커넥터를 설정합니다

Set up and administration

NetApp
July 15, 2022

목차

커넥터를 설정합니다 1
- 커넥터에 대해 자세히 알아보십시오 1
- 커넥터에 대한 네트워킹을 설정합니다 5
- Cloud Manager에서 AWS에 Connector를 생성합니다 10
- Cloud Manager에서 Azure에 Connector를 생성합니다 14
- Cloud Manager에서 Google Cloud에 Connector를 생성합니다 29

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 커넥터 가 작업 환경을 생성할 필요가 없는 경우, 볼륨 생성 및 관리, 데이터 복제, ONTAP용 FSx 를 데이터 감지 및 Cloud Sync 와 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 라이센스를 추가할 수 있습니다.

디지털 지갑에 라이센스를 추가하는 데 커넥터가 필요한 유일한 시간은 Cloud Volumes ONTAP_node-based_licenses입니다. 이 경우 Cloud Volumes ONTAP 시스템에 설치된 라이센스에서 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 계정 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 라이센스를 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 알아봅니다"
- "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
https://support.netapp.com 으로 문의하십시오	라이센스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다.

엔드포인트	목적
https://*.cloudmanager.cloud.netapp.com 으로 문의하십시오	Cloud Manager 내에서 SaaS 기능 및 서비스를 제공합니다.
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net 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 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
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

프로토콜	포트	목적
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 **Connector**에 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_ports를 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 알아봅니다".

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 사용자에 대한 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 사용자에 대한 AWS 액세스 키를 지정해야 합니다.

커넥터를 작성합니다

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

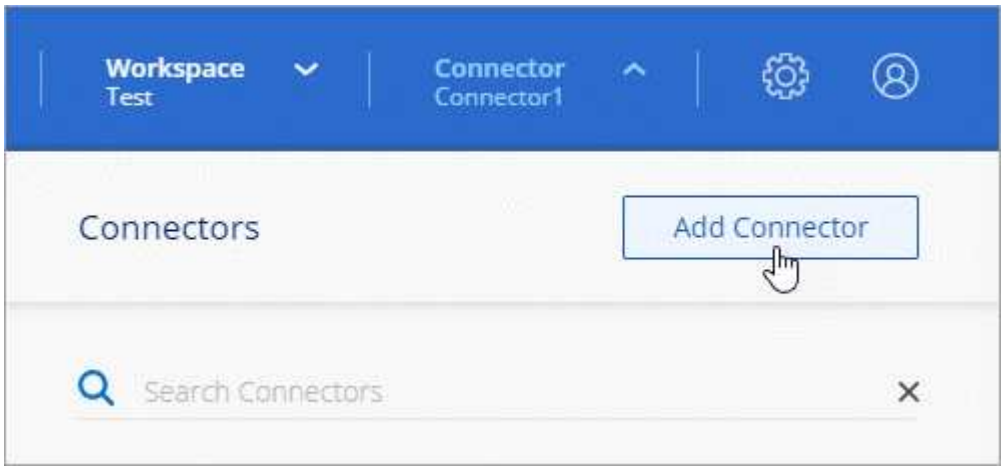
무엇을 '필요로 할거야

- 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 알아봅니다".

- * 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 알아봅니다".

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.

Azure 계정에 대한 권한을 설정합니다

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/rea
d",
        "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 *

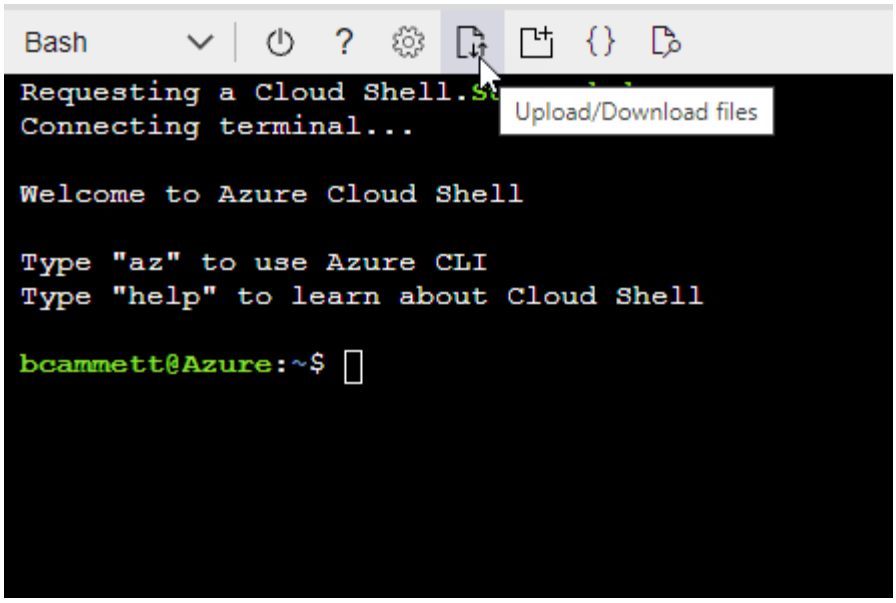
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],
```

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. Cloud Manager에서 Connector를 배포할 사용자에게 역할을 할당합니다.
   a. Subscriptions * 서비스를 열고 사용자의 구독을 선택합니다.
   b. IAM(액세스 제어) * 을 클릭합니다.
   c. 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.

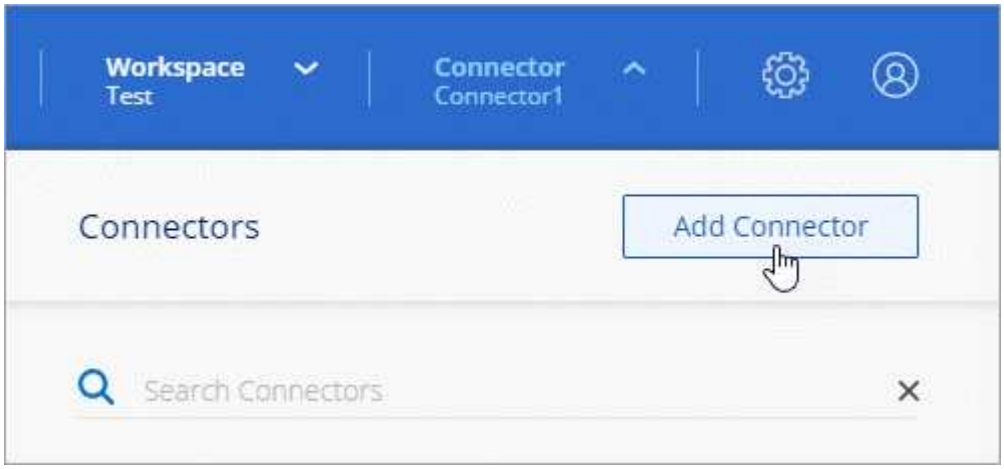
무엇을 '필요로 할거야

- 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.

> 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.

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].

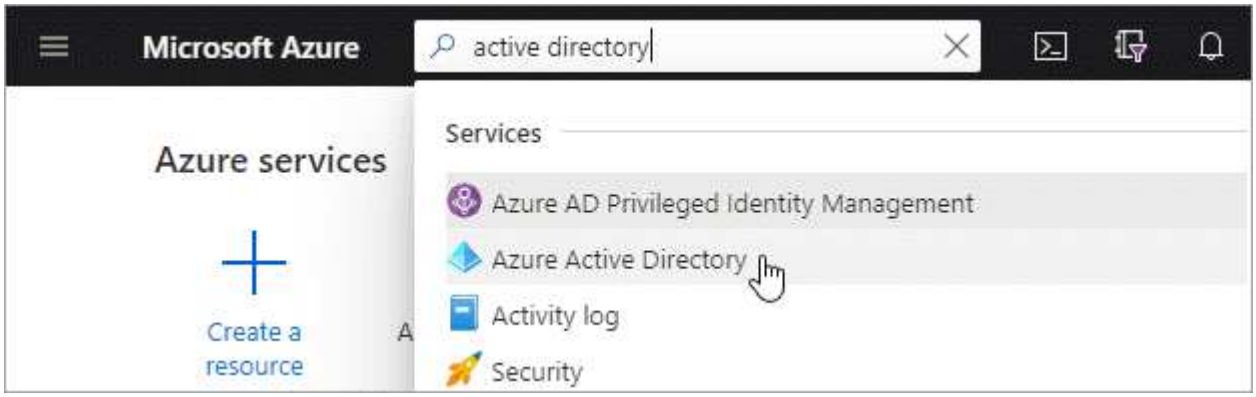
Azure Active Directory 응용 프로그램을 만듭니다

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 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.

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/rea
d",
        "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 *

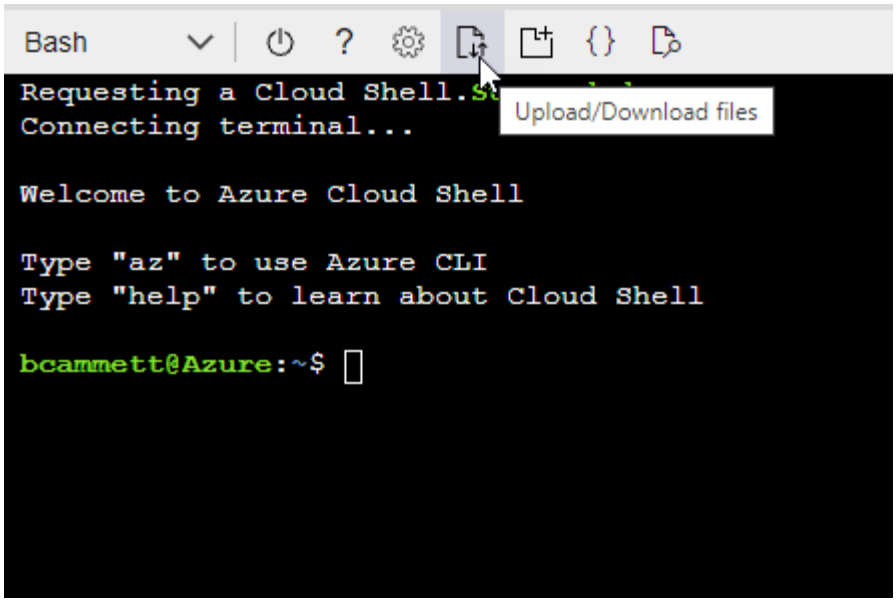
```
"AssignableScopes": [
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

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.



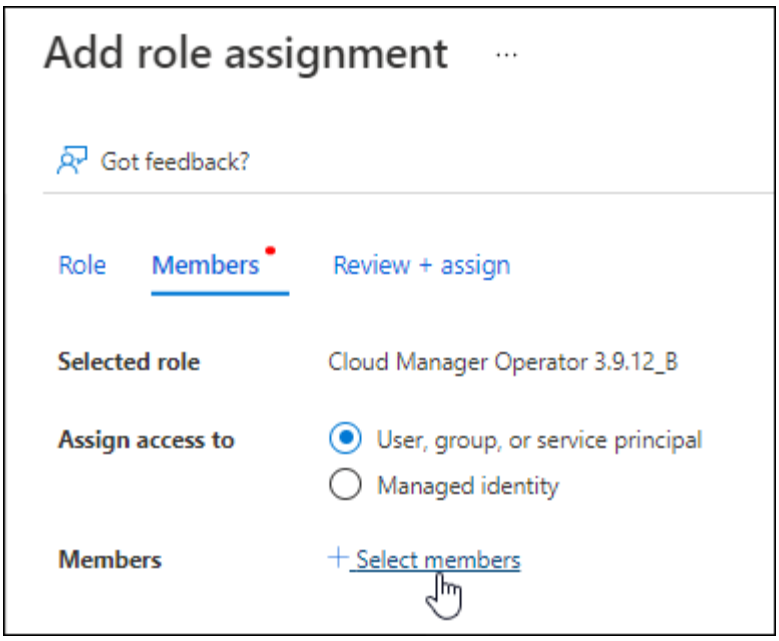
c. 다음 Azure CLI 명령을 입력합니다.

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

이제 _Azure SetupAsService_라는 사용자 지정 역할이 있어야 합니다.

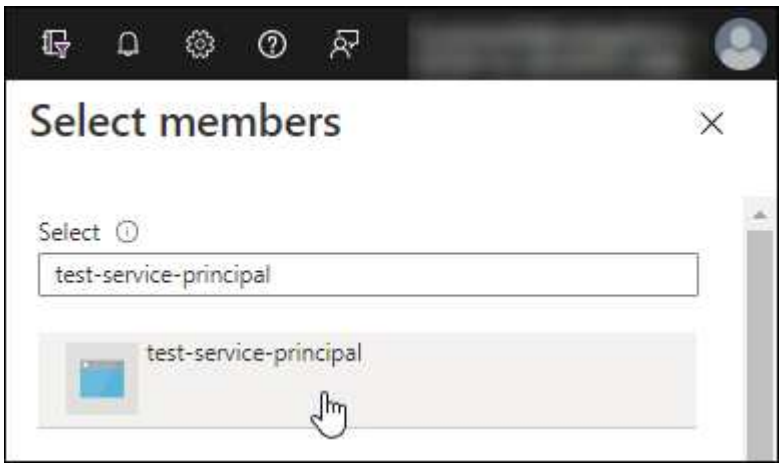
4. 역할에 응용 프로그램을 할당합니다.

   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.

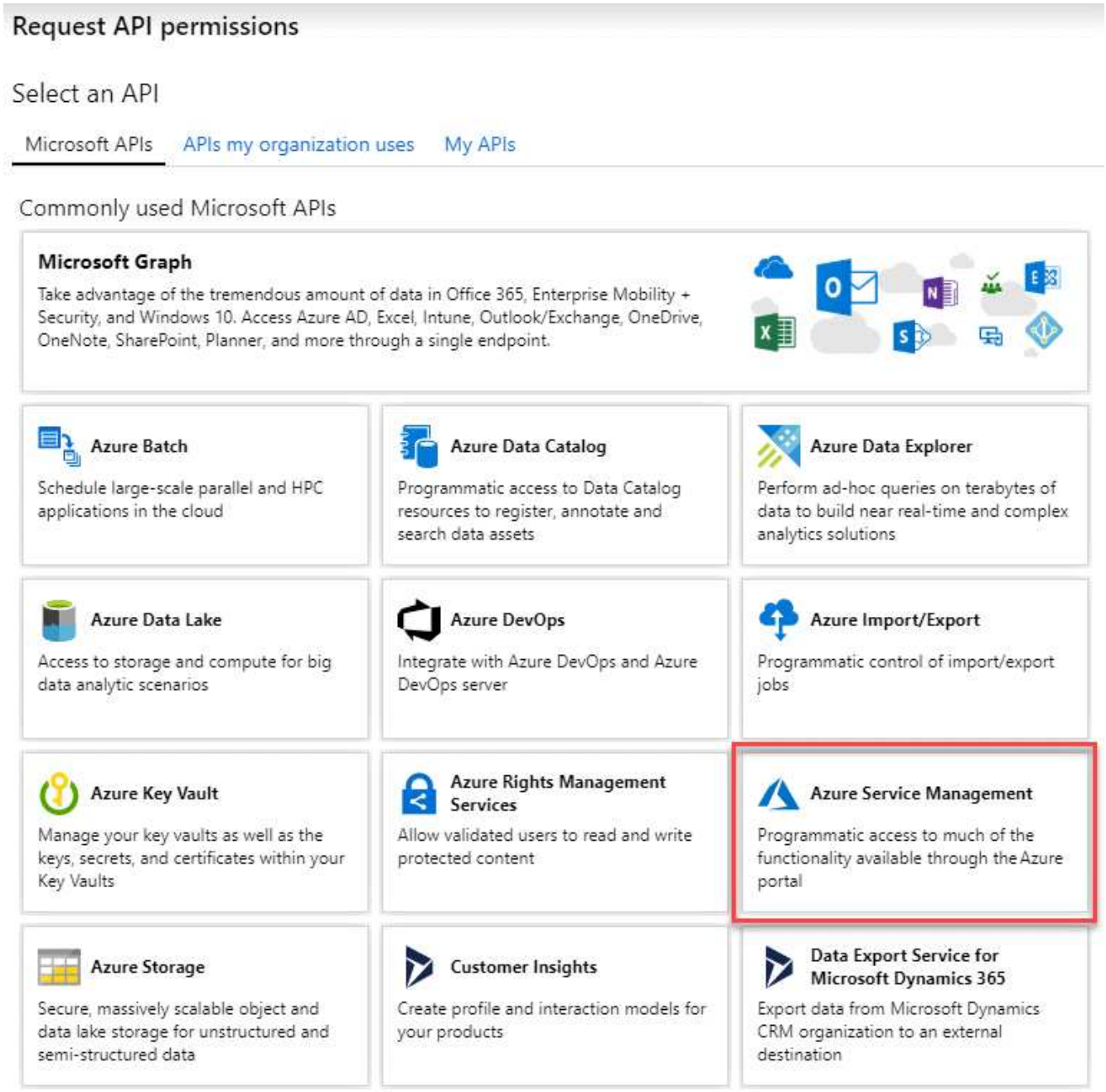
Windows Azure 서비스 관리 **API** 권한을 추가합니다

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

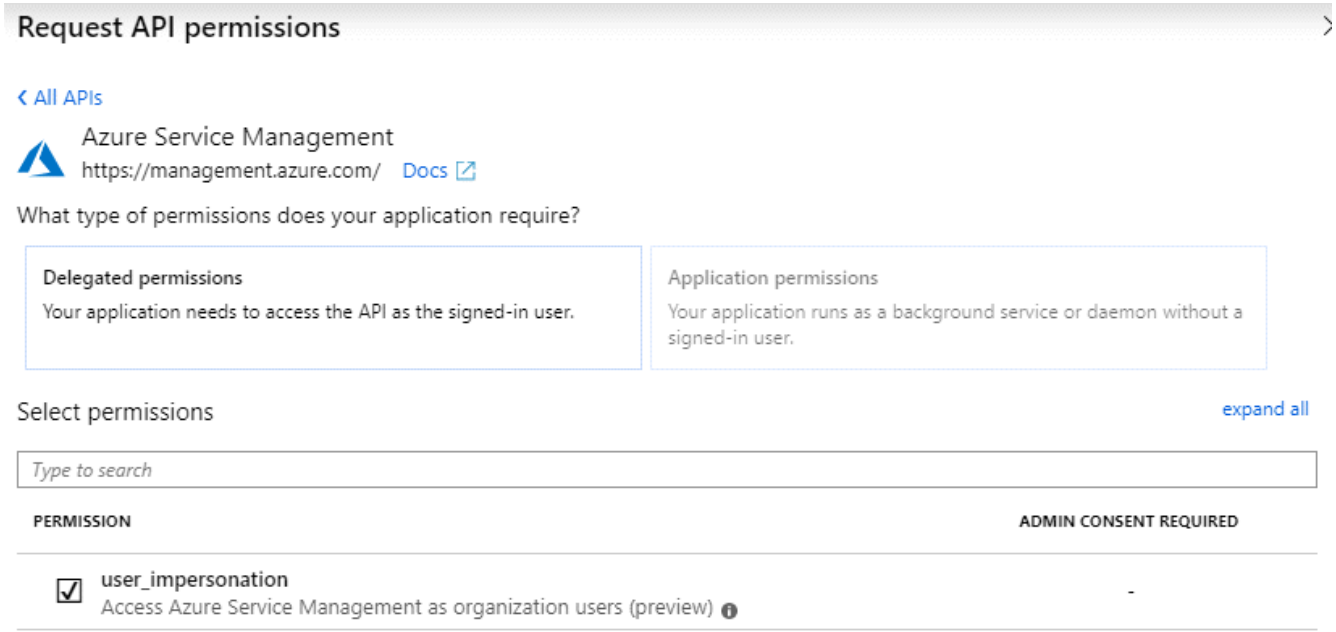
단계

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.



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

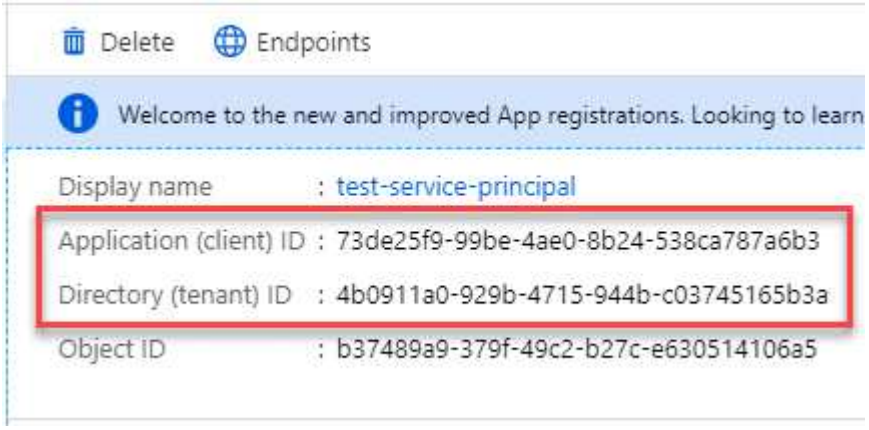


애플리케이션 **ID** 및 디렉토리 **ID**를 가져옵니다

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.

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.

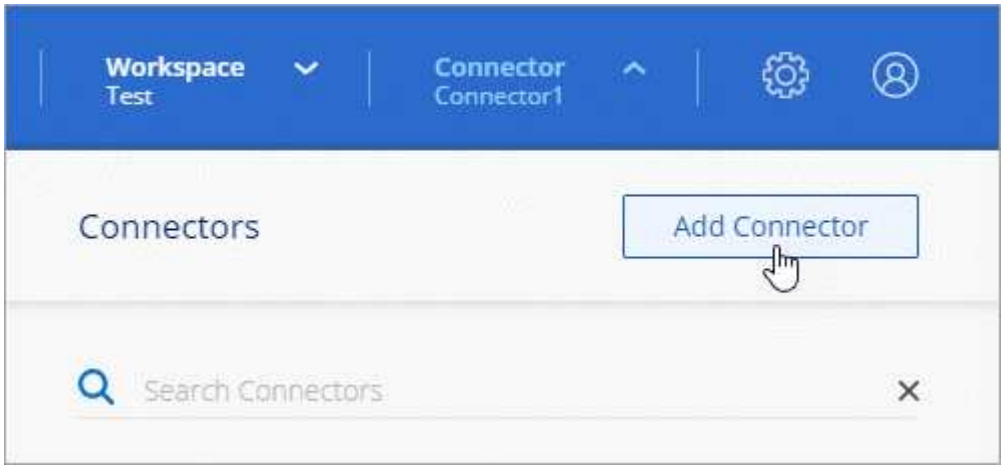
무엇을 '필요로 할거야

- 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.

     > ⓘ 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.

   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 사용자에 사용자 지정 역할을 연결합니다.

이제 Google Cloud 사용자에게 Connector를 만드는 데 필요한 권한이 있습니다.

Connector에 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 ONTAP를 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	• "위의 이 섹션에 있는 사용 권한"	• compute.networkUser	서비스 프로젝트에 Connector 배포
커넥터 서비스 계정	맞춤형	서비스 프로젝트	• "위의 이 섹션에 있는 사용 권한"	• compute.networkUser • 배포관리자.편집기	서비스 프로젝트에서 Cloud Volumes ONTAP 및 서비스를 배포 및 유지 관리합니다
Cloud Volumes ONTAP 서비스 계정입니다	맞춤형	서비스 프로젝트	• storage.admin을 선택합니다 • 회원: Cloud Manager 서비스 계정은 serviceAccount.user 입니다	해당 없음	(선택 사항) 데이터 계층화 및 Cloud Backup을 위한 솔루션
Google API 서비스 에이전트입니다	Google 클라우드	서비스 프로젝트	• (기본값) 편집기	• compute.networkUser	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

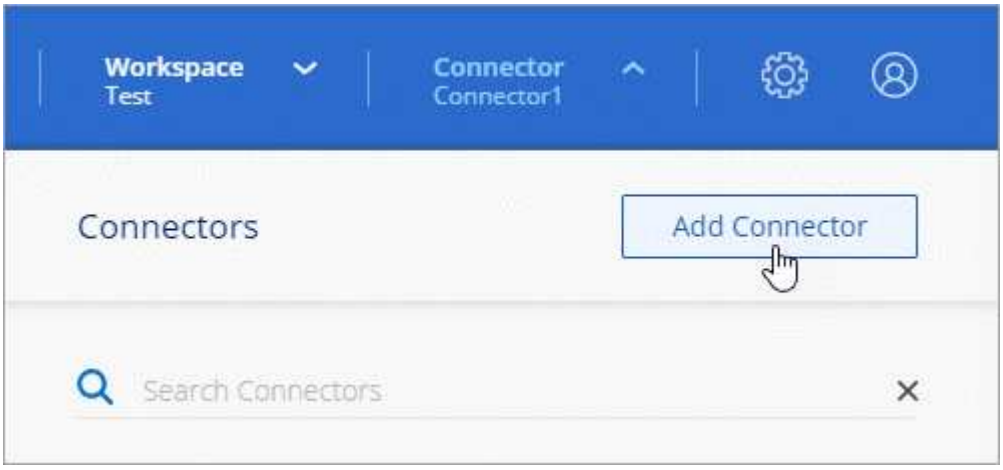
Cloud Manager 사용자 인터페이스에서 직접 또는 gcloud를 사용하여 Google Cloud에서 Connector를 생성합니다.

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 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.

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".