



Reference

Set up and administration

NetApp
July 17, 2022

Table of Contents

- Reference..... 1
 - Permissions summary for Cloud Manager..... 1
 - AWS permissions for the Connector 2
 - Azure permissions for the Connector..... 25
 - Google Cloud permissions for the Connector 33

Reference

Permissions summary for Cloud Manager

In order to use the features and services in Cloud Manager, you'll need to provide permissions so that Cloud Manager can perform operations in your cloud environment. Use the links on this page to quickly access the permissions that you need based on your goal.

AWS permissions

| Purpose | Description | Link |
|-------------------------------|--|--|
| Connector deployment | The user who creates a Connector from Cloud Manager needs specific permissions to deploy the instance in AWS. | Create a Connector in AWS from Cloud Manager |
| Connector operation | <p>When Cloud Manager launches the Connector, it attaches a policy to the instance that provides the permissions required to manage resources and processes in your AWS account.</p> <p>You need to set up the policy yourself if you launch a Connector from the marketplace or if you add more AWS credentials to a Connector.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p> | AWS permissions for the Connector |
| Cloud Volumes ONTAP operation | An IAM role must be attached to each Cloud Volumes ONTAP node in AWS. The same is true for the HA mediator. The default option is to let Cloud Manager create the IAM roles for you, but you can use your own. | Learn how to set up the IAM roles yourself |

Azure permissions

| Purpose | Description | Link |
|----------------------|---|--|
| Connector deployment | When you deploy a Connector from Cloud Manager, you need to use an Azure account or service principal that has permissions to deploy the Connector VM in Azure. | Create a Connector in Azure from Cloud Manager |

| Purpose | Description | Link |
|---------------------|---|---|
| Connector operation | <p>When Cloud Manager deploys the Connector VM in Azure, it creates a custom role that provides the permissions required to manage resources and processes within that Azure subscription.</p> <p>You need to set up the custom role yourself if you launch a Connector from the marketplace or if you add more Azure credentials to a Connector.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p> | Azure permissions for the Connector |

Google Cloud permissions

| Purpose | Description | Link |
|----------------------|--|--|
| Connector deployment | The Google Cloud user who deploys a Connector from Cloud Manager needs specific permissions to deploy the Connector in Google Cloud. | Set up permissions to deploy the Connector |
| Connector operation | <p>The service account for the Connector VM instance must have specific permissions for day-to-day operations. You need to associate the service account with the Connector when you deploy it from Cloud Manager.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p> | Set up a service account for the Connector |

AWS permissions for the Connector

When Cloud Manager launches the Connector instance in AWS, it attaches a policy to the instance that provides the Connector with permissions to manage resources and processes within that AWS account. The Connector uses the permissions to make API calls to several AWS services, including EC2, S3, CloudFormation, IAM, the Key Management Service (KMS), and more.

IAM policy

The IAM policy shown below provides the permissions that a Connector needs to manage resources and processes within your public cloud environment based on your AWS region.

When you create a Connector directly from Cloud Manager, Cloud Manager automatically applies this policy to the Connector.

If you deploy the Connector from the AWS Marketplace or if you manually install the Connector on a Linux host, then you'll need to set up the policy yourself.

You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.

Standard regions

```
{
  "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 (US) regions

```

{
    "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 environment

```

{
    "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/*"
        ]
    }
]
}

```

How the AWS permissions are used

The following sections describe how the permissions are used for each NetApp cloud service. This information can be helpful if your corporate policies dictate that permissions are only provided as needed.

AppTemplate tags

The Connector makes the following API requests to manage tags on AWS resources when you use the AppTemplate Tagging service:

- ec2:CreateTags

- ec2:DeleteTags
- ec2:DescribeTags
- tag:getResources
- tag:getTagKeys
- tag:getTagValues
- tag:TagResources
- tag:UntagResources

Cloud Backup

The Connector makes the following API requests to deploy the restore instance for Cloud Backup:

- 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

The Connector makes the following API requests to manage backups in Amazon S3:

- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:CreateBucket
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions

- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- kms:List*
- kms:Describe*
- s3:GetObject
- ec2:describeVpcEndpoints
- kms:ListAliases
- s3:PutEncryptionConfiguration

The Connector makes the following API requests when you use the Search & Restore method to restore volumes and files:

- s3:CreateBucket
- s3>DeleteObject
- s3>DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMultipartUpload
- s3:ListMultipartUploadParts
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- glue:CreateDatabase
- glue:CreateTable
- glue:BatchDeletePartition

Cloud Data Sense

The Connector makes the following API requests to deploy the Cloud Data Sense instance:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances

- ec2:CreateTags
- ec2:CreateVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2>DeleteSecurityGroup
- ec2:DescribeSecurityGroups
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2>DeleteNetworkInterface
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:CreateSnapshot
- ec2:DescribeRegions
- cloudformation:CreateStack
- cloudformation>DeleteStack
- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

The Connector makes the following API requests to scan S3 buckets when you use Cloud Data Sense:

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3>DeleteObject
- s3>DeleteObjectVersion
- s3:PutObject

- sts:AssumeRole

Cloud Tiering

The Connector makes the following API requests to tier data to Amazon S3 when you use Cloud Tiering.

| Action | Used for set up? | Used for daily operations? |
|------------------------------|------------------|----------------------------|
| s3:CreateBucket | Yes | No |
| s3:PutLifecycleConfiguration | Yes | No |
| s3:GetLifecycleConfiguration | Yes | Yes |
| ec2:DescribeRegions | Yes | Yes |

Cloud Volumes ONTAP

The Connector makes the following API requests to deploy and manage Cloud Volumes ONTAP in AWS.

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|--|----------------------|----------------------------|--------------------|
| Create and manage IAM roles and instance profiles for Cloud Volumes ONTAP instances | iam:ListInstanceProfiles | Yes | Yes | No |
| | iam:CreateRole | Yes | No | No |
| | iam>DeleteRole | No | Yes | Yes |
| | iam:PutRolePolicy | Yes | No | No |
| | iam:CreateInstanceProfile | Yes | No | No |
| | iam>DeleteRolePolicy | No | Yes | Yes |
| | iam:AddRoleToInstanceProfile | Yes | No | No |
| | iam:RemoveRoleFromInstanceProfile | No | Yes | Yes |
| | iam:DeleteInstanceProfile | No | Yes | Yes |
| | iam:PassRole | Yes | No | No |
| | ec2:AssociateIamInstanceProfile | Yes | Yes | No |
| | ec2:DescribeIamInstanceProfileAssociations | Yes | Yes | No |
| | ec2:DisassociateIamInstanceProfile | No | Yes | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|--|--------------------------------|----------------------|----------------------------|--------------------|
| Decode authorization status messages | sts:DecodeAuthorizationMessage | Yes | Yes | No |
| Describe the specified images (AMIs) available to the account | ec2:DescribeImages | Yes | Yes | No |
| Describe the route tables in a VPC (required for HA pairs only) | ec2:DescribeRouteTables | Yes | No | No |
| Stop, start, and monitor instances | ec2:StartInstances | Yes | Yes | No |
| | ec2:StopInstances | Yes | Yes | No |
| | ec2:DescribeInstances | Yes | Yes | No |
| | ec2:DescribeInstanceStatus | Yes | Yes | No |
| | ec2:RunInstances | Yes | No | No |
| | ec2:TerminateInstances | No | No | Yes |
| | ec2:ModifyInstanceAttribute | No | Yes | No |
| Verify that enhanced networking is enabled for supported instance types | ec2:DescribeInstanceAttribute | No | Yes | No |
| Tag resources with the "WorkingEnvironment" and "WorkingEnvironmentId" tags which are used for maintenance and cost allocation | ec2:CreateTags | Yes | Yes | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|-------------------------------------|----------------------|----------------------------|--------------------|
| Manage EBS volumes that Cloud Volumes ONTAP uses as back-end storage | ec2:CreateVolume | Yes | Yes | No |
| | ec2:DescribeVolumes | Yes | Yes | Yes |
| | ec2:ModifyVolumeAttribute | No | Yes | Yes |
| | ec2:AttachVolume | Yes | Yes | No |
| | ec2>DeleteVolume | No | Yes | Yes |
| | ec2:DetachVolume | No | Yes | Yes |
| Create and manage security groups for Cloud Volumes ONTAP | ec2:CreateSecurityGroup | Yes | No | No |
| | ec2>DeleteSecurityGroup | No | Yes | Yes |
| | ec2:DescribeSecurityGroups | Yes | Yes | Yes |
| | ec2:RevokeSecurityGroupEgress | Yes | No | No |
| | ec2:AuthorizeSecurityGroupEgress | Yes | No | No |
| | ec2:AuthorizeSecurityGroupIngress | Yes | No | No |
| | ec2:RevokeSecurityGroupIngress | Yes | Yes | No |
| Create and manage network interfaces for Cloud Volumes ONTAP in the target subnet | ec2:CreateNetworkInterface | Yes | No | No |
| | ec2:DescribeNetworkInterfaces | Yes | Yes | No |
| | ec2>DeleteNetworkInterface | No | Yes | Yes |
| | ec2:ModifyNetworkInterfaceAttribute | No | Yes | No |
| Get the list of destination subnets and security groups | ec2:DescribeSubnets | Yes | Yes | No |
| | ec2:DescribeVpcs | Yes | Yes | No |
| Get DNS servers and the default domain name for Cloud Volumes ONTAP instances | ec2:DescribeDhcpOptions | Yes | No | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|--|------------------------------------|----------------------|----------------------------|--------------------|
| Take snapshots of EBS volumes for Cloud Volumes ONTAP | ec2:CreateSnapshot | Yes | Yes | No |
| | ec2>DeleteSnapshot | No | Yes | Yes |
| | ec2:DescribeSnapshots | No | Yes | No |
| Capture the Cloud Volumes ONTAP console, which is attached to AutoSupport messages | ec2:GetConsoleOutput | Yes | Yes | No |
| Get the list of available key pairs | ec2:DescribeKeyPairs | Yes | No | No |
| Get the list of available AWS regions | ec2:DescribeRegions | Yes | Yes | No |
| Manage tags for resources associated with Cloud Volumes ONTAP instances | ec2:DeleteTags | No | Yes | Yes |
| | ec2:DescribeTags | No | Yes | No |
| Create and manage stacks for AWS CloudFormation templates | cloudformation:CreateStack | Yes | No | No |
| | cloudformation:DeleteStack | Yes | No | No |
| | cloudformation:DescribeStacks | Yes | Yes | No |
| | cloudformation:DescribeStackEvents | Yes | No | No |
| | cloudformation:ValidateTemplate | Yes | No | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|-------------------------------|----------------------|----------------------------|--------------------|
| Create and manage an S3 bucket that a Cloud Volumes ONTAP system uses as a capacity tier for data tiering | s3:CreateBucket | Yes | Yes | No |
| | s3>DeleteBucket | No | Yes | Yes |
| | s3:GetLifecycleConfiguration | No | Yes | No |
| | s3:PutLifecycleConfiguration | No | Yes | No |
| | s3:PutBucketTagging | No | Yes | No |
| | s3:ListBucketVersions | No | Yes | No |
| | s3:GetBucketPolicyStatus | No | Yes | No |
| | s3:GetBucketPublicAccessBlock | No | Yes | No |
| | s3:GetBucketAcl | No | Yes | No |
| | s3:GetBucketPolicy | No | Yes | No |
| | s3:PutBucketPublicAccessBlock | No | Yes | No |
| | s3:GetBucketTagging | No | Yes | No |
| | s3:GetBucketLocation | No | Yes | No |
| | s3:ListAllMyBuckets | No | No | No |
| | s3:ListBucket | No | Yes | No |
| Enable data encryption of Cloud Volumes ONTAP using the AWS Key Management Service (KMS) | kms:List* | Yes | Yes | No |
| | kms:ReEncrypt* | Yes | No | No |
| | kms:Describe* | Yes | Yes | No |
| | kms:CreateGrant | Yes | Yes | No |
| Obtain AWS cost data for Cloud Volumes ONTAP | ce:GetReservationUtilization | No | Yes | No |
| | ce:GetDimensionValues | No | Yes | No |
| | ce:GetCostAndUsage | No | Yes | No |
| | ce:GetTags | No | Yes | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|---------------------------------|----------------------|----------------------------|--------------------|
| Create and manage an AWS spread placement group for two HA nodes and the mediator in a single AWS Availability Zone | ec2:CreatePlacementGroup | Yes | No | No |
| | ec2:DeletePlacementGroup | No | Yes | Yes |
| Create reports | fsx:Describe* | No | Yes | No |
| | fsx:List* | No | Yes | No |
| Create and manage aggregates that support the Amazon EBS Elastic Volumes feature | ec2:DescribeVolumeModifications | No | Yes | No |
| | ec2:ModifyVolume | No | Yes | No |

Global File Cache

The Connector makes the following API requests to deploy Global File Cache instances during deployment:

- cloudformation:DescribeStacks
- cloudwatch:GetMetricStatistics
- cloudformation:ListStacks

Kubernetes

The Connector makes the following API requests to discover and manage Amazon EKS clusters:

- ec2:DescribeRegions
- eks:ListClusters
- eks:DescribeCluster
- iam:GetInstanceProfile

Azure permissions for the Connector

When Cloud Manager launches the Connector VM in Azure, it attaches a custom role to the VM that provides the Connector with permissions to manage resources and processes within that Azure subscription. The Connector uses the permissions to make API calls to several Azure services.

Custom role permissions

The custom role shown below provides the permissions that a Connector needs to manage resources and processes within your Azure network.

When you create a Connector directly from Cloud Manager, Cloud Manager automatically applies this custom

role to the Connector.

If you deploy the Connector from the Azure Marketplace or if you manually install the Connector on a Linux host, then you'll need to set up the custom role yourself.

You also need to ensure that the role is up to date as new permissions are added in subsequent releases.

```
{
  "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"
}

```

How Azure permissions are used

| Actions | Purpose |
|---|---|
| "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", | Creates Cloud Volumes ONTAP and stops, starts, deletes, and obtains the status of the system. |
| "Microsoft.Compute/images/write", "Microsoft.Compute/images/read", | Enables Cloud Volumes ONTAP deployment from a VHD. |
| "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/regeneratekey/action", "Microsoft.Storage/storageAccounts/write", "Microsoft.Storage/storageAccounts/delete", "Microsoft.Storage/usages/read", | Manages Azure storage accounts and disks, and attaches the disks to Cloud Volumes ONTAP. |
| "Microsoft.Storage/storageAccounts/blobServices/containers/read", "Microsoft.KeyVault/vaults/read", "Microsoft.KeyVault/vaults/accessPolicies/write" | Enables backups to Azure Blob storage and encryption of storage accounts |
| "Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write", "Microsoft.Network/networkInterfaces/join/action", | Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet. |
| "Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/join/action", | Creates predefined network security groups for Cloud Volumes ONTAP. |

| Actions | Purpose |
|---|--|
| "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", | Gets network information about regions, the target VNet and subnet, and adds Cloud Volumes ONTAP to VNets. |
| "Microsoft.Network/virtualNetworks/subnets/write", "Microsoft.Network/routeTables/join/action", | Enables VNet service endpoints for data tiering. |
| "Microsoft.Resources/deployments/operations/read", "Microsoft.Resources/deployments/read", "Microsoft.Resources/deployments/write", | Deploys Cloud Volumes ONTAP from a template. |
| "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", | Creates and manages resource groups for Cloud Volumes ONTAP. |
| "Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/snapshots/delete", "Microsoft.Compute/disks/beginGetAccess/action", | Creates and manages Azure managed snapshots. |
| "Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read", | Creates and manages availability sets for Cloud Volumes ONTAP. |
| "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read", "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write", | Enables programmatic deployments from the Azure Marketplace. |

| Actions | Purpose |
|---|---|
| "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", | Manages an Azure load balancer for HA pairs. |
| "Microsoft.Authorization/locks/**", | Enables management of locks on Azure disks. |
| "Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/sites/**" | Manages failover for HA pairs. |
| "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", | Enables the management of private endpoints. Private endpoints are used when connectivity isn't provided to outside the subnet. Cloud Manager creates the storage account for HA with only internal connectivity within the subnet. |
| "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete", | Enables Cloud Manager to delete volumes for Azure NetApp Files. |
| "Microsoft.Resources/deployments/operationStatuses/read" | Azure requires this permission for some virtual machine deployments (it depends on the underlying physical hardware that's used during deployment). |
| "Microsoft.Resources/deployments/operationStatuses/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", | Enables you to use Global File Cache. |

| Actions | Purpose |
|---|---|
| "Microsoft.Network/privateEndpoints/delete", "Microsoft.Compute/availabilitySets/delete", | Enables Cloud Manager to remove resources from a resource group that belong to Cloud Volumes ONTAP in case of deployment failure or deletion. |
| "Microsoft.Compute/diskEncryptionSets/read", "Microsoft.Compute/diskEncryptionSets/write", "Microsoft.Compute/diskEncryptionSets/delete", "Microsoft.KeyVault/vaults/deploy/action", "Microsoft.KeyVault/vaults/read", "Microsoft.KeyVault/vaults/accessPolicies/write", | Enables use of customer-managed encryption keys with Cloud Volumes ONTAP. This feature is supported using APIs. |
| "Microsoft.Resources/tags/read", "Microsoft.Resources/tags/write", "Microsoft.Resources/tags/delete" | Enables you to manage tags on your Azure resources using the Cloud Manager Tagging service. |
| "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" | Enables Cloud Manager to configure an application security group for an HA pair, which isolates the HA interconnect and cluster network NICs. |

Google Cloud permissions for the Connector

Cloud Manager requires permissions to perform actions in Google Cloud. These permissions are included in a custom role provided by NetApp. You might want to understand what Cloud Manager does with these permissions.

Service account permissions

The custom role shown below provides the permissions that a Connector needs to manage resources and processes within your Google Cloud network.

You'll need to apply this custom role to a service account that gets attached to the Connector VM. [View step-by-step instructions](#).

You also need to ensure that the role is up to date as new permissions are added in subsequent releases.

```
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

How Google Cloud permissions are used

| Actions | Purpose |
|---|--|
| <ul style="list-style-type: none"> - compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use | To create and manage disks for Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list | To create firewall rules for Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.globalOperations.get | To get the status of operations. |
| <ul style="list-style-type: none"> - compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly | To get images for VM instances. |
| <ul style="list-style-type: none"> - compute.instances.attachDisk - compute.instances.detachDisk | To attach and detach disks to Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.instances.create - compute.instances.delete | To create and delete Cloud Volumes ONTAP VM instances. |
| <ul style="list-style-type: none"> - compute.instances.get | To list VM instances. |
| <ul style="list-style-type: none"> - compute.instances.getSerialPortOutput | To get console logs. |
| <ul style="list-style-type: none"> - compute.instances.list | To retrieve the list of instances in a zone. |
| <ul style="list-style-type: none"> - compute.instances.setDeletionProtection | To set deletion protection on the instance. |
| <ul style="list-style-type: none"> - compute.instances.setLabels | To add labels. |
| <ul style="list-style-type: none"> - compute.instances.setMachineType - compute.instances.setMinCpuPlatform | To change the machine type for Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.instances.setMetadata | To add metadata. |
| <ul style="list-style-type: none"> - compute.instances.setTags | To add tags for firewall rules. |
| <ul style="list-style-type: none"> - compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice | To start and stop Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.machineTypes.get | To get the numbers of cores to check quotas. |
| <ul style="list-style-type: none"> - compute.projects.get | To support multi-projects. |
| <ul style="list-style-type: none"> - compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels | To create and manage persistent disk snapshots. |

| Actions | Purpose |
|---|--|
| <ul style="list-style-type: none"> - 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 | To get the networking information needed to create a new Cloud Volumes ONTAP virtual machine instance. |
| <ul style="list-style-type: none"> - 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 | To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Deployment Manager. |
| <ul style="list-style-type: none"> - logging.logEntries.list - logging.privateLogEntries.list | To get stack log drives. |
| <ul style="list-style-type: none"> - resourcemanager.projects.get | To support multi-projects. |
| <ul style="list-style-type: none"> - storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update | To create and manage a Google Cloud Storage bucket for data tiering. |
| <ul style="list-style-type: none"> - cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyRings.list | To use customer-managed encryption keys from the Cloud Key Management Service with Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects.get - storage.objects.list | To set a service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. |

| Actions | Purpose |
|--|--|
| <ul style="list-style-type: none"> - compute.addresses.list - compute.backendServices.create - compute.networks.updatePolicy - compute.regionBackendServices.create - compute.regionBackendServices.get - compute.regionBackendServices.list | To deploy HA pairs. |
| <ul style="list-style-type: none"> - compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig | To enable Cloud Data Sense. |
| <ul style="list-style-type: none"> - container.clusters.get - container.clusters.list | To discover Kubernetes clusters running in Google Kubernetes Engine. |
| <ul style="list-style-type: none"> - compute.instanceGroups.get - compute.addresses.get | To create and manage storage VMs on HA pairs. |
| <ul style="list-style-type: none"> - monitoring.timeSeries.list - storage.buckets.getIamPolicy | To discover information about Google Cloud Storage buckets. |

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.