮은 액세스 빈도

Azure에서는 30일 동안 사용하지 않으면 비활성 데이터가 _cool_storage 계층으로 이동하도록 계층화 레벨을 변경할 수 있습니다.

계층화 수준의 작동 방법에 대한 자세한 내용은 을 참조하십시오 "데이터 계층화 개요".

단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * 계층화 레벨 * 을 클릭합니다.
2. 계층화 수준을 선택한 다음 * 저장 * 을 클릭합니다.

Kubernetes용 영구 스토리지로 Cloud Volumes ONTAP 사용

Cloud Manager는 의 구축을 자동화할 수 있습니다 "NetApp 트라이던트" Kubernetes 클러스터에서 컨테이너용 영구 스토리지로 Cloud Volumes ONTAP를 사용할 수 있습니다. 시작에 몇 가지 단계가 있습니다.

를 사용하여 Kubernetes 클러스터를 구축하는 경우 "NetApp Kubernetes 서비스"Cloud Manager를 사용하면 NetApp Cloud Central 계정에서 클러스터를 자동으로 검색할 수 있습니다. 이 경우 처음 두 단계를 건너뛰고 3단계부터 시작합니다.

네트워크 연결을 확인합니다

1. Cloud Manager와 Kubernetes 클러스터 간, Kubernetes 클러스터에서 Cloud Volumes ONTAP 시스템까지 네트워크 연결을 사용할 수 있어야 합니다.
2. Trident를 설치할 때 Cloud Manager에서 다음 끝점에 액세스하려면 아웃바운드 인터넷 연결이 필요합니다.

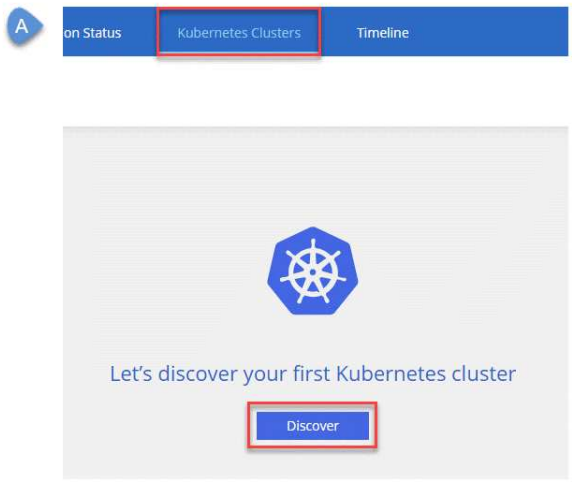
   https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ 으로 문의하십시오

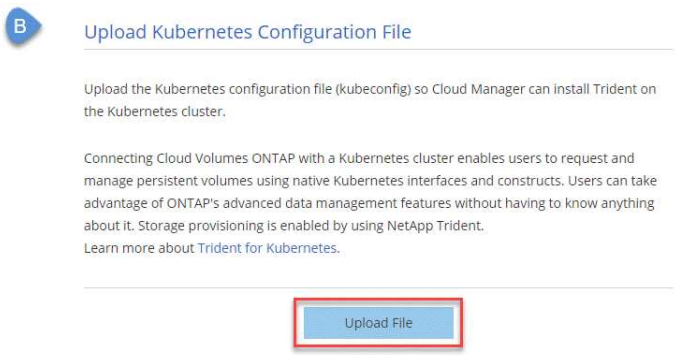
   Cloud Manager는 작업 환경을 클러스터에 연결할 때 Kubernetes 클러스터에 Trident를 설치합니다.

Kubernetes 구성 파일을 **Cloud Manager**에 업로드합니다

각 Kubernetes 클러스터의 Cloud Manager 관리자는 YAML 형식의 구성 파일(kubecononfig)을 업로드해야 합니다. 파일을 업로드하면 Cloud Manager가 클러스터에 대한 연결을 확인하고 kubecon무화파일의 암호화된 복사본을 저장합니다.

Kubernetes 클러스터 > 검색 > 파일 업로드 * 를 클릭하고 kubecononfig 파일을 선택합니다.





작업 환경을 **Kubernetes** 클러스터에 연결합니다

작업 환경에서 Kubernetes 아이콘을 클릭하고 화면의 지시를 따릅니다. 여러 클러스터를 서로 다른 Cloud Volumes ONTAP 시스템에 연결하고 여러 클러스터를 동일한 Cloud Volumes ONTAP 시스템에 연결할 수 있습니다.

NetApp 스토리지 클래스를 Kubernetes 클러스터의 기본 스토리지 클래스로 설정할 수 있습니다. 사용자가 영구 볼륨을 생성할 때 Kubernetes 클러스터는 연결된 Cloud Volumes ONTAP 시스템을 기본적으로 백엔드 스토리지로 사용할 수 있습니다.

영구 볼륨 프로비저닝을 시작합니다

네이티브 Kubernetes 인터페이스 및 구조를 사용하여 영구 볼륨을 요청 및 관리합니다. Cloud Manager에서는 영구 볼륨을 프로비저닝할 때 사용할 수 있는 2개의 Kubernetes 스토리지 클래스를 생성합니다.

- * NetApp-파일 *: 영구 볼륨을 단일 노드 Cloud Volumes ONTAP 시스템에 바인딩하는 데 사용됩니다
- * NetApp-파일-중복 *: 영구 볼륨을 Cloud Volumes ONTAP HA 쌍에 바인딩하는 데 사용됩니다

Cloud Manager는 기본적으로 다음 프로비저닝 옵션을 사용하도록 Trident를 구성합니다.

- 씬 볼륨
- 기본 스냅샷 정책입니다
- 액세스 가능한 스냅샷 디렉토리입니다

"Kubernetes용 Trident를 사용하여 첫 번째 볼륨을 프로비저닝하는 방법에 대해 자세히 알아보십시오"

Triment_triment 볼륨은 얼마입니까?

Cloud Manager는 Kubernetes 클러스터에 연결하는 첫 번째 Cloud Volumes ONTAP 시스템에 볼륨을 생성합니다. 볼륨의 이름은 "_triment_trifent"로 추가됩니다. Cloud Volumes ONTAP 시스템은 이 볼륨을 사용하여 Kubernetes 클러스터에 연결합니다. 이러한 볼륨을 삭제해서는 안 됩니다.

Kubernetes 클러스터를 분리하거나 제거하면 어떻게 됩니까?

Cloud Manager를 사용하면 Kubernetes 클러스터에서 개별 Cloud Volumes ONTAP 시스템의 연결을 끊을 수 있습니다. 시스템의 연결을 끊으면 해당 Cloud Volumes ONTAP 시스템을 더 이상 컨테이너용 영구 스토리지로 사용할 수 없습니다. 기존 영구 볼륨은 삭제되지 않습니다.

Kubernetes 클러스터에서 모든 시스템의 연결을 끊은 후 Cloud Manager에서 전체 Kubernetes 구성을 제거할 수도 있습니다. Cloud Manager는 클러스터를 제거할 때 Trident를 제거하지 않으며 영구 볼륨은 삭제하지 않습니다.

이러한 작업은 모두 API를 통해서만 사용할 수 있습니다. 향후 릴리즈에서 인터페이스에 작업을 추가할 계획입니다."API에 대한 자세한 내용을 보려면 여기를 클릭하십시오".

NetApp 볼륨 암호화로 볼륨 암호화

NetApp Volume Encryption(NVE)은 유휴 데이터를 한 번에 하나의 볼륨으로 암호화하는 소프트웨어 기반 기술입니다. 데이터, 스냅샷 복사본 및 메타데이터가 암호화됩니다. 데이터에 대한 액세스는 볼륨별로 고유한 XTS-AES-256 키를 통해 제공됩니다.

이 작업에 대해

현재 Cloud Volumes ONTAP는 외부 키 관리 서버로 NetApp 볼륨 암호화를 지원합니다. Onboard Key Manager는 지원되지 않습니다.

ONTAP CLI에서 NetApp 볼륨 암호화를 설정해야 합니다. 그런 다음 CLI 또는 System Manager를 사용하여 특정 볼륨에서 암호화를 활성화할 수 있습니다. Cloud Manager는 사용자 인터페이스 및 API에서 NetApp Volume Encryption을 지원하지 않습니다.

"지원되는 암호화 기술에 대해 자세히 알아보십시오".

단계

1. 에서 지원되는 주요 관리자 목록을 검토합니다 "NetApp 상호 운용성 매트릭스 툴".

   Key Managers * 솔루션을 검색합니다.

2. "Cloud Volumes ONTAP CLI에 연결합니다".
3. Cloud Volumes ONTAP 시스템에 NetApp 볼륨 암호화 라이센스를 설치합니다.

   "ONTAP 9 NetApp 암호화 전원 가이드: 라이센스 설치"

4. SSL 인증서를 설치하고 외부 키 관리 서버에 연결합니다.

   "ONTAP 9 NetApp 암호화 전원 가이드: 외부 키 관리 구성"

5. 암호화된 새 볼륨을 생성하거나 CLI 또는 System Manager를 사용하여 암호화되지 않은 기존 볼륨을 변환합니다.
   - CLI:
     - 새 볼륨의 경우 -encrypt 매개 변수와 함께 * volume create * 명령을 사용합니다.

"ONTAP 9 NetApp 암호화 기능 가이드: 새 볼륨에서 암호화 활성화"

- 기존 볼륨의 경우 * volume encryption conversion start * 명령을 사용합니다.

  "ONTAP 9 NetApp 암호화 전원 가이드: 볼륨 암호화 변환 시작 명령을 사용하여 기존 볼륨에서 암호화 사용"

◦ 시스템 관리자:

- 새 볼륨의 경우 * 스토리지 > 볼륨 > 생성 > FlexVol 생성 * 을 클릭한 다음 * 암호화 * 를 선택합니다.

  "시스템 관리자를 사용한 ONTAP 9 클러스터 관리: FlexVol 볼륨 생성"

- 기존 볼륨의 경우 볼륨을 선택하고 * Edit * 를 클릭한 다음 * Encrypted * 를 선택합니다.

  "ONTAP 9 시스템 관리자를 사용한 클러스터 관리: 볼륨 속성 편집"

기존 스토리지 관리

Cloud Manager를 사용하면 볼륨, 애그리게이트, CIFS 서버를 관리할 수 있습니다. 또한 용량 문제를 방지하기 위해 볼륨을 이동하라는 메시지가 표시됩니다.

기존 볼륨 관리

스토리지 요구사항의 변화에 따라 기존 볼륨을 관리할 수 있습니다. 볼륨을 보고, 편집하고, 클론, 복원 및 삭제할 수 있습니다.

단계

1. 작업 환경 페이지에서 볼륨을 관리할 Cloud Volumes ONTAP 작업 환경을 두 번 클릭합니다.
2. 볼륨 관리:

작업	조치
볼륨에 대한 정보를 봅니다	볼륨을 선택한 다음 * 정보 * 를 클릭합니다.
볼륨 편집(읽기-쓰기 볼륨만)	a. 볼륨을 선택한 다음 * 편집 * 을 클릭합니다. b. 볼륨의 스냅샷 정책, NFS 액세스 제어 목록 또는 공유 권한을 수정한 다음 * 업데이트 * 를 클릭합니다.
볼륨의 클론을 생성합니다	a. 볼륨을 선택한 다음 * 클론 * 을 클릭합니다. b. 필요에 따라 클론 이름을 수정한 다음 * Clone * 을 클릭합니다. 이 프로세스에서는 FlexClone 볼륨을 생성합니다. FlexClone 볼륨은 메타데이터에 작은 양의 공간을 사용하고 데이터가 변경 또는 추가됨에 따라 추가 공간만 사용하므로 공간 효율적인 쓰기 가능한 특정 시점 복사본입니다. FlexClone 볼륨에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 논리적 스토리지 관리 가이드".

작업	조치
스냅샷 복사본에서 새 볼륨으로 데이터를 복원합니다	a. 볼륨을 선택한 다음 * 스냅샷 복사본에서 복원 * 을 클릭합니다. b. 스냅샷 복사본을 선택하고 새 볼륨의 이름을 입력한 다음 * 복원 * 을 클릭합니다.
필요 시 스냅샷 복사본을 생성합니다	a. 볼륨을 선택한 다음 * 스냅샷 복사본 생성 * 을 클릭합니다. b. 필요한 경우 이름을 변경한 다음 * 만들기 * 를 클릭합니다.
NFS mount 명령을 가져옵니다	a. 볼륨을 선택한 다음 * 탑재 명령 * 을 클릭합니다. b. 복사 * 를 클릭합니다.
기본 디스크 유형을 변경합니다	a. 볼륨을 선택한 다음 * 디스크 유형 및 계층화 정책 변경 * 을 클릭합니다. b. 디스크 유형을 선택한 다음 * 변경 * 을 클릭합니다. Cloud Manager에서 볼륨을 선택한 디스크 유형을 사용하는 기존 Aggregate로 이동하거나 볼륨에 대한 새 Aggregate를 생성합니다.
계층화 정책을 변경합니다	a. 볼륨을 선택한 다음 * 디스크 유형 및 계층화 정책 변경 * 을 클릭합니다. b. Edit Policy * 를 클릭합니다. c. 다른 정책을 선택하고 * 변경 * 을 클릭합니다. Cloud Manager에서 선택한 디스크 유형을 사용하는 기존 애그리게이트로 볼륨을 이동하거나, 볼륨에 대한 새 애그리게이트를 생성합니다.
볼륨에 대해 S3로 동기화를 활성화 또는 비활성화합니다	볼륨을 선택한 다음 * S3 * 또는 * 동기화 관계 삭제 * 를 클릭합니다. 이 옵션을 사용하려면 먼저 S3로 동기화 기능을 활성화해야 합니다. 자세한 내용은 을 참조하십시오 "데이터를 AWS S3에 동기화 중입니다"
볼륨을 삭제합니다	a. 볼륨을 선택한 다음 * 삭제 * 를 클릭합니다. b. 확인하려면 * 삭제 * 를 다시 클릭합니다.

기존 애그리게이트 관리

디스크를 추가하고, 애그리게이트에 대한 정보를 확인하고, 삭제하여 애그리게이트를 직접 관리하십시오.

시작하기 전에

Aggregate를 삭제하려면 먼저 Aggregate의 볼륨을 삭제해야 합니다.

이 작업에 대해

Aggregate에 공간이 부족할 경우 OnCommand System Manager를 사용하여 볼륨을 다른 애그리게이트로 이동할 수 있습니다.

단계

1. 작업 환경 페이지에서 애그리게이트를 관리할 Cloud Volumes ONTAP 작업 환경을 두 번 클릭합니다.
2. 메뉴 아이콘을 클릭한 다음 * 고급 > 고급 할당 * 을 클릭합니다.
3. 애그리게이트 관리:

작업	조치
Aggregate에 대한 정보를 봅니다	Aggregate를 선택하고 * Info * 를 클릭합니다.
특정 Aggregate에 볼륨을 생성합니다	애그리게이트를 선택하고 * 볼륨 생성 * 을 클릭합니다.
Aggregate에 디스크를 추가합니다	a. 애그리게이트를 선택하고 * AWS 디스크 추가 * 또는 * Azure 디스크 추가 * 를 클릭합니다. b. 추가할 디스크 수를 선택하고 * 추가 * 를 클릭합니다. Aggregate의 모든 디스크는 동일한 크기여야 합니다.
애그리게이트 삭제	a. 볼륨이 없는 Aggregate를 선택하고 * Delete * 를 클릭합니다. b. 확인하려면 * 삭제 * 를 다시 클릭합니다.

CIFS 서버 수정

DNS 서버 또는 Active Directory 도메인을 변경하는 경우 Cloud Volumes ONTAP에서 CIFS 서버를 수정하여 스토리지에서 클라이언트로 계속 서비스를 제공할 수 있도록 해야 합니다.

단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * 고급 > CIFS 설정 * 을 클릭합니다.
2. CIFS 서버에 대한 설정을 지정합니다.

작업	조치
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.
도메인에 가입하도록 승인된 자격 증명입니다	AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.

작업	조치
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.
DNS 도메인	SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 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 참조하십시오 "Cloud Manager API 개발자 가이드 를 참조하십시오" 를 참조하십시오.

3. 저장 * 을 클릭합니다.

결과

Cloud Volumes ONTAP는 CIFS 서버를 변경 사항으로 업데이트합니다.

용량 문제를 피하기 위해 볼륨을 이동합니다

Cloud Manager에서 용량 문제를 방지하려면 볼륨을 이동해야 한다는 작업 필요 메시지를 표시할 수 있지만 문제를 해결하기 위한 권장 사항을 제공할 수 없습니다. 이 경우 문제를 해결하는 방법을 식별한 다음 하나 이상의 볼륨을 이동해야 합니다.

단계

1. 문제를 해결하는 방법을 식별합니다.
2. 분석을 기초로 용량 문제를 방지하려면 볼륨을 이동하십시오.
   - 볼륨을 다른 시스템으로 이동합니다.
   - 동일한 시스템에서 다른 애그리게이트로 볼륨 이동.

용량 문제 해결 방법 파악

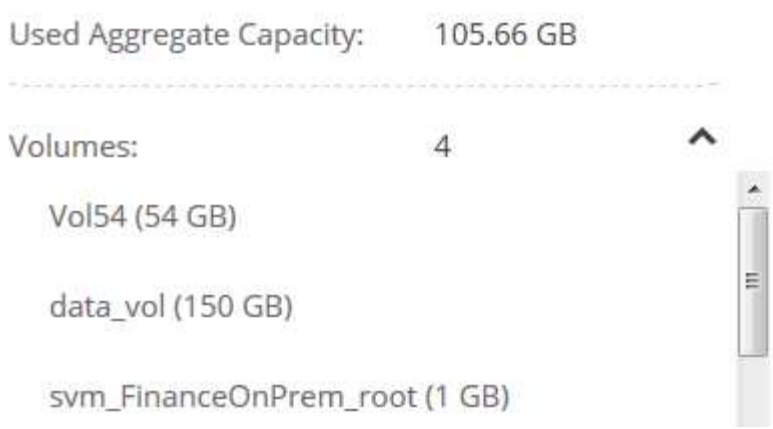
Cloud Manager에서 용량 문제를 피하기 위해 볼륨 이동을 위한 권장 사항을 제공할 수 없는 경우, 이동해야 하는 볼륨을 식별하고 동일한 시스템의 다른 애그리게이트로 이동해야 하는지 또는 다른 시스템으로 이동해야 하는지 여부를 확인해야 합니다.

단계

1. Action Required 메시지의 고급 정보를 확인하여 용량 제한에 도달한 애그리게이트를 식별합니다.

   예를 들어, 고급 정보에는 Aggregate aggr1이 용량 제한에 도달했음을 나타냅니다.

2. 애그리게이트에서 이동할 하나 이상의 볼륨을 식별합니다.
   a. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * 고급 > 고급 할당 * 을 클릭합니다.
   b. 애그리게이트를 선택한 다음 * 정보 * 를 클릭합니다.
   c. 볼륨 목록을 확장합니다.



d. 각 볼륨의 크기를 검토하고 애그리게이트에서 이동할 볼륨을 하나 이상 선택합니다.

나중에 추가 용량 문제를 방지할 수 있도록 aggregate에서 여유 공간을 확보하기 위해 충분히 큰 볼륨을 선택해야 합니다.

3. 시스템이 디스크 제한에 도달하지 않은 경우 볼륨을 동일한 시스템의 기존 애그리게이트 또는 새 aggregate로 이동해야 합니다.

자세한 내용은 을 참조하십시오 "용량 문제를 피하기 위해 볼륨을 다른 애그리게이트로 이동합니다".

4. 시스템이 디스크 제한에 도달한 경우 다음 중 하나를 수행합니다.

a. 사용하지 않는 볼륨을 모두 삭제합니다.

b. 볼륨을 재정렬하여 Aggregate의 여유 공간을 확보하십시오.

자세한 내용은 을 참조하십시오 "용량 문제를 피하기 위해 볼륨을 다른 애그리게이트로 이동합니다".

c. 둘 이상의 볼륨을 공간이 있는 다른 시스템으로 이동합니다.

자세한 내용은 을 참조하십시오 "용량 문제를 방지하기 위해 볼륨을 다른 시스템으로 이동합니다".

용량 문제를 방지하기 위해 볼륨을 다른 시스템으로 이동합니다

용량 문제를 방지하기 위해 하나 이상의 볼륨을 다른 Cloud Volumes ONTAP 시스템으로 이동할 수 있습니다. 시스템이 디스크 제한에 도달한 경우 이 작업을 수행해야 할 수 있습니다.

이 작업에 대해

이 작업의 단계를 따라 다음 작업 필요 메시지를 수정할 수 있습니다.

```
 Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
```

.단계

. 사용 가능한 용량이 있는 Cloud Volumes ONTAP 시스템을 식별하거나 새 시스템을 구축합니다.

. 타겟 작업 환경에서 소스 작업 환경을 끌어다 놓아 볼륨의 일회성 데이터 복제를 수행합니다.

+
자세한 내용은 을 참조하십시오 "시스템 간 데이터 복제".

1. 복제 상태 페이지로 이동한 다음 SnapMirror 관계를 끊어서 복제된 볼륨을 데이터 보호 볼륨에서 읽기/쓰기 볼륨으로 변환합니다.

   자세한 내용은 을 참조하십시오 "데이터 복제 일정 및 관계 관리".

2. 데이터 액세스를 위한 볼륨을 구성합니다.

   데이터 액세스를 위한 대상 볼륨을 구성하는 방법에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 볼륨 재해 복구 익스프레스 가이드".

3. 원래 볼륨을 삭제합니다.

   자세한 내용은 을 참조하십시오 "기존 볼륨 관리".

용량 문제를 피하기 위해 볼륨을 다른 애그리게이트로 이동합니다

용량 문제를 방지하기 위해 하나 이상의 볼륨을 다른 aggregate로 이동할 수 있습니다.

이 작업에 대해

이 작업의 단계를 따라 다음 작업 필요 메시지를 수정할 수 있습니다.

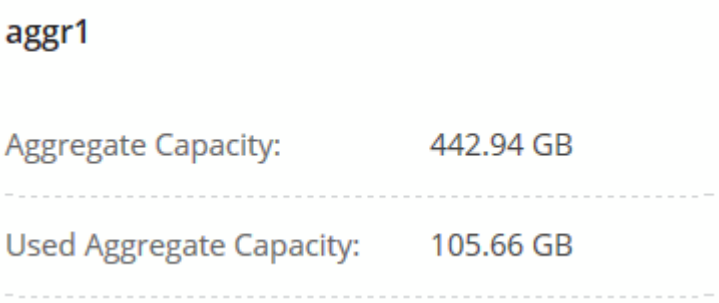
```
 Moving two or more volumes is necessary to avoid capacity issues;
however, Cloud Manager cannot perform this action for you.
```

.단계

. 기존 `Aggregate`에 이동해야 하는 볼륨에 대해 사용 가능한 용량이 있는지 확인합니다.

+
.. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * 고급 > 고급 할당 * 을 클릭합니다.
.. 각 애그리게이트를 선택하고 * 정보 * 를 클릭한 다음 사용 가능한 용량(총 용량에서 사용된 애그리게이트 용량)을 확인합니다.

+



1. 필요한 경우 기존 애그리게이트에 디스크를 추가합니다.
   a. 애그리게이트를 선택한 다음 * 디스크 추가 * 를 클릭합니다.
   b. 추가할 디스크 수를 선택한 다음 * 추가 * 를 클릭합니다.

2. 가용 용량이 있는 애그리게이트가 없는 경우 새 애그리게이트를 생성합니다.

   자세한 내용은 을 참조하십시오 "애그리게이트 생성".

3. System Manager 또는 CLI를 사용하여 볼륨을 애그리게이트로 이동합니다.
4. 대부분의 경우 System Manager를 사용하여 볼륨을 이동할 수 있습니다.

   자세한 내용은 를 참조하십시오 "ONTAP 9 볼륨 이동 익스프레스 가이드".

볼륨 보기에서 NFS 볼륨 프로비저닝

볼륨 보기로 변경합니다

Cloud Manager에서는 두 가지 관리 뷰, 즉 하이브리드 클라우드에서 스토리지 시스템을 관리하는 Storage System View와 스토리지 시스템을 관리할 필요 없이 AWS에서 볼륨을 생성하는 Volume View를 제공합니다. 이러한 보기 사이를 전환할 수 있지만 단일 보기가 사용자의 요구를 충족해야 하므로 이러한 경우는 드뭅니다.

볼륨 보기에 대한 자세한 내용은 을 참조하십시오 "볼륨 보기를 사용하여 스토리지 관리를 간소화했습니다".

단계

1. Cloud Manager 콘솔의 오른쪽 상단에서 메뉴를 클릭한 다음 * 선택 항목 보기 * 를 클릭합니다.
2. 선택 항목 보기 페이지에서 * 스토리지 시스템 보기 * 를 선택한 다음 * 전환 * 을 클릭합니다.

결과

Cloud Manager가 볼륨 보기로 전환됩니다.

NFS 볼륨 생성 및 마운트

Cloud Manager를 사용하여 AWS 스토리지에서 엔터프라이즈급 기능을 제공하는 NFS 볼륨을 생성할 수 있습니다.

NFS 볼륨 생성 중

단일 AWS 인스턴스 또는 다른 인스턴스로 미러링되는 인스턴스에 연결된 볼륨을 생성하여 고가용성을 제공할 수 있습니다.

단계

1. 볼륨 탭에서 * 새 볼륨 생성 * 을 클릭합니다.
2. 새 볼륨 생성 페이지에서 볼륨 유형을 선택합니다.

옵션을 선택합니다	설명
볼륨 생성	단일 AWS 인스턴스에 연결된 볼륨을 생성합니다.

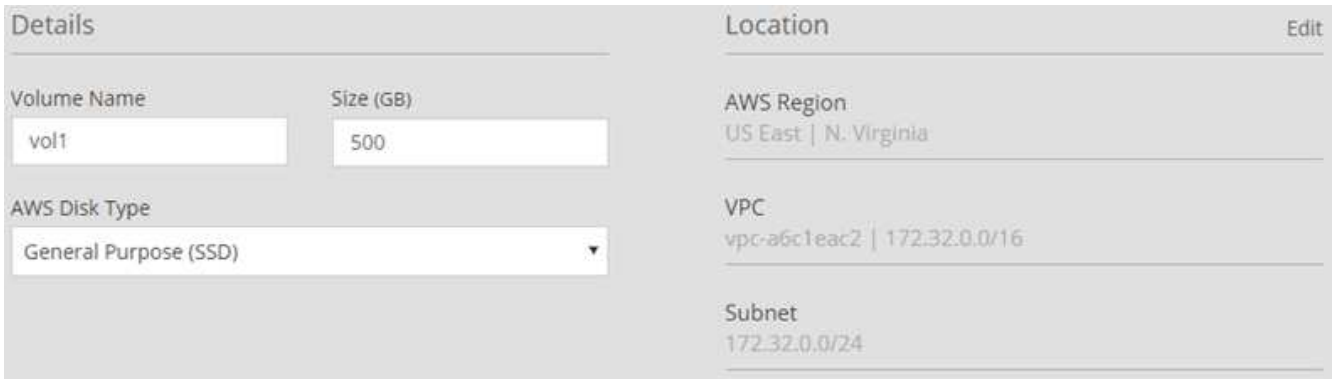
옵션을 선택합니다	설명
HA 볼륨 생성	단일 AWS 인스턴스에 연결된 볼륨을 생성한 후 다른 인스턴스에 미러링하여 장애 발생 시 높은 가용성을 제공합니다. HA 볼륨에 필요한 인스턴스에 대한 추가 세부 정보를 보려면 정보 아이콘을 클릭합니다.

3. 볼륨 생성을 선택한 경우 첫 번째 볼륨에 대한 세부 정보를 지정한 다음 * 생성 * 을 클릭합니다.

   다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
크기	볼륨의 최대 크기는 기존 스토리지 시스템에서 사용할 수 있는 용량에 따라 다릅니다. 볼륨에 씬 프로비저닝이 자동으로 활성화되어 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다. 스토리지 공간을 사전에 할당하는 대신 데이터가 기록될 때 각 볼륨에 공간이 할당됩니다.
AWS 디스크 유형	성능 및 비용 요구사항을 모두 충족하는 디스크를 선택해야 합니다. • 범용 SSD 디스크는 광범위한 워크로드에서 비용과 성능의 균형을 유지합니다. 성능은 IOPS 측면에서 정의됩니다. • 처리량 최적화된 HDD 디스크는 낮은 가격으로 빠르고 일관된 처리량을 필요로 하는 자주 액세스되는 워크로드에 적합합니다. • 콜드 HDD 디스크는 성능이 매우 낮기 때문에 백업 또는 자주 액세스하지 않는 데이터용으로 적합합니다. 처리량이 최적화된 HDD 디스크와 마찬가지로 성능은 처리량 측면에서 정의됩니다. 자세한 내용은 을 참조하십시오 "AWS 설명서:EBS 볼륨 유형".

   다음 이미지는 작성된 볼륨 생성 페이지를 보여줍니다.

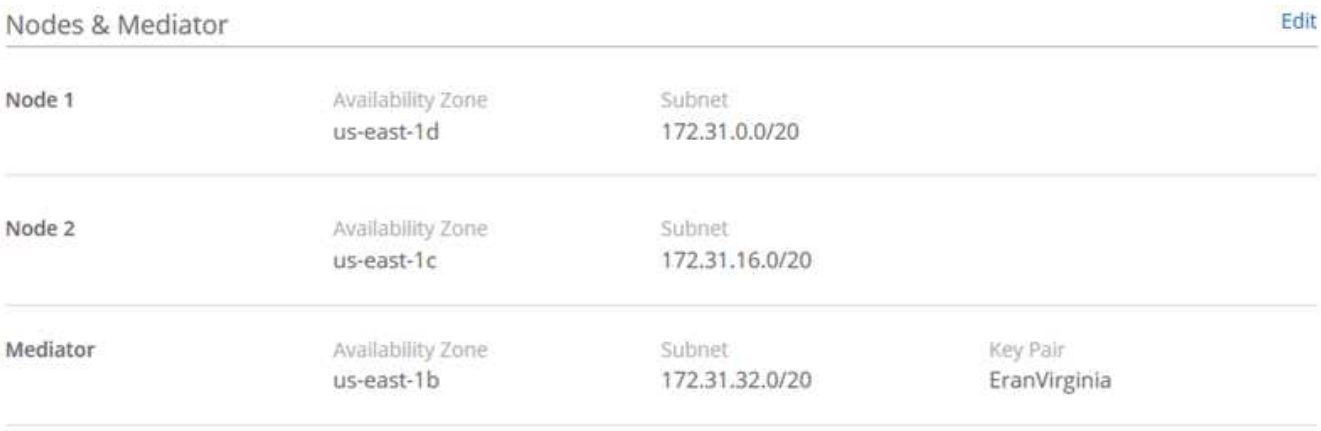


4. HA 볼륨 생성 을 선택한 경우 볼륨에 대한 세부 정보를 지정한 다음 * 생성 * 을 클릭합니다.

   다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
크기	볼륨의 최대 크기는 기존 스토리지 시스템에서 사용할 수 있는 용량에 따라 다릅니다. 볼륨에 씬 프로비저닝이 자동으로 활성화되어 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다. 스토리지 공간을 사전에 할당하는 대신 데이터가 기록될 때 각 볼륨에 공간이 할당됩니다.
AWS 디스크 유형	성능 및 비용 요구사항을 모두 충족하는 디스크를 선택해야 합니다. • 범용 SSD 디스크는 광범위한 워크로드에서 비용과 성능의 균형을 유지합니다. 성능은 IOPS 측면에서 정의됩니다. • 처리량 최적화된 HDD 디스크는 빠르고 일관된 처리량이 필요한 자주 액세스되는 워크로드에 적합합니다. 자세한 내용은 을 참조하십시오 "AWS 설명서:EBS 볼륨 유형".
위치	3개의 서브넷이 포함된 VPC를 3개의 개별 가용성 영역에 선택해야 합니다.
노드 및 중재자	가능한 경우 Cloud Manager는 지원되는 최적의 구성이므로 각 인스턴스에 대해 별도의 가용성 영역을 선택합니다.
유동 IP	IP 주소는 해당 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다.
라우팅 테이블	둘 이상의 라우팅 테이블이 있는 경우 올바른 라우팅 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 HA 쌍에 액세스하지 못할 수 있습니다. 자세한 내용은 을 참조하십시오 "AWS 설명서: 경로 테이블".

다음 이미지는 노드 및 중재자 페이지를 보여 줍니다. 각 인스턴스는 별도의 가용성 영역에 있습니다.



결과

Cloud Manager에서 기존 시스템 또는 새 시스템에 볼륨을 생성합니다. 새 시스템이 필요한 경우 볼륨을 생성하는 데 약 25분이 걸릴 수 있습니다.

Linux 호스트에 볼륨 마운트

볼륨을 생성한 후에는 볼륨을 액세스할 수 있도록 호스트에 마운트해야 합니다.

단계

1. 볼륨 탭에서 마우스 커서를 볼륨 위에 놓고 메뉴 아이콘을 선택한 다음 * 마운트 * 를 클릭합니다.
2. 복사 * 를 클릭합니다.
3. Linux 호스트에서 대상 디렉토리를 변경하여 복사된 텍스트를 수정한 다음 명령을 입력하여 볼륨을 마운트합니다.

NFS 볼륨 관리

NFS 볼륨을 클론 복제, 데이터 액세스 관리, 기본 디스크 유형 변경 등을 통해 관리할 수 있습니다.

볼륨 클론 복제

디스크 공간을 많이 사용하지 않고 데이터의 즉각적인 복사본이 필요한 경우 기존 볼륨의 클론을 생성할 수 있습니다.

이 작업에 대해

클론 복제된 볼륨은 메타데이터에 작은 양의 공간을 사용하고 데이터가 변경 또는 추가됨에 따라 추가 공간만 사용하므로 공간 효율적인 쓰기 가능한 특정 시점 복사본입니다.

단계

1. 볼륨 탭에서 마우스 커서를 볼륨 위에 놓고 메뉴 아이콘을 선택한 다음 * 클론 * 을 클릭합니다.
2. 필요한 경우 클론 복제된 볼륨의 이름을 수정한 다음 * Clone * 을 클릭합니다.

결과

Cloud Manager에서 기존 볼륨의 클론인 새 볼륨을 생성합니다.

볼륨에 대한 데이터 액세스 관리

볼륨을 생성할 때 Cloud Manager를 사용하면 볼륨이 생성된 VPC의 모든 EC2 인스턴스에서 볼륨을 사용할 수 있습니다. 볼륨에 대한 데이터 액세스를 제한해야 하는 경우 이 기본값을 수정할 수 있습니다.

단계

1. 볼륨 탭에서 볼륨 위에 마우스 커서를 놓고 메뉴 아이콘을 선택한 다음 * 액세스 관리 * 를 클릭합니다.
2. 볼륨 액세스 목록을 수정한 다음 * Save * 를 클릭합니다.

볼륨의 기본 **AWS** 디스크를 변경합니다

볼륨이 스토리지를 제공하는 데 사용하는 기본 AWS 디스크를 변경할 수 있습니다. 예를 들어, 더 높은 성능이 필요한 경우 처리량 최적화 HDD에서 범용 SSD로 변경할 수 있습니다.

단계

1. 볼륨 탭에서 마우스 커서를 볼륨 위에 놓고 메뉴 아이콘을 선택한 다음 * 디스크 변경 * 을 클릭합니다.
2. AWS 디스크 유형을 선택하고 * 변경 * 을 클릭합니다.

결과

Cloud Manager에서 볼륨을 선택한 디스크 유형을 사용하는 기존 Aggregate로 이동하거나 볼륨에 대한 새 Aggregate를 생성합니다.

AWS 리소스 보기 및 수정

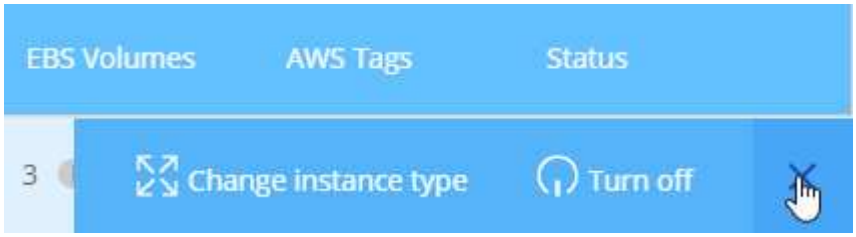
새 볼륨을 생성할 때 Cloud Manager는 해당 볼륨에 필요한 AWS 인스턴스 및 EBS 스토리지를 할당합니다. 필요한 경우 AWS 인스턴스 및 EBS 스토리지에 대한 세부 정보를 보고, 인스턴스 유형을 변경하고, 인스턴스를 설정 및 해제할 수 있습니다.

단계

1. AWS 리소스 * 를 클릭합니다.

   AWS 인스턴스 목록이 표시됩니다. 인스턴스 유형, AWS 위치 및 인스턴스에 연결된 볼륨과 같은 세부 정보를 볼 수 있습니다.

2. 필요한 경우 상태 열 옆에 있는 메뉴 아이콘을 선택한 다음 사용 가능한 작업 중 하나를 선택합니다.



볼륨을 삭제하는 중입니다

더 이상 필요하지 않은 볼륨을 삭제할 수 있습니다.

단계

1. 볼륨 탭에서 마우스 커서를 볼륨 위에 놓고 메뉴 아이콘을 선택한 다음 * 삭제 * 를 클릭합니다.
2. 볼륨 삭제를 확인하려면 * Delete * (삭제 *)를 클릭합니다.

하이브리드 클라우드에서 데이터 관리

ONTAP 클러스터 검색 및 관리

Cloud Manager를 사용하면 사내 환경, NetApp 프라이빗 스토리지 구성 및 IBM 클라우드에서 ONTAP 클러스터를 검색할 수 있습니다. 이 클러스터를 발견하면 Cloud Manager에서 직접 하이브리드 클라우드 환경 전반에서 데이터를 쉽게 복제할 수 있습니다.

ONTAP 클러스터 검색

Cloud Manager에서 ONTAP 클러스터를 검색할 경우 하이브리드 클라우드 전체에서 스토리지를 프로비저닝하고 데이터를 복제할 수 있습니다.

시작하기 전에

클러스터를 Cloud Manager에 추가하려면 클러스터 관리 IP 주소와 admin 사용자 계정의 암호가 있어야 합니다.

Cloud Manager는 HTTPS를 사용하여 ONTAP 클러스터를 검색합니다. 사용자 지정 방화벽 정책을 사용하는 경우 다음 요구 사항을 충족해야 합니다.

- Cloud Manager 호스트는 포트 443을 통한 아웃바운드 HTTPS 액세스를 허용해야 합니다.

  Cloud Manager가 AWS에 있는 경우 모든 아웃바운드 통신은 사전 정의된 보안 그룹에서 허용됩니다.

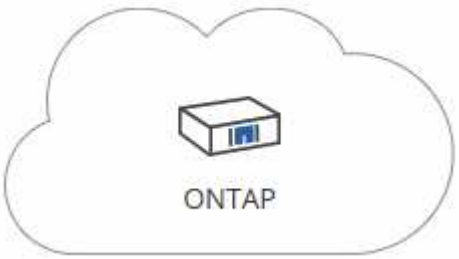
- ONTAP 클러스터는 포트 443을 통한 인바운드 HTTPS 액세스를 허용해야 합니다.

  기본 "관리" 방화벽 정책은 모든 IP 주소에서 인바운드 HTTPS 액세스를 허용합니다. 이 기본 정책을 수정하거나 자체 방화벽 정책을 생성한 경우 HTTPS 프로토콜을 해당 정책에 연결하고 Cloud Manager 호스트에서 액세스를 설정해야 합니다.

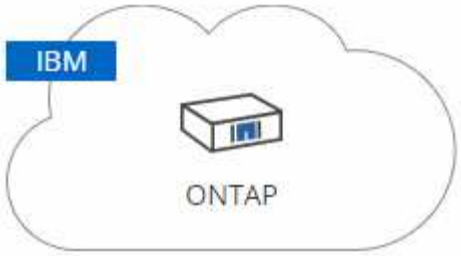
단계

1. 작업 환경 페이지에서 * 작업 환경 추가 * 를 클릭합니다.
2. Discover * 에서 ONTAP 클러스터를 검색할 아이콘 중 하나를 선택합니다.

   다음 아이콘을 사용하여 사내 클러스터 또는 NetApp 프라이빗 스토리지 구성을 검색할 수 있습니다.



   다음 아이콘을 사용하여 IBM 클라우드에서 ONTAP를 검색할 수 있습니다.



3. ONTAP 클러스터 세부 정보 * 페이지에서 클러스터 관리 IP 주소와 admin 사용자 계정의 암호를 입력합니다.

   첫 번째 아이콘을 선택한 경우 사내 클러스터 또는 NetApp 프라이빗 스토리지 구성의 작업 환경 유형도 선택해야 합니다.

4. 세부 정보 페이지에서 작업 환경의 이름과 설명을 입력한 다음 * GO * 를 클릭합니다.

결과

Cloud Manager가 클러스터를 검색합니다. 이제 볼륨을 생성하고, 클러스터에서 데이터를 복제하고, OnCommand System Manager를 시작하여 고급 작업을 수행할 수 있습니다.

ONTAP 클러스터에서 볼륨 프로비저닝

Cloud Manager를 사용하면 ONTAP 클러스터에서 NFS 및 CIFS 볼륨을 프로비저닝할 수 있습니다.

시작하기 전에

NFS 또는 CIFS가 클러스터에 설정되어 있어야 합니다. System Manager 또는 CLI를 사용하여 NFS 및 CIFS를 설정할 수 있습니다.

이 작업에 대해

기존 애그리게이트에서 볼륨을 생성할 수 있습니다. Cloud Manager에서 새 애그리게이트를 생성할 수 없습니다.

단계

1. 작업 환경 페이지에서 볼륨을 프로비저닝할 ONTAP 클러스터의 이름을 두 번 클릭합니다.
2. 새 볼륨 추가 * 를 클릭합니다.
3. 새 볼륨 생성 페이지에서 볼륨에 대한 세부 정보를 입력한 다음 * 생성 * 을 클릭합니다.

   이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝의 사용 여부에 따라 크게 달라집니다. 이를 통해 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다.
액세스 제어(NFS에만 해당)	엑스포트 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 Cloud Manager는 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.

필드에 입력합니다	설명
권한 및 사용자/그룹(CIFS 전용)	이러한 필드를 사용하면 사용자 및 그룹의 공유에 대한 액세스 수준(액세스 제어 목록 또는 ACL라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자 또는 그룹, UNIX 사용자 또는 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자의 도메인을 포함해야 합니다.
사용 프로필	사용 프로필은 볼륨에 대해 활성화된 NetApp 스토리지 효율성 기능을 정의합니다.
스냅샷 정책	스냅샷 복사본 정책은 자동으로 생성되는 NetApp 스냅샷 복사본의 수와 빈도를 지정합니다. NetApp 스냅샷 복사본은 성능 영향이 없고 최소한의 스토리지가 필요한 시점 파일 시스템 이미지입니다. 기본 정책을 선택하거나 선택하지 않을 수 있습니다. Microsoft SQL Server의 tempdb와 같이 임시 데이터에 대해 없음을 선택할 수 있습니다.

클라우드 간 데이터 복제

데이터 전송을 위한 일회성 데이터 복제 또는 재해 복구 또는 장기 보존을 위한 반복 일정을 선택하여 작업 환경 간에 데이터를 복제할 수 있습니다.

Cloud Manager는 SnapMirror 및 SnapVault 기술을 사용하여 개별 시스템의 볼륨 간 데이터 복제를 단순화합니다. 소스 볼륨과 타겟 볼륨을 확인한 다음 복제 정책 및 일정을 선택하기만 하면 됩니다. Cloud Manager는 필요한 디스크를 구매하고 관계를 구성하고 복제 정책을 적용한 다음 볼륨 간 기본 전송을 시작합니다.

기본 전송에는 소스 데이터의 전체 복사본이 포함됩니다. 후속 전송에는 소스 데이터의 차등 복제본이 포함됩니다.

복제 정책을 선택합니다

복제 정책은 스토리지 시스템이 소스 볼륨에서 대상 볼륨으로 데이터를 복제하는 방법을 정의합니다. Cloud Manager에서 데이터 복제를 설정할 때는 복제 정책을 선택해야 합니다.

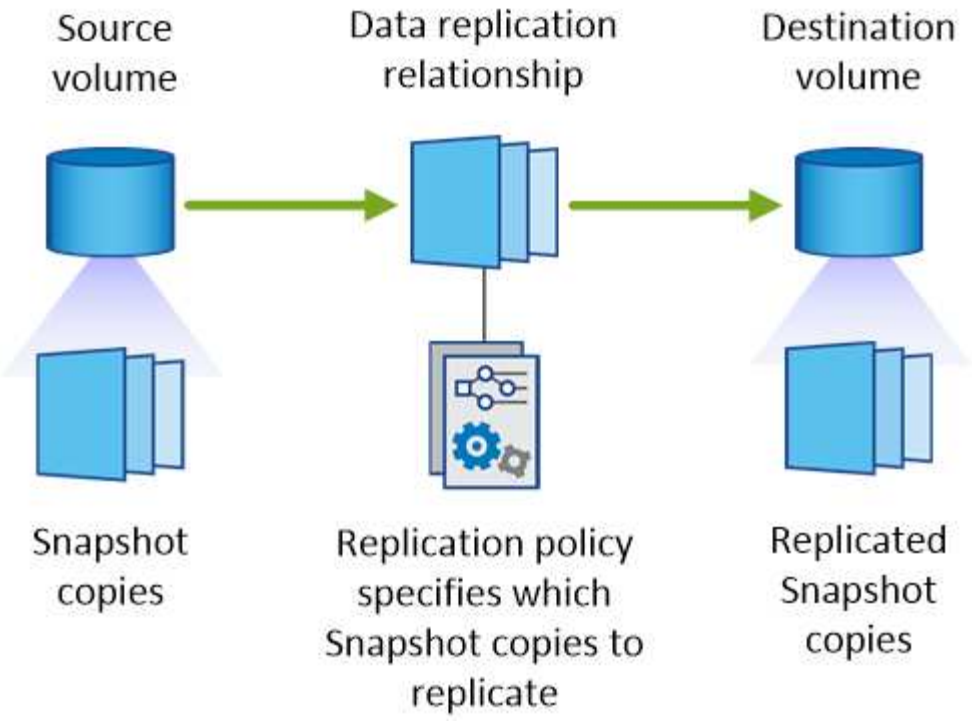
복제 정책의 기능

ONTAP 운영 체제는 스냅샷 복사본이라는 백업을 자동으로 생성합니다. 스냅샷 복사본은 특정 시점의 파일 시스템 상태를 캡처하는 볼륨의 읽기 전용 이미지입니다.

시스템 간에 데이터를 복제할 때 소스 볼륨에서 타겟 볼륨으로 스냅샷 복사본을 복제합니다. 복제 정책은 소스 볼륨에서 타겟 볼륨으로 복제할 스냅샷 복사본을 지정합니다.

복제 정책은 SnapMirror 및 SnapVault 기술을 기반으로 재해 복구 보호 및 D2D 백업 및 복구를 제공하기 때문에 _protection_policies라고도 합니다.

다음 이미지는 스냅샷 복사본과 복제 정책 간의 관계를 보여줍니다.



복제 정책의 유형입니다

다음과 같은 세 가지 유형의 복제 정책이 있습니다.

- Mirror_policy는 새로 생성된 스냅샷 복사본을 대상 볼륨에 복제합니다.

  이러한 스냅샷 복사본을 사용하여 재해 복구 또는 1회 데이터 복제에 대비하여 소스 볼륨을 보호할 수 있습니다. 언제든지 데이터 액세스를 위해 대상 볼륨을 활성화할 수 있습니다.

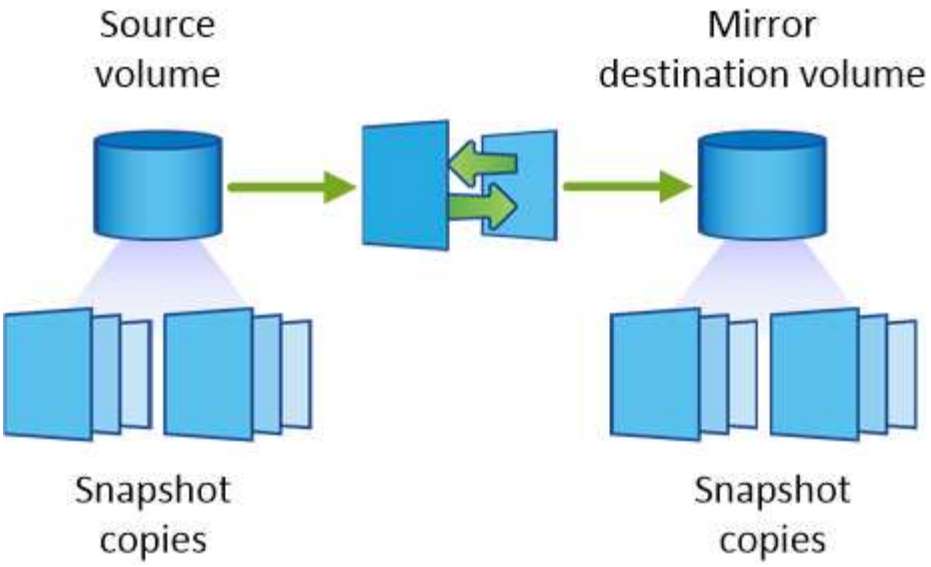
- A_Backup_policy는 특정 스냅샷 복사본을 대상 볼륨에 복제하고 일반적으로 소스 볼륨에서보다 더 오랜 기간 동안 유지합니다.

  데이터가 손상 또는 손실된 경우 이러한 스냅샷 복사본에서 데이터를 복원할 수 있으며 표준 준수 및 기타 거버넌스 관련 목적을 위해 데이터를 보존할 수 있습니다.

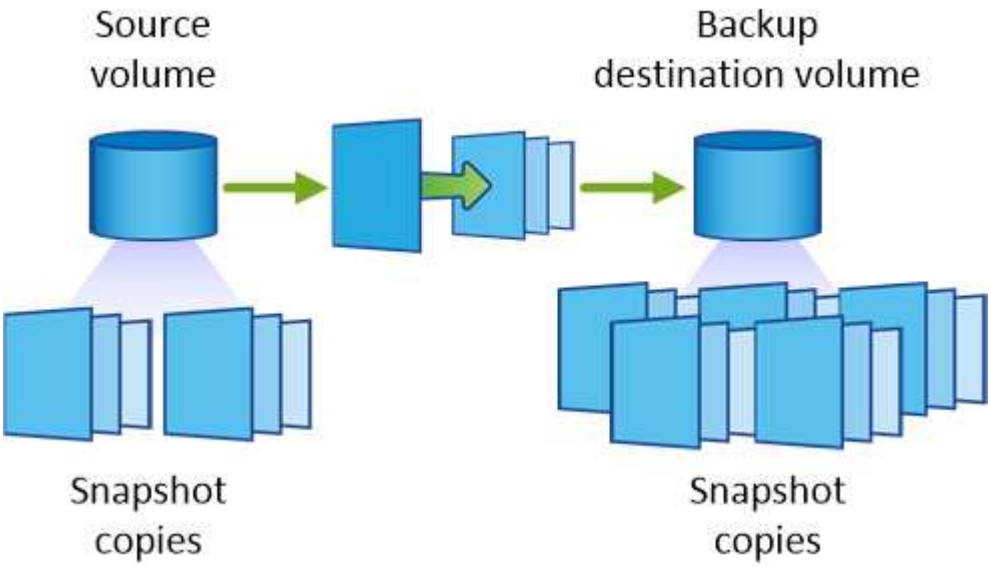
- A_Mirror 및 Backup_policy는 재해 복구와 장기 보존을 모두 제공합니다.

  각 시스템에는 다양한 상황에서 사용할 수 있는 기본 미러 및 백업 정책이 포함되어 있습니다. 사용자 지정 정책이 필요한 경우 System Manager를 사용하여 직접 만들 수 있습니다.

다음 이미지는 미러 정책과 백업 정책의 차이를 보여 줍니다. 미러 정책은 소스 볼륨에서 사용할 수 있는 스냅샷 복사본을 미러링합니다.



백업 정책은 일반적으로 소스 볼륨에 유지되는 것보다 더 오래 스냅샷 복사본을 유지합니다.



백업 정책의 작동 방식

미러 정책과 달리 백업(SnapVault) 정책은 특정 스냅샷 복사본을 타겟 볼륨에 복제합니다. 기본 정책 대신 고유한 정책을 사용하려는 경우 백업 정책의 작동 방식을 이해하는 것이 중요합니다.

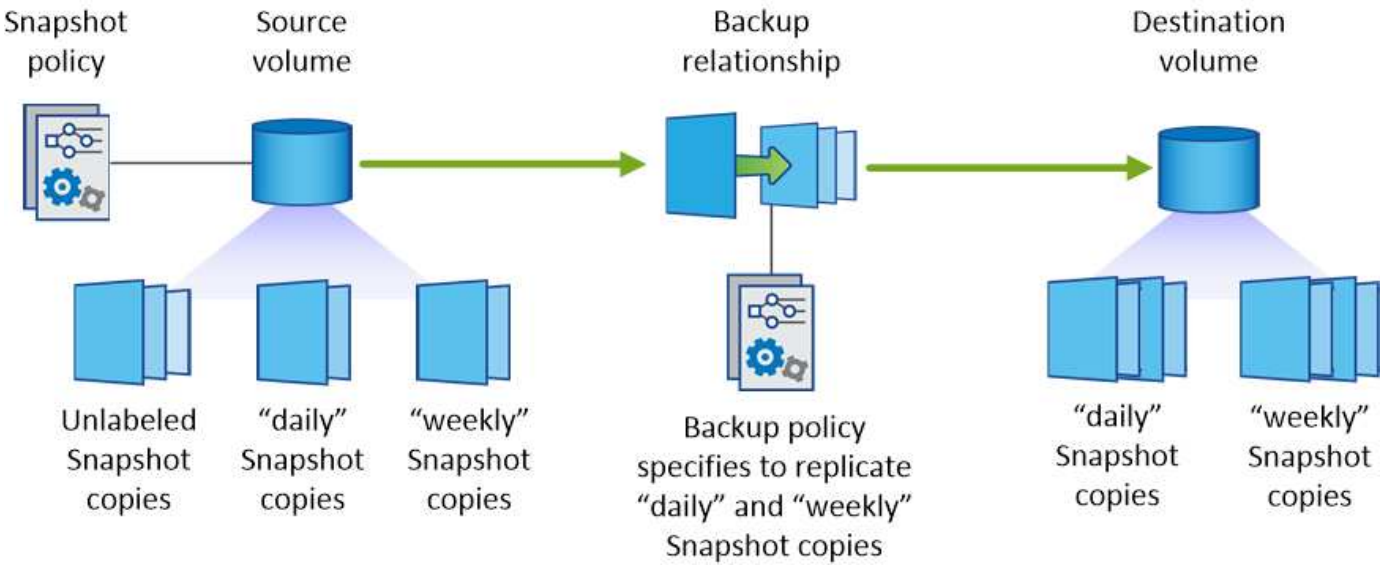
스냅샷 복사본 레이블과 백업 정책 간의 관계 이해

스냅샷 정책은 시스템에서 볼륨의 스냅샷 복사본을 생성하는 방법을 정의합니다. 이 정책에서는 스냅샷 복사본을 생성할 시기, 유지할 복사본 수 및 레이블 지정 방법을 지정합니다. 예를 들어, 시스템이 매일 오전 12:10에 스냅샷 복사본 하나를 생성하고 가장 최근의 복사본 2개를 보관하며 이 복사본을 "매일"이라고 지정할 수 있습니다.

백업 정책에는 레이블이 지정된 Snapshot 복사본을 대상 볼륨에 복제할 볼륨 및 유지할 복사본 수를 지정하는 규칙이 포함되어 있습니다. 백업 정책에 정의된 레이블은 스냅샷 정책에 정의된 하나 이상의 레이블과 일치해야 합니다. 그렇지 않으면 시스템에서 스냅샷 복사본을 복제할 수 없습니다.

예를 들어 "매일" 및 "매주" 레이블이 포함된 백업 정책을 사용하면 이러한 레이블만 포함된 스냅샷 복사본이 복제됩니다.

다음 이미지와 같이 다른 스냅샷 복사본은 복제되지 않습니다.



기본 정책 및 사용자 지정 정책

기본 스냅샷 정책은 매시간, 일별, 주별 스냅샷 복사본을 생성하여 6시간, 2일 및 2개의 주별 스냅샷 복사본을 유지합니다.

기본 스냅샷 정책과 함께 기본 백업 정책을 쉽게 사용할 수 있습니다. 기본 백업 정책은 매일 및 매주 스냅샷 복사본을 복제하며 매일 7개 및 매주 52개의 스냅샷 복사본을 유지합니다.

사용자 지정 정책을 만드는 경우 해당 정책에 정의된 레이블이 일치해야 합니다. System Manager를 사용하여 사용자 지정 정책을 생성할 수 있습니다.

데이터 복제 요구 사항

데이터를 복제하기 전에 Cloud Volumes ONTAP 시스템과 ONTAP 클러스터 모두에 대한 특정 요구사항이 충족되는지 확인해야 합니다.

버전 요구 사항

데이터를 복제하기 전에 소스 볼륨과 타겟 볼륨에서 호환되는 ONTAP 버전이 실행되고 있는지 확인해야 합니다. 자세한 내용은 를 참조하십시오 "데이터 보호 전원 가이드".

Cloud Volumes ONTAP 관련 요구사항

- 인스턴스의 보안 그룹에는 필요한 인바운드 및 아웃바운드 규칙, 특히 ICMP 및 포트 10000, 11104 및 11105에 대한 규칙이 포함되어야 합니다.

  이러한 규칙은 미리 정의된 보안 그룹에 포함되어 있습니다.

- 서로 다른 서브넷에 있는 두 Cloud Volumes ONTAP 시스템 간에 데이터를 복제하려면 서브넷을 함께 라우팅해야 합니다(기본 설정).
- AWS의 Cloud Volumes ONTAP 시스템과 Azure의 시스템 간에 데이터를 복제하려면 AWS VPC와 Azure VNET 간에 VPN 연결이 있어야 합니다.

ONTAP 클러스터별 요구사항

- 활성 SnapMirror 라이센스가 설치되어 있어야 합니다.
- 클러스터가 사내에 있는 경우 회사 네트워크에서 일반적으로 VPN 연결인 AWS 또는 Azure로 연결되어 있어야 합니다.
- ONTAP 클러스터는 추가 서브넷, 포트, 방화벽 및 클러스터 요구사항을 충족해야 합니다.

  자세한 내용은 사용 중인 ONTAP 버전에 대한 클러스터 및 SVM 피어링 익스프레스 가이드를 참조하십시오.

시스템 간 데이터 복제

1회 데이터 복제를 선택하여 Cloud Volumes ONTAP 시스템과 ONTAP 클러스터 간에 데이터를 복제할 수 있습니다. 이 경우 클라우드 간에 데이터를 이동하거나, 재해 복구 또는 장기 보존에 도움이 되는 반복 일정을 선택할 수 있습니다.

이 작업에 대해

Cloud Manager는 단순, 팬아웃 및 계단식 데이터 보호 구성을 지원합니다.

- 간단한 구성에서는 볼륨 A에서 볼륨 B로 복제가 수행됩니다
- 팬아웃 구성에서는 볼륨 A에서 여러 대상으로 복제가 수행됩니다.
- 다중 구간 구성에서는 볼륨 A에서 볼륨 B로, 볼륨 B에서 볼륨 C로 복제가 수행됩니다

시스템 간에 여러 데이터 복제를 설정하여 Cloud Manager에서 팬아웃 및 캐스케이드 구성을 구성할 수 있습니다. 예를 들어, 시스템 A에서 시스템 B로 볼륨을 복제한 다음 시스템 B에서 시스템 C로 동일한 볼륨을 복제합니다

단계

1. 작업 환경 페이지에서 소스 볼륨이 포함된 작업 환경을 선택한 다음 볼륨을 복제할 작업 환경으로 끌어다 놓습니다.

2. 소스 및 대상 피어링 설정 페이지가 나타나면 클러스터 피어 관계에 대한 인터클러스터 LIF를 모두 선택합니다.

   클러스터 피어가 _pair-wise full-mesh 연결_을 가지도록 인터클러스터 네트워크를 구성해야 합니다. 즉, 클러스터 피어 관계의 각 클러스터 쌍이 모든 인터클러스터 LIF 간에 연결을 가지도록 해야 합니다.

   이러한 페이지는 여러 LIF가 있는 ONTAP 클러스터가 소스 또는 대상인 경우 나타납니다.

3. 소스 볼륨 선택 페이지에서 복제할 볼륨을 선택합니다.
4. 대상 볼륨 이름 및 계층화 페이지에서 대상 볼륨 이름을 지정하고, 기본 디스크 유형을 선택하고, 고급 옵션을 변경한 다음 * 계속 * 을 클릭합니다.

   대상이 ONTAP 클러스터인 경우 대상 SVM 및 애그리게이트를 지정해야 합니다.

5. 최대 전송 속도 페이지에서 데이터를 전송할 수 있는 최대 속도(초당 메가바이트)를 지정합니다.
6. 복제 정책 페이지에서 기본 정책 중 하나를 선택하거나 * 추가 정책 * 을 클릭한 다음 고급 정책 중 하나를 선택합니다.

   자세한 내용은 을 참조하십시오 "복제 정책을 선택합니다".

   사용자 지정 백업(SnapVault) 정책을 선택한 경우 정책과 연결된 레이블이 소스 볼륨의 스냅샷 복사본 레이블과 일치해야 합니다. 자세한 내용은 을 참조하십시오 "백업 정책의 작동 방식".

7. 일정 페이지에서 1회 복사본 또는 반복 일정을 선택합니다.

   몇 가지 기본 스케줄을 사용할 수 있습니다. 다른 스케줄을 지정하려면 System Manager를 사용하여 _destination_cluster에 새 스케줄을 생성해야 합니다.

8. 검토 페이지에서 선택 항목을 검토한 다음 * Go * 를 클릭합니다.

결과

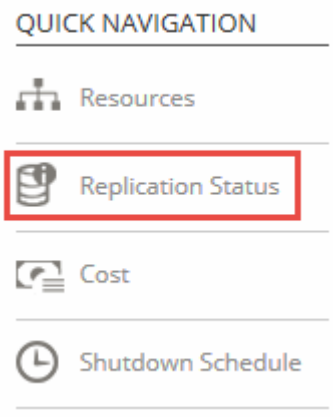
Cloud Manager가 데이터 복제 프로세스를 시작합니다. 복제 상태 페이지에서 복제에 대한 세부 정보를 볼 수 있습니다.

데이터 복제 일정 및 관계 관리

두 시스템 간에 데이터 복제를 설정한 후에는 Cloud Manager에서 데이터 복제 일정과 관계를 관리할 수 있습니다.

단계

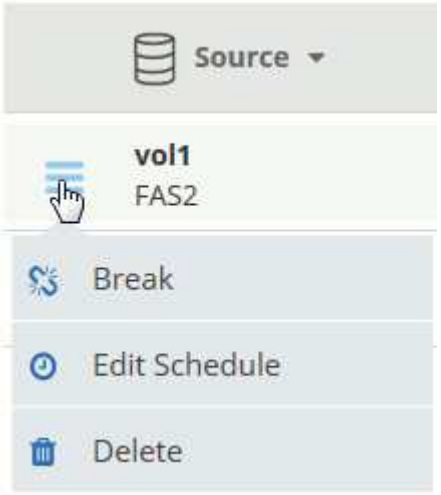
1. 작업 환경 페이지에서 테넌트 또는 특정 작업 환경의 할당된 모든 작업 환경에 대한 복제 상태를 확인합니다.

옵션을 선택합니다	조치
테넌트에서 할당된 모든 작업 환경	탐색 모음에서 복제 상태 를 클릭합니다.
특정 작업 환경	작업 환경을 선택한 다음 복제 상태 를 클릭합니다. 

2. 데이터 복제 관계의 상태를 검토하여 상태가 양호한지 확인합니다.

> 관계의 상태가 유휴 상태이고 미러 상태가 초기화되지 않은 경우 정의된 일정에 따라 데이터 복제가 수행되도록 대상 시스템에서 관계를 초기화해야 합니다. System Manager 또는 CLI(Command-Line Interface)를 사용하여 관계를 초기화할 수 있습니다. 이러한 상태는 대상 시스템에 장애가 발생한 후 다시 온라인 상태가 될 때 나타날 수 있습니다.

3. 소스 볼륨 옆의 메뉴 아이콘을 선택한 다음 사용 가능한 작업 중 하나를 선택합니다.



다음 표에는 사용 가능한 작업이 설명되어 있습니다.

조치	설명
휴식	소스 볼륨과 타겟 볼륨 간의 관계를 끊은 후 데이터 액세스를 위해 타겟 볼륨을 활성화합니다. 이 옵션은 일반적으로 소스 볼륨에서 데이터 손상, 실수로 인한 삭제 또는 오프라인 상태와 같은 이벤트로 인해 데이터를 제공할 수 없는 경우에 사용됩니다. 데이터 액세스를 위한 대상 볼륨을 구성하고 소스 볼륨을 재활성화하는 방법에 대한 자세한 내용은 ONTAP 9 볼륨 재해 복구 익스프레스 가이드를 참조하십시오.
재동기화	볼륨 간의 끊어진 관계를 다시 설정하고 정의된 일정에 따라 데이터 복제를 재개합니다. 볼륨을 재동기화하면 대상 볼륨의 내용이 소스 볼륨의 컨텐츠로 덮어쓰여집니다. 대상 볼륨에서 소스 볼륨으로 데이터를 재동기화하는 역방향 재동기화를 수행하려면 을 참조하십시오 "ONTAP 9 볼륨 재해 복구 익스프레스 가이드".
재동기화	소스 및 대상 볼륨의 역할을 바꿉니다. 원본 소스 볼륨의 컨텐츠는 대상 볼륨의 컨텐츠로 덮어쓰여집니다. 이 기능은 오프라인 상태인 소스 볼륨을 다시 활성화하려는 경우에 유용합니다. 마지막 데이터 복제와 소스 볼륨이 비활성화된 시간 사이에 원본 소스 볼륨에 기록된 데이터는 보존되지 않습니다.
일정 편집	데이터 복제에 다른 스케줄을 선택할 수 있습니다.
정책 정보	에는 데이터 복제 관계에 할당된 보호 정책이 나와 있습니다.
최대 전송 속도를 편집합니다	데이터를 전송할 수 있는 최대 속도(KB/초)를 편집할 수 있습니다.

조치	설명
삭제	소스 볼륨과 타겟 볼륨 간의 데이터 보호 관계를 삭제합니다. 즉, 볼륨 간에 데이터 복제가 더 이상 발생하지 않습니다. 이 작업을 수행해도 데이터 액세스를 위한 대상 볼륨은 활성화되지 않습니다. 이 작업을 수행하면 시스템 간에 다른 데이터 보호 관계가 없는 경우 클러스터 피어 관계 및 SVM(스토리지 가상 시스템) 피어 관계도 삭제됩니다.

결과

작업을 선택하면 Cloud Manager에서 관계 또는 일정을 업데이트합니다.

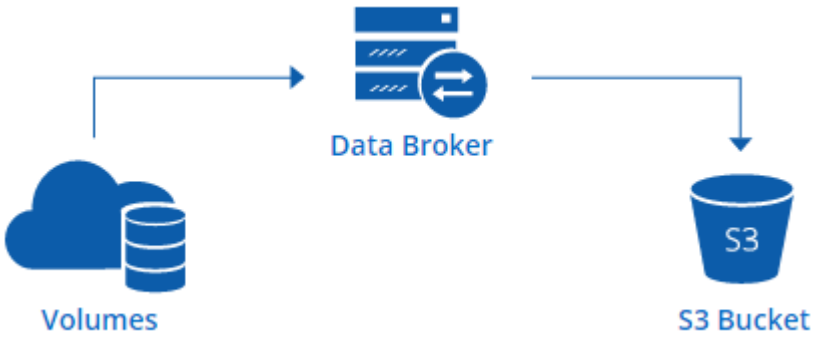
데이터를 AWS S3에 동기화 중입니다

와 작업 환경을 통합하여 ONTAP 볼륨에서 AWS S3 버킷으로 데이터를 동기화할 수 있습니다 "NetApp Cloud Sync를 참조하십시오". 그런 다음, 동기화된 데이터를 2차 복사본으로 사용하거나 EMR 및 Redshift와 같은 AWS 서비스를 사용하여 데이터를 처리할 수 있습니다.

S3로 동기화 기능의 작동 방식

작업 환경을 Cloud Sync 서비스와 언제든지 통합할 수 있습니다. 작업 환경을 통합하면 Cloud Sync 서비스가 선택한 볼륨의 데이터를 단일 S3 버킷으로 동기화합니다. 사내 또는 NPS(NetApp 프라이빗 스토리지) 구성의 일부인 ONTAP 클러스터뿐만 아니라 Cloud Volumes ONTAP 작업 환경과도 통합할 수 있습니다.

데이터를 동기화하려면 VPC에서 데이터 브로커 인스턴스를 시작합니다. Cloud Sync는 작업 환경당 하나의 데이터 브로커를 사용하여 볼륨의 데이터를 S3 버킷으로 동기화합니다. 초기 동기화 후, 서비스는 매일 자정에 변경된 데이터를 한 번 동기화합니다.



고급 Cloud Sync 작업을 수행하려면 Cloud Sync 서비스로 직접 이동합니다. 여기서 S3에서 NFS 서버로 동기화, 볼륨에 대해 다른 S3 버킷 선택, 일정 수정 등의 작업을 수행할 수 있습니다.

S3 동기화 기능은 Cloud Manager Admins 및 Tenant Admins에만 사용할 수 있습니다.

14일 무료 평가판

신규 Cloud Sync 사용자인 경우 처음 14일은 무료입니다. 무료 평가판이 종료된 후에는 각 _SYNC relationship_에 대해 시간당 요율로 지불하거나 라이센스를 구입해야 합니다. S3 버킷에 동기화하는 각 볼륨은 동기화 관계로 간주됩니다. 사용권 설정 페이지에서 Cloud Sync에서 직접 두 결제 옵션을 설정할 수 있습니다.

도움을 받는 방법

Cloud Manager가 S3 기능으로 동기화되거나 일반적으로 Cloud Sync에 대해 지원하는 경우 다음 옵션을 사용합니다.

- 일반 제품 피드백: ng-cloudsync-contact@netapp.com
- 기술 지원 옵션:
  - NetApp Cloud Sync 커뮤니티
  - 제품 내 채팅(Cloud Manager의 오른쪽 아래 모서리)

Cloud Sync 서비스와 작업 환경 통합

Cloud Manager에서 직접 볼륨을 AWS S3에 동기화하려면 작업 환경을 Cloud Sync 서비스와 통합해야 합니다.

[] | *https://img.youtube.com/vi/3hOtLs70_xE/maxresdefault.jpg*

단계

1. 작업 환경을 열고 * S3로 동기화 * 를 클릭합니다.
2. 동기화 * 를 클릭하고 화면의 지시에 따라 데이터를 S3로 동기화합니다.

데이터 보호 볼륨을 S3로 동기화할 수 없습니다. 볼륨은 쓰기 가능해야 합니다.

볼륨 동기화 관계 관리

작업 환경을 Cloud Sync 서비스와 통합한 후 추가 볼륨을 동기화하고 볼륨 동기화를 중지하고 Cloud Sync과의 통합을 제거할 수 있습니다.

단계

1. 작업 환경 페이지에서 동기화 관계를 관리할 작업 환경을 두 번 클릭합니다.
2. 볼륨에 대해 S3로의 동기화를 활성화 또는 비활성화하려면 볼륨을 선택한 다음 * S3로 동기화 * 또는 * 동기화 관계 삭제 * 를 클릭합니다.
3. 작업 환경의 모든 동기화 관계를 삭제하려면 * S3 * 로 동기화 탭을 클릭한 다음 * 동기화 삭제 * 를 클릭합니다.

   이 작업은 S3 버킷에서 동기화된 데이터를 삭제하지 않습니다. 데이터 브로커가 다른 동기화 관계에 사용되지 않는 경우 Cloud Sync 서비스는 데이터 브로커를 삭제합니다.

Cloud Volumes ONTAP 관리

Cloud Volumes ONTAP에 연결 중입니다

Cloud Volumes ONTAP의 고급 관리를 수행해야 하는 경우 OnCommand System Manager 또는 명령줄 인터페이스를 사용하여 관리할 수 있습니다.

OnCommand 시스템 관리자에 연결 중

OnCommand 시스템에서 실행되는 브라우저 기반 관리 툴인 Cloud Volumes ONTAP System Manager에서 Cloud Volumes ONTAP 작업을 수행해야 할 수 있습니다. 예를 들어, LUN을 생성하려면 System Manager를 사용해야 합니다.

시작하기 전에

Cloud Manager에 액세스하는 컴퓨터는 Cloud Volumes ONTAP에 대한 네트워크 연결이 있어야 합니다. 예를 들어, AWS 또는 Azure의 점프 호스트에서 Cloud Manager에 로그인해야 할 수 있습니다.

여러 AWS 가용성 영역에 구축된 Cloud Volumes ONTAP HA 구성에서는 클러스터 관리 인터페이스에 부동 IP 주소를 사용합니다. 즉, 외부 라우팅을 사용할 수 없습니다. 동일한 라우팅 도메인의 일부인 호스트에서 접속해야 합니다.

단계

1. 작업 환경 페이지에서 시스템 관리자로 관리할 Cloud Volumes ONTAP 시스템을 두 번 클릭합니다.
2. 메뉴 아이콘을 클릭한 다음 * 고급 > 시스템 관리자 * 를 클릭합니다.
3. 시작 * 을 클릭합니다.

   System Manager가 새 브라우저 탭에 로드됩니다.
4. 로그인 화면에서 사용자 이름 필드에 * admin * 을 입력하고 작업 환경을 만들 때 지정한 암호를 입력한 다음 * 로그인 * 을 클릭합니다.

결과

System Manager 콘솔이 로드됩니다. 이제 이 기능을 사용하여 Cloud Volumes ONTAP를 관리할 수 있습니다.

Cloud Volumes ONTAP CLI에 연결 중

Cloud Volumes ONTAP CLI를 사용하면 모든 관리 명령을 실행할 수 있으며 고급 작업 또는 CLI를 사용하는 것이 더 편한 경우에 적합합니다. SSH(Secure Shell)를 사용하여 CLI에 연결할 수 있습니다.

시작하기 전에

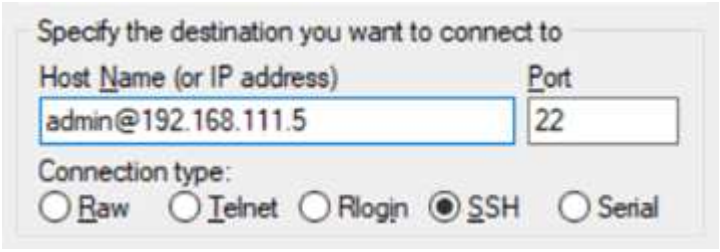
Cloud Volumes ONTAP에 연결하기 위해 SSH를 사용하는 호스트에는 Cloud Volumes ONTAP에 대한 네트워크 연결이 있어야 합니다. 예를 들어, AWS 또는 Azure의 점프 호스트에서 SSH를 사용해야 할 수 있습니다.

여러 AZs에 구축된 Cloud Volumes ONTAP HA 구성에서는 클러스터 관리 인터페이스에 부동 IP 주소를 사용합니다. 즉, 외부 라우팅을 사용할 수 없습니다. 동일한 라우팅 도메인의 일부인 호스트에서 접속해야 합니다.

단계

1. Cloud Manager에서 클러스터 관리 인터페이스의 IP 주소를 확인합니다.
   a. 작업 환경 페이지에서 Cloud Volumes ONTAP 시스템을 선택합니다.
   b. 오른쪽 창에 표시되는 클러스터 관리 IP 주소를 복사합니다.
2. SSH를 사용하여 admin 계정을 사용하여 클러스터 관리 인터페이스 IP 주소에 연결합니다.
   ◦ 예 *

   다음 이미지는 PuTTY를 사용하는 예를 보여 줍니다.



3. 로그인 프롬프트에서 admin 계정의 암호를 입력합니다.
   ◦ 예 *

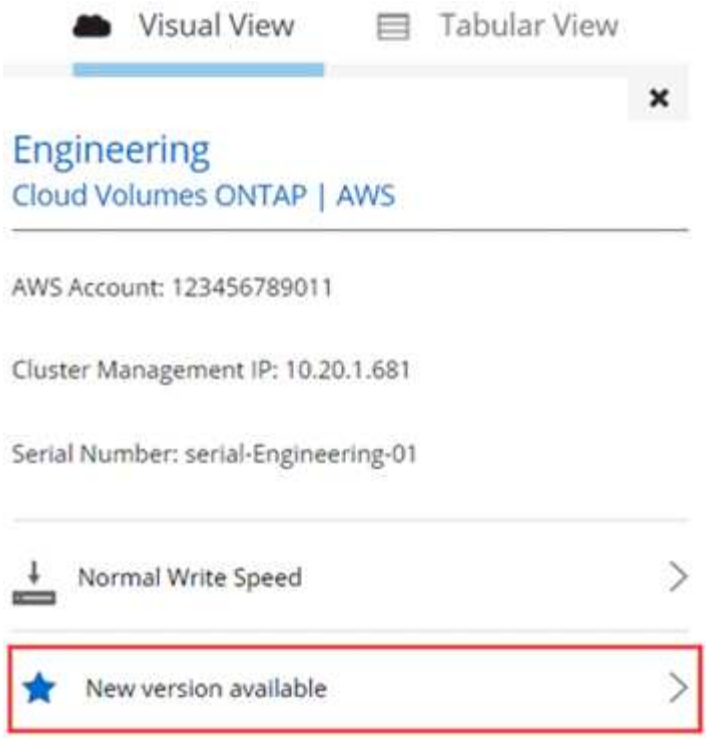
```
Password: ********
COT2::>
```

Cloud Volumes ONTAP 소프트웨어를 업데이트하는 중입니다

Cloud Manager에는 현재 Cloud Volumes ONTAP 릴리즈로 업그레이드하거나 Cloud Volumes ONTAP를 이전 릴리즈로 다운그레이드하는 데 사용할 수 있는 몇 가지 옵션이 포함되어 있습니다. 소프트웨어를 업그레이드하거나 다운그레이드하기 전에 Cloud Volumes ONTAP 시스템을 준비해야 합니다.

개요

새 버전의 Cloud Volumes ONTAP를 사용할 수 있는 경우 Cloud Manager에서 Cloud Volumes ONTAP 작업 환경에 알림을 표시합니다.



이 알림에서 업그레이드 프로세스를 시작하여 S3 버킷에서 소프트웨어 이미지를 가져온 다음 이미지를 설치한 다음 시스템을 다시 시작하여 프로세스를 자동화할 수 있습니다. 자세한 내용은 을 참조하십시오 Cloud Volumes ONTAP를 최신 버전으로 업그레이드 중입니다.

HA 시스템의 경우 Cloud Manager는 업그레이드 프로세스의 일부로 HA 중재자를 업그레이드할 수 있습니다.

소프트웨어 업데이트를 위한 고급 옵션

또한 Cloud Manager는 Cloud Volumes ONTAP 소프트웨어를 업데이트하기 위한 다음과 같은 고급 옵션을 제공합니다.

- 외부 URL의 이미지를 사용하여 소프트웨어를 업데이트합니다

  이 옵션은 Cloud Manager가 S3 버킷에 액세스하여 소프트웨어를 업그레이드할 수 없거나 패치가 제공되었거나 소프트웨어를 특정 버전으로 다운그레이드하려는 경우에 유용합니다.

  자세한 내용은 을 참조하십시오 HTTP 또는 FTP 서버를 사용하여 Cloud Volumes ONTAP 업그레이드 또는 다운그레이드.

- 시스템의 대체 이미지를 사용하여 소프트웨어를 업데이트합니다

  이 옵션을 사용하여 대체 소프트웨어 이미지를 기본 이미지로 만들어 이전 버전으로 다운그레이드할 수 있습니다. HA 쌍에는 이 옵션을 사용할 수 없습니다.

  자세한 내용은 을 참조하십시오 로컬 이미지를 사용하여 Cloud Volumes ONTAP 다운그레이드.

Cloud Volumes ONTAP 소프트웨어 업데이트 준비 중

업그레이드 또는 다운그레이드를 수행하기 전에 시스템이 준비되었는지 확인하고 필요한 구성을 변경해야 합니다.

- 다운타임을 계획 중입니다
- 버전 요구 사항 검토
- SnapMirror 전송 일시 중지
- 애그리게이트가 온라인 상태인지 확인

다운타임을 계획 중입니다

단일 노드 시스템을 업그레이드할 경우 업그레이드 프로세스에서는 I/O가 중단되는 동안 시스템을 최대 25분 동안 오프라인 상태로 전환합니다.

HA 쌍을 무중단 업그레이드할 수 있습니다. 무중단 업그레이드를 통해 HA 2노드에서 두 노드를 동시에 업그레이드하는 동시에 클라이언트에 대한 서비스를 유지할 수 있습니다.

버전 요구 사항 검토

업그레이드 또는 다운그레이드할 수 있는 ONTAP 버전은 현재 시스템에서 실행 중인 ONTAP 버전에 따라 다릅니다.

버전 요구 사항에 대한 자세한 내용은 을 참조하십시오 "ONTAP 9 설명서: 클러스터 업데이트 요구 사항".

SnapMirror 전송 일시 중지

Cloud Volumes ONTAP 시스템에 활성 SnapMirror 관계가 있는 경우 Cloud Volumes ONTAP 소프트웨어를 업데이트하기 전에 전송을 일시 중지하는 것이 좋습니다. 전송을 일시 중단하면 SnapMirror 장애가 방지됩니다. 대상 시스템에서 전송을 일시 중지해야 합니다.

이 작업에 대해

다음 단계에서는 버전 9.3 이상에서 System Manager를 사용하는 방법을 설명합니다.

단계

1. "System Manager에 로그인합니다" 를 대상 시스템에서 선택합니다.
2. 보호 > 관계 * 를 클릭합니다.
3. 관계를 선택하고 * 작업 > 정지 * 를 클릭합니다.

애그리게이트가 온라인 상태인지 확인

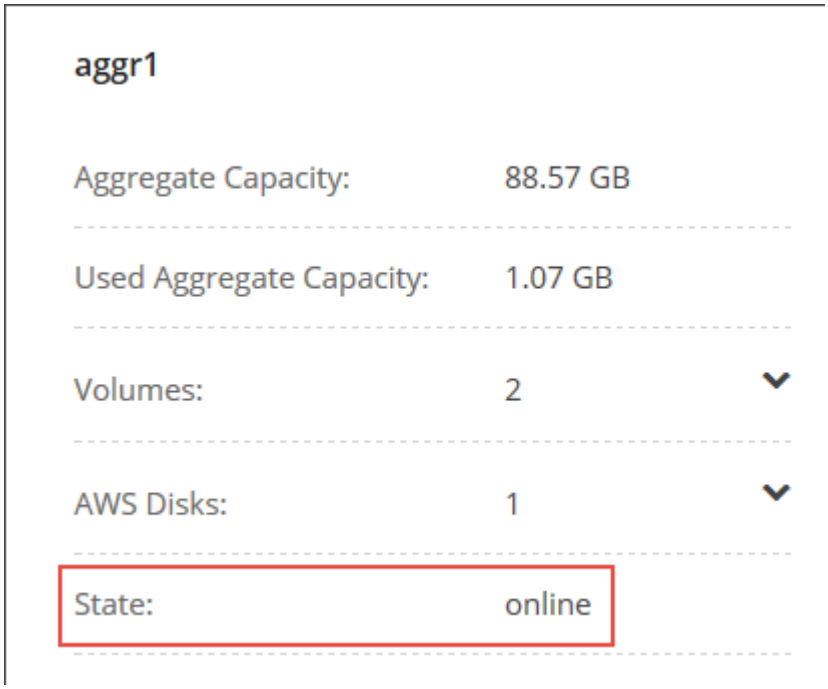
소프트웨어를 업데이트하기 전에 Cloud Volumes ONTAP용 애그리게이트가 온라인 상태여야 합니다. 애그리게이트는 대부분의 구성에서 온라인 상태여야 하지만, 그렇지 않을 경우 온라인 상태로 전환할 수 있습니다.

이 작업에 대해

다음 단계에서는 버전 9.3 이상에서 System Manager를 사용하는 방법을 설명합니다.

단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * 고급 > 고급 할당 * 을 클릭합니다.
2. Aggregate를 선택하고 * Info * 를 클릭한 다음 상태가 온라인인지 확인합니다.



3. 애그리게이트는 오프라인 상태인 경우 System Manager를 사용하여 애그리게이트를 온라인 상태로 전환합니다.
   a. "System Manager에 로그인합니다".
   b. 스토리지 > 애그리게이트 및 디스크 > 애그리게이트 * 를 클릭합니다.
   c. 애그리게이트를 선택한 다음 * 추가 작업 > 상태 > 온라인 * 을 클릭합니다.

Cloud Volumes ONTAP를 최신 버전으로 업그레이드 중입니다

Cloud Manager에서 Cloud Volumes ONTAP의 최신 버전으로 직접 업그레이드할 수 있습니다. Cloud Manager는 새 버전을 사용할 수 있을 때 사용자에게 알립니다.

시작하기 전에

Cloud Volumes ONTAP 시스템에서 볼륨 또는 애그리게이트 생성과 같은 Cloud Manager 작업이 진행 중이지 않아야 합니다.

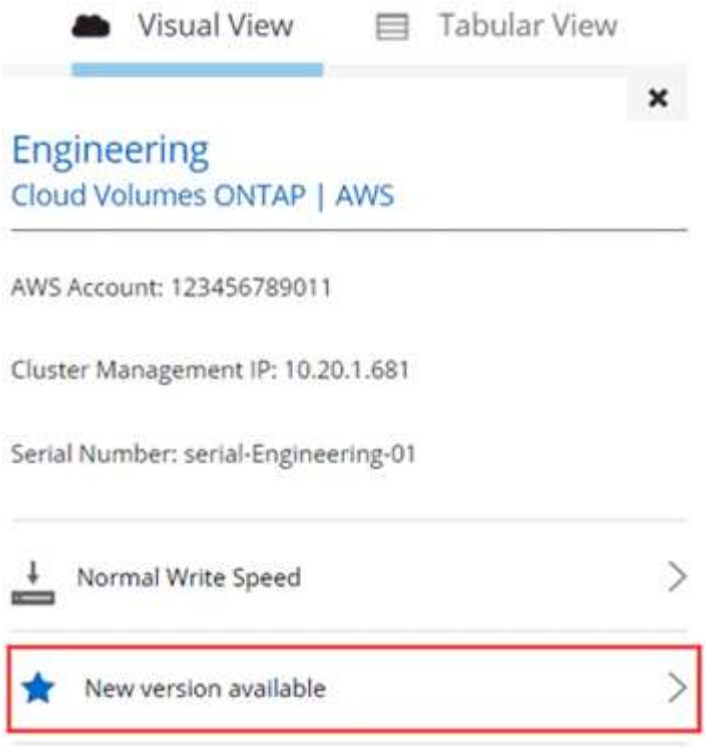
이 작업에 대해

- 단일 노드 시스템을 업그레이드할 경우 업그레이드 프로세스에서는 I/O가 중단되는 동안 시스템을 최대 25분 동안 오프라인 상태로 전환합니다.
- HA 쌍을 무중단 업그레이드할 수 있습니다. 무중단 업그레이드를 통해 HA 2노드에서 두 노드를 동시에 업그레이드하는 동시에 클라이언트에 대한 서비스를 유지할 수 있습니다.

단계

1. 작업 환경 * 을 클릭합니다.
2. 작업 환경을 선택합니다.

   새 버전을 사용할 수 있는 경우 오른쪽 창에 알림이 나타납니다.



3. 새 버전을 사용할 수 있는 경우 * 업그레이드 * 를 클릭합니다.
4. 릴리스 정보 페이지에서 링크를 클릭하여 지정된 버전의 릴리스 정보를 읽은 다음 * 읽었으면… * 확인란을 선택합니다.
5. 최종 사용자 사용권 계약(EULA) 페이지에서 EULA를 읽은 다음 * EULA * 를 읽고 승인합니다 * 를 선택합니다.
6. 검토 및 승인 페이지에서 중요한 메모를 읽고 * 이해했습니다… * 를 선택한 다음 * Go * 를 클릭합니다.

결과

Cloud Manager가 소프트웨어 업그레이드를 시작합니다. 소프트웨어 업데이트가 완료되면 작업 환경에서 작업을 수행할 수 있습니다.

작업을 마친 후

SnapMirror 전송을 일시 중지한 경우 System Manager를 사용하여 전송을 다시 시작합니다.

HTTP 또는 FTP 서버를 사용하여 Cloud Volumes ONTAP 업그레이드 또는 다운그레이드

Cloud Volumes ONTAP 소프트웨어 이미지를 HTTP 또는 FTP 서버에 배치한 다음 Cloud Manager에서 소프트웨어 업데이트를 시작할 수 있습니다. Cloud Manager가 S3 버킷에 액세스하여 소프트웨어를 업그레이드할 수 없거나 소프트웨어를 다운그레이드하려는 경우 이 옵션을 사용할 수 있습니다.

이 작업에 대해

- 단일 노드 시스템을 업그레이드할 경우 업그레이드 프로세스에서는 I/O가 중단되는 동안 시스템을 최대 25분 동안 오프라인 상태로 전환합니다.
- HA 쌍을 무중단 업그레이드할 수 있습니다. 무중단 업그레이드를 통해 HA 2노드에서 두 노드를 동시에 업그레이드하는 동시에 클라이언트에 대한 서비스를 유지할 수 있습니다.

단계

1. Cloud Volumes ONTAP 소프트웨어 이미지를 호스팅할 수 있는 HTTP 서버 또는 FTP 서버를 설정합니다.
2. VPC에 VPN이 연결되어 있는 경우 Cloud Volumes ONTAP 소프트웨어 이미지를 HTTP 서버 또는 FTP 서버에 자신의 네트워크에 배치할 수 있습니다. 그렇지 않으면 AWS의 HTTP 서버 또는 FTP 서버에 파일을 배치해야 합니다.
3. Cloud Volumes ONTAP에 대해 고유한 보안 그룹을 사용하는 경우 Cloud Volumes ONTAP가 소프트웨어 이미지에 액세스할 수 있도록 아웃바운드 규칙이 HTTP 또는 FTP 연결을 허용하는지 확인합니다.

미리 정의된 Cloud Volumes ONTAP 보안 그룹은 기본적으로 아웃바운드 HTTP 및 FTP 연결을 허용합니다.

4. 에서 소프트웨어 이미지를 가져옵니다 "NetApp Support 사이트".
5. 파일을 제공할 HTTP 또는 FTP 서버의 디렉토리에 소프트웨어 이미지를 복사합니다.
6. Cloud Manager의 작업 환경에서 메뉴 아이콘을 클릭한 다음 * 고급 > Cloud Volumes ONTAP 업데이트 * 를 클릭합니다.
7. 소프트웨어 업데이트 페이지에서 * URL * 에서 사용 가능한 이미지 선택 을 선택하고 URL을 입력한 다음 * 이미지 변경 * 을 클릭합니다.
8. 계속하려면 * Proceed * (진행 *)를 클릭합니다.

결과

Cloud Manager가 소프트웨어 업데이트를 시작합니다. 소프트웨어 업데이트가 완료되면 작업 환경에서 작업을 수행할 수 있습니다.

작업을 마친 후

SnapMirror 전송을 일시 중지한 경우 System Manager를 사용하여 전송을 다시 시작합니다.

로컬 이미지를 사용하여 **Cloud Volumes ONTAP** 다운그레이드

동일한 릴리스 제품군(예: 9.5에서 9.4)에서 Cloud Volumes ONTAP를 이전 릴리스로 전환하는 것을 다운그레이드로 합니다. 새 클러스터 또는 테스트 클러스터를 다운그레이드할 때 지원 없이 다운그레이드할 수 있지만 운영 클러스터를 다운그레이드하려면 기술 지원 부서에 문의해야 합니다.

각 Cloud Volumes ONTAP 시스템에는 실행 중인 현재 이미지와 부팅할 수 있는 대체 이미지의 두 소프트웨어 이미지가 포함될 수 있습니다. Cloud Manager에서 대체 이미지를 기본 이미지로 변경할 수 있습니다. 현재 이미지에 문제가 있는 경우 이 옵션을 사용하여 이전 버전의 Cloud Volumes ONTAP로 다운그레이드할 수 있습니다.

이 작업에 대해

이 다운그레이드 프로세스는 단일 Cloud Volumes ONTAP 시스템에서만 사용할 수 있습니다. HA 쌍에는 사용할 수 없습니다. 이 프로세스는 Cloud Volumes ONTAP 시스템을 최대 25분 동안 오프라인 상태로 전환합니다.

단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * 고급 > Cloud Volumes ONTAP 업데이트 * 를 클릭합니다.
2. 소프트웨어 업데이트 페이지에서 대체 이미지를 선택한 다음 * 이미지 변경 * 을 클릭합니다.
3. 계속하려면 * Proceed * (진행 *)를 클릭합니다.

결과

Cloud Manager가 소프트웨어 업데이트를 시작합니다. 소프트웨어 업데이트가 완료되면 작업 환경에서 작업을 수행할

수 있습니다.

작업을 마친 후

SnapMirror 전송을 일시 중지한 경우 System Manager를 사용하여 전송을 다시 시작합니다.

Cloud Volumes ONTAP 시스템 수정

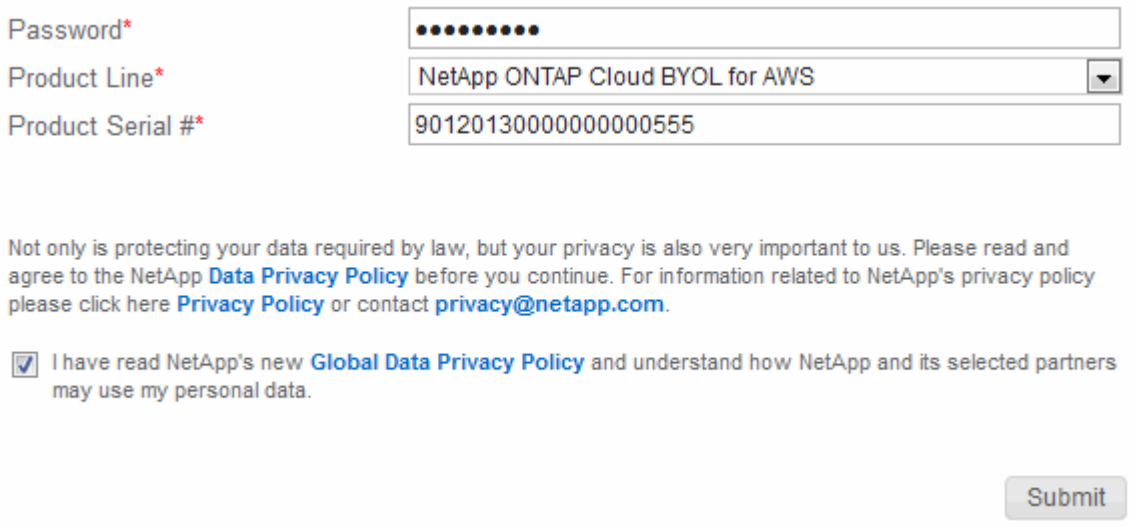
스토리지 요구사항이 변경됨에 따라 Cloud Volumes ONTAP 인스턴스의 구성을 변경해야 할 수 있습니다. 예를 들어 선불 종량제 구성 간에 변경하거나 인스턴스 또는 VM 유형을 변경하고 대체 구독으로 이동할 수 있습니다.

Cloud Volumes ONTAP BYOL 시스템에 라이센스 파일 설치

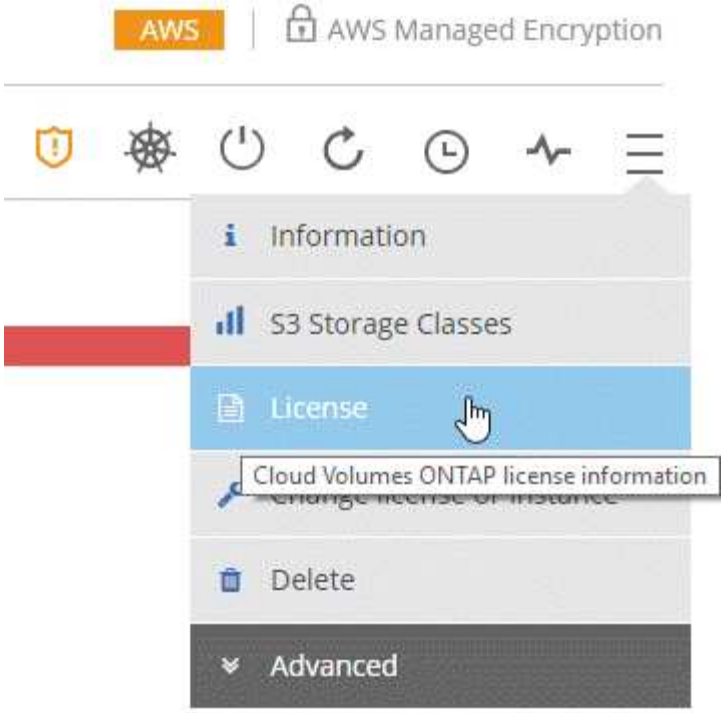
Cloud Manager가 NetApp에서 BYOL 라이센스 파일을 얻을 수 없는 경우 직접 파일을 가져온 다음 파일을 Cloud Manager에 수동으로 업로드하여 Cloud Volumes ONTAP 시스템에 라이센스를 설치할 수 있습니다.

단계

1. 로 이동합니다 "NetApp 라이센스 파일 생성기" 를 입력하고 NetApp Support 사이트 자격 증명을 사용하여 로그인합니다.
2. 암호를 입력하고 제품을 선택한 다음(* NetApp Cloud Volumes ONTAP BYOL for AWS *, * NetApp Cloud Volumes ONTAP BYOL for Azure * 또는 * NetApp Cloud Volumes ONTAP BYOL HA for AWS *), 일련 번호를 입력하고, 개인 정보 보호 정책을 읽고 동의했는지 확인한 다음 * 제출 * 을 클릭합니다.
   - 예 *



3. 이메일 또는 직접 다운로드를 통해 serialnumber.nlf JSON 파일을 수신할지 여부를 선택합니다.
4. Cloud Manager에서 Cloud Volumes ONTAP BYOL 작업 환경을 엽니다.
5. 메뉴 아이콘을 클릭한 다음 * 라이센스 * 를 클릭합니다.



6. 라이센스 파일 업로드 * 를 클릭합니다.
7. 업로드 * 를 클릭한 다음 파일을 선택합니다.

결과

Cloud Manager는 Cloud Volumes ONTAP 시스템에 새 라이센스 파일을 설치합니다.

Cloud Volumes ONTAP의 인스턴스 또는 가상 머신 유형 변경

AWS 또는 Azure에서 Cloud Volumes ONTAP를 시작할 때 여러 인스턴스 또는 가상 머신 유형 중에서 선택할 수 있습니다. 필요에 따라 크기가 작거나 지나치게 큰 것으로 판단될 경우 언제든지 인스턴스 또는 가상 머신 유형을 변경할 수 있습니다.

이 작업에 대해

- Cloud Volumes ONTAP가 다시 시작됩니다.

  단일 노드 시스템의 경우 입출력이 중단됩니다.

  HA 쌍의 경우 변경은 무중단 것입니다. HA 쌍이 계속해서 데이터를 제공합니다.

- 인스턴스 또는 가상 머신 유형을 변경하면 AWS 또는 Azure 서비스 요금이 변경됩니다.

단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * AWS의 라이센스 또는 인스턴스 * 변경 을 클릭하거나 * Azure의 경우 라이센스 또는 VM * 변경 을 클릭합니다.
2. 선불 종량제 구성을 사용하는 경우 필요에 따라 다른 라이센스를 선택할 수 있습니다.
3. 인스턴스 또는 가상 시스템 유형을 선택하고 확인란을 선택하여 변경의 영향을 이해했는지 확인한 다음 * 확인 * 을 클릭합니다.

결과

Cloud Volumes ONTAP가 새 구성으로 재부팅됩니다.

용량제 구성 간 전환

선불 종량제 Cloud Volumes ONTAP 시스템을 시작한 후 언제든지 라이센스를 수정하여 Explore, Standard 및 Premium 구성을 변경할 수 있습니다. 라이센스를 변경하면 물리적 용량 제한이 증가하거나 감소하므로 다양한 EC2 인스턴스 유형 또는 Azure 가상 머신 유형 중에서 선택할 수 있습니다.

이 작업에 대해

선불 종량제 라이센스 간 변경에는 다음과 같은 사항이 있습니다.

- Cloud Volumes ONTAP가 다시 시작됩니다.

  단일 노드 시스템의 경우 입출력이 중단됩니다.

  HA 쌍의 경우 변경은 무중단 것입니다. HA 쌍이 계속해서 데이터를 제공합니다.

- 인스턴스 또는 가상 머신 유형을 변경하면 AWS 또는 Azure 서비스 요금이 변경됩니다.

단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * AWS의 라이센스 또는 인스턴스 * 변경 을 클릭하거나 * Azure의 경우 라이센스 또는 VM * 변경 을 클릭합니다.
2. 사용권 유형과 인스턴스 유형 또는 가상 컴퓨터 유형을 선택하고 확인란을 선택하여 변경의 영향을 이해했는지 확인한 다음 * 확인 * 을 클릭합니다.

결과

Cloud Volumes ONTAP는 새 라이센스, 인스턴스 유형 또는 가상 머신 유형 또는 둘 다를 사용하여 재부팅됩니다.

대체 **Cloud Volumes ONTAP** 구성으로 이동

사용한 만큼만 지불하는 가입과 BYOL 가입형 간에 또는 단일 Cloud Volumes ONTAP 시스템과 HA 쌍 간에 이동하려는 경우, 새 시스템을 구축한 다음 기존 시스템에서 새로운 시스템으로 데이터를 복제할 수 있습니다.

단계

1. 새 Cloud Volumes ONTAP 작업 환경을 만듭니다.

   "AWS에서 Cloud Volumes ONTAP 실행"
   "Azure에서 Cloud Volumes ONTAP 실행"

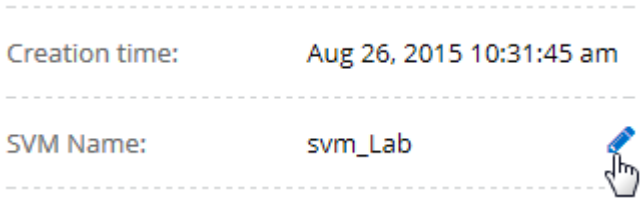
2. "일회성 데이터 복제를 설정합니다" 복제해야 하는 각 볼륨의 시스템 간.
3. 더 이상 필요하지 않은 Cloud Volumes ONTAP 시스템을 종료합니다 "원래 작업 환경 삭제".

스토리지 가상 머신 이름 수정

Cloud Manager에서 Cloud Volumes ONTAP용 스토리지 가상 시스템(SVM)의 이름을 자동으로 지정합니다. 엄격한 명명 규칙이 있으면 SVM의 이름을 수정할 수 있습니다. 예를 들어, ONTAP 클러스터에 대한 SVM의 이름을 일치시킬 수 있습니다.

단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * 정보 * 를 클릭합니다.
2. SVM 이름 오른쪽에 있는 편집 아이콘을 클릭합니다.



3. Modify SVM Name(SVM 이름 수정) 대화 상자에서 SVM 이름을 수정한 다음 * Save *(저장 *)를 클릭합니다.

Cloud Volumes ONTAP 암호 변경

Cloud Volumes ONTAP에는 클러스터 관리자 계정이 포함되어 있습니다. 필요한 경우 Cloud Manager에서 이 계정의 암호를 변경할 수 있습니다.

System Manager 또는 CLI를 통해 admin 계정의 암호를 변경하지 마십시오. 암호는 Cloud Manager에 반영되지 않습니다. 따라서 Cloud Manager에서 인스턴스를 제대로 모니터링할 수 없습니다.

단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * 고급 > 암호 설정 * 을 클릭합니다.
2. 새 암호를 두 번 입력한 다음 * 저장 * 을 클릭합니다.

   새 암호는 마지막으로 사용한 6개의 암호 중 하나와 달라야 합니다.

c4.4x4xLarge 및 c4.8xLarge 인스턴스의 네트워크 MTU 변경

기본적으로 Cloud Volumes ONTAP는 AWS에서 c4.4x4xLarge 인스턴스 또는 c4.8xLarge 인스턴스를 선택할 때 9,000 MTU(점보 프레임이라고도 함)를 사용하도록 구성됩니다. 네트워크 구성에 더 적합한 경우 네트워크 MTU를 1,500바이트로 변경할 수 있습니다.

이 작업에 대해

9,000바이트의 네트워크 최대 전송 단위(MTU)는 특정 구성에 대해 가능한 가장 높은 최대 네트워크 처리량을 제공할 수 있습니다.

9,000 MTU는 동일한 VPC의 클라이언트가 Cloud Volumes ONTAP 시스템과 통신하고 일부 또는 모든 클라이언트가 9,000 MTU를 지원하는 경우에 적합합니다. 트래픽이 VPC를 벗어나면 패킷 조각화가 발생하여 성능이 저하될 수 있습니다.

VPC 외부의 클라이언트 또는 시스템이 Cloud Volumes ONTAP 시스템과 통신할 경우 1,500바이트의 네트워크 MTU가 적합합니다.

단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * 고급 > 네트워크 사용률 * 을 클릭합니다.
2. 표준 * 또는 * 점보 프레임 * 을 선택합니다.

3. 변경 * 을 클릭합니다.

여러 **AWS AZs**에서 **HA** 쌍과 연결된 경로 테이블을 변경합니다

HA 쌍의 부동 IP 주소에 대한 라우트가 포함된 AWS 라우트 테이블을 수정할 수 있습니다. 새로운 NFS 또는 CIFS 클라이언트가 AWS의 HA 쌍에 액세스해야 하는 경우 이 작업을 수행할 수 있습니다.

단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * 정보 * 를 클릭합니다.
2. 배관 테이블 * 을 클릭합니다.
3. 선택한 라우팅 테이블 목록을 수정하고 * 저장 * 을 클릭합니다.

결과

Cloud Manager에서 AWS 요청을 보내 경로 테이블을 수정합니다.

Cloud Volumes ONTAP의 상태 관리

Cloud Volumes ONTAP를 Cloud Manager에서 중지하고 시작하여 클라우드 컴퓨팅 비용을 관리할 수 있습니다.

Cloud Volumes ONTAP의 자동 종료 예약

특정 시간 간격 동안 Cloud Volumes ONTAP를 종료하여 컴퓨팅 비용을 낮출 수 있습니다. 이 작업을 수동으로 수행하는 대신 Cloud Manager를 구성하여 시스템을 자동으로 종료한 다음 특정 시간에 다시 시작할 수 있습니다.

이 작업에 대해

Cloud Volumes ONTAP 시스템의 자동 종료를 예약하면, Cloud Manager가 활성 데이터 전송이 진행 중인 경우 종료를 연기합니다. 전송이 완료된 후 Cloud Manager가 시스템을 종료합니다.

이 작업은 HA 2노드에서 두 노드의 자동 종료를 예약합니다.

단계

1. 작업 환경에서 시계 아이콘을 클릭합니다.

2. 종료 일정을 지정합니다.

   a. 매일, 매주 평일, 매주 또는 세 가지 옵션의 조합을 종료할지 여부를 선택합니다.

   b. 시스템 전원을 끌 시기 및 시스템 전원을 끌 시간을 지정합니다.

      ▪ 예 *

      다음 이미지는 토요일 오전 12시에 Cloud Manager가 시스템을 종료하도록 지시하는 스케줄을 보여줍니다 48시간 동안 Cloud Manager는 매주 월요일 오전 12시에 시스템을 재시작합니다

3. 저장 * 을 클릭합니다.

결과

Cloud Manager가 일정을 저장합니다. 일정이 설정되었음을 나타내기 위해 시계 아이콘이 변경됩니다.

Cloud Volumes ONTAP를 중지하는 중입니다

Cloud Volumes ONTAP를 중지하면 계산 비용이 절약되고 루트 및 부팅 디스크의 스냅샷이 생성되므로 문제 해결에 도움이 됩니다.

이 작업에 대해

HA 쌍을 중지하면 Cloud Manager가 두 노드를 모두 종료합니다.

단계

1. 작업 환경에서 * 끄기 * 아이콘을 클릭합니다.

2. 스냅샷이 시스템 복구를 활성화할 수 있으므로 스냅샷을 생성하는 옵션을 활성 상태로 유지합니다.
3. 끄기 * 를 클릭합니다.

   시스템을 중지하는 데 몇 분 정도 걸릴 수 있습니다. 나중에 작업 환경 페이지에서 시스템을 다시 시작할 수 있습니다.

AWS 리소스 비용 모니터링

Cloud Manager를 사용하면 AWS에서 Cloud Volumes ONTAP를 실행하는 데 따른 리소스 비용을 확인할 수 있습니다. 또한 스토리지 비용을 줄일 수 있는 NetApp 기능을 사용하여 얼마나 많은 비용을 절감할 수 있는지도 확인할 수 있습니다.

이 작업에 대해

페이지를 새로 고치면 Cloud Manager에서 비용이 업데이트됩니다. 최종 비용 세부정보를 보려면 AWS를 참조해야 합니다.

단계

1. Cloud Manager가 AWS에서 비용 정보를 얻을 수 있는지 확인:

   a. Cloud Manager에 권한을 제공하는 IAM 정책에 다음 작업이 포함되어 있는지 확인합니다.

   ```
   "ce:GetReservationUtilization",
   "ce:GetDimensionValues",
   "ce:GetCostAndUsage",
   "ce:GetTags"
   ```

   이러한 작업은 최신 에 포함되어 있습니다 "Cloud Manager 정책". NetApp Cloud Central에서 구축한 새 시스템에 이러한 사용 권한이 자동으로 포함됩니다.

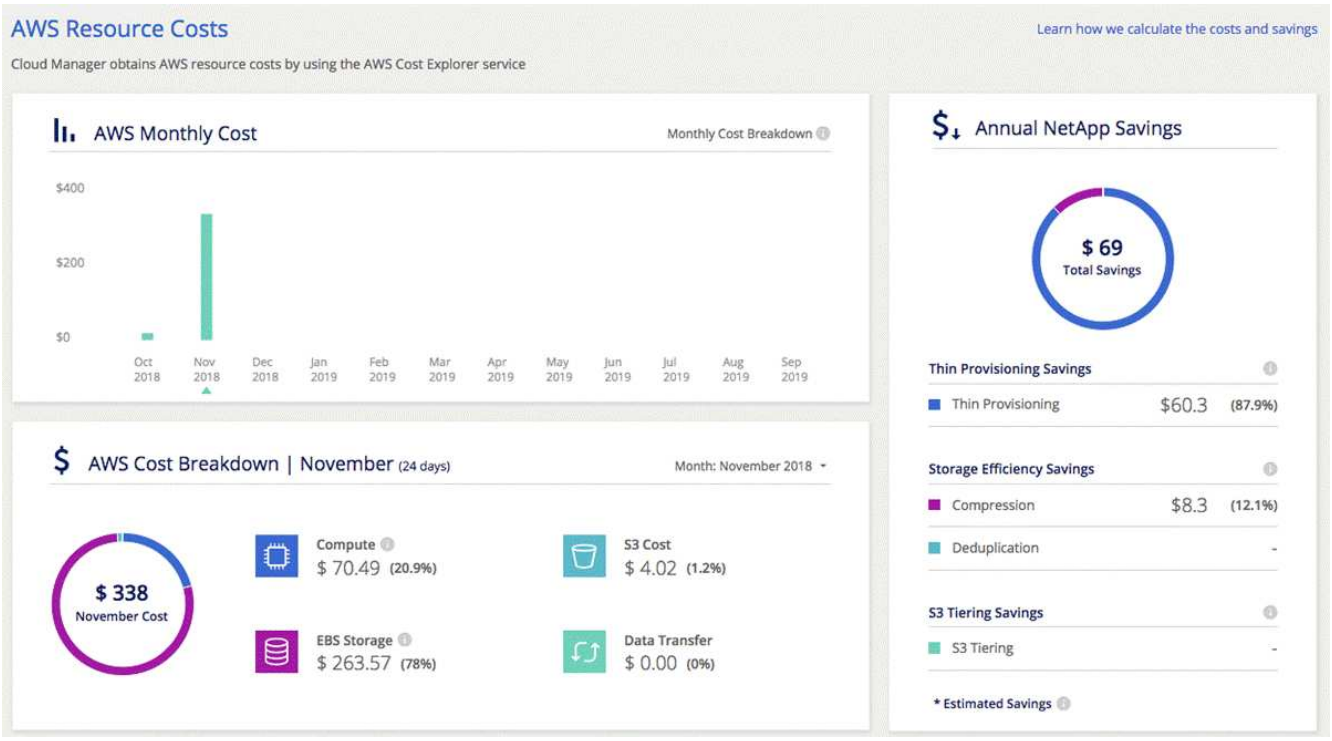
   b. "WorkingEnvironmentId* 태그를 활성화합니다".

   AWS 비용을 추적하기 위해 Cloud Manager에서 Cloud Volumes ONTAP 인스턴스에 비용 할당 태그를 할당합니다. 첫 번째 작업 환경을 만든 후 * WorkingEnvironmentId * 태그를 활성화합니다. 사용자 정의 태그는 청구 및 비용 관리 콘솔에서 활성화할 때까지 AWS 청구 보고서에 나타나지 않습니다.

2. 작업 환경 페이지에서 Cloud Volumes ONTAP 작업 환경을 선택한 다음 * 비용 * 을 클릭합니다.

   Cost 페이지에는 현재 및 이전 달의 비용이 표시되며, 볼륨에 NetApp의 비용 절감 기능을 활성화한 경우 연간 NetApp의 절감액이 표시됩니다.

   다음 이미지는 샘플 비용 페이지를 보여 줍니다.



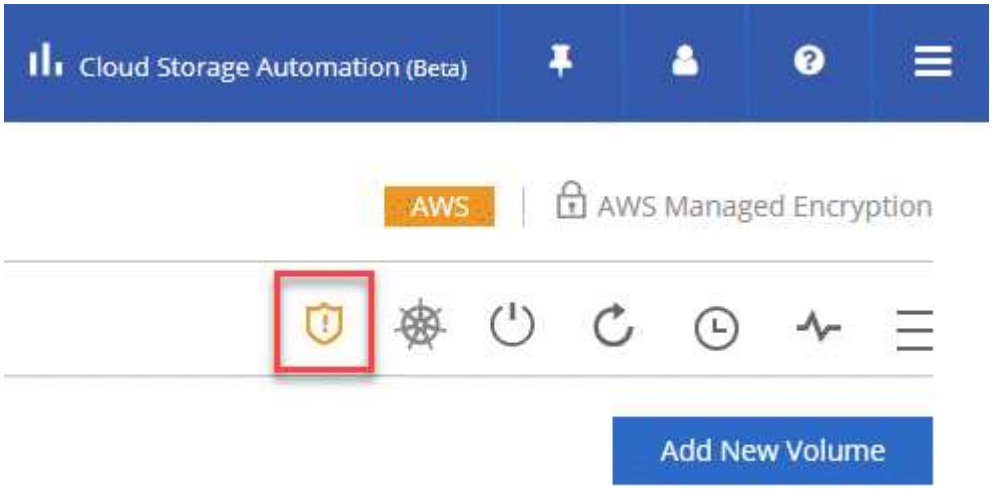
랜섬웨어에 대한 보호 개선

랜섬웨어 공격은 비즈니스 시간, 리소스 및 평판에 악영향을 줄 수 있습니다. Cloud Manager를

사용하면 랜섬웨어에 대한 NetApp 솔루션을 구축하고 가시성, 감지, 문제 해결을 위한 효율적인 툴을 제공할 수 있습니다.

단계

1. 작업 환경에서 * 랜섬웨어 * 아이콘을 클릭합니다.



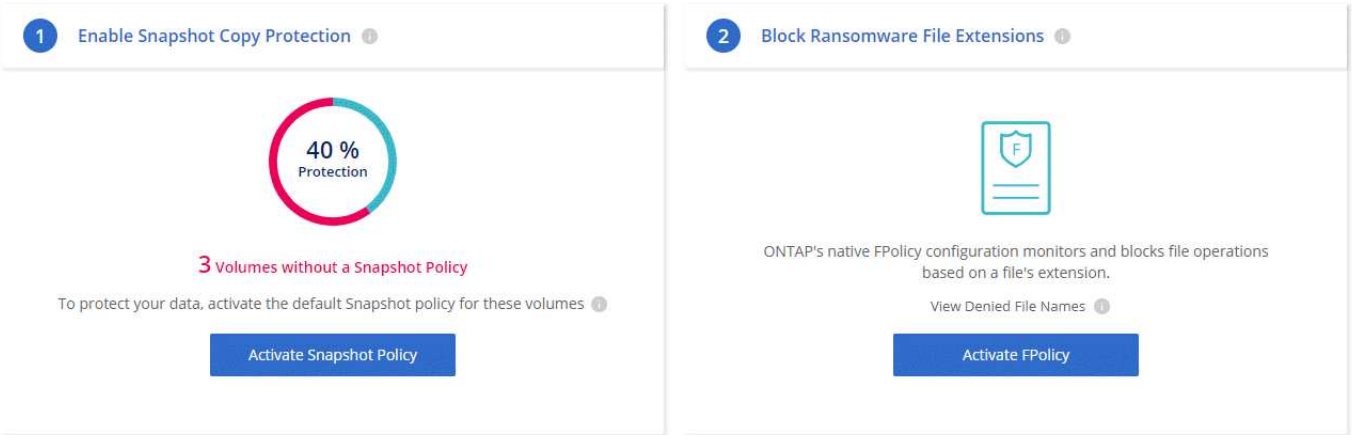
2. 랜섬웨어에 대한 NetApp 솔루션 구현:

   a. 스냅샷 정책이 활성화되지 않은 볼륨이 있는 경우 * 스냅샷 정책 활성화 * 를 클릭합니다.

      NetApp Snapshot 기술은 랜섬웨어 해결을 위한 업계 최고의 솔루션을 제공합니다. 성공적인 복구의 핵심은 감염되지 않은 백업에서 복원하는 것입니다. Snapshot 복사본은 읽기 전용이므로 랜섬웨어 손상을 방지합니다. 또한 세분화하여 단일 파일 복사본 또는 전체 재해 복구 솔루션의 이미지를 생성할 수도 있습니다.

   b. FPolicy * 활성화 를 클릭하여 ONTAP의 FPolicy 솔루션을 활성화합니다. FPolicy 솔루션은 파일의 확장명에 따라 파일 작업을 차단할 수 있습니다.

      이 예방적 솔루션은 일반적인 랜섬웨어 파일 유형을 차단하여 랜섬웨어 공격으로부터 보호를 개선합니다.



Cloud Manager에 기존 Cloud Volumes ONTAP 시스템 추가

기존 Cloud Volumes ONTAP 시스템을 검색하고 Cloud Manager에 추가할 수 있습니다. Cloud Manager 시스템을 사용할 수 없게 되고 새 시스템을 시작했지만 최근 Cloud Manager 백업에서 모든 Cloud Volumes ONTAP 시스템을 복원할 수 없는 경우 이 작업을 수행할 수 있습니다.

시작하기 전에

Cloud Volumes ONTAP admin 사용자 계정의 암호를 알아야 합니다.

단계

1. 작업 환경 페이지에서 * 작업 환경 추가 * 를 클릭합니다.
2. 검색 아래에서 * Cloud Volumes ONTAP * 를 선택합니다.

3. 영역 페이지에서 인스턴스가 실행 중인 영역을 선택한 다음 인스턴스를 선택합니다.
4. 자격 증명 페이지에서 Cloud Volumes ONTAP 관리자 사용자의 암호를 입력한 다음 * GO * 를 클릭합니다.

결과

Cloud Manager는 Cloud Volumes ONTAP 인스턴스를 테넌트에 추가합니다.

Cloud Volumes ONTAP 작업 환경 삭제

AWS 또는 Azure가 아니라 Cloud Manager에서 Cloud Volumes ONTAP 시스템을 삭제하는 것이 좋습니다. 예를 들어, AWS에서 라이센스가 부여된 Cloud Volumes ONTAP 인스턴스를 종료하는 경우 라이센스 키를 다른 인스턴스에 사용할 수 없습니다. 라이센스를 릴리즈하려면 Cloud Manager에서 작업 환경을 삭제해야 합니다.

이 작업에 대해

작업 환경을 삭제하면 Cloud Manager에서 인스턴스 종료, 디스크 삭제 및 스냅샷이 삭제됩니다.

Cloud Volumes ONTAP 인스턴스에는 AWS에서 우발적으로 종료되는 것을 방지하기 위한 종료 보호 기능이 있습니다. 그러나 AWS에서 Cloud Volumes ONTAP 인스턴스를 종료하는 경우 AWS CloudFormation 콘솔로 이동하여 인스턴스의 스택을 삭제해야 합니다. 스택 이름은 작업 환경의 이름입니다.

단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 * 삭제 * 를 클릭합니다.
2. 작업 환경의 이름을 입력한 다음 * 삭제 * 를 클릭합니다.

   작업 환경을 삭제하는 데 최대 5분이 걸릴 수 있습니다.

Cloud Manager 관리

Cloud Manager 업데이트 중

Cloud Manager를 최신 버전으로 업데이트하거나 NetApp 직원이 공유하는 패치를 사용할 수 있습니다.

자동 업데이트 활성화

새로운 버전이 출시되면 Cloud Manager가 자동으로 업데이트됩니다. 이렇게 하면 최신 버전을 실행할 수 있습니다.

이 작업에 대해

실행 중인 작업이 없는 경우 Cloud Manager는 자정 12시에 자동으로 업데이트됩니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 작업 드롭다운 목록을 클릭한 다음 * 설정 * 을 선택합니다.
2. 자동 Cloud Manager 업데이트 아래의 확인란을 선택한 다음 * 저장 * 을 클릭합니다.

Cloud Manager를 최신 버전으로 업데이트하는 중입니다

Cloud Manager에 대한 자동 업데이트를 활성화해야 하지만, 웹 콘솔에서 직접 수동 업데이트를 수행할 수는 있습니다. Cloud Manager는 AWS의 NetApp 소유 S3 버킷에서 소프트웨어 업데이트를 가져옵니다.

시작하기 전에

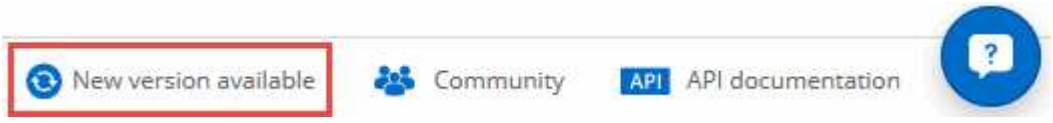
검토를 마친 상태여야 합니다 "릴리스의 새로운 기능" 새로운 요구 사항 및 지원 변경 사항 파악

이 작업에 대해

소프트웨어 업데이트는 몇 분 정도 걸립니다. 업데이트 중에는 Cloud Manager를 사용할 수 없습니다.

단계

1. 콘솔의 오른쪽 아래 모서리를 확인하여 새 버전을 사용할 수 있는지 확인합니다.



2. 새 버전을 사용할 수 있는 경우 * 시각표 * 를 클릭하여 진행 중인 작업이 있는지 확인합니다.

   진행 중인 작업이 있으면 작업이 완료될 때까지 기다린 후 다음 단계를 진행하십시오.

3. 콘솔 오른쪽 하단에서 * 새 버전 사용 가능 * 을 클릭합니다.
4. Cloud Manager 소프트웨어 업데이트 페이지에서 원하는 버전 옆에 있는 * 업데이트 * 를 클릭합니다.
5. 확인 대화 상자를 완료한 다음 * 확인 * 을 클릭합니다.
   a. 필요한 경우 백업을 사용하여 Cloud Manager 구성을 복원할 수 있으므로 백업 다운로드 옵션을 유지하십시오.
   b. 약관을 읽은 다음 * 약관(EULA) * 확인란을 읽고 승인합니다.

6. 메시지가 표시되면 Cloud Manager 백업을 저장합니다.

결과

Cloud Manager가 업데이트 프로세스를 시작합니다. 몇 분 후에 콘솔에 로그인할 수 있습니다.

패치를 사용하여 **Cloud Manager** 업데이트

NetApp이 패치를 공유한 경우 Cloud Manager 웹 콘솔에서 직접 제공되는 패치로 Cloud Manager를 업데이트할 수 있습니다.

이 작업에 대해

패치 업데이트는 일반적으로 몇 분 정도 걸립니다. 업데이트 중에는 Cloud Manager를 사용할 수 없습니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위 모서리에서 작업 드롭다운 목록을 클릭하고 * 업데이트 * 를 선택합니다.
2. 제공된 패치로 Cloud Manager를 업데이트하려면 링크를 클릭합니다.

3. 확인 대화 상자를 완성한 다음 * 확인 * 을 클릭합니다.
   a. 필요한 경우 Cloud Manager 구성을 복원하는 데 사용할 수 있으므로 백업 다운로드 옵션을 활성화합니다.
   b. 약관을 읽은 다음 * 약관(EULA) * 확인란을 읽고 승인합니다.
4. 제공된 패치를 선택합니다.
5. 메시지가 표시되면 Cloud Manager 백업을 저장합니다.

결과

Cloud Manager가 패치를 적용합니다. 몇 분 후에 콘솔에 로그인할 수 있습니다.

Cloud Manager 백업 및 복원

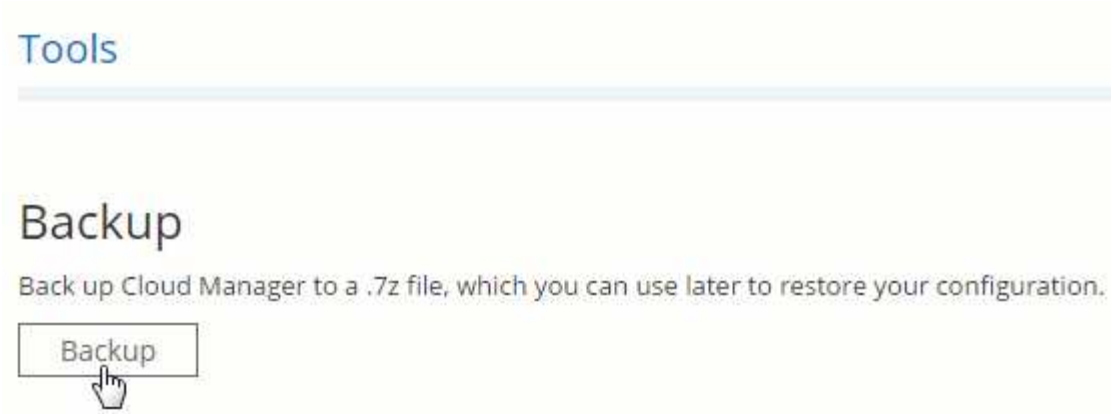
Cloud Manager를 사용하면 데이터베이스를 백업 및 복원하여 구성을 보호하고 문제를 해결할 수 있습니다.

Cloud Manager 백업

Cloud Manager 데이터베이스를 주기적으로 백업하는 것이 좋습니다. 문제가 발생할 경우 이전 백업에서 Cloud Manager를 복원할 수 있습니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 작업 드롭다운 목록을 클릭한 다음 * 도구 * 를 선택합니다.
2. 백업 * 을 클릭합니다.



3. 메시지가 표시되면 필요할 때 검색할 수 있도록 백업 파일을 안전한 위치에 저장합니다.

백업에서 **Cloud Manager** 복원

백업에서 Cloud Manager를 복원하면 기존 데이터가 백업의 데이터로 대체됩니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위 모서리에서 작업 드롭다운 목록을 클릭하고 * 도구 * 를 선택합니다.
2. 복원 * 을 클릭합니다.
3. 확인 * 을 클릭하여 확인합니다.
4. 백업을 선택합니다.

결과

Cloud Manager는 백업 파일에서 데이터베이스를 복원합니다.

Cloud Volumes ONTAP 작업 환경 제거

Cloud Manager 관리자는 Cloud Volumes ONTAP 작업 환경을 제거하여 다른 시스템으로 이동하거나 검색 문제를 해결할 수 있습니다.

이 작업에 대해

Cloud Volumes ONTAP 작업 환경을 제거하면 Cloud Manager에서 제거됩니다. Cloud Volumes ONTAP 시스템은 삭제되지 않습니다. 나중에 작업 환경을 다시 검색할 수 있습니다.

Cloud Manager에서 작업 환경을 제거하면 다음을 수행할 수 있습니다.

- 다른 테넌트에서 다시 검색합니다
- 다른 Cloud Manager 시스템에서 재검색합니다
- 초기 검색 중에 문제가 발생한 경우 다시 검색합니다

단계

1. Cloud Manager 콘솔의 오른쪽 위 모서리에서 작업 드롭다운 목록을 클릭하고 * 도구 * 를 선택합니다.
2. 도구 페이지에서 * 시작 * 을 클릭합니다.

3. 제거할 Cloud Volumes ONTAP 작업 환경을 선택합니다.
4. 검토 및 승인 페이지에서 * 이동 * 을 클릭합니다.

결과

Cloud Manager는 작업 환경을 제거합니다. 사용자는 작업 환경 페이지에서 언제든지 이 작업 환경을 다시 검색할 수 있습니다.

사용자 계정 편집

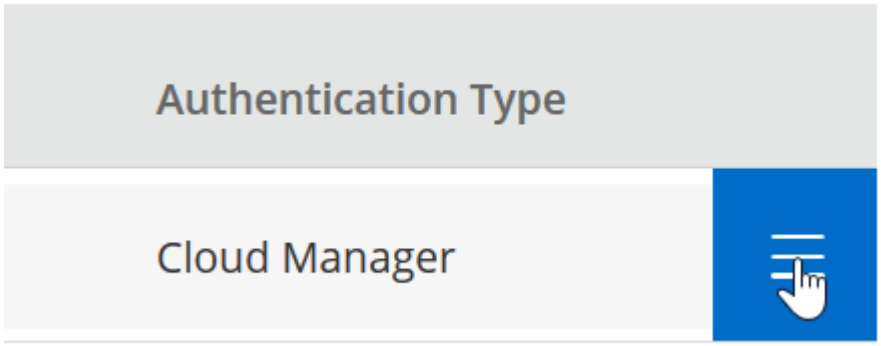
알림 보고서를 설정 및 해제하여 Cloud Manager에서 사용자 계정을 수정할 수 있습니다.

이 작업에 대해

에서 암호와 사용자 정보를 변경해야 합니다 "NetApp Cloud Central에서".

단계

1. Cloud Manager 콘솔의 오른쪽 위 모서리에서 사용자 아이콘을 클릭한 다음 * 사용자 보기 * 를 선택합니다.
2. 행 끝에 있는 메뉴 아이콘을 선택하고 * 사용자 편집 * 을 클릭합니다.



3. 사용자 설정 페이지에서 사용자 계정을 수정합니다.

프록시 서버를 사용하도록 **Cloud Manager** 구성

Cloud Manager를 처음 배포할 때 시스템에 인터넷에 액세스할 수 없는 경우 프록시 서버를 입력하라는 메시지가 표시됩니다. Cloud Manager의 설정에서 프록시를 수동으로 입력하고 수정할 수도 있습니다.

이 작업에 대해

회사 정책에 따라 인터넷에 대한 모든 HTTP 통신에 프록시 서버를 사용해야 하는 경우, 해당 프록시 서버를 사용하도록 Cloud Manager를 구성해야 합니다. 프록시 서버는 클라우드 또는 네트워크에 있을 수 있습니다.

프록시 서버를 사용하도록 Cloud Manager를 구성하면 Cloud Manager, Cloud Volumes ONTAP 및 HA 중재자가 모두 프록시 서버를 사용합니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위 모서리에서 작업 드롭다운 목록을 클릭한 다음 * 설정 * 을 선택합니다.

2. HTTP 프록시 아래에서 구문을 사용하여 서버를 입력합니다 http://address:port, 서버에 기본 인증이 필요한 경우 사용자 이름과 암호를 지정한 다음 * 저장 * 을 클릭합니다.

   Cloud Manager는 @ 문자를 포함하는 암호를 지원하지 않습니다.

결과

프록시 서버를 지정하면 AutoSupport 메시지를 보낼 때 프록시 서버를 사용하도록 새 Cloud Volumes ONTAP 시스템이 자동으로 구성됩니다. 사용자가 Cloud Volumes ONTAP 시스템을 생성하기 전에 프록시 서버를 지정하지 않으면 시스템 관리자를 사용하여 각 시스템의 AutoSupport 옵션에서 프록시 서버를 수동으로 설정해야 합니다.

Cloud Manager HTTPS 인증서를 갱신하는 중입니다

Cloud Manager 웹 콘솔에 안전하게 액세스하려면 만료되기 전에 Cloud Manager HTTPS 인증서를 갱신해야 합니다. 만료되기 전에 인증서를 갱신하지 않으면 사용자가 HTTPS를 사용하여 웹 콘솔에 액세스할 때 경고가 나타납니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 작업 드롭다운 목록을 클릭한 다음 * HTTPS 설정 * 을 선택합니다.

   만료 날짜를 포함하여 Cloud Manager 인증서에 대한 세부 정보가 표시됩니다.

2. HTTPS 인증서 갱신 * 을 클릭하고 단계에 따라 CSR을 생성하거나 고유한 CA 서명 인증서를 설치합니다.

결과

Cloud Manager는 새로운 CA 서명 인증서를 사용하여 안전한 HTTPS 액세스를 제공합니다.

Cloud Manager 제거 중

Cloud Manager에는 소프트웨어를 제거하여 문제를 해결하거나 소프트웨어를 호스트에서 영구적으로 제거하는 데 사용할 수 있는 제거 스크립트가 포함되어 있습니다.

단계

1. Cloud Manager를 다시 설치하려면 소프트웨어를 제거하기 전에 데이터베이스를 백업하십시오.
   a. Cloud Manager 콘솔의 오른쪽 위 모서리에서 작업 드롭다운 목록을 클릭하고 * 도구 * 를 선택합니다.
   b. 백업 * 을 클릭하고 백업 파일을 로컬 컴퓨터에 저장합니다.
2. Linux 호스트에서 제거 스크립트를 실행합니다.
   - /opt/application/netapp/cloudmanager/bin/uninstall.sh [silent] *

_silent_는 확인 메시지를 표시하지 않고 스크립트를 실행합니다.

API 및 자동화

코드로서 인프라를 위한 자동화 샘플

이 페이지의 리소스를 사용하여 Cloud Manager 및 Cloud Volumes ONTAP를 과 통합하는 데 도움을 받으십시오 "코드로서의 인프라".

DevOps 팀은 다양한 툴을 사용하여 새로운 환경의 설정을 자동화함으로써 인프라를 코드로 처리할 수 있습니다. 이러한 도구 두 가지는 Ansible과 Terraform입니다. DevOps 팀에서 Cloud Manager와 함께 사용하여 Cloud Volumes ONTAP를 자동화하고 인프라와 코드로 통합하는 Ansible 및 Terraform 샘플을 개발했습니다.

"자동화 샘플 보기".

예를 들어, Ansible 플레이북을 샘플사용하여 Cloud Manager 및 Cloud Volumes ONTAP를 배포하고, 애그리게이트를 만들고, 볼륨을 만들 수 있습니다. 환경에 맞는 샘플을 수정하거나 샘플을 바탕으로 새로운 플레이북을 생성하십시오.

- 관련 링크 *
- "NetApp 클라우드 블로그: Federated Access에서 Cloud Manager REST API 사용"
- "NetApp 클라우드 블로그: Cloud Volumes ONTAP 및 REST를 통한 클라우드 자동화"
- "NetApp 클라우드 블로그: 클라우드 기반 소프트웨어 애플리케이션 테스트를 위한 자동화된 데이터 복제"
- "NetApp 블로그: Ansible + NetApp을 사용하여 IAC(Infrastructure-as-Code) 가속화"
- "NetApp thePub: 구성 관리 및 amp; Ansible을 통한 자동화"
- "NetApp thePub: Ansible ONTAP에서 사용하는 역할"

참조하십시오

질문과 대답: Cloud Manager와 NetApp Cloud Central의 통합

Cloud Manager 3.5로 업그레이드할 때 NetApp은 NetApp Cloud Central과 통합할 특정 Cloud Manager 시스템을 선택하지 않을 경우 선택합니다. 이 FAQ는 프로세스에 관한 질문에 답할 수 있습니다.

NetApp Cloud Central이란?

NetApp Cloud Central은 NetApp 클라우드 데이터 서비스에 액세스하고 이를 관리할 수 있는 중앙의 위치입니다. 이러한 서비스를 사용하여 클라우드에서 중요한 애플리케이션을 실행하고, 자동화된 DR 사이트를 생성하고, SaaS 데이터를 백업하고, 여러 클라우드 간에 데이터를 효과적으로 마이그레이션 및 제어할 수 있습니다.

NetApp이 Cloud Central과 Cloud Manager 시스템을 통합하는 이유는 무엇입니까?

Cloud Manager와 NetApp Cloud Central의 통합은 간소화된 배포 경험, 여러 Cloud Manager 시스템을 보고 관리할 수 있는 단일 위치, 중앙 집중식 사용자 인증 등 여러 가지 이점을 제공합니다.

통합 프로세스 중에 발생하는 현상

NetApp은 Cloud Manager 시스템의 모든 로컬 사용자 계정을 Cloud Central에서 사용할 수 있는 중앙 집중식 사용자 인증으로 마이그레이션합니다.

중앙 집중식 사용자 인증은 어떻게 작동합니까?

중앙 집중식 사용자 인증을 통해 Cloud Manager 시스템과 Cloud Manager와 Cloud Sync 같은 다른 데이터 서비스 간에 동일한 자격 증명 세트를 사용할 수 있습니다. 또한 암호를 잊어버린 경우 쉽게 재설정할 수 있습니다.

Cloud Central 사용자 계정에 가입해야 합니까?

NetApp은 Cloud Manager 시스템을 Cloud Central과 통합할 때 사용할 Cloud Central 사용자 계정을 생성합니다. 등록 프로세스를 완료하려면 비밀번호를 재설정하기만 하면 됩니다.

Cloud Central 사용자 계정이 이미 있는 경우 어떻게 해야 합니까?

Cloud Manager에 로그인하는 데 사용하는 이메일 주소가 Cloud Central 사용자 계정의 이메일 주소와 일치하면 Cloud Manager 시스템에 직접 로그인할 수 있습니다.

Cloud Manager 시스템에 여러 사용자 계정이 있는 경우 어떻게 해야 합니까?

NetApp은 모든 로컬 사용자 계정을 Cloud Central 사용자 계정으로 마이그레이션합니다. 모든 사용자는 자신의 암호를 재설정해야 합니다.

여러 **Cloud Manager** 시스템에서 동일한 이메일 주소를 사용하는 사용자 계정이 있는 경우 어떻게 해야 합니까?

암호를 한 번만 재설정하기만 하면 동일한 Cloud Central 사용자 계정을 사용하여 각 Cloud Manager 시스템에 로그인할 수 있습니다.

로컬 사용자 계정이 잘못된 이메일 주소를 사용하는 경우 어떻게 해야 합니까?

암호를 재설정하려면 유효한 이메일 주소가 필요합니다. Cloud Manager 인터페이스 오른쪽 아래에 있는 채팅 아이콘을 통해 문의해 주십시오.

Cloud Manager API용 자동화 스크립트가 있는 경우 어떻게 됩니까?

모든 API는 이전 버전과 호환됩니다. 암호를 재설정할 때 암호를 변경하는 경우 암호를 사용하는 스크립트를 업데이트해야 합니다.

Cloud Manager 시스템에서 **LDAP**를 사용하는 경우 어떻게 됩니까?

시스템에서 LDAP를 사용하는 경우 NetApp은 시스템을 Cloud Central과 자동으로 통합할 수 없습니다. 다음 단계를 수동으로 수행해야 합니다.

1. 에서 새로운 Cloud Manager 시스템을 구축합니다 "NetApp Cloud Central에서".
2. "새 시스템으로 LDAP를 설정합니다".
3. "기존 Cloud Volumes ONTAP 시스템을 검색합니다" 을 참조하십시오.
4. 이전 Cloud Manager 시스템을 삭제합니다.

Cloud Manager 시스템을 어디에 설치해도 됩니까?

아니요 NetApp은 AWS, Azure 또는 사내 등 위치에 상관없이 Cloud Central과 시스템을 통합합니다.

단, AWS 상용 클라우드 서비스 환경은 예외입니다.

AWS의 보안 그룹 규칙

Cloud Manager는 Cloud Manager와 Cloud Volumes ONTAP가 성공적으로 운영하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함한 AWS 보안 그룹을 생성합니다. 테스트 목적으로 또는 자체 보안 그룹을 사용하려는 경우 포트를 참조할 수 있습니다.

Cloud Manager의 규칙

Cloud Manager의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

Cloud Manager의 인바운드 규칙

미리 정의된 보안 그룹의 인바운드 규칙 소스는 0.0.0.0/0입니다.

프로토콜	포트	목적
SSH를 클릭합니다	22	Cloud Manager 호스트에 대한 SSH 액세스를 제공합니다
HTTP	80	클라이언트 웹 브라우저에서 Cloud Manager 웹 콘솔로 HTTP 액세스를 제공합니다
HTTPS	443	클라이언트 웹 브라우저에서 Cloud Manager 웹 콘솔로 HTTPS 액세스를 제공합니다

Cloud Manager의 아웃바운드 규칙

Cloud Manager에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

Cloud Manager에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	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 Cloud Manager의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

소스 IP 주소는 Cloud Manager 호스트입니다.

서비스	프로토콜	포트	목적지	목적
Active Directory를 클릭합니다	TCP	88	Active Directory 포리스트입니다	Kerberos V 인증
	TCP	139	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP	389	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	TCP	749	Active Directory 포리스트입니다	Active Directory Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
	UDP입니다	137	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	138	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	UDP입니다	464	Active Directory 포리스트입니다	Kerberos 키 관리
API 호출 및 AutoSupport	HTTPS	443	아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF	API는 AWS 및 ONTAP를 호출하고 AutoSupport 메시지를 NetApp에 보냅니다
API 호출	TCP	3000입니다	ONTAP 클러스터 관리 LIF	ONTAP에 대한 API 호출
DNS	UDP입니다	53	DNS	Cloud Manager에서 DNS Resolve에 사용됩니다

Cloud Volumes ONTAP 규칙

Cloud Volumes ONTAP의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

Cloud Volumes ONTAP에 대한 인바운드 규칙

미리 정의된 보안 그룹의 인바운드 규칙 소스는 0.0.0.0/0입니다.

프로토콜	포트	목적
모든 ICMP	모두	인스턴스에 Ping을 수행 중입니다
HTTP	80	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTP 액세스

프로토콜	포트	목적
HTTPS	443	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTPS 액세스
SSH를 클릭합니다	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
TCP	111	NFS에 대한 원격 프로시저 호출
TCP	139	CIFS에 대한 NetBIOS 서비스 세션입니다
TCP	161-162	단순한 네트워크 관리 프로토콜
TCP	445	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
TCP	635	NFS 마운트
TCP	749	Kerberos
TCP	2049	NFS 서버 데몬
TCP	3260	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045	NFS 잠금 데몬
TCP	4046	NFS에 대한 네트워크 상태 모니터
TCP	10000입니다	NDMP를 사용한 백업
TCP	11104	SnapMirror에 대한 인터클러스터 통신 세션의 관리
TCP	11105	인터클러스터 LIF를 사용하여 SnapMirror 데이터 전송
UDP입니다	111	NFS에 대한 원격 프로시저 호출
UDP입니다	161-162	단순한 네트워크 관리 프로토콜
UDP입니다	635	NFS 마운트
UDP입니다	2049	NFS 서버 데몬
UDP입니다	4045	NFS 잠금 데몬
UDP입니다	4046	NFS에 대한 네트워크 상태 모니터
UDP입니다	4049	NFS rquotad 프로토콜

Cloud Volumes ONTAP의 아웃바운드 규칙

Cloud Volumes ONTAP에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

Cloud Volumes ONTAP에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	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 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Cloud Volumes ONTAP의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

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

서비스	프로토콜	포트	출처	목적지	목적
Active Directory를 클릭합니다	TCP	88	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니다	137	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	138	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	TCP	139	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP	389	노드 관리 LIF	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	노드 관리 LIF	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	UDP입니다	464	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos 키 관리
	TCP	749	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
	TCP	88	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니다	137	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	138	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	TCP	139	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP	389	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	UDP입니다	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos 키 관리
	TCP	749	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)

서비스	프로토콜	포트	출처	목적지	목적
클러스터	모든 교통 정보	모든 교통 정보	모든 LIF가 하나의 노드에 있습니다	다른 노드의 모든 LIF	인터클러스터 통신(Cloud Volumes ONTAP HA에만 해당)
	TCP	3000입니다	노드 관리 LIF	HA 중재자	ZAPI 호출(Cloud Volumes ONTAP HA 전용)
	ICMP	1	노드 관리 LIF	HA 중재자	활성 상태 유지(Cloud Volumes ONTAP HA만 해당)
DHCP를 선택합니다	UDP입니다	68	노드 관리 LIF	DHCP를 선택합니다	처음으로 설정하는 DHCP 클라이언트
DHCPS	UDP입니다	67	노드 관리 LIF	DHCP를 선택합니다	DHCP 서버
DNS	UDP입니다	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	노드 관리 LIF	대상 서버	NDMP 복제
SMTP	TCP	25	노드 관리 LIF	메일 서버	AutoSupport에 사용할 수 있는 SMTP 경고
SNMP를 선택합니다	TCP	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니다	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	TCP	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니다	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
SnapMirror를 참조하십시오	TCP	11104	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리
	TCP	11105	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror 데이터 전송
Syslog를 클릭합니다	UDP입니다	514	노드 관리 LIF	Syslog 서버	Syslog 메시지를 전달합니다

외부 보안 그룹의 **HA** 중재자를 위한 규칙

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

인바운드 규칙

인바운드 규칙의 소스는 0.0.0.0/0입니다.

프로토콜	포트	목적
SSH를 클릭합니다	22	HA 중재자로 SSH 연결

프로토콜	포트	목적
TCP	3000입니다	Cloud Manager에서 RESTful API 액세스

아웃바운드 규칙

HA 중재자를 위한 사전 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

HA 중재자를 위해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	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.

프로토콜	포트	목적지	목적
HTTP	80	Cloud Manager IP 주소입니다	중재자를 위한 업그레이드 다운로드
HTTPS	443	AWS API 서비스	스토리지 페일오버 지원
UDP입니다	53	AWS API 서비스	스토리지 페일오버 지원

포트 443과 53을 열지 않고 타겟 서브넷에서 AWS EC2 서비스로 인터페이스 VPC 엔드포인트를 생성할 수 있습니다.

HA 중재자 내부 보안 그룹의 규칙

Cloud Volumes ONTAP HA 중재자를 위해 미리 정의된 내부 보안 그룹에는 다음 규칙이 포함됩니다. Cloud Manager는 항상 이 보안 그룹을 생성합니다. 자신의 을(를) 사용할 수 있는 옵션이 없습니다.

인바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 인바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 교통 정보	모두	HA 중재자 및 HA 노드 간 통신

아웃바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 교통 정보	모두	HA 중재자 및 HA 노드 간 통신

Azure의 보안 그룹 규칙

Cloud Manager는 Cloud Manager와 Cloud Volumes ONTAP가 성공적으로 운영하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함하는 Azure 보안 그룹을 생성합니다. 테스트 목적으로 또는 자체 보안 그룹을 사용하려는 경우 포트를 참조할 수 있습니다.

Cloud Manager의 규칙

Cloud Manager의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

Cloud Manager의 인바운드 규칙

미리 정의된 보안 그룹의 인바운드 규칙 소스는 0.0.0.0/0입니다.

프로토콜	포트	목적
SSH를 클릭합니다	22	Cloud Manager 호스트에 대한 SSH 액세스를 제공합니다
HTTP	80	클라이언트 웹 브라우저에서 Cloud Manager 웹 콘솔로 HTTP 액세스를 제공합니다
HTTPS	443	클라이언트 웹 브라우저에서 Cloud Manager 웹 콘솔로 HTTPS 액세스를 제공합니다

Cloud Manager의 아웃바운드 규칙

Cloud Manager에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

Cloud Manager에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	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 Cloud Manager의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

소스 IP 주소는 Cloud Manager 호스트입니다.

서비스	프로토콜	포트	목적지	목적
Active Directory를 클릭합니다	TCP	88	Active Directory 포리스트입니다	Kerberos V 인증
	TCP	139	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP	389	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	TCP	749	Active Directory 포리스트입니다	Active Directory Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
	UDP입니다	137	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	138	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	UDP입니다	464	Active Directory 포리스트입니다	Kerberos 키 관리
API 호출 및 AutoSupport	HTTPS	443	아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF	API는 AWS 및 ONTAP를 호출하고 AutoSupport 메시지를 NetApp에 보냅니다
API 호출	TCP	3000입니다	ONTAP 클러스터 관리 LIF	ONTAP에 대한 API 호출
DNS	UDP입니다	53	DNS	Cloud Manager에서 DNS Resolve에 사용됩니다

Cloud Volumes ONTAP 규칙

Cloud Volumes ONTAP의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

단일 노드 시스템에 대한 인바운드 규칙입니다

우선 순위	이름	포트	프로토콜	출처	목적지	조치	설명
1000입니다	inbound_ssh입니다	22	TCP	모두	모두	허용	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다

우선 순위	이름	포트	프로토콜	출처	목적지	조치	설명
1001	inbound_http(인바운드_http	80	TCP	모두	모두	허용	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTP 액세스
1002	인바운드_111_TCP	111	TCP	모두	모두	허용	NFS에 대한 원격 프로시저 호출
1003	인바운드_111_UDP	111	UDP입니다	모두	모두	허용	NFS에 대한 원격 프로시저 호출
1004	인바운드_139	139	TCP	모두	모두	허용	CIFS에 대한 NetBIOS 서비스 세션입니다
1005	인바운드_161-162_TCP	161-162	TCP	모두	모두	허용	단순한 네트워크 관리 프로토콜
1006)을 참조하십시오	인바운드_161-162_UDP	161-162	UDP입니다	모두	모두	허용	단순한 네트워크 관리 프로토콜
1007	inbound_443	443	TCP	모두	모두	허용	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTPS 액세스
1008	IN인바운드_445	445	TCP	모두	모두	허용	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
1009	인바운드_635_TCP	635	TCP	모두	모두	허용	NFS 마운트
1010	인바운드_635_UDP	635	TCP	모두	모두	허용	NFS 마운트
1011	인바운드_749	749	TCP	모두	모두	허용	Kerberos
1012	인바운드_2049_TCP	2049	TCP	모두	모두	허용	NFS 서버 데몬
1013	인바운드_2049_UDP	2049	UDP입니다	모두	모두	허용	NFS 서버 데몬
1014	인바운드_3260	3260	TCP	모두	모두	허용	iSCSI 데이터 LIF를 통한 iSCSI 액세스
1015	인바운드_4045-4046_TCP	4045-4046	TCP	모두	모두	허용	NFS 잠금 데몬 및 네트워크 상태 모니터
1016	인바운드_4045-4046_UDP	4045-4046	UDP입니다	모두	모두	허용	NFS 잠금 데몬 및 네트워크 상태 모니터
1017	인바운드 _ 10000	10000입니다	TCP	모두	모두	허용	NDMP를 사용한 백업
1018	IN인바운드_11104-11105	11104-11105	TCP	모두	모두	허용	SnapMirror 데이터 전송

우선 순위	이름	포트	프로토콜	출처	목적지	조치	설명
3000입니다	inbound_deny_all_tcp입니다	모두	TCP	모두	모두	거부	다른 모든 TCP 인바운드 트래픽을 차단합니다
3001	inbound_deny_all_udp입니다	모두	UDP입니다	모두	모두	거부	다른 모든 UDP 인바운드 트래픽을 차단합니다
65000	AllowVnetInBound 를 참조하십시오	모두	모두	가상네트워크	가상네트워크	허용	VNET 내에서 들어오는 인바운드 트래픽입니다
65001)을 참조하십시오	AllowAzureLoad BalancerInBound 를 참조하십시오	모두	모두	AzureLoadBalancer	모두	허용	Azure 표준 로드 밸런서의 데이터 트래픽
6,5005	DenyAllInBound를 참조하십시오	모두	모두	모두	모두	거부	다른 모든 인바운드 트래픽을 차단합니다

HA 시스템에 대한 인바운드 규칙

인바운드 데이터 트래픽이 Azure 표준 로드 밸런서를 통과하기 때문에 HA 시스템은 단일 노드 시스템보다 인바운드 규칙이 적습니다. 따라서 "AllowAzureLoadBalancerInBound" 규칙에 나와 있는 것처럼 로드 밸런서의 트래픽이 열려 있어야 합니다.

우선 순위	이름	포트	프로토콜	출처	목적지	조치	설명
100	inbound_443	443	모두	모두	모두	허용	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTPS 액세스
101	인바운드_111_TCP	111	모두	모두	모두	허용	NFS에 대한 원격 프로시저 호출
102	인바운드_2049_TCP	2049	모두	모두	모두	허용	NFS 서버 데몬
111	inbound_ssh입니다	22	모두	모두	모두	허용	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
121	인바운드_53	53	모두	모두	모두	허용	DNS 및 CIFS를 지원합니다
65000	AllowVnetInBound 를 참조하십시오	모두	모두	가상네트워크	가상네트워크	허용	VNET 내에서 들어오는 인바운드 트래픽입니다
65001)을 참조하십시오	AllowAzureLoad BalancerInBound 를 참조하십시오	모두	모두	AzureLoadBalancer	모두	허용	Azure 표준 로드 밸런서의 데이터 트래픽

우선 순위	이름	포트	프로토콜	출처	목적지	조치	설명
6,5005	DenyAllInBound를 참조하십시오	모두	모두	모두	모두	거부	다른 모든 인바운드 트래픽을 차단합니다

Cloud Volumes ONTAP의 아웃바운드 규칙

Cloud Volumes ONTAP에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

Cloud Volumes ONTAP에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

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

고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Cloud Volumes ONTAP의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

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

서비스	프로토콜	포트	출처	목적지	목적
Active Directory를 클릭합니다	TCP	88	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니다	137	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	138	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	TCP	139	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP	389	노드 관리 LIF	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	노드 관리 LIF	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	UDP입니다	464	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos 키 관리
	TCP	749	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
	TCP	88	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니다	137	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	138	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	TCP	139	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP	389	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	UDP입니다	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos 키 관리
	TCP	749	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
DHCP를 선택합니다	UDP입니다	68	노드 관리 LIF	DHCP를 선택합니다	처음으로 설정하는 DHCP 클라이언트
DHCPS	UDP입니다	67	노드 관리 LIF	DHCP를 선택합니다	DHCP 서버

서비스	프로토콜	포트	출처	목적지	목적
DNS	UDP입니다	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	노드 관리 LIF	대상 서버	NDMP 복제
SMTP	TCP	25	노드 관리 LIF	메일 서버	AutoSupport에 사용할 수 있는 SMTP 경고
SNMP를 선택합니다	TCP	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니다	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	TCP	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니다	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
SnapMirror를 참조하십시오	TCP	11104	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리
	TCP	11105	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror 데이터 전송
Syslog를 클릭합니다	UDP입니다	514	노드 관리 LIF	Syslog 서버	Syslog 메시지를 전달합니다

Cloud Manager에 대한 AWS 및 Azure 권한

Cloud Manager를 사용하려면 대신 AWS 및 Azure에서 작업을 수행할 권한이 있어야 합니다. 이러한 권한은 에 포함되어 있습니다 "NetApp에서 제공하는 정책". Cloud Manager가 이러한 사용 권한을 통해 수행하는 작업을 이해하기를 원할 수 있습니다.

Cloud Manager에서 AWS 권한을 통해 수행하는 것

Cloud Manager는 AWS 계정을 사용하여 EC2, S3, CloudFormation, IAM, 보안 토큰 서비스(STS) 및 키 관리 서비스(KMS).

작업	목적
"EC2:StartInstances", "EC2:StopInstances", "EC2:DescribeInstances", "EC2:DescribeInstanceStatus", "EC2:RunInstances", "EC2: TerminateInstances", "EC2: ModifyInstanceAttribute",	Cloud Volumes ONTAP 인스턴스를 시작하고 인스턴스를 중지, 시작 및 모니터링합니다.
"EC2: DescribeInstanceAttribute",	지원되는 인스턴스 유형에 대해 향상된 네트워킹이 활성화되어 있는지 확인합니다.
"EC2: DescribeRouteTables", "EC2: DescribeImages",	Cloud Volumes ONTAP HA 구성을 시작합니다.

작업	목적
"EC2:CreateTags",	Cloud Manager가 만드는 모든 리소스에 "WorkingEnvironment" 및 "WorkingEnvironmentId" 태그를 지정합니다. Cloud Manager는 유지보수 및 비용 할당에 이러한 태그를 사용합니다.
"EC2:CreateVolume", "EC2:DescribeVolumes", "EC2:ModifyVolumeAttribute", "EC2:AttachVolume", "EC2:DeleteVolume", "EC2: DetachVolume(EC2: 멈춤쇠 볼륨)",	Cloud Volumes ONTAP가 백엔드 스토리지로 사용하는 EBS 볼륨을 관리합니다.
"EC2:CreateSecurityGroup", "EC2:DeleteSecurityGroup", "EC2:DescribeSecurityGroups", "EC2:RevokeSecurityGroupEgress", "EC2:AuthorizeSecurityGroupEgress", "EC2:AuthorizeSecurityGroupIngress", "EC2:RevokeSecurityGroupIngress",	Cloud Volumes ONTAP에 대해 미리 정의된 보안 그룹을 만듭니다.
"EC2:CreateNetworkInterface", "EC2:DescribeNetworkInterfaces", "EC2:DeleteNetworkInterface", "EC2:ModifyNetworkInterfaceAttribute",	대상 서브넷에서 Cloud Volumes ONTAP에 대한 네트워크 인터페이스를 생성하고 관리합니다.
"EC2: DescribeSubnet", "EC2: DescribeVpcs",	Cloud Volumes ONTAP 에 대한 새 작업 환경을 만들 때 필요한 대상 서브넷 및 보안 그룹 목록을 가져옵니다.
"EC2: DescribeDhcpOptions",	Cloud Volumes ONTAP 인스턴스를 시작할 때 DNS 서버와 기본 도메인 이름을 결정합니다.
"EC2:CreateSnapshot", "EC2:DeleteSnapshot", "EC2:DescribeSnapshots",	초기 설정 중에 및 Cloud Volumes ONTAP 인스턴스가 중지될 때마다 EBS 볼륨의 스냅샷을 생성합니다.
"EC2:GetConsoleOutput",	AutoSupport 메시지에 첨부된 Cloud Volumes ONTAP 콘솔을 캡처합니다.
"EC2: 설명",	인스턴스를 시작할 때 사용 가능한 키 쌍 목록을 가져옵니다.
"EC2: 설명 영역",	사용 가능한 AWS 영역 목록을 가져옵니다.
"EC2:DeleteTags", "EC2: DescribeTags",	Cloud Volumes ONTAP 인스턴스와 관련된 리소스의 태그를 관리합니다.
"CloudFormation:CreateStack", "CloudFormation:DeleteStack", "CloudFormation:DescribeStacks", "CloudFormation:DescribeStackEvents", "CloudFormation:ValidateTemplate",	Cloud Volumes ONTAP 인스턴스를 시작합니다.
"IAM:PassRole", "IAM:CreateRole", "IAM:DeleteRole", "IAM:PutRolePolicy", "IAM:CreateInstanceProfile", "IAM:DeleteRolePolicy", "IAM:AddRoleToInstanceProfile", "IAM:RemoveRoleFromInstanceProfile", "IAM:DeleteInstanceProfile",	Cloud Volumes ONTAP HA 구성을 시작합니다.

작업	목적
"IAM:ListInstanceProfiles", "STS:DecodeAuthorizationMessage", "EC2:AssociateIamInstanceProfile", "EC2:DescribeIamInstanceProfileAssociations", "EC2:DisconnectateIamInstanceProfile",	Cloud Volumes ONTAP 인스턴스의 인스턴스 프로파일을 관리합니다.
"S3:GetBucketTagging", "S3:GetBucketLocation", "S3:ListAllMyBucket", "S3:ListBucket"	Cloud Manager를 NetApp Data Fabric Cloud Sync 서비스와 통합할 수 있도록 AWS S3 버킷에 대한 정보 확보
"S3:CreateBucket", "S3:DeleteBucket", "S3:GetLifecycleConfiguration", "S3:PutLifecycleConfiguration", "S3:PutketTagging", "S3:ListBuckketVersions",	Cloud Volumes ONTAP 시스템에서 용량 계층으로 사용하는 S3 버킷을 관리합니다.
"kms:List * ", "kms:설명 *"	AWS Key Management Service에서 키에 대한 정보를 가져옵니다.
"CE:GetReservationUtilization", "CE:GetDimensionValues", "CE:GetCostAndUsage", "CE:GetTags"	Cloud Volumes ONTAP에 대한 AWS 비용 데이터를 가져옵니다.
"EC2:CreatePlacementGroup", "EC2:DeletePlacementGroup"	단일 AWS Availability Zone에 HA 구성을 구축하면 Cloud Manager가 두 개의 HA 노드를 시작하고 AWS Spread 배치 그룹에서 중재자를 실행합니다.

Cloud Manager가 Azure 권한으로 수행하는 기능

Cloud Manager Azure 정책에는 Cloud Manager가 Azure에서 Cloud Volumes ONTAP를 배포하고 관리하는 데 필요한 권한이 포함되어 있습니다.

작업	목적
"Microsoft.Compute/locations/operations/read", "Microsoft.Compute/locations/vmSizes/read", "Microsoft.Compute/operations/read", "Microsoft.Compute/virtualMachines/instanceView/read","Microsoft.Compute/virtualMachines/powerOff/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/virtualMachines/restart/action", "Microsoft.Compute/virtualMachines/start/action", "Microsoft.Compute/virtualMachines/deallocate/action","Microsoft.Compute/virtualMachines/vmSizes/read", "Microsoft.Compute/virtualMachines/write",	Cloud Volumes ONTAP를 생성하고 시스템 상태를 중지, 시작, 삭제 및 가져옵니다.
"Microsoft.Compute/images/write"," Microsoft.Compute/images/read",	VHD에서 Cloud Volumes ONTAP 배포를 활성화합니다.

작업	목적
"Microsoft.Compute/disks/delete", "Microsoft.Compute/disks/read", "Microsoft.Compute/disks/write", "Microsoft.Storage/checkknameAvailability/read", "Microsoft.Storage/operations/read", "Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/storageAccounts/read", "Microsoft.Storage/storageAccounts/REV/ACTION", "Microsoft.Storage/storageAccounts/write", "Microsoft.Storage/storageAccounts/delete", "Microsoft.Storage/en사용법/read",	Azure 스토리지 계정 및 디스크를 관리하고 디스크를 Cloud Volumes ONTAP에 연결합니다.
"Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write"," Microsoft.Network/networkInterfaces/join/action",	대상 서브넷에서 Cloud Volumes ONTAP에 대한 네트워크 인터페이스를 생성하고 관리합니다.
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write"," Microsoft.Network/networkSecurityGroups/join/action",	Cloud Volumes ONTAP에 대해 미리 정의된 네트워크 보안 그룹을 생성합니다.
"Microsoft.Resources/Subscriptions/locations/read", "Microsoft.Network/locations/operationResults/read", "Microsoft.Network/locations/operations/read", "Microsoft.Network/virtualNetworks/read"," Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", "Microsoft.Network/virtualNetworks/virtualMachines/read","Microsoft.Network/virtualNetworks/subnets/join/action",	지역, 대상 VNET 및 서브넷에 대한 네트워크 정보를 가져오고 Cloud Volumes ONTAP를 VNets에 추가합니다.
"Microsoft.Network/virtualNetworks/subnets/write"," Microsoft.Network/routeTables/join/action",	데이터 계층화를 위한 VNET 서비스 엔드포인트를 활성화합니다.
"Microsoft.Resources/Deployments/operations/read", "Microsoft.Resources/Deployments/read", "Microsoft.Resources/Deployments/Write",	템플릿에서 Cloud Volumes ONTAP를 배포합니다.
"Microsoft.Resources/Deployments/operations/read", "Microsoft.Resources/Deployments/read", "Microsoft.Resources/Deployments/write", "Microsoft.Resources/resources/read", "Microsoft.Resources/Subscriptions/operationresults/read", "Microsoft.Resources/Subscriptions/resourceGroups/delete", "Microsoft.Resources/Subscriptions/resourceGroups/read", "Microsoft.Resources/Subscriptions/resourcegroups/resourceGroups/read", "Microsoft.Resources/Subscriptions/resourceGroups/write",	Cloud Volumes ONTAP에 대한 리소스 그룹을 생성하고 관리합니다.

작업	목적
"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read"," Microsoft.Compute/disks/beginGetAccess/action"	Azure 관리 스냅샷을 생성하고 관리합니다.
"Microsoft.Compute/availabilitySets/write"," Microsoft.Compute/availabilitySets/read",	Cloud Volumes ONTAP의 가용성 세트를 생성하고 관리합니다.
"Microsoft.MarketplaceOrdering/offerstypes/publishers/Offers/Plans/Agreement/read", "Microsoft.MarketplaceOrdering/offerstypes/publisherTypes/publishers/Offers/Plans/Agreement/write"	Azure Marketplace에서 프로그래밍 방식으로 배포할 수 있습니다.
"Microsoft.Network/loadBalancers/read", "Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/backendAddressPools/read","Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read", "Microsoft.Network/loadBalancers/loadBalancingRules/read", "Microsoft.Network/loadBalancers/probes/read","Microsoft.Network/loadBalancers/probes/join/action",	HA 쌍에 대한 Azure 로드 밸런서를 관리합니다.
"Microsoft.Authorization/lock/ *"	Azure 디스크의 잠금 관리를 활성화합니다.
"Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/sites/ *"	HA 쌍의 페일오버 관리

기본 설정

Cloud Manager 및 Cloud Volumes ONTAP를 기본적으로 구성하는 방법에 대한 자세한 내용은 시스템을 관리하는 데 도움이 됩니다.

Linux 기반 Cloud Manager의 기본 구성

Cloud Manager 또는 Linux 호스트 문제를 해결해야 하는 경우 Cloud Manager 구성 방법을 이해하는 데 도움이 될 수 있습니다.

- NetApp Cloud Central(또는 AWS Marketplace 또는 Azure Marketplace에서 직접)에서 Cloud Manager를 구축한 경우 다음을 확인하십시오.
  - AWS에서 EC2 Linux 인스턴스의 사용자 이름은 EC2-user입니다.
  - AWS와 Azure 모두에서 Cloud Manager 이미지의 운영 체제는 Red Hat Enterprise Linux 7.4(HVM)입니다.

    운영 체제에는 GUI가 포함되어 있지 않습니다. 시스템에 액세스하려면 터미널을 사용해야 합니다.
- Cloud Manager 설치 폴더는 다음 위치에 있습니다.

  /opt/application/netapp/cloudmanager입니다

- 로그 파일은 다음 폴더에 들어 있습니다.

  /opt/application/netapp/cloudmanager/log입니다

- Cloud Manager 서비스의 이름은 occm입니다.
- occm 서비스는 MySQL 서비스에 따라 달라진다.

  MySQL 서비스가 다운되면 occm 서비스도 다운됩니다.

- Cloud Manager는 다음 패키지를 아직 설치하지 않은 경우 Linux 호스트에 설치합니다.
  - 7zip
  - AWSCLI
  - 자바
  - 쿠베틀입니다
  - MySQL
  - 트리엔ctl
  - 윙입니다

Cloud Volumes ONTAP의 기본 구성입니다

Cloud Volumes ONTAP가 기본적으로 어떻게 구성되어 있는지 이해하면 시스템을 설정하고 관리하는 데 도움이 됩니다. 특히 ONTAP에 익숙한 경우 Cloud Volumes ONTAP의 기본 설정은 ONTAP와 다르기 때문입니다.

- Cloud Volumes ONTAP는 단일 노드 시스템으로, AWS와 Azure 모두에서 HA 쌍으로 사용할 수 있습니다.
- Cloud Volumes ONTAP 구축 시 Cloud Manager에서 단일 데이터 서비스 SVM을 생성합니다. System Manager 또는 CLI에서 다른 데이터 지원 SVM을 생성할 수 있지만, 여러 데이터 제공 SVM을 사용하는 것은 지원되지 않습니다.
- 기본적으로 여러 네트워크 인터페이스가 생성됩니다.
  - 클러스터 관리 LIF
  - 인터클러스터 LIF
  - 노드 관리 LIF
  - iSCSI 데이터 LIF
  - CIFS 및 NFS 데이터 LIF

  > EC2 요구사항으로 인해 LIF 페일오버가 Cloud Volumes ONTAP에 대해 기본적으로 비활성화되어 있습니다. LIF를 다른 포트로 마이그레이션하면 IP 주소와 인스턴스 네트워크 인터페이스 간의 외부 매핑이 분리되므로 LIF에 액세스할 수 없습니다.

- Cloud Volumes ONTAP는 HTTPS를 사용하여 구성 백업을 Cloud Manager로 전송합니다.
- Cloud Manager에 로그인하면 에서 백업에 액세스할 수 있습니다 https://ipaddress/occm/offboxconfig/
- Cloud Manager에서는 다른 관리 툴(예: System Manager 또는 CLI)과 몇 가지 볼륨 특성을 다르게 설정합니다.

  다음 표에는 Cloud Manager가 기본값과 다르게 설정하는 볼륨 특성이 나열되어 있습니다.

속성	**Cloud Manager**에서 설정한 값입니다
자동 크기 조정 모드입니다	성장
최대 자동 크기 조정	1,000% Cloud Manager 관리자는 설정 페이지에서 이 값을 수정할 수 있습니다.
보안 스타일	CIFS 볼륨용 NTFS NFS 볼륨용 UNIX
공간 보장 스타일	없음
UNIX 권한(NFS에만 해당)	777

이러한 속성에 대한 자세한 내용은 _volume create_man 페이지를 참조하십시오.

Cloud Volumes ONTAP의 부팅 및 루트 데이터

사용자 데이터를 위한 스토리지 외에, Cloud Manager는 각 Cloud Volumes ONTAP 시스템에서 부팅 및 루트 데이터를 위한 클라우드 스토리지도 구매합니다.

설치하고

- Cloud Volumes ONTAP 부팅 데이터용 프로비저닝된 IOPS SSD 디스크 1개(약 45GB 및 1,250PIOPS
- Cloud Volumes ONTAP 루트 데이터용 범용 SSD 디스크 1개(약 140GB
- 각 부팅 디스크 및 루트 디스크마다 하나의 EBS 스냅샷

HA 2노드에서 두 Cloud Volumes ONTAP 노드 모두 루트 디스크를 파트너 노드로 복제합니다.

Azure를 지원합니다

- Cloud Volumes ONTAP 부팅 데이터용 프리미엄 스토리지 SSD 디스크 1개(약 73GB)
- Cloud Volumes ONTAP 루트 데이터용 프리미엄 스토리지 SSD 디스크 1개(약 140GB)
- 각 부팅 디스크 및 루트 디스크에 대해 Azure 스냅샷 1개

디스크가 상주하는 위치입니다

Cloud Manager는 AWS 및 Azure에서 다음과 같이 스토리지를 구축합니다.

- 부팅 데이터는 EC2 인스턴스 또는 Azure 가상 머신에 연결된 디스크에 있습니다.

  부팅 이미지가 포함된 이 디스크는 Cloud Volumes ONTAP에서 사용할 수 없습니다.

- 시스템 구성 및 로그가 포함된 루트 데이터는 aggr0에 상주합니다.
- 스토리지 가상 시스템(SVM) 루트 볼륨은 aggr1에 있습니다.

- 데이터 볼륨은 aggr1에도 상주합니다.

사용자 역할

각 Cloud Manager 사용자 계정에는 권한을 정의하는 역할이 할당됩니다.

작업	**Cloud Manager** 관리자	테넌트 관리자	작업 환경 관리자
테넌트 관리	예	아니요	아니요
작업 환경 관리	예	예, 할당된 테넌트에 대해	예, 할당된 작업 환경에 대해 가능합니다
작업 환경을 Cloud Sync와 통합합니다	예	예	아니요
데이터 복제 상태를 봅니다	예	예, 할당된 테넌트에 대해	예, 할당된 작업 환경에 대해 가능합니다
타임라인을 봅니다	예	예	예
사용자 계정을 만들고 삭제합니다	예	예, 할당된 테넌트에 대해	아니요
사용자 계정을 수정합니다	예	예, 할당된 테넌트에 대해	예, 자신의 계정에 대해 그렇습니다
계정 설정을 관리합니다	예	아니요	아니요
Kubernetes 설정	예	아니요	아니요
스토리지 시스템 보기와 볼륨 보기 간에 전환합니다	예	아니요	아니요
설정을 수정합니다	예	아니요	아니요
지원 대시보드 보기 및 관리	예	아니요	아니요
Cloud Manager 백업 및 복원	예	아니요	아니요
작업 환경을 제거합니다	예	아니요	아니요
Cloud Manager 업데이트	예	아니요	아니요
HTTPS 인증서를 설치합니다	예	아니요	아니요
Active Directory를 설정합니다	예	아니요	아니요
클라우드 스토리지 자동화 보고서 지원	예	아니요	아니요

도움을 받을 수 있는 곳 및 자세한 정보를 얻을 수 있는 곳

비디오, 포럼, 지원을 비롯한 다양한 리소스를 통해 도움을 얻고 Cloud Manager 및 Cloud Volumes ONTAP에 대한 자세한 정보를 확인할 수 있습니다.

- "Cloud Manager 및 Cloud Volumes ONTAP 비디오"

  AWS 및 Azure에서 Cloud Volumes ONTAP를 구축 및 관리하는 방법과 하이브리드 클라우드에서 데이터를 복제하는 방법을 비디오 에서 확인하십시오.

- "Cloud Manager에 대한 정책"

  Cloud Manager에서 AWS 및 Azure에서 작업을 수행하는 데 필요한 권한이 포함된 JSON 파일을 다운로드합니다.

- "Cloud Manager API 개발자 가이드 를 참조하십시오"

  API 개요, API 사용 방법의 예 및 API 참조를 읽어 보십시오.

- Cloud Volumes ONTAP 교육
  - "Cloud Volumes ONTAP 기본 원리"
  - "Azure용 Cloud Volumes ONTAP 배포 및 관리"
- 기술 보고서
  - "NetApp 기술 보고서 4383: 애플리케이션 워크로드를 포함한 Amazon Web Services의 Cloud Volumes ONTAP 성능 특성"
  - "NetApp 기술 보고서 4671: 애플리케이션 워크로드를 포함한 Azure의 Cloud Volumes ONTAP 성능 특성"
- "Cloud Volumes ONTAP 9 SVM 재해 복구 준비 Express 가이드"

  재해 복구 준비를 위해 대상 SVM을 빠르게 구성하는 방법에 대해 설명합니다.

- "Cloud Volumes ONTAP 9 SVM 재해 복구 익스프레스 가이드 를 참조하십시오"

  재해 발생 후 타겟 SVM을 빠르게 활성화한 다음 소스 SVM을 다시 활성화하는 방법을 설명합니다.

- "ONTAP 9 문서 센터"

  ONTAP를 사용하는 데 도움이 되는 Cloud Volumes ONTAP 제품 설명서를 참조하십시오.

- "NetApp Cloud Volumes ONTAP 지원"

  지원 리소스에 액세스하여 Cloud Volumes ONTAP 관련 문제를 해결하고 도움을 받으십시오.

- "NetApp 커뮤니티: 클라우드 데이터 서비스"

  동료와 소통하고, 질문을 하고, 아이디어를 교환하고, 리소스를 찾고, 모범 사례를 공유합니다.

- "NetApp Cloud Central에서"

  클라우드를 위한 추가 NetApp 제품 및 솔루션에 대한 정보를 찾아보십시오.

- "NetApp 제품 설명서"

  NetApp 제품 설명서에서 지침, 리소스, 답변을 찾아보십시오.

법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

http://www.netapp.com/us/legal/copyright.aspx

상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

http://www.netapp.com/us/legal/netapptmlist.aspx

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

https://www.netapp.com/us/media/patents-page.pdf

개인 정보 보호 정책

https://www.netapp.com/us/legal/privacypolicy/index.aspx

오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이센스에 대한 정보를 제공합니다.

- "OnCommand 클라우드 관리자 3.6.6에 대한 고지 사항"
- "OnCommand 클라우드 관리자 3.6.1에 대한 고지 사항"
- "OnCommand 클라우드 관리자 3.6에 대한 고지 사항"

저작권 정보

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

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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