# Referencia

## NetApp Console setup and administration

NetApp
January 23, 2026

# Tabla de contenidos

# Referencia

## Consola de mantenimiento del agente

### Validación del agente con la consola de mantenimiento

Puede utilizar la consola de mantenimiento del agente de consola para validar la instalación y configuración de un agente de consola.

#### Acceder a la consola de mantenimiento del agente

Puede acceder a la consola de mantenimiento desde el host del agente de la consola. Navegue al siguiente directorio:

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

#### Validación del comprobador de configuración

El `config-checker validate` El comando le permite validar la configuración de un agente de consola.

##### Parámetros

`--services <comma-separated list of services to validate>`**--REQUERIDO--**

Elija uno o más servicios para validar. Los nombres de servicio válidos son:*`PLATFORM` que valida la conectividad de la red a los puntos finales de la consola requeridos.

`--validationTypes <comma-separated list validation types to run>`**--OBLIGATORIO--** Elija entre uno o más tipos de validación para ejecutar. Los tipos de validación válidos son: * `NETWORK` que valida la conectividad de la red a los puntos finales de la consola requeridos.

`--proxy <url>`**--OPCIONAL--**

Especifica la URL del servidor proxy que se utilizará para la validación. Obligatorio si su agente está configurado para utilizar un servidor proxy.

`--certs <paths>`**--OPCIONAL--**

Especifica la ruta a uno o más archivos de certificado que se utilizarán para la validación. Los archivos del certificado deben estar en formato PEM. Separe varias rutas con comas. Este parámetro es necesario si su agente utiliza un certificado personalizado.

##### Ejemplos de validación del verificador de configuración

**Validación básica:**

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

**Validación donde se utiliza un servidor proxy para el agente:**

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

**Validación donde se utiliza un certificado para el agente:**

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

#### Ver ayuda para cualquier comando

Para ver la ayuda de cualquier comando, agregue `--help` al mando. Por ejemplo, para ver la ayuda de la `proxy add` Comando, utilice el siguiente comando:

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

## Comandos de proxy transparentes

Puede utilizar la consola de mantenimiento del agente de consola para configurar un agente de consola para que utilice un servidor proxy transparente.

### Acceder a la consola de mantenimiento del agente

Puede acceder a la consola de mantenimiento desde el host del agente de la consola. Navegue al siguiente directorio:

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

#### Ver ayuda para cualquier comando

Para ver la ayuda de cualquier comando, agregue `--help` al mando. Por ejemplo, para ver la ayuda de la `proxy add` Comando, utilice el siguiente comando:

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

### obtención de proxy

El `proxy get` El comando muestra información sobre la configuración actual del servidor proxy transparente. Para ver la configuración actual del servidor proxy transparente, utilice el siguiente comando:

#### Ejemplo de obtención de proxy

Para ver la configuración actual del servidor proxy transparente, utilice el siguiente comando:

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

### añadir proxy

El `proxy add` El comando configura el agente para utilizar un servidor proxy transparente.

#### Parámetros

`-c <certificate file>`

Especifica la ruta al archivo de certificado para el servidor proxy. El archivo del certificado debe estar en formato PEM. Asegúrese de que el archivo del certificado esté en el mismo directorio que el comando o especifique la ruta completa al archivo del certificado.

#### Ejemplo de adición de proxy

Para agregar un servidor proxy transparente, utilice el siguiente comando, donde `/home/ubuntu/myCA1.pem` es la ruta al archivo de certificado para el servidor proxy. El archivo del certificado debe estar en formato PEM:

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

### actualización de proxy

El `proxy update` El comando le permite actualizar el certificado de un proxy transparente.

#### Parámetros

`-c <certificate file>`Especifica la ruta al archivo de certificado para el servidor proxy. El archivo del certificado debe estar en formato PEM.

Asegúrese de que el archivo del certificado esté en el mismo directorio que el comando o especifique la ruta completa al archivo del certificado.

#### Ejemplo de actualización de proxy

Para actualizar el certificado de un servidor proxy transparente, utilice el siguiente comando, donde `/home/ubuntu/myCA1.pem` es la ruta al nuevo archivo de certificado para el servidor proxy. El archivo del certificado debe estar en formato PEM:

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

### eliminar proxy

El `proxy remove` El comando elimina la configuración del servidor proxy transparente del agente.

#### Ejemplo de eliminación de proxy

Para eliminar el servidor proxy transparente, utilice el siguiente comando:

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

# Permisos del agente del proveedor de nube y requisitos de red

## Resumen de permisos para la NetApp Console

Necesitará proporcionar al agente de consola los permisos adecuados para que pueda realizar operaciones en su entorno de nube. Utilice los enlaces de esta página para acceder rápidamente a los permisos que necesita según su objetivo.

### Permisos de AWS

La NetApp Console requiere permisos de AWS para un agente de consola y para servicios individuales.

#### Agentes de consola

| Meta | Descripción | Enlace |
|---|---|---|
| Implementar un agente de consola desde la consola Para implementar un agente de consola en AWS, el usuario necesita permisos específicos. | "Configurar permisos de AWS" | Proporcionar permisos para un agente de consola |

#### NetApp Backup and Recovery

| Meta | Descripción | Enlace |
|---|---|---|
| Realice copias de seguridad de clústeres ONTAP locales en Amazon S3 con NetApp Backup and Recovery | Al activar las copias de seguridad en sus volúmenes ONTAP , NetApp Backup and Recovery le solicita que ingrese una clave de acceso y un secreto para un usuario de IAM que tenga permisos específicos. | "Configurar permisos S3 para copias de seguridad" |

#### Cloud Volumes ONTAP

| Meta | Descripción | Enlace |
| --- | --- | --- |
| Proporcionar permisos para los nodos de Cloud Volumes ONTAP | Se debe asociar una función de IAM a cada nodo de Cloud Volumes ONTAP en AWS. Lo mismo ocurre con el mediador HA. La opción predeterminada es dejar que la consola cree los roles de IAM para usted, pero puede usar los suyos propios al crear el sistema en la consola. | "Aprenda a configurar usted mismo los roles de IAM" |

#### NetApp Copy and Sync

| Meta | Descripción | Enlace |
| --- | --- | --- |
| Implementar el agente de datos en AWS | La cuenta de usuario de AWS que utilice para implementar el agente de datos debe tener los permisos necesarios. | "Permisos necesarios para implementar el agente de datos en AWS" |
| Proporcionar permisos para el agente de datos | Cuando NetApp Copy and Sync implementa el agente de datos, crea una función de IAM para la instancia del agente de datos. Puede implementar el agente de datos utilizando su propio rol de IAM, si lo prefiere. | "Requisitos para utilizar su propio rol de IAM con el agente de datos de AWS" |
| Habilitar el acceso a AWS para un agente de datos instalado manualmente | Si utiliza el agente de datos con una relación de sincronización que incluye un bucket S3, deberá preparar el host Linux para el acceso a AWS. Cuando instale el agente de datos, deberá proporcionar claves de AWS para un usuario de IAM que tenga acceso programático y permisos específicos. | "Habilitación del acceso a AWS" |

#### FSx para ONTAP

| Meta | Descripción | Enlace |
| --- | --- | --- |
| Crear y administrar FSx para ONTAP | Para crear o administrar un sistema Amazon FSx for NetApp ONTAP , debe agregar credenciales de AWS a la consola proporcionando el ARN de una función de IAM que le otorga a la consola los permisos necesarios. | "Aprenda a configurar las credenciales de AWS para FSx" |

#### NetApp Cloud Tiering

| Meta | Descripción | Enlace |
| --- | --- | --- |
| Integración de clústeres ONTAP locales en Amazon S3 | Cuando habilita NetApp Cloud Tiering en AWS, ingresa una clave de acceso y una clave secreta. Estas credenciales se pasan al clúster de ONTAP para que ONTAP pueda organizar los datos en niveles en el depósito S3. | "Configurar permisos S3 para niveles" |

### Permisos de Azure

La consola requiere permisos de Azure para un agente de consola y para servicios individuales.

#### Agente de consola

| Meta | Descripción | Enlace |
|---|---|---|
| Implementar un agente de consola desde la consola | Cuando implementa un agente de consola desde la consola, debe usar una cuenta de Azure o una entidad de servicio que tenga permisos para implementar una máquina virtual del agente de consola en Azure. | "Configurar permisos de Azure" |
| Proporcionar permisos para un agente de consola | Cuando la consola implementa una máquina virtual del agente de consola en Azure, crea un rol personalizado que proporciona los permisos necesarios para administrar recursos y procesos dentro de esa suscripción de Azure.<br><br>Debe configurar usted mismo el rol personalizado si inicia un agente de consola desde el mercado, si instala manualmente un agente de consola o si"Agregar más credenciales de Azure a un agente de consola" .<br><br>Mantenga la política actualizada a medida que se agreguen nuevos permisos en versiones posteriores. | "Permisos de Azure para un agente de consola" |

#### NetApp Backup and Recovery

| Meta | Descripción | Enlace |
|---|---|---|
| Realice una copia de seguridad de Cloud Volumes ONTAP en el almacenamiento de blobs de Azure | Al usar NetApp Backup and Recovery para realizar copias de seguridad de Cloud Volumes ONTAP, debe agregar permisos a un agente de consola en los siguientes escenarios:<br><br>• Desea utilizar la función "Buscar y restaurar"<br>• Desea utilizar claves de cifrado administradas por el cliente (CMEK) | • "Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Azure Blob Storage con Backup and Recovery" |
| Realizar copias de seguridad de clústeres de ONTAP locales en el almacenamiento de blobs de Azure | Al usar NetApp Backup and Recovery para realizar copias de seguridad de clústeres ONTAP locales, debe agregar permisos a un agente de consola para usar la funcionalidad "Buscar y restaurar". | "Realice una copia de seguridad de los datos de ONTAP locales en el almacenamiento de blobs de Azure con Backup and Recovery" |

#### Copia y sincronización de NetApp

| Meta | Descripción | Enlace |
|---|---|---|
| Implementar el agente de datos en Azure | La cuenta de usuario de Azure que utilice para implementar el agente de datos debe tener los permisos necesarios. | "Permisos necesarios para implementar el agente de datos en Azure" |

### Permisos de Google Cloud

La consola requiere permisos de Google Cloud para un agente de consola y para servicios individuales.

#### Agentes de consola

| Meta | Descripción | Enlace |
|---|---|---|
| Implementar un agente de consola desde la consola | El usuario de Google Cloud que implementa un agente de consola desde la consola necesita permisos específicos para implementar un agente de consola en Google Cloud. | "Configurar permisos para crear un agente de consola" |
| Proporcionar permisos para un agente de consola | La cuenta de servicio de un agente de consola debe tener permisos específicos para las operaciones diarias. Debe asociar la cuenta de servicio con un agente de consola durante la implementación. Mantenga la política actualizada a medida que se agreguen nuevos permisos en versiones posteriores. | "Configurar permisos para un agente de consola" |

#### NetApp Backup and Recovery

| Meta | Descripción | Enlace |
|---|---|---|
| Realizar copias de seguridad de Cloud Volumes ONTAP en Google Cloud | Al usar NetApp Backup and Recovery para realizar copias de seguridad de Cloud Volumes ONTAP, debe agregar permisos a un agente de consola en los siguientes escenarios:<br>• Desea utilizar la función "Buscar y restaurar"<br>• Desea utilizar claves de cifrado administradas por el cliente (CMEK) | • "Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Google Cloud Storage con Backup and Recovery"<br>• "Permisos para CMEK" |
| Realice copias de seguridad de clústeres ONTAP locales en Google Cloud | Al usar NetApp Backup and Recovery para realizar copias de seguridad de clústeres ONTAP locales, debe agregar permisos a un agente de consola para usar la funcionalidad "Buscar y restaurar". | "Realice una copia de seguridad de los datos locales de ONTAP en Google Cloud Storage con Backup and Recovery" |

#### NetApp Copy and Sync

| Meta | Descripción | Enlace |
|---|---|---|
| Implementar el agente de datos en Google Cloud | Asegúrese de que el usuario de Google Cloud que implementa el agente de datos tenga los permisos necesarios. | "Permisos necesarios para implementar el agente de datos en Google Cloud" |

| Meta | Descripción | Enlace |
| --- | --- | --- |
| Habilitar el acceso a Google Cloud para un agente de datos instalado manualmente | Si planea utilizar el agente de datos con una relación de sincronización que incluye un depósito de Google Cloud Storage, entonces debe preparar el host Linux para el acceso a Google Cloud. Cuando instale el agente de datos, deberá proporcionar una clave para una cuenta de servicio que tenga permisos específicos. | "Habilitar el acceso a Google Cloud" |

#### Permisos de StorageGRID

La consola requiere permisos de StorageGRID para dos servicios.

##### NetApp Backup and Recovery

| Meta | Descripción | Enlace |
| --- | --- | --- |
| Realice copias de seguridad de clústeres ONTAP locales en StorageGRID | Cuando prepara StorageGRID como destino de respaldo para clústeres de ONTAP , NetApp Backup and Recovery le solicita que ingrese una clave de acceso y un secreto para un usuario de IAM que tenga permisos específicos. | "Prepare StorageGRID como su destino de respaldo" |

##### NetApp Cloud Tiering

| Meta | Descripción | Enlace |
| --- | --- | --- |
| Integración de clústeres ONTAP locales en StorageGRID | Cuando configura NetApp Cloud Tiering en StorageGRID, debe proporcionar a Cloud Tiering una clave de acceso S3 y una clave secreta. La organización en niveles de la nube utiliza las claves para acceder a sus buckets. | "Preparar la organización en niveles para StorageGRID" |

## Permisos del agente de AWS y reglas de seguridad

#### Permisos de AWS para el agente de consola

Cuando la NetApp Console inicia un agente de consola en AWS, adjunta una política al agente que le proporciona permisos para administrar recursos y procesos dentro de esa cuenta de AWS. El agente usa los permisos para realizar llamadas API a varios servicios de AWS, incluidos EC2, S3, CloudFormation, IAM, el Servicio de administración de claves (KMS) y más.

##### Políticas de IAM

Las políticas de IAM disponibles a continuación proporcionan los permisos que un agente de consola necesita para administrar recursos y procesos dentro de su entorno de nube pública en función de su región de AWS.

Tenga en cuenta lo siguiente:

- Si crea un agente de consola en una región estándar de AWS directamente desde la consola, esta aplicará automáticamente las políticas al agente.
- Debe configurar las políticas usted mismo si implementa el agente desde AWS Marketplace, si instala

manualmente el agente en un host Linux o si desea agregar credenciales de AWS adicionales a la consola.

- En cualquier caso, debe asegurarse de que las políticas estén actualizadas a medida que se agreguen nuevos permisos en versiones posteriores. Si se requieren nuevos permisos, se enumerarán en las notas de la versión.
- Si es necesario, puede restringir las políticas de IAM mediante el IAM `Condition` elemento. "Documentación de AWS: Elemento de condición"
- Para ver instrucciones paso a paso sobre cómo utilizar estas políticas, consulte las siguientes páginas:
  - "Configurar permisos para una implementación de AWS Marketplace"
  - "Configurar permisos para implementaciones locales"
  - "Configurar permisos para el modo restringido"

Seleccione su región para ver las políticas requeridas:

**Regiones estándar**

Para las regiones estándar, los permisos se distribuyen en dos políticas. Se requieren dos políticas debido a un límite máximo de tamaño de caracteres para las políticas administradas en AWS.

**Política #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"
    }
  ]
}
```

**Política #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"
    }
  ]
}
```

**Regiones de GovCloud (EE. UU.)**

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

**Regiones secretas**

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

**Regiones de alto secreto**

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

#### Cómo se utilizan los permisos de AWS

Las siguientes secciones describen cómo se utilizan los permisos para cada servicio de datos o administración de la NetApp Console . Esta información puede ser útil si sus políticas corporativas establecen que los permisos solo se otorgan cuando es necesario.

### Amazon FSx para ONTAP

El agente de la consola realiza las siguientes solicitudes de API para administrar un sistema de archivos de Amazon FSx para ONTAP :

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribute
- ec2:DescribeRouteTables
- ec2:DescribeImages
- ec2:CrearEtiquetas
- ec2:DescribeVolúmenes
- ec2:DescribeSecurityGroups
- ec2: Describir interfaces de red
- ec2:DescribeSubnets

- ec2:DescribeVpcs
- ec2:DescribeDhcpOptions
- ec2:DescribeSnapshots
- ec2:DescribeKeyPairs
- ec2:DescribirRegiones
- ec2:DescribeTags
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeReservedInstancesOfferings
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ec2:DescribeVolumesModifications
- ec2:DescribirGruposDeUbicación
- kms:CrearConcesión
- kms:ListAliases
- fsx:Describir*
- fsx:Lista*

**Descubrimiento de buckets de Amazon S3**

El agente de la consola realiza la siguiente solicitud de API para descubrir buckets de Amazon S3:

s3:Obtener configuración de cifrado

**NetApp Backup and Recovery**

El agente realiza las siguientes solicitudes de API para administrar copias de seguridad en Amazon S3:

- s3: Obtener ubicación del depósito
- s3: Listar todos mis cubos
- s3:ListBucket
- s3:CrearCubo
- s3:Obtener configuración del ciclo de vida
- s3:Configuración del ciclo de vida de PutLifecycle
- s3:Etiquetado de cubo de colocación
- s3:ListBucketVersions
- s3:ObtenerAcl del depósito
- s3:PonerCuboBloqueDeAccesoPúblico
- s3:Obtener objeto
- ec2:DescribeVpcEndpoints
- kms:ListAliases
- s3:PonerConfiguraciónDeCifrado

El agente realiza las siguientes solicitudes de API cuando utiliza el método de búsqueda y restauración para restaurar volúmenes y archivos:

- s3:CrearCubo
- s3:EliminarObjeto
- s3:EliminarVersiónDeObjeto
- s3:ObtenerAcl del depósito
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PonerObjeto
- s3:PonerCuboAcl
- s3:Configuración del ciclo de vida de PutLifecycle
- s3:PonerCuboBloqueDeAccesoPúblico
- s3:AbortarCargaMultiparte
- s3:ListaMultiparteSubirPartes

El agente realiza las siguientes solicitudes de API cuando utiliza DataLock y NetApp Ransomware Resilience para sus copias de seguridad de volumen:

- s3: Obtener etiquetado de versión de objeto
- s3:Configuración de bloqueo de objeto de depósito
- s3:ObtenerAcl de versión de objeto
- s3:Etiquetado de objetos de colocación
- s3:EliminarObjeto
- s3:EliminarEtiquetadoDeObjeto
- s3:ObtenerRetenciónDeObjeto
- s3: Eliminar etiquetado de versión de objeto
- s3:PonerObjeto
- s3:Obtener objeto
- s3:Configuración de bloqueo de objeto PutBucket
- s3:Obtener configuración del ciclo de vida
- s3:ListarCuboPorEtiquetas
- s3: Obtener etiquetado de cubo
- s3:EliminarVersiónDeObjeto
- s3:ListBucketVersions
- s3:ListBucket
- s3:Etiquetado de cubo de colocación
- s3:Obtener etiquetado de objeto
- s3:Versión de PutBucket

- s3:Etiquetado de versión de objeto de colocación
- s3: Obtener versiones de Bucket
- s3:ObtenerAcl del depósito
- s3: Retención de gobernanza de bypass
- s3:PonerRetenciónDeObjeto
- s3: Obtener ubicación del depósito
- s3:ObtenerVersiónDeObjeto

El agente realiza las siguientes solicitudes de API si utiliza una cuenta de AWS diferente para sus copias de seguridad de Cloud Volumes ONTAP que la que utiliza para los volúmenes de origen:

- s3:Política de depósito de colocación
- s3: Controles de propiedad del depósito de colocación

**Permisos heredados para Copia de seguridad y recuperación**

Solo necesitas los siguientes permisos si habilitaste las funciones de indexación heredadas antes del lanzamiento de la versión 2 de indexación:

- kms:Lista*
- kms:Describir*
- athena:IniciarEjecuciónDeConsulta
- atenea:ObtenerResultadosDeConsulta
- athena:ObtenerEjecuciónDeConsulta
- athena:DetenerEjecuciónDeConsulta
- pegamento:CrearBaseDeDatos
- pegamento:CrearTabla
- pegamento:LoteEliminarPartición

**Clasificación**

El agente realiza las siguientes solicitudes de API para implementar NetApp Data Classification:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:EjecutarInstancias
- ec2:Terminar instancias
- ec2:CrearEtiquetas
- ec2:CrearVolumen
- ec2:AdjuntarVolumen
- ec2:CrearGrupoDeSeguridad
- ec2:EliminarGrupoDeSeguridad
- ec2:DescribeSecurityGroups

- ec2:CrearInterfazDeRed
- ec2: Describir interfaces de red
- ec2:EliminarInterfazDeRed
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:CrearInstantánea
- ec2:DescribirRegiones
- formación de nubes:CreateStack
- formación de nubes:Eliminar pila
- formación de nubes: DescribeStacks
- formación de nubes: DescribeStackEvents
- iam:AñadirRolAlPerfilDeInstancia
- ec2:AsociarPerfilDeInstanciaSoy
- ec2:DescribeIamInstanceProfileAssociations

El agente realiza las siguientes solicitudes de API para escanear los depósitos S3 cuando utiliza la NetApp Data Classification:

- iam:AñadirRolAlPerfilDeInstancia
- ec2:AsociarPerfilDeInstanciaSoy
- ec2:DescribeIamInstanceProfileAssociations
- s3: Obtener etiquetado de cubo
- s3: Obtener ubicación del depósito
- s3: Listar todos mis cubos
- s3:ListBucket
- s3: Obtener estado de la política del depósito
- s3: Obtener política de depósito
- s3:ObtenerAcl del depósito
- s3:Obtener objeto
- soy:ObtenerRole
- s3:EliminarObjeto
- s3:EliminarVersiónDeObjeto
- s3:PonerObjeto
- sts:Asumir rol

**Cloud Volumes ONTAP**

El agente realiza las siguientes solicitudes de API para implementar y administrar Cloud Volumes ONTAP en AWS.

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Crear y administrar roles de IAM y perfiles de instancia para instancias de Cloud Volumes ONTAP | iam:ListInstanceProfiles | Sí | Sí | No |
| | soy:CreateRole | Sí | No | No |
| | iam:EliminarRole | No | Sí | Sí |
| | soy:PolíticaDeRolDePut | Sí | No | No |
| | iam:CreateInstanceProfile | Sí | No | No |
| | iam:DeleteRolePolicy | No | Sí | Sí |
| | iam:AñadirRolAlPerfilDeInstancia | Sí | No | No |
| | iam:EliminarRolDePerfilDeInstancia | No | Sí | Sí |
| | iam:EliminarPerfilDeInstancia | No | Sí | Sí |
| | yo soy:PassRole | Sí | No | No |
| | ec2:AsociarPerfilDeInstanciaSoy | Sí | Sí | No |
| | ec2:DescribeIamInstanceProfileAssociations | Sí | Sí | No |
| | ec2: Desasociar perfil de instancia de Iam | No | Sí | No |
| Decodificar mensajes de estado de autorización | sts:Decodificar mensaje de autorización | Sí | Sí | No |
| Describe las imágenes específicas (AMI) disponibles para la cuenta | ec2:DescribeImages | Sí | Sí | No |
| Describe las tablas de rutas en una VPC (requerida solo para pares de alta disponibilidad) | ec2:DescribeRouteTables | Sí | No | No |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Detener, iniciar y supervisar instancias | ec2:Instancias de inicio | Sí | Sí | No |
| | ec2:Detener instancias | Sí | Sí | No |
| | ec2:DescribeInstances | Sí | Sí | No |
| | ec2:DescribeInstanceStatus | Sí | Sí | No |
| | ec2:EjecutarInstancias | Sí | No | No |
| | ec2:Terminar instancias | No | No | Sí |
| | ec2:ModificarAtributoDeInstancia | No | Sí | No |
| Verifique que la red mejorada esté habilitada para los tipos de instancias compatibles | ec2:DescribeInstanceAttribute | No | Sí | No |
| Etiquete los recursos con las etiquetas "WorkingEnvironment" y "WorkingEnvironmentId", que se utilizan para el mantenimiento y la asignación de costos. | ec2:CrearEtiquetas | Sí | Sí | No |
| Administrar volúmenes EBS que Cloud Volumes ONTAP utiliza como almacenamiento de backend | ec2:CrearVolumen | Sí | Sí | No |
| | ec2:DescribeVolúmenes | Sí | Sí | Sí |
| | ec2:ModificarAtributoDeVolumen | No | Sí | Sí |
| | ec2:AdjuntarVolumen | Sí | Sí | No |
| | ec2:EliminarVolumen | No | Sí | Sí |
| | ec2:Separar volumen | No | Sí | Sí |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Crear y administrar grupos de seguridad para Cloud Volumes ONTAP | ec2:CrearGrupoDeSeguridad | Sí | No | No |
| | ec2:EliminarGrupoDeSeguridad | No | Sí | Sí |
| | ec2:DescribeSecurityGroups | Sí | Sí | Sí |
| | ec2:Revocar salida del grupo de seguridad | Sí | No | No |
| | ec2:AutorizarSalidaGrupoSeguridad | Sí | No | No |
| | ec2:AutorizarIngresoDeGrupoDeSeguridad | Sí | No | No |
| | ec2: Revocar entrada de grupo de seguridad | Sí | Sí | No |
| Cree y administre interfaces de red para Cloud Volumes ONTAP en la subred de destino | ec2:CrearInterfazDeRed | Sí | No | No |
| | ec2: Describir interfaces de red | Sí | Sí | No |
| | ec2:EliminarInterfazDeRed | No | Sí | Sí |
| | ec2:ModificarAtributoDeInterfazDeRed | No | Sí | No |
| Obtenga la lista de subredes de destino y grupos de seguridad | ec2:DescribeSubnets | Sí | Sí | No |
| | ec2:DescribeVpcs | Sí | Sí | No |
| Obtenga servidores DNS y el nombre de dominio predeterminado para las instancias de Cloud Volumes ONTAP | ec2:DescribeDhcpOptions | Sí | No | No |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Tomar instantáneas de volúmenes EBS para Cloud Volumes ONTAP | ec2:CrearInstantánea | Sí | Sí | No |
| | ec2:Eliminar instantánea | No | Sí | Sí |
| | ec2:DescribeSnapshots | No | Sí | No |
| Captura la consola Cloud Volumes ONTAP , que está adjunta a los mensajes de AutoSupport | ec2:ObtenerSalidaDeLaConsola | Sí | Sí | No |
| Obtenga la lista de pares de claves disponibles | ec2:DescribeKeyPairs | Sí | No | No |
| Obtenga la lista de regiones de AWS disponibles | ec2:DescribirRegiones | Sí | Sí | No |
| Administrar etiquetas para recursos asociados con instancias de Cloud Volumes ONTAP | ec2:EliminarEtiquetas | No | Sí | Sí |
| | ec2:DescribeTags | No | Sí | No |
| Crear y administrar pilas para plantillas de AWS CloudFormation | formación de nubes:CreateStack | Sí | No | No |
| | formación de nubes:Eliminar pila | Sí | No | No |
| | formación de nubes: DescribeStacks | Sí | Sí | No |
| | formación de nubes: DescribeStackEvents | Sí | No | No |
| | formación de nubes: Validar plantilla | Sí | No | No |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Cree y administre un bucket S3 que un sistema Cloud Volumes ONTAP utiliza como nivel de capacidad para la clasificación de datos | s3:CrearCubo | Sí | Sí | No |
| | s3:Eliminar depósito | No | Sí | Sí |
| | s3:Obtener configuración del ciclo de vida | No | Sí | No |
| | s3:Configuración del ciclo de vida de PutLifecycle | No | Sí | No |
| | s3:Etiquetado de cubo de colocación | No | Sí | No |
| | s3:ListBucketVersions | No | Sí | No |
| | s3: Obtener estado de la política del depósito | No | Sí | No |
| | s3:ObtenerBloqueDeAccesoPúblicoDeBucket | No | Sí | No |
| | s3:ObtenerAcl del depósito | No | Sí | No |
| | s3: Obtener política de depósito | No | Sí | No |
| | s3:PonerCuboBloqueDeAccesoPúblico | No | Sí | No |
| | s3: Obtener etiquetado de cubo | No | Sí | No |
| | s3: Obtener ubicación del depósito | No | Sí | No |
| | s3: Listar todos mis cubos | No | No | No |
| | s3:ListBucket | No | Sí | No |
| Habilite el cifrado de datos de Cloud Volumes ONTAP mediante el Servicio de administración de claves de AWS (KMS) | kms:ReEncrypt* | Sí | No | No |
| | kms:CrearConcesión | Sí | Sí | No |
| | kms:GenerarClaveDeDatosSinTextoSimple | Sí | Sí | No |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Cree y administre un grupo de ubicación distribuida de AWS para dos nodos de alta disponibilidad y el mediador en una única zona de disponibilidad de AWS | ec2:CrearGrupoDeUbicación | Sí | No | No |
| | ec2:EliminarGrupoDeUbicación | No | Sí | Sí |
| Crear informes | fsx:Describir* | No | Sí | No |
| | fsx:Lista* | No | Sí | No |
| Cree y administre agregados que admitan la función de volúmenes elásticos de Amazon EBS | ec2:DescribeVolumesModifications | No | Sí | No |
| | ec2:ModificarVolumen | No | Sí | No |
| Verifique si la zona de disponibilidad es una zona local de AWS y valide que todos los parámetros de implementación sean compatibles | ec2:Describir zonas de disponibilidad | Sí | No | Sí |

#### Registro de cambios

A medida que se agreguen y eliminen permisos, los indicaremos en las secciones siguientes.

### 11 de noviembre de 2025

Los siguientes permisos ya no son necesarios para NetApp Backup and Recovery a menos que utilice la indexación heredada. Estos permisos se han eliminado de las políticas de esta página:

- kms:Lista*
- kms:Describir*
- athena:IniciarEjecuciónDeConsulta
- atenea:ObtenerResultadosDeConsulta
- athena:ObtenerEjecuciónDeConsulta
- athena:DetenerEjecuciónDeConsulta
- pegamento:CrearBaseDeDatos
- pegamento:CrearTabla
- pegamento:LoteEliminarPartición

**9 de septiembre de 2024**

Se eliminaron los permisos de la política n.° 2 para las regiones estándar porque la NetApp Console ya no admite el almacenamiento en caché perimetral de NetApp ni el descubrimiento y la administración de clústeres de Kubernetes.

**Ver los permisos que se eliminaron de la política**

```
{
    "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"
}
```

**9 de mayo de 2024**

Ahora se requiere el siguiente permiso para Cloud Volumes ONTAP:

ec2:Describir zonas de disponibilidad

**6 de junio de 2023**

Ahora se requiere el siguiente permiso para Cloud Volumes ONTAP:

kms:GenerarClaveDeDatosSinTextoSimple

**14 de febrero de 2023**

Ahora se requiere el siguiente permiso para NetApp Cloud Tiering:

ec2:DescribeVpcEndpoints

#### Reglas del grupo de seguridad del agente de consola en AWS

El grupo de seguridad de AWS para el agente requiere reglas entrantes y salientes. La NetApp Console crea automáticamente este grupo de seguridad cuando usted crea un agente de consola desde la consola. Debe configurar este grupo de seguridad para todas las demás opciones de instalación.

##### Reglas de entrada

| Protocolo | Puerto | Objetivo |
|---|---|---|
| SSH | 22 | Proporciona acceso SSH al host del agente |
| HTTP | 80 | • Proporciona acceso HTTP desde los navegadores web del cliente a la interfaz de usuario local<br>• Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP |
| HTTPS | 443 | Proporciona acceso HTTPS a la interfaz de usuario local y conexiones desde la instancia de NetApp Data Classification |
| TCP | 3128 | Proporciona a Cloud Volumes ONTAP acceso a Internet. Debe abrir este puerto manualmente después de la implementación. |

##### Reglas de salida

El grupo de seguridad predefinido para el agente abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de salida. Si necesita reglas más rígidas, utilice las reglas de salida avanzadas.

### Reglas básicas de salida

El grupo de seguridad predefinido para el agente incluye las siguientes reglas de salida.

| Protocolo | Puerto | Objetivo |
|---|---|---|
| Todo TCP | Todo | Todo el tráfico saliente |
| Todos los UDP | Todo | Todo el tráfico saliente |

#### Reglas de salida avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede usar la siguiente información para abrir solo aquellos puertos que el agente requiere para la comunicación saliente.

La dirección IP de origen es el host del agente.

| Servicio | Protocolo | Puerto | Destino | Objetivo |
|---|---|---|---|---|
| Llamadas API y AutoSupport | HTTPS | 443 | LIF de gestión de clústeres ONTAP e Internet saliente | Llamadas API a AWS, a ONTAP, a NetApp Data Classification y envío de mensajes de AutoSupport a NetApp |
| Llamadas API | TCP | 3000 | Mediador de HA de ONTAP | Comunicación con el mediador de ONTAP HA |
| | TCP | 8080 | Clasificación de datos | Sonda a la instancia de clasificación de datos durante la implementación |
| DNS | UDP | 53 | DNS | Utilizado para la resolución de DNS por la consola |

## Permisos de Azure y reglas de seguridad requeridas

#### Permisos de Azure para el agente de consola

Cuando la NetApp Console inicia un agente de consola en Azure, adjunta un rol personalizado a la máquina virtual que proporciona al agente permisos para administrar recursos y procesos dentro de esa suscripción de Azure. El agente usa los permisos para realizar llamadas API a varios servicios de Azure.

Si necesita o no crear este rol personalizado para el agente depende de cómo lo haya implementado.

##### Implementación desde la NetApp Console

Cuando se usa la consola para implementar la máquina virtual del agente en Azure, se habilita una "identidad administrada asignada por el sistema" en la máquina virtual, crea un rol personalizado y lo asigna a la máquina virtual. El rol proporciona a la consola los permisos necesarios para administrar recursos y procesos dentro de esa suscripción de Azure. Los permisos del rol se mantienen actualizados cuando se actualiza el agente. No es necesario crear este rol para el agente ni administrar actualizaciones.

##### Implementación manual o desde Azure Marketplace

Cuando implementa el agente desde Azure Marketplace o si instala manualmente el agente en un host Linux, deberá configurar usted mismo el rol personalizado y mantener sus permisos con cualquier cambio.

Deberá asegurarse de que el rol esté actualizado a medida que se agreguen nuevos permisos en versiones posteriores. Si se requieren nuevos permisos, se enumerarán en las notas de la versión.

- Para ver instrucciones paso a paso sobre cómo utilizar estas políticas, consulte las siguientes páginas:
  - "Configurar permisos para una implementación de Azure Marketplace"
  - "Configurar permisos para implementaciones locales"
  - "Configurar permisos para el modo restringido"

```
{
  "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"
}
```

#### Cómo se utilizan los permisos de Azure

Las siguientes secciones describen cómo se utilizan los permisos para cada sistema de almacenamiento y servicio de datos de NetApp . Esta información puede ser útil si sus políticas corporativas establecen que los permisos solo se otorgan cuando es necesario.

### Azure NetApp Files

El agente realiza las siguientes solicitudes de API cuando se usa NetApp Data Classification para escanear datos de Azure NetApp Files :

- 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

### NetApp Backup and Recovery

Las siguientes secciones describen cómo se utilizan los permisos para NetApp Backup and Recovery.

### Permisos mínimos de NetApp Backup and Recovery

El agente de consola realiza las siguientes solicitudes a la API para la funcionalidad básica de NetApp Backup and Recovery :

- Microsoft.Storage/storageAccounts/listkeys/acción
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/cuentasDeAlmacenamiento/escritura
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/acción
- Microsoft.Recursos/suscripciones/ubicaciones/lectura
- Microsoft.Recursos/suscripciones/gruposderecursos/lectura
- Microsoft.Recursos/suscripciones/grupos de recursos/recursos/lectura

- Microsoft.Recursos/suscripciones/gruposderecursos/escritura
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Autorización/bloqueos/escritura
- Microsoft.Authorization/locks/read

La siguiente es una política personalizada para Copia de seguridad y recuperación que utiliza el menor número posible de permisos y el alcance más reducido posible:

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

### Permisos avanzados de copia de seguridad y recuperación

El agente de consola realiza las siguientes solicitudes de API para operaciones avanzadas de copia de seguridad y recuperación, así como para funciones de búsqueda y restauración. Estos permisos permiten la gestión de redes, almacenes de claves e identidades gestionadas:

- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.KeyVault/vaults/lectura
- Microsoft.ManagedIdentity/userAssignedIdentities/asignar/acción
- Microsoft.Network/networkInterfaces/eliminar
- Microsoft.Network/networkInterfaces/read
- Microsoft.Network/networkSecurityGroups/eliminar
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/virtualNetworks/join/acción
- Microsoft.Recursos/implementaciones/eliminar

### Permisos heredados para Copia de seguridad y recuperación

El agente realiza las siguientes solicitudes a la API cuando usted utiliza la funcionalidad de Búsqueda y Restauración. Solo necesita estos permisos si habilitó las funciones de indexación heredadas antes del lanzamiento de la indexación v2 en febrero de 2025:

- Microsoft.Synapse/espacios de trabajo/escritura
- Microsoft.Synapse/espacios de trabajo/lectura
- Microsoft.Synapse/espacios de trabajo/eliminar
- Microsoft.Synapse/registrar/acción
- Microsoft.Synapse/checkNameAvailability/acción
- Microsoft.Synapse/workspaces/operationStatuses/read
- Microsoft.Synapse/workspaces/firewallRules/read
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/acción
- Microsoft.Synapse/espacios de trabajo/resultadosdeoperación/lectura
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/acción

### NetApp Data Classification

El agente realiza las siguientes solicitudes de API cuando utiliza la clasificación de datos.

| Acción | ¿Se utiliza para la configuración? | ¿Se utiliza para operaciones diarias? |
|---|---|---|
| Microsoft.Compute/ubicaciones/operaciones/lectura | Sí | Sí |

| Acción | ¿Se utiliza para la configuración? | ¿Se utiliza para operaciones diarias? |
|---|---|---|
| Microsoft.Compute/ubicaciones/vmSizes/lectura | Sí | Sí |
| Microsoft.Compute/operaciones/lectura | Sí | Sí |
| Microsoft.Compute/virtualMachines/instanceView/read | Sí | Sí |
| Microsoft.Compute/virtualMachines/powerOff/acción | Sí | No |
| Microsoft.Compute/virtualMachines/read | Sí | Sí |
| Microsoft.Compute/virtualMachines/reiniciar/acción | Sí | No |
| Microsoft.Compute/virtualMachines/start/action | Sí | No |
| Microsoft.Compute/virtualMachines/vmSizes/read | No | Sí |
| Microsoft.Compute/virtualMachines/write | Sí | No |
| Microsoft.Compute/imágenes/lectura | Sí | Sí |
| Microsoft.Compute/discos/eliminar | Sí | No |
| Microsoft.Compute/discos/lectura | Sí | Sí |
| Microsoft.Compute/discos/escritura | Sí | No |
| Microsoft.Storage/checknameavailability/read | Sí | Sí |
| Microsoft.Storage/operaciones/lectura | Sí | Sí |
| Microsoft.Storage/storageAccounts/listkeys/acción | Sí | No |
| Microsoft.Storage/storageAccounts/read | Sí | Sí |
| Microsoft.Storage/cuentasDeAlmacenamiento/escritura | Sí | No |
| Microsoft.Storage/storageAccounts/blobServices/containers/read | Sí | Sí |
| Microsoft.Network/networkInterfaces/read | Sí | Sí |
| Microsoft.Network/interfacesdered/escritura | Sí | No |

| Acción | ¿Se utiliza para la configuración? | ¿Se utiliza para operaciones diarias? |
|---|---|---|
| Microsoft.Network/networkInterfaces/join/acción | Sí | No |
| Microsoft.Network/networkSecurityGroups/read | Sí | Sí |
| Microsoft.Network/networkSecurityGroups/write | Sí | No |
| Microsoft.Recursos/suscripciones/ubicaciones/lectura | Sí | Sí |
| Microsoft.Network/ubicaciones/resultadosdeoperación/lectura | Sí | Sí |
| Microsoft.Network/ubicaciones/operaciones/lectura | Sí | Sí |
| Microsoft.Network/virtualNetworks/read | Sí | Sí |
| Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read | Sí | Sí |
| Microsoft.Network/virtualNetworks/subnets/read | Sí | Sí |
| Microsoft.Network/virtualNetworks/subnets/virtualMachines/read | Sí | Sí |
| Microsoft.Network/virtualNetworks/virtualMachines/read | Sí | Sí |
| Microsoft.Network/virtualNetworks/subnets/join/action | Sí | No |
| Microsoft.Network/virtualNetworks/subnets/write | Sí | No |
| Microsoft.Network/routeTables/join/acción | Sí | No |
| Microsoft.Recursos/implementaciones/operaciones/lectura | Sí | Sí |
| Microsoft.Recursos/implementaciones/lectura | Sí | Sí |
| Microsoft.Recursos/implementaciones/escritura | Sí | No |
| Microsoft.Recursos/recursos/leer | Sí | Sí |
| Microsoft.Recursos/suscripciones/resultadosdeoperación/lectura | Sí | Sí |
| Microsoft.Recursos/suscripciones/gruposderecursos/eliminar | Sí | No |

| Acción | ¿Se utiliza para la configuración? | ¿Se utiliza para operaciones diarias? |
| --- | --- | --- |
| Microsoft.Recursos/suscripciones/gruposderecursos/lectura | Sí | Sí |
| Microsoft.Recursos/suscripciones/grupos de recursos/recursos/lectura | Sí | Sí |
| Microsoft.Recursos/suscripciones/gruposderecursos/escritura | Sí | No |

**Cloud Volumes ONTAP**

El agente realiza las siguientes solicitudes de API para implementar y administrar Cloud Volumes ONTAP en Azure.

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Crear y administrar máquinas virtuales | Microsoft.Compute/ubicaciones/operaciones/lectura | Sí | Sí | No |
| | Microsoft.Compute/ubicaciones/vmSizes/lectura | Sí | Sí | No |
| | Microsoft.Recursos/suscripciones/ubicaciones/lectura | Sí | No | No |
| | Microsoft.Compute/operaciones/lectura | Sí | Sí | No |
| | Microsoft.Compute/virtualMachines/instanceView/read | Sí | Sí | No |
| | Microsoft.Compute/virtualMachines/powerOff/acción | Sí | Sí | No |
| | Microsoft.Compute/virtualMachines/read | Sí | Sí | No |
| | Microsoft.Compute/virtualMachines/reiniciar/acción | Sí | Sí | No |
| | Microsoft.Compute/virtualMachines/start/action | Sí | Sí | No |
| | Microsoft.Compute/virtualMachines/desasignar/acción | No | Sí | Sí |
| | Microsoft.Compute/virtualMachines/vmSizes/read | No | Sí | No |
| | Microsoft.Compute/virtualMachines/write | Sí | Sí | No |
| | Microsoft.Compute/virtualMachines/eliminar | Sí | Sí | Sí |
| | Microsoft.Recursos/implementaciones/eliminar | Sí | No | No |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Habilitar la implementación desde un VHD | Microsoft.Compute/imágenes/lectura | Sí | No | No |
| | Microsoft.Compute/imágenes/escritura | Sí | No | No |
| Crear y administrar interfaces de red en la subred de destino | Microsoft.Network/networkInterfaces/read | Sí | Sí | No |
| | Microsoft.Network/interfacesdered/escritura | Sí | Sí | No |
| | Microsoft.Network/networkInterfaces/join/acción | Sí | Sí | No |
| | Microsoft.Network/networkInterfaces/eliminar | Sí | Sí | No |
| Crear y administrar grupos de seguridad de red | Microsoft.Network/networkSecurityGroups/read | Sí | Sí | No |
| | Microsoft.Network/networkSecurityGroups/write | Sí | Sí | No |
| | Microsoft.Network/networkSecurityGroups/join/acción | Sí | No | No |
| | Microsoft.Network/networkSecurityGroups/eliminar | No | Sí | Sí |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Obtenga información de red sobre las regiones, la red virtual y la subred de destino, y agregue las máquinas virtuales a las redes virtuales | Microsoft.Network/ubicaciones/resultadosdeoperación/lectura | Sí | Sí | No |
| | Microsoft.Network/ubicaciones/operaciones/lectura | Sí | Sí | No |
| | Microsoft.Network/virtualNetworks/read | Sí | No | No |
| | Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read | Sí | No | No |
| | Microsoft.Network/virtualNetworks/subnets/read | Sí | Sí | No |
| | Microsoft.Network/virtualNetworks/subnets/virtualMachines/read | Sí | Sí | No |
| | Microsoft.Network/virtualNetworks/virtualMachines/read | Sí | Sí | No |
| | Microsoft.Network/virtualNetworks/subnets/join/action | Sí | Sí | No |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Crear y administrar grupos de recursos | Microsoft.Recursos/implementaciones/operaciones/lectura | Sí | Sí | No |
| | Microsoft.Recursos/implementaciones/lectura | Sí | Sí | No |
| | Microsoft.Recursos/implementaciones/escritura | Sí | Sí | No |
| | Microsoft.Recursos/recursos/leer | Sí | Sí | No |
| | Microsoft.Recursos/suscripciones/resultadosdeoperación/lectura | Sí | Sí | No |
| | Microsoft.Recursos/suscripciones/gruposderecursos/eliminar | Sí | Sí | Sí |
| | Microsoft.Recursos/suscripciones/gruposderecursos/lectura | No | Sí | No |
| | Microsoft.Recursos/suscripciones/gruposde recursos/recursos/lectura | Sí | Sí | No |
| | Microsoft.Recursos/suscripciones/gruposderecursos/escritura | Sí | Sí | No |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Administrar cuentas y discos de almacenamiento de Azure | Microsoft.Compute/discos/lectura | Sí | Sí | Sí |
| | Microsoft.Compute/discos/escritura | Sí | Sí | No |
| | Microsoft.Compute/discos/eliminar | Sí | Sí | Sí |
| | Microsoft.Storage/checknameavailability/read | Sí | Sí | No |
| | Microsoft.Storage/operaciones/lectura | Sí | Sí | No |
| | Microsoft.Storage/storageAccounts/listkeys/acción | Sí | Sí | No |
| | Microsoft.Storage/storageAccounts/read | Sí | Sí | No |
| | Microsoft.Storage/cuentasDeAlmacenamiento/eliminar | No | Sí | Sí |
| | Microsoft.Storage/cuentasDeAlmacenamiento/escritura | Sí | Sí | No |
| | Microsoft.Storage/usos/lectura | No | Sí | No |
| Habilitar copias de seguridad en el almacenamiento de blobs y el cifrado de cuentas de almacenamiento | Microsoft.Storage/storageAccounts/blobServices/containers/read | Sí | Sí | No |
| | Microsoft.KeyVault/vaults/lectura | Sí | Sí | No |
| | Microsoft.KeyVault/vaults/accessPolicies/write | Sí | Sí | No |
| Habilitar puntos finales de servicio de VNet para la organización en niveles de datos | Microsoft.Network/virtualNetworks/subnets/write | Sí | Sí | No |
| | Microsoft.Network/routeTables/join/acción | Sí | Sí | No |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Crear y administrar instantáneas administradas de Azure | Microsoft.Compute/instantáneas/escritura | Sí | Sí | No |
| | Microsoft.Compute/instantáneas/lectura | Sí | Sí | No |
| | Microsoft.Compute/instantáneas/eliminar | No | Sí | Sí |
| | Microsoft.Compute/disks/beginGetAccess/acción | No | Sí | No |
| Crear y administrar conjuntos de disponibilidad | Microsoft.Compute/conjuntosdedisponibilidad/escritura | Sí | No | No |
| | Microsoft.Compute/conjuntosdedisponibilidad/lectura | Sí | No | No |
| Habilitar implementaciones programáticas desde el mercado | Microsoft.MarketplaceOrdering/offertypes/publishers/offers/planes/agreements/read | Sí | No | No |
| | Microsoft.MarketplaceOrdering/offertypes/publishers/offers/planes/agreements/write | Sí | Sí | No |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Administrar un balanceador de carga para pares de alta disponibilidad | Microsoft.Network/balanceadoresdecarga/lectura | Sí | Sí | No |
| | Microsoft.Network/balanceadoresdecarga/escritura | Sí | No | No |
| | Microsoft.Network/balanceadoresdecarga/eliminar | No | Sí | Sí |
| | Microsoft.Network/loadBalancers/backendAddressPools/read | Sí | No | No |
| | Microsoft.Network/loadBalancers/backendAddressPools/join/action | Sí | No | No |
| | Microsoft.Network/loadBalancers/frontendIPConfigurations/read | Sí | Sí | No |
| | Microsoft.Network/loadBalancers/loadBalancingRules/read | Sí | No | No |
| | Microsoft.Network/loadBalancers/probes/read | Sí | No | No |
| | Microsoft.Network/loadBalancers/probes/join/action | Sí | No | No |
| Habilitar la administración de bloqueos en discos de Azure | Microsoft.Autorización/bloqueos/* | Sí | Sí | No |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Habilite puntos finales privados para pares de alta disponibilidad cuando no haya conectividad fuera de la subred | Microsoft.Network/privateEndpoints/write | Sí | Sí | No |
| | Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acción | Sí | No | No |
| | Microsoft.Storage/storageAccounts/privateEndpointConnections/read | Sí | Sí | Sí |
| | Microsoft.Network/privateEndpoints/read | Sí | Sí | Sí |
| | Microsoft.Network/privateDnsZones/write | Sí | Sí | No |
| | Microsoft.Network/privateDnsZones/virtualNetworkLinks/write | Sí | Sí | No |
| | Microsoft.Network/virtualNetworks/join/acción | Sí | Sí | No |
| | Microsoft.Network/privateDnsZones/A/write | Sí | Sí | No |
| | Microsoft.Network/privateDnsZones/read | Sí | Sí | No |
| | Microsoft.Network/privateDnsZones/virtualNetworkLinks/read | Sí | Sí | No |
| Necesario para algunas implementaciones de máquinas virtuales, según el hardware físico subyacente | Microsoft.Recursos/implementaciones/estadosdeoperación/lectura | Sí | Sí | No |
| Eliminar recursos de un grupo de recursos en caso de falla o eliminación de la implementación | Microsoft.Network/privateEndpoints/eliminar | Sí | Sí | No |
| | Microsoft.Compute/disponibilidadConjuntos/eliminar | Sí | Sí | No |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Habilitar el uso de claves de cifrado administradas por el cliente al utilizar la API | Microsoft.Compute/diskEncryptionSets/lectura | Sí | Sí | Sí |
| | Microsoft.Compute/diskEncryptionSets/write | Sí | Sí | No |
| | Microsoft.KeyVault/vaults/deploy/action | Sí | No | No |
| | Microsoft.Compute/diskEncryptionSets/eliminar | Sí | Sí | Sí |
| Configurar un grupo de seguridad de aplicaciones para un par de alta disponibilidad (HA) para aislar la interconexión de HA y las NIC de red del clúster | Microsoft.Network/applicationSecurityGroups/write | No | Sí | No |
| | Microsoft.Network/applicationSecurityGroups/read | No | Sí | No |
| | Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/acción | No | Sí | No |
| | Microsoft.Network/networkSecurityGroups/securityRules/write | Sí | Sí | No |
| | Microsoft.Network/applicationSecurityGroups/eliminar | No | Sí | Sí |
| | Microsoft.Network/networkSecurityGroups/securityRules/eliminar | No | Sí | Sí |
| Leer, escribir y eliminar etiquetas asociadas con los recursos de Cloud Volumes ONTAP | Microsoft.Recursos/etiquetas/leer | No | Sí | No |
| | Microsoft.Recursos/etiquetas/escritura | Sí | Sí | No |
| | Microsoft.Resources/etiquetas/eliminar | Sí | No | No |
| Cifrar cuentas de almacenamiento durante la creación | Microsoft.ManagedIdentity/userAssignedIdentities/asignar/acción | Sí | Sí | No |

| Objetivo | Acción | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| Utilice conjuntos de escala de máquinas virtuales en el modo de orquestación flexible para especificar zonas específicas para Cloud Volumes ONTAP | Microsoft.Compute/virtualMachineScaleSets/write | Sí | No | No |
| | Microsoft.Compute/virtualMachineScaleSets/lectura | Sí | No | No |
| | Microsoft.Compute/virtualMachineScaleSets/eliminar | No | No | Sí |

**Nivelación**

El agente realiza las siguientes solicitudes de API cuando configura NetApp Cloud Tiering.

- Microsoft.Storage/storageAccounts/listkeys/acción
- Microsoft.Recursos/suscripciones/gruposderecursos/lectura
- Microsoft.Recursos/suscripciones/ubicaciones/lectura

El agente de consola realiza las siguientes solicitudes de API para las operaciones diarias.

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

#### Registro de cambios

A medida que se agreguen y eliminen permisos, los indicaremos en las secciones siguientes.

**11 de noviembre de 2025**

Se agregó una política JSON personalizada que refleja la menor cantidad de permisos posibles y el alcance más estrecho posible.

Se agregaron los siguientes permisos a la lista mínima de permisos de copia de seguridad y recuperación:

- Microsoft.Autorización/bloqueos/escritura
- Microsoft.Authorization/locks/read

Los siguientes permisos ya no son necesarios para Copia de seguridad y recuperación a menos que utilice la indexación heredada:

- Microsoft.Synapse/espacios de trabajo/escritura
- Microsoft.Synapse/espacios de trabajo/lectura
- Microsoft.Synapse/espacios de trabajo/eliminar

- Microsoft.Synapse/registrar/acción
- Microsoft.Synapse/checkNameAvailability/acción
- Microsoft.Synapse/workspaces/operationStatuses/read
- Microsoft.Synapse/workspaces/firewallRules/read
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/acción
- Microsoft.Synapse/espacios de trabajo/resultadosdeoperación/lectura
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/acción

Los siguientes permisos se han movido a la sección "Permisos adicionales de copia de seguridad y recuperación" porque no son necesarios para una configuración mínima:

- Microsoft.Storage/storageAccounts/listkeys/acción
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/cuentasDeAlmacenamiento/escritura
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/acción
- Microsoft.Recursos/suscripciones/ubicaciones/lectura
- Microsoft.Recursos/suscripciones/gruposderecursos/lectura
- Microsoft.Recursos/suscripciones/grupos de recursos/recursos/lectura
- Microsoft.Recursos/suscripciones/gruposderecursos/escritura
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write

**9 de septiembre de 2024**

Los siguientes permisos se eliminaron de la política JSON porque la consola ya no admite el descubrimiento y la administración de clústeres de Kubernetes:

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/acción
- Microsoft.ContainerService/managedClusters/lectura

**22 de agosto de 2024**

Se agregaron los siguientes permisos a la política JSON porque son necesarios para la compatibilidad de Cloud Volumes ONTAP con conjuntos de escalado de máquinas virtuales:

- Microsoft.Compute/virtualMachineScaleSets/write
- Microsoft.Compute/virtualMachineScaleSets/lectura
- Microsoft.Compute/virtualMachineScaleSets/eliminar

**5 de diciembre de 2023**

Los siguientes permisos ya no son necesarios para NetApp Backup and Recovery al realizar copias de seguridad de datos de volumen en Azure Blob Storage:

- Microsoft.Compute/virtualMachines/read

- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/desasignar/acción
- Microsoft.Compute/virtualMachines/extensiones/eliminar
- Microsoft.Compute/virtualMachines/eliminar

Estos permisos son necesarios para otros servicios de almacenamiento de la consola, por lo que permanecerán en la función personalizada para el agente si está utilizando esos otros servicios de almacenamiento.

**12 de mayo de 2023**

Se agregaron los siguientes permisos a la política JSON porque son necesarios para la administración de Cloud Volumes ONTAP :

- Microsoft.Compute/imágenes/escritura
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read

Los siguientes permisos se eliminaron de la política JSON porque ya no son necesarios:

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

**23 de marzo de 2023**

El permiso "Microsoft.Storage/storageAccounts/delete" ya no es necesario para la clasificación de datos.

Este permiso aún es necesario para Cloud Volumes ONTAP.

**5 de enero de 2023**

Se agregaron los siguientes permisos a la política JSON:

- Microsoft.Storage/storageAccounts/listAccountSas/acción
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/acción

  Estos permisos son necesarios para NetApp Backup and Recovery.

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

  Este permiso es necesario para la implementación de Cloud Volumes ONTAP .

**Reglas del grupo de seguridad del agente de consola en Azure**

El grupo de seguridad de Azure para el agente requiere reglas de entrada y de salida. La NetApp Console crea automáticamente este grupo de seguridad cuando crea un agente de consola desde la consola. Para otras opciones de instalación, debe configurar este grupo de seguridad manualmente.

#### Reglas de entrada

| Protocolo | Puerto | Objetivo |
|---|---|---|
| SSH | 22 | Proporciona acceso SSH al host del agente |
| HTTP | 80 | • Proporciona acceso HTTP desde los navegadores web del cliente a la interfaz de usuario local<br>• Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP |
| HTTPS | 443 | Proporciona acceso HTTPS desde los navegadores web del cliente a la interfaz de usuario local y conexiones desde la instancia de NetApp Data Classification |
| TCP | 3128 | Proporciona a Cloud Volumes ONTAP acceso a Internet para enviar mensajes de AutoSupport al soporte de NetApp . Debe abrir este puerto manualmente después de la implementación. "Descubra cómo se utiliza el agente como proxy para los mensajes de AutoSupport" |

#### Reglas de salida

El grupo de seguridad predefinido para el agente abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de salida. Si necesita reglas más rígidas, utilice las reglas de salida avanzadas.

### Reglas básicas de salida

El grupo de seguridad predefinido para el agente incluye las siguientes reglas de salida.

| Protocolo | Puerto | Objetivo |
|---|---|---|
| Todo TCP | Todo | Todo el tráfico saliente |
| Todos los UDP | Todo | Todo el tráfico saliente |

### Reglas de salida avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir solo aquellos puertos que el agente requiere para la comunicación saliente.

La dirección IP de origen es el host del agente.

| Servicio | Protocolo | Puerto | Destino | Objetivo |
|---|---|---|---|---|
| Llamadas API y AutoSupport | HTTPS | 443 | LIF de gestión de clústeres ONTAP e Internet saliente | Llamadas API a Azure, a ONTAP, a NetApp Data Classification y envío de mensajes de AutoSupport a NetApp |
| Llamadas API | TCP | 8080 | Clasificación de datos | Sonda a la instancia de clasificación de datos durante la implementación |
| DNS | UDP | 53 | DNS | Utilizado para la resolución de DNS por la consola |

## Permisos de Google Cloud y reglas de firewall requeridas

### Permisos de Google Cloud para el agente de la consola

El agente de la consola requiere permisos para realizar acciones en Google Cloud. Estos permisos están incluidos en una función personalizada proporcionada por NetApp. Debes comprender qué hace el agente con estos permisos.

#### Permisos de la cuenta de usuario de Google Cloud

La siguiente función personalizada otorga a un usuario de Google Cloud los permisos necesarios para implementar un agente. Aplique este rol personalizado al usuario que implementará el agente.

**Ver los permisos de la cuenta de usuario de Google Cloud**

```
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
```

**Permisos de la cuenta de servicio**

La función personalizada a continuación le otorga a la cuenta de servicio de Google Cloud asociada al agente de la consola los permisos necesarios para administrar recursos y procesos en su red de Google Cloud.

Aplique esta función personalizada a una cuenta de servicio asociada a la máquina virtual del agente de

consola.

- "Configurar los permisos de Google Cloud para el modo estándar"
- "Configurar permisos para el modo restringido"

**Ver los permisos de la cuenta de servicio de Google**

Asegúrese de que la función esté actualizada a medida que se agreguen o eliminen nuevos permisos en versiones posteriores. El registro de cambios enumera todos los nuevos permisos necesarios."Revisar el registro de cambios de permisos de Google" "Revisa cómo agregar cuentas de servicio de Google Cloud"

```
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
```

#### Cómo se utilizan los permisos de Google Cloud

El agente de la consola usa los permisos en la función personalizada para administrar los recursos de Cloud Volumes ONTAP y los procesos de servicios de datos de NetApp en su red de Google Cloud. Las siguientes secciones describen cómo el agente utiliza estos permisos.

### Permisos utilizados para Cloud Volumes ONTAP

El agente de la consola usa los permisos en la función personalizada para administrar los recursos y procesos de Cloud Volumes ONTAP en su red de Google Cloud. Las siguientes secciones describen cómo el agente utiliza estos permisos.

**Permisos para Cloud Volumes ONTAP**

| Comportamiento | Objetivo | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| config.deployments.create | Para implementar la instancia de máquina virtual Cloud Volumes ONTAP mediante Google Cloud Infrastructure Manager. | Sí | No | No |
| config.deployments.delete | | No | No | Sí |
| config.deployments.deleteState | | No | No | Sí |
| config.deployments.get | | No | Sí | No |
| config.deployments.getLock | | No | Sí | No |
| config.deployments.getState | | No | Sí | No |
| lista de configuraciones de despliegue | | No | Sí | No |
| config.deployments.lock | | No | Sí | No |
| config.deployments.update | | No | Sí | No |
| config.deployments.updateState | | No | Sí | No |
| config.operaciones.get | | No | Sí | No |
| config.previews.get | | No | Sí | No |
| lista de vistas previas de configuración | | No | Sí | No |
| lista de recursos de configuración | | No | Sí | No |
| config.revisions.get | | No | Sí | No |

| Comportamiento | Objetivo | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| crear.discos.computar | Para crear y administrar discos para Cloud Volumes ONTAP. | Sí | Sí | No |
| compute.disks.createSnapshot | | No | Sí | No |
| eliminar discos de cálculo | | No | Sí | Sí |
| compute.disks.get | | No | Sí | No |
| compute.disks.list | | Sí | Sí | No |
| computar.discos.establecerEtiquetas | | Sí | Sí | No |
| usar discos de cálculo | | No | Sí | No |
| crear.cortafuegos. | Para crear reglas de firewall para Cloud Volumes ONTAP. | Sí | No | No |
| compute.firewalls.delete | | No | Sí | Sí |
| compute.firewalls.get | | Sí | Sí | No |
| compute.firewalls.list | | Sí | Sí | No |
| calcular.reenvíoReglas.crear | Cree reglas de reenvío para enrutar el tráfico hacia los servicios backend. | No | Sí | No |
| calcular.reenvíoReglas.eliminar | Eliminar reglas de reenvío existentes. | No | Sí | No |
| calcular.reenvíoReglas.obtener | Recupere detalles sobre las reglas de reenvío existentes. | No | Sí | No |
| calcular.reenvíoReglas.establecerEtiquetas | Establecer o actualizar etiquetas en las reglas de reenvío para la organización. | No | Sí | No |
| computar.globalOperations.get | Para obtener el estado de las operaciones. | Sí | Sí | No |

| Comportamiento | Objetivo | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| computar.healthChecks.crear | Cree y administre controles de estado para supervisar el estado del servicio backend. | No | Sí | No |
| computar.healthChecks.eliminar | | No | Sí | No |
| computar.healthChecks.get | | No | Sí | No |
| computar.healthChecks.useReadOnly | | No | Sí | No |
| compute.images.get | Para obtener imágenes para instancias de VM. | Sí | No | No |
| compute.images.getFromFamily | | Sí | No | No |
| compute.images.list | | Sí | No | No |
| compute.images.useReadOnly | | Sí | No | No |
| compute.instances.attachDisk | Para conectar y desconectar discos a Cloud Volumes ONTAP. | Sí | Sí | No |
| compute.instances.detachDisk | | No | Sí | Sí |
| crear instancias de cómputo | Para crear y eliminar instancias de VM de Cloud Volumes ONTAP . | Sí | No | No |
| compute.instances.delete | | No | No | Sí |
| compute.instances.get | Para enumerar instancias de VM. | Sí | Sí | No |
| compute.instances.getSerialPortOutput | Para obtener registros de la consola. | Sí | Sí | No |
| compute.instances.list | Para recuperar la lista de instancias en una zona. | Sí | Sí | No |
| compute.instances.setDeletionProtection | Para establecer la protección contra eliminación en la instancia. | Sí | No | No |
| compute.instances.setLabels | Para agregar etiquetas. | Sí | No | No |

| Comportamiento | Objetivo | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| compute.instances.setMachineType | Para cambiar el tipo de máquina para Cloud Volumes ONTAP. | Sí | Sí | No |
| compute.instances.setMinCpuPlatform | | Sí | Sí | No |
| compute.instances.setMetadata | Para agregar metadatos. | Sí | Sí | No |
| compute.instances.setTags | Para agregar etiquetas para las reglas de firewall. | Sí | Sí | No |
| compute.instances.start | Para iniciar y detener Cloud Volumes ONTAP. | Sí | Sí | No |
| compute.instances.stop | | Sí | Sí | No |
| compute.instances.updateDisplayDevice | | Sí | Sí | No |
| computar.instancias.uso | Utilice instancias de máquinas virtuales (operaciones de inicio, detención y conexión). | No | Sí | No |
| compute.machineTypes.get | Para obtener el número de núcleos y comprobar las cuotas. | Sí | No | No |
| compute.projects.get | Para apoyar multiproyectos. | Sí | No | No |
| computar.políticasderecursos.crear | Cree y administre políticas de recursos para la gestión automatizada de recursos. | No | Sí | No |
| computar.políticasderecursos.eliminar | | No | Sí | No |
| computar.políticasderecursos.obtener | | No | Sí | No |

| Comportamiento | Objetivo | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| crear.instantáneas.computar | Para crear y administrar instantáneas de disco persistentes. | Sí | Sí | No |
| compute.snapshots.delete | | No | Sí | Sí |
| compute.snapshots.get | | No | Sí | No |
| compute.snapshots.list | | No | Sí | No |
| calcular.instantáneas.establecerEtiquetas | | Sí | Sí | No |
| compute.networks.get | Para obtener la información de red necesaria para crear una nueva instancia de máquina virtual Cloud Volumes ONTAP . | Sí | Sí | No |
| compute.networks.list | | Sí | Sí | No |
| compute.regions.get | | Sí | Sí | No |
| compute.regions.list | | Sí | Sí | No |
| compute.subnetworks.get | | Sí | Sí | No |
| compute.subnetworks.list | | Sí | Sí | No |
| compute.zoneOperations.get | | Sí | Sí | No |
| compute.zones.get | | Sí | Sí | No |
| compute.zones.list | | Sí | Sí | No |

| Comportamiento | Objetivo | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| deploymentmanager.compositeTypes.get | Para implementar la instancia de máquina virtual Cloud Volumes ONTAP mediante Google Cloud Deployment Manager. | Sí | No | No |
| deploymentmanager.compositeTypes.list | | Sí | No | No |
| gestor de despliegue.despliegues.crear | | Sí | No | No |
| gestor de despliegue.despliegues.eliminar | | Sí | No | No |
| deploymentmanager.deployments.get | | Sí | No | No |
| deploymentmanager.deployments.list | | Sí | No | No |
| deploymentmanager.manifests.get | | Sí | No | No |
| deploymentmanager.manifests.list | | Sí | No | No |
| deploymentmanager.operations.get | | Sí | No | No |
| lista de operaciones del administrador de despliegue | | Sí | No | No |
| deploymentmanager.resources.get | | Sí | No | No |
| deploymentmanager.resources.list | | Sí | No | No |
| deploymentmanager.typeProviders.get | | Sí | No | No |
| deploymentmanager.typeProviders.list | | Sí | No | No |
| deploymentmanager.types.get | | Sí | No | No |
| lista de tipos de gestor de despliegue | | Sí | No | No |

| Comportamiento | Objetivo | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| logging.logEntries.list | Para obtener unidades de registro de pila. | Sí | Sí | No |
| logging.privateLogEntries.list | | Sí | Sí | No |
| registro.logEntries.create | Cree y enrute archivos de registro para monitoreo, depuración y auditoría. | Sí | Sí | No |
| registro.logEntries.route | | Sí | Sí | No |
| resourcemanager.projects.get | Para apoyar multiproyectos. | Sí | Sí | No |
| almacenamiento.cubos.crear | Para crear y administrar un depósito de Google Cloud Storage para la organización en niveles de datos. | Sí | Sí | No |
| almacenamiento.cubos.eliminar | | No | Sí | Sí |
| almacenamiento.cubos.obtener | | No | Sí | No |
| lista de cubos de almacenamiento | | No | Sí | No |
| almacenamiento.cubos.actualizar | | No | Sí | No |
| cloudkms.cryptoKeyVersions.useToEncrypt | Para utilizar claves de cifrado administradas por el cliente desde el Servicio de administración de claves en la nube con Cloud Volumes ONTAP. | Sí | Sí | No |
| cloudkms.cryptoKeys.get | | Sí | Sí | No |
| cloudkms.cryptoKeys.lista | | Sí | Sí | No |
| lista de llaveros cloudkms | | Sí | Sí | No |
| cloudbuild.builds.get | | Sí | No | No |

| Comportamiento | Objetivo | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| compute.instances.setServiceAccount | Para configurar una cuenta de servicio en la instancia de Cloud Volumes ONTAP . Esta cuenta de servicio proporciona permisos para la organización de datos en niveles en un depósito de Google Cloud Storage. | Sí | Sí | No |
| soy.cuentasdeservicio.actuar como | | Sí | No | No |
| iam.serviceAccounts.create | | Sí | No | No |
| iam.serviceAccounts.getIamPolicy | | Sí | Sí | No |
| soy.serviceAccounts.list | | Sí | Sí | No |
| iam.serviceAccountKeys.create | | Sí | No | No |
| almacenamiento.objetos.crear | Cree y administre objetos (archivos) en el depósito de Google Cloud Storage. | Sí | Sí | No |
| almacenamiento.objetos.eliminar | | No | No | Sí |
| almacenamiento.objetos.obtener | | Sí | Sí | No |
| almacenamiento.objetos.lista | | Sí | Sí | No |
| calcular.direcciones.lista | Para recuperar las direcciones en una región al implementar un par HA. | Sí | No | No |
| computar.direcciones.crearInterno | Cree direcciones IP internas dentro de la red VPC para la asignación de recursos. | No | Sí | No |
| computar.direcciones.eliminarInterno | Eliminar direcciones IP internas para limpiar recursos. | No | Sí | No |
| calcular.direcciones.establecerEtiquetas | Actualizar etiquetas en el recurso Dirección. | No | Sí | No |
| computar.direcciones.useInternal | Utilice direcciones IP internas para la comunicación de red. | No | Sí | No |

| Comportamiento | Objetivo | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| compute.backendServices.create | Configurar un servicio de backend para distribuir el tráfico en un par HA. | Sí | No | No |
| compute.regionBackendServices.create | Crear y administrar servicios backend para enrutamiento de tráfico. | Sí | No | No |
| computar.regionBackendServices.eliminar | | No | Sí | No |
| compute.regionBackendServices.get | | Sí | No | No |
| computar.regionBackendServices.update | | Sí | Sí | No |
| compute.regionBackendServices.list | | Sí | No | No |
| computar.regiónBackendServices.uso | | No | Sí | No |
| política de actualización de redes de computación | Para aplicar reglas de firewall en las VPC y subredes de un par de alta disponibilidad. | Sí | No | No |
| compute.instanceGroups.get | Para crear y administrar máquinas virtuales de almacenamiento en pares HA de Cloud Volumes ONTAP . | Sí | Sí | No |
| calcular.direcciones.obtener | | Sí | Sí | No |
| computar.instancias.actualizarInterfazDeRed | | Sí | Sí | No |
| computar.gruposdeinstancias.crear | | No | Sí | No |
| calcular.gruposdeinstancias.eliminar | | No | Sí | No |
| computar.gruposdeinstancias.actualizar | | No | Sí | No |
| computar.gruposdeinstancias.uso | | No | Sí | No |

| Comportamiento | Objetivo | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| monitorización.lista de series temporales | Para descubrir información sobre los depósitos de Google Cloud Storage. | Sí | Sí | No |
| almacenamiento.cubos.obtenerPolíticaIam | | Sí | Sí | No |

**Permisos utilizados para NetApp Backup and Recovery**

El agente de consola usa los permisos en el rol personalizado para administrar los recursos y procesos de NetApp Backup and Recovery en su red de Google Cloud. Las siguientes secciones describen cómo el agente utiliza estos permisos.

**Ver permisos para NetApp Backup and Recovery**

| Comportamiento | Objetivo | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| • cloudkms.cryptoKeys.get<br>• cloudkms.cryptoKeys.getIamPolicy<br>• cloudkms.cryptoKeys.lista<br>• cloudkms.cryptoKeys.setIamPolicy<br>• cloudkms.keyRings.get<br>• cloudkms.keyRings.getIamPolicy<br>• lista de llaveros cloudkms<br>• cloudkms.keyRings.setIamPolicy | Para seleccionar sus propias claves administradas por el cliente en el asistente de activación de NetApp Backup and Recovery en lugar de utilizar las claves de cifrado administradas por Google predeterminadas. | Sí | Sí | No |

**Permisos utilizados para la NetApp Data Classification**

El agente de consola usa los permisos en la función personalizada para administrar los recursos y procesos de NetApp Data Classification en su red de Google Cloud. Las siguientes secciones describen cómo el agente utiliza estos permisos.

**Ver permisos para la NetApp Data Classification**

| Comportamiento | Objetivo | ¿Se utiliza para implementación? | ¿Se utiliza para operaciones diarias? | ¿Se utiliza para eliminar? |
|---|---|---|---|---|
| • usar subredes de computación<br>• compute.subnetworks.useExternalIp<br>• compute.instances.addAccessConfig | Para habilitar la NetApp Data Classification. | Sí | No | No |

**Registro de cambios**

Los permisos agregados y eliminados se detallan a continuación.

**08 de diciembre de 2025**

NetApp está migrando de Google Cloud Deployment Manager a Google Cloud Infrastructure Manager (IM) para implementar y ejecutar el agente de consola en Google Cloud. Se agregaron los siguientes permisos para respaldar este cambio.

Los siguientes permisos agregados son necesarios para el usuario de Google Cloud que implementa el agente:

- almacenamiento.cubos.crear
- almacenamiento.cubos.obtener
- almacenamiento.objetos.crear
- almacenamiento.carpetas.crear
- almacenamiento.objetos.lista
- iam.serviceAccount.actAs
- config.deployments.create
- config.operaciones.get

Se requieren los siguientes permisos adicionales para la cuenta de servicio en Google Cloud utilizada para las operaciones diarias:

- lista de conexiones de cloudbuild
- cloudbuild.repositories.accessReadToken
- lista de repositorios de cloudbuild
- cloudquotas.quotas.get

- config.artefactos.importar
- config.deployments.deleteState
- config.deployments.getLock
- config.deployments.getState
- config.deployments.updateState
- config.previews.upload
- config.revisions.getState
- registro.logEntries.create
- almacenamiento.objetos.crear
- almacenamiento.objetos.eliminar
- almacenamiento.objetos.actualizar
- iam.serviceAccounts.get

Se requieren los siguientes permisos agregados para implementar Cloud Volumes ONTAP:

- cloudbuild.builds.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- lista de configuraciones de despliegue
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- lista de vistas previas de configuración
- config.revisions.get
- lista de recursos de configuración
- iam.serviceAccountKeys.create
- iam.serviceAccounts.create

Los siguientes permisos agregados son necesarios para la cuenta de servicio utilizada para las operaciones diarias de Cloud Volumes ONTAP.

- computar.direcciones.crearInterno
- computar.direcciones.eliminarInterno
- calcular.direcciones.establecerEtiquetas
- computar.direcciones.useInternal
- calcular.reenvíoReglas.crear
- calcular.reenvíoReglas.eliminar
- calcular.reenvíoReglas.obtener

- calcular.reenvíoReglas.establecerEtiquetas
- computar.healthChecks.crear
- computar.healthChecks.eliminar
- computar.healthChecks.get
- computar.healthChecks.useReadOnly
- computar.gruposdeinstancias.crear
- calcular.gruposdeinstancias.eliminar
- computar.gruposdeinstancias.actualizar
- computar.gruposdeinstancias.uso
- computar.instancias.uso
- computar.regionBackendServices.eliminar
- computar.regionBackendServices.update
- computar.regiónBackendServices.uso
- computar.políticasderecursos.crear
- computar.políticasderecursos.eliminar
- computar.políticasderecursos.obtener
- registro.logEntries.route
- config.deployments.create
- config.deployments.delete
- config.deployments.get
- config.deployments.update
- config.revisions.get
- config.deployments.lock
- config.operaciones.get

**26 de noviembre de 2025**

Los permisos se han actualizado para aclarar su uso, pero no se han añadido ni eliminado permisos. Se añaden tres columnas para indicar si cada permiso se utiliza para la implementación, las operaciones diarias o la eliminación. Aparte de esto, algunos permisos están segregados en función de su uso para NetApp Data Classification y NetApp Backup and Recovery.

**6 de febrero de 2023**

Se agregó el siguiente permiso a esta política:

- computar.instancias.actualizarInterfazDeRed

Este permiso es necesario para Cloud Volumes ONTAP.

**27 de enero de 2023**

Se agregaron los siguientes permisos a esta política:

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

Estos permisos son necesarios para NetApp Backup and Recovery.

#### Reglas de firewall del agente en Google Cloud

Las reglas de firewall de Google Cloud para el agente requieren reglas tanto entrantes como salientes. La NetApp Console crea automáticamente este grupo de seguridad cuando crea un agente de consola desde la consola. Para otras opciones de instalación, debe configurar este grupo de seguridad manualmente.

##### Reglas de entrada

| Protocolo | Puerto | Objetivo |
|---|---|---|
| SSH | 22 | Proporciona acceso SSH al host del agente |
| HTTP | 80 | • Proporciona acceso HTTP desde los navegadores web del cliente a la interfaz de usuario local<br>• Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP |
| HTTPS | 443 | Proporciona acceso HTTPS desde los navegadores web del cliente a la interfaz de usuario local |
| TCP | 3128 | Proporciona a Cloud Volumes ONTAP acceso a Internet. Debe abrir este puerto manualmente después de la implementación. |

##### Reglas de salida

Las reglas de firewall predefinidas del agente abren todo el tráfico saliente. Siga las reglas básicas de salida si es aceptable o utilice reglas avanzadas de salida para requisitos más estrictos.

#### Reglas básicas de salida

Las reglas de firewall predefinidas para el agente incluyen las siguientes reglas de salida.

| Protocolo | Puerto | Objetivo |
|---|---|---|
| Todo TCP | Todo | Todo el tráfico saliente |
| Todos los UDP | Todo | Todo el tráfico saliente |

#### Reglas de salida avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir solo aquellos puertos que el agente requiere para la comunicación saliente.

La dirección IP de origen es el host del agente.

| Servicio | Protocolo | Puerto | Destino | Objetivo |
|---|---|---|---|---|
| Llamadas API y AutoSupport | HTTPS | 443 | LIF de gestión de clústeres ONTAP e Internet saliente | Llamadas API a Google Cloud, a ONTAP, a NetApp Data Classification y envío de mensajes de AutoSupport a NetApp |
| Llamadas API | TCP | 8080 | Clasificación de datos | Sonda a la instancia de clasificación de datos durante la implementación |
| DNS | UDP | 53 | DNS | Se utiliza para la resolución de DNS mediante clasificación de datos |

# Acceso a la red requerido para 3.9.55 y anteriores

La NetApp Console, el agente de la NetApp Console y los servicios de datos de NetApp requieren acceso a Internet saliente para comunicarse con los puntos finales necesarios.

Este tema documenta el acceso a la red necesario para las versiones del modo estándar de la NetApp Console 3.9.55 y anteriores. Para conocer los puntos finales necesarios para 4.0.0 y superiores, revise"los puntos finales necesarios para 4.0.0 y superiores" .

Debe configurar el acceso a la red para lo siguiente:

- Computadoras que acceden a la NetApp Console como software como servicio (SaaS)
- Agentes de consola que se instalan localmente o en la nube.

## Actualice su lista de puntos finales a la lista revisada para 4.0.0 y versiones superiores

A partir de la versión 4.0.0, los agentes de consola requieren menos puntos finales. Las implementaciones existentes anteriores a la versión 4.0.0 siguen siendo compatibles. Después de actualizar a 4.0.0 o posterior, puede eliminar los puntos finales antiguos de su lista de permitidos cuando sea conveniente.

NetApp recomienda actualizar las reglas de firewall para utilizar la lista de puntos finales revisada, que es más pequeña, más segura y más fácil de administrar. NetApp elimina la necesidad de entradas comodín y los puntos finales para actualizaciones de agentes admiten todos los servicios de datos.

| Puntos finales para la versión 3.9.55 y anteriores | Puntos finales para 4.0.0 y superiores | Objetivo |
|---|---|---|
| • \ https://support.netapp.com<br>• \ https://mysupport.netapp.com | • \ https://mysupport.netapp.com<br>• \ https://signin.b2c.netapp.com<br>• \ https://support.netapp.com | Para obtener licencias y comunicarse con el soporte técnico de NetApp . |
| • https://*.api.bluexp.netapp.com<br>• \ https://api.bluexp.netapp.com<br>• https://*.cloudmanager.cloud.netapp.com<br>• \ https://cloudmanager.cloud.netapp.com<br>• \ https://netapp-cloud-account.auth0.com<br>• \ https://netapp-cloud-account.us.auth0.com<br>• \ https://console.bluexp.netapp.com<br>• https://*.console.bluexp.netapp.com | • \ https://api.bluexp.netapp.com<br>• \ https://netapp-cloud-account.auth0.com<br>• \ https://netapp-cloud-account.us.auth0.com<br>• \ https://console.netapp.com<br>• \ https://components.console.bluexp.netapp.com<br>• \ https://cdn.auth0.com | Para operaciones diarias. |
| • https://*.blob.core.windows.net<br>• \ https://cloudmanagerinfraprod.azurecr.io | • \ https://bluexpinfraprod.eastus2.data.azurecr.io<br>• \ https://bluexpinfraprod.azurecr.io | Para obtener imágenes para las actualizaciones del agente de consola. |

**Pasos**

1. Verifique que su agente sea la versión 4.0.0 o superior."Ver la versión del agente."
2. Incluir en la lista blanca los puntos finales en"Puntos finales compatibles con 4.0.0 y superiores" .
3. Reinicie el servicio del administrador de servicios 2 en cada agente ejecutando el siguiente comando:

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

4. Ejecute el siguiente comando y verifique que el estado del agente se muestre como *activo(en ejecución)*: _

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

5. Elimina los puntos finales antiguos de la lista de permitidos de tu firewall.

## Puntos finales para la NetApp Console y los agentes de consola para la versión 3.9.55 y anteriores

Estos puntos finales se utilizan para agentes de consola 3.9.55 y anteriores.

| Puntos finales | Objetivo |
|---|---|
| \ https://support.netapp.com \ https://mysupport.netapp.com | Para obtener información de licencias y enviar mensajes de AutoSupport al soporte de NetApp . |
| https://*.api.bluexp.netapp.com \ https://api.bluexp.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 | Proporcionar funciones y servicios dentro de la NetApp Console. |
| Elija entre dos conjuntos de puntos finales:<br>• Opción 1 (recomendada)<br>\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io<br>• Opción 2<br>https://*.blob.core.windows.net\ https://cloudmanagerinfraprod.azurecr.io | Para obtener imágenes para las actualizaciones del agente de consola.<br>NetApp recomienda permitir los puntos finales de la Opción 1 en su firewall, ya que son más seguros, y no permitir los puntos finales de la Opción 2, a menos que esté usando Ransomware Resilience o Backup and Recovery. Tenga en cuenta lo siguiente acerca de estos puntos finales:<br>• Los puntos finales de la opción 1 son compatibles con 3.9.47 y versiones posteriores. Las versiones anteriores a 3.9.47 no admiten compatibilidad con versiones anteriores.<br>• El agente de consola inicia primero el contacto con los puntos finales en la opción 2. Si esos puntos finales no son accesibles, se contacta automáticamente con los puntos finales de la opción 1.<br>• Si utiliza el agente de consola con NetApp Backup and Recovery o Ransomware Resilience, el sistema no admite puntos finales de la Opción 1. Permitir puntos finales de la Opción 2 y no permitir la Opción 1. |

## Puntos finales del proveedor de la nube contactados por el agente de la consola

Los agentes de consola deben tener acceso a puntos finales adicionales si están implementados en su proveedor de nube.

Habilite el acceso a los puntos finales del proveedor de nube antes de instalar el agente de consola.

- "Configurar el acceso a la red de AWS para un agente de consola"
- "Configurar el acceso a la red de Azure para un agente de consola"
- "Configurar el acceso a la red de Google Cloud para un agente de la consola"

Los puntos finales del proveedor de nube son los mismos para todas las versiones.

### Puntos finales de servicios de datos contactados por el agente de la consola

El agente de consola requiere acceso a Internet saliente adicional para admitir algunos servicios de datos de NetApp y Cloud Volumes ONTAP.

#### Puntos finales para Cloud Volumes ONTAP

- "Puntos finales para Cloud Volumes ONTAP en AWS"
- "Puntos de conexión para Cloud Volumes ONTAP en Azure"
- "Puntos finales para Cloud Volumes ONTAP en Google Cloud"

# Requerir el uso de IMDSv2 en instancias de Amazon EC2

La NetApp Console admite el servicio de metadatos de instancia de Amazon EC2 versión 2 (IMDSv2) con el agente de consola y con Cloud Volumes ONTAP (incluido el mediador para implementaciones de alta disponibilidad). En la mayoría de los casos, IMDSv2 se configura automáticamente en las nuevas instancias EC2. IMDSv1 se habilitó antes de marzo de 2024. Si sus políticas de seguridad lo requieren, es posible que deba configurar manualmente IMDSv2 en sus instancias EC2.

#### Antes de empezar

- La versión del agente de consola debe ser 3.9.38 o posterior.
- Cloud Volumes ONTAP debe ejecutar una de las siguientes versiones:
  - 9.12.1 P2 (o cualquier parche posterior)
  - 9.13.0 P4 (o cualquier parche posterior)
  - 9.13.1 o cualquier versión posterior a esta
- Este cambio requiere que reinicie las instancias de Cloud Volumes ONTAP .
- Estos pasos requieren el uso de AWS CLI porque debe cambiar el límite de saltos de respuesta a 3.

#### Acerca de esta tarea

IMDSv2 proporciona protección mejorada contra vulnerabilidades. "Obtenga más información sobre IMDSv2 en el blog de seguridad de AWS."

El Servicio de metadatos de instancia (IMDS) se habilita de la siguiente manera en las instancias EC2:

- Para nuevas implementaciones de agentes de consola desde la consola o mediante "Scripts de Terraform" IMDSv2 está habilitado de forma predeterminada en la instancia EC2.
- Si lanza una nueva instancia EC2 en AWS y luego instala manualmente el software del agente de consola, IMDSv2 también estará habilitado de forma predeterminada.
- Si inicia el agente de consola desde AWS Marketplace, IMDSv1 estará habilitado de forma

predeterminada. Puede configurar manualmente IMDSv2 en la instancia EC2.

- Para los agentes de consola existentes, IMDSv1 aún es compatible, pero puede configurar manualmente IMDSv2 en la instancia EC2 si lo prefiere.
- Para Cloud Volumes ONTAP, IMDSv1 está habilitado de forma predeterminada en instancias nuevas y existentes. Puede configurar manualmente IMDSv2 en las instancias EC2 si lo prefiere.

**Pasos**

1. Requerir el uso de IMDSv2 en la instancia del agente de consola:

   a. Conéctese a la máquina virtual Linux para el agente de consola.

      Cuando creó la instancia del agente de consola en AWS, proporcionó una clave de acceso y una clave secreta de AWS. Puede utilizar este par de claves para conectarse mediante SSH a la instancia. El nombre de usuario para la instancia EC2 Linux es ubuntu (para los agentes de consola creados antes de mayo de 2023, el nombre de usuario era ec2-user).

      "Documentación de AWS: Conéctese a su instancia de Linux"

   b. Instalar la AWS CLI.

      "Documentación de AWS: Instalar o actualizar a la última versión de la AWS CLI"

   c. Utilice el `aws ec2 modify-instance-metadata-options` comando para requerir el uso de IMDSv2 y cambiar el límite de saltos de respuesta PUT a 3.

      **Ejemplo**

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

+

> El `http-tokens` conjuntos de parámetros IMDSv2 como obligatorios. Cuando `http-tokens` es obligatorio, también debes configurar `http-endpoint` para habilitar.

2. Requerir el uso de IMDSv2 en instancias de Cloud Volumes ONTAP :

   a. Ir a la "Consola de Amazon EC2"

   b. Desde el panel de navegación, seleccione **Instancias**.

   c. Seleccione una instancia de Cloud Volumes ONTAP .

   d. Seleccione **Acciones > Configuración de instancia > Modificar opciones de metadatos de instancia**.

   e. En el cuadro de diálogo **Modificar opciones de metadatos de instancia**, seleccione lo siguiente:

      - Para **Servicio de metadatos de instancia**, seleccione **Habilitar**.
      - Para **IMDSv2**, seleccione **Obligatorio**.

- Seleccione **Guardar**.

f. Repita estos pasos para otras instancias de Cloud Volumes ONTAP , incluido el mediador de HA.

g. "Detener e iniciar las instancias de Cloud Volumes ONTAP"

**Resultado**

La instancia del agente de consola y las instancias de Cloud Volumes ONTAP ahora están configuradas para usar IMDSv2.

# Configuración predeterminada para el agente de consola

Obtenga información sobre las configuraciones predeterminadas del agente de consola para implementaciones estándar (con acceso a Internet) en AWS, Azure y Google Cloud, así como para implementaciones restringidas (sin acceso a Internet) en entornos locales.

## Configuración predeterminada con acceso a Internet

Los siguientes detalles de configuración se aplican si implementó un agente de consola desde la NetApp Console, desde el mercado de su proveedor de nube o si instaló manualmente un agente de consola en un host Linux local que tiene acceso a Internet.

### Detalles de la máquina virtual del agente de consola para AWS

Si implementó un agente de consola desde la consola o desde el mercado del proveedor de la nube, tenga en cuenta lo siguiente:

- El tipo de instancia EC2 es t3.2xlarge.
- El sistema operativo de la imagen es Ubuntu 22.04 LTS.

  El sistema operativo no incluye una GUI. Debe utilizar una terminal para acceder al sistema.

- La instalación incluye Docker Engine, que es la herramienta de orquestación de contenedores necesaria.
- El nombre de usuario para la instancia EC2 Linux es ubuntu (para los agentes creados antes de mayo de 2023, el nombre de usuario es ec2-user).
- El disco del sistema predeterminado es un disco gp2 de 100 GiB.

### Detalles de la máquina virtual del agente de consola para Azure

Si implementó un agente de consola desde la consola o desde el mercado del proveedor de la nube, tenga en cuenta lo siguiente:

- El tipo de VM es Standard_D8s_v3.
- El sistema operativo de la imagen es Ubuntu 22.04 LTS.

  El sistema operativo no incluye una GUI. Debe utilizar una terminal para acceder al sistema.

- La instalación incluye Docker Engine, que es la herramienta de orquestación de contenedores necesaria.
- El disco del sistema predeterminado es un disco SSD premium de 100 GiB.

#### Detalles de la máquina virtual del agente de consola para Google Cloud

Si implementó un agente de consola desde la consola, tenga en cuenta lo siguiente:

- La instancia de VM es n2-standard-8.
- El sistema operativo de la imagen es Ubuntu 22.04 LTS.

  El sistema operativo no incluye una GUI. Debe utilizar una terminal para acceder al sistema.

- La instalación incluye Docker Engine, que es la herramienta de orquestación de contenedores necesaria.
- El disco del sistema predeterminado es un disco persistente SSD de 100 GiB.

#### Carpeta de instalación

La carpeta de instalación del agente se encuentra en la siguiente ubicación:

`/opt/application/netapp/cloudmanager`

#### Archivos de registro

Los archivos de registro se encuentran en las siguientes carpetas:

- `/opt/application/netapp/cloudmanager/log` o
- `/opt/application/netapp/service-manager-2/logs` (a partir de las nuevas instalaciones 3.9.23)

  Los registros de estas carpetas proporcionan detalles sobre el agente de la consola.

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

  Los registros de esta carpeta proporcionan detalles sobre los servicios en la nube y el servicio de consola que se ejecuta en el agente de consola.

#### Servicio de agente de consola

- El servicio del agente de consola se llama occm.
- El servicio occm depende del servicio MySQL.

  Si el servicio MySQL está inactivo, entonces el servicio occm también estará inactivo.

#### Puertos

El agente utiliza los siguientes puertos en el host Linux:

- 80 para acceso HTTP
- 443 para acceso HTTPS

## Configuración predeterminada sin acceso a Internet

La siguiente configuración se aplica si instaló manualmente el agente de consola en un host Linux local que no tiene acceso a Internet. "Obtenga más información sobre esta opción de instalación" .

- La carpeta de instalación del agente se encuentra en la siguiente ubicación:

  `/opt/application/netapp/ds`

- Los archivos de registro se encuentran en las siguientes carpetas:

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

  Los registros de esta carpeta proporcionan detalles sobre el agente de la consola y las imágenes de Docker.

- Todos los servicios se ejecutan dentro de contenedores Docker

  Los servicios dependen del servicio de tiempo de ejecución de Docker que se esté ejecutando

- El agente utiliza los siguientes puertos en el host Linux:
  - 80 para acceso HTTP
  - 443 para acceso HTTPS