시작하십시오
Setup and administration

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/bluexp-setup-admin/concept-overview.html on April 24, 2024. Always check docs.netapp.com for the latest.

목차

시작하십시오 1
기본 사항 학습 1
표준 모드로 시작하십시오 22
제한된 모드로 시작하십시오 127
비공개 모드로 시작하십시오 161
BlueXP에 로그인합니다 181

시작하십시오

기본 사항 학습

BlueXP에 대해 자세히 알아보십시오

NetApp BlueXP는 사내 및 클라우드 환경 전반에서 데이터를 구축, 보호, 관리할 수 있는 단일 제어 계층을 제공합니다. BlueXP SaaS 플랫폼에는 스토리지 관리, 데이터 이동성, 데이터 보호, 데이터 분석 및 제어 기능을 제공하는 서비스가 포함됩니다. 관리 기능은 웹 기반 콘솔 및 API를 통해 제공됩니다.

피처

BlueXP 플랫폼은 스토리지, 이동성, 보호, 분석 및 제어라는 네 가지 주요 데이터 관리 기능을 제공합니다.

스토리지

AWS, Azure, Google Cloud 또는 온프레미스에 상관없이 스토리지를 검색, 구축, 관리할 수 있습니다.

- 설정 및 사용 "Cloud Volumes ONTAP" 클라우드 전반에서 효율적인 멀티 프로토콜 데이터 관리
- 클라우드 파일 스토리지 서비스 설정 및 사용:
  - "Azure NetApp Files"
  - "ONTAP용 Amazon FSx"
  - "Google Cloud용 Cloud Volumes Service"
- 검색 및 관리 "높지 않습니다":
  - E-Series 시스템
  - ONTAP 클러스터
  - StorageGRID 시스템

이동성

데이터를 동기화, 복사, 계층화 및 캐싱하여 필요한 위치로 데이터를 이동합니다.

- "복사 및 동기화"
- "에지 캐싱"
- "계층화"

보호

자동화된 보호 메커니즘을 사용하여 데이터 손실, 계획되지 않은 운영 중단, 랜섬웨어 및 기타 사이버 위협으로부터 데이터를 보호합니다.

- "백업 및 복구"
- "복제"
- "Kubernetes 워크로드의 데이터 보호"

분석 및 제어

툴을 사용하여 데이터 스토리지 및 인프라를 모니터링, 매핑 및 최적화할 수 있습니다. 실행 가능한 인텔리전스를 확보하여 스토리지 상태, 복원력 및 경제성을 최적화합니다.

- "분류"
- "디지털 자문업체"
- "경제적인 효율성"
- "운영 복원력"

"BlueXP를 사용하여 조직에 도움을 주는 방법에 대해 자세히 알아보십시오"

지원되는 클라우드 공급자

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

비용

BlueXP의 가격은 사용할 서비스에 따라 다릅니다. "BlueXP 가격에 대해 알아보십시오"

BlueXP의 작동 방식

BlueXP에는 SaaS 계층을 통해 제공되는 웹 기반 콘솔, 멀티 테넌시를 제공하는 계정 및 작업 환경을 관리하고 BlueXP 클라우드 서비스를 지원하는 커넥터가 포함되어 있습니다.

서비스형 소프트웨어

BlueXP는 을 통해 액세스할 수 있습니다 "웹 기반 콘솔" API를 사용해 보십시오. 이 SaaS 환경을 통해 최신 기능이 릴리스될 때 자동으로 액세스할 수 있으며 BlueXP 계정과 커넥터 간에 쉽게 전환할 수 있습니다.

BlueXP 계정

BlueXP에 처음 로그인하면 _BlueXP 계정 _ 을(를) 생성하라는 메시지가 나타납니다. 이 계정은 다중 테넌시를 제공하며 사용자가 isolated_worksaces_에서 사용자 및 리소스를 구성할 수 있도록 합니다.

"어카운트에 대해 자세히 알아보십시오".

커넥터

BlueXP를 시작하기 위해 커넥터가 필요하지 않지만 모든 BlueXP 기능 및 서비스를 잠금 해제하려면 커넥터를 만들어야 합니다. Connector를 사용하면 사내 환경과 클라우드 환경 전반에서 리소스와 프로세스를 관리할 수 있습니다. 작업 환경(예: Cloud Volumes ONTAP 및 온프레미스 ONTAP 클러스터)을 관리하고 여러 BlueXP 데이터 서비스를 사용해야 합니다.

"커넥터에 대해 자세히 알아보십시오".

제한된 모드 및 비공개 모드

BlueXP는 보안 및 연결 제한이 있는 환경에서도 지원됩니다. _restricted mode_or_private mode_를 사용하여 BlueXP SaaS 계층에 대한 아웃바운드 연결을 제한할 수 있습니다.

"BlueXP 배포 모드에 대해 자세히 알아보십시오".

SOC 2 Type 2 인증

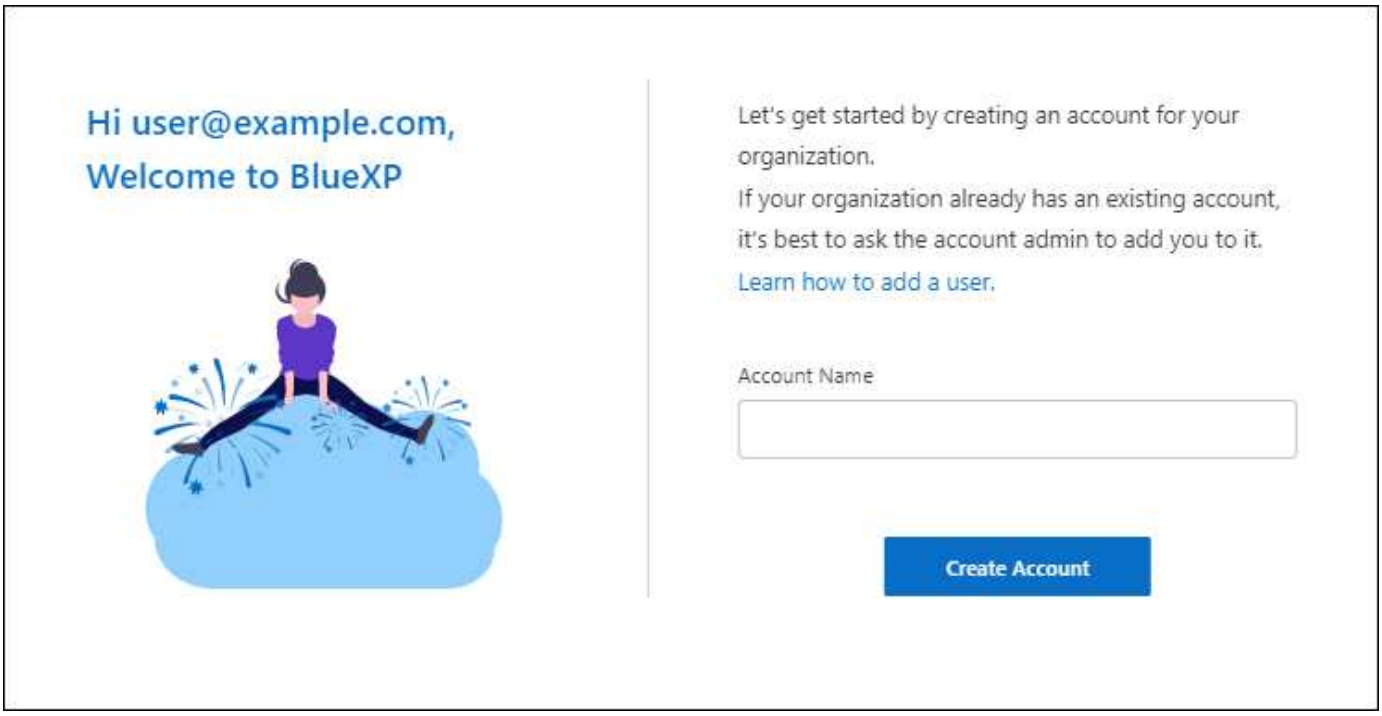
독립적인 공인회계사 및 서비스 감사원이 BlueXP를 조사하여 해당 신뢰 서비스 기준에 따라 SOC 2 Type 2 보고서를 획득하였다는 것을 확인했습니다.

"NetApp의 SOC 2 보고서 보기"

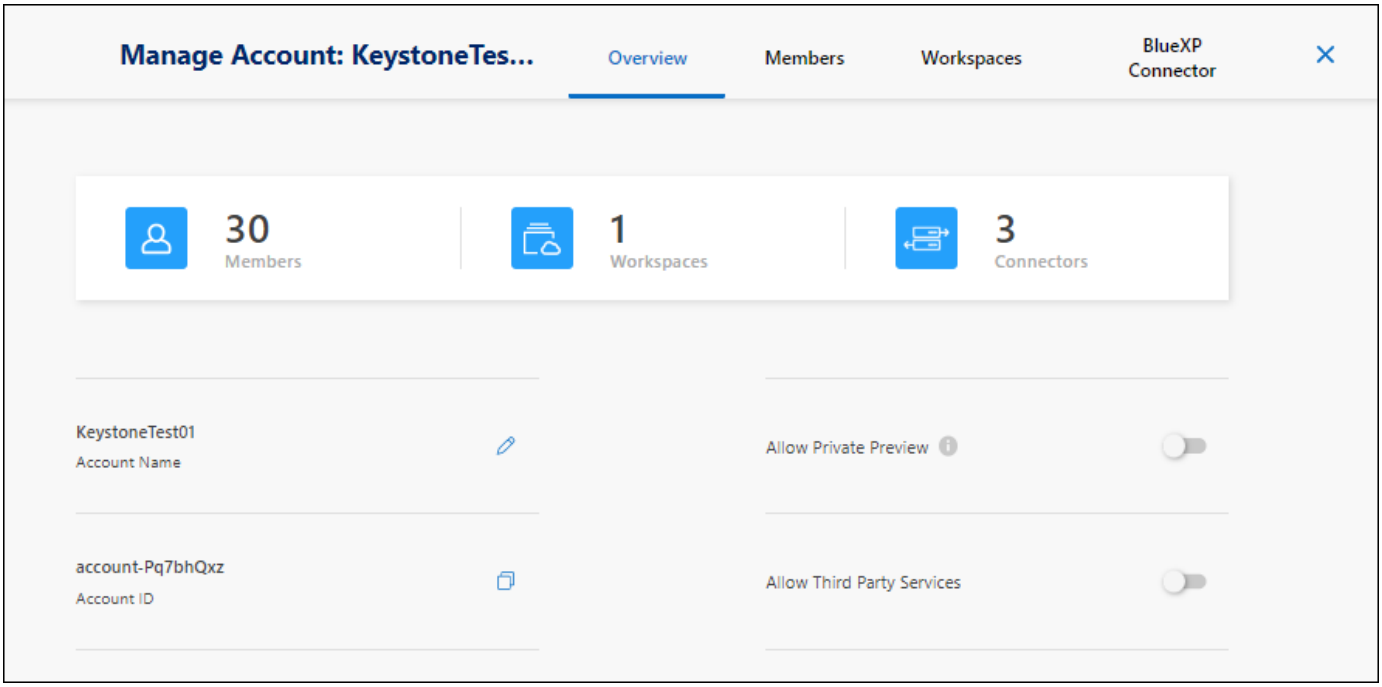
BlueXP 계정에 대해 알아보십시오

BlueXP 계정 _ 은(는) 조직에 멀티 테넌시를 제공하므로 사용자는 이를 통해 격리된_작업 공간 _ 에서 사용자와 리소스를 구성할 수 있습니다. 예를 들어 사용자 그룹은 다른 작업 영역에서 작업 환경을 관리하는 사용자에게 표시되지 않는 작업 영역에서 Cloud Volumes ONTAP 작업 환경을 배포하고 관리할 수 있습니다.

BlueXP에 처음 액세스하면 계정을 선택하거나 생성하라는 메시지가 표시됩니다. 예를 들어 아직 계정이 없는 경우 다음 화면이 표시됩니다.



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



"BlueXP 계정 관리 방법에 대해 알아보십시오".

배포 모드

BlueXP는 표준 모드, 제한된 모드 및 비공개 모드 등 계정에 대해 다음과 같은 배포 모드를 제공합니다. 이러한 모드는 다양한 수준의 보안 및 연결 제한을 가진 환경을 지원합니다.

"BlueXP 배포 모드에 대해 자세히 알아보십시오".

구성원

회원은 BlueXP 계정과 연결된 BlueXP 사용자입니다. 사용자와 계정 및 해당 계정의 하나 이상의 작업 영역을 연결하면 해당 사용자가 BlueXP에서 작업 환경을 만들고 관리할 수 있습니다.

사용자를 연결할 때 역할을 할당합니다.

- 계정 관리자: BlueXP에서 모든 작업을 수행할 수 있습니다.
- *Workspace* 관리자: 할당된 작업 영역에서 자원을 작성하고 관리할 수 있습니다.
- *Compliance Viewer*: BlueXP 분류에 대한 규정 준수 정보만 볼 수 있고 액세스 권한이 있는 작업 영역에 대한 보고서를 생성할 수 있습니다.

"이러한 역할에 대해 자세히 알아보십시오".

작업 공간

BlueXP에서 작업 영역은 계정의 다른 사용자와 모든 _ 작업 환경 _ 을(를) 격리합니다. 계정 관리자가 해당 작업 영역에 관리자를 연결해야만 작업 영역 관리자가 작업 영역의 작업 환경에 액세스할 수 있습니다.

작업 환경은 스토리지 시스템을 나타냅니다. 예를 들면 다음과 같습니다.

- Cloud Volumes ONTAP 시스템

- 사내 ONTAP 클러스터
- Kubernetes 클러스터

"작업 영역을 추가하는 방법에 대해 알아봅니다".

커넥터

Connector는 데이터 인프라를 관리하기 위해 BlueXP에서 수행해야 하는 작업을 실행합니다. Connector는 클라우드 공급자 또는 구성한 온프레미스 호스트에 배포하는 가상 머신 인스턴스에서 실행됩니다.

하나 이상의 BlueXP 서비스에 커넥터를 사용할 수 있습니다. 예를 들어, 커넥터를 사용하여 Cloud Volumes ONTAP를 관리하는 경우 BlueXP 계층화와 같은 다른 서비스와 동일한 커넥터를 사용할 수 있습니다.

"커넥터에 대해 자세히 알아보십시오".

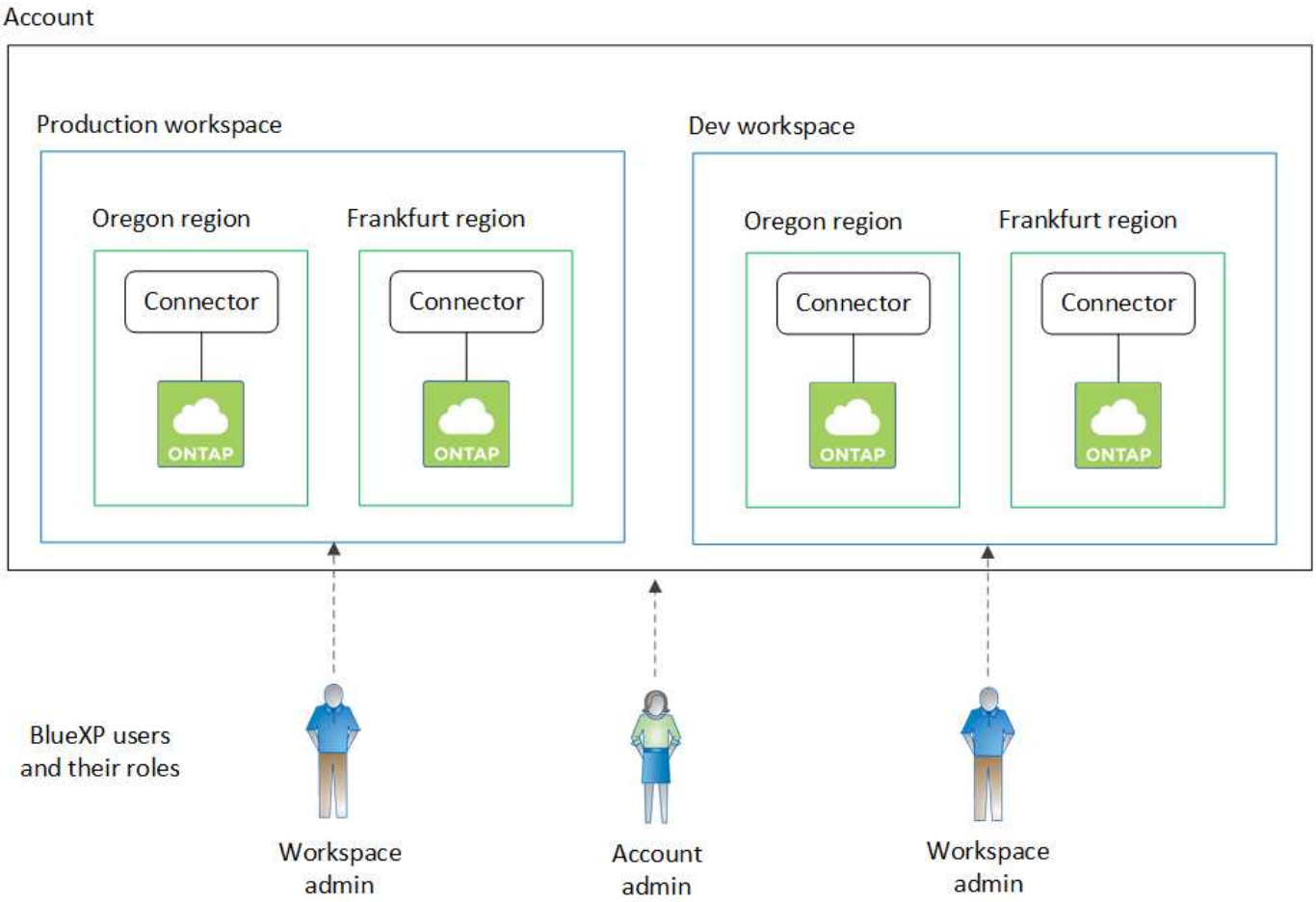
예

다음 예에서는 계정을 설정하는 방법을 보여 줍니다.

> 다음에 나오는 두 예제 이미지에서 Connector와 Cloud Volumes ONTAP 시스템은 BlueXP 계정 _ 에 실제로 상주하지 않습니다. 이러한 이미지는 클라우드 공급자에서 실행되고 있습니다. 각 구성 요소 간의 관계를 개념적으로 나타낸 것입니다.

여러 작업 공간

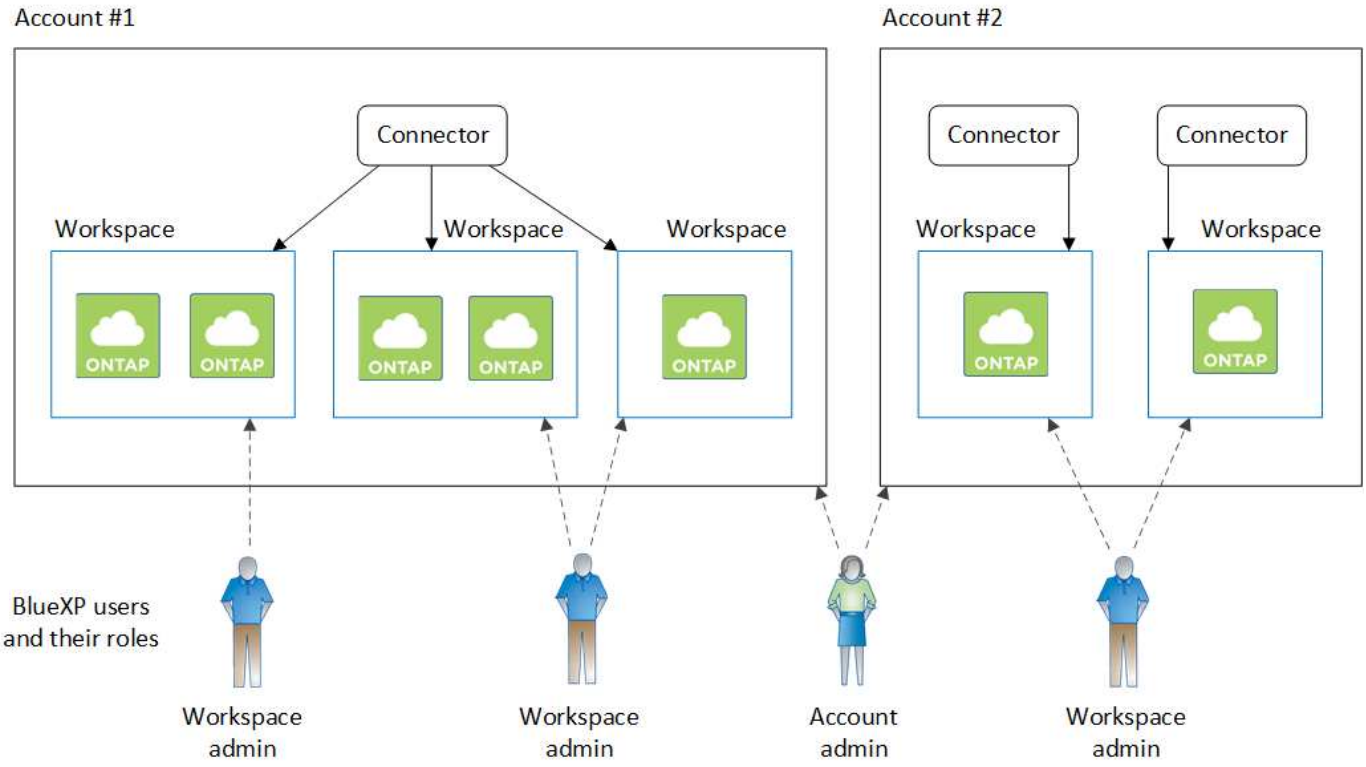
다음 예제에서는 두 개의 작업 영역을 사용하여 격리된 환경을 만드는 계정을 보여 줍니다. 첫 번째 작업 공간은 운영 환경이고 두 번째는 개발 환경입니다.



여러 계정

다음은 두 개의 개별 BlueXP 계정을 사용하여 가장 높은 수준의 멀티 테넌시를 보여 주는 또 다른 예입니다. 예를 들어, 서비스 제공업체는 한 계정에서 BlueXP를 사용하여 고객에게 서비스를 제공하는 한편 다른 계정을 사용하여 해당 사업부 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.



커넥터에 대해 자세히 알아보십시오

A_Connector _ 는 클라우드 네트워크 또는 사내 네트워크에서 실행되는 NetApp 소프트웨어입니다. 데이터 인프라를 관리하기 위해 BlueXP에서 수행해야 하는 작업을 실행합니다. Connector는 수행해야 하는 작업에 대해 BlueXP SaaS 레이어를 지속적으로 폴링합니다. BlueXP를 시작하기 위해 커넥터가 필요하지 않지만 모든 BlueXP 기능 및 서비스를 잠금 해제하려면 커넥터를 만들어야 합니다.

커넥터 없이 수행할 수 있는 작업

BlueXP를 시작하기 위해 커넥터가 필요하지 않습니다. Connector를 만들지 않고도 BlueXP 내에서 여러 기능 및 서비스를 사용할 수 있습니다.

커넥터 없이 다음 BlueXP 기능 및 서비스를 사용할 수 있습니다.

- NetApp ONTAP 작업 환경 생성을 위한 Amazon FSx

  Connector는 작업 환경을 만드는 데 필요하지 않지만 볼륨 생성 및 관리, 데이터 복제, ONTAP용 FSx를 BlueXP 분류 및 BlueXP 복사 및 동기화 등의 서비스와 통합해야 합니다.

- 자동화 카탈로그
- Azure NetApp Files

  Azure NetApp Files를 설정하고 관리하는 데 커넥터가 필요하지 않지만 Azure NetApp Files 데이터를 스캔하기 위해 BlueXP 분류를 사용하려면 커넥터가 필요합니다.

- Google Cloud용 Cloud Volumes Service

- 복사 및 동기화
- 디지털 자문업체
- 디지털 지갑

  거의 모든 경우 커넥터 없이 디지털 지갑에 라이센스를 추가할 수 있습니다.

  디지털 지갑에 라이센스를 추가하는 데 Connector가 필요한 유일한 시간은 Cloud Volumes ONTAP_node-based_licenses입니다. 이 경우 Cloud Volumes ONTAP 시스템에 설치된 라이센스에서 데이터를 가져왔기 때문에 커넥터가 필요합니다.

- 사내 ONTAP 클러스터를 직접 검색

  사내 ONTAP 클러스터를 직접 검색하는 데는 커넥터가 필요하지 않지만 추가 BlueXP 기능을 사용하려면 커넥터가 필요합니다.

  "온프레미스 ONTAP 클러스터를 위한 검색 및 관리 옵션에 대해 자세히 알아보십시오"

- 지속 가능성

커넥터가 필요한 경우

표준 모드에서 BlueXP를 사용하는 경우 BlueXP의 다음 기능 및 서비스에 커넥터가 필요합니다.

- ONTAP용 Amazon FSx 관리 기능
- Amazon S3 스토리지
- Azure Blob 저장소
- 백업 및 복구
- 분류
- Cloud Volumes ONTAP
- 재해 복구
- E-Series 시스템
- 경제 효율성 [1]
- 에지 캐싱
- Google Cloud Storage 버킷
- Kubernetes 클러스터
- 마이그레이션 보고서
- BlueXP 데이터 서비스와 사내 ONTAP 클러스터 통합
- 작업 복구 [1]
- 랜섬웨어 보호
- StorageGRID 시스템
- 계층화
- 볼륨 캐싱

[1] 커넥터 없이 이러한 서비스에 액세스할 수 있는 동안 서비스에서 작업을 시작하려면 Connector가 필요합니다.

BlueXP가 제한된 모드 또는 프라이빗 모드로 사용하려면 커넥터가 필요합니다.

커넥터는 항상 작동해야 합니다

커넥터는 BlueXP 서비스 아키텍처의 기본 부분입니다. 관련 커넥터가 항상 가동, 작동 및 액세스 가능한지 확인하는 것은 귀하의 책임입니다. 이 서비스는 커넥터 가용성의 짧은 중단을 극복하도록 설계되었지만, 인프라 장애를 해결하기 위해 필요한 경우 즉각적인 조치를 취해야 합니다.

이 문서는 EULA의 적용을 받습니다. 문서에 따라 제품을 작동하지 않는 경우 제품의 기능 및 작동, EULA에 따른 사용자의 권리에 부정적인 영향을 미칠 수 있습니다.

Cloud Volumes ONTAP에 미치는 영향

커넥터는 Cloud Volumes ONTAP의 상태 및 작동에 있어 중요한 구성요소입니다. 커넥터가 꺼져 있는 경우, Cloud Volumes ONTAP PAYGO 시스템 및 용량 기반 BYOL 시스템은 커넥터와 14일 이상 통신이 두절 이상 끊긴 후 종료됩니다. 이는 Connector가 매일 시스템의 라이센스를 갱신하기 때문에 발생합니다.

Cloud Volumes ONTAP 시스템에 노드 기반 BYOL 라이센스가 있는 경우 Cloud Volumes ONTAP 시스템에 라이센스가 설치되므로 시스템이 14일 후에도 계속 실행됩니다.

지원되는 위치

커넥터는 다음 위치에서 지원됩니다.

- Amazon Web Services에서 직접 지원합니다
- Microsoft Azure를 참조하십시오

  Azure의 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"

- Google 클라우드

  Google Cloud에서 BlueXP 서비스를 사용하려면 Google Cloud에서 실행되는 Connector를 사용해야 합니다.

- 온프레미스

제한된 모드 및 비공개 모드

제한된 모드 또는 비공개 모드에서 BlueXP를 사용하려면 Connector를 설치한 다음 Connector에서 로컬로 실행되는 사용자 인터페이스에 액세스하여 BlueXP를 시작합니다.

"BlueXP 배포 모드에 대해 알아보십시오".

커넥터 작성 방법

BlueXP 계정 관리자는 BlueXP, 클라우드 공급자의 마켓플레이스에서 직접 커넥터를 만들거나, 자체 Linux 호스트에 소프트웨어를 수동으로 설치할 수 있습니다. 표준 모드, 제한 모드 또는 비공개 모드에서 BlueXP를 사용하고 있는지 여부에 따라 시작 방법이 달라집니다.

- "BlueXP 배포 모드에 대해 알아보십시오"
- "표준 모드에서 BlueXP를 시작하십시오"
- "제한된 모드에서 BlueXP를 시작하십시오"
- "프라이빗 모드에서 BlueXP를 시작하십시오"

권한

BlueXP에서 직접 Connector를 만들려면 특정 권한이 필요하며 Connector 인스턴스 자체에 다른 권한 집합이 필요합니다. BlueXP에서 직접 AWS 또는 Azure에서 커넥터를 생성하는 경우 BlueXP는 필요한 권한으로 Connector를 생성합니다.

표준 모드에서 BlueXP를 사용할 때 사용 권한을 제공하는 방법은 Connector를 생성하는 계획에 따라 다릅니다.

사용 권한을 설정하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- 표준 모드
  - "AWS의 커넥터 설치 옵션"
  - "Azure의 커넥터 설치 옵션"
  - "Google Cloud의 커넥터 설치 옵션"
  - "온프레미스 구축을 위한 클라우드 권한 설정"
- "제한된 모드에 대한 권한을 설정합니다"
- "비공개 모드에 대한 권한을 설정합니다"

Connector에 일상적인 작업에 필요한 정확한 사용 권한을 보려면 다음 페이지를 참조하십시오.

- "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. BlueXP 플랫폼의 서비스 및 기능은 대부분 SaaS 기반 소프트웨어를 통해 제공되지만 커넥터 버전에 따라 몇 가지 기능이 달라집니다. 여기에는 Cloud Volumes ONTAP 관리, 온프레미스 ONTAP 클러스터 관리, 설정 및 도움말이 포함됩니다.

표준 모드 또는 제한된 모드에서 BlueXP를 사용할 경우, 소프트웨어 업데이트를 받을 수 있도록 아웃바운드 인터넷에 액세스할 수 있는 경우 Connector에서 소프트웨어를 자동으로 최신 버전으로 업데이트합니다. 비공개 모드에서 BlueXP를 사용하는 경우 커넥터를 수동으로 업그레이드해야 합니다.

"Connector 소프트웨어를 수동으로 업그레이드하는 방법에 대해 알아보십시오".

운영 체제 및 **VM** 유지 보수

커넥터 호스트에서 운영 체제를 유지 관리하는 것은 사용자의 책임입니다. 예를 들어, 회사의 운영 체제 배포 표준 절차에 따라 Connector 호스트의 운영 체제에 보안 업데이트를 적용해야 합니다.

OS 업데이트를 실행할 때 커넥터 호스트에서 서비스를 중지할 필요가 없습니다.

Connector VM을 중지한 다음 시작해야 하는 경우, 클라우드 공급자의 콘솔에서 또는 온프레미스 관리를 위한 표준 절차를 사용하여 시작해야 합니다.

커넥터는 항상 작동해야 합니다.

다양한 작업 환경

커넥터는 BlueXP에서 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.

다중 커넥터

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

다음은 몇 가지 예입니다.

- 다중 클라우드 환경(예: AWS 및 Azure)이 있고 AWS에 커넥터 1개와 Azure에 커넥터 1개가 있는 것을 선호합니다. 각 는 이러한 환경에서 실행되는 Cloud Volumes ONTAP 시스템을 관리합니다.
- 서비스 제공업체는 하나의 BlueXP 계정을 사용하여 고객에게 서비스를 제공하는 한편 다른 계정을 사용하여 사업부 중 하나의 재해 복구를 제공할 수 있습니다. 각 계정에는 별도의 커넥터가 있습니다.

전환 시기

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

"커넥터 간 전환 방법에 대해 알아보십시오".

재해 복구

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 BlueXP에 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.

BlueXP 배포 모드에 대해 알아보십시오

BlueXP는 비즈니스 및 보안 요구 사항을 충족하는 방식으로 BlueXP를 사용할 수 있는 다중 배포 모드 _ 를 제공합니다. 표준 모드 는 BlueXP SaaS 계층을 활용하여 모든 기능을 제공하며, 연결 제한이 있는 조직에서는 *restricted mode* 및 _private mode_를 사용할 수 있습니다.

BlueXP는 제한된 모드 또는 비공개 모드를 사용할 때 트래픽, 통신 및 데이터의 흐름을 억제하지만, 필요한 규정을 준수하는 환경(온프레미스 및 클라우드)을 유지하는 것은 사용자의 책임입니다.

개요

BlueXP는 계정에 다음과 같은 배포 모드를 제공합니다. 각 모드는 아웃바운드 연결 요구 사항, 배포 위치, 설치 프로세스, 인증 방법, 사용 가능한 데이터 및 스토리지 서비스, 충전 방법 측면에서 다릅니다.

표준 모드

BlueXP는 웹 기반 콘솔에서 클라우드 서비스로 액세스할 수 있습니다. 사용할 BlueXP 서비스에 따라 BlueXP 관리자는 하나 이상의 커넥터를 만들어 하이브리드 클라우드 환경 내에서 데이터를 관리합니다.

이 모드는 공용 인터넷을 통한 암호화된 데이터 전송을 사용합니다.

제한된 모드

BlueXP Connector는 정부 지역, 주권 클라우드 지역 또는 상업 지역의 클라우드에 설치되며 BlueXP SaaS 계층에 대한 아웃바운드 연결이 제한됩니다. 사용자는 SaaS 계층이 아닌 Connector에서 사용할 수 있는 웹 기반 콘솔에서 로컬로 BlueXP에 액세스합니다.

이 모드는 일반적으로 주 및 지방 정부와 규제 대상 기업에서 사용합니다.

SaaS 계층에 대한 아웃바운드 연결에 대해 자세히 알아보십시오.

비공개 모드

BlueXP Connector는 사내 또는 클라우드(보안 지역, 주권 클라우드 지역 또는 상업 지역)에 설치되며 BlueXP SaaS 계층에 _NO_를 연결할 수 있습니다. 사용자는 SaaS 계층이 아닌 Connector에서 사용할 수 있는 웹 기반 콘솔에서 로컬로 BlueXP에 액세스합니다.

보안 영역에는 다음이 포함됩니다 "AWS 비밀 클라우드", "AWS Top Secret Cloud의 약어입니다", 및 "Azure iL6"

다음 표는 이러한 모드를 비교한 것입니다.

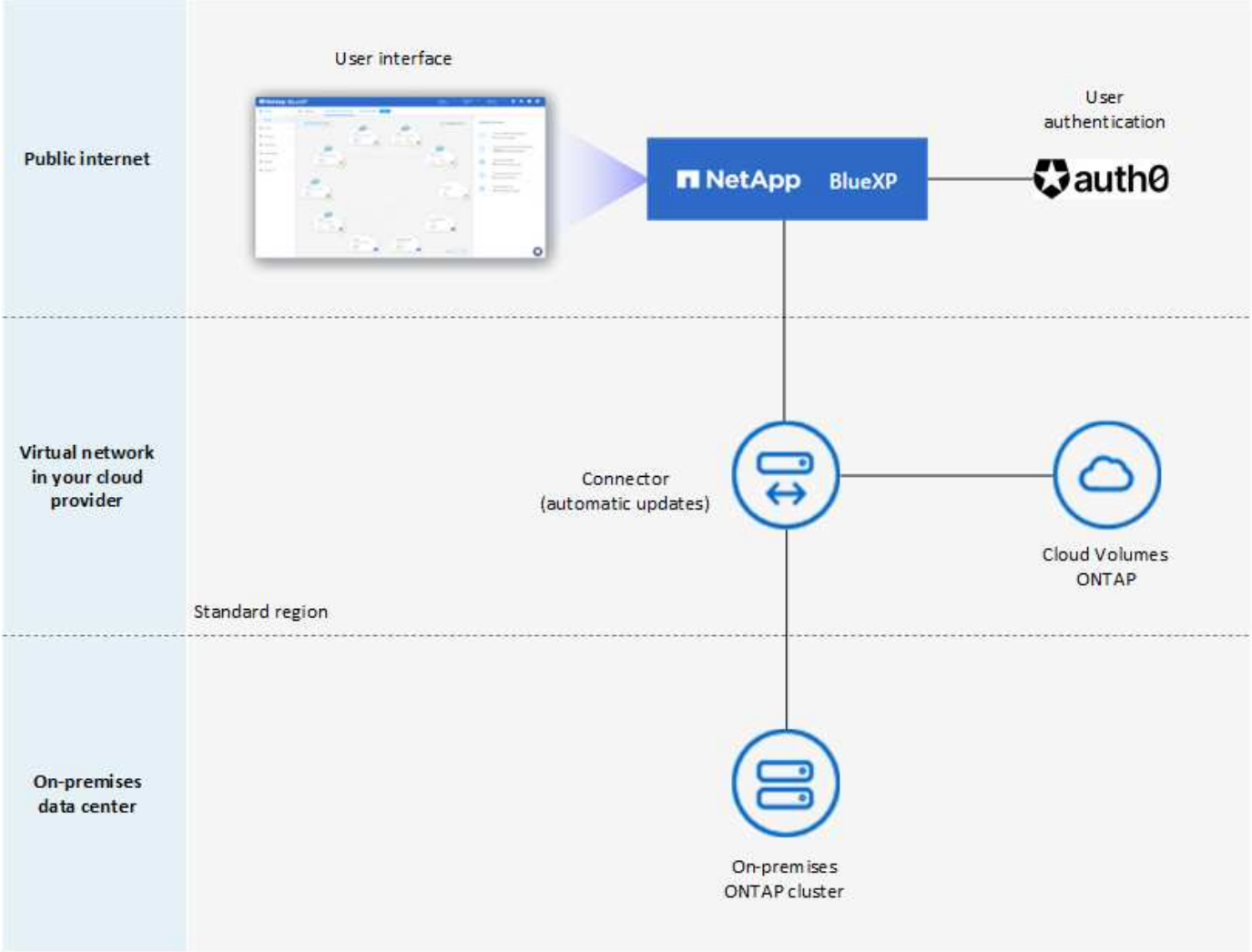
	표준 모드	제한된 모드	비공개 모드
BlueXP SaaS 계층에 연결해야 합니까**?**	예	아웃바운드 전용	아니요
클라우드 공급자에 연결해야 합니까**?**	예	예, 지역 내에 있습니다	예, 해당 지역 내(Cloud Volumes ONTAP를 사용하는 경우)
커넥터 설치	BlueXP, 클라우드 마켓플레이스 또는 수동 설치에서 가능합니다	클라우드 마켓플레이스 또는 수동 설치	수동 설치
커넥터 업그레이드	NetApp Connector 소프트웨어의 자동 업그레이드	NetApp Connector 소프트웨어의 자동 업그레이드	수동 업그레이드가 필요합니다

	표준 모드	제한된 모드	비공개 모드
UI 액세스	BlueXP SaaS 계층에서	커넥터 VM에서 로컬로	커넥터 VM에서 로컬로
API 종점	BlueXP SaaS 레이어	커넥터	커넥터
인증	SaaS를 통해 auth0, NSS 로그인 또는 ID 페더레이션을 사용합니다	SaaS를 통해 auth0 또는 ID 페더레이션을 사용합니다	로컬 사용자 인증
스토리지 및 데이터 서비스	모두 지원됩니다	많은 기능이 지원됩니다	여러 가지가 지원됩니다
라이센스 옵션	마켓플레이스 구독 및 BYOL	마켓플레이스 구독 및 BYOL	BYOL

지원되는 BlueXP 기능 및 서비스를 포함하여 이러한 모드에 대한 자세한 내용은 다음 섹션을 참조하십시오.

표준 모드

다음 그림은 표준 모드 배포의 예입니다.



BlueXP는 표준 모드에서 다음과 같이 작동합니다.

아웃바운드 통신

Connector에서 BlueXP SaaS 레이어, 클라우드 공급업체의 공개된 리소스, 일상적인 운영을 위한 기타 필수 구성 요소에 연결해야 합니다.

- "Connector가 AWS에 연결하는 엔드포인트에는"
- "Connector가 Azure에서 접촉하는 끝점"
- "Connector가 Google Cloud에 연결하는 엔드포인트에는"

커넥터에 대해 지원되는 위치입니다

표준 모드에서 Connector는 클라우드 또는 사내에서 지원됩니다.

커넥터 설치

커넥터 설치는 BlueXP의 설치 마법사, AWS 또는 Azure Marketplace에서 또는 설치 관리자를 사용하여 데이터 센터 또는 클라우드의 자체 Linux 호스트에 커넥터를 수동으로 설치할 수 있습니다.

커넥터 업그레이드

매월 업데이트되는 BlueXP에서 커넥터 소프트웨어의 자동 업그레이드를 사용할 수 있습니다.

사용자 인터페이스 액세스

사용자 인터페이스는 SaaS 계층을 통해 제공되는 웹 기반 콘솔에서 액세스할 수 있습니다.

API 종점

API 호출은 다음 끝점에 대해 이루어집니다.
https://cloudmanager.cloud.netapp.com

인증

인증은 auth0 또는 NSS(NetApp Support 사이트) 로그인을 사용하여 BlueXP의 클라우드 서비스를 통해 제공됩니다. ID 페더레이션을 사용할 수 있습니다.

지원되는 **BlueXP** 서비스

모든 BlueXP 서비스는 사용자가 사용할 수 있습니다.

지원되는 라이센스 옵션

마켓플레이스 가입 및 BYOL은 표준 모드에서 지원되지만 지원되는 라이센스 옵션은 사용 중인 BlueXP 서비스에 따라 다릅니다. 사용 가능한 라이센스 옵션에 대한 자세한 내용은 각 서비스 설명서를 참조하십시오.

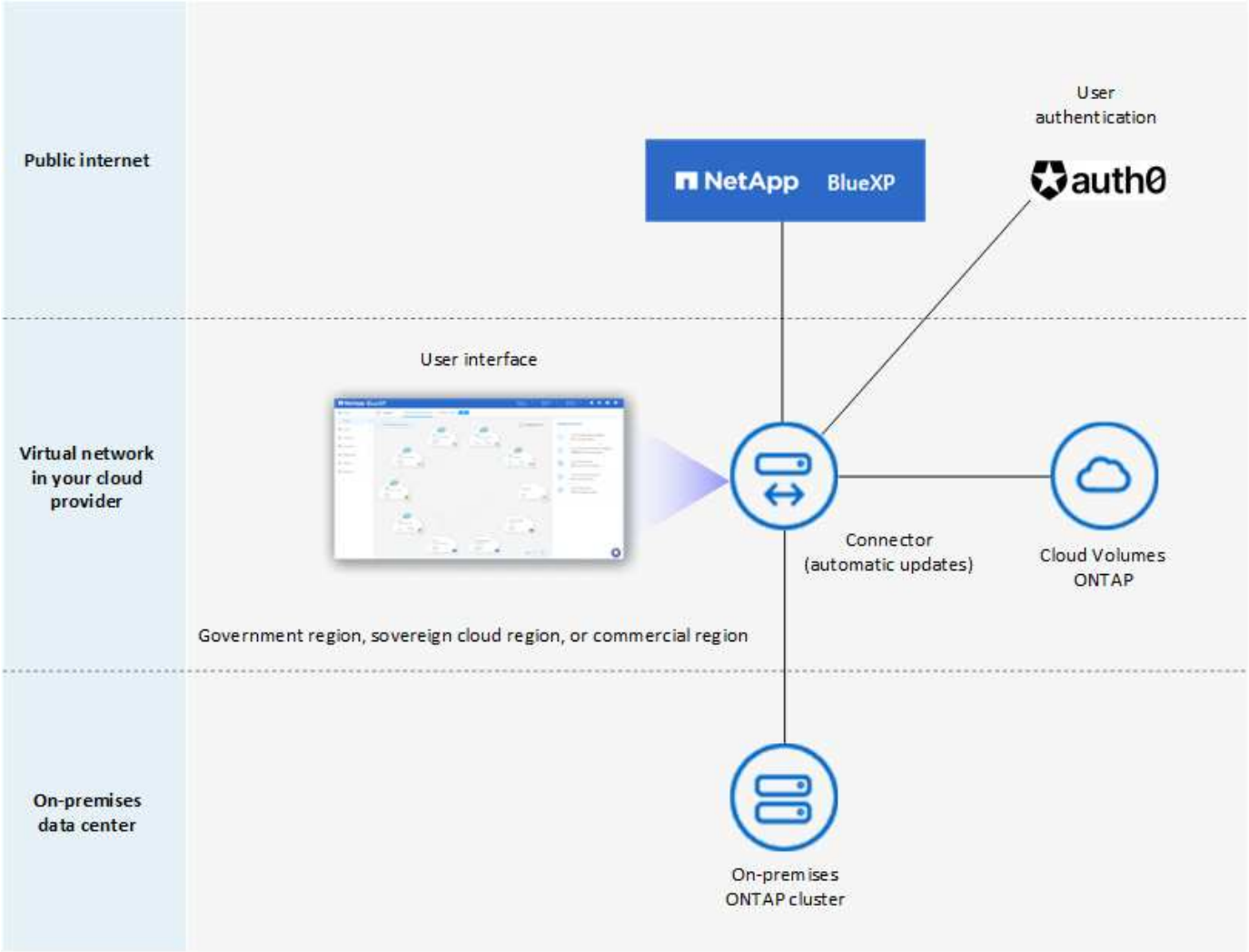
표준 모드 시작 방법

로 이동합니다 "BlueXP 웹 기반 콘솔" 을 클릭합니다.

"표준 모드를 시작하는 방법에 대해 알아봅니다".

제한된 모드

다음 이미지는 제한된 모드 배포의 예입니다.



BlueXP는 제한된 모드에서 다음과 같이 작동합니다.

아웃바운드 통신

Connector에서 BlueXP 데이터 서비스를 사용하고, Connector의 자동 소프트웨어 업그레이드를 사용하고, auth0 기반 인증을 사용하고, 과금 목적(스토리지 VM 이름, 할당된 용량, 볼륨 UUID, 유형 및 IOPS)을 위해 메타데이터를 전송하려면 Connector에서 BlueXP SaaS 계층으로 아웃바운드 연결이 필요합니다.

BlueXP SaaS 계층은 Connector와의 통신을 시작하지 않습니다. 모든 통신은 Connector에 의해 시작되며, Connector는 필요에 따라 SaaS 계층에서 데이터를 끌어가거나 SaaS 계층으로 이동할 수 있습니다.

또한 해당 지역 내의 클라우드 공급자 리소스에 연결해야 합니다.

커넥터에 대해 지원되는 위치입니다

제한 모드에서 Connector는 정부 지역, 주권 지역 또는 상업 지역의 클라우드에서 지원됩니다.

커넥터 설치

커넥터는 AWS 또는 Azure Marketplace에서 설치하거나 자체 Linux 호스트에 수동으로 설치할 수 있습니다.

커넥터 업그레이드

매월 업데이트되는 BlueXP에서 커넥터 소프트웨어의 자동 업그레이드를 사용할 수 있습니다.

사용자 인터페이스 액세스

사용자 인터페이스는 클라우드 지역에 배포된 Connector 가상 머신에서 액세스할 수 있습니다.

API 종점

API 호출은 Connector 가상 시스템으로 이루어집니다.

인증

인증은 auth0을 사용하여 BlueXP의 클라우드 서비스를 통해 제공됩니다. ID 페더레이션을 사용할 수도 있습니다.

지원되는 **BlueXP** 서비스

BlueXP는 제한된 모드에서 다음과 같은 스토리지 및 데이터 서비스를 지원합니다.

지원되는 서비스	참고
ONTAP용 Amazon FSx	완벽한 지원
Azure NetApp Files	완벽한 지원
백업 및 복구	제한 모드가 있는 정부 지역 및 상업 지역에서 지원됩니다. 제한된 모드의 주권 지역에서는 지원되지 않습니다. 제한된 모드에서 BlueXP 백업 및 복구는 ONTAP 볼륨 데이터의 백업 및 복원만 지원합니다. "ONTAP 데이터에 대해 지원되는 백업 대상 목록을 봅니다" 애플리케이션 데이터, 가상 머신 데이터 및 Kubernetes 데이터의 백업 및 복원은 지원되지 않습니다.
분류	제한 모드가 있는 정부 지역에서 지원됩니다. 상용 지역 또는 제한된 모드의 주권 지역에서는 지원되지 않습니다. 다음과 같은 제한 사항이 적용됩니다. • OneDrive 계정, SharePoint 계정 및 Google Drive 계정을 검색할 수 없습니다. • Microsoft Azure 정보 보호(AIP) 레이블 기능은 통합할 수 없습니다.
Cloud Volumes ONTAP	완벽한 지원
디지털 지갑	제한된 모드에 대해 아래 나열된 지원되는 라이센스 옵션과 함께 디지털 지갑을 사용할 수 있습니다.
온프레미스 ONTAP 클러스터	Connector를 사용하는 검색과 Connector를 사용하지 않는 검색(직접 검색) 모두 지원됩니다. 커넥터가 있는 온프레미스 클러스터를 검색할 때 고급 보기(System Manager)가 지원되지 않습니다.
복제	제한 모드가 있는 정부 지역에서 지원됩니다. 상용 지역 또는 제한된 모드의 주권 지역에서는 지원되지 않습니다.

지원되는 라이센스 옵션

제한된 모드에서 지원되는 라이센스 옵션은 다음과 같습니다.

- 마켓플레이스 구독(시간별 및 연간 계약)

  다음 사항에 유의하십시오.

  - Cloud Volumes ONTAP의 경우 용량 기반 라이센스만 지원됩니다.
  - Azure에서는 연차 계약이 정부 지역에서 지원되지 않습니다.

- BYOL

  Cloud Volumes ONTAP의 경우 용량 기반 라이센스와 노드 기반 라이센스가 모두 BYOL에서 지원됩니다.

제한된 모드로 시작하는 방법

BlueXP 계정을 생성할 때 제한된 모드를 활성화해야 합니다.

아직 계정이 없는 경우 수동으로 설치한 Connector 또는 클라우드 공급자의 마켓플레이스에서 만든 Connector에서 처음 BlueXP에 로그인할 때 계정을 만들고 제한된 모드를 활성화하라는 메시지가 표시됩니다.

이미 계정이 있고 다른 계정을 만들려면 Tenancy API를 사용해야 합니다.

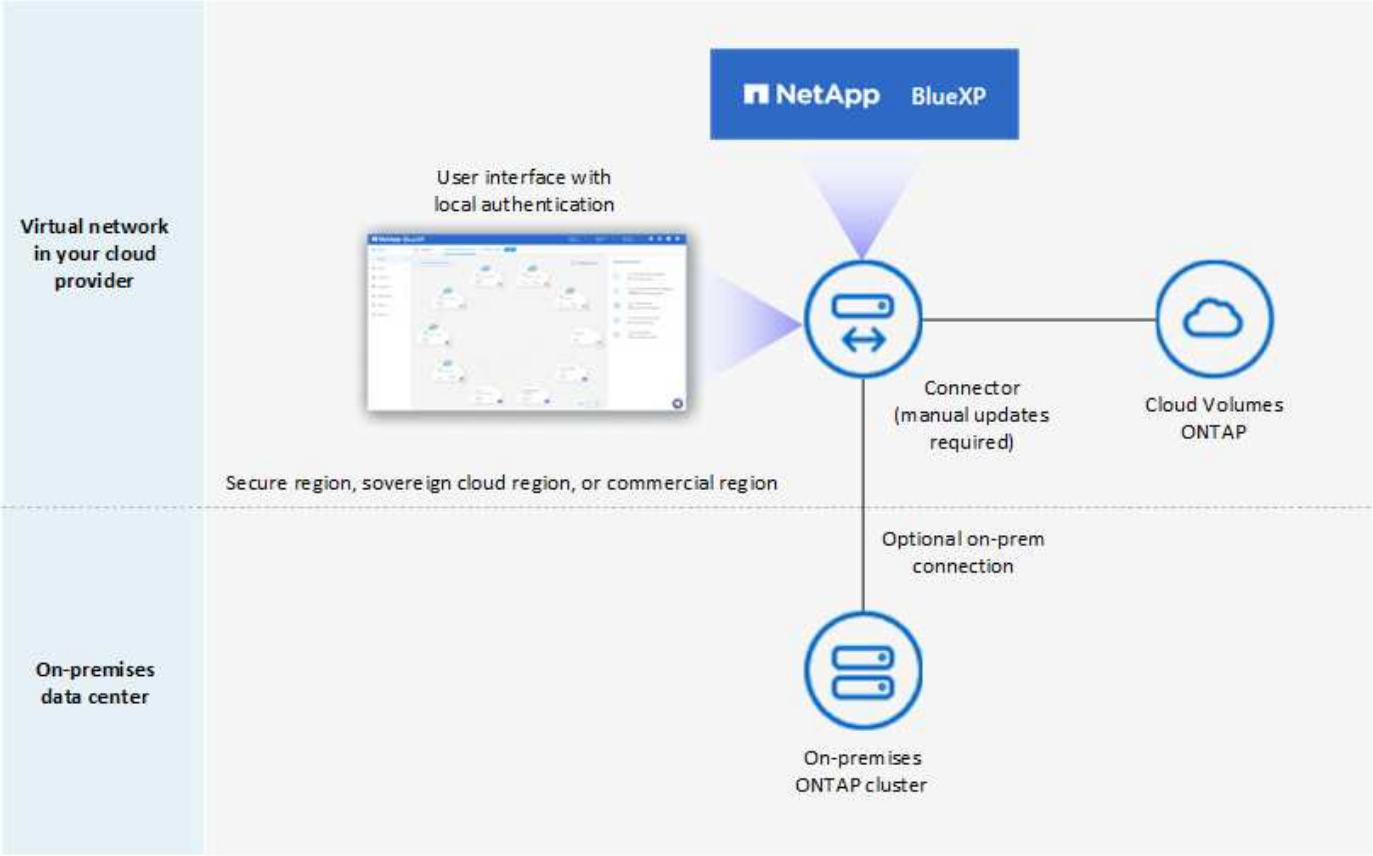
BlueXP에서 계정을 만든 후에는 제한된 모드 설정을 변경할 수 없습니다. 나중에 제한 모드를 활성화할 수 없으며 나중에 비활성화할 수 없습니다. 계정을 생성할 때 설정해야 합니다.

- "제한된 모드로 시작하는 방법에 대해 알아봅니다".
- "추가 BlueXP 계정을 만드는 방법에 대해 알아봅니다".

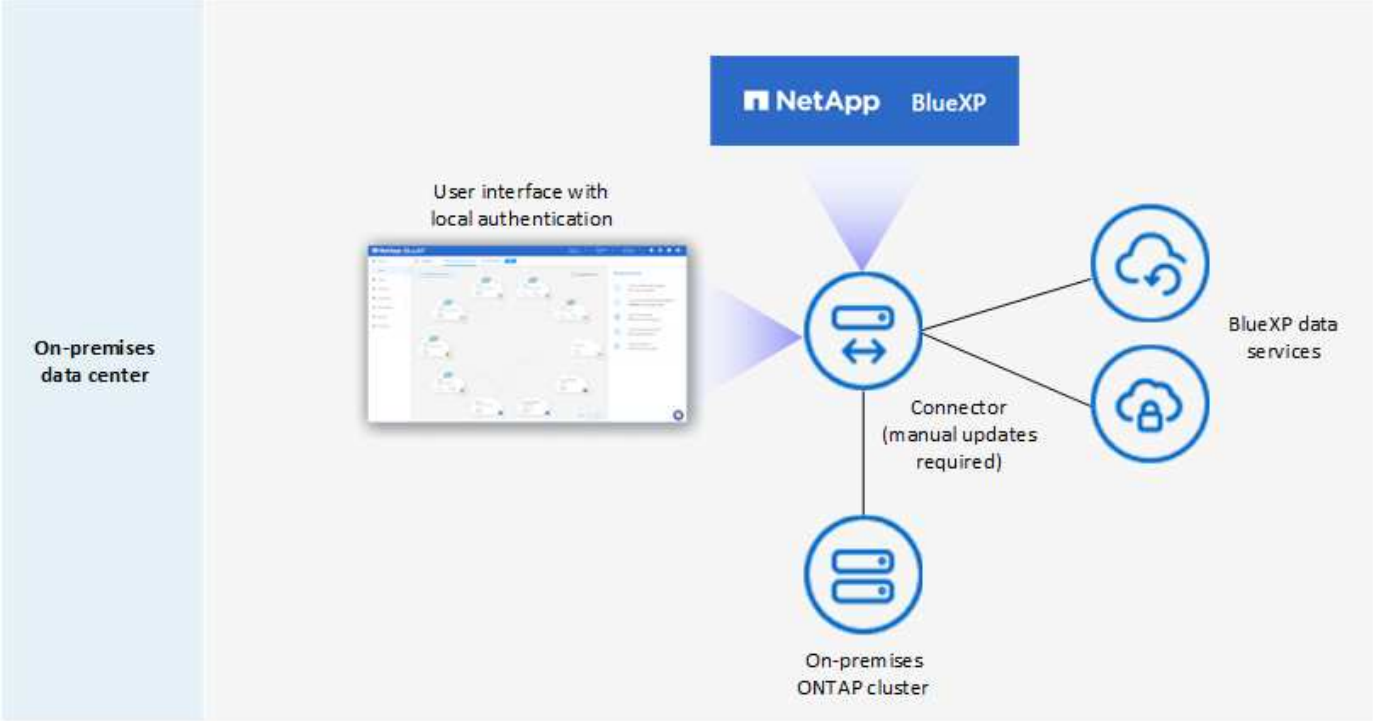
비공개 모드

비공개 모드에서는 Connector를 온프레미스 또는 클라우드에 설치한 다음 BlueXP를 사용하여 하이브리드 클라우드 전체에서 데이터를 관리할 수 있습니다. BlueXP SaaS 계층에 연결할 수 없습니다.

다음 이미지는 클라우드에서 커넥터가 설치되고 Cloud Volumes ONTAP 및 온프레미스 ONTAP 클러스터를 모두 관리하는 프라이빗 모드 구축의 예를 보여줍니다.



한편 두 번째 이미지는 커넥터가 사내에 설치되어 온프레미스 ONTAP 클러스터를 관리하고 지원되는 BlueXP 데이터 서비스에 대한 액세스를 제공하는 비공개 모드 배포의 예를 보여줍니다.



BlueXP는 개인 모드에서 다음과 같이 작동합니다.

아웃바운드 통신

BlueXP SaaS 계층에는 아웃바운드 연결이 필요하지 않습니다. 모든 패키지, 종속성 및 필수 구성 요소는 커넥터와 함께 패키지로 제공되며 로컬 시스템에서 제공됩니다. Cloud Volumes ONTAP를 구축하는 경우에만 클라우드 공급자의 공개 리소스에 연결해야 합니다.

커넥터에 대해 지원되는 위치입니다

프라이빗 모드에서 Connector는 클라우드 또는 온프레미스에서 지원됩니다.

커넥터 설치

Connector 수동 설치는 클라우드 또는 온프레미스 Linux 호스트에서 지원됩니다.

커넥터 업그레이드

커넥터 소프트웨어를 수동으로 업그레이드해야 합니다. 커넥터 소프트웨어는 정의되지 않은 간격으로 NetApp Support 사이트에 게시됩니다.

사용자 인터페이스 액세스

사용자 인터페이스는 클라우드 지역 또는 사내에 구축된 Connector에서 액세스할 수 있습니다.

API 종점

API 호출은 Connector 가상 시스템으로 이루어집니다.

인증

로컬 사용자 관리 및 액세스를 통해 인증이 제공됩니다. BlueXP의 클라우드 서비스를 통해 인증이 제공되지 않습니다.

클라우드 배포 시 **BlueXP** 서비스가 지원됩니다

BlueXP는 Connector를 클라우드에 설치할 때 다음과 같은 개인 모드로 저장 및 데이터 서비스를 지원합니다.

지원되는 서비스	참고
백업 및 복구	AWS 및 Azure 상용 지역에서 지원됩니다. Google Cloud 또는 에서는 지원되지 않습니다 "AWS 비밀 클라우드", "AWS Top Secret Cloud의 약어입니다", 또는 "Azure iL6" 프라이빗 모드에서 BlueXP 백업 및 복구는 ONTAP 볼륨 데이터의 백업 및 복원만 지원합니다. "ONTAP 데이터에 대해 지원되는 백업 대상 목록을 봅니다" 애플리케이션 데이터, 가상 머신 데이터 및 Kubernetes 데이터의 백업 및 복원은 지원되지 않습니다.
Cloud Volumes ONTAP	인터넷에 액세스할 수 없으므로 자동화된 소프트웨어 업그레이드 및 AutoSupport 기능을 사용할 수 없습니다.
디지털 지갑	개인 모드에서는 아래 나열된 지원되는 라이센스 옵션과 함께 디지털 지갑을 사용할 수 있습니다.

지원되는 서비스	참고
온프레미스 ONTAP 클러스터	Connector가 설치된 클라우드 및 사내 환경에 대한 연결이 필요합니다. 커넥터가 없는 검색(직접 검색)은 지원되지 않습니다.

사내 배포에서 지원되는 **BlueXP** 서비스

BlueXP는 Connector를 사내에 설치할 때 다음과 같은 개인 모드로 저장 및 데이터 서비스를 지원합니다.

지원되는 서비스	참고
백업 및 복구	프라이빗 모드에서 BlueXP 백업 및 복구는 ONTAP 볼륨 데이터의 백업 및 복원만 지원합니다. "ONTAP 볼륨 데이터에 대해 지원되는 백업 대상 목록을 봅니다" 애플리케이션 데이터, 가상 머신 데이터 및 Kubernetes 데이터의 백업 및 복원은 지원되지 않습니다.
분류	• 지원되는 데이터 원본은 로컬에서 검색할 수 있는 원본뿐입니다. "로컬로 검색할 수 있는 소스를 봅니다" • 아웃바운드 인터넷 액세스가 필요한 기능은 지원되지 않습니다. "기능 제한 사항을 봅니다"
디지털 지갑	개인 모드에서는 아래 나열된 지원되는 라이센스 옵션과 함께 디지털 지갑을 사용할 수 있습니다.
온프레미스 ONTAP 클러스터	커넥터가 없는 검색(직접 검색)은 지원되지 않습니다.
복제	완벽한 지원

지원되는 라이센스 옵션

BYOL은 프라이빗 모드에서만 지원됩니다.

Cloud Volumes ONTAP BYOL의 경우 노드 기반 라이센스만 지원됩니다. 용량 기반 라이센스는 지원되지 않습니다. 아웃바운드 인터넷 연결을 사용할 수 없으므로 BlueXP 디지털 지갑에서 Cloud Volumes ONTAP 라이선스 파일을 수동으로 업로드해야 합니다.

"BlueXP 디지털 지갑에 라이센스를 추가하는 방법에 대해 알아봅니다"

비공개 모드를 시작하는 방법

비공개 모드는 NetApp Support 사이트에서 "오프라인" 설치 프로그램을 다운로드하여 사용할 수 있습니다.

"비공개 모드를 시작하는 방법에 대해 알아보십시오".

에서 BlueXP를 사용하려는 경우 "AWS 비밀 클라우드" 또는 을 누릅니다 "AWS Top Secret Cloud의 약어입니다"그런 다음 별도의 지침에 따라 해당 환경에서 시작해야 합니다. "AWS Secret Cloud 또는 Top Secret Cloud에서 Cloud Volumes ONTAP을 시작하는 방법을 알아보십시오"

서비스 및 기능 비교

다음 표는 제한된 모드 및 비공개 모드에서 지원되는 BlueXP 서비스 및 기능을 신속하게 식별하는 데 도움이 됩니다.

일부 서비스는 제한 사항으로 지원될 수 있습니다. 제한된 모드 및 비공개 모드에서 이러한 서비스를 지원하는 방법에 대한 자세한 내용은 위의 섹션을 참조하십시오.

제품 영역	**BlueXP** 서비스 또는 기능	제한된 모드	비공개 모드
* 작업 환경 * 표의 이 부분에는 BlueXP 캔버스에서 작업 환경 관리를 위한 지원이 나와 있습니다. BlueXP 백업 및 복구에 지원되는 백업 대상은 표시되지 않습니다.	ONTAP용 Amazon FSx	예	아니요
	Amazon S3	아니요	아니요
	Azure Blob	아니요	아니요
	Azure NetApp Files	예	아니요
	Cloud Volumes ONTAP	예	예
	Google Cloud용 Cloud Volumes Service	아니요	아니요
	Google 클라우드 스토리지	아니요	아니요
	Kubernetes 클러스터	아니요	아니요
	온프레미스 ONTAP 클러스터	예	예
	E-Series 를 참조하십시오	아니요	아니요
	StorageGRID	아니요	아니요

제품 영역	**BlueXP** 서비스 또는 기능	제한된 모드	비공개 모드
서비스 *	백업 및 복구	예 "ONTAP 볼륨 데이터에 대해 지원되는 백업 대상 목록을 봅니다"	예 "ONTAP 볼륨 데이터에 대해 지원되는 백업 대상 목록을 봅니다"
	분류	예	예
	클라우드 운영	아니요	아니요
	복사 및 동기화	아니요	아니요
	디지털 자문업체	아니요	아니요
	디지털 지갑	예	예
	재해 복구	아니요	아니요
	경제적인 효율성	아니요	아니요
	에지 캐싱	아니요	아니요
	마이그레이션 보고서	아니요	아니요
	운영 복원력	아니요	아니요
	랜섬웨어 보호	아니요	아니요
	복제	예	예
	지속 가능성	아니요	아니요
	계층화	아니요	아니요
	볼륨 캐싱	아니요	아니요
* 기능 *	자격 증명	예	예
	NSS 계정	예	아니요
	알림	예	아니요
	검색	예	아니요
	타임라인	예	예

표준 모드로 시작하십시오

워크플로 시작(표준 모드)

BlueXP 콘솔을 위한 네트워킹을 준비하고, 계정을 등록 및 생성하고, 선택적으로 Connector를 생성하고, BlueXP를 구독하여 BlueXP를 표준 모드로 시작하십시오.

표준 모드에서 BlueXP는 웹 기반 콘솔에서 클라우드 서비스로 사용자에게 액세스할 수 있습니다. 시작하기 전에 에 대한 이해가 있어야 합니다 "BlueXP 계정", "커넥터", 및 "배포 모드".

1. **"BlueXP** 콘솔을 사용하기 위한 네트워킹을 준비합니다**"**

BlueXP 콘솔에 액세스하는 컴퓨터는 몇 가지 관리 작업을 완료할 수 있도록 특정 엔드포인트에 연결해야 합니다. 네트워크에서 아웃바운드 액세스를 제한하는 경우 이러한 엔드포인트가 허용되는지 확인해야 합니다.

2 **"등록하고 계정을 만듭니다"**

로 이동합니다 "BlueXP 콘솔" 을 클릭합니다. 계정을 만들 수 있는 옵션이 제공되지만 기존 계정에 초대되는 경우 이 단계를 건너뛸 수 있습니다.

이 시점에서 로그인하면 디지털 어드바이저, ONTAP용 Amazon FSx, Azure NetApp Files 등과 같은 여러 BlueXP 서비스를 사용할 수 있습니다. "커넥터 없이 수행할 수 있는 작업을 알아보십시오".

3 커넥터를 작성합니다

BlueXP를 시작하기 위해 커넥터가 필요하지 않지만 커넥터를 만들어 모든 BlueXP 기능 및 서비스를 잠금 해제할 수 있습니다. Connector는 BlueXP에서 하이브리드 클라우드 환경 내의 리소스 및 프로세스를 관리할 수 있도록 지원하는 NetApp 소프트웨어입니다.

BlueXP 계정 관리자는 클라우드 또는 온프레미스 네트워크에 커넥터를 생성할 수 있습니다.

- "커넥터가 필요한 시기와 작동 방식에 대해 자세히 알아보십시오"
- "AWS에서 커넥터를 생성하는 방법에 대해 알아보십시오"
- "Azure에서 커넥터를 만드는 방법에 대해 알아봅니다"
- "Google Cloud에서 Connector를 만드는 방법을 알아보십시오"
- "온-프레미스에서 커넥터를 만드는 방법에 대해 알아봅니다"

BlueXP 서비스를 사용하여 Google Cloud에서 스토리지 및 데이터를 관리하려면 Connector가 Google Cloud에서 실행되고 있어야 합니다.

4 **"BlueXP에 가입하십시오"**

클라우드 공급업체의 시장에서 BlueXP를 구독하여 시간당 요금(PAYGO)이나 연간 계약을 통해 BlueXP 서비스 비용을 지불하십시오.

BlueXP 콘솔을 사용하기 위한 네트워킹을 준비합니다

SaaS 계층을 통해 제공되는 BlueXP 웹 기반 콘솔을 사용할 때 몇 가지 관리 작업을 완료하면 여러 개의 엔드포인트에 연결됩니다. BlueXP 콘솔에 액세스하는 컴퓨터는 이러한 엔드포인트에 연결해야 합니다.

이러한 엔드포인트는 BlueXP 콘솔에서 특정 작업을 완료할 때 사용자 컴퓨터에서 연결됩니다. 커넥터 및 특정 BlueXP 서비스의 네트워킹 요구사항도 참조해야 합니다. 자세한 내용은 이 페이지 끝에 있는 관련 링크를 참조하십시오.

엔드포인트	목적
https://console.bluexp.netapp.com https://*.console.bluexp.netapp.com	웹 브라우저는 BlueXP 웹 기반 콘솔을 사용할 때 이러한 URL에 연락합니다.

엔드포인트	목적
https://aiq.netapp.com	BlueXP 디지털 어드바이저에 액세스하기 위해 필요합니다.
AWS 서비스(amazonaws.com): • CloudFormation 을 참조하십시오 • EC2(탄력적인 컴퓨팅 클라우드) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • S3(Simple Storage Service)	AWS의 BlueXP에서 커넥터를 구축하는 데 필요합니다. 정확한 끝점은 Connector를 배포하는 영역에 따라 다릅니다. "자세한 내용은 AWS 설명서를 참조하십시오."
https://management.azure.com https://login.microsoftonline.com	대부분의 Azure 지역에서 BlueXP의 커넥터를 배포하는 데 필요합니다.
https://management.microsoftazure.de https://login.microsoftonline.de	Azure 독일 지역의 BlueXP에서 커넥터를 배포하는 데 필요합니다.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Azure US Gov 지역의 BlueXP에서 커넥터를 배포하는 데 필요합니다.
https://www.googleapis.com	Google Cloud의 BlueXP에서 커넥터를 배포하는 데 필요합니다.
https://signin.b2c.netapp.com	NetApp Support 사이트(NSS) 자격 증명을 업데이트하거나 BlueXP에 새 NSS 자격 증명을 추가하는 데 필요합니다.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	웹 브라우저는 BlueXP를 통한 중앙 집중식 사용자 인증을 위해 이러한 엔드포인트에 연결됩니다.
https://widget.intercom.io	제품 내에서 NetApp 클라우드 전문가와 상담할 수 있는 채팅을 제공합니다.

이러한 엔드포인트 외에도, Connector가 일상적인 작업을 위해 특정 엔드포인트에 대한 아웃바운드 인터넷 액세스를 가지고 있는지 확인해야 합니다. 아래 다음 섹션의 링크를 따라 이러한 끝점 목록을 찾을 수 있습니다.

관련 링크

- 커넥터를 위한 네트워킹을 준비합니다
  - "AWS 네트워킹 설정"
  - "Azure 네트워킹을 설정합니다"
  - "Google Cloud 네트워킹을 설정합니다"
  - "사내 네트워킹을 설정합니다"

- BlueXP 서비스를 위한 네트워킹을 준비합니다

  각 BlueXP 서비스에 대한 문서를 참조하십시오.

  "BlueXP 설명서"

BlueXP에 등록하십시오

BlueXP는 웹 기반 콘솔에서 액세스할 수 있습니다. BlueXP를 시작할 때 첫 번째 단계는 기존 NetApp Support 사이트 자격 증명을 사용하거나 NetApp 클라우드 로그인을 생성하여 등록하는 것입니다.

이 작업에 대해

다음 옵션 중 하나를 사용하여 BlueXP에 등록할 수 있습니다.

- 기존 NetApp Support 사이트(NSS) 자격 증명
- 이메일 주소와 암호를 지정하여 NetApp 클라우드 로그인입니다

두 옵션 모두 통합 연결을 지원하므로 회사 디렉터리(통합 ID)의 자격 증명을 사용하여 단일 사인온이 가능합니다. 가입 후 페더레이션 연결을 설정할 수 있습니다. "BlueXP에서 ID 페더레이션을 사용하는 방법에 대해 알아봅니다".

단계

1. 웹 브라우저를 열고 로 이동합니다 "BlueXP 콘솔"
2. NetApp Support 사이트 계정이 있는 경우 NSS 계정과 연결된 이메일 주소를 * 로그인 * 페이지에 직접 입력합니다.

   NSS 계정이 있는 경우 등록 페이지를 건너뛸 수 있습니다. BlueXP가 이 초기 로그인의 일부로 등록하게 됩니다.

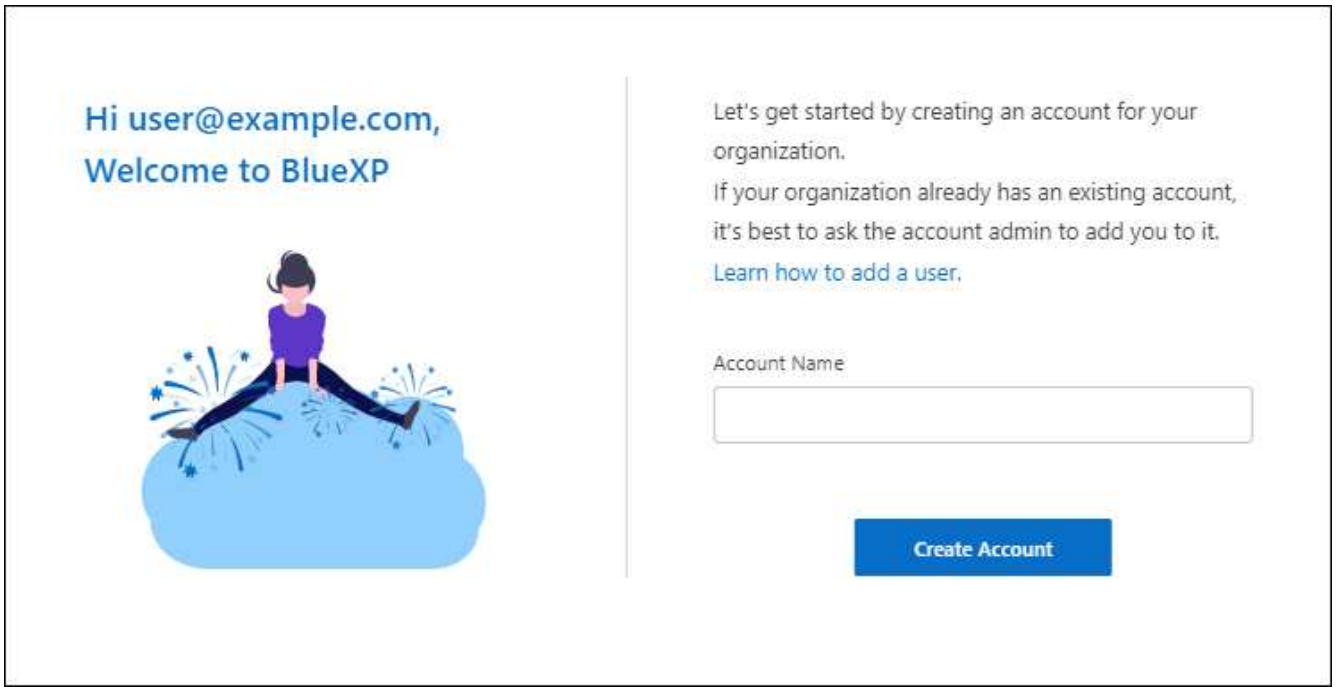
3. NSS 계정이 없는 경우 NetApp 클라우드 로그인을 생성하여 등록하려면 * 등록 * 을 선택하십시오.
4. 등록 * 페이지에서 NetApp 클라우드 로그인을 생성하는 데 필요한 정보를 입력합니다.

   등록 양식에는 영어 문자만 사용할 수 있습니다.

5. 메시지가 표시되면 최종 사용자 사용권 계약을 검토하고 약관에 동의합니다.
6. 시작 * 페이지에서 계정 이름을 입력합니다.

   회사에 이미 계정이 있는 경우 가입하려면 BlueXP를 종료하고 소유자에게 계정을 연계하도록 요청해야 합니다. 소유자가 사용자를 추가한 후 로그인하면 해당 계정에 액세스할 수 있습니다. "기존 계정에 구성원을 추가하는 방법에 대해 알아봅니다".

   계정은 NetApp의 ID 플랫폼에서 최상위 요소입니다. 사용자, 역할, 사용 권한 및 작업 환경을 추가하고 관리할 수 있습니다.



7. 계정 만들기 * 를 선택합니다.

결과

이제 BlueXP 로그인 및 계정이 있습니다. 대부분의 경우 다음 단계는 BlueXP의 서비스를 하이브리드 클라우드 환경에 연결하는 Connector를 만드는 것입니다.

커넥터를 작성합니다

설치하고

AWS의 커넥터 설치 옵션

AWS에서 커넥터를 생성하는 방법은 몇 가지가 있습니다. BlueXP에서 직접 연결하는 것이 가장 일반적인 방법입니다.

다음 설치 옵션을 사용할 수 있습니다.

- "BlueXP에서 직접 Connector를 생성합니다" (표준 옵션)

  이렇게 하면 선택한 VPC에서 Linux를 실행하는 EC2 인스턴스와 Connector 소프트웨어가 실행됩니다.

- "AWS Marketplace에서 Connector를 생성합니다"

  이 작업으로 Linux와 Connector 소프트웨어를 실행하는 EC2 인스턴스도 시작하지만 BlueXP가 아닌 AWS 마켓플레이스에서 직접 구축이 시작됩니다.

- "자체 Linux 호스트에 소프트웨어를 다운로드하고 수동으로 설치합니다"

선택하는 설치 옵션은 설치 준비 방법에 영향을 줍니다. 여기에는 AWS의 리소스를 인증하고 관리하는 데 필요한 권한을 BlueXP에 제공하는 방법이 포함됩니다.

BlueXP에서 AWS에 Connector를 생성하려면 네트워킹을 설정하고 AWS 권한을 준비한 다음 Connector를 생성해야 합니다.

시작하기 전에

을(를) 검토해야 합니다 "커넥터 제한".

단계 **1:** 네트워킹을 설정한다

커넥터를 설치할 네트워크 위치가 다음 요구 사항을 지원하는지 확인합니다. 이러한 요구사항을 충족하면 Connector가 하이브리드 클라우드 환경 내에서 리소스와 프로세스를 관리할 수 있습니다.

VPC 및 서브넷

Connector를 생성할 때 Connector가 상주할 VPC와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

Connector를 사용하려면 작업 환경을 만들고 관리할 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, 온프레미스 환경에서 Cloud Volumes ONTAP 시스템 또는 스토리지 시스템을 생성할 네트워크를 예로 들 수 있습니다.

아웃바운드 인터넷 액세스

커넥터를 배포하는 네트워크 위치에 특정 끝점에 연결하려면 아웃바운드 인터넷 연결이 있어야 합니다.

커넥터에서 접촉된 끝점

Connector는 일상적인 운영을 위해 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하려면 다음 엔드포인트에 연결하는 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 끝점은 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • CloudFormation 을 참조하십시오 • EC2(탄력적인 컴퓨팅 클라우드) • IAM(Identity and Access Management) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • S3(Simple Storage Service)	를 사용하여 AWS에서 리소스를 관리합니다. 정확한 끝점은 사용 중인 AWS 지역에 따라 다릅니다. "자세한 내용은 AWS 설명서를 참조하십시오"
https://support.netapp.com 으로 문의하십시오 https://mysupport.netapp.com 으로 문의하십시오	라이센스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다.

엔드포인트	목적
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXP 내에서 SaaS 기능 및 서비스를 제공합니다. 현재 Connector가 "cloudmanager.cloud.netapp.com" 에 문의하고 있지만 곧 출시될 릴리스에서 "api.bluexp.netapp.com" 에 연락하기 시작합니다.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Connector 및 해당 Docker 구성 요소를 업그레이드합니다.

BlueXP 콘솔에서 연결된 엔드포인트에는

SaaS 계층을 통해 제공되는 BlueXP 웹 기반 콘솔을 사용하면 여러 엔드포인트에 접속하여 데이터 관리 작업을 완료합니다. 여기에는 BlueXP 콘솔에서 커넥터를 배포하기 위해 연결된 엔드포인트가 포함됩니다.

"BlueXP 콘솔에서 연결된 엔드포인트 목록을 봅니다".

프록시 서버

조직에서 모든 나가는 인터넷 트래픽에 대해 프록시 서버를 배포해야 하는 경우 HTTP 또는 HTTPS 프록시에 대한 다음 정보를 가져옵니다. 설치하는 동안 이 정보를 제공해야 합니다.

- IP 주소입니다
- 자격 증명
- HTTPS 인증서

BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

포트

커넥터를 시작하거나 커넥터가 Cloud Volumes ONTAP에서 NetApp 지원으로 AutoSupport 메시지를 보내는 프록시로 사용되지 않는 한 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.
- 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 보내기 위한 아웃바운드 인터넷 연결이 없는 경우 BlueXP는 자동으로 해당 시스템이 커넥터에 포함된 프록시 서버를 사용하도록 구성합니다. 유일한 요구 사항은 커넥터 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

NTP를 활성화합니다

BlueXP 분류를 사용하여 회사 데이터 소스를 검사하려는 경우 BlueXP Connector 시스템과 BlueXP 분류 시스템

모두에서 NTP(Network Time Protocol) 서비스를 활성화하여 시스템 간에 시간이 동기화되도록 해야 합니다. "BlueXP 분류에 대해 자세히 알아보십시오"

Connector를 만든 후 이 네트워킹 요구 사항을 구현해야 합니다.

2단계: AWS 권한 설정

BlueXP는 VPC에 Connector 인스턴스를 구축하기 전에 AWS를 인증해야 합니다. 다음 인증 방법 중 하나를 선택할 수 있습니다.

- BlueXP에서 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 첫 번째 단계는 IAM 정책을 생성하는 것입니다. 이 정책에는 BlueXP에서 AWS에서 Connector 인스턴스를 시작하는 데 필요한 권한만 포함되어 있습니다.

필요한 경우 IAM을 사용하여 IAM 정책을 제한할 수 있습니다 `Condition` 요소. "AWS 설명서:조건 요소"

> BlueXP에서 Connector를 만들면 Connector가 AWS 리소스를 관리할 수 있도록 Connector 인스턴스에 새 권한 집합이 적용됩니다.

단계

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

   이 정책은 BlueXP에서 AWS에서 Connector 인스턴스를 실행하는 데 필요한 권한만 포함합니다. "Connector 인스턴스 자체에 필요한 권한을 봅니다".

```
{
  "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",
        "iam:ListRoles",
        "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",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "kms:ListAliases",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:TerminateInstances"
      ],
      "Condition": {
        "StringLike": {
```

```
            "ec2:ResourceTag/OCCMInstance": "*"
          }
        },
        "Resource": [
          "arn:aws:ec2:*:*:instance/*"
        ]
      }
    ]
}
```

5. 필요한 경우 * 다음 * 을 선택하고 태그를 추가합니다.
6. 다음 * 을 선택하고 이름과 설명을 입력합니다.
7. Create policy * 를 선택합니다.
8. BlueXP에서 사용할 수 있는 IAM 역할 또는 IAM 사용자에게 정책을 연결하여 BlueXP에 액세스 키를 제공할 수 있도록 합니다.
   - (옵션 1) BlueXP가 가정할 수 있는 IAM 역할을 설정합니다.
     i. 대상 계정에서 AWS IAM 콘솔로 이동합니다.
     ii. 액세스 관리에서 * 역할 > 역할 만들기 * 를 선택하고 단계를 따라 역할을 만듭니다.
     iii. 신뢰할 수 있는 엔터티 유형 * 에서 * AWS 계정 * 을 선택합니다.
     iv. 다른 AWS 계정 * 을 선택하고 BlueXP SaaS 계정의 ID를 입력합니다. 952013314444
     v. 이전 섹션에서 생성한 정책을 선택합니다.
     vi. 역할을 만든 후 역할 ARN을 복사하여 Connector를 만들 때 BlueXP에 붙여 넣을 수 있습니다.
   - (옵션 2) BlueXP에 액세스 키를 제공할 수 있도록 IAM 사용자에 대한 권한을 설정합니다.
     i. AWS IAM 콘솔에서 * Users * 를 선택한 다음 사용자 이름을 선택합니다.
     ii. Add permissions > Attach existing policies directly * 를 선택합니다.
     iii. 생성한 정책을 선택합니다.
     iv. 다음 * 을 선택한 다음 * 권한 추가 * 를 선택합니다.
     v. IAM 사용자를 위한 액세스 키와 비밀 키가 있는지 확인합니다.

결과

필요한 권한이 있는 IAM 역할 또는 필요한 권한이 있는 IAM 사용자가 있어야 합니다. BlueXP에서 커넥터를 생성할 때 역할 또는 액세스 키에 대한 정보를 제공할 수 있습니다.

3단계**:** 커넥터를 만듭니다

BlueXP 웹 기반 콘솔에서 직접 커넥터를 생성합니다.

이 작업에 대해

BlueXP에서 Connector를 생성하면 기본 구성을 사용하여 AWS에서 EC2 인스턴스를 배포합니다. 커넥터를 생성한 후에는 CPU 또는 RAM이 더 적은 더 작은 EC2 인스턴스 유형으로 변경하지 마십시오. "Connector의 기본 설정에 대해 알아봅니다".

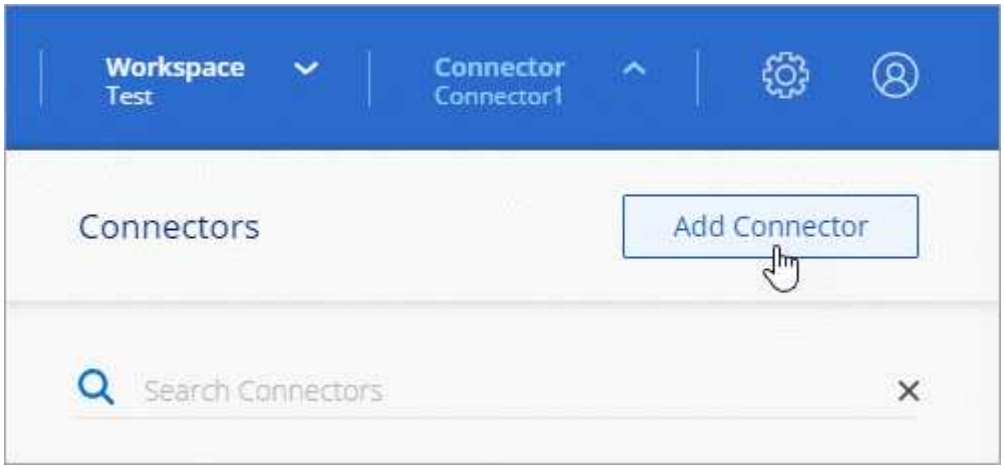
시작하기 전에

다음과 같은 항목이 있어야 합니다.

- AWS 인증 방법: 필요한 권한이 있는 IAM 사용자의 IAM 역할 또는 액세스 키
- 네트워킹 요구사항을 충족하는 VPC 및 서브넷
- EC2 인스턴스의 키 쌍입니다.
- Connector의 인터넷 액세스에 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

단계

1. 커넥터 * 드롭다운을 선택하고 * 커넥터 추가 * 를 선택합니다.



2. 클라우드 공급자로 * Amazon Web Services * 를 선택하고 * Continue * 를 선택합니다.
3. 커넥터 배포 * 페이지에서 필요한 사항에 대한 세부 정보를 검토합니다. 두 가지 옵션이 있습니다.
   a. 제품 내 가이드를 사용하여 배포를 준비하려면 * 계속 * 을 선택합니다. 제품 내 가이드의 각 단계에는 이 문서 페이지에 포함된 정보가 포함되어 있습니다.
   b. 이 페이지의 단계에 따라 이미 준비되었으면 * 배포로 건너뛰기 * 를 선택합니다.
4. 마법사의 단계에 따라 커넥터를 작성합니다.
   - * 준비 완료 *: 필요한 사항을 검토합니다.
   - * AWS 자격 증명 *: AWS 지역을 지정한 다음 BlueXP가 사용할 수 있는 IAM 역할 또는 AWS 액세스 키와 비밀 키를 선택하는 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.
     - 필요한 권한이 있는 새 역할을 BlueXP에서 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.

    커넥터와 함께 사용할 키 쌍이 올바른지 확인합니다. 키 쌍이 없으면 Connector 가상 머신에 액세스할 수 없습니다.

  - * 보안 그룹 *: 새 보안 그룹을 생성할지 또는 필요한 인바운드 및 아웃바운드 규칙을 허용하는 기존 보안 그룹을 선택할지 여부를 선택합니다.

    "AWS의 보안 그룹 규칙을 봅니다".

  - * 검토 *: 선택 사항을 검토하여 설정이 올바른지 확인합니다.
5. 추가 * 를 선택합니다.

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

결과

프로세스가 완료되면 BlueXP에서 커넥터를 사용할 수 있습니다.

Connector를 생성한 동일한 AWS 계정에 Amazon S3 버킷이 있는 경우 BlueXP 캔버스에 Amazon S3 작업 환경이 자동으로 표시됩니다. "BlueXP에서 S3 버킷을 관리하는 방법에 관해 알아보십시오"

AWS Marketplace에서 **Connector**를 생성합니다

AWS Marketplace에서 Connector를 만들려면 네트워킹을 설정하고 AWS 권한을 준비하고 인스턴스 요구 사항을 검토한 다음 Connector를 만들어야 합니다.

시작하기 전에

을(를) 검토해야 합니다 "커넥터 제한".

단계 **1:** 네트워킹을 설정한다

커넥터를 설치할 네트워크 위치가 다음 요구 사항을 지원하는지 확인합니다. 이러한 요구사항을 충족하면 Connector가 하이브리드 클라우드 환경 내에서 리소스와 프로세스를 관리할 수 있습니다.

VPC 및 서브넷

Connector를 생성할 때 Connector가 상주할 VPC와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

Connector를 사용하려면 작업 환경을 만들고 관리할 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, 온프레미스 환경에서 Cloud Volumes ONTAP 시스템 또는 스토리지 시스템을 생성할 네트워크를 예로 들 수 있습니다.

아웃바운드 인터넷 액세스

커넥터를 배포하는 네트워크 위치에 특정 끝점에 연결하려면 아웃바운드 인터넷 연결이 있어야 합니다.

커넥터에서 접촉된 끝점

Connector는 일상적인 운영을 위해 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하려면 다음 엔드포인트에 연결하는 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 끝점은 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • CloudFormation 을 참조하십시오 • EC2(탄력적인 컴퓨팅 클라우드) • IAM(Identity and Access Management) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • S3(Simple Storage Service)	를 사용하여 AWS에서 리소스를 관리합니다. 정확한 끝점은 사용 중인 AWS 지역에 따라 다릅니다. "자세한 내용은 AWS 설명서를 참조하십시오"
https://support.netapp.com 으로 문의하십시오 https://mysupport.netapp.com 으로 문의하십시오	라이센스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXP 내에서 SaaS 기능 및 서비스를 제공합니다. 현재 Connector가 "cloudmanager.cloud.netapp.com" 에 문의하고 있지만 곧 출시될 릴리스에서 "api.bluexp.netapp.com" 에 연락하기 시작합니다.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Connector 및 해당 Docker 구성 요소를 업그레이드합니다.

프록시 서버

조직에서 모든 나가는 인터넷 트래픽에 대해 프록시 서버를 배포해야 하는 경우 HTTP 또는 HTTPS 프록시에 대한 다음 정보를 가져옵니다. 설치하는 동안 이 정보를 제공해야 합니다.

- IP 주소입니다
- 자격 증명
- HTTPS 인증서

BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

포트

커넥터를 시작하거나 커넥터가 Cloud Volumes ONTAP에서 NetApp 지원으로 AutoSupport 메시지를 보내는 프록시로 사용되지 않는 한 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.
- 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 보내기 위한 아웃바운드 인터넷 연결이 없는 경우 BlueXP는 자동으로 해당 시스템이 커넥터에 포함된 프록시 서버를 사용하도록 구성합니다. 유일한 요구 사항은 커넥터 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

NTP를 활성화합니다

BlueXP 분류를 사용하여 회사 데이터 소스를 검사하려는 경우 BlueXP Connector 시스템과 BlueXP 분류 시스템 모두에서 NTP(Network Time Protocol) 서비스를 활성화하여 시스템 간에 시간이 동기화되도록 해야 합니다. "BlueXP 분류에 대해 자세히 알아보십시오"

Connector를 만든 후 이 네트워킹 요구 사항을 구현해야 합니다.

2단계**: AWS** 권한 설정

시장 구축을 준비하려면 AWS에서 IAM 정책을 생성하고 IAM 역할에 연결합니다. AWS Marketplace에서 Connector를 생성하면 해당 IAM 역할을 선택하라는 메시지가 표시됩니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책 생성:
   a. 정책 > 정책 생성 * 을 선택합니다.
   b. JSON * 을 선택하고 의 내용을 복사하여 붙여 넣습니다 "Connector에 대한 IAM 정책".
   c. 나머지 단계를 완료하고 정책을 생성합니다.

      사용할 BlueXP 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다. 표준 영역의 경우 권한이 두 정책에 분산됩니다. AWS에서 관리되는 정책의 최대 문자 크기 제한으로 인해 두 개의 정책이 필요합니다. "Connector에 대한 IAM 정책에 대해 자세히 알아보십시오".
3. IAM 역할 생성:
   a. 역할 > 역할 생성 * 을 선택합니다.
   b. AWS 서비스 > EC2 * 를 선택합니다.
   c. 방금 만든 정책을 첨부하여 사용 권한을 추가합니다.
   d. 나머지 단계를 완료해서 역할을 만듭니다.

결과

AWS Marketplace에서 구축하는 동안 IAM 역할을 EC2 인스턴스와 연결할 수 있습니다.

3단계**:** 인스턴스 요구 사항을 검토합니다

Connector를 생성할 때 다음 요구 사항을 충족하는 EC2 인스턴스 유형을 선택해야 합니다.

CPU
: 코어 4개 또는 vCPU 4개

RAM
: 14GB

AWS EC2 인스턴스 유형
: 위의 CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. T3.xLarge를 권장합니다.

4단계**:** 커넥터를 만듭니다

AWS Marketplace에서 직접 Connector를 생성합니다.

이 작업에 대해

AWS Marketplace에서 Connector를 생성하면 기본 구성을 사용하여 AWS에서 EC2 인스턴스를 배포합니다. "Connector의 기본 설정에 대해 알아봅니다".

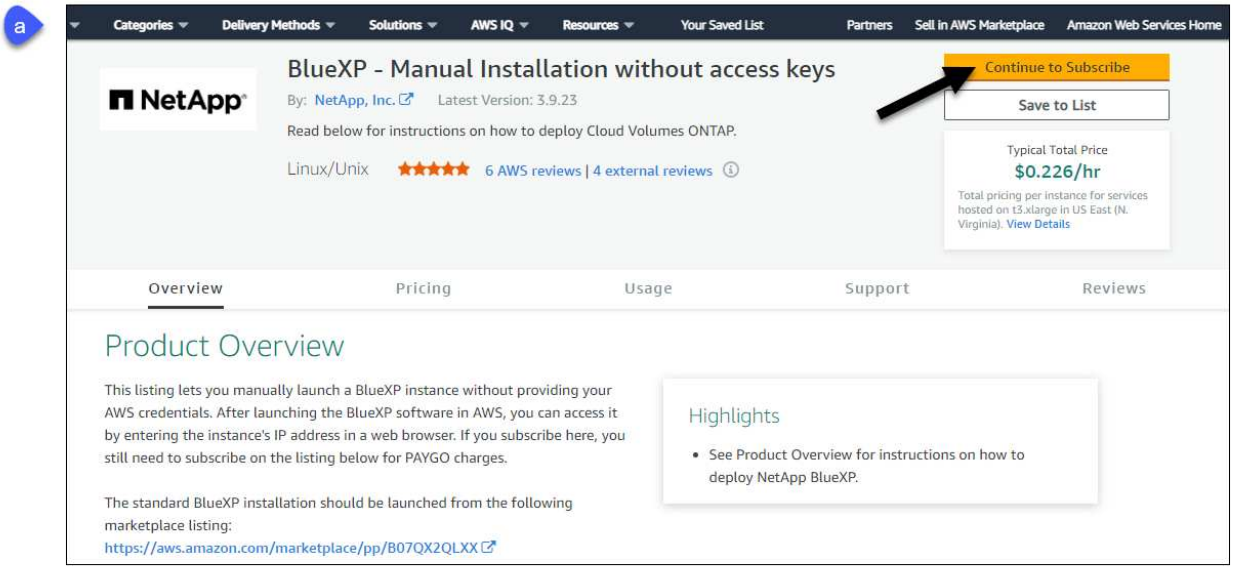
시작하기 전에

다음과 같은 항목이 있어야 합니다.

- 네트워킹 요구사항을 충족하는 VPC 및 서브넷
- Connector에 필요한 권한을 포함하는 정책이 첨부된 IAM 역할
- IAM 사용자에 대한 AWS 마켓플레이스의 구독 및 구독 취소 권한
- 인스턴스의 CPU 및 RAM 요구 사항 이해
- EC2 인스턴스의 키 쌍입니다.

단계

1. 로 이동합니다 "AWS 마켓플레이스의 BlueXP 페이지"
2. Marketplace 페이지에서 * Continue to Subscribe * 를 선택한 다음 * Continue to Configuration * 을 선택합니다.



3. 기본 옵션을 변경하고 * Continue to Launch * 를 선택합니다.
4. 작업 선택 * 에서 * EC2 * 를 통해 시작 * 을 선택한 다음 * 시작 * 을 선택합니다.

   다음 단계에서는 콘솔에서 IAM 역할을 Connector 인스턴스에 연결할 수 있으므로 EC2 콘솔에서 인스턴스를 실행하는 방법을 설명합니다. 웹 사이트에서 시작 * 작업을 사용하면 이 작업을 수행할 수 없습니다.

5. 프롬프트에 따라 인스턴스를 구성하고 배포합니다.
   - * 이름 및 태그 *: 인스턴스의 이름과 태그를 입력합니다.
   - * 응용 프로그램 및 OS 이미지 *: 이 섹션을 건너뜁니다. 커넥터 AMI가 이미 선택되어 있습니다.
   - * 인스턴스 유형 *: 지역 가용성에 따라 RAM 및 CPU 요구 사항을 충족하는 인스턴스 유형을 선택합니다(T3.xLarge가 권장됨).
   - * 키 쌍(로그인) *: 인스턴스에 안전하게 연결하는 데 사용할 키 쌍을 선택합니다.
   - * 네트워크 설정 *: 필요에 따라 네트워크 설정을 편집합니다.
     - 원하는 VPC 및 서브넷을 선택합니다.
     - 인스턴스에 공용 IP 주소가 있어야 하는지 여부를 지정합니다.
     - Connector 인스턴스에 필요한 연결 방법(SSH, HTTP 및 HTTPS)을 활성화하는 방화벽 설정을 지정합니다.

특정 구성에는 몇 가지 규칙이 더 필요합니다.

"AWS의 보안 그룹 규칙을 봅니다".

- * 스토리지 구성 *: 루트 볼륨의 기본 크기와 디스크 유형을 유지합니다.

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

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

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

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

   https://ipaddress

7. 로그인한 후 Connector를 설정합니다.
   a. Connector와 연결할 BlueXP 계정을 지정합니다.
   b. 시스템의 이름을 입력합니다.
   c. 에서 * 보안 환경에서 실행 중입니까? * 제한된 모드를 사용하지 않도록 설정합니다.

      이 단계에서는 표준 모드에서 BlueXP를 사용하는 방법을 설명하므로 제한된 모드를 사용하지 않도록 설정해야 합니다. 보안 환경이 있고 BlueXP 백엔드 서비스에서 이 계정의 연결을 끊으려면 제한된 모드만 활성화해야 합니다. 그렇다면 "제한된 모드에서 BlueXP를 시작하려면 다음 단계를 따르십시오".

   d. Let's start * 를 선택합니다.

결과

이제 커넥터가 설치되어 BlueXP 계정으로 설정됩니다.

웹 브라우저를 열고 로 이동합니다 "BlueXP 콘솔" 을 눌러 BlueXP에서 커넥터 사용을 시작합니다.

Connector를 생성한 동일한 AWS 계정에 Amazon S3 버킷이 있는 경우 BlueXP 캔버스에 Amazon S3 작업 환경이 자동으로 표시됩니다. "BlueXP에서 S3 버킷을 관리하는 방법에 관해 알아보십시오"

Connector를 **AWS**에 수동으로 설치합니다

자신의 Linux 호스트에 Connector를 수동으로 설치하려면 호스트 요구 사항을 검토하고 네트워킹을 설정하고 AWS 사용 권한을 준비하고 커넥터를 설치한 다음 준비한 사용 권한을 제공해야 합니다.

시작하기 전에

을(를) 검토해야 합니다 "커넥터 제한".

1단계: 호스트 요구 사항을 검토합니다

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

전용 호스트

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

지원되는 운영 체제

- 우분투 22.04 LTS
- CentOS 7.6, 7.7, 7.8 및 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 및 7.9

  호스트는 Red Hat Subscription Management에 등록되어 있어야 합니다. 등록되지 않은 경우 호스트는 Connector 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.

  Connector는 이러한 운영 체제의 영어 버전에서 지원됩니다.

하이퍼바이저

Ubuntu, CentOS 또는 Red Hat Enterprise Linux 실행 인증을 받은 베어 메탈 또는 호스팅된 하이퍼바이저가 필요합니다.

"Red Hat 솔루션: Red Hat Enterprise Linux 실행 인증을 받은 하이퍼바이저는 무엇입니까?"

CPU

코어 4개 또는 vCPU 4개

RAM

14GB

AWS EC2 인스턴스 유형

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

키 쌍

Connector를 생성할 때 인스턴스와 함께 사용할 EC2 키 쌍을 선택해야 합니다.

/opt의 디스크 공간입니다

100GiB의 공간을 사용할 수 있어야 합니다

/var의 디스크 공간입니다

20GiB의 공간을 사용할 수 있어야 합니다

Docker 엔진

Connector를 설치하기 전에 Docker 엔진이 호스트에 필요합니다.

- 지원되는 최소 버전은 19.3.1입니다.
- 지원되는 최대 버전은 25.0.5입니다.

"설치 지침을 봅니다"

2단계**:** 네트워킹을 설정한다

커넥터를 설치할 네트워크 위치가 다음 요구 사항을 지원하는지 확인합니다. 이러한 요구사항을 충족하면 Connector가 하이브리드 클라우드 환경 내에서 리소스와 프로세스를 관리할 수 있습니다.

대상 네트워크에 대한 연결

Connector를 사용하려면 작업 환경을 만들고 관리할 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, 온프레미스 환경에서 Cloud Volumes ONTAP 시스템 또는 스토리지 시스템을 생성할 네트워크를 예로 들 수 있습니다.

아웃바운드 인터넷 액세스

커넥터를 배포하는 네트워크 위치에 특정 끝점에 연결하려면 아웃바운드 인터넷 연결이 있어야 합니다.

수동 설치 중에 연결된 끝점입니다

자체 Linux 호스트에 커넥터를 수동으로 설치할 경우 Connector 설치 과정에서 다음 URL에 액세스해야 합니다.

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

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

커넥터에서 접촉된 끝점

Connector는 일상적인 운영을 위해 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하려면 다음 엔드포인트에 연결하는 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 끝점은 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • CloudFormation 을 참조하십시오 • EC2(탄력적인 컴퓨팅 클라우드) • IAM(Identity and Access Management) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • S3(Simple Storage Service)	를 사용하여 AWS에서 리소스를 관리합니다. 정확한 끝점은 사용 중인 AWS 지역에 따라 다릅니다. "자세한 내용은 AWS 설명서를 참조하십시오"

엔드포인트	목적
https://support.netapp.com 으로 문의하십시오 https://mysupport.netapp.com 으로 문의하십시오	라이센스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXP 내에서 SaaS 기능 및 서비스를 제공합니다. 현재 Connector가 "cloudmanager.cloud.netapp.com" 에 문의하고 있지만 곧 출시될 릴리스에서 "api.bluexp.netapp.com" 에 연락하기 시작합니다.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Connector 및 해당 Docker 구성 요소를 업그레이드합니다.

프록시 서버

조직에서 모든 나가는 인터넷 트래픽에 대해 프록시 서버를 배포해야 하는 경우 HTTP 또는 HTTPS 프록시에 대한 다음 정보를 가져옵니다. 설치하는 동안 이 정보를 제공해야 합니다.

- IP 주소입니다
- 자격 증명
- HTTPS 인증서

BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

포트

커넥터를 시작하거나 커넥터가 Cloud Volumes ONTAP에서 NetApp 지원으로 AutoSupport 메시지를 보내는 프록시로 사용되지 않는 한 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.
- 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 보내기 위한 아웃바운드 인터넷 연결이 없는 경우 BlueXP는 자동으로 해당 시스템이 커넥터에 포함된 프록시 서버를 사용하도록 구성합니다. 유일한 요구 사항은 커넥터 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

NTP를 활성화합니다

BlueXP 분류를 사용하여 회사 데이터 소스를 검사하려는 경우 BlueXP Connector 시스템과 BlueXP 분류 시스템 모두에서 NTP(Network Time Protocol) 서비스를 활성화하여 시스템 간에 시간이 동기화되도록 해야 합니다. "BlueXP 분류에 대해 자세히 알아보십시오"

3단계**:** 사용 권한 설정

다음 옵션 중 하나를 사용하여 BlueXP에 AWS 권한을 제공해야 합니다.

- 옵션 1: IAM 정책을 생성하고 EC2 인스턴스와 연결할 수 있는 IAM 역할에 정책을 연결합니다.
- 옵션 2: 필요한 권한이 있는 IAM 사용자를 위해 BlueXP에 AWS 액세스 키를 제공합니다.

단계에 따라 BlueXP 권한을 준비합니다.

IAM 역할

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책 생성:
   a. 정책 > 정책 생성 * 을 선택합니다.
   b. JSON * 을 선택하고 의 내용을 복사하여 붙여 넣습니다 "Connector에 대한 IAM 정책".
   c. 나머지 단계를 완료하고 정책을 생성합니다.

      사용할 BlueXP 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다. 표준 영역의 경우 권한이 두 정책에 분산됩니다. AWS에서 관리되는 정책의 최대 문자 크기 제한으로 인해 두 개의 정책이 필요합니다. "Connector에 대한 IAM 정책에 대해 자세히 알아보십시오".
3. IAM 역할 생성:
   a. 역할 > 역할 생성 * 을 선택합니다.
   b. AWS 서비스 > EC2 * 를 선택합니다.
   c. 방금 만든 정책을 첨부하여 사용 권한을 추가합니다.
   d. 나머지 단계를 완료해서 역할을 만듭니다.

결과

이제 Connector를 설치한 후 EC2 인스턴스와 연결할 수 있는 IAM 역할이 있습니다.

AWS 액세스 키입니다

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책 생성:
   a. 정책 > 정책 생성 * 을 선택합니다.
   b. JSON * 을 선택하고 의 내용을 복사하여 붙여 넣습니다 "Connector에 대한 IAM 정책".
   c. 나머지 단계를 완료하고 정책을 생성합니다.

      사용할 BlueXP 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다.

   표준 영역의 경우 권한이 두 정책에 분산됩니다. AWS에서 관리되는 정책의 최대 문자 크기 제한으로 인해 두 개의 정책이 필요합니다. "Connector에 대한 IAM 정책에 대해 자세히 알아보십시오".
3. IAM 사용자에게 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"
4. 커넥터를 설치한 후 BlueXP에 추가할 수 있는 액세스 키가 사용자에게 있는지 확인합니다.

결과

이제 필요한 권한이 있는 IAM 사용자와 BlueXP에 제공할 수 있는 액세스 키가 있습니다.

4단계: 커넥터를 설치합니다

필수 구성 요소를 완료한 후 자신의 Linux 호스트에 소프트웨어를 수동으로 설치할 수 있습니다.

시작하기 전에

다음과 같은 항목이 있어야 합니다.

- 커넥터를 설치할 수 있는 루트 권한
- Connector의 인터넷 액세스에 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

  설치 후 프록시 서버를 구성할 수 있지만 이렇게 하려면 커넥터를 다시 시작해야 합니다.

  BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

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

이 작업에 대해

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

단계

1. Docker가 설정 및 실행 중인지 확인합니다.

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

2. _http_proxy_or_https_proxy_system 변수가 호스트에 설정되어 있으면 이를 제거합니다.

   ```
   unset http_proxy
   unset https_proxy
   ```

   이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

3. 에서 Connector 소프트웨어를 다운로드합니다 "NetApp Support 사이트"를 선택한 다음 Linux 호스트에 복사합니다.

   네트워크 또는 클라우드에서 사용하도록 고안된 "온라인" 커넥터 설치 프로그램을 다운로드해야 합니다. Connector에 대해 별도의 "오프라인" 설치 프로그램을 사용할 수 있지만 전용 모드 배포에서만 지원됩니다.

4. 스크립트를 실행할 권한을 할당합니다.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

   여기서 <version>는 다운로드한 커넥터 버전입니다.

5. 설치 스크립트를 실행합니다.

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

proxy 및 — cacert 매개 변수는 선택 사항입니다. 프록시 서버가 있는 경우 그림과 같이 매개 변수를 입력해야 합니다. 설치 프로그램에서 프록시에 대한 정보를 제공하라는 메시지를 표시하지 않습니다.

다음은 두 가지 선택적 매개 변수를 사용하는 명령의 예입니다.

```
./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

— 프록시는 다음 형식 중 하나를 사용하여 커넥터가 HTTP 또는 HTTPS 프록시 서버를 사용하도록 구성합니다.

- http://address:port
- http://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  다음 사항에 유의하십시오.

  - 사용자는 로컬 사용자 또는 도메인 사용자일 수 있습니다.
  - 도메인 사용자의 경우 위에 표시된 \ 에 ASCII 코드를 사용해야 합니다.
  - BlueXP는 @ 문자를 포함하는 암호를 지원하지 않습니다.

cacert는 Connector와 프록시 서버 간의 HTTPS 액세스에 사용할 CA 서명 인증서를 지정합니다. 이 매개 변수는 HTTPS 프록시 서버를 지정하거나 프록시가 가로채기 프록시인 경우에만 필요합니다.

6. 설치가 완료될 때까지 기다립니다.

   프록시 서버를 지정한 경우 설치가 끝나면 커넥터 서비스(occm)가 두 번 다시 시작됩니다.

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

   https://ipaddress

8. 로그인한 후 Connector를 설정합니다.

   a. Connector와 연결할 BlueXP 계정을 지정합니다.

   b. 시스템의 이름을 입력합니다.

   c. 에서 * 보안 환경에서 실행 중입니까? * 제한된 모드를 사용하지 않도록 설정합니다.

      이 단계에서는 표준 모드에서 BlueXP를 사용하는 방법을 설명하므로 제한된 모드를 사용하지 않도록 설정해야 합니다. 보안 환경이 있고 BlueXP 백엔드 서비스에서 이 계정의 연결을 끊으려면 제한된 모드만 활성화해야

합니다. 그렇다면 "제한된 모드에서 BlueXP를 시작하려면 다음 단계를 따르십시오".

d. Let's start * 를 선택합니다.

결과

이제 커넥터가 설치되어 BlueXP 계정으로 설정됩니다.

Connector를 생성한 동일한 AWS 계정에 Amazon S3 버킷이 있는 경우 BlueXP 캔버스에 Amazon S3 작업 환경이 자동으로 표시됩니다. "BlueXP에서 S3 버킷을 관리하는 방법에 관해 알아보십시오"

5단계**: BlueXP**에 권한 제공

이제 커넥터를 설치했으므로 이전에 설정한 AWS 권한을 BlueXP에 제공해야 합니다. 권한을 제공하면 BlueXP에서 AWS의 데이터 및 스토리지 인프라를 관리할 수 있습니다.

IAM 역할

이전에 만든 IAM 역할을 Connector EC2 인스턴스에 연결합니다.

단계

1. Amazon EC2 콘솔로 이동합니다.
2. 인스턴스 * 를 선택합니다.
3. 커넥터 인스턴스를 선택합니다.
4. Actions > Security > Modify IAM role * 을 선택합니다.
5. IAM 역할을 선택하고 * Update IAM role * 을 선택합니다.

결과

BlueXP는 이제 AWS에서 사용자 대신 작업을 수행하는 데 필요한 권한을 가집니다.

로 이동합니다 "BlueXP 콘솔" 을 눌러 BlueXP에서 커넥터 사용을 시작합니다.

AWS 액세스 키입니다

필요한 권한이 있는 IAM 사용자를 위해 BlueXP에 AWS 액세스 키를 제공합니다.

단계

1. 현재 BlueXP에서 올바른 커넥터가 선택되어 있는지 확인합니다.
2. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

3. 자격 증명 추가 * 를 선택하고 마법사의 단계를 따릅니다.
   a. * 자격 증명 위치 *: * Amazon Web Services > Connector * 를 선택합니다.
   b. * 자격 증명 정의 *: AWS 액세스 키와 비밀 키를 입력합니다.
   c. * Marketplace 구독 *: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 선택합니다.

결과

BlueXP는 이제 AWS에서 사용자 대신 작업을 수행하는 데 필요한 권한을 가집니다.

로 이동합니다 "BlueXP 콘솔" 을 눌러 BlueXP에서 커넥터 사용을 시작합니다.

Azure를 지원합니다

Azure의 커넥터 설치 옵션

Azure에서 Connector를 만드는 몇 가지 방법이 있습니다. BlueXP에서 직접 연결하는 것이 가장

일반적인 방법입니다.

다음 설치 옵션을 사용할 수 있습니다.

- "BlueXP에서 직접 Connector를 생성합니다" (표준 옵션)

  이 작업은 선택한 VNET에서 Linux 및 Connector 소프트웨어를 실행하는 VM을 시작합니다.

- "Azure Marketplace에서 Connector를 생성합니다"

  이 동작은 Linux 및 Connector 소프트웨어를 실행하는 VM도 시작하지만 BlueXP가 아닌 Azure 마켓플레이스에서 직접 배포가 시작됩니다.

- "자체 Linux 호스트에 소프트웨어를 다운로드하고 수동으로 설치합니다"

선택하는 설치 옵션은 설치 준비 방법에 영향을 줍니다. 여기에는 Azure에서 리소스를 인증하고 관리하는 데 필요한 권한을 BlueXP에 제공하는 방법이 포함됩니다.

BlueXP에서 **Azure**에 커넥터를 만듭니다

BlueXP에서 Azure에서 Connector를 생성하려면 네트워킹을 설정하고 Azure 권한을 준비한 다음 Connector를 생성해야 합니다.

시작하기 전에

을(를) 검토해야 합니다 "커넥터 제한".

단계 **1:** 네트워킹을 설정한다

커넥터를 설치할 네트워크 위치가 다음 요구 사항을 지원하는지 확인합니다. 이러한 요구사항을 충족하면 Connector가 하이브리드 클라우드 환경 내에서 리소스와 프로세스를 관리할 수 있습니다.

Azure 지역

Cloud Volumes ONTAP를 사용하는 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"

VNET 및 서브넷

Connector를 생성할 때 Connector가 상주할 VNET와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

Connector를 사용하려면 작업 환경을 만들고 관리할 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, 온프레미스 환경에서 Cloud Volumes ONTAP 시스템 또는 스토리지 시스템을 생성할 네트워크를 예로 들 수 있습니다.

아웃바운드 인터넷 액세스

커넥터를 배포하는 네트워크 위치에 특정 끝점에 연결하려면 아웃바운드 인터넷 연결이 있어야 합니다.

커넥터에서 접촉된 끝점

Connector는 일상적인 운영을 위해 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하려면 다음 엔드포인트에 연결하는 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 끝점은 모두 CNAME 항목입니다.

엔드포인트	목적
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure 공공 지역의 리소스를 관리합니다.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure 중국 지역의 리소스를 관리합니다.
https://support.netapp.com 으로 문의하십시오 https://mysupport.netapp.com 으로 문의하십시오	라이센스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXP 내에서 SaaS 기능 및 서비스를 제공합니다. 현재 Connector가 "cloudmanager.cloud.netapp.com" 에 문의하고 있지만 곧 출시될 릴리스에서 "api.bluexp.netapp.com" 에 연락하기 시작합니다.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Connector 및 해당 Docker 구성 요소를 업그레이드합니다.

BlueXP 콘솔에서 연결된 엔드포인트에는

SaaS 계층을 통해 제공되는 BlueXP 웹 기반 콘솔을 사용하면 여러 엔드포인트에 접속하여 데이터 관리 작업을 완료합니다. 여기에는 BlueXP 콘솔에서 커넥터를 배포하기 위해 연결된 엔드포인트가 포함됩니다.

"BlueXP 콘솔에서 연결된 엔드포인트 목록을 봅니다".

프록시 서버

조직에서 모든 나가는 인터넷 트래픽에 대해 프록시 서버를 배포해야 하는 경우 HTTP 또는 HTTPS 프록시에 대한 다음 정보를 가져옵니다. 설치하는 동안 이 정보를 제공해야 합니다.

- IP 주소입니다
- 자격 증명
- HTTPS 인증서

BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

포트

커넥터를 시작하거나 커넥터가 Cloud Volumes ONTAP에서 NetApp 지원으로 AutoSupport 메시지를 보내는 프록시로 사용되지 않는 한 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.
- 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 보내기 위한 아웃바운드 인터넷 연결이 없는 경우 BlueXP는 자동으로 해당 시스템이 커넥터에 포함된 프록시 서버를 사용하도록 구성합니다. 유일한 요구 사항은 커넥터 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

NTP를 활성화합니다

BlueXP 분류를 사용하여 회사 데이터 소스를 검사하려는 경우 BlueXP Connector 시스템과 BlueXP 분류 시스템 모두에서 NTP(Network Time Protocol) 서비스를 활성화하여 시스템 간에 시간이 동기화되도록 해야 합니다. "BlueXP 분류에 대해 자세히 알아보십시오"

Connector를 만든 후 이 네트워킹 요구 사항을 구현해야 합니다.

2단계**:** 사용자 지정 역할을 만듭니다

Azure 계정 또는 Microsoft Entra 서비스 보안 주체에 할당할 수 있는 Azure 사용자 지정 역할을 만듭니다. BlueXP는 Azure를 사용하여 인증을 수행하고 이러한 권한을 사용하여 사용자를 대신하여 Connector 인스턴스를 만듭니다.

Azure 포털, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 생성할 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 생성하는 방법을 보여 줍니다. 다른 방법을 사용하려면 을 참조하십시오 "Azure 문서"

단계

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

> 이 사용자 지정 역할에는 BlueXP에서 Azure에서 Connector VM을 실행하는 데 필요한 권한만 포함됩니다. 다른 상황에서는 이 정책을 사용하지 마십시오. BlueXP에서 Connector를 만들면 Connector가 공용 클라우드 환경의 리소스를 관리할 수 있도록 Connector VM에 새로운 권한 집합이 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/agreem
ents/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/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.

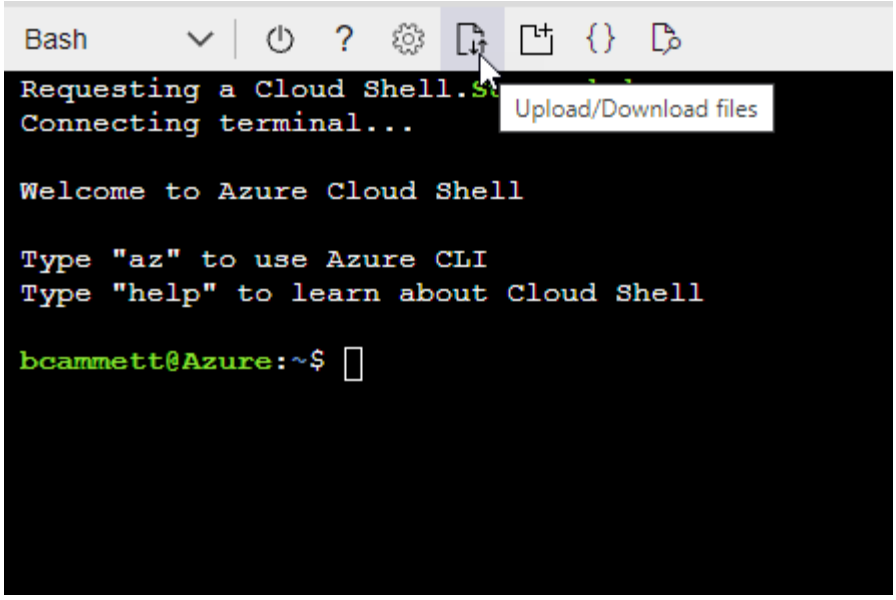
   - 예 *

```
"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. 이제 사용자 계정이나 서비스 보안 주체에 이 사용자 지정 역할을 적용할 수 있습니다.

단계 **3:** 인증을 설정합니다

BlueXP에서 커넥터를 생성할 때 BlueXP가 Azure에서 인증되고 VM을 배포할 수 있도록 로그인을 제공해야 합니다. 두 가지 옵션이 있습니다.

1. 메시지가 표시되면 Azure 계정으로 로그인합니다. 이 계정에는 특정 Azure 권한이 있어야 합니다. 이 옵션이 기본 옵션입니다.
2. Microsoft Entra 서비스 보안 주체에 대한 자세한 정보를 제공합니다. 이 서비스 보안 주체는 특정 권한도 필요합니다.

단계에 따라 BlueXP와 함께 사용할 인증 방법 중 하나를 준비합니다.

Azure 계정

BlueXP에서 커넥터를 배포할 사용자에게 사용자 지정 역할을 할당합니다.

단계

1. Azure 포털에서 * Subscriptions * 서비스를 열고 사용자의 구독을 선택합니다.
2. IAM(액세스 제어) * 을 클릭합니다.
3. Add * > * Add role assignment * 를 클릭한 후 권한을 추가합니다.
   a. 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.

   b. 사용자, 그룹 또는 서비스 보안 주체 * 를 선택한 상태로 유지합니다.
   c. 회원 선택 * 을 클릭하고 사용자 계정을 선택한 다음 * 선택 * 을 클릭합니다.
   d. 다음 * 을 클릭합니다.
   e. 검토 + 할당 * 을 클릭합니다.

결과

이제 Azure 사용자는 BlueXP에서 커넥터를 배포하는 데 필요한 권한을 갖게 됩니다.

서비스 책임자

Azure 계정으로 로그인하는 대신 필요한 권한이 있는 Azure 서비스 보안 주체에 대한 자격 증명을 BlueXP에 제공할 수 있습니다.

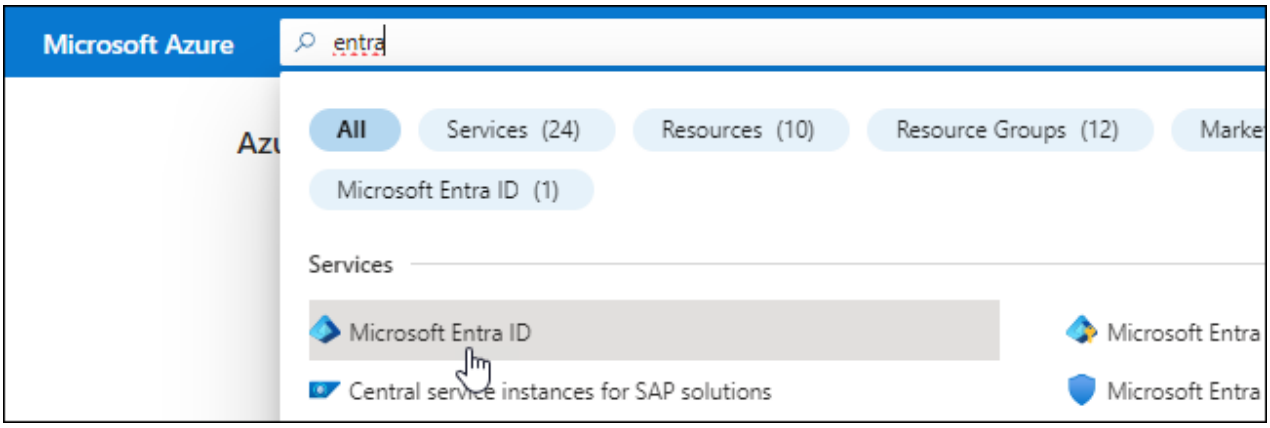
Microsoft Entra ID에서 서비스 주체를 생성 및 설정하고 BlueXP에 필요한 Azure 자격 증명을 받습니다.

역할 기반 액세스 제어를 위한 **Microsoft Entra** 응용 프로그램을 만듭니다

1. Azure에서 Active Directory 응용 프로그램을 만들고 응용 프로그램을 역할에 할당할 수 있는 권한이 있는지 확인합니다.

   자세한 내용은 을 참조하십시오 "Microsoft Azure 문서: 필요한 권한"

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

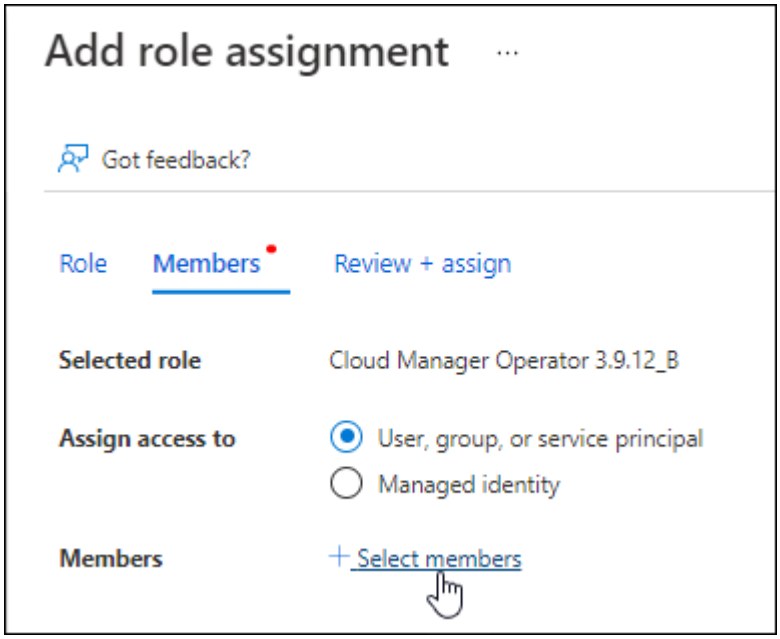


3. 메뉴에서 * 앱 등록 * 을 선택합니다.
4. 새 등록 * 을 선택합니다.
5. 응용 프로그램에 대한 세부 정보를 지정합니다.
   - * 이름 *: 응용 프로그램의 이름을 입력합니다.
   - * 계정 유형 *: 계정 유형을 선택합니다(모두 BlueXP에서 사용 가능).
   - * URI 리디렉션 *: 이 필드는 비워 둘 수 있습니다.
6. Register * 를 선택합니다.

   AD 응용 프로그램 및 서비스 보안 주체를 만들었습니다.

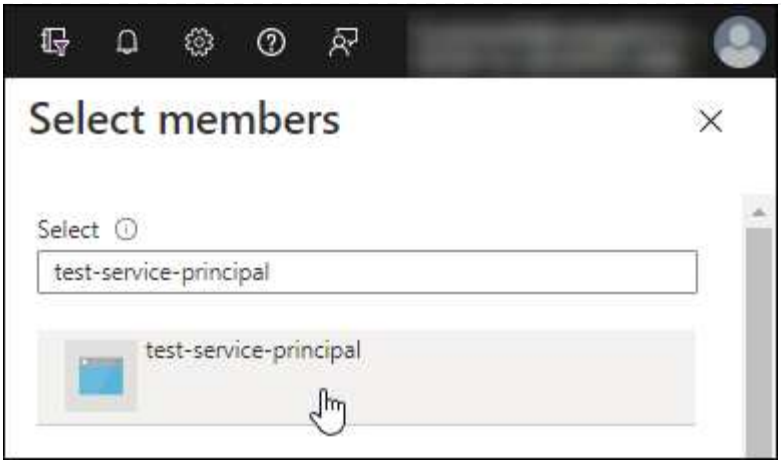
응용 프로그램에 사용자 지정 역할을 할당합니다

1. Azure 포털에서 * Subscriptions * 서비스를 엽니다.
2. 구독을 선택합니다.
3. IAM(Access Control) > 추가 > 역할 할당 추가 * 를 클릭합니다.
4. Role * 탭에서 * BlueXP Operator * 역할을 선택하고 * Next * 를 클릭합니다.
5. Members* 탭에서 다음 단계를 완료합니다.
   a. 사용자, 그룹 또는 서비스 보안 주체 * 를 선택한 상태로 유지합니다.
   b. 구성원 선택 * 을 클릭합니다.



   c. 응용 프로그램의 이름을 검색합니다.

   예를 들면 다음과 같습니다.



a. 응용 프로그램을 선택하고 * 선택 * 을 클릭합니다.

b. 다음 * 을 클릭합니다.

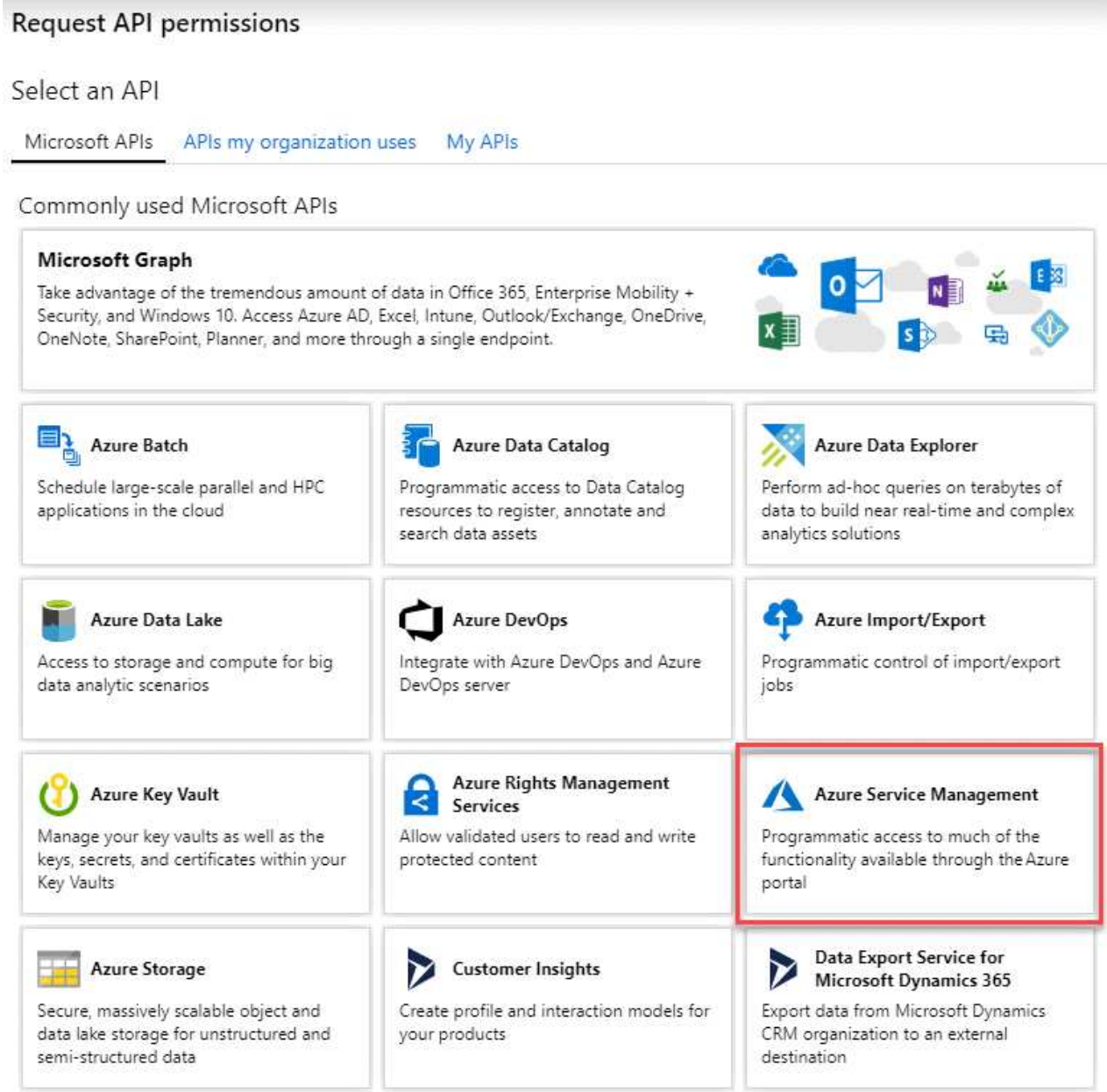
6. 검토 + 할당 * 을 클릭합니다.

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

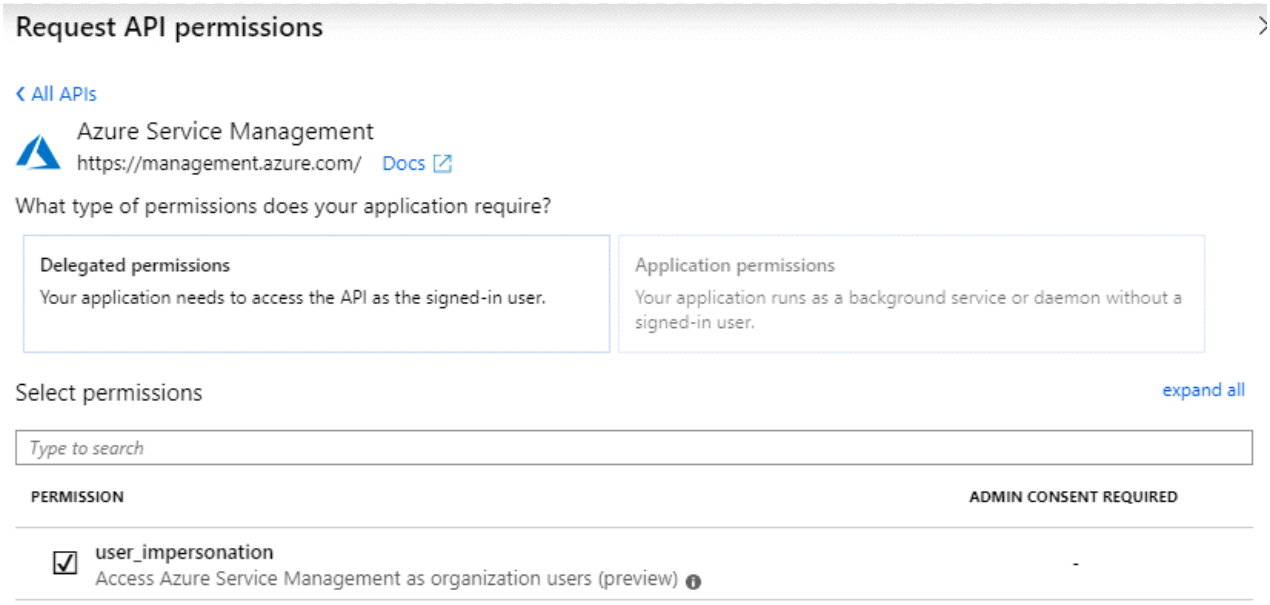
   여러 Azure 구독에서 리소스를 관리하려면 각 구독에 서비스 보안 주체를 바인딩해야 합니다. 예를 들어, BlueXP에서는 Cloud Volumes ONTAP를 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한을 추가합니다

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.

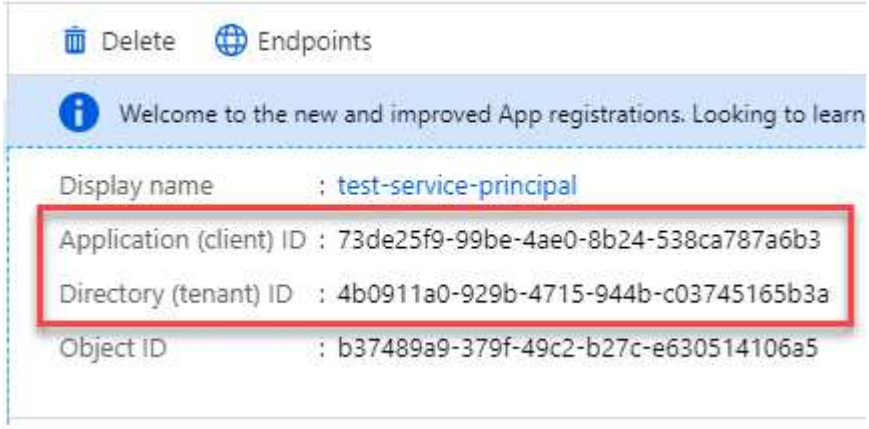


4. Access Azure Service Management as organization users * 를 선택한 다음 * Add permissions * 를 선택합니다.



응용 프로그램의 응용 프로그램 **ID** 및 디렉터리 **ID**를 가져옵니다

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



Azure 계정을 BlueXP에 추가하는 경우 응용 프로그램의 응용 프로그램(클라이언트) ID와 디렉터리(테넌트) ID를 제공해야 합니다. BlueXP는 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 암호를 생성합니다

1. Microsoft Entra ID * 서비스를 엽니다.
2. 앱 등록 * 을 선택하고 응용 프로그램을 선택합니다.
3. 인증서 및 비밀 > 새 클라이언트 비밀 * 을 선택합니다.
4. 비밀과 기간에 대한 설명을 제공하십시오.
5. 추가 * 를 선택합니다.
6. 클라이언트 암호 값을 복사합니다.

이제 BlueXP에서 Microsoft Entra ID를 사용하여 인증하는 클라이언트 암호가 있습니다.

결과

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

4단계**:** 커넥터를 만듭니다

BlueXP 웹 기반 콘솔에서 직접 커넥터를 생성합니다.

이 작업에 대해

BlueXP에서 Connector를 생성하면 기본 구성을 사용하여 Azure에서 가상 머신을 구축할 수 있습니다. Connector를 생성한 후에는 CPU 또는 RAM이 적은 더 작은 VM 유형으로 변경하지 마십시오. "Connector의 기본 설정에 대해 알아봅니다".

시작하기 전에

다음과 같은 항목이 있어야 합니다.

- Azure 구독.
- 선택한 Azure 지역에서 VNET 및 서브넷입니다.
- 프록시 서버에 대한 세부 정보(조직에서 모든 발신 인터넷 트래픽에 대한 프록시를 필요로 하는 경우):
  - IP 주소입니다
  - 자격 증명
  - HTTPS 인증서
- Connector 가상 머신에 해당 인증 방법을 사용하려는 경우 SSH 공개 키입니다. 인증 방법의 다른 옵션은 암호를 사용하는 것입니다.

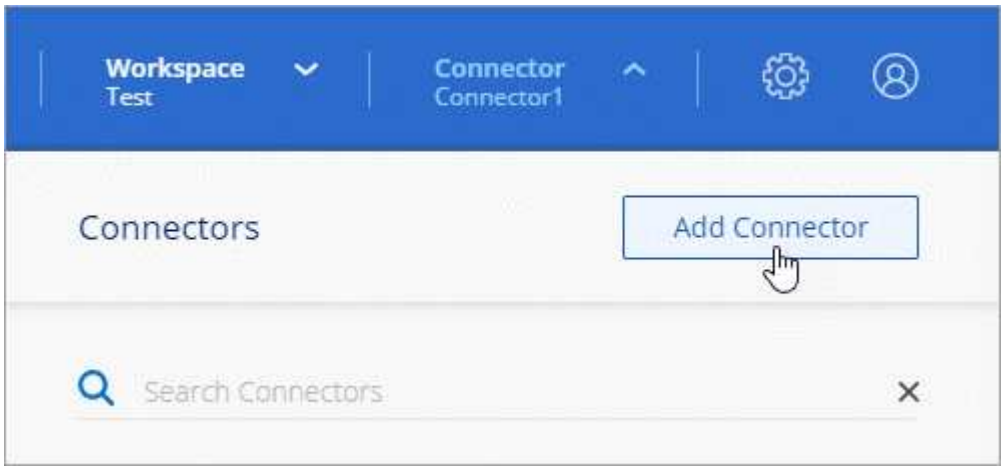
  "Azure에서 Linux VM에 연결하는 방법에 대해 알아보십시오"

- BlueXP에서 Connector에 대한 Azure 역할을 자동으로 생성하지 않으려면 고유한 역할을 만들어야 합니다 "이 페이지의 정책 사용".

  이러한 권한은 Connector 인스턴스 자체에 대한 것입니다. Connector VM을 배포하기 위해 이전에 설정한 것과 다른 권한 집합입니다.

단계

1. 커넥터 * 드롭다운을 선택하고 * 커넥터 추가 * 를 선택합니다.



2. 클라우드 공급자로 * Microsoft Azure * 를 선택합니다.
3. 커넥터 배포 * 페이지에서 다음을 수행합니다.

   a. Authentication * 에서 Azure 권한 설정 방법과 일치하는 인증 옵션을 선택합니다.

      - 필요한 권한이 있는 Microsoft 계정에 로그인하려면 * Azure 사용자 계정 * 을 선택합니다.

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

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

      - 필요한 권한을 부여하는 Microsoft Entra 서비스 보안 주체에 대한 정보를 입력하려면 * Active Directory 서비스 주체 * 를 선택합니다.
        - 애플리케이션(클라이언트) ID입니다
        - 디렉토리(테넌트) ID입니다
        - 클라이언트 암호

   서비스 보안 주체에 대해 이러한 값을 가져오는 방법에 대해 알아봅니다.

4. 마법사의 단계에 따라 커넥터를 작성합니다.

   - * VM 인증 *: Azure 구독, 위치, 새 리소스 그룹 또는 기존 리소스 그룹을 선택한 다음 만들려는 Connector 가상 머신에 대한 인증 방법을 선택합니다.

     가상 머신의 인증 방법은 암호 또는 SSH 공개 키일 수 있습니다.

   "Azure에서 Linux VM에 연결하는 방법에 대해 알아보십시오"

   - * 세부 정보 *: 인스턴스의 이름을 입력하고 태그를 지정한 다음 BlueXP에서 필요한 권한이 있는 새 역할을 생성할지 또는 로 설정한 기존 역할을 선택할지 여부를 선택합니다 "필요한 권한".

     이 역할과 연결된 Azure 구독을 선택할 수 있습니다. 선택한 각 구독은 해당 구독의 리소스를 관리하는 커넥터 권한을 제공합니다(예: Cloud Volumes ONTAP).

   - * 네트워크 *: VNET 및 서브넷을 선택하고, 공용 IP 주소를 활성화할지 여부를 선택한 다음 선택적으로 프록시 구성을 지정합니다.

- * 보안 그룹 *: 새 보안 그룹을 생성할지 또는 필요한 인바운드 및 아웃바운드 규칙을 허용하는 기존 보안 그룹을 선택할지 여부를 선택합니다.

  "Azure의 보안 그룹 규칙을 봅니다".

- * 검토 *: 선택 사항을 검토하여 설정이 올바른지 확인합니다.

5. 추가 * 를 클릭합니다.

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

결과

프로세스가 완료되면 BlueXP에서 커넥터를 사용할 수 있습니다.

Connector를 생성한 동일한 Azure 구독에 Azure Blob 스토리지가 있는 경우 BlueXP 캔버스에 Azure Blob 스토리지 작업 환경이 자동으로 표시됩니다. "BlueXP에서 Azure Blob 스토리지를 관리하는 방법에 관해 알아보십시오"

Azure Marketplace에서 **Connector**를 생성합니다

Azure 마켓플레이스에서 Connector를 만들려면 네트워킹을 설정하고 Azure 권한을 준비하고 인스턴스 요구 사항을 검토한 다음 Connector를 만들어야 합니다.

시작하기 전에

을(를) 검토해야 합니다 "커넥터 제한".

단계 **1:** 네트워킹을 설정한다

커넥터를 설치할 네트워크 위치가 다음 요구 사항을 지원하는지 확인합니다. 이러한 요구사항을 충족하면 Connector가 하이브리드 클라우드 환경 내에서 리소스와 프로세스를 관리할 수 있습니다.

Azure 지역

Cloud Volumes ONTAP를 사용하는 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"

VNET 및 서브넷

Connector를 생성할 때 Connector가 상주할 VNET와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

Connector를 사용하려면 작업 환경을 만들고 관리할 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, 온프레미스 환경에서 Cloud Volumes ONTAP 시스템 또는 스토리지 시스템을 생성할 네트워크를 예로 들 수 있습니다.

아웃바운드 인터넷 액세스

커넥터를 배포하는 네트워크 위치에 특정 끝점에 연결하려면 아웃바운드 인터넷 연결이 있어야 합니다.

커넥터에서 접촉된 끝점

Connector는 일상적인 운영을 위해 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하려면 다음

엔드포인트에 연결하는 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 끝점은 모두 CNAME 항목입니다.

엔드포인트	목적
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure 공공 지역의 리소스를 관리합니다.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure 중국 지역의 리소스를 관리합니다.
https://support.netapp.com 으로 문의하십시오 https://mysupport.netapp.com 으로 문의하십시오	라이센스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXP 내에서 SaaS 기능 및 서비스를 제공합니다. 현재 Connector가 "cloudmanager.cloud.netapp.com" 에 문의하고 있지만 곧 출시될 릴리스에서 "api.bluexp.netapp.com" 에 연락하기 시작합니다.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Connector 및 해당 Docker 구성 요소를 업그레이드합니다.

프록시 서버

조직에서 모든 나가는 인터넷 트래픽에 대해 프록시 서버를 배포해야 하는 경우 HTTP 또는 HTTPS 프록시에 대한 다음 정보를 가져옵니다. 설치하는 동안 이 정보를 제공해야 합니다.

- IP 주소입니다
- 자격 증명
- HTTPS 인증서

BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

포트

커넥터를 시작하거나 커넥터가 Cloud Volumes ONTAP에서 NetApp 지원으로 AutoSupport 메시지를 보내는 프록시로 사용되지 않는 한 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.
- 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 보내기 위한 아웃바운드 인터넷 연결이 없는 경우 BlueXP는 자동으로 해당 시스템이 커넥터에 포함된 프록시 서버를 사용하도록 구성합니다. 유일한 요구 사항은 커넥터 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

NTP를 활성화합니다

BlueXP 분류를 사용하여 회사 데이터 소스를 검사하려는 경우 BlueXP Connector 시스템과 BlueXP 분류 시스템 모두에서 NTP(Network Time Protocol) 서비스를 활성화하여 시스템 간에 시간이 동기화되도록 해야 합니다. "BlueXP 분류에 대해 자세히 알아보십시오"

Connector를 만든 후 이 네트워킹 요구 사항을 구현해야 합니다.

2단계**: VM** 요구 사항 검토

Connector를 생성할 때 다음 요구 사항을 충족하는 가상 머신 유형을 선택해야 합니다.

CPU

코어 4개 또는 vCPU 4개

RAM

14GB

Azure VM 크기입니다

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

3단계**:** 사용 권한 설정

다음과 같은 방법으로 사용 권한을 제공할 수 있습니다.

- 옵션 1: 시스템에서 할당한 관리 ID를 사용하여 Azure VM에 사용자 지정 역할을 할당합니다.
- 옵션 2: 필요한 권한이 있는 Azure 서비스 보안 주체에 대한 자격 증명을 BlueXP에 제공합니다.

BlueXP 권한을 설정하려면 다음 단계를 따르십시오.

사용자 지정 역할

Azure 포털, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 생성할 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 생성하는 방법을 보여 줍니다. 다른 방법을 사용하려면 을 참조하십시오 "Azure 문서"

단계

1. 소프트웨어를 자체 호스트에 수동으로 설치하려는 경우 사용자 지정 역할을 통해 필요한 Azure 권한을 제공할 수 있도록 VM에서 시스템에서 할당한 관리 ID를 사용하도록 설정합니다.

   "Microsoft Azure 설명서: Azure 포털을 사용하여 VM의 Azure 리소스에 대해 관리되는 ID를 구성합니다"

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

   BlueXP에서 사용할 각 Azure 구독에 대한 ID를 추가해야 합니다.

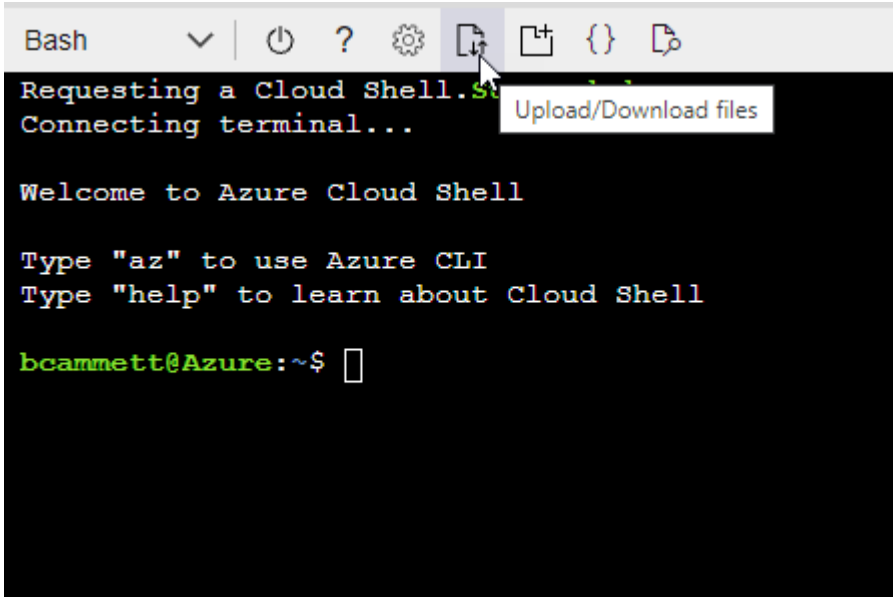
   - 예 *

```
"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 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. Azure CLI를 사용하여 사용자 지정 역할을 생성합니다.

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

결과

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

서비스 책임자

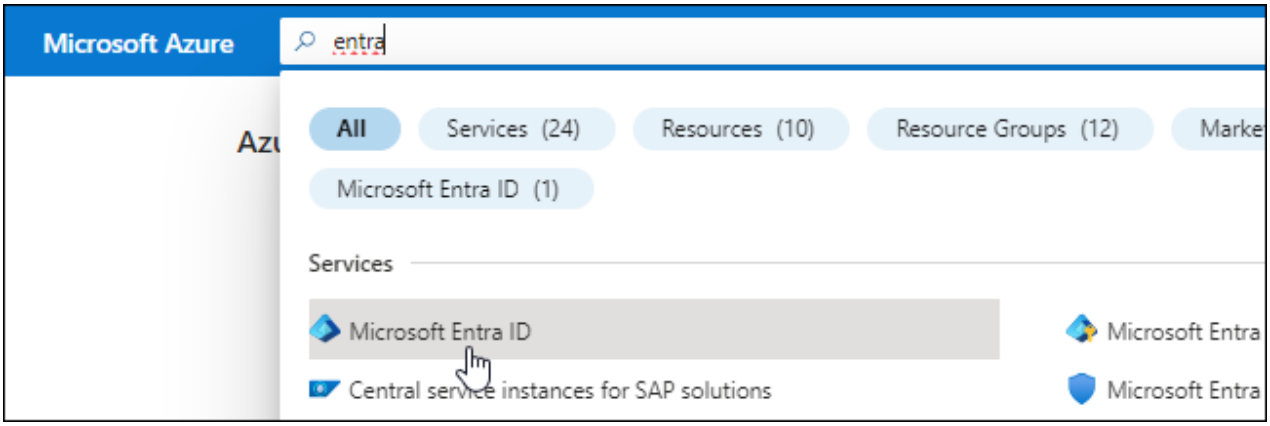
Microsoft Entra ID에서 서비스 주체를 생성 및 설정하고 BlueXP에 필요한 Azure 자격 증명을 받습니다.

역할 기반 액세스 제어를 위한 **Microsoft Entra** 응용 프로그램을 만듭니다

1. Azure에서 Active Directory 응용 프로그램을 만들고 응용 프로그램을 역할에 할당할 수 있는 권한이 있는지 확인합니다.

   자세한 내용은 을 참조하십시오 "Microsoft Azure 문서: 필요한 권한"

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



3. 메뉴에서 * 앱 등록 * 을 선택합니다.
4. 새 등록 * 을 선택합니다.
5. 응용 프로그램에 대한 세부 정보를 지정합니다.
   - * 이름 *: 응용 프로그램의 이름을 입력합니다.
   - * 계정 유형 *: 계정 유형을 선택합니다(모두 BlueXP에서 사용 가능).
   - * URI 리디렉션 *: 이 필드는 비워 둘 수 있습니다.
6. Register * 를 선택합니다.

   AD 응용 프로그램 및 서비스 보안 주체를 만들었습니다.

애플리케이션에 역할을 할당합니다

1. 사용자 지정 역할 만들기:

   Azure 포털, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 생성할 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 생성하는 방법을 보여 줍니다. 다른 방법을

사용하려면 을 참조하십시오 "Azure 문서"

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.

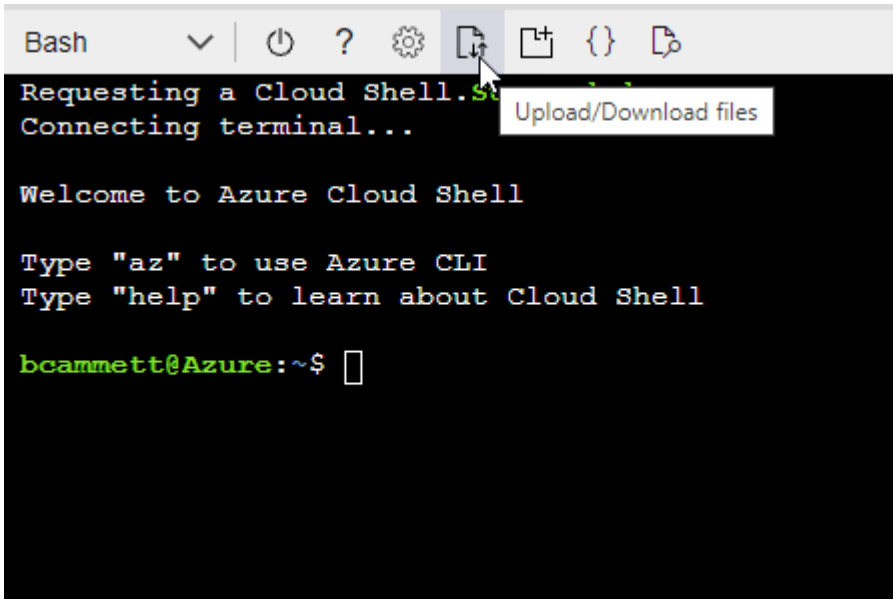
- 예 *

```
"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.



- Azure CLI를 사용하여 사용자 지정 역할을 생성합니다.

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

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

2. 역할에 응용 프로그램을 할당합니다.

a. Azure 포털에서 * Subscriptions * 서비스를 엽니다.

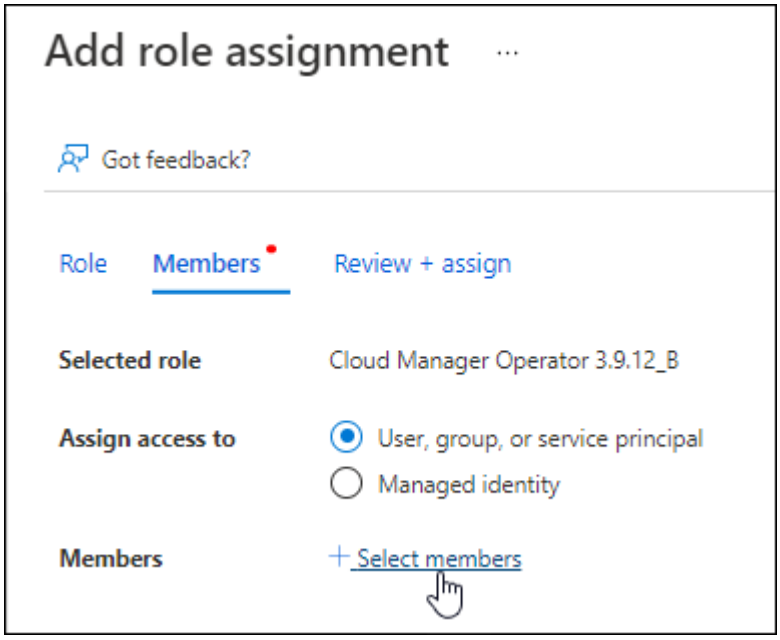
b. 구독을 선택합니다.

c. 액세스 제어(IAM) > 추가 > 역할 할당 추가 * 를 선택합니다.

d. Role * 탭에서 * BlueXP Operator * 역할을 선택하고 * Next * 를 선택합니다.

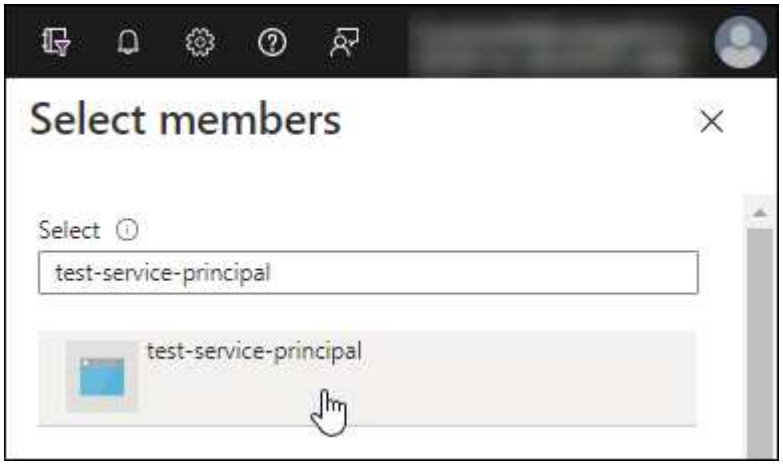
e. Members* 탭에서 다음 단계를 완료합니다.

- 사용자, 그룹 또는 서비스 보안 주체 * 를 선택한 상태로 유지합니다.
- 구성원 선택 * 을 선택합니다.



- 응용 프로그램의 이름을 검색합니다.

  예를 들면 다음과 같습니다.



- 응용 프로그램을 선택하고 * 선택 * 을 선택합니다.
- 다음 * 을 선택합니다.

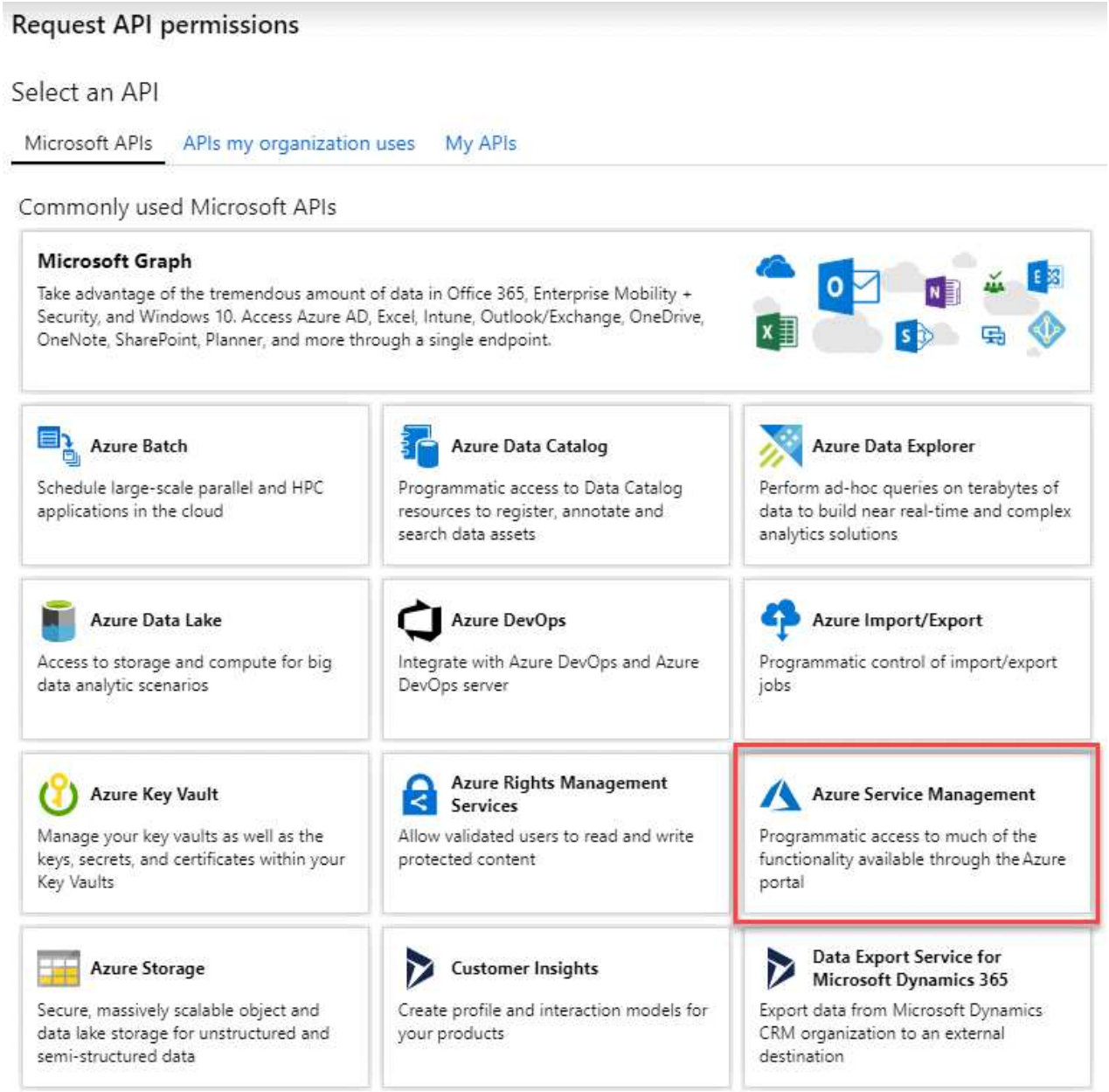
f. 검토 + 할당 * 을 선택합니다.

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

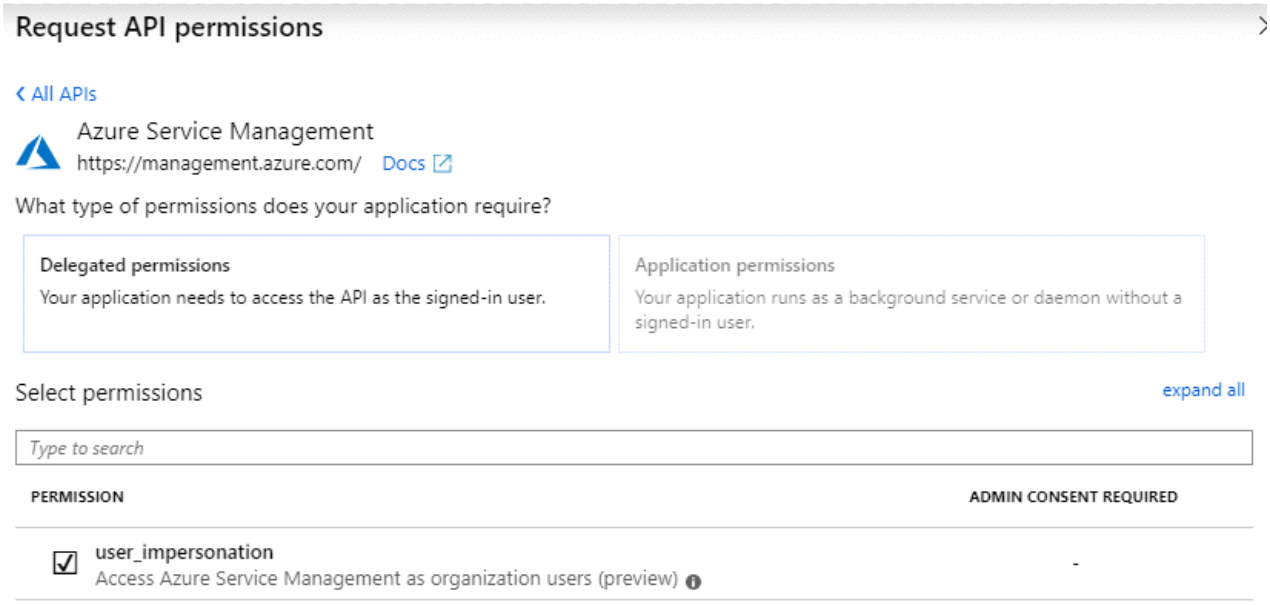
여러 Azure 구독에서 Cloud Volumes ONTAP를 배포하려면 서비스 보안 주체를 해당 구독 각각에 바인딩해야 합니다. BlueXP를 사용하면 Cloud Volumes ONTAP를 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한을 추가합니다

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.

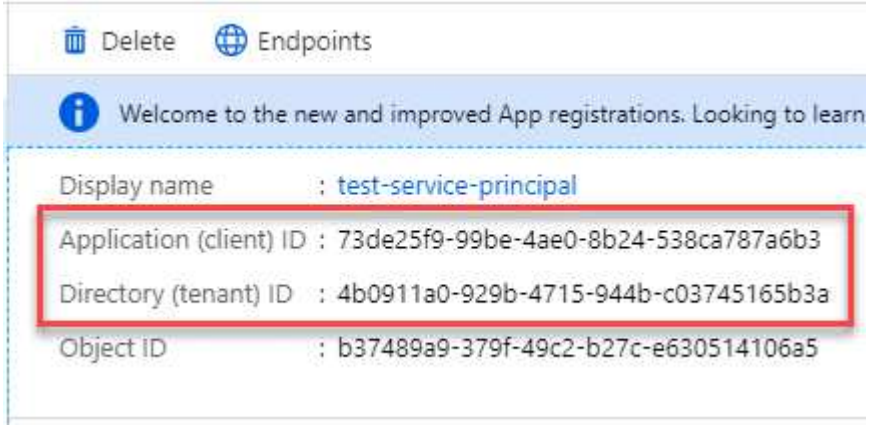


4. Access Azure Service Management as organization users * 를 선택한 다음 * Add permissions * 를 선택합니다.



응용 프로그램의 응용 프로그램 **ID** 및 디렉터리 **ID**를 가져옵니다

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



Azure 계정을 BlueXP에 추가하는 경우 응용 프로그램의 응용 프로그램(클라이언트) ID와 디렉터리(테넌트) ID를 제공해야 합니다. BlueXP는 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 암호를 생성합니다

1. Microsoft Entra ID * 서비스를 엽니다.
2. 앱 등록 * 을 선택하고 응용 프로그램을 선택합니다.
3. 인증서 및 비밀 > 새 클라이언트 비밀 * 을 선택합니다.
4. 비밀과 기간에 대한 설명을 제공하십시오.
5. 추가 * 를 선택합니다.
6. 클라이언트 암호 값을 복사합니다.

이제 BlueXP에서 Microsoft Entra ID를 사용하여 인증하는 클라이언트 암호가 있습니다.

결과

이제 서비스 보안 주체가 설정되었으므로 응용 프로그램(클라이언트) ID, 디렉터리(테넌트) ID 및 클라이언트 암호 값을 복사해야 합니다. Azure 계정을 추가할 때 BlueXP에 이 정보를 입력해야 합니다.

4단계**:** 커넥터를 만듭니다

Azure 마켓플레이스에서 직접 Connector를 실행합니다.

이 작업에 대해

Azure Marketplace에서 Connector를 생성하면 Azure에서 기본 구성을 사용하여 가상 머신을 구축할 수 있습니다. "Connector의 기본 설정에 대해 알아봅니다".

시작하기 전에

다음과 같은 항목이 있어야 합니다.

- Azure 구독.
- 선택한 Azure 지역에서 VNET 및 서브넷입니다.
- 프록시 서버에 대한 세부 정보(조직에서 모든 발신 인터넷 트래픽에 대한 프록시를 필요로 하는 경우):
  - IP 주소입니다
  - 자격 증명
  - HTTPS 인증서
- Connector 가상 머신에 해당 인증 방법을 사용하려는 경우 SSH 공개 키입니다. 인증 방법의 다른 옵션은 암호를 사용하는 것입니다.

  "Azure에서 Linux VM에 연결하는 방법에 대해 알아보십시오"

- BlueXP에서 Connector에 대한 Azure 역할을 자동으로 생성하지 않으려면 고유한 역할을 만들어야 합니다 "이 페이지의 정책 사용".

  이러한 권한은 Connector 인스턴스 자체에 대한 것입니다. Connector VM을 배포하기 위해 이전에 설정한 것과 다른 권한 집합입니다.

단계

1. Azure 마켓플레이스에서 NetApp Connector VM 페이지로 이동합니다.

"상용 지역에 대한 Azure Marketplace 페이지"

2. 지금 받기 * 를 선택한 다음 * 계속 * 을 선택합니다.
3. Azure 포털에서 * Create * 를 선택하고 다음 단계에 따라 가상 머신을 구성합니다.

   VM을 구성할 때 다음 사항에 유의하십시오.

   - * VM 크기 *: CPU 및 RAM 요구 사항에 맞는 VM 크기를 선택합니다. DS3 v2를 권장합니다.
   - * 디스크 *: 커넥터는 HDD 또는 SSD 디스크를 사용하여 최적의 성능을 발휘할 수 있습니다.
   - * 네트워크 보안 그룹 *: Connector는 SSH, HTTP 및 HTTPS를 사용하는 인바운드 연결을 필요로 합니다.

     "Azure의 보안 그룹 규칙을 봅니다".

   - * ID *: * Management * 에서 * 시스템에서 할당한 관리 ID 활성화 * 를 선택합니다.

     이 설정은 관리되는 ID를 통해 Connector 가상 컴퓨터가 자격 증명을 제공하지 않고 Microsoft Entra ID를 식별할 수 있기 때문에 중요합니다. "Azure 리소스의 관리 ID에 대해 자세히 알아보십시오".

4. Review + create * 페이지에서 선택 사항을 검토하고 * Create * 를 선택하여 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.

   https://ipaddress

6. 로그인한 후 Connector를 설정합니다.
   a. Connector와 연결할 BlueXP 계정을 지정합니다.
   b. 시스템의 이름을 입력합니다.
   c. 에서 * 보안 환경에서 실행 중입니까? * 제한된 모드를 사용하지 않도록 설정합니다.

      이 단계에서는 표준 모드에서 BlueXP를 사용하는 방법을 설명하므로 제한된 모드를 사용하지 않도록 설정해야 합니다. 보안 환경이 있고 BlueXP 백엔드 서비스에서 이 계정의 연결을 끊으려면 제한된 모드만 활성화해야 합니다. 그렇다면 "제한된 모드에서 BlueXP를 시작하려면 다음 단계를 따르십시오".

   d. Let's start * 를 선택합니다.

결과

이제 커넥터가 설치되어 BlueXP 계정으로 설정됩니다.

Connector를 생성한 동일한 Azure 구독에 Azure Blob 스토리지가 있는 경우 BlueXP 캔버스에 Azure Blob 스토리지 작업 환경이 자동으로 표시됩니다. "BlueXP에서 Azure Blob 스토리지를 관리하는 방법에 관해 알아보십시오"

5단계**: BlueXP**에 권한 제공

커넥터를 생성했으므로 이제 이전에 설정한 권한을 BlueXP에 제공해야 합니다. 권한을 제공하면 BlueXP가 Azure에서 데이터 및 스토리지 인프라를 관리할 수 있습니다.

사용자 지정 역할

Azure 포털로 이동하여 하나 이상의 구독에 대해 Connector 가상 머신에 Azure 사용자 지정 역할을 할당합니다.

단계

1. Azure Portal에서 * Subscriptions * 서비스를 열고 구독을 선택합니다.

   구독 수준에서의 역할 할당 범위를 지정하므로 * 구독 * 서비스에서 역할을 할당하는 것이 중요합니다. scope _ 는 액세스가 적용되는 리소스 집합을 정의합니다. 범위를 다른 수준(예: 가상 머신 레벨)으로 지정하면 BlueXP 내에서 작업을 완료하는 데 영향을 줍니다.

   "Microsoft Azure 설명서: Azure RBAC의 범위를 이해합니다"

2. IAM(액세스 제어) * > * 추가 * > * 역할 할당 추가 * 를 선택합니다.
3. Role * 탭에서 * BlueXP Operator * 역할을 선택하고 * Next * 를 선택합니다.

   BlueXP 오퍼레이터는 BlueXP 정책에 제공된 기본 이름입니다. 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

4. Members* 탭에서 다음 단계를 완료합니다.
   a. 관리되는 ID*에 대한 액세스를 할당합니다.
   b. 구성원 선택 * 을 선택하고 커넥터 가상 시스템이 생성된 구독을 선택한 다음 * 관리 ID * 에서 * 가상 머신 * 을 선택한 다음 커넥터 가상 머신을 선택합니다.
   c. 선택 * 을 선택합니다.
   d. 다음 * 을 선택합니다.
   e. 검토 + 할당 * 을 선택합니다.
   f. 추가 Azure 구독에서 리소스를 관리하려면 해당 구독으로 전환한 다음 이 단계를 반복합니다.

결과

이제 BlueXP는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 가지고 있습니다.

다음 단계

로 이동합니다 "BlueXP 콘솔" 을 눌러 BlueXP에서 커넥터 사용을 시작합니다.

서비스 책임자

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

2. 자격 증명 추가 * 를 선택하고 마법사의 단계를 따릅니다.
   a. * 자격 증명 위치 *: * Microsoft Azure > 커넥터 * 를 선택합니다.
   b. * 자격 증명 정의 *: 필요한 권한을 부여하는 Microsoft Entra 서비스 보안 주체에 대한 정보를 입력합니다.

- 애플리케이션(클라이언트) ID입니다
- 디렉토리(테넌트) ID입니다
- 클라이언트 암호

c. * Marketplace 구독 *: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.

d. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 선택합니다.

결과

이제 BlueXP는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 가지고 있습니다.

Azure에서 커넥터를 수동으로 설치합니다

자신의 Linux 호스트에 Connector를 수동으로 설치하려면 호스트 요구 사항을 검토하고 네트워킹을 설정하고 Azure 사용 권한을 준비하고 커넥터를 설치한 다음 준비한 사용 권한을 제공해야 합니다.

시작하기 전에

을(를) 검토해야 합니다 "커넥터 제한".

1단계**:** 호스트 요구 사항을 검토합니다

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

전용 호스트

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

지원되는 운영 체제

- 우분투 22.04 LTS
- CentOS 7.6, 7.7, 7.8 및 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 및 7.9

  호스트는 Red Hat Subscription Management에 등록되어 있어야 합니다. 등록되지 않은 경우 호스트는 Connector 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.

  Connector는 이러한 운영 체제의 영어 버전에서 지원됩니다.

하이퍼바이저

Ubuntu, CentOS 또는 Red Hat Enterprise Linux 실행 인증을 받은 베어 메탈 또는 호스팅된 하이퍼바이저가 필요합니다.

"Red Hat 솔루션: Red Hat Enterprise Linux 실행 인증을 받은 하이퍼바이저는 무엇입니까?"

CPU

코어 4개 또는 vCPU 4개

RAM

14GB

Azure VM 크기입니다

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

/opt의 디스크 공간입니다

100GiB의 공간을 사용할 수 있어야 합니다

/var의 디스크 공간입니다

20GiB의 공간을 사용할 수 있어야 합니다

Docker 엔진

Connector를 설치하기 전에 Docker 엔진이 호스트에 필요합니다.

- 지원되는 최소 버전은 19.3.1입니다.
- 지원되는 최대 버전은 25.0.5입니다.

"설치 지침을 봅니다"

2단계**:** 네트워킹을 설정한다

커넥터를 설치할 네트워크 위치가 다음 요구 사항을 지원하는지 확인합니다. 이러한 요구사항을 충족하면 Connector가 하이브리드 클라우드 환경 내에서 리소스와 프로세스를 관리할 수 있습니다.

Azure 지역

Cloud Volumes ONTAP를 사용하는 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"

대상 네트워크에 대한 연결

Connector를 사용하려면 작업 환경을 만들고 관리할 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, 온프레미스 환경에서 Cloud Volumes ONTAP 시스템 또는 스토리지 시스템을 생성할 네트워크를 예로 들 수 있습니다.

아웃바운드 인터넷 액세스

커넥터를 배포하는 네트워크 위치에 특정 끝점에 연결하려면 아웃바운드 인터넷 연결이 있어야 합니다.

수동 설치 중에 연결된 끝점입니다

자체 Linux 호스트에 커넥터를 수동으로 설치할 경우 Connector 설치 과정에서 다음 URL에 액세스해야 합니다.

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com

- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

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

커넥터에서 접촉된 끝점

Connector는 일상적인 운영을 위해 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하려면 다음 엔드포인트에 연결하는 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 끝점은 모두 CNAME 항목입니다.

엔드포인트	목적
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure 공공 지역의 리소스를 관리합니다.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure 중국 지역의 리소스를 관리합니다.
https://support.netapp.com 으로 문의하십시오 https://mysupport.netapp.com 으로 문의하십시오	라이센스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXP 내에서 SaaS 기능 및 서비스를 제공합니다. 현재 Connector가 "cloudmanager.cloud.netapp.com" 에 문의하고 있지만 곧 출시될 릴리스에서 "api.bluexp.netapp.com" 에 연락하기 시작합니다.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Connector 및 해당 Docker 구성 요소를 업그레이드합니다.

프록시 서버

조직에서 모든 나가는 인터넷 트래픽에 대해 프록시 서버를 배포해야 하는 경우 HTTP 또는 HTTPS 프록시에 대한 다음 정보를 가져옵니다. 설치하는 동안 이 정보를 제공해야 합니다.

- IP 주소입니다

- 자격 증명
- HTTPS 인증서

BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

포트

커넥터를 시작하거나 커넥터가 Cloud Volumes ONTAP에서 NetApp 지원으로 AutoSupport 메시지를 보내는 프록시로 사용되지 않는 한 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.
- 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 보내기 위한 아웃바운드 인터넷 연결이 없는 경우 BlueXP는 자동으로 해당 시스템이 커넥터에 포함된 프록시 서버를 사용하도록 구성합니다. 유일한 요구 사항은 커넥터 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

NTP를 활성화합니다

BlueXP 분류를 사용하여 회사 데이터 소스를 검사하려는 경우 BlueXP Connector 시스템과 BlueXP 분류 시스템 모두에서 NTP(Network Time Protocol) 서비스를 활성화하여 시스템 간에 시간이 동기화되도록 해야 합니다. "BlueXP 분류에 대해 자세히 알아보십시오"

3단계**:** 사용 권한 설정

다음 옵션 중 하나를 사용하여 BlueXP에 Azure 권한을 제공해야 합니다.

- 옵션 1: 시스템에서 할당한 관리 ID를 사용하여 Azure VM에 사용자 지정 역할을 할당합니다.
- 옵션 2: 필요한 권한이 있는 Azure 서비스 보안 주체에 대한 자격 증명을 BlueXP에 제공합니다.

단계에 따라 BlueXP 권한을 준비합니다.

사용자 지정 역할

Azure 포털, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 생성할 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 생성하는 방법을 보여 줍니다. 다른 방법을 사용하려면 을 참조하십시오 "Azure 문서"

단계

1. 소프트웨어를 자체 호스트에 수동으로 설치하려는 경우 사용자 지정 역할을 통해 필요한 Azure 권한을 제공할 수 있도록 VM에서 시스템에서 할당한 관리 ID를 사용하도록 설정합니다.

   "Microsoft Azure 설명서: Azure 포털을 사용하여 VM의 Azure 리소스에 대해 관리되는 ID를 구성합니다"

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

   BlueXP에서 사용할 각 Azure 구독에 대한 ID를 추가해야 합니다.

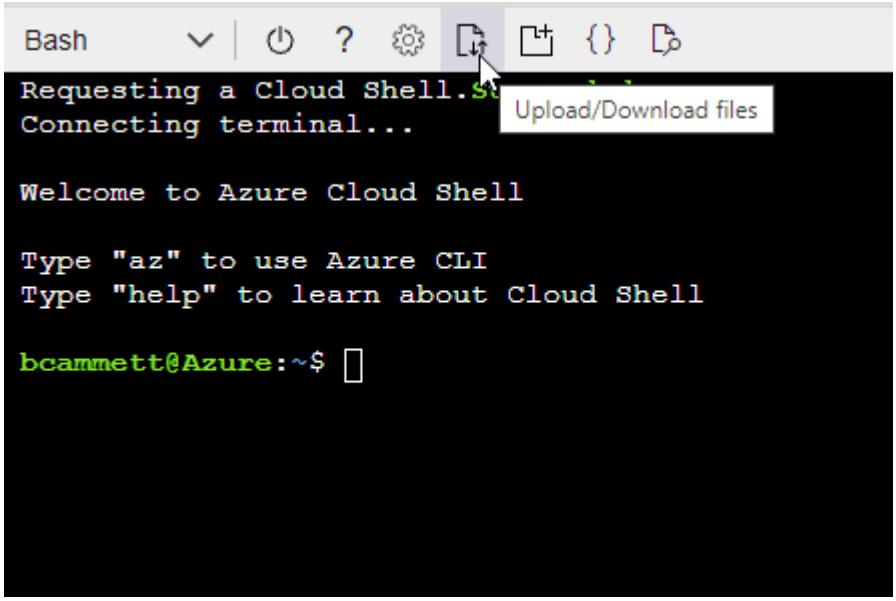
   - 예 *

```
"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 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. Azure CLI를 사용하여 사용자 지정 역할을 생성합니다.

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

결과

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

서비스 책임자

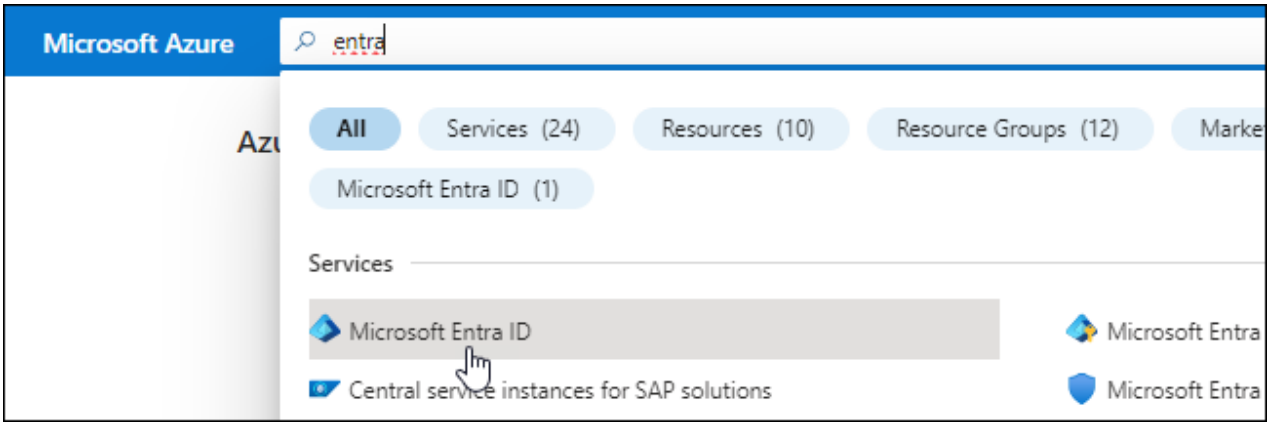
Microsoft Entra ID에서 서비스 주체를 생성 및 설정하고 BlueXP에 필요한 Azure 자격 증명을 받습니다.

역할 기반 액세스 제어를 위한 **Microsoft Entra** 응용 프로그램을 만듭니다

1. Azure에서 Active Directory 응용 프로그램을 만들고 응용 프로그램을 역할에 할당할 수 있는 권한이 있는지 확인합니다.

   자세한 내용은 을 참조하십시오 "Microsoft Azure 문서: 필요한 권한"

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



3. 메뉴에서 * 앱 등록 * 을 선택합니다.
4. 새 등록 * 을 선택합니다.
5. 응용 프로그램에 대한 세부 정보를 지정합니다.
   - * 이름 *: 응용 프로그램의 이름을 입력합니다.
   - * 계정 유형 *: 계정 유형을 선택합니다(모두 BlueXP에서 사용 가능).
   - * URI 리디렉션 *: 이 필드는 비워 둘 수 있습니다.
6. Register * 를 선택합니다.

   AD 응용 프로그램 및 서비스 보안 주체를 만들었습니다.

애플리케이션에 역할을 할당합니다

1. 사용자 지정 역할 만들기:

   Azure 포털, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 생성할 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 생성하는 방법을 보여 줍니다. 다른 방법을

사용하려면 을 참조하십시오 "Azure 문서"

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.

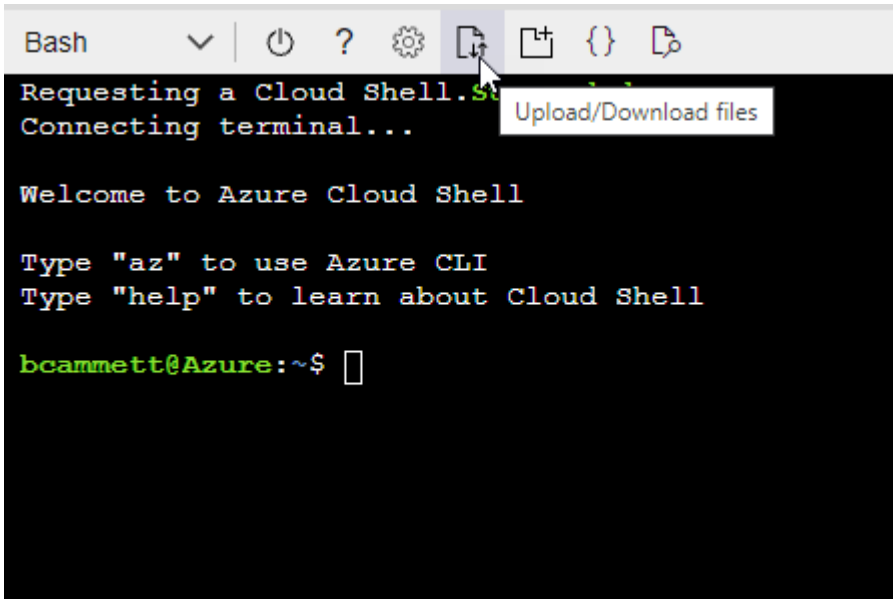
- 예 *

```
"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.



- Azure CLI를 사용하여 사용자 지정 역할을 생성합니다.

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

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

2. 역할에 응용 프로그램을 할당합니다.

a. Azure 포털에서 * Subscriptions * 서비스를 엽니다.

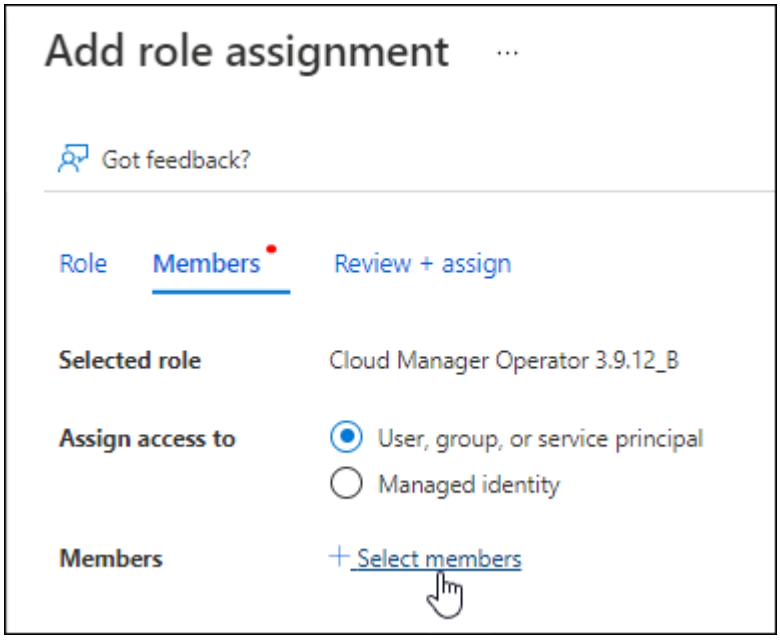
b. 구독을 선택합니다.

c. 액세스 제어(IAM) > 추가 > 역할 할당 추가 * 를 선택합니다.

d. Role * 탭에서 * BlueXP Operator * 역할을 선택하고 * Next * 를 선택합니다.

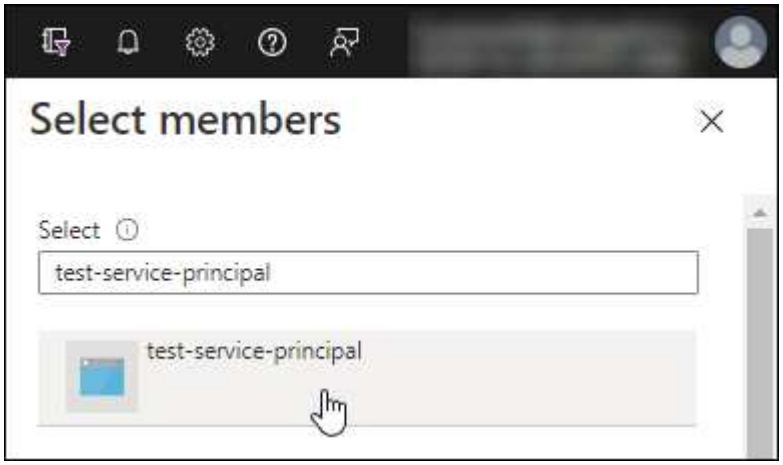
e. Members* 탭에서 다음 단계를 완료합니다.

- 사용자, 그룹 또는 서비스 보안 주체 * 를 선택한 상태로 유지합니다.
- 구성원 선택 * 을 선택합니다.



- 응용 프로그램의 이름을 검색합니다.

  예를 들면 다음과 같습니다.



- 응용 프로그램을 선택하고 * 선택 * 을 선택합니다.
- 다음 * 을 선택합니다.

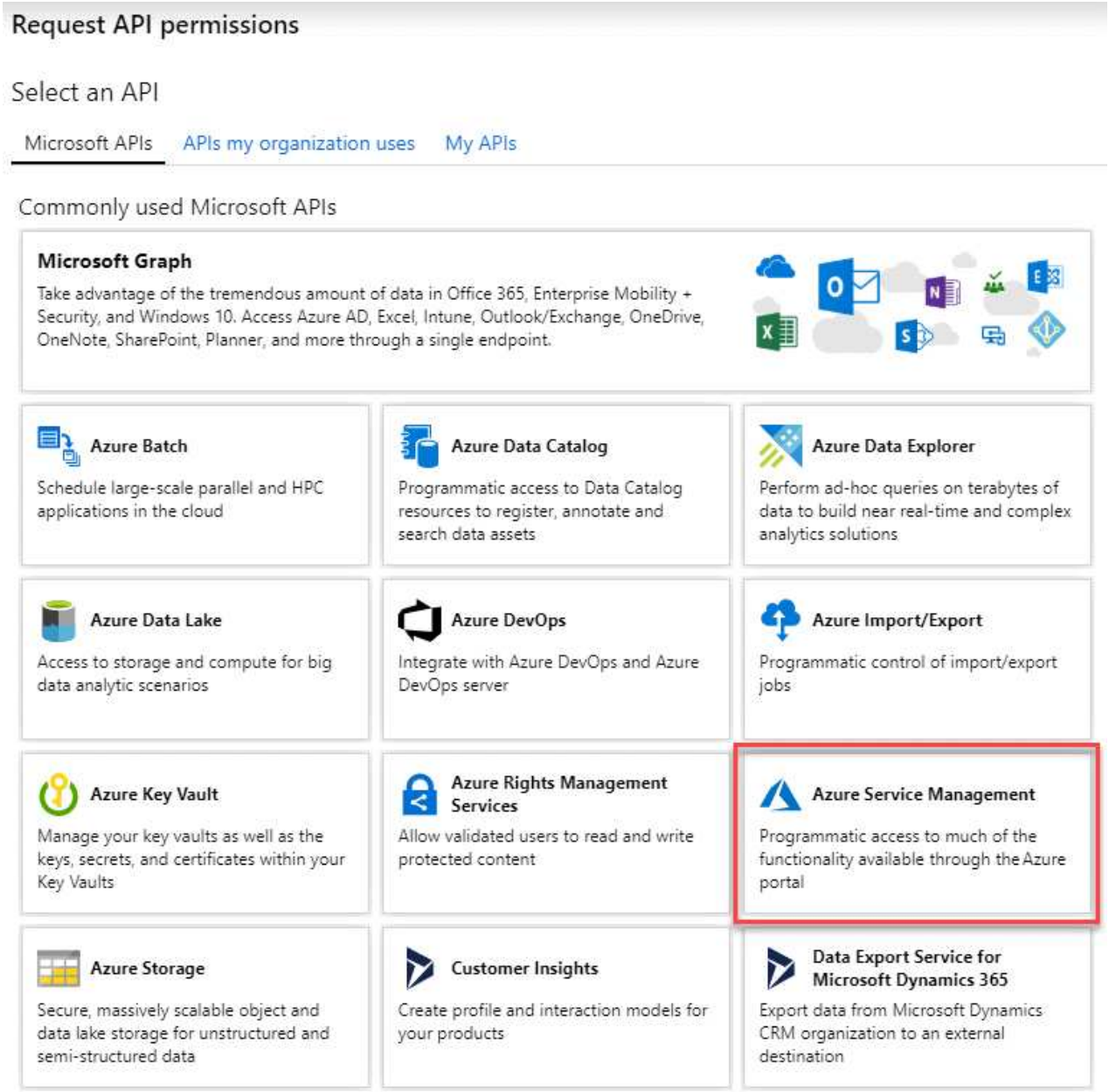
f. 검토 + 할당 * 을 선택합니다.

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

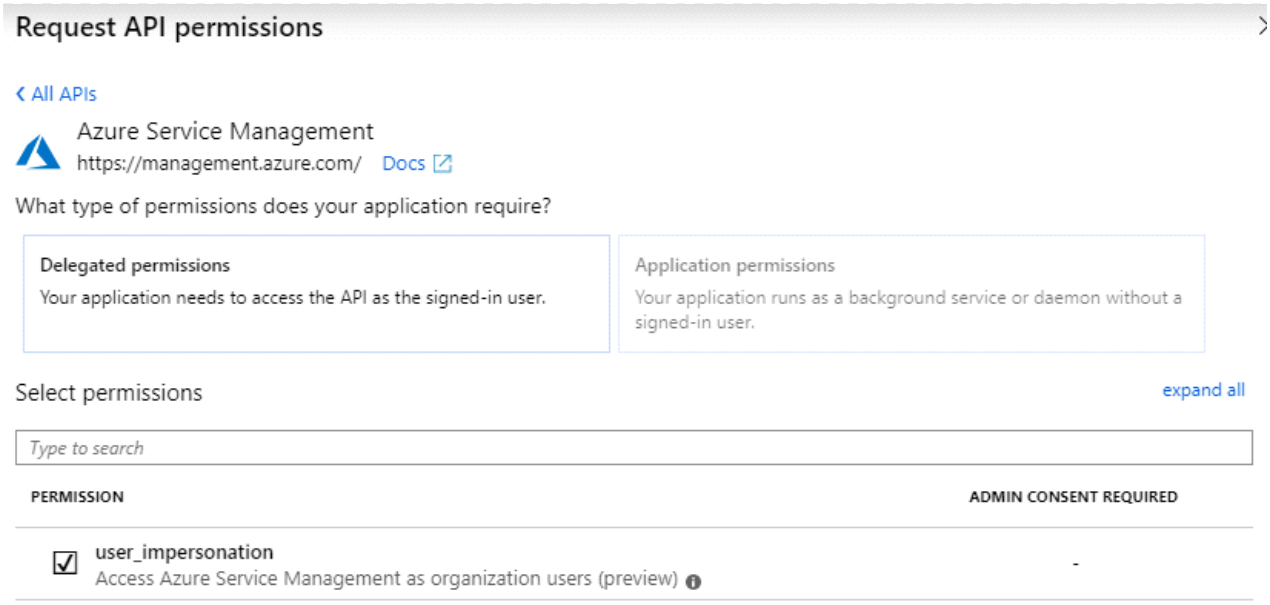
여러 Azure 구독에서 Cloud Volumes ONTAP를 배포하려면 서비스 보안 주체를 해당 구독 각각에 바인딩해야 합니다. BlueXP를 사용하면 Cloud Volumes ONTAP를 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한을 추가합니다

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.

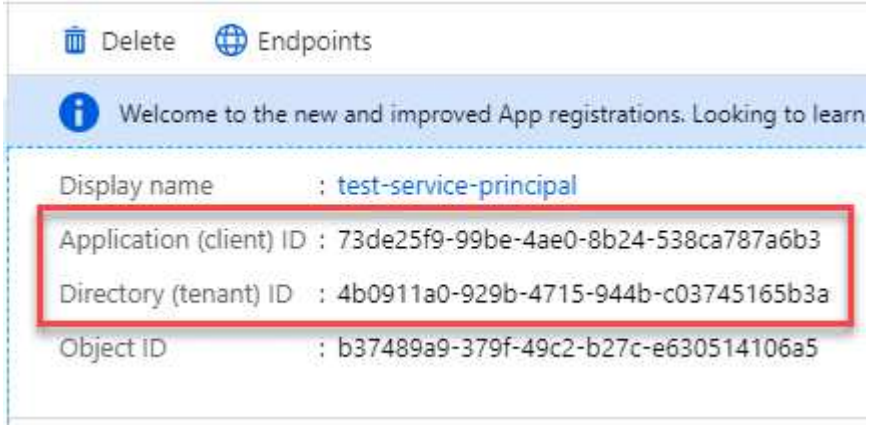


4. Access Azure Service Management as organization users * 를 선택한 다음 * Add permissions * 를 선택합니다.



응용 프로그램의 응용 프로그램 **ID** 및 디렉터리 **ID**를 가져옵니다

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



Azure 계정을 BlueXP에 추가하는 경우 응용 프로그램의 응용 프로그램(클라이언트) ID와 디렉터리(테넌트) ID를 제공해야 합니다. BlueXP는 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 암호를 생성합니다

1. Microsoft Entra ID * 서비스를 엽니다.
2. 앱 등록 * 을 선택하고 응용 프로그램을 선택합니다.
3. 인증서 및 비밀 > 새 클라이언트 비밀 * 을 선택합니다.
4. 비밀과 기간에 대한 설명을 제공하십시오.
5. 추가 * 를 선택합니다.
6. 클라이언트 암호 값을 복사합니다.

이제 BlueXP에서 Microsoft Entra ID를 사용하여 인증하는 클라이언트 암호가 있습니다.

결과

이제 서비스 보안 주체가 설정되었으므로 응용 프로그램(클라이언트) ID, 디렉터리(테넌트) ID 및 클라이언트 암호 값을 복사해야 합니다. Azure 계정을 추가할 때 BlueXP에 이 정보를 입력해야 합니다.

4단계**:** 커넥터를 설치합니다

필수 구성 요소를 완료한 후 자신의 Linux 호스트에 소프트웨어를 수동으로 설치할 수 있습니다.

시작하기 전에

다음과 같은 항목이 있어야 합니다.

- 커넥터를 설치할 수 있는 루트 권한
- Connector의 인터넷 액세스에 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

  설치 후 프록시 서버를 구성할 수 있지만 이렇게 하려면 커넥터를 다시 시작해야 합니다.

  BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

- 프록시 서버가 HTTPS를 사용하거나 프록시가 가로채기 프록시인 경우 CA 서명 인증서입니다.
- 사용자 지정 역할을 통해 필요한 Azure 권한을 제공할 수 있도록 Azure의 VM에서 활성화된 관리되는 ID입니다.

  "Microsoft Azure 설명서: Azure 포털을 사용하여 VM의 Azure 리소스에 대해 관리되는 ID를 구성합니다"

이 작업에 대해

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

단계

1. Docker가 설정 및 실행 중인지 확인합니다.

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

2. _http_proxy_or_https_proxy_system 변수가 호스트에 설정되어 있으면 이를 제거합니다.

```
unset http_proxy
unset https_proxy
```

이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

3. 에서 Connector 소프트웨어를 다운로드합니다 "NetApp Support 사이트"를 선택한 다음 Linux 호스트에 복사합니다.

   네트워크 또는 클라우드에서 사용하도록 고안된 "온라인" 커넥터 설치 프로그램을 다운로드해야 합니다. Connector에 대해 별도의 "오프라인" 설치 프로그램을 사용할 수 있지만 전용 모드 배포에서만 지원됩니다.

4. 스크립트를 실행할 권한을 할당합니다.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

   여기서 <version>는 다운로드한 커넥터 버전입니다.

5. 설치 스크립트를 실행합니다.

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

   proxy 및 — cacert 매개 변수는 선택 사항입니다. 프록시 서버가 있는 경우 그림과 같이 매개 변수를 입력해야 합니다. 설치 프로그램에서 프록시에 대한 정보를 제공하라는 메시지를 표시하지 않습니다.

   다음은 두 가지 선택적 매개 변수를 사용하는 명령의 예입니다.

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

   — 프록시는 다음 형식 중 하나를 사용하여 커넥터가 HTTP 또는 HTTPS 프록시 서버를 사용하도록 구성합니다.

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     다음 사항에 유의하십시오.

     - 사용자는 로컬 사용자 또는 도메인 사용자일 수 있습니다.

- 도메인 사용자의 경우 위에 표시된 \ 에 ASCII 코드를 사용해야 합니다.
- BlueXP는 @ 문자를 포함하는 암호를 지원하지 않습니다.

cacert는 Connector와 프록시 서버 간의 HTTPS 액세스에 사용할 CA 서명 인증서를 지정합니다. 이 매개 변수는 HTTPS 프록시 서버를 지정하거나 프록시가 가로채기 프록시인 경우에만 필요합니다.

6. 설치가 완료될 때까지 기다립니다.

   프록시 서버를 지정한 경우 설치가 끝나면 커넥터 서비스(occm)가 두 번 다시 시작됩니다.

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

   https://ipaddress

8. 로그인한 후 Connector를 설정합니다.
   a. Connector와 연결할 BlueXP 계정을 지정합니다.
   b. 시스템의 이름을 입력합니다.
   c. 에서 * 보안 환경에서 실행 중입니까? * 제한된 모드를 사용하지 않도록 설정합니다.

      이 단계에서는 표준 모드에서 BlueXP를 사용하는 방법을 설명하므로 제한된 모드를 사용하지 않도록 설정해야 합니다. 보안 환경이 있고 BlueXP 백엔드 서비스에서 이 계정의 연결을 끊으려면 제한된 모드만 활성화해야 합니다. 그렇다면 "제한된 모드에서 BlueXP를 시작하려면 다음 단계를 따르십시오".

   d. Let's start * 를 선택합니다.

결과

이제 커넥터가 설치되어 BlueXP 계정으로 설정됩니다.

Connector를 생성한 동일한 Azure 구독에 Azure Blob 스토리지가 있는 경우 BlueXP 캔버스에 Azure Blob 스토리지 작업 환경이 자동으로 표시됩니다. "BlueXP에서 Azure Blob 스토리지를 관리하는 방법에 관해 알아보십시오"

5단계**: BlueXP**에 권한 제공

이제 커넥터를 설치했으므로 이전에 설정한 Azure 권한을 BlueXP에 제공해야 합니다. 권한을 제공하면 BlueXP가 Azure에서 데이터 및 스토리지 인프라를 관리할 수 있습니다.

사용자 지정 역할

Azure 포털로 이동하여 하나 이상의 구독에 대해 Connector 가상 머신에 Azure 사용자 지정 역할을 할당합니다.

단계

1. Azure Portal에서 * Subscriptions * 서비스를 열고 구독을 선택합니다.

   구독 수준에서의 역할 할당 범위를 지정하므로 * 구독 * 서비스에서 역할을 할당하는 것이 중요합니다. scope _ 는 액세스가 적용되는 리소스 집합을 정의합니다. 범위를 다른 수준(예: 가상 머신 레벨)으로 지정하면 BlueXP 내에서 작업을 완료하는 데 영향을 줍니다.

   "Microsoft Azure 설명서: Azure RBAC의 범위를 이해합니다"

2. IAM(액세스 제어) * > * 추가 * > * 역할 할당 추가 * 를 선택합니다.
3. Role * 탭에서 * BlueXP Operator * 역할을 선택하고 * Next * 를 선택합니다.

   BlueXP 오퍼레이터는 BlueXP 정책에 제공된 기본 이름입니다. 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

4. Members* 탭에서 다음 단계를 완료합니다.
   a. 관리되는 ID*에 대한 액세스를 할당합니다.
   b. 구성원 선택 * 을 선택하고 커넥터 가상 시스템이 생성된 구독을 선택한 다음 * 관리 ID * 에서 * 가상 머신 * 을 선택한 다음 커넥터 가상 머신을 선택합니다.
   c. 선택 * 을 선택합니다.
   d. 다음 * 을 선택합니다.
   e. 검토 + 할당 * 을 선택합니다.
   f. 추가 Azure 구독에서 리소스를 관리하려면 해당 구독으로 전환한 다음 이 단계를 반복합니다.

결과

이제 BlueXP는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 가지고 있습니다.

다음 단계

로 이동합니다 "BlueXP 콘솔" 을 눌러 BlueXP에서 커넥터 사용을 시작합니다.

서비스 책임자

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

2. 자격 증명 추가 * 를 선택하고 마법사의 단계를 따릅니다.
   a. * 자격 증명 위치 *: * Microsoft Azure > 커넥터 * 를 선택합니다.
   b. * 자격 증명 정의 *: 필요한 권한을 부여하는 Microsoft Entra 서비스 보안 주체에 대한 정보를 입력합니다.

- 애플리케이션(클라이언트) ID입니다
- 디렉토리(테넌트) ID입니다
- 클라이언트 암호

c. * Marketplace 구독 *: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.

d. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 선택합니다.

결과

이제 BlueXP는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 가지고 있습니다.

Google 클라우드

Google Cloud의 커넥터 설치 옵션

Google Cloud에서 Connector를 생성하는 방법은 몇 가지가 있습니다. BlueXP에서 직접 연결하는 것이 가장 일반적인 방법입니다.

다음 설치 옵션을 사용할 수 있습니다.

- "BlueXP에서 직접 Connector를 생성합니다" (표준 옵션)

  이 작업을 수행하면 선택한 VPC에서 Linux 및 Connector 소프트웨어를 실행하는 VM 인스턴스가 시작됩니다.

- "gcloud를 사용하여 Connector를 작성합니다"

  이 동작은 Linux 및 Connector 소프트웨어를 실행하는 VM 인스턴스도 시작하지만 BlueXP가 아닌 Google Cloud에서 직접 배포됩니다.

- "자체 Linux 호스트에 소프트웨어를 다운로드하고 수동으로 설치합니다"

선택하는 설치 옵션은 설치 준비 방법에 영향을 줍니다. 여기에는 Google Cloud에서 리소스를 인증하고 관리하는 데 필요한 권한을 BlueXP에 제공하는 방법이 포함됩니다.

BlueXP 또는 **gcloud**에서 **Google Cloud**에 **Connector**를 생성합니다

BlueXP에서 또는 gcloud를 사용하여 Google Cloud에 Connector를 생성하려면 네트워킹을 설정하고 Google Cloud 권한을 준비하고 Google Cloud API를 활성화한 다음 Connector를 생성해야 합니다.

시작하기 전에

을(를) 검토해야 합니다 "커넥터 제한".

단계 **1:** 네트워킹을 설정한다

Connector가 하이브리드 클라우드 환경 내의 리소스 및 프로세스를 관리할 수 있도록 네트워킹을 설정합니다. 예를 들어 대상 네트워크에 대한 연결을 사용할 수 있고 아웃바운드 인터넷 액세스를 사용할 수 있는지 확인해야 합니다.

VPC 및 서브넷

Connector를 생성할 때 Connector가 상주할 VPC와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

Connector를 사용하려면 작업 환경을 만들고 관리할 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, 온프레미스 환경에서 Cloud Volumes ONTAP 시스템 또는 스토리지 시스템을 생성할 네트워크를 예로 들 수 있습니다.

아웃바운드 인터넷 액세스

커넥터를 배포하는 네트워크 위치에 특정 끝점에 연결하려면 아웃바운드 인터넷 연결이 있어야 합니다.

커넥터에서 접촉된 끝점

Connector는 일상적인 운영을 위해 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하려면 다음 엔드포인트에 연결하는 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 끝점은 모두 CNAME 항목입니다.

엔드포인트	목적
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://www.googleapis.com/deploymentmanager/v2/projects	Google Cloud에서 리소스를 관리합니다.
https://support.netapp.com 으로 문의하십시오 https://mysupport.netapp.com 으로 문의하십시오	라이센스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXP 내에서 SaaS 기능 및 서비스를 제공합니다. 현재 Connector가 "cloudmanager.cloud.netapp.com" 에 문의하고 있지만 곧 출시될 릴리스에서 "api.bluexp.netapp.com" 에 연락하기 시작합니다.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Connector 및 해당 Docker 구성 요소를 업그레이드합니다.

BlueXP 콘솔에서 연결된 엔드포인트에는

SaaS 계층을 통해 제공되는 BlueXP 웹 기반 콘솔을 사용하면 여러 엔드포인트에 접속하여 데이터 관리 작업을 완료합니다. 여기에는 BlueXP 콘솔에서 커넥터를 배포하기 위해 연결된 엔드포인트가 포함됩니다.

"BlueXP 콘솔에서 연결된 엔드포인트 목록을 봅니다".

프록시 서버

조직에서 모든 나가는 인터넷 트래픽에 대해 프록시 서버를 배포해야 하는 경우 HTTP 또는 HTTPS 프록시에 대한 다음 정보를 가져옵니다. 설치하는 동안 이 정보를 제공해야 합니다.

- IP 주소입니다
- 자격 증명
- HTTPS 인증서

BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

포트

커넥터를 시작하거나 커넥터가 Cloud Volumes ONTAP에서 NetApp 지원으로 AutoSupport 메시지를 보내는 프록시로 사용되지 않는 한 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.
- 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 보내기 위한 아웃바운드 인터넷 연결이 없는 경우 BlueXP는 자동으로 해당 시스템이 커넥터에 포함된 프록시 서버를 사용하도록 구성합니다. 유일한 요구 사항은 커넥터 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

NTP를 활성화합니다

BlueXP 분류를 사용하여 회사 데이터 소스를 검사하려는 경우 BlueXP Connector 시스템과 BlueXP 분류 시스템 모두에서 NTP(Network Time Protocol) 서비스를 활성화하여 시스템 간에 시간이 동기화되도록 해야 합니다. "BlueXP 분류에 대해 자세히 알아보십시오"

Connector를 만든 후 이 네트워킹 요구 사항을 구현해야 합니다.

2단계**:** 커넥터를 만들 수 있는 권한을 설정합니다

BlueXP에서 또는 gcloud를 사용하여 Connector를 배포하려면 Connector VM을 배포할 Google Cloud 사용자의 권한을 설정해야 합니다.

단계

1. Google Cloud에서 사용자 지정 역할 생성:

   a. 다음 권한이 포함된 YAML 파일을 생성합니다.

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
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
```

b. Google Cloud에서 클라우드 쉘을 활성화합니다.

c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

d. 을 사용하여 사용자 지정 역할을 만듭니다 `gcloud iam roles create` 명령.

다음 예제에서는 프로젝트 수준에서 "connectorDeployment"라는 역할을 만듭니다.

gcloud iam 역할은 connectorDeployment를 생성합니다.- project=MyProject—file=connector-deployment.yAML

"Google Cloud docs: 사용자 지정 역할 생성 및 관리"

2. BlueXP에서 Connector를 배포하거나 gcloud를 사용하는 사용자에게 이 사용자 지정 역할을 할당합니다.

"Google Cloud docs: 단일 역할 부여"

결과

이제 Google Cloud 사용자에게 Connector를 만드는 데 필요한 권한이 있습니다.

3단계**:** 커넥터에 대한 사용 권한을 설정합니다

BlueXP에 Google Cloud의 리소스를 관리하는 데 필요한 권한을 Connector에 제공하려면 Google Cloud 서비스 계정이 필요합니다. Connector를 생성할 때 이 서비스 계정을 Connector VM에 연결해야 합니다.

단계

1. Google Cloud에서 사용자 지정 역할 생성:

a. 의 내용이 포함된 YAML 파일을 생성합니다 "Connector에 대한 서비스 계정 권한".

b. Google Cloud에서 클라우드 쉘을 활성화합니다.

c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

d. 을 사용하여 사용자 지정 역할을 만듭니다 `gcloud iam roles create` 명령.

다음 예제에서는 프로젝트 수준에서 "connector"라는 역할을 만듭니다.

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

"Google Cloud docs: 사용자 지정 역할 생성 및 관리"

2. Google Cloud에서 서비스 계정을 생성하고 서비스 계정에 역할을 할당합니다.
   a. IAM 및 관리 서비스에서 * 서비스 계정 > 서비스 계정 생성 * 을 선택합니다.
   b. 서비스 계정 세부 정보를 입력하고 * 생성 및 계속 * 을 선택합니다.
   c. 방금 만든 역할을 선택합니다.
   d. 나머지 단계를 완료해서 역할을 만듭니다.

      "Google Cloud docs: 서비스 계정 생성"

3. 커넥터가 있는 프로젝트와 다른 프로젝트에 Cloud Volumes ONTAP 시스템을 배포하려는 경우 해당 프로젝트에 액세스할 수 있는 Connector의 서비스 계정을 제공해야 합니다.

   예를 들어, 커넥터가 프로젝트 1에 있고 프로젝트 2에서 Cloud Volumes ONTAP 시스템을 만들려는 경우를 가정해 보겠습니다. 프로젝트 2에서 서비스 계정에 대한 액세스 권한을 부여해야 합니다.

   a. IAM 및 관리자 서비스에서 Cloud Volumes ONTAP 시스템을 생성할 Google Cloud 프로젝트를 선택합니다.
   b. IAM * 페이지에서 * 액세스 권한 부여 * 를 선택하고 필요한 세부 정보를 제공합니다.
      - Connector의 서비스 계정의 이메일을 입력합니다.
      - Connector의 사용자 정의 역할을 선택합니다.
      - 저장 * 을 선택합니다.

   자세한 내용은 을 참조하십시오 "Google Cloud 설명서"

결과

Connector VM에 대한 서비스 계정이 설정되어 있습니다.

4단계**:** 공유 **VPC** 권한 설정

공유 VPC를 사용하여 리소스를 서비스 프로젝트에 배포하는 경우 사용 권한을 준비해야 합니다.

이 표는 참조용이며 IAM 구성이 완료되면 사용 권한 테이블이 환경에 반영되어야 합니다.

공유 **VPC** 권한을 봅니다

아이덴티티	창조자	에서 호스팅됩니다	서비스 프로젝트 권한	호스트 프로젝트 권한	목적
Connector를 배포하기 위한 Google 계정	맞춤형	서비스 프로젝트	"커넥터 배치 정책"	compute.networkUser	서비스 프로젝트에 Connector 배포
커넥터 서비스 계정	맞춤형	서비스 프로젝트	"커넥터 서비스 계정 정책"	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: BlueXP 서비스 계정(serviceAccount.user)	해당 없음	(선택 사항) 데이터 계층화 및 BlueXP 백업 및 복구
Google API 서비스 에이전트입니다	Google 클라우드	서비스 프로젝트	(기본값) 편집기	compute.networkUser	배포를 대신하여 Google Cloud API와 상호 작용합니다. BlueXP에서 공유 네트워크를 사용할 수 있습니다.
Google Compute Engine 기본 서비스 계정입니다	Google 클라우드	서비스 프로젝트	(기본값) 편집기	compute.networkUser	배포를 대신하여 Google Cloud 인스턴스 및 컴퓨팅 인프라를 배포합니다. BlueXP에서 공유 네트워크를 사용할 수 있습니다.

참고:

1. 배포관리자 .editor는 배포에 방화벽 규칙을 전달하지 않고 BlueXP에서 사용자를 위해 방화벽 규칙을 만들도록 선택한 경우에만 호스트 프로젝트에 필요합니다. BlueXP는 호스트 프로젝트에 VPC0 방화벽 규칙이 지정되지 않은 경우 이를 포함하는 배포를 생성합니다.
2. Firewall.create 및 firewall.delete 은 배포에 방화벽 규칙을 전달하지 않고 BlueXP에서 사용자를 위해 방화벽 규칙을 만들도록 선택한 경우에만 필요합니다. 이러한 권한은 BlueXP 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.

5단계: Google Cloud API를 활성화합니다

Google Cloud에서 Connector 및 Cloud Volumes ONTAP를 배포하기 전에 여러 Google Cloud API를 활성화해야 합니다.

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
    - 클라우드 키 관리 서비스(KMS) API

      (고객이 관리하는 암호화 키(CMEK)로 BlueXP 백업 및 복구를 사용하려는 경우에만 필요)

"Google Cloud 설명서: API 활성화"

6단계: 커넥터를 만듭니다

BlueXP 웹 기반 콘솔에서 직접 또는 gcloud를 사용하여 Connector를 생성합니다.

이 작업에 대해

Connector를 생성하면 기본 구성을 사용하여 Google Cloud에 가상 머신 인스턴스를 배포합니다. Connector를 생성한 후에는 CPU 또는 RAM이 적은 더 작은 VM 인스턴스로 변경하지 마십시오. "Connector의 기본 설정에 대해 알아봅니다".

BlueXP

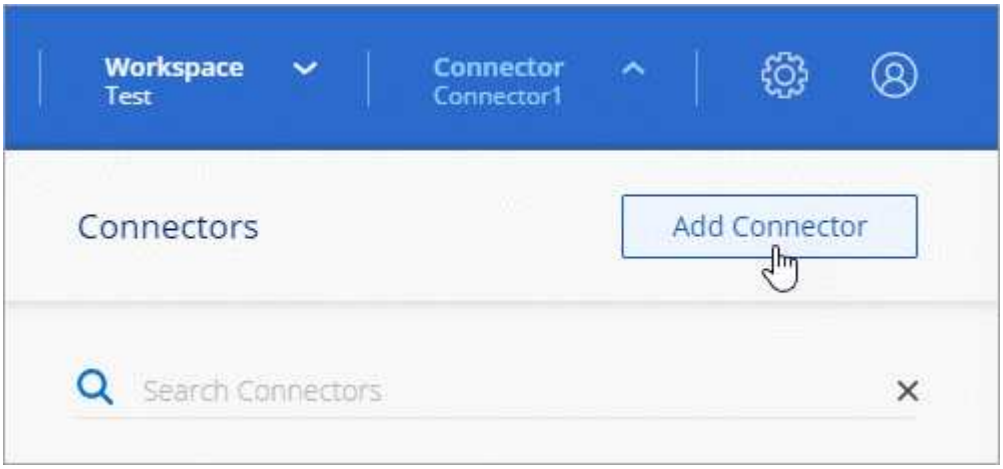
시작하기 전에

다음과 같은 항목이 있어야 합니다.

- Connector 및 Connector VM에 대한 서비스 계정을 생성하는 데 필요한 Google Cloud 권한.
- 네트워킹 요구사항을 충족하는 VPC 및 서브넷
- Connector의 인터넷 액세스에 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

단계

1. 커넥터 * 드롭다운을 선택하고 * 커넥터 추가 * 를 선택합니다.



2. 클라우드 공급자로 * Google Cloud Platform * 을 선택합니다.
3. 커넥터 배포 * 페이지에서 필요한 사항에 대한 세부 정보를 검토합니다. 두 가지 옵션이 있습니다.
   a. 제품 내 가이드를 사용하여 배포를 준비하려면 * 계속 * 을 선택합니다. 제품 내 가이드의 각 단계에는 이 문서 페이지에 포함된 정보가 포함되어 있습니다.
   b. 이 페이지의 단계에 따라 이미 준비되었으면 * 배포로 건너뛰기 * 를 선택합니다.
4. 마법사의 단계에 따라 커넥터를 작성합니다.
   - 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.
   - * 세부 정보 *: 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 필요한 인바운드 및 아웃바운드 규칙을 허용하는 기존 방화벽 정책을 선택할지 여부를 선택합니다.

     "Google Cloud의 방화벽 규칙"

- * 검토 *: 선택 사항을 검토하여 설정이 올바른지 확인합니다.

5. 추가 * 를 선택합니다.

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

결과

프로세스가 완료되면 BlueXP에서 커넥터를 사용할 수 있습니다.

Connector를 생성한 동일한 Google Cloud 계정에 Google Cloud Storage 버킷이 있는 경우 BlueXP 캔버스에 Google Cloud 스토리지 작업 환경이 자동으로 표시됩니다. "BlueXP에서 Google Cloud 스토리지를 관리하는 방법에 관해 알아보십시오"

gcloud를 선택합니다

시작하기 전에

다음과 같은 항목이 있어야 합니다.

- Connector 및 Connector VM에 대한 서비스 계정을 생성하는 데 필요한 Google Cloud 권한.
- 네트워킹 요구사항을 충족하는 VPC 및 서브넷
- VM 인스턴스 요구 사항 이해
  - * CPU *: 4코어 또는 4개의 vCPU
  - * RAM *: 14GB
  - * 기계 유형 * : 우리는 n2-standard-4를 권장합니다.

    Connector는 Shield로 보호된 VM 기능을 지원하는 OS가 있는 VM 인스턴스에서 Google Cloud에서 지원됩니다.

단계

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. 를 실행합니다 `gcloud compute instances create` 명령:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-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.

   https://ipaddress

2. 로그인한 후 Connector를 설정합니다.
   a. Connector와 연결할 BlueXP 계정을 지정합니다.

      "BlueXP 계정에 대해 알아보십시오".

   b. 시스템의 이름을 입력합니다.

결과

이제 커넥터가 설치되어 BlueXP 계정으로 설정됩니다.

웹 브라우저를 열고 로 이동합니다 "BlueXP 콘솔" 을 눌러 BlueXP에서 커넥터 사용을 시작합니다.

Google Cloud에 **Connector**를 수동으로 설치합니다

자신의 Linux 호스트에 Connector를 수동으로 설치하려면 호스트 요구 사항을 검토하고, 네트워킹을 설정하고, Google Cloud 권한을 준비하고, Google Cloud API를 활성화하고, Connector를 설치한 다음 준비된 사용 권한을 제공해야 합니다.

시작하기 전에

을(를) 검토해야 합니다 "커넥터 제한".

1단계**:** 호스트 요구 사항을 검토합니다

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

전용 호스트

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

지원되는 운영 체제

- 우분투 22.04 LTS
- CentOS 7.6, 7.7, 7.8 및 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 및 7.9

  호스트는 Red Hat Subscription Management에 등록되어 있어야 합니다. 등록되지 않은 경우 호스트는 Connector 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.

  Connector는 이러한 운영 체제의 영어 버전에서 지원됩니다.

하이퍼바이저

Ubuntu, CentOS 또는 Red Hat Enterprise Linux 실행 인증을 받은 베어 메탈 또는 호스팅된 하이퍼바이저가 필요합니다.

"Red Hat 솔루션: Red Hat Enterprise Linux 실행 인증을 받은 하이퍼바이저는 무엇입니까?"

CPU

코어 4개 또는 vCPU 4개

RAM

14GB

Google Cloud 컴퓨터 유형입니다

위의 CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. n2-standard-4를 추천합니다.

Connector는 를 지원하는 OS가 있는 VM 인스턴스의 Google Cloud에서 지원됩니다 "차폐된 VM 기능"

/opt의 디스크 공간입니다

100GiB의 공간을 사용할 수 있어야 합니다

/var의 디스크 공간입니다

20GiB의 공간을 사용할 수 있어야 합니다

Docker 엔진

Connector를 설치하기 전에 Docker 엔진이 호스트에 필요합니다.

- 지원되는 최소 버전은 19.3.1입니다.
- 지원되는 최대 버전은 25.0.5입니다.

  "설치 지침을 봅니다"

2단계**:** 네트워킹을 설정한다

Connector가 하이브리드 클라우드 환경 내의 리소스 및 프로세스를 관리할 수 있도록 네트워킹을 설정합니다. 예를 들어 대상 네트워크에 대한 연결을 사용할 수 있고 아웃바운드 인터넷 액세스를 사용할 수 있는지 확인해야 합니다.

대상 네트워크에 대한 연결

Connector를 사용하려면 작업 환경을 만들고 관리할 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, 온프레미스 환경에서 Cloud Volumes ONTAP 시스템 또는 스토리지 시스템을 생성할 네트워크를 예로 들 수 있습니다.

아웃바운드 인터넷 액세스

커넥터를 배포하는 네트워크 위치에 특정 끝점에 연결하려면 아웃바운드 인터넷 연결이 있어야 합니다.

수동 설치 중에 연결된 끝점입니다

자체 Linux 호스트에 커넥터를 수동으로 설치할 경우 Connector 설치 과정에서 다음 URL에 액세스해야 합니다.

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

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

커넥터에서 접촉된 끝점

Connector는 일상적인 운영을 위해 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하려면 다음 엔드포인트에 연결하는 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 끝점은 모두 CNAME 항목입니다.

엔드포인트	목적
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://www.googleapis.com/deploymentmanager/v2/projects	Google Cloud에서 리소스를 관리합니다.
https://support.netapp.com 으로 문의하십시오 https://mysupport.netapp.com 으로 문의하십시오	라이센스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다.

엔드포인트	목적
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXP 내에서 SaaS 기능 및 서비스를 제공합니다. 현재 Connector가 "cloudmanager.cloud.netapp.com" 에 문의하고 있지만 곧 출시될 릴리스에서 "api.bluexp.netapp.com" 에 연락하기 시작합니다.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Connector 및 해당 Docker 구성 요소를 업그레이드합니다.

프록시 서버

조직에서 모든 나가는 인터넷 트래픽에 대해 프록시 서버를 배포해야 하는 경우 HTTP 또는 HTTPS 프록시에 대한 다음 정보를 가져옵니다. 설치하는 동안 이 정보를 제공해야 합니다.

- IP 주소입니다
- 자격 증명
- HTTPS 인증서

BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

포트

커넥터를 시작하거나 커넥터가 Cloud Volumes ONTAP에서 NetApp 지원으로 AutoSupport 메시지를 보내는 프록시로 사용되지 않는 한 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.
- 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 보내기 위한 아웃바운드 인터넷 연결이 없는 경우 BlueXP는 자동으로 해당 시스템이 커넥터에 포함된 프록시 서버를 사용하도록 구성합니다. 유일한 요구 사항은 커넥터 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

NTP를 활성화합니다

BlueXP 분류를 사용하여 회사 데이터 소스를 검사하려는 경우 BlueXP Connector 시스템과 BlueXP 분류 시스템 모두에서 NTP(Network Time Protocol) 서비스를 활성화하여 시스템 간에 시간이 동기화되도록 해야 합니다. "BlueXP 분류에 대해 자세히 알아보십시오"

3단계**:** 커넥터에 대한 사용 권한을 설정합니다

BlueXP에 Google Cloud의 리소스를 관리하는 데 필요한 권한을 Connector에 제공하려면 Google Cloud 서비스

계정이 필요합니다. Connector를 생성할 때 이 서비스 계정을 Connector VM에 연결해야 합니다.

단계

1. Google Cloud에서 사용자 지정 역할 생성:

   a. 의 내용이 포함된 YAML 파일을 생성합니다 "Connector에 대한 서비스 계정 권한".

   b. Google Cloud에서 클라우드 쉘을 활성화합니다.

   c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

   d. 을 사용하여 사용자 지정 역할을 만듭니다 `gcloud iam roles create` 명령.

      다음 예제에서는 프로젝트 수준에서 "connector"라는 역할을 만듭니다.

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

   "Google Cloud docs: 사용자 지정 역할 생성 및 관리"

2. Google Cloud에서 서비스 계정을 생성하고 서비스 계정에 역할을 할당합니다.

   a. IAM 및 관리 서비스에서 * 서비스 계정 > 서비스 계정 생성 * 을 선택합니다.

   b. 서비스 계정 세부 정보를 입력하고 * 생성 및 계속 * 을 선택합니다.

   c. 방금 만든 역할을 선택합니다.

   d. 나머지 단계를 완료해서 역할을 만듭니다.

      "Google Cloud docs: 서비스 계정 생성"

3. 커넥터가 있는 프로젝트와 다른 프로젝트에 Cloud Volumes ONTAP 시스템을 배포하려는 경우 해당 프로젝트에 액세스할 수 있는 Connector의 서비스 계정을 제공해야 합니다.

   예를 들어, 커넥터가 프로젝트 1에 있고 프로젝트 2에서 Cloud Volumes ONTAP 시스템을 만들려는 경우를 가정해 보겠습니다. 프로젝트 2에서 서비스 계정에 대한 액세스 권한을 부여해야 합니다.

   a. IAM 및 관리자 서비스에서 Cloud Volumes ONTAP 시스템을 생성할 Google Cloud 프로젝트를 선택합니다.

   b. IAM * 페이지에서 * 액세스 권한 부여 * 를 선택하고 필요한 세부 정보를 제공합니다.

      - Connector의 서비스 계정의 이메일을 입력합니다.
      - Connector의 사용자 정의 역할을 선택합니다.
      - 저장 * 을 선택합니다.

   자세한 내용은 을 참조하십시오 "Google Cloud 설명서"

결과

Connector VM에 대한 서비스 계정이 설정되어 있습니다.

4단계: 공유 VPC 권한 설정

공유 VPC를 사용하여 리소스를 서비스 프로젝트에 배포하는 경우 사용 권한을 준비해야 합니다.

이 표는 참조용이며 IAM 구성이 완료되면 사용 권한 테이블이 환경에 반영되어야 합니다.

공유 **VPC** 권한을 봅니다

아이덴티티	창조자	에서 호스팅됩니다	서비스 프로젝트 권한	호스트 프로젝트 권한	목적
Connector를 배포하기 위한 Google 계정	맞춤형	서비스 프로젝트	"커넥터 배치 정책"	compute.networkUser	서비스 프로젝트에 Connector 배포
커넥터 서비스 계정	맞춤형	서비스 프로젝트	"커넥터 서비스 계정 정책"	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: BlueXP 서비스 계정(serviceAccount.user)	해당 없음	(선택 사항) 데이터 계층화 및 BlueXP 백업 및 복구
Google API 서비스 에이전트입니다	Google 클라우드	서비스 프로젝트	(기본값) 편집기	compute.networkUser	배포를 대신하여 Google Cloud API와 상호 작용합니다. BlueXP에서 공유 네트워크를 사용할 수 있습니다.
Google Compute Engine 기본 서비스 계정입니다	Google 클라우드	서비스 프로젝트	(기본값) 편집기	compute.networkUser	배포를 대신하여 Google Cloud 인스턴스 및 컴퓨팅 인프라를 배포합니다. BlueXP에서 공유 네트워크를 사용할 수 있습니다.

참고:

1. 배포관리자 .editor는 배포에 방화벽 규칙을 전달하지 않고 BlueXP에서 사용자를 위해 방화벽 규칙을 만들도록 선택한 경우에만 호스트 프로젝트에 필요합니다. BlueXP는 호스트 프로젝트에 VPC0 방화벽 규칙이 지정되지 않은 경우 이를 포함하는 배포를 생성합니다.
2. Firewall.create 및 firewall.delete 은 배포에 방화벽 규칙을 전달하지 않고 BlueXP에서 사용자를 위해 방화벽 규칙을 만들도록 선택한 경우에만 필요합니다. 이러한 권한은 BlueXP 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.

5단계: Google Cloud API를 활성화합니다

Google Cloud에 Cloud Volumes ONTAP 시스템을 배포하기 전에 여러 Google Cloud API를 활성화해야 합니다.

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
    - 클라우드 키 관리 서비스(KMS) API

      (고객이 관리하는 암호화 키(CMEK)로 BlueXP 백업 및 복구를 사용하려는 경우에만 필요)

"Google Cloud 설명서: API 활성화"

6단계: 커넥터를 설치합니다

필수 구성 요소를 완료한 후 자신의 Linux 호스트에 소프트웨어를 수동으로 설치할 수 있습니다.

시작하기 전에

다음과 같은 항목이 있어야 합니다.

- 커넥터를 설치할 수 있는 루트 권한
- Connector의 인터넷 액세스에 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

  설치 후 프록시 서버를 구성할 수 있지만 이렇게 하려면 커넥터를 다시 시작해야 합니다.

  BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

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

이 작업에 대해

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

단계

1. Docker가 설정 및 실행 중인지 확인합니다.

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

2. _http_proxy_or_https_proxy_system 변수가 호스트에 설정되어 있으면 이를 제거합니다.

```
unset http_proxy
unset https_proxy
```

이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

3. 에서 Connector 소프트웨어를 다운로드합니다 "NetApp Support 사이트"를 선택한 다음 Linux 호스트에 복사합니다.

   네트워크 또는 클라우드에서 사용하도록 고안된 "온라인" 커넥터 설치 프로그램을 다운로드해야 합니다. Connector에 대해 별도의 "오프라인" 설치 프로그램을 사용할 수 있지만 전용 모드 배포에서만 지원됩니다.

4. 스크립트를 실행할 권한을 할당합니다.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

   여기서 <version>는 다운로드한 커넥터 버전입니다.

5. 설치 스크립트를 실행합니다.

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

   proxy 및 — cacert 매개 변수는 선택 사항입니다. 프록시 서버가 있는 경우 그림과 같이 매개 변수를 입력해야 합니다. 설치 프로그램에서 프록시에 대한 정보를 제공하라는 메시지를 표시하지 않습니다.

   다음은 두 가지 선택적 매개 변수를 사용하는 명령의 예입니다.

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

   — 프록시는 다음 형식 중 하나를 사용하여 커넥터가 HTTP 또는 HTTPS 프록시 서버를 사용하도록 구성합니다.

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     다음 사항에 유의하십시오.

     - 사용자는 로컬 사용자 또는 도메인 사용자일 수 있습니다.

- 도메인 사용자의 경우 위에 표시된 \ 에 ASCII 코드를 사용해야 합니다.
- BlueXP는 @ 문자를 포함하는 암호를 지원하지 않습니다.

cacert는 Connector와 프록시 서버 간의 HTTPS 액세스에 사용할 CA 서명 인증서를 지정합니다. 이 매개 변수는 HTTPS 프록시 서버를 지정하거나 프록시가 가로채기 프록시인 경우에만 필요합니다.

6. 설치가 완료될 때까지 기다립니다.

   프록시 서버를 지정한 경우 설치가 끝나면 커넥터 서비스(occm)가 두 번 다시 시작됩니다.

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

   https://ipaddress

8. 로그인한 후 Connector를 설정합니다.
   a. Connector와 연결할 BlueXP 계정을 지정합니다.
   b. 시스템의 이름을 입력합니다.
   c. 에서 * 보안 환경에서 실행 중입니까? * 제한된 모드를 사용하지 않도록 설정합니다.

      이 단계에서는 표준 모드에서 BlueXP를 사용하는 방법을 설명하므로 제한된 모드를 사용하지 않도록 설정해야 합니다. 보안 환경이 있고 BlueXP 백엔드 서비스에서 이 계정의 연결을 끊으려면 제한된 모드만 활성화해야 합니다. 그렇다면 "제한된 모드에서 BlueXP를 시작하려면 다음 단계를 따르십시오".

   d. Let's start * 를 선택합니다.

결과

이제 커넥터가 설치되어 BlueXP 계정으로 설정됩니다.

Connector를 생성한 동일한 Google Cloud 계정에 Google Cloud Storage 버킷이 있는 경우 BlueXP 캔버스에 Google Cloud 스토리지 작업 환경이 자동으로 표시됩니다. "BlueXP에서 Google Cloud 스토리지를 관리하는 방법에 관해 알아보십시오"

7단계**: BlueXP**에 권한 제공

이전에 설정한 Google Cloud 권한을 BlueXP에 제공해야 합니다. 권한을 제공하면 BlueXP가 Google Cloud에서 데이터 및 스토리지 인프라를 관리할 수 있습니다.

단계

1. Google Cloud 포털로 이동하여 Connector VM 인스턴스에 서비스 계정을 할당합니다.

   "Google Cloud 설명서: 인스턴스에 대한 서비스 계정 및 액세스 범위 변경"

2. 다른 Google Cloud 프로젝트의 리소스를 관리하려면 해당 프로젝트에 BlueXP 역할의 서비스 계정을 추가하여 액세스 권한을 부여합니다. 각 프로젝트에 대해 이 단계를 반복해야 합니다.

결과

BlueXP는 이제 Google Cloud에서 대신 작업을 수행하는 데 필요한 권한을 가지고 있습니다.

온-프레미스에 커넥터를 설치하고 설정합니다

구내 커넥터를 설치한 다음 로그인하여 BlueXP 계정과 작동하도록 설정합니다.

시작하기 전에

을(를) 검토해야 합니다 "커넥터 제한".

1단계**:** 호스트 요구 사항을 검토합니다

Connector 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 포트 요구 사항 등을 충족하는 호스트에서 실행되어야 합니다. 커넥터를 설치하기 전에 호스트가 이러한 요구 사항을 충족하는지 확인하십시오.

전용 호스트

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

지원되는 운영 체제

- 우분투 22.04 LTS
- CentOS 7.6, 7.7, 7.8 및 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 및 7.9

  호스트는 Red Hat Subscription Management에 등록되어 있어야 합니다. 등록되지 않은 경우 호스트는 Connector 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.

  Connector는 이러한 운영 체제의 영어 버전에서 지원됩니다.

하이퍼바이저

Ubuntu, CentOS 또는 Red Hat Enterprise Linux 실행 인증을 받은 베어 메탈 또는 호스팅된 하이퍼바이저가 필요합니다.

"Red Hat 솔루션: Red Hat Enterprise Linux 실행 인증을 받은 하이퍼바이저는 무엇입니까?"

CPU

코어 4개 또는 vCPU 4개

RAM

14GB

/opt의 디스크 공간입니다

100GiB의 공간을 사용할 수 있어야 합니다

/var의 디스크 공간입니다

20GiB의 공간을 사용할 수 있어야 합니다

Docker 엔진

Connector를 설치하기 전에 Docker 엔진이 호스트에 필요합니다.

- 지원되는 최소 버전은 19.3.1입니다.
- 지원되는 최대 버전은 25.0.5입니다.

"설치 지침을 봅니다"

2단계**:** 네트워킹을 설정한다

Connector가 하이브리드 클라우드 환경 내의 리소스 및 프로세스를 관리할 수 있도록 네트워킹을 설정합니다. 예를 들어 대상 네트워크에 대한 연결을 사용할 수 있고 아웃바운드 인터넷 액세스를 사용할 수 있는지 확인해야 합니다.

대상 네트워크에 대한 연결

Connector를 사용하려면 작업 환경을 만들고 관리할 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, 온프레미스 환경에서 Cloud Volumes ONTAP 시스템 또는 스토리지 시스템을 생성할 네트워크를 예로 들 수 있습니다.

아웃바운드 인터넷 액세스

커넥터를 배포하는 네트워크 위치에 특정 끝점에 연결하려면 아웃바운드 인터넷 연결이 있어야 합니다.

수동 설치 중에 연결된 끝점입니다

자체 Linux 호스트에 커넥터를 수동으로 설치할 경우 Connector 설치 과정에서 다음 URL에 액세스해야 합니다.

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

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

커넥터에서 접촉된 끝점

Connector는 일상적인 운영을 위해 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하려면 다음 엔드포인트에 연결하는 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 끝점은 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • CloudFormation 을 참조하십시오 • EC2(탄력적인 컴퓨팅 클라우드) • IAM(Identity and Access Management) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • S3(Simple Storage Service)	를 사용하여 AWS에서 리소스를 관리합니다. 정확한 끝점은 사용 중인 AWS 지역에 따라 다릅니다. "자세한 내용은 AWS 설명서를 참조하십시오"

엔드포인트	목적
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure 공공 지역의 리소스를 관리합니다.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure 중국 지역의 리소스를 관리합니다.
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://www.googleapis.com/deploymentmanager/v2/projects	Google Cloud에서 리소스를 관리합니다.
https://support.netapp.com 으로 문의하십시오 https://mysupport.netapp.com 으로 문의하십시오	라이센스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXP 내에서 SaaS 기능 및 서비스를 제공합니다. 현재 Connector가 "cloudmanager.cloud.netapp.com" 에 문의하고 있지만 곧 출시될 릴리스에서 "api.bluexp.netapp.com" 에 연락하기 시작합니다.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Connector 및 해당 Docker 구성 요소를 업그레이드합니다.

프록시 서버

조직에서 모든 나가는 인터넷 트래픽에 대해 프록시 서버를 배포해야 하는 경우 HTTP 또는 HTTPS 프록시에 대한 다음 정보를 가져옵니다. 설치하는 동안 이 정보를 제공해야 합니다.

- IP 주소입니다
- 자격 증명
- HTTPS 인증서

BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

포트

커넥터를 시작하거나 커넥터가 Cloud Volumes ONTAP에서 NetApp 지원으로 AutoSupport 메시지를 보내는 프록시로 사용되지 않는 한 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.
- 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 보내기 위한 아웃바운드 인터넷 연결이 없는 경우 BlueXP는 자동으로 해당 시스템이 커넥터에 포함된 프록시 서버를 사용하도록 구성합니다. 유일한 요구 사항은 커넥터 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

NTP를 활성화합니다

BlueXP 분류를 사용하여 회사 데이터 소스를 검사하려는 경우 BlueXP Connector 시스템과 BlueXP 분류 시스템 모두에서 NTP(Network Time Protocol) 서비스를 활성화하여 시스템 간에 시간이 동기화되도록 해야 합니다. "BlueXP 분류에 대해 자세히 알아보십시오"

3단계**:** 클라우드 사용 권한 설정

온-프레미스 커넥터가 있는 AWS 또는 Azure에서 BlueXP 서비스를 사용하려면 클라우드 공급자에 권한을 설정해야 자격 증명을 설치한 후 Connector에 추가할 수 있습니다.

Google Cloud가 적합하지 않은 이유 Connector가 구내에 설치되어 있으면 Google Cloud에서 리소스를 관리할 수 없습니다. Google Cloud에 Connector를 설치하여 해당 위치에 있는 모든 리소스를 관리해야 합니다.

설치하고

Connector가 사내에 설치된 경우 필요한 권한이 있는 IAM 사용자에 대한 액세스 키를 추가하여 BlueXP에 AWS 권한을 제공해야 합니다.

Connector가 구내에 설치된 경우 이 인증 방법을 사용해야 합니다. IAM 역할을 사용할 수 없습니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책 생성:

   a. 정책 > 정책 생성 * 을 선택합니다.

   b. JSON * 을 선택하고 의 내용을 복사하여 붙여 넣습니다 "Connector에 대한 IAM 정책".

   c. 나머지 단계를 완료하고 정책을 생성합니다.

      사용할 BlueXP 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다.

   표준 영역의 경우 권한이 두 정책에 분산됩니다. AWS에서 관리되는 정책의 최대 문자 크기 제한으로 인해 두 개의 정책이 필요합니다. "Connector에 대한 IAM 정책에 대해 자세히 알아보십시오".

3. IAM 사용자에게 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"
4. 커넥터를 설치한 후 BlueXP에 추가할 수 있는 액세스 키가 사용자에게 있는지 확인합니다.

결과

이제 필요한 권한이 있는 IAM 사용자를 위한 액세스 키가 있어야 합니다. Connector를 설치한 후 이러한 자격 증명을 BlueXP의 커넥터와 연결해야 합니다.

Azure를 지원합니다

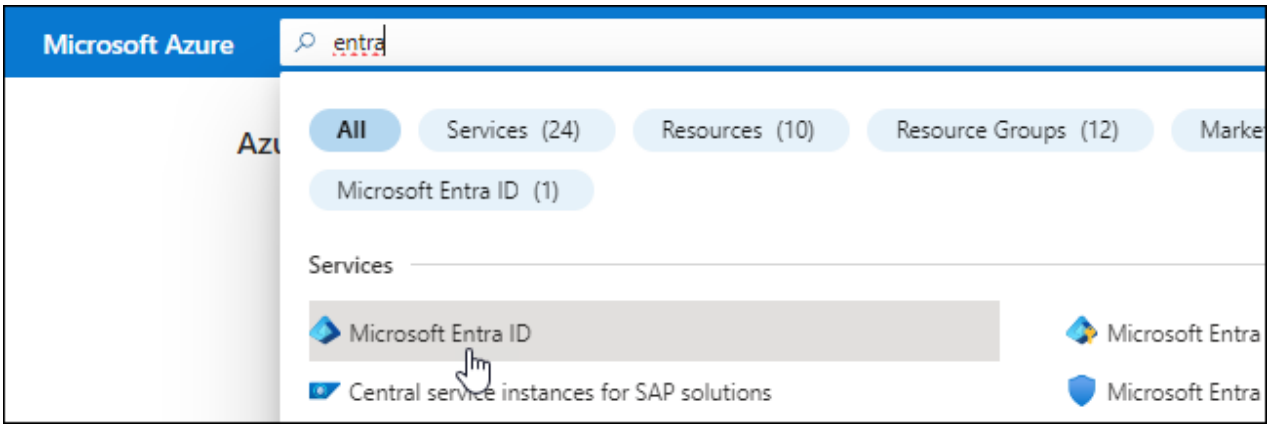
Connector를 사내에 설치한 경우 Microsoft Entra ID에서 서비스 주체를 설정하고 BlueXP에 필요한 Azure 자격 증명을 입수하여 BlueXP에 Azure 권한을 제공해야 합니다.

역할 기반 액세스 제어를 위한 **Microsoft Entra** 응용 프로그램을 만듭니다

1. Azure에서 Active Directory 응용 프로그램을 만들고 응용 프로그램을 역할에 할당할 수 있는 권한이 있는지 확인합니다.

   자세한 내용은 을 참조하십시오 "Microsoft Azure 문서: 필요한 권한"

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



3. 메뉴에서 * 앱 등록 * 을 선택합니다.
4. 새 등록 * 을 선택합니다.
5. 응용 프로그램에 대한 세부 정보를 지정합니다.
   - * 이름 *: 응용 프로그램의 이름을 입력합니다.
   - * 계정 유형 *: 계정 유형을 선택합니다(모두 BlueXP에서 사용 가능).
   - * URI 리디렉션 *: 이 필드는 비워 둘 수 있습니다.
6. Register * 를 선택합니다.

   AD 응용 프로그램 및 서비스 보안 주체를 만들었습니다.

애플리케이션에 역할을 할당합니다

1. 사용자 지정 역할 만들기:

   Azure 포털, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 생성할 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 생성하는 방법을 보여 줍니다. 다른 방법을 사용하려면 을 참조하십시오 "Azure 문서"

   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 *

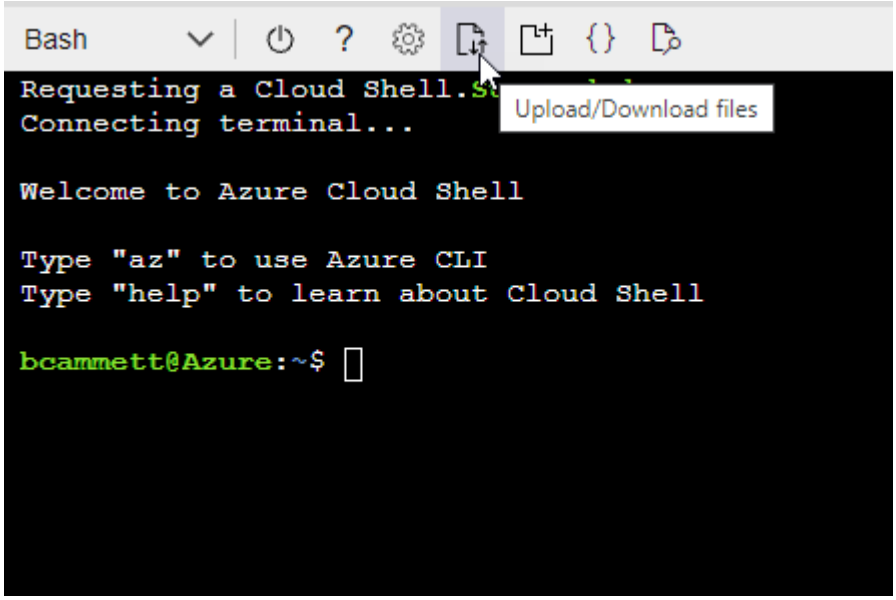
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

   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.



- Azure CLI를 사용하여 사용자 지정 역할을 생성합니다.

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

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

2. 역할에 응용 프로그램을 할당합니다.

   a. Azure 포털에서 * Subscriptions * 서비스를 엽니다.

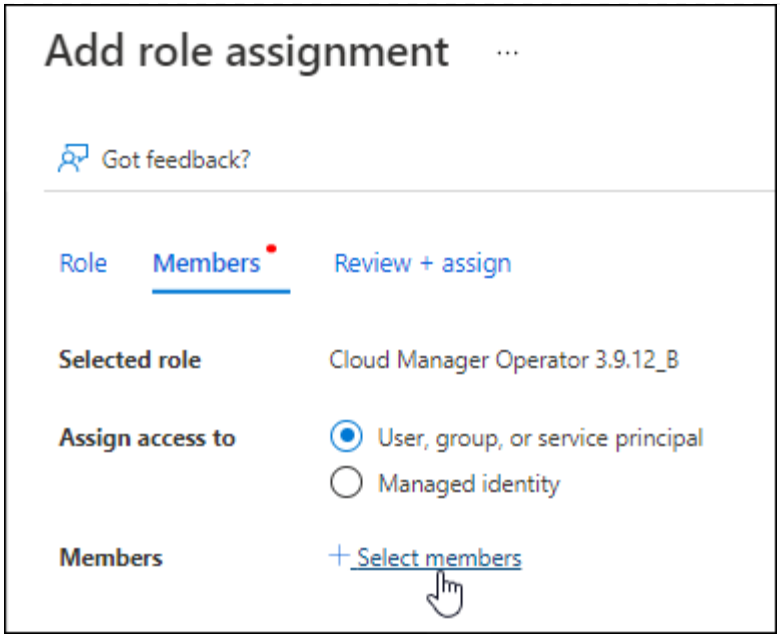
   b. 구독을 선택합니다.

   c. 액세스 제어(IAM) > 추가 > 역할 할당 추가 * 를 선택합니다.

   d. Role * 탭에서 * BlueXP Operator * 역할을 선택하고 * Next * 를 선택합니다.

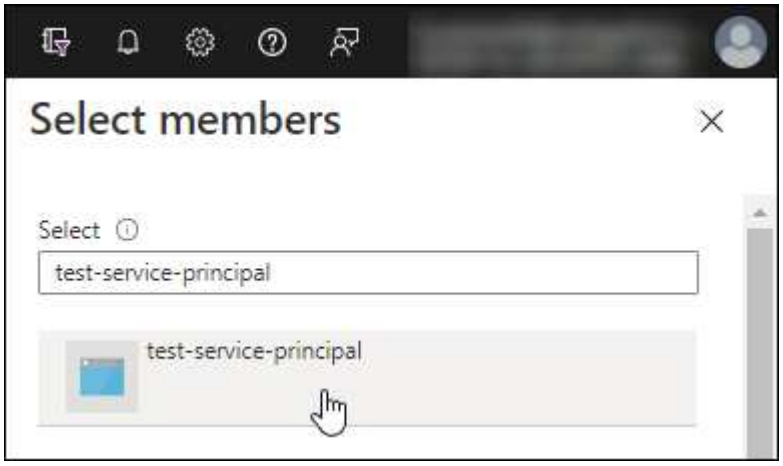
   e. Members* 탭에서 다음 단계를 완료합니다.

      - 사용자, 그룹 또는 서비스 보안 주체 * 를 선택한 상태로 유지합니다.
      - 구성원 선택 * 을 선택합니다.



- 응용 프로그램의 이름을 검색합니다.

  예를 들면 다음과 같습니다.



- 응용 프로그램을 선택하고 * 선택 * 을 선택합니다.
- 다음 * 을 선택합니다.

f. 검토 + 할당 * 을 선택합니다.

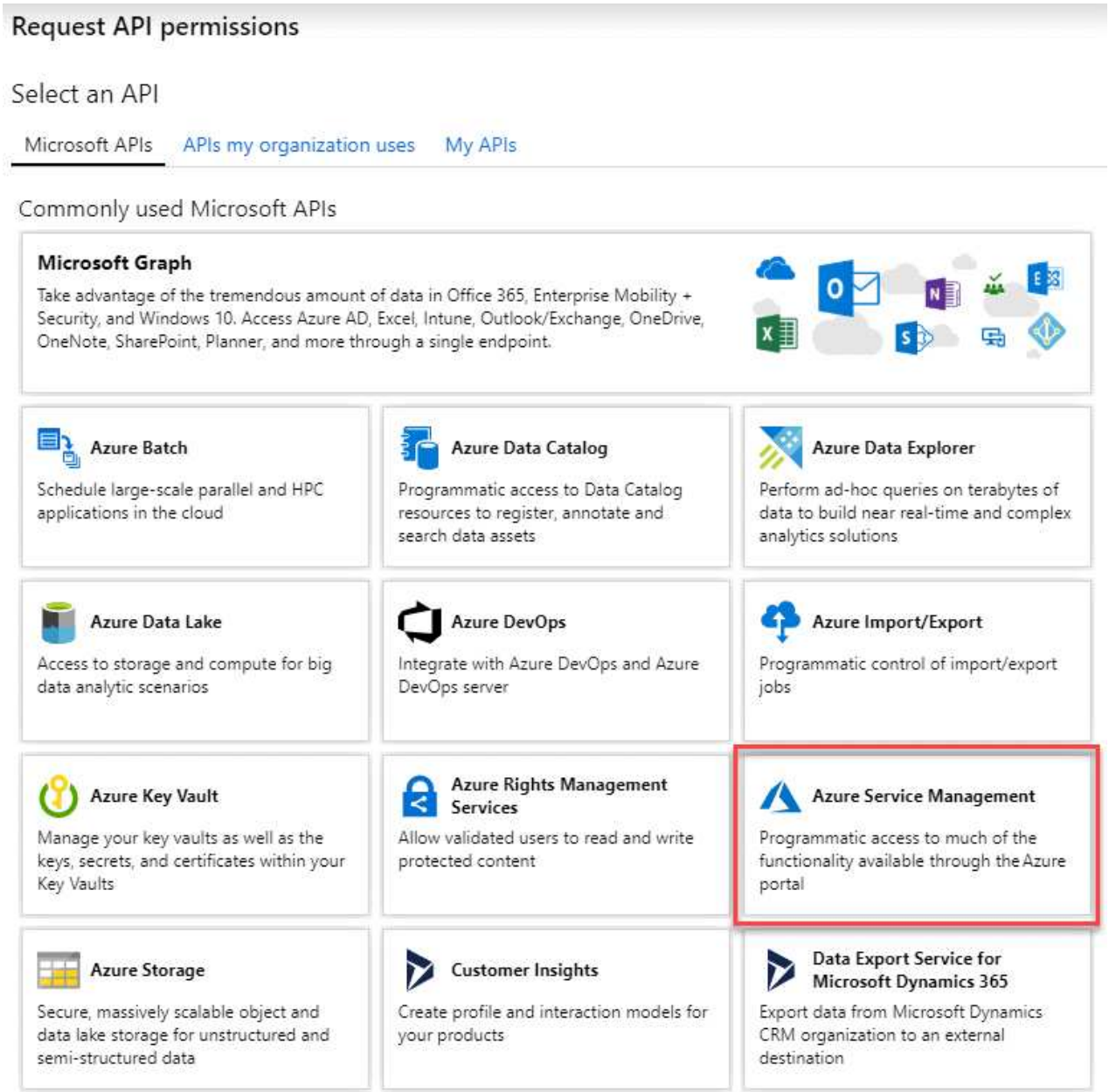
이제 서비스 보안 주체에 Connector를 배포하는 데 필요한 Azure 권한이 있습니다.

여러 Azure 구독에서 Cloud Volumes ONTAP를 배포하려면 서비스 보안 주체를 해당 구독 각각에 바인딩해야 합니다. BlueXP를 사용하면 Cloud Volumes ONTAP를 배포할 때 사용할 구독을 선택할 수 있습니다.

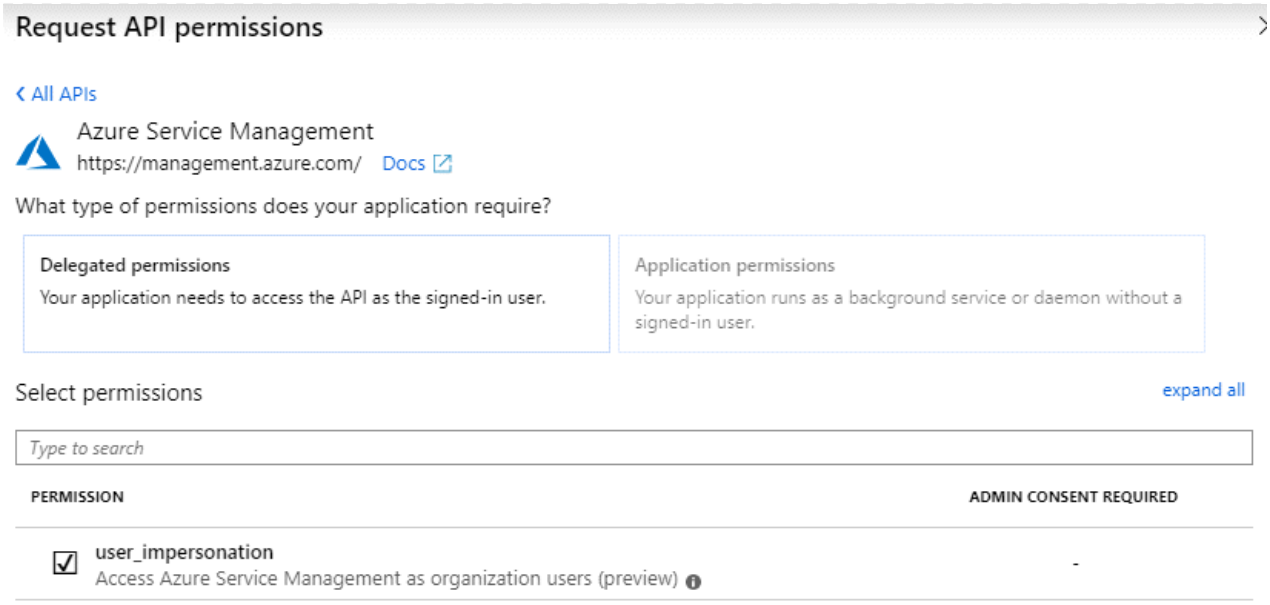
Windows Azure 서비스 관리 **API** 권한을 추가합니다

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.

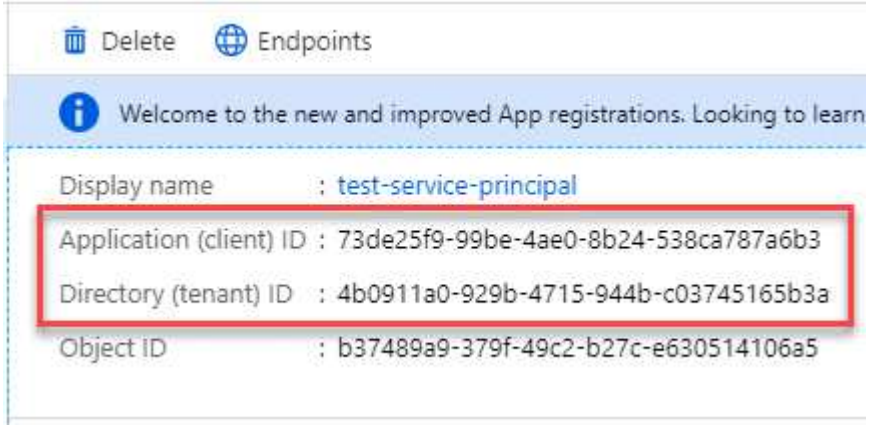


4. Access Azure Service Management as organization users * 를 선택한 다음 * Add permissions * 를 선택합니다.



응용 프로그램의 응용 프로그램 **ID** 및 디렉터리 **ID**를 가져옵니다

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



Azure 계정을 BlueXP에 추가하는 경우 응용 프로그램의 응용 프로그램(클라이언트) ID와 디렉터리(테넌트) ID를 제공해야 합니다. BlueXP는 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 암호를 생성합니다

1. Microsoft Entra ID * 서비스를 엽니다.
2. 앱 등록 * 을 선택하고 응용 프로그램을 선택합니다.
3. 인증서 및 비밀 > 새 클라이언트 비밀 * 을 선택합니다.
4. 비밀과 기간에 대한 설명을 제공하십시오.
5. 추가 * 를 선택합니다.
6. 클라이언트 암호 값을 복사합니다.

이제 BlueXP에서 Microsoft Entra ID를 사용하여 인증하는 클라이언트 암호가 있습니다.

결과

이제 서비스 보안 주체가 설정되었으므로 응용 프로그램(클라이언트) ID, 디렉터리(테넌트) ID 및 클라이언트 암호 값을 복사해야 합니다. Connector를 설치한 후 이러한 자격 증명을 BlueXP의 커넥터와 연결해야 합니다.

4단계**:** 커넥터를 설치합니다

기존 Linux 호스트에서 Connector 소프트웨어를 다운로드하여 설치합니다.

시작하기 전에

다음과 같은 항목이 있어야 합니다.

- 커넥터를 설치할 수 있는 루트 권한
- Connector의 인터넷 액세스에 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

  설치 후 프록시 서버를 구성할 수 있지만 이렇게 하려면 커넥터를 다시 시작해야 합니다.

  BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

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

이 작업에 대해

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

단계

1. Docker가 설정 및 실행 중인지 확인합니다.

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

2. _http_proxy_or_https_proxy_system 변수가 호스트에 설정되어 있으면 이를 제거합니다.

   ```
   unset http_proxy
   unset https_proxy
   ```

   이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

3. 에서 Connector 소프트웨어를 다운로드합니다 "NetApp Support 사이트"를 선택한 다음 Linux 호스트에 복사합니다.

   네트워크 또는 클라우드에서 사용하도록 고안된 "온라인" 커넥터 설치 프로그램을 다운로드해야 합니다. Connector에 대해 별도의 "오프라인" 설치 프로그램을 사용할 수 있지만 전용 모드 배포에서만 지원됩니다.

4. 스크립트를 실행할 권한을 할당합니다.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

   여기서 <version>는 다운로드한 커넥터 버전입니다.

5. 설치 스크립트를 실행합니다.

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

   proxy 및 — cacert 매개 변수는 선택 사항입니다. 프록시 서버가 있는 경우 그림과 같이 매개 변수를 입력해야 합니다. 설치 프로그램에서 프록시에 대한 정보를 제공하라는 메시지를 표시하지 않습니다.

   다음은 두 가지 선택적 매개 변수를 사용하는 명령의 예입니다.

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

   — 프록시는 다음 형식 중 하나를 사용하여 커넥터가 HTTP 또는 HTTPS 프록시 서버를 사용하도록 구성합니다.

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     다음 사항에 유의하십시오.

     - 사용자는 로컬 사용자 또는 도메인 사용자일 수 있습니다.
     - 도메인 사용자의 경우 위에 표시된 \ 에 ASCII 코드를 사용해야 합니다.
     - BlueXP는 @ 문자를 포함하는 암호를 지원하지 않습니다.

   cacert는 Connector와 프록시 서버 간의 HTTPS 액세스에 사용할 CA 서명 인증서를 지정합니다. 이 매개 변수는 HTTPS 프록시 서버를 지정하거나 프록시가 가로채기 프록시인 경우에만 필요합니다.

결과

이제 커넥터가 설치되었습니다. 프록시 서버를 지정한 경우 설치가 끝나면 커넥터 서비스(occm)가 두 번 다시 시작됩니다.

5단계: 커넥터를 설정합니다

등록 또는 로그인한 다음 Connector를 BlueXP 계정과 연동하도록 설정합니다.

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. 가입 또는 로그인
3. 로그인한 후 BlueXP를 설정합니다.
   a. Connector와 연결할 BlueXP 계정을 지정합니다.
   b. 시스템의 이름을 입력합니다.
   c. 에서 * 보안 환경에서 실행 중입니까? * 제한된 모드를 사용하지 않도록 설정합니다.

      이 단계에서는 표준 모드에서 BlueXP를 사용하는 방법을 설명하므로 제한된 모드를 사용하지 않도록 설정해야 합니다. (또한 Connector가 구내에 설치된 경우에는 제한된 모드가 지원되지 않습니다.)

   d. Let’s start * 를 선택합니다.

결과

BlueXP는 이제 방금 설치한 커넥터를 사용하여 설정됩니다.

6단계: BlueXP에 권한 제공

커넥터를 설치하고 설정한 후에 BlueXP가 AWS 또는 Azure에서 작업을 수행하는 데 필요한 권한을 갖도록 클라우드 자격 증명을 추가합니다.

설치하고

시작하기 전에

AWS에서 이러한 자격 증명을 방금 생성한 경우 사용할 수 있을 때까지 몇 분 정도 걸릴 수 있습니다. BlueXP에 자격 증명을 추가하기 전에 몇 분 정도 기다립니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

2. 자격 증명 추가 * 를 선택하고 마법사의 단계를 따릅니다.
   a. * 자격 증명 위치 *: * Amazon Web Services > Connector * 를 선택합니다.
   b. * 자격 증명 정의 *: AWS 액세스 키와 비밀 키를 입력합니다.
   c. * Marketplace 구독 *: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 선택합니다.

결과

BlueXP는 이제 AWS에서 사용자 대신 작업을 수행하는 데 필요한 권한을 가집니다.

이제 로 이동할 수 있습니다 "BlueXP 콘솔" 을 눌러 BlueXP에서 커넥터 사용을 시작합니다.

Azure를 지원합니다

시작하기 전에

Azure에서 이러한 자격 증명을 만든 경우 사용할 수 있을 때까지 몇 분 정도 걸릴 수 있습니다. BlueXP에 자격 증명을 추가하기 전에 몇 분 정도 기다립니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

2. 자격 증명 추가 * 를 선택하고 마법사의 단계를 따릅니다.
   a. * 자격 증명 위치 *: * Microsoft Azure > 커넥터 * 를 선택합니다.
   b. * 자격 증명 정의 *: 필요한 권한을 부여하는 Microsoft Entra 서비스 보안 주체에 대한 정보를 입력합니다.
      - 애플리케이션(클라이언트) ID입니다
      - 디렉토리(테넌트) ID입니다
      - 클라이언트 암호
   c. * Marketplace 구독 *: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과

연결합니다.

d. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 선택합니다.

결과

이제 BlueXP는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 가지고 있습니다. 이제 로 이동할 수 있습니다 "BlueXP 콘솔" 을 눌러 BlueXP에서 커넥터 사용을 시작합니다.

BlueXP 구독(표준 모드)

클라우드 공급업체의 시장에서 BlueXP를 구독하여 시간당 요금(PAYGO)이나 연간 계약을 통해 BlueXP 서비스 비용을 지불하십시오. NetApp(BYOL)에서 라이센스를 구입한 경우에도 마켓플레이스 제품을 구독해야 합니다. 라이센스 비용이 항상 먼저 청구되지만 라이센스 용량을 초과하거나 라이센스 기간이 만료되면 시간당 요금이 부과됩니다.

마켓플레이스에 가입하면 다음 BlueXP 서비스에 대한 비용을 청구할 수 있습니다.

- 백업 및 복구
- 분류
- Cloud Volumes ONTAP
- 계층화

시작하기 전에

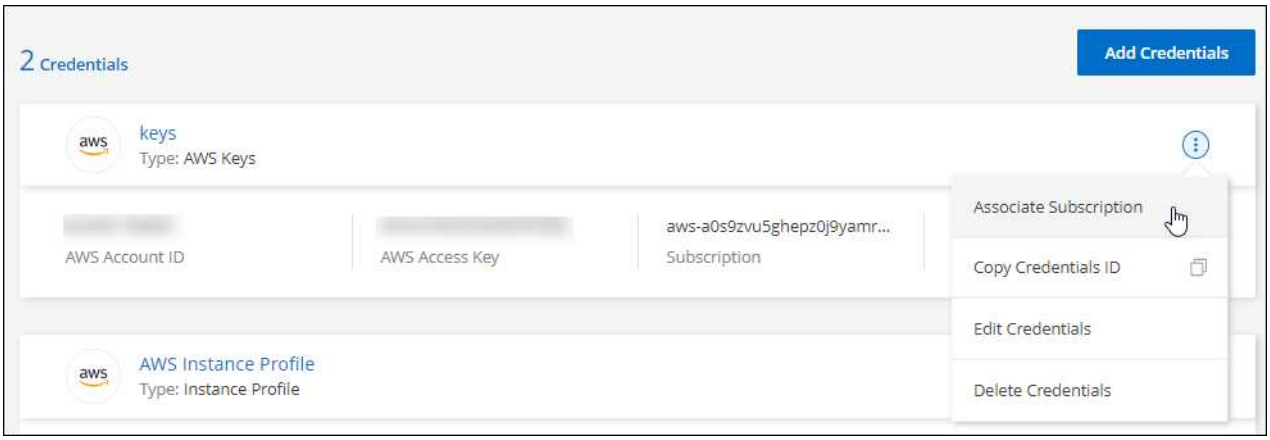
BlueXP를 구독하려면 Connector와 연결된 클라우드 자격 증명과 마켓플레이스 구독을 연결해야 합니다. "표준 모드 시작" 워크플로를 따랐다면 이미 Connector가 있는 것입니다. 자세한 내용은 를 참조하십시오 "표준 모드에서 BlueXP를 빠르게 시작합니다".

설치하고

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 선택한 다음 * 가입 연결 * 을 선택합니다.

   Connector와 연결된 자격 증명을 선택해야 합니다. BlueXP와 연결된 자격 증명과 마켓플레이스 구독을 연결할 수 없습니다.



3. 자격 증명을 기존 구독과 연결하려면 드롭다운 목록에서 구독을 선택하고 * Associate * 를 선택합니다.
4. 자격 증명을 새 구독과 연결하려면 * 구독 추가 > 계속 * 을 선택하고 AWS 마켓플레이스의 단계를 따릅니다.

   a. 구매 옵션 보기 * 를 선택합니다.
   b. 가입 * 을 선택합니다.
   c. 계정 설정 * 을 선택합니다.

      BlueXP 웹 사이트로 이동합니다.

   d. [구독 할당 *] 페이지에서:

      - 이 구독을 연결할 BlueXP 계정을 선택합니다.
      - 기존 구독 바꾸기 * 필드에서 하나의 계정에 대한 기존 구독을 이 새 구독으로 자동 대체할지 여부를 선택합니다.

        BlueXP는 계정의 모든 자격 증명에 대한 기존 구독을 이 새 구독으로 대체합니다. 자격 증명 집합이 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

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

      - 저장 * 을 선택합니다.

        다음 비디오에서는 AWS 마켓플레이스를 구독하는 단계를 보여줍니다.

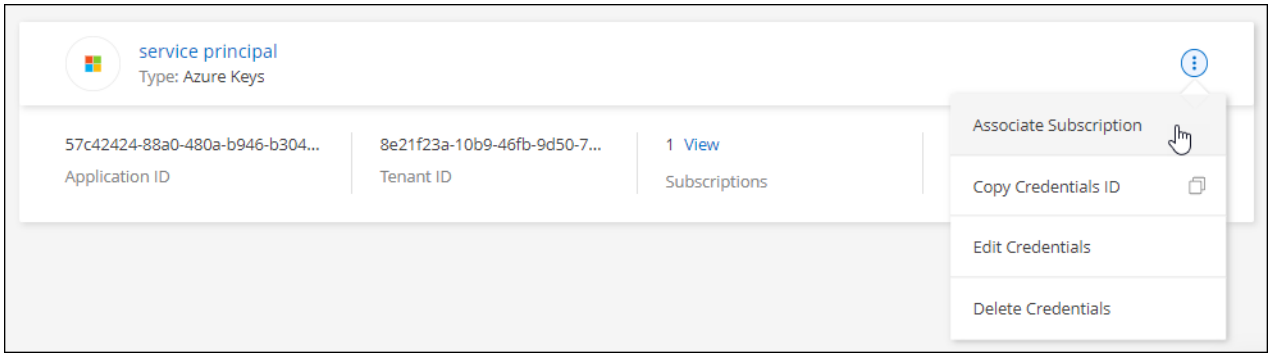
   AWS 마켓플레이스에서 BlueXP를 구독하십시오

Azure를 지원합니다

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 선택한 다음 * 가입 연결 * 을 선택합니다.

   Connector와 연결된 자격 증명을 선택해야 합니다. BlueXP와 연결된 자격 증명과 마켓플레이스 구독을 연결할 수 없습니다.



3. 자격 증명을 기존 구독과 연결하려면 드롭다운 목록에서 구독을 선택하고 * Associate * 를 선택합니다.
4. 자격 증명을 새 구독과 연결하려면 * 구독 추가 > 계속 * 을 선택하고 Azure 마켓플레이스의 단계를 따릅니다.

   a. 메시지가 표시되면 Azure 계정에 로그인합니다.
   b. 가입 * 을 선택합니다.
   c. 양식을 작성하고 * Subscribe * 를 선택합니다.
   d. 가입 프로세스가 완료되면 * 지금 계정 구성 * 을 선택합니다.

      BlueXP 웹 사이트로 이동합니다.

   e. [구독 할당 *] 페이지에서:

      - 이 구독을 연결할 BlueXP 계정을 선택합니다.
      - 기존 구독 바꾸기 * 필드에서 하나의 계정에 대한 기존 구독을 이 새 구독으로 자동 대체할지 여부를 선택합니다.

        BlueXP는 계정의 모든 자격 증명에 대한 기존 구독을 이 새 구독으로 대체합니다. 자격 증명 집합이 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

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

      - 저장 * 을 선택합니다.

        다음 비디오에서는 Azure 마켓플레이스에서 구독하는 단계를 보여 줍니다.

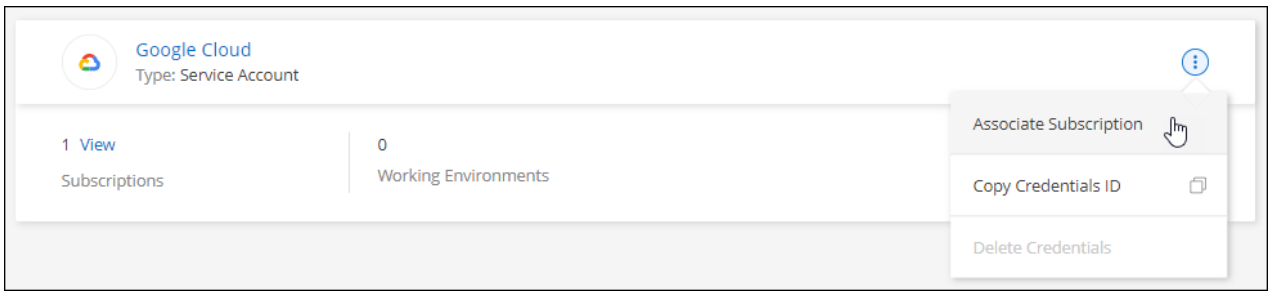
   Azure 마켓플레이스에서 BlueXP를 구독하십시오

Google 클라우드

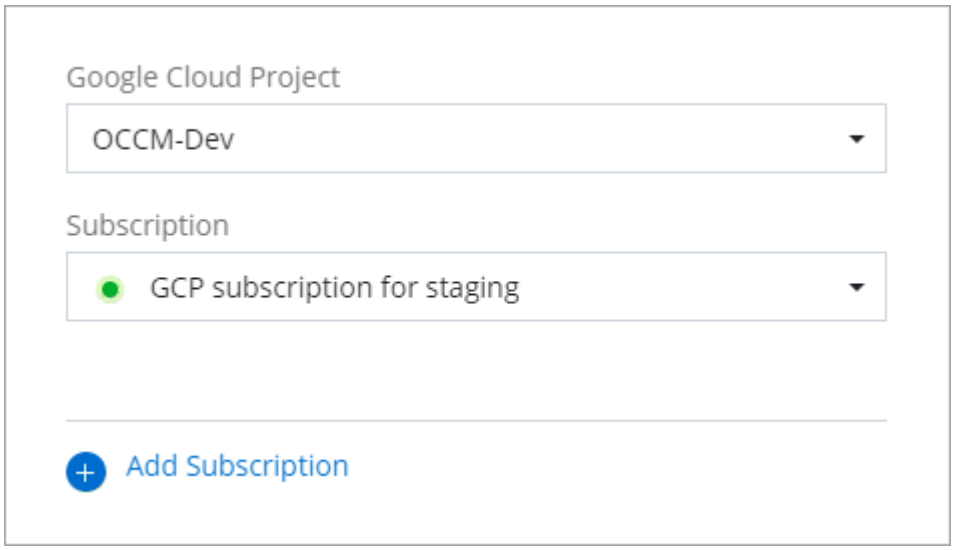
단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

2. 자격 증명 집합에 대한 작업 메뉴를 선택한 다음 * 가입 연결 * 을 선택합니다.



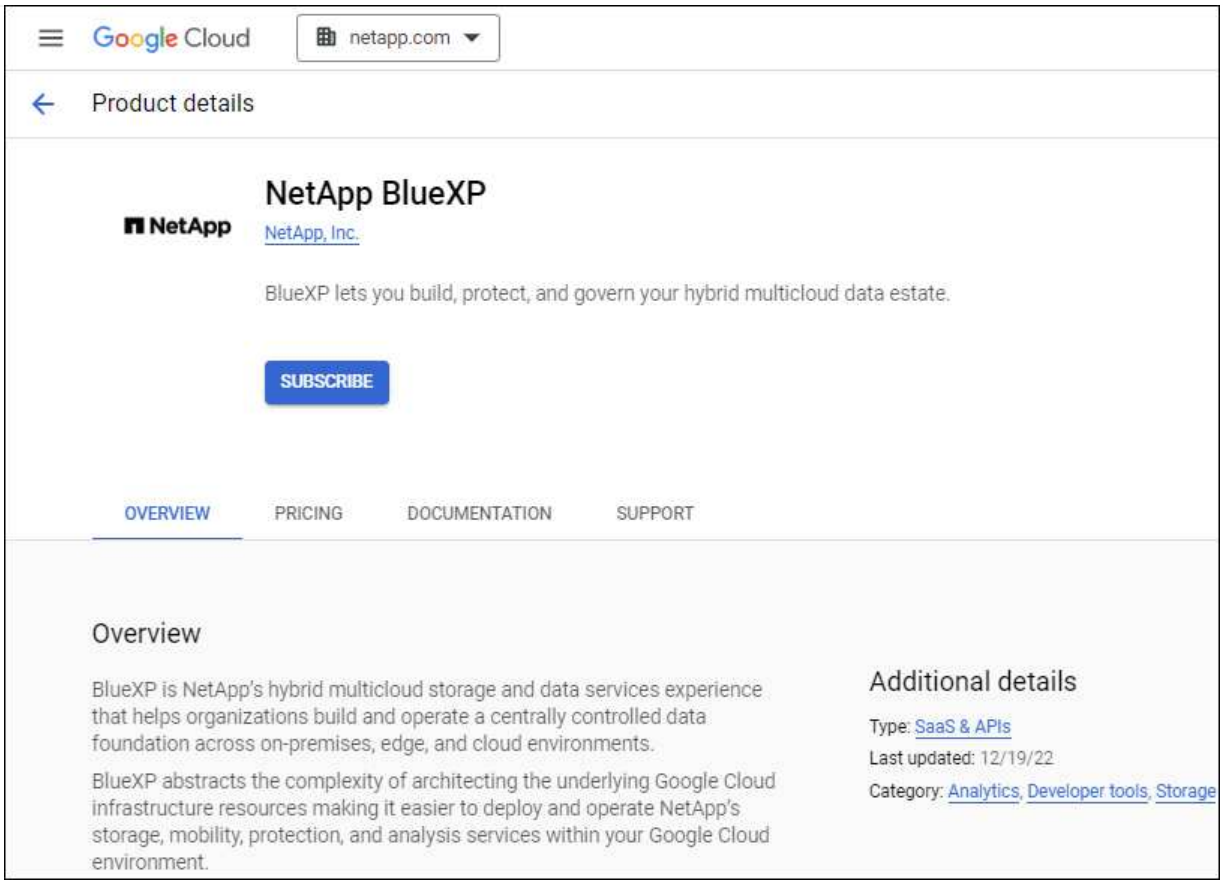
3. 자격 증명을 기존 구독과 연결하려면 아래 목록에서 Google Cloud 프로젝트 및 구독을 선택한 다음 * Associate * 를 선택합니다.



4. 아직 구독이 없는 경우 * 구독 추가 > 계속 * 을 선택하고 Google Cloud Marketplace의 단계를 따릅니다.

> 다음 단계를 완료하기 전에 Google Cloud 계정과 BlueXP 로그인에 Billing Admin 권한이 모두 있는지 확인하십시오.

   a. 로 리디렉션된 후 "Google Cloud 마켓플레이스의 NetApp BlueXP 페이지"상단 탐색 메뉴에서 올바른 프로젝트가 선택되어 있는지 확인합니다.



b. 가입 * 을 선택합니다.

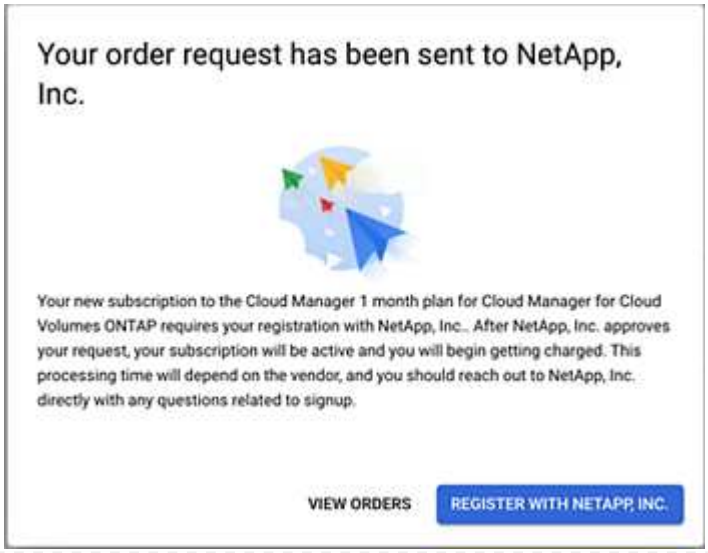
c. 적절한 청구 계정을 선택하고 이용 약관에 동의합니다.

d. 가입 * 을 선택합니다.

   이 단계에서는 전송 요청을 NetApp에 전송합니다.

e. 팝업 대화 상자에서 * Register with NetApp, Inc. * 를 선택합니다

   Google Cloud 구독을 BlueXP 계정에 연결하려면 이 단계를 완료해야 합니다. 이 페이지에서 리디렉션된 다음 BlueXP에 로그인할 때까지 가입 연결 프로세스가 완료되지 않습니다.



f. 구독 할당 * 페이지의 단계를 완료합니다.

> 조직의 누군가가 청구 계정에서 NetApp BlueXP 구독을 이미 구독한 경우 으로 리디렉션됩니다 "BlueXP 웹 사이트의 Cloud Volumes ONTAP 페이지" 대신 예기치 않은 상황인 경우 NetApp 세일즈 팀에 문의하십시오. Google은 Google 청구 계정당 하나의 가입만 활성화합니다.

- 이 구독을 연결할 BlueXP 계정을 선택합니다.
- 기존 구독 바꾸기 * 필드에서 하나의 계정에 대한 기존 구독을 이 새 구독으로 자동 대체할지 여부를 선택합니다.

  BlueXP는 계정의 모든 자격 증명에 대한 기존 구독을 이 새 구독으로 대체합니다. 자격 증명 집합이 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

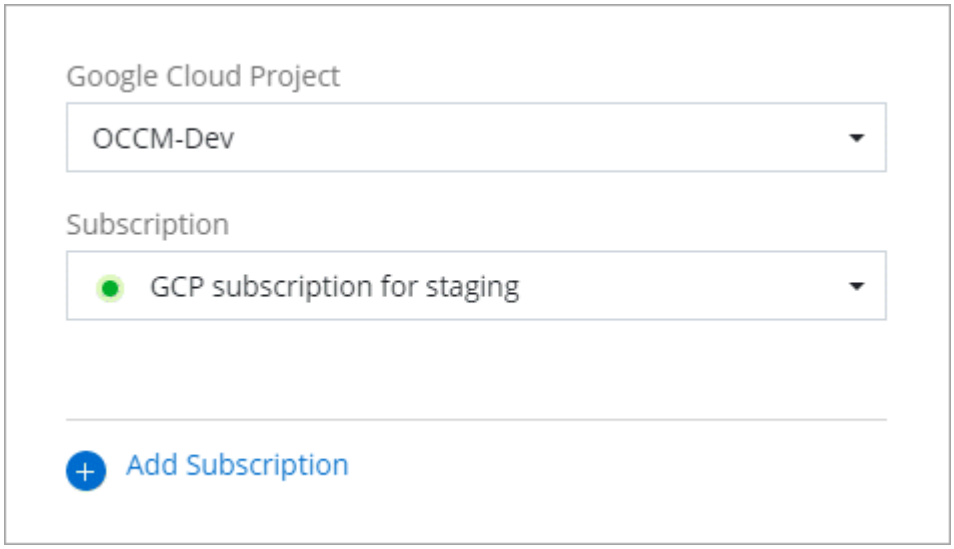
다른 모든 계정의 경우 이 단계를 반복하여 구독을 수동으로 연결해야 합니다.

- 저장 * 을 선택합니다.

  다음 비디오에서는 Google Cloud Marketplace를 구독하는 단계를 보여줍니다.

Google Cloud 마켓플레이스에서 BlueXP를 구독하십시오

a. 이 프로세스가 완료되면 BlueXP의 자격 증명 페이지로 돌아가서 이 새 구독을 선택합니다.



관련 링크

- "Cloud Volumes ONTAP용 BYOL 용량 기반 라이센스 관리"
- "BlueXP 데이터 서비스에 대한 BYOL 라이센스 관리"
- "BlueXP에 대한 AWS 자격 증명 및 구독을 관리합니다"
- "BlueXP용 Azure 자격 증명 및 구독을 관리합니다"
- "BlueXP용 Google Cloud 자격 증명 및 구독을 관리합니다"

다음에 할 수 있는 일(표준 모드)

이제 표준 모드에서 BlueXP에 로그인하고 설정했으므로 사용자는 작업 환경을 생성 및 검색하고 BlueXP 데이터 서비스를 사용할 수 있습니다.

> AWS, Microsoft Azure 또는 Google Cloud에 Connector를 설치한 경우 BlueXP는 Connector가 설치된 위치에서 Amazon S3 버킷, Azure Blob 스토리지 또는 Google Cloud 스토리지 버킷에 대한 정보를 자동으로 검색합니다. 작업 환경은 BlueXP 캔버스에 자동으로 추가됩니다.

도움말을 보려면 로 이동합니다 "BlueXP 설명서 홈 페이지" 모든 BlueXP 서비스에 대한 문서를 봅니다.

관련 링크

"BlueXP 배포 모드"

제한된 모드로 시작하십시오

워크플로 시작(제한된 모드)

사용자 환경을 준비하고 커넥터를 배포하고 BlueXP에 가입하여 제한된 모드에서 BlueXP를 시작하십시오.

제한 모드는 일반적으로 AWS GovCloud 및 Azure Government 지역의 구축을 비롯하여 주 정부 및 지방 정부 및 규제 회사에서 사용합니다. 시작하기 전에 에 대한 이해가 있어야 합니다 "BlueXP 계정", "커넥터", 및 "배포 모드".

1 "배포를 준비합니다"

1. CPU, RAM, 디스크 공간, Docker Engine 등에 대한 요구사항을 충족하는 전용 Linux 호스트를 준비합니다.
2. 대상 네트워크에 대한 액세스, 수동 설치를 위한 아웃바운드 인터넷 액세스 및 일상적인 액세스를 위한 아웃바운드 인터넷을 제공하는 네트워킹을 설정합니다.
3. 배포 후 해당 권한을 Connector 인스턴스에 연결할 수 있도록 클라우드 공급자에 권한을 설정합니다.

2 "커넥터를 배포합니다"

1. 클라우드 공급자의 마켓플레이스에서 Connector를 설치하거나 자체 Linux 호스트에 소프트웨어를 수동으로 설치합니다.
2. 웹 브라우저를 열고 Linux 호스트의 IP 주소를 입력하여 BlueXP를 설정합니다.
3. 이전에 설정한 권한을 BlueXP에 제공합니다.

3 **"BlueXP에 가입하십시오"**

클라우드 공급업체의 시장에서 BlueXP를 구독하여 시간당 요금(PAYGO)이나 연간 계약을 통해 BlueXP 서비스 비용을 지불하십시오.

제한된 모드에서 배포를 준비합니다

제한된 모드로 BlueXP를 배포하기 전에 환경을 준비합니다. 예를 들어 호스트 요구 사항을 검토하고, 네트워킹을 준비하고, 사용 권한을 설정하는 등의 작업을 수행해야 합니다.

1단계**:** 제한 모드의 작동 방식을 이해합니다

시작하기 전에 제한된 모드에서 BlueXP의 작동 방식을 이해해야 합니다.

예를 들어, 설치할 BlueXP Connector에서 로컬로 사용할 수 있는 브라우저 기반 인터페이스를 사용해야 합니다. SaaS 계층을 통해 제공되는 웹 기반 콘솔에서 BlueXP에 액세스할 수 없습니다.

또한 모든 BlueXP 서비스를 사용할 수 있는 것은 아닙니다.

"제한 모드의 작동 방식에 대해 알아보십시오".

단계 **2:** 설치 옵션을 검토합니다

제한된 모드에서는 클라우드에만 Connector를 설치할 수 있습니다. 다음 설치 옵션을 사용할 수 있습니다.

- 다운로드: AWS 마켓플레이스
- 다운로드: Azure 마켓플레이스
- AWS, Azure 또는 Google Cloud에서 실행 중인 자체 Linux 호스트에 Connector를 수동으로 설치합니다

3단계**:** 호스트 요구 사항을 검토합니다

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

AWS 또는 Azure Marketplace에서 Connector를 구축하면 필요한 OS 및 소프트웨어 구성요소가 이미지에 포함됩니다. CPU 및 RAM 요구 사항에 맞는 인스턴스 유형을 선택하기만 하면 됩니다.

전용 호스트

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

지원되는 운영 체제

- 우분투 22.04 LTS
- CentOS 7.6, 7.7, 7.8 및 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 및 7.9

  호스트는 Red Hat Subscription Management에 등록되어 있어야 합니다. 등록되지 않은 경우 호스트는 Connector 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.

  Connector는 이러한 운영 체제의 영어 버전에서 지원됩니다.

하이퍼바이저

Ubuntu, CentOS 또는 Red Hat Enterprise Linux 실행 인증을 받은 베어 메탈 또는 호스팅된 하이퍼바이저가 필요합니다.

"Red Hat 솔루션: Red Hat Enterprise Linux 실행 인증을 받은 하이퍼바이저는 무엇입니까?"

CPU

코어 4개 또는 vCPU 4개

RAM

14GB

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.

Google Cloud 컴퓨터 유형입니다

위의 CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. n2-standard-4를 추천합니다.

Connector는 를 지원하는 OS가 있는 VM 인스턴스의 Google Cloud에서 지원됩니다 "차폐된 VM 기능"

/opt의 디스크 공간입니다

100GiB의 공간을 사용할 수 있어야 합니다

/var의 디스크 공간입니다

20GiB의 공간을 사용할 수 있어야 합니다

Docker 엔진

Connector를 설치하기 전에 Docker 엔진이 호스트에 필요합니다.

- 지원되는 최소 버전은 19.3.1입니다.
- 지원되는 최대 버전은 25.0.5입니다.

"설치 지침을 봅니다"

4단계**:** 네트워킹을 준비합니다

Connector가 공용 클라우드 환경 내에서 리소스 및 프로세스를 관리할 수 있도록 네트워킹을 설정합니다. Connector에 대한 가상 네트워크 및 서브넷을 사용하는 것 외에 다음 요구 사항이 충족되는지 확인해야 합니다.

대상 네트워크에 대한 연결

Connector는 저장소를 관리하려는 위치에 대한 네트워크 연결이 있어야 합니다. 예를 들어, Cloud Volumes ONTAP를 구축할 계획인 VPC 또는 VNET, 온프레미스 ONTAP 클러스터가 상주하는 데이터 센터 등이 있습니다.

BlueXP 콘솔에 대한 사용자 액세스를 위한 네트워킹을 준비합니다

제한된 모드에서는 커넥터에서 BlueXP 사용자 인터페이스에 액세스할 수 있습니다. BlueXP 사용자 인터페이스를 사용할 때 데이터 관리 작업을 완료하기 위해 몇 개의 엔드포인트에 연결합니다. 이러한 엔드포인트는 BlueXP 콘솔에서 특정 작업을 완료할 때 사용자 컴퓨터에서 연결됩니다.

엔드포인트	목적
https://signin.b2c.netapp.com	NetApp Support 사이트(NSS) 자격 증명을 업데이트하거나 BlueXP에 새 NSS 자격 증명을 추가하는 데 필요합니다.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	웹 브라우저는 BlueXP를 통한 중앙 집중식 사용자 인증을 위해 이러한 엔드포인트에 연결됩니다.
https://widget.intercom.io	제품 내에서 NetApp 클라우드 전문가와 상담할 수 있는 채팅을 제공합니다.

수동 설치 중에 연결된 끝점입니다

자체 Linux 호스트에 커넥터를 수동으로 설치할 경우 Connector 설치 과정에서 다음 URL에 액세스해야 합니다.

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  Azure Government 지역에서는 이 끝점이 필요하지 않습니다.

- https://occmclientinfragov.azurecr.us

  이 엔드포인트는 Azure Government 지역에서만 필요합니다.

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

일상적인 작업을 위한 아웃바운드 인터넷 액세스

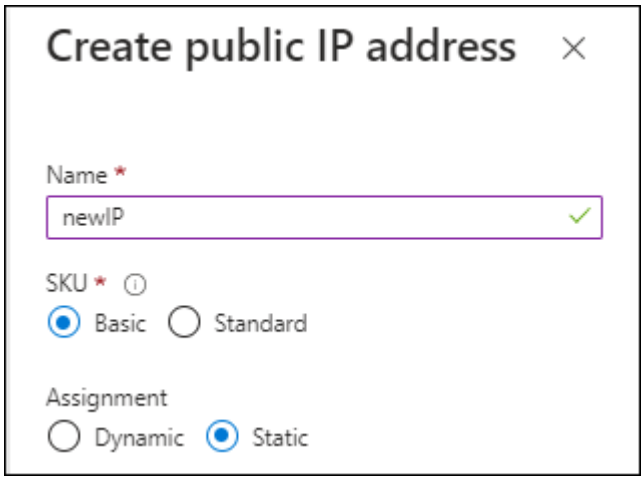
커넥터를 배포하는 네트워크 위치에 아웃바운드 인터넷 연결이 있어야 합니다. Connector는 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하기 위해 다음 엔드포인트에 연결하는 아웃바운드 인터넷 액세스를 필요로 합니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • CloudFormation 을 참조하십시오 • EC2(탄력적인 컴퓨팅 클라우드) • IAM(Identity and Access Management) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • S3(Simple Storage Service)	를 사용하여 AWS에서 리소스를 관리합니다. 정확한 끝점은 사용 중인 AWS 지역에 따라 다릅니다. "자세한 내용은 AWS 설명서를 참조하십시오"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure 공공 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 중국 지역의 리소스를 관리합니다.
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://www.googleapis.com/deploymentmanager/v2/projects	Google Cloud에서 리소스를 관리합니다.
https://support.netapp.com 으로 문의하십시오 https://mysupport.netapp.com 으로 문의하십시오	라이센스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다.

엔드포인트	목적
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	BlueXP 내에서 SaaS 기능 및 서비스를 제공합니다. 현재 Connector가 "cloudmanager.cloud.netapp.com" 에 문의하고 있지만 곧 출시될 릴리스에서 "api.bluexp.netapp.com" 에 연락하기 시작합니다.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io Azure Government 지역에서는 이 끝점이 필요하지 않습니다. https://occmclientinfragov.azurecr.us 이 엔드포인트는 Azure Government 지역에서만 필요합니다.	Connector 및 해당 Docker 구성 요소를 업그레이드합니다.

Azure의 공용 **IP** 주소입니다

Azure의 커넥터 VM에서 공용 IP 주소를 사용하려면 IP 주소가 기본 SKU를 사용하여 BlueXP가 이 공용 IP 주소를 사용하도록 해야 합니다.



대신 표준 SKU IP 주소를 사용하는 경우 BlueXP는 공용 IP 대신 Connector의 _private_ip 주소를 사용합니다. BlueXP 콘솔에 액세스하는 데 사용하는 시스템에서 해당 개인 IP 주소에 액세스할 수 없는 경우 BlueXP 콘솔의 작업이 실패합니다.

"Azure 설명서: 공용 IP SKU"

프록시 서버

조직에서 모든 나가는 인터넷 트래픽에 대해 프록시 서버를 배포해야 하는 경우 HTTP 또는 HTTPS 프록시에 대한 다음 정보를 가져옵니다. 설치하는 동안 이 정보를 제공해야 합니다.

- IP 주소입니다
- 자격 증명

- HTTPS 인증서

BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

포트

커넥터를 시작하거나 커넥터가 Cloud Volumes ONTAP에서 NetApp 지원으로 AutoSupport 메시지를 보내는 프록시로 사용되지 않는 한 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.
- 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 보내기 위한 아웃바운드 인터넷 연결이 없는 경우 BlueXP는 자동으로 해당 시스템이 커넥터에 포함된 프록시 서버를 사용하도록 구성합니다. 유일한 요구 사항은 커넥터 보안 그룹이 포트 3128을 통한 인바운드 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

NTP를 활성화합니다

BlueXP 분류를 사용하여 회사 데이터 소스를 검사하려는 경우 BlueXP Connector 시스템과 BlueXP 분류 시스템 모두에서 NTP(Network Time Protocol) 서비스를 활성화하여 시스템 간에 시간이 동기화되도록 해야 합니다. "BlueXP 분류에 대해 자세히 알아보십시오"

클라우드 공급자의 마켓플레이스에서 Connector를 만들려는 경우 Connector를 만든 후에 이 네트워킹 요구 사항을 구현해야 합니다.

단계**: 5** 클라우드 사용 권한을 준비합니다

BlueXP는 가상 네트워크에 Cloud Volumes ONTAP를 배포하고 BlueXP 데이터 서비스를 사용하려면 클라우드 공급업체의 권한이 필요합니다. 클라우드 공급자에서 사용 권한을 설정한 다음 해당 사용 권한을 Connector에 연결해야 합니다.

필요한 단계를 보려면 클라우드 공급자에 사용할 인증 옵션을 선택합니다.

AWS IAM 역할

IAM 역할을 사용하여 Connector에 권한을 제공합니다.

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

자체 Linux 호스트에 Connector를 수동으로 설치하는 경우 EC2 인스턴스에 해당 역할을 연결해야 합니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책 생성:
   a. 정책 > 정책 생성 * 을 선택합니다.
   b. JSON * 을 선택하고 의 내용을 복사하여 붙여 넣습니다 "Connector에 대한 IAM 정책".
   c. 나머지 단계를 완료하고 정책을 생성합니다.
3. IAM 역할 생성:
   a. 역할 > 역할 생성 * 을 선택합니다.
   b. AWS 서비스 > EC2 * 를 선택합니다.
   c. 방금 만든 정책을 첨부하여 사용 권한을 추가합니다.
   d. 나머지 단계를 완료해서 역할을 만듭니다.

결과

이제 커넥터 EC2 인스턴스에 대해 IAM 역할이 있습니다.

AWS 액세스 키입니다

IAM 사용자에 대한 권한 및 액세스 키를 설정합니다. Connector를 설치하고 BlueXP를 설정한 후 BlueXP에 AWS 액세스 키를 제공해야 합니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책 생성:
   a. 정책 > 정책 생성 * 을 선택합니다.
   b. JSON * 을 선택하고 의 내용을 복사하여 붙여 넣습니다 "Connector에 대한 IAM 정책".
   c. 나머지 단계를 완료하고 정책을 생성합니다.

      사용할 BlueXP 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다.

   표준 영역의 경우 권한이 두 정책에 분산됩니다. AWS에서 관리되는 정책의 최대 문자 크기 제한으로 인해 두 개의 정책이 필요합니다. "Connector에 대한 IAM 정책에 대해 자세히 알아보십시오".
3. IAM 사용자에게 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"

4. 커넥터를 설치한 후 BlueXP에 추가할 수 있는 액세스 키가 사용자에게 있는지 확인합니다.

결과

이제 계정에 필요한 권한이 있습니다.

Azure 역할

필요한 권한이 있는 Azure 사용자 지정 역할을 만듭니다. 이 역할을 Connector VM에 할당합니다.

Azure 포털, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 생성할 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 생성하는 방법을 보여 줍니다. 다른 방법을 사용하려면 을 참조하십시오 "Azure 문서"

단계

1. 소프트웨어를 자체 호스트에 수동으로 설치하려는 경우 사용자 지정 역할을 통해 필요한 Azure 권한을 제공할 수 있도록 VM에서 시스템에서 할당한 관리 ID를 사용하도록 설정합니다.

   "Microsoft Azure 설명서: Azure 포털을 사용하여 VM의 Azure 리소스에 대해 관리되는 ID를 구성합니다"

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

   BlueXP에서 사용할 각 Azure 구독에 대한 ID를 추가해야 합니다.

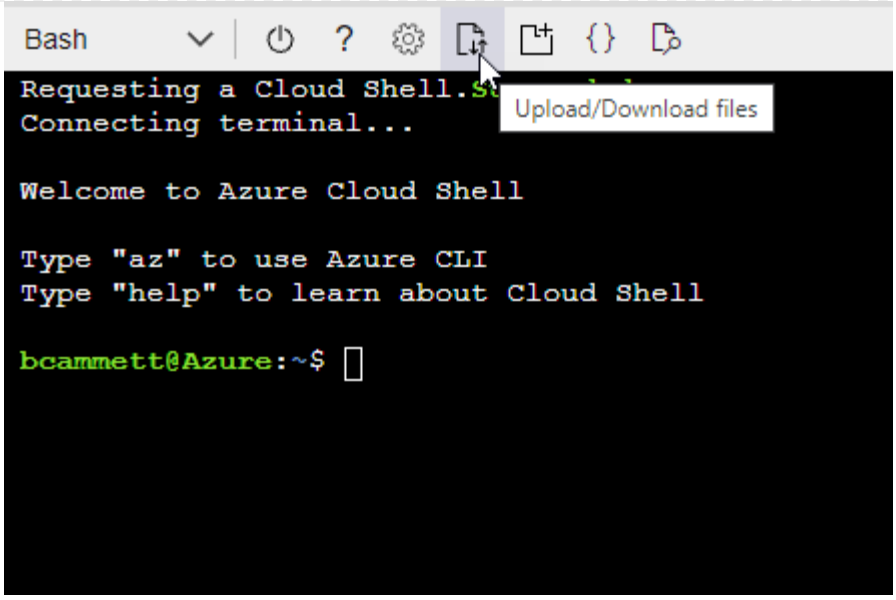
   - 예 *

```
"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 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. Azure CLI를 사용하여 사용자 지정 역할을 생성합니다.

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

결과

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

Azure 서비스 보안 주체

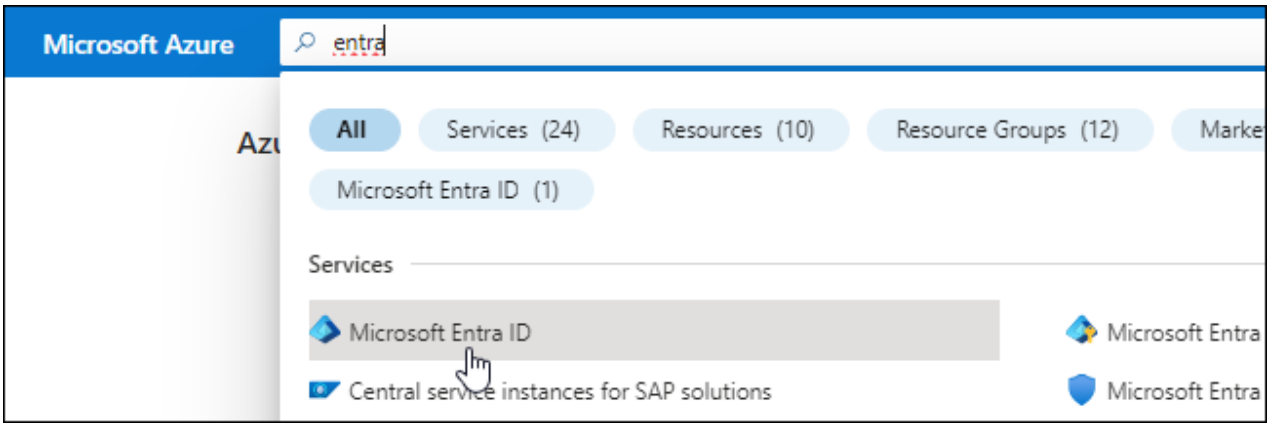
Microsoft Entra ID에서 서비스 주체를 생성 및 설정하고 BlueXP에 필요한 Azure 자격 증명을 받습니다. Connector를 설치하고 BlueXP를 설정한 후 이러한 자격 증명을 BlueXP에 제공해야 합니다.

역할 기반 액세스 제어를 위한 **Microsoft Entra** 응용 프로그램을 만듭니다

1. Azure에서 Active Directory 응용 프로그램을 만들고 응용 프로그램을 역할에 할당할 수 있는 권한이 있는지 확인합니다.

   자세한 내용은 을 참조하십시오 "Microsoft Azure 문서: 필요한 권한"

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



3. 메뉴에서 * 앱 등록 * 을 선택합니다.
4. 새 등록 * 을 선택합니다.
5. 응용 프로그램에 대한 세부 정보를 지정합니다.
   - * 이름 *: 응용 프로그램의 이름을 입력합니다.
   - * 계정 유형 *: 계정 유형을 선택합니다(모두 BlueXP에서 사용 가능).
   - * URI 리디렉션 *: 이 필드는 비워 둘 수 있습니다.
6. Register * 를 선택합니다.

   AD 응용 프로그램 및 서비스 보안 주체를 만들었습니다.

애플리케이션에 역할을 할당합니다

1. 사용자 지정 역할 만들기:

   Azure 포털, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 생성할 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 생성하는 방법을 보여 줍니다. 다른 방법을 사용하려면 을 참조하십시오 "Azure 문서"

   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.

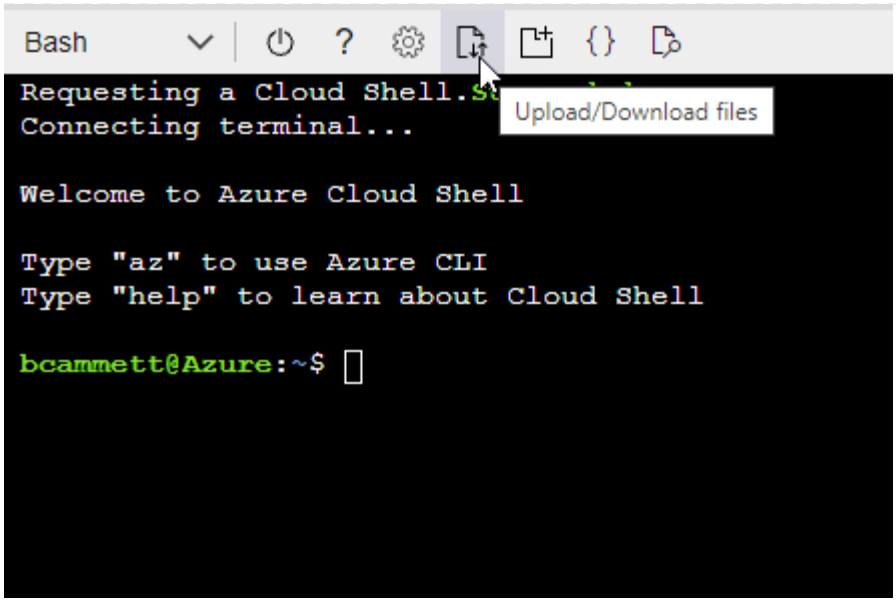
      - 예 *

      ```
      "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.



- Azure CLI를 사용하여 사용자 지정 역할을 생성합니다.

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

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

2. 역할에 응용 프로그램을 할당합니다.

   a. Azure 포털에서 * Subscriptions * 서비스를 엽니다.

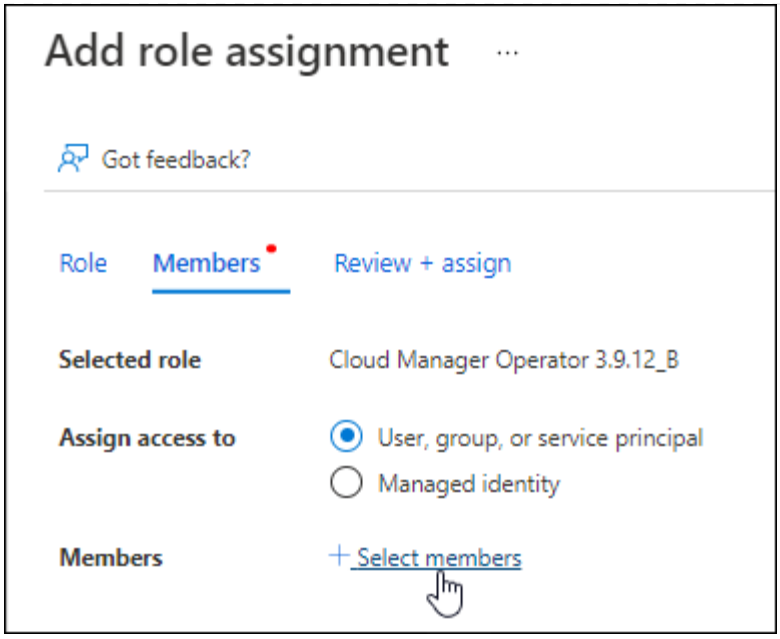
   b. 구독을 선택합니다.

   c. 액세스 제어(IAM) > 추가 > 역할 할당 추가 * 를 선택합니다.

   d. Role * 탭에서 * BlueXP Operator * 역할을 선택하고 * Next * 를 선택합니다.

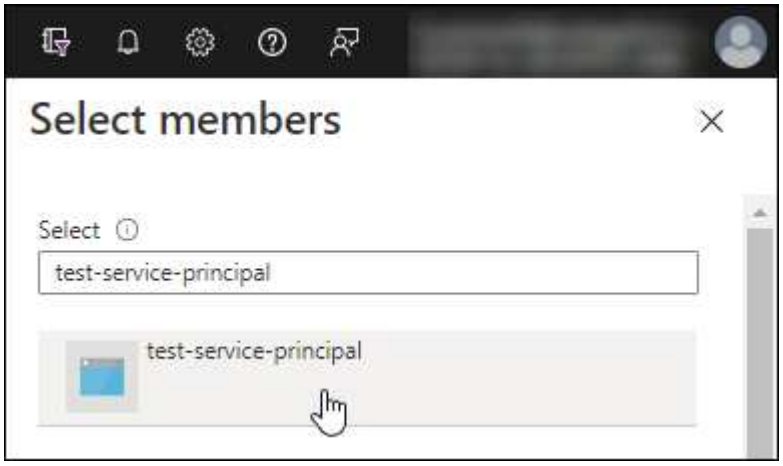
   e. Members* 탭에서 다음 단계를 완료합니다.

      - 사용자, 그룹 또는 서비스 보안 주체 * 를 선택한 상태로 유지합니다.
      - 구성원 선택 * 을 선택합니다.



- 응용 프로그램의 이름을 검색합니다.

  예를 들면 다음과 같습니다.



- 응용 프로그램을 선택하고 * 선택 * 을 선택합니다.
- 다음 * 을 선택합니다.

f. 검토 + 할당 * 을 선택합니다.

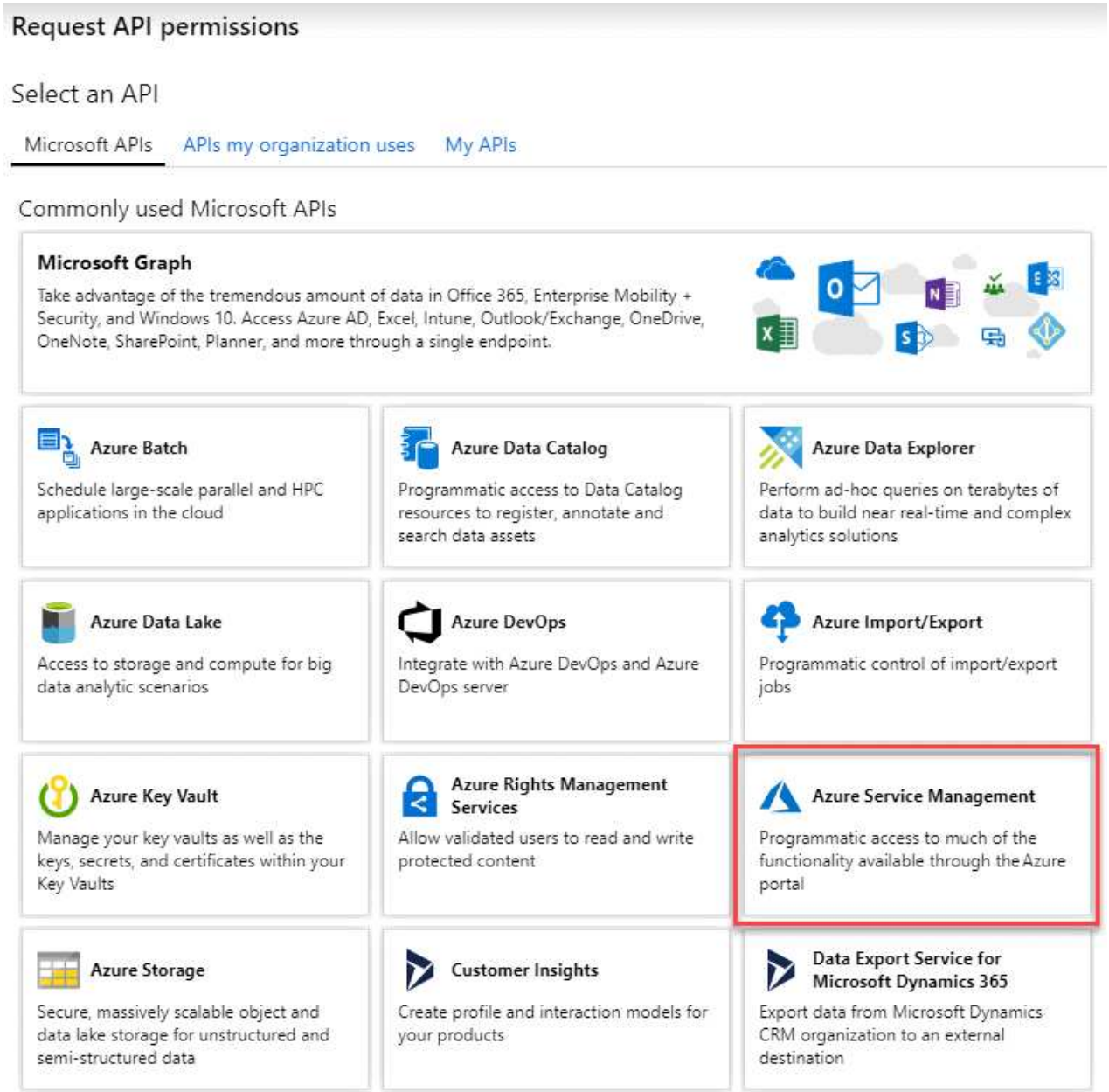
이제 서비스 보안 주체에 Connector를 배포하는 데 필요한 Azure 권한이 있습니다.

여러 Azure 구독에서 Cloud Volumes ONTAP를 배포하려면 서비스 보안 주체를 해당 구독 각각에 바인딩해야 합니다. BlueXP를 사용하면 Cloud Volumes ONTAP를 배포할 때 사용할 구독을 선택할 수 있습니다.

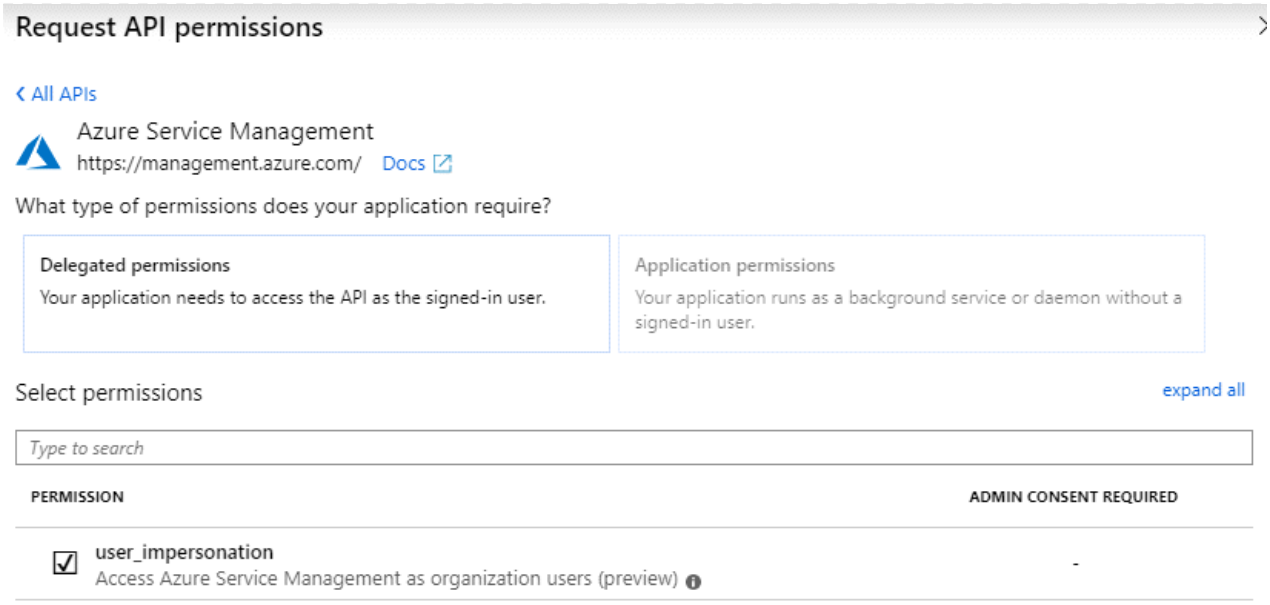
Windows Azure 서비스 관리 **API** 권한을 추가합니다

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.

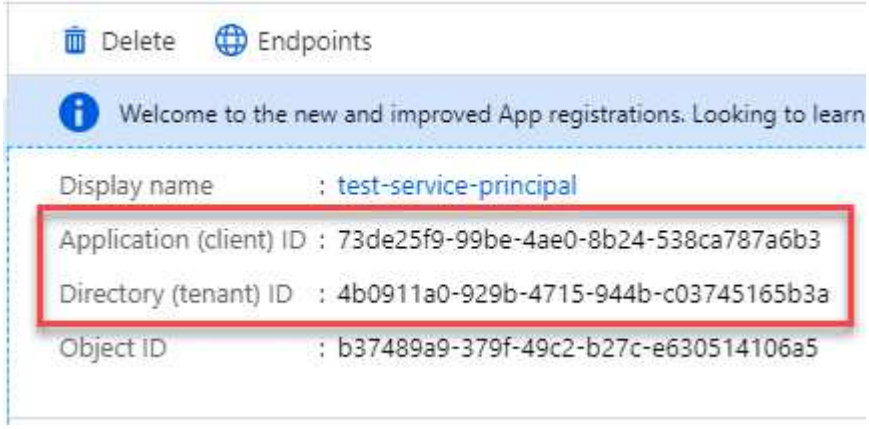


4. Access Azure Service Management as organization users * 를 선택한 다음 * Add permissions * 를 선택합니다.



응용 프로그램의 응용 프로그램 **ID** 및 디렉터리 **ID**를 가져옵니다

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



Azure 계정을 BlueXP에 추가하는 경우 응용 프로그램의 응용 프로그램(클라이언트) ID와 디렉터리(테넌트) ID를 제공해야 합니다. BlueXP는 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 암호를 생성합니다

1. Microsoft Entra ID * 서비스를 엽니다.
2. 앱 등록 * 을 선택하고 응용 프로그램을 선택합니다.
3. 인증서 및 비밀 > 새 클라이언트 비밀 * 을 선택합니다.
4. 비밀과 기간에 대한 설명을 제공하십시오.
5. 추가 * 를 선택합니다.
6. 클라이언트 암호 값을 복사합니다.

이제 BlueXP에서 Microsoft Entra ID를 사용하여 인증하는 클라이언트 암호가 있습니다.

결과

이제 서비스 보안 주체가 설정되었으므로 응용 프로그램(클라이언트) ID, 디렉터리(테넌트) ID 및 클라이언트 암호 값을 복사해야 합니다. Azure 계정을 추가할 때 BlueXP에 이 정보를 입력해야 합니다.

Google Cloud 서비스 계정

역할을 생성하여 Connector VM 인스턴스에 사용할 서비스 계정에 적용합니다.

단계

1. Google Cloud에서 사용자 지정 역할 생성:

   a. 에 정의된 권한이 포함된 YAML 파일을 생성합니다 "Google Cloud용 커넥터 정책".

   b. Google Cloud에서 클라우드 쉘을 활성화합니다.

   c. Connector에 필요한 권한이 포함된 YAML 파일을 업로드합니다.

   d. 을 사용하여 사용자 지정 역할을 만듭니다 `gcloud iam roles create` 명령.

      다음 예제에서는 프로젝트 수준에서 "connector"라는 역할을 만듭니다.

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

   +
   "Google Cloud docs: 사용자 지정 역할 생성 및 관리"

2. Google Cloud에서 서비스 계정 생성:

   a. IAM 및 관리 서비스에서 * 서비스 계정 > 서비스 계정 생성 * 을 선택합니다.

   b. 서비스 계정 세부 정보를 입력하고 * 생성 및 계속 * 을 선택합니다.

   c. 방금 만든 역할을 선택합니다.

   d. 나머지 단계를 완료해서 역할을 만듭니다.

      "Google Cloud docs: 서비스 계정 생성"

결과

이제 Connector VM 인스턴스에 할당할 수 있는 서비스 계정이 있습니다.

6단계**: Google Cloud API**를 활성화합니다

Google Cloud에 Cloud Volumes ONTAP을 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
    - 클라우드 키 관리 서비스(KMS) API

      (고객이 관리하는 암호화 키(CMEK)로 BlueXP 백업 및 복구를 사용하려는 경우에만 필요)

커넥터를 제한 모드로 전개합니다

BlueXP SaaS 계층에 대한 아웃바운드 연결이 제한된 BlueXP를 사용할 수 있도록 제한된 모드로 커넥터를 배포합니다. 시작하려면 Connector를 설치하고 Connector에서 실행 중인 사용자 인터페이스에 액세스하여 BlueXP를 설정한 다음 이전에 설정한 클라우드 권한을 제공합니다.

1단계**:** 커넥터를 설치합니다

클라우드 공급자의 마켓플레이스에서 Connector를 설치하거나 자체 Linux 호스트에 소프트웨어를 수동으로 설치합니다.

AWS 상용 마켓플레이스

시작하기 전에

다음과 같은 항목이 있어야 합니다.

- 네트워킹 요구사항을 충족하는 VPC 및 서브넷

  "네트워킹 요구 사항에 대해 알아보십시오"

- Connector에 필요한 권한을 포함하는 정책이 첨부된 IAM 역할

  "AWS 권한을 설정하는 방법에 대해 알아보십시오"

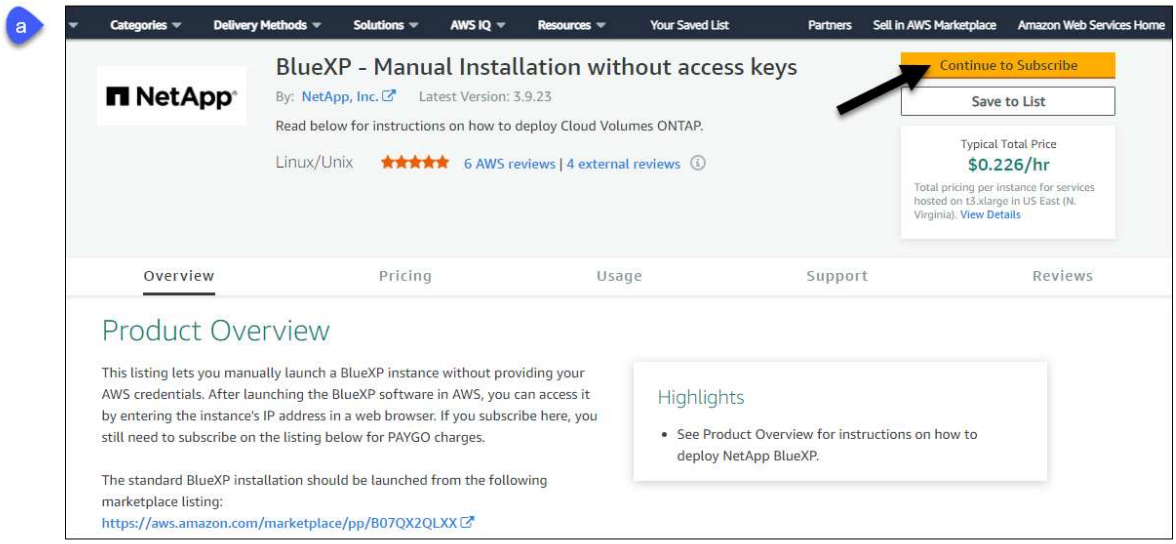
- IAM 사용자에 대한 AWS 마켓플레이스의 구독 및 구독 취소 권한
- 인스턴스의 CPU 및 RAM 요구 사항 이해

  "인스턴스 요구 사항 검토".

- EC2 인스턴스의 키 쌍입니다.

단계

1. 로 이동합니다 "AWS 마켓플레이스의 BlueXP 페이지"
2. Marketplace 페이지에서 * Continue to Subscribe * 를 선택한 다음 * Continue to Configuration * 을 선택합니다.



3. 기본 옵션을 변경하고 * Continue to Launch * 를 선택합니다.
4. 작업 선택 * 에서 * EC2 * 를 통해 시작 * 을 선택한 다음 * 시작 * 을 선택합니다.

   다음 단계에서는 콘솔에서 IAM 역할을 Connector 인스턴스에 연결할 수 있으므로 EC2 콘솔에서 인스턴스를 실행하는 방법을 설명합니다. 웹 사이트에서 시작 * 작업을 사용하면 이 작업을 수행할 수 없습니다.

5. 프롬프트에 따라 인스턴스를 구성하고 배포합니다.
   - * 이름 및 태그 *: 인스턴스의 이름과 태그를 입력합니다.
   - * 응용 프로그램 및 OS 이미지 *: 이 섹션을 건너뜁니다. 커넥터 AMI가 이미 선택되어 있습니다.
   - * 인스턴스 유형 *: 지역 가용성에 따라 RAM 및 CPU 요구 사항을 충족하는 인스턴스 유형을 선택합니다(T3.xLarge가 권장됨).
   - * 키 쌍(로그인) *: 인스턴스에 안전하게 연결하는 데 사용할 키 쌍을 선택합니다.
   - * 네트워크 설정 *: 필요에 따라 네트워크 설정을 편집합니다.
     - 원하는 VPC 및 서브넷을 선택합니다.
     - 인스턴스에 공용 IP 주소가 있어야 하는지 여부를 지정합니다.
     - Connector 인스턴스에 필요한 연결 방법(SSH, HTTP 및 HTTPS)을 활성화하는 방화벽 설정을 지정합니다.

       특정 구성에는 몇 가지 규칙이 더 필요합니다.

"AWS의 보안 그룹 규칙을 봅니다".

- * 스토리지 구성 *: 루트 볼륨의 기본 크기와 디스크 유형을 유지합니다.

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

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

결과

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

다음 단계

BlueXP를 설정합니다.

AWS 정부 마켓플레이스

시작하기 전에

다음과 같은 항목이 있어야 합니다.

- 네트워킹 요구사항을 충족하는 VPC 및 서브넷

  "네트워킹 요구 사항에 대해 알아보십시오"

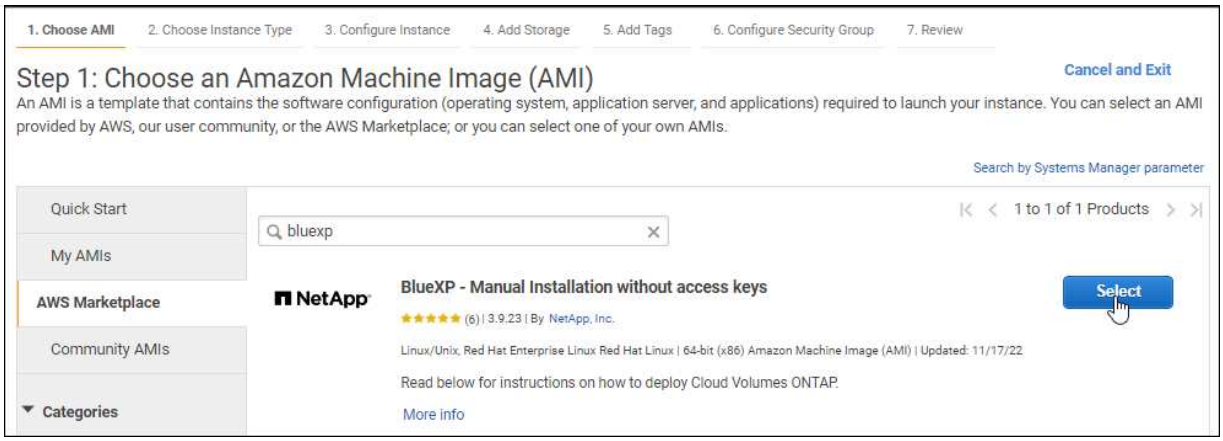
- Connector에 필요한 권한을 포함하는 정책이 첨부된 IAM 역할

  "AWS 권한을 설정하는 방법에 대해 알아보십시오"

- IAM 사용자에 대한 AWS 마켓플레이스의 구독 및 구독 취소 권한
- EC2 인스턴스의 키 쌍입니다.

단계

1. AWS Marketplace에서 BlueXP 오퍼링으로 이동합니다.
   a. EC2 서비스를 열고 * Launch instance * 를 선택합니다.
   b. AWS Marketplace * 를 선택합니다.
   c. BlueXP를 검색하고 서비스를 선택합니다.

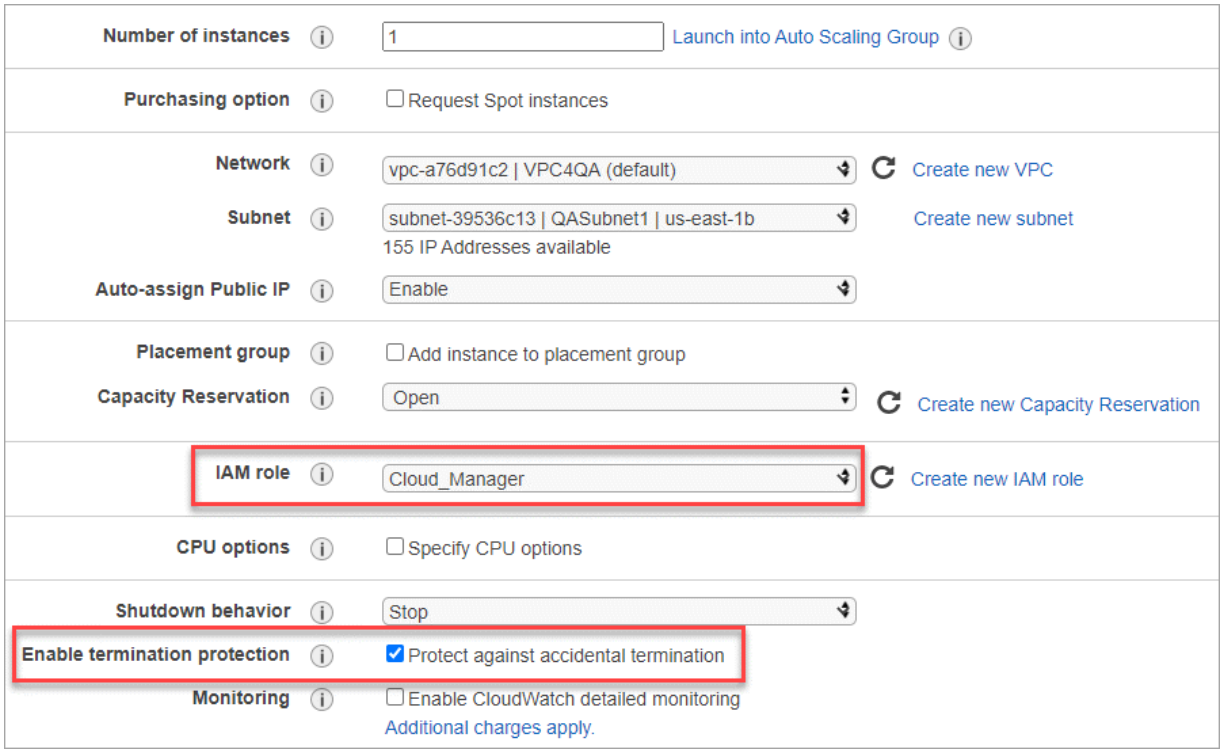


d. Continue * 를 선택합니다.

2. 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 세부 정보 구성 *: VPC 및 서브넷을 선택하고, 1단계에서 만든 IAM 역할을 선택하고, 종료 보호(권장)를 활성화하고, 요구 사항을 충족하는 다른 구성 옵션을 선택합니다.



   - * 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 선택합니다.

결과

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

다음 단계

BlueXP를 설정합니다.

Azure 마켓플레이스 를 참조하십시오

시작하기 전에

다음과 같은 항목이 있어야 합니다.

- 네트워크 요구 사항을 충족하는 VNET 및 서브넷

  "네트워킹 요구 사항에 대해 알아보십시오"

- Connector에 필요한 권한이 포함된 Azure 사용자 지정 역할입니다.

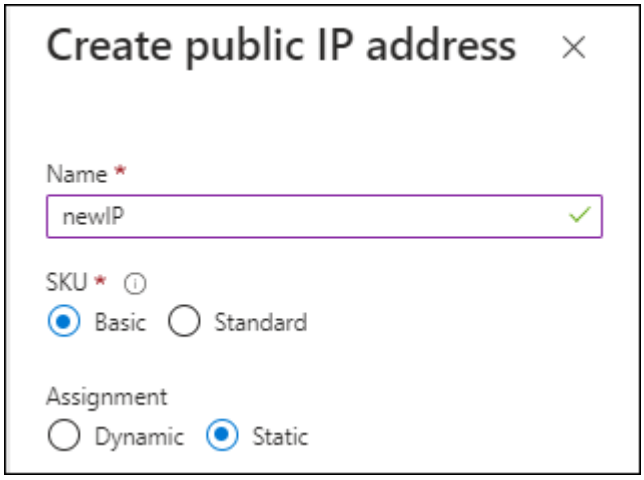
  "Azure 사용 권한을 설정하는 방법에 대해 알아봅니다"

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 선택한 다음 * 계속 * 을 선택합니다.
3. Azure 포털에서 * Create * 를 선택하고 다음 단계에 따라 가상 머신을 구성합니다.

   VM을 구성할 때 다음 사항에 유의하십시오.

   - * VM 크기 *: CPU 및 RAM 요구 사항에 맞는 VM 크기를 선택합니다. DS3 v2를 권장합니다.
   - * 디스크 *: 커넥터는 HDD 또는 SSD 디스크를 사용하여 최적의 성능을 발휘할 수 있습니다.
   - * 공용 IP *: 커넥터 VM에서 공용 IP 주소를 사용하려면 IP 주소가 기본 SKU를 사용하여 BlueXP가 이 공용 IP 주소를 사용하도록 해야 합니다.



대신 표준 SKU IP 주소를 사용하는 경우 BlueXP는 공용 IP 대신 Connector의 _private_ip 주소를 사용합니다. BlueXP 콘솔에 액세스하는 데 사용하는 시스템에서 해당 개인 IP 주소에 액세스할 수 없는 경우 BlueXP 콘솔의 작업이 실패합니다.

"Azure 설명서: 공용 IP SKU"

- * 네트워크 보안 그룹 *: Connector는 SSH, HTTP 및 HTTPS를 사용하는 인바운드 연결을 필요로 합니다.

  "Azure의 보안 그룹 규칙을 봅니다".

- * ID *: * Management * 에서 * 시스템에서 할당한 관리 ID 활성화 * 를 선택합니다.

  이 설정은 관리되는 ID를 통해 Connector 가상 컴퓨터가 자격 증명을 제공하지 않고 Microsoft Entra ID를 식별할 수 있기 때문에 중요합니다. "Azure 리소스의 관리 ID에 대해 자세히 알아보십시오".

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

결과

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

다음 단계

BlueXP를 설정합니다.

수동 설치

시작하기 전에

다음과 같은 항목이 있어야 합니다.

- 커넥터를 설치할 수 있는 루트 권한
- Connector의 인터넷 액세스에 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

  설치 후 프록시 서버를 구성할 수 있지만 이렇게 하려면 커넥터를 다시 시작해야 합니다.

  BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

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

이 작업에 대해

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

단계

1. Docker가 설정 및 실행 중인지 확인합니다.

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

2. _http_proxy_or_https_proxy_system 변수가 호스트에 설정되어 있으면 이를 제거합니다.

```
unset http_proxy
unset https_proxy
```

이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

3. 에서 Connector 소프트웨어를 다운로드합니다 "NetApp Support 사이트"를 선택한 다음 Linux 호스트에 복사합니다.

   네트워크 또는 클라우드에서 사용하도록 고안된 "온라인" 커넥터 설치 프로그램을 다운로드해야 합니다. Connector에 대해 별도의 "오프라인" 설치 프로그램을 사용할 수 있지만 전용 모드 배포에서만 지원됩니다.

4. 스크립트를 실행할 권한을 할당합니다.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

   여기서 <version>는 다운로드한 커넥터 버전입니다.

5. 설치 스크립트를 실행합니다.

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

   proxy 및 — cacert 매개 변수는 선택 사항입니다. 프록시 서버가 있는 경우 그림과 같이 매개 변수를 입력해야 합니다. 설치 프로그램에서 프록시에 대한 정보를 제공하라는 메시지를 표시하지 않습니다.

   다음은 두 가지 선택적 매개 변수를 사용하는 명령의 예입니다.

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

   — 프록시는 다음 형식 중 하나를 사용하여 커넥터가 HTTP 또는 HTTPS 프록시 서버를 사용하도록 구성합니다.

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     다음 사항에 유의하십시오.

- 사용자는 로컬 사용자 또는 도메인 사용자일 수 있습니다.
- 도메인 사용자의 경우 위에 표시된 \ 에 ASCII 코드를 사용해야 합니다.
- BlueXP는 @ 문자를 포함하는 암호를 지원하지 않습니다.

cacert는 Connector와 프록시 서버 간의 HTTPS 액세스에 사용할 CA 서명 인증서를 지정합니다. 이 매개변수는 HTTPS 프록시 서버를 지정하거나 프록시가 가로채기 프록시인 경우에만 필요합니다.

결과

이제 커넥터가 설치되었습니다. 프록시 서버를 지정한 경우 설치가 끝나면 커넥터 서비스(occm)가 두 번 다시 시작됩니다.

다음 단계

BlueXP를 설정합니다.

2단계**: BlueXP** 설정

BlueXP 콘솔에 처음 액세스할 때 Connector를 연결할 계정을 선택하라는 메시지가 표시되면 제한된 모드를 활성화해야 합니다.

> 이미 계정이 있고 다른 계정을 만들려면 Tenancy API를 사용해야 합니다. "추가 BlueXP 계정을 만드는 방법에 대해 알아봅니다".

단계

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

   https://ipaddress

2. BlueXP에 가입하거나 로그인합니다.
3. 로그인한 후 BlueXP를 설정합니다.

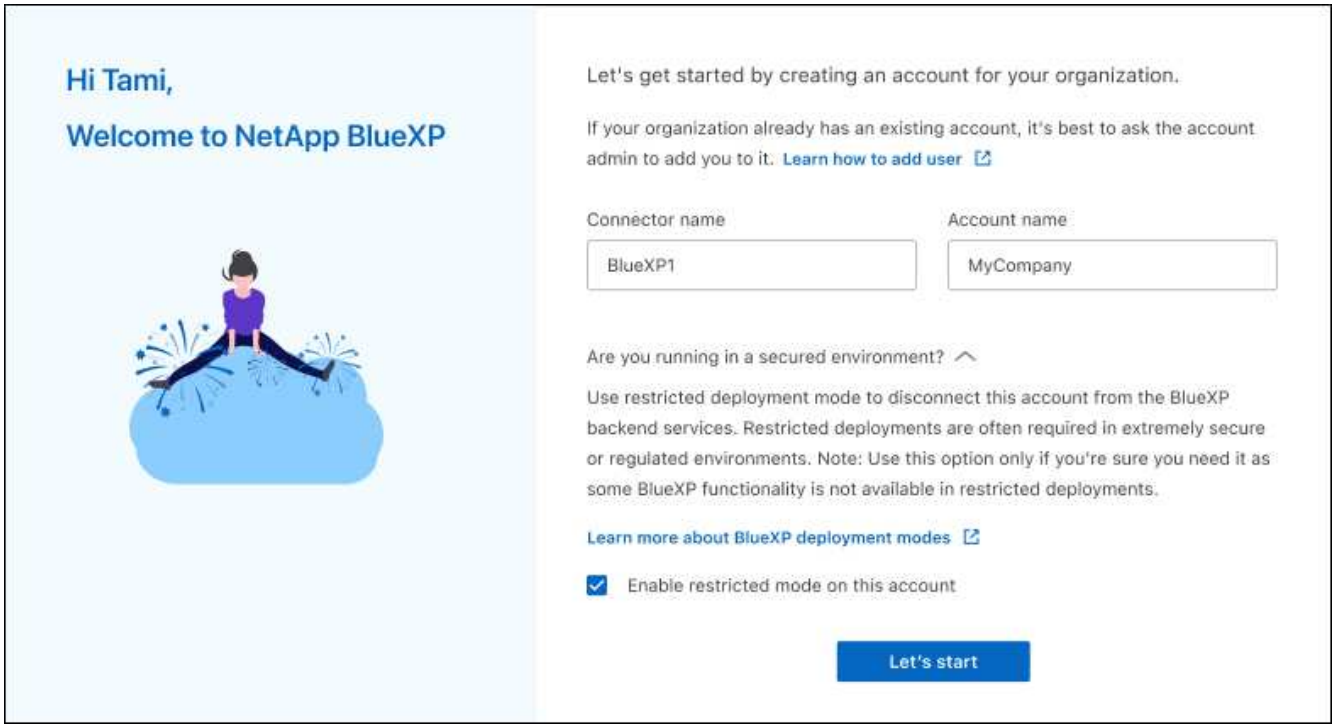
   a. 커넥터 이름을 입력합니다.
   b. 새 BlueXP 계정의 이름을 입력하거나 기존 계정을 선택합니다.

      로그인이 이미 BlueXP 계정과 연결되어 있는 경우 기존 계정을 선택할 수 있습니다.

   c. 보안 환경에서 실행 중입니까? * 를 선택합니다
   d. 이 계정에서 제한 모드 사용 * 을 선택합니다.

      BlueXP에서 계정을 만든 후에는 이 설정을 변경할 수 없습니다. 나중에 제한 모드를 활성화할 수 없으며 나중에 비활성화할 수 없습니다.

      정부 지역에 Connector를 구축한 경우 이 확인란은 이미 활성화되어 있으므로 변경할 수 없습니다. 이는 제한 모드가 정부 지역에서 지원되는 유일한 모드이기 때문입니다.



a. Let's start * 를 선택합니다.

결과

이제 커넥터가 설치되어 BlueXP 계정으로 설정됩니다. 모든 사용자는 Connector 인스턴스의 IP 주소를 사용하여 BlueXP에 액세스해야 합니다.

다음 단계

이전에 설정한 권한을 BlueXP에 제공합니다.

3단계**: BlueXP**에 권한 제공

Azure Marketplace에서 Connector를 배포했거나 Connector 소프트웨어를 수동으로 설치한 경우 BlueXP 서비스를 사용할 수 있도록 이전에 설정한 사용 권한을 제공해야 합니다.

구축 중에 필요한 IAM 역할을 선택했기 때문에 AWS Marketplace에서 Connector를 구축한 경우에는 이 단계가 적용되지 않습니다.

"클라우드 사용 권한을 준비하는 방법에 대해 알아봅니다".

AWS IAM 역할

이전에 만든 IAM 역할을 Connector를 설치한 EC2 인스턴스에 연결합니다.

다음 단계는 AWS에서 커넥터를 수동으로 설치한 경우에만 적용됩니다. AWS Marketplace 배포의 경우 필요한 권한이 포함된 IAM 역할과 Connector 인스턴스를 이미 연결한 것입니다.

단계

1. Amazon EC2 콘솔로 이동합니다.
2. 인스턴스 * 를 선택합니다.
3. 커넥터 인스턴스를 선택합니다.
4. Actions > Security > Modify IAM role * 을 선택합니다.
5. IAM 역할을 선택하고 * Update IAM role * 을 선택합니다.

결과

BlueXP는 이제 AWS에서 사용자 대신 작업을 수행하는 데 필요한 권한을 가집니다.

AWS 액세스 키입니다

필요한 권한이 있는 IAM 사용자를 위해 BlueXP에 AWS 액세스 키를 제공합니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

2. 자격 증명 추가 * 를 선택하고 마법사의 단계를 따릅니다.
   a. * 자격 증명 위치 *: * Amazon Web Services > Connector * 를 선택합니다.
   b. * 자격 증명 정의 *: AWS 액세스 키와 비밀 키를 입력합니다.
   c. * Marketplace 구독 *: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 선택합니다.

결과

BlueXP는 이제 AWS에서 사용자 대신 작업을 수행하는 데 필요한 권한을 가집니다.

Azure 역할

Azure 포털로 이동하여 하나 이상의 구독에 대해 Connector 가상 머신에 Azure 사용자 지정 역할을 할당합니다.

단계

1. Azure Portal에서 * Subscriptions * 서비스를 열고 구독을 선택합니다.

   구독 수준에서의 역할 할당 범위를 지정하므로 * 구독 * 서비스에서 역할을 할당하는 것이 중요합니다. scope _ 는 액세스가 적용되는 리소스 집합을 정의합니다. 범위를 다른 수준(예: 가상 머신 레벨)으로 지정하면

BlueXP 내에서 작업을 완료하는 데 영향을 줍니다.

"Microsoft Azure 설명서: Azure RBAC의 범위를 이해합니다"

2. IAM(액세스 제어) * > * 추가 * > * 역할 할당 추가 * 를 선택합니다.
3. Role * 탭에서 * BlueXP Operator * 역할을 선택하고 * Next * 를 선택합니다.

> BlueXP 오퍼레이터는 BlueXP 정책에 제공된 기본 이름입니다. 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

4. Members* 탭에서 다음 단계를 완료합니다.
   a. 관리되는 ID*에 대한 액세스를 할당합니다.
   b. 구성원 선택 * 을 선택하고 커넥터 가상 시스템이 생성된 구독을 선택한 다음 * 관리 ID * 에서 * 가상 머신 * 을 선택한 다음 커넥터 가상 머신을 선택합니다.
   c. 선택 * 을 선택합니다.
   d. 다음 * 을 선택합니다.
   e. 검토 + 할당 * 을 선택합니다.
   f. 추가 Azure 구독에서 리소스를 관리하려면 해당 구독으로 전환한 다음 이 단계를 반복합니다.

결과

이제 BlueXP는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 가지고 있습니다.

Azure 서비스 보안 주체

이전에 설정한 Azure 서비스 보안 주체에 대한 자격 증명을 BlueXP에 제공합니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

2. 자격 증명 추가 * 를 선택하고 마법사의 단계를 따릅니다.
   a. * 자격 증명 위치 *: * Microsoft Azure > 커넥터 * 를 선택합니다.
   b. * 자격 증명 정의 *: 필요한 권한을 부여하는 Microsoft Entra 서비스 보안 주체에 대한 정보를 입력합니다.
      - 애플리케이션(클라이언트) ID입니다
      - 디렉토리(테넌트) ID입니다
      - 클라이언트 암호
   c. * Marketplace 구독 *: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 선택합니다.

결과

이제 BlueXP는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 가지고 있습니다.

Google Cloud 서비스 계정

서비스 계정을 Connector VM에 연결합니다.

단계

1. Google Cloud 포털로 이동하여 Connector VM 인스턴스에 서비스 계정을 할당합니다.

   "Google Cloud 설명서: 인스턴스에 대한 서비스 계정 및 액세스 범위 변경"

2. 다른 프로젝트의 리소스를 관리하려면 해당 프로젝트에 BlueXP 역할의 서비스 계정을 추가하여 액세스 권한을 부여합니다. 각 프로젝트에 대해 이 단계를 반복해야 합니다.

결과

BlueXP는 이제 Google Cloud에서 대신 작업을 수행하는 데 필요한 권한을 가지고 있습니다.

BlueXP 가입(제한 모드)

클라우드 공급업체의 시장에서 BlueXP를 구독하여 시간당 요금(PAYGO)이나 연간 계약을 통해 BlueXP 서비스 비용을 지불하십시오. NetApp(BYOL)에서 라이센스를 구입한 경우에도 마켓플레이스 제품을 구독해야 합니다. 라이센스 비용이 항상 먼저 청구되지만 라이센스 용량을 초과하거나 라이센스 기간이 만료되면 시간당 요금이 부과됩니다.

마켓플레이스에 가입하면 제한된 모드로 다음 BlueXP 서비스를 충전할 수 있습니다.

- 백업 및 복구
- 분류
- Cloud Volumes ONTAP

시작하기 전에

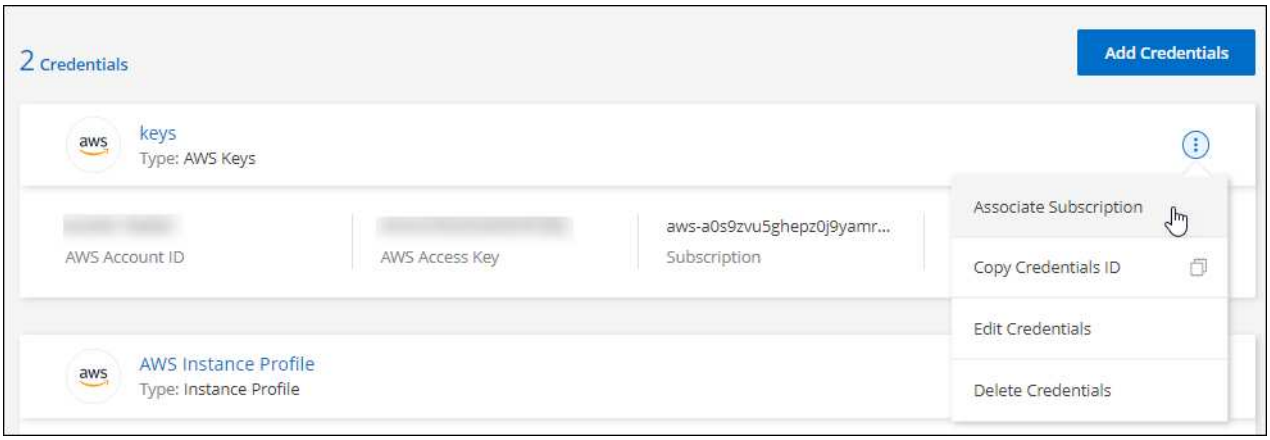
BlueXP를 구독하려면 Connector와 연결된 클라우드 자격 증명과 마켓플레이스 구독을 연결해야 합니다. "제한된 모드로 시작하기" 워크플로를 따랐다면 이미 Connector가 있는 것입니다. 자세한 내용은 를 참조하십시오 "제한된 모드에서 BlueXP를 빠르게 시작합니다".

설치하고

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 선택한 다음 * 가입 연결 * 을 선택합니다.

   Connector와 연결된 자격 증명을 선택해야 합니다. BlueXP와 연결된 자격 증명과 마켓플레이스 구독을 연결할 수 없습니다.



3. 자격 증명을 기존 구독과 연결하려면 드롭다운 목록에서 구독을 선택하고 * Associate * 를 선택합니다.
4. 자격 증명을 새 구독과 연결하려면 * 구독 추가 > 계속 * 을 선택하고 AWS 마켓플레이스의 단계를 따릅니다.

   a. 구매 옵션 보기 * 를 선택합니다.
   b. 가입 * 을 선택합니다.
   c. 계정 설정 * 을 선택합니다.

      BlueXP 웹 사이트로 이동합니다.

   d. [구독 할당 *] 페이지에서:

      - 이 구독을 연결할 BlueXP 계정을 선택합니다.
      - 기존 구독 바꾸기 * 필드에서 하나의 계정에 대한 기존 구독을 이 새 구독으로 자동 대체할지 여부를 선택합니다.

        BlueXP는 계정의 모든 자격 증명에 대한 기존 구독을 이 새 구독으로 대체합니다. 자격 증명 집합이 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

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

      - 저장 * 을 선택합니다.

        다음 비디오에서는 AWS 마켓플레이스를 구독하는 단계를 보여줍니다.

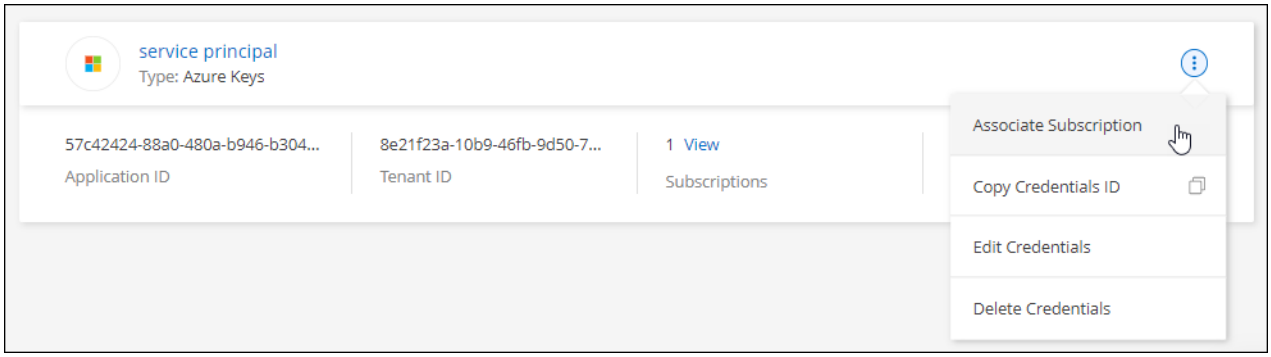
   AWS 마켓플레이스에서 BlueXP를 구독하십시오

Azure를 지원합니다

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
2. 자격 증명 집합에 대한 작업 메뉴를 선택한 다음 * 가입 연결 * 을 선택합니다.

   Connector와 연결된 자격 증명을 선택해야 합니다. BlueXP와 연결된 자격 증명과 마켓플레이스 구독을 연결할 수 없습니다.



3. 자격 증명을 기존 구독과 연결하려면 드롭다운 목록에서 구독을 선택하고 * Associate * 를 선택합니다.
4. 자격 증명을 새 구독과 연결하려면 * 구독 추가 > 계속 * 을 선택하고 Azure 마켓플레이스의 단계를 따릅니다.

   a. 메시지가 표시되면 Azure 계정에 로그인합니다.
   b. 가입 * 을 선택합니다.
   c. 양식을 작성하고 * Subscribe * 를 선택합니다.
   d. 가입 프로세스가 완료되면 * 지금 계정 구성 * 을 선택합니다.

      BlueXP 웹 사이트로 이동합니다.

   e. [구독 할당 *] 페이지에서:

      - 이 구독을 연결할 BlueXP 계정을 선택합니다.
      - 기존 구독 바꾸기 * 필드에서 하나의 계정에 대한 기존 구독을 이 새 구독으로 자동 대체할지 여부를 선택합니다.

        BlueXP는 계정의 모든 자격 증명에 대한 기존 구독을 이 새 구독으로 대체합니다. 자격 증명 집합이 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

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

      - 저장 * 을 선택합니다.

        다음 비디오에서는 Azure 마켓플레이스에서 구독하는 단계를 보여 줍니다.

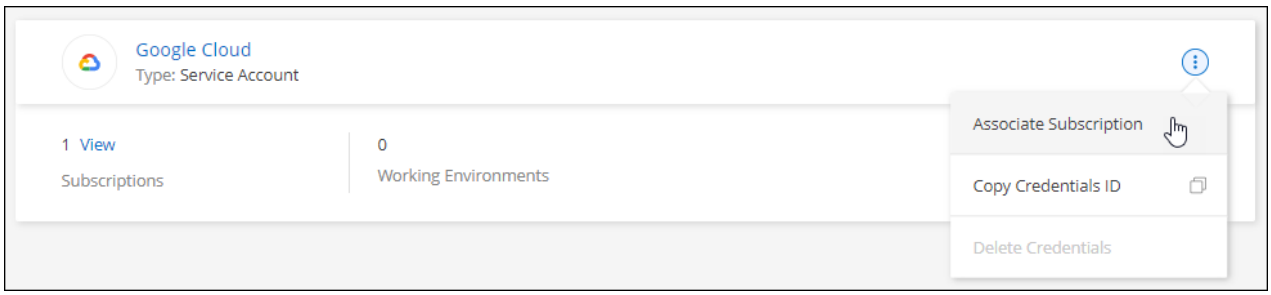
   Azure 마켓플레이스에서 BlueXP를 구독하십시오

Google 클라우드

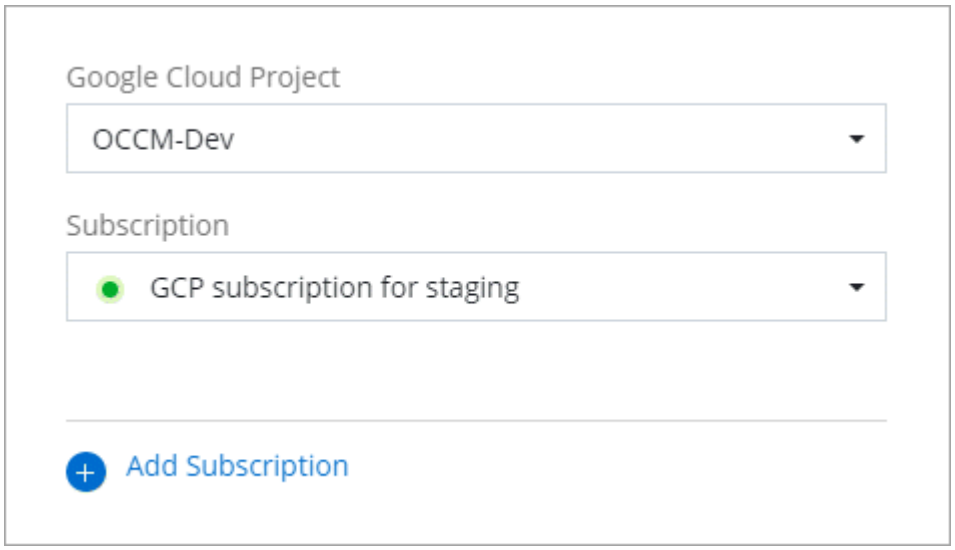
단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

2. 자격 증명 집합에 대한 작업 메뉴를 선택한 다음 * 가입 연결 * 을 선택합니다.



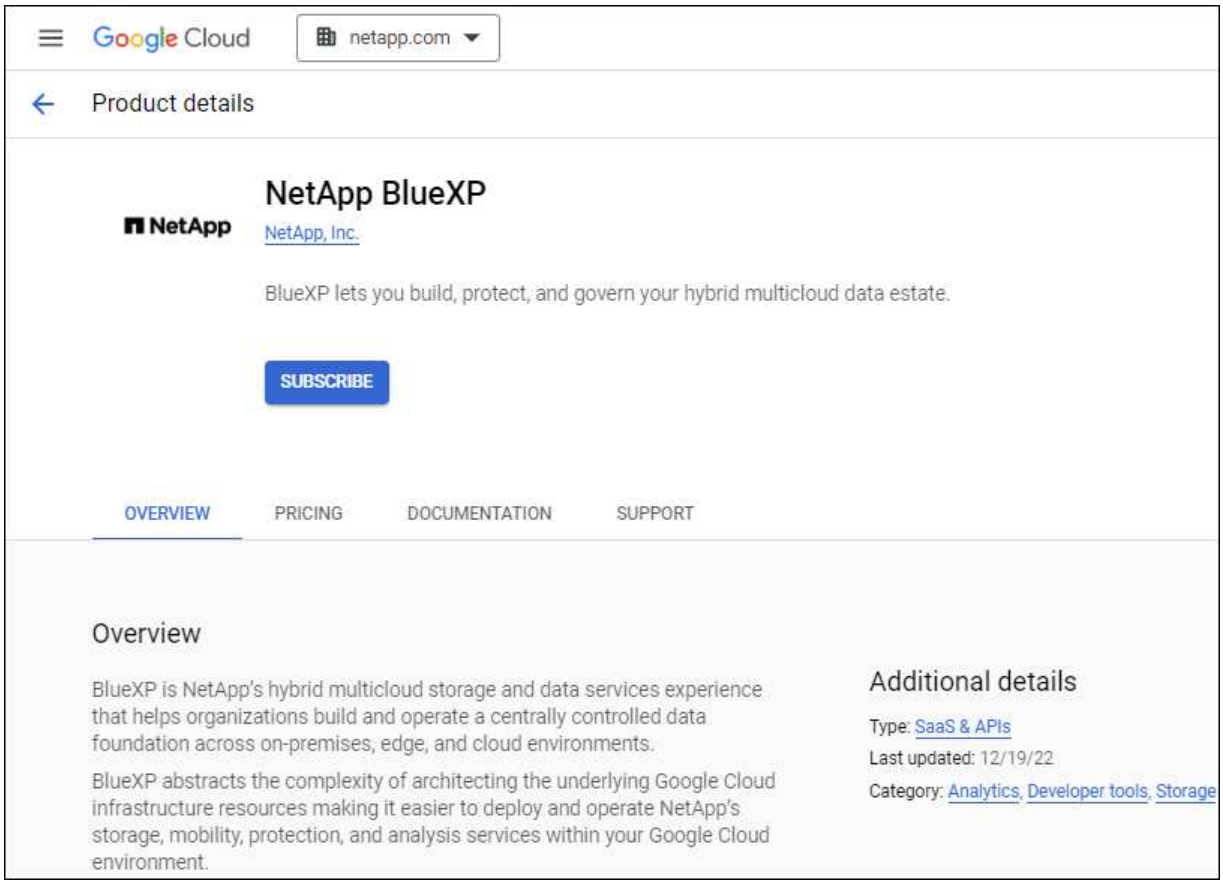
3. 자격 증명을 기존 구독과 연결하려면 아래 목록에서 Google Cloud 프로젝트 및 구독을 선택한 다음 * Associate * 를 선택합니다.



4. 아직 구독이 없는 경우 * 구독 추가 > 계속 * 을 선택하고 Google Cloud Marketplace의 단계를 따릅니다.

> 다음 단계를 완료하기 전에 Google Cloud 계정과 BlueXP 로그인에 Billing Admin 권한이 모두 있는지 확인하십시오.

a. 로 리디렉션된 후 "Google Cloud 마켓플레이스의 NetApp BlueXP 페이지"상단 탐색 메뉴에서 올바른 프로젝트가 선택되어 있는지 확인합니다.



b. 가입 * 을 선택합니다.

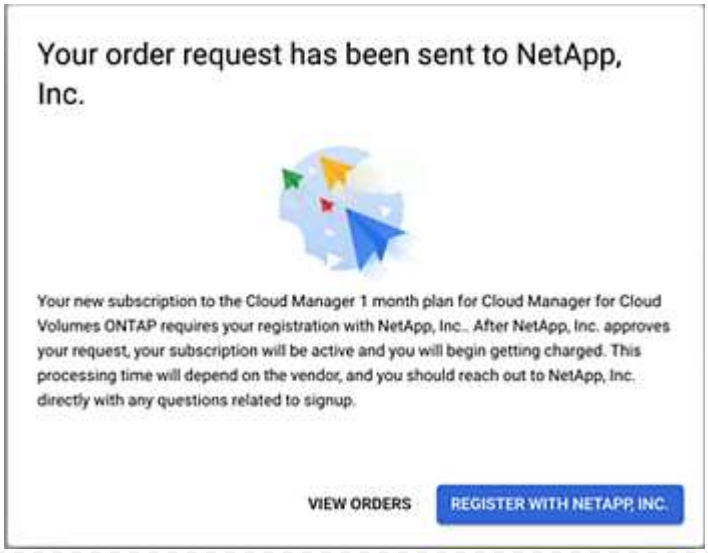
c. 적절한 청구 계정을 선택하고 이용 약관에 동의합니다.

d. 가입 * 을 선택합니다.

   이 단계에서는 전송 요청을 NetApp에 전송합니다.

e. 팝업 대화 상자에서 * Register with NetApp, Inc. * 를 선택합니다

   Google Cloud 구독을 BlueXP 계정에 연결하려면 이 단계를 완료해야 합니다. 이 페이지에서 리디렉션된 다음 BlueXP에 로그인할 때까지 가입 연결 프로세스가 완료되지 않습니다.



f. 구독 할당 * 페이지의 단계를 완료합니다.

> 조직의 누군가가 청구 계정에서 NetApp BlueXP 구독을 이미 구독한 경우 으로 리디렉션됩니다 "BlueXP 웹 사이트의 Cloud Volumes ONTAP 페이지" 대신 예기치 않은 상황인 경우 NetApp 세일즈 팀에 문의하십시오. Google은 Google 청구 계정당 하나의 가입만 활성화합니다.

- 이 구독을 연결할 BlueXP 계정을 선택합니다.
- 기존 구독 바꾸기 * 필드에서 하나의 계정에 대한 기존 구독을 이 새 구독으로 자동 대체할지 여부를 선택합니다.

  BlueXP는 계정의 모든 자격 증명에 대한 기존 구독을 이 새 구독으로 대체합니다. 자격 증명 집합이 구독과 연결되지 않은 경우 이 새 구독은 해당 자격 증명과 연결되지 않습니다.

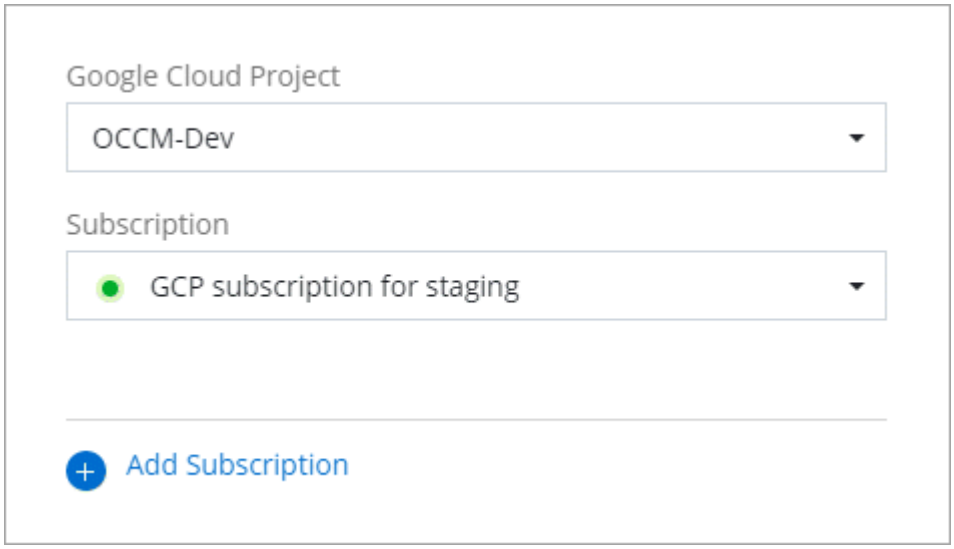
다른 모든 계정의 경우 이 단계를 반복하여 구독을 수동으로 연결해야 합니다.

- 저장 * 을 선택합니다.

  다음 비디오에서는 Google Cloud Marketplace를 구독하는 단계를 보여줍니다.

Google Cloud 마켓플레이스에서 BlueXP를 구독하십시오

a. 이 프로세스가 완료되면 BlueXP의 자격 증명 페이지로 돌아가서 이 새 구독을 선택합니다.



관련 링크

- "Cloud Volumes ONTAP용 BYOL 용량 기반 라이센스 관리"
- "BlueXP 데이터 서비스에 대한 BYOL 라이센스 관리"
- "BlueXP에 대한 AWS 자격 증명 및 구독을 관리합니다"
- "BlueXP용 Azure 자격 증명 및 구독을 관리합니다"
- "BlueXP용 Google Cloud 자격 증명 및 구독을 관리합니다"

다음에 수행할 수 있는 작업(제한된 모드)

제한된 모드에서 BlueXP를 시작하고 실행한 후 제한된 모드로 지원되는 BlueXP 서비스를 사용할 수 있습니다.

자세한 내용은 다음 서비스 설명서를 참조하십시오.

- "ONTAP용 Amazon FSx 문서"
- "Azure NetApp Files 문서"
- "백업 및 복구 문서"
- "분류 문서"
- "Cloud Volumes ONTAP 문서"
- "사내 ONTAP 클러스터 문서"
- "복제 문서"

관련 링크

"BlueXP 배포 모드"

비공개 모드로 시작하십시오

워크플로 시작(비공개 모드)

환경을 준비하고 Connector를 배포하여 BlueXP를 개인 모드로 시작하십시오.

프라이빗 모드는 일반적으로 인터넷에 연결되지 않고 을 포함하는 보안 클라우드 지역에서 사용되는 온프레미스 환경에서 사용됩니다 "AWS 비밀 클라우드", "AWS Top Secret Cloud의 약어입니다", 및 "Azure iL6"

시작하기 전에 에 대한 이해가 있어야 합니다 "BlueXP 계정", "커넥터", 및 "배포 모드".

1 "배포를 준비합니다"

1. CPU, RAM, 디스크 공간, Docker Engine 등에 대한 요구사항을 충족하는 전용 Linux 호스트를 준비합니다.
2. 대상 네트워크에 대한 액세스를 제공하는 네트워킹을 설정합니다.
3. 클라우드 배포의 경우 소프트웨어를 설치한 후 해당 권한을 Connector에 연결할 수 있도록 클라우드 공급자에 권한을 설정합니다.

2 "커넥터를 배포합니다"

1. 자신의 Linux 호스트에 Connector 소프트웨어를 설치합니다.
2. 웹 브라우저를 열고 Linux 호스트의 IP 주소를 입력하여 BlueXP를 설정합니다.
3. 클라우드 배포의 경우 이전에 설정한 권한을 BlueXP에 제공합니다.

프라이빗 모드로 구축을 준비합니다

BlueXP를 개인 모드로 배포하기 전에 환경을 준비합니다. 예를 들어 호스트 요구 사항을 검토하고, 네트워킹을 준비하고, 사용 권한을 설정하는 등의 작업을 수행해야 합니다.

> 에서 BlueXP를 사용하려는 경우 "AWS 비밀 클라우드" 또는 을 누릅니다 "AWS Top Secret Cloud의 약어입니다"그런 다음 별도의 지침에 따라 해당 환경에서 시작해야 합니다. "AWS Secret Cloud 또는 Top Secret Cloud에서 Cloud Volumes ONTAP을 시작하는 방법을 알아보십시오"

1단계**:** 비공개 모드의 작동 방식을 이해합니다

시작하기 전에 BlueXP가 개인 모드에서 작동하는 방식을 이해해야 합니다.

예를 들어, 설치할 BlueXP Connector에서 로컬로 사용할 수 있는 브라우저 기반 인터페이스를 사용해야 합니다. SaaS 계층을 통해 제공되는 웹 기반 콘솔에서 BlueXP에 액세스할 수 없습니다.

또한 모든 BlueXP 서비스를 사용할 수 있는 것은 아닙니다.

"비공개 모드의 작동 방식에 대해 알아보십시오".

단계 **2:** 설치 옵션을 검토합니다

비공개 모드에서 Connector를 자체 Linux 호스트에 수동으로 설치하여 온프레미스 또는 클라우드에 설치할 수 있습니다.

Google Cloud에서 Cloud Volumes ONTAP 시스템을 만들려면 Connector가 Google Cloud에서 실행 중이어야 합니다. 이는 사내에서 실행할 수 없습니다.

3단계**:** 호스트 요구 사항을 검토합니다

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

전용 호스트

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

지원되는 운영 체제

- 우분투 22.04 LTS
- CentOS 7.6, 7.7, 7.8 및 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 및 7.9

  호스트는 Red Hat Subscription Management에 등록되어 있어야 합니다. 등록되지 않은 경우 호스트는 Connector 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.

  Connector는 이러한 운영 체제의 영어 버전에서 지원됩니다.

하이퍼바이저

Ubuntu, CentOS 또는 Red Hat Enterprise Linux 실행 인증을 받은 베어 메탈 또는 호스팅된 하이퍼바이저가 필요합니다.

"Red Hat 솔루션: Red Hat Enterprise Linux 실행 인증을 받은 하이퍼바이저는 무엇입니까?"

CPU

코어 4개 또는 vCPU 4개

RAM

14GB

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.

Google Cloud 컴퓨터 유형입니다

위의 CPU 및 RAM 요구 사항을 충족하는 인스턴스 유형입니다. n2-standard-4를 추천합니다.

Connector는 를 지원하는 OS가 있는 VM 인스턴스의 Google Cloud에서 지원됩니다 "차폐된 VM 기능"

/opt의 디스크 공간입니다

100GiB의 공간을 사용할 수 있어야 합니다

/var의 디스크 공간입니다

20GiB의 공간을 사용할 수 있어야 합니다

Docker 엔진

Connector를 설치하기 전에 Docker 엔진이 호스트에 필요합니다.

- 지원되는 최소 버전은 19.3.1입니다.
- 지원되는 최대 버전은 25.0.5입니다.

"설치 지침을 봅니다"

4단계**:** 커넥터의 네트워킹을 준비합니다

Connector가 공용 클라우드 환경 내에서 리소스 및 프로세스를 관리할 수 있도록 네트워킹을 설정합니다. Connector에 대한 가상 네트워크 및 서브넷을 사용하는 것 외에 다음 요구 사항이 충족되는지 확인해야 합니다.

대상 네트워크에 대한 연결

Connector는 저장소를 관리하려는 위치에 대한 네트워크 연결이 있어야 합니다. 예를 들어, Cloud Volumes ONTAP를 구축할 계획인 VPC 또는 VNET, 온프레미스 ONTAP 클러스터가 상주하는 데이터 센터 등이 있습니다.

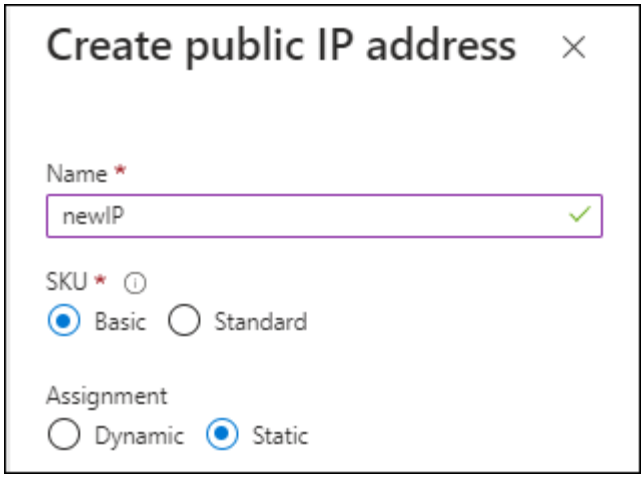
일상적 작업의 엔드포인트

Connector는 다음 엔드포인트를 접촉하여 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리합니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • CloudFormation 을 참조하십시오 • EC2(탄력적인 컴퓨팅 클라우드) • IAM(Identity and Access Management) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • S3(Simple Storage Service)	를 사용하여 AWS에서 리소스를 관리합니다. 정확한 끝점은 사용 중인 AWS 지역에 따라 다릅니다. "자세한 내용은 AWS 설명서를 참조하십시오"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure 공공 지역의 리소스를 관리합니다.
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Azure IL6 영역의 리소스를 관리합니다.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure 중국 지역의 리소스를 관리합니다.
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://www.googleapis.com/deploymentmanager/v2/projects	Google Cloud에서 리소스를 관리합니다.

Azure의 공용 **IP** 주소입니다

Azure의 커넥터 VM에서 공용 IP 주소를 사용하려면 IP 주소가 기본 SKU를 사용하여 BlueXP가 이 공용 IP 주소를 사용하도록 해야 합니다.



대신 표준 SKU IP 주소를 사용하는 경우 BlueXP는 공용 IP 대신 Connector의 _private_ip 주소를 사용합니다. BlueXP 콘솔에 액세스하는 데 사용하는 시스템에서 해당 개인 IP 주소에 액세스할 수 없는 경우 BlueXP 콘솔의 작업이 실패합니다.

"Azure 설명서: 공용 IP SKU"

프록시 서버

조직에서 모든 나가는 인터넷 트래픽에 대해 프록시 서버를 배포해야 하는 경우 HTTP 또는 HTTPS 프록시에 대한 다음 정보를 가져옵니다. 설치하는 동안 이 정보를 제공해야 합니다.

- IP 주소입니다
- 자격 증명
- HTTPS 인증서

BlueXP는 투명한 프록시 서버를 지원하지 않습니다.

를 누릅니다
비공개 모드에서 BlueXP가 아웃바운드 트래픽을 전송하는 유일한 시간은 클라우드 공급자에게 Cloud Volumes ONTAP 시스템을 생성하는 것입니다.

포트

커넥터 를 시작하지 않으면 커넥터로 들어오는 트래픽이 없습니다.

HTTP(80) 및 HTTPS(443)는 BlueXP 콘솔에 대한 액세스를 제공합니다. SSH(22)는 문제 해결을 위해 호스트에 연결해야 하는 경우에만 필요합니다.

NTP를 활성화합니다

BlueXP 분류를 사용하여 회사 데이터 소스를 검사하려는 경우 BlueXP Connector 시스템과 BlueXP 분류 시스템 모두에서 NTP(Network Time Protocol) 서비스를 활성화하여 시스템 간에 시간이 동기화되도록 해야 합니다. "BlueXP 분류에 대해 자세히 알아보십시오"

5단계**:** 클라우드 권한 준비

Cloud Volumes ONTAP 시스템을 생성할 계획이라면 BlueXP에 클라우드 공급업체의 권한이 필요합니다. 클라우드 공급자에서 사용 권한을 설정한 다음 설치한 후 해당 권한을 Connector 인스턴스에 연결해야 합니다.

필요한 단계를 보려면 클라우드 공급자에 사용할 인증 옵션을 선택합니다.

온-프레미스에 Connector를 설치하려면 AWS 액세스 키 또는 Azure 서비스 보안 주체를 사용하여 권한을 제공해야 합니다. 다른 옵션은 지원되지 않습니다.

AWS IAM 역할

IAM 역할을 사용하여 Connector에 권한을 제공합니다. Connector의 EC2 인스턴스에 역할을 수동으로 연결해야 합니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책 생성:
   a. 정책 > 정책 생성 * 을 선택합니다.
   b. JSON * 을 선택하고 의 내용을 복사하여 붙여 넣습니다 "Connector에 대한 IAM 정책".
   c. 나머지 단계를 완료하고 정책을 생성합니다.
3. IAM 역할 생성:
   a. 역할 > 역할 생성 * 을 선택합니다.
   b. AWS 서비스 > EC2 * 를 선택합니다.
   c. 방금 만든 정책을 첨부하여 사용 권한을 추가합니다.
   d. 나머지 단계를 완료해서 역할을 만듭니다.

결과

이제 커넥터 EC2 인스턴스에 대해 IAM 역할이 있습니다.

AWS 액세스 키입니다

IAM 사용자에 대한 권한 및 액세스 키를 설정합니다. Connector를 설치하고 BlueXP를 설정한 후 BlueXP에 AWS 액세스 키를 제공해야 합니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책 생성:
   a. 정책 > 정책 생성 * 을 선택합니다.
   b. JSON * 을 선택하고 의 내용을 복사하여 붙여 넣습니다 "Connector에 대한 IAM 정책".
   c. 나머지 단계를 완료하고 정책을 생성합니다.

      사용할 BlueXP 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다.

   표준 영역의 경우 권한이 두 정책에 분산됩니다. AWS에서 관리되는 정책의 최대 문자 크기 제한으로 인해 두 개의 정책이 필요합니다. "Connector에 대한 IAM 정책에 대해 자세히 알아보십시오".

3. IAM 사용자에게 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"
4. 커넥터를 설치한 후 BlueXP에 추가할 수 있는 액세스 키가 사용자에게 있는지 확인합니다.

결과

이제 계정에 필요한 권한이 있습니다.

Azure 역할

필요한 권한이 있는 Azure 사용자 지정 역할을 만듭니다. 이 역할을 Connector VM에 할당합니다.

Azure 포털, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 생성할 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 생성하는 방법을 보여 줍니다. 다른 방법을 사용하려면 을 참조하십시오 "Azure 문서"

단계

1. Connector를 설치할 VM에서 시스템 할당 관리 ID를 활성화하여 사용자 지정 역할을 통해 필요한 Azure 권한을 제공할 수 있습니다.

   "Microsoft Azure 설명서: Azure 포털을 사용하여 VM의 Azure 리소스에 대해 관리되는 ID를 구성합니다"

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

   BlueXP에서 사용할 각 Azure 구독에 대한 ID를 추가해야 합니다.

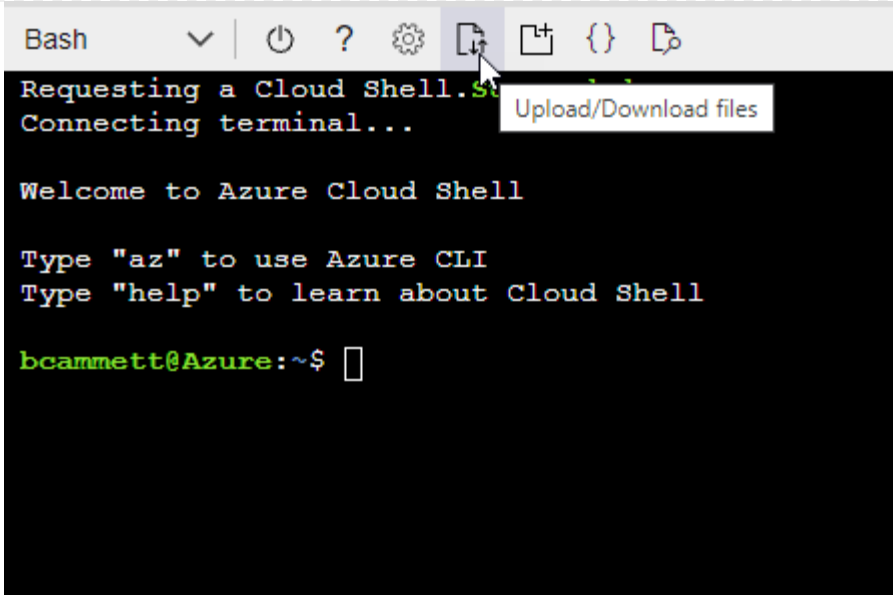
   - 예 *

```
"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 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. Azure CLI를 사용하여 사용자 지정 역할을 생성합니다.

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

결과

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

Azure 서비스 보안 주체

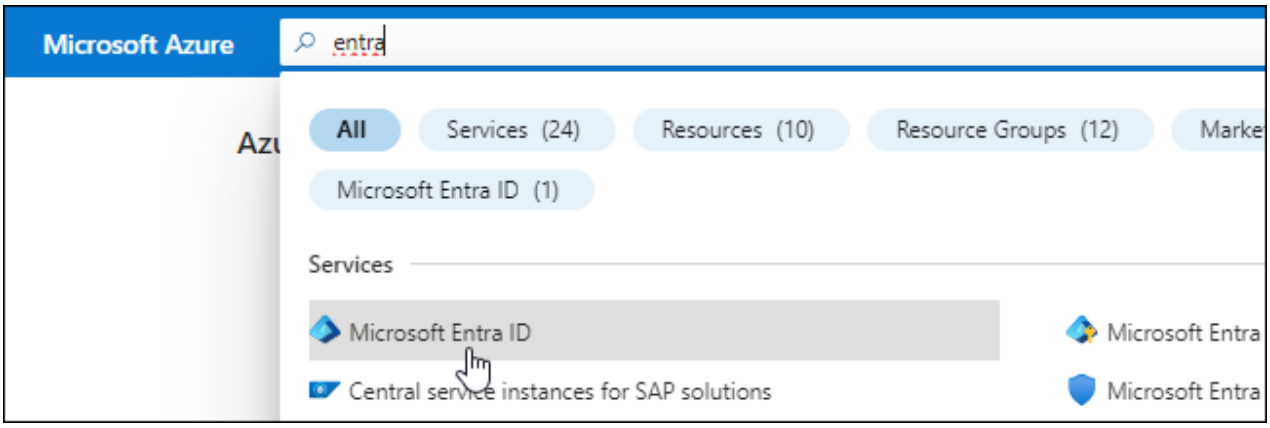
Microsoft Entra ID에서 서비스 주체를 생성 및 설정하고 BlueXP에 필요한 Azure 자격 증명을 받습니다. Connector를 설치하고 BlueXP를 설정한 후 이러한 자격 증명을 BlueXP에 제공해야 합니다.

역할 기반 액세스 제어를 위한 **Microsoft Entra** 응용 프로그램을 만듭니다

1. Azure에서 Active Directory 응용 프로그램을 만들고 응용 프로그램을 역할에 할당할 수 있는 권한이 있는지 확인합니다.

   자세한 내용은 을 참조하십시오 "Microsoft Azure 문서: 필요한 권한"

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



3. 메뉴에서 * 앱 등록 * 을 선택합니다.
4. 새 등록 * 을 선택합니다.
5. 응용 프로그램에 대한 세부 정보를 지정합니다.
   - * 이름 *: 응용 프로그램의 이름을 입력합니다.
   - * 계정 유형 *: 계정 유형을 선택합니다(모두 BlueXP에서 사용 가능).
   - * URI 리디렉션 *: 이 필드는 비워 둘 수 있습니다.
6. Register * 를 선택합니다.

   AD 응용 프로그램 및 서비스 보안 주체를 만들었습니다.

애플리케이션에 역할을 할당합니다

1. 사용자 지정 역할 만들기:

   Azure 포털, Azure PowerShell, Azure CLI 또는 REST API를 사용하여 Azure 사용자 지정 역할을 생성할 수 있습니다. 다음 단계에서는 Azure CLI를 사용하여 역할을 생성하는 방법을 보여 줍니다. 다른 방법을 사용하려면 을 참조하십시오 "Azure 문서"

   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.

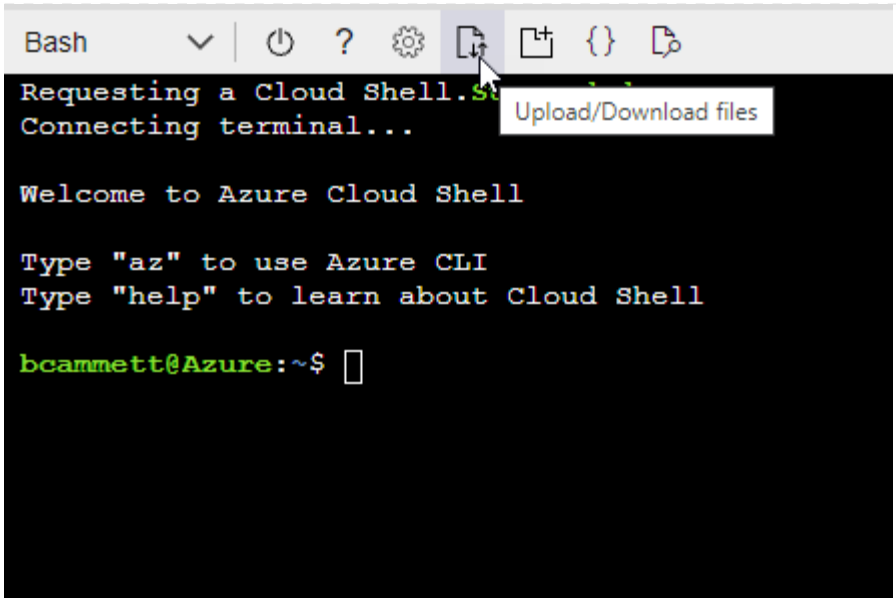
      - 예 *

      ```
      "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.



- Azure CLI를 사용하여 사용자 지정 역할을 생성합니다.

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

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

2. 역할에 응용 프로그램을 할당합니다.

   a. Azure 포털에서 * Subscriptions * 서비스를 엽니다.

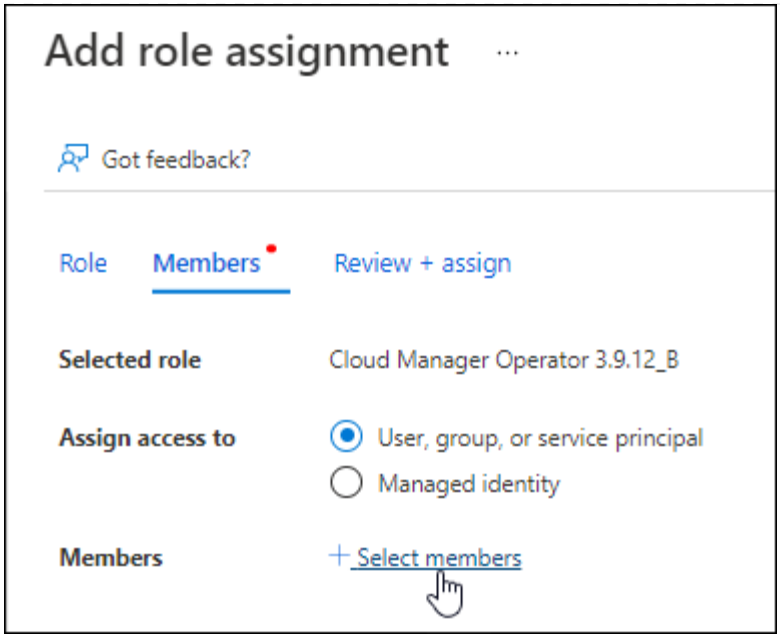
   b. 구독을 선택합니다.

   c. 액세스 제어(IAM) > 추가 > 역할 할당 추가 * 를 선택합니다.

   d. Role * 탭에서 * BlueXP Operator * 역할을 선택하고 * Next * 를 선택합니다.

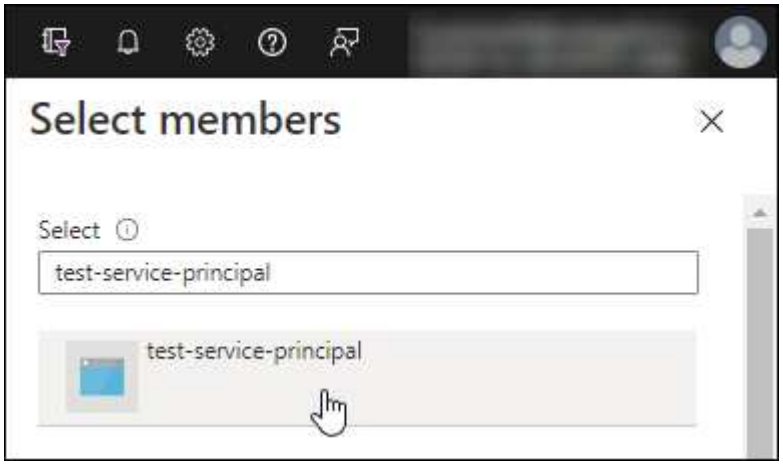
   e. Members* 탭에서 다음 단계를 완료합니다.

      - 사용자, 그룹 또는 서비스 보안 주체 * 를 선택한 상태로 유지합니다.
      - 구성원 선택 * 을 선택합니다.



- 응용 프로그램의 이름을 검색합니다.

  예를 들면 다음과 같습니다.



- 응용 프로그램을 선택하고 * 선택 * 을 선택합니다.
- 다음 * 을 선택합니다.

f. 검토 + 할당 * 을 선택합니다.

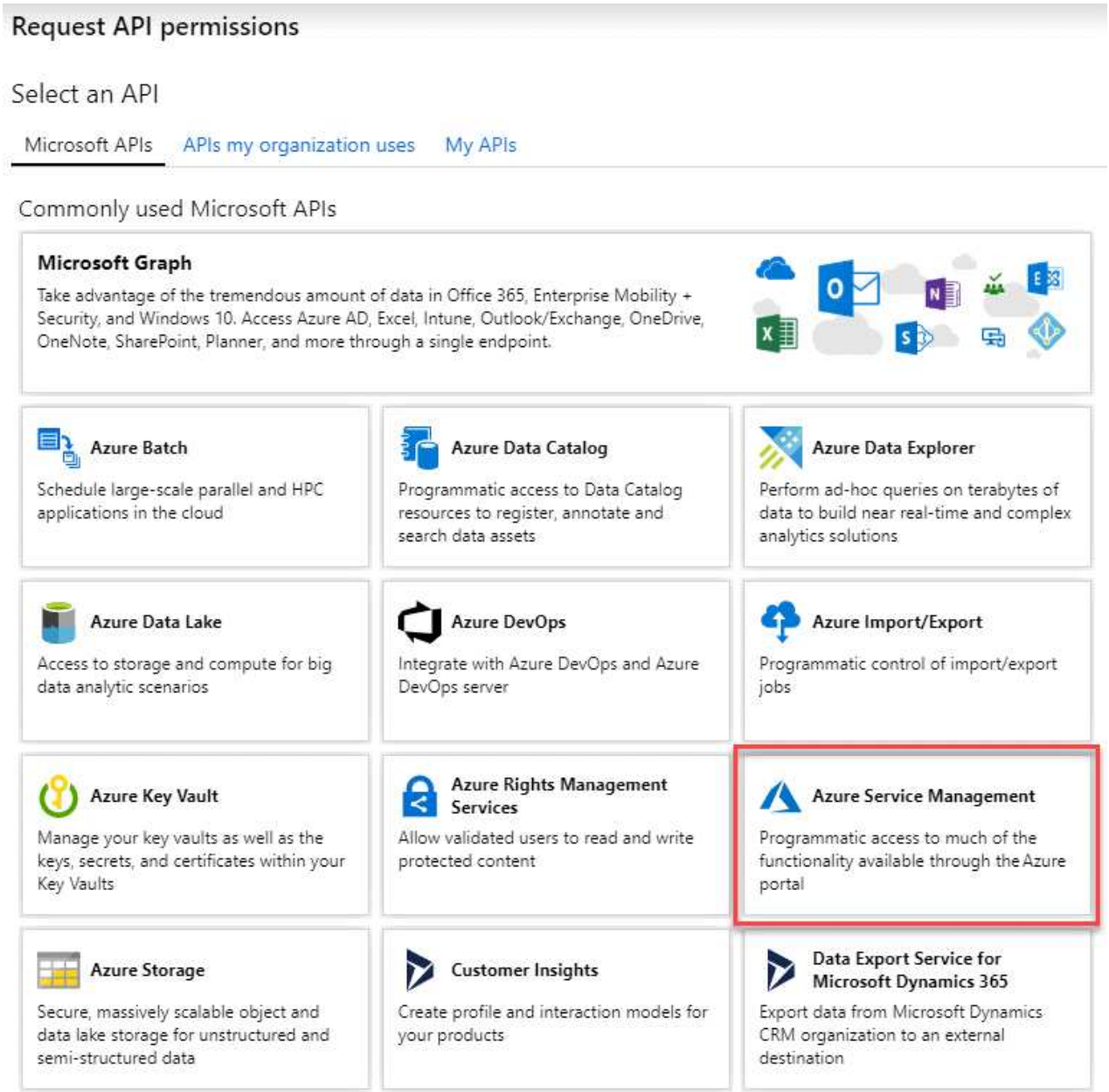
이제 서비스 보안 주체에 Connector를 배포하는 데 필요한 Azure 권한이 있습니다.

여러 Azure 구독에서 Cloud Volumes ONTAP를 배포하려면 서비스 보안 주체를 해당 구독 각각에 바인딩해야 합니다. BlueXP를 사용하면 Cloud Volumes ONTAP를 배포할 때 사용할 구독을 선택할 수 있습니다.

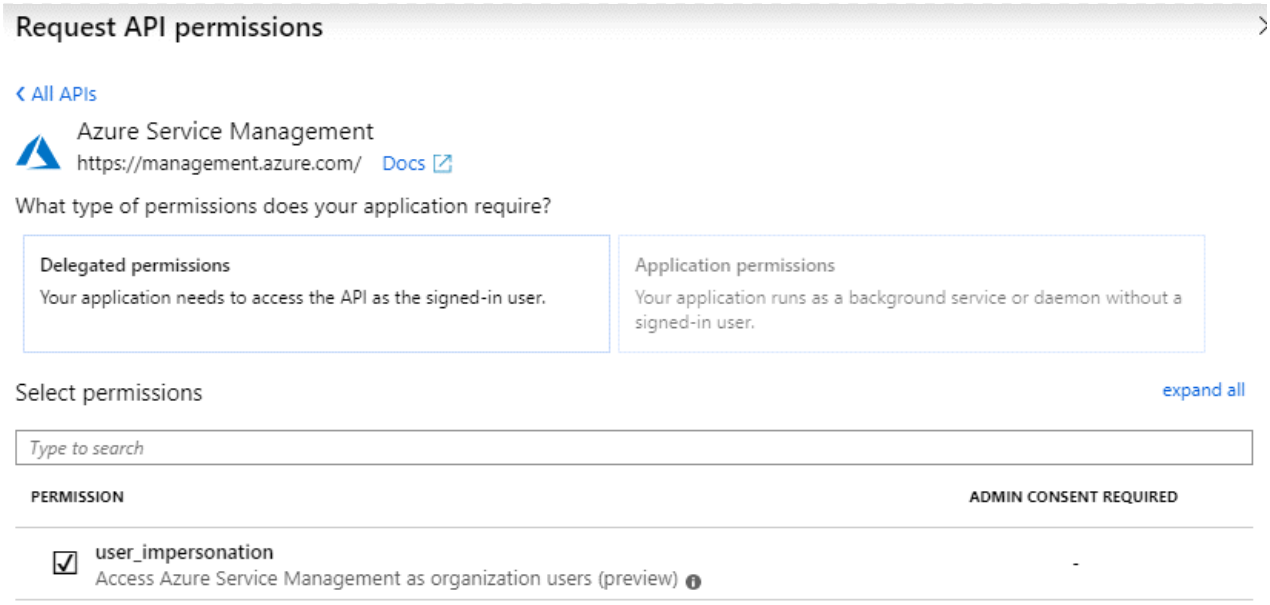
Windows Azure 서비스 관리 **API** 권한을 추가합니다

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.

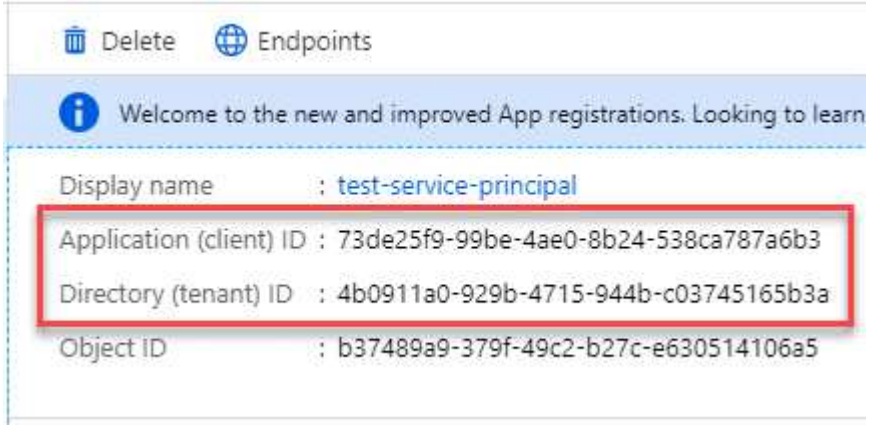


4. Access Azure Service Management as organization users * 를 선택한 다음 * Add permissions * 를 선택합니다.



응용 프로그램의 응용 프로그램 **ID** 및 디렉터리 **ID**를 가져옵니다

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



Azure 계정을 BlueXP에 추가하는 경우 응용 프로그램의 응용 프로그램(클라이언트) ID와 디렉터리(테넌트) ID를 제공해야 합니다. BlueXP는 ID를 사용하여 프로그래밍 방식으로 로그인합니다.

클라이언트 암호를 생성합니다

1. Microsoft Entra ID * 서비스를 엽니다.
2. 앱 등록 * 을 선택하고 응용 프로그램을 선택합니다.
3. 인증서 및 비밀 > 새 클라이언트 비밀 * 을 선택합니다.
4. 비밀과 기간에 대한 설명을 제공하십시오.
5. 추가 * 를 선택합니다.
6. 클라이언트 암호 값을 복사합니다.

이제 BlueXP에서 Microsoft Entra ID를 사용하여 인증하는 클라이언트 암호가 있습니다.

결과

이제 서비스 보안 주체가 설정되었으므로 응용 프로그램(클라이언트) ID, 디렉터리(테넌트) ID 및 클라이언트 암호 값을 복사해야 합니다. Azure 계정을 추가할 때 BlueXP에 이 정보를 입력해야 합니다.

Google Cloud 서비스 계정

역할을 생성하여 Connector VM 인스턴스에 사용할 서비스 계정에 적용합니다.

단계

1. Google Cloud에서 사용자 지정 역할 생성:

   a. 에 정의된 권한이 포함된 YAML 파일을 생성합니다 "Google Cloud용 커넥터 정책".

   b. Google Cloud에서 클라우드 쉘을 활성화합니다.

   c. Connector에 필요한 권한이 포함된 YAML 파일을 업로드합니다.

   d. 을 사용하여 사용자 지정 역할을 만듭니다 `gcloud iam roles create` 명령.

      다음 예제에서는 프로젝트 수준에서 "connector"라는 역할을 만듭니다.

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

   +
   "Google Cloud docs: 사용자 지정 역할 생성 및 관리"

2. Google Cloud에서 서비스 계정 생성:

   a. IAM 및 관리 서비스에서 * 서비스 계정 > 서비스 계정 생성 * 을 선택합니다.

   b. 서비스 계정 세부 정보를 입력하고 * 생성 및 계속 * 을 선택합니다.

   c. 방금 만든 역할을 선택합니다.

   d. 나머지 단계를 완료해서 역할을 만듭니다.

      "Google Cloud docs: 서비스 계정 생성"

결과

이제 Connector VM 인스턴스에 할당할 수 있는 서비스 계정이 있습니다.

6단계: Google Cloud API를 활성화합니다

Google Cloud에 Cloud Volumes ONTAP을 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
    - 클라우드 키 관리 서비스(KMS) API

      (고객이 관리하는 암호화 키(CMEK)로 BlueXP 백업 및 복구를 사용하려는 경우에만 필요)

커넥터를 비공개 모드로 배포합니다

BlueXP SaaS 계층에 대한 아웃바운드 연결 없이 BlueXP를 사용할 수 있도록 커넥터를 비공개 모드로 배포합니다. 시작하려면 Connector를 설치하고 Connector에서 실행 중인 사용자 인터페이스에 액세스하여 BlueXP를 설정한 다음 이전에 설정한 클라우드 권한을 제공합니다.

1단계: 커넥터를 설치합니다

NetApp Support 사이트에서 제품 설치 프로그램을 다운로드한 다음 자체 Linux 호스트에 커넥터를 수동으로 설치합니다.

에서 BlueXP를 사용하려는 경우 "AWS 비밀 클라우드" 또는 을 누릅니다 "AWS Top Secret Cloud의 약어입니다"그런 다음 별도의 지침에 따라 해당 환경에서 시작해야 합니다. "AWS Secret Cloud 또는 Top Secret Cloud에서 Cloud Volumes ONTAP을 시작하는 방법을 알아보십시오"

시작하기 전에

커넥터를 설치하려면 루트 권한이 필요합니다.

단계

1. Docker가 설정 및 실행 중인지 확인합니다.

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

2. 에서 Connector 소프트웨어를 다운로드합니다 "NetApp Support 사이트"

    인터넷 액세스 없이 개인 네트워크용 오프라인 설치 프로그램을 다운로드해야 합니다.

3. Linux 호스트에 설치 프로그램을 복사합니다.
4. 스크립트를 실행할 권한을 할당합니다.

```
chmod +x /path/BlueXP-Connector-offline-<version>
```

여기서 <version>는 다운로드한 커넥터 버전입니다.

5. 설치 스크립트를 실행합니다.

```
sudo /path/BlueXP-Connector-offline-<version>
```

여기서 <version>는 다운로드한 커넥터 버전입니다.

결과

커넥터 소프트웨어가 설치됩니다. 이제 BlueXP를 설정할 수 있습니다.

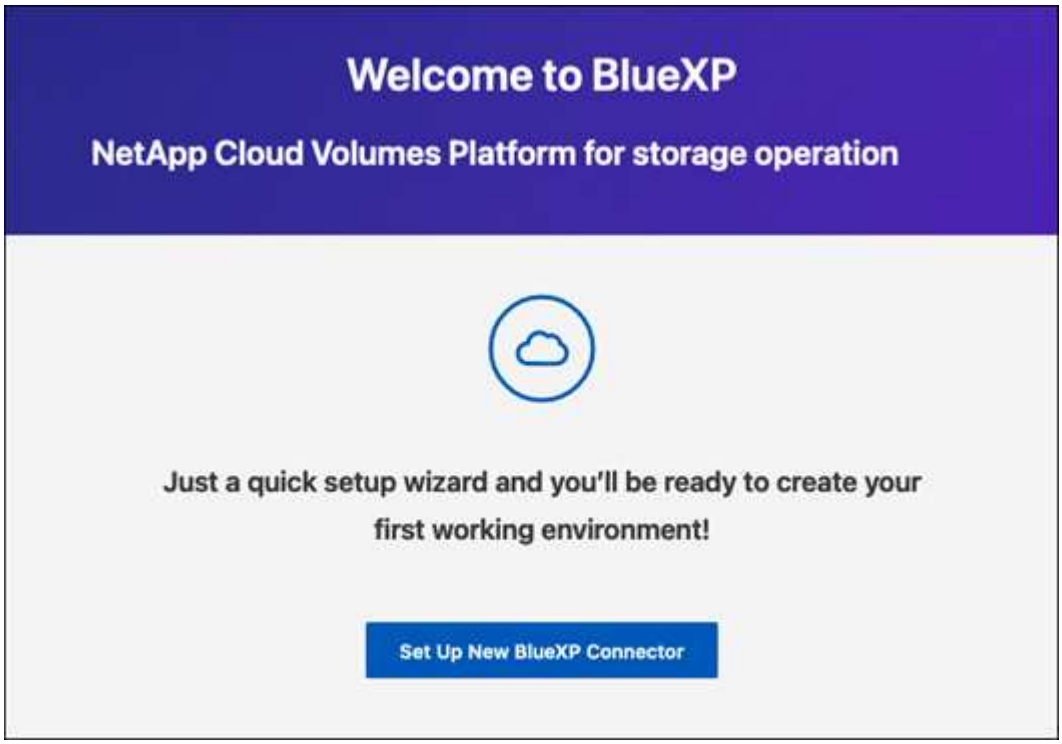
2단계**: BlueXP** 설정

BlueXP 콘솔에 처음 액세스하면 BlueXP를 설치하라는 메시지가 표시됩니다.

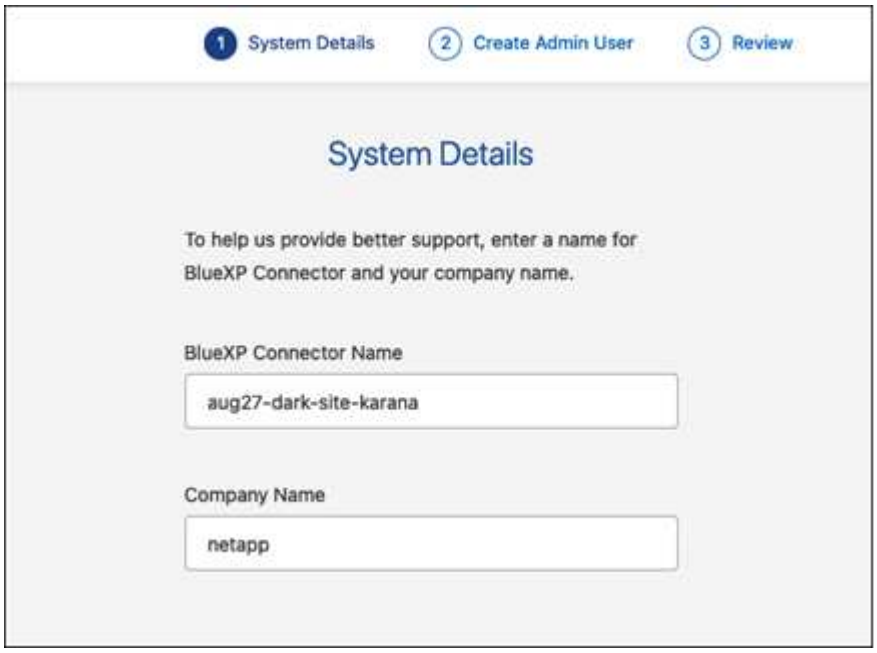
단계

1. 웹 브라우저를 열고 를 입력합니다 https://ipaddress 여기서 _ipaddress_는 Connector를 설치한 Linux 호스트의 IP 주소입니다.

   다음 화면이 나타납니다.



2. Set up New BlueXP Connector * 를 선택하고 프롬프트에 따라 시스템을 설정합니다.
   - * 시스템 세부 정보 *: 커넥터 이름과 회사 이름을 입력합니다.



- * 관리 사용자 생성 *: 시스템의 관리자 사용자를 생성합니다.

  이 사용자 계정은 시스템에서 로컬로 실행됩니다. BlueXP를 통해 사용할 수 있는 auth0 서비스에 연결할 수 없습니다.

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

3. 방금 생성한 admin 사용자를 사용하여 BlueXP에 로그인합니다.

결과

이제 커넥터가 설치되고 설정되었습니다.

Connector 소프트웨어의 새 버전을 사용할 수 있으면 NetApp Support 사이트에 게시됩니다. "Connector를 업그레이드하는 방법에 대해 알아보십시오".

다음 단계

이전에 설정한 권한을 BlueXP에 제공합니다.

3단계**: BlueXP**에 권한 제공

Cloud Volumes ONTAP 작업 환경을 만들려면 이전에 설정한 클라우드 권한을 BlueXP에 제공해야 합니다.

"클라우드 사용 권한을 준비하는 방법에 대해 알아봅니다".

AWS IAM 역할

이전에 만든 IAM 역할을 Connector EC2 인스턴스에 연결합니다.

단계

1. Amazon EC2 콘솔로 이동합니다.
2. 인스턴스 * 를 선택합니다.
3. 커넥터 인스턴스를 선택합니다.
4. Actions > Security > Modify IAM role * 을 선택합니다.
5. IAM 역할을 선택하고 * Update IAM role * 을 선택합니다.

결과

BlueXP는 이제 AWS에서 사용자 대신 작업을 수행하는 데 필요한 권한을 가집니다.

AWS 액세스 키입니다

필요한 권한이 있는 IAM 사용자를 위해 BlueXP에 AWS 액세스 키를 제공합니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

2. 자격 증명 추가 * 를 선택하고 마법사의 단계를 따릅니다.
   a. * 자격 증명 위치 *: * Amazon Web Services > Connector * 를 선택합니다.
   b. * 자격 증명 정의 *: AWS 액세스 키와 비밀 키를 입력합니다.
   c. * Marketplace 구독 *: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 선택합니다.

결과

BlueXP는 이제 AWS에서 사용자 대신 작업을 수행하는 데 필요한 권한을 가집니다.

Azure 역할

Azure 포털로 이동하여 하나 이상의 구독에 대해 Connector 가상 머신에 Azure 사용자 지정 역할을 할당합니다.

단계

1. Azure Portal에서 * Subscriptions * 서비스를 열고 구독을 선택합니다.

   구독 수준에서의 역할 할당 범위를 지정하므로 * 구독 * 서비스에서 역할을 할당하는 것이 중요합니다. scope _ 는 액세스가 적용되는 리소스 집합을 정의합니다. 범위를 다른 수준(예: 가상 머신 레벨)으로 지정하면 BlueXP 내에서 작업을 완료하는 데 영향을 줍니다.

   "Microsoft Azure 설명서: Azure RBAC의 범위를 이해합니다"

2. IAM(액세스 제어) * > * 추가 * > * 역할 할당 추가 * 를 선택합니다.
3. Role * 탭에서 * BlueXP Operator * 역할을 선택하고 * Next * 를 선택합니다.

> BlueXP 오퍼레이터는 BlueXP 정책에 제공된 기본 이름입니다. 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

4. Members* 탭에서 다음 단계를 완료합니다.
   a. 관리되는 ID*에 대한 액세스를 할당합니다.
   b. 구성원 선택 * 을 선택하고 커넥터 가상 시스템이 생성된 구독을 선택한 다음 * 관리 ID * 에서 * 가상 머신 * 을 선택한 다음 커넥터 가상 머신을 선택합니다.
   c. 선택 * 을 선택합니다.
   d. 다음 * 을 선택합니다.
   e. 검토 + 할당 * 을 선택합니다.
   f. 추가 Azure 구독에서 리소스를 관리하려면 해당 구독으로 전환한 다음 이 단계를 반복합니다.

결과

이제 BlueXP는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 가지고 있습니다.

Azure 서비스 보안 주체

이전에 설정한 Azure 서비스 보안 주체에 대한 자격 증명을 BlueXP에 제공합니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.

2. 자격 증명 추가 * 를 선택하고 마법사의 단계를 따릅니다.
   a. * 자격 증명 위치 *: * Microsoft Azure > 커넥터 * 를 선택합니다.
   b. * 자격 증명 정의 *: 필요한 권한을 부여하는 Microsoft Entra 서비스 보안 주체에 대한 정보를 입력합니다.
      - 애플리케이션(클라이언트) ID입니다
      - 디렉토리(테넌트) ID입니다
      - 클라이언트 암호
   c. * Marketplace 구독 *: 지금 가입하거나 기존 구독을 선택하여 마켓플레이스 구독을 이러한 자격 증명과 연결합니다.
   d. * 검토 *: 새 자격 증명에 대한 세부 정보를 확인하고 * 추가 * 를 선택합니다.

결과

이제 BlueXP는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 가지고 있습니다.

Google Cloud 서비스 계정

서비스 계정을 Connector VM에 연결합니다.

단계

1. Google Cloud 포털로 이동하여 Connector VM 인스턴스에 서비스 계정을 할당합니다.

   "Google Cloud 설명서: 인스턴스에 대한 서비스 계정 및 액세스 범위 변경"

2. 다른 프로젝트의 리소스를 관리하려면 해당 프로젝트에 BlueXP 역할의 서비스 계정을 추가하여 액세스 권한을 부여합니다. 각 프로젝트에 대해 이 단계를 반복해야 합니다.

결과

BlueXP는 이제 Google Cloud에서 대신 작업을 수행하는 데 필요한 권한을 가지고 있습니다.

다음에 할 수 있는 일(비공개 모드)

비공개 모드에서 BlueXP를 시작하고 실행한 후 비공개 모드로 지원되는 BlueXP 서비스를 사용할 수 있습니다.

자세한 내용은 다음 문서를 참조하십시오.

- "Cloud Volumes ONTAP 시스템을 생성합니다"
- "사내 ONTAP 클러스터에 대해 알아보십시오"
- "데이터 복제"
- "BlueXP 분류를 사용하여 온프레미스 ONTAP 볼륨 데이터를 스캔합니다"
- "BlueXP 백업 및 복구를 사용하여 사내 ONTAP 볼륨 데이터를 StorageGRID에 백업합니다"

관련 링크

"BlueXP 배포 모드"

BlueXP에 로그인합니다

BlueXP에 로그인하는 방법은 계정에 사용하는 BlueXP 구축 모드에 따라 다릅니다.

표준 모드

BlueXP에 등록하면 웹 기반 콘솔에서 로그인하여 데이터 및 스토리지 인프라 관리를 시작할 수 있습니다.

이 작업에 대해

다음 옵션 중 하나를 사용하여 BlueXP 웹 기반 콘솔에 로그인할 수 있습니다.

- 기존 NetApp Support 사이트(NSS) 자격 증명
- 이메일 주소 및 암호를 사용하여 NetApp 클라우드 로그인
- 통합 연결

  Single Sign-On을 사용하여 회사 디렉터리(통합 ID)의 자격 증명을 사용하여 로그인할 수 있습니다. "BlueXP에서 ID 페더레이션을 사용하는 방법에 대해 알아봅니다".

단계

1. 웹 브라우저를 열고 로 이동합니다 "BlueXP 콘솔"
2. 로그인 * 페이지에서 로그인과 관련된 이메일 주소를 입력합니다.
3. 로그인과 관련된 인증 방법에 따라 자격 증명을 입력하라는 메시지가 표시됩니다.
   - NetApp 클라우드 자격 증명: 암호를 입력합니다
   - 통합 사용자: 통합 ID 자격 증명을 입력합니다
   - NetApp Support 사이트 계정: NetApp Support 사이트 자격 증명을 입력합니다

결과

이제 로그인하고 BlueXP를 사용하여 하이브리드 멀티 클라우드 인프라를 관리할 수 있습니다.

제한된 모드

제한된 모드에서 BlueXP를 사용하는 경우 Connector에서 로컬로 실행되는 사용자 인터페이스에서 BlueXP 콘솔에 로그인해야 합니다.

이 작업에 대해

BlueXP에서는 계정이 제한된 모드로 설정된 경우 다음 옵션 중 하나로 로그인할 수 있습니다.

- 이메일 주소 및 암호를 사용하여 NetApp 클라우드 로그인
- 통합 연결

  Single Sign-On을 사용하여 회사 디렉터리(통합 ID)의 자격 증명을 사용하여 로그인할 수 있습니다. "BlueXP에서 ID 페더레이션을 사용하는 방법에 대해 알아봅니다".

단계

1. 웹 브라우저를 열고 다음 URL을 입력합니다.

   https://ipaddress

   _ipaddress_는 Connector를 설치한 호스트의 구성에 따라 localhost, 개인 IP 주소 또는 공용 IP 주소일 수 있습니다. 예를 들어, Connector 호스트에 접속되어 있는 호스트의 전용 IP 주소를 입력해야 할 수 있습니다.

2. 로그인하려면 사용자 이름과 암호를 입력하십시오.

결과

이제 로그인하고 BlueXP를 사용하여 하이브리드 멀티 클라우드 인프라를 관리할 수 있습니다.

비공개 모드

비공개 모드에서 BlueXP를 사용하는 경우 Connector에서 로컬로 실행되는 사용자 인터페이스에서 BlueXP 콘솔에 로그인해야 합니다.

이 작업에 대해

비공개 모드는 로컬 사용자 관리 및 액세스를 지원합니다. BlueXP의 클라우드 서비스를 통해 인증이 제공되지 않습니다.

단계

1. 웹 브라우저를 열고 다음 URL을 입력합니다.

   https://ipaddress

   _ipaddress_는 Connector를 설치한 호스트의 구성에 따라 localhost, 개인 IP 주소 또는 공용 IP 주소일 수 있습니다. 예를 들어, Connector 호스트에 접속되어 있는 호스트의 전용 IP 주소를 입력해야 할 수 있습니다.

2. 로그인하려면 사용자 이름과 암호를 입력하십시오.

결과

이제 로그인하고 BlueXP를 사용하여 하이브리드 멀티 클라우드 인프라를 관리할 수 있습니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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