# Permessi

## Setup and administration

NetApp
April 26, 2024

# Sommario

# Permessi

## Riepilogo delle autorizzazioni per BlueXP

Per utilizzare le funzionalità e i servizi di BlueXP, è necessario fornire le autorizzazioni in modo che BlueXP possa eseguire le operazioni nell'ambiente cloud. Utilizzare i collegamenti presenti in questa pagina per accedere rapidamente alle autorizzazioni necessarie in base all'obiettivo.

### Autorizzazioni AWS

BlueXP richiede le autorizzazioni AWS per il connettore e per i singoli servizi.

#### Connettori

| Obiettivo | Descrizione | Collegamento |
|---|---|---|
| Implementa il connettore da BlueXP | L'utente che crea un connettore da BlueXP ha bisogno di autorizzazioni specifiche per implementare l'istanza in AWS. | "Impostare le autorizzazioni AWS" |
| Fornire le autorizzazioni per il connettore | Quando BlueXP avvia il connettore, allega un criterio all'istanza che fornisce le autorizzazioni necessarie per gestire le risorse e i processi nell'account AWS.<br><br>Devi impostare la policy da solo se avvii un connettore da AWS Marketplace, se installi manualmente il connettore o se vuoi "Aggiungere altre credenziali AWS a un connettore".<br><br>Inoltre, è necessario assicurarsi che il criterio sia aggiornato quando vengono aggiunte nuove autorizzazioni nelle release successive. | "Autorizzazioni AWS per il connettore" |

#### Backup e recovery

| Obiettivo | Descrizione | Collegamento |
|---|---|---|
| Eseguire il backup dei cluster ONTAP on-premise su Amazon S3 | Quando si attivano i backup sui volumi ONTAP, il backup e ripristino di BlueXP richiede di inserire una chiave di accesso e un segreto per un utente IAM che dispone di autorizzazioni specifiche. | "Impostare le autorizzazioni S3 per i backup" |

#### Cloud Volumes ONTAP

| Obiettivo | Descrizione | Collegamento |
|---|---|---|
| Fornire autorizzazioni per i nodi Cloud Volumes ONTAP | Un ruolo IAM deve essere associato a ciascun nodo Cloud Volumes ONTAP in AWS. Lo stesso vale per il mediatore ha. L'opzione predefinita è consentire a BlueXP di creare i ruoli IAM per te, ma puoi utilizzarne uno personalizzato durante la creazione dell'ambiente di lavoro. | "Scopri come impostare i ruoli IAM da solo" |

### Copia e sincronizzazione

| Obiettivo | Descrizione | Collegamento |
|---|---|---|
| Implementa il broker dei dati in AWS | L'account utente AWS utilizzato per implementare il broker di dati deve disporre di autorizzazioni specifiche. | "Autorizzazioni necessarie per implementare il data broker in AWS" |
| Fornire le autorizzazioni per il broker di dati | Quando BlueXP copia e sincronizza implementa il data broker, crea un ruolo IAM per l'istanza del data broker. Se preferisci, puoi implementare il data broker utilizzando il tuo ruolo IAM. | "Requisiti per utilizzare il tuo ruolo IAM con il broker dei dati AWS" |
| Abilitare l'accesso AWS per un broker dei dati installato manualmente | Se utilizzi il broker di dati con un rapporto di sincronizzazione che include un bucket S3, devi preparare l'host Linux per l'accesso ad AWS. Quando installi il broker di dati, dovrai fornire le chiavi AWS a un utente IAM che dispone di accesso programmatico e autorizzazioni specifiche. | "Abilitazione dell'accesso ad AWS" |

### FSX per ONTAP

| Obiettivo | Descrizione | Collegamento |
|---|---|---|
| Crea e gestisci FSX per ONTAP | Per creare o gestire un ambiente di lavoro Amazon FSX per NetApp ONTAP, devi aggiungere le credenziali AWS a BlueXP fornendo l'ARN di un ruolo IAM che conferisce ad BlueXP le autorizzazioni necessarie per creare l'ambiente di lavoro. | "Scopri come configurare le credenziali AWS per FSX" |

### Tiering

| Obiettivo | Descrizione | Collegamento |
|---|---|---|
| Eseguire il Tier dei cluster ONTAP on-premise su Amazon S3 | Quando si attiva il tiering BlueXP su AWS, la procedura guidata richiede di inserire una chiave di accesso e una chiave segreta. Queste credenziali vengono passate al cluster ONTAP in modo che ONTAP possa eseguire il Tier dei dati al bucket S3. | "Impostare le autorizzazioni S3 per il tiering" |

## Autorizzazioni Azure

BlueXP richiede le autorizzazioni di Azure per il connettore e per i singoli servizi.

### Connettori

| Obiettivo | Descrizione | Collegamento |
|---|---|---|
| Implementa il connettore da BlueXP | Quando si implementa un connettore da BlueXP, è necessario utilizzare un account Azure o un'entità di servizio che disponga delle autorizzazioni per implementare la macchina virtuale del connettore in Azure. | "Impostare le autorizzazioni Azure" |

| Obiettivo | Descrizione | Collegamento |
|---|---|---|
| Fornire le autorizzazioni per il connettore | Quando BlueXP implementa la macchina virtuale del connettore in Azure, crea un ruolo personalizzato che fornisce le autorizzazioni necessarie per gestire le risorse e i processi all'interno dell'abbonamento Azure.<br><br>È necessario impostare il ruolo personalizzato se si avvia un connettore dal mercato, se si installa manualmente il connettore o se si desidera "Aggiungere altre credenziali Azure a un connettore".<br><br>Inoltre, è necessario assicurarsi che il criterio sia aggiornato quando vengono aggiunte nuove autorizzazioni nelle release successive. | "Autorizzazioni Azure per il connettore" |

### Copia e sincronizzazione

| Obiettivo | Descrizione | Collegamento |
|---|---|---|
| Implementa il broker di dati in Azure | L'account utente Azure utilizzato per implementare il broker di dati deve disporre delle autorizzazioni richieste. | "Autorizzazioni necessarie per implementare il data broker in Azure" |

## Permessi Google Cloud

BlueXP richiede le autorizzazioni di Google Cloud per il connettore e per i singoli servizi.

### Connettori

| Obiettivo | Descrizione | Collegamento |
|---|---|---|
| Implementa il connettore da BlueXP | L'utente di Google Cloud che implementa un connettore di BlueXP ha bisogno di autorizzazioni specifiche per implementare il connettore in Google Cloud. | "Impostare le autorizzazioni per creare il connettore" |
| Fornire le autorizzazioni per il connettore | L'account di servizio per l'istanza di Connector VM deve disporre di autorizzazioni specifiche per le operazioni quotidiane. È necessario associare l'account del servizio al connettore durante la distribuzione.<br><br>Inoltre, è necessario assicurarsi che il criterio sia aggiornato quando vengono aggiunte nuove autorizzazioni nelle release successive. | "Impostare le autorizzazioni per il connettore" |

### Backup e recovery

| Obiettivo | Descrizione | Collegamento |
| --- | --- | --- |
| Eseguire il backup di Cloud Volumes ONTAP su Google Cloud | Quando si utilizza il backup e ripristino di BlueXP per eseguire il backup di Cloud Volumes ONTAP, è necessario aggiungere autorizzazioni al connettore nei seguenti scenari:<br>• Si desidera utilizzare la funzionalità di ricerca e ripristino<br>• Si desidera utilizzare le chiavi di crittografia gestite dal cliente (CMEK) | • "Permessi per la funzionalità di ricerca Restore"<br>• "Permessi per i CMEK" |
| Eseguire il backup dei cluster ONTAP on-premise su Google Cloud | Quando si utilizza il backup e ripristino di BlueXP per eseguire il backup dei cluster ONTAP on-premise, è necessario aggiungere le autorizzazioni al connettore per utilizzare la funzionalità di ricerca e ripristino. | "Permessi per la funzionalità di ricerca Restore" |

### Cloud Volumes Service per Google Cloud

| Obiettivo | Descrizione | Collegamento |
| --- | --- | --- |
| Scopri Cloud Volumes Service per Google Cloud | BlueXP deve accedere all'API di Cloud Volumes Service e disporre delle autorizzazioni necessarie tramite un account di servizio Google Cloud. | "Impostare un account di servizio" |

### Copia e sincronizzazione

| Obiettivo | Descrizione | Collegamento |
| --- | --- | --- |
| Implementa il broker dei dati in Google Cloud | Verifica che l'utente Google Cloud che implementa il broker di dati disponga delle autorizzazioni richieste. | "Autorizzazioni necessarie per implementare il data broker in Google Cloud" |
| Attiva l'accesso a Google Cloud per un broker dei dati installato manualmente | Se intendi utilizzare il data broker con una relazione di sincronizzazione che include un bucket di storage Google Cloud, devi preparare l'host Linux per l'accesso a Google Cloud. Quando si installa il data broker, è necessario fornire una chiave per un account di servizio che dispone di autorizzazioni specifiche. | "Abilitazione dell'accesso a Google Cloud" |

## Permessi StorageGRID

BlueXP richiede autorizzazioni StorageGRID per due servizi.

### Backup e recovery

| Obiettivo | Descrizione | Collegamento |
| --- | --- | --- |
| Eseguire il backup dei cluster ONTAP on-premise su StorageGRID | Quando si prepara StorageGRID come destinazione di backup per i cluster ONTAP, il backup e ripristino di BlueXP richiede di inserire una chiave di accesso e un segreto per un utente IAM che dispone di autorizzazioni specifiche. | "Preparare StorageGRID come destinazione del backup" |

**Tiering**

| Obiettivo | Descrizione | Collegamento |
|---|---|---|
| Eseguire il Tier dei cluster ONTAP on-premise in StorageGRID | Quando si imposta il tiering BlueXP su StorageGRID, è necessario fornire il tiering BlueXP con una chiave di accesso S3 e una chiave segreta. BlueXP Tiering utilizza le chiavi per accedere ai bucket. | "Preparare il tiering a StorageGRID" |

# Autorizzazioni AWS per il connettore

Quando BlueXP avvia l'istanza del connettore in AWS, allega un criterio all'istanza che fornisce al connettore le autorizzazioni per gestire le risorse e i processi all'interno di tale account AWS. Il connettore utilizza le autorizzazioni per effettuare chiamate API a diversi servizi AWS, tra cui EC2, S3, CloudFormation, IAM, Il servizio di gestione delle chiavi (KMS) e molto altro ancora.

## Policy IAM

Le policy IAM disponibili di seguito forniscono le autorizzazioni necessarie a un connettore per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico in base alla tua regione AWS.

Tenere presente quanto segue:

- Se si crea un connettore in una regione AWS standard direttamente da BlueXP, BlueXP applica automaticamente i criteri al connettore. In questo caso, non è necessario eseguire alcuna operazione.
- È necessario impostare autonomamente i criteri se si implementa il connettore da AWS Marketplace, se si installa manualmente il connettore su un host Linux o se si desidera aggiungere ulteriori credenziali AWS a BlueXP.
- Inoltre, è necessario assicurarsi che i criteri siano aggiornati quando vengono aggiunte nuove autorizzazioni nelle release successive.
- Se necessario, è possibile limitare le policy IAM utilizzando il modulo IAM `Condition` elemento. "Documentazione AWS: Elemento Condition"
- Per visualizzare istruzioni dettagliate sull'utilizzo di questi criteri, fare riferimento alle seguenti pagine:
  - "Impostare le autorizzazioni per un'implementazione di AWS Marketplace"
  - "Impostare le autorizzazioni per le implementazioni on-premise"
  - "Impostare le autorizzazioni per la modalità limitata"
  - "Impostare le autorizzazioni per la modalità privata"

Selezionare la propria regione per visualizzare le policy richieste:

**Regioni standard**

Per le regioni standard, le autorizzazioni sono distribuite in due policy. Sono necessarie due policy a causa di un limite massimo di dimensioni dei caratteri per le policy gestite in AWS.

Il primo criterio fornisce le autorizzazioni per i seguenti servizi:

- Discovery bucket Amazon S3
- Backup e recovery
- Classificazione
- Cloud Volumes ONTAP
- FSX per ONTAP
- Tiering

Il secondo criterio fornisce le autorizzazioni per i seguenti servizi:

- Caching edge
- Kubernetes

**Policy n. 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:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "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",
                "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"
        }
    ]
```

```
}
```

**Policy n. 2**

```
{
    "Version": "2012-10-17",
    "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"
        }
    ]
}
```

**Regioni di GovCloud (USA)**

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

**Regioni segrete**

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

**Regioni più segrete**

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

## Modalità di utilizzo delle autorizzazioni AWS

Le sezioni seguenti descrivono come utilizzare le autorizzazioni per ciascun servizio BlueXP. Queste informazioni possono essere utili se le policy aziendali impongono che le autorizzazioni vengano fornite solo se necessario.

### Amazon FSX per ONTAP

Il connettore effettua le seguenti richieste API per gestire Amazon FSX per ONTAP:

- ec2:DescripbeInstances
- ec2:DescripbeInstanceStatus
- ec2:DescripbeInstanceAttribute
- ec2:DescripteRouteTable
- ec2:DescripteImages
- ec2:CreateTag
- ec2:DescripteVolumes
- ec2:DescripteSecurityGroups
- ec2:DescripteNetworkInterfaces
- ec2:DescripteSubnet

- ec2:DescripteVpcs
- ec2:DescripbeDhcpOptions
- ec2:DescripteSnapshot
- ec2:DescripteKeyPairs
- ec2:DescripteRegions
- ec2:DescripteTag
- ec2:DescripteIamInstanceProfileAssociations
- ec2:DescripteReservedInstancesOfferings
- ec2:DescripteVpcEndpoint
- ec2:DescripteVpcs
- ec2:DescripteVolumesModificazioni
- ec2:DescriptePlacementGroups
- Km: Elenco*
- Km:descrivere*
- Km: CreateGrant
- Km:ListAlias
- fsx:descrivere*
- fsx: Elenco*

**Discovery bucket Amazon S3**

Il connettore effettua la seguente richiesta API per scoprire i bucket Amazon S3:

s3:GetEncryptionConfiguration

**Backup e recovery**

Il connettore effettua le seguenti richieste API per gestire i backup in Amazon S3:

- s3:GetBucketLocation
- s3:ListAllMyBucket
- s3:ListBucket
- s3:CreateBucket
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- Km: Elenco*
- Km:descrivere*

- s3:GetObject
- ec2:DescripteVpcEndpoint
- Km:ListAlias
- s3:PutEncryptionConfiguration

Il connettore effettua le seguenti richieste API quando si utilizza il metodo Search & Restore per ripristinare volumi e file:

- s3:CreateBucket
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMultipartUpload
- s3:ListMultipartUploadParts
- athena:StartQueryExecution
- athena: GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- Incolla: CreateDatabase
- Incolla: CreateTable
- Incolla: BatchDeletePartition

Il connettore esegue le seguenti richieste API quando si utilizza la protezione DataLock e ransomware per i backup dei volumi:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- 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:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Il connettore effettua le seguenti richieste API se si utilizza un account AWS diverso per i backup Cloud Volumes ONTAP rispetto a quello utilizzato per i volumi di origine:

- s3:PutBucketPolicy
- s3:PutBucketOwnershipControls

**Classificazione**

Il connettore effettua le seguenti richieste API per implementare l'istanza di classificazione BlueXP:

- ec2:DescripbeInstances
- ec2:DescripbeInstanceStatus
- ec2:RunInstances
- ec2:installazioni terminate
- ec2:CreateTag
- ec2:CreateVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2:DeleteSecurityGroup
- ec2:DescripteSecurityGroups
- ec2:CreateNetworkInterface

- ec2:DescripteNetworkInterfaces
- ec2:DeleteNetworkInterface
- ec2:DescripteSubnet
- ec2:DescripteVpcs
- ec2:CreateSnapshot
- ec2:DescripteRegions
- Cloud formation: CreateStack
- Cloud formation:DeleteStack
- Cloudformation:DescripteStack
- Cloudformation:DescripbeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescripteIamInstanceProfileAssociations

Il connettore effettua le seguenti richieste API per eseguire la scansione dei bucket S3 quando si utilizza la classificazione BlueXP:

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

**Cloud Volumes ONTAP**

Il connettore effettua le seguenti richieste API per implementare e gestire Cloud Volumes ONTAP in AWS.

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Creare e gestire i ruoli IAM e i profili di istanza per le istanze di Cloud Volumes ONTAP | iam:ListInstanceProfiles | Sì | Sì | No |
| | iam: CreateRole | Sì | No | No |
| | iam: DeleteRole | No | Sì | Sì |
| | iam:PutRolePolicy | Sì | No | No |
| | iam:CreateInstanceProfile | Sì | No | No |
| | iam:DeleteRolePolicy | No | Sì | Sì |
| | iam:AddRoleToInstanceProfile | Sì | No | No |
| | iam:RemoveRoleFromInstanceProfile | No | Sì | Sì |
| | iam:DeleteInstanceProfile | No | Sì | Sì |
| | iam: PassRole | Sì | No | No |
| | ec2:AssociateIamInstanceProfile | Sì | Sì | No |
| | ec2:DescripteIamInstanceProfileAssociations | Sì | Sì | No |
| | ec2:DisassociateIamInstanceProfile | No | Sì | No |
| Decodificare i messaggi di stato dell'autorizzazione | sts:DecodeAuthorizationMessage | Sì | Sì | No |
| Descrivere le immagini specificate (Amis) disponibili per l'account | ec2:DescripteImages | Sì | Sì | No |
| Descrivere le tabelle di percorso in un VPC (richiesto solo per le coppie ha) | ec2:DescripteRouteTable | Sì | No | No |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Arrestare, avviare e monitorare le istanze | ec2:StartInstances | Sì | Sì | No |
| | ec2:StopInstances | Sì | Sì | No |
| | ec2:DescripbeInstances | Sì | Sì | No |
| | ec2:DescripbeInstanceStatus | Sì | Sì | No |
| | ec2:RunInstances | Sì | No | No |
| | ec2:installazioni terminate | No | No | Sì |
| | ec2:ModifyInstanceAttribute | No | Sì | No |
| Verificare che la rete avanzata sia abilitata per i tipi di istanze supportati | ec2:DescripbeInstanceAttribute | No | Sì | No |
| Contrassegnare le risorse con i tag "WorkingEnvironment" e "WorkingEnvironmentId" utilizzati per la manutenzione e l'allocazione dei costi | ec2:CreateTag | Sì | Sì | No |
| Gestire i volumi EBS utilizzati da Cloud Volumes ONTAP come storage back-end | ec2:CreateVolume | Sì | Sì | No |
| | ec2:DescripteVolumes | Sì | Sì | Sì |
| | ec2:ModifyVolumeAttribute | No | Sì | Sì |
| | ec2:AttachVolume | Sì | Sì | No |
| | ec2:DeleteVolume | No | Sì | Sì |
| | ec2:DetachVolume | No | Sì | Sì |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Creare e gestire gruppi di sicurezza per Cloud Volumes ONTAP | ec2:CreateSecurityGroup | Sì | No | No |
| | ec2:DeleteSecurityGroup | No | Sì | Sì |
| | ec2:DescripteSecurityGroups | Sì | Sì | Sì |
| | ec2:RevokeSecurity GroupErgress | Sì | No | No |
| | ec2:AuthorizeSecurityGroupErgress | Sì | No | No |
| | ec2:AuthorizeSecurityGroupIngress | Sì | No | No |
| | ec2:RevokeSecurity GroupIngress | Sì | Sì | No |
| Creare e gestire le interfacce di rete per Cloud Volumes ONTAP nella subnet di destinazione | ec2:CreateNetworkInterface | Sì | No | No |
| | ec2:DescripteNetworkInterfaces | Sì | Sì | No |
| | ec2:DeleteNetworkInterface | No | Sì | Sì |
| | ec2:ModifyNetworkInterfaceAttribute | No | Sì | No |
| Ottenere l'elenco delle subnet di destinazione e dei gruppi di protezione | ec2:DescripteSubnet | Sì | Sì | No |
| | ec2:DescripteVpcs | Sì | Sì | No |
| Ottenere i server DNS e il nome di dominio predefinito per le istanze di Cloud Volumes ONTAP | ec2:DescripbeDhcpOptions | Sì | No | No |
| Snapshot dei volumi EBS per Cloud Volumes ONTAP | ec2:CreateSnapshot | Sì | Sì | No |
| | ec2:DeleteSnapshot | No | Sì | Sì |
| | ec2:DescripteSnapshot | No | Sì | No |
| Acquisire la console Cloud Volumes ONTAP, che è allegata ai messaggi AutoSupport | ec2:GetConsoleOutput | Sì | Sì | No |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Ottieni l'elenco delle coppie di chiavi disponibili | ec2:DescripteKeyPairs | Sì | No | No |
| Ottieni l'elenco delle regioni AWS disponibili | ec2:DescripteRegions | Sì | Sì | No |
| Gestire i tag per le risorse associate alle istanze di Cloud Volumes ONTAP | ec2:DeleteMags | No | Sì | Sì |
| | ec2:DescripteTag | No | Sì | No |
| Creare e gestire gli stack per i modelli di AWS CloudFormation | Cloud formation: CreateStack | Sì | No | No |
| | Cloud formation:DeleteStack | Sì | No | No |
| | Cloudformation:DescripteStack | Sì | Sì | No |
| | Cloudformation:DescripbeStackEvents | Sì | No | No |
| | Cloud formation:ValidateTemplate | Sì | No | No |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Creare e gestire un bucket S3 che un sistema Cloud Volumes ONTAP utilizza come Tier di capacità per il tiering dei dati | s3:CreateBucket | Sì | Sì | No |
| | s3:Deletebucket | No | Sì | Sì |
| | s3:GetLifecycleConfiguration | No | Sì | No |
| | s3:PutLifecycleConfiguration | No | Sì | No |
| | s3:PutBucketTagging | No | Sì | No |
| | s3:ListBucketVersions | No | Sì | No |
| | s3:GetBucketPolicyStatus | No | Sì | No |
| | s3:GetBucketPublicAccessBlock | No | Sì | No |
| | s3:GetBucketAcl | No | Sì | No |
| | s3:GetBucketPolicy | No | Sì | No |
| | s3:PutBucketPublicAccessBlock | No | Sì | No |
| | s3:GetBucketTagging | No | Sì | No |
| | s3:GetBucketLocation | No | Sì | No |
| | s3:ListAllMyBucket | No | No | No |
| | s3:ListBucket | No | Sì | No |
| Abilitare la crittografia dei dati di Cloud Volumes ONTAP utilizzando il servizio di gestione delle chiavi AWS (KMS) | Km: Elenco* | Sì | Sì | No |
| | Kms: ReEncrypt* | Sì | No | No |
| | Km:descrivere* | Sì | Sì | No |
| | Km: CreateGrant | Sì | Sì | No |
| | Kms:GenerateDataKeyWithoutPlaintext | Sì | Sì | No |
| Creare e gestire un gruppo di posizionamento AWS Spread per due nodi ha e il mediatore in una singola AWS Availability zone | ec2:CreatePlacementGroup | Sì | No | No |
| | ec2:DeletePlacementGroup | No | Sì | Sì |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Creare report | fsx:descrivere* | No | Sì | No |
| | fsx: Elenco* | No | Sì | No |
| Crea e gestisci aggregati che supportano la funzionalità Amazon EBS Elastic Volumes | ec2:DescripteVolumesModificazioni | No | Sì | No |
| | ec2:ModifyVolume | No | Sì | No |

#### Caching edge

Il connettore effettua le seguenti richieste API per implementare istanze di caching edge BlueXP durante l'implementazione:

- Cloudformation:DescripteStack
- Cloudwatch:GetMetricStatistics
- Cloudformation:ListStack

#### Kubernetes

Il connettore effettua le seguenti richieste API per rilevare e gestire i cluster Amazon EKS:

- ec2:DescripteRegions
- eks:ListClusters
- eks: DescripbeCluster
- iam:GetInstanceProfile

## Registro delle modifiche

Man mano che le autorizzazioni vengono aggiunte e rimosse, le annoteremo nelle sezioni seguenti.

#### 8 marzo 2024

La seguente autorizzazione è ora inclusa nel criterio del connettore:

EC2:DescribeAvailabilityZones

Questa autorizzazione è necessaria per una prossima release. Aggiorneremo le note di rilascio con ulteriori dettagli quando tale release sarà disponibile.

#### 6 giugno 2023

Per Cloud Volumes ONTAP è ora richiesta la seguente autorizzazione:

Kms:GenerateDataKeyWithoutPlaintext

**14 febbraio 2023**

Per il tiering BlueXP è ora richiesta la seguente autorizzazione:

ec2:DescripteVpcEndpoint

# Autorizzazioni Azure per il connettore

Quando BlueXP avvia la macchina virtuale del connettore in Azure, allega un ruolo personalizzato alla macchina virtuale che fornisce al connettore le autorizzazioni per gestire le risorse e i processi all'interno dell'abbonamento Azure. Il connettore utilizza le autorizzazioni per effettuare chiamate API a diversi servizi Azure.

## Autorizzazioni di ruolo personalizzate

Il ruolo personalizzato mostrato di seguito fornisce le autorizzazioni necessarie a un connettore per gestire le risorse e i processi all'interno della rete Azure.

Quando si crea un connettore direttamente da BlueXP, BlueXP applica automaticamente questo ruolo personalizzato al connettore.

Se si implementa il connettore da Azure Marketplace o se si installa manualmente il connettore su un host Linux, sarà necessario impostare autonomamente il ruolo personalizzato.

Per visualizzare istruzioni dettagliate sull'utilizzo di questi criteri, fare riferimento alle seguenti pagine:

- "Impostare le autorizzazioni per un'implementazione di Azure Marketplace"
- "Impostare le autorizzazioni per le implementazioni on-premise"
- "Impostare le autorizzazioni per la modalità limitata"
- "Impostare le autorizzazioni per la modalità privata"

Inoltre, è necessario assicurarsi che il ruolo sia aggiornato quando vengono aggiunte nuove autorizzazioni nelle release successive.

```
{
    "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/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.Synapse/workspaces/privateEndpointConnectionsApproval/action",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.Compute/images/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "BlueXP Permissions",
    "IsCustom": "true"
}
```

## Modalità di utilizzo delle autorizzazioni Azure

Le sezioni seguenti descrivono come utilizzare le autorizzazioni per ciascun servizio BlueXP. Queste informazioni possono essere utili se le policy aziendali impongono che le autorizzazioni vengano fornite solo se necessario.

### Azure NetApp Files

Il connettore esegue le seguenti richieste API quando si utilizza la classificazione BlueXP per eseguire la scansione dei dati 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 e recovery

Il connettore effettua le seguenti richieste API per il backup e ripristino BlueXP:

- Microsoft.Storage/storageAccounts/listkeys/azione
- Microsoft.Storage/storageAccounts/Read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/Containers/Read

- Microsoft.Storage/storageAccountSas/action
- Microsoft.KeyVault/vault/Read
- Microsoft.KeyVault/vault/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Resources/subscriptions/locations/Read
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Resources/subscriptions/resourceGroups/Read
- Microsoft.Resources/subscriptions/resourcegroup/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.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/Deployments/delete
- Microsoft.ManagedIdentity/userAssistedIdentities/assign/action

Il connettore effettua le seguenti richieste API quando si utilizza la funzionalità di ricerca e ripristino:

- Microsoft.Synapse/aree di lavoro/scrittura
- Microsoft.Synapse/aree di lavoro/lettura
- Microsoft.Synapse/aree di lavoro/eliminazione
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameAvailability/azione
- Microsoft.Synapse/workspaces/operationStatuses/Read
- Microsoft.Synapse/Workspaces/firewallRules/Read
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft.Synapse/workspaces/operationResults/Read
- Microsoft.Synapse/Workspaces/privateEndpointConnectionsApproval/action

### Classificazione

Il connettore crea le seguenti richieste API quando si utilizza la classificazione BlueXP.

| Azione | Utilizzato per la configurazione? | Utilizzato per le operazioni quotidiane? |
|---|---|---|
| Microsoft.Compute/locations/operations/read | Sì | Sì |
| Microsoft.Compute/locations/vmSizes/read | Sì | Sì |
| Microsoft.Compute/operations/read | Sì | Sì |
| Microsoft.Compute/virtualMachines/instanceView/read | Sì | Sì |
| Microsoft.Compute/virtualMachines/powerOff/action | Sì | No |
| Microsoft.Compute/virtualMachines/read | Sì | Sì |
| Microsoft.Compute/virtualMachines/restart/action | Sì | No |
| Microsoft.Compute/virtualMachines/start/action | Sì | No |
| Microsoft.Compute/virtualMachines/vmSizes/read | No | Sì |
| Microsoft.Compute/virtualMachines/write | Sì | No |
| Microsoft.Compute/images/read | Sì | Sì |
| Microsoft.Compute/disks/delete | Sì | No |
| Microsoft.Compute/disks/read | Sì | Sì |
| Microsoft.Compute/disks/write | Sì | No |
| Microsoft.Storage/checknameAvailability/Read | Sì | Sì |
| Microsoft.Storage/Operations/Read | Sì | Sì |
| Microsoft.Storage/storageAccounts/listkeys/azione | Sì | No |
| Microsoft.Storage/storageAccounts/Read | Sì | Sì |
| Microsoft.Storage/storageAccounts/write | Sì | No |
| Microsoft.Storage/storageAccounts/blobServices/Containers/Read | Sì | Sì |
| Microsoft.Network/networkInterfaces/read | Sì | Sì |
| Microsoft.Network/networkInterfaces/write | Sì | No |

| Azione | Utilizzato per la configurazione? | Utilizzato per le operazioni quotidiane? |
|---|---|---|
| Microsoft.Network/networkInterfaces/join/action | Sì | No |
| Microsoft.Network/networkSecurityGroups/read | Sì | Sì |
| Microsoft.Network/networkSecurityGroups/write | Sì | No |
| Microsoft.Resources/subscriptions/locations/Read | Sì | Sì |
| Microsoft.Network/locations/operationResults/read | Sì | Sì |
| Microsoft.Network/locations/operations/read | Sì | Sì |
| Microsoft.Network/virtualNetworks/read | Sì | Sì |
| Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read | Sì | Sì |
| Microsoft.Network/virtualNetworks/subnets/read | Sì | Sì |
| Microsoft.Network/virtualNetworks/subnets/virtualMachines/read | Sì | Sì |
| Microsoft.Network/virtualNetworks/virtualMachines/read | Sì | Sì |
| Microsoft.Network/virtualNetworks/subnets/join/action | Sì | No |
| Microsoft.Network/virtualNetworks/subnets/write | Sì | No |
| Microsoft.Network/routeTables/join/action | Sì | No |
| Microsoft.Resources/Deployments/Operations/Read | Sì | Sì |
| Microsoft.Resources/Deployments/Read | Sì | Sì |
| Microsoft.Resources/Deployments/write | Sì | No |
| Microsoft.Resources/resources/Read | Sì | Sì |
| Microsoft.Resources/subscriptions/operationresults/Read | Sì | Sì |
| Microsoft.Resources/subscriptions/resourceGroups/delete | Sì | No |

| Azione | Utilizzato per la configurazione? | Utilizzato per le operazioni quotidiane? |
|---|---|---|
| Microsoft.Resources/subscriptions/resourceGroups/Read | Sì | Sì |
| Microsoft.Resources/subscriptions/resourcegroup/resources/Read | Sì | Sì |
| Microsoft.Resources/subscriptions/resourceGroups/write | Sì | No |

**Cloud Volumes ONTAP**

Il connettore effettua le seguenti richieste API per implementare e gestire Cloud Volumes ONTAP in Azure.

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Creare e gestire macchine virtuali | Microsoft.Compute/locations/operations/read | Sì | Sì | No |
| | Microsoft.Compute/locations/vmSizes/read | Sì | Sì | No |
| | Microsoft.Resources/subscriptions/locations/Read | Sì | No | No |
| | Microsoft.Compute/operations/read | Sì | Sì | No |
| | Microsoft.Compute/virtualMachines/instanceView/read | Sì | Sì | No |
| | Microsoft.Compute/virtualMachines/powerOff/action | Sì | Sì | No |
| | Microsoft.Compute/virtualMachines/read | Sì | Sì | No |
| | Microsoft.Compute/virtualMachines/restart/action | Sì | Sì | No |
| | Microsoft.Compute/virtualMachines/start/action | Sì | Sì | No |
| | Microsoft.Compute/virtualMachines/deallocate/action | No | Sì | Sì |
| | Microsoft.Compute/virtualMachines/vmSizes/read | No | Sì | No |
| | Microsoft.Compute/virtualMachines/write | Sì | Sì | No |
| | Microsoft.Compute/virtualMachines/delete | Sì | Sì | Sì |
| | Microsoft.Resources/Deployments/delete | Sì | No | No |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Abilitare l'implementazione da un VHD | Microsoft.Compute/images/read | Sì | No | No |
| | Microsoft.Compute/images/write | Sì | No | No |
| Creare e gestire le interfacce di rete nella subnet di destinazione | Microsoft.Network/networkInterfaces/read | Sì | Sì | No |
| | Microsoft.Network/networkInterfaces/write | Sì | Sì | No |
| | Microsoft.Network/networkInterfaces/join/action | Sì | Sì | No |
| | Microsoft.Network/networkInterfaces/delete | Sì | Sì | No |
| Creare e gestire gruppi di sicurezza di rete | Microsoft.Network/networkSecurityGroups/read | Sì | Sì | No |
| | Microsoft.Network/networkSecurityGroups/write | Sì | Sì | No |
| | Microsoft.Network/networkSecurityGroups/join/action | Sì | No | No |
| | Microsoft.Network/networkSecurityGroups/delete | No | Sì | Sì |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Ottenere informazioni di rete relative alle regioni, al VNET di destinazione e alla subnet e aggiungere le macchine virtuali ai VNets | Microsoft.Network/locations/operationResults/read | Sì | Sì | No |
| | Microsoft.Network/locations/operations/read | Sì | Sì | No |
| | Microsoft.Network/virtualNetworks/read | Sì | No | No |
| | Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read | Sì | No | No |
| | Microsoft.Network/virtualNetworks/subnets/read | Sì | Sì | No |
| | Microsoft.Network/virtualNetworks/subnets/virtualMachines/read | Sì | Sì | No |
| | Microsoft.Network/virtualNetworks/virtualMachines/read | Sì | Sì | No |
| | Microsoft.Network/virtualNetworks/subnets/join/action | Sì | Sì | No |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Creare e gestire gruppi di risorse | Microsoft.Resources/Deployments/Operations/Read | Sì | Sì | No |
| | Microsoft.Resources/Deployments/Read | Sì | Sì | No |
| | Microsoft.Resources/Deployments/write | Sì | Sì | No |
| | Microsoft.Resources/resources/Read | Sì | Sì | No |
| | Microsoft.Resources/subscriptions/operationresults/Read | Sì | Sì | No |
| | Microsoft.Resources/subscriptions/resourceGroups/delete | Sì | Sì | Sì |
| | Microsoft.Resources/subscriptions/resourceGroups/Read | No | Sì | No |
| | Microsoft.Resources/subscriptions/resourcegroup/resources/Read | Sì | Sì | No |
| | Microsoft.Resources/subscriptions/resourceGroups/write | Sì | Sì | No |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Gestione di dischi e account storage Azure | Microsoft.Compute/disks/read | Sì | Sì | Sì |
| | Microsoft.Compute/disks/write | Sì | Sì | No |
| | Microsoft.Compute/disks/delete | Sì | Sì | Sì |
| | Microsoft.Storage/checknameAvailability/Read | Sì | Sì | No |
| | Microsoft.Storage/Operations/Read | Sì | Sì | No |
| | Microsoft.Storage/storageAccounts/listkeys/azione | Sì | Sì | No |
| | Microsoft.Storage/storageAccounts/Read | Sì | Sì | No |
| | Microsoft.Storage/storageAccounts/delete | No | Sì | Sì |
| | Microsoft.Storage/storageAccounts/write | Sì | Sì | No |
| | Microsoft.Storage/uses/Read | No | Sì | No |
| Abilitare i backup per lo storage Blob e la crittografia degli account di storage | Microsoft.Storage/storageAccounts/blobServices/Containers/Read | Sì | Sì | No |
| | Microsoft.KeyVault/vault/Read | Sì | Sì | No |
| | Microsoft.KeyVault/vault/accessPolicies/write | Sì | Sì | No |
| Abilitare gli endpoint del servizio VNET per il tiering dei dati | Microsoft.Network/virtualNetworks/subnets/write | Sì | Sì | No |
| | Microsoft.Network/routeTables/join/action | Sì | Sì | No |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Creare e gestire snapshot gestite da Azure | Microsoft.Compute/snapshots/write | Sì | Sì | No |
| | Microsoft.Compute/snapshots/read | Sì | Sì | No |
| | Microsoft.Compute/snapshots/delete | No | Sì | Sì |
| | Microsoft.Compute/disks/beginGetAccess/action | No | Sì | No |
| Creare e gestire set di disponibilità | Microsoft.Compute/availabilitySets/write | Sì | No | No |
| | Microsoft.Compute/availabilitySets/read | Sì | No | No |
| Implementazione programmatica dal mercato | Microsoft.MarketplaceOrdazione/offertypes/publisher/offers/plans/agreements/Read | Sì | No | No |
| | Microsoft.MarketplaceOrdazione/offertypes/publisher/offers/plans/agreements/write | Sì | Sì | No |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Gestire un bilanciamento del carico per le coppie ha | Microsoft.Network/loadBalancers/read | Sì | Sì | No |
| | Microsoft.Network/loadBalancers/write | Sì | No | No |
| | Microsoft.Network/loadBalancers/delete | No | Sì | Sì |
| | Microsoft.Network/loadBalancers/backendAddressPools/read | Sì | No | No |
| | Microsoft.Network/loadBalancers/backendAddressPools/join/action | Sì | No | No |
| | Microsoft.Network/loadBalancers/frontendIPConfigurations/read | Sì | Sì | No |
| | Microsoft.Network/loadBalancers/loadBalancingRules/read | Sì | No | No |
| | Microsoft.Network/loadBalancers/probes/read | Sì | No | No |
| | Microsoft.Network/loadBalancers/probes/join/action | Sì | No | No |
| Abilitare la gestione dei blocchi sui dischi Azure | Microsoft.Authorization/locks/* | Sì | Sì | No |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Abilitare gli endpoint privati per le coppie ha in assenza di connettività all'esterno della subnet | Microsoft.Network/privateEndpoints/write | Sì | Sì | No |
| | Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action | Sì | No | No |
| | Microsoft.Storage/storageAccounts/privateEndpointConnections/Read | Sì | Sì | Sì |
| | Microsoft.Network/privateEndpoints/read | Sì | Sì | Sì |
| | Microsoft.Network/privateDnsZones/write | Sì | Sì | No |
| | Microsoft.Network/privateDnsZones/virtualNetworkLinks/write | Sì | Sì | No |
| | Microsoft.Network/virtualNetworks/join/action | Sì | Sì | No |
| | Microsoft.Network/privateDnsZones/A/write | Sì | Sì | No |
| | Microsoft.Network/privateDnsZones/read | Sì | Sì | No |
| | Microsoft.Network/privateDnsZones/virtualNetworkLinks/read | Sì | Sì | No |
| Necessario per alcune implementazioni di macchine virtuali, a seconda dell'hardware fisico sottostante | Microsoft.Resources/Deployments/OperationStatuses/Read | Sì | Sì | No |
| Rimuovere le risorse da un gruppo di risorse in caso di errore di implementazione o di eliminazione | Microsoft.Network/privateEndpoints/delete | Sì | Sì | No |
| | Microsoft.Compute/availabilitySets/delete | Sì | Sì | No |

| Scopo | Azione | Utilizzato per l'implementazione? | Utilizzato per le operazioni quotidiane? | Utilizzato per l'eliminazione? |
|---|---|---|---|---|
| Abilitare l'utilizzo di chiavi di crittografia gestite dal cliente quando si utilizza l'API | Microsoft.Compute/diskEncryptionSets/read | Sì | Sì | Sì |
| | Microsoft.Compute/diskEncryptionSets/write | Sì | Sì | No |
| | Microsoft.KeyVault/vault/implementazione/azione | Sì | No | No |
| | Microsoft.Compute/diskEncryptionSets/delete | Sì | Sì | Sì |
| Configurare un gruppo di sicurezza dell'applicazione per una coppia ha per isolare le NIC di interconnessione ha e di rete del cluster | Microsoft.Network/applicationSecurityGroups/write | No | Sì | No |
| | Microsoft.Network/applicationSecurityGroups/read | No | Sì | No |
| | Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action | No | Sì | No |
| | Microsoft.Network/networkSecurityGroups/securityRules/write | Sì | Sì | No |
| | Microsoft.Network/applicationSecurityGroups/delete | No | Sì | Sì |
| | Microsoft.Network/networkSecurityGroups/securityRules/delete | No | Sì | Sì |
| Lettura, scrittura ed eliminazione dei tag associati alle risorse Cloud Volumes ONTAP | Microsoft.Resources/tags/Read | No | Sì | No |
| | Microsoft.Resources/tags/write | Sì | Sì | No |
| | Microsoft.Resources/tags/delete | Sì | No | No |
| Crittografare gli account storage durante la creazione | Microsoft.ManagedIdentity/userAssistedIdentities/assign/action | Sì | Sì | No |

### Caching edge

Il connettore effettua le seguenti richieste API quando si utilizza il caching edge BlueXP:

- Microsoft.Insights/metriche/lettura
- 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/Deployments/delete

### Kubernetes

Il connettore effettua le seguenti richieste API per rilevare e gestire i cluster in esecuzione in Azure Kubernetes Service (AKS):

- Microsoft.Compute/virtualMachines/read
- Microsoft.Resources/subscriptions/locations/Read
- Microsoft.Resources/subscriptions/operationresults/Read
- Microsoft.Resources/subscriptions/resourceGroups/Read
- Microsoft.Resources/subscriptions/resourcegroup/resources/Read
- Microsoft.ContainerService/managedClusters/Read
- Microsoft.ContainerService/managedClusters/listClusterUserCredential/action

### Tiering

Il connettore crea le seguenti richieste API quando si imposta il tiering BlueXP.

- Microsoft.Storage/storageAccounts/listkeys/azione
- Microsoft.Resources/subscriptions/resourceGroups/Read
- Microsoft.Resources/subscriptions/locations/Read

Il connettore esegue le seguenti richieste API per le operazioni quotidiane.

- Microsoft.Storage/storageAccounts/blobServices/Containers/Read
- Microsoft.Storage/storageAccounts/managementPolicies/Read
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Storage/storageAccounts/Read

## Registro delle modifiche

Man mano che le autorizzazioni vengono aggiunte e rimosse, le annoteremo nelle sezioni seguenti.

**5 dicembre 2023**

Le seguenti autorizzazioni non sono più necessarie per il backup e recovery di BlueXP durante il backup dei dati dei volumi nell'storage Azure Blob:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete

Queste autorizzazioni sono necessarie per altri servizi storage BlueXP, pertanto resteranno nel ruolo personalizzato del connettore se utilizzi tali servizi storage.

**12 maggio 2023**

Le seguenti autorizzazioni sono state aggiunte al criterio JSON perché sono necessarie per la gestione di Cloud Volumes ONTAP:

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read

Le seguenti autorizzazioni sono state rimosse dal criterio JSON perché non sono più necessarie:

- Microsoft.Storage/storageAccounts/blobServices/container/write
- Microsoft.Network/publicIPAddresses/delete

**23 marzo 2023**

L'autorizzazione "Microsoft.Storage/storageAccounts/delete" non è più necessaria per la classificazione BlueXP.

Questa autorizzazione è ancora richiesta per Cloud Volumes ONTAP.

**5 gennaio 2023**

Al criterio JSON sono state aggiunte le seguenti autorizzazioni:

- Microsoft.Storage/storageAccountSas/action
- Microsoft.Synapse/Workspaces/privateEndpointConnectionsApproval/action

  Queste autorizzazioni sono necessarie per il backup e il ripristino di BlueXP.

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

  Questa autorizzazione è necessaria per l'implementazione di Cloud Volumes ONTAP.

# Permessi Google Cloud per il connettore

BlueXP richiede autorizzazioni per eseguire azioni in Google Cloud. Queste

autorizzazioni sono incluse in un ruolo personalizzato fornito da NetApp. È possibile comprendere le funzioni di BlueXP con queste autorizzazioni.

## Autorizzazioni dell'account di servizio

Il ruolo personalizzato mostrato di seguito fornisce le autorizzazioni necessarie a un connettore per gestire le risorse e i processi all'interno della rete Google Cloud.

È necessario applicare questo ruolo personalizzato a un account di servizio che viene collegato alla macchina virtuale del connettore.

- "Impostare le autorizzazioni di Google Cloud per la modalità standard"
- "Impostare le autorizzazioni per la modalità limitata"
- "Impostare le autorizzazioni per la modalità privata"

Inoltre, è necessario assicurarsi che il ruolo sia aggiornato quando vengono aggiunte nuove autorizzazioni nelle release successive.

```
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
```

## Modalità di utilizzo delle autorizzazioni Google Cloud

| Azioni | Scopo |
|---|---|
| - compute.disks.create<br>- Compute.disks.createSnapshot<br>- compute.disks.delete<br>- compute.disks.get<br>- compute.disks.list<br>- compute.disks.setLabels<br>- compute.disks.use | Per creare e gestire dischi per Cloud Volumes ONTAP. |
| - compute.firewalls.create<br>- compute.firewalls.delete<br>- compute.firewalls.get<br>- compute.firewalls.list | Per creare regole firewall per Cloud Volumes ONTAP. |

| Azioni | Scopo |
| --- | --- |
| - Compute.globalOperations.get | Per ottenere lo stato delle operazioni. |
| - compute.images.get<br>- Compute.images.getFromFamily<br>- compute.images.list<br>- compute.images.useReadOnly | Per ottenere immagini per istanze di macchine virtuali. |
| - compute.instances.attachDisk<br>- compute.instances.detachDisk | Per collegare e scollegare i dischi a Cloud Volumes ONTAP. |
| - compute.instances.create<br>- compute.instances.delete | Per creare ed eliminare istanze di Cloud Volumes ONTAP VM. |
| - compute.instances.get | Per elencare le istanze di macchine virtuali. |
| - compute.instances.getSerialPortOutput | Per ottenere i log della console. |
| - compute.instances.list | Per recuperare l'elenco di istanze in una zona. |
| - compute.instances.setDeletionProtection | Per impostare la protezione di eliminazione sull'istanza. |
| - compute.instances.setLabels | Per aggiungere etichette. |
| - compute.instances.setMachineType<br>- compute.instances.setMinCpuPlatform | Per modificare il tipo di macchina per Cloud Volumes ONTAP. |
| - compute.instances.setMetadata | Per aggiungere metadati. |
| - compute.instances.setTags | Per aggiungere tag per le regole del firewall. |
| - compute.instances.start<br>- compute.instances.stop<br>- compute.instances.updateDisplayDevice | Per avviare e arrestare Cloud Volumes ONTAP. |
| - Compute.machineTypes.get | Per ottenere il numero di core per controllare le qoutas. |
| - compute.projects.get | Per supportare progetti multipli. |
| - compute.snapshot.create<br>- compute.snapshots.delete<br>- compute.snapshot.get<br>- compute.snapshot.list<br>- compute.snapshots.setLabels | Per creare e gestire snapshot di dischi persistenti. |
| - compute.networks.get<br>- compute.networks.list<br>- compute.regions.get<br>- compute.regions.list<br>- compute.subnetworks.get<br>- compute.subnetworks.list<br>- Compute.zoneOperations.get<br>- compute.zones.get<br>- compute.zones.list | Per ottenere le informazioni di rete necessarie per creare una nuova istanza di macchina virtuale Cloud Volumes ONTAP. |

| Azioni | Scopo |
| --- | --- |
| - deploymentmanager.compositeTypes.get<br>- deploymentmanager.compositeTypes.list<br>- deploymentmanager.deployments.create<br>- deploymentmanager.deployments.delete<br>- deploymentmanager.deployments.get<br>- deploymentmanager.deployments.list<br>- deploymentmanager.manifests.get<br>- deploymentmanager.manifests.list<br>- deploymentmanager.operations.get<br>- deploymentmanager.operations.list<br>- deploymentmanager.resources.get<br>- deploymentmanager.resources.list<br>- Deploymentmanager.typeProviders.get<br>- Deploymentmanager.typeProviders.list<br>- deploymentmanager.types.get<br>- deploymentmanager.types.list | Per implementare l'istanza della macchina virtuale Cloud Volumes ONTAP utilizzando Google Cloud Deployment Manager. |
| - Logging.logEntries.list<br>- Logging.privateLogEntries.list | Per ottenere unità di log stack. |
| - resourcemanager.projects.get | Per supportare progetti multipli. |
| - storage.bucket.create<br>- storage.buckets.delete<br>- storage.bucket.get<br>- storage.bucket.list<br>- storage.bucket.update | Per creare e gestire un bucket di storage Google Cloud per il tiering dei dati. |
| - cloudkms.cryptoKeyVersions.useToEncrypt<br>- Cloudkms.cryptKeys.get<br>- Cloudkms.cryptKeys.list<br>- Cloudkms.keyrings.list | Per utilizzare le chiavi di crittografia gestite dal cliente dal servizio di gestione delle chiavi cloud con Cloud Volumes ONTAP. |
| - compute.instances.setServiceAccount<br>- iam.serviceAccounts.actAs<br>- iam.serviceAccounts.getIamPolicy<br>- iam.serviceAccounts.list<br>- storage.objects.get<br>- storage.objects.list | Per impostare un account di servizio sull'istanza di Cloud Volumes ONTAP. Questo account di servizio fornisce le autorizzazioni per il tiering dei dati a un bucket di storage Google Cloud. |
| - compute.addresses.list | Recuperare gli indirizzi in una regione durante l'implementazione di una coppia ha. |
| - Compute.backendServices.create<br>- Compute.regionBackendServices.create<br>- Compute.regionBackendServices.get<br>- Compute.regionBackendServices.list | Per configurare un servizio back-end per la distribuzione del traffico in una coppia ha. |
| - compute.networks.updatePolicy | Per applicare le regole del firewall ai VPC e alle subnet per una coppia ha. |
| - compute.subnetworks.use<br>- compute.subnetworks.useExternalIp<br>- compute.instances.addAccessConfig | Per attivare la classificazione BlueXP. |

| Azioni | Scopo |
| --- | --- |
| - container.cluster.get<br>- container.cluster.list | Per scoprire i cluster Kubernetes in esecuzione in Google Kubernetes Engine. |
| - compute.instanceGroups.get<br>- compute.addresses.get<br>- compute.instances.updateNetworkInterface | Per creare e gestire le VM di storage su coppie Cloud Volumes ONTAP ha. |
| - Monitoring.timeseries.list<br>- Storage.bucket.getIamPolicy | Per scoprire informazioni sui bucket di storage di Google Cloud. |
| - Cloudkms.cryptKeys.get<br>- Cloudkms.cryptKeys.getIamPolicy<br>- Cloudkms.cryptKeys.list<br>- cloudkms.cryptoKeys.setIamPolicy<br>- Cloudkms.keyrings.get<br>- Cloudkms.keyrings.getIamPolicy<br>- Cloudkms.keyrings.list<br>- cloudkms.keyRings.setIamPolicy | Per selezionare le proprie chiavi gestite dal cliente nella procedura guidata di attivazione del backup e ripristino BlueXP invece di utilizzare le chiavi di crittografia predefinite gestite da Google. |

## Registro delle modifiche

Man mano che le autorizzazioni vengono aggiunte e rimosse, le annoteremo nelle sezioni seguenti.

### 6 febbraio 2023

La seguente autorizzazione è stata aggiunta a questo criterio:

- compute.instances.updateNetworkInterface

Questa autorizzazione è richiesta per Cloud Volumes ONTAP.

### 27 gennaio 2023

Al criterio sono state aggiunte le seguenti autorizzazioni:

- Cloudkms.cryptKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- Cloudkms.keyrings.get
- Cloudkms.keyrings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

Queste autorizzazioni sono necessarie per il backup e il ripristino di BlueXP.