



참조하십시오 Set up and administration

NetApp
July 17, 2022

목차

참조하십시오	1
Cloud Manager에 대한 권한 요약	1
Connector에 대한 AWS 권한	2
Connector에 대한 Azure 권한	25
Connector에 대한 Google Cloud 권한	33

참조하십시오

Cloud Manager에 대한 권한 요약

Cloud Manager에서 기능과 서비스를 사용하려면 Cloud Manager가 클라우드 환경에서 작업을 수행할 수 있도록 권한을 제공해야 합니다. 이 페이지의 링크를 사용하여 목표에 따라 필요한 사용 권한에 빠르게 액세스할 수 있습니다.

AWS 권한

목적	설명	링크
커넥터 전개	Cloud Manager에서 Connector를 생성하는 사용자는 AWS에 인스턴스를 구축하기 위한 특정 권한이 필요합니다.	"Cloud Manager에서 AWS에 Connector를 생성합니다"
커넥터 작동	Cloud Manager에서 Connector를 시작하면 인스턴스에 정책이 연결되며, 이 정책은 AWS 계정의 리소스와 프로세스를 관리하는 데 필요한 권한을 제공합니다. 정책을 직접 설정해야 합니다 "마켓플레이스에서 Connector를 실행합니다" 아니면 "Connector에 AWS 자격 증명을 더 추가합니다" . 또한 새 권한이 후속 릴리스에 추가될 때 정책이 최신 상태인지 확인해야 합니다.	"Connector에 대한 AWS 권한"
Cloud Volumes ONTAP 작동	IAM 역할은 AWS의 각 Cloud Volumes ONTAP 노드에 연결되어야 합니다. HA 중재자의 경우도 마찬가지입니다. 기본 옵션은 Cloud Manager에서 IAM 역할을 생성할 수 있도록 하는 것이지만 직접 사용할 수 있습니다.	"IAM 역할을 직접 설정하는 방법에 대해 알아봅니다"

Azure 권한

목적	설명	링크
커넥터 전개	Cloud Manager에서 Connector를 배포하는 경우 Azure에 Connector VM을 배포할 수 있는 권한이 있는 Azure 계정 또는 서비스 보안 주체를 사용해야 합니다.	"Cloud Manager에서 Azure에 Connector를 생성합니다"
커넥터 작동	Cloud Manager는 Azure에서 Connector VM을 배포할 때 Azure 구독 내에서 리소스와 프로세스를 관리하는 데 필요한 권한을 제공하는 사용자 지정 역할을 생성합니다. 사용자 지정 역할을 직접 설정해야 합니다 "마켓플레이스에서 Connector를 실행합니다" 아니면 "Connector에 Azure 자격 증명을 더 추가합니다" . 또한 새 권한이 후속 릴리스에 추가될 때 정책이 최신 상태인지 확인해야 합니다.	"Connector에 대한 Azure 권한"

Google Cloud 권한

목적	설명	링크
커넥터 전개	Cloud Manager에서 Connector를 배포하는 Google Cloud 사용자는 Google Cloud에서 Connector를 배포하기 위한 특정 권한이 필요합니다.	"Connector 배포 권한을 설정합니다"
커넥터 작동	Connector VM 인스턴스의 서비스 계정에는 일상적인 작업에 대한 특정 권한이 있어야 합니다. Cloud Manager에서 서비스 계정을 배포할 때 Connector에 서비스 계정을 연결해야 합니다. 또한 새 권한이 후속 릴리스에 추가될 때 정책이 최신 상태인지 확인해야 합니다.	"Connector에 대한 서비스 계정을 설정합니다"

Connector에 대한 AWS 권한

Cloud Manager가 AWS에서 Connector 인스턴스를 시작하면 해당 AWS 계정 내의 리소스와 프로세스를 관리할 수 있는 권한을 Connector에 제공하는 인스턴스에 정책을 연결합니다. Connector는 권한을 사용하여 EC2, S3, CloudFormation, IAM, KMS(키 관리 서비스) 등

IAM 정책

아래에 표시된 IAM 정책은 Connector가 AWS 지역에 따라 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하는데 필요한 권한을 제공합니다.

Cloud Manager에서 직접 Connector를 생성하면 Cloud Manager가 이 정책을 Connector에 자동으로 적용합니다.

AWS Marketplace에서 Connector를 배포하거나 Linux 호스트에 Connector를 수동으로 설치하는 경우 정책을 직접 설정해야 합니다.

또한 새 권한이 후속 릴리스에 추가될 때 정책이 최신 상태인지 확인해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cvoServicePolicy",
      "Effect": "Allow",
      "Action": [
        "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",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
```

```
"iam:CreateInstanceProfile",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam:ListInstanceProfiles",
"sts:DecodeAuthorizationMessage",
"ec2:AssociateIamInstanceProfile",
"ec2:DescribeIamInstanceProfileAssociations",
"ec2:DisassociateIamInstanceProfile",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3:CreateBucket",
"s3:GetLifecycleConfiguration",
"s3:ListBucketVersions",
"s3:GetBucketPolicyStatus",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketPolicy",
"s3:GetBucketAcl",
"kms:List*",
"kms:ReEncrypt*",
"kms:Describe*",
"kms:CreateGrant",
"ce:GetReservationUtilization",
"ce:GetDimensionValues",
"ce:GetCostAndUsage",
"ce:GetTags",
"ec2:CreatePlacementGroup",
"ec2:DescribeReservedInstancesOfferings",
"sts:AssumeRole",
"ec2:AssignPrivateIpAddresses",
"ec2:CreateRoute",
"ec2:DescribeVpcs",
"ec2:ReplaceRoute",
"ec2:UnassignPrivateIpAddresses",
"s3:PutObjectTagging",
"s3:GetObjectTagging",
"fsx:Describe*",
"fsx:List*",
"ec2:DeleteSecurityGroup",
"ec2:DeleteNetworkInterface",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteRoute",
"ec2:DeletePlacementGroup",
"iam:DeleteRole",
"iam:DeleteRolePolicy",
```

```

        "iam:DeleteInstanceProfile",
        "cloudformation:DeleteStack",
        "ec2:DescribePlacementGroups",
        "iam:GetRolePolicy",
        "s3:ListAllMyBuckets",
        "s3:GetObject",
        "iam:GetRole",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutObject",
        "ec2:ModifyVolume",
        "ec2:DescribeVolumesModifications"
    ],
    "Resource": "*"
},
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "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",
        "kms:List*",
        "kms:Describe*",
        "ec2:describeVpcEndpoints",
        "kms:ListAliases",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "athena:StopQueryExecution",
        "glue:CreateDatabase",
        "glue:CreateTable",
    ]
}

```

```

        "glue:BatchDeletePartition"
    ],
    "Resource": "*"
},
{
    "Sid": "backupS3Policy",
    "Effect": "Allow",
    "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"
    ],
    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
},
{
    "Sid": "tagServicePolicy",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
    ],

```



```

    "Resource": "*"
  },
  {
    "Sid": "fabricPoolS3Policy",
    "Effect": "Allow",
    "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*"
    ]
  },
  {
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeRegions"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances"
    ],
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/netapp-adc-manager": "*"
      }
    },
    "Resource": [
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
},

```

```

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

```

```

    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/WorkingEnvironment": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid": "K8sServicePolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "iam:ListInstanceProfiles",
        "eks:ListClusters",
        "eks:DescribeCluster"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GFCservicePolicy",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudwatch:GetMetricStatistics",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    }
  ]
}

```

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:List*",
        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "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/*"
    ]
}
]
}

```

C2S 환경

```

{
    "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",
        "kms:List*",
        "kms:Describe*",
        "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 사용 권한

다음 섹션에서는 각 NetApp 클라우드 서비스에 대한 사용 권한을 어떻게 사용하는지 설명합니다. 이 정보는 기업 정책에 따라 사용 권한이 필요한 경우에만 제공된다는 내용이 지정되어 있는 경우에 유용합니다.

AppTemplate 태그

Connector는 AppTemplate Tagging 서비스를 사용할 때 AWS 리소스의 태그 관리를 위해 다음과 같은 API 요청을 수행합니다.

- EC2: CreateTags(태그 생성)
- EC2: 삭제 태그
- EC2: DescribeTags(설명 태그)
- 태그: getResources
- 태그: getTagKeys
- 태그: getTagValues
- 태그: 태그 리소스
- 태그: UntagResources

클라우드 백업

Connector는 다음과 같은 API 요청을 통해 Cloud Backup의 복원 인스턴스를 구축합니다.

- EC2: StartInstances(시작 인스턴스)
- EC2: StopInstances(중지 인스턴스)
- EC2: DescribeInstances(지시 인스턴스)
- EC2: DescribeInstanceStatus
- EC2: 런인스턴스
- EC2: 터미네이스
- EC2: DescribeInstanceAttribute
- EC2: DescribeImages(설명 영상)
- EC2: CreateTags(태그 생성)
- EC2: CreateVolume
- EC2:CreateSecurityGroup입니다
- EC2: DescribeSubnet
- EC2: 설명
- EC2: 설명
- CloudFormation:CreateStack
- CloudFormation:DeleteStack
- CloudFormation: DescribeStacks

Connector는 Amazon S3에서 백업을 관리하기 위해 다음과 같은 API 요청을 수행합니다.

- S3:GetBucketLocation
- S3:ListAllMyBucket
- S3:목록 버킷
- S3:생성 버킷
- S3:GetLifecycleConfiguration

- S3: PutLifecycleConfiguration
- S3: PutBucketTagging
- S3:목록 BucketVersions
- S3:GetBucketAcl
- S3: PutBucketPublicAccessBlock
- KMS: 목록 *
- KMS: 설명 *
- S3:GetObject
- EC2: describeVpcEndpoints입니다
- KMS: ListAliases
- S3:PutEncryptionConfiguration

Connector는 검색 및 복원 방법을 사용하여 볼륨 및 파일을 복원할 때 다음과 같은 API 요청을 수행합니다.

- S3:생성 버킷
- S3:DeleteObject 를 선택합니다
- S3:DeleteObjectVersion
- S3:GetBucketAcl
- S3:목록 버킷
- S3:목록 BucketVersions
- S3:ListBucketMultipartUploads
- S3:PutObject
- S3: PutBucketAcl
- S3: PutLifecycleConfiguration
- S3: PutBucketPublicAccessBlock
- S3:중단멀티업로드입니다
- S3:ListMultipartUploadParts(S3:ListMultipartUploadParts) 를
- Athena:StartQueryExecution
- Athena:GetQueryResults
- Athena:GetQueryExecution을 참조하십시오
- Athena: StopQueryExecution
- 글루:CreateDatabase
- 글루:CreateTable
- GLUE:BatchDeletePartition

클라우드 데이터 감지

Connector는 Cloud Data Sense 인스턴스를 구축하기 위해 다음과 같은 API 요청을 수행합니다.

- EC2: DescribeInstances(지시 인스턴스)
- EC2: DescribeInstanceStatus
- EC2: 런인스턴스
- EC2: 터미네이스
- EC2: CreateTags(태그 생성)
- EC2: CreateVolume
- EC2: AttachVolume
- EC2:CreateSecurityGroup입니다
- EC2: DeleteSecurityGroup
- EC2: DescribeSecurityGroups
- EC2: CreateNetworkInterface입니다
- EC2: DescribeNetworkInterfaces를 참조하십시오
- EC2: DeleteNetworkInterface
- EC2: DescribeSubnet
- EC2: 설명
- EC2: 스냅샷을 만듭니다
- EC2: 설명
- CloudFormation:CreateStack
- CloudFormation:DeleteStack
- CloudFormation: DescribeStacks
- CloudFormation: DescribeStackEvents
- IAM:AddRoleToInstanceProfile 을 참조하십시오
- EC2: AssociateIamInstanceProfile 을 참조하십시오
- EC2: DescribeIamInstanceProfileAssociations

Connector는 Cloud Data Sense를 사용할 때 S3 버킷을 스캔하기 위해 다음과 같은 API 요청을 수행합니다.

- IAM:AddRoleToInstanceProfile 을 참조하십시오
- EC2: AssociateIamInstanceProfile 을 참조하십시오
- EC2: DescribeIamInstanceProfileAssociations
- S3:GetBucketTagging
- S3:GetBucketLocation
- S3:ListAllMyBucket
- S3:목록 버킷
- S3:GetBucketPolicyStatus를 참조하십시오
- S3:GetBucketPolicy를 참조하십시오
- S3:GetBucketAcl

- S3:GetObject
- IAM:GetRole
- S3:DeleteObject 를 선택합니다
- S3:DeleteObjectVersion
- S3:PutObject
- STS:AssumeRole

클라우드 계층화

Connector는 Cloud Tiering을 사용할 때 Amazon S3에 데이터를 계층화하도록 다음과 같은 API 요청을 수행합니다.

조치	설정에 사용됩니까?	일상적 운영에 사용됩니까?
S3:생성 버킷	예	아니요
S3: PutLifecycleConfiguration	예	아니요
S3:GetLifecycleConfiguration	예	예
EC2: 설명	예	예

Cloud Volumes ONTAP

Connector는 AWS에서 Cloud Volumes ONTAP를 구축 및 관리하기 위해 다음과 같은 API 요청을 수행합니다.

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
Cloud Volumes ONTAP 인스턴스에 대한 IAM 역할 및 인스턴스 프로필을 생성하고 관리합니다	IAM: ListInstanceProfiles(인스턴스 프로필)	예	예	아니요
	IAM: CreateRole	예	아니요	아니요
	IAM: DeleteRole	아니요	예	예
	IAM: PutRolePolicy(입수 정책)	예	아니요	아니요
	IAM:CreateInstance Profile	예	아니요	아니요
	IAM: DeleteRolePolicy(삭 제 RolePolicy	아니요	예	예
	IAM:AddRoleToInsta nceProfile 을 참조하십시오	예	아니요	아니요
	IAM:RemoveRoleFro mInstanceProfile 을 참조하십시오	아니요	예	예
	IAM: DeleteInstanceProfil e	아니요	예	예
	IAM: 암호 역할	예	아니요	아니요
	EC2: AssociateIamInstanc eProfile 을 참조하십시오	예	예	아니요
	EC2: DescribeIamInstanc eProfileAssociations	예	예	아니요
	EC2: DiscassociateIamIns tanceProfile 을 참조하십시오	아니요	예	아니요
인증 상태 메시지를 디코딩합니다	STS:DecodeAuthoriz ationMessage 를 참조하십시오	예	예	아니요
계정에 사용할 수 있는 지정된 영상(AMI)을 설명합니다	EC2: DescribeImages(설 명 영상)	예	예	아니요
VPC의 라우트 테이블 설명(HA 쌍에만 필요)	EC2: 설명표	예	아니요	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
인스턴스를 중지, 시작 및 모니터링합니다	EC2: StartInstances(시작 인스턴스)	예	예	아니요
	EC2: StopInstances(중지 인스턴스)	예	예	아니요
	EC2: DescribeInstances(지시 인스턴스)	예	예	아니요
	EC2: DescribeInstanceStatus	예	예	아니요
	EC2: 런인스턴스	예	아니요	아니요
	EC2: 터미네이션	아니요	아니요	예
	EC2: ModifyInstanceAttribute	아니요	예	아니요
지원되는 인스턴스 유형에 대해 향상된 네트워킹이 활성화되어 있는지 확인합니다	EC2: DescribeInstanceAttribute	아니요	예	아니요
유지 관리 및 비용 할당에 사용되는 "WorkingEnvironment" 및 "WorkingEnvironmentId" 태그로 리소스에 태그를 지정합니다	EC2: CreateTags(태그 생성)	예	예	아니요
Cloud Volumes ONTAP가 백엔드 스토리지로 사용하는 EBS 볼륨을 관리합니다	EC2: CreateVolume	예	예	아니요
	EC2: 설명 볼륨을 참조하십시오	예	예	예
	EC2: ModifyVolumeAttribute	아니요	예	예
	EC2: AttachVolume	예	예	아니요
	EC2: DeleteVolume(삭제 볼륨)	아니요	예	예
	EC2: DetachVolume(분리 볼륨)	아니요	예	예

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
Cloud Volumes ONTAP에 대한 보안 그룹을 만들고 관리합니다	EC2:CreateSecurity Group입니다	예	아니요	아니요
	EC2: DeleteSecurityGroup	아니요	예	예
	EC2: DescribeSecurityGro ups	예	예	예
	EC2: RevokeSecurityGrou pEgress	예	아니요	아니요
	EC2: AuthorizeSecurityGr oupEgress 를 참조하십시오	예	아니요	아니요
	EC2: AuthorizeSecurityGr oupIngress 를 참조하십시오	예	아니요	아니요
	EC2: RevokeSecurityGrou pIngress 를 참조하십시오	예	예	아니요
대상 서브넷에서 Cloud Volumes ONTAP에 대한 네트워크 인터페이스를 생성하고 관리합니다	EC2: CreateNetworkInterf ace입니다	예	아니요	아니요
	EC2: DescribeNetworkInte rfaces를 참조하십시오	예	예	아니요
	EC2: DeleteNetworkInterf ace	아니요	예	예
	EC2: ModifyNetworkInterf aceAttribute 입니다	아니요	예	아니요
대상 서브넷 및 보안 그룹 목록을 가져옵니다	EC2: DescribeSubnet	예	예	아니요
	EC2: 설명	예	예	아니요
Cloud Volumes ONTAP 인스턴스의 DNS 서버와 기본 도메인 이름을 가져옵니다	EC2: DescribeDhcpOption s	예	아니요	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
Cloud Volumes ONTAP용 EBS 볼륨의 스냅샷을 생성합니다	EC2: 스냅샷을 만듭니다	예	예	아니요
	EC2: DeleteSnapshot	아니요	예	예
	EC2: 설명	아니요	예	아니요
AutoSupport 메시지에 첨부된 Cloud Volumes ONTAP 콘솔을 캡처합니다	EC2:GetConsoleOutput 을 참조하십시오	예	예	아니요
사용 가능한 키 쌍 목록을 가져옵니다	EC2: 설명	예	아니요	아니요
사용 가능한 AWS 지역 목록을 확인하십시오	EC2: 설명	예	예	아니요
Cloud Volumes ONTAP 인스턴스와 연결된 리소스의 태그를 관리합니다	EC2: 삭제 태그	아니요	예	예
	EC2: DescribeTags(설명 태그)	아니요	예	아니요
AWS CloudFormation 템플릿을 위한 스택을 만들고 관리합니다	CloudFormation:CreateStack	예	아니요	아니요
	CloudFormation:DeleteStack	예	아니요	아니요
	CloudFormation:DescribeStacks	예	예	아니요
	CloudFormation:DescribeStackEvents	예	아니요	아니요
	CloudFormation:ValidateTemplate 을 참조하십시오	예	아니요	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
Cloud Volumes ONTAP 시스템이 데이터 계층화를 위한 용량 계층으로 사용하는 S3 버킷을 생성 및 관리합니다	S3:생성 버킷	예	예	아니요
	S3:삭제 버킷	아니요	예	예
	S3:GetLifecycleConf iguration	아니요	예	아니요
	S3: PutLifecycleConfigur ation	아니요	예	아니요
	S3: PutBucketTagging	아니요	예	아니요
	S3:목록 BucketVersions	아니요	예	아니요
	S3:GetBuckketPolicy Status를 참조하십시오	아니요	예	아니요
	S3:GetBuckketPubli cAccessBlock	아니요	예	아니요
	S3:GetBuckketAcl	아니요	예	아니요
	S3:GetBuckketPolicy 를 참조하십시오	아니요	예	아니요
	S3: PutBucketPublicAcc essBlock	아니요	예	아니요
	S3:GetBucketTaggin g	아니요	예	아니요
	S3:GetBucketLocati on	아니요	예	아니요
	S3:ListAllMyBucket	아니요	아니요	아니요
	S3:목록 버킷	아니요	예	아니요
AWS KMS(키 관리 서비스)를 사용하여 Cloud Volumes ONTAP의 데이터 암호화 지원	KMS: 목록 *	예	예	아니요
	KMS: 재암호화 *	예	아니요	아니요
	KMS: 설명 *	예	예	아니요
	KMS: CreateGrant	예	예	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
Cloud Volumes ONTAP의 AWS 비용 데이터 확보	CE:GetReservationUtilization을 참조하십시오	아니요	예	아니요
	CE:GetDimensionValues	아니요	예	아니요
	CE:GetCostAndUsage	아니요	예	아니요
	CE:GetTags	아니요	예	아니요
단일 AWS Availability Zone에서 2개의 HA 노드를 위한 AWS 분산 배치 그룹과 종재자를 생성하고 관리합니다	EC2: CreatePlacementGroup(배치 그룹 생성)	예	아니요	아니요
	EC2: DeletePlacementGroup	아니요	예	예
보고서 작성	FSX: 설명 *	아니요	예	아니요
	FSX: 목록 *	아니요	예	아니요
Amazon EBS Elastic Volumes 기능을 지원하는 애그리게이트를 생성 및 관리합니다	EC2: 볼륨 수정 설명	아니요	예	아니요
	EC2: ModifyVolume(수정 볼륨)	아니요	예	아니요

글로벌 파일 캐시

Connector는 배포 중에 다음과 같은 API 요청을 통해 글로벌 파일 캐시 인스턴스를 구축합니다.

- CloudFormation: DescribeStacks
- CloudWatch: GetMetricStatistics
- CloudFormation: ListStacks

쿠버네티스

Connector는 다음과 같은 API 요청을 수행하여 Amazon EKS 클러스터를 검색하고 관리합니다.

- EC2: 설명
- EKS: ListClusters
- EKS: DescribeCluster
- IAM:GetInstanceProfile 을 참조하십시오

Connector에 대한 Azure 권한

Cloud Manager가 Azure에서 Connector VM을 시작하면 해당 Azure 구독 내에서 리소스와

프로세스를 관리할 수 있는 권한을 Connector에 제공하는 VM에 사용자 지정 역할을 연결합니다. Connector는 사용 권한을 사용하여 여러 Azure 서비스에 대한 API 호출을 수행합니다.

사용자 지정 역할 권한

아래 표시된 사용자 지정 역할은 Connector가 Azure 네트워크 내의 리소스 및 프로세스를 관리하는 데 필요한 권한을 제공합니다.

Cloud Manager에서 직접 Connector를 만들면 Cloud Manager가 자동으로 이 사용자 지정 역할을 Connector에 적용합니다.

Azure Marketplace에서 Connector를 배포하거나 Linux 호스트에 Connector를 수동으로 설치하는 경우 사용자 지정 역할을 직접 설정해야 합니다.

또한 후속 릴리스에 새 권한이 추가되므로 역할이 최신 상태인지 확인해야 합니다.

```
{
  "Name": "Cloud Manager 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/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/regeneratekey/action",
"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"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/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/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/frontendIPConfigurations/read",

"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/action",

"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.Network/loadBalancers/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"
    ],
    "NotActions": [],
    "AssignableScopes": [],

```

```

    "Description": "Cloud Manager Permissions",
    "IsCustom": "true"
  }

```

Azure 사용 권한 사용 방법

작업	목적
"Microsoft.Compute/locations/operations/read", "Microsoft.Compute/locations/vmSizes/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/start/action", "Microsoft.Compute/virtualMachines/deallocate/action", "Microsoft.Compute/virtualMachines/vmSizes/read", "Microsoft.Compute/virtualMachines/write",	Cloud Volumes ONTAP를 생성하고 시스템 상태를 중지, 시작, 삭제 및 가져옵니다.
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	VHD에서 Cloud Volumes ONTAP 배포를 활성화합니다.
"Microsoft.Compute/disks/delete", "Microsoft.Compute/disks/read", "Microsoft.Compute/disks/write", "Microsoft.Storage/checknameAvailability/read", "Microsoft.Storage/operations/read", "Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/storageAccounts/read", "Microsoft.Storage/storageAccounts/REV/ACTION", "Microsoft.Storage/storageAccounts/write", "Microsoft.Storage/storageAccounts/delete", "Microsoft.Storage/en사용법/read",	Azure 스토리지 계정 및 디스크를 관리하고 디스크를 Cloud Volumes ONTAP에 연결합니다.
"Microsoft.Storage/storageAccounts/blobServices/containers/read", "Microsoft.KeyVault/vaults/read", "Microsoft.KeyVault/vaults/accessPolicies/write"	Azure Blob 저장소에 백업 및 스토리지 계정 암호화를 지원합니다.
"Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write", "Microsoft.Network/networkInterfaces/join/action",	대상 서버넷에서 Cloud Volumes ONTAP에 대한 네트워크 인터페이스를 생성하고 관리합니다.
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/join/action",	Cloud Volumes ONTAP에 대해 미리 정의된 네트워크 보안 그룹을 생성합니다.

작업	목적
"Microsoft.Resources/Subscriptions/locations/read", "Microsoft.Network/locations/operationResults/read", "Microsoft.Network/locations/operations/read", "Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", "Microsoft.Network/virtualNetworks/virtualMachines/read", "Microsoft.Network/virtualNetworks/subnets/join/action",	지역, 대상 VNET 및 서브넷에 대한 네트워크 정보를 가져오고 Cloud Volumes ONTAP를 VNets에 추가합니다.
"Microsoft.Network/virtualNetworks/subnets/write", "Microsoft.Network/routeTables/join/action",	데이터 계층화를 위한 VNET 서비스 엔드포인트를 활성화합니다.
"Microsoft.Resources/Deployments/operations/read", "Microsoft.Resources/Deployments/read", "Microsoft.Resources/Deployments/Write",	템플릿에서 Cloud Volumes ONTAP를 배포합니다.
"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/resourceGroups/read", "Microsoft.Resources/Subscriptions/resourceGroups/write",	Cloud Volumes ONTAP에 대한 리소스 그룹을 생성하고 관리합니다.
"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/snapshots/delete", "Microsoft.Compute/disks/beginGetAccess/action",	Azure 관리 스냅샷을 생성하고 관리합니다.
"Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read",	Cloud Volumes ONTAP의 가용성 세트를 생성하고 관리합니다.
"Microsoft.MarketplaceOrdering/offerstypes/publishers/Offers/Plans/Agreement/read", "Microsoft.MarketplaceOrdering/offerstypes/publisherTypes/publishers/Offers/Plans/Agreement/write",	Azure Marketplace에서 프로그래밍 방식으로 배포할 수 있습니다.

작업	목적
"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/frontendIPConfigurations/read", "Microsoft.Network/loadBalancers/loadBalancingRules/read", "Microsoft.Network/loadBalancers/probes/read", "Microsoft.Network/loadBalancers/probes/join/action",	HA 쌍에 대한 Azure 로드 밸런서를 관리합니다.
"Microsoft.Authorization/lock/ **",	Azure 디스크의 잠금 관리를 활성화합니다.
"Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/sites/ **"	HA 쌍의 페일오버 관리
"Microsoft.Network/privateEndpoints/write", "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action", "Microsoft.Storage/storageAccounts/privateEndpointConnections/read", "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",	전용 엔드포인트를 관리할 수 있습니다. 전용 엔드포인트는 서브넷 외부에 접속이 제공되지 않을 때 사용됩니다. Cloud Manager는 서브넷 내에서 내부 연결만 제공하는 HA용 스토리지 계정을 생성합니다.
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",	Cloud Manager에서 Azure NetApp Files의 볼륨을 삭제할 수 있습니다.
"Microsoft.Resources/Deployments/operationStates/read"	Azure에서는 일부 가상 시스템 배포에 대해 이 권한이 필요합니다(배포 중에 사용되는 기본 물리적 하드웨어에 따라 다름).
"Microsoft.Resources/Deployments/operationStates/read", "Microsoft.Insights/Metrics/Read", "Microsoft.Compute/virtualMachines/extensions/write", "Microsoft.Compute/virtualMachines/extensions/read", "Microsoft.Compute/virtualMachines/extensions/delete", "Microsoft.Compute/virtualMachines/delete", "Microsoft.Network/networkInterfaces/delete", "Microsoft.Network/networkSecurityGroups/delete", "Microsoft.Resources/Deployments/delete",	글로벌 파일 캐시를 사용할 수 있습니다.
"Microsoft.Network/privateEndpoints/delete", "Microsoft.Compute/availabilitySets/delete",	Cloud Manager에서 배포 실패 또는 삭제 시 Cloud Volumes ONTAP에 속한 리소스 그룹에서 리소스를 제거할 수 있습니다.

작업	목적
"Microsoft.Compute/diskEncryptionSets/read" "Microsoft.Compute/diskEncryptionSets/write", "Microsoft.Compute/diskEncryptionSets/delete" "Microsoft.KeyVault/vaults/deploy/action", "Microsoft.KeyVault/vaults/waults/read", "Microsoft.KeyVault/vaults/accessPolicies/write",	Cloud Volumes ONTAP에서 고객이 관리하는 암호화 키를 사용할 수 있습니다. 이 기능은 API를 사용하여 지원됩니다.
"Microsoft.Resources/tags/read", "Microsoft.Resources/tags/write", "Microsoft.Resources/tags/delete"	Cloud Manager 태그 지정 서비스를 사용하여 Azure 리소스의 태그를 관리할 수 있습니다.
"Microsoft.Network/applicationSecurityGroups/write", "Microsoft.Network/applicationSecurityGroups/read", "Microsoft.Network/applicationSecurityGroups/joinIpC onfiguration/action", "Microsoft.Network/networkSecurityGroups/securityRu les/write","Microsoft.Network/applicationSecurityGrou ps/delete", "Microsoft.Network/networkSecurityGroups/securityRu les/delete" 참조하십시오	Cloud Manager에서 HA 인터커넥트 및 클러스터 네트워크 NIC를 격리하는 HA 쌍에 대한 애플리케이션 보안 그룹을 구성할 수 있습니다.

Connector에 대한 Google Cloud 권한

Cloud Manager를 사용하려면 Google Cloud에서 작업을 수행할 수 있는 권한이 필요합니다. 이러한 사용 권한은 NetApp에서 제공하는 사용자 지정 역할에 포함됩니다. Cloud Manager가 이러한 사용 권한을 통해 수행하는 작업을 이해하기를 원할 수 있습니다.

서비스 계정 권한

아래 표시된 사용자 지정 역할은 Connector가 Google Cloud 네트워크 내의 리소스 및 프로세스를 관리하는 데 필요한 권한을 제공합니다.

Connector VM에 연결되는 서비스 계정에 이 사용자 지정 역할을 적용해야 합니다. ["단계별 지침을 봅니다"](#).

또한 후속 릴리스에 새 권한이 추가되므로 역할이 최신 상태인지 확인해야 합니다.

```
title: NetApp Cloud Manager
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
```

- `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.globalOperations.get`
- `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.machineTypes.get`
- `compute.networks.get`
- `compute.networks.list`
- `compute.projects.get`
- `compute.regions.get`
- `compute.regions.list`
- `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
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy

Google Cloud 사용 권한 사용 방법

작업	목적
-compute.disks.create-compute.disks.createSnapshot -compute.disks.delete -compute.disks.get -compute.disks.list -compute.disks.setLabels -compute.disks.us e	Cloud Volumes ONTAP용 디스크를 생성하고 관리합니다.
-compute.w방화벽.create-compute.firewalls.delete- compute.w방화벽.get-compute.w방화벽.list를 참조하십시오	Cloud Volumes ONTAP에 대한 방화벽 규칙을 만듭니다.
-compute.globalOperations.get	작업 상태를 확인합니다.
-compute.images.get-compute.images.getFromFamily -compute.images.list-compute.images.useReadOnly 를 참조하십시오	VM 인스턴스의 이미지를 가져옵니다.
compute.instances.attachDisk - compute.instances.detachDisk 으로 문의하십시오	Cloud Volumes ONTAP에 디스크를 연결 및 분리합니다.
compute.instances.create - compute.instances.delete 으로 문의하십시오	Cloud Volumes ONTAP VM 인스턴스를 생성 및 삭제합니다.
compute.instances.get 으로 문의하십시오	VM 인스턴스를 나열합니다.
compute.instances.getSerialPortOutput 으로 문의하십시오	콘솔 로그를 가져옵니다.
compute.instances.list 으로 문의하십시오	영역에 있는 인스턴스 목록을 검색합니다.
compute.instances.setDeletionProtection 으로 문의하십시오	인스턴스에 대한 삭제 보호를 설정합니다.
compute.instances.setLabels 으로 문의하십시오	를 눌러 라벨을 추가합니다.
compute.instances.setMachineType - compute.instances.setMinCpuPlatform 으로 문의하십시오	Cloud Volumes ONTAP의 기계 유형을 변경합니다.
compute.instances.setMetadata 으로 문의하십시오	를 눌러 메타데이터를 추가합니다.
compute.instances.setTags 으로 문의하십시오	방화벽 규칙에 대한 태그를 추가하려면
compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Cloud Volumes ONTAP를 시작 및 중지합니다.
-compute.machineTypes.get	를 클릭하여 qoutas를 확인하십시오.
compute.projects.get 으로 문의하십시오	여러 프로젝트를 지원합니다.
-compute.snapshots.create-compute.snapshots.delete -compute.snapshots.get-compute.snapshots.list -compute.snapshots.setLabels 를 참조하십시오	영구 디스크 스냅샷을 생성하고 관리합니다.
-compute.networks.get -compute.networks.list -compute.regions.get-compute.regions.list -compute.subnetworks.get-compute.subnetworks.list -compute.zoneOperations.get-compute.zones.get -compute.zones.list 를 참조하십시오	새 Cloud Volumes ONTAP 가상 머신 인스턴스를 생성하는 데 필요한 네트워킹 정보를 가져옵니다.

작업	목적
deploymentmanager.compositeTypes.get -deploymentmanager.compositeTypes.list -deploymentmanager.deployments.create -deploymentmanager.deployments.delete -deploymentmanager.deployments.get -deploymentmanager.deployments.list deploymentmanager.manifests.get deploymentmanager.manager.manifests.list.deploymentmanager.operations.get deploymentmanager.resources.get deploymentmanager.resources.list.list.deploymentmanager.deploymentmanager.deploymentmanager.deploymentmanager.type.deploymentmanager.deploymentmanager.deploymentmanager.type.get.type.get	Google Cloud Deployment Manager를 사용하여 Cloud Volumes ONTAP 가상 머신 인스턴스를 구축합니다.
logging.logEntrys.list-logging.privateLogEntrys.list 를 참조하십시오	스택 로그 드라이브를 가져옵니다.
resourcemanager.projects.get 으로 문의하십시오	여러 프로젝트를 지원합니다.
-storage.버킷.create-storage.buckets.delete-storage.버킷.get-storage.버킷.list-storage.버킷.update	데이터 계층화를 위한 Google Cloud Storage 버킷 생성 및 관리
-cloudkms.cryptoKeyVersions.useToEncrypt -cloudkms.cryptoKeys.get-cloudkms.cryptoKeys.list -cloudkms.keyring.list를 참조하십시오	클라우드 키 관리 서비스(Cloud Volumes ONTAP 포함)에서 고객이 관리하는 암호화 키를 사용하려면
-compute.instances.setServiceAccount -iam.serviceAccounts.actAs -iam.serviceAccounts.getIamPolicy -iam.serviceAccounts.list -storage.objects.get -storage.objects.list 를 참조하십시오	Cloud Volumes ONTAP 인스턴스에서 서비스 계정을 설정하려면 이 서비스 계정은 Google Cloud Storage 버킷에 대한 데이터 계층화 권한을 제공합니다.
-compute.addresses.list -compute.backendServices.create -compute.networks.updatePolicy -compute.regionBackendServices.create -compute.regionBackendServices.get -compute.regionBackendServices.list를 참조하십시오	HA 쌍을 구축합니다.
compute.subnetworks.useExternalIp - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig 으로 문의하십시오	클라우드 데이터 센스를 활성화하려면
-container.clusters.get-container.clusters.list 를 참조하십시오	Google Kubernetes Engine에서 실행 중인 Kubernetes 클러스터를 검색할 수 있습니다.
-compute.instanceGroups.get -compute.addresses.get	를 사용하여 HA 쌍에서 스토리지 VM을 생성하고 관리합니다.
-monitoring.timeseries.list-storage.버킷.getIamPolicy	Google Cloud Storage 버킷에 대한 정보를 검색할 수 있습니다.

저작권 정보

Copyright © 2022 NetApp, Inc. All rights reserved. 미국에서 인쇄된 본 문서의 어떤 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 그래픽, 전자적 또는 기계적 수단(사진 복사, 레코딩 등)으로도 저작권 소유자의 사전 서면 승인 없이 전자 검색 시스템에 저장 또는 저장.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지 사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 "있는 그대로" 제공되며 상품성 및 특정 목적에 대한 적합성에 대한 명시적 또는 묵시적 보증을 포함하여 이에 제한되지 않고, 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 또는 파생적 손해(소계 물품 또는 서비스의 조달, 사용 손실, 데이터 또는 수익 손실, 계약, 엄격한 책임 또는 불법 행위(과실 또는 그렇지 않은 경우)에 관계없이 어떠한 책임도 지지 않으며, 이는 이러한 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구입의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허 또는 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 미국 출원 중인 특허로 보호됩니다.

권리 제한 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.277-7103(1988년 10월) 및 FAR 52-227-19(1987년 6월)의 기술 데이터 및 컴퓨터 소프트웨어의 권리(Rights in Technical Data and Computer Software) 조항의 하위 조항 (c)(1)(ii)에 설명된 제한사항이 적용됩니다.

상표 정보

NETAPP, NETAPP 로고 및 에 나열된 마크는 NetApp에 있습니다 <http://www.netapp.com/TM> 는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.