



AWS 代理權限和安全性規則

NetApp Console setup and administration

NetApp
February 11, 2026

目錄

AWS 代理權限和安全性規則	1
控制台代理的 AWS 權限	1
IAM 策略	1
如何使用 AWS 權限	19
更改日誌	28
AWS 中的控制台代理程式安全性群組規則	30
入站規則	30
出站規則	30

AWS 代理權限和安全性規則

控制台代理的 **AWS** 權限

當NetApp Console在 AWS 中啟動控制台代理時，它會將一個原則附加到該代理，該原則會為代理提供管理該 AWS 帳戶內的資源和流程的權限。代理程式使用權限對多個 AWS 服務進行 API 呼叫，包括 EC2、S3、CloudFormation、IAM、金鑰管理服務 (KMS) 等。

IAM 策略

下面提供的 IAM 政策提供了控制台代理根據您的 AWS 區域管理公有雲環境內的資源和流程所需的權限。

請注意以下事項：

- 如果直接從控制台在標準 AWS 區域中建立控制台代理，則控制台會自動將政策套用至該代理程式。
- 如果您從 AWS Marketplace 部署代理程式、在 Linux 主機上手動安裝代理程式或想要為控制台新增其他 AWS 憑證，則需要自行設定政策。
- 無論哪種情況，您都需要確保策略是最新的，因為在後續版本中新增了新的權限。如果需要新的權限，它們將在發行說明中列出。
- 如果需要，您可以使用 IAM 限制 IAM 策略 `Condition` 元素。"[AWS 文件：條件元素](#)"
- 若要查看使用這些策略的逐步說明，請參閱以下頁面：
 - "[設定 AWS Marketplace 部署的權限](#)"
 - "[設定本地部署的權限](#)"
 - "[設定限制模式的權限](#)"

選擇您所在的地區以查看所需的政策：

標準區域

對於標準區域，權限分佈在兩個策略中。由於 AWS 中託管策略的最大字元大小限制，因此需要兩個策略。

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"
    }
  ]
}
```

```

{
  "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/*"
  ]
}
]
```

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

```

```
{
  "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** 權限

以下部分介紹如何使用每個NetApp Console管理或資料服務的權限。如果您的公司政策規定僅在需要時提供權限，則此資訊會很有幫助。

適用於**ONTAP** 的**Amazon FSx**

控制台代理程式發出以下 API 請求來管理Amazon FSx for ONTAP檔案系統：

- ec2:描述實例
- ec2：描述實例狀態
- ec2:描述實例屬性
- ec2:描述路由表
- ec2:描述影像
- ec2:建立標籤
- ec2:描述卷
- ec2:描述安全群組
- ec2:描述網路介面

- ec2:描述子網
- ec2:描述Vpcs
- ec2:描述DHCP選項
- ec2:描述快照
- ec2:描述密鑰對
- ec2:描述區域
- ec2:描述標籤
- ec2：描述IamInstanceProfileAssociations
- ec2:描述預留實例產品
- ec2:描述Vpc端點
- ec2:描述Vpcs
- ec2：描述卷修改
- ec2:描述放置組
- kms:創建授權
- kms：列出別名
- fsx:描述*
- fsx:列表*

Amazon S3 儲存桶發現

控制台代理程式發出以下 API 請求來發現 Amazon S3 儲存桶：

s3:取得加密配置

NetApp Backup and Recovery

該代理程式發出以下 API 請求來管理 Amazon S3 中的備份：

- s3：取得儲存桶位置
- s3：列出所有我的儲存桶
- s3：列表桶
- s3：創建桶
- s3:獲取生命週期配置
- s3：PutLifecycle配置
- s3：PutBucket標記
- s3：列出儲存桶版本
- s3：取得儲存桶Acl
- s3：PutBucket公共存取區塊

- s3：獲取對象
- ec2:描述Vpc端點
- kms：列出別名
- s3：PutEncryption配置

當您使用搜尋和還原方法還原磁碟區和檔案時，代理程式會發出下列 API 請求：

- s3：創建桶
- s3：刪除對象
- s3：刪除物件版本
- s3：取得儲存桶Acl
- s3：列表桶
- s3：列出儲存桶版本
- s3：列出桶多部分上傳
- s3：Put對象
- s3：PutBucketAcl
- s3：PutLifecycle配置
- s3：PutBucket公共存取區塊
- s3：中止分段上傳
- s3:列出多部分上傳部分

當您使用 DataLock 和NetApp Ransomware Resilience進行磁碟區備份時，代理程式會發出以下 API 請求：

- s3:取得物件版本標記
- s3：取得儲存桶物件鎖配置
- s3:取得物件版本Acl
- s3：PutObjectTagging
- s3：刪除對象
- s3：刪除物件標記
- s3：取得對象保留
- s3：刪除物件版本標記
- s3：Put對象
- s3：獲取對象
- s3:PutBucketObjectLock配置
- s3:獲取生命週期配置
- s3：按標籤列出儲存桶
- s3：取得儲存桶標記

- s3：刪除物件版本
- s3：列出儲存桶版本
- s3：列表桶
- s3：PutBucket標記
- s3:取得物件標記
- s3：PutBucket版本控制
- s3：PutObjectVersionTagging
- s3：取得儲存桶版本
- s3：取得儲存桶Acl
- s3：繞過治理保留
- s3：PutObjectRetention
- s3：取得儲存桶位置
- s3：取得物件版本

如果您對Cloud Volumes ONTAP備份所使用的 AWS 帳號與對來源磁碟區所使用的帳號不同，則代理程式會發出下列 API 要求：

- s3：PutBucket策略
- s3：PutBucket所有權控制

備份和還原的舊版權限

如果您在索引版本 v2 發布之前啟用了舊版索引功能，則只需要下列權限：

- kms:列表*
- kms:描述*
- athena：開始查詢執行
- 雅典娜：取得查詢結果
- 雅典娜：取得查詢執行
- athena：停止查詢執行
- 膠水：建立資料庫
- 膠水：創建表
- 膠水：批量刪除分割區

分類

代理程式發出以下 API 請求來部署NetApp Data Classification：

- ec2:描述實例
- ec2：描述實例狀態

- ec2：運行實例
- ec2：終止實例
- ec2:建立標籤
- ec2：建立磁碟區
- ec2：附加卷
- ec2：建立安全群組
- ec2：刪除安全群組
- ec2:描述安全群組
- ec2:建立網路介面
- ec2:描述網路介面
- ec2:刪除網路介面
- ec2:描述子網
- ec2:描述Vpcs
- ec2：建立快照
- ec2:描述區域
- cloudformation:建立堆疊
- cloudformation:刪除堆疊
- cloudformation:描述Stacks
- cloudformation：描述堆疊事件
- iam:新增角色到實例設定檔
- ec2:AssociateIamInstanceProfile
- ec2：描述IamInstanceProfileAssociations

當您使用NetApp Data Classification時，代理程式會發出以下 API 請求來掃描 S3 儲存桶：

- iam:新增角色到實例設定檔
- ec2:AssociateIamInstanceProfile
- ec2：描述IamInstanceProfileAssociations
- s3：取得儲存桶標記
- s3：取得儲存桶位置
- s3：列出所有我的儲存桶
- s3：列表桶
- s3：取得儲存桶策略狀態
- s3：取得儲存桶策略
- s3：取得儲存桶Acl
- s3：獲取對象

- iam：取得角色
- s3：刪除對象
- s3：刪除物件版本
- s3：Put對象
- sts：AssumeRole

Cloud Volumes ONTAP

該代理程式發出以下 API 請求以在 AWS 中部署和管理Cloud Volumes ONTAP。

目的	行動	用於部署？	用於日常營運？	用於刪除？
為Cloud Volumes ONTAP實例建立和管理 IAM 角色和實例設定檔	iam:列出實例設定檔	是的	是的	不
	iam：創建角色	是的	不	不
	iam：刪除角色	不	是的	是的
	iam:PutRolePolicy	是的	不	不
	iam:建立實例設定檔	是的	不	不
	iam:刪除角色策略	不	是的	是的
	iam:新增角色到實例設定檔	是的	不	不
	iam:從實例設定檔中刪除角色	不	是的	是的
	iam:刪除實例配置文件	不	是的	是的
	iam：PassRole	是的	不	不
	ec2:AssociateIamInstanceProfile	是的	是的	不
	ec2：描述IamInstanceProfile Associations	是的	是的	不
	ec2：解除關聯IamInstanceProfile	不	是的	不
解碼授權狀態訊息	sts：解碼授權訊息	是的	是的	不
描述帳戶可用的指定鏡像（AMI）	ec2:描述影像	是的	是的	不
描述 VPC 中的路由表（僅 HA 對需要）	ec2:描述路由表	是的	不	不

目的	行動	用於部署？	用於日常營運？	用於刪除？
停止、啟動和監控實例	ec2：啟動實例	是的	是的	不
	ec2：停止實例	是的	是的	不
	ec2:描述實例	是的	是的	不
	ec2：描述實例狀態	是的	是的	不
	ec2：運行實例	是的	不	不
	ec2：終止實例	不	不	是的
	ec2:修改實例屬性	不	是的	不
驗證是否為受支援的實例類型啟用了增強聯網	ec2:描述實例屬性	不	是的	不
使用“WorkingEnvironment”和“WorkingEnvironmentId”標籤標記資源，用於維護和成本分配	ec2:建立標籤	是的	是的	不
管理Cloud Volumes ONTAP用作後端儲存的 EBS 卷	ec2：建立磁碟區	是的	是的	不
	ec2:描述卷	是的	是的	是的
	ec2:修改卷屬性	不	是的	是的
	ec2：附加卷	是的	是的	不
	ec2：刪除卷	不	是的	是的
	ec2：分離卷	不	是的	是的
為Cloud Volumes ONTAP建立和管理安全性群組	ec2：建立安全群組	是的	不	不
	ec2：刪除安全群組	不	是的	是的
	ec2:描述安全群組	是的	是的	是的
	ec2：撤銷安全群組出口	是的	不	不
	ec2：授權安全群組出口	是的	不	不
	ec2：授權安全群組入口	是的	不	不
	ec2：撤銷安全群組入口	是的	是的	不

目的	行動	用於部署？	用於日常營運？	用於刪除？
在目標子網路中建立和管理Cloud Volumes ONTAP的網路介面	ec2:建立網路介面	是的	不	不
	ec2:描述網路介面	是的	是的	不
	ec2:刪除網路介面	不	是的	是的
	ec2:修改網路介面屬性	不	是的	不
取得目標子網路和安全群組列表	ec2:描述子網	是的	是的	不
	ec2:描述Vpcs	是的	是的	不
取得Cloud Volumes ONTAP實例的 DNS 伺服器 and 預設域名	ec2:描述DHCP選項	是的	不	不
為Cloud Volumes ONTAP拍攝 EBS 磁碟區快照	ec2：建立快照	是的	是的	不
	ec2：刪除快照	不	是的	是的
	ec2:描述快照	不	是的	不
捕獲Cloud Volumes ONTAP控制台，該控制台附加到AutoSupport訊息	ec2：取得控制台輸出	是的	是的	不
取得可用密鑰對列表	ec2:描述密鑰對	是的	不	不
取得可用 AWS 區域列表	ec2:描述區域	是的	是的	不
管理與Cloud Volumes ONTAP實例關聯的資源的標籤	ec2:刪除標籤	不	是的	是的
	ec2:描述標籤	不	是的	不
建立和管理 AWS CloudFormation 範本的堆疊	cloudformation:建立堆疊	是的	不	不
	cloudformation:刪除堆疊	是的	不	不
	cloudformation:描述Stacks	是的	是的	不
	cloudformation：描述堆疊事件	是的	不	不
	雲端資訊：驗證模板	是的	不	不

目的	行動	用於部署？	用於日常營運？	用於刪除？
建立和管理Cloud Volumes ONTAP系統用作資料分層容量層的 S3 儲存桶	s3：創建桶	是的	是的	不
	s3：刪除桶	不	是的	是的
	s3:獲取生命週期配置	不	是的	不
	s3：PutLifecycle配置	不	是的	不
	s3：PutBucket標記	不	是的	不
	s3：列出儲存桶版本	不	是的	不
	s3：取得儲存桶策略狀態	不	是的	不
	s3：取得儲存桶公共存取區塊	不	是的	不
	s3：取得儲存桶Acl	不	是的	不
	s3：取得儲存桶策略	不	是的	不
	s3：PutBucket公共存取區塊	不	是的	不
	s3：取得儲存桶標記	不	是的	不
	s3：取得儲存桶位置	不	是的	不
	s3：列出所有我的儲存桶	不	不	不
	s3：列表桶	不	是的	不
使用 AWS 金鑰管理服務 (KMS) 啟用Cloud Volumes ONTAP的資料加密	kms:重新加密*	是的	不	不
	kms:創建授權	是的	是的	不
	kms:產生不含明文的資料金鑰	是的	是的	不
在單一 AWS 可用區中為兩個 HA 節點和中介器建立和管理 AWS 擴充置放群組	ec2:建立放置組	是的	不	不
	ec2:刪除放置群組	不	是的	是的
建立報告	fsx:描述*	不	是的	不
	fsx:列表*	不	是的	不
建立和管理支援 Amazon EBS 彈性磁碟區功能的聚合	ec2：描述卷修改	不	是的	不
	ec2：修改卷	不	是的	不
檢查可用區是否為 AWS 本地區域，並驗證所有部署參數是否相容	ec2:描述可用區域	是的	不	是的

更改日誌

當新增和刪除權限時，我們會在下面的部分中註明。

2025年11月11日

除非您使用舊版索引，否則NetApp Backup and Recovery不再需要以下權限。這些權限已從本頁面的策略移除：

- kms:列表*
- kms:描述*
- athena：開始查詢執行
- 雅典娜：取得查詢結果
- 雅典娜：取得查詢執行
- athena：停止查詢執行
- 膠水：建立資料庫
- 膠水：創建表
- 膠水：批量刪除分割區

2024年9月9日

由於NetApp Console不再支援NetApp邊緣快取以及 Kubernetes 叢集的發現和管理，因此從標準區域的策略 #2 中刪除了權限。

```
{
  "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現在需要以下權限：

ec2:描述可用區域

2023年6月6日

Cloud Volumes ONTAP現在需要以下權限：

kms:產生不含明文的資料金鑰

2023年2月14日

NetApp Cloud Tiering現在需要以下權限：

ec2:描述Vpc端點

AWS 中的控制台代理程式安全性群組規則

代理程式的 AWS 安全群組需要入站和出站規則。當您從控制台建立控制台代理程式時，NetApp Console會自動建立此安全性群組。您需要為所有其他安裝選項設定此安全群組。

入站規則

協定	港口	目的
SSH	22	提供對代理主機的 SSH 訪問
HTTP	80	- 提供從客戶端 Web 瀏覽器到本機使用者介面的 HTTP 訪問 - 在Cloud Volumes ONTAP升級過程中使用
HTTPS	443	提供對本機使用者介面的 HTTPS 存取以及來自NetApp Data Classification實例的連接
TCP	3128	為Cloud Volumes ONTAP提供網路存取。部署後您必須手動開啟此連接埠。

出站規則

代理程式的預定義安全群組開啟所有出站流量。如果可以接受，請遵循基本的出站規則。如果您需要更嚴格的規則，請使用進階出站規則。

基本出站規則

代理程式的預定義安全性群組包括以下出站規則。

協定	港口	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高級出站規則

如果您需要對出站流量製定嚴格的規則，則可以使用以下資訊僅打開代理出站通訊所需的端口



來源IP位址是代理主機。

服務	協定	港口	目的地	目的
API 呼叫 和AutoSupport	HTTPS	443	出站互聯網 和ONTAP叢集管理 LIF	對 AWS、ONTAP、 NetApp Data Classification的API 調用，以及向NetApp 發送AutoSupport訊 息
API 呼叫	TCP	3000	ONTAP HA 調解器	與ONTAP HA 調解器 的通信
	TCP	8080	資料分類	部署期間探測資料分 類實例
DNS	UDP	53	DNS	用於控制台的 DNS 解析

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。