콘솔 에이전트 배포

NetApp Console setup and administration

NetApp
February 11, 2026

목차

콘솔 에이전트 배포

AWS

AWS의 콘솔 에이전트 설치 옵션

AWS에서 콘솔 에이전트를 만드는 방법에는 여러 가지가 있습니다. 가장 일반적인 방법은 NetApp Console 에서 직접 실행하는 것입니다.

다음과 같은 설치 옵션을 사용할 수 있습니다.

- "콘솔에서 직접 콘솔 에이전트를 만듭니다."(이것은 표준 옵션입니다)

  이 작업을 수행하면 선택한 VPC에서 Linux와 콘솔 에이전트 소프트웨어를 실행하는 EC2 인스턴스가 시작됩니다.

- "AWS Marketplace에서 콘솔 에이전트 만들기"

  이 작업을 수행하면 Linux와 콘솔 에이전트 소프트웨어가 실행되는 EC2 인스턴스가 시작되지만 배포는 콘솔이 아닌 AWS Marketplace에서 직접 시작됩니다.

- "자신의 Linux 호스트에 소프트웨어를 다운로드하고 수동으로 설치하세요."

선택하는 설치 옵션은 설치를 준비하는 방법에 영향을 미칩니다. 여기에는 AWS에서 리소스를 인증하고 관리하는 데 필요한 권한을 콘솔에 제공하는 방법이 포함됩니다.

NetApp Console 에서 AWS에 콘솔 에이전트 만들기

NetApp Console 에서 직접 AWS에서 콘솔 에이전트를 만들 수 있습니다. AWS 콘솔에서 콘솔 에이전트를 생성하기 전에 네트워킹을 설정하고 AWS 권한을 준비해야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**: AWS**에 콘솔 에이전트를 배포하기 위한 네트워킹 설정

콘솔 에이전트를 설치하려는 네트워크 위치가 다음 요구 사항을 지원하는지 확인하세요. 이러한 요구 사항을 통해 콘솔 에이전트는 하이브리드 클라우드의 리소스와 프로세스를 관리할 수 있습니다.

VPC 및 서브넷

콘솔 에이전트를 생성할 때는 에이전트가 상주해야 하는 VPC와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 리소스를 관리합니다. 엔드포인트는 AWS 지역에 따라 달라집니다. "자세한 내용은 AWS 설명서를 참조하세요."
Amazon FsX for NetApp ONTAP: • api.workloads.netapp.com	웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.

엔드포인트	목적
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

NetApp 콘솔에서 연결된 엔드포인트

SaaS 계층을 통해 제공되는 웹 기반 NetApp Console 사용하면 여러 엔드포인트에 연결하여 데이터 관리 작업을 완료할 수 있습니다. 여기에는 콘솔에서 콘솔 에이전트를 배포하기 위해 연결된 엔드포인트가 포함됩니다.

"NetApp 콘솔에서 연결된 엔드포인트 목록 보기" .

프록시 서버

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

- IP 주소
- 신임장
- HTTPS 인증서

포트

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

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

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

NTP 활성화

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

콘솔 에이전트를 만든 후 이 네트워킹 요구 사항을 구현해야 합니다.

2단계**:** 콘솔 에이전트에 대한 **AWS** 권한 설정

VPC에 콘솔 에이전트를 배포하려면 먼저 콘솔이 AWS에서 인증을 받아야 합니다. 다음 인증 방법 중 하나를 선택할 수 있습니다.

- 콘솔이 필요한 권한이 있는 IAM 역할을 가정하도록 합니다.
- 필요한 권한이 있는 IAM 사용자에게 AWS 액세스 키와 비밀 키를 제공합니다.

두 옵션 모두 첫 번째 단계는 IAM 정책을 만드는 것입니다. 이 정책에는 AWS 콘솔에서 콘솔 에이전트를 시작하는 데 필요한 권한만 포함되어 있습니다.

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

단계

1. AWS IAM 콘솔로 이동합니다.
2. *정책 > 정책 만들기*를 선택합니다.
3. *JSON*을 선택하세요.
4. 다음 정책을 복사하여 붙여넣으세요.

   이 정책에는 AWS 콘솔에서 콘솔 에이전트를 시작하는 데 필요한 권한만 포함되어 있습니다. 콘솔이 콘솔 에이전트를 생성하면 콘솔 에이전트가 AWS 리소스를 관리할 수 있도록 하는 새로운 권한 집합이 콘솔 에이전트에 적용됩니다. "콘솔 에이전트 자체에 필요한 권한 보기".

```
{
  "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. *다음*을 선택하고 필요한 경우 태그를 추가합니다.
6. *다음*을 선택하고 이름과 설명을 입력합니다.
7. *정책 만들기*를 선택하세요.
8. 콘솔이 가정할 수 있는 IAM 역할이나 IAM 사용자에게 정책을 연결하여 콘솔에 액세스 키를 제공할 수 있습니다.
   - (옵션 1) 콘솔이 맡을 수 있는 IAM 역할을 설정합니다.
     i. 대상 계정의 AWS IAM 콘솔로 이동합니다.
     ii. 액세스 관리에서 *역할 > 역할 만들기*를 선택하고 단계에 따라 역할을 만듭니다.
     iii. *신뢰할 수 있는 엔터티 유형*에서 *AWS 계정*을 선택합니다.
     iv. *다른 AWS 계정*을 선택하고 콘솔 SaaS 계정의 ID를 입력하세요: 952013314444
     v. 이전 섹션에서 만든 정책을 선택하세요.
     vi. 역할을 만든 후 역할 ARN을 복사하여 콘솔 에이전트를 만들 때 콘솔에 붙여넣을 수 있습니다.
   - (옵션 2) 콘솔에 액세스 키를 제공할 수 있도록 IAM 사용자에 대한 권한을 설정합니다.
     i. AWS IAM 콘솔에서 *사용자*를 선택한 다음 사용자 이름을 선택합니다.
     ii. *권한 추가 > 기존 정책을 직접 첨부*를 선택합니다.
     iii. 생성한 정책을 선택하세요.
     iv. *다음*을 선택한 다음 *권한 추가*를 선택합니다.
     v. IAM 사용자에 대한 액세스 키와 비밀 키가 있는지 확인하세요.

결과

이제 필요한 권한이 있는 IAM 역할이나 필요한 권한이 있는 IAM 사용자가 생겼습니다. 콘솔에서 콘솔 에이전트를 만들 때 역할이나 액세스 키에 대한 정보를 제공할 수 있습니다.

3단계**:** 콘솔 에이전트 만들기

콘솔 웹 기반 콘솔에서 직접 콘솔 에이전트를 만듭니다.

이 작업에 관하여

- 콘솔에서 콘솔 에이전트를 생성하면 기본 구성을 사용하여 AWS에 EC2 인스턴스가 배포됩니다. 콘솔 에이전트를 생성한 후에는 CPU나 RAM이 적은 더 작은 EC2 인스턴스로 전환하지 마세요. "콘솔 에이전트의 기본 구성에 대해 알아보세요" .
- 콘솔에서 콘솔 에이전트를 생성하면 에이전트에 대한 IAM 역할과 프로필이 생성됩니다. 이 역할에는 콘솔 에이전트가 AWS 리소스를 관리할 수 있는 권한이 포함됩니다. 향후 릴리스에서 새로운 권한이 추가되면 역할이 업데이트되도록 하세요. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요.".

시작하기 전에

다음 사항이 있어야 합니다.

- AWS 인증 방법: 필요한 권한이 있는 IAM 사용자에 대한 IAM 역할 또는 액세스 키입니다.
- 네트워킹 요구 사항을 충족하는 VPC 및 서브넷.
- EC2 인스턴스에 대한 키 쌍입니다.
- 콘솔 에이전트에서 인터넷에 접속하는 데 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.
- 설정"네트워킹 요구 사항" .
- 설정"AWS 권한" .

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 *에이전트 배포 > AWS*를 선택합니다.
3. 마법사의 단계에 따라 콘솔 에이전트를 만듭니다.
4. 소개 페이지에서 프로세스 개요를 제공합니다.
5. **AWS** 자격 증명 페이지에서 AWS 지역을 지정한 다음 인증 방법을 선택합니다. 인증 방법은 콘솔에서 가정할 수 있는 IAM 역할이나 AWS 액세스 키 및 비밀 키입니다.

   *역할 가정*을 선택하면 콘솔 에이전트 배포 마법사에서 첫 번째 자격 증명 세트를 만들 수 있습니다. 추가 자격 증명 세트는 자격 증명 페이지에서 만들어야 합니다. 그러면 마법사의 드롭다운 목록에서 해당 항목을 사용할 수 있습니다. "추가 자격 증명을 추가하는 방법을 알아보세요" .

6. 세부정보 페이지에서 콘솔 에이전트에 대한 세부정보를 제공합니다.
   - 이름을 입력하세요.
   - 사용자 정의 태그(메타데이터)를 추가합니다.
   - 콘솔에서 필요한 권한이 있는 새 역할을 만들지 아니면 사용자가 설정한 기존 역할을 선택할지 선택합니다. "필요한 권한" .
   - 콘솔 에이전트의 EBS 디스크를 암호화할지 여부를 선택합니다. 기본 암호화 키를 사용하거나 사용자 지정 키를 사용할 수 있습니다.
7. 네트워크 페이지에서 에이전트에 대한 VPC, 서브넷 및 키 쌍을 지정하고, 공용 IP 주소를 활성화할지 여부를 선택하고, 선택적으로 프록시 구성을 지정합니다.

   콘솔 에이전트 가상 머신에 액세스하려면 올바른 키 쌍이 있는지 확인하세요. 키 쌍이 없으면 액세스할 수 없습니다.

8. 보안 그룹 페이지에서 새 보안 그룹을 만들지, 아니면 필요한 인바운드 및 아웃바운드 규칙을 허용하는 기존 보안

그룹을 선택할지 선택합니다.

"AWS에 대한 보안 그룹 규칙 보기" .

9. 선택 사항을 검토하여 설정이 올바른지 확인하세요.

   a. 에이전트 구성 검증 확인란은 배포 시 콘솔에서 네트워크 연결 요구 사항을 검증하도록 기본적으로 선택되어 있습니다. 콘솔에서 에이전트를 배포하지 못하면 문제 해결에 도움이 되는 보고서가 제공됩니다. 배포가 성공하면 보고서는 제공되지 않습니다.

   아직도 사용 중이라면"이전 종료점" 에이전트 업그레이드에 사용되면 유효성 검사가 오류로 인해 실패합니다. 이를 방지하려면 유효성 검사를 건너뛰려면 확인란의 선택을 취소하세요.

10. *추가*를 선택하세요.

    콘솔은 약 10분 안에 에이전트를 배포합니다. 프로세스가 완료될 때까지 페이지에 머물러주세요.

결과

프로세스가 완료되면 콘솔 에이전트를 콘솔에서 사용할 수 있습니다.

배포에 실패하면 콘솔에서 보고서와 로그를 다운로드하여 문제를 해결할 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

콘솔 에이전트를 생성한 동일한 AWS 계정에 Amazon S3 버킷이 있는 경우, 시스템 페이지에 Amazon S3 작업 환경이 자동으로 표시됩니다. "NetApp Console 에서 S3 버킷을 관리하는 방법을 알아보세요."

AWS Marketplace에서 콘솔 에이전트 만들기

AWS Marketplace에서 직접 AWS에서 콘솔 에이전트를 만들 수 있습니다. AWS Marketplace에서 콘솔 에이전트를 만들려면 네트워킹을 설정하고, AWS 권한을 준비하고, 인스턴스 요구 사항을 검토한 다음 콘솔 에이전트를 만들어야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 네트워킹 설정

하이브리드 클라우드 리소스를 관리하려면 콘솔 에이전트의 네트워크 위치가 다음 요구 사항을 충족하는지 확인하세요.

VPC 및 서브넷

콘솔 에이전트를 생성할 때는 에이전트가 상주해야 하는 VPC와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 리소스를 관리합니다. 엔드포인트는 AWS 지역에 따라 달라집니다. "자세한 내용은 AWS 설명서를 참조하세요."
Amazon FsX for NetApp ONTAP: • api.workloads.netapp.com	웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.

엔드포인트	목적
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

프록시 서버

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

- IP 주소
- 신임장
- HTTPS 인증서

포트

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

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

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

NTP 활성화

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

콘솔 에이전트를 만든 후 이 네트워크 액세스를 구현합니다.

2단계**: AWS** 권한 설정

마켓플레이스 배포를 준비하려면 AWS에서 IAM 정책을 만들고 이를 IAM 역할에 연결합니다. AWS Marketplace에서 콘솔 에이전트를 생성하면 해당 IAM 역할을 선택하라는 메시지가 표시됩니다.

단계

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

   사용하려는 NetApp 데이터 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다. 표준 지역의 경우 권한은 두 가지 정책에 걸쳐 분산됩니다. AWS의 관리형 정책에는 최대 문자 크기 제한이 있으므로 두 개의 정책이 필요합니다. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요." .
3. IAM 역할을 만듭니다.
   a. *역할 > 역할 만들기*를 선택합니다.
   b. *AWS 서비스 > EC2*를 선택합니다.
   c. 방금 만든 정책을 첨부하여 권한을 추가합니다.
   d. 나머지 단계를 완료하여 역할을 만듭니다.

결과

이제 AWS Marketplace에서 배포하는 동안 EC2 인스턴스와 연결할 수 있는 IAM 역할이 생겼습니다.

3단계**:** 인스턴스 요구 사항 검토

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

CPU

8개 코어 또는 8개 vCPU

숫양

32GB

AWS EC2 인스턴스 유형

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

4단계: 콘솔 에이전트 만들기

AWS Marketplace에서 직접 콘솔 에이전트를 만듭니다.

이 작업에 관하여

AWS Marketplace에서 콘솔 에이전트를 생성하면 기본 구성을 사용하여 AWS에 EC2 인스턴스가 배포됩니다. "콘솔 에이전트의 기본 구성에 대해 알아보세요" .

시작하기 전에

다음 사항이 있어야 합니다.

- 네트워킹 요구 사항을 충족하는 VPC 및 서브넷.
- 콘솔 에이전트에 필요한 권한이 포함된 정책이 첨부된 IAM 역할입니다.
- IAM 사용자가 AWS Marketplace를 구독하고 구독을 취소할 수 있는 권한입니다.
- 인스턴스에 필요한 CPU 및 RAM 요구 사항을 이해합니다.
- EC2 인스턴스에 대한 키 쌍입니다.

단계

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

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

   EC2 콘솔을 사용하여 인스턴스를 시작하고 IAM 역할을 연결합니다. 웹사이트에서 실행 작업에서는 이 작업이 불가능합니다.
7. 프롬프트에 따라 인스턴스를 구성하고 배포하세요.
   - 이름 및 태그: 인스턴스의 이름과 태그를 입력합니다.
   - 애플리케이션 및 **OS** 이미지: 이 섹션을 건너뜁니다. 콘솔 에이전트 AMI가 이미 선택되었습니다.
   - 인스턴스 유형: 지역별 가용성에 따라 RAM 및 CPU 요구 사항을 충족하는 인스턴스 유형을 선택합니다(t3.2xlarge가 미리 선택되어 권장됨).
   - 키 쌍(로그인): 인스턴스에 안전하게 연결하는 데 사용할 키 쌍을 선택하세요.
   - 네트워크 설정: 필요에 따라 네트워크 설정을 편집하세요.
     - 원하는 VPC와 서브넷을 선택하세요.
     - 인스턴스에 공용 IP 주소가 있어야 하는지 여부를 지정합니다.
     - 콘솔 에이전트 인스턴스에 필요한 연결 방법(SSH, HTTP, HTTPS)을 활성화하는 보안 그룹 설정을 지정합니다.

"AWS에 대한 보안 그룹 규칙 보기" .

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

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

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

  AWS는 지정된 설정으로 콘솔 에이전트를 시작하고, 콘솔 에이전트는 약 10분 후에 실행됩니다.

설치에 실패하면 로그와 보고서를 보고 문제 해결에 도움을 받을 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

8. 콘솔 에이전트 가상 머신에 연결되어 있고 콘솔 에이전트의 URL이 있는 호스트에서 웹 브라우저를 엽니다.
9. 로그인 후 콘솔 에이전트를 설정하세요.
   a. 콘솔 에이전트와 연결할 콘솔 조직을 지정합니다.
   b. 시스템 이름을 입력하세요.
   c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

      표준 모드에서 콘솔을 사용하려면 제한 모드를 비활성화하세요. 보안 환경이 있고 콘솔 백엔드 서비스에서 이 계정의 연결을 끊으려는 경우에만 제한 모드를 활성화해야 합니다. 그렇다면,"제한 모드에서 NetApp Console 시작하기 위한 단계를 따르세요." .

   d. *시작하기*를 선택하세요.

결과

이제 콘솔 에이전트가 설치되고 콘솔 조직에 설정되었습니다.

웹 브라우저를 열고 이동하세요 "NetApp Console" 콘솔과 함께 콘솔 에이전트를 사용하려면 다음을 수행합니다.

콘솔 에이전트를 생성한 동일한 AWS 계정에 Amazon S3 버킷이 있는 경우, 시스템 페이지에 Amazon S3 작업 환경이 자동으로 표시됩니다. "NetApp Console 에서 S3 버킷을 관리하는 방법을 알아보세요."

AWS에 콘솔 에이전트를 수동으로 설치합니다.

AWS에서 실행되는 Linux 호스트에 콘솔 에이전트를 수동으로 설치할 수 있습니다. Linux 호스트에 콘솔 에이전트를 수동으로 설치하려면 호스트 요구 사항을 검토하고, 네트워킹을 설정하고, AWS 권한을 준비하고, 콘솔 에이전트를 설치한 다음, 준비한 권한을 제공해야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 호스트 요구 사항 검토

콘솔 에이전트 소프트웨어가 실행되는 호스트가 운영 체제, RAM 및 포트 요구 사항을 충족하는지 확인하십시오.

콘솔 에이전트는 UID와 GID 범위를 19000~19200으로 예약합니다. 이 범위는 고정되어 있으며 수정할 수 없습니다. 호스트의 타사 소프트웨어가 이 범위 내의 UID나 GID를 사용하는 경우 에이전트 설치가 실패합니다. NetApp 충돌을 피하기 위해 타사 소프트웨어가 없는 호스트를 사용할 것을 권장합니다.

전담 호스트

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

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

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

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

AWS EC2 인스턴스 유형

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

하이퍼바이저

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

운영 체제 및 컨테이너 요구 사항

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

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

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

키 쌍

콘솔 에이전트를 생성할 때 인스턴스와 함께 사용할 EC2 키 쌍을 선택해야 합니다.

IMDSv2를 사용할 때 **PUT** 응답 홉 제한

IMDSv2가 활성화된 경우(새 EC2 인스턴스의 기본값) PUT 응답 홉 제한을 3으로 설정하십시오. 그렇게 하지 않으면 에이전트 설정 중에 시스템에 UI 초기화 오류가 표시됩니다.

- "Amazon EC2 인스턴스에서 IMDSv2 사용 요구"
- "AWS 설명서: PUT 응답 홉 제한 변경"

2단계**: Podman** 또는 **Docker Engine** 설치

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

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

  지원되는 Podman 버전 보기 .

- Ubuntu에는 Docker 엔진이 필요합니다.

지원되는 Docker Engine 버전 보기 .

예 **1.** 단계

포드만

Podman을 설치하고 구성하려면 다음 단계를 따르세요.

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

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

단계

1. 호스트에 podman-docker 패키지가 설치되어 있다면 제거합니다.

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

2. Podman을 설치하세요.

   공식 Red Hat Enterprise Linux 저장소에서 Podman을 다운로드할 수 있습니다.

   a. Red Hat Enterprise Linux 9.6의 경우:

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

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

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

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

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

   c. Red Hat Enterprise Linux 8의 경우:

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

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

3. podman.socket 서비스를 활성화하고 시작합니다.

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

4. python3를 설치합니다.

```
sudo dnf install python3
```

5. 시스템에 EPEL 저장소 패키지가 아직 없으면 설치하세요.

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

6. Red Hat Enterprise 9를 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

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

   +

   a. podman-compose 패키지 1.5.0을 설치합니다.

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

7. Red Hat Enterprise Linux 8을 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

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

   b. podman-compose 패키지 1.0.6을 설치합니다.

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

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

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

i. 다음 명령을 실행하여 networkBackend가 CNI로 설정되어 있는지 확인하세요.

```
podman info | grep networkBackend
```

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

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

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

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

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

v. Podman을 다시 시작하세요.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

도커 엔진

Docker Engine을 설치하려면 Docker 설명서를 따르세요.

단계

1. "Docker에서 설치 지침 보기"

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

2. Docker가 활성화되어 실행 중인지 확인하세요.

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

3단계**:** 네트워킹 설정

콘솔 에이전트가 하이브리드 클라우드의 리소스를 관리할 수 있도록 네트워크 위치가 다음 요구 사항을 충족하는지 확인하십시오.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

웹 기반 **NetApp Console** 사용할 때 컴퓨터에서 연결된 엔드포인트

웹 브라우저에서 콘솔에 액세스하는 컴퓨터는 여러 엔드포인트에 접속할 수 있어야 합니다. 콘솔 에이전트를 설정하고 콘솔을 일상적으로 사용하려면 콘솔을 사용해야 합니다.

"NetApp 콘솔을 위한 네트워킹 준비" .

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 리소스를 관리합니다. 엔드포인트는 AWS 지역에 따라 달라집니다. "자세한 내용은 AWS 설명서를 참조하세요."
Amazon FsX for NetApp ONTAP: • api.workloads.netapp.com	웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.

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

프록시 서버

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

- IP 주소
- 신임장
- HTTPS 인증서

포트

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

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

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

NTP 활성화

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

4단계**:** 콘솔에 대한 **AWS** 권한 설정

다음 옵션 중 하나를 사용하여 NetApp Console 에 AWS 권한을 부여하십시오.

- 옵션 1: IAM 정책을 만들고 EC2 인스턴스와 연결할 수 있는 IAM 역할에 정책을 연결합니다.
- 옵션 2: 필요한 권한이 있는 IAM 사용자의 AWS 액세스 키를 콘솔에 제공합니다.

콘솔에 대한 권한을 준비하려면 다음 단계를 따르세요.

IAM 역할

단계

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

      사용하려는 NetApp 데이터 서비스에 따라 두 번째 정책을 만들어야 할 수도 있습니다. 표준 지역의 경우 권한은 두 가지 정책에 걸쳐 분산됩니다. AWS의 관리형 정책에는 최대 문자 크기 제한이 있으므로 두 개의 정책이 필요합니다. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요." .
3. IAM 역할을 만듭니다.
   a. *역할 > 역할 만들기*를 선택합니다.
   b. *AWS 서비스 > EC2*를 선택합니다.
   c. 방금 만든 정책을 첨부하여 권한을 추가합니다.
   d. 나머지 단계를 완료하여 역할을 만듭니다.

결과

콘솔 에이전트를 설치한 후 이제 EC2 인스턴스와 연결할 수 있는 IAM 역할이 생겼습니다.

AWS 액세스 키

단계

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

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

   표준 지역의 경우 권한은 두 가지 정책에 걸쳐 분산됩니다. AWS의 관리형 정책에는 최대 문자 크기 제한이 있으므로 두 개의 정책이 필요합니다. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요." .
3. IAM 사용자에게 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"
4. 콘솔 에이전트를 설치한 후 NetApp Console 에 추가할 수 있는 액세스 키가 사용자에게 있는지 확인하세요.

결과

이제 필요한 권한이 있는 IAM 사용자와 콘솔에 제공할 수 있는 액세스 키가 생겼습니다.

5단계**:** 콘솔 에이전트 설치

필수 조건을 모두 충족한 후에는 Linux 호스트에 소프트웨어를 수동으로 설치하십시오.

시작하기 전에

다음 사항이 있어야 합니다.

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

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

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

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

이 작업에 관하여

설치 후, 새로운 버전이 나오면 콘솔 에이전트가 자동으로 업데이트됩니다.

단계

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

   ```
   unset http_proxy
   unset https_proxy
   ```

   이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

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

     에이전트 설치 파일 다운로드 또는 파일 URL 다운로드를 선택하십시오.

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

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

   여기서 <버전>은 다운로드한 콘솔 에이전트의 버전입니다.

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

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

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

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

+

다음은 CA 서명 인증서로 명시적 프록시 서버를 구성하는 예입니다.

+

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

+
`--proxy` 다음 형식 중 하나를 사용하여 Console 에이전트가 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 위와 같이 \의 ASCII 코드를 사용해야 합니다. **Console** 에이전트는 **@** 문자가 포함된 사용자 이름이나 암호를 지원하지 않습니다. 암호에 다음 특수 문자(& 또는 !)가 포함된 경우 백슬래시를 앞에 붙여 해당 특수 문자를 이스케이프해야 합니다.

+ 예를 들면:

+ http://bxpproxyuser:netapp1\!@address:3128

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

   a. 콘솔 에이전트 가상 머신에 SSH를 실행합니다.

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

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

      예를 들어:

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

a. 콘솔 에이전트 가상 머신을 재부팅합니다.

2. 설치가 완료될 때까지 기다리세요.

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

설치에 실패하면 설치 보고서와 로그를 보고 문제를 해결하는 데 도움이 됩니다."설치 문제를 해결하는 방법을 알아보세요."

1. 콘솔 에이전트 가상 머신에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

https://ipaddress

2. 로그인 후 콘솔 에이전트를 설정하세요.

a. 콘솔 에이전트와 연결할 조직을 지정합니다.

b. 시스템 이름을 입력하세요.

c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

이 단계에서는 표준 모드에서 콘솔을 사용하는 방법을 설명하므로 제한 모드를 비활성화해야 합니다. 보안 환경이 있고 백엔드 서비스에서 이 계정의 연결을 끊으려는 경우에만 제한 모드를 활성화해야 합니다. 그렇다면 ,"제한 모드에서 NetApp Console 시작하기 위한 단계를 따르세요." .

d. *시작하기*를 선택하세요.

콘솔 에이전트를 생성한 동일한 AWS 계정에 Amazon S3 버킷이 있는 경우, 시스템 페이지에 Amazon S3 스토리지 시스템이 자동으로 표시됩니다. "NetApp ConsoleP에서 S3 버킷을 관리하는 방법을 알아보세요."

6단계**: NetApp Console** 에 권한 제공

콘솔 에이전트를 설치한 후에는 콘솔 에이전트가 AWS에서 데이터 및 스토리지 인프라를 관리할 수 있도록 설정한 AWS 권한을 제공해야 합니다.

IAM 역할

생성한 IAM 역할을 콘솔 에이전트 EC2 인스턴스에 연결합니다.

단계

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

로 가다 "NetApp Console" 콘솔 에이전트를 사용하려면.

AWS 액세스 키

필요한 권한이 있는 IAM 사용자의 AWS 액세스 키를 콘솔에 제공합니다.

단계

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

로 가다 "NetApp Console" 콘솔 에이전트를 사용하려면.

하늘빛

Azure의 콘솔 에이전트 설치 옵션

Azure에서 콘솔 에이전트를 만드는 방법에는 여러 가지가 있습니다. 가장 일반적인 방법은 NetApp Console 에서 직접 실행하는 것입니다.

다음과 같은 설치 옵션을 사용할 수 있습니다.

- "NetApp Console 에서 직접 콘솔 에이전트를 만듭니다."(이것은 표준 옵션입니다)

  이 작업을 수행하면 선택한 VNet에서 Linux와 콘솔 에이전트 소프트웨어를 실행하는 VM이 시작됩니다.

- "Azure Marketplace에서 콘솔 에이전트 만들기"

이 작업을 수행하면 Linux와 콘솔 에이전트 소프트웨어가 실행되는 VM도 시작되지만 배포는 콘솔이 아닌 Azure Marketplace에서 직접 시작됩니다.

- "자신의 Linux 호스트에 소프트웨어를 다운로드하고 수동으로 설치하세요."

선택하는 설치 옵션은 설치를 준비하는 방법에 영향을 미칩니다. 여기에는 Azure에서 리소스를 인증하고 관리하는 데 필요한 권한을 콘솔 에이전트에 제공하는 방법이 포함됩니다.

NetApp Console 에서 Azure에 콘솔 에이전트 만들기

NetApp Console 에서 Azure에 콘솔 에이전트를 만들려면 네트워킹을 설정하고, Azure 권한을 준비한 다음 콘솔 에이전트를 만들어야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 네트워킹 설정

콘솔 에이전트를 설치하려는 네트워크 위치가 다음 요구 사항을 지원하는지 확인하세요. 이러한 요구 사항을 통해 콘솔 에이전트는 하이브리드 클라우드 리소스를 관리할 수 있습니다.

Azure 지역

Cloud Volumes ONTAP 사용하는 경우 콘솔 에이전트는 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 지역이나 "Azure 지역 쌍" Cloud Volumes ONTAP 시스템용. 이 요구 사항은 Cloud Volumes ONTAP 과 연결된 스토리지 계정 간에 Azure Private Link 연결이 사용되도록 보장합니다.

"Cloud Volumes ONTAP Azure Private Link를 사용하는 방법 알아보기"

VNet 및 서브넷

콘솔 에이전트를 만들 때는 에이전트가 상주해야 하는 VNet과 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Azure 공용 지역의 리소스를 관리합니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Azure China 지역의 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.

엔드포인트	목적
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

NetApp 콘솔에서 연결된 엔드포인트

SaaS 계층을 통해 제공되는 웹 기반 NetApp Console 사용하면 여러 엔드포인트에 연결하여 데이터 관리 작업을 완료할 수 있습니다. 여기에는 콘솔에서 콘솔 에이전트를 배포하기 위해 연결된 엔드포인트가 포함됩니다.

"NetApp 콘솔에서 연결된 엔드포인트 목록 보기" .

프록시 서버

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

- IP 주소
- 신임장
- HTTPS 인증서

포트

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

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

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

NTP 활성화

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

콘솔 에이전트를 만든 후 이 네트워킹 요구 사항을 구현해야 합니다.

2단계**:** 콘솔 에이전트 배포 정책**(**사용자 지정 역할**)** 만들기

Azure에서 콘솔 에이전트를 배포할 수 있는 권한이 있는 사용자 지정 역할을 만들어야 합니다.

Azure 계정이나 Microsoft Entra 서비스 주체에 할당할 수 있는 Azure 사용자 지정 역할을 만듭니다. 콘솔은 Azure에 인증하고 이러한 권한을 사용하여 사용자를 대신하여 콘솔 에이전트를 만듭니다.

콘솔은 Azure에 콘솔 에이전트 VM을 배포하고 다음을 활성화합니다. "시스템 할당 관리 ID" , 필요한 역할을 생성하고 이를 VM에 할당합니다. "콘솔이 권한을 사용하는 방식을 검토하세요." .

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

단계

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

이 사용자 지정 역할에는 콘솔에서 Azure의 콘솔 에이전트 VM을 시작하는 데 필요한 권한만 포함되어 있습니다. 다른 상황에서는 이 정책을 사용하지 마세요. 콘솔에서 콘솔 에이전트를 만들면 콘솔 에이전트 VM에 새로운 권한 집합이 적용되어 콘솔 에이전트가 Azure 리소스를 관리할 수 있게 됩니다.

```
{
  "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. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON을 수정합니다.

   예

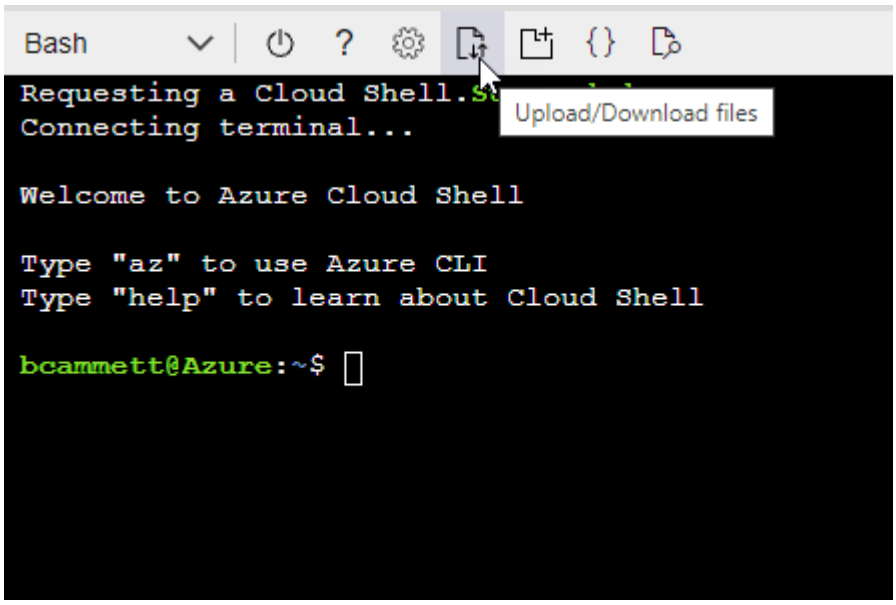
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
]
```

3. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 만듭니다.

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

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

   b. JSON 파일을 업로드합니다.



   c. 다음 Azure CLI 명령을 입력하세요.

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

이제 _Azure SetupAsService_라는 사용자 지정 역할이 생겼습니다. 이 사용자 지정 역할은 사용자 계정이나 서비스 주체에 적용할 수 있습니다.

3단계**:** 인증 설정

콘솔에서 콘솔 에이전트를 만들 때 콘솔이 Azure에 인증하고 VM을 배포할 수 있도록 하는 로그인을 제공해야 합니다. 두 가지 옵션이 있습니다.

1. 메시지가 표시되면 Azure 계정으로 Sign in . 이 계정에는 특정 Azure 권한이 있어야 합니다. 이는 기본 옵션입니다.
2. Microsoft Entra 서비스 주체에 대한 세부 정보를 제공합니다. 이 서비스 주체에도 특정 권한이 필요합니다.

콘솔에서 사용할 인증 방법 중 하나를 준비하려면 다음 단계를 따르세요.

Azure 계정

콘솔에서 콘솔 에이전트를 배포할 사용자에게 사용자 지정 역할을 할당합니다.

단계

1. Azure Portal에서 구독 서비스를 열고 사용자의 구독을 선택합니다.
2. *액세스 제어(IAM)*를 클릭합니다.
3. 추가 > *역할 할당 추가*를 클릭한 다음 권한을 추가합니다.
   a. **Azure SetupAsService** 역할을 선택하고 *다음*을 클릭합니다.

      Azure SetupAsService는 Azure의 콘솔 에이전트 배포 정책에 제공된 기본 이름입니다. 역할에 다른 이름을 선택한 경우 해당 이름을 대신 선택하세요.

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

서비스 주체

Azure 계정으로 로그인하는 대신, 필요한 권한이 있는 Azure 서비스 주체의 자격 증명을 콘솔에 제공할 수 있습니다.

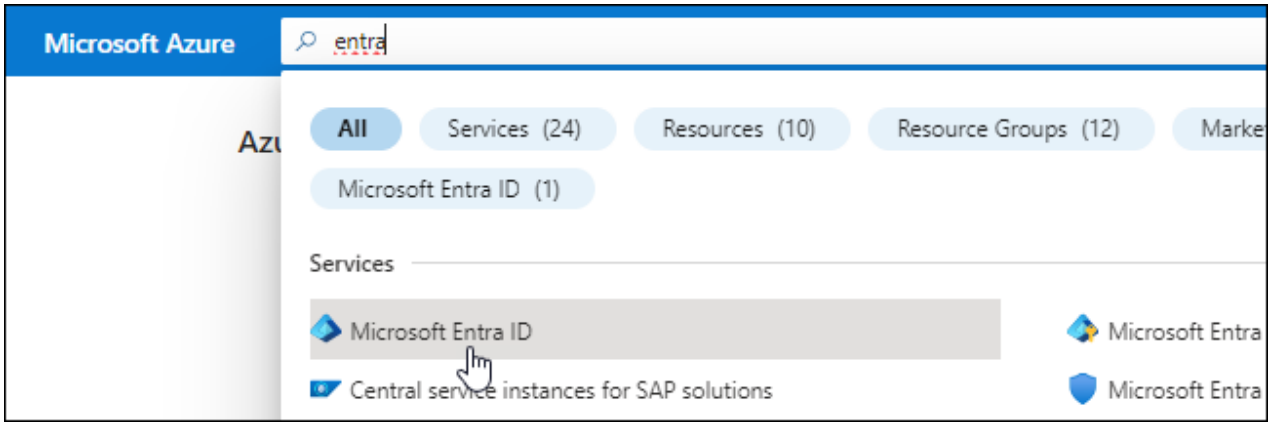
Microsoft Entra ID에서 서비스 주체를 만들고 설정하고 콘솔에 필요한 Azure 자격 증명을 얻습니다.

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

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

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

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



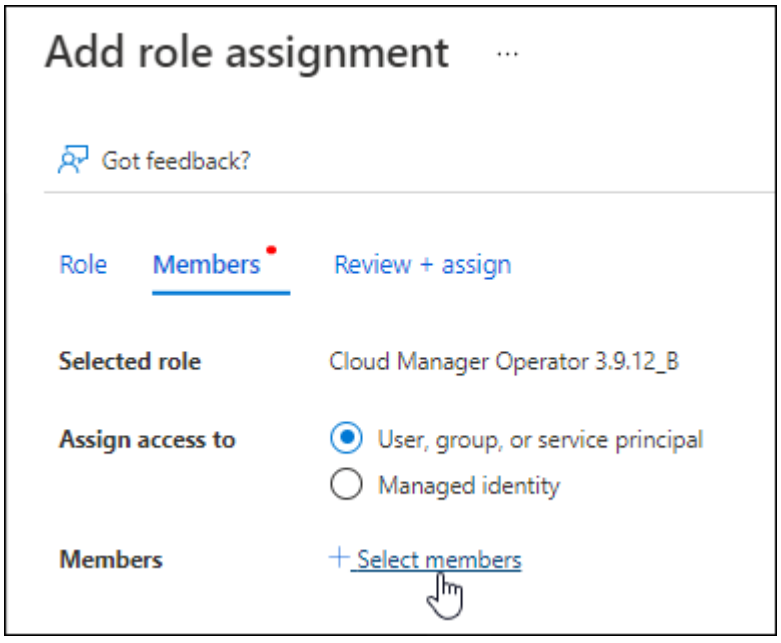
3. 메뉴에서 *앱 등록*을 선택하세요.
4. *신규 등록*을 선택하세요.

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

   AD 애플리케이션과 서비스 주체를 생성했습니다.

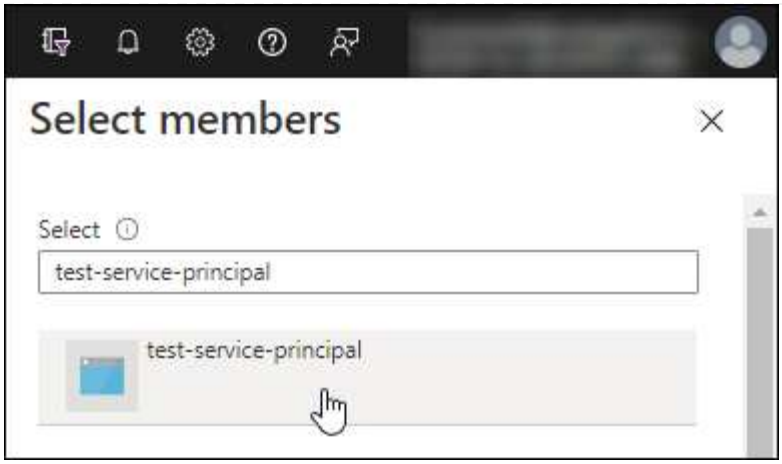
애플리케이션에 사용자 정의 역할 할당

1. Azure Portal에서 구독 서비스를 엽니다.
2. 구독을 선택하세요.
3. *액세스 제어(IAM) > 추가 > 역할 할당 추가*를 클릭합니다.
4. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 클릭합니다.
5. 멤버 탭에서 다음 단계를 완료하세요.
   a. *사용자, 그룹 또는 서비스 주체*를 선택된 상태로 유지합니다.
   b. *멤버 선택*을 클릭하세요.



   c. 애플리케이션 이름을 검색하세요.

      예를 들면 다음과 같습니다.



a. 해당 애플리케이션을 선택하고 *선택*을 클릭하세요.

b. *다음*을 클릭하세요.

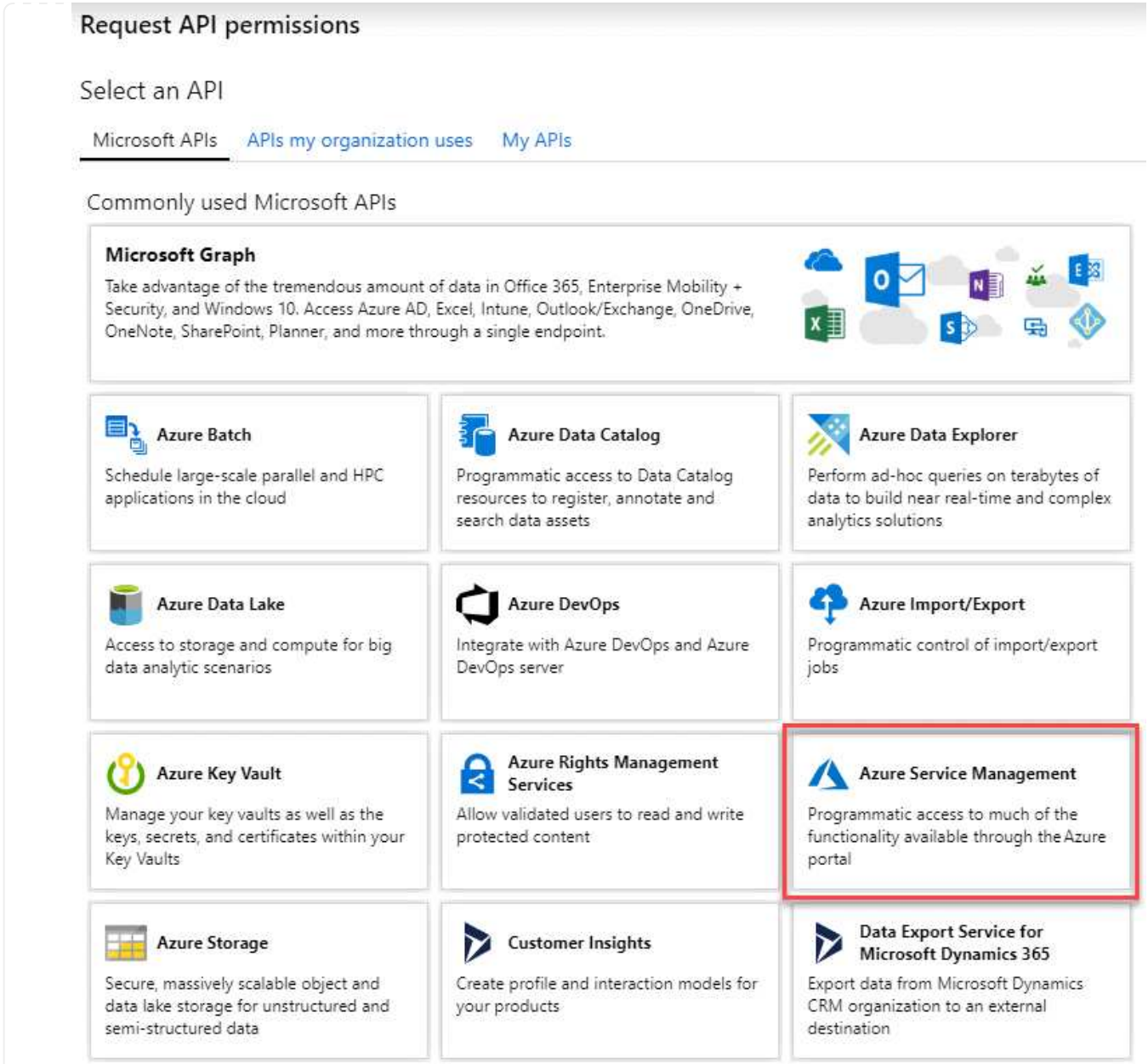
6. *검토 + 할당*을 클릭하세요.

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

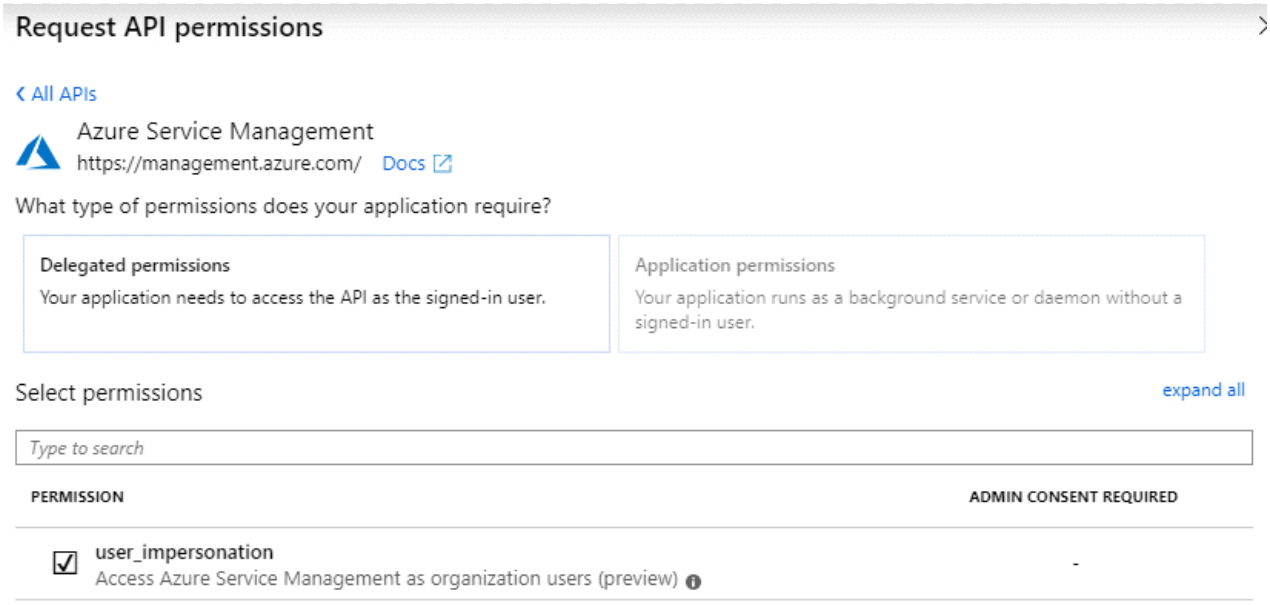
   여러 Azure 구독의 리소스를 관리하려면 각 구독에 서비스 주체를 바인딩해야 합니다. 예를 들어, 콘솔을 사용하면 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한 추가

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

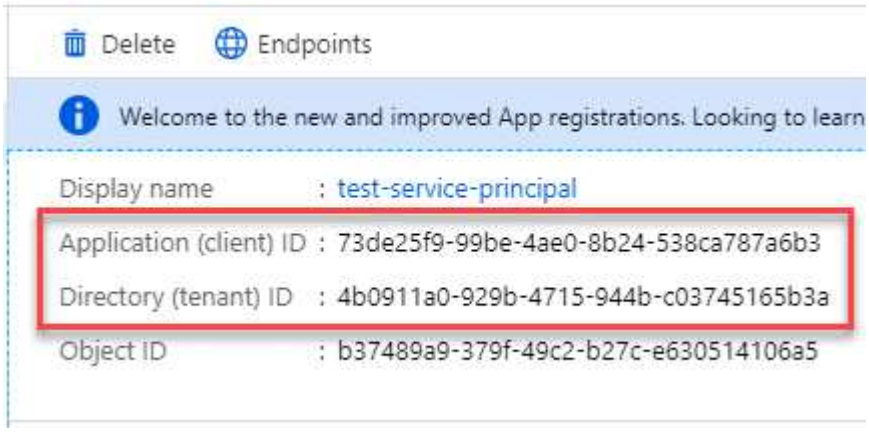


4. *조직 사용자로 Azure Service Management에 액세스*를 선택한 다음 *권한 추가*를 선택합니다.



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

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



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

클라이언트 비밀을 생성하세요

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

결과

이제 서비스 주체가 설정되었고 애플리케이션(클라이언트) ID, 디렉토리(테넌트) ID 및 클라이언트 비밀번호 값을 복사했어야 합니다. 콘솔 에이전트를 생성할 때 콘솔에 이 정보를 입력해야 합니다.

4단계: 콘솔 에이전트 만들기

NetApp Console 에서 직접 콘솔 에이전트를 만듭니다.

이 작업에 관하여

- 콘솔에서 콘솔 에이전트를 만들면 기본 구성을 사용하여 Azure에 가상 머신이 배포됩니다. 콘솔 에이전트를 만든 후에는 CPU나 RAM이 적은 더 작은 VM 인스턴스로 전환하지 마세요. "콘솔 에이전트의 기본 구성에 대해 알아보세요" .
- 콘솔이 콘솔 에이전트를 배포하면 사용자 지정 역할을 만들고 이를 콘솔 에이전트 VM에 할당합니다. 이 역할에는 콘솔 에이전트가 Azure 리소스를 관리할 수 있는 권한이 포함되어 있습니다. 이후 릴리스에서 새로운 권한이 추가되므로 역할이 최신 상태로 유지되도록 해야 합니다. "콘솔 에이전트의 사용자 정의 역할에 대해 자세히 알아보세요." .

시작하기 전에

다음 사항이 있어야 합니다.

- Azure 구독.
- 선택한 Azure 지역의 VNet 및 서브넷.
- 조직에서 모든 발신 인터넷 트래픽에 프록시가 필요한 경우 프록시 서버에 대한 세부 정보:
  - IP 주소
  - 신임장
  - HTTPS 인증서
- 콘솔 에이전트 가상 머신에 대한 인증 방법을 사용하려면 SSH 공개 키가 필요합니다. 인증 방법에 대한 또 다른 옵션은 비밀번호를 사용하는 것입니다.

  "Azure에서 Linux VM에 연결하는 방법에 대해 알아보세요."

- 콘솔에서 콘솔 에이전트에 대한 Azure 역할을 자동으로 생성하지 않으려면 직접 만들어야 합니다."이 페이지의 정책을 사용하여" .

  이러한 권한은 콘솔 에이전트 자체에 대한 것입니다. 이는 이전에 콘솔 에이전트 VM을 배포하기 위해 설정한 것과 다른 권한 집합입니다.

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 *에이전트 배포 > Azure*를 선택합니다.
3. 검토 페이지에서 에이전트 배포에 필요한 요구 사항을 검토합니다. 해당 요구 사항도 이 페이지의 위에 자세히 설명되어 있습니다.
4. 가상 머신 인증 페이지에서 Azure 권한을 설정하는 방법과 일치하는 인증 옵션을 선택합니다.
   - Microsoft 계정에 로그인하려면 *로그인*을 선택하세요. 이 계정에는 필요한 권한이 있어야 합니다.

     이 양식은 Microsoft에서 소유하고 호스팅합니다. 귀하의 자격 증명은 NetApp 에 제공되지 않습니다.

     이미 Azure 계정에 로그인한 경우 콘솔은 자동으로 해당 계정을 사용합니다. 여러 개의 계정이 있는 경우 먼저 로그아웃하여 올바른 계정을 사용하고 있는지 확인해야 할 수도 있습니다.
   - 필수 권한을 부여하는 Microsoft Entra 서비스 주체에 대한 정보를 입력하려면 *Active Directory 서비스 주체*를 선택하세요.
     - 애플리케이션(클라이언트) ID
     - 디렉토리(테넌트) ID
     - 클라이언트 비밀번호

   서비스 주체에 대한 이러한 값을 얻는 방법을 알아보세요. .
5. 가상 머신 인증 페이지에서 Azure 구독, 위치, 새 리소스 그룹 또는 기존 리소스 그룹을 선택한 다음, 만들고 있는 콘솔 에이전트 가상 머신에 대한 인증 방법을 선택합니다.

   가상 머신의 인증 방법은 비밀번호나 SSH 공개 키가 될 수 있습니다.

   "Azure에서 Linux VM에 연결하는 방법에 대해 알아보세요."
6. 세부 정보 페이지에서 에이전트의 이름을 입력하고 태그를 지정하고 콘솔에서 필요한 권한이 있는 새 역할을 생성할지 아니면 설정한 기존 역할을 선택할지 선택합니다."필요한 권한" .

   이 역할과 연결된 Azure 구독을 선택할 수 있습니다. 선택한 각 구독은 해당 구독의 리소스를 관리할 수 있는 콘솔 에이전트 권한을 제공합니다(예: Cloud Volumes ONTAP).
7. 네트워크 페이지에서 VNet과 서브넷을 선택하고, 공용 IP 주소를 활성화할지 여부를 지정하고, 선택적으로 프록시 구성을 지정합니다.
   - 보안 그룹 페이지에서 새 보안 그룹을 만들지, 아니면 필요한 인바운드 및 아웃바운드 규칙을 허용하는 기존 보안 그룹을 선택할지 선택합니다.

     "Azure에 대한 보안 그룹 규칙 보기" .
8. 선택 사항을 검토하여 설정이 올바른지 확인하세요.
   a. 에이전트 구성 검증 확인란은 배포 시 콘솔에서 네트워크 연결 요구 사항을 검증하도록 기본적으로 선택되어 있습니다. 콘솔에서 에이전트를 배포하지 못하면 문제 해결에 도움이 되는 보고서가 제공됩니다. 배포가 성공하면 보고서는 제공되지 않습니다.

아직도 사용 중이라면"이전 종료점" 에이전트 업그레이드에 사용되면 유효성 검사가 오류로 인해 실패합니다. 이를 방지하려면 유효성 검사를 건너뛰려면 확인란의 선택을 취소하세요.

9. *추가*를 선택하세요.

콘솔은 약 10분 안에 에이전트를 준비합니다. 프로세스가 완료될 때까지 페이지에 머물러주세요.

결과

프로세스가 완료되면 콘솔 에이전트를 콘솔에서 사용할 수 있습니다.

배포에 실패하면 콘솔에서 보고서와 로그를 다운로드하여 문제를 해결할 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

콘솔 에이전트를 만든 동일한 Azure 계정에 Azure Blob Storage가 있는 경우 Azure Blob Storage가 시스템 페이지에 자동으로 표시됩니다. "NetApp Console 에서 Azure Blob 스토리지를 관리하는 방법을 알아보세요."

Azure Marketplace에서 콘솔 에이전트 만들기

Azure Marketplace에서 직접 Azure에서 콘솔 에이전트를 만들 수 있습니다. Azure Marketplace에서 콘솔 에이전트를 만들려면 네트워킹을 설정하고, Azure 권한을 준비하고, 인스턴스 요구 사항을 검토한 다음 콘솔 에이전트를 만들어야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토"콘솔 에이전트 제한 사항" .

1단계**:** 네트워킹 설정

콘솔 에이전트를 설치하려는 네트워크 위치가 다음 요구 사항을 지원하는지 확인하세요. 이러한 요구 사항을 충족하면 콘솔 에이전트가 하이브리드 클라우드의 리소스를 관리할 수 있습니다.

Azure 지역

Cloud Volumes ONTAP 사용하는 경우 콘솔 에이전트는 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 지역이나 "Azure 지역 쌍" Cloud Volumes ONTAP 시스템용. 이 요구 사항은 Cloud Volumes ONTAP 과 연결된 스토리지 계정 간에 Azure Private Link 연결이 사용되도록 보장합니다.

"Cloud Volumes ONTAP Azure Private Link를 사용하는 방법 알아보기"

VNet 및 서브넷

콘솔 에이전트를 만들 때는 에이전트가 상주해야 하는 VNet과 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Azure 공용 지역의 리소스를 관리합니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Azure China 지역의 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.

엔드포인트	목적
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

프록시 서버

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

- IP 주소
- 신임장
- HTTPS 인증서

포트

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

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

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

NTP 활성화

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

콘솔 에이전트를 만든 후 네트워킹 요구 사항을 구현합니다.

2단계**: VM** 요구 사항 검토

콘솔 에이전트를 생성할 때 다음 요구 사항을 충족하는 가상 머신 유형을 선택하세요.

CPU

8개 코어 또는 8개 vCPU

숫양

32GB

Azure VM 크기

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

3단계**:** 권한 설정

다음과 같은 방법으로 권한을 부여할 수 있습니다.

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

콘솔에 대한 권한을 설정하려면 다음 단계를 따르세요.

사용자 정의 역할

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

단계

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

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

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

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

   예

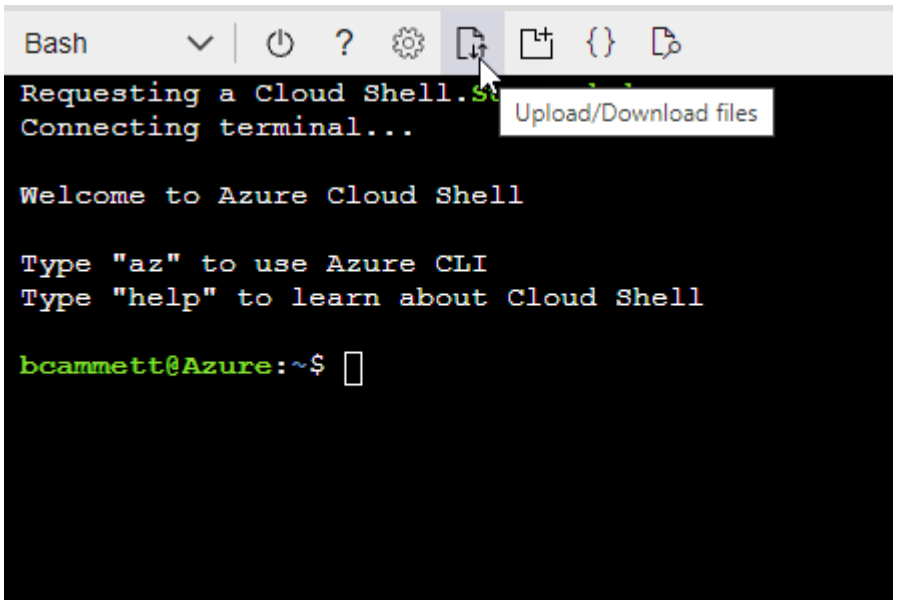
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ]
   ```

4. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 만듭니다.

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

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

   b. JSON 파일을 업로드합니다.



c. Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

서비스 주체

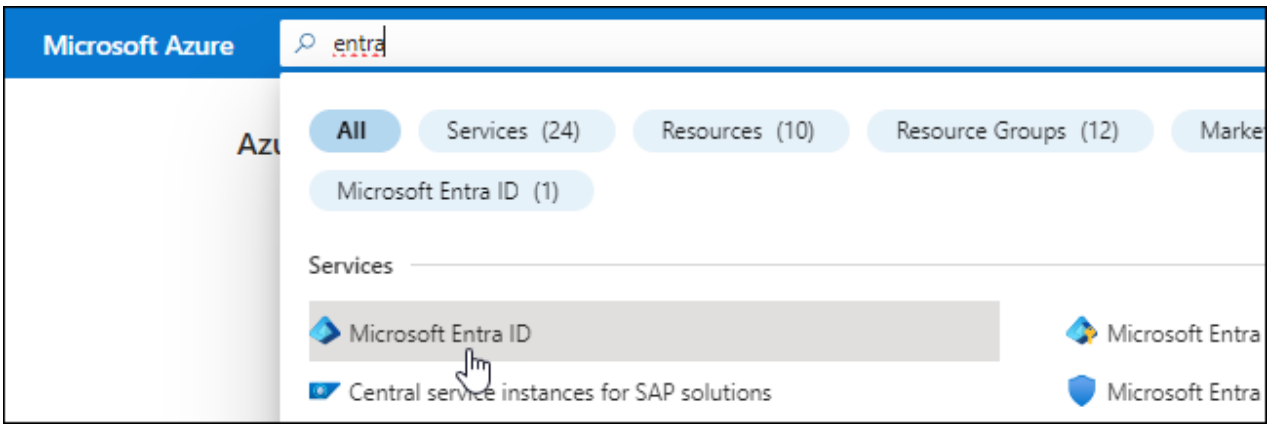
Microsoft Entra ID에서 서비스 주체를 만들고 설정하고 콘솔에 필요한 Azure 자격 증명을 얻습니다.

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

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

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

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



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

   AD 애플리케이션과 서비스 주체를 생성했습니다.

역할에 애플리케이션 할당

1. 사용자 정의 역할 만들기:

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

   a. 내용을 복사하세요"콘솔 에이전트에 대한 사용자 정의 역할 권한" JSON 파일에 저장합니다.

b. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

사용자가 Cloud Volumes ONTAP 시스템을 생성할 각 Azure 구독에 대한 ID를 추가해야 합니다.

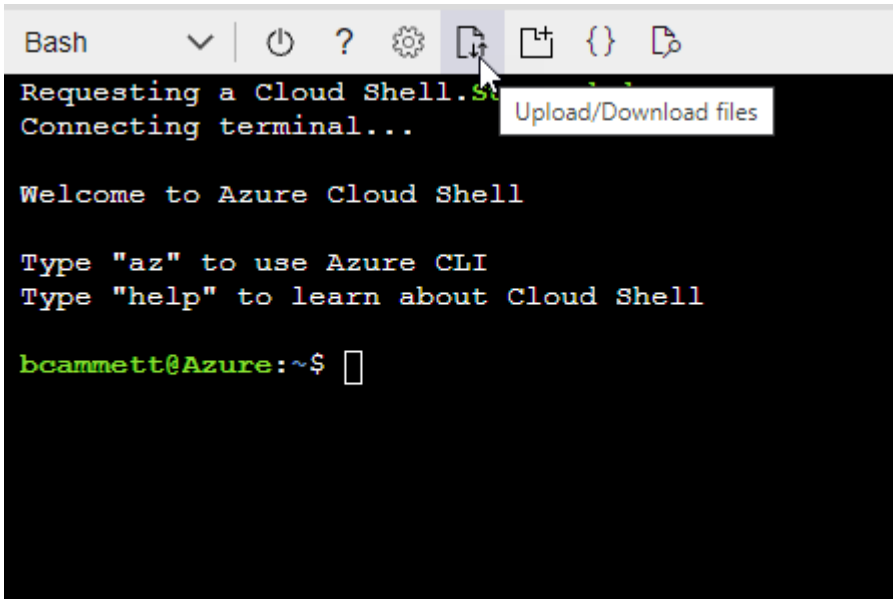
예

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

c. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 만듭니다.

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

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



- Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

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

2. 역할에 애플리케이션을 할당합니다.

a. Azure Portal에서 구독 서비스를 엽니다.

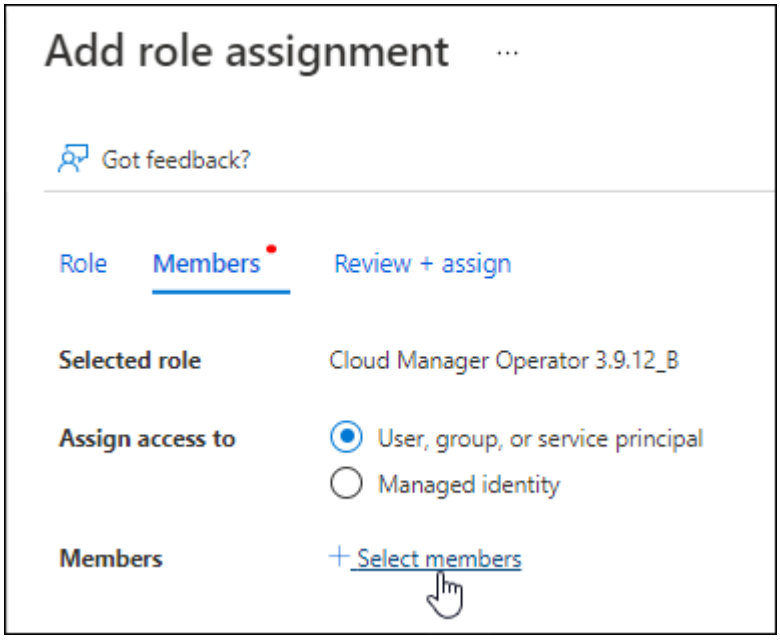
b. 구독을 선택하세요.

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

d. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.

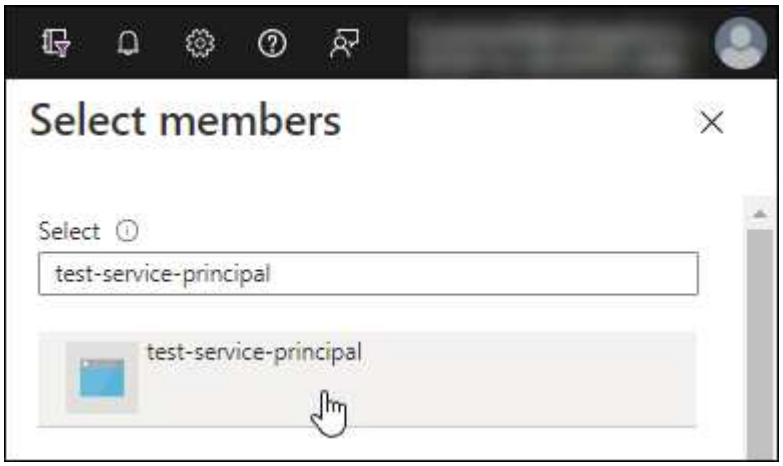
e. 멤버 탭에서 다음 단계를 완료하세요.

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



- 애플리케이션 이름을 검색하세요.

  예를 들면 다음과 같습니다.



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

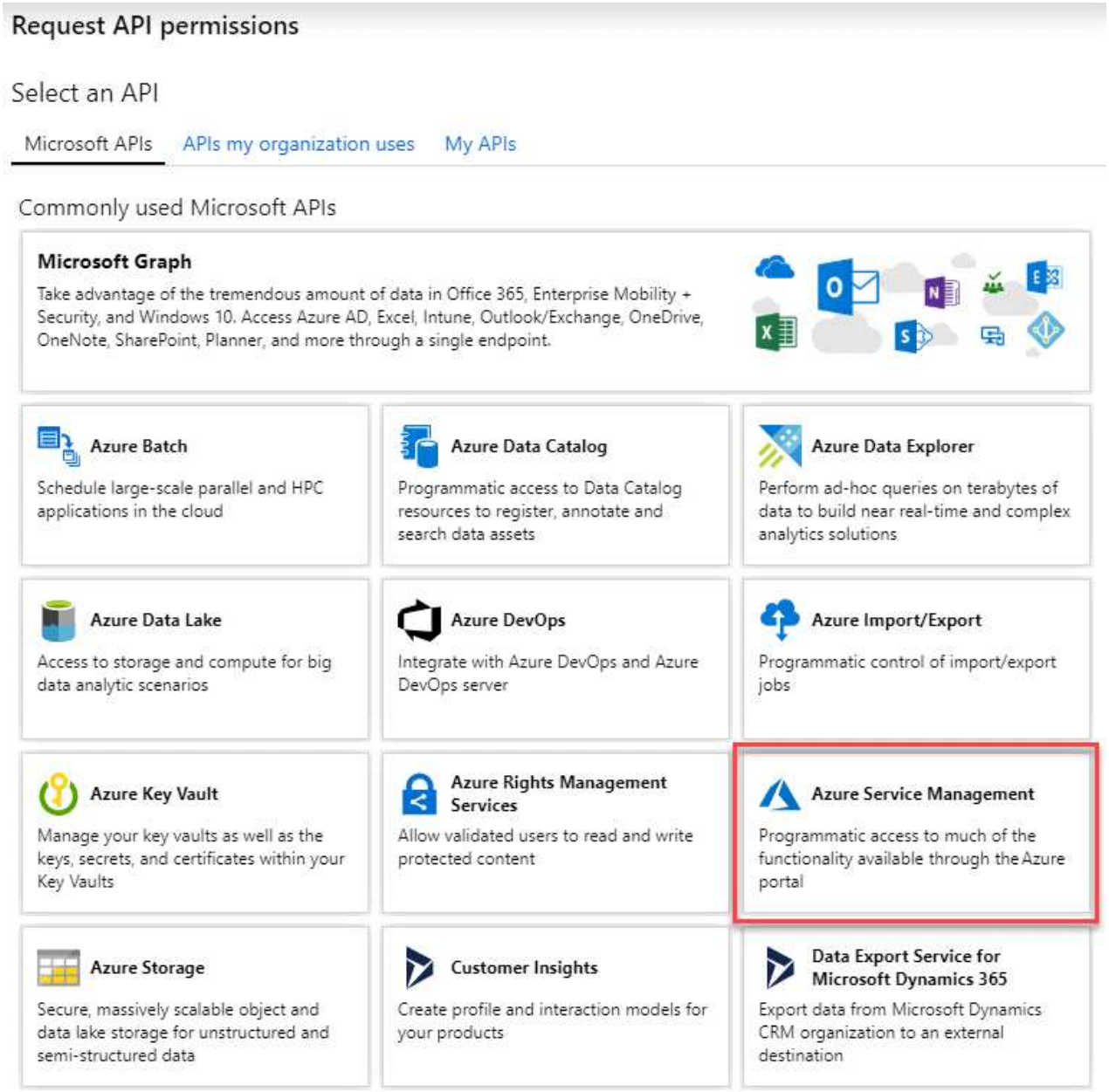
f. *검토 + 할당*을 선택하세요.

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

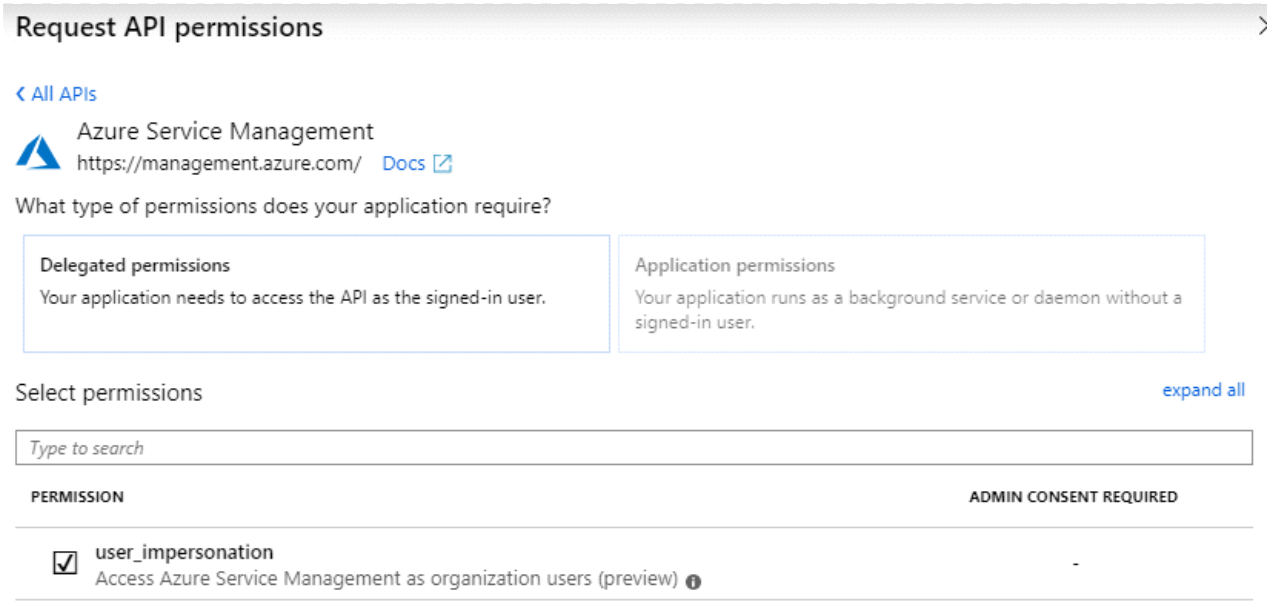
여러 Azure 구독에서 Cloud Volumes ONTAP 배포하려면 각 구독에 서비스 주체를 바인딩해야 합니다. NetApp Console 에서 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한 추가

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

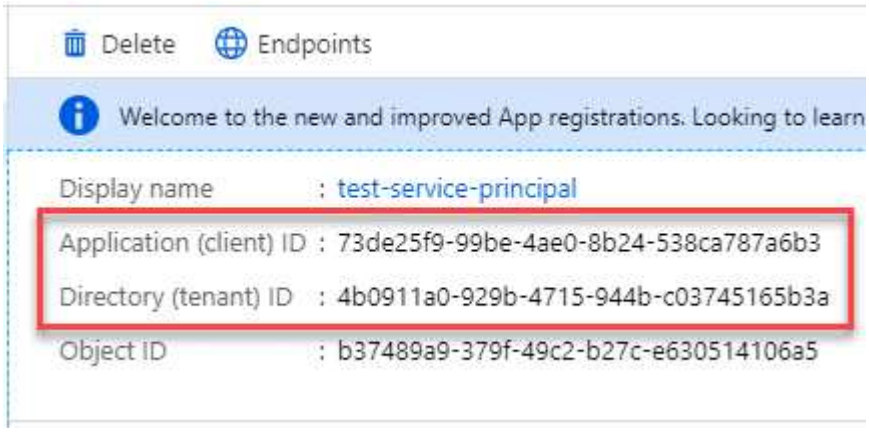


4. *조직 사용자로 Azure Service Management에 액세스*를 선택한 다음 *권한 추가*를 선택합니다.



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

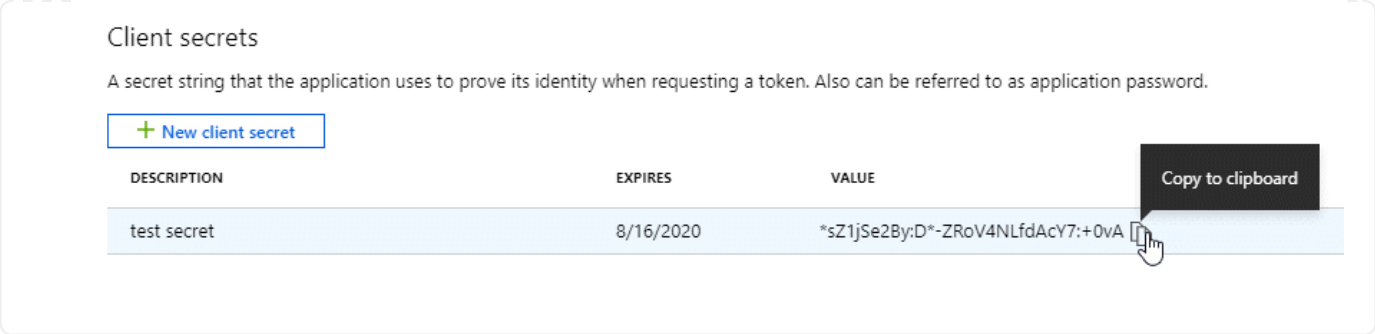
1. **Microsoft Entra ID** 서비스에서 *앱 등록*을 선택하고 애플리케이션을 선택합니다.
2. *애플리케이션(클라이언트) ID*와 *디렉토리(테넌트) ID*를 복사합니다.



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

클라이언트 비밀을 생성하세요

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



4단계**:** 콘솔 에이전트 만들기

Azure Marketplace에서 직접 콘솔 에이전트를 시작합니다.

이 작업에 관하여

Azure Marketplace에서 콘솔 에이전트를 만들면 기본 구성으로 가상 머신이 설정됩니다. "콘솔 에이전트의 기본 구성에 대해 알아보세요" .

시작하기 전에

다음 사항이 있어야 합니다.

- Azure 구독.
- 선택한 Azure 지역의 VNet 및 서브넷.
- 조직에서 모든 발신 인터넷 트래픽에 프록시가 필요한 경우 프록시 서버에 대한 세부 정보:
  - IP 주소
  - 신임장
  - HTTPS 인증서
- 콘솔 에이전트 가상 머신에 대한 인증 방법을 사용하려면 SSH 공개 키가 필요합니다. 인증 방법에 대한 또 다른 옵션은 비밀번호를 사용하는 것입니다.

  "Azure에서 Linux VM에 연결하는 방법에 대해 알아보세요."

- 콘솔에서 콘솔 에이전트에 대한 Azure 역할을 자동으로 생성하지 않으려면 직접 만들어야 합니다."이 페이지의 정책을 사용하여" .

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

단계

1. Azure Marketplace의 NetApp Console 에이전트 VM 페이지로 이동합니다.

   "상업 지역을 위한 Azure Marketplace 페이지"

2. *지금 받기*를 선택한 다음 *계속*을 선택하세요.
3. Azure Portal에서 *만들기*를 선택하고 단계에 따라 가상 머신을 구성합니다.

   VM을 구성할 때 다음 사항에 유의하세요.

- **VM** 크기: CPU 및 RAM 요구 사항을 충족하는 VM 크기를 선택하세요. Standard_D8s_v3을 권장합니다.
- 디스크: 콘솔 에이전트는 HDD 또는 SSD 디스크를 사용하면 최적의 성능을 발휘할 수 있습니다.
- 네트워크 보안 그룹: 콘솔 에이전트에는 SSH, HTTP, HTTPS를 사용하는 인바운드 연결이 필요합니다.

  "Azure에 대한 보안 그룹 규칙 보기" .

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

  이 설정은 관리되는 ID를 통해 콘솔 에이전트 가상 머신이 자격 증명을 제공하지 않고도 Microsoft Entra ID로 자신을 식별할 수 있기 때문에 중요합니다. "Azure 리소스에 대한 관리 ID에 대해 자세히 알아보세요." .

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

   Azure는 지정된 설정으로 가상 머신을 배포합니다. 약 10분 안에 가상 머신과 콘솔 에이전트 소프트웨어가 실행되는 것을 볼 수 있습니다.

   설치에 실패하면 로그와 보고서를 보고 문제 해결에 도움을 받을 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

5. 콘솔 에이전트 가상 머신에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

   https://ipaddress

6. 로그인 후 콘솔 에이전트를 설정하세요.
   a. 콘솔 에이전트와 연결할 콘솔 조직을 지정합니다.
   b. 시스템 이름을 입력하세요.
   c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

      표준 모드에서 콘솔을 사용하려면 제한 모드를 비활성화하세요. 보안 환경이 있고 콘솔 백엔드 서비스에서 이 계정의 연결을 끊으려는 경우에만 제한 모드를 활성화해야 합니다. 그렇다면,"제한 모드에서 콘솔을 시작하려면 다음 단계를 따르세요." .

   d. *시작하기*를 선택하세요.

결과

이제 콘솔 에이전트를 설치하고 콘솔 조직에 맞게 설정했습니다.

콘솔 에이전트를 만든 동일한 Azure 구독에 Azure Blob 저장소가 있는 경우 시스템 페이지에 Azure Blob 저장소 시스템이 자동으로 표시됩니다. "콘솔에서 Azure Blob 저장소를 관리하는 방법을 알아보세요."

5단계**:** 콘솔 에이전트에 권한 제공

이제 콘솔 에이전트를 만들었으므로 이전에 설정한 권한을 제공해야 합니다. 권한을 제공하면 콘솔 에이전트가 Azure에서 데이터 및 스토리지 인프라를 관리할 수 있습니다.

사용자 정의 역할

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

단계

1. Azure Portal에서 구독 서비스를 열고 구독을 선택합니다.

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

   "Microsoft Azure 설명서: Azure RBAC 범위 이해"

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

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

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

다음은 무엇인가요**?**

로 가다 "NetApp Console" 콘솔 에이전트를 사용하려면.

서비스 주체

단계

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

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

결과

이제 콘솔에는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한이 있습니다.

Azure에 콘솔 에이전트를 수동으로 설치합니다.

자신의 Linux 호스트에 콘솔 에이전트를 수동으로 설치하려면 호스트 요구 사항을 검토하고, 네트워킹을 설정하고, Azure 권한을 준비하고, 콘솔 에이전트를 설치한 다음, 준비한 권한을 제공해야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 호스트 요구 사항 검토

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

콘솔 에이전트는 UID와 GID 범위를 19000~19200으로 예약합니다. 이 범위는 고정되어 있으며 수정할 수 없습니다. 호스트의 타사 소프트웨어가 이 범위 내의 UID나 GID를 사용하는 경우 에이전트 설치가 실패합니다. NetApp 충돌을 피하기 위해 타사 소프트웨어가 없는 호스트를 사용할 것을 권장합니다.

전담 호스트

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

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

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

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

Azure VM 크기

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

하이퍼바이저

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

운영 체제 및 컨테이너 요구 사항

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

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

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

2단계**: Podman** 또는 **Docker Engine** 설치

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

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

  지원되는 Podman 버전 보기 .

- Ubuntu에는 Docker 엔진이 필요합니다.

  지원되는 Docker Engine 버전 보기 .

예 **2.** 단계

포드만

Podman을 설치하고 구성하려면 다음 단계를 따르세요.

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

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

단계

1. 호스트에 podman-docker 패키지가 설치되어 있다면 제거합니다.

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

2. Podman을 설치하세요.

   공식 Red Hat Enterprise Linux 저장소에서 Podman을 다운로드할 수 있습니다.

   a. Red Hat Enterprise Linux 9.6의 경우:

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

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

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

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

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

   c. Red Hat Enterprise Linux 8의 경우:

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

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

3. podman.socket 서비스를 활성화하고 시작합니다.

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

4. python3를 설치합니다.

```
sudo dnf install python3
```

5. 시스템에 EPEL 저장소 패키지가 아직 없으면 설치하세요.

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

6. Red Hat Enterprise 9를 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

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

   +

   a. podman-compose 패키지 1.5.0을 설치합니다.

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

7. Red Hat Enterprise Linux 8을 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

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

   b. podman-compose 패키지 1.0.6을 설치합니다.

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

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

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

i. 다음 명령을 실행하여 networkBackend가 CNI로 설정되어 있는지 확인하세요.

```
podman info | grep networkBackend
```

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

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

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

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

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

v. Podman을 다시 시작하세요.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

도커 엔진

Docker Engine을 설치하려면 Docker 설명서를 따르세요.

단계

1. "Docker에서 설치 지침 보기"

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

2. Docker가 활성화되어 실행 중인지 확인하세요.

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

3단계**:** 네트워킹 설정

콘솔 에이전트를 설치하려는 네트워크 위치가 다음 요구 사항을 지원하는지 확인하세요. 이러한 요구 사항을 충족하면 콘솔 에이전트가 하이브리드 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있습니다.

Azure 지역

Cloud Volumes ONTAP 사용하는 경우 콘솔 에이전트는 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 지역이나 "Azure 지역 쌍" Cloud Volumes ONTAP 시스템용. 이 요구 사항은 Cloud Volumes ONTAP 과 연결된 스토리지 계정 간에 Azure Private Link 연결이 사용되도록 보장합니다.

"Cloud Volumes ONTAP Azure Private Link를 사용하는 방법 알아보기"

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

웹 기반 **NetApp Console** 사용할 때 컴퓨터에서 연결된 엔드포인트

웹 브라우저에서 콘솔에 액세스하는 컴퓨터는 여러 엔드포인트에 접속할 수 있어야 합니다. 콘솔 에이전트를 설정하고 콘솔을 일상적으로 사용하려면 콘솔을 사용해야 합니다.

"NetApp 콘솔을 위한 네트워킹 준비" .

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Azure 공용 지역의 리소스를 관리합니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Azure China 지역의 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.

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

프록시 서버

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

- IP 주소
- 신임장
- HTTPS 인증서

포트

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

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

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

NTP 활성화

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

4단계**:** 콘솔 에이전트 배포 권한 설정

다음 옵션 중 하나를 사용하여 콘솔 에이전트에 Azure 권한을 제공해야 합니다.

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

콘솔 에이전트에 대한 권한을 준비하려면 다음 단계를 따르세요.

콘솔 에이전트 배포를 위한 사용자 지정 역할 만들기

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

단계

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

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

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

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

   예

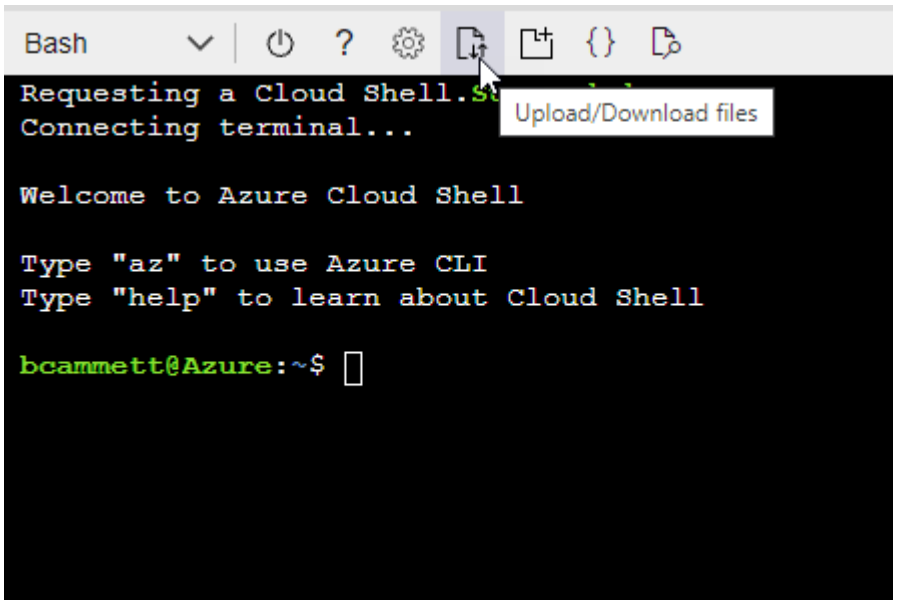
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ]
   ```

4. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 만듭니다.

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

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

   b. JSON 파일을 업로드합니다.



c. Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

서비스 주체

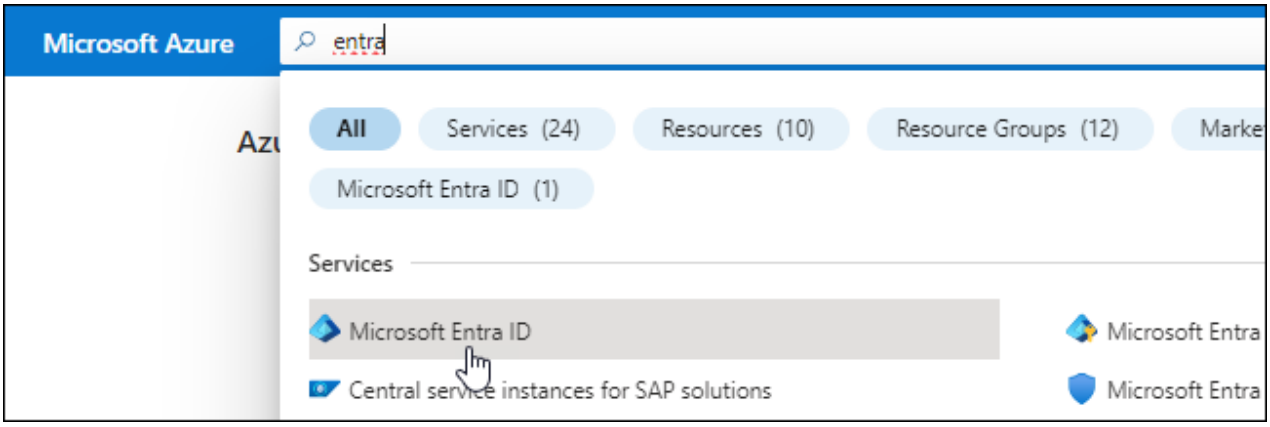
Microsoft Entra ID에서 서비스 주체를 만들고 설정하고 콘솔 에이전트에 필요한 Azure 자격 증명을 얻습니다.

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

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

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

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



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

   AD 애플리케이션과 서비스 주체를 생성했습니다.

역할에 애플리케이션 할당

1. 사용자 정의 역할 만들기:

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

   a. 내용을 복사하세요"콘솔 에이전트에 대한 사용자 정의 역할 권한" JSON 파일에 저장합니다.

b. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

사용자가 Cloud Volumes ONTAP 시스템을 생성할 각 Azure 구독에 대한 ID를 추가해야 합니다.

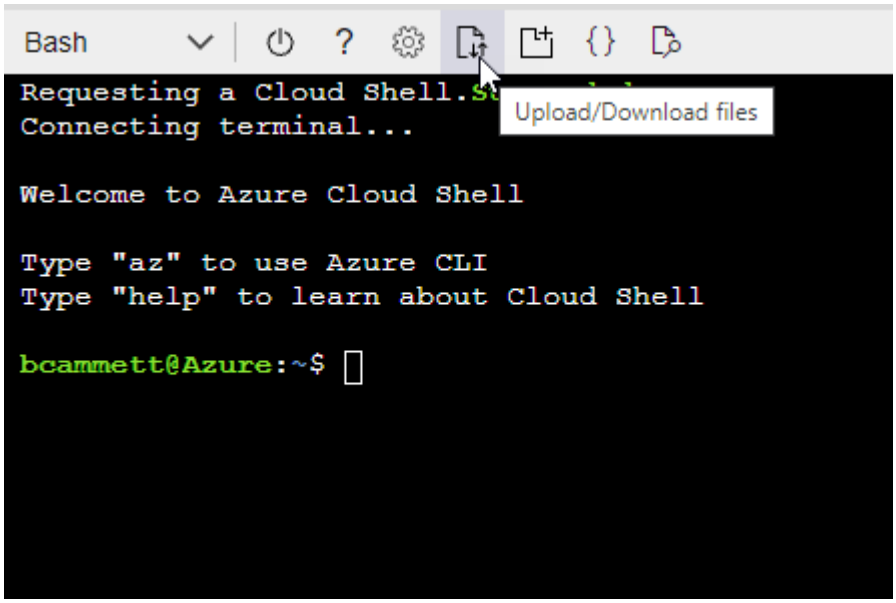
예

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

c. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 만듭니다.

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

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



- Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

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

2. 역할에 애플리케이션을 할당합니다.

a. Azure Portal에서 구독 서비스를 엽니다.

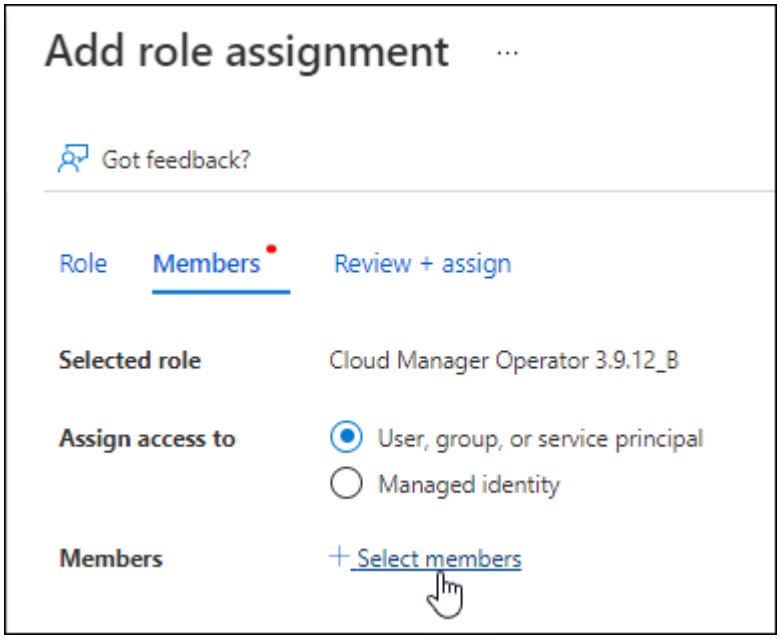
b. 구독을 선택하세요.

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

d. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.

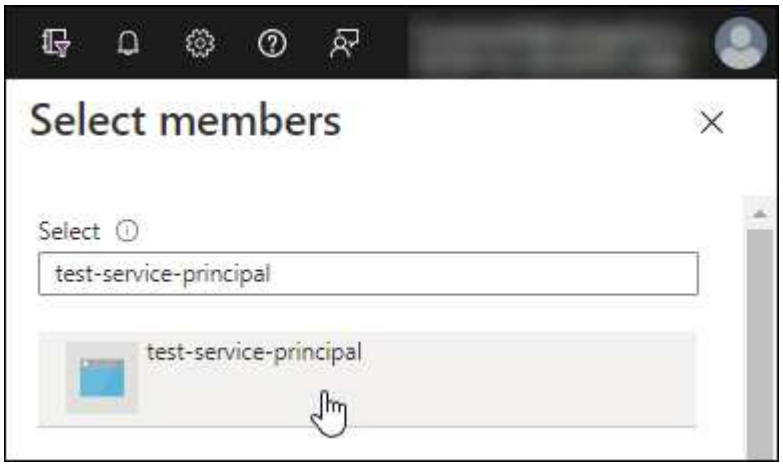
e. 멤버 탭에서 다음 단계를 완료하세요.

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



- 애플리케이션 이름을 검색하세요.

  예를 들면 다음과 같습니다.



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

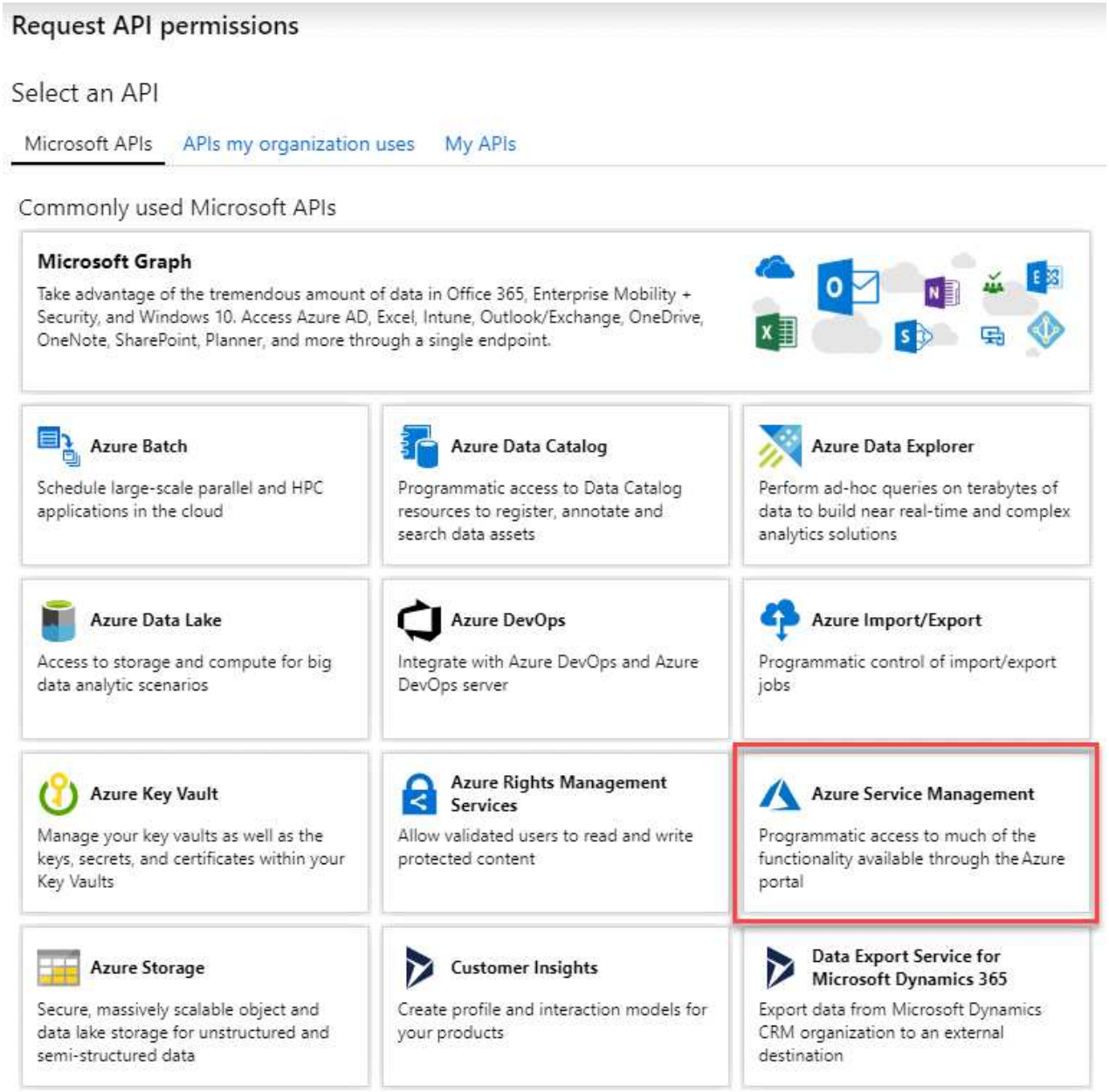
f. *검토 + 할당*을 선택하세요.

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

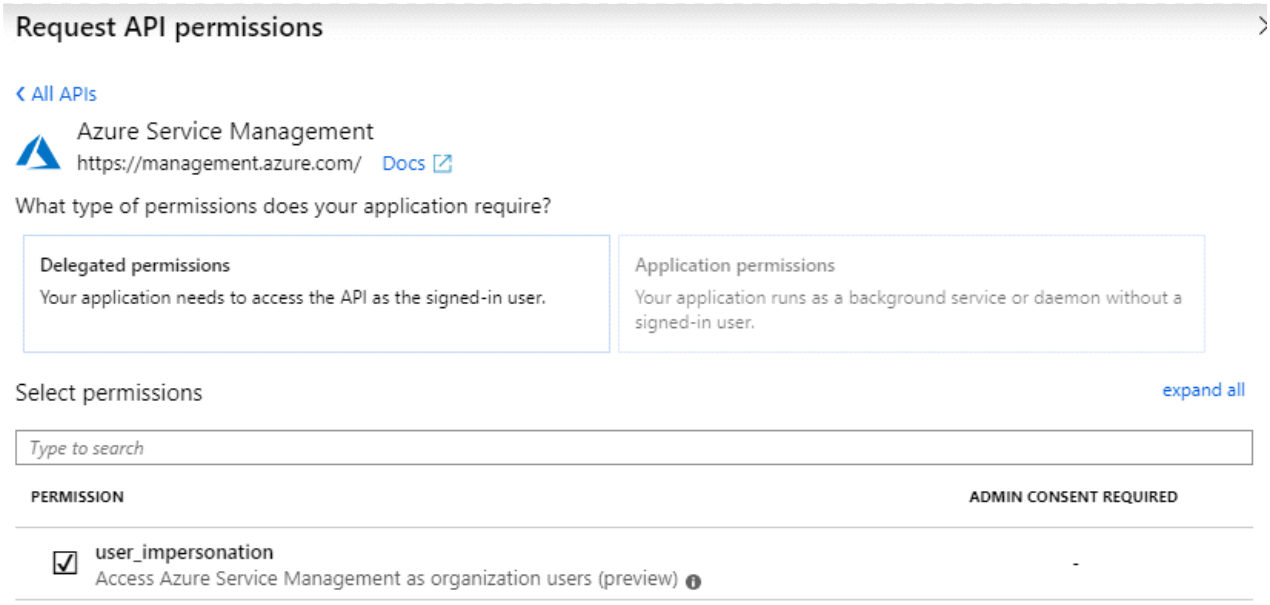
여러 Azure 구독에서 Cloud Volumes ONTAP 배포하려면 각 구독에 서비스 주체를 바인딩해야 합니다. NetApp Console 에서 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한 추가

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

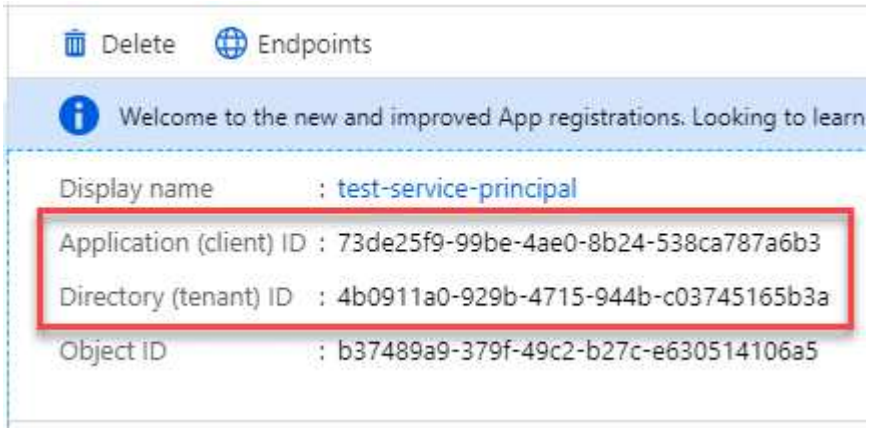


4. *조직 사용자로 Azure Service Management에 액세스*를 선택한 다음 *권한 추가*를 선택합니다.



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

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



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

클라이언트 비밀을 생성하세요

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

결과

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

5단계**:** 콘솔 에이전트 설치

필수 구성 요소를 모두 완료한 후에는 Linux 호스트에 소프트웨어를 수동으로 설치할 수 있습니다.

시작하기 전에

다음 사항이 있어야 합니다.

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

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

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

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

- 사용자 지정 역할을 통해 필요한 Azure 권한을 제공할 수 있도록 Azure의 VM에서 관리되는 ID를 활성화합니다.

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

이 작업에 관하여

설치 후, 새로운 버전이 나오면 콘솔 에이전트가 자동으로 업데이트됩니다.

단계

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

```
unset http_proxy
unset https_proxy
```

   이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

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

     에이전트 설치 파일 다운로드 또는 파일 URL 다운로드를 선택하십시오.

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

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

   여기서 <버전>은 다운로드한 콘솔 에이전트의 버전입니다.

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

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

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

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

+

다음은 CA 서명 인증서로 명시적 프록시 서버를 구성하는 예입니다.

+

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

+
`--proxy` 다음 형식 중 하나를 사용하여 Console 에이전트가 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 위와 같이 \의 ASCII 코드를 사용해야 합니다. **Console** 에이전트는 @ 문자가 포함된 사용자 이름이나 암호를 지원하지 않습니다. 암호에 다음 특수 문자(& 또는 !)가 포함된 경우 백슬래시를 앞에 붙여 해당 특수 문자를 이스케이프해야 합니다.

+ 예를 들면:

+ http://bxpproxyuser:netapp1\!@address:3128

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

   a. 콘솔 에이전트 가상 머신에 SSH를 실행합니다.

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

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

   예를 들어:

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

   a. 콘솔 에이전트 가상 머신을 재부팅합니다.

2. 설치가 완료될 때까지 기다리세요.

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

   설치에 실패하면 설치 보고서와 로그를 보고 문제를 해결하는 데 도움이 됩니다."설치 문제를 해결하는 방법을 알아보세요."

1. 콘솔 에이전트 가상 머신에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

   https://ipaddress

2. 로그인 후 콘솔 에이전트를 설정하세요.

   a. 콘솔 에이전트와 연결할 조직을 지정합니다.

   b. 시스템 이름을 입력하세요.

   c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

      이 단계에서는 표준 모드에서 콘솔을 사용하는 방법을 설명하므로 제한 모드를 비활성화해야 합니다. 보안 환경이 있고 백엔드 서비스에서 이 계정의 연결을 끊으려는 경우에만 제한 모드를 활성화해야 합니다. 그렇다면 ,"제한 모드에서 NetApp Console 시작하기 위한 단계를 따르세요." .

d. *시작하기*를 선택하세요.

콘솔 에이전트를 만든 동일한 Azure 구독에 Azure Blob 저장소가 있는 경우 시스템 페이지에 Azure Blob 저장소 시스템이 자동으로 표시됩니다. "NetApp Console 에서 Azure Blob 스토리지를 관리하는 방법을 알아보세요."

6단계**: NetApp Console** 에 권한 제공

이제 콘솔 에이전트를 설치했으므로 이전에 설정한 Azure 권한을 콘솔 에이전트에 제공해야 합니다. 권한을 제공하면 콘솔에서 Azure의 데이터 및 스토리지 인프라를 관리할 수 있습니다.

사용자 정의 역할

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

단계

1. Azure Portal에서 구독 서비스를 열고 구독을 선택합니다.

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

   "Microsoft Azure 설명서: Azure RBAC 범위 이해"

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

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

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

다음은 무엇인가요**?**

로 가다 "NetApp Console" 콘솔 에이전트를 사용하려면.

서비스 주체

단계

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

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

결과

이제 콘솔 에이전트는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 갖게 되었습니다.

구글 클라우드

Google Cloud의 콘솔 에이전트 설치 옵션

Google Cloud에서 콘솔 에이전트를 만드는 방법에는 여러 가지가 있습니다. 가장 일반적인 방법은 NetApp Console 에서 직접 실행하는 것입니다.

다음과 같은 설치 옵션을 사용할 수 있습니다.

- "콘솔에서 직접 콘솔 에이전트를 만듭니다."(이것은 표준 옵션입니다)

  이 작업을 수행하면 선택한 VPC에서 Linux와 콘솔 에이전트 소프트웨어를 실행하는 VM 인스턴스가 시작됩니다.

- "Google Platform을 사용하여 콘솔 에이전트 만들기"

  이 작업을 수행하면 Linux와 콘솔 에이전트 소프트웨어가 실행되는 VM 인스턴스가 시작되지만 배포는 콘솔이 아닌 Google Cloud에서 직접 시작됩니다.

- "자신의 Linux 호스트에 소프트웨어를 다운로드하고 수동으로 설치하세요."

선택하는 설치 옵션은 설치를 준비하는 방법에 영향을 미칩니다. 여기에는 Google Cloud에서 리소스를 인증하고 관리하는 데 필요한 권한을 콘솔에 제공하는 방법이 포함됩니다.

NetApp Console 에서 Google Cloud에 콘솔 에이전트 만들기

Google Cloud 콘솔에서 콘솔 에이전트를 만들 수 있습니다. 네트워킹을 설정하고, Google Cloud 권한을 준비하고, Google Cloud API를 활성화한 다음 콘솔 에이전트를 만들어야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 네트워킹 설정

콘솔 에이전트가 대상 네트워크에 연결하고 아웃바운드 인터넷에 접속하여 리소스를 관리할 수 있도록 네트워킹을 설정합니다.

VPC 및 서브넷

콘솔 에이전트를 생성할 때는 에이전트가 상주해야 하는 VPC와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어,

Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 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://config.googleapis.com/v1/projects	Google Cloud에서 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.

엔드포인트	목적
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

NetApp 콘솔에서 연결된 엔드포인트

SaaS 계층을 통해 제공되는 웹 기반 NetApp Console 사용하면 여러 엔드포인트에 연결하여 데이터 관리 작업을 완료할 수 있습니다. 여기에는 콘솔에서 콘솔 에이전트를 배포하기 위해 연결된 엔드포인트가 포함됩니다.

"NetApp 콘솔에서 연결된 엔드포인트 목록 보기" .

프록시 서버

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

- IP 주소
- 신임장
- HTTPS 인증서

포트

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

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

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

NTP 활성화

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

콘솔 에이전트를 만든 후 이 네트워킹 요구 사항을 구현합니다.

2단계**:** 콘솔 에이전트를 생성하기 위한 권한 설정

콘솔에서 콘솔 에이전트를 배포하려면 먼저 콘솔 에이전트 VM을 배포하는 Google 플랫폼 사용자의 권한을 설정해야 합니다.

단계

1. Google 플랫폼에서 사용자 지정 역할을 만듭니다.

   a. 다음 권한을 포함하는 YAML 파일을 만듭니다.

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- 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
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.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.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. Google Cloud에서 Cloud Shell을 활성화합니다.

c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

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

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

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

"Google Cloud 문서: 사용자 지정 역할 만들기 및 관리"

2. 콘솔이나 gcloud를 사용하여 콘솔 에이전트를 배포할 사용자에게 이 사용자 지정 역할을 할당합니다.

"Google Cloud 문서: 단일 역할 부여"

3단계**:** 에이전트와 함께 사용할 **Google Cloud** 서비스 계정을 생성합니다**.**

Google Cloud 서비스 계정은 콘솔 에이전트에 Google Cloud의 리소스를 관리하는 데 필요한 권한을 제공하는 데 필요합니다. 콘솔 에이전트를 만들 때 이 서비스 계정을 콘솔 에이전트 VM과 연결해야 합니다.

이후 릴리스에서 새로운 권한이 추가되면 사용자 지정 역할을 업데이트하는 것은 사용자의 책임입니다. 새로운 권한이 필요한 경우 릴리스 노트에 나열됩니다.

단계

1. Google Cloud에서 사용자 지정 역할을 만듭니다.

a. 내용을 포함하는 YAML 파일을 만듭니다."콘솔 에이전트에 대한 서비스 계정 권한" .

b. Google Cloud에서 Cloud Shell을 활성화합니다.

c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

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

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

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

"Google Cloud 문서: 사용자 지정 역할 만들기 및 관리"

2. Google Cloud에서 서비스 계정을 만들고 서비스 계정에 역할을 할당합니다.
   a. IAM 및 관리 서비스에서 *서비스 계정 > 서비스 계정 만들기*를 선택합니다.
   b. 서비스 계정 세부 정보를 입력하고 *만들기 및 계속*을 선택하세요.
   c. 방금 만든 역할을 선택하세요.
   d. 나머지 단계를 완료하여 역할을 만듭니다.

      "Google Cloud 문서: 서비스 계정 만들기"

3. 콘솔 에이전트가 있는 프로젝트와 다른 프로젝트에 Cloud Volumes ONTAP 시스템을 배포하려는 경우 콘솔 에이전트의 서비스 계정에 해당 프로젝트에 대한 액세스 권한을 제공해야 합니다.

   예를 들어, 콘솔 에이전트가 프로젝트 1에 있고 프로젝트 2에 Cloud Volumes ONTAP 시스템을 만들고 싶다고 가정해 보겠습니다. 프로젝트 2에서 서비스 계정에 대한 액세스 권한을 부여해야 합니다.

   a. IAM 및 관리 서비스에서 Cloud Volumes ONTAP 시스템을 만들려는 Google Cloud 프로젝트를 선택합니다.
   b. **IAM** 페이지에서 *액세스 권한 부여*를 선택하고 필요한 세부 정보를 제공합니다.
      - 콘솔 에이전트 서비스 계정의 이메일을 입력하세요.
      - 콘솔 에이전트의 사용자 지정 역할을 선택합니다.
      - *저장*을 선택하세요.

   자세한 내용은 다음을 참조하세요. "Google Cloud 문서"

4단계**:** 공유 **VPC** 권한 설정

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

이 표는 참조용이며 IAM 구성이 완료되면 사용자 환경에 권한 표가 반영되어야 합니다.

공유 **VPC** 권한 보기

신원	창조자	호스팅됨	서비스 프로젝트 권한	호스트 프로젝트 권한	목적
에이전트를 배포하기 위한 Google 계정	관습	봉사 프로젝트	"에이전트 배포 정책"	컴퓨팅.네트워크사용자	서비스 프로젝트에 에이전트 배포
에이전트 서비스 계정	관습	봉사 프로젝트	"에이전트 서비스 계정 정책"	compute.network User 배포 관리자 .편집기	서비스 프로젝트에서 Cloud Volumes ONTAP 및 서비스 배포 및 유지 관리
Cloud Volumes ONTAP 서비스 계정	관습	봉사 프로젝트	storage.admin 멤버: NetApp Console 서비스 계정(serviceAccount.user)	해당 없음	(선택 사항) NetApp Cloud Tiering 및 NetApp Backup and Recovery
Google API 서비스 에이전트	구글 클라우드	봉사 프로젝트	(기본값) 편집기	컴퓨팅.네트워크사용자	배포를 대신하여 Google Cloud API와 상호 작용합니다. 콘솔이 공유 네트워크를 사용할 수 있도록 합니다.
Google Compute Engine 기본 서비스 계정	구글 클라우드	봉사 프로젝트	(기본값) 편집기	컴퓨팅.네트워크사용자	배포를 대신하여 Google Cloud 인스턴스와 컴퓨팅 인프라를 배포합니다. 콘솔이 공유 네트워크를 사용할 수 있도록 합니다.

참고사항:

1. deploymentmanager.editor는 배포에 방화벽 규칙을 전달하지 않고 콘솔에서 규칙을 생성하도록 선택한 경우에만 호스트 프로젝트에서 필요합니다. 규칙이 지정되지 않으면 NetApp Console 호스트 프로젝트에 VPC0 방화벽 규칙을 포함하는 배포를 생성합니다.
2. firewall.create와 firewall.delete는 배포에 방화벽 규칙을 전달하지 않고 콘솔에서 해당 규칙을 생성하도록 선택한 경우에만 필요합니다. 이러한 권한은 콘솔 계정의 .yaml 파일에 있습니다. 공유 VPC를 사용하여 HA 쌍을 배포하는 경우 이러한 권한은 VPC1, 2, 3에 대한 방화벽 규칙을 만드는 데 사용됩니다. 다른 모든 배포의 경우 이러한 권한은 VPC0에 대한 규칙을 만드는 데에도 사용됩니다.
3. 클라우드 계층화의 경우 계층화 서비스 계정에는 프로젝트 수준뿐만 아니라 서비스 계정에 대한 serviceAccount.user 역할이 있어야 합니다. 현재 프로젝트 수준에서 serviceAccount.user를 할당하는 경우 getIAMPolicy로 서비스 계정을 쿼리할 때 권한이 표시되지 않습니다.

5단계**: Google Cloud API** 활성화

콘솔 에이전트와 Cloud Volumes ONTAP 배포하기 전에 여러 Google Cloud API를 활성화해야 합니다.

단계

1. 프로젝트에서 다음 Google Cloud API를 활성화하세요.

- 클라우드 배포 관리자 V2 API
- 클라우드 인프라 관리자 API
- 클라우드 로깅 API
- 클라우드 리소스 관리자 API
- 컴퓨트 엔진 API
- ID 및 액세스 관리(IAM) API
- Cloud Key Management Service(KMS) API(NetApp Backup and Recovery를 고객 관리 암호화 키(CMEK)와 함께 사용할 계획인 경우에만 필요)
- Cloud Quotas API(Infrastructure Manager를 사용하는 Cloud Volumes ONTAP 배포에 필요)

"Google Cloud 문서: API 활성화"

6단계**:** 콘솔 에이전트 만들기

콘솔에서 직접 콘솔 에이전트를 만듭니다.

콘솔 에이전트를 생성하면 기본 구성을 사용하여 Google Cloud에 가상 머신 인스턴스가 배포됩니다. 콘솔 에이전트를 만든 후에는 CPU나 RAM이 적은 더 작은 VM 인스턴스로 전환하지 마세요. "콘솔 에이전트의 기본 구성에 대해 알아보세요" .

Google Cloud에 에이전트를 배포하면 에이전트가 배포 파일을 저장할 버킷을 생성합니다.

시작하기 전에

다음 사항이 있어야 합니다.

- 콘솔 에이전트와 콘솔 에이전트 VM에 대한 서비스 계정을 생성하는 데 필요한 Google Cloud 권한입니다.
- 네트워킹 요구 사항을 충족하는 VPC 및 서브넷.
- 콘솔 에이전트에서 인터넷에 접속하는 데 프록시가 필요한 경우 프록시 서버에 대한 세부 정보입니다.

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 *에이전트 배포 > Google Cloud*를 선택합니다.
3. 에이전트 배치 페이지에서 필요한 사항에 대한 세부 정보를 검토하세요. 두 가지 옵션이 있습니다.
   a. 제품 내 가이드를 사용하여 배포를 준비하려면 *계속*을 선택하세요. 제품 내 가이드의 각 단계에는 이 문서 페이지에 포함된 정보가 포함되어 있습니다.
   b. 이 페이지의 단계에 따라 이미 준비가 되었다면 *배포로 건너뛰기*를 선택하세요.
4. 마법사의 단계에 따라 콘솔 에이전트를 만듭니다.
   - 메시지가 표시되면 가상 머신 인스턴스를 만드는 데 필요한 권한이 있는 Google 계정에 로그인하세요.

     이 양식은 Google에서 소유하고 호스팅합니다. 귀하의 자격 증명은 NetApp 에 제공되지 않습니다.

   - 세부 정보: 가상 머신 인스턴스의 이름을 입력하고, 태그를 지정하고, 프로젝트를 선택한 다음, 필요한 권한이 있는 서비스 계정을 선택합니다(자세한 내용은 위 섹션을 참조하세요).

- 위치: 인스턴스에 대한 지역, 영역, VPC 및 서브넷을 지정합니다.
- 네트워크: 공용 IP 주소를 사용할지 여부를 선택하고, 선택적으로 프록시 구성을 지정합니다.
- 네트워크 태그: 투명 프록시를 사용하는 경우 콘솔 에이전트 인스턴스에 네트워크 태그를 추가합니다. 네트워크 태그는 소문자로 시작해야 하며 소문자, 숫자, 하이픈을 포함할 수 있습니다. 태그는 소문자나 숫자로 끝나야 합니다. 예를 들어, "console-agent-proxy" 태그를 사용할 수 있습니다.
- 방화벽 정책: 새로운 방화벽 정책을 만들지, 아니면 필요한 인바운드 및 아웃바운드 규칙을 허용하는 기존 방화벽 정책을 선택할지 선택합니다.

  "Google Cloud의 방화벽 규칙"

5. 선택 사항을 검토하여 설정이 올바른지 확인하세요.

   a. 에이전트 구성 검증 확인란은 배포 시 콘솔에서 네트워크 연결 요구 사항을 검증하도록 기본적으로 선택되어 있습니다. 콘솔에서 에이전트를 배포하지 못하면 문제 해결에 도움이 되는 보고서가 제공됩니다. 배포가 성공하면 보고서는 제공되지 않습니다.

   아직도 사용 중이라면"이전 종료점" 에이전트 업그레이드에 사용되면 유효성 검사가 오류로 인해 실패합니다. 이를 방지하려면 유효성 검사를 건너뛰려면 확인란의 선택을 취소하세요.

6. *추가*를 선택하세요.

   에이전트는 약 10분 안에 준비됩니다. 프로세스가 완료될 때까지 페이지에 머물러 주세요.

결과

프로세스가 완료되면 콘솔 에이전트를 사용할 수 있습니다.

배포에 실패하면 콘솔에서 보고서와 로그를 다운로드하여 문제를 해결할 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

콘솔 에이전트를 생성한 동일한 Google Cloud 계정에 Google Cloud Storage 버킷이 있는 경우, 시스템 페이지에 Google Cloud Storage 시스템이 자동으로 표시됩니다. "콘솔에서 Google Cloud Storage를 관리하는 방법을 알아보세요."

Google Cloud에서 콘솔 에이전트 만들기

Google Cloud를 사용하여 Google Cloud에서 콘솔 에이전트를 만들려면 네트워킹을 설정하고, Google Cloud 권한을 준비하고, Google Cloud API를 활성화한 다음 콘솔 에이전트를 만들어야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 네트워킹 설정

콘솔 에이전트가 리소스를 관리하고 대상 네트워크와 인터넷에 연결할 수 있도록 네트워킹을 설정합니다.

VPC 및 서브넷

콘솔 에이전트를 생성할 때는 에이전트가 상주해야 하는 VPC와 서브넷을 지정해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 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://config.googleapis.com/v1/projects	Google Cloud에서 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.

엔드포인트	목적
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

NetApp 콘솔에서 연결된 엔드포인트

SaaS 계층을 통해 제공되는 웹 기반 NetApp Console 사용하면 여러 엔드포인트에 연결하여 데이터 관리 작업을 완료할 수 있습니다. 여기에는 콘솔에서 콘솔 에이전트를 배포하기 위해 연결된 엔드포인트가 포함됩니다.

"NetApp 콘솔에서 연결된 엔드포인트 목록 보기" .

프록시 서버

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

- IP 주소
- 신임장
- HTTPS 인증서

포트

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

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

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

NTP 활성화

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

콘솔 에이전트를 만든 후 이 네트워킹 요구 사항을 구현합니다.

2단계**:** 콘솔 에이전트를 생성하기 위한 권한 설정

Google Cloud 사용자가 Google Cloud에서 콘솔 에이전트 VM을 배포할 수 있는 권한을 설정합니다.

단계

1. Google 플랫폼에서 사용자 지정 역할을 만듭니다.

   a. 다음 권한을 포함하는 YAML 파일을 만듭니다.

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console
agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- 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
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.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.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. Google Cloud에서 Cloud Shell을 활성화합니다.

c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

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

다음 예제에서는 프로젝트 수준에서 "connectorDeployment"라는 역할을 만듭니다.

gcloud iam 역할 커넥터 배포 생성 --project=myproject --file=connector-deployment.yaml

"Google Cloud 문서: 사용자 지정 역할 만들기 및 관리"

2. Google Cloud에서 콘솔 에이전트를 배포하는 사용자에게 이 사용자 지정 역할을 할당합니다.

"Google Cloud 문서: 단일 역할 부여"

3단계**:** 콘솔 에이전트 작업에 대한 권한 설정

Google Cloud 서비스 계정은 콘솔 에이전트에 Google Cloud의 리소스를 관리하는 데 필요한 권한을 제공하는 데 필요합니다. 콘솔 에이전트를 만들 때 이 서비스 계정을 콘솔 에이전트 VM과 연결해야 합니다.

이후 릴리스에서 새로운 권한이 추가되면 사용자 지정 역할을 업데이트하는 것은 사용자의 책임입니다. 새로운 권한이 필요한 경우 릴리스 노트에 나열됩니다.

단계

1. Google Cloud에서 사용자 지정 역할을 만듭니다.

   a. 내용을 포함하는 YAML 파일을 만듭니다."콘솔 에이전트에 대한 서비스 계정 권한" .

   b. Google Cloud에서 Cloud Shell을 활성화합니다.

   c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

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

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

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

"Google Cloud 문서: 사용자 지정 역할 만들기 및 관리"

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

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

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

   c. 방금 만든 역할을 선택하세요.

   d. 나머지 단계를 완료하여 역할을 만듭니다.

   "Google Cloud 문서: 서비스 계정 만들기"

3. 콘솔 에이전트가 있는 프로젝트와 다른 프로젝트에 Cloud Volumes ONTAP 시스템을 배포하려는 경우 콘솔 에이전트의 서비스 계정에 해당 프로젝트에 대한 액세스 권한을 제공해야 합니다.

   예를 들어, 콘솔 에이전트가 프로젝트 1에 있고 프로젝트 2에 Cloud Volumes ONTAP 시스템을 만들고 싶다고 가정해 보겠습니다. 프로젝트 2에서 서비스 계정에 대한 액세스 권한을 부여해야 합니다.

   a. IAM 및 관리 서비스에서 Cloud Volumes ONTAP 시스템을 만들려는 Google Cloud 프로젝트를 선택합니다.

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

- 콘솔 에이전트 서비스 계정의 이메일을 입력하세요.
- 콘솔 에이전트의 사용자 지정 역할을 선택합니다.
- *저장*을 선택하세요.

자세한 내용은 다음을 참조하세요. "Google Cloud 문서"

4단계**:** 공유 **VPC** 권한 설정

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

이 표는 참조용이며 IAM 구성이 완료되면 사용자 환경에 권한 표가 반영되어야 합니다.

공유 **VPC** 권한 보기

신원	창조자	호스팅됨	서비스 프로젝트 권한	호스트 프로젝트 권한	목적
에이전트를 배포하기 위한 Google 계정	관습	봉사 프로젝트	"에이전트 배포 정책"	컴퓨팅.네트워크사용자	서비스 프로젝트에 에이전트 배포
에이전트 서비스 계정	관습	봉사 프로젝트	"에이전트 서비스 계정 정책"	compute.network User 배포 관리자 .편집기	서비스 프로젝트에서 Cloud Volumes ONTAP 및 서비스 배포 및 유지 관리
Cloud Volumes ONTAP 서비스 계정	관습	봉사 프로젝트	storage.admin 멤버: NetApp Console 서비스 계정(serviceAccount.user)	해당 없음	(선택 사항) NetApp Cloud Tiering 및 NetApp Backup and Recovery
Google API 서비스 에이전트	구글 클라우드	봉사 프로젝트	(기본값) 편집기	컴퓨팅.네트워크사용자	배포를 대신하여 Google Cloud API와 상호 작용합니다. 콘솔이 공유 네트워크를 사용할 수 있도록 합니다.
Google Compute Engine 기본 서비스 계정	구글 클라우드	봉사 프로젝트	(기본값) 편집기	컴퓨팅.네트워크사용자	배포를 대신하여 Google Cloud 인스턴스와 컴퓨팅 인프라를 배포합니다. 콘솔이 공유 네트워크를 사용할 수 있도록 합니다.

참고사항:

1. deploymentmanager.editor는 배포에 방화벽 규칙을 전달하지 않고 콘솔에서 규칙을 생성하도록 선택한 경우에만 호스트 프로젝트에서 필요합니다. 규칙이 지정되지 않으면 NetApp Console 호스트 프로젝트에 VPC0 방화벽 규칙을 포함하는 배포를 생성합니다.
2. firewall.create와 firewall.delete는 배포에 방화벽 규칙을 전달하지 않고 콘솔에서 해당 규칙을 생성하도록 선택한 경우에만 필요합니다. 이러한 권한은 콘솔 계정의 .yaml 파일에 있습니다. 공유 VPC를 사용하여 HA 쌍을 배포하는 경우 이러한 권한은 VPC1, 2, 3에 대한 방화벽 규칙을 만드는 데 사용됩니다. 다른 모든 배포의 경우 이러한 권한은 VPC0에 대한 규칙을 만드는 데에도 사용됩니다.
3. 클라우드 계층화의 경우 계층화 서비스 계정에는 프로젝트 수준뿐만 아니라 서비스 계정에 대한 serviceAccount.user 역할이 있어야 합니다. 현재 프로젝트 수준에서 serviceAccount.user를 할당하는 경우 getIAMPolicy로 서비스 계정을 쿼리할 때 권한이 표시되지 않습니다.

5단계**: Google Cloud API** 활성화

콘솔 에이전트와 Cloud Volumes ONTAP 배포하기 전에 여러 Google Cloud API를 활성화합니다.

단계

1. 프로젝트에서 다음 Google Cloud API를 활성화하세요.

- 클라우드 배포 관리자 V2 API
- 클라우드 인프라 관리자 API
- 클라우드 로깅 API
- 클라우드 리소스 관리자 API
- 컴퓨트 엔진 API
- ID 및 액세스 관리(IAM) API
- Cloud Key Management Service(KMS) API(NetApp Backup and Recovery를 고객 관리 암호화 키(CMEK)와 함께 사용할 계획인 경우에만 필요)
- Cloud Quotas API(Infrastructure Manager를 사용하는 Cloud Volumes ONTAP 배포에 필요)

"Google Cloud 문서: API 활성화"

6단계**:** 콘솔 에이전트 만들기

Google Cloud를 사용하여 콘솔 에이전트를 만듭니다.

콘솔 에이전트를 생성하면 기본 구성으로 Google Cloud에 VM 인스턴스가 배포됩니다. 콘솔 에이전트를 만든 후에는 CPU나 RAM이 적은 더 작은 VM 인스턴스로 전환하지 마세요. "콘솔 에이전트의 기본 구성에 대해 알아보세요" .

시작하기 전에

다음 사항이 있어야 합니다.

- 콘솔 에이전트와 콘솔 에이전트 VM에 대한 서비스 계정을 생성하는 데 필요한 Google Cloud 권한입니다.
- 네트워킹 요구 사항을 충족하는 VPC 및 서브넷.
- VM 인스턴스 요구 사항에 대한 이해.
  - **CPU**: 8개 코어 또는 8개 vCPU
  - 램: 32GB
  - 기계 유형: n2-standard-8을 권장합니다.

    콘솔 에이전트는 보호된 VM 기능을 지원하는 OS가 있는 VM 인스턴스의 Google Cloud에서 지원됩니다.

단계

1. 원하는 방법을 사용하여 Google Cloud SDK에 로그인하세요.

   이 예제에서는 gcloud SDK가 설치된 로컬 셸을 사용하지만 Google Cloud Shell을 사용할 수도 있습니다.

   Google Cloud SDK에 대한 자세한 내용은 다음을 참조하세요."Google Cloud SDK 문서 페이지" .

2. 위 섹션에 정의된 필수 권한이 있는 사용자로 로그인했는지 확인하세요.

   ```
   gcloud auth list
   ```

   출력에는 다음과 같은 내용이 표시되어야 합니다. 여기서 * 사용자 계정은 로그인에 사용할 사용자 계정입니다.

```
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. 실행하다 `gcloud compute instances create` 명령:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --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 대한 원하는 인스턴스 이름입니다.

프로젝트
: (선택 사항) VM을 배포할 프로젝트입니다.

서비스 계정
: 2단계의 출력에 지정된 서비스 계정입니다.

존
: VM을 배포하려는 영역

주소 없음
: (선택 사항) 외부 IP 주소가 사용되지 않습니다(트래픽을 공용 인터넷으로 라우팅하려면 클라우드 NAT 또는 프록시가 필요함)

네트워크 태그
: (선택 사항) 태그를 사용하여 방화벽 규칙을 콘솔 에이전트 인스턴스에 연결하기 위해 네트워크 태그를 추가합니다.

네트워크 경로

(선택 사항) 콘솔 에이전트를 배포할 네트워크 이름을 추가합니다(공유 VPC의 경우 전체 경로가 필요함)

서브넷 경로

(선택 사항) 콘솔 에이전트를 배포할 서브넷 이름을 추가합니다(공유 VPC의 경우 전체 경로가 필요함)

kms-키**-**경로

(선택 사항) 콘솔 에이전트의 디스크를 암호화하기 위해 KMS 키를 추가합니다(IAM 권한도 적용해야 함)

이러한 플래그에 대한 자세한 내용은 다음을 방문하세요."Google Cloud Compute SDK 문서" .

명령을 실행하면 콘솔 에이전트가 배포됩니다. 콘솔 에이전트 인스턴스와 소프트웨어는 약 5분 안에 실행될 것입니다.

4. 웹 브라우저를 열고 콘솔 에이전트 호스트 URL을 입력하세요.

   콘솔 호스트 URL은 호스트 구성에 따라 로컬호스트, 개인 IP 주소 또는 공용 IP 주소가 될 수 있습니다. 예를 들어, 콘솔 에이전트가 공용 IP 주소가 없는 퍼블릭 클라우드에 있는 경우 콘솔 에이전트 호스트에 연결된 호스트의 개인 IP 주소를 입력해야 합니다.

5. 로그인 후 콘솔 에이전트를 설정하세요.

   a. 콘솔 에이전트와 연결할 콘솔 조직을 지정합니다.

      "ID 및 액세스 관리에 대해 알아보세요" .

   b. 시스템 이름을 입력하세요.

결과

이제 콘솔 에이전트가 설치되고 콘솔 조직에 설정되었습니다.

웹 브라우저를 열고 이동하세요 "NetApp Console" 콘솔 에이전트를 사용하려면.

Google Cloud에 콘솔 에이전트를 수동으로 설치합니다**.**

Linux 호스트에 콘솔 에이전트를 수동으로 설치하려면 호스트 요구 사항을 검토하고, 네트워킹을 설정하고, Google Cloud 권한을 준비하고, Google Cloud API를 활성화하고, 콘솔을 설치한 다음, 준비한 권한을 제공해야 합니다.

시작하기 전에

- 당신은 ~을 가져야합니다"콘솔 에이전트에 대한 이해" .
- 검토해야 합니다"콘솔 에이전트 제한 사항" .

1단계**:** 호스트 요구 사항 검토

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

콘솔 에이전트는 UID와 GID 범위를 19000~19200으로 예약합니다. 이 범위는 고정되어 있으며 수정할 수 없습니다. 호스트의 타사 소프트웨어가 이 범위 내의 UID나 GID를 사용하는 경우 에이전트 설치가 실패합니다. NetApp 충돌을 피하기 위해 타사 소프트웨어가 없는 호스트를 사용할 것을 권장합니다.

전담 호스트

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

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

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

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

Google Cloud 머신 유형

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

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

하이퍼바이저

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

운영 체제 및 컨테이너 요구 사항

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

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

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

Google Cloud 머신 유형

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

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

2단계**: Podman** 또는 **Docker Engine** 설치

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

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

  지원되는 Podman 버전 보기 .

- Ubuntu에는 Docker 엔진이 필요합니다.

  지원되는 Docker Engine 버전 보기 .

예 **3.** 단계

포드만

Podman을 설치하고 구성하려면 다음 단계를 따르세요.

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

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

단계

1. 호스트에 podman-docker 패키지가 설치되어 있다면 제거합니다.

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

2. Podman을 설치하세요.

   공식 Red Hat Enterprise Linux 저장소에서 Podman을 다운로드할 수 있습니다.

   a. Red Hat Enterprise Linux 9.6의 경우:

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

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

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

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

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

   c. Red Hat Enterprise Linux 8의 경우:

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

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

3. podman.socket 서비스를 활성화하고 시작합니다.

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

4. python3를 설치합니다.

```
sudo dnf install python3
```

5. 시스템에 EPEL 저장소 패키지가 아직 없으면 설치하세요.

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

6. Red Hat Enterprise 9를 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

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

   +

   a. podman-compose 패키지 1.5.0을 설치합니다.

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

7. Red Hat Enterprise Linux 8을 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

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

   b. podman-compose 패키지 1.0.6을 설치합니다.

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

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

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

i. 다음 명령을 실행하여 networkBackend가 CNI로 설정되어 있는지 확인하세요.

```
podman info | grep networkBackend
```

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

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

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

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

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

v. Podman을 다시 시작하세요.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

도커 엔진

Docker Engine을 설치하려면 Docker 설명서를 따르세요.

단계

1. "Docker에서 설치 지침 보기"

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

2. Docker가 활성화되어 실행 중인지 확인하세요.

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

3단계**:** 네트워킹 설정

하이브리드 클라우드 환경 내에서 콘솔 에이전트가 리소스와 프로세스를 관리할 수 있도록 네트워킹을 설정합니다. 예를 들어, 대상 네트워크에 연결이 가능한지, 아웃바운드 인터넷 접속이 가능한지 확인해야 합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

웹 기반 **NetApp Console** 사용할 때 컴퓨터에서 연결된 엔드포인트

웹 브라우저에서 콘솔에 액세스하는 컴퓨터는 여러 엔드포인트에 접속할 수 있어야 합니다. 콘솔 에이전트를 설정하고 콘솔을 일상적으로 사용하려면 콘솔을 사용해야 합니다.

"NetApp 콘솔을 위한 네트워킹 준비" .

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 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://config.googleapis.com/v1/projects	Google Cloud에서 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.

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

프록시 서버

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

- IP 주소
- 신임장
- HTTPS 인증서

포트

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

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

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

NTP 활성화

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

4단계**:** 콘솔 에이전트에 대한 권한 설정

Google Cloud 서비스 계정은 콘솔 에이전트에 Google Cloud의 리소스를 관리하는 데 필요한 권한을 제공하는 데 필요합니다. 콘솔 에이전트를 만들 때 이 서비스 계정을 콘솔 에이전트 VM과 연결해야 합니다.

이후 릴리스에서 새로운 권한이 추가되면 사용자 지정 역할을 업데이트하는 것은 사용자의 책임입니다. 새로운 권한이 필요한 경우 릴리스 노트에 나열됩니다.

단계

1. Google Cloud에서 사용자 지정 역할을 만듭니다.

   a. 내용을 포함하는 YAML 파일을 만듭니다."콘솔 에이전트에 대한 서비스 계정 권한" .

   b. Google Cloud에서 Cloud Shell을 활성화합니다.

   c. 필요한 권한이 포함된 YAML 파일을 업로드합니다.

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

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

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

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

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

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

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

   c. 방금 만든 역할을 선택하세요.

   d. 나머지 단계를 완료하여 역할을 만듭니다.

      "Google Cloud 문서: 서비스 계정 만들기"

3. 콘솔 에이전트가 있는 프로젝트와 다른 프로젝트에 Cloud Volumes ONTAP 시스템을 배포하려는 경우 콘솔 에이전트의 서비스 계정에 해당 프로젝트에 대한 액세스 권한을 제공해야 합니다.

   예를 들어, 콘솔 에이전트가 프로젝트 1에 있고 프로젝트 2에 Cloud Volumes ONTAP 시스템을 만들고 싶다고 가정해 보겠습니다. 프로젝트 2에서 서비스 계정에 대한 액세스 권한을 부여해야 합니다.

   a. IAM 및 관리 서비스에서 Cloud Volumes ONTAP 시스템을 만들려는 Google Cloud 프로젝트를 선택합니다.

b. **IAM** 페이지에서 *액세스 권한 부여*를 선택하고 필요한 세부 정보를 제공합니다.
   - 콘솔 에이전트 서비스 계정의 이메일을 입력하세요.
   - 콘솔 에이전트의 사용자 지정 역할을 선택합니다.
   - *저장*을 선택하세요.

자세한 내용은 다음을 참조하세요. "Google Cloud 문서"

5단계**:** 공유 **VPC** 권한 설정

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

이 표는 참조용이며 IAM 구성이 완료되면 사용자 환경에 권한 표가 반영되어야 합니다.

공유 **VPC** 권한 보기

신원	창조자	호스팅됨	서비스 프로젝트 권한	호스트 프로젝트 권한	목적
에이전트를 배포하기 위한 Google 계정	관습	봉사 프로젝트	"에이전트 배포 정책"	컴퓨팅.네트워크사용자	서비스 프로젝트에 에이전트 배포
에이전트 서비스 계정	관습	봉사 프로젝트	"에이전트 서비스 계정 정책"	compute.network User 배포 관리자 .편집기	서비스 프로젝트에서 Cloud Volumes ONTAP 및 서비스 배포 및 유지 관리
Cloud Volumes ONTAP 서비스 계정	관습	봉사 프로젝트	storage.admin 멤버: NetApp Console 서비스 계정(serviceAccount.user)	해당 없음	(선택 사항) NetApp Cloud Tiering 및 NetApp Backup and Recovery
Google API 서비스 에이전트	구글 클라우드	봉사 프로젝트	(기본값) 편집기	컴퓨팅.네트워크사용자	배포를 대신하여 Google Cloud API와 상호 작용합니다. 콘솔이 공유 네트워크를 사용할 수 있도록 합니다.
Google Compute Engine 기본 서비스 계정	구글 클라우드	봉사 프로젝트	(기본값) 편집기	컴퓨팅.네트워크사용자	배포를 대신하여 Google Cloud 인스턴스와 컴퓨팅 인프라를 배포합니다. 콘솔이 공유 네트워크를 사용할 수 있도록 합니다.

참고사항:

1. deploymentmanager.editor는 배포에 방화벽 규칙을 전달하지 않고 콘솔에서 규칙을 생성하도록 선택한 경우에만 호스트 프로젝트에서 필요합니다. 규칙이 지정되지 않으면 NetApp Console 호스트 프로젝트에 VPC0 방화벽 규칙을 포함하는 배포를 생성합니다.
2. firewall.create와 firewall.delete는 배포에 방화벽 규칙을 전달하지 않고 콘솔에서 해당 규칙을 생성하도록 선택한 경우에만 필요합니다. 이러한 권한은 콘솔 계정의 .yaml 파일에 있습니다. 공유 VPC를 사용하여 HA 쌍을 배포하는 경우 이러한 권한은 VPC1, 2, 3에 대한 방화벽 규칙을 만드는 데 사용됩니다. 다른 모든 배포의 경우 이러한 권한은 VPC0에 대한 규칙을 만드는 데에도 사용됩니다.
3. 클라우드 계층화의 경우 계층화 서비스 계정에는 프로젝트 수준뿐만 아니라 서비스 계정에 대한 serviceAccount.user 역할이 있어야 합니다. 현재 프로젝트 수준에서 serviceAccount.user를 할당하는 경우 getIAMPolicy로 서비스 계정을 쿼리할 때 권한이 표시되지 않습니다.

6단계**: Google Cloud API** 활성화

Google Cloud에 콘솔 에이전트를 배포하려면 먼저 몇 가지 Google Cloud API를 사용 설정해야 합니다.

단계

1. 프로젝트에서 다음 Google Cloud API를 활성화하세요.

- 클라우드 배포 관리자 V2 API
- 클라우드 인프라 관리자 API
- 클라우드 로깅 API
- 클라우드 리소스 관리자 API
- 컴퓨트 엔진 API
- ID 및 액세스 관리(IAM) API
- Cloud Key Management Service(KMS) API(NetApp Backup and Recovery를 고객 관리 암호화 키(CMEK)와 함께 사용할 계획인 경우에만 필요)
- Cloud Quotas API(Infrastructure Manager를 사용하는 Cloud Volumes ONTAP 배포에 필요)

"Google Cloud 문서: API 활성화"

7단계**:** 콘솔 에이전트 설치

필수 구성 요소를 모두 완료한 후에는 Linux 호스트에 소프트웨어를 수동으로 설치할 수 있습니다.

에이전트를 배포하면 시스템에서 배포 파일을 저장할 Google Cloud 버킷도 생성합니다.

시작하기 전에

다음 사항이 있어야 합니다.

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

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

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

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

이 작업에 관하여

설치 후, 새로운 버전이 나오면 콘솔 에이전트가 자동으로 업데이트됩니다.

단계

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

   ```
   unset http_proxy
   unset https_proxy
   ```

   이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

2. 콘솔 에이전트 소프트웨어를 다운로드한 다음 Linux 호스트에 복사하십시오. NetApp Console 또는 NetApp 지원 사이트에서 다운로드할 수 있습니다.

- NetApp Console: *에이전트 > 관리 > 에이전트 배포 > 온프레미스 > 수동 설치*로 이동합니다.

  에이전트 설치 파일 다운로드 또는 파일 URL 다운로드를 선택하십시오.

- NetApp 지원 사이트 (콘솔에 대한 액세스 권한이 없는 경우 필요) "NetApp 지원 사이트" ,

3. 스크립트를 실행할 수 있는 권한을 할당합니다.

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

여기서 <버전>은 다운로드한 콘솔 에이전트의 버전입니다.

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

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

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

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

+

다음은 CA 서명 인증서로 명시적 프록시 서버를 구성하는 예입니다.

+

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

+
`--proxy` 다음 형식 중 하나를 사용하여 Console 에이전트가 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 위와 같이 \의 ASCII 코드를 사용해야 합니다. **Console** 에이전트는 **@** 문자가 포함된 사용자 이름이나 암호를 지원하지 않습니다. 암호에 다음 특수 문자(& 또는 !)가 포함된 경우 백슬래시를 앞에 붙여 해당 특수 문자를 이스케이프해야 합니다.

+ 예를 들면:

+ http://bxpproxyuser:netapp1\!@address:3128

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

   a. 콘솔 에이전트 가상 머신에 SSH를 실행합니다.

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

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

      예를 들어:

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

   a. 콘솔 에이전트 가상 머신을 재부팅합니다.

2. 설치가 완료될 때까지 기다리세요.

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

   설치에 실패하면 설치 보고서와 로그를 보고 문제를 해결하는 데 도움이 됩니다."설치 문제를 해결하는 방법을 알아보세요."

1. 콘솔 에이전트 가상 머신에 연결된 호스트에서 웹 브라우저를 열고 다음 URL을 입력합니다.

   https://ipaddress

2. 로그인 후 콘솔 에이전트를 설정하세요.

   a. 콘솔 에이전트와 연결할 조직을 지정합니다.

   b. 시스템 이름을 입력하세요.

   c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

      이 단계에서는 표준 모드에서 콘솔을 사용하는 방법을 설명하므로 제한 모드를 비활성화해야 합니다. 보안 환경이 있고 백엔드 서비스에서 이 계정의 연결을 끊으려는 경우에만 제한 모드를 활성화해야 합니다. 그렇다면 ,"제한 모드에서 NetApp Console 시작하기 위한 단계를 따르세요." .

   d. *시작하기*를 선택하세요.

설치에 실패하면 로그와 보고서를 보고 문제 해결에 도움을 받을 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

콘솔 에이전트를 생성한 동일한 Google Cloud 계정에 Google Cloud Storage 버킷이 있는 경우, 시스템 페이지에 Google Cloud Storage 시스템이 자동으로 표시됩니다. "NetApp Console 에서 Google Cloud Storage를 관리하는 방법을 알아보세요."

8단계**:** 콘솔 에이전트에 권한 제공

이전에 설정한 Google Cloud 권한을 콘솔 에이전트에 제공해야 합니다. 권한을 제공하면 콘솔 에이전트가 Google Cloud에서 데이터 및 스토리지 인프라를 관리할 수 있습니다.

단계

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

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

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

온프레미스에 에이전트 설치

온프레미스에 콘솔 에이전트를 수동으로 설치합니다.

온프레미스에 콘솔 에이전트를 설치한 다음 로그인하여 콘솔 조직에서 작동하도록 설정합니다.

VMWare 사용자인 경우 OVA를 사용하여 VCenter에 콘솔 에이전트를 설치할 수 있습니다."VCenter에 에이전트를 설치하는 방법에 대해 자세히 알아보세요."

설치하기 전에 호스트(VM 또는 Linux 호스트)가 요구 사항을 충족하는지 확인하고 콘솔 에이전트가 인터넷과 대상 네트워크에 아웃바운드 액세스할 수 있는지 확인해야 합니다. NetApp 데이터 서비스나 Cloud Volumes ONTAP 과 같은 클라우드 스토리지 옵션을 사용할 계획이라면 콘솔에 추가할 클라우드 공급자에서 자격 증명을 만들어야 합니다. 이렇게 하면 콘솔 에이전트가 사용자를 대신하여 클라우드에서 작업을 수행할 수 있습니다.

콘솔 에이전트 설치를 준비하세요

콘솔 에이전트를 설치하기 전에 설치 요구 사항을 충족하는 호스트 머신이 있는지 확인해야 합니다. 또한 네트워크 관리자와 협력하여 콘솔 에이전트가 필요한 엔드포인트에 대한 아웃바운드 액세스 권한과 대상 네트워크에 대한 연결 권한을 가지고 있는지 확인해야 합니다.

콘솔 에이전트 호스트 요구 사항 검토

운영 체제, RAM 및 포트 요구 사항을 충족하는 x86 호스트에서 콘솔 에이전트를 실행합니다. 콘솔 에이전트를 설치하기 전에 호스트가 이러한 요구 사항을 충족하는지 확인하세요.

콘솔 에이전트는 UID와 GID 범위를 19000~19200으로 예약합니다. 이 범위는 고정되어 있으며 수정할 수 없습니다. 호스트의 타사 소프트웨어가 이 범위 내의 UID나 GID를 사용하는 경우 에이전트 설치가 실패합니다. NetApp 충돌을 피하기 위해 타사 소프트웨어가 없는 호스트를 사용할 것을 권장합니다.

전담 호스트

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

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

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

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

하이퍼바이저

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

운영 체제 및 컨테이너 요구 사항

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

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

운영 체제	지원되는 **OS** 버전	지원되는 에이전트 버전	필수 컨테이너 도구	셀리눅스
강제 모드 또는 허용 모드에서 지원됨		9.1에서 9.4까지 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	3.9.50 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 4.9.4와 podman-compose 1.5.0. Podman 구성 요구 사항 보기 .
강제 모드 또는 허용 모드에서 지원됨		8.6에서 8.10까지 • 영어 버전만 제공됩니다. • 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우 호스트는 에이전트 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 액세스할 수 없습니다.	3.9.50 이상, 콘솔이 표준 모드 또는 제한 모드인 경우	Podman 버전 4.6.1 또는 4.9.4와 podman-compose 1.0.6. Podman 구성 요구 사항 보기 .
강제 모드 또는 허용 모드에서 지원됨	우분투		24.04 장기	표준 모드 또는 제한 모드에서 NetApp Console 사용하는 3.9.45 이상
Docker 엔진 23.06~28.0.0.	지원되지 않음		22.04 장기	3.9.50 이상

콘솔 에이전트가 리소스를 관리할 수 있도록 네트워크 액세스를 설정합니다. 대상 네트워크에 연결하고 특정 엔드포인트에 대한 아웃바운드 인터넷 액세스가 필요합니다.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

웹 기반 **NetApp Console** 사용할 때 컴퓨터에서 연결된 엔드포인트

웹 브라우저에서 콘솔에 액세스하는 컴퓨터는 여러 엔드포인트에 접속할 수 있어야 합니다. 콘솔 에이전트를 설정하고 콘솔을 일상적으로 사용하려면 콘솔을 사용해야 합니다.

"NetApp 콘솔을 위한 네트워킹 준비" .

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

사내에 설치된 콘솔 에이전트는 Google Cloud의 리소스를 관리할 수 없습니다. Google Cloud 리소스를 관리하려면 Google Cloud에 에이전트를 설치해야 합니다.

AWS

콘솔 에이전트가 온프레미스에 설치된 경우 AWS에 배포된 NetApp 시스템(예: Cloud Volumes ONTAP)을 관리하기 위해 다음 AWS 엔드포인트에 대한 네트워크 액세스가 필요합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 리소스를 관리합니다. 엔드포인트는 AWS 지역에 따라 달라집니다. "자세한 내용은 AWS 설명서를 참조하세요."
Amazon FsX for NetApp ONTAP: • api.workloads.netapp.com	웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.

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

하늘빛

콘솔 에이전트가 온프레미스에 설치된 경우 Azure에 배포된 NetApp 시스템(예: Cloud Volumes ONTAP)을 관리하기 위해 다음 Azure 엔드포인트에 대한 네트워크 액세스가 필요합니다.

엔드포인트	목적
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Azure 공용 지역의 리소스를 관리합니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Azure China 지역의 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.

엔드포인트	목적
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

프록시 서버

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

- IP 주소
- 신임장

- HTTPS 인증서

포트

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

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

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

NTP 활성화

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

AWS 또는 **Azure**에 대한 콘솔 에이전트 클라우드 권한 만들기

온프레미스 콘솔 에이전트와 함께 AWS 또는 Azure에서 NetApp 데이터 서비스를 사용하려면 클라우드 공급자에서 권한을 설정한 다음, 콘솔 에이전트를 설치한 후 자격 증명을 추가해야 합니다.

Google Cloud에 있는 모든 리소스를 관리하려면 콘솔 에이전트를 설치해야 합니다.

AWS

온프레미스에 콘솔 에이전트를 설치하는 경우 필요한 권한이 있는 IAM 사용자의 액세스 키를 추가하여 콘솔에 AWS 권한을 제공해야 합니다.

콘솔 에이전트가 온프레미스에 설치된 경우 이 인증 방법을 사용해야 합니다. IAM 역할을 사용할 수 없습니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책을 만듭니다.

   a. *정책 > 정책 만들기*를 선택합니다.

   b. *JSON*을 선택하고 내용을 복사하여 붙여넣습니다."콘솔 에이전트에 대한 IAM 정책" .

   c. 나머지 단계를 완료하여 정책을 만듭니다.

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

   표준 지역의 경우 권한은 두 가지 정책에 걸쳐 분산됩니다. AWS의 관리형 정책에는 최대 문자 크기 제한이 있으므로 두 개의 정책이 필요합니다. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요." .

3. IAM 사용자에게 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"
4. 콘솔 에이전트를 설치한 후 NetApp Console 에 추가할 수 있는 액세스 키가 사용자에게 있는지 확인하세요.

결과

이제 필요한 권한이 있는 IAM 사용자에 대한 액세스 키가 생겼습니다. 콘솔 에이전트를 설치한 후 콘솔에서 이러한 자격 증명을 콘솔 에이전트와 연결합니다.

하늘빛

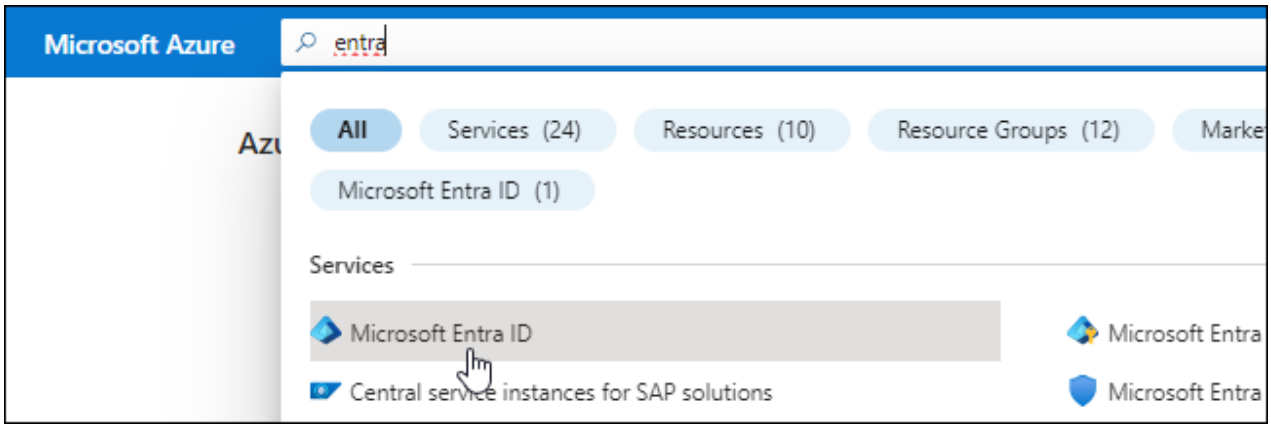
온프레미스에 콘솔 에이전트를 설치하는 경우 Microsoft Entra ID에서 서비스 주체를 설정하고 콘솔 에이전트에 필요한 Azure 자격 증명을 얻어 콘솔 에이전트에 Azure 권한을 제공해야 합니다.

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

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

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

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



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

   AD 애플리케이션과 서비스 주체를 생성했습니다.

역할에 애플리케이션 할당

1. 사용자 정의 역할 만들기:

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

   a. 내용을 복사하세요"콘솔 에이전트에 대한 사용자 정의 역할 권한" JSON 파일에 저장합니다.

   b. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

      사용자가 Cloud Volumes ONTAP 시스템을 생성할 각 Azure 구독에 대한 ID를 추가해야 합니다.

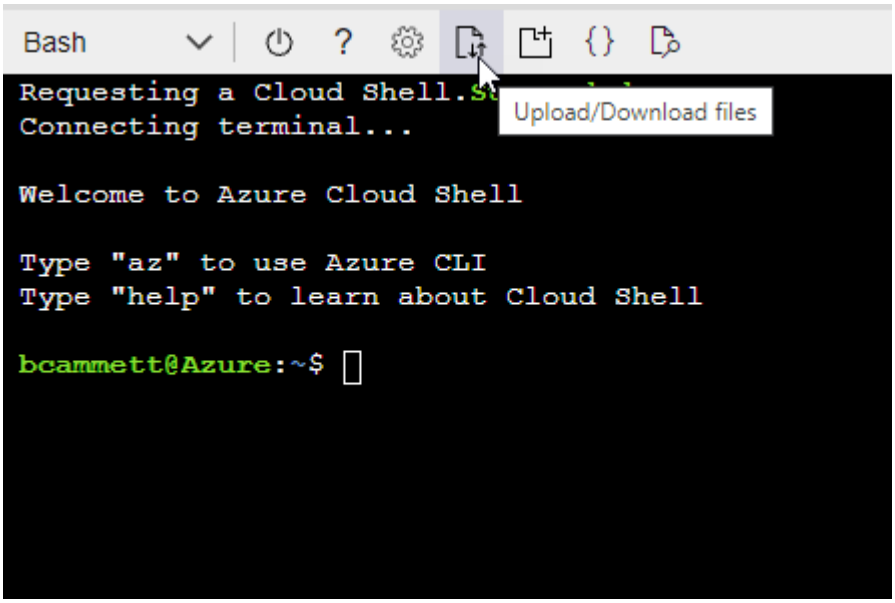
      예

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

   c. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 만듭니다.

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

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

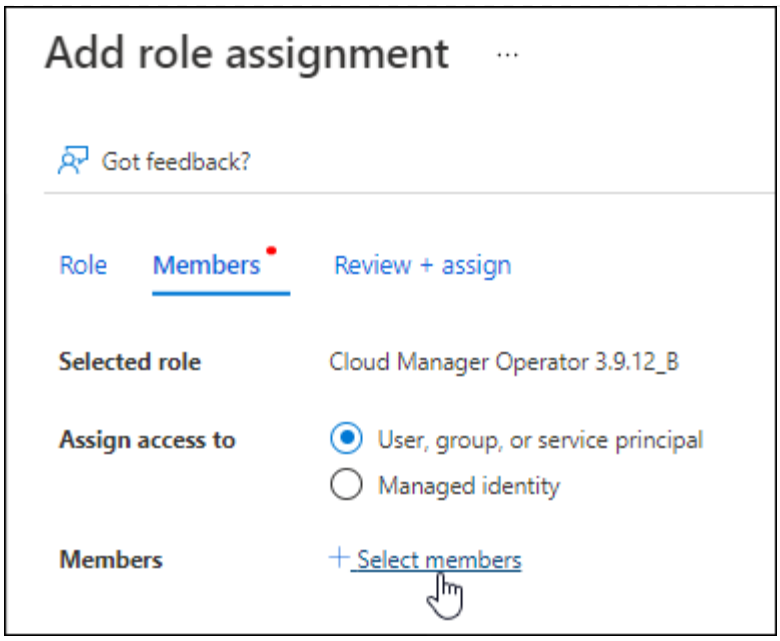


- Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

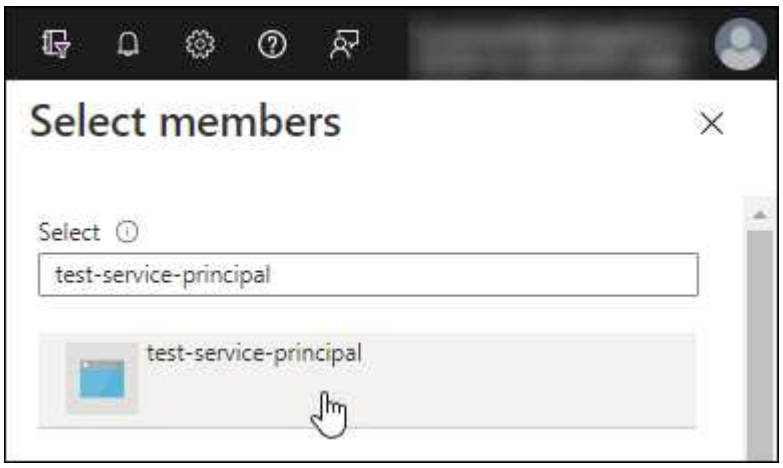
이제 콘솔 에이전트 가상 머신에 할당할 수 있는 콘솔 운영자라는 사용자 지정 역할이 생겼습니다.

2. 역할에 애플리케이션을 할당합니다.
   a. Azure Portal에서 구독 서비스를 엽니다.
   b. 구독을 선택하세요.
   c. *액세스 제어(IAM) > 추가 > 역할 할당 추가*를 선택합니다.
   d. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.
   e. 멤버 탭에서 다음 단계를 완료하세요.
      - *사용자, 그룹 또는 서비스 주체*를 선택된 상태로 유지합니다.
      - *멤버 선택*을 선택하세요.



- 애플리케이션 이름을 검색하세요.

  예를 들면 다음과 같습니다.



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

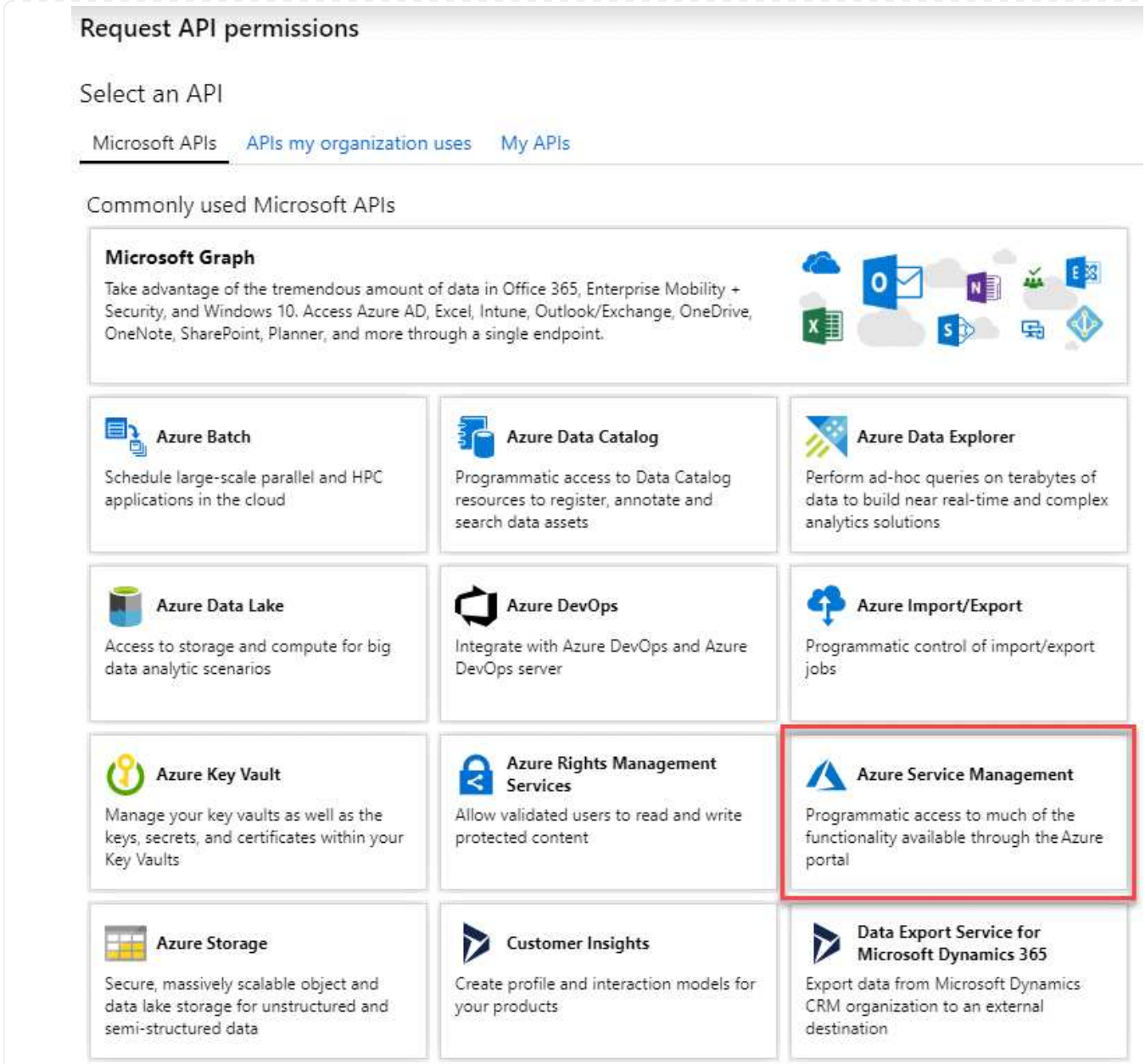
f. *검토 + 할당*을 선택하세요.

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

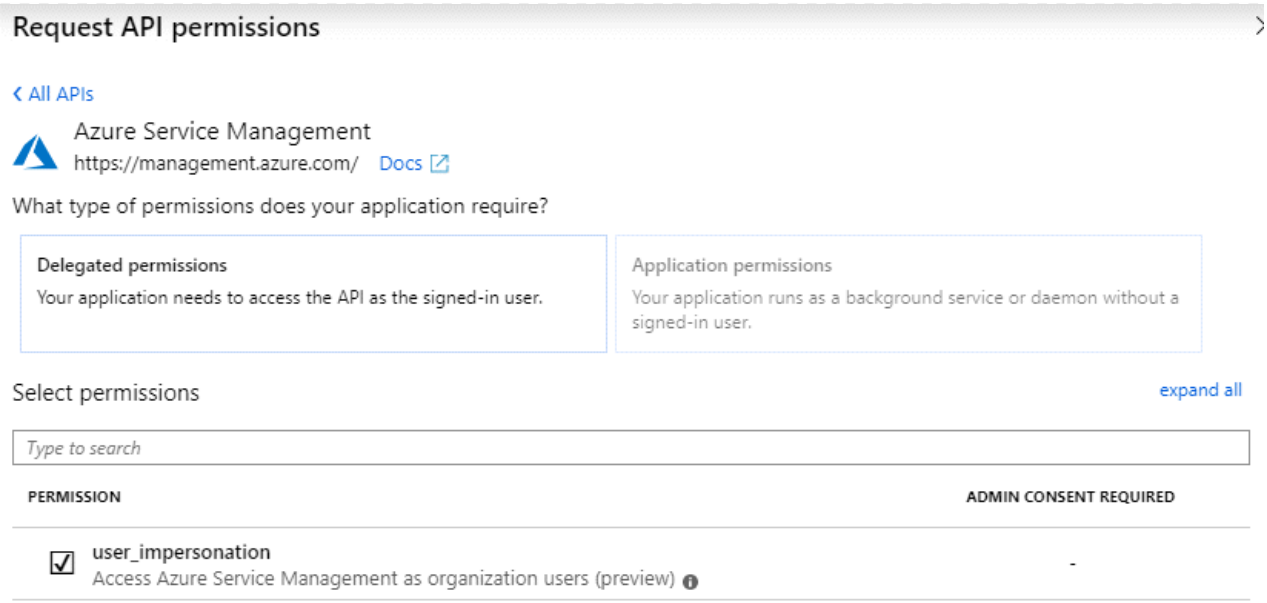
여러 Azure 구독에서 Cloud Volumes ONTAP 배포하려면 각 구독에 서비스 주체를 바인딩해야 합니다. NetApp Console 에서 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한 추가

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

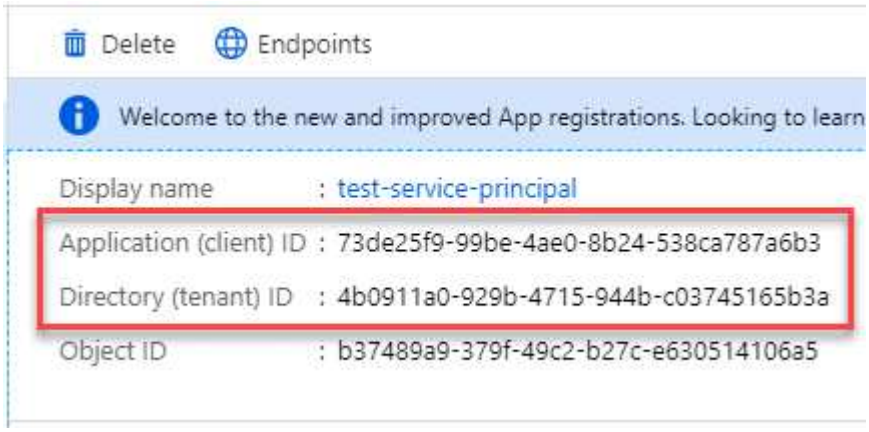


4. *조직 사용자로 Azure Service Management에 액세스*를 선택한 다음 *권한 추가*를 선택합니다.



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

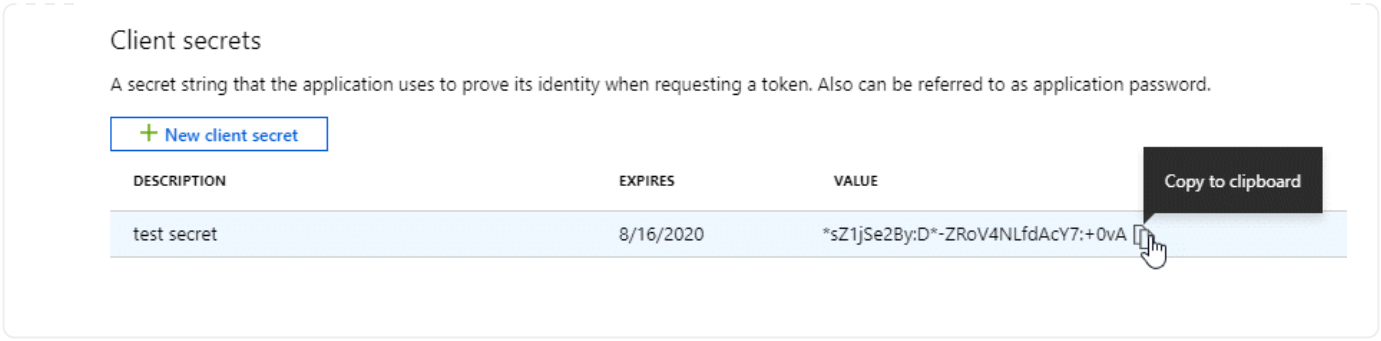
1. **Microsoft Entra ID** 서비스에서 *앱 등록*을 선택하고 애플리케이션을 선택합니다.
2. *애플리케이션(클라이언트) ID*와 *디렉토리(테넌트) ID*를 복사합니다.



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

클라이언트 비밀을 생성하세요

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



콘솔 에이전트를 수동으로 설치합니다.

콘솔 에이전트를 수동으로 설치하는 경우 요구 사항을 충족하도록 컴퓨터 환경을 준비해야 합니다. Linux 컴퓨터가 필요하며, Linux 운영 체제에 따라 Podman이나 Docker를 설치해야 합니다.

Podman 또는 Docker Engine 설치

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

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

  지원되는 Podman 버전 보기 .

- Ubuntu에는 Docker 엔진이 필요합니다.

  지원되는 Docker Engine 버전 보기 .

예 **4.** 단계

포드만

Podman을 설치하고 구성하려면 다음 단계를 따르세요.

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

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

단계

1. 호스트에 podman-docker 패키지가 설치되어 있다면 제거합니다.

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

2. Podman을 설치하세요.

   공식 Red Hat Enterprise Linux 저장소에서 Podman을 다운로드할 수 있습니다.

   a. Red Hat Enterprise Linux 9.6의 경우:

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

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

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

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

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

   c. Red Hat Enterprise Linux 8의 경우:

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

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

3. podman.socket 서비스를 활성화하고 시작합니다.

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

4. python3를 설치합니다.

```
sudo dnf install python3
```

5. 시스템에 EPEL 저장소 패키지가 아직 없으면 설치하세요.

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

6. Red Hat Enterprise 9를 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

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

   +

   a. podman-compose 패키지 1.5.0을 설치합니다.

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

7. Red Hat Enterprise Linux 8을 사용하는 경우:

   a. EPEL 저장소 패키지를 설치하세요.

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

   b. podman-compose 패키지 1.0.6을 설치합니다.

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

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

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

i. 다음 명령을 실행하여 networkBackend가 CNI로 설정되어 있는지 확인하세요.

```
podman info | grep networkBackend
```

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

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

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

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

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

v. Podman을 다시 시작하세요.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

도커 엔진

Docker Engine을 설치하려면 Docker 설명서를 따르세요.

단계

1. "Docker에서 설치 지침 보기"

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

2. Docker가 활성화되어 실행 중인지 확인하세요.

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

콘솔 에이전트를 수동으로 설치합니다.

기존 온프레미스 Linux 호스트에 콘솔 에이전트 소프트웨어를 다운로드하여 설치합니다.

시작하기 전에

다음 사항이 있어야 합니다.

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

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

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

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

이 작업에 관하여

설치 후, 새로운 버전이 나오면 콘솔 에이전트가 자동으로 업데이트됩니다.

단계

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

```
unset http_proxy
unset https_proxy
```

   이러한 시스템 변수를 제거하지 않으면 설치가 실패합니다.

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

     에이전트 설치 파일 다운로드 또는 파일 URL 다운로드를 선택하십시오.

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

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

   여기서 <버전>은 다운로드한 콘솔 에이전트의 버전입니다.

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

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

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

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

+

다음은 CA 서명 인증서로 명시적 프록시 서버를 구성하는 예입니다.

+

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

+
`--proxy` 다음 형식 중 하나를 사용하여 Console 에이전트가 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 위와 같이 \의 ASCII 코드를 사용해야 합니다. **Console** 에이전트는 **@** 문자가 포함된 사용자 이름이나 암호를 지원하지 않습니다. 암호에 다음 특수 문자(& 또는 !)가 포함된 경우 백슬래시를 앞에 붙여 해당 특수 문자를 이스케이프해야 합니다.

+ 예를 들면:

+ http://bxpproxyuser:netapp1\!@address:3128

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

   a. 콘솔 에이전트 가상 머신에 SSH를 실행합니다.

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

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

      예를 들어:

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

a. 콘솔 에이전트 가상 머신을 재부팅합니다.

다음은 무엇인가요?

NetApp Console 내에서 콘솔 에이전트를 등록해야 합니다.

NetApp Console 에 콘솔 에이전트 등록

콘솔에 로그인하고 콘솔 에이전트를 조직과 연결합니다. 로그인 방법은 콘솔을 사용하는 모드에 따라 달라집니다. 표준 모드로 콘솔을 사용하는 경우 SaaS 웹사이트를 통해 로그인합니다. 제한 모드에서 콘솔을 사용하는 경우 콘솔 에이전트 호스트에서 로컬로 로그인합니다.

단계

1. 웹 브라우저를 열고 콘솔 에이전트 호스트 URL을 입력하세요.

   콘솔 호스트 URL은 호스트 구성에 따라 로컬호스트, 개인 IP 주소 또는 공용 IP 주소가 될 수 있습니다. 예를 들어, 콘솔 에이전트가 공용 IP 주소가 없는 퍼블릭 클라우드에 있는 경우 콘솔 에이전트 호스트에 연결된 호스트의 개인 IP 주소를 입력해야 합니다.

2. 가입하거나 로그인하세요.
3. 로그인 후 콘솔을 설정하세요.
   a. 콘솔 에이전트와 연결할 콘솔 조직을 지정합니다.
   b. 시스템 이름을 입력하세요.
   c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

      콘솔 에이전트가 온프레미스에 설치된 경우 제한 모드는 지원되지 않습니다.

   d. *시작하기*를 선택하세요.

NetApp Console 에 클라우드 공급자 자격 증명 제공

콘솔 에이전트를 설치하고 설정한 후 클라우드 자격 증명을 추가하여 콘솔 에이전트가 AWS 또는 Azure에서 작업을 수행하는 데 필요한 권한을 갖도록 합니다.

AWS

시작하기 전에

AWS 자격 증명을 방금 만든 경우 사용할 수 있게 되는 데 몇 분이 걸릴 수 있습니다. 콘솔에 자격 증명을 추가하기 전에 몇 분 정도 기다리세요.

단계

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

이제 다음으로 이동할 수 있습니다. "NetApp Console" 콘솔 에이전트를 사용하려면.

하늘빛

시작하기 전에

Azure 자격 증명을 방금 만든 경우 사용 가능해지는 데 몇 분 정도 걸릴 수 있습니다. 콘솔 에이전트에 자격 증명을 추가하기 전에 몇 분 정도 기다리세요.

단계

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

결과

이제 콘솔 에이전트는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 갖게 되었습니다. 이제 다음으로 이동할 수 있습니다. "NetApp Console" 콘솔 에이전트를 사용하려면.

VCenter를 사용하여 온프레미스에 콘솔 에이전트 설치

VMWare 사용자인 경우 OVA를 사용하여 VCenter에 콘솔 에이전트를 설치할 수 있습니다.

OVA 다운로드 또는 URL은 NetApp Console 통해 이용할 수 있습니다.

VCenter 도구와 함께 콘솔 에이전트를 설치하면 VM 웹 콘솔을 사용하여 유지 관리 작업을 수행할 수 있습니다."에이전트의 VM 콘솔에 대해 자세히 알아보세요."

콘솔 에이전트 설치를 준비하세요

설치하기 전에 VM 호스트가 요구 사항을 충족하는지, 콘솔 에이전트가 인터넷과 대상 네트워크에 액세스할 수 있는지 확인하세요. NetApp 데이터 서비스 또는 Cloud Volumes ONTAP 사용하려면 콘솔 에이전트가 사용자를 대신하여 작업을 수행할 수 있도록 클라우드 공급자 자격 증명을 생성하세요.

콘솔 에이전트 호스트 요구 사항 검토

콘솔 에이전트를 설치하기 전에 호스트 머신이 설치 요구 사항을 충족하는지 확인하세요.

- CPU: 8개 코어 또는 8개 vCPU
- 램: 32GB
- 디스크 공간: 165GB(두꺼운 프로비저닝)
- vSphere 7.0 이상
- ESXi 호스트 7.03 이상

ESXi 호스트에 직접 설치하는 대신 vCenter 환경에 에이전트를 설치하세요.

콘솔 에이전트에 대한 네트워크 액세스 설정

네트워크 관리자와 협력하여 콘솔 에이전트가 필요한 엔드포인트에 대한 아웃바운드 액세스 권한과 대상 네트워크에 대한 연결을 가지고 있는지 확인하세요.

대상 네트워크에 대한 연결

콘솔 에이전트를 사용하려면 시스템을 만들고 관리하려는 위치에 대한 네트워크 연결이 필요합니다. 예를 들어, Cloud Volumes ONTAP 시스템이나 온프레미스 환경의 스토리지 시스템을 만들 계획인 네트워크입니다.

아웃바운드 인터넷 접속

콘솔 에이전트를 배포하는 네트워크 위치에는 특정 엔드포인트에 연결하기 위한 아웃바운드 인터넷 연결이 있어야 합니다.

웹 기반 **NetApp Console** 사용할 때 컴퓨터에서 연결된 엔드포인트

웹 브라우저에서 콘솔에 액세스하는 컴퓨터는 여러 엔드포인트에 접속할 수 있어야 합니다. 콘솔 에이전트를 설정하고 콘솔을 일상적으로 사용하려면 콘솔을 사용해야 합니다.

"NetApp 콘솔을 위한 네트워킹 준비" .

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

사내에 설치된 콘솔 에이전트로는 Google Cloud의 리소스를 관리할 수 없습니다. Google Cloud 리소스를 관리하려면 Google Cloud에 에이전트를 설치하세요.

AWS

콘솔 에이전트가 온프레미스에 설치된 경우 AWS에 배포된 NetApp 시스템(예: Cloud Volumes ONTAP)을 관리하기 위해 다음 AWS 엔드포인트에 대한 네트워크 액세스가 필요합니다.

콘솔 에이전트에서 연락한 엔드포인트

콘솔 에이전트는 일상 업무를 위해 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하기 위해 다음 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

아래 나열된 엔드포인트는 모두 CNAME 항목입니다.

엔드포인트	목적
AWS 서비스(amazonaws.com): • 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 리소스를 관리합니다. 엔드포인트는 AWS 지역에 따라 달라집니다. "자세한 내용은 AWS 설명서를 참조하세요."
Amazon FsX for NetApp ONTAP: • api.workloads.netapp.com	웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 ONTAP 기반 워크로드용 FSx를 관리하고 운영합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.

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

하늘빛

콘솔 에이전트가 온프레미스에 설치된 경우 Azure에 배포된 NetApp 시스템(예: Cloud Volumes ONTAP)을 관리하기 위해 다음 Azure 엔드포인트에 대한 네트워크 액세스가 필요합니다.

엔드포인트	목적
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Azure 공용 지역의 리소스를 관리합니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Azure China 지역의 리소스를 관리합니다.
\ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.

엔드포인트	목적
\ https://signin.b2c.netapp.com	NetApp 지원 사이트(NSS) 자격 증명을 업데이트하거나 NetApp Console 에 새로운 NSS 자격 증명을 추가합니다.
\ https://support.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보내고 Cloud Volumes ONTAP 에 대한 소프트웨어 업데이트를 받습니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. • 새로운 에이전트를 배포할 때 유효성 검사를 통해 현재 엔드포인트에 대한 연결성을 테스트합니다. 당신이 사용하는 경우"이전 종료점" , 유효성 검사에 실패합니다. 이러한 실패를 방지하려면 유효성 검사를 건너뛰세요. 이전 엔드포인트는 계속 지원되지만 NetApp 가능한 한 빨리 현재 엔드포인트에 맞게 방화벽 규칙을 업데이트할 것을 권장합니다. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" . • 방화벽의 현재 엔드포인트로 업데이트하면 기존 에이전트도 계속 작동합니다.

프록시 서버

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

- IP 주소
- 신임장

- HTTPS 인증서

포트

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

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

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

NTP 활성화

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

AWS 또는 **Azure**에 대한 콘솔 에이전트 클라우드 권한 만들기

온프레미스 콘솔 에이전트와 함께 AWS 또는 Azure에서 NetApp 데이터 서비스를 사용하려면 클라우드 공급자에서 권한을 설정해야 합니다. 그래야 콘솔 에이전트를 설치한 후 자격 증명을 추가할 수 있습니다.

사내에 설치된 콘솔 에이전트로는 Google Cloud의 리소스를 관리할 수 없습니다. Google Cloud 리소스를 관리하려면 Google Cloud에 에이전트를 설치해야 합니다.

AWS

온프레미스 콘솔 에이전트의 경우 IAM 사용자 액세스 키를 추가하여 AWS 권한을 제공합니다.

온프레미스 콘솔 에이전트에는 IAM 사용자 액세스 키를 사용하세요. 온프레미스 콘솔 에이전트에서는 IAM 역할이 지원되지 않습니다.

단계

1. AWS 콘솔에 로그인하고 IAM 서비스로 이동합니다.
2. 정책을 만듭니다.

   a. *정책 > 정책 만들기*를 선택합니다.

   b. *JSON*을 선택하고 내용을 복사하여 붙여넣습니다."콘솔 에이전트에 대한 IAM 정책" .

   c. 나머지 단계를 완료하여 정책을 만듭니다.

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

   표준 지역의 경우 권한은 두 가지 정책에 걸쳐 분산됩니다. AWS의 관리형 정책에는 최대 문자 크기 제한이 있으므로 두 개의 정책이 필요합니다. "콘솔 에이전트에 대한 IAM 정책에 대해 자세히 알아보세요." .

3. IAM 사용자에게 정책을 연결합니다.
   - "AWS 설명서: IAM 역할 생성"
   - "AWS 설명서: IAM 정책 추가 및 제거"
4. 콘솔 에이전트를 설치한 후 NetApp Console 에 추가할 수 있는 액세스 키가 사용자에게 있는지 확인하세요.

결과

이제 필요한 권한이 있는 IAM 사용자 액세스 키가 있어야 합니다. 콘솔 에이전트를 설치한 후 콘솔에서 이러한 자격 증명을 콘솔 에이전트와 연결합니다.

하늘빛

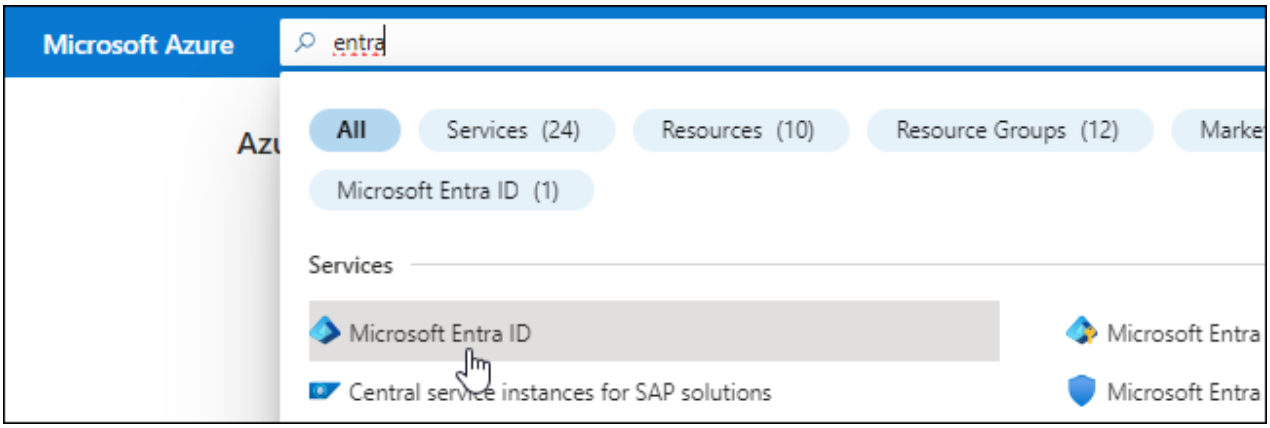
온프레미스에 콘솔 에이전트를 설치하는 경우 Microsoft Entra ID에서 서비스 주체를 설정하고 콘솔 에이전트에 필요한 Azure 자격 증명을 가져와서 콘솔 에이전트에 Azure 권한을 부여해야 합니다.

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

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

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

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



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

   AD 애플리케이션과 서비스 주체를 생성했습니다.

역할에 애플리케이션 할당

1. 사용자 정의 역할 만들기:

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

   a. 내용을 복사하세요"콘솔 에이전트에 대한 사용자 정의 역할 권한" JSON 파일에 저장합니다.

   b. 할당 가능한 범위에 Azure 구독 ID를 추가하여 JSON 파일을 수정합니다.

      사용자가 Cloud Volumes ONTAP 시스템을 생성할 각 Azure 구독에 대한 ID를 추가해야 합니다.

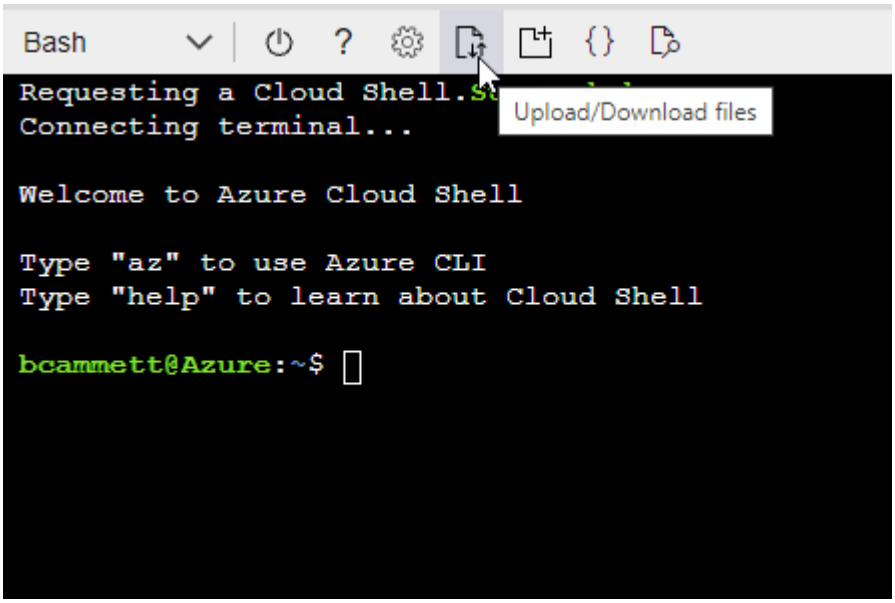
      예

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

   c. JSON 파일을 사용하여 Azure에서 사용자 지정 역할을 만듭니다.

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

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



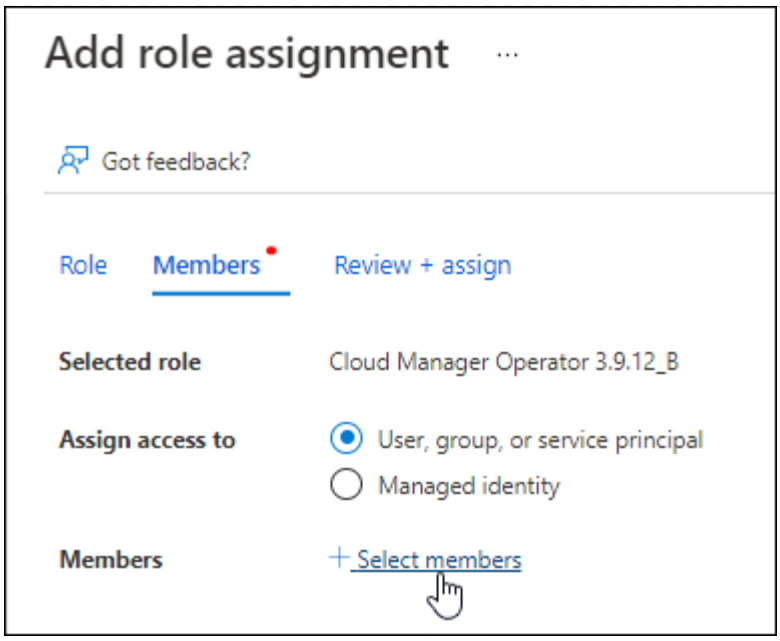
- Azure CLI를 사용하여 사용자 지정 역할을 만듭니다.

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

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

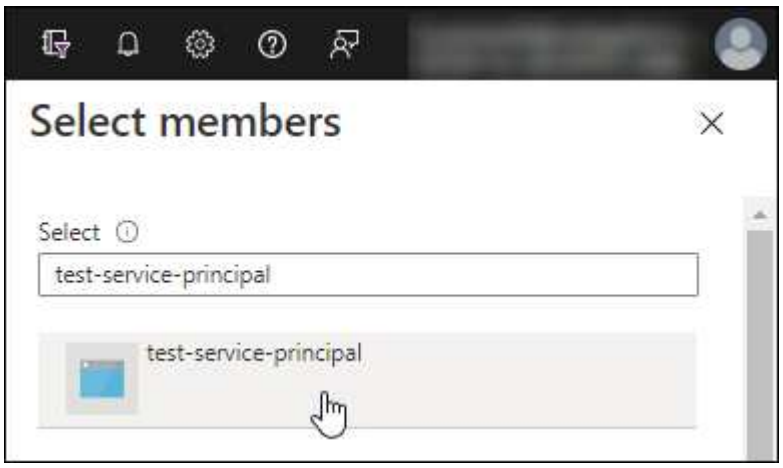
2. 역할에 애플리케이션을 할당합니다.

   a. Azure Portal에서 구독 서비스를 엽니다.
   b. 구독을 선택하세요.
   c. *액세스 제어(IAM) > 추가 > 역할 할당 추가*를 선택합니다.
   d. 역할 탭에서 콘솔 운영자 역할을 선택하고 *다음*을 선택합니다.
   e. 멤버 탭에서 다음 단계를 완료하세요.
      - *사용자, 그룹 또는 서비스 주체*를 선택된 상태로 유지합니다.
      - *멤버 선택*을 선택하세요.



- 애플리케이션 이름을 검색하세요.

  예를 들면 다음과 같습니다.



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

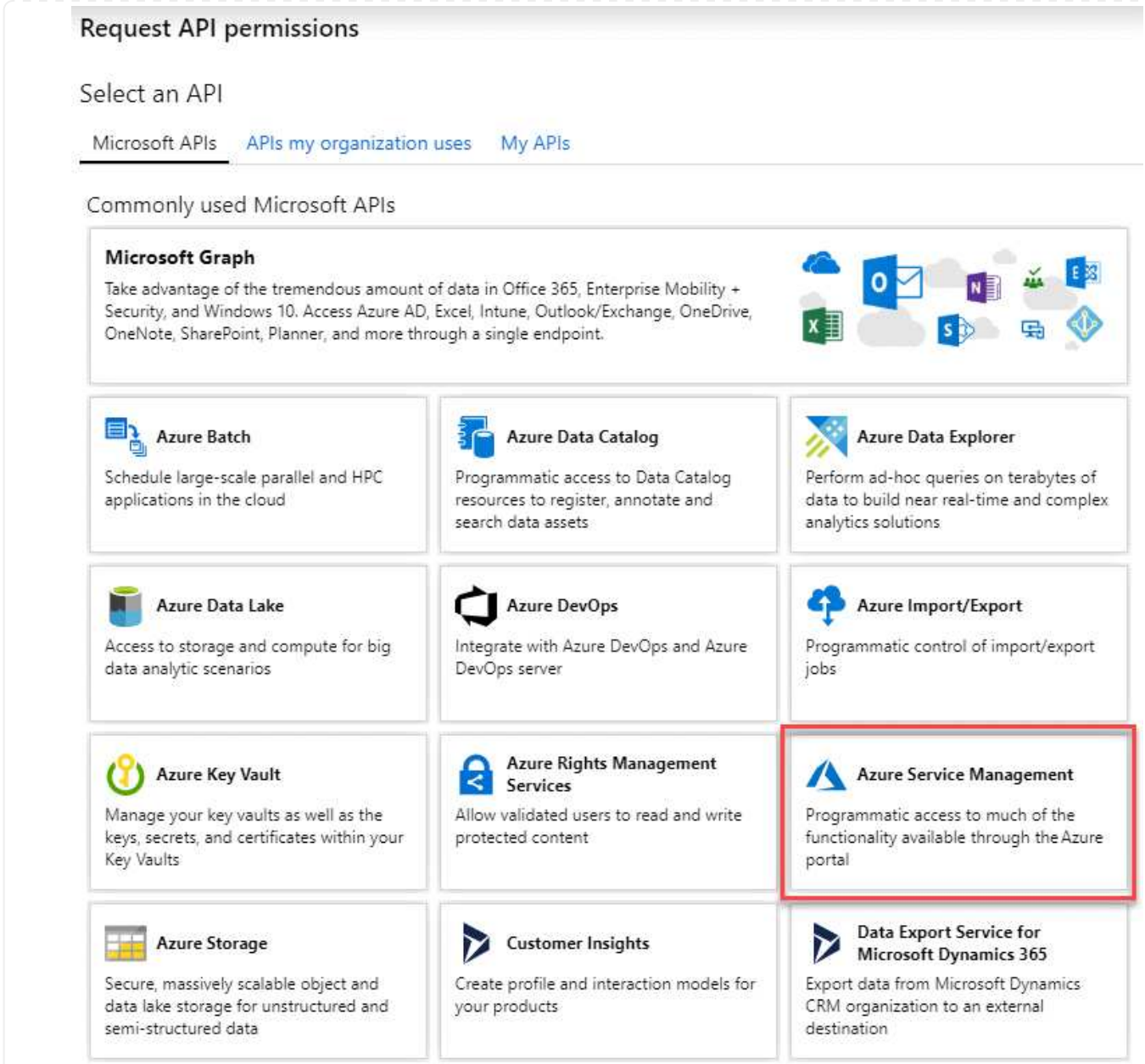
f. *검토 + 할당*을 선택하세요.

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

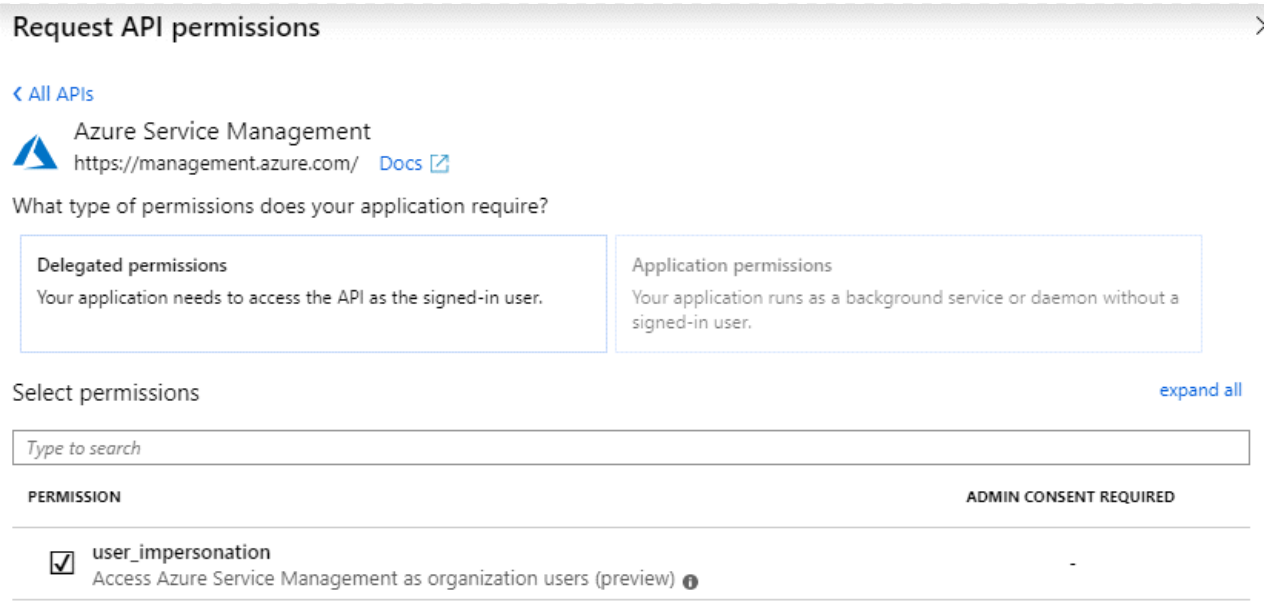
여러 Azure 구독에서 Cloud Volumes ONTAP 배포하려면 각 구독에 서비스 주체를 바인딩해야 합니다. NetApp Console 에서 Cloud Volumes ONTAP 배포할 때 사용할 구독을 선택할 수 있습니다.

Windows Azure 서비스 관리 **API** 권한 추가

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

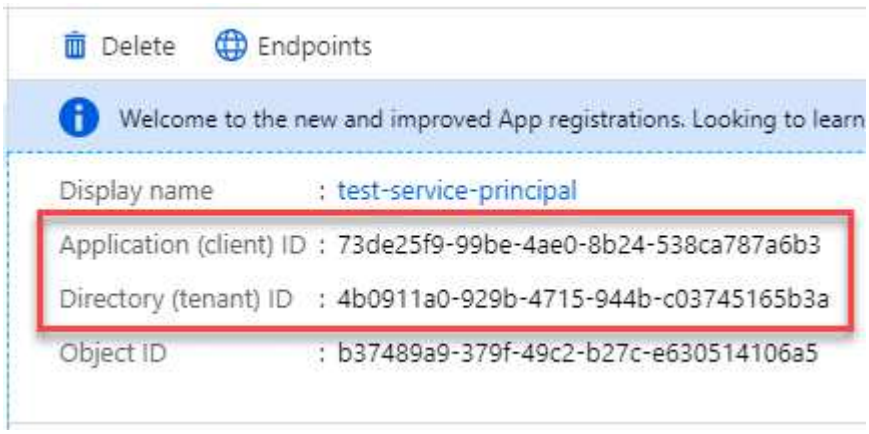


4. *조직 사용자로 Azure Service Management에 액세스*를 선택한 다음 *권한 추가*를 선택합니다.



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

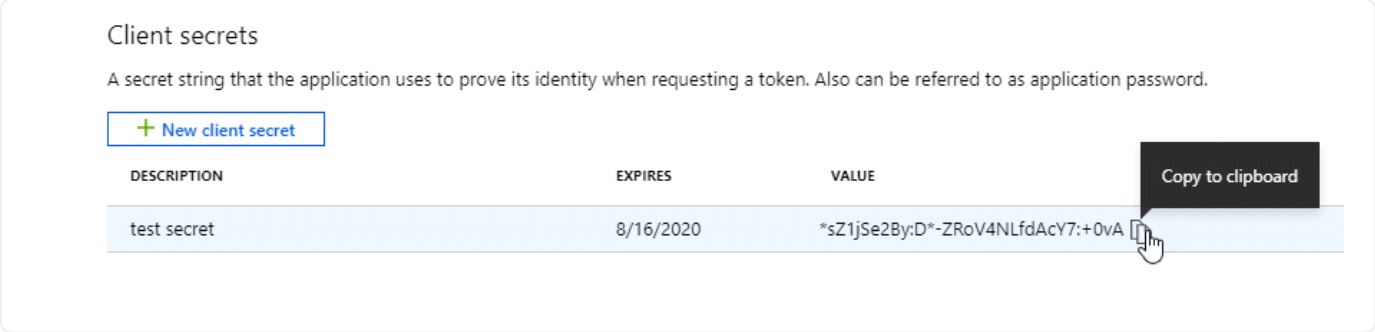
1. **Microsoft Entra ID** 서비스에서 *앱 등록*을 선택하고 애플리케이션을 선택합니다.
2. *애플리케이션(클라이언트) ID*와 *디렉토리(테넌트) ID*를 복사합니다.



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

클라이언트 비밀을 생성하세요

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



VCenter 환경에 콘솔 에이전트 설치

NetApp VCenter 환경에 콘솔 에이전트를 설치하는 것을 지원합니다. OVA 파일에는 VMware 환경에 배포할 수 있는 미리 구성된 VM 이미지가 포함되어 있습니다. 파일 다운로드나 URL 배포는 NetApp Console 에서 직접 사용할 수 있습니다. 여기에는 콘솔 에이전트 소프트웨어와 자체 서명 인증서가 포함됩니다.

OVA를 다운로드하거나 URL을 복사하세요

OVA를 다운로드하거나 NetApp Console 에서 OVA URL을 직접 복사하세요.

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 *에이전트 배포 > 온프레미스*를 선택합니다.
3. *OVA 포함*을 선택하세요.
4. OVA를 다운로드하거나 URL을 복사하여 VCenter에서 사용하세요.

VCenter에 에이전트를 배포하세요

에이전트를 배포하려면 VCenter 환경에 로그인하세요.

단계

1. 환경에 필요한 경우 신뢰할 수 있는 인증서에 자체 서명된 인증서를 업로드하세요. 설치 후 이 인증서를 교체합니다 ."자체 서명 인증서를 교체하는 방법을 알아보세요."
2. 콘텐츠 라이브러리나 로컬 시스템에서 OVA를 배포합니다.

로컬 시스템에서	콘텐츠 라이브러리에서
a. 마우스 오른쪽 버튼을 클릭하고 *OVF 템플릿 배포…*를 선택합니다. b. URL에서 OVA 파일을 선택하거나 해당 위치를 찾은 후 *다음*을 선택합니다.	a. 콘텐츠 라이브러리로 이동하여 콘솔 에이전트 OVA를 선택합니다. b. 작업 > *이 템플릿에서 새 VM*을 선택합니다.

3. OVF 템플릿 배포 마법사를 완료하여 콘솔 에이전트를 배포합니다.
4. VM의 이름과 폴더를 선택한 후 *다음*을 선택합니다.
5. 컴퓨팅 리소스를 선택한 후 *다음*을 선택합니다.
6. 템플릿의 세부 정보를 검토한 후 *다음*을 선택하세요.
7. 라이센스 계약에 동의한 후 *다음*을 선택하세요.
8. 사용할 프록시 구성 유형을 선택하세요: 명시적 프록시, 투명 프록시 또는 프록시 없음.

9. VM을 배포할 데이터 저장소를 선택한 후 *다음*을 선택합니다. 호스트 요구 사항을 충족하는지 확인하세요.
10. VM을 연결할 네트워크를 선택한 후 *다음*을 선택합니다. 네트워크가 IPv4이고 필요한 엔드포인트에 대한 아웃바운드 인터넷 액세스가 가능한지 확인하세요.
11. 템플릿 사용자 지정 창에서 다음 필드를 완료하세요.
    - 프록시 정보
      - 명시적 프록시를 선택한 경우 프록시 서버 호스트 이름이나 IP 주소, 포트 번호, 사용자 이름, 비밀번호를 입력하세요.
      - 투명 프록시를 선택한 경우 해당 인증서를 업로드하세요.
    - 가상 머신 구성
      - 구성 확인 건너뛰기: 이 확인란은 기본적으로 선택 해제되어 있으며, 이는 에이전트가 네트워크 액세스를 검증하기 위해 구성 확인을 실행한다는 것을 의미합니다.
        - NetApp 에이전트의 구성 검사를 설치 과정에 포함하도록 이 상자를 선택하지 않을 것을 권장합니다. 구성 검사는 에이전트가 필요한 엔드포인트에 대한 네트워크 액세스 권한이 있는지 확인합니다. 연결 문제로 인해 배포에 실패하면 에이전트 호스트에서 유효성 검사 보고서와 로그에 액세스할 수 있습니다. 어떤 경우에는 에이전트가 네트워크에 접속할 수 있다고 확신하는 경우 검사를 건너뛸 수 있습니다. 예를 들어, 여전히 다음을 사용하고 있는 경우"이전 종료점" 에이전트 업그레이드에 사용되면 유효성 검사가 오류로 인해 실패합니다. 이를 방지하려면 유효성 검사 없이 설치하려면 확인란을 선택하세요. "엔드포인트 목록을 업데이트하는 방법을 알아보세요" .
      - 유지관리 비밀번호 : 비밀번호를 설정하세요. `maint` 에이전트 유지 관리 콘솔에 액세스할 수 있는 사용자입니다.
      - **NTP** 서버: 시간 동기화를 위해 하나 이상의 NTP 서버를 지정합니다.
      - 호스트 이름: 이 VM의 호스트 이름을 설정합니다. 검색 도메인을 포함하면 안 됩니다. 예를 들어, console10.searchdomain.company.com의 FQDN은 console10으로 입력해야 합니다.
      - 기본 **DNS**: 이름 확인에 사용할 기본 DNS 서버를 지정합니다.
      - 보조 **DNS**: 이름 확인에 사용할 보조 DNS 서버를 지정합니다.
      - 검색 도메인: 호스트 이름을 확인할 때 사용할 검색 도메인 이름을 지정합니다. 예를 들어, FQDN이 console10.searchdomain.company.com이면 searchdomain.company.com을 입력합니다.
      - **IPv4** 주소: 호스트 이름에 매핑된 IP 주소입니다.
      - **IPv4** 서브넷 마스크: IPv4 주소의 서브넷 마스크입니다.
      - **IPv4** 게이트웨이 주소: IPv4 주소에 대한 게이트웨이 주소입니다.
12. *다음*을 선택하세요.
13. 완료 준비 창에서 세부 정보를 검토하고 *마침*을 선택하세요.

    vSphere 작업 표시줄에는 콘솔 에이전트가 배포됨에 따라 진행 상황이 표시됩니다.
14. VM의 전원을 켭니다.

> 배포에 실패하면 에이전트 호스트에서 검증 보고서와 로그에 액세스할 수 있습니다."설치 문제를 해결하는 방법을 알아보세요."

NetApp Console 에 콘솔 에이전트 등록

콘솔에 로그인하고 콘솔 에이전트를 조직과 연결합니다. 로그인 방법은 콘솔을 사용하는 모드에 따라 달라집니다. 표준 모드로 콘솔을 사용하는 경우 SaaS 웹사이트를 통해 로그인합니다. 제한 모드나 비공개 모드로 콘솔을 사용하는 경우 콘솔 에이전트 호스트에서 로컬로 로그인합니다.

단계

1. 웹 브라우저를 열고 콘솔 에이전트 호스트 URL을 입력하세요.

   콘솔 호스트 URL은 호스트 구성에 따라 로컬호스트, 개인 IP 주소 또는 공용 IP 주소가 될 수 있습니다. 예를 들어, 콘솔 에이전트가 공용 IP 주소가 없는 퍼블릭 클라우드에 있는 경우 콘솔 에이전트 호스트에 연결된 호스트의 개인 IP 주소를 입력해야 합니다.

2. 가입하거나 로그인하세요.
3. 로그인 후 콘솔을 설정하세요.
   a. 콘솔 에이전트와 연결할 콘솔 조직을 지정합니다.
   b. 시스템 이름을 입력하세요.
   c. *보안된 환경에서 실행하고 있습니까?*에서 제한 모드를 비활성화하세요.

      콘솔 에이전트가 온프레미스에 설치된 경우 제한 모드는 지원되지 않습니다.

   d. *시작하기*를 선택하세요.

콘솔에 클라우드 공급자 자격 증명 추가

콘솔 에이전트를 설치하고 설정한 후 클라우드 자격 증명을 추가하여 콘솔 에이전트가 AWS 또는 Azure에서 작업을 수행하는 데 필요한 권한을 갖도록 합니다.

AWS

시작하기 전에

AWS 자격 증명을 방금 만든 경우 사용할 수 있게 되는 데 몇 분이 걸릴 수 있습니다. 콘솔에 자격 증명을 추가하기 전에 몇 분 정도 기다리세요.

단계

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

이제 다음으로 이동할 수 있습니다. "NetApp Console" 콘솔 에이전트를 사용하려면.

하늘빛

시작하기 전에

Azure 자격 증명을 방금 만든 경우 사용 가능해지는 데 몇 분 정도 걸릴 수 있습니다. 콘솔 에이전트에 자격 증명을 추가하기 전에 몇 분 정도 기다리세요.

단계

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

결과

이제 콘솔 에이전트는 Azure에서 사용자를 대신하여 작업을 수행하는 데 필요한 권한을 갖게 되었습니다. 이제 다음으로 이동할 수 있습니다. "NetApp Console" 콘솔 에이전트를 사용하려면.

온프레미스 콘솔 에이전트용 포트

콘솔 에이전트는 온프레미스 Linux 호스트에 수동으로 설치되는 경우 인바운드 포트를

사용합니다. 계획 목적으로 다음 항구를 참조하세요.

이러한 인바운드 규칙은 모든 NetApp Console 배포 모드에 적용됩니다.

규약	포트	목적
HTTP	80	• 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다. • Cloud Volumes ONTAP 업그레이드 프로세스 중에 사용됨
HTTPS	443	클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTPS 액세스를 제공합니다.