参照

Set up and administration

NetApp
July 18, 2022

目次

参照

Cloud Managerの権限の概要

Cloud Managerの機能やサービスを使用するには、Cloud Managerがクラウド環境で処理を実行できるように、権限を付与する必要があります。このページのリンクを使用して、目的に応じて必要な権限にすばやくアクセスできます。

AWS権限

目的	説明	リンク
コネクタの展開	Cloud Managerからコネクタを作成するユーザには、AWSにインスタンスを導入するための特定の権限が必要です。	"Cloud Manager から AWS にコネクタを作成します"
コネクタの動作	Cloud Managerでコネクタを起動すると、AWSアカウントのリソースとプロセスの管理に必要な権限を提供するポリシーがインスタンスに適用されます。その場合は、自分でポリシーを設定する必要があります "マーケットプレイスからコネクターを起動します" またはあなたの場合 "AWSクレデンシャルをコネクタに追加します"。また、新しい権限が以降のリリースで追加されるときに、ポリシーが最新の状態であることを確認する必要があります。	"Connector の AWS 権限"
Cloud Volumes ONTAP 処理	AWSの各Cloud Volumes ONTAP ノードにIAMロールを関連付ける必要があります。HAメディエーターについても同様です。デフォルトでは、Cloud ManagerでIAMロールを作成することもできますが、独自のIAMロールを使用することもできます。	"IAMロールを自分で設定する方法について説明します"

Azure権限

目的	説明	リンク
コネクタの展開	Cloud ManagerからConnectorを導入する場合は、Connector VMをAzureに導入する権限を持つAzureアカウントまたはサービスプリンシパルを使用する必要があります。	"Cloud Manager から Azure にコネクタを作成します"

目的	説明	リンク
コネクタの動作	Cloud ManagerがConnector VMをAzureに導入すると、そのAzureサブスクリプション内でリソースとプロセスを管理するために必要な権限を提供するカスタムロールが作成されます。 カスタムロールは自分で設定する必要があります "マーケットプレイスからコネクターを起動します" またはあなたの場合 "Azureクレデンシャルをコネクタに追加します"。 また、新しい権限が以降のリリースで追加されるときに、ポリシーが最新の状態であることを確認する必要があります。	"Connector の Azure 権限"

Google Cloud権限

目的	説明	リンク
コネクタの展開	Cloud ManagerからConnectorを導入するGoogle Cloudユーザには、Google CloudにConnectorを導入するための特定の権限が必要です。	"Connectorを展開する権限を設定します"
コネクタの動作	Connector VMインスタンスのサービスアカウントには、日常処理に対する特定の権限が必要です。サービスアカウントは、Cloud Managerから導入するときにコネクタに関連付ける必要があります。また、新しい権限が以降のリリースで追加されるときに、ポリシーが最新の状態であることを確認する必要があります。	"コネクタのサービスアカウントを設定します"

Connector の AWS 権限

Cloud ManagerでAWSでコネクタインスタンスを起動するときに、そのAWSアカウント内のリソースとプロセスを管理するための権限を提供するポリシーがインスタンスに関連付けられます。Connectorでは、権限を使用してAPI呼び出しを実行することで、EC2、S3、CloudFormation、IAM、 Key Management Service（KMS；キー管理サービス）など。

IAMポリシー

以下のIAMポリシーは、ConnectorがAWSリージョンに基づいてパブリッククラウド環境内のリソースとプロセスを管理するために必要な権限を提供します。

Cloud Managerからコネクタを直接作成すると、Cloud Managerはこのポリシーをコネクタに自動的に適用します。

AWS MarketplaceからConnectorを導入する場合や、LinuxホストにConnectorを手動でインストールする場合は、手動でポリシーを設定する必要があります。

また、新しい権限が以降のリリースで追加されるときに、ポリシーが最新の状態であることを確認する必要があります。

標準領域

```
{
  "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（US）リージョン

```
{
    "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権限の使用方法

以降のセクションでは、各ネットアップクラウドサービスに対する権限の使用方法について説明します。この情報は、企業のポリシーによって、必要な場合にのみアクセス許可が指定されるように指定されている場合に役立ちます。

AppTemplateタグ

AppTemplate Taggingサービスを使用する場合、Connectorは次のAPI要求を実行してAWSリソースのタグを管理します。

- ec2：CreateTags
- EC2:タグを削除します
- EC2: DescribeTags (説明タグ)
- Tag:getResources
- tag:getTagKeys
- tag:getTagValues
- Tag:タグリソース
- タグ: UntagResources

クラウドバックアップ

コネクタは、Cloud Backupのリストアインスタンスを導入するために次のAPI要求を実行します。

- EC2：StartInstances（EC2：開始インスタンス
- EC2：StopInstances
- EC2: DescribeInstances
- EC2: DescribeInstanceStatus
- EC2：RunInstances
- EC2：TerminateInstances
- EC2: DescribeInstanceAttributeのこと
- EC2: DescribeImages
- ec2：CreateTags
- EC2：CreateVolume
- EC2：CreateSecurityGroup
- EC2: DescribeSubnets
- EC2: DescribeVpcs
- EC2: DescribeRegions (説明領域
- CloudFormation：CreateStack
- CloudFormation：DeleteStack
- CloudFormation：DescribeStack

Connectorは、Amazon S3でバックアップを管理するために次のAPI要求を実行します。

- S3 ： GetBucketLocation
- S3 ： ListAllMyBuckets
- S3 ： ListBucket
- S3 ： CreateBucket を指定します
- S3 ： GetLifecycleConfiguration

- S3 ： PutLifecycleConfiguration
- S3 ： PutBucketTagging
- S3 ： ListBucketVersions
- S3 ： GetBucketAcl
- S3：PutBucketPublicAccessBlock
- KMS：リスト*
- KMS：説明*
- S3 ： GetObject
- ec2c:ディスクエンドポイントの説明
- KMS：エイリアスを確認する
- S3 ： PutEncryptionConfiguration

コネクタは、Search & Restoreメソッドを使用してボリュームとファイルをリストアする場合に次のAPI要求を実行します。

- S3 ： CreateBucket を指定します
- 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：StartQueryExecutionc
- Athena: GetQueryResults.
- Athena: GetQueryExecution
- Athena：StopQueryExecution
- グルー：データベースを作成します
- グルー: CreateTable
- グルー: BatchDeletePartition

クラウドデータの意味

Connectorは、Cloud Data Senseインスタンスを導入するために次のAPI要求を実行します。

- 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の作成
- EC2: DescribeRegions (説明領域
- CloudFormation：CreateStack
- CloudFormation：DeleteStack
- CloudFormation：DescribeStack
- CloudFormation：DescribeStackEvents
- IAM：AddRoleToInstanceProfile
- EC2: AssociateIamInstanceProfile
- EC2: DescribeIamInstanceProfileAssociations

Cloud Data Senseを使用している場合、コネクタはS3バケットのスキャンを行うために次のAPI要求を実行します。

- 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

クラウド階層化

Cloud Tieringを使用すると、ConnectorはAmazon S3へのデータの階層化を求める次のAPI要求を実行します。

アクション	セットアップに使用？	日々の業務に使用されるか？
S3 ： CreateBucket を指定します	はい。	いいえ
S3 ： PutLifecycleConfiguration	はい。	いいえ
S3 ： GetLifecycleConfiguration	はい。	はい。
EC2: DescribeRegions (説明領域	はい。	はい。

Cloud Volumes ONTAP

Connectorは、AWSでのCloud Volumes ONTAP の導入と管理に対して次のAPI要求を実行します。

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Cloud Volumes ONTAP インスタンスのIAMロールとインスタンスプロファイルを作成および管理します	IAM：ListInstanceProfiles	はい。	はい。	いいえ
	IAM：CREATEROLE	はい。	いいえ	いいえ
	IAM：DeleteRole	いいえ	はい。	はい。
	IAM：PutRolePolicy	はい。	いいえ	いいえ
	IAM：CreateInstanceProfile	はい。	いいえ	いいえ
	IAM：DeleteRolePolicy	いいえ	はい。	はい。
	IAM：AddRoleToInstanceProfile	はい。	いいえ	いいえ
	IAM：RemoveRoleFromInstanceProfile	いいえ	はい。	はい。
	IAM：DeleteInstanceProfile	いいえ	はい。	はい。
	IAM：PassRole	はい。	いいえ	いいえ
	EC2: AssociateIamInstanceProfile	はい。	はい。	いいえ
	EC2: DescribeIamInstanceProfileAssociations	はい。	はい。	いいえ
	EC2: DisassociateIamInstanceProfile	いいえ	はい。	いいえ
読み取り許可ステータスメッセージ	STS: DecodeAuthorizationMessage	はい。	はい。	いいえ
アカウントで使用可能な指定イメージ（AMIS）について説明します	EC2: DescribeImages	はい。	はい。	いいえ
VPC内のルーティングテーブルの説明（HAペアの場合のみ必要）	EC2: DescribeRouteTables	はい。	いいえ	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
インスタンスの停止、開始、監視	EC2：StartInstances（EC2：開始インスタンス	はい。	はい。	いいえ
	EC2：StopInstances	はい。	はい。	いいえ
	EC2: DescribeInstances	はい。	はい。	いいえ
	EC2: DescribeInstanceStatus	はい。	はい。	いいえ
	EC2：RunInstances	はい。	いいえ	いいえ
	EC2 ：TerminateInstances	いいえ	いいえ	はい。
	EC2 ：ModifyInstanceAttribute	いいえ	はい。	いいえ
サポートされるインスタンスタイプに対して拡張ネットワークが有効になっていることを確認します	EC2: DescribeInstanceAttributeのこと	いいえ	はい。	いいえ
メンテナンスとコストの割り当てに使用する「WorkingEnvironment」タグと「WorkingEnvironmentId」タグを使用してリソースにタグを付けます	ec2：CreateTags	はい。	はい。	いいえ
Cloud Volumes ONTAP がバックエンドストレージとして使用するEBSボリュームを管理します	EC2：CreateVolume	はい。	はい。	いいえ
	EC2: DescribeVolumesの場合	はい。	はい。	はい。
	EC2 ：ModifyVolumeAttributeのことです	いいえ	はい。	はい。
	EC2：AttachVolume	はい。	はい。	いいえ
	EC2：DeleteVolume	いいえ	はい。	はい。
	EC2 ：DetachVolumeの場合	いいえ	はい。	はい。

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Cloud Volumes ONTAP のセキュリティグループを作成および管理します	EC2 ：CreateSecurityGroup	はい。	いいえ	いいえ
	EC2: DeleteSecurityGroup	いいえ	はい。	はい。
	EC2: DescribeSecurityGroups	はい。	はい。	はい。
	EC2: RevokeSecurityGroupEgress	はい。	いいえ	いいえ
	ec2 ：AuthorizeSecurityGroupEgress	はい。	いいえ	いいえ
	ec2 ：AuthorizeSecurityGroupIngress	はい。	いいえ	いいえ
	EC2: RevokeSecurityGroupIngress	はい。	はい。	いいえ
ターゲットサブネットのCloud Volumes ONTAP のネットワークインターフェイスを作成および管理します	EC2 ：CreateNetworkInterface	はい。	いいえ	いいえ
	EC2: DescribeNetworkInterfaces	はい。	はい。	いいえ
	EC2 ：DeleteNetworkInterface	いいえ	はい。	はい。
	EC2:ModifyNetworkInterfaceAttributeのいずれかです	いいえ	はい。	いいえ
デスティネーションのサブネットとセキュリティグループの一覧を取得します	EC2: DescribeSubnets	はい。	はい。	いいえ
	EC2: DescribeVpcs	はい。	はい。	いいえ
Cloud Volumes ONTAP インスタンスのDNSサーバおよびデフォルトのドメイン名を取得します	EC2: DescribeDhcpOptions	はい。	いいえ	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Cloud Volumes ONTAP 用のEBSボリュームのSnapshotを作成します	EC2: CreateSnapshotの作成	はい。	はい。	いいえ
	EC2 ：DeleteSnapshot	いいえ	はい。	はい。
	ec2: DescribeSnapshots	いいえ	はい。	いいえ
AutoSupport メッセージに添付されているCloud Volumes ONTAP コンソールをキャプチャします	EC2: GetConsoleOutput	はい。	はい。	いいえ
使用可能なキーペアのリストを取得します	EC2 ：DescribeKeyPairs	はい。	いいえ	いいえ
使用可能なAWSリージョンのリストを取得します	EC2: DescribeRegions (説明領域	はい。	はい。	いいえ
Cloud Volumes ONTAP インスタンスに関連付けられたリソースのタグを管理します	EC2:タグを削除します	いいえ	はい。	はい。
	EC2: DescribeTags (説明タグ)	いいえ	はい。	いいえ
AWS CloudFormationテンプレートのスタックの作成と管理	CloudFormation ：CreateStack	はい。	いいえ	いいえ
	CloudFormation ：DeleteStack	はい。	いいえ	いいえ
	CloudFormation ：DescribeStack	はい。	はい。	いいえ
	CloudFormation ：DescribeStackEvents	はい。	いいえ	いいえ
	CloudFormation ：ValidateTemplate	はい。	いいえ	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Cloud Volumes ONTAP システムでデータ階層として使用するS3バケットを作成および管理します	S3 ： CreateBucket を指定します	はい。	はい。	いいえ
	S3 ： DeleteBucket	いいえ	はい。	はい。
	S3 ： GetLifecycleConfiguration	いいえ	はい。	いいえ
	S3 ： PutLifecycleConfiguration	いいえ	はい。	いいえ
	S3 ： PutBucketTagging	いいえ	はい。	いいえ
	S3 ： ListBucketVersions	いいえ	はい。	いいえ
	S3 ：GetBucketPolicyStatus	いいえ	はい。	いいえ
	S3 ：GetBucketPublicAccessBlock	いいえ	はい。	いいえ
	S3 ： GetBucketAcl	いいえ	はい。	いいえ
	S3 ： GetBucketPolicy	いいえ	はい。	いいえ
	S3 ：PutBucketPublicAccessBlock	いいえ	はい。	いいえ
	S3 ： GetBucketTagging	いいえ	はい。	いいえ
	S3 ： GetBucketLocation	いいえ	はい。	いいえ
	S3 ： ListAllMyBuckets	いいえ	いいえ	いいえ
	S3 ： ListBucket	いいえ	はい。	いいえ
AWS Key Management Service（KMS；キー管理サービス）を使用してCloud Volumes ONTAP のデータ暗号化を有効にする	KMS：リスト*	はい。	はい。	いいえ
	KMS：再暗号化*	はい。	いいえ	いいえ
	KMS：説明*	はい。	はい。	いいえ
	KMS：CreateGrant	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
AWSからCloud Volumes ONTAP のコストデータを取得	CE ：GetReservationUtilization	いいえ	はい。	いいえ
	CE ：GetDimensionValues	いいえ	はい。	いいえ
	CE ：GetCostAndUsage	いいえ	はい。	いいえ
	CE: GetTags.	いいえ	はい。	いいえ
2つのHAノードとメディエーター用のAWS分散配置グループを1つのAWSアベイラビリティゾーンに作成して管理します	EC2 ：CreatePlacementGroup	はい。	いいえ	いいえ
	EC2: DeletePlacementGroup	いいえ	はい。	はい。
レポートを作成します	FSx：説明*	いいえ	はい。	いいえ
	FSx：リスト*	いいえ	はい。	いいえ
Amazon EBS Elastic Volumes機能をサポートするアグリゲートを作成して管理します	EC2: DescribeVolumesModifications (EC2 : DescribeVolumesMod	いいえ	はい。	いいえ
	EC2：ModifyVolume	いいえ	はい。	いいえ

グローバルファイルキャッシュ

このコネクタは、導入時にグローバルファイルキャッシュインスタンスを導入するために次のAPI要求を行います。

- CloudFormation：DescribeStack
- CloudWatch：GetMetricStatistics
- CloudFormation：リストスタック

Kubernetes

コネクタは、次のAPI要求を実行してAmazon EKSクラスタを検出および管理します。

- EC2: DescribeRegions (説明領域
- EKS：リストクラスタ
- EKS：DescribeCluster
- IAM：GetInstanceProfile

Connector の Azure 権限

Cloud ManagerがAzureでConnector VMを起動すると、そのVMにAzureサブスクリプション内のリソースとプロセスを管理するための権限を付与するカスタムロールが割り当てられます。Connectorは、権限を使用して複数のAzureサービスに対してAPI呼び出しを実行します。

カスタムロールの権限

以下のカスタムロールには、Azureネットワーク内のリソースとプロセスを管理するためにConnectorで必要となる権限が含まれています。

Cloud Managerからコネクタを直接作成すると、Cloud Managerはこのカスタムロールをコネクタに自動的に適用します。

Azure MarketplaceからConnectorを導入する場合、またはLinuxホストにConnectorを手動でインストールする場合は、カスタムロールを自分で設定する必要があります。

また、新しい権限が以降のリリースで追加されるときに、ロールが最新の状態であることを確認する必要があります。

```
{
    "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権限の使用方法

アクション	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" 」、	Cloud Volumes ONTAP を作成し、システムのステータスを停止、開始、削除、取得します。
「 microsoft.compute/images/write 」、「 microsoft.compute/images/read 」、	VHD から Cloud Volumes ONTAP を導入できます。
Microsoft.Compute/disks/delete" 、 Microsoft.Compute/disks/read" 、 Microsoft.Compute/disks/write" 、 "Microsoft.Storage/checknameavailability/read" 、 "Microsoft.Storage/operations/read" 、 "microsoft.StorageAccounts/listkeyss/action" 、 "microsoft.Storage/storageAccounts/read" 、 "microsoft.Storage/regenerateAccounts/action" 、 "Microsoft.Storage/storageAccounts/action" 、 "/writeStorageAccounts" 、 "/StorageAccounts/StorageAccounts/write/StorageAccounts" 、 ","Microsoft 。	Azure ストレージアカウントとディスクを管理し、ディスクを Cloud Volumes ONTAP に接続します。
"microsoft.StorageAccounts/blobServices/containers/read" 、 "microsoft.KeyVault/vaults/read" 、 "microsoft.KeyVault/vaults/accessPolicies/write"	Azure BLOB ストレージへのバックアップとストレージアカウントの暗号化を有効にします
「 microsoft.network/networkinterfaces/read 」、「 microsoft.network/networkinterfaces/write 」、「 microsoft.network/networkinterfaces/join/action 」、	ターゲットサブネット内の Cloud Volumes ONTAP のネットワークインターフェイスを作成および管理します。

アクション	目的
「 microsoft.network/networksecuritygroups/read 」、「 microsoft.network/networksecuritygroups/write 」、「 microsoft.network/networksecuritygroups/join/action 」、	Cloud Volumes ONTAP 用の定義済みネットワークセキュリティグループを作成します。
「 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" 」、	リージョン、ターゲット VNet 、およびサブネットに関するネットワーク情報を取得し、 vnet に Cloud Volumes ONTAP を追加します。
「 Microsoft.Network/virtualNetworks/subnets/write" 」、 Microsoft.Network/routeTables/join/action" 、	データ階層化のための VNet サービスエンドポイントを有効にします。
「 Microsoft.Resources/Deployments/Operations/Read 」、「 Microsoft.Resources/Deployments/Read 」、「 Microsoft.Resources/Deployments/Write 」、	テンプレートから Cloud Volumes ONTAP を導入します。
"microsoft.Resources/Deployments/operations/read" 、 "microsoft.Resources/Deployments/read" 、 "microsoft.Resources/resources/read" 、 "microsoft.resources/resources/operationresults/read" 、 "microsoft.resources/Subscriptions /resourceGroups/delete" 、 "microsoft.resources/Subscriptions /resources/groups/resources/resources/reads/resources/resources/resources/resources/resources/resources/reading" 、 ","","","","resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/groups/	Cloud Volumes ONTAP のリソースグループを作成および管理します。
「 Microsoft.Compute/snapshots/write" 」、「 Microsoft.Compute/snapshots/read" 」、「 Microsoft.Compute/snapshots/delete" 」、「 Microsoft.Compute/disks/beginGetAccess/action" 」、	Azure マネージドスナップショットを作成および管理します。
"microsoft.compute/availabilitySets/write", "microsoft.compute/availabilitySets/read",	Cloud Volumes ONTAP の可用性セットを作成および管理します。

アクション	目的
"Microsoft.MarketplaceOrdering/Offered Types/publishers/capers/plans/agreements/read" 、 "Microsoft.MarketplaceOrdering / offerTypes/publishers/capes/plans/agreements/write"	Azure Marketplace からのプログラムによる展開を可能にします。
「 Microsoft.Network/loadBalancers/read" 」、「 Microsoft.Network/loadBalancers/write" 」、「 Microsoft.Network/loadBalancers/delete" 」、「 Microsoft.Network/loadBalancers/backendAddressPools/read" 」、「 Microsoft.Network/loadBalancers/backendAddressPools/join/action" 」、「 Microsoft.Network/loadBalancers/frontendIPConfigurations/read" 」、「 Microsoft.Network/loadBalancers/loadBalancingRules/read" 」、「 Microsoft.Network/loadBalancers/probes/read" 」、「 Microsoft.Network/loadBalancers/probes/join/action" 」	HA ペアの Azure ロードバランサを管理します。
"Microsoft 許可 / ロック /*"	Azure ディスクのロックの管理を有効にします。
"Microsoft.Authorization/roleDefinites/write" 、 "Microsoft.Authorization/rolrolわり あて /write" 、 "Microsoft.Web/sites/*"	HA ペアのフェイルオーバーを管理します。
「 Microsoft.Network/privateEndpoints/write" 」、「 Microsoft.StorageAccounts/PrivateEndpointConnectionsApproval/action 」、「 microsoft.Storage/storageAccounts/privateEndpointConnections/read 」、「 Microsoft.Network/privateEndpoints/read" 」、「 Microsoft.Network/privateDnsZones/write" 」、「 Microsoft.Network/privateDnsZones/virtualNetworkLinks/write" 」、「 Microsoft.Network/privateDnsZones/A/write" 」、「 Microsoft.Network/privateDnsZones/virtualNetworkLinks/read" 」、「 Microsoft.Network/privateDnsZones/read" 」、「 Microsoft.Network/virtualNetworks/join/action" 」、「 」、「 」、「 」、「 」	プライベートエンドポイントの管理をイネーブルにします。プライベートエンドポイントは、サブネットの外部への接続が提供されない場合に使用されます。Cloud Manager は、サブネット内で内部接続のみを使用して HA 用のストレージアカウントを作成します。
" Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete" 、	Azure NetApp Files のボリュームを Cloud Manager で削除できます。
"microsoft.Resources/Deployments/operationStatuses/read"	Azure では、一部の仮想マシン環境に対してこの権限が必要です（導入時に使用する基盤となる物理ハードウェアによって異なります）。

アクション	目的
"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" 、	グローバルファイルキャッシュを使用できます。
「 Microsoft.Network/privateEndpoints/delete" 」、 Microsoft.Compute/availabilitySets/delete" 、	導入の失敗や削除が発生した場合に、 Cloud Manager が Cloud Volumes ONTAP に属するリソースグループからリソースを削除できるようにします。
「 Microsoft.Compute/diskEncryptionSets/read" 」 Microsoft.Compute/diskEncryptionSets/write" 、「 Microsoft.Compute/diskEncryptionSets/delete" 」「 microsoft.KeyVaults/vaults/deploy/action 」、「 microsoft.KeyVault/vaults/read 」、「 microsoft.KeyVaults/accessPolicies/write 」、	Cloud Volumes ONTAP で、お客様が管理する暗号化キーの使用を有効にします。この機能は API を使用してサポートされます。
"microsoft.Resources/tags/read" 、 "microsoft.Resources/tags/write" 、 "microsoft.Resources/tags/delete"	Cloud Manager Tagging サービスを使用して、 Azure リソースのタグを管理できます。
「 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"	Cloud Manager で HA ペアのアプリケーションセキュリティグループを設定できるため、 HA インターコネクトとクラスタネットワークの NIC が分離されます。

Connector の Google Cloud 権限

Cloud ManagerでGoogle Cloudの処理を実行するには権限が必要です。これらの権限は、ネットアップが提供するカスタムロールに含まれています。このような権限を持つ Cloud Manager の機能を理解しておく必要があるかもしれません。

サービスアカウントの権限

次のカスタムロールは、ConnectorがGoogle Cloudネットワーク内のリソースとプロセスを管理するために必要な権限を提供します。

このカスタムロールは、Connector VMに関連付けられているサービスアカウントに適用する必要がありま

す。 "ステップバイステップの手順を確認します"。

また、新しい権限が以降のリリースで追加されるときに、ロールが最新の状態であることを確認する必要があります。

```
title: NetApp Cloud Manager
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
```

```
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
```

```
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
```

Google Cloud権限の使用方法

アクション	目的
-compute.disks .create -computedisks .createsnapshot - compute.disks.delete -computedisks .get-compute.diskList - compute.disks.setLabels - compute.disks.us	Cloud Volumes ONTAP 用のディスクを作成および管理します。
-compute-firewalls .create - compute.firewalls.delete -comput領域 .firewalls .get-comput領域 .firewalls リスト	Cloud Volumes ONTAP のファイアウォールルールを作成します。
-computer.globalOperationsGet	処理のステータスを確認できます。
-compute.image.get-compute.image.getFromFamily -compute.image.list - compute.images.useReadOnly	VM インスタンスのイメージを取得します。
- compute.instances.attachDisk - compute.instances.detachDisk	ディスクを Cloud Volumes ONTAP に接続して接続解除します。
- compute.instances.create - compute.instances.delete	Cloud Volumes ONTAP VM インスタンスを作成および削除します。
- compute.instances.get	VM インスタンスを一覧表示します。
- compute.instances.getSerialPortOutput	をクリックしてコンソールログを取得してください
- compute.instances.list	ゾーン内のインスタンスのリストを取得します。
- compute.instances.setDeletionProtection	インスタンスに削除保護を設定します。
- compute.instances.setLabels	ラベルを追加します。
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	Cloud Volumes ONTAP のマシンタイプを変更します。
- compute.instances.setMetadata	をクリックしてください。
- compute.instances.setTags	ファイアウォールルールのタグを追加します。
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Cloud Volumes ONTAP を開始および停止します。
-computesCompute .machineTypes.get	コア数を取得して qoutas をチェックしてください。
- compute.projects.get	複数のプロジェクトをサポートするため。

アクション	目的
-compute-snapshots-create - compute.snapshots.delete -compute-snapshots -getCompute-snapshots-list - compute.snapshots.setLabels	永続ディスクスナップショットを作成および管理するには、次の手順に従います。
- compute.networks.get - compute.networks.list - comput.regions.Get-comput領域 .list-comput領域 .subnetworks -compute.subnetworks .listCompute.zoneOperations-get-compute.zones .get-compute.zones リスト	新しい Cloud Volumes ONTAP 仮想マシンインスタンスの作成に必要なネットワーク情報を取得するため。
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list -deploymentmanager. マニフェスト .get-deploymentmanager. マニフェスト .list-list-deploymentmanager. operations-get-deploymentmanager. operationlist -deploymentmanager. resources.get-deploymentmanager. resources.list-deploymentmanager. typeProviders.get-deploymentmanager. typeProviders.list-deploymentmanager. -deploymentmanager. types] リスト	Google Cloud Deployment Manager を使用して Cloud Volumes ONTAP 仮想マシンインスタンスを導入します。
-logging.logEntries.list-logging.privateLogEntries.list	スタックログドライブを取得する方法
- resourcemanager.projects.get	複数のプロジェクトをサポートするため。
-storagバケット 。 create - storage.buckets.delete -storagバケット .get-storagバケット .list-storagバケット .buckets-update	Google Cloud Storage バケットを作成して管理し、データを階層化します。
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms .cryptoKeys.get-cloudkms .cryptoKeys.list-cloudkm.keyringlist.list	Cloud Volumes ONTAP でクラウドキー管理サービスからお客様が管理する暗号化キーを使用するため。
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects-get -storage.objectlist	Cloud Volumes ONTAP インスタンスにサービスアカウントを設定します。このサービスアカウントは、Google Cloud Storage バケットへのデータ階層化の権限を提供します。
-compute.address.listCompute.backendServices. create -compute.networks.updatePolicy -compute.regionBackendServices.create -compute.regionBackendServices.get -compute.regionBackendServices.list	をクリックしてください。
- compute.subnetworks.us e-compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	クラウドデータの意味を有効にするため。

アクション	目的
-container-type コンテナクラスタリスト	Google Kubernetes Engine で実行されている Kubernetes クラスタを検出する。
- compute.instanceGroups.get - compute .address.get	HAペアでStorage VMを作成および管理する。
-monitoring timeseries.list -storage.buckets -getIamPolicyを選択します	をクリックして、Google Cloud Storageバケットに関する情報を確認してください。