Erste Schritte mit der NetApp Console (eingeschränkter Modus)

NetApp Console setup and administration

NetApp
February 11, 2026

Inhalt

Erste Schritte mit der NetApp Console (eingeschränkter Modus)

Workflow „Erste Schritte“ (eingeschränkter Modus)

Beginnen Sie mit der NetApp Console im eingeschränkten Modus, indem Sie Ihre Umgebung vorbereiten und den Konsolen-Agenten bereitstellen.

Der eingeschränkte Modus wird normalerweise von staatlichen und lokalen Behörden sowie regulierten Unternehmen verwendet, einschließlich Bereitstellungen in AWS GovCloud- und Azure Government-Regionen. Bevor Sie beginnen, stellen Sie sicher, dass Sie Folgendes verstehen:"Konsolenagenten" Und"Bereitstellungsmodi" .

1 "Vorbereiten der Bereitstellung"

1. Bereiten Sie einen dedizierten Linux-Host vor, der die Anforderungen hinsichtlich CPU, RAM, Speicherplatz, Container-Orchestrierungstool und mehr erfüllt.
2. Richten Sie ein Netzwerk ein, das Zugriff auf die Zielnetzwerke, ausgehenden Internetzugang für manuelle Installationen und ausgehendes Internet für den täglichen Zugriff bietet.
3. Richten Sie Berechtigungen bei Ihrem Cloud-Anbieter ein, damit Sie diese Berechtigungen nach der Bereitstellung der Konsolen-Agentinstanz zuordnen können.

2 "Bereitstellen des Konsolenagenten"

1. Installieren Sie den Konsolenagenten vom Marktplatz Ihres Cloud-Anbieters oder indem Sie die Software manuell auf Ihrem eigenen Linux-Host installieren.
2. Richten Sie die NetApp Console ein, indem Sie einen Webbrowser öffnen und die IP-Adresse des Linux-Hosts eingeben.
3. Geben Sie dem Konsolenagenten die Berechtigungen, die Sie zuvor eingerichtet haben.

3 "Abonnieren Sie NetApp Intelligent Services (optional)"

Optional: Abonnieren Sie NetApp Intelligent Services über den Marktplatz Ihres Cloud-Anbieters, um Datendienste zu einem Stundensatz (PAYGO) oder über einen Jahresvertrag zu bezahlen. Zu den NetApp Intelligent Services gehören NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience und NetApp Disaster Recovery. Die NetApp Data Classification ist ohne zusätzliche Kosten in Ihrem Abonnement enthalten.

Vorbereiten der Bereitstellung im eingeschränkten Modus

Bereiten Sie Ihre Umgebung vor, bevor Sie die NetApp Console im eingeschränkten Modus bereitstellen. Sie müssen die Hostanforderungen überprüfen, das Netzwerk vorbereiten, Berechtigungen einrichten und vieles mehr.

Schritt 1: Verstehen, wie der eingeschränkte Modus funktioniert

Machen Sie sich vor dem Start mit der Funktionsweise der NetApp Console im eingeschränkten Modus vertraut.

Verwenden Sie die browserbasierte Schnittstelle, die lokal über den installierten NetApp Console Agenten verfügbar ist. Sie können nicht über die webbasierte Konsole, die über die SaaS-Schicht bereitgestellt wird, auf die NetApp Console zugreifen.

Darüber hinaus sind nicht alle Konsolenfunktionen und NetApp Datendienste verfügbar.

"Erfahren Sie, wie der eingeschränkte Modus funktioniert" .

Schritt 2: Überprüfen der Installationsoptionen

Im eingeschränkten Modus können Sie den Konsolenagenten nur in der Cloud installieren. Folgende Installationsoptionen stehen zur Verfügung:

- Aus dem AWS Marketplace
- Aus dem Azure Marketplace
- Manuelle Installation des Konsolen-Agenten auf Ihrem eigenen Linux-Host, der in AWS, Azure oder Google Cloud ausgeführt wird

Schritt 3: Hostanforderungen prüfen

Ein Host muss bestimmte Betriebssystem-, RAM- und Portanforderungen erfüllen, um den Konsolenagenten auszuführen.

Wenn Sie den Konsolenagenten vom AWS- oder Azure Marketplace bereitstellen, enthält das Image die erforderlichen Betriebssystem- und Softwarekomponenten. Sie müssen lediglich einen Instanztyp auswählen, der die CPU- und RAM-Anforderungen erfüllt.

Dedizierter Host

Der Konsolenagent benötigt einen dedizierten Host. Jede Architektur wird unterstützt, sofern sie diese Größenanforderungen erfüllt:

- CPU: 8 Kerne oder 8 vCPUs
- Arbeitsspeicher: 32 GB
- Festplattenspeicher: Für den Host werden 165 GB empfohlen, mit den folgenden Partitionsanforderungen:
  - `/opt`: 120 GiB Speicherplatz müssen verfügbar sein

    Der Agent verwendet `/opt` zur Installation des `/opt/application/netapp` Verzeichnis und dessen Inhalt.

  - `/var`: 40 GiB Speicherplatz müssen verfügbar sein

    Der Konsolenagent benötigt diesen Speicherplatz. `/var` weil Podman oder Docker so konzipiert sind, dass die Container in diesem Verzeichnis erstellt werden. Konkret werden sie Container erstellen in der `/var/lib/containers/storage` Verzeichnis und `/var/lib/docker` für Docker. Externe Mounts oder Symlinks funktionieren für diesen Bereich nicht.

AWS EC2-Instanztyp

Ein Instanztyp, der die CPU- und RAM-Anforderungen erfüllt. NetApp empfiehlt t3.2xlarge.

Azure-VM-Größe

Ein Instanztyp, der die CPU- und RAM-Anforderungen erfüllt. NetApp empfiehlt Standard_D8s_v3.

Google Cloud-Maschinentyp

Ein Instanztyp, der die CPU- und RAM-Anforderungen erfüllt. NetApp empfiehlt n2-standard-8.

Der Konsolenagent wird in Google Cloud auf einer VM-Instanz mit einem Betriebssystem unterstützt, das "Funktionen von Shielded VM"

Hypervisor

Es ist ein Bare-Metal- oder gehosteter Hypervisor erforderlich, der für die Ausführung eines unterstützten Betriebssystems zertifiziert ist.

Betriebssystem- und Containeranforderungen

Der Konsolenagent wird von den folgenden Betriebssystemen unterstützt, wenn die Konsole im Standardmodus oder eingeschränkten Modus verwendet wird. Vor der Installation des Agenten ist ein Container-Orchestrierungstool erforderlich.

Betriebssystem	Unterstützte Betriebssystemversionen	Unterstützte Agent-Versionen	Erforderliches Container-Tool	SELinux
Red Hat Enterprise Linux		9,6 • Nur englischsprachige Versionen. • Der Host muss bei Red Hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann der Host während der Agenteninstallation nicht auf Repositories zugreifen, um erforderliche Software von Drittanbietern zu aktualisieren.	4.0.0 oder höher mit der Konsole im Standardmodus oder eingeschränkten Modus	Podman Version 5.4.0 mit podman-compose 1.5.0. Podman-Konfigurationsanforderungen anzeigen .

Betriebssystem	Unterstützte Betriebssystemversionen	Unterstützte Agent-Versionen	Erforderliches Container-Tool	SELinux
Unterstützt im Durchsetzungsmodus oder im Permissivmodus		9,1 bis 9,4 • Nur englischsprachige Versionen. • Der Host muss bei Red Hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann der Host während der Agenteninstallation nicht auf Repositories zugreifen, um erforderliche Software von Drittanbietern zu aktualisieren.	3.9.50 oder höher mit der Konsole im Standardmodus oder eingeschränkten Modus	Podman Version 4.9.4 mit podman-compose 1.5.0. Podman-Konfigurationsanforderungen anzeigen .
Unterstützt im Durchsetzungsmodus oder im Permissivmodus		8,6 bis 8,10 • Nur englischsprachige Versionen. • Der Host muss bei Red Hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann der Host während der Agenteninstallation nicht auf Repositories zugreifen, um erforderliche Software von Drittanbietern zu aktualisieren.	3.9.50 oder höher mit der Konsole im Standardmodus oder eingeschränkten Modus	Podman Version 4.6.1 oder 4.9.4 mit podman-compose 1.0.6. Podman-Konfigurationsanforderungen anzeigen .

Betriebssystem	Unterstützte Betriebssystemversionen	Unterstützte Agent-Versionen	Erforderliches Container-Tool	SELinux
Unterstützt im Durchsetzungsmodus oder im Permissivmodus	Ubuntu		24,04 LTS	3.9.45 oder höher mit der NetApp Console im Standardmodus oder eingeschränkten Modus
Docker Engine 23.06 bis 28.0.0.	Nicht unterstützt		22,04 LTS	3.9.50 oder höher

Schritt 4: Installieren Sie Podman oder Docker Engine

Um den Konsolenagenten manuell zu installieren, bereiten Sie den Host vor, indem Sie Podman oder Docker Engine installieren.

Abhängig von Ihrem Betriebssystem ist vor der Installation des Agenten entweder Podman oder Docker Engine erforderlich.

- Podman wird für Red Hat Enterprise Linux 8 und 9 benötigt.

  Sehen Sie sich die unterstützten Podman-Versionen an .

- Für Ubuntu ist Docker Engine erforderlich.

  Anzeigen der unterstützten Docker Engine-Versionen .

Beispiel 1. Schritte

Podman

Befolgen Sie diese Schritte, um Podman zu installieren und zu konfigurieren:

- Aktivieren und starten Sie den Dienst podman.socket
- Installieren Sie Python3
- Installieren Sie das Podman-Compose-Paket Version 1.0.6
- Fügen Sie podman-compose zur Umgebungsvariablen PATH hinzu
- Wenn Sie Red Hat Enterprise Linux verwenden, überprüfen Sie, ob Ihre Podman-Version Netavark Aardvark DNS anstelle von CNI verwendet

Passen Sie den Aardvark-DNS-Port (Standard: 53) nach der Installation des Agenten an, um DNS-Portkonflikte zu vermeiden. Befolgen Sie die Anweisungen zum Konfigurieren des Ports.

Schritte

1. Entfernen Sie das Podman-Docker-Paket, falls es auf dem Host installiert ist.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Installieren Sie Podman.

   Sie können Podman aus den offiziellen Red Hat Enterprise Linux-Repositories beziehen.

   a. Für Red Hat Enterprise Linux 9,6:

   ```
   sudo dnf install podman-5:<version>
   ```

   Dabei ist <Version> die unterstützte Version von Podman, die Sie installieren. Sehen Sie sich die unterstützten Podman-Versionen an .

   b. Für Red Hat Enterprise Linux 9.1 bis 9.4:

   ```
   sudo dnf install podman-4:<version>
   ```

   Dabei ist <Version> die unterstützte Version von Podman, die Sie installieren. Sehen Sie sich die unterstützten Podman-Versionen an .

   c. Für Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-4:<version>
   ```

   Dabei ist <Version> die unterstützte Version von Podman, die Sie installieren. Sehen Sie sich die

unterstützten Podman-Versionen an .

3. Aktivieren und starten Sie den Dienst podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Installieren Sie python3.

```
sudo dnf install python3
```

5. Installieren Sie das EPEL-Repository-Paket, falls es auf Ihrem System noch nicht verfügbar ist.

   Dieser Schritt ist erforderlich, da podman-compose im Repository „Extra Packages for Enterprise Linux“ (EPEL) verfügbar ist.

6. Bei Verwendung von Red Hat Enterprise 9:

   a. Installieren Sie das EPEL-Repository-Paket.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. Installieren Sie das Podman-Compose-Paket 1.5.0.

```
sudo dnf install podman-compose-1.5.0
```

7. Bei Verwendung von Red Hat Enterprise Linux 8:

   a. Installieren Sie das EPEL-Repository-Paket.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. Installieren Sie das Podman-Compose-Paket 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```

> Verwenden des `dnf install` Der Befehl erfüllt die Anforderung zum Hinzufügen von „podman-compose“ zur Umgebungsvariablen PATH. Der Installationsbefehl fügt podman-compose zu /usr/bin hinzu, das bereits im `secure_path` Option auf dem Host.

c. Wenn Sie Red Hat Enterprise Linux 8 verwenden, überprüfen Sie, ob Ihre Podman-Version NetAvark mit Aardvark DNS anstelle von CNI verwendet.

i. Überprüfen Sie, ob Ihr Netzwerk-Backend auf CNI eingestellt ist, indem Sie den folgenden Befehl ausführen:

```
podman info | grep networkBackend
```

ii. Wenn das Netzwerk-Backend auf `CNI` , müssen Sie es ändern in `netavark` .

iii. Installieren `netavark` Und `aardvark-dns` mit dem folgenden Befehl:

```
dnf install aardvark-dns netavark
```

iv. Öffnen Sie die `/etc/containers/containers.conf` Datei und ändern Sie die Option network_backend, um „netavark“ anstelle von „cni“ zu verwenden.

Wenn `/etc/containers/containers.conf` nicht vorhanden ist, nehmen Sie die Konfigurationsänderungen vor, um `/usr/share/containers/containers.conf` .

v. Starten Sie Podman neu.

```
systemctl restart podman
```

vi. Bestätigen Sie mit dem folgenden Befehl, dass networkBackend jetzt in „netavark“ geändert wurde:

```
podman info | grep networkBackend
```

Docker-Engine

Befolgen Sie die Dokumentation von Docker, um Docker Engine zu installieren.

Schritte

1. "Installationsanweisungen von Docker anzeigen"

   Befolgen Sie die Schritte, um eine unterstützte Docker Engine-Version zu installieren. Installieren Sie nicht die neueste Version, da diese von der Konsole nicht unterstützt wird.

2. Stellen Sie sicher, dass Docker aktiviert und ausgeführt wird.

```
sudo systemctl enable docker && sudo systemctl start docker
```

Schritt 5: Netzwerkzugriff vorbereiten

Richten Sie den Netzwerkzugriff ein, damit der Konsolenagent Ressourcen in Ihrer öffentlichen Cloud verwalten kann. Zusätzlich zum Vorhandensein eines virtuellen Netzwerks und Subnetzes für den Konsolenagenten müssen Sie sicherstellen, dass die folgenden Anforderungen erfüllt sind.

Verbindungen zu Zielnetzwerken

Stellen Sie sicher, dass der Konsolenagent über eine Netzwerkverbindung zu den Speicherorten verfügt. Beispielsweise das VPC oder VNet, in dem Sie Cloud Volumes ONTAP bereitstellen möchten, oder das Rechenzentrum, in dem sich Ihre lokalen ONTAP Cluster befinden.

Vorbereiten des Netzwerks für den Benutzerzugriff auf die NetApp Console

Im eingeschränkten Modus greifen Benutzer über die Konsolen-Agent-VM auf die Konsole zu. Der Konsolenagent kontaktiert einige Endpunkte, um Datenverwaltungsaufgaben abzuschließen. Diese Endpunkte werden vom Computer eines Benutzers aus kontaktiert, wenn bestimmte Aktionen von der Konsole aus ausgeführt werden.

Konsolenagenten vor Version 4.0.0 benötigen zusätzliche Endpunkte. Wenn Sie auf 4.0.0 oder höher aktualisiert haben, können Sie die alten Endpunkte aus Ihrer Zulassungsliste entfernen."Erfahren Sie mehr über den erforderlichen Netzwerkzugriff für Versionen vor 4.0.0."

+

Endpunkte	Zweck
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	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://cdn.auth0.com https://services.cloud.netapp.com	Ihr Webbrowser stellt über die NetApp Console eine Verbindung zu diesen Endpunkten her, um eine zentrale Benutzerauthentifizierung durchzuführen.

Ausgehender Internetzugang für den täglichen Betrieb

Der Netzwerkstandort des Konsolenagenten muss über ausgehenden Internetzugang verfügen. Es muss in der Lage sein, die SaaS-Dienste der NetApp Console sowie Endpunkte innerhalb Ihrer jeweiligen öffentlichen Cloud-Umgebung zu erreichen.

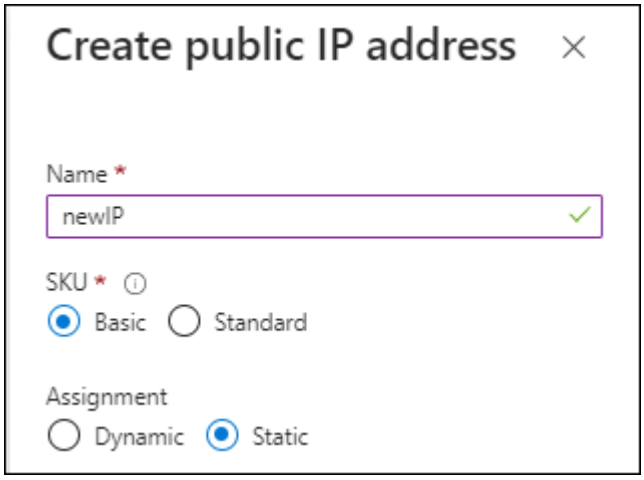
Endpunkte	Zweck
AWS-Umgebungen	AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)
Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab. "Weitere Einzelheiten finden Sie in der AWS-Dokumentation."	Amazon FsX für NetApp ONTAP: • api.workloads.netapp.com
Die webbasierte Konsole kontaktiert diesen Endpunkt, um mit den Workload Factory APIs zu interagieren und so FSx for ONTAP basierte Workloads zu verwalten und zu betreiben.	**Azure-Umgebungen**
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Zum Verwalten von Ressourcen in öffentlichen Azure-Regionen.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Zum Verwalten von Ressourcen in Azure Government-Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Zum Verwalten von Ressourcen in Azure China-Regionen.
Google Cloud-Umgebungen	https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://config.googleapis.com/v1/projects

Endpunkte	Zweck
Zum Verwalten von Ressourcen in Google Cloud.	• NetApp Console -Endpunkte*
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
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	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.

Endpunkte	Zweck
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. • Wenn Sie einen neuen Agenten bereitstellen, testet die Validierungsprüfung die Konnektivität zu aktuellen Endpunkten. Wenn Sie"vorherige Endpunkte" , schlägt die Validierungsprüfung fehl. Um diesen Fehler zu vermeiden, überspringen Sie die Validierungsprüfung. Obwohl die vorherigen Endpunkte weiterhin unterstützt werden, empfiehlt NetApp , Ihre Firewall-Regeln so schnell wie möglich auf die aktuellen Endpunkte zu aktualisieren. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" . • Wenn Sie auf die aktuellen Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Öffentliche IP-Adresse in Azure

Wenn Sie eine öffentliche IP-Adresse mit der Konsolen-Agent-VM in Azure verwenden möchten, muss die IP-Adresse eine Basic-SKU verwenden, um sicherzustellen, dass die Konsole diese öffentliche IP-Adresse verwendet.



Wenn Sie stattdessen eine Standard-SKU-IP-Adresse verwenden, verwendet die Konsole die *private* IP-

Adresse des Konsolenagenten anstelle der öffentlichen IP. Wenn der Computer, den Sie für den Zugriff auf die Konsole verwenden, keinen Zugriff auf diese private IP-Adresse hat, schlagen Aktionen von der Konsole fehl.

"Azure-Dokumentation: Öffentliche IP-SKU"

Proxyserver

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Wenn Sie einen transparenten Proxy verwenden, müssen Sie nur das Zertifikat für den Proxyserver angeben. Wenn Sie einen expliziten Proxy verwenden, benötigen Sie auch die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

Es gibt keinen eingehenden Datenverkehr zum Konsolenagenten, es sei denn, Sie initiieren ihn oder er wird als Proxy zum Senden von AutoSupport Nachrichten von Cloud Volumes ONTAP an den NetApp Support verwendet.

- HTTP (80) und HTTPS (443) ermöglichen den Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) wird nur benötigt, wenn Sie zur Fehlerbehebung eine Verbindung zum Host herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP -Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

  Wenn Cloud Volumes ONTAP -Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport Nachrichten haben, konfiguriert die Konsole diese Systeme automatisch für die Verwendung eines Proxyservers, der im Konsolenagenten enthalten ist. Die einzige Voraussetzung besteht darin, sicherzustellen, dass die Sicherheitsgruppe des Konsolenagenten eingehende Verbindungen über Port 3128 zulässt. Sie müssen diesen Port öffnen, nachdem Sie den Konsolenagenten bereitgestellt haben.

Aktivieren von NTP

Wenn Sie NetApp Data Classification zum Scannen Ihrer Unternehmensdatenquellen verwenden möchten, sollten Sie sowohl auf dem Konsolenagenten als auch auf dem NetApp Data Classification -System einen Network Time Protocol (NTP)-Dienst aktivieren, damit die Zeit zwischen den Systemen synchronisiert wird. "Erfahren Sie mehr über die NetApp Datenklassifizierung"

Wenn Sie vorhaben, einen Konsolen-Agenten aus dem Marktplatz Ihres Cloud-Anbieters zu erstellen, implementieren Sie diese Netzwerkanforderung, nachdem Sie den Konsolen-Agenten erstellt haben.

Schritt 6: Cloud-Berechtigungen vorbereiten

Der Konsolenagent benötigt Berechtigungen von Ihrem Cloud-Anbieter, um Cloud Volumes ONTAP in einem virtuellen Netzwerk bereitzustellen und NetApp -Datendienste zu verwenden. Sie müssen Berechtigungen bei Ihrem Cloud-Anbieter einrichten und diese Berechtigungen dann dem Konsolenagenten zuordnen.

Um die erforderlichen Schritte anzuzeigen, wählen Sie die Authentifizierungsoption aus, die für Ihren Cloud-Anbieter verwendet werden soll.

AWS IAM-Rolle

Verwenden Sie eine IAM-Rolle, um dem Konsolenagenten Berechtigungen zu erteilen.

Wenn Sie den Konsolenagenten vom AWS Marketplace aus erstellen, werden Sie beim Starten der EC2-Instance aufgefordert, diese IAM-Rolle auszuwählen.

Wenn Sie den Konsolenagenten manuell auf Ihrem eigenen Linux-Host installieren, fügen Sie die Rolle der EC2-Instance hinzu.

Schritte

1. Melden Sie sich bei der AWS-Konsole an und navigieren Sie zum IAM-Dienst.
2. Erstellen Sie eine Richtlinie:
   a. Wählen Sie **Richtlinien > Richtlinie erstellen**.
   b. Wählen Sie **JSON** und kopieren und fügen Sie den Inhalt des"IAM-Richtlinie für den Konsolenagenten" .
   c. Führen Sie die restlichen Schritte aus, um die Richtlinie zu erstellen.
3. Erstellen Sie eine IAM-Rolle:
   a. Wählen Sie **Rollen > Rolle erstellen**.
   b. Wählen Sie **AWS-Dienst > EC2**.
   c. Fügen Sie Berechtigungen hinzu, indem Sie die gerade erstellte Richtlinie anhängen.
   d. Führen Sie die restlichen Schritte aus, um die Rolle zu erstellen.

Ergebnis

Sie verfügen jetzt über eine IAM-Rolle für die EC2-Instanz des Konsolenagenten.

AWS-Zugriffsschlüssel

Richten Sie Berechtigungen und einen Zugriffsschlüssel für einen IAM-Benutzer ein. Sie müssen der Konsole den AWS-Zugriffsschlüssel bereitstellen, nachdem Sie den Konsolenagenten installiert und die Konsole eingerichtet haben.

Schritte

1. Melden Sie sich bei der AWS-Konsole an und navigieren Sie zum IAM-Dienst.
2. Erstellen Sie eine Richtlinie:
   a. Wählen Sie **Richtlinien > Richtlinie erstellen**.
   b. Wählen Sie **JSON** und kopieren und fügen Sie den Inhalt des"IAM-Richtlinie für den Konsolenagenten" .
   c. Führen Sie die restlichen Schritte aus, um die Richtlinie zu erstellen.

      Abhängig von den NetApp -Datendiensten, die Sie verwenden möchten, müssen Sie möglicherweise eine zweite Richtlinie erstellen.

   Für Standardregionen sind die Berechtigungen auf zwei Richtlinien verteilt. Aufgrund einer maximalen Zeichengrößenbeschränkung für verwaltete Richtlinien in AWS sind zwei Richtlinien erforderlich. "Weitere Informationen zu IAM-Richtlinien für den Konsolenagenten" .
3. Hängen Sie die Richtlinien an einen IAM-Benutzer an.

- "AWS-Dokumentation: Erstellen von IAM-Rollen"
- "AWS-Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"

4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie der NetApp Console hinzufügen können, nachdem Sie den Konsolen-Agenten installiert haben.

Azure-Rolle

Erstellen Sie eine benutzerdefinierte Azure-Rolle mit den erforderlichen Berechtigungen. Sie weisen diese Rolle der Konsolen-Agent-VM zu.

Beachten Sie, dass Sie eine benutzerdefinierte Azure-Rolle mithilfe des Azure-Portals, Azure PowerShell, Azure CLI oder REST-API erstellen können. Die folgenden Schritte zeigen, wie Sie die Rolle mithilfe der Azure CLI erstellen. Wenn Sie eine andere Methode bevorzugen, lesen Sie bitte "Azure-Dokumentation"

Schritte

1. Wenn Sie die Software manuell auf Ihrem eigenen Host installieren möchten, aktivieren Sie eine systemseitig zugewiesene verwaltete Identität auf der VM, damit Sie die erforderlichen Azure-Berechtigungen über eine benutzerdefinierte Rolle bereitstellen können.

   "Microsoft Azure-Dokumentation: Konfigurieren verwalteter Identitäten für Azure-Ressourcen auf einer VM mithilfe des Azure-Portals"

2. Kopieren Sie den Inhalt der"benutzerdefinierte Rollenberechtigungen für den Connector" und speichern Sie sie in einer JSON-Datei.
3. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

   Sie sollten die ID für jedes Azure-Abonnement hinzufügen, das Sie mit der NetApp Console verwenden möchten.

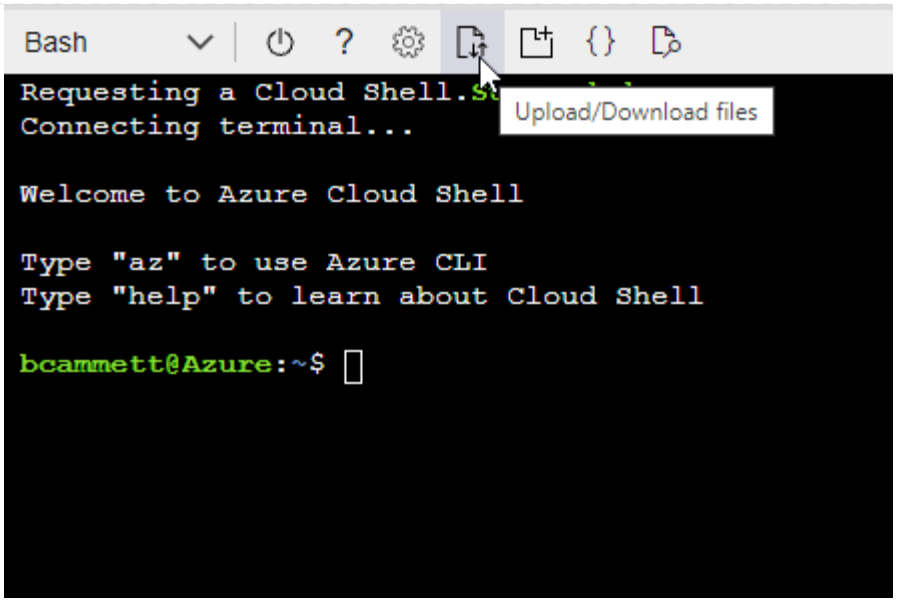
   Beispiel

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ]
   ```

4. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

   Die folgenden Schritte beschreiben, wie Sie die Rolle mithilfe von Bash in Azure Cloud Shell erstellen.

   a. Start "Azure Cloud Shell" und wählen Sie die Bash-Umgebung.
   b. Laden Sie die JSON-Datei hoch.



c. Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
az role definition create --role-definition agent_Policy.json
```

Azure-Dienstprinzipal

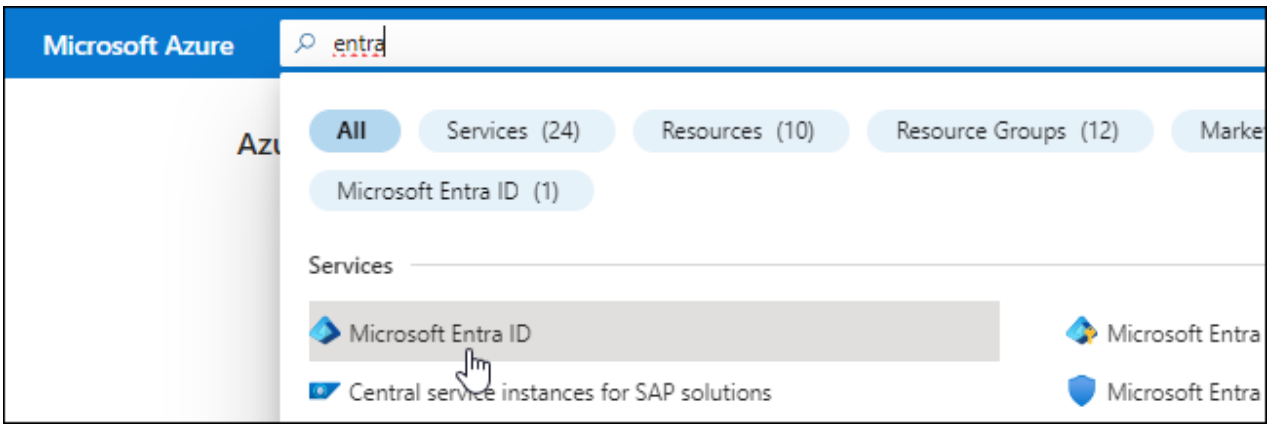
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die die Konsole benötigt. Sie müssen der Konsole diese Anmeldeinformationen bereitstellen, nachdem Sie den Konsolenagenten installiert haben.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffskontrolle

1. Stellen Sie sicher, dass Sie in Azure über die Berechtigung verfügen, eine Active Directory-Anwendung zu erstellen und die Anwendung einer Rolle zuzuweisen.

   Weitere Einzelheiten finden Sie unter "Microsoft Azure-Dokumentation: Erforderliche Berechtigungen"

2. Öffnen Sie im Azure-Portal den Dienst **Microsoft Entra ID**.



3. Wählen Sie im Menü **App-Registrierungen** aus.
4. Wählen Sie **Neuregistrierung**.

5. Geben Sie Details zur Anwendung an:
   - **Name**: Geben Sie einen Namen für die Anwendung ein.
   - **Kontotyp**: Wählen Sie einen Kontotyp aus (alle funktionieren mit der NetApp Console).
   - **Umleitungs-URI**: Sie können dieses Feld leer lassen.
6. Wählen Sie **Registrieren**.

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der Anwendung zu einer Rolle

1. Erstellen Sie eine benutzerdefinierte Rolle:

   Beachten Sie, dass Sie eine benutzerdefinierte Azure-Rolle mithilfe des Azure-Portals, Azure PowerShell, Azure CLI oder REST-API erstellen können. Die folgenden Schritte zeigen, wie Sie die Rolle mithilfe der Azure CLI erstellen. Wenn Sie eine andere Methode bevorzugen, lesen Sie bitte "Azure-Dokumentation"

   a. Kopieren Sie den Inhalt der"benutzerdefinierte Rollenberechtigungen für den Konsolenagenten" und speichern Sie sie in einer JSON-Datei.

   b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

      Sie sollten die ID für jedes Azure-Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP -Systeme erstellen.

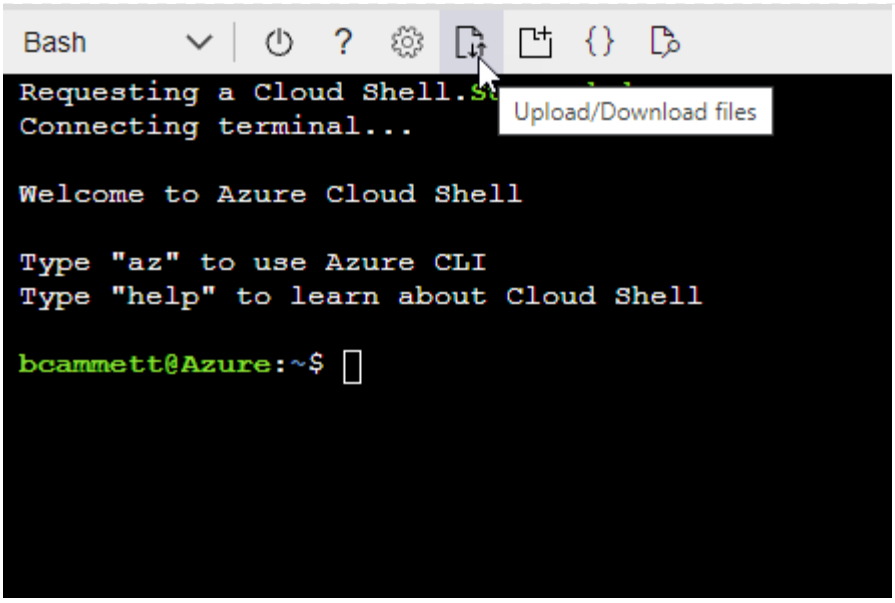
      Beispiel

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ]
      ```

   c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

      Die folgenden Schritte beschreiben, wie Sie die Rolle mithilfe von Bash in Azure Cloud Shell erstellen.

      - Start "Azure Cloud Shell" und wählen Sie die Bash-Umgebung.
      - Laden Sie die JSON-Datei hoch.



- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
az role definition create --role-definition agent_Policy.json
```

Sie sollten jetzt über eine benutzerdefinierte Rolle namens „Konsolenoperator“ verfügen, die Sie der virtuellen Maschine des Konsolenagenten zuweisen können.

2. Weisen Sie die Anwendung der Rolle zu:

   a. Öffnen Sie im Azure-Portal den Dienst **Abonnements**.

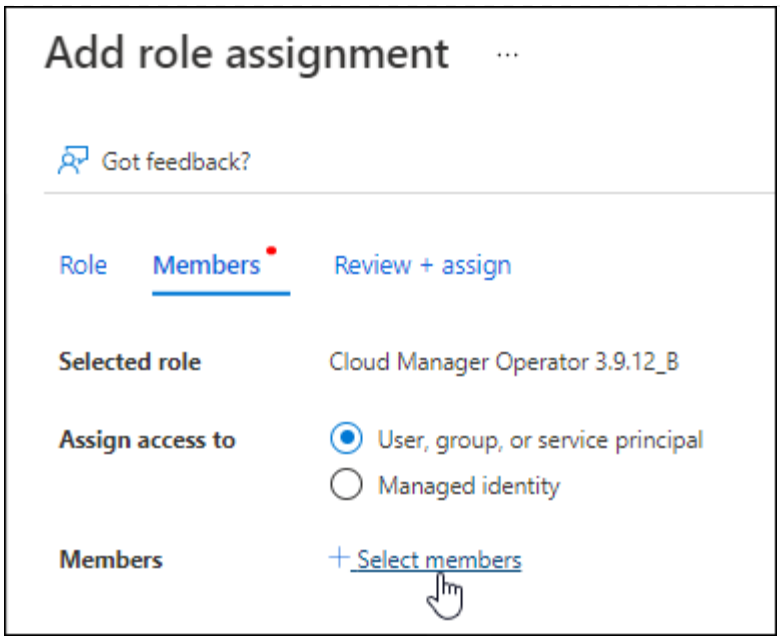
   b. Wählen Sie das Abonnement aus.

   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

   d. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.

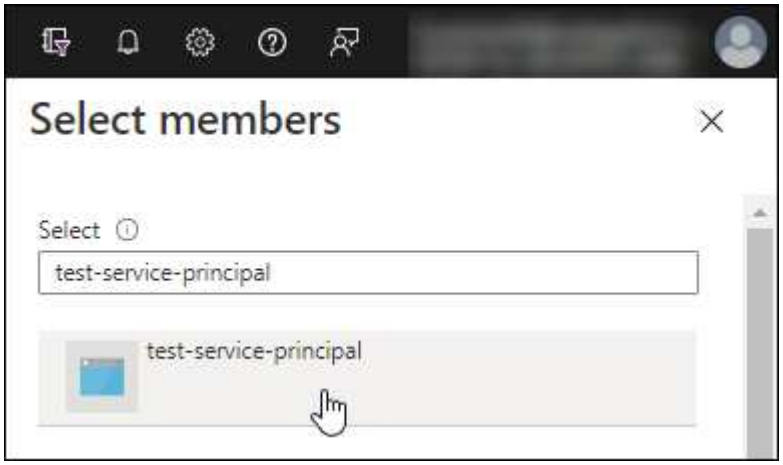
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - Behalten Sie die Auswahl von **Benutzer, Gruppe oder Dienstprinzipal** bei.
      - Wählen Sie **Mitglieder auswählen**.



- Suchen Sie nach dem Namen der Anwendung.

  Hier ist ein Beispiel:



- Wählen Sie die Anwendung aus und wählen Sie **Auswählen**.
- Wählen Sie **Weiter**.

f. Wählen Sie **Überprüfen + zuweisen**.

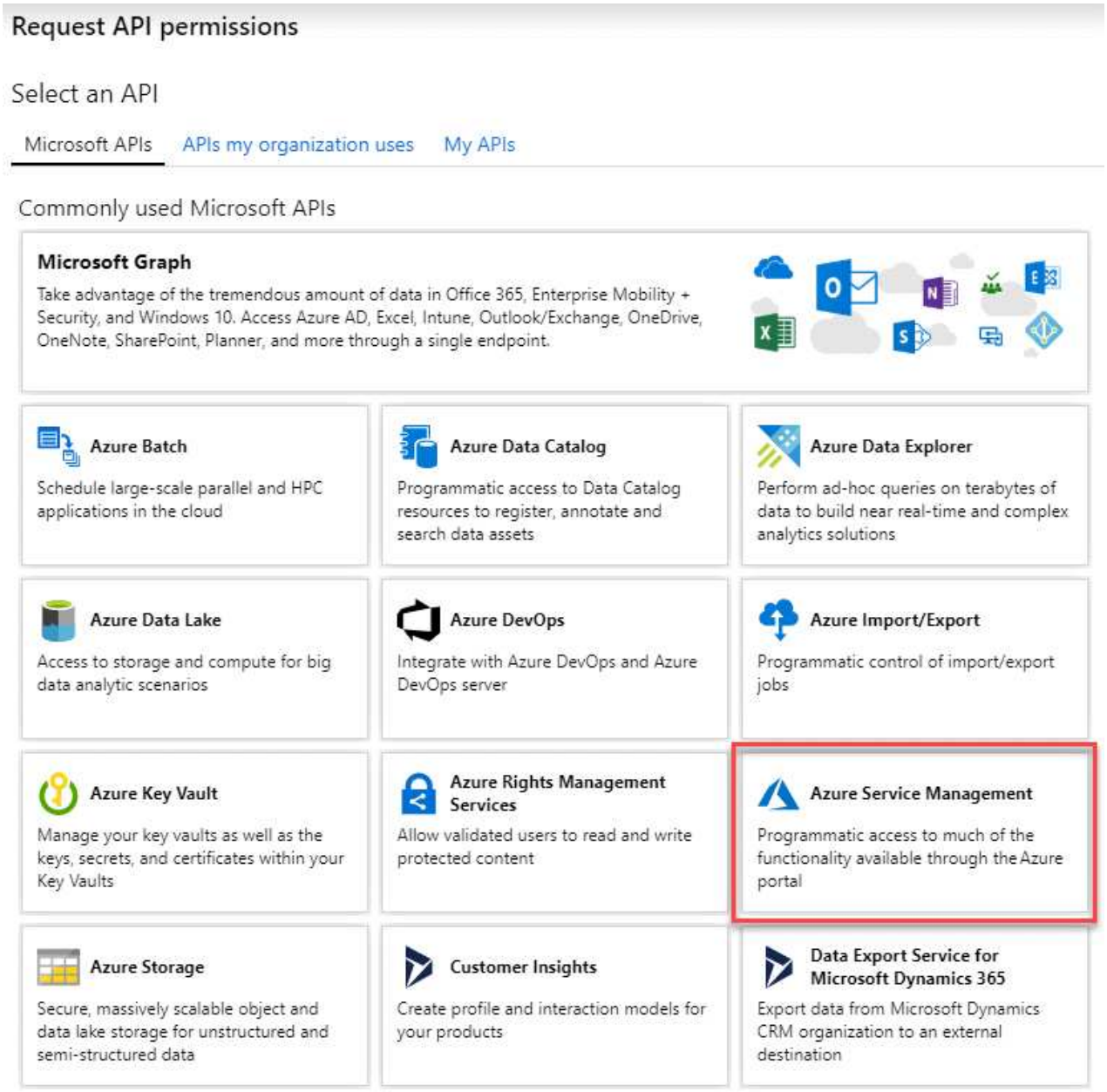
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

Wenn Sie Cloud Volumes ONTAP aus mehreren Azure-Abonnements bereitstellen möchten, müssen Sie den Dienstprinzipal an jedes dieser Abonnements binden. In der NetApp Console können Sie das Abonnement auswählen, das Sie beim Bereitstellen von Cloud Volumes ONTAP verwenden möchten.

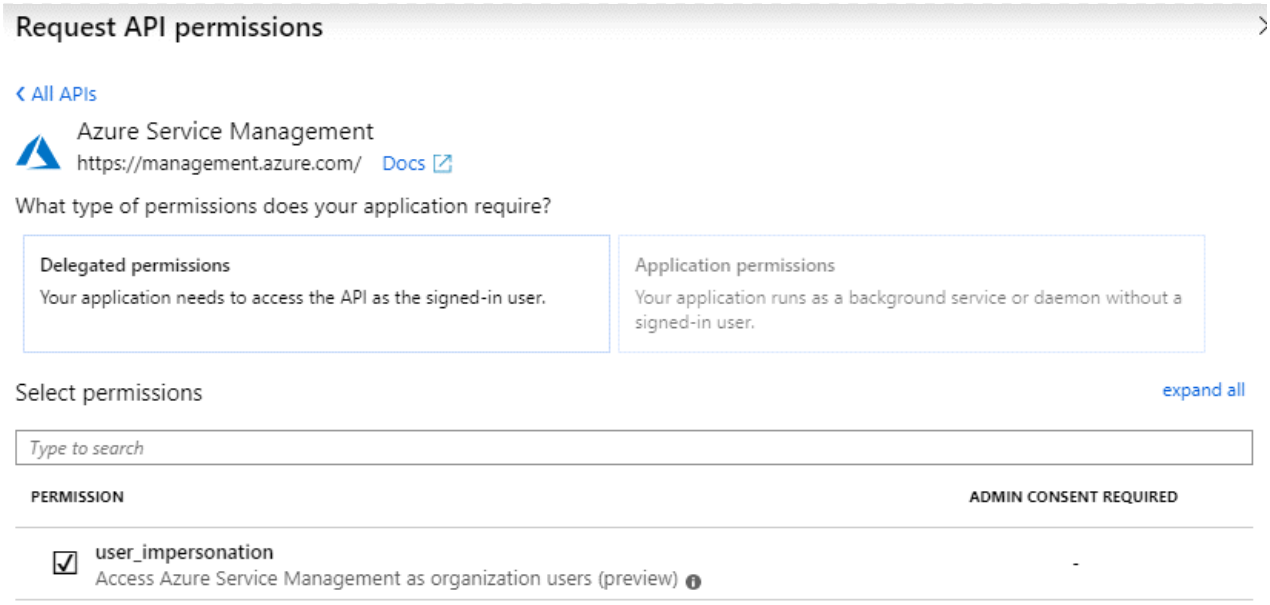
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Wählen Sie **API-Berechtigungen > Berechtigung hinzufügen**.

3. Wählen Sie unter **Microsoft-APIs Azure Service Management** aus.

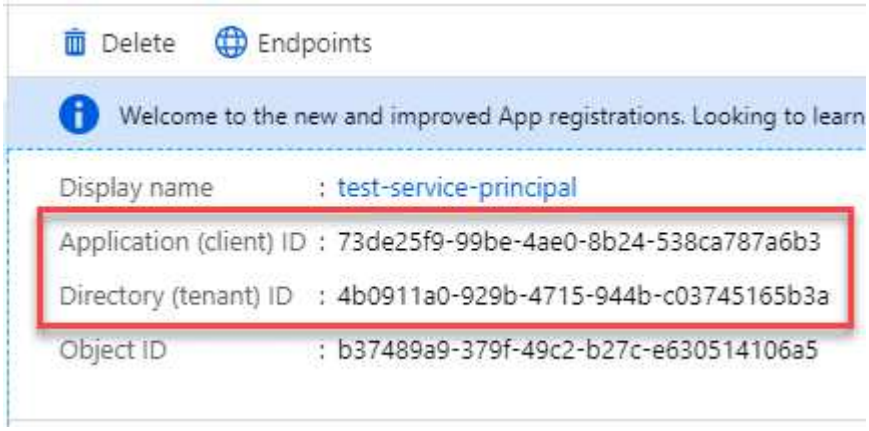


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



Abrufen der Anwendungs-ID und Verzeichnis-ID für die Anwendung

1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



Wenn Sie das Azure-Konto zur Konsole hinzufügen, müssen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) für die Anwendung angeben. Die Konsole verwendet die IDs zur programmgesteuerten Anmeldung.

Erstellen eines Client-Geheimnisses

1. Öffnen Sie den Dienst **Microsoft Entra ID**.
2. Wählen Sie **App-Registrierungen** und wählen Sie Ihre Anwendung aus.
3. Wählen Sie **Zertifikate und Geheimnisse > Neues Clientgeheimnis**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Wählen Sie **Hinzufügen**.
6. Kopieren Sie den Wert des Client-Geheimnisses.

Ergebnis

Ihr Dienstprinzipal ist jetzt eingerichtet und Sie sollten die Anwendungs-ID (Client-ID), die Verzeichnis-ID (Mandant-ID) und den Wert des Client-Geheimnisses kopiert haben. Sie müssen diese Informationen in der Konsole eingeben, wenn Sie ein Azure-Konto hinzufügen.

Google Cloud-Dienstkonto

Erstellen Sie eine Rolle und wenden Sie sie auf ein Dienstkonto an, das Sie für die VM-Instanz des Konsolenagenten verwenden.

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in Google Cloud:

   a. Erstellen Sie eine YAML-Datei, die die in der"Konsolen-Agent-Richtlinie für Google Cloud" .

   b. Aktivieren Sie Cloud Shell in Google Cloud.

   c. Laden Sie die YAML-Datei hoch, die die erforderlichen Berechtigungen für den Konsolenagenten enthält.

   d. Erstellen Sie eine benutzerdefinierte Rolle mithilfe der `gcloud iam roles create` Befehl.

      Das folgende Beispiel erstellt eine Rolle mit dem Namen „Agent“ auf Projektebene:

```
gcloud iam roles create agent --project=myproject --file=agent.yaml
```

   +
   "Google Cloud-Dokumente: Erstellen und Verwalten benutzerdefinierter Rollen"

2. Erstellen Sie ein Dienstkonto in Google Cloud:

   a. Wählen Sie im IAM- und Admin-Dienst **Dienstkonten > Dienstkonto erstellen**.

   b. Geben Sie die Details des Dienstkontos ein und wählen Sie **Erstellen und fortfahren**.

   c. Wählen Sie die Rolle aus, die Sie gerade erstellt haben.

   d. Führen Sie die restlichen Schritte aus, um die Rolle zu erstellen.

      "Google Cloud-Dokumente: Erstellen eines Dienstkontos"

Schritt 7: Google Cloud APIs aktivieren

Für die Bereitstellung von Cloud Volumes ONTAP in Google Cloud sind mehrere APIs erforderlich.

Schritt

1. "Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt"
    - Cloud Deployment Manager V2 API
    - Cloud Infrastructure Manager API
    - Cloud Logging API
    - Cloud Resource Manager-API
    - Compute Engine-API
    - API für Identitäts- und Zugriffsverwaltung (IAM)
    - Cloud Key Management Service (KMS) API (Nur erforderlich, wenn Sie NetApp Backup and Recovery mit kundenseitig verwalteten Verschlüsselungsschlüsseln (CMEK) verwenden möchten)
    - Cloud Quotas API (erforderlich für Cloud Volumes ONTAP Deployments mit Infrastructure Manager)

Bereitstellen des Konsolenagenten im eingeschränkten Modus

Stellen Sie den Konsolenagenten im eingeschränkten Modus bereit, damit Sie die NetApp Console mit eingeschränkter ausgehender Konnektivität verwenden können. Installieren Sie zunächst den Konsolen-Agenten, richten Sie die Konsole ein, indem Sie auf die Benutzeroberfläche zugreifen, die auf dem Konsolen-Agenten ausgeführt wird, und geben Sie dann die Cloud-Berechtigungen an, die Sie zuvor eingerichtet haben.

Schritt 1: Installieren des Konsolenagenten

Installieren Sie den Konsolenagenten vom Marktplatz Ihres Cloud-Anbieters oder manuell auf einem Linux-Host.

Sie müssen Ihre Umgebung vorbereitet haben, bevor Sie den Console-Agenten installieren. Sie können die Software über den AWS Marketplace, den Azure Marketplace oder manuell auf Ihrem eigenen Linux-Host installieren, der in AWS, Azure oder Google Cloud ausgeführt wird.

AWS Commercial Marketplace

Bevor Sie beginnen

Halten Sie Folgendes bereit:

- Eine VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt.

  "Informieren Sie sich über die Netzwerkanforderungen"

- Eine IAM-Rolle mit einer angehängten Richtlinie, die die erforderlichen Berechtigungen für den Konsolenagenten enthält.

  "Erfahren Sie, wie Sie AWS-Berechtigungen einrichten"

- Berechtigungen zum Abonnieren und Abbestellen des AWS Marketplace für Ihren IAM-Benutzer.
- Ein Verständnis der CPU- und RAM-Anforderungen für den Agenten.

  "Überprüfen Sie die Agentenanforderungen".

- Ein Schlüsselpaar für die EC2-Instanz.

Schritte

1. Gehen Sie zum "Auflistung des NetApp Console -Agenten im AWS Marketplace"
2. Wählen Sie auf der Marketplace-Seite **Weiter zum Abonnieren** aus.
3. Um die Software zu abonnieren, wählen Sie **Bedingungen akzeptieren**.

   Der Abonnementvorgang kann einige Minuten dauern.

4. Wählen Sie nach Abschluss des Abonnementvorgangs **Weiter zur Konfiguration**.
5. Stellen Sie auf der Seite **Diese Software konfigurieren** sicher, dass Sie die richtige Region ausgewählt haben, und wählen Sie dann **Weiter zum Starten**.
6. Wählen Sie auf der Seite **Diese Software starten** unter **Aktion auswählen** die Option **Über EC2 starten** und dann **Starten**.

   Verwenden Sie die EC2-Konsole, um die Instanz zu starten und eine IAM-Rolle anzuhängen. Dies ist mit der Aktion **Von Website starten** nicht möglich.

7. Folgen Sie den Anweisungen zum Konfigurieren und Bereitstellen der Instanz:
   - **Name und Tags**: Geben Sie einen Namen und Tags für die Instanz ein.
   - **Anwendungs- und Betriebssystem-Images**: Überspringen Sie diesen Abschnitt. Der Konsolenagent AMI ist bereits ausgewählt.
   - **Instanztyp**: Wählen Sie je nach regionaler Verfügbarkeit einen Instanztyp, der die RAM- und CPU-Anforderungen erfüllt (t3.2xlarge ist vorausgewählt und empfohlen).
   - **Schlüsselpaar (Anmeldung)**: Wählen Sie das Schlüsselpaar aus, das Sie für eine sichere Verbindung mit der Instanz verwenden möchten.
   - **Netzwerkeinstellungen**: Bearbeiten Sie die Netzwerkeinstellungen nach Bedarf:
     - Wählen Sie die gewünschte VPC und das gewünschte Subnetz.
     - Geben Sie an, ob die Instanz eine öffentliche IP-Adresse haben soll.

        - Geben Sie Sicherheitsgruppeneinstellungen an, die die erforderlichen Verbindungsmethoden für die Konsolen-Agenteninstanz aktivieren: SSH, HTTP und HTTPS.

          "Sicherheitsgruppenregeln für AWS anzeigen" .

    - **Speicher konfigurieren**: Behalten Sie die Standardgröße und den Standarddatenträgertyp für das Stammvolume bei.

      Wenn Sie die Amazon EBS-Verschlüsselung auf dem Stammvolume aktivieren möchten, wählen Sie **Erweitert**, erweitern Sie **Volume 1**, wählen Sie **Verschlüsselt** und wählen Sie dann einen KMS-Schlüssel.

    - **Erweiterte Details**: Wählen Sie unter **IAM-Instanzprofil** die IAM-Rolle aus, die die erforderlichen Berechtigungen für den Konsolenagenten enthält.
    - **Zusammenfassung**: Überprüfen Sie die Zusammenfassung und wählen Sie **Instanz starten**.

Ergebnis

AWS startet die Software mit den angegebenen Einstellungen. Die Bereitstellung des Konsolenagenten dauert etwa fünf Minuten.

Wie geht es weiter?

Richten Sie die NetApp Console ein.

AWS Gov Marketplace

Bevor Sie beginnen

Halten Sie Folgendes bereit:

- Eine VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt.

  "Informieren Sie sich über die Netzwerkanforderungen"

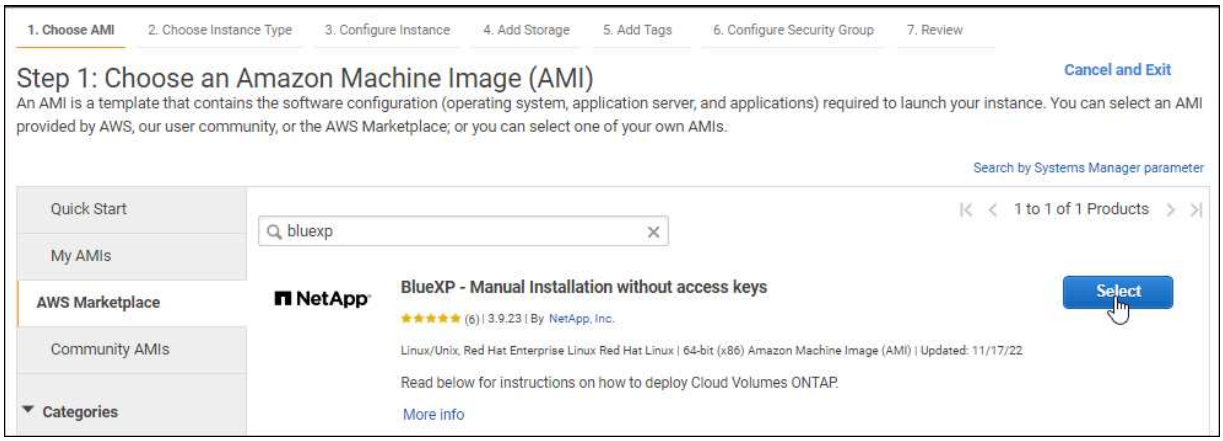
- Eine IAM-Rolle mit einer angehängten Richtlinie, die die erforderlichen Berechtigungen für den Konsolenagenten enthält.

  "Erfahren Sie, wie Sie AWS-Berechtigungen einrichten"

- Berechtigungen zum Abonnieren und Abbestellen des AWS Marketplace für Ihren IAM-Benutzer.
- Ein Schlüsselpaar für die EC2-Instanz.

Schritte

1. Gehen Sie zum NetApp Console -Agent-Angebot im AWS Marketplace.
   a. Öffnen Sie den EC2-Dienst und wählen Sie **Instanz starten**.
   b. Wählen Sie **AWS Marketplace** aus.
   c. Suchen Sie nach der NetApp Console und wählen Sie das Angebot aus.



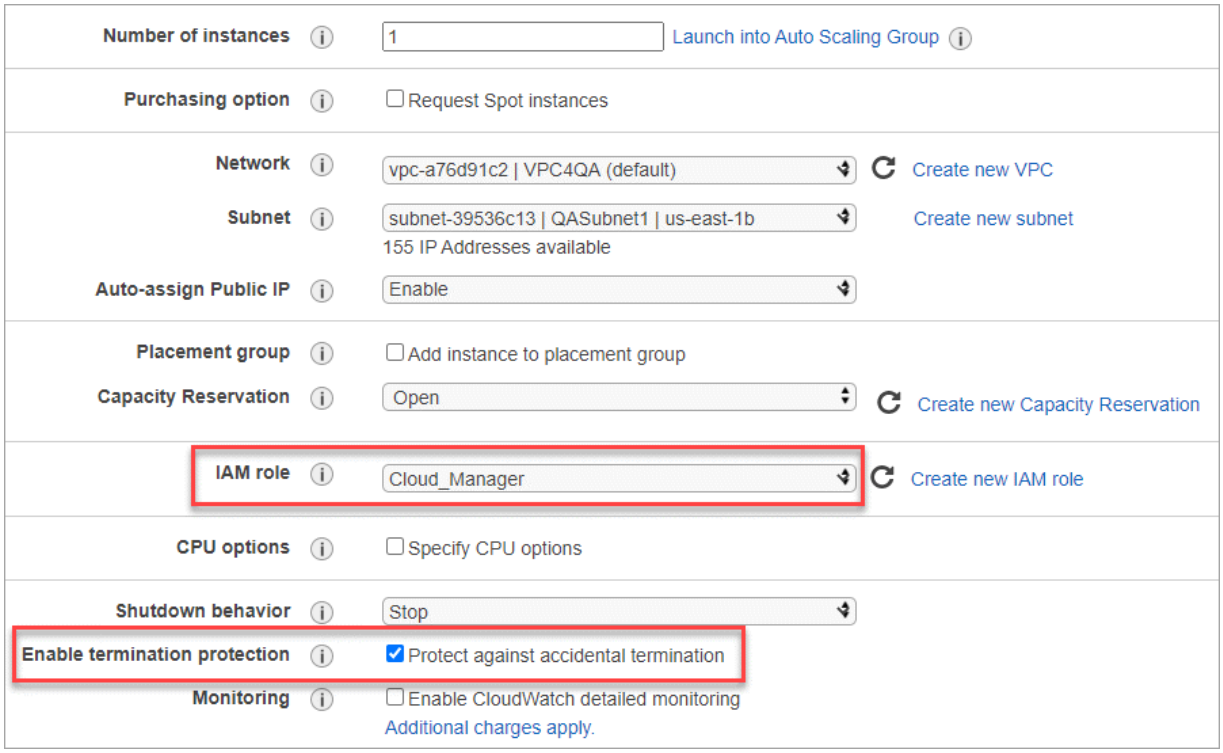
d. Wählen Sie **Weiter**.

2. Folgen Sie den Anweisungen, um die Instanz einzurichten und zu starten:

   - **Wählen Sie einen Instanztyp**: Wählen Sie je nach regionaler Verfügbarkeit einen der unterstützten Instanztypen (t3.2xlarge wird empfohlen).

     "Überprüfen der Instanzanforderungen" .

   - **Instanzdetails konfigurieren**: Wählen Sie eine VPC und ein Subnetz aus, wählen Sie die IAM-Rolle, die Sie in Schritt 1 erstellt haben, aktivieren Sie den Kündigungsschutz (empfohlen) und wählen Sie alle anderen Konfigurationsoptionen, die Ihren Anforderungen entsprechen.



   - **Speicher hinzufügen**: Behalten Sie die Standardspeicheroptionen bei.
   - **Tags hinzufügen**: Geben Sie bei Bedarf Tags für die Instanz ein.
   - **Sicherheitsgruppe konfigurieren**: Geben Sie die erforderlichen Verbindungsmethoden für die Konsolen-Agenteninstanz an: SSH, HTTP und HTTPS.
   - **Überprüfen**: Überprüfen Sie Ihre Auswahl und wählen Sie **Starten**.

Ergebnis

AWS startet die Software mit den angegebenen Einstellungen. Die Bereitstellung des Konsolenagenten dauert etwa fünf Minuten.

Wie geht es weiter?

Richten Sie die Konsole ein.

Azure Gov Marketplace

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Ein VNet und Subnetz, das die Netzwerkanforderungen erfüllt.

  "Informieren Sie sich über die Netzwerkanforderungen"

- Eine benutzerdefinierte Azure-Rolle, die die erforderlichen Berechtigungen für den Konsolen-Agent enthält.

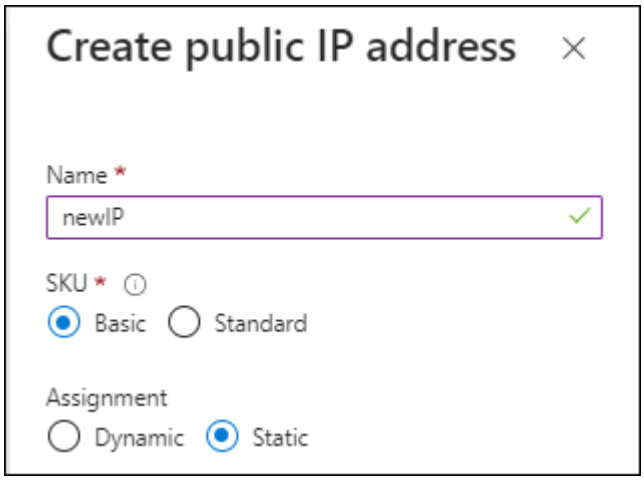
  "Erfahren Sie, wie Sie Azure-Berechtigungen einrichten"

Schritte

1. Gehen Sie zur VM-Seite des NetApp Console Agents im Azure Marketplace.
   - "Azure Marketplace-Seite für kommerzielle Regionen"
   - "Azure Marketplace-Seite für Azure Government-Regionen"
2. Wählen Sie **Jetzt holen** und dann **Weiter**.
3. Wählen Sie im Azure-Portal **Erstellen** aus und befolgen Sie die Schritte zum Konfigurieren der virtuellen Maschine.

   Beachten Sie beim Konfigurieren der VM Folgendes:

   - **VM-Größe**: Wählen Sie eine VM-Größe, die den CPU- und RAM-Anforderungen entspricht. Wir empfehlen Standard_D8s_v3.
   - **Festplatten**: Der Konsolenagent kann mit HDD- oder SSD-Festplatten optimal funktionieren.
   - **Öffentliche IP-Adresse**: Um eine öffentliche IP-Adresse mit der Console-Agent-VM zu verwenden, wählen Sie eine Basic-SKU.



Wenn Sie stattdessen eine Standard-SKU-IP-Adresse verwenden, verwendet die Konsole die *private* IP-Adresse des Konsolenagenten anstelle der öffentlichen IP. Wenn der Rechner, mit dem Sie auf die Konsole zugreifen, die private IP-Adresse nicht erreichen kann, funktioniert die Konsole nicht.

"Azure-Dokumentation: Öffentliche IP-SKU"

- **Netzwerksicherheitsgruppe**: Der Konsolenagent erfordert eingehende Verbindungen über SSH, HTTP und HTTPS.

  "Anzeigen von Sicherheitsgruppenregeln für Azure" .

- **Identität**: Wählen Sie unter **Verwaltung** die Option **Vom System zugewiesene verwaltete Identität aktivieren**.

  Eine verwaltete Identität ermöglicht es der Console-Agent-VM, sich gegenüber Microsoft Entra ID ohne Anmeldeinformationen zu identifizieren. "Erfahren Sie mehr über verwaltete Identitäten für Azure-Ressourcen" Die

4. Überprüfen Sie auf der Seite **Überprüfen + Erstellen** Ihre Auswahl und wählen Sie **Erstellen** aus, um die Bereitstellung zu starten.

Ergebnis

Azure stellt die virtuelle Maschine mit den angegebenen Einstellungen bereit. Die virtuelle Maschine und die Konsolenagent-Software sollten in etwa fünf Minuten ausgeführt werden.

Wie geht es weiter?

Richten Sie die NetApp Console ein.

Manuelle Installation (muss für Google Cloud verwendet werden)

Sie können den Console-Agenten manuell auf Ihrem eigenen Linux-Host installieren, der in AWS, Azure oder Google Cloud ausgeführt wird.

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Root-Berechtigungen zum Installieren des Konsolenagenten.
- Details zu einem Proxyserver, falls für den Internetzugriff vom Konsolenagenten ein Proxy erforderlich ist.

  Sie haben die Möglichkeit, nach der Installation einen Proxyserver zu konfigurieren, hierzu ist jedoch ein Neustart des Konsolenagenten erforderlich.

- Ein von einer Zertifizierungsstelle signiertes Zertifikat, wenn der Proxyserver HTTPS verwendet oder wenn es sich bei dem Proxy um einen abfangenden Proxy handelt.

  Sie können bei der manuellen Installation des Konsolenagenten kein Zertifikat für einen transparenten Proxyserver festlegen. Wenn Sie ein Zertifikat für einen transparenten Proxyserver festlegen müssen, müssen Sie nach der Installation die Wartungskonsole verwenden. Erfahren Sie mehr über die "Agenten-Wartungskonsole"Die

- Sie müssen die Konfigurationsprüfung deaktivieren, die während der Installation die ausgehende Konnektivität überprüft. Die manuelle Installation schlägt fehl, wenn diese Prüfung nicht deaktiviert

ist."Erfahren Sie, wie Sie Konfigurationsprüfungen für manuelle Installationen deaktivieren."

- Abhängig von Ihrem Betriebssystem ist entweder Podman oder Docker Engine erforderlich, bevor Sie den Konsolenagenten installieren.

Informationen zu diesem Vorgang

Nach der Installation aktualisiert sich der Konsolenagent automatisch, wenn eine neue Version verfügbar ist.

Schritte

1. Wenn die Systemvariablen *http_proxy* oder *https_proxy* auf dem Host festgelegt sind, entfernen Sie sie:

   ```
   unset http_proxy
   unset https_proxy
   ```

   Wenn Sie diese Systemvariablen nicht entfernen, schlägt die Installation fehl.

2. Laden Sie die Console-Agent-Software herunter und kopieren Sie sie anschließend auf den Linux-Host. Sie können es entweder von der NetApp Console oder von der NetApp -Support-Website herunterladen.

   - NetApp Console: Gehen Sie zu **Agents > Management > Agent bereitstellen > On-Premise > Manuelle Installation**.

     Wählen Sie entweder die Agenteninstallationsdateien oder eine URL zu den Dateien zum Herunterladen.

   - NetApp Supportseite (erforderlich, falls Sie noch keinen Zugriff auf die Konsole haben) "NetApp Support Site" ,

3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

   ```
   chmod +x NetApp_Console_Agent_Cloud_<version>
   ```

   Dabei ist <Version> die Version des Konsolenagenten, die Sie heruntergeladen haben.

4. Deaktivieren Sie bei der Installation in einer Government Cloud-Umgebung die Konfigurationsprüfungen."Erfahren Sie, wie Sie Konfigurationsprüfungen für manuelle Installationen deaktivieren."

5. Führen Sie das Installationsskript aus.

   ```
   ./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
   server> --cacert <path and file name of a CA-signed certificate>
   ```

   Sie müssen Proxy-Informationen hinzufügen, falls Ihr Netzwerk einen Proxy für den Internetzugang benötigt. Sie können während der Installation einen expliziten Proxy hinzufügen. Die `--proxy` und `--cacert` Parameter sind optional und Sie werden nicht dazu aufgefordert, sie hinzuzufügen. Wenn Sie einen expliziten Proxyserver haben, müssen Sie die Parameter wie gezeigt eingeben.

Wenn Sie einen transparenten Proxy konfigurieren möchten, können Sie dies nach der Installation tun. "Erfahren Sie mehr über die Agentenwartungskonsole."

+

Hier ist ein Beispiel für die Konfiguration eines expliziten Proxyservers mit einem von einer Zertifizierungsstelle signierten Zertifikat:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

+
`--proxy` konfiguriert den Konsolenagenten für die Verwendung eines HTTP- oder HTTPS-Proxyservers in einem der folgenden Formate:

+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-name:password@address:port * https://address:port * https://user-name:password@address:port * https://domain-name%92user-name:password@address:port

+ Beachten Sie Folgendes:

+ **Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.** Für einen Domänenbenutzer müssen Sie den ASCII-Code für ein \ verwenden, wie oben gezeigt. **Der Console-Agent unterstützt keine Benutzernamen oder Passwörter, die das @-Zeichen enthalten.** Wenn das Passwort eines der folgenden Sonderzeichen enthält, müssen Sie dieses Sonderzeichen durch Voranstellen eines Backslashs maskieren: & oder !

+ Zum Beispiel:

+ http://bxpproxyuser:netapp1\!@address:3128

1. Wenn Sie Podman verwendet haben, müssen Sie den Aardvark-DNS-Port anpassen.

   a. Stellen Sie eine SSH-Verbindung zur virtuellen Maschine des Konsolenagenten her.

   b. Öffnen Sie die Datei podman_/usr/share/containers/containers.conf_ und ändern Sie den gewählten Port für den Aardvark-DNS-Dienst. Ändern Sie ihn beispielsweise in 54.

      ```
      vi /usr/share/containers/containers.conf
      ```

      Beispiel:

```
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
```

a. Starten Sie die virtuelle Maschine des Konsolenagenten neu.

Ergebnis

Der Konsolenagent ist jetzt installiert. Am Ende der Installation wird der Konsolenagentdienst (occm) zweimal neu gestartet, wenn Sie einen Proxyserver angegeben haben.

Wie geht es weiter?

Richten Sie die NetApp Console ein.

Schritt 2: NetApp Console einrichten

Wenn Sie zum ersten Mal auf die Konsole zugreifen, werden Sie aufgefordert, eine Organisation für den Konsolenagenten auszuwählen und den eingeschränkten Modus zu aktivieren.

Bevor Sie beginnen

Die Person, die den Konsolenagenten einrichtet, muss sich mit einem Login bei der Konsole anmelden, der noch nicht zu einer Konsolenorganisation gehört.

Falls Ihr Login mit einer anderen Organisation verknüpft ist, müssen Sie sich mit einem neuen Login registrieren. Andernfalls wird Ihnen die Option zum Aktivieren des eingeschränkten Modus auf dem Einstellungsbildschirm nicht angezeigt.

Schritte

1. Öffnen Sie einen Webbrowser auf einem Host, der über eine Verbindung zur Konsolen-Agenteninstanz verfügt, und geben Sie die folgende URL des von Ihnen installierten Konsolen-Agenten ein.
2. Registrieren Sie sich oder melden Sie sich bei der NetApp Console an.
3. Nachdem Sie sich angemeldet haben, richten Sie die Konsole ein:

   a. Geben Sie einen Namen für den Konsolenagenten ein.

   b. Geben Sie einen Namen für eine neue Konsolenorganisation ein.

   c. Wählen Sie **Arbeiten Sie in einer sicheren Umgebung?**

   d. Wählen Sie **Eingeschränkten Modus für dieses Konto aktivieren**.

      Beachten Sie, dass Sie diese Einstellung nach der Kontoerstellung nicht mehr ändern können. Sie können den eingeschränkten Modus später weder aktivieren noch deaktivieren.

   Wenn Sie den Konsolenagenten in einer Regierungsregion bereitgestellt haben, ist das Kontrollkästchen bereits aktiviert und kann nicht geändert werden. Dies liegt daran, dass der eingeschränkte Modus der

einzige Modus ist, der in Regierungsregionen unterstützt wird.

a. Wählen Sie **Los geht's**.

Ergebnis

Der Konsolenagent ist jetzt installiert und mit Ihrer Konsolenorganisation eingerichtet. Alle Benutzer müssen über die IP-Adresse der Konsolen-Agentinstanz auf die Konsole zugreifen.

Wie geht es weiter?

Geben Sie der Konsole die Berechtigungen, die Sie zuvor eingerichtet haben.

Schritt 3: Erteilen Sie dem Konsolenagenten Berechtigungen

Wenn Sie den Console-Agenten über den Azure Marketplace oder manuell installiert haben, müssen Sie die zuvor eingerichteten Berechtigungen erteilen.

Diese Schritte gelten nicht, wenn Sie den Konsolenagenten vom AWS Marketplace bereitgestellt haben, da Sie während der Bereitstellung die erforderliche IAM-Rolle ausgewählt haben.

"Erfahren Sie, wie Sie Cloud-Berechtigungen vorbereiten" .

AWS IAM-Rolle

Fügen Sie die zuvor erstellte IAM-Rolle der EC2-Instance hinzu, auf der Sie den Konsolenagenten installiert haben.

Diese Schritte gelten nur, wenn Sie den Konsolenagenten manuell in AWS installiert haben. Für AWS Marketplace-Bereitstellungen haben Sie die Konsolen-Agent-Instanz bereits mit einer IAM-Rolle verknüpft, die die erforderlichen Berechtigungen enthält.

Schritte

1. Gehen Sie zur Amazon EC2-Konsole.
2. Wählen Sie **Instanzen** aus.
3. Wählen Sie die Konsolen-Agentinstanz aus.
4. Wählen Sie **Aktionen > Sicherheit > IAM-Rolle ändern**.
5. Wählen Sie die IAM-Rolle und dann **IAM-Rolle aktualisieren** aus.

AWS-Zugriffsschlüssel

Stellen Sie der NetApp Console den AWS-Zugriffsschlüssel für einen IAM-Benutzer bereit, der über die erforderlichen Berechtigungen verfügt.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
    a. **Speicherort der Anmeldeinformationen**: Wählen Sie *Amazon Web Services > Agent.
    b. **Anmeldeinformationen definieren**: Geben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel ein.
    c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.
    d. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Azure-Rolle

Gehen Sie zum Azure-Portal und weisen Sie der virtuellen Maschine des Konsolen-Agents für ein oder mehrere Abonnements die benutzerdefinierte Azure-Rolle zu.

Schritte

1. Öffnen Sie im Azure-Portal den Dienst **Abonnements** und wählen Sie Ihr Abonnement aus.

    Es ist wichtig, die Rolle vom Dienst **Abonnements** zuzuweisen, da dies den Umfang der Rollenzuweisung auf Abonnementebene angibt. Der *Bereich* definiert die Menge der Ressourcen, auf die der Zugriff angewendet wird. Wenn Sie einen Bereich auf einer anderen Ebene angeben (z. B. auf der Ebene der virtuellen Maschine), wird Ihre Fähigkeit, Aktionen innerhalb der NetApp Console auszuführen, beeinträchtigt.

    "Microsoft Azure-Dokumentation: Umfang von Azure RBAC verstehen"

2. Wählen Sie **Zugriffskontrolle (IAM)** > **Hinzufügen** > **Rollenzuweisung hinzufügen**.

3. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.

> „Konsolenoperator“ ist der in der Richtlinie angegebene Standardname. Wenn Sie einen anderen Namen für die Rolle gewählt haben, wählen Sie stattdessen diesen Namen aus.

4. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:
   a. Weisen Sie einer **verwalteten Identität** Zugriff zu.
   b. Wählen Sie **Mitglieder auswählen**, wählen Sie das Abonnement aus, in dem die virtuelle Maschine des Konsolen-Agents erstellt wurde, wählen Sie unter **Verwaltete Identität Virtuelle Maschine** und wählen Sie dann die virtuelle Maschine des Konsolen-Agents aus.
   c. Wählen Sie **Auswählen**.
   d. Wählen Sie **Weiter**.
   e. Wählen Sie **Überprüfen + zuweisen**.
   f. Wenn Sie Ressourcen in zusätzlichen Azure-Abonnements verwalten möchten, wechseln Sie zu diesem Abonnement und wiederholen Sie diese Schritte.

Azure-Dienstprinzipal

Geben Sie in der NetApp Console die Anmeldeinformationen für den Azure-Dienstprinzipal ein, den Sie zuvor eingerichtet haben.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Microsoft Azure > Agent**.
   b. **Anmeldeinformationen definieren**: Geben Sie Informationen zum Microsoft Entra-Dienstprinzipal ein, der die erforderlichen Berechtigungen erteilt:
      - Anwendungs-ID (Client-ID)
      - Verzeichnis-ID (Mandant)
      - Client-Geheimnis
   c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.
   d. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Ergebnis

Die NetApp Console verfügt jetzt über die erforderlichen Berechtigungen, um in Ihrem Namen Aktionen in Azure auszuführen.

Google Cloud-Dienstkonto

Verknüpfen Sie das Dienstkonto mit der Konsolen-Agent-VM.

Schritte

1. Gehen Sie zum Google Cloud-Portal und weisen Sie das Dienstkonto der VM-Instanz des Console-Agenten zu.

"Google Cloud-Dokumentation: Ändern des Dienstkontos und der Zugriffsbereiche für eine Instanz"

2. Wenn Sie Ressourcen in anderen Projekten verwalten möchten, gewähren Sie Zugriff, indem Sie das Dienstkonto mit der Rolle „Konsolenagent“ zu diesem Projekt hinzufügen. Sie müssen diesen Schritt für jedes Projekt wiederholen.

Abonnieren Sie NetApp Intelligent Services (eingeschränkter Modus)

Abonnieren Sie NetApp Intelligent Services über den Marktplatz Ihres Cloud-Anbieters, um Datendienste zu einem Stundensatz (PAYGO) oder über einen Jahresvertrag zu bezahlen. Wenn Sie eine Lizenz von NetApp (BYOL) erworben haben, müssen Sie auch das Marktplatzangebot abonnieren. Ihre Lizenz wird immer zuerst in Rechnung gestellt. Wenn Sie jedoch Ihre Lizenzkapazität überschreiten oder die Laufzeit der Lizenz abläuft, wird Ihnen der Stundensatz in Rechnung gestellt.

Ein Marktplatz-Abonnement ermöglicht die Abrechnung der folgenden Datendienste im eingeschränkten Modus:

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

Die NetApp Data Classification wird über Ihr Abonnement aktiviert, für die Verwendung der Klassifizierung fallen jedoch keine Gebühren an.

Bevor Sie beginnen

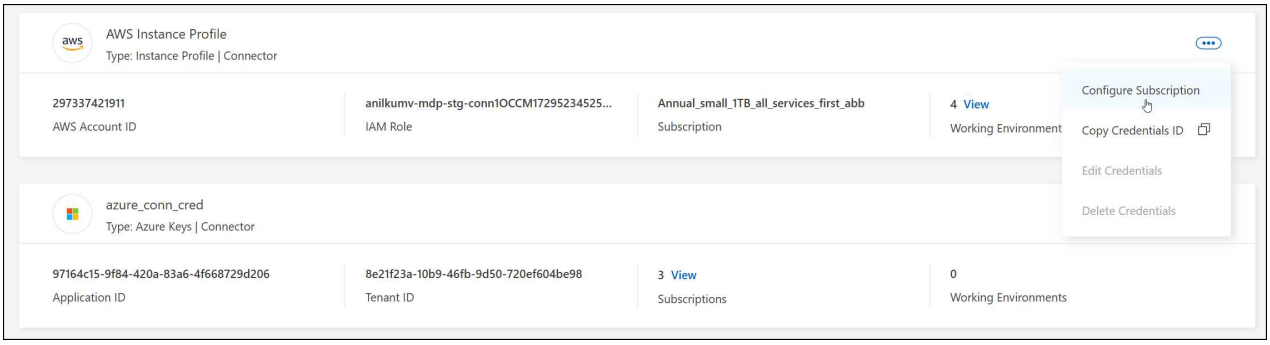
Sie müssen bereits einen Konsolenagenten bereitgestellt haben, um Datendienste abonnieren zu können. Sie müssen den mit einem Konsolenagenten verbundenen Cloud-Anmeldeinformationen ein Marktplatzabonnement zuordnen.

AWS

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen aus, die einem Konsolenagenten zugeordnet sind, und wählen Sie dann **Abonnement konfigurieren**.

   Sie müssen Anmeldeinformationen auswählen, die einem Konsolenagenten zugeordnet sind. Sie können ein Marktplatzabonnement nicht mit Anmeldeinformationen verknüpfen, die mit der NetApp Console verknüpft sind.



4. Um die Anmeldeinformationen mit einem vorhandenen Abonnement zu verknüpfen, wählen Sie das Abonnement aus der Dropdown-Liste aus und wählen Sie **Konfigurieren**.
5. Um die Anmeldeinformationen einem neuen Abonnement zuzuordnen, wählen Sie **Abonnement hinzufügen > Fortfahren** und folgen Sie den Schritten im AWS Marketplace:

   a. Wählen Sie **Kaufoptionen anzeigen**.

   b. Wählen Sie **Abonnieren**.

   c. Wählen Sie **Konto einrichten**.

      Sie werden zur NetApp Console weitergeleitet.

   d. Auf der Seite **Abonnementzuweisung**:

      - Wählen Sie die Konsolenorganisationen oder -konten aus, mit denen Sie dieses Abonnement verknüpfen möchten.
      - Wählen Sie im Feld **Vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

        Die Konsole ersetzt das vorhandene Abonnement für alle Anmeldeinformationen in der Organisation oder im Konto durch dieses neue Abonnement. Wenn ein Satz von Anmeldeinformationen nie mit einem Abonnement verknüpft war, wird dieses neue Abonnement nicht mit diesen Anmeldeinformationen verknüpft.

   Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.

   - Wählen Sie **Speichern**.

Azurblau

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen aus, die einem Konsolenagenten zugeordnet sind, und wählen Sie dann **Abonnement konfigurieren**.

   Sie müssen Anmeldeinformationen auswählen, die einem Konsolenagenten zugeordnet sind. Sie können ein Marktplatzabonnement nicht mit Anmeldeinformationen verknüpfen, die mit der NetApp Console verknüpft sind.

4. Um die Anmeldeinformationen mit einem vorhandenen Abonnement zu verknüpfen, wählen Sie das Abonnement aus der Dropdown-Liste aus und wählen Sie **Konfigurieren**.
5. Um die Anmeldeinformationen einem neuen Abonnement zuzuordnen, wählen Sie **Abonnement hinzufügen > Fortfahren** und befolgen Sie die Schritte im Azure Marketplace:

   a. Melden Sie sich bei entsprechender Aufforderung bei Ihrem Azure-Konto an.
   b. Wählen Sie **Abonnieren**.
   c. Füllen Sie das Formular aus und wählen Sie **Abonnieren**.
   d. Nachdem der Abonnementvorgang abgeschlossen ist, wählen Sie **Konto jetzt konfigurieren**.

      Sie werden zur NetApp Console weitergeleitet.

   e. Auf der Seite **Abonnementzuweisung**:
      - Wählen Sie die Konsolenorganisationen oder -konten aus, mit denen Sie dieses Abonnement verknüpfen möchten.
      - Wählen Sie im Feld **Vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

        Die Konsole ersetzt das vorhandene Abonnement für alle Anmeldeinformationen in der Organisation oder im Konto durch dieses neue Abonnement. Wenn ein Satz von Anmeldeinformationen nie mit einem Abonnement verknüpft war, wird dieses neue Abonnement nicht mit diesen Anmeldeinformationen verknüpft.

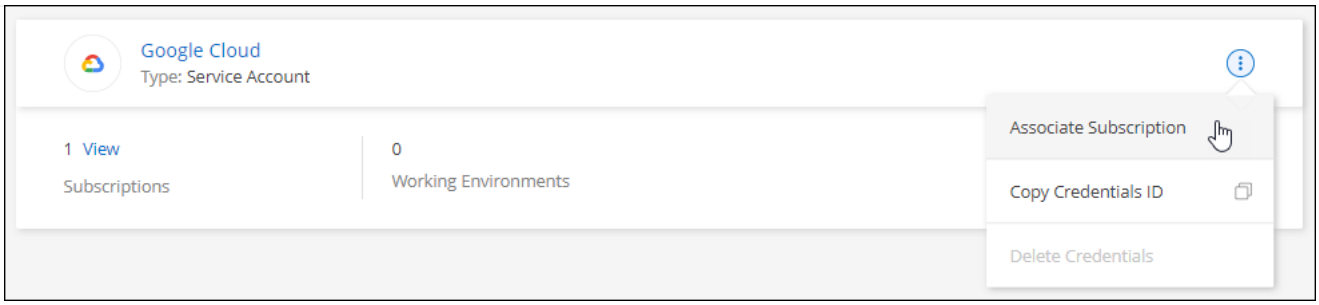
   Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.

   ◦ Wählen Sie **Speichern**.

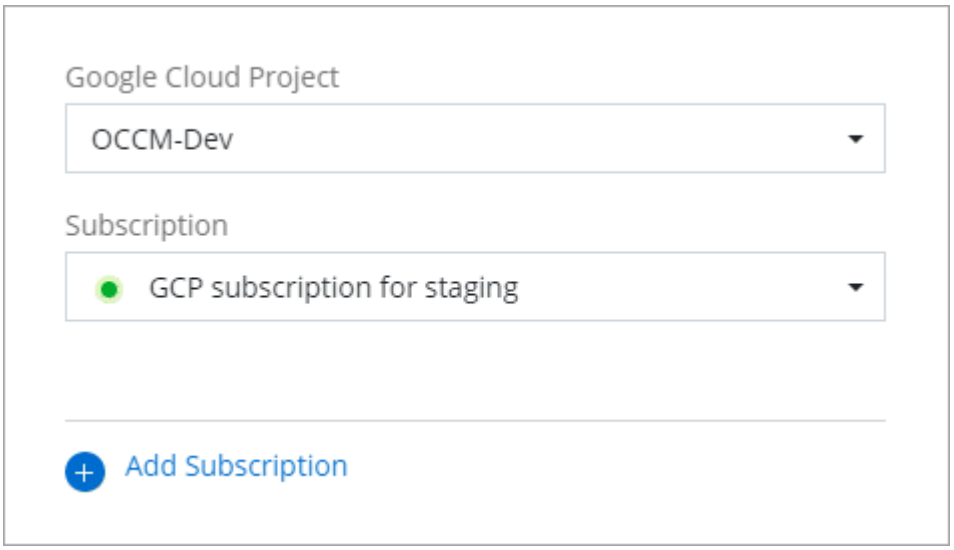
Google Cloud

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen aus, die einem Konsolenagenten zugeordnet sind, und wählen Sie dann **Abonnement konfigurieren**.



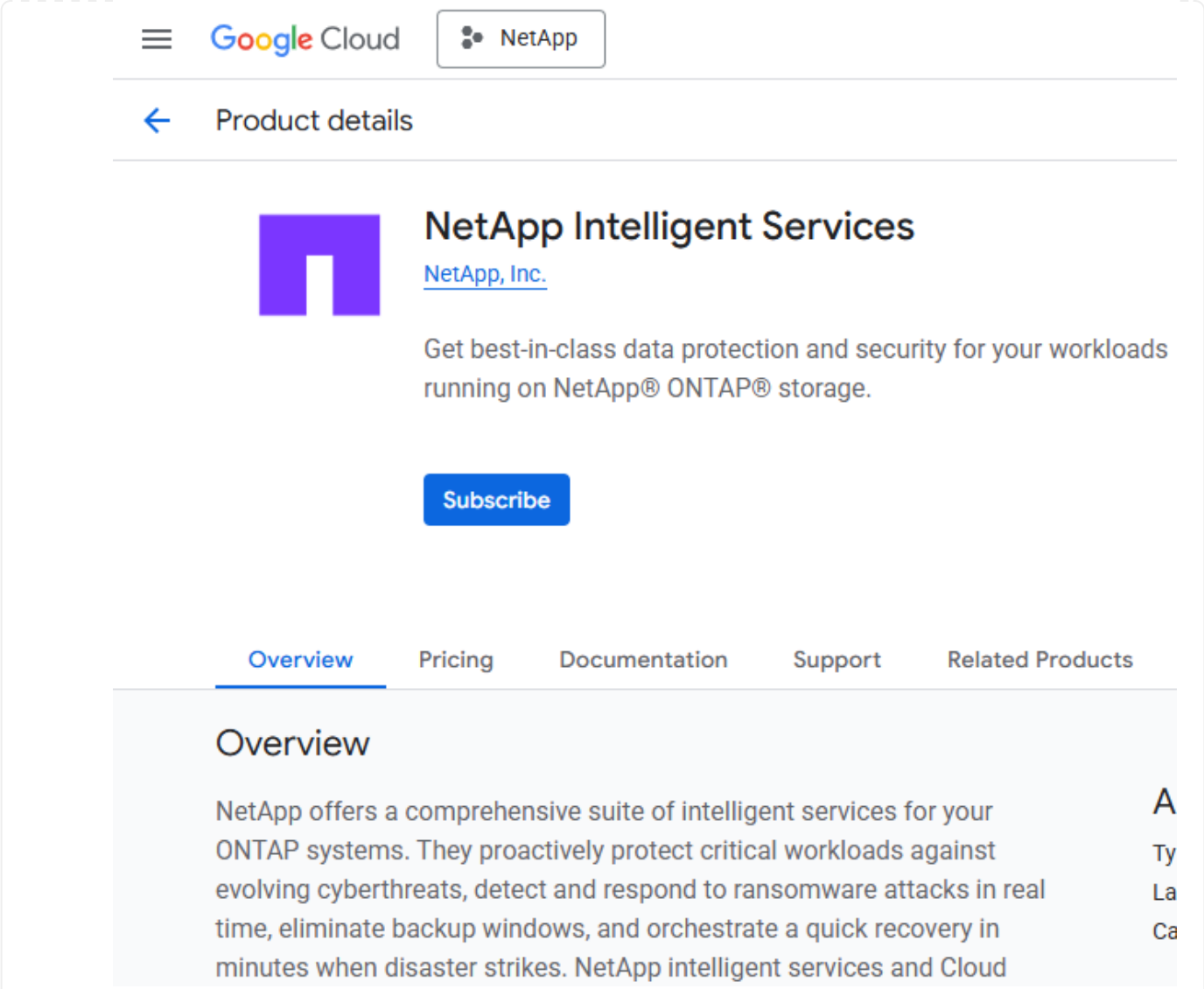
1. Um ein vorhandenes Abonnement mit den ausgewählten Anmeldeinformationen zu konfigurieren, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Dropdown-Liste aus und wählen Sie dann **Konfigurieren**.



2. Wenn Sie noch kein Abonnement haben, wählen Sie **Abonnement hinzufügen > Fortfahren** und folgen Sie den Schritten im Google Cloud Marketplace.

Bevor Sie die folgenden Schritte ausführen, stellen Sie sicher, dass Sie sowohl über Abrechnungsadministratorberechtigungen in Ihrem Google Cloud-Konto als auch über eine NetApp Console verfügen.

   a. Nachdem Sie weitergeleitet wurden auf die "NetApp Intelligent Services -Seite im Google Cloud Marketplace" , stellen Sie sicher, dass im oberen Navigationsmenü das richtige Projekt ausgewählt ist.



b. Wählen Sie **Abonnieren**.

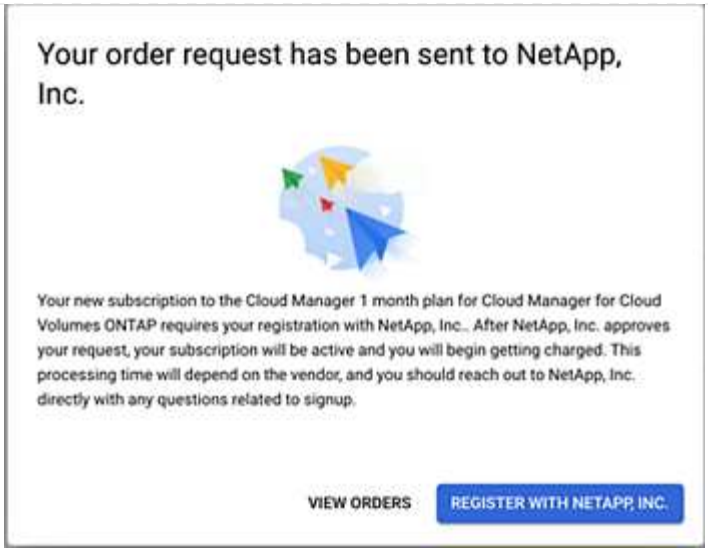
c. Wählen Sie das entsprechende Abrechnungskonto aus und stimmen Sie den Allgemeinen Geschäftsbedingungen zu.

d. Wählen Sie **Abonnieren**.

   Dieser Schritt sendet Ihre Übertragungsanforderung an NetApp.

e. Wählen Sie im Popup-Dialogfeld **Bei NetApp, Inc. registrieren** aus.

   Dieser Schritt muss abgeschlossen werden, um das Google Cloud-Abonnement mit Ihrer Konsolenorganisation oder Ihrem Konsolenkonto zu verknüpfen. Der Vorgang zum Verknüpfen eines Abonnements ist erst abgeschlossen, wenn Sie von dieser Seite umgeleitet werden und sich dann bei der Konsole anmelden.



f. Führen Sie die Schritte auf der Seite **Abonnementzuweisung** aus:

> Wenn jemand aus Ihrer Organisation bereits ein Marktplatz-Abonnement von Ihrem Abrechnungskonto hat, werden Sie weitergeleitet zu "die Cloud Volumes ONTAP -Seite in der NetApp Console" stattdessen. Wenn dies unerwartet vorkommt, wenden Sie sich an Ihr NetApp -Vertriebsteam. Google ermöglicht nur ein Abonnement pro Google-Abrechnungskonto.

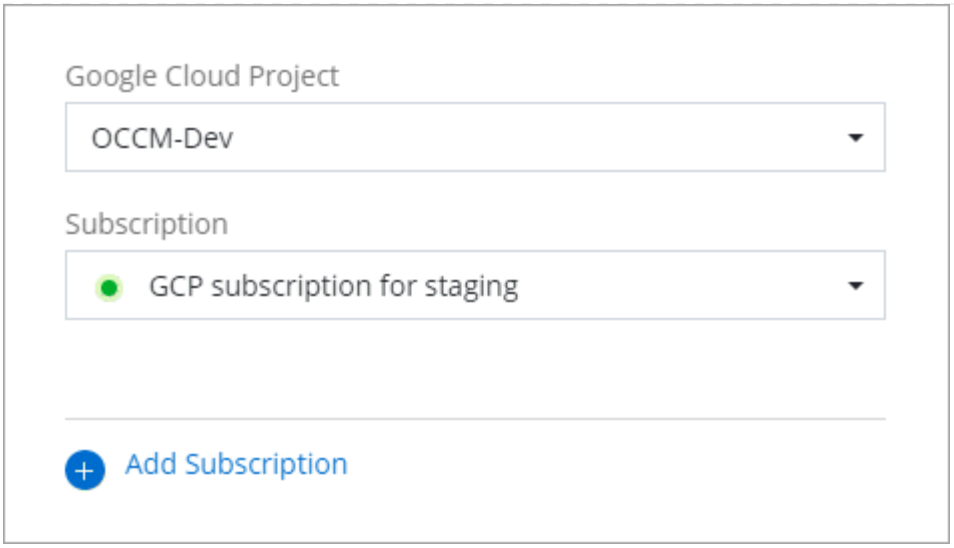
- Wählen Sie die Konsolenorganisation aus, mit der Sie dieses Abonnement verknüpfen möchten.
- Wählen Sie im Feld **Vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für eine Organisation automatisch durch dieses neue Abonnement ersetzen möchten.

  Die Konsole ersetzt das vorhandene Abonnement für alle Anmeldeinformationen in der Organisation durch dieses neue Abonnement. Wenn ein Satz von Anmeldeinformationen nie mit einem Abonnement verknüpft war, wird dieses neue Abonnement nicht mit diesen Anmeldeinformationen verknüpft.

Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.

◦ Wählen Sie **Speichern**.

3. Navigieren Sie nach Abschluss dieses Vorgangs zurück zur Seite „Anmeldeinformationen“ in der Konsole und wählen Sie dieses neue Abonnement aus.



Ähnliche Informationen

- "Verwalten Sie kapazitätsbasierte BYOL-Lizenzen für Cloud Volumes ONTAP"
- "Verwalten Sie BYOL-Lizenzen für Datendienste"
- "Verwalten von AWS-Anmeldeinformationen und Abonnements"
- "Verwalten von Azure-Anmeldeinformationen und Abonnements"
- "Verwalten Sie Google Cloud-Anmeldeinformationen und -Abonnements"

Was Sie als Nächstes tun können (eingeschränkter Modus)

Nachdem Sie die NetApp Console im eingeschränkten Modus eingerichtet und ausgeführt haben, können Sie mit der Verwendung der im eingeschränkten Modus unterstützten Dienste beginnen.

Hilfe finden Sie in der Dokumentation zu diesen Diensten:

- "Azure NetApp Files Dokumentation"
- "Sicherungs- und Wiederherstellungsdokumente"
- "Klassifizierungsdokumente"
- "Cloud Volumes ONTAP Dokumente"
- "Dokumente zur digitalen Geldbörse"
- "On-Premises- ONTAP -Cluster-Dokumente"
- "Replikationsdokumente"

Ähnliche Informationen

"Bereitstellungsmodi der NetApp Console"