Permisos del agente de AWS y reglas de seguridad

NetApp Console setup and administration

NetApp
February 11, 2026

Tabla de contenidos

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 • 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

Protocolo	Puerto	Objetivo
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

Información de copyright

Información de la marca comercial