



# Cloud Volumes ONTAP를 사용합니다

## Cloud Volumes ONTAP

NetApp  
June 27, 2024

# 목차

Cloud Volumes ONTAP를 사용합니다 .....	1
라이선스 관리 .....	1
볼륨 및 LUN 관리 .....	15
통합 관리 .....	41
스토리지 VM 관리 .....	47
보안 및 데이터 암호화 .....	82
시스템 관리 .....	95
시스템 상태 및 이벤트입니다 .....	127

# Cloud Volumes ONTAP를 사용합니다

## 라이선스 관리

### 용량 기반 라이선스 관리

BlueXP 디지털 지갑에서 용량 기반 라이선스를 관리하여 NetApp 계정의 Cloud Volumes ONTAP 시스템 용량이 충분한지 확인합니다.

[\\_용량 기반 라이선스\\_](#) Cloud Volumes ONTAP/TiB 용량 비용을 지불할 수 있습니다.

BlueXP 디지털 지갑 [\\_을\(를\)](#) 사용하면 한 곳에서 Cloud Volumes ONTAP에 대한 라이선스를 관리할 수 있습니다. 새 라이선스를 추가하고 기존 라이선스를 업데이트할 수 있습니다.

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

### BlueXP 디지털 지갑에 라이선스를 추가하는 방법

NetApp 세일즈 담당자로부터 라이선스를 구입하면 일련 번호와 추가 라이선스 세부 정보가 포함된 이메일이 전송됩니다.

그 동안 BlueXP는 NetApp의 라이선스 서비스에 대해 자동으로 쿼리하여 NetApp Support 사이트 계정과 연결된 라이선스에 대한 자세한 정보를 확인합니다. 오류가 없으면 BlueXP는 자동으로 디지털 지갑에 라이선스를 추가합니다.

BlueXP에서 라이선스를 추가할 수 없는 경우 디지털 지갑에 직접 추가해야 합니다. 예를 들어, 인터넷에 액세스할 수 없는 위치에 Connector가 설치되어 있는 경우 라이선스를 직접 추가해야 합니다. [구입한 라이선스를 계정에 추가하는 방법에 대해 알아봅니다](#).

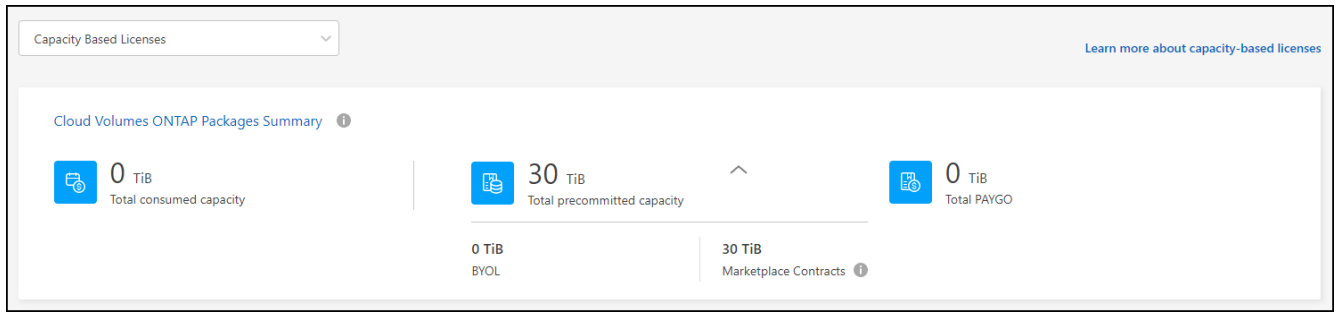
### 계정에서 사용된 용량을 확인합니다

BlueXP 디지털 지갑에는 계정의 총 소비된 용량과 라이선스 패키지를 통한 소비된 용량이 표시됩니다. 이를 통해 비용이 청구되는 방식 및 추가 용량을 구입해야 하는지 여부를 파악할 수 있습니다.

### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭에서 \* 용량 기반 라이선스 \* 를 선택한 상태로 유지합니다.
3. 사용된 용량, 사전 커밋된 총 용량 및 총 PAYGO 용량을 보여 주는 패키지 요약을 봅니다.
  - [\\_Total Consumed Capacity\\_](#) 는 NetApp 계정의 모든 Cloud Volumes ONTAP 시스템에 프로비저닝된 총 용량입니다. 충전은 볼륨 내의 로컬, 사용, 저장 또는 유효 공간에 관계없이 각 볼륨의 프로비저닝된 크기를 기준으로 합니다.
  - [\\_Total Prep커밋된 용량\\_](#) 은(는) NetApp에서 구매한 총 라이선스 용량(BYOL 또는 Marketplace 계약)입니다.
  - [\\_Total PAYGO\\_](#) 는 클라우드 마켓플레이스 서비스스크립션을 사용하여 프로비저닝된 총 용량입니다. PAYGO를 통한 충전은 사용된 용량이 BYOL 라이선스 용량보다 높거나 BlueXP 디지털 지갑에 사용 가능한 라이선스가 없는 경우에만 사용됩니다.

다음은 BlueXP 디지털 지갑의 Cloud Volumes ONTAP 패키지 요약의 예입니다.



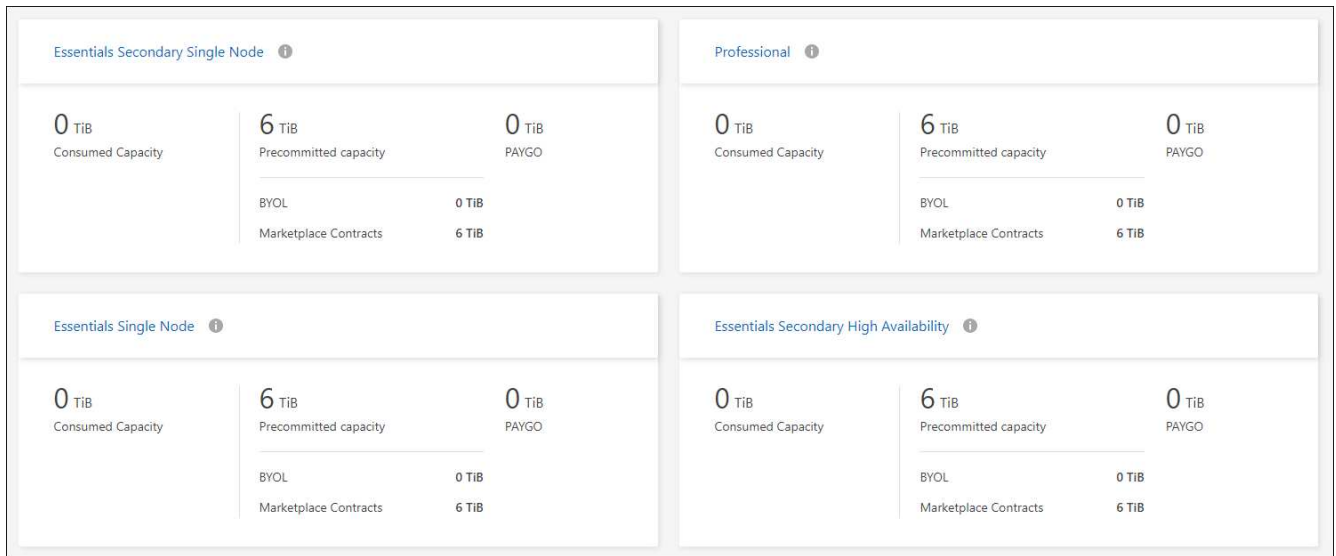
4. 요약에서 각 라이선스 패키지의 사용된 용량을 확인합니다.

- **\_Consumed capacity\_**는 해당 패키지의 볼륨 용량을 표시합니다. 특정 패키지에 대한 자세한 내용을 보려면 도구 설명 위로 마우스를 가져갑니다.

Essentials 패키지에 표시되는 용량을 더 잘 이해하려면 충전 작동 방식에 익숙해야 합니다. "[Essentials 패키지 충전 방법에 대해 알아봅니다](#)".

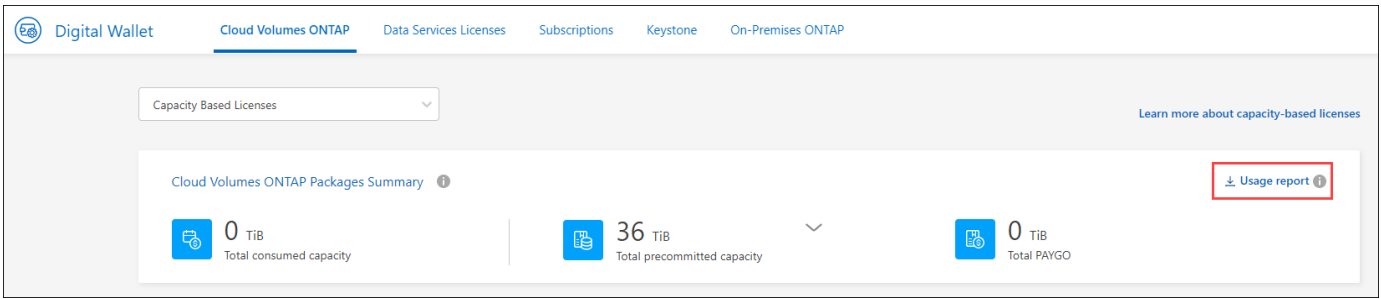
- **\_PreCommitted Capacity\_**는 NetApp에서 구매한 라이선스 용량(BYOL 또는 마켓플레이스 계약)입니다.
  - **\_BYOL\_**은 이 패키지 유형에 대해 NetApp에서 구입한 라이선스 용량을 보여 줍니다.
  - **Marketplace** 계약 은 이 패키지 유형에 대한 마켓플레이스 계약과 함께 구입한 라이선스 용량을 표시합니다.
- **\_PAYGO\_**는 라이선스 소비 모델에 따라 사용된 용량을 보여줍니다.

다음은 여러 라이선스 패키지가 있는 계정의 예입니다.



사용 보고서를 다운로드합니다

계정 관리자는 BlueXP의 디지털 지갑에서 네 가지 사용 보고서를 다운로드할 수 있습니다. 이러한 사용 보고서는 구독의 용량 세부 정보를 제공하고 Cloud Volumes ONTAP 구독에 포함된 리소스에 대한 비용 청구 방식을 알려줍니다. 다운로드할 수 있는 보고서는 특정 시점에 데이터를 캡처하여 다른 사람과 쉽게 공유할 수 있습니다.



다음 보고서를 다운로드할 수 있습니다. 표시된 용량 값은 TiB입니다.

- \* 고급 사용량\*: 이 보고서는 디지털 지갑의 “Cloud Volumes ONTAP 패키지 요약” 카드에 있는 내용을 정확하게 보여줍니다. 여기에는 다음 정보가 포함됩니다.
  - 사용된 총 용량입니다
  - 사전 커밋된 총 용량입니다
  - 총 BYOL 용량
  - 총 마켓플레이스 계약 용량입니다
  - 총 PAYGO 용량
- \* Cloud Volumes ONTAP 패키지 사용 \*: 이 보고서는 디지털 지갑의 패키지 카드에 있는 내용을 정확하게 보여줍니다. 최적화된 I/O 패키지를 제외한 각 패키지에 대한 다음 정보가 포함되어 있습니다.
  - 사용된 총 용량입니다
  - 사전 커밋된 총 용량입니다
  - 총 BYOL 용량
  - 총 마켓플레이스 계약 용량입니다
  - 총 PAYGO 용량
- \* 스토리지 VM 사용량 \*: 이 보고서는 Cloud Volumes ONTAP 시스템과 스토리지 가상 시스템(SVM)에서 청구 용량이 얼마나 분석되는지를 보여줍니다. 이 정보는 디지털 지갑의 화면에서는 사용할 수 없습니다. 여기에는 다음 정보가 포함됩니다.
  - 작업 환경 ID 및 이름(UUID로 표시됨)
  - 클라우드
  - NetApp 계정 ID입니다
  - 작업 환경 구성
  - SVM 이름
  - 용량을 프로비저닝합니다
  - 데이터 중복 제거 용량
  - 마켓플레이스 청구 기간
  - Cloud Volumes ONTAP 패키지 또는 기능
  - SaaS Marketplace 구독 이름 충전 중
  - SaaS Marketplace 구독 ID를 충전하는 중입니다

- 워크로드 유형
- \* Volumes usage \*: 이 보고서는 작업 환경의 볼륨에 의해 청구된 용량이 어떻게 분할되는지 보여줍니다. 이 정보는 디지털 지갑의 화면에서는 사용할 수 없습니다. 여기에는 다음 정보가 포함됩니다.
  - 작업 환경 ID 및 이름(UUID로 표시됨)
  - SVN 이름
  - 볼륨 ID입니다
  - 볼륨 유형입니다
  - 볼륨 프로비저닝 용량입니다



FlexClone 볼륨은 이러한 유형의 볼륨에 비용이 발생하지 않으므로 이 보고서에 포함되지 않습니다.

#### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭에서 \* Capacity Based Licenses \* 를 선택한 상태로 두고 \* Usage report \* 를 클릭합니다.

사용량 보고서가 다운로드됩니다.

3. 다운로드한 파일을 열어 보고서에 액세스합니다.

#### 구입한 라이선스를 계정에 추가합니다

BlueXP 디지털 지갑에 구입한 라이선스가 없으면 Cloud Volumes ONTAP에 사용할 수 있도록 BlueXP에 라이선스를 추가해야 합니다.

#### 필요한 것

- 라이선스 또는 라이선스 파일의 일련 번호를 BlueXP에 제공해야 합니다.
- 일련 번호를 입력하려면 먼저 해야 합니다 ["NetApp Support 사이트 계정을 BlueXP에 추가합니다"](#). 일련 번호에 액세스할 수 있는 권한이 있는 NetApp Support 사이트 계정입니다.

#### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭에서 \* 용량 기반 라이선스 \* 를 선택한 상태로 두고 \* 라이선스 추가 \* 를 클릭합니다.
3. 용량 기반 라이선스의 일련 번호를 입력하거나 라이선스 파일을 업로드하십시오.

일련 번호를 입력한 경우 일련 번호에 액세스할 수 있는 권한이 있는 NetApp Support 사이트 계정도 선택해야 합니다.

4. 라이선스 추가 \* 를 클릭합니다.

#### 용량 기반 라이선스를 업데이트합니다

추가 용량을 구매하거나 라이선스 기간을 연장한 경우 BlueXP는 디지털 지갑에서 라이선스를 자동으로 업데이트합니다. 당신이 해야 할 일은 아무것도 없습니다.

하지만 인터넷에 액세스할 수 없는 위치에 BlueXP를 배포한 경우에는 BlueXP에서 라이선스를 수동으로 업데이트해야 합니다.

필요한 것

라이선스 파일(또는 HA 쌍이 있는 경우 \_ 파일 \_).

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP\* 탭에서 사용권 옆에 있는 작업 메뉴를 클릭하고 \* 사용권 업데이트 \* 를 선택합니다.
3. 라이선스 파일을 업로드합니다.
4. 라이선스 업로드 \* 를 클릭합니다.

충전 방법을 변경합니다

용량 기반 라이선스를 사용하는 Cloud Volumes ONTAP 시스템의 충전 방법을 변경할 수 있습니다. 예를 들어, Essentials 패키지와 함께 Cloud Volumes ONTAP 시스템을 배포한 경우 비즈니스 요구사항이 변경되면 이를 Professional 패키지로 변경할 수 있습니다.

제한

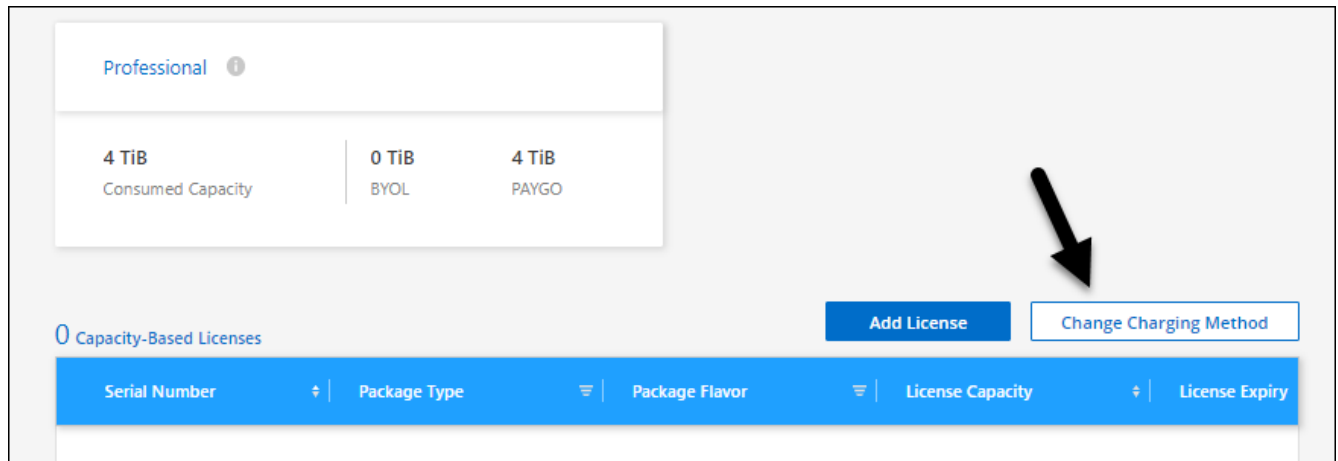
Edge Cache 라이선스로 변경하거나 변경하는 것은 지원되지 않습니다.

중요 참고 사항

클라우드 공급자 마켓플레이스에서 프라이빗 오퍼 또는 계약을 체결한 경우, 계약에 포함되지 않은 충전 방법으로 변경하면 BYOL(NetApp에서 라이선스를 구매한 경우) 또는 PAYGO에 대해 충전이 생성됩니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭에서 \* 충전 방법 변경 \* 을 클릭합니다.



3. 작업 환경을 선택하고 새 충전 방법을 선택한 다음 패키지 유형을 변경하면 서비스 요금이 달라지게 된다는 것을 이해했는지 확인합니다.

4. 충전 방법 변경 \* 을 클릭합니다.

결과

BlueXP는 Cloud Volumes ONTAP 시스템의 충전 방법을 변경합니다.

BlueXP 디지털 지갑은 각 패키지 유형의 소비된 용량을 새로 고쳐 방금 변경한 내용을 고려할 수도 있습니다.

용량 기반 라이선스를 제거합니다

용량 기반 라이선스가 만료되어 더 이상 사용되지 않는 경우 언제든지 라이선스를 제거할 수 있습니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP\* 탭에서 사용권 옆에 있는 작업 메뉴를 클릭하고 \* 사용권 제거 \* 를 선택합니다.
3. 확인하려면 \* 제거 \* 를 클릭합니다.

## Keystone 구독 관리

Cloud Volumes ONTAP에서 사용할 수 있도록 구독을 활성화하여 BlueXP 디지털 지갑에서 Keystone 가입을 관리하십시오. 또한 커밋된 용량에 대한 변경 내용을 요청하고 구독 연결을 해제할 수 있습니다.

Keystone 가입 \_ 은 NetApp이 제공하는 종량제 스토리지 서비스입니다.



BlueXP 디지털 지갑 \_을(를) 사용하면 한 곳에서 Cloud Volumes ONTAP에 대한 라이선스를 관리할 수 있습니다. 새 라이선스를 추가하고 기존 라이선스를 업데이트할 수 있습니다.

"Cloud Volumes ONTAP 라이선스에 대해 자세히 알아보십시오".

계정을 인증합니다

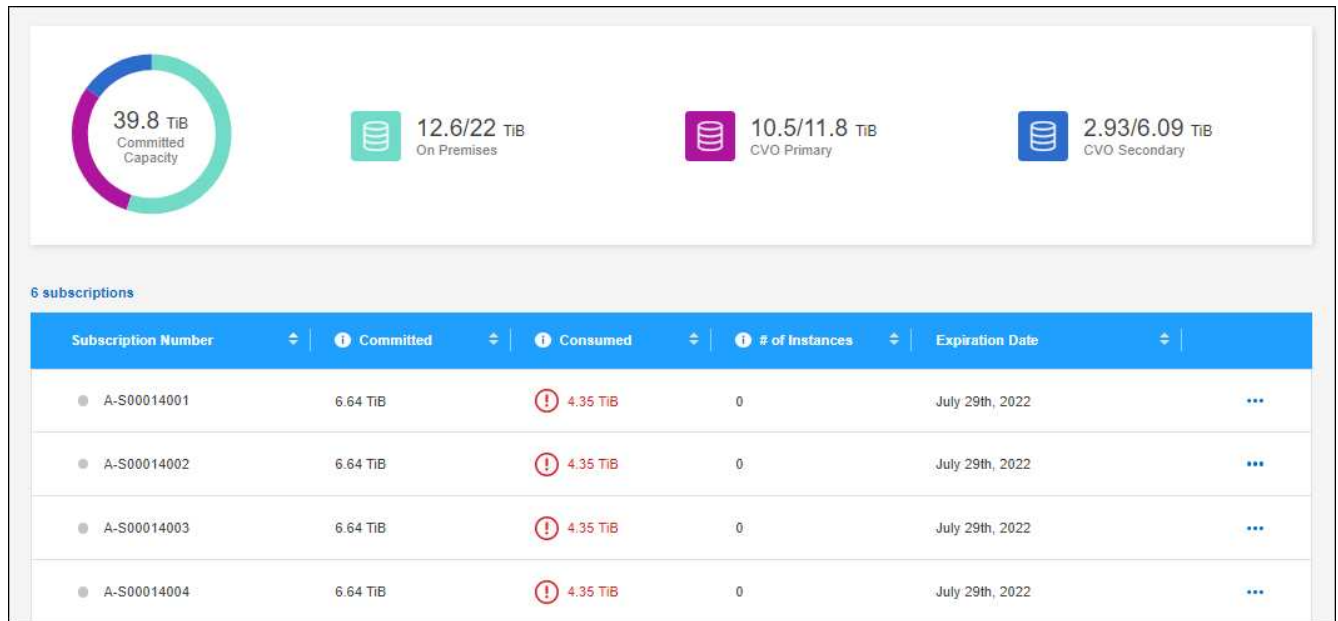
BlueXP에서 Keystone 등록을 사용하고 관리하려면 NetApp에 문의하여 Keystone 구독으로 BlueXP 사용자 계정을 인증해야 합니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Keystone \* 을 선택합니다.
3. NetApp Keystone\* 시작 페이지가 나타나면 페이지에 나열된 주소로 이메일을 보냅니다.

NetApp 담당자가 사용자 계정에 구독 액세스를 승인하여 요청을 처리합니다.

4. 가입을 보려면 \* Keystone 가입 \* 으로 돌아갑니다.



다음 단계

Cloud Volumes ONTAP에 사용할 구독을 연결합니다.

구독 링크

NetApp에서 사용자 계정을 승인한 후 Cloud Volumes ONTAP에 사용할 수 있도록 Keystone 구독을 연결해야 합니다. 이 작업을 통해 사용자는 새 Cloud Volumes ONTAP 시스템의 충전 방법으로 구독을 선택할 수 있습니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Keystone \* 을 선택합니다.

3. 연결할 구독의 경우 을 클릭합니다 ... 링크 \* 를 선택합니다.

Subscription Number	Committed	Consumed	# of Instances	Expiration Date	
A-S00014001	6.64 TiB	4.35 TiB	0	July 29th, 2022	...
A-S00014002	6.64 TiB	4.35 TiB	0	July 29th, 2022	View detail and edit
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022	Link

결과

이제 가입이 BlueXP 계정에 연결되어 있으며 Cloud Volumes ONTAP 작업 환경을 생성할 때 선택할 수 있습니다.



커밋된 용량을 더 많이 또는 적게 요청합니다

구독에 대해 커밋된 용량을 조정해야 하는 경우 BlueXP 인터페이스에서 바로 요청을 보낼 수 있습니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Keystone \* 을 선택합니다.
3. 용량을 조정하려는 구독의 경우 을 클릭합니다 ... 를 선택하고 \* 상세 정보 보기 및 편집 \* 을 선택합니다.
4. 하나 이상의 구독에 대해 요청된 커밋 용량을 입력합니다.

### Subscription Modification for A-S00014001

Service Level	Current Committed Capacity	Current Consumed Capacity	Requested Committed Capacity
Extreme	0.977 TiB	0.293 TiB	<input type="text" value="Enter amount"/> TiB
Premium	0.977 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB
Performance	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
Standard	0.732 TiB	0.439 TiB	<input type="text" value="Enter amount"/> TiB
Value	0.977 TiB	 0.879 TiB	<input type="text" value="Enter amount"/> TiB
Data Tiering	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
CVO Primary	1.96 TiB	 1.76 TiB	<input type="text" value="3"/> TiB
CVO Secondary	1.02 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB

#### Additional Information

Is there anything else we should know about your request?  
Please be as descriptive as possible.

Enter your notes here

5. 아래로 스크롤하여 요청에 대한 추가 세부 정보를 입력한 다음 \* 제출 \* 을 클릭합니다.

결과

요청이 NetApp의 시스템에서 처리를 위한 티켓을 생성합니다.

구독 연결을 해제합니다

새 Cloud Volumes ONTAP 시스템에 Keystone 가입을 더 이상 사용하지 않으려면 가입을 연결 해제할 수 있습니다. 기존 Cloud Volumes ONTAP 구독에 연결되지 않은 구독만 연결 해제할 수 있습니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Keystone \* 을 선택합니다.
3. 연결을 해제할 구독의 경우 을 클릭합니다 ... 를 클릭하고 \* 연결 해제 \* 를 선택합니다.

결과

가입이 BlueXP 계정과 연결되어 있지 않으며 Cloud Volumes ONTAP 작업 환경을 생성할 때 더 이상 선택할 수 없습니다.

## 노드 기반 라이선스 관리

BlueXP 디지털 지갑에서 노드 기반 라이선스를 관리하여 각 Cloud Volumes ONTAP 시스템에 필요한 용량의 유효한 라이선스가 있는지 확인합니다.

\_노드 기반 라이선스\_ 은(는) 이전 세대 라이선스 모델입니다(신규 고객은 사용할 수 없습니다).

- NetApp에서 BYOL 라이선스를 구입함
- 클라우드 공급자 마켓플레이스에서 시간별 PAYGO(Pay-as-you-go) 구독을 지원합니다

BlueXP 디지털 지갑 \_을(를) 사용하면 한 곳에서 Cloud Volumes ONTAP에 대한 라이선스를 관리할 수 있습니다. 새 라이선스를 추가하고 기존 라이선스를 업데이트할 수 있습니다.

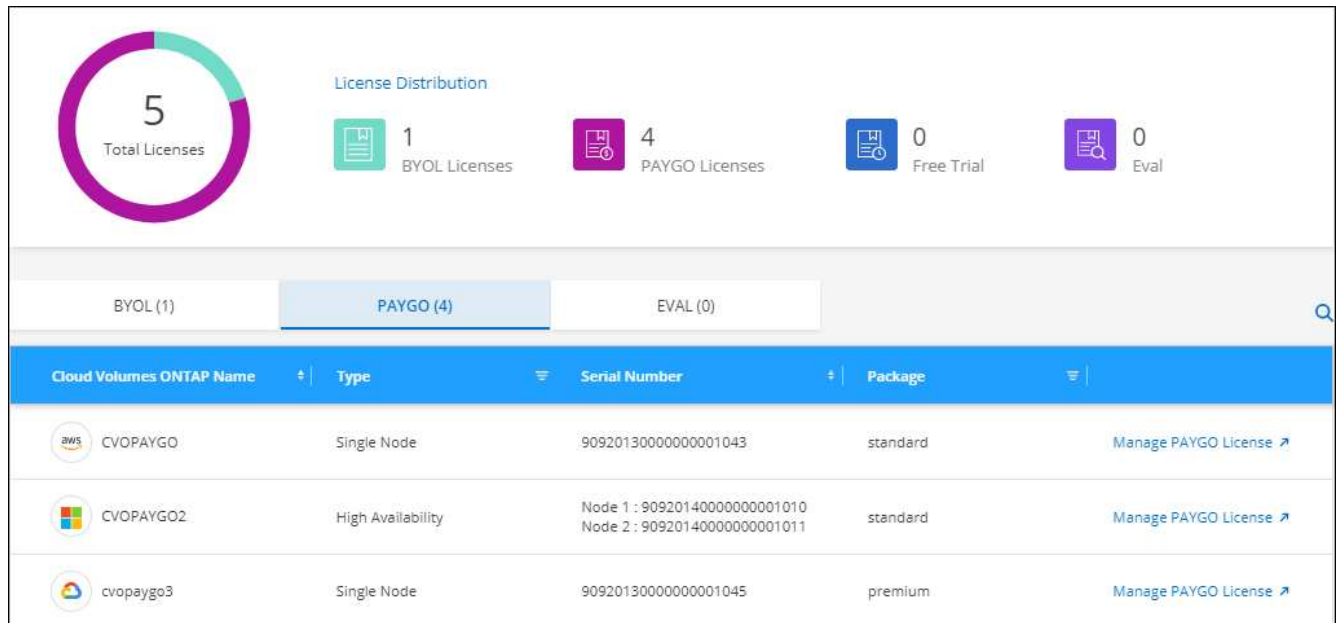
"Cloud Volumes ONTAP 라이선스에 대해 자세히 알아보십시오".

### PAYGO 라이선스를 관리합니다

BlueXP 디지털 지갑 페이지에서 일련 번호 및 PAYGO 라이선스 유형을 비롯한 각 PAYGO Cloud Volumes ONTAP 시스템에 대한 세부 정보를 볼 수 있습니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. PAYGO \* 를 클릭합니다.
4. 각 PAYGO 라이선스에 대한 자세한 내용은 표에서 확인하십시오.



The screenshot displays the 'License Distribution' section of the BlueXP Digital Wallet. It features a donut chart showing 5 Total Licenses, broken down into 1 BYOL License, 4 PAYGO Licenses, 0 Free Trial, and 0 Eval. Below the chart, there are tabs for 'BYOL (1)', 'PAYGO (4)', and 'EVAL (0)'. The 'PAYGO (4)' tab is selected, showing a table of licenses.

Cloud Volumes ONTAP Name	Type	Serial Number	Package	Actions
CVOPAYGO	Single Node	90920130000000001043	standard	<a href="#">Manage PAYGO License</a>
CVOPAYGO2	High Availability	Node 1 : 90920140000000001010 Node 2 : 90920140000000001011	standard	<a href="#">Manage PAYGO License</a>
cvopayo3	Single Node	90920130000000001045	premium	<a href="#">Manage PAYGO License</a>

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

## BYOL 라이선스 관리

시스템 라이선스 및 추가 용량 라이선스를 추가 및 제거하여 NetApp에서 직접 구매한 라이선스를 관리합니다.

할당되지 않은 라이선스를 추가합니다

BlueXP 디지털 지갑에 노드 기반 라이선스를 추가하여 새 Cloud Volumes ONTAP 시스템을 생성할 때 라이선스를 선택할 수 있습니다. 디지털 지갑에서 이러한 라이선스를 할당되지 않음으로 식별합니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. 할당되지 않음 \* 을 클릭합니다.
4. 할당되지 않은 라이선스 추가 \* 를 클릭합니다.
5. 라이선스의 일련 번호를 입력하거나 라이선스 파일을 업로드하십시오.

라이선스 파일이 아직 없는 경우 아래 섹션을 참조하십시오.

6. 라이선스 추가 \* 를 클릭합니다.

결과

BlueXP는 디지털 지갑에 라이선스를 추가합니다. 라이선스는 새 Cloud Volumes ONTAP 시스템에 연결할 때까지 할당되지 않은 것으로 식별됩니다. 그런 다음 디지털 지갑에서 \* BYOL \* 탭으로 라이선스가 이동됩니다.

할당되지 않은 **Exchange** 노드 기반 라이선스

아직 사용하지 않은 Cloud Volumes ONTAP에 대해 할당되지 않은 노드 기반 라이선스가 있는 경우 라이선스를 BlueXP 백업 및 복구 라이선스, BlueXP 분류 라이선스 또는 BlueXP 계층화 라이선스로 변환하여 교환할 수 있습니다.

라이선스 교환은 Cloud Volumes ONTAP 라이선스를 해지하고 서비스에 대해 달러 상당 라이선스를 생성합니다.

- Cloud Volumes ONTAP HA 쌍의 라이선스는 51TiB 데이터 서비스 라이선스로 변환됩니다
- Cloud Volumes ONTAP 단일 노드의 라이선스는 32TiB 데이터 서비스 라이선스로 변환됩니다

변환된 라이선스의 만료일은 Cloud Volumes ONTAP 라이선스와 동일합니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. 할당되지 않음 \* 을 클릭합니다.
4. Exchange 라이선스 \* 를 클릭합니다.

BYOL (14)		Eval (2)		Unassigned (3)		PAYGO (6)		Add Unassigned Licenses	
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					

- 라이센스를 교환할 서비스를 선택합니다.
- 메시지가 표시되면 HA 쌍에 대한 추가 라이선스를 선택합니다.
- 법적 동의를 읽고 \* 동의 \* 를 클릭합니다.

#### 결과

BlueXP는 할당되지 않은 라이선스를 선택한 서비스로 변환합니다. 데이터 서비스 라이선스 \* 탭에서 새 라이선스를 볼 수 있습니다.

시스템 라이선스 파일을 얻습니다

대부분의 경우 BlueXP는 NetApp Support 사이트 계정을 사용하여 라이선스 파일을 자동으로 가져올 수 있습니다. 그러나 그렇지 않으면 라이선스 파일을 수동으로 업로드해야 합니다. 라이선스 파일이 없는 경우 netapp.com 에서 얻을 수 있습니다.

#### 단계

- 로 이동합니다 "NetApp 라이선스 파일 생성기" 를 입력하고 NetApp Support 사이트 자격 증명을 사용하여 로그인합니다.
- 비밀번호를 입력하고 제품을 선택한 다음 일련 번호를 입력하고 개인정보 보호정책을 읽고 동의했는지 확인한 다음 \* 제출 \* 을 클릭합니다.
  - 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	
Company	Network Appliance, Inc
Email Address	
Username	

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

I have read NetApp's new **Global Data** may use my personal data.

3. 이메일 또는 직접 다운로드를 통해 serialnumber.nlf JSON 파일을 수신할지 여부를 선택합니다.

시스템 라이선스를 업데이트합니다

NetApp 담당자에게 연락하여 BYOL 구독을 갱신하면, BlueXP는 NetApp에서 새로운 라이선스를 자동으로 얻어 Cloud Volumes ONTAP 시스템에 설치합니다.

보안 인터넷 연결을 통해 BlueXP에서 라이선스 파일에 액세스할 수 없는 경우 직접 파일을 얻은 다음 파일을 BlueXP에 수동으로 업로드할 수 있습니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. BYOL \* 탭에서 Cloud Volumes ONTAP 시스템의 세부 정보를 확장합니다.
4. 시스템 라이선스 옆에 있는 작업 메뉴를 클릭하고 \* 라이선스 업데이트 \* 를 선택합니다.
5. 라이선스 파일(또는 HA 쌍이 있는 경우 파일)을 업로드합니다.
6. Update License \* 를 클릭합니다.

결과

BlueXP는 Cloud Volumes ONTAP 시스템의 라이선스를 업데이트합니다.

추가 용량 라이선스 관리

Cloud Volumes ONTAP BYOL 시스템용 추가 용량 라이선스를 구입하여 368TiB 이상의 용량을 BYOL 시스템

라이선스와 함께 할당할 수 있습니다. 예를 들어, 라이선스 용량을 하나 더 구매하여 Cloud Volumes ONTAP에 최대 736TiB의 용량을 할당할 수 있습니다. 또는 최대 1.4PiB까지 추가 용량 라이선스를 3개 구매할 수 있습니다.

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

#### 용량 라이선스 추가

BlueXP의 오른쪽 하단에 있는 채팅 아이콘을 통해 문의하여 추가 용량 라이선스를 구입하십시오. 라이선스를 구입한 후 Cloud Volumes ONTAP 시스템에 적용할 수 있습니다.

#### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. BYOL \* 탭에서 Cloud Volumes ONTAP 시스템의 세부 정보를 확장합니다.
4. 용량 라이선스 추가 \* 를 클릭합니다.
5. 일련 번호를 입력하거나 라이선스 파일(또는 HA 쌍이 있는 경우 파일)을 업로드합니다.
6. 용량 라이선스 추가 \* 를 클릭합니다.

#### 용량 라이선스를 업데이트합니다

추가 용량 라이선스 기간을 연장한 경우 BlueXP에서 라이선스를 업데이트해야 합니다.

#### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. BYOL \* 탭에서 Cloud Volumes ONTAP 시스템의 세부 정보를 확장합니다.
4. 용량 라이선스 옆에 있는 작업 메뉴를 클릭하고 \* 라이선스 업데이트 \* 를 선택합니다.
5. 라이선스 파일(또는 HA 쌍이 있는 경우 파일)을 업로드합니다.
6. Update License \* 를 클릭합니다.

#### 용량 라이선스를 제거합니다

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

#### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. BYOL \* 탭에서 Cloud Volumes ONTAP 시스템의 세부 정보를 확장합니다.
4. 용량 라이선스 옆에 있는 작업 메뉴를 클릭하고 \* 라이선스 제거 \* 를 선택합니다.
5. 제거 \* 를 클릭합니다.

#### Eval 라이선스를 BYOL로 변환합니다

평가판 라이선스는 30일간 사용할 수 있습니다. 현재 위치 업그레이드에 대한 평가 라이선스 위에 새로운 BYOL



라이센스를 적용할 수 있습니다.

평가판 라이선스를 BYOL로 변환하면 BlueXP가 Cloud Volumes ONTAP 시스템을 다시 시작합니다.

- 단일 노드 시스템의 경우 재시작 시 재부팅 프로세스 중에 I/O가 중단됩니다.
- HA 쌍의 경우, 재시작은 테이크오버 및 반환을 시작하여 클라이언트에 계속 I/O를 제공합니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. Eval \* 을 클릭합니다.
4. 표에서 Cloud Volumes ONTAP 시스템용 BYOL 라이선스 \* 로 변환 을 클릭합니다.
5. 일련 번호를 입력하거나 라이선스 파일을 업로드하십시오.
6. 사용권 변환 \* 을 클릭합니다.

결과

BlueXP가 변환 프로세스를 시작합니다. 이 프로세스의 일부로 Cloud Volumes ONTAP가 자동으로 다시 시작됩니다. 백업하는 경우 라이선스 정보에 새 라이선스가 반영됩니다.

## PAYGO와 BYOL 간 변경

시스템을 PAYGO by-node 라이선싱에서 BYOL by-node 라이선싱으로 변환하는 것은 지원되지 않으며 그 반대의 경우도 마찬가지입니다. 사용한 만큼만 지불하는 가입과 BYOL 가입형 간에 전환하려면 새 시스템을 구축하고 기존 시스템에서 새 시스템으로 데이터를 복제해야 합니다.

단계

1. 새 Cloud Volumes ONTAP 작업 환경을 만듭니다.
2. 복제해야 하는 각 볼륨에 대해 시스템 간에 일회성 데이터 복제를 설정합니다.

"시스템 간에 데이터를 복제하는 방법에 대해 알아보십시오"

3. 원래 작업 환경을 삭제하여 더 이상 필요하지 않은 Cloud Volumes ONTAP 시스템을 종료합니다.

"Cloud Volumes ONTAP 작업 환경을 삭제하는 방법에 대해 알아보십시오".

## 볼륨 및 LUN 관리

### FlexVol 볼륨을 생성합니다

초기 Cloud Volumes ONTAP 시스템을 시작한 후 더 많은 스토리지가 필요한 경우 BlueXP에서 NFS, CIFS 또는 iSCSI용 새 FlexVol 볼륨을 생성할 수 있습니다.

BlueXP에서는 여러 가지 방법으로 새 볼륨을 만들 수 있습니다.

- 새 볼륨에 대한 세부 정보를 지정하고 BlueXP에서 기본 데이터 집계를 처리하도록 합니다. [자세한 정보](#)

- 선택한 데이터 애그리게이트에 볼륨을 생성합니다. [자세한 정보](#)
- 템플릿에서 볼륨을 생성하여 데이터베이스 또는 스트리밍 서비스와 같은 특정 애플리케이션의 워크로드 요구사항에 맞게 볼륨을 최적화합니다. [자세한 정보](#)
- HA 구성의 두 번째 노드에 볼륨을 생성합니다. [자세한 정보](#)

시작하기 전에

볼륨 프로비저닝에 대한 몇 가지 참고 사항:

- iSCSI 볼륨을 생성할 때 BlueXP에서 자동으로 LUN을 생성합니다. 볼륨 당 하나의 LUN만 생성하므로 관리가 필요 없습니다. 볼륨을 생성한 후 "[iQN을 사용하여 호스트에서 LUN에 연결합니다](#)".
- System Manager 또는 CLI에서 추가 LUN을 생성할 수 있습니다.
- AWS에서 CIFS를 사용하려면 DNS와 Active Directory를 설정해야 합니다. 자세한 내용은 [을 참조하십시오 "Cloud Volumes ONTAP for AWS의 네트워킹 요구사항"](#).
- Cloud Volumes ONTAP 구성에서 Amazon EBS Elastic Volumes 기능을 지원하는 경우 원하는 대로 구성할 수 있습니다 "[볼륨을 생성할 때 발생하는 상황에 대해 자세히 알아보십시오](#)".

볼륨을 생성합니다

볼륨을 생성하는 가장 일반적인 방법은 필요한 볼륨 유형을 지정한 다음 BlueXP에서 디스크 할당을 처리하는 것입니다. 그러나 볼륨을 생성할 특정 Aggregate를 선택할 수도 있습니다.

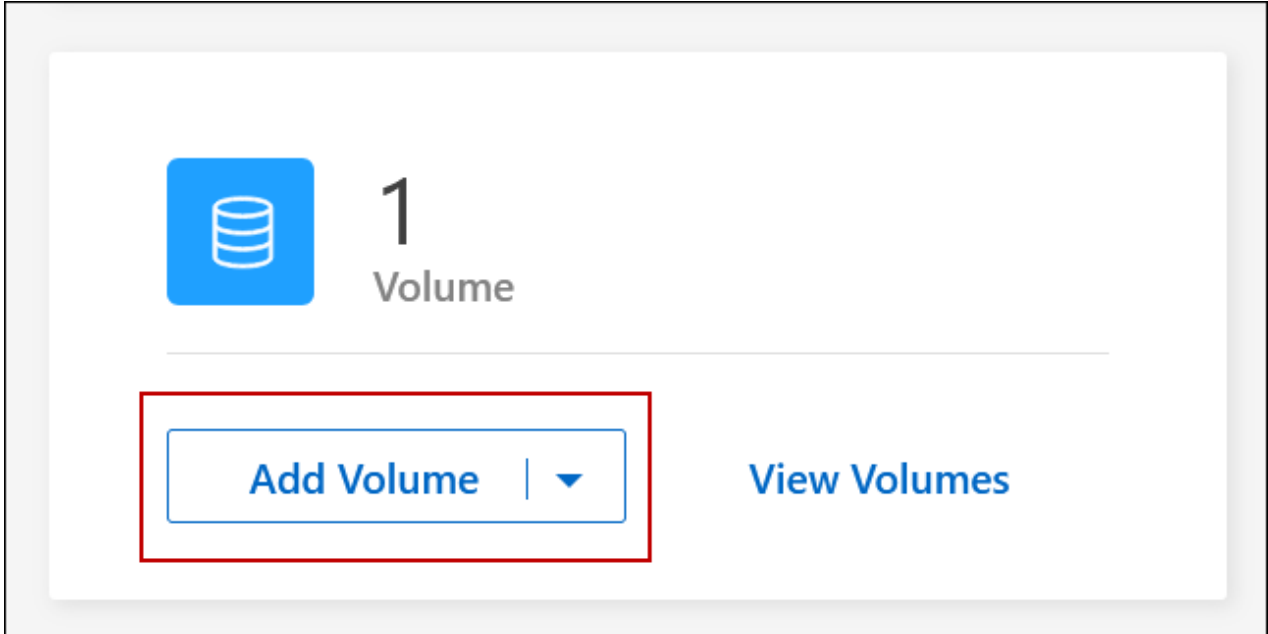
단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 FlexVol 볼륨을 프로비저닝할 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
3. BlueXP에서 디스크 할당을 처리하도록 하거나 볼륨에 대한 특정 집계를 선택하여 새 볼륨을 생성합니다.

Cloud Volumes ONTAP 시스템의 데이터 애그리게이트를 잘 알고 있는 경우에만 특정 애그리게이트를 선택하는 것이 좋습니다.

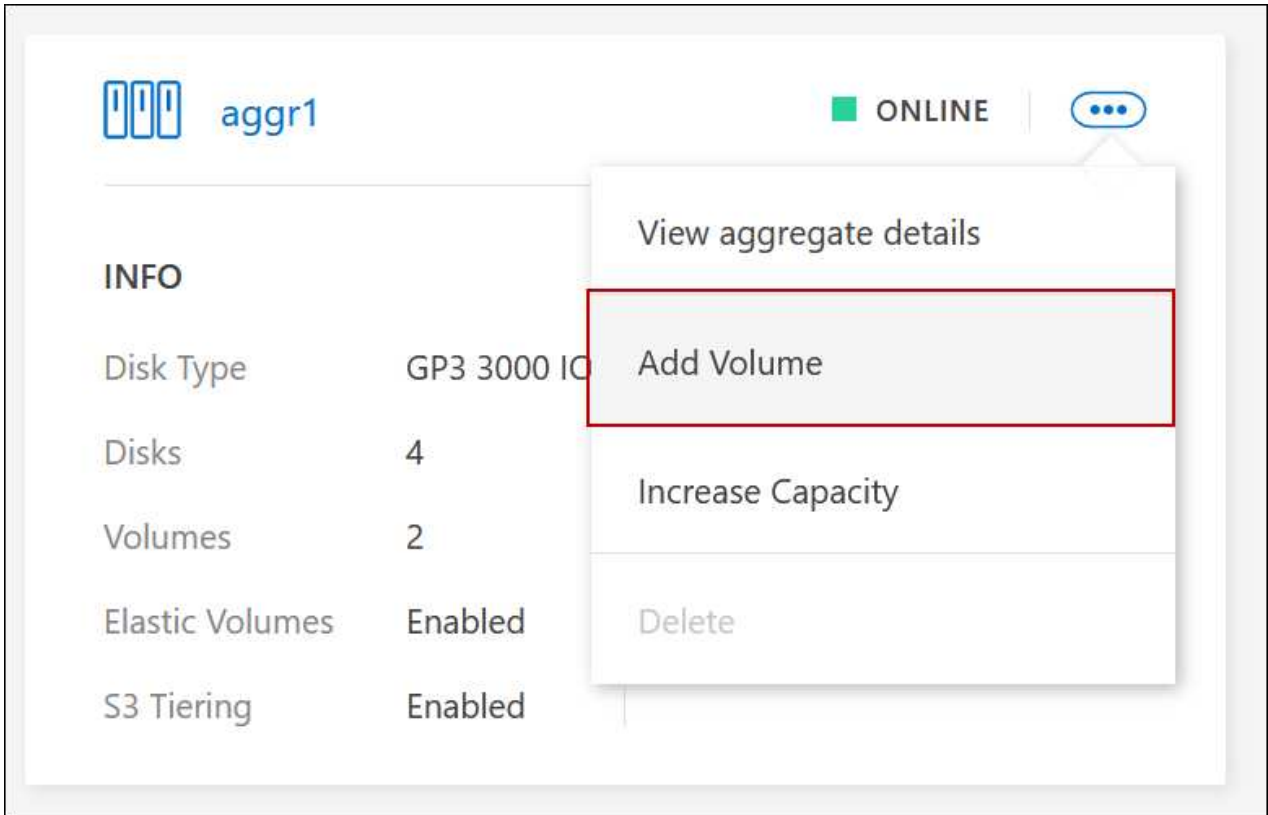
모든 애그리게이트

개요 탭에서 볼륨 타일로 이동한 다음 \* 볼륨 추가 \* 를 클릭합니다.



특정 애그리게이트

애그리게이트 탭에서 원하는 애그리게이트 타일로 이동합니다. 메뉴 아이콘을 클릭한 다음 \* 볼륨 추가 \* 를 클릭합니다.



4. 마법사의 단계에 따라 볼륨을 생성합니다.

a. \* 볼륨, 세부 정보, 보호 및 태그 \*: 볼륨에 대한 기본 세부 정보를 입력하고 스냅샷 정책을 선택합니다.

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

필드에 입력합니다	설명
볼륨 이름	새 볼륨에 입력할 수 있는 식별 가능한 이름입니다.
볼륨 크기	입력할 수 있는 최대 크기는 씬 프로비저닝의 사용 여부에 따라 크게 달라집니다. 이를 통해 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다.
태그	볼륨에 추가하는 태그는 과 연결됩니다 "응용 프로그램 템플릿 서비스"을 사용하면 리소스 관리를 구성하고 단순화할 수 있습니다.
스토리지 VM(SVM)	스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에 스토리지 및 데이터 서비스를 제공합니다. SVM 또는 가상 서버로서 이를 알 수 있습니다. Cloud Volumes ONTAP는 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다. 새 볼륨에 대해 스토리지 VM을 지정할 수 있습니다.
스냅샷 정책	스냅샷 복사본 정책은 자동으로 생성되는 NetApp 스냅샷 복사본의 수와 빈도를 지정합니다. NetApp 스냅샷 복사본은 성능 영향이 없고 최소한의 스토리지가 필요한 시점 파일 시스템 이미지입니다. 기본 정책을 선택하거나 선택하지 않을 수 있습니다. Microsoft SQL Server의 tempdb와 같이 임시 데이터에 대해 없음을 선택할 수 있습니다.

b. \* 프로토콜 \*: 볼륨의 프로토콜(NFS, CIFS 또는 iSCSI)을 선택한 다음 필요한 정보를 제공합니다.

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

"지원되는 클라이언트 프로토콜 및 버전에 대해 알아보십시오".

다음 섹션에서는 지침이 필요한 필드에 대해 설명합니다. 설명은 프로토콜별로 구성되어 있습니다.

## NFS 를 참조하십시오

### 액세스 제어

클라이언트에서 볼륨을 사용할 수 있도록 사용자 지정 익스포트 정책을 선택합니다.

### 익스포트 정책

볼륨을 액세스할 수 있는 서버넷의 클라이언트를 정의합니다. 기본적으로 BlueXP는 서버넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.

## CIFS를 선택합니다

### 권한 및 사용자/그룹

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

## DNS 기본 및 보조 IP 주소

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

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

### 연결할 **Active Directory** 도메인입니다

CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.

### 도메인에 가입하도록 승인된 자격 증명입니다

AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.

## CIFS 서버 NetBIOS 이름입니다

AD 도메인에서 고유한 CIFS 서버 이름입니다.

### 조직 구성 단위

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

- AWS 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 \* OU=Computers, OU=Corp \* 를 입력합니다.
- Azure AD 도메인 서비스를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 \* OU=ADDC 컴퓨터 \* 또는 \* OU=ADDC 사용자 \* 를 입력합니다.  
"Azure 설명서: Azure AD 도메인 서비스 관리 도메인에 OU(조직 구성 단위)를 만듭니다"
- Google 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 \* OU=Computers, OU=Cloud \* 를 입력합니다.  
"Google 클라우드 문서: Google Managed Microsoft AD의 조직 단위"

## DNS 도메인

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

## NTP 서버

Active Directory DNS를 사용하여 NTP 서버를 구성하려면 \* Active Directory 도메인 사용 \* 을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 를 참조하십시오 ["BlueXP 자동화 문서"](#) 를 참조하십시오.

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

## iSCSI

### LUN을 클릭합니다

iSCSI 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 표시됩니다. iSCSI 볼륨을 생성할 때 BlueXP에서 자동으로 LUN을 생성합니다. 우리는 볼륨당 하나의 LUN만 생성하므로 관리가 필요하지 않습니다. 볼륨을 생성한 후 ["IQN을 사용하여 호스트에서 LUN에 연결합니다"](#).

### 이니시에이터 그룹

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

### 호스트 이니시에이터(IQN)

iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 통합 네트워크 어댑터(CNA) 또는 전용 호스트 파스트 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 공인 이름(IQN)으로 식별됩니다.

a. \* 디스크 유형 \*: 성능 요구 사항 및 비용 요구 사항에 따라 볼륨의 기본 디스크 유형을 선택합니다.

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

5. \* Usage Profile & Tiering Policy \*: 볼륨에서 스토리지 효율성 기능을 활성화 또는 비활성화할지 여부를 선택한 다음 를 선택합니다 ["볼륨 계층화 정책"](#).

ONTAP에는 필요한 총 스토리지 양을 줄일 수 있는 몇 가지 스토리지 효율성 기능이 포함되어 있습니다. NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

### 씬 프로비저닝

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

### 중복 제거

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

### 압축

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

6. \* Review \* (검토 \*): 볼륨에 대한 세부 정보를 검토한 다음 \* Add \* (추가 \*)를 클릭합니다.

## 결과

BlueXP는 Cloud Volumes ONTAP 시스템에 볼륨을 생성합니다.

템플릿에서 볼륨을 생성합니다

조직에서 Cloud Volumes ONTAP 볼륨 템플릿을 만들어 특정 애플리케이션의 워크로드 요구사항에 최적화된 볼륨을 구축한 경우 이 섹션의 단계를 수행하십시오.

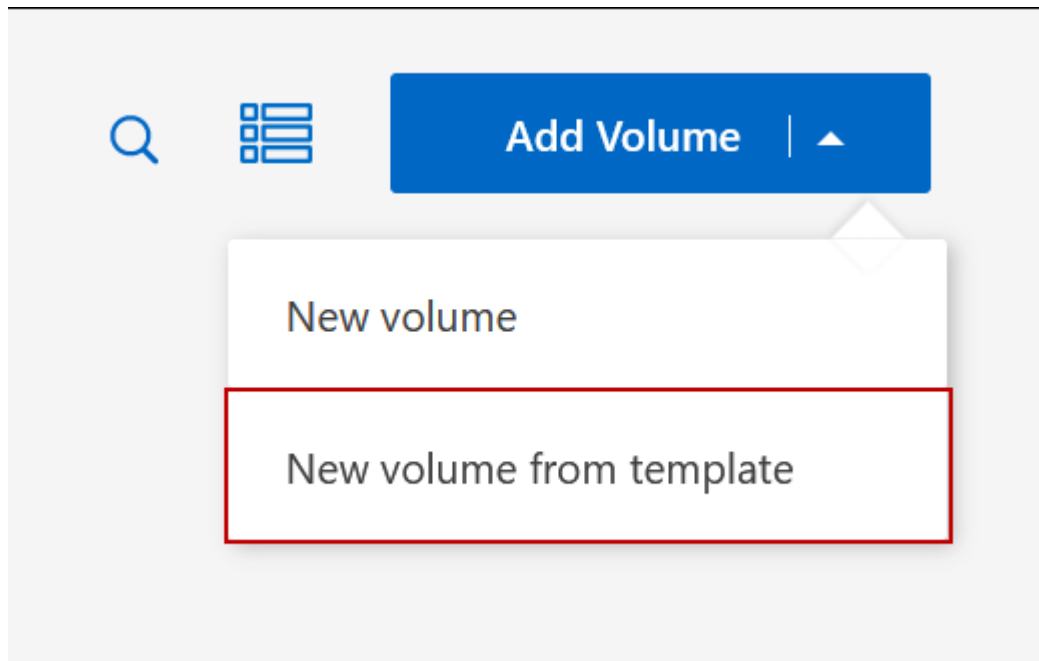
템플릿에 디스크 유형, 크기, 프로토콜, 스냅샷 정책, 클라우드 공급자 등 특정 볼륨 매개 변수가 이미 정의되어 있기 때문에 템플릿을 사용하면 작업을 보다 쉽게 수행할 수 있습니다. 있습니다. 매개 변수가 이미 미리 정의된 경우 다음 볼륨 매개 변수로 건너뛸 수 있습니다.



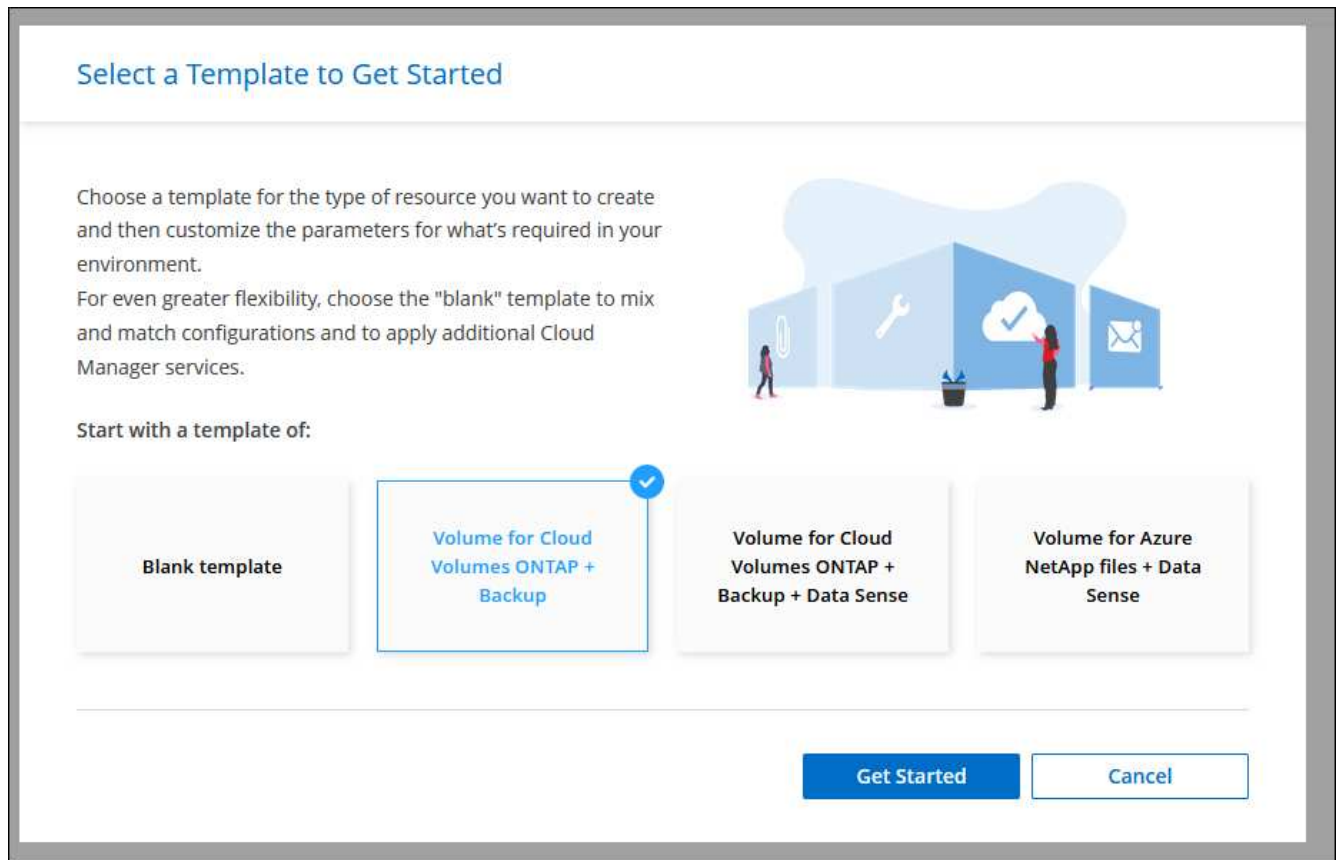
템플릿을 사용하는 경우에만 NFS 또는 CIFS 볼륨을 생성할 수 있습니다.

단계

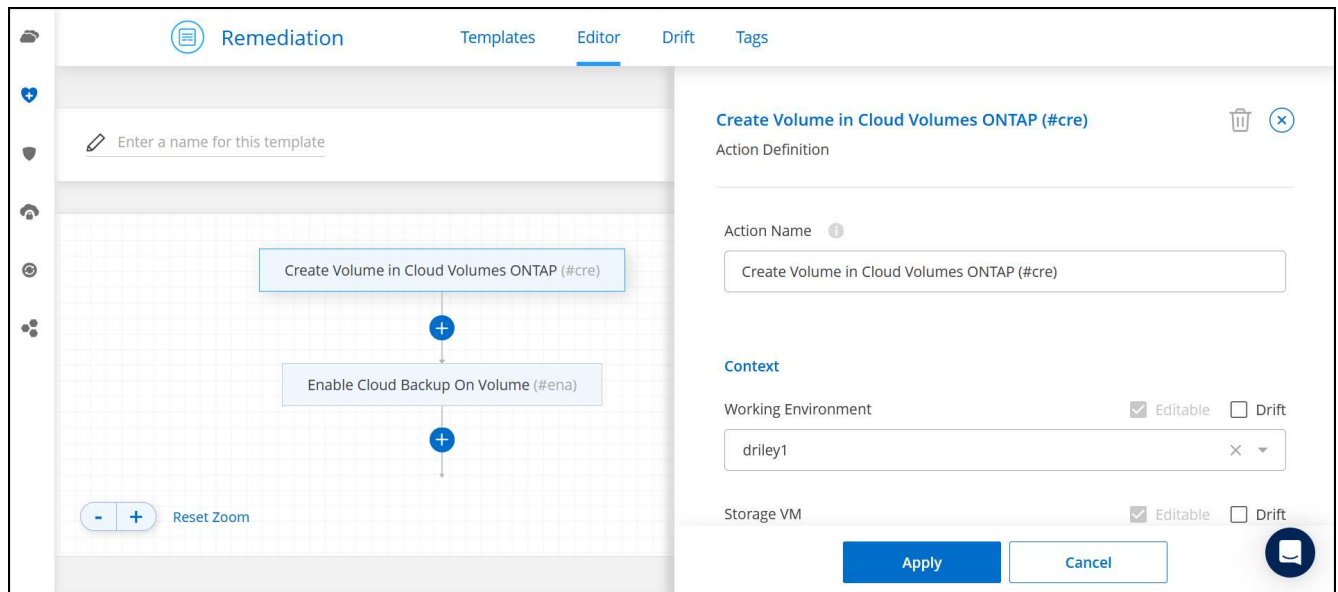
1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 볼륨을 프로비저닝할 Cloud Volumes ONTAP 시스템의 이름을 클릭합니다.
3. 볼륨 탭으로 이동하고 \* 볼륨 추가 \* > \* 템플릿에서 새 볼륨 \* 을 클릭합니다.



4. Select Template\_page에서 볼륨을 생성하는 데 사용할 템플릿을 선택하고 \* Next \* 를 클릭합니다.



Editor\_page가 표시됩니다.

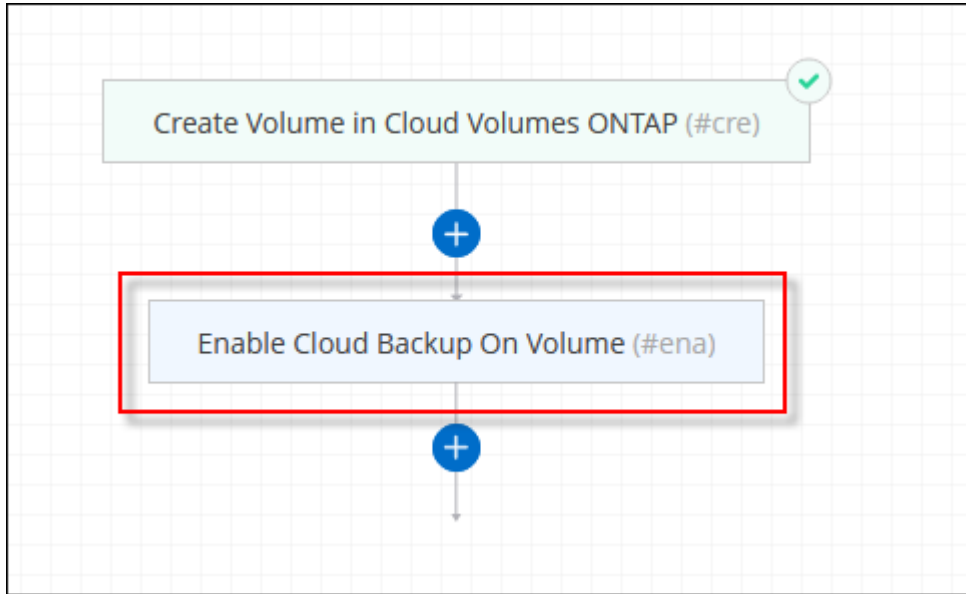


5. Action\_panel 위에 템플릿 이름을 입력합니다.
6. context\_에서 작업 환경은 시작한 작업 환경의 이름으로 채워집니다. 볼륨을 생성할 \* 스토리지 VM \* 을 선택합니다.
7. 템플릿에서 하드 코딩되지 않은 모든 매개변수에 대한 값을 추가합니다. 을 참조하십시오 [볼륨을 생성합니다](#) Cloud Volumes ONTAP 볼륨 구축을 완료하는 데 필요한 모든 매개 변수에 대한 자세한 내용은 를 참조하십시오.
8. Apply \* (적용 \*)를 클릭하여 구성된 매개변수를 선택한 작업에 저장합니다.



9. 정의해야 할 다른 작업이 없는 경우(예: BlueXP 백업 및 복구 구성) \* 템플릿 저장 \* 을 클릭합니다.

다른 작업이 있는 경우 왼쪽 창에서 작업을 클릭하여 완료해야 하는 매개 변수를 표시합니다.



예를 들어 Enable Cloud Backup on Volume 작업이 백업 정책을 선택해야 하는 경우 지금 선택할 수 있습니다.

10. 템플릿 작업에 대한 구성이 완료되면 \* 템플릿 저장 \* 을 클릭합니다.

결과

Cloud Volumes ONTAP에서는 진행 상황을 볼 수 있도록 볼륨을 프로비저닝하고 페이지를 표시합니다.

Creating your resources

This process can take a few minutes.  
Keep this page open to monitor progress, or you can close this page  
and check the [Timeline](#) later for details.

Actions status	
Create Volume in Cloud Volumes ONTAP	Success
Enable Cloud Backup	Pending

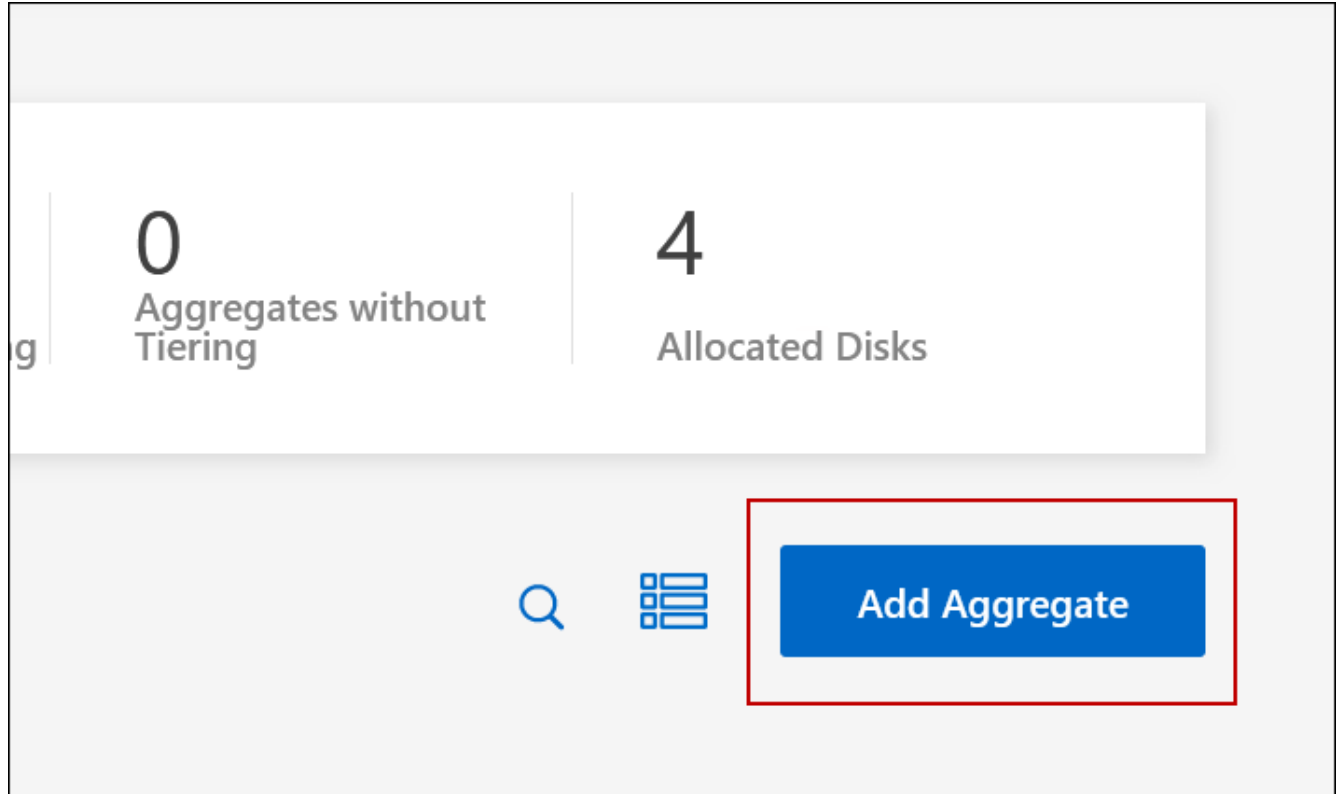
또한 볼륨에 대해 BlueXP 백업 및 복구를 활성화하는 등 템플릿에 보조 작업이 구현된 경우 해당 작업도 수행됩니다.

**HA** 구성의 두 번째 노드에 볼륨을 생성합니다

기본적으로 BlueXP는 HA 구성의 첫 번째 노드에 볼륨을 생성합니다. 두 노드에서 모두 클라이언트에 데이터를 제공하는 액티브-액티브 구성이 필요한 경우 두 번째 노드에서 애그리게이트와 볼륨을 생성해야 합니다.

## 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 집계를 관리할 Cloud Volumes ONTAP 작업 환경의 이름을 두 번 클릭합니다.
3. 집계 탭에서 \* 집계 추가 \* 를 클릭합니다.
4. Add Aggregate\_screen에서 Aggregate를 생성합니다.



5. 홈 노드의 경우 HA 쌍의 두 번째 노드를 선택합니다.
6. BlueXP에서 애그리게이트를 생성한 후 해당 애그리게이트를 선택한 다음 \* 볼륨 생성 \* 을 클릭합니다.
7. 새 볼륨에 대한 세부 정보를 입력한 다음 \* Create \* 를 클릭합니다.

## 결과

BlueXP는 HA 쌍의 두 번째 노드에 볼륨을 생성합니다.



여러 AWS Availability Zone에 구축된 HA 쌍의 경우 볼륨이 상주하는 노드의 부동 IP 주소를 사용하여 볼륨을 클라이언트에 마운트해야 합니다.

## 볼륨을 생성한 후

CIFS 공유를 프로비저닝한 경우 파일 및 폴더에 대한 사용자 또는 그룹 권한을 제공하고 해당 사용자가 공유를 액세스하고 파일을 생성할 수 있는지 확인합니다.

볼륨에 할당량을 적용하려면 System Manager 또는 CLI를 사용해야 합니다. 할당량을 사용하면 사용자, 그룹 또는 qtree가 사용하는 파일 수와 디스크 공간을 제한하거나 추적할 수 있습니다.

## 기존 볼륨 관리

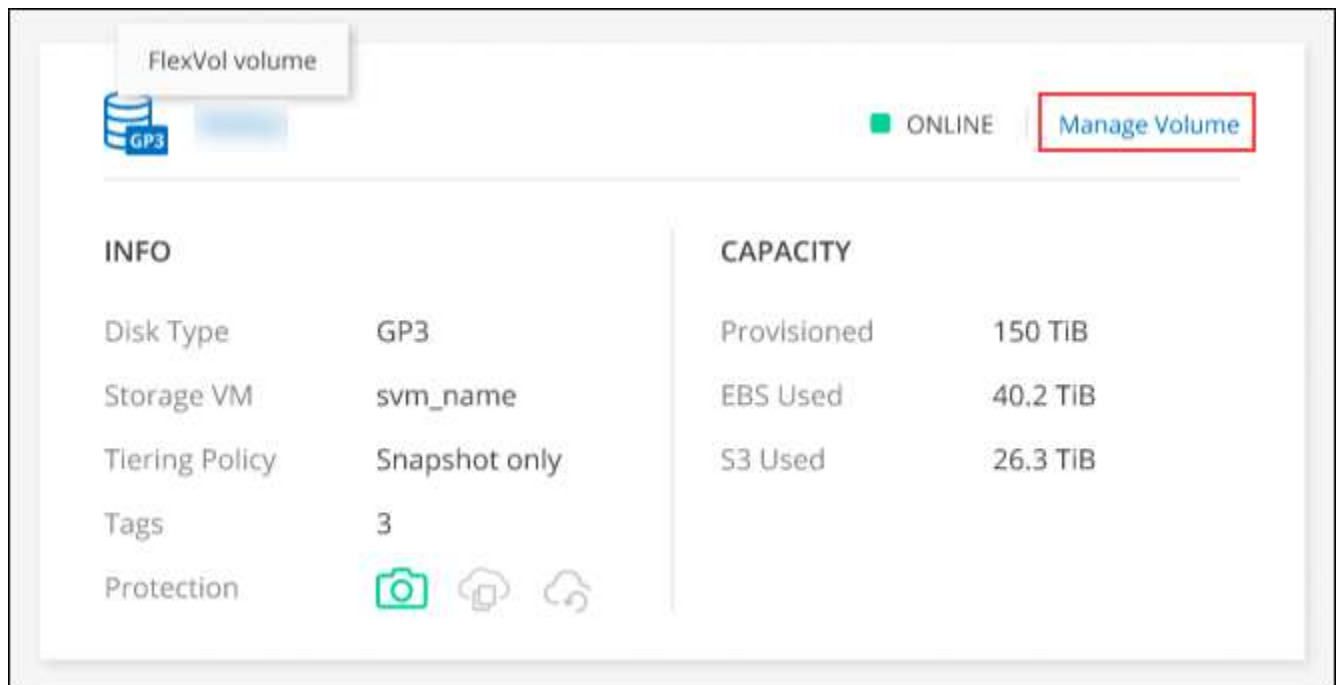
BlueXP를 사용하면 볼륨 및 CIFS 서버를 관리할 수 있습니다. 또한 용량 문제를 방지하기 위해 볼륨을 이동하라는 메시지가 표시됩니다.

### 볼륨 관리

스토리지 요구사항의 변화에 따라 볼륨을 관리할 수 있습니다. 볼륨을 보고, 편집하고, 클론, 복원 및 삭제할 수 있습니다.

#### 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 볼륨을 관리할 Cloud Volumes ONTAP 작업 환경을 두 번 클릭합니다.
3. 작업 환경에서 \* Volumes \* 탭을 클릭합니다.



4. Volumes(볼륨) 탭에서 원하는 볼륨 제목으로 이동한 다음 \* Manage volume(볼륨 관리) \* 을 클릭하여 Manage Volumes(볼륨 관리) 오른쪽 패널에 액세스합니다.

작업	조치
볼륨에 대한 정보를 봅니다	Manage volumes(볼륨 관리) 패널의 Volume Actions(볼륨 작업) 에서 * View volume details(볼륨 세부 정보 보기) * 를 클릭합니다.
NFS mount 명령을 가져옵니다	<ol style="list-style-type: none"> <li>a. 볼륨 관리 패널의 볼륨 작업 에서 * 탑재 명령 * 을 클릭합니다.</li> <li>b. 복사 * 를 클릭합니다.</li> </ol>

작업	조치
볼륨의 클론을 생성합니다	<p>a. Manage volumes(볼륨 관리) 패널의 Volume Actions(볼륨 작업) 에서 * Clone the volume(볼륨 복제) * 을 클릭합니다.</p> <p>b. 필요에 따라 클론 이름을 수정한 다음 * Clone * 을 클릭합니다.</p> <p>이 프로세스에서는 FlexClone 볼륨을 생성합니다. FlexClone 볼륨은 메타데이터에 작은 양의 공간을 사용하고 데이터가 변경 또는 추가됨에 따라 추가 공간만 사용하므로 공간 효율적인 쓰기 가능한 특정 시점 복사본입니다.</p> <p>FlexClone 볼륨에 대한 자세한 내용은 를 참조하십시오 "<a href="#">ONTAP 9 논리적 스토리지 관리 가이드</a>".</p>
볼륨 태그 편집(읽기-쓰기 볼륨만 해당)	<p>a. 볼륨 관리 패널의 볼륨 작업 에서 * 볼륨 태그 편집 * 을 클릭하여 선택한 볼륨에 할당된 볼륨 태그를 수정합니다.</p> <p>b. 제공된 필드에 볼륨 태그 키 및 값을 입력합니다.</p> <p>c. 추가 태그를 포함하려면 * 새 태그 추가 * 를 클릭합니다.</p> <p>d. 저장 * 을 클릭합니다.</p>
볼륨 편집(읽기-쓰기 볼륨만)	<p>a. 볼륨 관리 패널의 볼륨 작업 에서 * 볼륨 설정 편집 * 을 클릭합니다</p> <p>b. 볼륨의 스냅샷 정책, NFS 프로토콜 버전, NFS 액세스 제어 목록(엑스포트 정책) 또는 공유 권한을 수정한 다음 * 적용 * 을 클릭합니다.</p> <div data-bbox="609 1031 667 1094" style="border: 1px solid gray; border-radius: 50%; width: 36px; height: 36px; display: flex; align-items: center; justify-content: center; margin: 10px 0;"> <span style="font-size: 24px; font-weight: bold;">i</span> </div> <p style="margin-left: 40px;">사용자 지정 스냅샷 정책이 필요한 경우 System Manager를 사용하여 생성할 수 있습니다.</p>
볼륨을 삭제합니다	<p>a. Manage volumes(볼륨 관리) 패널의 Volume Actions(볼륨 작업) 에서 * Delete the volume(볼륨 삭제) * 을 클릭합니다.</p> <p>b. Delete Volume(볼륨 삭제) 창에서 삭제할 볼륨의 이름을 입력합니다.</p> <p>c. 확인하려면 * 삭제 * 를 다시 클릭합니다.</p>
필요 시 스냅샷 복사본을 생성합니다	<p>a. 볼륨 관리 패널의 보호 작업 에서 * 스냅샷 복사본 생성 * 을 클릭합니다.</p> <p>b. 필요한 경우 이름을 변경한 다음 * 만들기 * 를 클릭합니다.</p>
스냅샷 복사본에서 새 볼륨으로 데이터를 복원합니다	<p>a. Manage Volumes(볼륨 관리) 패널의 Protection Actions(보호 작업) 에서 * Restore from Snapshot copy(스냅샷 복사본에서 복원) * 를 클릭합니다.</p> <p>b. 스냅샷 복사본을 선택하고 새 볼륨의 이름을 입력한 다음 * 복원 * 을 클릭합니다.</p>

작업	조치
기본 디스크 유형을 변경합니다	<p>a. 볼륨 관리 패널의 고급 작업 아래에서 * 디스크 유형 변경 * 을 클릭합니다.</p> <p>b. 디스크 유형을 선택한 다음 * 변경 * 을 클릭합니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  BlueXP는 볼륨을 선택한 디스크 유형을 사용하는 기존 Aggregate로 이동하거나 볼륨에 대한 새 Aggregate를 생성합니다. </div>
계층화 정책을 변경합니다	<p>a. 볼륨 관리 패널의 고급 작업 에서 * 계층화 정책 변경 * 을 클릭합니다.</p> <p>b. 다른 정책을 선택하고 * 변경 * 을 클릭합니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  BlueXP는 계층화를 통해 선택한 디스크 유형을 사용하는 기존 Aggregate로 볼륨을 이동하거나 볼륨에 대한 새 Aggregate를 생성합니다. </div>
볼륨을 삭제합니다	<p>a. 볼륨을 선택한 다음 * 삭제 * 를 클릭합니다.</p> <p>b. 대화 상자에 볼륨의 이름을 입력합니다.</p> <p>c. 확인하려면 * 삭제 * 를 다시 클릭합니다.</p>

### 볼륨 크기를 조정합니다

기본적으로, 공간이 부족할 때 볼륨이 자동으로 최대 크기로 커집니다. 기본값은 1,000이며 이는 볼륨이 크기가 11배로 커질 수 있음을 의미합니다. 이 값은 커넥터 설정에서 구성할 수 있습니다.

볼륨 크기를 조정해야 하는 경우 에서 조정할 수 있습니다 "[ONTAP 시스템 관리자](#)". 볼륨 크기를 조정할 때 시스템의 용량 제한을 고려해야 합니다. 로 이동합니다 "[Cloud Volumes ONTAP 릴리즈 노트](#)" 를 참조하십시오.

### CIFS 서버를 수정합니다

DNS 서버 또는 Active Directory 도메인을 변경하는 경우 Cloud Volumes ONTAP에서 CIFS 서버를 수정하여 스토리지에서 클라이언트로 계속 서비스를 제공할 수 있도록 해야 합니다.

#### 단계

1. 작업 환경의 개요 탭에서 오른쪽 패널 아래의 기능 탭을 클릭합니다.
2. CIFS Setup(CIFS 설정) 필드에서 \* 연필 아이콘 \* 을 클릭하여 CIFS Setup(CIFS 설정) 창을 표시합니다.
3. CIFS 서버에 대한 설정을 지정합니다.

작업	조치
스토리지 VM(SVM) 선택	Cloud Volume ONTAP SVM(스토리지 가상 시스템)을 선택하면 구성된 CIFS 정보가 표시됩니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.

작업	조치
도메인에 가입하도록 승인된 자격 증명입니다	AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다.  나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.  Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.  엔디프::GCP[]
DNS 도메인	SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 대부분의 경우 도메인은 AD 도메인과 동일합니다.
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.  <ul style="list-style-type: none"> <li>• AWS 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=Computers, OU=Corp * 를 입력합니다.</li> <li>• Azure AD 도메인 서비스를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=ADDC 컴퓨터 * 또는 * OU=ADDC 사용자 * 를 입력합니다. "Azure 설명서: Azure AD 도메인 서비스 관리 도메인에 OU(조직 구성 단위)를 만듭니다"</li> <li>• Google 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=Computers, OU=Cloud * 를 입력합니다. "Google 클라우드 문서: Google Managed Microsoft AD의 조직 단위"</li> </ul>

4. Set \* 를 클릭합니다.

결과

Cloud Volumes ONTAP는 CIFS 서버를 변경 사항으로 업데이트합니다.

볼륨을 이동합니다

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

볼륨 및 대상 애그리게이트를 선택하고, 볼륨 이동 작업을 시작하고, 선택적으로 볼륨 이동 작업을 모니터링하여 System Manager에서 볼륨을 이동할 수 있습니다. System Manager를 사용하면 볼륨 이동 작업이 자동으로 완료됩니다.

단계

1. System Manager 또는 CLI를 사용하여 볼륨을 애그리게이트로 이동합니다.

대부분의 경우 System Manager를 사용하여 볼륨을 이동할 수 있습니다.

자세한 내용은 를 참조하십시오 ["ONTAP 9 볼륨 이동 익스프레스 가이드"](#).

**BlueXP에 작업 필요 메시지가 표시되면 볼륨을 이동합니다**

용량 문제를 방지하려면 볼륨을 이동해야 하지만 직접 문제를 해결해야 한다는 작업 필요 메시지가 BlueXP에 표시될 수 있습니다. 이 경우 문제를 해결하는 방법을 식별한 다음 하나 이상의 볼륨을 이동해야 합니다.



BlueXP는 총 사용 용량이 90%에 도달하면 이러한 작업 필요 메시지를 표시합니다. 데이터 계층화를 사용할 경우 aggregate가 80% 사용 용량에 도달하면 메시지가 표시됩니다. 기본적으로 10%의 여유 공간은 데이터 계층화로 예약되어 있습니다. ["데이터 계층화를 위한 여유 공간 비율에 대해 자세히 알아보십시오"](#).

단계

1. 용량 문제를 해결하는 방법 파악.
2. 분석을 기초로 용량 문제를 방지하려면 볼륨을 이동하십시오.
  - 용량 문제를 방지하려면 볼륨을 다른 시스템으로 이동합니다.
  - 용량 문제를 방지하려면 볼륨을 다른 애그리게이트로 이동하십시오.

용량 문제를 해결하는 방법 파악

용량 문제를 방지하기 위해 BlueXP에서 볼륨 이동을 위한 권장 사항을 제공할 수 없는 경우 이동해야 할 볼륨과 동일한 시스템의 다른 aggregate 또는 다른 시스템으로 볼륨을 이동해야 하는지 여부를 확인해야 합니다.

단계

1. Action Required 메시지의 고급 정보를 확인하여 용량 제한에 도달한 애그리게이트를 식별합니다.

예를 들어, 고급 정보에는 Aggregate aggr1이 용량 제한에 도달했음을 나타냅니다.
2. 애그리게이트에서 이동할 하나 이상의 볼륨을 식별합니다.
  - a. 작업 환경에서 \* 집계 탭 \* 을 클릭합니다.
  - b. 원하는 집계 타일로 이동한 다음 \*... (타원 아이콘) > 애그리게이트 세부 정보 보기 \*.
  - c. Aggregate Details(집계 세부 정보) 화면의 Overview(개요) 탭에서 각 볼륨의 크기를 검토하고 aggregate에서 이동할 볼륨을 하나 이상 선택합니다.

나중에 추가 용량 문제를 방지할 수 있도록 aggregate에서 여유 공간을 확보하기 위해 충분히 큰 볼륨을 선택해야 합니다.

Aggregate Details	
aggr1	
Overview	Capacity Allocation
State	online
Home Node	iblog1-01
Encryption Type	cloudEncrypted
Volumes	2 ^
	www_iblog1_root (1 GiB)
	DATA01 (500 GiB)

3. 시스템이 디스크 제한에 도달하지 않은 경우 볼륨을 동일한 시스템의 기존 애그리게이트 또는 새 aggregate로 이동해야 합니다.

자세한 내용은 [을 참조하십시오 용량 문제를 방지하려면 볼륨을 다른 애그리게이트로 이동하십시오.](#)

4. 시스템이 디스크 제한에 도달한 경우 다음 중 하나를 수행합니다.

- 사용하지 않는 볼륨을 모두 삭제합니다.
- 볼륨을 재정렬하여 Aggregate의 여유 공간을 확보하십시오.

자세한 내용은 [을 참조하십시오 용량 문제를 방지하려면 볼륨을 다른 애그리게이트로 이동하십시오.](#)

- 둘 이상의 볼륨을 공간이 있는 다른 시스템으로 이동합니다.

자세한 내용은 [을 참조하십시오 용량 문제를 방지하려면 볼륨을 다른 애그리게이트로 이동하십시오.](#)

용량 문제를 방지하려면 볼륨을 다른 시스템으로 이동합니다

용량 문제를 방지하기 위해 하나 이상의 볼륨을 다른 Cloud Volumes ONTAP 시스템으로 이동할 수 있습니다. 시스템이 디스크 제한에 도달한 경우 이 작업을 수행해야 할 수 있습니다.

이 작업에 대해

이 작업의 단계를 따라 다음 작업 필요 메시지를 수정할 수 있습니다.

용량 문제를 방지하려면 볼륨을 이동해야 하지만 시스템이 디스크 제한에 도달했으므로 BlueXP에서 이 작업을 수행할 수 없습니다.

단계



1. 사용 가능한 용량이 있는 Cloud Volumes ONTAP 시스템을 식별하거나 새 시스템을 구축합니다.

2. 타겟 작업 환경에서 소스 작업 환경을 끌어다 놓아 볼륨의 일회성 데이터 복제를 수행합니다.

자세한 내용은 을 참조하십시오 ["시스템 간 데이터 복제"](#).

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

자세한 내용은 을 참조하십시오 ["데이터 복제 일정 및 관계 관리"](#).

4. 데이터 액세스를 위한 볼륨을 구성합니다.

데이터 액세스를 위한 대상 볼륨을 구성하는 방법에 대한 자세한 내용은 를 참조하십시오 ["ONTAP 9 볼륨 재해 복구 익스프레스 가이드"](#).

5. 원래 볼륨을 삭제합니다.

자세한 내용은 을 참조하십시오 ["볼륨 관리"](#).

용량 문제를 방지하려면 볼륨을 다른 애그리게이트로 이동하십시오

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

이 작업에 대해

이 작업의 단계를 따라 다음 작업 필요 메시지를 수정할 수 있습니다.

용량 문제를 방지하려면 두 개 이상의 볼륨을 이동해야 하지만 BlueXP에서는 이 작업을 수행할 수 없습니다.

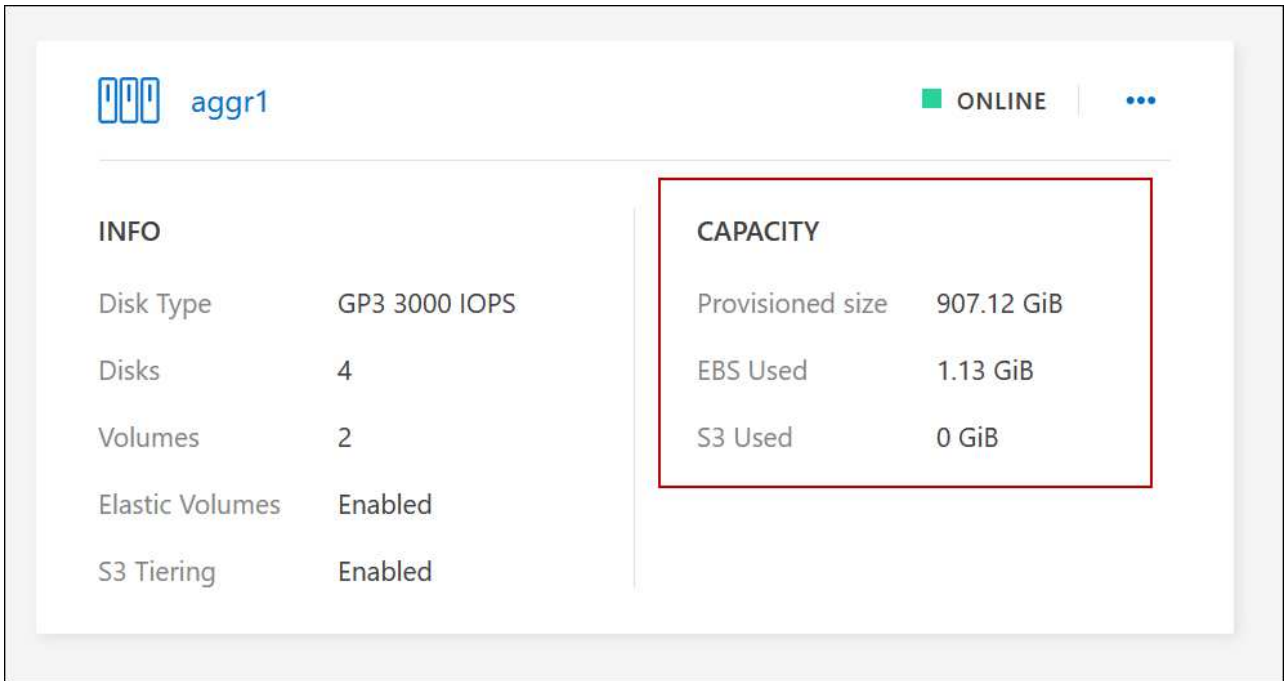
단계

1. 기존 Aggregate에 이동해야 하는 볼륨에 대해 사용 가능한 용량이 있는지 확인합니다.

a. 작업 환경에서 \* 집계 탭 \* 을 클릭합니다.

b. 원하는 집계 타일로 이동한 다음 \*... (타원 아이콘) > 애그리게이트 세부 정보 보기 \*.

c. 애그리게이트 타일에서 사용 가능한 용량(프로비저닝된 크기 - 사용된 애그리게이트 용량)을 확인합니다.



2. 필요한 경우 기존 애그리게이트에 디스크를 추가합니다.
  - a. 애그리게이트를 선택한 다음 \*... (타원 아이콘) > 디스크 추가 \*.
  - b. 추가할 디스크 수를 선택한 다음 \* 추가 \* 를 클릭합니다.
3. 가용 용량이 있는 애그리게이트가 없는 경우 새 애그리게이트를 생성합니다.  
자세한 내용은 을 참조하십시오 ["애그리게이트 생성"](#).
4. System Manager 또는 CLI를 사용하여 볼륨을 애그리게이트로 이동합니다.
5. 대부분의 경우 System Manager를 사용하여 볼륨을 이동할 수 있습니다.  
자세한 내용은 를 참조하십시오 ["ONTAP 9 볼륨 이동 익스프레스 가이드"](#).

#### 볼륨 이동이 느리게 수행될 수 있는 이유

Cloud Volumes ONTAP에 대해 다음 조건 중 하나가 참인 경우 볼륨을 이동하는 데 예상보다 시간이 오래 걸릴 수 있습니다.

- 볼륨이 클론입니다.
- 볼륨이 클론의 부모입니다.
- 소스 또는 대상 Aggregate에는 단일 Throughput Optimized HDD(st1) 디스크가 있습니다.
- 애그리게이트 중 하나에서 객체에 대해 이전 명명 체계를 사용합니다. 두 애그리게이트 모두에서 같은 이름 형식을 사용해야 합니다.

9.4 릴리즈 이전 버전에서 데이터 계층화가 애그리게이트에서 활성화된 경우 이전 명명 체계가 사용됩니다.

- 소스 및 대상 애그리게이트에서 암호화 설정이 일치하지 않거나 키를 다시 입력하다
- 계층화 정책을 변경하기 위해 볼륨 이동에 `_-Tiering-policy_option`이 지정되었습니다.

- 볼륨 이동 시 `_generate-destination-key_option`이 지정되었습니다.

## FlexGroup 볼륨을 봅니다

CLI 또는 System Manager를 통해 생성된 FlexGroup 볼륨은 BlueXP의 볼륨 탭을 통해 직접 볼 수 있습니다. FlexVol 볼륨에 대해 제공된 정보와 동일한 BlueXP는 전용 볼륨 타일을 통해 생성된 FlexGroup 볼륨에 대한 자세한 정보를 제공합니다. 볼륨 타일에서 아이콘의 호버 텍스트를 통해 각 FlexGroup 볼륨 그룹을 식별할 수 있습니다. 또한 볼륨 스타일 열을 통해 볼륨 목록 보기에서 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			



현재 BlueXP에서만 기존 FlexGroup 볼륨을 볼 수 있습니다. BlueXP에서 FlexGroup 볼륨을 생성하는 기능은 사용할 수 없지만 향후 릴리스에서 제공될 예정입니다.

## 비활성 데이터를 저비용 오브젝트 스토리지로 계층화

사용 빈도가 높은 데이터를 위한 SSD 또는 HDD 성능 계층과 비활성 데이터를 위한 오브젝트 스토리지 용량 계층을 결합하여 Cloud Volumes ONTAP의 스토리지 비용을 절감할 수 있습니다. 데이터 계층화는 FabricPool 기술을 기반으로 합니다. 개괄적인 개요는 을 참조하십시오 ["데이터 계층화 개요"](#).

데이터 계층화를 설정하려면 다음을 수행해야 합니다.

1

지원되는 구성을 선택합니다

대부분의 구성은 지원됩니다. 최신 버전을 실행하는 Cloud Volumes ONTAP 시스템이 있는 경우 실행하는 것이 좋습니다. ["자세한 정보"](#).

2

Cloud Volumes ONTAP와 오브젝트 스토리지 간의 연결을 보장합니다

- AWS의 경우 S3에 VPC 엔드 포인트가 필요합니다. [자세한 정보](#).
- Azure의 경우 BlueXP에 필요한 권한이 있으면 아무 작업도 수행할 필요가 없습니다. [자세한 정보](#).
- Google Cloud의 경우, 전용 Google Access에 대한 서브넷을 구성하고 서비스 계정을 설정해야 합니다. [자세한 정보](#).

3

계층화가 설정된 **Aggregate**가 있는지 확인합니다

볼륨에서 데이터 계층화를 사용하려면 애그리게이트에서 데이터 계층화를 활성화해야 합니다. 새 볼륨 및 기존 볼륨에 대한 요구사항을 알고 있어야 합니다. [자세한 정보](#).

4

볼륨을 생성, 수정 또는 복제할 때 계층화 정책을 선택합니다

볼륨을 생성, 수정 또는 복제할 때 BlueXP에서 계층화 정책을 선택하라는 메시지가 표시됩니다.

- "읽기-쓰기 볼륨의 데이터 계층화"
- "데이터 보호 볼륨의 데이터 계층화"

i

데이터 계층화에 필요하지 않은'은 무엇입니까?

- 데이터 계층화를 사용하기 위해 기능 라이선스를 설치할 필요가 없습니다.
- 용량 계층에 대해 오브젝트 저장소를 생성할 필요가 없습니다. BlueXP가 이러한 작업을 수행합니다.
- 시스템 레벨에서 데이터 계층화를 설정할 필요가 없습니다.

BlueXP는 시스템이 생성될 때 콜드 데이터에 대한 오브젝트 저장소를 생성합니다. [연결 또는 사용 권한 문제가 없는 경우](#). 그런 다음 볼륨에 대해 데이터 계층화를 활성화해야 합니다. 경우에 따라 [애그리게이트](#))를 클릭합니다.

데이터 계층화를 지원하는 구성

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

**AWS** 지원

- Cloud Volumes ONTAP 9.2부터 AWS에서 데이터 계층화가 지원됩니다.
- 성능 계층은 범용 SSD(GP3 또는 GP2) 또는 프로비저닝된 IOPS SSD(io1)일 수 있습니다.

i

처리량 최적화 HDD(st1)를 사용하는 경우에는 데이터를 오브젝트 스토리지에 계층화하지 않는 것이 좋습니다.

**Azure**에서 지원

- 데이터 계층화는 다음과 같이 Azure에서 지원됩니다.
  - 단일 노드 시스템의 경우 버전 9.4인치
  - HA 쌍이 포함된 버전 9.6인치

- 성능 계층은 프리미엄 SSD 관리 디스크, 표준 SSD 관리 디스크 또는 표준 HDD 관리 디스크일 수 있습니다.

#### Google Cloud 지원

- 데이터 계층화는 Cloud Volumes ONTAP 9.6부터 Google Cloud에서 지원됩니다.
- 성능 계층은 SSD 영구 디스크, 균형 잡힌 영구 디스크 또는 표준 영구 디스크일 수 있습니다.

#### 기능 상호 운용성

- 데이터 계층화는 암호화 기술을 통해 지원됩니다.
- 볼륨에 씬 프로비저닝이 설정되어 있어야 합니다.

#### 요구 사항

클라우드 공급자에 따라 Cloud Volumes ONTAP에서 콜드 데이터를 오브젝트 스토리지에 계층화할 수 있도록 특정 연결과 사용 권한을 설정해야 합니다.

#### 콜드 데이터를 **AWS S3**에 계층화해야 하는 요구 사항

Cloud Volumes ONTAP가 S3에 연결되어 있는지 확인합니다. 이 연결을 제공하는 가장 좋은 방법은 S3 서비스에 VPC 엔드포인트를 생성하는 것입니다. 자세한 내용은 [을 참조하십시오 "AWS 설명서: 게이트웨이 엔드포인트 생성"](#).

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

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

#### 콜드 데이터를 **Azure Blob** 저장소에 계층화하기 위한 요구사항

BlueXP에 필요한 권한이 있는 경우 성능 계층과 용량 계층 간에 연결을 설정할 필요가 없습니다. BlueXP는 Connector의 사용자 지정 역할에 다음과 같은 권한이 있는 경우 VNET 서비스 끝점을 활성화합니다.

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

사용 권한은 기본적으로 사용자 지정 역할에 포함됩니다. ["Connector에 대한 Azure 권한을 봅니다"](#)

#### 콜드 데이터를 **Google Cloud Storage** 버킷에 계층화해야 하는 요구 사항

- Cloud Volumes ONTAP가 상주하는 서브넷은 개인 Google 액세스용으로 구성해야 합니다. 자세한 지침은 [을 참조하십시오 "Google Cloud 설명서: 개인 Google Access 구성"](#).
- 서비스 계정을 Cloud Volumes ONTAP에 연결해야 합니다.

["이 서비스 계정을 설정하는 방법에 대해 알아보십시오"](#).

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

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

- 고객이 관리하는 암호화 키로 버킷을 암호화하려면 Google Cloud 스토리지 버킷에서 키를 사용할 수 있습니다.

["Cloud Volumes ONTAP에서 고객이 관리하는 암호화 키를 사용하는 방법에 대해 알아보십시오"](#).

요구사항을 구현한 후 데이터 계층화를 사용하도록 설정

BlueXP는 연결 또는 사용 권한 문제가 없는 한 시스템이 생성될 때 콜드 데이터에 대한 개체 저장소를 생성합니다. 시스템을 생성하기 전까지는 위에 나열된 요구 사항을 구현하지 않았다면 개체 저장소를 생성하는 API 또는 System Manager를 통해 계층화를 수동으로 활성화해야 합니다.



BlueXP 사용자 인터페이스를 통해 계층화를 활성화하는 기능은 향후 Cloud Volumes ONTAP 릴리스에서 제공될 예정입니다.

애그리게이트에서 계층화가 설정되었는지 확인합니다

볼륨에서 데이터 계층화를 사용하려면 애그리게이트에서 데이터 계층화를 활성화해야 합니다. 새 볼륨 및 기존 볼륨에 대한 요구사항을 알고 있어야 합니다.

- \* 새 볼륨 \*

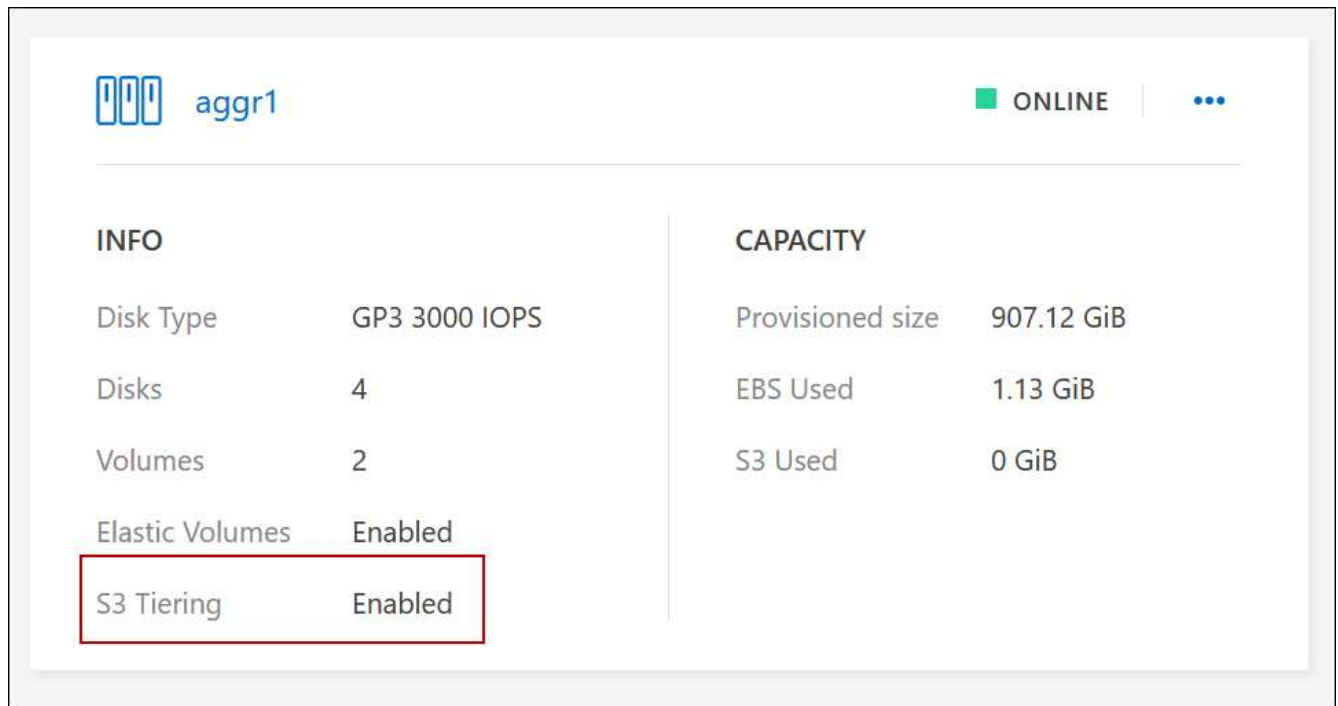
새 볼륨에서 데이터 계층화를 사용하는 경우에는 애그리게이트에서 데이터 계층화를 사용할 필요가 없습니다. BlueXP는 계층화가 활성화된 기존 애그리게이트에 볼륨을 생성하거나, 데이터 계층화가 활성화된 애그리게이트가 아직 존재하지 않는 경우 볼륨에 대한 새 애그리게이트를 생성합니다.

- \* 기존 볼륨 \*

기존 볼륨에서 데이터 계층화를 사용하려면 기본 애그리게이트에 데이터 계층화가 설정되어 있는지 확인해야 합니다. 기존 애그리게이트에서 데이터 계층화를 사용하지 않는 경우 System Manager를 사용하여 기존 애그리게이트를 오브젝트 저장소에 연결해야 합니다.

**Aggregate**에서 계층화가 설정되었는지 확인하는 단계입니다

1. BlueXP에서 작업 환경을 엽니다.
2. 애그리게이트 탭을 클릭합니다.
3. 원하는 타일로 이동하여 애그리게이트에서 계층화가 설정되었는지 여부를 확인합니다.



Aggregate에서 계층화를 활성화하는 단계입니다

1. System Manager에서 \* Storage > Tiers \* 를 클릭합니다.
2. Aggregate에 대한 작업 메뉴를 클릭하고 \* Attach Cloud Tiers \* 를 선택합니다.
3. 연결할 클라우드 계층을 선택하고 \* 저장 \* 을 클릭합니다.

다음 단계

이제 다음 섹션에 설명된 대로 새 볼륨과 기존 볼륨에 대해 데이터 계층화를 설정할 수 있습니다.

읽기-쓰기 볼륨의 데이터 계층화

Cloud Volumes ONTAP는 읽기-쓰기 볼륨의 비활성 데이터를 비용 효율적인 오브젝트 스토리지에 계층화하여 핫 데이터에 대한 성능 계층을 확보할 수 있습니다.

단계

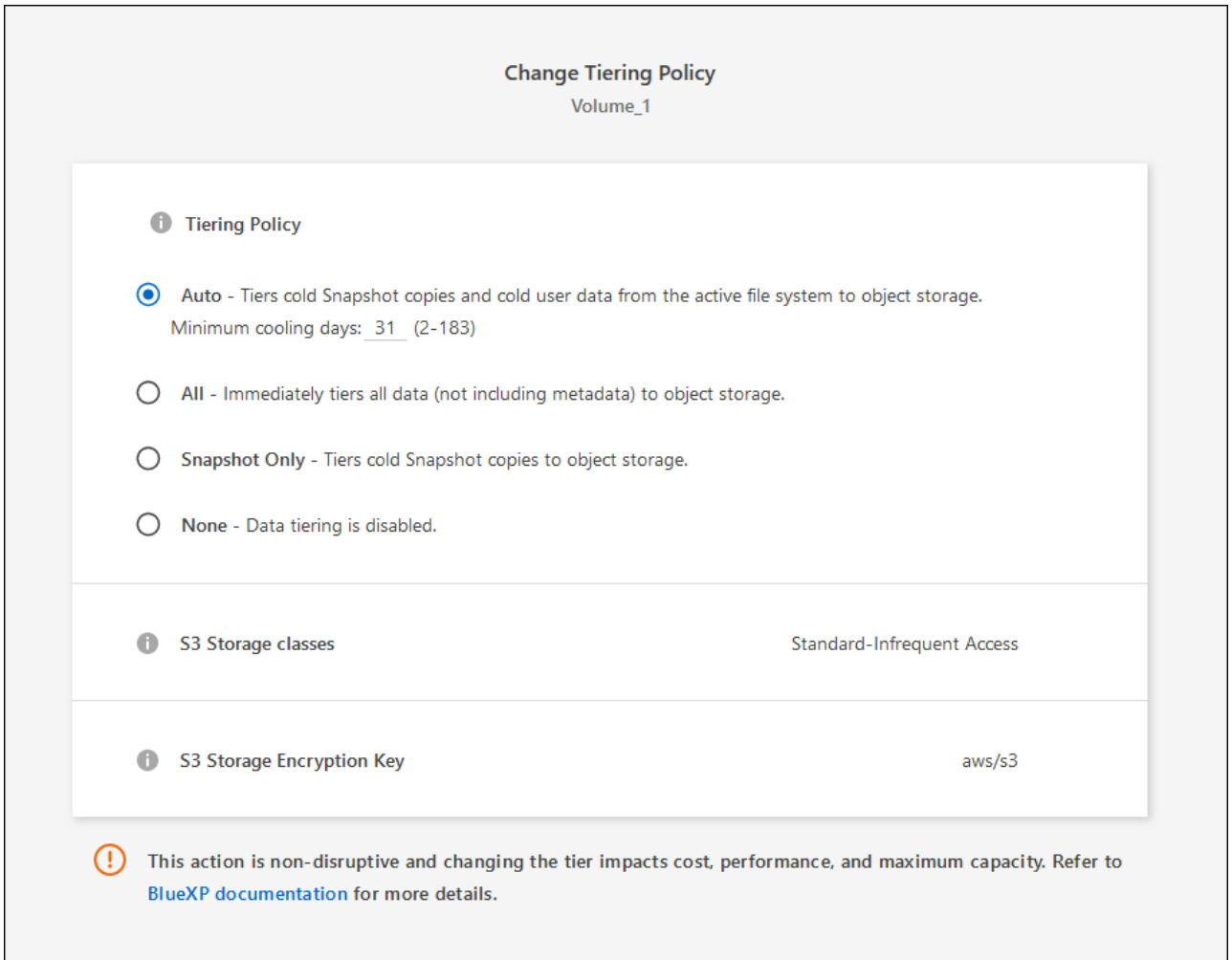
1. 작업 환경의 볼륨 탭에서 새 볼륨을 생성하거나 기존 볼륨의 계층을 변경합니다.

작업	조치
새 볼륨을 생성합니다	새 볼륨 추가 * 를 클릭합니다.
기존 볼륨을 수정합니다	원하는 볼륨 타일을 선택하고 * 볼륨 관리 * 를 클릭하여 볼륨 관리 오른쪽 패널에 액세스한 다음 오른쪽 패널에서 * 고급 작업 * 및 * 계층화 정책 변경 * 을 클릭합니다.

2. 계층화 정책을 선택합니다.

이러한 정책에 대한 설명은 를 참조하십시오 ["데이터 계층화 개요"](#).

- 예 \*



데이터 계층화가 활성화된 애그리게이트가 아직 존재하지 않는 경우 BlueXP는 볼륨에 대한 새로운 애그리게이트를 생성합니다.

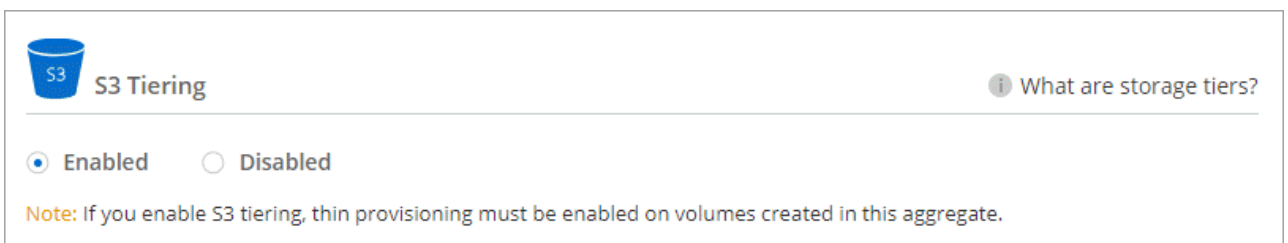
### 데이터 보호 볼륨에서 데이터 계층화

Cloud Volumes ONTAP는 데이터 보호 볼륨의 데이터를 용량 계층으로 계층화할 수 있습니다. 대상 볼륨을 활성화하면 데이터가 읽혀지면서 성능 계층으로 서서히 이동합니다.

### 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 소스 볼륨이 포함된 작업 환경을 선택한 다음 볼륨을 복제할 작업 환경으로 끌어다 놓습니다.
3. 표시되는 메시지에 따라 계층화 페이지로 이동한 다음 오브젝트 스토리지에 데이터 계층화를 설정합니다.

◦ 예 \*





데이터 복제에 대한 도움말은 을 참조하십시오 "[클라우드 간 데이터 복제](#)".

### 계층화된 데이터에 대한 스토리지 클래스 변경

Cloud Volumes ONTAP를 구축한 후 30일 동안 액세스하지 않은 비활성 데이터의 스토리지 클래스를 변경하여 스토리지 비용을 절감할 수 있습니다. 데이터에 액세스하는 경우 액세스 비용이 더 높아지므로 스토리지 클래스를 변경하기 전에 액세스 비용을 고려해야 합니다.

계층형 데이터를 위한 스토리지 클래스는 시스템 전체에 적용됩니다. 즉, 볼륨을 기준으로 하지 않습니다.

지원되는 스토리지 클래스에 대한 자세한 내용은 를 참조하십시오 "[데이터 계층화 개요](#)".

#### 단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 \* 스토리지 클래스 \* 또는 \* Blob 스토리지 계층화 \* 를 클릭합니다.
2. 스토리지 클래스를 선택한 다음 \* 저장 \* 을 클릭합니다.

### 데이터 계층화의 사용 가능한 공간 비율을 변경합니다

데이터 계층화를 위한 여유 공간 비율은 데이터를 오브젝트 스토리지로 계층화할 때 Cloud Volumes ONTAP SSD/HDD에 필요한 여유 공간을 정의합니다. 기본 설정은 10%의 여유 공간이지만 요구 사항에 따라 설정을 조정할 수 있습니다.

예를 들어, 구입한 용량을 사용하기 위해 10% 미만의 여유 공간을 선택할 수 있습니다. 그런 다음 BlueXP는 추가 용량이 필요할 때 추가 디스크를 구입할 수 있습니다(최대 Aggregate의 디스크 한도에 도달할 때까지).

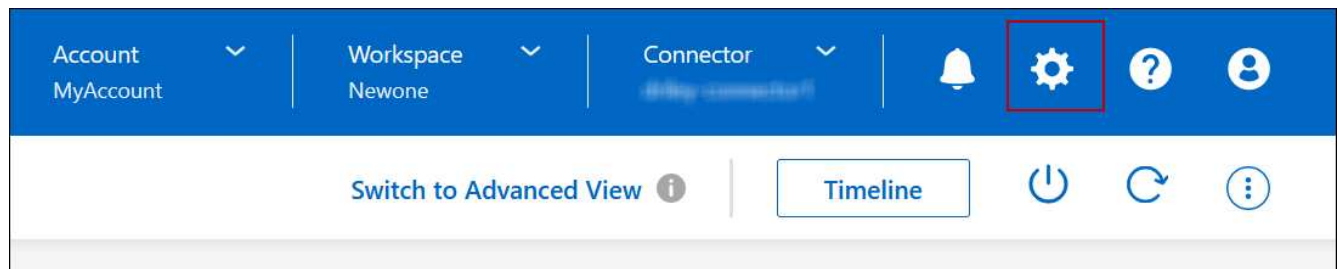


공간이 부족하면 Cloud Volumes ONTAP에서 데이터를 이동할 수 없어 성능이 저하될 수 있습니다. 모든 변경은 신중하게 수행해야 합니다. 확실하지 않은 경우 NetApp 지원 팀에 연락하여 안내를 받으십시오.

이 비율은 오브젝트 저장소에서 데이터를 읽을 때 Cloud Volumes ONTAP 더 나은 성능을 제공하기 위해 데이터를 SSD/HDD로 이동하기 때문에 재해 복구 시나리오에 중요합니다. 공간이 부족하면 Cloud Volumes ONTAP에서 데이터를 이동할 수 없습니다. 이 점을 고려하여 비율을 변경하면 비즈니스 요구 사항을 충족할 수 있습니다.

#### 단계

1. BlueXP 콘솔의 오른쪽 상단에서 \* 설정 \* 아이콘을 클릭하고 \* 커넥터 설정 \* 을 선택합니다.



2. Capacity \* 에서 \* Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering \* 을 클릭합니다.
3. 요구 사항에 따라 여유 공간 비율을 변경하고 \* Save \* 를 클릭합니다.

## 자동 계층화 정책의 냉각 기간 변경

Cloud Volumes ONTAP 볼륨에서 `_auto_Tiering` 정책을 사용하여 데이터 계층화를 활성화한 경우 비즈니스 요구에 따라 기본 냉각 기간을 조정할 수 있습니다. 이 작업은 API 및 CLI에서만 지원됩니다.

냉각 기간은 볼륨의 사용자 데이터가 "콜드" 상태로 간주되어 오브젝트 스토리지로 이동되기 전에 비활성 상태로 유지해야 하는 일 수입니다.

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

- 9.8 이상: 2일에서 183일
- 9.7 이하: 2일~63일

### 단계

1. 볼륨을 생성하거나 기존 볼륨을 수정할 때 API 요청과 함께 `_minimumCoolingDays_` 매개 변수를 사용하십시오.

## LUN을 호스트에 연결합니다

iSCSI 볼륨을 생성할 때 BlueXP에서 자동으로 LUN을 생성합니다. NetApp은 볼륨당 하나의 LUN만 생성하므로 관리가 필요하지 않습니다. 볼륨을 생성한 후 IQN을 사용하여 호스트에서 LUN에 연결합니다.

다음 사항에 유의하십시오.

- BlueXP의 자동 용량 관리는 LUN에 적용되지 않습니다. BlueXP에서 LUN을 생성하면 자동 확장 기능이 비활성화됩니다.
- System Manager 또는 CLI에서 추가 LUN을 생성할 수 있습니다.

### 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 볼륨을 관리할 Cloud Volumes ONTAP 작업 환경을 두 번 클릭합니다.
3. 작업 환경에서 \* Volumes \* 탭을 클릭합니다.
4. Volumes(볼륨) 탭에서 원하는 볼륨 제목으로 이동한 다음 \* Manage volume(볼륨 관리) \* 을 클릭하여 Manage Volumes(볼륨 관리) 오른쪽 패널에 액세스합니다.
5. 대상 IQN \* 을 클릭합니다.
6. IQN 이름을 복사하려면 \* Copy \* 를 클릭합니다.
7. 호스트에서 LUN으로의 iSCSI 접속을 설정합니다.
  - ["Red Hat Enterprise Linux용 ONTAP 9 iSCSI Express 구성: 대상으로 iSCSI 세션 시작"](#)
  - ["Windows용 ONTAP 9 iSCSI Express 구성: 타겟으로 iSCSI 세션 시작"](#)
  - ["ONTAP SAN 호스트 구성"](#)

## FlexCache 볼륨을 사용하여 데이터 액세스 가속화

FlexCache 볼륨은 원본(또는 소스) 볼륨에서 SMB 및 NFS 읽기 데이터를 캐싱하는 스토리지 볼륨입니다. 이후에 캐싱된 데이터를 읽으면 해당 데이터에 더 빠르게 액세스할 수 있습니다.

FlexCache 볼륨을 사용하면 데이터 액세스 속도를 높이거나 자주 액세스하는 볼륨에서 트래픽을 오프로드할 수 있습니다. FlexCache 볼륨은 원본 볼륨에 액세스하지 않고도 직접 데이터를 제공할 수 있으므로 클라이언트가 동일한 데이터에 반복적으로 액세스해야 할 때 성능을 개선할 수 있습니다. FlexCache 볼륨은 읽기 집약적인 시스템 워크로드에 적합합니다.

BlueXP는 를 사용하여 FlexCache 볼륨을 관리할 수 있는 기능을 제공합니다 "BlueXP 볼륨 캐싱" 서비스.

ONTAP CLI 또는 ONTAP System Manager를 사용하여 FlexCache 볼륨을 생성하고 관리할 수도 있습니다.

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

BlueXP는 모든 새로운 Cloud Volumes ONTAP 시스템에 대한 FlexCache 라이선스를 생성합니다. 이 라이선스에는 500GiB 사용 제한이 포함됩니다.



## 통합 관리

### 애그리게이트 생성

볼륨을 생성할 때 직접 애그리게이트를 생성하거나 BlueXP에서 자동으로 집계하도록 할 수 있습니다. 애그리게이트를 직접 생성할 때의 이점은 기본 디스크 크기를 선택할 수 있다는 것입니다. 이를 통해 필요한 용량 또는 성능에 맞게 애그리게이트 크기를 조정할 수 있습니다.



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

## 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 집계를 관리할 Cloud Volumes ONTAP 인스턴스의 이름을 두 번 클릭합니다.
3. 애그리게이트 탭에서 \* 애그리게이트 추가 \* 를 클릭한 다음 애그리게이트의 세부 정보를 지정합니다.

## 설치하고

- 디스크 유형과 디스크 크기를 선택하라는 메시지가 표시되면 을 참조하십시오 "[AWS에서 Cloud Volumes ONTAP 구성 계획](#)".
- 애그리게이트의 용량 크기를 입력하라는 메시지가 표시되면 Amazon EBS Elastic Volumes 기능을 지원하는 구성에 애그리게이트를 생성합니다. 다음 스크린샷은 GP3 디스크로 구성된 새로운 Aggregate의 예를 보여줍니다.

1 Disk Type   2 Aggregate details   3 Tiering Data   4 Review

### Select Disk Type

Disk Type

GP3 - General Purpose SSD Dynamic Performance

General Purpose SSD (gp3) Disk Properties

**Description:** General purpose SSD volume that balances price and performance (performance level is independent of storage capacity)

IOPS Value     Throughput MB/s  

12000     250  

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

## Azure를 지원합니다

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

## Google 클라우드

디스크 유형 및 디스크 크기에 대한 도움말은 을 참조하십시오 "[Google Cloud에서 Cloud Volumes ONTAP 구성을 계획하십시오](#)".

4. Go \* 를 클릭한 다음 \* Approve and Purchase \* 를 클릭합니다.

## 애그리게이트 관리

디스크를 추가하고, 애그리게이트에 대한 정보를 확인하고, 삭제하여 애그리게이트를 직접 관리하십시오.



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

시작하기 전에

Aggregate를 삭제하려면 먼저 Aggregate의 볼륨을 삭제해야 합니다.

이 작업에 대해


Aggregate에 공간이 부족할 경우 System Manager를 사용하여 볼륨을 다른 애그리게이트로 이동할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 집계를 관리할 Cloud Volumes ONTAP 작업 환경을 두 번 클릭합니다.
3. 작업 환경에서 \* 집계 \* 탭을 클릭합니다.
4. 애그리게이트 탭에서 원하는 제목으로 이동한 다음 \*... (타원 아이콘) \*.

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		

5. 애그리게이트 관리:

작업	조치
Aggregate에 대한 정보를 봅니다	아래에서... (타원 아이콘) 메뉴에서 * 애그리게이트 세부 정보 보기 * 를 클릭합니다.
특정 Aggregate에 볼륨을 생성합니다	아래에서... (타원 아이콘) 메뉴에서 * 볼륨 추가 * 를 클릭합니다.
Aggregate에 디스크를 추가합니다	<p>a. 아래에서... (타원 아이콘) 메뉴에서 * 디스크 추가 * 를 클릭합니다.</p> <p>b. 추가할 디스크 수를 선택하고 * 추가 * 를 클릭합니다.</p> <p> Aggregate의 모든 디스크는 동일한 크기여야 합니다.</p>
Amazon EBS Elastic Volumes를 지원하는 애그리게이트의 용량을 늘립니다	<p>a. 아래에서... (타원 아이콘) 메뉴에서 * 용량 증가 * 를 클릭합니다.</p> <p>b. 추가할 추가 용량을 입력한 다음 * 증가 * 를 클릭합니다.</p> <p>Aggregate의 용량을 최소 256GiB 또는 애그리게이트 크기의 10% 이상으로 늘려야 합니다.</p> <p>예를 들어 1.77TiB Aggregate가 있는 경우 10%는 181GiB입니다. 이 값이 256GiB보다 낮으므로 애그리게이트의 크기를 최소 256GiB까지 늘려야 합니다.</p>
애그리게이트 삭제	<p>a. 볼륨을 포함하지 않는 집계 타일을 선택합니다. *...를 클릭합니다. (타원 아이콘) &gt; 삭제 *.</p> <p>b. 확인하려면 * 삭제 * 를 다시 클릭합니다.</p>

## 커넥터의 용량 설정을 관리합니다

각 커넥터에는 Cloud Volumes ONTAP의 총 용량을 관리하는 방법을 결정하는 설정이 있습니다.

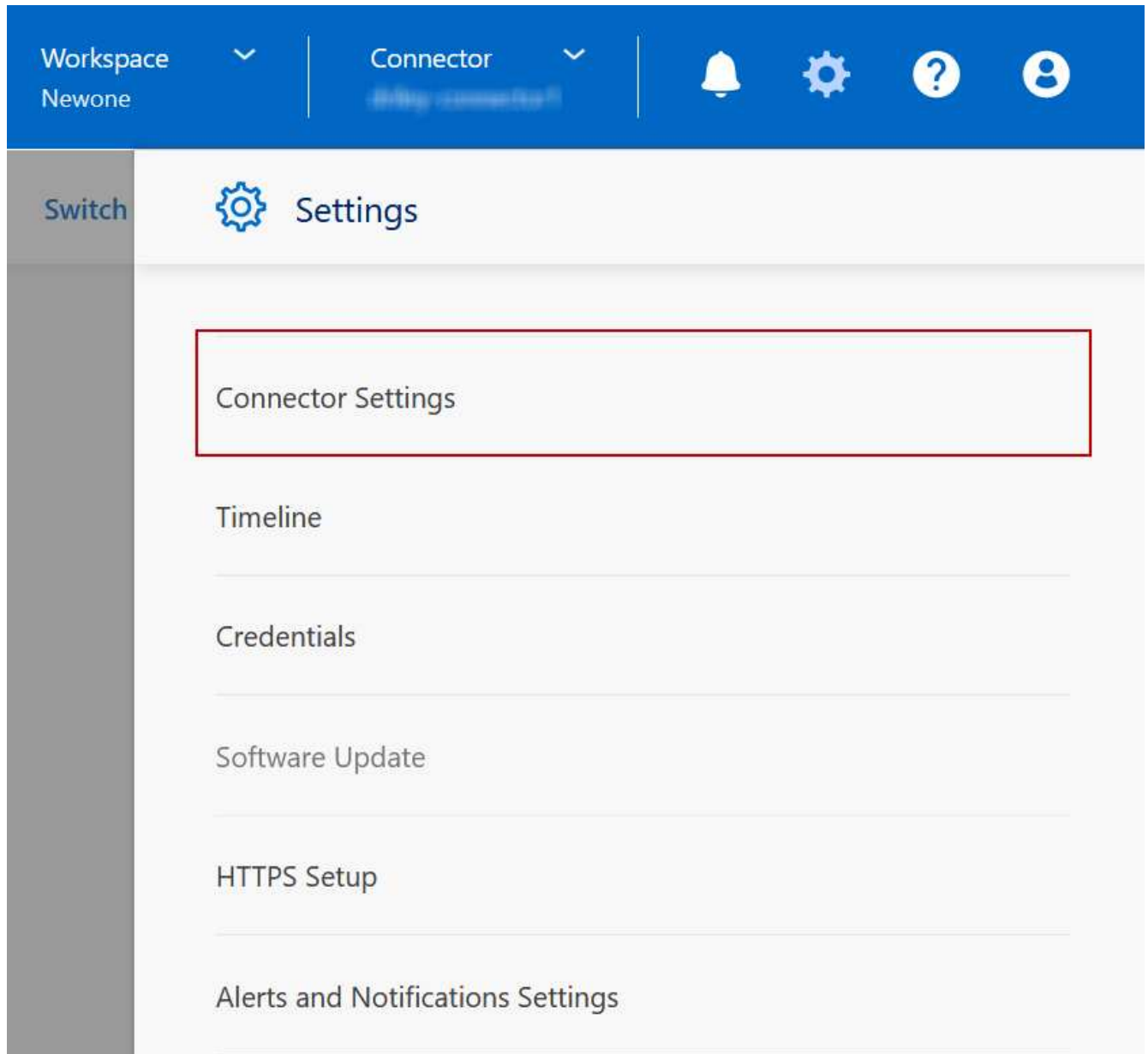
이러한 설정은 커넥터에 의해 관리되는 모든 Cloud Volumes ONTAP 시스템에 영향을 줍니다. 다른 커넥터가 있는 경우 다르게 구성할 수 있습니다.

### 필수 권한

커넥터 설정을 수정하려면 계정 관리자 권한이 필요합니다.

### 단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 클릭하고 \* 커넥터 설정 \* 을 선택합니다.



2. Capacity \* 에서 다음 설정을 수정합니다.

#### 용량 관리 모드

BlueXP에서 스토리지 용량 결정을 통지할지 아니면 BlueXP에서 자동으로 용량 요구 사항을 관리할지 여부를 선택합니다.

["용량 관리 모드의 작동 방식에 대해 알아보십시오"](#).

#### 애그리게이트 용량 임계값 - 사용 가능한 공간 비율

Aggregate의 여유 공간 비율이 지정된 임계값 아래로 떨어지면 알림을 트리거합니다.

여유 공간 비율은 다음과 같이 계산됩니다.

$(\text{Aggregate capacity} - \text{애그리게이트에서 사용하는 총 용량}) / \text{애그리게이트 용량}$



## Aggregate Capacity Thresholds - Data Tiering의 여유 공간 비율입니다

데이터를 용량 계층(오브젝트 스토리지)으로 계층화할 때 성능 계층(디스크)에 필요한 여유 공간을 정의합니다.

이 비율은 재해 복구 시나리오에 중요합니다. 용량 계층에서 데이터를 읽으면 Cloud Volumes ONTAP는 더 나은 성능을 제공하기 위해 데이터를 성능 계층으로 이동합니다. 공간이 부족하면 Cloud Volumes ONTAP에서 데이터를 이동할 수 없습니다.

3. 저장 \* 을 클릭합니다.

## 스토리지 VM 관리

### BlueXP에서 스토리지 VM 관리

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에 스토리지 및 데이터 서비스를 제공합니다. 이를 SVM 또는 `_vserver_`로 알고 있을 수 있습니다. Cloud Volumes ONTAP는 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다.

지원되는 스토리지 VM 수입니다

특정 구성에서는 여러 스토리지 VM이 지원됩니다. 로 이동합니다 "[Cloud Volumes ONTAP 릴리즈 노트](#)" 사용 중인 Cloud Volumes ONTAP 버전에 대해 지원되는 스토리지 VM 수를 확인하려면 다음을 수행합니다.

여러 스토리지 VM과 함께 작업

BlueXP는 System Manager 또는 CLI에서 생성한 추가 스토리지 VM을 지원합니다.

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

### Details & Protection

Storage VM Name ?

svm\_name1 ▼

Volume Name Size (GiB) ?

Snapshot Policy

default ▼

? Default Policy

다음 이미지는 다른 시스템으로 볼륨을 복제할 때 스토리지 VM을 선택하는 방법을 보여 줍니다.

Destination Volume Name

volume\_copy

Destination Storage VM Name

svm\_name1 ▼

Destination Aggregate

Automatically select the best aggregate ▼

기본 스토리지 **VM**의 이름을 수정합니다

BlueXP는 Cloud Volumes ONTAP용으로 생성한 단일 스토리지 VM의 이름을 자동으로 지정합니다. 엄격한 명명 규칙이 있는 경우 System Manager, CLI 또는 API에서 스토리지 VM 이름을 수정할 수 있습니다. 예를 들어, 이름이 ONTAP 클러스터에 대한 스토리지 VM의 이름을 지정하는 방법과 일치할 수 있습니다.

## AWS에서 Cloud Volumes ONTAP를 위한 데이터 서비스 스토리지 VM을 생성합니다

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에 스토리지 및 데이터 서비스를 제공합니다. 이를 SVM 또는 `_vserver_`로 알고 있을 수 있습니다. Cloud Volumes ONTAP는 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다.

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

지원되는 스토리지 VM 수입니다

9.7 릴리즈부터 특정 Cloud Volumes ONTAP 구성에서 여러 스토리지 VM이 지원됩니다. 로 이동합니다 ["Cloud Volumes ONTAP 릴리즈 노트"](#) 사용 중인 Cloud Volumes ONTAP 버전에 대해 지원되는 스토리지 VM 수를 확인하려면 다음을 수행합니다.

다른 모든 Cloud Volumes ONTAP 구성에서는 재해 복구에 사용되는 1개의 데이터 서비스 스토리지 VM과 1개의 대상 스토리지 VM을 지원합니다. 소스 스토리지 VM에 중단이 발생할 경우 데이터 액세스를 위해 대상 스토리지 VM을 활성화할 수 있습니다.

구성에 대한 제한을 확인합니다

각 EC2 인스턴스는 네트워크 인터페이스당 최대 수의 전용 IPv4 주소를 지원합니다. 새 스토리지 VM에 대해 AWS에서 IP 주소를 할당하기 전에 한도를 확인해야 합니다.

단계

1. 로 이동합니다 ["Cloud Volumes ONTAP 릴리즈 노트의 스토리지 제한 사항 섹션을 참조하십시오"](#).
2. 인스턴스 유형에 대한 인터페이스당 최대 IP 주소 수를 식별합니다.
3. AWS에서 IP 주소를 할당할 때 다음 섹션에서 필요하므로 이 번호를 기록해 두십시오.

**AWS에서 IP 주소를 할당합니다**

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

스토리지 VM을 위한 선택적 관리 LIF는 단일 노드 시스템과 단일 AZ의 HA 쌍에서 프라이빗 IP 주소를 필요로 합니다. 이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

단계

1. AWS에 로그인하고 EC2 서비스를 엽니다.
2. Cloud Volumes ONTAP 인스턴스를 선택하고 \* 네트워크 \* 을 클릭합니다.  
  
HA 쌍에서 스토리지 VM을 생성하는 경우 노드 1을 선택합니다.
3. 아래로 \* 네트워크 인터페이스 \* 로 스크롤하고 포트 e0a의 \* 인터페이스 ID \* 를 클릭합니다.

Name	Insta...	Instance state	Instance type	Status check
<input type="checkbox"/> danielleAws	i-070...	Running	m5.2xlarge	2/2 check
<input type="checkbox"/> occmTiering0702	i-0a7...	Stopped	m5.2xlarge	-
<input checked="" type="checkbox"/> cvoTiering1	i-02a...	Stopped	m5.2xlarge	-

Interface ID	Description
<input checked="" type="checkbox"/> <a href="#">eni-07c301...</a>	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 주소 확인:
  - a. 할당된 IP 주소의 수를 세어하여 포트에 추가 IP를 위한 공간이 있는지 확인합니다.  
이 페이지의 이전 섹션에서 인터페이스당 지원되는 최대 IP 주소 수를 확인해야 합니다.
  - b. 선택 사항: Cloud Volumes ONTAP용 CLI로 이동하여 \* network interface show \* 를 실행하여 각 IP 주소가 사용 중인지 확인합니다.  
IP 주소를 사용하지 않는 경우 새 스토리지 VM에서 사용할 수 있습니다.
7. AWS 콘솔로 돌아가서 \* Assign new IP address \* 를 클릭하여 새 스토리지 VM에 필요한 양에 따라 추가 IP 주소를 할당합니다.
  - 단일 노드 시스템: 사용되지 않는 1개의 보조 전용 IP가 필요합니다.  
스토리지 VM에 관리 LIF를 생성하려면 선택적인 보조 프라이빗 IP가 필요합니다.
  - 단일 AZ의 HA 쌍: 노드 1에 사용되지 않는 2차 프라이빗 IP가 1개 필요합니다.  
스토리지 VM에 관리 LIF를 생성하려면 선택적인 보조 프라이빗 IP가 필요합니다.
  - 여러 AZs의 HA 쌍: 각 노드에 사용하지 않는 2차 프라이빗 IP가 1개 필요합니다.
8. 단일 AZ의 HA 쌍에서 IP 주소를 할당하는 경우 \* Allow secondary private IPv4 address to be reassigned되도록 \* 를 활성화합니다.
9. 저장 \* 을 클릭합니다.
10. 여러 AZs에 HA 쌍이 있는 경우 노드 2에 대해 이 단계를 반복해야 합니다.

단일 노드 시스템에 스토리지 **VM**을 생성합니다

다음 단계에서는 단일 노드 시스템에 새 스토리지 VM을 생성합니다. NAS LIF를 생성하려면 하나의 프라이빗 IP 주소가 필요하며, 관리 LIF를 생성하려면 또 다른 선택적 프라이빗 IP 주소가 필요합니다.

## 단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
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 e0a에서 사용되지 않는 보조 전용 IP입니다.

3. 선택 사항: 스토리지 VM 관리 LIF를 생성합니다.

```
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 e0a에서 사용되지 않는 또 다른 보조 전용 IP입니다.

4. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

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

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

## 단일 AZ에서 HA 쌍에 스토리지 VM을 생성합니다

다음 단계에서는 단일 AZ의 HA 쌍에서 새 스토리지 VM을 생성합니다. NAS LIF를 생성하려면 하나의 프라이빗 IP 주소가 필요하며, 관리 LIF를 생성하려면 또 다른 선택적 프라이빗 IP 주소가 필요합니다.

이 두 LIF는 모두 노드 1에 할당됩니다. 장애가 발생할 경우 전용 IP 주소를 노드 간에 이동할 수 있습니다.

## 단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
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-node1`의 `e0a`에서 사용되지 않는 보조 전용 IP입니다. 서비스 정책 `default-data-files`는 IP가 파트너 노드로 마이그레이션할 수 있음을 나타내므로 테이크오버의 경우 이 IP 주소를 `cvo-node2`의 `e0a`로 재배치할 수 있습니다.

## 3. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 생성합니다.

```
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 `e0a`에서 사용되지 않는 또 다른 보조 전용 IP입니다.

## 4. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

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

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

## 5. Cloud Volumes ONTAP 9.11.1 이상을 실행 중인 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정합니다.

Cloud Volumes ONTAP가 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하기 때문에 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 AZs의 HA 쌍에서 스토리지 VM을 생성합니다

다음 단계에서는 여러 AZs의 HA 쌍에서 새 스토리지 VM을 생성합니다.

NAS LIF에는 `_floating_IP` 주소가 필요하며 관리 LIF에는 선택 사항입니다. 이러한 부동 IP 주소는 AWS에서 전용 IP를 할당할 필요가 없습니다. 대신, 동일한 VPC에서 특정 노드의 ENI를 가리키도록 AWS 라우트 테이블에 유동 IP가 자동으로 구성됩니다.

유동 IP가 ONTAP와 연동하려면 각 노드의 모든 스토리지 VM에 전용 IP 주소를 구성해야 합니다. 이 내용은 아래 단계에서 iSCSI LIF가 노드 1과 노드 2에 생성되는 것으로 반영됩니다.

단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
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
```

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

## 3. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 생성합니다.

```
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 VM에 있는 유동 IP의 LIF 마이그레이션을 지원하는 데 필요합니다. iSCSI LIF가 될 필요는 없지만 노드 간에 마이그레이션하도록 구성할 수는 없습니다.
- -service-policy default-data-block IP 주소가 노드 간에 마이그레이션되지 않음을 나타냅니다.
- `_private_ip_`은 `cvo_node1`의 `eth0(e0a)`에서 사용되지 않는 보조 전용 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 VM에 있는 유동 IP의 LIF 마이그레이션을 지원하는 데 필요합니다. iSCSI LIF가 될



필요는 없지만 노드 간에 마이그레이션하도록 구성할 수는 없습니다.

- `-service-policy default-data-block` IP 주소가 노드 간에 마이그레이션되지 않음을 나타냅니다.
- `_private_ip_`는 `cvo_node2`의 `eth0(e0a)`에서 사용되지 않는 보조 전용 IP 주소입니다.

6. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

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

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

7. Cloud Volumes ONTAP 9.11.1 이상을 실행 중인 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정합니다.

Cloud Volumes ONTAP가 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하기 때문에 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 ONTAP를 위한 데이터 서비스 스토리지 VM을 생성합니다

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에 스토리지 및 데이터 서비스를 제공합니다. 이를 SVM 또는 `_vserver_`로 알고 있을 수 있습니다. Cloud Volumes ONTAP는 기본적으로 하나의 스토리지 VM으로 구성되지만 Azure에서 Cloud Volumes ONTAP를 실행할 때 추가 스토리지 VM이 지원됩니다.

데이터를 지원하는 스토리지 VM을 추가로 생성하려면 Azure에서 IP 주소를 할당한 다음 ONTAP 명령을 실행하여 스토리지 VM 및 데이터 LIF를 생성해야 합니다.

지원되는 스토리지 VM 수입니다

9.9.0 릴리즈부터 특정 Cloud Volumes ONTAP 구성에서 여러 스토리지 VM이 지원됩니다. 로 이동합니다 ["Cloud Volumes ONTAP 릴리즈 노트"](#) 사용 중인 Cloud Volumes ONTAP 버전에 대해 지원되는 스토리지 VM 수를

확인하려면 다음을 수행합니다.

다른 모든 Cloud Volumes ONTAP 구성에서는 재해 복구에 사용되는 1개의 데이터 서비스 스토리지 VM과 1개의 대상 스토리지 VM을 지원합니다. 소스 스토리지 VM에 중단이 발생할 경우 데이터 액세스를 위해 대상 스토리지 VM을 활성화할 수 있습니다.

### Azure에서 IP 주소를 할당합니다

스토리지 VM을 생성하고 LIF를 할당하기 전에 Azure에서 IP 주소를 할당해야 합니다.

단일 노드 시스템

스토리지 VM을 생성하고 LIF를 할당하기 전에 Azure에서 nic0에 IP 주소를 할당해야 합니다.

데이터 LIF 액세스를 위한 IP 주소와 스토리지 VM(SVM) 관리 LIF를 위한 선택적 IP 주소를 생성해야 합니다. 이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

단계

1. Azure 포털에 로그인하고 \* Virtual Machine \* 서비스를 엽니다.
2. Cloud Volumes ONTAP VM의 이름을 클릭합니다.
3. 네트워킹 \* 을 클릭합니다.
4. nic0의 네트워크 인터페이스 이름을 클릭합니다.
5. 설정 \* 에서 \* IP 구성 \* 을 클릭합니다.
6. 추가 \* 를 클릭합니다.
7. IP 구성의 이름을 입력하고 \* Dynamic \* 을 선택한 다음 \* OK \* 를 클릭합니다.
8. 방금 만든 IP 구성의 이름을 클릭하고 \* Assignment \* 를 \* Static \* 으로 변경한 다음 \* Save \* 를 클릭합니다.

정적 IP 주소를 사용하면 IP 주소가 변경되지 않으므로 정적 IP 주소를 사용하는 것이 가장 좋습니다. 이렇게 하면 응용 프로그램이 불필요하게 중단되는 것을 방지할 수 있습니다.

SVM 관리 LIF를 생성하려면 이 단계를 반복하여 추가 IP 주소를 생성합니다.

작업을 마친 후

방금 만든 개인 IP 주소를 복사합니다. 새 스토리지 VM에 대한 LIF를 생성할 때 이러한 IP 주소를 지정해야 합니다.

HA 쌍

HA 쌍에 대한 IP 주소를 할당하는 방법은 사용 중인 스토리지 프로토콜에 따라 다릅니다.

## iSCSI

스토리지 VM을 생성하고 LIF를 할당하기 전에 Azure의 nic0에 iSCSI IP 주소를 할당해야 합니다. iSCSI는 페일오버에 ALUA를 사용하므로 iSCSI용 IPS는 로드 밸런서가 아니라 nic0에 할당됩니다.

다음 IP 주소를 만들어야 합니다.

- 노드 1에서 iSCSI 데이터 LIF 액세스를 위한 단일 IP 주소
- 노드 2의 iSCSI 데이터 LIF 액세스를 위한 하나의 IP 주소
- 스토리지 VM(SVM) 관리 LIF의 선택적 IP 주소입니다

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

### 단계

1. Azure 포털에 로그인하고 \* Virtual Machine \* 서비스를 엽니다.
2. 노드 1의 Cloud Volumes ONTAP VM 이름을 클릭합니다.
3. 네트워킹 \* 을 클릭합니다.
4. nic0의 네트워크 인터페이스 이름을 클릭합니다.
5. 설정 \* 에서 \* IP 구성 \* 을 클릭합니다.
6. 추가 \* 를 클릭합니다.
7. IP 구성의 이름을 입력하고 \* Dynamic \* 을 선택한 다음 \* OK \* 를 클릭합니다.
8. 방금 만든 IP 구성의 이름을 클릭하고 \* Assignment \* 를 \* Static \* 으로 변경한 다음 \* Save \* 를 클릭합니다.

정적 IP 주소를 사용하면 IP 주소가 변경되지 않으므로 정적 IP 주소를 사용하는 것이 가장 좋습니다. 이렇게 하면 응용 프로그램이 불필요하게 중단되는 것을 방지할 수 있습니다.

9. 노드 2에서 이 단계를 반복합니다.
10. SVM 관리 LIF를 생성하려면 노드 1에서 이 단계를 반복합니다.

### NFS 를 참조하십시오

NFS에 사용하는 IP 주소는 로드 밸런싱 장치에 할당되어 페일오버 이벤트가 발생할 경우 IP 주소가 다른 노드로 마이그레이션될 수 있습니다.

다음 IP 주소를 만들어야 합니다.

- 노드 1에서 NAS 데이터 LIF 액세스를 위한 단일 IP 주소
- 노드 2의 NAS 데이터 LIF 액세스를 위한 하나의 IP 주소
- 스토리지 VM(SVM) 관리 LIF의 선택적 IP 주소입니다

DNS 통신을 위해 iSCSI LIF가 필요합니다. iSCSI LIF는 페일오버 시 마이그레이션되지 않으므로 이 용도로 사용됩니다.

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

### 단계

1. Azure 포털에서 \* 로드 밸런서 \* 서비스를 엽니다.
2. HA 쌍에 대한 로드 밸런싱 장치의 이름을 클릭합니다.
3. 노드 1에서 데이터 LIF 액세스를 위한 프론트엔드 IP 구성을 하나 생성하고, 노드 2에서 데이터 LIF 액세스를 위한 또 다른 프론트엔드 IP를 생성하고, 스토리지 VM(SVM) 관리 LIF를 위한 또 다른 선택적 프론트엔드 IP를 생성합니다.
  - a. Settings \* 에서 \* Frontend IP configuration \* 을 클릭합니다.
  - b. 추가 \* 를 클릭합니다.
  - c. 프론트엔드 IP의 이름을 입력하고, Cloud Volumes ONTAP HA 쌍의 서브넷을 선택하고, \* Dynamic \* 을 선택한 상태로 두고, 가용성 영역이 있는 지역에서는 \* Zone-Redundant \* 를 선택된 상태로 두어 존이 실패하는 경우 IP 주소를 계속 사용할 수 있도록 합니다.

The screenshot shows the 'Add frontend IP configuration' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The main heading is 'Add frontend IP configuration' with a three-dot menu icon. Below the heading, the resource name 'azureha1011s3-rg-lb' is displayed. The configuration form includes the following fields:

- Name \***: A text input field containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet \***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow icon.
- Assignment**: Radio buttons for 'Dynamic' (which is selected) and 'Static'.
- Availability zone \* ⓘ**: A dropdown menu showing 'Zone-redundant' with a downward arrow icon.

- d. 방금 만든 프론트엔드 IP 구성의 이름을 클릭하고 \* Assignment \* 를 \* Static \* 으로 변경하고 \* Save \* 를 클릭합니다.

정적 IP 주소를 사용하면 IP 주소가 변경되지 않으므로 정적 IP 주소를 사용하는 것이 가장 좋습니다. 이렇게 하면 응용 프로그램이 불필요하게 중단되는 것을 방지할 수 있습니다.

4. 방금 생성한 각 프론트엔드 IP에 대해 상태 탐침을 추가합니다.
  - a. 부하 분산 장치의 \* 설정 \* 에서 \* 상태 프로브 \* 를 클릭합니다.
  - b. 추가 \* 를 클릭합니다.
  - c. 상태 프로브의 이름을 입력하고 63005에서 65000 사이의 포트 번호를 입력합니다. 다른 필드의 기본값을 유지합니다.

포트 번호는 63005에서 65000 사이여야 합니다. 예를 들어 상태 프로브를 3개 생성하는 경우 포트 번호 63005, 63006 및 63007을 사용하는 프로브를 입력할 수 있습니다.



Home &gt; Load balancers &gt; azureha1011s3-rg-lb &gt;

## Add health probe ...

azureha1011s3-rg-lb

Name *	svm2-health-probe1 ✓
Protocol *	TCP ▾
Port * ⓘ	63005 ✓
Interval * ⓘ	5 seconds
Unhealthy threshold * ⓘ	2 consecutive failures
Used by ⓘ	Not used

5. 각 프런트엔드 IP에 대한 새 로드 밸런싱 규칙을 생성합니다.

a. 부하 분산 장치의 \* 설정 \* 아래에서 \* 로드 밸런싱 규칙 \* 을 클릭합니다.

b. 추가 \* 를 클릭하고 필요한 정보를 입력합니다.

- \* 이름 \*: 규칙의 이름을 입력합니다.
- \* IP 버전 \*: \* IPv4 \* 를 선택합니다.
- \* 프런트엔드 IP 주소 \*: 방금 생성한 프런트엔드 IP 주소 중 하나를 선택합니다.
- \* HA 포트 \*: 이 옵션을 활성화합니다.
- \* 백엔드 풀 \*: 이미 선택된 기본 백엔드 풀을 유지합니다.
- \* 상태 프로브 \*: 선택한 프런트엔드 IP에 대해 생성한 상태 프로브를 선택합니다.
- \* 세션 지속성 \*: \* 없음 \* 을 선택합니다.
- \* Floating IP \*: \* Enabled \* 를 선택합니다.

## Add load balancing rule

chandanaTcpRst3-rg-lb

**i** A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name \*  
jimmy\_new\_rule ✓

IP Version \*  
 IPv4  IPv6

Frontend IP address \* ⓘ  
10.1.0.156 (dataAFIP) ▾

HA Ports ⓘ

Backend pool ⓘ  
backendPool (2 virtual machines) ▾

Health probe ⓘ  
dataProbe (TCP:63002) ▾

Session persistence ⓘ  
None ▾

Floating IP ⓘ  
 Disabled  Enabled

6. Cloud Volumes ONTAP에 대한 네트워크 보안 그룹 규칙을 통해 로드 밸런서가 위의 4단계에서 만든 상태 탐침에 대한 TCP 탐침을 보낼 수 있는지 확인합니다. 이 작업은 기본적으로 허용됩니다.

### 중소기업

SMB 데이터에 사용하는 IP 주소는 로드 밸런서에 할당되어 파일오버 이벤트가 발생할 경우 IP 주소가 다른 노드로 마이그레이션될 수 있습니다.

로드 밸런서에 다음 IP 주소를 만들어야 합니다.

- 노드 1에서 NAS 데이터 LIF 액세스를 위한 단일 IP 주소
- 노드 2의 NAS 데이터 LIF 액세스를 위한 하나의 IP 주소
- 각 VM의 해당 NIC0에 있는 노드 1의 iSCSI LIF에 대한 IP 주소 1개
- 노드 2의 iSCSI LIF에 대한 IP 주소 1개

iSCSI LIF는 DNS 및 SMB 통신에 필요합니다. iSCSI LIF는 파일오버 시 마이그레이션되지 않으므로 이 용도로 사용됩니다.

- 스토리지 VM(SVM) 관리 LIF의 선택적 IP 주소입니다

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

## 단계

1. Azure 포털에서 \* 로드 밸런서 \* 서비스를 엽니다.
2. HA 쌍에 대한 로드 밸런싱 장치의 이름을 클릭합니다.
3. 데이터 및 SVM LIF에 필요한 수의 프론트엔드 IP 구성을 생성합니다.



프론트엔드 IP는 각 해당 SVM에 대해 NIC0 아래에 생성되어야 합니다. SVM NIC0에 IP 주소를 추가하는 방법에 대한 자세한 내용은 "7단계[하이퍼링크]" 를 참조하십시오.

- a. Settings \* 에서 \* Frontend IP configuration \* 을 클릭합니다.
- b. 추가 \* 를 클릭합니다.
- c. 프론트엔드 IP의 이름을 입력하고, Cloud Volumes ONTAP HA 쌍의 서브넷을 선택하고, \* Dynamic \* 을 선택한 상태로 두고, 가용성 영역이 있는 지역에서는 \* Zone-Redundant \* 를 선택된 상태로 두어 존이 실패하는 경우 IP 주소를 계속 사용할 수 있도록 합니다.

The screenshot shows the 'Add frontend IP configuration' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The page title is 'Add frontend IP configuration' with a three-dot menu icon. Below the title is the resource name 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name \***: A dropdown menu with 'ip-for-svm2' selected.
- Virtual network**: A dropdown menu with 'Default-Networking-vnet' selected.
- Subnet \***: A dropdown menu with 'default (172.19.2.0/24)' selected.
- Assignment**: Radio buttons for 'Dynamic' (selected) and 'Static'.
- Availability zone \***: A dropdown menu with 'Zone-redundant' selected.

- d. 방금 만든 프론트엔드 IP 구성의 이름을 클릭하고 \* Assignment \* 를 \* Static \* 으로 변경하고 \* Save \* 를 클릭합니다.

정적 IP 주소를 사용하면 IP 주소가 변경되지 않으므로 정적 IP 주소를 사용하는 것이 가장 좋습니다. 이렇게 하면 응용 프로그램이 불필요하게 중단되는 것을 방지할 수 있습니다.

4. 방금 생성한 각 프론트엔드 IP에 대해 상태 탐침을 추가합니다.
  - a. 부하 분산 장치의 \* 설정 \* 에서 \* 상태 프로브 \* 를 클릭합니다.
  - b. 추가 \* 를 클릭합니다.
  - c. 상태 프로브의 이름을 입력하고 63005에서 65000 사이의 포트 번호를 입력합니다. 다른 필드의 기본값을 유지합니다.

포트 번호는 63005에서 65000 사이여야 합니다. 예를 들어 상태 프로브를 3개 생성하는 경우 포트 번호 63005, 63006 및 63007을 사용하는 프로브를 입력할 수 있습니다.





Home &gt; Load balancers &gt; azureha1011s3-rg-lb &gt;

## Add health probe ...

azureha1011s3-rg-lb

Name *	svm2-health-probe1 ✓
Protocol *	TCP ▾
Port * ⓘ	63005 ✓
Interval * ⓘ	5 seconds
Unhealthy threshold * ⓘ	2 consecutive failures
Used by ⓘ	Not used

5. 각 프런트엔드 IP에 대한 새 로드 밸런싱 규칙을 생성합니다.

a. 부하 분산 장치의 \* 설정 \* 아래에서 \* 로드 밸런싱 규칙 \* 을 클릭합니다.

b. 추가 \* 를 클릭하고 필요한 정보를 입력합니다.

- \* 이름 \*: 규칙의 이름을 입력합니다.
- \* IP 버전 \*: \* IPv4 \* 를 선택합니다.
- \* 프런트엔드 IP 주소 \*: 방금 생성한 프런트엔드 IP 주소 중 하나를 선택합니다.
- \* HA 포트 \*: 이 옵션을 활성화합니다.
- \* 백엔드 풀 \*: 이미 선택된 기본 백엔드 풀을 유지합니다.
- \* 상태 프로브 \*: 선택한 프런트엔드 IP에 대해 생성한 상태 프로브를 선택합니다.
- \* 세션 지속성 \*: \* 없음 \* 을 선택합니다.
- \* Floating IP \*: \* Enabled \* 를 선택합니다.

## Add load balancing rule ⋮

chandanaTcpRst3-rg-lb

**i** A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

**Name \***  
jimmy\_new\_rule ✓

**IP Version \***  
 IPv4  IPv6

**Frontend IP address \* ⓘ**  
10.1.0.156 (dataAFIP) ▾

HA Ports ⓘ

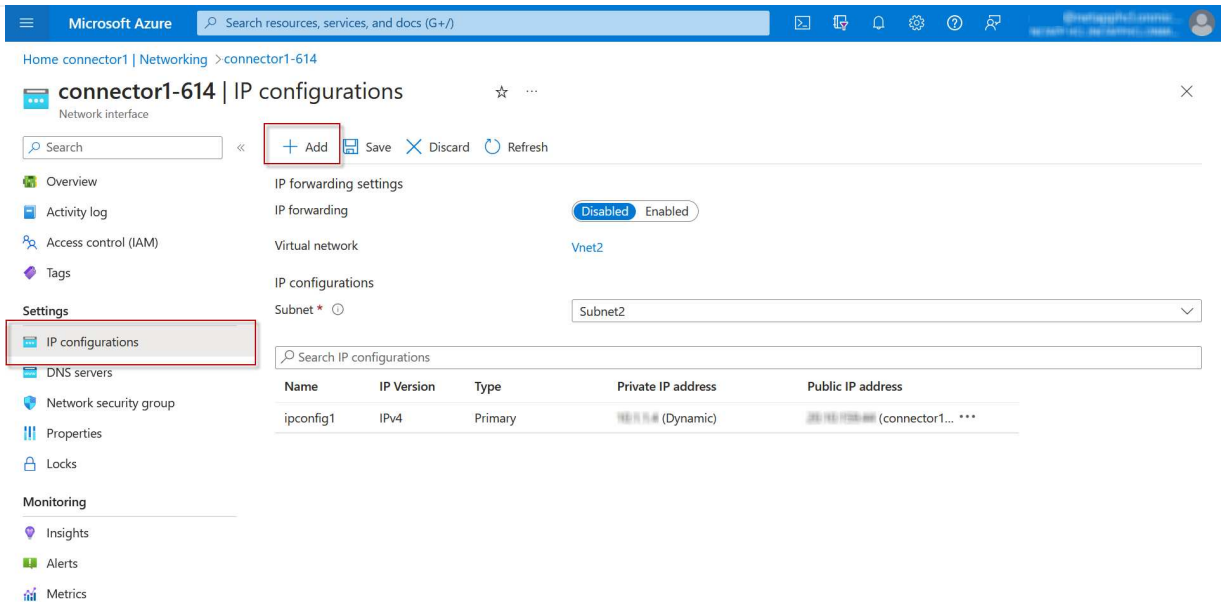
**Backend pool ⓘ**  
backendPool (2 virtual machines) ▾

**Health probe ⓘ**  
dataProbe (TCP:63002) ▾

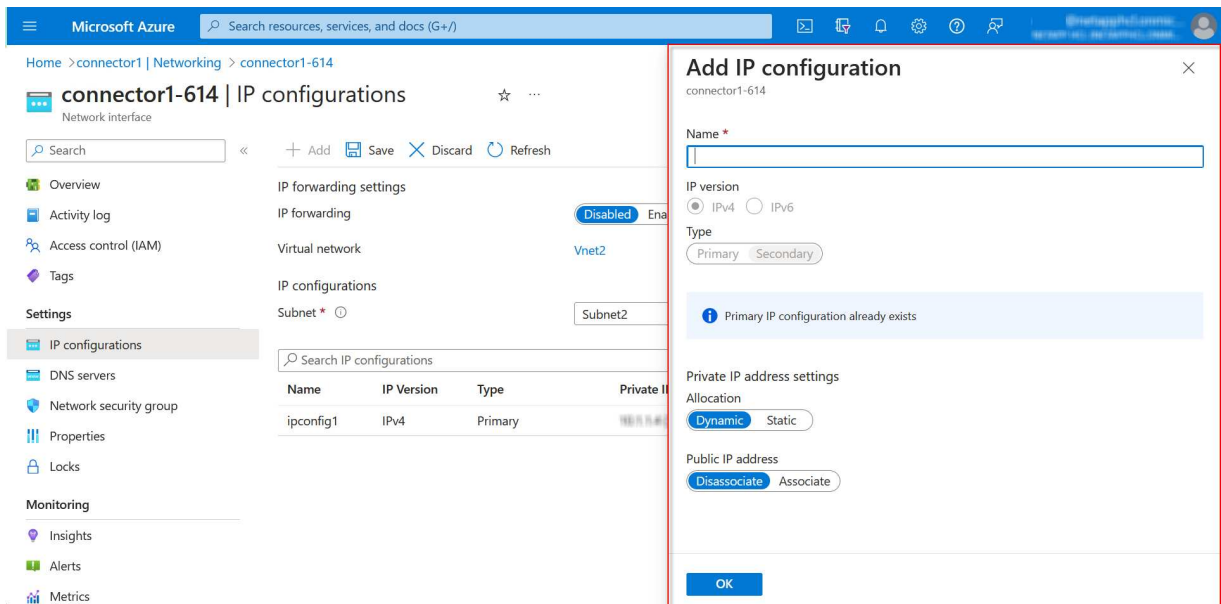
**Session persistence ⓘ**  
None ▾

**Floating IP ⓘ**  
Disabled **Enabled**

6. Cloud Volumes ONTAP에 대한 네트워크 보안 그룹 규칙을 통해 로드 밸런서가 위의 4단계에서 만든 상태 탐침에 대한 TCP 탐침을 보낼 수 있는지 확인합니다. 이 작업은 기본적으로 허용됩니다.
7. iSCSI LIF의 경우 NIC0의 IP 주소를 추가합니다.
  - a. Cloud Volumes ONTAP VM의 이름을 클릭합니다.
  - b. 네트워킹 \* 을 클릭합니다.
  - c. nic0의 네트워크 인터페이스 이름을 클릭합니다.
  - d. 설정에서 \* IP 설정 \* 을 클릭합니다.
  - e. 추가 \* 를 클릭합니다.



f. IP 구성의 이름을 입력하고 Dynamic 을 선택한 다음 \* OK \* 를 클릭합니다.



g. 방금 만든 IP 구성의 이름을 클릭하고 Assignment 를 Static 으로 변경한 다음 \* Save \* 를 클릭합니다.



정적 IP 주소를 사용하면 IP 주소가 변경되지 않으므로 정적 IP 주소를 사용하는 것이 가장 좋습니다. 이렇게 하면 응용 프로그램이 불필요하게 중단되는 것을 방지할 수 있습니다.

작업을 마친 후

방금 만든 개인 IP 주소를 복사합니다. 새 스토리지 VM에 대한 LIF를 생성할 때 이러한 IP 주소를 지정해야 합니다.

스토리지 VM 및 LIF 생성

Azure에서 IP 주소를 할당한 후에는 단일 노드 시스템 또는 HA 쌍 에 새 스토리지 VM을 생성할 수 있습니다.

단일 노드 시스템

단일 노드 시스템에서 스토리지 VM 및 LIF를 생성하는 방법은 사용 중인 스토리지 프로토콜에 따라 다릅니다.

## iSCSI

필요한 LIF와 함께 새 스토리지 VM을 생성하려면 다음 단계를 따르십시오.

### 단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. 데이터 LIF 생성:

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -netmask-length <# of mask bits> -lif <lif-name>  
-home-node <name-of-nodel> -data-protocol iscsi
```

3. 선택 사항: 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-nodel> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

4. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

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

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

## NFS 를 참조하십시오

필요한 LIF와 함께 새 스토리지 VM을 생성하려면 다음 단계를 따르십시오.

### 단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway <ip-of-gateway-server>
```

## 2. 데이터 LIF 생성:

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol cifs,nfs -address <nas-ip-address> -netmask -length <length> -home-node <name-of-node1> -status-admin up -failover-policy disabled -firewall-policy data -home-port e0a -auto-revert true -failover-group Default
```

## 3. 선택 사항: 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol none -address <svm-mgmt-ip-address> -netmask -length <length> -home-node <name-of-node1> -status-admin up -failover-policy system-defined -firewall-policy mgmt -home-port e0a -auto-revert false -failover-group Default
```

## 4. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

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

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

### 중소기업

필요한 LIF와 함께 새 스토리지 VM을 생성하려면 다음 단계를 따르십시오.

#### 단계

##### 1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

## 2. 데이터 LIF 생성:

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nas-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

## 3. 선택 사항: 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

## 4. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

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

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

## HA 쌍

HA 쌍에서 스토리지 VM 및 LIF를 생성하는 방법은 사용 중인 스토리지 프로토콜에 따라 다릅니다.

## iSCSI

필요한 LIF와 함께 새 스토리지 VM을 생성하려면 다음 단계를 따르십시오.

### 단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. 데이터 LIF 생성:

- a. 다음 명령을 사용하여 노드 1에 iSCSI LIF를 생성합니다.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif  
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

- b. 다음 명령을 사용하여 노드 2에 iSCSI LIF를 생성합니다.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif  
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

3. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

4. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

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



스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

5. Cloud Volumes ONTAP 9.11.1 이상을 실행 중인 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정합니다.

- a. 다음 명령을 입력하여 고급 모드에 액세스합니다.

```
::> set adv -con off
```

Cloud Volumes ONTAP가 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하기 때문에 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
```

**NFS** 를 참조하십시오

필요한 LIF와 함께 새 스토리지 VM을 생성하려면 다음 단계를 따르십시오.

단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. 데이터 LIF 생성:

- a. 다음 명령을 사용하여 노드 1에 NAS LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-nod1> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

- b. 다음 명령을 사용하여 노드 2에 NAS LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

3. DNS 통신을 제공하기 위해 iSCSI LIF 생성:

- a. 다음 명령을 사용하여 노드 1에 iSCSI LIF를 생성합니다.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif  
<lif-name> -home-node <name-of-nod1> -data-protocol iscsi
```

- b. 다음 명령을 사용하여 노드 2에 iSCSI LIF를 생성합니다.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

5. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

6. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

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

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

7. Cloud Volumes ONTAP 9.11.1 이상을 실행 중인 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정합니다.

- a. 다음 명령을 입력하여 고급 모드에 액세스합니다.

```
::> set adv -con off
```

Cloud Volumes ONTAP가 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하기 때문에 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

```

## 중소기업

필요한 LIF와 함께 새 스토리지 VM을 생성하려면 다음 단계를 따르십시오.

### 단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```

vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix

```

```

network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>

```

## 2. NAS 데이터 LIF 생성:

- a. 다음 명령을 사용하여 노드 1에 NAS LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

- b. 다음 명령을 사용하여 노드 2에 NAS LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

## 3. DNS 통신을 제공하기 위해 iSCSI LIF 생성:

- a. 다음 명령을 사용하여 노드 1에 iSCSI LIF를 생성합니다.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

- b. 다음 명령을 사용하여 노드 2에 iSCSI LIF를 생성합니다.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

## 4. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

5. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

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

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

6. Cloud Volumes ONTAP 9.11.1 이상을 실행 중인 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정합니다.

- a. 다음 명령을 입력하여 고급 모드에 액세스합니다.

```
::> set adv -con off
```

Cloud Volumes ONTAP가 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하기 때문에 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

```

#### 다음 단계

HA 쌍에서 스토리지 VM을 생성하면 해당 SVM에서 스토리지를 프로비저닝하기 전에 12시간을 기다리는 것이 좋습니다. Cloud Volumes ONTAP 9.10.1 릴리즈부터 BlueXP는 12시간 간격으로 HA 쌍의 로드 밸런서에 대한 설정을 검색합니다. 새로운 SVM이 있는 경우 BlueXP에서 계획되지 않은 페일오버 시간을 단축해 주는 설정을 사용할 수 있습니다.

### Google Cloud에서 Cloud Volumes ONTAP용 데이터 서비스 스토리지 VM을 생성합니다

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에 스토리지 및 데이터 서비스를 제공합니다. 이를 SVM 또는 `_vserver_`로 알고 있을 수 있습니다. Cloud Volumes ONTAP는 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다.

지원되는 스토리지 **VM** 수입니다

9.11.1 릴리즈부터 Google Cloud의 특정 Cloud Volumes ONTAP 구성에서 여러 스토리지 VM이 지원됩니다. 로 이동합니다 "[Cloud Volumes ONTAP 릴리즈 노트](#)" 사용 중인 Cloud Volumes ONTAP 버전에 대해 지원되는 스토리지 VM 수를 확인하려면 다음을 수행합니다.

다른 모든 Cloud Volumes ONTAP 구성에서는 재해 복구에 사용되는 1개의 데이터 서비스 스토리지 VM과 1개의 대상 스토리지 VM을 지원합니다. 소스 스토리지 VM에 중단이 발생할 경우 데이터 액세스를 위해 대상 스토리지 VM을 활성화할 수 있습니다.

스토리지 **VM**을 생성합니다

라이선스로 지원되는 경우 단일 노드 시스템 또는 HA 쌍에서 여러 스토리지 VM을 생성할 수 있습니다. BlueXP API를 사용하여 HA 쌍에서 스토리지 VM을 생성해야 하지만, CLI 또는 System Manager를 사용하여 단일 노드 시스템에 스토리지 VM을 생성할 수 있습니다.

단일 노드 시스템

다음 단계에서는 CLI를 사용하여 단일 노드 시스템에 새 스토리지 VM을 생성합니다. 데이터 LIF를 생성하려면 하나의 프라이빗 IP 주소가 필요하며, 관리 LIF를 생성하려면 또 다른 선택적 프라이빗 IP 주소가 필요합니다.

단계

1. Google Cloud에서 Cloud Volumes ONTAP 인스턴스로 이동하고 각 LIF에 대한 IP 주소를 nic0에 추가합니다.



**Edit network interface**

Network \*  
default

Subnetwork \*  
default IPv4 (10.138.0.0/20)

**i** To use IPv6, you need an IPv6 subnet range. [LEARN MORE](#)

**IP stack type**

IPv4 (single-stack)

IPv4 and IPv6 (dual-stack)

Primary internal IP  
gpcvo-vm-ip-nic0-nodemgmt (10.138.0.46)

**Alias IP ranges**

Subnet range	Alias IP range *
Subnet range 1 Primary (10.138.0.0/20)	Alias IP range 1 * 10.138.0.25/32
Subnet range 2 Primary (10.138.0.0/20)	Alias IP range 2 * 10.138.0.23/32
Subnet range 3 Primary (10.138.0.0/20)	Alias IP range 3 * 10.138.0.21/32
Subnet range 4 Primary (10.138.0.0/20)	Alias IP range 4 * 10.138.0.31/32

**+ ADD IP RANGE**

External IPv4 address  
None

스토리지 VM에서 관리 LIF를 생성하려면 데이터 LIF에 하나의 IP 주소와 다른 선택적 IP 주소가 필요합니다.

"[Google Cloud 설명서: 기존 인스턴스에 별칭 IP 범위 추가](#)"

2. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway <ip-of-gateway-server>
```

3. Google Cloud에 추가한 IP 주소를 지정하여 데이터 LIF를 생성합니다.

## iSCSI

```
network interface create -vserver <svm-name> -home-port e0a -address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-nodel> -data -protocol iscsi
```

## NFS 또는 SMB

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask -length <length> -home-node <name-of-nodel> -status-admin up -failover-policy disabled -firewall-policy data -home-port e0a -auto -revert true -failover-group Default
```

4. 선택 사항: Google Cloud에 추가한 IP 주소를 지정하여 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol none -address <svm-mgmt-ip-address> -netmask-length <length> -home-node <name-of-nodel> -status-admin up -failover-policy system-defined -firewall-policy mgmt -home-port e0a -auto-revert false -failover-group Default
```

5. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

```
vserver add-aggregates -vserver <svm-name> -aggregates <aggr1,aggr2>
```

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

## HA 쌍

BlueXP API를 사용하여 Google Cloud의 Cloud Volumes ONTAP 시스템에서 스토리지 VM을 생성해야 합니다. BlueXP는 필요한 LIF 서비스와 아웃바운드 SMB/CIFS 통신에 필요한 iSCSI LIF를 사용하여 스토리지 VM을 구성하기 때문에 System Manager 또는 CLI가 아닌 API를 사용해야 합니다.

BlueXP는 Google Cloud에 필요한 IP 주소를 할당하고 SMB/NFS 액세스를 위한 데이터 LIF와 아웃바운드 SMB 통신을 위한 iSCSI LIF를 사용하여 스토리지 VM을 생성합니다.

## Google Cloud 권한이 필요합니다

Connector에는 Cloud Volumes ONTAP HA 쌍에 대한 스토리지 VM을 생성하고 관리할 수 있는 특정 권한이 필요합니다. 필요한 권한은 에 포함되어 있습니다 ["NetApp에서 제공하는 정책"](#).

단계

1. 다음 API 호출을 사용하여 스토리지 VM을 생성합니다.

```
POST /occm/api/gcp/ha/working-environments/{WE_ID}/svm/
```

요청 본문에는 다음이 포함되어야 합니다.

```
{ "svmName": "myNewSvm1" }
```

## HA 쌍에서 스토리지 VM 관리

또한 BlueXP API는 HA 쌍에서 스토리지 VM의 이름 변경 및 삭제를 지원합니다.

스토리지 VM의 이름을 바꿉니다

필요한 경우 언제든지 스토리지 VM의 이름을 변경할 수 있습니다.

단계

1. 다음 API 호출을 사용하여 스토리지 VM의 이름을 바꿉니다.

```
PUT /occm/api/gcp/ha/working-environments/{WE_ID}/svm
```

요청 본문에는 다음이 포함되어야 합니다.

```
{  
  "svmNewName": "newSvmName",  
  "svmName": "oldSvmName"  
}
```

스토리지 VM을 삭제합니다

스토리지 VM이 더 이상 필요하지 않은 경우 Cloud Volumes ONTAP에서 삭제할 수 있습니다.

단계

1. 다음 API 호출을 사용하여 스토리지 VM을 삭제합니다.

```
DELETE /occm/api/gcp/ha/working-environments/{WE_ID}/svm/{SVM_NAME}
```

## SVM 재해 복구 설정

BlueXP는 스토리지 VM(SVM) 재해 복구에 대한 설정 또는 오케스트레이션 지원을 제공하지 않습니다. System Manager 또는 CLI를 사용해야 합니다.

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

CLI 지침은 다음 문서를 참조하십시오.

- "SVM 재해 복구 준비 Express 가이드"
- "SVM 재해 복구 익스프레스 가이드 를 참조하십시오"

## 보안 및 데이터 암호화

### NetApp 암호화 솔루션으로 볼륨 암호화

Cloud Volumes ONTAP는 NVE(NetApp Volume Encryption) 및 NAE(NetApp Aggregate Encryption)를 지원합니다. NVE와 NAE는 FIPS 140-2를 준수하는 볼륨 유희 데이터 암호화를 지원하는 소프트웨어 기반 솔루션입니다. ["이러한 암호화 솔루션에 대해 자세히 알아보십시오"](#).

NVE와 NAE는 모두 외부 키 관리자로 지원됩니다.

### AWS 키 관리 서비스로 키를 관리합니다

을 사용할 수 있습니다 ["AWS KMS\(Key Management Service\)"](#) Google Cloud Platform에서 구축한 응용 프로그램에서 ONTAP 암호화 키를 보호합니다.

AWS KMS를 사용한 키 관리는 CLI 또는 ONTAP REST API를 통해 활성화할 수 있습니다.

KMS를 사용할 때는 기본적으로 데이터 SVM의 LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용됩니다. 노드 관리 네트워크는 AWS의 인증 서비스와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않은 경우 클러스터는 키 관리 서비스를 제대로 사용하지 않습니다.

시작하기 전에

- Cloud Volumes ONTAP는 버전 9.12.0 이상을 실행해야 합니다
- 볼륨 암호화(VE) 라이선스 및 을(를) 설치해야 합니다
- MTEKM(멀티 테넌트 암호화 키 관리) 라이선스가 설치되어 있어야 합니다.
- 클러스터 또는 SVM 관리자여야 합니다
- 활성 AWS 구독이 있어야 합니다



데이터 SVM에 대한 키만 구성할 수 있습니다.

구성

설치하고

1. 을(를) 만들어야 합니다 ["허가"](#) 암호화를 관리하는 IAM 역할에 사용되는 AWS KMS 키의 경우 IAM 역할에는 다음 작업을 허용하는 정책이 포함되어야 합니다.
  - DescribeKey
  - Encrypt
  - Decrypt보조금을 생성하려면 을 참조하십시오 ["AWS 문서"](#).

2. "적절한 IAM 역할에 정책을 추가합니다." 이 정책은 을 지원해야 합니다 DescribeKey, Encrypt, 및 Decrypt 운영:

### Cloud Volumes ONTAP

1. Cloud Volumes ONTAP 환경으로 전환하십시오.
2. 고급 권한 레벨로 전환합니다.  
`set -privilege advanced`
3. AWS 키 관리자를 활성화합니다.  
`security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. 메시지가 표시되면 비밀 키를 입력합니다.
5. AWS KMS가 올바르게 구성되었는지 확인합니다.  
`security key-manager external aws show -vserver svm_name`

### Azure Key Vault를 사용하여 키를 관리합니다

을 사용할 수 있습니다 "Azure 키 저장소(AKV)" Azure로 배포된 응용 프로그램에서 ONTAP 암호화 키를 보호합니다.

AKV를 사용하여 보호할 수 있습니다 "NVE(NetApp Volume Encryption) 키" 데이터 SVM에만 해당.

AKV를 사용한 키 관리는 CLI 또는 ONTAP REST API를 사용하여 활성화할 수 있습니다.

AKV를 사용할 때는 기본적으로 데이터 SVM LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용됩니다. 노드 관리 네트워크는 클라우드 공급자의 인증 서비스(login.microsoftonline.com 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않은 경우 클러스터는 키 관리 서비스를 제대로 사용하지 않습니다.

#### 시작하기 전에

- Cloud Volumes ONTAP에서 버전 9.10.1 이상을 실행해야 합니다
- 설치된 볼륨 암호화(VE) 라이선스(NetApp 볼륨 암호화 라이선스는 NetApp Support에 등록된 각 Cloud Volumes ONTAP 시스템에 자동으로 설치됨)
- 멀티 테넌트 암호화 키 관리(MT\_EK\_MGMT) 라이선스가 있어야 합니다
- 클러스터 또는 SVM 관리자여야 합니다
- Active Azure 구독

#### 제한 사항

- AKV는 데이터 SVM에서만 구성할 수 있습니다

#### 구성 프로세스

이 단계에서는 Azure에 Cloud Volumes ONTAP 구성을 등록하는 방법과 Azure 키 저장소 및 키를 생성하는 방법을 설명합니다. 이 단계를 이미 완료한 경우, 특히 에서 올바른 구성 설정이 있는지 확인하십시오 [Azure Key Vault를 작성합니다](#)을 클릭한 다음 로 진행합니다 [Cloud Volumes ONTAP 구성](#).

- [Azure 애플리케이션 등록](#)
- [Azure 클라이언트 암호를 생성합니다](#)

- Azure Key Vault를 작성합니다
- 암호화 키를 생성합니다
- Azure Active Directory 끝점 생성(HA만 해당)
- Cloud Volumes ONTAP 구성

#### Azure 애플리케이션 등록

1. 먼저 Cloud Volumes ONTAP가 Azure 키 저장소에 액세스하기 위해 사용할 Azure 구독에 응용 프로그램을 등록해야 합니다. Azure 포털에서 앱 등록 을 선택합니다.
2. 새 등록\*\* 을 선택합니다.
3. 응용 프로그램의 이름을 제공하고 지원되는 응용 프로그램 유형을 선택합니다. Azure Key Vault 사용에 대한 기본 단일 테넌트 접미사 **Register** (등록\*\*)을 선택합니다.
4. Azure 개요 창에서 등록한 애플리케이션을 선택합니다. 애플리케이션(클라이언트) ID 및 디렉토리(테넌트) ID 를 안전한 위치에 복사합니다. 등록 프로세스 후반부에 필요합니다.

#### Azure 클라이언트 암호를 생성합니다

1. Azure 키 저장소 앱 등록을 위한 Azure 포털에서 인증서 및 비밀 창을 선택합니다.
2. 새 클라이언트 암호\*\* 를 선택합니다. 클라이언트 비밀에 의미 있는 이름을 입력합니다. NetApp에서는 24개월의 만료 기간을 권장합니다. 단, 특정 클라우드 거버넌스 정책에는 다른 설정이 필요할 수 있습니다.
3. 클라이언트 암호를 만들려면 추가 를 클릭합니다. 값\*\* 열에 나열된 암호 문자열을 복사하여 에서 나중에 사용할 수 있도록 안전한 위치에 저장합니다 [Cloud Volumes ONTAP 구성](#). 페이지를 벗어나 이동하면 암호 값이 다시 표시되지 않습니다.

#### Azure Key Vault를 작성합니다

1. 기존 Azure 키 저장소가 있는 경우 Cloud Volumes ONTAP 구성에 연결할 수 있지만 이 프로세스의 설정에 액세스 정책을 적용해야 합니다.
2. Azure 포털에서 **Key Vaults** 섹션으로 이동합니다.
3. **+Create**를 클릭하고 리소스 그룹, 지역 및 가격 책정 계층을 포함한 필수 정보를 입력합니다. 또한, 삭제된 볼트를 보관할 일 수를 입력하고 키 볼트에서 삭제 보호 활성화를 선택합니다.
4. 액세스 정책을 선택하려면 다음 을 선택합니다.
5. 다음 옵션을 선택합니다.
  - a. **Access configuration** 아래에서 **Vault access policy**를 선택합니다.
  - b. 리소스 액세스 아래에서 볼륨 암호화를 위한 **Azure** 디스크 암호화 를 선택합니다.
6. 액세스 정책을 추가하려면 **+ Create** 를 선택합니다.
7. 템플릿에서 구성 아래에서 드롭다운 메뉴를 클릭한 다음 키, 암호 및 인증서 관리\*\* 템플릿을 선택합니다.
8. 각 드롭다운 권한 메뉴(키, 암호, 인증서)를 선택한 다음 메뉴 목록 상단의 모두 선택 을 선택하여 사용 가능한 모든 권한을 선택합니다. 다음과 같은 항목이 있어야 합니다.
  - 키 권한:20이 선택되었습니다
  - 비밀 권한:8 선택됨
  - 인증서 권한:16 선택됨

# Create an access policy



- 1 Permissions
- 2 Principal
- 3 Application (optional)
- 4 Review + create

Configure from a template

Key, Secret, & Certificate Management

## Key permissions

### Key Management Operations

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

### Cryptographic Operations

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

### Privileged Key Operations

- Select all
- Purge
- Release

### Rotation Policy Operations

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

## Secret permissions

### Secret Management Operations

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

### Privileged Secret Operations

- Select all
- Purge

## Certificate permissions

### Certificate Management Operations

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

### Privileged Certificate Operations

- Select all
- Purge

Previous

Next

9. 에서 만든 기본 Azure 등록 응용 프로그램을 선택하려면 다음 을 클릭합니다 [Azure 애플리케이션 등록](#). 다음\*\* 을 선택합니다.



정책당 하나의 보안 주기만 할당할 수 있습니다.

**Create an access policy** [X]

1 Permissions 2 **Principal** 3 Application (optional) 4 Review + create

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. 검토 후 작성 이 나타날 때까지 다음 을 두 번 클릭합니다. 그런 다음 만들기 를 클릭합니다.

11. 다음 을 선택하여 네트워킹 옵션으로 진행합니다.

12. 적절한 네트워크 액세스 방법을 선택하거나 모든 네트워크 및 검토 + 작성을 선택하여 키 볼트를 작성합니다.  
(네트워크 액세스 방법은 거버넌스 정책 또는 회사 클라우드 보안 팀에서 규정할 수 있습니다.)

13. 키 볼트 URI 기록: 작성한 키 볼트에서 개요 메뉴로 이동하여 오른쪽 컬럼에서 볼트 **URI**를 복사합니다. 이 작업은 나중에 수행해야 합니다.

암호화 키를 생성합니다

1. Cloud Volumes ONTAP에 대해 만든 키 저장소 메뉴에서 키 옵션으로 이동합니다.

2. 새 키를 만들려면 **Generate/import** 를 선택합니다.

3. 기본 옵션을 **Generate** 로 설정된 상태로 둡니다.

4. 다음 정보를 제공합니다.

◦ 암호화 키 이름입니다



- 키 유형: RSA
- RSA 키 크기: 2048
- 사용: 예

5. 암호화 키를 만들려면 만들기 를 선택합니다.
6. 키 메뉴로 돌아가서 방금 만든 키를 선택합니다.
7. 키 속성을 보려면 현재 버전 아래에서 키 ID를 선택합니다.
8. 키 식별자 필드를 찾습니다. 16진수 문자열을 포함하지만 포함되지 않는 최대 URI를 복사합니다.

#### Azure Active Directory 끝점 생성(HA만 해당)

1. 이 프로세스는 HA Cloud Volumes ONTAP 작업 환경을 위해 Azure 키 저장소를 구성하는 경우에만 필요합니다.
2. Azure 포털에서 가상 네트워크로 이동합니다.
3. Cloud Volumes ONTAP 작업 환경을 배포한 가상 네트워크를 선택하고 페이지 왼쪽의 **Subnets** 메뉴를 선택합니다.
4. 목록에서 Cloud Volumes ONTAP 구축의 서브넷 이름을 선택합니다.
5. 서비스 엔드포인트 제목으로 이동합니다. 드롭다운 메뉴에서 다음을 선택합니다.
  - NET Framework 클래스 라이브러리 Control.OnEventArgs 클래스 참고: 이 속성은 .NET Framework 버전 2.0
  - **Microsoft.KeyVault**
  - **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. 설정을 캡처하려면 저장을 선택합니다.

#### Cloud Volumes ONTAP 구성

1. 기본 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.
2. ONTAP에서 고급 권한 모드로 들어갑니다.

```
set advanced -con off
```

3. 원하는 Data SVM을 식별하고 DNS 구성을 확인합니다.

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

- a. 원하는 데이터 SVM에 대한 DNS 항목이 있고 Azure DNS에 대한 항목이 포함된 경우 별도의 조치가 필요하지 않습니다. 그렇지 않으면 Azure DNS, 프라이빗 DNS 또는 사내 서버를 가리키는 데이터 SVM용 DNS 서버 항목을 추가합니다. 이 값은 클러스터 관리자 SVM의 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 확인합니다.

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

4. 응용 프로그램 등록 후 저장된 클라이언트 ID 및 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 Azure_key_vault_name -key-id  
Azure_key_ID
```

5. 키 관리자의 상태를 확인합니다.

```
security key-manager external azure check  
출력은 다음과 같이 표시됩니다.
```

```
::*> 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.
```

를 누릅니다 `service_reachability` 상태가 아닙니다 `OK` SVM은 필요한 모든 연결 및 사용 권한으로 Azure Key Vault 서비스에 연결할 수 없습니다. Azure 네트워크 정책 및 라우팅으로 인해 프라이빗 VNET가 Azure KeyVault Public 엔드포인트에 도달하지 못하도록 차단하지 않는지 확인합니다. 이러한 경우, VNET 내에서 키 볼트에 액세스하기 위해 Azure 프라이빗 끝점을 사용하는 것이 좋습니다. 또한 종점의 전용 IP 주소를 확인하기 위해 SVM에 정적 호스트 항목을 추가해야 할 수도 있습니다.

를 클릭합니다 `kms_wrapped_key_status` 보고합니다 UNKNOWN 초기 구성 시 상태가 로 변경됩니다 OK 첫 번째 볼륨이 암호화된 후

6. 선택 사항: NVE의 기능을 확인하기 위한 테스트 볼륨을 생성합니다.

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

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

7. 볼륨이 올바르게 생성되고 암호화되었는지 확인합니다. 있다면, 입니다 `-is-encrypted` 매개 변수는 로 표시됩니다 `true`.

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

## Google의 클라우드 키 관리 서비스로 키를 관리합니다

을 사용할 수 있습니다 "[Google Cloud Platform의 키 관리 서비스\(Cloud KMS\)](#)" Google Cloud Platform에서 구축한 응용 프로그램에서 ONTAP 암호화 키를 보호합니다.

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

Cloud KMS를 사용할 때는 기본적으로 데이터 SVM의 LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용됩니다. 노드 관리 네트워크는 클라우드 공급자의 인증 서비스(`oauth2.googleapis.com` 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않은 경우 클러스터는 키 관리 서비스를 제대로 사용하지 않습니다.

시작하기 전에

- Cloud Volumes ONTAP에서 버전 9.10.1 이상을 실행해야 합니다
- VE(Volume Encryption) 라이선스가 설치되었습니다
- 멀티 테넌트 암호화 키 관리(MTEKM) 라이선스가 설치되어 있으며 Cloud Volumes ONTAP 9.12.1 GA부터 시작합니다.
- 클러스터 또는 SVM 관리자여야 합니다
- Google Cloud Platform의 활성 서브스크립션입니다

제한 사항

- 클라우드 KMS는 데이터 SVM에서만 구성할 수 있습니다

구성

### Google 클라우드

1. Google Cloud 환경에서는 "[대칭 GCP 키 링 및 키를 생성합니다](#)".
2. Cloud Volumes ONTAP 서비스 계정에 대한 사용자 지정 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.locat
ions.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA

```

- 클라우드 KMS 키 및 Cloud Volumes ONTAP 서비스 계정에 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

```

- 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

- 기본 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.

- 고급 권한 레벨로 전환합니다.

```
set -privilege advanced
```

- 데이터 SVM을 위한 DNS를 생성합니다.

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

- CMEK 항목 작성:

```
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
```

- 메시지가 표시되면 GCP 계정의 서비스 계정 JSON 키를 입력합니다.

- 활성화된 프로세스가 성공했는지 확인합니다.

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

- 선택 사항: 암호화를 테스트할 볼륨을 생성합니다
- ```
vol create volume_name -aggregate aggregate
-vserver vserver_name -size 10G
```

## 문제 해결

문제를 해결해야 하는 경우 위의 마지막 두 단계에서 원시 REST API 로그를 지정할 수 있습니다.

- set d

- systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2\_client.log

## 랜섬웨어에 대한 보호 개선









랜섬웨어 공격은 비즈니스 시간, 리소스 및 평판에 악영향을 줄 수 있습니다. BlueXP를 사용하면 일반적인 랜섬웨어 파일 확장으로부터 보호하는 것과 자율적 랜섬웨어 방어(ARP)라는 두 가지 NetApp 솔루션을 랜섬웨어용 구현할 수 있습니다. 이러한 솔루션은 가시성, 감지, 문제 해결을 위한 효과적인 툴을 제공합니다.

### 일반적인 랜섬웨어 파일 확장명으로부터 보호

BlueXP를 통해 제공되는 랜섬웨어 방어 설정에서 ONTAP FPolicy 기능을 활용하여 일반적인 랜섬웨어 파일 확장 유형을 방지할 수 있습니다.

### 단계

1. Canvas 페이지에서 랜섬웨어 보호를 구성하는 시스템의 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 랜섬웨어 보호 \* 옆에 있는 연필 아이콘을 클릭합니다.

| Information              | Features                                                                                                       |
|--------------------------|----------------------------------------------------------------------------------------------------------------|
| Working Environment 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               |                           |

3. 랜섬웨어에 대한 NetApp 솔루션 구현:

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

NetApp Snapshot 기술은 랜섬웨어 해결을 위한 업계 최고의 솔루션을 제공합니다. 성공적인 복구의 핵심은 감염되지 않은 백업에서 복원하는 것입니다. Snapshot 복사본은 읽기 전용이므로 랜섬웨어 손상을 방지합니다. 또한 세분화하여 단일 파일 복사본 또는 전체 재해 복구 솔루션의 이미지를 생성할 수도 있습니다.

- b. FPolicy \* 활성화 를 클릭하여 ONTAP의 FPolicy 솔루션을 활성화합니다. FPolicy 솔루션은 파일의 확장명에 따라 파일 작업을 차단할 수 있습니다.

이 예방적 솔루션은 일반적인 랜섬웨어 파일 유형을 차단하여 랜섬웨어 공격으로부터 보호를 개선합니다.

기본 FPolicy 범위는 다음 확장명의 파일을 차단합니다.

마이크로, 암호화, 잠김, 암호화, 암호화, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, 양호, LOL!, OMG!, RDM, RK, encryptedRS, crjoker, enciped, LeChiffre



Cloud Volumes ONTAP에서 FPolicy를 활성화하면 BlueXP에서 이 범위가 생성됩니다. 이 목록은 일반적인 랜섬웨어 파일 유형을 기반으로 합니다. Cloud Volumes ONTAP CLI에서 `vserver FPolicy scope` 명령을 사용하여 차단된 파일 확장명을 사용자 지정할 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](#)

## 자율 랜섬웨어 보호

Cloud Volumes ONTAP는 워크로드 분석을 수행하여 랜섬웨어 공격을 나타낼 수 있는 비정상적인 활동을 사전에 감지하고 경고하는 ARP(Autonomous 랜섬웨어 Protection) 기능을 지원합니다.

를 통해 제공되는 파일 확장자 보호와 분리됩니다 "랜섬웨어 차단 설정"ARP 기능은 워크로드 분석을 사용하여 감지된 "비정상적인 활동"을 기반으로 잠재적인 공격에 대해 사용자에게 경고합니다. 랜섬웨어 차단 설정과 ARP 기능을 모두 포괄적인 랜섬웨어 방어에 함께 사용할 수 있습니다.

ARP 기능은 노드 기반 및 용량 기반 라이선스 모델 모두에서 BYOL 라이선스(1년, 2년, 3년 조건)에만 사용할 수 있습니다. Cloud Volumes ONTAP의 ARP 기능과 함께 사용하기 위해 별도의 새 애드온 라이선스를 구입하려면 NetApp 영업 담당자에게 문의해야 합니다.

추가 라이선스를 구입하여 디지털 지갑에 추가하면 Cloud Volumes ONTAP를 사용하여 볼륨별로 ARP를 활성화할 수 있습니다. 볼륨에 대한 ARP 구성은 ONTAP 시스템 관리자 및 ONTAP CLI를 통해 수행됩니다.

ONTAP 시스템 관리자 및 CLI에서 ARP를 활성화하는 방법에 대한 자세한 내용은 를 참조하십시오 "자율주행 랜섬웨어 보호 활성화".





라이선스가 없는 경우 라이선스가 부여된 기능을 사용할 수 없습니다.

**Autonomous Ransomware Protection** i

---

|                                               |                                                                                                                                                                                                                                            |                                  |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| <p><b>0</b> TiB</p> <p>Protected Capacity</p> | <p><b>100</b> TiB</p> <p>Precommitted capacity</p> <hr style="width: 50%; margin: 10px auto;"/> <p>BYOL <span style="float: right;"><b>100 TiB</b></span></p> <p>Marketplace Contracts <span style="float: right;"><b>0 TiB</b></span></p> | <p><b>0</b> TiB</p> <p>PAYGO</p> |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|

## 시스템 관리

### Cloud Volumes ONTAP 소프트웨어를 업그레이드합니다

BlueXP에서 Cloud Volumes ONTAP를 업그레이드하여 최신 새 기능 및 향상된 기능을 이용할 수 있습니다. 소프트웨어를 업그레이드하기 전에 Cloud Volumes ONTAP 시스템을 준비해야 합니다.

#### 업그레이드 개요

Cloud Volumes ONTAP 업그레이드 프로세스를 시작하기 전에 다음 사항을 숙지해야 합니다.

#### BlueXP에서만 업그레이드합니다

Cloud Volumes ONTAP 업그레이드는 BlueXP에서 완료해야 합니다. System Manager 또는 CLI를 사용하여 Cloud Volumes ONTAP를 업그레이드해서는 안 됩니다. 이렇게 하면 시스템 안정성에 영향을 줄 수 있습니다.

#### 업그레이드 방법

BlueXP는 Cloud Volumes ONTAP를 업그레이드할 수 있는 두 가지 방법을 제공합니다.

- 작업 환경에 나타나는 업그레이드 알림을 따릅니다
- 업그레이드 이미지를 HTTPS 위치에 배치한 다음 BlueXP에 URL을 제공합니다

#### 지원되는 업그레이드 경로

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

|              |                        |
|--------------|------------------------|
| 현재 버전        | 로 직접 업그레이드할 수 있는 버전입니다 |
| 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 를 참조하십시오 | 9.5                    |
| 9.3          | 9.4 를 참조하십시오           |
| 9.2          | 9.3                    |
| 9.1          | 9.2                    |
| 9.0          | 9.1                    |
| 8.3          | 9.0                    |

다음 사항에 유의하십시오.

- Cloud Volumes ONTAP에 대해 지원되는 업그레이드 경로는 사내 ONTAP 클러스터에 대한 업그레이드 경로와 다릅니다.
- 작업 환경에 나타나는 업그레이드 알림에 따라 업그레이드하는 경우 BlueXP에서 지원되는 업그레이드 경로 다음에 나오는 릴리스로 업그레이드하라는 메시지가 표시됩니다.
- HTTPS 위치에 업그레이드 이미지를 배치하여 업그레이드하는 경우 지원되는 업그레이드 경로를 따르십시오.
- 경우에 따라 타겟 릴리스로 업그레이드하기 위해 몇 차례 업그레이드해야 할 수도 있습니다.

예를 들어 9.8 버전을 실행 중이고 9.10.1로 업그레이드하려면 먼저 9.9.1 버전으로 업그레이드한 다음 9.10.1로 업그레이드해야 합니다.

- 패치(P) 릴리스의 경우 한 버전 릴리스에서 다음 버전의 모든 P 릴리스로 업그레이드할 수 있습니다.

다음은 몇 가지 예입니다.

- 9.13.0 > 9.13.1P15
- 9.12.1 > 9.13.1P2

되돌리기 또는 다운그레이드

Cloud Volumes ONTAP를 이전 릴리즈로 되돌리거나 다운그레이드하는 것은 지원되지 않습니다.

지원 등록

이 페이지에 설명된 방법을 사용하여 소프트웨어를 업그레이드하려면 Cloud Volumes ONTAP를 NetApp 지원 팀에 등록해야 합니다. 이 내용은 PAYGO 및 BYOL 모두에 적용됩니다. 필요한 것이 있습니다 **"PAYGO 시스템을 수동으로 등록합니다"** BYOL 시스템은 기본적으로 등록되지만



지원이 등록되지 않은 시스템은 새 버전이 출시되어도 BlueXP에 나타나는 소프트웨어 업데이트 알림을 계속 받게 됩니다. 그러나 소프트웨어를 업그레이드하기 전에 시스템을 등록해야 합니다.

HA 중재자의 업그레이드

또한 BlueXP는 Cloud Volumes ONTAP 업그레이드 프로세스 중에 필요에 따라 중재자 인스턴스를 업데이트합니다.

업그레이드 준비

업그레이드를 수행하기 전에 시스템이 준비되어 있는지 확인하고 필요한 구성을 변경해야 합니다.

- [다운타임을 계획합니다](#)
- [자동 반환이 여전히 활성화되어 있는지 확인합니다](#)
- [SnapMirror 전송을 일시 중단합니다](#)
- [애그리게이트가 온라인 상태인지 확인합니다](#)

다운타임을 계획합니다

단일 노드 시스템을 업그레이드할 경우 업그레이드 프로세스에서는 I/O가 중단되는 동안 시스템을 최대 25분 동안 오프라인 상태로 전환합니다.

대부분의 경우 HA 쌍의 업그레이드는 무중단으로 가능하며 I/O는 중단되지 않습니다. 이 무중단 업그레이드 프로세스 중에 각 노드가 동시 업그레이드되어 클라이언트에 I/O를 계속 제공합니다.

세션 지향 프로토콜은 업그레이드 중 특정 영역의 클라이언트 및 애플리케이션에 부정적인 영향을 미칠 수 있습니다. 자세한 내용은 ["ONTAP 설명서를 참조하십시오"](#)

자동 반환이 여전히 활성화되어 있는지 확인합니다

Cloud Volumes ONTAP HA 쌍(기본 설정)에서 자동 반환이 활성화되어 있어야 합니다. 그렇지 않으면 작업이 실패합니다.

["ONTAP 9 설명서: 자동 반환 구성을 위한 명령입니다"](#)

## SnapMirror 전송을 일시 중단합니다

Cloud Volumes ONTAP 시스템에 활성 SnapMirror 관계가 있는 경우 Cloud Volumes ONTAP 소프트웨어를 업데이트하기 전에 전송을 일시 중지하는 것이 좋습니다. 전송을 일시 중단하면 SnapMirror 장애가 방지됩니다. 대상 시스템에서 전송을 일시 중지해야 합니다.



BlueXP 백업 및 복구는 SnapMirror 구현을 사용하여 백업 파일(SnapMirror Cloud라고 함)을 생성하지만 시스템을 업그레이드할 때 백업을 일시 중단할 필요가 없습니다.

이 작업에 대해

다음 단계에서는 버전 9.3 이상에서 System Manager를 사용하는 방법을 설명합니다.

단계

1. 대상 시스템에서 System Manager에 로그인합니다.

웹 브라우저에서 클러스터 관리 LIF의 IP 주소를 지정하면 System Manager에 로그인할 수 있습니다. Cloud Volumes ONTAP 작업 환경에서 IP 주소를 찾을 수 있습니다.



BlueXP에 액세스하는 컴퓨터에는 Cloud Volumes ONTAP에 대한 네트워크 연결이 있어야 합니다. 예를 들어, 클라우드 제공업체 네트워크에 있는 점프 호스트에서 BlueXP에 로그인해야 할 수 있습니다.

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

애그리게이트가 온라인 상태인지 확인합니다

소프트웨어를 업데이트하기 전에 Cloud Volumes ONTAP용 애그리게이트가 온라인 상태여야 합니다. 애그리게이트는 대부분의 구성에서 온라인 상태여야 하지만, 그렇지 않을 경우 온라인 상태로 전환할 수 있습니다.

이 작업에 대해

다음 단계에서는 버전 9.3 이상에서 System Manager를 사용하는 방법을 설명합니다.

단계

1. 작업 환경에서 \* 집계 \* 탭을 클릭합니다.
2. 집계 제목 아래에서 타원 버튼을 클릭한 다음 \* 집계 세부 정보 보기 \* 를 선택합니다.

| Aggregate Details |                     |
|-------------------|---------------------|
| aggr1             |                     |
| Overview          | Capacity Allocation |
| State             | online              |
| Home Node         | *****               |
| Encryption Type   | cloudEncrypted      |
| Volumes           | 2 ▾                 |

3. 애그리게이트는 오프라인 상태인 경우 System Manager를 사용하여 애그리게이트를 온라인 상태로 전환합니다.
  - a. 스토리지 > 애그리게이트 및 디스크 > 애그리게이트 \* 를 클릭합니다.
  - b. 애그리게이트를 선택한 다음 \* 추가 작업 > 상태 > 온라인 \* 을 클릭합니다.

### Cloud Volumes ONTAP를 업그레이드합니다

BlueXP는 새 버전을 업그레이드할 수 있을 때 사용자에게 알립니다. 이 알림에서 업그레이드 프로세스를 시작할 수 있습니다. 자세한 내용은 [을 참조하십시오](#) [BlueXP 알림에서 업그레이드합니다](#).

외부 URL의 이미지를 사용하여 소프트웨어 업그레이드를 수행하는 또 다른 방법입니다. 이 옵션은 BlueXP가 S3 버킷을 액세스하여 소프트웨어를 업그레이드할 수 없거나 패치가 제공된 경우에 유용합니다. 자세한 내용은 [을 참조하십시오](#) [URL에서 사용할 수 있는 이미지에서 업그레이드합니다](#).

### BlueXP 알림에서 업그레이드합니다

BlueXP는 새 버전의 Cloud Volumes ONTAP를 사용할 수 있을 때 Cloud Volumes ONTAP 작업 환경에 알림을 표시합니다.



이 알림에서 업그레이드 프로세스를 시작하여 S3 버킷에서 소프트웨어 이미지를 가져온 다음 이미지를 설치한 다음 시스템을 다시 시작하여 프로세스를 자동화할 수 있습니다.

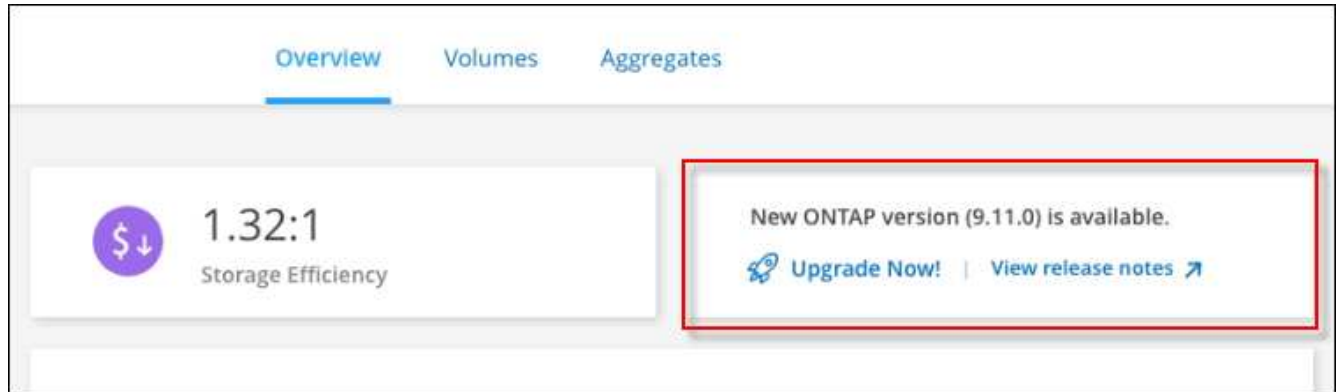
시작하기 전에

볼륨 또는 애그리게이트 생성과 같은 BlueXP 작업은 Cloud Volumes ONTAP 시스템에서 진행 중이지 않아야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. 작업 환경을 선택합니다.

새 버전을 사용할 수 있는 경우 개요 탭에 알림이 나타납니다.



3. 새 버전을 사용할 수 있는 경우 \* 지금 업그레이드! \* 를 클릭합니다

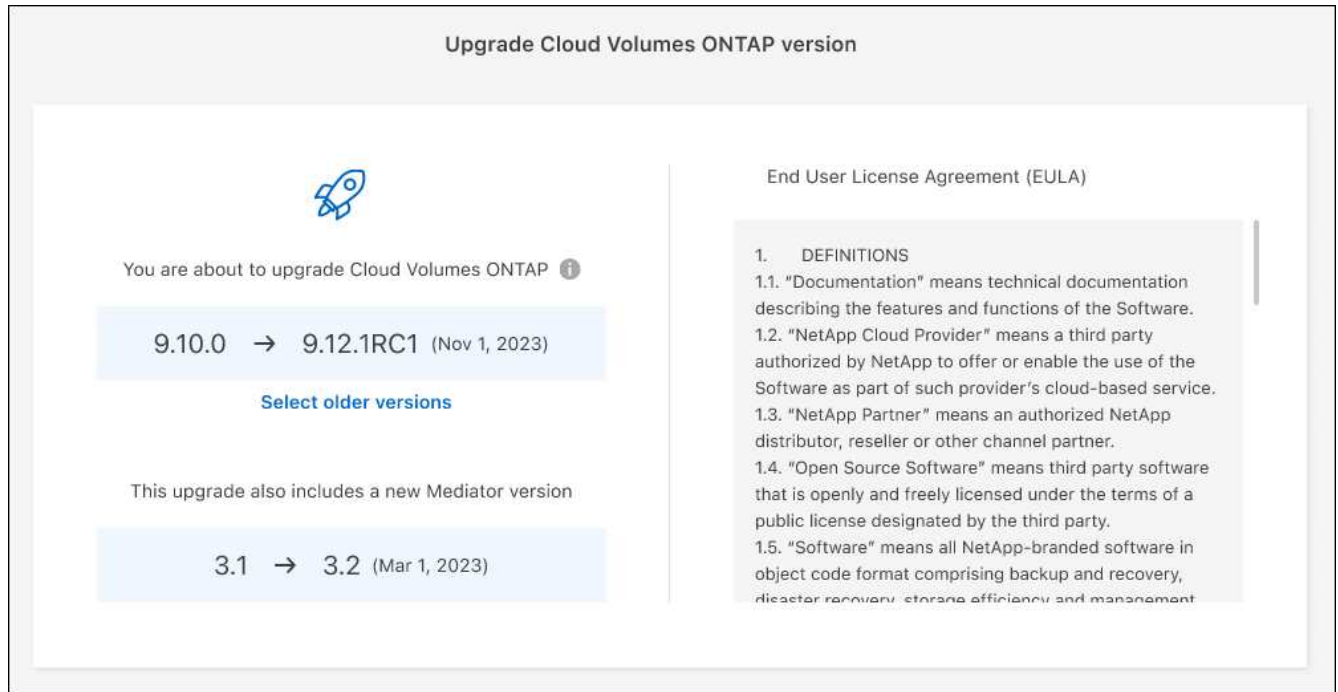


BlueXP 알림을 통해 Cloud Volumes ONTAP를 업그레이드하려면 먼저 NetApp Support 사이트 계정이 있어야 합니다.

4. Upgrade Cloud Volumes ONTAP 페이지에서 EULA를 읽은 다음 \* EULA \* 를 읽고 승인합니다 \* 를 선택합니다.
5. 업그레이드 \* 를 클릭합니다.



Upgrade Cloud Volumes ONTAP 페이지에서는 기본적으로 업그레이드할 최신 Cloud Volumes ONTAP 버전을 선택합니다. 사용 가능한 경우 \* 이전 버전 선택 \* 을 클릭하여 업그레이드를 위해 이전 버전의 Cloud Volumes ONTAP를 선택할 수 있습니다.  
을 참조하십시오 "지원되는 업그레이드 경로 목록입니다" 현재 Cloud Volumes ONTAP 버전을 기반으로 적절한 업그레이드 경로를 선택합니다.



6. 업그레이드 상태를 확인하려면 설정 아이콘을 클릭하고 \* 타임라인 \* 을 선택합니다.

#### 결과

BlueXP가 소프트웨어 업그레이드를 시작합니다. 소프트웨어 업데이트가 완료되면 작업 환경에서 작업을 수행할 수 있습니다.

#### 작업을 마친 후

SnapMirror 전송을 일시 중지한 경우 System Manager를 사용하여 전송을 다시 시작합니다.

URL에서 사용할 수 있는 이미지에서 업그레이드합니다

Cloud Volumes ONTAP 소프트웨어 이미지를 커넥터 또는 HTTP 서버에 배치한 다음 BlueXP에서 소프트웨어 업그레이드를 시작할 수 있습니다. BlueXP에서 S3 버킷을 액세스하여 소프트웨어를 업그레이드할 수 없는 경우 이 옵션을 사용할 수 있습니다.

#### 시작하기 전에

- 볼륨 또는 애그리게이트 생성과 같은 BlueXP 작업은 Cloud Volumes ONTAP 시스템에서 진행 중이지 않아야 합니다.
- HTTPS를 사용하여 ONTAP 이미지를 호스팅하는 경우 인증서 누락으로 인한 SSL 인증 문제로 인해 업그레이드가 실패할 수 있습니다. 해결 방법은 ONTAP와 BlueXP 간의 인증에 사용할 CA 서명 인증서를 생성하고 설치하는 것입니다.

NetApp 기술 문서로 이동하여 단계별 지침을 확인하십시오.

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

#### 단계

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

가상 네트워크에 VPN이 연결되어 있는 경우 Cloud Volumes ONTAP 소프트웨어 이미지를 자체 네트워크의

HTTP 서버에 배치할 수 있습니다. 그렇지 않으면 클라우드에 있는 HTTP 서버에 파일을 배치해야 합니다.

2. Cloud Volumes ONTAP에 대해 고유한 보안 그룹을 사용하는 경우 Cloud Volumes ONTAP가 소프트웨어 이미지에 액세스할 수 있도록 아웃바운드 규칙이 HTTP 연결을 허용하는지 확인합니다.



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

3. 에서 소프트웨어 이미지를 가져옵니다 "[NetApp Support 사이트](#)".
4. 파일을 제공할 Connector 또는 HTTP 서버의 디렉토리에 소프트웨어 이미지를 복사합니다.

두 개의 경로를 사용할 수 있습니다. 올바른 경로는 커넥터 버전에 따라 다릅니다.

- /opt/application/netapp/cloudmanager/docker\_occm/data/ontap/images/
- /opt/application/netapp/cloudmanager/ontap/images/

5. BlueXP의 작업 환경에서 \*... (타원 아이콘) \* 을 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 커넥터에 소프트웨어 이미지를 복사한 경우 다음 URL을 입력합니다.

http://<Connector-private-IP-address>/ontap/images/<image-file-name> 를 참조하십시오



URL에서 \* image-file-name \* 은 "cot.image.9.13.1P2.tgz" 형식을 따라야 합니다.

7. 계속하려면 \* Proceed \* (진행 \*)를 클릭합니다.

#### 결과

BlueXP가 소프트웨어 업데이트를 시작합니다. 소프트웨어 업데이트가 완료되면 작업 환경에서 작업을 수행할 수 있습니다.

#### 작업을 마친 후

SnapMirror 전송을 일시 중지한 경우 System Manager를 사용하여 전송을 다시 시작합니다.

#### Google Cloud NAT 게이트웨이를 사용할 때 다운로드 오류를 수정합니다

커넥터는 Cloud Volumes ONTAP용 소프트웨어 업데이트를 자동으로 다운로드합니다. 구성에서 Google Cloud NAT 게이트웨이를 사용하는 경우 다운로드가 실패할 수 있습니다. 소프트웨어 이미지를 분할하는 부품 수를 제한하여 이 문제를 해결할 수 있습니다. 이 단계는 BlueXP API를 사용하여 완료해야 합니다.

#### 단계

1. 다음과 같은 JSON을 본문으로 /occm/config에 PUT 요청을 제출합니다.

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



maxDownloadSessions\_ 값은 1이거나 1보다 큰 정수일 수 있습니다. 값이 1이면 다운로드한 이미지는 분할되지 않습니다.

32는 예제 값입니다. 사용할 값은 NAT 구성과 동시에 사용할 수 있는 세션 수에 따라 다릅니다.

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

## 선불 종량제 시스템을 등록하는 중입니다

NetApp의 지원은 Cloud Volumes ONTAP PAYGO 시스템에 포함되어 있지만 먼저 NetApp에 시스템을 등록하여 지원을 활성화해야 합니다.

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











지원이 등록되지 않은 시스템은 새 버전이 출시되어도 BlueXP에 나타나는 소프트웨어 업데이트 알림을 계속 받게 됩니다. 그러나 소프트웨어를 업그레이드하기 전에 시스템을 등록해야 합니다.

### 단계

1. NetApp Support 사이트 계정을 BlueXP에 아직 추가하지 않은 경우 \* 계정 설정 \* 으로 이동하여 지금 추가하십시오.

["NetApp Support 사이트 계정을 추가하는 방법을 알아보십시오"](#).

2. Canvas 페이지에서 등록할 시스템의 이름을 두 번 클릭합니다.
3. 개요 탭에서 기능 패널을 클릭한 다음 \* 지원 등록 \* 옆에 있는 연필 아이콘을 클릭합니다.

| Information              |                            | Features                                                                                      |
|--------------------------|----------------------------|-----------------------------------------------------------------------------------------------|
| Working Environment 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               |                            |          |

4. NetApp Support 사이트 계정을 선택하고 \* Register \* 를 클릭합니다.

결과

BlueXP는 시스템을 NetApp에 등록합니다.

## Cloud Volumes ONTAP의 상태 관리

BlueXP에서 Cloud Volumes ONTAP를 중지하고 시작하여 클라우드 컴퓨팅 비용을 관리할 수 있습니다.

### Cloud Volumes ONTAP의 자동 종료 예약

특정 시간 간격 동안 Cloud Volumes ONTAP를 종료하여 컴퓨팅 비용을 낮출 수 있습니다. 이 작업을 수동으로 수행하는 대신 특정 시간에 시스템이 자동으로 종료된 후 다시 시작하도록 BlueXP를 구성할 수 있습니다.

이 작업에 대해

- Cloud Volumes ONTAP 시스템의 자동 종료를 예약하면 활성 데이터 전송이 진행 중인 경우 BlueXP가 종료를 연기합니다.









전송이 완료된 후 BlueXP가 시스템을 종료합니다.

- 이 작업은 HA 2노드에서 두 노드의 자동 종료를 예약합니다.
- 예약된 종료를 통해 Cloud Volumes ONTAP를 끝 때 부팅 및 루트 디스크의 스냅샷이 생성되지 않습니다.

스냅샷은 다음 섹션에 설명된 대로 수동 종료를 수행할 때만 자동으로 생성됩니다.

단계

1. Canvas 페이지에서 원하는 작업 환경을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 예정된 가동 중지 시간 \* 옆에 있는 연필 아이콘을 클릭합니다.

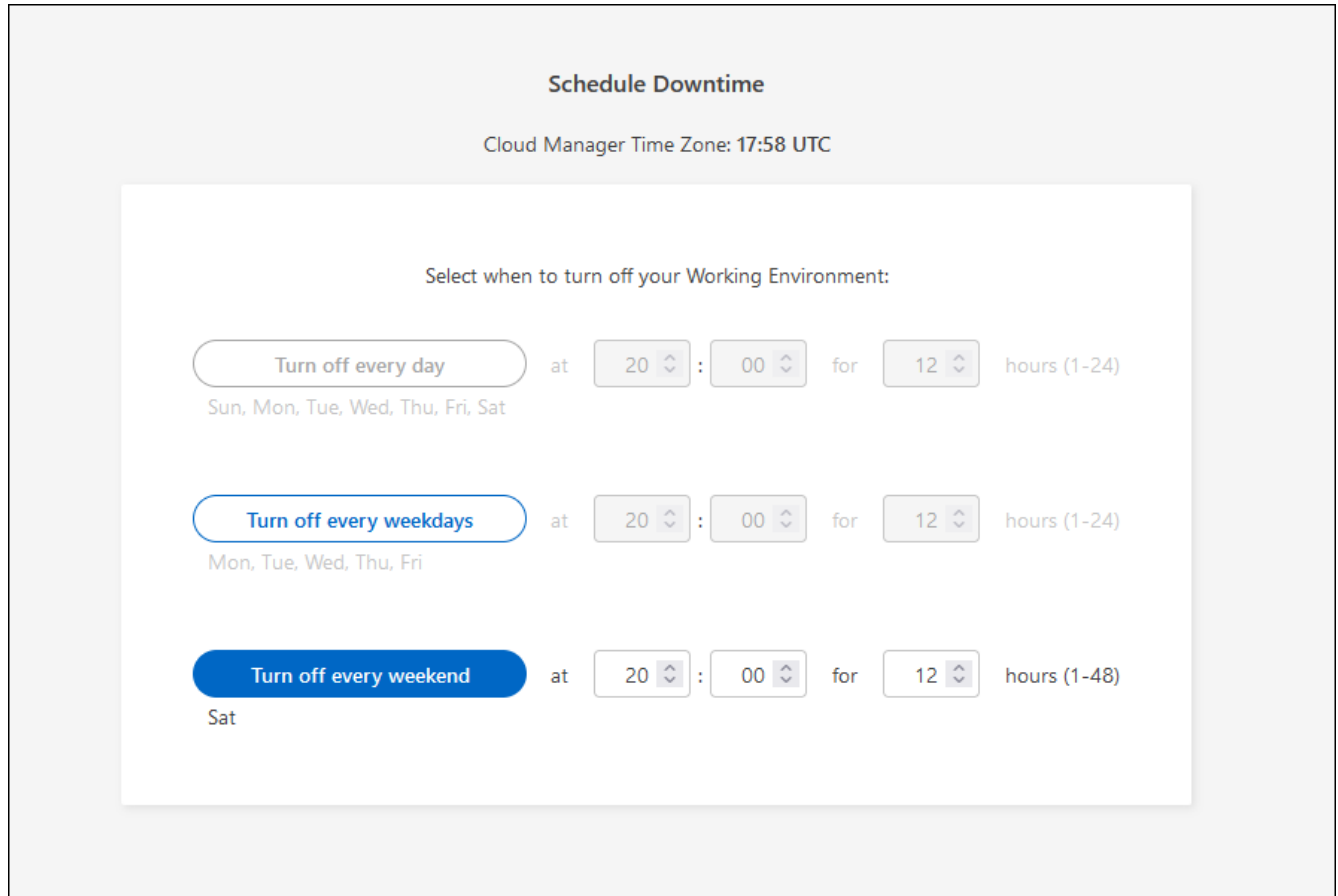
| Information              | Features                                                                                                       |
|--------------------------|----------------------------------------------------------------------------------------------------------------|
| Working Environment 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               |                           |

3. 종료 일정을 지정합니다.

- 매일, 매주 평일, 매주 또는 세 가지 옵션의 조합을 종료할지 여부를 선택합니다.
- 시스템 전원을 끌 시기 및 시스템 전원을 끌 시간을 지정합니다.

▪ 예 \*

다음 이미지는 매주 토요일 오후 20시에 BlueXP가 시스템을 종료하도록 지시하는 스케줄을 보여줍니다 (오후 8:00) 12시간 동안 BlueXP는 매주 월요일 오전 12시에 시스템을 다시 시작합니다



4. 저장 \* 을 클릭합니다.

결과

BlueXP는 일정을 저장합니다. Features(기능) 패널 아래의 해당 Scheduled Downtime line(예정된 가동 중지 라인) 항목에 'On(켜짐)'이 표시됩니다.

**Cloud Volumes ONTAP**를 중지하는 중입니다

Cloud Volumes ONTAP를 중지하면 계산 비용이 절약되고 루트 및 부팅 디스크의 스냅샷이 생성되므로 문제 해결에 도움이 됩니다.



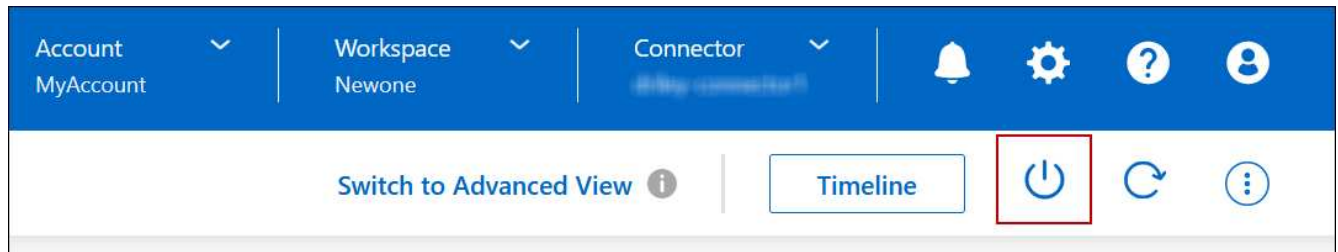
비용을 줄이기 위해 BlueXP는 루트 및 부팅 디스크의 이전 스냅샷을 주기적으로 삭제합니다. 루트와 부팅 디스크 모두에 대해 가장 최근의 두 스냅샷만 보존됩니다.

이 작업에 대해

HA 쌍을 중지하면 BlueXP가 두 노드를 모두 종료합니다.

단계

1. 작업 환경에서 \* 끄기 \* 아이콘을 클릭합니다.



2. 스냅샷이 시스템 복구를 활성화할 수 있으므로 스냅샷을 생성하는 옵션을 활성 상태로 유지합니다.
3. 끄기 \* 를 클릭합니다.

시스템을 중지하는 데 몇 분 정도 걸릴 수 있습니다. 나중에 작업 환경 페이지에서 시스템을 다시 시작할 수 있습니다.



스냅샷은 재부팅 시 자동으로 생성됩니다.

## NTP를 사용하여 시스템 시간을 동기화합니다

NTP 서버를 지정하면 네트워크 시스템 간의 시간이 동기화되어 시간 차이로 인한 문제를 방지할 수 있습니다.

를 사용하여 NTP 서버를 지정합니다 **"BlueXP API"** 또는 사용자 인터페이스에서 **"CIFS 서버를 생성합니다"**.

## 시스템 쓰기 속도를 수정합니다

BlueXP를 사용하면 Cloud Volumes ONTAP에 대한 일반 또는 고속 쓰기 속도를 선택할 수 있습니다. 기본 쓰기 속도는 정상입니다. 워크로드에 빠른 쓰기 성능이 필요한 경우 빠른 쓰기 속도로 변경할 수 있습니다.

모든 유형의 단일 노드 시스템 및 일부 HA 쌍 구성에서 고속 쓰기 속도가 지원됩니다. 에서 지원되는 구성을 봅니다 **"Cloud Volumes ONTAP 릴리즈 노트"**









쓰기 속도를 변경하려면 먼저 해야 합니다 **"정상 설정과 높음 설정의 차이를 이해합니다"**.

이 작업에 대해

- 볼륨 또는 애그리게이트 생성과 같은 작업이 진행 중이 아닌지 확인합니다.
- 이 변경 사항은 Cloud Volumes ONTAP 시스템을 다시 시작합니다. 이는 전체 시스템의 다운타임이 필요한 업무 중단입니다.

단계

1. Canvas 페이지에서 쓰기 속도로 구성하는 시스템의 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 쓰기 속도 \* 옆에 있는 연필 아이콘을 클릭합니다.

| Information              | Features                                                                                                       |
|--------------------------|----------------------------------------------------------------------------------------------------------------|
| Working Environment 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               |                           |

3. Normal \* (정상 \*) 또는 \* High \* (높음 \*)를 선택합니다.

높음 을 선택한 경우 "이해했습니다..." 문장을 읽고 확인란을 선택하여 확인해야 합니다.



고속 \* 쓰기 속도 옵션은 버전 9.13.0부터 Google Cloud의 Cloud Volumes ONTAP HA 쌍에서 지원됩니다.

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

## Cloud Volumes ONTAP의 암호를 변경합니다

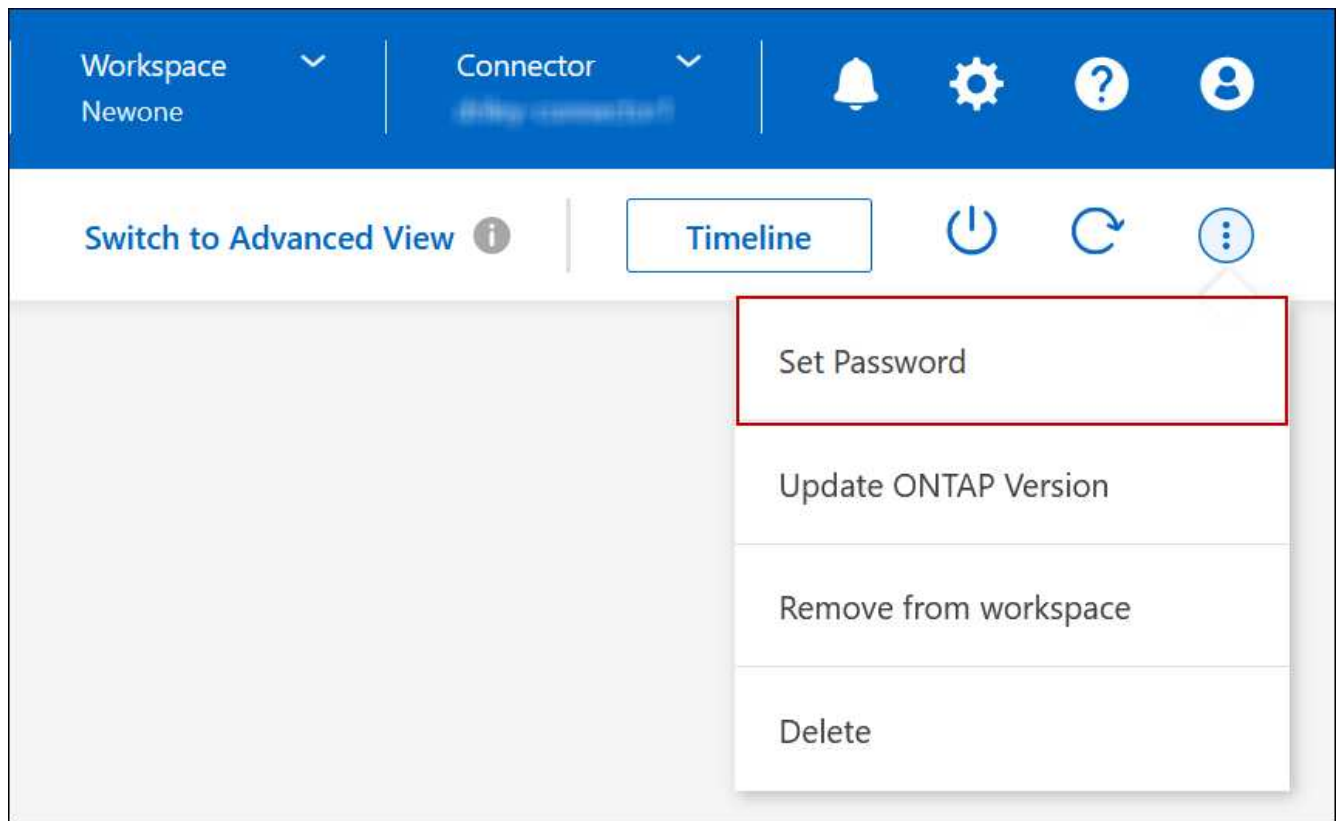
Cloud Volumes ONTAP에는 클러스터 관리자 계정이 포함되어 있습니다. 필요한 경우 BlueXP에서 이 계정의 암호를 변경할 수 있습니다.



System Manager 또는 CLI를 통해 admin 계정의 암호를 변경하지 마십시오. 암호는 BlueXP에 반영되지 않습니다. 따라서 BlueXP는 인스턴스를 제대로 모니터링할 수 없습니다.

단계

1. Canvas 페이지에서 Cloud Volumes ONTAP 작업 환경의 이름을 두 번 클릭합니다.
2. BlueXP 콘솔의 오른쪽 상단에서 타원 아이콘을 클릭하고 \* 암호 설정 \* 을 선택합니다.



새 암호는 마지막으로 사용한 6개의 암호 중 하나와 달라야 합니다.

## 시스템을 추가, 제거 또는 삭제합니다

기존 **Cloud Volumes ONTAP** 시스템을 **BlueXP**에 추가

기존 Cloud Volumes ONTAP 시스템을 검색하고 BlueXP에 추가할 수 있습니다. 새 BlueXP



시스템을 배포한 경우 이 작업을 수행할 수 있습니다.

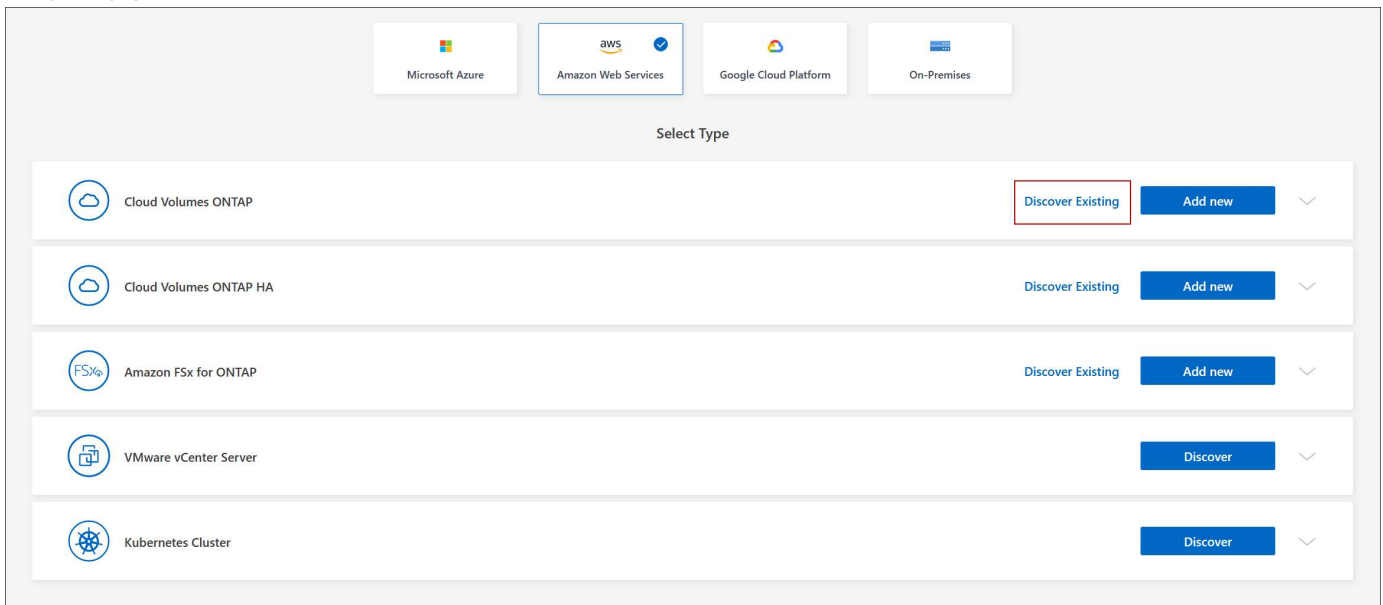
시작하기 전에

Cloud Volumes ONTAP admin 사용자 계정의 암호를 알아야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭합니다.
3. 시스템이 상주하는 클라우드 공급자를 선택합니다.
4. Cloud Volumes ONTAP 시스템의 유형을 선택합니다.
5. 기존 시스템을 검색하려면 링크를 클릭하십시오.

를 누릅니다



1. 영역 페이지에서 인스턴스가 실행 중인 영역을 선택한 다음 인스턴스를 선택합니다.
2. 자격 증명 페이지에서 Cloud Volumes ONTAP 관리자 사용자의 암호를 입력한 다음 \* GO \* 를 클릭합니다.

결과

BlueXP는 Cloud Volumes ONTAP 인스턴스를 작업 영역에 추가합니다.

### Cloud Volumes ONTAP 작업 환경 제거

계정 관리자는 Cloud Volumes ONTAP 작업 환경을 제거하여 다른 시스템으로 이동하거나 검색 문제를 해결할 수 있습니다.

이 작업에 대해

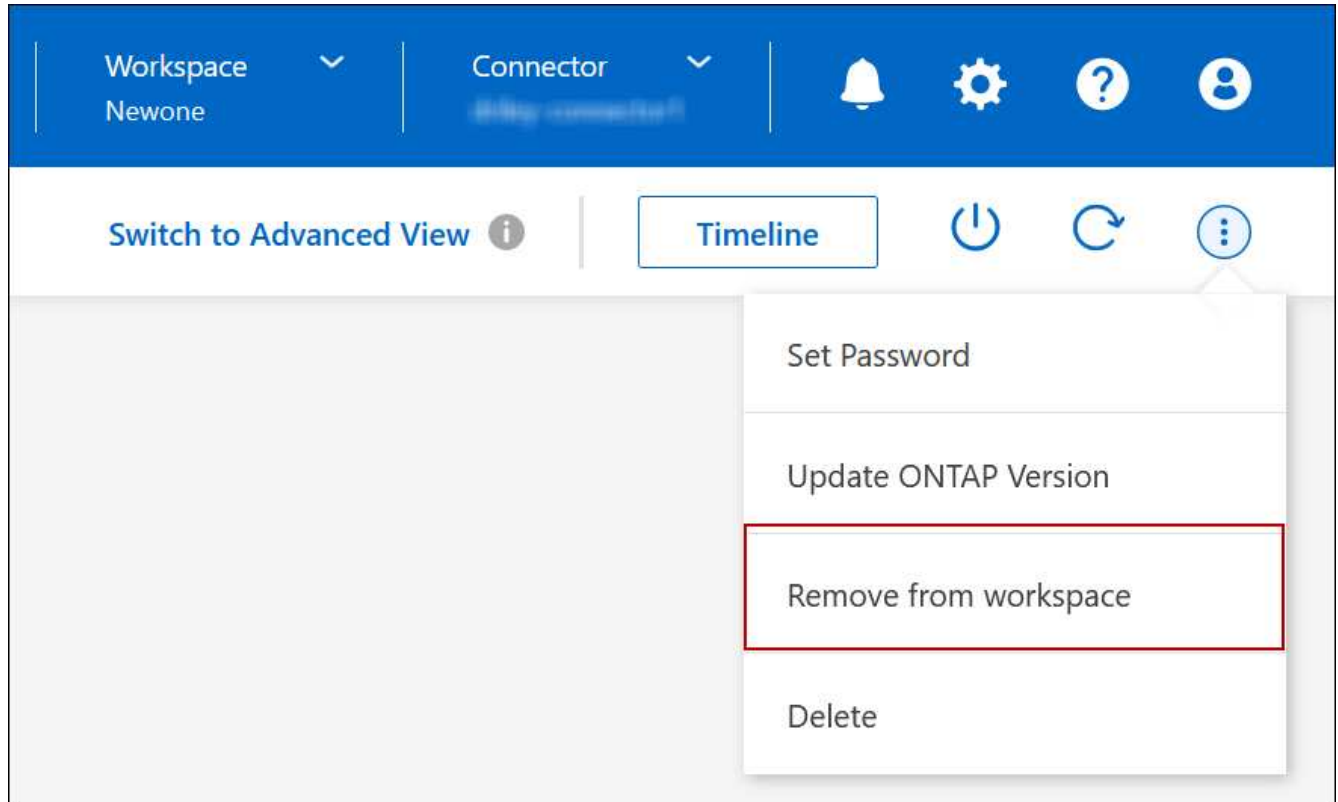
Cloud Volumes ONTAP 작업 환경을 제거하면 BlueXP에서 제거됩니다. Cloud Volumes ONTAP 시스템은 삭제되지 않습니다. 나중에 작업 환경을 다시 검색할 수 있습니다.

BlueXP에서 작업 환경을 제거하면 다음과 같은 작업을 수행할 수 있습니다.

- 다른 작업 공간에서 다시 검색합니다
- 다른 BlueXP 시스템에서 재검색합니다
- 초기 검색 중에 문제가 발생한 경우 다시 검색합니다

단계

1. Canvas 페이지에서 제거할 작업 환경을 두 번 클릭합니다.
2. BlueXP 콘솔의 오른쪽 상단에서 타원 아이콘을 클릭하고 \* 작업 영역에서 제거 \* 를 선택합니다.



3. 작업 공간에서 검토 창에서 \* 제거 \* 를 클릭합니다.

결과

BlueXP는 작업 환경을 제거합니다. 사용자는 언제든지 Canvas 페이지에서 이 작업 환경을 다시 검색할 수 있습니다.

### Cloud Volumes ONTAP 시스템 삭제

클라우드 공급자의 콘솔이 아닌 BlueXP에서 Cloud Volumes ONTAP 시스템을 항상 삭제해야 합니다. 예를 들어, 클라우드 공급자로부터 라이선스가 부여된 Cloud Volumes ONTAP 인스턴스를 종료하는 경우 다른 인스턴스에 대해 라이선스 키를 사용할 수 없습니다. 라이선스를 해제하려면 BlueXP에서 작업 환경을 삭제해야 합니다.

작업 환경을 삭제하면 BlueXP에서 Cloud Volumes ONTAP 인스턴스를 종료하고 디스크 및 스냅샷을 삭제합니다.

BlueXP 백업 및 복구, BlueXP 분류 인스턴스 등과 같은 다른 서비스에서 관리하는 리소스는 작업 환경을 삭제할 때 삭제되지 않습니다. 수동으로 삭제해야 합니다. 그렇지 않으면 이러한 리소스에 대한 비용을 계속 받게 됩니다.



BlueXP가 클라우드 공급업체에 Cloud Volumes ONTAP를 배포할 때 인스턴스에 대한 종료 보호를 활성화합니다. 이 옵션은 우발적인 종료를 방지하는 데 도움이 됩니다.

## 단계

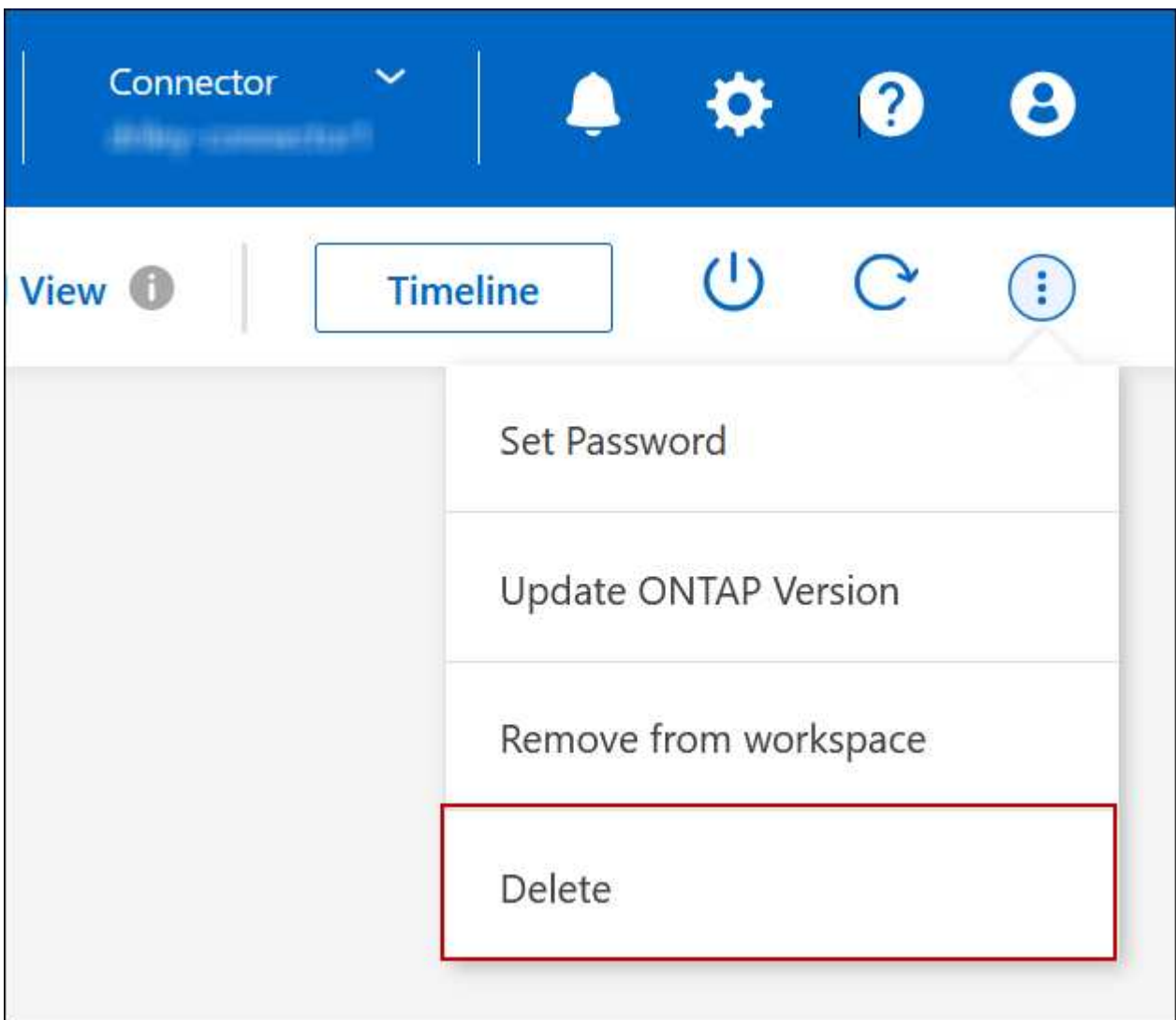
1. 작업 환경에서 BlueXP 백업 및 복구를 활성화한 경우 백업된 데이터가 여전히 필요한지 확인한 다음 **"필요한 경우 백업을 삭제합니다"**.

BlueXP 백업 및 복구는 설계상 Cloud Volumes ONTAP와 독립적입니다. Cloud Volumes ONTAP 시스템을 삭제할 때 BlueXP 백업 및 복구는 자동으로 백업을 삭제하지 않으며, 시스템이 삭제된 후 백업을 삭제할 수 있도록 UI에 현재 지원이 없습니다.

2. 이 작업 환경에서 BlueXP 분류를 사용하도록 설정했고 다른 작업 환경에서 이 서비스를 사용하지 않는 경우 서비스 인스턴스를 삭제해야 합니다.

**"BlueXP 분류 인스턴스에 대해 자세히 알아보십시오"**.

3. Cloud Volumes ONTAP 작업 환경을 삭제합니다.
  - a. Canvas 페이지에서 삭제할 Cloud Volumes ONTAP 작업 환경의 이름을 두 번 클릭합니다.
  - b. BlueXP 콘솔의 오른쪽 상단에서 타원 아이콘을 클릭하고 \* 삭제 \* 를 선택합니다.



c. 작업 환경 삭제 창에서 작업 환경의 이름을 입력한 다음 \* 삭제 \* 를 클릭합니다.

작업 환경을 삭제하는 데 최대 5분이 걸릴 수 있습니다.

## 설치하고

**Cloud Volumes ONTAP**의 **EC2** 인스턴스 유형을 변경합니다

AWS에서 Cloud Volumes ONTAP를 시작할 때 여러 인스턴스 또는 유형 중에서 선택할 수 있습니다. 필요에 따라 크기가 작거나 크기 초과로 결정되면 언제든지 인스턴스 유형을 변경할 수 있습니다.

이 작업에 대해

- Cloud Volumes ONTAP HA 쌍(기본 설정)에서 자동 반환이 활성화되어 있어야 합니다. 그렇지 않으면 작업이 실패합니다.

"ONTAP 9 설명서: 자동 반환 구성을 위한 명령입니다"

- 인스턴스 유형을 변경하면 AWS 서비스 요금에 영향을 줄 수 있습니다.
- Cloud Volumes ONTAP가 다시 시작됩니다.

단일 노드 시스템의 경우 입출력이 중단됩니다.

HA 쌍의 경우 변경은 무중단 것입니다. HA 쌍이 계속해서 데이터를 제공합니다.











BlueXP는 테이크오버를 시작하고 Giveback을 기다리면서 한 번에 하나의 노드를 정상적으로 변경합니다. NetApp의 QA 팀은 이 프로세스 중에 파일 쓰기와 읽기를 모두 테스트했지만 클라이언트 측에서는 문제가 발생하지 않았습니다. 접속이 변경됨에 따라 입출력 레벨에서 재시도 횟수가 확인되었지만 애플리케이션 계층은 NFS/CIFS 연결의 이러한 짧은 "재연결"을 극복했습니다.

참조하십시오

AWS에서 지원되는 인스턴스 유형 목록은 를 참조하십시오 "[지원되는 EC2 인스턴스](#)".

단계

1. Canvas 페이지에서 작업 환경을 선택합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 인스턴스 유형 \* 옆에 있는 연필 아이콘을 클릭합니다.

| Information              | Features                                                                                                       |
|--------------------------|----------------------------------------------------------------------------------------------------------------|
| Working Environment 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               |                           |

a. 노드 기반 PAYGO 라이선스를 사용하는 경우 \* 라이선스 유형 \* 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스 및 인스턴스 유형을 선택할 수도 있습니다.

3. 인스턴스 유형을 선택하고 확인란을 선택하여 변경의 영향을 이해했는지 확인한 다음 \* 변경 \* 을 클릭합니다.

결과

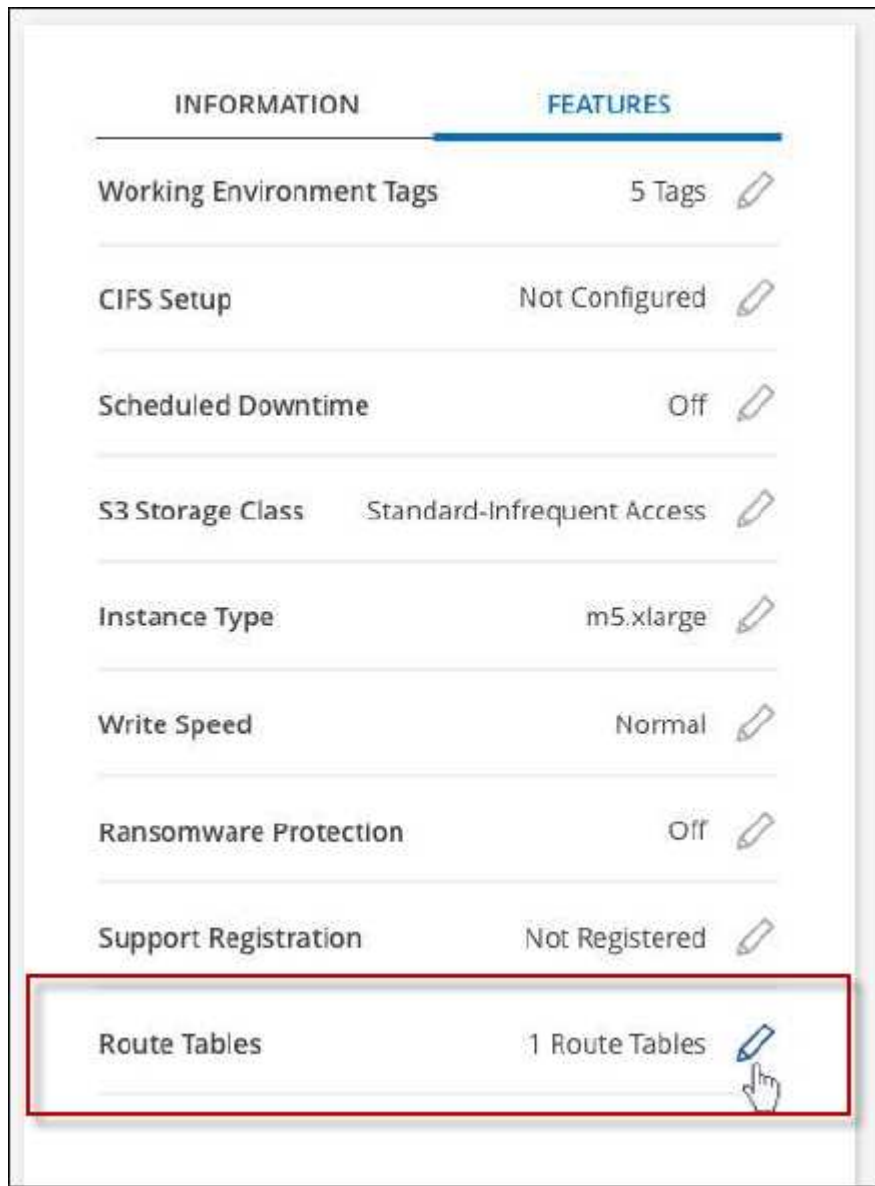
Cloud Volumes ONTAP가 새 구성으로 재부팅됩니다.

여러 AZs에서 HA 쌍의 경로 테이블을 변경합니다

여러 AZs(AWS Availability Zone)에 구축된 HA 쌍의 부동 IP 주소에 대한 라우트가 포함된 AWS 경로 테이블을 수정할 수 있습니다. 새로운 NFS 또는 CIFS 클라이언트가 AWS의 HA 쌍에 액세스해야 하는 경우 이 작업을 수행할 수 있습니다.

단계

1. Canvas 페이지에서 작업 환경을 선택합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 경로 표 \* 옆에 있는 연필 아이콘을 클릭합니다.



3. 선택한 라우팅 테이블 목록을 수정하고 \* 저장 \* 을 클릭합니다.

결과

BlueXP는 AWS 요청을 전송하여 경로 테이블을 수정합니다.

## Azure 관리

### Cloud Volumes ONTAP의 Azure VM 유형을 변경합니다

Microsoft Azure에서 Cloud Volumes ONTAP를 시작할 때 여러 VM 유형 중에서 선택할 수 있습니다. 필요에 따라 크기가 작거나 특대형 것으로 판단될 경우 언제든지 VM 유형을 변경할 수 있습니다.

이 작업에 대해

- Cloud Volumes ONTAP HA 쌍(기본 설정)에서 자동 반환이 활성화되어 있어야 합니다. 그렇지 않으면 작업이 실패합니다.

"ONTAP 9 설명서: 자동 반환 구성을 위한 명령입니다"

- VM 유형을 변경하면 Microsoft Azure 서비스 요금에 영향을 줄 수 있습니다.
- Cloud Volumes ONTAP가 다시 시작됩니다.

단일 노드 시스템의 경우 입출력이 중단됩니다.

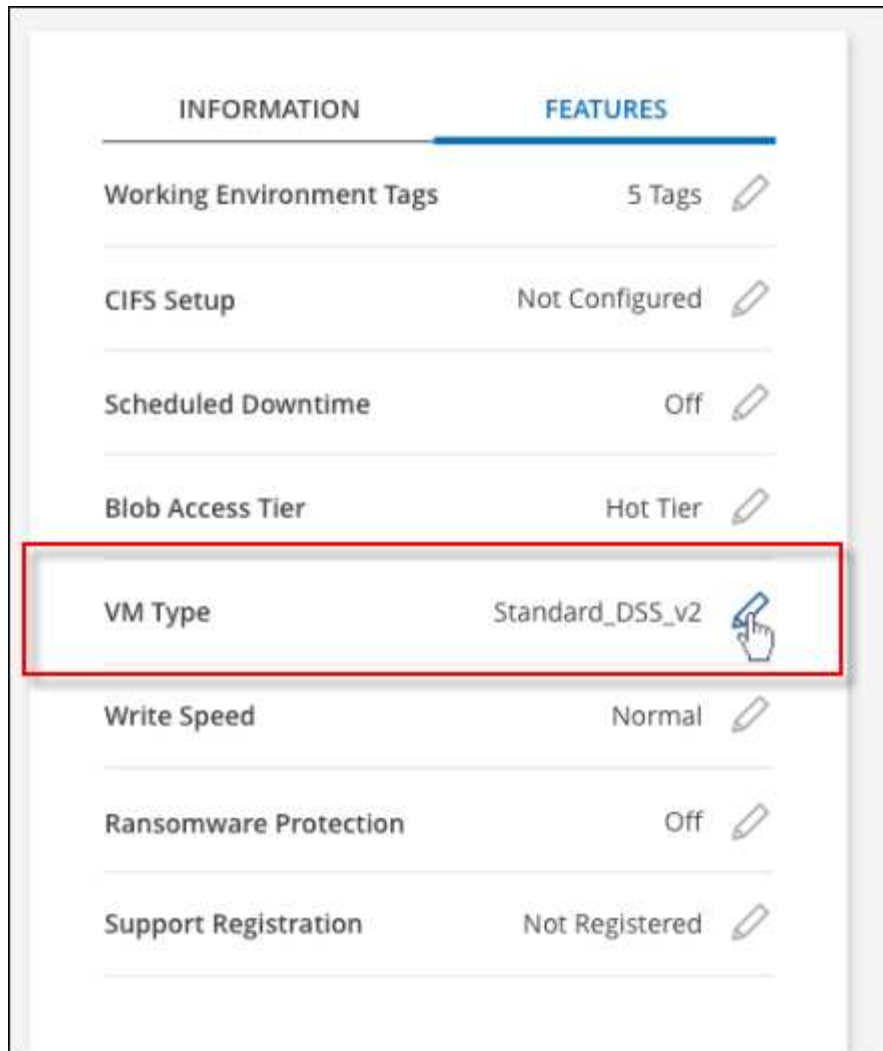
HA 쌍의 경우 변경은 무중단 것입니다. HA 쌍이 계속해서 데이터를 제공합니다.



BlueXP는 테이크오버를 시작하고 Giveback을 기다리면서 한 번에 하나의 노드를 정상적으로 변경합니다. NetApp의 QA 팀은 이 프로세스 중에 파일 쓰기와 읽기를 모두 테스트했지만 클라이언트 측에서는 문제가 발생하지 않았습니다. 접속이 변경됨에 따라 입출력 레벨에서 재시도 횟수가 확인되었지만 애플리케이션 계층은 NFS/CIFS 연결의 이러한 짧은 "재연결"을 극복했습니다.

단계

1. Canvas 페이지에서 작업 환경을 선택합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* VM 유형 \* 옆에 있는 연필 아이콘을 클릭합니다.



a. 노드 기반 PAYGO 라이선스를 사용하는 경우 \* 라이선스 유형 \* 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스 및 VM 유형을 선택할 수 있습니다.

3. VM 유형을 선택하고 확인란을 선택하여 변경의 영향을 이해했는지 확인한 다음 \* 변경 \* 을 클릭합니다.

결과

Cloud Volumes ONTAP가 새 구성으로 재부팅됩니다.

### Azure의 Cloud Volumes ONTAP HA 쌍에 대한 CIFS 잠금 재정의

계정 관리자는 BlueXP에서 Azure 유지 관리 이벤트 중에 Cloud Volumes ONTAP 스토리지 반환과 관련된 문제를 방지하는 설정을 활성화할 수 있습니다. 이 설정을 활성화하면 Cloud Volumes ONTAP가 CIFS 잠금을 확인하고 활성 CIFS 세션을 재설정합니다.

이 작업에 대해

Microsoft Azure는 가상 시스템에서 정기적인 유지 관리 이벤트를 예약합니다. Cloud Volumes ONTAP HA 쌍에서 유지보수 이벤트가 발생하면 HA 쌍이 스토리지 테이크오버 시작됩니다. 이 유지 관리 이벤트 중에 활성 CIFS 세션이 있는 경우 CIFS 파일의 잠금이 스토리지 반환을 방지할 수 있습니다.

이 설정을 활성화하면 Cloud Volumes ONTAP가 잠금을 거부하여 활성 CIFS 세션을 재설정합니다. 따라서 HA 쌍이 이러한 유지보수 이벤트 중에 스토리지 반환을 완료할 수 있습니다.





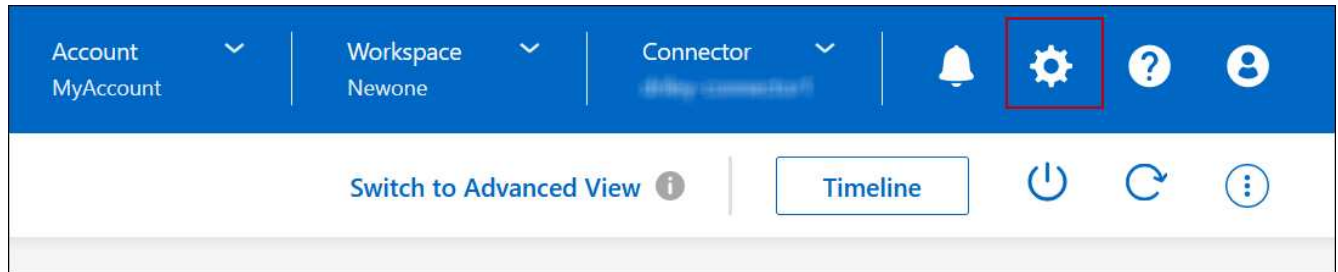
이 프로세스는 CIFS 클라이언트에 영향을 줄 수 있습니다. CIFS 클라이언트에서 커밋되지 않은 데이터는 손실될 수 있습니다.

#### 필요한 것

BlueXP 설정을 변경하려면 먼저 커넥터를 만들어야 합니다. "[자세히 알아보기](#)".

#### 단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 클릭하고 \* 커넥터 설정 \* 을 선택합니다.



2. Azure \* 에서 \* Azure HA 작업 환경에 대한 \* Azure CIFS 잠금을 클릭합니다.
3. 확인란을 클릭하여 기능을 활성화한 다음 \* 저장 \* 을 클릭합니다.

#### Azure Private Link 또는 서비스 끝점을 사용합니다

Cloud Volumes ONTAP는 Azure 프라이빗 링크를 사용하여 연결된 저장소 계정에 연결합니다. 필요한 경우 Azure Private Links를 비활성화하고 서비스 끝점을 대신 사용할 수 있습니다.

#### 개요

기본적으로 BlueXP는 Cloud Volumes ONTAP과 관련 저장소 계정 간의 연결을 위해 Azure 개인 링크를 활성화합니다. Azure Private Link는 Azure의 엔드포인트 간 연결을 보호하고 성능상의 이점을 제공합니다.

필요한 경우 Azure 프라이빗 링크 대신 서비스 끝점을 사용하도록 Cloud Volumes ONTAP를 구성할 수 있습니다.

BlueXP는 두 가지 구성 모두 Cloud Volumes ONTAP 및 스토리지 계정 간의 연결을 위해 항상 네트워크 액세스를 제한합니다. 네트워크 액세스는 Cloud Volumes ONTAP가 배포된 VNET와 커넥터가 배포된 VNET로 제한됩니다.

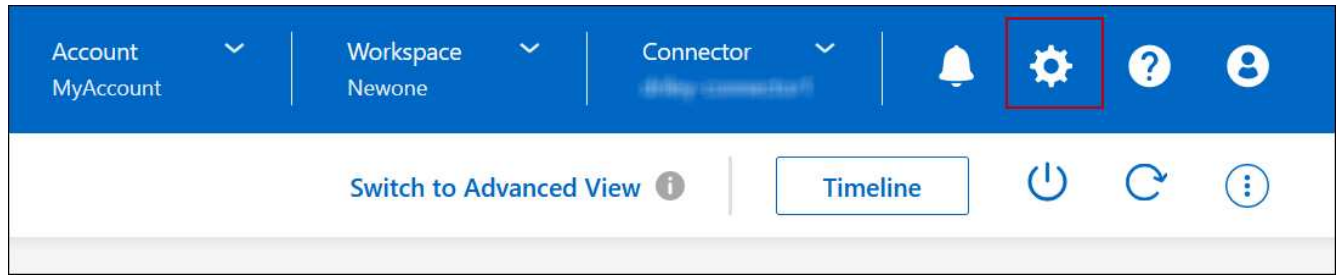
대신 **Azure** 전용 링크를 비활성화하고 서비스 끝점을 사용합니다

회사에서 요구하는 경우, BlueXP에서 Azure Private Link 대신 서비스 끝점을 사용하도록 Cloud Volumes ONTAP를 구성하도록 설정을 변경할 수 있습니다. 이 설정을 변경하면 새로 만든 Cloud Volumes ONTAP 시스템에 적용됩니다. 서비스 끝점은 에서만 지원됩니다 "[Azure 지역 쌍](#)" 커넥터와 Cloud Volumes ONTAP VNETs 사이.

커넥터는 해당 커넥터가 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 영역에 배포하거나 에 배포되어야 합니다 "[Azure 지역 쌍](#)" Cloud Volumes ONTAP 시스템의 경우

#### 단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 클릭하고 \* 커넥터 설정 \* 을 선택합니다.



2. Azure \* 에서 \* Azure Private Link \* 를 클릭합니다.
3. Cloud Volumes ONTAP 및 스토리지 계정 간 \* 프라이빗 링크 연결을 선택 취소합니다.
4. 저장 \* 을 클릭합니다.

작업을 마친 후

Azure Private Links를 사용하지 않도록 설정하고 Connector가 프록시 서버를 사용하는 경우 직접 API 트래픽을 활성화해야 합니다.

["Connector에서 직접 API 트래픽을 활성화하는 방법에 대해 알아봅니다"](#)

#### Azure 개인 링크 사용

대부분의 경우 Cloud Volumes ONTAP로 Azure Private 링크를 설정할 필요가 없습니다. BlueXP는 Azure 프라이빗 링크를 관리합니다. 그러나 기존 Azure Private DNS 영역을 사용하는 경우에는 구성 파일을 편집해야 합니다.

#### 사용자 지정 DNS 요구 사항

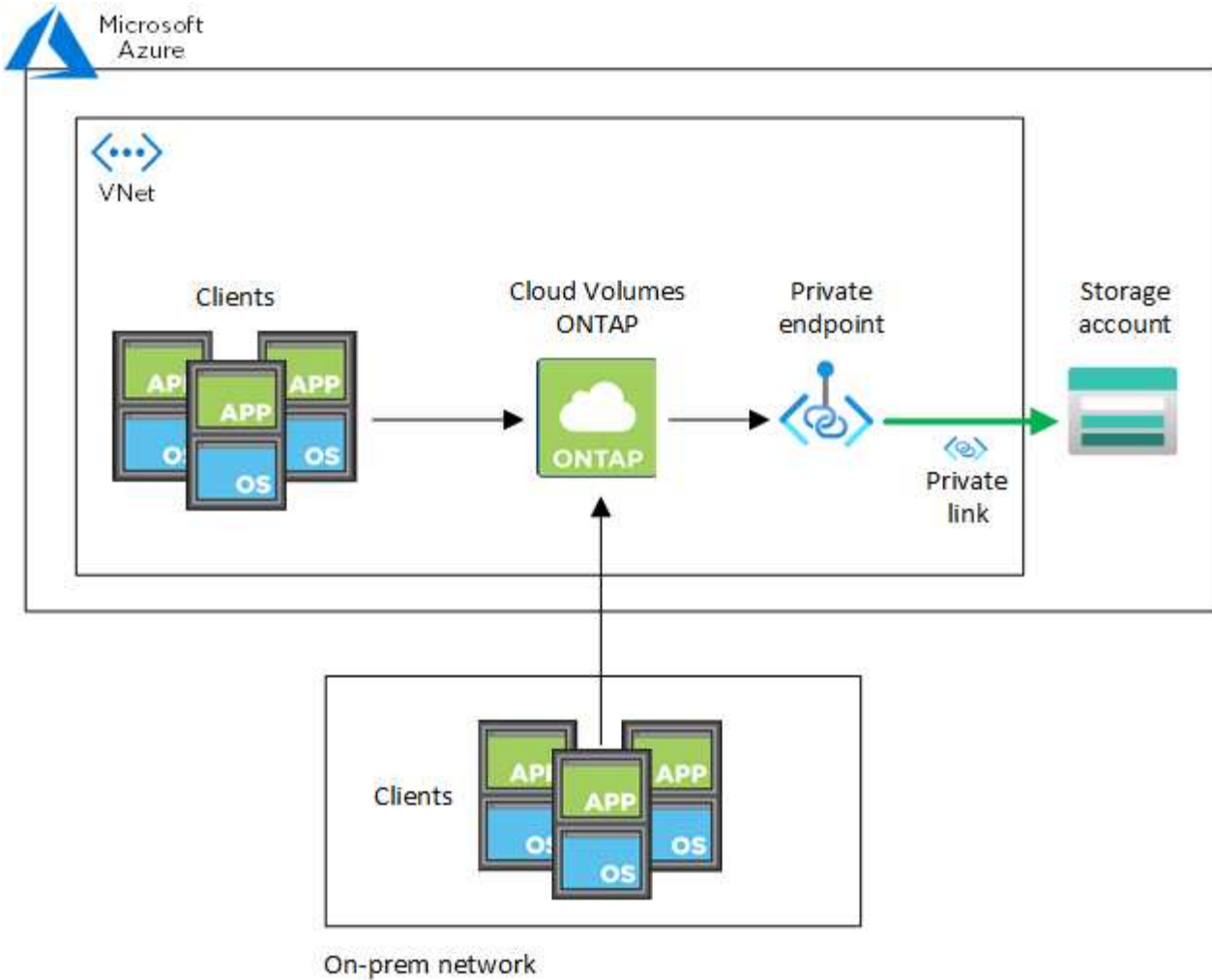
필요에 따라 사용자 지정 DNS로 작업하는 경우 사용자 지정 DNS 서버에서 Azure 개인 DNS 영역에 조건부 전달자를 만들어야 합니다. 자세한 내용은 [을 참조하십시오 "DNS 전달자 사용에 대한 Azure의 설명서"](#).

#### 개별 링크 연결의 작동 방식

BlueXP는 Azure에 Cloud Volumes ONTAP를 배포할 때 리소스 그룹에 개인 끝점을 만듭니다. 프라이빗 엔드포인트는 Cloud Volumes ONTAP의 스토리지 계정과 연결되어 있습니다. 따라서 Cloud Volumes ONTAP 스토리지에 대한 액세스는 Microsoft 백본 네트워크를 통해 이루어집니다.

클라이언트가 Cloud Volumes ONTAP와 동일한 VNET 내에 있거나, 피어링된 VNETs 내에 있거나, VNET에 대한 전용 VPN 또는 ExpressRoute 연결을 사용할 때 사내 네트워크에 있는 경우 클라이언트 액세스는 개인 링크를 통해 이루어집니다.

이 예에서는 동일한 VNET 내의 전용 링크와 전용 VPN 또는 ExpressRoute 연결이 있는 온프레미스 네트워크에서 클라이언트 액세스를 보여 줍니다.



커넥터 및 Cloud Volumes ONTAP 시스템이 다른 VNets에 구축된 경우 커넥터가 배포된 VNET와 Cloud Volumes ONTAP 시스템이 배포된 VNET 간에 VNET 피어링을 설정해야 합니다.

**Azure** 프라이빗 DNS에 대한 자세한 내용은 **BlueXP**를 참조하십시오

를 사용하는 경우 "**Azure 프라이빗 DNS**" 그런 다음 각 Connector에서 설정 파일을 수정해야 합니다. 그렇지 않으면 BlueXP에서 Cloud Volumes ONTAP 및 관련 저장소 계정 간에 Azure Private Link 연결을 활성화할 수 없습니다.

DNS 이름은 Azure DNS 명명 요구 사항과 일치해야 합니다 "**Azure 설명서에 나와 있는 대로 적용됩니다**".

단계

1. 커넥터 호스트에 SSH로 접속하고 로그인합니다.
2. /opt/application/netapp/cloudmanager/docker\_occm/data 디렉토리로 이동합니다
3. "user-private-dns-zone-settings" 매개 변수를 다음 키워드 값 쌍으로 추가하여 app.conf를 편집합니다.

```
"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
}
```

아래와 같이 "system-id"와 동일한 수준으로 매개 변수를 입력해야 합니다.

```
"system-id" : "<system ID>",
"user-private-dns-zone-settings" : {
```

전용 DNS 영역이 Connector와 다른 구독에 있는 경우에만 subscription 키워드가 필요합니다.

#### 4. 파일을 저장하고 Connector를 로그오프합니다.

재부팅할 필요는 없습니다.

### 장애 시 롤백 사용

BlueXP가 특정 작업의 일부로 Azure Private Link를 생성하지 못할 경우 Azure Private Link 연결이 없어도 작업이 완료됩니다. 이는 새 작업 환경(단일 노드 또는 HA 쌍)을 생성하거나 HA 쌍에서 다음 작업이 발생하는 경우, 즉 새 애그리게이트 생성, 기존 애그리게이트에 디스크 추가, 32TiB 이상으로 진행할 때 발생할 수 있습니다.

BlueXP에서 Azure Private Link를 생성하지 못할 경우 롤백을 활성화하여 이 기본 동작을 변경할 수 있습니다. 이를 통해 회사의 보안 규정을 완벽하게 준수할 수 있습니다.

롤백을 활성화하면 BlueXP는 작업을 중지하고 작업의 일부로 생성된 모든 리소스를 롤백합니다.

API를 통해 또는 app.conf 파일을 업데이트하여 롤백을 활성화할 수 있습니다.

- API를 통한 롤백 활성화 \*

#### 단계

1. 를 사용합니다 PUT /occm/config 다음 요청 본문이 있는 API 호출:

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

- app.conf \* 를 업데이트하여 롤백 기능을 활성화합니다

#### 단계

1. 커넥터 호스트에 SSH로 접속하고 로그인합니다.
2. /opt/application/netapp/cloudmanager/docker\_occm/data 디렉토리로 이동합니다
3. 다음 매개 변수와 값을 추가하여 app.conf를 편집합니다.

```
"rollback-on-private-link-failure": true
```

. 파일을 저장하고 Connector를 로그오프합니다.

재부팅할 필요는 없습니다.

리소스 그룹 이동 중

Cloud Volumes ONTAP는 Azure 리소스 그룹 이동을 지원하지만 워크플로는 Azure 콘솔에서만 실행됩니다.

동일한 Azure 가입 내에서 하나의 리소스 그룹에서 Azure의 다른 리소스 그룹으로 작업 환경을 이동할 수 있습니다. 서로 다른 Azure 구독 간에 리소스 그룹을 이동하는 것은 지원되지 않습니다.

단계

1. Canvas \* 에서 작업 환경을 제거합니다.

작업 환경을 제거하는 방법에 대한 자세한 내용은 을 참조하십시오 "[Cloud Volumes ONTAP 작업 환경 제거](#)".

2. Azure 콘솔에서 리소스 그룹 이동을 실행합니다.

이동을 완료하려면 을 참조하십시오 "[리소스를 새 리소스 그룹 또는 Microsoft Azure 설명서에 있는 구독으로 이동합니다](#)".

3. Canvas \* 에서 작업 환경을 검색합니다.
4. 작업 환경에 대한 정보에서 새 리소스 그룹을 찾습니다.

결과

작업 환경 및 해당 리소스(VM, 디스크, 스토리지 계정, 네트워크 인터페이스, 스냅샷)가 새 리소스 그룹에 있습니다.

## Google Cloud 관리

Cloud Volumes ONTAP의 Google Cloud 컴퓨터 유형을 변경합니다

Google Cloud에서 Cloud Volumes ONTAP를 시작할 때 여러 컴퓨터 유형 중에서 선택할 수 있습니다. 필요에 따라 크기가 작거나 너무 큰 것으로 판단될 경우 언제든지 인스턴스 또는 컴퓨터 유형을 변경할 수 있습니다.

이 작업에 대해

- Cloud Volumes ONTAP HA 쌍(기본 설정)에서 자동 반환이 활성화되어 있어야 합니다. 그렇지 않으면 작업이 실패합니다.

["ONTAP 9 설명서: 자동 반환 구성을 위한 명령입니다"](#)

- 컴퓨터 유형을 변경하면 Google Cloud 서비스 요금에 영향을 줄 수 있습니다.
- Cloud Volumes ONTAP가 다시 시작됩니다.

단일 노드 시스템의 경우 입출력이 중단됩니다.

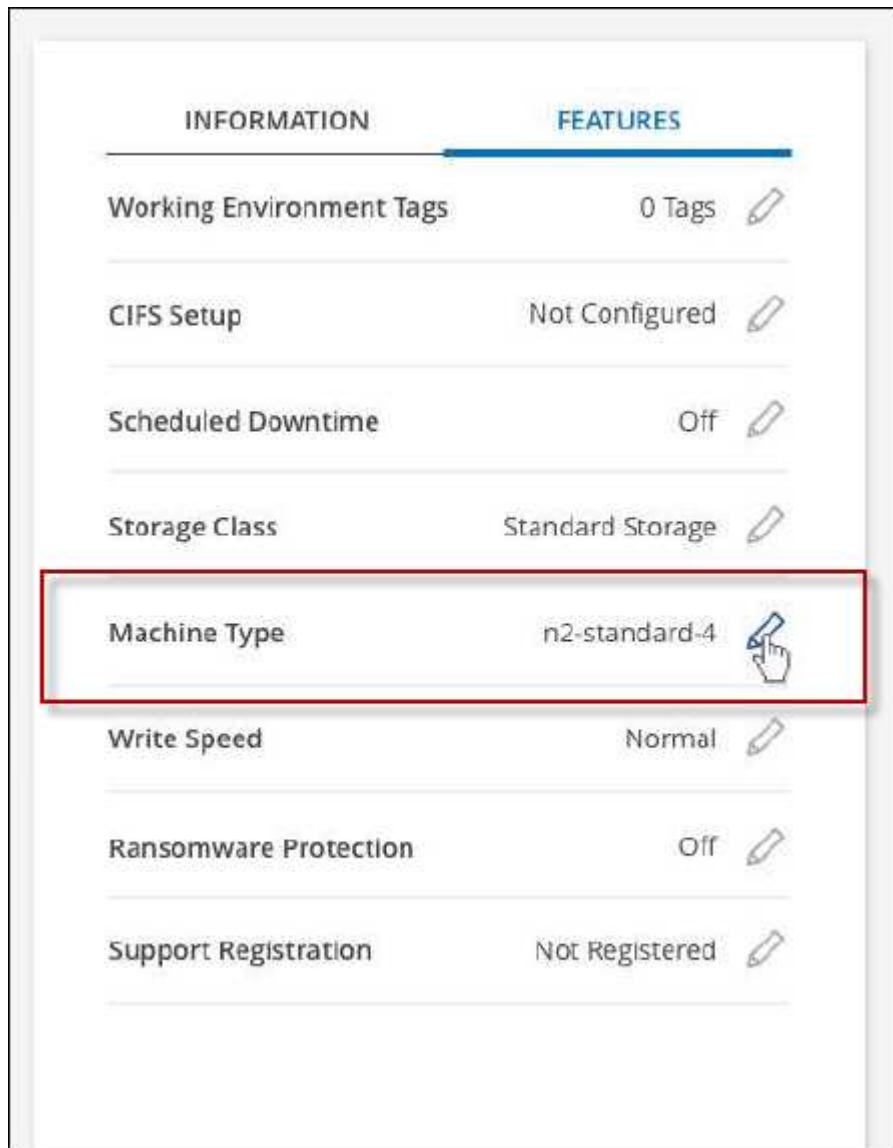
HA 쌍의 경우 변경은 무중단 것입니다. HA 쌍이 계속해서 데이터를 제공합니다.



BlueXP는 테이크오버를 시작하고 Giveback을 기다리면서 한 번에 하나의 노드를 정상적으로 변경합니다. NetApp의 QA 팀은 이 프로세스 중에 파일 쓰기와 읽기를 모두 테스트했지만 클라이언트 측에서는 문제가 발생하지 않았습니다. 접속이 변경됨에 따라 입출력 레벨에서 재시도 횟수가 확인되었지만 애플리케이션 계층은 NFS/CIFS 연결의 이러한 짧은 "재연결"을 극복했습니다.

단계

1. Canvas 페이지에서 작업 환경을 선택합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 기계 유형 \* 옆에 있는 연필 아이콘을 클릭합니다.



- a. 노드 기반 PAYGO 라이선스를 사용하는 경우 \* 라이선스 유형 \* 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스 및 컴퓨터 유형을 선택할 수 있습니다.
3. 시스템 유형을 선택하고 확인란을 선택하여 변경의 영향을 이해했는지 확인한 다음 \* 변경 \* 을 클릭합니다.

결과

Cloud Volumes ONTAP가 새 구성으로 재부팅됩니다.

## 고급 보기를 사용하여 **Cloud Volumes ONTAP**를 관리합니다

Cloud Volumes ONTAP의 고급 관리를 수행해야 하는 경우, ONTAP 시스템과 함께 제공되는 관리 인터페이스인 ONTAP System Manager를 사용하면 됩니다. BlueXP에 System Manager 인터페이스를 직접 포함하므로 고급 관리를 위해 BlueXP를 떠날 필요가 없습니다.

이 고급 보기는 미리 보기로 사용할 수 있습니다. NetApp은 이 경험을 개선하고 다음 릴리즈에서 향상된 기능을 추가할 계획입니다. 제품 내 채팅을 사용하여 피드백을 보내주십시오.

### 피처

BlueXP의 고급 보기를 통해 다음과 같은 추가 관리 기능을 사용할 수 있습니다.

- 고급 스토리지 관리  
일관성 그룹, 공유, Qtree, 할당량 및 스토리지 VM을 관리합니다.
- 네트워킹 관리  
IPspace, 네트워크 인터페이스, 포트 세트 및 이더넷 포트 관리
- 이벤트 및 작업  
이벤트 로그, 시스템 경고, 작업 및 감사 로그를 봅니다.
- 고급 데이터 보호  
스토리지 VM, LUN 및 일관성 그룹을 보호합니다.
- 호스트 관리  
SAN 이니시에이터 그룹 및 NFS 클라이언트를 설정합니다.

### 지원되는 구성

System Manager를 통한 고급 관리는 표준 클라우드 지역에서 Cloud Volumes ONTAP 9.10.0 이상에서 지원됩니다.

GovCloud 지역 또는 아웃바운드 인터넷 액세스가 없는 지역에서는 System Manager 통합이 지원되지 않습니다.

### 제한 사항

Cloud Volumes ONTAP에서는 System Manager 인터페이스에 표시되는 몇 가지 기능을 지원하지 않습니다.

- BlueXP 계층화  
Cloud Volumes ONTAP에서는 BlueXP 계층화 서비스가 지원되지 않습니다. 볼륨 생성 시 BlueXP의 표준 보기에서 데이터를 오브젝트 스토리지로 계층화하도록 직접 설정해야 합니다.
- 계층

System Manager에서는 애그리게이트 관리(로컬 계층 및 클라우드 계층 포함)가 지원되지 않습니다. BlueXP의 표준 보기에서 직접 애그리게이트를 관리해야 합니다.

- 펌웨어 업그레이드

Cloud Volumes ONTAP에서는 \* 클러스터 > 설정 \* 페이지의 자동 펌웨어 업데이트가 지원되지 않습니다.

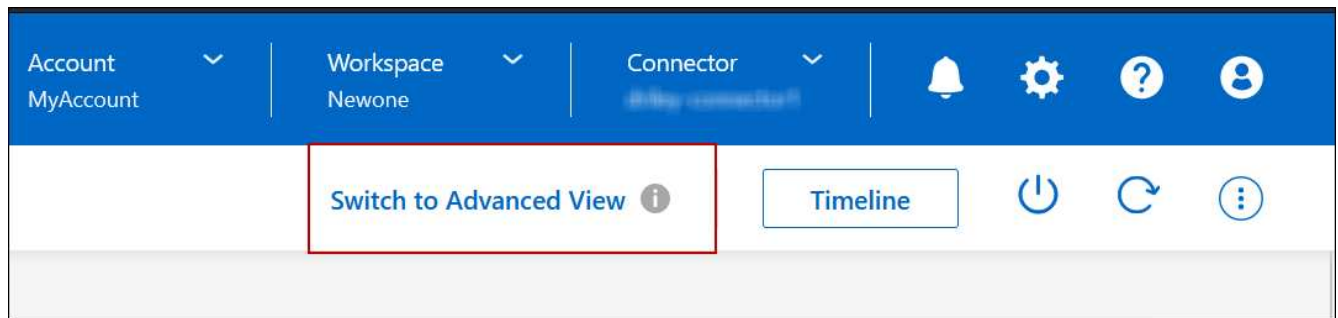
또한 System Manager의 역할 기반 액세스 제어가 지원되지 않습니다.

시작하는 방법

Cloud Volumes ONTAP 작업 환경을 열고 고급 보기 옵션을 클릭합니다.

단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
3. 오른쪽 상단에서 \* 고급 보기로 전환 \* 을 클릭합니다.



4. 확인 메시지가 나타나면 메시지를 읽고 \* 닫기 \* 를 클릭합니다.
5. 시스템 관리자를 사용하여 Cloud Volumes ONTAP를 관리합니다.
6. 필요한 경우 \* 표준 보기로 전환 \* 을 클릭하여 BlueXP를 통한 표준 관리로 돌아갑니다.

### System Manager 사용에 대한 도움말

Cloud Volumes ONTAP에서 System Manager를 사용하는 데 도움이 필요한 경우 을 참조하십시오 ["ONTAP 설명서"](#) 을 참조하십시오. 다음은 도움이 될 수 있는 몇 가지 링크입니다.

- ["볼륨 및 LUN 관리"](#)
- ["네트워크 관리"](#)
- ["데이터 보호"](#)

### CLI에서 Cloud Volumes ONTAP를 관리합니다

Cloud Volumes ONTAP CLI를 사용하면 모든 관리 명령을 실행할 수 있으며 고급 작업에 이상적이고 CLI를 사용하는 것이 더 편할 경우 적합합니다. SSH(Secure Shell)를 사용하여 CLI에 연결할 수 있습니다.



## 시작하기 전에

Cloud Volumes ONTAP에 연결하기 위해 SSH를 사용하는 호스트에는 Cloud Volumes ONTAP에 대한 네트워크 연결이 있어야 합니다. 예를 들어, 클라우드 공급자 네트워크에 있는 점프 호스트에서 SSH를 사용해야 할 수 있습니다.



여러 AZs에 구축된 Cloud Volumes ONTAP HA 구성에서는 클러스터 관리 인터페이스에 부동 IP 주소를 사용합니다. 즉, 외부 라우팅을 사용할 수 없습니다. 동일한 라우팅 도메인의 일부인 호스트에서 접속해야 합니다.

## 단계

1. BlueXP에서 클러스터 관리 인터페이스의 IP 주소를 확인합니다.
  - a. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
  - b. Canvas 페이지에서 Cloud Volumes ONTAP 시스템을 선택합니다.
  - c. 오른쪽 창에 표시되는 클러스터 관리 IP 주소를 복사합니다.
2. SSH를 사용하여 admin 계정을 사용하여 클러스터 관리 인터페이스 IP 주소에 연결합니다.

◦ 예 \*

다음 이미지는 PuTTY를 사용하는 예를 보여 줍니다.



3. 로그인 프롬프트에서 admin 계정의 암호를 입력합니다.

◦ 예 \*

```
Password: *****  
COT2::>
```

## 시스템 상태 및 이벤트입니다

### AutoSupport 설정을 확인합니다

AutoSupport은 능동적으로 시스템 상태를 모니터링하고 NetApp 기술 지원 팀에 메시지를 보냅니다. 기본적으로 AutoSupport는 각 노드에서 HTTPS 전송 프로토콜을 사용하여 기술 지원 부서에 메시지를 보내도록 설정됩니다. AutoSupport에서 이러한 메시지를 보낼 수 있는지 확인하는 것이 가장 좋습니다.

필요한 유일한 구성 단계는 Cloud Volumes ONTAP가 아웃바운드 인터넷 연결을 사용할 수 있도록 하는 것입니다. 자세한 내용은 해당 클라우드 공급자의 네트워킹 요구 사항을 참조하십시오.

## AutoSupport 요구 사항

Cloud Volumes ONTAP 노드를 사용하려면 NetApp AutoSupport에 대한 아웃바운드 인터넷 액세스가 필요합니다. 사전 예방적으로 시스템의 상태를 모니터링하고 메시지를 NetApp 기술 지원으로 보냅니다.

라우팅 및 방화벽 정책은 Cloud Volumes ONTAP가 AutoSupport 메시지를 보낼 수 있도록 다음 엔드포인트에 대한 HTTP/HTTPS 트래픽을 허용해야 합니다.

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

AutoSupport 메시지를 보내는 데 아웃바운드 인터넷 연결을 사용할 수 없는 경우 BlueXP는 자동으로 Cloud Volumes ONTAP 시스템에서 커넥터를 프록시 서버로 사용하도록 구성합니다. 유일한 요구 사항은 커넥터의 보안 그룹이 포트 3128을 통한 `_IN`인바운드\_연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

Cloud Volumes ONTAP에 대해 엄격한 아웃바운드 규칙을 정의한 경우 Cloud Volumes ONTAP 보안 그룹이 포트 3128을 통한 `_outbound_connection`을 허용하는지 확인해야 합니다.

아웃바운드 인터넷 액세스가 가능한지 확인한 후 AutoSupport를 테스트하여 메시지를 보낼 수 있는지 확인할 수 있습니다. 자세한 지침은 을 참조하십시오 ["ONTAP 문서: AutoSupport 설정"](#).

## AutoSupport 구성 문제를 해결합니다

아웃바운드 연결을 사용할 수 없고 BlueXP에서 커넥터를 프록시 서버로 사용하도록 Cloud Volumes ONTAP 시스템을 구성할 수 없는 경우 "<작업 환경 이름>이(가) AutoSupport 메시지를 보낼 수 없습니다."라는 제목의 BlueXP에서 알림을 받게 됩니다.

네트워킹 문제로 인해 이 메시지가 표시될 가능성이 높습니다.

이 문제를 해결하려면 다음 단계를 수행하십시오.

단계

1. Cloud Volumes ONTAP 시스템에 SSH를 사용하여 CLI에서 시스템을 관리할 수 있습니다.

["Cloud Volumes ONTAP에 SSH를 사용하는 방법에 대해 알아보십시오"](#).

2. AutoSupport 하위 시스템의 세부 상태를 표시합니다.

```
autosupport check show-details
```

응답은 다음과 비슷해야 합니다.

```

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 범주의 상태가 "ok"이면 AutoSupport가 올바르게 구성되어 메시지를 보낼 수 있음을 의미합니다.

3. 상태가 정상이 아닌 경우 각 Cloud Volumes ONTAP 노드의 프록시 URL을 확인합니다.

```
autosupport show -fields proxy-url
```

4. 프록시 URL 매개 변수가 비어 있는 경우 Cloud Volumes ONTAP에서 커넥터를 프록시로 사용하도록 구성합니다.

```
autosupport modify -proxy-url http://<connector private ip>:3128
```

5. AutoSupport 상태 다시 확인:

```
autosupport check show-details
```

6. 상태가 여전히 FAILED인 경우 Cloud Volumes ONTAP와 포트 3128을 통한 커넥터 사이에 연결이 있는지

확인합니다.

7. 연결이 있는지 확인한 후에도 상태 ID가 계속 실패하면 커넥터에 SSH를 연결합니다.

"Connector용 Linux VM에 연결하는 방법에 대해 자세히 알아보십시오"

8. 로 이동합니다 /opt/application/netapp/cloudmanager/docker\_occm/data/
9. 프록시 구성 파일을 엽니다 squid.conf

파일의 기본 구조는 다음과 같습니다.

```
http_port 3128
acl localnet src 172.31.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

localnet src 값은 Cloud Volumes ONTAP 시스템의 CIDR입니다.

10. Cloud Volumes ONTAP 시스템의 CIDR 블록이 파일에 지정된 범위에 있지 않으면 다음과 같이 값을 업데이트하거나 새 항목을 추가합니다.

```
acl cvonet src <cidr>
```

이 새 항목을 추가하는 경우 허용 항목도 추가해야 합니다.

```
http_access allow cvonet
```

예를 들면 다음과 같습니다.

```
http_port 3128
acl localnet src 172.31.0.0/16
acl cvonet src 172.33.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access allow cvonet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

11. 구성 파일을 편집한 후 프록시 컨테이너를 sudo로 다시 시작합니다.

```
docker restart squid
```

12. Cloud Volumes ONTAP CLI로 돌아가서 Cloud Volumes ONTAP가 AutoSupport 메시지를 보낼 수 있는지 확인합니다.

```
autosupport check show-details
```

## EMS를 설정한다

EMS(이벤트 관리 시스템)는 ONTAP 시스템에서 발생하는 이벤트에 대한 정보를 수집하여 표시합니다. 이벤트 알림을 수신하려면 이벤트 대상(이메일 주소, SNMP 트랩 호스트 또는 syslog 서버)과 이벤트 경로를 특정 이벤트 심각도에 대해 설정할 수 있습니다.

CLI를 이용하여 EMS를 구성할 수 있다. 자세한 지침은 을 참조하십시오 "[ONTAP 문서: EMS 구성 개요](#)".

## 저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 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.