Referenz

NetApp Console setup and administration

NetApp
January 23, 2026

Inhalt

Referenz

Agenten-Wartungskonsole

Agentenvalidierung mit der Wartungskonsole

Mit der Wartungskonsole des Console-Agenten können Sie die Installation und Konfiguration eines Console-Agenten überprüfen.

Zugriff auf die Agenten-Wartungskonsole

Sie können vom Konsolenagent-Host aus auf die Wartungskonsole zugreifen. Navigieren Sie zum folgenden Verzeichnis:

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

config-checker validate

Der `config-checker validate` Mit diesem Befehl können Sie die Konfiguration eines Konsolenagenten überprüfen.

Parameter

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

Wählen Sie einen oder mehrere Dienste zur Validierung aus. Gültige Dienstnamen sind:*`PLATFORM` wodurch die Netzwerkverbindung zu den erforderlichen Konsolenendpunkten überprüft wird.

`--validationTypes <comma-separated list validation types to run>`**--ERFORDERLICH--** Wählen Sie einen oder mehrere Validierungstypen aus, die ausgeführt werden sollen. Gültige Validierungstypen sind: * `NETWORK` wodurch die Netzwerkverbindung zu den erforderlichen Konsolenendpunkten überprüft wird.

`--proxy <url>`**--OPTIONAL--**

Gibt die URL des Proxy-Servers an, der für die Validierung verwendet werden soll. Erforderlich, wenn Ihr Agent für die Verwendung eines Proxy-Servers konfiguriert ist.

`--certs <paths>`**--OPTIONAL--**

Gibt den Pfad zu einer oder mehreren Zertifikatsdateien an, die für die Validierung verwendet werden sollen. Die Zertifikatsdateien müssen im PEM-Format vorliegen. Mehrere Pfade durch Kommas trennen. Dieser Parameter ist erforderlich, wenn Ihr Agent ein benutzerdefiniertes Zertifikat verwendet.

Config-Checker-Validierungsbeispiele

Grundlegende Validierung:

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

Validierung, bei der ein Proxy-Server für den Agenten verwendet wird:

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

Validierung, bei der ein Zertifikat für den Agenten verwendet wird:

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

Hilfe zu jedem Befehl anzeigen

Um Hilfe zu einem Befehl anzuzeigen, fügen Sie an `--help` zum Befehl. Um beispielsweise Hilfe für die `proxy add` Befehl, verwenden Sie den folgenden Befehl:

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

Transparente Proxy-Befehle

Sie können die Wartungskonsole des Konsolenagenten verwenden, um einen Konsolenagenten für die Verwendung eines transparenten Proxyservers zu konfigurieren.

Zugriff auf die Agenten-Wartungskonsole

Sie können vom Konsolenagent-Host aus auf die Wartungskonsole zugreifen. Navigieren Sie zum folgenden Verzeichnis:

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

Hilfe zu jedem Befehl anzeigen

Um Hilfe zu einem Befehl anzuzeigen, fügen Sie an `--help` zum Befehl. Um beispielsweise Hilfe für die `proxy add` Befehl, verwenden Sie den folgenden Befehl:

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

Proxy abrufen

Der `proxy get` Der Befehl zeigt Informationen über die aktuelle Konfiguration des transparenten Proxy-

Servers an. Um die aktuelle Konfiguration des transparenten Proxy-Servers anzuzeigen, verwenden Sie folgenden Befehl:

Proxy-Abfragebeispiel

Um die aktuelle Konfiguration des transparenten Proxy-Servers anzuzeigen, verwenden Sie folgenden Befehl:

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

Proxy hinzufügen

Der `proxy add` Der Befehl konfiguriert den Agenten zur Verwendung eines transparenten Proxy-Servers.

Parameter

`-c <certificate file>`

Gibt den Pfad zur Zertifikatsdatei für den Proxy-Server an. Die Zertifikatsdatei muss im PEM-Format vorliegen. Stellen Sie sicher, dass sich die Zertifikatsdatei im selben Verzeichnis wie der Befehl befindet, oder geben Sie den vollständigen Pfad zur Zertifikatsdatei an.

Beispiel zum Hinzufügen eines Proxys

Um einen transparenten Proxyserver hinzuzufügen, verwenden Sie den folgenden Befehl, wobei `/home/ubuntu/myCA1.pem` ist der Pfad zur Zertifikatsdatei für den Proxyserver. Die Zertifikatsdatei muss im PEM-Format vorliegen:

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

Proxy-Update

Der `proxy update` Mit diesem Befehl können Sie das Zertifikat eines transparenten Proxys aktualisieren.

Parameter

`-c <certificate file>`gibt den Pfad zur Zertifikatsdatei für den Proxy-Server an. Die Zertifikatsdatei muss im PEM-Format vorliegen.

Stellen Sie sicher, dass sich die Zertifikatsdatei im selben Verzeichnis wie der Befehl befindet, oder geben Sie den vollständigen Pfad zur Zertifikatsdatei an.

Proxy-Update-Beispiel

Um das Zertifikat für einen transparenten Proxyserver zu aktualisieren, verwenden Sie den folgenden Befehl, wobei `/home/ubuntu/myCA1.pem` ist der Pfad zur neuen Zertifikatsdatei für den Proxyserver. Die Zertifikatsdatei muss im PEM-Format vorliegen:

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

Proxy entfernen

Der `proxy remove` Der Befehl entfernt die Konfiguration des transparenten Proxy-Servers vom Agenten.

Beispiel zum Entfernen eines Proxys

Um den transparenten Proxyserver zu entfernen, verwenden Sie den folgenden Befehl:

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

Berechtigungen und Netzwerkanforderungen des Cloud-Anbieters

Berechtigungsübersicht für die NetApp Console

Sie müssen dem Konsolenagenten die entsprechenden Berechtigungen erteilen, damit er Operationen in Ihrer Cloud-Umgebung durchführen kann. Über die Links auf dieser Seite erhalten Sie schnell Zugriff auf die Berechtigungen, die Sie je nach Ihrem Ziel benötigen.

AWS-Berechtigungen

Die NetApp Console erfordert AWS-Berechtigungen für einen Konsolenagenten und für einzelne Dienste.

Konsolenagenten

Ziel	Beschreibung	Link
Einen Konsolenagenten über die Konsole bereitstellen Um einen Konsolenagenten in AWS bereitzustellen, benötigt der Benutzer bestimmte Berechtigungen.	"AWS-Berechtigungen einrichten"	Berechtigungen für einen Konsolenagenten bereitstellen

NetApp Backup and Recovery

Ziel	Beschreibung	Link
Sichern Sie lokale ONTAP -Cluster mit NetApp Backup and Recovery auf Amazon S3	Beim Aktivieren von Backups auf Ihren ONTAP Volumes werden Sie von NetApp Backup and Recovery aufgefordert, einen Zugriffsschlüssel und ein Geheimnis für einen IAM-Benutzer mit bestimmten Berechtigungen einzugeben.	"S3-Berechtigungen für Backups einrichten"

Cloud Volumes ONTAP

Ziel	Beschreibung	Link
Berechtigungen für Cloud Volumes ONTAP -Knoten bereitstellen	Jedem Cloud Volumes ONTAP Knoten in AWS muss eine IAM-Rolle zugeordnet werden. Dasselbe gilt für den HA-Mediator. Die Standardoption besteht darin, die IAM-Rollen von der Konsole erstellen zu lassen. Sie können jedoch auch Ihre eigenen Rollen verwenden, wenn Sie das System in der Konsole erstellen.	"Erfahren Sie, wie Sie die IAM-Rollen selbst einrichten"

NetApp Copy and Sync

Ziel	Beschreibung	Link
Bereitstellen des Datenbrokers in AWS	Das AWS-Benutzerkonto, das Sie zum Bereitstellen des Datenbrokers verwenden, muss über die erforderlichen Berechtigungen verfügen.	"Erforderliche Berechtigungen zum Bereitstellen des Datenbrokers in AWS"
Berechtigungen für den Datenbroker bereitstellen	Wenn NetApp Copy and Sync den Datenbroker bereitstellt, wird eine IAM-Rolle für die Datenbrokerinstanz erstellt. Sie können den Datenbroker bei Bedarf mit Ihrer eigenen IAM-Rolle bereitstellen.	"Voraussetzungen für die Nutzung einer eigenen IAM-Rolle beim AWS-Datenbroker"
Aktivieren Sie den AWS-Zugriff für einen manuell installierten Datenbroker	Wenn Sie den Datenbroker mit einer Synchronisierungsbeziehung verwenden, die einen S3-Bucket umfasst, sollten Sie den Linux-Host für den AWS-Zugriff vorbereiten. Wenn Sie den Datenbroker installieren, müssen Sie AWS-Schlüssel für einen IAM-Benutzer bereitstellen, der über programmgesteuerten Zugriff und bestimmte Berechtigungen verfügt.	"Aktivieren des Zugriffs auf AWS"

FSx für ONTAP

Ziel	Beschreibung	Link
Erstellen und verwalten Sie FSx für ONTAP	Um ein Amazon FSx for NetApp ONTAP System zu erstellen oder zu verwalten, müssen Sie der Konsole AWS-Anmeldeinformationen hinzufügen, indem Sie die ARN einer IAM-Rolle angeben, die der Konsole die erforderlichen Berechtigungen erteilt.	"Erfahren Sie, wie Sie AWS-Anmeldeinformationen für FSx einrichten"

NetApp Cloud Tiering

Ziel	Beschreibung	Link
Tiering von lokalen ONTAP -Clustern auf Amazon S3	Wenn Sie NetApp Cloud Tiering für AWS aktivieren, geben Sie einen Zugriffsschlüssel und einen geheimen Schlüssel ein. Diese Zugangsdaten werden an den ONTAP Cluster übergeben, damit ONTAP Daten in den S3-Bucket verschieben kann.	"Einrichten von S3-Berechtigungen für das Tiering"

Azure-Berechtigungen

Die Konsole erfordert Azure-Berechtigungen für einen Konsolen-Agenten und für einzelne Dienste.

Konsolenagent

Ziel	Beschreibung	Link
Bereitstellen eines Konsolenagenten über die Konsole	Wenn Sie einen Konsolen-Agenten über die Konsole bereitstellen, müssen Sie ein Azure-Konto oder einen Dienstprinzipal verwenden, der über die Berechtigung zum Bereitstellen einer Konsolen-Agent-VM in Azure verfügt.	"Einrichten von Azure-Berechtigungen"
Berechtigungen für einen Konsolenagenten bereitstellen	Wenn die Konsole eine Konsolen-Agent-VM in Azure bereitstellt, erstellt sie eine benutzerdefinierte Rolle, die die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen innerhalb dieses Azure-Abonnements bereitstellt. Sie müssen die benutzerdefinierte Rolle selbst einrichten, wenn Sie einen Konsolen-Agenten vom Marktplatz aus starten, wenn Sie einen Konsolen-Agenten manuell installieren oder wenn Sie"Fügen Sie einem Konsolen-Agenten weitere Azure-Anmeldeinformationen hinzu" . Halten Sie die Richtlinie auf dem neuesten Stand, da in späteren Versionen neue Berechtigungen hinzugefügt werden.	"Azure-Berechtigungen für einen Konsolen-Agent"

NetApp Backup and Recovery

Ziel	Beschreibung	Link
Sichern Sie Cloud Volumes ONTAP im Azure Blob Storage	Wenn Sie NetApp Backup and Recovery zum Sichern von Cloud Volumes ONTAP verwenden, müssen Sie in den folgenden Szenarien einem Konsolenagenten Berechtigungen hinzufügen: • Sie möchten die Funktion „Suchen und Wiederherstellen“ verwenden • Sie möchten vom Kunden verwaltete Verschlüsselungsschlüssel (CMEK) verwenden	• "Sichern Sie Cloud Volumes ONTAP Daten mit Backup und Recovery im Azure Blob-Speicher"
Sichern Sie lokale ONTAP -Cluster im Azure Blob Storage	Wenn Sie NetApp Backup and Recovery zum Sichern von On-Premises ONTAP Clustern verwenden, müssen Sie einem Console-Agenten Berechtigungen hinzufügen, um die Funktion „Suchen & Wiederherstellen“ nutzen zu können.	"Sichern Sie lokale ONTAP -Daten mit Backup und Recovery im Azure Blob-Speicher"

NetApp Kopieren und Synchronisieren

Ziel	Beschreibung	Link
Bereitstellen des Datenbrokers in Azure	Das Azure-Benutzerkonto, das Sie zum Bereitstellen des Datenbrokers verwenden, muss über die erforderlichen Berechtigungen verfügen.	"Erforderliche Berechtigungen zum Bereitstellen des Datenbrokers in Azure"

Google Cloud-Berechtigungen

Die Konsole erfordert Google Cloud-Berechtigungen für einen Konsolenagenten und für einzelne Dienste.

Konsolenagenten

Ziel	Beschreibung	Link
Bereitstellen eines Konsolenagenten über die Konsole	Der Google Cloud-Benutzer, der einen Konsolen-Agenten von der Konsole aus bereitstellt, benötigt bestimmte Berechtigungen, um einen Konsolen-Agenten in Google Cloud bereitzustellen.	"Richten Sie Berechtigungen zum Erstellen eines Konsolenagenten ein"
Berechtigungen für einen Konsolenagenten bereitstellen	Das Dienstkonto eines Konsolenagenten muss für den täglichen Betrieb über spezifische Berechtigungen verfügen. Sie müssen das Dienstkonto während der Bereitstellung mit einem Konsolenagenten verknüpfen. Halten Sie die Richtlinie auf dem neuesten Stand, da in späteren Versionen neue Berechtigungen hinzugefügt werden.	"Einrichten von Berechtigungen für einen Konsolenagenten"

NetApp Backup and Recovery

Ziel	Beschreibung	Link
Sichern Sie Cloud Volumes ONTAP in Google Cloud	Wenn Sie NetApp Backup and Recovery zum Sichern von Cloud Volumes ONTAP verwenden, müssen Sie in den folgenden Szenarien einem Konsolenagenten Berechtigungen hinzufügen: • Sie möchten die Funktion „Suchen und Wiederherstellen“ verwenden • Sie möchten vom Kunden verwaltete Verschlüsselungsschlüssel (CMEK) verwenden	• "Sichern Sie Cloud Volumes ONTAP Daten mit Backup und Recovery in Google Cloud Storage" • "Berechtigungen für CMEKs"
Sichern Sie lokale ONTAP -Cluster in der Google Cloud	Wenn Sie NetApp Backup and Recovery zum Sichern von On-Premises ONTAP Clustern verwenden, müssen Sie einem Console-Agenten Berechtigungen hinzufügen, um die Funktion „Suchen & Wiederherstellen“ nutzen zu können.	"Sichern Sie lokale ONTAP -Daten mit Backup und Recovery in Google Cloud Storage"

NetApp Copy and Sync

Ziel	Beschreibung	Link
Bereitstellen des Datenbrokers in Google Cloud	Stellen Sie sicher, dass der Google Cloud-Benutzer, der den Datenbroker bereitstellt, über die erforderlichen Berechtigungen verfügt.	"Erforderliche Berechtigungen zum Bereitstellen des Datenbrokers in Google Cloud"
Aktivieren Sie den Google Cloud-Zugriff für einen manuell installierten Datenbroker	Wenn Sie den Datenbroker mit einer Synchronisierungsbeziehung verwenden möchten, die einen Google Cloud Storage-Bucket umfasst, sollten Sie den Linux-Host für den Google Cloud-Zugriff vorbereiten. Wenn Sie den Datenbroker installieren, müssen Sie einen Schlüssel für ein Dienstkonto mit bestimmten Berechtigungen angeben.	"Zugriff auf Google Cloud aktivieren"

StorageGRID Berechtigungen

Die Konsole benötigt StorageGRID -Berechtigungen für zwei Dienste.

NetApp Backup and Recovery

Ziel	Beschreibung	Link
Sichern Sie lokale ONTAP -Cluster auf StorageGRID	Wenn Sie StorageGRID als Sicherungsziel für ONTAP Cluster vorbereiten, werden Sie von NetApp Backup and Recovery aufgefordert, einen Zugriffsschlüssel und ein Geheimnis für einen IAM-Benutzer mit bestimmten Berechtigungen einzugeben.	"Bereiten Sie StorageGRID als Ihr Sicherungsziel vor"

NetApp Cloud Tiering

Ziel	Beschreibung	Link
Tiering von lokalen ONTAP -Clustern auf StorageGRID	Wenn Sie NetApp Cloud Tiering für StorageGRID einrichten, müssen Sie Cloud Tiering einen S3-Zugriffsschlüssel und einen geheimen Schlüssel bereitstellen. Beim Cloud-Tiering werden die Schlüssel für den Zugriff auf Ihre Buckets verwendet.	"Tiering für StorageGRID vorbereiten"

AWS-Agentenberechtigungen und Sicherheitsregeln

AWS-Berechtigungen für den Konsolenagenten

Wenn die NetApp Console einen Konsolenagenten in AWS startet, fügt sie dem Agenten eine Richtlinie hinzu, die dem Agenten die Berechtigung zum Verwalten von Ressourcen und Prozessen innerhalb dieses AWS-Kontos erteilt. Der Agent verwendet die Berechtigungen, um API-Aufrufe an mehrere AWS-Dienste zu tätigen, darunter EC2, S3, CloudFormation, IAM, den Key Management Service (KMS) und mehr.

IAM-Richtlinien

Die unten verfügbaren IAM-Richtlinien bieten die Berechtigungen, die ein Konsolenagent benötigt, um Ressourcen und Prozesse in Ihrer öffentlichen Cloud-Umgebung basierend auf Ihrer AWS-Region zu verwalten.

Beachten Sie Folgendes:

- Wenn Sie einen Console-Agenten in einer Standard-AWS-Region direkt über die Console erstellen, wendet die Console automatisch Richtlinien auf den Agenten an.
- Sie müssen die Richtlinien selbst einrichten, wenn Sie den Agenten vom AWS Marketplace bereitstellen, wenn Sie den Agenten manuell auf einem Linux-Host installieren oder wenn Sie der Konsole zusätzliche AWS-Anmeldeinformationen hinzufügen möchten.
- In beiden Fällen müssen Sie sicherstellen, dass die Richtlinien auf dem neuesten Stand sind, da in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. Wenn neue Berechtigungen erforderlich sind, werden diese in den Versionshinweisen aufgeführt.
- Bei Bedarf können Sie die IAM-Richtlinien einschränken, indem Sie die IAM `Condition` Element. "AWS-Dokumentation: Bedingungselement"
- Schritt-für-Schritt-Anleitungen zur Verwendung dieser Richtlinien finden Sie auf den folgenden Seiten:
  - "Einrichten von Berechtigungen für eine AWS Marketplace-Bereitstellung"
  - "Einrichten von Berechtigungen für lokale Bereitstellungen"
  - "Berechtigungen für den eingeschränkten Modus einrichten"

Wählen Sie Ihre Region aus, um die erforderlichen Richtlinien anzuzeigen:

Standardregionen

Für Standardregionen sind die Berechtigungen auf zwei Richtlinien verteilt. Aufgrund einer maximalen Zeichengrößenbeschränkung für verwaltete Richtlinien in AWS sind zwei Richtlinien erforderlich.

Richtlinie Nr. 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"
    }
  ]
}
```

Richtlinie Nr. 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"
    }
  ]
}
```

GovCloud (USA)-Regionen

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

Geheime Regionen

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

Streng geheime Regionen

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

So werden die AWS-Berechtigungen verwendet

In den folgenden Abschnitten wird beschrieben, wie die Berechtigungen für die einzelnen NetApp Console -Verwaltungs- oder Datendienste verwendet werden. Diese Informationen können hilfreich sein, wenn Ihre Unternehmensrichtlinien vorschreiben, dass Berechtigungen nur bei Bedarf erteilt werden.

Amazon FSx für ONTAP

Der Konsolenagent stellt die folgenden API-Anfragen, um ein Amazon FSx for ONTAP Dateisystem zu verwalten:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribute
- ec2:DescribeRouteTables
- ec2:DescribeImages
- ec2:CreateTags
- ec2:DescribeVolumes
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSubnets

- ec2:Vpcs beschreiben
- ec2:DescribeDhcpOptions
- ec2:DescribeSnapshots
- ec2:DescribeKeyPairs
- ec2:DescribeRegions
- ec2:DescribeTags
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeReservedInstancesOfferings
- ec2:DescribeVpcEndpoints
- ec2:Vpcs beschreiben
- ec2:DescribeVolumesModifications
- ec2:DescribePlacementGroups
- kms:CreateGrant
- kms:ListAliases
- fsx:Beschreiben*
- fsx:Liste*

Amazon S3 Bucket-Erkennung

Der Konsolenagent stellt die folgende API-Anfrage, um Amazon S3-Buckets zu ermitteln:

s3:GetEncryptionConfiguration

NetApp Backup and Recovery

Der Agent stellt die folgenden API-Anfragen, um Backups in Amazon S3 zu verwalten:

- s3:GetBucketLocation
- s3:ListeAlleMeineBuckets
- s3:ListBucket
- s3:Bucket erstellen
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- s3:GetObject
- ec2:DescribeVpcEndpoints
- kms:ListAliases
- s3:PutEncryptionConfiguration

Der Agent stellt die folgenden API-Anfragen, wenn Sie die Methode „Suchen und Wiederherstellen“ zum Wiederherstellen von Volumes und Dateien verwenden:

- s3:Bucket erstellen
- s3:Objekt löschen
- s3:DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMultipartUpload
- s3:ListMultipartUploadParts

Der Agent stellt die folgenden API-Anfragen, wenn Sie DataLock und NetApp Ransomware Resilience für Ihre Volume-Backups verwenden:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:Objekt löschen
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:ListBucketByTags
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketVersioning

- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Der Agent stellt die folgenden API-Anfragen, wenn Sie für Ihre Cloud Volumes ONTAP -Backups ein anderes AWS-Konto verwenden als für die Quellvolumes:

- s3:PutBucketPolicy
- s3:PutBucketOwnershipControls

Legacy-Berechtigungen für Sicherung und Wiederherstellung

Die folgenden Berechtigungen benötigen Sie nur, wenn Sie vor der Veröffentlichung von Indexing v2 ältere Indexierungsfunktionen aktiviert haben:

- km:Liste*
- km:Beschreiben*
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- Kleber: Datenbank erstellen
- Kleber: Tabelle erstellen
- Kleber: BatchDeletePartition

Einstufung

Der Agent stellt die folgenden API-Anfragen, um NetApp Data Classification bereitzustellen:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:CreateTags
- ec2:CreateVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2:DeleteSecurityGroup
- ec2:DescribeSecurityGroups

- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface
- ec2:DescribeSubnets
- ec2:Vpcs beschreiben
- ec2:CreateSnapshot
- ec2:DescribeRegions
- Cloudformation:CreateStack
- Cloudformation:DeleteStack
- Cloudformation:DescribeStacks
- Cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

Der Agent stellt die folgenden API-Anfragen, um S3-Buckets zu scannen, wenn Sie NetApp Data Classification verwenden:

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:ListeAlleMeineBuckets
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3:Objekt löschen
- s3:DeleteObjectVersion
- s3:PutObject
- sts:Rolle übernehmen

Cloud Volumes ONTAP

Der Agent stellt die folgenden API-Anfragen, um Cloud Volumes ONTAP in AWS bereitzustellen und zu verwalten.

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und verwalten Sie IAM-Rollen und Instanzprofile für Cloud Volumes ONTAP -Instanzen	iam:ListInstanceProfiles	Ja	Ja	Nein
	iam:CreateRole	Ja	Nein	Nein
	iam:DeleteRole	Nein	Ja	Ja
	iam:PutRolePolicy	Ja	Nein	Nein
	iam:CreateInstanceProfile	Ja	Nein	Nein
	iam:DeleteRolePolicy	Nein	Ja	Ja
	iam:AddRoleToInstanceProfile	Ja	Nein	Nein
	iam:RemoveRoleFromInstanceProfile	Nein	Ja	Ja
	iam:DeleteInstanceProfile	Nein	Ja	Ja
	iam:PassRole	Ja	Nein	Nein
	ec2:AssociateIamInstanceProfile	Ja	Ja	Nein
	ec2:DescribeIamInstanceProfileAssociations	Ja	Ja	Nein
	ec2:DisassociateIamInstanceProfile	Nein	Ja	Nein
Dekodieren von Autorisierungsstatusmeldungen	sts:DecodeAuthorizationMessage	Ja	Ja	Nein
Beschreiben Sie die angegebenen Bilder (AMIs), die für das Konto verfügbar sind	ec2:DescribeImages	Ja	Ja	Nein
Beschreiben Sie die Routentabellen in einer VPC (nur für HA-Paare erforderlich)	ec2:DescribeRouteTables	Ja	Nein	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Stoppen, Starten und Überwachen von Instanzen	ec2:StartInstances	Ja	Ja	Nein
	ec2:StopInstances	Ja	Ja	Nein
	ec2:DescribeInstances	Ja	Ja	Nein
	ec2:DescribeInstanceStatus	Ja	Ja	Nein
	ec2:RunInstances	Ja	Nein	Nein
	ec2:TerminateInstances	Nein	Nein	Ja
	ec2:ModifyInstanceAttribute	Nein	Ja	Nein
Überprüfen Sie, ob Enhanced Networking für unterstützte Instance-Typen aktiviert ist.	ec2:DescribeInstanceAttribute	Nein	Ja	Nein
Kennzeichnen Sie Ressourcen mit den Tags „WorkingEnvironment“ und „WorkingEnvironmentId“, die für die Wartung und Kostenzuordnung verwendet werden	ec2:CreateTags	Ja	Ja	Nein
Verwalten Sie EBS-Volumes, die Cloud Volumes ONTAP als Backend-Speicher verwendet	ec2:CreateVolume	Ja	Ja	Nein
	ec2:DescribeVolumes	Ja	Ja	Ja
	ec2:ModifyVolumeAttribute	Nein	Ja	Ja
	ec2:AttachVolume	Ja	Ja	Nein
	ec2:DeleteVolume	Nein	Ja	Ja
	ec2:DetachVolume	Nein	Ja	Ja

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und verwalten Sie Sicherheitsgruppen für Cloud Volumes ONTAP	ec2:CreateSecurityGroup	Ja	Nein	Nein
	ec2:DeleteSecurityGroup	Nein	Ja	Ja
	ec2:DescribeSecurityGroups	Ja	Ja	Ja
	ec2:RevokeSecurityGroupEgress	Ja	Nein	Nein
	ec2:AuthorizeSecurityGroupEgress	Ja	Nein	Nein
	ec2:AuthorizeSecurityGroupIngress	Ja	Nein	Nein
	ec2:RevokeSecurityGroupIngress	Ja	Ja	Nein
Erstellen und Verwalten von Netzwerkschnittstellen für Cloud Volumes ONTAP im Zielsubnetz	ec2:CreateNetworkInterface	Ja	Nein	Nein
	ec2:DescribeNetworkInterfaces	Ja	Ja	Nein
	ec2:DeleteNetworkInterface	Nein	Ja	Ja
	ec2:ModifyNetworkInterfaceAttribute	Nein	Ja	Nein
Abrufen der Liste der Zielsubnetze und Sicherheitsgruppen	ec2:DescribeSubnets	Ja	Ja	Nein
	ec2:Vpcs beschreiben	Ja	Ja	Nein
DNS-Server und den Standarddomänennamen für Cloud Volumes ONTAP -Instanzen abrufen	ec2:DescribeDhcpOptions	Ja	Nein	Nein
Erstellen Sie Snapshots von EBS-Volumes für Cloud Volumes ONTAP	ec2:CreateSnapshot	Ja	Ja	Nein
	ec2:DeleteSnapshot	Nein	Ja	Ja
	ec2:DescribeSnapshots	Nein	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erfassen Sie die Cloud Volumes ONTAP Konsole, die an AutoSupport -Nachrichten angehängt ist	ec2:GetConsoleOutput	Ja	Ja	Nein
Holen Sie sich die Liste der verfügbaren Schlüsselpaare	ec2:DescribeKeyPairs	Ja	Nein	Nein
Holen Sie sich die Liste der verfügbaren AWS-Regionen	ec2:DescribeRegions	Ja	Ja	Nein
Verwalten von Tags für Ressourcen, die mit Cloud Volumes ONTAP -Instanzen verknüpft sind	ec2:DeleteTags	Nein	Ja	Ja
	ec2:DescribeTags	Nein	Ja	Nein
Erstellen und Verwalten von Stacks für AWS CloudFormation-Vorlagen	Cloudformation:CreateStack	Ja	Nein	Nein
	Cloudformation:DeleteStack	Ja	Nein	Nein
	Cloudformation:DescribeStacks	Ja	Ja	Nein
	Cloudformation:DescribeStackEvents	Ja	Nein	Nein
	Cloudformation:ValidateTemplate	Ja	Nein	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und verwalten Sie einen S3-Bucket, den ein Cloud Volumes ONTAP System als Kapazitätsebene für das Daten-Tiering verwendet.	s3:Bucket erstellen	Ja	Ja	Nein
	s3:Bucket löschen	Nein	Ja	Ja
	s3:GetLifecycleConfiguration	Nein	Ja	Nein
	s3:PutLifecycleConfiguration	Nein	Ja	Nein
	s3:PutBucketTagging	Nein	Ja	Nein
	s3:ListBucketVersions	Nein	Ja	Nein
	s3:GetBucketPolicyStatus	Nein	Ja	Nein
	s3:GetBucketPublicAccessBlock	Nein	Ja	Nein
	s3:GetBucketAcl	Nein	Ja	Nein
	s3:GetBucketPolicy	Nein	Ja	Nein
	s3:PutBucketPublicAccessBlock	Nein	Ja	Nein
	s3:GetBucketTagging	Nein	Ja	Nein
	s3:GetBucketLocation	Nein	Ja	Nein
	s3:ListeAlleMeineBuckets	Nein	Nein	Nein
	s3:ListBucket	Nein	Ja	Nein
Aktivieren Sie die Datenverschlüsselung von Cloud Volumes ONTAP mithilfe des AWS Key Management Service (KMS).	kms:Neuverschlüsseln*	Ja	Nein	Nein
	kms:CreateGrant	Ja	Ja	Nein
	kms:GenerateDataKeyWithoutPlaintext	Ja	Ja	Nein
Erstellen und verwalten Sie eine AWS-Spread-Placement-Gruppe für zwei HA-Knoten und den Mediator in einer einzigen AWS-Verfügbarkeitszone	ec2:CreatePlacementGroup	Ja	Nein	Nein
	ec2:DeletePlacementGroup	Nein	Ja	Ja

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen von Berichten	fsx:Beschreiben*	Nein	Ja	Nein
	fsx:Liste*	Nein	Ja	Nein
Erstellen und verwalten Sie Aggregate, die die Funktion „Amazon EBS Elastic Volumes“ unterstützen	ec2:DescribeVolumesModifications	Nein	Ja	Nein
	ec2:ModifyVolume	Nein	Ja	Nein
Überprüfen Sie, ob die Availability Zone eine lokale AWS-Zone ist und ob alle Bereitstellungsparameter kompatibel sind.	ec2:DescribeAvailabilityZones	Ja	Nein	Ja

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt oder entfernt werden, vermerken wir dies in den folgenden Abschnitten.

11. November 2025

Die folgenden Berechtigungen sind für NetApp Backup and Recovery nicht mehr erforderlich, es sei denn, Sie verwenden die Legacy-Indexierung. Diese Berechtigungen wurden aus den Richtlinien auf dieser Seite entfernt:

- km:Liste*
- km:Beschreiben*
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- Kleber: Datenbank erstellen
- Kleber: Tabelle erstellen
- Kleber: BatchDeletePartition

9. September 2024

Berechtigungen wurden aus Richtlinie Nr. 2 für Standardregionen entfernt, da die NetApp Console NetApp -Edge-Caching sowie die Erkennung und Verwaltung von Kubernetes-Clustern nicht mehr unterstützt.

Anzeigen der Berechtigungen, die aus der Richtlinie entfernt wurden

```
{
    "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. Mai 2024

Für Cloud Volumes ONTAP ist jetzt die folgende Berechtigung erforderlich:

ec2:DescribeAvailabilityZones

6. Juni 2023

Für Cloud Volumes ONTAP ist jetzt die folgende Berechtigung erforderlich:

kms:GenerateDataKeyWithoutPlaintext

14. Februar 2023

Für NetApp Cloud Tiering ist nun folgende Berechtigung erforderlich:

ec2:DescribeVpcEndpoints

Sicherheitsgruppenregeln für Konsolenagenten in AWS

Die AWS-Sicherheitsgruppe für den Agenten erfordert sowohl eingehende als auch ausgehende Regeln. Die NetApp Console erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Konsolenagenten von der Konsole aus erstellen. Sie müssen diese Sicherheitsgruppe für alle anderen Installationsoptionen einrichten.

Eingehende Regeln

Protokoll	Hafen	Zweck
SSH	22	Bietet SSH-Zugriff auf den Agent-Host
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Upgrade-Prozesses von Cloud Volumes ONTAP verwendet
HTTPS	443	Bietet HTTPS-Zugriff auf die lokale Benutzeroberfläche und Verbindungen von der NetApp Data Classification Instanz
TCP	3128	Bietet Cloud Volumes ONTAP Internetzugang. Sie müssen diesen Port nach der Bereitstellung manuell öffnen.

Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den Agenten öffnet den gesamten ausgehenden Datenverkehr. Wenn das akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Nachrichten. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Ausgangsregeln.

Grundlegende Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den Agenten umfasst die folgenden ausgehenden Regeln.

Protokoll	Hafen	Zweck
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für den ausgehenden Verkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Agenten benötigt werden

Die Quell-IP-Adresse ist der Agent-Host.

Service	Protokoll	Hafen	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster-Management-LIF	API-Aufrufe an AWS, ONTAP, NetApp Data Classification und Senden von AutoSupport -Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP HA-Mediator	Kommunikation mit dem ONTAP HA Mediator
	TCP	8080	Datenklassifizierung	Testen der Datenklassifizierung sinstanz während der Bereitstellung
DNS	UDP	53	DNS	Wird von der Konsole für die DNS-Auflösung verwendet

Azure-Berechtigungen und erforderliche Sicherheitsregeln

Azure-Berechtigungen für den Konsolen-Agent

Wenn die NetApp Console einen Konsolenagenten in Azure startet, weist sie der VM eine benutzerdefinierte Rolle zu, die dem Agenten die Berechtigung zum Verwalten von Ressourcen und Prozessen innerhalb dieses Azure-Abonnements erteilt. Der Agent verwendet die Berechtigungen, um API-Aufrufe an mehrere Azure-Dienste zu tätigen.

Ob Sie diese benutzerdefinierte Rolle für den Agenten erstellen müssen, hängt davon ab, wie Sie sie bereitgestellt haben.

Bereitstellen über die NetApp Console

Wenn Sie die Konsole verwenden, um die Agent-VM in Azure bereitzustellen, ermöglicht dies eine "systemseitig zugewiesene verwaltete Identität" auf der virtuellen Maschine, erstellt eine benutzerdefinierte Rolle und weist sie der virtuellen Maschine zu. Die Rolle stellt der Konsole die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen innerhalb dieses Azure-Abonnements zur Verfügung. Die Berechtigungen der Rolle werden beim Upgrade des Agenten auf dem neuesten Stand gehalten. Sie müssen diese Rolle für den Agenten nicht erstellen oder Updates verwalten.

Manuelle Bereitstellung oder Bereitstellung über den Azure Marketplace

Wenn Sie den Agenten vom Azure Marketplace bereitstellen oder den Agenten manuell auf einem Linux-Host installieren, müssen Sie die benutzerdefinierte Rolle selbst einrichten und ihre Berechtigungen bei allen Änderungen beibehalten.

Sie müssen sicherstellen, dass die Rolle auf dem neuesten Stand ist, da in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. Wenn neue Berechtigungen erforderlich sind, werden diese in den Versionshinweisen aufgeführt.

- Schritt-für-Schritt-Anleitungen zur Verwendung dieser Richtlinien finden Sie auf den folgenden Seiten:
  - "Einrichten von Berechtigungen für eine Azure Marketplace-Bereitstellung"
  - "Einrichten von Berechtigungen für lokale Bereitstellungen"
  - "Berechtigungen für den eingeschränkten Modus einrichten"

```
{
  "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"
}
```

So werden Azure-Berechtigungen verwendet

In den folgenden Abschnitten wird beschrieben, wie die Berechtigungen für jedes NetApp -Speichersystem und jeden Datendienst verwendet werden. Diese Informationen können hilfreich sein, wenn Ihre Unternehmensrichtlinien vorschreiben, dass Berechtigungen nur bei Bedarf erteilt werden.

Azure NetApp Files

Der Agent stellt die folgenden API-Anforderungen, wenn Sie die NetApp Data Classification zum Scannen von Azure NetApp Files -Daten verwenden:

- NetApp/netAppAccounts/read
- 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

In den folgenden Abschnitten wird beschrieben, wie Berechtigungen für NetApp Backup and Recovery verwendet werden.

Minimale NetApp Backup and Recovery

Der Console-Agent stellt die folgenden API-Anfragen für die grundlegende NetApp Backup and Recovery :

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

Nachfolgend finden Sie eine benutzerdefinierte Richtlinie für Sicherung und Wiederherstellung, die mit möglichst wenigen Berechtigungen und einem möglichst engen Geltungsbereich arbeitet:

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

Erweiterte Berechtigungen für Datensicherung und -wiederherstellung

Der Konsolenagent stellt die folgenden API-Anfragen für erweiterte Sicherungs- und Wiederherstellungsvorgänge sowie Such- und Wiederherstellungsfunktionen. Diese Berechtigungen ermöglichen die Verwaltung von Netzwerken, Schlüsseltresoren und verwalteten Identitäten:

- 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/read
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Resources/deployments/delete

Legacy-Berechtigungen für Sicherung und Wiederherstellung

Der Agent führt die folgenden API-Anfragen aus, wenn Sie die Such- und Wiederherstellungsfunktion verwenden. Diese Berechtigungen benötigen Sie nur, wenn Sie vor der Veröffentlichung von Indexing v2 im Februar 2025 ältere Indexierungsfunktionen aktiviert haben:

- 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

Der Agent stellt die folgenden API-Anfragen, wenn Sie die Datenklassifizierung verwenden.

Aktion	Für die Einrichtung verwendet?	Wird es für den täglichen Betrieb verwendet?
Microsoft.Compute/Standorte/Operationen/Lesen	Ja	Ja

Aktion	Für die Einrichtung verwendet?	Wird es für den täglichen Betrieb verwendet?
Microsoft.Compute/locations/vmSizes/read	Ja	Ja
Microsoft.Compute/operations/read	Ja	Ja
Microsoft.Compute/virtualMachines/instanceView/read	Ja	Ja
Microsoft.Compute/virtualMachines/powerOff/action	Ja	Nein
Microsoft.Compute/virtualMachines/read	Ja	Ja
Microsoft.Compute/virtualMachines/restart/action	Ja	Nein
Microsoft.Compute/virtualMachines/start/action	Ja	Nein
Microsoft.Compute/virtualMachines/vmSizes/read	Nein	Ja
Microsoft.Compute/virtualMachines/write	Ja	Nein
Microsoft.Compute/images/read	Ja	Ja
Microsoft.Compute/disks/delete	Ja	Nein
Microsoft.Compute/disks/read	Ja	Ja
Microsoft.Compute/disks/write	Ja	Nein
Microsoft.Storage/checknameavailability/read	Ja	Ja
Microsoft.Storage/operations/read	Ja	Ja
Microsoft.Storage/storageAccounts/listkeys/action	Ja	Nein
Microsoft.Storage/storageAccounts/read	Ja	Ja
Microsoft.Storage/storageAccounts/write	Ja	Nein
Microsoft.Storage/storageAccounts/blobServices/containers/read	Ja	Ja
Microsoft.Network/networkInterfaces/read	Ja	Ja
Microsoft.Network/networkInterfaces/write	Ja	Nein
Microsoft.Network/networkInterfaces/join/action	Ja	Nein

Aktion	Für die Einrichtung verwendet?	Wird es für den täglichen Betrieb verwendet?
Microsoft.Network/networkSecurityGroups/read	Ja	Ja
Microsoft.Network/networkSecurityGroups/write	Ja	Nein
Microsoft.Resources/subscriptions/locations/read	Ja	Ja
Microsoft.Network/locations/operationResults/read	Ja	Ja
Microsoft.Network/locations/operations/read	Ja	Ja
Microsoft.Network/virtualNetworks/read	Ja	Ja
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Ja	Ja
Microsoft.Network/virtualNetworks/subnets/read	Ja	Ja
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Ja	Ja
Microsoft.Network/virtualNetworks/virtualMachines/read	Ja	Ja
Microsoft.Network/virtualNetworks/subnets/join/action	Ja	Nein
Microsoft.Network/virtualNetworks/subnets/write	Ja	Nein
Microsoft.Network/routeTables/join/action	Ja	Nein
Microsoft.Resources/deployments/operations/read	Ja	Ja
Microsoft.Resources/deployments/read	Ja	Ja
Microsoft.Resources/deployments/write	Ja	Nein
Microsoft.Resources/resources/read	Ja	Ja
Microsoft.Resources/subscriptions/operationresults/read	Ja	Ja
Microsoft.Resources/subscriptions/resourceGroups/delete	Ja	Nein
Microsoft.Resources/subscriptions/resourceGroups/read	Ja	Ja

Aktion	Für die Einrichtung verwendet?	Wird es für den täglichen Betrieb verwendet?
Microsoft.Resources/subscriptions/resourcegroups/resources/read	Ja	Ja
Microsoft.Resources/subscriptions/resourceGroups/write	Ja	Nein

Cloud Volumes ONTAP

Der Agent stellt die folgenden API-Anfragen, um Cloud Volumes ONTAP in Azure bereitzustellen und zu verwalten.

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Verwalten von VMs	Microsoft.Compute/Standorte/Operationen/Lesen	Ja	Ja	Nein
	Microsoft.Compute/locations/vmSizes/read	Ja	Ja	Nein
	Microsoft.Resources/subscriptions/locations/read	Ja	Nein	Nein
	Microsoft.Compute/operations/read	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/instanceView/read	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/powerOff/action	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/read	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/restart/action	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/start/action	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/deallocate/action	Nein	Ja	Ja
	Microsoft.Compute/virtualMachines/vmSizes/read	Nein	Ja	Nein
	Microsoft.Compute/virtualMachines/write	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/delete	Ja	Ja	Ja
	Microsoft.Resources/deployments/delete	Ja	Nein	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Aktivieren der Bereitstellung von einer VHD	Microsoft.Compute/images/read	Ja	Nein	Nein
	Microsoft.Compute/images/write	Ja	Nein	Nein
Erstellen und Verwalten von Netzwerkschnittstellen im Zielsubnetz	Microsoft.Network/networkInterfaces/read	Ja	Ja	Nein
	Microsoft.Network/networkInterfaces/write	Ja	Ja	Nein
	Microsoft.Network/networkInterfaces/join/action	Ja	Ja	Nein
	Microsoft.Network/networkInterfaces/delete	Ja	Ja	Nein
Erstellen und Verwalten von Netzwerksicherheitsgruppen	Microsoft.Network/networkSecurityGroups/read	Ja	Ja	Nein
	Microsoft.Network/networkSecurityGroups/write	Ja	Ja	Nein
	Microsoft.Network/networkSecurityGroups/join/action	Ja	Nein	Nein
	Microsoft.Network/networkSecurityGroups/delete	Nein	Ja	Ja

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Abrufen von Netzwerkinformationen zu Regionen, dem Ziel-VNet und Subnetz und Hinzufügen der VMs zu VNets	Microsoft.Network/locations/operationResults/read	Ja	Ja	Nein
	Microsoft.Network/locations/operations/read	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/read	Ja	Nein	Nein
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Ja	Nein	Nein
	Microsoft.Network/virtualNetworks/subnets/read	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/virtualMachines/read	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/subnets/join/action	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Verwalten von Ressourcengruppen	Microsoft.Resources /deployments/operations/read	Ja	Ja	Nein
	Microsoft.Resources /deployments/read	Ja	Ja	Nein
	Microsoft.Resources /deployments/write	Ja	Ja	Nein
	Microsoft.Resources /resources/read	Ja	Ja	Nein
	Microsoft.Resources /subscriptions/operationresults/read	Ja	Ja	Nein
	Microsoft.Resources /subscriptions/resourceGroups/delete	Ja	Ja	Ja
	Microsoft.Resources /subscriptions/resourceGroups/read	Nein	Ja	Nein
	Microsoft.Resources /subscriptions/resourcegroups/resources/read	Ja	Ja	Nein
	Microsoft.Resources /subscriptions/resourceGroups/write	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Verwalten von Azure-Speicherkonten und -Datenträgern	Microsoft.Compute/disks/read	Ja	Ja	Ja
	Microsoft.Compute/disks/write	Ja	Ja	Nein
	Microsoft.Compute/disks/delete	Ja	Ja	Ja
	Microsoft.Storage/checknameavailability/read	Ja	Ja	Nein
	Microsoft.Storage/operations/read	Ja	Ja	Nein
	Microsoft.Storage/storageAccounts/listkeys/action	Ja	Ja	Nein
	Microsoft.Storage/storageAccounts/read	Ja	Ja	Nein
	Microsoft.Storage/storageAccounts/delete	Nein	Ja	Ja
	Microsoft.Storage/storageAccounts/write	Ja	Ja	Nein
	Microsoft.Storage/usages/read	Nein	Ja	Nein
Aktivieren Sie Sicherungen im Blob-Speicher und die Verschlüsselung von Speicherkonten	Microsoft.Storage/storageAccounts/blobServices/containers/read	Ja	Ja	Nein
	Microsoft.KeyVault/vaults/read	Ja	Ja	Nein
	Microsoft.KeyVault/vaults/accessPolicies/write	Ja	Ja	Nein
Aktivieren von VNet-Dienstendpunkten für Datentiering	Microsoft.Network/virtualNetworks/subnets/write	Ja	Ja	Nein
	Microsoft.Network/routeTables/join/action	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Verwalten von Azure-verwalteten Snapshots	Microsoft.Compute/Snapshots/Schreiben	Ja	Ja	Nein
	Microsoft.Compute/snapshots/read	Ja	Ja	Nein
	Microsoft.Compute/snapshots/delete	Nein	Ja	Ja
	Microsoft.Compute/disks/beginGetAccess/action	Nein	Ja	Nein
Erstellen und Verwalten von Verfügbarkeitsgruppen	Microsoft.Compute/availabilitySets/write	Ja	Nein	Nein
	Microsoft.Compute/availabilitySets/read	Ja	Nein	Nein
Aktivieren Sie programmgesteuerte Bereitstellungen vom Marktplatz aus	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read	Ja	Nein	Nein
	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Verwalten eines Load Balancers für HA-Paare	Microsoft.Network/loadBalancers/read	Ja	Ja	Nein
	Microsoft.Network/loadBalancers/write	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/delete	Nein	Ja	Ja
	Microsoft.Network/loadBalancers/backendAddressPools/read	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	Ja	Ja	Nein
	Microsoft.Network/loadBalancers/loadBalancingRules/read	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/probes/read	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/probes/join/action	Ja	Nein	Nein
Aktivieren der Sperrverwaltung auf Azure-Datenträgern	Microsoft.Authorization/locks/*	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Aktivieren Sie private Endpunkte für HA-Paare, wenn außerhalb des Subnetzes keine Konnektivität besteht.	Microsoft.Network/privateEndpoints/write	Ja	Ja	Nein
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	Ja	Nein	Nein
	Microsoft.Storage/storageAccounts/privateEndpointConnections/read	Ja	Ja	Ja
	Microsoft.Network/privateEndpoints/read	Ja	Ja	Ja
	Microsoft.Network/privateDnsZones/write	Ja	Ja	Nein
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/join/action	Ja	Ja	Nein
	Microsoft.Network/privateDnsZones/A/write	Ja	Ja	Nein
	Microsoft.Network/privateDnsZones/read	Ja	Ja	Nein
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	Ja	Ja	Nein
Erforderlich für einige VM-Bereitstellungen, abhängig von der zugrunde liegenden physischen Hardware	Microsoft.Resources/deployments/operationStatuses/read	Ja	Ja	Nein
Entfernen Sie Ressourcen aus einer Ressourcengruppe, falls die Bereitstellung fehlschlägt oder gelöscht wird	Microsoft.Network/privateEndpoints/delete	Ja	Ja	Nein
	Microsoft.Compute/availabilitySets/delete	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Aktivieren Sie die Verwendung von vom Kunden verwalteten Verschlüsselungsschlüsseln bei der Verwendung der API	Microsoft.Compute/diskEncryptionSets/read	Ja	Ja	Ja
	Microsoft.Compute/diskEncryptionSets/write	Ja	Ja	Nein
	Microsoft.KeyVault/vaults/deploy/action	Ja	Nein	Nein
	Microsoft.Compute/diskEncryptionSets/delete	Ja	Ja	Ja
Konfigurieren Sie eine Anwendungssicherheitsgruppe für ein HA-Paar, um die HA-Verbindung und die Cluster-Netzwerk-NICs zu isolieren.	Microsoft.Network/applicationSecurityGroups/write	Nein	Ja	Nein
	Microsoft.Network/applicationSecurityGroups/read	Nein	Ja	Nein
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	Nein	Ja	Nein
	Microsoft.Network/networkSecurityGroups/securityRules/write	Ja	Ja	Nein
	Microsoft.Network/applicationSecurityGroups/delete	Nein	Ja	Ja
	Microsoft.Network/networkSecurityGroups/securityRules/delete	Nein	Ja	Ja
Mit Cloud Volumes ONTAP -Ressourcen verknüpfte Tags lesen, schreiben und löschen	Microsoft.Resources/tags/read	Nein	Ja	Nein
	Microsoft.Resources/tags/write	Ja	Ja	Nein
	Microsoft.Resources/tags/delete	Ja	Nein	Nein
Verschlüsseln von Speicherkonten während der Erstellung	Microsoft.ManagedIdentity/userAssignedIdentities/assign/action	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Verwenden Sie Virtual Machine Scale Sets im flexiblen Orchestrierungsmodus, um bestimmte Zonen für Cloud Volumes ONTAP anzugeben	Microsoft.Compute/virtualMachineScaleSets/write	Ja	Nein	Nein
	Microsoft.Compute/virtualMachineScaleSets/read	Ja	Nein	Nein
	Microsoft.Compute/virtualMachineScaleSets/delete	Nein	Nein	Ja

Abstufung

Der Agent stellt die folgenden API-Anfragen, wenn Sie NetApp Cloud Tiering einrichten.

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

Der Konsolenagent stellt für den täglichen Betrieb die folgenden API-Anfragen.

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

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt oder entfernt werden, vermerken wir dies in den folgenden Abschnitten.

11. November 2025

Es wurde eine benutzerdefinierte JSON-Richtlinie hinzugefügt, die die geringstmöglichen Berechtigungen und den kleinstmöglichen Geltungsbereich widerspiegelt.

Folgende Berechtigungen wurden der minimalen Berechtigungsliste für Sicherung und Wiederherstellung hinzugefügt:

- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

Die folgenden Berechtigungen werden für die Datensicherung und -wiederherstellung nicht mehr benötigt, es sei denn, Sie verwenden die Legacy-Indexierung:

- 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

Die folgenden Berechtigungen wurden in den Abschnitt „Zusätzliche Sicherungs- und Wiederherstellungsberechtigungen“ verschoben, da sie für eine minimale Konfiguration nicht erforderlich sind:

- 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/read
- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write

9. September 2024

Die folgenden Berechtigungen wurden aus der JSON-Richtlinie entfernt, da die Konsole die Erkennung und Verwaltung von Kubernetes-Clustern nicht mehr unterstützt:

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

22. August 2024

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt, da sie für die Cloud Volumes ONTAP Unterstützung von Virtual Machine Scale Sets erforderlich sind:

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

5. Dezember 2023

Die folgenden Berechtigungen werden für NetApp Backup and Recovery beim Sichern von Volumedaten im Azure Blob-Speicher nicht mehr benötigt:

- Microsoft.Compute/virtualMachines/read

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

Diese Berechtigungen sind für andere Konsolenspeicherdienste erforderlich, sodass sie weiterhin in der benutzerdefinierten Rolle für den Agenten verbleiben, wenn Sie diese anderen Speicherdienste verwenden.

12. Mai 2023

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt, da sie für die Verwaltung von Cloud Volumes ONTAP erforderlich sind:

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

Die folgenden Berechtigungen wurden aus der JSON-Richtlinie entfernt, da sie nicht mehr benötigt werden:

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

23. März 2023

Die Berechtigung „Microsoft.Storage/storageAccounts/delete“ wird für die Datenklassifizierung nicht mehr benötigt.

Diese Berechtigung ist für Cloud Volumes ONTAP weiterhin erforderlich.

5. Januar 2023

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt:

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

  Diese Berechtigungen sind für NetApp Backup and Recovery erforderlich.

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

  Diese Berechtigung ist für die Bereitstellung von Cloud Volumes ONTAP erforderlich.

Sicherheitsgruppenregeln für Konsolen-Agents in Azure

Die Azure-Sicherheitsgruppe für den Agenten erfordert sowohl eingehende als auch ausgehende Regeln. Die NetApp Console erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Konsolenagenten von der Konsole aus erstellen. Für andere Installationsoptionen müssen Sie diese Sicherheitsgruppe manuell einrichten.

Eingehende Regeln

Protokoll	Hafen	Zweck
SSH	22	Bietet SSH-Zugriff auf den Agent-Host
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Upgrade-Prozesses von Cloud Volumes ONTAP verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche und Verbindungen von der NetApp Data Classification -Instanz
TCP	3128	Bietet Cloud Volumes ONTAP Internetzugang, um AutoSupport Nachrichten an den NetApp Support zu senden. Sie müssen diesen Port nach der Bereitstellung manuell öffnen. "Erfahren Sie, wie der Agent als Proxy für AutoSupport -Nachrichten verwendet wird"

Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den Agenten öffnet den gesamten ausgehenden Datenverkehr. Wenn das akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Nachrichten. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Ausgangsregeln.

Grundlegende Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den Agenten umfasst die folgenden ausgehenden Regeln.

Protokoll	Hafen	Zweck
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für den ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Agenten erforderlich sind.

Die Quell-IP-Adresse ist der Agent-Host.

Service	Protokoll	Hafen	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster-Management-LIF	API-Aufrufe an Azure, an ONTAP, an NetApp Data Classification und Senden von AutoSupport -Nachrichten an NetApp
API-Aufrufe	TCP	8080	Datenklassifizierung	Testen der Datenklassifizierung sinstanz während der Bereitstellung
DNS	UDP	53	DNS	Wird von der Konsole für die DNS-Auflösung verwendet

Google Cloud-Berechtigungen und erforderliche Firewall-Regeln

Google Cloud-Berechtigungen für den Konsolenagenten

Der Konsolenagent benötigt Berechtigungen zum Ausführen von Aktionen in Google Cloud. Diese Berechtigungen sind in einer benutzerdefinierten Rolle enthalten, die von NetApp bereitgestellt wird. Sie sollten verstehen, was der Agent mit diesen Berechtigungen macht.

Berechtigungen für Google Cloud-Nutzerkonten

Die unten stehende benutzerdefinierte Rolle gewährt einem Google Cloud-Benutzer die erforderlichen Berechtigungen zum Bereitstellen eines Agenten. Weisen Sie diese benutzerdefinierte Rolle dem Benutzer zu, der den Agenten bereitstellen wird.

Google Cloud-Nutzerkontoberechtigungen anzeigen

```
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
```

Dienstkontoberechtigungen

Die unten stehende benutzerdefinierte Rolle weist dem mit dem Console-Agenten verknüpften Google Cloud-Dienstkonto die Berechtigungen zu, die zum Verwalten von Ressourcen und Prozessen in Ihrem Google Cloud-Netzwerk erforderlich sind.

Weisen Sie diese benutzerdefinierte Rolle einem Dienstkonto zu, das mit der Console-Agent-VM verbunden ist.

- "Google Cloud-Berechtigungen für den Standardmodus einrichten"
- "Berechtigungen für den eingeschränkten Modus einrichten"

Google-Dienstkontoberechtigungen anzeigen

Stellen Sie sicher, dass die Rolle auf dem neuesten Stand ist, da in nachfolgenden Versionen neue Berechtigungen hinzugefügt oder entfernt werden. Im Änderungsprotokoll sind alle erforderlichen neuen Berechtigungen aufgeführt."Überprüfen Sie das Änderungsprotokoll der Google-Berechtigungen." "Lesen Sie, wie Sie Google Cloud-Dienstkonten hinzufügen."

```
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
```

So werden Google Cloud-Berechtigungen verwendet

Der Console-Agent nutzt die Berechtigungen in der benutzerdefinierten Rolle, um Cloud Volumes ONTAP Ressourcen und NetApp -Datendienstprozesse in Ihrem Google Cloud-Netzwerk zu verwalten. In den folgenden Abschnitten wird beschrieben, wie der Agent diese Berechtigungen nutzt.

Für Cloud Volumes ONTAP verwendete Berechtigungen

Der Console-Agent nutzt die Berechtigungen in der benutzerdefinierten Rolle, um Cloud Volumes ONTAP Ressourcen und -Prozesse in Ihrem Google Cloud-Netzwerk zu verwalten. In den folgenden Abschnitten wird beschrieben, wie der Agent diese Berechtigungen nutzt.

Berechtigungen für Cloud Volumes ONTAP

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
config.deployments.create	Um die virtuelle Maschineninstanz Cloud Volumes ONTAP mithilfe von Google Cloud Infrastructure Manager bereitzustellen.	Ja	Nein	Nein
config.deployments.delete		Nein	Nein	Ja
config.deployments.deleteState		Nein	Nein	Ja
config.deployments.get		Nein	Ja	Nein
config.deployments.getLock		Nein	Ja	Nein
config.deployments.getState		Nein	Ja	Nein
config.deployments.list		Nein	Ja	Nein
config.deployments.lock		Nein	Ja	Nein
config.deployments.update		Nein	Ja	Nein
config.deployments.updateState		Nein	Ja	Nein
config.operations.get		Nein	Ja	Nein
config.previews.get		Nein	Ja	Nein
config.previews.list		Nein	Ja	Nein
config.resources.list		Nein	Ja	Nein
config.revisions.get		Nein	Ja	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
compute.disks.create	Zum Erstellen und Verwalten von Festplatten für Cloud Volumes ONTAP.	Ja	Ja	Nein
compute.disks.createSnapshot		Nein	Ja	Nein
compute.disks.delete		Nein	Ja	Ja
compute.disks.get		Nein	Ja	Nein
compute.disks.list		Ja	Ja	Nein
compute.disks.setLabels		Ja	Ja	Nein
compute.disks.use		Nein	Ja	Nein
compute.firewalls.create	So erstellen Sie Firewall-Regeln für Cloud Volumes ONTAP.	Ja	Nein	Nein
compute.firewalls.delete		Nein	Ja	Ja
compute.firewalls.get		Ja	Ja	Nein
compute.firewalls.list		Ja	Ja	Nein
compute.forwardingRules.create	Erstellen Sie Weiterleitungsregeln für das Routing des Datenverkehrs zu Backend-Diensten.	Nein	Ja	Nein
compute.forwardingRules.delete	Vorhandene Weiterleitungsregeln löschen.	Nein	Ja	Nein
compute.forwardingRules.get	Details zu bestehenden Weiterleitungsregeln abrufen.	Nein	Ja	Nein
compute.forwardingRules.setLabels	Labels für Weiterleitungsregeln der Organisation festlegen oder aktualisieren.	Nein	Ja	Nein
compute.globalOperations.get	Um den Status von Vorgängen abzurufen.	Ja	Ja	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
compute.healthChecks.create	Erstellung und Verwaltung von Gesundheitsprüfungen zur Überwachung des Zustands der Backend-Dienste.	Nein	Ja	Nein
compute.healthChecks.delete		Nein	Ja	Nein
compute.healthChecks.get		Nein	Ja	Nein
compute.healthChecks.useReadOnly		Nein	Ja	Nein
compute.images.get	Um Bilder für VM-Instanzen zu erhalten.	Ja	Nein	Nein
compute.images.getFromFamily		Ja	Nein	Nein
compute.images.list		Ja	Nein	Nein
compute.images.useReadOnly		Ja	Nein	Nein
compute.instances.attachDisk	So schließen Sie Festplatten an Cloud Volumes ONTAP an und trennen sie davon.	Ja	Ja	Nein
compute.instances.detachDisk		Nein	Ja	Ja
compute.instances.create	Zum Erstellen und Löschen von Cloud Volumes ONTAP VM-Instanzen.	Ja	Nein	Nein
compute.instances.delete		Nein	Nein	Ja
compute.instances.get	Zum Auflisten von VM-Instanzen.	Ja	Ja	Nein
compute.instances.getSerialPortOutput	Um Konsolenprotokolle zu erhalten.	Ja	Ja	Nein
compute.instances.list	Zum Abrufen der Liste der Instanzen in einer Zone.	Ja	Ja	Nein
compute.instances.setDeletionProtection	Um den Löschschutz für die Instanz festzulegen.	Ja	Nein	Nein
compute.instances.setLabels	Um Beschriftungen hinzuzufügen.	Ja	Nein	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
compute.instances.setMachineType	So ändern Sie den Maschinentyp für Cloud Volumes ONTAP.	Ja	Ja	Nein
compute.instances.setMinCpuPlatform		Ja	Ja	Nein
compute.instances.setMetadata	Um Metadaten hinzuzufügen.	Ja	Ja	Nein
compute.instances.setTags	So fügen Sie Tags für Firewall-Regeln hinzu.	Ja	Ja	Nein
compute.instances.start	So starten und stoppen Sie Cloud Volumes ONTAP.	Ja	Ja	Nein
compute.instances.stop		Ja	Ja	Nein
compute.instances.updateDisplayDevice		Ja	Ja	Nein
compute.instances.use	Nutzen Sie virtuelle Maschineninstanzen (Start-, Stopp- und Verbindungsvorgänge).	Nein	Ja	Nein
compute.machineTypes.get	Um die Anzahl der Kerne zu ermitteln und die Quoten zu überprüfen.	Ja	Nein	Nein
compute.projects.get	Zur Unterstützung mehrerer Projekte.	Ja	Nein	Nein
compute.resourcePolicies.create	Ressourcenrichtlinien für die automatisierte Ressourcenverwaltung erstellen und verwalten.	Nein	Ja	Nein
compute.resourcePolicies.delete		Nein	Ja	Nein
compute.resourcePolicies.get		Nein	Ja	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
compute.snapshots.create	Zum Erstellen und Verwalten persistenter Festplatten-Snapshots.	Ja	Ja	Nein
compute.snapshots.delete		Nein	Ja	Ja
compute.snapshots.get		Nein	Ja	Nein
compute.snapshots.list		Nein	Ja	Nein
compute.snapshots.setLabels		Ja	Ja	Nein
compute.networks.get	Um die Netzwerkinformationen zu erhalten, die zum Erstellen einer neuen Cloud Volumes ONTAP VM-Instanz erforderlich sind.	Ja	Ja	Nein
compute.networks.list		Ja	Ja	Nein
compute.regions.get		Ja	Ja	Nein
compute.regions.list		Ja	Ja	Nein
compute.subnetworks.get		Ja	Ja	Nein
compute.subnetworks.list		Ja	Ja	Nein
compute.zoneOperations.get		Ja	Ja	Nein
compute.zones.get		Ja	Ja	Nein
compute.zones.list		Ja	Ja	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
deploymentmanager.compositeTypes.get	So stellen Sie die Cloud Volumes ONTAP VM-Instanz mithilfe von Google Cloud Deployment Manager bereit.	Ja	Nein	Nein
deploymentmanager.compositeTypes.list		Ja	Nein	Nein
deploymentmanager.deployments.create		Ja	Nein	Nein
deploymentmanager.deployments.delete		Ja	Nein	Nein
deploymentmanager.deployments.get		Ja	Nein	Nein
deploymentmanager.deployments.list		Ja	Nein	Nein
deploymentmanager.manifests.get		Ja	Nein	Nein
deploymentmanager.manifests.list		Ja	Nein	Nein
deploymentmanager.operations.get		Ja	Nein	Nein
deploymentmanager.operations.list		Ja	Nein	Nein
deploymentmanager.resources.get		Ja	Nein	Nein
deploymentmanager.resources.list		Ja	Nein	Nein
deploymentmanager.typeProviders.get		Ja	Nein	Nein
deploymentmanager.typeProviders.list		Ja	Nein	Nein
deploymentmanager.types.get		Ja	Nein	Nein
deploymentmanager.types.list		Ja	Nein	Nein
logging.logEntries.list	Um Stack-Log-Laufwerke zu erhalten.	Ja	Ja	Nein
logging.privateLogEntries.list		Ja	Ja	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
logging.logEntries.create	Protokolleinträge erstellen und weiterleiten für Überwachung, Fehlersuche und Prüfung.	Ja	Ja	Nein
logging.logEntries.route		Ja	Ja	Nein
resourcemanager.projects.get	Zur Unterstützung mehrerer Projekte.	Ja	Ja	Nein
storage.buckets.create	So erstellen und verwalten Sie einen Google Cloud Storage-Bucket für die Datenschichtung.	Ja	Ja	Nein
storage.buckets.delete		Nein	Ja	Ja
storage.buckets.get		Nein	Ja	Nein
storage.buckets.list		Nein	Ja	Nein
storage.buckets.update		Nein	Ja	Nein
cloudkms.cryptoKeyVersions.useToEncrypt	So verwenden Sie vom Kunden verwaltete Verschlüsselungsschlüssel vom Cloud Key Management Service mit Cloud Volumes ONTAP.	Ja	Ja	Nein
cloudkms.cryptoKeys.get		Ja	Ja	Nein
cloudkms.cryptoKeys.list		Ja	Ja	Nein
cloudkms.keyRings.list		Ja	Ja	Nein
cloudbuild.builds.get		Ja	Nein	Nein
compute.instances.setServiceAccount	So richten Sie ein Dienstkonto auf der Cloud Volumes ONTAP -Instanz ein. Dieses Dienstkonto bietet Berechtigungen für die Datenschichtung in einem Google Cloud Storage-Bucket.	Ja	Ja	Nein
iam.serviceAccounts.actAs		Ja	Nein	Nein
iam.serviceAccounts.create		Ja	Nein	Nein
iam.serviceAccounts.getIamPolicy		Ja	Ja	Nein
iam.serviceAccounts.list		Ja	Ja	Nein
iam.serviceAccountKeys.create		Ja	Nein	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
storage.objects.create	Objekte (Dateien) im Google Cloud Storage-Bucket erstellen und verwalten.	Ja	Ja	Nein
storage.objects.delete		Nein	Nein	Ja
storage.objects.get		Ja	Ja	Nein
storage.objects.list		Ja	Ja	Nein
compute.addresses.list	Zum Abrufen der Adressen in einer Region beim Bereitstellen eines HA-Paares.	Ja	Nein	Nein
compute.addresses.createInternal	Erstellen Sie interne IP-Adressen innerhalb des VPC-Netzwerks zur Ressourcenzuweisung.	Nein	Ja	Nein
compute.addresses.deleteInternal	Interne IP-Adressen zur Ressourcenbereinigung löschen.	Nein	Ja	Nein
compute.addresses.setLabels	Aktualisieren Sie die Bezeichnungen der Adressressource.	Nein	Ja	Nein
compute.addresses.useInternal	Für die Netzwerkkommunikation interne IP-Adressen verwenden.	Nein	Ja	Nein
compute.backendServices.create	So konfigurieren Sie einen Backend-Dienst zum Verteilen des Datenverkehrs in einem HA-Paar.	Ja	Nein	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
compute.regionBackendServices.create	Backend-Dienste für das Traffic-Routing erstellen und verwalten.	Ja	Nein	Nein
compute.regionBackendServices.delete		Nein	Ja	Nein
compute.regionBackendServices.get		Ja	Nein	Nein
compute.regionBackendServices.update		Ja	Ja	Nein
compute.regionBackendServices.list		Ja	Nein	Nein
compute.regionBackendServices.use		Nein	Ja	Nein
compute.networks.updatePolicy	So wenden Sie Firewall-Regeln auf die VPCs und Subnetze für ein HA-Paar an.	Ja	Nein	Nein
compute.instanceGroups.get	Zum Erstellen und Verwalten von Speicher-VMs auf Cloud Volumes ONTAP HA-Paaren.	Ja	Ja	Nein
compute.addresses.get		Ja	Ja	Nein
compute.instances.updateNetworkInterface		Ja	Ja	Nein
compute.instanceGroups.create		Nein	Ja	Nein
compute.instanceGroups.delete		Nein	Ja	Nein
compute.instanceGroups.update		Nein	Ja	Nein
compute.instanceGroups.use		Nein	Ja	Nein
monitoring.timeSerieslist	Um Informationen zu Google Cloud Storage-Buckets zu erhalten.	Ja	Ja	Nein
storage.buckets.getIamPolicy		Ja	Ja	Nein

Für NetApp Backup and Recovery verwendete Berechtigungen

Der Console-Agent nutzt die Berechtigungen in der benutzerdefinierten Rolle, um NetApp Backup and Recovery Ressourcen und -Prozesse in Ihrem Google Cloud-Netzwerk zu verwalten. In den folgenden Abschnitten wird beschrieben, wie der Agent diese Berechtigungen nutzt.

Berechtigungen für NetApp Backup and Recovery anzeigen

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
• cloudkms.cryptoKeys.get • cloudkms.cryptoKeys.getIamPolicy • cloudkms.cryptoKeys.list • cloudkms.cryptoKeys.setIamPolicy • cloudkms.keyRings.get • cloudkms.keyRings.getIamPolicy • cloudkms.keyRings.list • cloudkms.keyRings.setIamPolicy	So wählen Sie im Aktivierungsassistenten von NetApp Backup and Recovery Ihre eigenen, vom Kunden verwalteten Schlüssel aus, anstatt die standardmäßigen, von Google verwalteten Verschlüsselungsschlüssel zu verwenden.	Ja	Ja	Nein

Für die NetApp Data Classification verwendete Berechtigungen

Der Console-Agent nutzt die Berechtigungen in der benutzerdefinierten Rolle, um NetApp Data Classification Ressourcen und -Prozesse in Ihrem Google Cloud-Netzwerk zu verwalten. In den folgenden Abschnitten wird beschrieben, wie der Agent diese Berechtigungen nutzt.

Berechtigungen für die NetApp Data Classification anzeigen

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
• compute.subnetworks.use • compute.subnetworks.useExternalIp • compute.instances.addAccessConfig	So aktivieren Sie die NetApp Data Classification.	Ja	Nein	Nein

Änderungsprotokoll

Die hinzugefügten und entfernten Berechtigungen sind unten aufgeführt.

8. Dezember 2025

NetApp wechselt von Google Cloud Deployment Manager zu Google Cloud Infrastructure Manager (IM), um den Console-Agenten in Google Cloud bereitzustellen und auszuführen. Um diese Änderung zu unterstützen, wurden die folgenden Berechtigungen hinzugefügt.

Für den Google Cloud-Nutzer, der den Agenten bereitstellt, sind folgende zusätzliche Berechtigungen erforderlich:

- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
- iam.serviceAccount.actAs
- config.deployments.create
- config.operations.get

Für das Dienstkonto in Google Cloud, das für den täglichen Betrieb verwendet wird, sind folgende zusätzliche Berechtigungen erforderlich:

- 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.previews.upload
- config.revisions.getState
- logging.logEntries.create
- storage.objects.create
- storage.objects.delete
- storage.objects.update
- iam.serviceAccounts.get

Für die Bereitstellung von Cloud Volumes ONTAP sind folgende zusätzliche Berechtigungen erforderlich:

- 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.previews.list
- config.revisions.get
- config.resources.list
- iam.serviceAccountKeys.create
- iam.serviceAccounts.create

Für das Dienstkonto, das für den täglichen Betrieb von Cloud Volumes ONTAP verwendet wird, sind die folgenden zusätzlichen Berechtigungen erforderlich.

- compute.addresses.createInternal
- compute.addresses.deleteInternal
- compute.addresses.setLabels
- compute.addresses.useInternal
- compute.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get

- compute.forwardingRules.setLabels
- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.instances.use
- compute.regionBackendServices.delete
- compute.regionBackendServices.update
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- logging.logEntries.route
- config.deployments.create
- config.deployments.delete
- config.deployments.get
- config.deployments.update
- config.revisions.get
- config.deployments.lock
- config.operations.get

26. November 2025

Die Berechtigungen wurden aktualisiert, um ihre Verwendung klarer zu gestalten; es wurden jedoch keine Berechtigungen hinzugefügt oder entfernt. Es wurden drei Spalten hinzugefügt, um anzuzeigen, ob die jeweilige Berechtigung für die Bereitstellung, den täglichen Betrieb oder die Löschung verwendet wird. Darüber hinaus sind einige Berechtigungen nach ihrer Verwendung für NetApp Data Classification und NetApp Backup and Recovery getrennt.

06. Februar 2023

Die folgende Berechtigung wurde dieser Richtlinie hinzugefügt:

- compute.instances.updateNetworkInterface

Diese Berechtigung ist für Cloud Volumes ONTAP erforderlich.

27.01.2023

Folgende Berechtigungen wurden dieser Richtlinie hinzugefügt:

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

Diese Berechtigungen sind für NetApp Backup and Recovery erforderlich.

Agent-Firewallregeln in Google Cloud

Die Google Cloud-Firewallregeln für den Agenten erfordern sowohl eingehende als auch ausgehende Regeln. Die NetApp Console erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Konsolenagenten aus der Konsole erstellen. Für andere Installationsoptionen müssen Sie diese Sicherheitsgruppe manuell einrichten.

Eingehende Regeln

Protokoll	Hafen	Zweck
SSH	22	Bietet SSH-Zugriff auf den Agent-Host
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Upgrade-Prozesses von Cloud Volumes ONTAP verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
TCP	3128	Bietet Cloud Volumes ONTAP Internetzugang. Sie müssen diesen Port nach der Bereitstellung manuell öffnen.

Ausgangsregeln

Die vordefinierten Firewall-Regeln des Agenten öffnen den gesamten ausgehenden Datenverkehr. Befolgen Sie die grundlegenden Ausgangsregeln, sofern dies akzeptabel ist, oder verwenden Sie erweiterte Ausgangsregeln für strengere Anforderungen.

Grundlegende Ausgangsregeln

Die vordefinierten Firewall-Regeln für den Agenten umfassen die folgenden ausgehenden Regeln.

Protokoll	Hafen	Zweck
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für den ausgehenden Datenverkehr benötigen, können Sie die folgenden

Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Agenten erforderlich sind.

Die Quell-IP-Adresse ist der Agent-Host.

Service	Protokoll	Hafen	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster-Management-LIF	API-Aufrufe an Google Cloud, an ONTAP, an NetApp Data Classification und Senden von AutoSupport -Nachrichten an NetApp
API-Aufrufe	TCP	8080	Datenklassifizierung	Testen der Datenklassifizierung sinstanz während der Bereitstellung
DNS	UDP	53	DNS	Wird für die DNS-Auflösung durch Datenklassifizierung verwendet

Erforderlicher Netzwerkzugriff für 3.9.55 und darunter

NetApp Console, der NetApp Console Agent und NetApp Datendienste erfordern ausgehenden Internetzugang, um die erforderlichen Endpunkte zu kontaktieren.

In diesem Thema wird der Netzwerkzugriff dokumentiert, der für Versionen des NetApp Console Standardmodus 3.9.55 und darunter erforderlich ist. Informationen zu den erforderlichen Endpunkten für 4.0.0 und höher finden Sie unter"die erforderlichen Endpunkte für 4.0.0 und höher" .

Sie müssen den Netzwerkzugriff für Folgendes einrichten:

- Computer, die als Software as a Service (SaaS) auf die NetApp Console zugreifen
- Konsolenagenten, die Sie vor Ort oder in der Cloud installieren.

Aktualisieren Sie Ihre Endpunktliste auf die überarbeitete Liste für 4.0.0 und höher

Ab Version 4.0.0 benötigen Konsolenagenten weniger Endpunkte. Vorhandene Bereitstellungen vor 4.0.0 werden weiterhin unterstützt. Nach dem Upgrade auf 4.0.0 oder höher können Sie die alten Endpunkte bei Bedarf aus Ihrer Zulassungsliste entfernen.

NetApp empfiehlt, die Firewall-Regeln zu aktualisieren, um die überarbeitete Endpunktliste zu verwenden, die kleiner, sicherer und einfacher zu verwalten ist. NetApp macht Platzhaltereinträge überflüssig und Endpunkte für Agent-Upgrades unterstützen alle Datendienste.

Endpunkte für Version 3.9.55 und älter	Endpunkte für 4.0.0 und höher	Zweck
• https://support.netapp.com • https://mysupport.netapp.com	• https://mysupport.netapp.com • https://signin.b2c.netapp.com • https://support.netapp.com	Informationen zur Lizenzierung und Kontaktaufnahme mit dem NetApp -Support.
• 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	Für den täglichen Betrieb.
• https://*.blob.core.windows.net • https://cloudmanagerinfraprod.azurecr.io	• https://bluexpinfraprod.eastus2.data.azurecr.io • https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten.

Schritte

1. Stellen Sie sicher, dass Ihr Agent die Version 4.0.0 oder höher hat."Agentenversion anzeigen."
2. Whitelist der Endpunkte in"Unterstützte Endpunkte für 4.0.0 und höher" .
3. Starten Sie den Dienst „Service Manager 2“ auf jedem Agenten neu, indem Sie den folgenden Befehl ausführen:

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

4. Führen Sie den folgenden Befehl aus und überprüfen Sie, ob der Status des Agenten als *aktiv (wird ausgeführt)* angezeigt wird: _

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

5. Entfernen Sie die alten Endpunkte aus der Zulassungsliste Ihrer Firewall.

Endpunkte für NetApp Console und Konsolenagenten für 3.9.55 und darunter

Diese Endpunkte werden für Konsolenagenten 3.9.55 und darunter verwendet.

Endpunkte	Zweck
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
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	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
Wählen Sie zwischen zwei Endpunktsätzen: • Option 1 (empfohlen) https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. NetApp empfiehlt, Endpunkte der Option 1 in Ihrer Firewall zuzulassen, da diese sicherer sind, und Endpunkte der Option 2 nicht zuzulassen, es sei denn, Sie verwenden Ransomware Resilience oder Backup and Recovery. Beachten Sie Folgendes zu diesen Endpunkten: • Endpunkte der Option 1 werden in 3.9.47 und höher unterstützt. Versionen vor 3.9.47 unterstützen keine Abwärtskompatibilität. • Der Konsolenagent initiiert zuerst den Kontakt mit den Endpunkten in Option 2. Wenn diese Endpunkte nicht erreichbar sind, werden automatisch die Endpunkte in Option 1 kontaktiert. • Wenn Sie den Konsolenagenten mit NetApp Backup and Recovery oder Ransomware Resilience verwenden, unterstützt das System keine Endpunkte der Option 1. Erlauben Sie Endpunkte der Option 2 und verbieten Sie Option 1.

Vom Konsolenagenten kontaktierte Cloud-Provider-Endpunkte

Konsolenagenten müssen Zugriff auf zusätzliche Endpunkte haben, wenn diese bei Ihrem Cloud-Anbieter bereitgestellt werden.

Aktivieren Sie den Zugriff auf die Endpunkte des Cloud-Anbieters, bevor Sie den Konsolenagenten installieren.

- "Einrichten des AWS-Netzwerkzugriffs für einen Konsolenagenten"
- "Einrichten des Azure-Netzwerkzugriffs für einen Konsolen-Agent"
- "Einrichten des Google Cloud-Netzwerkzugriffs für einen Konsolenagenten"

Die Endpunkte des Cloud-Anbieters sind für alle Versionen gleich.

Vom Konsolenagenten kontaktierte Datendienstendpunkte

Der Konsolenagent erfordert zusätzlichen ausgehenden Internetzugang, um einige NetApp Datendienste und Cloud Volumes ONTAP zu unterstützen.

Endpunkte für Cloud Volumes ONTAP

- "Endpunkte für Cloud Volumes ONTAP in AWS"
- "Endpunkte für Cloud Volumes ONTAP in Azure"
- "Endpunkte für Cloud Volumes ONTAP in Google Cloud"

Erfordert die Verwendung von IMDSv2 auf Amazon EC2-Instanzen

Die NetApp Console unterstützt den Amazon EC2 Instance Metadata Service Version 2 (IMDSv2) mit dem Konsolenagenten und mit Cloud Volumes ONTAP (einschließlich des Mediators für HA-Bereitstellungen). In den meisten Fällen wird IMDSv2 auf neuen EC2-Instanzen automatisch konfiguriert. IMDSv1 wurde vor März 2024 aktiviert. Falls Ihre Sicherheitsrichtlinien dies erfordern, müssen Sie IMDSv2 möglicherweise manuell auf Ihren EC2-Instances konfigurieren.

Bevor Sie beginnen

- Die Version des Konsolenagenten muss 3.9.38 oder höher sein.
- Cloud Volumes ONTAP muss eine der folgenden Versionen ausführen:
  - 9.12.1 P2 (oder ein nachfolgender Patch)
  - 9.13.0 P4 (oder ein nachfolgender Patch)
  - 9.13.1 oder jede Version nach dieser Veröffentlichung
- Diese Änderung erfordert einen Neustart der Cloud Volumes ONTAP Instanzen.
- Für diese Schritte ist die Verwendung der AWS CLI erforderlich, da Sie das Antwort-Hop-Limit auf 3 ändern müssen.

Informationen zu diesem Vorgang

IMDSv2 bietet verbesserten Schutz vor Schwachstellen. "Weitere Informationen zu IMDSv2 finden Sie im AWS Security Blog"

Der Instance Metadata Service (IMDS) wird auf EC2-Instances wie folgt aktiviert:

- Für neue Konsolen-Agent-Bereitstellungen über die Konsole oder mithilfe von "Terraform-Skripte" , IMDSv2 ist auf der EC2-Instance standardmäßig aktiviert.

- Wenn Sie eine neue EC2-Instanz in AWS starten und dann die Konsolenagent-Software manuell installieren, ist IMDSv2 standardmäßig ebenfalls aktiviert.
- Wenn Sie den Konsolenagenten vom AWS Marketplace aus starten, ist IMDSv1 standardmäßig aktiviert. Sie können IMDSv2 auf der EC2-Instance manuell konfigurieren.
- Für vorhandene Konsolenagenten wird IMDSv1 weiterhin unterstützt, Sie können IMDSv2 jedoch auch manuell auf der EC2-Instance konfigurieren, wenn Sie dies bevorzugen.
- Für Cloud Volumes ONTAP ist IMDSv1 standardmäßig auf neuen und vorhandenen Instanzen aktiviert. Sie können IMDSv2 auf den EC2-Instanzen manuell konfigurieren, wenn Sie dies bevorzugen.

Schritte

1. Erfordert die Verwendung von IMDSv2 auf der Konsolen-Agenteninstanz:

   a. Stellen Sie eine Verbindung zur Linux-VM für den Konsolen-Agenten her.

      Als Sie die Konsolen-Agent-Instanz in AWS erstellt haben, haben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel angegeben. Sie können dieses Schlüsselpaar verwenden, um per SSH auf die Instanz zuzugreifen. Der Benutzername für die EC2-Linux-Instanz ist ubuntu (für Konsolenagenten, die vor Mai 2023 erstellt wurden, war der Benutzername ec2-user).

      "AWS Docs: Verbinden Sie sich mit Ihrer Linux-Instance"

   b. Installieren Sie die AWS CLI.

      "AWS-Dokumente: Installieren oder aktualisieren Sie auf die neueste Version der AWS CLI"

   c. Verwenden Sie die `aws ec2 modify-instance-metadata-options` Befehl, um die Verwendung von IMDSv2 zu verlangen und das Hop-Limit für PUT-Antworten auf 3 zu ändern.

      Beispiel

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

   +

   Der `http-tokens` Der Parameter setzt IMDSv2 auf „erforderlich“. Wann `http-tokens` erforderlich ist, müssen Sie auch `http-endpoint` auf aktiviert.

2. Erfordert die Verwendung von IMDSv2 auf Cloud Volumes ONTAP -Instanzen:

   a. Gehen Sie zum "Amazon EC2-Konsole"

   b. Wählen Sie im Navigationsbereich **Instanzen** aus.

   c. Wählen Sie eine Cloud Volumes ONTAP Instanz aus.

   d. Wählen Sie **Aktionen > Instanzeinstellungen > Optionen für Instanzmetadaten ändern**.

   e. Wählen Sie im Dialogfeld **Optionen für Instanzmetadaten ändern** Folgendes aus:

- Wählen Sie für **Instanzmetadatendienst Aktivieren** aus.
- Wählen Sie für **IMDSv2 Erforderlich** aus.
- Wählen Sie **Speichern**.

f. Wiederholen Sie diese Schritte für andere Cloud Volumes ONTAP Instanzen, einschließlich des HA-Mediators.

g. "Stoppen und starten Sie die Cloud Volumes ONTAP -Instanzen"

Ergebnis

Die Konsolen-Agent-Instanz und die Cloud Volumes ONTAP Instanzen sind jetzt für die Verwendung von IMDSv2 konfiguriert.

Standardkonfiguration für den Konsolenagenten

Erfahren Sie mehr über die Standardkonfigurationen des Console-Agenten für Standardbereitstellungen (mit Internetzugang) in AWS, Azure und Google Cloud sowie für eingeschränkte Bereitstellungen (ohne Internetzugang) in lokalen Umgebungen.

Standardkonfiguration mit Internetzugang

Die folgenden Konfigurationsdetails gelten, wenn Sie einen Konsolenagenten von der NetApp Console oder vom Marktplatz Ihres Cloud-Anbieters bereitgestellt haben oder wenn Sie einen Konsolenagenten manuell auf einem lokalen Linux-Host mit Internetzugang installiert haben.

VM-Details des Konsolenagenten für AWS

Wenn Sie einen Konsolenagenten über die Konsole oder den Marktplatz des Cloud-Anbieters bereitgestellt haben, beachten Sie Folgendes:

- Der EC2-Instanztyp ist t3.2xlarge.
- Das Betriebssystem für das Image ist Ubuntu 22.04 LTS.

  Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Die Installation umfasst Docker Engine, das erforderliche Container-Orchestrierungstool.
- Der Benutzername für die EC2-Linux-Instanz ist ubuntu (für Agenten, die vor Mai 2023 erstellt wurden, lautet der Benutzername ec2-user).
- Die Standardsystemfestplatte ist eine 100-GiB-gp2-Festplatte.

VM-Details des Konsolenagenten für Azure

Wenn Sie einen Konsolenagenten über die Konsole oder den Marktplatz des Cloud-Anbieters bereitgestellt haben, beachten Sie Folgendes:

- Der VM-Typ ist Standard_D8s_v3.
- Das Betriebssystem für das Image ist Ubuntu 22.04 LTS.

  Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Die Installation umfasst Docker Engine, das erforderliche Container-Orchestrierungstool.
- Die Standardsystemfestplatte ist eine 100-GiB-Premium-SSD-Festplatte.

VM-Details des Console-Agenten für Google Cloud

Wenn Sie einen Konsolenagenten über die Konsole bereitgestellt haben, beachten Sie Folgendes:

- Die VM-Instanz ist n2-standard-8.
- Das Betriebssystem für das Image ist Ubuntu 22.04 LTS.

  Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Die Installation umfasst Docker Engine, das erforderliche Container-Orchestrierungstool.
- Die Standardsystemfestplatte ist eine persistente SSD-Festplatte mit 100 GiB.

Installationsordner

Der Ordner für die Agenteninstallation befindet sich an folgendem Speicherort:

`/opt/application/netapp/cloudmanager`

Protokolldateien

Protokolldateien sind in den folgenden Ordnern enthalten:

- `/opt/application/netapp/cloudmanager/log` oder
- `/opt/application/netapp/service-manager-2/logs` (beginnend mit Neuinstallationen der Version 3.9.23)

  Die Protokolle in diesen Ordnern enthalten Details zum Konsolenagenten.

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

  Die Protokolle in diesem Ordner enthalten Details zu Cloud-Diensten und dem Konsolendienst, der auf dem Konsolenagenten ausgeführt wird.

Konsolenagentdienst

- Der Konsolenagentdienst heißt occm.
- Der OCCM-Dienst ist vom MySQL-Dienst abhängig.

  Wenn der MySQL-Dienst ausfällt, fällt auch der OCCM-Dienst aus.

Häfen

Der Agent verwendet die folgenden Ports auf dem Linux-Host:

- 80 für HTTP-Zugriff
- 443 für HTTPS-Zugriff

Standardkonfiguration ohne Internetzugang

Die folgende Konfiguration gilt, wenn Sie den Konsolen-Agent manuell auf einem lokalen Linux-Host installiert haben, der keinen Internetzugang hat. "Erfahren Sie mehr über diese Installationsoption" .

- Der Ordner für die Agenteninstallation befindet sich an folgendem Speicherort:

  `/opt/application/netapp/ds`

- Protokolldateien sind in den folgenden Ordnern enthalten:

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

  Die Protokolle in diesem Ordner enthalten Details zum Konsolenagenten und zu Docker-Images.

- Alle Dienste werden in Docker-Containern ausgeführt

  Die Dienste sind abhängig vom laufenden Docker-Runtime-Dienst

- Der Agent verwendet die folgenden Ports auf dem Linux-Host:
  - 80 für HTTP-Zugriff
  - 443 für HTTPS-Zugriff