Installieren eines Agenten vor Ort

NetApp Console setup and administration

NetApp
January 27, 2026

Inhalt

Installieren eines Agenten vor Ort

Manuelle Installation eines Konsolen-Agenten vor Ort

Installieren Sie einen Konsolenagenten vor Ort, melden Sie sich dann an und richten Sie ihn für die Arbeit mit Ihrer Konsolenorganisation ein.

Wenn Sie ein VMWare-Benutzer sind, können Sie eine OVA verwenden, um einen Konsolenagenten in Ihrem VCenter zu installieren."Erfahren Sie mehr über die Installation eines Agenten in einem VCenter."

Vor der Installation müssen Sie sicherstellen, dass Ihr Host (VM oder Linux-Host) die Anforderungen erfüllt und dass der Konsolenagent ausgehenden Zugriff auf das Internet sowie auf Zielnetzwerke hat. Wenn Sie NetApp -Datendienste oder Cloud-Speicheroptionen wie Cloud Volumes ONTAP nutzen möchten, müssen Sie bei Ihrem Cloud-Anbieter Anmeldeinformationen erstellen, die Sie der Konsole hinzufügen, damit der Konsolenagent in Ihrem Namen Aktionen in der Cloud ausführen kann.

Vorbereiten der Installation des Konsolenagenten

Bevor Sie einen Konsolenagenten installieren, sollten Sie sicherstellen, dass Sie über einen Hostcomputer verfügen, der die Installationsanforderungen erfüllt. Sie müssen außerdem mit Ihrem Netzwerkadministrator zusammenarbeiten, um sicherzustellen, dass der Konsolenagent ausgehenden Zugriff auf die erforderlichen Endpunkte und Verbindungen zu Zielnetzwerken hat.

Überprüfen der Hostanforderungen für den Konsolenagenten

Führen Sie den Konsolenagenten auf einem x86-Host aus, der die Anforderungen an Betriebssystem, RAM und Port erfüllt. Stellen Sie sicher, dass Ihr Host diese Anforderungen erfüllt, bevor Sie den Konsolenagenten installieren.

Der Konsolenagent reserviert den UID- und GID-Bereich von 19000 bis 19200. Dieser Bereich ist fest und kann nicht geändert werden. Wenn Drittanbietersoftware auf Ihrem Host UIDs oder GIDs innerhalb dieses Bereichs verwendet, schlägt die Agenteninstallation fehl. NetApp empfiehlt die Verwendung eines Hosts, der frei von Software von Drittanbietern ist, um Konflikte zu vermeiden.

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.

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

Einrichten des Netzwerkzugriffs für den Konsolenagenten

Richten Sie den Netzwerkzugriff ein, um sicherzustellen, dass der Konsolenagent Ressourcen verwalten kann. Es benötigt Verbindungen zu Zielnetzwerken und ausgehenden Internetzugang zu bestimmten Endpunkten.

Verbindungen zu Zielnetzwerken

Der Konsolenagent erfordert eine Netzwerkverbindung zu dem Standort, an dem Sie Systeme erstellen und verwalten möchten. Beispielsweise das Netzwerk, in dem Sie Cloud Volumes ONTAP -Systeme oder ein Speichersystem in Ihrer lokalen Umgebung erstellen möchten.

Ausgehender Internetzugang

Der Netzwerkstandort, an dem Sie den Konsolenagenten bereitstellen, muss über eine ausgehende Internetverbindung verfügen, um bestimmte Endpunkte zu kontaktieren.

Von Computern kontaktierte Endpunkte bei Verwendung der webbasierten NetApp Console

Computer, die über einen Webbrowser auf die Konsole zugreifen, müssen in der Lage sein, mehrere Endpunkte zu kontaktieren. Sie müssen die Konsole verwenden, um den Konsolenagenten einzurichten und für die tägliche Verwendung der Konsole.

"Vorbereiten des Netzwerks für die NetApp Konsole" .

Vom Konsolenagenten kontaktierte Endpunkte

Der Konsolenagent benötigt ausgehenden Internetzugang, um die folgenden Endpunkte zu kontaktieren und Ressourcen und Prozesse innerhalb Ihrer öffentlichen Cloud-Umgebung für den täglichen Betrieb zu verwalten.

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Ein bei Ihnen vor Ort installierter Konsolenagent kann keine Ressourcen in Google Cloud verwalten. Wenn Sie Google Cloud-Ressourcen verwalten möchten, müssen Sie einen Agenten in Google Cloud installieren.

AWS

Wenn der Konsolenagent vor Ort installiert wird, benötigt er Netzwerkzugriff auf die folgenden AWS-Endpunkte, um in AWS bereitgestellte NetApp -Systeme (wie Cloud Volumes ONTAP) zu verwalten.

Vom Konsolenagenten kontaktierte Endpunkte

Der Konsolenagent benötigt ausgehenden Internetzugang, um die folgenden Endpunkte zu kontaktieren und Ressourcen und Prozesse innerhalb Ihrer öffentlichen Cloud-Umgebung für den täglichen Betrieb zu verwalten.

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
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.
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.

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://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.

Azurblau

Wenn der Konsolenagent vor Ort installiert wird, benötigt er Netzwerkzugriff auf die folgenden Azure-Endpunkte, um in Azure bereitgestellte NetApp -Systeme (wie Cloud Volumes ONTAP) zu verwalten.

Endpunkte	Zweck
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.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Zum Verwalten von Ressourcen in Azure China-Regionen.

Endpunkte	Zweck
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.

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"

Erstellen Sie Cloud-Berechtigungen für den Konsolenagenten für AWS oder Azure

Wenn Sie NetApp Datendienste in AWS oder Azure mit einem lokalen Konsolenagenten verwenden möchten, müssen Sie bei Ihrem Cloud-Anbieter Berechtigungen einrichten und nach der Installation die Anmeldeinformationen zum Konsolenagenten hinzufügen.

Sie müssen den Konsolenagenten in Google Cloud installieren, um alle dort vorhandenen Ressourcen zu verwalten.

AWS

Wenn der Konsolenagent vor Ort installiert ist, müssen Sie der Konsole AWS-Berechtigungen erteilen, indem Sie Zugriffsschlüssel für einen IAM-Benutzer hinzufügen, der über die erforderlichen Berechtigungen verfügt.

Sie müssen diese Authentifizierungsmethode verwenden, wenn der Konsolenagent vor Ort installiert ist. Sie können keine IAM-Rolle verwenden.

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.

Ergebnis

Sie sollten jetzt Zugriffsschlüssel für einen IAM-Benutzer haben, der über die erforderlichen Berechtigungen verfügt. Nachdem Sie den Konsolenagenten installiert haben, verknüpfen Sie diese Anmeldeinformationen mit dem Konsolenagenten von der Konsole aus.

Azurblau

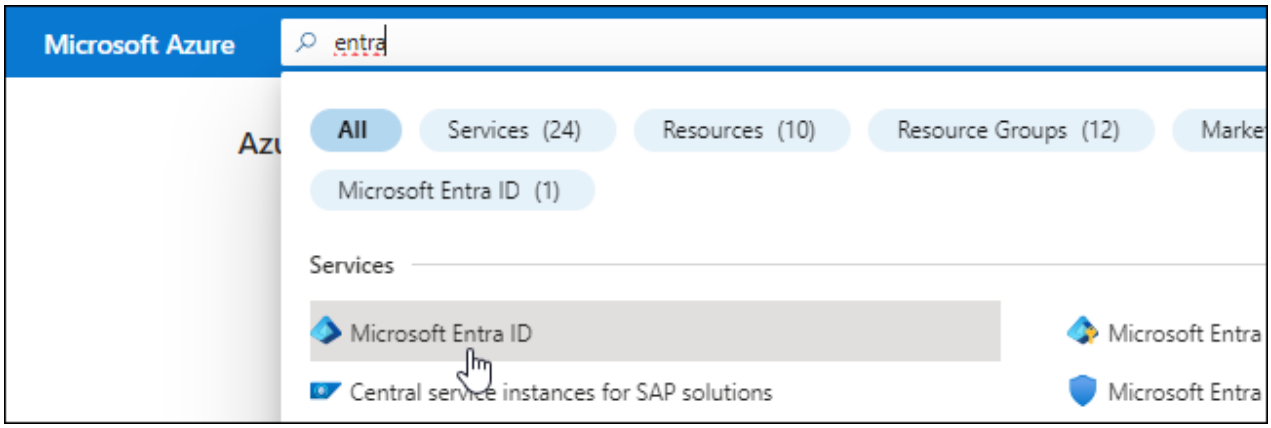
Wenn der Konsolen-Agent vor Ort installiert ist, müssen Sie dem Konsolen-Agenten Azure-Berechtigungen erteilen, indem Sie einen Dienstprinzipal in der Microsoft Entra ID einrichten und die Azure-Anmeldeinformationen abrufen, die der Konsolen-Agent benötigt.

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.

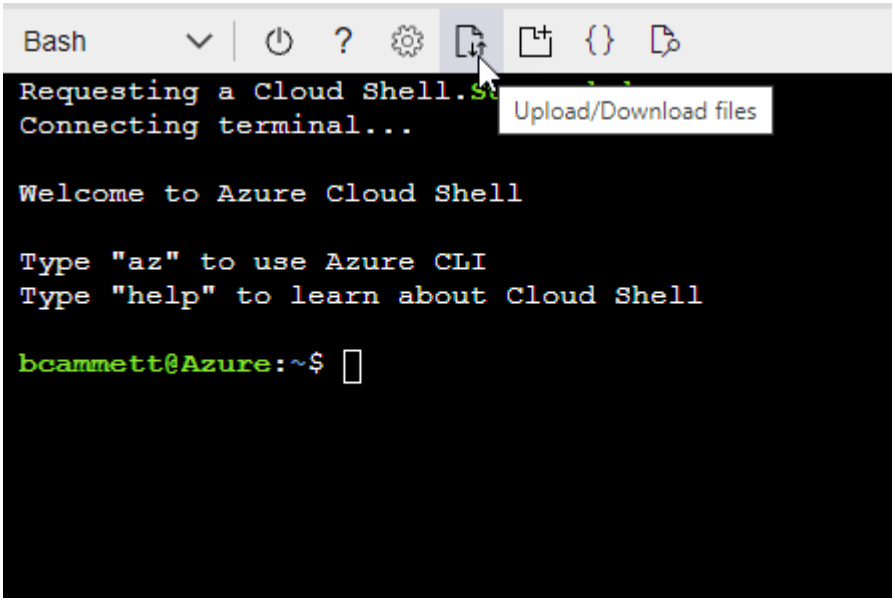
      Beispiel

      ```
      "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**.

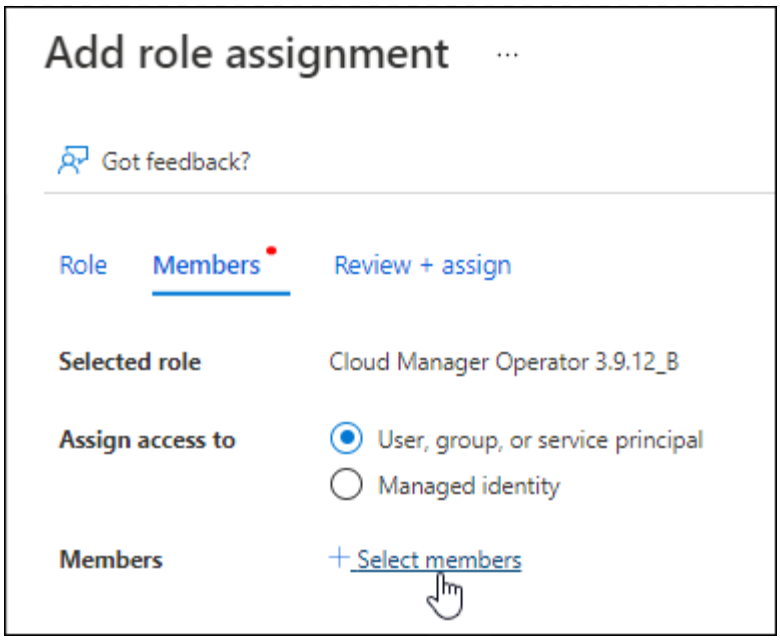
   b. Wählen Sie das Abonnement aus.

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

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

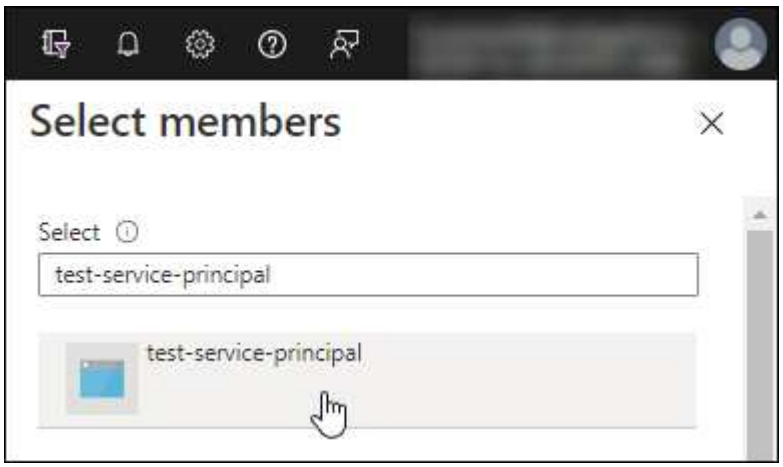
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - 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**.

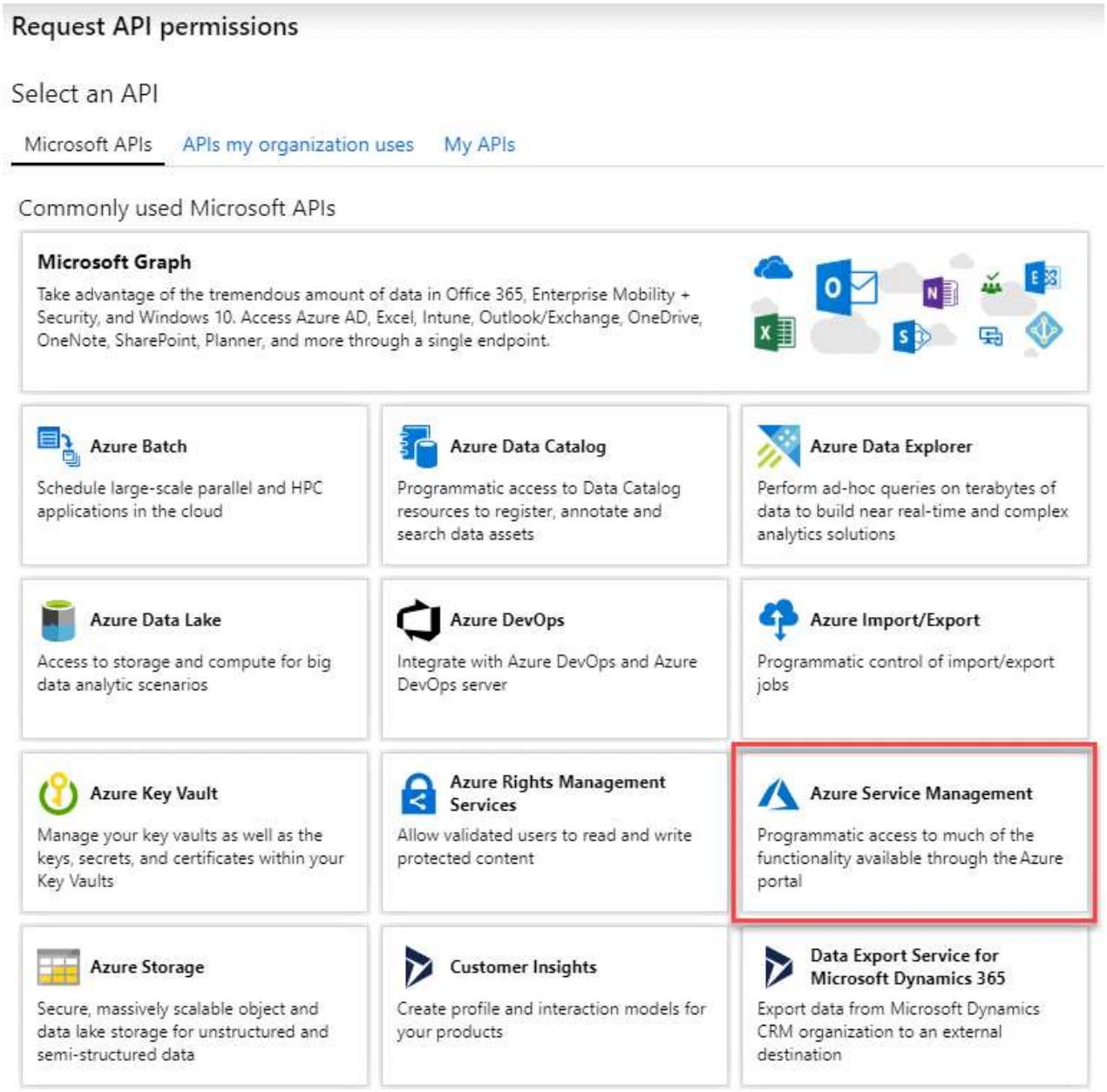
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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.

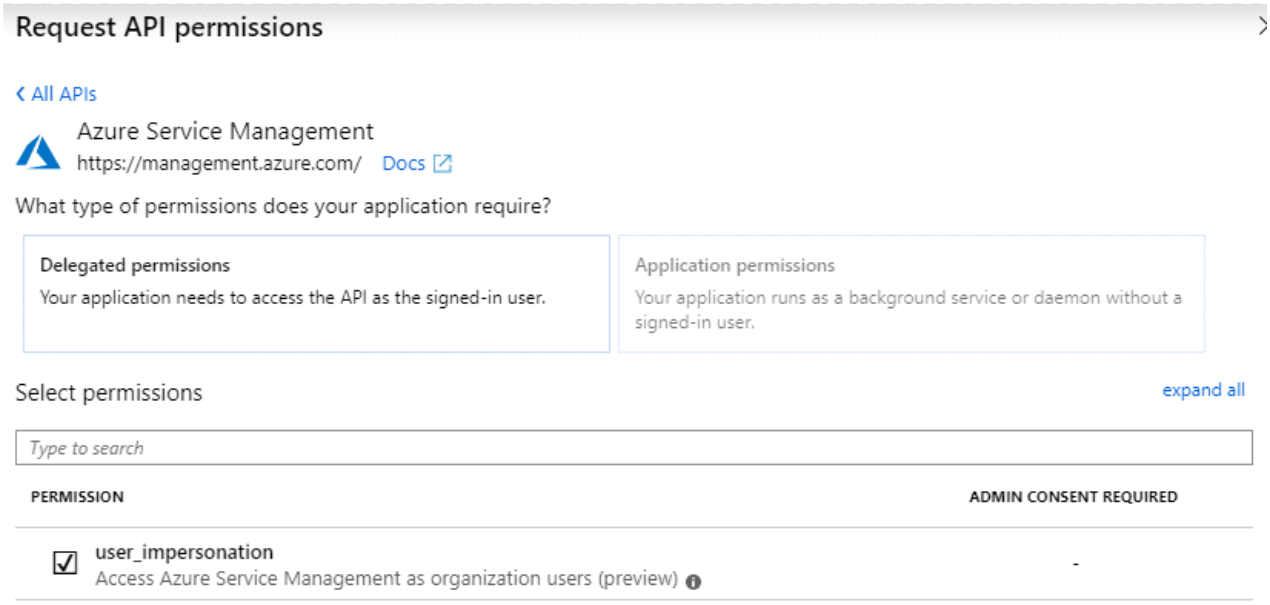
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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.

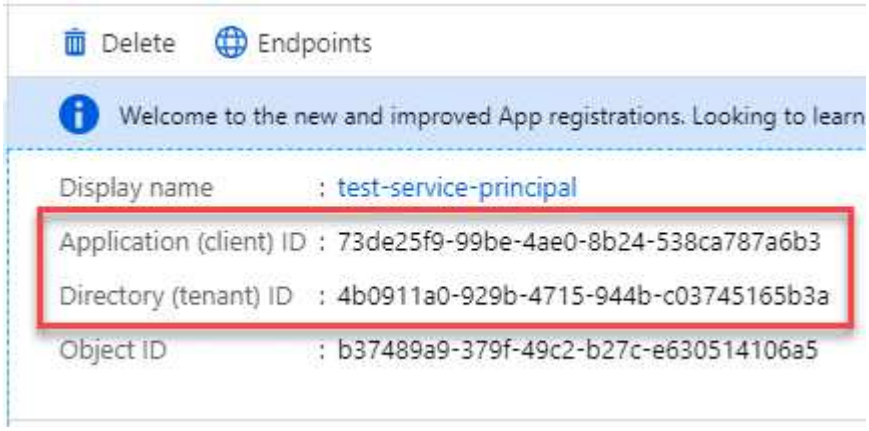


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

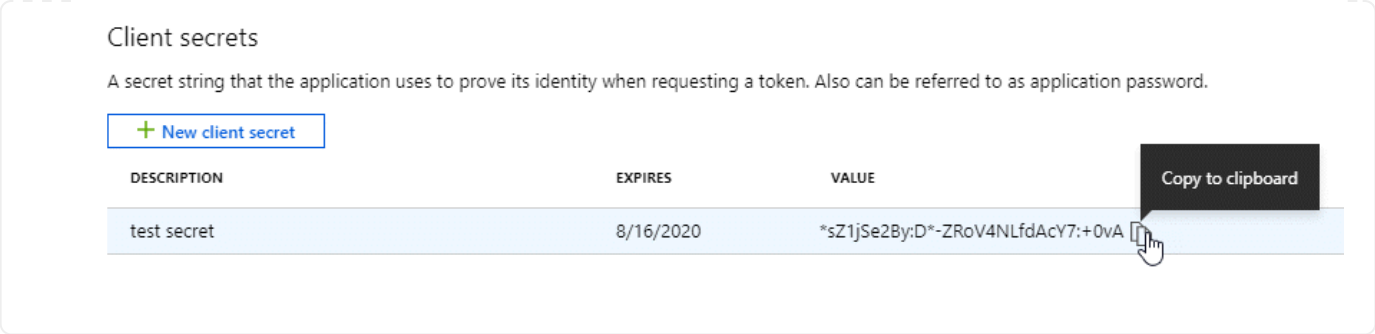
1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



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.



Manuelles Installieren eines Konsolenagenten

Wenn Sie einen Konsolenagenten manuell installieren, müssen Sie Ihre Computerumgebung so vorbereiten, dass sie die Anforderungen erfüllt. Sie benötigen eine Linux-Maschine und müssen je nach Linux-Betriebssystem Podman oder Docker installieren.

Installieren Sie Podman oder Docker Engine

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
```

Installieren Sie den Konsolenagenten manuell

Laden Sie die Konsolen-Agent-Software herunter und installieren Sie sie auf einem vorhandenen Linux-Host vor Ort.

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

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.

Wie geht es weiter?

Sie müssen den Konsolenagenten in der NetApp Console registrieren.

Registrieren Sie den Konsolenagenten bei der NetApp Console

Melden Sie sich bei der Konsole an und verknüpfen Sie den Konsolenagenten mit Ihrer Organisation. Die Art der Anmeldung hängt vom Modus ab, in dem Sie die Konsole verwenden. Wenn Sie die Konsole im Standardmodus verwenden, melden Sie sich über die SaaS-Website an. Wenn Sie die Konsole im eingeschränkten Modus verwenden, melden Sie sich lokal vom Konsolen-Agent-Host aus an.

Schritte

1. Öffnen Sie einen Webbrowser und geben Sie die Host-URL des Konsolenagenten ein:

   Die Host-URL der Konsole kann je nach Konfiguration des Hosts ein lokaler Host, eine private IP-Adresse oder eine öffentliche IP-Adresse sein. Wenn sich der Konsolenagent beispielsweise in der öffentlichen Cloud ohne öffentliche IP-Adresse befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der über eine Verbindung zum Host des Konsolenagenten verfügt.

2. Registrieren oder anmelden.
3. Richten Sie nach der Anmeldung die Konsole ein:
   a. Geben Sie die Konsolenorganisation an, die mit dem Konsolenagenten verknüpft werden soll.
   b. Geben Sie einen Namen für das System ein.
   c. Lassen Sie unter **Arbeiten Sie in einer sicheren Umgebung?** den eingeschränkten Modus deaktiviert.

      Der eingeschränkte Modus wird nicht unterstützt, wenn der Konsolen-Agent vor Ort installiert ist.

   d. Wählen Sie **Los geht’s**.

Geben Sie die Anmeldeinformationen des Cloud-Anbieters an die NetApp Console weiter

Nachdem Sie den Konsolen-Agenten installiert und eingerichtet haben, fügen Sie Ihre Cloud-Anmeldeinformationen hinzu, damit der Konsolen-Agent über die erforderlichen Berechtigungen zum Ausführen von Aktionen in AWS oder Azure verfügt.

AWS

Bevor Sie beginnen

Wenn Sie diese AWS-Anmeldeinformationen gerade erstellt haben, kann es einige Minuten dauern, bis sie verfügbar sind. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zur Konsole hinzufügen.

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**.

Sie können jetzt zu "NetApp Console" um mit der Verwendung des Konsolenagenten zu beginnen.

Azurblau

Bevor Sie beginnen

Wenn Sie diese Azure-Anmeldeinformationen gerade erstellt haben, kann es einige Minuten dauern, bis sie verfügbar sind. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zum Konsolenagenten hinzufügen.

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

Der Konsolenagent verfügt jetzt über die erforderlichen Berechtigungen, um in Ihrem Namen Aktionen in Azure auszuführen. Sie können jetzt zu "NetApp Console" um mit der Verwendung des Konsolenagenten

zu beginnen.

Installieren Sie einen Konsolenagenten vor Ort mit VCenter

Wenn Sie ein VMWare-Benutzer sind, können Sie eine OVA verwenden, um einen Konsolenagenten in Ihrem VCenter zu installieren. Der OVA-Download oder die URL ist über die NetApp Console verfügbar.

Wenn Sie einen Konsolenagenten mit Ihren VCenter-Tools installieren, können Sie die VM-Webkonsole verwenden, um Wartungsaufgaben durchzuführen."Erfahren Sie mehr über die VM-Konsole für den Agenten."

Vorbereiten der Installation des Konsolenagenten

Stellen Sie vor der Installation sicher, dass Ihr VM-Host die Anforderungen erfüllt und der Konsolenagent auf das Internet und die Zielnetzwerke zugreifen kann. Um NetApp -Datendienste oder Cloud Volumes ONTAP zu verwenden, erstellen Sie Anmeldeinformationen für den Cloud-Anbieter, damit der Konsolenagent Aktionen in Ihrem Namen ausführen kann.

Überprüfen der Hostanforderungen für den Konsolenagenten

Stellen Sie sicher, dass Ihr Hostcomputer die Installationsanforderungen erfüllt, bevor Sie den Konsolenagenten installieren.

- CPU: 8 Kerne oder 8 vCPUs
- Arbeitsspeicher: 32 GB
- Festplattenspeicher: 165 GB (Thick Provisioning)
- vSphere 7.0 oder höher
- ESXi-Host 7.03 oder höher

Installieren Sie den Agenten in einer vCenter-Umgebung und nicht direkt auf einem ESXi-Host.

Einrichten des Netzwerkzugriffs für den Konsolenagenten

Arbeiten Sie mit Ihrem Netzwerkadministrator zusammen, um sicherzustellen, dass der Konsolenagent ausgehenden Zugriff auf die erforderlichen Endpunkte und Verbindungen zu Zielnetzwerken hat.

Verbindungen zu Zielnetzwerken

Der Konsolenagent erfordert eine Netzwerkverbindung zu dem Standort, an dem Sie Systeme erstellen und verwalten möchten. Beispielsweise das Netzwerk, in dem Sie Cloud Volumes ONTAP -Systeme oder ein Speichersystem in Ihrer lokalen Umgebung erstellen möchten.

Ausgehender Internetzugang

Der Netzwerkstandort, an dem Sie den Konsolenagenten bereitstellen, muss über eine ausgehende Internetverbindung verfügen, um bestimmte Endpunkte zu kontaktieren.

Von Computern kontaktierte Endpunkte bei Verwendung der webbasierten NetApp Console

Computer, die über einen Webbrowser auf die Konsole zugreifen, müssen in der Lage sein, mehrere Endpunkte zu kontaktieren. Sie müssen die Konsole verwenden, um den Konsolenagenten einzurichten

und für die tägliche Verwendung der Konsole.

"Vorbereiten des Netzwerks für die NetApp Konsole" .

Vom Konsolenagenten kontaktierte Endpunkte

Der Konsolenagent benötigt ausgehenden Internetzugang, um die folgenden Endpunkte zu kontaktieren und Ressourcen und Prozesse innerhalb Ihrer öffentlichen Cloud-Umgebung für den täglichen Betrieb zu verwalten.

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Sie können keine Ressourcen in Google Cloud verwalten, wenn bei Ihnen vor Ort ein Konsolenagent installiert ist. Installieren Sie zum Verwalten von Google Cloud-Ressourcen einen Agenten in Google Cloud.

AWS

Wenn der Konsolenagent vor Ort installiert wird, benötigt er Netzwerkzugriff auf die folgenden AWS-Endpunkte, um in AWS bereitgestellte NetApp -Systeme (wie Cloud Volumes ONTAP) zu verwalten.

Vom Konsolenagenten kontaktierte Endpunkte

Der Konsolenagent benötigt ausgehenden Internetzugang, um die folgenden Endpunkte zu kontaktieren und Ressourcen und Prozesse innerhalb Ihrer öffentlichen Cloud-Umgebung für den täglichen Betrieb zu verwalten.

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
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.
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.

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://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.

Azurblau

Wenn der Konsolenagent vor Ort installiert wird, benötigt er Netzwerkzugriff auf die folgenden Azure-Endpunkte, um in Azure bereitgestellte NetApp -Systeme (wie Cloud Volumes ONTAP) zu verwalten.

Endpunkte	Zweck
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.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Zum Verwalten von Ressourcen in Azure China-Regionen.

Endpunkte	Zweck
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.

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"

Erstellen Sie Cloud-Berechtigungen für den Konsolenagenten für AWS oder Azure

Wenn Sie NetApp Datendienste in AWS oder Azure mit einem lokalen Konsolenagenten verwenden möchten, müssen Sie bei Ihrem Cloud-Anbieter Berechtigungen einrichten, damit Sie dem Konsolenagenten nach der Installation die Anmeldeinformationen hinzufügen können.

Sie können keine Ressourcen in Google Cloud verwalten, wenn bei Ihnen vor Ort ein Konsolenagent installiert ist. Wenn Sie Google Cloud-Ressourcen verwalten möchten, müssen Sie einen Agenten in Google Cloud installieren.

AWS

Stellen Sie für lokale Konsolenagenten AWS-Berechtigungen bereit, indem Sie IAM-Benutzerzugriffsschlüssel hinzufügen.

Verwenden Sie IAM-Benutzerzugriffsschlüssel für lokale Konsolen-Agenten. IAM-Rollen werden für lokale Konsolen-Agenten nicht unterstützt.

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.

Ergebnis

Sie sollten jetzt über IAM-Benutzerzugriffsschlüssel mit den erforderlichen Berechtigungen verfügen. Nachdem Sie den Konsolenagenten installiert haben, verknüpfen Sie diese Anmeldeinformationen mit dem Konsolenagenten aus der Konsole.

Azurblau

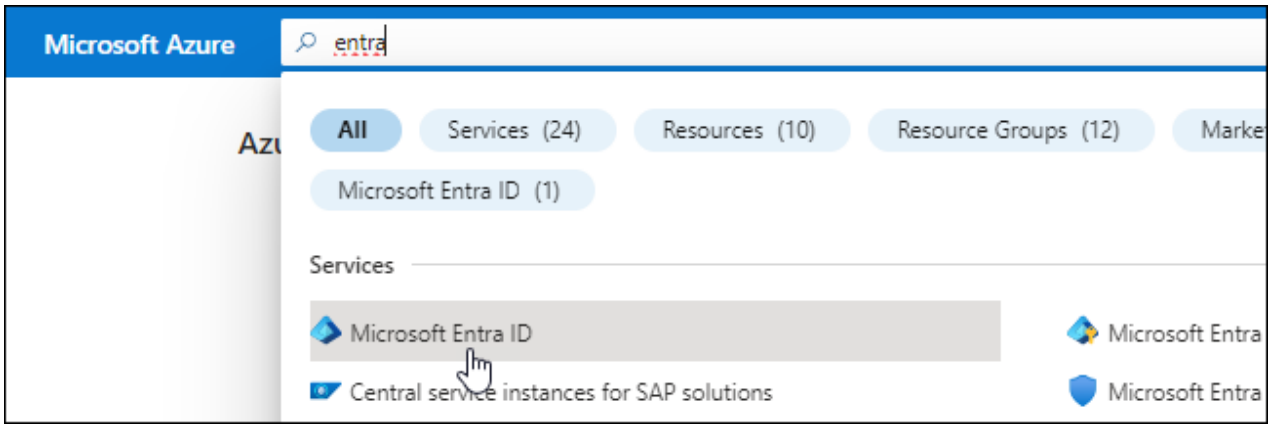
Wenn der Konsolen-Agent vor Ort installiert ist, müssen Sie dem Konsolen-Agenten Azure-Berechtigungen erteilen, indem Sie einen Dienstprinzipal in der Microsoft Entra ID einrichten und die Azure-Anmeldeinformationen abrufen, die der Konsolen-Agent benötigt.

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.

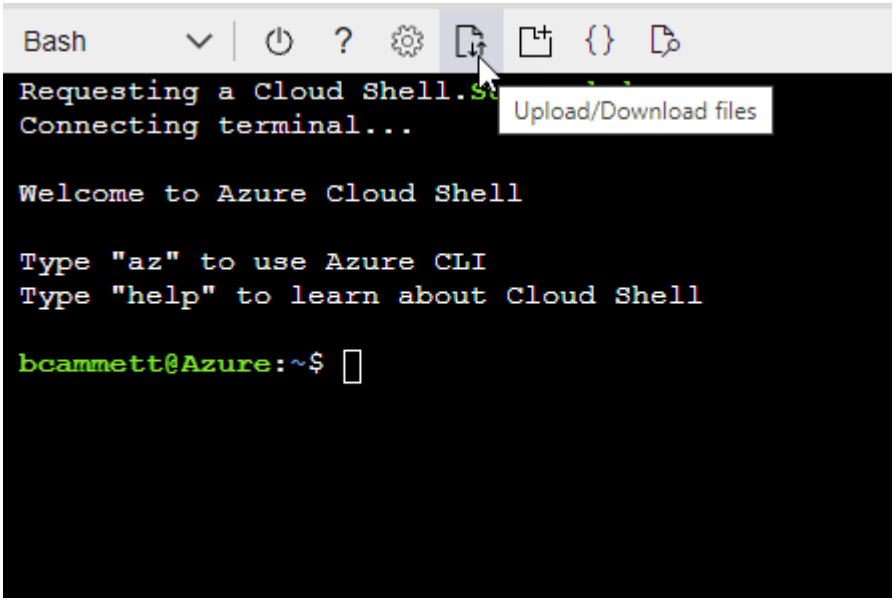
      Beispiel

      ```
      "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**.

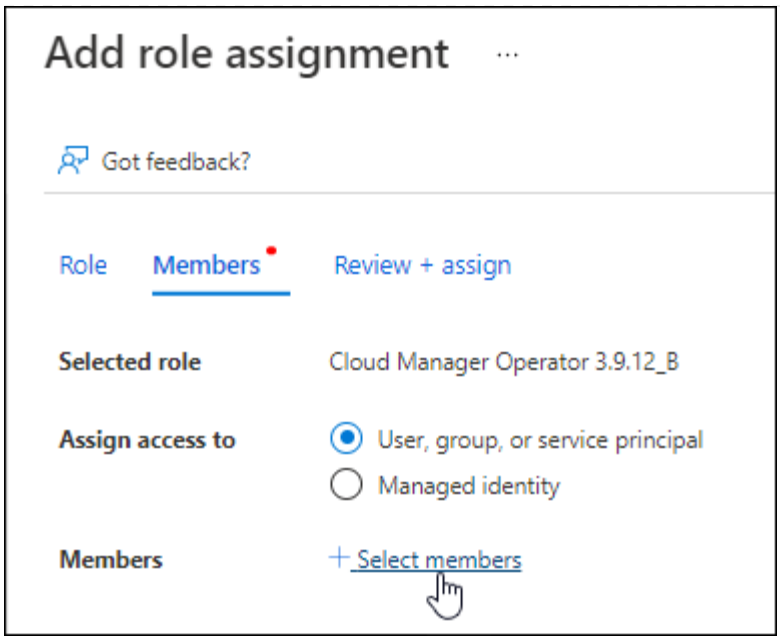
   b. Wählen Sie das Abonnement aus.

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

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

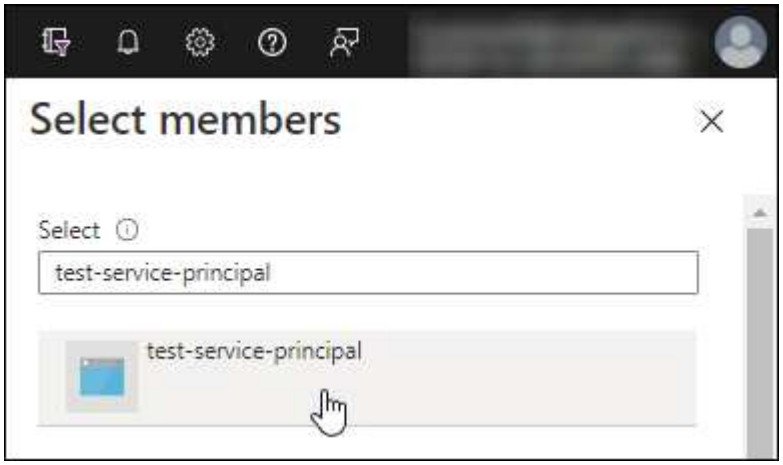
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - 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**.

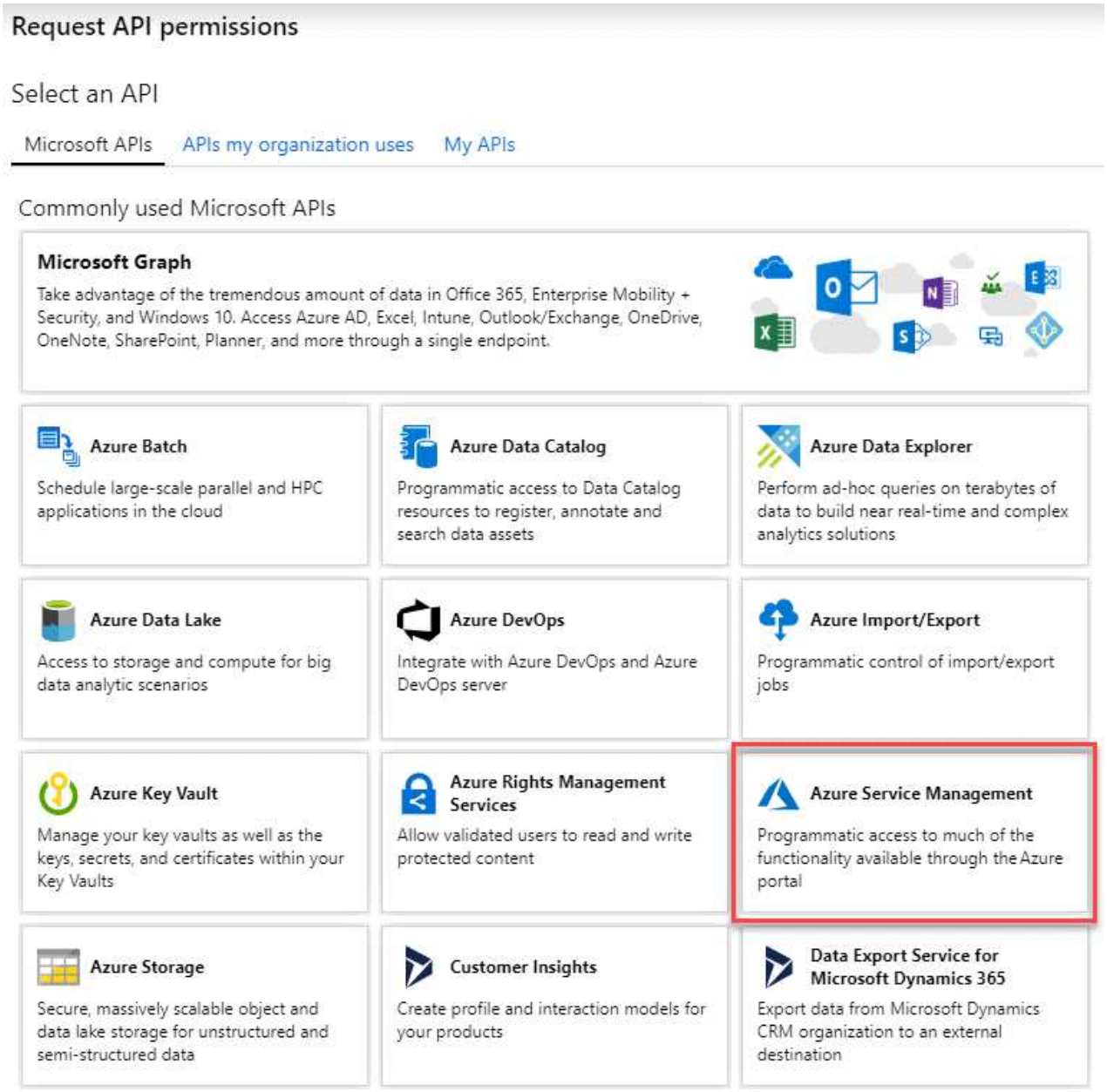
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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.

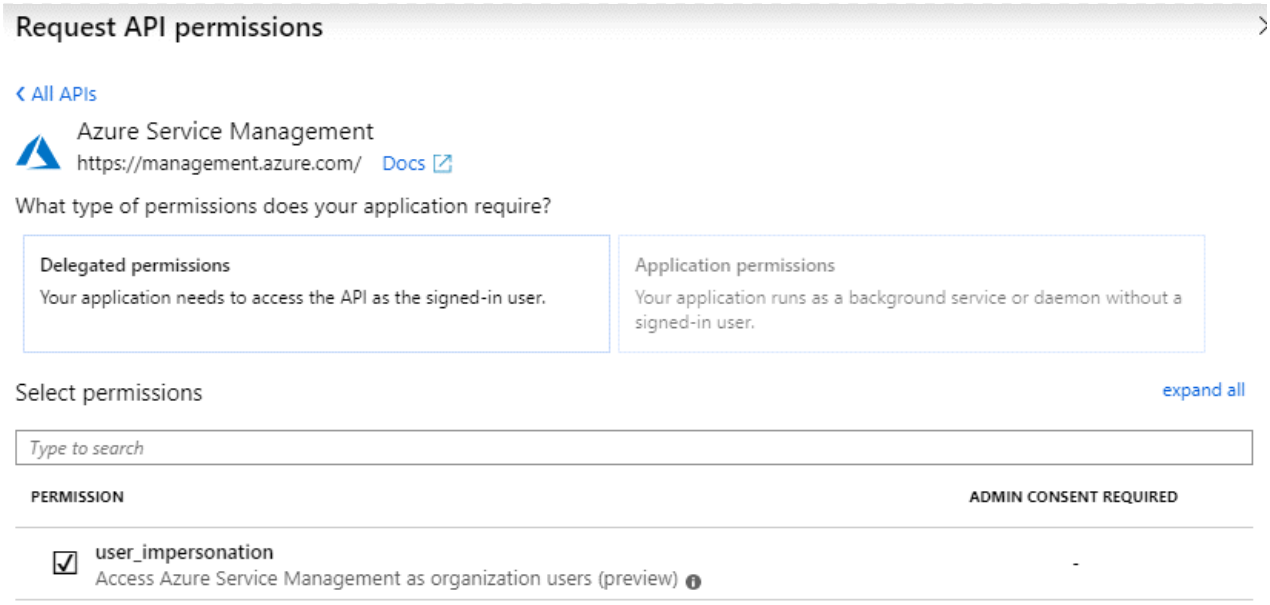
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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.

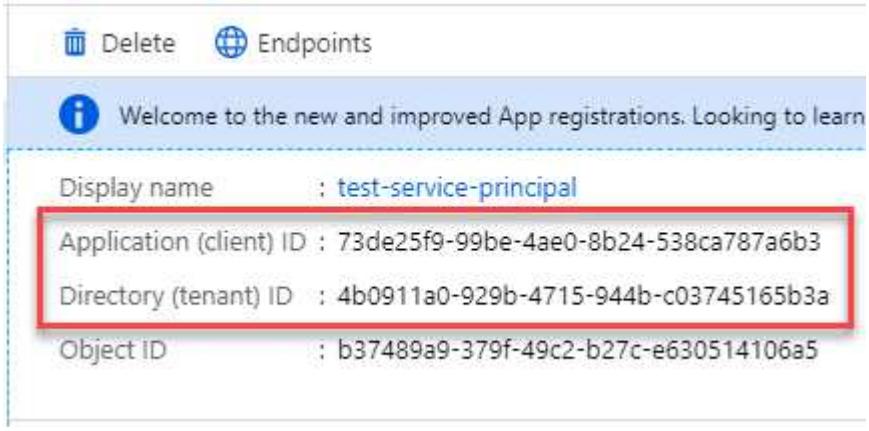


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

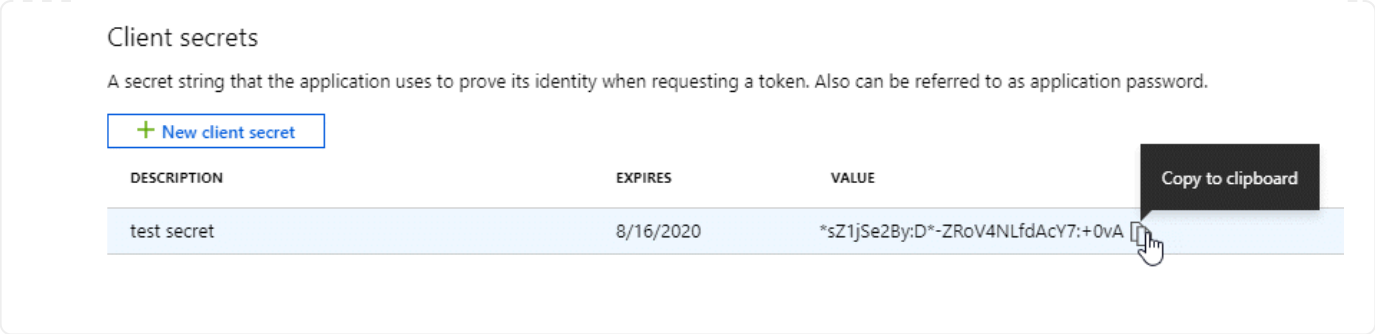
1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



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.



Installieren Sie einen Konsolenagenten in Ihrer VCenter-Umgebung

NetApp unterstützt die Installation des Konsolenagenten in Ihrer VCenter-Umgebung. Die OVA-Datei enthält ein vorkonfiguriertes VM-Image, das Sie in Ihrer VMware-Umgebung bereitstellen können. Ein Dateidownload oder eine URL-Bereitstellung ist direkt über die NetApp Console möglich. Es umfasst die Konsolenagent-Software und ein selbstsigniertes Zertifikat.

Laden Sie die OVA herunter oder kopieren Sie die URL

Laden Sie die OVA herunter oder kopieren Sie die OVA-URL direkt von der NetApp Console.

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** die Option **Agent bereitstellen > Vor Ort** aus.
3. Wählen Sie **Mit OVA**.
4. Sie können entweder die OVA herunterladen oder die URL zur Verwendung in VCenter kopieren.

Stellen Sie den Agenten in Ihrem VCenter bereit

Melden Sie sich bei Ihrer VCenter-Umgebung an, um den Agenten bereitzustellen.

Schritte

1. Laden Sie das selbstsignierte Zertifikat zu Ihren vertrauenswürdigen Zertifikaten hoch, wenn Ihre Umgebung dies erfordert. Sie ersetzen dieses Zertifikat nach der Installation."Erfahren Sie, wie Sie das selbstsignierte Zertifikat ersetzen."
2. Stellen Sie die OVA aus der Inhaltsbibliothek oder dem lokalen System bereit.

Vom lokalen System	Aus der Inhaltsbibliothek
a. Klicken Sie mit der rechten Maustaste und wählen Sie **OVF-Vorlage bereitstellen…**. b. Wählen Sie die OVA-Datei aus der URL aus oder navigieren Sie zu ihrem Speicherort und wählen Sie dann **Weiter**.	a. Gehen Sie zu Ihrer Inhaltsbibliothek und wählen Sie die OVA des Konsolenagenten aus. b. Wählen Sie **Aktionen** > **Neue VM aus dieser Vorlage**

3. Schließen Sie den Assistenten „OVF-Vorlage bereitstellen“ ab, um den Konsolenagenten bereitzustellen.
4. Wählen Sie einen Namen und einen Ordner für die VM aus und wählen Sie dann **Weiter**.
5. Wählen Sie eine Computeressource aus und klicken Sie dann auf **Weiter**.
6. Überprüfen Sie die Details der Vorlage und wählen Sie dann **Weiter**.
7. Akzeptieren Sie die Lizenzvereinbarung und wählen Sie dann **Weiter**.

8. Wählen Sie den Typ der Proxy-Konfiguration, den Sie verwenden möchten: expliziter Proxy, transparenter Proxy oder kein Proxy.
9. Wählen Sie den Datenspeicher aus, in dem Sie die VM bereitstellen möchten, und wählen Sie dann **Weiter**. Stellen Sie sicher, dass es die Hostanforderungen erfüllt.
10. Wählen Sie das Netzwerk aus, mit dem Sie die VM verbinden möchten, und wählen Sie dann **Weiter**. Stellen Sie sicher, dass das Netzwerk IPv4 ist und über ausgehenden Internetzugriff auf die erforderlichen Endpunkte verfügt.
11. Füllen Sie im Fenster **Vorlage anpassen** die folgenden Felder aus:
    - **Proxy-Informationen**
      - Wenn Sie einen expliziten Proxy ausgewählt haben, geben Sie den Hostnamen oder die IP-Adresse und die Portnummer des Proxyservers sowie den Benutzernamen und das Kennwort ein.
      - Wenn Sie einen transparenten Proxy ausgewählt haben, laden Sie das entsprechende Zertifikat hoch.
    - **Konfiguration der virtuellen Maschine**
      - **Konfigurationsprüfung überspringen**: Dieses Kontrollkästchen ist standardmäßig deaktiviert, was bedeutet, dass der Agent eine Konfigurationsprüfung durchführt, um den Netzwerkzugriff zu validieren.
        - NetApp empfiehlt, dieses Kontrollkästchen deaktiviert zu lassen, damit die Installation eine Konfigurationsprüfung des Agenten umfasst. Die Konfigurationsprüfung bestätigt, dass der Agent Netzwerkzugriff auf die erforderlichen Endpunkte hat. Wenn die Bereitstellung aufgrund von Verbindungsproblemen fehlschlägt, können Sie auf den Validierungsbericht und die Protokolle vom Agent-Host zugreifen. In einigen Fällen können Sie die Prüfung überspringen, wenn Sie sicher sind, dass der Agent über Netzwerkzugriff verfügt. Wenn Sie beispielsweise immer noch die"vorherige Endpunkte" für Agent-Upgrades verwendet wird, schlägt die Validierung mit einem Fehler fehl. Um dies zu vermeiden, aktivieren Sie das Kontrollkästchen, um die Installation ohne Validierungsprüfung durchzuführen. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" .
      - **Wartungskennwort**: Legen Sie das Kennwort für die `maint` Benutzer, der Zugriff auf die Agenten-Wartungskonsole ermöglicht.
      - **NTP-Server**: Geben Sie einen oder mehrere NTP-Server für die Zeitsynchronisierung an.
      - **Hostname**: Legen Sie den Hostnamen für diese VM fest. Die Suchdomäne darf nicht enthalten sein. Beispielsweise sollte ein FQDN von console10.searchdomain.company.com als console10 eingegeben werden.
      - **Primärer DNS**: Geben Sie den primären DNS-Server an, der für die Namensauflösung verwendet werden soll.
      - **Sekundärer DNS**: Geben Sie den sekundären DNS-Server an, der für die Namensauflösung verwendet werden soll.
      - Suchdomänen: Geben Sie den Suchdomänennamen an, der beim Auflösen des Hostnamens verwendet werden soll. Wenn der FQDN beispielsweise console10.searchdomain.company.com lautet, geben Sie searchdomain.company.com ein.
      - **IPv4-Adresse**: Die IP-Adresse, die dem Hostnamen zugeordnet ist.
      - **IPv4-Subnetzmaske**: Die Subnetzmaske für die IPv4-Adresse.
      - **IPv4-Gateway-Adresse**: Die Gateway-Adresse für die IPv4-Adresse.
12. Wählen Sie **Weiter**.
13. Überprüfen Sie die Details im Fenster **Bereit zum Abschließen** und wählen Sie **Fertig**.

Die vSphere-Taskleiste zeigt den Fortschritt der Bereitstellung des Konsolenagenten an.

14. Schalten Sie die VM ein.

> Wenn die Bereitstellung fehlschlägt, können Sie auf den Validierungsbericht und die Protokolle vom Agent-Host zugreifen."Erfahren Sie, wie Sie Installationsprobleme beheben."

Registrieren Sie den Konsolenagenten bei der NetApp Console

Melden Sie sich bei der Konsole an und verknüpfen Sie den Konsolenagenten mit Ihrer Organisation. Die Art der Anmeldung hängt vom Modus ab, in dem Sie die Konsole verwenden. Wenn Sie die Konsole im Standardmodus verwenden, melden Sie sich über die SaaS-Website an. Wenn Sie die Konsole im eingeschränkten oder privaten Modus verwenden, melden Sie sich lokal vom Konsolen-Agent-Host aus an.

Schritte

1. Öffnen Sie einen Webbrowser und geben Sie die Host-URL des Konsolenagenten ein:

   Die Host-URL der Konsole kann je nach Konfiguration des Hosts ein lokaler Host, eine private IP-Adresse oder eine öffentliche IP-Adresse sein. Wenn sich der Konsolenagent beispielsweise in der öffentlichen Cloud ohne öffentliche IP-Adresse befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der über eine Verbindung zum Host des Konsolenagenten verfügt.

2. Registrieren oder anmelden.
3. Richten Sie nach der Anmeldung die Konsole ein:
   a. Geben Sie die Konsolenorganisation an, die mit dem Konsolenagenten verknüpft werden soll.
   b. Geben Sie einen Namen für das System ein.
   c. Lassen Sie unter **Arbeiten Sie in einer sicheren Umgebung?** den eingeschränkten Modus deaktiviert.

      Der eingeschränkte Modus wird nicht unterstützt, wenn der Konsolen-Agent vor Ort installiert ist.

   d. Wählen Sie **Los geht's**.

Fügen Sie der Konsole Anmeldeinformationen des Cloud-Anbieters hinzu

Nachdem Sie den Konsolen-Agenten installiert und eingerichtet haben, fügen Sie Ihre Cloud-Anmeldeinformationen hinzu, damit der Konsolen-Agent über die erforderlichen Berechtigungen zum Ausführen von Aktionen in AWS oder Azure verfügt.

AWS

Bevor Sie beginnen

Wenn Sie diese AWS-Anmeldeinformationen gerade erstellt haben, kann es einige Minuten dauern, bis sie verfügbar sind. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zur Konsole hinzufügen.

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**.

Sie können jetzt zu "NetApp Console" um mit der Verwendung des Konsolenagenten zu beginnen.

Azurblau

Bevor Sie beginnen

Wenn Sie diese Azure-Anmeldeinformationen gerade erstellt haben, kann es einige Minuten dauern, bis sie verfügbar sind. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zum Konsolenagenten hinzufügen.

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

Der Konsolenagent verfügt jetzt über die erforderlichen Berechtigungen, um in Ihrem Namen Aktionen in Azure auszuführen. Sie können jetzt zu "NetApp Console" um mit der Verwendung des Konsolenagenten

zu beginnen.

Ports für den lokalen Konsolenagenten

Der Konsolenagent verwendet *eingehende* Ports, wenn er manuell auf einem lokalen Linux-Host installiert wird. Beziehen Sie sich bei Planungen auf diese Häfen.

Diese eingehenden Regeln gelten für alle Bereitstellungsmodi der NetApp Console .

Protokoll	Hafen	Zweck
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