



Cloud Volumes ONTAP 사용

Cloud Volumes ONTAP

NetApp
December 18, 2025

This PDF was generated from <https://docs.netapp.com/ko-kr/storage-management-cloud-volumes-ontap/task-manage-capacity-licenses.html> on December 18, 2025. Always check docs.netapp.com for the latest.

목차

Cloud Volumes ONTAP 사용	1
라이선스 관리	1
Cloud Volumes ONTAP에 대한 용량 기반 라이선싱 관리	1
NetApp Console 통해 Cloud Volumes ONTAP 대한 Keystone 구독 관리	6
Cloud Volumes ONTAP에 대한 노드 기반 라이선싱 관리	8
볼륨 및 LUN 관리	13
Cloud Volumes ONTAP 시스템에서 FlexVol volume 생성	13
Cloud Volumes ONTAP 시스템에서 볼륨 관리	20
비활성 Cloud Volumes ONTAP 데이터를 저렴한 개체 스토리지로 계층화합니다.	29
호스트 시스템에서 Cloud Volumes ONTAP의 LUN에 연결합니다.	37
Cloud Volumes ONTAP 시스템에서 FlexCache 볼륨을 사용하여 데이터 액세스 가속화	38
집계 관리	39
Cloud Volumes ONTAP 시스템에 대한 집계를 만듭니다.	39
Cloud Volumes ONTAP 클러스터에 대한 집계 관리	42
콘솔 에이전트에서 Cloud Volumes ONTAP 집계 용량 관리	43
Azure에서 디스크 성능 관리	45
스토리지 VM 관리	47
Cloud Volumes ONTAP의 스토리지 VM 관리	48
AWS에서 Cloud Volumes ONTAP 위한 데이터 제공 스토리지 VM 관리	49
Azure에서 Cloud Volumes ONTAP 대한 데이터 제공 스토리지 VM 관리	56
Google Cloud에서 Cloud Volumes ONTAP 위한 데이터 제공 스토리지 VM 관리	59
Cloud Volumes ONTAP에 대한 스토리지 VM 재해 복구 설정	62
보안 및 데이터 암호화	62
NetApp 암호화 솔루션을 사용하여 Cloud Volumes ONTAP에서 볼륨 암호화	62
AWS Key Management Service를 사용하여 Cloud Volumes ONTAP 암호화 키 관리	62
Azure Key Vault를 사용하여 Cloud Volumes ONTAP 암호화 키 관리	63
Google Cloud KMS를 사용하여 Cloud Volumes ONTAP 암호화 키 관리	71
Cloud Volumes ONTAP에 NetApp 랜섬웨어 보호 솔루션 활성화	73
Cloud Volumes ONTAP에서 WORM 파일의 변조 방지 스냅샷 복사본을 만듭니다.	76
시스템 관리	77
Cloud Volumes ONTAP 업그레이드	77
Cloud Volumes ONTAP 종량제 시스템 등록	87
Cloud Volumes ONTAP 노드 기반 라이선스를 용량 기반 라이선스로 변환	88
Cloud Volumes ONTAP 시스템 시작 및 중지	91
NTP 서버를 사용하여 Cloud Volumes ONTAP 시스템 시간 동기화	94
시스템 쓰기 속도 수정	94
Cloud Volumes ONTAP 클러스터 관리자 비밀번호 변경	95
시스템 추가, 제거 또는 삭제	96
AWS 관리	98

Azure 관리	101
Google Cloud 관리	113
System Manager를 사용하여 Cloud Volumes ONTAP 관리	114
CLI에서 Cloud Volumes ONTAP 관리	117
시스템 상태 및 이벤트	118
Cloud Volumes ONTAP에 대한 AutoSupport 설정 확인	118
Cloud Volumes ONTAP 시스템에 대한 EMS 구성	121

Cloud Volumes ONTAP 사용

라이선스 관리

Cloud Volumes ONTAP에 대한 용량 기반 라이선싱 관리

NetApp Console에서 용량 기반 라이선스를 관리하여 NetApp 계정에 Cloud Volumes ONTAP 시스템에 필요한 용량이 충분한지 확인하세요.

용량 기반 라이선스를 사용하면 TiB 용량당 Cloud Volumes ONTAP 비용을 지불할 수 있습니다.

NetApp Console에서 용량 기반 Cloud Volumes ONTAP 라이선스를 관리할 수 있습니다.



콘솔에서 관리되는 제품과 서비스의 실제 사용량과 측정은 항상 GiB와 TiB로 계산되지만, GB/GiB와 TB/TiB라는 용어도 서로 바꿔 사용됩니다. 이는 Cloud Marketplace 목록, 가격 견적, 목록 설명 및 기타 지원 문서에 반영됩니다.

["Cloud Volumes ONTAP 라이선스에 대해 자세히 알아보세요"](#).

NetApp Console에 라이센스가 추가되는 방식

NetApp 영업 담당자로부터 라이선스를 구매하면 NetApp 일련 번호와 추가 라이선스 세부 정보가 포함된 이메일을 보내드립니다.

그 사이에 콘솔은 NetApp 지원 사이트 계정과 연결된 라이선스에 대한 세부 정보를 얻기 위해 NetApp 라이선스 서비스에 자동으로 쿼리를 보냅니다. 오류가 없으면 라이센스를 추가합니다.

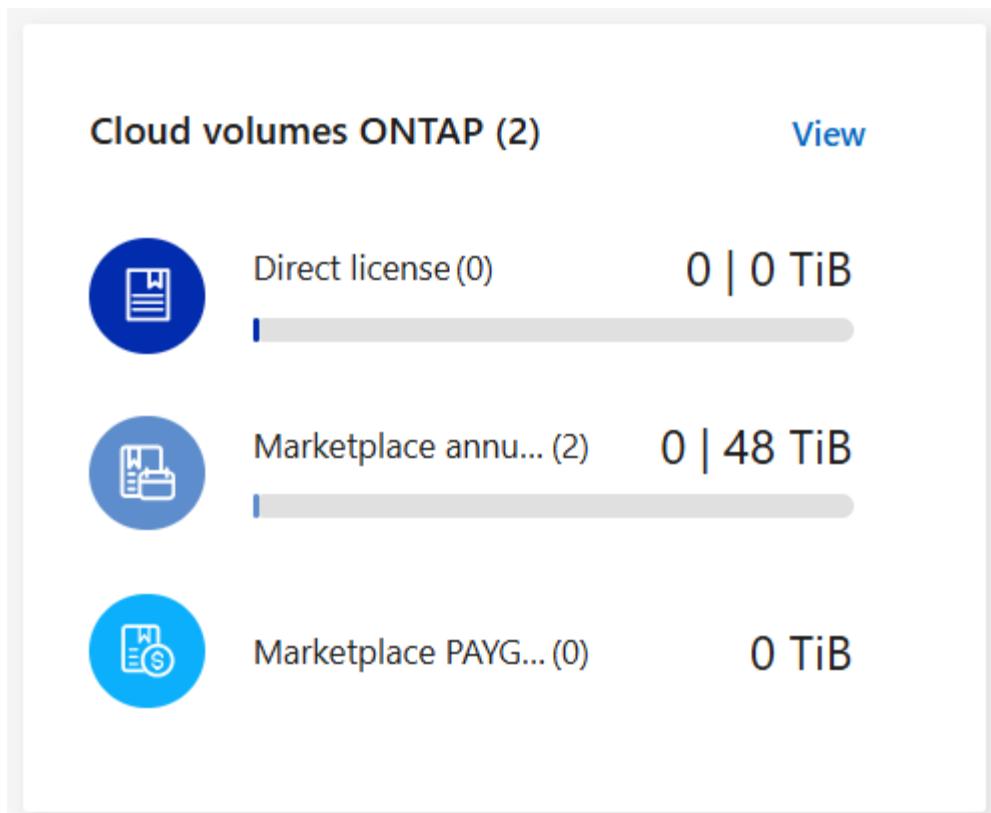
콘솔에서 라이선스를 추가할 수 없는 경우 수동으로 추가해야 합니다. 예를 들어, 콘솔 에이전트가 인터넷 접속이 불가능한 위치에 설치된 경우 라이선스를 직접 추가해야 합니다. ["구매한 라이선스를 계정에 추가하는 방법을 알아보세요."](#).

계정에서 사용된 용량을 확인하세요

콘솔은 계정에서 사용된 총 용량과 라이선스 패키지별로 사용된 용량을 보여줍니다. 이를 통해 요금이 어떻게 청구되는지, 추가 용량을 구매해야 하는지 파악하는 데 도움이 될 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭에서 Cloud Volumes ONTAP 타일은 계정에 대해 현재 프로비저닝된 용량을 표시합니다.



- 직접 라이선스 는 NetApp 계정의 모든 Cloud Volumes ONTAP 시스템에 프로비저닝된 총 용량입니다. 요금은 볼륨 내의 로컬, 사용, 저장 또는 유효 공간에 관계없이 각 볼륨의 프로비저닝된 크기를 기준으로 부과됩니다.
- 연간 계약 은 NetApp에서 구매한 총 라이선스 용량(BYOL(자체 라이선스 사용) 또는 마켓플레이스 계약)입니다.
- PAYGO 는 클라우드 마켓플레이스 구독을 사용하여 프로비저닝된 총 용량입니다. PAYGO를 통한 요금 청구는 사용된 용량이 라이선스 용량보다 높거나 콘솔에서 사용 가능한 BYOL 라이선스가 없는 경우에만 사용됩니다.

3. *보기*를 선택하면 각 라이선스 패키지의 사용된 용량을 확인할 수 있습니다.

4. 구매한 각 패키지 라이선스에 대한 세부 정보를 보려면 라이선스 탭을 선택하세요.

Essentials 패키지에 표시되는 용량을 더 잘 이해하려면 충전 방식을 알아야 합니다. ["Essentials 패키지 요금 청구에 대해 알아보세요"](#).

5. 라이선스 소비 모델에 따른 소비 용량을 확인하려면 구독 탭을 선택하세요. 이 탭에는 PAYGO 및 연간 계약 라이선스가 모두 포함되어 있습니다.

현재 보고 있는 조직과 연관된 구독만 볼 수 있습니다.

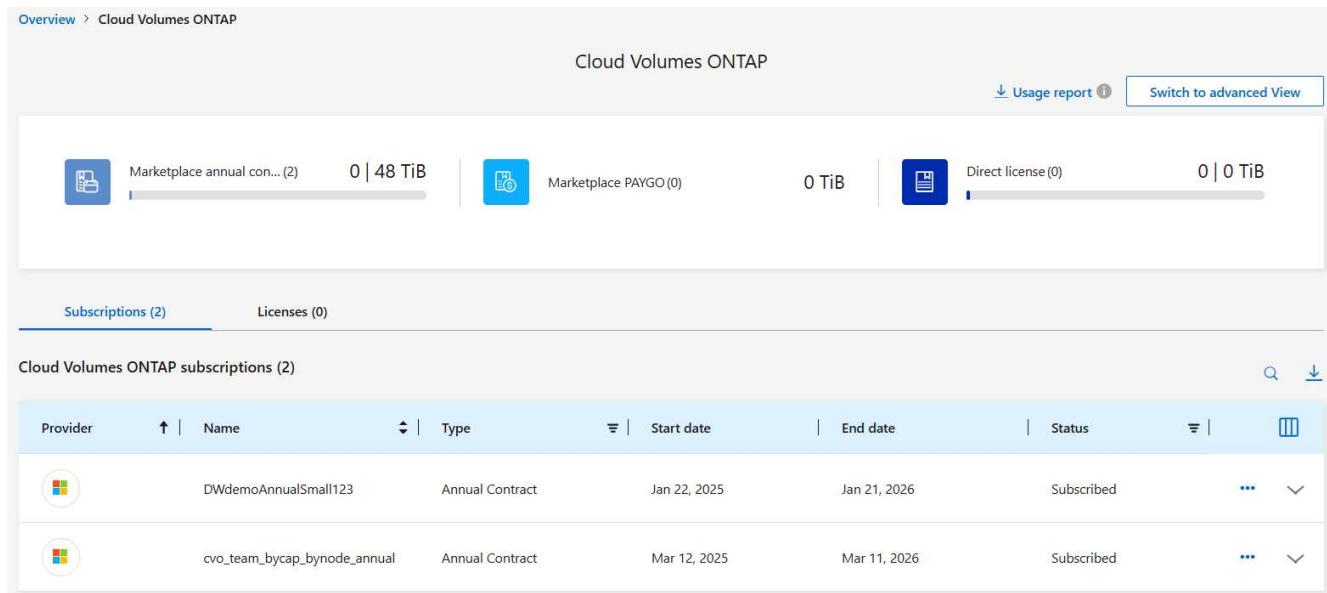
6. 구독에 대한 정보를 볼 때 표에 있는 세부 정보와 상호 작용할 수 있습니다. 더 자세한 내용을 보려면 행을 확장하세요.

- 선택하다  표에 어떤 열을 표시할지 선택합니다. 기본적으로 기간 및 자동 갱신 열은 나타나지 않습니다. 자동 갱신 열에는 Azure 계약에 대한 갱신 정보만 표시됩니다.

패키지 세부 정보 보기

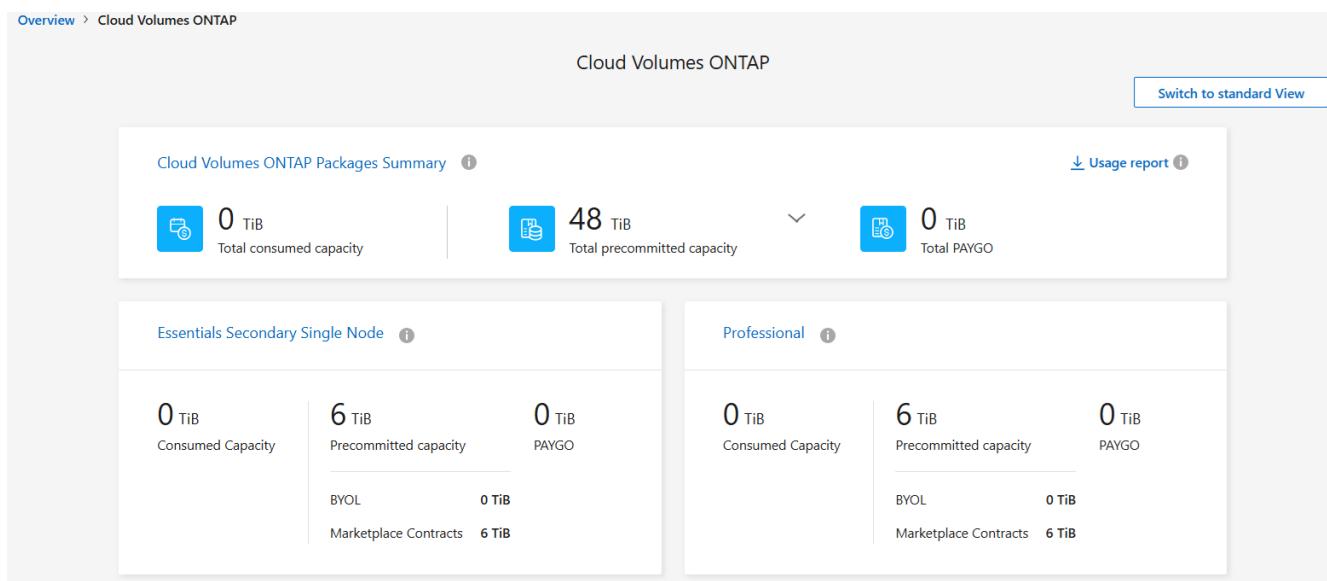
Cloud Volumes ONTAP 페이지에서 레거시 모드로 전환하면 패키지별로 사용된 용량에 대한 세부 정보를 볼 수 있습니다.

1. 원쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭에서 Cloud Volumes ONTAP 타일은 계정에 대해 현재 프로비저닝된 용량을 표시합니다.
3. *보기*를 선택하여 각 라이선스 패키지에 대해 제공된 용량을 확인하세요.
4. *고급 보기로 전환*을 선택하세요.



Provider	Name	Type	Start date	End date	Status
Microsoft	DWdemoAnnualSmall123	Annual Contract	Jan 22, 2025	Jan 21, 2026	Subscribed
Microsoft	cvo_team_bycap_bynode_annual	Annual Contract	Mar 12, 2025	Mar 11, 2026	Subscribed

5. 원하는 패키지의 세부 정보를 확인하세요.



Consumed Capacity	Precommitted capacity	PAYGO
0 TiB	6 TiB	0 TiB
BYOL	0 TiB	
Marketplace Contracts	6 TiB	

충전 방법 변경

용량 기반 라이선싱은 패키지 형태로 제공됩니다. Cloud Volumes ONTAP 시스템을 만들면 비즈니스 요구 사항에 따라 여러 가지 라이선스 패키지 중에서 선택할 수 있습니다. 시스템을 만든 후에 요구 사항이 변경되면 언제든지 패키지를

변경할 수 있습니다. 예를 들어, Essentials 패키지에서 Professional 패키지로 변경할 수 있습니다.

"용량 기반 라이선싱 패키지에 대해 자세히 알아보세요" .

이 작업에 관하여

- 요금 청구 방식을 변경해 NetApp (BYOL)에서 구매한 라이선스를 통해 요금이 청구되는지, 아니면 클라우드 공급업체의 마켓플레이스에서 사용량에 따라 지불하는(PAYGO) 구독을 통해 요금이 청구되는지에는 영향을 미치지 않습니다.

콘솔은 항상 라이선스에 대해 먼저 요금을 청구하려고 시도합니다. 라이선스를 사용할 수 없는 경우 마켓플레이스 구독료에 대한 요금이 부과됩니다. BYOL 구독을 마켓플레이스 구독으로 전환할 필요는 없으며, 그 반대의 경우도 마찬가지입니다.

- 클라우드 공급업체의 마켓플레이스에서 개인 제안이나 계약을 체결한 경우, 계약에 포함되지 않은 청구 방식으로 변경하면 BYOL(NetApp 에서 라이선스를 구매한 경우) 또는 PAYGO로 요금이 청구됩니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 탭에서 *보기*를 선택합니다.
4. *고급 보기로 전환*을 선택하세요.

Provider	Name	Type	Start date	End date	Status	Actions
Microsoft	DWdemoAnnualSmall123	Annual Contract	Jan 22, 2025	Jan 21, 2026	Subscribed	...
Microsoft	cvo_team_bycap_bynode_annual	Annual Contract	Mar 12, 2025	Mar 11, 2026	Subscribed	...

5. 용량 기반 라이선스 표까지 아래로 스크롤하여 *청구 방법 변경*을 선택하세요.

Licenses (0) Subscriptions (4)

Cloud Volumes ONTAP licenses (0)

Serial number ↑ | Package type | Package sub-type | Type | Consumed capacity

No licenses

Change charging method

6. 청구 방법 변경 팝업에서 Cloud Volumes ONTAP 시스템을 선택하고 새로운 청구 방법을 선택한 다음, 패키지 유형을 변경하면 서비스 요금이 변경된다는 사실을 이해했는지 확인하세요.
7. *충전 방법 변경*을 선택하세요.

사용 보고서 다운로드

콘솔에서 4개의 사용 보고서를 다운로드할 수 있습니다. 이러한 사용 보고서는 구독의 용량 세부 정보를 제공하고 Cloud Volumes ONTAP 구독의 리소스에 대한 요금이 어떻게 청구되는지 알려줍니다. 다운로드 가능한 보고서는 특정 시점의 데이터를 수집하여 다른 사람들과 쉽게 공유할 수 있습니다.

Cloud Volumes ONTAP

↓ Usage report ⓘ Switch to advanced View

Marketplace annual con... (2) 0 | 48 TiB Marketplace PAYGO (0) 0 TiB Direct license (0) 0 | 0 TiB

다음 보고서를 다운로드할 수 있습니다. 표시된 용량 값은 TiB 단위입니다.

- 높은 수준의 사용: 이 보고서에는 다음 정보가 포함되어 있습니다.
 - 총 소비 용량
 - 총 사전 약속 용량
 - 총 BYOL 용량
 - 총 마켓플레이스 계약 용량
 - 총 PAYGO 용량
- * Cloud Volumes ONTAP 패키지 사용*: 이 보고서에는 각 패키지에 대한 다음 정보가 포함되어 있습니다.
 - 총 소비 용량
 - 총 사전 약속 용량
 - 총 BYOL 용량
 - 총 마켓플레이스 계약 용량
 - 총 PAYGO 용량
- 스토리지 VM 사용량: 이 보고서는 Cloud Volumes ONTAP 시스템과 스토리지 가상 머신(SVM)에서 청구된 용량이 어떻게 세분화되는지 보여줍니다. 이 정보는 보고서에서만 제공됩니다. 여기에는 다음 정보가 포함되어

있습니다.

- 시스템 ID 및 이름(UUID로 표시됨)
- 클라우드
- NetApp 계정 ID
- 시스템 구성
- SVM 이름
- 프로비저닝된 용량
- 충전 용량 반올림
- 마켓플레이스 청구 기간
- Cloud Volumes ONTAP 패키지 또는 기능
- SaaS Marketplace 구독 이름 청구
- SaaS 마켓플레이스 구독 ID 청구
- 작업 유형

• 볼륨 사용량: 이 보고서는 Cloud Volumes ONTAP 시스템에서 볼륨별로 청구된 용량을 어떻게 세분화하는지 보여줍니다. 이 정보는 콘솔의 어떤 화면에서도 사용할 수 없습니다. 여기에는 다음 정보가 포함됩니다.

- 시스템 ID 및 이름(UUID로 표시됨)
- SVN 이름
- 볼륨 ID
- 볼륨 유형
- 볼륨 프로비저닝 용량



FlexClone 볼륨은 이 보고서에 포함되지 않습니다. 이러한 유형의 볼륨에는 요금이 부과되지 않기 때문입니다.

단계

1. 원쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭에서 Cloud Volumes ONTAP 타일의 *보기*를 선택합니다.
3. *사용 보고서*를 선택하세요.

사용 보고서를 다운로드합니다.

4. 다운로드한 파일을 열어 보고서에 접근하세요.

NetApp Console 통해 Cloud Volumes ONTAP 대한 Keystone 구독 관리

NetApp Console에서 Cloud Volumes ONTAP과 함께 사용할 구독을 활성화하고 구독 서비스 수준에 대한 커밋된 용량 변경을 요청하여 Keystone 구독을 관리합니다. 서비스 수준에 대한 추가 용량을 요청하면 Cloud Volumes ONTAP 시스템에 더 많은 스토리지가 제공됩니다.

NetApp Keystone CapEx나 리스보다 OpEx를 선호하는 고객에게 하이브리드 클라우드 환경을 제공하는 유연한

종량제 구독 기반 서비스입니다.

["Keystone에 대해 자세히 알아보세요"](#)

계정 승인

콘솔에서 Keystone 구독을 사용하고 관리하려면 먼저 NetApp에 문의하여 Keystone 구독으로 콘솔 계정을 인증해야 합니다.

단계

1. NetApp Console 메뉴에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. *Keystone 구독*을 선택하세요.
3. *NetApp Keystone*에 오신 것을 환영합니다* 페이지가 보이면 페이지에 나열된 주소로 이메일을 보내주세요.

NetApp 담당자가 귀하의 계정에 구독에 대한 액세스를 승인하여 귀하의 요청을 처리합니다.

4. 구독 내역을 보려면 *Keystone 구독* 탭으로 돌아가세요.

구독 연결

NetApp 계정을 승인한 후 Keystone 구독을 연결하여 Cloud Volumes ONTAP과 함께 사용할 수 있습니다. 이 작업을 통해 사용자는 새로운 Cloud Volumes ONTAP 시스템에 대한 요금 청구 방법으로 구독을 선택할 수 있습니다.

단계

1. NetApp Console 메뉴에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. *Keystone 구독*을 선택하세요.
3. 연결하려는 구독의 경우 클릭하세요. **... 그리고 *링크***를 선택하세요.

결과

이제 구독이 콘솔 조직이나 계정에 연결되었으며 Cloud Volumes ONTAP 작업 환경을 만들 때 선택할 수 있습니다.

더 많거나 적은 용량을 요청하세요

구독 서비스 수준에 대한 약정 용량을 변경하려면 콘솔에서 직접 NetApp에 요청을 보낼 수 있습니다. 서비스 수준에 대한 추가 용량을 요청하면 Cloud Volumes ONTAP 시스템에 더 많은 스토리지가 제공됩니다.

단계

1. NetApp Console 메뉴에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. *Keystone 구독*을 선택하세요.
3. 용량을 조정하려는 구독의 경우 클릭하세요. **... *자세히 보기 및 편집***을 선택하세요.
4. 하나 이상의 구독에 대해 요청된 약정 용량을 입력하세요.
5. 아래로 스크롤하여 요청에 대한 추가 세부 정보를 입력한 다음 *제출*을 클릭합니다.

결과

귀하의 요청은 NetApp 시스템에 처리를 위한 티켓을 생성합니다.

모니터 사용

Digital Advisor 대시보드를 사용하면 Keystone 구독 사용량을 모니터링하고 보고서를 생성할 수 있습니다.

["구독 사용량 모니터링에 대해 자세히 알아보세요"](#)

구독 연결 해제

콘솔에서 Keystone 구독을 더 이상 사용하지 않으려면 구독 연결을 해제할 수 있습니다. 기존 Cloud Volumes ONTAP 구독에 연결되지 않은 구독만 연결 해제할 수 있습니다.

단계

1. NetApp Console 메뉴에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. *Keystone*을 선택하세요.
3. 연결을 해제하려는 구독의 경우 다음을 클릭하세요. **... *연결 해제***를 선택하세요.

결과

구독이 콘솔 조직 또는 계정에서 연결 해제되어 Cloud Volumes ONTAP 작업 환경을 생성할 때 더 이상 선택할 수 없습니다.

Cloud Volumes ONTAP에 대한 노드 기반 라이선싱 관리

NetApp Console에서 노드 기반 라이선스를 관리하여 각 Cloud Volumes ONTAP 시스템에 필요한 용량을 갖춘 유효한 라이선스가 있는지 확인하세요.

노드 기반 라이선스는 이전 세대 라이선스 모델입니다(신규 고객은 사용할 수 없습니다).

- NetApp에서 구매한 BYOL(Bring Your Own License) 라이선스
- 클라우드 제공업체의 마켓플레이스에서 시간당 결제(PAYGO) 구독

NetApp Console에서 노드 기반 Cloud Volumes ONTAP 라이선스를 관리할 수 있습니다.

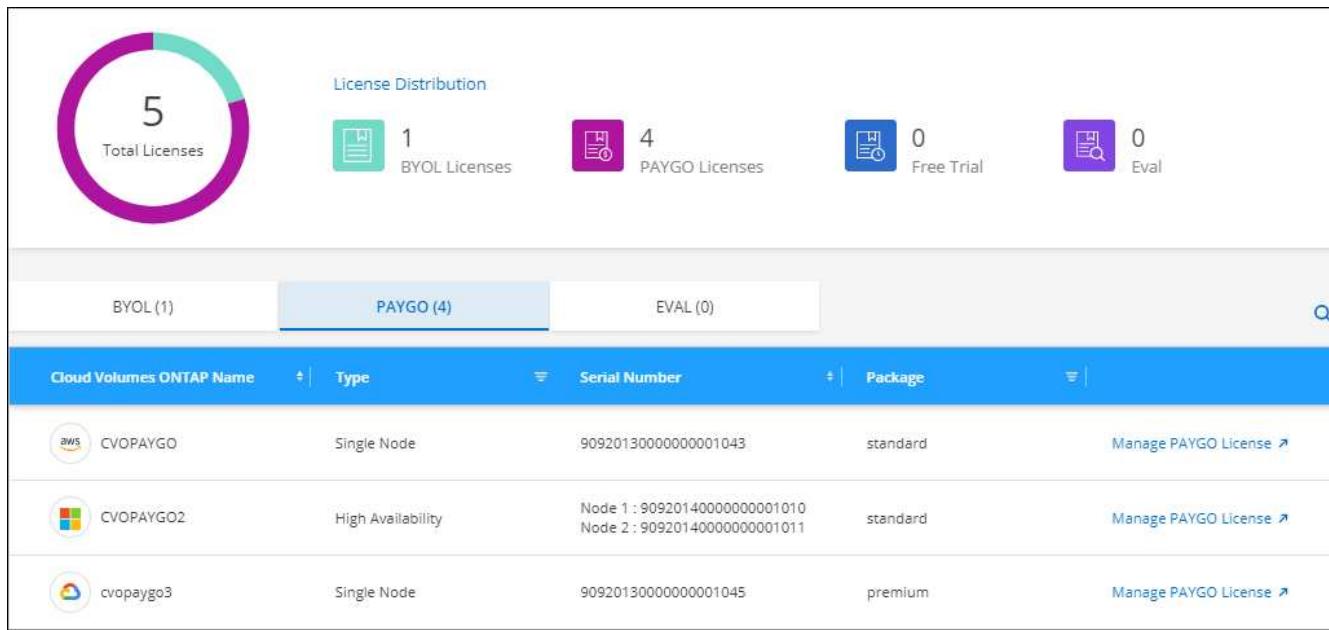
["Cloud Volumes ONTAP 라이선스에 대해 자세히 알아보세요"](#).

PAYGO 라이선스 관리

Licenses and subscriptions 메뉴를 사용하면 일련 번호와 PAYGO 라이선스 유형을 포함하여 각 PAYGO Cloud Volumes ONTAP 시스템에 대한 세부 정보를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. *PAYGO*를 클릭하세요.
6. 각 PAYGO 라이선스에 대한 세부 정보를 표에서 확인하세요.



7. 필요한 경우 *PAYGO 라이선스 관리*를 클릭하여 PAYGO 라이선스를 변경하거나 인스턴스 유형을 변경합니다.

BYOL 라이선스 관리

NetApp에서 직접 구매한 라이선스를 관리하려면 시스템 라이선스와 추가 용량 라이선스를 추가하거나 제거하세요.



NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. ["Cloud Volumes ONTAP에 대한 BYOL 라이선싱의 제한된 가용성"](#).

할당되지 않은 라이선스 추가

새로운 Cloud Volumes ONTAP 시스템을 생성할 때 라이선스를 선택할 수 있도록 콘솔에 노드 기반 라이선스를 추가합니다. 콘솔에서는 이러한 라이선스를 할당되지 않음으로 식별합니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. *할당되지 않음*을 클릭합니다.
6. *할당되지 않은 라이선스 추가*를 클릭합니다.
7. 라이선스의 일련번호를 입력하거나 라이선스 파일을 업로드하세요.

아직 라이센스 파일이 없다면 아래 섹션을 참조하세요.

8. *라이선스 추가*를 클릭하세요.

결과

콘솔은 라이센스를 추가합니다. 라이선스는 새로운 Cloud Volumes ONTAP 시스템과 연결할 때까지 할당되지 않은 것으로 표시됩니다. 그런 다음 라이선스는 * Licenses and subscriptions*의 **BYOL** 탭으로 이동합니다.

할당되지 않은 노드 기반 라이선스 교환

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

라이선스를 교환하면 Cloud Volumes ONTAP 라이선스가 취소되고 서비스에 대한 달러 상당의 라이선스가 생성됩니다.

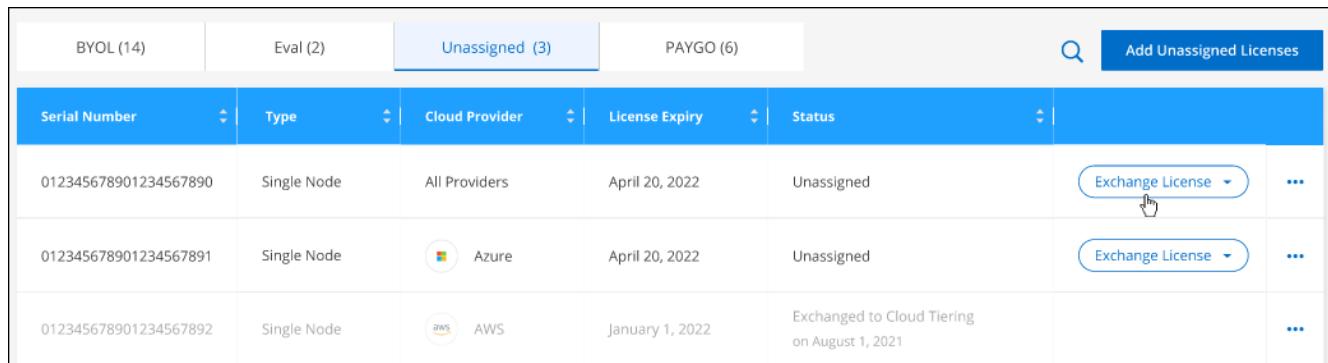
- Cloud Volumes ONTAP HA 쌍에 대한 라이선싱은 51TiB 직접 라이선스로 변환됩니다.
- Cloud Volumes ONTAP 단일 노드에 대한 라이선싱은 32TiB 직접 라이선스로 변환됩니다.

변환된 라이선스의 만료일은 Cloud Volumes ONTAP 라이선스와 동일합니다.

["노드 기반 라이선스를 교환하는 방법에 대한 연습을 확인하세요."](#)

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. *할당되지 않음*을 클릭합니다.
6. *라이선스 교환*을 클릭하세요.



Licenses and Subscriptions					Cloud Volumes ONTAP	
BYOL (14)		Eval (2)		Unassigned (3)		PAYGO (6)
Serial Number	Type	Cloud Provider	License Expiry	Status		
012345678901234567890	Single Node	All Providers	April 20, 2022	Unassigned	Exchange License	...
012345678901234567891	Single Node	 Azure	April 20, 2022	Unassigned	Exchange License	...
012345678901234567892	Single Node	 AWS	January 1, 2022	Exchanged to Cloud Tiering on August 1, 2021		...

7. 라이센스를 교환할 서비스를 선택하세요.
8. 메시지가 표시되면 HA 쌍에 대한 추가 라이선스를 선택하세요.
9. 법적 동의서를 읽고 *동의*를 클릭하세요.

결과

콘솔은 할당되지 않은 라이선스를 선택한 서비스로 변환합니다. 데이터 서비스 라이선스 탭에서 새 라이선스를 볼 수 있습니다.

시스템 라이센스 파일을 얻으세요

대부분의 경우 콘솔은 NetApp 지원 사이트 계정을 사용하여 자동으로 라이선스 파일을 가져올 수 있습니다. 하지만 그렇지 않은 경우에는 라이선스 파일을 수동으로 업로드해야 합니다. 라이선스 파일이 없으면 netapp.com에서 받을 수 있습니다.

단계

1. 로 가다 "[NetApp 라이선스 파일 생성기](#)" NetApp 지원 사이트 자격 증명을 사용하여 로그인하세요.
2. 비밀번호를 입력하고, 제품을 선택하고, 일련번호를 입력하고, 개인정보 보호정책을 읽고 동의함을 확인한 후 ***제출***을 클릭하세요.

예

License Generator

The following fields are pre-populated based on the NetApp SSO login provided.
To download the corresponding NetApp license file, re-enter your SSO password along with the correct Product Line and Product Serial number.

First Name: Ben

Last Name: [redacted]

Company: Network Appliance, Inc

Email Address: [redacted]

Username: [redacted]

Product Line*:

ONTAP Select - Standard

ONTAP Select - Premium

ONTAP Select - Premium XL

Cloud Volumes ONTAP for AWS (single node)

Cloud Volumes ONTAP for AWS (HA)

Cloud Volumes ONTAP for GCP (single node or HA)

Cloud Volumes ONTAP for Microsoft Azure (single node)

Cloud Volumes ONTAP for Microsoft Azure (HA)

Service Level Manager - SLO Advanced

StorageGRID Webscale

StorageGRID WhiteBox

SnapCenter Standard (capacity-based)

Not only is protecting your data required by law, but it may also be required by your organization's policies.

I have read NetApp's new [Global Data Protection Policy](#) and agree to its terms. This may affect my use of my personal data.

3. serialnumber.NLF JSON 파일을 이메일로 받을지, 아니면 직접 다운로드할지 선택하세요.

시스템 라이선스 업데이트

NetApp 담당자에게 연락하여 BYOL 구독을 갱신하면 콘솔이 자동으로 NetApp에서 새 라이선스를 받아 Cloud Volumes ONTAP 시스템에 설치합니다. 콘솔이 보안 인터넷 연결을 통해 라이선스 파일에 액세스할 수 없는 경우 직접 파일을 얻은 다음 수동으로 파일을 업로드할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 ***관리 > Licenses and subscriptions***을 선택합니다.
2. **개요** 탭을 선택하세요.
3. Cloud Volumes ONTAP 탭에서 ***보기***를 선택합니다.
4. 드롭다운에서 ***노드 기반 라이선스***를 선택합니다.
5. **BYOL** 탭에서 Cloud Volumes ONTAP 시스템에 대한 세부 정보를 확장합니다.
6. 시스템 라이선스 옆에 있는 작업 메뉴를 클릭하고 ***라이선스 업데이트***를 선택하세요.
7. 라이선스 파일(HA 쌍이 있는 경우 여러 개)을 업로드합니다.

8. *라이선스 업데이트*를 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 시스템의 라이선스를 업데이트합니다.

추가 용량 라이선스 관리

BYOL 시스템 라이선스로 제공되는 368TiB의 용량보다 더 많은 용량을 할당하려면 Cloud Volumes ONTAP BYOL 시스템에 대한 추가 용량 라이선스를 구매할 수 있습니다. 예를 들어, Cloud Volumes ONTAP에 최대 736TiB의 용량을 할당하기 위해 추가 라이선스 용량 하나를 구매할 수 있습니다. 또는 추가 용량 라이선스 3개를 구매하여 최대 1.4 PiB까지 확보할 수 있습니다.

단일 노드 시스템 또는 HA 쌍에 대해 구매할 수 있는 라이선스 수는 무제한입니다.

용량 라이선스 추가

콘솔 오른쪽 하단에 있는 채팅 아이콘을 통해 문의하여 추가 용량 라이선스를 구매하세요. 라이선스를 구매한 후에는 Cloud Volumes ONTAP 시스템에 적용할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. **BYOL** 탭에서 Cloud Volumes ONTAP 시스템에 대한 세부 정보를 확장합니다.
6. *용량 라이선스 추가*를 클릭하세요.
7. 일련 번호를 입력하거나 라이선스 파일(HA 쌍이 있는 경우 여러 파일)을 업로드합니다.
8. *용량 라이선스 추가*를 클릭하세요.

용량 라이선스 업데이트

추가 용량 라이선스 기간을 연장한 경우 콘솔에서 라이선스를 업데이트해야 합니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. **BYOL** 탭에서 Cloud Volumes ONTAP 시스템에 대한 세부 정보를 확장합니다.
6. 용량 라이선스 옆에 있는 작업 메뉴를 클릭하고 *라이선스 업데이트*를 선택합니다.
7. 라이선스 파일(HA 쌍이 있는 경우 여러 개)을 업로드합니다.
8. *라이선스 업데이트*를 클릭하세요.

용량 라이센스 제거

추가 용량 라이선스가 만료되어 더 이상 사용하지 않는 경우 언제든지 제거할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *관리 > Licenses and subscriptions*을 선택합니다.
2. 개요 탭을 선택하세요.
3. Cloud Volumes ONTAP 타일에서 *보기*를 선택합니다.
4. 드롭다운에서 *노드 기반 라이선스*를 선택합니다.
5. **BYOL** 탭에서 Cloud Volumes ONTAP 시스템에 대한 세부 정보를 확장합니다.
6. 용량 라이선스 옆에 있는 작업 메뉴를 클릭하고 *라이선스 제거*를 선택합니다.
7. *제거*를 클릭하세요.

PAYGO와 BYOL 간 변경

PAYGO 노드별 라이선싱에서 BYOL 노드별 라이선싱으로 시스템을 변환하는 것(또는 그 반대)은 지원되지 않습니다. 사용량에 따른 요금제 구독과 BYOL 구독 간에 전환하려면 새로운 시스템을 배포하고 기존 시스템의 데이터를 새로운 시스템으로 복제해야 합니다.

단계

1. 새로운 Cloud Volumes ONTAP 시스템을 만듭니다.
2. 복제해야 하는 각 볼륨에 대해 시스템 간에 일회성 데이터 복제를 설정합니다.

["시스템 간에 데이터를 복제하는 방법을 알아보세요"](#)

3. 더 이상 필요하지 않은 Cloud Volumes ONTAP 시스템을 종료하려면 원래 시스템을 삭제합니다.

["Cloud Volumes ONTAP 시스템을 삭제하는 방법을 알아보세요"](#).

관련 링크

링크:["노드 기반 라이선스 제공 종료"](#) ["노드 기반 라이센스를 용량 기반으로 변환"](#)

볼륨 및 LUN 관리

Cloud Volumes ONTAP 시스템에서 **FlexVol volume** 생성

초기 Cloud Volumes ONTAP 시스템을 시작한 후 더 많은 스토리지가 필요한 경우 NetApp Console에서 NFS, CIFS 또는 iSCSI에 대한 새로운 FlexVol 볼륨을 생성할 수 있습니다.

새 볼륨을 생성하는 방법은 여러 가지가 있습니다.

- 새 볼륨에 대한 세부 정보를 지정하고 콘솔에서 기본 데이터 집계를 처리하도록 하세요.[자세히 알아보기](#)
- 원하는 데이터 집계에 볼륨을 생성합니다.[자세히 알아보기](#)
- HA 구성의 두 번째 노드에 볼륨을 생성합니다.[자세히 알아보기](#)

시작하기 전에

볼륨 프로비저닝에 대한 몇 가지 참고 사항:

- iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후, "[IQN을 사용하여 호스트에서 LUN에 연결합니다.](#)" .
- ONTAP 시스템 관리자나 ONTAP CLI에서 추가 LUN을 생성할 수 있습니다.
- AWS에서 CIFS를 사용하려면 DNS와 Active Directory를 설정해야 합니다. 자세한 내용은 다음을 참조하세요 . "[AWS용 Cloud Volumes ONTAP에 대한 네트워킹 요구 사항](#)" .
- Cloud Volumes ONTAP 구성이 Amazon EBS Elastic Volumes 기능을 지원하는 경우 다음을 수행할 수 있습니다. "[볼륨을 생성하면 어떤 일이 발생하는지 자세히 알아보세요.](#)" .

볼륨을 생성합니다

볼륨을 생성하는 가장 일반적인 방법은 필요한 볼륨 유형을 지정한 다음 콘솔에서 디스크 할당을 처리하도록 하는 것입니다. 하지만 볼륨을 생성할 특정 집계를 선택할 수도 있습니다.

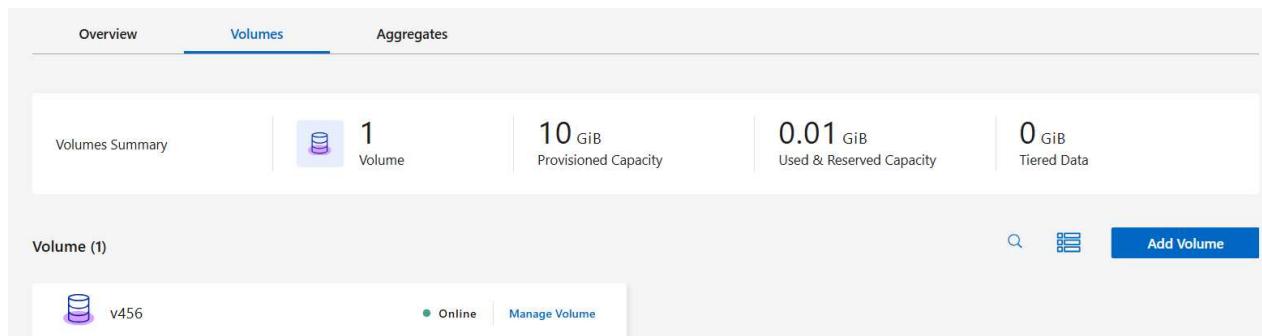
단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 FlexVol volume 프로비저닝하려는 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.

콘솔에서 디스크 할당을 처리하도록 하여 볼륨을 만들거나 볼륨에 대한 특정 집계를 선택할 수 있습니다. Cloud Volumes ONTAP 시스템의 데이터 집계에 대해 잘 이해하고 있는 경우에만 특정 집계를 선택하는 것이 좋습니다.

모든 집계

볼륨 탭을 선택하고 *볼륨 추가*를 클릭합니다



Overview **Volumes** Aggregates

Volumes Summary 1 Volume 10 GiB Provisioned Capacity 0.01 GiB Used & Reserved Capacity 0 GiB Tiered Data

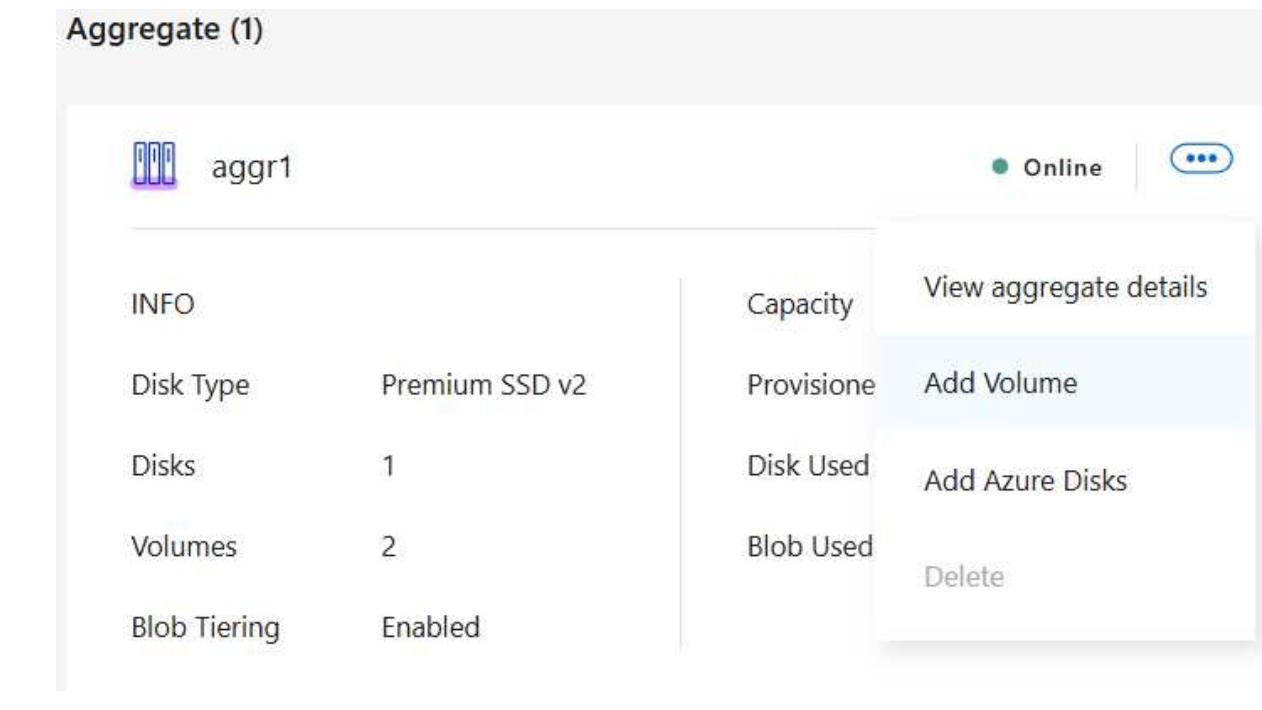
Volume (1)

v456 Online Manage Volume

Add Volume

특정 집계

- 집계 탭에서 필요한 집계로 이동하여 클릭하십시오. **...** 상.
- *볼륨 추가*를 선택하세요



Aggregate (1)

aggr1 Online

View aggregate details

INFO	Capacity
Disk Type: Premium SSD v2	Provisioned
Disks: 1	Disk Used
Volumes: 2	Blob Used
Blob Tiering: Enabled	Delete

3. 마법사의 단계에 따라 볼륨을 생성합니다.

- 세부 정보, 보호 및 태그: 볼륨에 대한 기본 세부 정보를 입력하고 스냅샷 정책을 선택합니다.

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

필드	설명
볼륨 이름	새 볼륨에 입력할 수 있는 식별 가능한 이름입니다.

필드	설명
볼륨 크기	입력할 수 있는 최대 크기는 씬 프로비저닝을 활성화하는지 여부에 따라 크게 달라집니다. 씬 프로비저닝을 활성화하면 현재 사용 가능한 물리적 저장소보다 큰 볼륨을 만들 수 있습니다.
스토리지 VM(SVM)	스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에게 스토리지 및 데이터 서비스를 제공합니다. 이것을 SVM이나 vserver라고 알고 있을 수도 있습니다. Cloud Volumes ONTAP은 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다. 새 볼륨에 대한 스토리지 VM을 지정할 수 있습니다.
스냅샷 정책	스냅샷 복사 정책은 NetApp 스냅샷 복사본이 자동으로 생성되는 빈도와 수를 지정합니다. NetApp 스냅샷 복사본은 성능에 영향을 미치지 않고 최소한의 저장 공간만 필요한 특정 시점의 파일 시스템 이미지입니다. 기본 정책을 선택하거나 아무것도 선택하지 않을 수 있습니다. 일시적인 데이터의 경우 '없음'을 선택할 수 있습니다. 예를 들어 Microsoft SQL Server의 경우 tempdb를 선택합니다.

b. 프로토콜: 볼륨에 대한 프로토콜(NFS, CIFS 또는 iSCSI)을 선택한 다음 필요한 정보를 제공합니다.

CIFS를 선택하고 서버가 설정되지 않은 경우, *다음*을 클릭하면 콘솔에서 CIFS 연결을 설정하라는 메시지가 표시됩니다.

["지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요"](#) .

다음 섹션에서는 지침이 필요할 수 있는 분야에 대해 설명합니다. 설명은 프로토콜별로 구성되어 있습니다.

NFS

접근 제어

볼륨을 클라이언트가 사용할 수 있도록 사용자 지정 내보내기 정책을 선택합니다.

수출 정책

볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 콘솔은 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.

CIFS

권한 및 사용자/그룹

사용자 및 그룹의 SMB 공유에 대한 액세스 수준을 제어할 수 있습니다(액세스 제어 목록 또는 ACL이라고도 함). 로컬 또는 도메인 Windows 사용자나 그룹, 또는 UNIX 사용자나 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자 도메인을 포함해야 합니다.

DNS 기본 및 보조 IP 주소

CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인의 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.

Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.

가입할 Active Directory 도메인

CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.

도메인에 가입할 수 있는 권한이 있는 자격 증명

AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.

CIFS 서버 NetBIOS 이름

AD 도메인에서 고유한 CIFS 서버 이름입니다.

조직 단위

CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.

- Cloud Volumes ONTAP 의 AD 서버로 AWS Managed Microsoft AD를 구성하려면 이 필드에 *OU=Computers,OU=corp*를 입력합니다.
- Cloud Volumes ONTAP 의 AD 서버로 Azure AD Domain Services를 구성하려면 이 필드에 **OU=AADDC Computers** 또는 *OU=AADDC Users*를 입력합니다.<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou>["Azure 설명서: Azure AD Domain Services 관리 도메인에서 OU(조직 단위) 만들기"]
- Cloud Volumes ONTAP 의 AD 서버로 Google Managed Microsoft AD를 구성하려면 이 필드에 *OU=Computers,OU=Cloud*를 입력합니다.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 문서: Google Managed Microsoft AD의 조직 단위"]

DNS 도메인

Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 대부분의 경우 도메인은 AD 도메인과 동일합니다.

NTP 서버

Active Directory DNS를 사용하여 NTP 서버를 구성하려면 *Active Directory 도메인 사용*을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 자세한 내용은 다음을 참조하세요. ["NetApp Console 자동화 문서"](#).

CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

iSCSI

LUN

iSCSI 스토리지 대상은 LUN(논리 단위)이라고 하며 호스트에 표준 블록 장치로 표시됩니다. iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후, ["IQN을 사용하여 호스트에서 LUN에 연결합니다."](#).

개시자 그룹

이니시에이터 그룹(igroup)은 스토리지 시스템의 지정된 LUN에 액세스할 수 있는 호스트를 지정합니다.

호스트 개시자(IQN)

iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 컨버지도 네트워크 어댑터(CNA) 또는 전용 호스트 버스트 어댑터(HBA)를 통해 네트워크에 연결되면 iSCSI 정규 이름(IQN)으로 식별됩니다.

a. 디스크 유형: 성능 요구 사항과 비용 요구 사항에 따라 볼륨의 기본 디스크 유형을 선택합니다.

- ["AWS에서 시스템 크기 조정"](#)
 - ["Azure에서 시스템 크기 조정"](#)
 - ["Google Cloud에서 시스템 크기 조정"](#)

4. 사용 프로필 및 계층화 정책: 볼륨에서 스토리지 효율성 기능을 활성화할지 비활성화할지 선택한 다음 다음을 선택합니다. ["볼륨 티어링 정책"](#).

ONTAP에는 필요한 총 저장 용량을 줄일 수 있는 여러 가지 저장 효율성 기능이 포함되어 있습니다. NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

씬 프로비저닝

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

중복제거

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

압축

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

5. 검토: 볼륨에 대한 세부 정보를 검토한 후 *추가*를 클릭합니다.

결과

콘솔은 Cloud Volumes ONTAP 시스템에 볼륨을 생성합니다.

HA 구성의 두 번째 노드에 볼륨을 생성합니다.

기본적으로 콘솔은 HA 구성의 첫 번째 노드에 볼륨을 생성합니다. 두 노드 모두 클라이언트에 데이터를 제공하는 액티브-액티브 구성이 필요한 경우 두 번째 노드에서 집계와 볼륨을 만들어야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 집계를 관리하려는 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
3. 집계 탭에서 *집계 추가*를 클릭하고 집계를 만듭니다.

4. 홈 노드의 경우 HA 쌍에서 두 번째 노드를 선택합니다.
5. 콘솔에서 집계를 생성한 후, 해당 집계를 선택한 다음 *볼륨 생성*을 클릭합니다.
6. 새 볼륨에 대한 세부 정보를 입력한 다음 *만들기*를 클릭합니다.

결과

콘솔은 HA 쌍의 두 번째 노드에 볼륨을 생성합니다.



여러 AWS 가용성 영역에 배포된 HA 쌍의 경우 볼륨이 있는 노드의 부동 IP 주소를 사용하여 볼륨을 클라이언트에 마운트해야 합니다.

볼륨을 생성한 후

CIFS 공유를 프로비저닝한 경우 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인합니다.

볼륨에 할당량을 적용하려면 ONTAP System Manager나 ONTAP CLI를 사용해야 합니다. 할당량을 사용하면 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템에서 볼륨 관리

NetApp Console에서 볼륨과 CIFS 서버를 관리할 수 있습니다. 용량 문제를 피하기 위해 볼륨을 이동할 수도 있습니다.

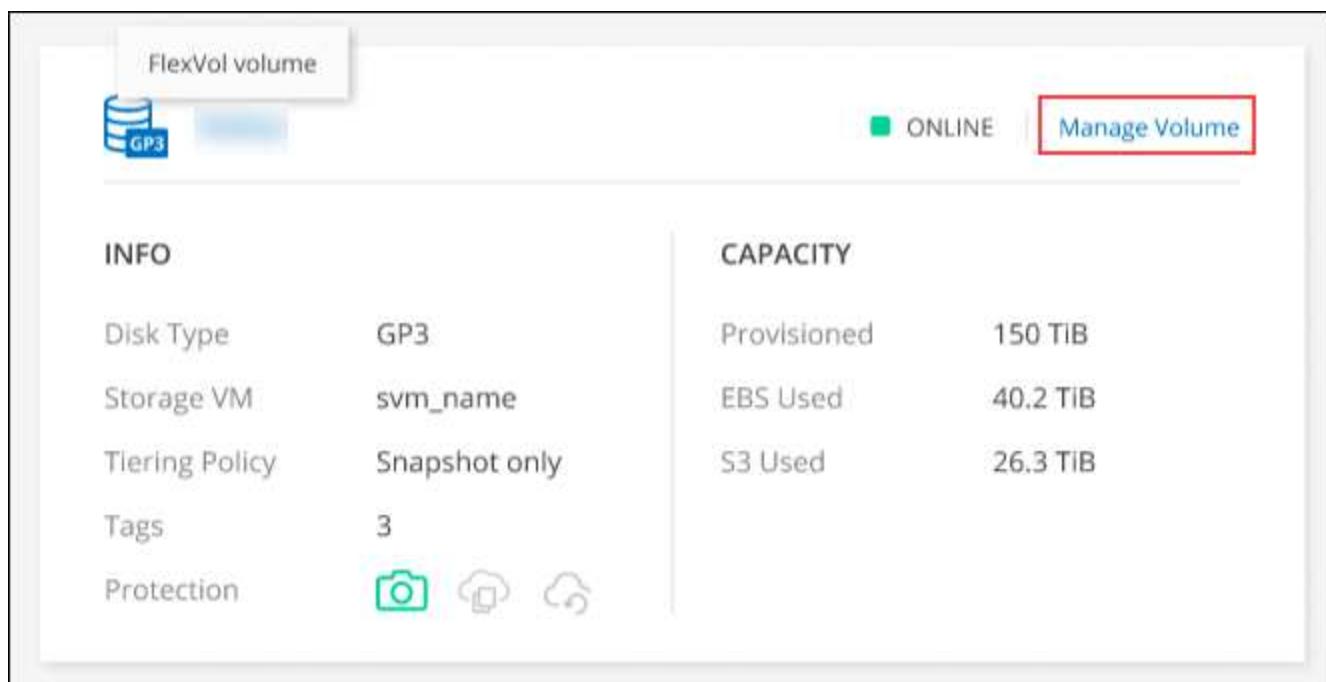
NetApp Console 표준 보기에서 볼륨을 관리하거나 고급 볼륨 관리를 위해 콘솔에 포함된 ONTAP 시스템 관리자를 통해 볼륨을 관리할 수 있습니다. 표준 보기는 볼륨을 수정하기 위한 제한된 옵션 세트를 제공합니다. System Manager는 복제, 크기 조정, 랜섬웨어 방지 설정 변경, 분석, 보호 및 활동 추적, 계층 간 볼륨 이동 등 고급 수준의 관리 기능을 제공합니다. 자세한 내용은 다음을 참조하세요. ["System Manager를 사용하여 Cloud Volumes ONTAP 관리"](#).

볼륨 관리

콘솔의 표준 보기를 사용하면 스토리지 요구 사항에 따라 볼륨을 관리할 수 있습니다. 볼륨을 보고, 편집하고, 복제하고, 복원하고, 삭제할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 볼륨을 관리할 Cloud Volumes ONTAP 시스템을 두 번 클릭합니다.
3. 볼륨 탭을 선택하세요.



The screenshot shows a detailed view of a volume named 'GP3'. The top navigation bar includes 'FlexVol volume' and a 'Manage Volume' button, which is highlighted with a red box. The main area is divided into 'INFO' and 'CAPACITY' sections. The 'INFO' section contains the following data:

Disk Type	GP3
Storage VM	svm_name
Tiering Policy	Snapshot only
Tags	3
Protection	

The 'CAPACITY' section displays the following data:

Provisioned	150 TiB
EBS Used	40.2 TiB
S3 Used	26.3 TiB

4. 필요한 볼륨 탭에서 *볼륨 관리*를 클릭합니다.

일	행동
볼륨에 대한 정보 보기	볼륨 관리 패널의 볼륨 작업에서 *볼륨 세부 정보 보기*를 클릭합니다.
NFS 마운트 명령 받기	a. 볼륨 관리 패널의 볼륨 작업에서 *마운트 명령*을 클릭합니다. b. *복사*를 클릭하세요.

일	행동
볼륨 복제	<p>a. 볼륨 관리 패널의 볼륨 작업에서 *볼륨 복제*를 클릭합니다.</p> <p>b. 필요에 따라 복제 이름을 수정한 다음 *복제*를 클릭합니다.</p> <p>이 프로세스는 FlexClone 볼륨을 생성합니다. FlexClone 볼륨은 메타데이터에 소량의 공간을 사용하고 데이터가 변경되거나 추가될 때만 추가 공간을 사용하기 때문에 공간 효율적인 쓰기 가능한 지정 시간 복사본입니다.</p> <p>FlexClone 볼륨에 대해 자세히 알아보려면 다음을 참조하세요. "ONTAP 9 논리 스토리지 관리 가이드".</p>
볼륨 편집(읽기-쓰기 볼륨만 해당)	<p>a. 볼륨 관리 패널의 볼륨 작업에서 *볼륨 설정 편집*을 클릭합니다.</p> <p>b. 볼륨의 스냅샷 정책, NFS 프로토콜 버전, NFS 액세스 제어 목록(내보내기 정책) 또는 공유 권한을 수정한 다음 *적용*을 클릭합니다.</p> <p> 사용자 정의 스냅샷 정책이 필요한 경우 ONTAP System Manager를 사용하여 만들 수 있습니다.</p>
볼륨 삭제	<p>a. 볼륨 관리 패널의 볼륨 작업에서 *볼륨 삭제*를 클릭합니다.</p> <p>b. 볼륨 삭제 창에서 삭제하려는 볼륨의 이름을 입력합니다.</p> <p>c. 다시 한번 *삭제*를 클릭하여 확인하세요.</p>
필요에 따라 스냅샷 사본을 만듭니다.	<p>a. 볼륨 관리 패널의 보호 작업에서 *스냅샷 복사본 만들기*를 클릭합니다.</p> <p>b. 필요한 경우 이름을 변경한 다음 *만들기*를 클릭합니다.</p>
스냅샷 복사본에서 새 볼륨으로 데이터 복원	<p>a. 볼륨 관리 패널의 보호 작업에서 *스냅샷 복사본에서 복원*을 클릭합니다.</p> <p>b. 스냅샷 복사본을 선택하고 새 볼륨의 이름을 입력한 다음 *복원*을 클릭합니다.</p>
기본 디스크 유형 변경	<p>a. 볼륨 관리 패널의 고급 작업에서 *디스크 유형 변경*을 클릭합니다.</p> <p>b. 디스크 유형을 선택한 다음 *변경*을 클릭합니다.</p> <p> 콘솔은 선택한 디스크 유형을 사용하는 기존 집계로 볼륨을 이동하거나 볼륨에 대한 새 집계를 만듭니다.</p>
티어링 정책 변경	<p>a. 볼륨 관리 패널의 고급 작업에서 *계층화 정책 변경*을 클릭합니다.</p> <p>b. 다른 정책을 선택하고 *변경*을 클릭하세요.</p> <p> 콘솔은 계층화를 통해 선택한 디스크 유형을 사용하는 기존 집계로 볼륨을 이동하거나 볼륨에 대한 새 집계를 만듭니다.</p>

일	행동
볼륨 삭제	<ul style="list-style-type: none"> a. 볼륨을 선택한 다음 *삭제*를 클릭합니다. b. 대화 상자에 볼륨 이름을 입력합니다. c. 다시 한번 *삭제*를 클릭하여 확인하세요.

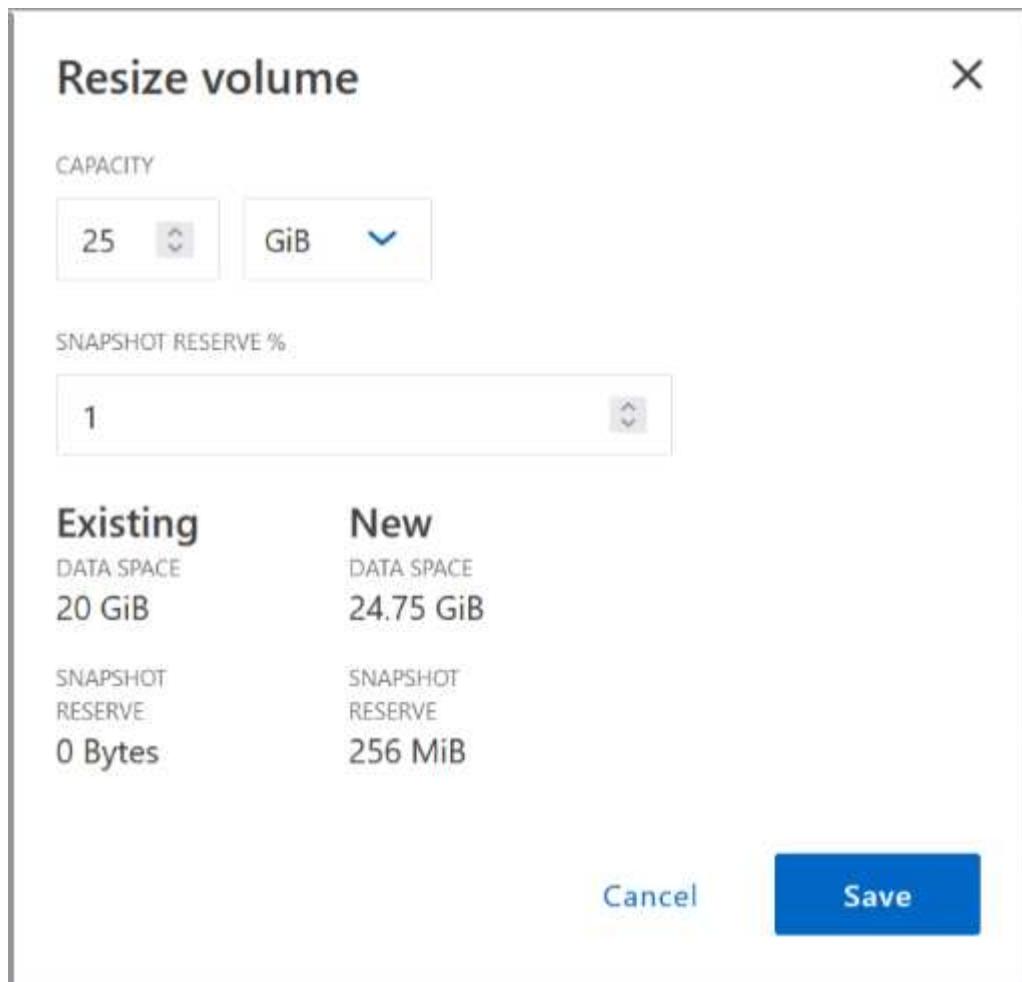
볼륨 크기 조정

기본적으로 볼륨은 공간이 부족하면 자동으로 최대 크기로 커집니다. 기본값은 1,000이며, 이는 볼륨이 원래 크기의 11배까지 커질 수 있음을 의미합니다. 이 값은 콘솔 에이전트 설정에서 구성할 수 있습니다.

볼륨 크기를 조정해야 하는 경우 콘솔의 ONTAP 시스템 관리자에서 조정할 수 있습니다.

단계

1. ONTAP 시스템 관리자를 통해 볼륨 크기를 조정하려면 시스템 관리자 보기 를 클릭합니다. ["시작하는 방법"](#) .
2. 왼쪽 탐색 메뉴에서 *저장소 > 볼륨*을 선택합니다.
3. 볼륨 목록에서 크기를 조절해야 하는 볼륨을 식별합니다.
4. 옵션 아이콘을 클릭하세요  .
5. *크기 조정*을 선택하세요.
6. 볼륨 크기 조정 화면에서 필요에 따라 용량과 스냅샷 예약 비율을 편집합니다. 기존의 사용 가능한 공간과 수정된 용량을 비교할 수 있습니다.
7. *저장*을 클릭하세요.



볼륨 크기를 조정할 때는 시스템의 용량 제한을 고려해야 합니다. 로 가다 ["Cloud Volumes ONTAP 릴리스 노트"](#) 자세한 내용은.

CIFS 서버 수정

DNS 서버나 Active Directory 도메인을 변경하는 경우 Cloud Volumes ONTAP 의 CIFS 서버를 수정해야 클라이언트에 계속해서 스토리지를 제공할 수 있습니다.

단계

1. Cloud Volumes ONTAP 시스템의 개요 탭에서 오른쪽 패널 아래에 있는 기능 탭을 클릭합니다.
2. CIFS 설정 필드에서 *연필 아이콘*을 클릭하여 CIFS 설정 창을 표시합니다.
3. CIFS 서버에 대한 설정을 지정합니다.

일	행동
스토리지 VM(SVM) 선택	Cloud Volume ONTAP 스토리지 가상 머신(SVM)을 선택하면 구성된 CIFS 정보가 표시됩니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.
도메인에 가입할 수 있는 권한이 있는 자격 증명	AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.

일	행동
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인에 대한 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 SRV(서비스 위치 레코드)가 포함되어야 합니다. <code>ifdef::gcp[]</code> Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다. <code>endif::gcp[]</code>
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 대부분의 경우 도메인은 AD 도메인과 동일합니다.
CIFS 서버 NetBIOS 이름	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. <ul style="list-style-type: none"> Cloud Volumes ONTAP 의 AD 서버로 AWS Managed Microsoft AD를 구성하려면 이 필드에 *OU=Computers,OU=corp*를 입력합니다. Cloud Volumes ONTAP 의 AD 서버로 Azure AD Domain Services를 구성하려면 이 필드에 OU=AADDC Computers 또는 *OU=AADDC Users*를 입력합니다. "Azure 설명서: Azure AD Domain Services 관리 도메인에서 OU(조직 단위) 만들기" Cloud Volumes ONTAP 의 AD 서버로 Google Managed Microsoft AD를 구성하려면 이 필드에 *OU=Computers,OU=Cloud*를 입력합니다. "Google Cloud 문서: Google Managed Microsoft AD의 조직 단위"

4. *설정*을 클릭하세요.

결과

Cloud Volumes ONTAP CIFS 서버에 변경 사항을 업데이트합니다.

볼륨 이동

용량 활용도, 성능 향상, 서비스 수준 계약 충족을 위해 볼륨을 이동합니다.

ONTAP 시스템 관리자에서 볼륨과 대상 집계를 선택하고, 볼륨 이동 작업을 시작하고, 선택적으로 볼륨 이동 작업을 모니터링하여 볼륨을 이동할 수 있습니다. 시스템 관리자를 사용하면 볼륨 이동 작업이 자동으로 완료됩니다.

단계

1. ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 볼륨을 집계로 이동합니다.

대부분의 경우 시스템 관리자를 사용하여 볼륨을 이동할 수 있습니다.

지침은 다음을 참조하세요. ["ONTAP 9 볼륨 이동 익스프레스 가이드"](#) .

콘솔에 작업 필요 메시지가 표시되면 볼륨을 이동합니다.

콘솔에 볼륨을 이동하면 용량 문제를 방지할 수 있지만, 문제를 직접 해결해야 한다는 내용의 '조치 필요' 메시지가 표시될 수 있습니다. 이런 일이 발생하면 문제를 해결하는 방법을 파악한 다음 하나 이상의 볼륨을 이동해야 합니다.



집계된 용량이 90% 사용률에 도달하면 콘솔에 다음과 같은 조치 필요 메시지가 표시됩니다. 데이터 계층화가 활성화된 경우 집계가 사용 용량의 80%에 도달하면 메시지가 표시됩니다. 기본적으로 10%의 여유 공간이 데이터 계층화를 위해 예약되어 있습니다. ["데이터 계층화를 위한 여유 공간 비율에 대해 자세히 알아보세요"](#).

단계

1. 용량 문제를 해결하는 방법을 식별합니다. .
2. 분석에 따라 용량 문제를 방지하기 위해 볼륨을 이동합니다.
 - 용량 문제를 피하기 위해 볼륨을 다른 시스템으로 이동합니다. .
 - 용량 문제를 방지하기 위해 볼륨을 다른 집계로 이동합니다. .

용량 문제를 해결하는 방법을 식별합니다.

콘솔에서 용량 문제를 방지하기 위한 볼륨 이동에 대한 권장 사항을 제공할 수 없는 경우 이동해야 할 볼륨을 식별하고 동일한 시스템의 다른 집계로 이동해야 할지 아니면 다른 시스템으로 이동해야 할지 결정해야 합니다.

단계

1. 집계가 용량 한도에 도달한 것을 식별하려면 작업 필요 메시지의 고급 정보를 확인하세요.

예를 들어, 고급 정보에는 다음과 비슷한 내용이 나와 있어야 합니다. 집계 aggr1이 용량 한도에 도달했습니다.
2. 집계에서 이동할 하나 이상의 볼륨을 식별합니다.
 - a. Cloud Volumes ONTAP 시스템에서 *집계 탭*을 클릭합니다.
 - b. 집계 타일에서 다음을 클릭합니다. *** 아이콘을 클릭한 다음 *집계 세부 정보 보기*를 클릭하세요.
 - c. 집계 세부 정보 화면의 개요 탭에서 각 볼륨의 크기를 검토하고 집계에서 이동할 볼륨을 하나 이상 선택합니다.

나중에 추가 용량 문제가 발생하지 않도록 전체적으로 여유 공간을 확보할 수 있을 만큼 큰 볼륨을 선택해야 합니다.

Aggregate Details			
aggr1			
Overview		Capacity Allocation	Provider Properties
State	online		
Home Node	Storage 1		
Encryption Type	cloudEncrypted		
Volumes	2 ^		
	Volume 1 (1 GiB)		
	Volume 2 (500 GiB)		

3. 시스템이 디스크 한도에 도달하지 않은 경우 볼륨을 동일한 시스템의 기존 집계나 새 집계로 이동해야 합니다.

자세한 내용은 다음을 참조하세요. [용량 문제를 방지하기 위해 볼륨을 다른 집계로 이동합니다.](#)

4. 시스템이 디스크 한도에 도달한 경우 다음 중 하나를 수행하세요.

- 사용하지 않는 볼륨을 삭제합니다.
- 집계된 공간을 확보하기 위해 볼륨을 재배열합니다.

자세한 내용은 다음을 참조하세요. [용량 문제를 방지하기 위해 볼륨을 다른 집계로 이동합니다.](#)

- 두 개 이상의 볼륨을 공간이 있는 다른 시스템으로 이동합니다.

자세한 내용은 다음을 참조하세요. [용량 문제를 방지하기 위해 볼륨을 다른 집계로 이동합니다.](#)

용량 문제를 피하기 위해 볼륨을 다른 시스템으로 이동합니다.

용량 문제를 방지하기 위해 하나 이상의 볼륨을 다른 Cloud Volumes ONTAP 시스템으로 이동할 수 있습니다. 시스템이 디스크 한도에 도달한 경우 이 작업이 필요할 수 있습니다.

이 작업에 관하여

이 작업의 단계에 따라 다음과 같은 작업 필요 메시지를 수정할 수 있습니다.

볼륨을 이동하는 것은 용량 문제를 방지하기 위해 필요합니다. 하지만 시스템이 디스크 한도에 도달했기 때문에 콘솔에서 이 작업을 수행할 수 없습니다.

단계

- 사용 가능한 용량이 있는 Cloud Volumes ONTAP 시스템을 확인하거나 새로운 시스템을 배포합니다.

2. 볼륨의 일회성 데이터 복제를 수행하려면 소스 시스템을 대상 시스템으로 끌어서 놓습니다.

자세한 내용은 다음을 참조하세요.["시스템 간 데이터 복제"](#) .

3. 복제 상태 페이지로 이동한 다음 SnapMirror 관계를 해제하여 복제된 볼륨을 데이터 보호 볼륨에서 읽기/쓰기 볼륨으로 변환합니다.

자세한 내용은 다음을 참조하세요.["데이터 복제 일정 및 관계 관리"](#) .

4. 데이터 액세스를 위한 볼륨을 구성합니다.

데이터 액세스를 위한 대상 볼륨 구성에 대한 정보는 다음을 참조하십시오.["ONTAP 9권 재해 복구 익스프레스 가이드"](#) .

5. 원본 볼륨을 삭제합니다.

자세한 내용은 다음을 참조하세요.["볼륨 관리"](#) .

용량 문제를 방지하기 위해 볼륨을 다른 집계로 이동합니다.

용량 문제를 방지하기 위해 하나 이상의 볼륨을 다른 집계로 이동할 수 있습니다.

이 작업에 관하여

이 작업의 단계에 따라 다음과 같은 작업 필요 메시지를 수정할 수 있습니다.

용량 문제를 방지하려면 두 개 이상의 볼륨을 이동하는 것이 필요합니다. 하지만 콘솔에서는 이 작업을 대신 수행할 수 없습니다.

단계

1. 이동해야 하는 볼륨에 대한 사용 가능한 용량이 기준 집계에 있는지 확인하세요.

a. Cloud Volumes ONTAP 시스템에서 *집계 탭*을 클릭합니다.

b. 필요한 집계 타일에서 다음을 클릭합니다.*** 아이콘을 클릭한 다음 *집계 세부 정보 보기*를 클릭하면 사용 가능한 용량(프로비저닝된 크기에서 사용된 집계 용량을 뺀 값)을 볼 수 있습니다.

INFO		CAPACITY	
Disk Type	GP3 3000 IOPS	Provisioned size	907.12 GiB
Disks	4	EBS Used	1.13 GiB
Volumes	2	S3 Used	0 GiB
Elastic Volumes	Enabled		
S3 Tiering	Enabled		

2. 필요한 경우 기존 집계에 디스크를 추가합니다.
 - a. 집계를 선택한 다음 클릭하세요. **...** 아이콘 > 디스크 추가.
 - b. 추가할 디스크 수를 선택한 다음 *추가*를 클릭합니다.
3. 사용 가능한 용량이 있는 집계가 없으면 새 집계를 만듭니다.

자세한 내용은 다음을 참조하세요. ["집계 생성"](#) .

4. ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 볼륨을 집계로 이동합니다.
5. 대부분의 경우 시스템 관리자를 사용하여 볼륨을 이동할 수 있습니다.

지침은 다음을 참조하세요. ["ONTAP 9 볼륨 이동 익스프레스 가이드"](#) .

볼륨 이동이 느리게 수행되는 이유

다음 조건 중 하나라도 Cloud Volumes ONTAP 에 해당하는 경우 볼륨을 이동하는 데 예상보다 시간이 더 오래 걸릴 수 있습니다.

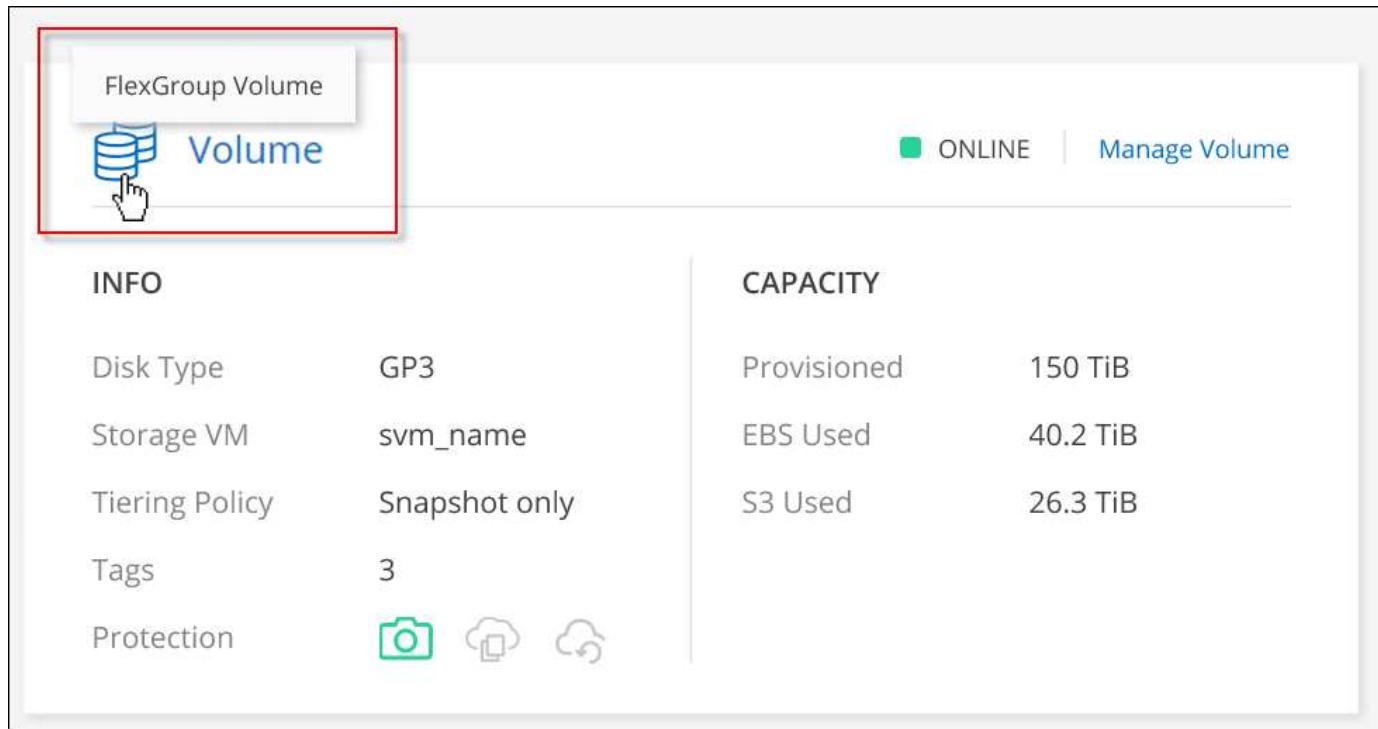
- 볼륨은 복제본입니다.
- 볼륨은 클론의 부모입니다.
- 소스 또는 대상 집계에는 단일 처리량 최적화 HDD(st1) 디스크가 있습니다.
- 집계 중 하나는 객체에 대해 이전의 명명 체계를 사용합니다. 두 집계 모두 동일한 이름 형식을 사용해야 합니다.

9.4 릴리스 또는 이전 릴리스에서 집계에 대한 데이터 계층화가 활성화된 경우 이전 명명 체계가 사용됩니다.

- 소스 및 대상 집계의 암호화 설정이 일치하지 않거나 키 재지정이 진행 중입니다.
- 볼륨 이동 시 계층화 정책을 변경하기 위해 *-tiering-policy* 옵션이 지정되었습니다.
- 볼륨 이동 시 *-generate-destination-key* 옵션이 지정되었습니다.

FlexGroup 볼륨 보기

ONTAP 시스템 관리자나 ONTAP CLI를 통해 생성된 FlexGroup 볼륨은 콘솔의 볼륨 탭을 통해 직접 볼 수 있습니다. 전용 볼륨 타일을 통해 FlexGroup 볼륨에 대한 자세한 정보를 볼 수 있으며, 아이콘에 마우스를 올려 놓으면 각 FlexGroup 볼륨 그룹이 식별됩니다. 또한 볼륨 목록 보기에서 볼륨 스타일 열을 통해 FlexGroup 볼륨을 식별하고 정렬할 수 있습니다.



INFO		CAPACITY	
Disk Type	GP3	Provisioned	150 TiB
Storage VM	svm_name	EBS Used	40.2 TiB
Tiering Policy	Snapshot only	S3 Used	26.3 TiB
Tags	3		
Protection	  		



현재는 콘솔에서만 기존 FlexGroup 볼륨을 볼 수 있습니다. 콘솔에서 FlexGroup 볼륨을 생성할 수 없습니다.

비활성 Cloud Volumes ONTAP 데이터를 저렴한 개체 스토리지로 계층화합니다.

자주 사용되는 데이터의 경우 SSD 또는 HDD 성능 계층을 사용하고, 비활성 데이터의 경우 객체 스토리지 용량 계층을 사용하면 Cloud Volumes ONTAP의 스토리지 비용을 줄일 수 있습니다. 데이터 계층화는 FabricPool 기술을 기반으로 합니다. 상위 수준 개요는 다음을 참조하세요. ["데이터 계층화 개요"](#).

데이터 계층화를 설정하려면 다음을 수행해야 합니다.

1

지원되는 구성을 선택하세요

대부분의 구성이 지원됩니다. 최신 버전을 실행하는 Cloud Volumes ONTAP 시스템이 있다면 문제없이 사용할 수 있습니다. ["자세히 알아보기"](#).

2

Cloud Volumes ONTAP과 개체 스토리지 간 연결을 보장합니다.

- AWS의 경우 S3에 대한 VPC 엔드포인트가 필요합니다. [자세히 알아보기](#).

- Azure의 경우 NetApp Console 필요한 권한이 있는 한 아무것도 할 필요가 없습니다. [자세히 알아보기](#).
- Google Cloud의 경우 Private Google Access에 대한 서브넷을 구성하고 서비스 계정을 설정해야 합니다. [자세히 알아보기](#).

3

계층화가 활성화된 집계가 있는지 확인하세요.

볼륨에서 데이터 계층화를 활성화하려면 집계에서 데이터 계층화를 활성화해야 합니다. 새로운 볼륨과 기존 볼륨에 대한 요구 사항을 알고 있어야 합니다. [자세히 알아보기](#).

4

볼륨을 생성, 수정 또는 복제할 때 계층화 정책을 선택하세요.

NetApp Console 볼륨을 생성, 수정 또는 복제할 때 계층화 정책을 선택하라는 메시지를 표시합니다.

- ["읽기-쓰기 볼륨의 계층 데이터"](#)
- ["데이터 보호 볼륨의 계층 데이터"](#)

데이터 계층화에 필요하지 않은 것은 무엇입니까?

- 데이터 계층화를 활성화하기 위해 기능 라이선스를 설치할 필요는 없습니다.
- 용량 계층에 대한 객체 저장소를 만들 필요가 없습니다. 콘솔이 그 일을 대신해 줍니다.
- 시스템 수준에서 데이터 계층화를 활성화할 필요는 없습니다.

콘솔은 시스템을 생성할 때 콜드 데이터에 대한 객체 저장소를 생성합니다. [연결이나 권한 문제가 없는 한](#) 그 후에는 볼륨에서 데이터 계층화를 활성화하기만 하면 됩니다(어떤 경우에는 [집계에 대하여](#)).

데이터 계층화를 지원하는 구성

특정 구성 및 기능을 사용할 때 데이터 계층화를 활성화할 수 있습니다.

AWS 지원

- AWS에서는 Cloud Volumes ONTAP 9.2부터 데이터 계층화가 지원됩니다.
- 성능 계층은 일반 용도 SSD(gp3 또는 gp2) 또는 프로비저닝된 IOPS SSD(io1)가 될 수 있습니다.



처리량 최적화 HDD(st1)를 사용할 때 개체 스토리지에 데이터를 계층화하는 것은 권장하지 않습니다.

- 비활성 데이터는 Amazon S3 버킷에 계층화됩니다. 다른 공급자로의 계층화는 지원되지 않습니다.

Azure 지원

- Azure에서는 데이터 계층화가 다음과 같이 지원됩니다.
 - 단일 노드 시스템을 갖춘 버전 9.4
 - HA 쌍이 포함된 버전 9.6

- 성능 계층은 프리미엄 SSD 관리 디스크, 표준 SSD 관리 디스크 또는 표준 HDD 관리 디스크가 될 수 있습니다.
- 비활성 데이터는 Microsoft Azure Blob에 계층화됩니다. 다른 공급자로의 계층화는 지원되지 않습니다.

Google Cloud 지원

- Google Cloud에서는 Cloud Volumes ONTAP 9.6부터 데이터 계층화가 지원됩니다.
- 성능 계층은 SSD 영구 디스크, 균형 영구 디스크 또는 표준 영구 디스크가 될 수 있습니다.
- 비활성 데이터는 Google Cloud Storage에 저장됩니다. 다른 공급자로의 계층화는 지원되지 않습니다.

기능 상호 운용성

- 데이터 계층화는 암호화 기술을 통해 지원됩니다.
- 볼륨에서 씬 프로비저닝을 활성화해야 합니다.

요구 사항

클라우드 제공업체에 따라 Cloud Volumes ONTAP 콜드 데이터를 개체 스토리지로 계층화할 수 있도록 특정 연결 및 권한을 설정해야 합니다.

AWS S3에 콜드 데이터를 계층화하기 위한 요구 사항

Cloud Volumes ONTAP S3에 연결되어 있는지 확인하세요. 해당 연결을 제공하는 가장 좋은 방법은 S3 서비스에 대한 VPC 엔드포인트를 만드는 것입니다. 자침은 다음을 참조하세요. ["AWS 설명서: 게이트웨이 엔드포인트 생성"](#).

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

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

Azure Blob 스토리지에 콜드 데이터를 계층화하기 위한 요구 사항

콘솔에 필요한 권한이 있는 한 성능 계층과 용량 계층 간에 연결을 설정할 필요가 없습니다. 콘솔 에이전트의 사용자 지정 역할에 다음 권한이 있는 경우 콘솔에서 VNet 서비스 엔드포인트를 사용할 수 있습니다.

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

사용자 정의 역할에는 기본적으로 권한이 포함됩니다. ["콘솔 에이전트에 대한 Azure 권한 보기"](#)

Google Cloud Storage 버킷에 콜드 데이터를 계층화하기 위한 요구 사항

- Cloud Volumes ONTAP 이 있는 서브넷은 비공개 Google 액세스로 구성되어야 합니다. 자침은 다음을 참조하세요. ["Google Cloud 문서: 비공개 Google 액세스 구성"](#).
- 서비스 계정은 Cloud Volumes ONTAP 에 연결되어야 합니다.

["이 서비스 계정을 설정하는 방법을 알아보세요"](#).

Cloud Volumes ONTAP 시스템을 생성할 때 이 서비스 계정을 선택하라는 메시지가 표시됩니다.

배포 중에 서비스 계정을 선택하지 않으면 Cloud Volumes ONTAP 종료하고 Google Cloud 콘솔로 이동한 다음 서비스 계정을 Cloud Volumes ONTAP 인스턴스에 연결해야 합니다. 그런 다음 다음 섹션에 설명된 대로 데이터 계층화를 활성화할 수 있습니다.

- 고객 관리 암호화 키로 버킷을 암호화하려면 Google Cloud Storage 버킷에서 해당 키를 사용하도록 설정합니다.

["Cloud Volumes ONTAP에서 고객 관리 암호화 키를 사용하는 방법을 알아보세요."](#) .

요구 사항 구현 후 데이터 계층화 활성화

콘솔은 연결이나 권한 문제가 없는 한 시스템이 생성될 때 콜드 데이터에 대한 개체 저장소를 생성합니다. 시스템을 생성한 후에 위에 나열된 요구 사항을 구현하지 않은 경우, 객체 저장소를 생성하는 API나 ONTAP 시스템 관리자를 통해 수동으로 계층화를 활성화해야 합니다.



콘솔을 통해 계층화를 활성화하는 기능은 향후 Cloud Volumes ONTAP 릴리스에서 제공될 예정입니다.

집계에서 계층화가 활성화되었는지 확인하세요.

볼륨에서 데이터 계층화를 활성화하려면 집계에서 데이터 계층화를 활성화해야 합니다. 새로운 볼륨과 기존 볼륨에 대한 요구 사항을 알고 있어야 합니다.

- 새로운 권

새 볼륨에서 데이터 계층화를 활성화하는 경우 집계에서 데이터 계층화를 활성화하는 것에 대해 걱정할 필요가 없습니다. 콘솔은 계층화가 활성화된 기존 집계에 볼륨을 생성하거나, 데이터 계층화가 활성화된 집계가 아직 없는 경우 볼륨에 대한 새 집계를 생성합니다.

- 기존 볼륨

기존 볼륨에서 데이터 계층화를 활성화하려면 기본 집계에서도 활성화되어 있는지 확인하세요. 기존 집계에서 데이터 계층화가 활성화되어 있지 않으면 ONTAP System Manager를 사용하여 기존 집계를 개체 저장소에 연결해야 합니다.

집계에서 계층화가 활성화되었는지 확인하는 단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. Cloud Volumes ONTAP 시스템을 엽니다.
3. 집계 탭을 선택하고 집계에서 계층화가 활성화되어 있는지 비활성화되어 있는지 확인합니다.

	aggr1	ONLINE	...
INFO		CAPACITY	
Disk Type GP3 3000 IOPS		Provisioned size 907.12 GiB	
Disks 4		EBS Used 1.13 GiB	
Volumes 2		S3 Used 0 GiB	
Elastic Volumes Enabled			
S3 Tiering Enabled			

집계에서 계층화를 활성화하는 단계

1. ONTAP 시스템 관리자에서 *스토리지 > 계층*을 클릭합니다.
2. 집계에 대한 작업 메뉴를 클릭하고 *클라우드 계층 연결*을 선택합니다.
3. 연결할 클라우드 계층을 선택하고 *저장*을 클릭합니다.

다음은 무엇인가요?

다음 섹션에서 설명하는 대로 이제 새 볼륨과 기존 볼륨에서 데이터 계층화를 활성화할 수 있습니다.

읽기-쓰기 볼륨의 계층 데이터

Cloud Volumes ONTAP 읽기-쓰기 볼륨의 비활성 데이터를 비용 효율적인 개체 스토리지로 계층화하여 성능 계층을 핫 데이터에 사용할 수 있도록 확보합니다.

단계

1. 시스템 아래의 볼륨 탭에서 새 볼륨을 생성하거나 기존 볼륨의 계층을 변경합니다.

일	행동
새 볼륨을 만듭니다	*새 볼륨 추가*를 클릭합니다.
기존 볼륨 수정	원하는 볼륨 타일을 선택하고 *볼륨 관리*를 클릭하여 오른쪽 패널의 볼륨 관리에 액세스한 다음 오른쪽 패널 아래에서 *고급 작업*과 *계층화 정책 변경*을 클릭합니다.

2. 계층화 정책을 선택하세요.

이러한 정책에 대한 설명은 다음을 참조하세요. ["데이터 계층화 개요"](#).

예

Change Tiering Policy
Volume_1

Tiering Policy

Auto - Tiers cold Snapshot copies and cold user data from the active file system to object storage.
Minimum cooling days: 31 (2-183)

All - Immediately tiers all data (not including metadata) to object storage.

Snapshot Only - Tiers cold Snapshot copies to object storage.

None - Data tiering is disabled.

S3 Storage classes Standard-Infrequent Access

S3 Storage Encryption Key aws/s3

데이터 계층화가 가능한 집계가 아직 없는 경우 콘솔은 볼륨에 대한 새로운 집계를 생성합니다.

데이터 보호 볼륨의 계층 데이터

Cloud Volumes ONTAP 데이터 보호 볼륨에서 용량 계층으로 데이터를 계층화할 수 있습니다. 대상 볼륨을 활성화하면 데이터는 읽혀지면서 점차 성능 계층으로 이동합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 소스 볼륨이 포함된 Cloud Volumes ONTAP 시스템을 선택한 다음 볼륨을 복제하려는 시스템으로 끌어다 놓습니다.
3. 계층화 페이지에 도달할 때까지 안내를 따르고 개체 스토리지에 대한 데이터 계층화를 활성화합니다.

예

 **S3 Tiering** [What are storage tiers?](#)

Enabled **Disabled**

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

데이터 복제에 대한 도움말은 다음을 참조하세요. ["클라우드에서 데이터 복제 및 클라우드로 데이터 복제"](#).

계층화된 데이터의 스토리지 클래스 변경

Cloud Volumes ONTAP 배포한 후 30일 동안 액세스되지 않은 비활성 데이터의 스토리지 클래스를 변경하여 스토리지 비용을 줄일 수 있습니다. 데이터에 액세스하는 경우 액세스 비용이 더 높아지므로 스토리지 클래스를 변경하기 전에 이 점을 고려해야 합니다.

계층형 데이터의 저장 클래스는 볼륨별이 아닌 시스템 전체에 적용됩니다.

지원되는 스토리지 클래스에 대한 정보는 다음을 참조하세요. ["데이터 계층화 개요"](#).

단계

1. Cloud Volumes ONTAP 시스템에서 메뉴 아이콘을 클릭한 다음 스토리지 클래스 또는 *Blob 스토리지 계층화*를 클릭합니다.
2. 저장 클래스를 선택한 다음 *저장*을 클릭합니다.

데이터 계층화를 위한 여유 공간 비율 변경

데이터 계층화를 위한 여유 공간 비율은 데이터를 개체 스토리지에 계층화할 때 Cloud Volumes ONTAP SSD/HDD에 필요한 여유 공간의 양을 정의합니다. 기본 설정은 10%의 여유 공간이지만, 요구 사항에 맞게 설정을 조정할 수 있습니다.

예를 들어, 구매한 용량을 충분히 활용하려면 10% 미만의 여유 공간을 선택하는 것이 좋습니다. 콘솔은 추가 용량이 필요할 때(전체 디스크 한도에 도달할 때까지) 추가 디스크를 구매할 수 있습니다.

 충분한 공간이 없으면 Cloud Volumes ONTAP 이 데이터를 이동할 수 없으며 성능 저하가 발생할 수 있습니다. 모든 변경은 신중하게 이루어져야 합니다. 확실하지 않은 경우 NetApp 지원팀에 문의하여 안내를 받으세요.

재해 복구 시나리오에서는 이 비율이 중요합니다. 왜냐하면 개체 저장소에서 데이터를 읽을 때 Cloud Volumes ONTAP 해당 데이터를 SSD/HDD로 옮겨 더 나은 성능을 제공하기 때문입니다. 충분한 공간이 없으면 Cloud Volumes ONTAP 이 데이터를 이동할 수 없습니다. 비즈니스 요구 사항을 충족할 수 있도록 비율을 변경할 때 이 점을 고려하세요.

단계

1. 왼쪽 탐색 창에서 *관리 > 에이전트*로 이동합니다.
2. 클릭  Cloud Volumes ONTAP 시스템을 관리하는 콘솔 에이전트의 아이콘입니다.
3. * Cloud Volumes ONTAP 설정*을 선택합니다.

4. *용량*에서 *데이터 계층화를 위한 집계 용량 임계값 - 여유 공간 비율*을 클릭합니다.

5. 요구 사항에 맞게 여유 공간 비율을 변경하고 *저장*을 클릭하세요.

자동 티어링 정책의 냉각 기간 변경

자동 계층화 정책을 사용하여 Cloud Volumes ONTAP 볼륨에서 데이터 계층화를 활성화한 경우 비즈니스 요구 사항에 따라 기본 냉각 기간을 조정할 수 있습니다. 이 작업은 ONTAP CLI 및 API를 사용해서만 지원됩니다.

쿨링 기간이란 볼륨의 사용자 데이터가 "콜드" 상태로 간주되어 개체 스토리지로 이동되기 전에 비활성 상태를 유지해야 하는 일 수입니다.

자동 티어링 정책의 기본 냉각 기간은 31일입니다. 냉각 기간은 다음과 같이 변경할 수 있습니다.

- 9.8 이상: 2일 ~ 183일
- 9.7 이하: 2일 ~ 63일

단계

1. 볼륨을 생성하거나 기존 볼륨을 수정할 때 API 요청과 함께 *minimumCoolingDays* 매개변수를 사용하세요.

시스템 해체 시 S3 버킷 제거

환경을 해제할 때 Cloud Volumes ONTAP 시스템에서 계층화된 데이터가 있는 S3 버킷을 삭제할 수 있습니다.

다음과 같은 경우에만 S3 버킷을 삭제할 수 있습니다.

- Cloud Volume ONTAP 시스템이 콘솔에서 삭제됩니다.
- 버킷에서 모든 객체가 삭제되고 S3 버킷이 비어 있습니다.

Cloud Volumes ONTAP 시스템을 해제해도 해당 환경을 위해 생성된 S3 버킷은 자동으로 삭제되지 않습니다. 대신 실수로 데이터가 손실되는 것을 방지하기 위해 고아 상태로 유지됩니다. 버킷에 있는 객체를 삭제한 다음 S3 버킷 자체를 제거하거나 나중에 사용하기 위해 보관할 수 있습니다. 참조하다 "[ONTAP CLI: vserver 객체-저장소-서버 버킷 삭제](#)".

호스트 시스템에서 Cloud Volumes ONTAP 의 LUN에 연결합니다.

iSCSI 볼륨을 생성하면 NetApp Console 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후 IQN을 사용하여 호스트에서 LUN에 연결합니다.

다음 사항에 유의하세요.

- 콘솔의 자동 용량 관리 기능은 LUN에 적용되지 않습니다. LUN을 생성하면 자동 증가 기능이 비활성화됩니다.
- ONTAP 시스템 관리자나 ONTAP CLI에서 추가 LUN을 생성할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 볼륨을 관리할 Cloud Volumes ONTAP 시스템을 두 번 클릭합니다.
3. 시스템에서 볼륨 탭을 선택합니다.
4. 필요한 볼륨 타일로 이동한 다음 *볼륨 관리*를 선택하여 오른쪽의 볼륨 관리 패널에 액세스합니다.
5. *대상 IQN*을 클릭합니다.

6. *복사*를 클릭하여 iQN 이름을 복사합니다.
7. 호스트에서 LUN으로 iSCSI 연결을 설정합니다.
 - "Red Hat Enterprise Linux를 위한 ONTAP 9 iSCSI express 구성: 대상에서 iSCSI 세션 시작"
 - "Windows용 ONTAP 9 iSCSI express 구성: 대상과 iSCSI 세션 시작"
 - "ONTAP SAN 호스트 구성"

Cloud Volumes ONTAP 시스템에서 **FlexCache** 볼륨을 사용하여 데이터 액세스 가속화

FlexCache 볼륨은 원본(또는 소스) 볼륨에서 SMB 및 NFS 읽기 데이터를 캐시하는 스토리지 볼륨입니다. 캐시된 데이터를 이어서 읽으면 해당 데이터에 더 빨리 액세스할 수 있습니다.

FlexCache 볼륨을 사용하면 데이터 액세스 속도를 높이거나 액세스 빈도가 높은 볼륨의 트래픽을 오프로드할 수 있습니다. FlexCache 볼륨은 특히 클라이언트가 동일한 데이터에 반복적으로 액세스해야 할 때 성능을 개선하는데 도움이 됩니다. 원본 볼륨에 액세스하지 않고도 데이터를 직접 제공할 수 있기 때문입니다. FlexCache 볼륨은 읽기 작업이 많은 시스템 작업 부하에 적합합니다.

NetApp Console FlexCache 볼륨 관리를 제공합니다. ["NetApp Volume Caching"](#) .

ONTAP CLI 또는 ONTAP 시스템 관리자를 사용하여 FlexCache 볼륨을 생성하고 관리할 수도 있습니다.

- "더 빠른 데이터 액세스를 위한 FlexCache 볼륨 전원 가이드"
- "System Manager에서 FlexCache 볼륨 생성"



원본이 암호화된 경우 **FlexCache** 와 함께 작업합니다.

원본 볼륨이 암호화된 Cloud Volumes ONTAP 시스템에서 FlexCache 구성하는 경우 FlexCache 볼륨이 암호화된

데이터에 적절하게 액세스하고 캐싱할 수 있도록 추가 단계가 필요합니다.

시작하기 전에

- 암호화 설정: 소스 볼륨이 완전히 암호화되어 작동 가능한지 확인합니다. Cloud Volumes ONTAP 시스템의 경우 클라우드별 키 관리 서비스와의 통합이 필요합니다.

AWS의 경우 일반적으로 AWS Key Management Service(KMS)를 사용하는 것을 의미합니다. 자세한 내용은 다음을 참조하세요.["AWS Key Management Service로 키 관리"](#).

Azure의 경우 NetApp 볼륨 암호화(NVE)를 위해 Azure Key Vault를 설정해야 합니다. 자세한 내용은 다음을 참조하세요.["Azure Key Vault를 사용하여 키 관리"](#).

Google Cloud의 경우 Google Cloud Key Management Service입니다. 자세한 내용은 다음을 참조하세요.["Google의 Cloud Key Management Service로 키 관리"](#).

- 키 관리 서비스: FlexCache 볼륨을 생성하기 전에 Cloud Volumes ONTAP 시스템에서 키 관리 서비스가 올바르게 구성되었는지 확인하세요. 이 구성은 FlexCache 볼륨이 원본 볼륨의 데이터를 암호 해독하는 데 필수적입니다.
- 라이선스: 유효한 FlexCache 라이선스가 Cloud Volumes ONTAP 시스템에서 사용 가능하고 활성화되었는지 확인합니다.
- * ONTAP 버전*: Cloud Volumes ONTAP 시스템의 ONTAP 버전이 암호화된 볼륨이 있는 FlexCache 지원하는지 확인하세요. 최신 내용을 참조하세요 ["ONTAP 릴리스 노트"](#) 자세한 내용은 호환성 매트릭스를 참조하세요.
- 네트워크 구성: 네트워크 구성이 원본 볼륨과 FlexCache 볼륨 간의 원활한 통신을 허용하는지 확인하세요. 여기에는 클라우드 환경에서의 적절한 라우팅과 DNS 확인이 포함됩니다.

단계

암호화된 소스 볼륨을 사용하여 Cloud Volumes ONTAP 시스템에 FlexCache 볼륨을 만듭니다. 자세한 단계와 추가 고려 사항은 다음 섹션을 참조하세요.

- ["더 빠른 데이터 액세스를 위한 FlexCache 볼륨 전원 가이드"](#)
- ["System Manager에서 FlexCache 볼륨 생성"](#)

집계 관리

Cloud Volumes ONTAP 시스템에 대한 집계를 만듭니다.

직접 집계를 만들 수도 있고 NetApp Console 볼륨을 생성할 때 집계를 대신 만들어 줄 수도 있습니다. 집계를 직접 만드는 이점은 기본 디스크 크기를 선택할 수 있다는 점입니다. 즉, 필요한 용량이나 성능에 맞게 집계 크기를 조정할 수 있습니다.



모든 디스크와 집계는 콘솔에서 직접 만들고 삭제해야 합니다. 다른 관리 도구에서는 이러한 작업을 수행해서는 안 됩니다. 그렇게 하면 시스템 안정성에 영향을 미치고, 나중에 디스크를 추가하는 기능을 방해할 수 있으며, 잠재적으로 중복된 클라우드 공급자 수수료가 발생할 수 있습니다.

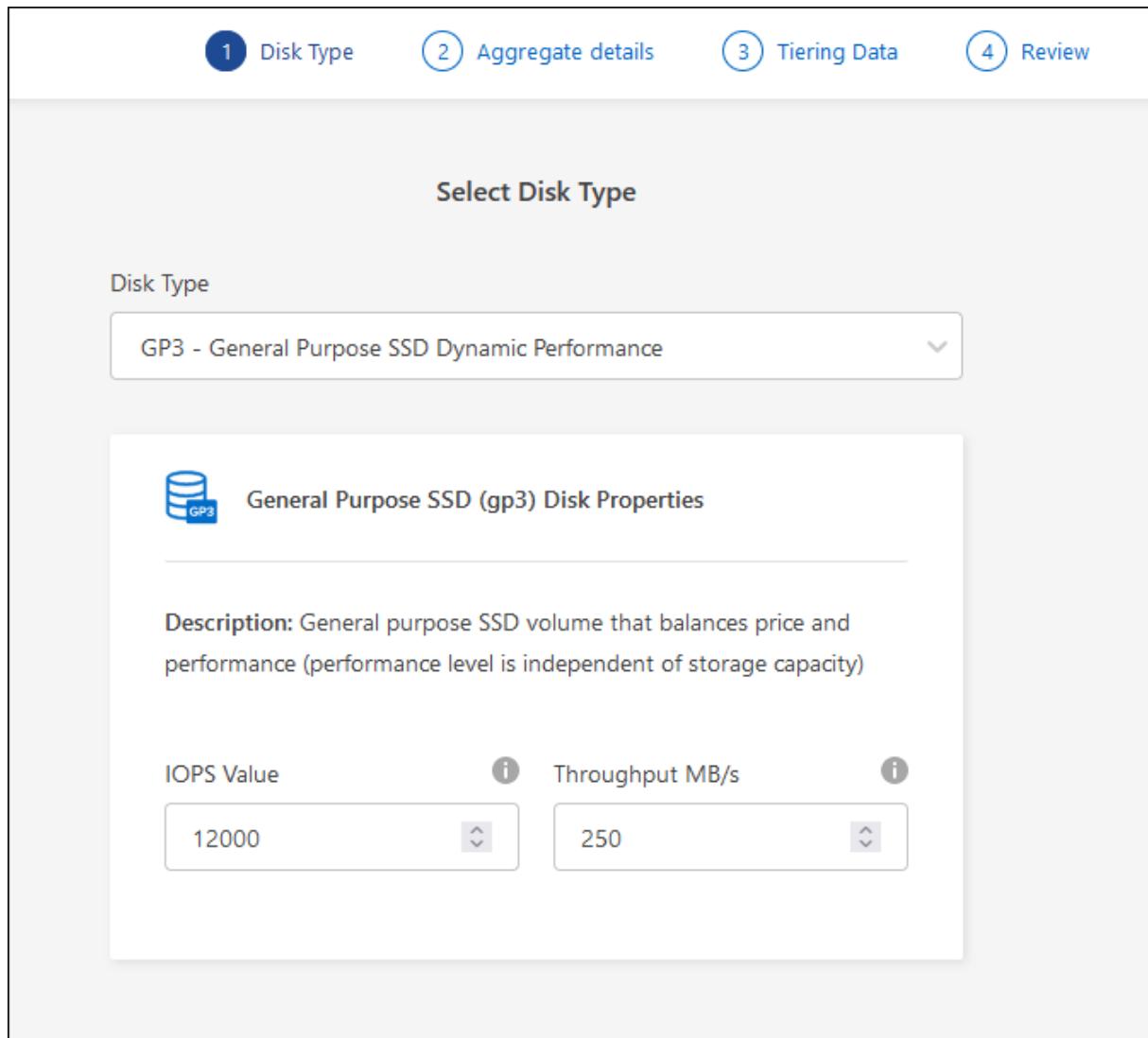
단계

- 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
- 시스템 페이지에서 집계를 관리하려는 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.

3. 집계 탭에서 *집계 추가*를 클릭한 다음 집계에 대한 세부 정보를 지정합니다.

AWS

- 디스크 유형 및 디스크 크기를 선택하라는 메시지가 표시되면 다음을 참조하세요. "[AWS에서 Cloud Volumes ONTAP 구성을 계획하세요](#)".
- 집계의 용량 크기를 입력하라는 메시지가 표시되면 Amazon EBS Elastic Volumes 기능을 지원하는 구성에서 집계를 생성하고 있는 것입니다. 다음 스크린샷은 gp3 디스크로 구성된 새로운 집계의 예를 보여줍니다.



"[Elastic Volumes 지원에 대해 자세히 알아보세요](#)".

하늘빛

디스크 유형 및 디스크 크기에 대한 도움말은 다음을 참조하세요. "[Azure에서 Cloud Volumes ONTAP 구성 계획](#)".

구글 클라우드

디스크 유형 및 디스크 크기에 대한 도움말은 다음을 참조하세요. "[Google Cloud에서 Cloud Volumes ONTAP 구성 계획하세요](#)".

- *추가*를 클릭한 다음 *승인 및 구매*를 클릭합니다.

Cloud Volumes ONTAP 클러스터에 대한 집계 관리

디스크를 추가하고, 집계에 대한 정보를 보고, 삭제하여 집계를 직접 관리합니다.



모든 디스크와 집계는 NetApp Console에서 직접 만들고 삭제해야 합니다. 다른 관리 도구에서는 이러한 작업을 수행해서는 안 됩니다. 그렇게 하면 시스템 안정성에 영향을 미치고, 나중에 디스크를 추가하는 기능을 방해할 수 있으며, 잠재적으로 중복된 클라우드 공급자 수수료가 발생할 수 있습니다.

시작하기 전에

집계를 삭제하려면 먼저 집계에서 볼륨을 삭제해야 합니다.

이 작업에 관하여

집계된 공간이 부족한 경우 ONTAP System Manager를 사용하여 볼륨을 다른 집계로 이동할 수 있습니다.

단계

- 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
- 시스템 페이지에서 집계를 관리할 Cloud Volumes ONTAP 시스템을 두 번 클릭합니다.
- 시스템 세부 정보에서 집계 탭을 클릭합니다.
- 필요한 집계를 위해 다음을 클릭하세요. **...** 관리 작업에 대한 아이콘입니다.

- 사용 가능한 옵션에서 집계를 관리하세요. **...** 메뉴.



집계에 디스크를 추가하려면 집계에 있는 모든 디스크의 크기가 동일해야 합니다.

AWS의 경우 Amazon EBS Elastic Volumes를 지원하는 집계의 용량을 늘릴 수 있습니다.

1. 아래에 **...** 메뉴에서 *용량 늘리기*를 클릭하세요.
2. 추가하려는 용량을 입력한 다음 *증가*를 클릭하세요.

집계 용량을 최소 256GiB 또는 집계 크기의 10%만큼 늘려야 합니다. 예를 들어, 1.77TiB 집계가 있는 경우 10%는 181GiB입니다. 이는 256GiB보다 작으므로 집계 크기도 최소 256GiB만큼 늘어나야 합니다.

콘솔 에이전트에서 Cloud Volumes ONTAP 집계 용량 관리

각 콘솔 에이전트에는 Cloud Volumes ONTAP 의 집계 용량을 관리하는 방법을 결정하는 설정이 있습니다.

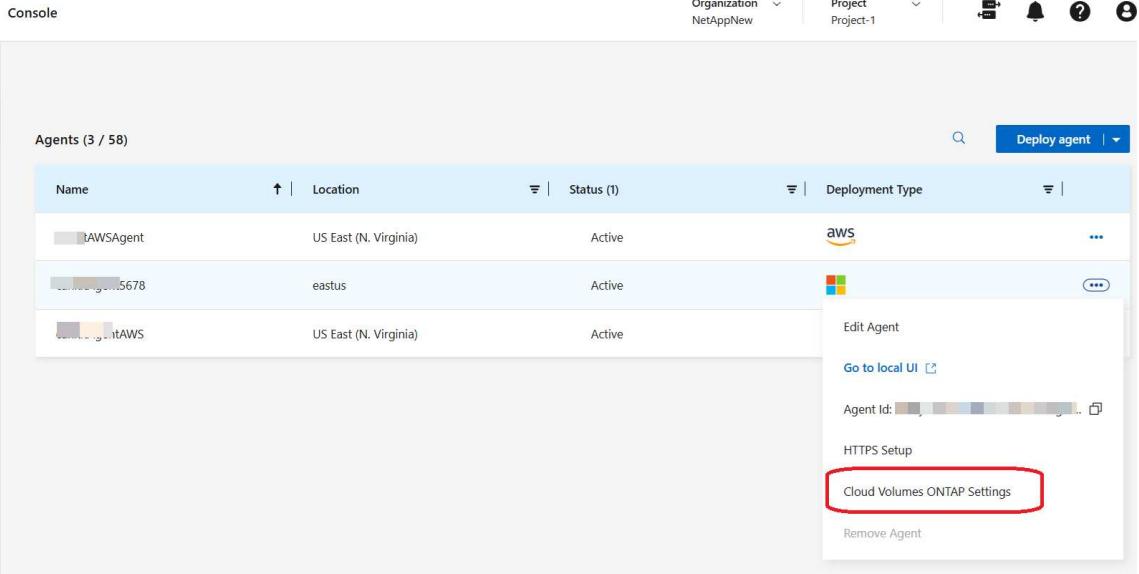
이러한 설정은 콘솔 에이전트에서 관리하는 모든 Cloud Volumes ONTAP 시스템에 영향을 미칩니다. 다른 콘솔 에이전트가 있는 경우 다르게 구성할 수 있습니다.

필요한 권한

Cloud Volumes ONTAP 설정을 수정하려면 NetApp Console 의 조직 또는 계정 관리자 권한이 필요합니다.

단계

1. 왼쪽 탐색 창에서 *관리 > 에이전트*로 이동합니다.
2. 클릭 **...** Cloud Volumes ONTAP 시스템을 관리하는 콘솔 에이전트의 아이콘입니다.
3. * Cloud Volumes ONTAP 설정*을 선택합니다.



The screenshot shows the NetApp Console interface. The top navigation bar includes 'NetApp Console', 'Organization: NetAppNew', 'Project: Project-1', and various icons for search, refresh, and help. The left sidebar has 'Agents' and 'Overview' tabs, with 'Overview' selected. The main content area is titled 'Agents (3 / 58)' and displays a table with columns: Name, Location, Status, Deployment Type, and Actions. Three agents are listed: 'AWSAgent' (AWS icon, Active, US East (N. Virginia)), '5678' (Azure icon, Active, eastus), and 'itAWS' (AWS icon, Active, US East (N. Virginia)). A context menu is open for the 'itAWS' agent, showing options: 'Edit Agent', 'Go to local UI', 'Agent Id: [redacted]', 'HTTPS Setup', and 'Cloud Volumes ONTAP Settings'. The 'Cloud Volumes ONTAP Settings' option is highlighted with a red box.

4. *용량*에서 다음 설정을 수정하세요.

Edit Cloud Volumes ONTAP settings

Capacity

① Capacity Management Mode	Automatic Mode	▼
① Aggregate Capacity Thresholds - Free Space Ratio	10%	▼
① Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering	10%	▼
① Volume Autosize - Additional Size in Percentage to Which Volumes Can Grow	1000%	▼

General

① Automatic Cloud Volumes ONTAP update during deployment	On	▼
--	----	---

Azure

① Azure CIFS locks for Azure HA systems	Off	▼
① Use Azure Private Link	On	▼

용량 관리 모드

콘솔에서 저장 용량 결정 사항을 알려야 하는지, 아니면 자동으로 용량 요구 사항을 관리해야 하는지 선택하세요.

["용량 관리 모드의 작동 방식 알아보기".](#)

총 용량 임계값 - 여유 공간 비율

이 비율은 용량 관리 결정에 있어 핵심 매개변수이며, 용량 관리 모드가 자동이든 수동이든 관계없이 이 비율의 영향을 이해하는 것이 필수적입니다. 리소스 활용도와 비용 간의 균형을 유지하려면 특정 저장 요구 사항과 예상되는 성장 상황을 고려하여 이 임계값을 설정하는 것이 좋습니다.

수동 모드에서 집계의 여유 공간 비율이 지정된 임계값 아래로 떨어지면 알림이 트리거되어 여유 공간 비율이 낮은 문제를 해결하기 위한 조치를 취해야 함을 알려줍니다. 서비스 중단을 방지하고 최적의 성능을 보장하려면 이러한 알림을 모니터링하고 집계 용량을 수동으로 관리하는 것이 중요합니다.

여유 공간 비율은 다음과 같이 계산됩니다. (집계 용량 - 집계에서 사용된 총 용량) / 집계 용량

참조하다 ["자동 용량 관리"](#) 이제 Cloud Volumes ONTAP에서 용량이 자동으로 관리됩니다.

집계 용량 임계값 - 데이터 계층화를 위한 여유 공간 비율

데이터를 용량 계층(개체 스토리지)으로 계층화할 때 성능 계층(디스크)에 얼마나 많은 여유 공간이 필요한지 정의합니다.

이 비율은 재해 복구 시나리오에서 중요합니다. 데이터가 용량 계층에서 읽히면 Cloud Volumes ONTAP 더 나은 성능을 제공하기 위해 데이터를 성능 계층으로 이동합니다. 충분한 공간이 없으면 Cloud Volumes ONTAP

이 데이터를 이동할 수 없습니다.

5. *저장*을 클릭하세요.

Azure에서 디스크 성능 관리

Azure Cloud Volumes ONTAP에서 Premium SSD v2 디스크 성능을 관리하세요.

Azure에서 Cloud Volumes ONTAP 성능을 최적화하려면 Premium SSD v2 디스크의 IOPS 및 처리량 매개변수를 구성하면 됩니다. 이 기능은 Cloud Volumes ONTAP Azure Premium SSD v2 디스크 유형으로 이미 배포된 경우에만 사용할 수 있으며, 초기 배포 시에는 사용할 수 없습니다. 성능을 향상시키면 Azure Premium SSD v2 디스크의 모든 유연성과 고성능 기능을 활용할 수 있습니다.

프리미엄 SSD v2 디스크는 낮은 지연 시간, 높은 IOPS 및 높은 처리량을 통해 빠르고 안정적인 성능이 필요한 워크로드를 지원합니다. IOPS 및 처리량 설정을 조정하여 배포 환경에서 집계 도구의 성능을 맞춤 설정할 수 있습니다. Premium SSD v2 디스크에 대한 자세한 내용은 다음을 참조하십시오. ["Premium SSD v2 디스크를 배포하세요"](#).

API를 사용하여 Premium SSD v2 디스크 설정 수정 프로세스를 자동화하세요. Cloud Volumes ONTAP API 호출 실행에 대한 자세한 내용은 다음을 참조하십시오. ["첫 번째 API 호출"](#).

이 작업에 관하여

- 이 기능은 Azure 단일 가용성 영역의 Cloud Volumes ONTAP 배포에 적용됩니다.
- 디스크 설정을 변경하면 RAID 그룹 또는 집합체의 성능이 일괄적으로 변경됩니다. 집합체 내 모든 디스크의 성능은 집합체 전체에서 일관된 성능을 보장하기 위해 동일한 수준으로 조정됩니다.
- 이러한 변화는 단일 집합체에만 영향을 미치며 그룹 내의 다른 집합체에는 영향을 미치지 않습니다.
- NetApp Console에서 Cloud Volumes ONTAP 배포 또는 용량 최적화 중에 자동으로 프로비저닝되거나 API를 통해 추가된 Premium SSD v2 디스크는 모두 수정 가능합니다.
- 디스크 크기 조정(디스크 용량 변경)은 지원되지 않습니다.

시작하기 전에

Premium SSD v2 디스크의 IOPS 및 처리량 매개변수를 구성하기 전에 다음 사항에 유의하십시오.

- 프리미엄 SSD v2 데이터 디스크만 선택했는지 확인하십시오. 프리미엄 SSD v1 디스크 또는 루트 및 부팅 디스크는 이 변경 사항의 적용 대상이 아닙니다.
- 배포 중에 Cloud Volumes ONTAP에서 설정한 사전 구성된 기준 설정을 해당 디스크 크기에 대한 최소 IOPS 및 처리량 값으로 사용하십시오. 이러한 기본 설정은 Premium SSD v1의 성능 특성과 일치합니다.
- 디스크 크기에 맞는 최소 기준선 이상으로 IOPS 및 처리량 값을 설정하십시오. 예를 들어, 1TB 디스크 크기의 경우 최소 IOPS 값을 5,000으로, 최소 처리량 값을 200MBps로 설정하십시오. 이 최소값보다 높은 값은 설정할 수 있지만 낮은 값은 설정할 수 없습니다.
- 지원되는 Premium SSD v2 범위 내에서 값을 구성하십시오. IOPS는 3000~80000, 처리량은 125~1200MBps입니다.
- Azure의 Cloud Volumes ONTAP에서 지원되는 범위인 500GB~32TB 내에 Premium SSD v2 디스크 크기가 있는지 확인하십시오. 참고로 이러한 크기 제한은 Azure에서 Premium SSD v2 디스크에 대해 제공하는 최소 및 최대 값과 다릅니다.

단계

- 다음 API 호출을 사용하여 IOPS 및 처리량 속성 값을 변경하십시오.



이 API는 24시간 내에 최대 4회까지 호출할 수 있습니다.

```
PUT /azure/vsa/aggregates/{workingEnvironmentId}/{aggregateName}
```

요청 본문에 다음 매개변수를 포함합니다.

```
{
  "aggregateName": "aggr_name",
  "iops": "modified_iops_value",
  "throughput": "modified_throughput_value",
  "workingEnvironmentId": "we_id"
}
```

당신이 완료한 후

API에서 작업이 성공했다는 응답이 반환되면 Azure 포털에서 Cloud Volumes ONTAP 시스템의 디스크 세부 정보를 확인하여 수정된 매개변수를 검증하십시오.

관련 정보

- ["API 사용을 준비하세요"](#)
- ["Cloud Volumes ONTAP 워크플로"](#)
- ["필수 식별자 가져오기"](#)
- ["Cloud Volumes ONTAP 용 REST API 사용"](#)
- ["가용성 세트의 VM에서 Premium SSD v2를 사용하세요."](#)

Azure Cloud Volumes ONTAP에서 프리미엄 SSD 디스크의 성능 계층을 변경합니다.

Azure 포털을 사용하여 Azure의 Cloud Volumes ONTAP에서 프리미엄 SSD 관리 디스크의 성능 등급을 업그레이드할 수 있습니다. 이는 각 프리미엄 SSD 디스크의 디스크 티어를 더 높은 성능 티어로 변경하는 수동 프로세스입니다. NVRAM 디스크의 성능 등급을 변경하면 더 높은 IOPS 및 처리량 기능을 제공하여 성능 병목 현상을 완화하고 Cloud Volumes ONTAP 시스템의 효율성을 향상시킬 수 있습니다.



NetApp 지원팀과 협력하여 환경에서 발생하는 병목 현상이 NVRAM 디스크 때문인지 확인하고, 티어 업그레이드를 통해 문제가 해결되는지 확인하십시오.

이 작업에 관하여

- Azure의 Cloud Volumes ONTAP 기본적으로 P20 계층에 NVRAM 용으로 프리미엄 SSD 디스크를 배포합니다. P20 등급은 대부분의 작업 부하에 적합한 균형 잡힌 성능을 제공합니다. 하지만 작업 부하에 더 높은 성능이 요구되는 경우 NVRAM 디스크를 P30과 같은 상위 등급으로 업그레이드할 수 있습니다.



현재로서는 Azure 포털을 통해서만 NVRAM 디스크를 P20 티어에서 P30 티어로 업그레이드할 수 있습니다.

- 디스크 크기는 변경하지 않습니다. 용량은 여전히 512GB입니다. 이 절차는 디스크의 성능 등급만 변경합니다.

시작하기 전에

- NVRAM 디스크를 더 높은 성능 등급으로 업그레이드하면 추가 비용이 발생하므로 이러한 변경의 필요성을 신중하게 평가하십시오.
- Cloud Volumes ONTAP 버전은 9.11.1 이상이어야 합니다. 하위 버전의 경우 9.11.1 이상 버전으로 업그레이드하거나 NetApp 지원팀에 기능 정책 변경 요청(FPVR)을 제출할 수 있습니다.

단계

이 시나리오는 노드가 두 개 있다고 가정합니다. node01 그리고 node02 Cloud Volumes ONTAP 고가용성(HA) 배포에서. Azure 포털을 사용하여 티어를 업그레이드하세요.

1. 만들기 위해 이 명령어를 실행하세요 node01 활성 노드. 수동 페일오버 node02.

```
storage failover takeover -ofnode <Node02>
```

2. Azure Portal에 Sign in .
3. 인수 작업이 완료되면 VM 인스턴스로 이동하세요. 'node02' 그리고 정지 버튼을 클릭하여 전원을 끄세요.
4. 해당 리소스 그룹으로 이동하세요. node02 디스크 목록에서 티어를 변경할 NVRAM 디스크를 선택합니다.
5. 크기와 성능을 모두 고려하여 선택하세요.
6. 성능 등급 드롭다운 메뉴에서 선택하세요. P30 - 5000 IOPS, 200MB/s.
7. *크기 조정*을 선택하세요.
8. 스위치를 켜세요 node02 사례.
9. Azure 시리얼 콘솔에서 메시지가 표시될 때까지 확인하세요. waiting for giveback.
10. 이 명령어를 실행하여 돌려주세요 node02:

```
storage failover giveback -ofnode <Node02>
```

11. 다음 단계를 반복하세요. node01 만들다 node02 인수하다 node01 이를 통해 NVRAM 디스크 계층을 업그레이드할 수 있습니다. `node01.

당신이 완료한 후

두 노드를 모두 켜 후에는 Azure 포털에서 Cloud Volumes ONTAP 시스템의 디스크 세부 정보를 확인하여 수정된 매개변수를 검증하십시오.

관련 정보

- Azure 설명서: "[다운타임 없이 성능 등급을 변경하세요](#)"
- 지원팀을 위한 지식 기반: "[Azure CVO에서 NVRAM 디스크의 성능 계층을 업그레이드하는 방법](#)"
- "[Cloud Volumes ONTAP 소프트웨어 버전 업그레이드](#)"

스토리지 VM 관리

Cloud Volumes ONTAP 의 스토리지 VM 관리

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에게 스토리지 및 데이터 서비스를 제공합니다. 이것을 SVM 또는 `_vserver_` 라고 알고 있을 수도 있습니다. Cloud Volumes ONTAP은 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다.

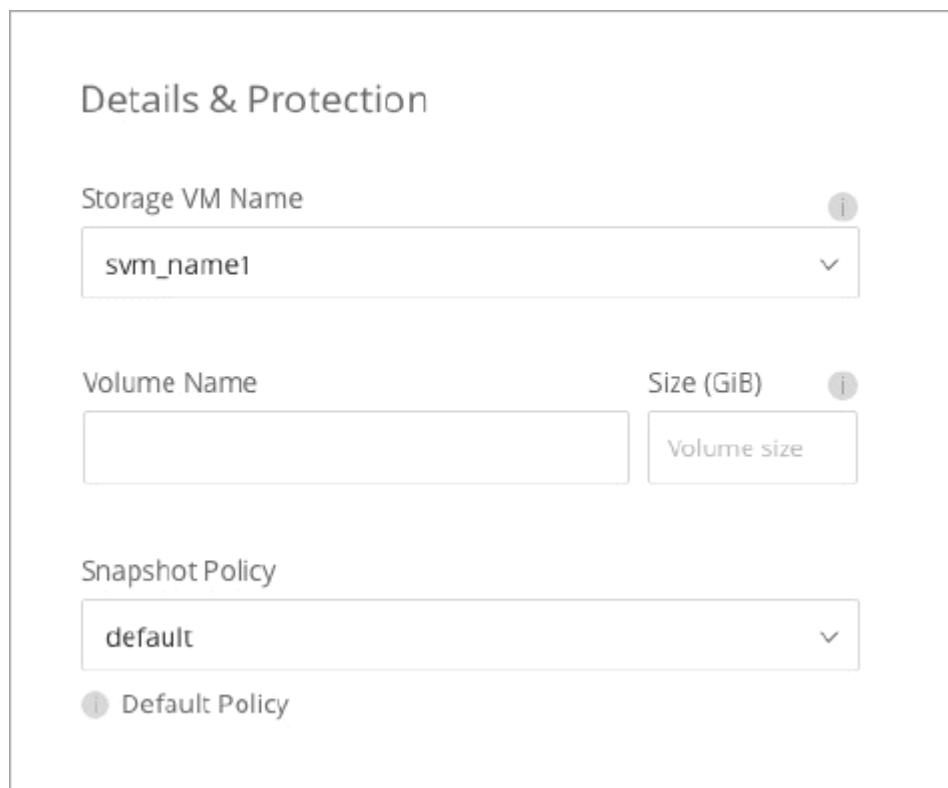
지원되는 스토리지 VM 수

특정 구성에서는 여러 개의 스토리지 VM이 지원됩니다. 로 가다 ["Cloud Volumes ONTAP 릴리스 노트"](#) Cloud Volumes ONTAP 버전에 지원되는 스토리지 VM 수를 확인하세요.

여러 스토리지 VM으로 작업

NetApp Console ONTAP System Manager나 ONTAP CLI에서 생성하는 모든 추가 스토리지 VM을 지원합니다.

예를 들어, 다음 이미지는 볼륨을 생성할 때 스토리지 VM을 선택하는 방법을 보여줍니다.



다음 이미지는 볼륨을 다른 시스템에 복제할 때 스토리지 VM을 선택하는 방법을 보여줍니다.

The screenshot shows the 'Destination Volume Name' field containing 'volume_copy', the 'Destination Storage VM Name' dropdown set to 'svm_name1', and the 'Destination Aggregate' dropdown set to 'Automatically select the best aggregate'.

기본 스토리지 **VM**의 이름을 수정합니다.

콘솔은 Cloud Volumes ONTAP에 대해 생성하는 단일 스토리지 VM의 이름을 자동으로 지정합니다. 엄격한 명명 기준이 있는 경우 ONTAP 시스템 관리자, ONTAP CLI 또는 API를 사용하여 스토리지 VM의 이름을 수정할 수 있습니다. 예를 들어, ONTAP 클러스터의 스토리지 VM에 지정한 이름과 일치하도록 이름을 지정할 수 있습니다.

AWS에서 Cloud Volumes ONTAP 위한 데이터 제공 스토리지 **VM** 관리

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에게 스토리지 및 데이터 서비스를 제공합니다. 이것을 SVM 또는 `_vserver_`라고 알고 있을 수도 있습니다. Cloud Volumes ONTAP은 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다.

추가 데이터 제공 스토리지 VM을 생성하려면 AWS에서 IP 주소를 할당한 다음 Cloud Volumes ONTAP 구성에 따라 ONTAP 명령을 실행해야 합니다.

지원되는 스토리지 **VM** 수

9.7 릴리스부터 특정 Cloud Volumes ONTAP 구성에서 여러 스토리지 VM이 지원됩니다. 로 가다 ["Cloud Volumes ONTAP 릴리스 노트"](#) Cloud Volumes ONTAP 버전에 지원되는 스토리지 VM 수를 확인하세요.

다른 모든 Cloud Volumes ONTAP 구성은 재해 복구에 사용되는 하나의 데이터 제공 스토리지 VM과 하나의 대상 스토리지 VM을 지원합니다. 소스 스토리지 VM에 장애가 발생하는 경우 데이터 액세스를 위해 대상 스토리지 VM을 활성화할 수 있습니다.

구성에 대한 제한 사항을 확인하세요

각 EC2 인스턴스는 네트워크 인터페이스당 최대 개수의 개인 IPv4 주소를 지원합니다. AWS에서 새로운 스토리지 VM에 IP 주소를 할당하기 전에 제한을 확인해야 합니다.

단계

1. 가다 ["Cloud Volumes ONTAP 릴리스 노트의 스토리지 한도 섹션"](#).

2. 인스턴스 유형에 대한 인터페이스당 최대 IP 주소 수를 식별합니다.
3. 다음 섹션에서 AWS에서 IP 주소를 할당할 때 필요하므로 이 번호를 기록해 두세요.

AWS에서 IP 주소 할당

새 스토리지 VM에 대한 LIF를 생성하기 전에 AWS의 포트 e0a에 개인 IPv4 주소를 할당해야 합니다.

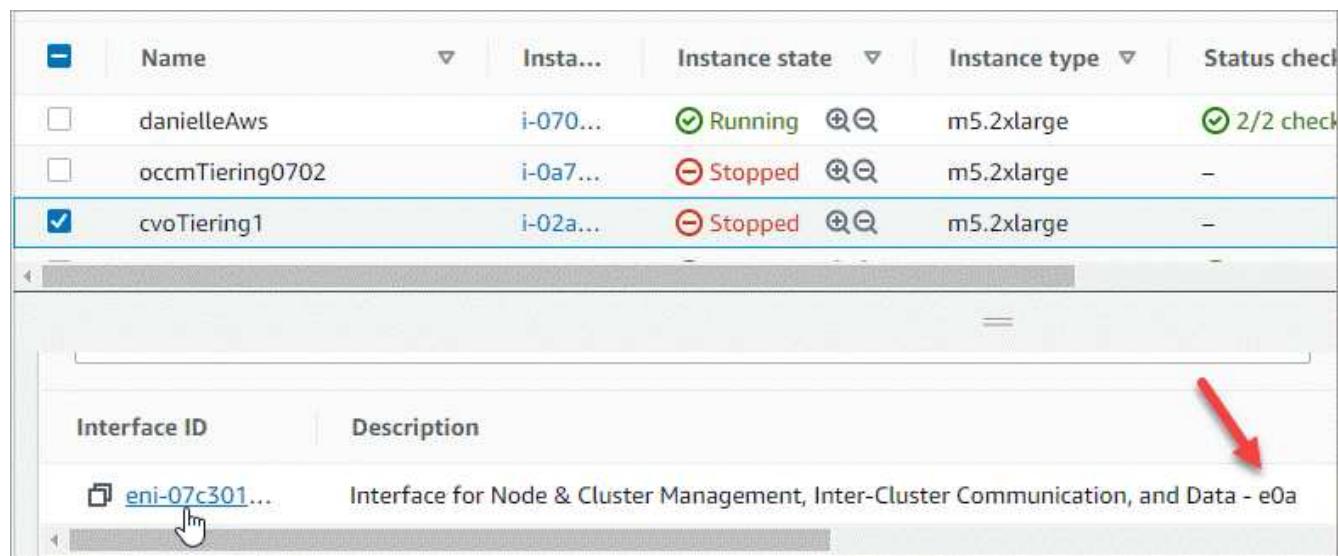
스토리지 VM에 대한 선택적 관리 LIF에는 단일 노드 시스템과 단일 AZ의 HA 쌍에 개인 IP 주소가 필요합니다. 이 관리 LIF는 SnapCenter 와 같은 관리 도구에 대한 연결을 제공합니다.

단계

1. AWS에 로그인하고 EC2 서비스를 엽니다.
2. Cloud Volumes ONTAP 인스턴스를 선택하고 *네트워킹*을 클릭합니다.

HA 쌍에 스토리지 VM을 생성하는 경우 노드 1을 선택합니다.

3. *네트워크 인터페이스*로 스크롤하여 포트 e0a의 *인터페이스 ID*를 클릭합니다.



Name	Insta...	Instance state	Instance type	Status check
danielleAws	i-070...	Running	m5.2xlarge	2/2 check
occmTiering0702	i-0a7...	Stopped	m5.2xlarge	-
cvoTiering1	i-02a...	Stopped	m5.2xlarge	-

Interface ID	Description
eni-07c301...	Interface for Node & Cluster Management, Inter-Cluster Communication, and Data - e0a

4. 네트워크 인터페이스를 선택하고 *작업 > IP 주소 관리*를 클릭합니다.
5. e0a의 IP 주소 목록을 확장합니다.
6. IP 주소를 확인하세요:
 - a. 할당된 IP 주소의 수를 세어 포트에 추가 IP를 위한 공간이 있는지 확인하세요.
이 페이지의 이전 섹션에서 인터페이스당 지원되는 IP 주소의 최대 개수를 확인했어야 합니다.
 - b. 선택 사항: Cloud Volumes ONTAP 의 ONTAP CLI로 이동하여 *network interface show*를 실행하여 각 IP 주소가 사용 중인지 확인합니다.
- IP 주소가 사용되지 않으면 새 스토리지 VM에서 해당 IP 주소를 사용할 수 있습니다.
7. AWS 콘솔로 돌아와서 *새 IP 주소 할당*을 클릭하여 새 스토리지 VM에 필요한 양에 따라 추가 IP 주소를 할당합니다.

◦ 단일 노드 시스템: 사용되지 않는 보조 개인 IP가 하나 필요합니다.

스토리지 VM에 관리 LIF를 생성하려면 선택적 보조 개인 IP가 필요합니다.

◦ 단일 AZ의 HA 쌍: 노드 1에 사용되지 않는 보조 개인 IP가 하나 필요합니다.

스토리지 VM에 관리 LIF를 생성하려면 선택적 보조 개인 IP가 필요합니다.

◦ 여러 AZ의 HA 쌍: 각 노드에 사용되지 않는 보조 개인 IP가 하나씩 필요합니다.

8. 단일 AZ의 HA 쌍에 IP 주소를 할당하는 경우 *보조 개인 IPv4 주소 재할당 허용*을 활성화합니다.

9. *저장*을 클릭하세요.

10. 여러 AZ에 HA 쌍이 있는 경우 노드 2에 대해 이 단계를 반복해야 합니다.

단일 노드 시스템에 스토리지 VM 생성

이 단계에서는 단일 노드 시스템에 새로운 스토리지 VM을 만듭니다. NAS LIF를 생성하려면 개인 IP 주소 하나가 필요하고, 관리 LIF를 생성하려면 선택적으로 개인 IP 주소가 하나 더 필요합니다.

단계

1. 스토리지 VM과 스토리지 VM으로의 경로를 만듭니다.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. NAS LIF를 생성합니다.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node
```

여기서 `_private_ip_x`는 e0a의 사용되지 않는 보조 개인 IP입니다.

3. 선택 사항: 스토리지 VM 관리 LIF를 만듭니다.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

여기서 `_private_ip_y`는 e0a의 사용되지 않는 또 다른 보조 개인 IP입니다.

4. 스토리지 VM에 하나 이상의 집계를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

이 단계는 새 스토리지 VM이 볼륨을 생성하기 전에 최소한 하나의 집계에 액세스해야 하기 때문에 필요합니다.

단일 AZ의 HA 쌍에 스토리지 VM 생성

이 단계에서는 단일 AZ의 HA 쌍에 새로운 스토리지 VM을 만듭니다. NAS LIF를 생성하려면 개인 IP 주소 하나가 필요하고, 관리 LIF를 생성하려면 선택적으로 개인 IP 주소가 하나 더 필요합니다.

두 LIF는 모두 노드 1에 할당됩니다. 장애가 발생하면 개인 IP 주소가 노드 간에 이동할 수 있습니다.

단계

1. 스토리지 VM과 스토리지 VM으로의 경로를 만듭니다.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. 노드 1에 NAS LIF를 생성합니다.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

여기서 `_private_ip_x`는 cvo-node1의 e0a에 있는 사용되지 않는 보조 개인 IP입니다. 서비스 정책 `default-data-files`은 IP가 파트너 노드로 마이그레이션될 수 있음을 나타내므로 인수 시 이 IP 주소는 cvo-node2의 e0a로 이전될 수 있습니다.

3. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 만듭니다.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

여기서 `_private_ip_y`는 e0a의 사용되지 않는 또 다른 보조 개인 IP입니다.

4. 스토리지 VM에 하나 이상의 집계를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

이 단계는 새 스토리지 VM이 볼륨을 생성하기 전에 최소한 하나의 집계에 액세스해야 하기 때문에 필요합니다.

5. Cloud Volumes ONTAP 9.11.1 이상을 실행하는 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정하세요.

Cloud Volumes ONTAP 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하려면 서비스를 수정해야 합니다.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

여러 AZ의 HA 쌍에 스토리지 VM 생성

이 단계에서는 여러 AZ의 HA 쌍에 새로운 스토리지 VM을 만듭니다.

NAS LIF에는 유동 IP 주소가 필요하지만 관리 LIF에는 선택 사항입니다. 이러한 유동 IP 주소를 사용하면 AWS에서

개인 IP를 할당할 필요가 없습니다. 대신, AWS 라우팅 테이블에서 플로팅 IP가 자동으로 구성되어 동일한 VPC에 있는 특정 노드의 ENI를 가리킵니다.

ONTAP에서 플로팅 IP를 사용하려면 각 노드의 모든 스토리지 VM에 개인 IP 주소를 구성해야 합니다. 이는 노드 1과 노드 2에서 iSCSI LIF가 생성되는 아래 단계에 반영됩니다.

단계

1. 스토리지 VM과 스토리지 VM으로의 경로를 만듭니다.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. 노드 1에 NAS LIF를 생성합니다.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

- HA 구성을 배포하는 AWS 지역의 모든 VPC에 대한 CIDR 블록 외부에 부동 IP 주소가 있어야 합니다. 192.168.209.27은 유동 IP 주소의 예입니다. ["플로팅 IP 주소 선택에 대해 자세히 알아보세요"](#).
- `-service-policy default-data-files` IP가 파트너 노드로 마이그레이션될 수 있음을 나타냅니다.

3. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 만듭니다.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. 노드 1에 iSCSI LIF를 생성합니다.

```
network interface create -vserver svm_2 -service-policy default-data-  
blocks -home-port e0a -address private_ip -netmask node1Mask -lif  
ip_node1_iscsi_2 -home-node cvo-node1
```

- 이 iSCSI LIF는 스토리지 VM의 플로팅 IP의 LIF 마이그레이션을 지원하는 데 필요합니다. iSCSI LIF일 필요는 없지만 노드 간 마이그레이션을 위해 구성할 수는 없습니다.
- `-service-policy default-data-block` IP 주소가 노드 간에 마이그레이션되지 않음을 나타냅니다.
- `_private_ip_`는 cvo_node1의 eth0(e0a)에 있는 사용되지 않는 보조 개인 IP 주소입니다.

5. 노드 2에 iSCSI LIF를 생성합니다.

```
network interface create -vserver svm_2 -service-policy default-data-blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif ip_node2_iscsi_2 -home-node cvo-node2
```

- 이 iSCSI LIF는 스토리지 VM의 플로팅 IP의 LIF 마이그레이션을 지원하는 데 필요합니다. iSCSI LIF일 필요는 없지만 노드 간 마이그레이션을 위해 구성할 수는 없습니다.
- `-service-policy default-data-block` IP 주소가 노드 간에 마이그레이션되지 않음을 나타냅니다.
- `_private_ip_`는 cvo_node2의 eth0(e0a)에 있는 사용되지 않는 보조 개인 IP 주소입니다.

6. 스토리지 VM에 하나 이상의 집계를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

이 단계는 새 스토리지 VM이 볼륨을 생성하기 전에 최소한 하나의 집계에 액세스해야 하기 때문에 필요합니다.

7. Cloud Volumes ONTAP 9.11.1 이상을 실행하는 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정하세요.

Cloud Volumes ONTAP 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하려면 서비스를 수정해야 합니다.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Azure에서 Cloud Volumes ONTAP 대한 데이터 제공 스토리지 VM 관리

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에게 스토리지 및 데이터 서비스를 제공합니다. 이것을 SVM 또는 _vserver_라고 알고 있을 수도 있습니다. Cloud Volumes ONTAP 기본적으로 하나의 스토리지 VM으로 구성되지만 Azure에서 Cloud Volumes ONTAP 실행할 때 추가 스토리지 VM을 만들 수 있습니다.

Azure에서 추가 데이터 제공 스토리지 VM을 만들고 관리하려면 API를 사용해야 합니다. API는 스토리지 VM을 생성하고 필요한 네트워크 인터페이스를 구성하는 프로세스를 자동화하기 때문입니다. 스토리지 VM을 생성할 때 NetApp Console 필수 LIF 서비스와 스토리지 VM에서 아웃바운드 SMB/CIFS 통신에 필요한 iSCSI LIF를 구성합니다.

Cloud Volumes ONTAP API 호출 실행에 대한 정보는 다음을 참조하세요. ["첫 번째 API 호출"](#).

지원되는 스토리지 VM 수

Cloud Volumes ONTAP 9.9.0부터 라이선스에 따라 특정 구성으로 여러 스토리지 VM이 지원됩니다. 를 참조하세요 ["Cloud Volumes ONTAP 릴리스 노트"](#) Cloud Volumes ONTAP 버전에 지원되는 스토리지 VM 수를 확인하세요.

9.9.0 이전의 모든 Cloud Volumes ONTAP 버전은 재해 복구에 사용되는 하나의 데이터 제공 스토리지 VM과 하나의 대상 스토리지 VM을 지원합니다. 소스 스토리지 VM에 장애가 발생하는 경우 데이터 액세스를 위해 대상 스토리지 VM을 활성화할 수 있습니다.

스토리지 VM 생성

구성 및 라이선스 유형에 따라 NetApp Console 용 API를 사용하여 단일 노드 시스템이나 고가용성(HA) 구성에서 여러 스토리지 VM을 만들 수 있습니다.

이 작업에 관하여

API를 사용하여 스토리지 VM을 생성하고 필요한 네트워크 인터페이스를 구성하는 경우 콘솔도 다음을 수정합니다. default-data-files 다음 서비스를 NAS 데이터 LIF에서 제거하고 아웃바운드 관리 연결에 사용되는 iSCSI 데이터 LIF에 추가하여 데이터 스토리지 VM에 대한 정책을 적용합니다.

- data-fpolicy-client
- management-ad-client
- management-dns-client
- management-ldap-client
- management-nis-client

시작하기 전에

콘솔 에이전트에는 Cloud Volumes ONTAP 에 대한 스토리지 VM을 생성하기 위한 특정 권한이 필요합니다. 필요한 권한이 포함되어 있습니다. ["NetApp 에서 제공하는 정책"](#).

단일 노드 시스템

다음 API 호출을 사용하여 단일 노드 시스템에 스토리지 VM을 생성합니다.

```
POST /azure/vsa/working-environments/{workingEnvironmentId}/svm
```

요청 본문에 다음 매개변수를 포함합니다.

```
{ "svmName": "myNewSvm1",  
  "svmPassword": "optional, the API takes the cluster password if not  
  provided",  
  "mgmtLif": "optional, to create an additional management LIF, if you  
  want to use the storage VM for management purposes"}
```

HA 쌍

다음 API 호출을 사용하여 HA 쌍에 스토리지 VM을 만듭니다.

```
POST /azure/ha/working-environments/{workingEnvironmentId}/svm
```

요청 본문에 다음 매개변수를 포함합니다.

```
{ "svmName": "NewSvmName"  
  "svmPassword": "optional value, the API takes the cluster password if  
  not provided"  
  "mgmtLif": "optional value, to create an additional management LIF, if  
  you want to use the storage VM for management purposes"}
```

단일 노드 시스템 및 **HA** 쌍에서 스토리지 **VM** 관리

API를 사용하면 단일 노드와 HA 구성 모두에서 스토리지 VM의 이름을 바꾸고 삭제할 수 있습니다.

시작하기 전에

콘솔 에이전트에는 Cloud Volumes ONTAP 의 스토리지 VM을 관리하기 위한 특정 권한이 필요합니다. 필요한 권한이 포함되어 있습니다. ["NetApp에서 제공하는 정책"](#).

스토리지 **VM** 이름 바꾸기

스토리지 VM의 이름을 바꾸려면 기존 스토리지 VM과 새 스토리지 VM의 이름을 매개변수로 제공해야 합니다.

단계

- 다음 API 호출을 사용하여 단일 노드 시스템에서 스토리지 VM의 이름을 바꾸세요.

```
PUT /azure/vsa/working-environments/{workingEnvironmentId}/svm
```

요청 본문에 다음 매개변수를 포함합니다.

```
{  
  "svmNewName": "NewSvmName",  
  "svmName": "OldSvmName"  
}
```

- 다음 API 호출을 사용하여 HA 쌍의 스토리지 VM 이름을 바꾸세요.

```
PUT /azure/ha/working-environments/{workingEnvironmentId}/svm
```

요청 본문에 다음 매개변수를 포함합니다.

```
{  
  "svmNewName": "NewSvmName",  
  "svmName": "OldSvmName"  
}
```

스토리지 VM 삭제

단일 노드 또는 HA 구성에서는 활성 볼륨이 없는 스토리지 VM을 제거할 수 있습니다.

단계

- 다음 API 호출을 사용하여 단일 노드 시스템에서 스토리지 VM을 삭제합니다.

```
DELETE /azure/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- HA 쌍에서 스토리지 VM을 삭제하려면 다음 API 호출을 사용하세요.

```
DELETE /azure/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

관련 정보

- ["API 사용을 준비하세요"](#)
- ["Cloud Volumes ONTAP 워크플로"](#)
- ["필수 식별자 가져오기"](#)
- ["NetApp Console에 REST API 사용"](#)

Google Cloud에서 Cloud Volumes ONTAP 위한 데이터 제공 스토리지 VM 관리

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에게 스토리지 및 데이터 서비스를 제공합니다. 이것을 SVM 또는 `_vserver_`라고 알고 있을 수도 있습니다. Cloud Volumes ONTAP은 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다.

Google Cloud에서 추가 데이터 제공 스토리지 VM을 만들고 관리하려면 API를 사용해야 합니다. API는 스토리지 VM을 생성하고 필요한 네트워크 인터페이스를 구성하는 프로세스를 자동화하기 때문입니다. 스토리지 VM을 생성할 때 NetApp Console 필수 LIF 서비스와 스토리지 VM에서 아웃바운드 SMB/CIFS 통신에 필요한 iSCSI LIF를 구성합니다.

Cloud Volumes ONTAP API 호출 실행에 대한 정보는 다음을 참조하세요. ["첫 번째 API 호출"](#).

지원되는 스토리지 VM 수

Cloud Volumes ONTAP 9.11.1부터 라이선스에 따라 특정 구성으로 여러 스토리지 VM이 지원됩니다. 를 참조하세요. ["Cloud Volumes ONTAP 릴리스 노트"](#) Cloud Volumes ONTAP 버전에 지원되는 스토리지 VM 수를 확인하세요.

9.11.1 이전의 모든 Cloud Volumes ONTAP 버전은 재해 복구에 사용되는 하나의 데이터 제공 스토리지 VM과 하나의 대상 스토리지 VM을 지원합니다. 소스 스토리지 VM에 장애가 발생하는 경우 데이터 액세스를 위해 대상 스토리지 VM을 활성화할 수 있습니다.

스토리지 VM 생성

구성 및 라이선스 유형에 따라 API를 사용하여 단일 노드 시스템이나 고가용성(HA) 구성에서 여러 스토리지 VM을 만들 수 있습니다.

이 작업에 관하여

API를 사용하여 스토리지 VM을 생성하고 필요한 네트워크 인터페이스를 구성하는 경우 콘솔도 다음을 수정합니다.

default-data-files 다음 서비스를 NAS 데이터 LIF에서 제거하고 아웃바운드 관리 연결에 사용되는 iSCSI 데이터 LIF에 추가하여 데이터 스토리지 VM에 대한 정책을 적용합니다.

- data-fpolicy-client
- management-ad-client
- management-dns-client
- management-ldap-client
- management-nis-client

시작하기 전에

콘솔 에이전트에는 Cloud Volumes ONTAP HA 쌍에 대한 스토리지 VM을 생성하기 위한 특정 권한이 필요합니다. 필요한 권한이 포함되어 있습니다. ["NetApp에서 제공하는 정책"](#).

단일 노드 시스템

다음 API 호출을 사용하여 단일 노드 시스템에 스토리지 VM을 생성합니다.

POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm

요청 본문에 다음 매개변수를 포함합니다.

```
{ "svmName": "NewSvmName"  
  "svmPassword": "optional value, the API takes the cluster password if  
  not provided"  
  "mgmtLif": "optional value, to create an additional management LIF, if  
  you want to use the storage VM for management purposes"}
```

HA 쌍

다음 API 호출을 사용하여 HA 쌍에 스토리지 VM을 만듭니다.

POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/

요청 본문에 다음 매개변수를 포함합니다.

```
{ "svmName": "NewSvmName"  
  "svmPassword": "optional value, the API takes the cluster password if  
  not provided"  
 }
```

스토리지 **VM** 관리

API를 사용하면 단일 노드와 HA 구성 모두에서 스토리지 VM의 이름을 바꾸고 삭제할 수 있습니다.

시작하기 전에

콘솔 에이전트에는 Cloud Volumes ONTAP HA 쌍의 스토리지 VM을 관리하기 위한 특정 권한이 필요합니다. 필요한 권한이 포함되어 있습니다. ["NetApp에서 제공하는 정책"](#).

스토리지 VM 이름 바꾸기

스토리지 VM의 이름을 바꾸려면 기존 스토리지 VM과 새 스토리지 VM의 이름을 매개변수로 제공해야 합니다.

단계

- 다음 API 호출을 사용하여 단일 노드 시스템에서 스토리지 VM의 이름을 바꾸세요.

```
PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

요청 본문에 다음 매개변수를 포함합니다.

```
{  
  "svmNewName": "NewSvmName",  
  "svmName": "OldSvmName"  
}
```

- 다음 API 호출을 사용하여 HA 쌍의 스토리지 VM 이름을 바꾸세요.

```
PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm
```

요청 본문에 다음 매개변수를 포함합니다.

```
{  
  "svmNewName": "NewSvmName",  
  "svmName": "OldSvmName"  
}
```

스토리지 VM 삭제

단일 노드 또는 HA 구성에서는 활성 볼륨이 없는 스토리지 VM을 제거할 수 있습니다.

단계

- 다음 API 호출을 사용하여 단일 노드 시스템에서 스토리지 VM을 삭제합니다.

```
DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- HA 쌍에서 스토리지 VM을 삭제하려면 다음 API 호출을 사용하세요.

```
DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

관련 정보

- ["API 사용을 준비하세요"](#)
- ["Cloud Volumes ONTAP 워크플로"](#)

- "필수 식별자 가져오기"
- "NetApp Console에 REST API 사용"

Cloud Volumes ONTAP에 대한 스토리지 VM 재해 복구 설정

NetApp Console 스토리지 VM(SVM) 재해 복구에 대한 설정이나 오케스트레이션 지원을 제공하지 않습니다. 이러한 작업을 수행하려면 ONTAP 시스템 관리자나 ONTAP CLI를 사용하세요.

두 개의 Cloud Volumes ONTAP 시스템 간에 SnapMirror SVM 복제를 설정하는 경우 복제는 두 개의 HA 쌍 시스템 또는 두 개의 단일 노드 시스템 간에 이루어져야 합니다. HA 쌍과 단일 노드 시스템 간에는 SnapMirror SVM 복제를 설정할 수 없습니다.

ONTAP CLI 지침은 다음 문서를 참조하세요.

- "SVM 재해 복구 준비 익스프레스 가이드"
- "SVM 재해 복구 익스프레스 가이드"

보안 및 데이터 암호화

NetApp 암호화 솔루션을 사용하여 Cloud Volumes ONTAP에서 볼륨 암호화

Cloud Volumes ONTAP NetApp Volume Encryption(NVE)과 NetApp Aggregate Encryption(NAE)을 지원합니다. NVE와 NAE는 볼륨의 FIPS 140-2 호환 저장 데이터 암호화를 지원하는 소프트웨어 기반 솔루션입니다. ["이러한 암호화 솔루션에 대해 자세히 알아보세요"](#).

NVE와 NAE는 모두 외부 키 관리자를 통해 지원됩니다.

```
] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[] ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[
```

AWS Key Management Service를 사용하여 Cloud Volumes ONTAP 암호화 키 관리

사용할 수 있습니다 ["AWS의 키 관리 서비스\(KMS\)"](#) AWS에 배포된 애플리케이션에서 ONTAP 암호화 키를 보호합니다.

AWS KMS를 통한 키 관리 기능은 CLI 또는 ONTAP REST API를 통해 활성화할 수 있습니다.

KMS를 사용할 때 기본적으로 데이터 SVM의 LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용된다는 점에 유의하세요. 노드 관리 네트워크는 AWS 인증 서비스와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않으면 클러스터가 키 관리 서비스를 제대로 활용하지 못합니다.

시작하기 전에

- Cloud Volumes ONTAP 버전 9.12.0 이상을 실행해야 합니다.
- 볼륨 암호화(VE) 라이선스를 설치해야 합니다.
- MTEKM(Multi-tenant Encryption Key Management) 라이선스가 설치되어 있어야 합니다.

- 클러스터 또는 SVM 관리자여야 합니다.

- 활성 AWS 구독이 있어야 합니다.



데이터 SVM에 대해서만 키를 구성할 수 있습니다.

구성

AWS

- 당신은 만들어야합니다 "승인하다" 암호화를 관리하는 IAM 역할에서 사용될 AWS KMS 키에 대한 것입니다. IAM 역할에는 다음 작업을 허용하는 정책이 포함되어야 합니다.
 - DescribeKey
 - Encrypt
 - Decrypt' 보조금을 생성하려면 다음을 참조하세요. ["AWS 문서"](#).
- "적절한 IAM 역할에 정책을 추가합니다." 정책은 다음을 지원해야 합니다. DescribeKey, Encrypt, 그리고 Decrypt 운영.

Cloud Volumes ONTAP

- Cloud Volumes ONTAP 환경으로 전환하세요.

- 고급 권한 수준으로 전환:

```
set -privilege advanced
```

- AWS 키 관리자를 활성화합니다.

```
security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context
```

- 메시지가 표시되면 비밀 키를 입력하세요.

- AWS KMS가 올바르게 구성되었는지 확인하세요.

```
security key-manager external aws show -vserver svm_name
```

Azure Key Vault를 사용하여 Cloud Volumes ONTAP 암호화 키 관리

Azure Key Vault(AKV)를 사용하면 Azure에 배포된 애플리케이션에서 ONTAP 암호화 키를 보호할 수 있습니다. 를 참조하세요 ["Microsoft 설명서"](#).

AKV는 데이터 SVM에 대해서만 NetApp 볼륨 암호화(NVE) 키를 보호하는 데 사용할 수 있습니다. 자세한 내용은 다음을 참조하세요. ["ONTAP 문서"](#).

AKV를 사용한 키 관리 기능은 CLI 또는 ONTAP REST API를 통해 활성화할 수 있습니다.

AKV를 사용할 때 기본적으로 데이터 SVM LIF를 사용하여 클라우드 키 관리 엔드포인트와 통신한다는 점에 유의하세요. 노드 관리 네트워크는 클라우드 공급자의 인증 서비스(login.microsoftonline.com)와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않으면 클러스터가 키 관리 서비스를 제대로 활용하지 못합니다.

시작하기 전에

- Cloud Volumes ONTAP 버전 9.10.1 이상을 실행해야 합니다.
- 볼륨 암호화(VE) 라이선스가 설치됨(NetApp 볼륨 암호화 라이선스는 NetApp 지원에 등록된 각 Cloud Volumes ONTAP 시스템에 자동으로 설치됨)

- 다중 테넌트 암호화 키 관리(MT_EK_MGMT) 라이선스가 있어야 합니다.
- 클러스터 또는 SVM 관리자여야 합니다.
- 활성 Azure 구독

제한 사항

- AKV는 데이터 SVM에서만 구성될 수 있습니다.
- NAE는 AKV와 함께 사용할 수 없습니다. NAE에는 외부 지원 KMIP 서버가 필요합니다.
- Cloud Volumes ONTAP 노드는 15분마다 AKV를 폴링하여 접근성과 키 가용성을 확인합니다. 이 폴링 기간은 구성할 수 없으며, 폴링 시도에서 4번 연속 실패하면(총 1시간) 볼륨이 오프라인으로 전환됩니다.

구성 프로세스

설명된 단계에서는 Cloud Volumes ONTAP 구성 Azure에 등록하는 방법과 Azure Key Vault 및 키를 만드는 방법을 설명합니다. 이미 이러한 단계를 완료한 경우 특히 올바른 구성 설정이 있는지 확인하십시오. [Azure Key Vault 만들기](#), 그리고 다음으로 진행합니다 [Cloud Volumes ONTAP 구성](#).

- [Azure 애플리케이션 등록](#)
- [Azure 클라이언트 비밀 만들기](#)
- [Azure Key Vault 만들기](#)
- [암호화 키 생성](#)
- [Azure Active Directory 엔드포인트 만들기\(HA 전용\)](#)
- [Cloud Volumes ONTAP 구성](#)

Azure 애플리케이션 등록

1. 먼저 Cloud Volumes ONTAP Azure Key Vault에 액세스하는 데 사용할 Azure 구독에 애플리케이션을 등록해야 합니다. Azure Portal에서 앱 등록을 선택합니다.
2. 신규 등록을 선택하세요.
3. 애플리케이션 이름을 입력하고 지원되는 애플리케이션 유형을 선택하세요. Azure Key Vault를 사용하려면 기본 단일 테넌트로 충분합니다. 등록을 선택하세요.
4. Azure 개요 창에서 등록한 애플리케이션을 선택합니다. 애플리케이션(클라이언트) ID와 디렉토리(테넌트) ID를 안전한 위치에 복사합니다. 이는 나중에 등록 과정에서 필요합니다.

Azure 클라이언트 비밀 만들기

1. Azure Key Vault 앱 등록을 위한 Azure Portal에서 인증서 및 비밀 창을 선택합니다.
2. 새로운 클라이언트 비밀번호를 선택하세요. 클라이언트 비밀번호에 의미 있는 이름을 입력하세요. NetApp 24개월 만료 기간을 권장하지만, 특정 클라우드 거버넌스 정책에는 다른 설정이 필요할 수 있습니다.
3. 추가를 클릭하여 클라이언트 비밀번호를 생성합니다. 값 열에 나열된 비밀 문자열을 복사하여 나중에 사용할 수 있도록 안전한 위치에 저장하세요. [Cloud Volumes ONTAP 구성](#). 해당 페이지에서 벗어나면 비밀번호 값은 다시 표시되지 않습니다.

Azure Key Vault 만들기

1. 기존 Azure Key Vault가 있는 경우 Cloud Volumes ONTAP 구성에 연결할 수 있습니다. 하지만 이 프로세스에서는 설정에 맞게 액세스 정책을 조정해야 합니다.

2. Azure Portal에서 키 자격 증명 모음 섹션으로 이동합니다.
3. **+만들기**를 클릭하고 리소스 그룹, 지역, 가격 책정 계층을 포함한 필수 정보를 입력합니다. 또한 삭제된 볼트를 보관할 일수를 입력하고 키 볼트에서 퍼지 보호 사용을 선택합니다.
4. 다음을 선택하여 액세스 정책을 선택하세요.
5. 다음 옵션을 선택하세요:
 - a. 액세스 구성에서 **Vault** 액세스 정책을 선택합니다.
 - b. 리소스 액세스에서 볼륨 암호화를 위해 **Azure Disk Encryption**을 선택합니다.
6. **+만들기**를 선택하여 액세스 정책을 추가합니다.
7. 템플릿에서 구성에서 드롭다운 메뉴를 클릭한 다음 키, 비밀번호 및 인증서 관리 템플릿을 선택합니다.
8. 각 드롭다운 권한 메뉴(키, 비밀, 인증서)를 선택한 다음 메뉴 목록 상단에서 모두 선택을 클릭하여 사용 가능한 모든 권한을 선택합니다. 다음이 있어야 합니다.
 - 주요 권한: 20개 선택됨
 - 비밀 권한: 8개 선택됨
 - 인증서 권한: 16개 선택됨

Create an access policy

X

1 Permissions

2 Principal

3 Application (optional)

4 Review + create

Configure from a template

Key, Secret, & Certificate Management

Key permissions

Key Management Operations

- Select all
- Get
- List
- Update
- Create
- Import
- Delete
- Recover
- Backup
- Restore

Cryptographic Operations

- Select all
- Decrypt
- Encrypt
- Unwrap Key
- Wrap Key
- Verify
- Sign

Privileged Key Operations

- Select all
- Purge
- Release

Rotation Policy Operations

- Select all
- Rotate
- Get Rotation Policy
- Set Rotation Policy

Secret permissions

Secret Management Operations

- Select all
- Get
- List
- Set
- Delete
- Recover
- Backup
- Restore

Privileged Secret Operations

- Select all
- Purge

Certificate permissions

Certificate Management Operations

- Select all
- Get
- List
- Update
- Create
- Import
- Delete
- Recover
- Backup
- Restore
- Manage Contacts
- Manage Certificate Authorities
- Get Certificate Authorities
- List Certificate Authorities
- Set Certificate Authorities
- Delete Certificate Authorities

Privileged Certificate Operations

- Select all
- Purge

Previous

Next

9. 다음을 클릭하여 주 Azure 등록 애플리케이션을 선택하십시오. [Azure 애플리케이션 등록](#). 다음을 선택하세요.



정책당 한 명의 주체만 할당할 수 있습니다.

Create an access policy

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Search by object ID, name, or email address

Selected item
No item selected

Previous Next

10. 다음을 두 번 클릭하여 검토 및 생성에 도달합니다. 그런 다음 만들기를 클릭합니다.
11. 다음을 선택하여 네트워킹 옵션으로 넘어갑니다.
12. 적절한 네트워크 액세스 방법을 선택하거나 모든 네트워크와 검토 + 생성을 선택하여 키 보관소를 만듭니다.
(네트워크 액세스 방법은 거버넌스 정책이나 회사 클라우드 보안 팀에서 규정할 수 있습니다.)
13. 키 보관소 URI를 기록합니다. 생성한 키 보관소에서 개요 메뉴로 이동하여 오른쪽 열에서 보관소 **URI**를 복사합니다. 이것은 나중의 단계에서 필요합니다.

암호화 키 생성

1. Cloud Volumes ONTAP에 대해 생성한 Key Vault 메뉴에서 키 옵션으로 이동합니다.
2. 생성/가져오기를 선택하여 새 키를 만듭니다.
3. 기본 옵션을 생성으로 설정된 상태로 둡니다.
4. 다음 정보를 제공하세요.
 - 암호화 키 이름

- 키 유형: RSA

- RSA 키 크기: 2048

- 활성화됨: 예

5. 암호화 키를 생성하려면 생성을 선택하세요.

6. 키 메뉴로 돌아가서 방금 만든 키를 선택하세요.

7. 현재 버전에서 키 ID를 선택하여 키 속성을 확인하세요.

8. 키 식별자 필드를 찾으세요. 16진수 문자열을 제외하고 URI를 해당 문자열까지 복사합니다.

Azure Active Directory 엔드포인트 만들기(HA 전용)

1. 이 프로세스는 HA Cloud Volumes ONTAP 시스템에 대해 Azure Key Vault를 구성하는 경우에만 필요합니다.

2. Azure Portal에서 가상 네트워크로 이동합니다.

3. Cloud Volumes ONTAP 시스템을 배포한 가상 네트워크를 선택하고 페이지 왼쪽에 있는 서브넷 메뉴를 선택합니다.

4. 목록에서 Cloud Volumes ONTAP 배포에 대한 서브넷 이름을 선택합니다.

5. 서비스 엔드포인트 제목으로 이동합니다. 드롭다운 메뉴에서 다음을 선택하세요.

- **Microsoft.AzureActiveDirectory**

- 마이크로소프트 키볼트

- **Microsoft.Storage** (선택 사항)

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

Save

Cancel

6. 저장을 선택하여 설정을 적용합니다.

Cloud Volumes ONTAP 구성

- 원하는 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.
- ONTAP에서 고급 권한 모드로 들어가세요:

```
set advanced -con off
```

3. 원하는 데이터 SVM을 식별하고 DNS 구성을 확인합니다.

```
vserver services name-service dns show
```

a. 원하는 데이터 SVM에 대한 DNS 항목이 있고 Azure DNS에 대한 항목이 포함되어 있는 경우 아무 작업도 필요하지 않습니다. 그렇지 않은 경우 Azure DNS, 개인 DNS 또는 온-프레미스 서버를 가리키는 데이터 SVM에 대한 DNS 서버 항목을 추가합니다. 이는 클러스터 관리 SVM 항목과 일치해야 합니다.

```
vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address
```

b. 데이터 SVM에 대한 DNS 서비스가 생성되었는지 확인하세요.

```
vserver services name-service dns show
```

4. 애플리케이션 등록 후 저장된 클라이언트 ID와 테넌트 ID를 사용하여 Azure Key Vault를 활성화합니다.

```
security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI
```



그만큼 _full_key_URI 가치는 활용되어야 합니다 <https://<key vault host name>/keys/<key label> 체재.

5. Azure Key Vault를 성공적으로 활성화한 후 다음을 입력하십시오. client secret value 메시지가 표시되면.

6. 키 관리자의 상태를 확인하세요.

```
security key-manager external azure check
```

```
::*: security key-manager external azure check
```

```
Vserver: data_svm_name
```

```
Node: akvlab01-01
```

```
Category: service_reachability
```

```
Status: OK
```

```
Category: ekmip_server
```

```
Status: OK
```

```
Category: kms_wrapped_key_status
```

```
Status: UNKNOWN
```

```
Details: No volumes created yet for the vserver. Wrapped KEK status will be available after creating encrypted volumes.
```

```
3 entries were displayed.
```

만약 service_reachability 상태가 아닙니다 OK SVM은 필요한 모든 연결 및 권한을 통해 Azure Key Vault 서비스에 연결할 수 없습니다. Azure 네트워크 정책과 라우팅이 개인 vNet이 Azure Key Vault 공용 엔드포인트에 도달하는 것을 차단하지 않는지 확인하세요. 그렇다면 vNet 내에서 Key Vault에 액세스하기 위해 Azure Private 엔드포인트를 사용하는 것을 고려하세요. 엔드포인트의 개인 IP 주소를 확인하려면 SVM에 정적 호스트 항목을 추가해야 할 수도 있습니다.

그만큼 `kms_wrapped_key_status` 보고할 것이다 UNKNOWN 초기 구성에서. 상태가 다음으로 변경됩니다. OK 첫 번째 볼륨이 암호화된 후.

7. 선택 사항: NVE의 기능을 확인하기 위해 테스트 볼륨을 만듭니다.

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size  
-state online -policy default
```

올바르게 구성된 경우 Cloud Volumes ONTAP 자동으로 볼륨을 생성하고 볼륨 암호화를 활성화합니다.

8. 볼륨이 올바르게 생성되고 암호화되었는지 확인하세요. 그렇다면, `-is-encrypted` 매개변수는 다음과 같이 표시됩니다. `true`.

```
vol show -vserver SVM_name -fields is-encrypted
```

9. 선택 사항: Azure Key Vault 인증 인증서의 자격 증명을 업데이트하려면 다음 명령을 사용하세요.

```
security key-manager external azure update-credentials -vserver v1  
-authentication-method certificate
```

관련 링크

- ["Azure에서 고객 관리 키를 사용하도록 Cloud Volumes ONTAP 설정"](#)
- ["Microsoft Azure 설명서: Azure Key Vault 정보"](#)
- ["ONTAP 명령 참조 가이드"](#)

Google Cloud KMS를 사용하여 Cloud Volumes ONTAP 암호화 키 관리

사용할 수 있습니다 ["Google Cloud Platform의 키 관리 서비스\(Cloud KMS\)"](#) Google Cloud Platform에 배포된 애플리케이션에서 Cloud Volumes ONTAP 암호화 키를 보호합니다.

Cloud KMS를 사용한 키 관리 기능은 ONTAP CLI 또는 ONTAP REST API를 통해 활성화할 수 있습니다.

Cloud KMS를 사용할 때 기본적으로 데이터 SVM의 LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용된다는 점에 유의하세요. 노드 관리 네트워크는 클라우드 제공자의 인증 서비스(oauth2.googleapis.com)와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않으면 클러스터가 키 관리 서비스를 제대로 활용하지 못합니다.

시작하기 전에

- 시스템에서는 Cloud Volumes ONTAP 9.10.1 이상을 실행해야 합니다.
- 데이터 SVM을 사용해야 합니다. Cloud KMS는 데이터 SVM에서만 구성할 수 있습니다.
- 클러스터 또는 SVM 관리자여야 합니다.
- SVM에 볼륨 암호화(VE) 라이선스를 설치해야 합니다.
- Cloud Volumes ONTAP 9.12.1 GA부터 다중 테넌트 암호화 키 관리(MTEKM) 라이선스도 설치해야 합니다.
- 활성화된 Google Cloud Platform 구독이 필요합니다.

구성

구글 클라우드

1. Google Cloud 환경에서 ["대칭 GCP 키 링과 키를 생성합니다."](#).
2. Cloud KMS 키와 Cloud Volumes ONTAP 서비스 계정에 사용자 지정 역할을 할당합니다.

a. 사용자 정의 역할을 만듭니다.

```
gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

  --permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.locations.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

b. 생성한 사용자 지정 역할을 할당합니다.

```
gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
  --location key_location --member serviceAccount:_service_account_Name_
  --role projects/customer_project_id/roles/kmsCustomRole
```



Cloud Volumes ONTAP 9.13.0 이상을 사용하는 경우 사용자 지정 역할을 만들 필요가 없습니다. 미리 정의된 것을 할당할 수 있습니다
[cloudkms.cryptoKeyEncrypterDecrypter ^] 역할.

3. 서비스 계정 JSON 키 다운로드:

```
gcloud iam service-accounts keys create key-file --iam-account=sa-name
  @project-id.iam.gserviceaccount.com
```

Cloud Volumes ONTAP

1. 원하는 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.

2. 고급 권한 수준으로 전환:

```
set -privilege advanced
```

3. 데이터 SVM에 대한 DNS를 생성합니다.

```
dns create -domains c.<project>.internal -name-servers server_address -vserver
  SVM_name
```

4. CMEK 항목 생성:

```
security key-manager external gcp enable -vserver SVM_name -project-id project
  -key-ring-name key_ring_name -key-ring-location key_ring_location -key-name
  key_name
```

5. 메시지가 표시되면 GCP 계정의 서비스 계정 JSON 키를 입력합니다.

6. 활성화된 프로세스가 성공했는지 확인하세요.

```
security key-manager external gcp check -vserver svm_name
```

7. 선택 사항: 암호화를 테스트하기 위한 볼륨 생성 vol create volume_name -aggregate aggregate
 -vserver vserver_name -size 10G

문제 해결

문제 해결이 필요한 경우 위의 마지막 두 단계에서 원시 REST API 로그를 추적할 수 있습니다.

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Cloud Volumes ONTAP에 NetApp 랜섬웨어 보호 솔루션 활성화

랜섬웨어 공격은 기업의 시간, 자원, 평판을 앗아갈 수 있습니다. NetApp Console 사용하면 랜섬웨어에 대한 두 가지 NetApp 솔루션, 즉 일반적인 랜섬웨어 파일 확장자로부터의 보호 및 자율 랜섬웨어 보호(ARP)를 구현할 수 있습니다. 이러한 솔루션은 가시성, 탐지 및 복구를 위한 효과적인 도구를 제공합니다.

일반적인 랜섬웨어 파일 확장자로부터 보호

콘솔에서 사용할 수 있는 랜섬웨어 보호 설정을 사용하면 ONTAP FPolicy 기능을 활용하여 일반적인 랜섬웨어 파일 확장자 유형으로부터 보호할 수 있습니다.

단계

1. 시스템 페이지에서 랜섬웨어 보호를 사용하도록 구성한 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 랜섬웨어 보호 옆에 있는 연필 아이콘을 클릭합니다.

Information	Features
System Tags	3 Tags 
Scheduled Downtime	Off 
Blob Access Tiering	Hot 
Instance Type	Standard_E8ds_v4 
Charging Method	Capacity-based 
Write Speed	<i>Not Supported</i> 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

3. 랜섬웨어에 대한 NetApp 솔루션 구현:

a. 스냅샷 정책이 활성화되지 않은 볼륨이 있는 경우 *스냅샷 정책 활성화*를 클릭합니다.

NetApp Snapshot 기술은 랜섬웨어 치료를 위한 업계 최고의 솔루션을 제공합니다. 성공적인 복구의 핵심은 감염되지 않은 백업에서 복원하는 것입니다. 스냅샷 사본은 읽기 전용이므로 랜섬웨어로 인한 손상을 방지할 수 있습니다. 또한 단일 파일 사본이나 완벽한 재해 복구 솔루션의 이미지를 만드는 세분성을 제공할 수도 있습니다.

b. ONTAP의 FPolicy 솔루션을 활성화하려면 *FPolicy 활성화*를 클릭하세요. 이 솔루션은 파일 확장자를 기준으로 파일 작업을 차단할 수 있습니다.

이 예방 솔루션은 일반적인 랜섬웨어 파일 유형을 차단하여 랜섬웨어 공격으로부터의 보호 기능을 강화합니다.

기본 FPolicy 범위는 다음 확장자를 가진 파일을 차단합니다.

マイクロ, 암호화된, 잠긴, 크립토, 크립토, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, 좋은, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre



이 범위는 Cloud Volumes ONTAP에서 FPolicy를 활성화할 때 생성됩니다. 이 목록은 일반적인 랜섬웨어 파일 유형을 기반으로 작성되었습니다. Cloud Volumes ONTAP CLI의 *vserver fpolicy policy scope* 명령을 사용하여 차단된 파일 확장자를 사용자 정의할 수 있습니다.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection

50 % Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

[Activate Snapshot Policy](#)

2 Block Ransomware File Extensions

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names](#)

[Activate FPolicy](#)

자율형 랜섬웨어 보호

Cloud Volumes ONTAP 랜섬웨어 공격을 나타낼 수 있는 비정상적인 활동을 사전에 감지하고 경고하기 위해 워크로드에 대한 분석을 수행하는 ARP(Autonomous Ransomware Protection) 기능을 지원합니다.

다음을 통해 제공되는 파일 확장자 보호와 별도로 [랜섬웨어 보호 설정](#) ARP 기능은 작업 부하 분석을 사용하여 감지된 "비정상적인 활동"을 기반으로 잠재적인 공격에 대해 사용자에게 경고합니다. 랜섬웨어 보호 설정과 ARP 기능은 모두 종합적인 랜섬웨어 보호를 위해 함께 사용할 수 있습니다.

ARP 기능은 추가 비용 없이 BYOL(Bring Your Own License) 및 마켓플레이스 구독을 통해 라이선스를 사용할 수 있습니다.

ARP 지원 볼륨에는 "학습 모드" 또는 "활성" 상태가 지정됩니다.

볼륨에 대한 ARP 구성은 ONTAP 시스템 관리자와 ONTAP CLI를 통해 수행됩니다.

ONTAP System Manager 및 ONTAP CLI를 사용하여 ARP를 활성화하는 방법에 대한 자세한 내용은 다음을 참조하십시오. ["ONTAP 설명서: 자율 랜섬웨어 보호 활성화"](#).

Autonomous Ransomware Protection i

0 TiB

Protected Capacity

100 TiB

Precommitted capacity

0 TiB

PAYGO

BYOL

100 TiB

Marketplace Contracts 0 TiB

Cloud Volumes ONTAP에서 WORM 파일의 변조 방지 스냅샷 복사본을 만듭니다.

Cloud Volumes ONTAP 시스템에서 한 번 쓰고 여러 번 읽을 수 있는(WORM) 파일의 변조 방지 스냅샷 사본을 만들고 특정 보존 기간 동안 수정되지 않은 형태로 스냅샷을 보관할 수 있습니다. 이 기능은 SnapLock 기술을 기반으로 하며, 데이터 보호 및 규정 준수를 한층 더 강화합니다.

시작하기 전에

스냅샷 복사본을 만드는 데 사용하는 볼륨이 SnapLock 볼륨인지 확인하세요. 볼륨에서 SnapLock 보호를 활성화하는 방법에 대한 자세한 내용은 다음을 참조하십시오. ["ONTAP 설명서: SnapLock 구성"](#).

단계

1. SnapLock 볼륨에서 스냅샷 복사본을 만듭니다. CLI 또는 시스템 관리자를 사용하여 스냅샷 복사본을 만드는 방법에 대한 자세한 내용은 다음을 참조하십시오. ["ONTAP 설명서: 로컬 스냅샷 복사본 관리 개요"](#).

스냅샷 복사본은 볼륨의 WORM 속성을 상속하므로 변조가 불가능합니다. 기본 SnapLock 기술은 지정된 보존 기간이 경과할 때까지 스냅샷이 편집 및 삭제되지 않도록 보호합니다.

2. 스냅샷을 편집해야 하는 경우 보존 기간을 수정할 수 있습니다. 자세한 내용은 다음을 참조하세요. ["ONTAP 문서: 보존 시간 설정"](#).



스냅샷 사본은 특정 보존 기간 동안 보호되지만, Cloud Volumes ONTAP의 WORM 스토리지는 "신뢰할 수 있는 스토리지 관리자" 모델에서 작동하므로 클러스터 관리자가 소스 볼륨을 삭제할 수 있습니다. 또한 신뢰할 수 있는 클라우드 관리자는 클라우드 스토리지 리소스를 조작하여 WORM 데이터를 삭제할 수 있습니다.

관련 링크

- WORM에 대한 자세한 내용은 다음을 참조하세요. ["Cloud Volumes ONTAP의 WORM 스토리지에 대해 알아보세요"](#).

- SnapLock 볼륨 충전에 대한 정보는 다음을 참조하세요. ["Cloud Volumes ONTAP 의 라이선싱 및 요금 청구"](#) .

시스템 관리

Cloud Volumes ONTAP 업그레이드

NetApp Console에서 Cloud Volumes ONTAP 업그레이드하여 최신 새 기능과 향상된 기능을 활용하세요. 소프트웨어를 업그레이드하기 전에 Cloud Volumes ONTAP 시스템을 준비해야 합니다.

업그레이드 개요

Cloud Volumes ONTAP 업그레이드 프로세스를 시작하기 전에 다음 사항을 알고 있어야 합니다.

콘솔에서만 업그레이드

ONTAP System Manager나 ONTAP CLI를 사용해서는 안 되며, 오직 콘솔을 사용해서만 Cloud Volumes ONTAP 업그레이드해야 합니다. 그렇지 않으면 시스템 안정성에 영향을 미칠 수 있습니다.

업그레이드 방법

콘솔은 Cloud Volumes ONTAP을 업그레이드하는 두 가지 방법을 제공합니다.

- 시스템에 나타나는 업그레이드 알림을 따르면
- HTTPS 위치에 업그레이드 이미지를 배치한 다음 콘솔에 URL을 제공합니다.

지원되는 업그레이드 경로

업그레이드할 수 있는 Cloud Volumes ONTAP 버전은 현재 실행 중인 Cloud Volumes ONTAP 버전에 따라 달라집니다.

현재 버전	직접 업그레이드할 수 있는 버전
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1 9.15.0
9.14.0	9.14.1
9.13.1	9.14.1 9.14.0
9.13.0	9.13.1
9.12.1	9.13.1 9.13.0

현재 버전	직접 업그레이드할 수 있는 버전
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

현재 버전	직접 업그레이드할 수 있는 버전
9.16.1 P3	9.17.1 RC1
9.15.1 P10	9.16.1 P3
9.14.1 P13	9.15.1 P10
9.13.1 P16	9.14.1 P13
9.12.1 P18	9.13.1 P16
9.11.1 P20	9.12.1 P18

Azure에 이전 버전의 Cloud Volumes ONTAP 있는 경우 먼저 다음 버전으로 업그레이드한 후 지원되는 업그레이드 경로를 따라 대상 버전에 도달해야 합니다. 예를 들어 Cloud Volumes ONTAP 9.7 P7이 있는 경우 다음 업그레이드 경로를 따르세요.

- 9.7 P7 → 9.8 P18
- 9.8 P18 → 9.9.1 P15
- 9.9.1 P15 → 9.10.1 P12

- 9.10.1 P12 → 9.11.1 P20

현재 버전	직접 업그레이드할 수 있는 버전
9.16.1	9.17.1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

다음 사항에 유의하세요.

- Cloud Volumes ONTAP 에 지원되는 업그레이드 경로는 온프레미스 ONTAP 클러스터와 다릅니다.
- 시스템에 나타나는 알림에 따라 업그레이드하는 경우, 콘솔에서 지원되는 업그레이드 경로를 따르는 릴리스로 업그레이드하라는 메시지가 표시됩니다.
- HTTPS 위치에 업그레이드 이미지를 배치하여 업그레이드하는 경우, 지원되는 다음 업그레이드 경로를 따라야 합니다.
- 어떤 경우에는 대상 릴리스에 도달하기 위해 여러 번 업그레이드해야 할 수도 있습니다.

예를 들어, 버전 9.8을 사용 중이고 9.10.1로 업그레이드하려는 경우 먼저 버전 9.9.1로 업그레이드한 다음 9.10.1로 업그레이드해야 합니다.

패치 릴리스

2024년 1월부터 Cloud Volumes ONTAP 의 최신 버전 3개에 대한 패치 릴리스가 있는 경우에만 패치 업그레이드가 가능합니다. RC 또는 GA 버전을 배포할 수 없을 때 패치 버전을 배포할 수 있는 경우가 있습니다.

콘솔에 표시할 최신 버전 3개를 결정하기 위해 최신 GA 릴리스를 사용합니다. 예를 들어, 현재 GA 릴리스가 9.13.10이면 9.11.1-9.13.1에 대한 패치가 콘솔에 나타납니다.

패치 버전 9.11.1 이하의 경우 수동 업그레이드 절차를 사용해야 합니다.[ONTAP 이미지 다운로드](#) .

패치 릴리스에 대한 일반적인 규칙에 따라 동일하거나 다음 Cloud Volumes ONTAP 릴리스에서 낮은 패치 버전에서 더 높은 패치 버전으로 업그레이드할 수 있습니다.

다음은 몇 가지 예입니다.

- 9.13.0 → 9.13.1 P15
- 9.12.1 → 9.13.1 P2

되돌리기 또는 다운그레이드

Cloud Volumes ONTAP 이전 릴리스로 되돌리거나 다운그레이드하는 것은 지원되지 않습니다.

지원 등록

이 페이지에 설명된 방법을 사용하여 소프트웨어를 업그레이드하려면 Cloud Volumes ONTAP NetApp 지원팀에 등록해야 합니다. 이는 종량제(PAYGO)와 자체 라이선스 사용(BYOL) 모두에 적용됩니다. 당신은 필요합니다 "["PAYGO 시스템 수동 등록"](#) BYOL 시스템은 기본적으로 등록됩니다.



지원에 등록되지 않은 시스템도 새 버전이 출시되면 콘솔에 표시되는 소프트웨어 업데이트 알림을 받게 됩니다. 하지만 소프트웨어를 업그레이드하려면 먼저 시스템을 등록해야 합니다.

HA 중재자의 업그레이드

콘솔은 Cloud Volumes ONTAP 업그레이드 프로세스 중에 필요에 따라 중재자 인스턴스도 업데이트합니다.

c4, m4 및 r4 EC2 인스턴스 유형을 사용한 AWS 업그레이드

Cloud Volumes ONTAP 더 이상 c4, m4, r4 EC2 인스턴스 유형을 지원하지 않습니다. 다음 인스턴스 유형을 사용하면 기존 배포를 Cloud Volumes ONTAP 버전 9.8-9.12.1로 업그레이드할 수 있습니다. 업그레이드하기 전에 다음을 권장합니다.[인스턴스 유형을 변경합니다](#) . 인스턴스 유형을 변경할 수 없는 경우 다음을 수행해야 합니다.[향상된](#)

네트워킹을 활성화하세요 업그레이드하기 전에 인스턴스 유형을 변경하고 향상된 네트워킹을 활성화하는 방법에 대해 자세히 알아보려면 다음 섹션을 읽어보세요.

9.13.0 이상 버전을 실행하는 Cloud Volumes ONTAP에서는 c4, m4, r4 EC2 인스턴스 유형으로 업그레이드할 수 없습니다. 이 경우에는 디스크 개수를 줄여야 합니다.[인스턴스 유형을 변경합니다](#) 또는 c5, m5, r5 EC2 인스턴스 유형을 사용하여 새로운 HA 쌍 구성을 배포하고 데이터를 마이그레이션합니다.

인스턴스 유형 변경

c4, m4 및 r4 EC2 인스턴스 유형은 c5, m5 및 r5 EC2 인스턴스 유형보다 노드당 더 많은 디스크를 허용합니다. 실행 중인 c4, m4 또는 r4 EC2 인스턴스의 노드당 디스크 수가 c5, m5 및 r5 인스턴스의 노드당 최대 디스크 허용량보다 낮은 경우 EC2 인스턴스 유형을 c5, m5 또는 r5로 변경할 수 있습니다.

["EC2 인스턴스별 디스크 및 계층화 제한 확인" "Cloud Volumes ONTAP 의 EC2 인스턴스 유형 변경"](#)

인스턴스 유형을 변경할 수 없는 경우 다음 단계를 따르세요.[향상된 네트워킹 활성화](#).

향상된 네트워킹 활성화

Cloud Volumes ONTAP 버전 9.8 이상으로 업그레이드하려면 c4, m4 또는 r4 인스턴스 유형을 실행하는 클러스터에서 향상된 네트워킹을 활성화해야 합니다. ENA를 활성화하려면 기술 자료 문서를 참조하세요.["AWS Cloud Volumes ONTAP 인스턴스에서 SR-IOV 또는 ENA와 같은 향상된 네트워킹을 활성화하는 방법"](#).

업그레이드 준비

업그레이드를 수행하기 전에 시스템이 준비되었는지 확인하고 필요한 구성을 변경해야 합니다.

- [가동 중지 시간을 계획하세요](#)
- [자동 환불이 여전히 활성화되어 있는지 확인하세요.](#)
- [SnapMirror 전송 일시 중단](#)
- [집계가 온라인인지 확인하세요](#)
- [모든 LIF가 홈 포트에 있는지 확인하세요.](#)

가동 중지 시간을 계획하세요

단일 노드 시스템을 업그레이드하면 업그레이드 프로세스로 인해 시스템이 최대 25분 동안 오프라인 상태가 되며, 이 기간 동안 I/O가 중단됩니다.

많은 경우 HA 쌍을 업그레이드하는 작업은 중단 없이 진행되며 I/O도 중단되지 않습니다. 이러한 중단 없는 업그레이드 프로세스 동안 각 노드는 클라이언트에 I/O를 계속 제공하기 위해 동시에 업그레이드됩니다.

세션 지향 프로토콜은 업그레이드 중 특정 영역의 클라이언트와 애플리케이션에 부정적인 영향을 미칠 수 있습니다. 자세한 내용은 다음을 참조하세요. ["ONTAP 문서"](#)

자동 환불이 여전히 활성화되어 있는지 확인하세요.

Cloud Volumes ONTAP HA 쌍에서 자동 반환 기능을 활성화해야 합니다(이는 기본 설정입니다). 그렇지 않으면 작업이 실패합니다.

["ONTAP 설명서: 자동 반환 구성을 위한 명령"](#)

SnapMirror 전송 일시 중단

Cloud Volumes ONTAP 시스템에 활성 SnapMirror 관계가 있는 경우 Cloud Volumes ONTAP 소프트웨어를 업데이트하기 전에 전송을 일시 중단하는 것이 가장 좋습니다. 전송을 일시 중단하면 SnapMirror 오류가 방지됩니다. 대상 시스템에서 전송을 중단해야 합니다.



NetApp Backup and Recovery SnapMirror 구현(SnapMirror Cloud라고 함)을 사용하여 백업 파일을 생성하지만, 시스템을 업그레이드할 때 백업을 중단할 필요는 없습니다.

이 작업에 관하여

이 단계에서는 ONTAP System Manager 9.3 이상을 사용하는 방법을 설명합니다.

단계

1. 대상 시스템에서 시스템 관리자에 로그인합니다.

웹 브라우저에서 클러스터 관리 LIF의 IP 주소를 입력하면 System Manager에 로그인할 수 있습니다. IP 주소는 Cloud Volumes ONTAP 시스템에서 찾을 수 있습니다.



콘솔에 액세스하는 컴퓨터는 Cloud Volumes ONTAP에 네트워크로 연결되어 있어야 합니다. 예를 들어, 클라우드 공급자 네트워크에 있는 점프 호스트에서 콘솔에 로그인해야 할 수도 있습니다.

2. *보호 > 관계*를 클릭합니다.
3. 관계를 선택하고 *작업 > 정지*를 클릭합니다.

집계가 온라인인지 확인하세요

소프트웨어를 업데이트하기 전에 Cloud Volumes ONTAP의 집계가 온라인 상태여야 합니다. 대부분의 구성에서 집계는 온라인 상태여야 하지만, 그렇지 않은 경우 온라인으로 전환해야 합니다.

이 작업에 관하여

이 단계에서는 ONTAP System Manager 9.3 이상을 사용하는 방법을 설명합니다.

단계

1. Cloud Volumes ONTAP 시스템에서 집계 탭을 클릭합니다.
2. 필요한 집계 타일에서 다음을 클릭합니다. **...** 아이콘을 클릭한 다음 *집계 세부 정보 보기*를 선택하세요.

Aggregate Details

aggr1

Overview	Capacity Allocation	Provider Properties
State online		
Home Node [redacted]		
Encryption Type cloudEncrypted		
Volumes 2		

3. 집계가 오프라인인 경우 ONTAP 시스템 관리자를 사용하여 집계를 온라인으로 전환합니다.
 - a. *저장소 > 집계 및 디스크 > 집계*를 클릭합니다.
 - b. 집계를 선택한 다음 *추가 작업 > 상태 > 온라인*을 클릭합니다.

모든 LIF가 홈 포트에 있는지 확인하세요.

업그레이드하기 전에 모든 LIF가 홈 포트에 있어야 합니다. ONTAP 설명서를 참조하세요.["모든 LIF가 홈 포트에 있는지 확인하세요"](#) .

업그레이드 실패 오류가 발생하면 기술 자료(KB) 문서를 참조하세요.["Cloud Volumes ONTAP 업그레이드 실패"](#) .

Cloud Volumes ONTAP 업그레이드

콘솔은 업그레이드할 수 있는 새로운 버전이 있을 때 알려줍니다. 이 알림에서 업그레이드 프로세스를 시작할 수 있습니다. 자세한 내용은 다음을 참조하세요. [콘솔 알림에서 업그레이드](#) .

외부 URL의 이미지를 사용하여 소프트웨어 업그레이드를 수행하는 또 다른 방법입니다. 이 옵션은 콘솔이 S3 버킷에 액세스하여 소프트웨어를 업그레이드할 수 없거나 패치가 제공된 경우에 유용합니다. 자세한 내용은 다음을 참조하세요. [URL에서 사용 가능한 이미지에서 업그레이드](#) .

콘솔 알림에서 업그레이드

Cloud Volumes ONTAP Cloud Volumes ONTAP ONTAP 작업 환경에 알림을 표시합니다.



알림을 통해 Cloud Volumes ONTAP 업그레이드하려면 NetApp 지원 사이트 계정이 있어야 합니다.

이 알림을 통해 업그레이드 프로세스를 시작할 수 있습니다. 이 알림은 S3 버킷에서 소프트웨어 이미지를 얻고, 이미지를 설치한 다음 시스템을 다시 시작하여 프로세스를 자동화합니다.

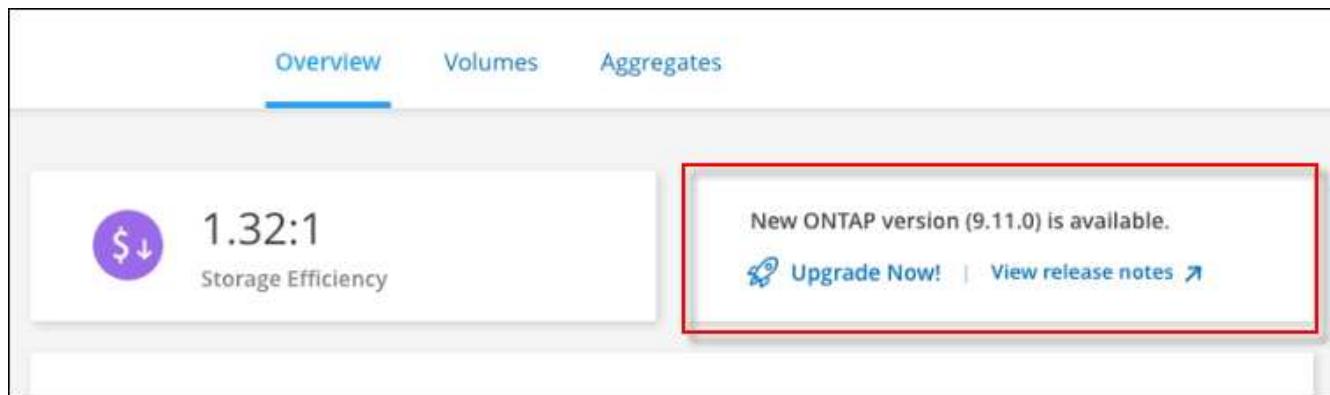
시작하기 전에

볼륨이나 집계 생성과 같은 작업은 Cloud Volumes ONTAP 시스템에서 진행 중이어서는 안 됩니다.

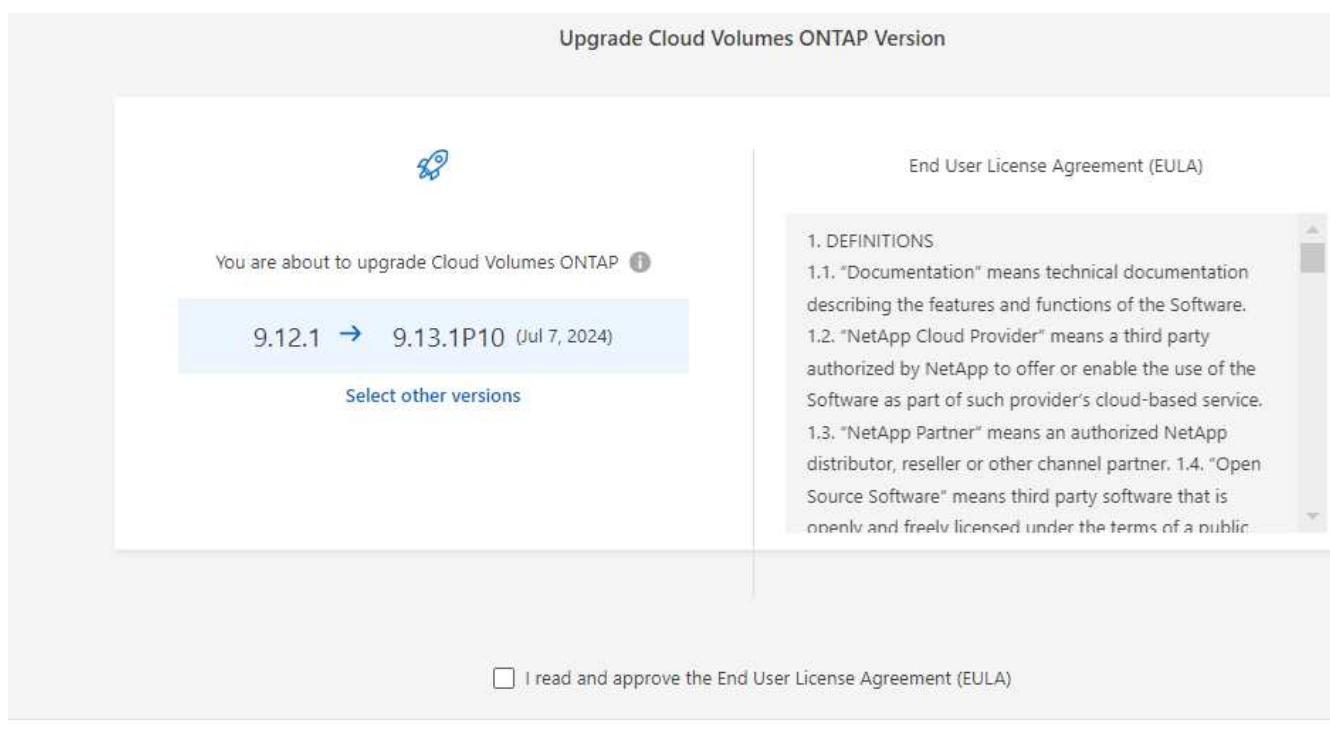
단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. Cloud Volumes ONTAP 시스템을 선택하세요.

새 버전이 출시되면 개요 탭에 알림이 표시됩니다.



3. 설치된 Cloud Volumes ONTAP 버전을 업그레이드하려면 *지금 업그레이드!*를 클릭하세요. 기본적으로 업그레이드할 수 있는 최신 호환 버전이 표시됩니다.



다른 버전으로 업그레이드하려면 *다른 버전 선택*을 클릭하세요. 시스템에 설치된 버전과 호환되는 최신 Cloud Volumes ONTAP 버전이 나열되어 있습니다. 예를 들어, 시스템에 설치된 버전이 9.12.1P3이고, 다음과 같은 호환 버전을 사용할 수 있습니다.

- 9.12.1P4부터 9.12.1P14까지
- 9.13.1 및 9.13.1P1 업그레이드를 위한 기본 버전으로 9.13.1P1이 표시되고, 다른 사용 가능한 버전으로 9.12.1P13, 9.13.1P14, 9.13.1 및 9.13.1P10이 표시됩니다.

- 선택적으로, *모든 버전*을 클릭하여 업그레이드하려는 다른 버전(예: 설치된 버전의 다음 패치)을 입력할 수 있습니다. 현재 Cloud Volumes ONTAP 버전의 호환 업그레이드 경로는 다음을 참조하세요."[지원되는 업그레이드 경로](#)".
- *저장*을 클릭한 다음 *적용*을 클릭합니다

Select the ONTAP version you want to upgrade to:

Version	Date
<input type="radio"/> 9.12.1P14	Aug 22, 2024
<input type="radio"/> 9.12.1P13	Jul 7, 2024
<input type="radio"/> 9.13.1P10	Jul 7, 2024
<input type="radio"/> 9.13.1P9	May 9, 2024

All versions ^

Write the version you want to upgrade to:

Write the version here

Save Cancel

Apply Cancel

- 업그레이드 Cloud Volumes ONTAP 페이지에서 EULA를 읽은 다음 *EULA를 읽고 승인합니다*를 선택합니다.
- *업그레이드*를 선택하세요.
- 진행 상황을 보려면 Cloud Volumes ONTAP 시스템에서 *감사*를 선택하세요.

결과

콘솔에서 소프트웨어 업그레이드가 시작됩니다. 소프트웨어 업데이트가 완료되면 시스템에서 작업을 수행할 수 있습니다.

당신이 완료한 후

SnapMirror 전송을 중단한 경우 시스템 관리자를 사용하여 전송을 재개하세요.

URL에서 사용 가능한 이미지에서 업그레이드

Cloud Volumes ONTAP 소프트웨어 이미지를 콘솔 에이전트나 HTTP 서버에 배치한 다음 콘솔에서 소프트웨어 업그레이드를 시작할 수 있습니다. 콘솔이 S3 버킷에 액세스하여 소프트웨어를 업그레이드할 수 없는 경우 이 옵션을

사용할 수 있습니다.

시작하기 전에

- 볼륨이나 집계 생성과 같은 작업은 Cloud Volumes ONTAP 시스템에서 진행 중이어서는 안 됩니다.
- ONTAP 이미지를 호스팅하기 위해 HTTPS를 사용하는 경우 인증서 누락으로 인해 SSL 인증 문제가 발생하여 업그레이드가 실패할 수 있습니다. 해결 방법은 ONTAP과 콘솔 간 인증에 사용할 CA 서명 인증서를 생성하고 설치하는 것입니다.

NetApp 기술 자료로 이동하여 단계별 지침을 확인하세요.

["NetApp KB: 업그레이드 이미지를 호스팅하기 위해 콘솔을 HTTPS 서버로 구성하는 방법"](#)

단계

1. 선택 사항: Cloud Volumes ONTAP 소프트웨어 이미지를 호스팅할 수 있는 HTTP 서버를 설정합니다.

가상 네트워크에 VPN 연결이 있는 경우 Cloud Volumes ONTAP 소프트웨어 이미지를 자체 네트워크의 HTTP 서버에 배치할 수 있습니다. 그렇지 않은 경우 클라우드의 HTTP 서버에 파일을 저장해야 합니다.

2. Cloud Volumes ONTAP에 자체 보안 그룹을 사용하는 경우 아웃바운드 규칙에서 HTTP 연결을 허용하여 Cloud Volumes ONTAP이 소프트웨어 이미지에 액세스할 수 있는지 확인하세요.



미리 정의된 Cloud Volumes ONTAP 보안 그룹은 기본적으로 아웃바운드 HTTP 연결을 허용합니다.

3. 소프트웨어 이미지를 얻으세요 ["NetApp 지원 사이트"](#).

4. 소프트웨어 이미지를 콘솔 에이전트나 파일이 제공될 HTTP 서버의 디렉토리에 복사합니다.

두 가지 경로가 있습니다. 올바른 경로는 콘솔 에이전트 버전에 따라 다릅니다.

◦ /opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/
◦ /opt/application/netapp/cloudmanager/ontap/images/

5. 시스템에서 다음을 클릭합니다. 아이콘을 클릭한 다음 *Cloud Volumes ONTAP 업데이트*를 클릭합니다.

6. Cloud Volumes ONTAP 버전 업데이트 페이지에서 URL을 입력한 다음 *이미지 변경*을 클릭합니다.

위에 표시된 경로의 콘솔 에이전트에 소프트웨어 이미지를 복사한 경우 다음 URL을 입력합니다.

`http://<콘솔_에이전트_개인-IP-주소>/ontap/images/<이미지-파일-이름>`



URL에서 *이미지 파일 이름*은 "cot.image.9.13.1P2.tgz" 형식을 따라야 합니다.

7. 확인하려면 *계속*을 클릭하세요.

결과

콘솔에서 소프트웨어 업데이트가 시작됩니다. 소프트웨어 업데이트가 완료되면 시스템에서 작업을 수행할 수 있습니다.

당신이 완료한 후

SnapMirror 전송을 중단한 경우 시스템 관리자를 사용하여 전송을 재개하세요.

Google Cloud NAT 게이트웨이 사용 시 다운로드 실패 문제 해결

콘솔 에이전트는 Cloud Volumes ONTAP에 대한 소프트웨어 업데이트를 자동으로 다운로드합니다. 구성에서 Google Cloud NAT 게이트웨이를 사용하는 경우 다운로드가 실패할 수 있습니다. 이 문제는 소프트웨어 이미지가 나누어지는 부분의 수를 제한하면 해결할 수 있습니다. 이 단계를 완료하려면 API를 사용해야 합니다.

단계

1. 다음 JSON을 본문으로 하여 `/occm/config`에 PUT 요청을 제출합니다.

```
{  
  "maxDownloadSessions": 32  
}
```

`maxDownloadSessions`의 값은 10이거나 1보다 큰 정수일 수 있습니다. 값이 1이면 다운로드한 이미지는 분할되지 않습니다.

32는 예시 값입니다. 사용해야 하는 값은 NAT 구성과 동시에 가질 수 있는 세션 수에 따라 달라집니다.

["/occm/config API 호출에 대해 자세히 알아보세요"](#).

Cloud Volumes ONTAP 종량제 시스템 등록

NetApp의 지원은 Cloud Volumes ONTAP PAYGO(Pay-as-you-go) 시스템에 포함되어 있지만, 먼저 NetApp에 시스템을 등록하여 지원을 활성화해야 합니다.

ONTAP 소프트웨어를 업그레이드하려면 NetApp에 PAYGO 시스템을 등록해야 합니다. ["이 페이지에 설명되어 있습니다"](#).



지원에 등록되지 않은 시스템에서도 새로운 버전이 출시되면 NetApp Console에 표시되는 소프트웨어 업데이트 알림을 받게 됩니다. 하지만 소프트웨어를 업그레이드하려면 먼저 시스템을 등록해야 합니다.

단계

1. 아직 NetApp 지원 사이트 계정을 콘솔에 추가하지 않았다면 *계정 설정*으로 이동하여 지금 추가하세요.
["NetApp 지원 사이트 계정을 추가하는 방법을 알아보세요"](#).
2. 시스템 페이지에서 등록하려는 시스템 이름을 두 번 클릭합니다.
3. 개요 탭에서 기능 패널을 클릭한 다음 지원 등록 옆에 있는 연필 아이콘을 클릭합니다.

Information	Features
System Tags	3 Tags 
Scheduled Downtime	Off 
Blob Access Tiering	Hot 
Instance Type	Standard_E8ds_v4 
Charging Method	Capacity-based 
Write Speed	<i>Not Supported</i> 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

4. NetApp 지원 사이트 계정을 선택하고 *등록*을 클릭하세요.

결과

해당 시스템은 NetApp 에 등록되어 있습니다.

Cloud Volumes ONTAP 노드 기반 라이선스를 용량 기반 라이선스로 변환

노드 기반 라이선스의 사용 가능 기간 종료(EOA) 후에는 NetApp Console 의 라이선스 변환

도구를 사용하여 용량 기반 라이선스로 전환해야 합니다.

연간 또는 장기 약정의 경우 NetApp EOA 날짜(2024년 11월 11일) 또는 라이선스 만료일 전에 NetApp 담당자에게 연락하여 전환에 필요한 전제 조건이 충족되었는지 확인하는 것을 권장합니다. Cloud Volumes ONTAP 노드에 대한 장기 계약이 없고 온디맨드 종량제(PAYGO) 구독으로 시스템을 실행하는 경우 2024년 12월 31일 지원 종료(EOS) 전에 전환을 계획하는 것이 중요합니다. 두 경우 모두 NetApp Console 의 라이선스 변환 도구를 사용하여 원활하게 전환하기 전에 시스템이 요구 사항을 충족하는지 확인해야 합니다.

EOA 및 EOS에 대한 정보는 다음을 참조하세요.["노드 기반 라이선스 제공 종료"](#).

이 작업에 관하여

- 라이선스 변환 도구를 사용하면 노드 기반에서 용량 기반 라이선스 모델로의 전환이 현장에서 온라인에서 수행되므로 데이터 마이그레이션이나 추가 클라우드 리소스 프로비저닝이 필요 없습니다.
- 이는 중단 없는 작업이므로 서비스 중단이나 애플리케이션 가동 중지가 발생하지 않습니다.
- Cloud Volumes ONTAP 시스템의 계정 및 애플리케이션 데이터는 그대로 유지됩니다.
- 기본 클라우드 리소스는 변환 후에도 영향을 받지 않습니다.
- 라이선스 변환 도구는 단일 노드, 단일 가용성 영역(AZ)의 고가용성(HA), 여러 AZ의 HA, 자체 라이선스 사용(BYOL), PAYGO 등 모든 배포 유형을 지원합니다.
- 이 도구는 모든 노드 기반 라이선스를 소스로, 모든 용량 기반 라이선스를 대상으로 지원합니다. 예를 들어 PAYGO Standard 노드 기반 라이선스가 있는 경우 마켓플레이스를 통해 구매한 모든 용량 기반 라이선스로 변환할 수 있습니다. NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요.
["Cloud Volumes ONTAP에 대한 BYOL 라이선싱의 제한된 가용성"](#).
- 이러한 변환은 AWS, Azure, Google Cloud 등 모든 클라우드 제공업체에서 지원됩니다.
- 변환 후 노드 기반 라이센스의 일련 번호는 용량 기반 형식으로 대체됩니다. 이 작업은 변환의 일부로 수행되며 NetApp 지원 사이트(NSS) 계정에 반영됩니다.
- 용량 기반 모델로 전환하면 데이터는 노드 기반 라이선싱과 동일한 위치에 계속 보관됩니다. 이러한 접근 방식은 데이터 배치에 어떠한 중단도 발생하지 않도록 보장하며, 전환 과정 전반에 걸쳐 데이터 주권 원칙을 지지합니다.

시작하기 전에

- 고객 액세스 또는 관리자 액세스 권한이 있는 NSS 계정이 있어야 합니다.
- 귀하의 NSS 계정은 콘솔에 액세스하는 데 사용한 사용자 자격 증명으로 등록되어야 합니다.
- Cloud Volumes ONTAP 시스템은 고객 액세스 또는 관리자 액세스 권한이 있는 NSS 계정에 연결되어야 합니다.
- BYOL 라이선스 또는 마켓플레이스 구독 등 유효한 용량 기반 라이선스가 있어야 합니다.
- 귀하의 계정에는 용량 기반 라이선스가 사용 가능해야 합니다. 이 라이선스는 콘솔의 * Licenses and subscriptions*에서 사용할 수 있는 마켓플레이스 구독 또는 BYOL/개인 제공 패키지일 수 있습니다.
- 목적지 패키지를 선택하기 전에 다음 기준을 이해하세요.
 - 계정에 용량 기반 BYOL 라이선스가 있는 경우 선택한 대상 패키지는 계정의 BYOL 용량 기반 라이선스와 일치해야 합니다.
 - 언제 Professional 대상 패키지로 선택된 경우 계정에 Professional 패키지가 포함된 BYOL 라이선스가 있어야 합니다.
 - 언제 Essentials 대상 패키지로 선택된 경우, 계정에 Essentials 패키지가 포함된 BYOL 라이선스가 있어야 합니다.
 - 대상 패키지가 계정의 BYOL 라이선스 가용성과 일치하지 않으면 용량 기반 라이선스에 선택한 패키지가

포함되지 않을 수 있습니다. 이 경우 마켓플레이스 구독을 통해 요금이 청구됩니다.

- 용량 기반 BYOL 라이선스가 없고 마켓플레이스 구독만 있는 경우, 선택한 패키지가 용량 기반 마켓플레이스 구독에 포함되어 있는지 확인해야 합니다.
- 기존 용량 기반 라이선스에 충분한 용량이 없고, 추가 용량 사용에 대해 요금을 청구하는 마켓플레이스 구독이 있는 경우, 마켓플레이스 구독을 통해 추가 용량에 대한 요금이 청구됩니다.
- 기존 용량 기반 라이선스에 충분한 용량이 없고, 추가 용량 사용에 대한 요금을 청구할 마켓플레이스 구독이 없으면 변환이 이루어질 수 없습니다. 추가 용량에 대한 요금을 청구하거나 현재 라이선스의 사용 가능한 용량을 확장하려면 마켓플레이스 구독을 추가해야 합니다.
- 대상 패키지가 계정의 BYOL 라이선스 가용성과 맞지 않고 기존 용량 기반 라이선스에 충분한 용량이 없는 경우 마켓플레이스 구독을 통해 요금이 청구됩니다.



이러한 요구 사항 중 하나라도 충족되지 않으면 라이센스 전환이 이루어지지 않습니다. 특정한 경우 라이센스는 변환되지만 사용할 수 없을 수도 있습니다. 정보 아이콘을 클릭하여 문제를 파악하고 시정 조치를 취하세요.

단계

1. 시스템 페이지에서 라이선스 유형을 수정하려는 시스템의 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭합니다.
3. 충전 방법 옆에 있는 연필 아이콘을 확인하세요. 시스템의 충전 방법이 다음과 같은 경우 Node Based, 용량별 요금으로 변환할 수 있습니다.



Cloud Volumes ONTAP 시스템이 이미 용량에 따라 요금이 청구되었거나 요구 사항 중 하나라도 충족되지 않으면 아이콘이 비활성화됩니다.

4. 노드 기반 라이선스를 용량 기반으로 변환 화면에서 시스템 이름과 소스 라이선스 세부 정보를 확인합니다.
5. 기존 라이선스를 변환할 대상 패키지를 선택하세요.
 - 골자. 기본값은 Essentials .
 - 전문적인
6. BYOL 라이선스가 있는 경우 변환이 완료된 후 콘솔에서 노드 기반 라이선스를 삭제하기 위한 확인란을 선택할 수 있습니다. 변환이 진행 중이면 이 확인란을 선택해도 콘솔에서 라이센스가 제거되지 않습니다. 이 옵션은 마켓플레이스 구독에는 사용할 수 없습니다.
7. 변경 사항의 의미를 이해했음을 확인하려면 확인란을 선택한 다음 *계속*을 클릭합니다.

당신이 완료한 후

새로운 라이선스 일련 번호를 보고 콘솔의 * Licenses and subscriptions* 메뉴에서 변경 사항을 확인하세요.

다양한 하이퍼스칼라 가격 책정

가격에 대한 자세한 내용은 다음을 참조하세요. ["NetApp Console 웹사이트"](#) .

특정 하이퍼스칼라에 대한 개인 제안에 대한 자세한 내용은 다음 주소로 문의하세요.

- AWS - awspo@netapp.com
- Azure - azurepo@netapp.com

- 구글 클라우드 - gcpoo@netapp.com

Cloud Volumes ONTAP 시스템 시작 및 중지

NetApp Console에서 Cloud Volumes ONTAP 중지하고 시작하여 클라우드 컴퓨팅 비용을 관리할 수 있습니다.

Cloud Volumes ONTAP 자동 종료 예약

컴퓨팅 비용을 낮추려면 특정 시간 간격으로 Cloud Volumes ONTAP 종료해야 할 수도 있습니다. 이 작업을 수동으로 수행하는 대신, 콘솔을 구성하여 특정 시간에 시스템을 자동으로 종료한 다음 다시 시작할 수 있습니다.

이 작업에 관하여

- Cloud Volumes ONTAP 시스템의 자동 종료를 예약하는 경우, 활성 데이터 전송이 진행 중이면 콘솔에서 종료를 연기합니다.

전송이 완료되면 시스템이 종료됩니다.

- 이 작업은 HA 쌍의 두 노드를 자동으로 종료하도록 예약합니다.
- 예약된 종료를 통해 Cloud Volumes ONTAP 끄면 부팅 및 루트 디스크의 스냅샷이 생성되지 않습니다.

다음 섹션에서 설명하는 대로, 스냅샷은 수동 종료를 수행할 때만 자동으로 생성됩니다.

단계

- 시스템 페이지에서 Cloud Volumes ONTAP 시스템을 두 번 클릭합니다.
- 개요 탭에서 기능 패널을 클릭한 다음 예약된 가동 중지 시간 옆에 있는 연필 아이콘을 클릭합니다.

Information	Features
System Tags	3 Tags 
Scheduled Downtime	On 
S3 Storage Classes	Standard 
Instance Type	m5.xlarge 
Charging Method	Capacity-based 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

3. 종료 일정을 지정하세요:

- 매일, 주중마다, 주말마다 시스템을 종료할지 또는 이 세 가지 옵션을 조합하여 종료할지 선택하세요.
- 시스템을 끄고 싶은 시점과 끄고 싶은 시간을 지정하세요.

예

다음 이미지는 콘솔에 매주 토요일 오후 8시(오후 8시)에 12시간 동안 시스템을 종료하도록 지시하는 일정을 보여줍니다. 콘솔은 매주 월요일 오전 12시에 시스템을 다시 시작합니다.

Schedule Downtime

Console Time Zone: 13:48 UTC

Select when to turn off your system:

Turn off every day at 20 : 00 for 12 hours (1-24)

Sun, Mon, Tue, Wed, Thu, Fri, Sat

Turn off every weekdays at 20 : 00 for 12 hours (1-24)

Mon, Tue, Wed, Thu, Fri

Turn off every weekend at 08 : 00 for 48 hours (1-48)

Sat

4. *저장*을 클릭하세요.

결과

일정이 저장되었습니다. 기능 패널 아래의 해당 예약된 가동 중지 시간 항목에 '커짐'이 표시됩니다.

Cloud Volumes ONTAP 중지

Cloud Volumes ONTAP 중지하면 컴퓨팅 비용이 발생하지 않고 루트 및 부팅 디스크의 스냅샷이 생성되므로 문제 해결에 도움이 될 수 있습니다.



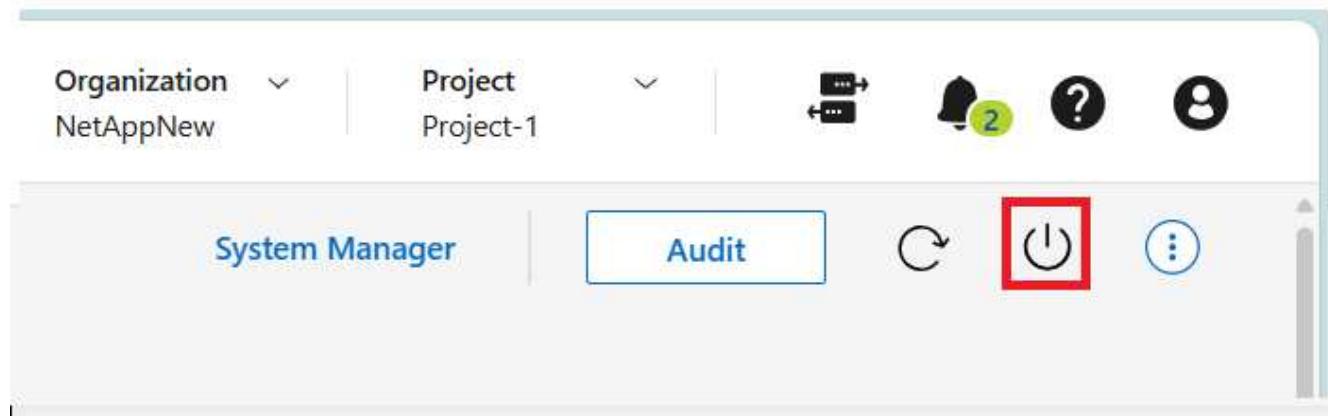
비용을 줄이기 위해 콘솔은 루트 및 부팅 디스크의 오래된 스냅샷을 주기적으로 삭제합니다. 루트 디스크와 부팅 디스크 모두에 가장 최근의 스냅샷 두 개만 보존됩니다.

이 작업에 관하여

HA 쌍을 중지하면 콘솔은 두 노드를 모두 종료합니다.

단계

1. 시스템에서 끄기 아이콘을 클릭합니다.



2. 스냅샷을 생성하면 시스템 복구가 가능하므로 스냅샷 생성 옵션을 활성화해 두세요.

3. *끄기*를 클릭하세요.

시스템을 중지하는 데 최대 몇 분이 걸릴 수 있습니다. 나중에 시스템 페이지에서 시스템을 다시 시작할 수 있습니다.



재부팅 시 스냅샷이 자동으로 생성됩니다.

NTP 서버를 사용하여 Cloud Volumes ONTAP 시스템 시간 동기화

정확한 시간 동기화를 위해서는 Cloud Volumes ONTAP 시스템에 네트워크 시간 프로토콜(NTP) 서버를 설정해야 합니다. Cloud Volumes ONTAP 시스템의 네트워크 내 시간 동기화를 일관되게 유지하려면 모든 클라우드 공급자에 NTP 서버를 구성해야 합니다.



NTP 서버를 구성하지 않으면 서비스 중단 및 시간 동기화 오류가 발생할 수 있습니다.

다음과 같이 NTP 서버를 지정할 수 있습니다.

- ["NetApp Console API"](#).
- ONTAP CLI 명령 ["클러스터 시간 서비스 NTP 서버 생성"](#).

관련 링크

- 기술 자료(KB) 문서: ["CVO 클러스터는 NTP를 어떻게 사용합니까?"](#)
- ["API 사용을 준비하세요"](#)
- ["Cloud Volumes ONTAP 워크플로"](#)
- ["필수 식별자 가져오기"](#)
- ["NetApp Console에 REST API 사용"](#)

시스템 쓰기 속도 수정

NetApp Console에서 Cloud Volumes ONTAP에 대한 일반 쓰기 속도 또는 높은 쓰기 속도를 선택할 수 있습니다. 기본 쓰기 속도는 보통입니다. 작업 부하에 빠른 쓰기 성능이 필요한 경우 높은 쓰기 속도로 변경할 수 있습니다.

모든 유형의 단일 노드 시스템과 일부 HA 쌍 구성에서는 높은 쓰기 속도가 지원됩니다. 지원되는 구성의 보려면 ["Cloud Volumes ONTAP 릴리스 노트"](#)

쓰기 속도를 변경하기 전에 다음을 수행해야 합니다. ["일반 설정과 높은 설정의 차이점을 이해하세요"](#).

이 작업에 관하여

- 볼륨이나 집계 생성과 같은 작업이 진행 중이 아닌지 확인하세요.
- 이 변경으로 인해 Cloud Volumes ONTAP 시스템이 다시 시작된다는 점에 유의하세요. 이는 전체 시스템의 가동 중지를 필요로 하는 파괴적인 프로세스입니다.

단계

1. 시스템 페이지에서 쓰기 속도를 구성할 시스템 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 쓰기 속도 옆에 있는 연필 아이콘을 클릭합니다.
3. 보통 또는 *높음*을 선택하세요.

높음을 선택한 경우, "이해합니다..."라는 문장을 읽고 상자를 체크하여 확인해야 합니다.



높음 쓰기 속도 옵션은 Google Cloud의 Cloud Volumes ONTAP HA 쌍에서 버전 9.13.0부터 지원됩니다.

4. *저장*을 클릭하고 확인 메시지를 검토한 다음 *승인*을 클릭합니다.

Cloud Volumes ONTAP 클러스터 관리자 비밀번호 변경

Cloud Volumes ONTAP 클러스터 관리자 계정이 포함되어 있습니다. 필요한 경우 NetApp Console에서 이 계정의 비밀번호를 변경할 수 있습니다.



ONTAP 시스템 관리자나 ONTAP CLI를 통해 관리자 계정의 비밀번호를 변경해서는 안 됩니다. 비밀번호는 콘솔에 반영되지 않습니다. 결과적으로 콘솔에서 인스턴스를 제대로 모니터링할 수 없습니다.

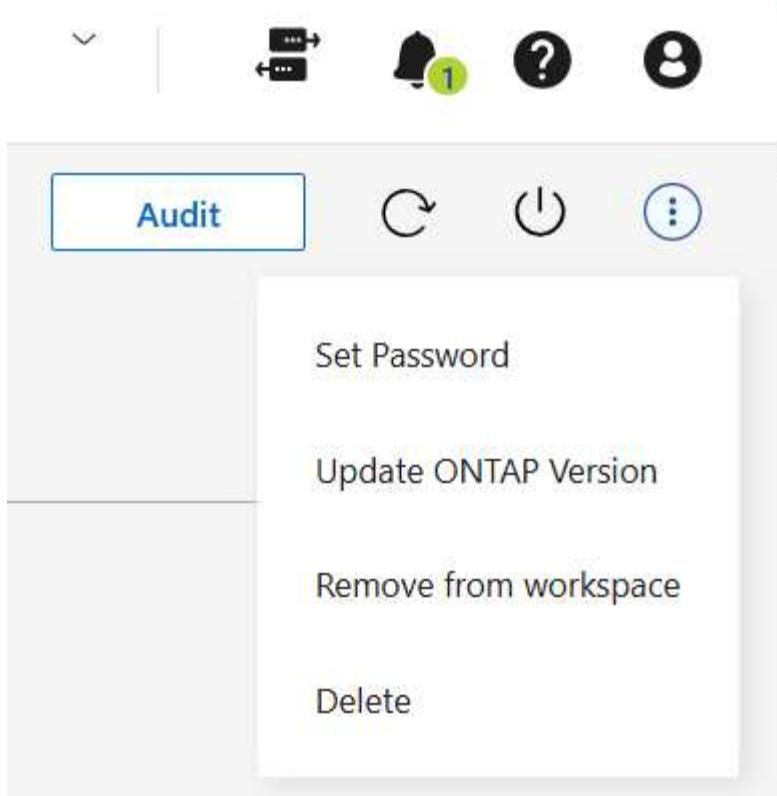
이 작업에 관하여

비밀번호는 몇 가지 규칙을 따라야 합니다. 새로운 비밀번호:

- 단어를 포함해서는 안 됩니다 admin
- 길이는 8~50자 사이여야 합니다.
- 영어 문자 1개와 숫자 1개 이상을 포함해야 합니다.
- 다음 특수문자는 포함할 수 없습니다: / () { } [] # : % " ? \

단계

1. 시스템 페이지에서 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
2. 콘솔의 오른쪽 상단에서 다음을 클릭하세요. 아이콘을 클릭하고 *비밀번호 설정*을 선택하세요.



시스템 추가, 제거 또는 삭제

NetApp Console 에 기존 Cloud Volumes ONTAP 시스템 추가

기존 Cloud Volumes ONTAP 시스템을 검색하여 NetApp Console 에 추가할 수 있습니다. 새로운 시스템을 배포한 경우 이 작업을 수행할 수 있습니다.



콘솔에 로그인하는 데 사용한 계정으로 등록된 시스템만 추가할 수 있습니다. 여러 계정이나 조직이 있는 경우 시스템을 추가하기 전에 올바른 계정에 로그인했는지 확인하세요. 다른 계정이나 조직에 등록된 시스템은 검색, 보기 또는 관리할 수 없습니다.

시작하기 전에

Cloud Volumes ONTAP 관리자 사용자 계정의 비밀번호를 알아야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭합니다.
3. 시스템이 있는 클라우드 공급자를 선택하세요.
4. 추가할 Cloud Volumes ONTAP 시스템 유형을 선택하세요.
5. 링크를 클릭하여 기존 시스템을 알아보세요.

+

1. 지역 페이지에서 지역을 선택하세요. 선택한 지역에서 실행 중인 시스템을 볼 수 있습니다.



이 페이지에서는 Cloud Volumes ONTAP 시스템이 인스턴스로 표시됩니다. 목록에서 현재 계정에 등록된 인스턴스만 선택할 수 있습니다.

2. 자격 증명 페이지에서 Cloud Volumes ONTAP 관리자의 비밀번호를 입력한 다음 *시작*을 선택합니다.

결과

콘솔은 Cloud Volumes ONTAP 시스템을 시스템 페이지에 추가합니다.

NetApp Console에서 Cloud Volumes ONTAP 시스템 제거

Cloud Volumes ONTAP 시스템을 제거하여 다른 시스템으로 이동하거나 검색 문제를 해결할 수 있습니다.

이 작업에 관하여

Cloud Volumes ONTAP 시스템을 제거하면 NetApp Console에서도 제거됩니다. Cloud Volumes ONTAP 시스템은 삭제되지 않습니다. 나중에 필요할 경우 시스템을 다시 검색할 수 있습니다.

단계

1. 시스템 페이지에서 제거하려는 시스템을 두 번 클릭합니다.
2. 콘솔의 오른쪽 상단에서 다음을 클릭합니다. 아이콘을 클릭하고 *작업 공간에서 제거*를 선택합니다.
3. 작업 공간에서 제거 창에서 *제거*를 클릭합니다.

결과

콘솔은 시스템을 제거합니다. 사용자는 언제든지 시스템 페이지에서 삭제된 시스템을 다시 찾을 수 있습니다.

NetApp Console에서 Cloud Volumes ONTAP 시스템 삭제

클라우드 공급업체의 애플리케이션이 아닌 NetApp Console에서 Cloud Volumes ONTAP 시스템을 항상 삭제해야 합니다. 예를 들어, 클라우드 공급자로부터 라이선스가 부여된 Cloud

Volumes ONTAP 인스턴스를 종료하는 경우 다른 인스턴스에 해당 라이선스 키를 사용할 수 없습니다. 라이선스를 해제하려면 콘솔에서 Cloud Volumes ONTAP 시스템을 삭제해야 합니다.

시스템을 삭제하면 콘솔에서 Cloud Volumes ONTAP 인스턴스를 종료하고 디스크와 스냅샷을 삭제합니다.



NetApp Backup and Recovery에서 관리하는 백업과 NetApp Data Classification의 인스턴스와 같은 기타 리소스는 시스템을 삭제해도 삭제되지 않습니다. 수동으로 삭제해야 합니다. 그렇지 않으면 이러한 리소스에 대한 요금이 계속 부과됩니다.

콘솔이 클라우드 공급자에 Cloud Volumes ONTAP 배포하면 인스턴스에 대한 종료 보호가 활성화됩니다. 이 옵션은 실수로 종료되는 것을 방지하는 데 도움이 됩니다.

단계

1. 시스템에서 백업 및 복구를 활성화한 경우 백업된 데이터가 여전히 필요한지 확인한 다음 ["필요한 경우 백업을 삭제하세요"](#).

백업 및 복구는 설계상 Cloud Volumes ONTAP과 독립적입니다. 백업 및 복구 기능은 Cloud Volumes ONTAP 시스템을 삭제할 때 자동으로 백업을 삭제하지 않으며, 시스템이 삭제된 후 백업을 삭제하는 UI 지원도 현재 제공되지 않습니다.

2. 이 시스템에서 데이터 분류를 활성화했고 다른 시스템에서 이 서비스를 사용하지 않는 경우 해당 서비스의 인스턴스를 삭제해야 합니다.

["데이터 분류 인스턴스에 대해 자세히 알아보세요"](#).

3. Cloud Volumes ONTAP 시스템을 삭제합니다.

- a. 시스템 페이지에서 삭제하려는 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
- b. 콘솔의 오른쪽 상단에서 다음을 클릭하세요. **...** 아이콘을 클릭하고 ***삭제***를 선택하세요.
- c. 삭제하려는 시스템 이름을 입력한 다음 ***삭제***를 클릭합니다. 시스템을 삭제하는 데 최대 5분이 걸릴 수 있습니다.



백업 및 복구는 Cloud Volumes ONTAP Professional 라이선스에 대해서만 무료입니다. 이 무료 혜택은 삭제된 환경에는 적용되지 않습니다. Cloud Volumes ONTAP 환경의 백업된 사본이 백업 및 복구 인스턴스에 보관되는 경우, 해당 사본이 삭제될 때까지 백업된 사본에 대한 요금이 청구됩니다.

AWS 관리

AWS에서 Cloud Volumes ONTAP 시스템에 대한 EC2 인스턴스 유형 설정

AWS에서 Cloud Volumes ONTAP 시작하면 여러 인스턴스나 유형 중에서 선택할 수 있습니다. 필요에 따라 인스턴스 유형이 너무 크거나 작다고 판단되면 언제든지 인스턴스 유형을 변경할 수 있습니다.

이 작업에 관하여

- Cloud Volumes ONTAP HA 쌍에서 자동 반환 기능을 활성화해야 합니다(이는 기본 설정입니다). 그렇지 않으면 작업이 실패합니다.

["ONTAP 9 설명서: 자동 반환 구성을 위한 명령"](#)

- 인스턴스 유형을 변경하면 AWS 서비스 요금에 영향을 미칠 수 있습니다.

- 이 작업은 Cloud Volumes ONTAP 다시 시작합니다.

단일 노드 시스템의 경우 I/O가 중단됩니다.

HA 쌍의 경우 변경은 중단되지 않습니다. HA 쌍은 계속해서 데이터를 제공합니다.



NetApp Console 인수를 시작하고 반환을 기다리는 방식으로 한 번에 한 노드씩 변경합니다. NetApp의 품질 보증 팀은 이 프로세스 동안 파일 쓰기와 읽기를 모두 테스트했으며 클라이언트 측에서 아무런 문제도 발견하지 못했습니다. 연결이 변경됨에 따라 I/O 수준에서 일부 재시도가 관찰되었지만 애플리케이션 계층은 NFS/CIFS 연결의 재배선을 극복했습니다.

참조

AWS에서 지원되는 인스턴스 유형 목록은 다음을 참조하세요. ["지원되는 EC2 인스턴스"](#).

c4, m4 또는 r4 인스턴스에서 인스턴스 유형을 변경할 수 없는 경우 KB 문서를 참조하세요. ["AWS Xen CVO 인스턴스를 Nitro\(KVM\)로 변환"](#).

단계

- 시스템 페이지에서 시스템을 선택하세요.
- 개요 탭에서 기능 패널을 클릭한 다음 인스턴스 유형 옆에 있는 연필 아이콘을 클릭합니다.

Information	Features
System Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

노드 기반 사용량 기반(PAYGO) 라이선스를 사용하는 경우, 라이선스 유형 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스와 인스턴스 유형을 선택할 수 있습니다.

3. 인스턴스 유형을 선택하고, 변경 사항의 의미를 이해했음을 확인하는 확인란을 선택한 다음 *변경*을 클릭합니다.

결과

Cloud Volumes ONTAP 새로운 구성으로 재부팅됩니다.

여러 AWS AZ에서 **Cloud Volumes ONTAP HA** 쌍에 대한 경로 테이블 수정

여러 AWS 가용성 영역(AZ)에 배포된 HA 쌍에 대한 플로팅 IP 주소에 대한 경로를 포함하는 AWS 경로 테이블을 수정할 수 있습니다. AWS에서 새로운 NFS 또는 CIFS 클라이언트가 HA 쌍에 액세스해야 하는 경우 이 작업을 수행할 수 있습니다.

단계

1. 시스템 페이지에서 시스템을 선택하세요.
2. 개요 탭에서 기능 패널을 클릭한 다음 경로 테이블 옆에 있는 연필 아이콘을 클릭합니다.
3. 선택한 경로 테이블 목록을 수정한 다음 *저장*을 클릭합니다.

결과

NetApp Console AWS 요청을 보내 경로 테이블을 수정합니다.

Azure 관리

Cloud Volumes ONTAP에 대한 **Azure VM** 유형 변경

Microsoft Azure에서 Cloud Volumes ONTAP 시작하면 여러 VM 유형 중에서 선택할 수 있습니다. 필요에 따라 VM 유형이 너무 크거나 작다고 판단되면 언제든지 VM 유형을 변경할 수 있습니다.

이 작업에 관하여

- Cloud Volumes ONTAP HA 쌍에서 자동 반환 기능을 활성화해야 합니다(이는 기본 설정입니다). 그렇지 않으면 작업이 실패합니다.

"ONTAP 9 설명서: 자동 반환 구성을 위한 명령"

- VM 유형을 변경하면 Microsoft Azure 서비스 요금에 영향을 미칠 수 있습니다.
- 이 작업은 Cloud Volumes ONTAP 다시 시작합니다.

단일 노드 시스템의 경우 I/O가 중단됩니다.

HA 쌍의 경우 변경은 중단되지 않습니다. HA 쌍은 계속해서 데이터를 제공합니다.



NetApp Console 인수를 시작하고 반환을 기다리는 방식으로 한 번에 한 노드씩 변경합니다. NetApp의 품질 보증 팀은 이 프로세스 동안 파일 쓰기와 읽기를 모두 테스트했으며 클라이언트 측에서 아무런 문제도 발견하지 못했습니다. 연결이 변경됨에 따라 I/O 수준에서 일부 재시도가 관찰되었지만 애플리케이션 계층은 NFS/CIFS 연결의 재배선을 극복했습니다.

단계

1. 시스템 페이지에서 시스템을 선택하세요.
2. 개요 탭에서 기능 패널을 클릭한 다음 **VM** 유형 옆에 있는 연필 아이콘을 클릭합니다.

노드 기반 사용량 기반(PAYGO) 라이선스를 사용하는 경우, 라이선스 유형 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스와 VM 유형을 선택할 수 있습니다.

3. VM 유형을 선택하고, 변경 사항의 의미를 이해했음을 확인하는 확인란을 선택한 다음 *변경*을 클릭합니다.

결과

Cloud Volumes ONTAP 새로운 구성으로 재부팅됩니다.

Azure에서 Cloud Volumes ONTAP HA 쌍에 대한 CIFS 잠금 재정의

조직 또는 계정 관리자는 NetApp Console에서 Azure 유지 관리 이벤트 중에 Cloud Volumes ONTAP 저장소 반환 문제를 방지하는 설정을 활성화할 수 있습니다. 이 설정을 활성화하면 Cloud Volumes ONTAP CIFS 잠금을 거부하고 활성 CIFS 세션을 재설정합니다.

이 작업에 관하여

Microsoft Azure는 가상 머신에 대한 정기적인 유지 관리 이벤트를 예약합니다. Cloud Volumes ONTAP HA 쌍에서 유지 관리 이벤트가 발생하면 HA 쌍이 스토리지 인수를 시작합니다. 이 유지 관리 이벤트 중에 활성 CIFS 세션이 있는 경우 CIFS 파일에 대한 잠금으로 인해 저장소 반환이 방해받을 수 있습니다.

이 설정을 활성화하면 Cloud Volumes ONTAP 이 잠금을 거부하고 활성 CIFS 세션을 재설정합니다. 결과적으로 HA 쌍은 이러한 유지 관리 이벤트 중에 스토리지 반환을 완료할 수 있습니다.



이 프로세스는 CIFS 클라이언트에 방해가 될 수 있습니다. CIFS 클라이언트에서 커밋되지 않은 데이터는 손실될 수 있습니다.

시작하기 전에

콘솔 설정을 변경하려면 먼저 콘솔 에이전트를 만들어야 합니다. ["방법을 알아보세요"](#).

단계

1. 왼쪽 탐색 창에서 *관리 > 에이전트*로 이동합니다.
2. 클릭 **...** Cloud Volumes ONTAP 시스템을 관리하는 콘솔 에이전트의 아이콘입니다.
3. * Cloud Volumes ONTAP 설정*을 선택합니다.

4. *Azure*에서 *Azure HA 시스템에 대한 Azure CIFS 잠금*을 클릭합니다.

5. 해당 기능을 활성화하려면 확인란을 클릭한 다음 *저장*을 클릭하세요.

Cloud Volumes ONTAP 시스템에 Azure Private Link 또는 서비스 엔드포인트 사용

Cloud Volumes ONTAP 연결된 스토리지 계정에 연결하기 위해 Azure Private Link를 사용합니다. 필요한 경우 Azure Private Links를 비활성화하고 대신 서비스 엔드포인트를 사용할 수 있습니다.

개요

기본적으로 NetApp Console Cloud Volumes ONTAP 과 연결된 스토리지 계정 간의 연결을 위해 Azure Private Link를 활성화합니다. Azure Private Link는 Azure의 엔드포인트 간 연결을 보호하고 성능 이점을 제공합니다.

필요한 경우 Azure Private Link 대신 서비스 엔드포인트를 사용하도록 Cloud Volumes ONTAP 구성할 수 있습니다.

두 구성 모두에서 콘솔은 항상 Cloud Volumes ONTAP 과 스토리지 계정 간 연결에 대한 네트워크 액세스를 제한합니다. 네트워크 액세스는 Cloud Volumes ONTAP 배포된 VNet과 콘솔 에이전트가 배포된 VNet으로 제한됩니다.

Azure Private Links를 비활성화하고 대신 서비스 엔드포인트를 사용하세요.

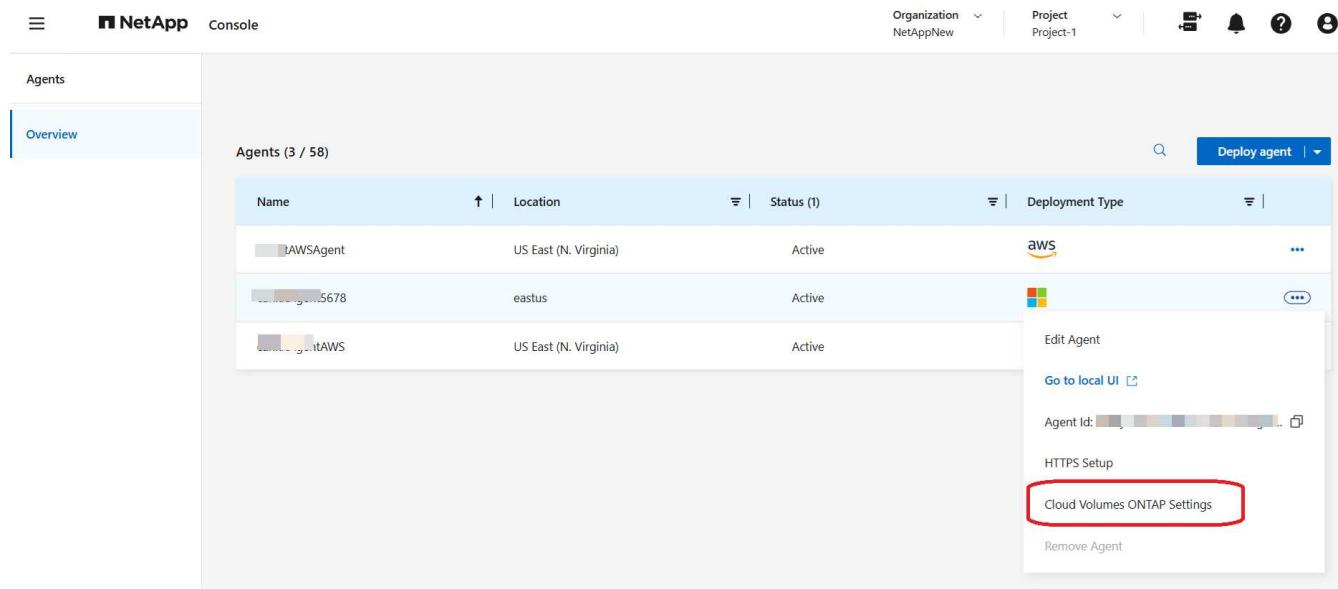
비즈니스에 필요한 경우 콘솔에서 설정을 변경하여 Azure Private Link 대신 서비스 엔드포인트를 사용하도록 Cloud Volumes ONTAP 구성할 수 있습니다. 이 설정을 변경하면 새로 만든 Cloud Volumes ONTAP 시스템에 적용됩니다. 서비스 엔드포인트는 다음에서만 지원됩니다. ["Azure 지역 쌍"](#) 콘솔 에이전트와 Cloud Volumes ONTAP VNet 사이.

콘솔 에이전트는 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 지역이나 ["Azure 지역 쌍"](#) Cloud Volumes ONTAP 시스템용.

단계

1. 왼쪽 탐색 창에서 *관리 > 에이전트*로 이동합니다.
2. 클릭 **...** Cloud Volumes ONTAP 시스템을 관리하는 콘솔 에이전트의 아이콘입니다.

3. * Cloud Volumes ONTAP 설정*을 선택합니다.



The screenshot shows the NetApp Console interface. On the left, there's a sidebar with 'Agents' and 'Overview' tabs. The main area is titled 'Agents (3 / 58)' and lists three agents: 'AWSAgent' (Location: US East (N. Virginia), Status: Active, Deployment Type: AWS), 'eastus' (Location: eastus, Status: Active, Deployment Type: Microsoft), and 'itAWS' (Location: US East (N. Virginia), Status: Active, Deployment Type: AWS). A context menu is open for the 'itAWS' agent, with options like 'Edit Agent', 'Go to local UI', 'Agent Id', 'HTTPS Setup', and 'Cloud Volumes ONTAP Settings' (which is highlighted with a red box). Other menu items include 'Remove Agent'.

4. *Azure*에서 *Azure Private Link 사용*을 클릭합니다.

5. Cloud Volumes ONTAP 과 스토리지 계정 간의 개인 링크 연결을 선택 해제합니다.

6. *저장*을 클릭하세요.

당신이 완료한 후

Azure Private Links를 비활성화하고 콘솔 에이전트가 프록시 서버를 사용하는 경우 직접 API 트래픽을 활성화해야 합니다.

["콘솔 에이전트에서 직접 API 트래픽을 활성화하는 방법을 알아보세요."](#)

Azure Private Links로 작업

대부분의 경우 Cloud Volumes ONTAP 사용하여 Azure Private Link를 설정하는 데 필요한 작업은 없습니다. 콘솔은 Azure Private Links를 관리합니다. 하지만 기존 Azure Private DNS 영역을 사용하는 경우 구성 파일을 편집해야 합니다.

사용자 정의 DNS에 대한 요구 사항

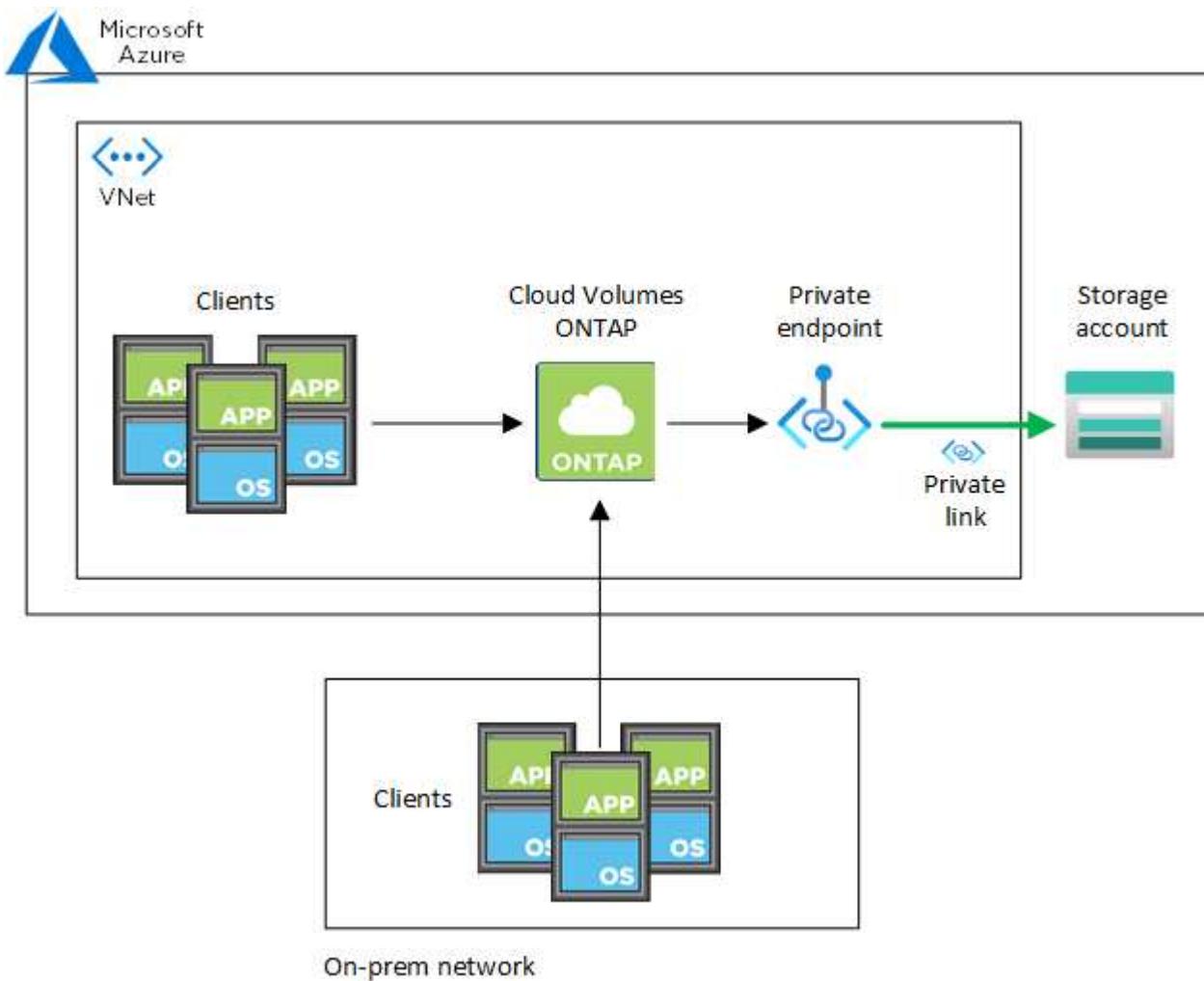
선택적으로 사용자 지정 DNS를 사용하는 경우 사용자 지정 DNS 서버에서 Azure 개인 DNS 영역에 대한 조건부 전달자를 만들어야 합니다. 자세한 내용은 다음을 참조하세요. ["DNS 전달자 사용에 대한 Azure 설명서"](#).

Private Link 연결 작동 방식

콘솔이 Azure에 Cloud Volumes ONTAP 배포하면 리소스 그룹에 개인 엔드포인트가 생성됩니다. 개인 엔드포인트는 Cloud Volumes ONTAP 의 스토리지 계정과 연결됩니다. 결과적으로 Cloud Volumes ONTAP 스토리지에 대한 액세스는 Microsoft 백본 네트워크를 통해 이루어집니다.

클라이언트가 Cloud Volumes ONTAP 과 동일한 VNet에 있거나, 피어링된 VNet에 있거나, VNet에 대한 개인 VPN이나 ExpressRoute 연결을 사용할 때 온프레미스 네트워크에 있는 경우 클라이언트 액세스는 개인 링크를 통해 이루어집니다.

다음은 동일한 VNet 내부와 개인 VPN 또는 ExpressRoute 연결이 있는 온프레미스 네트워크에서 개인 링크를 통해 클라이언트 액세스를 보여주는 예입니다.



콘솔 에이전트와 Cloud Volumes ONTAP 시스템이 서로 다른 VNet에 배포된 경우 콘솔 에이전트가 배포된 VNet과 Cloud Volumes ONTAP 시스템이 배포된 VNet 간에 VNet 피어링을 설정해야 합니다.

Azure Private DNS에 대한 세부 정보를 제공하세요.

당신이 사용하는 경우 ["Azure 프라이빗 DNS"](#) 그러면 각 콘솔 에이전트에서 구성 파일을 수정해야 합니다. 그렇지 않으면 콘솔은 Cloud Volumes ONTAP 과 연결된 스토리지 계정 간에 Azure Private Link 연결을 설정할 수 없습니다.

DNS 이름은 Azure DNS 명명 요구 사항과 일치해야 합니다. ["Azure 설명서에 표시된 대로"](#).

단계

1. 콘솔 에이전트 호스트에 SSH를 실행하고 로그인합니다.
2. 로 이동합니다 /opt/application/netapp/cloudmanager/docker_occm/data 예배 규칙서.
3. 편집하다 app.conf 추가하여 user-private-dns-zone-settings 다음 키워드-값 쌍을 포함하는 매개변수:

```

"user-private-dns-zone-settings" : {
    "resource-group" : "<resource group name of the DNS zone>",
    "subscription" : "<subscription ID>",
    "use-existing" : true,
    "create-private-dns-zone-link" : true
}

```

그만큼 `subscription` 키워드는 개인 DNS 영역이 콘솔 에이전트와 다른 구독에 있는 경우에만 필요합니다.

- 파일을 저장하고 콘솔 에이전트에서 로그오프합니다.

재부팅이 필요하지 않습니다.

실패 시 롤백 활성화

콘솔이 특정 작업의 일부로 Azure Private Link를 만들지 못하면 Azure Private Link 연결 없이 작업을 완료합니다. 이는 새로운 시스템(단일 노드 또는 HA 쌍)을 생성할 때 또는 HA 쌍에서 다음 작업이 발생할 때 발생할 수 있습니다. 새로운 집계 생성, 기존 집계에 디스크 추가 또는 32TiB를 초과할 때 새로운 스토리지 계정 생성.

콘솔에서 Azure Private Link를 만들지 못하는 경우 롤백을 활성화하여 이 기본 동작을 변경할 수 있습니다. 이를 통해 회사의 보안 규정을 완벽하게 준수하는 데 도움이 될 수 있습니다.

롤백을 활성화하면 콘솔에서 작업이 중지되고 작업의 일부로 생성된 모든 리소스가 롤백됩니다.

API를 통해 롤백을 활성화하거나 `app.conf` 파일을 업데이트할 수 있습니다.

API를 통한 롤백 활성화

단계

- 사용하다 `PUT /occm/config` 다음 요청 본문을 포함하는 API 호출:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

`app.conf`를 업데이트하여 롤백을 활성화합니다

단계

- 콘솔 에이전트 호스트에 SSH를 실행하고 로그인합니다.
- 다음 디렉토리로 이동합니다: `/opt/application/netapp/cloudmanager/docker_occm/data`
- 다음 매개변수와 값을 추가하여 `app.conf`를 편집합니다.

```
"rollback-on-private-link-failure": true
. 파일을 저장하고 콘솔 에이전트에서 로그오프합니다.
```

재부팅이 필요하지 않습니다.

Azure 콘솔에서 Cloud Volumes ONTAP 대한 Azure 리소스 그룹 이동

Cloud Volumes ONTAP Azure 리소스 그룹 이동을 지원하지만 워크플로는 Azure 콘솔에서만 발생합니다.

동일한 Azure 구독 내에서 Azure의 한 리소스 그룹에서 다른 리소스 그룹으로 Cloud Volumes ONTAP 시스템을 이동할 수 있습니다. 서로 다른 Azure 구독 간에 리소스 그룹을 이동하는 것은 지원되지 않습니다.

단계

1. Cloud Volumes ONTAP 시스템을 제거합니다. ["Cloud Volumes ONTAP 시스템 제거"](#).
2. Azure 콘솔에서 리소스 그룹 이동을 실행합니다.

이동을 완료하려면 다음을 참조하세요. ["Microsoft Azure 설명서에서 리소스를 새 리소스 그룹 또는 구독으로 이동"](#)

3. 시스템 페이지에서 시스템을 알아보세요.
4. 시스템 정보에서 새로운 리소스 그룹을 찾으세요.

결과

시스템과 해당 리소스(VM, 디스크, 스토리지 계정, 네트워크 인터페이스, 스냅샷)는 새 리소스 그룹에 있습니다.

Azure에서 SnapMirror 트래픽 분리

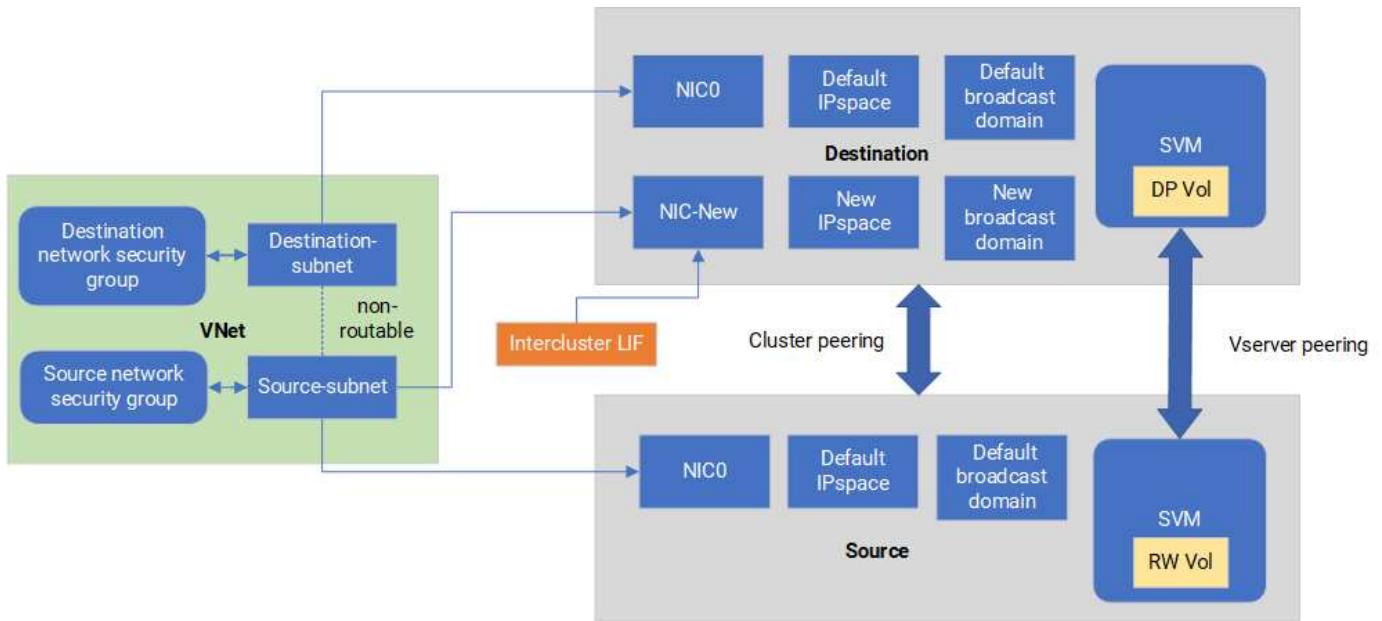
Azure의 Cloud Volumes ONTAP 사용하면 SnapMirror 복제 트래픽을 데이터 및 관리 트래픽에서 분리할 수 있습니다. SnapMirror 복제 트래픽을 데이터 트래픽에서 분리하려면 새 네트워크 인터페이스 카드(NIC), 연관된 클러스터 간 LIF 및 라우팅이 불가능한 서브넷을 추가합니다.

Azure의 SnapMirror 트래픽 분리에 관하여

기본적으로 NetApp Console 동일한 서브넷의 Cloud Volumes ONTAP 배포에 있는 모든 NIC와 LIF를 구성합니다. 이러한 구성에서는 SnapMirror 복제 트래픽과 데이터 및 관리 트래픽이 동일한 서브넷을 사용합니다. SnapMirror 트래픽을 분리하면 데이터 및 관리 트래픽에 사용되는 기존 서브넷으로 라우팅할 수 없는 추가 서브넷을 활용할 수 있습니다.

그림 1

다음 다이어그램은 단일 노드 배포에서 추가 NIC, 연관된 클러스터 간 LIF 및 라우팅 불가능한 서브넷을 사용하여 SnapMirror 복제 트래픽을 분리하는 방식을 보여줍니다. HA 쌍 배포는 약간 다릅니다.



시작하기 전에

다음 고려 사항을 검토하세요.

- SnapMirror 트래픽 분리를 위해 Cloud Volumes ONTAP 단일 노드 또는 HA 쌍 배포(VM 인스턴스)에 단일 NIC만 추가할 수 있습니다.
- 새로운 NIC를 추가하려면 배포하는 VM 인스턴스 유형에 사용되지 않는 NIC가 있어야 합니다.
- 소스 및 대상 클러스터는 동일한 가상 네트워크(VNet)에 액세스할 수 있어야 합니다. 대상 클러스터는 Azure의 Cloud Volumes ONTAP 시스템입니다. 소스 클러스터는 Azure의 Cloud Volumes ONTAP 시스템이나 ONTAP 시스템이 될 수 있습니다.

1단계: 추가 NIC를 생성하고 대상 VM에 연결합니다.

이 섹션에서는 추가 NIC를 생성하고 대상 VM에 연결하는 방법에 대한 지침을 제공합니다. 대상 VM은 Azure의 Cloud Volumes ONTAP에 있는 단일 노드 또는 HA 쌍 시스템으로, 여기에 추가 NIC를 설정하려는 것입니다.

단계

1. ONTAP CLI에서 노드를 중지합니다.

```
dest::: > halt -node <dest_node-vm>
```

2. Azure Portal에서 VM(노드) 상태가 중지되었는지 확인하세요.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Azure Cloud Shell의 Bash 환경을 사용하여 노드를 중지합니다.

a. 노드를 중지합니다.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. 노드의 할당을 해제합니다.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. 두 서브넷(소스 클러스터 서브넷과 대상 클러스터 서브넷)이 서로 라우팅되지 않도록 네트워크 보안 그룹 규칙을 구성합니다.

a. 대상 VM에 새 NIC를 만듭니다.

b. 소스 클러스터 서브넷의 서브넷 ID를 찾습니다.

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet-name <vnet> --query id
```

c. 소스 클러스터 서브넷의 서브넷 ID를 사용하여 대상 VM에 새 NIC를 만듭니다. 여기에 새 NIC의 이름을 입력합니다.

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

d. 개인IP주소를 저장합니다. 이 IP 주소 <new_added_nic_primary_addr>는 클러스터 간 LIF를 생성하는 데 사용됩니다.[브로드캐스트 도메인, 새 NIC에 대한 클러스터 간 LIF](#).

5. 새 NIC를 VM에 연결합니다.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. VM(노드)을 시작합니다.

```
az vm start --resource-group <dest_node-rg> --name <dest_node-vm>
```

7. Azure Portal에서 *네트워킹*으로 이동하여 새 NIC(예: nic-new)가 있는지, 가속 네트워킹이 활성화되어 있는지 확인합니다.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

HA 쌍 배포의 경우 파트너 노드에 대해 단계를 반복합니다.

2단계: 새 NIC에 대한 새 IP 공간, 브로드캐스트 도메인 및 클러스터 간 LIF 만들기

클러스터 간 LIF를 위한 별도의 IP 공간은 클러스터 간 복제를 위한 네트워킹 기능 간의 논리적 분리를 제공합니다.

다음 단계에서는 ONTAP CLI를 사용하세요.

단계

1. 새로운 IPspace(new_ipspace)를 생성합니다.

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. 새로운 IPspace(new_ipspace)에 브로드캐스트 도메인을 만들고 nic-new 포트를 추가합니다.

```
dest::> network port show
```

3. 단일 노드 시스템의 경우 새로 추가된 포트는 _e0b_입니다. 관리형 디스크를 사용한 HA 쌍 배포의 경우 새로 추가된 포트는 _e0d_입니다. 페이지 블롭이 있는 HA 쌍 배포의 경우 새로 추가된 포트는 _e0e_입니다. VM 이름이 아닌 노드 이름을 사용하세요. 다음을 실행하여 노드 이름을 찾으세요. node show .

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500  
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. 새로운 브로드캐스트 도메인(new_bd)과 새로운 NIC(nic-new)에 클러스터 간 LIF를 만듭니다.

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-lif> -service-policy default-intercluster -address  
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask  
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. 새로운 클러스터 간 LIF 생성을 확인합니다.

```
dest::> net int show
```

HA 쌍 배포의 경우 파트너 노드에 대해 단계를 반복합니다.

3단계: 소스 시스템과 대상 시스템 간 클러스터 피어링 확인

이 섹션에서는 소스 시스템과 대상 시스템 간의 피어링을 확인하는 방법에 대한 지침을 제공합니다.

다음 단계에서는 ONTAP CLI를 사용하세요.

단계

1. 대상 클러스터의 클러스터 간 LIF가 소스 클러스터의 클러스터 간 LIF를 ping할 수 있는지 확인합니다. 대상 클러스터가 이 명령을 실행하므로 대상 IP 주소는 소스의 클러스터 간 LIF IP 주소입니다.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>  
-destination <10.161.189.6>
```

2. 소스 클러스터의 클러스터 간 LIF가 대상 클러스터의 클러스터 간 LIF를 ping할 수 있는지 확인합니다. 목적지는 목적지에 생성된 새로운 NIC의 IP 주소입니다.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination  
<10.161.189.18>
```

HA 쌍 배포의 경우 파트너 노드에 대해 단계를 반복합니다.

4단계: 소스 시스템과 대상 시스템 간 **SVM** 피어링 생성

이 섹션에서는 소스 시스템과 대상 시스템 간에 SVM 피어링을 생성하는 방법에 대한 지침을 제공합니다.

다음 단계에서는 ONTAP CLI를 사용하세요.

단계

1. 소스 클러스터 간 LIF IP 주소를 사용하여 대상에서 클러스터 피어링을 생성합니다. `-peer-addrs`. HA 쌍의 경우 두 노드의 소스 클러스터 간 LIF IP 주소를 다음과 같이 나열합니다. `-peer-addrs`.

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace  
<new_ipspace>
```

2. 암호를 입력하고 확인하세요.
3. 대상 클러스터 LIF IP 주소를 사용하여 소스에서 클러스터 피어링을 생성합니다. `peer-addrs`. HA 쌍의 경우 두 노드 모두에 대한 대상 클러스터 간 LIF IP 주소를 다음과 같이 나열합니다. `-peer-addrs`.

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. 암호를 입력하고 확인하세요.
5. 클러스터가 피어링되었는지 확인하세요.

```
src::> cluster peer show
```

피어링이 성공하면 가용성 필드에 *사용 가능*이 표시됩니다.

6. 목적지에 SVM 피어링을 생성합니다. 소스 SVM과 대상 SVM은 모두 데이터 SVM이어야 합니다.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. SVM 피어링을 허용합니다.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. SVM이 피어링되었는지 확인하세요.

```
dest::> vserver peer show
```

피어 스테이트 쇼*peered* 및 피어링 애플리케이션이 표시됩니다.*snapmirror*.

5단계: 소스 시스템과 대상 시스템 간에 **SnapMirror** 복제 관계 생성

이 섹션에서는 소스 시스템과 대상 시스템 간에 SnapMirror 복제 관계를 만드는 방법에 대한 지침을 제공합니다.

기존 SnapMirror 복제 관계를 이동하려면 새 SnapMirror 복제 관계를 만들기 전에 먼저 기존 SnapMirror 복제 관계를 해제해야 합니다.

다음 단계에서는 ONTAP CLI를 사용하세요.

단계

1. 대상 SVM에 데이터 보호 볼륨을 만듭니다.

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. SnapMirror 정책과 복제 일정을 포함하는 대상에 SnapMirror 복제 관계를 만듭니다.

```
dest::> snapmirror create -source-path src_svm:src_vol -destination
-path dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. 대상에서 SnapMirror 복제 관계를 초기화합니다.

```
dest::> snapmirror initialize -destination-path <dest_svm:new_dest_vol>
```

4. ONTAP CLI에서 다음 명령을 실행하여 SnapMirror 관계 상태를 확인합니다.

```
dest::> snapmirror show
```

관계 상태는 다음과 같습니다. Snapmirrored 그리고 관계의 건강은 true .

5. 선택 사항: ONTAP CLI에서 다음 명령을 실행하여 SnapMirror 관계에 대한 작업 기록을 확인합니다.

```
dest::> snapmirror show-history
```

선택적으로 소스 및 대상 볼륨을 마운트하고, 소스에 파일을 쓰고, 볼륨이 대상에 복제되는지 확인할 수 있습니다.

Google Cloud 관리

Cloud Volumes ONTAP에 대한 Google Cloud 머신 유형 변경

Google Cloud에서 Cloud Volumes ONTAP 실행하면 여러 가지 머신 유형 중에서 선택할 수 있습니다. 필요에 따라 인스턴스나 머신 유형이 너무 크거나 작다고 판단되면 언제든지 변경할 수 있습니다.

이 작업에 관하여

- Cloud Volumes ONTAP HA 쌍에서 자동 반환 기능을 활성화해야 합니다(이는 기본 설정입니다). 그렇지 않으면 작업이 실패합니다.

"ONTAP 9 설명서: 자동 반환 구성을 위한 명령"

- 머신 유형을 변경하면 Google Cloud 서비스 요금에 영향을 미칠 수 있습니다.
- 이 작업은 Cloud Volumes ONTAP 다시 시작합니다.

단일 노드 시스템의 경우 I/O가 중단됩니다.

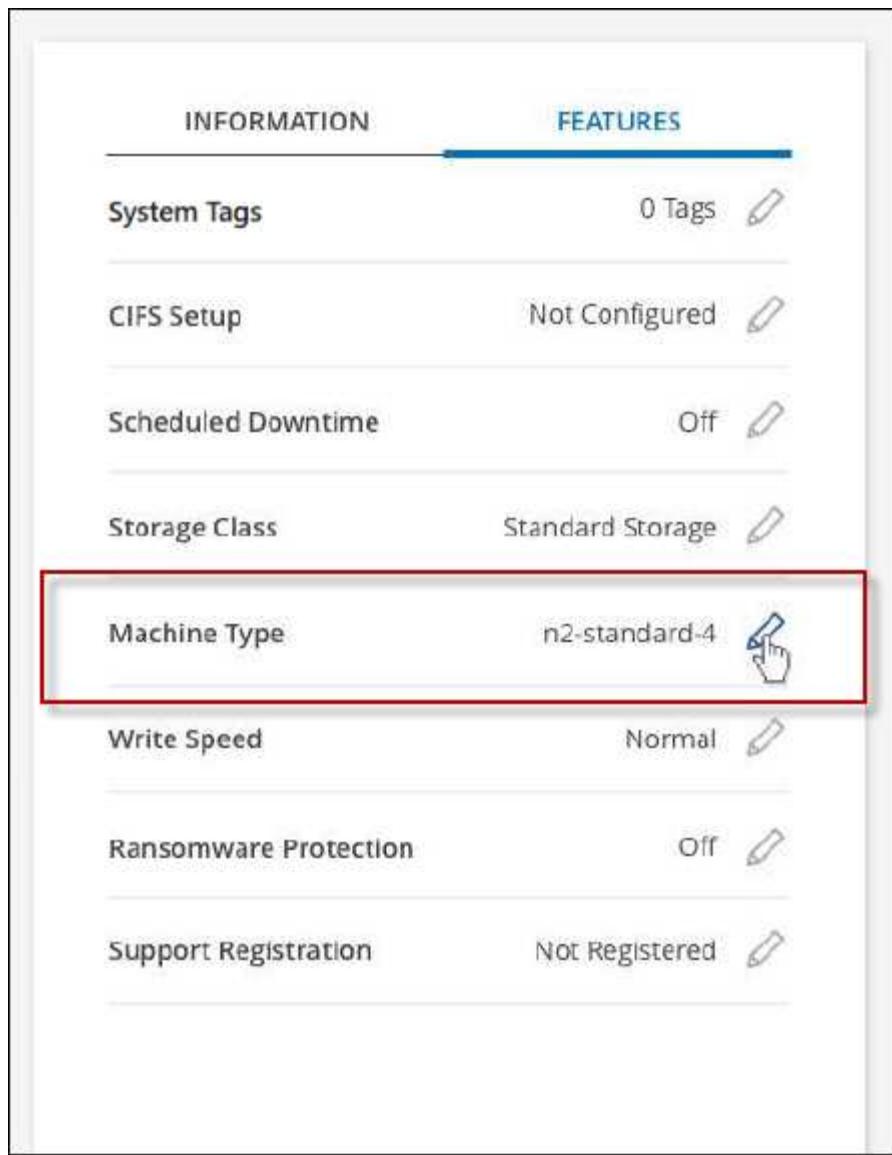
HA 쌍의 경우 변경은 중단되지 않습니다. HA 쌍은 계속해서 데이터를 제공합니다.



NetApp Console 인수를 시작하고 반환을 기다리는 방식으로 한 번에 한 노드씩 변경합니다. NetApp의 품질 보증 팀은 이 프로세스 동안 파일 쓰기와 읽기를 모두 테스트했으며 클라이언트에서 아무런 문제도 발견하지 못했습니다. 연결이 변경됨에 따라 I/O 수준에서 일부 재시도가 관찰되었지만 애플리케이션 계층은 NFS/CIFS 연결의 재배선을 극복했습니다.

단계

- 시스템 페이지에서 시스템을 선택하세요.
- 개요 탭에서 기능 패널을 클릭한 다음 머신 유형 옆에 있는 연필 아이콘을 클릭합니다.



노드 기반 사용량 기반(PAYGO) 라이선스를 사용하는 경우, 라이선스 유형 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스와 머신 유형을 선택할 수 있습니다.

1. 머신 유형을 선택하고, 변경 사항의 의미를 이해했음을 확인하는 확인란을 선택한 다음 *변경*을 클릭합니다.

결과

Cloud Volumes ONTAP 새로운 구성으로 재부팅됩니다.

System Manager를 사용하여 Cloud Volumes ONTAP 관리

Cloud Volumes ONTAP의 고급 스토리지 관리 기능은 ONTAP 시스템과 함께 제공되는 관리 인터페이스인 ONTAP System Manager를 통해 제공됩니다. NetApp Console에서 직접 System Manager에 액세스할 수 있습니다.

특징

콘솔에서 ONTAP 시스템 관리자를 사용하여 다양한 스토리지 관리 기능을 수행할 수 있습니다. 다음 목록에는 일부 기능이 포함되어 있지만, 전체 목록은 아닙니다.

- 고급 스토리지 관리: 일관성 그룹, 공유, Q트리, 할당량 및 스토리지 VM을 관리합니다.
- 볼륨 이동: "볼륨을 다른 집계로 이동합니다."
- 네트워킹 관리: IP 공간, 네트워크 인터페이스, 포트셋, 이더넷 포트를 관리합니다.
- FlexGroup 볼륨 관리: FlexGroup 볼륨은 System Manager를 통해서만 생성하고 관리할 수 있습니다. 콘솔은 FlexGroup 볼륨 생성을 지원하지 않습니다.
- 이벤트 및 작업: 이벤트 로그, 시스템 알림, 작업 및 감사 로그를 확인합니다.
- 고급 데이터 보호: 스토리지 VM, LUN 및 일관성 그룹을 보호합니다.
- 호스트 관리: SAN 이니시에이터 그룹과 NFS 클라이언트를 설정합니다.
- S3 개체 스토리지 관리: Cloud Volumes ONTAP의 S3 스토리지 관리 기능은 System Manager에서만 사용할 수 있으며 Console에서는 사용할 수 없습니다.

지원되는 구성

- ONTAP System Manager를 통한 고급 스토리지 관리 기능은 표준 클라우드 지역에서 Cloud Volumes ONTAP 9.10.0 이상에서 사용할 수 있습니다.
- GovCloud 지역이나 아웃바운드 인터넷 액세스가 없는 지역에서는 System Manager 통합이 지원되지 않습니다.

제한 사항

System Manager 인터페이스에 나타나는 몇 가지 기능은 Cloud Volumes ONTAP에서 지원되지 않습니다.

- NetApp Cloud Tiering: Cloud Volumes ONTAP 클라우드 계층화를 지원하지 않습니다. 볼륨을 생성할 때 표준 보기에서 직접 개체 스토리지에 대한 데이터 계층화를 설정해야 합니다.
- 계층: System Manager에서는 집계 관리(로컬 계층 및 클라우드 계층 포함)가 지원되지 않습니다. 표준 보기에서 직접 집계를 관리해야 합니다.
- 펌웨어 업그레이드: Cloud Volumes ONTAP 시스템 관리자의 클러스터 > 설정 페이지에서 자동 펌웨어 업데이트를 지원하지 않습니다.
- 역할 기반 액세스 제어: System Manager의 역할 기반 액세스 제어는 지원되지 않습니다.
- SMB 지속적 가용성(CA): Cloud Volumes ONTAP 지원하지 않습니다. "지속적으로 이용 가능한 SMB 주식" 중단 없는 운영을 위해.

시스템 관리자에 액세스하기 위한 인증 구성

관리자는 콘솔에서 ONTAP System Manager에 액세스하는 사용자에 대한 인증을 활성화할 수 있습니다. ONTAP 사용자 역할에 따라 적절한 수준의 액세스 권한을 결정하고 필요에 따라 인증을 활성화하거나 비활성화할 수 있습니다. 인증을 활성화하면 사용자는 콘솔에서 System Manager에 액세스할 때마다 또는 페이지를 다시 로드할 때마다 ONTAP 사용자 자격 증명을 입력해야 합니다. 콘솔은 자격 증명을 내부적으로 저장하지 않기 때문입니다. 인증을 비활성화하면 사용자는 관리자 자격 증명을 사용하여 시스템 관리자에 액세스할 수 있습니다.



이 설정은 Cloud Volumes ONTAP 시스템과 관계없이 조직 또는 계정의 ONTAP 사용자에 대한 각 콘솔 에이전트에 적용됩니다.

필요한 권한

Cloud Volumes ONTAP 사용자 인증을 위한 콘솔 에이전트 설정을 수정하려면 조직 또는 계정 관리자 권한이 지정되어야 합니다.

단계

1. 원쪽 탐색 창에서 *관리 > 에이전트*로 이동합니다.
2. 클릭 *** 필요한 콘솔 에이전트의 아이콘을 클릭하고 *콘솔 에이전트 편집*을 선택합니다.
3. 사용자 자격 증명 강제 적용*에서 *활성화/비활성화 확인란을 선택합니다. 기본적으로 인증은 비활성화되어 있습니다.



이 값을 *사용*으로 설정하면 인증이 재설정되고 이 변경 사항을 수용하기 위해 기존 워크플로를 수정해야 합니다.

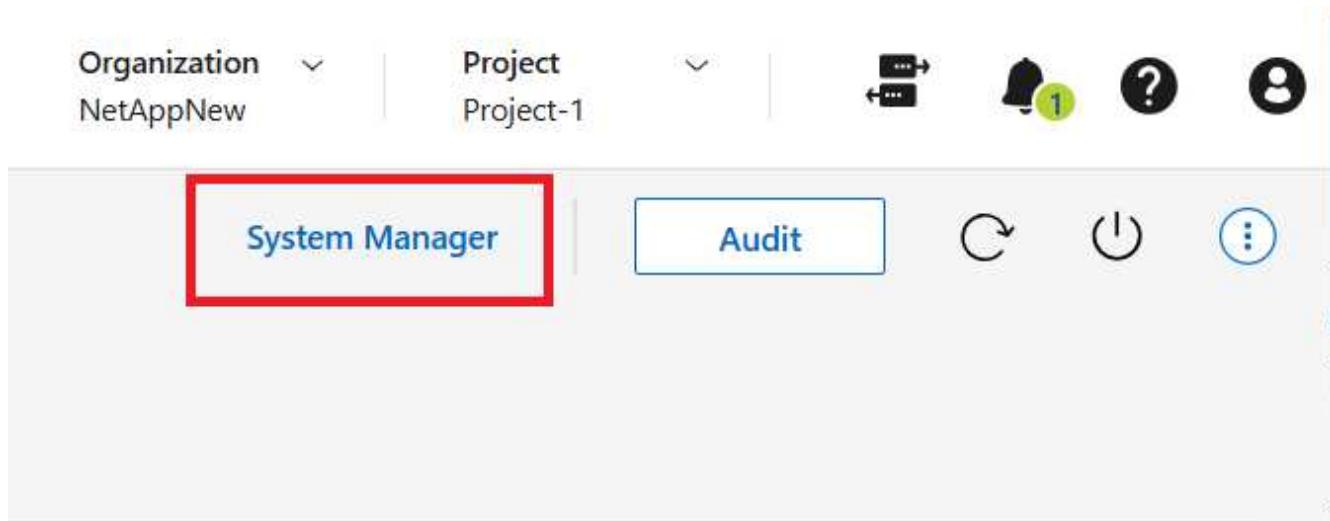
4. *저장*을 클릭하세요.

시스템 관리자 시작하기

Cloud Volumes ONTAP 시스템에서 ONTAP System Manager에 액세스할 수 있습니다.

단계

1. 원쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 필요한 Cloud Volumes ONTAP 시스템을 두 번 클릭합니다.
3. *시스템 관리자*를 클릭하세요.



4. 메시지가 표시되면 ONTAP 사용자 자격 증명을 입력하고 *로그인*을 클릭합니다.
5. 확인 메시지가 나타나면, 내용을 읽고 *닫기*를 클릭하세요.

System Manager를 사용하여 Cloud Volumes ONTAP 시스템을 관리하세요. *돌아가기*를 클릭하면 콘솔로 돌아갈 수 있습니다.

시스템 관리자 사용에 대한 도움말

Cloud Volumes ONTAP 과 함께 System Manager를 사용하는 데 도움이 필요한 경우 다음을 참조할 수 있습니다. ["ONTAP 문서"](#) 단계별 지침을 확인하세요. 도움이 될 만한 몇 가지 ONTAP 문서 링크는 다음과 같습니다.

- ["ONTAP 역할, 애플리케이션 및 인증"](#)

- "시스템 관리자를 사용하여 클러스터에 액세스합니다." .
- "볼륨 및 LUN 관리"
- "네트워크 관리"
- "데이터 보호"
- "지속적으로 사용 가능한 SMB 공유 생성"

CLI에서 Cloud Volumes ONTAP 관리

Cloud Volumes ONTAP CLI를 사용하면 모든 관리 명령을 실행할 수 있으며 고급 작업을 수행하거나 CLI를 사용하는 것이 더 편리한 경우에 좋은 선택입니다. SSH(Secure Shell)를 사용하여 CLI에 연결할 수 있습니다.

시작하기 전에

SSH를 사용하여 Cloud Volumes ONTAP에 연결하는 호스트에는 Cloud Volumes ONTAP에 대한 네트워크 연결이 있어야 합니다. 예를 들어, 클라우드 공급자 네트워크에 있는 점프 호스트에서 SSH를 수행해야 할 수도 있습니다.



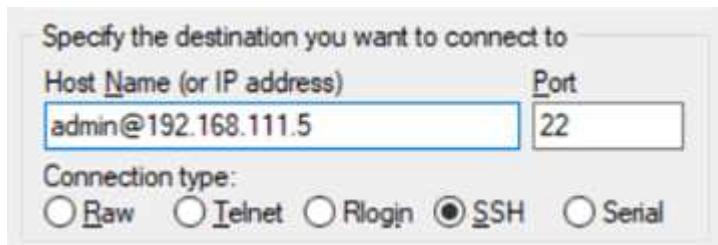
여러 AZ에 배포하는 경우 Cloud Volumes ONTAP HA 구성은 클러스터 관리 인터페이스에 부동 IP 주소를 사용하므로 외부 라우팅을 사용할 수 없습니다. 동일한 라우팅 도메인에 속한 호스트에서 연결해야 합니다.

단계

1. NetApp Console에서 클러스터 관리 인터페이스의 IP 주소를 식별합니다.
 - a. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
 - b. 시스템 페이지에서 Cloud Volumes ONTAP 시스템을 선택합니다.
 - c. 오른쪽 창에 나타나는 클러스터 관리 IP 주소를 복사합니다.
2. 관리자 계정을 사용하여 SSH를 사용하여 클러스터 관리 인터페이스 IP 주소에 연결합니다.

예

다음 이미지는 PuTTY를 사용하는 예를 보여줍니다.



3. 로그인 프롬프트에서 관리자 계정의 비밀번호를 입력하세요.

예

Password: *****

COT2::>

시스템 상태 및 이벤트

Cloud Volumes ONTAP에 대한 AutoSupport 설정 확인

AutoSupport 시스템 상태를 사전에 모니터링하고 NetApp 기술 지원팀에 메시지를 전송합니다. 기본적으로 AutoSupport 각 노드에서 HTTPS 전송 프로토콜을 사용하여 기술 지원팀에 메시지를 보낼 수 있도록 활성화되어 있습니다. AutoSupport 이러한 메시지를 보낼 수 있는지 확인하는 것이 가장 좋습니다.

유일하게 필요한 구성 단계는 Cloud Volumes ONTAP 아웃바운드 인터넷 연결이 있는지 확인하는 것입니다. 자세한 내용은 클라우드 제공업체의 네트워킹 요구 사항을 참조하세요.

AutoSupport 요구 사항

Cloud Volumes ONTAP 노드에는 NetApp AutoSupport에 대한 아웃바운드 인터넷 액세스가 필요합니다. NetApp AutoSupport는 시스템 상태를 사전에 모니터링하고 NetApp 기술 지원팀에 메시지를 전송합니다.

라우팅 및 방화벽 정책은 Cloud Volumes ONTAP AutoSupport 메시지를 보낼 수 있도록 다음 엔드포인트에 대한 HTTPS 트래픽을 허용해야 합니다.

- \ <https://mysupport.netapp.com/aods/asupmessage>
- \ <https://mysupport.netapp.com/asupprod/post/1.0/postAsup>

AutoSupport 메시지를 보내기 위한 아웃바운드 인터넷 연결이 불가능한 경우 NetApp Console Cloud Volumes ONTAP 시스템이 콘솔 에이전트를 프록시 서버로 사용하도록 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

Cloud Volumes ONTAP에 대해 엄격한 아웃바운드 규칙을 정의한 경우 Cloud Volumes ONTAP 보안 그룹이 포트 3128을 통한 아웃바운드 연결을 허용하는지 확인해야 합니다.



HA 쌍을 사용하는 경우 HA 중재자는 아웃바운드 인터넷 액세스가 필요하지 않습니다.

아웃바운드 인터넷 접속이 가능한지 확인한 후 AutoSupport 메시지를 보낼 수 있는지 테스트할 수 있습니다. 지침은 다음을 참조하세요. ["ONTAP 설명서: AutoSupport 설정"](#).

AutoSupport 구성 문제 해결

외부 연결이 불가능하고 콘솔에서 Cloud Volumes ONTAP 시스템을 콘솔 에이전트를 프록시 서버로 사용하도록 구성할 수 없는 경우, 시스템에서 AutoSupport 메시지를 보낼 수 없다는 알림이 콘솔에서 표시됩니다. 이 문제를 해결하려면 다음 단계를 따르십시오.

단계

1. ONTAP CLI를 사용하려면 SSH를 사용하여 Cloud Volumes ONTAP 시스템에 안전하게 연결하십시오.

"Cloud Volumes ONTAP 에 SSH하는 방법 알아보기" .

2. AutoSupport 하위 시스템의 자세한 상태를 확인하십시오.

```
autosupport check show-details
```

응답은 다음과 같습니다.

```
Category: smtp
  Component: mail-server
  Status: failed
  Detail: SMTP connectivity check failed for destination:
          mailhost. Error: Could not resolve host -
'mailhost'

  Corrective Action: Check the hostname of the SMTP server

Category: http-https
  Component: http-put-destination
  Status: ok
  Detail: Successfully connected to:
          <https://support.netapp.com/put/AsupPut/>.

  Component: http-post-destination
  Status: ok
  Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

Category: on-demand
  Component: ondemand-server
  Status: ok
  Detail: Successfully connected to:
          https://support.netapp.com/aods/asupmessage.

Category: configuration
  Component: configuration
  Status: ok
  Detail: No configuration issues found.

5 entries were displayed.
```

http-https 카테고리의 상태가 다음과 같으면 OK 이는 AutoSupport 제대로 구성되어 메시지를 보낼 수 있음을 의미합니다.

3. 그렇지 않다면 각 Cloud Volumes ONTAP 노드의 프록시 URL을 확인하십시오.

```
autosupport show -fields proxy-url
```

4. 프록시 URL 매개변수가 비어 있으면 Cloud Volumes ONTAP 구성하여 콘솔 에이전트를 프록시로 사용합니다.

```
autosupport modify -proxy-url http://<console agent private ip>:3128
```

5. AutoSupport 상태를 다시 확인하십시오.

```
autosupport check show-details
```

6. 상태가 여전히 실패로 표시되는 경우, Cloud Volumes ONTAP 과 콘솔 에이전트 간에 포트를 통해 연결이 제대로 되어 있는지 확인하십시오. 3128.

7. 확인 후에도 상태가 여전히 실패로 표시되면 콘솔 에이전트에 SSH로 접속하십시오.

["콘솔 에이전트를 위한 Linux VM 연결에 대해 자세히 알아보세요."](#)

8. 가다 /opt/application/netapp/cloudmanager/docker_occm/data/.

9. 프록시 구성 파일을 엽니다. squid.conf. 파일의 구조는 다음과 같습니다.

```
http_port 3128
acl netapp_support dst support.netapp.com
http_access allow netapp_support
request_header_max_size 21 KB
reply_header_max_size 21 KB
http_access deny all
httpd_suppress_version_string on
```

10. 파일에 Cloud Volumes ONTAP 시스템의 CIDR 블록에 대한 항목이 없는 경우 새 항목을 추가하고 액세스를 허용하십시오.

```
acl cvonet src <cidr>
http_access allow cvonet
```

예를 들면 다음과 같습니다.

```
http_port 3128
acl netapp_support dst support.netapp.com
acl cvonet src <cidr>
http_access allow netapp_support
http_access allow cvonet
request_header_max_size 21 KB
reply_header_max_size 21 KB
http_access deny all
httpd_suppress_version_string on
```

11. 설정 파일을 편집한 후 프록시 컨테이너를 다시 시작하십시오. sudo. 그런 다음 Docker 또는 Podman을 사용하는지에 따라 다음 명령을 실행하세요.

Docker의 경우, 다음 명령을 실행하세요. `docker restart squid`.

Podman을 사용 중이라면 다음 명령을 실행하세요. `podman restart squid`.

12. ONTAP CLI로 돌아가서 Cloud Volumes ONTAP AutoSupport 메시지를 보낼 수 있는지 확인하십시오.

```
autosupport check show-details
```

관련 링크

- "[AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구 사항](#)"
- "[Azure에서 Cloud Volumes ONTAP의 네트워킹 요구 사항](#)"
- "[Google Cloud에서 Cloud Volumes ONTAP 사용하기 위한 네트워킹 요구 사항](#)"

Cloud Volumes ONTAP 시스템에 대한 EMS 구성

이벤트 관리 시스템(EMS)은 ONTAP 시스템에서 발생하는 이벤트에 대한 정보를 수집하고 표시합니다. 이벤트 알림을 받으려면 특정 이벤트 심각도에 대한 이벤트 대상(이메일 주소, SNMP 트랩 호스트 또는 시스템 로그 서버)과 이벤트 경로를 설정할 수 있습니다.

CLI를 사용하여 EMS를 구성할 수 있습니다. 자침은 다음을 참조하세요. "[ONTAP 문서: EMS 구성 개요](#)".

저작권 정보

Copyright © 2025 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 그레픽, 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/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.