Permisos

Set up and administration

NetApp
March 10, 2023

Tabla de Contenido

Permisos

Resumen de permisos para BlueXP

Para poder utilizar las funciones y servicios de BlueXP, deberá proporcionar permisos para que BlueXP pueda realizar operaciones en su entorno de nube. Utilice los vínculos de esta página para acceder rápidamente a los permisos que necesita en función de su objetivo.

Permisos de AWS

Específico	Descripción	Enlace
Despliegue del conector	El usuario que crea un conector a partir de BlueXP necesita permisos específicos para implementar la instancia en AWS.	"Cree un conector en AWS desde BlueXP"
Funcionamiento del conector	Cuando BlueXP inicia el conector, adjunta una directiva a la instancia que proporciona los permisos necesarios para administrar los recursos y procesos de su cuenta de AWS. Usted debe establecer la política usted mismo si usted "Inicie un conector desde el mercado" o si usted "Agregue más credenciales de AWS a un conector". También debe asegurarse de que la directiva esté actualizada a medida que se añadan nuevos permisos en versiones posteriores.	"Permisos de AWS para Connector"
Funcionamiento de Cloud Volumes ONTAP	Se debe conectar un rol de IAM a cada nodo Cloud Volumes ONTAP en AWS. Lo mismo sucede con el mediador de alta disponibilidad. La opción predeterminada es dejar que BlueXP cree las funciones IAM para usted, pero puede utilizar las suyas propias.	"Aprenda a configurar las funciones del IAM usted mismo"

Permisos de Azure

Específico	Descripción	Enlace
Despliegue del conector	Al implementar un conector desde BlueXP, necesita utilizar una cuenta de Azure o una entidad de servicio con permisos para implementar Connector VM en Azure.	"Cree un conector en Azure desde BlueXP"

Específico	Descripción	Enlace
Funcionamiento del conector	Cuando BlueXP implementa Connector VM en Azure, crea una función personalizada que proporciona los permisos necesarios para gestionar los recursos y procesos dentro de esa suscripción a Azure. Debe configurar la función personalizada si lo desea "Inicie un conector desde el mercado" o si usted "Agregue más credenciales de Azure a un conector". También debe asegurarse de que la directiva esté actualizada a medida que se añadan nuevos permisos en versiones posteriores.	"Permisos de Azure para Connector"

Permisos de Google Cloud

Específico	Descripción	Enlace
Despliegue del conector	El usuario de Google Cloud que implementa un conector de BlueXP necesita permisos específicos para implementar el conector en Google Cloud.	"Configure los permisos para desplegar el conector"
Funcionamiento del conector	La cuenta de servicio de la instancia de Connector VM debe tener permisos específicos para las operaciones del día a día. Debe asociar la cuenta de servicio al conector cuando la despliegue desde BlueXP. También debe asegurarse de que la directiva esté actualizada a medida que se añadan nuevos permisos en versiones posteriores.	"Configure una cuenta de servicio para el conector"

Permisos de AWS para Connector

Cuando BlueXP inicia la instancia de Connector en AWS, asocia una directiva a la instancia que proporciona al conector permisos para administrar recursos y procesos dentro de esa cuenta de AWS. El conector utiliza los permisos para realizar llamadas API a varios servicios de AWS, incluidos EC2, S3, CloudFormation, IAM, El Servicio de gestión de claves (KMS), etc.

Políticas IAM

Las políticas de IAM disponibles a continuación proporcionan los permisos que un conector necesita para gestionar recursos y procesos dentro de su entorno de cloud público basado en su región de AWS.

Si crea un conector en una región estándar de AWS directamente desde BlueXP, BlueXP aplica automáticamente directivas al conector. En este caso no es necesario hacer nada.

Si pone en marcha el conector desde AWS Marketplace o si instala manualmente el conector en un host Linux, deberá configurar las políticas usted mismo.

También debe asegurarse de que las directivas estén actualizadas a medida que se añadan nuevos permisos en versiones posteriores.

Seleccione su región para ver las políticas necesarias:

Regiones estándar

Para las regiones estándar, los permisos se distribuyen en dos directivas. Son necesarias dos políticas debido a un límite máximo de tamaño de carácter para las políticas gestionadas en AWS.

La primera directiva proporciona permisos para los siguientes servicios:

- Backup en el cloud
- Cloud Data SENSE
- Organización en niveles del cloud
- Cloud Volumes ONTAP
- FSX para ONTAP
- Detección de bloques de S3

La segunda directiva proporciona permisos para los siguientes servicios:

- Etiquetado de AppTemplate
- Caché de archivos global
- Kubernetes

Política #1

```
{
    "Statement": [
        {
            "Action": [
                "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:List*",
```

```
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ce:GetReservationUtilization",
                "ce:GetDimensionValues",
                "ce:GetCostAndUsage",
                "ce:GetTags",
                "fsx:Describe*",
                "fsx:List*"
            ],
            "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",
                "kms:List*",
                "kms:Describe*",
                "ec2:DescribeVpcEndpoints",
                "kms:ListAliases",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
```

```
                "glue:BatchDeletePartition"
            ],
            "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

```
{
    "Statement": [
        {
            "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"
        },
        {
```

```
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "tag:getResources",
                "tag:getTagKeys",
                "tag:getTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "tagServicePolicy"
        }
    ]
}
```

Regiones 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:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ce:GetReservationUtilization",
                "ce:GetDimensionValues",
                "ce:GetCostAndUsage",
                "ce:GetTags",
                "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/*"
            ]
        }
    ]
}
```

Entorno C2S

```
{
    "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",
                "kms:List*",
                "kms:Describe*",
                "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

En las siguientes secciones se describe cómo se utilizan los permisos para cada servicio cloud de NetApp. Esta información puede ser útil si sus políticas corporativas dictan que los permisos sólo se proporcionan según sea necesario.

Etiquetas de AppTemplate

El conector realiza las siguientes solicitudes de API para administrar etiquetas en recursos de AWS cuando utiliza el servicio de etiquetado AppTemplate:

- ec2:CreateTags
- ec2:DeleteTags
- ec2:etiquetas a describTags
- Tag:getResources
- Etiqueta:getTagKeys
- Etiqueta:getTagValues
- Tag:TagResources
- Tag:UntagResources

Backup en el cloud

El conector realiza las siguientes solicitudes API para implementar la instancia de restauración para Cloud Backup:

- ec2:StartuStarInstances
- ec2:StopInstances
- ec2:DescribInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:DescribeInstanceAttribute
- ec2:DescribeImages
- ec2:CreateTags
- ec2:CreateVolume
- ec2:CreateSecurityGroup
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:regiones describidas
- Cloudformation:CreateStack
- Cloudformation:DeleteStack
- Cloudformation:Describacks

El conector realiza las siguientes solicitudes API para gestionar backups en Amazon S3:

- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:CreateBucket
- s3:GetLifecycleConfiguration
- s3:PutLipeycleConfiguration
- s3:PutBucketEtiquetado
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- Kms:Lista*
- Kms:describir*
- s3:GetObject
- ec2:DescribeVpcEndpoints
- Kms:ListAliases

- s3:PutEncryptionConfiguration

El conector realiza las siguientes solicitudes API cuando utiliza el método Search & Restore para restaurar volúmenes y archivos:

- s3:CreateBucket
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLipeycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMultipartUpload
- s3:ListMultipartUploadParts
- athena:StartQueryExecutionc
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- Cola:CreateDatabase
- Pegar:CreateTable
- Cola:BatchDeletePartition

El conector realiza las siguientes solicitudes de API al usar la protección DataLock y ransomware para los backups de volúmenes:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectEtiquetado
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration

- s3:GetLifecycleConfiguration
- s3:ListBucketByTags
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketEtiquetado
- s3:GetObjectTagging
- s3:PutBucketVersioning
- s3:PutObjectVersionEtiquetado
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

El conector realiza las siguientes solicitudes de API si utiliza una cuenta de AWS diferente para los backups de Cloud Volumes ONTAP de la que usa en los volúmenes de origen:

- s3:PutBucketPolicy
- s3:PutBucketOwnershipControls

Cloud Data SENSE

El conector realiza las siguientes solicitudes de API para implementar la instancia de Cloud Data Sense:

- ec2:DescribInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:CreateTags
- ec2:CreateVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2:DeleteSecurityGroup
- ec2:DescribeSecurityGroups
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkinterfaces
- ec2:DeleteNetworkInterface
- ec2:DescribeSubnets

- ec2:DescribeVpcs
- ec2:CreateSnapshot
- ec2:regiones describidas
- Cloudformation:CreateStack
- Cloudformation:DeleteStack
- Cloudformation:Describacks
- Cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

El conector realiza las siguientes solicitudes de API para analizar bloques de S3 cuando utiliza Cloud Data Sense:

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:PutObject
- sts:AssumeRole

Organización en niveles del cloud

El conector realiza las siguientes solicitudes de API para organizar los datos en niveles en Amazon S3 cuando se utiliza Cloud Tiering.

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
s3:CreateBucket	Sí	No
s3:PutLipeycleConfiguration	Sí	No
s3:GetLifecycleConfiguration	Sí	Sí

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
ec2:regiones describidas	Sí	No
ec2:DescribeVpcEndpoints	Sí	No

Cloud Volumes ONTAP

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

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Crear y gestionar roles e perfiles de instancia de IAM para instancias de Cloud Volumes ONTAP	iam:ListInstanceProfiles	Sí	Sí	No
	iam:CreateRole	Sí	No	No
	iam:DeleteRole	No	Sí	Sí
	iam:PutRolePolicy	Sí	No	No
	iam:CreateInstanceProfile	Sí	No	No
	iam:DeleteRolePolicy	No	Sí	Sí
	iam:AddRoleToInstanceProfile	Sí	No	No
	iam:RemoveRoleFromInstanceProfile	No	Sí	Sí
	iam:DeleteInstanceProfile	No	Sí	Sí
	iam:PassRole	Sí	No	No
	ec2:AssociateIamInstanceProfile	Sí	Sí	No
	ec2:DescribeIamInstanceProfileAssociations	Sí	Sí	No
	ec2:DisasociateIamInstanceProfile	No	Sí	No
Descodificar mensajes de estado de autorización	sts:DecodeAuthorizationMessage	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Describa las imágenes especificadas (AMI) disponibles para la cuenta	ec2:DescribeImages	Sí	Sí	No
Describir las tablas de rutas en un VPC (solo necesarias para los pares de alta disponibilidad)	ec2:DescribeRouteTables	Sí	No	No
Detener, iniciar y supervisar instancias	ec2:StartuStarInstances	Sí	Sí	No
	ec2:StopInstances	Sí	Sí	No
	ec2:DescribInstances	Sí	Sí	No
	ec2:DescribeInstanceStatus	Sí	Sí	No
	ec2:RunInstances	Sí	No	No
	ec2:TerminateInstances	No	No	Sí
	ec2:ModificyInstanceAttribute	No	Sí	No
Compruebe que las redes mejoradas estén habilitadas para los tipos de instancia 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 costes	ec2:CreateTags	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Gestione volúmenes de EBS que Cloud Volumes ONTAP utiliza como almacenamiento back-end	ec2:CreateVolume	Sí	Sí	No
	ec2:DescribeVolumes	Sí	Sí	Sí
	ec2:ModifyVolumeAttribute	No	Sí	Sí
	ec2:AttachVolume	Sí	Sí	No
	ec2:DeleteVolume	No	Sí	Sí
	ec2:DetachVolume	No	Sí	Sí
Crear y administrar grupos de seguridad para Cloud Volumes ONTAP	ec2:CreateSecurityGroup	Sí	No	No
	ec2:DeleteSecurityGroup	No	Sí	Sí
	ec2:DescribeSecurityGroups	Sí	Sí	Sí
	ec2:RevokeSecurityGroupEgress	Sí	No	No
	ec2:AuthorizeSecurityGroupEgress	Sí	No	No
	ec2:AuthorizeSecurityGroupIngress	Sí	No	No
	ec2:RevokeSecurityGroupIngress	Sí	Sí	No
Cree y gestione interfaces de red para Cloud Volumes ONTAP en la subred de destino	ec2:CreateNetworkInterface	Sí	No	No
	ec2:DescribeNetworkinterfaces	Sí	Sí	No
	ec2:DeleteNetworkInterface	No	Sí	Sí
	ec2:ModificyNetworkInterfaceAttribute	No	Sí	No
Obtenga la lista de subredes de destino y grupos de seguridad	ec2:DescribeSubnets	Sí	Sí	No
	ec2:DescribeVpcs	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Obtenga los servidores DNS y el nombre de dominio predeterminado para las instancias de Cloud Volumes ONTAP	ec2:DescribDhcpOptions	Sí	No	No
Tome snapshots de volúmenes de EBS para Cloud Volumes ONTAP	ec2:CreateSnapshot	Sí	Sí	No
	ec2:DeleteSnapshot	No	Sí	Sí
	ec2:DescribSnapshots	No	Sí	No
Capture la consola Cloud Volumes ONTAP, que está conectada a mensajes de AutoSupport	ec2:GetConsoleOutput	Sí	Sí	No
Obtenga la lista de pares de claves disponibles	ec2:DescribeKeyPairs	Sí	No	No
Obtenga la lista de regiones disponibles de AWS	ec2:regiones describidas	Sí	Sí	No
Gestione etiquetas para los recursos asociados a instancias de Cloud Volumes ONTAP	ec2:DeleteTags	No	Sí	Sí
	ec2:etiquetas a describTags	No	Sí	No
Cree y administre pilas para plantillas CloudFormation de AWS	Cloudformation:CreateStack	Sí	No	No
	Cloudformation:DeleteStack	Sí	No	No
	Cloudformation:Describacks	Sí	Sí	No
	Cloudformation:DescribeStackEvents	Sí	No	No
	Cloudformation:ValidateTemplate	Sí	No	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Cree y gestione un bloque de S3 que un sistema Cloud Volumes ONTAP utiliza como nivel de capacidad para la organización en niveles de datos	s3:CreateBucket	Sí	Sí	No
	s3:DeleteBucket	No	Sí	Sí
	s3:GetLifecycleConfiguration	No	Sí	No
	s3:PutLipeycleConfiguration	No	Sí	No
	s3:PutBucketEtiquetado	No	Sí	No
	s3:ListBucketVersions	No	Sí	No
	s3:GetBucketPolicyStatus	No	Sí	No
	s3:GetBucketPublicAccessBlock	No	Sí	No
	s3:GetBucketAcl	No	Sí	No
	s3:GetBucketPolicy	No	Sí	No
	s3:PutBucketPublicAccessBlock	No	Sí	No
	s3:GetBucketTagging	No	Sí	No
	s3:GetBucketLocation	No	Sí	No
	s3:ListAllMyBuckets	No	No	No
	s3:ListBucket	No	Sí	No
Habilitar el cifrado de datos de Cloud Volumes ONTAP mediante el servicio de gestión de claves (KMS) de AWS	Kms:Lista*	Sí	Sí	No
	Kms:Recifrar*	Sí	No	No
	Kms:describir*	Sí	Sí	No
	Kms:CreateGrant	Sí	Sí	No
Obtenga datos de coste de AWS para Cloud Volumes ONTAP	ce:GetReservationUtilización	No	Sí	No
	ce:GetDimensionValues	No	Sí	No
	ce:GetCostAndUsage	No	Sí	No
	ce:getTags	No	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Cree y gestione un grupo de colocación extendido de AWS para dos nodos de alta disponibilidad y el mediador en una única zona de disponibilidad de AWS	ec2:CreatePlacementGroup	Sí	No	No
	ec2:DeletePlacementGroup	No	Sí	Sí
Crear informes	fsx:describe*	No	Sí	No
	fsx:List*	No	Sí	No
Cree y gestione agregados que admitan la función Amazon EBS Elastic Volumes	ec2:DescribVolumes Modificaciones	No	Sí	No
	ec2:ModifiyVolume	No	Sí	No

Caché de archivos global

El conector realiza las siguientes solicitudes de API para implementar instancias de caché de archivos global durante la implementación:

- Cloudformation:Describacks
- Cloudwatch:GetMetricStatistics
- Cloudformation:ListStacks

FSX para ONTAP

El conector realiza las siguientes solicitudes de API para administrar FSX para ONTAP:

- ec2:DescribInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribute
- ec2:DescribeRouteTables
- ec2:DescribeImages
- ec2:CreateTags
- ec2:DescribeVolumes
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkinterfaces
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribDhcpOptions

- ec2:DescribSnapshots
- ec2:DescribeKeyPairs
- ec2:regiones describidas
- ec2:etiquetas a describTags
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeReservedInstancesOfferings
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ec2:DescribVolumesModificaciones
- ec2:DescribePlacementGroups
- Kms:Lista*
- Kms:describir*
- Kms:CreateGrant
- Kms:ListAliases
- fsx:describe*
- fsx:List*

Kubernetes

El conector realiza las siguientes solicitudes de API para detectar y gestionar clústeres de Amazon EKS:

- ec2:regiones describidas
- eks:ListClusters
- eks:DescribeCluster
- iam:GetInstanceProfile

Detección de bloques de S3

El conector hace la siguiente solicitud de API para detectar bloques de Amazon S3:

s3:GetEncryptionConfiguration

Registro de cambios

A medida que se añadan y eliminen permisos, los anotaremos en las secciones siguientes.

14 de febrero de 2023

Ahora se necesita el siguiente permiso para la organización en niveles del cloud:

ec2:DescribeVpcEndpoints

Permisos de Azure para Connector

Cuando BlueXP inicia Connector VM en Azure, asocia una función personalizada a la

máquina virtual que proporciona al conector permisos para gestionar recursos y procesos en esa suscripción a Azure. El conector utiliza los permisos para realizar llamadas API a varios servicios de Azure.

Permisos de roles personalizados

El rol personalizado que se muestra a continuación proporciona los permisos que un conector necesita para administrar recursos y procesos dentro de su red de Azure.

Al crear un conector directamente desde BlueXP, BlueXP aplica automáticamente esta función personalizada al conector.

Si pone en marcha el conector desde Azure Marketplace o si instala manualmente el conector en un host Linux, deberá configurar el rol personalizado usted mismo.

También debe asegurarse de que el rol esté actualizado a medida que se añadan nuevos permisos en versiones posteriores.

```
{
    "Name": "BlueXP 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/blobServices/containers/write",

"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.ContainerService/managedClusters/listClusterUserCredential/acti
on",
                    "Microsoft.ContainerService/managedClusters/read",
                    "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.Network/publicIPAddresses/delete",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
    ],
    "NotActions": [],
```

```
    "AssignableScopes": [],
    "Description": "BlueXP Permissions",
    "IsCustom": "true"
}
```

Cómo se utilizan los permisos de Azure

En las siguientes secciones se describe cómo se utilizan los permisos para cada servicio cloud de NetApp. Esta información puede ser útil si sus políticas corporativas dictan que los permisos sólo se proporcionan según sea necesario.

Etiquetas de AppTemplate

El conector realiza las siguientes solicitudes de API para administrar etiquetas en recursos de Azure cuando utiliza el servicio de etiquetado AppTemplate:

- Microsoft.Resources/resources/read
- Microsoft.Resources/subscripciones/operationResults/read
- Microsoft.Resources/subscriptions/ResourceGroups/read
- Microsoft.Resources/subscripciones/resourcegroups/resources/read
- Microsoft.Resources/etiquetas/leer
- Microsoft.Resources/etiquetas/escritura

Azure NetApp Files

El conector realiza las siguientes solicitudes de API para gestionar entornos de trabajo 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

Backup en el cloud

El conector realiza las siguientes solicitudes de API para operaciones de backup y restauración:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/Write
- Microsoft.Storage/storageAccounts/blobServices/contenedores/lectura
- Microsoft.Storage/storageAccounts/listAccountSas/action

- Microsoft.KeyVault/vaults/read
- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Resources/suscripciones/ubicaciones/leer
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Resources/subscriptions/ResourceGroups/read
- Microsoft.Resources/subscripciones/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/ResourceGroups/write
- Microsoft.Authorization/locks/*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- 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.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/despliegues/DELETE
- Microsoft.Network/publicIPAddresses/delete
- Microsoft.Storage/storageAccounts/blobServices/contenedores/escritura
- Microsoft.ManagedIdentity/userAssignedIdentities/ASSIGN/action

El conector realiza las siguientes solicitudes de API cuando utiliza la funcionalidad Buscar y restaurar:

- Microsoft.Synapse/Sáreas de trabajo/escritura
- Microsoft.Synapse/áreas de trabajo/lectura
- Microsoft.Synapse/áreas de trabajo/eliminar
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameAvailability/Action
- Microsoft.Synapse/Sáreas de trabajo/operationStatuses/Read
- Microsoft.Synapse/áreas de trabajo/firewallRules/read
- Microsoft.Synapse/spaces/replaceAllIpFirewallRules/acción
- Microsoft.Synapse/áreas de trabajo/operationResults/read
- Microsoft.Synapse/spots/privateEndpointConnectionsApproval/action

Cloud Data SENSE

El conector realiza las siguientes solicitudes de API cuando utiliza Cloud Data Sense.

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
Microsoft.Compute/locations/operations/read	Sí	Sí
Microsoft.Compute/locations/vmSizes/read	Sí	Sí
Microsoft.Compute/operations/read	Sí	Sí
Microsoft.Compute/virtualMachines/instanceView/read	Sí	Sí
Microsoft.Compute/virtualMachines/powerOff/action	Sí	No
Microsoft.Compute/virtualMachines/read	Sí	Sí
Microsoft.Compute/virtualMachines/restart/action	Sí	No
Microsoft.Compute/virtualMachines/start/action	Sí	No
Microsoft.Compute/virtualMachines/vmSizes/read	No	Sí
Microsoft.Compute/virtualMachines/write	Sí	No
Microsoft.Compute/images/read	Sí	Sí
Microsoft.Compute/disks/delete	Sí	No
Microsoft.Compute/disks/read	Sí	Sí
Microsoft.Compute/disks/write	Sí	No
Microsoft.Storage/checknameavailability/leer	Sí	Sí
Microsoft.almacenamiento/operaciones/lectura	Sí	Sí
Microsoft.Storage/storageAccounts/listkeys/action	Sí	No
Microsoft.Storage/storageAccounts/read	Sí	Sí
Microsoft.Storage/storageAccounts/Write	Sí	No
Microsoft.Storage/storageAccounts/DELETE	No	Sí

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
Microsoft.Storage/storageAccounts/blobServices/contenedores/lectura	Sí	Sí
Microsoft.Network/networkInterfaces/read	Sí	Sí
Microsoft.Network/networkInterfaces/write	Sí	No
Microsoft.Network/networkInterfaces/join/action	Sí	No
Microsoft.Network/networkSecurityGroups/read	Sí	Sí
Microsoft.Network/networkSecurityGroups/write	Sí	No
Microsoft.Resources/suscripciones/ubicaciones/leer	Sí	Sí
Microsoft.Network/locations/operationResults/read	Sí	Sí
Microsoft.Network/locations/operations/read	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/action	Sí	No
Microsoft.Resources/despliegues/operaciones/lectura	Sí	Sí
Microsoft.Resources/despliegues/leer	Sí	Sí
Microsoft.Resources/implementaciones/escritura	Sí	No

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
Microsoft.Resources/resources/read	Sí	Sí
Microsoft.Resources/subscripciones/operationResults/read	Sí	Sí
Microsoft.Resources/subscriptions/ResourceGroups/delete	Sí	No
Microsoft.Resources/subscriptions/ResourceGroups/read	Sí	Sí
Microsoft.Resources/subscripciones/resourcegroups/resources/read	Sí	Sí
Microsoft.Resources/subscriptions/ResourceGroups/write	Sí	No

Organización en niveles del cloud

El conector realiza las siguientes solicitudes de API al configurar Cloud Tiering.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/subscriptions/ResourceGroups/read
- Microsoft.Resources/suscripciones/ubicaciones/leer

El conector realiza las siguientes solicitudes API para operaciones diarias.

- Microsoft.Storage/storageAccounts/blobServices/contenedores/lectura
- Microsoft.Storage/storageAccounts/blobServices/contenedores/escritura
- Microsoft.Storage/storageAccounts/managementPolicies/Read
- Microsoft.Storage/storageAccounts/managementPolicies/Write
- Microsoft.Storage/storageAccounts/read

Cloud Volumes ONTAP

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

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Permite crear y gestionar máquinas virtuales	Microsoft.Compute/locations/operations/read	Sí	Sí	No
	Microsoft.Compute/locations/vmSizes/read	Sí	Sí	No
	Microsoft.Resources/suscripciones/ubicaciones/leer	Sí	No	No
	Microsoft.Compute/operations/read	Sí	Sí	No
	Microsoft.Compute/virtualMachines/instanceView/read	Sí	Sí	No
	Microsoft.Compute/virtualMachines/powerOff/action	Sí	Sí	No
	Microsoft.Compute/virtualMachines/read	Sí	Sí	No
	Microsoft.Compute/virtualMachines/restart/action	Sí	Sí	No
	Microsoft.Compute/virtualMachines/start/action	Sí	Sí	No
	Microsoft.Compute/virtualMachines/deallocate/action	No	Sí	Sí
	Microsoft.Compute/virtualMachines/vmSizes/read	No	Sí	No
	Microsoft.Compute/virtualMachines/write	Sí	Sí	No
	Microsoft.Compute/virtualMachines/delete	Sí	Sí	Sí
	Microsoft.Resources/despliegues/DELETE	Sí	No	No
Habilite la puesta en marcha desde un disco duro virtual	Microsoft.Compute/images/read	Sí	No	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Cree y gestione interfaces de red en la subred de destino	Microsoft.Network/networkInterfaces/read	Sí	Sí	No
	Microsoft.Network/networkInterfaces/write	Sí	Sí	No
	Microsoft.Network/networkInterfaces/join/action	Sí	Sí	No
	Microsoft.Network/networkInterfaces/delete	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/action	Sí	No	No
	Microsoft.Network/networkSecurityGroups/delete	No	Sí	Sí

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Obtenga información de la red acerca de las regiones, la red virtual de destino y la subred, y agregue las máquinas virtuales a los VNets	Microsoft.Network/locations/operationResults/read	Sí	Sí	No
	Microsoft.Network/locations/operations/read	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

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Cree y gestione grupos de recursos	Microsoft.Resources /despliegues/operaciones/lectura	Sí	Sí	No
	Microsoft.Resources /despliegues/leer	Sí	Sí	No
	Microsoft.Resources /implementaciones/escritura	Sí	Sí	No
	Microsoft.Resources /resources/read	Sí	Sí	No
	Microsoft.Resources /subscripciones/operationResults/read	Sí	Sí	No
	Microsoft.Resources /subscriptions/ResourceGroups/delete	Sí	Sí	Sí
	Microsoft.Resources /subscriptions/ResourceGroups/read	No	Sí	No
	Microsoft.Resources /subscripciones/resourcegroups/resources/read	Sí	Sí	No
	Microsoft.Resources /subscriptions/ResourceGroups/write	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Gestione cuentas de almacenamiento de Azure y discos	Microsoft.Compute/disks/read	Sí	Sí	Sí
	Microsoft.Compute/disks/write	Sí	Sí	No
	Microsoft.Compute/disks/delete	Sí	Sí	Sí
	Microsoft.Storage/checknameavailability/leer	Sí	Sí	No
	Microsoft.almacenamiento/operaciones/lectura	Sí	Sí	No
	Microsoft.Storage/storageAccounts/listkeys/action	Sí	Sí	No
	Microsoft.Storage/storageAccounts/read	Sí	Sí	No
	Microsoft.Storage/storageAccounts/DELETE	No	Sí	Sí
	Microsoft.Storage/storageAccounts/Write	Sí	Sí	No
	Microsoft.almacenamiento/usos/lectura	No	Sí	No
Permita los backups al almacenamiento BLOB y el cifrado de cuentas de almacenamiento	Microsoft.Storage/storageAccounts/blobServices/contenedores/lectura	Sí	Sí	No
	Microsoft.KeyVault/vaults/read	Sí	Sí	No
	Microsoft.KeyVault/vaults/accessPolicies/write	Sí	Sí	No
Habilite extremos de servicio vnet para la organización en niveles de los datos	Microsoft.Network/virtualNetworks/subnets/write	Sí	Sí	No
	Microsoft.Network/routeTables/join/action	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Cree y gestione copias Snapshot gestionadas de Azure	Microsoft.Compute/snapshots/write	Sí	Sí	No
	Microsoft.Compute/snapshots/read	Sí	Sí	No
	Microsoft.Compute/snapshots/delete	No	Sí	Sí
	Microsoft.Compute/disks/beginGetAccess/action	No	Sí	No
Crear y gestionar conjuntos de disponibilidad	Microsoft.Compute/availabilitySets/write	Sí	No	No
	Microsoft.Compute/availabilitySets/read	Sí	No	No
Permita puestas en marcha programáticas desde el mercado	Microsoft.MarketPlaceOrdenar/offertypes/editores/ofertas/planes/acuerdos/leer	Sí	No	No
	Microsoft.MarketPlaceOrdenar/offertypes/editores/ofertas/planes/acuerdos/escribir	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Gestione un equilibrador de carga para pares de ha	Microsoft.Network/loadBalancers/read	Sí	Sí	No
	Microsoft.Network/loadBalancers/write	Sí	No	No
	Microsoft.Network/loadBalancers/delete	No	Sí	Sí
	Microsoft.Network/loadBalancers/backendAddressPools/read	Sí	No	No
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Sí	No	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
Habilite la gestión de bloqueos en discos de Azure	Microsoft.Authorization/locks/*	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Habilite extremos 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/action	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/action	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, en función del hardware físico subyacente	Microsoft.Resources/despliegues/operationStatuses/read	Sí	Sí	No
Quite recursos de un grupo de recursos en caso de un error de implementación o de su eliminación	Microsoft.Network/privateEndpoints/delete	Sí	Sí	No
	Microsoft.Compute/availabilitySets/delete	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Habilite el uso de claves de cifrado gestionadas por el cliente al usar la API	Microsoft.Compute/diskEncryptionSets/read	Sí	Sí	Sí
	Microsoft.Compute/diskEncryptionSets/write	Sí	Sí	No
	Microsoft.KeyVault/vaults/Deploy/action	Sí	No	No
	Microsoft.Compute/diskEncryptionSets/delete	Sí	Sí	Sí
Configurar un grupo de seguridad de aplicaciones para un par de alta disponibilidad para aislar las NIC de interconexión de alta disponibilidad y de red de clúster	Microsoft.Network/applicationSecurityGroups/write	No	Sí	No
	Microsoft.Network/applicationSecurityGroups/read	No	Sí	No
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	No	Sí	No
	Microsoft.Network/networkSecurityGroups/securityRules/write	Sí	Sí	No
	Microsoft.Network/applicationSecurityGroups/delete	No	Sí	Sí
	Microsoft.Network/networkSecurityGroups/securityRules/delete	No	Sí	Sí
Lea, escriba y elimine las etiquetas asociadas a los recursos de Cloud Volumes ONTAP	Microsoft.Resources/etiquetas/leer	No	Sí	No
	Microsoft.Resources/etiquetas/escritura	Sí	Sí	No
	Microsoft.Resources/etiquetas/eliminar	Sí	No	No
Cifre cuentas de almacenamiento durante la creación	Microsoft.ManagedIdentity/userAssignedIdentities/ASSIGN/action	Sí	Sí	No

Caché de archivos global

El conector realiza las siguientes solicitudes API cuando utiliza la caché de archivos global:

- Microsoft.Insights/Metrics/Read
- Microsoft.Compute/virtualMachines/extensions/write
- Microsoft.Compute/virtualMachines/extensions/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/despliegues/DELETE

Kubernetes

El conector realiza las siguientes solicitudes de API para detectar y gestionar clústeres que se ejecutan en Azure Kubernetes Service (AKS):

- Microsoft.Compute/virtualMachines/read
- Microsoft.Resources/suscripciones/ubicaciones/leer
- Microsoft.Resources/subscripciones/operationResults/read
- Microsoft.Resources/subscriptions/ResourceGroups/read
- Microsoft.Resources/subscripciones/resourcegroups/resources/read
- Microsoft.ContainerService/managedClusters/read
- Microsoft.ContainerService/managedClusters/listClusterUserCredential/acción

Registro de cambios

A medida que se añadan y eliminen permisos, los anotaremos en las secciones siguientes.

5 de enero de 2023

Se han agregado los siguientes permisos a la política de JSON:

- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Synapse/spots/privateEndpointConnectionsApproval/action

  Estos permisos son necesarios para Cloud Backup.

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

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

1 de diciembre de 2022

Se han agregado los siguientes permisos a la política de JSON:

- Microsoft.Storage/storageAccounts/blobServices/contenedores/escritura

Este permiso es necesario para Cloud Backup y Cloud Tiering.

- Microsoft.Network/publicIPAddresses/delete

  Estos permisos son necesarios para Cloud Backup.

Se han eliminado los siguientes permisos de la política JSON porque ya no son necesarios:

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read
- Microsoft.Storage/storageAccounts/regeneratekey/acción

Permisos de Google Cloud para Connector

BlueXP requiere permisos para realizar acciones en Google Cloud. Estos permisos se incluyen en un rol personalizado que proporciona NetApp. Puede que desee entender lo que BlueXP hace con estos permisos.

Permisos de cuenta de servicio

La función personalizada que se muestra a continuación proporciona los permisos que un conector necesita para administrar recursos y procesos dentro de su red de Google Cloud.

Tendrá que aplicar esta función personalizada a una cuenta de servicio que se conecta a la máquina virtual del conector. "Vea las instrucciones paso a paso".

También debe asegurarse de que el rol esté actualizado a medida que se añadan nuevos permisos en versiones posteriores.

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- 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.globalOperations.get
- 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.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- 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
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
```

Cómo se utilizan los permisos de Google Cloud

Acciones	Específico
- Compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	Para crear y gestionar discos para Cloud Volumes ONTAP.
- computar.firewalls.create - compute.firewalls.delete - computar.firewalls.get - computar.firewalls.list	Para crear reglas de firewall para Cloud Volumes ONTAP.
- Compute.globalOperations.get	Para obtener el estado de las operaciones.
- compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	Para obtener imágenes para instancias de equipos virtuales.
- compute.instances.attachDisk - compute.instances.detachDisk	Para conectar y desconectar discos en Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Para crear y eliminar instancias de Cloud Volumes ONTAP VM.
- compute.instances.get	Para mostrar instancias de máquina virtual.
- compute.instances.getSerialPortOutput	Para obtener los registros de la consola.
- compute.instances.list	Para recuperar la lista de instancias de una zona.
- compute.instances.setDeletionProtection	Para establecer la protección de eliminación en la instancia.
- compute.instances.setLabels	Para agregar etiquetas.
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	Para cambiar el tipo de máquina para Cloud Volumes ONTAP.
- compute.instances.setMetadata	Para añadir metadatos.
- compute.instances.setTags	Para agregar etiquetas para reglas de firewall.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Para iniciar y detener Cloud Volumes ONTAP.
- computar.machineTypes.get	Para obtener el número de núcleos para comprobar qoutras.
- compute.projects.get	Para dar soporte a proyectos múltiples.
- Compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels	Para crear y gestionar instantáneas de disco persistentes.
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regises.list - compute.subnetworks.get - Compute.subNetworks.list - Compute.zoneOperations.get - Compute.zones.get - Compute.zones.list	Para obtener la información de red necesaria para crear una nueva instancia de máquina virtual de Cloud Volumes ONTAP.

Acciones	Específico
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifest.list - deploymentmanager.opers.get - deploymentmanager.opers.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.Types.get - deploymentmanager.types.list	Para poner en marcha la instancia de máquina virtual de Cloud Volumes ONTAP mediante Google Cloud Deployment Manager.
- logEntries.list - logging.privateLogEntries.list	Para obtener unidades de registro de pila.
- resourcemanager.projects.get	Para dar soporte a proyectos múltiples.
- storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update	Para crear y gestionar un bucket de Google Cloud Storage para la organización de datos en niveles.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudKMS.cryptoKeys.get - cloudKMS.cryptoKeys.list - cloudKMS.Keyring.list	Para utilizar claves de cifrado gestionadas por el cliente desde el Servicio de gestión de claves cloud con Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - Storage.objects.get - storage.objects.list	Para establecer una cuenta de servicio en la instancia de Cloud Volumes ONTAP. Esta cuenta de servicio proporciona permisos para organizar los datos en niveles en un bloque de Google Cloud Storage.
- compute.ads.list	Para recuperar las direcciones de una región cuando se implementa un par de alta disponibilidad.
- Computar.backendServices.create - compuso.regionBackendServices.create - compuso.regionBackendServices.get - computar.regionBackendServices.list	Para configurar un servicio back-end para distribuir el tráfico en un par de alta disponibilidad.
- compute.networks.updatePolicy	Para aplicar reglas de firewall en las PC y subredes para un par ha.
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	Para habilitar Cloud Data Sense.
- container.clusters.get - container.clusters.list	Para detectar los clústeres de Kubernetes que se ejecutan en Google Kubernetes Engine.
- compute.instanceGroups.get - computar.ads.get - compute.instances.updateNetworkInterface	Crear y gestionar máquinas virtuales de almacenamiento en pares de alta disponibilidad de Cloud Volumes ONTAP.

Acciones	Específico
- Monitoring.timeries.list - Storage.buckets.getIamPolicy	Para descubrir información sobre cubos de Google Cloud Storage.
- CloudKMS.criptocryKeys.get - cloudKMS.criptocryKeys.getIamPolicy - cloudKMS.criptoKeyKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudKMS.Keyring.get - cloudKMS.Keyring.getIamPolicy - cloudKMS.Keyring.list - cloudkms.keyRings.setIamPolicy	Para seleccionar sus propias claves gestionadas por el cliente en el asistente de activación de Cloud Backup en lugar de usar las claves de cifrado predeterminadas gestionadas por Google.

Registro de cambios

A medida que se añadan y eliminen permisos, los anotaremos en las secciones siguientes.

6 de febrero de 2023

Se ha agregado el siguiente permiso a esta directiva:

- compute.instances.updateNetworkInterface

Este permiso es obligatorio para Cloud Volumes ONTAP.

27 de enero de 2023

Se han agregado los siguientes permisos a la directiva:

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

Estos permisos son necesarios para Cloud Backup.