AWS 代理权限和安全规则

NetApp Console setup and administration

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/console-setup-admin/reference-permissions-aws.html on February 11, 2026. Always check docs.netapp.com for the latest.

目录

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"

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: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: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: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: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

分类

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
- 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。

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

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。