제한 모드 시작하기

NetApp Console setup and administration

NetApp
December 12, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/console-setup-admin/task-quick-start-restricted-mode.html on December 12, 2025. Always check docs.netapp.com for the latest.

목차

제한 모드 시작하기 1
- 시작하기 워크플로(제한 모드) 1
- 제한 모드에서 배포 준비 1
  - 1단계: 제한 모드 작동 방식 이해 1
  - 2단계: 설치 옵션 검토 2
  - 3단계: 호스트 요구 사항 검토 2
  - 4단계: Podman 또는 Docker Engine 설치 4
  - 5단계: 네트워크 액세스 준비 7
  - 6단계: 클라우드 권한 준비 11
  - 7단계: Google Cloud API 활성화 20
- 제한 모드로 콘솔 에이전트 배포 21
  - 1단계: 콘솔 에이전트 설치 21
  - 2단계: NetApp Console 설정 29
  - 3단계: 콘솔 에이전트에 권한 제공 29
- NetApp Intelligent Services 구독(제한 모드) 32
- 다음에 할 수 있는 일(제한 모드) 38

제한 모드 시작하기

시작하기 워크플로(제한 모드)

환경을 준비하고 콘솔 에이전트를 배포하여 제한 모드에서 NetApp Console 을 시작하세요.

제한 모드는 일반적으로 주 및 지방 정부와 규제 대상 기업에서 사용하며, 여기에는 AWS GovCloud 및 Azure Government 지역에 배포하는 것도 포함됩니다. 시작하기 전에 다음 사항을 이해했는지 확인하십시오."콘솔 에이전트" 그리고"배포 모드" .

1 "배치 준비"

1. CPU, RAM, 디스크 공간, 컨테이너 오케스트레이션 도구 등의 요구 사항을 충족하는 전용 Linux 호스트를 준비합니다.
2. 대상 네트워크에 대한 액세스, 수동 설치를 위한 아웃바운드 인터넷 액세스, 일상적인 액세스를 위한 아웃바운드 인터넷을 제공하는 네트워킹을 설정합니다.
3. 콘솔 에이전트 인스턴스를 배포한 후 해당 권한과 연결할 수 있도록 클라우드 공급자에서 권한을 설정합니다.

2 "콘솔 에이전트 배포"

1. 클라우드 공급업체의 마켓플레이스에서 콘솔 에이전트를 설치하거나, Linux 호스트에 소프트웨어를 수동으로 설치하세요.
2. 웹 브라우저를 열고 Linux 호스트의 IP 주소를 입력하여 NetApp Console 설정합니다.
3. 이전에 설정한 권한을 콘솔 에이전트에 제공합니다.

3 "NetApp Intelligent Services 구독(선택 사항)"

선택 사항: 클라우드 공급업체의 마켓플레이스에서 NetApp Intelligent Services 구독하여 시간당 요금(PAYGO) 또는 연간 계약을 통해 데이터 서비스 비용을 지불하세요. NetApp Intelligent Services 에는 NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience 및 NetApp Disaster Recovery 포함됩니다. NetApp Data Classification 추가 비용 없이 구독에 포함되어 있습니다.

제한 모드에서 배포 준비

제한 모드에서 NetApp Console 배포하기 전에 환경을 준비하세요. 호스트 요구 사항을 검토하고, 네트워킹을 준비하고, 권한을 설정하는 등의 작업이 필요합니다.

1단계: 제한 모드 작동 방식 이해

시작하기 전에 NetApp Console 제한 모드에서 어떻게 작동하는지 이해하세요.

설치된 NetApp Console 에이전트에서 로컬로 사용할 수 있는 브라우저 기반 인터페이스를 사용합니다. SaaS 계층을 통해 제공되는 웹 기반 콘솔에서는 NetApp Console 액세스할 수 없습니다.

또한, 일부 콘솔 기능과 NetApp 데이터 서비스를 이용할 수 없습니다.

"제한 모드의 작동 방식 알아보기" .

2단계: 설치 옵션 검토

제한 모드에서는 클라우드에만 콘솔 에이전트를 설치할 수 있습니다. 다음과 같은 설치 옵션을 사용할 수 있습니다.

- AWS Marketplace에서
- Azure Marketplace에서
- AWS, Azure 또는 Google Cloud에서 실행되는 자체 Linux 호스트에 콘솔 에이전트를 수동으로 설치합니다.

3단계: 호스트 요구 사항 검토

콘솔 에이전트를 실행하려면 호스트가 특정 OS, RAM 및 포트 요구 사항을 충족해야 합니다.

AWS 또는 Azure Marketplace에서 콘솔 에이전트를 배포하는 경우 이미지에는 필요한 OS 및 소프트웨어 구성 요소가 포함됩니다. CPU와 RAM 요구 사항을 충족하는 인스턴스 유형을 선택하기만 하면 됩니다.

전담 호스트

콘솔 에이전트를 실행하려면 전용 호스트가 필요합니다. 다음의 크기 요건을 충족하는 모든 아키텍처가 지원됩니다.

- CPU: 8개 코어 또는 8개 vCPU
- 램: 32GB
- 디스크 공간: 호스트에 권장되는 디스크 공간은 165GB이며, 다음 파티션 요구 사항이 적용됩니다.
  - `/opt`: 120GiB의 공간이 사용 가능해야 합니다.

    에이전트는 다음을 사용합니다. `/opt` 설치하려면 `/opt/application/netapp` 디렉토리와 그 내용.
  - `/var`: 40GiB의 공간이 사용 가능해야 합니다.

    콘솔 에이전트는 다음 공간이 필요합니다. `/var` Podman이나 Docker는 컨테이너를 이 디렉터리 내에 생성하도록 설계되었기 때문입니다. 구체적으로, 그들은 컨테이너를 생성할 것입니다. `/var/lib/containers/storage` 디렉토리 및 `/var/lib/docker` Docker용입니다. 이 공간에서는 외부 마운트나 심볼릭 링크가 작동하지 않습니다.

AWS EC2 인스턴스 유형

CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. NetApp t3.2xlarge를 권장합니다.

Azure VM 크기

CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. NetApp Standard_D8s_v3를 권장합니다.

Google Cloud 머신 유형

CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. NetApp n2-standard-8을 권장합니다.

콘솔 에이전트는 OS가 있는 VM 인스턴스의 Google Cloud에서 지원됩니다. "보호된 VM 기능"

하이퍼바이저

지원되는 운영 체제를 실행하도록 인증된 베어 메탈 또는 호스팅 하이퍼바이저가 필요합니다.

운영 체제 및 컨테이너 요구 사항

콘솔 에이전트는 표준 모드 또는 제한 모드에서 콘솔을 사용할 때 다음 운영 체제에서 지원됩니다. 에이전트를 설치하기 전에 컨테이너 오케스트레이션 도구가 필요합니다.

운영 체제	지원되는 **OS** 버전	지원되는 에이전트 버전	필수 컨테이너 도구	셀리눅스
레드햇 엔터프라이즈 리눅스		9.6 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	4.0.0 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 5.4.0과 podman-compose 1.5.0. Podman 구성 요구 사항 보기 .
강제 모드 또는 허용 모드에서 지원됨		9.1에서 9.4까지 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	3.9.50 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 4.9.4와 podman-compose 1.5.0. Podman 구성 요구 사항 보기 .

운영 체제	지원되는 **OS** 버전	지원되는 에이전트 버전	필수 컨테이너 도구	셀리눅스
강제 모드 또는 허용 모드에서 지원됨		8.6에서 8.10까지 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	3.9.50 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 4.6.1 또는 4.9.4와 podman-compose 1.0.6. Podman 구성 요구 사항 보기 .
강제 모드 또는 허용 모드에서 지원됨	우분투		24.04 장기	표준 모드 또는 제한 모드에서 NetApp Console 사용하는 3.9.45 이상
Docker 엔진 23.06~28.0.0.	지원되지 않음		22.04 장기	3.9.50 이상

4단계: **Podman** 또는 **Docker Engine** 설치

콘솔 에이전트를 수동으로 설치하려면 Podman이나 Docker Engine을 설치하여 호스트를 준비하세요.

운영 체제에 따라 에이전트를 설치하기 전에 Podman 또는 Docker Engine이 필요합니다.

- Red Hat Enterprise Linux 8 및 9에는 Podman이 필요합니다.

  지원되는 Podman 버전 보기 .

- Ubuntu에는 Docker 엔진이 필요합니다.

  지원되는 Docker Engine 버전 보기 .

예 **1.** 단계

포드만

Podman을 설치하고 구성하려면 다음 단계를 따르세요.

- podman.socket 서비스를 활성화하고 시작합니다.
- python3 설치
- podman-compose 패키지 버전 1.0.6을 설치하세요
- PATH 환경 변수에 podman-compose를 추가합니다.
- Red Hat Enterprise Linux를 사용하는 경우 Podman 버전이 CNI 대신 Netavark Aardvark DNS를 사용하는지 확인하십시오.

DNS 포트 충돌을 피하기 위해 에이전트를 설치한 후 aardvark-dns 포트(기본값: 53)를 조정하세요. 지침에 따라 포트를 구성하세요.

단계

1. 호스트에 podman-docker 패키지가 설치되어 있다면 제거합니다.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Podman을 설치하세요.

   공식 Red Hat Enterprise Linux 저장소에서 Podman을 다운로드할 수 있습니다.

   a. Red Hat Enterprise Linux 9.6의 경우:

   ```
   sudo dnf install podman-5:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

   b. Red Hat Enterprise Linux 9.1~9.4 버전의 경우:

   ```
   sudo dnf install podman-4:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

   c. Red Hat Enterprise Linux 8의 경우:

   ```
   sudo dnf install podman-4:<version>
   ```

   여기서 <버전>은 설치하려는 Podman의 지원되는 버전입니다. 지원되는 Podman 버전 보기 .

3. podman.socket 서비스를 활성화하고 시작합니다.

```
sudo systemctl enable --now podman.socket
```

4. python3를 설치합니다.

```
sudo dnf install python3
```

5. 시스템에 EPEL 저장소 패키지가 아직 없으면 설치하세요.

   이 단계는 podman-compose가 EPEL(Enterprise Linux용 추가 패키지) 저장소에서 사용 가능하기 때문에 필요합니다.

6. Red Hat Enterprise 9를 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. podman-compose 패키지 1.5.0을 설치합니다.

```
sudo dnf install podman-compose-1.5.0
```

7. Red Hat Enterprise Linux 8을 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. podman-compose 패키지 1.0.6을 설치합니다.

```
sudo dnf install podman-compose-1.0.6
```

> ⓘ 를 사용하여 `dnf install` 명령은 PATH 환경 변수에 podman-compose를 추가하는 요구 사항을 충족합니다. 설치 명령은 이미 포함되어 있는 /usr/bin에 podman-compose를 추가합니다. `secure_path` 호스트의 옵션.

   c. Red Hat Enterprise Linux 8을 사용하는 경우 Podman 버전이 CNI 대신 Aardvark DNS와 함께 NetAvark를 사용하는지 확인하세요.

i. 다음 명령을 실행하여 networkBackend가 CNI로 설정되어 있는지 확인하세요.

```
podman info | grep networkBackend
```

ii. networkBackend가 설정된 경우 `CNI` , 당신은 그것을 변경해야 합니다 `netavark` .

iii. 설치하다 `netavark` 그리고 `aardvark-dns` 다음 명령을 사용합니다.

```
dnf install aardvark-dns netavark
```

iv. 열기 `/etc/containers/containers.conf` 파일을 열고 network_backend 옵션을 "cni" 대신 "netavark"를 사용하도록 수정합니다.

만약에 `/etc/containers/containers.conf` 존재하지 않습니다. 구성을 변경하세요. `/usr/share/containers/containers.conf` .

v. Podman을 다시 시작하세요.

```
systemctl restart podman
```

vi. 다음 명령을 사용하여 networkBackend가 이제 "netavark"로 변경되었는지 확인하세요.

```
podman info | grep networkBackend
```

도커 엔진

Docker Engine을 설치하려면 Docker 설명서를 따르세요.

단계

1. "Docker에서 설치 지침 보기"

   지원되는 Docker Engine 버전을 설치하려면 다음 단계를 따르세요. 콘솔에서 지원되지 않으므로 최신 버전을 설치하지 마세요.

2. Docker가 활성화되어 실행 중인지 확인하세요.

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

5단계: 네트워크 액세스 준비

콘솔 에이전트가 퍼블릭 클라우드의 리소스를 관리할 수 있도록 네트워크 액세스를 설정합니다. 콘솔 에이전트에 대한 가상 네트워크와 서브넷을 갖추는 것 외에도 다음 요구 사항이 충족되는지 확인해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트가 저장 위치에 네트워크로 연결되어 있는지 확인하세요. 예를 들어, Cloud Volumes ONTAP 배포할 VPC 또는 VNet이나 온프레미스 ONTAP 클러스터가 있는 데이터 센터입니다.

NetApp Console 에 대한 사용자 액세스를 위한 네트워킹 준비

제한 모드에서는 사용자가 콘솔 에이전트 VM에서 콘솔에 액세스합니다. 콘솔 에이전트는 몇몇 엔드포인트에 연락하여 데이터 관리 작업을 완료합니다. 이러한 엔드포인트는 콘솔에서 특정 작업을 완료할 때 사용자 컴퓨터에서 접속됩니다.

버전 4.0.0 이전의 콘솔 에이전트에는 추가 엔드포인트가 필요합니다. 4.0.0 이상으로 업그레이드한 경우 허용 목록에서 이전 엔드포인트를 제거할 수 있습니다."4.0.0 이전 버전에 필요한 네트워크 액세스에 대해 자세히 알아보세요."

+

엔드포인트	목적
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.
\ https://cdn.auth0.com \ https://services.cloud.netapp.com	웹 브라우저는 NetApp Console 통해 중앙화된 사용자 인증을 위해 이러한 엔드포인트에 연결합니다.

일상 업무를 위한 아웃바운드 인터넷 접속

콘솔 에이전트의 네트워크 위치에는 아웃바운드 인터넷 액세스가 가능해야 합니다. NetApp Console 의 SaaS 서비스와 해당 퍼블릭 클라우드 환경 내의 엔드포인트에 도달할 수 있어야 합니다.

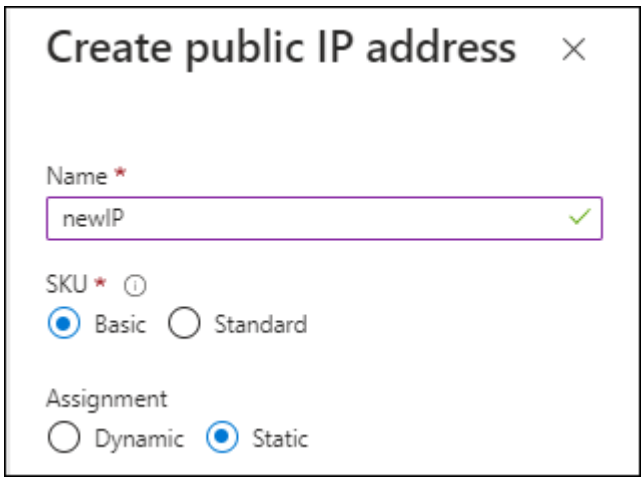
엔드포인트	목적
AWS 환경	AWS 서비스(amazonaws.com): • 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)
AWS 리소스를 관리합니다. 엔드포인트는 AWS 지역에 따라 달라집니다. "자세한 내용은 AWS 설명서를 참조하세요."	Amazon FsX for NetApp ONTAP: • api.workloads.netapp.com
웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.	**Azure** 환경

엔드포인트	목적
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Azure 공용 지역의 리소스를 관리합니다.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Azure Government 지역의 리소스를 관리합니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Azure China 지역의 리소스를 관리합니다.
Google Cloud 환경	https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 // https://config.googleapis.com/v1/projects
Google Cloud에서 리소스를 관리합니다.	• NetApp Console 엔드포인트*
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.

엔드포인트	목적
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

Azure의 공용 **IP** 주소

Azure의 콘솔 에이전트 VM에서 공용 IP 주소를 사용하려면 콘솔에서 이 공용 IP 주소를 사용하도록 IP 주소에 기본 SKU를 사용해야 합니다.



대신 표준 SKU IP 주소를 사용하면 콘솔은 공용 IP 대신 콘솔 에이전트의 개인 IP 주소를 사용합니다. 콘솔에 액세스하는 데 사용하는 컴퓨터가 해당 개인 IP 주소에 액세스할 수 없는 경우 콘솔의 작업은 실패합니다.

"Azure 설명서: 공용 IP SKU"

프록시 서버

NetApp 명시적 프록시 구성과 투명 프록시 구성을 모두 지원합니다. 투명 프록시를 사용하는 경우 프록시 서버에 대한 인증서만 제공하면 됩니다. 명시적 프록시를 사용하는 경우 IP 주소와 자격 증명도 필요합니다.

- IP 주소
- 신임장
- HTTPS 인증서

포트

Cloud Volumes ONTAP 에서 NetApp 지원팀으로 AutoSupport 메시지를 보내기 위한 프록시로 사용되거나 사용자가 시작하지 않는 한 콘솔 에이전트로 들어오는 트래픽이 없습니다.

- HTTP(80) 및 HTTPS(443)는 로컬 UI에 대한 액세스를 제공하며 이는 드문 상황에서 사용됩니다.
- SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.
- 아웃바운드 인터넷 연결을 사용할 수 없는 서브넷에 Cloud Volumes ONTAP 시스템을 배포하는 경우 포트 3128을 통한 인바운드 연결이 필요합니다.

  Cloud Volumes ONTAP 시스템에 AutoSupport 메시지를 보낼 아웃바운드 인터넷 연결이 없는 경우 콘솔은 콘솔 에이전트에 포함된 프록시 서버를 사용하도록 해당 시스템을 자동으로 구성합니다. 유일한 요구 사항은 콘솔 에이전트의 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는 것입니다. 콘솔 에이전트를 배포한 후 이 포트를 열어야 합니다.

NTP 활성화

NetApp Data Classification 사용하여 회사 데이터 소스를 스캔하려는 경우 콘솔 에이전트와 NetApp Data Classification 시스템 모두에서 NTP(네트워크 시간 프로토콜) 서비스를 활성화하여 시스템 간의 시간을 동기화해야 합니다. "NetApp 데이터 분류에 대해 자세히 알아보세요"

클라우드 공급업체의 마켓플레이스에서 콘솔 에이전트를 만들 계획이라면 콘솔 에이전트를 만든 후 이 네트워킹 요구 사항을 구현하세요.

6단계: 클라우드 권한 준비

콘솔 에이전트는 가상 네트워크에 Cloud Volumes ONTAP 배포하고 NetApp 데이터 서비스를 사용하려면 클라우드 공급자의 권한이 필요합니다. 클라우드 공급자에서 권한을 설정한 다음 해당 권한을 콘솔 에이전트와 연결해야 합니다.

필요한 단계를 보려면 클라우드 공급자에 사용할 인증 옵션을 선택하세요.

AWS IAM 역할

IAM 역할을 사용하여 콘솔 에이전트에 권한을 제공합니다.

AWS Marketplace에서 콘솔 에이전트를 생성하는 경우 EC2 인스턴스를 시작할 때 해당 IAM 역할을 선택하라는 메시지가 표시됩니다.

Linux 호스트에 콘솔 에이전트를 수동으로 설치하는 경우 해당 역할을 EC2 인스턴스에 연결합니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책을 만듭니다.
   a. *정책 > 정책 만들기*를 선택합니다.
   b. *JSON*을 선택하고 내용을 복사하여 붙여넣습니다."콘솔 에이전트에 대한 IAM 정책" .
   c. 나머지 단계를 완료하여 정책을 만듭니다.
3. IAM 역할을 만듭니다.
   a. *역할 > 역할 만들기*를 선택합니다.
   b. *AWS 서비스 > EC2*를 선택합니다.
   c. 방금 만든 정책을 첨부하여 권한을 추가합니다.
   d. 나머지 단계를 완료하여 역할을 만듭니다.

결과

이제 콘솔 에이전트 EC2 인스턴스에 대한 IAM 역할이 생겼습니다.

AWS 액세스 키

IAM 사용자에 대한 권한과 액세스 키를 설정합니다. 콘솔 에이전트를 설치하고 콘솔을 설정한 후에는 콘솔에 AWS 액세스 키를 제공해야 합니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책을 만듭니다.
   a. *정책 > 정책 만들기*를 선택합니다.
   b. *JSON*을 선택하고 내용을 복사하여 붙여넣습니다."콘솔 에이전트에 대한 IAM 정책" .
   c. 나머지 단계를 완료하여 정책을 만듭니다.

      사용하려는 NetApp 데이터 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다.

   표준 지역의 경우 권한은 두 가지 정책에 걸쳐 분산됩니다. AWS의 관리형 정책에는 최대 문자 크기 제한이 있으므로 두 개의 정책이 필요합니다. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요." .
3. IAM 사용자에게 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"

4. 콘솔 에이전트를 설치한 후 NetApp Console 에 추가할 수 있는 액세스 키가 사용자에게 있는지 확인하세요.

Azure 역할

필요한 권한이 있는 Azure 사용자 지정 역할을 만듭니다. 이 역할은 콘솔 에이전트 VM에 할당합니다.

Azure Portal, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 만들 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 만드는 방법을 보여줍니다. 다른 방법을 사용하려면 다음을 참조하세요. "Azure 설명서"

단계

1. 자체 호스트에 소프트웨어를 수동으로 설치하려는 경우 VM에서 시스템이 할당한 관리 ID를 활성화하여 사용자 지정 역할을 통해 필요한 Azure 권한을 제공할 수 있습니다.

   "Microsoft Azure 설명서: Azure Portal을 사용하여 VM의 Azure 리소스에 대한 관리 ID 구성"

2. 내용을 복사하세요"커넥터에 대한 사용자 정의 역할 권한" JSON 파일에 저장합니다.
3. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

   NetApp Console 과 함께 사용하려는 각 Azure 구독에 대한 ID를 추가해야 합니다.

   예

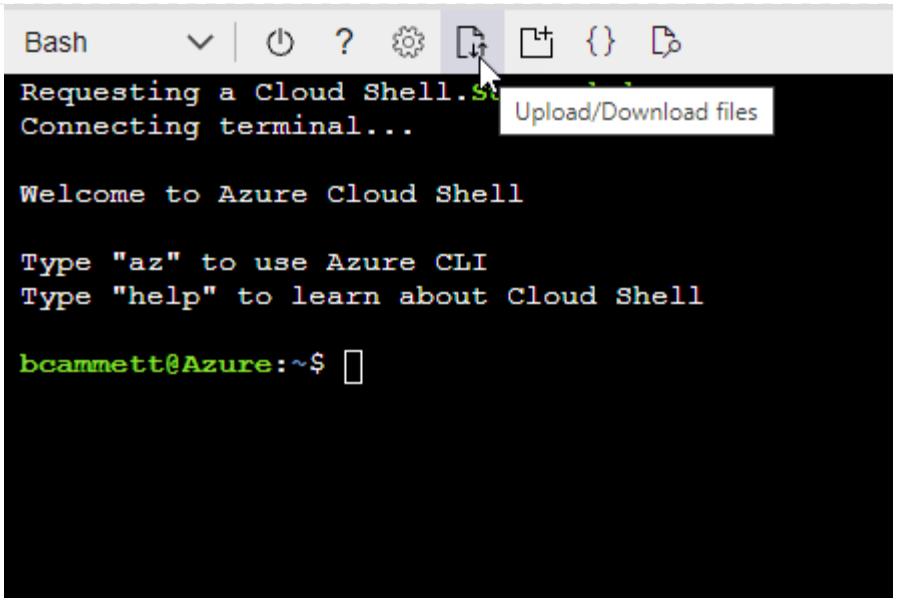
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ]
   ```

4. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 만듭니다.

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

   a. 시작 "Azure 클라우드 셸" Bash 환경을 선택하세요.

   b. JSON 파일을 업로드합니다.



c. Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

Azure 서비스 주체

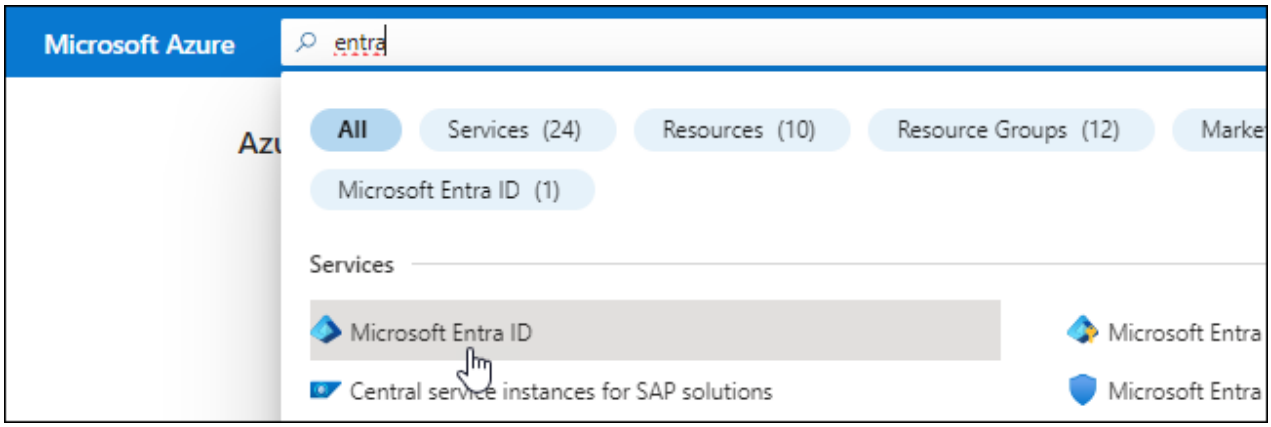
Microsoft Entra ID에서 서비스 주체를 만들고 설정하고 콘솔에 필요한 Azure 자격 증명을 얻습니다. 콘솔 에이전트를 설치한 후 콘솔에 이러한 자격 증명을 제공해야 합니다.

역할 기반 액세스 제어를 위한 **Microsoft Entra** 애플리케이션 만들기

1. Azure에서 Active Directory 애플리케이션을 만들고 해당 애플리케이션에 역할을 할당할 수 있는 권한이 있는지 확인하세요.

   자세한 내용은 다음을 참조하세요. "Microsoft Azure 설명서: 필요한 권한"

2. Azure Portal에서 **Microsoft Entra ID** 서비스를 엽니다.



3. 메뉴에서 *앱 등록*을 선택하세요.
4. *신규 등록*을 선택하세요.

5. 신청서에 대한 세부 사항을 지정하세요:
   - 이름: 애플리케이션의 이름을 입력하세요.
   - 계정 유형: 계정 유형을 선택하세요(모든 계정 유형이 NetApp Console 에서 작동합니다).
   - 리디렉션 **URI**: 이 필드는 비워두어도 됩니다.
6. *등록*을 선택하세요.

   AD 애플리케이션과 서비스 주체를 생성했습니다.

역할에 애플리케이션 할당

1. 사용자 정의 역할 만들기:

   Azure Portal, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 만들 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 만드는 방법을 보여줍니다. 다른 방법을 사용하려면 다음을 참조하세요. "Azure 설명서"

   a. 내용을 복사하세요"콘솔 에이전트에 대한 사용자 정의 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.

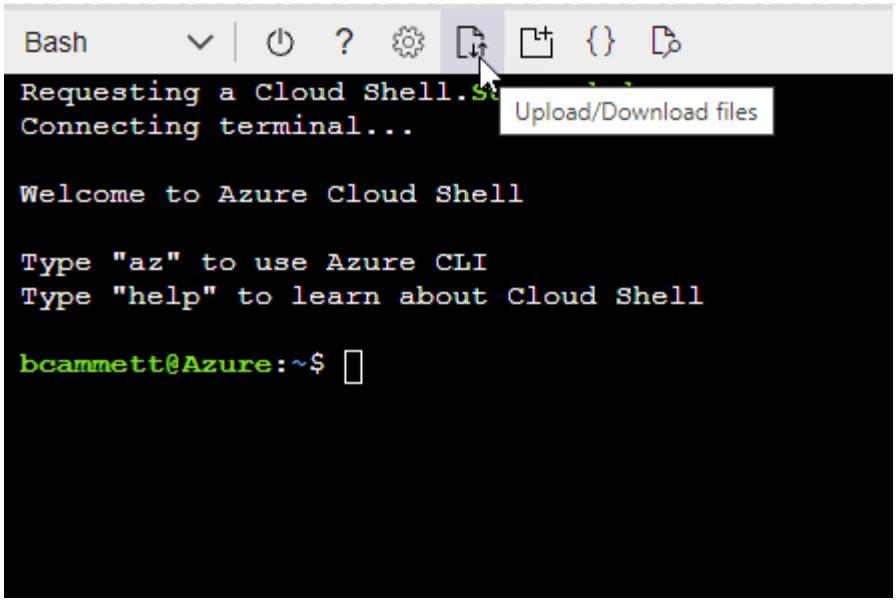
      예

      ```
      "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 만듭니다.

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

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



- Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

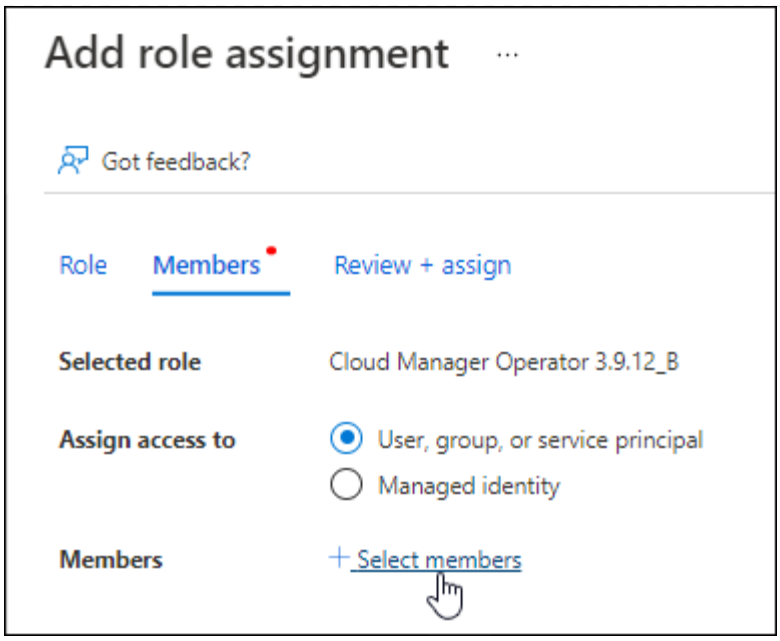
```
az role definition create --role-definition agent_Policy.json
```

이제 콘솔 에이전트 가상 머신에 할당할 수 있는 콘솔 운영자라는 사용자 지정 역할이 생겼습니다.

2. 역할에 애플리케이션을 할당합니다.

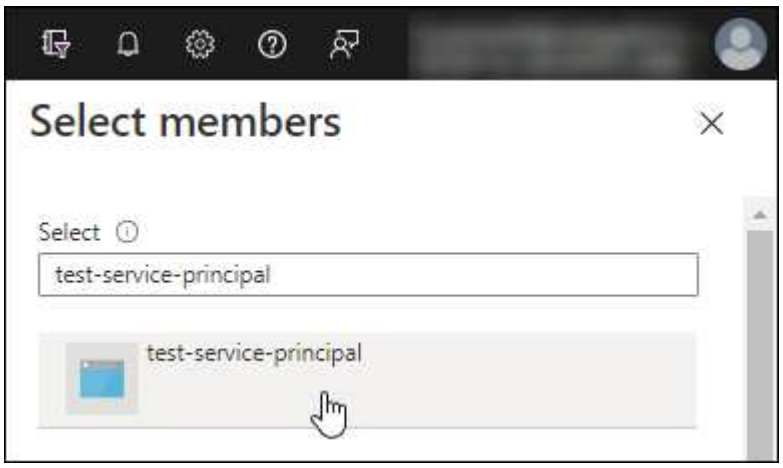
   a. Azure Portal에서 구독 서비스를 엽니다.
   b. 구독을 선택하세요.
   c. *액세스 제어(IAM) > 추가 > 역할 할당 추가*를 선택합니다.
   d. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.
   e. 멤버 탭에서 다음 단계를 완료하세요.

      - *사용자, 그룹 또는 서비스 주체*를 선택된 상태로 유지합니다.
      - *멤버 선택*을 선택하세요.



- 애플리케이션 이름을 검색하세요.

  예를 들면 다음과 같습니다.



- 애플리케이션을 선택하고 *선택*을 선택하세요.
- *다음*을 선택하세요.

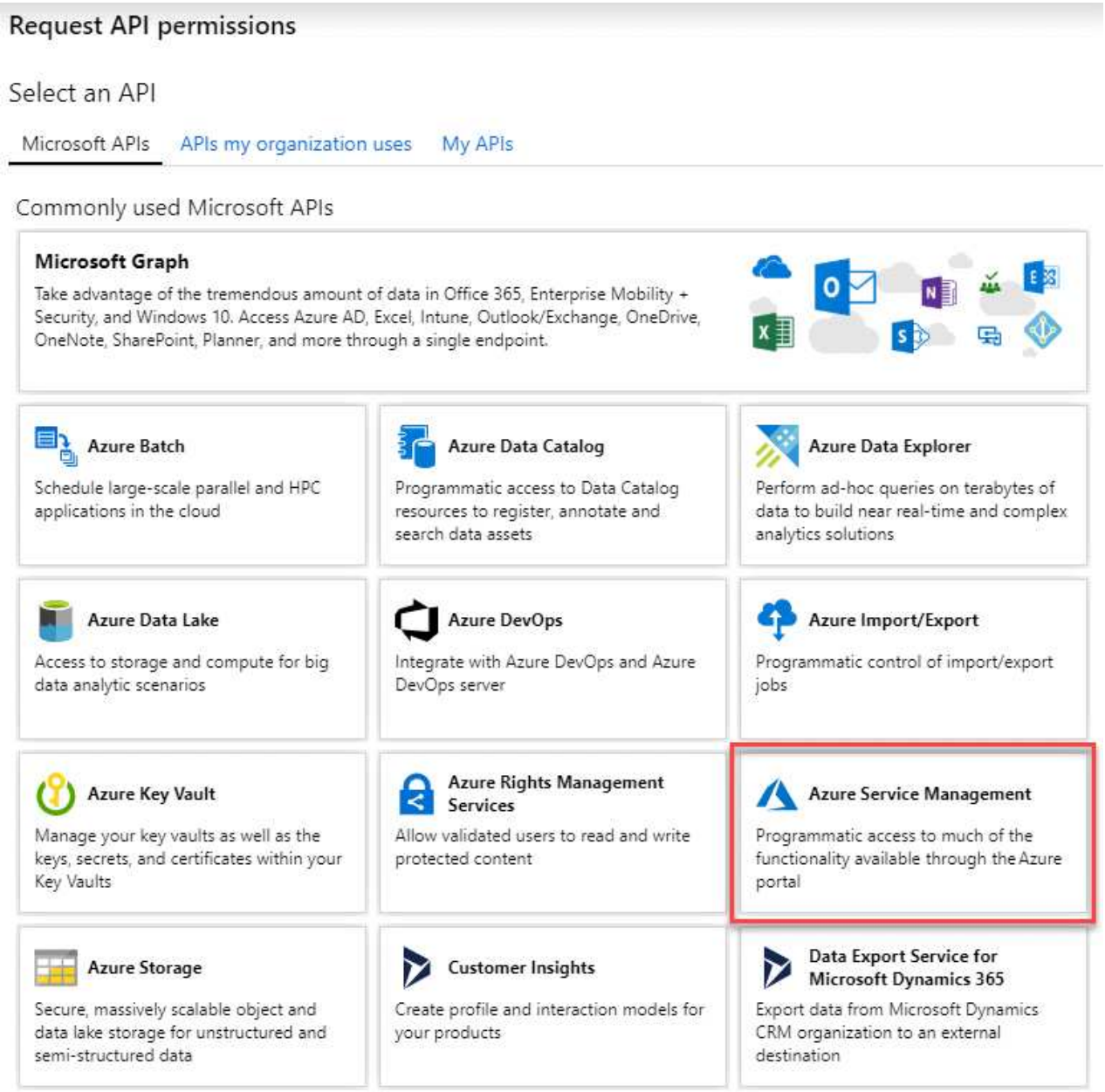
f. *검토 + 할당*을 선택하세요.

이제 서비스 주체는 콘솔 에이전트를 배포하는 데 필요한 Azure 권한을 갖게 되었습니다.

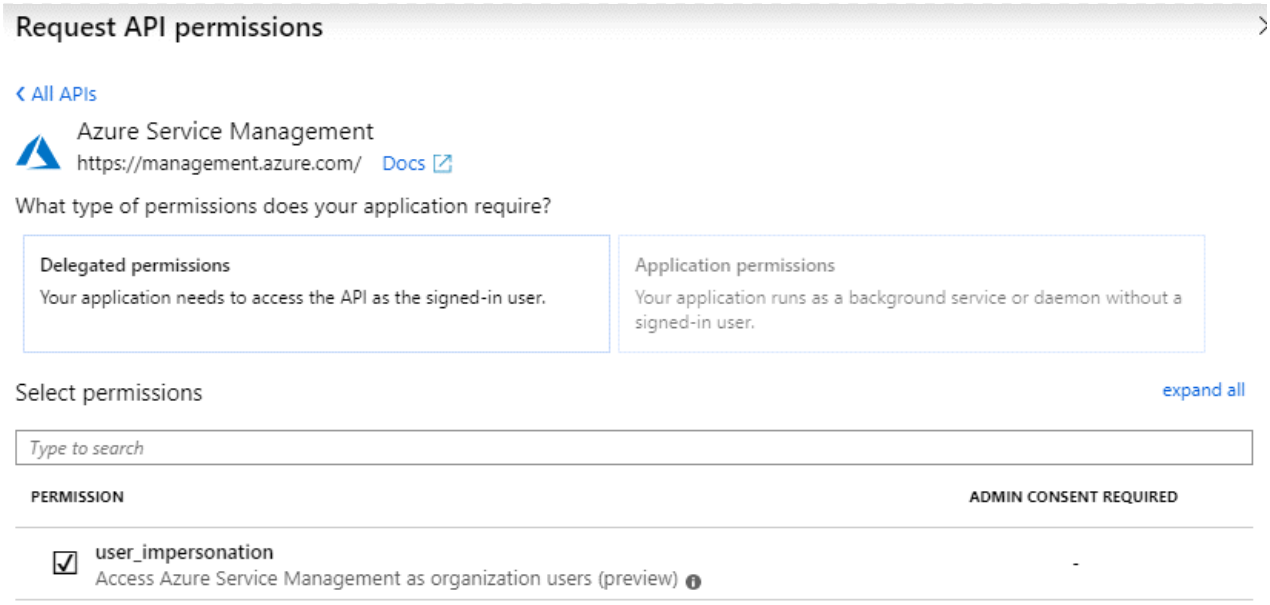
여러 Azure 구독에서 Cloud Volumes ONTAP 배포하려면 각 구독에 서비스 주체를 바인딩해야 합니다. NetApp Console 에서 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한 추가

1. **Microsoft Entra ID** 서비스에서 *앱 등록*을 선택하고 애플리케이션을 선택합니다.
2. *API 권한 > 권한 추가*를 선택합니다.
3. *Microsoft API*에서 *Azure Service Management*를 선택합니다.

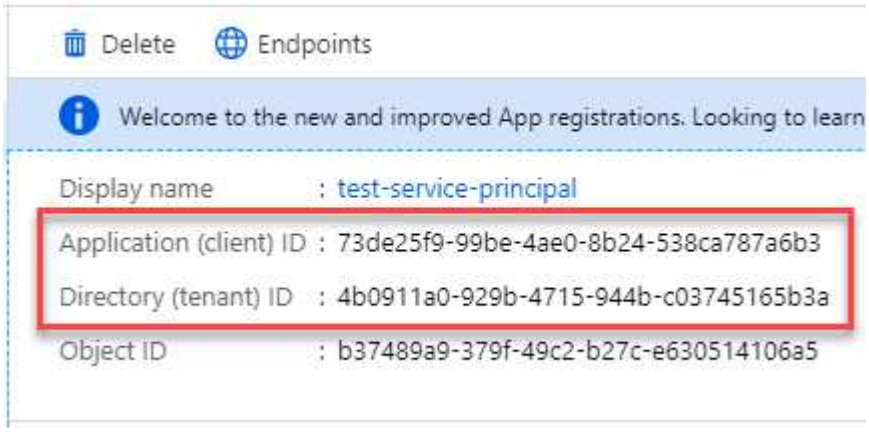


4. *조직 사용자로 Azure Service Management에 액세스*를 선택한 다음 *권한 추가*를 선택합니다.



애플리케이션의 애플리케이션 **ID**와 디렉토리 **ID**를 가져옵니다**.**

1. **Microsoft Entra ID** 서비스에서 *앱 등록*을 선택하고 애플리케이션을 선택합니다.
2. *애플리케이션(클라이언트) ID*와 *디렉토리(테넌트) ID*를 복사합니다.



콘솔에 Azure 계정을 추가하는 경우 애플리케이션(클라이언트) ID와 애플리케이션의 디렉터리(테넌트) ID를 제공해야 합니다. 콘솔은 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 비밀을 생성하세요

1. **Microsoft Entra ID** 서비스를 엽니다.
2. *앱 등록*을 선택하고 애플리케이션을 선택하세요.
3. *인증서 및 비밀번호 > 새 클라이언트 비밀번호*를 선택합니다.
4. 비밀에 대한 설명과 기간을 제공하세요.
5. *추가*를 선택하세요.
6. 클라이언트 비밀번호 값을 복사합니다.

결과

이제 서비스 주체가 설정되었고 애플리케이션(클라이언트) ID, 디렉토리(테넌트) ID 및 클라이언트 비밀번호 값을 복사했어야 합니다. Azure 계정을 추가할 때 콘솔에 이 정보를 입력해야 합니다.

Google Cloud 서비스 계정

역할을 만들고 콘솔 에이전트 VM 인스턴스에 사용할 서비스 계정에 적용합니다.

단계

1. Google Cloud에서 사용자 지정 역할을 만듭니다.

   a. 정의된 권한을 포함하는 YAML 파일을 만듭니다."Google Cloud용 콘솔 에이전트 정책" .

   b. Google Cloud에서 Cloud Shell을 활성화합니다.

   c. 콘솔 에이전트에 필요한 권한이 포함된 YAML 파일을 업로드합니다.

   d. 다음을 사용하여 사용자 정의 역할을 만듭니다. `gcloud iam roles create` 명령.

      다음 예제는 프로젝트 수준에서 "agent"라는 이름의 역할을 생성합니다.

```
gcloud iam roles create agent --project=myproject --file=agent.yaml
```

   +
   "Google Cloud 문서: 사용자 지정 역할 만들기 및 관리"

2. Google Cloud에서 서비스 계정을 만듭니다.

   a. IAM 및 관리 서비스에서 *서비스 계정 > 서비스 계정 만들기*를 선택합니다.

   b. 서비스 계정 세부 정보를 입력하고 *만들기 및 계속*을 선택하세요.

   c. 방금 만든 역할을 선택하세요.

   d. 나머지 단계를 완료하여 역할을 만듭니다.

      "Google Cloud 문서: 서비스 계정 만들기"

7단계: **Google Cloud API** 활성화

Google Cloud에 Cloud Volumes ONTAP 배포하려면 여러 API가 필요합니다.

단계

1. "프로젝트에서 다음 Google Cloud API를 활성화하세요."
    - 클라우드 인프라 관리자 API
    - 클라우드 배포 관리자 V2 API
    - 클라우드 로깅 API
    - 클라우드 리소스 관리자 API
    - 컴퓨트 엔진 API
    - ID 및 액세스 관리(IAM) API
    - 클라우드 키 관리 서비스(KMS) API

      (고객 관리 암호화 키(CMEK)와 함께 NetApp Backup and Recovery 사용하려는 경우에만 필요함)

제한 모드로 콘솔 에이전트 배포

NetApp Console 제한된 아웃바운드 연결로 사용할 수 있도록 콘솔 에이전트를 제한 모드로 배포합니다. 시작하려면 콘솔 에이전트를 설치하고, 콘솔 에이전트에서 실행되는 사용자 인터페이스에 액세스하여 콘솔을 설정한 다음, 이전에 설정한 클라우드 권한을 제공하세요.

1단계: 콘솔 에이전트 설치

클라우드 공급업체의 마켓플레이스에서 콘솔 에이전트를 설치하거나 Linux 호스트에 수동으로 설치합니다.

AWS 커머셜 마켓플레이스

시작하기 전에

다음 사항을 숙지하십시오:

- 네트워킹 요구 사항을 충족하는 VPC 및 서브넷.

  "네트워킹 요구 사항에 대해 알아보세요"

- 콘솔 에이전트에 필요한 권한이 포함된 정책이 첨부된 IAM 역할입니다.

  "AWS 권한을 설정하는 방법을 알아보세요"

- IAM 사용자가 AWS Marketplace를 구독하고 구독을 취소할 수 있는 권한입니다.
- 에이전트의 CPU 및 RAM 요구 사항에 대한 이해.

  "에이전트 요구 사항 검토".

- EC2 인스턴스에 대한 키 쌍입니다.

단계

1. 로 가다 "AWS Marketplace에 NetApp Console 에이전트 목록이 추가되었습니다."
2. 마켓플레이스 페이지에서 *구독 계속하기*를 선택하세요.
3. 소프트웨어를 구독하려면 *약관 동의*를 선택하세요.

   구독 절차는 몇 분 정도 걸릴 수 있습니다.

4. 구독 프로세스가 완료되면 *구성 계속*을 선택하세요.
5. 이 소프트웨어 구성 페이지에서 올바른 지역을 선택했는지 확인한 다음 *계속 실행*을 선택합니다.
6. 이 소프트웨어 실행 페이지의 *작업 선택*에서 *EC2를 통해 실행*을 선택한 다음 *실행*을 선택합니다.

   EC2 콘솔을 사용하여 인스턴스를 시작하고 IAM 역할을 연결합니다. 웹사이트에서 실행 작업에서는 이 작업이 불가능합니다.

7. 프롬프트에 따라 인스턴스를 구성하고 배포하세요.
   - 이름 및 태그: 인스턴스의 이름과 태그를 입력합니다.
   - 애플리케이션 및 **OS** 이미지: 이 섹션을 건너뜁니다. 콘솔 에이전트 AMI가 이미 선택되었습니다.
   - 인스턴스 유형: 지역별 가용성에 따라 RAM 및 CPU 요구 사항을 충족하는 인스턴스 유형을 선택합니다(t3.2xlarge가 미리 선택되어 권장됨).
   - 키 쌍(로그인): 인스턴스에 안전하게 연결하는 데 사용할 키 쌍을 선택하세요.
   - 네트워크 설정: 필요에 따라 네트워크 설정을 편집하세요.
     - 원하는 VPC와 서브넷을 선택하세요.
     - 인스턴스에 공용 IP 주소가 있어야 하는지 여부를 지정합니다.
     - 콘솔 에이전트 인스턴스에 필요한 연결 방법(SSH, HTTP, HTTPS)을 활성화하는 보안 그룹 설정을 지정합니다.

"AWS에 대한 보안 그룹 규칙 보기" .

- 저장소 구성: 루트 볼륨의 기본 크기와 디스크 유형을 유지합니다.

  루트 볼륨에서 Amazon EBS 암호화를 활성화하려면 *고급*을 선택하고 *볼륨 1*을 확장한 다음 *암호화*를 선택하고 KMS 키를 선택합니다.

- 고급 세부 정보: *IAM 인스턴스 프로필*에서 콘솔 에이전트에 필요한 권한이 포함된 IAM 역할을 선택합니다.
- 요약: 요약을 검토하고 *인스턴스 시작*을 선택합니다.

결과

AWS는 지정된 설정으로 소프트웨어를 시작합니다. 콘솔 에이전트는 약 5분 안에 배포됩니다.

다음은 무엇인가요?

NetApp Console 설정합니다.

AWS Gov 마켓플레이스

시작하기 전에

다음 사항을 숙지하십시오:

- 네트워킹 요구 사항을 충족하는 VPC 및 서브넷.

  "네트워킹 요구 사항에 대해 알아보세요"

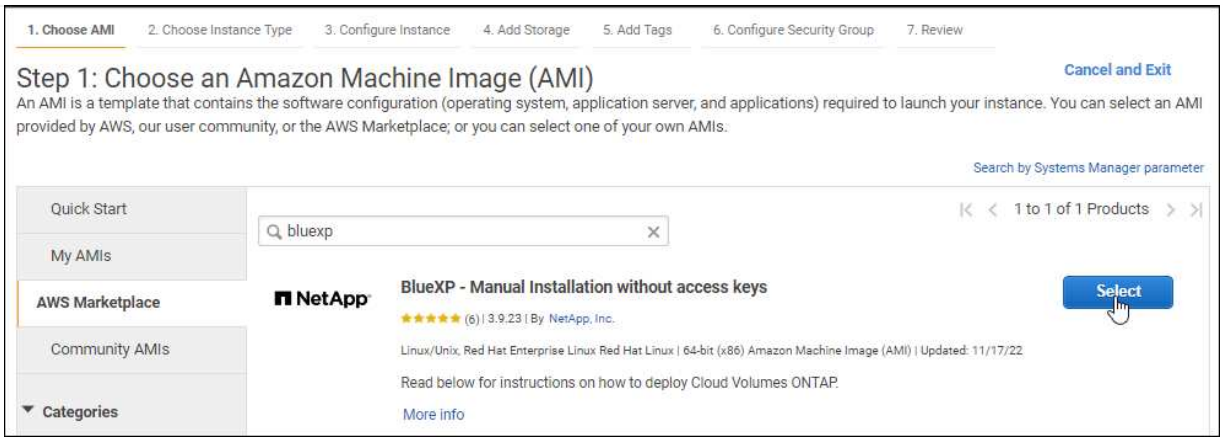
- 콘솔 에이전트에 필요한 권한이 포함된 정책이 첨부된 IAM 역할입니다.

  "AWS 권한을 설정하는 방법을 알아보세요"

- IAM 사용자가 AWS Marketplace를 구독하고 구독을 취소할 수 있는 권한입니다.
- EC2 인스턴스에 대한 키 쌍입니다.

단계

1. AWS Marketplace에서 NetApp Console 에이전트 제품으로 이동합니다.
   a. EC2 서비스를 열고 *인스턴스 시작*을 선택합니다.
   b. *AWS Marketplace*를 선택하세요.
   c. NetApp Console 검색하고 제품을 선택하세요.



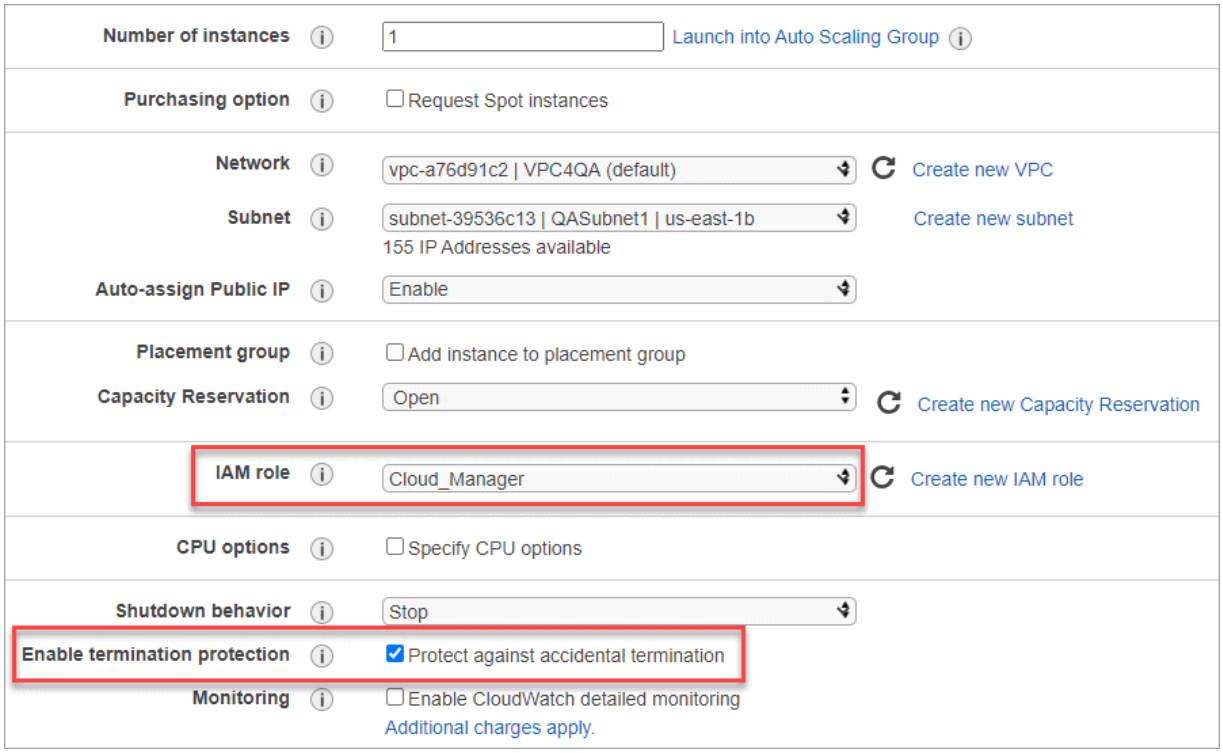
d. *계속*을 선택하세요.

2. 안내에 따라 인스턴스를 설정하고 시작하십시오.

   - 인스턴스 유형 선택: 지역별 가용성에 따라 지원되는 인스턴스 유형 중 하나를 선택합니다(t3.2xlarge 권장).

     "인스턴스 요구 사항 검토" .

   - 인스턴스 세부 정보 구성: VPC와 서브넷을 선택하고, 1단계에서 생성한 IAM 역할을 선택하고, 종료 보호를 활성화(권장)하고, 요구 사항을 충족하는 다른 구성 옵션을 선택합니다.



   - 저장 공간 추가: 기본 저장 공간 옵션을 유지합니다.
   - 태그 추가: 원하는 경우 인스턴스에 대한 태그를 입력합니다.
   - 보안 그룹 구성: 콘솔 에이전트 인스턴스에 필요한 연결 방법(SSH, HTTP, HTTPS)을 지정합니다.
   - 검토: 선택 사항을 검토하고 *실행*을 선택합니다.

결과

AWS는 지정된 설정으로 소프트웨어를 시작합니다. 콘솔 에이전트는 약 5분 안에 배포됩니다.

다음은 무엇인가요?

콘솔을 설정합니다.

Azure Gov 마켓플레이스

시작하기 전에

다음 사항이 있어야 합니다.

- 네트워킹 요구 사항을 충족하는 VNet 및 서브넷.

  "네트워킹 요구 사항에 대해 알아보세요"

- 콘솔 에이전트에 필요한 권한이 포함된 Azure 사용자 지정 역할입니다.

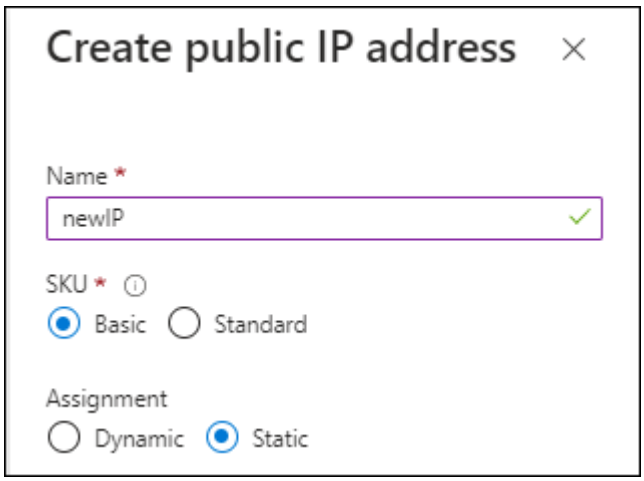
  "Azure 권한을 설정하는 방법 알아보기"

단계

1. Azure Marketplace의 NetApp Console 에이전트 VM 페이지로 이동합니다.
   - "상업 지역을 위한 Azure Marketplace 페이지"
   - "Azure Government 지역에 대한 Azure Marketplace 페이지"
2. *지금 받기*를 선택한 다음 *계속*을 선택하세요.
3. Azure Portal에서 *만들기*를 선택하고 단계에 따라 가상 머신을 구성합니다.

   VM을 구성할 때 다음 사항에 유의하세요.

   - **VM** 크기: CPU 및 RAM 요구 사항을 충족하는 VM 크기를 선택하세요. Standard_D8s_v3을 권장합니다.
   - 디스크: 콘솔 에이전트는 HDD 또는 SSD 디스크를 사용하면 최적의 성능을 발휘할 수 있습니다.
   - 공용 **IP**: 콘솔 에이전트 VM에서 공용 IP 주소를 사용하려면 기본 SKU를 선택하십시오.



   대신 표준 SKU IP 주소를 사용하면 콘솔은 공용 IP 대신 콘솔 에이전트의 개인 IP 주소를 사용합니다.

콘솔에 접속하는 데 사용하는 기기가 사설 IP 주소에 연결할 수 없는 경우 콘솔이 작동하지 않습니다.

"Azure 설명서: 공용 IP SKU"

- 네트워크 보안 그룹: 콘솔 에이전트에는 SSH, HTTP, HTTPS를 사용하는 인바운드 연결이 필요합니다.

  "Azure에 대한 보안 그룹 규칙 보기" .

- **ID**: *관리*에서 *시스템에서 할당한 관리 ID 사용*을 선택합니다.

  관리되는 ID를 사용하면 콘솔 에이전트 VM이 자격 증명 없이 Microsoft Entra ID에 자신을 식별할 수 있습니다. "Azure 리소스에 대한 관리 ID에 대해 자세히 알아보세요." .

4. 검토 **+** 생성 페이지에서 선택 사항을 검토하고 *생성*을 선택하여 배포를 시작합니다.

결과

Azure는 지정된 설정으로 가상 머신을 배포합니다. 가상 머신과 콘솔 에이전트 소프트웨어는 약 5분 안에 실행될 것입니다.

다음은 무엇인가요**?**

NetApp Console 설정합니다.

수동 설치

시작하기 전에

다음 사항이 있어야 합니다.

- 콘솔 에이전트를 설치하려면 루트 권한이 필요합니다.
- 콘솔 에이전트에서 인터넷에 접속하는 데 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

  설치 후 프록시 서버를 구성할 수 있지만, 그렇게 하려면 콘솔 에이전트를 다시 시작해야 합니다.

- 프록시 서버가 HTTPS를 사용하거나 프록시가 가로채기 프록시인 경우 CA 서명 인증서가 필요합니다.

> ⓘ 콘솔 에이전트를 수동으로 설치하는 경우 투명 프록시 서버에 대한 인증서를 설정할 수 없습니다. 투명 프록시 서버에 대한 인증서를 설정해야 하는 경우 설치 후 유지 관리 콘솔을 사용해야 합니다. 자세히 알아보세요"에이전트 유지 관리 콘솔" .

- 설치 중에 아웃바운드 연결을 확인하는 구성 검사를 비활성화해야 합니다. 이 검사를 비활성화하지 않으면 수동 설치가 실패합니다."수동 설치에 대한 구성 검사를 비활성화하는 방법을 알아보세요."
- 콘솔 에이전트를 설치하기 전에 운영 체제에 따라 Podman 또는 Docker Engine이 필요합니다.

이 작업에 관하여

설치 후, 새로운 버전이 나오면 콘솔 에이전트가 자동으로 업데이트됩니다.

단계

1. 호스트에 *http_proxy* 또는 *https_proxy* 시스템 변수가 설정되어 있으면 제거합니다.

```
unset http_proxy
unset https_proxy
```

이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

2. 콘솔 에이전트 소프트웨어를 다운로드한 다음 Linux 호스트에 복사하십시오. NetApp Console 또는 NetApp 지원 사이트에서 다운로드할 수 있습니다.
   - NetApp Console: *에이전트 > 관리 > 에이전트 배포 > 온프레미스 > 수동 설치*로 이동합니다.

     에이전트 설치 파일 다운로드 또는 파일 URL 다운로드를 선택하십시오.

   - NetApp 지원 사이트 (콘솔에 대한 액세스 권한이 없는 경우 필요) "NetApp 지원 사이트" ,
3. 스크립트를 실행할 수 있는 권한을 할당합니다.

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

여기서 <버전>은 다운로드한 콘솔 에이전트의 버전입니다.

4. 정부 클라우드 환경에 설치하는 경우 구성 검사를 비활성화하세요."수동 설치에 대한 구성 검사를 비활성화하는 방법을 알아보세요."
5. 설치 스크립트를 실행합니다.

```
./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

네트워크에 인터넷 접속을 위한 프록시가 필요한 경우 프록시 정보를 추가해야 합니다. 설치 중에 명시적 프록시를 추가할 수 있습니다. --proxy 및 --cacert 매개변수는 선택 사항이므로 추가하라는 메시지가 표시되지 않습니다. 명시적 프록시 서버가 있는 경우 표시된 대로 매개변수를 입력해야 합니다.

다음은 CA 서명 인증서로 명시적 프록시 서버를 구성하는 예입니다.

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

`--proxy`다음 형식 중 하나를 사용하여 HTTP 또는 HTTPS 프록시 서버를 사용하도록 콘솔 에이전트를 구성합니다.

- http://주소:포트
- http://사용자 이름:비밀번호@주소:포트
- http://도메인 이름%92사용자 이름:비밀번호@주소:포트
- https://주소:포트

- https://사용자 이름:비밀번호@주소:포트
- https://도메인 이름%92사용자 이름:비밀번호@주소:포트

다음 사항에 유의하세요.

- 사용자는 로컬 사용자 또는 도메인 사용자일 수 있습니다.
- 도메인 사용자의 경우 위에 표시된 대로 \에 대한 ASCII 코드를 사용해야 합니다.
- 콘솔 에이전트는 @ 문자가 포함된 사용자 이름이나 비밀번호를 지원하지 않습니다.
- 비밀번호에 다음과 같은 특수 문자가 포함되어 있는 경우, 백슬래시를 앞에 붙여 해당 특수 문자를 이스케이프해야 합니다: & 또는 !

  예를 들어:

http://bxpproxyuser:netapp1\!@주소:3128

투명 프록시를 구성하려면 설치 후에 구성하면 됩니다. "에이전트 유지 관리 콘솔에 대해 알아보세요"

1. Podman을 사용한 경우 aardvark-dns 포트를 조정해야 합니다.

   a. 콘솔 에이전트 가상 머신에 SSH를 실행합니다.

   b. podman */usr/share/containers/containers.conf* 파일을 열고 Aardvark DNS 서비스에 대해 선택한 포트를 수정합니다. 예를 들어, 54로 변경합니다.

   ```
   vi /usr/share/containers/containers.conf
   ```

   예를 들어:

   ```
   # Port to use for dns forwarding daemon with netavark in rootful
   bridge
   # mode and dns enabled.
   # Using an alternate port might be useful if other DNS services
   should
   # run on the machine.
   #
   dns_bind_port = 54
   ```

   a. 콘솔 에이전트 가상 머신을 재부팅합니다.

결과

콘솔 에이전트가 설치되었습니다. 설치가 끝나면 프록시 서버를 지정한 경우 콘솔 에이전트 서비스(occm)가 두 번 다시 시작됩니다.

다음은 무엇인가요?

NetApp Console 설정합니다.

2단계: NetApp Console 설정

처음으로 콘솔에 액세스하면 콘솔 에이전트의 조직을 선택하라는 메시지가 표시되고 제한 모드를 활성화해야 합니다.

시작하기 전에

콘솔 에이전트를 설정하는 사람은 콘솔 조직에 속하지 않은 로그인을 사용하여 콘솔에 로그인해야 합니다.

로그인 정보가 다른 기관과 연결되어 있는 경우, 새 로그인 정보를 사용하여 가입해야 합니다. 그렇지 않으면 설정 화면에서 제한 모드를 활성화하는 옵션이 표시되지 않습니다.

단계

1. 콘솔 에이전트 인스턴스에 연결된 호스트에서 웹 브라우저를 열고 설치한 콘솔 에이전트의 다음 URL을 입력합니다.
2. NetApp Console 에 가입하거나 로그인하세요.
3. 로그인한 후 콘솔을 설정하세요.
    a. 콘솔 에이전트의 이름을 입력하세요.
    b. 새로운 콘솔 조직의 이름을 입력하세요.
    c. *보안된 환경에서 실행하고 있습니까?*를 선택하세요.
    d. *이 계정에서 제한 모드 사용*을 선택하세요.

        계정이 생성된 후에는 이 설정을 변경할 수 없습니다. 제한 모드는 나중에 활성화할 수 없고, 나중에 비활성화할 수도 없습니다.

    정부 지역에 콘솔 에이전트를 배포한 경우 확인란이 이미 활성화되어 있으므로 변경할 수 없습니다. 제한 모드는 정부 지역에서 지원되는 유일한 모드이기 때문입니다.

    a. *시작하기*를 선택하세요.

결과

이제 콘솔 에이전트가 설치되고 콘솔 조직에 설정되었습니다. 모든 사용자는 콘솔 에이전트 인스턴스의 IP 주소를 사용하여 콘솔에 액세스해야 합니다.

다음은 무엇인가요?

이전에 설정한 권한을 콘솔에 제공하세요.

3단계: 콘솔 에이전트에 권한 제공

Azure Marketplace에서 또는 수동으로 콘솔 에이전트를 설치한 경우 이전에 설정한 권한을 부여해야 합니다.

배포 중에 필요한 IAM 역할을 선택했기 때문에 AWS Marketplace에서 콘솔 에이전트를 배포한 경우에는 이러한 단계가 적용되지 않습니다.

"클라우드 권한을 준비하는 방법을 알아보세요" .

AWS IAM 역할

이전에 생성한 IAM 역할을 콘솔 에이전트를 설치한 EC2 인스턴스에 연결합니다.

이 단계는 AWS에 콘솔 에이전트를 수동으로 설치한 경우에만 적용됩니다. AWS Marketplace 배포의 경우 이미 필요한 권한이 포함된 IAM 역할과 콘솔 에이전트 인스턴스를 연결했습니다.

단계

1. Amazon EC2 콘솔로 이동합니다.
2. *인스턴스*를 선택하세요.
3. 콘솔 에이전트 인스턴스를 선택합니다.
4. *작업 > 보안 > IAM 역할 수정*을 선택합니다.
5. IAM 역할을 선택하고 *IAM 역할 업데이트*를 선택합니다.

AWS 액세스 키

필요한 권한이 있는 IAM 사용자의 AWS 액세스 키를 NetApp Console 에 제공합니다.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *조직 자격 증명*을 선택하세요.
3. *자격 증명 추가*를 선택하고 마법사의 단계를 따르세요.
   a. 자격 증명 위치: *Amazon Web Services > 에이전트를 선택하세요.
   b. 자격 증명 정의: AWS 액세스 키와 비밀 키를 입력합니다.
   c. 마켓플레이스 구독: 지금 구독하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. 검토: 새로운 자격 증명에 대한 세부 정보를 확인하고 *추가*를 선택합니다.

Azure 역할

Azure Portal로 이동하여 하나 이상의 구독에 대한 콘솔 에이전트 가상 머신에 Azure 사용자 지정 역할을 할당합니다.

단계

1. Azure Portal에서 구독 서비스를 열고 구독을 선택합니다.

   구독 서비스에서 역할을 할당하는 것이 중요한 이유는 이를 통해 구독 수준에서 역할 할당의 범위가 지정되기 때문입니다. _scope_는 액세스가 적용되는 리소스 집합을 정의합니다. 다른 수준(예: 가상 머신 수준)에서 범위를 지정하는 경우 NetApp Console 내에서 작업을 완료하는 기능에 영향을 미칩니다.

   "Microsoft Azure 설명서: Azure RBAC 범위 이해"

2. 액세스 제어**(IAM)** > 추가 > *역할 할당 추가*를 선택합니다.
3. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.

콘솔 운영자는 정책에 제공된 기본 이름입니다. 역할에 다른 이름을 선택한 경우 해당 이름을 대신 선택하세요.

4. 멤버 탭에서 다음 단계를 완료하세요.
   a. *관리되는 ID*에 대한 액세스 권한을 할당합니다.
   b. *멤버 선택*을 선택하고, 콘솔 에이전트 가상 머신이 생성된 구독을 선택하고, *관리 ID*에서 *가상 머신*을 선택한 다음, 콘솔 에이전트 가상 머신을 선택합니다.
   c. *선택*을 선택하세요.
   d. *다음*을 선택하세요.
   e. *검토 + 할당*을 선택하세요.
   f. 추가 Azure 구독의 리소스를 관리하려면 해당 구독으로 전환한 다음 이러한 단계를 반복합니다.

Azure 서비스 주체

이전에 설정한 Azure 서비스 주체에 대한 자격 증명을 NetApp Console 제공합니다.

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *자격 증명 추가*를 선택하고 마법사의 단계를 따르세요.
   a. 자격 증명 위치: *Microsoft Azure > 에이전트*를 선택합니다.
   b. 자격 증명 정의: 필요한 권한을 부여하는 Microsoft Entra 서비스 주체에 대한 정보를 입력합니다.
      - 애플리케이션(클라이언트) ID
      - 디렉토리(테넌트) ID
      - 클라이언트 비밀번호
   c. 마켓플레이스 구독: 지금 구독하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. 검토: 새로운 자격 증명에 대한 세부 정보를 확인하고 *추가*를 선택합니다.

결과

이제 NetApp Console Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 갖게 되었습니다.

Google Cloud 서비스 계정

서비스 계정을 콘솔 에이전트 VM과 연결합니다.

단계

1. Google Cloud 포털로 이동하여 콘솔 에이전트 VM 인스턴스에 서비스 계정을 할당합니다.

   "Google Cloud 문서: 인스턴스의 서비스 계정 및 액세스 범위 변경"

2. 다른 프로젝트의 리소스를 관리하려면 해당 프로젝트에 콘솔 에이전트 역할이 있는 서비스 계정을 추가하여 액세스 권한을 부여하세요. 각 프로젝트마다 이 단계를 반복해야 합니다.

NetApp Intelligent Services 구독(제한 모드)

클라우드 공급업체의 마켓플레이스에서 NetApp Intelligent Services 구독하면 시간당 요금(PAYGO) 또는 연간 계약을 통해 데이터 서비스 비용을 지불할 수 있습니다. NetApp (BYOL)에서 라이선스를 구매한 경우 마켓플레이스 제공 서비스도 구독해야 합니다. 귀하의 라이센스 요금이 항상 먼저 청구되지만, 라이센스 용량을 초과하거나 라이센스 기간이 만료되면 시간당 요금이 청구됩니다.

마켓플레이스 구독을 통해 제한 모드로 다음 데이터 서비스에 대한 요금을 청구할 수 있습니다.

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

NetApp Data Classification 구독을 통해 활성화되지만 분류 사용에는 비용이 청구되지 않습니다.

시작하기 전에

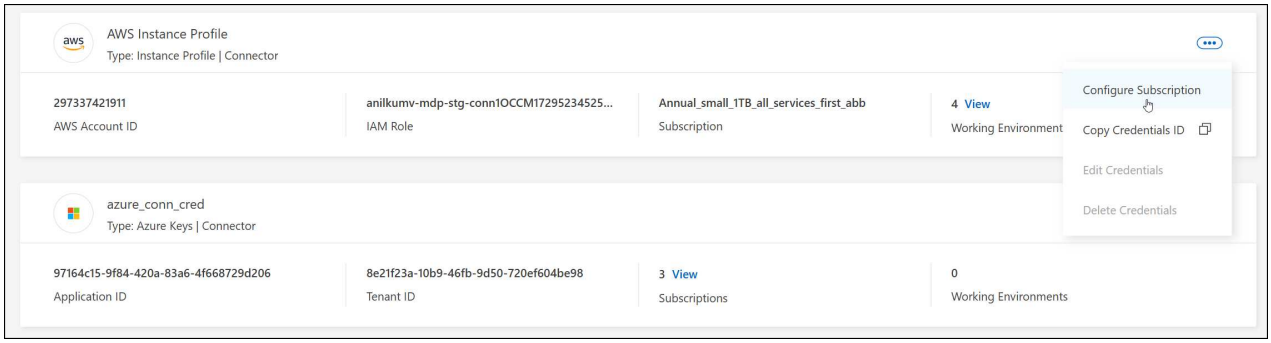
데이터 서비스를 구독하려면 콘솔 에이전트를 이미 배포했어야 합니다. 콘솔 에이전트에 연결된 클라우드 자격 증명에 마켓플레이스 구독을 연결해야 합니다.

AWS

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *조직 자격 증명*을 선택하세요.
3. 콘솔 에이전트와 연결된 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *구독 구성*을 선택합니다.

   콘솔 에이전트와 연결된 자격 증명을 선택해야 합니다. NetApp Console 과 연결된 자격 증명에는 마켓플레이스 구독을 연결할 수 없습니다.



4. 자격 증명을 기존 구독과 연결하려면 아래쪽 목록에서 구독을 선택하고 *구성*을 선택합니다.
5. 자격 증명을 새 구독과 연결하려면 *구독 추가 > 계속*을 선택하고 AWS Marketplace의 단계를 따르세요.

   a. *구매 옵션 보기*를 선택하세요.

   b. *구독*을 선택하세요.

   c. *계정 설정*을 선택하세요.

      NetApp Console 로 리디렉션됩니다.

   d. 구독 할당 페이지에서:

      - 이 구독을 연결할 콘솔 조직이나 계정을 선택하세요.
      - 기존 구독 교체 필드에서 하나의 조직 또는 계정에 대한 기존 구독을 이 새로운 구독으로 자동으로 교체할지 여부를 선택합니다.

        콘솔은 조직 또는 계정의 모든 자격 증명에 대한 기존 구독을 이 새로운 구독으로 대체합니다. 자격 증명 세트가 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

   다른 모든 조직이나 계정의 경우 이 단계를 반복하여 구독을 수동으로 연결해야 합니다.

   ◦ *저장*을 선택하세요.

하늘빛

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *조직 자격 증명*을 선택하세요.
3. 콘솔 에이전트와 연결된 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *구독 구성*을 선택합니다.

콘솔 에이전트와 연결된 자격 증명을 선택해야 합니다. NetApp Console 과 연결된 자격 증명에는 마켓플레이스 구독을 연결할 수 없습니다.

4. 자격 증명을 기존 구독과 연결하려면 아래쪽 목록에서 구독을 선택하고 *구성*을 선택합니다.
5. 자격 증명을 새 구독과 연결하려면 *구독 추가 > 계속*을 선택하고 Azure Marketplace의 단계를 따르세요.

    a. 메시지가 표시되면 Azure 계정에 로그인하세요.

    b. *구독*을 선택하세요.

    c. 양식을 작성하고 *구독*을 선택하세요.

    d. 구독 절차가 완료되면 *지금 계정 구성*을 선택하세요.

    NetApp Console 로 리디렉션됩니다.

    e. 구독 할당 페이지에서:

    - 이 구독을 연결할 콘솔 조직이나 계정을 선택하세요.
    - 기존 구독 교체 필드에서 하나의 조직 또는 계정에 대한 기존 구독을 이 새로운 구독으로 자동으로 교체할지 여부를 선택합니다.

    콘솔은 조직 또는 계정의 모든 자격 증명에 대한 기존 구독을 이 새로운 구독으로 대체합니다. 자격 증명 세트가 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

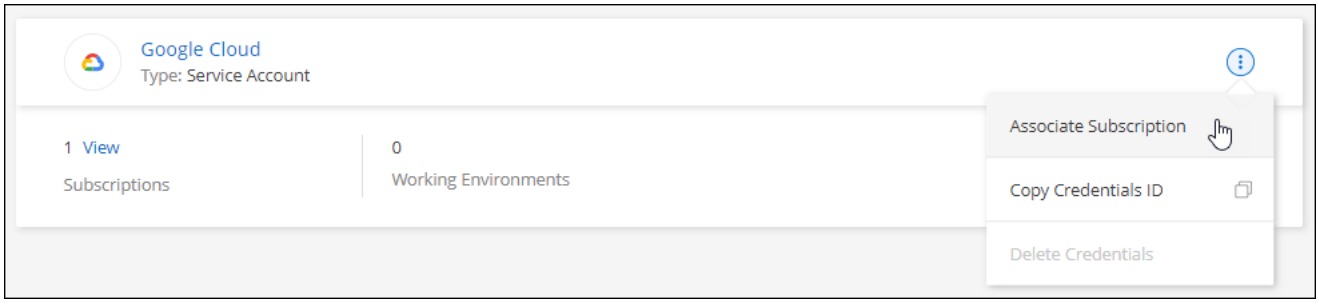
다른 모든 조직이나 계정의 경우 이 단계를 반복하여 구독을 수동으로 연결해야 합니다.

    ◦ *저장*을 선택하세요.

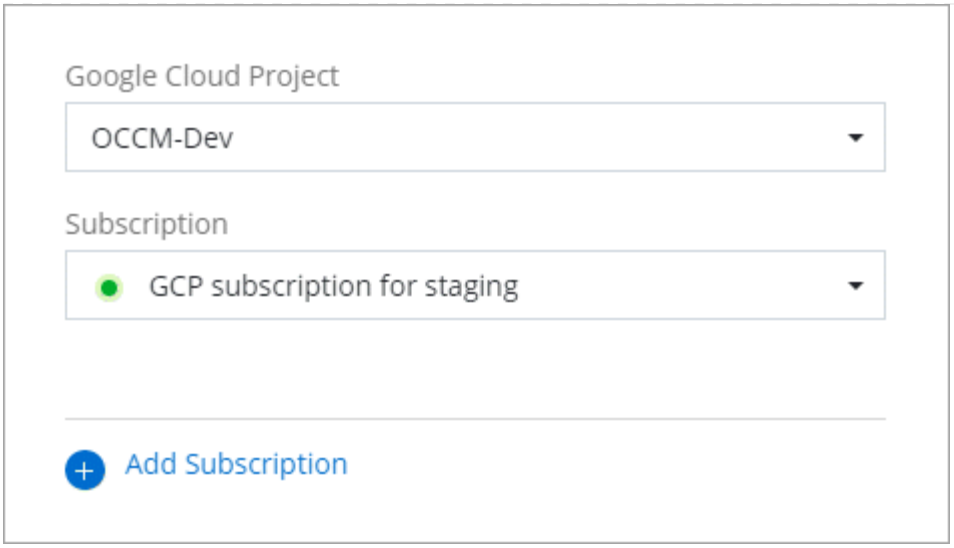
구글 클라우드

단계

1. *관리 > 자격 증명*을 선택합니다.
2. *조직 자격 증명*을 선택하세요.
3. 콘솔 에이전트와 연결된 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *구독 구성*을 선택합니다.



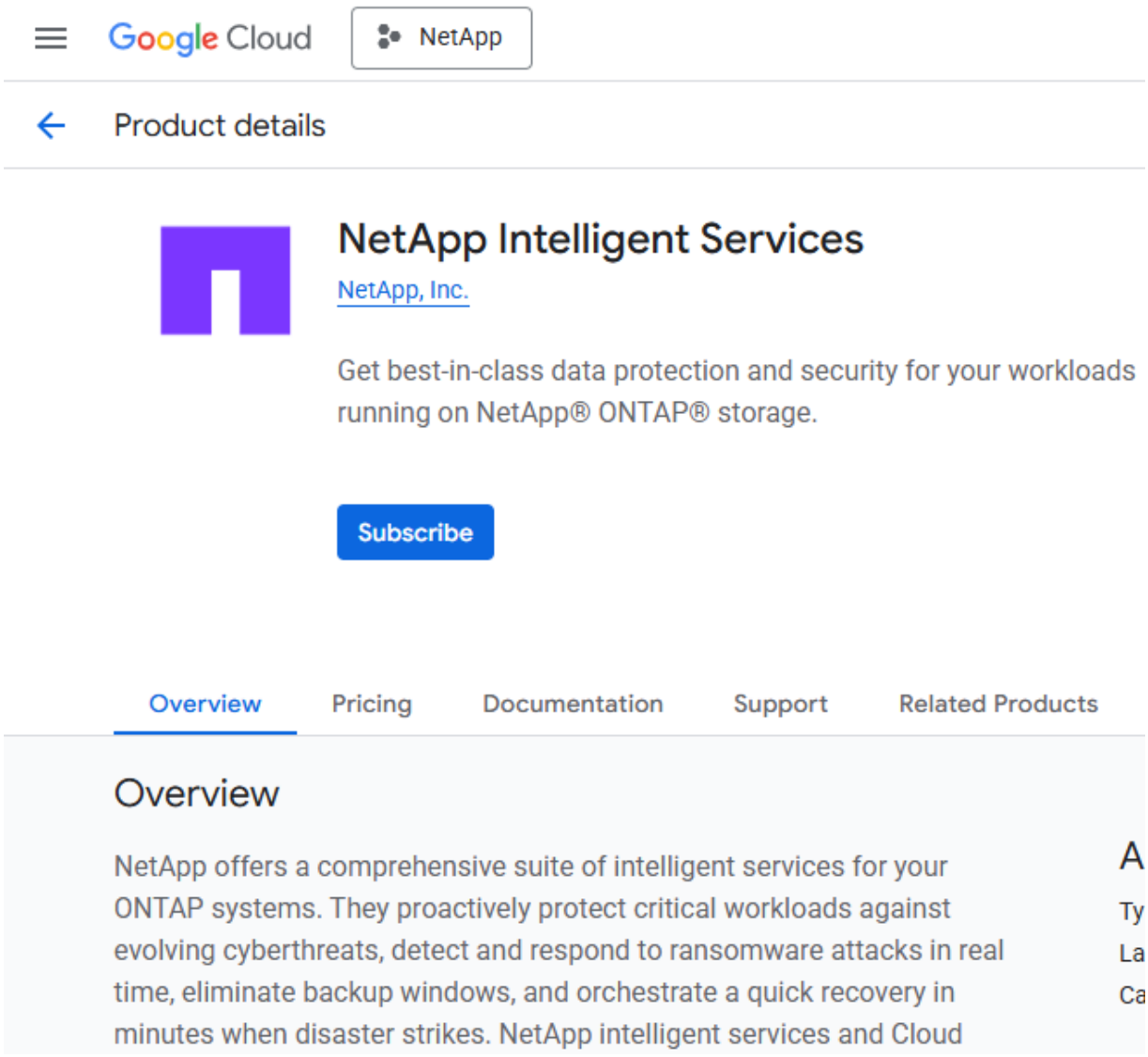
1. 선택한 자격 증명으로 기존 구독을 구성하려면 드롭다운 목록에서 Google Cloud 프로젝트와 구독을 선택한 다음 *구성*을 선택합니다.



2. 아직 구독이 없다면 *구독 추가 > 계속*을 선택하고 Google Cloud Marketplace의 단계를 따르세요.

   다음 단계를 완료하기 전에 Google Cloud 계정에서 청구 관리자 권한과 NetApp Console 로그인 권한이 모두 있는지 확인하세요.

   a. 당신이 리디렉션된 후 "Google Cloud Marketplace의 NetApp Intelligent Services 페이지" 상단 탐색 메뉴에서 올바른 프로젝트가 선택되었는지 확인하세요.



b. *구독*을 선택하세요.

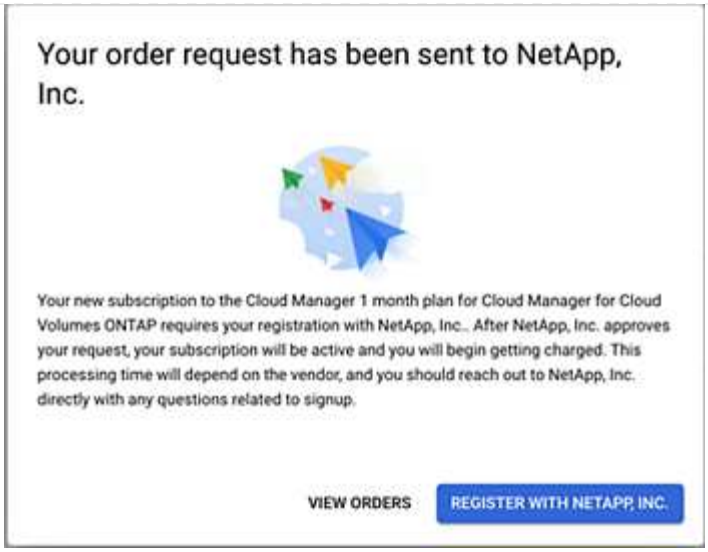
c. 적절한 청구 계정을 선택하고 약관에 동의하세요.

d. *구독*을 선택하세요.

   이 단계에서는 귀하의 전송 요청이 NetApp 으로 전송됩니다.

e. 팝업 대화 상자에서 * NetApp, Inc.에 등록*을 선택합니다.

   Google Cloud 구독을 Console 조직 또는 계정과 연결하려면 이 단계를 완료해야 합니다. 구독 연결 프로세스는 이 페이지에서 리디렉션된 후 콘솔에 로그인할 때까지 완료되지 않습니다.



f. 구독 할당 페이지의 단계를 완료하세요.

> 귀하의 조직에서 이미 귀하의 청구 계정에서 마켓플레이스 구독을 보유한 사람이 있는 경우 귀하는 다음으로 리디렉션됩니다. "NetApp Console 내 Cloud Volumes ONTAP 페이지" 대신에. 예상치 못한 상황이라면 NetApp 영업팀에 문의하세요. Google은 Google 결제 계정당 하나의 구독만 허용합니다.

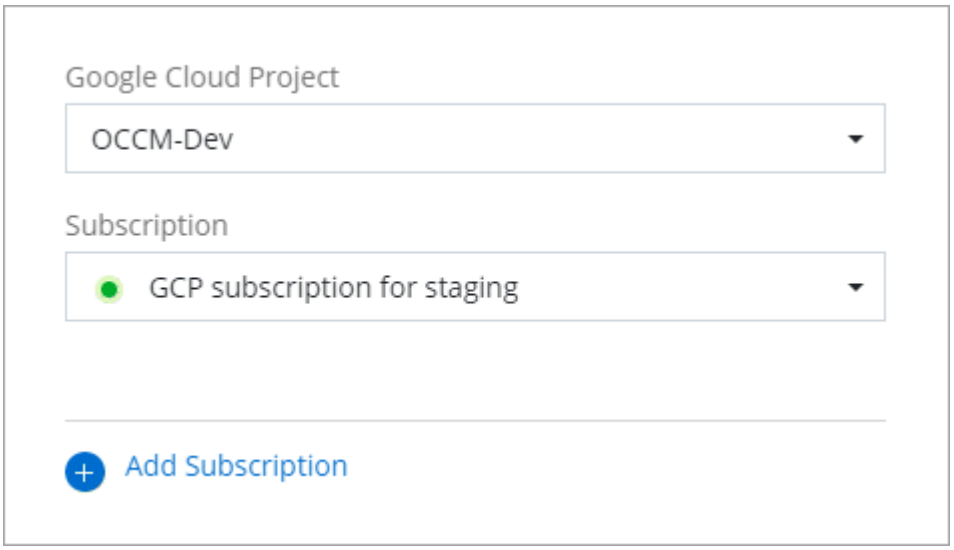
- 이 구독을 연결할 콘솔 조직을 선택하세요.
- 기존 구독 교체 필드에서 한 조직의 기존 구독을 이 새로운 구독으로 자동으로 교체할지 여부를 선택합니다.

  콘솔은 조직의 모든 자격 증명에 대한 기존 구독을 이 새로운 구독으로 대체합니다. 자격 증명 세트가 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

다른 모든 조직이나 계정의 경우 이 단계를 반복하여 구독을 수동으로 연결해야 합니다.

◦ *저장*을 선택하세요.

3. 이 프로세스가 완료되면 콘솔의 자격 증명 페이지로 돌아가서 새 구독을 선택하세요.



관련 정보

- "Cloud Volumes ONTAP 대한 BYOL 용량 기반 라이선스 관리"
- "데이터 서비스에 대한 BYOL 라이선스 관리"
- "AWS 자격 증명 및 구독 관리"
- "Azure 자격 증명 및 구독 관리"
- "Google Cloud 자격 증명 및 구독 관리"

다음에 할 수 있는 일(제한 모드)

제한 모드에서 NetApp Console 실행한 후에는 제한 모드에서 지원되는 서비스를 사용할 수 있습니다.

도움이 필요하면 다음 서비스에 대한 설명서를 참조하세요.

- "Azure NetApp Files 문서"
- "백업 및 복구 문서"
- "분류 문서"
- "Cloud Volumes ONTAP 문서"
- "디지털 지갑 문서"
- "온프레미스 ONTAP 클러스터 문서"
- "복제 문서"

관련 정보

"NetApp Console 배포 모드"

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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