참조

NetApp Console setup and administration

NetApp
January 23, 2026

목차

참조

에이전트 유지 관리 콘솔

유지 관리 콘솔을 사용한 에이전트 유효성 검사

콘솔 에이전트 유지 관리 콘솔을 사용하여 콘솔 에이전트의 설치 및 구성을 검증할 수 있습니다.

에이전트 유지 관리 콘솔에 액세스하세요

콘솔 에이전트 호스트에서 유지 관리 콘솔에 액세스할 수 있습니다. 다음 디렉토리로 이동하세요:

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

설정 검사기 유효성 검사

그만큼 `config-checker validate` 이 명령어를 사용하면 콘솔 에이전트의 구성을 검증할 수 있습니다.

매개변수

`--services <comma-separated list of services to validate>`--필수의--

검증할 서비스를 하나 이상 선택하세요. 유효한 서비스 이름은 다음과 같습니다.*`PLATFORM` 필수 콘솔 엔드포인트에 대한 네트워크 연결 상태를 검증합니다.

`--validationTypes <comma-separated list validation types to run>`--필수-- 실행할 유효성 검사 유형을 하나 이상 선택하세요. 유효한 유효성 검사 유형은 다음과 같습니다. * `NETWORK` 필수 콘솔 엔드포인트에 대한 네트워크 연결 상태를 검증합니다.

`--proxy <url>`--선택 과목--

유효성 검사에 사용할 프록시 서버 URL을 지정합니다. 에이전트가 프록시 서버를 사용하도록 구성된 경우 필수입니다.

`--certs <paths>`--선택 과목--

유효성 검사에 사용할 하나 이상의 인증서 파일의 경로를 지정합니다. 인증서 파일은 PEM 형식이어야 합니다. 여러 경로를 쉼표로 구분하세요. 에이전트에서 사용자 지정 인증서를 사용하는 경우 이 매개변수가 필수입니다.

설정 검사기 유효성 검사 예제

기본 유효성 검사:

```
./agent-maint-console config-checker validate --services PLATFORM
--validationTypes NETWORK
```

에이전트에 프록시 서버가 사용되는 경우의 유효성 검사:

```
./agent-maint-console config-checker validate --services PLATFORM
--validationTypes NETWORK --proxy http://proxy.company.com:8080
```

에이전트에 인증서가 사용되는 유효성 검사:

```
./agent-maint-console config-checker validate --services PLATFORM
--validationTypes NETWORK --certs /path/to/cert1.pem,/path/to/cert2.pem
```

모든 명령에 대한 도움말 보기

모든 명령에 대한 도움말을 보려면 다음을 추가하세요. `--help` 명령에. 예를 들어, 도움말을 보려면 `proxy add` 명령을 사용하려면 다음 명령을 사용하세요.

```
./agent-maint-console proxy add --help
```

투명 프록시 명령

콘솔 에이전트 유지 관리 콘솔을 사용하여 콘솔 에이전트가 투명 프록시 서버를 사용하도록 구성할 수 있습니다.

에이전트 유지 관리 콘솔에 액세스하세요

콘솔 에이전트 호스트에서 유지 관리 콘솔에 액세스할 수 있습니다. 다음 디렉토리로 이동하세요:

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

모든 명령에 대한 도움말 보기

모든 명령에 대한 도움말을 보려면 다음을 추가하세요. `--help` 명령에. 예를 들어, 도움말을 보려면 `proxy add` 명령을 사용하려면 다음 명령을 사용하세요.

```
./agent-maint-console proxy add --help
```

프록시 가져오기

그만큼 `proxy get` 이 명령은 현재 투명 프록시 서버 구성에 대한 정보를 표시합니다. 현재 투명 프록시 서버 구성을 보려면 다음 명령을 사용하십시오.

프록시 가져오기 예시

현재 투명 프록시 서버 구성을 보려면 다음 명령을 사용하십시오.

```
./agent-maint-console proxy get
```

프록시 추가

그만큼 `proxy add` 이 명령은 에이전트가 투명 프록시 서버를 사용하도록 구성합니다.

매개변수

```
-c <certificate file>
```

프록시 서버의 인증서 파일 경로를 지정합니다. 인증서 파일은 PEM 형식이어야 합니다. 인증서 파일이 명령과 같은 디렉토리에 있는지 확인하거나 인증서 파일의 전체 경로를 지정하세요.

프록시 추가 예시

투명 프록시 서버를 추가하려면 다음 명령을 사용하십시오. `/home/ubuntu/myCA1.pem` 프록시 서버의 인증서 파일 경로입니다. 인증서 파일은 PEM 형식이어야 합니다.

```
./agent-maint-console proxy add -c /home/ubuntu/myCA1.pem
```

프록시 업데이트

그만큼 `proxy update` 이 명령어를 사용하면 투명 프록시의 인증서를 업데이트할 수 있습니다.

매개변수

`-c <certificate file>`프록시 서버의 인증서 파일 경로를 지정합니다. 인증서 파일은 PEM 형식이어야 합니다.

인증서 파일이 명령과 같은 디렉토리에 있는지 확인하거나 인증서 파일의 전체 경로를 지정하세요.

프록시 업데이트 예시

투명 프록시 서버의 인증서를 업데이트하려면 다음 명령을 사용하십시오. `/home/ubuntu/myCA1.pem` 프록시 서버의 새 인증서 파일 경로입니다. 인증서 파일은 PEM 형식이어야 합니다.

```
./agent-maint-console proxy update -c /home/ubuntu/myCA1.pem
```

프록시 제거

그만큼 `proxy remove` 이 명령은 에이전트에서 투명 프록시 서버 구성을 제거합니다.

프록시 제거 예시

투명 프록시 서버를 제거하려면 다음 명령을 사용하세요.

```
./agent-maint-console proxy remove
```

클라우드 공급자 에이전트 권한 및 네트워크 요구 사항

NetApp Console 에 대한 권한 요약

콘솔 에이전트가 클라우드 환경에서 작업을 수행할 수 있도록 적절한 권한을 부여해야 합니다. 이 페이지의 링크를 사용하여 목표에 따라 필요한 권한에 빠르게 접근하세요.

AWS 권한

NetApp Console 콘솔 에이전트와 개별 서비스에 대한 AWS 권한이 필요합니다.

콘솔 에이전트

목표	설명	링크
콘솔에서 콘솔 에이전트를 배포하려면 AWS에 콘솔 에이전트를 배포하기 위해 사용자에게 특정 권한이 필요합니다.	"AWS 권한 설정"	콘솔 에이전트에 대한 권한 제공

NetApp Backup and Recovery

목표	설명	링크
NetApp Backup and Recovery 사용하여 온프레미스 ONTAP 클러스터를 Amazon S3에 백업	ONTAP 볼륨에서 백업을 활성화할 때 NetApp Backup and Recovery 특정 권한이 있는 IAM 사용자의 액세스 키와 비밀번호를 입력하라는 메시지가 표시됩니다.	"백업을 위한 S3 권한 설정"

Cloud Volumes ONTAP

목표	설명	링크
Cloud Volumes ONTAP 노드에 대한 권한 제공	AWS의 각 Cloud Volumes ONTAP 노드에 IAM 역할을 연결해야 합니다. HA 중재자의 경우도 마찬가지입니다. 기본 옵션은 콘솔에서 IAM 역할을 자동으로 생성하도록 하는 것이지만, 콘솔에서 시스템을 생성할 때 사용자가 직접 IAM 역할을 생성할 수도 있습니다.	"IAM 역할을 직접 설정하는 방법을 알아보세요"

NetApp Copy and Sync

목표	설명	링크
AWS에 데이터 브로커 배포	데이터 브로커를 배포하는 데 사용하는 AWS 사용자 계정에는 필요한 권한이 있어야 합니다.	"AWS에 데이터 브로커를 배포하는 데 필요한 권한"
데이터 브로커에 대한 권한 제공	NetApp Copy and Sync 데이터 브로커를 배포하면 데이터 브로커 인스턴스에 대한 IAM 역할이 생성됩니다. 원하는 경우 사용자 고유의 IAM 역할을 사용하여 데이터 브로커를 배포할 수 있습니다.	"AWS 데이터 브로커에서 자체 IAM 역할을 사용하기 위한 요구 사항"
수동으로 설치된 데이터 브로커에 대한 AWS 액세스 활성화	S3 버킷을 포함하는 동기화 관계로 데이터 브로커를 사용하는 경우 AWS 액세스를 위해 Linux 호스트를 준비해야 합니다. 데이터 브로커를 설치할 때 프로그래밍 방식 액세스와 특정 권한이 있는 IAM 사용자에 대한 AWS 키를 제공해야 합니다.	"AWS에 대한 액세스 활성화"

ONTAP 용 FSx

목표	설명	링크
ONTAP 용 FSx 생성 및 관리	Amazon FSx for NetApp ONTAP 시스템을 생성하거나 관리하려면 콘솔에 AWS 자격 증명을 추가해야 합니다. 이를 위해 콘솔에 필요한 권한을 부여하는 IAM 역할의 ARN을 제공해야 합니다.	"FSx에 대한 AWS 자격 증명을 설정하는 방법을 알아보세요"

NetApp Cloud Tiering

목표	설명	링크
온프레미스 ONTAP 클러스터를 Amazon S3로 계층화	NetApp Cloud Tiering AWS에 활성화할 때 액세스 키와 비밀 키를 입력해야 합니다. 이러한 자격 증명은 ONTAP 클러스터로 전달되어 ONTAP 데이터를 S3 버킷으로 계층화할 수 있도록 합니다.	"계층화를 위한 S3 권한 설정"

Azure 권한

콘솔에는 콘솔 에이전트와 개별 서비스에 대한 Azure 권한이 필요합니다.

콘솔 에이전트

목표	설명	링크
콘솔에서 콘솔 에이전트 배포	콘솔에서 콘솔 에이전트를 배포하는 경우 Azure에서 콘솔 에이전트 VM을 배포할 수 있는 권한이 있는 Azure 계정이나 서비스 주체를 사용해야 합니다.	"Azure 권한 설정"
콘솔 에이전트에 대한 권한 제공	콘솔이 Azure에 콘솔 에이전트 VM을 배포하면 해당 Azure 구독 내에서 리소스와 프로세스를 관리하는 데 필요한 권한을 제공하는 사용자 지정 역할이 생성됩니다. 마켓플레이스에서 콘솔 에이전트를 시작하거나 콘솔 에이전트를 수동으로 설치하거나 사용자 지정 역할을 직접 설정해야 합니다."콘솔 에이전트에 Azure 자격 증명 추가" . 향후 릴리스에서 새로운 권한이 추가될 경우 정책을 최신 상태로 유지하십시오.	"콘솔 에이전트에 대한 Azure 권한"

NetApp Backup and Recovery

목표	설명	링크
Cloud Volumes ONTAP Azure Blob 스토리지에 백업	NetApp Backup and Recovery 사용하여 Cloud Volumes ONTAP 백업하는 경우 다음 시나리오에서 콘솔 에이전트에 권한을 추가해야 합니다. • "검색 및 복원" 기능을 사용하려고 합니다. • 고객 관리 암호화 키(CMEK)를 사용하려고 합니다.	• "백업 및 복구를 사용하여 Cloud Volumes ONTAP 데이터를 Azure Blob 스토리지에 백업합니다."
온프레미스 ONTAP 클러스터를 Azure Blob Storage에 백업	NetApp Backup and Recovery 사용하여 온프레미스 ONTAP 클러스터를 백업할 때 콘솔 에이전트가 "검색 및 복원" 기능을 사용할 수 있도록 권한을 추가해야 합니다.	"백업 및 복구를 사용하여 온-프레미스 ONTAP 데이터를 Azure Blob 저장소에 백업합니다."

NetApp 복사 및 동기화

목표	설명	링크
Azure에 데이터 브로커 배포	데이터 브로커를 배포하는 데 사용하는 Azure 사용자 계정에는 필요한 권한이 있어야 합니다.	"Azure에서 데이터 브로커를 배포하는 데 필요한 권한"

Google Cloud 권한

콘솔에는 콘솔 에이전트와 개별 서비스에 대한 Google Cloud 권한이 필요합니다.

콘솔 에이전트

목표	설명	링크
콘솔에서 콘솔 에이전트 배포	Google Cloud 콘솔에서 콘솔 에이전트를 배포하는 Google Cloud 사용자는 Google Cloud에서 콘솔 에이전트를 배포하기 위한 특정 권한이 필요합니다.	"콘솔 에이전트를 생성하기 위한 권한 설정"
콘솔 에이전트에 대한 권한 제공	콘솔 에이전트의 서비스 계정은 일상적인 운영을 위해 특정 권한을 보유해야 합니다. 배포 중에 서비스 계정을 콘솔 에이전트와 연결해야 합니다. 향후 릴리스에서 새로운 권한이 추가될 경우 정책을 최신 상태로 유지하십시오.	"콘솔 에이전트에 대한 권한 설정"

NetApp Backup and Recovery

목표	설명	링크
Google Cloud에 Cloud Volumes ONTAP 백업	NetApp Backup and Recovery 사용하여 Cloud Volumes ONTAP 백업하는 경우 다음 시나리오에서 콘솔 에이전트에 권한을 추가해야 합니다. • "검색 및 복원" 기능을 사용하려고 합니다. • 고객 관리 암호화 키(CMEK)를 사용하려고 합니다.	• "백업 및 복구를 사용하여 Cloud Volumes ONTAP 데이터를 Google Cloud Storage에 백업합니다." • "CMEK에 대한 권한"
온프레미스 ONTAP 클러스터를 Google Cloud에 백업	NetApp Backup and Recovery 사용하여 온프레미스 ONTAP 클러스터를 백업할 때 콘솔 에이전트가 "검색 및 복원" 기능을 사용할 수 있도록 권한을 추가해야 합니다.	"백업 및 복구를 사용하여 온프레미스 ONTAP 데이터를 Google Cloud Storage에 백업하세요."

NetApp Copy and Sync

목표	설명	링크
Google Cloud에 데이터 브로커 배포	데이터 브로커를 배포하는 Google Cloud 사용자에게 필요한 권한이 있는지 확인하세요.	"Google Cloud에 데이터 브로커를 배포하는 데 필요한 권한"
수동으로 설치된 데이터 브로커에 대한 Google Cloud 액세스 활성화	Google Cloud Storage 버킷을 포함하는 동기화 관계로 데이터 브로커를 사용하려는 경우 Google Cloud 액세스를 위해 Linux 호스트를 준비해야 합니다. 데이터 브로커를 설치할 때 특정 권한이 있는 서비스 계정에 대한 키를 제공해야 합니다.	"Google Cloud에 대한 액세스 활성화"

StorageGRID 권한

콘솔에는 두 가지 서비스에 대한 StorageGRID 권한이 필요합니다.

NetApp Backup and Recovery

목표	설명	링크
온프레미스 ONTAP 클러스터를 StorageGRID 에 백업	ONTAP 클러스터의 백업 대상으로 StorageGRID 준비하면 NetApp Backup and Recovery 특정 권한이 있는 IAM 사용자의 액세스 키와 비밀번호를 입력하라는 메시지가 표시됩니다.	"StorageGRID 백업 대상으로 준비하세요"

NetApp Cloud Tiering

목표	설명	링크
온프레미스 ONTAP 클러스터를 StorageGRID 로 계층화	StorageGRID 에 NetApp Cloud Tiering 설정하는 경우 Cloud Tiering에 S3 액세스 키와 비밀 키를 제공해야 합니다. 클라우드 티어링은 키를 사용하여 버킷에 액세스합니다.	"StorageGRID 에 대한 계층화 준비"

AWS 에이전트 권한 및 보안 규칙

콘솔 에이전트에 대한 **AWS** 권한

NetApp Console AWS에서 콘솔 에이전트를 시작하면 에이전트에 해당 AWS 계정 내의 리소스와 프로세스를 관리할 수 있는 권한을 제공하는 정책이 에이전트에 연결됩니다. 에이전트는 EC2, S3, CloudFormation, IAM, 키 관리 서비스(KMS) 등 여러 AWS 서비스에 대한 API 호출을 수행하기 위한 권한을 사용합니다.

IAM 정책

아래에서 제공되는 IAM 정책은 콘솔 에이전트가 AWS 지역에 따라 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하는 데 필요한 권한을 제공합니다.

다음 사항에 유의하세요.

- 콘솔에서 직접 표준 AWS 지역에 콘솔 에이전트를 생성하면 콘솔이 자동으로 에이전트에 정책을 적용합니다.
- AWS Marketplace에서 에이전트를 배포하는 경우, Linux 호스트에 에이전트를 수동으로 설치하는 경우 또는 콘솔에 추가 AWS 자격 증명을 추가하려는 경우에는 정책을 직접 설정해야 합니다.
- 어느 경우든 후속 릴리스에서 새로운 권한이 추가되므로 정책이 최신 상태인지 확인해야 합니다. 새로운 권한이 필요한 경우 릴리스 노트에 나열됩니다.
- 필요한 경우 IAM을 사용하여 IAM 정책을 제한할 수 있습니다. `Condition` 요소. "AWS 설명서: 조건 요소"
- 이러한 정책을 사용하기 위한 단계별 지침을 보려면 다음 페이지를 참조하세요.
  - "AWS Marketplace 배포에 대한 권한 설정"
  - "온프레미스 배포에 대한 권한 설정"
  - "제한 모드에 대한 권한 설정"

필요한 정책을 보려면 해당 지역을 선택하세요.

표준 지역

표준 지역의 경우 권한은 두 가지 정책에 걸쳐 분산됩니다. AWS의 관리형 정책에는 최대 문자 크기 제한이 있으므로 두 개의 정책이 필요합니다.

정책 **#1**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:CreatePlacementGroup",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateRoute",
        "ec2:DescribeVpcs",
```

```
        "ec2:ReplaceRoute",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:DeleteRoute",
        "ec2:DeletePlacementGroup",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:ModifyVolume",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "cloudformation:DeleteStack",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:ListInstanceProfiles",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DeleteInstanceProfile",
        "iam:GetRolePolicy",
        "iam:GetRole",
        "sts:DecodeAuthorizationMessage",
        "sts:AssumeRole",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutObject",
        "s3:ListAllMyBuckets",
```

```
            "s3:GetObject",
            "s3:GetEncryptionConfiguration",
            "kms:ReEncrypt*",
            "kms:CreateGrant",
            "fsx:Describe*",
            "fsx:List*",
            "kms:GenerateDataKeyWithoutPlaintext"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "cvoServicePolicy"
    },
    {
        "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceStatus",
            "ec2:RunInstances",
            "ec2:TerminateInstances",
            "ec2:DescribeInstanceAttribute",
            "ec2:DescribeImages",
            "ec2:CreateTags",
            "ec2:CreateVolume",
            "ec2:CreateSecurityGroup",
            "ec2:DescribeSubnets",
            "ec2:DescribeVpcs",
            "ec2:DescribeRegions",
            "cloudformation:CreateStack",
            "cloudformation:DeleteStack",
            "cloudformation:DescribeStacks",
            "ec2:DescribeVpcEndpoints",
            "kms:ListAliases",
            "glue:GetDatabase",
            "glue:GetTable",
            "glue:GetPartitions"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "backupPolicy"
    },
    {
        "Action": [
            "s3:GetBucketLocation",
            "s3:ListAllMyBuckets",
            "s3:ListBucket",
```

```
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetObject",
        "s3:PutEncryptionConfiguration",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:DeleteBucket",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectRetention",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketVersioning",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketVersioning",
        "s3:BypassGovernanceRetention",
        "s3:PutBucketPolicy",
        "s3:PutBucketOwnershipControls"
      ],
      "Resource": [
        "arn:aws:s3:::netapp-backup-*"
      ],
      "Effect": "Allow",
      "Sid": "backupS3Policy"
    },
    {
      "Action": [
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
```

```
            "s3:ListBucketVersions",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketAcl",
            "s3:GetBucketPolicy",
            "s3:PutBucketPublicAccessBlock",
            "s3:DeleteBucket"
        ],
        "Resource": [
            "arn:aws:s3:::fabric-pool*"
        ],
        "Effect": "Allow",
        "Sid": "fabricPoolS3Policy"
    },
    {
        "Action": [
            "ec2:DescribeRegions"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "fabricPoolPolicy"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/netapp-adc-manager": "*"
            }
        },
        "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Effect": "Allow"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Action": [
            "ec2:StartInstances",
```

```
            "ec2:TerminateInstances",
            "ec2:AttachVolume",
            "ec2:DetachVolume",
            "ec2:StopInstances",
            "ec2:DeleteVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:volume/*"
        ],
        "Effect": "Allow"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Action": [
            "ec2:DeleteVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:volume/*"
        ],
        "Effect": "Allow"
    }
  ]
}
```

정책 **#2**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "tagServicePolicy"
    }
  ]
}
```

GovCloud(미국) 지역

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListInstanceProfiles",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "ec2:ModifyVolumeAttribute",
        "sts:DecodeAuthorizationMessage",
        "ec2:DescribeImages",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstances",
        "iam:PassRole",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:DeleteVolume",
        "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:CreateSnapshot",
```

```
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:StopInstances",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:CreateBucket",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
```

```
            "s3:GetBucketPolicy",
            "s3:PutBucketPublicAccessBlock"
        ],
        "Resource": [
            "arn:aws-us-gov:s3:::fabric-pool*"
        ]
    },
    {
        "Sid": "backupPolicy",
        "Effect": "Allow",
        "Action": [
            "s3:DeleteBucket",
            "s3:GetLifecycleConfiguration",
            "s3:PutLifecycleConfiguration",
            "s3:PutBucketTagging",
            "s3:ListBucketVersions",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:ListAllMyBuckets",
            "s3:GetBucketTagging",
            "s3:GetBucketLocation",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketAcl",
            "s3:GetBucketPolicy",
            "s3:PutBucketPublicAccessBlock"
        ],
        "Resource": [
            "arn:aws-us-gov:s3:::netapp-backup-*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:StartInstances",
            "ec2:TerminateInstances",
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Resource": [
            "arn:aws-us-gov:ec2:*:*:instance/*"
```

```
        ]
      },
      {
        "Effect": "Allow",
        "Action": [
          "ec2:AttachVolume",
          "ec2:DetachVolume"
        ],
        "Resource": [
          "arn:aws-us-gov:ec2:*:*:volume/*"
        ]
      }
    ]
}
```

비밀 지역

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
```

```
        "cloudformation:ValidateTemplate",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListinstanceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
      ],
      "Resource": [
        "arn:aws-iso-b:s3:::fabric-pool*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
```

```
            "ec2:DetachVolume"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Resource": [
            "arn:aws-iso-b:ec2:*:*:instance/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-iso-b:ec2:*:*:volume/*"
        ]
    }
  ]
}
```

극비 지역

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
```

```
        "cloudformation:ValidateTemplate",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListinstanceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
      ],
      "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
```

```
            "ec2:DetachVolume"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Resource": [
            "arn:aws-iso:ec2:*:*:instance/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-iso:ec2:*:*:volume/*"
        ]
    }
  ]
}
```

AWS 권한은 어떻게 사용되나요**?**

다음 섹션에서는 각 NetApp Console 관리 또는 데이터 서비스에 대한 권한이 어떻게 사용되는지 설명합니다. 회사 정책에 따라 필요한 경우에만 권한이 부여되는 경우 이 정보가 유용할 수 있습니다.

ONTAP 용 Amazon FSx

콘솔 에이전트는 Amazon FSx for ONTAP 파일 시스템을 관리하기 위해 다음과 같은 API 요청을 합니다.

- ec2:인스턴스 설명
- ec2:인스턴스 상태 설명
- ec2:인스턴스 속성 설명
- ec2:라우트테이블 설명
- ec2:이미지 설명
- ec2:태그 생성
- ec2:볼륨 설명
- ec2:보안 그룹 설명
- ec2:네트워크 인터페이스 설명
- ec2:서브넷 설명

- ec2:Vpcs 설명
- ec2:Dhcp옵션 설명
- ec2:스냅샷 설명
- ec2:키 쌍 설명
- ec2:지역 설명
- ec2:태그 설명
- ec2:DescribeIamInstanceProfileAssociations
- ec2:예약된 인스턴스 설명 제공
- ec2:Vpc엔드포인트 설명
- ec2:Vpcs 설명
- ec2:볼륨 수정 설명
- ec2:배치 그룹 설명
- kms:CreateGrant
- kms:별칭 목록
- fsx:설명*
- fsx:리스트*

Amazon S3 버킷 검색

콘솔 에이전트는 Amazon S3 버킷을 검색하기 위해 다음 API 요청을 합니다.

s3:암호화 구성 가져오기

NetApp Backup and Recovery

에이전트는 Amazon S3에서 백업을 관리하기 위해 다음과 같은 API 요청을 합니다.

- s3:버킷 위치 가져오기
- s3:내 버킷 모두 나열
- s3:리스트버킷
- s3:버킷 만들기
- s3:수명주기구성 가져오기
- s3:PutLifecycleConfiguration
- s3:PutBucket태깅
- s3:리스트버킷버전
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- s3:객체 가져오기
- ec2:Vpc엔드포인트 설명

- kms:별칭 목록
- s3:PutEncryptionConfiguration

볼륨과 파일을 복원하기 위해 검색 및 복원 방법을 사용할 때 에이전트는 다음과 같은 API 요청을 합니다.

- s3:버킷 만들기
- s3:객체 삭제
- s3:객체 버전 삭제
- s3:GetBucketAcl
- s3:리스트버킷
- s3:리스트버킷버전
- s3:ListBucketMultipartUploads
- s3:객체 넣기
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:멀티파트업로드 중단
- s3:ListMultipartUploadParts

볼륨 백업에 DataLock 및 NetApp Ransomware Resilience 사용하는 경우 에이전트는 다음과 같은 API 요청을 합니다.

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:객체 삭제
- s3:객체태깅 삭제
- s3:객체 보존 가져오기
- s3:DeleteObjectVersionTagging
- s3:객체 넣기
- s3:객체 가져오기
- s3:PutBucketObjectLock구성
- s3:수명주기구성 가져오기
- s3:ListBucketByTags
- s3:버킷태깅 가져오기
- s3:객체 버전 삭제
- s3:리스트버킷버전

- s3:리스트버킷
- s3:PutBucket태깅
- s3:객체태깅 가져오기
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:버킷 버전 가져오기
- s3:GetBucketAcl
- s3:바이패스거버넌스보존
- s3:객체 보존 넣기
- s3:버킷 위치 가져오기
- s3:객체 버전 가져오기

소스 볼륨에 사용하는 AWS 계정과 다른 AWS 계정을 Cloud Volumes ONTAP 백업에 사용하는 경우 에이전트는 다음과 같은 API 요청을 합니다.

- s3:PutBucketPolicy
- s3:PutBucketOwnershipControls

백업 및 복구에 대한 레거시 권한

인덱싱 v2가 출시되기 전에 레거시 인덱싱 기능을 활성화한 경우에만 다음 권한이 필요합니다.

- kms:목록*
- kms:설명*
- 아테나:StartQueryExecution
- 아테나:GetQueryResults
- 아테나:GetQueryExecution
- 아테나:쿼리 실행 중지
- glue:CreateDatabase
- 접착제:CreateTable
- 접착제:일괄 삭제 파티션

분류

에이전트는 NetApp Data Classification 배포하기 위해 다음 API 요청을 합니다.

- ec2:인스턴스 설명
- ec2:인스턴스 상태 설명
- ec2:실행 인스턴스
- ec2:인스턴스 종료
- ec2:태그 생성

- ec2:볼륨 생성
- ec2:볼륨 첨부
- ec2:보안 그룹 생성
- ec2:보안 그룹 삭제
- ec2:보안 그룹 설명
- ec2:네트워크 인터페이스 생성
- ec2:네트워크 인터페이스 설명
- ec2:네트워크 인터페이스 삭제
- ec2:서브넷 설명
- ec2:Vpcs 설명
- ec2:스냅샷 생성
- ec2:지역 설명
- 클라우드포메이션:CreateStack
- 클라우드포메이션:DeleteStack
- 클라우드포메이션:DescribeStacks
- 클라우드포메이션:스택이벤트 설명
- iam:인스턴스 프로필에 역할 추가
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

NetApp Data Classification 사용할 때 에이전트는 S3 버킷을 스캔하기 위해 다음 API 요청을 만듭니다.

- iam:인스턴스 프로필에 역할 추가
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations
- s3:버킷태깅 가져오기
- s3:버킷 위치 가져오기
- s3:내 버킷 모두 나열
- s3:리스트버킷
- s3:버킷정책 상태 가져오기
- s3:버킷 정책 가져오기
- s3:GetBucketAcl
- s3:객체 가져오기
- iam:역할 가져오기
- s3:객체 삭제
- s3:객체 버전 삭제

- s3:객체 넣기
- sts:역할 가정

Cloud Volumes ONTAP

에이전트는 AWS에서 Cloud Volumes ONTAP 배포하고 관리하기 위해 다음과 같은 API 요청을 합니다.

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
Cloud Volumes ONTAP 인스턴스에 대한 IAM 역할 및 인스턴스 프로필을 생성하고 관리합니다.	iam:ListInstanceProfiles	예	예	아니요
	iam:역할 생성	예	아니요	아니요
	iam:역할 삭제	아니요	예	예
	iam:역할 정책 넣기	예	아니요	아니요
	iam:인스턴스 프로필 생성	예	아니요	아니요
	iam:역할 정책 삭제	아니요	예	예
	iam:인스턴스 프로필에 역할 추가	예	아니요	아니요
	iam:인스턴스 프로필에서 역할 제거	아니요	예	예
	iam:인스턴스 프로필 삭제	아니요	예	예
	iam:PassRole	예	아니요	아니요
	ec2:AssociateIamInstanceProfile	예	예	아니요
	ec2:DescribeIamInstanceProfileAssociations	예	예	아니요
	ec2:IamInstanceProfile 연결 해제	아니요	예	아니요
권한 상태 메시지 디코딩	sts:디코드인증메시지	예	예	아니요
계정에서 사용 가능한 지정된 이미지(AMI)를 설명합니다.	ec2:이미지 설명	예	예	아니요
VPC의 경로 테이블 설명(HA 쌍에만 필요)	ec2:라우트테이블 설명	예	아니요	아니요

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
인스턴스 중지, 시작 및 모니터링	ec2:시작인스턴스	예	예	아니요
	ec2:인스턴스 중지	예	예	아니요
	ec2:인스턴스 설명	예	예	아니요
	ec2:인스턴스 상태 설명	예	예	아니요
	ec2:실행 인스턴스	예	아니요	아니요
	ec2:인스턴스 종료	아니요	아니요	예
	ec2:ModifyInstanceAttribute	아니요	예	아니요
지원되는 인스턴스 유형에 대해 향상된 네트워킹이 활성화되어 있는지 확인하세요.	ec2:인스턴스 속성 설명	아니요	예	아니요
유지 관리 및 비용 할당에 사용되는 "WorkingEnvironment" 및 "WorkingEnvironmentId" 태그를 사용하여 리소스에 태그를 지정합니다.	ec2:태그 생성	예	예	아니요
Cloud Volumes ONTAP 이 백엔드 스토리지로 사용하는 EBS 볼륨을 관리합니다.	ec2:볼륨 생성	예	예	아니요
	ec2:볼륨 설명	예	예	예
	ec2:볼륨 속성 수정	아니요	예	예
	ec2:볼륨 첨부	예	예	아니요
	ec2:볼륨 삭제	아니요	예	예
	ec2:볼륨 분리	아니요	예	예
Cloud Volumes ONTAP 에 대한 보안 그룹을 만들고 관리합니다.	ec2:보안 그룹 생성	예	아니요	아니요
	ec2:보안 그룹 삭제	아니요	예	예
	ec2:보안 그룹 설명	예	예	예
	ec2:보안그룹퇴장취소	예	아니요	아니요
	ec2:보안그룹 송신 권한 부여	예	아니요	아니요
	ec2:보안그룹인증	예	아니요	아니요
	ec2:보안그룹 수신 거부	예	예	아니요

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
대상 서브넷에서 Cloud Volumes ONTAP 에 대한 네트워크 인터페이스를 생성하고 관리합니다.	ec2:네트워크 인터페이스 생성	예	아니요	아니요
	ec2:네트워크 인터페이스 설명	예	예	아니요
	ec2:네트워크 인터페이스 삭제	아니요	예	예
	ec2:ModifyNetworkInterfaceAttribute	아니요	예	아니요
대상 서브넷 및 보안 그룹 목록 가져오기	ec2:서브넷 설명	예	예	아니요
	ec2:Vpcs 설명	예	예	아니요
Cloud Volumes ONTAP 인스턴스에 대한 DNS 서버 및 기본 도메인 이름 가져오기	ec2:Dhcp옵션 설명	예	아니요	아니요
Cloud Volumes ONTAP 위한 EBS 볼륨의 스냅샷을 찍습니다.	ec2:스냅샷 생성	예	예	아니요
	ec2:스냅샷 삭제	아니요	예	예
	ec2:스냅샷 설명	아니요	예	아니요
AutoSupport 메시지에 연결된 Cloud Volumes ONTAP 콘솔을 캡처합니다.	ec2:GetConsoleOutput	예	예	아니요
사용 가능한 키 쌍 목록 가져오기	ec2:키 쌍 설명	예	아니요	아니요
사용 가능한 AWS 지역 목록을 가져옵니다.	ec2:지역 설명	예	예	아니요
Cloud Volumes ONTAP 인스턴스와 연결된 리소스에 대한 태그 관리	ec2:태그 삭제	아니요	예	예
	ec2:태그 설명	아니요	예	아니요

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
AWS CloudFormation 템플릿에 대한 스택 생성 및 관리	클라우드포메이션:CreateStack	예	아니요	아니요
	클라우드포메이션:DeleteStack	예	아니요	아니요
	클라우드포메이션:DescribeStacks	예	예	아니요
	클라우드포메이션:스택이벤트 설명	예	아니요	아니요
	cloudformation:ValidateTemplate	예	아니요	아니요
Cloud Volumes ONTAP 시스템이 데이터 계층화를 위한 용량 계층으로 사용하는 S3 버킷을 생성하고 관리합니다.	s3:버킷 만들기	예	예	아니요
	s3:버킷 삭제	아니요	예	예
	s3:수명주기구성 가져오기	아니요	예	아니요
	s3:PutLifecycleConfiguration	아니요	예	아니요
	s3:PutBucket태깅	아니요	예	아니요
	s3:리스트버킷버전	아니요	예	아니요
	s3:버킷정책 상태 가져오기	아니요	예	아니요
	s3:GetBucketPublicAccessBlock	아니요	예	아니요
	s3:GetBucketAcl	아니요	예	아니요
	s3:버킷 정책 가져오기	아니요	예	아니요
	s3:PutBucketPublicAccessBlock	아니요	예	아니요
	s3:버킷태깅 가져오기	아니요	예	아니요
	s3:버킷 위치 가져오기	아니요	예	아니요
	s3:내 버킷 모두 나열	아니요	아니요	아니요
	s3:리스트버킷	아니요	예	아니요
AWS Key Management Service(KMS)를 사용하여 Cloud Volumes ONTAP 의 데이터 암호화를 활성화합니다.	kms:재암호화*	예	아니요	아니요
	kms:CreateGrant	예	예	아니요
	kms:GenerateDataKeyWithoutPlaintext	예	예	아니요

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
단일 AWS 가용성 영역에서 두 개의 HA 노드와 중재자에 대한 AWS 스프레드 배치 그룹을 생성하고 관리합니다.	ec2:배치 그룹 생성	예	아니요	아니요
	ec2:배치 그룹 삭제	아니요	예	예
보고서 만들기	fsx:설명*	아니요	예	아니요
	fsx:리스트*	아니요	예	아니요
Amazon EBS Elastic Volumes 기능을 지원하는 집계를 생성하고 관리합니다.	ec2:볼륨 수정 설명	아니요	예	아니요
	ec2:볼륨 수정	아니요	예	아니요
가용성 영역이 AWS 로컬 영역인지 확인하고 모든 배포 매개변수가 호환되는지 확인합니다.	ec2:가용성 구역 설명	예	아니요	예

변경 로그

권한이 추가되거나 제거되면 아래 섹션에 기록됩니다.

2025년 **11**월 **11**일

레거시 인덱싱을 사용하지 않는 한 NetApp Backup and Recovery 에는 다음 권한이 더 이상 필요하지 않습니다. 이 페이지의 정책에서 다음 권한이 제거되었습니다.

- kms:목록*
- kms:설명*
- 아테나:StartQueryExecution
- 아테나:GetQueryResults
- 아테나:GetQueryExecution
- 아테나:쿼리 실행 중지
- glue:CreateDatabase
- 접착제:CreateTable
- 접착제:일괄 삭제 파티션

2024년 **9**월 **9**일

NetApp Console 더 이상 NetApp 에지 캐싱 및 Kubernetes 클러스터의 검색과 관리를 지원하지 않기 때문에 표준 지역에 대한 정책 #2에서 권한이 제거되었습니다.

정책에서 제거된 권한 보기

```
{
    "Action": [
        "ec2:DescribeRegions",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "iam:GetInstanceProfile"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "K8sServicePolicy"
},
{
    "Action": [
        "cloudformation:DescribeStacks",
        "cloudwatch:GetMetricStatistics",
        "cloudformation:ListStacks"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "GFCservicePolicy"
},
{
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/GFCInstance": "*"
        }
    },
    "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Effect": "Allow"
}
```

2024년 5월 9일

이제 Cloud Volumes ONTAP 에 다음 권한이 필요합니다.

ec2:가용성 구역 설명

2023년 **6**월 **6**일

이제 Cloud Volumes ONTAP 에 다음 권한이 필요합니다.

kms:GenerateDataKeyWithoutPlaintext

2023년 **2**월 **14**일

NetApp Cloud Tiering 에는 이제 다음 권한이 필요합니다.

ec2:Vpc엔드포인트 설명

AWS의 콘솔 에이전트 보안 그룹 규칙

에이전트의 AWS 보안 그룹에는 인바운드 규칙과 아웃바운드 규칙이 모두 필요합니다. NetApp 콘솔에서 콘솔 에이전트를 생성하면 NetApp Console 자동으로 이 보안 그룹을 생성합니다. 다른 모든 설치 옵션의 경우 이 보안 그룹을 설정해야 합니다.

인바운드 규칙

규약	포트	목적
SSH	22	에이전트 호스트에 SSH 액세스를 제공합니다.
HTTP	80	• 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다. • Cloud Volumes ONTAP 업그레이드 프로세스 중에 사용됨
HTTPS	443	로컬 사용자 인터페이스에 대한 HTTPS 액세스와 NetApp Data Classification 인스턴스의 연결을 제공합니다.
TCP	3128	Cloud Volumes ONTAP 에 인터넷 접속을 제공합니다. 배포 후에는 수동으로 이 포트를 열어야 합니다.

아웃바운드 규칙

에이전트에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 개방합니다. 이것이 허용된다면, 기본적인 아웃바운드 규칙을 따르세요. 더욱 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

에이전트에 대한 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

규약	포트	목적
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 에이전트의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

소스 IP 주소는 에이전트 호스트입니다.

서비스	규약	포트	목적지	목적
API 호출 및 AutoSupport	HTTPS	443	아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF	AWS, ONTAP, NetApp Data Classification 대한 API 호출 및 NetApp 에 대한 AutoSupport 메시지 전송
API 호출	TCP	3000	ONTAP HA 중재자	ONTAP HA 중재자와의 커뮤니케이션
	TCP	8080	데이터 분류	배포 중 데이터 분류 인스턴스에 대한 프로브
DNS	UDP	53	DNS	콘솔에서 DNS를 확인하는 데 사용됩니다.

Azure 권한 및 필수 보안 규칙

콘솔 에이전트에 대한 **Azure** 권한

NetApp Console Azure에서 콘솔 에이전트를 시작하면 VM에 사용자 지정 역할을 연결하여 에이전트에 해당 Azure 구독 내의 리소스와 프로세스를 관리할 수 있는 권한을 부여합니다. 에이전트는 이러한 권한을 사용하여 여러 Azure 서비스에 대한 API 호출을 수행합니다.

에이전트에 대해 이 사용자 지정 역할을 만들어야 하는지 여부는 해당 역할을 배포한 방법에 따라 달라집니다.

NetApp Console 에서 배포

콘솔을 사용하여 Azure에 에이전트 가상 머신을 배포하면 다음을 수행할 수 있습니다. "시스템 할당 관리 ID" 가상 머신에서 사용자 지정 역할을 만들고 이를 가상 머신에 할당합니다. 이 역할은 Azure 구독 내에서 리소스와 프로세스를 관리하는 데 필요한 권한을 콘솔에 제공합니다. 에이전트가 업그레이드되면 역할의 권한도 최신 상태로 유지됩니다. 에이전트에 대한 이 역할을 만들거나 업데이트를 관리할 필요는 없습니다.

수동으로 또는 **Azure Marketplace**에서 배포

Azure Marketplace에서 에이전트를 배포하거나 Linux 호스트에 에이전트를 수동으로 설치하는 경우 사용자 지정 역할을 직접 설정하고 변경 사항에 따라 해당 역할을 유지 관리해야 합니다.

이후 릴리스에서 새로운 권한이 추가되므로 역할이 최신 상태인지 확인해야 합니다. 새로운 권한이 필요한 경우 릴리스 노트에 나열됩니다.

- 이러한 정책을 사용하기 위한 단계별 지침을 보려면 다음 페이지를 참조하세요.

- "Azure Marketplace 배포에 대한 권한 설정"
- "온프레미스 배포에 대한 권한 설정"
- "제한 모드에 대한 권한 설정"

```
{
  "Name": "Console Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/deallocate/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/images/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/write",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/write",
    "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.Storage/checknameavailability/read",
    "Microsoft.Storage/operations/read",
    "Microsoft.Storage/storageAccounts/listkeys/action",
    "Microsoft.Storage/storageAccounts/read",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Storage/storageAccounts/blobServices/containers/read",
    "Microsoft.Storage/storageAccounts/listAccountSas/action",
    "Microsoft.Storage/usages/read",
    "Microsoft.Compute/snapshots/write",
    "Microsoft.Compute/snapshots/read",
    "Microsoft.Compute/availabilitySets/write",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
    "Microsoft.Network/loadBalancers/read",
    "Microsoft.Network/loadBalancers/write",
    "Microsoft.Network/loadBalancers/delete",
    "Microsoft.Network/loadBalancers/backendAddressPools/read",
    "Microsoft.Network/loadBalancers/backendAddressPools/join/action",
    "Microsoft.Network/loadBalancers/loadBalancingRules/read",
    "Microsoft.Network/loadBalancers/probes/read",
    "Microsoft.Network/loadBalancers/probes/join/action",
    "Microsoft.Authorization/locks/*",
    "Microsoft.Network/routeTables/join/action",
    "Microsoft.NetApp/netAppAccounts/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",
    "Microsoft.Storage/storageAccounts/privateEndpointConnections/read",
    "Microsoft.Storage/storageAccounts/managementPolicies/read",
    "Microsoft.Storage/storageAccounts/managementPolicies/write",
    "Microsoft.Network/privateEndpoints/read",
    "Microsoft.Network/privateDnsZones/write",
```

```
    "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
    "Microsoft.Network/virtualNetworks/join/action",
    "Microsoft.Network/privateDnsZones/A/write",
    "Microsoft.Network/privateDnsZones/read",
    "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Insights/Metrics/Read",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/delete",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Compute/diskEncryptionSets/read",
    "Microsoft.Compute/snapshots/delete",
    "Microsoft.Network/privateEndpoints/delete",
    "Microsoft.Compute/availabilitySets/delete",
    "Microsoft.KeyVault/vaults/read",
    "Microsoft.KeyVault/vaults/accessPolicies/write",
    "Microsoft.Compute/diskEncryptionSets/write",
    "Microsoft.KeyVault/vaults/deploy/action",
    "Microsoft.Compute/diskEncryptionSets/delete",
    "Microsoft.Resources/tags/read",
    "Microsoft.Resources/tags/write",
    "Microsoft.Resources/tags/delete",
    "Microsoft.Network/applicationSecurityGroups/write",
    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/applicationSecurityGroups/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Synapse/workspaces/write",
    "Microsoft.Synapse/workspaces/read",
    "Microsoft.Synapse/workspaces/delete",
    "Microsoft.Synapse/register/action",
    "Microsoft.Synapse/checkNameAvailability/action",
    "Microsoft.Synapse/workspaces/operationStatuses/read",
    "Microsoft.Synapse/workspaces/firewallRules/read",
    "Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",
    "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
    "Microsoft.Compute/images/write",
```

```
    "Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
    "Microsoft.Compute/virtualMachineScaleSets/write",
    "Microsoft.Compute/virtualMachineScaleSets/read",
    "Microsoft.Compute/virtualMachineScaleSets/delete"
  ],
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Console Permissions",
  "IsCustom": "true"
}
```

Azure 권한이 사용되는 방식

다음 섹션에서는 각 NetApp 스토리지 시스템과 데이터 서비스에 대한 권한이 어떻게 사용되는지 설명합니다. 회사 정책에 따라 필요한 경우에만 권한이 부여되는 경우 이 정보가 유용할 수 있습니다.

Azure NetApp Files

NetApp Data Classification 사용하여 Azure NetApp Files 데이터를 스캔할 때 에이전트는 다음과 같은 API 요청을 합니다.

- NetApp/netAppAccounts/read
- Microsoft. NetApp/netAppAccounts/capacityPools/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/delete

NetApp Backup and Recovery

다음 섹션에서는 NetApp Backup and Recovery 에서 권한이 사용되는 방식을 설명합니다.

최소 **NetApp Backup and Recovery** 권한

콘솔 에이전트는 기본 NetApp Backup and Recovery 기능에 대해 다음과 같은 API 요청을 합니다.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/구독/리소스그룹/리소스/읽기
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Storage/storageAccounts/managementPolicies/read

- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

다음은 가능한 가장 적은 권한과 가장 좁은 범위를 사용하는 백업 및 복구용 사용자 지정 정책입니다.

```
{
  "id":
"/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/roleDef
initions/{roleDefinitionGuid}",
  "properties": {
    "roleName": "Custom Role",
    "description": "Minimal permissions required for Backup and
Recovery.",
    "assignableScopes": [
      "/subscriptions/{subscriptionId}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}/providers/Microsoft.Storage/storageAccounts/
{storageAccountNameWithObjectLockPreprovisioned}"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/storageAccounts/listkeys/action",
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
          "Microsoft.Storage/storageAccounts/listAccountSas/action",
          "Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
          "Microsoft.Resources/subscriptions/resourceGroups/write",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/write",
          "Microsoft.Authorization/locks/write",
          "Microsoft.Authorization/locks/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

고급 백업 및 복구 권한

콘솔 에이전트는 고급 백업 및 복구 작업과 검색 및 복원 기능을 위해 다음 API 요청을 합니다. 이러한 권한을 통해 네트워킹, 키 보관소 및 관리 ID를 관리할 수 있습니다.

- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.KeyVault/vaults/read
- Microsoft.ManagedIdentity/userAssignedIdentities/할당/작업
- Microsoft.Network/networkInterfaces/삭제
- Microsoft.Network/networkInterfaces/read
- Microsoft.Network/networkSecurityGroups/삭제
- Microsoft.Network/privateDnsZones/읽기
- Microsoft.Network/privateDnsZones/write
- Microsoft.Network/privateEndpoints/읽기
- Microsoft.Network/privateEndpoints/쓰기
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Resources/deployments/delete

백업 및 복구에 대한 레거시 권한

검색 및 복원 기능을 사용하면 에이전트는 다음과 같은 API 요청을 합니다. 2025년 2월 인덱싱 v2 출시 이전에 레거시 인덱싱 기능을 활성화한 경우에만 이러한 권한이 필요합니다.

- Microsoft.Synapse/workspaces/write
- Microsoft.Synapse/workspaces/read
- Microsoft.Synapse/workspaces/삭제
- Microsoft.Synapse/등록/작업
- Microsoft.Synapse/checkNameAvailability/action
- Microsoft.Synapse/workspaces/operationStatuses/read
- Microsoft.Synapse/workspaces/firewallRules/read
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft.Synapse/workspaces/operationResults/read
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

NetApp Data Classification

데이터 분류를 사용하면 에이전트는 다음과 같은 API 요청을 합니다.

행동	설정에 사용**?**	일상 업무에 사용되나요**?**
Microsoft.Compute/위치/작업/읽기	예	예
Microsoft.Compute/위치/vmSizes/읽기	예	예

행동	설정에 사용?	일상 업무에 사용되나요?
Microsoft.Compute/운영/읽기	예	예
Microsoft.Compute/virtualMachines/instanceView/read	예	예
Microsoft.Compute/virtualMachines/powerOff/action	예	아니요
Microsoft.Compute/virtualMachines/읽기	예	예
Microsoft.Compute/virtualMachines/다시 시작/작업	예	아니요
Microsoft.Compute/virtualMachines/시작/작업	예	아니요
Microsoft.Compute/virtualMachines/vmSizes/읽기	아니요	예
Microsoft.Compute/virtualMachines/쓰기	예	아니요
Microsoft.Compute/이미지/읽기	예	예
Microsoft.Compute/디스크/삭제	예	아니요
Microsoft.Compute/디스크/읽기	예	예
Microsoft.Compute/디스크/쓰기	예	아니요
Microsoft.Storage/checknameavailability/read	예	예
Microsoft.Storage/operations/read	예	예
Microsoft.Storage/storageAccounts/listkeys/action	예	아니요
Microsoft.Storage/storageAccounts/read	예	예
Microsoft.Storage/storageAccounts/write	예	아니요
Microsoft.Storage/storageAccounts/blobServices/containers/read	예	예
Microsoft.Network/networkInterfaces/read	예	예
Microsoft.Network/networkInterfaces/write	예	아니요
Microsoft.Network/networkInterfaces/join/action	예	아니요
Microsoft.Network/networkSecurityGroups/read	예	예
Microsoft.Network/networkSecurityGroups/write	예	아니요

행동	설정에 사용?	일상 업무에 사용되나요?
Microsoft.Resources/subscriptions/locations/read	예	예
Microsoft.Network/locations/operationResults/read	예	예
Microsoft.Network/locations/operations/read	예	예
Microsoft.Network/virtualNetworks/read	예	예
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/읽기	예	예
Microsoft.Network/virtualNetworks/subnets/read	예	예
Microsoft.Network/virtualNetworks/서브넷/virtualMachines/read	예	예
Microsoft.Network/virtualNetworks/virtualMachines/read	예	예
Microsoft.Network/virtualNetworks/subnets/join/action	예	아니요
Microsoft.Network/virtualNetworks/subnets/write	예	아니요
Microsoft.Network/routeTables/join/action	예	아니요
Microsoft.Resources/deployments/operations/read	예	예
Microsoft.Resources/deployments/read	예	예
Microsoft.Resources/deployments/write	예	아니요
Microsoft.Resources/resources/read	예	예
Microsoft.Resources/subscriptions/operationresults/read	예	예
Microsoft.Resources/구독/resourceGroups/삭제	예	아니요
Microsoft.Resources/subscriptions/resourceGroups/read	예	예
Microsoft.Resources/구독/리소스그룹/리소스/읽기	예	예
Microsoft.Resources/subscriptions/resourceGroups/write	예	아니요

Cloud Volumes ONTAP

에이전트는 Azure에서 Cloud Volumes ONTAP 배포하고 관리하기 위해 다음과 같은 API 요청을 합니다.

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
VM 생성 및 관리	Microsoft.Compute/위치/작업/읽기	예	예	아니요
	Microsoft.Compute/위치/vmSizes/읽기	예	예	아니요
	Microsoft.Resources/subscriptions/locations/read	예	아니요	아니요
	Microsoft.Compute/운영/읽기	예	예	아니요
	Microsoft.Compute/virtualMachines/instanceView/read	예	예	아니요
	Microsoft.Compute/virtualMachines/powerOff/action	예	예	아니요
	Microsoft.Compute/virtualMachines/읽기	예	예	아니요
	Microsoft.Compute/virtualMachines/다시 시작/작업	예	예	아니요
	Microsoft.Compute/virtualMachines/시작/작업	예	예	아니요
	Microsoft.Compute/virtualMachines/할당 해제/작업	아니요	예	예
	Microsoft.Compute/virtualMachines/vmSizes/읽기	아니요	예	아니요
	Microsoft.Compute/virtualMachines/쓰기	예	예	아니요
	Microsoft.Compute/virtualMachines/삭제	예	예	예
	Microsoft.Resources/deployments/delete	예	아니요	아니요
VHD에서 배포 활성화	Microsoft.Compute/이미지/읽기	예	아니요	아니요
	Microsoft.Compute/이미지/쓰기	예	아니요	아니요

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
대상 서브넷에서 네트워크 인터페이스를 생성하고 관리합니다.	Microsoft.Network/networkInterfaces/read	예	예	아니요
	Microsoft.Network/networkInterfaces/write	예	예	아니요
	Microsoft.Network/networkInterfaces/join/action	예	예	아니요
	Microsoft.Network/networkInterfaces/삭제	예	예	아니요
네트워크 보안 그룹 생성 및 관리	Microsoft.Network/networkSecurityGroups/read	예	예	아니요
	Microsoft.Network/networkSecurityGroups/write	예	예	아니요
	Microsoft.Network/networkSecurityGroups/join/action	예	아니요	아니요
	Microsoft.Network/networkSecurityGroups/삭제	아니요	예	예

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
지역, 대상 VNet 및 서브넷에 대한 네트워크 정보를 가져오고 VNet에 VM을 추가합니다.	Microsoft.Network/locations/operationResults/read	예	예	아니요
	Microsoft.Network/locations/operations/read	예	예	아니요
	Microsoft.Network/virtualNetworks/read	예	아니요	아니요
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/읽기	예	아니요	아니요
	Microsoft.Network/virtualNetworks/subnets/read	예	예	아니요
	Microsoft.Network/virtualNetworks/서브넷/virtualMachines/read	예	예	아니요
	Microsoft.Network/virtualNetworks/virtualMachines/read	예	예	아니요
	Microsoft.Network/virtualNetworks/subnets/join/action	예	예	아니요

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
리소스 그룹 생성 및 관리	Microsoft.Resources/deployments/operations/read	예	예	아니요
	Microsoft.Resources/deployments/read	예	예	아니요
	Microsoft.Resources/deployments/write	예	예	아니요
	Microsoft.Resources/resources/read	예	예	아니요
	Microsoft.Resources/subscriptions/operationresults/read	예	예	아니요
	Microsoft.Resources/구독/resourceGroups/삭제	예	예	예
	Microsoft.Resources/subscriptions/resourceGroups/read	아니요	예	아니요
	Microsoft.Resources/구독/리소스그룹/리소스/읽기	예	예	아니요
	Microsoft.Resources/subscriptions/resourceGroups/write	예	예	아니요

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
Azure Storage 계정 및 디스크 관리	Microsoft.Compute/디스크/읽기	예	예	예
	Microsoft.Compute/디스크/쓰기	예	예	아니요
	Microsoft.Compute/디스크/삭제	예	예	예
	Microsoft.Storage/checknameavailability/read	예	예	아니요
	Microsoft.Storage/operations/read	예	예	아니요
	Microsoft.Storage/storageAccounts/listkeys/action	예	예	아니요
	Microsoft.Storage/storageAccounts/read	예	예	아니요
	Microsoft.Storage/storageAccounts/삭제	아니요	예	예
	Microsoft.Storage/storageAccounts/write	예	예	아니요
	Microsoft.Storage/사용법/읽기	아니요	예	아니요
Blob 스토리지에 대한 백업 및 스토리지 계정 암호화 활성화	Microsoft.Storage/storageAccounts/blobServices/containers/read	예	예	아니요
	Microsoft.KeyVault/vaults/read	예	예	아니요
	Microsoft.KeyVault/vaults/accessPolicies/write	예	예	아니요
데이터 계층화를 위해 VNet 서비스 엔드포인트 활성화	Microsoft.Network/virtualNetworks/subnets/write	예	예	아니요
	Microsoft.Network/routeTables/join/action	예	예	아니요

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
Azure 관리 스냅샷 만들기 및 관리	Microsoft.Compute/스냅샷/쓰기	예	예	아니요
	Microsoft.Compute/스냅샷/읽기	예	예	아니요
	Microsoft.Compute/스냅샷/삭제	아니요	예	예
	Microsoft.Compute/디스크/beginGetAccess/작업	아니요	예	아니요
가용성 집합을 만들고 관리합니다.	Microsoft.Compute/가용성 세트/쓰기	예	아니요	아니요
	Microsoft.Compute/가용성 세트/읽기	예	아니요	아니요
마켓플레이스에서 프로그래밍 방식 배포 활성화	Microsoft.Marketplace주문/제안 유형/게시자/제안/계획/계약/읽기	예	아니요	아니요
	Microsoft.Marketplace주문/제안 유형/게시자/제안/계획/계약/쓰기	예	예	아니요

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
HA 쌍에 대한 로드 밸런서 관리	Microsoft.Network/loadBalancers/읽기	예	예	아니요
	Microsoft.Network/loadBalancers/쓰기	예	아니요	아니요
	Microsoft.Network/loadBalancers/삭제	아니요	예	예
	Microsoft.Network/loadBalancers/backendAddressPools/read	예	아니요	아니요
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	예	아니요	아니요
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	예	예	아니요
	Microsoft.Network/loadBalancers/loadBalancingRules/read	예	아니요	아니요
	Microsoft.Network/loadBalancers/프로브/읽기	예	아니요	아니요
	Microsoft.Network/loadBalancers/probes/join/action	예	아니요	아니요
Azure 디스크의 잠금 관리 활성화	Microsoft.Authorization/locks/*	예	예	아니요

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
서브넷 외부에 연결이 없는 경우 HA 쌍에 대한 개인 엔드포인트를 활성화합니다.	Microsoft.Network/privateEndpoints/쓰기	예	예	아니요
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	예	아니요	아니요
	Microsoft.Storage/storageAccounts/privateEndpointConnections/읽기	예	예	예
	Microsoft.Network/privateEndpoints/읽기	예	예	예
	Microsoft.Network/privateDnsZones/write	예	예	아니요
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	예	예	아니요
	Microsoft.Network/virtualNetworks/join/action	예	예	아니요
	Microsoft.Network/privateDnsZones/A/write	예	예	아니요
	Microsoft.Network/privateDnsZones/읽기	예	예	아니요
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	예	예	아니요
기본 물리적 하드웨어에 따라 일부 VM 배포에 필요함	Microsoft.Resources/deployments/operationStatuses/read	예	예	아니요
배포 실패 또는 삭제 시 리소스 그룹에서 리소스 제거	Microsoft.Network/privateEndpoints/삭제	예	예	아니요
	Microsoft.Compute/availabilitySets/삭제	예	예	아니요

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
API를 사용할 때 고객 관리 암호화 키 사용을 활성화합니다.	Microsoft.Compute/diskEncryptionSets/읽기	예	예	예
	Microsoft.Compute/diskEncryptionSets/쓰기	예	예	아니요
	Microsoft.KeyVault/vaults/deploy/action	예	아니요	아니요
	Microsoft.Compute/diskEncryptionSets/삭제	예	예	예
HA 쌍에 대한 애플리케이션 보안 그룹을 구성하여 HA 상호 연결 및 클러스터 네트워크 NIC를 격리합니다.	Microsoft.Network/applicationSecurityGroups/write	아니요	예	아니요
	Microsoft.Network/applicationSecurityGroups/read	아니요	예	아니요
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	아니요	예	아니요
	Microsoft.Network/networkSecurityGroups/securityRules/write	예	예	아니요
	Microsoft.Network/applicationSecurityGroups/삭제	아니요	예	예
	Microsoft.Network/networkSecurityGroups/securityRules/삭제	아니요	예	예
Cloud Volumes ONTAP 리소스와 관련된 태그를 읽고, 쓰고, 삭제합니다.	Microsoft.Resources/태그/읽기	아니요	예	아니요
	Microsoft.Resources/태그/쓰기	예	예	아니요
	Microsoft.Resources/태그/삭제	예	아니요	아니요
생성 중에 저장소 계정을 암호화합니다.	Microsoft.ManagedIdentity/userAssignedIdentities/할당/작업	예	예	아니요

목적	행동	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
Cloud Volumes ONTAP 에 대한 특정 영역을 지정하려면 유연한 오케스트레이션 모드에서 가상 머신 확장 세트를 사용하세요.	Microsoft.Compute/virtualMachineScaleSets/쓰기	예	아니요	아니요
	Microsoft.Compute/virtualMachineScaleSets/읽기	예	아니요	아니요
	Microsoft.Compute/virtualMachineScaleSets/삭제	아니요	아니요	예

티어링

NetApp Cloud Tiering 설정하면 에이전트는 다음 API 요청을 합니다.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/locations/read

콘솔 에이전트는 일상적인 작업을 위해 다음과 같은 API 요청을 합니다.

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Storage/storageAccounts/read

변경 로그

권한이 추가되거나 제거되면 아래 섹션에 기록됩니다.

2025년 **11**월 **11**일

최소한의 권한과 최소한의 범위를 반영하는 사용자 지정 JSON 정책이 추가되었습니다.

최소 백업 및 복구 권한 목록에 다음 권한이 추가되었습니다.

- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

레거시 인덱싱을 사용하지 않는 한 다음 권한은 더 이상 백업 및 복구에 필요하지 않습니다.

- Microsoft.Synapse/workspaces/write
- Microsoft.Synapse/workspaces/read
- Microsoft.Synapse/workspaces/삭제
- Microsoft.Synapse/등록/작업
- Microsoft.Synapse/checkNameAvailability/action

- Microsoft.Synapse/workspaces/operationStatuses/read
- Microsoft.Synapse/workspaces/firewallRules/read
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft.Synapse/workspaces/operationResults/read
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

다음 권한은 최소 구성에 필요하지 않으므로 "추가 백업 및 복구 권한" 섹션으로 이동되었습니다.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/구독/리소스그룹/리소스/읽기
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write

2024년 **9**월 **9**일

콘솔이 더 이상 Kubernetes 클러스터의 검색 및 관리를 지원하지 않으므로 다음 권한이 JSON 정책에서 제거되었습니다.

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/작업
- Microsoft.ContainerService/managedClusters/읽기

2024년 **8**월 **22**일

다음 권한은 Virtual Machine Scale Sets에 대한 Cloud Volumes ONTAP 지원에 필요하므로 JSON 정책에 추가되었습니다.

- Microsoft.Compute/virtualMachineScaleSets/쓰기
- Microsoft.Compute/virtualMachineScaleSets/읽기
- Microsoft.Compute/virtualMachineScaleSets/삭제

2023년 **12**월 **5**일

NetApp Backup and Recovery 에서 볼륨 데이터를 Azure Blob 스토리지에 백업할 때 다음 권한은 더 이상 필요하지 않습니다.

- Microsoft.Compute/virtualMachines/읽기
- Microsoft.Compute/virtualMachines/시작/작업

- Microsoft.Compute/virtualMachines/할당 해제/작업
- Microsoft.Compute/virtualMachines/확장/삭제
- Microsoft.Compute/virtualMachines/삭제

이러한 권한은 다른 콘솔 스토리지 서비스에 필요하므로 다른 스토리지 서비스를 사용하는 경우 에이전트의 사용자 지정 역할에 그대로 유지됩니다.

2023년 **5**월 **12**일

다음 권한은 Cloud Volumes ONTAP 관리에 필요하므로 JSON 정책에 추가되었습니다.

- Microsoft.Compute/이미지/쓰기
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read

다음 권한은 더 이상 필요하지 않으므로 JSON 정책에서 제거되었습니다.

- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.Network/publicIPAddresses/삭제

2023년 **3**월 **23**일

데이터 분류에는 "Microsoft.Storage/storageAccounts/delete" 권한이 더 이상 필요하지 않습니다.

이 권한은 Cloud Volumes ONTAP 에 여전히 필요합니다.

2023년 **1**월 **5**일

JSON 정책에 다음 권한이 추가되었습니다.

- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

  이러한 권한은 NetApp Backup and Recovery 에 필요합니다.

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

  이 권한은 Cloud Volumes ONTAP 배포에 필요합니다.

Azure의 콘솔 에이전트 보안 그룹 규칙

에이전트의 Azure 보안 그룹에는 인바운드 규칙과 아웃바운드 규칙이 모두 필요합니다. NetApp Console 에서 콘솔 에이전트를 만들면 이 보안 그룹이 자동으로 생성됩니다. 다른 설치 옵션의 경우 이 보안 그룹을 수동으로 설정해야 합니다.

인바운드 규칙

규약	포트	목적
SSH	22	에이전트 호스트에 SSH 액세스를 제공합니다.
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 인터페이스로의 HTTPS 액세스와 NetApp Data Classification 인스턴스로부터의 연결을 제공합니다.
TCP	3128	NetApp 지원팀에 AutoSupport 메시지를 보내기 위해 Cloud Volumes ONTAP 에 인터넷 액세스를 제공합니다. 배포 후에는 수동으로 이 포트를 열어야 합니다. "에이전트가 AutoSupport 메시지의 프록시로 사용되는 방식을 알아보세요."

아웃바운드 규칙

에이전트에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 개방합니다. 이것이 허용된다면, 기본적인 아웃바운드 규칙을 따르세요. 더욱 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

에이전트에 대한 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

규약	포트	목적
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 에이전트의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

소스 IP 주소는 에이전트 호스트입니다.

서비스	규약	포트	목적지	목적
API 호출 및 AutoSupport	HTTPS	443	아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF	Azure, ONTAP, NetApp Data Classification 대한 API 호출 및 NetApp 에 대한 AutoSupport 메시지 전송
API 호출	TCP	8080	데이터 분류	배포 중 데이터 분류 인스턴스에 대한 프로브
DNS	UDP	53	DNS	콘솔에서 DNS를 확인하는 데 사용됩니다.

Google 클라우드 권한 및 필수 방화벽 규칙

콘솔 에이전트에 대한 **Google Cloud** 권한

콘솔 에이전트에는 Google Cloud에서 작업을 수행하려면 권한이 필요합니다. 이러한 권한은 NetApp 에서 제공하는 사용자 정의 역할에 포함되어 있습니다. 에이전트가 이러한 권한을 어떻게 사용하는지 이해해야 합니다.

Google Cloud 사용자 계정 권한

아래의 사용자 지정 역할은 Google Cloud 사용자에게 에이전트를 배포하는 데 필요한 권한을 부여합니다. 에이전트를 배포할 사용자에게 이 사용자 지정 역할을 적용하십시오.

Google Cloud 사용자 계정 권한 보기

```
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
```

서비스 계정 권한

아래의 사용자 지정 역할은 콘솔 에이전트에 연결된 Google Cloud 서비스 계정에 Google Cloud 네트워크의 리소스 및 프로세스를 관리하는 데 필요한 권한을 부여합니다.

콘솔 에이전트 VM에 연결된 서비스 계정에 이 사용자 지정 역할을 적용합니다.

- "표준 모드에 대한 Google Cloud 권한 설정"
- "제한 모드에 대한 권한 설정"

Google 서비스 계정 권한 보기

향후 릴리스에서 새로운 권한이 추가되거나 제거될 경우 역할이 최신 상태인지 확인하십시오. 변경 로그에는 필요한 새 권한이 나열되어 있습니다."Google 권한 변경 로그를 검토하세요." "Google 클라우드 서비스 계정을 추가하는 방법을 살펴보세요."

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent.
stage: GA
includedPermissions:
- cloudbuild.builds.get
- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken
- cloudbuild.repositories.list
- cloudquotas.quotas.get
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
- config.artifacts.import
- config.deployments.create
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getLock
- config.deployments.getState
- config.deployments.update
- config.deployments.updateState
- config.previews.upload
- config.revisions.get
- config.revisions.getState
- config.deployments.getLock
- config.deployments.list
- config.deployments.lock
- config.operations.get
- config.previews.get
- config.previews.list
- config.resources.list
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.regionBackendServices.update
- compute.networks.updatePolicy
- compute.addresses.createInternal
```

```
- compute.addresses.deleteInternal
- compute.addresses.list
- compute.addresses.setLabels
- compute.addresses.useInternal
- compute.backendServices.create
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels
- compute.globalOperations.get
- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instances.use
```

```
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.get
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.instances.setMinCpuPlatform
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.regionBackendServices.delete
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
```

```
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- logging.logEntries.create
- logging.logEntries.route
- monitoring.timeSeries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- storage.objects.create
- storage.objects.delete
- storage.objects.list
- storage.objects.update
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.get
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.objects.get
- storage.objects.list
- storage.buckets.getIamPolicy
```

Google Cloud 권한 사용 방법

콘솔 에이전트는 사용자 지정 역할의 권한을 사용하여 Google Cloud 네트워크에서 Cloud Volumes ONTAP 리소스와 NetApp 데이터 서비스 프로세스를 관리합니다. 다음 섹션에서는 에이전트가 이러한 권한을 사용하는 방법을 설명합니다.

Cloud Volumes ONTAP 에 사용되는 권한

콘솔 에이전트는 사용자 지정 역할의 권한을 사용하여 Google Cloud 네트워크에서 Cloud Volumes ONTAP 리소스 및 프로세스를 관리합니다. 다음 섹션에서는 에이전트가 이러한 권한을 사용하는 방법을 설명합니다.

Cloud Volumes ONTAP 에 대한 권한

행위	목적	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
config.deployments.create	Google Cloud Infrastructure Manager를 사용하여 Cloud Volumes ONTAP 가상 머신 인스턴스를 배포하는 방법입니다.	예	아니요	아니요
config.deployments.delete		아니요	아니요	예
config.deployments.deleteState		아니요	아니요	예
config.deployments.get		아니요	예	아니요
config.deployments.getLock		아니요	예	아니요
config.deployments.getState		아니요	예	아니요
config.deployments.list		아니요	예	아니요
config.deployments.lock		아니요	예	아니요
config.deployments.update		아니요	예	아니요
config.deployments.updateState		아니요	예	아니요
구성.작업.get		아니요	예	아니요
config.previews.get		아니요	예	아니요
설정 미리보기 목록		아니요	예	아니요
구성 리소스 목록		아니요	예	아니요
config.revisions.get		아니요	예	아니요
계산.디스크.생성	Cloud Volumes ONTAP 에 대한 디스크를 생성하고 관리합니다.	예	예	아니요
컴퓨팅.디스크.스냅샷 생성		아니요	예	아니요
컴퓨팅.디스크.삭제		아니요	예	예
컴퓨팅.디스크.get		아니요	예	아니요
컴퓨팅.디스크.목록		예	예	아니요
컴퓨팅.디스크.레이블 설정		예	예	아니요
컴퓨팅.디스크.사용		아니요	예	아니요

행위	목적	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
컴퓨팅.방화벽.생성	Cloud Volumes ONTAP 에 대한 방화벽 규칙을 만듭니다.	예	아니요	아니요
컴퓨팅.방화벽.삭제		아니요	예	예
컴퓨팅.방화벽.get		예	예	아니요
컴퓨팅.방화벽.목록		예	예	아니요
계산.전달규칙.생성	백엔드 서비스로의 트래픽 라우팅을 위한 포워딩 규칙을 생성합니다.	아니요	예	아니요
compute.forwardingRules.delete	기존 전달 규칙을 삭제합니다.	아니요	예	아니요
compute.forwardingRules.get	기존 전달 규칙에 대한 세부 정보를 검색합니다.	아니요	예	아니요
compute.forwardingRules.setLabels	조직에 대한 전달 규칙의 레이블을 설정하거나 업데이트합니다.	아니요	예	아니요
compute.globalOperations.get	작업 상태를 파악하려면	예	예	아니요
compute.healthChecks.create	백엔드 서비스 상태를 모니터링하기 위한 상태 점검을 생성하고 관리합니다.	아니요	예	아니요
compute.healthChecks.delete		아니요	예	아니요
compute.healthChecks.get		아니요	예	아니요
compute.healthChecks.useReadOnly		아니요	예	아니요
계산.이미지.get	VM 인스턴스에 대한 이미지를 가져옵니다.	예	아니요	아니요
계산.이미지.패밀리에서 가져오기		예	아니요	아니요
계산.이미지.목록		예	아니요	아니요
계산.이미지.읽기 전용 사용		예	아니요	아니요
컴퓨팅.인스턴스.디스크 연결	Cloud Volumes ONTAP 에 디스크를 연결하고 분리합니다.	예	예	아니요
컴퓨팅.인스턴스.디스크 분리		아니요	예	예

행위	목적	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
컴퓨팅.인스턴스.생성	Cloud Volumes ONTAP VM 인스턴스를 생성하고 삭제합니다.	예	아니요	아니요
컴퓨팅.인스턴스.삭제		아니요	아니요	예
컴퓨팅.인스턴스.get	VM 인스턴스를 나열합니다.	예	예	아니요
컴퓨팅.인스턴스.get SerialPortOutput	콘솔 로그를 얻으려면.	예	예	아니요
컴퓨팅.인스턴스.목록	영역의 인스턴스 목록을 검색합니다.	예	예	아니요
컴퓨팅.인스턴스.삭제 보호 설정	인스턴스에 삭제 보호를 설정합니다.	예	아니요	아니요
컴퓨팅.인스턴스.setLabels	라벨을 추가하려면.	예	아니요	아니요
컴퓨팅.인스턴스.set MachineType	Cloud Volumes ONTAP 의 머신 유형을 변경하려면	예	예	아니요
컴퓨팅.인스턴스.set MinCpuPlatform		예	예	아니요
컴퓨팅.인스턴스.메타데이터 설정	메타데이터를 추가합니다.	예	예	아니요
컴퓨팅.인스턴스.태그 설정	방화벽 규칙에 대한 태그를 추가합니다.	예	예	아니요
컴퓨팅.인스턴스.시작	Cloud Volumes ONTAP 시작하고 중지합니다.	예	예	아니요
컴퓨팅.인스턴스.중지		예	예	아니요
컴퓨팅.인스턴스.업데이트디스플레이장치		예	예	아니요
compute.instances.use	가상 머신 인스턴스를 사용합니다(시작, 중지, 연결 작업).	아니요	예	아니요
계산.머신타입.get	할당량을 확인하기 위해 코어 수를 얻습니다.	예	아니요	아니요
계산.프로젝트.get	다양한 프로젝트를 지원합니다.	예	아니요	아니요
compute.resourcePolicies.create	자동화된 리소스 관리를 위한 리소스 정책을 생성하고 관리합니다.	아니요	예	아니요
compute.resourcePolicies.delete		아니요	예	아니요
compute.resourcePolicies.get		아니요	예	아니요

행위	목적	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
계산.스냅샷.생성	영구 디스크 스냅샷을 만들고 관리합니다.	예	예	아니요
계산.스냅샷.삭제		아니요	예	예
계산.스냅샷.get		아니요	예	아니요
컴퓨팅.스냅샷.목록		아니요	예	아니요
계산.스냅샷.설정.레이블		예	예	아니요
컴퓨팅.네트워크.get	새로운 Cloud Volumes ONTAP 가상 머신 인스턴스를 만드는 데 필요한 네트워킹 정보를 얻으세요.	예	예	아니요
컴퓨팅.네트워크.목록		예	예	아니요
계산.지역.get		예	예	아니요
계산.지역.목록		예	예	아니요
컴퓨팅.서브네트워크.get		예	예	아니요
컴퓨팅.서브네트워크.목록		예	예	아니요
컴퓨팅.zoneOperations.get		예	예	아니요
컴퓨팅.존.get		예	예	아니요
컴퓨팅.존.리스트		예	예	아니요

행위	목적	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
배포 관리자.compositeTypes.get	Google Cloud Deployment Manager를 사용하여 Cloud Volumes ONTAP 가상 머신 인스턴스를 배포합니다.	예	아니요	아니요
배포 관리자.compositeTypes.list		예	아니요	아니요
배포 관리자.배포.생성		예	아니요	아니요
배포 관리자.배포.삭제		예	아니요	아니요
배포 관리자.배포.get		예	아니요	아니요
배포 관리자.배포.목록		예	아니요	아니요
배포 관리자.매니페스트.get		예	아니요	아니요
배포 관리자.매니페스트.목록		예	아니요	아니요
배포 관리자.운영.get		예	아니요	아니요
배포 관리자.운영.목록		예	아니요	아니요
배포 관리자.리소스.get		예	아니요	아니요
배포 관리자.리소스.목록		예	아니요	아니요
배포 관리자.typeProviders.get		예	아니요	아니요
배포 관리자.유형 공급자.목록		예	아니요	아니요
배포 관리자.유형.get		예	아니요	아니요
배포 관리자.유형.목록		예	아니요	아니요
로깅.로그 항목.목록	스택 로그 드라이브를 얻으려면.	예	예	아니요
로깅.privateLogEntries.list		예	예	아니요
logging.logEntries.create	모니터링, 디버깅 및 감사를 위한 로그 항목을 생성하고 라우팅합니다.	예	예	아니요
logging.logEntries.route		예	예	아니요

행위	목적	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
리소스 관리자 .프로젝트.get	다양한 프로젝트를 지원합니다.	예	예	아니요
저장소.버킷.생성	데이터 계층화를 위해 Google Cloud Storage 버킷을 만들고 관리합니다.	예	예	아니요
저장소.버킷.삭제		아니요	예	예
스토리지.버킷.get		아니요	예	아니요
스토리지.버킷.리스트		아니요	예	아니요
저장소.버킷.업데이트		아니요	예	아니요
cloudkms.cryptoKeyVersions.useToEncrypt	Cloud Volumes ONTAP 과 함께 Cloud Key Management Service의 고객 관리 암호화 키를 사용합니다.	예	예	아니요
cloudkms.cryptoKeys.get		예	예	아니요
cloudkms.cryptoKeys.list		예	예	아니요
cloudkms.keyRings.list		예	예	아니요
클라우드빌드.빌드.겟		예	아니요	아니요
컴퓨팅.인스턴스.서비스 계정 설정	Cloud Volumes ONTAP 인스턴스에 서비스 계정을 설정하려면 이 서비스 계정은 Google Cloud Storage 버킷에 대한 데이터 계층화 권한을 제공합니다.	예	예	아니요
iam.serviceAccounts.actAs		예	아니요	아니요
iam.serviceAccounts.create		예	아니요	아니요
iam.serviceAccounts.getIamPolicy		예	예	아니요
iam.serviceAccounts.list		예	예	아니요
iam.serviceAccountKeys.create		예	아니요	아니요
스토리지.객체.생성	Google Cloud Storage 버킷에 객체(파일)를 생성하고 관리합니다.	예	예	아니요
저장소.객체.삭제		아니요	아니요	예
저장소.객체.get		예	예	아니요
저장소.객체.목록		예	예	아니요
계산.주소.목록	HA 쌍을 배포할 때 지역의 주소를 검색합니다.	예	아니요	아니요

행위	목적	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
compute.addresses.createInternal	리소스 할당을 위해 VPC 네트워크 내에 내부 IP 주소를 생성합니다.	아니요	예	아니요
compute.addresses.deleteInternal	리소스 정리를 위해 내부 IP 주소를 삭제합니다.	아니요	예	아니요
compute.addresses.setLabels	Address 리소스의 레이블을 업데이트합니다.	아니요	예	아니요
compute.addresses.useInternal	네트워크 통신에는 내부 IP 주소를 사용하십시오.	아니요	예	아니요
컴퓨팅.백엔드서비스.생성	HA 쌍에서 트래픽을 분산하기 위한 백엔드 서비스를 구성합니다.	예	아니요	아니요
컴퓨팅.regionBackendServices.생성	트래픽 라우팅을 위한 백엔드 서비스를 생성하고 관리합니다.	예	아니요	아니요
compute.regionBackendServices.delete		아니요	예	아니요
컴퓨팅.regionBackendServices.get		예	아니요	아니요
compute.regionBackendServices.업데이트		예	예	아니요
컴퓨팅.regionBackendServices.list		예	아니요	아니요
compute.regionBackendServices.use		아니요	예	아니요
컴퓨팅.네트워크.업데이트 정책	HA 쌍의 VPC와 서브넷에 방화벽 규칙을 적용합니다.	예	아니요	아니요

행위	목적	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
컴퓨팅.인스턴스그룹.get	Cloud Volumes ONTAP HA 쌍에서 스토리지 VM을 생성하고 관리합니다.	예	예	아니요
계산.주소.가져오기		예	예	아니요
컴퓨팅.인스턴스.네트워크인터페이스 업데이트		예	예	아니요
compute.instanceGroups.create		아니요	예	아니요
compute.instanceGroups.delete		아니요	예	아니요
compute.instanceGroups.update		아니요	예	아니요
compute.instanceGroups.use		아니요	예	아니요
모니터링.timeSeries.list	Google Cloud Storage 버킷에 대한 정보를 알아보세요.	예	예	아니요
저장소.버킷.getIamPolicy		예	예	아니요

NetApp Backup and Recovery 에 사용되는 권한

콘솔 에이전트는 사용자 지정 역할의 권한을 사용하여 Google Cloud 네트워크에서 NetApp Backup and Recovery 리소스와 프로세스를 관리합니다. 다음 섹션에서는 에이전트가 이러한 권한을 사용하는 방법을 설명합니다.

NetApp Backup and Recovery 에 대한 보기 권한을 확인하세요.

행위	목적	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
• cloudkms.cryptoKeys.get • cloudkms.cryptoKeys.getIamPolicy • cloudkms.cryptoKeys.list • cloudkms.cryptoKeys.setIamPolicy • cloudkms.keyRings.get • cloudkms.keyRings.getIamPolicy • cloudkms.keyRings.list • cloudkms.keyRings.setIamPolicy	기본 Google 관리 암호화 키를 사용하는 대신 NetApp Backup and Recovery 활성화 마법사에서 고객이 관리하는 키를 직접 선택합니다.	예	예	아니요

NetApp Data Classification 에 사용되는 권한

콘솔 에이전트는 사용자 지정 역할의 권한을 사용하여 Google Cloud 네트워크에서 NetApp Data Classification 리소스 및 프로세스를 관리합니다. 다음 섹션에서는 에이전트가 이러한 권한을 사용하는 방법을 설명합니다.

NetApp Data Classification 에 대한 보기 권한

행위	목적	배포에 사용되나요?	일상 업무에 사용되나요?	삭제에 사용되나요?
• 컴퓨팅 .서브네트워크.사용 • 컴퓨팅 .서브네트워크.외부 IP 사용 • 컴퓨팅. 인스턴스.addAccessConfig	NetApp Data Classification 활성화하려면.	예	아니요	아니요

변경 로그

추가되거나 삭제된 권한은 아래에 명시되어 있습니다.

2025년 **12**월 **8**일

NetApp Google Cloud에서 콘솔 에이전트를 배포하고 실행하기 위해 Google Cloud Deployment Manager에서 Google Cloud Infrastructure Manager(IM)로 전환하고 있습니다. 이러한 변경 사항을 지원하기 위해 다음과 같은 권한이 추가되었습니다.

에이전트를 배포하는 Google Cloud 사용자에게는 다음과 같은 추가 권한이 필요합니다.

- 저장소.버킷.생성
- 스토리지.버킷.get
- 스토리지.객체.생성
- 저장 폴더 생성
- 저장소.객체.목록
- iam.serviceAccount.actAs
- config.deployments.create
- 구성.작업.get

일상적인 운영에 사용되는 Google Cloud 서비스 계정에 다음과 같은 추가 권한이 필요합니다.

- 클라우드빌드.연결.목록
- 클라우드빌드.리포지토리.액세스리드토큰
- 클라우드빌드.리포지토리.리스트
- 클라우드 할당량.할당량.받기
- config.artifacts.import
- config.deployments.deleteState

- config.deployments.getLock
- config.deployments.getState
- config.deployments.updateState
- 설정 미리보기 업로드
- config.revisions.getState
- logging.logEntries.create
- 스토리지.객체.생성
- 저장소.객체.삭제
- 저장소 객체 업데이트
- iam.serviceAccounts.get

Cloud Volumes ONTAP 배포하려면 다음과 같은 추가 권한이 필요합니다.

- 클라우드빌드.빌드.겟
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- 설정 미리보기 목록
- config.revisions.get
- 구성 리소스 목록
- iam.serviceAccountKeys.create
- iam.serviceAccounts.create

Cloud Volumes ONTAP 의 일상적인 운영에 사용되는 서비스 계정에 다음과 같은 추가 권한이 필요합니다.

- compute.addresses.createInternal
- compute.addresses.deleteInternal
- compute.addresses.setLabels
- compute.addresses.useInternal
- 계산.전달규칙.생성
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels
- compute.healthChecks.create

- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.instances.use
- compute.regionBackendServices.delete
- compute.regionBackendServices.업데이트
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- logging.logEntries.route
- config.deployments.create
- config.deployments.delete
- config.deployments.get
- config.deployments.update
- config.revisions.get
- config.deployments.lock
- 구성.작업.get

2025년 **11**월 **26**일

사용에 대한 명확성을 높이기 위해 권한이 업데이트되었지만, 권한이 추가되거나 제거되지는 않았습니다. 각 권한이 배포, 일상 작업 또는 삭제에 사용되는지 여부를 나타내는 세 개의 열이 추가되었습니다. 이 외에도 몇 가지 권한은 NetApp Data Classification 및 NetApp Backup and Recovery 에 대한 사용 여부에 따라 분리됩니다.

2023년 **2**월 **6**일

이 정책에 다음 권한이 추가되었습니다.

- 컴퓨팅.인스턴스.네트워크인터페이스 업데이트

이 권한은 Cloud Volumes ONTAP 에 필요합니다.

2023년 **1**월 **27**일

다음 권한이 이 정책에 추가되었습니다.

- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy

- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

이러한 권한은 NetApp Backup and Recovery 에 필요합니다.

Google Cloud의 에이전트 방화벽 규칙

에이전트에 대한 Google Cloud 방화벽 규칙에는 인바운드 규칙과 아웃바운드 규칙이 모두 필요합니다. NetApp Console 에서 콘솔 에이전트를 만들면 이 보안 그룹이 자동으로 생성됩니다. 다른 설치 옵션의 경우 이 보안 그룹을 수동으로 설정해야 합니다.

인바운드 규칙

규약	포트	목적
SSH	22	에이전트 호스트에 SSH 액세스를 제공합니다.
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.
TCP	3128	Cloud Volumes ONTAP 에 인터넷 접속을 제공합니다. 배포 후에는 수동으로 이 포트를 열어야 합니다.

아웃바운드 규칙

에이전트의 사전 정의된 방화벽 규칙은 모든 아웃바운드 트래픽을 개방합니다. 허용되는 경우 기본 아웃바운드 규칙을 따르고, 더 엄격한 요구 사항이 있는 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

에이전트에 대한 미리 정의된 방화벽 규칙에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

규약	포트	목적
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 에이전트의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

소스 IP 주소는 에이전트 호스트입니다.

서비스	규약	포트	목적지	목적
API 호출 및 AutoSupport	HTTPS	443	아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF	Google Cloud, ONTAP, NetApp Data Classification 대한 API 호출 및 NetApp 에 대한 AutoSupport 메시지 전송
API 호출	TCP	8080	데이터 분류	배포 중 데이터 분류 인스턴스에 대한 프로브
DNS	UDP	53	DNS	데이터 분류에 의한 DNS 확인에 사용됨

3.9.55 이하 버전에 필요한 네트워크 액세스

NetApp Console, NetApp Console 에이전트 및 NetApp 데이터 서비스는 필요한 엔드포인트에 연결하기 위해 아웃바운드 인터넷 액세스가 필요합니다.

이 항목에서는 NetApp Console 표준 모드 3.9.55 이하 버전에 필요한 네트워크 액세스에 대해 설명합니다. 4.0.0 이상에 필요한 엔드포인트에 대해서는 다음을 검토하세요."4.0.0 이상에 필요한 엔드포인트" .

다음에 대한 네트워크 액세스를 설정해야 합니다.

- SaaS(Software as a Service)로 NetApp Console 액세스하는 컴퓨터
- 온프레미스 또는 클라우드에 설치하는 콘솔 에이전트입니다.

4.0.0 이상에 대한 개정된 목록으로 엔드포인트 목록을 업데이트하세요.

버전 4.0.0부터 콘솔 에이전트에 필요한 엔드포인트 수가 줄었습니다. 4.0.0 이전의 기존 배포는 계속 지원됩니다. 4.0.0 이상으로 업그레이드한 후, 편리한 시기에 허용 목록에서 이전 엔드포인트를 제거할 수 있습니다.

NetApp 더 작고, 더 안전하며, 관리하기 쉬운 개정된 엔드포인트 목록을 사용하도록 방화벽 규칙을 업데이트할 것을 권장합니다. NetApp 와일드카드 입력이 필요 없으며, 에이전트 업그레이드를 위한 엔드포인트는 모든 데이터 서비스를 지원합니다.

3.9.55 이하 엔드포인트	4.0.0 이상용 엔드포인트	목적
• \ https://support.netapp.com • \ https://mysupport.netapp.com	• \ https://mysupport.netapp.com • \ https://signin.b2c.netapp.com • \ https://support.netapp.com	NetApp 지원팀에 라이선스를 요청하고 문의하세요.

3.9.55 이하 엔드포인트	**4.0.0** 이상용 엔드포인트	목적
• https://*.api.bluexp.netapp.com • \ https://api.bluexp.netapp.com • https://*.cloudmanager.cloud.netapp.com • \ https://cloudmanager.cloud.netapp.com • \ https://netapp-cloud-account.auth0.com • \ https://netapp-cloud-account.us.auth0.com • \ https://console.bluexp.netapp.com • https://*.console.bluexp.netapp.com	• \ 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	일상 업무에 사용.
• https://*.blob.core.windows.net • \ https://cloudmanagerinfraprod.azurecr.io	• \ https://bluexpinfraprod.eastus2.data.azurecr.io • \ https://bluexpinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면.

단계

1. 에이전트 버전이 4.0.0 이상인지 확인하세요."에이전트 버전 보기."
2. 엔드포인트를 허용 목록에 추가"4.0.0 이상에서 지원되는 엔드포인트" .
3. 다음 명령을 실행하여 각 에이전트에서 서비스 관리자 2 서비스를 다시 시작합니다.

```
systemctl restart netapp-service-manager.service
```

4. 다음 명령을 실행하고 에이전트 상태가 _active(running)_로 표시되는지 확인하세요.

```
systemctl status netapp-service-manager.service
```

5. 방화벽 허용 목록에서 이전 엔드포인트를 제거합니다.

3.9.55 이하 NetApp Console 및 콘솔 에이전트의 엔드포인트

이러한 엔드포인트는 콘솔 에이전트 3.9.55 이하에 사용됩니다.

엔드포인트	목적
\ https://support.netapp.com \ https://mysupport.netapp.com	라이선스 정보를 얻고 NetApp 지원팀에 AutoSupport 메시지를 보냅니다.
https://*.api.bluexp.netapp.com \ https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com \ https://cloudmanager.cloud.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com	NetApp Console 내에서 기능과 서비스를 제공합니다.
두 가지 엔드포인트 세트 중에서 선택하세요. • 옵션 1(권장) \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • 옵션 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	콘솔 에이전트 업그레이드를 위한 이미지를 얻으려면. NetApp 랜섬웨어 복원력이나 백업 및 복구를 사용하지 않는 한, 보안이 더 뛰어난 옵션 1 엔드포인트를 방화벽에서 허용하고 옵션 2 엔드포인트는 허용하지 않을 것을 권장합니다. 이러한 종료점에 대해 다음 사항을 참고하세요. • 옵션 1 엔드포인트는 3.9.47 이상에서 지원됩니다. 3.9.47 이전 릴리스에서는 이전 버전과의 호환성이 지원되지 않습니다. • 콘솔 에이전트는 먼저 옵션 2의 엔드포인트와 접촉을 시작합니다. 해당 엔드포인트에 접근할 수 없는 경우 옵션 1의 엔드포인트에 자동으로 접속합니다. • NetApp Backup and Recovery 또는 Ransomware Resilience와 함께 콘솔 에이전트를 사용하는 경우 시스템은 옵션 1 엔드포인트를 지원하지 않습니다. 옵션 2 엔드포인트를 허용하고 옵션 1을 허용하지 않습니다.

콘솔 에이전트가 연락한 클라우드 공급자 엔드포인트

콘솔 에이전트가 클라우드 공급자에 배포된 경우 추가 엔드포인트에 액세스할 수 있어야 합니다.

콘솔 에이전트를 설치하기 전에 클라우드 공급자 엔드포인트에 대한 액세스를 활성화하세요.

- "콘솔 에이전트에 대한 AWS 네트워크 액세스 설정"
- "콘솔 에이전트에 대한 Azure 네트워크 액세스 설정"
- "콘솔 에이전트에 대한 Google Cloud 네트워크 액세스 설정"

클라우드 공급자 엔드포인트는 모든 버전에서 동일합니다.

콘솔 에이전트가 접속한 데이터 서비스 엔드포인트

콘솔 에이전트는 일부 NetApp 데이터 서비스와 Cloud Volumes ONTAP 지원하기 위해 추가적인 아웃바운드 인터넷 액세스가 필요합니다.

Cloud Volumes ONTAP 의 엔드포인트

- "AWS의 Cloud Volumes ONTAP 엔드포인트"
- "Azure의 Cloud Volumes ONTAP 엔드포인트"
- "Google Cloud의 Cloud Volumes ONTAP 엔드포인트"

Amazon EC2 인스턴스에서 IMDSv2 사용 요구

NetApp Console 콘솔 에이전트와 Cloud Volumes ONTAP (HA 배포를 위한 중재자 포함)을 통해 Amazon EC2 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 지원합니다. 대부분의 경우 IMDSv2는 새 EC2 인스턴스에 자동으로 구성됩니다. IMDSv1은 2024년 3월 이전에 활성화되었습니다. 보안 정책에 따라 EC2 인스턴스에서 IMDSv2를 수동으로 구성해야 할 수도 있습니다.

시작하기 전에

- 콘솔 에이전트 버전은 3.9.38 이상이어야 합니다.
- Cloud Volumes ONTAP 다음 버전 중 하나를 실행해야 합니다.
  - 9.12.1 P2(또는 이후 패치)
  - 9.13.0 P4(또는 이후 패치)
  - 9.13.1 또는 이 릴리스 이후의 모든 버전
- 이 변경을 수행하려면 Cloud Volumes ONTAP 인스턴스를 다시 시작해야 합니다.
- 이러한 단계에서는 응답 홉 제한을 3으로 변경해야 하므로 AWS CLI를 사용해야 합니다.

이 작업에 관하여

IMDSv2는 취약점에 대한 강화된 보호 기능을 제공합니다. "AWS 보안 블로그에서 IMDSv2에 대해 자세히 알아보세요."

EC2 인스턴스에서 IMDS(인스턴스 메타데이터 서비스)는 다음과 같이 활성화됩니다.

- 콘솔에서 새 콘솔 에이전트를 배포하거나 다음을 사용하는 경우 "Terraform 스크립트" IMDSv2는 EC2 인스턴스에서 기본적으로 활성화되어 있습니다.
- AWS에서 새로운 EC2 인스턴스를 시작한 다음 콘솔 에이전트 소프트웨어를 수동으로 설치하면 IMDSv2도 기본적으로 활성화됩니다.
- AWS Marketplace에서 콘솔 에이전트를 실행하면 IMDSv1이 기본적으로 활성화됩니다. EC2 인스턴스에서 IMDSv2를 수동으로 구성할 수 있습니다.
- 기존 콘솔 에이전트의 경우 IMDSv1이 계속 지원되지만 원하는 경우 EC2 인스턴스에서 IMDSv2를 수동으로 구성할 수 있습니다.
- Cloud Volumes ONTAP 의 경우 IMDSv1은 새 인스턴스와 기존 인스턴스에서 기본적으로 활성화됩니다. 원하는 경우 EC2 인스턴스에서 IMDSv2를 수동으로 구성할 수 있습니다.

단계

1. 콘솔 에이전트 인스턴스에서 IMDSv2를 사용해야 합니다.

   a. 콘솔 에이전트를 위해 Linux VM에 연결합니다.

      AWS에서 콘솔 에이전트 인스턴스를 생성할 때 AWS 액세스 키와 비밀 키를 제공했습니다. 이 키 쌍을 사용하여 인스턴스에 SSH를 실행할 수 있습니다. EC2 Linux 인스턴스의 사용자 이름은 ubuntu입니다 (2023년 5월 이전에 생성된 콘솔 에이전트의 경우 사용자 이름은 ec2-user였습니다).

      "AWS Docs: Linux 인스턴스에 연결"

   b. AWS CLI를 설치합니다.

      "AWS Docs: AWS CLI 최신 버전 설치 또는 업데이트"

   c. 사용하다 `aws ec2 modify-instance-metadata-options` IMDSv2 사용을 요구하고 PUT 응답 홉 제한을 3으로 변경하는 명령입니다.

      예

```
aws ec2 modify-instance-metadata-options \
    --instance-id <instance-id> \
    --http-put-response-hop-limit 3 \
    --http-tokens required \
    --http-endpoint enabled
```

+

> 그만큼 `http-tokens` 매개변수는 IMDSv2를 필수로 설정합니다. 언제 `http-tokens` 필수입니다. 또한 설정해야 합니다. `http-endpoint` 활성화됨.

2. Cloud Volumes ONTAP 인스턴스에서 IMDSv2를 사용해야 합니다.

   a. 로 가다 "Amazon EC2 콘솔"

   b. 탐색 창에서 *인스턴스*를 선택합니다.

   c. Cloud Volumes ONTAP 인스턴스를 선택하세요.

   d. *작업 > 인스턴스 설정 > 인스턴스 메타데이터 옵션 수정*을 선택합니다.

   e. 인스턴스 메타데이터 옵션 수정 대화 상자에서 다음을 선택합니다.

      - *인스턴스 메타데이터 서비스*에 대해 *활성화*를 선택합니다.
      - *IMDSv2*의 경우 *필수*를 선택하세요.
      - *저장*을 선택하세요.

   f. HA 중재자를 포함한 다른 Cloud Volumes ONTAP 인스턴스에 대해 이 단계를 반복합니다.

   g. "Cloud Volumes ONTAP 인스턴스를 중지하고 시작합니다."

결과

콘솔 에이전트 인스턴스와 Cloud Volumes ONTAP 인스턴스는 이제 IMDSv2를 사용하도록 구성되었습니다.

콘솔 에이전트의 기본 구성

AWS, Azure, Google Cloud에서 인터넷 접속이 가능한 표준 배포에 대한 콘솔 에이전트 기본 구성과 온프레미스 환경에서 인터넷 접속이 불가능한 제한된 배포에 대한 콘솔 에이전트 기본 구성에 대해 알아보세요.

인터넷 접속이 가능한 기본 구성

다음 구성 세부 정보는 NetApp Console, 클라우드 공급업체의 마켓플레이스에서 콘솔 에이전트를 배포한 경우 또는 인터넷 액세스가 가능한 온프레미스 Linux 호스트에 콘솔 에이전트를 수동으로 설치한 경우에 적용됩니다.

AWS용 콘솔 에이전트 **VM** 세부 정보

콘솔이나 클라우드 공급자의 마켓플레이스에서 콘솔 에이전트를 배포한 경우 다음 사항에 유의하세요.

- EC2 인스턴스 유형은 t3.2xlarge입니다.
- 이미지의 운영 체제는 Ubuntu 22.04 LTS입니다.

  운영 체제에는 GUI가 포함되어 있지 않습니다. 시스템에 접근하려면 터미널을 사용해야 합니다.

- 설치에는 컨테이너 오케스트레이션 도구인 Docker Engine이 포함되어 있습니다.
- EC2 Linux 인스턴스의 사용자 이름은 ubuntu입니다(2023년 5월 이전에 생성된 에이전트의 경우 사용자 이름은 ec2-user입니다).
- 기본 시스템 디스크는 100GiB gp2 디스크입니다.

Azure용 콘솔 에이전트 **VM** 세부 정보

콘솔이나 클라우드 공급자의 마켓플레이스에서 콘솔 에이전트를 배포한 경우 다음 사항에 유의하세요.

- VM 유형은 Standard_D8s_v3입니다.
- 이미지의 운영 체제는 Ubuntu 22.04 LTS입니다.

  운영 체제에는 GUI가 포함되어 있지 않습니다. 시스템에 접근하려면 터미널을 사용해야 합니다.

- 설치에는 컨테이너 오케스트레이션 도구인 Docker Engine이 포함되어 있습니다.
- 기본 시스템 디스크는 100GiB 프리미엄 SSD 디스크입니다.

Google Cloud용 콘솔 에이전트 **VM** 세부 정보

콘솔에서 콘솔 에이전트를 배포한 경우 다음 사항에 유의하세요.

- VM 인스턴스는 n2-standard-8입니다.
- 이미지의 운영 체제는 Ubuntu 22.04 LTS입니다.

  운영 체제에는 GUI가 포함되어 있지 않습니다. 시스템에 접근하려면 터미널을 사용해야 합니다.

- 설치에는 컨테이너 오케스트레이션 도구인 Docker Engine이 포함되어 있습니다.
- 기본 시스템 디스크는 100GiB SSD 영구 디스크입니다.

설치 폴더

에이전트 설치 폴더는 다음 위치에 있습니다.

`/opt/application/netapp/cloudmanager`

로그 파일

로그 파일은 다음 폴더에 있습니다.

- `/opt/application/netapp/cloudmanager/log` 또는
- `/opt/application/netapp/service-manager-2/logs` (새로운 3.9.23 설치부터)

  이러한 폴더의 로그는 콘솔 에이전트에 대한 세부 정보를 제공합니다.

- `/opt/application/netapp/cloudmanager/docker_occm/data/log`

  이 폴더의 로그는 클라우드 서비스와 콘솔 에이전트에서 실행되는 콘솔 서비스에 대한 세부 정보를 제공합니다.

콘솔 에이전트 서비스

- 콘솔 에이전트 서비스의 이름은 occm입니다.
- occm 서비스는 MySQL 서비스에 종속됩니다.

  MySQL 서비스가 중단되면 occm 서비스도 중단됩니다.

포트

에이전트는 Linux 호스트에서 다음 포트를 사용합니다.

- HTTP 접근을 위한 80
- HTTPS 액세스를 위한 443

인터넷 접속이 없는 기본 구성

인터넷 접속이 불가능한 온프레미스 Linux 호스트에 콘솔 에이전트를 수동으로 설치한 경우 다음 구성이 적용됩니다. "이 설치 옵션에 대해 자세히 알아보세요" .

- 에이전트 설치 폴더는 다음 위치에 있습니다.

  `/opt/application/netapp/ds`

- 로그 파일은 다음 폴더에 있습니다.

  `/var/lib/docker/volumes/ds_occmdata/_data/log`

이 폴더의 로그는 콘솔 에이전트와 Docker 이미지에 대한 세부 정보를 제공합니다.

- 모든 서비스는 Docker 컨테이너 내부에서 실행됩니다.

  서비스는 실행 중인 Docker 런타임 서비스에 따라 달라집니다.

- 에이전트는 Linux 호스트에서 다음 포트를 사용합니다.
  - HTTP 접근을 위한 80
  - HTTPS 액세스를 위한 443

저작권 정보

상표 정보