參考資料
Set up and administration

NetApp
July 17, 2022

目錄

參考資料

Cloud Manager的權限摘要

若要使用Cloud Manager中的功能和服務、您必須提供權限、以便Cloud Manager能在雲端環境中執行作業。使用此頁面上的連結、根據您的目標快速存取所需的權限。

AWS權限

目的	說明	連結
連接器部署	從Cloud Manager建立Connector的使用者需要特定權限、才能在AWS中部署執行個體。	"從Cloud Manager在AWS中建立連接器"
連接器操作	Cloud Manager啟動Connector時、會將原則附加至執行個體、以提供管理AWS帳戶中資源和程序所需的權限。您需要自行設定原則 "從市場推出Connector" 或是您 "將更多AWS認證資料新增至Connector"。您也必須確保在後續版本中新增權限時、原則保持在最新狀態。	"Connector的AWS權限"
作業系統Cloud Volumes ONTAP	必須將IAM角色附加至Cloud Volumes ONTAP AWS中的每個節點。HA中介者也是如此。預設選項是讓Cloud Manager為您建立IAM角色、但您可以自行使用。	"瞭解如何自行設定IAM角色"

Azure權限

目的	說明	連結
連接器部署	當您從Cloud Manager部署Connector時、您需要使用Azure帳戶或服務主體、該用戶必須具有在Azure中部署Connector VM的權限。	"從Cloud Manager在Azure中建立Connector"
連接器操作	Cloud Manager在Azure中部署Connector VM時、會建立自訂角色、提供必要的權限來管理該Azure訂閱中的資源和程序。 您需要自行設定自訂角色（如果您） "從市場推出Connector" 或是您 "將更多Azure認證資料新增至Connector"。 您也必須確保在後續版本中新增權限時、原則保持在最新狀態。	"連接器的Azure權限"

Google Cloud權限

目的	說明	連結
連接器部署	從Cloud Manager部署Connector的Google Cloud使用者需要特定權限、才能在Google Cloud中部署Connector。	"設定部署Connector的權限"
連接器操作	Connector VM執行個體的服務帳戶必須具有特定的日常作業權限。從Cloud Manager部署時、您需要將服務帳戶與Connector建立關聯。您也必須確保在後續版本中新增權限時、原則保持在最新狀態。	"設定Connector的服務帳戶"

Connector的AWS權限

Cloud Manager在AWS中啟動Connector執行個體時、會將原則附加至執行個體、讓Connector有權管理該AWS帳戶內的資源和程序。連接器使用權限來撥打API呼叫數個AWS服務、包括EC2、S3、CloudForecation、IAM、 金鑰管理服務（KMS）等。

IAM原則

下列IAM原則提供Connector所需的權限、以便根據AWS區域管理公有雲環境中的資源和程序。

直接從Cloud Manager建立Connector時、Cloud Manager會自動將此原則套用至Connector。

如果您是從AWS Marketplace部署Connector、或是在Linux主機上手動安裝Connector、則必須自行設定原則。

您也必須確保在後續版本中新增權限時、原則保持在最新狀態。

標準區域

```
{
  "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（美國）地區

```
{
    "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環境

```
{
    "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/*"
                ]
            }
        ]
}
```

AWS權限的使用方式

以下各節說明如何將權限用於每項NetApp雲端服務。如果您的企業原則規定只有在需要時才提供權限、此資訊就很有幫助。

應用程式範本標記

當您使用應用程式範本標記服務時、Connector會發出下列API要求來管理AWS資源上的標記：

- EC2：建立標記
- EC2：刪除標記
- EC2：取消標示
- 標記：getResources
- 標記：getTagKeys
- 標記：getTagValues
- 標記：TagResources
- 標記：取消標記資源

雲端備份

Connector會提出下列API要求、以部署Cloud Backup的還原執行個體：

- EC2：啟動安裝
- EC2：停止執行
- EC2：資料說明
- EC2：取消訂閱即時狀態
- EC2：RunInstances
- EC2：終端安裝
- EC2：取消訂閱實例屬性
- EC2：取消影像
- EC2：建立標記
- EC2：建立磁碟區
- EC2：建立安全性群組
- EC2：無資料子網路
- EC2：取消功能Vpcs
- EC2：取消註冊
- 雲端：建立堆疊
- 雲端：刪除堆疊
- 雲端：無標準堆疊

Connector會提出下列API要求、以管理Amazon S3中的備份：

- S3：GetBucketLocation
- S3：ListAllMyb桶
- S3：清單庫
- S3：建立桶
- S3：Get生命 週期組態

- S3：Putt升降 器組態
- S3：PuttBucketting
- S3：listBucketVerions
- S3：GetBucketAcl
- S3：PuttBucketPublicAccessBlock
- 公里：清單*
- 公里：描述*
- S3：GetObject
- EC2：已描述VpcEndpoints
- kms：清單別名
- S3：PuttEncryptionConfiguration

當您使用搜尋與還原方法還原磁碟區和檔案時、Connector會發出下列API要求：

- S3：建立桶
- S3：刪除物件
- S3：刪除ObjectVersion
- S3：GetBucketAcl
- S3：清單庫
- S3：listBucketVerions
- S3：listBucketMultiPartUploads
- S3：PuttObject
- S3：PuttBucketAcl
- S3：Putt升降 器組態
- S3：PuttBucketPublicAccessBlock
- S3：中止多重角色上傳
- S3：列出多個零件上傳零件
- Athena：StartQueryExecutionc
- Athena：GetQueryResults
- Athena：GetQueryExecution
- Athena：停止查詢執行
- 黏著劑：建立資料庫
- 黏著劑：CreateTable
- 黏著劑：批字刪除分割區

雲端資料感測

Connector會提出下列API要求來部署Cloud Data Sense執行個體：

- EC2：資料說明
- EC2：取消訂閱即時狀態
- EC2：RunInstances
- EC2：終端安裝
- EC2：建立標記
- EC2：建立磁碟區
- EC2：AttachVolume
- EC2：建立安全性群組
- EC2：刪除安全性群組
- EC2：取消安全性群組
- EC2：建立網路介面
- EC2：網路介面
- EC2：刪除網路介面
- EC2：無資料子網路
- EC2：取消功能Vpcs
- EC2：建立Snapshot
- EC2：取消註冊
- 雲端：建立堆疊
- 雲端：刪除堆疊
- 雲端：無標準堆疊
- 雲端：取消功能堆疊事件
- IAM：AddRoleToInstanceProfile
- EC2：Associate IamInstanceProfile
- EC2：解讀IamInstanceProfileAssociations

使用Cloud Data Sense時、Connector會發出下列API要求來掃描S3儲存區：

- IAM：AddRoleToInstanceProfile
- EC2：Associate IamInstanceProfile
- EC2：解讀IamInstanceProfileAssociations
- S3：GetBucketting
- S3：GetBucketLocation
- S3：ListAllMyb桶

- S3：清單庫
- S3：GetBucketPolicyStatus
- S3：GetBucketPolicy
- S3：GetBucketAcl
- S3：GetObject
- IAM：GetRole
- S3：刪除物件
- S3：刪除ObjectVersion
- S3：PuttObject
- STS: Assume勞力

雲端分層

連接器會在您使用雲端分層時、提出下列API要求、將資料分層至Amazon S3。

行動	用於設定？	用於日常營運？
S3：建立桶	是的	否
S3：Putt升降 器組態	是的	否
S3：Get生命 週期組態	是的	是的
EC2：取消註冊	是的	是的

Cloud Volumes ONTAP

Connector會提出下列API要求、要求在Cloud Volumes ONTAP AWS中部署及管理功能。

目的	行動	用於部署？	用於日常營運？	用於刪除？
建立及管理IAM角色及Cloud Volumes ONTAP 執行個體設定檔以利執行個體	IAM：清單執行設定檔	是的	是的	否
	IAM：建立角色	是的	否	否
	IAM：刪除角色	否	是的	是的
	IAM：Putt角色 原則	是的	否	否
	IAM ：CreatanceProfile	是的	否	否
	IAM：刪除角色原則	否	是的	是的
	IAM ：AddRoleToInstanceProfile	是的	否	否
	IAM ：RemoveRoleFromInstanceProfile	否	是的	是的
	IAM：刪除InstanceProfile	否	是的	是的
	IAM：密碼	是的	否	否
	EC2：Associate IamInstanceProfile	是的	是的	否
	EC2：解讀IamInstanceProfile Associations	是的	是的	否
	EC2：中斷IamInstanceProfile	否	是的	否
解碼授權狀態訊息	STS:解碼授權訊息	是的	是的	否
說明帳戶可使用的指定映像（Amis）	EC2：取消影像	是的	是的	否
描述VPC中的路由表（僅HA配對需要）	EC2：取消功能表	是的	否	否
停止、啟動及監控執行個體	EC2：啟動安裝	是的	是的	否
	EC2：停止執行	是的	是的	否
	EC2：資料說明	是的	是的	否
	EC2：取消訂閱即時狀態	是的	是的	否
	EC2：RunInstances	是的	否	否
	EC2：終端安裝	否	否	是的
	EC2：修改實例屬性	否	是的	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
確認已針對支援的執行個體類型啟用增強式網路功能	EC2：取消訂閱實例屬性	否	是的	否
使 用「WorkingEnvironment」 和「WorkingEnvironmentId」標記來標記資源、這些標記用於維護和成本分配	EC2：建立標記	是的	是的	否
管理Cloud Volumes ONTAP EBS磁碟區、這些磁碟區可作為後端儲存設備使用	EC2：建立磁碟區	是的	是的	否
	EC2：減量磁碟區	是的	是的	是的
	EC2：修改Volume屬性	否	是的	是的
	EC2：AttachVolume	是的	是的	否
	EC2：刪除Volume	否	是的	是的
	EC2：分離Volume	否	是的	是的
建立及管理安全性群組Cloud Volumes ONTAP 以利執行	EC2：建立安全性群組	是的	否	否
	EC2：刪除安全性群組	否	是的	是的
	EC2：取消安全性群組	是的	是的	是的
	EC2 ：RevokeSecurityGroupEgress	是的	否	否
	EC2：授權安全性群組出口	是的	否	否
	EC2：授權安全性群組入口	是的	否	否
	EC2 ：RevokeSecurityGroupIngress	是的	是的	否
在Cloud Volumes ONTAP 目標子網路中建立及管理用於實現效能不中斷的網路介面	EC2：建立網路介面	是的	否	否
	EC2：網路介面	是的	是的	否
	EC2：刪除網路介面	否	是的	是的
	EC2：修改網路互連屬性	否	是的	否
取得目的地子網路和安全性群組清單	EC2：無資料子網路	是的	是的	否
	EC2：取消功能Vpcs	是的	是的	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
取得DNS伺服器和Cloud Volumes ONTAP 預設的網域名稱以供執行個體使用	EC2：取消功能DhcpOptions	是的	否	否
拍攝EBS Volume的快照Cloud Volumes ONTAP 以供其使用	EC2：建立Snapshot	是的	是的	否
	EC2：刪除Snapshot	否	是的	是的
	EC2：取消快照	否	是的	否
擷取Cloud Volumes ONTAP 附加於AutoSupport 資訊畫面的功能	EC2：GetConsole輸出	是的	是的	否
取得可用金鑰組的清單	EC2：評量會議	是的	否	否
取得可用AWS區域的清單	EC2：取消註冊	是的	是的	否
管理Cloud Volumes ONTAP 與實例相關的資源標記	EC2：刪除標記	否	是的	是的
	EC2：取消標示	否	是的	否
建立及管理AWS CloudForation範本的堆疊	雲端：建立堆疊	是的	否	否
	雲端：刪除堆疊	是的	否	否
	雲端：無標準堆疊	是的	是的	否
	雲端：取消功能堆疊事件	是的	否	否
	cloudformation：驗證範本	是的	否	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
建立並管理Cloud Volumes ONTAP S3儲存區、讓整個系統做為資料分層的容量層	S3：建立桶	是的	是的	否
	S3：刪除資源桶	否	是的	是的
	S3：Get生命 週期組態	否	是的	否
	S3：Putt升降 器組態	否	是的	否
	S3：PuttBucketting	否	是的	否
	S3：listBucketVerions	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：PuttBucketPublicAccessBlock	否	是的	否
	S3：GetBucketting	否	是的	否
	S3：GetBucketLocation	否	是的	否
	S3：ListAllMyb桶	否	否	否
	S3：清單庫	否	是的	否
使用Cloud Volumes ONTAP AWS金鑰管理服務（KMS）啟用資料加密功能	公里：清單*	是的	是的	否
	公里：ReEncrypt *	是的	否	否
	公里：描述*	是的	是的	否
	公里：建立授予	是的	是的	否
取得AWS成本資料Cloud Volumes ONTAP 以供使用	CE：GetReservationUtilization	否	是的	否
	CE：GetDimensionValues	否	是的	否
	CE：GetCostAndusage	否	是的	否
	CE：GetTags	否	是的	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
在單一AWS可用性區域中、為兩個HA節點建立並管理AWS分散放置群組、以及協調器	EC2：建立位置群組	是的	否	否
	EC2：刪除位置群組	否	是的	是的
建立報告	FSX：說明*	否	是的	否
	FSX：清單*	否	是的	否
建立及管理可支援Amazon EBS彈性Volume功能的集合體	EC2：說明體積修改	否	是的	否
	EC2：修改Volume	否	是的	否

全域檔案快取

Connector會在部署期間提出下列API要求、以部署全域檔案快取執行個體：

- 雲端：無標準堆疊
- cloudwatch：GetMetricStatistics
- 雲端：清單堆疊

Kubernetes

Connector會提出下列API要求、以探索及管理Amazon EKS叢集：

- EC2：取消註冊
- EKS：清單叢集
- EKS：取消叢集
- IAM：GetInstanceProfile

連接器的Azure權限

Cloud Manager在Azure中啟動Connector VM時、會將自訂角色附加至VM、讓Connector有權管理該Azure訂閱中的資源和程序。Connector會使用權限來撥打API呼叫數個Azure服務。

自訂角色權限

下列自訂角色提供Connector管理Azure網路中資源與程序所需的權限。

直接從Cloud Manager建立Connector時、Cloud Manager會自動將此自訂角色套用至Connector。

如果您從Azure Marketplace部署Connector、或是在Linux主機上手動安裝Connector、則必須自行設定自訂角色。

您也必須確保在後續版本中新增權限時、該角色是最新的。

```
{
    "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/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
                        "Microsoft.Network/loadBalancers/read",
                        "Microsoft.Network/loadBalancers/write",
                        "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",
```

```
"Microsoft.Network/loadBalancers/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/acti
on",

"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
                        "Microsoft.Network/privateEndpoints/read",
                        "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
                        "Microsoft.Network/virtualNetworks/join/action",
                        "Microsoft.Network/privateDnsZones/A/write",
                        "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
                        "Microsoft.Insights/Metrics/Read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Compute/virtualMachines/extensions/delete",

"Microsoft.Compute/virtualMachines/extensions/read",
                        "Microsoft.Compute/virtualMachines/delete",
```

```
                        "Microsoft.Network/networkInterfaces/delete",
                        "Microsoft.Network/networkSecurityGroups/delete",
                        "Microsoft.Resources/deployments/delete",
                        "Microsoft.Compute/diskEncryptionSets/read",
                        "Microsoft.Compute/snapshots/delete",
                        "Microsoft.Network/privateEndpoints/delete",
                        "Microsoft.Compute/availabilitySets/delete",
                        "Microsoft.Network/loadBalancers/delete",
                        "Microsoft.KeyVault/vaults/read",
                        "Microsoft.KeyVault/vaults/accessPolicies/write",
                        "Microsoft.Compute/diskEncryptionSets/write",
                        "Microsoft.KeyVault/vaults/deploy/action",
                        "Microsoft.Compute/diskEncryptionSets/delete",
                        "Microsoft.Resources/tags/read",
                        "Microsoft.Resources/tags/write",
                        "Microsoft.Resources/tags/delete",

"Microsoft.Network/applicationSecurityGroups/write",

"Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",

"Microsoft.Network/applicationSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Cloud Manager Permissions",
    "IsCustom": "true"
}
```

Azure權限的使用方式

行動	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" 、	建立 Cloud Volumes ONTAP 不同時停止、啟動、刪除及取得系統狀態。
「 Microsoft.Compute/images/write" 、 Microsoft.Compute/images/read" 、	可 Cloud Volumes ONTAP 從 VHD 進行支援功能性部署。
Microsoft.Compute/disks/delete" 、 "Microsoft.Compute/disks/read" 、 "Microsoft.Compute/disks/write" 、 "microsoft.Storage/checkamed可用 度 / 讀取 " 、 "microsoft.Storage/operations / 讀取 " 、 "Microsoft.Storage/storageAccounts/listkeys/action 、 "Microsoft.Storage/storageAccounts/read" 、 "Microsoft.Storage/storageAccounts/再生 金鑰 / 行動 " 、 "Microsoft.Storage/storageAccounts/write 、 "Microsoft.Storage/storageAccounts/storageAccounts/delete" 、 "Microsoft.Storage/改 用 / 讀取 " 、	管理 Azure 儲存帳戶和磁碟、並將磁碟附加 Cloud Volumes ONTAP 至
"Microsoft.Storage/storageAccounts/blobServices/contains/read"、"Microsoft.KeyVault/Vaults/read"、"Microsoft.KeyVault/Vaults/accessPolicys/write	可備份至Azure Blob儲存設備、並加密儲存帳戶
「 Microsoft.Network/networkInterfaces/read" 、 Microsoft.Network/networkInterfaces/write" 、「 Microsoft.Network/networkInterfaces/join/action" 、	建立並管理 Cloud Volumes ONTAP 目標子網路中的網路介面以供其使用。
「 Microsoft.Network/networkSecurityGroups/read" 、 Microsoft.Network/networkSecurityGroups/write" 、「 Microsoft.Network/networkSecurityGroups/join/action" 、	建立預先定義 Cloud Volumes ONTAP 的網路安全群組以供使用。
"Microsoft.Resources/訂購 / 位置 / 讀取 " 、 "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" 、	取得區域、目標 Vnet 和子網路的網路資訊、並將 Cloud Volumes ONTAP 之新增至 VNets 。

行動	目的
「 Microsoft.Network/virtualNetworks/subnets/write" 、 Microsoft.Network/routeTables/join/action" 、	啟用 vnet 服務端點以進行資料分層。
"microsoft.Resources/edes/operations / read" 、 "microsoft.Resources/edes/read" 、 "microsoft.Resources/edes/write 、	從 Cloud Volumes ONTAP 範本部署功能。
"microsoft.Resources/edations/operations/read" 、 "microsoft.Resources/edations/read" 、 "microsoft.Resources/dations/read" 、 "microsoft.Resources/read" 、 "microsoft.Resources/dations/operations/read" 、 "Microsoft.Resources / 訂閱 / 資源群組 / 刪除 " 、 "Microsoft.Resources / 訂閱 / 資源群組 / 讀取 " 、 "Microsoft.Resources / 訂閱 / 資源群組 / 資源 / 讀取 " 、 "Microsoft.Resources / 訂閱 / 資源群組 / 寫入 " 、	建立及管理 Cloud Volumes ONTAP 資源群組以供參考。
「Microsoft.Compute/snapshots/write"、Microsoft.Compute/snapshots/read"、「Microsoft.Compute/snapshots/delete"、Microsoft.Compute/disks/beginGetAccess/action"、	建立及管理 Azure 託管快照。
「 Microsoft.Compute/availabilitySets/write" 、 Microsoft.Compute/availabilitySets/read" 、	建立及管理 Cloud Volumes ONTAP 可用度集以供使用。
"Microsoft.MarketplaceOrdination/offersTypes /出版商/服務/方案/協議/讀取" 、"Microsoft.MarketplaceOrdinations/offersTypes /出版商/服務/計畫/協議/寫入"、	可從 Azure Marketplace 進行程式化部署。
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 Azure 負載平衡器以供 HA 配對使用。
"Microsoft.Authorization/Locks/*、	可管理 Azure 磁碟上的鎖定。
"Microsoft.Authorization/RoleDefinitions/write （ Microsoft 授權 / 角色指派 / 寫入） " 、 "Microsoft.Web/sites/* （ Microsoft 網站 / 網站 / * ） "	管理 HA 配對的容錯移轉。

行動	目的
Microsoft.Network/privateEndpoints/write" 、 "Microsoft.Storage/storageAccounts/privateEndpointConnectionsApproval / AC巨 集指令 " 、 "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" 、	可管理私有端點。未將連線提供給子網路外部時、會使用私有端點。Cloud Manager 會為 HA 建立儲存帳戶、但僅在子網路內建立內部連線功能。
「 Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete" 、	讓 Cloud Manager 能夠刪除 Volume 以 Azure NetApp Files 供使用。
"Microsoft.Resources / 部署 / 作業狀態 / 讀取 "	Azure 在某些虛擬機器部署中需要此權限（視部署期間所使用的基礎實體硬體而定）。
"microsoft.Resources/edes/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/edes/delete" 、	可讓您使用全域檔案快取。
「Microsoft.Network/privateEndpoints/delete"、Microsoft.Compute/availabilitySets/delete"、	可讓Cloud Manager在Cloud Volumes ONTAP 部署失敗或刪除時、從屬於支援的資源群組移除資源。
Microsoft.Compute/diskEncryptionSets/read"「Microsoft.Compute/diskEncryptionSets/write"」、「Microsoft.Compute/diskEncryptionSets/delete""microsoft.KeyVault/Vaults/Deploy / action 」、「microsoft.KeyVault/Vaults/read」、「microsoft.KeyVault/Vaults/accesss/write」、	可搭配Cloud Volumes ONTAP 使用客戶管理的加密金鑰。API 支援此功能。
"Microsoft.Resources/標記/讀取" 、"Microsoft.Resources/標記/寫入" 、"Microsoft.Resources/標記/刪除"	可讓您使用Cloud Manager標記服務來管理Azure資源上的標記。

行動	目的
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"	可讓Cloud Manager設定HA配對的應用程式安全群組、隔離HA互連和叢集網路NIC。

Connector的Google Cloud權限

Cloud Manager需要權限才能在Google Cloud中執行動作。這些權限包含在NetApp提供的自訂角色中。您可能想要瞭解 Cloud Manager 使用這些權限的功能。

服務帳戶權限

下方顯示的自訂角色提供Connector在Google Cloud網路中管理資源和程序所需的權限。

您必須將此自訂角色套用至連接器VM的服務帳戶。 "檢視逐步指示"。

您也必須確保在後續版本中新增權限時、該角色是最新的。

```
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
```

如何使用Google Cloud權限

行動	目的
- compute 、 disks.create - compute 、 disks.createSnapshot - compute.disks.delete - compute 、 disks.Get - compute 、 disks.list - compute.disks.setLabels - compute.disks.use	建立及管理 Cloud Volumes ONTAP 磁碟以供使用。
- compute 、防火牆、 create - compute.firewalls.delete - compute 、防火牆、 Get - compute 、防火牆、 list	建立 Cloud Volumes ONTAP 防火牆規則以供使用。
運算： globalOperations 。 Get	以取得作業狀態。
- compiler.images.Get - compile.images.getFromFamily - compile.images.list - compute.images.useReadOnly	取得 VM 執行個體的映像。
- compute.instances.attachDisk - compute.instances.detachDisk	可將磁碟安裝到 Cloud Volumes ONTAP 實體上、並將其拆離。

行動	目的
- compute.instances.create - compute.instances.delete	建立及刪除 Cloud Volumes ONTAP 不顯示的 VM 執行個體。
- compute.instances.get	列出 VM 執行個體。
- compute.instances.getSerialPortOutput	以取得主控台記錄。
- compute.instances.list	可檢索區域中的實例列表。
- compute.instances.setDeletionProtection	設定執行個體的刪除保護。
- compute.instances.setLabels	以新增標籤。
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	變更 Cloud Volumes ONTAP 機器類型以供使用。
- compute.instances.setMetadata	新增中繼資料。
- compute.instances.setTags	新增防火牆規則的標記。
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	開始和停止 Cloud Volumes ONTAP 功能。
- compute 。 machineTypes 。 Get	取得要檢查 qoutas 的核心數量。
- compute.projects.get	支援多個專案。
- compute 、 snapshots.create - compute.snapshots.delete - compute 、 snapshots.Get - compute 、 snapshots.list - compute.snapshots.setLabels	以建立及管理持續磁碟快照。
- compute.networks.get - compute.networks.list - compute .regions.Get - compute .regions.list - compute .subnetworks .Get - compute .subnetworks .list - compute .zonewores.Get - compute .zones.list	取得建立全新 Cloud Volumes ONTAP 的物件虛擬機器執行個體所需的網路資訊。
deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.in清單 - deploymentmanager.in清 - deploymentmanager.in清單 - deploymentmanager.operations - deploymentmanager.operations .list - deploymentmanager.separes.Get - deploymentmanager.operations - deploymentmanager.types.list - deploymentmanager.list	使用 Cloud Volumes ONTAP Google Cloud Deployment Manager 部署物件虛擬機器執行個體。
- logging.logEntries .list - logging.privateLogEntries .list	以取得堆疊記錄磁碟機。
- resourcemanager.projects.get	支援多個專案。

行動	目的
- storage 、 buckets 、 create - storage.buckets.delete - storage 、 buckets 、 storage 、 buckets 、 list - storage 、 buckets 、 update	建立及管理 Google Cloud Storage 儲存庫以進行資料分層。
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.Get - cloudkms.cryptoKeys.list - cloudkms.keycles.list	搭配 Cloud Volumes ONTAP 使用 Cloud Key Management Service 的客戶管理加密金鑰。
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - 儲存空間 .objects.Get - 儲存空間 .objects.list	在 Cloud Volumes ONTAP 整個過程中設定服務帳戶。此服務帳戶提供資料分層至 Google Cloud Storage 儲存庫的權限。
- compute 、 addresses.list - compute 、 backendServices.create - compute.networks.updatePolicy - compute 、 Region. 、 BackendServices.create - compute 、 Region. 、 BackendServices.list	部署 HA 配對。
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	以實現Cloud Data Sense。
- container。叢集。Get - container。叢集。清單	探索在Google Kubernetes Engine中執行的Kubernetes叢集。
- compute.instanceGroups.get - compute 、addresses.Get	在HA配對上建立及管理儲存VM。
-監控.timeSeries.list -儲存區.buckes.getIamPolicy	探索Google Cloud Storage儲存桶的相關資訊。