시스템 관리

Cloud Volumes ONTAP

NetApp
March 28, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/bluexp-cloud-volumes-ontap/task-updating-ontap-cloud.html on March 28, 2024. Always check docs.netapp.com for the latest.

목차

시스템 관리 . . . 1
Cloud Volumes ONTAP 소프트웨어를 업그레이드합니다 . . . 1
선불 종량제 시스템을 등록하는 중입니다 . . . 9
Cloud Volumes ONTAP의 상태 관리 . . . 11
NTP를 사용하여 시스템 시간을 동기화합니다 . . . 14
시스템 쓰기 속도를 수정합니다 . . . 14
Cloud Volumes ONTAP의 암호를 변경합니다 . . . 16
시스템을 추가, 제거 또는 삭제합니다 . . . 16
설치하고 . . . 20
Azure 관리 . . . 24
Google Cloud 관리 . . . 36
고급 보기를 사용하여 Cloud Volumes ONTAP를 관리합니다 . . . 37
CLI에서 Cloud Volumes ONTAP를 관리합니다 . . . 39

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
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0

현재 버전	로 직접 업그레이드할 수 있는 버전입니다
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

다음 사항에 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 릴리즈로 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 릴리스

2024년 1월부터 패치 업그레이드는 Cloud Volumes ONTAP의 3가지 최신 버전에 대한 패치 릴리즈인 경우에만 BlueXP에서 사용할 수 있습니다. 최신 GA 릴리즈를 사용하여 BlueXP에 표시할 3가지 최신 버전을 결정합니다. 예를 들어, 현재 GA 릴리즈가 9.13.1인 경우 9.11.1~9.13.1용 패치가 BlueXP에 표시됩니다. 버전 9.11.1 이하의 패치 릴리스로 업그레이드하려면 에서 수동 업그레이드 절차를 사용해야 합니다 ONTAP 이미지를 다운로드하는 중입니다.

패치(P) 릴리스의 일반적인 규칙으로, 하나의 버전 릴리스에서 실행 중인 현재 버전 또는 다음 버전의 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.

C4, M4 및 **R4 EC2** 인스턴스 유형으로 **AWS**에서 업그레이드

Cloud Volumes ONTAP은 더 이상 C4, M4 및 R4 EC2 인스턴스 유형을 지원하지 않습니다. 이러한 인스턴스 유형을 사용하여 기존 배포를 Cloud Volumes ONTAP 버전 9.8-9.12.1로 업그레이드할 수 있습니다. 업그레이드하기 전에 다음을 수행하는 것이 좋습니다 인스턴스 유형을 변경합니다. 인스턴스 유형을 변경할 수 없는 경우 을 변경해야 합니다 향상된 네트워킹을 활성화합니다 업그레이드 전. 인스턴스 유형 변경 및 향상된 네트워킹 활성화에 대한 자세한 내용은 다음 섹션을 참조하십시오.

9.13.0 이상을 실행하는 Cloud Volumes ONTAP에서는 C4, M4 및 R4 EC2 인스턴스 유형으로 업그레이드할 수 없습니다. 이 경우 디스크 수를 줄인 다음 인스턴스 유형을 변경합니다 또는 C5, M5, R5 EC2 인스턴스 유형으로 새로운 HA 쌍 구성을 배포하고 데이터를 마이그레이션합니다.

인스턴스 유형을 변경합니다

C4, M4 및 R4 EC2 인스턴스 유형을 사용하면 C5, M5 및 R5 EC2 인스턴스 유형보다 노드당 더 많은 디스크를 지원할 수 있습니다. 실행 중인 C4, M4 또는 R4 EC2 인스턴스의 노드당 디스크 수가 C5, M5 및 R5 인스턴스에 대한 노드당 최대 디스크 허용치보다 작은 경우 EC2 인스턴스 유형을 C5, M5 또는 R5로 변경할 수 있습니다.

"EC2 인스턴스별로 디스크 및 계층화 제한을 확인합니다"
"Cloud Volumes ONTAP의 EC2 인스턴스 유형을 변경합니다"

인스턴스 유형을 변경할 수 없는 경우 의 단계를 따릅니다 향상된 네트워킹을 활성화합니다.

향상된 네트워킹을 활성화합니다

Cloud Volumes ONTAP 9.8 이상 버전으로 업그레이드하려면 C4, M4 또는 R4 인스턴스 유형을 실행하는 클러스터에서 enable_enhanced networking_을 사용해야 합니다. ENA를 활성화하려면 기술 문서 를 참조하십시오 "AWS Cloud Volumes ONTAP 인스턴스에서 SR-IOV 또는 ENA와 같은 향상된 네트워킹을 활성화하는 방법".

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
- 모든 LIF가 홈 포트에 있는지 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

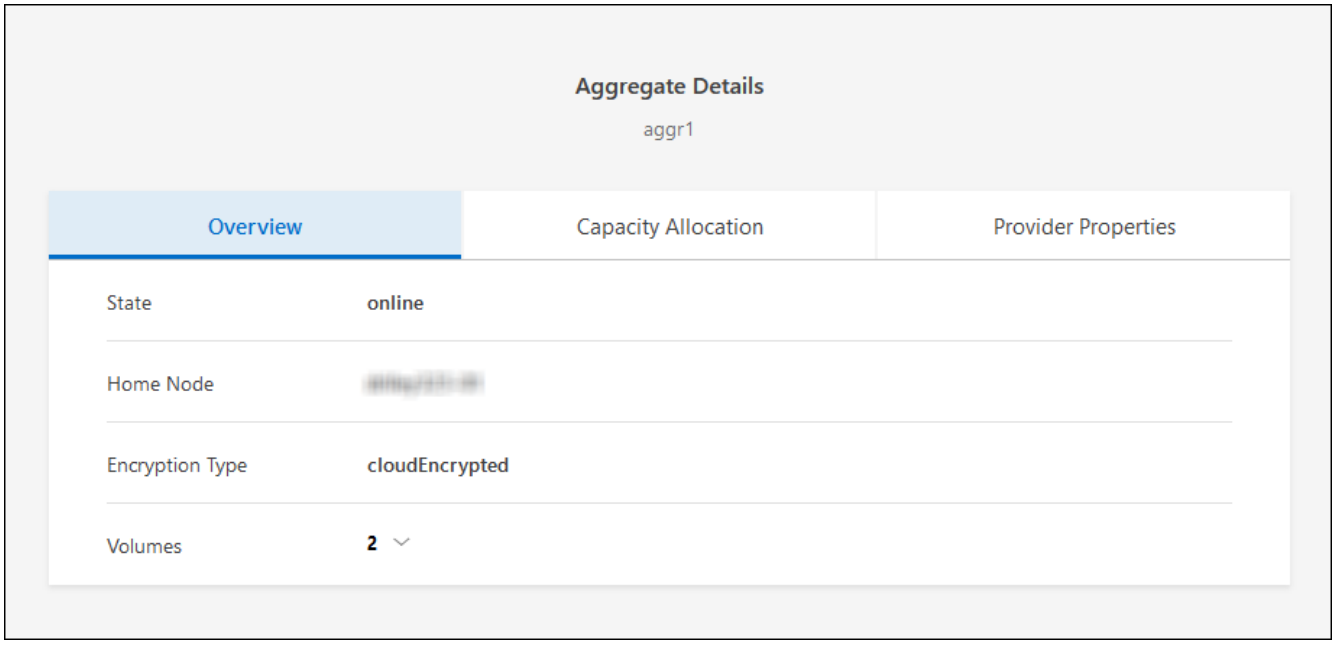
소프트웨어를 업데이트하기 전에 Cloud Volumes ONTAP용 애그리게이트가 온라인 상태여야 합니다. 애그리게이트는 대부분의 구성에서 온라인 상태여야 하지만, 그렇지 않을 경우 온라인 상태로 전환할 수 있습니다.

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.



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.

모든 **LIF**가 홈 포트에 있는지 확인합니다

업그레이드하기 전에 모든 LIF가 홈 포트에 있어야 합니다. ONTAP 설명서를 참조하십시오 "모든 LIF가 홈 포트에 있는지 확인합니다".

업그레이드 실패 오류가 발생하면 를 참조하십시오 "기술 문서 "Cloud Volumes ONTAP 업그레이드 실패"".

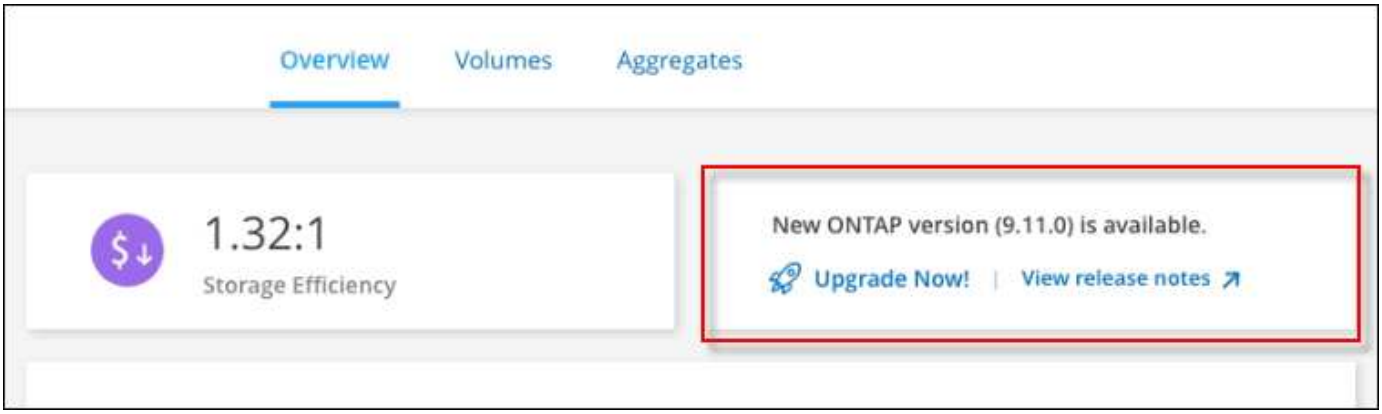
Cloud Volumes ONTAP를 업그레이드합니다

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.

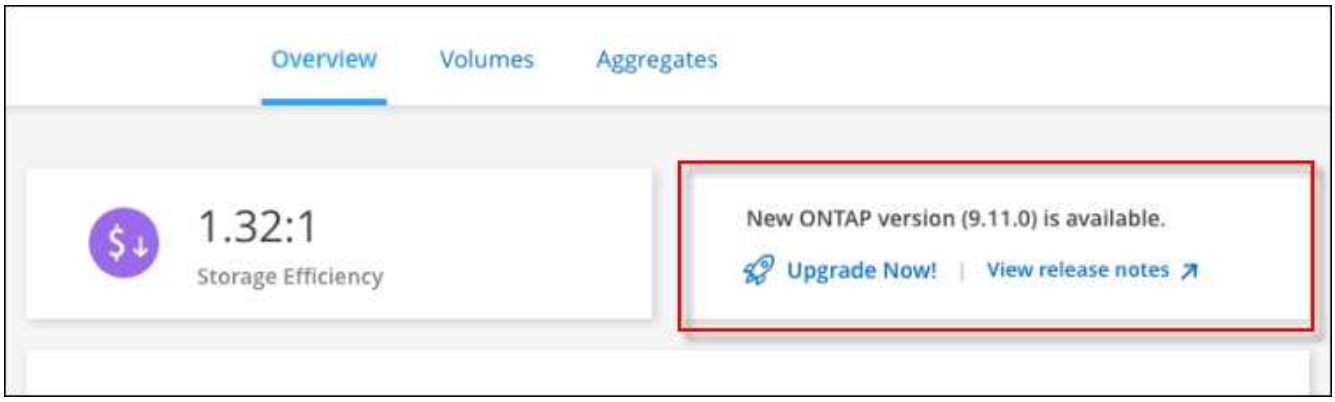
시작하기 전에

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.

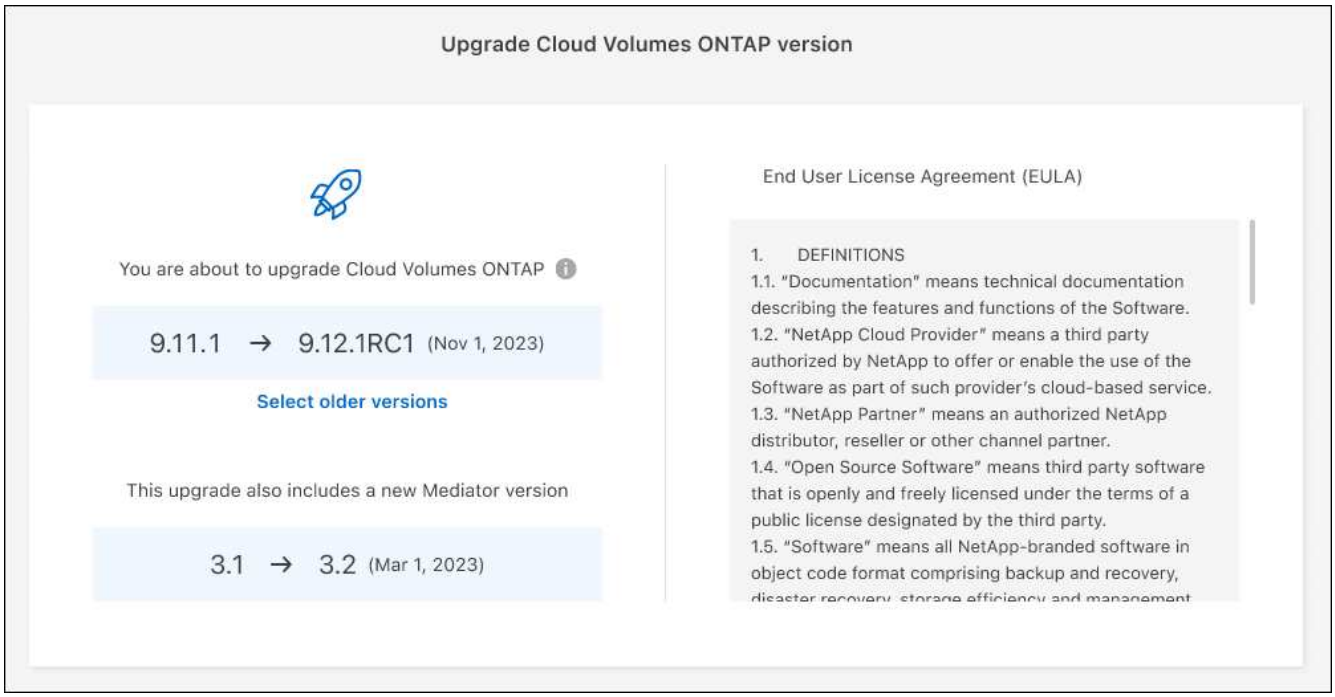


3. 새 버전을 사용할 수 있는 경우 * 지금 업그레이드! * 를 클릭합니다

   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/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.

   <a href="http://<Connector-private-IP-address>/ontap/images/<image-file-name&gt" class="bare">http://<Connector-private-IP-address>/ontap/images/<image-file-name&gt; 으로 문의하십시오

   > 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".

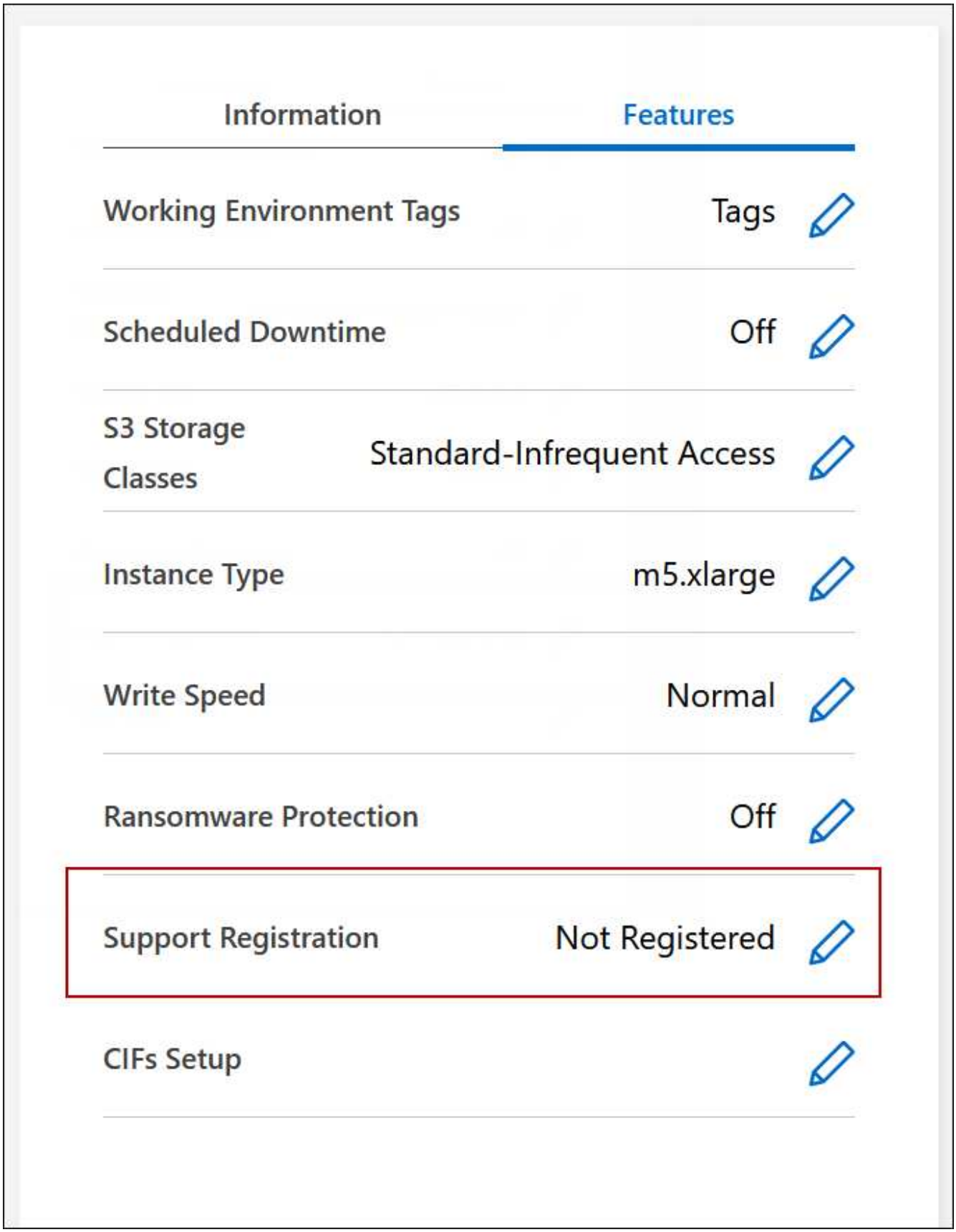
> 지원이 등록되지 않은 시스템은 새 버전이 출시되어도 BlueXP에 나타나는 소프트웨어 업데이트 알림을 계속 받게 됩니다. 그러나 소프트웨어를 업그레이드하기 전에 시스템을 등록해야 합니다.

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.



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.

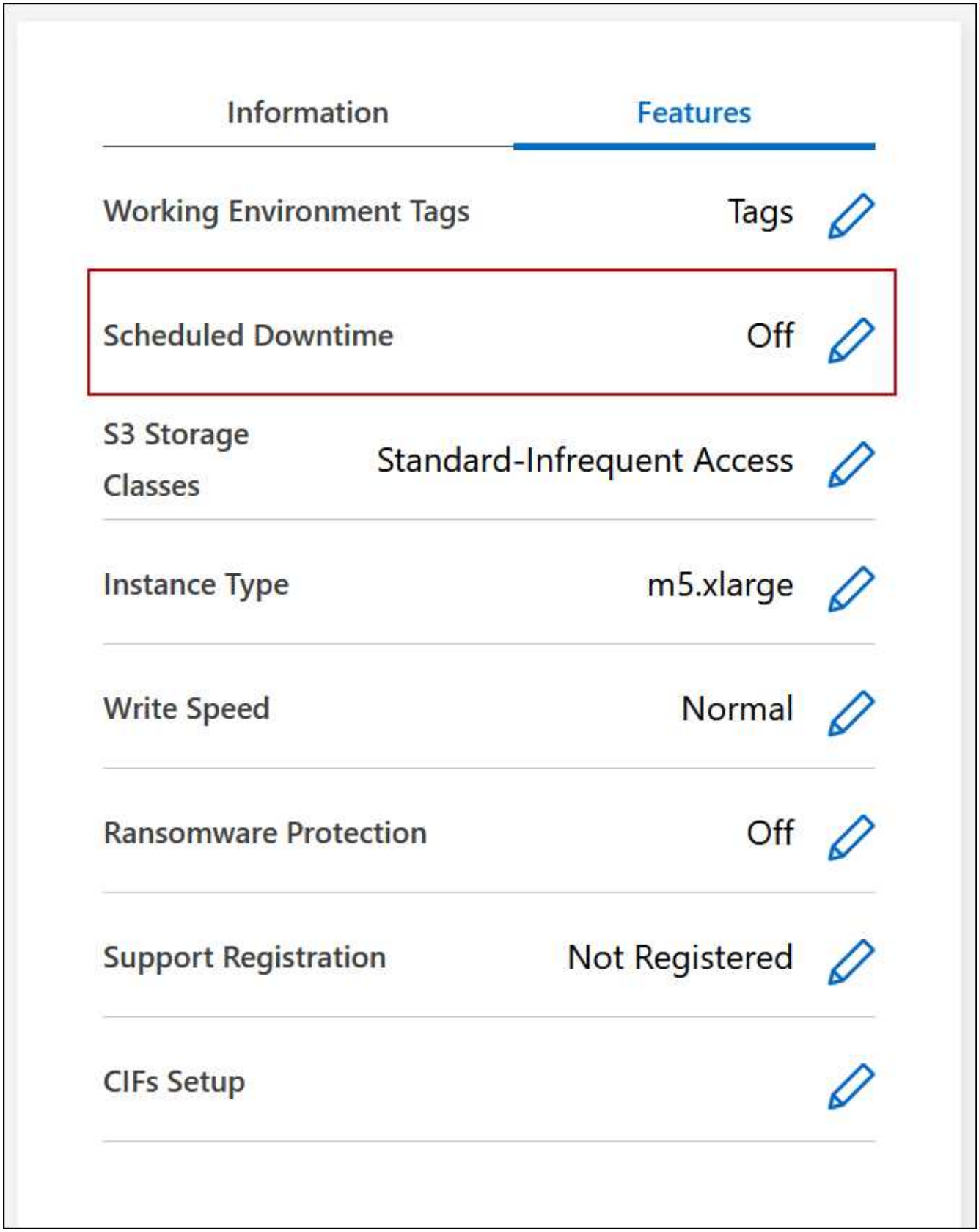
  전송이 완료된 후 BlueXP가 시스템을 종료합니다.

- 이 작업은 HA 2노드에서 두 노드의 자동 종료를 예약합니다.
- 예약된 종료를 통해 Cloud Volumes ONTAP를 끌 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.



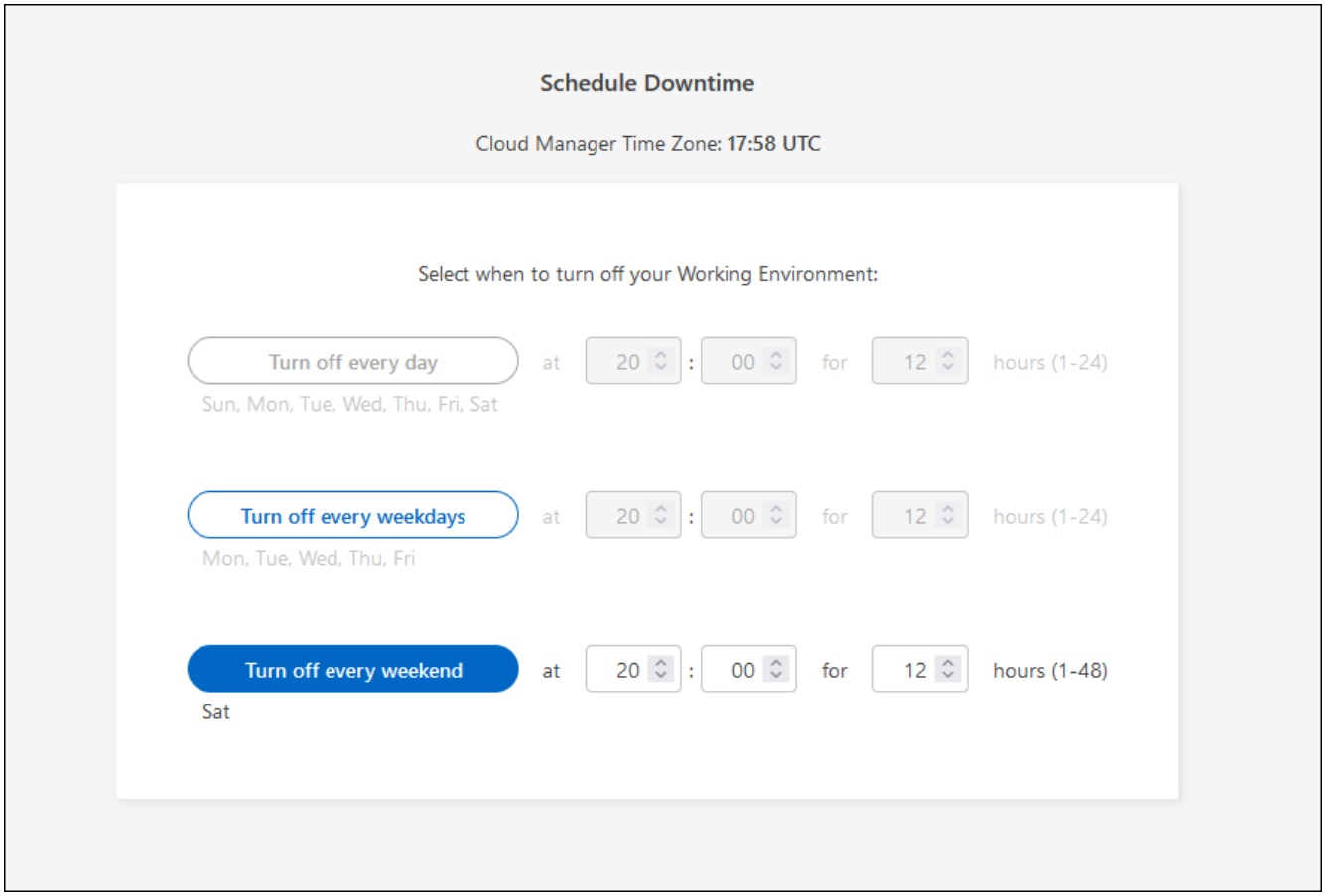
3. 종료 일정을 지정합니다.

   a. 매일, 매주 평일, 매주 또는 세 가지 옵션의 조합을 종료할지 여부를 선택합니다.

   b. 시스템 전원을 끌 시기 및 시스템 전원을 끌 시간을 지정합니다.

- 예 *

다음 이미지는 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 ONTAP를 중지하는 중입니다

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

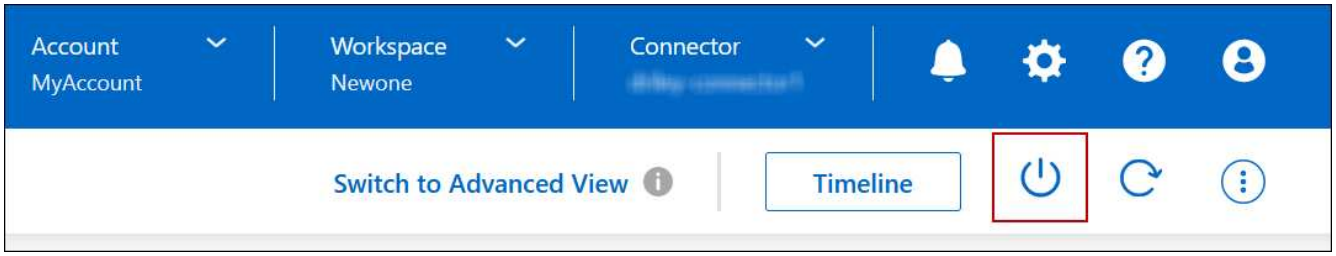
> 비용을 줄이기 위해 BlueXP는 루트 및 부팅 디스크의 이전 스냅샷을 주기적으로 삭제합니다. 루트와 부팅 디스크 모두에 대해 가장 최근의 두 스냅샷만 보존됩니다.

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"

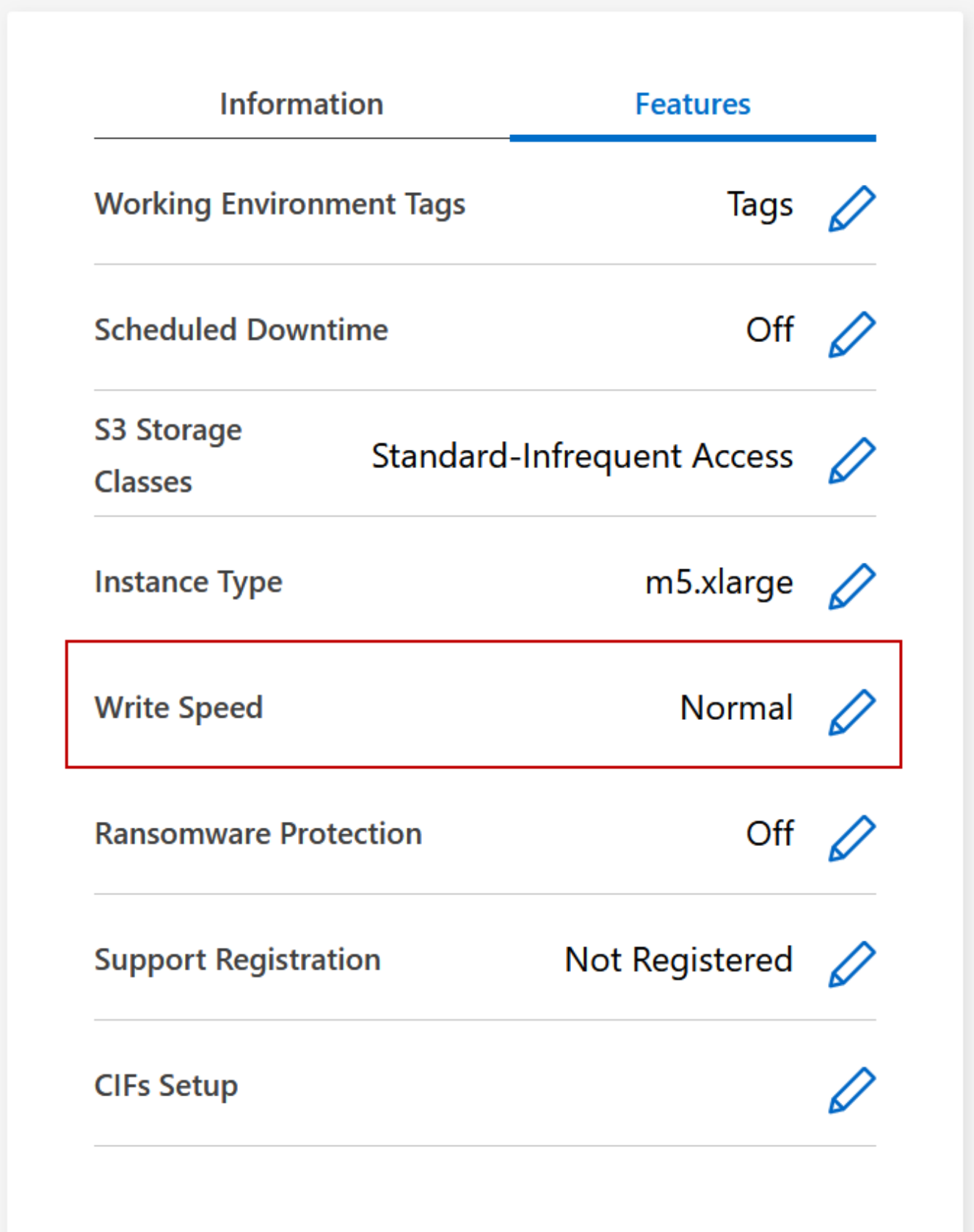
쓰기 속도를 변경하려면 먼저 해야 합니다 "정상 설정과 높음 설정의 차이를 이해합니다".

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.



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.

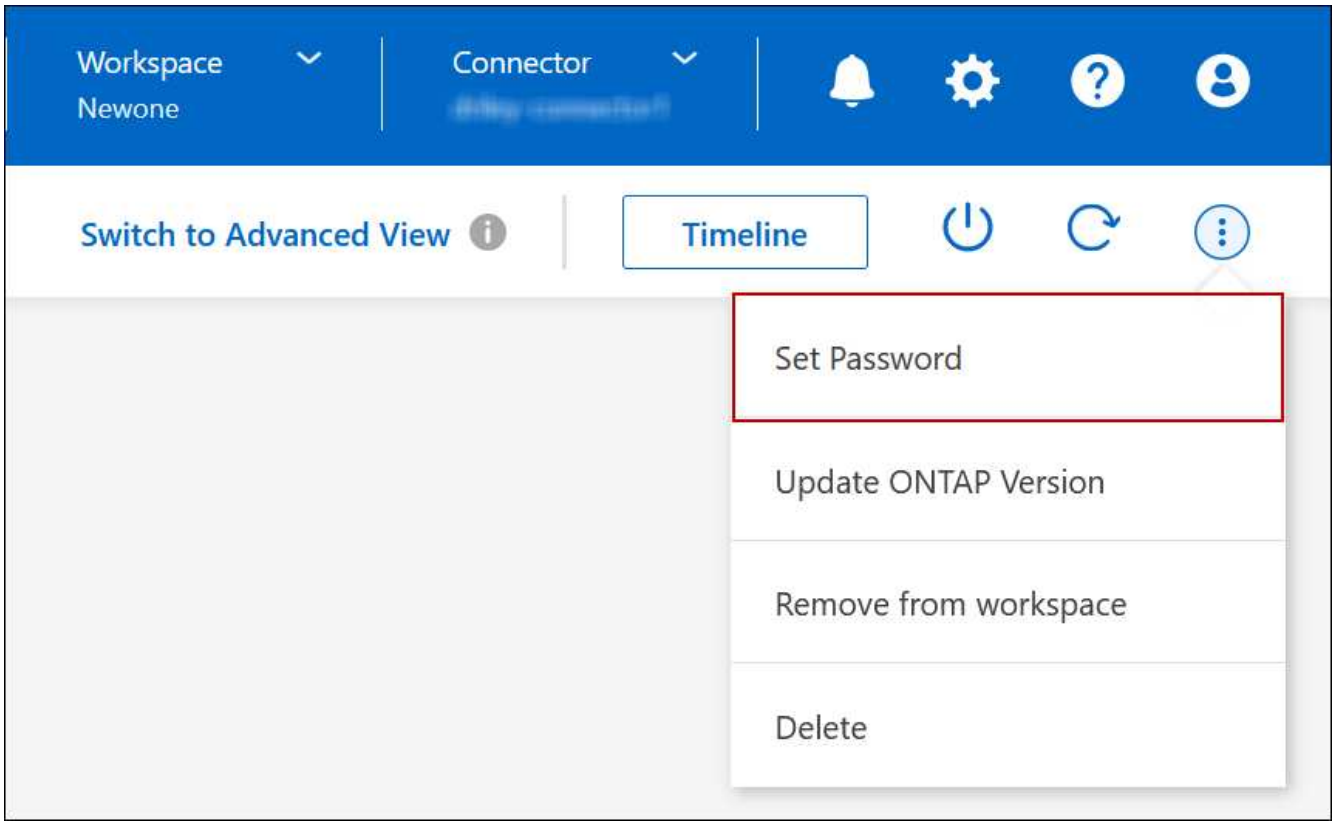
Cloud Volumes ONTAP의 암호를 변경합니다

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.

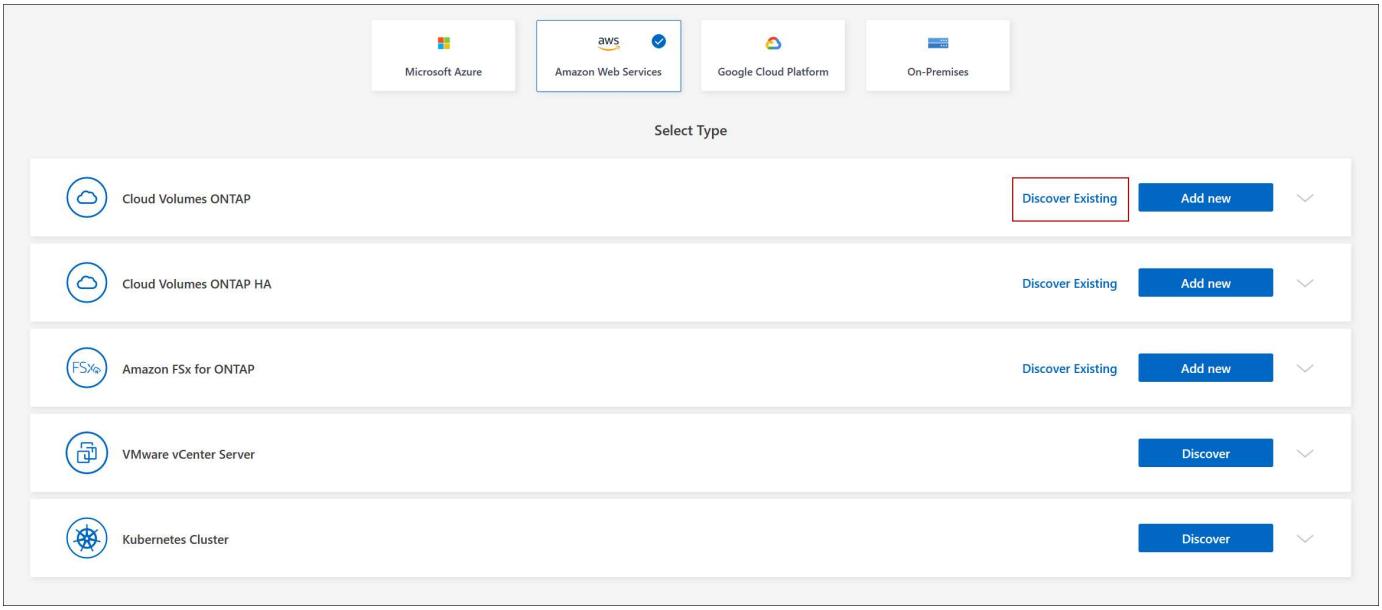
시작하기 전에

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

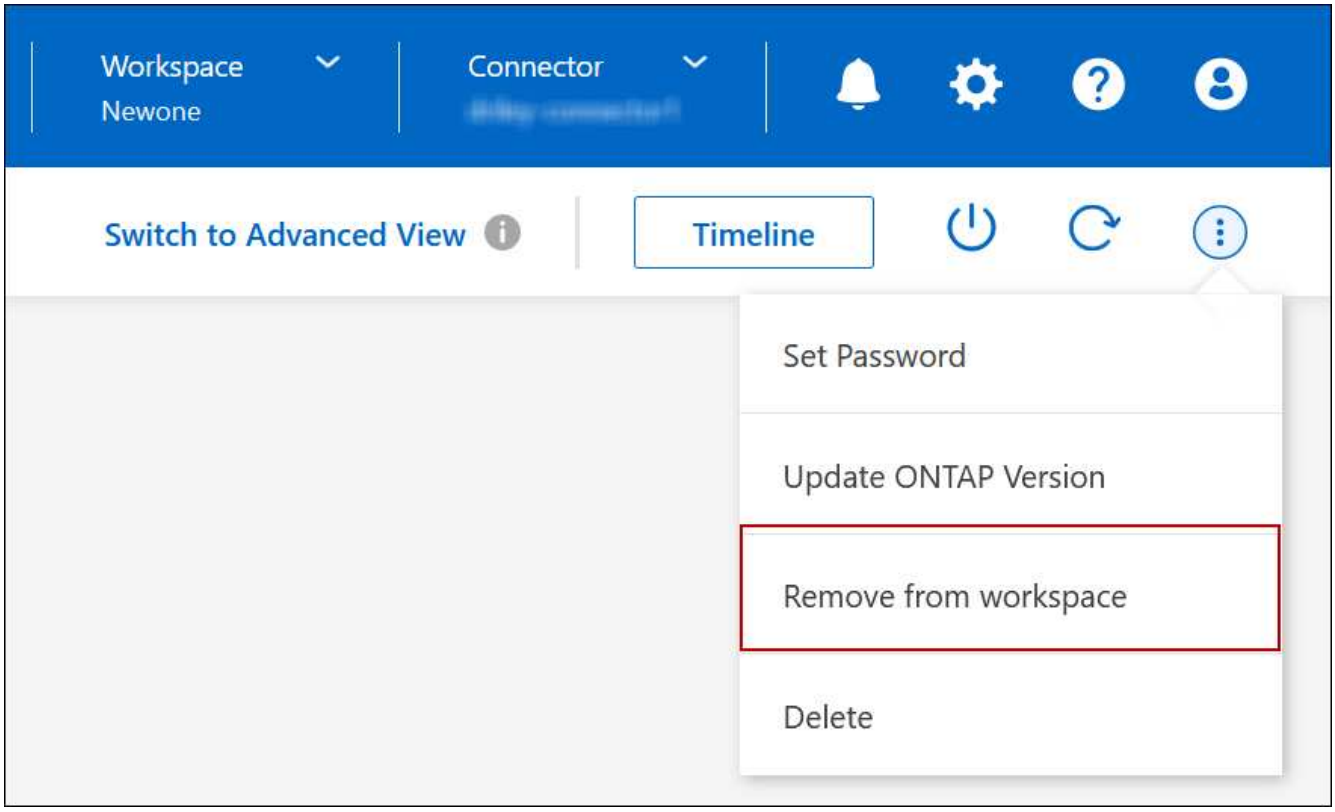
Cloud Volumes ONTAP 작업 환경을 제거하면 BlueXP에서 제거됩니다. Cloud Volumes ONTAP 시스템은 삭제되지 않습니다. 나중에 작업 환경을 다시 검색할 수 있습니다.

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 라이센스가 부여된 Cloud Volumes ONTAP 인스턴스를 종료하는 경우 다른 인스턴스에 대해 라이센스 키를 사용할 수 없습니다. 라이센스를 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.

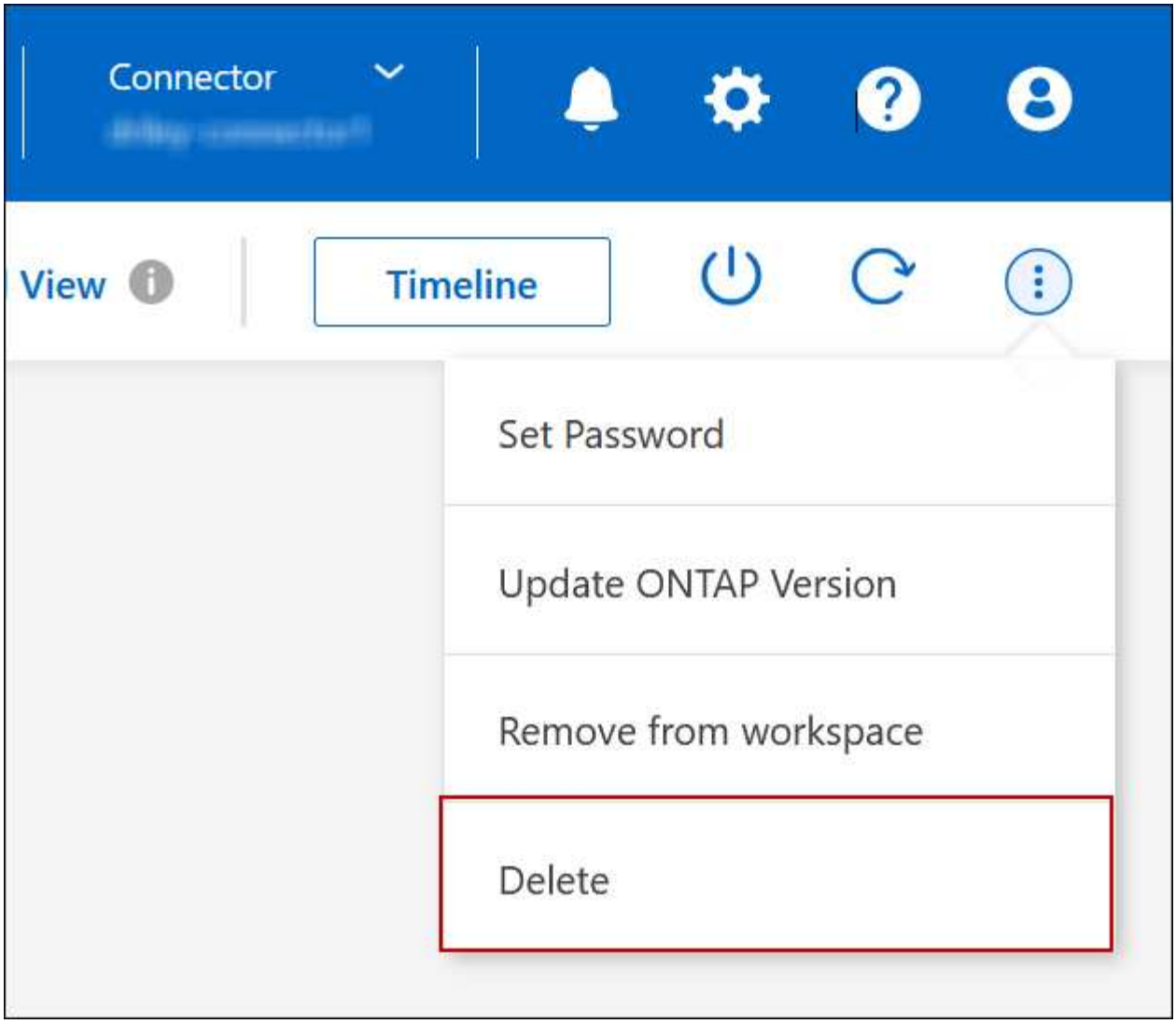
2. 이 작업 환경에서 BlueXP 분류를 사용하도록 설정했고 다른 작업 환경에서 이 서비스를 사용하지 않는 경우 서비스 인스턴스를 삭제해야 합니다.

   "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 ONTAP의 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.

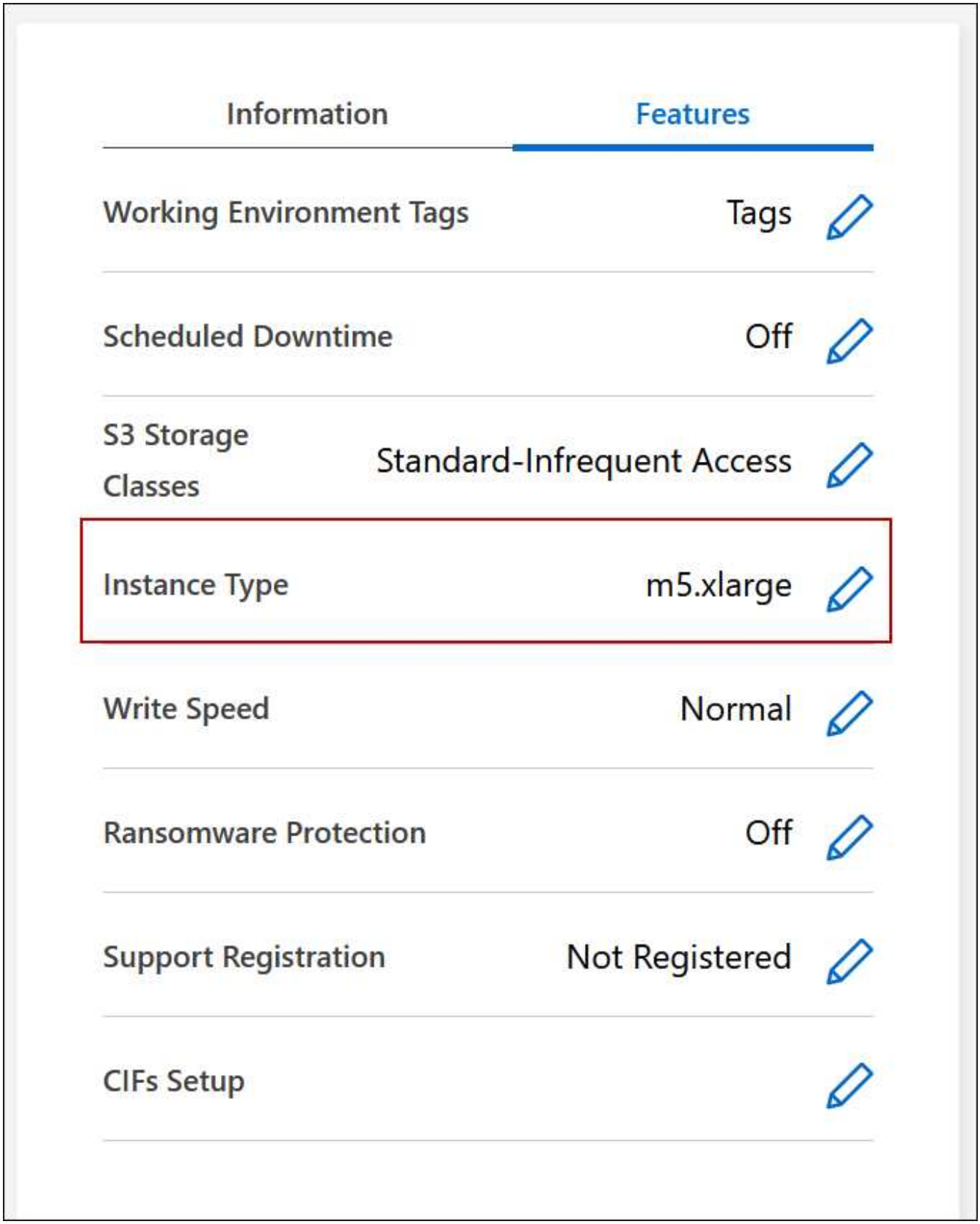
참조하십시오

AWS에서 지원되는 인스턴스 유형 목록은 를 참조하십시오 "지원되는 EC2 인스턴스".

C4, M4 또는 R4 인스턴스에서 인스턴스 유형을 변경할 수 없는 경우 KB 문서를 참조하십시오 "디스크 수 오류로 인해 인스턴스 유형을 R4에서 R5로 변경할 수 없습니다".

단계

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



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

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

결과

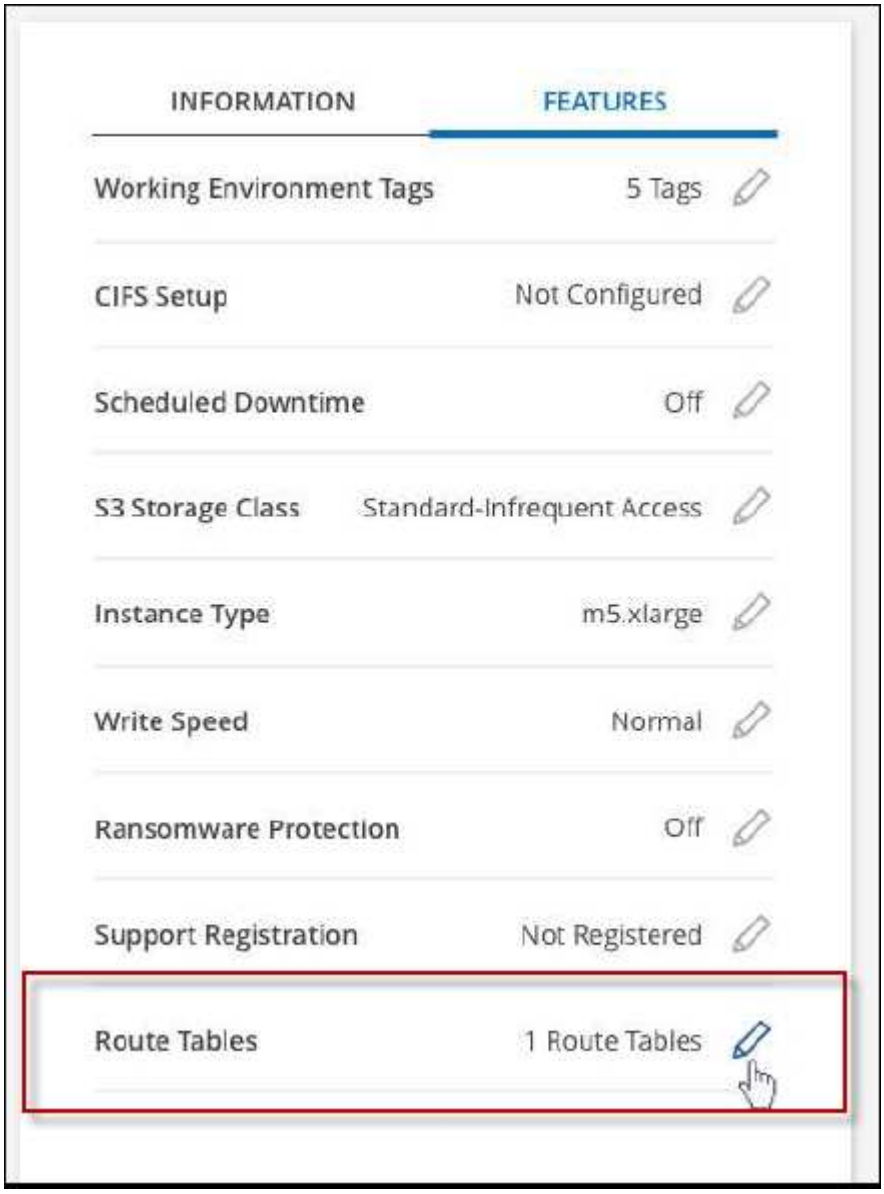
Cloud Volumes ONTAP가 새 구성으로 재부팅됩니다.

여러 **AZs**에서 **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.

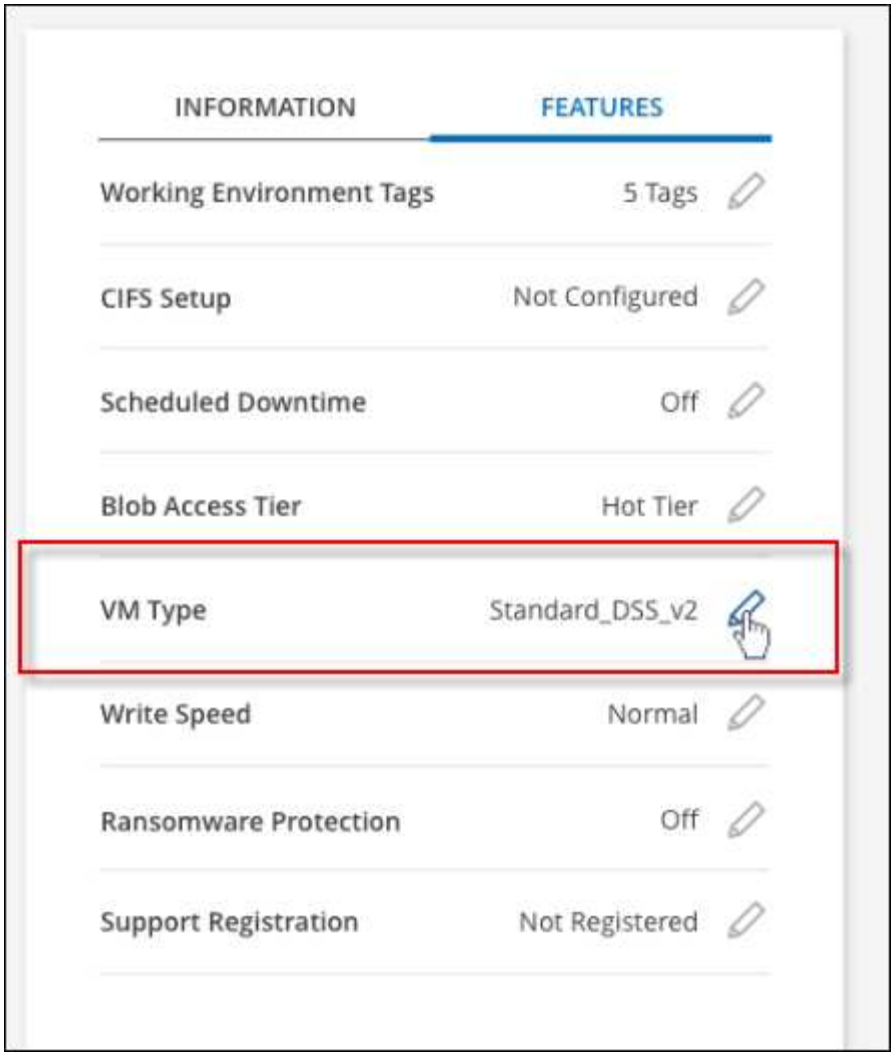
  단일 노드 시스템의 경우 입출력이 중단됩니다.

  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 라이센스를 사용하는 경우 * 라이센스 유형 * 옆에 있는 연필 아이콘을 클릭하여 다른 라이센스 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.

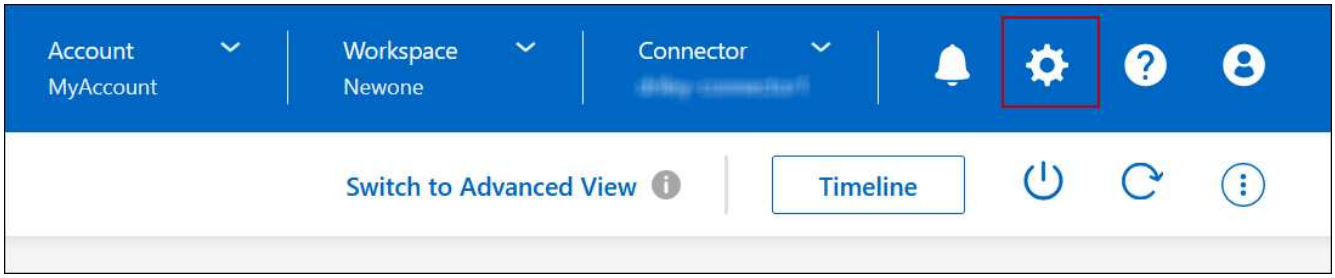
이 프로세스는 CIFS 클라이언트에 영향을 줄 수 있습니다. CIFS 클라이언트에서 커밋되지 않은 데이터는 손실될 수 있습니다.

필요한 것

BlueXP 설정을 변경하려면 먼저 커넥터를 만들어야 합니다. "자세히 알아보기".

단계

1. BlueXP 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 * Cloud Volumes ONTAP Settings * 를 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.

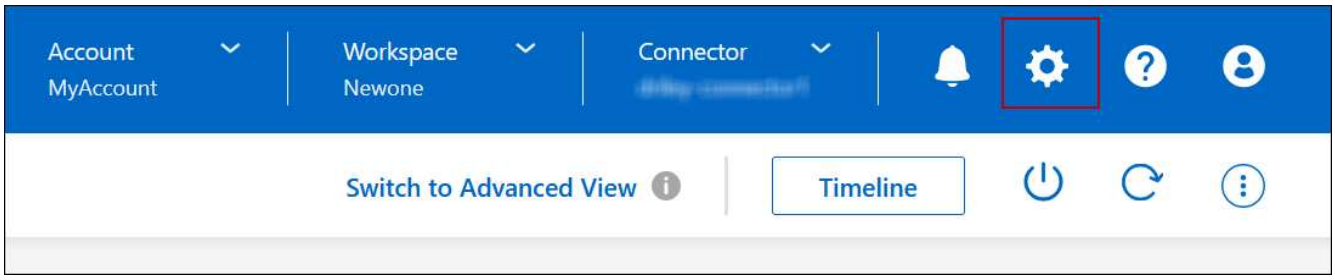
대신 **Azure** 전용 링크를 비활성화하고 서비스 끝점을 사용합니다

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 위에서 설정 아이콘을 클릭하고 * Cloud Volumes ONTAP Settings * 를 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

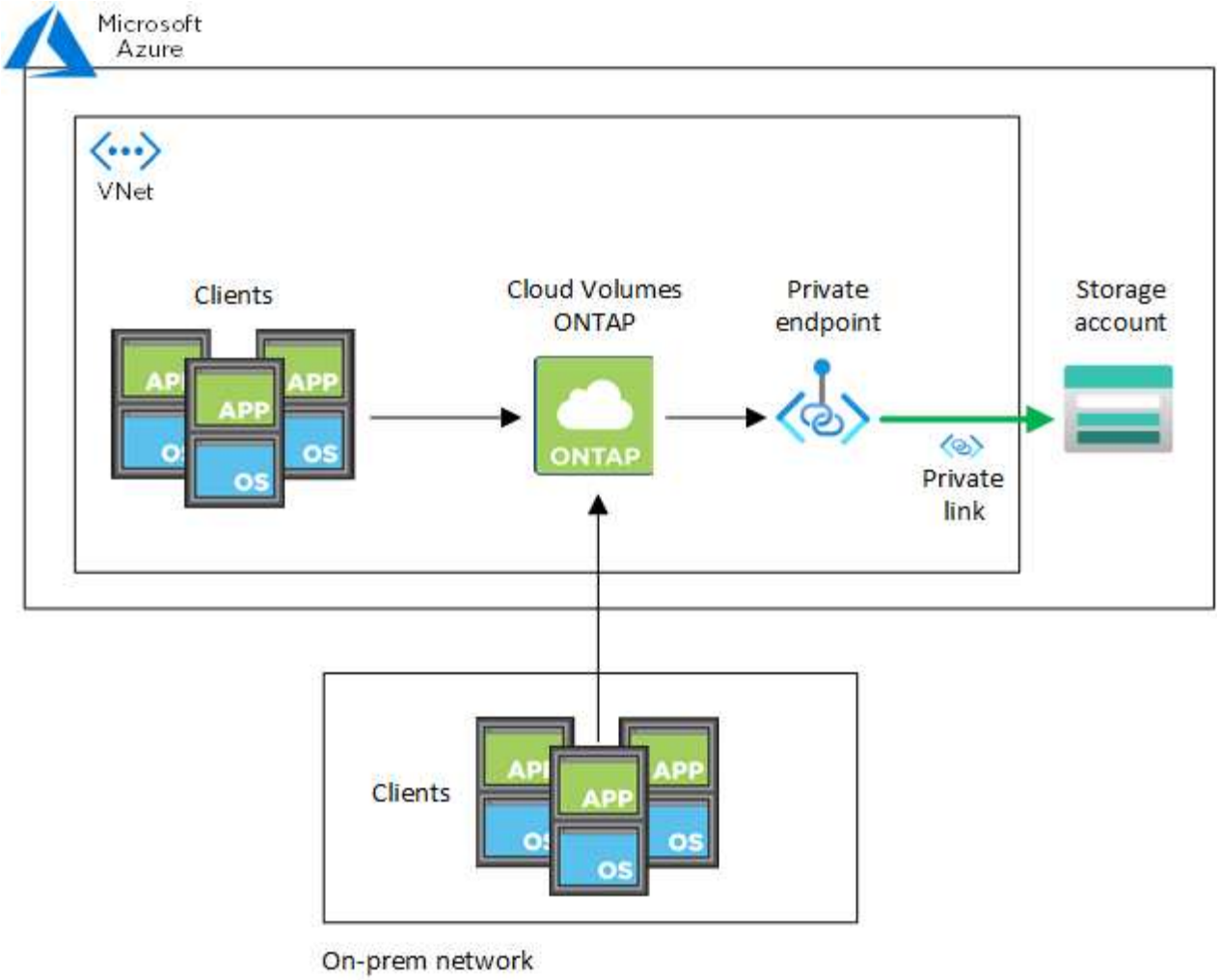
필요에 따라 사용자 지정 DNS로 작업하는 경우 사용자 지정 DNS 서버에서 Azure 개인 DNS 영역에 조건부 전달자를 만들어야 합니다. 자세한 내용은 을 참조하십시오 "DNS 전달자 사용에 대한 Azure의 설명서".

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 **DNS**에 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. 다음 요청 본문과 함께 'Put/occm/config' API 호출 사용:

```
{ "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.

Azure에서 **SnapMirror** 트래픽을 분리합니다

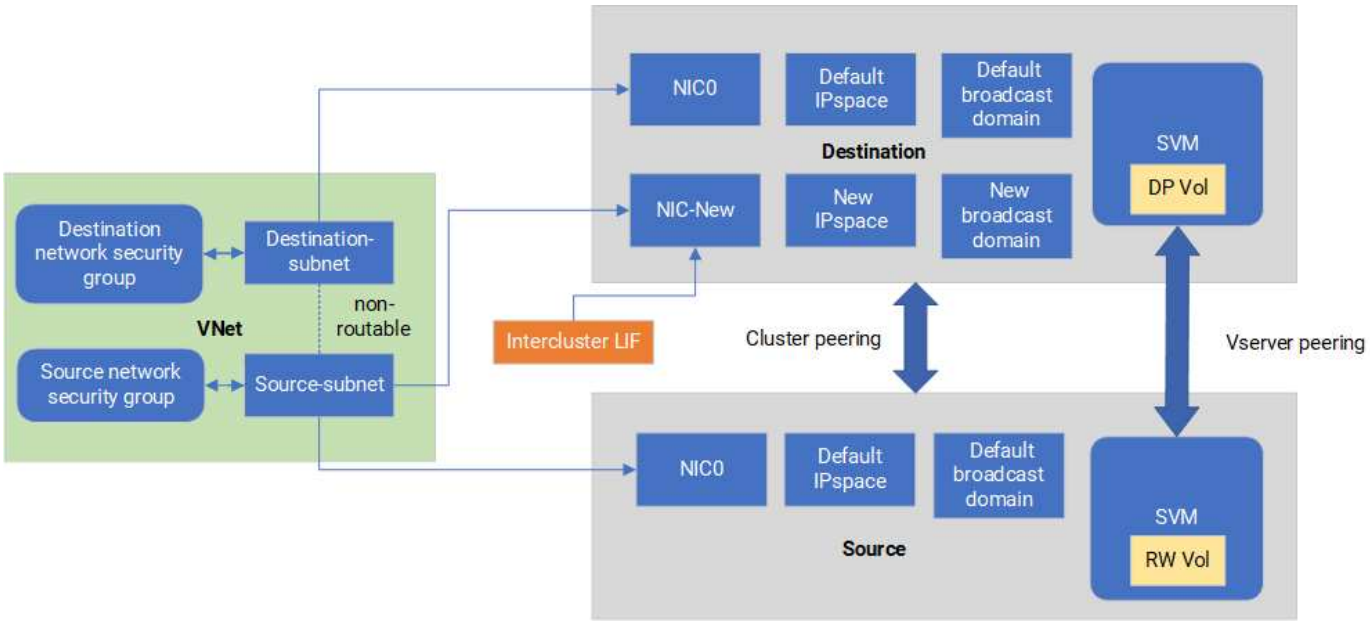
Azure의 Cloud Volumes ONTAP를 사용하면 SnapMirror 복제 트래픽을 데이터와 관리 트래픽에서 분리할 수 있습니다. SnapMirror 복제 트래픽을 데이터 트래픽에서 분리하려면 새 네트워크 인터페이스 카드(NIC), 관련 인터클러스터 LIF 및 라우팅할 수 없는 서브넷을 추가합니다.

Azure에서 **SnapMirror** 트래픽 분리 에 대해 자세히 알아보십시오

기본적으로 BlueXP는 동일한 서브넷에 있는 Cloud Volumes ONTAP 구축의 모든 NIC 및 LIF를 구성합니다. 이러한 구성에서는 SnapMirror 복제 트래픽과 데이터 및 관리 트래픽이 동일한 서브넷을 사용합니다. SnapMirror 트래픽을 분리하면 데이터 및 관리 트래픽에 사용되는 기존 서브넷으로 라우팅할 수 없는 추가 서브넷을 활용합니다.

그림 **1**

다음 다이어그램은 단일 노드 배포에서 추가 NIC, 관련 인터클러스터 LIF 및 라우팅할 수 없는 서브넷과 SnapMirror 복제 트래픽의 분리 과정을 보여줍니다. HA 쌍 구축이 약간 다릅니다.



시작하기 전에

다음 고려 사항을 검토하십시오.

- SnapMirror 트래픽 분리를 위해 단일 NIC를 Cloud Volumes ONTAP 단일 노드 또는 HA 쌍 구축(VM 인스턴스)에 추가할 수 있습니다.
- 새 NIC를 추가하려면 배포하는 VM 인스턴스 유형에 미사용 NIC가 있어야 합니다.
- 소스 및 대상 클러스터는 동일한 VNet(Virtual Network)에 액세스할 수 있어야 합니다. 대상 클러스터는 Azure의 Cloud Volumes ONTAP 시스템입니다. 소스 클러스터는 Azure의 Cloud Volumes ONTAP 시스템 또는 ONTAP 시스템이 될 수 있습니다.

1단계**:** 추가 **NIC**를 생성하고 대상 **VM**에 연결합니다

이 섹션에서는 추가 NIC를 생성하여 대상 VM에 연결하는 방법에 대한 지침을 제공합니다. 대상 VM은 Cloud Volumes ONTAP의 Azure에서 추가 NIC를 설정하려는 단일 노드 또는 HA 쌍 시스템입니다.

단계

1. ONTAP CLI에서 노드를 중지합니다.

```
dest::> halt -node <dest_node-vm>
```

2. Azure 포털에서 VM(노드) 상태가 Stopped인지 확인합니다.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Azure Cloud Shell의 Bash 환경을 사용하여 노드를 중지합니다.
   a. 노드를 중지합니다.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. 노드 할당 해제

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-
vm>
```

4. 두 서브넷(소스 클러스터 서브넷 및 대상 클러스터 서브넷)을 서로 라우팅할 수 없도록 네트워크 보안 그룹 규칙을 구성합니다.

   a. 대상 VM에 새 NIC를 생성합니다.

   b. 소스 클러스터 서브넷의 서브넷 ID를 조회합니다.

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet
-name <vnet> --query id
```

   c. 소스 클러스터 서브넷의 서브넷 ID를 사용하여 대상 VM에 새 NIC를 생성합니다. 여기에 새 NIC의 이름을 입력합니다.

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new>
--subnet <id_from_prev_command> --accelerated-networking true
```

   d. privateIPAddress를 저장합니다. 이 IP 주소인 <new_added_nic_primary_addr>는 에서 인터클러스터 LIF를 생성하는 데 사용됩니다 새 NIC의 브로드캐스트 도메인, 인터클러스터 LIF.

5. 새 NIC를 VM에 연결합니다.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics
<dest_node-vm-nic-new>
```

6. VM(노드)을 시작합니다.

```
az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
```

7. Azure 포털에서 * Networking * 으로 이동하여 새 NIC(예: NIC-NEW)가 존재하고 가속 네트워킹이 활성화되었는지 확인합니다.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg
--query "[].{NIC: name, VM: virtualMachine.id}"
```

HA 쌍 구축의 경우 파트너 노드에 대해 단계를 반복합니다.

2단계**:** 새 **NIC**에 대한 새 **IPspace,** 브로드캐스트 도메인 및 인터클러스터 **LIF**를 생성합니다

인터클러스터 LIF에 대한 별도의 IPspace를 통해 클러스터 간 복제를 위해 네트워킹 기능 간에 논리적으로 분리할 수 있습니다.

다음 단계에서는 ONTAP CLI를 사용합니다.

단계

1. 새 IPspace(new_IPspace)를 생성합니다.

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. 새 IPspace(new_IPspace)에 브로드캐스트 도메인을 만들고 nic-new 포트를 추가합니다.

```
dest::> network port show
```

3. 단일 노드 시스템의 경우 새로 추가된 포트는_e0b_입니다. 관리형 디스크가 있는 HA Pair 배포의 경우 새로 추가된 포트는_e0d_입니다. 페이지 Blob이 있는 HA 쌍 구축의 경우 새로 추가된 포트는_e0e_입니다. VM 이름이 아닌 노드 이름을 사용합니다. 를 실행하여 노드 이름을 찾습니다 `node show`.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. 새 브로드캐스트 도메인(new_BD) 및 새 NIC(NIC-NEW)에 인터클러스터 LIF를 생성합니다.

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. 새 인터클러스터 LIF가 생성되었는지 확인합니다.

```
dest::> net int show
```

HA 쌍 구축의 경우 파트너 노드에 대해 단계를 반복합니다.

3단계**:** 소스 시스템과 타겟 시스템 간 클러스터 피어링을 확인합니다

이 섹션에서는 소스 시스템과 대상 시스템 간의 피어링을 확인하는 방법에 대한 지침을 제공합니다.

다음 단계에서는 ONTAP CLI를 사용합니다.

단계

1. 대상 클러스터의 인터클러스터 LIF가 소스 클러스터의 인터클러스터 LIF를 ping할 수 있는지 확인합니다. 대상 클러스터가 이 명령을 실행하므로 대상 IP 주소가 소스에서 인터클러스터 LIF IP 주소가 됩니다.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. 소스 클러스터의 인터클러스터 LIF가 대상 클러스터의 인터클러스터 LIF를 ping할 수 있는지 확인합니다. 대상은 대상에 생성된 새 NIC의 IP 주소입니다.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

HA 쌍 구축의 경우 파트너 노드에 대해 단계를 반복합니다.

4단계**:** 소스 시스템과 타겟 시스템 간에 **SVM** 피어링을 생성합니다

이 섹션은 소스 시스템과 타겟 시스템 간에 SVM 피어링을 생성하는 방법에 대한 지침을 제공합니다.

다음 단계에서는 ONTAP CLI를 사용합니다.

단계

1. 소스 인터클러스터 LIF IP 주소를 로 사용하여 대상에서 클러스터 피어링을 생성합니다 `-peer-addrs`. HA 페어의 경우 두 노드에 대한 소스 인터클러스터 LIF IP 주소를 로 나열합니다 `-peer-addrs`.

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. 암호를 입력하고 확인합니다.
3. 타겟 클러스터 LIF IP 주소를 로 사용하여 소스에서 클러스터 피어링을 생성합니다 `peer-addrs`. HA 쌍의 경우, 두 노드의 대상 인터클러스터 LIF IP 주소를 로 나열합니다 `-peer-addrs`.

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. 암호를 입력하고 확인합니다.
5. 클러스터가 피어링되었는지 확인합니다.

```
src::> cluster peer show
```

성공적인 피어링은 가용성 필드에 * 사용 가능 * 을 표시합니다.

6. 타겟에서 SVM 피어링을 생성합니다. 소스 및 대상 SVM 모두 데이터 SVM이어야 합니다.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. SVM 피어링을 수락합니다.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. SVM이 피어링되었는지 확인합니다.

```
dest::> vserver peer show
```

피어 상태가 표시됩니다 **`peered`**와 피어링 응용 프로그램이 표시됩니다 **`*`snapmirror`**.

5단계**:** 소스 시스템과 대상 시스템 사이에 **SnapMirror** 복제 관계를 생성합니다

이 섹션에서는 소스 시스템과 대상 시스템 간에 SnapMirror 복제 관계를 생성하는 방법에 대해 설명합니다.

기존 SnapMirror 복제 관계를 이동하려면 새 SnapMirror 복제 관계를 생성하기 전에 먼저 기존 SnapMirror 복제 관계를 해제해야 합니다.

다음 단계에서는 ONTAP CLI를 사용합니다.

단계

1. 대상 SVM에 데이터로 보호된 볼륨을 생성합니다.

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. 복제 일정 및 SnapMirror 정책을 포함하는 대상에서 SnapMirror 복제 관계를 생성합니다.

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. 타겟에서 SnapMirror 복제 관계를 초기화합니다.

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. ONTAP CLI에서 다음 명령을 실행하여 SnapMirror 관계 상태를 확인합니다.

```
dest::> snapmirror show
```

관계 상태는 입니다 `Snapmirrored` 그리고 관계의 상태는 이다 `true`.

5. 선택 사항: ONTAP CLI에서 다음 명령을 실행하여 SnapMirror 관계에 대한 작업 기록을 봅니다.

```
dest::> snapmirror show-history
```

필요에 따라 소스 및 대상 볼륨을 마운트하고, 소스에 파일을 쓰고, 볼륨이 대상에 복제되는지 확인할 수 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.

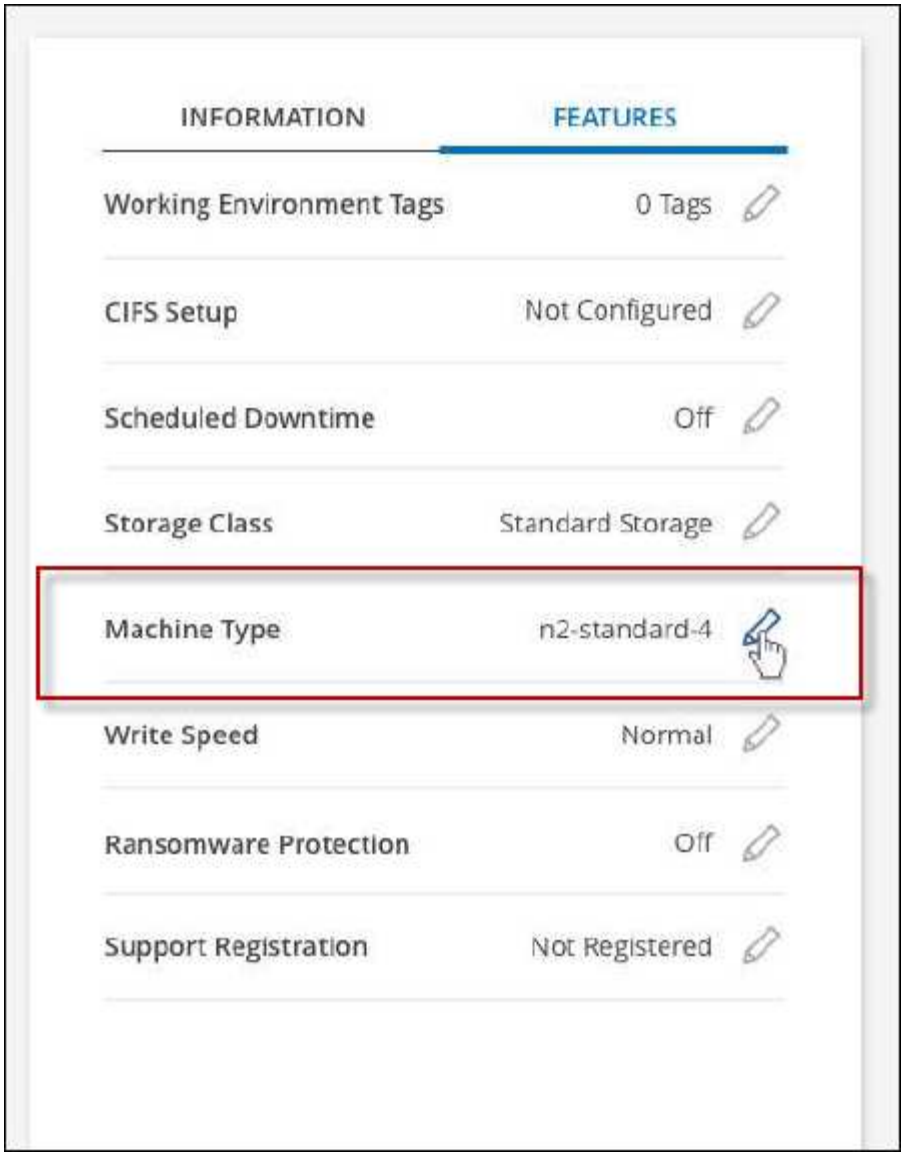
  단일 노드 시스템의 경우 입출력이 중단됩니다.

  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 라이센스를 사용하는 경우 * 라이센스 유형 * 옆에 있는 연필 아이콘을 클릭하여 다른 라이센스 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.

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.

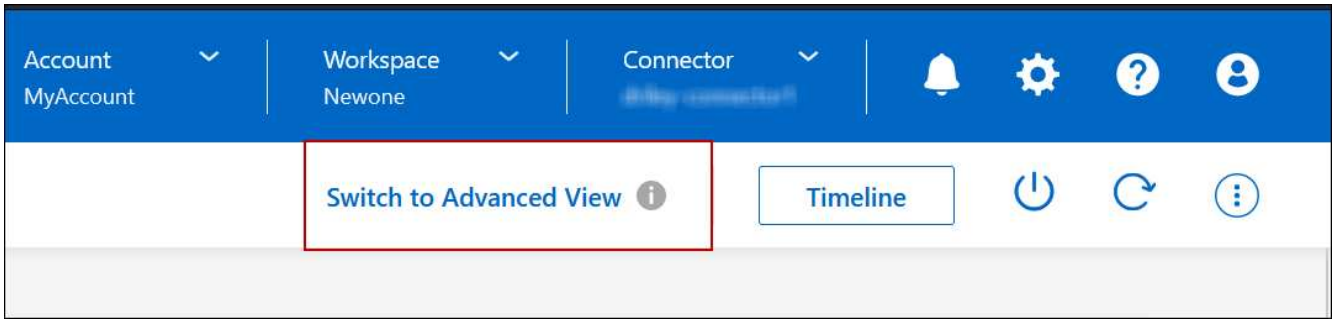
또한 System Manager의 역할 기반 액세스 제어가 지원되지 않습니다.

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

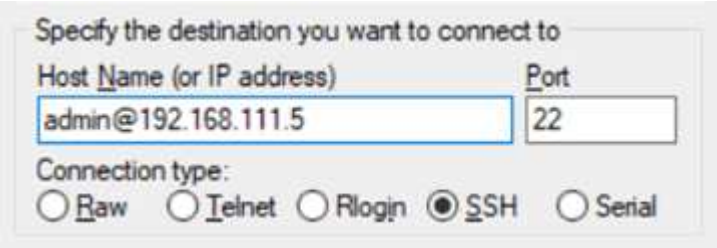
1. BlueXP에서 클러스터 관리 인터페이스의 IP 주소를 확인합니다.
   a. 왼쪽 탐색 메뉴에서 * Storage > Canvas * 를 선택합니다.
   b. Canvas 페이지에서 Cloud Volumes ONTAP 시스템을 선택합니다.

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::>
```

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 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.