Riferimento

NetApp Console setup and administration

NetApp
January 23, 2026

Sommario

Riferimento

Console di manutenzione dell’agente

Convalida dell’agente con la console di manutenzione

È possibile utilizzare la console di manutenzione dell’agente Console per convalidare l’installazione e la configurazione di un agente Console.

Accedi alla console di manutenzione dell’agente

È possibile accedere alla Console di manutenzione dall’host dell’agente della Console. Passare alla seguente directory:

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

verifica della configurazione convalida

IL `config-checker validate` Il comando consente di convalidare la configurazione di un agente Console.

Parametri

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

Scegli uno o più servizi da convalidare. I nomi di servizio validi sono:*`PLATFORM` che convalida la connettività di rete agli endpoint della console richiesti.

`--validationTypes <comma-separated list validation types to run>`**--OBBLIGATORIO--**
Scegliere uno o più tipi di convalida da eseguire. I tipi di convalida validi sono: * `NETWORK` che convalida la connettività di rete agli endpoint della console richiesti.

`--proxy <url>`**--OPZIONALE--**

Specifica l’URL del server proxy da utilizzare per la convalida. Obbligatorio se l’agente è configurato per utilizzare un server proxy.

`--certs <paths>`**--OPZIONALE--**

Specifica il percorso di uno o più file di certificato da utilizzare per la convalida. I file del certificato devono essere in formato PEM. Separare i percorsi multipli con virgole. Questo parametro è obbligatorio se l’agente utilizza un certificato personalizzato.

Esempi di convalida del controllo di configurazione

Validazione di base:

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

Convalida in cui viene utilizzato un server proxy per l'agente:

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

Convalida in cui viene utilizzato un certificato per l'agente:

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

Visualizza la guida per qualsiasi comando

Per visualizzare la guida per qualsiasi comando, aggiungi `--help` al comando. Ad esempio, per visualizzare la guida per `proxy add` comando, utilizzare il seguente comando:

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

Comandi proxy trasparenti

È possibile utilizzare la console di manutenzione dell'agente Console per configurare un agente Console in modo che utilizzi un server proxy trasparente.

Accedi alla console di manutenzione dell'agente

È possibile accedere alla Console di manutenzione dall'host dell'agente della Console. Passare alla seguente directory:

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

Visualizza la guida per qualsiasi comando

Per visualizzare la guida per qualsiasi comando, aggiungi `--help` al comando. Ad esempio, per visualizzare la guida per `proxy add` comando, utilizzare il seguente comando:

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

ottenere proxy

IL `proxy get` Il comando visualizza informazioni sulla configurazione corrente del server proxy trasparente. Per visualizzare la configurazione corrente del server proxy trasparente, utilizzare il seguente comando:

Esempio di proxy get

Per visualizzare la configurazione corrente del server proxy trasparente, utilizzare il seguente comando:

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

aggiunta proxy

IL `proxy add` Il comando configura l'agente per utilizzare un server proxy trasparente.

Parametri

`-c <certificate file>`

Specifica il percorso del file del certificato per il server proxy. Il file del certificato deve essere in formato PEM. Assicurarsi che il file del certificato si trovi nella stessa directory del comando oppure specificare il percorso completo del file del certificato.

Esempio di aggiunta proxy

Per aggiungere un server proxy trasparente, utilizzare il seguente comando, dove `/home/ubuntu/myCA1.pem` è il percorso al file del certificato per il server proxy. Il file del certificato deve essere in formato PEM:

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

aggiornamento proxy

IL `proxy update` Il comando consente di aggiornare il certificato di un proxy trasparente.

Parametri

`-c <certificate file>`specifica il percorso al file del certificato per il server proxy. Il file del certificato deve essere in formato PEM.

Assicurarsi che il file del certificato si trovi nella stessa directory del comando oppure specificare il percorso completo del file del certificato.

Esempio di aggiornamento proxy

Per aggiornare il certificato per un server proxy trasparente, utilizzare il seguente comando, dove `/home/ubuntu/myCA1.pem` è il percorso al nuovo file di certificato per il server proxy. Il file del certificato deve essere in formato PEM:

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

rimozione proxy

IL `proxy remove` Il comando rimuove la configurazione del server proxy trasparente dall'agente.

Esempio di rimozione del proxy

Per rimuovere il server proxy trasparente, utilizzare il seguente comando:

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

Autorizzazioni dell'agente del fornitore cloud e requisiti di rete

Riepilogo delle autorizzazioni per NetApp Console

Sarà necessario fornire all'agente della console le autorizzazioni appropriate affinché possa eseguire operazioni nel tuo ambiente cloud. Utilizza i link presenti in questa pagina per accedere rapidamente alle autorizzazioni di cui hai bisogno in base al tuo obiettivo.

Autorizzazioni AWS

La NetApp Console richiede le autorizzazioni AWS per un agente della console e per i singoli servizi.

Agenti della console

Obiettivo	Descrizione	Collegamento
Distribuire un agente Console dalla Console Per distribuire un agente Console in AWS, l'utente necessita di autorizzazioni specifiche.	"Imposta le autorizzazioni AWS"	Fornire autorizzazioni per un agente della console

NetApp Backup and Recovery

Obiettivo	Descrizione	Collegamento
Esegui il backup dei cluster ONTAP locali su Amazon S3 con NetApp Backup and Recovery	Quando si attivano i backup sui volumi ONTAP , NetApp Backup and Recovery richiede di immettere 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 quella di lasciare che la Console crei i ruoli IAM per te, ma puoi utilizzare i tuoi ruoli quando crei il sistema nella Console.	"Scopri come impostare autonomamente i ruoli IAM"

NetApp Copy and Sync

Obiettivo	Descrizione	Collegamento
Distribuisci il broker di dati in AWS	L'account utente AWS utilizzato per distribuire il broker di dati deve disporre delle autorizzazioni necessarie.	"Autorizzazioni necessarie per distribuire il broker di dati in AWS"
Fornire autorizzazioni per il broker di dati	Quando NetApp Copy and Sync distribuisce il broker di dati, crea un ruolo IAM per l'istanza del broker di dati. Se preferisci, puoi distribuire il data broker utilizzando il tuo ruolo IAM.	"Requisiti per utilizzare il proprio ruolo IAM con AWS Data Broker"
Abilitare l'accesso AWS per un broker di dati installato manualmente	Se si utilizza il broker di dati con una relazione di sincronizzazione che include un bucket S3, è necessario preparare l'host Linux per l'accesso ad AWS. Quando installi il broker di dati, dovrai fornire le chiavi AWS per 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 sistema Amazon FSx for NetApp ONTAP , è necessario aggiungere le credenziali AWS alla Console fornendo l'ARN di un ruolo IAM che fornisce alla Console le autorizzazioni necessarie.	"Scopri come configurare le credenziali AWS per FSx"

NetApp Cloud Tiering

Obiettivo	Descrizione	Collegamento
Cluster ONTAP locali di livello superiore su Amazon S3	Quando si abilita NetApp Cloud Tiering su AWS, si immette una chiave di accesso e una chiave segreta. Queste credenziali vengono trasmesse al cluster ONTAP in modo che ONTAP possa suddividere i dati nel bucket S3.	"Impostare le autorizzazioni S3 per la suddivisione in livelli"

Autorizzazioni di Azure

La console richiede le autorizzazioni di Azure per un agente della console e per i singoli servizi.

Agente console

Obiettivo	Descrizione	Collegamento
Distribuisci un agente Console dalla Console	Quando si distribuisce un agente Console dalla Console, è necessario utilizzare un account Azure o un'entità servizio che disponga delle autorizzazioni per distribuire una VM dell'agente Console in Azure.	"Configurare le autorizzazioni di Azure"
Fornire autorizzazioni per un agente della console	Quando la Console distribuisce una VM dell'agente Console in Azure, crea un ruolo personalizzato che fornisce le autorizzazioni necessarie per gestire risorse e processi all'interno di tale sottoscrizione di Azure. È necessario impostare autonomamente il ruolo personalizzato se si avvia un agente Console dal marketplace, se si installa manualmente un agente Console o se"aggiungere altre credenziali di Azure a un agente della console" . Mantenere aggiornata la policy man mano che nuove autorizzazioni vengono aggiunte nelle versioni successive.	"Autorizzazioni di Azure per un agente della console"

NetApp Backup and Recovery

Obiettivo	Descrizione	Collegamento
Backup Cloud Volumes ONTAP nell'archiviazione BLOB di Azure	Quando si utilizza NetApp Backup and Recovery per eseguire il backup Cloud Volumes ONTAP, è necessario aggiungere autorizzazioni a un agente Console nei seguenti scenari: • Vuoi utilizzare la funzionalità "Cerca e ripristina" • Vuoi utilizzare chiavi di crittografia gestite dal cliente (CMEK)	• "Esegui il backup dei dati Cloud Volumes ONTAP nell'archiviazione BLOB di Azure con Backup e ripristino"
Eseguire il backup dei cluster ONTAP locali nell'archiviazione BLOB di Azure	Quando si utilizza NetApp Backup and Recovery per eseguire il backup di cluster ONTAP locali, è necessario aggiungere autorizzazioni a un agente della console per utilizzare la funzionalità "Cerca e ripristina".	"Esegui il backup dei dati ONTAP locali nell'archiviazione BLOB di Azure con Backup e ripristino"

Copia e sincronizzazione NetApp

Obiettivo	Descrizione	Collegamento
Distribuire il broker di dati in Azure	L'account utente di Azure utilizzato per distribuire il broker di dati deve disporre delle autorizzazioni richieste.	"Autorizzazioni necessarie per distribuire il broker di dati in Azure"

Autorizzazioni di Google Cloud

La Console richiede le autorizzazioni di Google Cloud per un agente della Console e per i singoli servizi.

Agenti della console

Obiettivo	Descrizione	Collegamento
Distribuisci un agente Console dalla Console	L'utente di Google Cloud che distribuisce un agente Console dalla Console necessita di autorizzazioni specifiche per distribuire un agente Console in Google Cloud.	"Imposta le autorizzazioni per creare un agente Console"
Fornire autorizzazioni per un agente della console	L'account di servizio per un agente della console deve disporre di autorizzazioni specifiche per le operazioni quotidiane. Durante la distribuzione è necessario associare l'account di servizio a un agente della console. Mantenere aggiornata la policy man mano che nuove autorizzazioni vengono aggiunte nelle versioni successive.	"Impostare le autorizzazioni per un agente della console"

NetApp Backup and Recovery

Obiettivo	Descrizione	Collegamento
Esegui il backup Cloud Volumes ONTAP su Google Cloud	Quando si utilizza NetApp Backup and Recovery per eseguire il backup Cloud Volumes ONTAP, è necessario aggiungere autorizzazioni a un agente Console nei seguenti scenari: • Vuoi utilizzare la funzionalità "Cerca e ripristina" • Vuoi utilizzare chiavi di crittografia gestite dal cliente (CMEK)	• "Esegui il backup dei dati Cloud Volumes ONTAP su Google Cloud Storage con Backup e ripristino" • "Autorizzazioni per CMEK"
Eseguire il backup dei cluster ONTAP locali su Google Cloud	Quando si utilizza NetApp Backup and Recovery per eseguire il backup di cluster ONTAP locali, è necessario aggiungere autorizzazioni a un agente della console per utilizzare la funzionalità "Cerca e ripristina".	"Esegui il backup dei dati ONTAP locali su Google Cloud Storage con Backup e ripristino"

NetApp Copy and Sync

Obiettivo	Descrizione	Collegamento
Distribuisci il broker di dati in Google Cloud	Assicurarsi che l'utente di Google Cloud che distribuisce il broker di dati disponga delle autorizzazioni necessarie.	"Autorizzazioni necessarie per distribuire il broker di dati in Google Cloud"
Abilita l'accesso a Google Cloud per un broker di dati installato manualmente	Se si prevede di utilizzare il broker di dati con una relazione di sincronizzazione che include un bucket di Google Cloud Storage, è necessario preparare l'host Linux per l'accesso a Google Cloud. Quando installi il broker di dati, dovrai fornire una chiave per un account di servizio che abbia autorizzazioni specifiche.	"Abilitazione dell'accesso a Google Cloud"

Autorizzazioni StorageGRID

La console richiede le autorizzazioni StorageGRID per due servizi.

NetApp Backup and Recovery

Obiettivo	Descrizione	Collegamento
Eseguire il backup dei cluster ONTAP locali su StorageGRID	Quando si prepara StorageGRID come destinazione di backup per i cluster ONTAP , NetApp Backup and Recovery richiede di immettere una chiave di accesso e un segreto per un utente IAM che dispone di autorizzazioni specifiche.	"Prepara StorageGRID come destinazione di backup"

NetApp Cloud Tiering

Obiettivo	Descrizione	Collegamento
Suddivisione dei cluster ONTAP locali in livelli su StorageGRID	Quando si configura NetApp Cloud Tiering su StorageGRID, è necessario fornire a Cloud Tiering una chiave di accesso S3 e una chiave segreta. Il cloud tiering utilizza le chiavi per accedere ai bucket.	"Preparare il tiering per StorageGRID"

Autorizzazioni e regole di sicurezza dell'agente AWS

Autorizzazioni AWS per l'agente della console

Quando la NetApp Console avvia un agente della console in AWS, associa all'agente una policy che gli fornisce le autorizzazioni per gestire risorse e processi all'interno di quell'account AWS. L'agente utilizza le autorizzazioni per effettuare chiamate API a diversi servizi AWS, tra cui EC2, S3, CloudFormation, IAM, Key Management Service (KMS) e altri ancora.

Politiche IAM

Le policy IAM disponibili di seguito forniscono le autorizzazioni di cui un agente della console ha bisogno per gestire risorse e processi all'interno del tuo ambiente cloud pubblico in base alla tua regione AWS.

Notare quanto segue:

- Se si crea un agente della Console in una regione AWS standard direttamente dalla Console, la Console applica automaticamente le policy all'agente.
- È necessario impostare autonomamente le policy se si distribuisce l'agente da AWS Marketplace, se si installa manualmente l'agente su un host Linux o se si desidera aggiungere ulteriori credenziali AWS alla Console.
- In entrambi i casi, è necessario assicurarsi che i criteri siano aggiornati poiché nelle versioni successive verranno aggiunte nuove autorizzazioni. Se saranno necessarie nuove autorizzazioni, queste saranno elencate nelle note di rilascio.
- Se necessario, è possibile limitare i criteri IAM utilizzando IAM `Condition` elemento. "Documentazione AWS: Elemento Condizione"
- Per visualizzare le istruzioni dettagliate sull'utilizzo di queste policy, fare riferimento alle seguenti pagine:
  - "Impostare le autorizzazioni per una distribuzione AWS Marketplace"

- "Impostare le autorizzazioni per le distribuzioni in locale"
- "Imposta le autorizzazioni per la modalità limitata"

Seleziona la tua regione per visualizzare le policy richieste:

Regioni standard

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

Politica 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:ReEncrypt*",
        "kms:CreateGrant",
        "fsx:Describe*",
        "fsx:List*",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "cvoServicePolicy"
    },
    {
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:GetPartitions"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:CreateBucket",
```

```
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetObject",
        "s3:PutEncryptionConfiguration",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:DeleteBucket",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectRetention",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketVersioning",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketVersioning",
        "s3:BypassGovernanceRetention",
        "s3:PutBucketPolicy",
        "s3:PutBucketOwnershipControls"
      ],
      "Resource": [
        "arn:aws:s3:::netapp-backup-*"
      ],
      "Effect": "Allow",
      "Sid": "backupS3Policy"
    },
    {
      "Action": [
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
```

```
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketAcl",
            "s3:GetBucketPolicy",
            "s3:PutBucketPublicAccessBlock",
            "s3:DeleteBucket"
        ],
        "Resource": [
            "arn:aws:s3:::fabric-pool*"
        ],
        "Effect": "Allow",
        "Sid": "fabricPoolS3Policy"
    },
    {
        "Action": [
            "ec2:DescribeRegions"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "fabricPoolPolicy"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/netapp-adc-manager": "*"
            }
        },
        "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Effect": "Allow"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Action": [
            "ec2:StartInstances",
            "ec2:TerminateInstances",
```

```
            "ec2:AttachVolume",
            "ec2:DetachVolume",
            "ec2:StopInstances",
            "ec2:DeleteVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:volume/*"
        ],
        "Effect": "Allow"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Action": [
            "ec2:DeleteVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:volume/*"
        ],
        "Effect": "Allow"
    }
  ]
}
```

Politica n. 2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "tagServicePolicy"
    }
  ]
}
```

Regioni 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:ReEncrypt*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
```

```
            "s3:PutBucketPublicAccessBlock"
        ],
        "Resource": [
            "arn:aws-us-gov:s3:::fabric-pool*"
        ]
    },
    {
        "Sid": "backupPolicy",
        "Effect": "Allow",
        "Action": [
            "s3:DeleteBucket",
            "s3:GetLifecycleConfiguration",
            "s3:PutLifecycleConfiguration",
            "s3:PutBucketTagging",
            "s3:ListBucketVersions",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:ListAllMyBuckets",
            "s3:GetBucketTagging",
            "s3:GetBucketLocation",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketAcl",
            "s3:GetBucketPolicy",
            "s3:PutBucketPublicAccessBlock"
        ],
        "Resource": [
            "arn:aws-us-gov:s3:::netapp-backup-*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:StartInstances",
            "ec2:TerminateInstances",
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Resource": [
            "arn:aws-us-gov:ec2:*:*:instance/*"
        ]
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": [
        "arn:aws-us-gov:ec2:*:*:volume/*"
      ]
    }
  ]
}
```

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",
        "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 top secret

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
```

```
        "iam:PassRole",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListinstanceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
      ],
      "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
```

```
        ],
        "Condition": {
          "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
          }
        },
        "Resource": [
          "arn:aws-iso:ec2:*:*:instance/*"
        ]
      },
      {
        "Effect": "Allow",
        "Action": [
          "ec2:AttachVolume",
          "ec2:DetachVolume"
        ],
        "Resource": [
          "arn:aws-iso:ec2:*:*:volume/*"
        ]
      }
    ]
}
```

Come vengono utilizzate le autorizzazioni AWS

Le sezioni seguenti descrivono come vengono utilizzate le autorizzazioni per ogni servizio dati o di gestione NetApp Console . Queste informazioni possono essere utili se le politiche aziendali stabiliscono che le autorizzazioni vengano concesse solo se necessario.

Amazon FSx per ONTAP

L'agente della console effettua le seguenti richieste API per gestire un file system Amazon FSx for ONTAP :

- ec2:DescriviIstanze
- ec2:DescriviStatoIstanza
- ec2:Descriviattributoistanza
- ec2:DescriviRouteTables
- ec2:DescriviImmagini
- ec2:CreaTag
- ec2:DescriviVolumi
- ec2:Descrivi gruppi di sicurezza
- ec2:DescriviInterfacceDiRete
- ec2:Descrivi sottoreti
- ec2:DescriviVpcs

- ec2:DescriviDhcpOptions
- ec2:Descrivi istantanee
- ec2:Descrivi coppie di chiavi
- ec2:DescriviRegioni
- ec2:DescriviTag
- ec2:DescribeIamInstanceProfileAssociations
- ec2:Descrivi le offerte di istanze riservate
- ec2:DescriviVpcEndpoints
- ec2:DescriviVpcs
- ec2:DescribeVolumesModifications
- ec2:DescribePlacementGroups
- kms:CreateGrant
- kms:ListAliases
- fsx:Descrivi*
- fsx:Elenco*

Rilevamento del bucket Amazon S3

L'agente della console effettua la seguente richiesta API per individuare i bucket Amazon S3:

s3:Ottieni configurazione crittografia

NetApp Backup and Recovery

L'agente effettua le seguenti richieste API per gestire i backup in Amazon S3:

- s3:OttieniPosizioneBucket
- s3:ElencaTuttiIMieBucket
- s3:ElencoBucket
- s3:CreaBucket
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- s3:OttieniOggetto
- ec2:DescriviVpcEndpoints
- kms:ListAliases
- s3:PutEncryptionConfiguration

L'agente effettua le seguenti richieste API quando si utilizza il metodo Cerca e ripristina per ripristinare volumi

e file:

- s3:CreaBucket
- s3:EliminaOggetto
- s3:EliminaVersioneOggetto
- s3:GetBucketAcl
- s3:ElencoBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:AnnullaCaricamentoMultipart
- s3:ListMultipartUploadParts

L'agente effettua le seguenti richieste API quando si utilizzano DataLock e NetApp Ransomware Resilience per i backup dei volumi:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:EliminaOggetto
- s3:EliminaTaggingOggetto
- s3:OttieniRitenzioneOggetto
- s3:EliminaObjectVersionTagging
- s3:PutObject
- s3:OttieniOggetto
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:ListBucketByTags
- s3:OttieniTaggingBucket
- s3:EliminaVersioneOggetto
- s3:ListBucketVersions
- s3:ElencoBucket
- s3:PutBucketTagging
- s3:OttieniTaggingOggetto
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging

- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:OttieniPosizioneBucket
- s3:GetObjectVersion

L'agente effettua le seguenti richieste API se per i backup Cloud Volumes ONTAP utilizzi un account AWS diverso da quello utilizzato per i volumi di origine:

- s3:PoliticaPutBucket
- s3:PutBucketOwnershipControls

Autorizzazioni legacy per backup e ripristino

Sono necessarie solo le seguenti autorizzazioni se sono state abilitate le funzionalità di indicizzazione legacy prima del rilascio dell'indicizzazione v2:

- km:Elenco*
- km:Descrivi*
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- colla:CreaDatabase
- colla:CreaTabella
- colla:BatchDeletePartition

Classificazione

L'agente effettua le seguenti richieste API per distribuire NetApp Data Classification:

- ec2:DescriviIstanze
- ec2:DescriviStatoIstanza
- ec2:EseguiIstanze
- ec2:Termina le istanze
- ec2:CreaTag
- ec2:CreaVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2:EliminaGruppoDiSicurezza
- ec2:Descrivi gruppi di sicurezza
- ec2:CreateNetworkInterface

- ec2:DescriviInterfacceDiRete
- ec2:EliminaInterfacciaDiRete
- ec2:Descrivi sottoreti
- ec2:DescriviVpcs
- ec2:CreaSnapshot
- ec2:DescriviRegioni
- cloudformation:CreateStack
- cloudformation:EliminaStack
- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

L'agente effettua le seguenti richieste API per eseguire la scansione dei bucket S3 quando si utilizza NetApp Data Classification:

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations
- s3:OttieniTaggingBucket
- s3:OttieniPosizioneBucket
- s3:ElencaTuttiIMieBucket
- s3:ElencoBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:OttieniOggetto
- iam:GetRole
- s3:EliminaOggetto
- s3:EliminaVersioneOggetto
- s3:PutObject
- sts:AssumeRole

Cloud Volumes ONTAP

L'agente effettua le seguenti richieste API per distribuire e gestire Cloud Volumes ONTAP in AWS.

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Crea e gestisci ruoli IAM e profili di istanza per istanze Cloud Volumes ONTAP	iam:ListInstanceProfiles	SÌ	SÌ	NO
	iam:CreateRole	SÌ	NO	NO
	iam:EliminaRuolo	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:DescribeIamInstanceProfileAssociations	SÌ	SÌ	NO
	ec2:DisassociateIamInstanceProfile	NO	SÌ	NO
Decodifica i messaggi sullo stato di autorizzazione	sts:DecodeAuthorizationMessage	SÌ	SÌ	NO
Descrivi le immagini specificate (AMI) disponibili per l'account	ec2:DescriviImmagini	SÌ	SÌ	NO
Descrivere le tabelle di routing in una VPC (richiesto solo per le coppie HA)	ec2:DescriviRouteTables	SÌ	NO	NO

Scopo	Azione	Utilizzato per la distribuzione?	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:DescriviIstanze	SÌ	SÌ	NO
	ec2:DescriviStatoIstanza	SÌ	SÌ	NO
	ec2:EseguiIstanze	SÌ	NO	NO
	ec2:Termina le istanze	NO	NO	SÌ
	ec2:ModificaAttributoIstanza	NO	SÌ	NO
Verificare che la rete avanzata sia abilitata per i tipi di istanza supportati	ec2:Descriviattributoistanza	NO	SÌ	NO
Etichettare le risorse con i tag "WorkingEnvironment" e "WorkingEnvironmentId" che vengono utilizzati per la manutenzione e l'allocazione dei costi	ec2:CreaTag	SÌ	SÌ	NO
Gestire i volumi EBS che Cloud Volumes ONTAP utilizza come storage back-end	ec2:CreaVolume	SÌ	SÌ	NO
	ec2:DescriviVolumi	SÌ	SÌ	SÌ
	ec2:ModificaAttributoVolume	NO	SÌ	SÌ
	ec2:AttachVolume	SÌ	SÌ	NO
	ec2:EliminaVolume	NO	SÌ	SÌ
	ec2:DetachVolume	NO	SÌ	SÌ

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Crea e gestisci gruppi di sicurezza per Cloud Volumes ONTAP	ec2:CreateSecurityGroup	SÌ	NO	NO
	ec2:EliminaGruppoDiSicurezza	NO	SÌ	SÌ
	ec2:Descrivi gruppi di sicurezza	SÌ	SÌ	SÌ
	ec2:RevokeSecurityGroupEgress	SÌ	NO	NO
	ec2:AuthorizeSecurityGroupEgress	SÌ	NO	NO
	ec2:AuthorizeSecurityGroupIngress	SÌ	NO	NO
	ec2:RevokeSecurityGroupIngress	SÌ	SÌ	NO
Crea e gestisci le interfacce di rete per Cloud Volumes ONTAP nella subnet di destinazione	ec2:CreateNetworkInterface	SÌ	NO	NO
	ec2:DescriviInterfacceDiRete	SÌ	SÌ	NO
	ec2:EliminaInterfacciaDiRete	NO	SÌ	SÌ
	ec2:ModificaAttributoInterfacciaRete	NO	SÌ	NO
Ottieni l'elenco delle subnet di destinazione e dei gruppi di sicurezza	ec2:Descrivi sottoreti	SÌ	SÌ	NO
	ec2:DescriviVpcs	SÌ	SÌ	NO
Ottieni i server DNS e il nome di dominio predefinito per le istanze Cloud Volumes ONTAP	ec2:DescriviDhcpOptions	SÌ	NO	NO
Acquisisci snapshot dei volumi EBS per Cloud Volumes ONTAP	ec2:CreaSnapshot	SÌ	SÌ	NO
	ec2:EliminaSnapshot	NO	SÌ	SÌ
	ec2:Descrivi istantanee	NO	SÌ	NO
Acquisisci la console Cloud Volumes ONTAP , che è allegata ai messaggi AutoSupport	ec2:GetConsoleOutput	SÌ	SÌ	NO

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Ottieni l'elenco delle coppie di chiavi disponibili	ec2:Descrivi coppie di chiavi	SÌ	NO	NO
Ottieni l'elenco delle regioni AWS disponibili	ec2:DescriviRegioni	SÌ	SÌ	NO
Gestisci i tag per le risorse associate alle istanze Cloud Volumes ONTAP	ec2:EliminaTag	NO	SÌ	SÌ
	ec2:DescriviTag	NO	SÌ	NO
Crea e gestisci stack per i modelli AWS CloudFormation	cloudformation:CreateStack	SÌ	NO	NO
	cloudformation:EliminaStack	SÌ	NO	NO
	cloudformation:DescribeStacks	SÌ	SÌ	NO
	cloudformation:DescribeStackEvents	SÌ	NO	NO
	cloudformation:ValidateTemplate	SÌ	NO	NO

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Crea e gestisci un bucket S3 che un sistema Cloud Volumes ONTAP utilizza come livello di capacità per la suddivisione in livelli dei dati	s3:CreaBucket	SÌ	SÌ	NO
	s3:EliminaBucket	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:OttieniTaggingBucket	NO	SÌ	NO
	s3:OttieniPosizioneBucket	NO	SÌ	NO
	s3:ElencaTuttiIMieBucket	NO	NO	NO
	s3:ElencoBucket	NO	SÌ	NO
Abilita la crittografia dei dati di Cloud Volumes ONTAP utilizzando AWS Key Management Service (KMS)	kms:Ricrittografa*	SÌ	NO	NO
	kms:CreateGrant	SÌ	SÌ	NO
	kms:GenerateDataKeyWithoutPlaintext	SÌ	SÌ	NO
Crea e gestisci un gruppo di posizionamento diffuso AWS per due nodi HA e il mediatore in una singola zona di disponibilità AWS	ec2:CreatePlacementGroup	SÌ	NO	NO
	ec2:EliminaGruppoPosizionamento	NO	SÌ	SÌ

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Crea report	fsx:Descrivi*	NO	SÌ	NO
	fsx:Elenco*	NO	SÌ	NO
Crea e gestisci aggregati che supportano la funzionalità Amazon EBS Elastic Volumes	ec2:DescribeVolumesModifications	NO	SÌ	NO
	ec2:ModificaVolume	NO	SÌ	NO
Verifica se la zona di disponibilità è una zona locale AWS e convalida che tutti i parametri di distribuzione siano compatibili	ec2:Descrivi le zone di disponibilità	SÌ	NO	SÌ

Registro delle modifiche

Man mano che vengono aggiunte o rimosse autorizzazioni, ne daremo nota nelle sezioni seguenti.

11 novembre 2025

Le seguenti autorizzazioni non sono più necessarie per NetApp Backup and Recovery, a meno che non si utilizzi l'indicizzazione legacy. Queste autorizzazioni sono state rimosse dalle policy presenti in questa pagina:

- km:Elenco*
- km:Descrivi*
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- colla:CreaDatabase
- colla:CreaTabella
- colla:BatchDeletePartition

9 settembre 2024

Le autorizzazioni sono state rimosse dalla policy n. 2 per le regioni standard perché la NetApp Console non supporta più la memorizzazione nella cache edge NetApp e la scoperta e la gestione dei cluster Kubernetes.

Visualizza le autorizzazioni che sono state rimosse dalla policy

```
{
    "Action": [
        "ec2:DescribeRegions",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "iam:GetInstanceProfile"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "K8sServicePolicy"
},
{
    "Action": [
        "cloudformation:DescribeStacks",
        "cloudwatch:GetMetricStatistics",
        "cloudformation:ListStacks"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "GFCservicePolicy"
},
{
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/GFCInstance": "*"
        }
    },
    "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Effect": "Allow"
}
```

9 maggio 2024

Per Cloud Volumes ONTAP è ora richiesta la seguente autorizzazione:

ec2:Descrivi le zone di disponibilità

6 giugno 2023

Per Cloud Volumes ONTAP è ora richiesta la seguente autorizzazione:

kms:GenerateDataKeyWithoutPlaintext

14 febbraio 2023

Per NetApp Cloud Tiering è ora richiesta la seguente autorizzazione:

ec2:DescriviVpcEndpoints

Regole del gruppo di sicurezza dell'agente della console in AWS

Il gruppo di sicurezza AWS per l'agente richiede regole sia in entrata che in uscita. La NetApp Console crea automaticamente questo gruppo di sicurezza quando si crea un agente della console dalla console. È necessario impostare questo gruppo di sicurezza per tutte le altre opzioni di installazione.

Regole in entrata

Protocollo	Porta	Scopo
SSH	22	Fornisce accesso SSH all'host dell'agente
HTTP	80	• Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale • Utilizzato durante il processo di aggiornamento Cloud Volumes ONTAP
HTTPS	443	Fornisce accesso HTTPS all'interfaccia utente locale e connessioni dall'istanza di NetApp Data Classification
TCP	3128	Fornisce a Cloud Volumes ONTAP l'accesso a Internet. Dopo la distribuzione, è necessario aprire manualmente questa porta.

Regole in uscita

Il gruppo di sicurezza predefinito per l'agente apre tutto il traffico in uscita. Se ciò è accettabile, seguite le regole di base per le comunicazioni in uscita. Se hai bisogno di regole più rigide, usa le regole in uscita avanzate.

Regole di base in uscita

Il gruppo di sicurezza predefinito per l'agente include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutto TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole in uscita avanzate

Se hai bisogno di regole rigide per il traffico in uscita, puoi utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita da parte dell'agente

L'indirizzo IP di origine è l'host dell'agente.

Servizio	Protocollo	Porta	Destinazione	Scopo
Chiamate API e AutoSupport	HTTPS	443	Gestione cluster ONTAP e Internet in uscita LIF	Chiamate API ad AWS, a ONTAP, a NetApp Data Classification e invio di messaggi AutoSupport a NetApp
chiamate API	TCP	3000	Mediatore ONTAP HA	Comunicazione con il mediatore ONTAP HA
	TCP	8080	Classificazione dei dati	Sonda per l'istanza di classificazione dei dati durante la distribuzione
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte della console

Autorizzazioni di Azure e regole di sicurezza richieste

Autorizzazioni di Azure per l'agente della console

Quando la NetApp Console avvia un agente console in Azure, associa un ruolo personalizzato alla macchina virtuale che fornisce all'agente le autorizzazioni per gestire risorse e processi all'interno di tale sottoscrizione di Azure. L'agente utilizza le autorizzazioni per effettuare chiamate API a diversi servizi di Azure.

La necessità o meno di creare questo ruolo personalizzato per l'agente dipende da come lo hai distribuito.

Distribuzione dalla NetApp Console

Quando si utilizza la console per distribuire la macchina virtuale dell'agente in Azure, viene abilitato un "identità gestita assegnata dal sistema" sulla macchina virtuale, crea un ruolo personalizzato e lo assegna alla macchina virtuale. Il ruolo fornisce alla Console le autorizzazioni necessarie per gestire risorse e processi all'interno di tale sottoscrizione di Azure. Le autorizzazioni del ruolo vengono mantenute aggiornate quando l'agente viene aggiornato. Non è necessario creare questo ruolo per l'agente né gestire gli aggiornamenti.

Distribuzione manuale o da Azure Marketplace

Quando si distribuisce l'agente da Azure Marketplace o se si installa manualmente l'agente su un host Linux, è necessario configurare autonomamente il ruolo personalizzato e mantenerne le autorizzazioni con qualsiasi modifica.

Sarà necessario assicurarsi che il ruolo sia aggiornato poiché nelle versioni successive verranno aggiunte

nuove autorizzazioni. Se saranno necessarie nuove autorizzazioni, queste saranno elencate nelle note di rilascio.

- Per visualizzare le istruzioni dettagliate sull'utilizzo di queste policy, fare riferimento alle seguenti pagine:
  - "Impostare le autorizzazioni per una distribuzione di Azure Marketplace"
  - "Impostare le autorizzazioni per le distribuzioni in locale"
  - "Imposta le autorizzazioni per la modalità limitata"

```
{
  "Name": "Console Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/deallocate/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/images/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/write",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/resources/read",
```

```
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Storage/checknameavailability/read",
    "Microsoft.Storage/operations/read",
    "Microsoft.Storage/storageAccounts/listkeys/action",
    "Microsoft.Storage/storageAccounts/read",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Storage/storageAccounts/blobServices/containers/read",
    "Microsoft.Storage/storageAccounts/listAccountSas/action",
    "Microsoft.Storage/usages/read",
    "Microsoft.Compute/snapshots/write",
    "Microsoft.Compute/snapshots/read",
    "Microsoft.Compute/availabilitySets/write",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
    "Microsoft.Network/loadBalancers/read",
    "Microsoft.Network/loadBalancers/write",
    "Microsoft.Network/loadBalancers/delete",
    "Microsoft.Network/loadBalancers/backendAddressPools/read",
    "Microsoft.Network/loadBalancers/backendAddressPools/join/action",
    "Microsoft.Network/loadBalancers/loadBalancingRules/read",
    "Microsoft.Network/loadBalancers/probes/read",
    "Microsoft.Network/loadBalancers/probes/join/action",
    "Microsoft.Authorization/locks/*",
    "Microsoft.Network/routeTables/join/action",
    "Microsoft.NetApp/netAppAccounts/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",
    "Microsoft.Storage/storageAccounts/privateEndpointConnections/read",
    "Microsoft.Storage/storageAccounts/managementPolicies/read",
```

```
    "Microsoft.Storage/storageAccounts/managementPolicies/write",
    "Microsoft.Network/privateEndpoints/read",
    "Microsoft.Network/privateDnsZones/write",
    "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
    "Microsoft.Network/virtualNetworks/join/action",
    "Microsoft.Network/privateDnsZones/A/write",
    "Microsoft.Network/privateDnsZones/read",
    "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Insights/Metrics/Read",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/delete",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Compute/diskEncryptionSets/read",
    "Microsoft.Compute/snapshots/delete",
    "Microsoft.Network/privateEndpoints/delete",
    "Microsoft.Compute/availabilitySets/delete",
    "Microsoft.KeyVault/vaults/read",
    "Microsoft.KeyVault/vaults/accessPolicies/write",
    "Microsoft.Compute/diskEncryptionSets/write",
    "Microsoft.KeyVault/vaults/deploy/action",
    "Microsoft.Compute/diskEncryptionSets/delete",
    "Microsoft.Resources/tags/read",
    "Microsoft.Resources/tags/write",
    "Microsoft.Resources/tags/delete",
    "Microsoft.Network/applicationSecurityGroups/write",
    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/applicationSecurityGroups/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Synapse/workspaces/write",
    "Microsoft.Synapse/workspaces/read",
    "Microsoft.Synapse/workspaces/delete",
    "Microsoft.Synapse/register/action",
    "Microsoft.Synapse/checkNameAvailability/action",
    "Microsoft.Synapse/workspaces/operationStatuses/read",
    "Microsoft.Synapse/workspaces/firewallRules/read",
    "Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
    "Microsoft.Synapse/workspaces/operationResults/read",
```

```
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",
    "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
    "Microsoft.Compute/images/write",
    "Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
    "Microsoft.Compute/virtualMachineScaleSets/write",
    "Microsoft.Compute/virtualMachineScaleSets/read",
    "Microsoft.Compute/virtualMachineScaleSets/delete"
  ],
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Console Permissions",
  "IsCustom": "true"
}
```

Come vengono utilizzate le autorizzazioni di Azure

Le sezioni seguenti descrivono come vengono utilizzate le autorizzazioni per ciascun sistema di storage e servizio dati NetApp . Queste informazioni possono essere utili se le politiche aziendali stabiliscono che le autorizzazioni vengano concesse solo se necessario.

Azure NetApp Files

L'agente effettua le seguenti richieste API quando si utilizza NetApp Data Classification per analizzare i dati di Azure NetApp Files :

- Microsoft. NetApp/netAppAccounts/lettura
- Microsoft. NetApp/netAppAccounts/capacityPools/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/delete

NetApp Backup and Recovery

Le sezioni seguenti descrivono come vengono utilizzate le autorizzazioni per NetApp Backup and Recovery.

Autorizzazioni minime NetApp Backup and Recovery

L'agente Console effettua le seguenti richieste API per le funzionalità di base NetApp Backup and Recovery :

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/lettura
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Resources/subscriptions/resourceGroups/read

- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Autorizzazione/blocchi/scrittura
- Microsoft.Authorization/locks/read

Di seguito è riportato un criterio personalizzato per Backup e Ripristino che utilizza il minor numero possibile di autorizzazioni e l'ambito più ristretto possibile:

```
{
  "id":
"/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/roleDef
initions/{roleDefinitionGuid}",
  "properties": {
    "roleName": "Custom Role",
    "description": "Minimal permissions required for Backup and
Recovery.",
    "assignableScopes": [
      "/subscriptions/{subscriptionId}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}/providers/Microsoft.Storage/storageAccounts/
{storageAccountNameWithObjectLockPreprovisioned}"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/storageAccounts/listkeys/action",
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
          "Microsoft.Storage/storageAccounts/listAccountSas/action",
          "Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
          "Microsoft.Resources/subscriptions/resourceGroups/write",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/write",
          "Microsoft.Authorization/locks/write",
          "Microsoft.Authorization/locks/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

Autorizzazioni avanzate di backup e ripristino

L'agente della console effettua le seguenti richieste API per operazioni avanzate di backup e ripristino e funzionalità di ricerca e ripristino. Queste autorizzazioni consentono la gestione della rete, degli archivi di chiavi e delle identità gestite:

- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.KeyVault/vaults/read
- Microsoft.ManagedIdentity/userAssignedIdentities/assign/action
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkInterfaces/read
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/write
- Microsoft.Network/privateEndpoints/lettura
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Resources/deployments/delete

Autorizzazioni legacy per backup e ripristino

L'agente effettua le seguenti richieste API quando si utilizza la funzionalità Cerca e ripristina. Queste autorizzazioni sono necessarie solo se hai abilitato le funzionalità di indicizzazione legacy prima del rilascio dell'indicizzazione v2 a febbraio 2025:

- 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

NetApp Data Classification

L'agente effettua le seguenti richieste API quando si utilizza la classificazione dei dati.

Azione	Utilizzato per l'installazione?	Utilizzato per le operazioni quotidiane?
Microsoft.Compute/locations/operations/read	SÌ	SÌ

Azione	Utilizzato per l'installazione?	Utilizzato per le operazioni quotidiane?
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/dischi/elimina	SÌ	NO
Microsoft.Compute/dischi/lettura	SÌ	SÌ
Microsoft.Compute/dischi/scrittura	SÌ	NO
Microsoft.Storage/checknameavailability/read	SÌ	SÌ
Microsoft.Storage/operations/read	SÌ	SÌ
Microsoft.Storage/storageAccounts/listkeys/action	SÌ	NO
Microsoft.Storage/storageAccounts/lettura	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
Microsoft.Network/networkInterfaces/join/action	SÌ	NO

Azione	Utilizzato per l'installazione?	Utilizzato per le operazioni quotidiane?
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
Microsoft.Resources/subscriptions/resourceGroups/read	SÌ	SÌ

Azione	Utilizzato per l'installazione?	Utilizzato per le operazioni quotidiane?
Microsoft.Resources/subscriptions/resourcegroups/resources/read	SÌ	SÌ
Microsoft.Resources/subscriptions/resourceGroups/write	SÌ	NO

Cloud Volumes ONTAP

L'agente effettua le seguenti richieste API per distribuire e gestire Cloud Volumes ONTAP in Azure.

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Creare e gestire VM	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 la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Abilita la distribuzione da un VHD	Microsoft.Compute/images/read	SÌ	NO	NO
	Microsoft.Compute/images/write	SÌ	NO	NO
Crea e gestisci 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 la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Ottieni informazioni di rete sulle regioni, sulla VNet di destinazione e sulla subnet e aggiungi le VM alle VNet	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 la distribuzione?	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/resourcegroups/resources/read	SÌ	SÌ	NO
	Microsoft.Resources /subscriptions/resourceGroups/write	SÌ	SÌ	NO

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Gestire gli account di archiviazione e i dischi di Azure	Microsoft.Compute/dischi/lettura	SÌ	SÌ	SÌ
	Microsoft.Compute/dischi/scrittura	SÌ	SÌ	NO
	Microsoft.Compute/dischi/elimina	SÌ	SÌ	SÌ
	Microsoft.Storage/checknameavailability/read	SÌ	SÌ	NO
	Microsoft.Storage/operations/read	SÌ	SÌ	NO
	Microsoft.Storage/storageAccounts/listkeys/action	SÌ	SÌ	NO
	Microsoft.Storage/storageAccounts/lettura	SÌ	SÌ	NO
	Microsoft.Storage/storageAccounts/delete	NO	SÌ	SÌ
	Microsoft.Storage/storageAccounts/write	SÌ	SÌ	NO
	Microsoft.Storage/usages/read	NO	SÌ	NO
Abilita i backup nell'archiviazione BLOB e la crittografia degli account di archiviazione	Microsoft.Storage/storageAccounts/blobServices/containers/read	SÌ	SÌ	NO
	Microsoft.KeyVault/vaults/read	SÌ	SÌ	NO
	Microsoft.KeyVault/vaults/accessPolicies/write	SÌ	SÌ	NO
Abilita gli endpoint del servizio VNet per la suddivisione in livelli dei dati	Microsoft.Network/virtualNetworks/subnets/write	SÌ	SÌ	NO
	Microsoft.Network/routeTables/join/action	SÌ	SÌ	NO

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Crea e gestisci snapshot gestiti da Azure	Microsoft.Compute/snapshot/write	SÌ	SÌ	NO
	Microsoft.Compute/snapshot/lettura	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
Abilitare le distribuzioni programmatiche dal marketplace	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read	SÌ	NO	NO
	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	SÌ	SÌ	NO

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Gestire un bilanciatore del carico per 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/lettura	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
Abilita la gestione dei blocchi sui dischi di Azure	Microsoft.Authorization/locks/*	SÌ	SÌ	NO

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Abilita endpoint privati per coppie HA quando non c'è connettività al di fuori 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/lettura	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
Richiesto per alcune distribuzioni di VM, 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 distribuzione o eliminazione	Microsoft.Network/privateEndpoints/delete	SÌ	SÌ	NO
	Microsoft.Compute/availabilitySets/delete	SÌ	SÌ	NO

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Abilita l'uso 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/vaults/deploy/action	SÌ	NO	NO
	Microsoft.Compute/diskEncryptionSets/delete	SÌ	SÌ	SÌ
Configurare un gruppo di sicurezza delle applicazioni per una coppia HA per isolare l'interconnessione HA e le schede di rete del cluster	Microsoft.Network/applicationSecurityGroups/write	NO	SÌ	NO
	Microsoft.Network/applicationSecurityGroups/lettura	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
Leggere, scrivere ed eliminare i 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 di archiviazione durante la creazione	Microsoft.ManagedIdentity/userAssignedIdentities/assign/action	SÌ	SÌ	NO

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Utilizzare i set di scalabilità delle macchine virtuali in modalità di orchestrazione flessibile per specificare zone specifiche per Cloud Volumes ONTAP	Microsoft.Compute/virtualMachineScaleSets/write	SÌ	NO	NO
	Microsoft.Compute/virtualMachineScaleSets/read	SÌ	NO	NO
	Microsoft.Compute/virtualMachineScaleSets/delete	NO	NO	SÌ

Livelli

L'agente effettua le seguenti richieste API quando si configura NetApp Cloud Tiering.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/locations/read

L'agente Console effettua 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/lettura

Registro delle modifiche

Man mano che vengono aggiunte o rimosse autorizzazioni, ne daremo nota nelle sezioni seguenti.

11 novembre 2025

È stata aggiunta una policy JSON personalizzata che riflette il minor numero possibile di autorizzazioni e l'ambito più ristretto possibile.

Le seguenti autorizzazioni sono state aggiunte all'elenco minimo delle autorizzazioni di backup e ripristino:

- Microsoft.Autorizzazione/blocchi/scrittura
- Microsoft.Authorization/locks/read

Le seguenti autorizzazioni non sono più necessarie per Backup e Ripristino, a meno che non si utilizzi l'indicizzazione legacy:

- 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

Le seguenti autorizzazioni sono state spostate nella sezione "Autorizzazioni aggiuntive per backup e ripristino" perché non sono necessarie per una configurazione minima:

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/lettura
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write

9 settembre 2024

Le seguenti autorizzazioni sono state rimosse dalla policy JSON perché la Console non supporta più l'individuazione e la gestione dei cluster Kubernetes:

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/action
- Microsoft.ContainerService/managedClusters/read

22 agosto 2024

Le seguenti autorizzazioni sono state aggiunte alla policy JSON perché sono necessarie per il supporto Cloud Volumes ONTAP dei set di scalabilità delle macchine virtuali:

- Microsoft.Compute/virtualMachineScaleSets/write
- Microsoft.Compute/virtualMachineScaleSets/read
- Microsoft.Compute/virtualMachineScaleSets/delete

5 dicembre 2023

Le seguenti autorizzazioni non sono più necessarie per NetApp Backup and Recovery quando si esegue il backup dei dati del volume nell'archiviazione BLOB di Azure:

- 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 di archiviazione della console, pertanto rimarranno comunque nel ruolo personalizzato per l'agente se si utilizzano tali altri servizi di archiviazione.

12 maggio 2023

Le seguenti autorizzazioni sono state aggiunte alla policy JSON perché sono necessarie per la gestione Cloud Volumes ONTAP :

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

Le seguenti autorizzazioni sono state rimosse dalla policy JSON perché non sono più necessarie:

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

23 marzo 2023

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

Questa autorizzazione è ancora necessaria per Cloud Volumes ONTAP.

5 gennaio 2023

Sono state aggiunte le seguenti autorizzazioni alla policy JSON:

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

  Queste autorizzazioni sono necessarie per NetApp Backup and Recovery.

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

  Questa autorizzazione è necessaria per la distribuzione Cloud Volumes ONTAP .

Regole del gruppo di sicurezza dell'agente della console in Azure

Il gruppo di sicurezza di Azure per l'agente richiede regole sia in ingresso che in uscita. La NetApp Console crea automaticamente questo gruppo di sicurezza quando si crea un agente della console dalla console. Per altre opzioni di installazione, è necessario impostare manualmente questo gruppo di sicurezza.

Regole in entrata

Protocollo	Porta	Scopo
SSH	22	Fornisce accesso SSH all'host dell'agente
HTTP	80	• Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale • Utilizzato durante il processo di aggiornamento Cloud Volumes ONTAP
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale e connessioni dall'istanza NetApp Data Classification
TCP	3128	Fornisce a Cloud Volumes ONTAP l'accesso a Internet per inviare messaggi AutoSupport al supporto NetApp . Dopo la distribuzione, è necessario aprire manualmente questa porta. "Scopri come l'agente viene utilizzato come proxy per i messaggi AutoSupport"

Regole in uscita

Il gruppo di sicurezza predefinito per l'agente apre tutto il traffico in uscita. Se ciò è accettabile, seguite le regole di base per le comunicazioni in uscita. Se hai bisogno di regole più rigide, usa le regole in uscita avanzate.

Regole di base in uscita

Il gruppo di sicurezza predefinito per l'agente include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutto TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole in uscita avanzate

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita da parte dell'agente.

L'indirizzo IP di origine è l'host dell'agente.

Servizio	Protocollo	Porta	Destinazione	Scopo
Chiamate API e AutoSupport	HTTPS	443	Gestione cluster ONTAP e Internet in uscita LIF	Chiamate API ad Azure, a ONTAP, a NetApp Data Classification e invio di messaggi AutoSupport a NetApp
chiamate API	TCP	8080	Classificazione dei dati	Sonda per l'istanza di classificazione dei dati durante la distribuzione
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte della console

Autorizzazioni di Google Cloud e regole del firewall richieste

Autorizzazioni di Google Cloud per l'agente della console

L'agente della console necessita delle autorizzazioni per eseguire azioni in Google Cloud. Queste autorizzazioni sono incluse in un ruolo personalizzato fornito da NetApp. Dovresti capire cosa fa l'agente con queste autorizzazioni.

Autorizzazioni dell'account utente di Google Cloud

Il ruolo personalizzato riportato di seguito fornisce a un utente Google Cloud le autorizzazioni necessarie per distribuire un agente. Applica questo ruolo personalizzato all'utente che distribuirà l'agente.

Visualizza le autorizzazioni dell'account utente di Google Cloud

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

Autorizzazioni dell'account di servizio

Il ruolo personalizzato riportato di seguito fornisce all'account del servizio Google Cloud associato all'agente della console le autorizzazioni necessarie per gestire risorse e processi nella rete Google Cloud.

Applica questo ruolo personalizzato a un account di servizio collegato alla VM dell'agente Console.

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

Visualizza le autorizzazioni dell'account di servizio Google

Assicurarsi che il ruolo sia aggiornato poiché nuove autorizzazioni vengono aggiunte o rimosse nelle versioni successive. Il registro delle modifiche elenca tutte le nuove autorizzazioni richieste."Esamina il registro delle modifiche alle autorizzazioni di Google" "Scopri come aggiungere account di servizi Google Cloud"

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent.
stage: GA
includedPermissions:
- cloudbuild.builds.get
- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken
- cloudbuild.repositories.list
- cloudquotas.quotas.get
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
- config.artifacts.import
- config.deployments.create
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getLock
- config.deployments.getState
- config.deployments.update
- config.deployments.updateState
- config.previews.upload
- config.revisions.get
- config.revisions.getState
- config.deployments.getLock
- config.deployments.list
- config.deployments.lock
- config.operations.get
- config.previews.get
- config.previews.list
- config.resources.list
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.regionBackendServices.update
- compute.networks.updatePolicy
```

```
- compute.addresses.createInternal
- compute.addresses.deleteInternal
- compute.addresses.list
- compute.addresses.setLabels
- compute.addresses.useInternal
- compute.backendServices.create
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels
- compute.globalOperations.get
- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
```

```
- compute.instances.use
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.get
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.instances.setMinCpuPlatform
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.regionBackendServices.delete
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
```

```
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- logging.logEntries.create
- logging.logEntries.route
- monitoring.timeSeries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- storage.objects.create
- storage.objects.delete
- storage.objects.list
- storage.objects.update
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.get
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.objects.get
- storage.objects.list
- storage.buckets.getIamPolicy
```

Come vengono utilizzate le autorizzazioni di Google Cloud

L'agente Console utilizza le autorizzazioni nel ruolo personalizzato per gestire le risorse Cloud Volumes ONTAP e i processi dei servizi dati NetApp nella rete Google Cloud. Le sezioni seguenti descrivono come l'agente utilizza queste autorizzazioni.

Autorizzazioni utilizzate per Cloud Volumes ONTAP

L'agente Console utilizza le autorizzazioni nel ruolo personalizzato per gestire le risorse e i processi Cloud Volumes ONTAP nella rete Google Cloud. Le sezioni seguenti descrivono come l'agente utilizza queste autorizzazioni.

Autorizzazioni per Cloud Volumes ONTAP

Azioni	Scopo	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
config.deployments.create	Per distribuire l'istanza della macchina virtuale Cloud Volumes ONTAP utilizzando Google Cloud Infrastructure Manager.	SÌ	NO	NO
config.deployments.delete		NO	NO	SÌ
config.deployments.deleteState		NO	NO	SÌ
config.deployments.get		NO	SÌ	NO
config.deployments.getLock		NO	SÌ	NO
config.deployments.getState		NO	SÌ	NO
config.deployments.list		NO	SÌ	NO
configurazione.distribuzioni.blocco		NO	SÌ	NO
config.deployments.update		NO	SÌ	NO
config.deployments.updateState		NO	SÌ	NO
config.operations.get		NO	SÌ	NO
config.previews.get		NO	SÌ	NO
config.anteprime.elenco		NO	SÌ	NO
elenco risorse di configurazione		NO	SÌ	NO
config.revisions.get		NO	SÌ	NO

Azioni	Scopo	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
calcola.dischi.crea	Per creare e gestire dischi per Cloud Volumes ONTAP.	SÌ	SÌ	NO
calcola.dischi.creaSnapshot		NO	SÌ	NO
calcola.dischi.elimina		NO	SÌ	SÌ
compute.disks.get		NO	SÌ	NO
elenco.dischi.di calcolo		SÌ	SÌ	NO
calcola.dischi.imposta etichette		SÌ	SÌ	NO
calcolo.dischi.uso		NO	SÌ	NO
calcola.firewall.crea	Per creare regole firewall per Cloud Volumes ONTAP.	SÌ	NO	NO
calcola.firewall.elimina		NO	SÌ	SÌ
calcola.firewall.ottieni		SÌ	SÌ	NO
elenco.firewall.di.calcolo		SÌ	SÌ	NO
calcola.regolediinoltro.crea	Creare regole di inoltro per l'instradamento del traffico verso i servizi backend.	NO	SÌ	NO
calcola.regolediinoltro.elimina	Elimina le regole di inoltro esistenti.	NO	SÌ	NO
calcola.regolediinoltro.ottieni	Recupera i dettagli sulle regole di inoltro esistenti.	NO	SÌ	NO
calcola.regolediinoltro.impostaetichette	Imposta o aggiorna le etichette sulle regole di inoltro per l'organizzazione.	NO	SÌ	NO
compute.globalOperations.get	Per conoscere lo stato delle operazioni.	SÌ	SÌ	NO

Azioni	Scopo	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
calcola.controlli.salute.crea	Crea e gestisci controlli di integrità per monitorare lo stato di salute del servizio backend.	NO	SÌ	NO
compute.healthChecks.delete		NO	SÌ	NO
compute.healthChecks.get		NO	SÌ	NO
compute.healthChecks.useReadOnly		NO	SÌ	NO
calcola.immagini.ottieni	Per ottenere immagini per istanze VM.	SÌ	NO	NO
calcola.immagini.getFromFamily		SÌ	NO	NO
calcola.elenco.immagini		SÌ	NO	NO
calcola.immagini.usasola lettura		SÌ	NO	NO
calcola.istanze.attachDisk	Per collegare e scollegare i dischi a Cloud Volumes ONTAP.	SÌ	SÌ	NO
calcola.istanze.staccaDisco		NO	SÌ	SÌ
calcola.istanze.crea	Per creare ed eliminare istanze VM Cloud Volumes ONTAP .	SÌ	NO	NO
calcola.istanze.elimina		NO	NO	SÌ
calcola.istanze.ottieni	Per elencare le istanze VM.	SÌ	SÌ	NO
calcola.istanze.getSerialPortOutput	Per ottenere i log della console.	SÌ	SÌ	NO
elenco.istanze.di.calcolo	Per recuperare l'elenco delle istanze in una zona.	SÌ	SÌ	NO
compute.instances.setDeletionProtection	Per impostare la protezione dall'eliminazione sull'istanza.	SÌ	NO	NO
calcola.istanze.imposta etichette	Per aggiungere etichette.	SÌ	NO	NO

Azioni	Scopo	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
calcola.istanze.impostatipomacchina	Per modificare il tipo di macchina per Cloud Volumes ONTAP.	SÌ	SÌ	NO
calcola.istanze.impostaMinCpuPlatform		SÌ	SÌ	NO
calcola.istanze.impostaMetadati	Per aggiungere metadati.	SÌ	SÌ	NO
calcola.istanze.impostaTag	Per aggiungere tag per le regole del firewall.	SÌ	SÌ	NO
calcola.istanze.avvio	Per avviare e arrestare Cloud Volumes ONTAP.	SÌ	SÌ	NO
calcola.istanze.arresto		SÌ	SÌ	NO
calcola.istanze.aggiorna.dispositivo di visualizzazione		SÌ	SÌ	NO
calcola.istanze.uso	Utilizzare istanze di macchine virtuali (operazioni di avvio, arresto e connessione).	NO	SÌ	NO
calcola.tipimacchina.ottieni	Per ottenere il numero di core per controllare le quote.	SÌ	NO	NO
calcola.progetti.ottieni	Per supportare progetti multipli.	SÌ	NO	NO
calcola.risorsePolitiche.crea	Crea e gestisci policy sulle risorse per la gestione automatizzata delle risorse.	NO	SÌ	NO
compute.resourcePolicies.delete		NO	SÌ	NO
compute.resourcePolicies.get		NO	SÌ	NO

Azioni	Scopo	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
calcola.istantanee.crea	Per creare e gestire snapshot persistenti del disco.	SÌ	SÌ	NO
calcola.istantanee.elimina		NO	SÌ	SÌ
calcola.istantanee.ottieni		NO	SÌ	NO
elenco di istantanee di calcolo		NO	SÌ	NO
calcola.istantanee.imposta etichette		SÌ	SÌ	NO
compute.networks.get	Per ottenere le informazioni di rete necessarie per creare una nuova istanza di macchina virtuale Cloud Volumes ONTAP .	SÌ	SÌ	NO
elenco.reti.di.calcolo		SÌ	SÌ	NO
calcola.regioni.ottieni		SÌ	SÌ	NO
calcola.elenco.regioni		SÌ	SÌ	NO
calcola.sottoreti.ottenere		SÌ	SÌ	NO
elenco.sottoreti.di.calcolo		SÌ	SÌ	NO
compute.zoneOperations.get		SÌ	SÌ	NO
calcola.zone.get		SÌ	SÌ	NO
elenco.zone.di.calcolo		SÌ	SÌ	NO

Azioni	Scopo	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
deploymentmanager.compositeTypes.get	Per distribuire l'istanza della macchina virtuale Cloud Volumes ONTAP utilizzando Google Cloud Deployment Manager.	SÌ	NO	NO
deploymentmanager.compositeTypes.list		SÌ	NO	NO
deploymentmanager.deployments.create		SÌ	NO	NO
deploymentmanager.deployments.delete		SÌ	NO	NO
deploymentmanager.deployments.get		SÌ	NO	NO
gestoredistribuzioni.elencodistribuzioni		SÌ	NO	NO
deploymentmanager.manifests.get		SÌ	NO	NO
deploymentmanager.manifests.list		SÌ	NO	NO
deploymentmanager.operations.get		SÌ	NO	NO
gestoredistribuzioni.elencooperazioni		SÌ	NO	NO
deploymentmanager.resources.get		SÌ	NO	NO
elenco risorse del gestore di distribuzione		SÌ	NO	NO
deploymentmanager.typeProviders.get		SÌ	NO	NO
deploymentmanager.typeProviders.list		SÌ	NO	NO
deploymentmanager.types.get		SÌ	NO	NO
elenco dei tipi di deploymentmanager		SÌ	NO	NO

Azioni	Scopo	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
logging.logEntries.list	Per ottenere unità di registro dello stack.	SÌ	SÌ	NO
logging.privateLogEntries.list		SÌ	SÌ	NO
registrazione.logEntries.create	Crea e instrada voci di registro per il monitoraggio, il debug e l'audit.	SÌ	SÌ	NO
registrazione.logEntries.route		SÌ	SÌ	NO
resourcemanager.projects.get	Per supportare progetti multipli.	SÌ	SÌ	NO
storage.buckets.create	Per creare e gestire un bucket di Google Cloud Storage per la suddivisione in livelli dei dati.	SÌ	SÌ	NO
storage.buckets.delete		NO	SÌ	SÌ
storage.buckets.get		NO	SÌ	NO
elenco.secchi.di.archiviazione		NO	SÌ	NO
aggiornamento.storage.buckets		NO	SÌ	NO
cloudkms.cryptoKeyVersions.useToEncrypt	Per utilizzare le chiavi di crittografia gestite dal cliente dal Cloud Key Management Service con Cloud Volumes ONTAP.	SÌ	SÌ	NO
cloudkms.cryptoKeys.get		SÌ	SÌ	NO
cloudkms.cryptoKeys.list		SÌ	SÌ	NO
cloudkms.keyRings.list		SÌ	SÌ	NO
cloudbuild.builds.get		SÌ	NO	NO

Azioni	Scopo	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
calcola.istanze.impostaAccountServizio	Per impostare un account di servizio sull'istanza Cloud Volumes ONTAP . Questo account di servizio fornisce le autorizzazioni per il tiering dei dati in un bucket di Google Cloud Storage.	SÌ	SÌ	NO
iam.serviceAccounts.actAs		SÌ	NO	NO
iam.serviceAccounts.create		SÌ	NO	NO
iam.serviceAccounts.getIamPolicy		SÌ	SÌ	NO
iam.serviceAccounts.list		SÌ	SÌ	NO
iam.serviceAccountKeys.create		SÌ	NO	NO
archiviazione.oggetti.crea	Crea e gestisci oggetti (file) nel bucket di Google Cloud Storage.	SÌ	SÌ	NO
archiviazione.oggetti.elimina		NO	NO	SÌ
storage.objects.get		SÌ	SÌ	NO
elenco.oggetti.di.archiviazione		SÌ	SÌ	NO
calcola.elenco.indirizzi	Per recuperare gli indirizzi in una regione durante la distribuzione di una coppia HA.	SÌ	NO	NO
calcola.indirizzi.crea.interno	Creare indirizzi IP interni all'interno della rete VPC per l'allocazione delle risorse.	NO	SÌ	NO
calcola.indirizzi.eliminaInterno	Elimina gli indirizzi IP interni per la pulizia delle risorse.	NO	SÌ	NO
calcola.indirizzi.imposta.etichette	Aggiorna le etichette sulla risorsa Indirizzo.	NO	SÌ	NO
calcola.indirizzi.usaInterno	Utilizzare indirizzi IP interni per la comunicazione di rete.	NO	SÌ	NO

Azioni	Scopo	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
compute.backendServices.create	Per configurare un servizio backend per la distribuzione del traffico in una coppia HA.	SÌ	NO	NO
compute.regionBackendServices.create	Crea e gestisci servizi backend per l'instradamento del traffico.	SÌ	NO	NO
compute.regionBackendServices.delete		NO	SÌ	NO
compute.regionBackendServices.get		SÌ	NO	NO
compute.regionBackendServices.update		SÌ	SÌ	NO
compute.regionBackendServices.list		SÌ	NO	NO
compute.regionBackendServices.use		NO	SÌ	NO
compute.networks.updatePolicy	Per applicare regole firewall alle VPC e alle subnet per una coppia HA.	SÌ	NO	NO
compute.instanceGroups.get	Per creare e gestire VM di storage su coppie Cloud Volumes ONTAP HA.	SÌ	SÌ	NO
calcola.indirizzi.ottieni		SÌ	SÌ	NO
calcola.istanze.aggiornaInterfaccia di rete		SÌ	SÌ	NO
compute.instanceGroups.create		NO	SÌ	NO
compute.instanceGroups.delete		NO	SÌ	NO
compute.instanceGroups.update		NO	SÌ	NO
compute.instanceGroups.use		NO	SÌ	NO

Azioni	Scopo	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
monitoraggio.timeSeries.list	Per scoprire informazioni sui bucket di Google Cloud Storage.	SÌ	SÌ	NO
storage.buckets.getIamPolicy		SÌ	SÌ	NO

Autorizzazioni utilizzate per NetApp Backup and Recovery

L'agente Console utilizza le autorizzazioni nel ruolo personalizzato per gestire le risorse e i processi NetApp Backup and Recovery nella rete Google Cloud. Le sezioni seguenti descrivono come l'agente utilizza queste autorizzazioni.

Visualizza le autorizzazioni per NetApp Backup and Recovery

Azioni	Scopo	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
• cloudkms.cryptoKeys.get • cloudkms.cryptoKeys.getIamPolicy • cloudkms.cryptoKeys.list • cloudkms.cryptoKeys.setIamPolicy • cloudkms.keyRings.get • cloudkms.keyRings.getIamPolicy • cloudkms.keyRings.list • cloudkms.keyRings.setIamPolicy	Per selezionare le chiavi gestite dal cliente nella procedura guidata di attivazione NetApp Backup and Recovery anziché utilizzare le chiavi di crittografia predefinite gestite da Google.	SÌ	SÌ	NO

Autorizzazioni utilizzate per la NetApp Data Classification

L'agente Console utilizza le autorizzazioni nel ruolo personalizzato per gestire le risorse e i processi NetApp Data Classification nella rete Google Cloud. Le sezioni seguenti descrivono come l'agente utilizza queste autorizzazioni.

Visualizza le autorizzazioni per la NetApp Data Classification

Azioni	Scopo	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
• calcolo.sottoreti.uso • calcola.sottoreti.usaIPesterno • calcola.istanze.aggiungiAccessConfig	Per abilitare la NetApp Data Classification.	SÌ	NO	NO

Registro delle modifiche

Di seguito sono riportati i permessi aggiunti e rimossi.

08 dicembre 2025

NetApp sta passando da Google Cloud Deployment Manager a Google Cloud Infrastructure Manager (IM) per distribuire ed eseguire l'agente Console in Google Cloud. Per supportare questa modifica sono state aggiunte le seguenti autorizzazioni.

Per l'utente Google Cloud che distribuisce l'agente sono necessarie le seguenti autorizzazioni aggiuntive:

- storage.buckets.create
- storage.buckets.get
- archiviazione.oggetti.crea
- archiviazione.cartelle.crea
- elenco.oggetti.di.archiviazione
- iam.serviceAccount.actAs
- config.deployments.create
- config.operations.get

Per l'account di servizio in Google Cloud utilizzato per le operazioni quotidiane sono necessarie le seguenti autorizzazioni aggiuntive:

- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken
- cloudbuild.repositories.list
- cloudquotas.quotas.get
- config.artifacts.import

- config.deployments.deleteState
- config.deployments.getLock
- config.deployments.getState
- config.deployments.updateState
- config.anteprime.carica
- config.revisions.getState
- registrazione.logEntries.create
- archiviazione.oggetti.crea
- archiviazione.oggetti.elimina
- aggiornamento.oggetti.di.archiviazione
- iam.serviceAccounts.get

Per distribuire Cloud Volumes ONTAP sono necessarie le seguenti autorizzazioni aggiuntive:

- cloudbuild.builds.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.anteprime.elenco
- config.revisions.get
- elenco risorse di configurazione
- iam.serviceAccountKeys.create
- iam.serviceAccounts.create

Per l'account di servizio utilizzato per le operazioni quotidiane di Cloud Volumes ONTAP sono necessarie le seguenti autorizzazioni aggiuntive.

- calcola.indirizzi.crea.interno
- calcola.indirizzi.eliminaInterno
- calcola.indirizzi.imposta.etichette
- calcola.indirizzi.usaInterno
- calcola.regolediinoltro.crea
- calcola.regolediinoltro.elimina
- calcola.regolediinoltro.ottieni
- calcola.regolediinoltro.impostaetichette

- calcola.controlli.salute.crea
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.update
- compute.instanceGroups.use
- calcola.istanze.uso
- compute.regionBackendServices.delete
- compute.regionBackendServices.update
- compute.regionBackendServices.use
- calcola.risorsePolitiche.crea
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- registrazione.logEntries.route
- config.deployments.create
- config.deployments.delete
- config.deployments.get
- config.deployments.update
- config.revisions.get
- configurazione.distribuzioni.blocco
- config.operations.get

26 novembre 2025

Le autorizzazioni sono state aggiornate per chiarire il loro utilizzo, ma non sono state aggiunte o rimosse autorizzazioni. Sono state aggiunte tre colonne per indicare se ogni autorizzazione viene utilizzata per la distribuzione, le operazioni quotidiane o l'eliminazione. Oltre a ciò, alcune autorizzazioni sono separate in base al loro utilizzo per NetApp Data Classification e NetApp Backup and Recovery.

06 febbraio 2023

A questa policy è stata aggiunta la seguente autorizzazione:

- calcola.istanze.aggiornaInterfaccia di rete

Questa autorizzazione è richiesta per Cloud Volumes ONTAP.

2023-01-27

A questa policy sono state aggiunte le seguenti autorizzazioni:

- cloudkms.cryptoKeys.getIamPolicy

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

Queste autorizzazioni sono necessarie per NetApp Backup and Recovery.

Regole del firewall dell'agente in Google Cloud

Le regole del firewall di Google Cloud per l'agente richiedono sia regole in entrata che in uscita. La NetApp Console crea automaticamente questo gruppo di sicurezza quando si crea un agente della console dalla console. Per altre opzioni di installazione, è necessario impostare manualmente questo gruppo di sicurezza.

Regole in entrata

Protocollo	Porta	Scopo
SSH	22	Fornisce accesso SSH all'host dell'agente
HTTP	80	• Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale • Utilizzato durante il processo di aggiornamento Cloud Volumes ONTAP
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale
TCP	3128	Fornisce a Cloud Volumes ONTAP l'accesso a Internet. Dopo la distribuzione, è necessario aprire manualmente questa porta.

Regole in uscita

Le regole del firewall predefinite dell'agente aprono tutto il traffico in uscita. Seguire le regole di base in uscita, se accettabili, oppure utilizzare regole di uscita avanzate per requisiti più rigorosi.

Regole di base in uscita

Le regole del firewall predefinite per l'agente includono le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutto TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole in uscita avanzate

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita da parte dell'agente.

L'indirizzo IP di origine è l'host dell'agente.

Servizio	Protocollo	Porta	Destinazione	Scopo
Chiamate API e AutoSupport	HTTPS	443	Gestione cluster ONTAP e Internet in uscita LIF	Chiamate API a Google Cloud, a ONTAP, a NetApp Data Classification e invio di messaggi AutoSupport a NetApp
chiamate API	TCP	8080	Classificazione dei dati	Sonda per l'istanza di classificazione dei dati durante la distribuzione
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS tramite classificazione dei dati

Accesso di rete richiesto per 3.9.55 e versioni precedenti

NetApp Console, l'agente NetApp Console e i servizi dati NetApp necessitano di accesso a Internet in uscita per contattare gli endpoint necessari.

In questo argomento viene documentato l'accesso alla rete richiesto per le versioni della modalità standard 3.9.55 e precedenti della NetApp Console . Per gli endpoint richiesti per 4.0.0 e versioni successive, rivedere"gli endpoint richiesti per 4.0.0 e versioni successive" .

È necessario configurare l'accesso alla rete per quanto segue:

- Computer che accedono alla NetApp Console come software come servizio (SaaS)
- Agenti console installabili in locale o nel cloud.

Aggiorna l'elenco degli endpoint all'elenco rivisto per la versione 4.0.0 e successive

A partire dalla versione 4.0.0, gli agenti della console richiedono meno endpoint. Le distribuzioni esistenti precedenti alla versione 4.0.0 continuano a essere supportate. Dopo aver effettuato l'aggiornamento alla versione 4.0.0 o successiva, puoi rimuovere i vecchi endpoint dall'elenco consentito quando preferisci.

NetApp consiglia di aggiornare le regole del firewall per utilizzare l'elenco degli endpoint rivisto, che è più piccolo, più sicuro e più facile da gestire. NetApp elimina la necessità di voci jolly e gli endpoint per gli aggiornamenti degli agenti supportano tutti i servizi dati.

Punti finali per 3.9.55 e precedenti	Endpoint per 4.0.0 e versioni successive	Scopo
• \ https://support.netapp.com • \ https://mysupport.netapp.com	• \ https://mysupport.netapp.com • \ https://signin.b2c.netapp.com • \ https://support.netapp.com	Per ottenere le licenze e contattare l'assistenza NetApp .
• https://*.api.bluexp.netapp.com • \ https://api.bluexp.netapp.com • https://*.cloudmanager.cloud.netapp.com • \ https://cloudmanager.cloud.netapp.com • \ https://netapp-cloud-account.auth0.com • \ https://netapp-cloud-account.us.auth0.com • \ https://console.bluexp.netapp.com • https://*.console.bluexp.netapp.com	• \ https://api.bluexp.netapp.com • \ https://netapp-cloud-account.auth0.com • \ https://netapp-cloud-account.us.auth0.com • \ https://console.netapp.com • \ https://components.console.bluexp.netapp.com • \ https://cdn.auth0.com	Per le operazioni quotidiane.
• https://*.blob.core.windows.net • \ https://cloudmanagerinfraprod.azurecr.io	• \ https://bluexpinfraprod.eastus2.data.azurecr.io • \ https://bluexpinfraprod.azurecr.io	Per ottenere immagini per gli aggiornamenti dell'agente della console.

Passi

1. Verifica che la versione dell'agente sia 4.0.0 o successiva."Visualizza la versione dell'agente."
2. Aggiungi alla whitelist gli endpoint in"Endpoint supportati per 4.0.0 e versioni successive" .
3. Riavviare il servizio Service Manager 2 su ciascun agente eseguendo il seguente comando:

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

4. Eseguire il seguente comando e verificare che lo stato dell'agente sia *attivo(in esecuzione)*: _

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

5. Rimuovi i vecchi endpoint dall'elenco consentito del firewall.

Endpoint per NetApp Console e agenti Console per 3.9.55 e versioni precedenti

Questi endpoint vengono utilizzati per gli agenti Console 3.9.55 e versioni precedenti.

Punti finali	Scopo
\ https://support.netapp.com \ https://mysupport.netapp.com	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
https://*.api.blueexp.netapp.com \ https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com \ https://cloudmanager.cloud.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com	Per fornire funzionalità e servizi all'interno della NetApp Console.
Scegli tra due serie di endpoint: • Opzione 1 (consigliata) \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • Opzione 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	Per ottenere immagini per gli aggiornamenti dell'agente della console. NetApp consiglia di consentire gli endpoint dell'Opzione 1 nel firewall in quanto più sicuri e di non consentire gli endpoint dell'Opzione 2, a meno che non si utilizzi Ransomware Resilience o Backup and Recovery. Si tenga presente quanto segue in merito a questi endpoint: • Gli endpoint dell'opzione 1 sono supportati nella versione 3.9.47 e successive. Le versioni precedenti alla 3.9.47 non supportano la compatibilità con le versioni precedenti. • L'agente della console avvia prima il contatto con gli endpoint nell'opzione 2. Se tali endpoint non sono accessibili, vengono contattati automaticamente gli endpoint nell'opzione 1. • Se si utilizza l'agente Console con NetApp Backup and Recovery o Ransomware Resilience, il sistema non supporta gli endpoint Opzione 1. Consentire gli endpoint dell'opzione 2 e non consentire l'opzione 1.

Endpoint del provider cloud contattati dall'agente della console

Gli agenti della console devono avere accesso ad endpoint aggiuntivi se sono distribuiti nel tuo provider cloud.

Abilitare l'accesso agli endpoint del provider cloud prima di installare l'agente Console.

- "Configurare l'accesso alla rete AWS per un agente della console"
- "Configurare l'accesso alla rete di Azure per un agente della console"

- "Configurare l'accesso alla rete Google Cloud per un agente della console"

Gli endpoint del provider cloud sono gli stessi per tutte le versioni.

Endpoint dei servizi dati contattati dall'agente della console

L'agente Console richiede un accesso Internet in uscita aggiuntivo per supportare alcuni servizi dati NetApp e Cloud Volumes ONTAP.

Endpoint per Cloud Volumes ONTAP

- "Endpoint per Cloud Volumes ONTAP in AWS"
- "Endpoint per Cloud Volumes ONTAP in Azure"
- "Endpoint per Cloud Volumes ONTAP in Google Cloud"

Richiedere l'uso di IMDSv2 sulle istanze Amazon EC2

La NetApp Console supporta Amazon EC2 Instance Metadata Service versione 2 (IMDSv2) con l'agente della console e con Cloud Volumes ONTAP (incluso il mediatore per le distribuzioni HA). Nella maggior parte dei casi, IMDSv2 viene configurato automaticamente sulle nuove istanze EC2. IMDSv1 era abilitato prima di marzo 2024. Se richiesto dalle policy di sicurezza, potrebbe essere necessario configurare manualmente IMDSv2 sulle istanze EC2.

Prima di iniziare

- La versione dell'agente della console deve essere 3.9.38 o successiva.
- Cloud Volumes ONTAP deve eseguire una delle seguenti versioni:
  - 9.12.1 P2 (o qualsiasi patch successiva)
  - 9.13.0 P4 (o qualsiasi patch successiva)
  - 9.13.1 o qualsiasi versione successiva a questa versione
- Questa modifica richiede il riavvio delle istanze Cloud Volumes ONTAP .
- Questi passaggi richiedono l'uso dell'AWS CLI perché è necessario modificare il limite di hop di risposta a 3.

Informazioni su questo compito

IMDSv2 offre una protezione avanzata contro le vulnerabilità. "Scopri di più su IMDSv2 dal blog sulla sicurezza di AWS"

Il servizio metadati dell'istanza (IMDS) è abilitato come segue sulle istanze EC2:

- Per le nuove distribuzioni degli agenti della Console dalla Console o tramite "Script di Terraform" , IMDSv2 è abilitato per impostazione predefinita sull'istanza EC2.
- Se avvii una nuova istanza EC2 in AWS e poi installi manualmente il software dell'agente della console, IMDSv2 è abilitato per impostazione predefinita.
- Se si avvia l'agente Console da AWS Marketplace, IMDSv1 è abilitato per impostazione predefinita. È possibile configurare manualmente IMDSv2 sull'istanza EC2.

- Per gli agenti Console esistenti, IMDSv1 è ancora supportato, ma se preferisci puoi configurare manualmente IMDSv2 sull'istanza EC2.
- Per Cloud Volumes ONTAP, IMDSv1 è abilitato per impostazione predefinita sulle istanze nuove ed esistenti. Se preferisci, puoi configurare manualmente IMDSv2 sulle istanze EC2.

Passi

1. Richiede l'uso di IMDSv2 sull'istanza dell'agente Console:

   a. Connettersi alla VM Linux per l'agente della console.

      Quando hai creato l'istanza dell'agente Console in AWS, hai fornito una chiave di accesso AWS e una chiave segreta. È possibile utilizzare questa coppia di chiavi per connettersi tramite SSH all'istanza. Il nome utente per l'istanza EC2 Linux è ubuntu (per gli agenti Console creati prima di maggio 2023, il nome utente era ec2-user).

      "Documentazione AWS: connettiti alla tua istanza Linux"

   b. Installare l'AWS CLI.

      "Documentazione AWS: installa o aggiorna all'ultima versione di AWS CLI"

   c. Utilizzare il `aws ec2 modify-instance-metadata-options` comando per richiedere l'uso di IMDSv2 e per modificare il limite di hop della risposta PUT a 3.

      Esempio

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

   +

   IL `http-tokens` il parametro imposta IMDSv2 su obbligatorio. Quando `http-tokens` è obbligatorio, devi anche impostare `http-endpoint` per abilitare.

2. Richiede l'uso di IMDSv2 sulle istanze Cloud Volumes ONTAP :

   a. Vai al "Console Amazon EC2"

   b. Dal riquadro di navigazione, seleziona **Istanze**.

   c. Selezionare un'istanza Cloud Volumes ONTAP .

   d. Selezionare **Azioni > Impostazioni istanza > Modifica opzioni metadati istanza**.

   e. Nella finestra di dialogo **Modifica opzioni metadati istanza**, seleziona quanto segue:

      - Per **Servizio metadati istanza**, seleziona **Abilita**.
      - Per **IMDSv2**, selezionare **Obbligatorio**.
      - Seleziona **Salva**.

   f. Ripetere questi passaggi per le altre istanze Cloud Volumes ONTAP , incluso il mediatore HA.

g. "Arresta e avvia le istanze Cloud Volumes ONTAP"

Risultato

L'istanza dell'agente Console e le istanze Cloud Volumes ONTAP sono ora configurate per utilizzare IMDSv2.

Configurazione predefinita per l'agente della console

Scopri di più sulle configurazioni predefinite dell'agente della console per distribuzioni standard (con accesso a Internet) su AWS, Azure e Google Cloud, nonché sulle distribuzioni limitate (senza accesso a Internet) per ambienti on-premise.

Configurazione predefinita con accesso a Internet

I seguenti dettagli di configurazione si applicano se hai distribuito un agente Console dalla NetApp Console, dal marketplace del tuo provider cloud o se hai installato manualmente un agente Console su un host Linux locale con accesso a Internet.

Dettagli della VM dell'agente console per AWS

Se hai distribuito un agente Console dalla Console o dal marketplace del provider cloud, tieni presente quanto segue:

- Il tipo di istanza EC2 è t3.2xlarge.
- Il sistema operativo per l'immagine è Ubuntu 22.04 LTS.

  Il sistema operativo non include un'interfaccia grafica utente (GUI). Per accedere al sistema è necessario utilizzare un terminale.

- L'installazione include Docker Engine, lo strumento di orchestrazione dei container richiesto.
- Il nome utente per l'istanza EC2 Linux è ubuntu (per gli agenti creati prima di maggio 2023, il nome utente è ec2-user).
- Il disco di sistema predefinito è un disco gp2 da 100 GiB.

Dettagli della macchina virtuale dell'agente console per Azure

Se hai distribuito un agente Console dalla Console o dal marketplace del provider cloud, tieni presente quanto segue:

- Il tipo di VM è Standard_D8s_v3.
- Il sistema operativo per l'immagine è Ubuntu 22.04 LTS.

  Il sistema operativo non include un'interfaccia grafica utente (GUI). Per accedere al sistema è necessario utilizzare un terminale.

- L'installazione include Docker Engine, lo strumento di orchestrazione dei container richiesto.
- Il disco di sistema predefinito è un disco SSD premium da 100 GiB.

Dettagli della VM dell'agente della console per Google Cloud

Se hai distribuito un agente Console dalla Console, tieni presente quanto segue:

- L’istanza della VM è n2-standard-8.
- Il sistema operativo per l’immagine è Ubuntu 22.04 LTS.

  Il sistema operativo non include un’interfaccia grafica utente (GUI). Per accedere al sistema è necessario utilizzare un terminale.

- L’installazione include Docker Engine, lo strumento di orchestrazione dei container richiesto.
- Il disco di sistema predefinito è un disco persistente SSD da 100 GiB.

Cartella di installazione

La cartella di installazione dell’agente si trova nel seguente percorso:

`/opt/application/netapp/cloudmanager`

File di registro

I file di registro sono contenuti nelle seguenti cartelle:

- `/opt/application/netapp/cloudmanager/log` O
- `/opt/application/netapp/service-manager-2/logs` (a partire dalle nuove installazioni 3.9.23)

  I registri in queste cartelle forniscono dettagli sull’agente della console.

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

  I registri in questa cartella forniscono dettagli sui servizi cloud e sul servizio Console in esecuzione sull’agente Console.

Servizio agente console

- Il servizio agente della console si chiama occm.
- Il servizio occm dipende dal servizio MySQL.

  Se il servizio MySQL è inattivo, lo è anche il servizio occm.

porti

L’agente utilizza le seguenti porte sull’host Linux:

- 80 per l’accesso HTTP
- 443 per l’accesso HTTPS

Configurazione predefinita senza accesso a Internet

La seguente configurazione si applica se hai installato manualmente l’agente Console su un host Linux locale che non ha accesso a Internet. "Scopri di più su questa opzione di installazione" .

- La cartella di installazione dell’agente si trova nel seguente percorso:

  `/opt/application/netapp/ds`

- I file di registro sono contenuti nelle seguenti cartelle:

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

  I registri in questa cartella forniscono dettagli sull'agente Console e sulle immagini Docker.

- Tutti i servizi sono in esecuzione all'interno di contenitori Docker

  I servizi dipendono dal servizio runtime Docker in esecuzione

- L'agente utilizza le seguenti porte sull'host Linux:
  - 80 per l'accesso HTTP
  - 443 per l'accesso HTTPS