시작하기
Cloud Manager 3.6

NetApp
March 25, 2024

목차

시작하기

구축 개요

시작하기 전에 OnCommand Cloud Manager 및 Cloud Volumes ONTAP 구축 옵션에 대해 잘 알고 싶을 수 있습니다.

Cloud Manager 설치

Cloud Volumes ONTAP를 구축 및 관리하려면 Cloud Manager 소프트웨어가 필요합니다. Cloud Manager는 다음 위치 중 원하는 곳에 구축할 수 있습니다.

- AWS(Amazon Web Services)
- Microsoft Azure를 참조하십시오
- IBM 클라우드
- 직접 네트워크를 통해

Cloud Manager의 구축 방법은 선택한 위치에 따라 다릅니다.

위치	**Cloud Manager** 구축 방법
설치하고	"NetApp Cloud Central에서 Cloud Manager 구축"
AWS C2S	"AWS Intelligence Community Marketplace에서 Cloud Manager 구축"
Azure는 일반적으로 사용 가능한 지역입니다	"NetApp Cloud Central에서 Cloud Manager 구축"
Azure 정부	"Azure US Government Marketplace에서 Cloud Manager를 구현합니다"
Azure 독일	"Linux 호스트에 소프트웨어를 다운로드하고 설치합니다"
IBM 클라우드	"Linux 호스트에 소프트웨어를 다운로드하고 설치합니다"
온프레미스 네트워크	"Linux 호스트에 소프트웨어를 다운로드하고 설치합니다"

Cloud Manager 설정

클라우드 공급자 계정 추가, HTTPS 인증서 설치 등과 같은 Cloud Manager를 설치한 후 추가 설정을 수행할 수 있습니다.

- "Cloud Manager에 클라우드 공급자 계정 추가"
- "HTTPS 인증서 설치"
- "사용자 및 테넌트 설정"
- "AWS KMS 설정"

Cloud Volumes ONTAP 구축

Cloud Manager를 시작 및 실행한 후 AWS 및 Microsoft Azure에서 Cloud Volumes ONTAP 구축을 시작할 수

있습니다.

"AWS 시작하기" 및 "Azure에서 시작하기" Cloud Volumes ONTAP를 빠르게 시작하고 실행하기 위한 지침을 제공합니다. 추가 도움말은 다음을 참조하십시오.

- "Cloud Volumes ONTAP 9.5에 지원되는 구성입니다"
- "구성 계획"
- "AWS에서 Cloud Volumes ONTAP 실행"
- "Azure에서 Cloud Volumes ONTAP 실행"

AWS에서 Cloud Volumes ONTAP 시작하기

NetApp Cloud Central에서 AWS의 Cloud Volumes ONTAP를 시작할 수 있습니다.

네트워크 설정

1. Cloud Manager 및 Cloud Volumes ONTAP가 여러 엔드포인트에 연결할 수 있도록 타겟 VPC에서 아웃바운드 인터넷 액세스를 지원합니다.

   이 단계는 Cloud Manager가 아웃바운드 인터넷 액세스 없이 Cloud Volumes ONTAP를 구축할 수 없기 때문에 중요합니다. 아웃바운드 연결을 제한해야 하는 경우 의 끝점 목록을 참조하십시오 "클라우드 관리자" 및 "Cloud Volumes ONTAP".

2. VPC 엔드포인트를 S3 서비스로 설정합니다.

   Cloud Volumes ONTAP의 콜드 데이터를 저비용 오브젝트 스토리지로 계층화하려는 경우 VPC 엔드포인트가 필요합니다.

AWS Marketplace에서 **Cloud Volumes ONTAP**를 구독하십시오

가입 "AWS 마켓플레이스" 소프트웨어 약관에 동의해야 합니다. 마켓플레이스에서만 구독해야 합니다. 어디서나 Cloud Volumes ONTAP를 시작할 수는 있지만 Cloud Manager는 지원되지 않습니다.

필요한 **AWS** 권한을 제공합니다

NetApp Cloud Central에서 Cloud Manager를 구축할 때 인스턴스를 배포할 수 있는 권한이 있는 AWS 계정을 사용해야 합니다.

1. AWS IAM 콘솔로 이동하여 의 내용을 복사하여 붙여 넣어 정책을 생성합니다 "AWS를 위한 NetApp Cloud Central 정책".
2. 정책을 IAM 사용자에게 연결합니다.

NetApp Cloud Central에서 **Cloud Manager**를 실행합니다

Cloud Volumes ONTAP를 구축 및 관리하려면 Cloud Manager 소프트웨어가 필요합니다. Cloud Manager 인스턴스를 시작하는 데는 몇 분 밖에 걸리지 않습니다 "Cloud Central을 참조하십시오".

Cloud Manager를 사용하여 **Cloud Volumes ONTAP**를 실행합니다

Cloud Manager가 준비되면 생성 을 클릭하고 시작할 시스템 유형을 선택한 다음 마법사의 단계를 완료합니다. 25분 후 첫 번째 Cloud Volumes ONTAP 시스템이 가동되어 실행 중이어야 합니다.

관련 링크

- "평가 중"
- "Cloud Manager의 네트워킹 요구사항"
- "AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항"
- "AWS의 보안 그룹 규칙"
- "Cloud Manager에 클라우드 공급자 계정 추가"
- "Cloud Manager에서 AWS 권한을 통해 수행하는 것"
- "AWS에서 Cloud Volumes ONTAP 실행"
- "AWS Marketplace에서 Cloud Manager 시작"

Azure에서 Cloud Volumes ONTAP 시작하기

NetApp Cloud Central에서 Azure의 Cloud Volumes ONTAP를 시작할 수 있습니다. Cloud Manager를 구축할 수 있는 별도의 지침이 제공됩니다 "Azure 미국 정부 지역" 및 IN "Azure 독일 지역".

네트워크 설정

클라우드 관리자 및 Cloud Volumes ONTAP가 여러 엔드포인트에 연결할 수 있도록 대상 VNET에서 아웃바운드 인터넷 액세스를 활성화합니다.

이 단계는 Cloud Manager가 아웃바운드 인터넷 액세스 없이 Cloud Volumes ONTAP를 구축할 수 없기 때문에 중요합니다. 아웃바운드 연결을 제한해야 하는 경우 의 끝점 목록을 참조하십시오 "클라우드 관리자" 및 "Cloud Volumes ONTAP".

필요한 **Azure** 권한을 제공합니다

NetApp Cloud Central에서 Cloud Manager를 구축할 때 Cloud Manager 가상 머신을 구축할 권한이 있는 Azure 계정을 사용해야 합니다.

1. 를 다운로드합니다 "Azure를 위한 NetApp Cloud Central 정책".

2. Azure 구독 ID를 "AssignableScopes" 필드에 추가하여 JSON 파일을 수정합니다.
3. JSON 파일을 사용하여 이름이 _Azure SetupAsService_인 Azure에서 사용자 지정 역할을 생성합니다.

   예: * az 역할 정의 create — role-definition C:\Policy_for_Setup_as_Service_Azure.json *

4. Azure 포털에서 Cloud Central에서 Cloud Manager를 배포할 사용자에게 사용자 지정 역할을 할당합니다.

NetApp Cloud Central에서 **Cloud Manager**를 실행합니다

Cloud Volumes ONTAP를 구축 및 관리하려면 Cloud Manager 소프트웨어가 필요합니다. Cloud Manager 인스턴스를 시작하는 데는 몇 분 밖에 걸리지 않습니다 "Cloud Central을 참조하십시오".

Cloud Manager를 사용하여 **Cloud Volumes ONTAP**를 실행합니다

Cloud Manager가 준비되면 생성 을 클릭하고 구축할 시스템 유형을 선택한 다음 마법사의 단계를 완료합니다. 25분 후 첫 번째 Cloud Volumes ONTAP 시스템이 가동되어 실행 중이어야 합니다.

관련 링크

- "평가 중"
- "Cloud Manager의 네트워킹 요구사항"
- "Azure의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항"
- "Azure의 보안 그룹 규칙"
- "Cloud Manager에 클라우드 공급자 계정 추가"
- "Cloud Manager가 Azure 권한으로 수행하는 기능"
- "Azure에서 Cloud Volumes ONTAP 실행"
- "Azure 마켓플레이스에서 Cloud Manager 시작"

Cloud Manager 설정

Cloud Manager에 클라우드 공급자 계정 추가

다른 클라우드 계정에 Cloud Volumes ONTAP를 배포하려면 해당 계정에 필요한 권한을 제공한 다음 세부 정보를 Cloud Manager에 추가해야 합니다.

Cloud Central에서 Cloud Manager를 구축하면 Cloud Manager가 자동으로 을 추가합니다 "클라우드 공급자 계정입니다" Cloud Manager를 구축한 계정의 경우 기존 시스템에 Cloud Manager 소프트웨어를 수동으로 설치한 경우 초기 클라우드 공급자 계정이 추가되지 않습니다.

Cloud Manager에 AWS 계정 설정 및 추가

다른 AWS 계정에 Cloud Volumes ONTAP를 구축하려는 경우 해당 계정에 필요한 권한을 제공한 다음 세부 정보를 Cloud Manager에 추가해야 합니다. 사용 권한을 제공하는 방법은 Cloud Manager에 AWS 키를 제공할지, 아니면 신뢰할 수 있는 계정에서 역할의 ARN을 제공하는지에 따라 달라집니다.

- AWS 키를 제공할 때 사용 권한 부여
- 다른 계정에서 IAM 역할을 가정하여 권한 부여

AWS 키를 제공할 때 사용 권한 부여

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

단계

1. 에서 Cloud Manager IAM 정책을 다운로드합니다 "Cloud Manager 정책 페이지".
2. IAM 콘솔에서 Cloud Manager IAM 정책의 텍스트를 복사하여 붙여넣어 고유한 정책을 생성합니다.

   "AWS 설명서: IAM 정책 생성"

3. IAM 역할 또는 IAM 사용자에 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"

결과

이제 계정에 필요한 권한이 있습니다. 이제 Cloud Manager에 추가할 수 있습니다.

다른 계정에서 IAM 역할을 가정하여 권한 부여

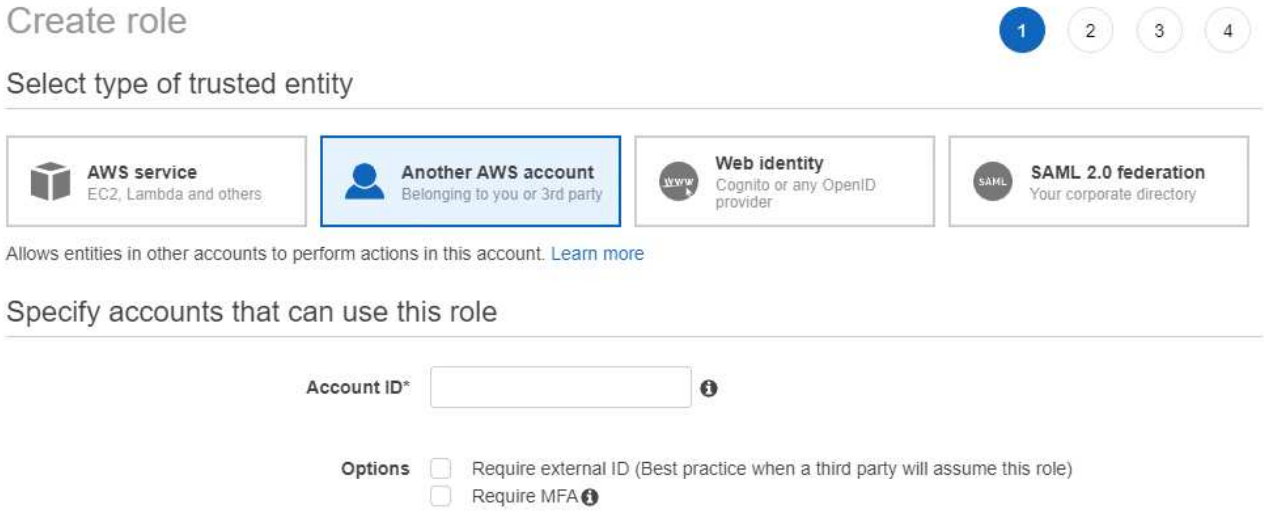
IAM 역할을 사용하여 Cloud Manager 인스턴스와 다른 AWS 계정을 구축한 소스 AWS 계정과 신뢰 관계를 설정할 수 있습니다. 그런 다음 Cloud Manager에 신뢰할 수 있는 계정의 IAM 역할 ARN을 제공합니다.

단계

1. Cloud Volumes ONTAP를 배포하려는 대상 계정으로 이동하여 * 다른 AWS 계정 * 을 선택하여 IAM 역할을 생성합니다.

   다음을 수행하십시오.

   - Cloud Manager 인스턴스가 있는 계정의 ID를 입력합니다.
   - 에서 사용할 수 있는 Cloud Manager IAM 정책을 연결합니다 "Cloud Manager 정책 페이지".



2. Cloud Manager 인스턴스가 있는 소스 계정으로 이동하여 인스턴스에 연결된 IAM 역할을 선택합니다.

   a. 신뢰 관계 > 신뢰 관계 편집 * 을 클릭합니다.

   b. "STS:AssumRole" 작업과 대상 계정에서 생성한 역할의 ARN을 추가합니다.

      ▪ 예 *

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

결과

이제 계정에 필요한 권한이 있습니다. 이제 Cloud Manager에 추가할 수 있습니다.

Cloud Manager에 AWS 계정 추가

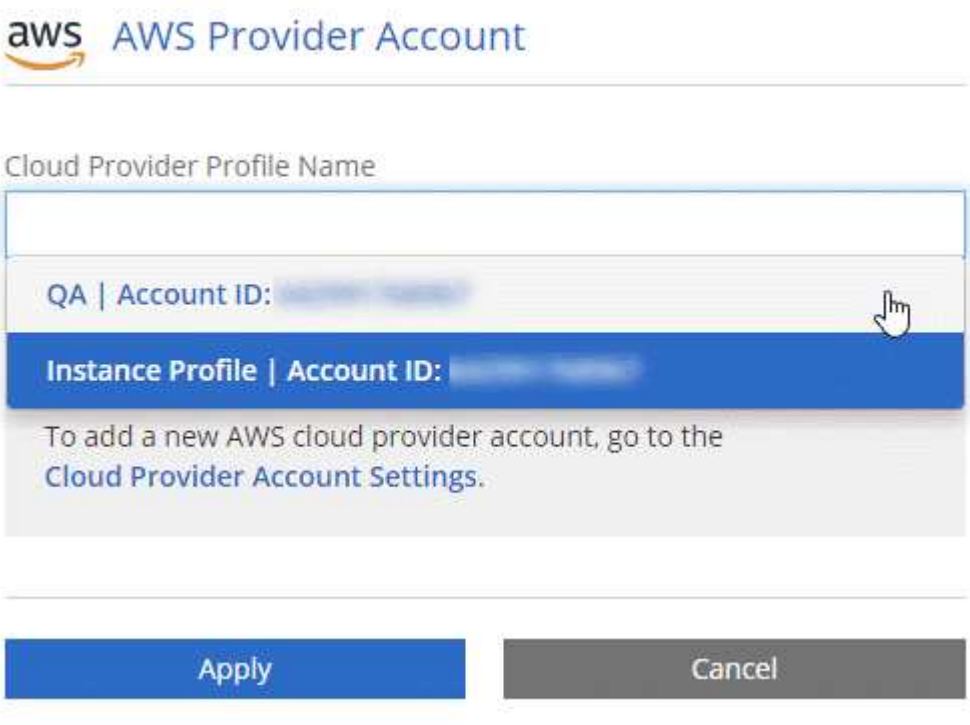
필요한 권한이 있는 AWS 계정을 제공한 후 Cloud Manager에 계정을 추가할 수 있습니다. 그러면 해당 계정에서 Cloud Volumes ONTAP 시스템을 시작할 수 있습니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 작업 드롭다운 목록을 클릭한 다음 * 계정 설정 * 을 선택합니다.
2. 새 계정 추가 * 를 클릭하고 * AWS * 를 선택합니다.
3. AWS 키를 제공할지 또는 신뢰할 수 있는 IAM 역할의 ARN을 제공할지 여부를 선택합니다.
4. 정책 요구 사항이 충족되었는지 확인한 다음 * 계정 생성 * 을 클릭합니다.

결과

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



Cloud Manager에 **Azure** 계정 설정 및 추가

다른 Azure 계정에 Cloud Volumes ONTAP를 배포하려는 경우 해당 계정에 필요한 권한을 제공한 다음 Cloud Manager에 계정에 대한 세부 정보를 추가해야 합니다.

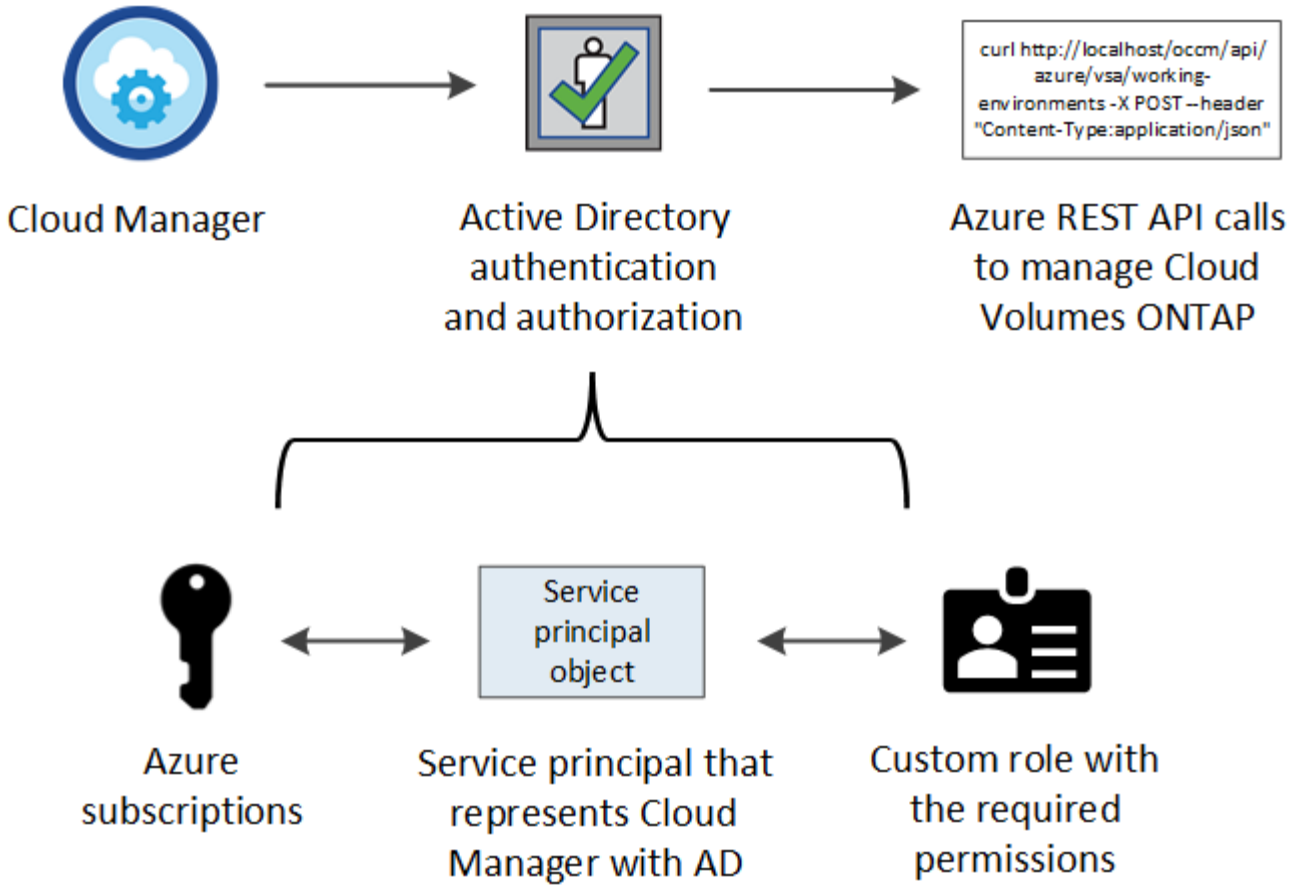
- 서비스 보안 주체를 사용하여 Azure 사용 권한 부여
- Cloud Manager에 Azure 계정 추가

서비스 보안 주체를 사용하여 **Azure** 사용 권한 부여

Cloud Manager는 Azure에서 작업을 수행할 수 있는 권한이 필요합니다. Azure Active Directory에서 서비스 보안 주체를 생성 및 설정하고 Cloud Manager에 필요한 Azure 자격 증명을 획득하여 Azure 계정에 필요한 권한을 부여할 수 있습니다.

이 작업에 대해

다음 그림에서는 Cloud Manager가 Azure에서 작업을 수행할 수 있는 권한을 얻는 방법을 보여 줍니다. 하나 이상의 Azure 구독에 연결된 서비스 보안 주체 개체는 Azure Active Directory의 Cloud Manager를 나타내며 필요한 권한을 허용하는 사용자 지정 역할에 할당됩니다.



다음 단계에서는 새로운 Azure 포털을 사용합니다. 문제가 발생하는 경우 Azure Classic 포털을 사용해야 합니다.

단계

1. 필요한 Cloud Manager 권한으로 사용자 지정 역할을 생성합니다.
2. Active Directory 서비스 보안 사용자를 생성합니다.
3. 사용자 지정 Cloud Manager 운영자 역할을 서비스 보안 주체에 할당합니다.

필요한 **Cloud Manager** 권한으로 사용자 지정 역할 생성

Azure에서 Cloud Volumes ONTAP를 시작 및 관리하는 데 필요한 권한을 클라우드 관리자에게 제공하려면 사용자 지정 역할이 필요합니다.

단계

1. 를 다운로드합니다 "Cloud Manager Azure 정책".
2. 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"
```

3. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 생성합니다.

   다음 예에서는 Azure CLI 2.0을 사용하여 사용자 지정 역할을 생성하는 방법을 보여 줍니다.

   ◦ az 역할 정의 create — 역할 정의 C:\Policy_for_cloud_Manager_Azure_3.6.1.json *

결과

이제 OnCommand 클라우드 관리자 운영자 라는 사용자 지정 역할을 갖게 됩니다.

Active Directory 서비스 보안 주체 만들기

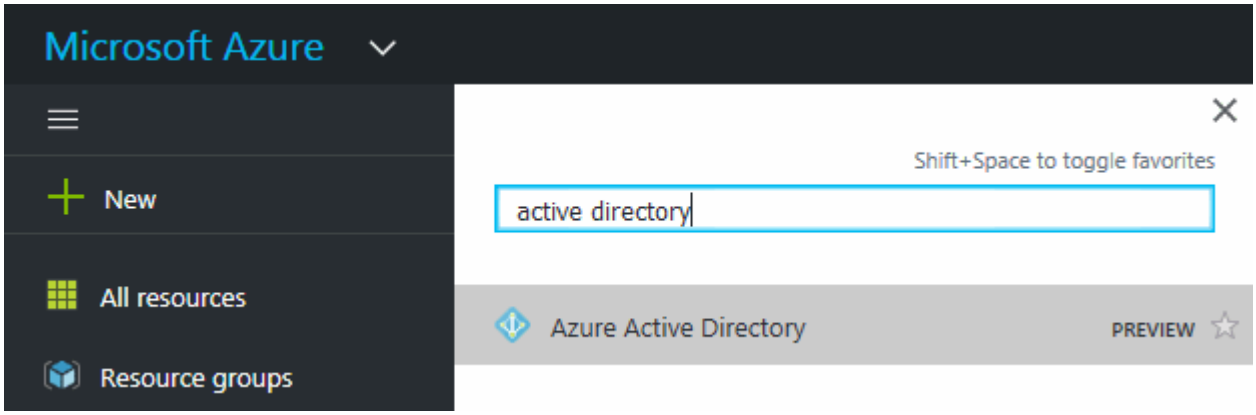
Cloud Manager가 Azure Active Directory로 인증할 수 있도록 Active Directory 서비스 보안 주체를 만들어야 합니다.

시작하기 전에

Active Directory 응용 프로그램을 만들고 응용 프로그램을 역할에 할당하려면 Azure에 적절한 권한이 있어야 합니다. 자세한 내용은 을 참조하십시오 "Microsoft Azure 설명서: 포털을 사용하여 리소스에 액세스할 수 있는 Active Directory 응용 프로그램 및 서비스 보안 주체를 만듭니다".

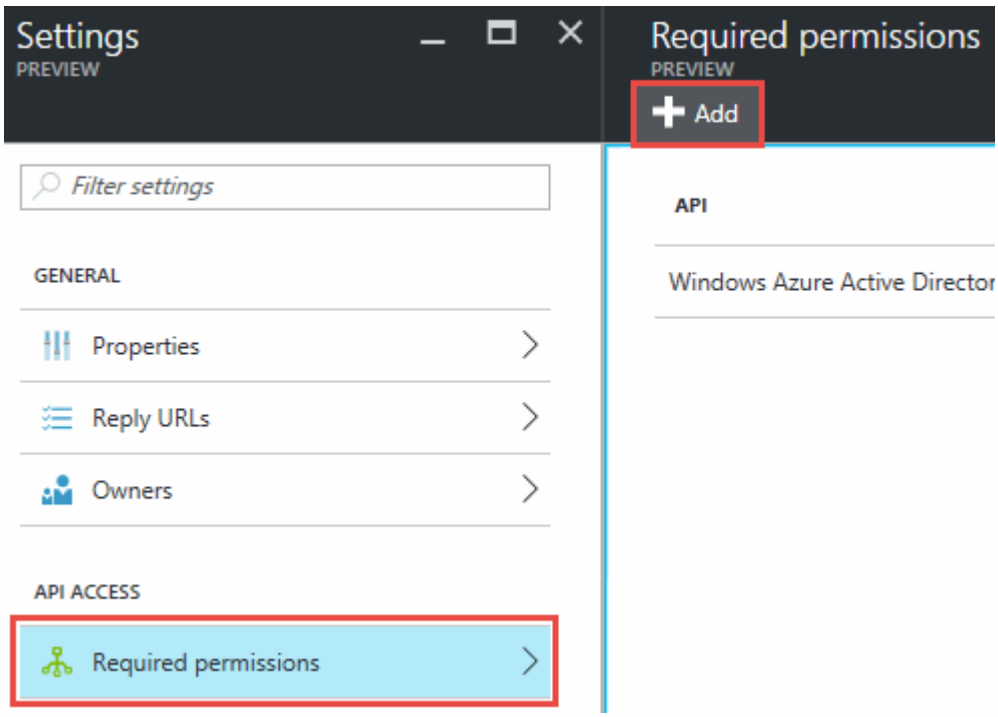
단계

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

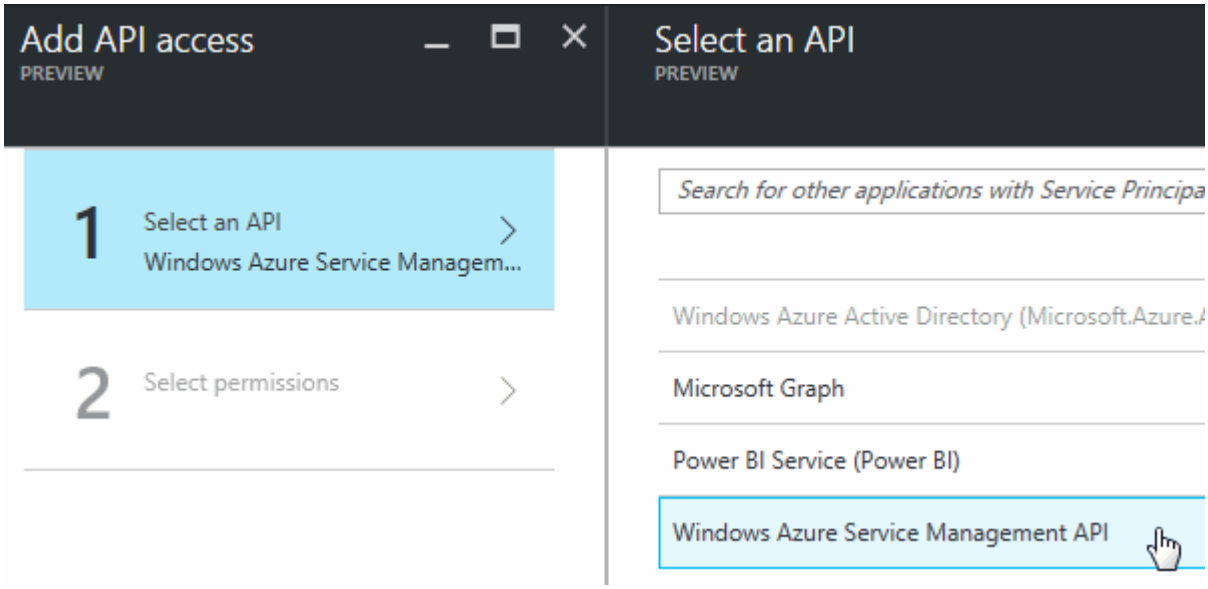


2. 메뉴에서 * 앱 등록(레거시) * 을 클릭합니다.
3. 서비스 보안 주체 만들기:
   a. 새 응용 프로그램 등록 * 을 클릭합니다.
   b. 응용 프로그램 이름을 입력하고 * Web App/API * 를 선택한 상태로 URL을 입력합니다(예: http://url
   c. Create * 를 클릭합니다.
4. 응용 프로그램을 수정하여 필요한 권한을 추가합니다.
   a. 생성된 애플리케이션을 선택합니다.

b. 설정에서 * 필요한 권한 * 을 클릭한 다음 * 추가 * 를 클릭합니다.



c. Select an API * 를 클릭하고 * Windows Azure Service Management API * 를 선택한 다음 * Select * 를 클릭합니다.



d. 조직 사용자로 Azure 서비스 관리 액세스 * 를 클릭하고 * 선택 * 을 클릭한 다음 * 완료 * 를 클릭합니다.

5. 서비스 보안 주체에 대한 키를 생성합니다.

a. 설정에서 * 키 * 를 클릭합니다.

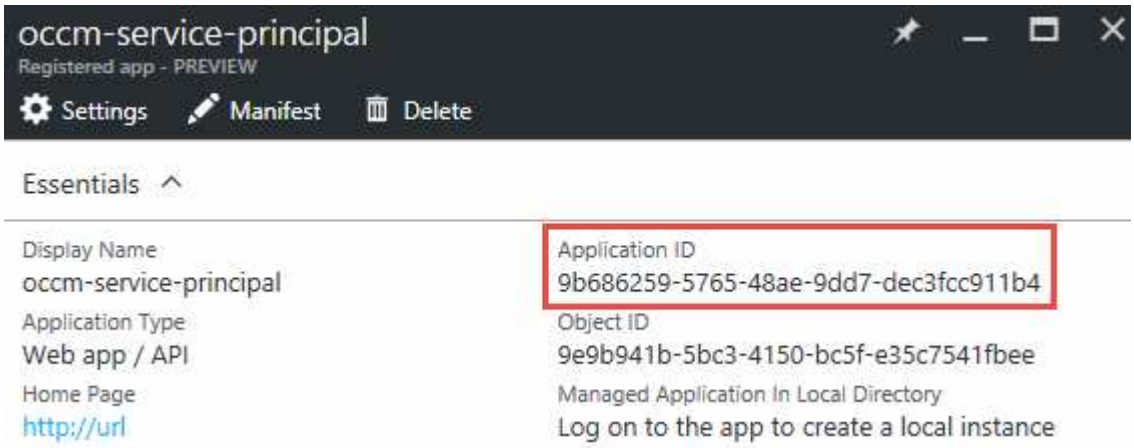
b. 설명을 입력하고 기간을 선택한 다음 * 저장 * 을 클릭합니다.

c. 키 값을 복사합니다.

클라우드 공급자 계정을 Cloud Manager에 추가할 때 키 값을 입력해야 합니다.

d. 속성 * 을 클릭한 다음 서비스 보안 주체에 대한 응용 프로그램 ID를 복사합니다.

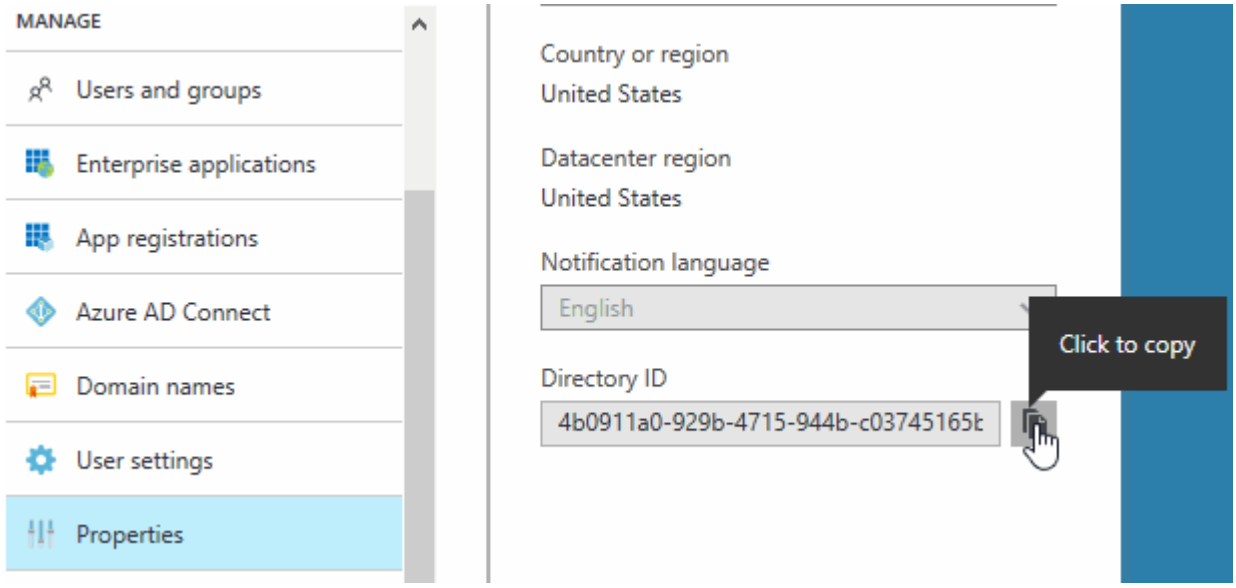
키 값과 마찬가지로, Cloud Manager에 클라우드 공급자 계정을 추가할 때 Cloud Manager에 애플리케이션 ID를 입력해야 합니다.



6. 조직의 Active Directory 테넌트 ID를 가져옵니다.

a. Active Directory 메뉴에서 * 속성 * 을 클릭합니다.

b. 디렉터리 ID를 복사합니다.



애플리케이션 ID 및 애플리케이션 키와 마찬가지로 클라우드 공급자 계정을 Cloud Manager에 추가할 때 Active Directory 테넌트 ID를 입력해야 합니다.

결과

이제 Active Directory 서비스 보안 주체가 있어야 하며 응용 프로그램 ID, 응용 프로그램 키 및 Active Directory 테넌트 ID를 복사해야 합니다. 클라우드 공급자 계정을 추가할 때는 Cloud Manager에 이 정보를 입력해야 합니다.

서비스 보안 주체에 **Cloud Manager** 운영자 역할 할당

서비스 보안 주체를 하나 이상의 Azure 구독에 바인딩하고 Cloud Manager 운영자 역할을 할당해야만 Cloud

Manager가 Azure에서 권한을 갖게 됩니다.

이 작업에 대해

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

단계

1. Azure 포털의 왼쪽 창에서 * 구독 * 을 선택합니다.
2. 구독을 선택합니다.
3. IAM(Access Control) * 을 클릭한 다음 * 추가 * 를 클릭합니다.
4. OnCommand 클라우드 관리자 운영자 * 역할을 선택하십시오.
5. 응용 프로그램의 이름을 검색합니다(스크롤하면 목록에서 찾을 수 없음).
6. 응용 프로그램을 선택하고 * 선택 * 을 클릭한 다음 * 확인 * 을 클릭합니다.

결과

이제 Cloud Manager의 서비스 보안 주체에 필요한 Azure 권한이 있습니다.

Cloud Manager에 **Azure** 계정 추가

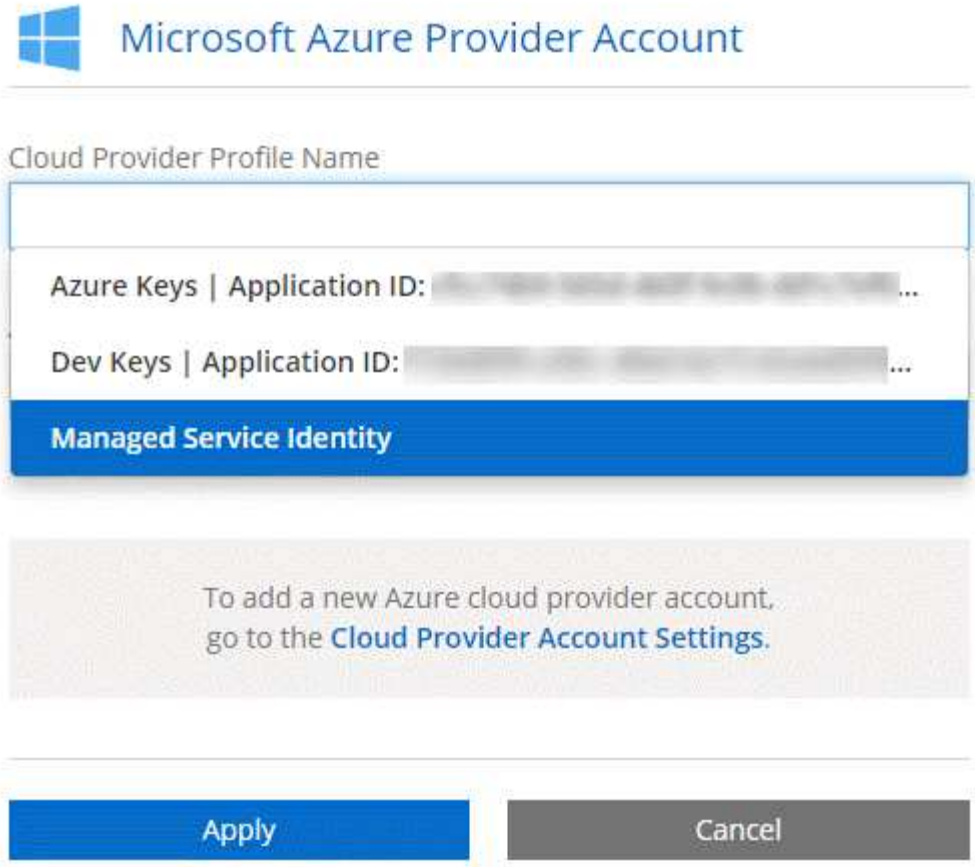
필요한 권한이 있는 Azure 계정을 제공한 후 Cloud Manager에 계정을 추가할 수 있습니다. 그러면 해당 계정에서 Cloud Volumes ONTAP 시스템을 시작할 수 있습니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 작업 드롭다운 목록을 클릭한 다음 * 계정 설정 * 을 선택합니다.
2. 새 계정 추가 * 를 클릭하고 * Microsoft Azure * 를 선택합니다.
3. 필요한 권한을 부여하는 Azure Active Directory 서비스 보안 주체에 대한 정보를 입력합니다.
4. 정책 요구 사항이 충족되었는지 확인한 다음 * 계정 생성 * 을 클릭합니다.

결과

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



관리되는 **ID**와 추가 **Azure** 구독을 연결합니다

Cloud Manager를 사용하면 Cloud Volumes ONTAP를 배포할 Azure 계정 및 구독을 선택할 수 있습니다. 를 연결하지 않으면 관리 ID 프로필에 대해 다른 Azure 구독을 선택할 수 없습니다 "관리 ID" 있습니다.

이 작업에 대해

관리 ID가 초기 ID입니다 "클라우드 공급자 계정입니다" NetApp Cloud Central에서 Cloud Manager를 구축할 때 Cloud Manager를 구축하면 Cloud Central에서 OnCommand Cloud Manager 운영자 역할을 생성하여 Cloud Manager 가상 머신에 할당합니다.

단계

1. Azure 포털에 로그인합니다.
2. Subscriptions * 서비스를 연 다음 Cloud Volumes ONTAP 시스템을 배포할 구독을 선택합니다.
3. IAM(액세스 제어) * 을 클릭합니다.
   a. Add * > * Add role assignment * 를 클릭한 후 권한을 추가합니다.
      - OnCommand 클라우드 관리자 운영자 * 역할을 선택하십시오.

        OnCommand Cloud Manager Operator는 에 제공되는 기본 이름입니다 "Cloud Manager 정책". 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

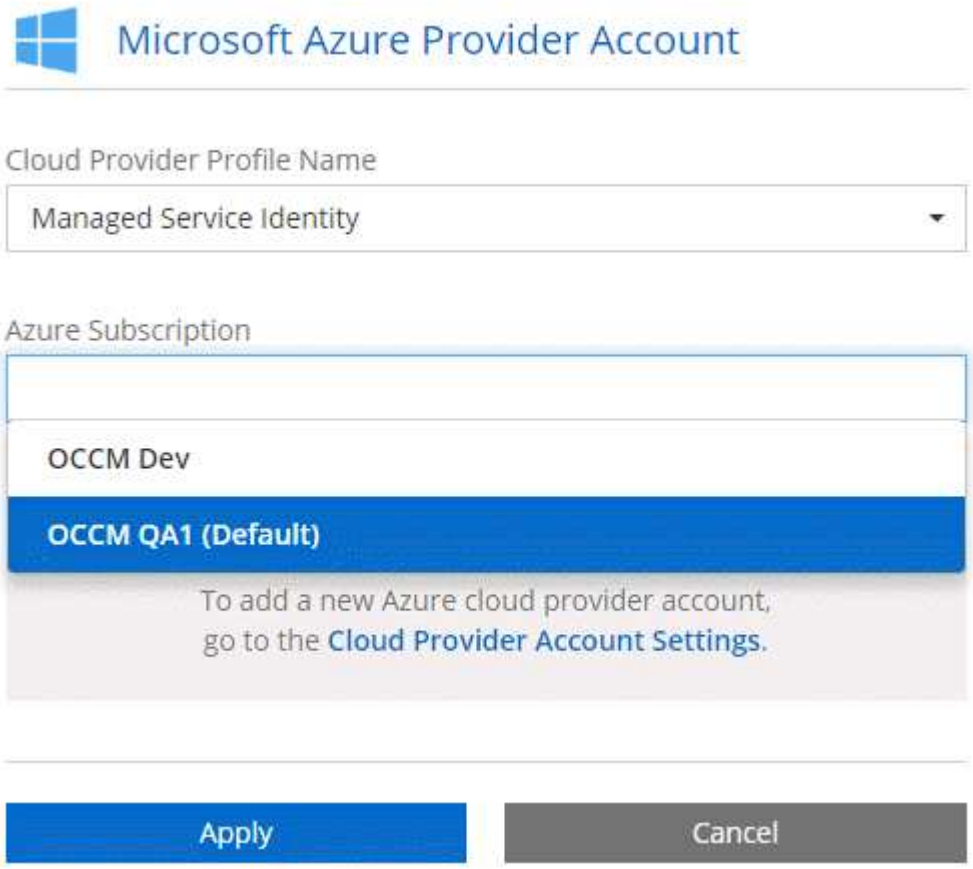
      - Virtual Machine * 에 대한 액세스 권한을 할당합니다.
      - Cloud Manager 가상 머신이 생성된 서브스크립션을 선택합니다.

- Cloud Manager 가상 머신을 선택합니다.
- 저장 * 을 클릭합니다.

4. 추가 구독에 대해 이 단계를 반복합니다.

결과

새 작업 환경을 만들 때 이제 관리되는 ID 프로필에 대해 여러 Azure 구독에서 선택할 수 있습니다.



Cloud Manager에 NetApp Support 사이트 계정 추가

BYOL 시스템을 구축하려면 NetApp Support 사이트 계정을 Cloud Manager에 추가해야 합니다. 또한 종량제 시스템을 등록하고 ONTAP 소프트웨어를 업그레이드해야 합니다.

다음 비디오에서 Cloud Manager에 NetApp Support 사이트 계정을 추가하는 방법을 알아보십시오. 또는 아래로 스크롤하여 단계를 읽습니다.

[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

단계

1. 아직 NetApp Support 사이트 계정이 없는 경우 "1인 등록".
2. Cloud Manager 콘솔의 오른쪽 위에서 작업 드롭다운 목록을 클릭한 다음 * 계정 설정 * 을 선택합니다.
3. 새 계정 추가 * 를 클릭하고 * NetApp Support 사이트 * 를 선택합니다.

4. 계정의 이름을 지정한 다음 사용자 이름과 암호를 입력합니다.
   - 계정은 고객 수준 계정이어야 합니다(게스트 또는 임시 계정이 아님).
   - BYOL 시스템을 구축하려는 경우:
     - 이 계정은 BYOL 시스템의 일련 번호에 액세스할 수 있는 권한이 있어야 합니다.
     - 안전한 BYOL 구독을 구입한 경우 보안 NSS 계정이 필요합니다.
5. 계정 만들기 * 를 클릭합니다

다음 단계

이제 사용자는 새 Cloud Volumes ONTAP 시스템을 생성할 때와 기존 시스템을 등록할 때 계정을 선택할 수 있습니다.

- "AWS에서 Cloud Volumes ONTAP 실행"
- "Azure에서 Cloud Volumes ONTAP 실행"
- "선불 종량제 시스템을 등록하는 중입니다"
- "Cloud Manager로 라이센스 파일을 관리하는 방법에 대해 알아보십시오"

보안 액세스를 위해 **HTTPS** 인증서 설치

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

단계

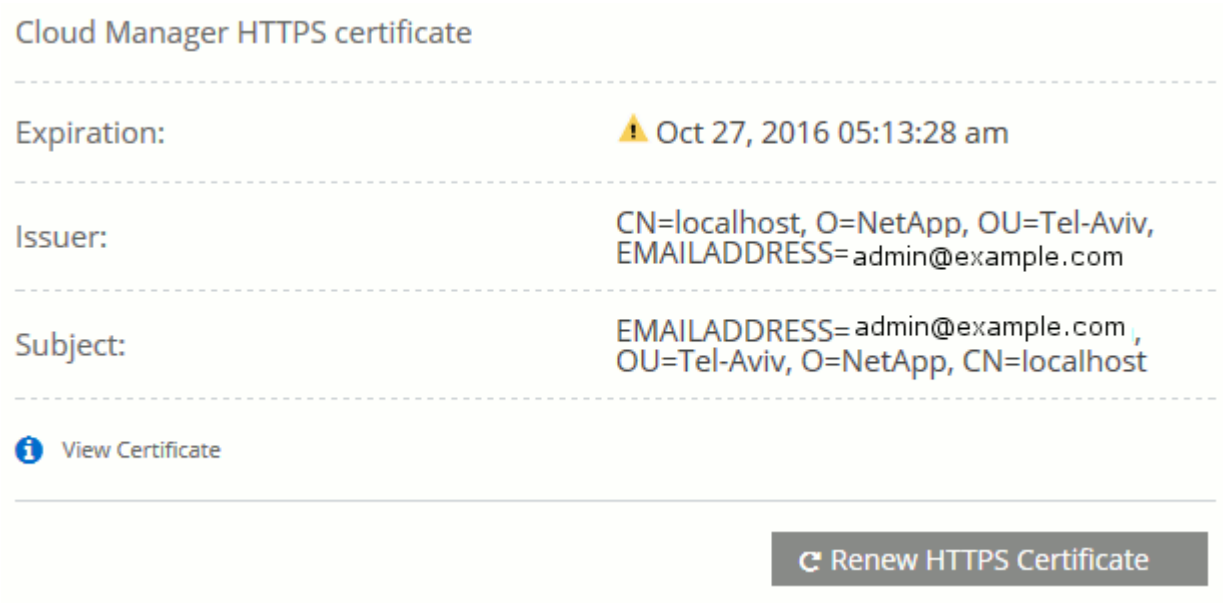
1. Cloud Manager 콘솔의 오른쪽 위에서 작업 드롭다운 목록을 클릭한 다음 * HTTPS 설정 * 을 선택합니다.
2. HTTPS 설정 페이지에서 인증서 서명 요청(CSR)을 생성하거나 고유한 CA 서명 인증서를 설치하여 인증서를 설치합니다.

옵션을 선택합니다	설명
CSR을 생성합니다	a. Cloud Manager 호스트(공통 이름)의 호스트 이름 또는 DNS를 입력한 다음 * CSR 생성 * 을 클릭합니다. Cloud Manager는 인증서 서명 요청을 표시합니다. b. CSR을 사용하여 CA에 SSL 인증서 요청을 제출합니다. 인증서는 PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식을 사용해야 합니다. c. 서명된 인증서의 내용을 복사하여 인증서 필드에 붙여 넣은 다음 * 설치 * 를 클릭합니다.

옵션을 선택합니다	설명
고유한 CA 서명 인증서를 설치합니다	a. CA 서명 인증서 설치 * 를 선택합니다. b. 인증서 파일과 개인 키를 모두 로드한 다음 * 설치 * 를 클릭합니다. 인증서는 PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식을 사용해야 합니다.

결과

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



사용자 및 테넌트 설정

Cloud Manager를 사용하면 Cloud Manager에 Cloud Central 사용자를 추가하고 테넌트를 사용하여 작업 환경을 격리할 수 있습니다.

Cloud Manager에 사용자 추가

추가 사용자가 Cloud Manager 시스템을 사용해야 하는 경우 NetApp Cloud Central에서 계정을 등록해야 합니다. 그런 다음 Cloud Manager에 사용자를 추가할 수 있습니다.

단계

1. 아직 NetApp Cloud Central에 계정이 없는 경우 Cloud Manager 시스템에 대한 링크를 보내 등록하도록 하십시오.

   사용자가 계정 등록을 확인할 때까지 기다립니다.

2. Cloud Manager에서 사용자 아이콘을 클릭한 다음 * 사용자 보기 * 를 클릭합니다.
3. 새 사용자 * 를 클릭합니다.

4. 사용자 계정과 연결된 이메일 주소를 입력하고 역할을 선택한 다음 * 추가 * 를 클릭합니다.

다음 단계

이제 Cloud Manager 시스템에 로그인할 수 있다고 알려줍니다.

테넌트 생성

테넌트를 사용하면 작업 환경을 별도의 그룹으로 격리할 수 있습니다. 테넌트 내에서 하나 이상의 작업 환경을 생성합니다. "테넌트에 대해 자세히 알아보십시오".

단계

1. 테넌트 아이콘을 클릭한 다음 * 테넌트 추가 * 를 클릭합니다.

2. 필요한 경우 이름, 설명 및 비용 센터를 입력합니다.
3. 저장 * 을 클릭합니다.

다음 단계

이제 이 새 테넌트로 전환하고 테넌트 관리자 및 작업 환경 관리자를 이 테넌트에 추가할 수 있습니다.

AWS KMS 설정

Cloud Volumes ONTAP에서 Amazon 암호화를 사용하려면 AWS KMS(키 관리 서비스)를 설정해야 합니다.

단계

1. 활성 CMK(Customer Master Key)가 있는지 확인합니다.

   CMK는 AWS로 관리되는 CMK 또는 고객이 관리하는 CMK가 될 수 있습니다. Cloud Manager 및 Cloud Volumes ONTAP와 동일한 AWS 계정 또는 다른 AWS 계정에 있을 수 있습니다.

   "AWS 설명서:CMK(Customer Master Key)"

2. Cloud Manager에 권한을 제공하는 IAM 역할을 _KEY USER_로 추가하여 각 CMK에 대한 키 정책을 수정합니다.

IAM 역할을 주요 사용자로 추가하면 Cloud Manager에서 Cloud Volumes ONTAP와 함께 CMK를 사용할 수 있는 권한이 부여됩니다.

"AWS 설명서:키 편집"

3. CMK가 다른 AWS 계정에 있는 경우 다음 단계를 수행하십시오.

   a. CMK가 상주하는 계정에서 KMS 콘솔로 이동합니다.

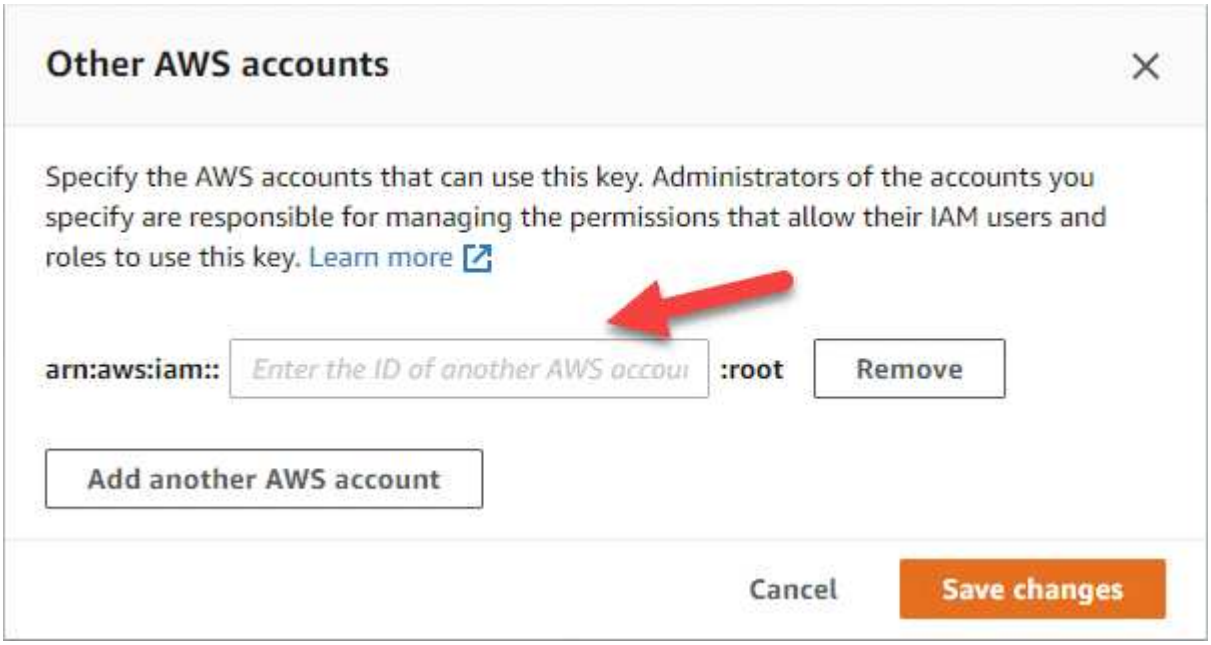
   b. 키를 선택합니다.

   c. General configuration * 창에서 키의 ARN을 복사합니다.

      Cloud Volumes ONTAP 시스템을 생성할 때 클라우드 관리자에게 ARN을 제공해야 합니다.

   d. 다른 AWS 계정 * 창에서 Cloud Manager에 사용 권한을 제공하는 AWS 계정을 추가합니다.

      대부분의 경우 Cloud Manager가 상주하는 계정입니다. Cloud Manager가 AWS에 설치되어 있지 않으면, Cloud Manager에 AWS 액세스 키를 제공한 계정이 될 수 있습니다.



   e. 이제 Cloud Manager에 사용 권한을 제공하는 AWS 계정으로 전환하고 IAM 콘솔을 엽니다.

   f. 아래에 나열된 권한을 포함하는 IAM 정책을 생성합니다.

   g. Cloud Manager에 권한을 제공하는 IAM 역할 또는 IAM 사용자에 정책을 연결합니다.

      다음 정책은 Cloud Manager가 외부 AWS 계정에서 CMK를 사용하는 데 필요한 권한을 제공합니다. "리소스"

섹션에서 지역 및 계정 ID를 수정해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
이 프로세스에 대한 자세한 내용은 을 참조하십시오 "AWS 설명서: CMK에 외부 AWS 계정 액세스 허용".

네트워킹 요구 사항

Cloud Manager의 네트워킹 요구사항

Cloud Manager가 AWS 또는 Microsoft Azure에 Cloud Volumes ONTAP 시스템을 구축할 수 있도록 네트워킹을 설정해야 합니다. 가장 중요한 단계는 다양한 엔드포인트에 대한 아웃바운드 인터넷 액세스를 보장하는 것입니다.

네트워크에서 인터넷에 대한 모든 통신에 프록시 서버를 사용하는 경우 Cloud Manager에서 설정 중에 프록시를 지정하라는 메시지를 표시합니다. 설정 페이지에서 프록시 서버를 지정할 수도 있습니다. 을 참조하십시오 "프록시 서버를 사용하도록 Cloud Manager 구성".

대상 네트워크에 연결

Cloud Manager를 사용하려면 Cloud Volumes ONTAP를 구축할 AWS VPC 및 Azure VNets에 대한 네트워크 연결이 필요합니다.

예를 들어, 회사 네트워크에 Cloud Manager를 설치하는 경우 Cloud Volumes ONTAP를 실행하는 AWS VPC 또는 Azure VNET에 대한 VPN 연결을 설정해야 합니다.

아웃바운드 인터넷 액세스

Cloud Manager는 Cloud Volumes ONTAP를 배포 및 관리하기 위해 아웃바운드 인터넷 액세스를 필요로 합니다. 웹 브라우저에서 Cloud Manager에 액세스하고 Linux 호스트에서 Cloud Manager 설치 프로그램을 실행할 때도 아웃바운드 인터넷 액세스가 필요합니다.

다음 섹션에서는 특정 끝점을 식별합니다.

AWS에서 Cloud Volumes ONTAP를 관리하기 위한 아웃바운드 인터넷 액세스

AWS에서 Cloud Volumes ONTAP를 구축 및 관리할 때 Cloud Manager에서 다음 엔드포인트에 액세스하려면 아웃바운드 인터넷 액세스가 필요합니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • CloudFormation 을 참조하십시오 • EC2(탄력적인 컴퓨팅 클라우드) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • S3(Simple Storage Service) 정확한 끝점은 Cloud Volumes ONTAP를 배포하는 지역에 따라 다릅니다. "자세한 내용은 AWS 설명서를 참조하십시오."	Cloud Manager를 사용하여 AWS에서 Cloud Volumes ONTAP를 구축 및 관리할 수 있습니다.
https://api.services.cloud.netapp.com:443 으로 문의하십시오	NetApp Cloud Central에 API 요청

엔드포인트	목적
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com 으로 문의하십시오	소프트웨어 이미지, 매니페스트 및 템플릿에 대한 액세스를 제공합니다.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com 으로 문의하십시오	Cloud Manager에서 매니페스트, 템플릿 및 Cloud Volumes ONTAP 업그레이드 이미지에 액세스하고 다운로드할 수 있습니다.
https://kinesis.us-east-1.amazonaws.com 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.
https://cloudmanager.cloud.netapp.com 으로 문의하십시오	Cloud Central 계정을 포함한 Cloud Manager 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com 으로 문의하십시오	NetApp Cloud Central과 통신하여 중앙 집중식 사용자 인증 제공
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup 으로 문의하십시오	NetApp AutoSupport과 커뮤니케이션:
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement 으로 문의하십시오	라이센싱 및 지원 등록에 대해 NetApp과 커뮤니케이션
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ 으로 문의하십시오	Cloud Volumes ONTAP 시스템을 Kubernetes 클러스터에 연결하는 데 필요합니다. 엔드포인트를 통해 NetApp Trident를 설치할 수 있습니다.
다음과 같은 다양한 타사 위치: • https://repo1.maven.org/maven2 으로 문의하십시오 • https://oss.sonatype.org/content/repositories 으로 문의하십시오 • https://repo.typesafe.org 으로 문의하십시오 타사 위치는 변경될 수 있습니다.	업그레이드하는 동안 Cloud Manager는 타사 종속성을 위한 최신 패키지를 다운로드합니다.

Azure에서 **Cloud Volumes ONTAP**를 관리하기 위한 아웃바운드 인터넷 액세스

Microsoft Azure에서 Cloud Volumes ONTAP를 배포 및 관리할 때 Cloud Manager는 다음 엔드포인트에 연락할 수 있는 아웃바운드 인터넷 액세스를 필요로 합니다.

엔드포인트	목적
https://management.azure.com https://login.microsoftonline.com 으로 문의하십시오	Cloud Manager를 사용하면 대부분의 Azure 지역에서 Cloud Volumes ONTAP를 구축 및 관리할 수 있습니다.
https://management.microsoftazure.de https://login.microsoftonline.de 으로 문의하십시오	Cloud Manager를 사용하여 Azure 독일 지역에서 Cloud Volumes ONTAP를 구축 및 관리할 수 있습니다.

엔드포인트	목적
https://management.usgovcloudapi.net https://login.microsoftonline.com 으로 문의하십시오	Cloud Manager를 사용하여 Azure US Gov 지역에 Cloud Volumes ONTAP를 배포하고 관리할 수 있습니다.
https://api.services.cloud.netapp.com:443 으로 문의하십시오	NetApp Cloud Central에 API 요청
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com 으로 문의하십시오	소프트웨어 이미지, 매니페스트 및 템플릿에 대한 액세스를 제공합니다.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com 를 참조하십시오	Cloud Manager에서 매니페스트, 템플릿 및 Cloud Volumes ONTAP 업그레이드 이미지에 액세스하고 다운로드할 수 있습니다.
https://kinesis.us-east-1.amazonaws.com 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.
https://netapp-cloud-account.auth0.com 으로 문의하십시오	NetApp Cloud Central과 통신하여 중앙 집중식 사용자 인증 제공
https://mysupport.netapp.com 으로 문의하십시오	NetApp AutoSupport과 커뮤니케이션:
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement 으로 문의하십시오	라이센싱 및 지원 등록에 대해 NetApp과 커뮤니케이션
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ 으로 문의하십시오	Cloud Volumes ONTAP 시스템을 Kubernetes 클러스터에 연결하는 데 필요합니다. 엔드포인트를 통해 NetApp Trident를 설치할 수 있습니다.
다음과 같은 다양한 타사 위치: • https://repo1.maven.org/maven2 으로 문의하십시오 • https://oss.sonatype.org/content/repositories 으로 문의하십시오 • https://repo.typesafe.org 으로 문의하십시오 타사 위치는 변경될 수 있습니다.	업그레이드하는 동안 Cloud Manager는 타사 종속성을 위한 최신 패키지를 다운로드합니다.

웹 브라우저에서 아웃바운드 인터넷 액세스

사용자는 웹 브라우저에서 Cloud Manager에 액세스해야 합니다. 웹 브라우저를 실행하는 컴퓨터는 다음 끝점에 연결되어 있어야 합니다.

엔드포인트	목적
Cloud Manager 호스트	Cloud Manager 콘솔을 로드하려면 웹 브라우저에서 호스트의 IP 주소를 입력해야 합니다. 클라우드 공급자에 대한 연결에 따라 호스트에 할당된 프라이빗 IP 또는 공용 IP를 사용할 수 있습니다. • 개인 IP는 VPN이 있고 가상 네트워크에 직접 연결할 수 있는 경우 작동합니다 • 공용 IP는 모든 네트워킹 시나리오에서 작동합니다 어떤 경우든 보안 그룹 규칙이 승인된 IP 또는 서브넷에서의 액세스만 허용하도록 하여 네트워크 액세스를 보호해야 합니다.
https://auth0.com\https://cdn.auth0.com\https://netapp-cloud-account.auth0.com\https://services.cloud.netapp.com	웹 브라우저는 NetApp Cloud Central을 통해 중앙 집중식 사용자 인증을 위해 이러한 엔드포인트에 연결됩니다.
https://widget.intercom.io 으로 문의하십시오	제품 내에서 NetApp 클라우드 전문가와 상담할 수 있는 채팅을 제공합니다.

Linux 호스트에 **Cloud Manager**를 설치하기 위한 아웃바운드 인터넷 액세스

설치 프로세스 중에 Cloud Manager 설치 관리자가 다음 URL에 액세스해야 합니다.

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm 으로 문의하십시오
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm 으로 문의하십시오
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip 으로 문의하십시오

포트 및 보안 그룹

- Cloud Central 또는 마켓플레이스 이미지에서 Cloud Manager를 배포하는 경우 다음을 참조하십시오.
  - "AWS의 Cloud Manager에 대한 보안 그룹 규칙"
  - "Azure의 Cloud Manager에 대한 보안 그룹 규칙"
- 기존 Linux 호스트에 Cloud Manager를 설치하는 경우 를 참조하십시오 "Cloud Manager 호스트 요구사항".

AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항

Cloud Volumes ONTAP 시스템이 올바르게 작동할 수 있도록 AWS 네트워킹을 설정합니다.

Cloud Manager에 액세스해야 하는 엔드포인트 목록을 찾고 계십니까? 이제 단일 위치에서 유지 관리됩니다. "자세한 내용을 보려면 여기를 클릭하십시오".

Cloud Volumes ONTAP의 일반적인 AWS 네트워킹 요구사항

AWS에서 다음 요구사항을 충족해야 합니다.

Cloud Volumes ONTAP 노드에 대한 아웃바운드 인터넷 액세스

Cloud Volumes ONTAP 노드를 사용하려면 스토리지 상태를 사전에 모니터링하는 NetApp AutoSupport에 메시지를 보내기 위해 아웃바운드 인터넷 액세스가 필요합니다.

라우팅 및 방화벽 정책은 Cloud Volumes ONTAP가 AutoSupport 메시지를 전송할 수 있도록 다음 엔드포인트로 AWS HTTP/HTTPS 트래픽을 허용해야 합니다.

- https://support.netapp.com/aods/asupmessage 으로 문의하십시오
- https://support.netapp.com/asupprod/post/1.0/postAsup 으로 문의하십시오

NAT 인스턴스가 있는 경우 개인 서브넷에서 인터넷으로 HTTPS 트래픽을 허용하는 인바운드 보안 그룹 규칙을 정의해야 합니다.

HA 중재자를 위한 아웃바운드 인터넷 액세스

HA 중재자 인스턴스는 스토리지 페일오버를 지원할 수 있도록 AWS EC2 서비스에 대한 아웃바운드 연결이 있어야 합니다. 연결을 제공하기 위해 공용 IP 주소를 추가하거나 프록시 서버를 지정하거나 수동 옵션을 사용할 수 있습니다.

수동 옵션은 대상 서브넷에서 AWS EC2 서비스로 연결되는 NAT 게이트웨이 또는 인터페이스 VPC 엔드포인트일 수 있습니다. VPC 엔드포인트에 대한 자세한 내용은 을 참조하십시오 "AWS 문서:인터페이스 VPC 엔드포인트(AWS PrivateLink)".

보안 그룹

Cloud Manager에서 보안 그룹을 생성할 수 있으므로 보안 그룹을 생성할 필요가 없습니다. 직접 사용해야 하는 경우 을 참조하십시오 "보안 그룹 규칙".

데이터 계층화를 위해 Cloud Volumes ONTAP에서 AWS S3로 연결

EBS를 성능 계층으로 사용하고 AWS S3를 용량 계층으로 사용하려면 Cloud Volumes ONTAP이 S3에 연결되어 있는지 확인해야 합니다. 이 연결을 제공하는 가장 좋은 방법은 S3 서비스에 VPC 엔드포인트를 생성하는 것입니다. 자세한 내용은 을 참조하십시오 "AWS 설명서: 게이트웨이 엔드포인트 생성".

VPC 끝점을 만들 때 Cloud Volumes ONTAP 인스턴스에 해당하는 영역, VPC 및 라우팅 테이블을 선택해야 합니다. 또한 S3 엔드포인트에 대한 트래픽을 활성화하는 아웃바운드 HTTPS 규칙을 추가하려면 보안 그룹을 수정해야 합니다. 그렇지 않으면 Cloud Volumes ONTAP에서 S3 서비스에 연결할 수 없습니다.

문제가 발생하면 을 참조하십시오 "AWS 지원 지식 센터: 게이트웨이 VPC 엔드포인트를 사용하여 S3 버킷에 연결할 수 없는 이유는 무엇입니까?"

다른 네트워크의 ONTAP 시스템에 대한 연결

AWS의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 AWS VPC와 다른 네트워크(예: Azure VNET 또는 회사 네트워크) 간에 VPN 연결이 있어야 합니다. 자세한 내용은 을 참조하십시오 "AWS 설명서: AWS VPN 연결 설정".

CIFS용 DNS 및 Active Directory

CIFS 스토리지를 프로비저닝하려면 AWS에서 DNS 및 Active Directory를 설정하거나 사내 설정을 AWS로 확장해야 합니다.

DNS 서버는 Active Directory 환경에 대한 이름 확인 서비스를 제공해야 합니다. Active Directory 환경에서 사용되는 DNS 서버가 아니어야 하는 기본 EC2 DNS 서버를 사용하도록 DHCP 옵션 집합을 구성할 수 있습니다.

자세한 지침은 을 참조하십시오 "AWS 설명서: AWS 클라우드의 Active Directory 도메인 서비스 빠른 시작 참조 구축".

여러 **AZs**에서 **Cloud Volumes ONTAP HA**를 위한 **AWS** 네트워킹 요구사항

추가 AWS 네트워킹 요구사항은 ZS(Multiple Availability Zones)를 사용하는 Cloud Volumes ONTAP HA 구성에 적용됩니다. Cloud Manager에 네트워킹 세부 정보를 입력해야 하므로 HA 쌍을 실행하기 전에 이러한 요구사항을 검토해야 합니다.

HA 쌍의 작동 방식을 이해하려면 를 참조하십시오 "고가용성 쌍".

가용성 영역

이 HA 구축 모델은 여러 대의 AZs를 사용하여 데이터의 고가용성을 보장합니다. 각 Cloud Volumes ONTAP 인스턴스와 중재자 인스턴스에 전용 AZ를 사용해야 하며 HA 쌍 간의 통신 채널을 제공합니다.

NAS 데이터 및 클러스터**/SVM** 관리를 위한 부동 **IP** 주소

여러 AZs의 HA 구성에서는 장애가 발생할 경우 노드 간에 이동하는 부동 IP 주소를 사용합니다. 고객이 아니라면 VPC 외부에서 기본적으로 액세스할 수 없습니다 "AWS 전송 게이트웨이를 설정합니다".

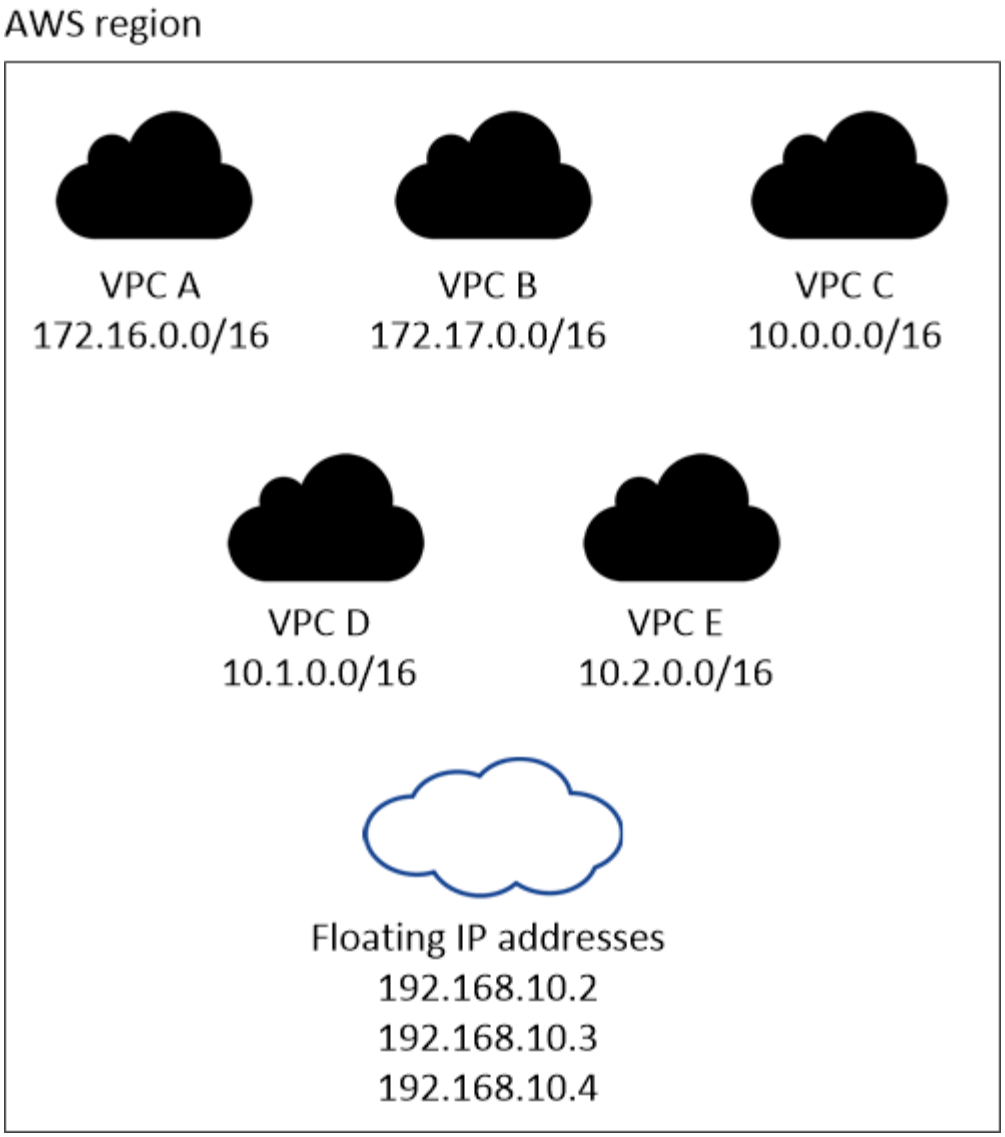
하나의 부동 IP 주소는 클러스터 관리용, 하나는 노드 1의 NFS/CIFS 데이터용으로, 다른 하나는 노드 2의 NFS/CIFS 데이터용으로 사용됩니다. SVM 관리를 위한 네 번째 유동 IP 주소는 선택 사항입니다.

Windows용 SnapDrive 또는 HA 쌍을 지원하는 SnapCenter를 사용하는 경우 SVM 관리 LIF에는 부동 IP 주소가 필요합니다. 시스템을 구축할 때 IP 주소를 지정하지 않으면 나중에 LIF를 생성할 수 있습니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP 설정".

Cloud Volumes ONTAP HA 작업 환경을 생성할 때 Cloud Manager에 부동 IP 주소를 입력해야 합니다. Cloud Manager는 시스템을 시작할 때 HA 쌍에 IP 주소를 할당합니다.

부동 IP 주소는 HA 구성을 배포하는 AWS 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 유동 IP 주소를 해당 지역의 VPC 외부에 있는 논리적 서브넷으로 생각해 보십시오.

다음 예에서는 AWS 영역에 있는 VPC와 유동 IP 주소 간의 관계를 보여 줍니다. 부동 IP 주소는 모든 VPC에 대한 CIDR 블록 외부에 있지만 라우팅 테이블을 통해 서브넷으로 라우팅할 수 있습니다.



Cloud Manager는 VPC 외부의 클라이언트에서 iSCSI 액세스 및 NAS 액세스를 위한 정적 IP 주소를 자동으로 생성합니다. 이러한 유형의 IP 주소에 대한 요구 사항을 충족할 필요는 없습니다.

VPC 외부에서 유동 **IP** 액세스를 지원하는 전송 게이트웨이

"AWS 전송 게이트웨이를 설정합니다" HA 쌍이 상주하는 VPC 외부에서 HA 쌍의 부동 IP 주소에 액세스할 수 있도록 합니다.

배관 테이블

Cloud Manager에서 부동 IP 주소를 지정한 후 부동 IP 주소에 대한 라우트를 포함해야 하는 라우팅 테이블을 선택해야 합니다. 이렇게 하면 클라이언트가 HA 쌍에 액세스할 수 있습니다.

VPC(기본 경로 테이블)에 있는 서브넷에 대해 하나의 라우팅 테이블만 있는 경우 Cloud Manager는 해당 라우팅 테이블에 부동 IP 주소를 자동으로 추가합니다. 둘 이상의 라우트 테이블이 있는 경우 HA 쌍을 시작할 때 올바른 라우트 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP에 액세스하지 못할 수 있습니다.

예를 들어, 서로 다른 라우팅 테이블에 연결된 두 개의 서브넷이 있을 수 있습니다. 라우트 테이블 A를 선택했지만 라우트 테이블 B는 선택하지 않은 경우, 라우트 테이블 A와 연결된 서브넷에 있는 클라이언트는 HA 쌍에 액세스할 수 있지만, 라우트 테이블 B와 연결된 서브넷에 있는 클라이언트는 액세스할 수 없습니다.

라우팅 테이블에 대한 자세한 내용은 을 참조하십시오 "AWS 설명서: 경로 테이블".

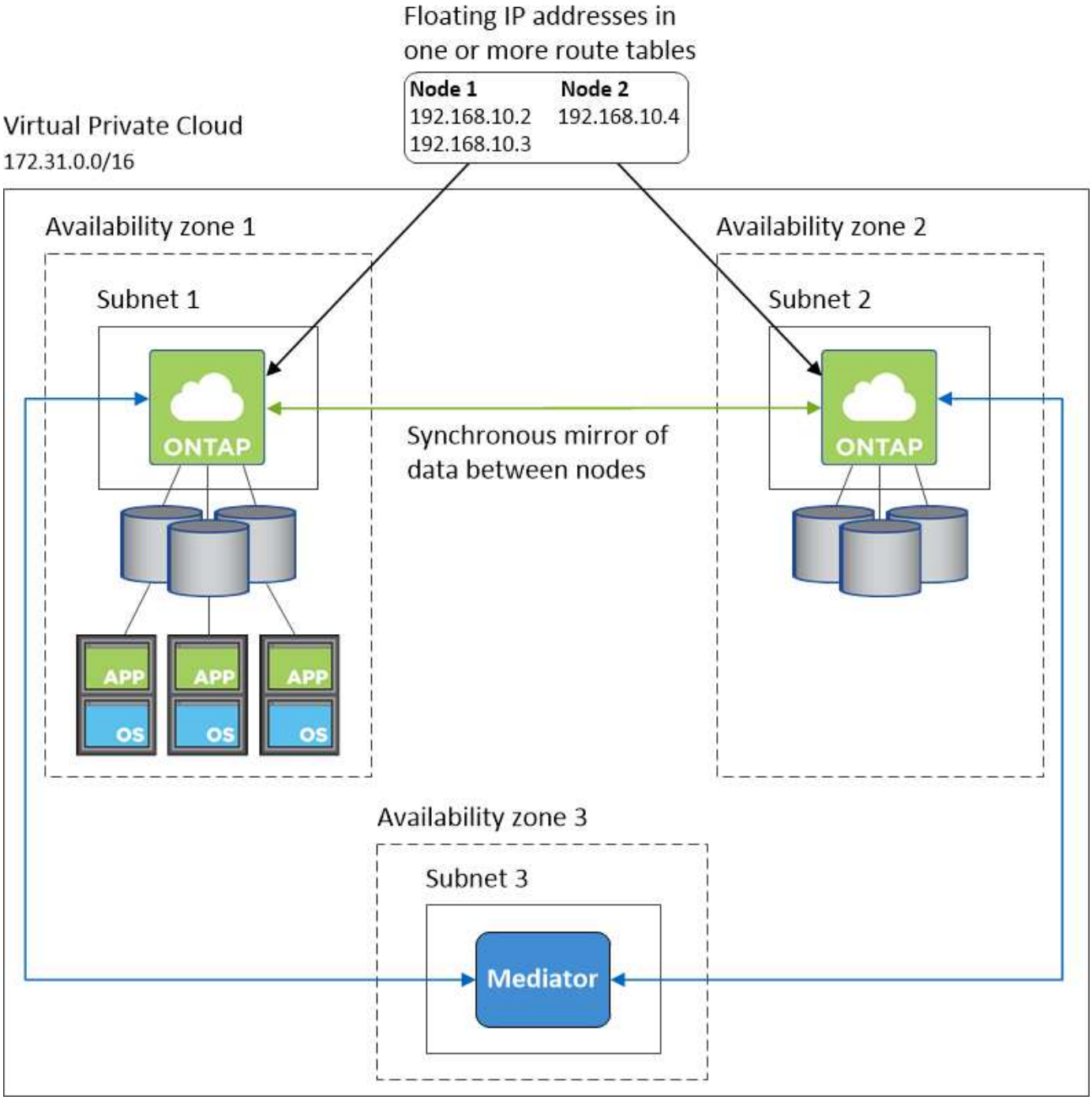
NetApp 관리 툴에 연결

여러 AZs에 있는 HA 구성에서 NetApp 관리 툴을 사용하려면 다음 두 가지 연결 옵션을 사용할 수 있습니다.

1. NetApp 관리 툴을 다른 VPC 및 에 구축할 수 있습니다 "AWS 전송 게이트웨이를 설정합니다". 게이트웨이를 사용하면 VPC 외부에서 클러스터 관리 인터페이스의 부동 IP 주소에 액세스할 수 있습니다.
2. NAS 클라이언트와 비슷한 라우팅 구성을 사용하여 동일한 VPC에 NetApp 관리 툴을 구축합니다.

구성의 예

다음 이미지는 액티브-패시브 구성으로 작동하는 AWS의 최적의 HA 구성을 보여줍니다.



VPC 구성의 예

AWS에서 Cloud Manager 및 Cloud Volumes ONTAP를 구축하는 방법을 자세히 알아보려면 가장 일반적인 VPC 구성을 검토해야 합니다.

- 공용 및 전용 서브넷과 NAT 장치가 있는 VPC입니다
- 개인 서브넷과 네트워크에 대한 VPN 연결을 지원하는 VPC입니다

공용 및 전용 서브넷과 **NAT** 장치가 있는 **VPC**입니다

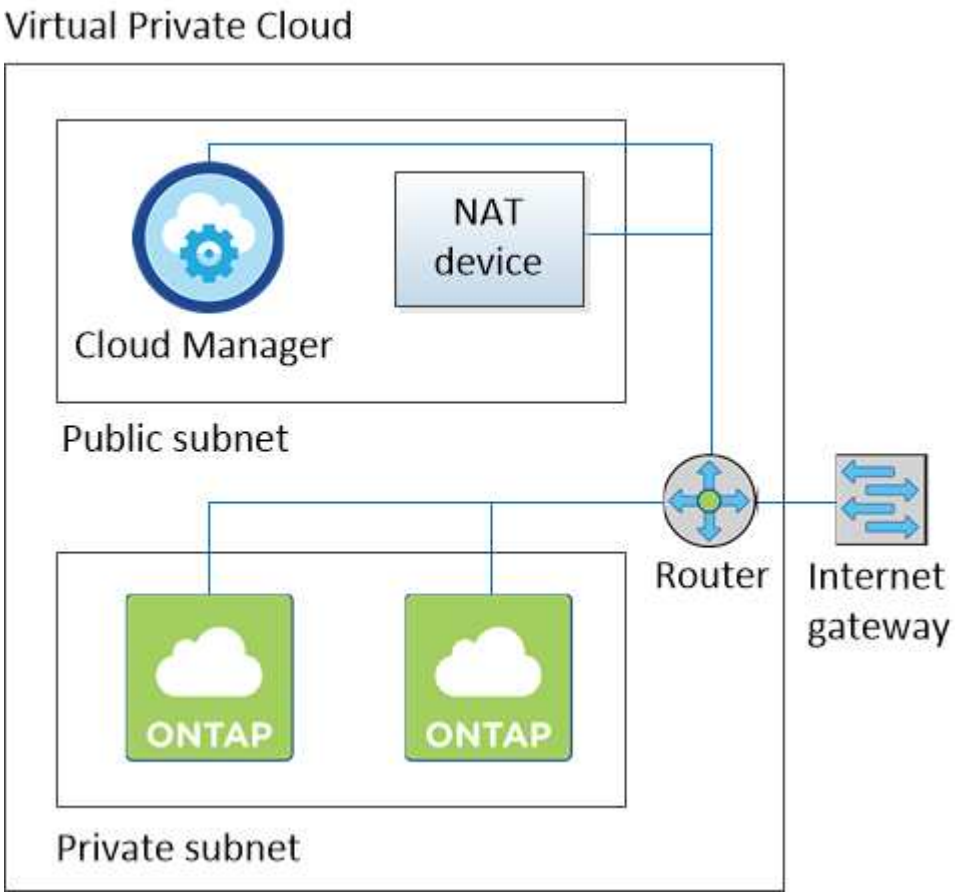
이 VPC 구성에는 공용 및 전용 서브넷, VPC를 인터넷에 연결하는 인터넷 게이트웨이, 사설 서브넷의 아웃바운드 인터넷 트래픽을 지원하는 공용 서브넷의 NAT 게이트웨이 또는 NAT 인스턴스가 포함됩니다. 이 구성에서는 퍼블릭

서브넷 또는 프라이빗 서브넷에서 Cloud Manager를 실행할 수 있지만, VPC 외부의 호스트에서 액세스할 수 있기 때문에 퍼블릭 서브넷을 사용하는 것이 좋습니다. 그런 다음 전용 서브넷에서 Cloud Volumes ONTAP 인스턴스를 시작할 수 있습니다.

NAT 장치 대신 HTTP 프록시를 사용하여 인터넷 연결을 제공할 수 있습니다.

이 시나리오에 대한 자세한 내용은 을 참조하십시오 "AWS 문서:시나리오 2: 공용 및 사설 서브넷(NAT)이 있는 VPC".

다음 그림에서는 공용 서브넷에서 실행되는 Cloud Manager와 프라이빗 서브넷에서 실행되는 단일 노드 시스템을 보여 줍니다.



개인 서브넷과 네트워크에 대한 **VPN** 연결을 지원하는 **VPC**입니다

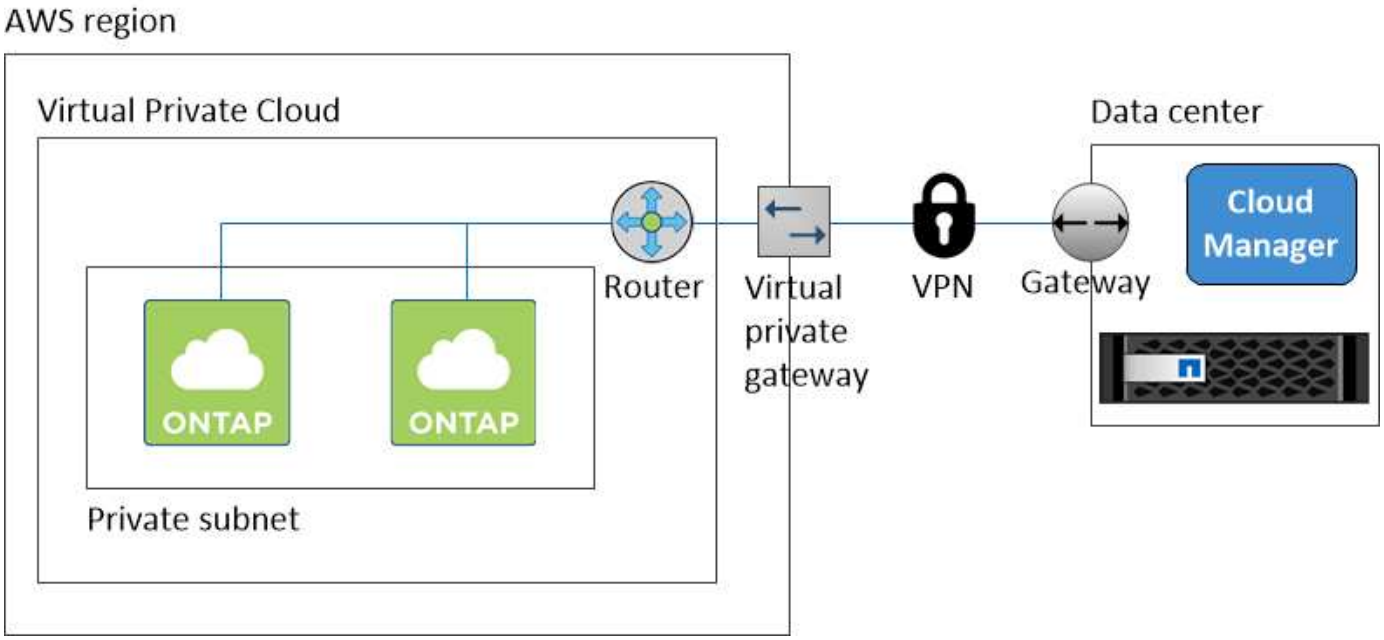
이 VPC 구성은 Cloud Volumes ONTAP가 프라이빗 환경의 확장이 되는 하이브리드 클라우드 구성입니다. 이 구성에는 네트워크에 대한 VPN 연결이 있는 전용 서브넷 및 가상 전용 게이트웨이가 포함됩니다. VPN 터널을 통해 라우팅하면 EC2 인스턴스가 네트워크 및 방화벽을 통해 인터넷에 액세스할 수 있습니다. 프라이빗 서브넷 또는 데이터 센터에서 Cloud Manager를 실행할 수 있습니다. 그런 다음 개인 서브넷에서 Cloud Volumes ONTAP를 실행합니다.

이 구성에서 프록시 서버를 사용하여 인터넷 액세스를 허용할 수도 있습니다. 프록시 서버는 데이터 센터 또는 AWS에 있을 수 있습니다.

데이터 센터의 FAS 시스템과 AWS의 Cloud Volumes ONTAP 시스템 간에 데이터를 복제하려면 링크가 안전하도록 VPN 연결을 사용해야 합니다.

이 시나리오에 대한 자세한 내용은 을 참조하십시오 "AWS 문서: 시나리오 4: 전용 서브넷만 있는 VPC 및 AWS 관리형 VPN 액세스".

다음 그래픽은 데이터 센터에서 실행되는 Cloud Manager와 프라이빗 서브넷에서 실행되는 단일 노드 시스템을 보여 줍니다.



여러 **AZs**에서 **HA** 쌍에 대한 **AWS** 전송 게이트웨이 설정

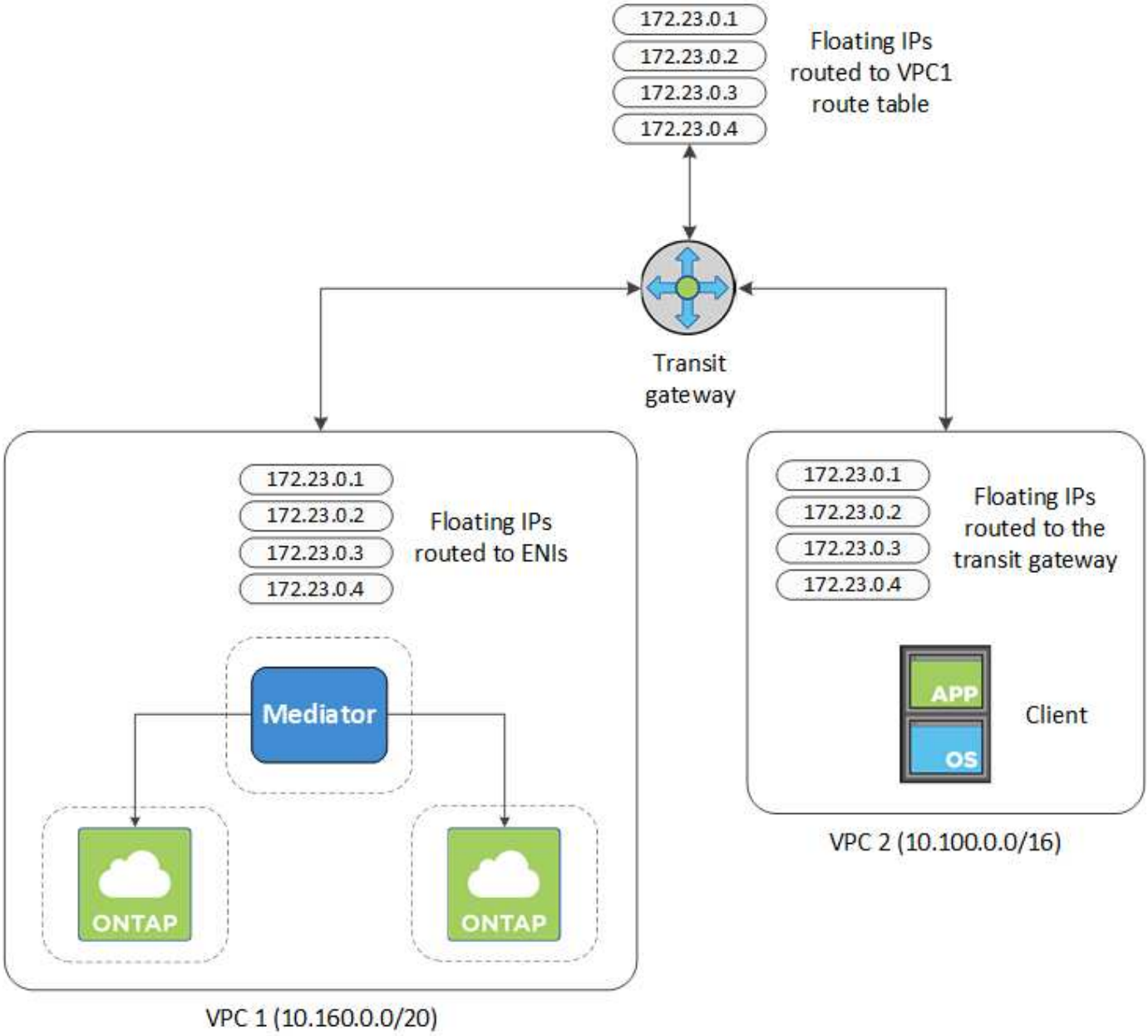
HA 쌍이 상주하는 VPC 외부에서 HA 쌍의 부동 IP 주소에 액세스할 수 있도록 AWS 전송 게이트웨이를 설정합니다.

Cloud Volumes ONTAP HA 구성이 여러 AWS 가용성 영역에 분산되면 VPC 내에서 NAS 데이터 액세스에 유동 IP 주소가 필요합니다. 이러한 부동 IP 주소는 장애가 발생할 때 노드 간에 마이그레이션할 수 있지만 VPC 외부에서 기본적으로 액세스할 수 없습니다. 별도의 프라이빗 IP 주소를 통해 VPC 외부에서 데이터에 액세스할 수 있지만 자동 페일오버를 제공하지 않습니다.

클러스터 관리 인터페이스와 선택적 SVM 관리 LIF에도 부동 IP 주소가 필요합니다.

AWS 전송 게이트웨이를 설정한 경우 HA 쌍이 상주하는 VPC 외부의 유동 IP 주소에 액세스할 수 있습니다. 즉, VPC 외부에 있는 NAS 클라이언트와 NetApp 관리 툴이 유동 IP에 액세스할 수 있습니다.

다음은 전송 게이트웨이에 의해 연결된 두 대의 VPC를 보여 주는 예입니다. HA 시스템은 VPC 하나에 상주하고 클라이언트는 다른 VPC에 상주합니다. 그런 다음 부동 IP 주소를 사용하여 클라이언트에 NAS 볼륨을 마운트할 수 있습니다.

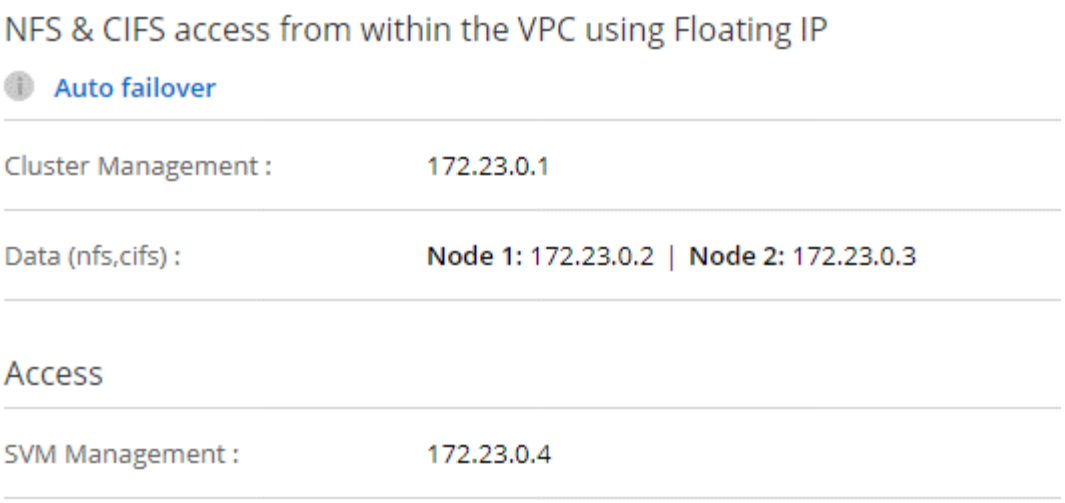


다음 단계에서는 유사한 구성을 설정하는 방법을 보여 줍니다.

단계

1. "전송 게이트웨이를 만들고 VPC를 게이트웨이에 연결합니다".
2. HA 쌍의 부동 IP 주소를 지정하여 전송 게이트웨이의 라우팅 테이블에서 경로를 만듭니다.

   Cloud Manager의 작업 환경 정보 페이지에서 부동 IP 주소를 찾을 수 있습니다. 예를 들면 다음과 같습니다.



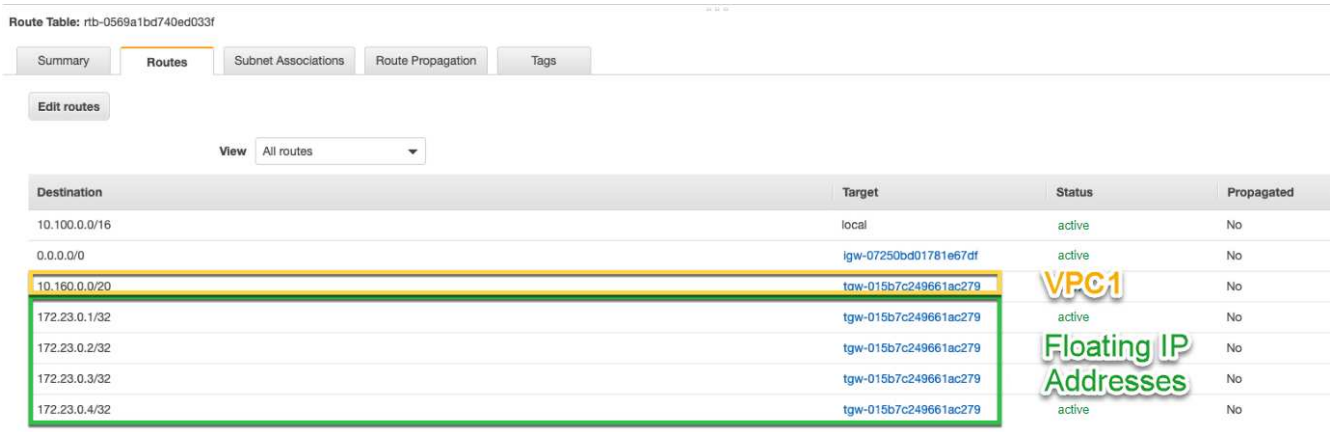
다음 샘플 이미지는 전송 게이트웨이의 라우트 테이블을 보여 줍니다. 여기에는 2개의 VPC의 CIDR 블록에 대한 경로와 Cloud Volumes ONTAP에서 사용하는 4개의 부동 IP 주소가 포함됩니다.

3. 부동 IP 주소에 액세스해야 하는 VPC의 라우팅 테이블을 수정합니다.

   a. 부동 IP 주소에 라우트 항목을 추가합니다.

   b. HA 쌍이 상주하는 VPC의 CIDR 블록에 경로 항목을 추가합니다.

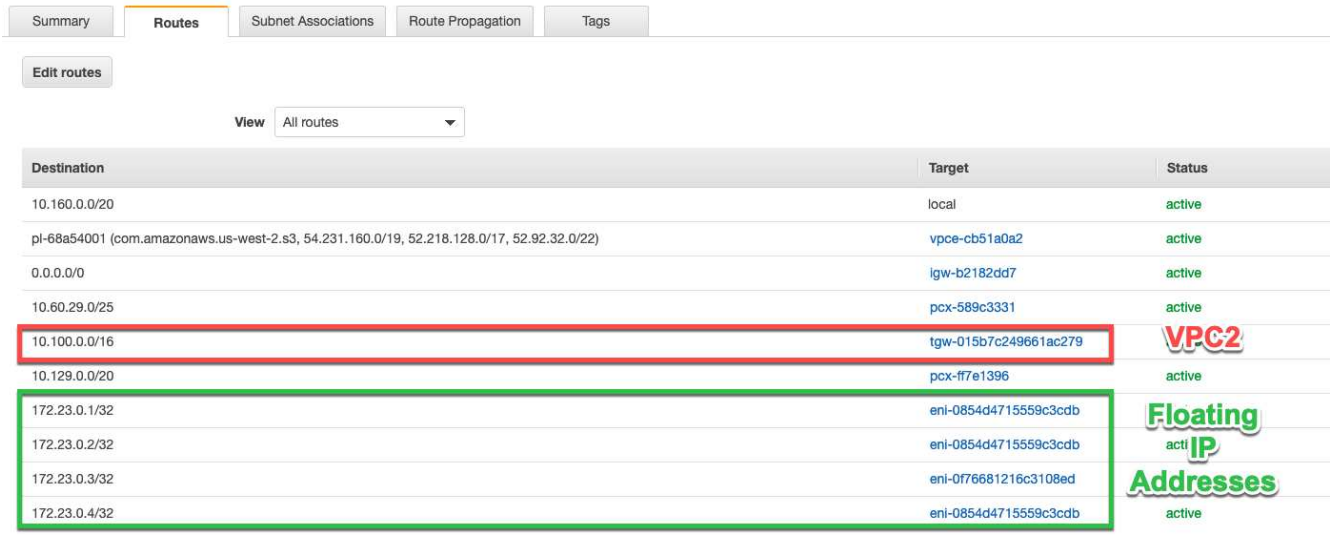
      다음 샘플 이미지는 VPC 1에 대한 라우트 및 부동 IP 주소를 포함하는 VPC 2용 라우팅 테이블을 보여 줍니다.



4. 유동 IP 주소에 액세스해야 하는 VPC에 경로를 추가하여 HA 쌍 VPC의 경로 테이블을 수정합니다.

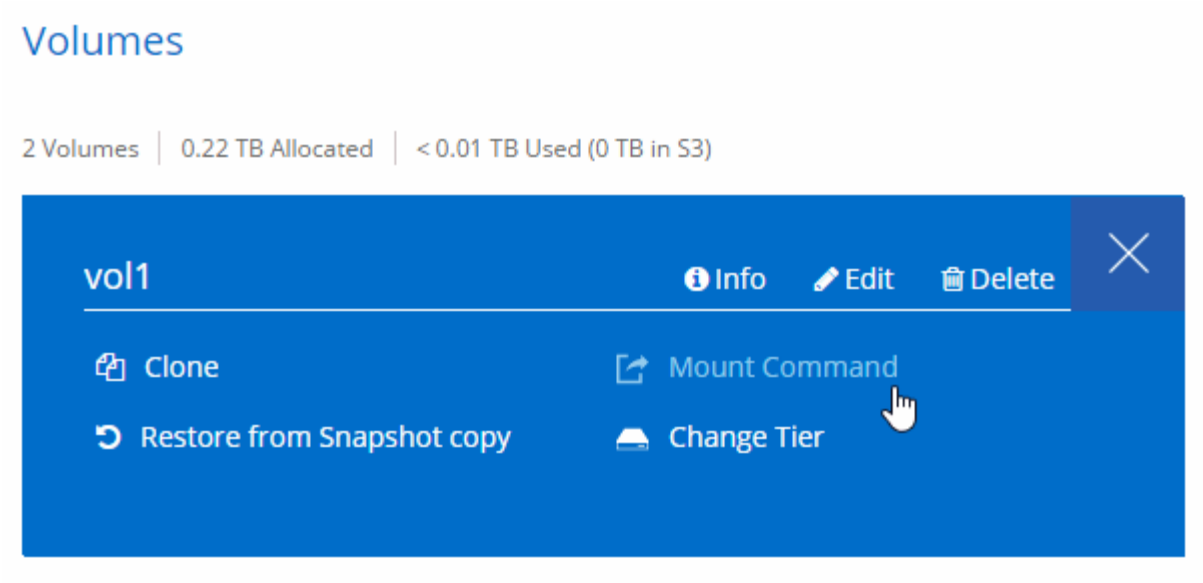
   이 단계는 VPC 간 라우팅을 완료하기 때문에 중요합니다.

   다음 샘플 이미지는 VPC 1의 라우트 테이블을 보여 줍니다. 여기에는 부동 IP 주소 및 클라이언트가 있는 VPC 2로의 라우트가 포함됩니다. Cloud Manager에서 HA 쌍을 구축하면 라우팅 테이블에 유동 IP가 자동으로 추가됩니다.



5. 부동 IP 주소를 사용하여 클라이언트에 볼륨을 마운트합니다.

   볼륨을 선택하고 * 탑재 명령 * 을 클릭하여 Cloud Manager에서 올바른 IP 주소를 찾을 수 있습니다.



◦ 관련 링크 *

◦ "AWS의 고가용성 쌍"

◦ "AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항"

Azure의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항

Cloud Volumes ONTAP 시스템이 올바르게 작동할 수 있도록 Azure 네트워킹을 설정해야 합니다.

Cloud Manager에 액세스해야 하는 엔드포인트 목록을 찾고 계십니까? 이제 단일 위치에서 유지 관리됩니다. "자세한 내용을 보려면 여기를 클릭하십시오".

Cloud Volumes ONTAP에 대한 아웃바운드 인터넷 액세스

Cloud Volumes ONTAP에서 스토리지 상태를 능동적으로 모니터링하는 NetApp AutoSupport에 메시지를 보내려면 아웃바운드 인터넷 액세스가 필요합니다.

라우팅 및 방화벽 정책은 Cloud Volumes ONTAP가 AutoSupport 메시지를 전송할 수 있도록 다음 엔드포인트로 AWS HTTP/HTTPS 트래픽을 허용해야 합니다.

- https://support.netapp.com/aods/asupmessage 으로 문의하십시오
- https://support.netapp.com/asupprod/post/1.0/postAsup 으로 문의하십시오

보안 그룹

Cloud Manager에서 보안 그룹을 생성할 수 있으므로 보안 그룹을 생성할 필요가 없습니다. 직접 사용해야 하는 경우 을 참조하십시오 "보안 그룹 규칙".

데이터 계층화를 위해 **Cloud Volumes ONTAP**에서 **Azure Blob** 저장소로 연결

콜드 데이터를 Azure Blob 저장소에 계층화하려는 경우 Cloud Manager에 필요한 권한이 있는 한 VNET 서비스 엔드포인트를 설정할 필요가 없습니다.

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

이러한 권한은 최신 에 포함되어 있습니다 "Cloud Manager 정책".

데이터 계층화 설정에 대한 자세한 내용은 을 참조하십시오 "콜드 데이터를 저비용 오브젝트 스토리지로 계층화".

다른 네트워크의 **ONTAP** 시스템에 대한 연결

Azure의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 Azure VNET와 다른 네트워크(예: AWS VPC 또는 기업 네트워크) 간에 VPN 연결이 있어야 합니다.

자세한 지침은 을 참조하십시오 "Microsoft Azure 문서: Azure 포털에서 사이트 간 연결을 만듭니다".

추가 구축 옵션

Cloud Manager 호스트 요구사항

자체 호스트에 Cloud Manager를 설치하는 경우 운영 체제 요구사항, 포트 요구사항 등이 포함된 구성에 대한 지원을 확인해야 합니다.

지원되는 **AWS EC2** 인스턴스 유형

T3.MEDIUM(권장), T2.MEDIUM 및 M4.Large

지원되는 **Azure VM** 크기입니다

A2, D2 v2 또는 D2 v3(가용성 기준)

지원되는 운영 체제

- CentOS 7.2
- CentOS 7.3
- CentOS 7.4
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4

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

  Cloud Manager는 이러한 운영 체제의 영어 버전에서 지원됩니다.

하이퍼바이저

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

CPU

코어 2개가 있는 경우 2.27GHz 이상

RAM

4GB

사용 가능한 디스크 공간

50GB

아웃바운드 인터넷 액세스

Cloud Manager를 설치할 때와 Cloud Manager를 사용하여 Cloud Volumes ONTAP를 구축할 때는 아웃바운드 인터넷 액세스가 필요합니다. 끝점 목록은 을 참조하십시오 "Cloud Manager의 네트워킹 요구사항".

포트

다음 포트를 사용할 수 있어야 합니다.

- HTTP 액세스용 80
- HTTPS 액세스용 443
- Cloud Manager 데이터베이스용 3306
- Cloud Manager API 프록시의 경우 8080

다른 서비스에서 이러한 포트를 사용하는 경우 Cloud Manager 설치가 실패합니다.

포트 3306과 충돌할 가능성이 있습니다. MySQL의 다른 인스턴스가 호스트에서 실행 중인 경우 기본적으로 포트 3306을 사용합니다. 기존 MySQL 인스턴스가 사용하는 포트를 변경해야 합니다.

Cloud Manager를 설치할 때 기본 HTTP 및 HTTPS 포트를 변경할 수 있습니다. MySQL 데이터베이스의 기본 포트는 변경할 수 없습니다. HTTP 및 HTTPS 포트를 변경하는 경우 사용자가 원격 호스트에서 Cloud Manager 웹 콘솔에 액세스할 수 있는지 확인해야 합니다.

- 포트를 통한 인바운드 연결을 허용하도록 보안 그룹을 수정합니다.
- Cloud Manager 웹 콘솔에 대한 URL을 입력할 때 포트를 지정합니다.

기존 **Linux** 호스트에 **Cloud Manager** 설치

Cloud Manager를 구축하는 가장 일반적인 방법은 Cloud Central 또는 클라우드 공급자의 마켓플레이스에서 구축하는 것입니다. 네트워크 또는 클라우드의 기존 Linux 호스트에 Cloud Manager 소프트웨어를 다운로드하고 설치할 수 있습니다.

시작하기 전에

- Red Hat Enterprise Linux 시스템은 Red Hat 서브스크립션 관리 에 등록되어 있어야 합니다. 등록되지 않은 경우 시스템은 Cloud Manager 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.
- Cloud Manager 설치 프로그램은 설치 프로세스 중에 여러 URL에 액세스합니다. 이러한 엔드포인트에 아웃바운드 인터넷 액세스가 허용되는지 확인해야 합니다. 을 참조하십시오 "Cloud Manager의 네트워킹 요구사항".

이 작업에 대해

- Cloud Manager를 설치하는 데 루트 권한이 필요하지 않습니다.
- Cloud Manager는 AWS 명령줄 툴(awscli)을 설치하여 NetApp 지원으로부터 복구 절차를 지원합니다.

  awscli 설치에 실패했다는 메시지가 표시되면 메시지를 무시해도 됩니다. Cloud Manager는 툴 없이 성공적으로 운영될 수 있습니다.

- NetApp Support 사이트에서 제공되는 설치 프로그램은 이전 버전일 수 있습니다. 새 버전을 사용할 수 있는 경우 설치 후 Cloud Manager가 자동으로 업데이트됩니다.

단계

1. 네트워킹 요구 사항 검토:
   - "Cloud Manager의 네트워킹 요구사항"
   - "Cloud Volumes ONTAP for AWS의 네트워킹 요구사항"
   - "Azure용 Cloud Volumes ONTAP의 네트워킹 요구사항"
2. 검토 "Cloud Manager 호스트 요구사항".
3. 에서 소프트웨어를 다운로드합니다 "NetApp Support 사이트"를 선택한 다음 Linux 호스트에 복사합니다.

   AWS에서 EC2 인스턴스에 파일을 연결하고 복사하는 방법은 를 참조하십시오 "AWS 설명서: SSH를 사용하여 Linux 인스턴스에 연결".

4. 스크립트를 실행할 권한을 할당합니다.
   - 예 *

   ```
   chmod +x OnCommandCloudManager-V3.6.3.sh
   . 설치 스크립트를 실행합니다.
   ```

   ```
   ./OnCommandCloudManager-V3.6.3.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   _silent_는 정보를 묻지 않고 설치를 실행합니다.

   Cloud Manager 호스트가 프록시 서버 뒤에 있으면 _proxy_가 필요합니다.

   _proxyPort_는 프록시 서버의 포트입니다.

   _proxyuser_는 기본 인증이 필요한 경우 프록시 서버의 사용자 이름입니다.

   _proxypwd_는 지정한 사용자 이름의 암호입니다.

5. silent 매개 변수를 지정하지 않은 경우 스크립트를 계속하려면 * Y * 를 입력하고 메시지가 표시되면 HTTP 및 HTTPS 포트를 입력합니다.

   HTTP 및 HTTPS 포트를 변경하는 경우 사용자가 원격 호스트에서 Cloud Manager 웹 콘솔에 액세스할 수 있는지 확인해야 합니다.

- 포트를 통한 인바운드 연결을 허용하도록 보안 그룹을 수정합니다.
- Cloud Manager 웹 콘솔에 대한 URL을 입력할 때 포트를 지정합니다.

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

6. 웹 브라우저를 열고 다음 URL을 입력합니다.

   https://ipaddress:port

   _ipaddress_는 Cloud Manager 호스트 구성에 따라 localhost, 전용 IP 주소 또는 공용 IP 주소일 수 있습니다. 예를 들어, Cloud Manager가 퍼블릭 IP 주소 없이 퍼블릭 클라우드에 있는 경우 Cloud Manager 호스트에 대한 연결이 있는 호스트의 프라이빗 IP 주소를 입력해야 합니다.

   기본 HTTP(80) 또는 HTTPS(443) 포트를 변경한 경우 port_가 필요합니다. 예를 들어, HTTPS 포트가 8443으로 변경된 경우 를 입력합니다 https://_ipaddress:8443

7. NetApp Cloud Central 계정에 가입하거나 이미 가지고 있는 경우 로그인하십시오.
8. 등록 또는 로그인하면 Cloud Manager에서 자동으로 사용자 계정을 이 시스템의 관리자로 추가합니다.
9. 로그인한 후 이 Cloud Manager 시스템의 이름을 입력합니다.

작업을 마친 후

Cloud Manager에서 Cloud Volumes ONTAP를 구축할 수 있도록 AWS 및 Azure 계정에 대한 권한 설정:

- AWS에 Cloud Volumes ONTAP를 구축하려는 경우, "AWS 계정을 설정한 다음 Cloud Manager에 추가합니다".
- Azure에서 Cloud Volumes ONTAP를 배포하려는 경우 "Azure 계정을 설정한 다음 Cloud Manager에 추가합니다".

AWS Marketplace에서 Cloud Manager 시작

AWS에서 Cloud Manager를 시작하는 것이 가장 좋습니다 "NetApp Cloud Central에서"하지만 필요한 경우 AWS Marketplace에서 시작할 수 있습니다.

AWS 마켓플레이스에서 Cloud Manager를 시작하면 Cloud Manager가 NetApp Cloud Central과 통합됩니다. "통합에 대해 자세히 알아보십시오".

이 작업에 대해

다음 단계에서는 콘솔에서 IAM 역할을 Cloud Manager 인스턴스에 연결할 수 있으므로 EC2 콘솔에서 인스턴스를 시작하는 방법을 설명합니다. 1-클릭 옵션은 사용할 수 없습니다.

단계

1. EC2 인스턴스에 대해 IAM 정책 및 역할을 생성합니다.
   a. 다음 위치에서 Cloud Manager IAM 정책을 다운로드합니다.

      "NetApp OnCommand 클라우드 관리자: AWS 및 Azure 정책"

b. IAM 콘솔에서 Cloud Manager IAM 정책의 텍스트를 복사하여 붙여넣어 고유한 정책을 생성합니다.

c. Amazon EC2 역할 유형으로 IAM 역할을 생성하고 이전 단계에서 생성한 정책을 역할에 연결합니다.

2. 로 이동합니다 "Cloud Manager 페이지로 이동하여 AWS 마켓플레이스를 확인하십시오".
3. 계속 * 을 클릭합니다.
4. 사용자 지정 시작 탭에서 해당 지역의 * EC2 콘솔 * 로 시작 을 클릭한 후 다음을 선택합니다.

a. 지역 사용 가능 여부에 따라 T3.MEDIUM(권장), T2.MEDIUM 또는 M4.Large instance type을 선택합니다.

b. 요구 사항을 충족하는 VPC, 서브넷, IAM 역할 및 기타 구성 옵션을 선택합니다.

c. 기본 스토리지 옵션을 유지합니다.

d. 필요한 경우 인스턴스에 대한 태그를 입력합니다.

e. Cloud Manager 인스턴스에 필요한 SSH, HTTP 및 HTTPS 연결 방법을 지정합니다.

f. 시작 * 을 클릭합니다.

결과

AWS가 지정된 설정으로 소프트웨어를 시작합니다. Cloud Manager 인스턴스와 소프트웨어는 약 5분 내에 실행되어야 합니다.

작업을 마친 후

웹 브라우저에 공용 IP 주소 또는 전용 IP 주소를 입력하여 Cloud Manager에 로그인한 다음 설정 마법사를 완료합니다.

Azure 마켓플레이스에서 Cloud Manager 구축

Azure에서 Cloud Manager를 구축하는 것이 가장 좋습니다 "NetApp Cloud Central에서 "필요한 경우 Azure 마켓플레이스에서 구축할 수 있습니다.

Cloud Manager를 구축할 수 있는 별도의 지침이 제공됩니다 "Azure 미국 정부 지역" 및 IN "Azure 독일 지역".

Azure Marketplace에서 Cloud Manager를 구축한 경우에도 Cloud Manager는 NetApp Cloud Central과 통합됩니다. "통합에 대해 자세히 알아보십시오".

Azure에 **Cloud Manager** 배포

Azure에서 Cloud Volumes ONTAP를 시작하는 데 사용할 수 있도록 Cloud Manager를 설치 및 설정해야 합니다.

단계

1. "Cloud Manager의 Azure 마켓플레이스 페이지로 이동합니다".
2. 지금 받기 * 를 클릭한 다음 * 계속 * 을 클릭합니다.
3. Azure 포털에서 * Create * 를 클릭하고 다음 단계에 따라 가상 시스템을 구성합니다.

   VM을 구성할 때 다음 사항에 유의하십시오.

   - Cloud Manager는 HDD 또는 SSD 디스크를 최적의 상태로 사용할 수 있습니다.
   - A2, D2 v2 또는 D2 v3(사용 가능 여부에 따라)의 권장 가상 머신 크기 중 하나를 선택합니다.

◦ 네트워크 보안 그룹의 경우 Cloud Manager에는 SSH, HTTP 및 HTTPS를 사용한 인바운드 연결이 필요합니다.

"Cloud Manager의 보안 그룹 규칙에 대해 자세히 알아보십시오".

◦ 관리 * 에서 * 켜기 * 를 선택하여 클라우드 관리자에 대해 * 시스템 할당 관리 ID * 를 활성화합니다.

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

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

Azure는 지정된 설정으로 가상 머신을 구축합니다. 가상 머신과 Cloud Manager 소프트웨어가 약 5분 이내에 실행되어야 합니다.

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

http://ipaddress:80

로그인하면 Cloud Manager에서 자동으로 사용자 계정을 이 시스템의 관리자로 추가합니다.

6. 로그인한 후 Cloud Manager 시스템의 이름을 입력합니다.

결과

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

Cloud Manager에 **Azure** 사용 권한 부여

Azure에 Cloud Manager를 구축한 경우 를 활성화해야 합니다 "시스템에서 할당한 관리 ID입니다". 이제 사용자 지정 역할을 만든 다음 하나 이상의 구독에 대해 Cloud Manager 가상 머신에 역할을 할당하여 필요한 Azure 권한을 부여해야 합니다.

단계

1. Cloud Manager 정책을 사용하여 사용자 지정 역할 생성:

a. 를 다운로드합니다 "Cloud Manager Azure 정책".

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-c25fbzzzzzzzz","/Subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz","/Subscripts/398e471c-3bzzzzzzzzzzz-4bzbzz-4bzbzbzz-4959-4bzz

c. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 생성합니다.

다음 예에서는 Azure CLI 2.0을 사용하여 사용자 지정 역할을 생성하는 방법을 보여 줍니다.

▪ az 역할 정의 create — 역할 정의 C:\Policy_for_cloud_Manager_Azure_3.6.1.json *

이제 OnCommand Cloud Manager 운영이라는 사용자 지정 역할을 갖게 됩니다. 이 역할은 Cloud Manager 가상 머신에 할당할 수 있습니다.

2. 하나 이상의 구독에 대해 Cloud Manager 가상 머신에 역할을 할당합니다.
   a. Subscriptions * 서비스를 연 다음 Cloud Volumes ONTAP 시스템을 배포할 구독을 선택합니다.
   b. IAM(액세스 제어) * 을 클릭합니다.
   c. Add * > * Add role assignment * 를 클릭한 후 권한을 추가합니다.
      - OnCommand 클라우드 관리자 운영자 * 역할을 선택하십시오.

        OnCommand Cloud Manager Operator는 에 제공되는 기본 이름입니다 "Cloud Manager 정책". 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

      - Virtual Machine * 에 대한 액세스 권한을 할당합니다.
      - Cloud Manager 가상 머신이 생성된 서브스크립션을 선택합니다.
      - Cloud Manager 가상 머신을 선택합니다.
      - 저장 * 을 클릭합니다.
   d. 추가 구독에서 Cloud Volumes ONTAP를 배포하려면 해당 구독으로 전환한 다음 이 단계를 반복합니다.

결과

이제 Cloud Manager에 Azure에서 Cloud Volumes ONTAP를 배포하고 관리하는 데 필요한 권한이 있습니다.

Azure 미국 정부 지역에서 Cloud Manager 구축

미국 정부 지역에서 Cloud Manager를 시작 및 실행하려면 먼저 Azure Government Marketplace에서 Cloud Manager를 구축해야 합니다. 그런 다음, Cloud Manager에서 Cloud Volumes ONTAP 시스템을 구축하고 관리하는 데 필요한 권한을 제공합니다.

지원되는 Azure 미국 정부 지역 목록은 를 참조하십시오 "Cloud Volumes 글로벌 지역".

Azure US Government Marketplace에서 Cloud Manager 구축

Cloud Manager는 Azure US Government Marketplace에서 이미지로 사용할 수 있습니다.

단계

1. Azure US Government 포털에서 OnCommand Cloud Manager를 검색하십시오.
2. Create * 를 클릭하고 다음 단계에 따라 가상 머신을 구성합니다.

   가상 머신을 구성할 때 다음 사항에 유의하십시오.

   - Cloud Manager는 HDD 또는 SSD 디스크를 최적의 상태로 사용할 수 있습니다.
   - A2, D2 v2 또는 D2 v3(사용 가능 여부에 따라)의 권장 가상 머신 크기 중 하나를 선택해야 합니다.
   - 네트워크 보안 그룹의 경우 * 고급 * 을 선택하는 것이 가장 좋습니다.

     고급 * 옵션은 Cloud Manager에 필요한 인바운드 규칙을 포함하는 새 보안 그룹을 만듭니다. 기본 을 선택한 경우 을 참조하십시오 "보안 그룹 규칙" 필수 규칙 목록을 참조하십시오.

3. 요약 페이지에서 선택 사항을 검토하고 * 생성 * 을 클릭하여 배포를 시작합니다.

   Azure는 지정된 설정으로 가상 머신을 구축합니다. 가상 머신과 Cloud Manager 소프트웨어가 약 5분 이내에 실행되어야 합니다.

4. Cloud Manager 가상 머신에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

   http://ipaddress:80

   로그인하면 Cloud Manager에서 자동으로 사용자 계정을 이 시스템의 관리자로 추가합니다.

5. 로그인한 후 Cloud Manager 시스템의 이름을 입력합니다.

결과

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

관리되는 **ID**를 사용하여 **Cloud Manager**에 **Azure** 사용 권한 부여

사용 권한을 제공하는 가장 쉬운 방법은 을 사용하는 것입니다 "관리 ID" Cloud Manager 가상 머신에서 가상 머신에 필요한 사용 권한을 할당합니다. 원하는 경우, 다른 방법은 입니다 "서비스 보안 주체를 사용하여 Azure 사용 권한을 부여합니다".

단계

1. Cloud Manager 가상 시스템에서 관리 ID 사용:
   a. Cloud Manager 가상 머신으로 이동하여 * Identity * 를 선택합니다.
   b. System Assigned * 에서 * On * 을 클릭한 다음 * Save * 를 클릭합니다.
2. Cloud Manager 정책을 사용하여 사용자 지정 역할 생성:
   a. 를 다운로드합니다 "Cloud Manager Azure 정책".
   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-c25fbzzzzzzzz","/Subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz","/Subscripts/398e471c-3bzzzzzzzzzzz-4bzbzz-4bzbzbzz-4959-4bzz

   c. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 생성합니다.

      다음 예에서는 Azure CLI 2.0을 사용하여 사용자 지정 역할을 생성하는 방법을 보여 줍니다.

      - az 역할 정의 create — 역할 정의 C:\Policy_for_cloud_Manager_Azure_3.6.1.json *

   이제 OnCommand Cloud Manager 운영이라는 사용자 지정 역할을 갖게 됩니다. 이 역할은 Cloud Manager 가상 머신에 할당할 수 있습니다.

3. 하나 이상의 구독에 대해 Cloud Manager 가상 머신에 역할을 할당합니다.

a. Subscriptions * 서비스를 연 다음 Cloud Volumes ONTAP 시스템을 배포할 구독을 선택합니다.

b. IAM(액세스 제어) * 을 클릭합니다.

c. 추가 * 를 클릭하고 * 역할 할당 추가 * 를 클릭한 다음 권한을 추가합니다.

- OnCommand 클라우드 관리자 운영자 * 역할을 선택하십시오.

  OnCommand Cloud Manager Operator는 에 제공되는 기본 이름입니다 "Cloud Manager 정책". 역할에 다른 이름을 선택한 경우 대신 해당 이름을 선택합니다.

- Virtual Machine * 에 대한 액세스 권한을 할당합니다.
- Cloud Manager 가상 머신이 생성된 서브스크립션을 선택합니다.
- 가상 머신의 이름을 입력한 다음 선택합니다.
- 저장 * 을 클릭합니다.

d. 추가 구독에서 Cloud Volumes ONTAP를 배포하려면 해당 구독으로 전환한 다음 이 단계를 반복합니다.

결과

이제 Cloud Manager에 Azure에서 Cloud Volumes ONTAP를 배포하고 관리하는 데 필요한 권한이 있습니다.

Azure 독일 지역에 Cloud Manager 설치

Azure 마켓플레이스는 Azure 독일 지역에서 사용할 수 없으므로 NetApp Support 사이트에서 Cloud Manager 설치 프로그램을 다운로드하고 이 지역의 기존 Linux 호스트에 설치해야 합니다.

단계

1. "Azure의 네트워킹 요구 사항을 검토합니다".
2. "Cloud Manager 호스트 요구사항을 검토합니다".
3. "Cloud Manager를 다운로드하고 설치합니다".
4. "서비스 보안 주체를 사용하여 Cloud Manager에 Azure 권한을 부여합니다".

작업을 마친 후

Cloud Manager는 이제 다른 지역과 마찬가지로 Azure 독일 지역에 Cloud Volumes ONTAP를 구축할 준비가 되었습니다. 그러나 먼저 추가 설정을 수행할 수 있습니다.

저작권 정보

상표 정보