



# **Cloud Manager** 설정 및 관리

## Set up and administration

NetApp  
July 15, 2022

# 목차

|   |     |
|---|-----|
| Cloud Manager 설정 및 관리                             | 1   |
| 릴리스 정보  | 2   |
| 새로운 기능  | 2   |
| 알려진 제한 사항   | 10  |
| 시작하십시오  | 13  |
| Cloud Manager에 대해 자세히 알아보십시오                      | 13  |
| 시작 체크리스트  | 14  |
| NetApp Cloud Central에 등록                          | 18  |
| Cloud Manager에 로그인                                | 19  |
| NetApp 계정 설정                                      | 21  |
| 커넥터를 설정합니다  | 29  |
| 다음 단계로 넘어갑니다                                      | 67  |
| Cloud Manager 관리                                  | 69  |
| NetApp 계정   | 69  |
| 커넥터   | 84  |
| 검색된 클라우드 스토리지                                     | 111 |
| AWS 자격 증명   | 117 |
| Azure 자격 증명                                       | 125 |
| Google Cloud 자격 증명                                | 137 |
| Cloud Manager에서 NetApp Support 사이트 계정을 추가하고 관리합니다 | 145 |
| 참조하십시오  | 152 |
| Cloud Manager에 대한 권한 요약                           | 152 |
| Connector에 대한 AWS 권한                              | 153 |
| Connector에 대한 Azure 권한                            | 176 |
| Connector에 대한 Google Cloud 권한                     | 184 |
| 지식 및 지원   | 189 |
| 지원을 위해 등록하십시오                                     | 189 |
| 도움을 받으십시오   | 190 |
| 법적 고지   | 192 |
| 저작권   | 192 |
| 상표  | 192 |
| 특허  | 192 |
| 개인 정보 보호 정책                                       | 192 |
| 오픈 소스   | 192 |

# Cloud Manager 설정 및 관리

# 릴리스 정보

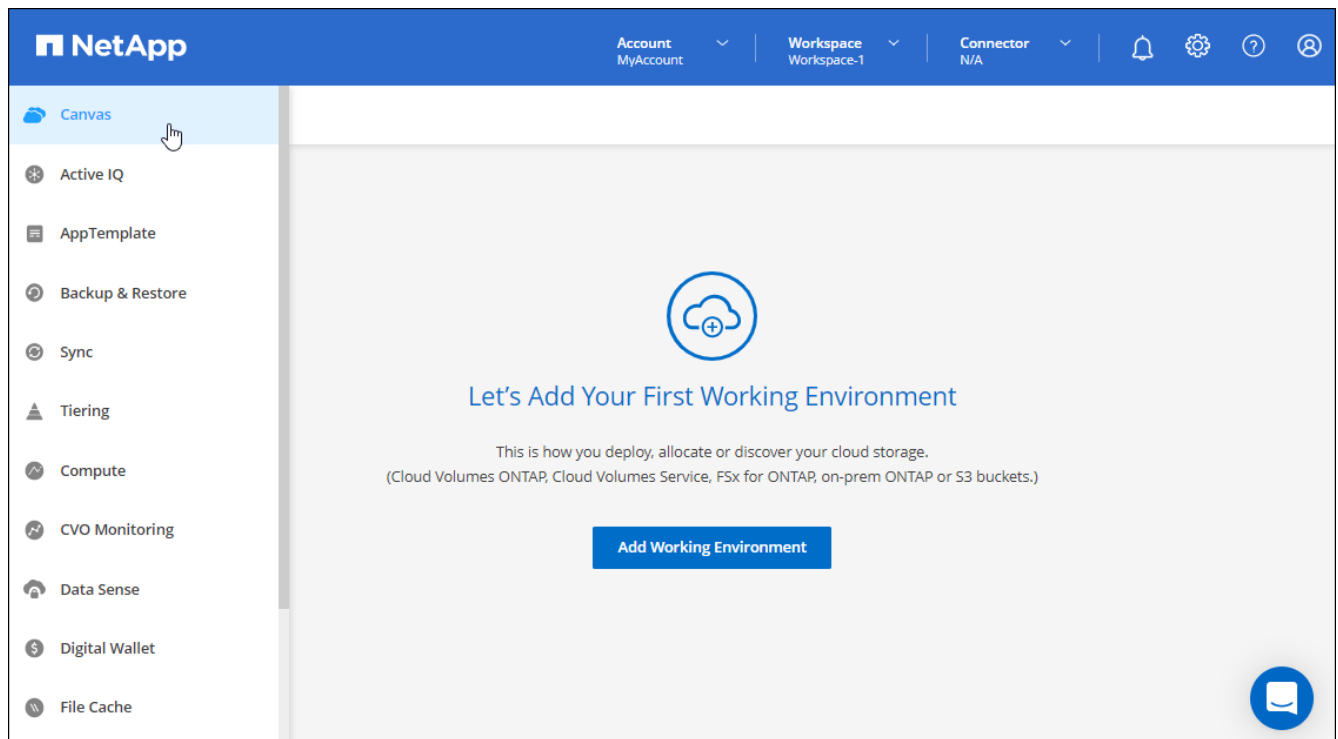
## 새로운 기능

Cloud Manager의 관리 기능, 즉 NetApp 계정, 커넥터, 클라우드 공급자 자격 증명 등과 관련된 새로운 기능에 대해 알아보십시오.

**2022년 7월 3일**

커넥터 **3.9.20**

- Cloud Manager 인터페이스에 추가된 새로운 기능을 탐색하는 방법이 도입되었습니다. 이제 왼쪽 패널 위로 마우스를 이동하면 익숙한 Cloud Manager 기능을 모두 쉽게 찾을 수 있습니다.



- 이제 Cloud Manager를 구성하여 시스템에 로그인하지 않아도 중요한 시스템 작업을 이메일로 통지할 수 있습니다.

["계정의 작업 모니터링에 대해 자세히 알아보십시오."](#)

- Cloud Manager는 이제 Amazon S3 지원과 비슷하게 Azure Blob 스토리지 및 Google Cloud Storage를 작업 환경으로 지원합니다.

Azure 또는 Google Cloud에 Connector를 설치한 후 Cloud Manager는 이제 Connector가 설치된 프로젝트의 Azure Blob 스토리지 또는 Google Cloud Storage에 대한 정보를 자동으로 검색합니다. Cloud Manager는 오브젝트 스토리지를 작업 환경으로 표시하여 더 자세한 정보를 볼 수 있도록 합니다.

Azure Blob 작업 환경의 예는 다음과 같습니다.

[상위 수준의 개요와 스토리지 계정에 대한 자세한 정보를 볼 수 있는 Azure Blob 작업 환경을 보여 주는 스크린샷]

- NetApp은 용량, 암호화 세부 정보 등과 같은 S3 버킷에 대한 자세한 정보를 제공하여 Amazon S3 작업 환경의 리소스 페이지를 재설계했습니다.
- Connector는 이제 다음 Google Cloud 영역에서 지원됩니다.
  - 마드리드(유럽 - 남서쪽1)
  - 파리(유럽 - west9)
  - 바르샤바(유럽-중중심2)
- 이제 커넥터는 Azure West US 3 지역에서 지원됩니다.

["지원되는 영역의 전체 목록을 봅니다"](#)

- 이 커넥터 릴리스에는 Cloud Volumes ONTAP의 향상된 기능도 포함되어 있습니다.

["Cloud Volumes ONTAP의 향상된 기능에 대해 알아보십시오"](#)

## 2022년 6월 28일

### NetApp 자격 증명으로 로그인합니다

새로운 사용자가 Cloud Central에 등록하면 이제 NetApp \* 옵션을 사용하여 로그인 \* 을 선택하여 NetApp Support 사이트 자격 증명으로 로그인할 수 있습니다. 이 방법은 전자 메일 주소와 암호를 입력하는 대신 사용됩니다.



전자 메일 주소와 암호를 사용하는 기존 로그인 방법은 해당 로그인 방법을 계속 사용해야 합니다. NetApp으로 로그인 옵션은 등록하는 새 사용자를 위해 사용할 수 있습니다.

## 2022년 6월 7일

### 커넥터 3.9.19

- 커넥터는 현재 AWS 자카르타 지역(AP-동남동-3)에서 지원됩니다.
- 이제 Connector는 Azure Brazil Southeast 지역에서 지원됩니다.

["지원되는 영역의 전체 목록을 봅니다"](#)

- 이번 커넥터 릴리즈에는 Cloud Volumes ONTAP의 향상된 기능과 사내 ONTAP 클러스터의 향상된 기능도 포함되어 있습니다.
  - ["Cloud Volumes ONTAP의 향상된 기능에 대해 알아보십시오"](#)
  - ["ONTAP 온프레미스 클러스터 개선 사항에 대해 알아보십시오"](#)

## 2022년 5월 12일

### 커넥터 3.9.18 패치

버그 수정을 소개하기 위해 Connector를 업데이트했습니다. 가장 주목할 만한 수정 사항은 커넥터가 공유 VPC에 있을 때 Google Cloud의 Cloud Volumes ONTAP 구축에 영향을 미치는 문제입니다.

2022년 5월 2일

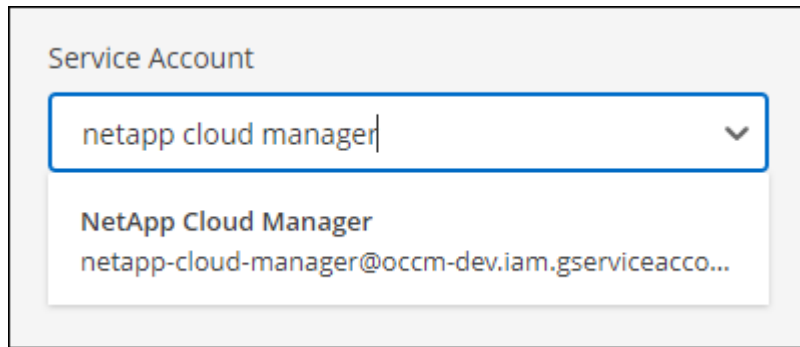
### 커넥터 3.9.18

- Connector는 이제 다음 Google Cloud 영역에서 지원됩니다.

- 델리(아시아 - 남쪽 2)
- 멜번(호주 - 수테스토2)
- 밀라노(유럽 - west8)
- 산티아고(사우스메리카 - 웨스트투어)

"지원되는 영역의 전체 목록을 봅니다"

- Connector에 사용할 Google Cloud 서비스 계정을 선택하면 Cloud Manager에 각 서비스 계정과 연결된 이메일 주소가 표시됩니다. 이메일 주소를 보면 동일한 이름을 공유하는 서비스 계정을 쉽게 구별할 수 있습니다.



- 당사는 지원하는 OS를 통해 VM 인스턴스에서 Google Cloud의 Connector를 인증했습니다 ["차폐된 VM 기능"](#)
- 이 커넥터 릴리스에는 Cloud Volumes ONTAP의 향상된 기능도 포함되어 있습니다. ["이러한 향상된 기능에 대해 알아보십시오"](#)
- Connector에서 Cloud Volumes ONTAP를 구축하려면 새로운 AWS 권한이 필요합니다.

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

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

이제 Cloud Manager에서 배치 그룹을 만드는 방법을 최적화하려면 이러한 권한이 필요합니다.

Cloud Manager에 추가한 각 AWS 자격 증명 세트에 이러한 권한을 제공해야 합니다. ["Connector에 대한 최신 IAM 정책을 봅니다"](#).

2022년 4월 3일

### 커넥터 3.9.17

- 이제 Cloud Manager가 사용자 환경에서 설정한 IAM 역할을 가정하도록 하여 Connector를 생성할 수 있습니다. 이 인증 방법은 AWS 액세스 키와 비밀 키를 공유하는 것보다 더 안전합니다.

"IAM 역할을 사용하여 커넥터를 생성하는 방법에 대해 알아봅니다".

- 이 커넥터 릴리스에는 Cloud Volumes ONTAP의 향상된 기능도 포함되어 있습니다. ["이러한 향상된 기능에 대해 알아보십시오"](#)

## 2022년 2월 27일

### 커넥터 3.9.16

- Google Cloud에서 새 Connector를 만들면 Cloud Manager에 기존의 모든 방화벽 정책이 표시됩니다. 이전에는 Cloud Manager에 타겟 태그가 없는 정책이 표시되지 않았습니다.
- 이 커넥터 릴리스에는 Cloud Volumes ONTAP의 향상된 기능도 포함되어 있습니다. ["이러한 향상된 기능에 대해 알아보십시오"](#)

## 2022년 1월 30일

### 커넥터 3.9.15

이 커넥터 릴리스에는 Cloud Volumes ONTAP의 향상된 기능이 포함되어 있습니다. ["이러한 향상된 기능에 대해 알아보십시오"](#)

## 2022년 1월 2일

커넥터 끝점이 줄어듭니다

Connector가 퍼블릭 클라우드 환경 내에서 리소스와 프로세스를 관리하는 데 필요한 엔드포인트 수를 줄였습니다.

["필요한 끝점 목록을 봅니다"](#).

커넥터에 대한 **EBS** 디스크 암호화

Cloud Manager에서 AWS에 새 Connector를 구축하는 경우 이제 기본 마스터 키 또는 관리 키를 사용하여 Connector의 EBS 디스크를 암호화할 수 있습니다.

✓ Get Ready

✓ AWS Credentials

3 Details

4 Network

5 Security Group

6 Review

### Details

Connector Instance Name

Connector1

Connector Role

☒ Create Role ☐ Select an existing Role

Role Name

Cloud-Manager-Operator-9yils3K

+ Add Tags to Connector Instance

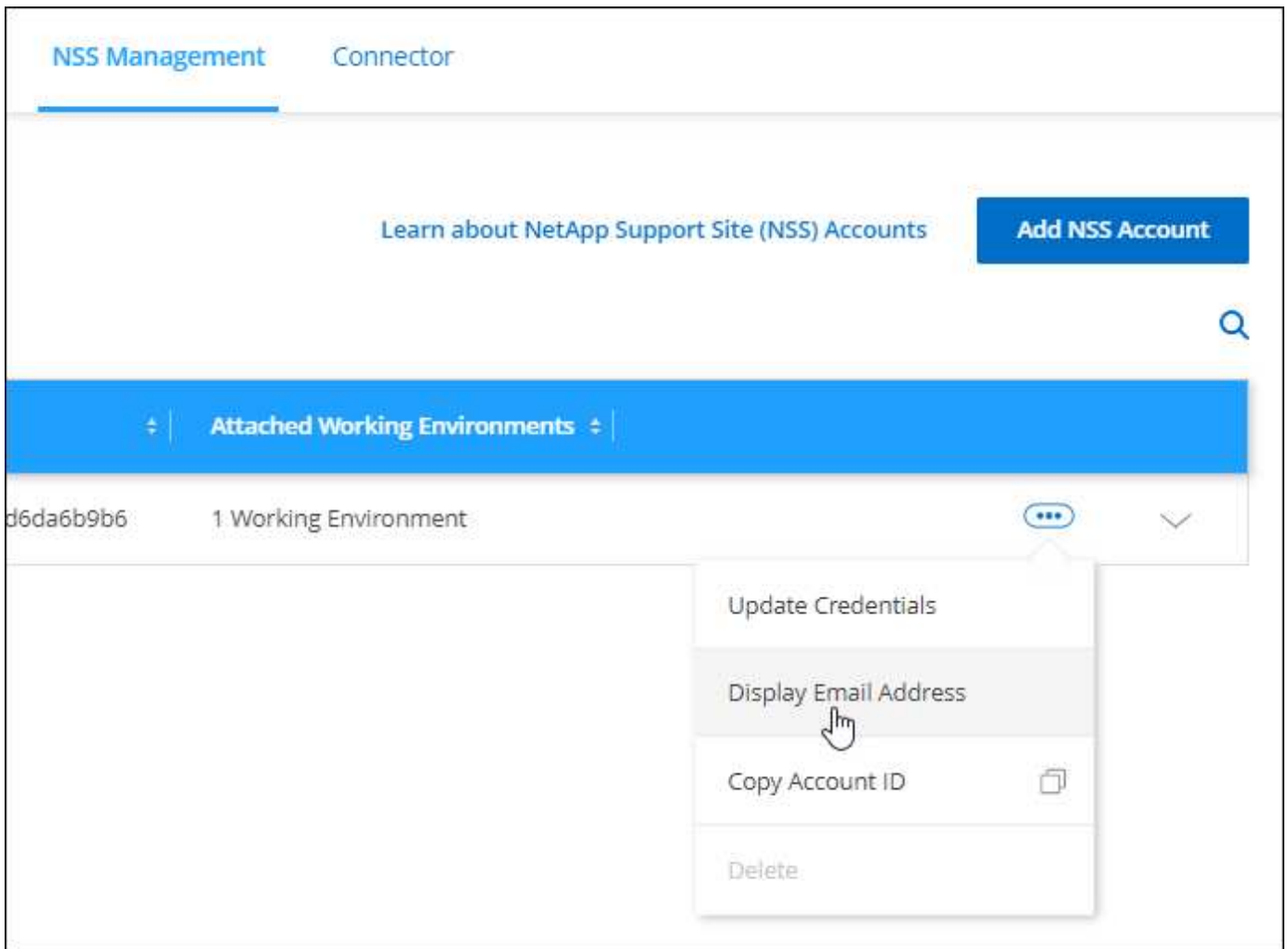
☒ AWS Managed Encryption

Master Key: aws/ebs (default) [Change Key](#)

**NSS** 계정의 이메일 주소입니다

이제 Cloud Manager에서 NetApp Support 사이트 계정과 연결된 이메일 주소를 표시할 수 있습니다.





**2021년 11월 28일**

**NetApp Support** 사이트 계정을 위해 업데이트해야 합니다

2021년 12월부터 NetApp은 Microsoft Azure Active Directory를 지원 및 라이선싱과 관련된 인증 서비스의 ID 공급자로 사용합니다. 이 업데이트의 결과로, Cloud Manager에서 이전에 추가한 기존 NetApp Support 사이트 계정의 자격 증명을 업데이트하라는 메시지를 표시합니다.

NSS 계정을 IDaaS로 마이그레이션하지 않은 경우 먼저 계정을 마이그레이션한 다음 Cloud Manager에서 자격 증명을 업데이트해야 합니다.

- ["NSS 계정을 새 인증 방법으로 업데이트하는 방법을 알아봅니다"](#).
- ["NetApp에서 ID 관리를 위해 Microsoft Azure AD를 사용하는 방법에 대해 자세히 알아보십시오"](#)

**Cloud Volumes ONTAP의 NSS** 계정을 변경합니다

조직에 여러 NetApp Support 사이트 계정이 있는 경우, 이제 Cloud Volumes ONTAP 시스템과 연결된 계정을 변경할 수 있습니다.

["작업 환경을 다른 NSS 계정에 연결하는 방법에 대해 알아봅니다"](#).

## 2021년 11월 4일

### SOC 2 Type 2 인증

독립적인 인증 퍼블릭 회계 업체 및 서비스 감사자는 Cloud Manager, Cloud Sync, Cloud Tiering, Cloud Data Sense 및 Cloud Backup(Cloud Manager 플랫폼)을 검토하여 해당 Trust Services 기준을 기반으로 SOC 2 Type 2 보고서를 작성했다고 확인했습니다.

["NetApp의 SOC 2 보고서 보기"](#).

커넥터가 더 이상 프록시로 지원되지 않습니다

더 이상 Cloud Manager 커넥터를 프록시 서버로 사용하여 Cloud Volumes ONTAP에서 AutoSupport 메시지를 보낼 수 없습니다. 이 기능은 제거되었으며 더 이상 지원되지 않습니다. NAT 인스턴스 또는 환경의 프록시 서비스를 통해 AutoSupport 연결을 제공해야 합니다.

["Cloud Volumes ONTAP를 사용하여 AutoSupport를 확인하는 방법에 대해 자세히 알아보십시오"](#)

## 2021년 10월 31일

서비스 보안 주체를 사용한 인증

Microsoft Azure에서 새 Connector를 만들면 Azure 계정 자격 증명이 아닌 Azure 서비스 보안 주체를 사용하여 인증할 수 있습니다.

["Azure 서비스 보안 주체를 인증하는 방법에 대해 알아보십시오"](#).

자격 증명 향상

사용하기 쉽고 Cloud Manager 인터페이스의 현재 모양과 느낌을 맞추기 위해 자격 증명 페이지를 다시 설계했습니다.

## 2021년 9월 2일

새 알림 서비스가 추가되었습니다

알림 서비스가 도입되어 현재 로그인 세션 중에 시작한 Cloud Manager 작업의 상태를 확인할 수 있습니다. 작업이 성공했는지 또는 실패했는지 확인할 수 있습니다. ["계정의 작업을 모니터링하는 방법을 확인하십시오"](#).

## 2021년 8월 1일

커넥터를 통한 RHEL 7.9 지원

이제 Connector는 Red Hat Enterprise Linux 7.9를 실행하는 호스트에서 지원됩니다.

["커넥터에 대한 시스템 요구 사항을 봅니다"](#).

## 2021년 7월 7일

## 커넥터 추가 마법사 기능 향상

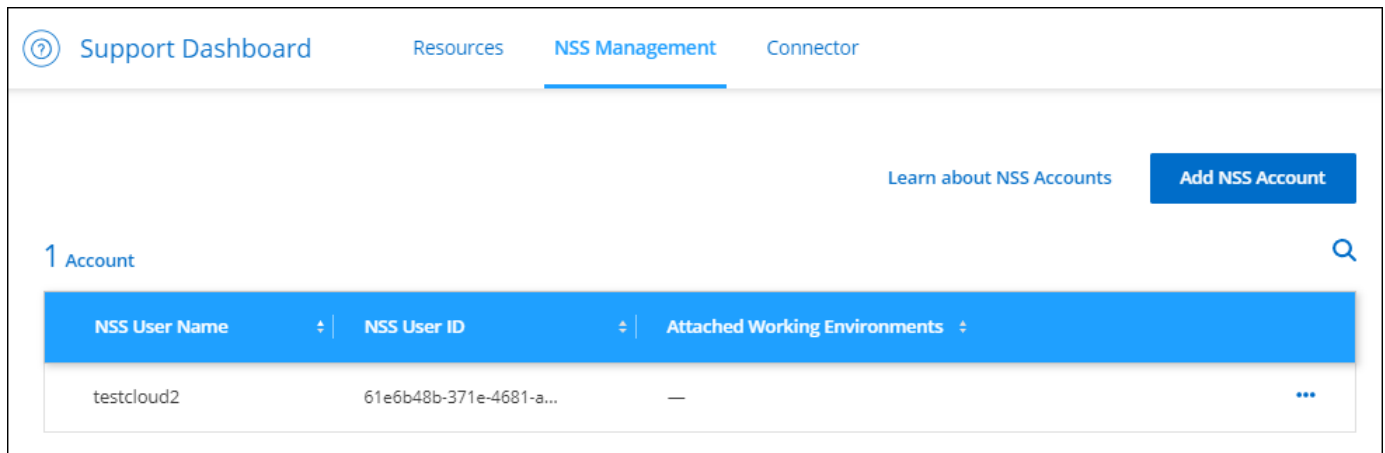
새 옵션을 추가하고 사용하기 쉽도록 \* 커넥터 추가 \* 마법사를 다시 설계했습니다. 이제 태그를 추가하고, 역할을 지정하고(AWS 또는 Azure의 경우), 프록시 서버에 대한 루트 인증서를 업로드하고, Terraform 자동화에 대한 코드를 보고, 진행률 세부 정보를 보는 등의 작업을 수행할 수 있습니다.

- ["AWS에서 커넥터를 생성합니다"](#)
- ["Azure에서 커넥터를 만듭니다"](#)
- ["GCP에서 커넥터를 생성합니다"](#)

## NSS 지원 대시보드의 계정 관리

이제 NSS(NetApp Support Site) 계정은 Settings(설정) 메뉴가 아니라 Support Dashboard에서 관리됩니다. 이러한 변경을 통해 단일 위치에서 모든 지원 관련 정보를 쉽게 찾고 관리할 수 있습니다.

["NSS 계정 관리 방법에 대해 알아봅니다"](#).



## 2021년 5월 5일

### 타임라인의 계정

이제 Cloud Manager의 타임라인에 계정 관리와 관련된 작업 및 이벤트가 표시됩니다. 이러한 동작에는 사용자 연결, 작업 영역 만들기, 커넥터 만들기 등이 있습니다. 특정 작업을 수행한 사람을 확인해야 하거나 작업의 상태를 확인해야 하는 경우 시간 표시 막대를 확인하는 것이 도움이 됩니다.

["타임라인을 Tenancy 서비스로 필터링하는 방법에 대해 알아보십시오"](#).

## 2021년 4월 11일

### API는 Cloud Manager로 직접 호출합니다

프록시 서버를 구성한 경우 프록시를 통하지 않고 API 호출을 Cloud Manager로 직접 전송하는 옵션을 사용할 수 있습니다. 이 옵션은 AWS 또는 Google Cloud에서 실행되는 커넥터에서 지원됩니다.

["이 설정에 대해 자세히 알아보십시오"](#).

## 서비스 계정 사용자

이제 서비스 계정 사용자를 만들 수 있습니다.

서비스 계정은 자동화를 위해 Cloud Manager에 승인된 API 호출을 수행할 수 있는 "사용자" 역할을 합니다. 따라서 언제든지 퇴사할 수 있는 실제 사용자의 계정을 기반으로 자동화 스크립트를 작성할 필요가 없으므로 자동화를 더욱 쉽게 관리할 수 있습니다. 페더레이션을 사용하는 경우 클라우드에서 새로 고침 토큰을 생성하지 않고 토큰을 생성할 수 있습니다.

["서비스 계정 사용에 대해 자세히 알아보십시오."](#)

## 개인 미리보기

이제 고객 어카운트의 프라이빗 미리보기 기능을 사용하여 Cloud Manager의 미리보기 기능을 이용하여 새로운 NetApp 클라우드 서비스에 액세스할 수 있습니다.

["이 옵션에 대해 자세히 알아보십시오."](#)

## 타사 서비스

또한 사용자 계정의 타사 서비스가 Cloud Manager에서 사용 가능한 타사 서비스에 액세스하도록 허용할 수도 있습니다.

["이 옵션에 대해 자세히 알아보십시오."](#)

## 2021년 2월 9일

### 지원 대시보드 개선 사항

NetApp Support 사이트 자격 증명을 추가하여 지원을 등록할 수 있도록 지원 대시보드를 업데이트했습니다. 대시보드에서 직접 NetApp 지원 케이스를 시작할 수도 있습니다. 도움말 아이콘을 클릭한 다음 \* 지원 \* 을 클릭하십시오.

## 알려진 제한 사항

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

이러한 제한은 Cloud Manager 설정 및 관리, 즉 커넥터, SaaS 플랫폼 등에 적용됩니다.

### 커넥터 제한

#### 172 범위의 IP 주소와 충돌할 수 있습니다

Cloud Manager는 172.17.0.0/16 및 172.18.0.0/16 범위의 IP 주소를 가진 두 개의 인터페이스로 커넥터를 배포합니다.

네트워크에 이러한 범위 중 하나로 구성된 서브넷이 있는 경우 Cloud Manager에서 연결 장애가 발생할 수 있습니다. 예를 들어, Cloud Manager에서 온프레미스 ONTAP 클러스터를 검색하지 못할 수 있습니다.

기술 자료 문서를 참조하십시오 ["Cloud Manager Connector IP가 기존 네트워크와 충돌합니다"](#) 커넥터 인터페이스의

IP 주소를 변경하는 방법에 대한 지침은 을 참조하십시오.

## HTTP 프록시 서버만 지원됩니다

회사 정책에 따라 인터넷에 대한 모든 HTTP 통신에 프록시 서버를 사용해야 하는 경우 해당 HTTP 프록시 서버를 사용하도록 커넥터를 구성해야 합니다. 프록시 서버는 클라우드 또는 네트워크에 있을 수 있습니다.

Cloud Manager는 Connector에서 HTTPS 프록시 사용을 지원하지 않습니다.

## SSL 암호 해독은 지원되지 않습니다

Cloud Manager는 SSL 암호 해독이 활성화된 방화벽 구성을 지원하지 않습니다. SSL 암호 해독이 활성화된 경우 Cloud Manager에 오류 메시지가 나타나고 Connector 인스턴스가 비활성으로 표시됩니다.

보안 강화를 위해 을(를) 선택할 수 있습니다 ["CA\(인증 기관\)에서 서명한 HTTPS 인증서 설치"](#).

## 로컬 UI를 로드할 때 빈 페이지입니다

Connector에 대한 로컬 사용자 인터페이스를 로드하면 UI가 표시되지 않을 수 있으며 빈 페이지가 표시될 수도 있습니다.

이 문제는 캐싱 문제와 관련이 있습니다. 해결 방법은 익명 또는 개인 웹 브라우저 세션을 사용하는 것입니다.

## 공유 Linux 호스트는 지원되지 않습니다

Connector는 다른 애플리케이션과 공유되는 VM에서 지원되지 않습니다. VM은 Connector 소프트웨어 전용이어야 합니다.

## 타사 에이전트 및 내선 번호

타사 에이전트 또는 VM 확장은 커넥터 VM에서 지원되지 않습니다.

## SaaS 제한 사항

정부 지역에서는 **SaaS** 플랫폼을 사용할 수 없습니다

AWS GovCloud 지역, Azure Gov 지역 또는 Azure DoD 지역에 Connector를 구축하는 경우 Connector의 호스트 IP 주소를 통해서만 Cloud Manager에 액세스할 수 있습니다. 전체 계정에 대해 SaaS 플랫폼에 대한 액세스가 비활성화되었습니다.

즉, 최종 사용자 내부 VPC/VNET에 액세스할 수 있는 권한이 있는 사용자만 Cloud Manager의 UI 또는 API를 사용할 수 있습니다.

이러한 지역에서 지원되는 유일한 서비스는 Cloud Volumes ONTAP, 클라우드 백업, 클라우드 데이터 감지 및 복제입니다. 정부 지역에서는 다른 NetApp 서비스가 지원되지 않습니다.

["Connector에서 로컬 UI에 액세스하는 방법에 대해 알아봅니다"](#).

## 시장 제한

**Azure** 및 **Google Cloud** 파트너는 사용한 만큼만 지불하는 방식을 사용할 수 없습니다

Microsoft 클라우드 솔루션 공급자(CSP) 파트너이거나 Google Cloud 파트너인 경우 NetApp의 용량제 구독을 사용할 수 없습니다. BYOL 라이선스를 통해 NetApp 클라우드 솔루션을 구축하고 라이선스를 구입해야 함

다음 NetApp 클라우드 서비스에서는 용량제 구독을 사용할 수 없습니다.

- Cloud Volumes ONTAP
- 클라우드 계층화
- 클라우드 백업
- 클라우드 데이터 감지

# 시작하십시오

## Cloud Manager에 대해 자세히 알아보십시오

Cloud Manager를 사용하면 IT 전문가 및 클라우드 설계자가 NetApp의 클라우드 솔루션을 사용하여 하이브리드 멀티 클라우드 인프라를 중앙에서 관리할 수 있습니다.

### 피처

Cloud Manager는 엔터프라이즈급 SaaS 기반 관리 플랫폼으로, 데이터의 위치에 상관없이 데이터를 제어할 수 있습니다.

- 설정 및 사용 ["Cloud Volumes ONTAP"](#) 클라우드 전반에서 효율적인 멀티 프로토콜 데이터 관리
- 파일 스토리지 서비스 설정 및 사용:
  - ["Azure NetApp Files"](#)
  - ["ONTAP용 Amazon FSx"](#)
  - ["AWS 환경을 위한 Cloud Volumes Service"](#)
  - ["Google Cloud용 Cloud Volumes Service"](#)
- 볼륨 생성, 클라우드에 백업, 하이브리드 클라우드 간 데이터 복제, 콜드 데이터를 클라우드로 계층화하여 온프레미스 ONTAP 클러스터를 검색하고 관리할 수 있습니다.
- 다음과 같은 통합 클라우드 서비스 지원:
  - ["클라우드 데이터 감지"](#)
  - ["Cloud Insights"](#)
  - ["클라우드 백업"](#)

["Cloud Manager에 대해 자세히 알아보십시오"](#).

### 지원되는 오브젝트 스토리지 공급자

Cloud Manager를 사용하면 Amazon Web Services, Microsoft Azure, Google Cloud에서 클라우드 스토리지를 관리하고 클라우드 서비스를 사용할 수 있습니다.

### 비용

Cloud Manager 소프트웨어는 NetApp에서 무료로 제공합니다.

대부분의 작업에서 Cloud Manager는 클라우드 네트워크에 Connector를 배포하라는 메시지를 표시합니다. 그러면 컴퓨팅 인스턴스 및 관련 스토리지에 대한 클라우드 공급자의 요금이 부과됩니다. 구내에서 Connector 소프트웨어를 실행할 수 있는 옵션이 있습니다.

["Connector의 기본 설정에 대해 알아봅니다"](#).

## Cloud Manager의 작동 방식

Cloud Manager에는 NetApp Cloud Central과 통합된 SaaS 기반 인터페이스 및 Cloud Volumes ONTAP 및 기타 클라우드 서비스를 관리하는 커넥터가 포함되어 있습니다.

### 서비스형 소프트웨어

Cloud Manager는 를 통해 액세스할 수 있습니다 ["SaaS 기반 사용자 인터페이스"](#) API를 사용해 보십시오. 이러한 SaaS 환경을 통해 최신 기능에 자동으로 액세스하고 NetApp 계정과 커넥터 간에 쉽게 전환할 수 있습니다.

### NetApp Cloud Central에서

["NetApp Cloud Central에서"](#) 액세스 및 관리를 위한 중앙 집중식 위치를 제공합니다 ["NetApp 클라우드 서비스"](#). 중앙 집중식 사용자 인증을 통해 동일한 자격 증명 세트를 사용하여 Cloud Manager와 Cloud Insights 같은 다른 클라우드 서비스에 액세스할 수 있습니다.

### NetApp 계정

Cloud Manager에 처음 로그인하면 `_NetApp 계정_`을 생성하라는 메시지가 표시됩니다. 이 계정은 다중 테넌시를 제공하며 사용자가 `isolated_workspaces_`에서 사용자 및 리소스를 구성할 수 있도록 합니다.

### 커넥터

대부분의 경우 계정 관리자는 클라우드 또는 온-프레미스 네트워크에 `_Connector_`를 배포해야 합니다. Connector를 사용하면 Cloud Manager에서 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있습니다.

커넥터는 항상 작동 상태를 유지해야 합니다. 이는 여러분이 제공하는 서비스의 지속적인 상태 및 운영에 중요합니다.

예를 들어, Connector는 Cloud Volumes ONTAP의 상태 및 작동에 있어 핵심 구성 요소입니다. 커넥터 전원이 꺼져 있는 경우 노드 기반 라이선스를 가진 Cloud Volumes ONTAP PAYGO 시스템은 커넥터 통신이 14일 이상 끊긴 후 종료됩니다.

["커넥터가 필요한 시기와 작동 방식에 대해 자세히 알아보십시오"](#).

## SOC 2 Type 2 인증

독립적인 인증 퍼블릭 회계 업체 및 서비스 감사자는 Cloud Manager, Cloud Sync, Cloud Tiering, Cloud Data Sense 및 Cloud Backup(Cloud Manager 플랫폼)을 검토하여 해당 Trust Services 기준을 기반으로 SOC 2 Type 2 보고서를 작성했다고 확인했습니다.

["NetApp의 SOC 2 보고서 보기"](#)

## 시작 체크리스트

이 체크리스트를 사용하여 Connector가 아웃바운드 인터넷 액세스를 지원하는 일반적인 구축 환경에서 Cloud Manager를 설치하고 실행하는 데 필요한 사항을 파악하십시오.

### NetApp Cloud Central 로그인

에 가입해야 합니다 ["NetApp Cloud Central에서"](#) Cloud Manager 및 기타 클라우드 서비스에 액세스할 수 있습니다.



## 웹 브라우저에서 여러 엔드포인트로 네트워크 액세스

Cloud Manager 사용자 인터페이스는 웹 브라우저에서 액세스할 수 있습니다. Cloud Manager 사용자 인터페이스를 사용하면 여러 엔드포인트에 접속하여 데이터 관리 작업을 완료할 수 있습니다. 웹 브라우저를 실행하는 컴퓨터는 다음 끝점에 연결되어 있어야 합니다.

| 엔드포인트  | 목적  |
|--|---|
| <a href="http://cloudmanager.netapp.com">http://cloudmanager.netapp.com</a> 으로 문의하십시오  | SaaS UI를 사용할 때 웹 브라우저가 이 URL에 연락합니다.  |
| AWS 서비스(amazonaws.com): <ul style="list-style-type: none"> <li>• CloudFormation 을 참조하십시오</li> <li>• 코니토</li> <li>• EC2(탄력적인 컴퓨팅 클라우드)</li> <li>• 키 관리 서비스(KMS)</li> <li>• 보안 토큰 서비스(STS)</li> <li>• S3(Simple Storage Service)</li> </ul>              | AWS의 Cloud Manager에서 커넥터를 구축하는 데 필요 정확한 끝점은 Connector를 배포하는 영역에 따라 다릅니다. " <a href="#">자세한 내용은 AWS 설명서를 참조하십시오.</a> " |
| <a href="https://management.azure.com">https://management.azure.com</a><br><a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> 으로 문의하십시오   | 대부분의 Azure 지역에서 Cloud Manager의 Connector를 구축하는 데 필요합니다.   |
| <a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a><br><a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a> 으로 문의하십시오   | Azure 독일 지역의 Cloud Manager에서 커넥터를 배포하는 데 필요   |
| <a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a><br><a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> 으로 문의하십시오   | Azure US Gov 지역의 Cloud Manager에서 커넥터를 배포하는 데 필요합니다.   |
| <a href="https://www.googleapis.com">https://www.googleapis.com</a> 으로 문의하십시오  | Google Cloud의 Cloud Manager에서 커넥터를 구축하는 데 필요합니다.  |
| <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a> 으로 문의하십시오  | NSS(NetApp Support Site) 자격 증명을 업데이트하거나 Cloud Manager에 새 NSS 자격 증명을 추가하는 데 필요합니다.                                     |
| <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a><br><a href="https://cdn.auth0.com">https://cdn.auth0.com</a><br><a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a> 를 참조하십시오 | 웹 브라우저는 NetApp Cloud Central을 통해 중앙 집중식 사용자 인증을 위해 이러한 엔드포인트에 연결됩니다.  |
| <a href="https://widget.intercom.io">https://widget.intercom.io</a> 으로 문의하십시오  | 제품 내에서 NetApp 클라우드 전문가와 상담할 수 있는 채팅을 제공합니다.   |

| 엔드포인트         | 목적   |
|---------------|--|
| 커넥터의 IP 주소입니다 | <p>대부분의 경우 SaaS UI에서 Cloud Manager로 작업해야 하지만 "로컬 UI를 사용하는 경우" 그런 다음 웹 브라우저에서 호스트의 IP 주소를 입력해야 합니다.</p> <p>클라우드 공급자에 대한 연결에 따라 호스트에 할당된 프라이빗 IP 또는 공용 IP를 사용합니다.</p> <ul style="list-style-type: none"> <li>• 개인 IP는 VPN이 있고 가상 네트워크에 직접 액세스할 수 있는 경우에 작동합니다</li> <li>• 공용 IP는 모든 네트워킹 시나리오에서 작동합니다</li> </ul> <p>두 경우 모두 보안 그룹 규칙이 승인된 IP 또는 서브넷에서만 액세스를 허용하여 네트워크 액세스를 보호합니다.</p> |

### 커넥터의 아웃바운드 네트워킹

Cloud Manager에 로그인한 후 계정 관리자는 클라우드 공급자 또는 온-프레미스 네트워크에 \_Connector\_를 배포해야 합니다. Connector를 사용하면 Cloud Manager에서 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있습니다. Azure NetApp Files, Cloud Volumes Service 또는 Cloud Sync에는 커넥터가 필요하지 않지만 Cloud Manager의 다른 모든 서비스와 기능에는 커넥터가 필요합니다. "커넥터 및 커넥터 작동 방식에 대해 자세히 알아보십시오".

- 커넥터를 배포하는 네트워크 위치에 아웃바운드 인터넷 연결이 있어야 합니다.

Connector는 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하기 위해 다음 엔드포인트에 연결하는 아웃바운드 인터넷 액세스를 필요로 합니다.

| 엔드포인트  | 목적   |
|--|--|
| <a href="https://support.netapp.com">https://support.netapp.com</a> 으로 문의하십시오  | 라이선스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다. |
| <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a> 으로 문의하십시오  | Cloud Manager 내에서 SaaS 기능 및 서비스를 제공합니다.          |
| <a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a><br><a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a> 으로 문의하십시오 | Connector 및 해당 Docker 구성 요소를 업그레이드합니다.           |

- Connector를 직접 Cloud Manager 인터페이스에서 설치하지 않고 자체 Linux 호스트에 수동으로 설치하는 경우 Connector 설치 과정에서 다음 끝점에 액세스해야 합니다.
  - <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm> 으로 문의하십시오
  - <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip> 으로 문의하십시오
  - [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net) 또는 <https://hub.docker.com> 으로 문의하십시오

설치 중에 호스트가 운영 체제 패키지를 업데이트하려고 할 수 있습니다. 호스트는 이러한 OS 패키지의 서로 다른 미러링 사이트에 연결할 수 있습니다.

- 커넥터 를 시작하지 않으면 커넥터로 들어오는 트래픽이 없습니다.

HTTP(80) 및 HTTPS(443)는 드물게 사용되는 로컬 UI에 대한 액세스를 제공합니다. SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.

## 클라우드 공급자 권한

Cloud Manager에서 직접 클라우드 공급자에 Connector를 배포할 수 있는 권한이 있는 계정이 필요합니다.



커넥터를 작성하는 다른 방법이 있습니다. 에서 커넥터를 작성할 수 있습니다 ["AWS 마켓플레이스 를 참조하십시오"](#), ["Azure 마켓플레이스 를 참조하십시오"](#) 또는 직접 할 수 있습니다 ["소프트웨어를 수동으로 설치합니다"](#).

| 위치           | 높은 수준의 단계  | 세부 단계                                      |
|--------------|--|--|
| 설치하고         | <ol style="list-style-type: none"> <li>1. AWS에서 IAM 정책을 생성하는 데 필요한 권한이 포함된 JSON 파일을 사용하십시오.</li> <li>2. IAM 역할 또는 IAM 사용자에게 정책을 연결합니다.</li> <li>3. Connector를 생성할 때 Cloud Manager에 IAM 역할의 ARN 또는 IAM 사용자를 위한 AWS 액세스 키 및 비밀 키를 제공합니다.</li> </ol>  | <a href="#">"자세한 단계를 보려면 여기를 클릭하십시오"</a> . |
| Azure를 지원합시다 | <ol style="list-style-type: none"> <li>1. Azure에서 사용자 지정 역할을 만드는 데 필요한 권한이 포함된 JSON 파일을 사용합니다.</li> <li>2. Cloud Manager에서 Connector를 생성할 사용자에게 역할을 할당합니다.</li> <li>3. Connector를 만들 때 필요한 권한이 있는 Microsoft 계정(Microsoft가 소유하고 호스팅하는 로그인 프롬프트)으로 로그인합니다.</li> </ol>  | <a href="#">"자세한 단계를 보려면 여기를 클릭하십시오"</a> . |
| Google 클라우드  | <ol style="list-style-type: none"> <li>1. Google Cloud에서 사용자 지정 역할을 생성하는 데 필요한 권한이 포함된 YAML 파일을 사용합니다.</li> <li>2. Cloud Manager에서 Connector를 생성할 사용자에게 해당 역할을 연결합니다.</li> <li>3. Cloud Volumes ONTAP를 사용하려는 경우 필요한 권한이 있는 서비스 계정을 설정합니다.</li> <li>4. Google Cloud API를 활성화합니다.</li> <li>5. Connector를 만들 때 필요한 권한이 있는 Google 계정으로 로그인합니다(로그인 프롬프트는 Google에서 소유 및 호스팅).</li> </ol> | <a href="#">"자세한 단계를 보려면 여기를 클릭하십시오"</a> . |

## 개별 서비스를 위한 네트워킹

설치가 완료되면 Cloud Manager에서 제공하는 서비스를 사용할 수 있습니다. 각 서비스에는 고유한 네트워킹 요구 사항이 있습니다. 자세한 내용은 다음 페이지를 참조하십시오.

- ["AWS 환경을 위한 Cloud Volumes ONTAP"](#)
- ["Azure용 Cloud Volumes ONTAP"](#)

- "GCP용 Cloud Volumes ONTAP"
- "ONTAP 시스템 간 데이터 복제"
- "클라우드 데이터 센스를 구축하는 중입니다"
- "온프레미스 ONTAP 클러스터"
- "클라우드 계층화"
- "클라우드 백업"

## NetApp Cloud Central에 등록

NetApp Cloud Central에 등록하여 NetApp의 클라우드 서비스에 액세스할 수 있습니다.



Single Sign-On을 사용하여 회사 디렉터리(통합 ID)의 자격 증명을 사용하여 로그인할 수 있습니다. 자세한 내용은 [로 이동하십시오 "Cloud Central 도움말 센터"](#) 그런 다음 \* Cloud Central 로그인 옵션 \* 을 클릭합니다.

단계

1. 웹 브라우저를 열고 [로 이동합니다 "NetApp Cloud Central에서"](#).
2. 등록 \* 을 클릭합니다.
3. 두 가지 옵션이 있습니다.
  - a. 양식을 작성하고 \* 등록 \* 을 클릭합니다.

## Log In to NetApp Cloud Central

Already signed up? [Login](#)

*\*optional*

SIGN UP

☒ I accept the [terms and conditions](#).

- b. 등록된 NetApp Support 사이트 계정이 있는 경우 \* NetApp으로 로그인 \* 을 클릭하고 NetApp Support 사이트 자격 증명을 입력합니다.

로그인할 때마다 이 등록 과정에서 선택한 옵션을 사용해야 합니다.



NetApp에 로그인하면 NetApp Support 사이트 자격 증명에 지원 대시보드의 Cloud Manager에 추가되지 않습니다.

4. NetApp Cloud Central에서 이메일을 받을 때까지 기다립니다.
5. 이메일의 링크를 클릭하여 이메일 주소를 확인합니다.

이제 Cloud Central 사용자 로그인이 활성화되었습니다.

## Cloud Manager에 로그인

Cloud Manager 인터페이스는 로 이동하여 SaaS 기반 사용자 인터페이스를 통해 액세스할 수 있습니다 <https://cloudmanager.netapp.com>.

정부 지역 또는 아웃바운드 인터넷 액세스가 없는 사이트에서 Cloud Manager에 액세스하는 경우 Connector에서 실행 중인 로컬 사용자 인터페이스에 로그인해야 합니다. "[Connector에서 로컬 UI에 액세스하는 방법에 대해 알아봅니다](#)".



Single Sign-On을 사용하여 회사 디렉터리(통합 ID)의 자격 증명을 사용하여 로그인할 수 있습니다. 자세한 내용은 로 이동하십시오 "[Cloud Central 도움말 센터](#)" 그런 다음 \* Cloud Central 로그인 옵션 \* 을 클릭합니다.

#### 단계

1. 웹 브라우저를 열고 로 이동합니다 <https://cloudmanager.netapp.com>.
2. NetApp Cloud Central 자격 증명을 입력하거나 \* NetApp \* 으로 로그인 \* 을 클릭하고 NetApp Support 사이트 자격 증명을 입력하여 로그인합니다.

Cloud Central에 등록할 때 사용한 옵션을 선택해야 합니다.

- 전자 메일 및 암호를 입력하여 등록한 경우 로그인할 때마다 해당 자격 증명을 입력해야 합니다.
- NetApp Support 사이트 자격 증명으로 로그인하여 등록한 경우 매번 해당 로그인 옵션을 사용해야 합니다.

## Log In to NetApp Cloud Central

Don't have an account yet? [Sign Up](#)

Email

Password

LOG IN

[Forgot password?](#)

Or

Have a registered NetApp Support Site account?

Log In with NetApp

이제 로그인했으므로 Cloud Manager를 사용하여 하이브리드 멀티 클라우드 인프라를 관리할 수 있습니다.

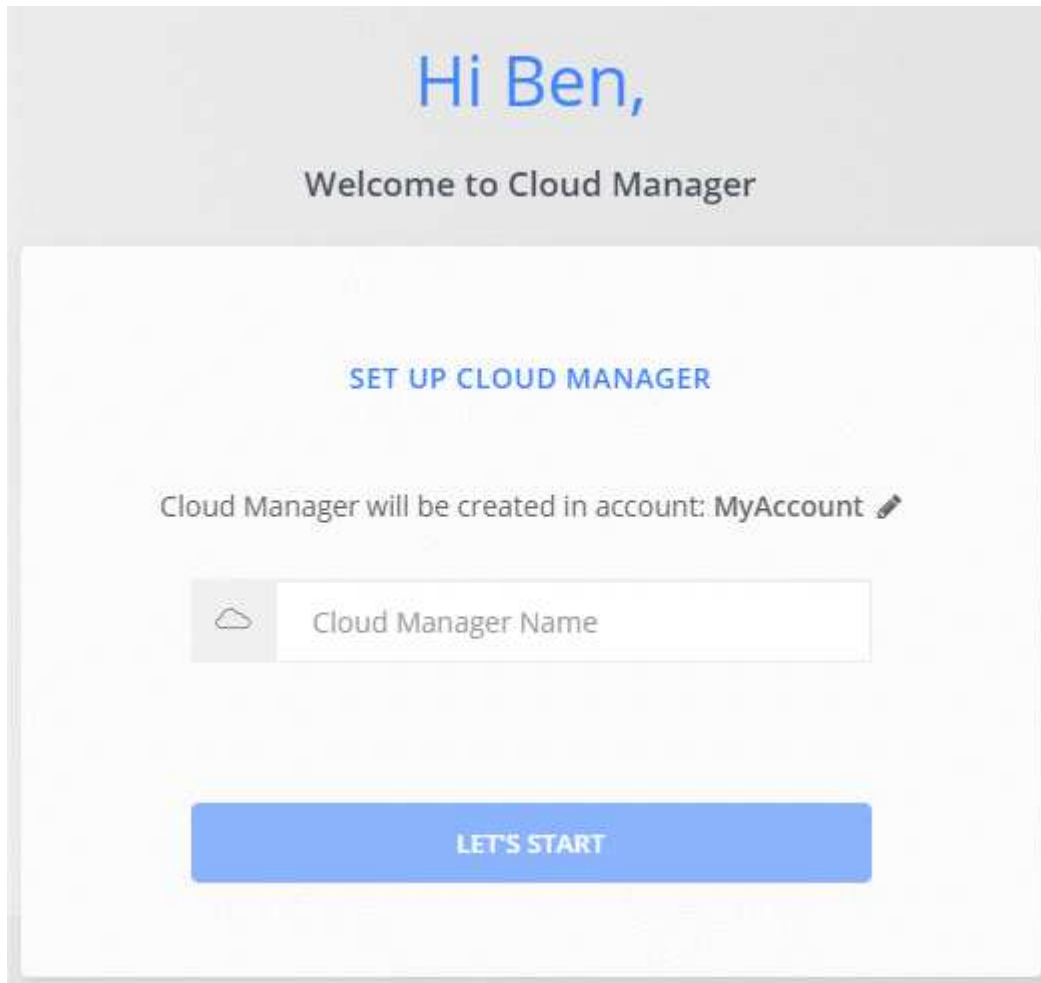
# NetApp 계정 설정

## NetApp 계정 에 대해 알아보십시오

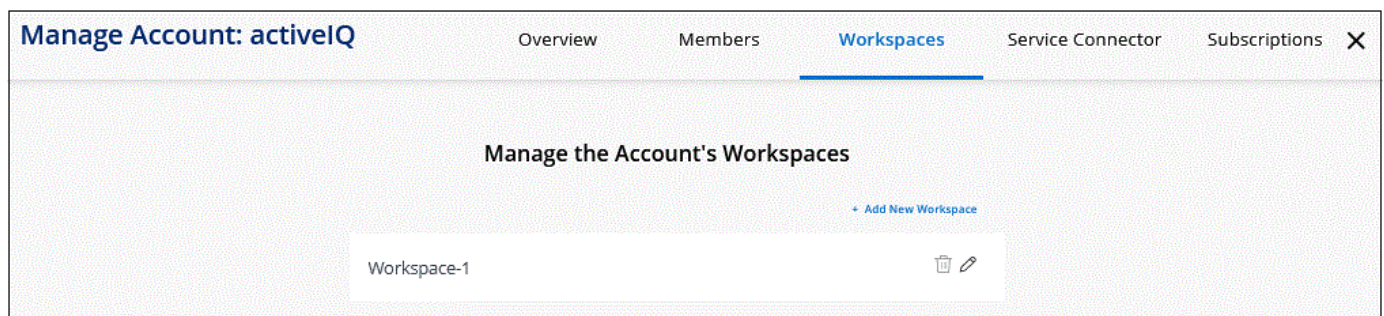
a\_NetApp account\_는 멀티 테넌시를 제공하고 Cloud Manager 내에서 격리된 작업 공간에 사용자와 리소스를 구성할 수 있도록 합니다.

예를 들어, 여러 사용자가 \_worksaces\_라는 격리된 환경에서 Cloud Volumes ONTAP 시스템을 배포하고 관리할 수 있습니다. 이러한 작업 영역은 다른 사용자가 공유하지 않는 한 표시되지 않습니다.

Cloud Manager에 처음 액세스할 때 NetApp 계정을 선택하거나 생성하라는 메시지가 표시됩니다.



그런 다음 계정 관리자는 사용자(구성원), 작업 영역, 커넥터 및 구독을 관리하여 이 계정의 설정을 수정할 수 있습니다.



단계별 지침은 을 참조하십시오 ["NetApp 계정 설정"](#).

## 계정 설정

Cloud Manager의 계정 관리 위젯을 사용하면 계정 관리자가 NetApp 계정을 관리할 수 있습니다. 방금 계정을 만든 경우 처음부터 다시 시작할 수 있습니다. 그러나 이미 계정을 설정한 경우에는 계정과 연결된 사용자, 작업 영역, 커넥터 및 구독이 `_ALL_`으로 표시됩니다.

## 개요

개요 페이지에는 계정 이름과 계정 ID가 표시됩니다. 일부 서비스를 등록할 때 계정 ID를 제공해야 할 수 있습니다. 이 페이지에는 몇 가지 Cloud Manager 구성 옵션도 포함되어 있습니다.

## 구성원

회원은 NetApp 계정과 연결된 NetApp Cloud Central 사용자입니다. 사용자를 계정과 연결하고 해당 계정에서 하나 이상의 작업 공간을 만들면 해당 사용자가 Cloud Manager에서 작업 환경을 만들고 관리할 수 있습니다.

사용자를 연결할 때 역할을 할당합니다.

- **계정 관리자:** Cloud Manager에서 모든 작업을 수행할 수 있습니다.
- **Workspace 관리자:** 할당된 작업 영역에서 자원을 작성하고 관리할 수 있습니다.
- **Compliance Viewer:** Cloud Data Sense 준수 정보만 보고 액세스 권한이 있는 시스템에 대한 보고서를 생성할 수 있습니다.
- **SnapCenter 관리자:** SnapCenter 서비스를 사용하여 애플리케이션 적합성이 보장되는 백업을 생성하고 이러한 백업을 사용하여 데이터를 복구할 수 있습니다. \_ 이 서비스는 현재 베타 상태입니다. \_

["이러한 역할에 대해 자세히 알아보십시오"](#).

## 작업 공간

Cloud Manager에서 작업 공간은 다른 작업 환경과 \_ 작업 환경 \_ 의 수를 분리합니다. 계정 관리자가 해당 작업 영역에 관리자를 연결해야만 작업 영역 관리자가 작업 영역의 작업 환경에 액세스할 수 있습니다.

작업 환경은 스토리지 시스템을 나타냅니다.

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

["작업 영역을 추가하는 방법에 대해 알아봅니다"](#).

## 커넥터

Connector를 사용하면 Cloud Manager에서 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있습니다. Connector는 클라우드 공급업체에 구축하는 가상 머신 인스턴스 또는 구성된 온프레미스 호스트에서 실행됩니다.

Connector를 두 개 이상의 NetApp 클라우드 데이터 서비스와 함께 사용할 수 있습니다. 예를 들어, Connector for Cloud Manager가 이미 있는 경우 Cloud Tiering 서비스를 설정할 때 선택할 수 있습니다.



"커넥터에 대해 자세히 알아보십시오".

## 구독

선택한 계정과 연결된 NetApp 구독입니다.

클라우드 공급자의 마켓플레이스에서 Cloud Manager를 구독하면 Cloud Central로 리디렉션되어 구독을 저장하고 특정 계정에 연결해야 합니다.

구독한 후에는 계정 관리 위젯에서 각 구독을 사용할 수 있습니다. 현재 보고 있는 계정과 연결된 구독만 표시됩니다.

구독의 이름을 바꾸고 하나 이상의 계정에서 구독을 연결 해제할 수 있습니다.

예를 들어, 두 개의 계정이 있고 각각 별도의 구독을 통해 비용이 청구된다고 가정해 보겠습니다. Cloud Volume ONTAP 작업 환경을 생성할 때 해당 계정의 사용자가 실수로 잘못된 구독을 선택하지 않도록 계정 중 하나에서 구독을 연결 해제할 수 있습니다.

"서브스크립션 관리 방법에 대해 알아보십시오".

## 예

다음 예에서는 계정을 설정하는 방법을 보여 줍니다.

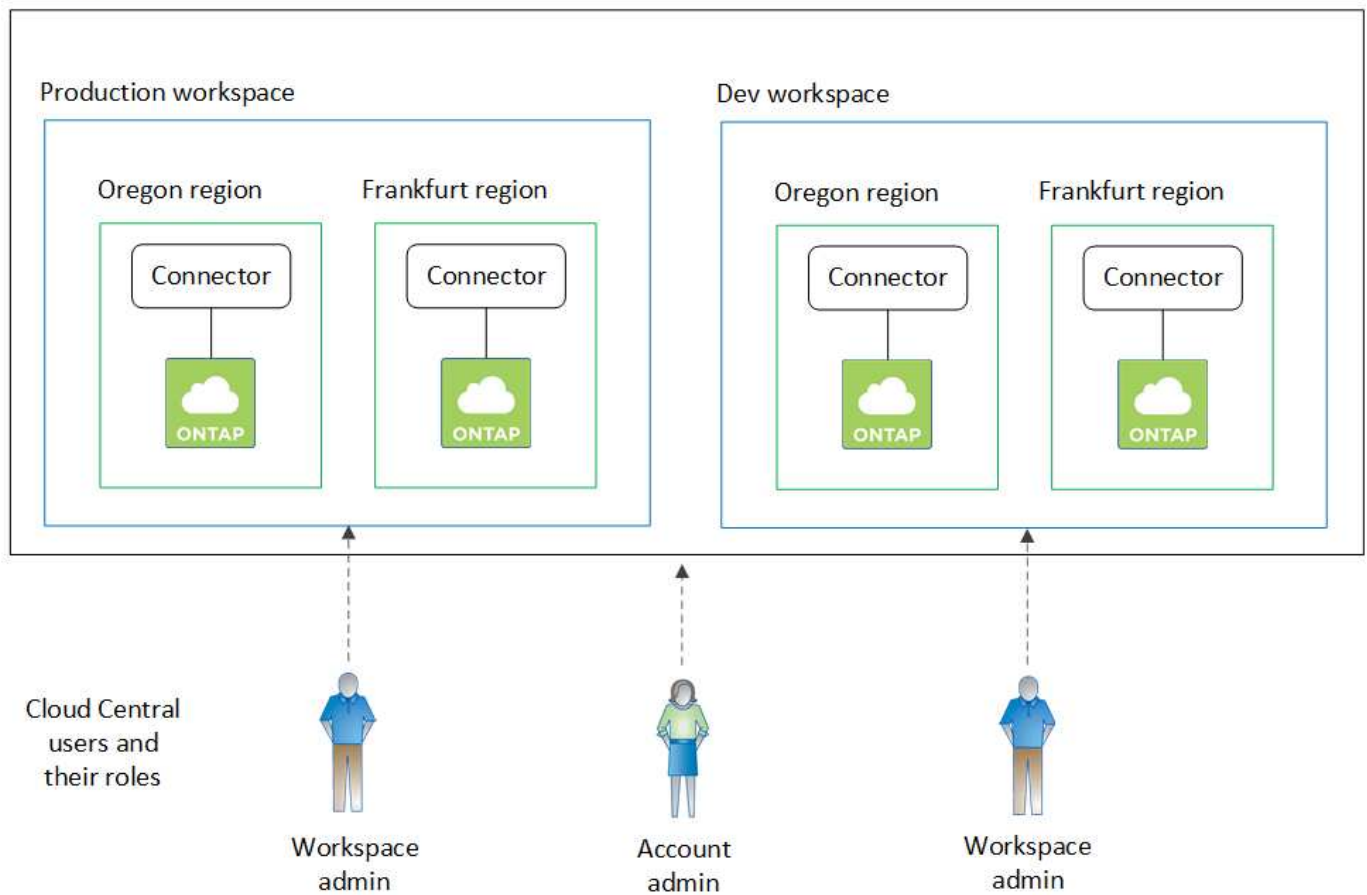


이어지는 두 예제 이미지 모두에서 Connector와 Cloud Volumes ONTAP 시스템은 실제로 클라우드 공급자에서 실행 중인 \_ in \_ 에 상주하지 않습니다. 각 구성 요소 간의 관계를 개념적으로 나타낸 것입니다.

## 예 1

다음 예제에서는 두 개의 작업 영역을 사용하여 격리된 환경을 만드는 계정을 보여 줍니다. 첫 번째 작업 공간은 운영 환경이고 두 번째는 개발 환경입니다.

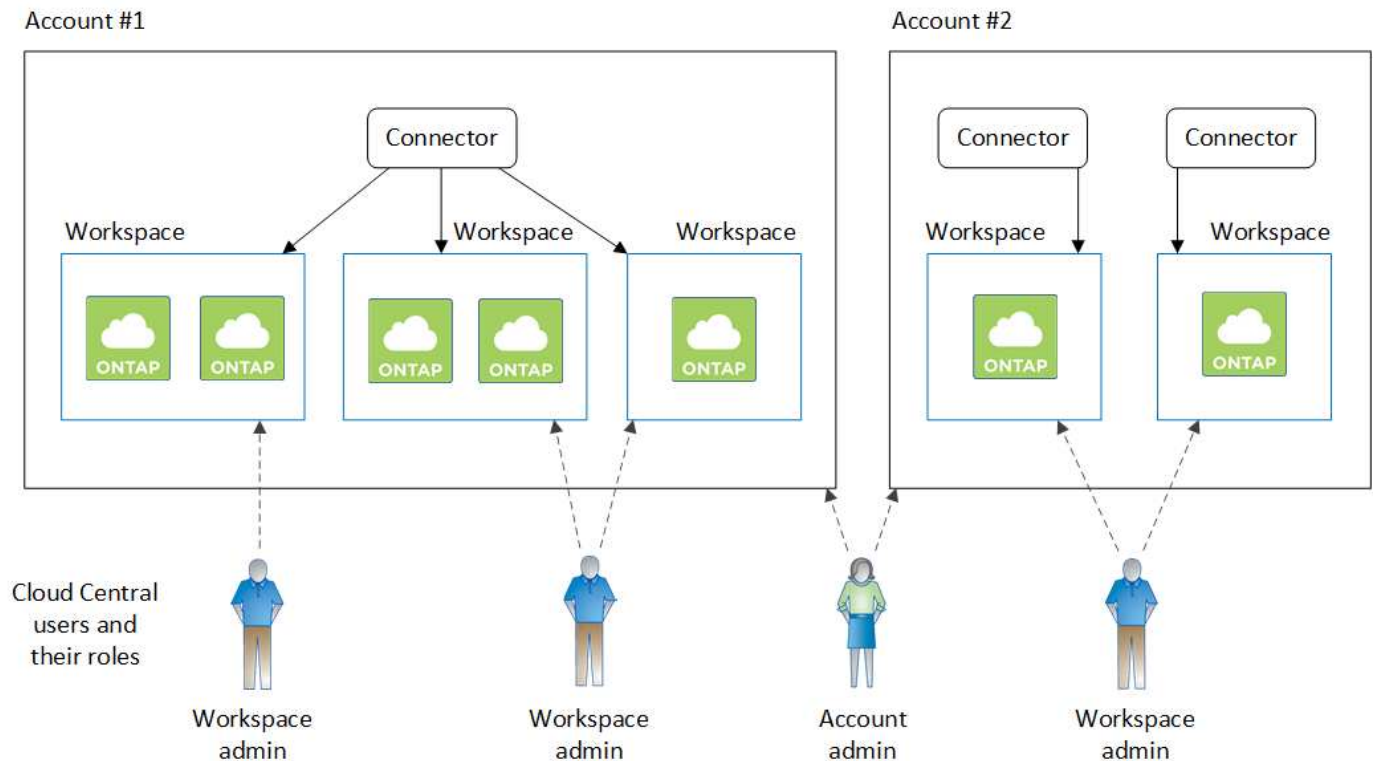
## Account



### 예 2

다음 예에서는 두 개의 개별 NetApp 계정을 사용하여 가장 높은 수준의 멀티 테넌시를 보여 줍니다. 예를 들어, 서비스 공급자는 하나의 계정에서 Cloud Manager를 사용하여 고객에게 서비스를 제공하는 동시에 다른 계정을 사용하여 부서 중 하나의 재해 복구를 제공할 수 있습니다.

계정 2에는 별도의 커넥터가 2개 포함되어 있습니다. 시스템이 다른 지역이나 별도의 클라우드 공급자에 있는 경우 이러한 문제가 발생할 수 있습니다.



## NetApp 계정의 작업 공간과 사용자를 설정합니다

Cloud Manager에 처음 로그인하면 **\_NetApp 계정\_**을 생성하라는 메시지가 표시됩니다. 이 계정은 다중 테넌시를 제공하며 사용자가 **isolated\_workspaces\_**에서 사용자 및 리소스를 구성할 수 있도록 합니다.

["NetApp 계정의 작동 방식에 대해 자세히 알아보십시오"](#).

사용자가 Cloud Manager에 액세스하고 작업 공간에서 작업 환경에 액세스할 수 있도록 NetApp 계정을 설정합니다. 단일 사용자를 추가하거나 여러 사용자 및 작업 영역을 추가하기만 하면 됩니다.

작업 영역을 추가합니다

Cloud Manager의 작업 영역을 사용하면 작업 환경 집합을 다른 작업 환경 및 다른 사용자와 격리할 수 있습니다. 예를 들어 두 개의 작업 영역을 만들고 각 작업 영역에 개별 사용자를 연결할 수 있습니다.

단계

1. 의 상단에서 **"클라우드 관리자"**에서 \* 계정 \* 드롭다운을 클릭합니다.



2. 현재 선택한 계정 옆에 있는 \* 계정 관리 \* 를 클릭합니다.



3. 작업 공간 \* 을 클릭합니다.
4. 새 작업 공간 추가 \* 를 클릭합니다.
5. 작업 영역의 이름을 입력하고 \* 추가 \* 를 클릭합니다.

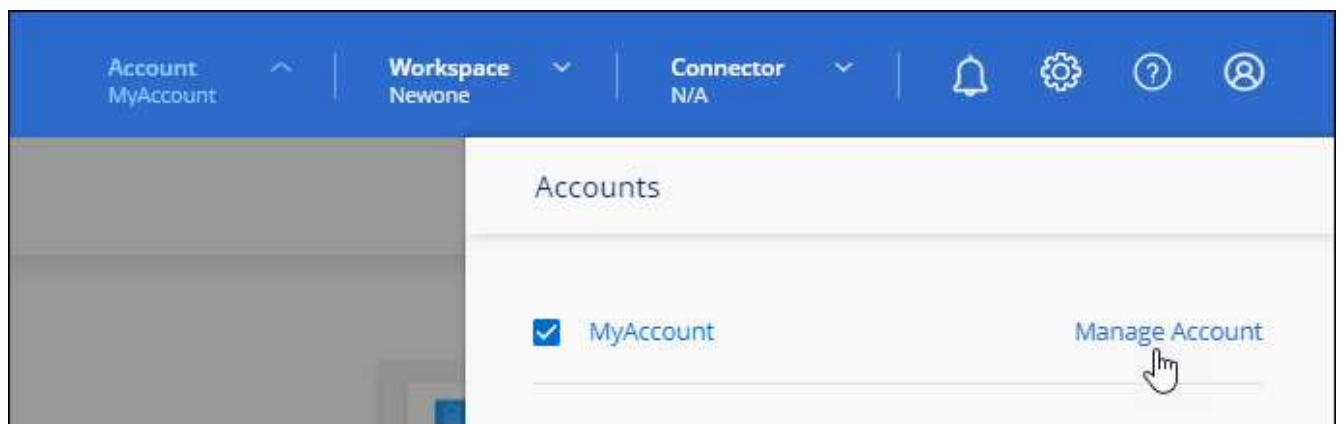
작업 영역 관리자가 이 작업 영역에 액세스해야 하는 경우 사용자를 연결해야 합니다. 또한 Workspace 관리자가 해당 커넥터를 사용할 수 있도록 작업 영역에 커넥터를 연결해야 합니다.

#### 사용자 추가

Cloud Central 사용자를 NetApp 계정과 연결하여 Cloud Manager에서 작업 환경을 만들고 관리할 수 있습니다.

#### 단계

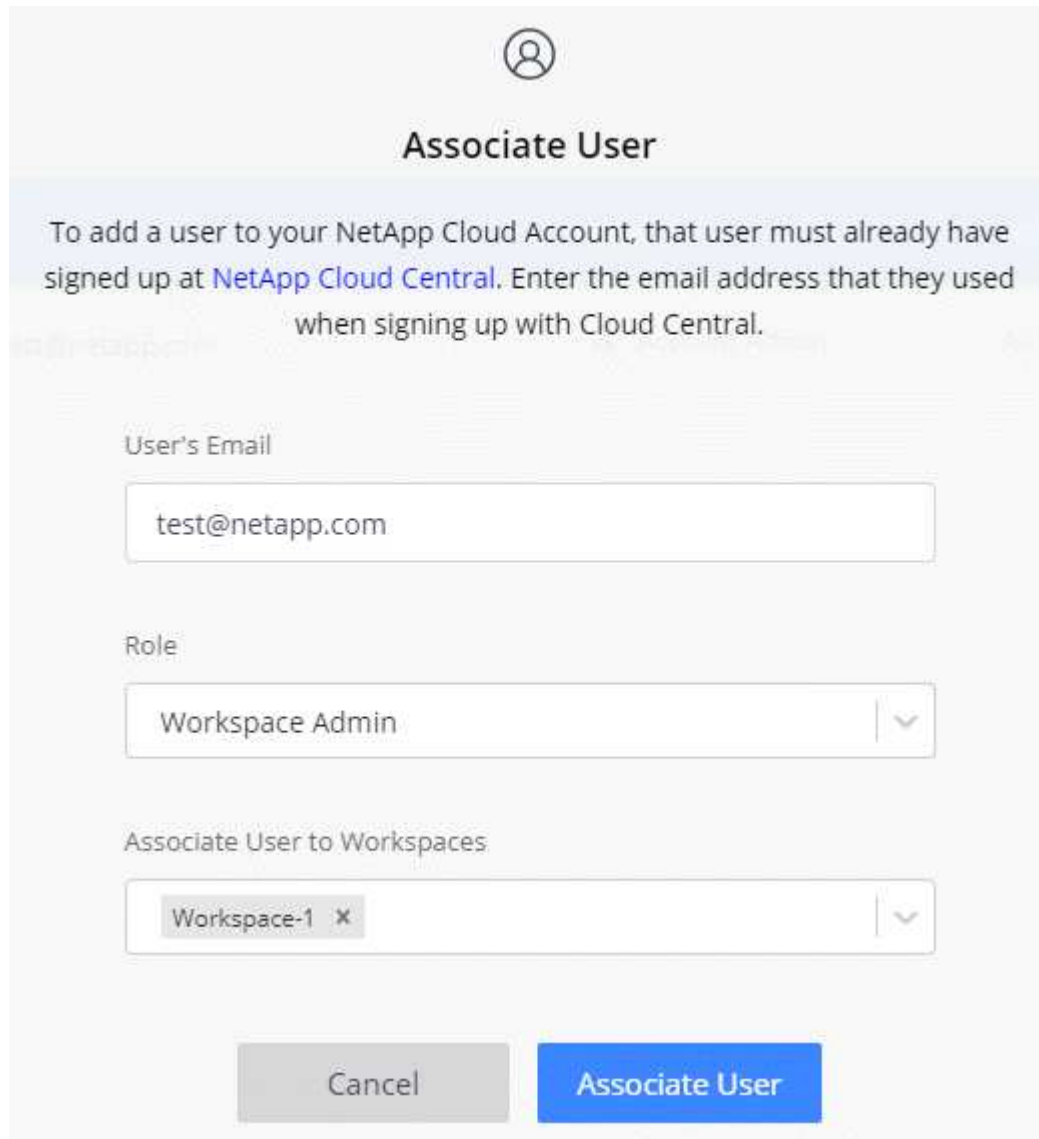
1. 사용자가 아직 이 작업을 수행하지 않은 경우 사용자에게 로 이동하라고 요청합니다 ["NetApp Cloud Central에서"](#) 을 클릭합니다.
2. 의 상단에서 ["클라우드 관리자"](#)에서 \* 계정 \* 드롭다운을 클릭하고 \* 계정 관리 \* 를 클릭합니다.



3. 구성원 탭에서 \* 사용자 연결 \* 을 클릭합니다.
4. 사용자의 이메일 주소를 입력하고 사용자의 역할을 선택합니다.
  - \* 계정 관리자 \*: Cloud Manager에서 모든 작업을 수행할 수 있습니다.
  - \* Workspace Admin \*: 할당된 작업 영역에서 리소스를 만들고 관리할 수 있습니다.
  - \* Compliance Viewer \*: Cloud Data Sense 거버넌스 및 규정 준수 정보만 볼 수 있고 액세스 권한이 있는 작업 공간에 대한 보고서를 생성할 수 있습니다.

- \* SnapCenter 관리자 \*: SnapCenter 서비스를 사용하여 애플리케이션 정합성이 보장되는 백업을 생성하고 이러한 백업을 사용하여 데이터를 복원할 수 있습니다. 이 서비스는 현재 베타 버전입니다.

5. 계정 관리자 이외의 계정을 선택한 경우 해당 사용자와 연결할 작업 영역을 하나 이상 선택합니다.



The image shows a dialog box titled "Associate User" with a user icon at the top. Below the title, there is a light blue informational box containing the text: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." Below this, there are three input fields: "User's Email" with the value "test@netapp.com", "Role" with a dropdown menu showing "Workspace Admin", and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close button (X). At the bottom, there are two buttons: "Cancel" and "Associate User".

6. Associate \* 를 클릭합니다.

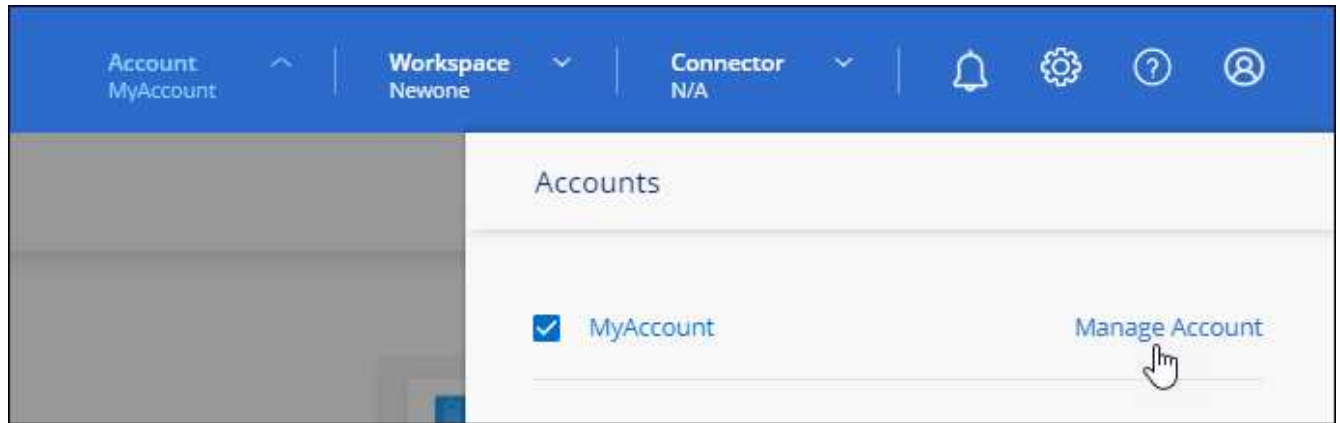
사용자는 NetApp Cloud Central에서 "Account Association"이라는 제목의 이메일을 받아야 합니다. 이 이메일에는 Cloud Manager에 액세스하는 데 필요한 정보가 포함되어 있습니다.

#### 작업 영역 관리자와 작업 영역 연결

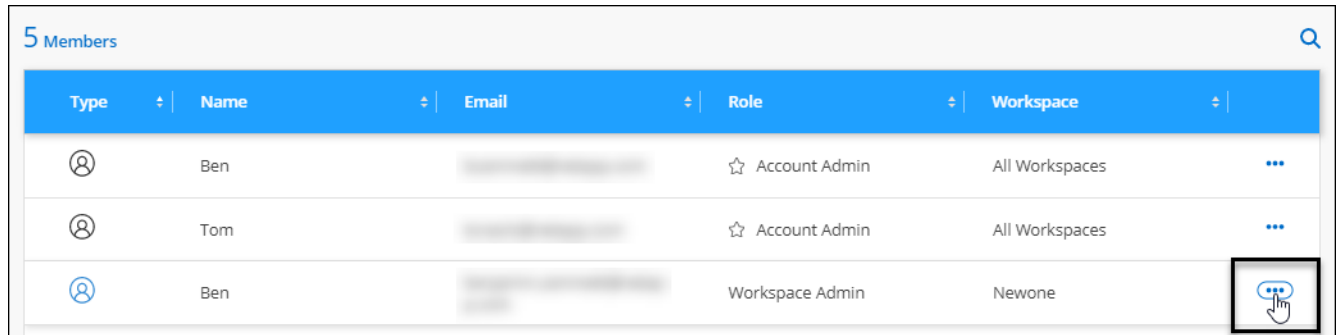
언제든지 Workspace Admins를 추가 작업 영역에 연결할 수 있습니다. 사용자를 연결하면 해당 작업 영역에서 작업 환경을 만들고 볼 수 있습니다.

#### 단계

1. Cloud Manager 상단에서 \* 계정 \* 드롭다운을 클릭하고 \* 계정 관리 \* 를 클릭합니다.



2. 구성원 탭의 행에 있는 해당 사용자에게 해당하는 작업 메뉴를 클릭합니다.



3. 작업 영역 관리 \* 를 클릭합니다.

4. 하나 이상의 작업 공간을 선택하고 \* 적용 \* 을 클릭합니다.

Connector가 작업 공간에도 연결되어 있는 한 이제 사용자는 Cloud Manager에서 이러한 작업 영역에 액세스할 수 있습니다.

작업 영역에 커넥터를 연결합니다

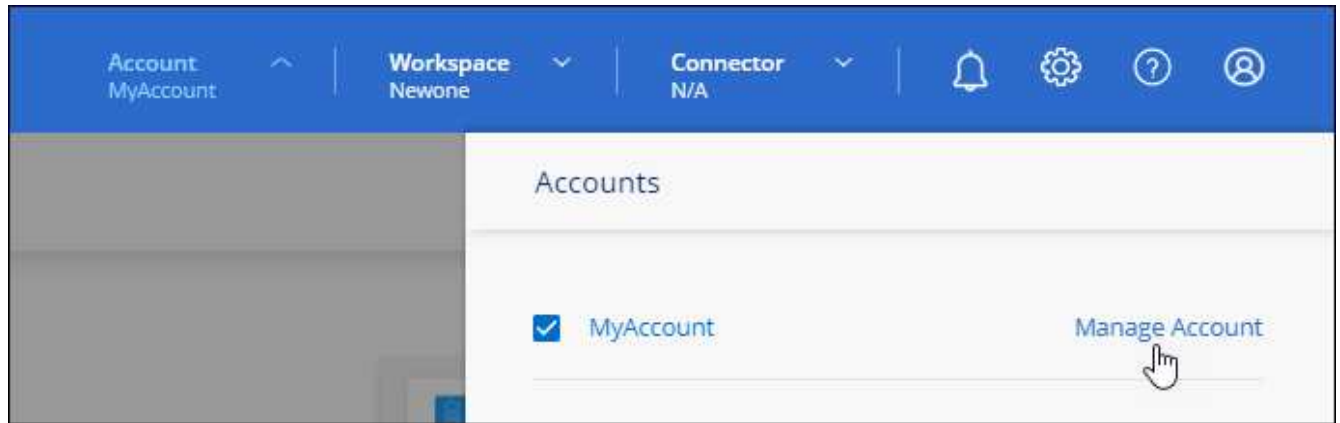
작업 영역 관리자가 이러한 커넥터를 사용하여 Cloud Volumes ONTAP 시스템을 만들 수 있도록 작업 영역과 커넥터를 연결해야 합니다.

Account Admins만 있는 경우에는 Connector를 작업 영역과 연결할 필요가 없습니다. 계정 관리자는 기본적으로 Cloud Manager의 모든 작업 영역에 액세스할 수 있습니다.

"사용자, 작업 영역 및 커넥터에 대해 자세히 알아보십시오".

단계

1. Cloud Manager 상단에서 \* 계정 \* 드롭다운을 클릭하고 \* 계정 관리 \* 를 클릭합니다.



2. 커넥터 \* 를 클릭합니다.
3. 연결하려는 Connector의 \* 작업 영역 관리 \* 를 클릭합니다.
4. 하나 이상의 작업 공간을 선택하고 \* 적용 \* 을 클릭합니다.

이제 Workspace 관리자가 이러한 커넥터를 사용하여 Cloud Volumes ONTAP 시스템을 생성할 수 있습니다.

다음 단계

이제 계정을 설정했으므로 사용자 제거, 작업 영역, 커넥터 및 구독을 관리하여 언제든지 계정을 관리할 수 있습니다. ["계정을 관리하는 방법에 대해 알아보십시오"](#).

## 커넥터를 설정합니다

커넥터에 대해 자세히 알아보십시오

대부분의 경우 계정 관리자는 클라우드 또는 온-프레미스 네트워크에 \_Connector\_를 배포해야 합니다. Connector는 Cloud Manager의 일상적인 사용에 있어 중요한 구성요소입니다. Connector를 사용하면 Cloud Manager에서 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있습니다.

커넥터가 필요한 경우

Connector는 Cloud Manager의 다양한 기능과 서비스를 사용하는 데 필요합니다.

서비스

- ONTAP용 Amazon FSx 관리 기능
- Amazon S3 검색
- Azure Blob 검색
- 클라우드 백업
- 클라우드 데이터 감지
- 클라우드 계층화
- Cloud Volumes ONTAP

- 글로벌 파일 캐시
- Google Cloud Storage 검색
- Kubernetes 클러스터
- 모니터링
- 온프레미스 ONTAP 클러스터

커넥터는 *\*NOT\** 다음 서비스에 필요합니다.

- Active IQ 디지털 자문업체
- ONTAP 작업 환경을 위한 Amazon FSx 커넥터가 작업 환경을 생성할 필요가 없는 경우, 볼륨 생성 및 관리, 데이터 복제, ONTAP용 FSx를 데이터 감지 및 Cloud Sync와 같은 NetApp 클라우드 서비스와 통합해야 합니다.
- Azure NetApp Files

Azure NetApp Files를 설정하고 관리하는 데 커넥터가 필요하지 않지만 클라우드 데이터 센스를 사용하여 Azure NetApp Files 데이터를 스캔하려면 커넥터가 필요합니다.

- Google Cloud용 Cloud Volumes Service
- Cloud Sync

#### 디지털 지갑

거의 모든 경우에 Connector 없이 디지털 지갑에 라이선스를 추가할 수 있습니다.

디지털 지갑에 라이선스를 추가하는 데 커넥터가 필요한 유일한 시간은 Cloud Volumes ONTAP\_node-based\_licenses입니다. 이 경우 Cloud Volumes ONTAP 시스템에 설치된 라이선스에서 데이터를 가져왔기 때문에 커넥터가 필요합니다.

#### 지원되는 위치

커넥터는 다음 위치에서 지원됩니다.

- Amazon Web Services에서 직접 지원합니다
- Microsoft Azure를 참조하십시오
- Google 클라우드
- 온프레미스
- 인터넷 접속 없이 구내

#### Azure 배포에 대한 참고 사항

Azure에 커넥터를 배포하는 경우, 커넥터가 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 영역에 배포되거나 에 배포되어야 합니다. ["Azure 지역 쌍"](#) Cloud Volumes ONTAP 시스템의 경우 이 요구 사항은 Cloud Volumes ONTAP와 연결된 스토리지 계층 간에 Azure 전용 링크 연결이 사용되도록 합니다. ["Cloud Volumes ONTAP에서 Azure 프라이빗 링크를 사용하는 방법에 대해 알아보십시오"](#).

#### Google Cloud 배포에 대한 참고 사항

Google Cloud에서 Cloud Volumes ONTAP 시스템을 만들려면 Google Cloud에서도 실행되는 커넥터가 있어야



합니다. AWS, Azure 또는 온프레미스에서 실행되는 Connector를 사용할 수 없습니다.

커넥터는 계속 작동 중이어야 합니다

커넥터는 항상 작동 상태를 유지해야 합니다. 이는 여러분이 제공하는 서비스의 지속적인 상태 및 운영에 중요합니다.

예를 들어, Connector는 Cloud Volumes ONTAP의 상태 및 작동에 있어 핵심 구성 요소입니다. 커넥터 전원이 꺼져 있는 경우 노드 기반 라이선스를 가진 Cloud Volumes ONTAP PAYGO 시스템은 커넥터 통신이 14일 이상 끊긴 후 종료됩니다.

## 커넥터 작성 방법

작업 영역 관리자가 Cloud Volumes ONTAP 작업 환경을 만들고 위에 나열된 다른 서비스를 사용하려면 계정 관리자가 커넥터를 만들어야 합니다. 관리자는 다음과 같은 여러 가지 방법으로 커넥터를 만들 수 있습니다.

- Cloud Manager에서 직접(권장)
  - ["AWS에서 생성"](#)
  - ["Azure에서 생성"](#)
  - ["GCP에서 생성"](#)
- 자체 Linux 호스트에 소프트웨어를 수동으로 설치합니다
  - ["인터넷에 액세스할 수 있는 호스트"](#)
  - ["인터넷에 액세스할 수 없는 온프레미스 호스트입니다"](#)
- 더 높은 경쟁력을 강화할 수 있습니다
  - ["AWS 마켓플레이스 를 참조하십시오"](#)
  - ["Azure 마켓플레이스 를 참조하십시오"](#)

작업을 완료하는 데 필요한 경우 Cloud Manager에서 커넥터를 생성하라는 메시지가 표시됩니다.

## 권한

Connector를 만들려면 특정 권한이 필요하며 Connector 인스턴스 자체에 다른 권한 집합이 필요합니다.

### Connector를 만들 수 있는 권한

Cloud Manager에서 Connector를 생성하는 사용자는 선택한 클라우드 공급자에 인스턴스를 배포하기 위한 특정 권한이 필요합니다. Cloud Manager는 Connector를 생성할 때 권한 요구 사항을 상기시킵니다.

- ["필요한 AWS 권한을 확인합니다"](#)
- ["필요한 Azure 권한을 봅니다"](#)
- ["필요한 Google Cloud 권한을 봅니다"](#)

### Connector 인스턴스에 대한 권한

Connector는 사용자를 대신하여 작업을 수행하려면 특정 클라우드 공급자 권한이 필요합니다. 예를 들어, Cloud Volumes ONTAP를 구축하고 관리하는 경우를 들 수 있습니다.

Cloud Manager에서 직접 Connector를 생성하면 Cloud Manager에서 필요한 권한이 있는 Connector가 생성됩니다.

당신이 해야 할 일은 아무것도 없습니다.

AWS Marketplace, Azure Marketplace 또는 소프트웨어를 수동으로 설치하여 직접 Connector를 생성하는 경우 올바른 권한이 있는지 확인해야 합니다.

- ["Connector에서 AWS 권한을 사용하는 방법에 대해 알아보십시오"](#)
- ["Connector에서 Azure 권한을 사용하는 방법에 대해 알아보십시오"](#)
- ["Connector가 Google Cloud 권한을 사용하는 방법에 대해 알아보십시오"](#)

## 커넥터 업그레이드

일반적으로 매월 커넥터 소프트웨어를 업데이트하여 새로운 기능을 소개하고 안정성 향상을 제공합니다. Cloud Manager 플랫폼의 대부분의 서비스와 기능은 SaaS 기반 소프트웨어를 통해 제공되지만, Connector의 버전에 따라 몇 가지 기능이 달라집니다. 여기에는 Cloud Volumes ONTAP 관리, 온프레미스 ONTAP 클러스터 관리, 설정 및 도움말이 포함됩니다.

Connector는 소프트웨어가 있는 한 소프트웨어를 최신 버전으로 자동 업데이트합니다 ["아웃바운드 인터넷 액세스"](#) 를 클릭하여 소프트웨어 업데이트를 얻습니다.

## 커넥터당 작업 환경 수

Connector는 Cloud Manager에서 여러 작업 환경을 관리할 수 있습니다. 단일 커넥터가 관리해야 하는 최대 작업 환경 수는 서로 다릅니다. 운영 환경의 유형, 볼륨 수, 관리되는 용량 및 사용자 수에 따라 달라집니다.

대규모 구축이 있는 경우 NetApp 담당자와 협력하여 환경을 사이징합니다. 도중에 문제가 발생하는 경우 제품 내 채팅을 통해 문의해 주십시오.

## 여러 커넥터를 사용하는 경우

경우에 따라 하나의 커넥터만 필요할 수 있지만 둘 이상의 커넥터가 필요할 수 있습니다.

다음은 몇 가지 예입니다.

- 멀티 클라우드 환경(AWS 및 Azure)을 사용 중이라면 AWS에, Azure에 각각 Connector를 설치하고, 각 는 이러한 환경에서 실행되는 Cloud Volumes ONTAP 시스템을 관리합니다.
- 서비스 공급자는 NetApp 계정 하나를 사용하여 고객에게 서비스를 제공하는 한편, 다른 계정을 사용하여 부서 중 하나에 대해 재해 복구를 제공할 수 있습니다. 각 계정에는 별도의 커넥터가 있습니다.

## 동일한 작업 환경에서 여러 커넥터 사용

재해 복구를 위해 여러 커넥터가 있는 작업 환경을 동시에 관리할 수 있습니다. 하나의 커넥터가 다운되면 다른 커넥터로 전환하여 작업 환경을 즉시 관리할 수 있습니다.

이 구성을 설정하려면 다음을 수행하십시오.

1. ["다른 커넥터로 전환합니다"](#)
2. 기존 작업 환경을 파악합니다.
  - ["기존 Cloud Volumes ONTAP 시스템을 Cloud Manager에 추가합니다"](#)
  - ["ONTAP 클러스터에 대해 알아보십시오"](#)

### 3. 를 설정합니다 "용량 관리 모드"

주 커넥터만 \* 자동 모드 \* 로 설정해야 합니다. DR 목적으로 다른 커넥터로 전환하면 필요에 따라 용량 관리 모드를 변경할 수 있습니다.

#### 커넥터 간 전환 시기

첫 번째 Connector를 만들면 Cloud Manager는 사용자가 생성한 각 추가 작업 환경에 대해 해당 Connector를 자동으로 사용합니다. 추가 커넥터를 만든 후에는 각 Connector에 해당하는 작업 환경을 보기 위해 커넥터 사이를 전환해야 합니다.

"커넥터 간 전환 방법에 대해 알아보십시오".

#### 로컬 사용자 인터페이스입니다

에서 거의 모든 작업을 수행해야 합니다 "SaaS 사용자 인터페이스"로컬 사용자 인터페이스는 Connector에서 계속 사용할 수 있습니다. 이 인터페이스는 인터넷에 액세스할 수 없는 환경에 Connector를 설치하고 SaaS 인터페이스 대신 Connector 자체에서 수행해야 하는 몇 가지 작업에 필요합니다.

- "프록시 서버 설정"
- 패치 설치(일반적으로 NetApp 직원과 협력하여 패치 설치)
- AutoSupport 메시지 다운로드(일반적으로 문제가 있을 때 NetApp 담당자가 지시)

"로컬 UI에 액세스하는 방법을 알아보십시오".

#### 커넥터에 대한 네트워킹을 설정합니다

Connector가 공용 클라우드 환경 내에서 리소스 및 프로세스를 관리할 수 있도록 네트워킹을 설정합니다. 가장 중요한 단계는 다양한 엔드포인트에 대한 아웃바운드 인터넷 액세스를 보장하는 것입니다.

이 페이지의 정보는 커넥터가 아웃바운드 인터넷 액세스를 가지고 있는 일반적인 배포를 위한 것입니다.



네트워크에서 인터넷에 대한 모든 통신에 프록시 서버를 사용하는 경우 설정 페이지에서 프록시 서버를 지정할 수 있습니다. 을 참조하십시오 "프록시 서버를 사용하도록 Connector 구성".

#### 대상 네트워크에 연결

Connector를 사용하려면 만들고 있는 작업 환경의 유형과 활성화할 서비스에 대한 네트워크 연결이 필요합니다.

예를 들어 회사 네트워크에 커넥터를 설치하는 경우 Cloud Volumes ONTAP를 실행하는 VPC 또는 VNET에 대한 VPN 연결을 설정해야 합니다.

#### 172 범위의 IP 주소와 충돌할 수 있습니다

Cloud Manager는 172.17.0.0/16 및 172.18.0.0/16 범위의 IP 주소를 가진 두 개의 인터페이스로 커넥터를 배포합니다.

네트워크에 이러한 범위 중 하나로 구성된 서브넷이 있는 경우 Cloud Manager에서 연결 장애가 발생할 수 있습니다.

예를 들어, Cloud Manager에서 온프레미스 ONTAP 클러스터를 검색하지 못할 수 있습니다.

기술 자료 문서를 참조하십시오 "[Cloud Manager Connector IP가 기존 네트워크와 충돌합니다](#)" 커넥터 인터페이스의 IP 주소를 변경하는 방법에 대한 지침은 을 참조하십시오.

## 아웃바운드 인터넷 액세스

커넥터에서 아웃바운드 인터넷 액세스가 필요합니다.

엔드포인트에서 퍼블릭 클라우드 환경의 리소스를 관리합니다

Connector를 사용하려면 공용 클라우드 환경 내의 리소스와 프로세스를 관리하기 위한 아웃바운드 인터넷 액세스가 필요합니다.

| 엔드포인트  | 목적   |
|--|--|
| <a href="https://support.netapp.com">https://support.netapp.com</a> 으로 문의하십시오  | 라이선스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다. |
| <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a> 으로 문의하십시오  | Cloud Manager 내에서 SaaS 기능 및 서비스를 제공합니다.          |
| <a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a><br><a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a> 으로 문의하십시오 | Connector 및 해당 Docker 구성 요소를 업그레이드합니다.           |

**Linux** 호스트에 커넥터를 설치하기 위한 엔드포인트

자신의 Linux 호스트에 Connector 소프트웨어를 수동으로 설치할 수 있습니다. 이렇게 하면 설치 프로세스 중에 Connector의 설치 관리자가 다음 URL에 액세스해야 합니다.

- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm> 으로 문의하십시오
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip> 으로 문의하십시오
- [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net) 또는 <https://hub.docker.com> 으로 문의하십시오

설치 중에 호스트가 운영 체제 패키지를 업데이트하려고 할 수 있습니다. 호스트는 이러한 OS 패키지의 서로 다른 미러링 사이트에 연결할 수 있습니다.

## 포트 및 보안 그룹

커넥터 를 시작하지 않으면 커넥터로 들어오는 트래픽이 없습니다. HTTP 및 HTTPS는 에 대한 액세스를 제공합니다 "[로컬 UI](#)" 이는 드문 경우지만 사용할 수 있습니다. SSH는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.

## AWS의 커넥터 규칙

Connector의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

## 인바운드 규칙

| 프로토콜       | 포트   | 목적   |
|------------|------|--|
| SSH를 클릭합니다 | 22   | 커넥터 호스트에 대한 SSH 액세스를 제공합니다   |
| HTTP       | 80   | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다                                 |
| HTTPS      | 443  | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스에 대한 HTTPS 액세스 및 Cloud Data Sense 인스턴스의 연결을 제공합니다 |
| TCP        | 3128 | AWS 네트워크에서 NAT 또는 프록시를 사용하지 않는 경우 인터넷 액세스가 가능한 클라우드 데이터 감지 인스턴스를 제공합니다       |
| TCP        | 9060 | Cloud Data Sense를 활성화하고 사용할 수 있는 기능 제공(GovCloud 구축에만 필요)                     |

## 아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

## 기본 아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 프로토콜   | 포트 | 목적           |
|--------|----|--------------|
| 모든 TCP | 모두 | 모든 아웃바운드 트래픽 |
| 모든 UDP | 모두 | 모든 아웃바운드 트래픽 |

## 고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Connector의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스 IP 주소는 커넥터 호스트입니다.

| 서비스                  | 프로토콜  | 포트      | 목적지                           | 목적   |
|----------------------|-------|---------|-------------------------------|--|
| API 호출 및 AutoSupport | HTTPS | 443     | 아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF | API는 AWS 및 ONTAP, 클라우드 데이터 감지, 랜섬웨어 서비스 요청, AutoSupport 메시지를 NetApp에 전송합니다 |
| API 호출               | TCP   | 3000입니다 | ONTAP HA 중재자                  | ONTAP HA 중재인과의 커뮤니케이션  |
|                      | TCP   | 8088    | S3로 백업                        | API에서 S3로 백업을 호출합니다  |

| 서비스 | 프로토콜   | 포트 | 목적지 | 목적                                 |
|-----|--------|----|-----|------------------------------------|
| DNS | UDP입니다 | 53 | DNS | Cloud Manager에서 DNS Resolve에 사용됩니다 |

#### Azure의 커넥터 규칙

Connector의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

#### 인바운드 규칙

| 프로토콜       | 포트   | 목적   |
|------------|------|--|
| SSH를 클릭합니다 | 22   | 커넥터 호스트에 대한 SSH 액세스를 제공합니다   |
| HTTP       | 80   | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다                                 |
| HTTPS      | 443  | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스에 대한 HTTPS 액세스 및 Cloud Data Sense 인스턴스의 연결을 제공합니다 |
| TCP        | 9060 | Cloud Data Sense를 활성화하고 사용할 수 있는 기능 제공(정부 클라우드 구축에만 필요)                      |

#### 아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

#### 기본 아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 프로토콜   | 포트 | 목적           |
|--------|----|--------------|
| 모든 TCP | 모두 | 모든 아웃바운드 트래픽 |
| 모든 UDP | 모두 | 모든 아웃바운드 트래픽 |

#### 고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Connector의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스 IP 주소는 커넥터 호스트입니다.

| 서비스                  | 프로토콜   | 포트  | 목적지                           | 목적   |
|----------------------|--------|-----|-------------------------------|--|
| API 호출 및 AutoSupport | HTTPS  | 443 | 아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF | API는 AWS 및 ONTAP, 클라우드 데이터 감지, 랜섬웨어 서비스 요청, AutoSupport 메시지를 NetApp에 전송합니다 |
| DNS                  | UDP입니다 | 53  | DNS                           | Cloud Manager에서 DNS Resolve에 사용됩니다   |

#### GCP의 Connector에 대한 규칙입니다

Connector의 방화벽 규칙에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

#### 인바운드 규칙

| 프로토콜       | 포트  | 목적  |
|------------|-----|---|
| SSH를 클릭합니다 | 22  | 커넥터 호스트에 대한 SSH 액세스를 제공합니다                    |
| HTTP       | 80  | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다  |
| HTTPS      | 443 | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTPS 액세스를 제공합니다 |

#### 아웃바운드 규칙

Connector에 대해 미리 정의된 방화벽 규칙은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

#### 기본 아웃바운드 규칙

Connector에 대해 미리 정의된 방화벽 규칙에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 프로토콜   | 포트 | 목적           |
|--------|----|--------------|
| 모든 TCP | 모두 | 모든 아웃바운드 트래픽 |
| 모든 UDP | 모두 | 모든 아웃바운드 트래픽 |

#### 고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Connector의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스 IP 주소는 커넥터 호스트입니다.

| 서비스                  | 프로토콜   | 포트  | 목적지                           | 목적  |
|----------------------|--------|-----|-------------------------------|---|
| API 호출 및 AutoSupport | HTTPS  | 443 | 아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF | API는 GCP 및 ONTAP, 클라우드 데이터 센스, 랜섬웨어 서비스 요청 및 AutoSupport 메시지를 NetApp에 전송합니다 |
| DNS                  | UDP입니다 | 53  | DNS                           | Cloud Manager에서 DNS Resolve에 사용됩니다  |

#### 사내 커넥터용 포트

Connector는 온-프레미스 Linux 호스트에 수동으로 설치할 때 다음과 같은 `_inbound_ports`를 사용합니다.

이러한 인바운드 규칙은 인터넷 액세스 또는 인터넷 액세스 없이 설치된 온프레미스 커넥터의 두 배포 모델에 모두 적용됩니다.

| 프로토콜  | 포트  | 목적  |
|-------|-----|---|
| HTTP  | 80  | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다  |
| HTTPS | 443 | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTPS 액세스를 제공합니다 |

## Cloud Manager에서 AWS에 Connector를 생성합니다

대부분의 Cloud Manager 기능을 사용하려면 계정 관리자가 `_Connector_`를 배포해야 합니다. Connector를 사용하면 Cloud Manager에서 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있습니다. ["커넥터가 필요한 시기를 알아보십시오"](#).

이 페이지에서는 Cloud Manager에서 직접 AWS에 Connector를 생성하는 방법에 대해 설명합니다. ["커넥터를 배포하는 다른 방법에 대해 알아보십시오"](#).

이러한 단계는 계정 관리자 역할을 가진 사용자가 완료해야 합니다. 작업 영역 관리자가 연결선을 만들 수 없습니다.

### AWS 인증 설정

VPC에 Connector 인스턴스를 구축하려면 Cloud Manager에서 AWS를 인증해야 합니다. 다음 인증 방법 중 하나를 선택할 수 있습니다.

- Cloud Manager에서 필요한 권한이 있는 IAM 역할을 가정하도록 합니다
- 필요한 권한이 있는 IAM 사용자를 위해 AWS 액세스 키 및 비밀 키를 제공합니다

두 옵션 중 하나를 사용할 경우 먼저 필요한 권한이 포함된 IAM 정책을 생성하여 시작해야 합니다.

#### IAM 정책을 생성합니다

이 정책에는 Cloud Manager에서 AWS에서 Connector 인스턴스를 시작하는 데 필요한 권한만 포함되어 있습니다. 다른 상황에서는 이 정책을 사용하지 마십시오.



Cloud Manager가 Connector를 만들면 Connector가 퍼블릭 클라우드 환경에서 리소스를 관리할 수 있도록 Connector 인스턴스에 새로운 권한 세트가 적용됩니다.

단계

1. AWS IAM 콘솔로 이동합니다.
2. 정책 > 정책 생성 \* 을 클릭합니다.
3. JSON \* 을 클릭합니다.
4. 다음 정책을 복사하여 붙여 넣습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam:DeleteRole",
      "iam:PutRolePolicy",
      "iam:CreateInstanceProfile",
      "iam:DeleteRolePolicy",
      "iam:AddRoleToInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile",
      "iam:DeleteInstanceProfile",
      "iam:PassRole",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:CreateSecurityGroup",
      "ec2:DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2:DescribeInstances",
      "ec2:CreateTags",
      "ec2:DescribeImages",
```

```

        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "iam:ListRoles",
        "kms:ListAliases"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
        }
    },
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
}

```

5. 필요한 경우 \* 다음 \* 을 클릭하고 태그를 추가합니다.
6. 다음 \* 을 클릭하고 이름과 설명을 입력합니다.
7. Create policy \* 를 클릭합니다.

Cloud Manager가 추정할 수 있는 IAM 역할 또는 IAM 사용자에게 정책을 첨부합니다.

**IAM** 역할을 설정합니다

Cloud Manager가 AWS에 Connector를 구축하기 위해 수행할 수 있는 IAM 역할을 설정합니다.

단계

1. 대상 계정에서 AWS IAM 콘솔로 이동합니다.
2. 액세스 관리에서 \* 역할 > 역할 만들기 \* 를 클릭하고 단계를 따라 역할을 만듭니다.

다음을 수행하십시오.

- 신뢰할 수 있는 엔터티 유형 \* 에서 \* AWS 계정 \* 을 선택합니다.
- 다른 AWS 계정 \* 을 선택하고 Cloud Manager SaaS 계정의 ID를 입력합니다. 952013314444
- 이전 섹션에서 생성한 정책을 선택합니다.

3. 역할을 생성한 후 Connector를 생성할 때 Cloud Manager에 붙여넣을 수 있도록 Role ARN을 복사합니다.

이제 IAM 역할에 필요한 권한이 있습니다.

**IAM** 사용자에게 권한을 설정합니다

Connector를 생성할 때 Connector 인스턴스를 배포하는 데 필요한 권한이 있는 IAM 사용자에게 AWS 액세스 키와 비밀 키를 제공할 수 있습니다.

단계

1. AWS IAM 콘솔에서 \* Users \* 를 클릭한 다음 사용자 이름을 선택합니다.
2. Add permissions > Attach existing policies directly \* 를 클릭합니다.
3. 생성한 정책을 선택합니다.
4. 다음 \* 을 클릭한 다음 \* 권한 추가 \* 를 클릭합니다.
5. IAM 사용자의 액세스 키 및 비밀 키에 액세스할 수 있는지 확인합니다.

이제 AWS 사용자에게 Cloud Manager에서 Connector를 생성하는 데 필요한 권한이 있습니다. Cloud Manager에서 메시지가 표시되면 이 사용자에게 대한 AWS 액세스 키를 지정해야 합니다.

커넥터를 작성합니다

Cloud Manager를 사용하면 AWS에서 사용자 인터페이스에서 직접 Connector를 생성할 수 있습니다.

무엇을 '필요로 할거야

- AWS 인증 방법: Cloud Manager가 가정할 수 있는 IAM 역할의 ARN 또는 IAM 사용자의 AWS 액세스 키 및 비밀 키
- 선택한 AWS 지역에서 VPC, 서브넷 및 키 쌍을 제공합니다.
- Cloud Manager가 Connector에 대해 IAM 역할을 자동으로 생성하지 않도록 하려면 자체 IAM을 생성해야 합니다 ["이 페이지의 정책 사용"](#).

Connector가 퍼블릭 클라우드 환경에서 리소스를 관리하는 데 필요한 권한입니다. Connector 인스턴스를 만들기 위해 제공한 것과 다른 권한 집합입니다.

단계

1. 처음 작업 환경을 만드는 경우 \* 작업 환경 추가 \* 를 클릭하고 화면의 지시를 따릅니다. 그렇지 않으면 \* 커넥터 \* 드롭다운을 클릭하고 \* 커넥터 추가 \* 를 선택합니다.



2. 클라우드 공급자로 \* Amazon Web Services \* 를 선택하고 \* 계속 \* 을 클릭합니다.

Connector는 만들고 있는 작업 환경 유형과 활성화할 서비스에 대한 네트워크 연결이 있어야 합니다.

"Connector의 네트워킹 요구 사항에 대해 자세히 알아보십시오".

3. 마법사의 단계에 따라 커넥터를 작성합니다.

- \* 준비 완료 \*: 필요한 사항을 검토합니다.
- \* AWS 자격 증명 \*: AWS 지역을 지정한 다음, Cloud Manager가 가정할 수 있는 IAM 역할 또는 AWS 액세스 키와 비밀 키를 선택할 수 있는 인증 방법을 선택합니다.



역할 \* 가정 \* 을 선택한 경우 커넥터 배포 마법사에서 첫 번째 자격 증명 집합을 만들 수 있습니다. 자격 증명 페이지에서 추가 자격 증명 세트를 생성해야 합니다. 그런 다음 드롭다운 목록의 마법사에서 사용할 수 있습니다. ["자격 증명을 추가하는 방법에 대해 알아보십시오"](#).

- \* 세부 정보 \*: 커넥터에 대한 세부 정보를 제공합니다.
  - 인스턴스의 이름을 입력합니다.
  - 인스턴스에 사용자 지정 태그(메타데이터)를 추가합니다.
  - Cloud Manager에서 필요한 권한이 있는 새 역할을 생성할지 또는 로 설정한 기존 역할을 선택할지 여부를 선택합니다 ["필요한 권한"](#).
  - Connector의 EBS 디스크를 암호화할지 여부를 선택합니다. 기본 암호화 키를 사용하거나 사용자 지정 키를 사용할 수 있습니다.
- \* 네트워크 \*: 인스턴스에 대한 VPC, 서브넷 및 키 쌍을 지정하고, 공용 IP 주소를 사용할지 여부를 선택하고, 선택적으로 프록시 구성을 지정합니다.
- \* 보안 그룹 \*: 새 보안 그룹을 생성할지 또는 인바운드 HTTP, HTTPS 및 SSH 액세스를 허용하는 기존 보안 그룹을 선택할지 여부를 선택합니다.



커넥터 를 시작하지 않으면 커넥터로 들어오는 트래픽이 없습니다. HTTP 및 HTTPS는 에 대한 액세스를 제공합니다 ["로컬 UI"](#) 이는 드문 경우지만 사용할 수 있습니다. SSH는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.

- \* 검토 \*: 선택 사항을 검토하여 설정이 올바른지 확인합니다.

4. 추가 \* 를 클릭합니다.

인스턴스는 약 7분 내에 준비되어야 합니다. 프로세스가 완료될 때까지 페이지를 유지해야 합니다.

작업 영역 관리자가 이러한 커넥터를 사용하여 Cloud Volumes ONTAP 시스템을 만들 수 있도록 작업 영역과 커넥터를 연결해야 합니다. Account Admins만 있는 경우에는 Connector를 작업 영역과 연결할 필요가 없습니다. 계정 관리자는 기본적으로 Cloud Manager의 모든 작업 영역에 액세스할 수 있습니다. ["자세한 정보"](#).

Connector를 생성한 동일한 AWS 계정에 Amazon S3 버킷이 있는 경우 Amazon S3 작업 환경이 Canvas에 자동으로 표시됩니다. ["이 작업 환경에서 수행할 수 있는 작업에 대해 자세히 알아보십시오"](#).

## Cloud Manager에서 Azure에 Connector를 생성합니다

대부분의 Cloud Manager 기능을 사용하려면 계정 관리자가 \_Connector\_를 배포해야 합니다. Connector를 사용하면 Cloud Manager에서 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있습니다. ["커넥터가 필요한 시기를 알아보십시오"](#).

이 페이지에서는 Cloud Manager에서 직접 Azure에 Connector를 생성하는 방법을 설명합니다. ["커넥터를 배포하는 다른 방법에 대해 알아보십시오"](#).

이러한 단계는 계정 관리자 역할을 가진 사용자가 완료해야 합니다. 작업 영역 관리자가 연결선을 만들 수 없습니다.

### 개요

Connector를 배포하려면 Azure에서 Connector VM을 생성하는 데 필요한 권한이 있는 로그인을 Cloud Manager에 제공해야 합니다.

두 가지 옵션이 있습니다.

1. 메시지가 나타나면 Microsoft 계정으로 로그인합니다. 이 계정에는 특정 Azure 권한이 있어야 합니다. 이 옵션이 기본 옵션입니다.

[시작하려면 아래 단계를 따르십시오.](#)

2. Azure AD 서비스 보안 주체에 대한 세부 정보를 제공합니다. 이 서비스 보안 주체는 특정 권한도 필요합니다.

[시작하려면 아래 단계를 따르십시오.](#)

### Azure 지역에 대한 참고 사항

커넥터는 해당 커넥터가 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 영역에 배포하거나 에 배포되어야 합니다. ["Azure 지역 쌍"](#) Cloud Volumes ONTAP 시스템의 경우 이 요구 사항은 Cloud Volumes ONTAP와 연결된 스토리지 계정 간에 Azure 전용 링크 연결이 사용되도록 합니다. ["Cloud Volumes ONTAP에서 Azure 프라이빗 링크를 사용하는 방법에 대해 알아보십시오"](#).

### Azure 계정을 사용하여 커넥터를 만듭니다

Azure에서 Connector를 만드는 기본 방법은 메시지가 표시되면 Azure 계정으로 로그인하는 것입니다. 로그인 양식은 Microsoft에서 소유하고 호스팅됩니다. 자격 증명이 NetApp에 제공되지 않습니다.

Cloud Manager에서 Connector를 배포하기 전에 Azure 계정에 올바른 권한이 있는지 확인해야 합니다.

단계

1. Azure에서 새 사용자 지정 역할에 필요한 권한을 복사하여 JSON 파일에 저장합니다.



이 정책에는 Cloud Manager에서 Azure에서 Connector VM을 실행하는 데 필요한 권한만 포함되어 있습니다. 다른 상황에서는 이 정책을 사용하지 마십시오. Cloud Manager가 Connector를 만들면 Connector가 퍼블릭 클라우드 환경에서 리소스를 관리할 수 있도록 Connector VM에 새로운 권한 세트가 적용됩니다.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",

    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",

    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
```

```

        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/networkSecurityGroups/securityRules/read",
        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",

        "Microsoft.Network/networkInterfaces/ipConfigurations/read",
        "Microsoft.Resources/deployments/operations/read",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Resources/deployments/delete",
        "Microsoft.Resources/deployments/cancel/action",
        "Microsoft.Resources/deployments/validate/action",
        "Microsoft.Resources/resources/read",
        "Microsoft.Resources/subscriptions/operationresults/read",
        "Microsoft.Resources/subscriptions/resourceGroups/delete",
        "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
        "Microsoft.Resources/subscriptions/resourceGroups/write",
        "Microsoft.Authorization/roleDefinitions/write",
        "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}

```

2. Azure 구독 ID를 할당 가능한 범위에 추가하여 JSON을 수정합니다.

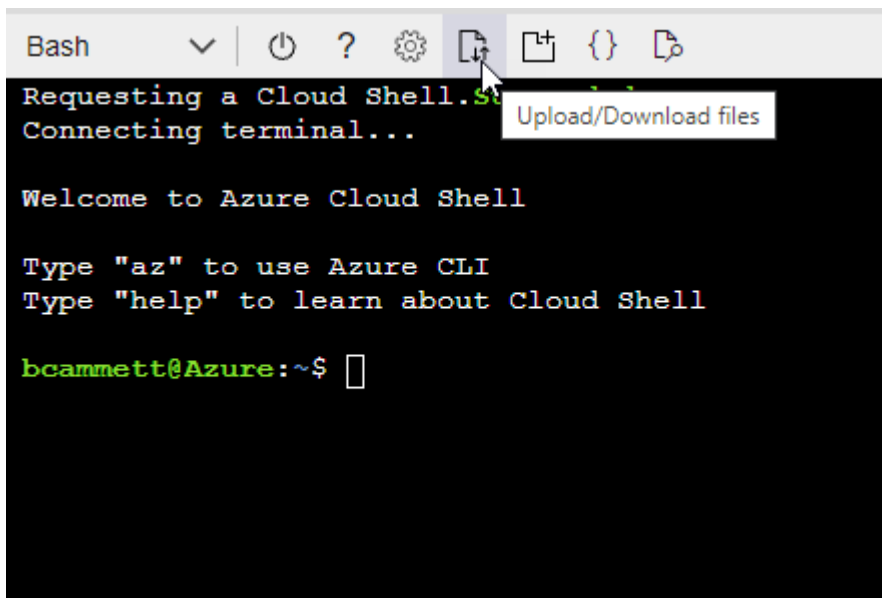
◦ 예 \*

```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzzz"
],
```

3. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 생성합니다.

다음 단계에서는 Azure Cloud Shell에서 Bash를 사용하여 역할을 생성하는 방법을 설명합니다.

- 시작 "Azure 클라우드 셸" Bash 환경을 선택하십시오.
- JSON 파일을 업로드합니다.



c. 다음 Azure CLI 명령을 입력합니다.

```
az role definition create --role-definition
Policy_for_Setup_As_Service_Azure.json
```

이제 \_Azure SetupAsService\_라는 사용자 지정 역할이 있어야 합니다.

4. Cloud Manager에서 Connector를 배포할 사용자에게 역할을 할당합니다.

- Subscriptions \* 서비스를 열고 사용자의 구독을 선택합니다.
- IAM(액세스 제어) \* 을 클릭합니다.
- Add \* > \* Add role assignment \* 를 클릭한 후 권한을 추가합니다.
  - Azure SetupAsService \* 역할을 선택하고 \* 다음 \* 을 클릭합니다.



Azure SetupAsService는 Azure의 커넥터 배포 정책에 제공된 기본 이름입니다. 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

- 사용자, 그룹 또는 서비스 보안 주체 \* 를 선택한 상태로 유지합니다.



- 회원 선택 \* 을 클릭하고 사용자 계정을 선택한 다음 \* 선택 \* 을 클릭합니다.
- 다음 \* 을 클릭합니다.
- 검토 + 할당 \* 을 클릭합니다.

이제 Azure 사용자는 Cloud Manager에서 Connector를 배포하는 데 필요한 권한을 갖게 됩니다.

**Azure** 계정으로 로그인하여 **Connector**를 생성합니다

Cloud Manager를 사용하면 사용자 인터페이스에서 직접 Azure에 Connector를 생성할 수 있습니다.

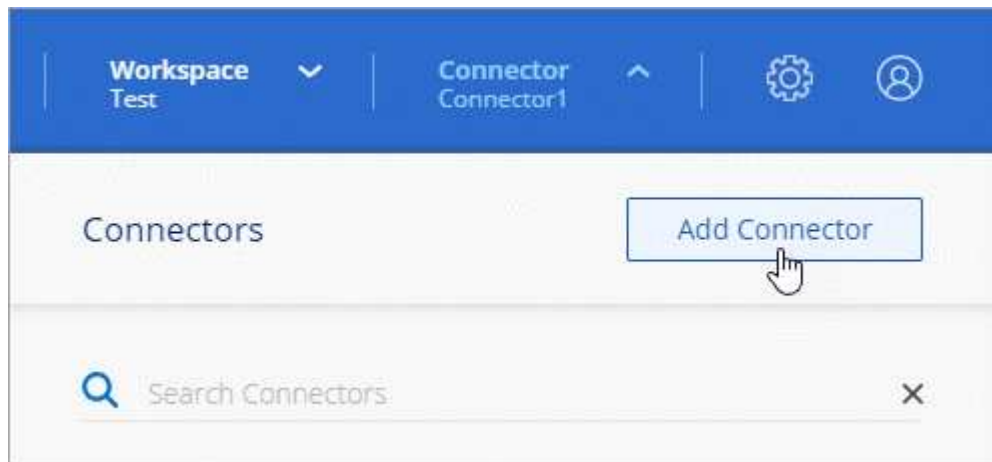
무엇을 '필요로 할거야

- Azure 구독.
- 선택한 Azure 지역에서 VNET 및 서브넷입니다.
- Cloud Manager가 Connector에 대한 Azure 역할을 자동으로 생성하지 않도록 하려면 고유한 역할을 만들어야 합니다 "[이 페이지의 정책 사용](#)".

이러한 권한은 Connector 인스턴스 자체에 대한 것입니다. 이전 설정과는 다른 사용 권한 집합으로 Connector를 배포하기만 하면 됩니다.

단계

1. 처음 작업 환경을 만드는 경우 \* 작업 환경 추가 \* 를 클릭하고 화면의 지시를 따릅니다. 그렇지 않으면 \* 커넥터 \* 드롭다운을 클릭하고 \* 커넥터 추가 \* 를 선택합니다.



2. 클라우드 공급자로 \* Microsoft Azure \* 를 선택합니다.

Connector는 만들고 있는 작업 환경 유형과 활성화할 서비스에 대한 네트워크 연결이 있어야 합니다.

"[Connector의 네트워킹 요구 사항에 대해 자세히 알아보십시오](#)".

3. 마법사의 단계에 따라 커넥터를 작성합니다.

- \* 준비 완료 \*: 필요한 항목을 검토하고 \* 다음 \* 을 클릭합니다.
- 메시지가 표시되면 Microsoft 계정에 로그인합니다. 이 계정에는 가상 컴퓨터를 만드는 데 필요한 권한이 있어야 합니다.

이 양식은 Microsoft에서 소유하고 호스팅됩니다. 자격 증명이 NetApp에 제공되지 않습니다.



이미 Azure 계정에 로그인한 경우 Cloud Manager는 해당 계정을 자동으로 사용합니다. 계정이 여러 개인 경우 먼저 로그아웃해야 올바른 계정을 사용할 수 있습니다.

- \* VM 인증 \*: Azure 구독, 위치, 새 리소스 그룹 또는 기존 리소스 그룹을 선택한 다음 인증 방법을 선택합니다.
- \* 세부 정보 \*: 인스턴스의 이름을 입력하고 태그를 지정한 다음 Cloud Manager에서 필요한 권한이 있는 새 역할을 생성할지 또는 로 설정한 기존 역할을 선택할지 여부를 선택합니다 ["필요한 권한"](#).

이 역할과 연결된 구독을 선택할 수 있습니다. 선택한 각 구독은 해당 구독에 Cloud Volumes ONTAP를 배포할 수 있는 권한을 커넥터에 제공합니다.

- \* 네트워크 \*: VNET 및 서브넷을 선택하고, 공용 IP 주소를 활성화할지 여부를 선택한 다음 선택적으로 프록시 구성을 지정합니다.
- \* 보안 그룹 \*: 새 보안 그룹을 생성할지 또는 인바운드 HTTP, HTTPS 및 SSH 액세스를 허용하는 기존 보안 그룹을 선택할지 여부를 선택합니다.



커넥터를 시작하지 않으면 커넥터로 들어오는 트래픽이 없습니다. HTTP 및 HTTPS는 에 대한 액세스를 제공합니다 ["로컬 UI"](#) 이는 드문 경우지만 사용할 수 있습니다. SSH는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.

- \* 검토 \*: 선택 사항을 검토하여 설정이 올바른지 확인합니다.

#### 4. 추가 \* 를 클릭합니다.

가상 시스템은 약 7분 내에 준비되어야 합니다. 프로세스가 완료될 때까지 페이지를 유지해야 합니다.

작업 영역 관리자가 이러한 커넥터를 사용하여 Cloud Volumes ONTAP 시스템을 만들 수 있도록 작업 영역과 커넥터를 연결해야 합니다. Account Admins만 있는 경우에는 Connector를 작업 영역과 연결할 필요가 없습니다. 계정 관리자는 기본적으로 Cloud Manager의 모든 작업 영역에 액세스할 수 있습니다. ["자세한 정보"](#).

Connector를 만든 Azure 계정에 Azure Blob 저장소가 있는 경우 Canvas에 Azure Blob 작업 환경이 자동으로 표시됩니다. ["이 작업 환경에서 수행할 수 있는 작업에 대해 자세히 알아보십시오"](#).

서비스 보안 주체를 사용하여 커넥터를 만듭니다

Azure 계정으로 로그인하는 대신 필요한 권한이 있는 Azure 서비스 보안 주체에 대한 자격 증명을 Cloud Manager에 제공할 수도 있습니다.

서비스 보안 주체를 사용하여 **Azure** 사용 권한 부여

Azure Active Directory에서 서비스 보안 주체를 생성 및 설정하고 Cloud Manager에 필요한 Azure 자격 증명을 획득하여 Azure에 Connector를 배포하는 데 필요한 권한을 부여합니다.

단계

1. [\[Create an Azure Active Directory application\]](#).
2. [\[Assign the application to a role\]](#).
3. [\[Add Windows Azure Service Management API permissions\]](#).
4. [\[Get the application ID and directory ID\]](#).

## 5. [\[Create a client secret\]](#).

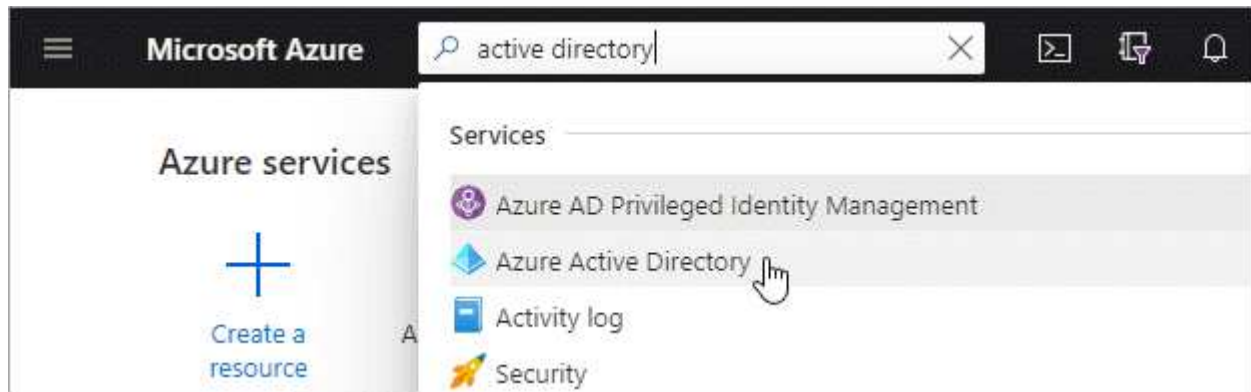
### Azure Active Directory 응용 프로그램을 만듭니다

Cloud Manager가 Connector를 배포하는 데 사용할 수 있는 Azure AD(Active Directory) 애플리케이션 및 서비스 보안 주체를 생성합니다.

Active Directory 응용 프로그램을 만들고 응용 프로그램을 역할에 할당하려면 Azure에 적절한 권한이 있어야 합니다. 자세한 내용은 [참조하십시오 "Microsoft Azure 문서: 필요한 권한"](#).

단계

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



2. 메뉴에서 \* 앱 등록 \* 을 클릭합니다.
3. 새 등록 \* 을 클릭합니다.
4. 응용 프로그램에 대한 세부 정보를 지정합니다.
  - \* 이름 \*: 응용 프로그램의 이름을 입력합니다.
  - \* 계정 유형 \*: 계정 유형을 선택합니다(모두 Cloud Manager와 연동함).
  - \* URI 리디렉션 \*: 이 필드는 비워 둘 수 있습니다.
5. Register \* 를 클릭합니다.

AD 응용 프로그램 및 서비스 보안 주체를 만들었습니다.

애플리케이션에 역할을 할당합니다

Connector를 배포하려는 Azure 구독에 서비스 보안 주체를 바인딩하고 사용자 지정 "Azure SetupAsService" 역할을 할당해야 합니다.

단계

1. Azure에서 새 사용자 지정 역할에 필요한 권한을 복사하여 JSON 파일에 저장합니다.



이 정책에는 Cloud Manager에서 Azure에서 Connector VM을 실행하는 데 필요한 권한만 포함되어 있습니다. 다른 상황에서는 이 정책을 사용하지 마십시오. Cloud Manager가 Connector를 만들면 Connector가 퍼블릭 클라우드 환경에서 리소스를 관리할 수 있도록 Connector VM에 새로운 권한 세트가 적용됩니다.

```

{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",

    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",

    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

    "Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
  ]
}

```

```

    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",

    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

    "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

    "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
  ],
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Azure SetupAsService",
  "IsCustom": "true"
}

```

2. 할당 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

◦ 예 \*

```

"AssignableScopes": [
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]

```

3. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 생성합니다.

다음 단계에서는 Azure Cloud Shell에서 Bash를 사용하여 역할을 생성하는 방법을 설명합니다.

- a. 시작 "Azure 클라우드 셸" Bash 환경을 선택하십시오.
- b. JSON 파일을 업로드합니다.



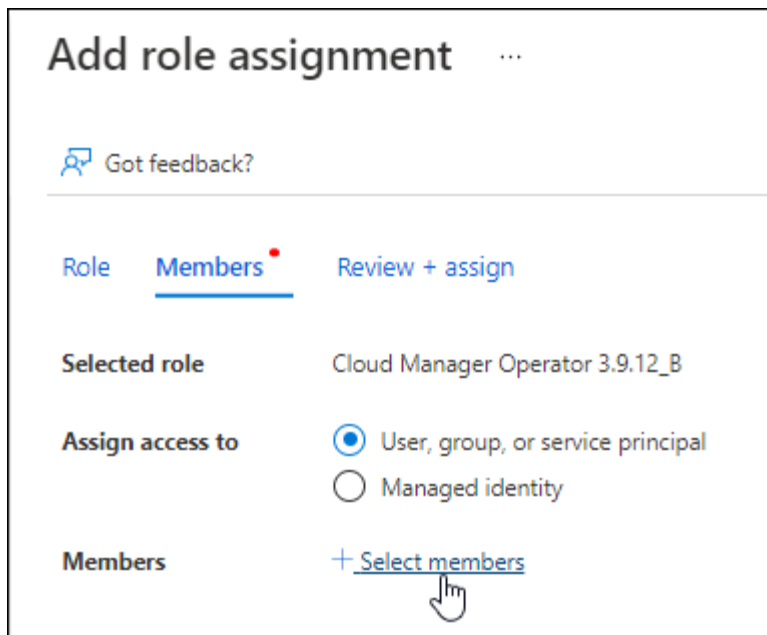
c. 다음 Azure CLI 명령을 입력합니다.

```
az role definition create --role-definition  
Policy_for_Setup_As_Service_Azure.json
```

이제 \_Azure SetupAsService\_라는 사용자 지정 역할이 있어야 합니다.

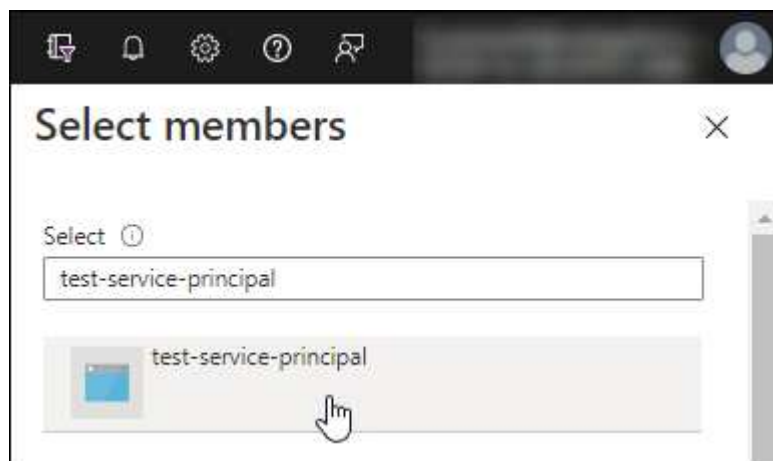
4. 역할에 응용 프로그램을 할당합니다.

- a. Azure 포털에서 \* Subscriptions \* 서비스를 엽니다.
- b. 구독을 선택합니다.
- c. IAM(Access Control) > 추가 > 역할 할당 추가 \* 를 클릭합니다.
- d. 역할\* 탭에서 \* Azure SetupAsService\* 역할을 선택하고 \* 다음 \* 을 클릭합니다.
- e. Members\* 탭에서 다음 단계를 완료합니다.
  - 사용자, 그룹 또는 서비스 보안 주체 \* 를 선택한 상태로 유지합니다.
  - 구성원 선택 \* 을 클릭합니다.



- 응용 프로그램의 이름을 검색합니다.

예를 들면 다음과 같습니다.



- 응용 프로그램을 선택하고 \* 선택 \* 을 클릭합니다.
- 다음 \* 을 클릭합니다.
  - a. 검토 + 할당 \* 을 클릭합니다.

이제 서비스 보안 주체에 Connector를 배포하는 데 필요한 Azure 권한이 있습니다.

## Windows Azure 서비스 관리 API 권한을 추가합니다

서비스 보안 주체는 "Windows Azure Service Management API" 권한이 있어야 합니다.

단계

1. Azure Active Directory \* 서비스에서 \* 앱 등록 \* 을 클릭하고 응용 프로그램을 선택합니다.
2. API 권한 > 권한 추가 \* 를 클릭합니다.

3. Microsoft API \* 에서 \* Azure Service Management \* 를 선택합니다.


## Request API permissions


### Select an API


Microsoft APIs APIs my organization uses My APIs


#### Commonly used Microsoft APIs


**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.





**Azure Batch**  
Schedule large-scale parallel and HPC applications in the cloud


**Azure Data Catalog**  
Programmatic access to Data Catalog resources to register, annotate and search data assets


**Azure Data Explorer**  
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions


**Azure Data Lake**  
Access to storage and compute for big data analytic scenarios


**Azure DevOps**  
Integrate with Azure DevOps and Azure DevOps server


**Azure Import/Export**  
Programmatic control of import/export jobs


**Azure Key Vault**  
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

**Azure Rights Management Services**  
Allow validated users to read and write protected content

**Azure Service Management**  
Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**  
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

**Customer Insights**  
Create profile and interaction models for your products

**Data Export Service for Microsoft Dynamics 365**  
Export data from Microsoft Dynamics CRM organization to an external destination

4. Access Azure Service Management as organization users \* 를 클릭한 다음 \* Add permissions \* 를 클릭합니다.



## Request API permissions

< All APIs



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user\_impersonation

Access Azure Service Management as organization users (preview) ⓘ

애플리케이션 ID 및 디렉토리 ID를 가져옵니다

Cloud Manager에서 Connector를 생성할 때 애플리케이션의 애플리케이션(클라이언트) ID와 디렉토리(테넌트) ID를 제공해야 합니다. Cloud Manager는 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

단계

1. Azure Active Directory \* 서비스에서 \* 앱 등록 \* 을 클릭하고 응용 프로그램을 선택합니다.
2. 응용 프로그램(클라이언트) ID \* 와 \* 디렉터리(테넌트) ID \* 를 복사합니다.



클라이언트 암호를 생성합니다

클라이언트 암호를 생성한 다음 Cloud Manager가 이 암호를 사용하여 Azure AD를 인증할 수 있도록 Cloud Manager에 비밀의 값을 제공해야 합니다.

단계

1. Azure Active Directory \* 서비스를 엽니다.
2. 앱 등록 \* 을 클릭하고 응용 프로그램을 선택합니다.

3. 인증서 및 비밀 > 새 클라이언트 비밀 \* 을 클릭합니다.
4. 비밀과 기간에 대한 설명을 제공하십시오.
5. 추가 \* 를 클릭합니다.
6. 클라이언트 암호 값을 복사합니다.

#### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

| + New client secret |           |                                  |
|---------------------|-----------|----------------------------------|
| DESCRIPTION         | EXPIRES   | VALUE                            |
| test secret         | 8/16/2020 | *sZ1jSe2By:D*-ZRov4NLfdAcY7:+0vA |

Copy to clipboard

이제 서비스 보안 주체가 설정되었으므로 응용 프로그램(클라이언트) ID, 디렉터리(테넌트) ID 및 클라이언트 암호 값을 복사해야 합니다. Connector를 생성할 때 Cloud Manager에 이 정보를 입력해야 합니다.

서비스 보안 주체에 로그인하여 **Connector**를 작성합니다

Cloud Manager를 사용하면 사용자 인터페이스에서 직접 Azure에 Connector를 생성할 수 있습니다.

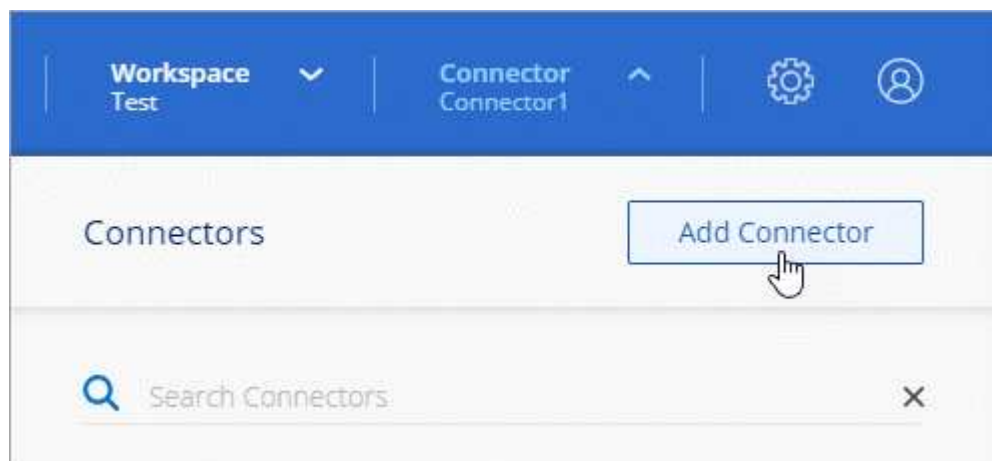
무엇을 '필요로 할거야

- Azure 구독.
- 선택한 Azure 지역에서 VNET 및 서브넷입니다.
- Cloud Manager가 Connector에 대한 Azure 역할을 자동으로 생성하지 않도록 하려면 고유한 역할을 만들어야 합니다 ["이 페이지의 정책 사용"](#).

이러한 권한은 Connector 인스턴스 자체에 대한 것입니다. 이전 설정과는 다른 사용 권한 집합으로 Connector를 배포하기만 하면 됩니다.

단계

1. 처음 작업 환경을 만드는 경우 \* 작업 환경 추가 \* 를 클릭하고 화면의 지시를 따릅니다. 그렇지 않으면 \* 커넥터 \* 드롭다운을 클릭하고 \* 커넥터 추가 \* 를 선택합니다.



## 2. 클라우드 공급자로 \* Microsoft Azure \* 를 선택합니다.

Connector는 만들고 있는 작업 환경 유형과 활성화할 서비스에 대한 네트워크 연결이 있어야 합니다.

"Connector의 네트워킹 요구 사항에 대해 자세히 알아보십시오".

## 3. 마법사의 단계에 따라 커넥터를 작성합니다.

- \* 준비 완료 \*: \* Azure AD 서비스 보안 주체 \* 를 클릭하고 필요한 권한을 부여하는 Azure Active Directory 서비스 보안 주체에 대한 정보를 입력합니다.
  - 응용 프로그램(클라이언트) ID: 을 참조하십시오 [\[Get the application ID and directory ID\]](#).
  - 디렉토리(테넌트) ID: 을 참조하십시오 [\[Get the application ID and directory ID\]](#).
  - 클라이언트 암호: 을 참조하십시오 [\[Create a client secret\]](#).
- \* VM 인증 \*: Azure 구독, 위치, 새 리소스 그룹 또는 기존 리소스 그룹을 선택한 다음 인증 방법을 선택합니다.
- \* 세부 정보 \*: 인스턴스의 이름을 입력하고 태그를 지정한 다음 Cloud Manager에서 필요한 권한이 있는 새 역할을 생성할지 또는 로 설정한 기존 역할을 선택할지 여부를 선택합니다 **"필요한 권한"**.

이 역할과 연결된 구독을 선택할 수 있습니다. 선택한 각 구독은 해당 구독에 Cloud Volumes ONTAP를 배포할 수 있는 권한을 커넥터에 제공합니다.
- \* 네트워크 \*: VNET 및 서브넷을 선택하고, 공용 IP 주소를 활성화할지 여부를 선택한 다음 선택적으로 프록시 구성을 지정합니다.
- \* 보안 그룹 \*: 새 보안 그룹을 생성할지 또는 인바운드 HTTP, HTTPS 및 SSH 액세스를 허용하는 기존 보안 그룹을 선택할지 여부를 선택합니다.



커넥터를 시작하지 않으면 커넥터로 들어오는 트래픽이 없습니다. HTTP 및 HTTPS는 에 대한 액세스를 제공합니다 **"로컬 UI"** 이는 드문 경우지만 사용할 수 있습니다. SSH는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.

- \* 검토 \*: 선택 사항을 검토하여 설정이 올바른지 확인합니다.

## 4. 추가 \* 를 클릭합니다.

가상 시스템은 약 7분 내에 준비되어야 합니다. 프로세스가 완료될 때까지 페이지를 유지해야 합니다.

작업 영역 관리자가 이러한 커넥터를 사용하여 Cloud Volumes ONTAP 시스템을 만들 수 있도록 작업 영역과 커넥터를 연결해야 합니다. Account Admins만 있는 경우에는 Connector를 작업 영역과 연결할 필요가 없습니다. 계정 관리자는 기본적으로 Cloud Manager의 모든 작업 영역에 액세스할 수 있습니다. **"자세한 정보"**.

Connector를 만든 Azure 계정에 Azure Blob 저장소가 있는 경우 Canvas에 Azure Blob 작업 환경이 자동으로 표시됩니다. **"이 작업 환경에서 수행할 수 있는 작업에 대해 자세히 알아보십시오"**.

## Cloud Manager에서 Google Cloud에 Connector를 생성합니다

대부분의 Cloud Manager 기능을 사용하려면 계정 관리자가 \_Connector\_를 배포해야 합니다. **"커넥터가 필요한 시기를 알아보십시오"**. Connector를 사용하면 Cloud Manager에서 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있습니다.

이 페이지에서는 Cloud Manager에서 직접 Google Cloud에 Connector를 생성하는 방법을 설명합니다. **"커넥터를"**

배포하는 다른 방법에 대해 알아봅니다".

이러한 단계는 계정 관리자 역할을 가진 사용자가 완료해야 합니다. 작업 영역 관리자가 연결선을 만들 수 없습니다.



첫 번째 Cloud Volumes ONTAP 작업 환경을 생성할 때 커넥터가 아직 없는 경우 Cloud Manager에서 커넥터를 생성하라는 메시지를 표시합니다.

## Connector 배포 권한을 설정합니다

Connector를 배포하기 전에 Google Cloud 계정에 올바른 권한이 있는지 확인해야 합니다.

단계

1. "사용자 지정 역할을 만듭니다" 여기에는 다음 권한이 포함됩니다.

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
Cloud Manager
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
```

- `compute.networks.list`
- `compute.networks.updatePolicy`
- `compute.projects.get`
- `compute.regions.get`
- `compute.regions.list`
- `compute.subnetworks.get`
- `compute.subnetworks.list`
- `compute.zoneOperations.get`
- `compute.zones.get`
- `compute.zones.list`
- `deploymentmanager.compositeTypes.get`
- `deploymentmanager.compositeTypes.list`
- `deploymentmanager.deployments.create`
- `deploymentmanager.deployments.delete`
- `deploymentmanager.deployments.get`
- `deploymentmanager.deployments.list`
- `deploymentmanager.manifests.get`
- `deploymentmanager.manifests.list`
- `deploymentmanager.operations.get`
- `deploymentmanager.operations.list`
- `deploymentmanager.resources.get`
- `deploymentmanager.resources.list`
- `deploymentmanager.typeProviders.get`
- `deploymentmanager.typeProviders.list`
- `deploymentmanager.types.get`
- `deploymentmanager.types.list`
- `resourcemanager.projects.get`
- `compute.instances.setServiceAccount`
- `iam.serviceAccounts.list`

2. Cloud Manager에서 Connector를 배포할 사용자에게 사용자 지정 역할을 연결합니다.

이제 Google Cloud 사용자에게 Connector를 만드는 데 필요한 권한이 있습니다.

**Connector**에 대한 서비스 계정을 설정합니다

Connector에 Google Cloud의 리소스를 관리하는 데 필요한 권한을 제공하려면 서비스 계정이 필요합니다. 이 서비스 계정을 만들 때 Connector VM에 연결합니다.

서비스 계정에 대한 사용 권한이 이전 섹션에서 설정한 사용 권한과 다릅니다.

단계

1. "사용자 지정 역할을 만듭니다" 여기에는 다음 권한이 포함됩니다.

```
title: NetApp Cloud Manager
description: Permissions for the service account associated with the
```

```
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
```

- `compute.regions.get`
- `compute.regions.list`
- `compute.snapshots.create`
- `compute.snapshots.delete`
- `compute.snapshots.get`
- `compute.snapshots.list`
- `compute.snapshots.setLabels`
- `compute.subnetworks.get`
- `compute.subnetworks.list`
- `compute.subnetworks.use`
- `compute.subnetworks.useExternalIp`
- `compute.zoneOperations.get`
- `compute.zones.get`
- `compute.zones.list`
- `compute.instances.setServiceAccount`
- `deploymentmanager.compositeTypes.get`
- `deploymentmanager.compositeTypes.list`
- `deploymentmanager.deployments.create`
- `deploymentmanager.deployments.delete`
- `deploymentmanager.deployments.get`
- `deploymentmanager.deployments.list`
- `deploymentmanager.manifests.get`
- `deploymentmanager.manifests.list`
- `deploymentmanager.operations.get`
- `deploymentmanager.operations.list`
- `deploymentmanager.resources.get`
- `deploymentmanager.resources.list`
- `deploymentmanager.typeProviders.get`
- `deploymentmanager.typeProviders.list`
- `deploymentmanager.types.get`
- `deploymentmanager.types.list`
- `logging.logEntries.list`
- `logging.privateLogEntries.list`
- `resourcemanager.projects.get`
- `storage.buckets.create`
- `storage.buckets.delete`
- `storage.buckets.get`
- `storage.buckets.list`
- `cloudkms.cryptoKeyVersions.useToEncrypt`
- `cloudkms.cryptoKeys.get`
- `cloudkms.cryptoKeys.list`
- `cloudkms.keyRings.list`
- `storage.buckets.update`
- `iam.serviceAccounts.getIamPolicy`
- `iam.serviceAccounts.list`
- `storage.objects.get`

- `storage.objects.list`

2. "Google Cloud 서비스 계정을 만들고 방금 만든 사용자 지정 역할을 적용합니다".
3. 다른 프로젝트에 Cloud Volumes ONTAP을 배포하려는 경우 "Cloud Manager 역할을 가진 서비스 계정을 해당 프로젝트에 추가하여 액세스 권한을 부여합니다". 각 프로젝트에 대해 이 단계를 반복해야 합니다.

Connector VM에 대한 서비스 계정이 설정되어 있습니다.

#### 공유 VPC 권한

공유 VPC를 사용하여 리소스를 서비스 프로젝트에 구축하는 경우 다음과 같은 권한이 필요합니다. 이 표는 참조용이며 IAM 구성이 완료되면 사용 권한 테이블이 환경에 반영되어야 합니다.

| 아이덴티티                               | 창조자         | 에서 호스팅됩니다 | 서비스 프로젝트 권한   | 호스트 프로젝트 권한   | 목적  |
|-------------------------------------|-------------|-----------|---|---|---|
| Connector를 배포하는 데 사용되는 Google 계정입니다 | 맞춤형         | 서비스 프로젝트  | <ul style="list-style-type: none"><li>"위의 이 섹션에 있는 사용 권한"</li></ul>   | <ul style="list-style-type: none"><li>compute.networkUser</li></ul>                   | 서비스 프로젝트에 Connector 배포  |
| 커넥터 서비스 계정                          | 맞춤형         | 서비스 프로젝트  | <ul style="list-style-type: none"><li>"위의 이 섹션에 있는 사용 권한"</li></ul>   | <ul style="list-style-type: none"><li>compute.networkUser</li><li>배포관리자.편집기</li></ul> | 서비스 프로젝트에서 Cloud Volumes ONTAP 및 서비스를 배포 및 유지 관리합니다                       |
| Cloud Volumes ONTAP 서비스 계정입니다       | 맞춤형         | 서비스 프로젝트  | <ul style="list-style-type: none"><li>storage.admin을 선택합니다</li><li>회원: Cloud Manager 서비스 계정은 serviceAccount.user입니다</li></ul> | 해당 없음   | (선택 사항) 데이터 계층화 및 Cloud Backup을 위한 솔루션                                    |
| Google API 서비스 에이전트입니다              | Google 클라우드 | 서비스 프로젝트  | <ul style="list-style-type: none"><li>(기본값) 편집기</li></ul>   | <ul style="list-style-type: none"><li>compute.networkUser</li></ul>                   | 배포를 대신하여 Google Cloud API와 상호 작용합니다. Cloud Manager에서 공유 네트워크를 사용할 수 있습니다. |



| 아이덴티티                              | 창조자         | 에서 호스팅됩니다 | 서비스 프로젝트 권한 | 호스트 프로젝트 권한           | 목적  |
|------------------------------------|-------------|-----------|-------------|-----------------------|---|
| Google Compute Engine 기본 서비스 계정입니다 | Google 클라우드 | 서비스 프로젝트  | • (기본값) 편집기 | • compute.networkUser | 배포를 대신하여 Google Cloud 인스턴스 및 컴퓨팅 인프라를 배포합니다. Cloud Manager에서 공유 네트워크를 사용할 수 있습니다. |

참고:

1. deploymentmanager.editor는 배포에 방화벽 규칙을 전달하지 않고 Cloud Manager가 사용자를 위해 방화벽 규칙을 만들도록 선택한 경우에만 호스트 프로젝트에 필요합니다. 규칙이 지정되지 않은 경우 Cloud Manager는 VPC0 방화벽 규칙이 포함된 호스트 프로젝트에 배포를 생성합니다.
2. Firewall.create 및 firewall.delete 은 배포에 방화벽 규칙을 전달하지 않고 Cloud Manager에서 이러한 규칙을 만들도록 선택한 경우에만 필요합니다. 이러한 권한은 Cloud Manager 서비스 계정 .YAML 파일에 있습니다. 공유 VPC를 사용하여 HA 쌍을 구축하는 경우 이러한 사용 권한을 사용하여 VPC1, 2 및 3에 대한 방화벽 규칙을 생성합니다. 다른 모든 배포의 경우 이러한 사용 권한을 사용하여 VPC0에 대한 규칙을 만들 수도 있습니다.
3. 데이터 계층화의 경우 계층화 서비스 계정은 프로젝트 수준뿐만 아니라 서비스 계정에서 serviceAccount.user 역할을 가져야 합니다. 현재 프로젝트 수준에서 serviceAccount.user 를 할당하는 경우 getIAMPolicy를 사용하여 서비스 계정을 쿼리할 때 사용 권한이 표시되지 않습니다.

## Google Cloud API 활성화

Connector와 Cloud Volumes ONTAP를 구축하려면 여러 API가 필요합니다.

단계

1. "프로젝트에서 다음 Google Cloud API를 활성화합니다".
  - Cloud Deployment Manager V2 API
  - 클라우드 로깅 API
  - Cloud Resource Manager API를 참조하십시오
  - 컴퓨팅 엔진 API
  - IAM(Identity and Access Management) API

## Google Cloud에서 커넥터 만들기

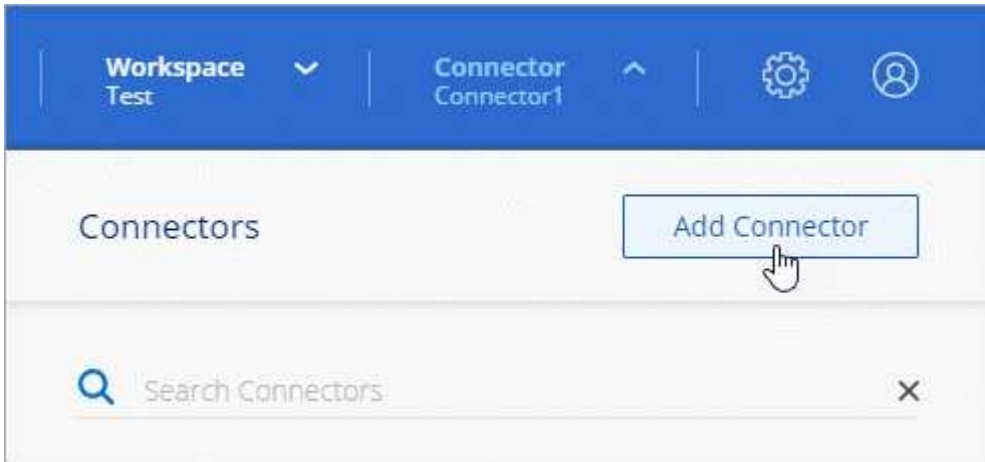
Cloud Manager 사용자 인터페이스에서 직접 또는 gcloud를 사용하여 Google Cloud에서 Connector를 생성합니다.

무엇을 '필요로 할거야

- 이 페이지의 첫 번째 섹션에 설명된 대로 Google Cloud 계정에 필요한 사용 권한.
- Google Cloud 프로젝트.
- 이 페이지의 첫 번째 섹션에 설명된 대로 Cloud Volumes ONTAP를 만들고 관리하는 데 필요한 권한이 있는 서비스 계정입니다.
- Google Cloud 지역에서 VPC 및 서브넷을 선택할 수 있습니다.

## 클라우드 관리자

1. 처음 작업 환경을 만드는 경우 \* 작업 환경 추가 \* 를 클릭하고 화면의 지시를 따릅니다. 그렇지 않으면 \* 커넥터 \* 드롭다운을 클릭하고 \* 커넥터 추가 \* 를 선택합니다.



2. 클라우드 공급자로 \* Google Cloud Platform \* 을 선택합니다.

Connector는 만들고 있는 작업 환경 유형과 활성화할 서비스에 대한 네트워크 연결이 있어야 합니다.

["Connector의 네트워킹 요구 사항에 대해 자세히 알아보십시오"](#).

3. 마법사의 단계에 따라 커넥터를 작성합니다.

- \* 준비 완료 \*: 필요한 사항을 검토합니다.
- 메시지가 표시되면 Google 계정에 로그인합니다. 이 계정에는 가상 머신 인스턴스를 생성하는 데 필요한 권한이 있어야 합니다.

이 양식은 Google에서 소유하고 호스팅됩니다. 자격 증명이 NetApp에 제공되지 않습니다.

- \* 기본 설정 \*: 가상 머신 인스턴스의 이름을 입력하고 태그를 지정하고 프로젝트를 선택한 다음 필요한 권한이 있는 서비스 계정을 선택합니다(자세한 내용은 위의 섹션 참조).
- \* 위치 \*: 인스턴스의 영역, 영역, VPC 및 서브넷을 지정합니다.
- \* 네트워크 \*: 공용 IP 주소를 사용할지 여부를 선택하고 선택적으로 프록시 구성을 지정합니다.
- \* 방화벽 정책 \*: 새 방화벽 정책을 생성할지 또는 인바운드 HTTP, HTTPS 및 SSH 액세스를 허용하는 기존 방화벽 정책을 선택할지 여부를 선택합니다.



커넥터 를 시작하지 않으면 커넥터로 들어오는 트래픽이 없습니다. HTTP 및 HTTPS는 예 대한 액세스를 제공합니다 ["로컬 UI"](#) 이는 드문 경우지만 사용할 수 있습니다. SSH는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.

- \* 검토 \*: 선택 사항을 검토하여 설정이 올바른지 확인합니다.

4. 추가 \* 를 클릭합니다.

인스턴스는 약 7분 내에 준비되어야 합니다. 프로세스가 완료될 때까지 페이지를 유지해야 합니다.

## gcloud를 선택합니다

1. 원하는 방법을 사용하여 gcloud SDK에 로그인합니다.

이 예에서는 gcloud SDK가 설치된 로컬 셸을 사용하지만 Google Cloud 콘솔에서 기본 Google Cloud Shell을 사용할 수 있습니다.

Google Cloud SDK에 대한 자세한 내용은 [를 참조하십시오 "Google Cloud SDK 설명서 페이지"](#).

2. 위 섹션에 정의된 필수 권한이 있는 사용자로 로그인했는지 확인합니다.

```
gcloud auth list
```

출력에는 \* 사용자 계정이 로그인하려는 사용자 계정인 경우 다음과 같이 표시됩니다.

```
Credentialed Accounts
ACTIVE  ACCOUNT
      some_user_account@domain.com
*      desired_user_account@domain.com
To set the active account, run:
$ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. gcloud compute instances create 명령을 실행합니다.

```
gcloud compute instances create <instance-name>
  --machine-type=n1-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<<service-account>>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

## 인스턴스 이름

VM 인스턴스에 대해 원하는 인스턴스 이름입니다.

#### 프로젝트

(선택 사항) VM을 배포할 프로젝트입니다.

#### 서비스 계정

2단계의 출력에 지정된 서비스 계정입니다.

#### Zone(영역)

VM을 배포할 영역입니다

#### 주소 없음

(선택 사항) 외부 IP 주소가 사용되지 않습니다(공용 인터넷에 트래픽을 라우팅하려면 클라우드 NAT 또는 프록시가 필요합니다).

#### 네트워크 태그

(선택 사항) 태그를 사용하여 방화벽 규칙을 Connector 인스턴스에 연결하는 네트워크 태그를 추가합니다

#### 네트워크 경로

(선택 사항) Connector를 구축할 네트워크 이름 추가(공유 VPC의 경우 전체 경로 필요)

#### subnet-path를 입력합니다

(선택 사항) Connector를 구축할 서브넷의 이름 추가(공유 VPC의 경우 전체 경로 필요)

#### kms - 키 경로

(선택 사항) 커넥터 디스크를 암호화하는 KMS 키 추가(IAM 사용 권한도 적용해야 함)

이러한 플래그에 대한 자세한 내용은 를 참조하십시오 "[Google Cloud Compute SDK 설명서](#)".

+

명령을 실행하면 NetApp 골드 이미지를 사용하여 Connector가 구축됩니다. Connector 인스턴스 및 소프트웨어는 약 5분 내에 실행되어야 합니다.

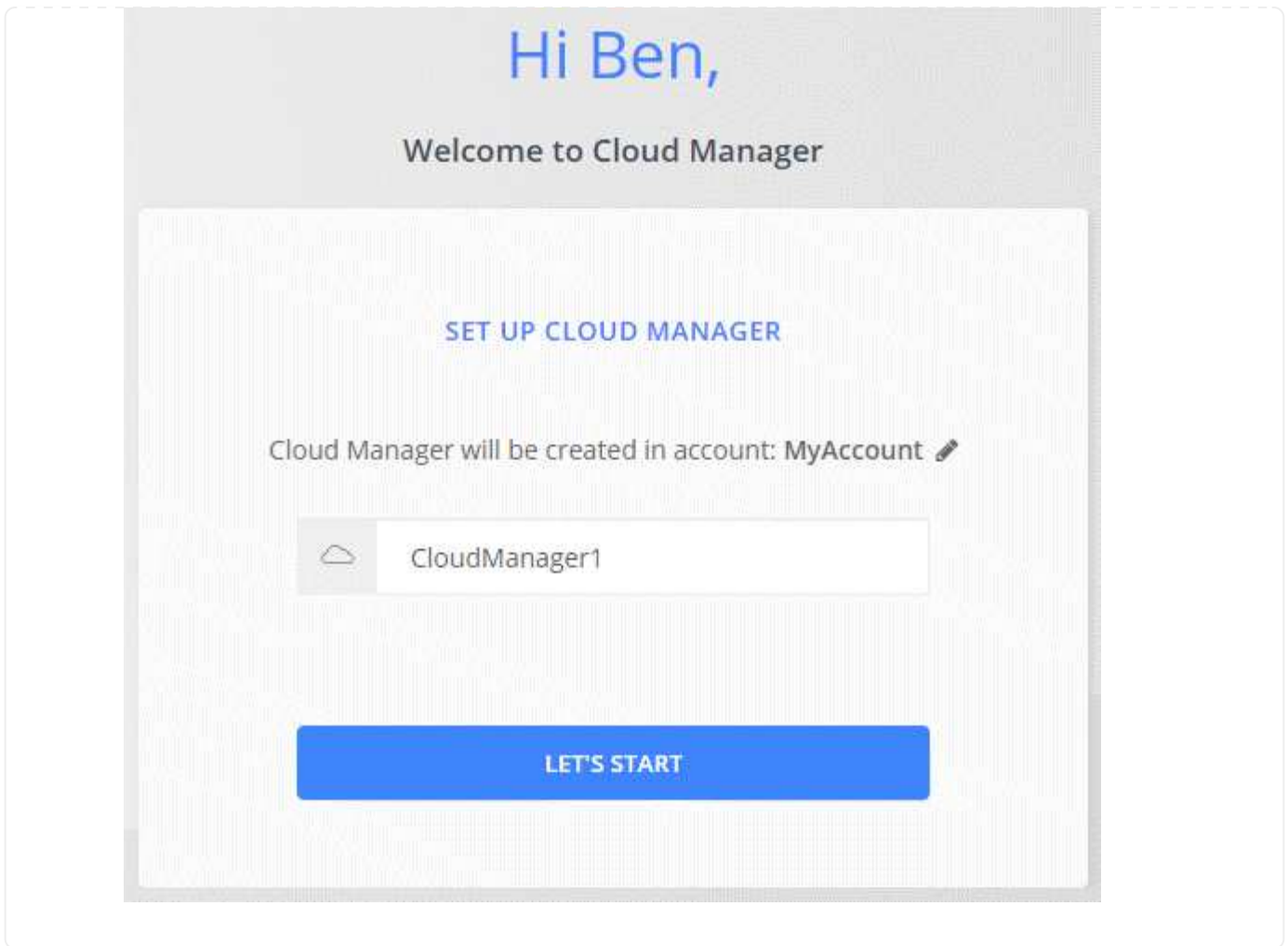
1. Connector 인스턴스에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

`http://ipaddress:80[]`

2. 로그인한 후 Connector를 설정합니다.
  - a. Connector와 연결할 NetApp 계정을 지정합니다.

["NetApp 계정 에 대해 알아보십시오"](#).

- b. 시스템의 이름을 입력합니다.



이제 Connector가 NetApp 계정으로 설치 및 설정됩니다. 새로운 작업 환경을 만들 때 Cloud Manager가 이 Connector를 자동으로 사용합니다. 그러나 둘 이상의 커넥터가 있는 경우 이 작업을 수행해야 합니다 ["둘 사이를 전환합니다"](#).

Connector를 생성한 동일한 Google Cloud 계정에 Google Cloud Storage 버킷을 사용하는 경우 Google Cloud Storage 작업 환경이 Canvas에 자동으로 표시됩니다. ["이 작업 환경에서 수행할 수 있는 작업에 대해 자세히 알아보십시오"](#).

## 다음 단계로 넘어갑니다

로그인한 후 Cloud Manager를 설정했으므로 사용자는 작업 환경을 생성하고 검색을 시작할 수 있습니다.

- ["Cloud Volumes ONTAP for AWS 시작하기"](#)
- ["Azure용 Cloud Volumes ONTAP를 시작하십시오"](#)
- ["Cloud Volumes ONTAP for Google Cloud를 시작해 보십시오"](#)
- ["Azure NetApp Files를 설정합니다"](#)
- ["ONTAP용 Amazon FSx를 설정합니다"](#)
- ["Cloud Volumes Service for AWS 설정"](#)

- "사내 ONTAP 클러스터를 검색합니다"
- "Amazon S3 버킷을 검색합니다"

# Cloud Manager 관리

## NetApp 계정

### NetApp 계정 관리

"초기 설정을 수행한 후", 나중에 사용자, 서비스 계정, 작업 영역, 커넥터 및 구독을 관리하여 계정 설정을 관리할 수 있습니다.

"NetApp 계정의 작동 방식에 대해 자세히 알아보십시오".

### Tenancy API로 계정 관리

API 요청을 전송하여 계정 설정을 관리하려면 \_Tenancy\_API를 사용해야 합니다. 이 API는 Cloud Volumes ONTAP 작업 환경을 만들고 관리하는 데 사용하는 Cloud Manager API와 다릅니다.

"Tenancy API에 대한 끝점을 봅니다"

### 사용자 생성 및 관리

계정의 사용자는 계정 작업 영역의 리소스 관리에 액세스할 수 있습니다.

### 사용자 추가

Cloud Central 사용자를 NetApp 계정과 연결하여 Cloud Manager에서 작업 환경을 만들고 관리할 수 있습니다.

### 단계

1. 사용자가 아직 이 작업을 수행하지 않은 경우 사용자에게 로 이동하라고 요청합니다 "NetApp Cloud Central에서" 을 클릭합니다.
2. Cloud Manager 상단에서 \* Account \* (계정 \*) 드롭다운을 클릭합니다.

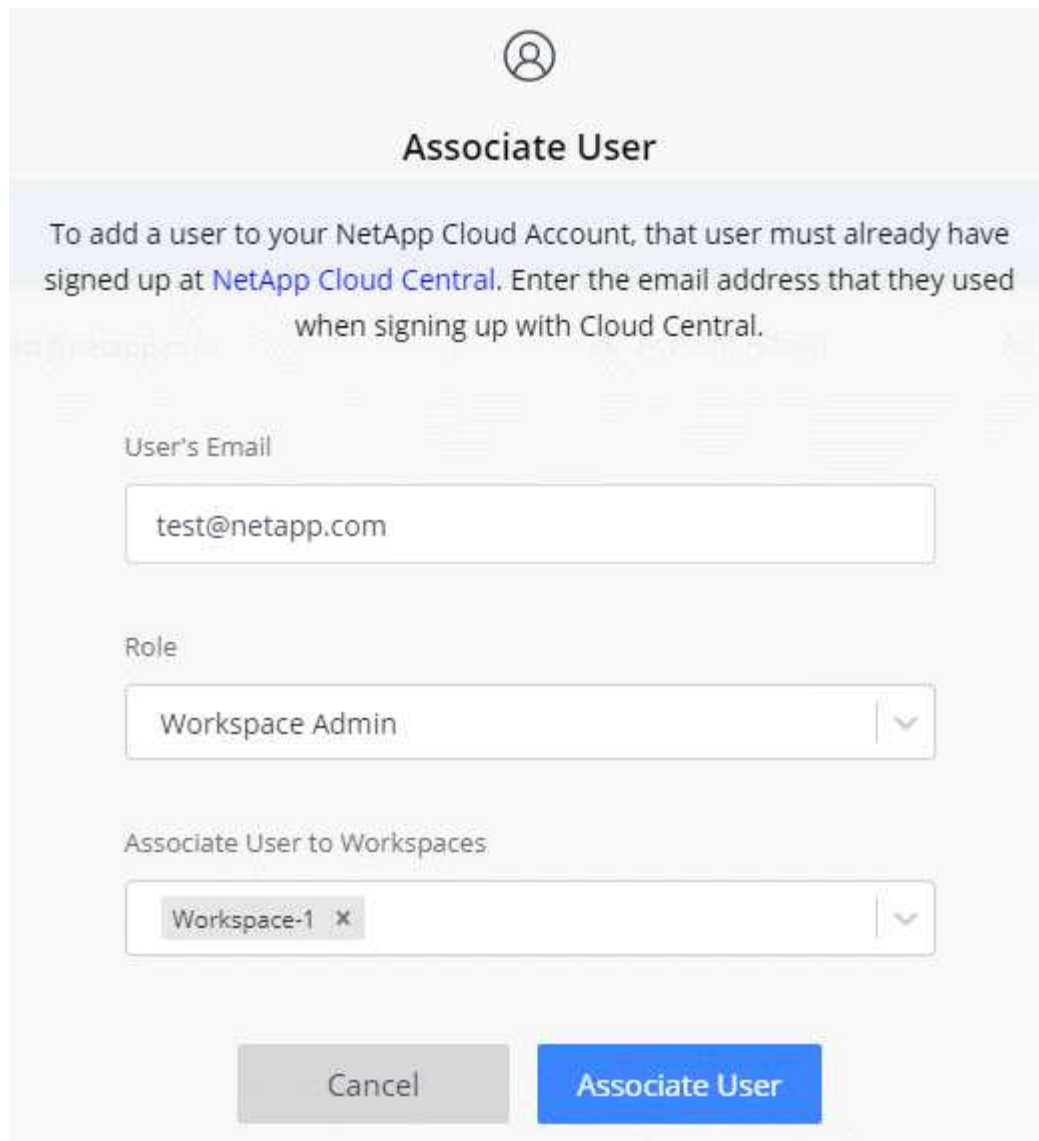


3. 현재 선택한 계정 옆에 있는 \* 계정 관리 \* 를 클릭합니다.



4. 구성원 탭에서 \* 사용자 연결 \* 을 클릭합니다.
5. 사용자의 이메일 주소를 입력하고 사용자의 역할을 선택합니다.
  - \* 계정 관리자 \*: Cloud Manager에서 모든 작업을 수행할 수 있습니다.
  - \* Workspace Admin \*: 할당된 작업 영역에서 리소스를 만들고 관리할 수 있습니다.
  - \* Compliance Viewer \*: 클라우드 데이터 감지 규정 준수 정보만 보고 액세스 권한이 있는 작업 영역에 대한 보고서를 생성할 수 있습니다.
  - \* SnapCenter 관리자 \*: SnapCenter 서비스를 사용하여 애플리케이션 정합성이 보장되는 백업을 생성하고 이러한 백업을 사용하여 데이터를 복원할 수 있습니다. \_ 이 서비스는 현재 베타 상태입니다. \_
6. 작업 영역 관리자 또는 규정 준수 뷰어를 선택한 경우 해당 사용자와 연결할 작업 영역을 하나 이상 선택합니다.





The image shows a web-based dialog box titled "Associate User". At the top, there is a user icon. Below the title, a light blue banner contains the text: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." The main form area has three sections: "User's Email" with a text input field containing "test@netapp.com"; "Role" with a dropdown menu showing "Workspace Admin"; and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close button (X). At the bottom, there are two buttons: a grey "Cancel" button and a blue "Associate User" button.

7. Associate \* 를 클릭합니다.

사용자는 NetApp Cloud Central에서 "Account Association"이라는 제목의 이메일을 받아야 합니다. 이 이메일에는 Cloud Manager에 액세스하는 데 필요한 정보가 포함되어 있습니다.

사용자를 제거하는 중입니다

사용자를 연결하면 NetApp 계정의 리소스에 더 이상 액세스할 수 없습니다.

단계

1. Cloud Manager 상단에서 \* 계정 \* 드롭다운을 클릭하고 \* 계정 관리 \* 를 클릭합니다.



2. 구성원 탭의 행에 있는 해당 사용자에게 해당하는 작업 메뉴를 클릭합니다.



3. 사용자 연결 해제 \* 를 클릭하고 \* 연결 해제 \* 를 클릭하여 확인합니다.

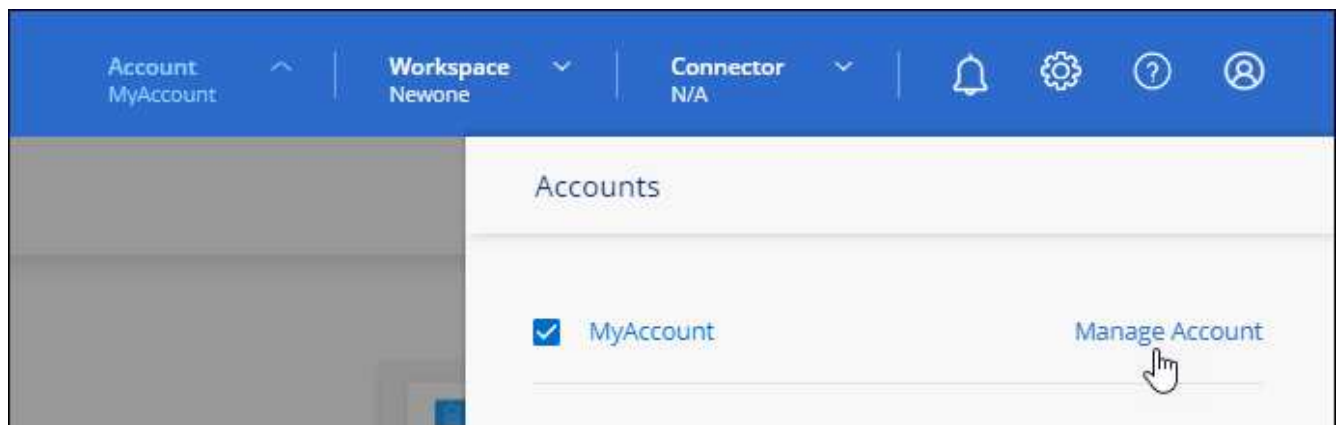
사용자는 더 이상 이 NetApp 계정의 리소스에 액세스할 수 없습니다.

작업 영역 관리자의 작업 영역 관리

언제든지 Workspace Admins를 작업 영역과 연결 및 연결 해제할 수 있습니다. 사용자를 연결하면 해당 작업 영역에서 작업 환경을 만들고 볼 수 있습니다.

단계

1. Cloud Manager 상단에서 \* 계정 \* 드롭다운을 클릭하고 \* 계정 관리 \* 를 클릭합니다.



2. 구성원 탭의 행에 있는 해당 사용자에게 해당하는 작업 메뉴를 클릭합니다.

| 5 Members |      |       |                 |                |     |
|-----------|------|-------|-----------------|----------------|-----|
| Type      | Name | Email | Role            | Workspace      |     |
|           | Ben  |       | ☆ Account Admin | All Workspaces | ... |
|           | Tom  |       | ☆ Account Admin | All Workspaces | ... |
|           | Ben  |       | Workspace Admin | Newone         |     |

3. 작업 영역 관리 \* 를 클릭합니다.

4. 사용자와 연결할 작업 영역을 선택하고 \* 적용 \* 을 클릭합니다.

Connector가 작업 공간에도 연결되어 있는 한 이제 사용자는 Cloud Manager에서 이러한 작업 영역에 액세스할 수 있습니다.

### 서비스 계정 생성 및 관리

서비스 계정은 자동화를 위해 Cloud Manager에 승인된 API 호출을 수행할 수 있는 "사용자" 역할을 합니다. 따라서 언제든지 퇴사할 수 있는 실제 사용자의 계정을 기반으로 자동화 스크립트를 작성할 필요가 없으므로 자동화를 더욱 쉽게 관리할 수 있습니다. 페더레이션을 사용하는 경우 클라우드에서 새로 고침 토큰을 생성하지 않고 토큰을 생성할 수 있습니다.

다른 Cloud Manager 사용자와 마찬가지로 서비스 계정에 역할을 할당하여 서비스 계정에 권한을 부여합니다. 또한 서비스 계정을 특정 작업 영역에 연결하여 서비스가 액세스할 수 있는 작업 환경(리소스)을 제어할 수도 있습니다.

서비스 계정을 생성할 때 Cloud Manager를 사용하면 서비스 계정에 대한 클라이언트 ID 및 클라이언트 암호를 복사하거나 다운로드할 수 있습니다. 이 키 쌍은 Cloud Manager와의 인증에 사용됩니다.

서비스 계정을 만드는 중입니다

작업 환경의 리소스를 관리하는 데 필요한 만큼 서비스 계정을 만듭니다.

### 단계

1. Cloud Manager 상단에서 \* Account \* (계정 \*) 드롭다운을 클릭합니다.



2. 현재 선택한 계정 옆에 있는 \* 계정 관리 \* 를 클릭합니다.



3. 구성원 탭에서 \* 서비스 계정 만들기 \* 를 클릭합니다.
4. 이름을 입력하고 역할을 선택합니다. 계정 관리자 이외의 역할을 선택한 경우 이 서비스 계정과 연결할 작업 영역을 선택합니다.
5. Create \* 를 클릭합니다.
6. 클라이언트 ID 및 클라이언트 암호를 복사하거나 다운로드합니다.

클라이언트 암호는 한 번만 표시되며 Cloud Manager가 어느 곳에도 저장할 수 없습니다. 암호를 복사하거나 다운로드한 후 안전하게 보관하십시오.

7. 닫기 \* 를 클릭합니다.

서비스 계정에 대한 베어러 토큰을 가져오는 중입니다

를 API 호출하기 위해 "테넌시 API" 서비스 계정에 대한 베어러 토큰을 얻어야 합니다.

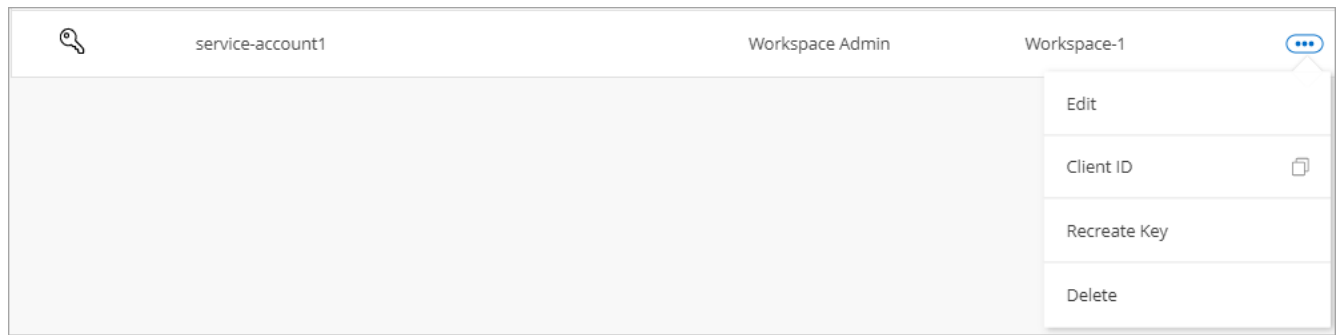
```
curl --location --request POST 'https://netapp-cloud-account.auth0.com/oauth/token' \
--header 'Content-Type: application/json' \
--data-raw '{
  "grant_type": "client_credentials",
  "client_secret": "<client secret>",
  "audience": "https://api.cloud.netapp.com",
  "client_id": "<client id>"
}'
```

클라이언트 ID를 복사하는 중입니다

서비스 계정의 클라이언트 ID는 언제든지 복사할 수 있습니다.

단계

1. 구성원 탭에서 서비스 계정에 해당하는 행의 작업 메뉴를 클릭합니다.



2. 클라이언트 ID \* 를 클릭합니다.

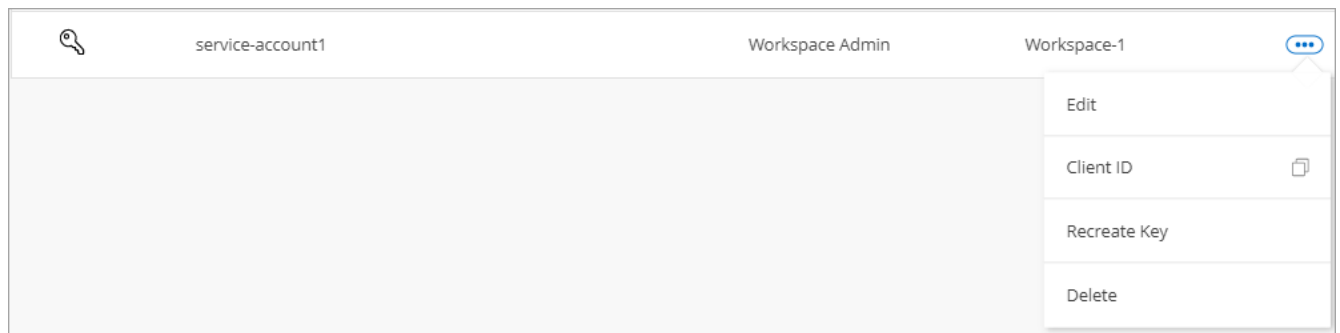
3. ID가 클립보드에 복사됩니다.

키를 다시 만드는 중입니다

키를 다시 생성하면 이 서비스 계정의 기존 키가 삭제되며 새 키가 생성됩니다. 이전 키를 사용할 수 없습니다.

단계

1. 구성원 탭에서 서비스 계정에 해당하는 행의 작업 메뉴를 클릭합니다.



2. 키 재생성 \* 을 클릭합니다.

3. reate \* 를 클릭하여 확인합니다.

4. 클라이언트 ID 및 클라이언트 암호를 복사하거나 다운로드합니다.

클라이언트 암호는 한 번만 표시되며 Cloud Manager가 어느 곳에도 저장할 수 없습니다. 암호를 복사하거나 다운로드한 후 안전하게 보관하십시오.

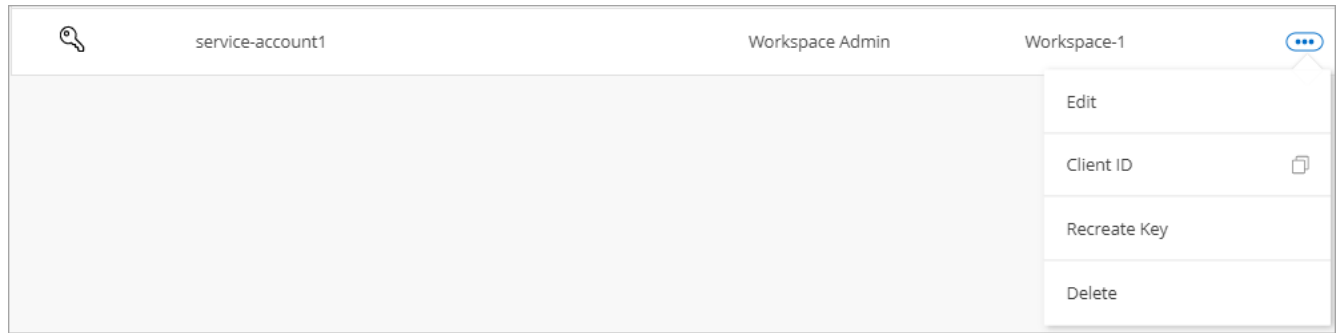
5. 닫기 \* 를 클릭합니다.

서비스 계정을 삭제하는 중입니다

더 이상 사용할 필요가 없는 경우 서비스 계정을 삭제합니다.

단계

1. 구성원 탭에서 서비스 계정에 해당하는 행의 작업 메뉴를 클릭합니다.



2. 삭제 \* 를 클릭합니다.
3. 확인하려면 \* 삭제 \* 를 다시 클릭합니다.

### 작업 영역 관리

작업 영역을 만들고 이름을 바꾸고 삭제하여 관리합니다. 작업 영역에 자원이 포함된 경우에는 작업 영역을 삭제할 수 없습니다. 비어 있어야 합니다.

#### 단계

1. Cloud Manager 상단에서 \* 계정 \* 드롭다운을 클릭하고 \* 계정 관리 \* 를 클릭합니다.
2. 작업 공간 \* 을 클릭합니다.
3. 다음 옵션 중 하나를 선택합니다.
  - 새 작업 영역을 만들려면 \* 새 작업 영역 추가 \* 를 클릭합니다.
  - 작업 영역의 이름을 바꾸려면 \* Rename \* (이름 바꾸기 \*)을 클릭합니다.
  - 작업 공간을 삭제하려면 \* 삭제 \* 를 클릭합니다.

### Connector의 작업 영역 관리

Workspace 관리자가 Cloud Manager에서 해당 작업 영역에 액세스할 수 있도록 Connector를 작업 공간에 연결해야 합니다.

Account Admins만 있는 경우에는 Connector를 작업 영역과 연결할 필요가 없습니다. 계정 관리자는 기본적으로 Cloud Manager의 모든 작업 영역에 액세스할 수 있습니다.

["사용자, 작업 영역 및 커넥터에 대해 자세히 알아보십시오"](#).

#### 단계

1. Cloud Manager 상단에서 \* 계정 \* 드롭다운을 클릭하고 \* 계정 관리 \* 를 클릭합니다.
2. 커넥터 \* 를 클릭합니다.
3. 연결하려는 Connector의 \* 작업 영역 관리 \* 를 클릭합니다.
4. 커넥터와 연결할 작업 영역을 선택하고 \* 적용 \* 을 클릭합니다.

### 구독 관리

클라우드 공급자의 마켓플레이스에서 구독하면 계정 설정 위젯에서 각 구독을 사용할 수 있습니다. 구독의 이름을 바꾸고 하나 이상의 계정에서 구독을 연결 해제할 수 있습니다.

예를 들어, 두 개의 계정이 있고 각각 별도의 구독을 통해 비용이 청구된다고 가정해 보겠습니다. Cloud Volume ONTAP 작업 환경을 생성할 때 해당 계정의 사용자가 실수로 잘못된 구독을 선택하지 않도록 계정 중 하나에서 구독을 연결 해제할 수 있습니다.

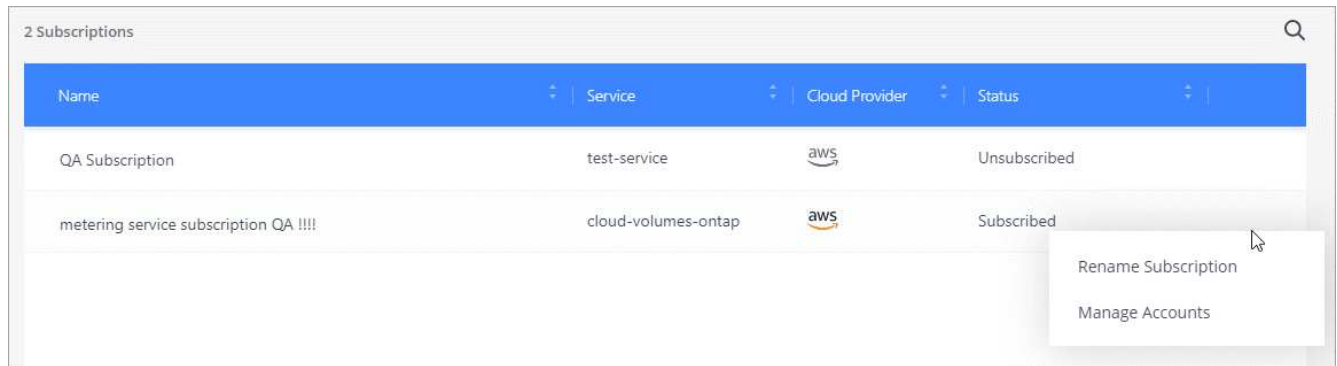
### "구독에 대해 자세히 알아보십시오".

#### 단계

1. Cloud Manager 상단에서 \* 계정 \* 드롭다운을 클릭하고 \* 계정 관리 \* 를 클릭합니다.
2. 구독 \* 을 클릭합니다.

현재 보고 있는 계정과 연결된 구독만 표시됩니다.

3. 관리할 구독에 해당하는 행의 작업 메뉴를 클릭합니다.



4. 구독의 이름을 바꾸거나 구독과 연결된 계정을 관리하도록 선택합니다.

#### 계정 이름을 변경하는 중입니다

언제든지 계정 이름을 변경하여 의미 있는 내용으로 바꿀 수 있습니다.

#### 단계

1. Cloud Manager 상단에서 \* 계정 \* 드롭다운을 클릭하고 \* 계정 관리 \* 를 클릭합니다.
2. 개요 \* 탭에서 계정 이름 옆에 있는 편집 아이콘을 클릭합니다.
3. 새 계정 이름을 입력하고 \* 저장 \* 을 클릭합니다.

#### 개인 미리 보기 허용

계정의 프라이빗 미리 보기를 통해 Cloud Manager에서 미리 보기로 제공되는 새로운 NetApp 클라우드 서비스에 액세스할 수 있습니다.

개인 미리 보기의 서비스는 예상대로 작동하지 않을 뿐만 아니라 중단 및 기능 누락이 발생할 수 있습니다.

#### 단계

1. Cloud Manager 상단에서 \* 계정 \* 드롭다운을 클릭하고 \* 계정 관리 \* 를 클릭합니다.
2. 개요 \* 탭에서 \* 개인 미리 보기 허용 \* 설정을 활성화합니다.

## 타사 서비스 허용

계정의 타사 서비스가 Cloud Manager에서 사용 가능한 타사 서비스에 액세스할 수 있도록 허용합니다. 타사 서비스는 NetApp에서 제공하는 서비스와 유사한 클라우드 서비스이지만 타사의 관리 및 지원을 받습니다.

### 단계

1. Cloud Manager 상단에서 \* 계정 \* 드롭다운을 클릭하고 \* 계정 관리 \* 를 클릭합니다.
2. 개요 \* 탭에서 \* 타사 서비스 허용 \* 설정을 활성화합니다.

## SaaS 플랫폼 비활성화

회사의 보안 정책을 준수할 필요가 없는 한 SaaS 플랫폼을 사용하지 않는 것이 좋습니다. SaaS 플랫폼을 사용하지 않도록 설정하면 NetApp의 통합 클라우드 서비스를 사용할 수 없게 됩니다.

SaaS 플랫폼을 사용하지 않도록 설정하는 경우 Cloud Manager에서 다음 서비스를 사용할 수 없습니다.

- 클라우드 데이터 감지
- 쿠버네티스
- 클라우드 계층화
- 글로벌 파일 캐시

SaaS 플랫폼을 사용하지 않도록 설정하는 경우 에서 모든 작업을 수행해야 합니다 ["Connector에서 사용할 수 있는 로컬 사용자 인터페이스입니다"](#).



이 작업은 되돌릴 수 없는 작업으로 Cloud Manager SaaS 플랫폼을 사용할 수 없습니다. 로컬 커넥터에서 작업을 수행해야 합니다. NetApp의 다양한 통합 클라우드 서비스를 사용할 수 없으며 SaaS 플랫폼을 재활용하려면 NetApp의 지원이 필요합니다.

### 단계

1. Cloud Manager 상단에서 \* 계정 \* 드롭다운을 클릭하고 \* 계정 관리 \* 를 클릭합니다.
2. 개요 탭에서 옵션을 전환하여 SaaS 플랫폼 사용을 비활성화합니다.

## 계정 내 작업 모니터링

Cloud Manager에서 수행하는 작업의 상태를 모니터링하여 해결해야 할 문제가 있는지 확인할 수 있습니다. 알림 센터, 시각표에서 상태를 보거나 이메일로 알림을 보낼 수 있습니다.

이 표에서는 각 에서 제공해야 할 사항을 이해할 수 있도록 알림 센터와 일정을 비교합니다.


| 알림 센터  | 타임라인                                   |
|--|--|
| 이벤트 및 작업에 대한 상위 상태를 표시합니다                            | 추가 조사를 위한 각 이벤트 또는 조치에 대한 세부 정보를 제공합니다 |
| 현재 로그인 세션의 상태를 표시합니다. 로그오프한 후에는 알림 센터에 정보가 나타나지 않습니다 | 지난 달의 상태를 유지합니다                        |
| 사용자 인터페이스에서 시작된 작업만 표시합니다                            | UI 또는 API의 모든 작업을 표시합니다                |

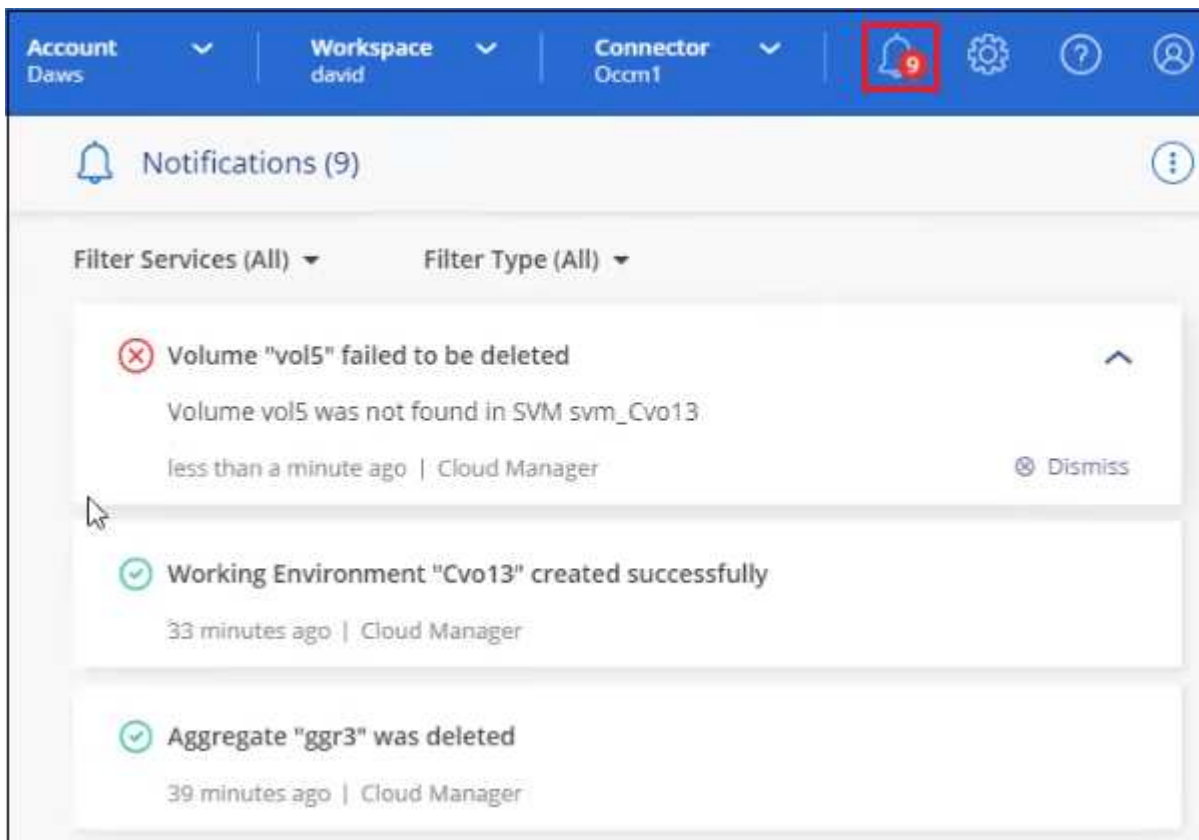


|  |  |
|--|--|
| 알림 센터  | 타임라인   |
| 사용자가 시작한 작업을 표시합니다                           | 사용자가 시작했는지 또는 시스템이 시작되었는지에 관계없이 모든 작업을 표시합니다 |
| 중요도에 따라 결과를 필터링합니다                           | 서비스, 작업, 사용자, 상태 등을 기준으로 필터링합니다              |
| 계정 사용자 및 다른 사용자에게 알림을 이메일로 보낼 수 있는 기능을 제공합니다 | 이메일 기능이 없습니다                                 |

### 알림 센터를 사용하여 활동 모니터링

알림은 Cloud Manager에서 시작한 작업의 진행률을 추적하므로 작업의 성공 여부를 확인할 수 있습니다. 이 뷰를 사용하면 현재 로그인 세션 중에 시작한 많은 Cloud Manager 작업의 상태를 볼 수 있습니다. 현재 모든 서비스에서 알림 센터에 정보를 보고하는 것은 아닙니다.

알림 벨()를 선택합니다. 벨의 작은 거품의 색상은 활성 상태인 최상위 심각도 알림을 나타냅니다. 따라서 빨간색 기포가 나타나면 확인해야 할 중요한 알림이 있다는 의미입니다.



또한 Cloud Manager를 구성하여 시스템에 로그인하지 않은 경우에도 중요한 시스템 작업을 확인할 수 있도록 이메일로 알림을 보낼 수 있습니다. 이메일은 NetApp 클라우드 계정의 일부인 Cloud Central 사용자 또는 특정 유형의 시스템 활동을 알아야 하는 다른 수신자에게 보낼 수 있습니다. 을 참조하십시오 [이메일 알림 설정 설정](#) 아래에 있습니다.

### 알림 유형

알림은 다음 범주로 분류됩니다.

| 알림 유형입니다 | 설명   |
|----------|--|
| 심각       | 수정 조치를 즉시 취하지 않으면 서비스가 중단될 수 있는 문제가 발생했습니다.  |
| 오류       | 조치 또는 프로세스가 실패로 끝나거나 시정 조치가 취해지지 않을 경우 실패로 이어질 수 있습니다.                                     |
| 경고       | 심각한 심각도에 도달하지 않도록 주의해야 할 문제입니다. 이 심각도에 대한 알림은 서비스 중단을 유발하지 않으며 즉각적인 수정 조치가 필요하지 않을 수 있습니다. |
| 권장 사항    | 시스템 또는 특정 서비스 개선을 위한 조치를 취할 것을 권장하는 시스템 권장 사항(예: 비용 절감, 새로운 서비스 제안, 권장 보안 구성 등)            |
| 정보       | 작업 또는 프로세스에 대한 추가 정보를 제공하는 메시지입니다.   |
| 성공       | 작업 또는 프로세스가 성공적으로 완료되었습니다.   |

알림을 필터링하는 중입니다

기본적으로 모든 알림이 표시됩니다. 알림 센터에 표시되는 알림을 필터링하여 사용자에게 중요한 알림만 표시할 수 있습니다. Cloud Manager "서비스" 및 알림 "유형"별로 필터링할 수 있습니다.

예를 들어, Cloud Manager 작업에 대한 "오류" 및 "경고" 알림만 표시하려면 해당 항목을 선택하면 해당 유형의 알림만 표시됩니다.

#### 이메일 알림 설정 설정

Cloud Manager에 로그인하지 않아도 특정 유형의 알림을 이메일로 전송하여 중요한 시스템 활동을 확인할 수 있습니다. 이메일은 NetApp 계정의 일부인 사용자나 특정 유형의 시스템 활동을 알아야 하는 다른 수신자에게 보낼 수 있습니다.

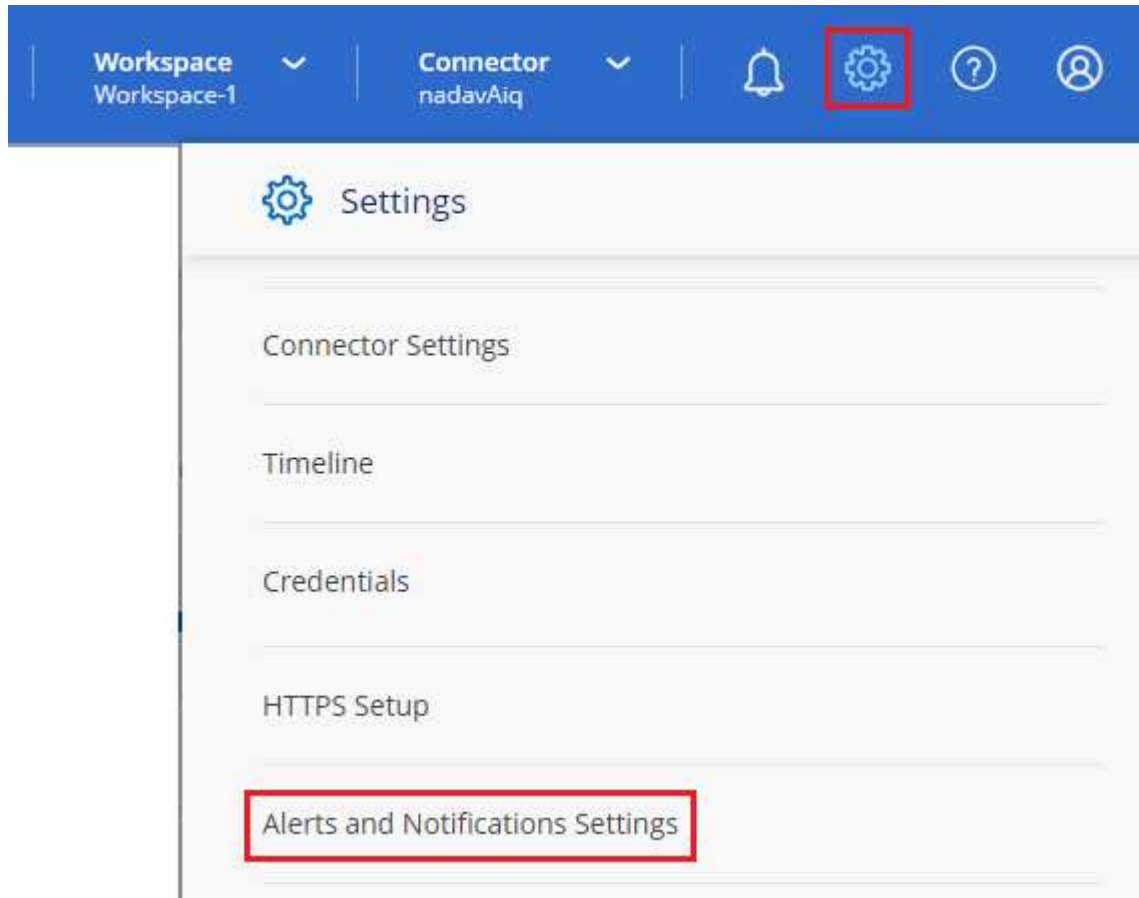
- 참고: \* Connector가 인터넷에 연결되지 않은 사이트에 설치된 경우 이메일 알림 전송은 지원되지 않습니다.

기본적으로 계정 관리자는 모든 "중요" 및 "권장 사항" 알림에 대한 이메일을 받게 됩니다. 다른 모든 사용자와 수신자는 기본적으로 알림 이메일을 수신하지 않도록 구성되어 있습니다.

알림 설정을 사용자 지정하려면 계정 관리자여야 합니다.

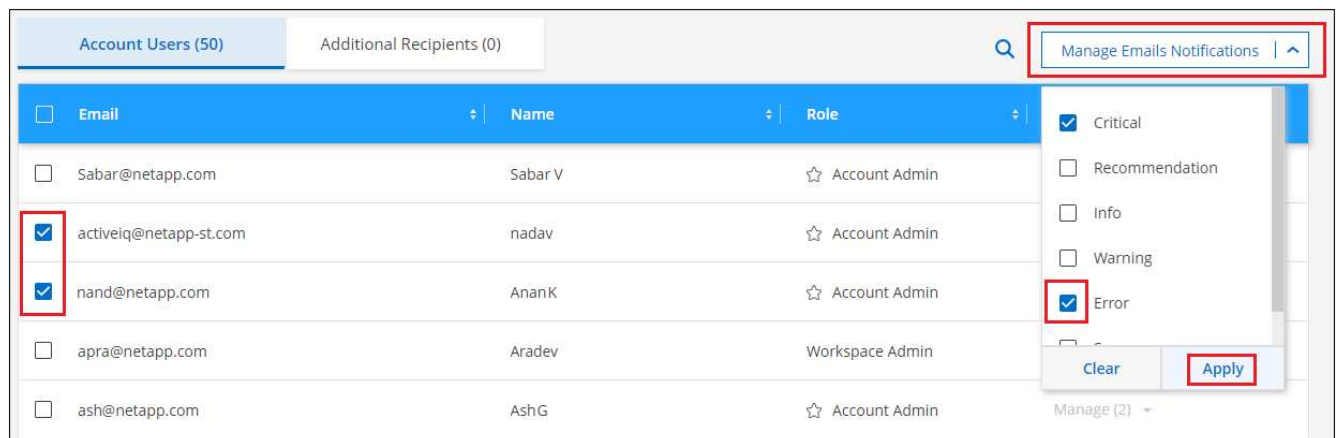
단계

1. Cloud Manager 메뉴 표시줄에서 \* 설정 > 알림 및 알림 설정 \* 을 클릭합니다.



2. 계정 사용자\_탭 또는 \_Additional Recipients\_tab에서 사용자 또는 여러 사용자를 선택하고 보낼 알림 유형을 선택합니다.

- 단일 사용자를 변경하려면 해당 사용자의 알림 옆에 있는 메뉴를 클릭하고 보낼 알림 유형을 선택한 다음 \* 적용 \* 을 클릭합니다.
- 여러 사용자를 변경하려면 각 사용자에 대한 확인란을 선택하고 \* 이메일 알림 관리 \* 를 클릭한 후 전송할 알림 유형을 선택하고 \* 적용 \* 을 클릭합니다.

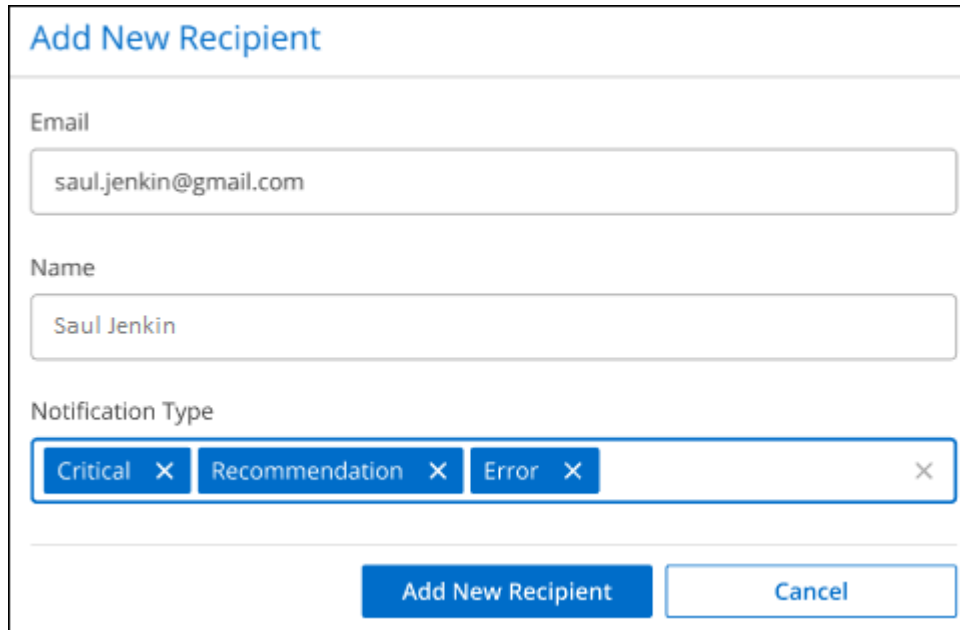


## 추가 이메일 수신자 추가

Account Users\_Tab에 표시되는 사용자는 NetApp 계정의 사용자(에서)로부터 자동으로 채워집니다 "[계정 관리 페이지](#)")를 클릭합니다. Cloud Manager에 액세스할 수 없지만 특정 유형의 경고와 알림에 대해 알림을 받아야 하는 다른 사람 또는 그룹에 대해서는 \_Additional Recipients\_tab에서 이메일 주소를 추가할 수 있습니다.

### 단계

1. 알림 및 알림 설정 페이지에서 \* 새 받는 사람 추가 \* 를 클릭합니다.



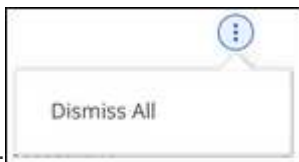
The image shows a form titled "Add New Recipient". It contains three input fields: "Email" with the value "saul.jenkin@gmail.com", "Name" with the value "Saul Jenkin", and "Notification Type" which is a multi-select dropdown menu containing "Critical", "Recommendation", and "Error". At the bottom of the form are two buttons: "Add New Recipient" and "Cancel".

2. 이름, 이메일 주소를 입력하고 수신인이 수신할 알림 유형을 선택한 다음 \* 새 수신자 추가 \* 를 클릭합니다.

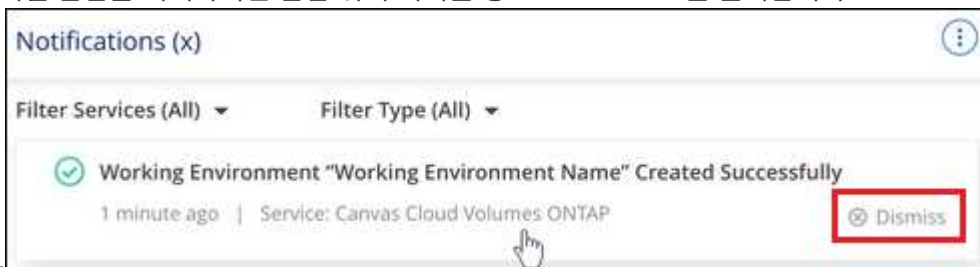
### 알림을 해제합니다

더 이상 알림을 볼 필요가 없는 경우 페이지에서 알림을 제거할 수 있습니다. 모든 알림을 한 번에 해제하거나 개별 알림을 해제할 수 있습니다.

모든 알림을 해제하려면 알림 센터에서 을 클릭합니다 : 를 선택하고 \* 모두 해제 \* 를 선택합니다



개별 알림을 해제하려면 알림 위에 커서를 놓고 \* Dismiss \* 를 클릭합니다



## 사용자 계정의 사용자 활동 감사

Cloud Manager의 타임라인에는 사용자가 계정 관리를 위해 완료한 작업이 표시됩니다. 여기에는 사용자 연결, 작업 영역 만들기, 커넥터 만들기 등의 관리 작업이 포함됩니다.

특정 작업을 수행한 사람을 확인해야 하거나 작업의 상태를 확인해야 하는 경우 시간 표시 막대를 확인하는 것이 도움이 됩니다.

### 단계

1. Cloud Manager 메뉴 표시줄에서 \* 설정 > 타임라인 \* 을 클릭합니다.
2. 필터 아래에서 \* 서비스 \* 를 클릭하고 \* 임차 \* 를 활성화한 다음 \* 적용 \* 을 클릭합니다.

계정 관리 작업이 표시되도록 타임라인이 업데이트됩니다.

### 역할

계정 관리자, 작업 영역 관리자, 규정 준수 뷰어 및 SnapCenter 관리자 역할은 사용자에게 특정 권한을 제공합니다.

Compliance Viewer 역할은 읽기 전용 클라우드 데이터 감지 액세스를 위한 것입니다.

| 작업                            | 계정 관리자 | 작업 영역 관리자 | 규정 준수 뷰어 | SnapCenter 관리자 |
|-------------------------------|--------|-----------|----------|----------------|
| 작업 환경 관리                      | 예      | 예         | 아니요      | 아니요            |
| 작업 환경에 대한 서비스를 활성화합니다         | 예      | 예         | 아니요      | 아니요            |
| 데이터 복제 상태를 봅니다                | 예      | 예         | 아니요      | 아니요            |
| 타임라인을 봅니다                     | 예      | 예         | 아니요      | 아니요            |
| 작업 공간 간 전환                    | 예      | 예         | 예        | 아니요            |
| 데이터 감지 스캔 결과를 봅니다             | 예      | 예         | 예        | 아니요            |
| 작업 환경을 삭제합니다                  | 예      | 아니요       | 아니요      | 아니요            |
| Kubernetes 클러스터를 작업 환경에 연결    | 예      | 아니요       | 아니요      | 아니요            |
| Cloud Volumes ONTAP 보고서를 받습니다 | 예      | 아니요       | 아니요      | 아니요            |
| 커넥터 작성                        | 예      | 아니요       | 아니요      | 아니요            |
| NetApp 계정 관리                  | 예      | 아니요       | 아니요      | 아니요            |
| 자격 증명 관리                      | 예      | 아니요       | 아니요      | 아니요            |
| Cloud Manager 설정을 수정합니다       | 예      | 아니요       | 아니요      | 아니요            |
| 지원 대시보드 보기 및 관리               | 예      | 아니요       | 아니요      | 아니요            |
| Cloud Manager에서 작업 환경을 제거합니다  | 예      | 아니요       | 아니요      | 아니요            |

| 작업                    | 계정 관리자 | 작업 영역 관리자 | 규정 준수 뷰어 | SnapCenter 관리자 |
|-----------------------|--------|-----------|----------|----------------|
| HTTPS 인증서를 설치합니다      | 예      | 아니요       | 아니요      | 아니요            |
| SnapCenter 서비스를 사용합니다 | 예      | 예         | 아니요      | 예              |

#### 관련 링크

- ["NetApp 계정의 작업 공간 및 사용자 설정"](#)
- ["NetApp 계정의 작업 공간 및 사용자 관리"](#)

## 커넥터

### 고급 구축

**AWS Marketplace**에서 **Connector**를 생성합니다

Cloud Manager에서 직접 Connector를 생성하는 것이 가장 좋지만 AWS 액세스 키를 지정하지 않는 경우 AWS Marketplace에서 Connector를 시작할 수 있습니다. Connector를 만들고 설정하면 Cloud Manager는 새 작업 환경을 만들 때 이 커넥터를 자동으로 사용합니다.

#### 단계

1. AWS에서 권한 설정:
  - a. IAM 콘솔에서 의 내용을 복사하여 붙여넣어 고유한 정책을 만듭니다 ["Connector에 대한 IAM 정책"](#).
  - b. Amazon EC2 역할 유형으로 IAM 역할을 생성하고 이전 단계에서 생성한 정책을 역할에 연결합니다.
2. 이제 로 이동합니다 ["Cloud Manager 페이지로 이동하여 AWS 마켓플레이스를 확인하십시오"](#) AMI에서 Cloud Manager를 구축합니다.

IAM 사용자는 AWS Marketplace 권한을 가지고 있어야 가입 및 가입 해제할 수 있습니다.

3. Marketplace 페이지에서 \* Continue to Subscribe \* 를 클릭한 다음 \* Continue to Configuration \* 을 클릭합니다.

**a**

Cloud Manager - Manual Installation without access keys

By: [NetApp, Inc.](#) Latest Version: 3.8.4

Read below for instructions on how to deploy Cloud Volumes ONTAP.

Linux/Unix ★★★★★ 6 AWS reviews

Typical Total Price  
**\$0.226/hr**  
Total pricing per instance for services hosted on t3.xlarge in US East (N. Virginia). [View Details](#)

Continue to Subscribe

Save to List

Overview Pricing Usage Support Reviews

### Product Overview

Do NOT subscribe on this page unless instructed by NetApp or redirected here from the NetApp website.

This listing lets you manually launch a Cloud Manager instance without providing your AWS credentials. After launching the Cloud Manager software in AWS, you can access it by entering the instance's IP address in a web browser. If you subscribe here, you still need to subscribe on the listing below for PAYGO charges.

### Highlights

- See Product Overview for instructions on how to deploy NetApp Cloud Manager.

**b**

Cloud Manager - Manual Installation without access keys

Continue to Configuration

< Product Detail Subscribe

### Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

### Terms and Conditions

#### NetApp, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

4. 기본 옵션을 변경하고 \* 계속 시작 \* 을 클릭합니다.

5. 작업 선택 \* 에서 \* EC2 \* 를 통해 시작 \* 을 선택한 다음 \* 시작 \* 을 클릭합니다.

다음 단계에서는 콘솔에서 IAM 역할을 Cloud Manager 인스턴스에 연결할 수 있으므로 EC2 콘솔에서 인스턴스를 시작하는 방법을 설명합니다. 웹 사이트에서 시작 \* 작업을 사용하면 이 작업을 수행할 수 없습니다.

6. 프롬프트에 따라 인스턴스를 구성하고 배포합니다.

- \* 인스턴스 유형 선택 \*: 지역 가용성에 따라 지원되는 인스턴스 유형 중 하나를 선택합니다(T3.xLarge가 권장됨).

"인스턴스 요구 사항을 검토합니다".

- \* 인스턴스 구성 \*: VPC 및 서브넷을 선택하고, 1단계에서 만든 IAM 역할을 선택하고, 종료 보호를 활성화하고 (권장), 요구 사항을 충족하는 다른 구성 옵션을 선택합니다.

|                               |   |   |
|-------------------------------|---|---|
| Number of instances           | 1   | <a href="#">Launch into Auto Scaling Group</a>  |
| Purchasing option             | <input type="checkbox"/> Request Spot instances   |   |
| Network                       | vpc-a76d91c2   VPC4QA (default)   | <a href="#">Create new VPC</a>                  |
| Subnet                        | subnet-39536c13   QASubnet1   us-east-1b<br>155 IP Addresses available                                      | <a href="#">Create new subnet</a>               |
| Auto-assign Public IP         | Enable  |   |
| Placement group               | <input type="checkbox"/> Add instance to placement group  |   |
| Capacity Reservation          | Open  | <a href="#">Create new Capacity Reservation</a> |
| IAM role                      | Cloud_Manager   | <a href="#">Create new IAM role</a>             |
| CPU options                   | <input type="checkbox"/> Specify CPU options  |   |
| Shutdown behavior             | Stop  |   |
| Enable termination protection | <input checked="" type="checkbox"/> Protect against accidental termination                                  |   |
| Monitoring                    | <input type="checkbox"/> Enable CloudWatch detailed monitoring<br><a href="#">Additional charges apply.</a> |   |

- \* 스토리지 추가 \*: 기본 스토리지 옵션을 유지합니다.
- \* 태그 추가 \*: 필요한 경우 인스턴스에 대한 태그를 입력합니다.
- \* 보안 그룹 구성 \*: 커넥터 인스턴스에 필요한 연결 방법(SSH, HTTP 및 HTTPS)을 지정합니다.
- \* 검토 \*: 선택 사항을 검토하고 \* 시작 \* 을 클릭합니다.

AWS가 지정된 설정으로 소프트웨어를 시작합니다. Connector 인스턴스 및 소프트웨어는 약 5분 내에 실행되어야 합니다.

- Connector 인스턴스에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

`http://ipaddress:80`

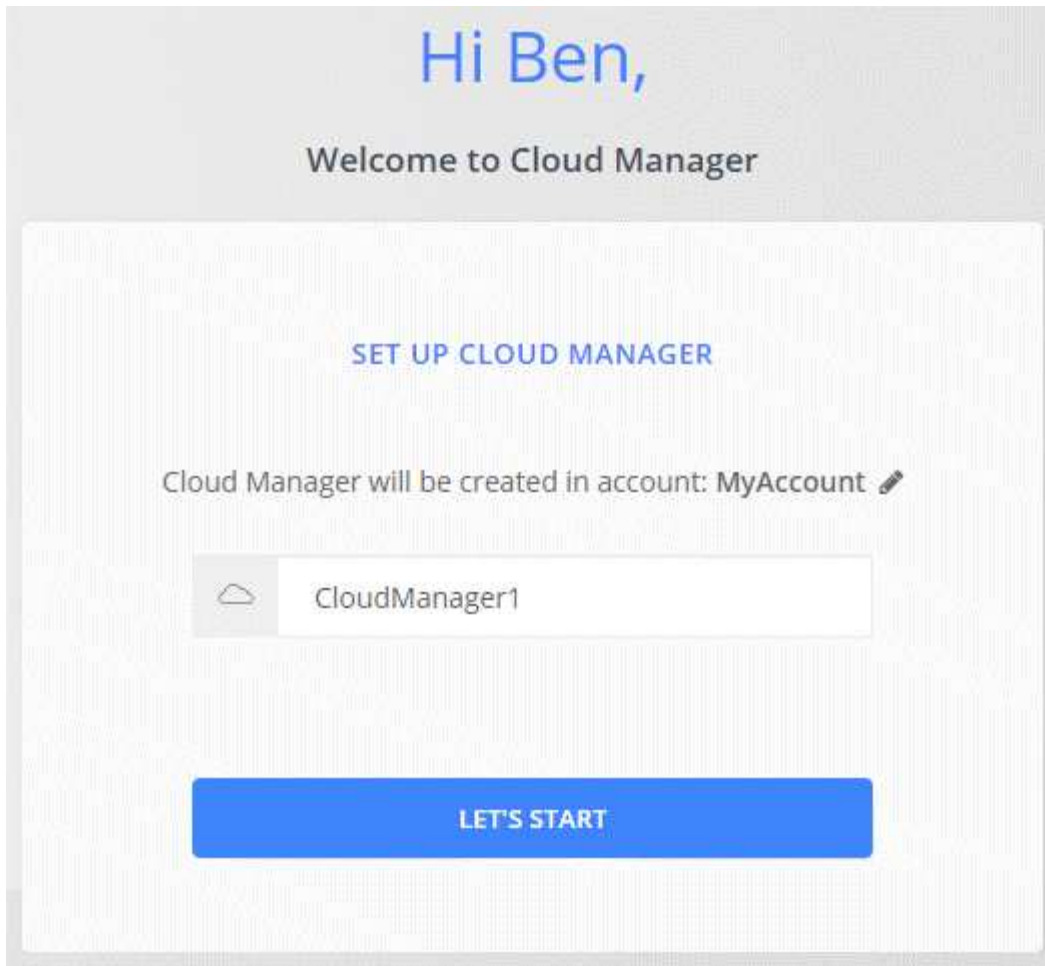
- 로그인한 후 Connector를 설정합니다.

- Connector와 연결할 NetApp 계정을 지정합니다.

["NetApp 계정 에 대해 알아보십시오"](#).

- 시스템의 이름을 입력합니다.





이제 Connector가 NetApp 계정으로 설치 및 설정됩니다. 새로운 작업 환경을 만들 때 Cloud Manager가 이 Connector를 자동으로 사용합니다. 그러나 둘 이상의 커넥터가 있는 경우 이 작업을 수행해야 합니다 ["둘 사이를 전환합니다"](#).

Connector를 생성한 동일한 AWS 계정에 Amazon S3 버킷이 있는 경우 Amazon S3 작업 환경이 Canvas에 자동으로 표시됩니다. ["이 작업 환경에서 수행할 수 있는 작업에 대해 자세히 알아보십시오"](#).

**Azure Marketplace**에서 **Connector**를 생성합니다

Cloud Manager에서 직접 Connector를 생성하는 것이 가장 좋지만 원하는 경우 Azure Marketplace에서 Connector를 실행할 수 있습니다. Connector를 만들고 설정하면 Cloud Manager는 새 작업 환경을 만들 때 이 커넥터를 자동으로 사용합니다.

**Azure**에서 커넥터 만들기

Azure Marketplace의 이미지를 사용하여 Azure에서 Connector를 구축한 다음 Connector에 로그인하여 NetApp 계정을 지정합니다.

단계

1. Azure 마켓플레이스에서 NetApp Connector VM 페이지로 이동합니다.
  - ["상용 지역에 대한 Azure Marketplace 페이지"](#)
  - ["Azure Government 지역의 Azure Marketplace 페이지"](#)

2. 지금 받기 \* 를 클릭한 다음 \* 계속 \* 을 클릭합니다.
3. Azure 포털에서 \* Create \* 를 클릭하고 다음 단계에 따라 가상 시스템을 구성합니다.

VM을 구성할 때 다음 사항에 유의하십시오.

- Cloud Manager는 HDD 또는 SSD 디스크를 최적의 상태로 사용할 수 있습니다.
- CPU 및 RAM 요구 사항에 맞는 VM 크기를 선택합니다. DS3 v2를 권장합니다.

"VM 요구 사항을 검토합니다".

- 네트워크 보안 그룹의 경우 Connector는 SSH, HTTP 및 HTTPS를 사용하는 인바운드 연결을 필요로 합니다.

"Connector의 보안 그룹 규칙에 대해 자세히 알아보십시오".

- 관리 \* 에서 \* 커기 \* 를 선택하여 커넥터에 대해 \* 시스템 할당 관리 ID \* 를 활성화합니다.

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

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

Azure는 지정된 설정으로 가상 머신을 구축합니다. 가상 머신 및 커넥터 소프트웨어는 약 5분 내에 실행되어야 합니다.

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

http://ipaddress:80[]

6. 로그인한 후 Connector를 설정합니다.

- a. Connector와 연결할 NetApp 계정을 지정합니다.

"NetApp 계정 에 대해 알아보십시오".

- b. 시스템의 이름을 입력합니다.



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

#### Azure 사용 권한 부여

Azure에서 커넥터를 배포한 경우 을 활성화해야 합니다 **"시스템에서 할당한 관리 ID입니다"**. 이제 사용자 지정 역할을 만든 다음 하나 이상의 구독에 대해 Connector 가상 머신에 역할을 할당하여 필요한 Azure 권한을 부여해야 합니다.

#### 단계

##### 1. 사용자 지정 역할 만들기:

- 의 내용을 복사합니다 **"Connector에 대한 사용자 지정 역할 권한"** JSON 파일에 저장합니다.
- 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

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

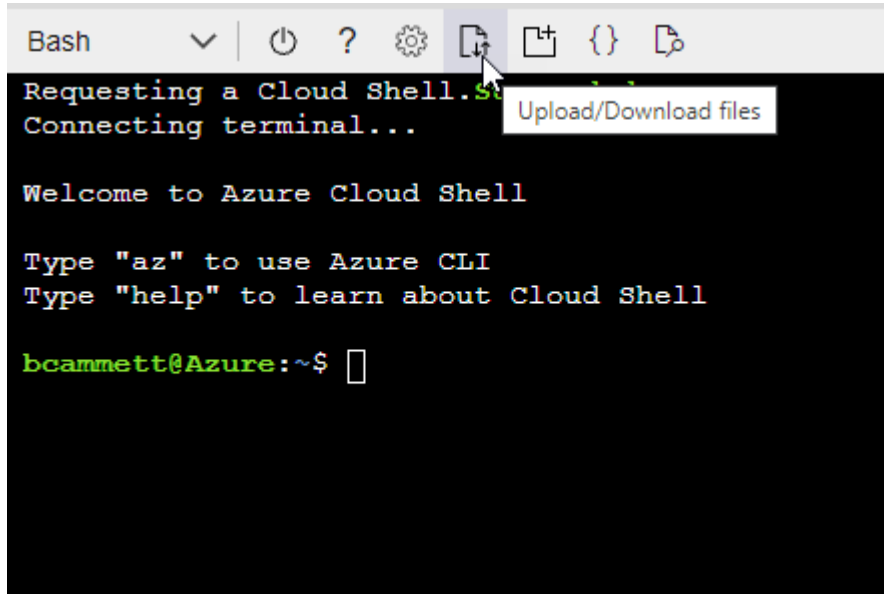
▪ 예 \*

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

c. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 생성합니다.

다음 단계에서는 Azure Cloud Shell에서 Bash를 사용하여 역할을 생성하는 방법을 설명합니다.

- 시작 "Azure 클라우드 셸" Bash 환경을 선택하십시오.
- JSON 파일을 업로드합니다.



- 다음 Azure CLI 명령을 입력합니다.

```
az role definition create --role-definition  
Policy_for_Setup_As_Service_Azure.json
```

이제 Connector 가상 머신에 할당할 수 있는 Cloud Manager Operator라는 사용자 지정 역할이 있어야 합니다.

2. 하나 이상의 구독에 대해 Connector 가상 머신에 역할을 할당합니다.

- a. Subscriptions \* 서비스를 연 다음 Cloud Volumes ONTAP 시스템을 배포할 구독을 선택합니다.
- b. IAM(Access Control) \* > \* 추가 \* > \* 역할 할당 추가 \* 를 클릭합니다.
- c. Role \* 탭에서 \* Cloud Manager Operator \* 역할을 선택하고 \* Next \* 를 클릭합니다.



Cloud Manager Operator는 Cloud Manager 정책에서 제공하는 기본 이름입니다. 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

d. Members\* 탭에서 다음 단계를 완료합니다.

- 관리되는 ID\*에 대한 액세스를 할당합니다.
- 구성원 선택 \* 을 클릭하고 Connector 가상 머신이 생성된 구독을 선택한 다음 \* 가상 머신 \* 을 선택하고 Connector 가상 머신을 선택합니다.
- 선택 \* 을 클릭합니다.

- 다음 \* 을 클릭합니다.
- e. 검토 + 할당 \* 을 클릭합니다.
- f. 추가 구독에서 Cloud Volumes ONTAP를 배포하려면 해당 구독으로 전환한 다음 이 단계를 반복합니다.

이제 Connector는 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하는 데 필요한 권한을 갖습니다. 새로운 작업 환경을 만들 때 Cloud Manager가 이 Connector를 자동으로 사용합니다. 그러나 둘 이상의 커넥터가 있는 경우 이 작업을 수행해야 합니다 ["둘 사이를 전환합니다"](#).

Connector를 만든 Azure 계정에 Azure Blob 저장소가 있는 경우 Canvas에 Azure Blob 작업 환경이 자동으로 표시됩니다. ["이 작업 환경에서 수행할 수 있는 작업에 대해 자세히 알아보십시오"](#).

인터넷에 액세스할 수 있는 기존 **Linux** 호스트에 커넥터를 설치합니다

Connector를 생성하는 가장 일반적인 방법은 Cloud Manager 또는 클라우드 공급자의 마켓플레이스에서 직접 생성하는 것입니다. 그러나 네트워크 또는 클라우드의 기존 Linux 호스트에 Connector 소프트웨어를 다운로드하여 설치할 수 있습니다. 이 단계는 인터넷 액세스가 있는 호스트에만 적용됩니다.

["커넥터를 배포하는 다른 방법에 대해 알아봅니다"](#).



Google Cloud에서 Cloud Volumes ONTAP 시스템을 만들려면 Google Cloud에서도 실행되는 커넥터가 있어야 합니다. AWS, Azure 또는 온프레미스에서 실행되는 Connector를 사용할 수 없습니다.

호스트 요구 사항을 확인합니다

Connector 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 포트 요구 사항 등을 충족하는 호스트에서 실행되어야 합니다.

전용 호스트가 필요합니다

다른 애플리케이션과 공유되는 호스트에서는 Connector가 지원되지 않습니다. 호스트는 전용 호스트여야 합니다.

## CPU

코어 4개 또는 vCPU 4개

## RAM

16GB

## AWS EC2 인스턴스 유형

위의 CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. T3.xLarge를 권장합니다.

## Azure VM 크기입니다

위의 CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. DS3 v2를 권장합니다.

## GCP 시스템 유형입니다

위의 CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. n1-standard-4를 권장합니다.

Connector는 를 지원하는 OS가 있는 VM 인스턴스의 Google Cloud에서 지원됩니다 ["차폐된 VM 기능"](#)

## 지원되는 운영 체제

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

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

Connector는 이러한 운영 체제의 영어 버전에서 지원됩니다.

## 하이퍼바이저

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

## /opt의 디스크 공간입니다

100GiB의 공간을 사용할 수 있어야 합니다

## /var의 디스크 공간입니다

20GiB의 공간을 사용할 수 있어야 합니다

## 아웃바운드 인터넷 액세스

Connector를 설치하고 Connector가 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하려면 아웃바운드 인터넷 액세스가 필요합니다. 끝점 목록은 을 참조하십시오 "[커넥터에 대한 네트워킹 요구 사항](#)".

## 커넥터를 설치합니다

지원되는 Linux 호스트가 있는지 확인한 후 Connector 소프트웨어를 받은 다음 설치할 수 있습니다.

커넥터를 설치하려면 루트 권한이 필요합니다.

## 이 작업에 대해

- 설치를 통해 AWS 명령줄 툴(awscli)을 설치하여 NetApp 지원으로부터 복구 절차를 수행할 수 있습니다.

awscli 설치에 실패했다는 메시지가 표시되면 메시지를 무시해도 됩니다. 도구 없이 커넥터가 제대로 작동할 수 있습니다.

- NetApp Support 사이트에서 제공되는 설치 프로그램은 이전 버전일 수 있습니다. 새 버전이 있는 경우 설치 후 커넥터가 자동으로 업데이트됩니다.

## 단계

1. 에서 Cloud Manager 소프트웨어를 다운로드합니다 "[NetApp Support 사이트](#)"를 선택한 다음 Linux 호스트에 복사합니다.

AWS에서 EC2 인스턴스에 파일을 연결하고 복사하는 방법은 를 참조하십시오 "[AWS 설명서: SSH를 사용하여 Linux 인스턴스에 연결](#)".

2. 스크립트를 실행할 권한을 할당합니다.

```
chmod +x OnCommandCloudManager-V3.9.19.sh
```

3. 설치 스크립트를 실행합니다.

프록시 서버가 있는 경우 아래와 같이 명령 매개 변수를 입력해야 합니다. 설치 프로그램에서 프록시에 대한 정보를 제공하라는 메시지를 표시하지 않습니다.

```
./OnCommandCloudManager-V3.9.19.sh [silent] [proxy=ipaddress]  
[proxyport=port] [proxyuser=user_name] [proxypwd=password]
```

\_silent\_는 정보를 묻지 않고 설치를 실행합니다.

호스트가 프록시 서버 뒤에 있으면 \_proxy\_가 필요합니다.

\_proxyPort\_는 프록시 서버의 포트입니다.

\_proxyuser\_는 기본 인증이 필요한 경우 프록시 서버의 사용자 이름입니다.

\_proxypwd\_는 지정한 사용자 이름의 암호입니다.

4. 자동 매개변수를 지정하지 않은 경우 \*Y\* 를 입력하여 설치를 계속합니다.

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

5. 웹 브라우저를 열고 다음 URL을 입력합니다.

[https://ipaddress\[\]](https://ipaddress[])

\_ipaddress\_는 호스트 구성에 따라 localhost, 개인 IP 주소 또는 공용 IP 주소일 수 있습니다. 예를 들어, Connector가 공용 IP 주소가 없는 공용 클라우드에 있는 경우 Connector 호스트에 대한 연결이 있는 호스트의 전용 IP 주소를 입력해야 합니다.

6. NetApp Cloud Central에 등록 하거나 로그인 하십시오.

7. Google Cloud에 Connector를 설치한 경우 Cloud Manager가 프로젝트에서 Cloud Volumes ONTAP 시스템을 만들고 관리하는 데 필요한 권한이 있는 서비스 계정을 설정합니다.

- a. "[GCP에서 역할을 생성합니다](#)" 여기에는 에 정의된 권한이 포함됩니다 "[GCP에 대한 커넥터 정책입니다](#)".
- b. "[GCP 서비스 계정을 생성하고 방금 생성한 사용자 지정 역할을 적용합니다](#)".
- c. "[이 서비스 계정을 Connector VM에 연결합니다](#)".

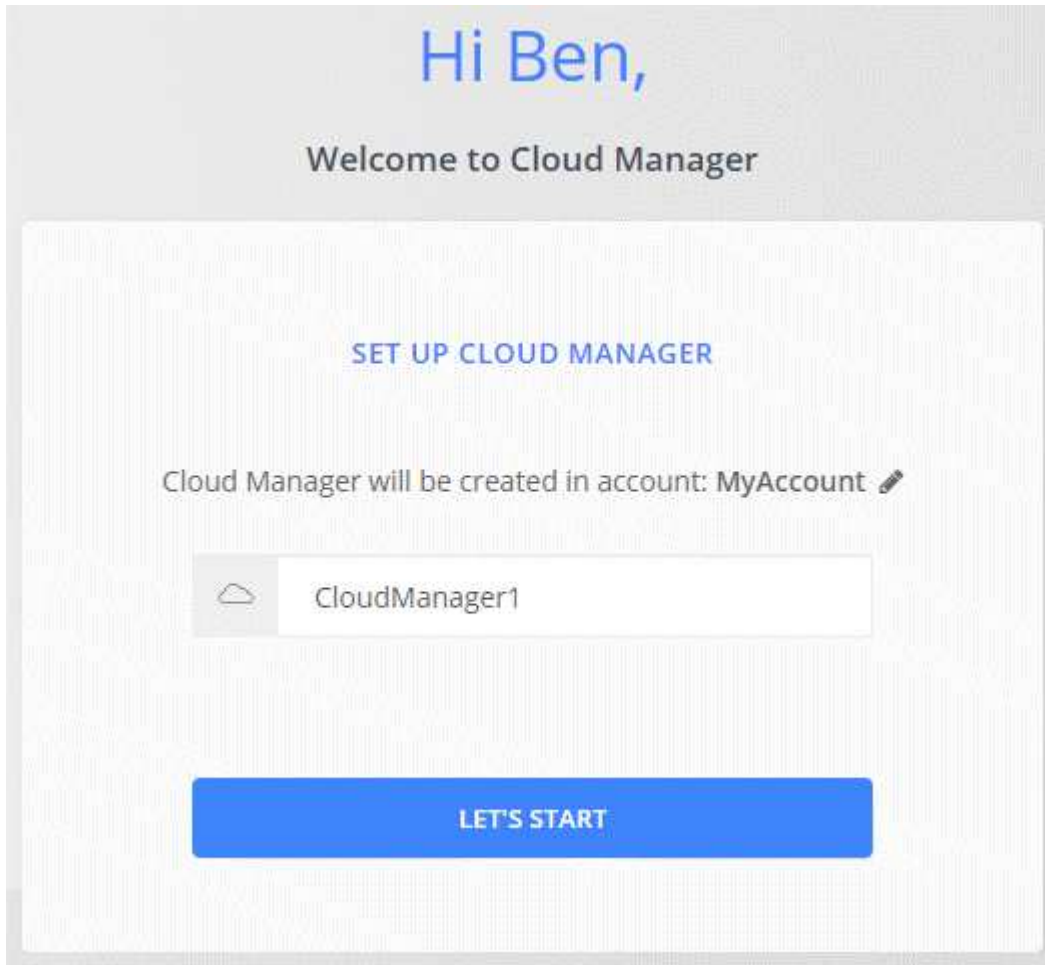
- d. 다른 프로젝트에 Cloud Volumes ONTAP를 배포하려는 경우 "[Cloud Manager 역할을 가진 서비스 계정을 해당 프로젝트에 추가하여 액세스 권한을 부여합니다](#)". 각 프로젝트에 대해 이 단계를 반복해야 합니다.

8. 로그인한 후 Cloud Manager를 설정합니다.

- a. Connector와 연결할 NetApp 계정을 지정합니다.

["NetApp 계정 에 대해 알아보십시오"](#).

- b. 시스템의 이름을 입력합니다.



이제 Connector가 NetApp 계정으로 설치 및 설정됩니다. 새로운 작업 환경을 만들 때 Cloud Manager가 이 Connector를 자동으로 사용합니다.

Cloud Manager가 퍼블릭 클라우드 환경 내에서 리소스 및 프로세스를 관리할 수 있도록 권한 설정:

- AWS: "[AWS 계정을 설정한 다음 Cloud Manager에 추가합니다](#)"
- Azure(Azure): "[Azure 계정을 설정한 다음 Cloud Manager에 추가합니다](#)"
- Google Cloud: 위의 7단계를 참조하십시오

인터넷에 접속하지 않고 커넥터를 내부에 설치합니다

인터넷에 액세스할 수 없는 온프레미스 Linux 호스트에 커넥터를 설치할 수 있습니다. 그런 다음,



온프레미스 ONTAP 클러스터를 검색하고, 클러스터 간에 데이터를 복제하고, 클라우드 백업을 사용하여 볼륨을 백업하고, 클라우드 데이터 센스로 검색할 수 있습니다.

이러한 설치 지침은 위에서 설명한 사용 사례를 위한 것입니다. ["커넥터를 배포하는 다른 방법에 대해 알아봅니다"](#).

호스트 요구 사항을 확인합니다

Connector 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 포트 요구 사항 등을 충족하는 호스트에서 실행되어야 합니다.

전용 호스트가 필요합니다

다른 애플리케이션과 공유되는 호스트에서는 Connector가 지원되지 않습니다. 호스트는 전용 호스트여야 합니다.

## CPU

코어 4개 또는 vCPU 4개

## RAM

16GB

지원되는 운영 체제

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

Red Hat Enterprise Linux 시스템은 Red Hat 서브스크립션 관리에 등록되어 있어야 합니다. 등록되지 않은 경우 시스템은 Connector 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.

Connector는 이러한 운영 체제의 영어 버전에서 지원됩니다.

하이퍼바이저

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

디스크 유형입니다

SSD가 필요합니다

/opt의 디스크 공간입니다

100GiB의 공간을 사용할 수 있어야 합니다

/var의 디스크 공간입니다

20GiB의 공간을 사용할 수 있어야 합니다

## Docker 엔진

커넥터를 설치하기 전에 호스트에 Docker Engine 버전 19 이상이 필요합니다. ["설치 지침을 봅니다"](#).

커넥터를 설치합니다

지원되는 Linux 호스트가 있는지 확인한 후 Connector 소프트웨어를 받은 다음 설치할 수 있습니다.

커넥터를 설치하려면 루트 권한이 필요합니다.

단계

1. Docker가 설정 및 실행 중인지 확인합니다.

```
sudo systemctl enable docker && sudo systemctl start docker
```

2. 에서 Cloud Manager 소프트웨어를 다운로드합니다 ["NetApp Support 사이트"](#).
3. Linux 호스트에 설치 프로그램을 복사합니다.
4. 스크립트를 실행할 권한을 할당합니다.

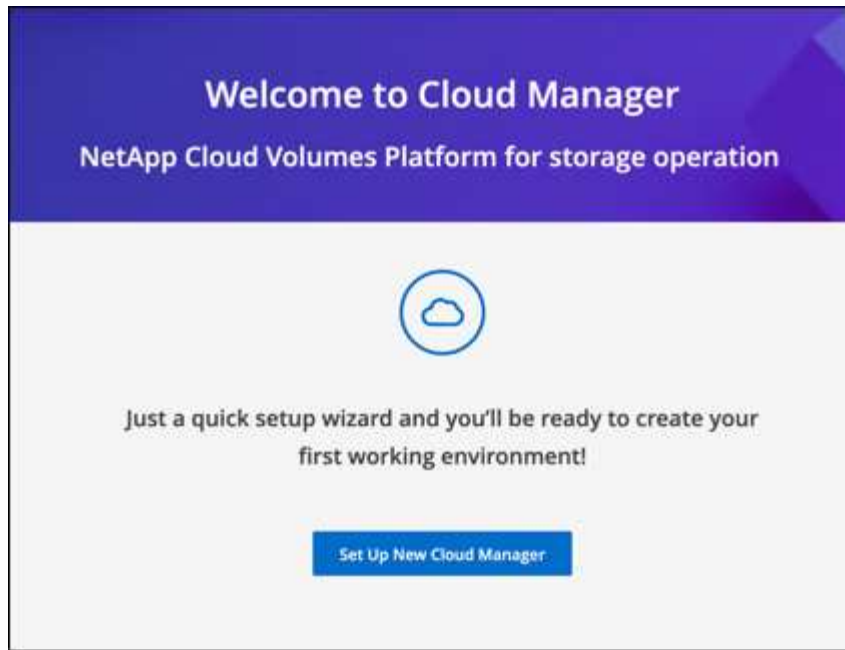
```
chmod +x /path/cloud-manager-connector-offline-v3.9.19
```

5. 설치 스크립트를 실행합니다.

```
sudo /path/cloud-manager-connector-offline-v3.9.19
```

6. 웹 브라우저를 열고 를 입력합니다 `https://ipaddress[]` 여기서 `_ipaddress_`는 Linux 호스트의 IP 주소입니다.

다음 화면이 나타납니다.



7. Set Up New Cloud Manager \* 를 클릭하고 화면의 지시에 따라 시스템을 설정합니다.

- \* 시스템 세부 정보 \*: Cloud Manager 시스템의 이름과 회사 이름을 입력합니다.

- \* 관리자 사용자 생성 \*: 시스템에 대한 관리자 사용자를 생성합니다.

이 사용자 계정은 시스템에서 로컬로 실행됩니다. NetApp Cloud Central과 연결되지 않았습니다.

- \* 검토 \*: 세부 정보를 검토하고 사용권 계약에 동의한 다음 \* 설정 \* 을 클릭합니다.

8. 방금 생성한 admin 사용자를 사용하여 Cloud Manager에 로그인합니다.

이제 Connector가 설치되어 다크 사이트 구축에 사용할 수 있는 Cloud Manager 기능을 사용할 수 있습니다.

다음 단계 's

- ["온프레미스 ONTAP 클러스터에 대해 알아보십시오"](#)
- ["온프레미스 ONTAP 클러스터 간에 데이터를 복제합니다"](#)

- "클라우드 백업을 사용하여 사내 ONTAP 볼륨 데이터를 StorageGRID에 백업합니다"
- "클라우드 데이터 센스를 사용하여 온프레미스 ONTAP 볼륨 데이터를 스캔합니다"

Connector 소프트웨어의 새 버전을 사용할 수 있으면 NetApp Support 사이트에 게시됩니다. "[Connector를 업그레이드하는 방법에 대해 알아보십시오](#)".

## 커넥터의 시스템 ID 찾기

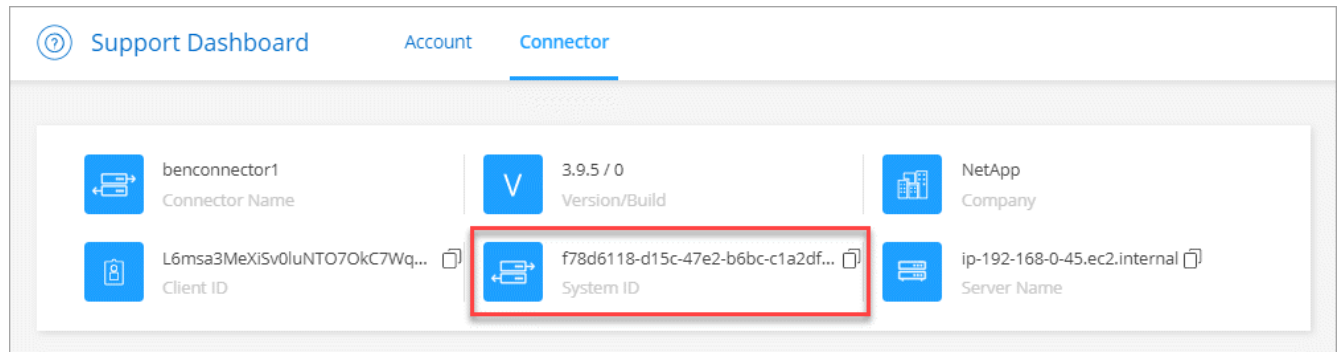
시작하려면 NetApp 담당자가 시스템 ID for Connector를 요청할 수 있습니다. ID는 일반적으로 라이선스 및 문제 해결 목적으로 사용됩니다.

단계

1. Cloud Manager 콘솔 오른쪽 위에서 도움말 아이콘을 클릭합니다.
2. 지원 > 커넥터 \* 를 클릭합니다.

시스템 ID가 맨 위에 나타납니다.

◦ 예 \*



## 기존 커넥터 관리

하나 이상의 커넥터를 만든 후에는 커넥터 간 전환, 커넥터에서 실행되는 로컬 사용자 인터페이스에 연결 등을 통해 커넥터를 관리할 수 있습니다.

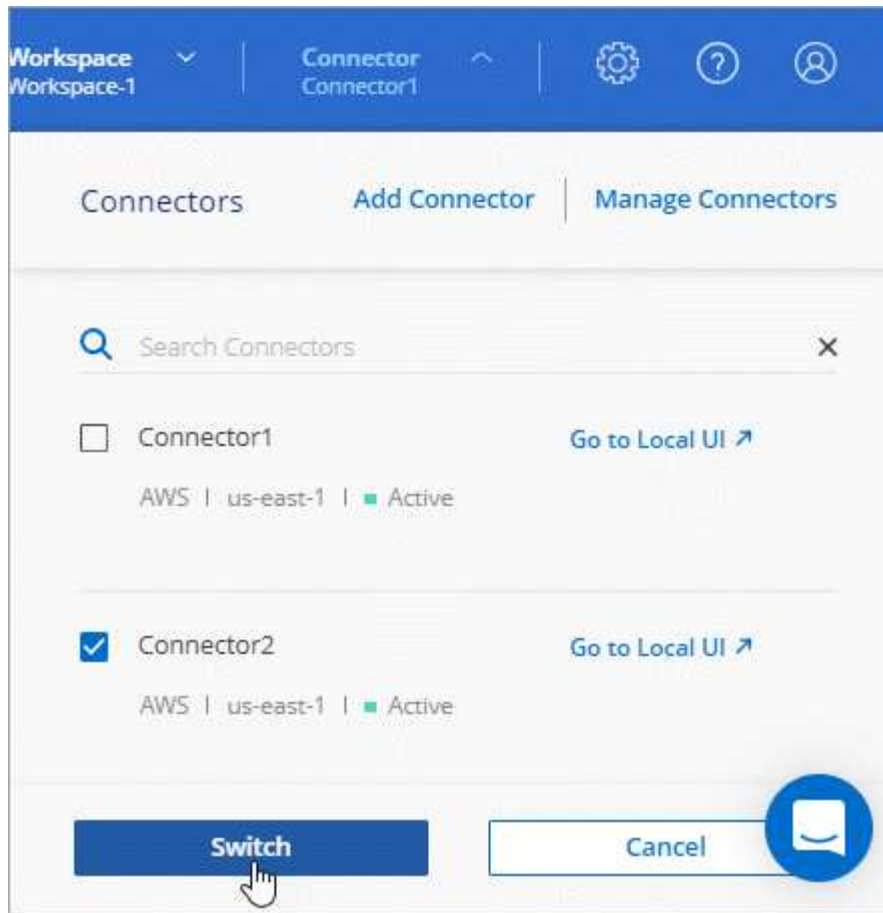
커넥터 사이를 전환합니다

커넥터가 여러 개 있는 경우 커넥터 사이를 전환하여 특정 커넥터와 연결된 작업 환경을 볼 수 있습니다.

예를 들어, 멀티클라우드 환경에서 일하고 있다고 가정해 보겠습니다. AWS에 Connector가 있고 Google Cloud에 Connector가 있을 수 있습니다. 이러한 클라우드에서 실행되는 Cloud Volumes ONTAP 시스템을 관리하려면 이러한 커넥터 사이를 전환해야 합니다.

단계

1. 커넥터 \* 드롭다운을 클릭하고 다른 커넥터를 선택한 다음 \* 스위치 \* 를 클릭합니다.



Cloud Manager는 선택한 커넥터와 연결된 작업 환경을 새로 고치고 표시합니다.

#### 로컬 UI에 액세스합니다

SaaS 사용자 인터페이스에서 거의 모든 작업을 수행해야 하지만 로컬 사용자 인터페이스는 Connector에서 계속 사용할 수 있습니다. 정부 지역 또는 아웃바운드 인터넷 액세스가 없는 사이트에서 Cloud Manager에 액세스하는 경우 Connector에서 실행되는 로컬 사용자 인터페이스를 사용해야 합니다.

#### 단계

1. 웹 브라우저를 열고 다음 URL을 입력합니다.

`https://ipaddress[]`

`_ipaddress_`는 호스트 구성에 따라 localhost, 개인 IP 주소 또는 공용 IP 주소일 수 있습니다. 예를 들어, Connector가 공용 IP 주소가 없는 공용 클라우드에 있는 경우 Connector 호스트에 대한 연결이 있는 호스트의 전용 IP 주소를 입력해야 합니다.

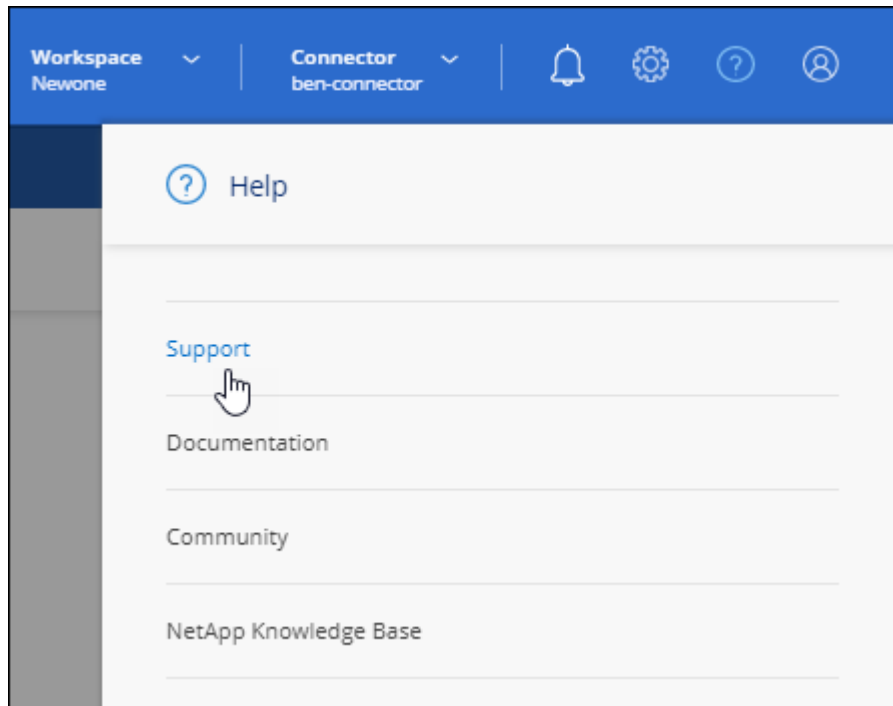
2. 로그인하려면 사용자 이름과 암호를 입력하십시오.

#### AutoSupport 메시지를 다운로드하거나 보냅니다

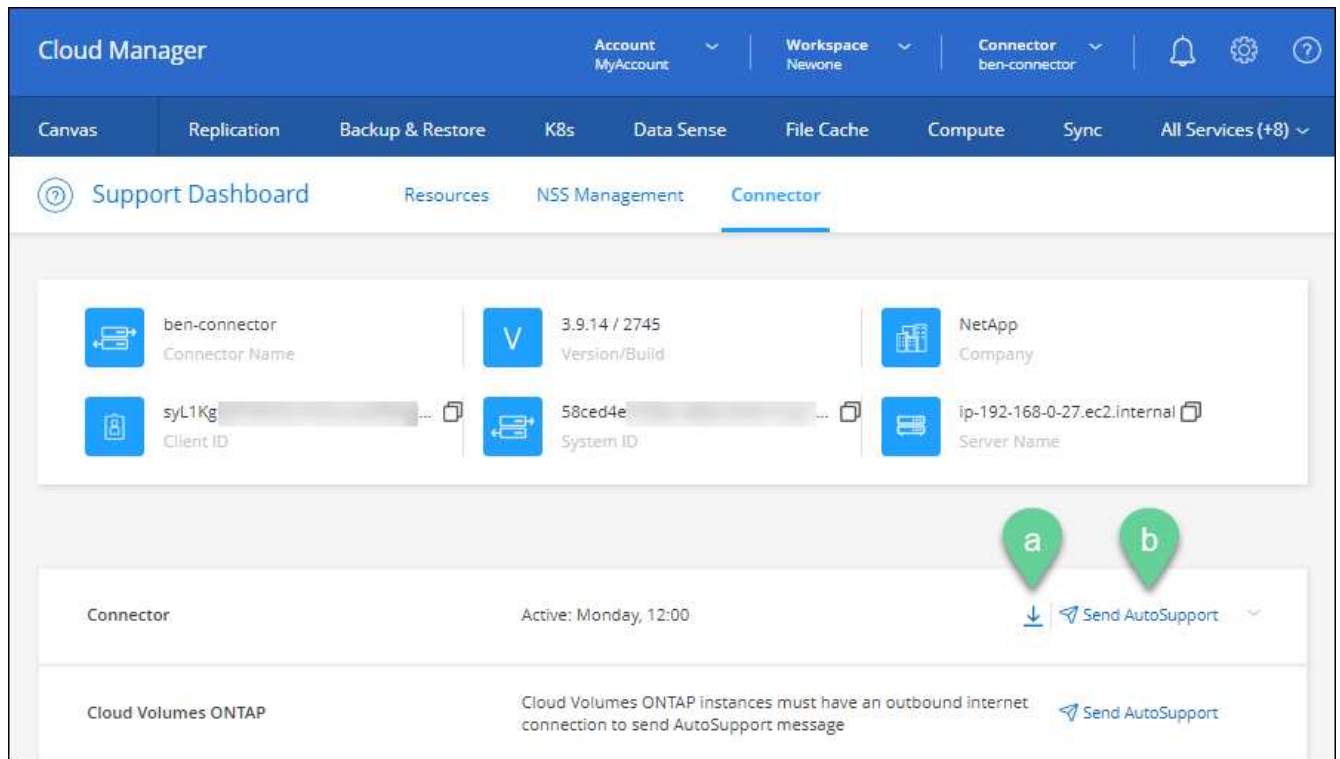
문제가 있는 경우 NetApp 직원이 문제 해결을 위해 NetApp 지원에 AutoSupport 메시지를 보내도록 요청할 수 있습니다.

#### 단계

1. 위의 섹션에 설명된 대로 Connector 로컬 UI에 연결합니다.
2. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 \* 지원 \* 을 선택합니다.



3. 커넥터 \* 를 클릭합니다.
4. NetApp 지원에 정보를 보내는 방법에 따라 다음 옵션 중 하나를 선택합니다.
  - a. 로컬 컴퓨터에 AutoSupport 메시지를 다운로드하는 옵션을 선택합니다. 그런 다음 원하는 방법을 사용하여 NetApp Support로 보낼 수 있습니다.
  - b. AutoSupport\* 전송을 클릭하여 메시지를 NetApp 지원팀에 직접 전송하십시오.



## Linux VM에 연결합니다

Connector가 실행되는 Linux VM에 연결해야 하는 경우 클라우드 공급자에서 제공하는 연결 옵션을 사용하여 연결할 수 있습니다.

### 설치하고

AWS에서 Connector 인스턴스를 생성한 경우 AWS 액세스 키와 암호 키를 제공했습니다. 이 키 쌍을 사용하여 인스턴스에 SSH를 사용할 수 있습니다.

["AWS Docs: Linux 인스턴스에 연결합니다"](#)

### Azure를 지원합니다

Azure에서 Connector VM을 생성한 경우 암호 또는 SSH 공개 키로 인증하도록 선택했습니다. VM에 연결하도록 선택한 인증 방법을 사용합니다.

["Azure Docs: VM에 SSH를 연결합니다"](#)

### Google 클라우드

Google Cloud에서 Connector를 만들 때는 인증 방법을 지정할 수 없습니다. 그러나 Google Cloud Console 또는 Google Cloud CLI(gcloud)를 사용하여 Linux VM 인스턴스에 연결할 수 있습니다.

["Google Cloud Docs: Linux VM에 연결합니다"](#)

### 보안 업데이트를 적용합니다

Connector의 운영 체제를 업데이트하여 최신 보안 업데이트로 패치되었는지 확인합니다.

## 단계

1. 커넥터 호스트에서 CLI 셸에 액세스합니다.
2. 상승된 권한으로 다음 명령을 실행합니다.

```
sudo -s
service service-manager stop
yum -y update --security
service service-manager start
```

## 커넥터의 IP 주소를 변경합니다

비즈니스에 필요한 경우 클라우드 공급자가 자동으로 할당하는 Connector 인스턴스의 내부 IP 주소와 공용 IP 주소를 변경할 수 있습니다.

## 단계

1. 클라우드 공급자의 지침에 따라 Connector 인스턴스의 로컬 IP 주소 또는 공용 IP 주소(또는 둘 다)를 변경합니다.
2. 공용 IP 주소를 변경한 경우 Connector에서 실행 중인 로컬 사용자 인터페이스에 연결해야 하는 경우 Connector 인스턴스를 다시 시작하여 Cloud Manager에 새 IP 주소를 등록합니다.
3. 전용 IP 주소를 변경한 경우 백업이 커넥터의 새 전용 IP 주소로 전송되도록 Cloud Volumes ONTAP 구성 파일의 백업 위치를 업데이트합니다.
  - a. Cloud Volumes ONTAP CLI에서 다음 명령을 실행하여 현재 백업 타겟을 제거합니다.

```
system configuration backup settings modify -destination ""
```

- b. Cloud Manager로 이동하여 작업 환경을 엽니다.
- c. 메뉴를 클릭하고 \* 고급 > 구성 백업 \* 을 선택합니다.
- d. 백업 대상 설정 \* 을 클릭합니다.

## Connector의 URI를 편집합니다

Connector에 대한 URI를 추가하고 제거합니다.

## 단계

1. Cloud Manager 헤더에서 \* Connector \* 드롭다운을 클릭합니다.
2. 커넥터 관리 \* 를 클릭합니다.
3. Connector에 대한 작업 메뉴를 클릭하고 \* URI 편집 \* 을 클릭합니다.
4. URI를 추가 및 제거한 다음 \* 적용 \* 을 클릭합니다.

## 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 Cloud Manager 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."](#)

인터넷에 접속하지 않고 **Connector**를 사내에서 업그레이드합니다

있다면 ["인터넷에 액세스할 수 없는 온프레미스 호스트에 커넥터를 설치했습니다"](#), 최신 버전이 NetApp Support 사이트에서 제공되는 경우 Connector를 업그레이드할 수 있습니다.

업그레이드 프로세스 중에 커넥터를 다시 시작해야 업그레이드 중에 사용자 인터페이스를 사용할 수 있습니다.

#### 단계

1. 에서 Cloud Manager 소프트웨어를 다운로드합니다 ["NetApp Support 사이트"](#).
2. Linux 호스트에 설치 프로그램을 복사합니다.
3. 스크립트를 실행할 권한을 할당합니다.

```
chmod +x /path/cloud-manager-connector-offline-v3.9.14
```

4. 설치 스크립트를 실행합니다.

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

5. 업그레이드가 완료되면 \* 도움말 > 지원 > 커넥터 \* 로 이동하여 커넥터 버전을 확인할 수 있습니다.

### 인터넷 액세스가 있는 호스트의 소프트웨어 업그레이드는 어떻습니까?

Connector는 소프트웨어가 있는 한 소프트웨어를 최신 버전으로 자동 업데이트합니다 ["아웃바운드 인터넷 액세스"](#) 를 클릭하여 소프트웨어 업데이트를 얻습니다.

## Cloud Manager에서 커넥터를 제거합니다

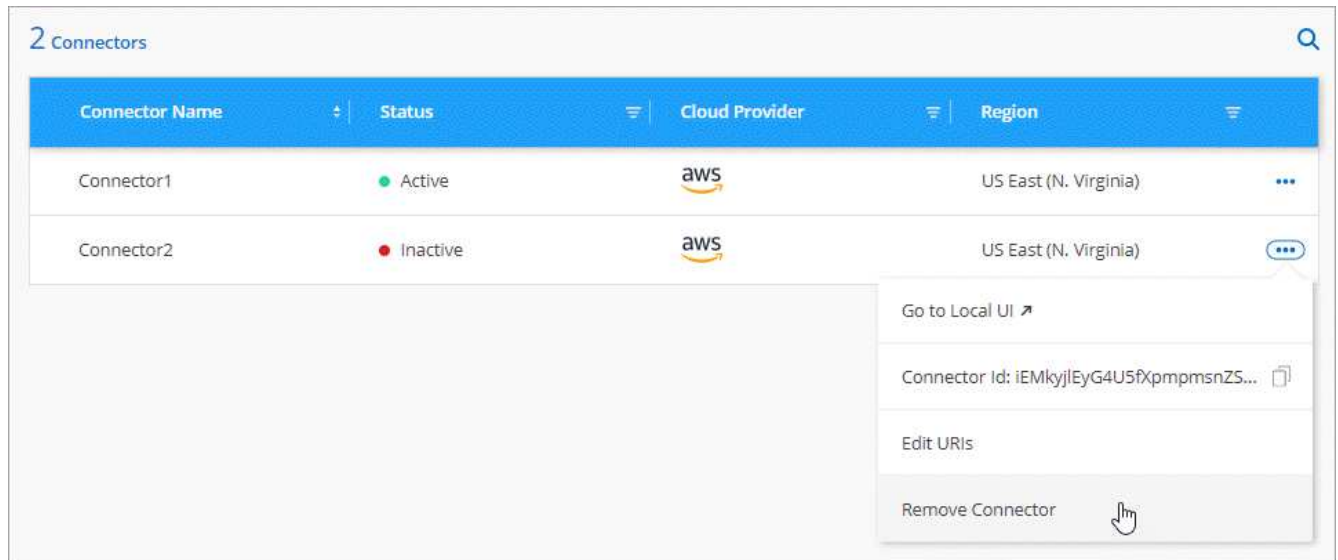
커넥터가 비활성 상태이면 Cloud Manager의 커넥터 목록에서 제거할 수 있습니다. Connector 가상 시스템을 삭제하거나 Connector 소프트웨어를 제거한 경우 이 작업을 수행할 수 있습니다.

커넥터 분리에 대한 내용은 다음과 같습니다.

- 이 작업은 가상 머신을 삭제하지 않습니다.
- 이 작업은 되돌릴 수 없습니다. Cloud Manager에서 커넥터를 제거한 후에는 Cloud Manager에 다시 추가할 수 없습니다.

단계

1. Cloud Manager 헤더에서 \* Connector \* 드롭다운을 클릭합니다.
2. 커넥터 관리 \* 를 클릭합니다.
3. 비활성 커넥터의 작업 메뉴를 클릭하고 \* 커넥터 제거 \* 를 클릭합니다.



4. 확인할 커넥터 이름을 입력한 다음 제거를 클릭합니다.

Cloud Manager는 레코드에서 Connector를 제거합니다.

## Connector 소프트웨어를 제거합니다

커넥터 소프트웨어를 제거하여 문제를 해결하거나 호스트에서 소프트웨어를 영구적으로 제거합니다. 필요한 단계는 인터넷 액세스가 있는 호스트에 커넥터를 설치했는지 아니면 인터넷 액세스가 없는 제한된 네트워크에 있는 호스트를 설치했는지에 따라 다릅니다.

인터넷 액세스 권한이 있는 호스트에서 제거합니다

온라인 커넥터에는 소프트웨어를 제거하는 데 사용할 수 있는 제거 스크립트가 포함되어 있습니다.

단계

1. Linux 호스트에서 제거 스크립트를 실행합니다.
  - `/opt/application/netapp/cloudmanager/bin/uninstall.sh [silent] *`

`_silent_`는 확인 메시지를 표시하지 않고 스크립트를 실행합니다.

인터넷에 액세스하지 않고 호스트에서 제거합니다

NetApp Support 사이트에서 Connector 소프트웨어를 다운로드하고 인터넷에 액세스할 수 없는 제한된 네트워크에 설치한 경우 다음 명령을 사용하십시오.

단계

1. Linux 호스트에서 다음 명령을 실행합니다.

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v  
rm -rf /opt/application/netapp/ds
```

## 보안 액세스를 위한 **HTTPS** 인증서 관리

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

시작하기 전에

Cloud Manager 설정을 변경하려면 먼저 Connector를 생성해야 합니다. ["자세히 알아보기"](#).

### HTTPS 인증서 설치

보안 액세스를 위해 CA에서 서명한 인증서를 설치합니다.

단계

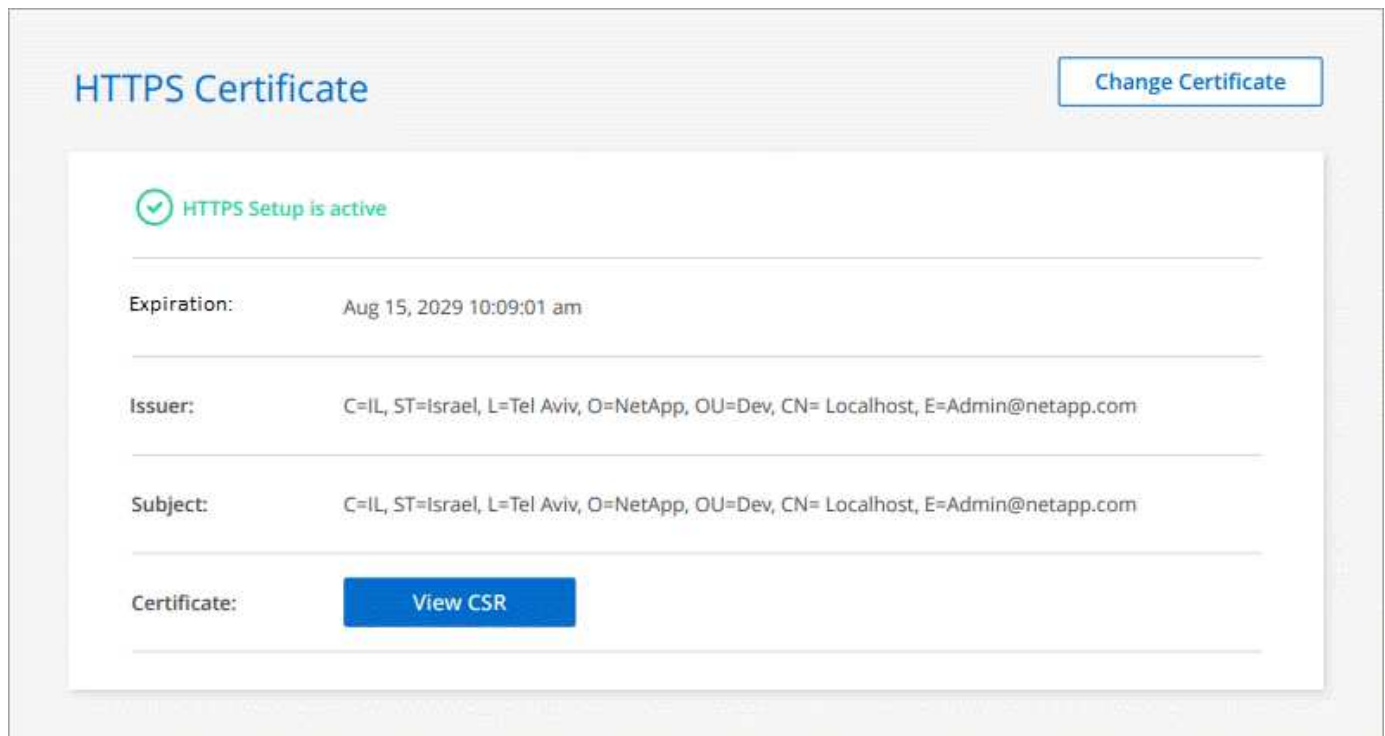
1. Cloud Manager 콘솔의 오른쪽 상단에서 설정 아이콘을 클릭하고 \* HTTPS 설정 \* 을 선택합니다.



2. HTTPS 설정 페이지에서 인증서 서명 요청(CSR)을 생성하거나 고유한 CA 서명 인증서를 설치하여 인증서를 설치합니다.

| 옵션을 선택합니다            | 설명  |
|----------------------|---|
| CSR을 생성합니다           | <p>a. 커넥터 호스트의 호스트 이름 또는 DNS(일반 이름)를 입력한 다음 * CSR 생성 * 을 클릭합니다.</p> <p>Cloud Manager는 인증서 서명 요청을 표시합니다.</p> <p>b. CSR을 사용하여 CA에 SSL 인증서 요청을 제출합니다.</p> <p>인증서는 PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식을 사용해야 합니다.</p> <p>c. 인증서 파일을 업로드한 다음 * 설치 * 를 클릭합니다.</p> |
| 고유한 CA 서명 인증서를 설치합니다 | <p>a. CA 서명 인증서 설치 * 를 선택합니다.</p> <p>b. 인증서 파일과 개인 키를 모두 로드한 다음 * 설치 * 를 클릭합니다.</p> <p>인증서는 PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식을 사용해야 합니다.</p>  |

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



### Cloud Manager HTTPS 인증서를 갱신하는 중입니다

Cloud Manager 웹 콘솔에 안전하게 액세스하려면 만료되기 전에 Cloud Manager HTTPS 인증서를 갱신해야 합니다. 만료되기 전에 인증서를 갱신하지 않으면 사용자가 HTTPS를 사용하여 웹 콘솔에 액세스할 때 경고가 나타납니다.

단계

1. Cloud Manager 콘솔의 오른쪽 상단에서 설정 아이콘을 클릭하고 \* HTTPS 설정 \* 을 선택합니다.

만료 날짜를 포함하여 Cloud Manager 인증서에 대한 세부 정보가 표시됩니다.

2. 인증서 변경 \* 을 클릭하고 단계에 따라 CSR을 생성하거나 고유한 CA 서명 인증서를 설치합니다.

Cloud Manager는 새로운 CA 서명 인증서를 사용하여 안전한 HTTPS 액세스를 제공합니다.

## HTTP 프록시 서버를 사용하도록 Connector 구성

회사 정책에 따라 인터넷에 대한 모든 HTTP 통신에 프록시 서버를 사용해야 하는 경우 해당 HTTP 프록시 서버를 사용하도록 커넥터를 구성해야 합니다. 프록시 서버는 클라우드 또는 네트워크에 있을 수 있습니다.

Cloud Manager는 Connector에서 HTTPS 프록시 사용을 지원하지 않습니다.

### Connector에서 프록시를 활성화합니다

커넥터가 관리하는 프록시 서버(HA 중개자 포함)와 Cloud Volumes ONTAP 시스템을 사용하도록 커넥터를 구성하는 경우 모두 프록시 서버를 사용합니다.

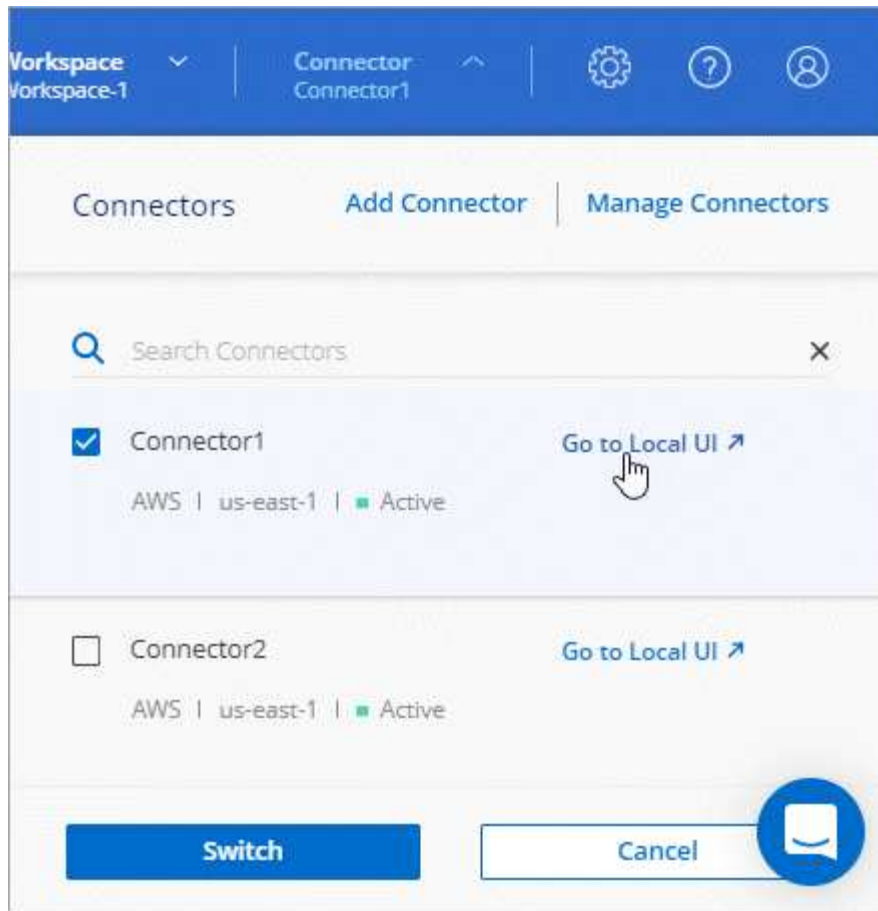
이 작업은 Connector를 다시 시작합니다. 계속하기 전에 커넥터가 어떠한 작업도 수행하지 않는지 확인하십시오.

단계

1. ["Cloud Manager SaaS 인터페이스에 로그인합니다"](#) Connector 인스턴스에 대한 네트워크 연결이 있는 컴퓨터에서

커넥터에 공용 IP 주소가 없는 경우 VPN 연결이 필요하거나 Connector와 동일한 네트워크에 있는 점프 호스트에서 연결해야 합니다.

2. Connector \* 드롭다운을 클릭한 다음 \* Go to local UI \* 를 클릭하여 특정 Connector를 선택합니다.



Connector에서 실행되는 Cloud Manager 인터페이스는 새 브라우저 탭에 로드됩니다.

3. Cloud Manager 콘솔의 오른쪽 상단에서 설정 아이콘을 클릭하고 \* 커넥터 설정 \* 을 선택합니다.



4. 일반 \* 에서 \* HTTP 프록시 구성 \* 을 클릭합니다.
5. 프록시 설정:
  - a. 프록시 사용 \* 을 클릭합니다.
  - b. 구문을 사용하여 서버를 지정합니다 `http://address:port[]`
  - c. 서버에 기본 인증이 필요한 경우 사용자 이름과 암호를 지정합니다
  - d. 저장 \* 을 클릭합니다.



Cloud Manager는 @ 문자를 포함하는 암호를 지원하지 않습니다.

프록시 서버를 지정하면 AutoSupport 메시지를 보낼 때 프록시 서버를 사용하도록 새 Cloud Volumes ONTAP 시스템이 자동으로 구성됩니다. 사용자가 Cloud Volumes ONTAP 시스템을 생성하기 전에 프록시 서버를 지정하지 않은 경우 시스템 관리자를 사용하여 각 시스템의 AutoSupport 옵션에서 프록시 서버를 수동으로 설정해야 합니다.

## 직접 API 트래픽을 활성화합니다

프록시 서버를 구성한 경우 프록시를 통하지 않고 API 호출을 Cloud Manager로 직접 전송할 수 있습니다. 이 옵션은 AWS, Azure 또는 Google Cloud에서 실행되는 커넥터에서 지원됩니다.

### 단계

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



2. 일반 \* 에서 \* 직접 API 트래픽 지원 \* 을 클릭합니다.
3. 확인란을 클릭하여 옵션을 활성화한 다음 \* 저장 \* 을 클릭합니다.

## Connector의 기본 설정

Connector를 배포하기 전에 또는 문제를 해결해야 하는 경우에 대해 자세히 알아볼 수 있습니다.

### 인터넷 액세스가 가능한 기본 구성

다음 구성 정보는 클라우드 공급자의 마켓플레이스에서 Connector를 배포했거나 인터넷에 액세스할 수 있는 온프레미스 Linux 호스트에 Connector를 수동으로 설치한 경우에 적용됩니다.

#### AWS 세부 정보

Cloud Manager 또는 클라우드 공급자의 마켓플레이스에서 Connector를 구축한 경우 다음을 참조하십시오.

- EC2 인스턴스 유형은 T3.xLarge입니다.
- 이미지의 운영 체제는 Red Hat Enterprise Linux 7.6(HVM)입니다.

운영 체제에는 GUI가 포함되어 있지 않습니다. 시스템에 액세스하려면 터미널을 사용해야 합니다.

- EC2 Linux 인스턴스의 사용자 이름은 EC2-user입니다.
- 기본 시스템 디스크는 50GiB GP2 디스크입니다.

#### Azure 세부 정보

Cloud Manager 또는 클라우드 공급자의 마켓플레이스에서 Connector를 구축한 경우 다음을 참조하십시오.

- VM 유형은 DS3 v2입니다.
- 이미지의 운영 체제는 CentOS 7.6입니다.

운영 체제에는 GUI가 포함되어 있지 않습니다. 시스템에 액세스하려면 터미널을 사용해야 합니다.

- 기본 시스템 디스크는 100GiB 프리미엄 SSD 디스크입니다.

## Google Cloud 세부 정보

Cloud Manager 또는 클라우드 공급자의 마켓플레이스에서 Connector를 구축한 경우 다음을 참조하십시오.

- VM 인스턴스는 n1-standard-4입니다.
- 이미지의 운영 체제는 CentOS 7.9입니다.

운영 체제에는 GUI가 포함되어 있지 않습니다. 시스템에 액세스하려면 터미널을 사용해야 합니다.

- 기본 시스템 디스크는 100GiB SSD 영구 디스크입니다.

### 설치 폴더

Connector 설치 폴더는 다음 위치에 있습니다.

/opt/application/netapp/cloudmanager입니다

### 로그 파일

로그 파일은 다음 폴더에 들어 있습니다.

- /opt/application/netapp/cloudmanager/log입니다

이 폴더의 로그에는 Connector 및 Docker 이미지에 대한 세부 정보가 나와 있습니다.

- /opt/application/netapp/cloudmanager/docker/데이터/로그

이 폴더의 로그에는 Connector에서 실행되는 클라우드 서비스와 Cloud Manager 서비스에 대한 세부 정보가 나와 있습니다.

### 커넥터 서비스

- Cloud Manager 서비스의 이름은 occm입니다.
- occm 서비스는 MySQL 서비스에 따라 달라진다.

MySQL 서비스가 다운되면 occm 서비스도 다운됩니다.

### 패키지

Cloud Manager는 다음 패키지를 아직 설치하지 않은 경우 Linux 호스트에 설치합니다.

- 7zip
- AWSCLI
- Docker 를 참조하십시오
- 자바
- 쿠베틀입니다
- MySQL
- 트리엔ctl



- 잡아당깁니다
- 뺏깁니다

#### 포트

커넥터는 Linux 호스트에서 다음 포트를 사용합니다.

- HTTP 액세스용 80
- HTTPS 액세스용 443
- Cloud Manager 데이터베이스용 3306
- Cloud Manager API 프록시의 경우 8080
- 서비스 관리자 API용 8666
- 8777)을 참조하십시오

#### 인터넷 액세스가 없는 기본 구성

인터넷 액세스가 없는 온프레미스 Linux 호스트에 커넥터를 수동으로 설치한 경우 다음 구성이 적용됩니다. ["이 설치 옵션에 대해 자세히 알아보십시오"](#).

- Connector 설치 폴더는 다음 위치에 있습니다.

`/opt/application/netapp/DS`

- 로그 파일은 다음 폴더에 들어 있습니다.

`/var/lib/docker/volumes/DS_occmpdata/_data/log`

이 폴더의 로그에는 Connector 및 Docker 이미지에 대한 세부 정보가 나와 있습니다.

- 모든 서비스가 Docker 컨테이너 내부에서 실행 중입니다

서비스는 실행 중인 Docker 런타임 서비스에 따라 다릅니다

- 커넥터는 Linux 호스트에서 다음 포트를 사용합니다.

- HTTP 액세스용 80
- HTTPS 액세스용 443

## 검색된 클라우드 스토리지

### Amazon S3 버킷을 봅니다

AWS에 Connector를 설치한 후 Cloud Manager는 Connector가 설치된 AWS 계정에 상주하는 Amazon S3 버킷에 대한 정보를 자동으로 검색할 수 있습니다. Amazon S3 작업 환경이 Canvas에 추가되어 이 정보를 볼 수 있습니다.

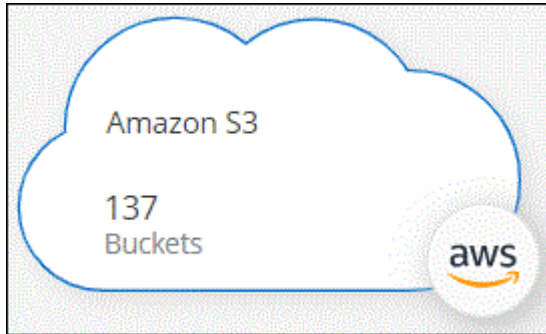
지역, 액세스 정책, 계정, 총 용량 및 사용된 용량 등을 비롯한 S3 버킷에 대한 세부 정보를 볼 수 있습니다. 이러한 버킷은 Cloud Backup, Cloud Tiering 또는 Cloud Sync 작업의 대상으로 사용할 수 있습니다. 또한, Cloud Data

Sense를 사용하여 이러한 버킷을 스캔할 수 있습니다.

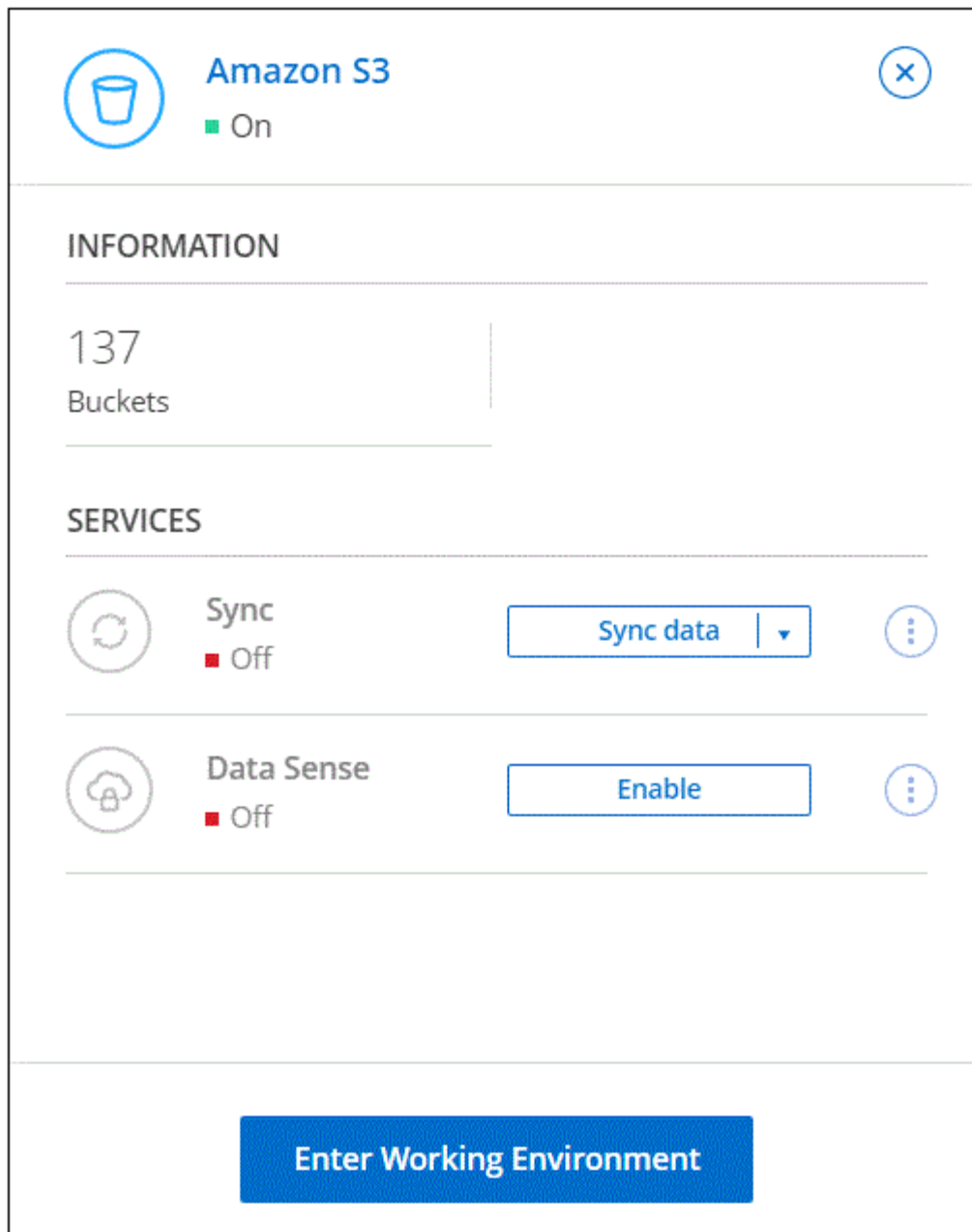
단계

1. "커넥터를 설치합니다" AWS 계정에서 Amazon S3 버킷을 확인할 수 있습니다.

잠시 후 Amazon S3 작업 환경이 자동으로 표시됩니다.



2. 작업 환경을 클릭하고 오른쪽 창에서 작업을 선택합니다.



3. 클라우드 데이터 센스에서 개인 및 중요 데이터를 위해 S3 버킷을 스캔하려면 \* 활성화 \* 를 클릭합니다.

자세한 내용은 을 참조하십시오 "[Amazon S3에 대한 Cloud Data Sense 시작하기](#)".

4. AWS 계정에서 S3 버킷에 대한 세부 정보를 보려면 \* 작업 환경 입력 \* 을 클릭합니다.

Amazon S3

Overview

137 Total Buckets

3.47 TiB Total Capacity

18 Total Regions

137 Buckets

| Bucket Name               | AWS Account | Region                | Creation Date     | Encryption | Is Public             | Size       | Total Objects |
|---------------------------|-------------|-----------------------|-------------------|------------|-----------------------|------------|---------------|
| cloudsync02               | 75999547048 | US East (N. Virginia) | March 14, 2022    | Error ⓘ    | Public                | 12.58 MiB  | 788           |
| datasensedemo             | 75999547048 | US East (N. Virginia) | March 28, 2022    | Disabled   | Public                | 1.89 MiB   | 143           |
| netapp-jam-bucket         | 75999547048 | EU (Ireland)          | November 2, 2020  | Error ⓘ    | Public                | 263.54 MiB | 7             |
| alle-demo-tlveng          | 75999547048 | US East (N. Virginia) | November 8, 2021  | Error ⓘ    | Objects can be public | 8.24 GiB   | 7             |
| amir-occm                 | 75999547048 | US West (Oregon)      | December 28, 2021 | Error ⓘ    | Objects can be public | 1.43 GiB   | 11            |
| aws-75999547048-us-east-1 | 75999547048 | US East (N. Virginia) | March 18, 2019    | Error ⓘ    | Objects can be public | 106.48 MiB | 827           |
| aws-75999547048-us-west-2 | 75999547048 | US West (Oregon)      | March 19, 2019    | Error ⓘ    | Objects can be public | 974.1 KiB  | 127           |

1 - 50 of 137

## Azure Blob 계정 보기

Azure에 Connector를 설치한 후 Cloud Manager는 Connector가 설치된 Azure 구독에 있는 Azure 저장소 계정에 대한 정보를 자동으로 검색할 수 있습니다. Azure Blob 작업 환경이 Canvas에 추가되어 이 정보를 볼 수 있습니다.

위치, 리소스 그룹, 총 용량 및 사용된 용량 등 Azure 저장소 계정에 대한 세부 정보를 볼 수 있습니다. 이러한 계정은 Cloud Backup, Cloud Tiering 또는 Cloud Sync 작업의 대상으로 사용할 수 있습니다.

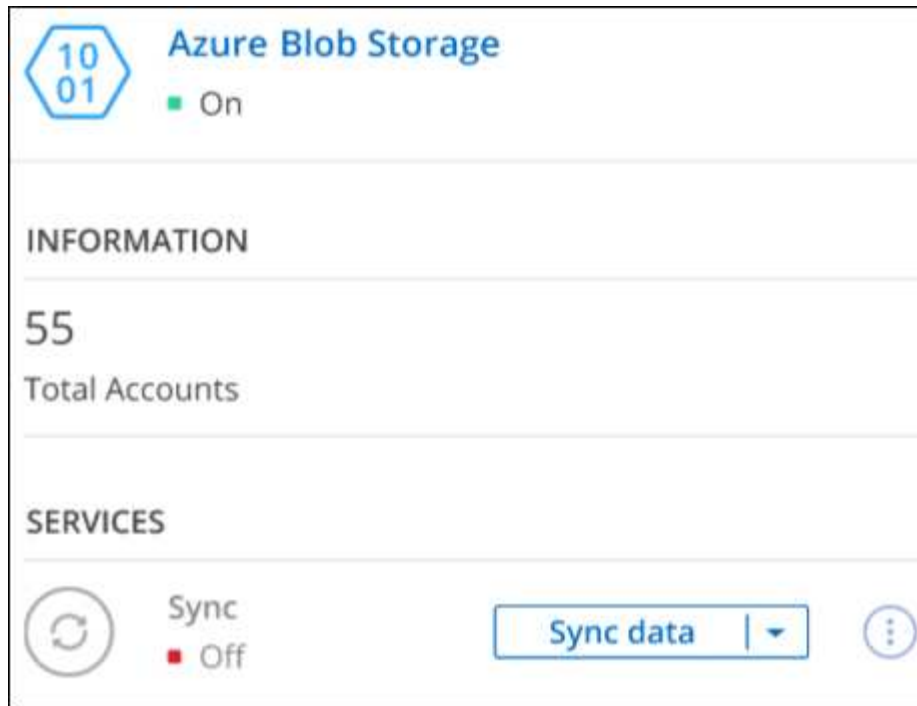
단계

1. "커넥터를 설치합니다" Azure 저장소 계정을 보려는 Azure 계정에서

Azure Blob 작업 환경이 곧 자동으로 표시됩니다.



2. 작업 환경을 클릭하고 오른쪽 창에서 작업을 선택합니다.



3. Azure Blob 저장소와 데이터를 동기화하려면 \* 데이터 동기화 \* 를 클릭합니다.

자세한 내용은 을 참조하십시오 "[Cloud Sync 서비스에 대한 개요입니다](#)".

4. Azure Blob의 Azure 저장소 계정에 대한 세부 정보를 보려면 \* 작업 환경 입력 \* 을 클릭합니다.

| Storage Account Name | Subscription | Location       | Creation Date     | Resource Group | Blob Capacity |
|----------------------|--------------|----------------|-------------------|----------------|---------------|
| ovu8llxvdfypxn       | OCCM QA1     | West US        | June 24, 2021     | AdmAzureHa-rg  | 170 B         |
| rootsa9ktpjzcm       | OCCM QA1     | West US        | June 24, 2021     | AdmAzureHa-rg  | 950.22 GiB    |
| scvdwjcwehswli       | OCCM QA1     | West US        | June 24, 2021     | AdmAzureHa-rg  | 22.12 MiB     |
| 65qtx0smegmq2vt      | OCCM QA1     | West US        | June 24, 2021     | AdmAzureVsa-rg | 170 B         |
| bu9kixthymr1be       | OCCM QA1     | West US        | June 24, 2021     | AdmAzureVsa-rg | 1.01 MiB      |
| 8jzsvybvjwieww8      | OCCM QA1     | Canada Central | December 12, 2019 | aff1-rg        | 170 B         |

## Google Cloud Storage 버킷 보기

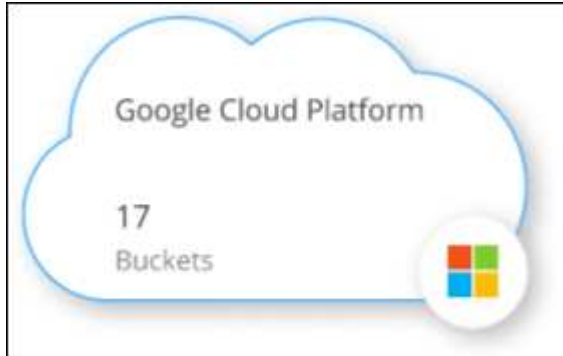
Google Cloud에 Connector를 설치한 후 Cloud Manager는 Connector가 설치된 Google 계정에 있는 Google Cloud Storage 버킷에 대한 정보를 자동으로 검색할 수 있습니다. Google Cloud Storage 작업 환경이 Canvas에 추가되어 이 정보를 볼 수 있습니다.

위치, 액세스 상태, 스토리지 클래스, 총 용량 및 사용된 용량 등 Google Cloud Storage 버킷에 대한 자세한 정보를 볼 수 있습니다. 이러한 버킷은 Cloud Backup, Cloud Tiering 또는 Cloud Sync 작업의 대상으로 사용할 수 있습니다.

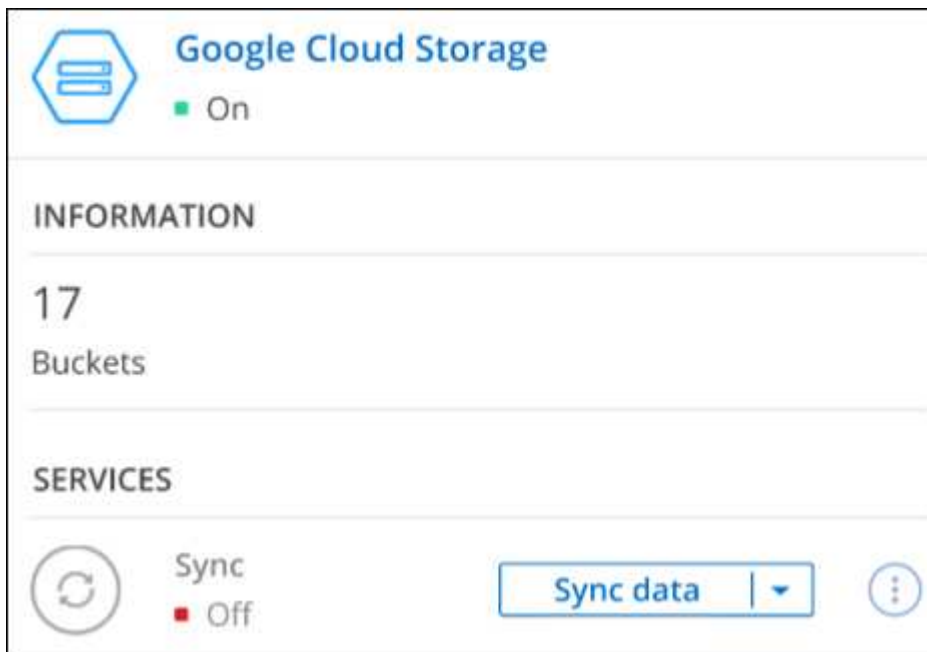
단계

1. ["커넥터를 설치합니다"](#) Google Cloud Storage 버킷을 보려는 Google 계정입니다.

곧 Google Cloud Storage 작업 환경이 자동으로 표시됩니다.



2. 작업 환경을 클릭하고 오른쪽 창에서 작업을 선택합니다.



3. Google Cloud Storage 버킷과 데이터를 동기화하려면 \* 데이터 동기화 \* 를 클릭합니다.

자세한 내용은 을 참조하십시오 ["Cloud Sync 서비스에 대한 개요입니다"](#).

4. Google 계정의 버킷에 대한 세부 정보를 보려면 \* 작업 환경 입력 \* 을 클릭합니다.

Google Cloud Storage

Overview

17

Total buckets

1.76 TiB

Total capacity | Calculating ●●●

6

Total locations

17 Buckets

| Bucket Name  | Location              | Creation Date | Public Access | Default Storage Class | Total Capacity |  |
|--------------|-----------------------|---------------|---------------|-----------------------|----------------|--|
| BucketName 1 | US East (N. Virginia) | May 04 2021   | Yes           | StorageClass 1        | ●●●            |  |
| BucketName 2 | US West (Oregon)      | May 04 2021   | Yes           | StorageClass 2        | ●●●            |  |
| BucketName 3 | US East (N. Virginia) | May 04 2021   | No            | StorageClass 3        | ●●●            |  |
| BucketName 4 | US East (N. Virginia) | May 04 2021   | No            | StorageClass 4        | ●●●            |  |
| BucketName 5 | US East (N. Virginia) | May 04 2021   | Yes           | StorageClass 5        | ●●●            |  |

## AWS 자격 증명

### AWS 자격 증명 및 권한

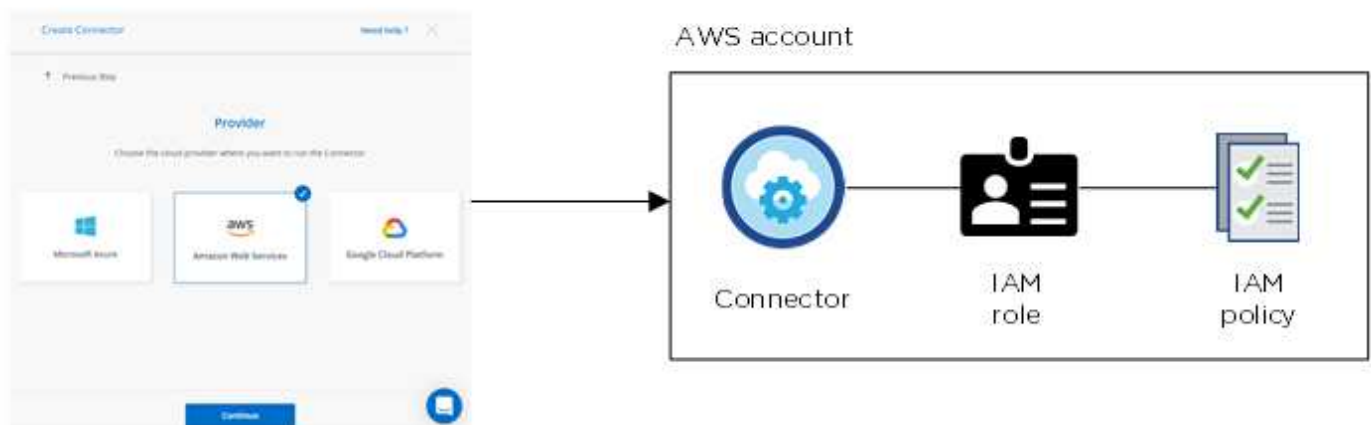
Cloud Manager를 사용하면 Cloud Volumes ONTAP 구축 시 사용할 AWS 자격 증명을 선택할 수 있습니다. 초기 AWS 자격 증명을 사용하여 모든 Cloud Volumes ONTAP 시스템을 구축하거나 추가 자격 증명을 추가할 수 있습니다.

#### 초기 AWS 자격 증명

Cloud Manager에서 Connector를 구축하는 경우 IAM 사용자의 ARN 또는 액세스 키를 제공해야 합니다. 사용하는 인증 방법에는 Connector 인스턴스를 AWS에 구축하는 데 필요한 권한이 있어야 합니다. 필요한 권한이 에 나열됩니다 ["AWS의 커넥터 구축 정책"](#).

Cloud Manager가 AWS에서 Connector 인스턴스를 시작하면 IAM 역할과 인스턴스에 대한 인스턴스 프로필이 생성됩니다. 또한 Connector에 해당 AWS 계정 내의 리소스 및 프로세스를 관리할 수 있는 권한을 제공하는 정책을 첨부합니다. ["Cloud Manager에서 사용 권한을 사용하는 방법을 검토합니다"](#).

#### Cloud Manager



Cloud Volumes ONTAP에 대한 새로운 작업 환경을 생성할 때 Cloud Manager에서 기본적으로 다음 AWS 자격

증명을 선택합니다.

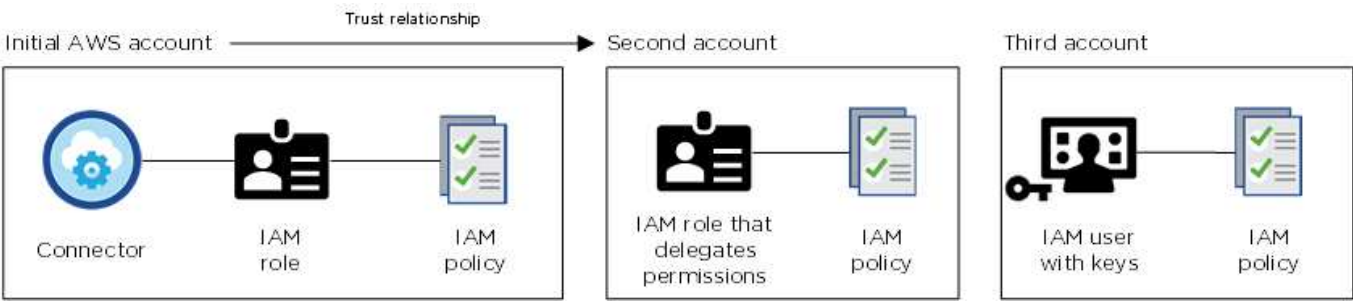
| Details & Credentials |            |                          |                  |
|-----------------------|------------|--------------------------|------------------|
| Instance Profile      |            | QA Subscription          | Edit Credentials |
| Credentials           | Account ID | Marketplace Subscription |                  |

추가 **AWS** 자격 증명

AWS 자격 증명을 추가하는 방법에는 두 가지가 있습니다.

기존 커넥터에 **AWS** 자격 증명을 추가합니다

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



그러면 됩니다 **"Cloud Manager에 계정 자격 증명을 추가합니다"** IAM 역할의 ARN(Amazon Resource Name) 또는 IAM 사용자의 AWS 키를 지정합니다.

다른 자격 증명 세트를 추가한 후 새 작업 환경을 만들 때 자격 증명으로 전환할 수 있습니다.



Cloud Manager에 AWS 자격 증명을 직접 추가합니다

Cloud Manager에 새 AWS 자격 증명을 추가하면 Cloud Manager에서 ONTAP 작업 환경을 위한 FSx를 생성 및 관리하거나 커넥터를 생성하는 데 필요한 권한을 얻을 수 있습니다.

### Marketplace 구축 및 온프레미스 배포는 어떻습니까?

위 섹션에서는 Cloud Manager에서 Connector를 위한 권장 구축 방법을 설명합니다. 에서 AWS에 Connector를 구축할 수도 있습니다 ["AWS 마켓플레이스 를 참조하십시오"](#) 여러분도 가능합니다 ["Connector On-Premises를 설치합니다"](#).

Marketplace를 사용하는 경우 사용 권한이 동일한 방식으로 제공됩니다. IAM 역할을 수동으로 생성 및 설정한 다음 추가 계정에 대한 권한을 제공하면 됩니다.

사내 구축의 경우 Cloud Manager 시스템에 대해 IAM 역할을 설정할 수 없지만 추가 AWS 계정에 대한 사용 권한을 제공할 수는 있습니다.

### AWS 자격 증명을 안전하게 회전하려면 어떻게 해야 합니까?

위에서 설명한 것처럼 Cloud Manager를 사용하면 몇 가지 방법으로 AWS 자격 증명을 제공할 수 있습니다. 예를 들어, Connector 인스턴스와 연관된 IAM 역할이나 신뢰할 수 있는 계정에서 IAM 역할을 가정하거나 AWS 액세스 키를 제공하여 AWS 자격 증명을 제공할 수 있습니다.

처음 두 옵션을 사용할 때 Cloud Manager는 AWS 보안 토큰 서비스를 사용하여 지속적으로 회전하는 임시 자격 증명을 얻습니다. 이 프로세스는 자동 및 안전의 모범 사례입니다.

Cloud Manager에 AWS 액세스 키를 제공하는 경우 Cloud Manager에서 키를 정기적으로 업데이트하여 키를 회전해야 합니다. 이는 완전히 수동으로 진행되는 프로세스입니다.

## Cloud Manager의 AWS 자격 증명 및 구독을 관리합니다

AWS 자격 증명을 추가 및 관리하여 Cloud Manager가 AWS 계정에 클라우드 리소스를 구축 및 관리하는 데 필요한 권한을 갖도록 합니다. 여러 AWS 구독을 관리하는 경우 자격 증명 페이지에서 각 AWS 자격 증명을 서로 다른 AWS 자격 증명에 할당할 수 있습니다.

### 개요

AWS 자격 증명을 기존 Connector에 추가하거나 Cloud Manager에 직접 추가할 수 있습니다.

- 기존 커넥터에 AWS 자격 증명을 추가합니다

기존 커넥터에 새로운 AWS 자격 증명을 추가하면 동일한 커넥터를 사용하여 다른 AWS 계정에 Cloud Volumes ONTAP를 구축할 수 있습니다. [Connector에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오.](#)

- Connector를 생성하기 위해 Cloud Manager에 AWS 자격 증명을 추가합니다

Cloud Manager에 새로운 AWS 자격 증명을 추가하면 Cloud Manager에서 Connector를 생성하는 데 필요한 권한을 얻을 수 있습니다. [Cloud Manager에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오.](#)

- ONTAP용 FSx에 대한 AWS 자격 증명을 Cloud Manager에 추가합니다

Cloud Manager에 새 AWS 자격 증명을 추가하면 Cloud Manager에서 ONTAP용 FSx를 생성하고 관리하는 데 필요한 권한을 얻을 수 있습니다. ["ONTAP용 FSx에 대한 사용 권한을 설정하는 방법에 대해 알아보십시오"](#)

### 자격 증명을 회전하는 방법

Cloud Manager를 사용하면 몇 가지 방법으로 AWS 자격 증명을 제공할 수 있습니다. 예를 들어, Connector 인스턴스와 연관된 IAM 역할이나 신뢰할 수 있는 계정에서 IAM 역할을 가정하거나 AWS 액세스 키를 제공하여 AWS 자격 증명을 제공할 수 있습니다. ["AWS 자격 증명 및 권한에 대해 자세히 알아보십시오"](#).

처음 두 옵션을 사용할 때 Cloud Manager는 AWS 보안 토큰 서비스를 사용하여 지속적으로 회전하는 임시 자격 증명을 얻습니다. 이 프로세스는 자동적이며 안전하기 때문에 가장 좋은 방법입니다.

Cloud Manager에 AWS 액세스 키를 제공하는 경우 Cloud Manager에서 키를 정기적으로 업데이트하여 키를 회전해야 합니다. 이는 완전히 수동으로 진행되는 프로세스입니다.

### Connector에 추가 자격 증명을 추가합니다

다른 AWS 계정에 Cloud Volumes ONTAP를 구축 및 관리할 수 있도록 커넥터에 AWS 자격 증명을 추가합니다. 다른 계정에서 IAM 역할의 ARN을 제공하거나 AWS 액세스 키를 제공할 수 있습니다.

### 권한을 부여합니다

Connector에 AWS 자격 증명을 추가하기 전에 필요한 권한을 제공해야 합니다. Cloud Manager에서 사용 권한을 통해 해당 AWS 계정 내의 리소스와 프로세스를 관리할 수 있습니다. 사용 권한을 제공하는 방법은 Cloud Manager에 신뢰할 수 있는 계정 또는 AWS 키에서 역할의 ARN을 제공할지 여부에 따라 달라집니다.



Cloud Manager에서 Connector를 구축한 경우 Cloud Manager는 Connector를 구축한 계정에 대한 AWS 자격 증명을 자동으로 추가합니다. 기존 시스템에 Connector 소프트웨어를 수동으로 설치한 경우에는 이 초기 계정이 추가되지 않습니다. ["AWS 자격 증명 및 권한에 대해 알아보십시오"](#).

- 선택 \*
- [\[Grant permissions by assuming an IAM role in another account\]](#)
- [\[Grant permissions by providing AWS keys\]](#)

다른 계정에서 **IAM** 역할을 가정하여 권한을 부여합니다

IAM 역할을 사용하여 Connector 인스턴스를 구축한 소스 AWS 계정과 다른 AWS 계정 간에 신뢰 관계를 설정할 수 있습니다. 그런 다음 Cloud Manager에 신뢰할 수 있는 계정의 IAM 역할 ARN을 제공합니다.

단계

1. Cloud Volumes ONTAP를 배포하려는 대상 계정의 IAM 콘솔로 이동합니다.
2. 액세스 관리에서 \* 역할 > 역할 만들기 \* 를 클릭하고 단계를 따라 역할을 만듭니다.

다음을 수행하십시오.

- 신뢰할 수 있는 엔터티 유형 \* 에서 \* AWS 계정 \* 을 선택합니다.
  - 다른 AWS 계정 \* 을 선택하고 Connector 인스턴스가 있는 계정의 ID를 입력합니다.
  - 의 내용을 복사하여 붙여 넣어 정책을 만듭니다 "[Connector에 대한 IAM 정책](#)".
3. 나중에 Cloud Manager에 붙여넣을 수 있도록 IAM 역할의 역할 ARN을 복사합니다.

이제 계정에 필요한 권한이 있습니다. [이제 Connector에 자격 증명을 추가할 수 있습니다.](#)

**AWS** 키를 제공하여 권한을 부여합니다

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

단계

1. IAM 콘솔에서 의 내용을 복사하여 붙여 넣어 정책을 생성합니다 "[Connector에 대한 IAM 정책](#)".

["AWS 설명서: IAM 정책 생성"](#)

2. IAM 역할 또는 IAM 사용자에게 정책을 연결합니다.

- "[AWS 설명서: IAM 역할 생성](#)"
- "[AWS 설명서: IAM 정책 추가 및 제거](#)"

이제 계정에 필요한 권한이 있습니다. [이제 Connector에 자격 증명을 추가할 수 있습니다.](#)

자격 증명을 추가합니다

필요한 권한이 있는 AWS 계정을 제공한 후 해당 계정의 자격 증명을 기존 Connector에 추가할 수 있습니다. 이렇게 하면 동일한 커넥터를 사용하여 해당 계정에서 Cloud Volumes ONTAP 시스템을 시작할 수 있습니다.

클라우드 공급자에서 이러한 자격 증명을 만든 경우 사용할 수 있을 때까지 몇 분 정도 걸릴 수 있습니다. 몇 분 후에 Cloud Manager에 자격 증명을 추가합니다.

단계

1. Cloud Manager에서 현재 올바른 커넥터가 선택되어 있는지 확인합니다.
2. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 \* 자격 증명 \* 을 선택합니다.



3. 자격 증명 추가 \* 를 클릭하고 마법사의 단계를 따릅니다.
  - a. \* 자격 증명 위치 \*: \* Amazon Web Services > Connector \* 를 선택합니다.
  - b. \* 자격 증명 정의 \*: 신뢰할 수 있는 IAM 역할의 ARN(Amazon Resource Name)을 제공하거나 AWS 액세스 키와 비밀 키를 입력합니다.
  - c. \* Marketplace 구독 \*: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.

PAYGO(시간당 급여) 또는 연간 계약으로 Cloud Volumes ONTAP를 지불하려면 AWS 마켓플레이스의 Cloud Volumes ONTAP 구독과 AWS 자격 증명이 연결되어 있어야 합니다.

- d. \* 검토 \*: 새 자격 증명에 대한 세부 정보를 확인하고 \* 추가 \* 를 클릭합니다.

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

### Edit Credentials & Add Subscription

---

#### Associate Subscription to Credentials ?

Credentials

|  |  |
|--|--|
| keys   Account ID:                               |  |
| Instance Profile   Account ID:                   |  |
| <div> <span>casaba QA subscription</span> </div> |  |

+ Add Subscription

---

Apply
Cancel

**Connector**를 생성하기 위해 **Cloud Manager**에 자격 증명을 추가합니다

Cloud Manager에 Connector 생성에 필요한 권한을 제공하는 IAM 역할의 ARN을 제공하여 Cloud Manager에 AWS 자격 증명을 추가합니다. 새 Connector를 만들 때 이러한 자격 증명을 선택할 수 있습니다.

## IAM 역할을 설정합니다

Cloud Manager SaaS가 역할을 맡을 수 있도록 IAM 역할을 설정합니다.

### 단계

1. 대상 계정에서 IAM 콘솔로 이동합니다.
2. 액세스 관리에서 \* 역할 > 역할 만들기 \* 를 클릭하고 단계를 따라 역할을 만듭니다.

다음을 수행하십시오.

- 신뢰할 수 있는 엔터티 유형 \* 에서 \* AWS 계정 \* 을 선택합니다.
- 다른 AWS 계정 \* 을 선택하고 Cloud Manager SaaS:952013314444의 ID를 입력합니다
- Connector를 만드는 데 필요한 권한을 포함하는 정책을 만듭니다.
  - "ONTAP용 FSx에 필요한 권한을 봅니다"
  - "Connector 배포 정책을 봅니다"

3. 다음 단계에서 Cloud Manager에 붙여넣을 수 있도록 IAM 역할의 역할 ARN을 복사합니다.

이제 IAM 역할에 필요한 권한이 있습니다. 이제 Cloud Manager에 추가할 수 있습니다.

### 자격 증명을 추가합니다

필요한 권한을 IAM 역할에 제공한 후 ARN 역할을 Cloud Manager에 추가합니다.

방금 IAM 역할을 생성한 경우 사용할 수 있을 때까지 몇 분 정도 걸릴 수 있습니다. 몇 분 후에 Cloud Manager에 자격 증명을 추가합니다.

### 단계

1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 \* 자격 증명 \* 을 선택합니다.



2. 자격 증명 추가 \* 를 클릭하고 마법사의 단계를 따릅니다.
  - a. \* 자격 증명 위치 \*: \* Amazon Web Services > Cloud Manager \* 를 선택합니다.
  - b. \* 자격 증명 정의 \*: IAM 역할의 ARN(Amazon Resource Name)을 제공합니다.
  - c. \* 검토 \*: 새 자격 증명에 대한 세부 정보를 확인하고 \* 추가 \* 를 클릭합니다.

이제 새 커넥터를 만들 때 자격 증명을 사용할 수 있습니다.

## AWS 구독을 연결합니다

AWS 자격 증명을 Cloud Manager에 추가한 후 AWS Marketplace 구독을 해당 자격 증명과 연결할 수 있습니다. 구독을 통해 PAYGO(시간당 급여) 또는 연간 계약을 사용하여 Cloud Volumes ONTAP에 대한 비용을 지불하고, 다른 NetApp 클라우드 서비스를 사용할 수 있습니다.

Cloud Manager에 자격 증명을 이미 추가한 후에 AWS Marketplace 구독을 연결할 수 있는 두 가지 시나리오가

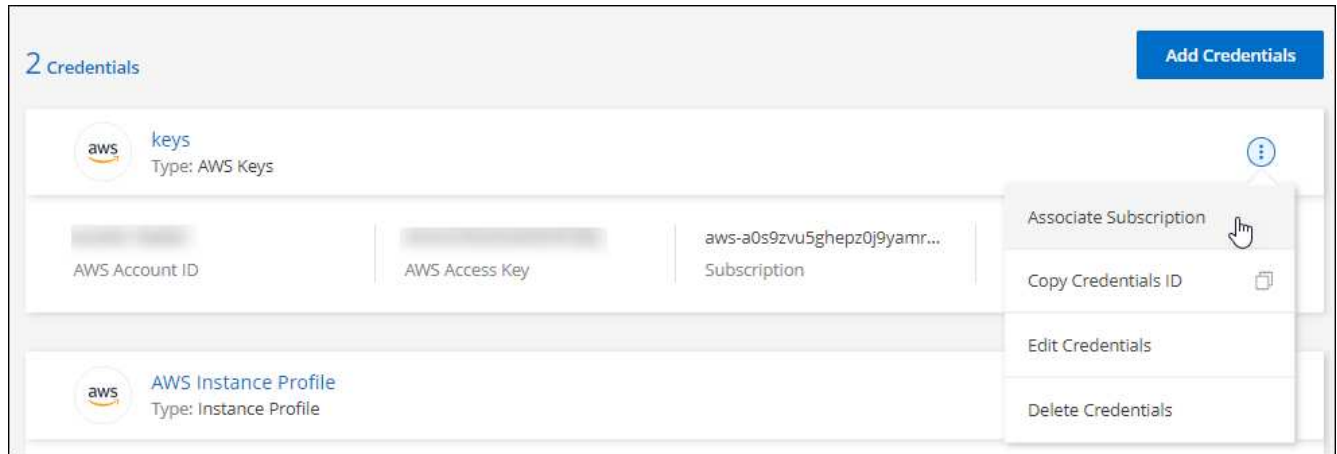
있습니다.

- 처음에 Cloud Manager에 자격 증명을 추가했을 때 구독을 연결하지 않았습니다.
- 기존 AWS Marketplace 구독을 새 구독으로 교체하려고 합니다.

Cloud Manager 설정을 변경하려면 먼저 Connector를 생성해야 합니다. ["커넥터를 만드는 방법에 대해 알아봅니다"](#).

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 \* 자격 증명 \* 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 클릭한 다음 \* 가입 연결 \* 을 선택합니다.



3. 드롭다운 목록에서 기존 구독을 선택하거나 \* 구독 추가 \* 를 클릭하고 단계에 따라 새 구독을 만듭니다.

▶ [https://docs.netapp.com/ko-kr/cloud-manager-setup-admin//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/ko-kr/cloud-manager-setup-admin//media/video_subscribing_aws.mp4) (video)

자격 증명을 편집합니다

Cloud Manager에서 계정 유형(AWS 키 또는 역할이라고 함)을 변경하거나, 이름을 편집하거나, 자격 증명(키 또는 ARN 역할)을 업데이트하여 AWS 자격 증명을 편집합니다.



Connector 인스턴스와 연결된 인스턴스 프로파일의 자격 증명은 편집할 수 없습니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 \* 자격 증명 \* 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 클릭한 다음 \* 자격 증명 편집 \* 을 선택합니다.
3. 필요한 내용을 변경한 다음 \* 적용 \* 을 클릭합니다.

자격 증명을 삭제하는 중입니다

자격 증명 세트가 더 이상 필요하지 않으면 Cloud Manager에서 삭제할 수 있습니다. 작업 환경과 연결되지 않은 자격 증명만 삭제할 수 있습니다.



Connector 인스턴스와 연결된 인스턴스 프로파일의 자격 증명은 삭제할 수 없습니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 \* 자격 증명 \* 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 클릭한 다음 \* 자격 증명 삭제 \* 를 선택합니다.
3. 확인하려면 \* 삭제 \* 를 클릭합니다.

## Azure 자격 증명

### Azure 자격 증명 및 권한

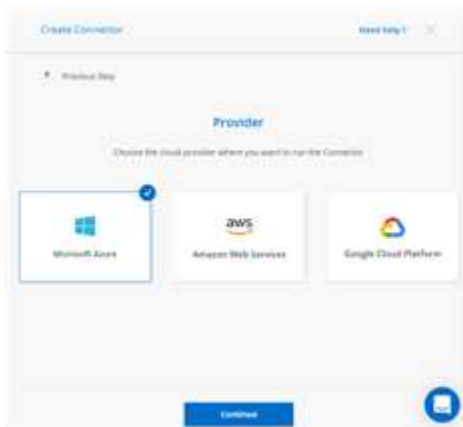
Cloud Manager를 사용하면 Cloud Volumes ONTAP 구축 시 사용할 Azure 자격 증명을 선택할 수 있습니다. 초기 Azure 자격 증명을 사용하여 모든 Cloud Volumes ONTAP 시스템을 배포하거나 추가 자격 증명을 추가할 수 있습니다.

#### 초기 Azure 자격 증명

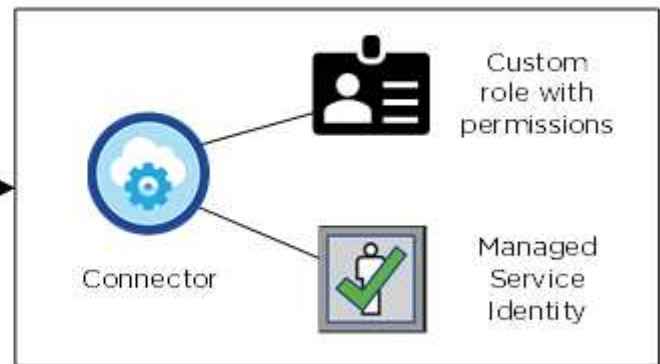
Cloud Manager에서 Connector를 배포하는 경우 Connector 가상 시스템을 배포할 수 있는 권한이 있는 Azure 계정 또는 서비스 보안 주체를 사용해야 합니다. 필요한 권한이 에 나열됩니다 ["Azure용 커넥터 배포 정책"](#).

Cloud Manager가 Azure에 Connector 가상 머신을 구축하면 가 활성화됩니다 ["시스템에서 할당한 관리 ID입니다"](#) 가상 머신에서 사용자 지정 역할을 생성하고 가상 머신에 할당합니다. 이 역할은 Cloud Manager에 해당 Azure 구독 내의 리소스 및 프로세스를 관리할 수 있는 권한을 제공합니다. ["Cloud Manager에서 사용 권한을 사용하는 방법을 검토합니다"](#).

Cloud Manager



Azure account



Cloud Volumes ONTAP에 대한 새 작업 환경을 생성할 때 Cloud Manager는 기본적으로 다음과 같은 Azure 자격 증명을 선택합니다.

| Details & Credentials  |                    |                               |                                  |
|------------------------|--------------------|-------------------------------|----------------------------------|
| Managed Service Ide... | OCCM QA1           | No subscription is associated | <a href="#">Edit Credentials</a> |
| Credential Name        | Azure Subscription | Marketplace Subscription      |                                  |

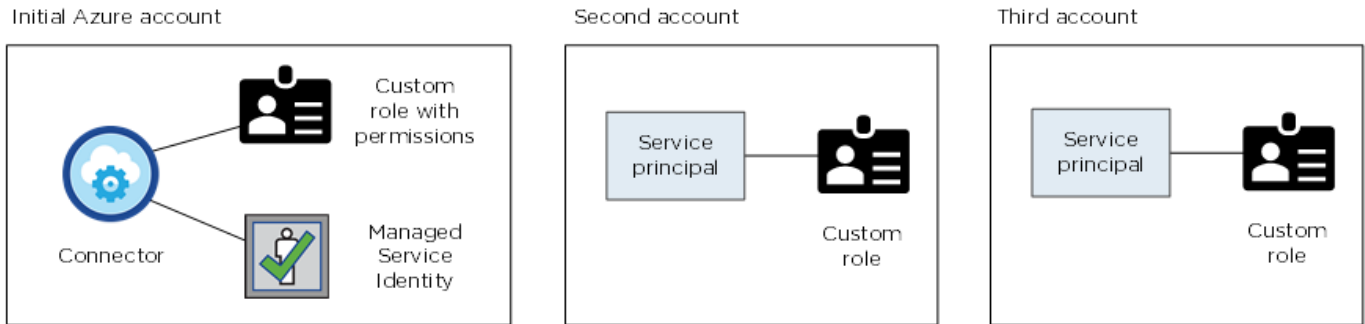


## 관리되는 ID에 대한 추가 Azure 구독

관리되는 ID는 Connector를 시작한 구독과 연결됩니다. 다른 Azure 구독을 선택하려면 를 수행해야 합니다 ["관리되는 ID를 해당 구독과 연결합니다"](#).

## 추가 Azure 자격 증명

다른 Azure 자격 증명을 사용하여 Cloud Volumes ONTAP를 배포하려는 경우 에서 필요한 권한을 부여해야 합니다 ["Azure Active Directory에서 서비스 보안 주체 만들기 및 설정"](#) 각 Azure 계정에 대해. 다음 그림에서는 두 개의 추가 계정을 보여 줍니다. 각 계정에는 권한을 제공하는 서비스 보안 주체와 사용자 지정 역할이 설정되어 있습니다.



그러면 됩니다 ["Cloud Manager에 계정 자격 증명을 추가합니다"](#) AD 서비스 보안 주체에 대한 세부 정보를 제공합니다.

다른 자격 증명 세트를 추가한 후 새 작업 환경을 만들 때 자격 증명으로 전환할 수 있습니다.

The screenshot shows the 'Edit Account & Add Subscription' dialog box. It has a title bar and a 'Credentials' section. The 'Credentials' section contains a text input field with a dropdown menu. The dropdown menu is open, showing the following options:

- cloud-manager-app | Application ID: 57c42424-88a0-480a.
- Managed Service Identity** (highlighted in blue)
- OCCM QA1 (Default)



## Marketplace 구축 및 온프레미스 배포는 어떻습니까?

위 섹션에서는 NetApp Cloud Central에서 제공하는 Connector의 권장 구축 방법에 대해 설명합니다. 에서 Azure에 Connector를 배포할 수도 있습니다 "[Azure 마켓플레이스 를 참조하십시오](#)", 그리고 당신은 할 수 있다 "[Connector On-Premises를 설치합니다](#)".

Marketplace를 사용하는 경우 사용 권한이 동일한 방식으로 제공됩니다. Connector에 대해 관리되는 ID를 수동으로 만들고 설정한 다음 추가 계정에 대한 사용 권한을 제공하면 됩니다.

온-프레미스 배포의 경우 Connector에 대해 관리되는 ID를 설정할 수 없지만 서비스 보안 주체를 사용하여 추가 계정에 대해 원하는 권한을 제공할 수 있습니다.

## Cloud Manager에 대한 Azure 자격 증명 및 구독 관리

Cloud Volumes ONTAP 시스템을 생성할 때 해당 시스템에서 사용할 Azure 자격 증명을 선택해야 합니다. 또한 선불 종량제 라이선스를 사용하는 경우 Marketplace 구독을 선택해야 합니다. Cloud Volumes ONTAP에 대해 여러 Azure 자격 증명 또는 여러 Azure 마켓플레이스 구독을 사용해야 하는 경우 이 페이지의 단계를 따릅니다.

Cloud Manager에서 Azure 구독 및 자격 증명을 추가하는 방법에는 두 가지가 있습니다.

1. Azure 구독과 Azure 관리 ID를 추가로 연결합니다.
2. 다른 Azure 자격 증명을 사용하여 Cloud Volumes ONTAP를 배포하려는 경우 서비스 보안 주체를 사용하여 Azure 사용 권한을 부여하고 해당 자격 증명을 Cloud Manager에 추가합니다.

관리되는 ID와 추가 **Azure** 구독을 연결합니다

Cloud Manager를 사용하면 Cloud Volumes ONTAP를 구축할 Azure 자격 증명 및 Azure 구독을 선택할 수 있습니다. 를 연결하지 않으면 관리 ID 프로필에 대해 다른 Azure 구독을 선택할 수 없습니다 "[관리 ID](#)" 있습니다.

관리되는 ID는입니다 "[초기 Azure 계정입니다](#)" Connector를 Cloud Manager에서 구축하는 경우 Connector를 구축한 경우 Cloud Manager는 Cloud Manager 운영자 역할을 생성하여 Connector 가상 머신에 할당합니다.

단계

1. Azure 포털에 로그인합니다.
2. Subscriptions \* 서비스를 연 다음 Cloud Volumes ONTAP를 배포할 구독을 선택합니다.
3. IAM(액세스 제어) \* 을 클릭합니다.
  - a. Add \* > \* Add role assignment \* 를 클릭한 후 권한을 추가합니다.
    - Cloud Manager Operator \* 역할을 선택합니다.



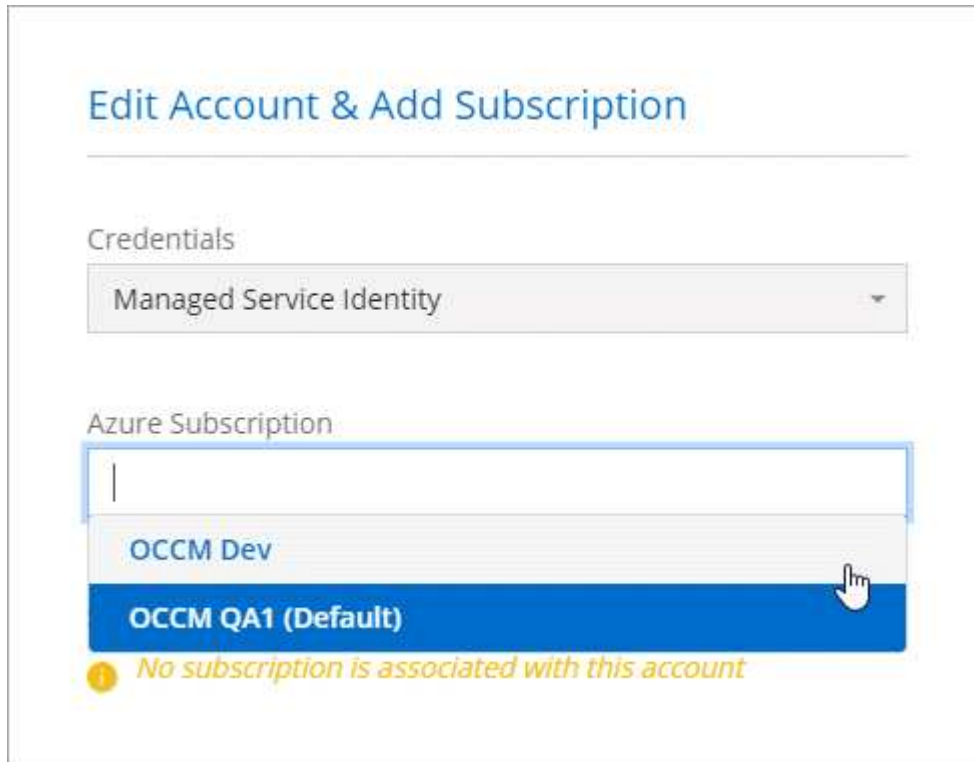
Cloud Manager Operator는 Connector 정책에 제공된 기본 이름입니다. 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

- Virtual Machine \* 에 대한 액세스 권한을 할당합니다.
- Connector 가상 머신이 생성된 서브스크립션을 선택합니다.

- Connector 가상 머신을 선택합니다.
- 저장 \* 을 클릭합니다.

4. 추가 구독에 대해 이 단계를 반복합니다.

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



### Cloud Manager에 Azure 자격 증명을 추가하는 중입니다

Cloud Manager에서 Connector를 구축하면 Cloud Manager가 필요한 권한이 있는 가상 머신에서 시스템에서 시스템에 할당된 관리 ID를 활성화합니다. Cloud Volumes ONTAP에 대한 새 작업 환경을 생성할 때 Cloud Manager는 기본적으로 이러한 Azure 자격 증명을 선택합니다.



기존 시스템에 Connector 소프트웨어를 수동으로 설치한 경우 초기 자격 증명 세트가 추가되지 않습니다. ["Azure 자격 증명 및 권한에 대해 알아보십시오"](#).

\_different\_sAzure 자격 증명을 사용하여 Cloud Volumes ONTAP를 배포하려는 경우 각 Azure 계정에 대해 Azure Active Directory에서 서비스 보안 주체를 만들고 설정하여 필요한 권한을 부여해야 합니다. 그런 다음 Cloud Manager에 새 자격 증명을 추가할 수 있습니다.

서비스 보안 주체를 사용하여 **Azure** 사용 권한 부여

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

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



단계

1. [Azure Active Directory 응용 프로그램을 만듭니다.](#)
2. [애플리케이션에 역할을 할당합니다.](#)
3. [Windows Azure 서비스 관리 API 권한을 추가합니다.](#)
4. [애플리케이션 ID 및 디렉토리 ID를 가져옵니다.](#)
5. [클라이언트 암호를 생성합니다.](#)

**Azure Active Directory** 응용 프로그램을 만드는 중입니다

Cloud Manager가 역할 기반 액세스 제어에 사용할 수 있는 Azure AD(Active Directory) 응용 프로그램 및 서비스 보안 주체를 만듭니다.

Active Directory 응용 프로그램을 만들고 응용 프로그램을 역할에 할당하려면 Azure에 적절한 권한이 있어야 합니다. 자세한 내용은 [을 참조하십시오 "Microsoft Azure 문서: 필요한 권한"](#).

단계

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



2. 메뉴에서 \* 앱 등록 \* 을 클릭합니다.
3. 새 등록 \* 을 클릭합니다.
4. 응용 프로그램에 대한 세부 정보를 지정합니다.
  - \* 이름 \*: 응용 프로그램의 이름을 입력합니다.
  - \* 계정 유형 \*: 계정 유형을 선택합니다(모두 Cloud Manager와 연동함).
  - \* URI 리디렉션 \*: 이 필드는 비워 둘 수 있습니다.
5. Register \* 를 클릭합니다.

AD 응용 프로그램 및 서비스 보안 주체를 만들었습니다.

#### 역할에 애플리케이션 할당

서비스 보안 주체를 하나 이상의 Azure 구독에 바인딩하고 사용자 지정 "OnCommand 클라우드 관리자 운영자" 역할을 할당해야 클라우드 관리자가 Azure에서 권한을 갖게 됩니다.

#### 단계

1. 사용자 지정 역할 만들기:
  - a. 의 내용을 복사합니다 "[Connector에 대한 사용자 지정 역할 권한](#)" JSON 파일에 저장합니다.
  - b. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

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

▪ 예 \*

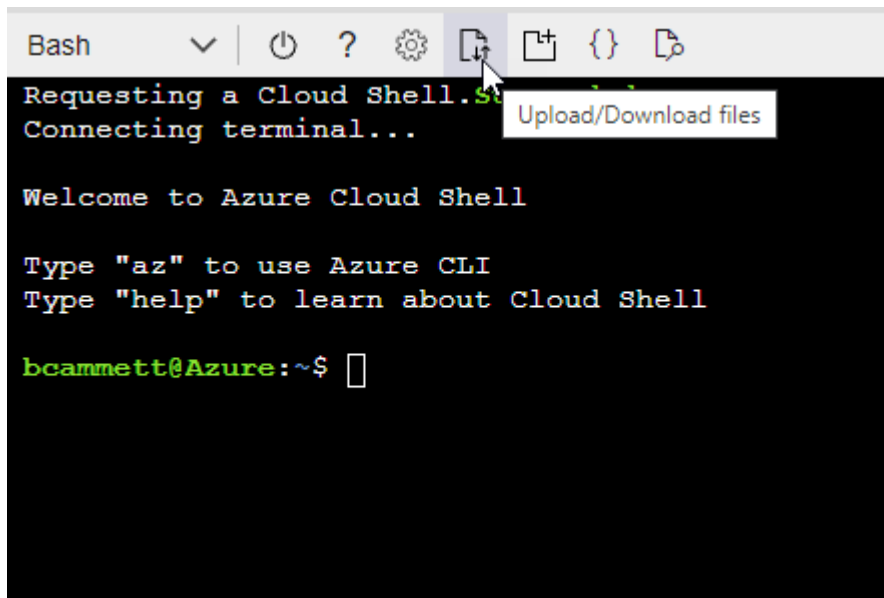
```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

- c. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 생성합니다.

다음 단계에서는 Azure Cloud Shell에서 Bash를 사용하여 역할을 생성하는 방법을 설명합니다.

▪ 시작 "[Azure 클라우드 셸](#)" Bash 환경을 선택하십시오.

- JSON 파일을 업로드합니다.



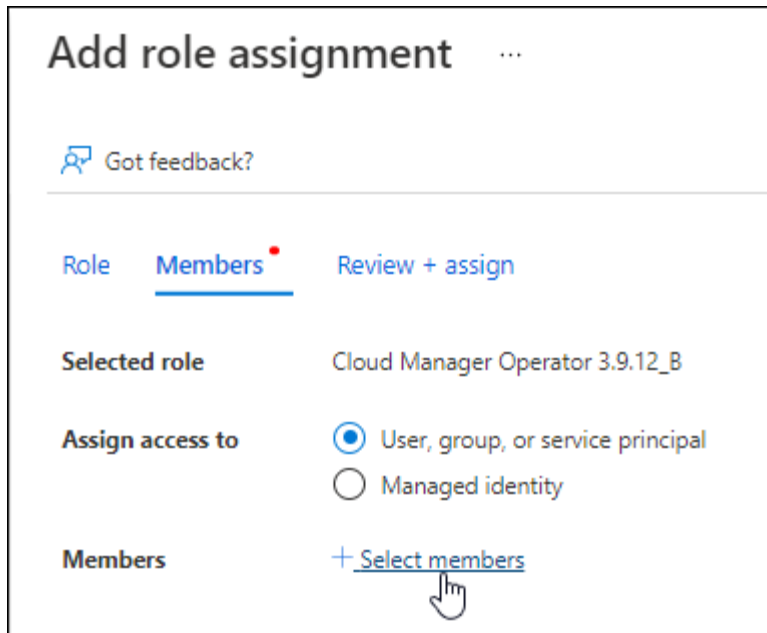
- 다음 Azure CLI 명령을 입력합니다.

```
az role definition create --role-definition
Policy_for_Setup_As_Service_Azure.json
```

이제 Connector 가상 머신에 할당할 수 있는 Cloud Manager Operator라는 사용자 지정 역할이 있어야 합니다.

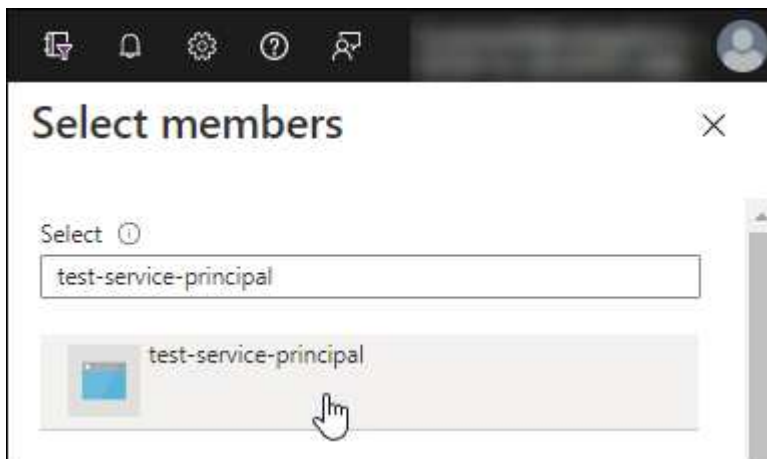
## 2. 역할에 응용 프로그램을 할당합니다.

- a. Azure 포털에서 \* Subscriptions \* 서비스를 엽니다.
- b. 구독을 선택합니다.
- c. IAM(Access Control) > 추가 > 역할 할당 추가 \* 를 클릭합니다.
- d. Role \* 탭에서 \* Cloud Manager Operator \* 역할을 선택하고 \* Next \* 를 클릭합니다.
- e. Members\* 탭에서 다음 단계를 완료합니다.
  - 사용자, 그룹 또는 서비스 보안 주체 \* 를 선택한 상태로 유지합니다.
  - 구성원 선택 \* 을 클릭합니다.



- 응용 프로그램의 이름을 검색합니다.

예를 들면 다음과 같습니다.



- 응용 프로그램을 선택하고 \* 선택 \* 을 클릭합니다.
  - 다음 \* 을 클릭합니다.
- f. 검토 + 할당 \* 을 클릭합니다.

이제 서비스 보안 주체에 Connector를 배포하는 데 필요한 Azure 권한이 있습니다.

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

**Windows Azure** 서비스 관리 **API** 권한을 추가하는 중입니다

서비스 보안 주체는 "Windows Azure Service Management API" 권한이 있어야 합니다.

단계


1. Azure Active Directory \* 서비스에서 \* 앱 등록 \* 을 클릭하고 응용 프로그램을 선택합니다.
2. API 권한 > 권한 추가 \* 를 클릭합니다.
3. Microsoft API \* 에서 \* Azure Service Management \* 를 선택합니다.

## Request API permissions













Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs



**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

|   |   |  |
|---|---|--|
|  <p><b>Azure Batch</b><br/>Schedule large-scale parallel and HPC applications in the cloud</p>                                       |  <p><b>Azure Data Catalog</b><br/>Programmatic access to Data Catalog resources to register, annotate and search data assets</p> |  <p><b>Azure Data Explorer</b><br/>Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</p>          |
|  <p><b>Azure Data Lake</b><br/>Access to storage and compute for big data analytic scenarios</p>                                    |  <p><b>Azure DevOps</b><br/>Integrate with Azure DevOps and Azure DevOps server</p>   |  <p><b>Azure Import/Export</b><br/>Programmatic control of import/export jobs</p>  |
|  <p><b>Azure Key Vault</b><br/>Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</p>    |  <p><b>Azure Rights Management Services</b><br/>Allow validated users to read and write protected content</p>                  |  <p><b>Azure Service Management</b><br/>Programmatic access to much of the functionality available through the Azure portal</p>                   |
|  <p><b>Azure Storage</b><br/>Secure, massively scalable object and data lake storage for unstructured and semi-structured data</p> |  <p><b>Customer Insights</b><br/>Create profile and interaction models for your products</p>                                   |  <p><b>Data Export Service for Microsoft Dynamics 365</b><br/>Export data from Microsoft Dynamics CRM organization to an external destination</p> |

4. Access Azure Service Management as organization users \* 를 클릭한 다음 \* Add permissions \* 를 클릭합니다.

## Request API permissions

< All APIs



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user\_impersonation

Access Azure Service Management as organization users (preview) ⓘ

애플리케이션 ID 및 디렉토리 ID를 가져오는 중입니다

Azure 계정을 Cloud Manager에 추가하는 경우 응용 프로그램의 응용 프로그램(클라이언트) ID와 디렉터리(테넌트) ID를 제공해야 합니다. Cloud Manager는 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

단계

1. Azure Active Directory \* 서비스에서 \* 앱 등록 \* 을 클릭하고 응용 프로그램을 선택합니다.
2. 응용 프로그램(클라이언트) ID \* 와 \* 디렉터리(테넌트) ID \* 를 복사합니다.



클라이언트 암호 생성

클라이언트 암호를 생성한 다음 Cloud Manager가 이 암호를 사용하여 Azure AD를 인증할 수 있도록 Cloud Manager에 비밀의 값을 제공해야 합니다.

단계

1. Azure Active Directory \* 서비스를 엽니다.
2. 앱 등록 \* 을 클릭하고 응용 프로그램을 선택합니다.



3. 인증서 및 비밀 > 새 클라이언트 비밀 \* 을 클릭합니다.
4. 비밀과 기간에 대한 설명을 제공하십시오.
5. 추가 \* 를 클릭합니다.
6. 클라이언트 암호 값을 복사합니다.

#### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

| <a href="#">+ New client secret</a> |           |                                  |
|-------------------------------------|-----------|----------------------------------|
| DESCRIPTION                         | EXPIRES   | VALUE                            |
| test secret                         | 8/16/2020 | *sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA |

Copy to clipboard

이제 서비스 보안 주체가 설정되었으므로 응용 프로그램(클라이언트) ID, 디렉터리(테넌트) ID 및 클라이언트 암호 값을 복사해야 합니다. Azure 계정을 추가할 때 Cloud Manager에 이 정보를 입력해야 합니다.

#### Cloud Manager에 자격 증명 추가

필요한 권한이 있는 Azure 계정을 제공한 후 해당 계정에 대한 자격 증명을 Cloud Manager에 추가할 수 있습니다. 이 단계를 완료하면 다른 Azure 자격 증명을 사용하여 Cloud Volumes ONTAP를 시작할 수 있습니다.

클라우드 공급자에서 이러한 자격 증명을 만든 경우 사용할 수 있을 때까지 몇 분 정도 걸릴 수 있습니다. 몇 분 후에 Cloud Manager에 자격 증명을 추가합니다.

Cloud Manager 설정을 변경하려면 먼저 Connector를 생성해야 합니다. ["자세히 알아보기"](#).

#### 단계

1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 \* 자격 증명 \* 을 선택합니다.

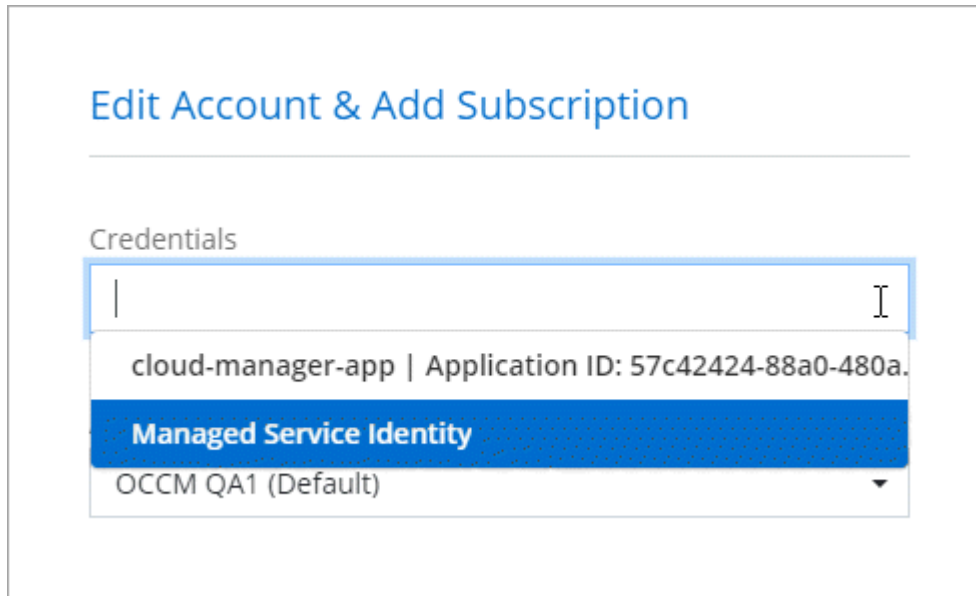


2. 자격 증명 추가 \* 를 클릭하고 마법사의 단계를 따릅니다.
  - a. \* 자격 증명 위치 \*: \* Microsoft Azure > 커넥터 \* 를 선택합니다.
  - b. \* 자격 증명 정의 \*: 필요한 권한을 부여하는 Azure Active Directory 서비스 보안 주체에 대한 정보를 입력합니다.
    - 응용 프로그램(클라이언트) ID: 을 참조하십시오 [\[Getting the application ID and directory ID\]](#).
    - 디렉터리(테넌트) ID: 을 참조하십시오 [\[Getting the application ID and directory ID\]](#).
    - 클라이언트 암호: 을 참조하십시오 [\[Creating a client secret\]](#).
  - c. \* Marketplace 구독 \*: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.

PAYGO(시간당 급여)로 Cloud Volumes ONTAP를 지불하려면 Azure 마켓플레이스의 구독과 Azure 자격 증명이 연결되어 있어야 합니다.

d. \* 검토 \*: 새 자격 증명에 대한 세부 정보를 확인하고 \* 추가 \* 를 클릭합니다.

이제 세부 정보 및 자격 증명 페이지에서 다른 자격 증명 집합으로 전환할 수 있습니다 ["새 작업 환경을 만들 때"](#)



기존 자격 증명을 관리합니다

Marketplace 구독을 연결하고 자격 증명을 편집하고 삭제하여 Cloud Manager에 이미 추가한 Azure 자격 증명을 관리합니다.

#### **Azure Marketplace** 구독을 자격 증명에 연결

Azure 자격 증명을 Cloud Manager에 추가한 후 Azure Marketplace 구독을 해당 자격 증명에 연결할 수 있습니다. 구독을 통해 선불 종량제 Cloud Volumes ONTAP 시스템을 생성하고 다른 NetApp 클라우드 서비스를 사용할 수 있습니다.

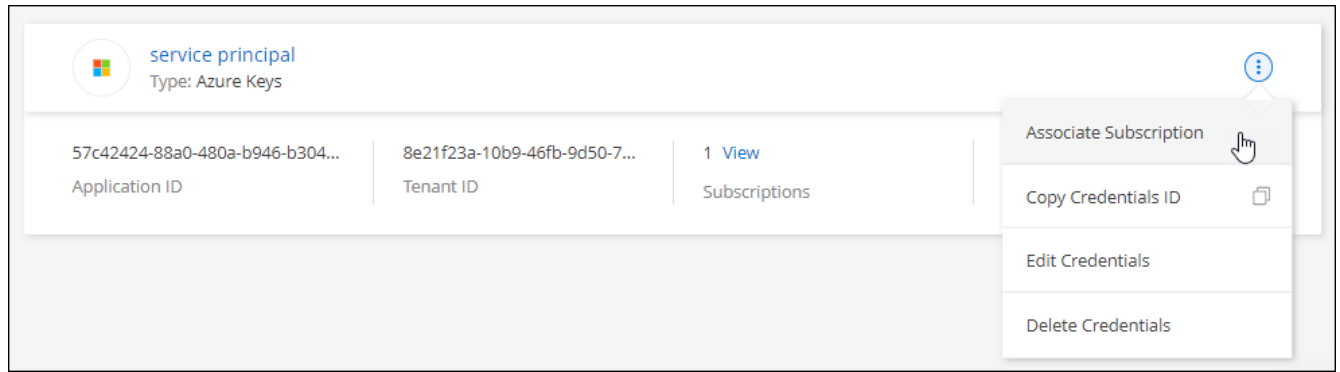
Cloud Manager에 자격 증명을 이미 추가한 후에 Azure Marketplace 구독을 연결할 수 있는 두 가지 시나리오가 있습니다.

- 처음에 Cloud Manager에 자격 증명을 추가했을 때 구독을 연결하지 않았습니다.
- 기존 Azure Marketplace 구독을 새 구독으로 바꾸려는 경우

Cloud Manager 설정을 변경하려면 먼저 Connector를 생성해야 합니다. ["자세히 알아보기"](#).

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 \* 자격 증명 \* 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 클릭한 다음 \* 가입 연결 \* 을 선택합니다.



3. 드롭다운 목록에서 구독을 선택하거나 \* 구독 추가 \* 를 클릭하고 단계에 따라 새 구독을 만듭니다.

다음 비디오는 작업 환경 마법사의 컨텍스트에서 시작되지만 \* 구독 추가 \* 를 클릭한 후 동일한 워크플로를 보여 줍니다.

▶ [https://docs.netapp.com/ko-kr/cloud-manager-setup-admin//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/ko-kr/cloud-manager-setup-admin//media/video_subscribing_azure.mp4) (video)

#### 자격 증명 편집

Azure 서비스 자격 증명에 대한 세부 정보를 수정하여 Cloud Manager에서 Azure 자격 증명을 편집합니다. 예를 들어, 서비스 보안 주체 응용 프로그램에 대해 새 암호가 만들어진 경우 클라이언트 암호를 업데이트해야 할 수 있습니다.

#### 단계

1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 \* 자격 증명 \* 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 클릭한 다음 \* 자격 증명 편집 \* 을 선택합니다.
3. 필요한 내용을 변경한 다음 \* 적용 \* 을 클릭합니다.

자격 증명을 삭제하는 중입니다

자격 증명 세트가 더 이상 필요하지 않으면 Cloud Manager에서 삭제할 수 있습니다. 작업 환경과 연결되지 않은 자격 증명만 삭제할 수 있습니다.

#### 단계

1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 \* 자격 증명 \* 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 클릭한 다음 \* 자격 증명 삭제 \* 를 선택합니다.
3. 확인하려면 \* 삭제 \* 를 클릭합니다.

## Google Cloud 자격 증명

### Google Cloud 프로젝트, 권한 및 계정

서비스 계정은 Cloud Manager에 Connector와 동일한 프로젝트 또는 다른 프로젝트에 있는 Cloud Volumes ONTAP 시스템을 배포 및 관리할 수 있는 권한을 제공합니다.

## Cloud Manager에 대한 프로젝트 및 권한

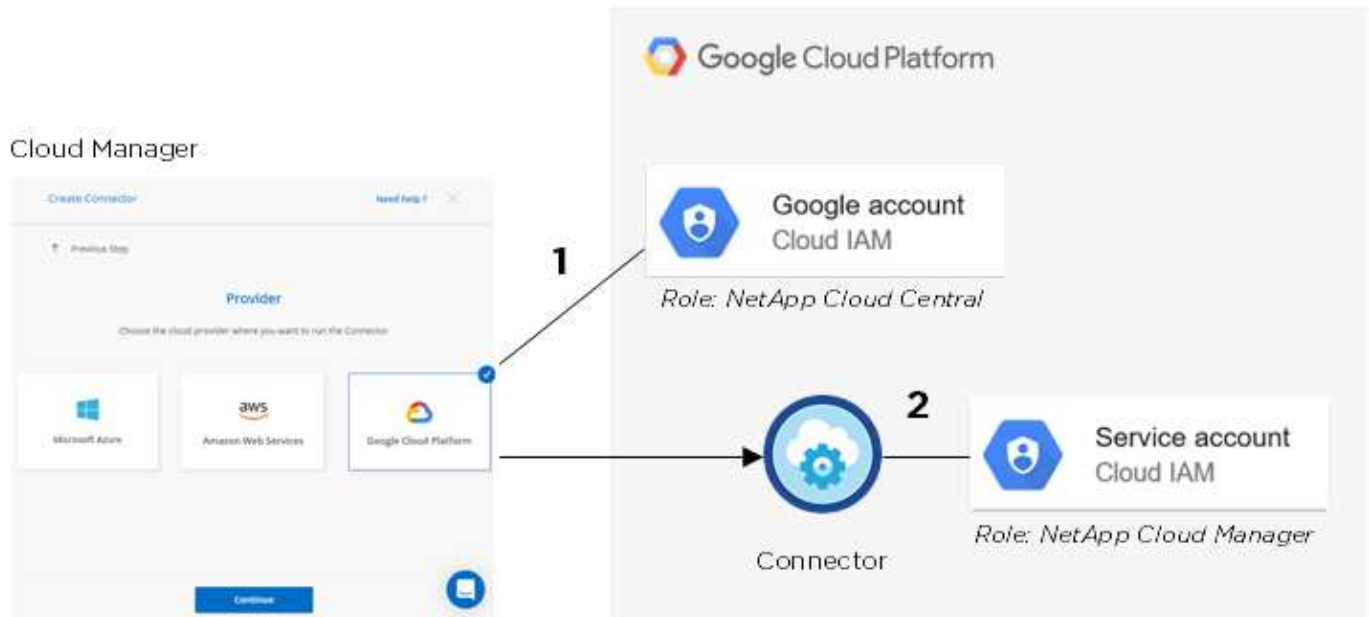
Google Cloud에서 Cloud Volumes ONTAP를 배포하려면 먼저 Google Cloud 프로젝트에 Connector를 배포해야 합니다. Connector는 사내 또는 다른 클라우드 공급자에서 실행할 수 없습니다.

Cloud Manager에서 직접 Connector를 구축하기 전에 다음 두 가지 권한 세트가 있어야 합니다.

1. Cloud Manager에서 Connector VM 인스턴스를 시작할 수 있는 권한이 있는 Google 계정을 사용하여 Connector를 배포해야 합니다.
2. 커넥터를 배포할 때 를 선택하라는 메시지가 나타납니다 **"서비스 계정"** VM 인스턴스의 경우. Cloud Manager는 서비스 계정에서 권한을 받아 사용자를 대신하여 Cloud Volumes ONTAP 시스템을 생성하고 관리합니다. 권한은 서비스 계정에 사용자 지정 역할을 첨부하여 제공됩니다.

사용자와 서비스 계정에 필요한 권한이 포함된 YAML 파일을 두 개 설정했습니다. **"YAML 파일을 사용하여 권한을 설정하는 방법을 알아보십시오"**.

다음 이미지는 위의 숫자 1과 2에 설명된 사용 권한 요구 사항을 보여 줍니다.



## Cloud Volumes ONTAP 프로젝트

Cloud Volumes ONTAP는 Connector와 같은 프로젝트나 다른 프로젝트에 상주할 수 있습니다. 다른 프로젝트에 Cloud Volumes ONTAP를 배포하려면 먼저 해당 프로젝트에 Connector 서비스 계정 및 역할을 추가해야 합니다.

- **"서비스 계정 설정 방법에 대해 알아보십시오"**
- **"GCP에서 Cloud Volumes ONTAP를 구축하고 프로젝트를 선택하는 방법에 대해 알아보십시오"**

## Cloud Manager의 GCP 자격 증명 및 구독 관리

Connector VM 인스턴스와 연결된 자격 증명을 관리할 수 있습니다.

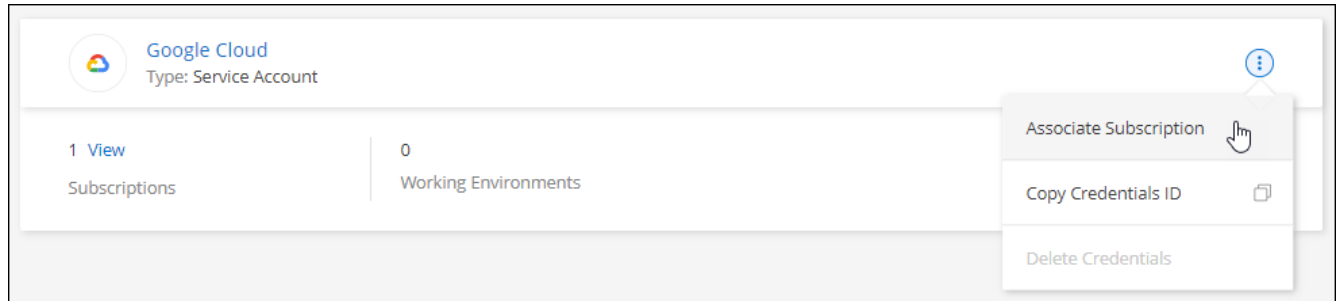
## Marketplace 구독을 GCP 자격 증명과 연결합니다

GCP에서 Connector를 구축하면 Cloud Manager가 Connector VM 인스턴스와 연결된 기본 자격 증명 세트를 생성합니다. Cloud Manager에서 Cloud Volumes ONTAP를 구축하는 데 사용하는 자격 증명입니다.

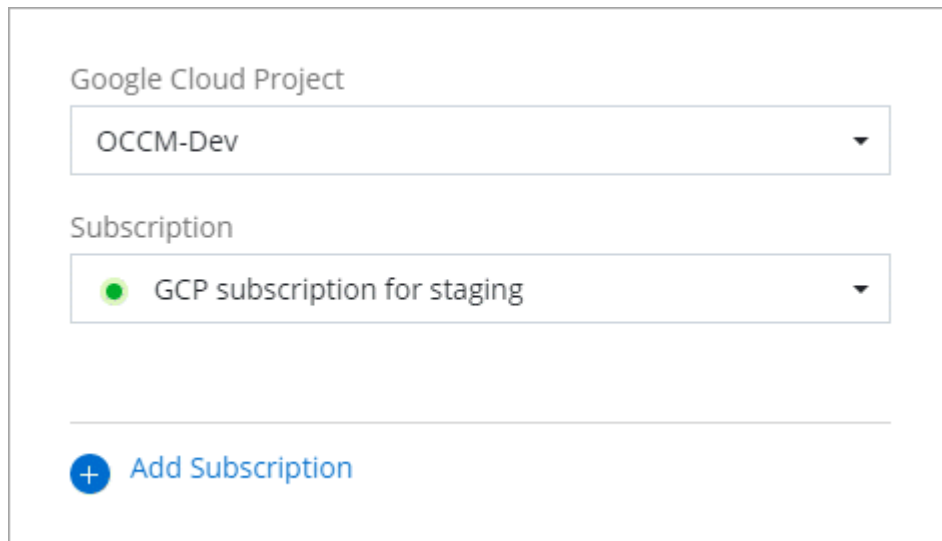
언제든지 이러한 자격 증명과 연결된 마켓플레이스 구독을 변경할 수 있습니다. 구독을 통해 선불 종량제 Cloud Volumes ONTAP 시스템을 생성하고 다른 NetApp 클라우드 서비스를 사용할 수 있습니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 \* 자격 증명 \* 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 클릭한 다음 \* 가입 연결 \* 을 선택합니다.



3. 드롭다운 목록에서 Google Cloud 프로젝트 및 구독을 선택합니다.



4. Associate \* 를 클릭합니다.
5. 아직 구독이 없는 경우 \* 구독 추가 \* 를 클릭하고 아래 단계에 따라 새 구독을 만듭니다.



다음 단계를 완료하기 전에 Google Cloud 계정뿐만 아니라 NetApp Cloud Central 로그인에서도 청구 관리자 권한이 모두 있는지 확인하십시오.

6. 구독 단계를 보고 \* 계속 \* 을 클릭합니다.

## Add Subscription


### Subscription Steps:


- ① **Cloud Manager**  
Clicking **Continue** to create your subscription from the Google Cloud Marketplace.
  - ② **Google Cloud Marketplace**  
Subscribe and then then click **Register With NetApp** to configure your account from Cloud Central.
  - ③ **Cloud Central**  
Save your subscription.
  - ④ **Cloud Manager**  
Associate the Marketplace subscription with your Google Cloud project.
- ▶ View video instructions


Continue


Cancel

7. 로 리디렉션된 후 "[Google Cloud Marketplace의 NetApp Cloud Manager 페이지를 참조하십시오](#)"상단 탐색 메뉴에서 올바른 프로젝트가 선택되어 있는지 확인합니다.


Google Cloud Platform


My First Project





# Cloud Manager for Cloud Volumes ONTAP

NetApp, Inc.

Enterprise-grade data management and protection

SUBSCRIBE

OVERVIEW

PRICING

SUPPORT

## Overview

Cloud Volumes ONTAP is a data-management layer that runs natively on Google Cloud infrastructure enabling enhanced control, data protection, mobility and agility for business application data. Get consistent enterprise-grade storage across your hybrid cloud platforms with built-in disaster recovery, backup and ransomware protection. Seamlessly migrate enterprise applications without reengineering. Create company-wide file shares with simultaneous NFS and CIFS/SMB access and iSCSI block storage for GCE instances with scalability up to 368TB. Automate persistent storage provisioning for your Kubernetes clusters. Accelerate CI/CD cycles with instant, zero-capacity data replication. Reduce storage costs by 70% with advanced storage efficiencies. Cloud Manager is the console used to deploy, manage and automate Cloud Volumes ONTAP instances across the hybrid multi-cloud.

[Learn more](#)

## Additional details

Type: [APIs & services](#)

Last updated: 3/26/21

Category: [Storage](#)

Runs on: NetApp, Inc. Cloud Servers

8. 구독 \* 을 클릭합니다.
9. 적절한 청구 계정을 선택하고 이용 약관에 동의합니다.

## 2. Purchase details

Select a billing account \*

Secondary\_Billing\_Account

## 3. Terms

### Cancellation and change policy

- Usage fee is billed every month.
- You can cancel the service at any time and it will take effect immediately. You will be billed by the amount you used for that month.

### Additional terms

- ☒ I understand this subscription will be automatically renewed at the end of the current term.
- ☒ I authorize Google LLC and its affiliates ("Google") to share my purchase, usage, operational (e.g., project lifecycle events), support ticket, and account information with NetApp, Inc., its affiliates and subcontractors, for the purposes of providing the service, sales attribution, and technical support. I represent that I have the authority to bind my company.
- ☒ By deploying the software or accessing the service you are agreeing to comply with the [End User License Agreement](#), [GCP Marketplace Terms of Service](#), and the terms of applicable open source software licenses bundled with the software or service. Please review these terms and licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.
- By using this product, you understand that certain account and usage information may be shared with NetApp, Inc. for the purposes of financial accounting, sales attribution, performance analysis, and support. ⓘ
- Google is providing this software or service "as-is" and any support for this software or service will be provided by NetApp, Inc. under their terms of service.

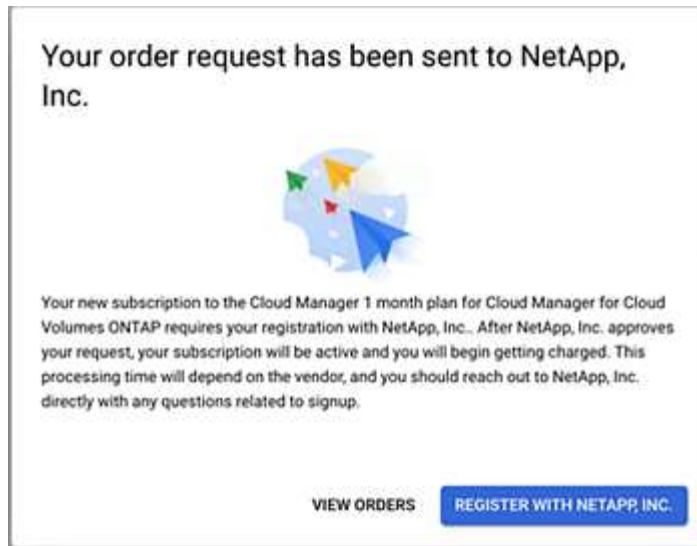
SUBSCRIBE

10. 구독 \* 을 클릭합니다.

이 단계에서는 전송 요청을 NetApp에 전송합니다.

11. 팝업 대화 상자에서 \* Register with NetApp, Inc. \* 를 클릭하여 NetApp Cloud Central로 리디렉션합니다.

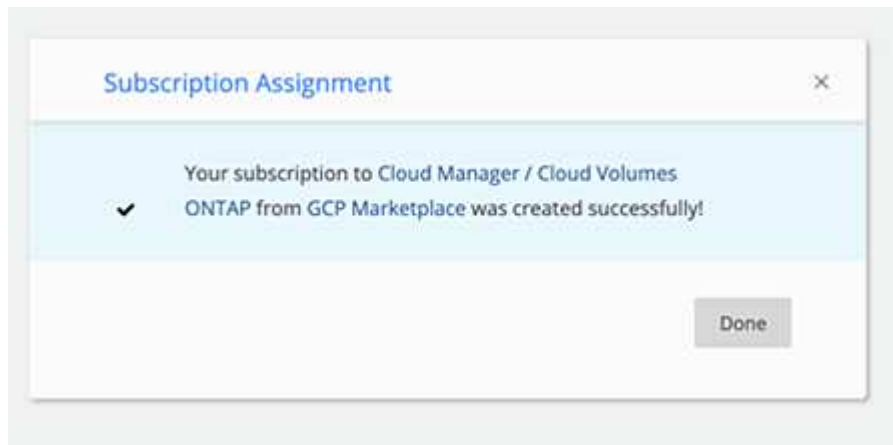




GCP 구독을 NetApp 계정에 연결하려면 이 단계를 완료해야 합니다. 이 페이지에서 리디렉션되어 NetApp Cloud Central에 로그인할 때까지 구독 연결 프로세스가 완료되지 않습니다.

12. Cloud Central로 리디렉션되면 NetApp Cloud Central에 로그인하거나 등록하고 \* 완료 \* 를 클릭하여 계속 진행하십시오.

GCP 구독은 사용자 로그인과 연결된 모든 NetApp 계정에 연결됩니다.



조직의 누군가가 이미 청구 계정에서 NetApp Cloud Manager 구독을 신청하면 로 리디렉션됩니다 ["NetApp Cloud Central의 Cloud Volumes ONTAP 페이지"](#) 대신 예기치 않은 상황인 경우 NetApp 세일즈 팀에 문의하십시오. Google은 Google 청구 계정당 하나의 가입만 활성화합니다.

13. 이 프로세스가 완료되면 Cloud Manager의 자격 증명 페이지로 돌아가 이 새 구독을 선택합니다.

Google Cloud Project

OCCM-Dev
▼

Subscription

GCP subscription for staging
▼

+ Add Subscription

## 마켓플레이스 가입 프로세스 문제 해결

Google Cloud Marketplace를 통해 Cloud Volumes ONTAP을 구독하는 경우 잘못된 권한이 있거나 NetApp Cloud Central로 리디렉션된 후 우연히 팔로우하지 않아 조각화될 수 있습니다. 이 경우 다음 단계를 사용하여 구독 프로세스를 완료합니다.

### 단계

- 로 이동합니다 "[Google Cloud Marketplace의 NetApp Cloud Manager 페이지를 참조하십시오](#)" 주문 상태를 확인합니다. 페이지에 \* 공급자 \* 에서 관리 \* 가 표시되면 아래로 스크롤하여 \* 주문 관리 \* 를 클릭합니다.

Pricing

The product was purchased on 12/9/20.
MANAGE ORDERS

- 주문에 녹색 확인 표시가 있고 예상치 못한 경우 동일한 대금 청구 계정을 사용하는 조직의 다른 사용자가 이미 구독 중인 것일 수 있습니다. 예기치 않은 요청이거나 이 구독에 대한 자세한 정보가 필요한 경우 NetApp 세일즈 팀에 문의하십시오.

| Filter Enter property name or value |              |               |          |              |               |          |                  |            |           |   |
|-------------------------------------|--------------|---------------|----------|--------------|---------------|----------|------------------|------------|-----------|---|
| Status                              | Order number | Plan          | Discount | Start date ↓ | Plan duration | End date | Payment Schedule | Auto-renew | Next plan |   |
| <span></span>                       | 2eebbc...    | Cloud Manager | -        | 10/21/21     | 1 month       | -        | Postpay          | N/A        | N/A       | ⋮ |

- 주문에 시계 및 \* 보류 \* 상태가 표시되면 마켓플레이스 페이지로 돌아가서 \* 공급자 관리 \* 를 선택하여 위에 설명된 프로세스를 완료합니다.

| Filter Enter property name or value |              |               |          |              |               |          |                  |            |           |   |
|-------------------------------------|--------------|---------------|----------|--------------|---------------|----------|------------------|------------|-----------|---|
| Status                              | Order number | Plan          | Discount | Start date ↓ | Plan duration | End date | Payment Schedule | Auto-renew | Next plan |   |
| <span></span>                       | d56c66...    | Cloud Manager | -        | Pending      | 1 month       | Pending  | Postpay          | N/A        | N/A       | ⋮ |

# Cloud Manager에서 NetApp Support 사이트 계정을 추가하고 관리합니다

NSS(NetApp Support Site) 계정의 자격 증명을 제공하여 Cloud Volumes ONTAP의 주요 워크플로우를 활성화하고 Active IQ를 통해 예측 분석 및 사전 지원을 활성화합니다.

## 개요

다음 작업을 수행하려면 NetApp Support 사이트 계정을 Cloud Manager에 추가해야 합니다.

- BYOL(Bring Your Own License) 방식으로 Cloud Volumes ONTAP 구축

NSS 계정을 제공해야 Cloud Manager가 라이선스 키를 업로드하고 구입한 용어에 대한 구독을 활성화할 수 있습니다. 여기에는 기간 갱신을 위한 자동 업데이트가 포함됩니다.

- 선불 종량제 Cloud Volumes ONTAP 시스템을 등록합니다

NSS 계정을 제공하면 시스템에 대한 지원을 활성화하고 NetApp 기술 지원 리소스에 액세스할 수 있습니다.

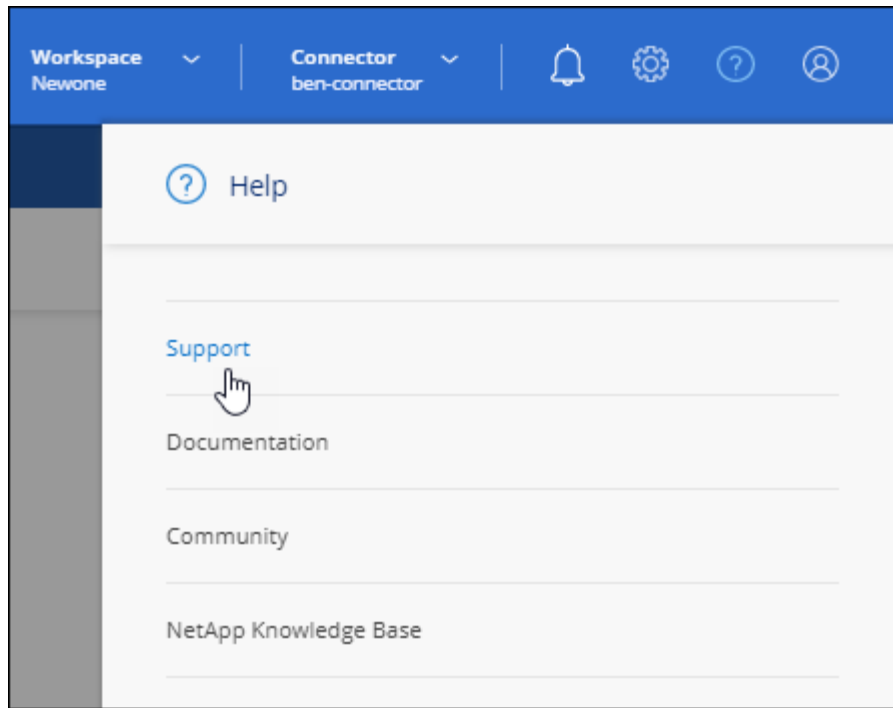
- Cloud Volumes ONTAP 소프트웨어를 최신 릴리즈로 업그레이드합니다
- 클라우드 관리자 내에서 Active IQ 디지털 자문업체 사용

## NSS 계정을 추가합니다

지원 대시보드를 이용하면 모든 NetApp Support 사이트 계정을 단일 위치에서 추가 및 관리할 수 있습니다.

### 단계

1. 아직 NetApp Support 사이트 계정이 없는 경우 **"1인 등록"**.
2. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 \* 지원 \* 을 선택합니다.



3. NSS 관리 > NSS 계정 추가 \* 를 클릭합니다.
4. 메시지가 표시되면 \* 계속 \* 을 클릭하여 Microsoft 로그인 페이지로 리디렉션됩니다.

NetApp은 Microsoft Azure Active Directory를 지원 및 라이선싱과 관련된 인증 서비스의 ID 공급자로 사용합니다.

5. 로그인 페이지에서 인증 프로세스를 수행할 수 있도록 NetApp Support 사이트의 등록 이메일 주소와 암호를 제공합니다.

이 작업을 수행하면 Cloud Manager에서 NSS 계정을 사용할 수 있습니다.

계정에 대한 다음 요구 사항을 참고하십시오.

- 계정은 고객 수준 계정이어야 합니다(게스트 또는 임시 계정이 아님).
- 노드 기반 BYOL 시스템을 구축하려는 경우:
  - 이 계정은 BYOL 시스템의 일련 번호에 액세스할 수 있는 권한이 있어야 합니다.
  - 안전한 BYOL 구독을 구입한 경우 보안 NSS 계정이 필요합니다.

이제 사용자는 새 Cloud Volumes ONTAP 시스템을 생성할 때, 기존 Cloud Volumes ONTAP 시스템을 등록할 때, 그리고 Active IQ에서 데이터를 볼 때 계정을 선택할 수 있습니다.

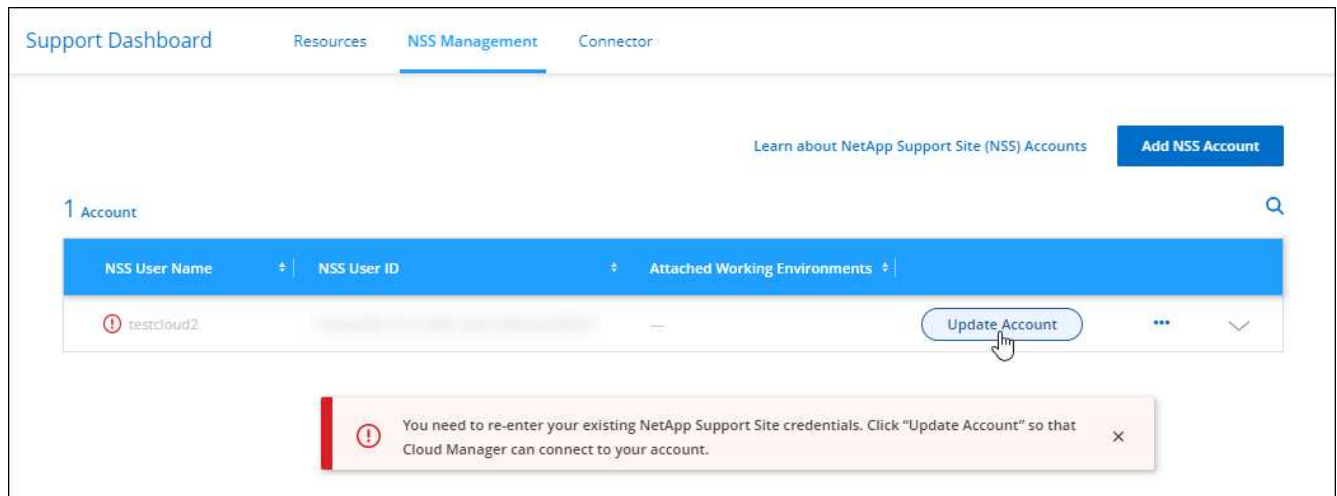
- ["AWS에서 Cloud Volumes ONTAP 실행"](#)
- ["Azure에서 Cloud Volumes ONTAP 실행"](#)
- ["GCP에서 Cloud Volumes ONTAP를 시작합니다"](#)
- ["선불 종량제 시스템을 등록하는 중입니다"](#)

## NSS 계정을 업데이트하여 새 인증 방법을 확인합니다

2021년 11월부터 NetApp은 Microsoft Azure Active Directory를 지원 및 라이선싱과 관련된 인증 서비스의 ID 공급자로 사용합니다. 이 업데이트의 결과로, Cloud Manager에서 이전에 추가한 기존 계정의 자격 증명을 업데이트하라는 메시지를 표시합니다.

단계

1. 아직 수행하지 않았다면 ["현재 NetApp 계정에 연결할 Microsoft Azure Active Directory B2C 계정을 만듭니다"](#).
2. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 \* 지원 \* 을 선택합니다.
3. NSS 관리 \* 를 클릭합니다.
4. 업데이트할 NSS 계정의 경우 \* 계정 업데이트 \* 를 클릭합니다.



5. 메시지가 표시되면 \* 계속 \* 을 클릭하여 Microsoft 로그인 페이지로 리디렉션됩니다.

NetApp은 Microsoft Azure Active Directory를 지원 및 라이선싱과 관련된 인증 서비스의 ID 공급자로 사용합니다.

6. 로그인 페이지에서 인증 프로세스를 수행할 수 있도록 NetApp Support 사이트의 등록 이메일 주소와 암호를 제공합니다.

프로세스가 완료되면 업데이트한 계정이 이제 테이블에 `_new_account` 로 나열됩니다. 기존 작업 환경 연관을 비롯하여 계정의 `_listed_version`이 테이블에 계속 나열되어 있습니다.

7. 기존 Cloud Volumes ONTAP 작업 환경이 기존 버전의 계정에 연결된 경우, 다음 ~ 단계를 수행하십시오 [이러한 작업 환경을 다른 NSS 계정에 연결합니다](#).
8. NSS 계정의 이전 버전으로 이동하고 를 클릭합니다 ... 그런 다음 \* 삭제 \* 를 선택합니다.

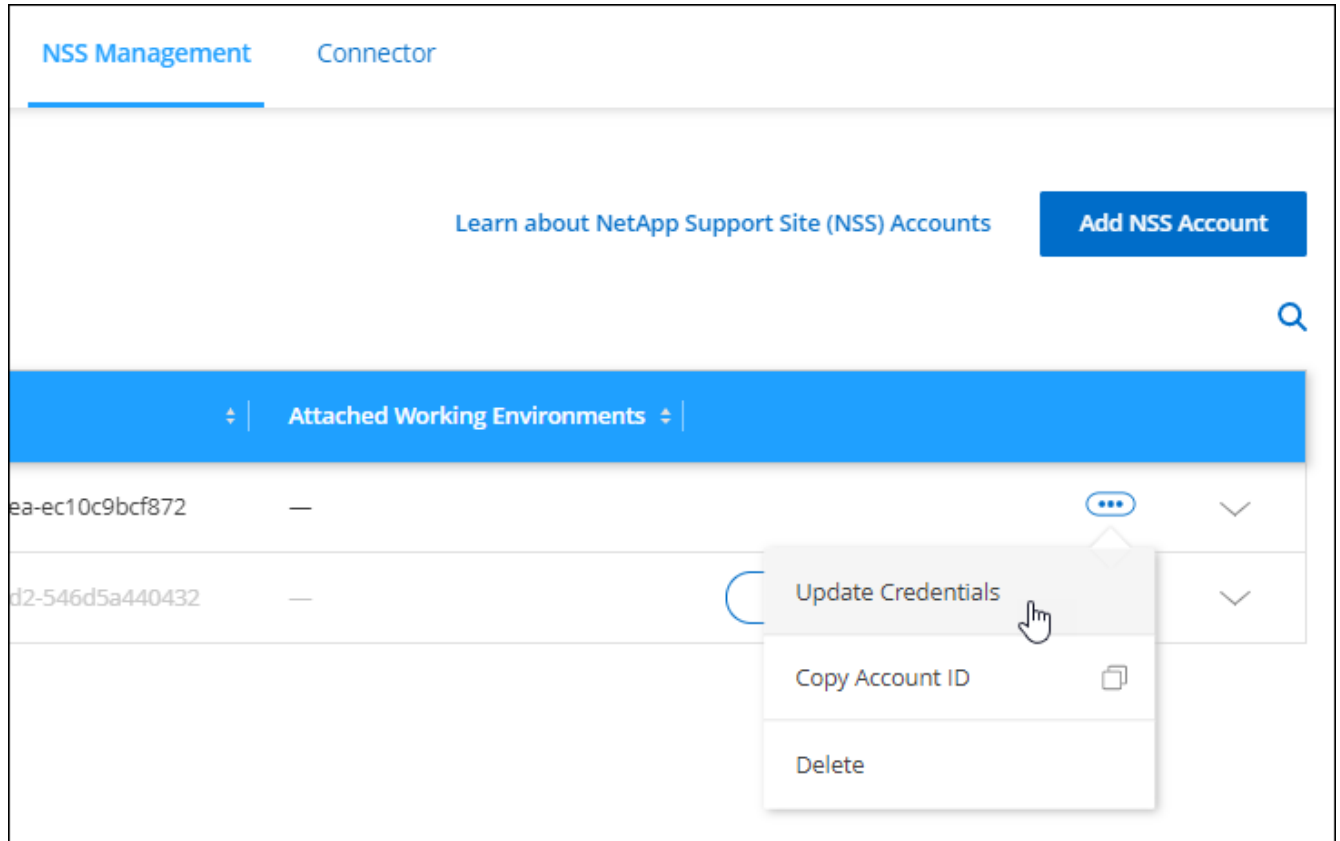
## NSS 자격 증명을 업데이트합니다

NSS 계정의 자격 증명을 변경할 때마다 Cloud Manager에서 자격 증명을 업데이트해야 합니다.

단계

1. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 \* 지원 \* 을 선택합니다.
2. NSS 관리 \* 를 클릭합니다.

3. 업데이트할 NSS 계정의 경우 을 클릭합니다 ... 그런 다음 \* 자격 증명 업데이트 \* 를 선택합니다.



4. 메시지가 표시되면 \* 계속 \* 을 클릭하여 Microsoft 로그인 페이지로 리디렉션됩니다.

NetApp은 Microsoft Azure Active Directory를 지원 및 라이선싱과 관련된 인증 서비스의 ID 공급자로 사용합니다.

5. 로그인 페이지에서 인증 프로세스를 수행할 수 있도록 NetApp Support 사이트의 등록 이메일 주소와 암호를 제공합니다.

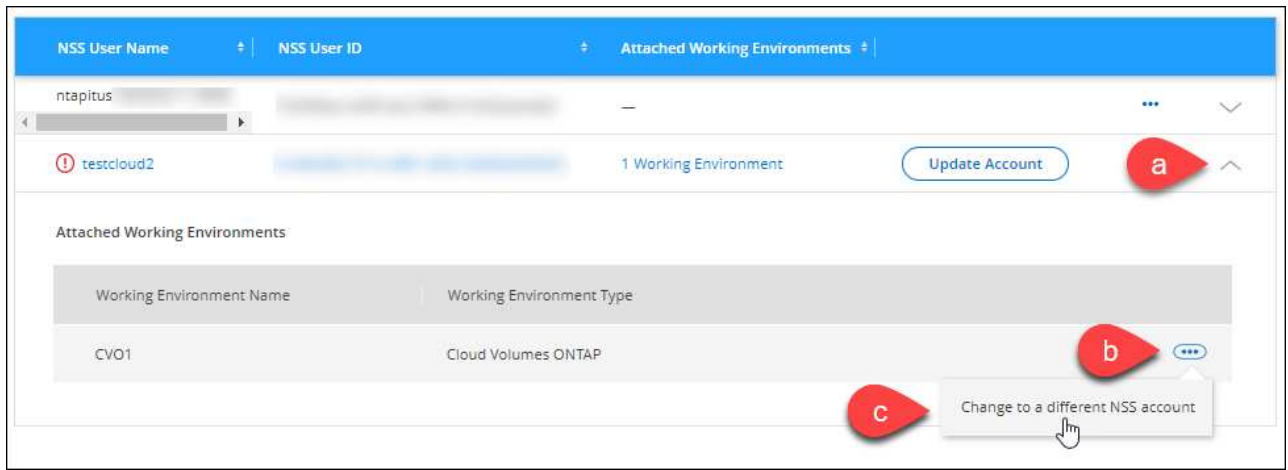
## 작업 환경을 다른 **NSS** 계정에 연결합니다

조직에 여러 NetApp Support 사이트 계정이 있는 경우 Cloud Volumes ONTAP 시스템과 연결된 계정을 변경할 수 있습니다.

이 기능은 NetApp에서 ID 관리를 위해 채택한 Microsoft Azure AD를 사용하도록 구성된 NSS 계정에서만 지원됩니다. 이 기능을 사용하려면 \* NSS 계정 추가 \* 또는 \* 계정 업데이트 \* 를 클릭해야 합니다.

### 단계

1. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 \* 지원 \* 을 선택합니다.
2. NSS 관리 \* 를 클릭합니다.
3. NSS 계정을 변경하려면 다음 단계를 수행하십시오.
  - a. 작업 환경이 현재 연결되어 있는 NetApp Support 사이트 계정의 행을 확장합니다.
  - b. 연결을 변경할 작업 환경의 경우 을 클릭합니다 ...
  - c. 다른 NSS 계정으로 변경 \* 을 선택합니다.



d. 계정을 선택한 다음 \* 저장 \* 을 클릭합니다.

## NSS 계정의 이메일 주소를 표시합니다

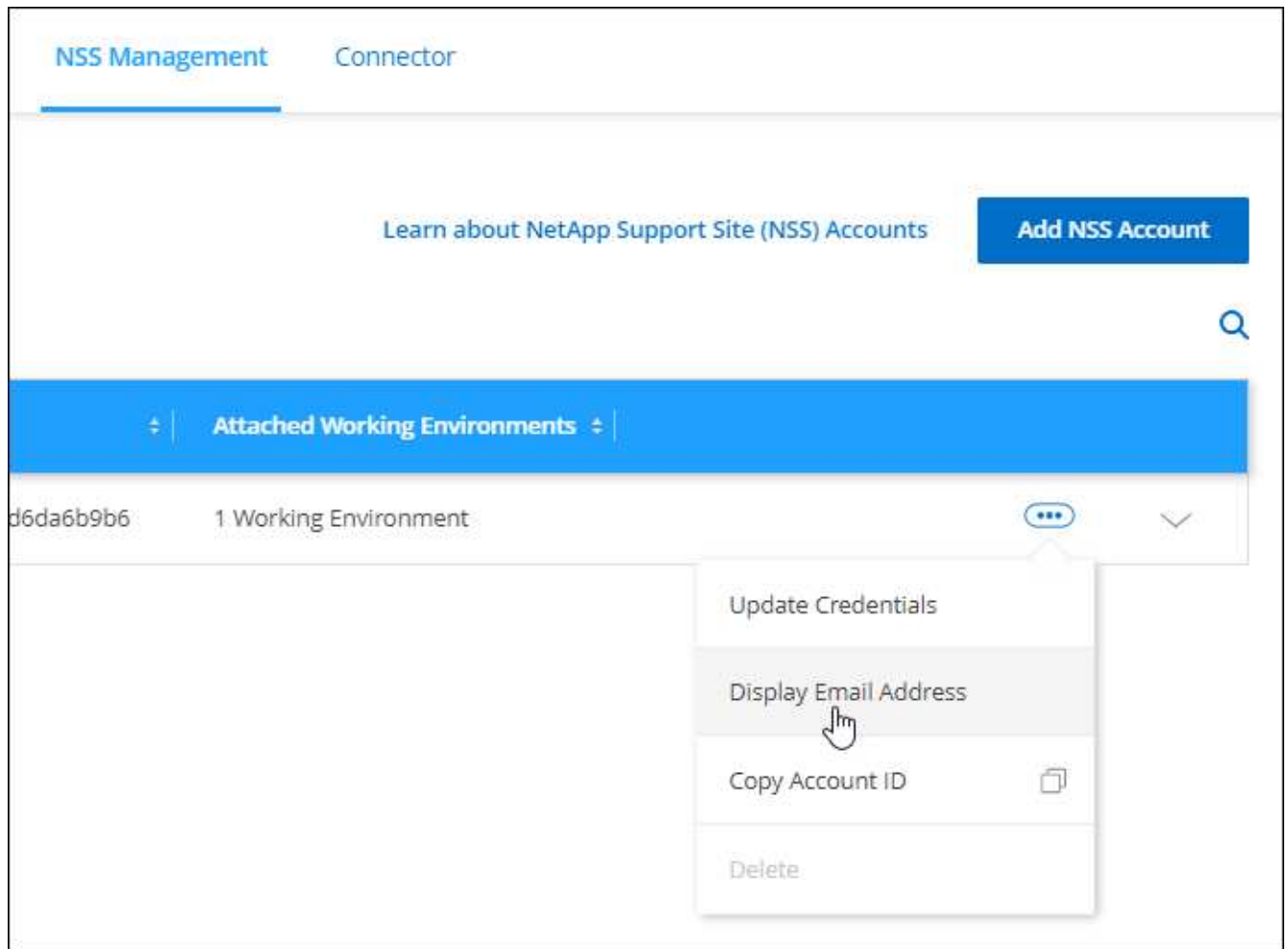
이제 NetApp Support 사이트 계정이 인증 서비스에 Microsoft Azure Active Directory를 사용하므로 Cloud Manager에 표시되는 NSS 사용자 이름은 일반적으로 Azure AD에서 생성한 식별자입니다. 따라서 해당 계정과 연결된 전자 메일 주소를 즉시 알지 못할 수 있습니다. Cloud Manager에는 관련 이메일 주소를 표시하는 옵션이 있습니다.



NSS 관리 페이지로 이동하면 Cloud Manager에서 테이블의 각 계정에 대한 토큰을 생성합니다. 이 토큰에는 연결된 이메일 주소에 대한 정보가 포함됩니다. 그런 다음 페이지를 나갈 때 토큰이 제거됩니다. 정보는 캐싱되지 않으며 개인 정보를 보호하는 데 도움이 됩니다.

단계

1. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 \* 지원 \* 을 선택합니다.
2. NSS 관리 \* 를 클릭합니다.
3. 업데이트할 NSS 계정의 경우 을 클릭합니다 ... 그런 다음 \* 이메일 주소 표시 \* 를 선택합니다.



Cloud Manager에는 NetApp Support 사이트의 사용자 이름과 관련 이메일 주소가 표시됩니다. 복사 버튼을 사용하여 이메일 주소를 복사할 수 있습니다.

## NSS 계정을 제거합니다

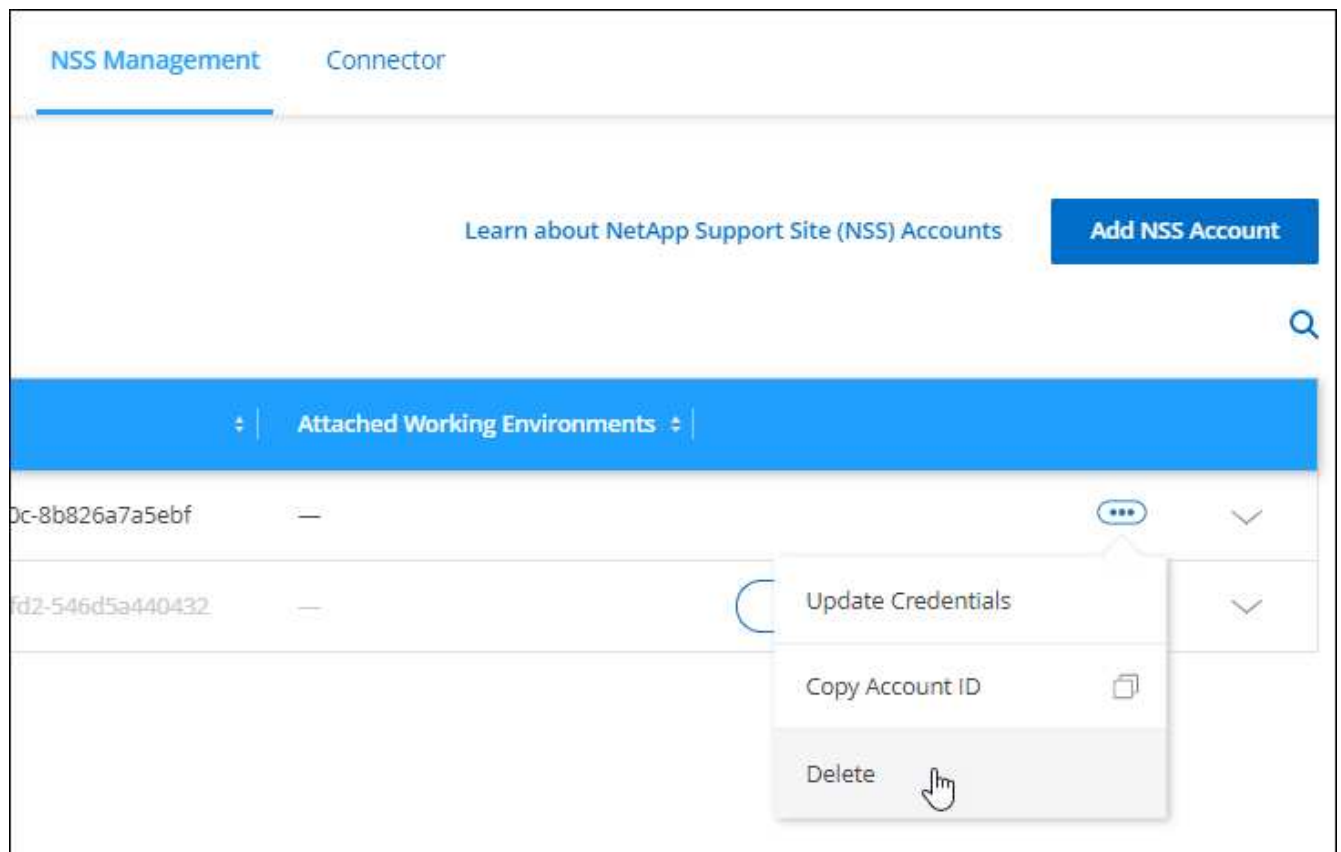
Cloud Manager에서 더 이상 사용하지 않을 NSS 계정을 삭제합니다.

현재 Cloud Volumes ONTAP 작업 환경과 연결된 계정은 삭제할 수 없습니다. 먼저 해야 할 일 [이러한 작업 환경을 다른 NSS 계정에 연결합니다](#).

단계

1. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 \* 지원 \* 을 선택합니다.
2. NSS 관리 \* 를 클릭합니다.
3. 삭제할 NSS 계정의 경우 을 클릭합니다 ... 그런 다음 \* 삭제 \* 를 선택합니다.





4. 확인하려면 \* 삭제 \* 를 클릭합니다.

# 참조하십시오

## Cloud Manager에 대한 권한 요약

Cloud Manager에서 기능과 서비스를 사용하려면 Cloud Manager가 클라우드 환경에서 작업을 수행할 수 있도록 권한을 제공해야 합니다. 이 페이지의 링크를 사용하여 목표에 따라 필요한 사용 권한에 빠르게 액세스할 수 있습니다.

### AWS 권한

| 목적                     | 설명   | 링크  |
|------------------------|--|---|
| 커넥터 전개                 | Cloud Manager에서 Connector를 생성하는 사용자는 AWS에 인스턴스를 구축하기 위한 특정 권한이 필요합니다.  | <a href="#">"Cloud Manager에서 AWS에 Connector를 생성합니다"</a> |
| 커넥터 작동                 | Cloud Manager에서 Connector를 시작하면 인스턴스에 정책이 연결되며, 이 정책은 AWS 계정의 리소스와 프로세스를 관리하는 데 필요한 권한을 제공합니다. 정책을 직접 설정해야 합니다<br><a href="#">"마켓플레이스에서 Connector를 실행합니다"</a> 아니면 <a href="#">"Connector에 AWS 자격 증명을 더 추가합니다"</a> . 또한 새 권한이 후속 릴리스에 추가될 때 정책이 최신 상태인지 확인해야 합니다. | <a href="#">"Connector에 대한 AWS 권한"</a>                  |
| Cloud Volumes ONTAP 작동 | IAM 역할은 AWS의 각 Cloud Volumes ONTAP 노드에 연결되어야 합니다. HA 중재자의 경우도 마찬가지입니다. 기본 옵션은 Cloud Manager에서 IAM 역할을 생성할 수 있도록 하는 것이지만 직접 사용할 수 있습니다.   | <a href="#">"IAM 역할을 직접 설정하는 방법에 대해 알아봅니다"</a>          |

### Azure 권한

| 목적     | 설명  | 링크  |
|--------|---|---|
| 커넥터 전개 | Cloud Manager에서 Connector를 배포하는 경우 Azure에 Connector VM을 배포할 수 있는 권한이 있는 Azure 계정 또는 서비스 보안 주체를 사용해야 합니다.  | <a href="#">"Cloud Manager에서 Azure에 Connector를 생성합니다"</a> |
| 커넥터 작동 | Cloud Manager는 Azure에서 Connector VM을 배포할 때 Azure 구독 내에서 리소스와 프로세스를 관리하는 데 필요한 권한을 제공하는 사용자 지정 역할을 생성합니다.<br><br>사용자 지정 역할을 직접 설정해야 합니다<br><a href="#">"마켓플레이스에서 Connector를 실행합니다"</a> 아니면 <a href="#">"Connector에 Azure 자격 증명을 더 추가합니다"</a> .<br><br>또한 새 권한이 후속 릴리스에 추가될 때 정책이 최신 상태인지 확인해야 합니다. | <a href="#">"Connector에 대한 Azure 권한"</a>                  |

## Google Cloud 권한

| 목적     | 설명  | 링크  |
|--------|---|---|
| 커넥터 전개 | Cloud Manager에서 Connector를 배포하는 Google Cloud 사용자는 Google Cloud에서 Connector를 배포하기 위한 특정 권한이 필요합니다.   | <a href="#">"Connector 배포 권한을 설정합니다"</a>      |
| 커넥터 작동 | Connector VM 인스턴스의 서비스 계정에는 일상적인 작업에 대한 특정 권한이 있어야 합니다. Cloud Manager에서 서비스 계정을 배포할 때 Connector에 서비스 계정을 연결해야 합니다. 또한 새 권한이 후속 릴리스에 추가될 때 정책이 최신 상태인지 확인해야 합니다. | <a href="#">"Connector에 대한 서비스 계정을 설정합니다"</a> |

## Connector에 대한 AWS 권한

Cloud Manager가 AWS에서 Connector 인스턴스를 시작하면 해당 AWS 계정 내의 리소스와 프로세스를 관리할 수 있는 권한을 Connector에 제공하는 인스턴스에 정책을 연결합니다. Connector는 권한을 사용하여 EC2, S3, CloudFormation, IAM, KMS(키 관리 서비스) 등

### IAM 정책

아래에 표시된 IAM 정책은 Connector가 AWS 지역에 따라 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하는데 필요한 권한을 제공합니다.

Cloud Manager에서 직접 Connector를 생성하면 Cloud Manager가 이 정책을 Connector에 자동으로 적용합니다.

AWS Marketplace에서 Connector를 배포하거나 Linux 호스트에 Connector를 수동으로 설치하는 경우 정책을 직접 설정해야 합니다.

또한 새 권한이 후속 릴리스에 추가될 때 정책이 최신 상태인지 확인해야 합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cvoServicePolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",

```

```
"iam:CreateInstanceProfile",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam:ListInstanceProfiles",
"sts:DecodeAuthorizationMessage",
"ec2:AssociateIamInstanceProfile",
"ec2:DescribeIamInstanceProfileAssociations",
"ec2:DisassociateIamInstanceProfile",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3:CreateBucket",
"s3:GetLifecycleConfiguration",
"s3:ListBucketVersions",
"s3:GetBucketPolicyStatus",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketPolicy",
"s3:GetBucketAcl",
"kms:List*",
"kms:ReEncrypt*",
"kms:Describe*",
"kms:CreateGrant",
"ce:GetReservationUtilization",
"ce:GetDimensionValues",
"ce:GetCostAndUsage",
"ce:GetTags",
"ec2:CreatePlacementGroup",
"ec2:DescribeReservedInstancesOfferings",
"sts:AssumeRole",
"ec2:AssignPrivateIpAddresses",
"ec2:CreateRoute",
"ec2:DescribeVpcs",
"ec2:ReplaceRoute",
"ec2:UnassignPrivateIpAddresses",
"s3:PutObjectTagging",
"s3:GetObjectTagging",
"fsx:Describe*",
"fsx:List*",
"ec2:DeleteSecurityGroup",
"ec2:DeleteNetworkInterface",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteRoute",
"ec2:DeletePlacementGroup",
"iam:DeleteRole",
"iam:DeleteRolePolicy",
```

```

        "iam:DeleteInstanceProfile",
        "cloudformation:DeleteStack",
        "ec2:DescribePlacementGroups",
        "iam:GetRolePolicy",
        "s3:ListAllMyBuckets",
        "s3:GetObject",
        "iam:GetRole",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutObject",
        "ec2:ModifyVolume",
        "ec2:DescribeVolumesModifications"
    ],
    "Resource": "*"
},
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "kms:List*",
        "kms:Describe*",
        "ec2:describeVpcEndpoints",
        "kms:ListAliases",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "athena:StopQueryExecution",
        "glue:CreateDatabase",
        "glue:CreateTable",
    ]
}

```

```

        "glue:BatchDeletePartition"
    ],
    "Resource": "*"
},
{
    "Sid": "backupS3Policy",
    "Effect": "Allow",
    "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetObject",
        "s3:PutEncryptionConfiguration",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:DeleteBucket"
    ],
    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
},
{
    "Sid": "tagServicePolicy",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
    ],

```

```

    "Resource": "*"
  },
  {
    "Sid": "fabricPoolS3Policy",
    "Effect": "Allow",
    "Action": [
      "s3:CreateBucket",
      "s3:GetLifecycleConfiguration",
      "s3:PutLifecycleConfiguration",
      "s3:PutBucketTagging",
      "s3:ListBucketVersions",
      "s3:GetBucketPolicyStatus",
      "s3:GetBucketPublicAccessBlock",
      "s3:GetBucketAcl",
      "s3:GetBucketPolicy",
      "s3:PutBucketPublicAccessBlock",
      "s3>DeleteBucket"
    ],
    "Resource": [
      "arn:aws:s3:::fabric-pool*"
    ]
  },
  {
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeRegions"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances"
    ],
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/netapp-adc-manager": "*"
      }
    },
    "Resource": [
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
},

```



```

{
  "Effect": "Allow",
  "Action": [
    "ec2:StartInstances",
    "ec2:TerminateInstances",
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Condition": {
    "StringLike": {
      "ec2:ResourceTag/GFCInstance": "*"
    }
  },
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:StartInstances",
    "ec2:TerminateInstances",
    "ec2:AttachVolume",
    "ec2:DetachVolume",
    "ec2:StopInstances",
    "ec2>DeleteVolume"
  ],
  "Condition": {
    "StringLike": {
      "ec2:ResourceTag/WorkingEnvironment": "*"
    }
  },
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:volume/*"
  ]
},

```

```

    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/WorkingEnvironment": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid": "K8sServicePolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "iam:ListInstanceProfiles",
        "eks:ListClusters",
        "eks:DescribeCluster"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GFCservicePolicy",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudwatch:GetMetricStatistics",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    }
  ]
}

```

### GovCloud(미국) 지역

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [

```

```
"iam:ListInstanceProfiles",
"iam:CreateRole",
"iam:DeleteRole",
"iam:PutRolePolicy",
"iam:CreateInstanceProfile",
"iam:DeleteRolePolicy",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam:DeleteInstanceProfile",
"ec2:ModifyVolumeAttribute",
"sts:DecodeAuthorizationMessage",
"ec2:DescribeImages",
"ec2:DescribeRouteTables",
"ec2:DescribeInstances",
"iam:PassRole",
"ec2:DescribeInstanceStatus",
"ec2:RunInstances",
"ec2:ModifyInstanceAttribute",
"ec2:CreateTags",
"ec2:CreateVolume",
"ec2:DescribeVolumes",
"ec2>DeleteVolume",
"ec2:CreateSecurityGroup",
"ec2>DeleteSecurityGroup",
"ec2:DescribeSecurityGroups",
"ec2:RevokeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:RevokeSecurityGroupIngress",
"ec2:CreateNetworkInterface",
"ec2:DescribeNetworkInterfaces",
"ec2>DeleteNetworkInterface",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeDhcpOptions",
"ec2:CreateSnapshot",
"ec2>DeleteSnapshot",
"ec2:DescribeSnapshots",
"ec2:StopInstances",
"ec2:GetConsoleOutput",
"ec2:DescribeKeyPairs",
"ec2:DescribeRegions",
"ec2>DeleteTags",
"ec2:DescribeTags",
"cloudformation:CreateStack",
```

```

        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:CreateBucket",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "kms:List*",
        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],

```

```

        "Resource": [
            "arn:aws-us-gov:s3:::fabric-pool*"
        ]
    },
    {
        "Sid": "backupPolicy",
        "Effect": "Allow",
        "Action": [
            "s3:DeleteBucket",
            "s3:GetLifecycleConfiguration",
            "s3:PutLifecycleConfiguration",
            "s3:PutBucketTagging",
            "s3:ListBucketVersions",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:ListAllMyBuckets",
            "s3:GetBucketTagging",
            "s3:GetBucketLocation",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketAcl",
            "s3:GetBucketPolicy",
            "s3:PutBucketPublicAccessBlock"
        ],
        "Resource": [
            "arn:aws-us-gov:s3:::netapp-backup-*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:StartInstances",
            "ec2:TerminateInstances",
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Resource": [
            "arn:aws-us-gov:ec2:*:*:instance/*"
        ]
    },
    {

```

```

        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-us-gov:ec2:*:*:volume/*"
        ]
    }
]
}

```

## C2S 환경

```

{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceStatus",
            "ec2:RunInstances",
            "ec2:ModifyInstanceAttribute",
            "ec2:DescribeRouteTables",
            "ec2:DescribeImages",
            "ec2:CreateTags",
            "ec2:CreateVolume",
            "ec2:DescribeVolumes",
            "ec2:ModifyVolumeAttribute",
            "ec2>DeleteVolume",
            "ec2:CreateSecurityGroup",
            "ec2>DeleteSecurityGroup",
            "ec2:DescribeSecurityGroups",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupIngress",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:CreateNetworkInterface",
            "ec2:DescribeNetworkInterfaces",
            "ec2>DeleteNetworkInterface",
            "ec2:ModifyNetworkInterfaceAttribute",
            "ec2:DescribeSubnets",
            "ec2:DescribeVpcs",
            "ec2:DescribeDhcpOptions",
            "ec2:CreateSnapshot",
            "ec2>DeleteSnapshot",

```

```

        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2>DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "iam:PassRole",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam>DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup",
        "iam:ListInstanceProfiles"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3>DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ]
}

```

```

    ],
    "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [
        "arn:aws-iso:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-iso:ec2:*:*:volume/*"
    ]
}
]
}

```

## AWS 사용 권한

다음 섹션에서는 각 NetApp 클라우드 서비스에 대한 사용 권한을 어떻게 사용하는지 설명합니다. 이 정보는 기업 정책에 따라 사용 권한이 필요한 경우에만 제공된다는 내용이 지정되어 있는 경우에 유용합니다.

### AppTemplate 태그

Connector는 AppTemplate Tagging 서비스를 사용할 때 AWS 리소스의 태그 관리를 위해 다음과 같은 API 요청을 수행합니다.



- EC2: CreateTags(태그 생성)
- EC2: 삭제 태그
- EC2: DescribeTags(설명 태그)
- 태그: getResources
- 태그: getTagKeys
- 태그: getTagValues
- 태그: 태그 리소스
- 태그: UntagResources

## 클라우드 백업

Connector는 다음과 같은 API 요청을 통해 Cloud Backup의 복원 인스턴스를 구축합니다.

- EC2: StartInstances(시작 인스턴스)
- EC2: StopInstances(중지 인스턴스)
- EC2: DescribeInstances(지시 인스턴스)
- EC2: DescribeInstanceStatus
- EC2: 런인스턴스
- EC2: 터미네이스
- EC2: DescribeInstanceAttribute
- EC2: DescribeImages(설명 영상)
- EC2: CreateTags(태그 생성)
- EC2: CreateVolume
- EC2:CreateSecurityGroup입니다
- EC2: DescribeSubnet
- EC2: 설명
- EC2: 설명
- CloudFormation:CreateStack
- CloudFormation:DeleteStack
- CloudFormation: DescribeStacks

Connector는 Amazon S3에서 백업을 관리하기 위해 다음과 같은 API 요청을 수행합니다.

- S3:GetBucketLocation
- S3:ListAllMyBucket
- S3:목록 버킷
- S3:생성 버킷
- S3:GetLifecycleConfiguration

- S3: PutLifecycleConfiguration
- S3: PutBucketTagging
- S3:목록 BucketVersions
- S3:GetBucketAcl
- S3: PutBucketPublicAccessBlock
- KMS: 목록 \*
- KMS: 설명 \*
- S3:GetObject
- EC2: describeVpcEndpoints입니다
- KMS: ListAliases
- S3:PutEncryptionConfiguration

Connector는 검색 및 복원 방법을 사용하여 볼륨 및 파일을 복원할 때 다음과 같은 API 요청을 수행합니다.

- S3:생성 버킷
- S3:DeleteObject 를 선택합니다
- S3:DeleteObjectVersion
- S3:GetBucketAcl
- S3:목록 버킷
- S3:목록 BucketVersions
- S3:ListBucketMultipartUploads
- S3:PutObject
- S3: PutBucketAcl
- S3: PutLifecycleConfiguration
- S3: PutBucketPublicAccessBlock
- S3:중단멀티업로드입니다
- S3:ListMultipartUploadParts(S3:ListMultipartUploadParts) 를
- Athena:StartQueryExecution
- Athena:GetQueryResults
- Athena:GetQueryExecution을 참조하십시오
- Athena: StopQueryExecution
- 글루:CreateDatabase
- 글루:CreateTable
- GLUE:BatchDeletePartition

## 클라우드 데이터 감지

Connector는 Cloud Data Sense 인스턴스를 구축하기 위해 다음과 같은 API 요청을 수행합니다.

- EC2: DescribeInstances(지시 인스턴스)
- EC2: DescribeInstanceStatus
- EC2: 런인스턴스
- EC2: 터미네이스
- EC2: CreateTags(태그 생성)
- EC2: CreateVolume
- EC2: AttachVolume
- EC2:CreateSecurityGroup입니다
- EC2: DeleteSecurityGroup
- EC2: DescribeSecurityGroups
- EC2: CreateNetworkInterface입니다
- EC2: DescribeNetworkInterfaces를 참조하십시오
- EC2: DeleteNetworkInterface
- EC2: DescribeSubnet
- EC2: 설명
- EC2: 스냅샷을 만듭니다
- EC2: 설명
- CloudFormation:CreateStack
- CloudFormation:DeleteStack
- CloudFormation: DescribeStacks
- CloudFormation: DescribeStackEvents
- IAM:AddRoleToInstanceProfile 을 참조하십시오
- EC2: AssociateIamInstanceProfile 을 참조하십시오
- EC2: DescribeIamInstanceProfileAssociations

Connector는 Cloud Data Sense를 사용할 때 S3 버킷을 스캔하기 위해 다음과 같은 API 요청을 수행합니다.

- IAM:AddRoleToInstanceProfile 을 참조하십시오
- EC2: AssociateIamInstanceProfile 을 참조하십시오
- EC2: DescribeIamInstanceProfileAssociations
- S3:GetBucketTagging
- S3:GetBucketLocation
- S3:ListAllMyBucket
- S3:목록 버킷
- S3:GetBucketPolicyStatus를 참조하십시오
- S3:GetBucketPolicy를 참조하십시오
- S3:GetBucketAcl

- S3:GetObject
- IAM:GetRole
- S3:DeleteObject 를 선택합니다
- S3:DeleteObjectVersion
- S3:PutObject
- STS:AssumeRole

## 클라우드 계층화

Connector는 Cloud Tiering을 사용할 때 Amazon S3에 데이터를 계층화하도록 다음과 같은 API 요청을 수행합니다.

| 조치                            | 설정에 사용됩니까? | 일상적 운영에 사용됩니까? |
|-------------------------------|------------|----------------|
| S3:생성 버킷                      | 예          | 아니요            |
| S3: PutLifecycleConfiguration | 예          | 아니요            |
| S3:GetLifecycleConfiguration  | 예          | 예              |
| EC2: 설명                       | 예          | 예              |

## Cloud Volumes ONTAP

Connector는 AWS에서 Cloud Volumes ONTAP를 구축 및 관리하기 위해 다음과 같은 API 요청을 수행합니다.

| 목적   | 조치  | 배포에<br>사용되었습니까? | 일상적 운영에<br>사용됩니까? | 삭제에<br>사용되었습니까? |
|--|---|-----------------|-------------------|-----------------|
| Cloud Volumes<br>ONTAP 인스턴스에<br>대한 IAM 역할 및<br>인스턴스 프로필을<br>생성하고 관리합니다 | IAM:<br>ListInstanceProfiles(<br>인스턴스 프로필)              | 예               | 예                 | 아니요             |
|  | IAM: CreateRole   | 예               | 아니요               | 아니요             |
|  | IAM: DeleteRole   | 아니요             | 예                 | 예               |
|  | IAM:<br>PutRolePolicy(입수<br>정책)                         | 예               | 아니요               | 아니요             |
|  | IAM:CreateInstance<br>Profile                           | 예               | 아니요               | 아니요             |
|  | IAM:<br>DeleteRolePolicy(삭<br>제 RolePolicy              | 아니요             | 예                 | 예               |
|  | IAM:AddRoleToInsta<br>nceProfile 을<br>참조하십시오            | 예               | 아니요               | 아니요             |
|  | IAM:RemoveRoleFro<br>mInstanceProfile 을<br>참조하십시오       | 아니요             | 예                 | 예               |
|  | IAM:<br>DeleteInstanceProfil<br>e                       | 아니요             | 예                 | 예               |
|  | IAM: 암호 역할  | 예               | 아니요               | 아니요             |
|  | EC2:<br>AssociateIamInstanc<br>eProfile 을<br>참조하십시오     | 예               | 예                 | 아니요             |
|  | EC2:<br>DescribeIamInstanc<br>eProfileAssociations      | 예               | 예                 | 아니요             |
|  | EC2:<br>DiscassociateIamIns<br>tanceProfile 을<br>참조하십시오 | 아니요             | 예                 | 아니요             |
| 인증 상태 메시지를<br>디코딩합니다   | STS:DecodeAuthoriz<br>ationMessage 를<br>참조하십시오          | 예               | 예                 | 아니요             |
| 계정에 사용할 수 있는<br>지정된 영상(AMI)을<br>설명합니다                                  | EC2:<br>DescribeImages(설<br>명 영상)                       | 예               | 예                 | 아니요             |
| VPC의 라우트 테이블<br>설명(HA 쌍에만 필요)  | EC2: 설명표  | 예               | 아니요               | 아니요             |

| 목적   | 조치                              | 배포에 사용되었습니까? | 일상적 운영에 사용됩니까? | 삭제에 사용되었습니까? |
|--|---------------------------------|--------------|----------------|--------------|
| 인스턴스를 중지, 시작 및 모니터링합니다   | EC2: StartInstances(시작 인스턴스)    | 예            | 예              | 아니요          |
|  | EC2: StopInstances(중지 인스턴스)     | 예            | 예              | 아니요          |
|  | EC2: DescribeInstances(지시 인스턴스) | 예            | 예              | 아니요          |
|  | EC2: DescribeInstanceStatus     | 예            | 예              | 아니요          |
|  | EC2: 런인스턴스                      | 예            | 아니요            | 아니요          |
|  | EC2: 터미네이션                      | 아니요          | 아니요            | 예            |
|  | EC2: ModifyInstanceAttribute    | 아니요          | 예              | 아니요          |
| 지원되는 인스턴스 유형에 대해 향상된 네트워킹이 활성화되어 있는지 확인합니다   | EC2: DescribeInstanceAttribute  | 아니요          | 예              | 아니요          |
| 유지 관리 및 비용 할당에 사용되는 "WorkingEnvironment" 및 "WorkingEnvironmentId" 태그로 리소스에 태그를 지정합니다 | EC2: CreateTags(태그 생성)          | 예            | 예              | 아니요          |
| Cloud Volumes ONTAP가 백엔드 스토리지로 사용하는 EBS 볼륨을 관리합니다                                    | EC2: CreateVolume               | 예            | 예              | 아니요          |
|  | EC2: 설명 볼륨을 참조하십시오              | 예            | 예              | 예            |
|  | EC2: ModifyVolumeAttribute      | 아니요          | 예              | 예            |
|  | EC2: AttachVolume               | 예            | 예              | 아니요          |
|  | EC2: DeleteVolume(삭제 볼륨)        | 아니요          | 예              | 예            |
|  | EC2: DetachVolume(분리 볼륨)        | 아니요          | 예              | 예            |

| 목적   | 조치  | 배포에<br>사용되었습니까? | 일상적 운영에<br>사용됩니까? | 삭제에<br>사용되었습니까? |
|--|---|-----------------|-------------------|-----------------|
| Cloud Volumes<br>ONTAP에 대한 보안<br>그룹을 만들고<br>관리합니다                      | EC2:CreateSecurity<br>Group입니다                    | 예               | 아니요               | 아니요             |
|  | EC2:<br>DeleteSecurityGroup                       | 아니요             | 예                 | 예               |
|  | EC2:<br>DescribeSecurityGroups                    | 예               | 예                 | 예               |
|  | EC2:<br>RevokeSecurityGroupEgress                 | 예               | 아니요               | 아니요             |
|  | EC2:<br>AuthorizeSecurityGroupEgress 를<br>참조하십시오  | 예               | 아니요               | 아니요             |
|  | EC2:<br>AuthorizeSecurityGroupIngress 를<br>참조하십시오 | 예               | 아니요               | 아니요             |
|  | EC2:<br>RevokeSecurityGroupIngress 를<br>참조하십시오    | 예               | 예                 | 아니요             |
| 대상 서브넷에서<br>Cloud Volumes<br>ONTAP에 대한<br>네트워크<br>인터페이스를<br>생성하고 관리합니다 | EC2:<br>CreateNetworkInterface입니다                 | 예               | 아니요               | 아니요             |
|  | EC2:<br>DescribeNetworkInterfaces를<br>참조하십시오      | 예               | 예                 | 아니요             |
|  | EC2:<br>DeleteNetworkInterface                    | 아니요             | 예                 | 예               |
|  | EC2:<br>ModifyNetworkInterfaceAttribute 입니다       | 아니요             | 예                 | 아니요             |
| 대상 서브넷 및 보안<br>그룹 목록을<br>가져옵니다   | EC2:<br>DescribeSubnet                            | 예               | 예                 | 아니요             |
|  | EC2: 설명   | 예               | 예                 | 아니요             |
| Cloud Volumes<br>ONTAP 인스턴스의<br>DNS 서버와 기본<br>도메인 이름을<br>가져옵니다         | EC2:<br>DescribeDhcpOptions                       | 예               | 아니요               | 아니요             |

| 목적   | 조치                                       | 배포에 사용되었습니까? | 일상적 운영에 사용됩니까? | 삭제에 사용되었습니까? |
|--|--|--------------|----------------|--------------|
| Cloud Volumes ONTAP용 EBS 볼륨의 스냅샷을 생성합니다            | EC2: 스냅샷을 만듭니다                           | 예            | 예              | 아니요          |
|  | EC2: DeleteSnapshot                      | 아니요          | 예              | 예            |
|  | EC2: 설명                                  | 아니요          | 예              | 아니요          |
| AutoSupport 메시지에 첨부된 Cloud Volumes ONTAP 콘솔을 캡처합니다 | EC2:GetConsoleOutput 을 참조하십시오            | 예            | 예              | 아니요          |
| 사용 가능한 키 쌍 목록을 가져옵니다                               | EC2: 설명                                  | 예            | 아니요            | 아니요          |
| 사용 가능한 AWS 지역 목록을 확인하십시오                           | EC2: 설명                                  | 예            | 예              | 아니요          |
| Cloud Volumes ONTAP 인스턴스와 연결된 리소스의 태그를 관리합니다       | EC2: 삭제 태그                               | 아니요          | 예              | 예            |
|  | EC2: DescribeTags(설명 태그)                 | 아니요          | 예              | 아니요          |
| AWS CloudFormation 템플릿을 위한 스택을 만들고 관리합니다           | CloudFormation:CreateStack               | 예            | 아니요            | 아니요          |
|  | CloudFormation:DeleteStack               | 예            | 아니요            | 아니요          |
|  | CloudFormation:DescribeStacks            | 예            | 예              | 아니요          |
|  | CloudFormation:DescribeStackEvents       | 예            | 아니요            | 아니요          |
|  | CloudFormation:ValidateTemplate 을 참조하십시오 | 예            | 아니요            | 아니요          |



| 목적   | 조치                                       | 배포에<br>사용되었습니까? | 일상적 운영에<br>사용됩니까? | 삭제에<br>사용되었습니까? |
|--|--|-----------------|-------------------|-----------------|
| Cloud Volumes<br>ONTAP 시스템이<br>데이터 계층화를 위한<br>용량 계층으로<br>사용하는 S3 버킷을<br>생성 및 관리합니다 | S3:생성 버킷                                 | 예               | 예                 | 아니요             |
|  | S3:삭제 버킷                                 | 아니요             | 예                 | 예               |
|  | S3:GetLifecycleConf<br>iguration         | 아니요             | 예                 | 아니요             |
|  | S3:<br>PutLifecycleConfigur<br>ation     | 아니요             | 예                 | 아니요             |
|  | S3:<br>PutBucketTagging                  | 아니요             | 예                 | 아니요             |
|  | S3:목록<br>BucketVersions                  | 아니요             | 예                 | 아니요             |
|  | S3:GetBuckketPolicy<br>Status를<br>참조하십시오 | 아니요             | 예                 | 아니요             |
|  | S3:GetBuckketPubli<br>cAccessBlock       | 아니요             | 예                 | 아니요             |
|  | S3:GetBuckketAcl                         | 아니요             | 예                 | 아니요             |
|  | S3:GetBuckketPolicy<br>를 참조하십시오          | 아니요             | 예                 | 아니요             |
|  | S3:<br>PutBucketPublicAcc<br>essBlock    | 아니요             | 예                 | 아니요             |
|  | S3:GetBucketTaggin<br>g                  | 아니요             | 예                 | 아니요             |
|  | S3:GetBucketLocati<br>on                 | 아니요             | 예                 | 아니요             |
|  | S3:ListAllMyBucket                       | 아니요             | 아니요               | 아니요             |
|  | S3:목록 버킷                                 | 아니요             | 예                 | 아니요             |
| AWS KMS(키 관리<br>서비스)를 사용하여<br>Cloud Volumes<br>ONTAP의 데이터<br>암호화 지원                | KMS: 목록 *                                | 예               | 예                 | 아니요             |
|  | KMS: 재암호화 *                              | 예               | 아니요               | 아니요             |
|  | KMS: 설명 *                                | 예               | 예                 | 아니요             |
|  | KMS: CreateGrant                         | 예               | 예                 | 아니요             |

| 목적   | 조치                                   | 배포에 사용되었습니까? | 일상적 운영에 사용됩니까? | 삭제에 사용되었습니까? |
|--|--------------------------------------|--------------|----------------|--------------|
| Cloud Volumes ONTAP의 AWS 비용 데이터 확보                                     | CE:GetReservationUtilization을 참조하십시오 | 아니요          | 예              | 아니요          |
|  | CE:GetDimensionValues                | 아니요          | 예              | 아니요          |
|  | CE:GetCostAndUsage                   | 아니요          | 예              | 아니요          |
|  | CE:GetTags                           | 아니요          | 예              | 아니요          |
| 단일 AWS Availability Zone에서 2개의 HA 노드를 위한 AWS 분산 배치 그룹과 종재자를 생성하고 관리합니다 | EC2: CreatePlacementGroup(배치 그룹 생성)  | 예            | 아니요            | 아니요          |
|  | EC2: DeletePlacementGroup            | 아니요          | 예              | 예            |
| 보고서 작성   | FSX: 설명 *                            | 아니요          | 예              | 아니요          |
|  | FSX: 목록 *                            | 아니요          | 예              | 아니요          |
| Amazon EBS Elastic Volumes 기능을 지원하는 애그리게이트를 생성 및 관리합니다                 | EC2: 볼륨 수정 설명                        | 아니요          | 예              | 아니요          |
|  | EC2: ModifyVolume(수정 볼륨)             | 아니요          | 예              | 아니요          |

## 글로벌 파일 캐시

Connector는 배포 중에 다음과 같은 API 요청을 통해 글로벌 파일 캐시 인스턴스를 구축합니다.

- CloudFormation: DescribeStacks
- CloudWatch: GetMetricStatistics
- CloudFormation: ListStacks

## 쿠버네티스

Connector는 다음과 같은 API 요청을 수행하여 Amazon EKS 클러스터를 검색하고 관리합니다.

- EC2: 설명
- EKS: ListClusters
- EKS: DescribeCluster
- IAM:GetInstanceProfile 을 참조하십시오

# Connector에 대한 Azure 권한

Cloud Manager가 Azure에서 Connector VM을 시작하면 해당 Azure 구독 내에서 리소스와

프로세스를 관리할 수 있는 권한을 Connector에 제공하는 VM에 사용자 지정 역할을 연결합니다. Connector는 사용 권한을 사용하여 여러 Azure 서비스에 대한 API 호출을 수행합니다.

## 사용자 지정 역할 권한

아래 표시된 사용자 지정 역할은 Connector가 Azure 네트워크 내의 리소스 및 프로세스를 관리하는 데 필요한 권한을 제공합니다.

Cloud Manager에서 직접 Connector를 만들면 Cloud Manager가 자동으로 이 사용자 지정 역할을 Connector에 적용합니다.

Azure Marketplace에서 Connector를 배포하거나 Linux 호스트에 Connector를 수동으로 설치하는 경우 사용자 지정 역할을 직접 설정해야 합니다.

또한 후속 릴리스에 새 권한이 추가되므로 역할이 최신 상태인지 확인해야 합니다.

```
{
  "Name": "Cloud Manager Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",

    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",

    "Microsoft.Compute/virtualMachines/instanceView/read",

    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Compute/virtualMachines/read",

    "Microsoft.Compute/virtualMachines/restart/action",

    "Microsoft.Compute/virtualMachines/deallocate/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/images/write",
    "Microsoft.Compute/images/read",

    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
```

```
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/resources/read",

"Microsoft.Resources/subscriptions/operationresults/read",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/operations/read",

"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/regeneratekey/action",
"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/usages/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/availabilitySets/write",
"Microsoft.Compute/availabilitySets/read",
```

```

        "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",

        "Microsoft.Network/loadBalancers/read",
        "Microsoft.Network/loadBalancers/write",
        "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
        "Microsoft.Network/loadBalancers/probes/read",

"Microsoft.Network/loadBalancers/probes/join/action",
        "Microsoft.Authorization/locks/*",
        "Microsoft.Network/routeTables/join/action",
        "Microsoft.NetApp/netAppAccounts/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
        "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action",

"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
        "Microsoft.Network/privateEndpoints/read",
        "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",

```

```

        "Microsoft.Network/virtualNetworks/join/action",
        "Microsoft.Network/privateDnsZones/A/write",
        "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Insights/Metrics/Read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Compute/virtualMachines/extensions/delete",

"Microsoft.Compute/virtualMachines/extensions/read",
        "Microsoft.Compute/virtualMachines/delete",
        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Resources/deployments/delete",
        "Microsoft.Compute/diskEncryptionSets/read",
        "Microsoft.Compute/snapshots/delete",
        "Microsoft.Network/privateEndpoints/delete",
        "Microsoft.Compute/availabilitySets/delete",
        "Microsoft.Network/loadBalancers/delete",
        "Microsoft.KeyVault/vaults/read",
        "Microsoft.KeyVault/vaults/accessPolicies/write",
        "Microsoft.Compute/diskEncryptionSets/write",
        "Microsoft.KeyVault/vaults/deploy/action",
        "Microsoft.Compute/diskEncryptionSets/delete",
        "Microsoft.Resources/tags/read",
        "Microsoft.Resources/tags/write",
        "Microsoft.Resources/tags/delete",

"Microsoft.Network/applicationSecurityGroups/write",

"Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",

"Microsoft.Network/applicationSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete"
    ],
    "NotActions": [],
    "AssignableScopes": [],

```

```

    "Description": "Cloud Manager Permissions",
    "IsCustom": "true"
  }

```

## Azure 사용 권한 사용 방법

| 작업  | 목적   |
|---|--|
| "Microsoft.Compute/locations/operations/read",<br>"Microsoft.Compute/locations/vmSizes/read",<br>"Microsoft.Compute/operations/read",<br>"Microsoft.Compute/virtualMachines/instanceView/read",<br>"Microsoft.Compute/virtualMachines/powerOff/action",<br>"Microsoft.Compute/virtualMachines/read",<br>"Microsoft.Compute/virtualMachines/restart/action",<br>"Microsoft.Compute/virtualMachines/start/action",<br>"Microsoft.Compute/virtualMachines/deallocate/action",<br>"Microsoft.Compute/virtualMachines/vmSizes/read",<br>"Microsoft.Compute/virtualMachines/write", | Cloud Volumes ONTAP를 생성하고 시스템 상태를 중지, 시작, 삭제 및 가져옵니다.      |
| "Microsoft.Compute/images/write",<br>"Microsoft.Compute/images/read",   | VHD에서 Cloud Volumes ONTAP 배포를 활성화합니다.                      |
| "Microsoft.Compute/disks/delete",<br>"Microsoft.Compute/disks/read",<br>"Microsoft.Compute/disks/write",<br>"Microsoft.Storage/checknameAvailability/read",<br>"Microsoft.Storage/operations/read",<br>"Microsoft.Storage/storageAccounts/listkeys/action",<br>"Microsoft.Storage/storageAccounts/read",<br>"Microsoft.Storage/storageAccounts/REV/ACTION",<br>"Microsoft.Storage/storageAccounts/write",<br>"Microsoft.Storage/storageAccounts/delete",<br>"Microsoft.Storage/en사용법/read",   | Azure 스토리지 계정 및 디스크를 관리하고 디스크를 Cloud Volumes ONTAP에 연결합니다. |
| "Microsoft.Storage/storageAccounts/blobServices/containers/read",<br>"Microsoft.KeyVault/vaults/read",<br>"Microsoft.KeyVault/vaults/accessPolicies/write"  | Azure Blob 저장소에 백업 및 스토리지 계정 암호화를 지원합니다.                   |
| "Microsoft.Network/networkInterfaces/read",<br>"Microsoft.Network/networkInterfaces/write",<br>"Microsoft.Network/networkInterfaces/join/action",   | 대상 서버넷에서 Cloud Volumes ONTAP에 대한 네트워크 인터페이스를 생성하고 관리합니다.   |
| "Microsoft.Network/networkSecurityGroups/read",<br>"Microsoft.Network/networkSecurityGroups/write",<br>"Microsoft.Network/networkSecurityGroups/join/action",   | Cloud Volumes ONTAP에 대해 미리 정의된 네트워크 보안 그룹을 생성합니다.          |

| 작업  | 목적   |
|---|--|
| "Microsoft.Resources/Subscriptions/locations/read",<br>"Microsoft.Network/locations/operationResults/read",<br>"Microsoft.Network/locations/operations/read",<br>"Microsoft.Network/virtualNetworks/read",<br>"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",<br>"Microsoft.Network/virtualNetworks/subnets/read",<br>"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",<br>"Microsoft.Network/virtualNetworks/virtualMachines/read",<br>"Microsoft.Network/virtualNetworks/subnets/join/action", | 지역, 대상 VNET 및 서브넷에 대한 네트워크 정보를 가져오고 Cloud Volumes ONTAP를 VNets에 추가합니다. |
| "Microsoft.Network/virtualNetworks/subnets/write",<br>"Microsoft.Network/routeTables/join/action",  | 데이터 계층화를 위한 VNET 서비스 엔드포인트를 활성화합니다.                                    |
| "Microsoft.Resources/Deployments/operations/read",<br>"Microsoft.Resources/Deployments/read",<br>"Microsoft.Resources/Deployments/Write",   | 템플릿에서 Cloud Volumes ONTAP를 배포합니다.                                      |
| "Microsoft.Resources/Deployments/operations/read",<br>"Microsoft.Resources/Deployments/read",<br>"Microsoft.Resources/Deployments/write",<br>"Microsoft.Resources/resources/read",<br>"Microsoft.Resources/Subscriptions/operationresults/read",<br>"Microsoft.Resources/Subscriptions/resourceGroups/delete",<br>"Microsoft.Resources/Subscriptions/resourceGroups/read",<br>"Microsoft.Resources/Subscriptions/resourceGroups/resourceGroups/read",<br>"Microsoft.Resources/Subscriptions/resourceGroups/write",                    | Cloud Volumes ONTAP에 대한 리소스 그룹을 생성하고 관리합니다.                            |
| "Microsoft.Compute/snapshots/write",<br>"Microsoft.Compute/snapshots/read",<br>"Microsoft.Compute/snapshots/delete",<br>"Microsoft.Compute/disks/beginGetAccess/action",  | Azure 관리 스냅샷을 생성하고 관리합니다.  |
| "Microsoft.Compute/availabilitySets/write",<br>"Microsoft.Compute/availabilitySets/read",   | Cloud Volumes ONTAP의 가용성 세트를 생성하고 관리합니다.                               |
| "Microsoft.MarketplaceOrdering/offerstypes/publishers/Offers/Plans/Agreement/read",<br>"Microsoft.MarketplaceOrdering/offerstypes/publisherTypes/publishers/Offers/Plans/Agreement/write",  | Azure Marketplace에서 프로그래밍 방식으로 배포할 수 있습니다.                             |



| 작업  | 목적  |
|---|---|
| "Microsoft.Network/loadBalancers/read",<br>"Microsoft.Network/loadBalancers/write",<br>"Microsoft.Network/loadBalancers/delete",<br>"Microsoft.Network/loadBalancers/backendAddressPools/read",<br>"Microsoft.Network/loadBalancers/backendAddressPools/join/action",<br>"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",<br>"Microsoft.Network/loadBalancers/loadBalancingRules/read",<br>"Microsoft.Network/loadBalancers/probes/read",<br>"Microsoft.Network/loadBalancers/probes/join/action",  | HA 쌍에 대한 Azure 로드 밸런서를 관리합니다.   |
| "Microsoft.Authorization/lock/ **",   | Azure 디스크의 잠금 관리를 활성화합니다.   |
| "Microsoft.Authorization/roleDefinitions/write",<br>"Microsoft.Authorization/roleAssignments/write",<br>"Microsoft.Web/sites/ **"   | HA 쌍의 페일오버 관리   |
| "Microsoft.Network/privateEndpoints/write",<br>"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action",<br>"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",<br>"Microsoft.Network/privateEndpoints/read",<br>"Microsoft.Network/privateDnsZones/write",<br>"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",<br>"Microsoft.Network/virtualNetworks/join/action",<br>"Microsoft.Network/privateDnsZones/A/write",<br>"Microsoft.Network/privateDnsZones/read",<br>"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read", | 전용 엔드포인트를 관리할 수 있습니다. 전용 엔드포인트는 서브넷 외부에 접속이 제공되지 않을 때 사용됩니다. Cloud Manager는 서브넷 내에서 내부 연결만 제공하는 HA용 스토리지 계정을 생성합니다. |
| "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",   | Cloud Manager에서 Azure NetApp Files의 볼륨을 삭제할 수 있습니다.   |
| "Microsoft.Resources/Deployments/operationStates/read"  | Azure에서는 일부 가상 시스템 배포에 대해 이 권한이 필요합니다(배포 중에 사용되는 기본 물리적 하드웨어에 따라 다름).   |
| "Microsoft.Resources/Deployments/operationStates/read",<br>"Microsoft.Insights/Metrics/Read",<br>"Microsoft.Compute/virtualMachines/extensions/write",<br>"Microsoft.Compute/virtualMachines/extensions/read",<br>"Microsoft.Compute/virtualMachines/extensions/delete",<br>"Microsoft.Compute/virtualMachines/delete",<br>"Microsoft.Network/networkInterfaces/delete",<br>"Microsoft.Network/networkSecurityGroups/delete",<br>"Microsoft.Resources/Deployments/delete",  | 글로벌 파일 캐시를 사용할 수 있습니다.  |
| "Microsoft.Network/privateEndpoints/delete",<br>"Microsoft.Compute/availabilitySets/delete",  | Cloud Manager에서 배포 실패 또는 삭제 시 Cloud Volumes ONTAP에 속한 리소스 그룹에서 리소스를 제거할 수 있습니다.                                     |

| 작업  | 목적  |
|---|---|
| "Microsoft.Compute/diskEncryptionSets/read"<br>"Microsoft.Compute/diskEncryptionSets/write",<br>"Microsoft.Compute/diskEncryptionSets/delete"<br>"Microsoft.KeyVault/vaults/deploy/action",<br>"Microsoft.KeyVault/vaults/waults/read",<br>"Microsoft.KeyVault/vaults/accessPolicies/write",  | Cloud Volumes ONTAP에서 고객이 관리하는 암호화 키를 사용할 수 있습니다. 이 기능은 API를 사용하여 지원됩니다.          |
| "Microsoft.Resources/tags/read",<br>"Microsoft.Resources/tags/write",<br>"Microsoft.Resources/tags/delete"  | Cloud Manager 태그 지정 서비스를 사용하여 Azure 리소스의 태그를 관리할 수 있습니다.                          |
| "Microsoft.Network/applicationSecurityGroups/write",<br>"Microsoft.Network/applicationSecurityGroups/read",<br>"Microsoft.Network/applicationSecurityGroups/joinIpC onfiguration/action",<br>"Microsoft.Network/networkSecurityGroups/securityRu les/write", "Microsoft.Network/applicationSecurityGrou ps/delete",<br>"Microsoft.Network/networkSecurityGroups/securityRu les/delete" 참조하십시오 | Cloud Manager에서 HA 인터커넥트 및 클러스터 네트워크 NIC를 격리하는 HA 쌍에 대한 애플리케이션 보안 그룹을 구성할 수 있습니다. |

## Connector에 대한 Google Cloud 권한

Cloud Manager를 사용하려면 Google Cloud에서 작업을 수행할 수 있는 권한이 필요합니다. 이러한 사용 권한은 NetApp에서 제공하는 사용자 지정 역할에 포함됩니다. Cloud Manager가 이러한 사용 권한을 통해 수행하는 작업을 이해하기를 원할 수 있습니다.

### 서비스 계정 권한

아래 표시된 사용자 지정 역할은 Connector가 Google Cloud 네트워크 내의 리소스 및 프로세스를 관리하는 데 필요한 권한을 제공합니다.

Connector VM에 연결되는 서비스 계정에 이 사용자 지정 역할을 적용해야 합니다. ["단계별 지침을 봅니다"](#).

또한 후속 릴리스에 새 권한이 추가되므로 역할이 최신 상태인지 확인해야 합니다.

```

title: NetApp Cloud Manager
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list

```

- `compute.disks.create`
- `compute.disks.createSnapshot`
- `compute.disks.delete`
- `compute.disks.get`
- `compute.disks.list`
- `compute.disks.setLabels`
- `compute.disks.use`
- `compute.firewalls.create`
- `compute.firewalls.delete`
- `compute.firewalls.get`
- `compute.firewalls.list`
- `compute.globalOperations.get`
- `compute.images.get`
- `compute.images.getFromFamily`
- `compute.images.list`
- `compute.images.useReadOnly`
- `compute.instances.addAccessConfig`
- `compute.instances.attachDisk`
- `compute.instances.create`
- `compute.instances.delete`
- `compute.instances.detachDisk`
- `compute.instances.get`
- `compute.instances.getSerialPortOutput`
- `compute.instances.list`
- `compute.instances.setDeletionProtection`
- `compute.instances.setLabels`
- `compute.instances.setMachineType`
- `compute.instances.setMetadata`
- `compute.instances.setTags`
- `compute.instances.start`
- `compute.instances.stop`
- `compute.instances.updateDisplayDevice`
- `compute.machineTypes.get`
- `compute.networks.get`
- `compute.networks.list`
- `compute.projects.get`
- `compute.regions.get`
- `compute.regions.list`
- `compute.snapshots.create`
- `compute.snapshots.delete`
- `compute.snapshots.get`
- `compute.snapshots.list`
- `compute.snapshots.setLabels`
- `compute.subnetworks.get`
- `compute.subnetworks.list`
- `compute.subnetworks.use`

- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list

## Google Cloud 사용 권한 사용 방법

| 작업  | 목적                                    |
|---|---------------------------------------|
| -compute.disks.create-compute.disks.createSnapshot<br>-compute.disks.delete -compute.disks.get<br>-compute.disks.list -compute.disks.setLabels<br>-compute.disks.us e | Cloud Volumes ONTAP용 디스크를 생성하고 관리합니다. |

| 작업  | 목적  |
|---|---|
| -compute.w방화벽.create-compute.firewalls.delete-compute.w방화벽.get-compute.w방화벽.list를 참조하십시오  | Cloud Volumes ONTAP에 대한 방화벽 규칙을 만듭니다.                           |
| -compute.globalOperations.get   | 작업 상태를 확인합니다.   |
| -compute.images.get-compute.images.getFromFamily<br>-compute.images.list-compute.images.useReadOnly를 참조하십시오   | VM 인스턴스의 이미지를 가져옵니다.  |
| compute.instances.attachDisk -<br>compute.instances.detachDisk 으로 문의하십시오  | Cloud Volumes ONTAP에 디스크를 연결 및 분리합니다.                           |
| compute.instances.create - compute.instances.delete<br>으로 문의하십시오  | Cloud Volumes ONTAP VM 인스턴스를 생성 및 삭제합니다.                        |
| compute.instances.get 으로 문의하십시오   | VM 인스턴스를 나열합니다.   |
| compute.instances.getSerialPortOutput 으로<br>문의하십시오  | 콘솔 로그를 가져옵니다.   |
| compute.instances.list 으로 문의하십시오  | 영역에 있는 인스턴스 목록을 검색합니다.  |
| compute.instances.setDeletionProtection 으로<br>문의하십시오  | 인스턴스에 대한 삭제 보호를 설정합니다.  |
| compute.instances.setLabels 으로 문의하십시오   | 를 눌러 라벨을 추가합니다.   |
| compute.instances.setMachineType -<br>compute.instances.setMinCpuPlatform 으로<br>문의하십시오  | Cloud Volumes ONTAP의 기계 유형을 변경합니다.                              |
| compute.instances.setMetadata 으로 문의하십시오   | 를 눌러 메타데이터를 추가합니다.  |
| compute.instances.setTags 으로 문의하십시오   | 방화벽 규칙에 대한 태그를 추가하려면  |
| compute.instances.start - compute.instances.stop -<br>compute.instances.updateDisplayDevice   | Cloud Volumes ONTAP를 시작 및 중지합니다.                                |
| -compute.machineTypes.get   | 를 클릭하여 quotas를 확인하십시오.  |
| compute.projects.get 으로 문의하십시오  | 여러 프로젝트를 지원합니다.   |
| -compute.snapshots.create-compute.snapshots.delete<br>-compute.snapshots.get-compute.snapshots.list<br>-compute.snapshots.setLabels 를 참조하십시오  | 영구 디스크 스냅샷을 생성하고 관리합니다.   |
| -compute.networks.get -compute.networks.list<br>-compute.regions.get-compute.regions.list<br>-compute.subnetworks.get-compute.subnetworks.list<br>-compute.zoneOperations.get-compute.zones.get<br>-compute.zones.list 를 참조하십시오 | 새 Cloud Volumes ONTAP 가상 머신 인스턴스를<br>생성하는 데 필요한 네트워킹 정보를 가져옵니다. |

| 작업   | 목적  |
|--|---|
| deploymentmanager.compositeTypes.get<br>-deploymentmanager.compositeTypes.list<br>-deploymentmanager.deployments.create<br>-deploymentmanager.deployments.delete<br>-deploymentmanager.deployments.get<br>-deploymentmanager.deployments.list<br>deploymentmanager.manifests.get<br>deploymentmanager.manager.manifests.list.deploymentmanager.operations.get<br>deploymentmanager.resources.get<br>deploymentmanager.resources.list.list.deploymentmanager.deploymentmanager.deploymentmanager.deploymentmanager.type.deploymentmanager.deploymentmanager.deploymentmanager.type.get.type.get | Google Cloud Deployment Manager를 사용하여 Cloud Volumes ONTAP 가상 머신 인스턴스를 구축합니다.                      |
| logging.logEntrys.list-logging.privateLogEntrys.list 를 참조하십시오  | 스택 로그 드라이브를 가져옵니다.  |
| resourcemanager.projects.get 으로 문의하십시오   | 여러 프로젝트를 지원합니다.   |
| -storage.버킷.create-storage.buckets.delete-storage.버킷.get-storage.버킷.list-storage.버킷.update   | 데이터 계층화를 위한 Google Cloud Storage 버킷 생성 및 관리   |
| -cloudkms.cryptoKeyVersions.useToEncrypt<br>-cloudkms.cryptoKeys.get-cloudkms.cryptoKeys.list<br>-cloudkms.keyring.list를 참조하십시오  | 클라우드 키 관리 서비스(Cloud Volumes ONTAP 포함)에서 고객이 관리하는 암호화 키를 사용하려면                                     |
| -compute.instances.setServiceAccount<br>-iam.serviceAccounts.actAs<br>-iam.serviceAccounts.getIamPolicy<br>-iam.serviceAccounts.list -storage.objects.get<br>-storage.objects.list 를 참조하십시오  | Cloud Volumes ONTAP 인스턴스에서 서비스 계정을 설정하려면 이 서비스 계정은 Google Cloud Storage 버킷에 대한 데이터 계층화 권한을 제공합니다. |
| -compute.addresses.list<br>-compute.backendServices.create<br>-compute.networks.updatePolicy<br>-compute.regionBackendServices.create<br>-compute.regionBackendServices.get<br>-compute.regionBackendServices.list를 참조하십시오   | HA 쌍을 구축합니다.  |
| compute.subnetworks.useExternalIp -<br>compute.subnetworks.useExternalIp -<br>compute.instances.addAccessConfig 으로<br>문의하십시오   | 클라우드 데이터 센스를 활성화하려면   |
| -container.clusters.get-container.clusters.list 를<br>참조하십시오  | Google Kubernetes Engine에서 실행 중인 Kubernetes 클러스터를 검색할 수 있습니다.                                     |
| -compute.instanceGroups.get<br>-compute.addresses.get  | 를 사용하여 HA 쌍에서 스토리지 VM을 생성하고<br>관리합니다.   |

# 지식 및 지원

## 지원을 위해 등록하십시오

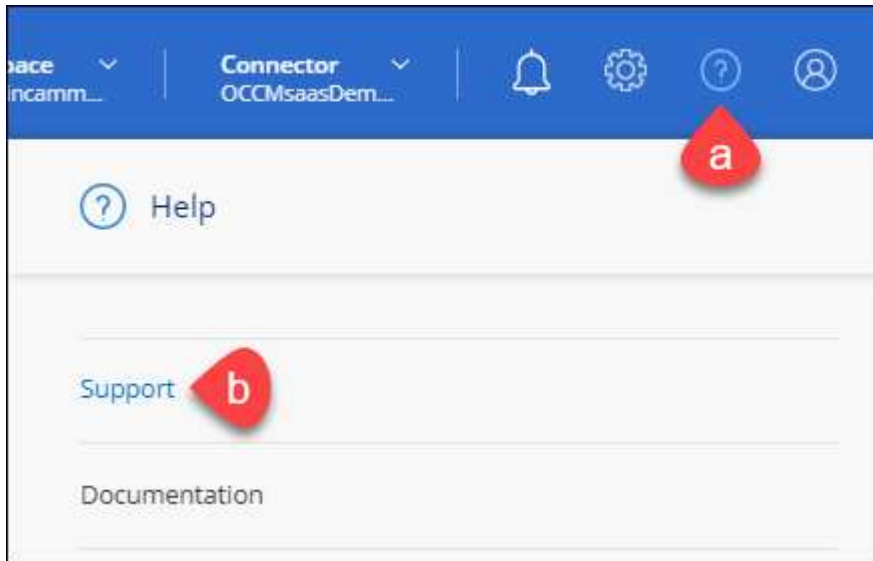
NetApp 기술 지원으로 지원 케이스를 생성하기 전에 NetApp Support 사이트 계정을 Cloud Manager에 추가한 다음 지원을 위해 등록해야 합니다.

### NSS 계정을 추가합니다

지원 대시보드를 이용하면 모든 NetApp Support 사이트 계정을 단일 위치에서 추가 및 관리할 수 있습니다.

단계

1. 아직 NetApp Support 사이트 계정이 없는 경우 **"1인 등록"**.
2. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 \* 지원 \* 을 선택합니다.



3. NSS 관리 > NSS 계정 추가 \* 를 클릭합니다.
4. 메시지가 표시되면 \* 계속 \* 을 클릭하여 Microsoft 로그인 페이지로 리디렉션됩니다.

NetApp은 Microsoft Azure Active Directory를 지원 및 라이선싱과 관련된 인증 서비스의 ID 공급자로 사용합니다.

5. 로그인 페이지에서 인증 프로세스를 수행할 수 있도록 NetApp Support 사이트의 등록 이메일 주소와 암호를 제공합니다.

이 작업을 수행하면 Cloud Manager에서 NSS 계정을 사용할 수 있습니다.

참고 계정은 고객 수준 계정이어야 합니다(게스트 또는 임시 계정이 아님).

### 계정을 등록하여 지원을 받을 수 있습니다

지원 등록은 지원 대시보드의 Cloud Manager에서 가능합니다.

단계

1. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 \* 지원 \* 을 선택합니다.



2. Resources \* 탭에서 \* Register for Support \* 를 클릭합니다.
3. 등록할 NSS 자격 증명을 선택한 다음 \* 등록 \* 을 클릭합니다.

## 도움을 받으십시오

NetApp은 다양한 방법으로 Cloud Manager 및 클라우드 서비스를 지원합니다. 기술 자료(KB) 기사 및 커뮤니티 포럼과 같은 광범위한 무료 셀프 지원 옵션이 24x7 제공됩니다. 지원 등록에는 웹 티켓팅을 통한 원격 기술 지원이 포함됩니다.

### 자체 지원

이 옵션은 하루 24시간, 주 7일 동안 무료로 사용할 수 있습니다.

- "기술 자료"

Cloud Manager 기술 자료를 검색하여 문제를 해결할 수 있는 유용한 문서를 찾습니다.

- "커뮤니티"

Cloud Manager 커뮤니티에 가입하여 진행 중인 토론을 팔로우하거나 새 토론을 만들어보십시오.

- 문서화

현재 보고 있는 Cloud Manager 문서입니다.

- <mailto:ng-cloudmanager-feedback@netapp.com> [피드백 이메일]

저희는 귀하의 의견을 소중하게 생각합니다. 클라우드 관리자 개선에 도움이 되는 피드백을 제출해 주십시오.



## NetApp 지원

위의 자체 지원 옵션 외에도 NetApp 지원 엔지니어와 협력하여 지원을 활성화한 이후의 모든 문제를 해결할 수 있습니다.

단계

1. Cloud Manager에서 \* 도움말 > 지원 \* 을 클릭합니다.
2. 기술 지원 아래에서 사용 가능한 옵션 중 하나를 선택합니다.
  - a. NetApp 기술 지원을 위한 전화 번호를 찾으려면 \* 문의하다
  - b. 문제 열기 \* 를 클릭하고 옵션 중 하나를 선택한 다음 \* 보내기 \* 를 클릭합니다.

NetApp 담당자가 귀하의 케이스를 검토하고 곧 다시 귀하에 연락을 드릴 것입니다.

# 법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

## 저작권

<http://www.netapp.com/us/legal/copyright.aspx>

## 상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## 특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

<https://www.netapp.com/us/media/patents-page.pdf>

## 개인 정보 보호 정책

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## 오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이선스에 대한 정보를 제공합니다.

- ["Cloud Manager 3.9에 대한 고지 사항"](#)

## 저작권 정보

Copyright © 2022 NetApp, Inc. All rights reserved. 미국에서 인쇄된 본 문서의 어떤 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 그래픽, 전자적 또는 기계적 수단(사진 복사, 레코딩 등)으로도 저작권 소유자의 사전 서면 승인 없이 전자 검색 시스템에 저장 또는 저장.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지 사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 "있는 그대로" 제공되며 상품성 및 특정 목적에 대한 적합성에 대한 명시적 또는 묵시적 보증을 포함하여 이에 제한되지 않고, 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 또는 파생적 손해(소계 물품 또는 서비스의 조달, 사용 손실, 데이터 또는 수익 손실, 계약, 엄격한 책임 또는 불법 행위(과실 또는 그렇지 않은 경우)에 관계없이 어떠한 책임도 지지 않으며, 이는 이러한 손해의 가능성을 사전에 알고 있던 경우에도 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 구입의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

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

권리 제한 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.277-7103(1988년 10월) 및 FAR 52-227-19(1987년 6월)의 기술 데이터 및 컴퓨터 소프트웨어의 권리(Rights in Technical Data and Computer Software) 조항의 하위 조항 (c)(1)(ii)에 설명된 제한사항이 적용됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 에 나열된 마크는 NetApp에 있습니다 <http://www.netapp.com/TM> 는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.