云提供商代理权限和网络要求

NetApp Console setup and administration

NetApp
March 03, 2026

目录

云提供商代理权限和网络要求

NetApp Console的权限摘要

您需要为控制台代理提供适当的权限，以便它可以在您的云环境中执行操作。使用此页面上的链接，您可以根据目标快速访问所需的权限。

AWS 权限

NetApp Console需要控制台代理和各个服务的 AWS 权限。

控制台代理

目标	描述	链路
从控制台部署控制台代理 要在 AWS 中部署控制台代理，用户需要特定的权限。	"设置 AWS 权限"	为控制台代理提供权限

NetApp Backup and Recovery

目标	描述	链路
使用NetApp Backup and Recovery将本地ONTAP集群备份到 Amazon S3	在ONTAP卷上激活备份时， NetApp Backup and Recovery会提示您输入具有特定权限的 IAM 用户的访问密钥和密码。	"设置备份的 S3 权限"

Cloud Volumes ONTAP

目标	描述	链路
为Cloud Volumes ONTAP节点提供权限	必须将 IAM 角色附加到 AWS 中的每个Cloud Volumes ONTAP节点。对于 HA 调解员来说也是如此。默认选项是让控制台为您创建 IAM 角色，但您可以在控制台中创建系统时使用自己的角色。	"了解如何自行设置 IAM 角色"

NetApp Copy and Sync

目标	描述	链路
在 AWS 中部署数据代理	用于部署数据代理的 AWS 用户账户必须具有所需的权限。	"在 AWS 中部署数据代理所需的权限"
为数据经纪人提供权限	当NetApp Copy and Sync部署数据代理时，它会为数据代理实例创建一个 IAM 角色。如果您愿意，您可以使用自己的 IAM 角色部署数据代理。	"使用您自己的 IAM 角色与 AWS 数据代理的要求"
为手动安装的数据代理启用 AWS 访问	如果您使用包含 S3 存储桶的同步关系的数据代理，那么您应该准备好 Linux 主机以供 AWS 访问。安装数据代理时，您需要为具有编程访问权限和特定权限的 IAM 用户提供 AWS 密钥。	"启用对 AWS 的访问"

适用于**ONTAP**的 **FSx**

目标	描述	链路
创建和管理 FSx for ONTAP	要创建或管理Amazon FSx for NetApp ONTAP系统，您需要通过提供 IAM 角色的 ARN（为控制台提供所需的权限）将 AWS 凭证添加到控制台。	"了解如何为 FSx 设置 AWS 凭证"

NetApp Cloud Tiering

目标	描述	链路
将本地ONTAP集群分层到 Amazon S3	启用NetApp Cloud Tiering到 AWS 时，您需要输入访问密钥和秘密密钥。这些凭证将传递给ONTAP集群，以便ONTAP可以将数据分层存储到 S3 存储桶中。	"设置 S3 分层权限"

Azure 权限

控制台需要控制台代理和各个服务的 Azure 权限。

控制台代理

目标	描述	链路
从控制台部署控制台代理	从控制台部署控制台代理时，您需要使用具有在 Azure 中部署控制台代理 VM 的权限的 Azure 帐户或服务主体。	"设置 Azure 权限"
为控制台代理提供权限	当控制台在 Azure 中部署控制台代理 VM 时，它会创建一个自定义角色，该角色提供管理该 Azure 订阅中的资源和流程所需的权限。 如果您从市场启动控制台代理，如果您手动安装控制台代理，或者如果您"向控制台代理添加更多 Azure 凭据"。 随着后续版本添加新的权限，请及时更新策略。	"控制台代理的 Azure 权限"

NetApp Backup and Recovery

目标	描述	链路
将Cloud Volumes ONTAP备份到 Azure Blob 存储	使用NetApp Backup and Recovery备份Cloud Volumes ONTAP时，您需要在以下情况下向控制台代理添加权限： • 您想使用“搜索和恢复”功能 • 您想要使用客户管理的加密密钥 (CMEK)	• "使用备份和恢复将Cloud Volumes ONTAP数据备份到 Azure Blob 存储"
将本地ONTAP集群备份到 Azure Blob 存储	使用NetApp Backup and Recovery备份本地ONTAP集群时，需要向控制台代理添加权限才能使用“搜索和恢复”功能。	"使用备份和恢复将本地ONTAP数据备份到 Azure Blob 存储"

NetApp复制和同步

目标	描述	链路
在 Azure 中部署数据代理	用于部署数据代理的 Azure 用户帐户必须具有所需的权限。	"在 Azure 中部署数据代理所需的权限"

Google Cloud 权限

控制台需要控制台代理和各个服务的 Google Cloud 权限。

控制台代理

目标	描述	链路
从控制台部署控制台代理	从控制台部署控制台代理的 Google Cloud 用户需要特定权限才能在 Google Cloud 中部署控制台代理。	"设置权限以创建控制台代理"
为控制台代理提供权限	控制台代理的服务帐户必须具有日常操作所需的特定权限。部署期间需要将服务帐户与控制台代理关联。随着后续版本添加新的权限，请及时更新策略。	"设置控制台代理的权限"

NetApp Backup and Recovery

目标	描述	链路
将Cloud Volumes ONTAP备份到 Google Cloud	使用NetApp Backup and Recovery备份Cloud Volumes ONTAP时，您需要在以下情况下向控制台代理添加权限： • 您想使用“搜索和恢复”功能 • 您想要使用客户管理的加密密钥 (CMEK)	• "使用备份和恢复将Cloud Volumes ONTAP数据备份到 Google Cloud Storage" • "CMEK 的权限"
将本地ONTAP集群备份到 Google Cloud	使用NetApp Backup and Recovery备份本地ONTAP集群时，需要向控制台代理添加权限才能使用“搜索和恢复”功能。	"使用备份和恢复将本地ONTAP数据备份到 Google Cloud Storage"

NetApp Copy and Sync

目标	描述	链路
在 Google Cloud 中部署数据代理	确保部署数据代理的 Google Cloud 用户具有所需的权限。	"在 Google Cloud 中部署数据代理所需的权限"
为手动安装的数据代理启用 Google Cloud 访问权限	如果您计划使用包含 Google Cloud Storage 存储桶的同步关系的数据代理，那么您应该准备 Linux 主机以供 Google Cloud 访问。安装数据代理时，您需要为具有特定权限的服务帐户提供密钥。	"启用对 Google Cloud 的访问"

StorageGRID权限

控制台需要两项服务的StorageGRID权限。

NetApp Backup and Recovery

目标	描述	链路
将本地ONTAP集群备份到StorageGRID	当您准备将StorageGRID作为ONTAP集群的备份目标时， NetApp Backup and Recovery会提示您输入具有特定权限的 IAM 用户的访问密钥和密码。	"准备StorageGRID作为备份目标"

NetApp Cloud Tiering

目标	描述	链路
将本地ONTAP集群分层到StorageGRID	当您将NetApp Cloud Tiering设置为StorageGRID时，您需要向 Cloud Tiering 提供 S3 访问密钥和密钥。云分层使用密钥来访问您的存储桶。	"准备分层到StorageGRID"

AWS 代理权限和安全规则

控制台代理的 AWS 权限

当NetApp Console在 AWS 中启动控制台代理时，它会将一个策略附加到该代理，该策略为代理提供管理该 AWS 账户内的资源和流程的权限。代理使用权限对多个 AWS 服务进行 API 调用，包括 EC2、S3、CloudFormation、IAM、密钥管理服务 (KMS) 等。

IAM 策略

下面提供的 IAM 策略提供了控制台代理根据您的 AWS 区域管理公共云环境内的资源和流程所需的权限。

请注意以下事项：

- 如果直接从控制台在标准 AWS 区域中创建控制台代理，控制台会自动将策略应用于该代理。
- 如果您从 AWS Marketplace 部署代理、在 Linux 主机上手动安装代理或者想要向控制台添加其他 AWS 凭证，则需要自行设置策略。
- 无论哪种情况，您都需要确保策略是最新的，因为在后续版本中添加了新的权限。如果需要新的权限，它们将在发行说明中列出。
- 如果需要，您可以使用 IAM 限制 IAM 策略 `Condition`元素。 "AWS 文档：条件元素"
- 要查看使用这些策略的分步说明，请参阅以下页面：
  - "设置 AWS Marketplace 部署的权限"
  - "设置本地部署的权限"
  - "设置限制模式的权限"
  - "设置专用模式的权限"

选择您所在的地区以查看所需的政策：

标准区域

对于标准区域，权限分布在两个策略中。由于 AWS 中托管策略的最大字符大小限制，因此需要两个策略。

政策 **#1**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "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",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:CreatePlacementGroup",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateRoute",
        "ec2:DescribeVpcs",
```

```
        "ec2:ReplaceRoute",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:DeleteRoute",
        "ec2:DeletePlacementGroup",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:ModifyVolume",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ListStacks",
        "cloudformation:ValidateTemplate",
        "cloudformation:DeleteStack",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:ListInstanceProfiles",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DeleteInstanceProfile",
        "iam:GetRolePolicy",
        "iam:GetRole",
        "sts:DecodeAuthorizationMessage",
        "sts:AssumeRole",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutObject",
```

```
            "s3:ListAllMyBuckets",
            "s3:GetObject",
            "s3:GetEncryptionConfiguration",
            "kms:ReEncrypt*",
            "kms:CreateGrant",
            "fsx:Describe*",
            "fsx:List*",
            "kms:GenerateDataKeyWithoutPlaintext"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "cvoServicePolicy"
    },
    {
        "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",
            "ec2:DescribeVpcEndpoints",
            "kms:ListAliases",
            "glue:GetDatabase",
            "glue:GetTable",
            "glue:GetPartitions"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "backupPolicy"
    },
    {
        "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",
            "s3:GetObjectVersionTagging",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectRetention",
            "s3:GetObjectTagging",
            "s3:GetObjectVersion",
            "s3:PutObjectVersionTagging",
            "s3:PutObjectRetention",
            "s3:DeleteObjectTagging",
            "s3:DeleteObjectVersionTagging",
            "s3:GetBucketObjectLockConfiguration",
            "s3:GetBucketVersioning",
            "s3:PutBucketObjectLockConfiguration",
            "s3:PutBucketVersioning",
            "s3:BypassGovernanceRetention",
            "s3:PutBucketPolicy",
            "s3:PutBucketOwnershipControls"
        ],
        "Resource": [
            "arn:aws:s3:::netapp-backup-*"
        ],
        "Effect": "Allow",
        "Sid": "backupS3Policy"
    },
    {
        "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*"
        ],
        "Effect": "Allow",
        "Sid": "fabricPoolS3Policy"
    },
    {
        "Action": [
            "ec2:DescribeRegions"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "fabricPoolPolicy"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/netapp-adc-manager": "*"
            }
        },
        "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Effect": "Allow"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Action": [
```

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

政策 **#2**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "tagServicePolicy"
    }
  ]
}
```

GovCloud（美国）区域

```
{
  "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:ListStacks",
        "cloudformation:ValidateTemplate",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:CreateBucket",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "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/*"
      ]
    }
  ]
}
```

秘密区域

```
{
  "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:ListStacks",
        "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",
        "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-b: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-b:ec2:*:*:instance/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-iso-b:ec2:*:*:volume/*"
        ]
    }
  ]
}
```

绝密地区

```
{
  "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:ListStacks",
        "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",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListinstanceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
      ],
      "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
```

```
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Resource": [
            "arn:aws-iso:ec2:*:*:instance/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-iso:ec2:*:*:volume/*"
        ]
    }
  ]
}
```

如何使用 **AWS** 权限

以下部分介绍了如何使用每个NetApp Console管理或数据服务的权限。如果您的公司政策规定仅在需要时提供权限，则此信息会很有帮助。

适用于**ONTAP** 的**Amazon FSx**

控制台代理发出以下 API 请求来管理Amazon FSx for ONTAP文件系统：

- ec2:描述实例
- ec2：描述实例状态
- ec2:描述实例属性
- ec2:描述路由表
- ec2:描述图像
- ec2:创建标签
- ec2:描述卷
- ec2:描述安全组
- ec2:描述网络接口

- ec2:描述子网
- ec2:描述Vpcs
- ec2:描述DHCP选项
- ec2:描述快照
- ec2:描述密钥对
- ec2:描述区域
- ec2:描述标签
- ec2：描述IamInstanceProfileAssociations
- ec2:描述预留实例产品
- ec2:描述Vpc端点
- ec2:描述Vpcs
- ec2：描述卷修改
- ec2:描述放置组
- kms:创建授权
- kms：列出别名
- fsx:描述*
- fsx:列表*

Amazon S3 存储桶发现

控制台代理发出以下 API 请求来发现 Amazon S3 存储桶：

s3:获取加密配置

NetApp Backup and Recovery

该代理发出以下 API 请求来管理 Amazon S3 中的备份：

- s3：获取存储桶位置
- s3：列出所有我的存储桶
- s3：列表桶
- s3：创建桶
- s3:获取生命周期配置
- s3：PutLifecycle配置
- s3：PutBucket标记
- s3：列出存储桶版本
- s3：获取存储桶Acl
- s3：PutBucket公共访问块
- s3：获取对象

- ec2:描述Vpc端点
- kms：列出别名
- s3：PutEncryption配置

当您使用搜索和还原方法还原卷和文件时，代理会发出以下 API 请求：

- s3：创建桶
- s3：删除对象
- s3：删除对象版本
- s3：获取存储桶Acl
- s3：列表桶
- s3：列出存储桶版本
- s3：列出桶多部分上传
- s3：Put对象
- s3:PutBucketAcl
- s3：PutLifecycle配置
- s3：PutBucket公共访问块
- s3：中止分段上传
- s3:列出多部分上传部分

当您使用 DataLock 和NetApp Ransomware Resilience进行卷备份时，代理会发出以下 API 请求：

- s3:获取对象版本标记
- s3：获取存储桶对象锁配置
- s3:获取对象版本Acl
- s3：PutObjectTagging
- s3：删除对象
- s3：删除对象标记
- s3：获取对象保留
- s3：删除对象版本标记
- s3：Put对象
- s3：获取对象
- s3:PutBucketObjectLock配置
- s3:获取生命周期配置
- s3：按标签列出存储桶
- s3：获取存储桶标记
- s3：删除对象版本

- s3：列出存储桶版本
- s3：列表桶
- s3：PutBucket标记
- s3:获取对象标记
- s3：PutBucket版本控制
- s3：PutObjectVersionTagging
- s3：获取存储桶版本
- s3：获取存储桶Acl
- s3：绕过治理保留
- s3：PutObjectRetention
- s3：获取存储桶位置
- s3：获取对象版本

如果您对Cloud Volumes ONTAP备份使用的 AWS 账户与对源卷使用的账户不同，则代理会发出以下 API 请求：

- s3：PutBucket策略
- s3：PutBucket所有权控制

备份和恢复的旧版权限

如果您在索引版本 v2 发布之前启用了旧版索引功能，则只需要以下权限：

- kms:列表*
- kms:描述*
- athena：开始查询执行
- 雅典娜：获取查询结果
- 雅典娜：获取查询执行
- athena：停止查询执行
- 胶水：创建数据库
- 胶水：创建表
- 胶水：批量删除分区

NetApp Data Classification

代理发出以下 API 请求来部署NetApp Data Classification：

- ec2:描述实例
- ec2：描述实例状态
- ec2：运行实例

- ec2：终止实例
- ec2:创建标签
- ec2：创建卷
- ec2：附加卷
- ec2：创建安全组
- ec2：删除安全组
- ec2:描述安全组
- ec2:创建网络接口
- ec2:描述网络接口
- ec2:删除网络接口
- ec2:描述子网
- ec2:描述Vpcs
- ec2：创建快照
- ec2:描述区域
- cloudformation:创建堆栈
- cloudformation:删除堆栈
- cloudformation:描述Stacks
- cloudformation：描述堆栈事件
- cloudformation：ListStacks
- iam:添加角色到实例配置文件
- ec2:AssociateIamInstanceProfile
- ec2：描述IamInstanceProfileAssociations

当您使用NetApp Data Classification时，代理会发出以下 API 请求来扫描 S3 存储桶：

- iam:添加角色到实例配置文件
- ec2:AssociateIamInstanceProfile
- ec2：描述IamInstanceProfileAssociations
- s3：获取存储桶标记
- s3：获取存储桶位置
- s3：列出所有我的存储桶
- s3：列表桶
- s3：获取存储桶策略状态
- s3：获取存储桶策略
- s3：获取存储桶Acl
- s3：获取对象

- iam：获取角色
- s3：删除对象
- s3：删除对象版本
- s3：Put对象
- sts：AssumeRole

Cloud Volumes ONTAP

该代理发出以下 API 请求以在 AWS 中部署和管理Cloud Volumes ONTAP 。

目的	操作	用于部署?	用于日常运营?	用于删除?
为Cloud Volumes ONTAP实例创建和管理 IAM 角色和实例配置文件	iam:列出实例配置文件	是	是	否
	iam：创建角色	是	否	否
	iam：删除角色	否	是	是
	iam:PutRolePolicy	是	否	否
	iam:创建实例配置文件	是	否	否
	iam:删除角色策略	否	是	是
	iam:添加角色到实例配置文件	是	否	否
	iam:从实例配置文件中删除角色	否	是	是
	iam:删除实例配置文件	否	是	是
	iam：PassRole	是	否	否
	ec2:AssociateIamInstanceProfile	是	是	否
	ec2：描述IamInstanceProfileAssociations	是	是	否
	ec2：解除关联IamInstanceProfile	否	是	否
解码授权状态消息	sts：解码授权消息	是	是	否
描述账户可用的指定镜像（AMI）	ec2:描述图像	是	是	否
描述 VPC 中的路由表（仅 HA 对需要）	ec2:描述路由表	是	否	否

目的	操作	用于部署?	用于日常运营?	用于删除?
停止、启动和监控实例	ec2：启动实例	是	是	否
	ec2：停止实例	是	是	否
	ec2:描述实例	是	是	否
	ec2：描述实例状态	是	是	否
	ec2：运行实例	是	否	否
	ec2：终止实例	否	否	是
	ec2:修改实例属性	否	是	否
验证是否为受支持的实例类型启用了增强联网	ec2:描述实例属性	否	是	否
使用“WorkingEnvironment”和“WorkingEnvironmentId”标签标记资源，用于维护和成本分配	ec2:创建标签	是	是	否
管理Cloud Volumes ONTAP用作后端存储的 EBS 卷	ec2：创建卷	是	是	否
	ec2:描述卷	是	是	是
	ec2:修改卷属性	否	是	是
	ec2：附加卷	是	是	否
	ec2：删除卷	否	是	是
	ec2：分离卷	否	是	是
为Cloud Volumes ONTAP创建和管理安全组	ec2：创建安全组	是	否	否
	ec2：删除安全组	否	是	是
	ec2:描述安全组	是	是	是
	ec2：撤销安全组出口	是	否	否
	ec2：授权安全组出口	是	否	否
	ec2：授权安全组入口	是	否	否
	ec2：撤销安全组入口	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
在目标子网中创建和管理Cloud Volumes ONTAP的网络接口	ec2:创建网络接口	是	否	否
	ec2:描述网络接口	是	是	否
	ec2:删除网络接口	否	是	是
	ec2:修改网络接口属性	否	是	否
获取目标子网和安全组列表	ec2:描述子网	是	是	否
	ec2:描述Vpcs	是	是	否
获取Cloud Volumes ONTAP实例的 DNS 服务器和默认域名	ec2:描述DHCP选项	是	否	否
为Cloud Volumes ONTAP拍摄 EBS 卷快照	ec2：创建快照	是	是	否
	ec2：删除快照	否	是	是
	ec2:描述快照	否	是	否
捕获Cloud Volumes ONTAP控制台，该控制台附加到AutoSupport消息	ec2：获取控制台输出	是	是	否
获取可用密钥对列表	ec2:描述密钥对	是	否	否
获取可用 AWS 区域列表	ec2:描述区域	是	是	否
管理与Cloud Volumes ONTAP实例关联的资源的标签	ec2:删除标签	否	是	是
	ec2:描述标签	否	是	否
创建和管理 AWS CloudFormation 模板的堆栈	cloudformation:创建堆栈	是	否	否
	cloudformation:删除堆栈	是	否	否
	cloudformation:描述Stacks	是	是	否
	cloudformation：描述堆栈事件	是	否	否
	云信息：验证模板	是	否	否

目的	操作	用于部署?	用于日常运营?	用于删除?
创建和管理Cloud Volumes ONTAP系统用作数据分层容量层的 S3 存储桶	s3：创建桶	是	是	否
	s3：删除桶	否	是	是
	s3:获取生命周期配置	否	是	否
	s3：PutLifecycle配置	否	是	否
	s3：PutBucket标记	否	是	否
	s3：列出存储桶版本	否	是	否
	s3：获取存储桶策略状态	否	是	否
	s3：获取存储桶公共访问块	否	是	否
	s3：获取存储桶Acl	否	是	否
	s3：获取存储桶策略	否	是	否
	s3：PutBucket公共访问块	否	是	否
	s3：获取存储桶标记	否	是	否
	s3：获取存储桶位置	否	是	否
	s3：列出所有我的存储桶	否	否	否
	s3：列表桶	否	是	否
使用 AWS 密钥管理服务 (KMS) 启用Cloud Volumes ONTAP的数据加密	kms:重新加密*	是	否	否
	kms:创建授权	是	是	否
	kms:生成不带明文的数据密钥	是	是	否
在单个 AWS 可用区中为两个 HA 节点和中介器创建和管理 AWS 扩展置放群组	ec2:创建放置组	是	否	否
	ec2:删除放置组	否	是	是
创建报告	fsx:描述*	否	是	否
	fsx:列表*	否	是	否
创建和管理支持 Amazon EBS 弹性卷功能的聚合	ec2：描述卷修改	否	是	否
	ec2：修改卷	否	是	否
检查可用区是否为 AWS 本地区域，并验证所有部署参数是否兼容	ec2：描述可用区域	是	否	是

更改日志

当添加和删除权限时，我们会在下面的部分中注明。

2026 年 **2** 月 **24** 日

数据分类现在需要以下权限：

cloudformation：ListStacks

2025年**11**月**11**日

除非您使用旧版索引，否则NetApp Backup and Recovery不再需要以下权限。这些权限已从本页面的策略中移除：

- kms:列表*
- kms:描述*
- athena：开始查询执行
- 雅典娜：获取查询结果
- 雅典娜：获取查询执行
- athena：停止查询执行
- 胶水：创建数据库
- 胶水：创建表
- 胶水：批量删除分区

2024年**9**月**9**日

由于NetApp Console不再支持NetApp边缘缓存以及 Kubernetes 集群的发现和管理，因此从标准区域的策略 #2 中删除了权限。

查看从策略中删除的权限

```
{
    "Action": [
        "ec2:DescribeRegions",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "iam:GetInstanceProfile"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "K8sServicePolicy"
},
{
    "Action": [
        "cloudformation:DescribeStacks",
        "cloudwatch:GetMetricStatistics",
        "cloudformation:ListStacks"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "GFCservicePolicy"
},
{
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/GFCInstance": "*"
        }
    },
    "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Effect": "Allow"
}
```

2024年5月9日

Cloud Volumes ONTAP现在需要以下权限：

ec2：描述可用区域

2023年6月6日

Cloud Volumes ONTAP现在需要以下权限：

kms:生成不带明文的数据密钥

2023年2月14日

NetApp Cloud Tiering现在需要以下权限：

ec2:描述Vpc端点

AWS 中的控制台代理安全组规则

代理的 AWS 安全组需要入站和出站规则。当您从控制台创建控制台代理时， NetApp Console会自动创建此安全组。您需要为所有其他安装选项设置此安全组。

入站规则

协议	端口	目的
SSH	22	提供对代理主机的 SSH 访问
HTTP	80	• 提供从客户端 Web 浏览器到本地用户界面的 HTTP 访问 • 在Cloud Volumes ONTAP升级过程中使用
HTTPS	443	提供对本地用户界面的 HTTPS 访问以及来自NetApp Data Classification实例的连接
TCP	3128	为Cloud Volumes ONTAP提供互联网访问。部署后您必须手动打开此端口。

出站规则

代理的预定义安全组打开所有出站流量。如果可以接受，请遵循基本的出站规则。如果您需要更严格的规则，请使用高级出站规则。

基本出站规则

代理的预定义安全组包括以下出站规则。

协议	端口	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开代理出站通信所需的端口

源IP地址是代理主机。

服务	协议	端口	目标	目的
API 调用 和AutoSupport	HTTPS	443	出站互联网 和ONTAP集群管理 LIF	对 AWS、 ONTAP、 NetApp Data Classification的API 调用，以及向NetApp 发送AutoSupport消 息
API 调用	TCP	3000	ONTAP HA 调解器	与ONTAP HA 调解器 的通信
	TCP	8080	数据分类	部署期间探测数据分 类实例
DNS	UDP	53	DNS	用于控制台的 DNS 解析

Azure 权限和所需安全规则

控制台代理的 Azure 权限

当NetApp Console在 Azure 中启动控制台代理时，它会将一个自定义角色附加到 VM，该 VM 为代理提供管理该 Azure 订阅中的资源和流程的权限。代理使用权限对多个 Azure 服务进行 API 调用。

是否需要为代理创建此自定义角色取决于您如何部署它。

从NetApp Console部署

当您使用控制台在 Azure 中部署代理虚拟机时，它会启用 "系统分配的托管标识"在虚拟机上，创建自定义角色，并将其分配给虚拟机。该角色为控制台提供管理该 Azure 订阅内的资源和流程所需的权限。当代理升级时，角色的权限保持最新。您不需要为代理创建此角色或管理更新。

手动部署或从 Azure 市场部署

当您从 Azure 市场部署代理或在 Linux 主机上手动安装代理时，您需要自行设置自定义角色并在任何更改时维护其权限。

您需要确保角色是最新的，因为后续版本中会添加新的权限。如果需要新的权限，它们将在发行说明中列出。

- 要查看使用这些策略的分步说明，请参阅以下页面：
  - "设置 Azure 市场部署的权限"
  - "设置本地部署的权限"
  - "设置限制模式的权限"
  - "设置专用模式的权限"

```
{
  "Name": "Console 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/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/write",
    "Microsoft.Storage/storageAccounts/blobServices/containers/read",
```

```
    "Microsoft.Storage/storageAccounts/listAccountSas/action",
    "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/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.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",
    "Microsoft.Synapse/workspaces/write",
    "Microsoft.Synapse/workspaces/read",
    "Microsoft.Synapse/workspaces/delete",
    "Microsoft.Synapse/register/action",
    "Microsoft.Synapse/checkNameAvailability/action",
    "Microsoft.Synapse/workspaces/operationStatuses/read",
    "Microsoft.Synapse/workspaces/firewallRules/read",
    "Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",
    "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
    "Microsoft.Compute/images/write",
    "Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
    "Microsoft.Compute/virtualMachineScaleSets/write",
    "Microsoft.Compute/virtualMachineScaleSets/read",
    "Microsoft.Compute/virtualMachineScaleSets/delete"
  ],
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Console Permissions",
  "IsCustom": "true"
```

```
}
```

如何使用 **Azure** 权限

以下部分介绍了如何对每个NetApp存储系统和数据服务使用权限。如果您的公司政策规定仅在需要时提供权限，则此信息会很有帮助。

Azure NetApp Files

当您使用NetApp Data Classification扫描Azure NetApp Files数据时，代理会发出以下 API 请求：

- NetApp。NetApp /netAppAccounts/read
- NetApp。NetApp /netAppAccounts/capacityPools/read
- NetApp/netAppAccounts/capacityPools/volumes/write
- NetApp/netAppAccounts/capacityPools/volumes/read
- NetApp/netAppAccounts/capacityPools/volumes/delete

NetApp Backup and Recovery

以下各节描述了NetApp Backup and Recovery如何使用权限。

NetApp Backup and Recovery权限

控制台代理会发出以下 API 请求以实现基本的NetApp Backup and Recovery功能：

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/读取
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/订阅/位置/读取
- Microsoft.Resources/订阅/资源组/读取
- Microsoft.Resources/订阅/资源组/资源/读取
- Microsoft.Resources/订阅/资源组/写入
- Microsoft.Storage/storageAccounts/managementPolicies/读取
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

以下是用于备份和恢复的自定义策略，它使用的权限最少，范围也最窄：

```
{
  "id":
"/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/roleDef
initions/{roleDefinitionGuid}",
  "properties": {
    "roleName": "Custom Role",
    "description": "Minimal permissions required for Backup and
Recovery.",
    "assignableScopes": [
      "/subscriptions/{subscriptionId}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}/providers/Microsoft.Storage/storageAccounts/
{storageAccountNameWithObjectLockPreprovisioned}"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/storageAccounts/listkeys/action",
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
          "Microsoft.Storage/storageAccounts/listAccountSas/action",
          "Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
          "Microsoft.Resources/subscriptions/resourceGroups/write",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/write",
          "Microsoft.Authorization/locks/write",
          "Microsoft.Authorization/locks/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

高级备份和恢复权限

控制台代理发出以下 API 请求，以实现高级备份和恢复操作以及搜索和恢复功能。这些权限允许管理网络、密钥库和受管身份：

- Microsoft.KeyVault/保管库/访问策略/写入
- Microsoft.KeyVault/保管库/读取
- Microsoft.ManagedIdentity/userAssignedIdentities/分配/操作
- Microsoft.Network/networkInterfaces/删除
- Microsoft.Network/网络接口/读取
- Microsoft.Network/networkSecurityGroups/删除
- Microsoft.Network/privateDnsZones/读取
- Microsoft.Network/privateDnsZones/写入
- Microsoft.Network/privateEndpoints/读取
- Microsoft.Network/privateEndpoints/写入
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Resources/部署/删除

备份和恢复的旧版权限

当您使用搜索和恢复功能时，代理会发出以下 API 请求。只有在 2025 年 2 月索引版本 v2 发布之前启用了旧版索引功能，才需要这些权限：

- Microsoft.Synapse/工作区/写入
- Microsoft.Synapse/工作区/读取
- Microsoft.Synapse/工作区/删除
- Microsoft.Synapse/注册/操作
- Microsoft.Synapse/checkNameAvailability/操作
- Microsoft.Synapse/工作区/operationStatuses/读取
- Microsoft.Synapse/工作区/防火墙规则/读取
- Microsoft.Synapse/工作区/replaceAllIpFirewallRules/操作
- Microsoft.Synapse/工作区/操作结果/读取
- Microsoft.Synapse/工作区/privateEndpointConnectionsApproval/操作

NetApp Data Classification

当您使用数据分类时，代理会发出以下 API 请求。

操作	用于设置吗?	用于日常运营?
Microsoft.Compute/位置/操作/读取	是	是

操作	用于设置吗?	用于日常运营?
Microsoft.Compute/位置/vmSizes/读取	是	是
Microsoft.Compute/操作/读取	是	是
Microsoft.Compute/virtualMachines/instanceView/读取	是	是
Microsoft.Compute/virtualMachines/powerOff/action	是	否
Microsoft.Compute/虚拟机/读取	是	是
Microsoft.Compute/虚拟机/重启/操作	是	否
Microsoft.Compute/virtualMachines/启动/操作	是	否
Microsoft.Compute/virtualMachines/vmSizes/读取	否	是
Microsoft.Compute/虚拟机/写入	是	否
Microsoft.Compute/图像/读取	是	是
Microsoft.Compute/磁盘/删除	是	否
Microsoft.Compute/磁盘/读取	是	是
Microsoft.Compute/磁盘/写入	是	否
Microsoft.Storage/checknameavailability/读取	是	是
Microsoft.Storage/操作/读取	是	是
Microsoft.Storage/storageAccounts/listkeys/action	是	否
Microsoft.Storage/storageAccounts/读取	是	是
Microsoft.Storage/storageAccounts/write	是	否
Microsoft.Storage/storageAccounts/blobServices/containers/read	是	是
Microsoft.Network/网络接口/读取	是	是
Microsoft.Network/网络接口/写入	是	否
Microsoft.Network/networkInterfaces/join/action	是	否
Microsoft.Network/networkSecurityGroups/读取	是	是
Microsoft.Network/networkSecurityGroups/写入	是	否

操作	用于设置吗?	用于日常运营?
Microsoft.Resources/订阅/位置/读取	是	是
Microsoft.Network/locations/operationResults/read	是	是
Microsoft.Network/位置/操作/读取	是	是
Microsoft.Network/virtualNetworks/读取	是	是
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/读取	是	是
Microsoft.Network/virtualNetworks/子网/读取	是	是
Microsoft.Network/virtualNetworks/子网/virtualMachines/读取	是	是
Microsoft.Network/virtualNetworks/virtualMachines/读取	是	是
Microsoft.Network/virtualNetworks/子网/加入/操作	是	否
Microsoft.Network/virtualNetworks/子网/写入	是	否
Microsoft.Network/routeTables/join/action	是	否
Microsoft.Resources/部署/操作/读取	是	是
Microsoft.Resources/部署/读取	是	是
Microsoft.Resources/部署/写入	是	否
Microsoft.Resources/资源/读取	是	是
Microsoft.Resources/subscriptions/operationresults/read	是	是
Microsoft.Resources/subscriptions/resourceGroups/delete	是	否
Microsoft.Resources/订阅/资源组/读取	是	是
Microsoft.Resources/订阅/资源组/资源/读取	是	是
Microsoft.Resources/订阅/资源组/写入	是	否

Cloud Volumes ONTAP

该代理发出以下 API 请求以在 Azure 中部署和管理Cloud Volumes ONTAP 。

目的	操作	用于部署?	用于日常运营?	用于删除?
创建和管理虚拟机	Microsoft.Compute/位置/操作/读取	是	是	否
	Microsoft.Compute/位置/vmSizes/读取	是	是	否
	Microsoft.Resources/订阅/位置/读取	是	否	否
	Microsoft.Compute/操作/读取	是	是	否
	Microsoft.Compute/virtualMachines/instanceView/读取	是	是	否
	Microsoft.Compute/virtualMachines/powerOff/action	是	是	否
	Microsoft.Compute/虚拟机/读取	是	是	否
	Microsoft.Compute/虚拟机/重启/操作	是	是	否
	Microsoft.Compute/virtualMachines/启动/操作	是	是	否
	Microsoft.Compute/virtualMachines/解除分配/操作	否	是	是
	Microsoft.Compute/virtualMachines/vmSizes/读取	否	是	否
	Microsoft.Compute/虚拟机/写入	是	是	否
	Microsoft.Compute/虚拟机/删除	是	是	是
	Microsoft.Resources/部署/删除	是	否	否
启用从 VHD 部署	Microsoft.Compute/图像/读取	是	否	否
	Microsoft.Compute/图像/写入	是	否	否

目的	操作	用于部署?	用于日常运营?	用于删除?
在目标子网中创建和管理网络接口	Microsoft.Network/网络接口/读取	是	是	否
	Microsoft.Network/网络接口/写入	是	是	否
	Microsoft.Network/networkInterfaces/join/action	是	是	否
	Microsoft.Network/networkInterfaces/删除	是	是	否
创建和管理网络安全组	Microsoft.Network/networkSecurityGroups/读取	是	是	否
	Microsoft.Network/networkSecurityGroups/写入	是	是	否
	Microsoft.Network/networkSecurityGroups/加入/操作	是	否	否
	Microsoft.Network/networkSecurityGroups/删除	否	是	是

目的	操作	用于部署?	用于日常运营?	用于删除?
获取有关区域、目标 VNet 和子网的网络信息，并将 VM 添加到 VNet	Microsoft.Network/locations/operationResults/read	是	是	否
	Microsoft.Network/位置/操作/读取	是	是	否
	Microsoft.Network/virtualNetworks/读取	是	否	否
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/读取	是	否	否
	Microsoft.Network/virtualNetworks/子网/读取	是	是	否
	Microsoft.Network/virtualNetworks/子网/virtualMachines/读取	是	是	否
	Microsoft.Network/virtualNetworks/virtualMachines/读取	是	是	否
	Microsoft.Network/virtualNetworks/子网/加入/操作	是	是	否
创建和管理资源组	Microsoft.Resources/部署/操作/读取	是	是	否
	Microsoft.Resources/部署/读取	是	是	否
	Microsoft.Resources/部署/写入	是	是	否
	Microsoft.Resources/资源/读取	是	是	否
	Microsoft.Resources/subscriptions/operationresults/read	是	是	否
	Microsoft.Resources/subscriptions/resourceGroups/delete	是	是	是
	Microsoft.Resources/订阅/资源组/读取	否	是	否
	Microsoft.Resources/订阅/资源组/资源/读取	是	是	否
	Microsoft.Resources/订阅/资源组/写入	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
管理 Azure 存储帐户和磁盘	Microsoft.Compute/磁盘/读取	是	是	是
	Microsoft.Compute/磁盘/写入	是	是	否
	Microsoft.Compute/磁盘/删除	是	是	是
	Microsoft.Storage/checknameavailability/读取	是	是	否
	Microsoft.Storage/操作/读取	是	是	否
	Microsoft.Storage/storageAccounts/listkeys/action	是	是	否
	Microsoft.Storage/storageAccounts/读取	是	是	否
	Microsoft.Storage/storageAccounts/删除	否	是	是
	Microsoft.Storage/storageAccounts/write	是	是	否
	Microsoft.Storage/使用情况/读取	否	是	否
启用 Blob 存储备份和存储帐户加密	Microsoft.Storage/storageAccounts/blobServices/containers/read	是	是	否
	Microsoft.KeyVault/保管库/读取	是	是	否
	Microsoft.KeyVault/保管库/访问策略/写入	是	是	否
启用 VNet 服务终结点以进行数据分层	Microsoft.Network/virtualNetworks/子网/写入	是	是	否
	Microsoft.Network/routeTables/join/action	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
创建和管理 Azure 托管快照	Microsoft.Compute/快照/写入	是	是	否
	Microsoft.Compute/快照/读取	是	是	否
	Microsoft.Compute/快照/删除	否	是	是
	Microsoft.Compute/磁盘/beginGetAccess/操作	否	是	否
创建和管理可用性集	Microsoft.Compute/可用性集/写入	是	否	否
	Microsoft.Compute/可用性集/读取	是	否	否
启用来自市场的程序化部署	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read	是	否	否
	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
管理 HA 对的负载均衡器	Microsoft.Network/loadBalancers/读取	是	是	否
	Microsoft.Network/loadBalancers/写入	是	否	否
	Microsoft.Network/loadBalancers/删除	否	是	是
	Microsoft.Network/loadBalancers/backendAddressPools/读取	是	否	否
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	是	否	否
	Microsoft.Network/loadBalancers/frontendIPConfigurations/读取	是	是	否
	Microsoft.Network/loadBalancers/loadBalancingRules/读取	是	否	否
	Microsoft.Network/loadBalancers/探测/读取	是	否	否
	Microsoft.Network/loadBalancers/探测/加入/操作	是	否	否
启用 Azure 磁盘上的锁管理	Microsoft.授权/锁/*	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
当子网外部没有连接时，为 HA 对启用专用端点	Microsoft.Network/privateEndpoints/写入	是	是	否
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	是	否	否
	Microsoft.Storage/storageAccounts/privateEndpointConnections/读取	是	是	是
	Microsoft.Network/privateEndpoints/读取	是	是	是
	Microsoft.Network/privateDnsZones/写入	是	是	否
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/写入	是	是	否
	Microsoft.Network/virtualNetworks/join/action	是	是	否
	Microsoft.Network/privateDnsZones/A/写入	是	是	否
	Microsoft.Network/privateDnsZones/读取	是	是	否
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/读取	是	是	否
对于某些虚拟机部署是必需的，具体取决于底层物理硬件	Microsoft.Resources/deployments/operationStatuses/read	是	是	否
在部署失败或删除的情况下从资源组中删除资源	Microsoft.Network/privateEndpoints/删除	是	是	否
	Microsoft.Compute/可用性集/删除	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
使用 API 时启用客户管理的加密密钥	Microsoft.Compute/diskEncryptionSets/读取	是	是	是
	Microsoft.Compute/diskEncryptionSets/写入	是	是	否
	Microsoft.KeyVault/保管库/部署/操作	是	否	否
	Microsoft.Compute/diskEncryptionSets/删除	是	是	是
为 HA 对配置应用程序安全组，以隔离 HA 互连和集群网络 NIC	Microsoft.Network/applicationSecurityGroups/写入	否	是	否
	Microsoft.Network/applicationSecurityGroups/读取	否	是	否
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	否	是	否
	Microsoft.Network/networkSecurityGroups/securityRules/写入	是	是	否
	Microsoft.Network/applicationSecurityGroups/删除	否	是	是
	Microsoft.Network/networkSecurityGroups/securityRules/删除	否	是	是
读取、写入和删除与Cloud Volumes ONTAP资源关联的标签	Microsoft.Resources/标签/阅读	否	是	否
	Microsoft.Resources/标签/写入	是	是	否
	Microsoft.Resources/标签/删除	是	否	否
在创建期间加密存储帐户	Microsoft.ManagedIdentity/userAssignedIdentities/分配/操作	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
在灵活编排模式下使用虚拟机规模集来为Cloud Volumes ONTAP指定特定区域	Microsoft.Compute/virtualMachineScaleSets/写入	是	否	否
	Microsoft.Compute/virtualMachineScaleSets/读取	是	否	否
	Microsoft.Compute/virtualMachineScaleSets/删除	否	否	是

分层

当您设置NetApp Cloud Tiering时，代理会发出以下 API 请求。

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/订阅/资源组/读取
- Microsoft.Resources/订阅/位置/读取

控制台代理针对日常操作发出以下 API 请求。

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/managementPolicies/读取
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Storage/storageAccounts/读取

更改日志

当添加和删除权限时，我们会在下面的部分中注明。

2025年**11**月**11**日

添加了一个自定义 JSON 策略，该策略体现了尽可能少的权限和尽可能小的范围。

以下权限已添加到最小备份和恢复权限列表中：

- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

除非您使用的是旧版索引，否则备份和恢复不再需要以下权限：

- Microsoft.Synapse/工作区/写入
- Microsoft.Synapse/工作区/读取
- Microsoft.Synapse/工作区/删除
- Microsoft.Synapse/注册/操作
- Microsoft.Synapse/checkNameAvailability/操作

- Microsoft.Synapse/工作区/operationStatuses/读取
- Microsoft.Synapse/工作区/防火墙规则/读取
- Microsoft.Synapse/工作区/replaceAllIpFirewallRules/操作
- Microsoft.Synapse/工作区/操作结果/读取
- Microsoft.Synapse/工作区/privateEndpointConnectionsApproval/操作

以下权限已移至“其他备份和恢复权限”部分，因为最小配置不需要这些权限：

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/读取
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/订阅/位置/读取
- Microsoft.Resources/订阅/资源组/读取
- Microsoft.Resources/订阅/资源组/资源/读取
- Microsoft.Resources/订阅/资源组/写入
- Microsoft.Storage/storageAccounts/managementPolicies/读取
- Microsoft.Storage/storageAccounts/managementPolicies/write

2024年9月9日

由于控制台不再支持发现和管理 Kubernetes 集群，因此从 JSON 策略中删除了以下权限：

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/操作
- Microsoft.ContainerService/managedClusters/读取

2024年8月22日

以下权限已添加到 JSON 策略中，因为它们是Cloud Volumes ONTAP支持虚拟机规模集所必需的：

- Microsoft.Compute/virtualMachineScaleSets/写入
- Microsoft.Compute/virtualMachineScaleSets/读取
- Microsoft.Compute/virtualMachineScaleSets/删除

2023年12月5日

将卷数据备份到 Azure Blob 存储时， NetApp Backup and Recovery不再需要以下权限：

- Microsoft.Compute/虚拟机/读取
- Microsoft.Compute/virtualMachines/启动/操作
- Microsoft.Compute/virtualMachines/解除分配/操作

- Microsoft.Compute/virtualMachines/扩展/删除
- Microsoft.Compute/虚拟机/删除

其他控制台存储服务需要这些权限，因此如果您使用其他存储服务，它们仍将保留在代理的自定义角色中。

2023年5月12日

以下权限已添加到 JSON 策略，因为它们是Cloud Volumes ONTAP管理所必需的：

- Microsoft.Compute/图像/写入
- Microsoft.Network/loadBalancers/frontendIPConfigurations/读取

以下权限已从 JSON 策略中删除，因为不再需要它们：

- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.Network/publicIPAddresses/删除

2023年3月23日

数据分类不再需要“Microsoft.Storage/storageAccounts/delete”权限。

Cloud Volumes ONTAP仍然需要此权限。

2023年1月5日

以下权限已添加到 JSON 策略：

- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Synapse/工作区/privateEndpointConnectionsApproval/操作

  NetApp Backup and Recovery需要这些权限。

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

  Cloud Volumes ONTAP部署需要此权限。

Azure 中的控制台代理安全组规则

代理的 Azure 安全组需要入站和出站规则。当您从控制台创建控制台代理时， NetApp Console会自动创建此安全组。对于其他安装选项，您需要手动设置此安全组。

入站规则

协议	端口	目的
SSH	22	提供对代理主机的 SSH 访问

协议	端口	目的
HTTP	80	• 提供从客户端 Web 浏览器到本地用户界面的 HTTP 访问 • 在Cloud Volumes ONTAP升级过程中使用
HTTPS	443	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问，以及来自NetApp Data Classification实例的连接
TCP	3128	为Cloud Volumes ONTAP提供互联网访问权限，以便将AutoSupport消息发送给NetApp支持。部署后您必须手动打开此端口。 "了解如何将代理用作AutoSupport消息的代理"

出站规则

代理的预定义安全组打开所有出站流量。如果可以接受，请遵循基本的出站规则。如果您需要更严格的规则，请使用高级出站规则。

基本出站规则

代理的预定义安全组包括以下出站规则。

协议	端口	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开代理出站通信所需的端口。

源IP地址是代理主机。

服务	协议	端口	目标	目的
API 调用和AutoSupport	HTTPS	443	出站互联网和ONTAP集群管理 LIF	对 Azure、ONTAP、 NetApp Data Classification的API 调用，以及向NetApp发送AutoSupport消息
API 调用	TCP	8080	数据分类	部署期间探测数据分类实例
DNS	UDP	53	DNS	用于控制台的 DNS 解析

Google Cloud 权限和所需的防火墙规则

控制台代理的 Google Cloud 权限

控制台代理需要权限才能在 Google Cloud 中执行操作。这些权限包含在NetApp提供的自定义角色中。您应该了解代理使用这些权限做什么。

Google Cloud 用户帐户权限

以下自定义角色赋予 Google Cloud 用户部署代理所需的权限。将此自定义角色分配给将要部署代理的用户。

查看 **Google Cloud** 用户帐户权限

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- 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.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
```

```
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- 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
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

服务帐户权限

以下自定义角色赋予附加到控制台代理的 Google Cloud 服务帐号管理 Google Cloud 网络中的资源和进程所需的权限。

将此自定义角色应用于附加到控制台代理虚拟机的服务帐户。

- "设置标准模式的 Google Cloud 权限"
- "设置限制模式的权限"

查看 **Google** 服务帐号权限

随着后续版本中权限的增加或删除，请确保角色信息保持最新。变更日志列出了所有需要的新权限。"查看 Google 权限变更日志" "查看如何添加 Google Cloud 服务帐号"

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent.
stage: GA
includedPermissions:
- cloudbuild.builds.get
- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken
- cloudbuild.repositories.list
- cloudbuild.workerpools.list
- cloudbuild.workerpools.get
- cloudquotas.quotas.get
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
- config.artifacts.import
- config.deployments.create
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getLock
- config.deployments.getState
- config.deployments.list
- config.deployments.lock
- config.deployments.update
- config.deployments.updateState
- config.previews.upload
- config.revisions.get
- config.revisions.getState
- config.operations.get
- config.previews.get
- config.previews.list
- config.resources.list
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.regionBackendServices.update
- compute.networks.updatePolicy
- compute.addresses.createInternal
```

```
- compute.addresses.deleteInternal
- compute.addresses.list
- compute.addresses.setLabels
- compute.addresses.useInternal
- compute.backendServices.create
- 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.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels
- compute.forwardingRules.update
- compute.globalOperations.get
- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- 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.instances.use
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.get
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.instances.setMinCpuPlatform
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.regionBackendServices.delete
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- 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
- logging.logEntries.create
- logging.logEntries.route
- monitoring.timeSeries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.list
- storage.objects.update
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.get
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.getIamPolicy
```

Google Cloud 权限的使用方式

控制台代理使用自定义角色中的权限来管理 Google Cloud 网络中的Cloud Volumes ONTAP资源和NetApp数据服务进程。以下各节描述了代理如何使用这些权限。

Cloud Volumes ONTAP使用的权限

控制台代理使用自定义角色中的权限来管理 Google Cloud 网络中的Cloud Volumes ONTAP资源和进程。以下各节描述了代理如何使用这些权限。

Cloud Volumes ONTAP的权限

操作	目的	用于部署?	用于日常运营?	用于删除?
config.deployments.create	使用 Google Cloud Infrastructure Manager 部署Cloud Volumes ONTAP虚拟机实例。	是	否	否
config.deployments.delete		否	否	是
config.deployments.deleteState		否	否	是
config.deployments.get		否	是	是
config.deployments.getLock		否	是	否
config.deployments.getState		否	是	否
config.deployments.list		否	是	否
config.deployments.lock		否	是	否
config.deployments.update		否	是	否
config.deployments.updateState		否	是	否
config.operations.get		否	是	否
config.previews.get		否	是	否
config.previews.list		否	是	否
config.resources.list		否	是	否
config.revisions.get		否	是	否
计算磁盘创建	为Cloud Volumes ONTAP创建和管理磁盘。	是	是	否
compute.disk.createSnapshot		否	是	否
计算磁盘删除		否	是	是
计算磁盘获取		否	是	否
计算磁盘列表		是	是	否
计算磁盘设置标签		是	是	否
计算磁盘使用		否	是	否

操作	目的	用于部署?	用于日常运营?	用于删除?
计算防火墙创建	为Cloud Volumes ONTAP创建防火墙规则。	是	否	否
计算防火墙删除		否	是	是
计算防火墙		是	是	否
计算防火墙列表		是	是	否
计算转发规则创建	创建转发规则，将流量路由到后端服务。	否	是	否
计算转发规则删除	删除现有转发规则。	否	是	否
计算转发规则	获取现有转发规则的详细信息。	否	是	否
计算转发规则.设置标签	设置或更新组织转发规则的标签。	否	是	否
compute.forwardingRules.update	更新流量管理的现有转发规则。	否	是	否
compute.globalOperations.get	获取操作状态。	是	是	否
计算健康检查创建	创建和管理健康检查，以监控后端服务的运行状况。	否	是	否
compute.healthChecks.delete		否	是	否
compute.healthChecks.get		否	是	否
compute.healthChecks.useReadOnly		否	是	否
compute.images.get	获取虚拟机实例的图像。	是	否	否
compute.images.getFromFamily		是	否	否
计算图像列表		是	否	否
compute.images.useReadOnly		是	否	否
compute.instances.attachDisk	将磁盘附加到Cloud Volumes ONTAP中分离磁盘。	是	是	否
compute.instances.detachDisk		否	是	是
compute.instances.create	创建和删除Cloud Volumes ONTAP VM 实例。	是	否	否
compute.instances.delete		否	否	是

操作	目的	用于部署?	用于日常运营?	用于删除?
compute.instances.get	列出虚拟机实例。	是	是	否
compute.instances.getSerialPortOutput	获取控制台日志。	是	是	否
compute.instances.list	检索区域中的实例列表。	是	是	否
compute.instances.setDeletionProtection	对实例设置删除保护。	是	否	否
compute.instances.setLabels	添加标签。	是	否	否
compute.instances.setMachineType	更改Cloud Volumes ONTAP的机器类型。	是	是	否
compute.instances.setMinCpuPlatform		是	是	否
compute.instances.setMetadata	添加元数据。	是	是	否
compute.instances.setTags	为防火墙规则添加标签。	是	是	否
计算实例开始	启动和停止Cloud Volumes ONTAP。	是	是	否
compute.instances.stop		是	是	否
compute.instances.updateDisplayDevice		是	是	否
compute.instances.use	使用虚拟机实例（启动、停止、连接操作）。	否	是	否
compute.machineTypes.get	获取核心数以检查配额。	是	否	否
compute.projects.get	支持多项目。	是	否	否
计算资源策略创建	创建和管理资源策略，实现资源自动化管理。	否	是	否
计算资源策略删除		否	是	否
compute.resourcePolicies.get		否	是	否

操作	目的	用于部署?	用于日常运营?	用于删除?
计算快照创建	创建和管理持久磁盘快照。	是	是	否
计算快照删除		否	是	是
计算快照获取		否	是	否
计算快照列表		否	是	否
计算快照.设置标签		是	是	否
compute.networks.get	获取创建新的Cloud Volumes ONTAP虚拟机实例所需的网络信息。	是	是	否
计算网络列表		是	是	否
计算区域		是	是	否
计算区域列表		是	是	否
计算子网络		是	是	否
计算子网络列表		是	是	否
compute.zoneOperations.get		是	是	否
计算区域		是	是	否
计算区域列表		是	是	否

操作	目的	用于部署?	用于日常运营?	用于删除?
deploymentmanager.compositeTypes.get	使用 Google Cloud Deployment Manager 部署Cloud Volumes ONTAP虚拟机实例。	是	否	否
deploymentmanager.compositeTypes.list		是	否	否
deploymentmanager.deployments.create		是	否	否
deploymentmanager.deployments.delete		是	否	否
deploymentmanager.deployments.get		是	否	否
deploymentmanager.deployments.list		是	否	否
deploymentmanager.manifests.get		是	否	否
deploymentmanager.manifests.list		是	否	否
deploymentmanager.operations.get		是	否	否
deploymentmanager.operations.list		是	否	否
deploymentmanager.resources.get		是	否	否
deploymentmanager.resources.list		是	否	否
deploymentmanager.typeProviders.get		是	否	否
deploymentmanager.typeProviders.list		是	否	否
deploymentmanager.types.get		是	否	否
deploymentmanager.types.list		是	否	否
日志记录条目列表	获取堆栈日志驱动器。	是	是	否
logging.privateLogEntries.list		是	是	否

操作	目的	用于部署?	用于日常运营?	用于删除?
日志记录条目创建	创建并路由日志条目，用于监控、调试和审计。	是	是	否
日志记录.日志条目.路由		是	是	否
resourcemanager.projects.get	支持多项目。	是	是	否
存储桶创建	创建和管理用于数据分层的 Google Cloud Storage 存储桶。	是	是	否
存储桶删除		否	是	是
存储桶获取		否	是	否
存储桶列表		否	是	否
存储桶更新		否	是	否
cloudkms.cryptoKeyVersions.useToEncrypt	将来自 Cloud Key Management Service 的客户管理加密密钥与Cloud Volumes ONTAP结合使用。	是	是	否
cloudkms.cryptoKeys.get		是	是	否
cloudkms.cryptoKeys.列表		是	是	否
cloudkms.keyRings.列表		是	是	否
cloudbuild.builds.get		是	否	否
cloudbuild.workerpools.get	使用 Infrastructure Manager 在 Cloud Volumes ONTAP 系统的专用模式部署和转换期间访问工作池信息。	是	是	是
cloudbuild.workerpools.list	在使用 Infrastructure Manager 部署 Cloud Volumes ONTAP 系统的专用模式期间列出工作池信息。	是	否	否

操作	目的	用于部署?	用于日常运营?	用于删除?
compute.instances.setServiceAccount	在Cloud Volumes ONTAP实例上设置服务帐户。此服务帐户提供将数据分层到 Google Cloud Storage 存储桶的权限。	是	是	否
iam.serviceAccounts.actAs		是	否	否
iam.serviceAccounts.create		是	否	否
iam.serviceAccounts.getIamPolicy		是	是	否
iam.serviceAccounts.list		是	是	否
iam.serviceAccountKeys.create		是	否	否
storage.objects.create	在 Google Cloud Storage 存储桶中创建和管理对象（文件）。	是	是	否
存储对象删除		否	否	是
storage.objects.get		是	是	否
存储对象列表		是	是	否
计算地址列表	在部署 HA 对时检索区域中的地址。	是	否	否
计算.地址.创建内部	在VPC网络内创建内部IP地址以进行资源分配。	否	是	否
计算.地址.删除内部	删除内部 IP 地址以进行资源清理。	否	是	否
计算.地址.设置标签	更新地址资源上的标签。	否	是	否
计算.地址.使用内部地址	网络通信请使用内部IP地址。	否	是	否
compute.backendServices.create	配置后端服务以在 HA 对中分配流量。	是	否	否

操作	目的	用于部署?	用于日常运营?	用于删除?
compute.regionBackendServices.create	创建和管理流量路由的后端服务。	是	否	否
compute.regionBackendServices.delete		否	是	否
compute.regionBackendServices.get		是	否	否
compute.regionBackendServices.update		是	是	否
compute.regionBackendServices.list		是	否	否
compute.regionBackendServices.use		否	是	否
compute.networks.updatePolicy	在 HA 对的 VPC 和子网上应用防火墙规则。	是	否	否
compute.instanceGroups.get	在Cloud Volumes ONTAP HA 对上创建和管理存储虚拟机。	是	是	否
计算地址		是	是	否
计算.实例.更新网络接口		是	是	否
compute.instanceGroups.create		否	是	否
compute.instanceGroups.delete		否	是	否
compute.instanceGroups.update		否	是	否
compute.instanceGroups.use		否	是	否
监控时间序列列表	发现有关 Google Cloud Storage 存储桶的信息。	是	是	否
storage.buckets.getIamPolicy		是	是	否

NetApp Backup and Recovery所使用的权限

控制台代理使用自定义角色中的权限来管理 Google Cloud 网络中的NetApp Backup and Recovery资源和进程。以下各节描述了代理如何使用这些权限。

查看**NetApp Backup and Recovery**的权限

操作	目的	用于部署?	用于日常运营?	用于删除?
• cloudkms.cryptoKeys.get • cloudkms.cryptoKeys.getIamPolicy • cloudkms.cryptoKeys.列表 • cloudkms.cryptoKeys.setIamPolicy • cloudkms.keyRings.get • cloudkms.keyRings.getIamPolicy • cloudkms.keyRings.列表 • cloudkms.keyRings.setIamPolicy	在NetApp Backup and Recovery激活向导中选择您自己的客户管理密钥，而不是使用默认的 Google 管理加密密钥。	是	是	否

NetApp Data Classification所使用的权限

控制台代理使用自定义角色中的权限来管理 Google Cloud 网络中的NetApp Data Classification资源和进程。以下各节描述了代理如何使用这些权限。

查看**NetApp Data Classification**的权限

操作	目的	用于部署?	用于日常运营?	用于删除?
• 计算子网络使用 • compute.subnetworks.useExternalIp • compute.instances.addAccessConfig	启用NetApp Data Classification。	是	否	否

更改日志

新增和移除的权限如下所示。

2026 年 **2** 月 **26** 日

添加了 `cloudbuild.workerpools.get` 和 `cloudbuild.workerpools.list` 权限，用于在 Google Cloud 中 Cloud Volumes ONTAP 的私有模式部署中支持 Infrastructure Manager。

2026 年 **2** 月 **09** 日

已添加 `compute.forwardingRules.update`权限，用于支持 Google Cloud 中 Cloud Volumes ONTAP 部署中的 Infrastructure Manager。

2025年**12**月**8**日

NetApp正在从 Google Cloud Deployment Manager 迁移到 Google Cloud Infrastructure Manager (IM)，以便在 Google Cloud 中部署和运行控制台代理。为支持此更改，添加了以下权限。

部署代理的 Google Cloud 用户需要以下附加权限：

- 存储桶创建
- 存储桶获取
- storage.objects.create
- 存储文件夹创建
- 存储对象列表
- iam.serviceAccount.actAs
- config.deployments.create
- config.operations.get

用于日常运营的 Google Cloud 服务帐号需要以下额外权限：

- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken
- cloudbuild.repositories.list
- cloudquotas.quotas.get
- config.artifacts.import
- config.deployments.deleteState
- config.deployments.getLock
- config.deployments.getState
- config.deployments.updateState
- config.previews.upload
- config.revisions.getState
- 日志记录条目创建
- storage.objects.create
- 存储对象删除
- 存储对象更新
- iam.serviceAccounts.get

部署Cloud Volumes ONTAP需要以下附加权限：

- cloudbuild.builds.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- iam.serviceAccountKeys.create
- iam.serviceAccounts.create

对于用于Cloud Volumes ONTAP日常操作的服务帐户，需要以下附加权限。

- 计算.地址.创建内部
- 计算.地址.删除内部
- 计算.地址.设置标签

- 计算.地址.使用内部地址
- 计算转发规则创建
- 计算转发规则删除
- 计算转发规则
- 计算转发规则.设置标签
- 计算健康检查创建
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.instances.use
- compute.regionBackendServices.delete
- compute.regionBackendServices.update
- compute.regionBackendServices.use
- 计算资源策略创建
- 计算资源策略删除
- compute.resourcePolicies.get
- 日志记录.日志条目.路由
- config.deployments.create
- config.deployments.delete
- config.deployments.get
- config.deployments.update
- config.revisions.get
- config.deployments.lock
- config.operations.get

2025年**11**月**26**日

权限已更新，以使其用途更加清晰，但未添加或删除任何权限。新增三列，分别指示每个权限是用于部署、日常操作还是删除。除此之外，还有一些权限根据其在NetApp Data Classification和NetApp Backup and Recovery的用途进行了划分。

2023年**2**月**6**日

此策略中添加了以下权限：

- 计算.实例.更新网络接口

Cloud Volumes ONTAP需要此权限。

2023年1月27日

此策略新增了以下权限：

- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

NetApp Backup and Recovery需要这些权限。

Google Cloud 中的代理防火墙规则

代理的 Google Cloud 防火墙规则需要入站和出站规则。当您从控制台创建控制台代理时，NetApp Console会自动创建此安全组。对于其他安装选项，您需要手动设置此安全组。

入站规则

协议	端口	目的
SSH	22	提供对代理主机的 SSH 访问
HTTP	80	• 提供从客户端 Web 浏览器到本地用户界面的 HTTP 访问 • 在Cloud Volumes ONTAP升级过程中使用
HTTPS	443	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问
TCP	3128	为Cloud Volumes ONTAP提供互联网访问。部署后您必须手动打开此端口。

出站规则

代理的预定义防火墙规则打开所有出站流量。如果可以接受，请遵循基本出站规则，或者使用高级出站规则来满足更严格的要求。

基本出站规则

代理的预定义防火墙规则包括以下出站规则。

协议	端口	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开代理出站通信所需的端口。

源IP地址是代理主机。

服务	协议	端口	目标	目的
API 调用和AutoSupport	HTTPS	443	出站互联网和ONTAP集群管理LIF	对 Google Cloud、ONTAP、 NetApp Data Classification 的API 调用，以及向NetApp发送AutoSupport消息
API 调用	TCP	8080	数据分类	部署期间探测数据分类实例
DNS	UDP	53	DNS	用于数据分类的 DNS 解析