제한된 모드로 시작하십시오

Setup and administration

NetApp
April 11, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/bluexp-setup-admin/task-quick-start-restricted-mode.html on April 11, 2024. Always check docs.netapp.com for the latest.

목차

제한된 모드로 시작하십시오 1
워크플로 시작(제한된 모드) 1
제한된 모드에서 배포를 준비합니다 1
커넥터를 제한 모드로 전개합니다 17
BlueXP 가입(제한 모드) 29
다음에 수행할 수 있는 작업(제한된 모드) 35

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

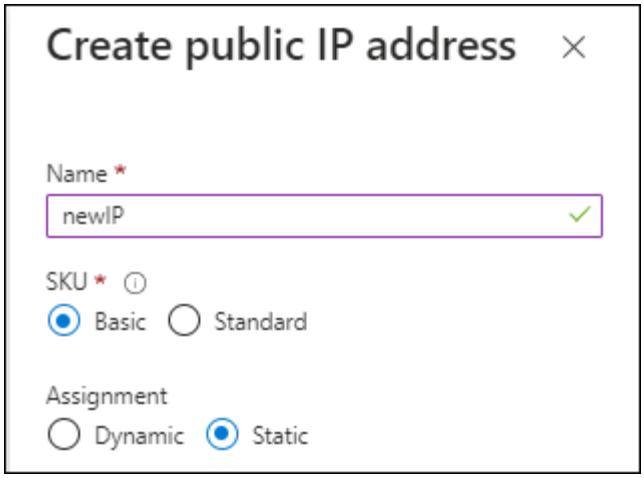
커넥터를 배포하는 네트워크 위치에 아웃바운드 인터넷 연결이 있어야 합니다. Connector는 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하기 위해 다음 엔드포인트에 연결하는 아웃바운드 인터넷 액세스를 필요로 합니다.

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.

엔드포인트	목적
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 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.

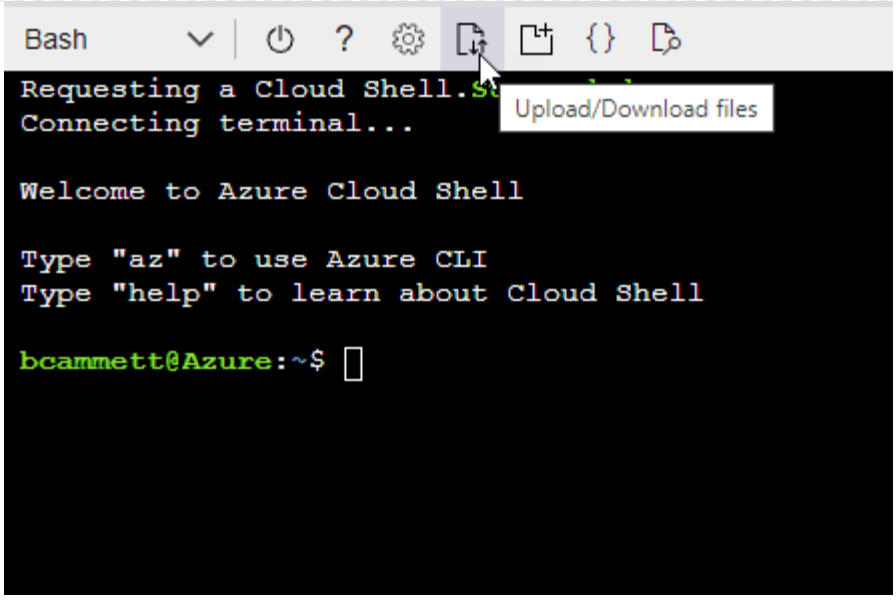
   - 예 *

```
"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

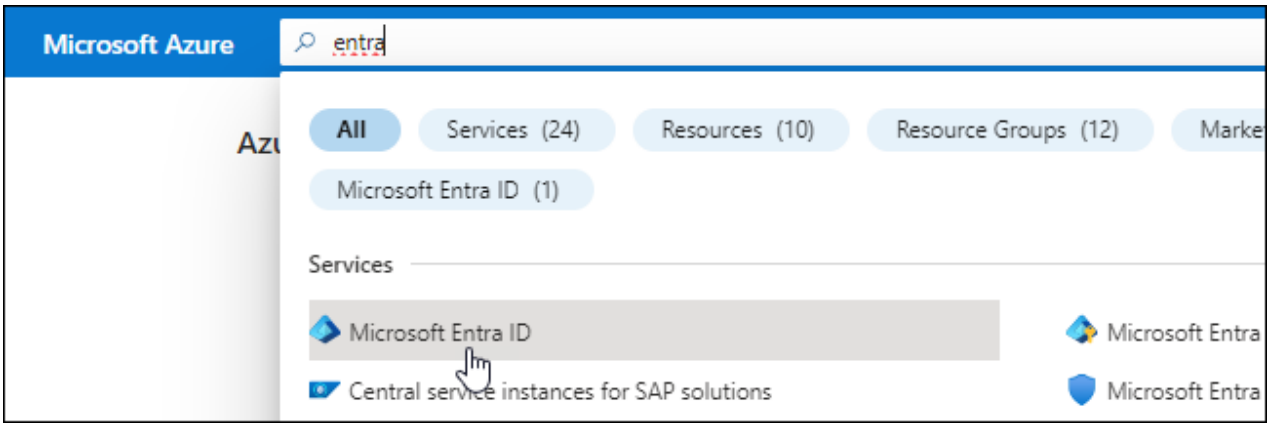
Microsoft Entra ID에서 서비스 주체를 생성 및 설정하고 BlueXP에 필요한 Azure 자격 증명을 받습니다. Connector를 설치하고 BlueXP를 설정한 후 이러한 자격 증명을 BlueXP에 제공해야 합니다.

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.

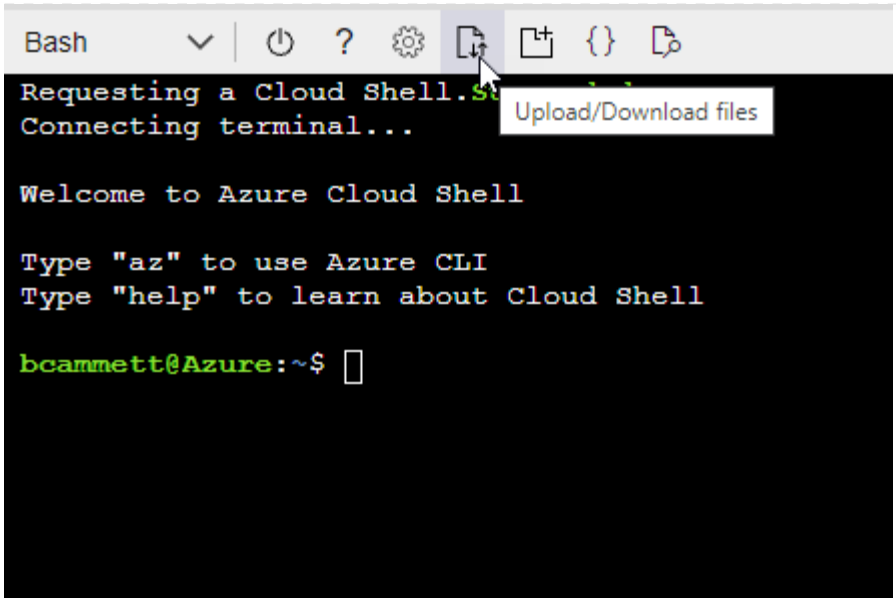
      - 예 *

      ```
      "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.

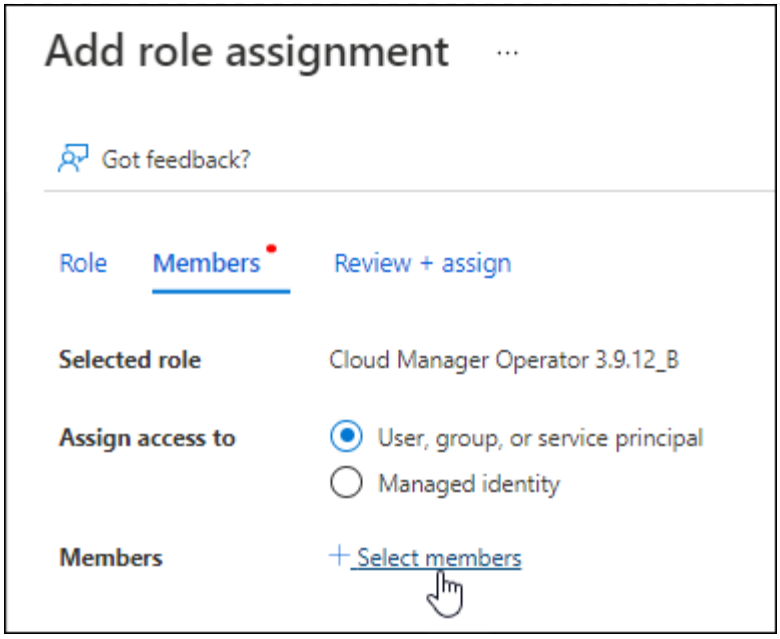
   b. 구독을 선택합니다.

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

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

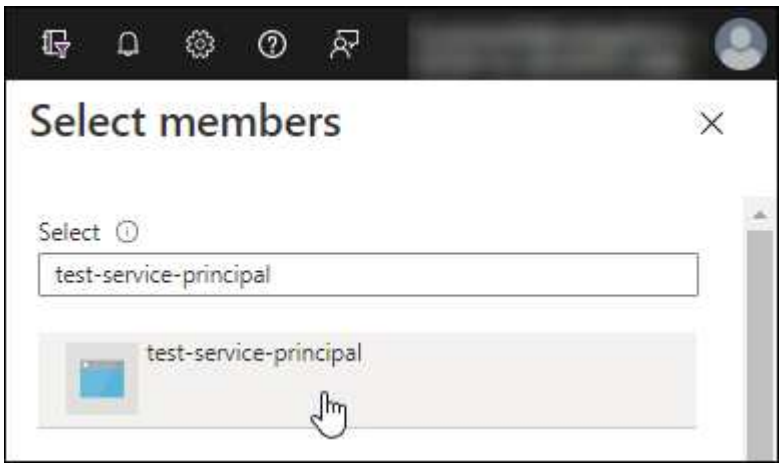
   e. Members* 탭에서 다음 단계를 완료합니다.

      - 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.

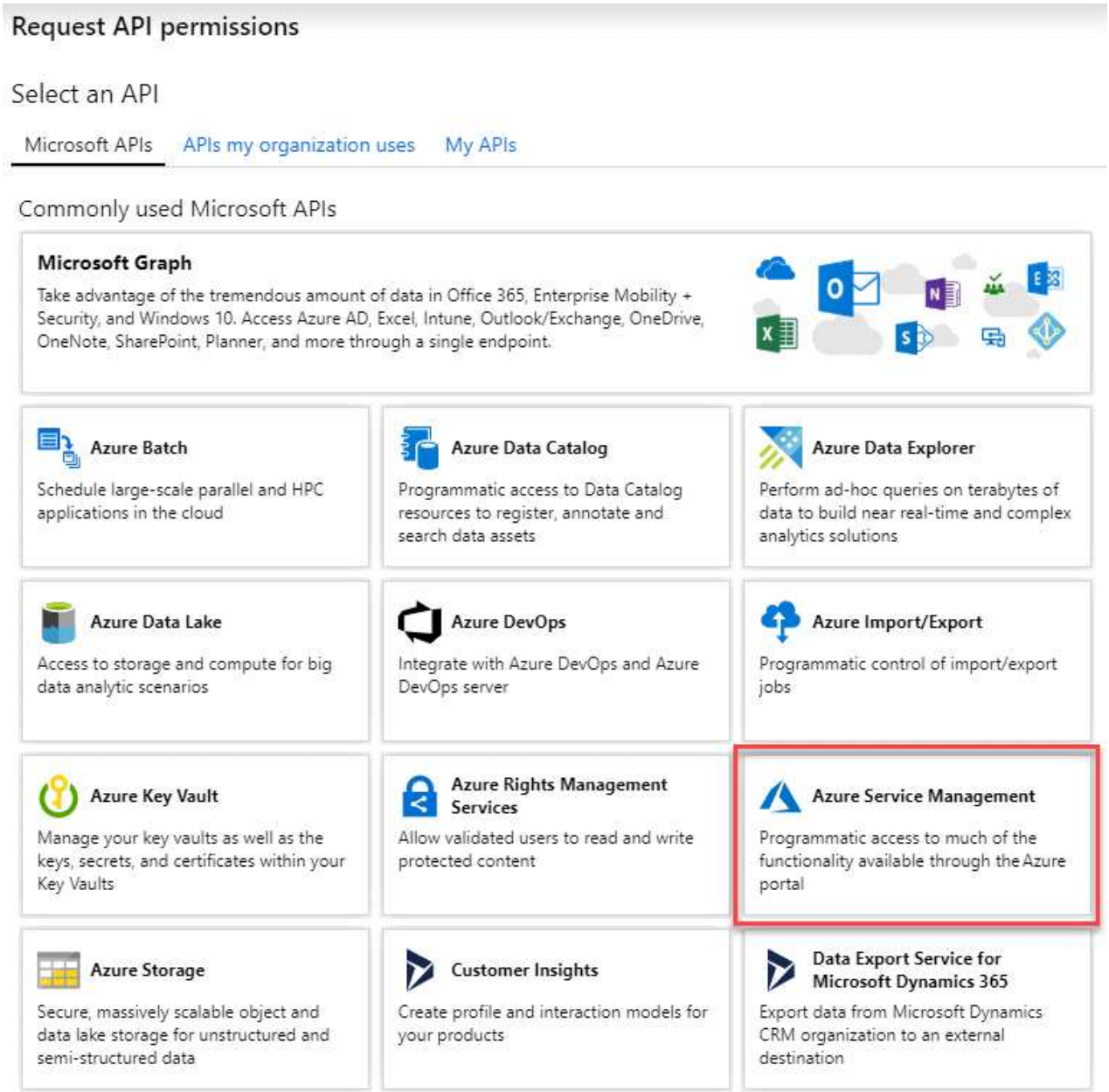
이제 서비스 보안 주체에 Connector를 배포하는 데 필요한 Azure 권한이 있습니다.

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.

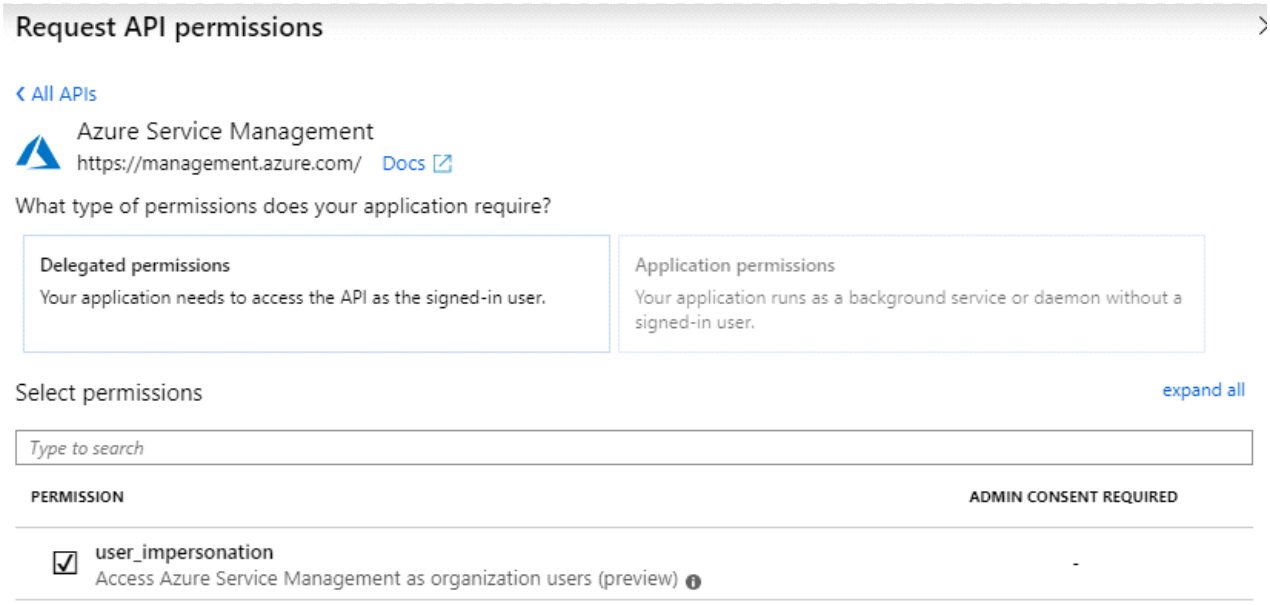
Windows Azure 서비스 관리 **API** 권한을 추가합니다

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.

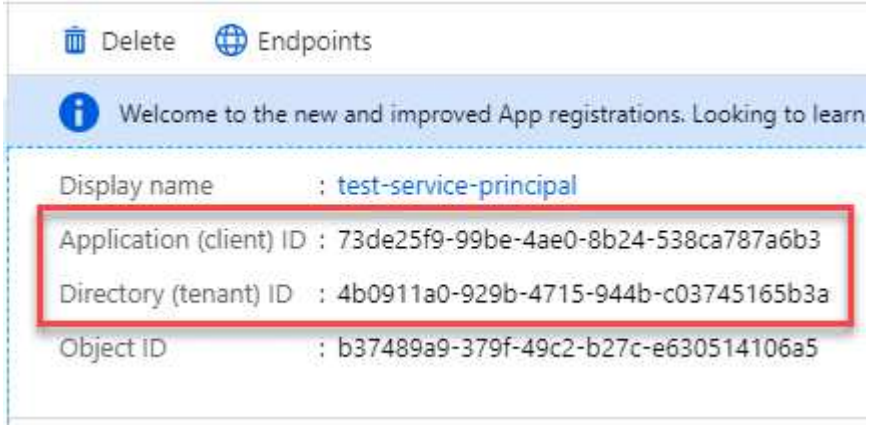


4. Access Azure Service Management as organization users * 를 선택한 다음 * Add permissions * 를 선택합니다.



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 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 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"

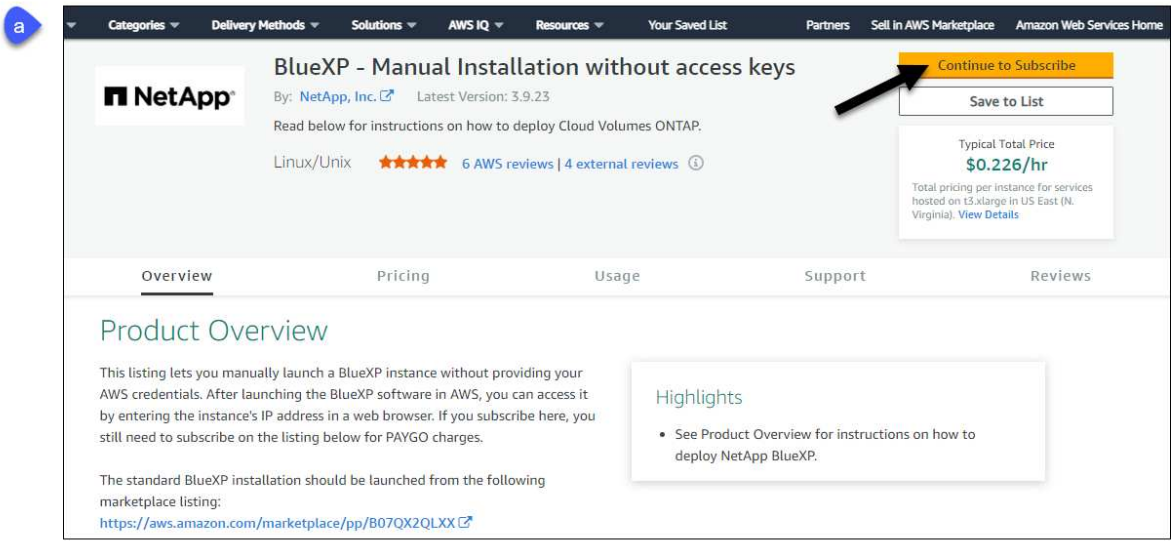
- IAM 사용자에 대한 AWS 마켓플레이스의 구독 및 구독 취소 권한
- 인스턴스의 CPU 및 RAM 요구 사항 이해

  "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"

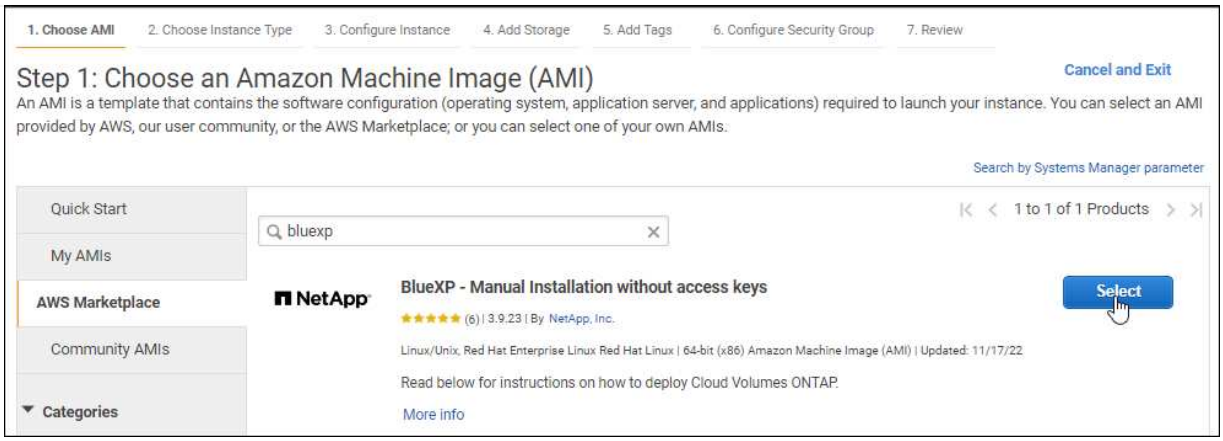
- Connector에 필요한 권한을 포함하는 정책이 첨부된 IAM 역할

  "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.

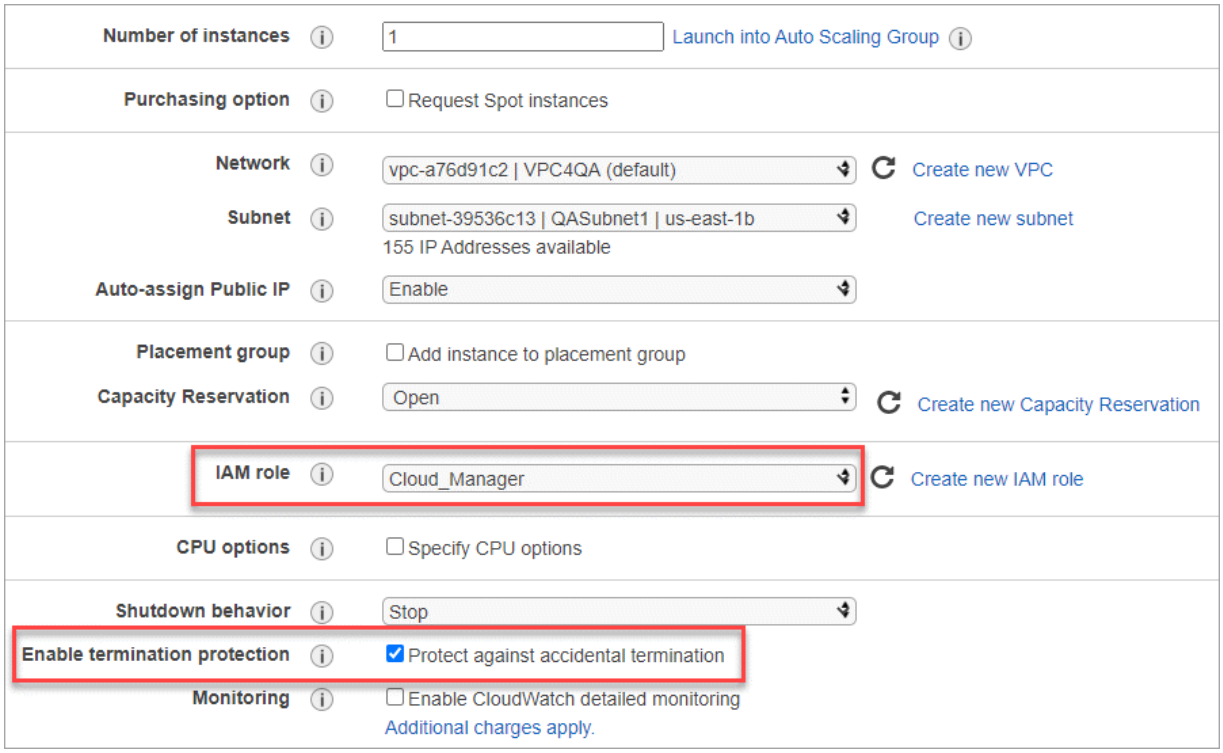


d. Continue * 를 선택합니다.

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.

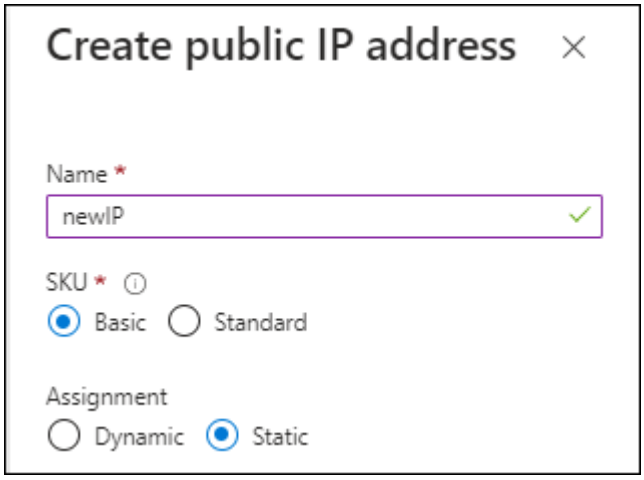
  "Azure 사용 권한을 설정하는 방법에 대해 알아봅니다"

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.

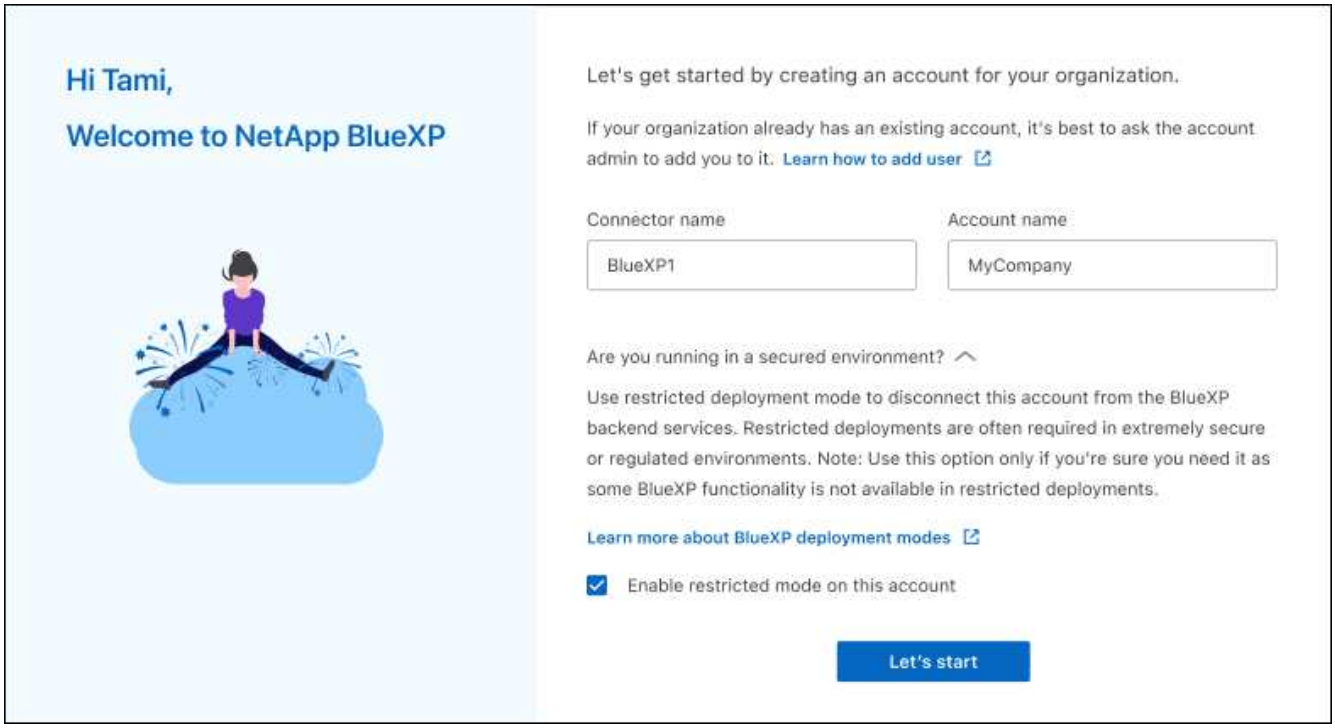
   a. 커넥터 이름을 입력합니다.
   b. 새 BlueXP 계정의 이름을 입력하거나 기존 계정을 선택합니다.

      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: BlueXP에 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.
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 Connector 가상 머신이 생성된 구독을 선택한 다음 * 가상 머신 * 을 선택하고 Connector 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

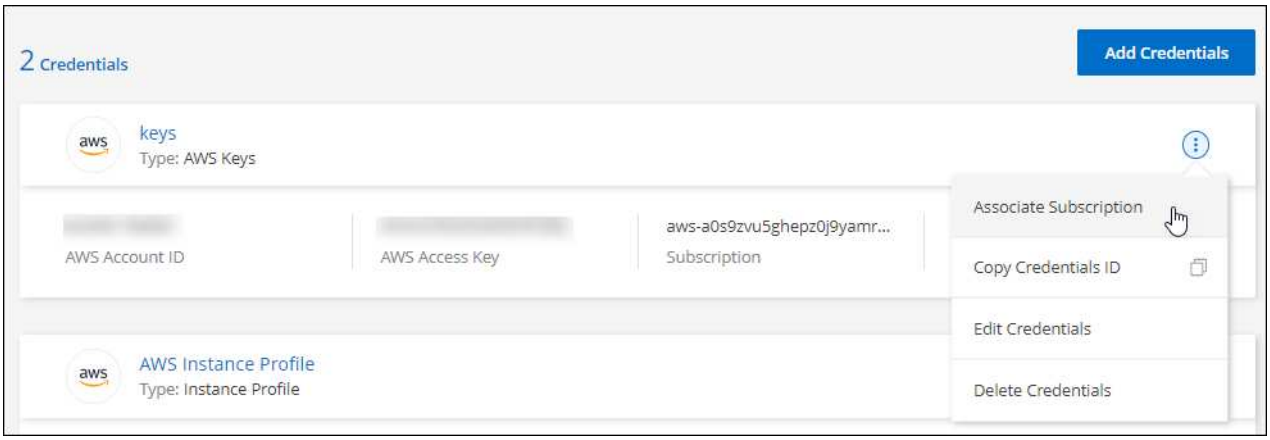
BlueXP를 구독하려면 Connector와 연결된 클라우드 자격 증명과 마켓플레이스 구독을 연결해야 합니다. "제한된 모드로 시작하기" 워크플로를 따랐다면 이미 Connector가 있는 것입니다. 자세한 내용은 를 참조하십시오 "제한된 모드에서 BlueXP를 빠르게 시작합니다".

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.

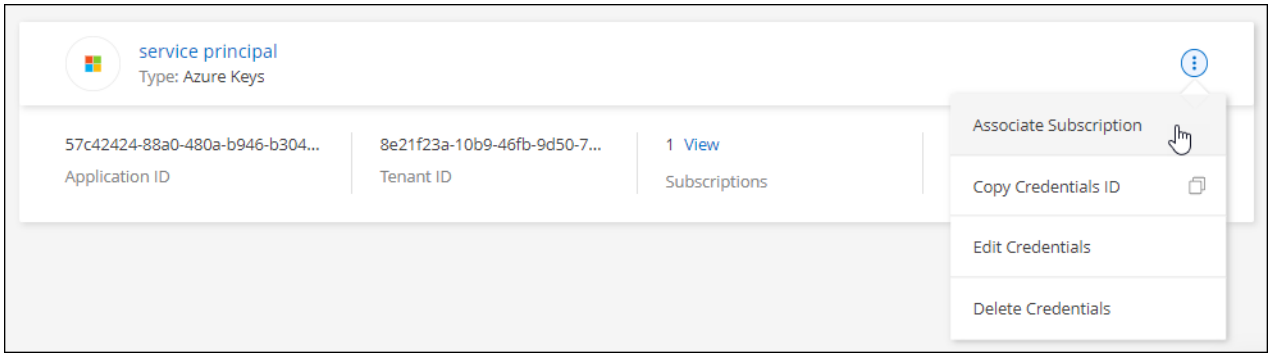
   AWS 마켓플레이스에서 BlueXP를 구독하십시오

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.

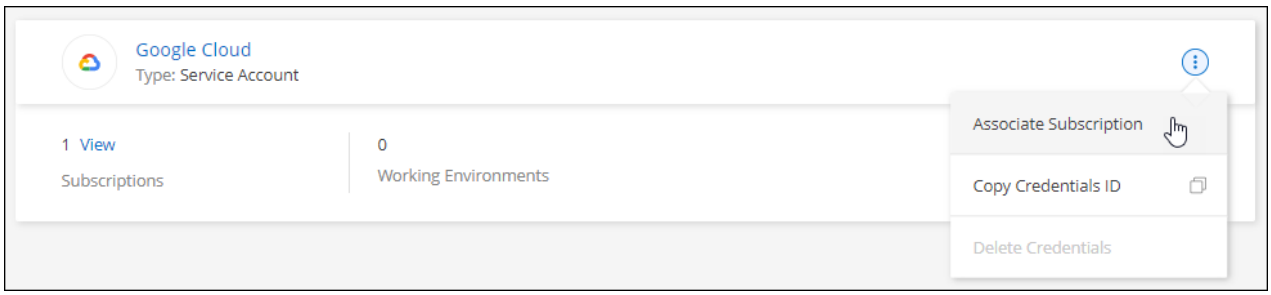
   Azure 마켓플레이스에서 BlueXP를 구독하십시오

Google 클라우드

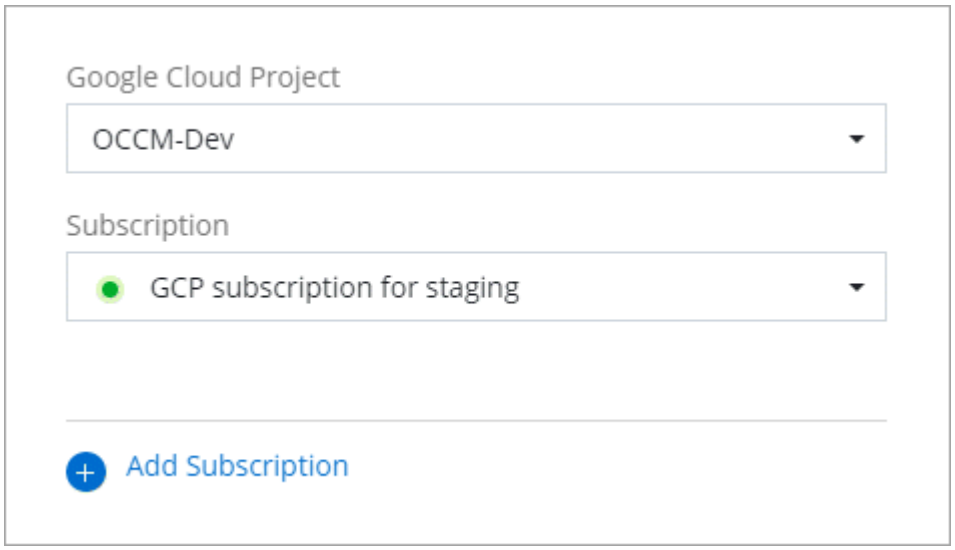
단계

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.



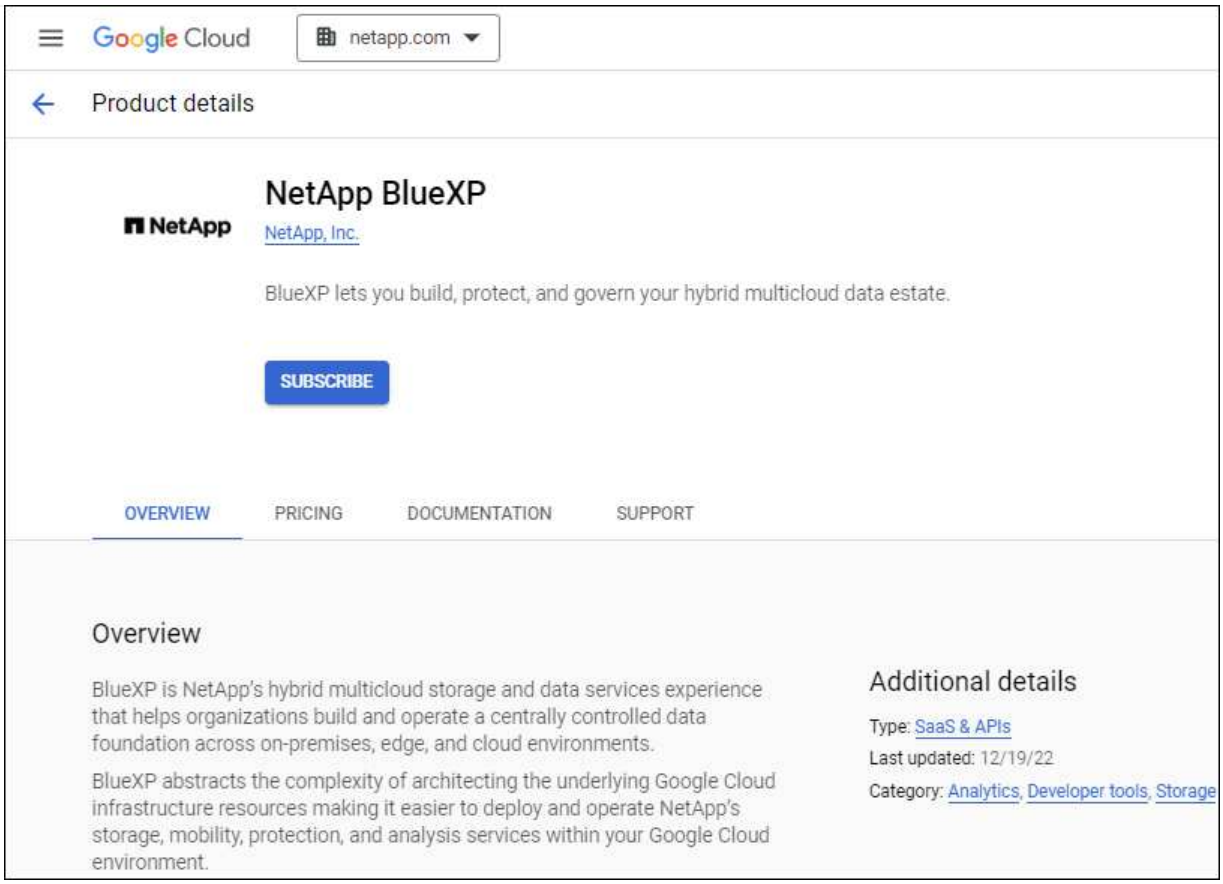
3. 자격 증명을 기존 구독과 연결하려면 아래 목록에서 Google Cloud 프로젝트 및 구독을 선택한 다음 * Associate * 를 선택합니다.



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.

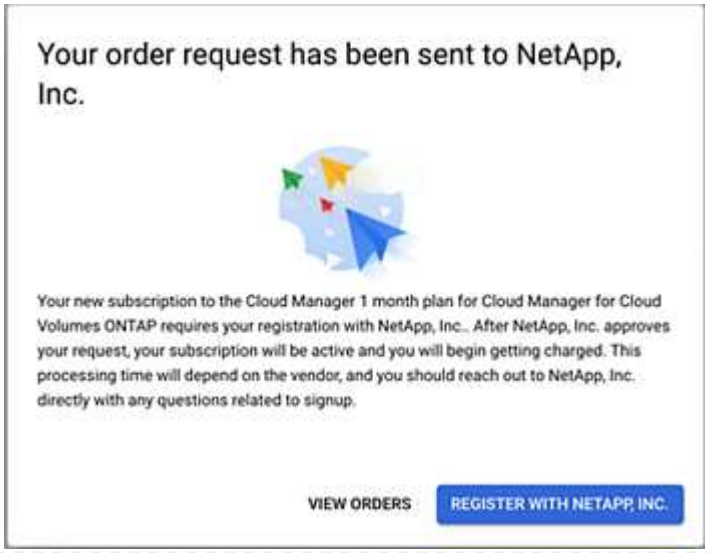
c. 적절한 청구 계정을 선택하고 이용 약관에 동의합니다.

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.

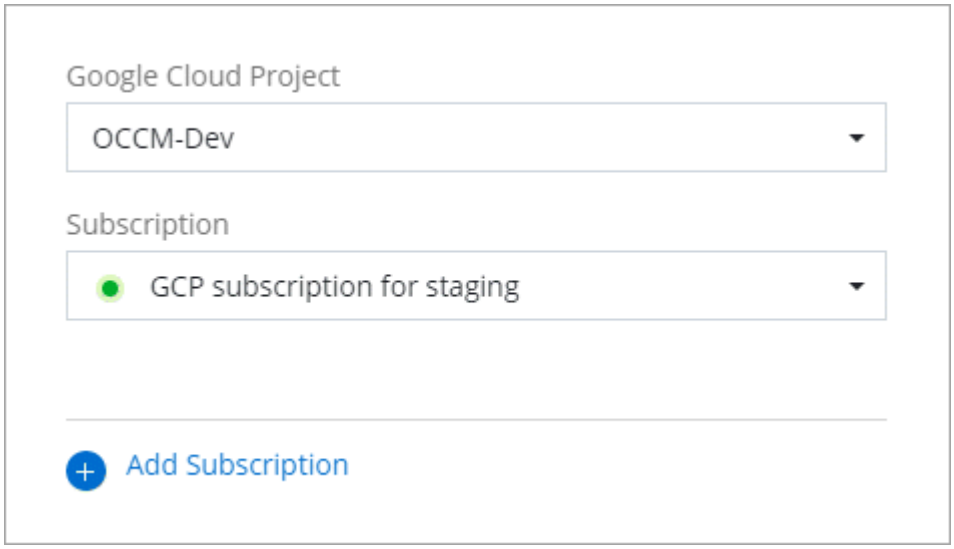
다른 모든 계정의 경우 이 단계를 반복하여 구독을 수동으로 연결해야 합니다.

- 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"

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.