雲端提供者代理權限和網路要求

NetApp Console setup and administration

NetApp
March 03, 2026

目錄

雲端提供者代理權限和網路要求

NetApp Console的權限摘要

您需要為控制台代理提供適當的權限，以便它可以在您的雲端環境中執行操作。使用此頁面上的鏈接，您可以根據目標快速存取所需的權限。

AWS 權限

NetApp Console需要控制台代理程式和各服務的 AWS 權限。

控制台代理

目標	描述	關聯
從控制台部署控制台代理程式 若要在 AWS 中部署控制台代理，使用者需要特定的權限。	"設定 AWS 權限"	為控制台代理提供權限

NetApp Backup and Recovery

目標	描述	關聯
使用NetApp Backup and Recovery將本機ONTAP叢集備份到 Amazon S3	在ONTAP磁碟區上啟動備份時， NetApp Backup and Recovery會提示您輸入具有特定權限的 IAM 使用者的存取金鑰和密碼。	"設定備份的 S3 權限"

Cloud Volumes ONTAP

目標	描述	關聯
為Cloud Volumes ONTAP節點提供權限	必須將 IAM 角色附加到 AWS 中的每個Cloud Volumes ONTAP節點。對於 HA 調解員也是如此。預設選項是讓控制台為您建立 IAM 角色，但您可以在控制台中建立系統時使用您自己的角色。	"了解如何自行設定 IAM 角色"

NetApp Copy and Sync

目標	描述	關聯
在 AWS 中部署資料代理	用於部署資料代理程式的 AWS 使用者帳戶必須具有所需的權限。	"在 AWS 中部署資料代理程式所需的權限"
為數據經紀人提供權限	當NetApp Copy and Sync部署資料代理程式時，它會為資料代理實例建立一個 IAM 角色。如果您願意，您可以使用自己的 IAM 角色部署資料代理程式。	"使用您自己的 IAM 角色與 AWS 資料代理程式的要求"

目標	描述	關聯
為手動安裝的資料代理程式啟用 AWS 訪問	如果您使用包含 S3 儲存桶的同步關係的資料代理，那麼您應該準備好 Linux 主機以供 AWS 存取。安裝資料代理程式時，您需要為具有程式存取權限和特定權限的 IAM 使用者提供 AWS 金鑰。	"啟用對 AWS 的訪問"

適用於**ONTAP**的 **FSx**

目標	描述	關聯
建立和管理 FSx for ONTAP	若要建立或管理Amazon FSx for NetApp ONTAP系統，您需要透過提供 IAM 角色的 ARN（為控制台提供所需的權限）將 AWS 憑證新增至控制台。	"了解如何為 FSx 設定 AWS 憑證"

NetApp Cloud Tiering

目標	描述	關聯
將本機ONTAP叢集分層到 Amazon S3	啟用NetApp Cloud Tiering到 AWS 時，您需要輸入存取金鑰和秘密金鑰。這些憑證將傳遞給ONTAP集群，以便ONTAP可以將資料分層儲存到 S3 儲存桶中。	"設定 S3 分層權限"

Azure 權限

控制台需要控制台代理程式和各個服務的 Azure 權限。

控制台代理

目標	描述	關聯
從控制台部署控制台代理	從控制台部署控制台代理程式時，您需要使用具有在 Azure 中部署控制台代理程式 VM 的權限的 Azure 帳戶或服務主體。	"設定 Azure 權限"
為控制台代理提供權限	當控制台在 Azure 中部署控制台代理程式 VM 時，它會建立一個自訂角色，該角色提供管理該 Azure 訂閱中的資源和流程所需的權限。 如果您從市場啟動控制台代理，如果您手動安裝控制台代理，或者如果您"新增更多 Azure 憑證"。 隨著後續版本新增的權限，請及時更新策略。	"控制台代理程式的 Azure 權限"

NetApp Backup and Recovery

目標	描述	關聯
將Cloud Volumes ONTAP備份到 Azure Blob 存儲	使用NetApp Backup and Recovery備份Cloud Volumes ONTAP時，您需要在下列情況下新增權限至控制台代理： • 您想使用“搜尋和恢復”功能 • 您想要使用客戶管理的加密金鑰 (CMEK)	• "使用備份和還原將Cloud Volumes ONTAP資料備份到 Azure Blob 存儲"

目標	描述	關聯
將本機ONTAP叢集備份到 Azure Blob 存儲	使用NetApp Backup and Recovery備份本機ONTAP叢集時，需要新增權限至控制台代理才能使用「搜尋與復原」功能。	"使用備份和還原將本機ONTAP資料備份到 Azure Blob 存儲"

NetApp複製與同步

目標	描述	關聯
在 Azure 中部署資料代理	用於部署資料代理程式的 Azure 使用者帳戶必須具有所需的權限。	"在 Azure 中部署資料代理程式所需的權限"

Google Cloud 權限

控制台需要控制台代理程式和各個服務的 Google Cloud 權限。

控制台代理

目標	描述	關聯
從控制台部署控制台代理	從控制台部署控制台代理程式的 Google Cloud 使用者需要特定權限才能在 Google Cloud 中部署控制台代理程式。	"設定權限以建立控制台代理"
為控制台代理提供權限	控制台代理程式的服務帳戶必須具有日常操作所需的特定權限。部署期間需要將服務帳戶與控制台代理程式關聯。隨著後續版本新增的權限，請及時更新策略。	"設定控制台代理的權限"

NetApp Backup and Recovery

目標	描述	關聯
將Cloud Volumes ONTAP備份到 Google Cloud	使用NetApp Backup and Recovery備份Cloud Volumes ONTAP時，您需要在下列情況下新增權限至控制台代理： • 您想使用“搜尋和恢復”功能 • 您想要使用客戶管理的加密金鑰 (CMEK)	• "使用備份和還原將Cloud Volumes ONTAP資料備份到 Google Cloud Storage" • "CMEK 的權限"
將本地ONTAP叢集備份到 Google Cloud	使用NetApp Backup and Recovery備份本機ONTAP叢集時，需要新增權限至控制台代理才能使用「搜尋與復原」功能。	"使用備份和還原將本地ONTAP資料備份到 Google Cloud Storage"

NetApp Copy and Sync

目標	描述	關聯
在 Google Cloud 中部署資料代理	確保部署資料代理程式的 Google Cloud 使用者俱有所需的權限。	"在 Google Cloud 中部署資料代理程式所需的權限"
為手動安裝的資料代理啟用 Google Cloud 存取權限	如果您打算使用包含 Google Cloud Storage 儲存桶的同步關係的資料代理，那麼您應該準備 Linux 主機以供 Google Cloud 存取。安裝資料代理程式時，您需要為具有特定權限的服務帳戶提供金鑰。	"啟用對 Google Cloud 的訪問"

StorageGRID權限

控制台需要兩項服務的StorageGRID權限。

NetApp Backup and Recovery

目標	描述	關聯
將本機ONTAP叢集備份到StorageGRID	當您準備將StorageGRID作為ONTAP叢集的備份目標時， NetApp Backup and Recovery會提示您輸入具有特定權限的 IAM 使用者的存取金鑰和密碼。	"準備StorageGRID作為備份目標"

NetApp Cloud Tiering

目標	描述	關聯
將本地ONTAP集群分層到StorageGRID	當您將NetApp Cloud Tiering設定為StorageGRID時，您需要向 Cloud Tiering 提供 S3 存取金鑰和金鑰。雲端分層使用密鑰來存取您的儲存桶。	"準備分層到StorageGRID"

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"
  - "設定私密模式的權限"

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: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（美國）區域

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

秘密區域

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

絕密地區

```
{
  "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** 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

NetApp Data Classification

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
- cloudformation：ListStacks
- 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IamInstanceProfileAssociations	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 伺服器和預設域名	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。

2026 年 **2** 月 **24** 日

資料分類現在需要以下權限：

cloudformation：ListStacks

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。

查看從策略中刪除的權限

```
{
    "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

Azure 權限和所需安全性規則

控制台代理程式的 Azure 權限

當NetApp Console在 Azure 中啟動控制台代理程式時，它會將自訂角色附加到 VM，該 VM 為代理程式提供管理該 Azure 訂閱中的資源和流程的權限。代理程式使用權限對多個 Azure 服務進行 API 呼叫。

是否需要為代理程式建立此自訂角色取決於您如何部署它。

從NetApp Console部署

當您使用控制台在 Azure 中部署代理虛擬機器時，它會啟用 "系統分配的託管標識"在虛擬機器上，建立自訂角色，並將其指派給虛擬機器。此角色為控制台提供管理該 Azure 訂閱內的資源和流程所需的權限。當代理升級時，角色的權限保持最新。您不需要為代理程式建立此角色或管理更新。

手動部署或從 Azure 市場部署

當您從 Azure 市場部署代理程式或在 Linux 主機上手動安裝代理程式時，您需要自行設定自訂角色並在任何變更時維護其權限。

您需要確保角色是最新的，因為後續版本中會新增新的權限。如果需要新的權限，它們將在發行說明中列出。

- 若要查看使用這些策略的逐步說明，請參閱以下頁面：
  - "設定 Azure 市場部署的權限"
  - "設定本地部署的權限"
  - "設定限制模式的權限"
  - "設定私密模式的權限"

```
{
  "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** 權限

以下部分介紹如何對每個NetApp儲存系統和資料服務使用權限。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。

Azure NetApp Files

當您使用NetApp Data Classification掃描Azure NetApp Files資料時，代理程式會發出以下 API 請求：

- 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

以下各節描述了NetApp Backup and Recovery如何使用權限。

NetApp Backup and Recovery權限

控制台代理程式會發出以下 API 請求以實現基本的NetApp Backup and Recovery功能：

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/讀取
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/訂閱/位置/讀取
- Microsoft.Resources/訂閱/resourceGroups/讀取
- Microsoft.Resources/訂閱/資源群組/資源/讀取
- Microsoft.Resources/訂閱/資源群組/寫入
- Microsoft.Storage/storageAccounts/managementPolicies/讀取
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

以下是用於備份和復原的自訂策略，它使用的權限最少，範圍也最窄：

```
{
  "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": []
      }
    ]
  }
}
```

進階備份和恢復權限

控制台代理程式發出以下 API 請求，以實現進階備份和復原作業以及搜尋和復原功能。這些權限允許管理網路、金鑰庫和受管身分：

- Microsoft.KeyVault/保管庫/存取策略/寫入
- Microsoft.KeyVault/保管庫/讀取
- Microsoft.ManagedIdentity/userAssignedIdentities/分配/操作
- Microsoft.Network/networkInterfaces/刪除
- Microsoft.Network/網路介面/讀取
- Microsoft.Network/networkSecurityGroups/刪除
- Microsoft.Network/privateDnsZones/讀取
- Microsoft.Network/privateDnsZones/寫入
- Microsoft.Network/privateEndpoints/讀取
- Microsoft.Network/privateEndpoints/寫入
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Resources/部署/刪除

備份和還原的舊版權限

當您使用搜尋和復原功能時，代理程式會發出以下 API 請求。只有在 2025 年 2 月索引版本 v2 發布之前啟用了舊版索引功能，才需要這些權限：

- Microsoft.Synapse/工作區/寫入
- Microsoft.Synapse/工作區/讀取
- Microsoft.Synapse/工作區/刪除
- Microsoft.Synapse/註冊/操作
- Microsoft.Synapse/checkNameAvailability/操作
- Microsoft.Synapse/工作區/operationStatuses/讀取
- Microsoft.Synapse/工作區/防火牆規則/讀取
- Microsoft.Synapse/工作區/replaceAllIpFirewallRules/操作
- Microsoft.Synapse/工作區/操作結果/讀取
- Microsoft.Synapse/工作區/privateEndpointConnectionsApproval/操作

NetApp Data Classification

當您使用資料分類時，代理程式會發出以下 API 請求。

行動	用於設定嗎？	用於日常營運？
Microsoft.Compute/位置/操作/讀取	是的	是的

行動	用於設定嗎？	用於日常營運？
Microsoft.Compute/位置/vmSizes/讀取	是的	是的
Microsoft.Compute/操作/讀取	是的	是的
Microsoft.Compute/virtualMachines/instanceView/讀取	是的	是的
Microsoft.Compute/virtualMachines/powerOff/action	是的	不
Microsoft.Compute/虛擬機器/讀取	是的	是的
Microsoft.Compute/virtualMachines/重新啟動/操作	是的	不
Microsoft.Compute/virtualMachines/啟動/操作	是的	不
Microsoft.Compute/virtualMachines/vmSizes/讀取	不	是的
Microsoft.Compute/虛擬機器/寫入	是的	不
Microsoft.Compute/圖片/讀取	是的	是的
Microsoft.Compute/磁碟/刪除	是的	不
Microsoft.Compute/磁碟/讀取	是的	是的
Microsoft.Compute/磁碟/寫入	是的	不
Microsoft.Storage/checknameavailability/讀取	是的	是的
Microsoft.Storage/操作/讀取	是的	是的
Microsoft.Storage/storageAccounts/listkeys/action	是的	不
Microsoft.Storage/storageAccounts/讀取	是的	是的
Microsoft.Storage/storageAccounts/write	是的	不
Microsoft.Storage/storageAccounts/blobServices/containers/read	是的	是的
Microsoft.Network/網路介面/讀取	是的	是的
Microsoft.Network/網路介面/寫入	是的	不
Microsoft.Network/networkInterfaces/join/action	是的	不
Microsoft.Network/networkSecurityGroups/讀取	是的	是的
Microsoft.Network/networkSecurityGroups/寫入	是的	不

行動	用於設定嗎？	用於日常營運？
Microsoft.Resources/訂閱/位置/讀取	是的	是的
Microsoft.Network/locations/operationResults/read	是的	是的
Microsoft.Network/位置/操作/讀取	是的	是的
Microsoft.Network/virtualNetworks/讀取	是的	是的
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/讀取	是的	是的
Microsoft.Network/virtualNetworks/子網路/讀取	是的	是的
Microsoft.Network/virtualNetworks/子網路/virtualMachines/讀取	是的	是的
Microsoft.Network/virtualNetworks/virtualMachines/讀取	是的	是的
Microsoft.Network/virtualNetworks/子網路/加入/操作	是的	不
Microsoft.Network/virtualNetworks/子網路/寫入	是的	不
Microsoft.Network/routeTables/join/action	是的	不
Microsoft.Resources/部署/操作/讀取	是的	是的
Microsoft.Resources/部署/讀取	是的	是的
Microsoft.Resources/部署/寫入	是的	不
Microsoft.Resources/資源/讀取	是的	是的
Microsoft.Resources/subscriptions/operationresults/read	是的	是的
Microsoft.Resources/subscriptions/resourceGroups/delete	是的	不
Microsoft.Resources/訂閱/resourceGroups/讀取	是的	是的
Microsoft.Resources/訂閱/資源群組/資源/讀取	是的	是的
Microsoft.Resources/訂閱/資源群組/寫入	是的	不

Cloud Volumes ONTAP

該代理程式發出以下 API 請求以在 Azure 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？
建立和管理虛擬機	Microsoft.Compute/位置/操作/讀取	是的	是的	不
	Microsoft.Compute/位置/vmSizes/讀取	是的	是的	不
	Microsoft.Resources/訂閱/位置/讀取	是的	不	不
	Microsoft.Compute/操作/讀取	是的	是的	不
	Microsoft.Compute/virtualMachines/instanceView/讀取	是的	是的	不
	Microsoft.Compute/virtualMachines/powerOff/action	是的	是的	不
	Microsoft.Compute/虛擬機器/讀取	是的	是的	不
	Microsoft.Compute/virtualMachines/重新啟動/操作	是的	是的	不
	Microsoft.Compute/virtualMachines/啟動/操作	是的	是的	不
	Microsoft.Compute/virtualMachines/解除指派/操作	不	是的	是的
	Microsoft.Compute/virtualMachines/vmSizes/讀取	不	是的	不
	Microsoft.Compute/虛擬機器/寫入	是的	是的	不
	Microsoft.Compute/virtualMachines/刪除	是的	是的	是的
	Microsoft.Resources/部署/刪除	是的	不	不
啟用從 VHD 部署	Microsoft.Compute/圖片/讀取	是的	不	不
	Microsoft.Compute/圖片/寫入	是的	不	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網路介面	Microsoft.Network/網路介面/讀取	是的	是的	不
	Microsoft.Network/網路介面/寫入	是的	是的	不
	Microsoft.Network/networkInterfaces/join/action	是的	是的	不
	Microsoft.Network/networkInterfaces/刪除	是的	是的	不
建立和管理網路安全群組	Microsoft.Network/networkSecurityGroups/讀取	是的	是的	不
	Microsoft.Network/networkSecurityGroups/寫入	是的	是的	不
	Microsoft.Network/networkSecurityGroups/加入/操作	是的	不	不
	Microsoft.Network/networkSecurityGroups/刪除	不	是的	是的

目的	行動	用於部署？	用於日常營運？	用於刪除？
取得有關區域、目標 VNet 和子網的網路信息，並將 VM 新增至 VNet	Microsoft.Network/locations/operationResults/read	是的	是的	不
	Microsoft.Network/位置/操作/讀取	是的	是的	不
	Microsoft.Network/virtualNetworks/讀取	是的	不	不
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/讀取	是的	不	不
	Microsoft.Network/virtualNetworks/子網路/讀取	是的	是的	不
	Microsoft.Network/virtualNetworks/子網路/virtualMachines/讀取	是的	是的	不
	Microsoft.Network/virtualNetworks/virtualMachines/讀取	是的	是的	不
	Microsoft.Network/virtualNetworks/子網路/加入/操作	是的	是的	不

目的	行動	用於部署？	用於日常營運？	用於刪除？
建立和管理資源組	Microsoft.Resources/部署/操作/讀取	是的	是的	不
	Microsoft.Resources/部署/讀取	是的	是的	不
	Microsoft.Resources/部署/寫入	是的	是的	不
	Microsoft.Resources/資源/讀取	是的	是的	不
	Microsoft.Resources/subscriptions/operationresults/read	是的	是的	不
	Microsoft.Resources/subscriptions/resourceGroups/delete	是的	是的	是的
	Microsoft.Resources/訂閱/resourceGroups/讀取	不	是的	不
	Microsoft.Resources/訂閱/資源群組/資源/讀取	是的	是的	不
	Microsoft.Resources/訂閱/資源群組/寫入	是的	是的	不

目的	行動	用於部署？	用於日常營運？	用於刪除？
管理 Azure 儲存帳戶和磁碟	Microsoft.Compute/磁碟/讀取	是的	是的	是的
	Microsoft.Compute/磁碟/寫入	是的	是的	不
	Microsoft.Compute/磁碟/刪除	是的	是的	是的
	Microsoft.Storage/checknameavailability/讀取	是的	是的	不
	Microsoft.Storage/操作/讀取	是的	是的	不
	Microsoft.Storage/storageAccounts/listkeys/action	是的	是的	不
	Microsoft.Storage/storageAccounts/讀取	是的	是的	不
	Microsoft.Storage/storageAccounts/刪除	不	是的	是的
	Microsoft.Storage/storageAccounts/write	是的	是的	不
	Microsoft.Storage/使用/讀取	不	是的	不
啟用 Blob 儲存備份和儲存帳戶加密	Microsoft.Storage/storageAccounts/blobServices/containers/read	是的	是的	不
	Microsoft.KeyVault/保管庫/讀取	是的	是的	不
	Microsoft.KeyVault/保管庫/存取策略/寫入	是的	是的	不
啟用 VNet 服務終點以進行資料分層	Microsoft.Network/virtualNetworks/子網路/寫入	是的	是的	不
	Microsoft.Network/routeTables/join/action	是的	是的	不

目的	行動	用於部署？	用於日常營運？	用於刪除？
建立和管理 Azure 託管快照	Microsoft.Compute/快照/寫入	是的	是的	不
	Microsoft.Compute/快照/讀取	是的	是的	不
	Microsoft.Compute/快照/刪除	不	是的	是的
	Microsoft.Compute/磁碟/beginGetAccess/操作	不	是的	不
建立和管理可用性集	Microsoft.Compute/可用性集/寫入	是的	不	不
	Microsoft.Compute/可用性集/讀取	是的	不	不
啟用來自市場的程式化部署	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read	是的	不	不
	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	是的	是的	不

目的	行動	用於部署？	用於日常營運？	用於刪除？
管理 HA 對的負載平衡器	Microsoft.Network/loadBalancers/讀取	是的	是的	不
	Microsoft.Network/loadBalancers/寫入	是的	不	不
	Microsoft.Network/loadBalancers/刪除	不	是的	是的
	Microsoft.Network/loadBalancers/backendAddressPools/讀取	是的	不	不
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	是的	不	不
	Microsoft.Network/loadBalancers/frontendIPConfigurations/讀取	是的	是的	不
	Microsoft.Network/loadBalancers/loadBalancingRules/讀取	是的	不	不
	Microsoft.Network/loadBalancers/探測/讀取	是的	不	不
	Microsoft.Network/loadBalancers/探測/加入/操作	是的	不	不
啟用 Azure 磁碟上的鎖定管理	Microsoft.授權/鎖定/*	是的	是的	不

目的	行動	用於部署？	用於日常營運？	用於刪除？
當子網路外部沒有連線時，為 HA 對啟用專用端點	Microsoft.Network/privateEndpoints/寫入	是的	是的	不
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	是的	不	不
	Microsoft.Storage/storageAccounts/privateEndpointConnections/讀取	是的	是的	是的
	Microsoft.Network/privateEndpoints/讀取	是的	是的	是的
	Microsoft.Network/privateDnsZones/寫入	是的	是的	不
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/寫入	是的	是的	不
	Microsoft.Network/virtualNetworks/join/action	是的	是的	不
	Microsoft.Network/privateDnsZones/A/寫入	是的	是的	不
	Microsoft.Network/privateDnsZones/讀取	是的	是的	不
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/讀取	是的	是的	不
對於某些虛擬機器部署是必需的，具體取決於底層實體硬體	Microsoft.Resources/deployments/operationStatuses/read	是的	是的	不
在部署失敗或刪除的情況下從資源組中刪除資源	Microsoft.Network/privateEndpoints/刪除	是的	是的	不
	Microsoft.Compute/可用性集/刪除	是的	是的	不

目的	行動	用於部署？	用於日常營運？	用於刪除？
使用 API 時啟用客戶管理的加密金鑰	Microsoft.Compute/diskEncryptionSets/讀取	是的	是的	是的
	Microsoft.Compute/diskEncryptionSets/寫入	是的	是的	不
	Microsoft.KeyVault/保管庫/部署/操作	是的	不	不
	Microsoft.Compute/diskEncryptionSets/刪除	是的	是的	是的
為 HA 對配置應用程式安全性群組，以隔離 HA 互連和叢集網路 NIC	Microsoft.Network/applicationSecurityGroups/寫入	不	是的	不
	Microsoft.Network/applicationSecurityGroups/讀取	不	是的	不
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	不	是的	不
	Microsoft.Network/networkSecurityGroups/securityRules/寫入	是的	是的	不
	Microsoft.Network/applicationSecurityGroups/刪除	不	是的	是的
	Microsoft.Network/networkSecurityGroups/securityRules/刪除	不	是的	是的
讀取、寫入和刪除與Cloud Volumes ONTAP資源關聯的標籤	Microsoft.Resources/標籤/閱讀	不	是的	不
	Microsoft.Resources/標籤/寫入	是的	是的	不
	Microsoft.Resources/標籤/刪除	是的	不	不
在建立期間加密儲存帳戶	Microsoft.ManagedIdentity/userAssignedIdentities/分配/操作	是的	是的	不

目的	行動	用於部署？	用於日常營運？	用於刪除？
在彈性編排模式下使用虛擬機器規模集合來為Cloud Volumes ONTAP指定特定區域	Microsoft.Compute/virtualMachineScaleSets/寫入	是的	不	不
	Microsoft.Compute/virtualMachineScaleSets/讀取	是的	不	不
	Microsoft.Compute/virtualMachineScaleSets/刪除	不	不	是的

分層

當您設定NetApp Cloud Tiering時，代理會發出以下 API 請求。

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/訂閱/resourceGroups/讀取
- Microsoft.Resources/訂閱/位置/讀取

控制台代理程式針對日常操作發出以下 API 請求。

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

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

新增了一個自訂 JSON 策略，該策略體現了盡可能少的權限和盡可能小的範圍。

以下權限已新增至最小備份和復原權限清單：

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

除非您使用的是舊版索引，否則備份和還原不再需要以下權限：

- Microsoft.Synapse/工作區/寫入
- Microsoft.Synapse/工作區/讀取
- Microsoft.Synapse/工作區/刪除
- Microsoft.Synapse/註冊/操作
- Microsoft.Synapse/checkNameAvailability/操作

- Microsoft.Synapse/工作區/operationStatuses/讀取
- Microsoft.Synapse/工作區/防火牆規則/讀取
- Microsoft.Synapse/工作區/replaceAllIpFirewallRules/操作
- Microsoft.Synapse/工作區/操作結果/讀取
- Microsoft.Synapse/工作區/privateEndpointConnectionsApproval/操作

以下權限已移至「其他備份和復原權限」部分，因為最小配置不需要這些權限：

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/讀取
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/訂閱/位置/讀取
- Microsoft.Resources/訂閱/resourceGroups/讀取
- Microsoft.Resources/訂閱/資源群組/資源/讀取
- Microsoft.Resources/訂閱/資源群組/寫入
- Microsoft.Storage/storageAccounts/managementPolicies/讀取
- Microsoft.Storage/storageAccounts/managementPolicies/write

2024年9月9日

由於控制台不再支援發現和管理 Kubernetes 集群，因此從 JSON 策略中刪除了以下權限：

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/作業
- Microsoft.ContainerService/managedClusters/讀取

2024年8月22日

以下權限已新增至 JSON 策略中，因為它們是Cloud Volumes ONTAP支援虛擬機器規模集所必需的：

- Microsoft.Compute/virtualMachineScaleSets/寫入
- Microsoft.Compute/virtualMachineScaleSets/讀取
- Microsoft.Compute/virtualMachineScaleSets/刪除

2023年12月5日

將磁碟區資料備份到 Azure Blob 儲存體時， NetApp Backup and Recovery不再需要以下權限：

- Microsoft.Compute/虛擬機器/讀取
- Microsoft.Compute/virtualMachines/啟動/操作
- Microsoft.Compute/virtualMachines/解除指派/操作

- Microsoft.Compute/virtualMachines/擴充/刪除
- Microsoft.Compute/virtualMachines/刪除

其他控制台儲存服務需要這些權限，因此如果您使用其他儲存服務，它們仍將保留在代理程式的自訂角色中。

2023年5月12日

以下權限已新增至 JSON 策略，因為它們是Cloud Volumes ONTAP管理所必需的：

- Microsoft.Compute/圖片/寫入
- Microsoft.Network/loadBalancers/frontendIPConfigurations/讀取

以下權限已從 JSON 策略中刪除，因為不再需要它們：

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

2023年3月23日

資料分類不再需要「Microsoft.Storage/storageAccounts/delete」權限。

Cloud Volumes ONTAP仍需要此權限。

2023年1月5日

以下權限已新增至 JSON 策略：

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

  NetApp Backup and Recovery需要這些權限。

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

  Cloud Volumes ONTAP部署需要此權限。

Azure 中的控制台代理程式安全性群組規則

代理程式的 Azure 安全性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。對於其他安裝選項，您需要手動設定此安全性群組。

入站規則

協定	港口	目的
SSH	22	提供對代理主機的 SSH 訪問

協定	港口	目的
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	提供從客戶端 Web 瀏覽器到本機使用者介面的 HTTPS 訪問，以及來自NetApp Data Classification實例的連接
TCP	3128	為Cloud Volumes ONTAP提供網路存取權限，以便將AutoSupport訊息傳送給NetApp支援。部署後您必須手動開啟此連接埠。 "了解如何將代理用作AutoSupport訊息的代理"

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開啟代理出站通訊所需的連接埠。

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 Azure、 ONTAP、 NetApp Data Classification 的API 調用，以及向NetApp發送AutoSupport訊息
API 呼叫	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

Google Cloud 權限和所需的防火牆規則

控制台代理的 Google Cloud 權限

控制台代理程式需要權限才能在 Google Cloud 中執行操作。這些權限包含在NetApp提供的自訂角色中。您應該了解代理程式使用這些權限做什麼。

Google Cloud 使用者帳戶權限

以下自訂角色賦予 Google Cloud 使用者部署代理程式所需的權限。將此自訂角色指派給將要部署代理程式的使用者。

查看 **Google Cloud** 使用者帳戶權限

```
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
```

服務帳戶權限

以下自訂角色可賦予附加至控制台代理程式的 Google Cloud 服務帳號管理 Google Cloud 網路中的資源和流程所需的權限。

將此自訂角色套用至附加至控制台代理虛擬機器的服務帳戶。

- "設定標準模式的 Google Cloud 權限"
- "設定限制模式的權限"

查看 **Google** 服務帳號權限

隨著後續版本中權限的增加或刪除，請確保角色資訊保持最新。變更日誌列出了所有需要的新權限。"查看 Google 權限變更日誌" "查看如何新增 Google Cloud 服務帳號"

```
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 權限的使用方式

控制台代理程式使用自訂角色中的權限來管理 Google Cloud 網路中的Cloud Volumes ONTAP資源和NetApp資料服務流程。以下各節描述了代理如何使用這些權限。

Cloud Volumes ONTAP所使用的權限

控制台代理程式使用自訂角色中的權限來管理 Google Cloud 網路中的Cloud Volumes ONTAP資源和進程。以下各節描述了代理如何使用這些權限。

Cloud Volumes ONTAP的權限

行動	目的	用於部署？	用於日常營運？	用於刪除？
config.deployments.create	使用 Google Cloud Infrastructure Manager 部署Cloud Volumes ONTAP虛擬機器實例。	是的	不	不
config.deployments.delete		不	不	是的
config.deployments.deleteState		不	不	是的
config.deployments.get		不	是的	是的
config.deployments.getLock		不	是的	不
config.deployments.getState		不	是的	不
config.deployments.list		不	是的	不
config.deployments.lock		不	是的	不
config.deployments.update		不	是的	不
config.deployments.updateState		不	是的	不
config.operations.get		不	是的	不
config.previews.get		不	是的	不
config.previews.list		不	是的	不
config.resources.list		不	是的	不
config.revisions.get		不	是的	不
計算磁碟創建	為Cloud Volumes ONTAP建立和管理磁碟。	是的	是的	不
compute.disk.createSnapshot		不	是的	不
計算磁碟刪除		不	是的	是的
計算磁碟獲取		不	是的	不
計算磁碟列表		是的	是的	不
計算磁碟設定標籤		是的	是的	不
計算磁碟使用		不	是的	不

行動	目的	用於部署？	用於日常營運？	用於刪除？
計算防火牆創建	為Cloud Volumes ONTAP建立防火牆規則。	是的	不	不
計算防火牆刪除		不	是的	是的
計算防火牆		是的	是的	不
計算防火牆列表		是的	是的	不
計算轉送規則創建	建立轉送規則，將流量路由到後端服務。	不	是的	不
計算轉送規則刪除	刪除現有轉送規則。	不	是的	不
計算轉送規則	取得現有轉送規則的詳細資訊。	不	是的	不
計算.轉送規則.設定標籤	設定或更新組織轉送規則的標籤。	不	是的	不
compute.forwardingRules.update	更新現有的流量管理轉送規則。	不	是的	不
compute.globalOperations.get	獲取操作狀態。	是的	是的	不
計算健康檢查創建	建立和管理健康檢查，以監控後端服務的運作狀況。	不	是的	不
compute.healthChecks.delete		不	是的	不
compute.healthChecks.get		不	是的	不
compute.healthChecks.useReadOnly		不	是的	不
compute.images.get	取得虛擬機器實例的影像。	是的	不	不
compute.images.getFromFamily		是的	不	不
計算圖像列表		是的	不	不
compute.images.useReadOnly		是的	不	不
compute.instances.attachDisk	將磁碟附加到Cloud Volumes ONTAP中分離磁碟。	是的	是的	不
compute.instances.detachDisk		不	是的	是的
compute.instances.create	建立和刪除Cloud Volumes ONTAP VM 實例。	是的	不	不
compute.instances.delete		不	不	是的

行動	目的	用於部署？	用於日常營運？	用於刪除？
compute.instances.get	列出虛擬機器實例。	是的	是的	不
compute.instances.getSerialPortOutput	取得控制台日誌。	是的	是的	不
compute.instances.list	檢索區域中的實例清單。	是的	是的	不
compute.instances.setDeletionProtection	對實例設定刪除保護。	是的	不	不
compute.instances.setLabels	新增標籤。	是的	不	不
compute.instances.setMachineType	變更Cloud Volumes ONTAP的機器類型。	是的	是的	不
compute.instances.setMinCpuPlatform		是的	是的	不
compute.instances.setMetadata	新增元資料。	是的	是的	不
compute.instances.setTags	為防火牆規則新增標籤。	是的	是的	不
計算實例開始	啟動和停止Cloud Volumes ONTAP。	是的	是的	不
compute.instances.stop		是的	是的	不
compute.instances.updateDisplayDevice		是的	是的	不
compute.instances.use	使用虛擬機器實例（啟動、停止、連線操作）。	不	是的	不
compute.machineTypes.get	取得核心數以檢查配額。	是的	不	不
compute.projects.get	支援多項目。	是的	不	不
計算資源策略創建	建立和管理資源策略，實現資源自動化管理。	不	是的	不
計算資源策略刪除		不	是的	不
compute.resourcePolicies.get		不	是的	不

行動	目的	用於部署？	用於日常營運？	用於刪除？
計算快照創建	建立和管理持久性磁碟快照。	是的	是的	不
計算快照刪除		不	是的	是的
計算快照獲取		不	是的	不
計算快照列表		不	是的	不
計算快照.設定標籤		是的	是的	不
compute.networks.get	取得建立新的Cloud Volumes ONTAP虛擬機器實例所需的網路資訊。	是的	是的	不
計算網路列表		是的	是的	不
計算區域		是的	是的	不
計算區域列表		是的	是的	不
計算子網路		是的	是的	不
計算子網路列表		是的	是的	不
compute.zoneOperations.get		是的	是的	不
計算區域		是的	是的	不
計算區域列表		是的	是的	不

行動	目的	用於部署？	用於日常營運？	用於刪除？
deploymentmanager.compositeTypes.get	使用 Google Cloud Deployment Manager 部署Cloud Volumes ONTAP虛擬機器實例。	是的	不	不
deploymentmanager.compositeTypes.list		是的	不	不
deploymentmanager.deployments.create		是的	不	不
deploymentmanager.deployments.delete		是的	不	不
deploymentmanager.deployments.get		是的	不	不
deploymentmanager.deployments.list		是的	不	不
deploymentmanager.manifests.get		是的	不	不
deploymentmanager.manifests.list		是的	不	不
deploymentmanager.operations.get		是的	不	不
deploymentmanager.operations.list		是的	不	不
deploymentmanager.resources.get		是的	不	不
deploymentmanager.resources.list		是的	不	不
deploymentmanager.typeProviders.get		是的	不	不
deploymentmanager.typeProviders.list		是的	不	不
deploymentmanager.types.get		是的	不	不
deploymentmanager.types.list		是的	不	不
日誌記錄條目列表	取得堆疊日誌驅動器。	是的	是的	不
logging.privateLogEntries.list		是的	是的	不

行動	目的	用於部署？	用於日常營運？	用於刪除？
日誌記錄條目創建	建立並路由日誌條目，用於監控、偵錯和稽核。	是的	是的	不
日誌記錄.日誌條目.路由		是的	是的	不
resourcemanager.projects.get	支援多項目。	是的	是的	不
儲存桶創建	建立和管理用於資料分層的 Google Cloud Storage 儲存桶。	是的	是的	不
儲存桶刪除		不	是的	是的
存儲桶獲取		不	是的	不
儲存桶列表		不	是的	不
儲存桶更新		不	是的	不
cloudkms.cryptoKeyVersions.useToEncrypt	將來自 Cloud Key Management Service 的客戶管理加密金鑰與Cloud Volumes ONTAP結合使用。	是的	是的	不
cloudkms.cryptoKeys.get		是的	是的	不
cloudkms.cryptoKeys.列表		是的	是的	不
cloudkms.keyRings.列表		是的	是的	不
cloudbuild.builds.get		是的	不	不
cloudbuild.workerpools.get	使用 Infrastructure Manager 在私有模式部署和轉換 Cloud Volumes ONTAP 系統期間存取工作池資訊。	是的	是的	是的
cloudbuild.workerpools.list	使用 Infrastructure Manager 在私有模式下部署 Cloud Volumes ONTAP 系統時，列出工作池資訊。	是的	不	不

行動	目的	用於部署？	用於日常營運？	用於刪除？
compute.instances.setServiceAccount	在Cloud Volumes ONTAP實例上設定服務帳戶。此服務帳戶提供將資料分層至 Google Cloud Storage 儲存桶的權限。	是的	是的	不
iam.serviceAccounts.actAs		是的	不	不
iam.serviceAccounts.create		是的	不	不
iam.serviceAccounts.getIamPolicy		是的	是的	不
iam.serviceAccounts.list		是的	是的	不
iam.serviceAccountKeys.create		是的	不	不
storage.objects.create	在 Google Cloud Storage 儲存桶中建立和管理物件（檔案）。	是的	是的	不
儲存物件刪除		不	不	是的
storage.objects.get		是的	是的	不
儲存物件列表		是的	是的	不
計算地址列表	在部署 HA 對時檢索區域中的位址。	是的	不	不
計算.位址.建立內部	在VPC網路內建立內部IP位址以進行資源分配。	不	是的	不
計算.位址.刪除內部	刪除內部 IP 位址以進行資源清理。	不	是的	不
計算.位址.設定標籤	更新地址資源上的標籤。	不	是的	不
計算.位址.使用內部位址	網路通訊請使用內部IP位址。	不	是的	不
compute.backendServices.create	配置後端服務以在 HA 對中分配流量。	是的	不	不

行動	目的	用於部署？	用於日常營運？	用於刪除？
compute.regionBackendServices.create	建立和管理用於流量路由的後端服務。	是的	不	不
compute.regionBackendServices.delete		不	是的	不
compute.regionBackendServices.get		是的	不	不
compute.regionBackendServices.update		是的	是的	不
compute.regionBackendServices.list		是的	不	不
compute.regionBackendServices.use		不	是的	不
compute.networks.updatePolicy	在 HA 對的 VPC 和子網路上套用防火牆規則。	是的	不	不
compute.instanceGroups.get	在Cloud Volumes ONTAP HA 對上建立和管理儲存虛擬機器。	是的	是的	不
計算地址		是的	是的	不
計算.實例.更新網路介面		是的	是的	不
compute.instanceGroups.create		不	是的	不
compute.instanceGroups.delete		不	是的	不
compute.instanceGroups.update		不	是的	不
compute.instanceGroups.use		不	是的	不
監控時間序列列表	發現有關 Google Cloud Storage 儲存桶的資訊。	是的	是的	不
storage.buckets.getIamPolicy		是的	是的	不

NetApp Backup and Recovery所使用的權限

控制台代理程式使用自訂角色中的權限來管理 Google Cloud 網路中的NetApp Backup and Recovery資源和進程。以下各節描述了代理如何使用這些權限。

查看**NetApp Backup and Recovery**的權限

行動	目的	用於部署？	用於日常營運？	用於刪除？
• 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啟動精靈中選擇您自己的客戶管理金鑰，而不是使用預設的 Google 管理加密金鑰。	是的	是的	不

NetApp Data Classification所使用的權限

控制台代理程式使用自訂角色中的權限來管理 Google Cloud 網路中的NetApp Data Classification資源和進程。以下各節描述了代理如何使用這些權限。

查看**NetApp Data Classification**的權限

行動	目的	用於部署？	用於日常營運？	用於刪除？
• 計算子網路使用 • compute.subnetworks.useExternalIp • compute.instances.addAccessConfig	啟用NetApp Data Classification。	是的	不	不

更改日誌

新增和移除的權限如下所示。

2026 年 **2** 月 **26** 日

新增 `cloudbuild.workerpools.get` 和 `cloudbuild.workerpools.list` 權限是為了支援 Google Cloud 中 Cloud Volumes ONTAP 私有模式部署的 Infrastructure Manager。

2026 年 **2** 月 **09** 日

新增 `compute.forwardingRules.update`權限是為了支援 Google Cloud 中 Cloud Volumes ONTAP 部署的 Infrastructure Manager。

2025年**12**月**8**日

NetApp正在從 Google Cloud Deployment Manager 遷移到 Google Cloud Infrastructure Manager (IM)，以便在 Google Cloud 中部署和執行控制台代理程式。為支援此更改，新增了以下權限。

部署代理程式的 Google Cloud 使用者需要以下附加權限：

- 儲存桶創建
- 存儲桶獲取
- storage.objects.create
- 儲存資料夾創建
- 儲存物件列表
- iam.serviceAccount.actAs
- config.deployments.create
- config.operations.get

用於日常運營的 Google Cloud 服務帳號需要以下額外權限：

- 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
- 日誌記錄條目創建
- storage.objects.create
- 儲存物件刪除
- 儲存物件更新
- iam.serviceAccounts.get

部署Cloud Volumes ONTAP需要以下附加權限：

- 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

對於用於Cloud Volumes ONTAP日常操作的服務帳戶，需要下列附加權限。

- 計算.位址.建立內部
- 計算.位址.刪除內部
- 計算.位址.設定標籤

- 計算.位址.使用內部位址
- 計算轉送規則創建
- 計算轉送規則刪除
- 計算轉送規則
- 計算.轉送規則.設定標籤
- 計算健康檢查創建
- 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
- 計算資源策略創建
- 計算資源策略刪除
- compute.resourcePolicies.get
- 日誌記錄.日誌條目.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

權限已更新，以使其用途更加清晰，但未添加或刪除任何權限。新增三列，分別指示每個權限是用於部署、日常操作或刪除。除此之外，還有一些權限根據其在NetApp Data Classification和NetApp Backup and Recovery的用途進行了劃分。

2023年2月6日

此策略中新增了以下權限：

- 計算.實例.更新網路介面

Cloud Volumes ONTAP需要此權限。

2023年1月27日

此策略新增了以下權限：

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

NetApp Backup and Recovery需要這些權限。

Google Cloud 中的代理防火牆規則

代理程式的 Google Cloud 防火牆規則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。對於其他安裝選項，您需要手動設定此安全性群組。

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	提供從客戶端 Web 瀏覽器到本機使用者介面的 HTTPS 訪問
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

代理程式的預定義防火牆規則開啟所有出站流量。如果可以接受，請遵循基本出站規則，或使用進階出站規則來滿足更嚴格的要求。

基本出站規則

代理程式的預定義防火牆規則包括以下出站規則。

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

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開啟代理出站通訊所需的連接埠。

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 Google Cloud、 ONTAP、 NetApp Data Classification 的API 調用，以及 向NetApp發 送AutoSupport訊息
API 呼叫	TCP	8080	資料分類	部署期間探測資料分 類實例
DNS	UDP	53	DNS	用於資料分類的 DNS 解析