



参考

Set up and administration

NetApp

July 13, 2022

# 目录

- 参考 ..... 1
  - Cloud Manager权限摘要 ..... 1
  - Connector 的 AWS 权限 ..... 2
  - Connector 的 Azure 权限 ..... 25
  - 适用于 Connector 的 Google Cloud 权限 ..... 33

# 参考

## Cloud Manager权限摘要

要使用Cloud Manager中的功能和服务、您需要提供权限、以便Cloud Manager可以在您的云环境中执行操作。使用此页面上的链接可根据您的目标快速访问所需的权限。

### AWS权限

目的	Description	链接。
连接器部署	从Cloud Manager创建Connector的用户需要特定权限才能在AWS中部署实例。	<a href="#">"从 Cloud Manager 在 AWS 中创建连接器"</a>
连接器操作	Cloud Manager启动Connector时、它会将一个策略附加到实例、该实例提供管理AWS帐户中资源和进程所需的权限。如果需要、您需要自行设置策略 <a href="#">"从市场启动Connector"</a> 或者 <a href="#">"向Connector添加更多AWS凭据"</a> 。此外、您还需要确保在后续版本中添加新权限时策略是最新的。	<a href="#">"Connector 的 AWS 权限"</a>
Cloud Volumes ONTAP 操作	必须将IAM角色附加到AWS中的每个Cloud Volumes ONTAP 节点。HA调解器也是如此。默认选项是让Cloud Manager为您创建IAM角色、但您可以使用自己的角色。	<a href="#">"了解如何自己设置IAM角色"</a>

### Azure权限

目的	Description	链接。
连接器部署	从Cloud Manager部署Connector时、您需要使用有权在Azure中部署Connector VM的Azure帐户或服务主体。	<a href="#">"从 Cloud Manager 在 Azure 中创建 Connector"</a>
连接器操作	当Cloud Manager在Azure中部署Connector VM时、它会创建一个自定义角色、此角色可提供在该Azure订阅中管理资源和进程所需的权限。  如果需要、您需要自己设置自定义角色 <a href="#">"从市场启动Connector"</a> 或者 <a href="#">"向Connector添加更多Azure凭据"</a> 。  此外、您还需要确保在后续版本中添加新权限时策略是最新的。	<a href="#">"Connector 的 Azure 权限"</a>

### Google Cloud权限

目的	Description	链接。
连接器部署	从Cloud Manager部署Connector的Google Cloud用户需要特定权限才能在Google Cloud中部署Connector。	<a href="#">"设置部署Connector的权限"</a>
连接器操作	Connector VM实例的服务帐户必须具有执行日常操作的特定权限。在从Cloud Manager部署服务帐户时、您需要将其与Connector相关联。此外、您还需要确保在后续版本中添加新权限时策略是最新的。	<a href="#">"为Connector设置服务帐户"</a>

## Connector 的 AWS 权限

当Cloud Manager在AWS中启动Connector实例时、它会向此实例附加一个策略、此策略可为Connector提供管理该AWS帐户中资源和进程的权限。Connector使用这些权限对多个AWS服务进行API调用、包括EC2、S3、CloudFormation、IAM、密钥管理服务(KMS)等。

### IAM策略

下面显示的IAM策略提供了Connector根据您的AWS区域管理公有云环境中的资源和流程所需的权限。

直接从Cloud Manager创建Connector时、Cloud Manager会自动将此策略应用于Connector。

如果您从AWS Marketplace部署Connector、或者在Linux主机上手动安装Connector、则需要自己设置策略。

此外、您还需要确保在后续版本中添加新权限时策略是最新的。

```
{
  "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 (美国)地区

```

{
  "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环境

```

{
    "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/*"
    ]
}
]
}

```

## 如何使用AWS权限

以下各节介绍了如何对每个NetApp云服务使用权限。如果您的公司策略规定仅在需要时提供权限、则此信息会很有用。

### AppTemplate标记

在使用AppTemplate标记服务时、Connector会发出以下API请求来管理AWS资源上的标记：

- EC2: CreateTags
- EC2: DeleteTags
- EC2: Describe标记
- 标记: getResources
- 标记: getTag密钥
- 标记: getTagValues
- 标记: 标记资源
- 标记: 未标记资源

## 云备份

Connector会发出以下API请求来部署Cloud Backup的还原实例:

- EC2: StartInstances
- EC2: StopInstances
- EC2: Describe实例
- EC2: Describe实例状态
- EC2: RunInstances
- EC2: 终端状态
- EC2: Describe实例属性
- EC2: Describe
- EC2: CreateTags
- EC2: CreateVolume
- EC2: CreateSecurityGroup
- EC2: Describe子网
- EC2: Describe
- EC2: Describe注册
- CloudFormation: CreateStack
- CloudFormation: DeleteStack
- CloudFormation: Describe堆栈

Connector会发出以下API请求来管理Amazon S3中的备份:

- S3 : GetBucketLocation
- S3 : ListAllMy桶
- S3 : ListBucket
- S3 : CreateBucket
- S3 : GetLifecycleConfiguration

- S3 : PutLifecycleConfiguration
- S3 : PutBucketTagging
- S3 : ListBucketVersions
- S3 : GetBucketAcl
- S3: PutBucketPublicAccessBlock
- 公里: 列表\*
- 公里: 描述\*
- S3 : GetObject
- EC2: 介绍VpcEndpoints
- Kms: ListAliases
- S3 : PutEncryptionConfiguration

在使用搜索和还原方法还原卷和文件时、Connector会发出以下API请求:

- 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 : ListMultipartUploadPart
- Athena: StartQueryExecutionc
- Athena: GetQueryResults
- Athena: GetQueryExecution
- Athena: StopQueryExecution
- 胶水: CreateDatabase
- 胶水: CreateTable
- 粘附: BatechDelete分区

Connector发出以下API请求以部署Cloud Data sense实例：

- EC2: Describe实例
- EC2: Describe实例状态
- EC2: RunInstances
- EC2: 终端状态
- EC2: CreateTags
- EC2: CreateVolume
- EC2: Attach卷
- EC2: CreateSecurityGroup
- EC2: DeleteSecurityGroup
- EC2: Describe安全性组
- EC2: CreateNetworkInterface
- EC2: Describe网络接口
- EC2: DeleteNetworkInterface
- EC2: Describe子网
- EC2: Describe
- EC2: CreateSnapshot
- EC2: Describe注册
- CloudFormation: CreateStack
- CloudFormation: DeleteStack
- CloudFormation: Describe堆栈
- CloudFormation: Describe StackEvents
- IAM: AddRoleToInstanceProfile
- EC2: AssociateIamInstanceProfile
- EC2: Describe IamInstanceProfileAssociations

在使用Cloud Data sense时、Connector会发出以下API请求来扫描S3存储分段：

- IAM: AddRoleToInstanceProfile
- EC2: AssociateIamInstanceProfile
- EC2: Describe IamInstanceProfileAssociations
- S3 : GetBucketTagging
- S3 : GetBucketLocation
- S3 : ListAllMy桶

- S3 : ListBucket
- S3: GetBucketPolicyStatus
- S3 : GetBucketPolicy
- S3 : GetBucketAcl
- S3 : GetObject
- IAM: GetRole
- S3 : DeleteObject
- S3 : DeleteObjectVersion
- S3 : PutObject
- STS: AssumeRole

## 云分层

在使用Cloud Tiering时、Connector会发出以下API请求、将数据分层到Amazon S3。

Action	用于设置?	用于日常操作?
S3 : CreateBucket	是的。	否
S3 : PutLifecycleConfiguration	是的。	否
S3 : GetLifecycleConfiguration	是的。	是的。
EC2: Describe注册	是的。	是的。

## Cloud Volumes ONTAP

Connector会发出以下API请求、以便在AWS中部署和管理Cloud Volumes ONTAP。

目的	Action	用于部署?	用于日常操作?	用于删除?
创建和管理Cloud Volumes ONTAP 实例的IAM角色和实例配置文件	IAM : ListInstanceProfile	是的。	是的。	否
	IAM: CreateRole	是的。	否	否
	IAM: DeleteRole	否	是的。	是的。
	IAM: PutRolePolicy	是的。	否	否
	IAM : CreateInstanceProfile	是的。	否	否
	IAM : DeleteRolePolicy	否	是的。	是的。
	IAM : AddRoleToInstanceProfile	是的。	否	否
	IAM : RemoveRoleFromInstanceProfile	否	是的。	是的。
	IAM : DeleteInstanceProfile	否	是的。	是的。
	IAM: PassRole	是的。	否	否
	EC2 : AssociateIamInstanceProfile	是的。	是的。	否
	EC2: DescribeIamInstanceProfileAssociations	是的。	是的。	否
	EC2 : DisassociateIamInstanceProfile	否	是的。	否
对授权状态消息进行解码	STS : DecodeAuthorizationMessage	是的。	是的。	否
描述可供帐户使用的指定映像(AMI)	EC2: Describe	是的。	是的。	否
描述VPC中的路由表(仅HA对需要)	EC2: Describe RouteTables	是的。	否	否

目的	Action	用于部署?	用于日常操作?	用于删除?
停止、启动和监控实例	EC2: StartInstances	是的。	是的。	否
	EC2: StopInstances	是的。	是的。	否
	EC2: Describe实例	是的。	是的。	否
	EC2: Describe实例状态	是的。	是的。	否
	EC2: RunInstances	是的。	否	否
	EC2: 终端状态	否	否	是的。
	EC2: ModifyInstance属性	否	是的。	否
验证是否已为支持的实例类型启用增强型网络连接	EC2: Describe实例属性	否	是的。	否
使用"WorkingEnvironment"和"WorkingEnvironmentId"标记标记资源、用于维护和成本分配	EC2: CreateTags	是的。	是的。	否
管理Cloud Volumes ONTAP 用作后端存储的EBS卷	EC2: CreateVolume	是的。	是的。	否
	EC2: Describe卷	是的。	是的。	是的。
	EC2: ModifyVolumeAttribute	否	是的。	是的。
	EC2: Attach卷	是的。	是的。	否
	EC2: DeleteVolume	否	是的。	是的。
	EC2: 分离卷	否	是的。	是的。

目的	Action	用于部署?	用于日常操作?	用于删除?
创建和管理Cloud Volumes ONTAP 的安全组	EC2 : CreateSecurityGroup	是的。	否	否
	EC2 : DeleteSecurityGroup	否	是的。	是的。
	EC2: Describe安全性组	是的。	是的。	是的。
	EC2 : RevokeSecurityGroupEgress	是的。	否	否
	EC2 : AuthorizeSecurityGroupEgress	是的。	否	否
	EC2 : AuthorizeSecurityGroupIngress	是的。	否	否
	EC2 : RevokeSecurityGroupIngress	是的。	是的。	否
在目标子网中为Cloud Volumes ONTAP 创建和管理网络接口	EC2 : CreateNetworkInterface	是的。	否	否
	EC2: Describe网络接口	是的。	是的。	否
	EC2 : DeleteNetworkInterface	否	是的。	是的。
	EC2 : ModifyNetworkInterfaceAttribute	否	是的。	否
获取目标子网和安全组的列表	EC2: Describe子网	是的。	是的。	否
	EC2: Describe	是的。	是的。	否
获取DNS服务器和Cloud Volumes ONTAP 实例的默认域名	EC2: Describe DhcpOptions	是的。	否	否
为Cloud Volumes ONTAP 的EBS卷创建快照	EC2 : CreateSnapshot	是的。	是的。	否
	EC2 : DeleteSnapshot	否	是的。	是的。
	EC2: Describe Snapshot	否	是的。	否



目的	Action	用于部署?	用于日常操作?	用于删除?
捕获附加到AutoSupport 消息的Cloud Volumes ONTAP 控制台	EC2 : GetConsoleOutput	是的。	是的。	否
获取可用密钥对的列表	EC2: Describe KeyPairs	是的。	否	否
获取可用AWS区域的列表	EC2: Describe注册	是的。	是的。	否
管理与Cloud Volumes ONTAP 实例关联的资源的标记	EC2: DeleteTags	否	是的。	是的。
	EC2: Describe标记	否	是的。	否
为AWS CloudFormation模板创建和管理堆栈	CloudFormation : CreateStack	是的。	否	否
	CloudFormation : DeleteStack	是的。	否	否
	CloudFormation : Describe堆栈	是的。	是的。	否
	CloudFormation : Describe StackEvents	是的。	否	否
	CloudFormation: 验证模板	是的。	否	否

目的	Action	用于部署?	用于日常操作?	用于删除?
创建和管理Cloud Volumes ONTAP 系统用作数据分层容量层的S3存储分段	S3 : CreateBucket	是的。	是的。	否
	S3 : DeleteBucket	否	是的。	是的。
	S3 : GetLifecycleConfiguration	否	是的。	否
	S3 : PutLifecycleConfiguration	否	是的。	否
	S3 : PutBucketTagging	否	是的。	否
	S3 : ListBucketVersions	否	是的。	否
	S3 : GetBucketPolicyStatus	否	是的。	否
	S3 : GetBucketPublicAccessBlock	否	是的。	否
	S3 : GetBucketAcl	否	是的。	否
	S3 : GetBucketPolicy	否	是的。	否
	S3 : PutBucketPublicAccessBlock	否	是的。	否
	S3 : GetBucketTagging	否	是的。	否
	S3 : GetBucketLocation	否	是的。	否
	S3 : ListAllMy桶	否	否	否
	S3 : ListBucket	否	是的。	否
使用AWS密钥管理服务(KMS)对Cloud Volumes ONTAP 启用数据加密	公里: 列表*	是的。	是的。	否
	kms: 重新加密*	是的。	否	否
	公里: 描述*	是的。	是的。	否
	公里: CreateGrant	是的。	是的。	否

目的	Action	用于部署?	用于日常操作?	用于删除?
获取Cloud Volumes ONTAP 的AWS成本数据	CE : GetReservationUtilization	否	是的。	否
	CE : GetDimensionValues	否	是的。	否
	CE : GetCostAndUsage	否	是的。	否
	CE: GetTags	否	是的。	否
在一个AWS可用性区域中为两个HA节点和调解器创建和管理一个AWS分布式放置组	EC2 : CreatePlacementGroup	是的。	否	否
	EC2 : DeletePlacementGroup	否	是的。	是的。
创建报告	FSX: 描述*	否	是的。	否
	FSX: List*	否	是的。	否
创建和管理支持Amazon EBS弹性卷功能的聚合	EC2: Describe卷修改	否	是的。	否
	EC2: ModifyVolume	否	是的。	否

## 全局文件缓存

Connector会发出以下API请求、以便在部署期间部署全局文件缓存实例：

- CloudFormation：Describe堆栈
- CloudWatch：GetMetricStatistics
- CloudFormation：ListStack

## Kubernetes

Connector会发出以下API请求来发现和管理Amazon EKS集群：

- EC2：Describe注册
- EKS：ListClusters
- EKS：Describe集群
- IAM：GetInstanceProfile

## Connector 的 Azure 权限

当Cloud Manager在Azure中启动Connector VM时、它会将一个自定义角色附加到该VM、从而使Connector能够管理该Azure订阅中的资源和进程。Connector使用权限对多个Azure

服务进行API调用。

## 自定义角色权限

下面显示的自定义角色提供了Connector管理Azure网络中的资源和进程所需的权限。

直接从Cloud Manager创建Connector时、Cloud Manager会自动将此自定义角色应用于Connector。

如果您从Azure Marketplace部署Connector、或者在Linux主机上手动安装Connector、则需要您自己设置自定义角色。

您还需要确保角色是最新的、因为在后续版本中添加了新权限。

```
{
  "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"
}

```

## 如何使用Azure权限

操作	目的
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" ,	创建 Cloud Volumes ONTAP 并停止、启动、删除和获取系统状态。
"Microsoft.compute/images/write" 、 "Microsoft.compute/images/read" 、	支持从 VHD 部署 Cloud Volumes ONTAP 。
Microsoft.Compute/disks/delete" , Microsoft.Compute/disks/read" , Microsoft.Compute/disks/write" , "microsoft.Storage/SchecknameAvailability /Read" , "microsoft.Storage/operations/Read" , "microsoft.Storage/storageAccounts" , "microsoft.Storage/storageAccouns/Read" , "microsoft.Storage/storageAccounts" , "microsoft.Storage/storageAccounts" , "microsoft.Storage/storageAccounts" , "microsoft.Storage/storageAccounts" , "microsoft.Storage/Acces/ Read" ,	管理 Azure 存储帐户和磁盘、并将磁盘连接到 Cloud Volumes ONTAP 。
"microsoft.Storage/storageAccounts/blobServices/containers/read" , "microsoft.KeyVault/vaults/read" , "microsoft.KeyVault/vaults/accessPolicies/write"	可备份到 Azure Blob 存储并对存储帐户进行加密
"microsoft.network/networkinterfaces/read" 、 "microsoft.network/networkinterfaces/write" 、 "microsoft.network/networkinterfaces/join/action" 、	在目标子网中为 Cloud Volumes ONTAP 创建和管理网络接口。
"microsoft.network/networksecuritygroups/read" 、 "microsoft.network/networksecuritygroups/write" 、 "microsoft.network/networksecuritygroups/join/action" 、	为 Cloud Volumes ONTAP 创建预定义的网络安全组。



操作	目的
"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" ,	获取有关区域、目标 VNet 和子网的网络信息、并将 Cloud Volumes ONTAP 添加到 VNETS 。
Microsoft.Network/virtualNetworks/subnets/write" , Microsoft.Network/routeTables/join/action" ,	启用 VNet 服务端点以进行数据分层。
"Microsoft.Resources/deployments/operations/read" 、 "Microsoft.Resources/deployments/read" 、 "Microsoft.Resources/deployments/write" 、	从模板部署 Cloud Volumes ONTAP 。
"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/write" ,	为 Cloud Volumes ONTAP 创建和管理资源组。
Microsoft.Compute/snapshots/write" , Microsoft.Compute/snapshots/read" , Microsoft.Compute/snapshots/delete" , Microsoft.Compute/disks/beginGetAccess/action" ,	创建和管理 Azure 管理的快照。
"microsoft.compute/availabilitysets/write" 、 "microsoft.compute/availabilitysets/read" 、	创建和管理 Cloud Volumes ONTAP 的可用性集。
"Microsoft.MarketplaceCatalog/服务类型/发布者/服务/计划/协议/读取" 、 "Microsoft.MarketplaceCatalog/服务类型/发布者/服务/计划/协议/写入" 、	支持从 Azure Marketplace 进行编程部署。

操作	目的
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" , ,	管理 HA 对的 Azure 负载均衡器。
"Microsoft.Authorization/Locks/*"	支持管理 Azure 磁盘上的锁定。
"microsoft.Authorization/roleDefinitions/write" , "microsoft.Authorization/roleAssignments/write" , "microsoft.Web/sites/*"	管理 HA 对的故障转移。
Microsoft.Network/privateEndpoints/write" , "microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/Actions" , "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" ,	用于管理私有端点。如果未向子网外部提供连接, 则会使用私有端点。Cloud Manager 会为 HA 创建存储帐户, 但子网中只有内部连接。
" Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete" ,	允许 Cloud Manager 删除 Azure NetApp Files 的卷。
"microsoft.resources/deployments/operationStatuss/Read"	Azure 在某些虚拟机部署中需要此权限 (取决于部署期间使用的底层物理硬件) 。
"microsoft.resources/deployments/operationStatuss/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" ,	用于使用全局文件缓存。

操作	目的
Microsoft.Network/privateEndpoints/delete" , Microsoft.Compute/availabilitySets/delete" ,	允许 Cloud Manager 在部署失败或删除时从属于 Cloud Volumes ONTAP 的资源组中删除资源。
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" ,	支持将客户管理的加密密钥与 Cloud Volumes ONTAP 结合使用。使用 API 支持此功能。
"microsoft.resources/tags /read" , "microsoft.resources/tags /write" , "microsoft.resources/tags /delete"	用于使用 Cloud Manager 标记服务管理 Azure 资源上的标记。
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"	通过 Cloud Manager 可以为 HA 对配置应用程序安全组，从而隔离 HA 互连和集群网络 NIC 。

## 适用于 Connector 的 Google Cloud 权限

Cloud Manager 需要在 Google Cloud 中执行操作的权限。这些权限包含在 NetApp 提供的自定义角色中。您可能希望了解 Cloud Manager 使用这些权限执行的操作。

### 服务帐户权限

下面显示的自定义角色提供了 Connector 在 Google Cloud 网络中管理资源和进程所需的权限。

您需要将此自定义角色应用于连接到 Connector VM 的服务帐户。"查看分步说明"。

您还需要确保角色是最新的、因为在后续版本中添加了新权限。

```

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

## 如何使用Google Cloud权限

操作	目的
— compute.disks.create — compute.disks.createSnapshot — compute.disks.delete — compute.disks.get — compute.disks.list — compute.disks.setLabels — compute.disks.use	为 Cloud Volumes ONTAP 创建和管理磁盘。
— compute.v防火墙 创建— compute.firewalls.delete — compute.v防火墙 .get — compute.v防火墙 列表	为 Cloud Volumes ONTAP 创建防火墙规则。
— compute.globalOperations.get	以获取操作状态。
— compute.images.get — compute.images.getFromFamily — compute.images.list — compute.images.useReadOnly	为 VM 实例获取映像。
— compute.instances.attachDisk — compute.instances.detachDisk	将磁盘连接和断开与 Cloud Volumes ONTAP 的连接。
— compute.instances.create — compute.instances.delete	创建和删除 Cloud Volumes ONTAP VM 实例。
— compute.instances.get	列出 VM 实例。
— compute.instances.getSerialPortOutput	以获取控制台日志。
— compute.instances.list	检索区域中实例的列表。
— compute.instances.setDeletionProtection	为实例设置删除保护。
— compute.instances.setLabels	以添加标签。
— compute.instances.setMachineType — compute.instances.setMinCpuPlatform	更改 Cloud Volumes ONTAP 的计算机类型。
— compute.instances.setMetadata	以添加元数据。
— compute.instances.setTags	为防火墙规则添加标记。
— compute.instances.start — compute.instances.stop — compute.instances.updateDisplayDevice	启动和停止 Cloud Volumes ONTAP 。
— compute.machineTypes.get	获取要检查 qoutas 的核心数。
— compute.projects.get	以支持多个项目。
— compute.snapshots.create — compute.snapshots.delete — compute.snapshots.get — compute.snapshots.list — compute.snapshots.setLabels	创建和管理永久性磁盘快照。
— 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	获取创建新 Cloud Volumes ONTAP 虚拟机实例所需的网络信息。

操作	目的
- 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.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProvider.get - deploymentmanager.typeProvider.get - deploymentmanager.typeProvider.list - get	使用 Google Cloud 部署管理器部署 Cloud Volumes ONTAP 虚拟机实例。
— logging.logEntries.list — logging.privateLogEntries.list	获取堆栈日志驱动器。
— resourceManager.projects.get	以支持多个项目。
— storage.buckets.create — storage.buckets.delete — storage.buckets.get — storage.buckets.list — storage.buckets.update	创建和管理用于数据分层的 Google Cloud Storage 存储分段。
— cloudkms.cryptoKeyVersions.useToEncrypt — cloudkms.encryptKeys.get — cloudkms.encryptKeys.list — cloudkms.keyrings.list	将云密钥管理服务中由客户管理的加密密钥与 Cloud Volumes ONTAP 结合使用。
— compute.instances.setServiceAccount — iam.serviceAccounts.actAs — iam.serviceAccounts.getIamPolicy — iam.serviceAccounts.list — storage.objects.get — storage.objects.list	在 Cloud Volumes ONTAP 实例上设置服务帐户。此服务帐户提供将数据分层到 Google Cloud Storage 存储分段的权限。
— compute.addresses ... list — compute.backendServices.create — compute.networks.updatePolicy — compute.regionBackendServices.create — compute.regionBackendServices.get — compute.regionBackendServices.list	部署 HA 对。
— compute.subnetworks.use — compute.subnetworks.useExternalIp — compute.instances.addAccessConfig	启用 Cloud Data sense 。
— container.clusters 。 get — container.clusters 。 list	发现在 Google Kubernetes Engine 中运行的 Kubernetes 集群。
—compute.instanceGroups.get—compute.addresses 。 get	在HA对上创建和管理Storage VM。

## 版权信息

版权所有©2022 NetApp、Inc.。保留所有权利。Printed in the U.S.版权所涵盖的本文档的任何部分不得以任何形式或任何手段复制、包括影印、录制、磁带或存储在电子检索系统中—未经版权所有者事先书面许可。

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

本软件由NetApp按"原样"提供、不含任何明示或默示担保、包括但不限于适销性和特定用途适用性的默示担保、特此声明不承担任何任何责任。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).

## 商标信息

NetApp、NetApp标识和中列出的标记 <http://www.netapp.com/TM> 是NetApp、Inc.的商标。其他公司和产品名称可能是其各自所有者的商标。