



參考

NetApp Console setup and administration

NetApp

January 23, 2026

目錄

參考	1
代理維護控制台	1
使用維護控制台進行代理驗證	1
透明代理命令	2
雲端提供者代理權限和網路要求	4
NetApp Console的權限摘要	4
AWS 代理權限和安全性規則	7
Azure 權限和所需安全性規則	37
Google Cloud 權限和所需的防火牆規則	59
3.9.55 及以下版本需要網路訪問	80
將您的終端機清單更新為 4.0.0 及更高版本的修訂清單	80
3.9.55 及以下版本的NetApp Console和控制台代理的端點	82
控制台代理聯繫的雲端提供者端點	82
控制台代理聯繫的資料服務端點	82
要求在 Amazon EC2 執行個體上使用 IMDSv2	83
控制台代理的預設配置	84
可存取互聯網的預設配置	85
無需互聯網訪問的預設配置	86

參考

代理維護控制台

使用維護控制台進行代理驗證

您可以使用控制台代理維護控制台來驗證控制台代理程式的安裝和配置。

存取代理維護控制台

您可以從控制台代理主機存取維護控制台。導航到以下目錄：

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

配置檢查器驗證

這 `config-checker validate` 此命令可讓您驗證控制台代理的配置。

參數

`--services <comma-separated list of services to validate>` - 必需的 -

選擇一項或多項服務進行驗證。有效的服務名稱包括：* `PLATFORM` 驗證與所需控制台端點的網路連線。

`--validationTypes <comma-separated list validation types to run>` -- 必填 -- 選擇要執行的一種或多種驗證類型。有效的驗證類型包括：* `NETWORK` 驗證與所需控制台端點的網路連線。

`--proxy <url>` - 選修的 -

指定用於驗證的代理伺服器 URL。如果您的代理程式配置為使用代理伺服器，則此項目為必填項。

`--certs <paths>` - 選修的 -

指定用於驗證的一個或多個證書檔案的路徑。證書文件必須為 PEM 格式。多個路徑之間以逗號分隔。如果您的代理程式使用自訂證書，則此參數為必填項。

配置檢查器驗證範例

基本驗證：

```
./agent-maint-console config-checker validate --services PLATFORM  
--validationTypes NETWORK
```

使用代理伺服器作為代理時的驗證：

```
./agent-maint-console config-checker validate --services PLATFORM  
--validationTypes NETWORK --proxy http://proxy.company.com:8080
```

使用證書驗證代理程式：

```
./agent-maint-console config-checker validate --services PLATFORM  
--validationTypes NETWORK --certs /path/to/cert1.pem,/path/to/cert2.pem
```

查看任何命令的幫助

若要查看任何命令的協助，請附加 `--help` 到命令。例如，要查看 `proxy add` 命令，使用以下命令：

```
./agent-maint-console proxy add --help
```

透明代理命令

您可以使用控制台代理維護控制台來設定控制台代理以使用透明代理伺服器。

存取代理維護控制台

您可以從控制台代理主機存取維護控制台。導航到以下目錄：

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

查看任何命令的幫助

若要查看任何命令的協助，請附加 `--help` 到命令。例如，要查看 `proxy add` 命令，使用以下命令：

```
./agent-maint-console proxy add --help
```

代理獲取

這 `proxy get` 此命令顯示有關目前透明代理伺服器配置的資訊。若要查看目前透明代理伺服器配置，請使用下列命令：

代理獲取範例

若要查看目前透明代理伺服器配置，請使用下列命令：

```
./agent-maint-console proxy get
```

新增代理

這 `proxy add` 該命令將代理配置為使用透明代理伺服器。

參數

`-c <certificate file>`

指定代理伺服器憑證檔案的路徑。證書文件必須為 PEM 格式。確保證書檔案與命令位於同一目錄中，或指定證書檔案的完整路徑。

代理添加範例

若要新增透明代理伺服器，請使用以下命令，其中 `/home/ubuntu/myCA1.pem` 是代理伺服器憑證檔案的路徑。證書文件必須為 PEM 格式：

```
./agent-maint-console proxy add -c /home/ubuntu/myCA1.pem
```

代理更新

這 `proxy update` 該命令允許您更新透明代理的憑證。

參數

`-c <certificate file>` 指定代理伺服器憑證檔案的路徑。證書文件必須為 PEM 格式。

確保證書檔案與命令位於同一目錄中，或指定證書檔案的完整路徑。

代理更新範例

若要更新透明代理伺服器的證書，請使用下列命令，其中 `/home/ubuntu/myCA1.pem` 是代理伺服器的新憑證檔案的路徑。證書文件必須為 PEM 格式：

```
./agent-maint-console proxy update -c /home/ubuntu/myCA1.pem
```

代理移除

這 `proxy remove` 此命令從代理程式中移除透明代理伺服器設定。

代理移除範例

若要刪除透明代理伺服器，請使用以下命令：

```
./agent-maint-console proxy remove
```

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"
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"
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"](#)

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:AssociatelamInstanceProfile	是的	是的	不
	ec2：描述lamInstanceProfile Associations	是的	是的	不
	ec2：解除關聯lamInstanceProfile	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 金鑰管理服务 (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

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

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](#)"

```
{  
  "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/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/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/action",
    "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/v irtualMachines/insta nceView/讀取	是的	是的	不
	Microsoft.Compute/v irtualMachines/powe rOff/action	是的	是的	不
	Microsoft.Compute/ 虛擬機器/讀取	是的	是的	不
	Microsoft.Compute/v irtualMachines/重新 啟動/操作	是的	是的	不
	Microsoft.Compute/v irtualMachines/啟動/ 操作	是的	是的	不
	Microsoft.Compute/v irtualMachines/解除 指派/操作	不	是的	是的
	Microsoft.Compute/v irtualMachines/vmSi zes/讀取	不	是的	不
	Microsoft.Compute/ 虛擬機器/寫入	是的	是的	不
	Microsoft.Compute/v irtualMachines/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。

```
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"

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
- 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.update
- config.deployments.updateState
- config.previews.upload
- config.revisions.get
- config.revisions.getState
- config.deployments.getLock
- config.deployments.list
- config.deployments.lock
- 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.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.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.objects.get
- storage.objects.list
- 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	不
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.preview.get		不	是的	不
config.preview.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.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
compute.instances.get	列出虛擬機器實例。	是的	是的	不

行動	目的	用於部署？	用於日常營運？	用於刪除？
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
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

行動	目的	用於部署？	用於日常營運？	用於刪除？
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
儲存桶獲取		不	是的	不
儲存桶列表		不	是的	不
儲存桶更新		不	是的	不
cloudkms.cryptoKeysVersions.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
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

行動	目的	用於部署？	用於日常營運？	用於刪除？
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
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

行動	目的	用於部署？	用於日常營運？	用於刪除？
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.useExternally • 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。

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

用於日常營運的 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

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 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

3.9.55 及以下版本需要網路訪問

NetApp Console、NetApp Console代理程式和NetApp資料服務需要出站網路存取才能聯絡必要的端點。



本主題記錄了NetApp Console標準模式 3.9.55 及以下版本所需的網路存取。對於 4.0.0 及更高版本所需的端點，請查看["4.0.0 及更高版本所需的端點"](#)。

您需要為以下內容設定網路存取：

- 以軟體即服務 (SaaS) 形式存取NetApp Console的計算機
- 您在本機或雲端安裝的控制台代理程式。

將您的終端機清單更新為 4.0.0 及更高版本的修訂清單

從 4.0.0 版本開始，控制台代理需要的端點更少。4.0.0 之前的現有部署仍然受支援。升級到 4.0.0 或更高版本後，您可以在方便時從允許清單中刪除舊端點。

NetApp建議更新防火牆規則以使用修訂後的端點列表，該列表更小、更安全且更易於管理。NetApp消除了對通配符條目的需求，且代理程式升級的端點支援所有資料服務。

適用於 3.9.55 及以下版本的端點	4.0.0 以上版本的端點	目的
• \ https://support.netapp.com • \ https://mysupport.netapp.com	• \ https://mysupport.netapp.com • \ https://signin.b2c.netapp.com • \ https://support.netapp.com	用於許可和聯繫NetApp支援。

適用於 3.9.55 及以下版本的端點	4.0.0 以上版本的端點	目的
• https://*.api.blueexp.netapp.com • \ https://api.blueexp.netapp.com • https://*.cloudmanager.cloud.netapp.com • \ https://cloudmanager.cloud.netapp.com • \ https://netapp-cloud-account.auth0.com • \ https://netapp-cloud-account.us.auth0.com • \ https://console.blueexp.netapp.com • https://*.console.blueexp.netapp.com	• \ https://api.blueexp.netapp.com • \ https://netapp-cloud-account.auth0.com • \ https://netapp-cloud-account.us.auth0.com • \ https://console.netapp.com • \ https://components.console.blueexp.netapp.com • \ https://cdn.auth0.com	用於日常營運。
• https://*.blob.core.windows.net • \ https://cloudmanagerinfraprod.azurecr.io	• \ https://bluexpinfraprod.eastus2.data.azurecr.io • \ https://bluexpinfraprod.azurecr.io	取得控制台代理升級的影像。

步驟

1. 驗證您的代理是否為 4.0.0 或更高版本。["查看代理版本。"](#)
2. 將端點列入白名單["4.0.0 及更高版本支援的端點"](#)。
3. 透過執行以下命令重新啟動每個代理程式上的服務管理員 2 服務：

```
systemctl restart netapp-service-manager.service
```

4. 執行以下指令並驗證代理程式的狀態是否顯示為 `_active(running)`：

```
systemctl status netapp-service-manager.service
```

5. 從防火牆允許清單中刪除舊端點。

3.9.55 及以下版本的NetApp Console和控制台代理的端點

這些端點用於控制台代理 3.9.55 及以下版本。

端點	目的
\ https://support.netapp.com \ https://mysupport.netapp.com	取得許可資訊並向NetApp支援發送AutoSupport訊息。
https://*.api.bluelxp.netapp.com \ https://api.bluelxp.netapp.com https://*.cloudmanager.cloud.netapp.com \ https://cloudmanager.cloud.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com	在NetApp Console中提供功能和服務。
在兩組端點之間進行選擇： • 選項 1（建議） \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • 選項 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	取得控制台代理升級的影像。 NetApp建議在防火牆中允許選項 1 端點，因為它們更安全，並禁止選項 2 端點，除非您使用勒索軟體復原或備份和復原。請注意有關這些端點的以下事項： • 3.9.47 及更高版本支援選項 1 端點。3.9.47 之前的版本不支援向後相容。 • 控制台代理首先啟動與選項 2 中的端點的聯繫。如果這些端點不可訪問，它會自動聯繫選項 1 中的端點。 • 如果將控制台代理程式與NetApp Backup and Recovery或 Ransomware Resilience 一起使用，則系統不支援選項 1 端點。允許選項 2 端點並不允許選項 1。

控制台代理聯繫的雲端提供者端點

如果控制台代理程式部署在您的雲端提供者中，則它們必須能夠存取其他端點。

在安裝控制台代理之前啟用對雲端提供者端點的存取。

- "為控制台代理程式設定 [AWS 網路訪問](#)"
- "為控制台代理程式設定 [Azure 網路訪問](#)"
- "為控制台代理設定 [Google Cloud 網路訪問](#)"

所有版本的雲端供應商端點都是相同的。

控制台代理聯繫的資料服務端點

控制台代理程式需要額外的外部網路存取來支援某些NetApp資料服務和Cloud Volumes ONTAP。

Cloud Volumes ONTAP的端點

- ["AWS 中的Cloud Volumes ONTAP端點"](#)
- ["Azure 中的Cloud Volumes ONTAP端點"](#)
- ["Google Cloud 中Cloud Volumes ONTAP的端點"](#)

要求在 Amazon EC2 執行個體上使用 IMDSv2

NetApp Console透過控制台代理程式和Cloud Volumes ONTAP（包括 HA 部署的中介）支援 Amazon EC2 執行個體元資料服務版本 2 (IMDSv2)。大多數情況下，IMDSv2 會在新的 EC2 執行個體上自動設定。IMDSv1 於 2024 年 3 月前啟用。如果您的安全性原則需要，您可能需要在 EC2 執行個體上手動設定 IMDSv2。

開始之前

- 控制台代理版本必須為 3.9.38 或更高版本。
- Cloud Volumes ONTAP必須執行下列版本之一：
 - 9.12.1 P2（或任何後續補丁）
 - 9.13.0 P4（或任何後續補丁）
 - 9.13.1 或此版本之後的任何版本
- 此變更要求您重新啟動Cloud Volumes ONTAP實例。
- 這些步驟需要使用 AWS CLI，因為您必須將回應跳數限制變更為 3。

關於此任務

IMDSv2 提供了增強的針對漏洞的保護。 ["從 AWS 安全部落格了解有關 IMDSv2 的更多信息"](#)

執行個體元資料服務 (IMDS) 在 EC2 執行個體上啟用如下：

- 對於從控制台或使用 ["Terraform 腳本"](#)，IMDSv2 在 EC2 執行個體上預設啟用。
- 如果您在 AWS 中啟動新的 EC2 實例，然後手動安裝控制台代理軟體，則 IMDSv2 也會預設為啟用。
- 如果您從 AWS Marketplace 啟動控制台代理，則預設啟用 IMDSv1。您可以在 EC2 執行個體上手動設定 IMDSv2。
- 對於現有的控制台代理，仍然支援 IMDSv1，但如果您願意，可以在 EC2 執行個體上手動設定 IMDSv2。
- 對於Cloud Volumes ONTAP，IMDSv1 在新實例和現有實例上預設為啟用。如果願意，您可以在 EC2 執行個體上手動設定 IMDSv2。

步驟

1. 要求在控制台代理實例上使用 IMDSv2：

- a. 連接到控制台代理的 Linux VM。

當您在 AWS 中建立控制台代理執行個體時，您提供了 AWS 存取金鑰和金鑰。您可以使用此金鑰對透過 SSH 連線到執行個體。EC2 Linux 執行個體的使用者名稱是 ubuntu（對於 2023 年 5 月之前建立的控制台代理，使用者名稱是 ec2-user）。

"AWS 文件：連接到您的 Linux 實例"

- b. 安裝 AWS CLI。

"AWS 文件：安裝或更新至最新版本的 AWS CLI"

- c. 使用 `aws ec2 modify-instance-metadata-options` 命令要求使用 IMDSv2 並將 PUT 回應跳數限制更改為 3。

例子

```
aws ec2 modify-instance-metadata-options \
  --instance-id <instance-id> \
  --http-put-response-hop-limit 3 \
  --http-tokens required \
  --http-endpoint enabled
```

+



這 `http-tokens` 參數將 IMDSv2 設定為必要。什麼時候 `http-tokens` 是必需的，您還必須設置 `http-endpoint` 啟用。

2. 要求在 Cloud Volumes ONTAP 實例上使用 IMDSv2：

- a. 前往 "[Amazon EC2 主機](#)"
- b. 從導覽窗格中，選擇*實例*。
- c. 選擇一個 Cloud Volumes ONTAP 實例。
- d. 選擇*操作>實例設定>修改實例元資料選項*。
- e. 在「修改實例元資料選項」對話方塊中，選擇以下內容：
 - 對於*實例元資料服務*，選擇*啟用*。
 - 對於 **IMDSv2**，選擇 必要。
 - 選擇*儲存*。
- f. 對其他 Cloud Volumes ONTAP 實例（包括 HA 中介）重複這些步驟。
- g. "[停止並啟動 Cloud Volumes ONTAP 實例](#)"

結果

控制台代理實例和 Cloud Volumes ONTAP 實例現在已配置為使用 IMDSv2。

控制台代理的預設配置

了解 AWS、Azure 和 Google Cloud 上標準部署（可存取網際網路）的控制台代理預設配置，以及本機環境受限部署（無法存取網際網路）的控制台代理程式預設配置。

可存取互聯網的預設配置

如果您從NetApp Console、雲端提供者的市場部署了控制台代理，或在具有 Internet 存取權限的本機 Linux 主機上手動安裝了控制台代理，則下列設定詳細資訊適用。

AWS 控制台代理 VM 詳細信息

如果您從控制台或雲端提供者的市場部署了控制台代理，請注意以下事項：

- EC2 執行個體類型為 t3.2xlarge。
- 該映像的作業系統是 Ubuntu 22.04 LTS。

該作業系統不包含 GUI。您必須使用終端來存取系統。

- 安裝包括 Docker Engine，它是必需的容器編排工具。
- EC2 Linux 執行個體的使用者名稱是 ubuntu（對於 2023 年 5 月之前建立的代理，使用者名稱是 ec2-user）。
- 預設系統磁碟是 100 GiB gp2 磁碟。

Azure 控制台代理 VM 詳細信息

如果您從控制台或雲端提供者的市場部署了控制台代理，請注意以下事項：

- VM 類型為 Standard_D8s_v3。
- 該映像的作業系統是 Ubuntu 22.04 LTS。

該作業系統不包含 GUI。您必須使用終端來存取系統。

- 安裝包括 Docker Engine，它是必需的容器編排工具。
- 預設系統碟為100GiB高級SSD碟。

Google Cloud 控制台代理 VM 詳細信息

如果您從控制台部署了控制台代理，請注意以下事項：

- VM 實例是 n2-standard-8。
- 該映像的作業系統是 Ubuntu 22.04 LTS。

該作業系統不包含 GUI。您必須使用終端來存取系統。

- 安裝包括 Docker Engine，它是必需的容器編排工具。
- 預設系統磁碟是 100 GiB SSD 持久性磁碟。

安裝資料夾

代理程式安裝資料夾位於下列位置：

/opt/application/netapp/cloudmanager

紀錄檔案

日誌檔案包含在以下資料夾中：

- `/opt/application/netapp/cloudmanager/log` 或者
- `/opt/application/netapp/service-manager-2/logs` （從新安裝的 3.9.23 版本開始）

這些資料夾中的日誌提供了有關控制台代理的詳細資訊。

- `/opt/application/netapp/cloudmanager/docker_occm/data/log`

此資料夾中的日誌提供有關雲端服務和在控制台代理程式上運行的控制台服務的詳細資訊。

控制台代理服務

- 控制台代理服務名為 `occm`。
- `occm` 服務依賴 MySQL 服務。

如果 MySQL 服務關閉，那麼 `occm` 服務也會關閉。

連接埠

代理在 Linux 主機上使用下列連接埠：

- 80 用於 HTTP 訪問
- 443 用於 HTTPS 訪問

無需互聯網訪問的預設配置

如果您在沒有網際網路存取權限的本機 Linux 主機上手動安裝了控制台代理，則適用下列設定。["了解有關此安裝選項的更多信息"](#)。

- 代理程式安裝資料夾位於下列位置：

`/opt/application/netapp/ds`

- 日誌檔案包含在以下資料夾中：

`/var/lib/docker/volumes/ds_occmdata/_data/log`

此資料夾中的日誌提供有關控制台代理程式和 Docker 映像的詳細資訊。

- 所有服務都在docker容器內運行

這些服務依賴docker運行時服務的運行

- 代理在 Linux 主機上使用下列連接埠：
 - 80 用於 HTTP 訪問

- 443 用於 HTTPS 訪問

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。