Konsolenagenten

NetApp Console setup and administration

NetApp
January 27, 2026

Inhalt

Konsolenagenten

Erfahren Sie mehr über NetApp Console -Agenten

Sie verwenden einen Console-Agenten, um die NetApp Console mit Ihrer Infrastruktur zu verbinden und Speicherlösungen sicher über AWS-, Azure-, Google Cloud- oder On-Premises-Umgebungen hinweg zu orchestrieren sowie Datensicherungsdienste zu nutzen.

Ein Konsolenagent ermöglicht Ihnen Folgendes:

- Orchestrieren Sie Speicherverwaltungsaufgaben über die NetApp Console , wie z. B. die Bereitstellung von Cloud Volumes ONTAP, das Einrichten von Speichervolumes, die Verwendung der Datenklassifizierung und vieles mehr.
- Authentifizieren Sie sich mithilfe der IAM-Rollen Ihres Cloud-Anbieters für die Integration der Abonnementabrechnung.
- Nutzen Sie erweiterte Datendienste (NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience und NetApp Cloud Tiering).
- Verwenden Sie die Konsole im eingeschränkten Modus.

Wenn Sie keine erweiterte Orchestrierung oder Datensicherung benötigen, können Sie lokale ONTAP Cluster und Cloud-native Speicherdienste zentral verwalten, ohne einen Agenten einzusetzen. Überwachungs- und Datenmobilitätstools sind ebenfalls verfügbar.

Die folgende Tabelle zeigt, welche Funktionen und Dienste Sie mit und ohne Console-Agent nutzen können.

	Beim Agenten erhältlich	**Ohne Makler erhältlich**
Unterstützte Speichersysteme:		
Amazon FSx für ONTAP	Ja (Erkennungs- und Verwaltungsfunktionen)	Ja (nur Discovery)
Amazon S3-Speicher	Ja	Nein
Azure Blob-Speicher	Ja	Ja
Azure NetApp Files	Ja	Ja
Cloud Volumes ONTAP	Ja	Nein
Systeme der E-Serie	Ja	Nein
Google Cloud NetApp Volumes	Ja	Ja
Google Cloud-Speicher-Buckets	Ja	Nein

	Beim Agenten erhältlich	Ohne Makler erhältlich
StorageGRID -Systeme	Ja	Nein
On-Premises ONTAP Cluster (erweiterte Verwaltung und Erkennung)	Ja (fortschrittliches Management und Entdeckung)	Nein (nur grundlegende Entdeckung)
Verfügbare Speichermanagementdienste:		
Warnungen	Ja	Nein
Automatisierungszentrum	Ja	Ja
Digital Advisor (Active IQ)	Ja	Nein
Lizenz- und Abonnementverwaltung	Ja	Nein
Wirtschaftlichkeit	Ja	Nein
Dashboard-Metriken der Startseite	Ja[2]	Nein
Lebenszyklusplanung	Ja	Nr. 1
Nachhaltigkeit	Ja	Nein
Software-Updates	Ja	Ja
NetApp Workloads	Ja	Ja
Verfügbare Datendienste:		
NetApp Backup and Recovery	Ja	Nein
Datenklassifizierung	Ja	Nein
NetApp Cloud Tiering	Ja	Nein
NetApp Copy and Sync	Ja	Nein
NetApp Disaster Recovery	Ja	Nein
NetApp Ransomware Resilience	Ja	Nein
NetApp Volume Caching	Ja	Nein

[1] Die Lebenszyklusplanung kann auch ohne Konsolenagent angezeigt werden, jedoch ist ein Konsolenagent

erforderlich, um Aktionen auszulösen.

[2] Für genaue Messwerte auf der Startseite sind entsprechend dimensionierte und konfigurierte Konsolenagenten erforderlich.

Konsolenagenten müssen jederzeit betriebsbereit sein

Konsolenagenten sind ein grundlegender Bestandteil der NetApp Console. Es liegt in Ihrer Verantwortung (des Kunden), sicherzustellen, dass die relevanten Agenten jederzeit aktiv, betriebsbereit und erreichbar sind. Die Konsole kann kurze Agentenausfälle bewältigen, Infrastrukturfehler müssen Sie jedoch schnell beheben.

Diese Dokumentation unterliegt der EULA. Der Betrieb des Produkts außerhalb der Dokumentation kann seine Funktionalität und Ihre EULA-Rechte beeinträchtigen.

Unterstützte Standorte

Sie können Agenten an den folgenden Orten installieren:

- Amazon Web Services
- Microsoft Azure

  Stellen Sie einen Konsolenagenten in Azure in derselben Region bereit wie die von ihm verwalteten Cloud Volumes ONTAP -Systeme. Alternativ können Sie es in der "Azure-Regionenpaar" . Dadurch wird sichergestellt, dass zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten eine Azure Private Link-Verbindung verwendet wird. "Erfahren Sie, wie Cloud Volumes ONTAP einen Azure Private Link verwendet"

- Google Cloud

  Um die Konsole und Datendienste mit Google Cloud zu verwenden, stellen Sie Ihren Agenten in Google Cloud bereit.

- Bei Ihnen vor Ort

Kommunikation mit Cloud-Anbietern

Der Agent verwendet TLS 1.3 für die gesamte Kommunikation mit AWS, Azure und Google Cloud.

Eingeschränkter Modus

Um die Konsole im eingeschränkten Modus zu verwenden, installieren Sie einen Konsolenagenten und greifen auf die Konsolenschnittstelle zu, die lokal auf dem Konsolenagenten ausgeführt wird.

"Erfahren Sie mehr über die Bereitstellungsmodi der NetApp Console" .

So installieren Sie einen Konsolenagenten

Sie können einen Konsolenagenten direkt von der Konsole, vom Marktplatz Ihres Cloud-Anbieters oder durch manuelle Installation der Software auf Ihrem eigenen Linux-Host oder in Ihrer VCenter-Umgebung installieren.

- "Erfahren Sie mehr über die Bereitstellungsmodi der NetApp Console"
- "Erste Schritte mit der NetApp Console im Standardmodus"

- "Erste Schritte mit der NetApp Console im eingeschränkten Modus"

Cloud-Anbieter-Berechtigungen

Sie benötigen spezielle Berechtigungen, um den Konsolenagenten direkt von der NetApp Console aus zu erstellen, und einen weiteren Satz von Berechtigungen für den Konsolenagenten selbst. Wenn Sie den Konsolenagenten in AWS oder Azure direkt von der Konsole aus erstellen, erstellt die Konsole den Konsolenagenten mit den erforderlichen Berechtigungen.

Wenn Sie die Konsole im Standardmodus verwenden, hängt die Art und Weise, wie Sie Berechtigungen erteilen, davon ab, wie Sie den Konsolenagenten erstellen möchten.

Informationen zum Einrichten von Berechtigungen finden Sie hier:

- Standardmodus
  - "Agent-Installationsoptionen in AWS"
  - "Agent-Installationsoptionen in Azure"
  - "Agent-Installationsoptionen in Google Cloud"
  - "Einrichten von Cloudberechtigungen für lokale Bereitstellungen"
- "Berechtigungen für den eingeschränkten Modus einrichten"

Informationen zu den genauen Berechtigungen, die der Konsolenagent für den täglichen Betrieb benötigt, finden Sie auf den folgenden Seiten:

- "Erfahren Sie, wie der Konsolenagent AWS-Berechtigungen verwendet"
- "Erfahren Sie, wie der Konsolen-Agent Azure-Berechtigungen verwendet."
- "Erfahren Sie, wie der Konsolenagent Google Cloud-Berechtigungen verwendet"

Es liegt in Ihrer Verantwortung, die Richtlinien des Konsolenagenten zu aktualisieren, wenn in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. In den Versionshinweisen sind neue Berechtigungen aufgeführt.

Agent-Upgrades

NetApp aktualisiert die Agentensoftware monatlich, um Funktionen hinzuzufügen und die Stabilität zu verbessern. Einige Konsolenfunktionen, wie Cloud Volumes ONTAP und die lokale ONTAP Clusterverwaltung, basieren auf der Version und den Einstellungen des Konsolenagenten.

Wenn Sie Ihren Agenten in der Cloud installieren, aktualisiert sich der Console-Agent automatisch, sofern er über einen Internetzugang verfügt.

Betriebssystem- und VM-Wartung

Die Wartung des Betriebssystems auf dem Konsolenagent-Host liegt in Ihrer (Kunden-)Verantwortung. Beispielsweise sollten Sie (der Kunde) Sicherheitsupdates auf das Betriebssystem auf dem Konsolenagent-Host anwenden, indem Sie die Standardverfahren Ihres Unternehmens zur Betriebssystemverteilung befolgen.

Beachten Sie, dass Sie (der Kunde) beim Anwenden kleinerer Sicherheitsupdates keine Dienste auf dem Console Gent-Host stoppen müssen.

Wenn Sie (der Kunde) die Konsolen-Agent-VM stoppen und dann starten müssen, sollten Sie dies über die

Konsole Ihres Cloud-Anbieters oder mithilfe der Standardverfahren für die lokale Verwaltung tun.

Der Konsolenagent muss jederzeit betriebsbereit sein .

Mehrere Systeme und Agenten

Ein Agent kann mehrere Systeme verwalten und Datendienste in der Konsole unterstützen. Sie können einen einzelnen Agenten verwenden, um mehrere Systeme basierend auf der Bereitstellungsgröße und den von Ihnen verwendeten Datendiensten zu verwalten.

Arbeiten Sie bei groß angelegten Bereitstellungen mit Ihrem NetApp -Vertreter zusammen, um die Größe Ihrer Umgebung festzulegen. Wenden Sie sich bei Problemen an den NetApp -Support.

Hier sind einige Beispiele für Agentenbereitstellungen:

- Sie verfügen über eine Multicloud-Umgebung (z. B. AWS und Azure) und möchten lieber einen Agenten in AWS und einen anderen in Azure haben. Jedes verwaltet die in diesen Umgebungen ausgeführten Cloud Volumes ONTAP -Systeme.
- Ein Dienstanbieter könnte eine Konsolenorganisation nutzen, um seinen Kunden Dienste bereitzustellen, während er eine andere Organisation für die Notfallwiederherstellung einer seiner Geschäftseinheiten nutzt. Jede Organisation benötigt ihren eigenen Agenten.

Bereitstellen eines Konsolenagenten

AWS

Installationsoptionen für Konsolenagenten in AWS

Es gibt verschiedene Möglichkeiten, einen Konsolenagenten in AWS zu erstellen. Der gängigste Weg ist die direkte Nutzung der NetApp Console .

Folgende Installationsoptionen stehen zur Verfügung:

- "Erstellen Sie den Konsolenagenten direkt aus der Konsole"(Dies ist die Standardoption)

  Diese Aktion startet eine EC2-Instance mit Linux und der Konsolenagent-Software in einer VPC Ihrer Wahl.

- "Erstellen Sie einen Konsolenagenten aus dem AWS Marketplace"

  Diese Aktion startet auch eine EC2-Instance, auf der Linux und die Konsolen-Agent-Software ausgeführt werden, die Bereitstellung wird jedoch direkt vom AWS Marketplace und nicht von der Konsole aus initiiert.

- "Laden Sie die Software herunter und installieren Sie sie manuell auf Ihrem eigenen Linux-Host"

Die von Ihnen gewählte Installationsoption wirkt sich darauf aus, wie Sie sich auf die Installation vorbereiten. Dazu gehört, wie Sie der Konsole die erforderlichen Berechtigungen erteilen, die sie zum Authentifizieren und Verwalten von Ressourcen in AWS benötigt.

Erstellen Sie einen Konsolenagenten in AWS über die NetApp Console

Sie können einen Konsolenagenten in AWS direkt von der NetApp Console aus erstellen. Bevor Sie über die Konsole einen Konsolenagenten in AWS erstellen, müssen Sie Ihr

Netzwerk einrichten und AWS-Berechtigungen vorbereiten.

Bevor Sie beginnen

- Sie sollten über eine"Verständnis von Konsolenagenten" .
- Sie sollten überprüfen"Einschränkungen des Konsolenagenten" .

Schritt 1: Einrichten des Netzwerks für die Bereitstellung eines Konsolenagenten in AWS

Stellen Sie sicher, dass der Netzwerkspeicherort, an dem Sie den Konsolenagenten installieren möchten, die folgenden Anforderungen unterstützt. Diese Anforderungen ermöglichen es dem Konsolenagenten, Ressourcen und Prozesse in Ihrer Hybrid Cloud zu verwalten.

VPC und Subnetz

Wenn Sie den Konsolenagenten erstellen, müssen Sie die VPC und das Subnetz angeben, in dem er sich befinden soll.

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.

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.

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.

Von der NetApp Konsole kontaktierte Endpunkte

Wenn Sie die webbasierte NetApp Console verwenden, die über die SaaS-Schicht bereitgestellt wird, kontaktiert diese mehrere Endpunkte, um Datenverwaltungsaufgaben abzuschließen. Dazu gehören Endpunkte, die kontaktiert werden, um den Konsolenagenten von der Konsole aus bereitzustellen.

"Zeigen Sie die Liste der von der NetApp Konsole kontaktierten Endpunkte an" .

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"

Sie müssen diese Netzwerkanforderung implementieren, nachdem Sie den Konsolenagenten erstellt haben.

Schritt 2: AWS-Berechtigungen für den Konsolenagenten einrichten

Die Konsole muss sich bei AWS authentifizieren, bevor sie den Konsolenagenten in Ihrem VPC bereitstellen kann. Sie können eine dieser Authentifizierungsmethoden auswählen:

- Lassen Sie die Konsole eine IAM-Rolle übernehmen, die über die erforderlichen Berechtigungen verfügt
- Geben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel für einen IAM-Benutzer an, der über die erforderlichen Berechtigungen verfügt.

Bei beiden Optionen besteht der erste Schritt darin, eine IAM-Richtlinie zu erstellen. Diese Richtlinie enthält nur die Berechtigungen, die zum Starten des Konsolenagenten in AWS von der Konsole aus erforderlich sind.

Bei Bedarf können Sie die IAM-Richtlinie einschränken, indem Sie die IAM `Condition` Element. "AWS-Dokumentation: Bedingungselement"

Schritte

1. Gehen Sie zur AWS IAM-Konsole.
2. Wählen Sie **Richtlinien > Richtlinie erstellen**.
3. Wählen Sie **JSON**.
4. Kopieren Sie die folgende Richtlinie und fügen Sie sie ein:

   Diese Richtlinie enthält nur die Berechtigungen, die zum Starten des Konsolenagenten in AWS von der Konsole aus erforderlich sind. Wenn die Konsole den Konsolenagenten erstellt, wendet sie einen neuen Satz von Berechtigungen auf den Konsolenagenten an, der es dem Konsolenagenten ermöglicht, AWS-Ressourcen zu verwalten. "Anzeigen der für den Konsolenagenten selbst erforderlichen Berechtigungen".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
```

```
            "ec2:AssociateIamInstanceProfile",
            "ec2:DescribeIamInstanceProfileAssociations",
            "ec2:DisassociateIamInstanceProfile",
            "iam:GetRole",
            "iam:TagRole",
            "kms:ListAliases",
            "cloudformation:ListStacks"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:TerminateInstances"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/OCCMInstance": "*"
            }
        },
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ]
    }
  ]
}
```

5. Wählen Sie **Weiter** und fügen Sie bei Bedarf Tags hinzu.
6. Wählen Sie **Weiter** und geben Sie einen Namen und eine Beschreibung ein.
7. Wählen Sie **Richtlinie erstellen**.
8. Hängen Sie die Richtlinie entweder an eine IAM-Rolle an, die die Konsole übernehmen kann, oder an einen IAM-Benutzer, damit Sie der Konsole Zugriffsschlüssel bereitstellen können:
   - (Option 1) Richten Sie eine IAM-Rolle ein, die die Konsole übernehmen kann:
     i. Gehen Sie zur AWS IAM-Konsole im Zielkonto.
     ii. Wählen Sie unter „Zugriffsverwaltung“ **Rollen > Rolle erstellen** und befolgen Sie die Schritte zum Erstellen der Rolle.
     iii. Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
     iv. Wählen Sie **Ein anderes AWS-Konto** und geben Sie die ID des Console SaaS-Kontos ein: 952013314444
     v. Wählen Sie die Richtlinie aus, die Sie im vorherigen Abschnitt erstellt haben.
     vi. Nachdem Sie die Rolle erstellt haben, kopieren Sie die Rollen-ARN, damit Sie sie beim Erstellen des Konsolen-Agenten in die Konsole einfügen können.
   - (Option 2) Richten Sie Berechtigungen für einen IAM-Benutzer ein, damit Sie der Konsole Zugriffsschlüssel bereitstellen können:

i. Wählen Sie in der AWS IAM-Konsole **Benutzer** und dann den Benutzernamen aus.

ii. Wählen Sie **Berechtigungen hinzufügen > Vorhandene Richtlinien direkt anhängen**.

iii. Wählen Sie die von Ihnen erstellte Richtlinie aus.

iv. Wählen Sie **Weiter** und dann **Berechtigungen hinzufügen**.

v. Stellen Sie sicher, dass Sie den Zugriffsschlüssel und den geheimen Schlüssel für den IAM-Benutzer haben.

Ergebnis

Sie sollten jetzt über eine IAM-Rolle mit den erforderlichen Berechtigungen oder einen IAM-Benutzer mit den erforderlichen Berechtigungen verfügen. Wenn Sie den Konsolenagenten aus der Konsole erstellen, können Sie Informationen zur Rolle oder zu Zugriffsschlüsseln angeben.

Schritt 3: Erstellen des Konsolenagenten

Erstellen Sie den Konsolenagenten direkt von der webbasierten Konsole aus.

Informationen zu diesem Vorgang

- Durch Erstellen des Konsolenagenten aus der Konsole wird eine EC2-Instanz in AWS mithilfe einer Standardkonfiguration bereitgestellt. Wechseln Sie nach dem Erstellen des Konsolenagenten nicht zu einer kleineren EC2-Instance mit weniger CPUs oder weniger RAM. "Erfahren Sie mehr über die Standardkonfiguration für den Konsolenagenten" .
- Wenn die Konsole den Konsolenagenten erstellt, erstellt sie eine IAM-Rolle und ein Profil für den Agenten. Diese Rolle umfasst Berechtigungen, die es dem Konsolenagenten ermöglichen, AWS-Ressourcen zu verwalten. Stellen Sie sicher, dass die Rolle aktualisiert wird, wenn in zukünftigen Versionen neue Berechtigungen hinzugefügt werden. "Erfahren Sie mehr über die IAM-Richtlinie für den Konsolenagenten".

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Eine AWS-Authentifizierungsmethode: entweder eine IAM-Rolle oder Zugriffsschlüssel für einen IAM-Benutzer mit den erforderlichen Berechtigungen.
- Eine VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt.
- Ein Schlüsselpaar für die EC2-Instanz.
- Details zu einem Proxyserver, falls für den Internetzugriff vom Konsolenagenten ein Proxy erforderlich ist.
- Aufstellen"Netzwerkanforderungen" .
- Aufstellen"AWS-Berechtigungen" .

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht Agent bereitstellen > AWS**
3. Befolgen Sie die Schritte im Assistenten, um den Konsolenagenten zu erstellen:
4. Auf der Seite **Einführung** erhalten Sie einen Überblick über den Prozess
5. Geben Sie auf der Seite **AWS-Anmeldeinformationen** Ihre AWS-Region an und wählen Sie dann eine Authentifizierungsmethode aus. Dabei kann es sich entweder um eine IAM-Rolle handeln, die die Konsole übernehmen kann, oder um einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel.

Wenn Sie „Rolle übernehmen“ wählen, können Sie den ersten Satz Anmeldeinformationen über den Bereitstellungsassistenten des Konsolenagenten erstellen. Alle zusätzlichen Anmeldeinformationen müssen auf der Seite „Anmeldeinformationen“ erstellt werden. Sie stehen dann im Assistenten in einer Dropdown-Liste zur Verfügung. "Erfahren Sie, wie Sie zusätzliche Anmeldeinformationen hinzufügen" .

6. Geben Sie auf der Seite **Details** Details zum Konsolenagenten an.
   - Geben Sie einen Namen ein.
   - Fügen Sie benutzerdefinierte Tags (Metadaten) hinzu.
   - Wählen Sie, ob die Konsole eine neue Rolle mit den erforderlichen Berechtigungen erstellen soll oder ob Sie eine vorhandene Rolle auswählen möchten, die Sie mit"die erforderlichen Berechtigungen" .
   - Wählen Sie, ob Sie die EBS-Festplatten des Konsolen-Agenten verschlüsseln möchten. Sie haben die Möglichkeit, den Standardverschlüsselungsschlüssel oder einen benutzerdefinierten Schlüssel zu verwenden.
7. Geben Sie auf der Seite **Netzwerk** eine VPC, ein Subnetz und ein Schlüsselpaar für den Agenten an, wählen Sie, ob eine öffentliche IP-Adresse aktiviert werden soll, und geben Sie optional eine Proxy-Konfiguration an.

   Stellen Sie sicher, dass Sie über das richtige Schlüsselpaar für den Zugriff auf die virtuelle Maschine des Konsolenagenten verfügen. Ohne Schlüsselpaar ist ein Zugriff nicht möglich.
8. Wählen Sie auf der Seite **Sicherheitsgruppe** aus, ob Sie eine neue Sicherheitsgruppe erstellen oder eine vorhandene Sicherheitsgruppe auswählen möchten, die die erforderlichen eingehenden und ausgehenden Regeln zulässt.

   "Sicherheitsgruppenregeln für AWS anzeigen" .
9. Überprüfen Sie Ihre Auswahl, um sicherzustellen, dass Ihre Einrichtung korrekt ist.
   a. Das Kontrollkästchen **Agentenkonfiguration validieren** ist standardmäßig aktiviert, damit die Konsole bei der Bereitstellung die Anforderungen an die Netzwerkkonnektivität validiert. Wenn die Bereitstellung des Agenten durch die Konsole fehlschlägt, wird ein Bericht bereitgestellt, der Sie bei der Fehlerbehebung unterstützt. Wenn die Bereitstellung erfolgreich ist, wird kein Bericht bereitgestellt.

   Wenn Sie immer noch die"vorherige Endpunkte" für Agent-Upgrades verwendet wird, schlägt die Validierung mit einem Fehler fehl. Um dies zu vermeiden, deaktivieren Sie das Kontrollkästchen, um die Validierungsprüfung zu überspringen.
10. Wählen Sie **Hinzufügen**.

    Die Konsole stellt den Agenten in etwa 10 Minuten bereit. Bleiben Sie auf der Seite, bis der Vorgang abgeschlossen ist.

Ergebnis

Nachdem der Vorgang abgeschlossen ist, steht der Konsolenagent für die Verwendung über die Konsole zur Verfügung.

Wenn die Bereitstellung fehlschlägt, können Sie einen Bericht und Protokolle von der Konsole herunterladen, die Ihnen bei der Behebung der Probleme helfen."Erfahren Sie, wie Sie Installationsprobleme beheben."

Wenn Sie Amazon S3-Buckets im selben AWS-Konto haben, in dem Sie den Konsolenagenten erstellt haben, wird auf der Seite **Systeme** automatisch eine Amazon S3-Arbeitsumgebung angezeigt. "Erfahren Sie, wie Sie S3-Buckets über die NetApp Console verwalten"

Erstellen Sie einen Konsolenagenten aus dem AWS Marketplace

Sie erstellen einen Konsolenagenten in AWS direkt vom AWS Marketplace. Um einen Konsolenagenten aus dem AWS Marketplace zu erstellen, müssen Sie Ihr Netzwerk einrichten, AWS-Berechtigungen vorbereiten, die Instanzanforderungen überprüfen und dann den Konsolenagenten erstellen.

Bevor Sie beginnen

- Sie sollten über eine"Verständnis von Konsolenagenten" .
- Sie sollten überprüfen"Einschränkungen des Konsolenagenten" .

Schritt 1: Einrichten des Netzwerks

Stellen Sie sicher, dass der Netzwerkstandort für den Konsolenagenten die folgenden Anforderungen erfüllt, um Hybrid Cloud-Ressourcen zu verwalten.

VPC und Subnetz

Wenn Sie den Konsolenagenten erstellen, müssen Sie die VPC und das Subnetz angeben, in dem er sich befinden soll.

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.

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.
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"

Implementieren Sie diesen Netzwerkzugriff, nachdem Sie den Konsolenagenten erstellt haben.

Schritt 2: AWS-Berechtigungen einrichten

Um eine Marktplatzbereitstellung vorzubereiten, erstellen Sie IAM-Richtlinien in AWS und ordnen Sie sie einer IAM-Rolle zu. Wenn Sie den Konsolenagenten aus dem AWS Marketplace erstellen, werden Sie aufgefordert, diese IAM-Rolle auszuwählen.

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.

      Möglicherweise müssen Sie basierend auf den NetApp -Datendiensten, die Sie verwenden möchten, 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. 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, die Sie während der Bereitstellung vom AWS Marketplace aus mit der EC2-Instance verknüpfen können.

Schritt 3: Überprüfen der Instanzanforderungen

Wenn Sie den Konsolenagenten erstellen, müssen Sie einen EC2-Instance-Typ auswählen, der die folgenden

Anforderungen erfüllt.

CPU
: 8 Kerne oder 8 vCPUs

RAM
: 32 GB

AWS EC2-Instanztyp
: Ein Instanztyp, der die CPU- und RAM-Anforderungen erfüllt. NetApp empfiehlt t3.2xlarge.

Schritt 4: Erstellen des Konsolenagenten

Erstellen Sie den Konsolenagenten direkt vom AWS Marketplace.

Informationen zu diesem Vorgang

Durch Erstellen des Konsolenagenten aus dem AWS Marketplace wird eine EC2-Instanz in AWS mithilfe einer Standardkonfiguration bereitgestellt. "Erfahren Sie mehr über die Standardkonfiguration für den Konsolenagenten" .

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Eine VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt.
- Eine IAM-Rolle mit einer angehängten Richtlinie, die die erforderlichen Berechtigungen für den Konsolenagenten enthält.
- Berechtigungen zum Abonnieren und Abbestellen des AWS Marketplace für Ihren IAM-Benutzer.
- Ein Verständnis der CPU- und RAM-Anforderungen für die Instanz.
- 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**.

  AWS startet den Konsolenagenten mit den angegebenen Einstellungen und der Konsolenagent wird in etwa zehn Minuten ausgeführt.

> ⓘ Wenn die Installation fehlschlägt, können Sie Protokolle und einen Bericht anzeigen, die Ihnen bei der Fehlerbehebung helfen."Erfahren Sie, wie Sie Installationsprobleme beheben."

8. Öffnen Sie einen Webbrowser auf einem Host, der über eine Verbindung zur virtuellen Maschine des Konsolen-Agenten und zur URL des Konsolen-Agenten verfügt.
9. Richten Sie nach der Anmeldung den Konsolenagenten 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.

      Lassen Sie den eingeschränkten Modus deaktiviert, um die Konsole im Standardmodus zu verwenden. Sie sollten den eingeschränkten Modus nur aktivieren, wenn Sie über eine sichere Umgebung verfügen und dieses Konto von den Backend-Diensten der Konsole trennen möchten. Wenn das der Fall ist,"Befolgen Sie die Schritte, um mit der NetApp Console im eingeschränkten Modus zu beginnen" .
   d. Wählen Sie **Los geht's**.

Ergebnis

Der Konsolenagent ist jetzt installiert und mit Ihrer Konsolenorganisation eingerichtet.

Öffnen Sie einen Webbrowser und gehen Sie zu "NetApp Console" um den Konsolenagenten mit der Konsole

zu verwenden.

Wenn Sie Amazon S3-Buckets im selben AWS-Konto haben, in dem Sie den Konsolenagenten erstellt haben, wird auf der Seite **Systeme** automatisch eine Amazon S3-Arbeitsumgebung angezeigt. "Erfahren Sie, wie Sie S3-Buckets über die NetApp Console verwalten"

Manuelle Installation des Konsolenagenten in AWS

Sie können einen Konsolenagenten manuell auf einem Linux-Host installieren, der in AWS ausgeführt wird. Um den Konsolen-Agenten manuell auf Ihrem eigenen Linux-Host zu installieren, müssen Sie die Hostanforderungen überprüfen, Ihr Netzwerk einrichten, AWS-Berechtigungen vorbereiten, den Konsolen-Agenten installieren und dann die vorbereiteten Berechtigungen bereitstellen.

Bevor Sie beginnen

- Sie sollten über eine"Verständnis von Konsolenagenten" .
- Sie sollten überprüfen"Einschränkungen des Konsolenagenten" .

Schritt 1: Hostanforderungen prüfen

Stellen Sie sicher, dass der Host, auf dem die Console-Agent-Software ausgeführt wird, die Anforderungen an Betriebssystem, RAM und Ports erfüllt.

> 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.

AWS EC2-Instanztyp

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

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

Schlüsselpaar

Wenn Sie den Konsolenagenten erstellen, müssen Sie ein EC2-Schlüsselpaar zur Verwendung mit der Instanz auswählen.

PUT-Antwort-Hop-Limit bei Verwendung von IMDSv2

Wenn IMDSv2 aktiviert ist (Standardeinstellung für neue EC2-Instanzen), setzen Sie das Hop-Limit für PUT-Antworten auf 3. Andernfalls wird während der Agenteneinrichtung ein UI-Initialisierungsfehler angezeigt.

- "Erfordert die Verwendung von IMDSv2 auf Amazon EC2-Instanzen"
- "AWS-Dokumentation: Ändern des Hop-Limits für PUT-Antworten"

Schritt 2: 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
```

Schritt 3: Einrichten des Netzwerks

Stellen Sie sicher, dass der Netzwerkstandort die folgenden Anforderungen erfüllt, damit der Console-Agent Ressourcen in Ihrer Hybrid-Cloud verwalten kann.

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.

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.

Endpunkte	Zweck
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.
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"

Schritt 4: AWS-Berechtigungen für die Konsole einrichten

Erteilen Sie der NetApp Console AWS-Berechtigungen mithilfe einer dieser Optionen:

- Option 1: Erstellen Sie IAM-Richtlinien und fügen Sie die Richtlinien einer IAM-Rolle hinzu, die Sie der EC2-Instance zuordnen können.
- Option 2: Stellen Sie der Konsole den AWS-Zugriffsschlüssel für einen IAM-Benutzer zur Verfügung, der über die erforderlichen Berechtigungen verfügt.

Befolgen Sie die Schritte, um Berechtigungen für die Konsole vorzubereiten.

IAM-Rolle

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. 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, die Sie nach der Installation des Konsolenagenten mit der EC2-Instance verknüpfen können.

AWS-Zugriffsschlüssel

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 verfügen jetzt über einen IAM-Benutzer mit den erforderlichen Berechtigungen und einem Zugriffsschlüssel, den Sie der Konsole bereitstellen können.

Schritt 5: Installieren des Konsolenagenten

Nachdem Sie die Voraussetzungen erfüllt haben, installieren Sie die Software manuell auf Ihrem Linux-Host.

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.

2. Warten Sie, bis die Installation abgeschlossen ist.

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

   > Wenn die Installation fehlschlägt, können Sie den Installationsbericht und die Protokolle anzeigen, die Ihnen bei der Behebung der Probleme helfen."Erfahren Sie, wie Sie Installationsprobleme beheben."

1. Öffnen Sie einen Webbrowser auf einem Host, der über eine Verbindung zur virtuellen Maschine des Konsolenagenten verfügt, und geben Sie die folgende URL ein:

   https://ipaddress

2. Richten Sie nach der Anmeldung den Konsolenagenten ein:

   a. Geben Sie die Organisation 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.

      Sie sollten den eingeschränkten Modus deaktiviert lassen, da diese Schritte die Verwendung der Konsole im Standardmodus beschreiben. Sie sollten den eingeschränkten Modus nur aktivieren, wenn Sie über eine sichere Umgebung verfügen und dieses Konto von den Backend-Diensten trennen möchten. Wenn das der Fall ist,"Befolgen Sie die Schritte, um mit der NetApp Console im eingeschränkten Modus zu beginnen" .

   d. Wählen Sie **Los geht’s**.

Wenn Sie Amazon S3-Buckets im selben AWS-Konto haben, in dem Sie den Konsolenagenten erstellt haben, wird auf der Seite **Systeme** automatisch ein Amazon S3-Speichersystem angezeigt. "Erfahren Sie, wie Sie S3-Buckets über die NetApp ConsoleP verwalten"

Schritt 6: Berechtigungen für die NetApp Console erteilen

Nach der Installation des Console-Agenten müssen Sie die von Ihnen eingerichteten AWS-Berechtigungen bereitstellen, damit der Console-Agent Ihre Daten- und Speicherinfrastruktur in AWS verwalten kann.

IAM-Rolle

Ordnen Sie die von Ihnen erstellte IAM-Rolle der Console-Agent-EC2-Instanz zu.

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.

Gehen Sie zum "NetApp Console" um mit der Verwendung des Konsolenagenten zu beginnen.

AWS-Zugriffsschlüssel

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

Schritte

1. Stellen Sie sicher, dass in der Konsole derzeit der richtige Konsolenagent ausgewählt ist.
2. Wählen Sie **Administration > Anmeldeinformationen**.
3. Wählen Sie **Anmeldeinformationen der Organisation** aus.
4. 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**.

Gehen Sie zum "NetApp Console" um mit der Verwendung des Konsolenagenten zu beginnen.

Azurblau

Installationsoptionen für den Konsolen-Agenten in Azure

Es gibt verschiedene Möglichkeiten, einen Konsolen-Agent in Azure zu erstellen. Der

gängigste Weg ist die direkte Nutzung der NetApp Console .

Folgende Installationsoptionen stehen zur Verfügung:

- "Erstellen Sie einen Konsolenagenten direkt aus der NetApp Console"(Dies ist die Standardoption)

  Diese Aktion startet eine VM mit Linux und der Konsolen-Agent-Software in einem VNet Ihrer Wahl.

- "Erstellen eines Konsolen-Agents aus dem Azure Marketplace"

  Diese Aktion startet auch eine VM, auf der Linux und die Konsolen-Agent-Software ausgeführt werden, die Bereitstellung wird jedoch direkt vom Azure Marketplace und nicht von der Konsole aus initiiert.

- "Laden Sie die Software herunter und installieren Sie sie manuell auf Ihrem eigenen Linux-Host"

Die von Ihnen gewählte Installationsoption wirkt sich darauf aus, wie Sie sich auf die Installation vorbereiten. Dazu gehört, wie Sie dem Konsolen-Agenten die erforderlichen Berechtigungen erteilen, die er zum Authentifizieren und Verwalten von Ressourcen in Azure benötigt.

Erstellen Sie einen Konsolen-Agenten in Azure über die NetApp Console

Um einen Konsolenagenten in Azure aus der NetApp Console zu erstellen, müssen Sie Ihr Netzwerk einrichten, Azure-Berechtigungen vorbereiten und dann den Konsolenagenten erstellen.

Bevor Sie beginnen

- Sie sollten über eine"Verständnis von Konsolenagenten" .
- Sie sollten überprüfen"Einschränkungen des Konsolenagenten" .

Schritt 1: Einrichten des Netzwerks

Stellen Sie sicher, dass der Netzwerkspeicherort, an dem Sie den Konsolenagenten installieren möchten, die folgenden Anforderungen unterstützt. Diese Anforderungen ermöglichen dem Konsolenagenten die Verwaltung hybrider Cloud-Ressourcen.

Azure-Region

Wenn Sie Cloud Volumes ONTAP verwenden, sollte der Konsolenagent in derselben Azure-Region wie die von ihm verwalteten Cloud Volumes ONTAP -Systeme oder in der "Azure-Regionenpaar" für die Cloud Volumes ONTAP -Systeme. Diese Anforderung stellt sicher, dass zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten eine Azure Private Link-Verbindung verwendet wird.

"Erfahren Sie, wie Cloud Volumes ONTAP einen Azure Private Link verwendet"

VNet und Subnetz

Wenn Sie den Konsolenagenten erstellen, müssen Sie das VNet und das Subnetz angeben, in dem er sich befinden soll.

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.

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
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.
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.

Von der NetApp Konsole kontaktierte Endpunkte

Wenn Sie die webbasierte NetApp Console verwenden, die über die SaaS-Schicht bereitgestellt wird, kontaktiert diese mehrere Endpunkte, um Datenverwaltungsaufgaben abzuschließen. Dazu gehören Endpunkte, die kontaktiert werden, um den Konsolenagenten von der Konsole aus bereitzustellen.

"Zeigen Sie die Liste der von der NetApp Konsole kontaktierten Endpunkte an" .

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"

Sie müssen diese Netzwerkanforderung implementieren, nachdem Sie den Konsolenagenten erstellt haben.

Schritt 2: Erstellen einer Bereitstellungsrichtlinie für den Konsolen-Agenten (benutzerdefinierte Rolle)

Sie müssen eine benutzerdefinierte Rolle erstellen, die über die Berechtigung zum Bereitstellen des Konsolen-Agenten in Azure verfügt.

Erstellen Sie eine benutzerdefinierte Azure-Rolle, die Sie Ihrem Azure-Konto oder einem Microsoft Entra-Dienstprinzipal zuweisen können. Die Konsole authentifiziert sich bei Azure und verwendet diese Berechtigungen, um den Konsolen-Agenten in Ihrem Namen zu erstellen.

Die Konsole stellt die Konsolen-Agent-VM in Azure bereit und ermöglicht eine "systemseitig zugewiesene verwaltete Identität" , erstellt die erforderliche Rolle und weist sie der VM zu. "Überprüfen Sie, wie die Konsole die Berechtigungen verwendet" .

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. Kopieren Sie die erforderlichen Berechtigungen für eine neue benutzerdefinierte Rolle in Azure und speichern Sie sie in einer JSON-Datei.

   Diese benutzerdefinierte Rolle enthält nur die Berechtigungen, die zum Starten der Konsolen-Agent-VM in Azure von der Konsole aus erforderlich sind. Verwenden Sie diese Richtlinie nicht für andere Situationen. Wenn die Konsole den Konsolen-Agenten erstellt, wendet sie einen neuen Satz von Berechtigungen auf die Konsolen-Agenten-VM an, der es dem Konsolen-Agenten ermöglicht, Azure-Ressourcen zu verwalten.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
```

```
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
  ],
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Azure SetupAsService",
  "IsCustom": "true"
}
```

2. Ändern Sie das JSON, indem Sie Ihre Azure-Abonnement-ID zum zuweisbaren Bereich hinzufügen.

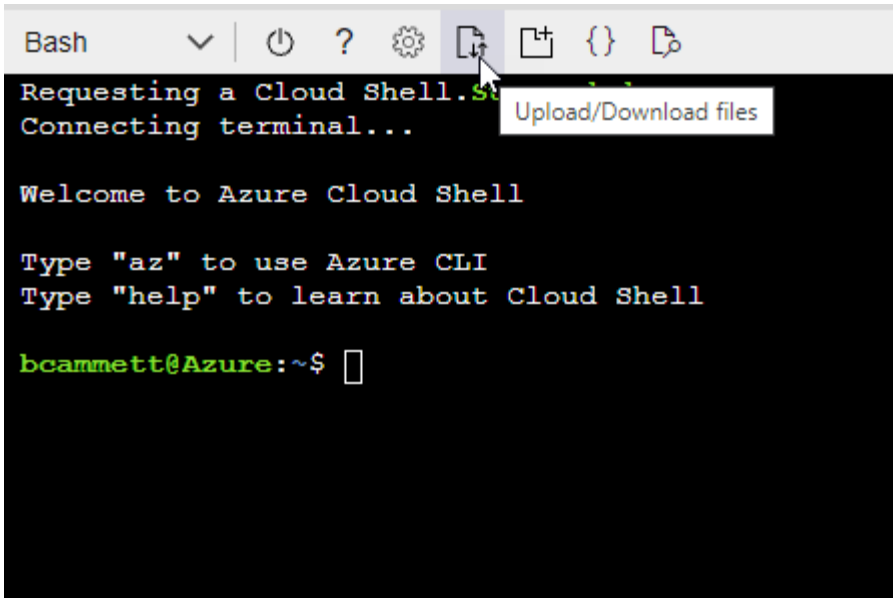
   Beispiel

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
]
```

3. 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. Geben Sie den folgenden Azure CLI-Befehl ein:

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

Sie verfügen jetzt über eine benutzerdefinierte Rolle namens *Azure SetupAsService*. Sie können diese benutzerdefinierte Rolle auf Ihr Benutzerkonto oder einen Dienstprinzipal anwenden.

Schritt 3: Authentifizierung einrichten

Wenn Sie den Konsolen-Agenten von der Konsole aus erstellen, müssen Sie eine Anmeldung angeben, die es der Konsole ermöglicht, sich bei Azure zu authentifizieren und die VM bereitzustellen. Sie haben zwei Möglichkeiten:

1. Sign in, wenn Sie dazu aufgefordert werden. Dieses Konto muss über bestimmte Azure-Berechtigungen verfügen. Dies ist die Standardoption.
2. Geben Sie Details zu einem Microsoft Entra-Dienstprinzipal an. Dieser Dienstprinzipal erfordert auch bestimmte Berechtigungen.

Befolgen Sie die Schritte, um eine dieser Authentifizierungsmethoden für die Verwendung mit der Konsole vorzubereiten.

Azure-Konto

Weisen Sie die benutzerdefinierte Rolle dem Benutzer zu, der den Konsolenagenten von der Konsole aus bereitstellt.

Schritte

1. Öffnen Sie im Azure-Portal den Dienst **Abonnements** und wählen Sie das Abonnement des Benutzers aus.
2. Klicken Sie auf **Zugriffskontrolle (IAM)**.
3. Klicken Sie auf **Hinzufügen** > **Rollenzuweisung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
   a. Wählen Sie die Rolle **Azure SetupAsService** aus und klicken Sie auf **Weiter**.

   „Azure SetupAsService“ ist der Standardname, der in der Bereitstellungsrichtlinie des Konsolen-Agenten für Azure angegeben ist. Wenn Sie einen anderen Namen für die Rolle gewählt haben, wählen Sie stattdessen diesen Namen aus.

   b. Behalten Sie die Auswahl von **Benutzer, Gruppe oder Dienstprinzipal** bei.
   c. Klicken Sie auf **Mitglieder auswählen**, wählen Sie Ihr Benutzerkonto aus und klicken Sie auf **Auswählen**.
   d. Klicken Sie auf **Weiter**.
   e. Klicken Sie auf **Überprüfen + zuweisen**.

Dienstprinzipal

Anstatt sich mit Ihrem Azure-Konto anzumelden, können Sie der Konsole die Anmeldeinformationen für einen Azure-Dienstprinzipal bereitstellen, der über die erforderlichen Berechtigungen verfügt.

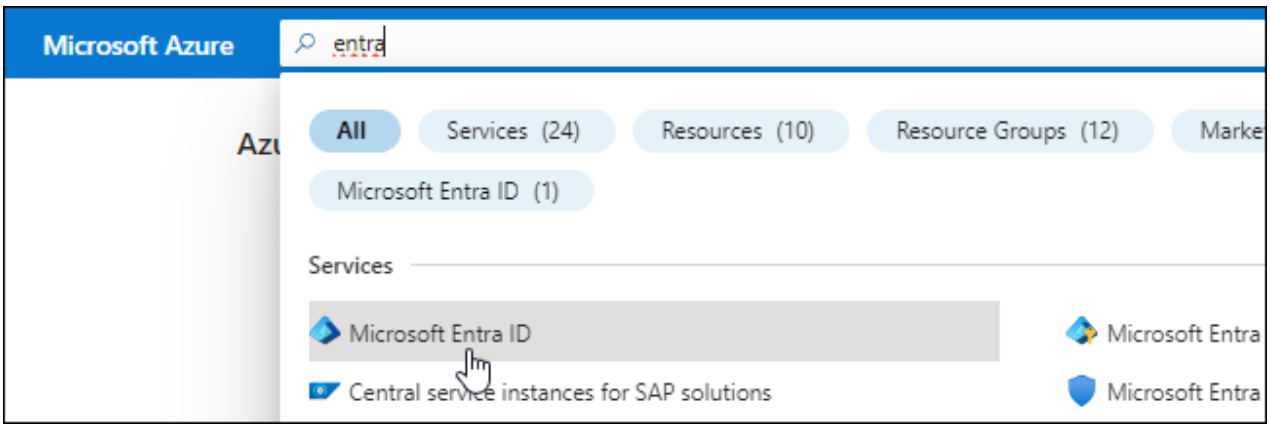
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die die Konsole benötigt.

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**.



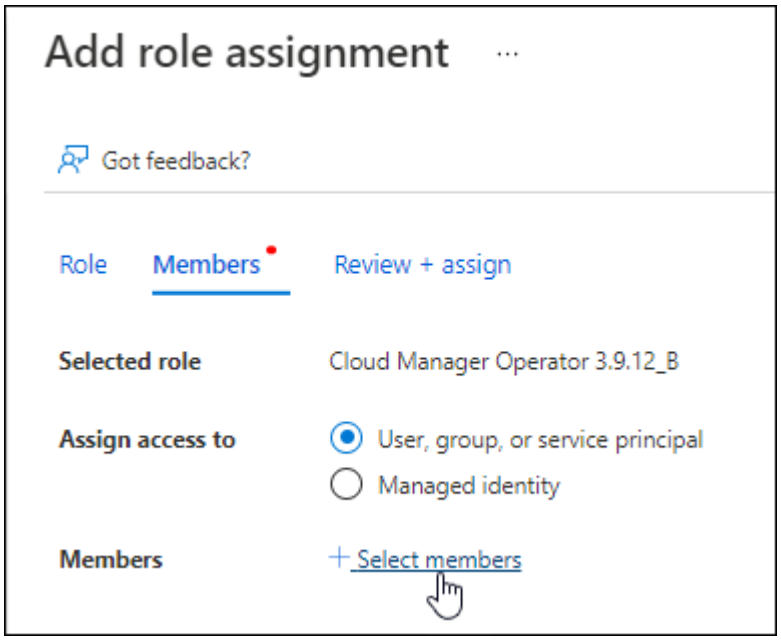
3. Wählen Sie im Menü **App-Registrierungen** aus.
4. Wählen Sie **Neuregistrierung**.
5. Geben Sie Details zur Anwendung an:
   - **Name**: Geben Sie einen Namen für die Anwendung ein.
   - **Kontotyp**: Wählen Sie einen Kontotyp aus (alle funktionieren mit der NetApp Console).
   - **Umleitungs-URI**: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

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der benutzerdefinierten Rolle zur Anwendung

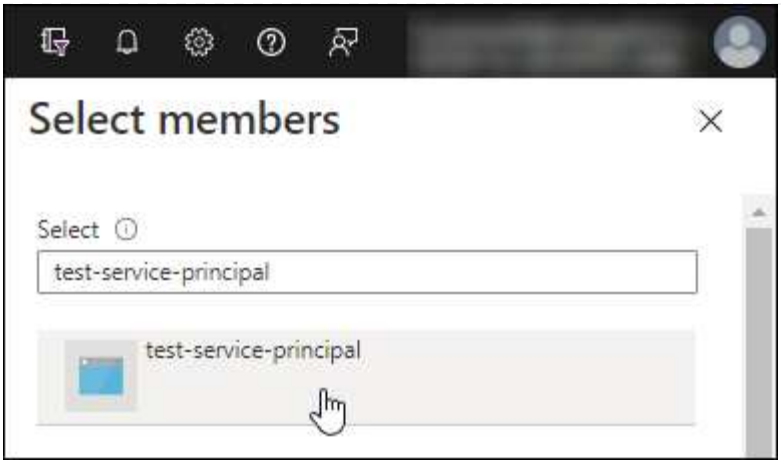
1. Öffnen Sie im Azure-Portal den Dienst **Abonnements**.
2. Wählen Sie das Abonnement aus.
3. Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
4. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenoperator** aus und klicken Sie auf **Weiter**.
5. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

   a. Behalten Sie die Auswahl von **Benutzer, Gruppe oder Dienstprinzipal** bei.
   b. Klicken Sie auf **Mitglieder auswählen**.



   c. Suchen Sie nach dem Namen der Anwendung.

      Hier ist ein Beispiel:



a. Wählen Sie die Anwendung aus und klicken Sie auf **Auswählen**.

b. Klicken Sie auf **Weiter**.

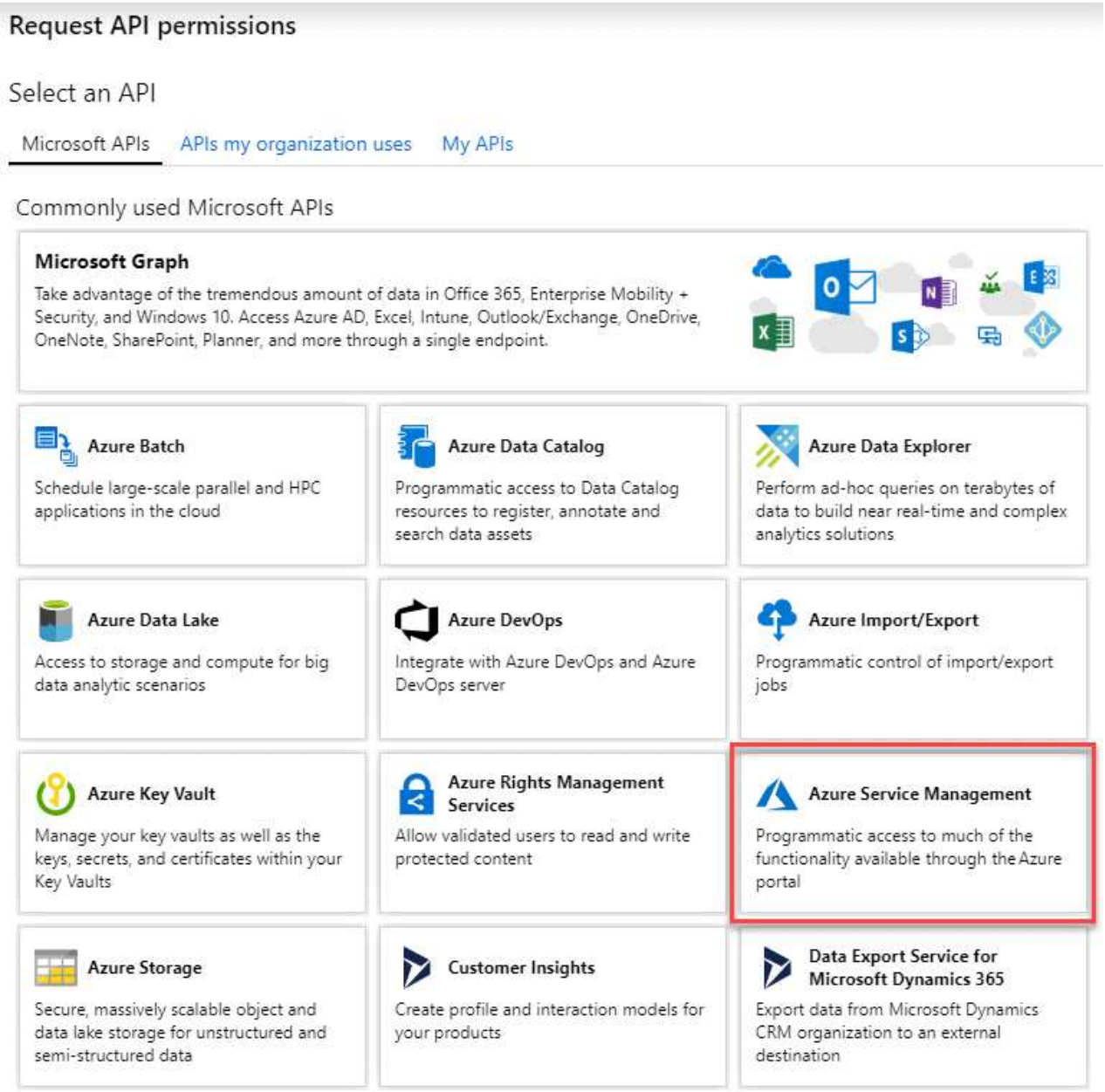
6. Klicken Sie auf **Überprüfen + zuweisen**.

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

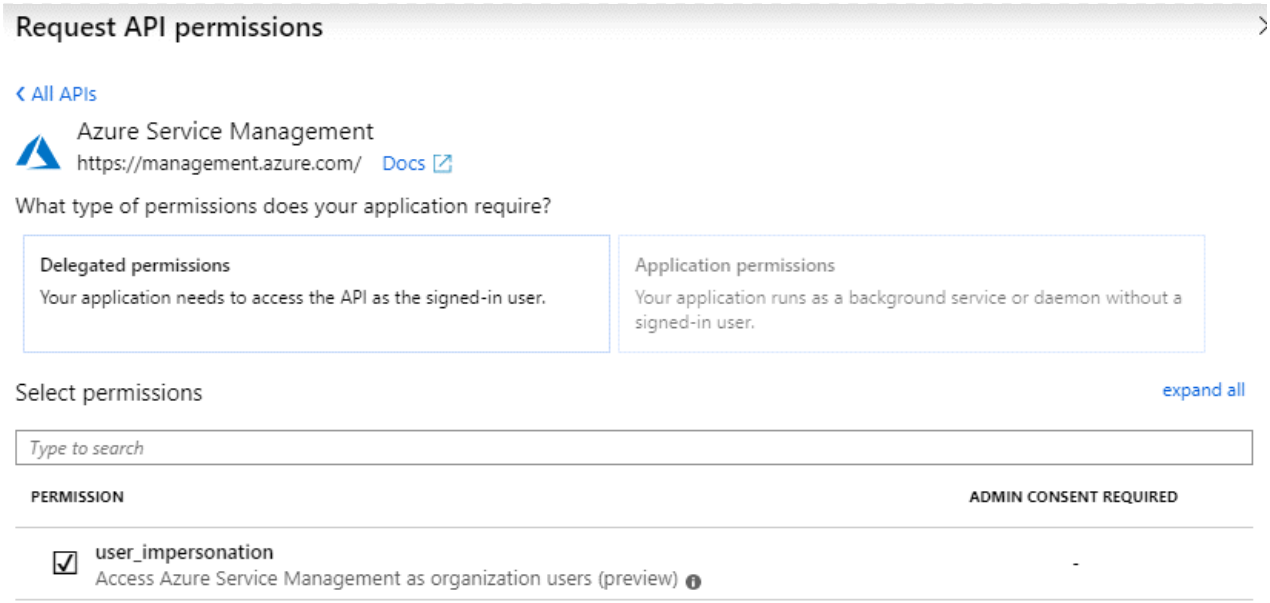
   Wenn Sie Ressourcen in mehreren Azure-Abonnements verwalten möchten, müssen Sie den Dienstprinzipal an jedes dieser Abonnements binden. Beispielsweise können Sie in der Konsole das Abonnement auswählen, das Sie bei der Bereitstellung von Cloud Volumes ONTAP verwenden möchten.

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.

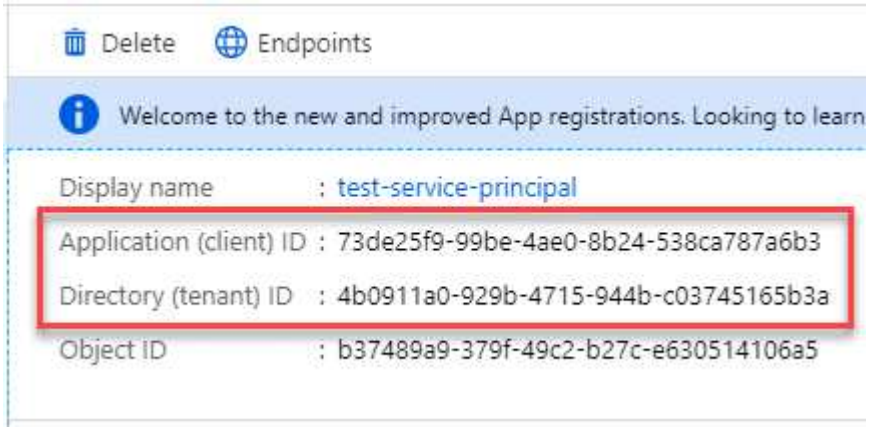


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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 (Mandanten-ID) und den Wert des Client-Geheimnisses kopiert haben. Sie müssen diese Informationen in die Konsole eingeben, wenn Sie den Konsolenagenten erstellen.

Schritt 4: Erstellen des Konsolenagenten

Erstellen Sie den Konsolenagenten direkt von der NetApp Console aus.

Informationen zu diesem Vorgang

- Durch das Erstellen des Konsolenagenten aus der Konsole wird eine virtuelle Maschine in Azure mit einer Standardkonfiguration bereitgestellt. Wechseln Sie nach dem Erstellen des Konsolenagenten nicht zu einer kleineren VM-Instanz mit weniger CPUs oder weniger RAM. "Erfahren Sie mehr über die Standardkonfiguration für den Konsolenagenten" .
- Wenn die Konsole den Konsolenagenten bereitstellt, erstellt sie eine benutzerdefinierte Rolle und weist sie der Konsolenagent-VM zu. Diese Rolle umfasst Berechtigungen, die es dem Konsolenagenten ermöglichen, Azure-Ressourcen zu verwalten. Sie müssen sicherstellen, dass die Rolle auf dem neuesten Stand gehalten wird, da in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. "Erfahren Sie mehr über die benutzerdefinierte Rolle für den Konsolenagenten" .

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Ein Azure-Abonnement.
- Ein VNet und Subnetz in der Azure-Region Ihrer Wahl.
- Details zu einem Proxyserver, wenn Ihre Organisation einen Proxy für den gesamten ausgehenden Internetverkehr benötigt:
  - IP-Adresse
  - Anmeldeinformationen
  - HTTPS-Zertifikat
- Ein öffentlicher SSH-Schlüssel, wenn Sie diese Authentifizierungsmethode für die virtuelle Maschine des Konsolenagenten verwenden möchten. Die andere Möglichkeit der Authentifizierungsmethode ist die Verwendung eines Kennworts.

  "Erfahren Sie mehr über die Verbindung mit einer Linux-VM in Azure."

- Wenn Sie nicht möchten, dass die Konsole automatisch eine Azure-Rolle für den Konsolen-Agenten erstellt, müssen Sie Ihre eigene erstellen."unter Verwendung der Richtlinien auf dieser Seite" .

  Diese Berechtigungen gelten für den Konsolenagenten selbst. Es handelt sich um einen anderen Satz von

Berechtigungen als den, den Sie zuvor zum Bereitstellen der Konsolen-Agent-VM eingerichtet haben.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** die Option **Agent bereitstellen > Azure** aus.
3. Überprüfen Sie auf der Seite **Überprüfen** die Anforderungen für die Bereitstellung eines Agenten. Diese Anforderungen werden oben auf dieser Seite ebenfalls ausführlich beschrieben.
4. Wählen Sie auf der Seite **Virtual Machine Authentication** die Authentifizierungsoption aus, die Ihrer Einrichtung der Azure-Berechtigungen entspricht:

   - Wählen Sie **Anmelden**, um sich bei Ihrem Microsoft-Konto anzumelden, das über die erforderlichen Berechtigungen verfügen sollte.

     Das Formular ist Eigentum von Microsoft und wird von Microsoft gehostet. Ihre Anmeldeinformationen werden NetApp nicht zur Verfügung gestellt.

     Wenn Sie bereits bei einem Azure-Konto angemeldet sind, verwendet die Konsole automatisch dieses Konto. Wenn Sie mehrere Konten haben, müssen Sie sich möglicherweise zuerst abmelden, um sicherzustellen, dass Sie das richtige Konto verwenden.

   - Wählen Sie **Active Directory-Dienstprinzipal** aus, um Informationen zum Microsoft Entra-Dienstprinzipal einzugeben, der die erforderlichen Berechtigungen erteilt:
     - Anwendungs-ID (Client-ID)
     - Verzeichnis-ID (Mandant)
     - Client-Geheimnis

   Erfahren Sie, wie Sie diese Werte für einen Dienstprinzipal erhalten .

5. Wählen Sie auf der Seite **Virtual Machine Authentication** ein Azure-Abonnement, einen Standort, eine neue Ressourcengruppe oder eine vorhandene Ressourcengruppe aus und wählen Sie dann eine Authentifizierungsmethode für die virtuelle Maschine des Konsolen-Agenten aus, die Sie erstellen.

   Die Authentifizierungsmethode für die virtuelle Maschine kann ein Kennwort oder ein öffentlicher SSH-Schlüssel sein.

   "Erfahren Sie mehr über die Verbindung mit einer Linux-VM in Azure."

6. Geben Sie auf der Seite **Details** einen Namen für den Agenten ein, geben Sie Tags an und wählen Sie, ob die Konsole eine neue Rolle mit den erforderlichen Berechtigungen erstellen soll oder ob Sie eine vorhandene Rolle auswählen möchten, die Sie mit"die erforderlichen Berechtigungen" .

   Beachten Sie, dass Sie die mit dieser Rolle verknüpften Azure-Abonnements auswählen können. Jedes von Ihnen ausgewählte Abonnement erteilt dem Konsolenagenten die Berechtigung, Ressourcen in diesem Abonnement zu verwalten (z. B. Cloud Volumes ONTAP).

7. Wählen Sie auf der Seite **Netzwerk** ein VNet und ein Subnetz aus, geben Sie an, ob eine öffentliche IP-Adresse aktiviert werden soll, und geben Sie optional eine Proxy-Konfiguration an.
   - Wählen Sie auf der Seite **Sicherheitsgruppe** aus, ob Sie eine neue Sicherheitsgruppe erstellen oder eine vorhandene Sicherheitsgruppe auswählen möchten, die die erforderlichen eingehenden und ausgehenden Regeln zulässt.

"Anzeigen von Sicherheitsgruppenregeln für Azure" .

8. Überprüfen Sie Ihre Auswahl, um sicherzustellen, dass Ihre Einrichtung korrekt ist.

   a. Das Kontrollkästchen **Agentenkonfiguration validieren** ist standardmäßig aktiviert, damit die Konsole bei der Bereitstellung die Anforderungen an die Netzwerkkonnektivität validiert. Wenn die Bereitstellung des Agenten durch die Konsole fehlschlägt, wird ein Bericht bereitgestellt, der Sie bei der Fehlerbehebung unterstützt. Wenn die Bereitstellung erfolgreich ist, wird kein Bericht bereitgestellt.

   Wenn Sie immer noch die"vorherige Endpunkte" für Agent-Upgrades verwendet wird, schlägt die Validierung mit einem Fehler fehl. Um dies zu vermeiden, deaktivieren Sie das Kontrollkästchen, um die Validierungsprüfung zu überspringen.

9. Wählen Sie **Hinzufügen**.

   Die Konsole bereitet den Agenten in etwa 10 Minuten vor. Bleiben Sie auf der Seite, bis der Vorgang abgeschlossen ist.

Ergebnis

Nachdem der Vorgang abgeschlossen ist, steht der Konsolenagent für die Verwendung über die Konsole zur Verfügung.

Wenn die Bereitstellung fehlschlägt, können Sie einen Bericht und Protokolle von der Konsole herunterladen, die Ihnen bei der Behebung der Probleme helfen."Erfahren Sie, wie Sie Installationsprobleme beheben."

Wenn Sie Azure Blob Storage im selben Azure-Konto haben, in dem Sie den Konsolen-Agent erstellt haben, wird Azure Blob Storage automatisch auf der Seite **Systeme** angezeigt. "Erfahren Sie, wie Sie Azure Blob Storage über die NetApp Console verwalten"

Erstellen eines Konsolen-Agents aus dem Azure Marketplace

Sie können einen Konsolen-Agent in Azure direkt vom Azure Marketplace aus erstellen. Um einen Konsolen-Agenten aus dem Azure Marketplace zu erstellen, müssen Sie Ihr Netzwerk einrichten, Azure-Berechtigungen vorbereiten, die Instanzanforderungen überprüfen und dann den Konsolen-Agenten erstellen.

Bevor Sie beginnen

- Sie sollten über eine"Verständnis von Konsolenagenten" .
- Rezension"Einschränkungen des Konsolenagenten" .

Schritt 1: Einrichten des Netzwerks

Stellen Sie sicher, dass der Netzwerkstandort, an dem Sie den Konsolen-Agenten installieren möchten, die folgenden Anforderungen unterstützt. Diese Anforderungen ermöglichen dem Konsolen-Agenten die Verwaltung von Ressourcen in Ihrer Hybrid Cloud.

Azure-Region

Wenn Sie Cloud Volumes ONTAP verwenden, sollte der Konsolenagent in derselben Azure-Region wie die von ihm verwalteten Cloud Volumes ONTAP -Systeme oder in der "Azure-Regionenpaar" für die Cloud Volumes ONTAP -Systeme. Diese Anforderung stellt sicher, dass zwischen Cloud Volumes ONTAP und

den zugehörigen Speicherkonten eine Azure Private Link-Verbindung verwendet wird.

"Erfahren Sie, wie Cloud Volumes ONTAP einen Azure Private Link verwendet"

VNet und Subnetz

Wenn Sie den Konsolenagenten erstellen, müssen Sie das VNet und das Subnetz angeben, in dem er sich befinden soll.

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.

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
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.
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.

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"

Implementieren Sie die Netzwerkanforderungen, nachdem Sie den Konsolenagenten erstellt haben.

Schritt 2: Überprüfen der VM-Anforderungen

Wählen Sie beim Erstellen des Konsolenagenten einen virtuellen Maschinentyp aus, der die folgenden Anforderungen erfüllt.

CPU

8 Kerne oder 8 vCPUs

RAM

32 GB

Azure-VM-Größe

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

Schritt 3: Berechtigungen einrichten

Sie können Berechtigungen auf folgende Weise erteilen:

- Option 1: Weisen Sie der Azure-VM mithilfe einer systemseitig zugewiesenen verwalteten Identität eine benutzerdefinierte Rolle zu.
- Option 2: Geben Sie der Konsole die Anmeldeinformationen für einen Azure-Dienstprinzipal mit den erforderlichen Berechtigungen.

Befolgen Sie diese Schritte, um Berechtigungen für die Konsole einzurichten.

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"

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.

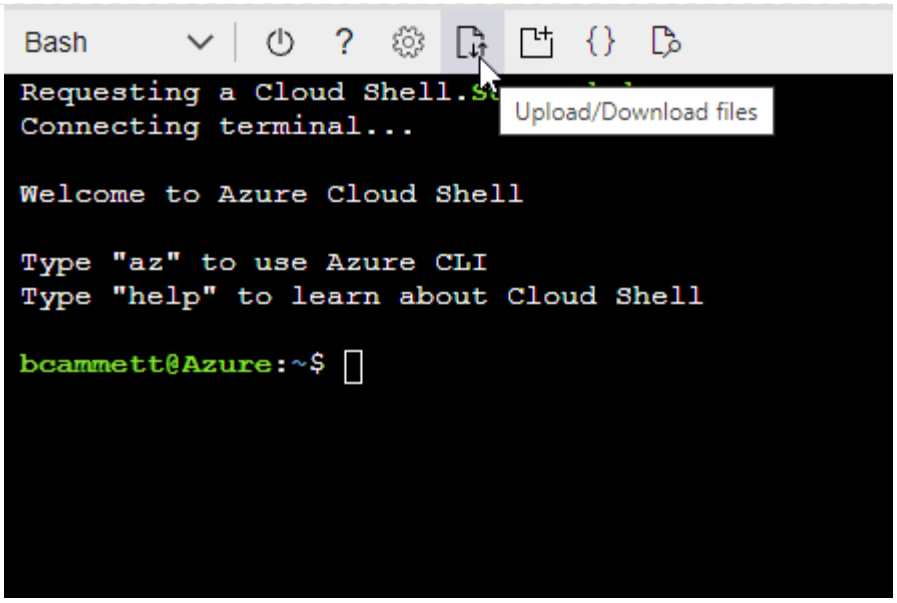
   Beispiel

   ```
   "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
```

Dienstprinzipal

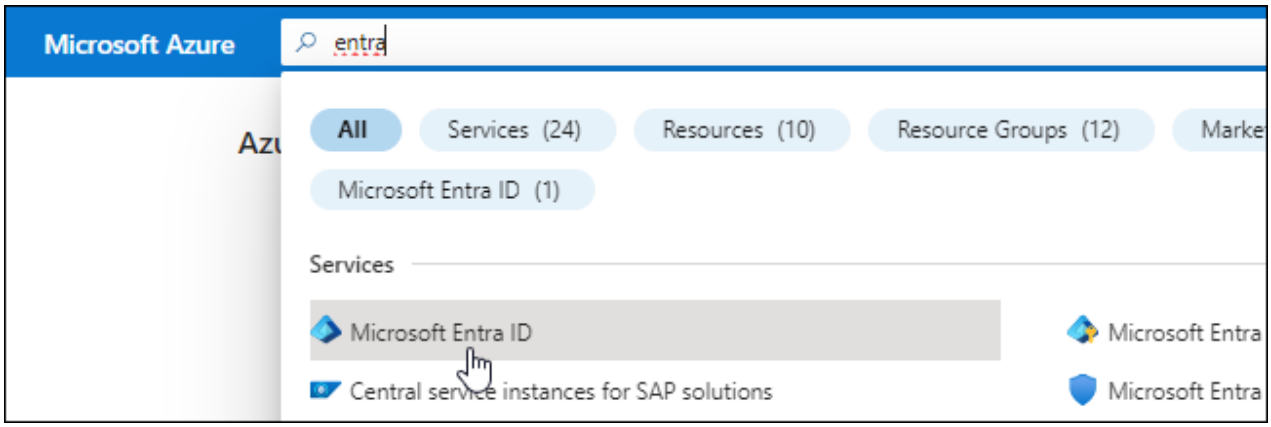
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die die Konsole benötigt.

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.

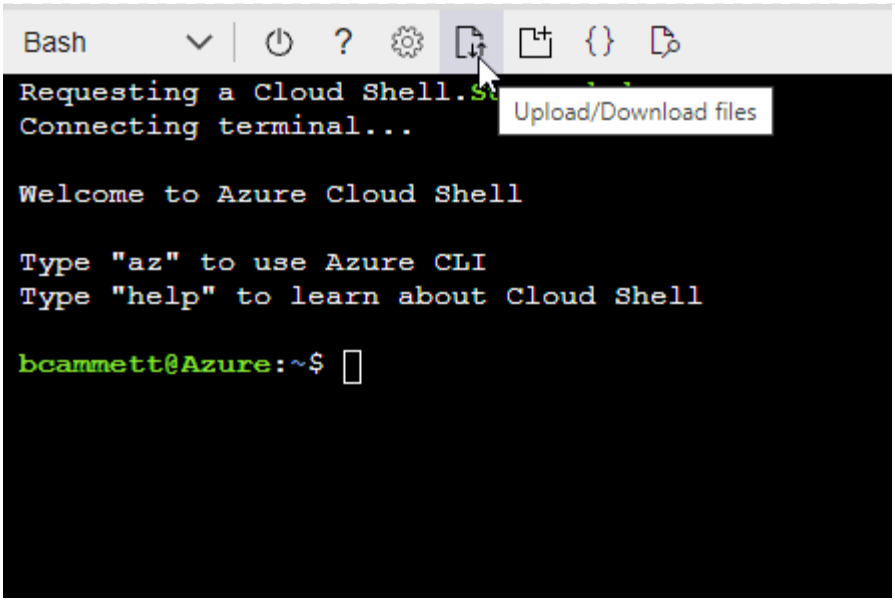
      Beispiel

      ```
      "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**.

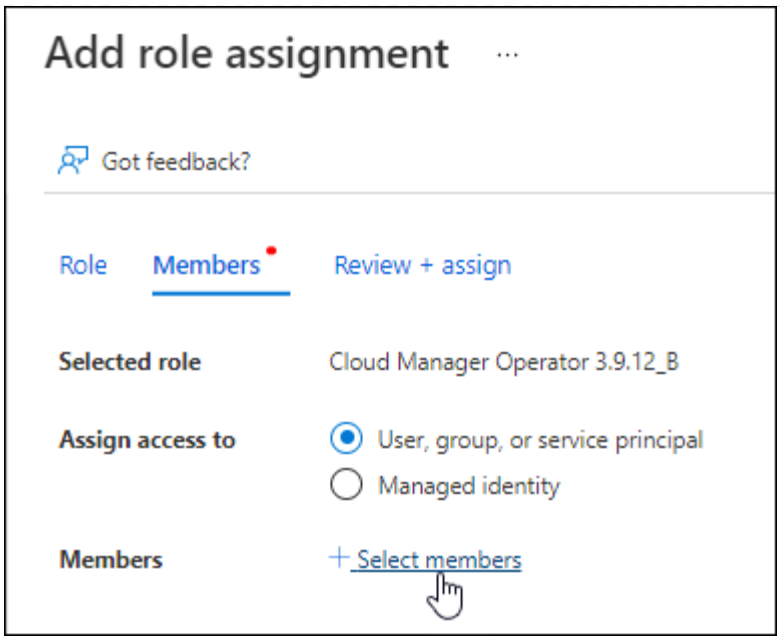
   b. Wählen Sie das Abonnement aus.

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

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

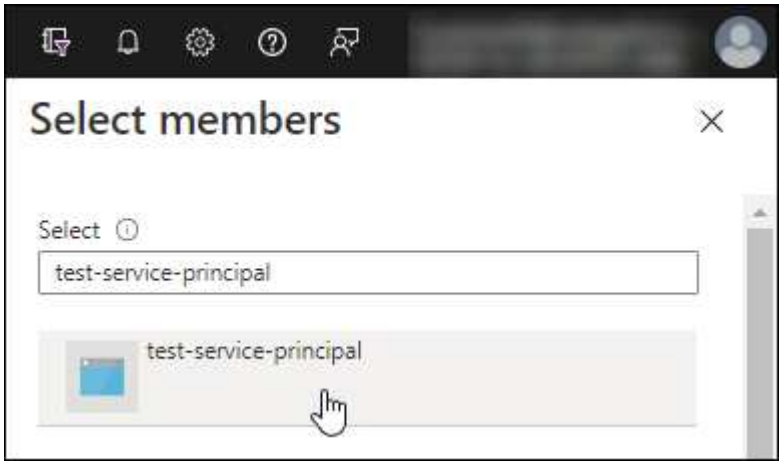
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - 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**.

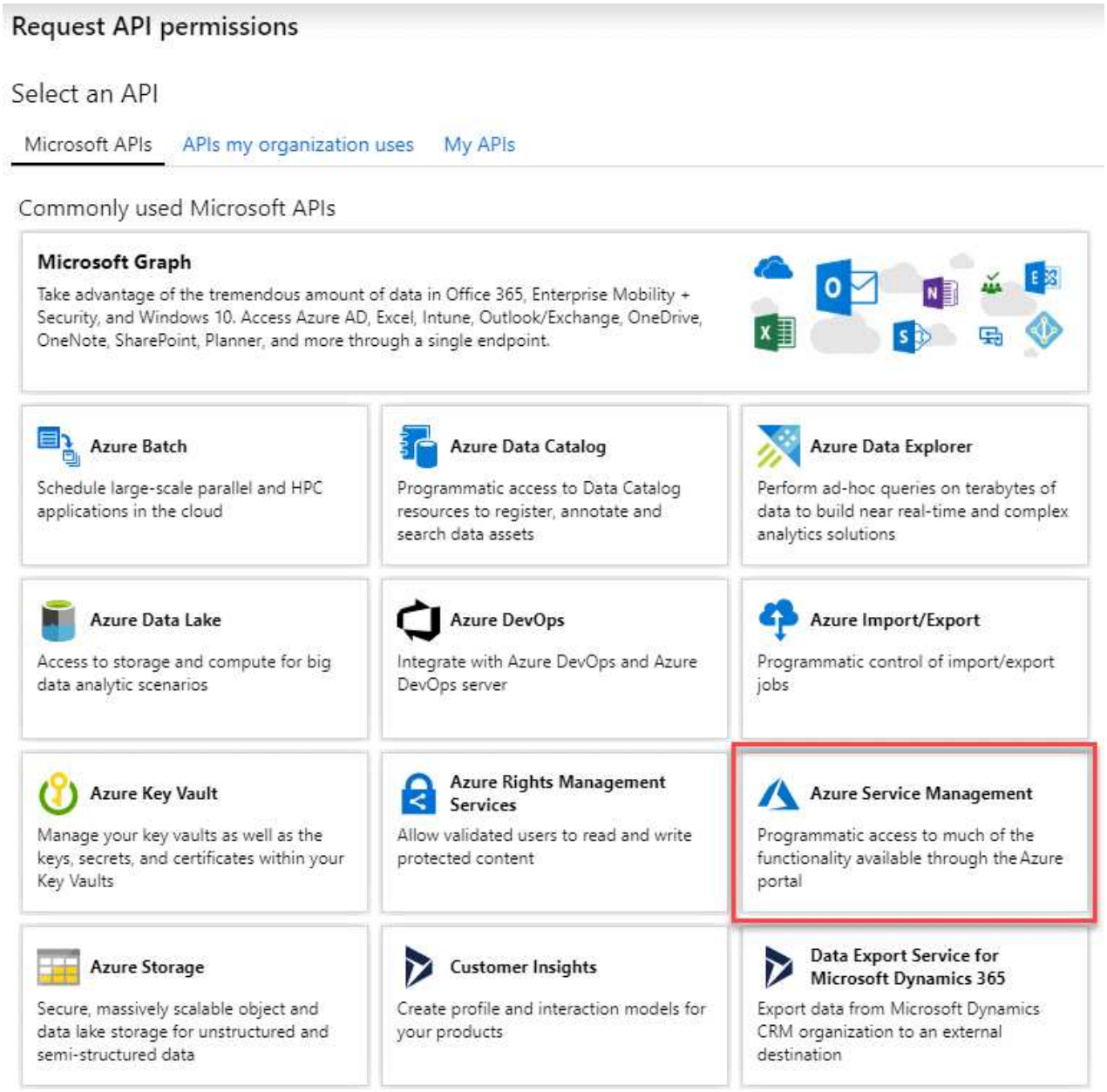
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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.

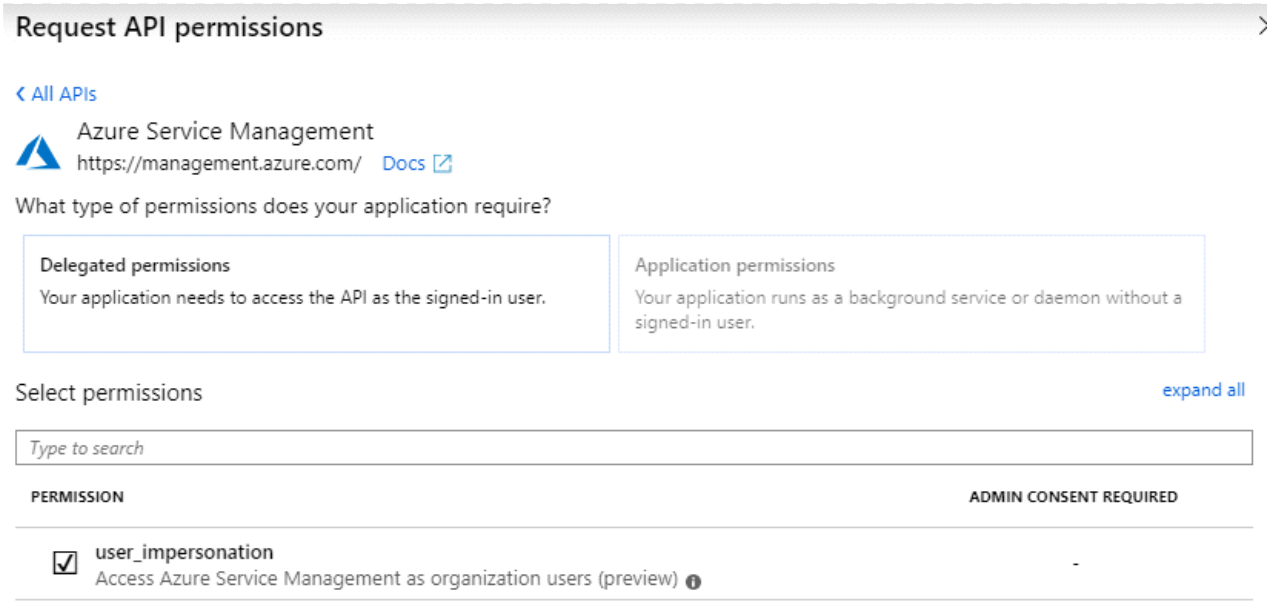
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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.

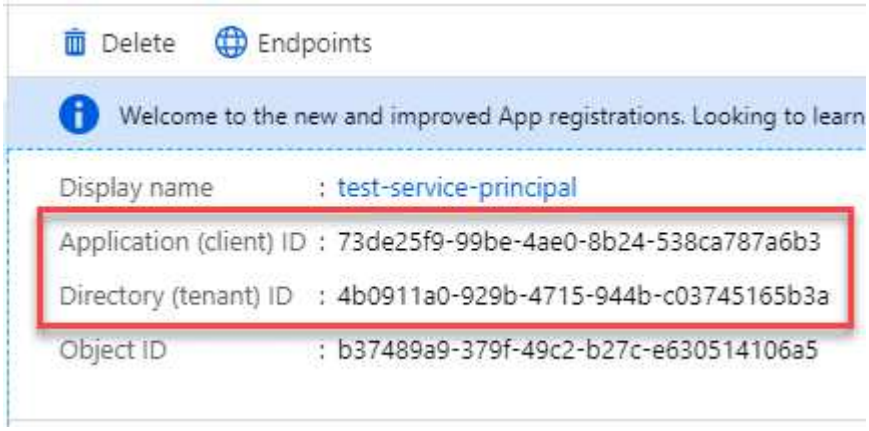


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

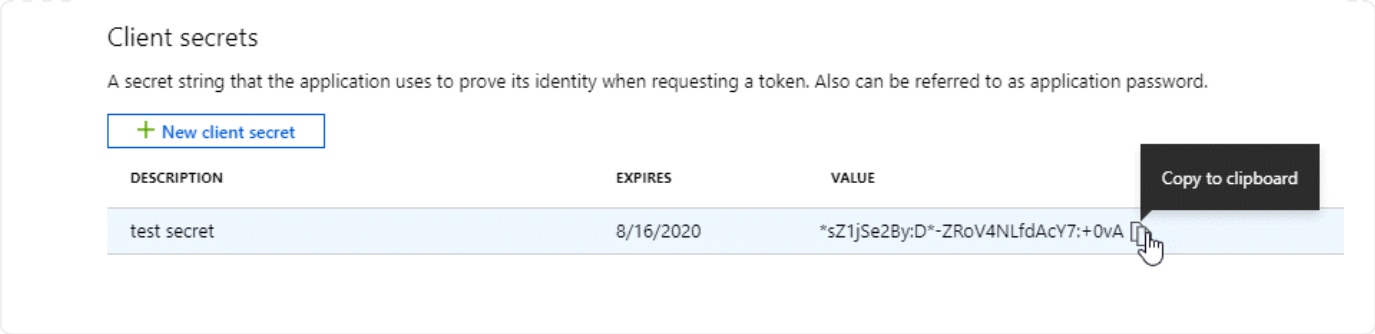
1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



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.



Schritt 4: Erstellen des Konsolenagenten

Starten Sie den Konsolen-Agent direkt vom Azure Marketplace.

Informationen zu diesem Vorgang

Durch Erstellen des Konsolen-Agenten aus dem Azure Marketplace wird eine virtuelle Maschine mit einer Standardkonfiguration eingerichtet. "Erfahren Sie mehr über die Standardkonfiguration für den Konsolenagenten" .

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Ein Azure-Abonnement.
- Ein VNet und Subnetz in der Azure-Region Ihrer Wahl.
- Details zu einem Proxyserver, wenn Ihre Organisation einen Proxy für den gesamten ausgehenden Internetverkehr benötigt:
  - IP-Adresse
  - Anmeldeinformationen
  - HTTPS-Zertifikat
- Ein öffentlicher SSH-Schlüssel, wenn Sie diese Authentifizierungsmethode für die virtuelle Maschine des Konsolenagenten verwenden möchten. Die andere Möglichkeit der Authentifizierungsmethode ist die Verwendung eines Kennworts.

  "Erfahren Sie mehr über die Verbindung mit einer Linux-VM in Azure."

- Wenn Sie nicht möchten, dass die Konsole automatisch eine Azure-Rolle für den Konsolen-Agenten erstellt, müssen Sie Ihre eigene erstellen."unter Verwendung der Richtlinien auf dieser Seite" .

  Diese Berechtigungen gelten für die Konsolen-Agentinstanz selbst. Es handelt sich um einen anderen Satz von Berechtigungen als den, den Sie zuvor zum Bereitstellen der Konsolen-Agent-VM eingerichtet haben.

Schritte

1. Gehen Sie zur VM-Seite des NetApp Console Agents im Azure Marketplace.

   "Azure Marketplace-Seite für kommerzielle 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.
- **Netzwerksicherheitsgruppe**: Der Konsolenagent erfordert eingehende Verbindungen über SSH, HTTP und HTTPS.

  "Anzeigen von Sicherheitsgruppenregeln für Azure" .

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

  Diese Einstellung ist wichtig, da eine verwaltete Identität es der virtuellen Maschine des Konsolenagenten ermöglicht, sich gegenüber der Microsoft Entra ID zu identifizieren, ohne Anmeldeinformationen angeben zu müssen. "Erfahren Sie mehr über verwaltete Identitäten für Azure-Ressourcen" .

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

   Azure stellt die virtuelle Maschine mit den angegebenen Einstellungen bereit. Sie sollten sehen, dass die virtuelle Maschine und die Konsolenagent-Software in etwa zehn Minuten ausgeführt werden.

   Wenn die Installation fehlschlägt, können Sie Protokolle und einen Bericht anzeigen, die Ihnen bei der Fehlerbehebung helfen."Erfahren Sie, wie Sie Installationsprobleme beheben."

5. Öffnen Sie einen Webbrowser auf einem Host, der über eine Verbindung zur virtuellen Maschine des Konsolenagenten verfügt, und geben Sie die folgende URL ein:

   https://ipaddress

6. Richten Sie nach der Anmeldung den Konsolenagenten 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.

      Lassen Sie den eingeschränkten Modus deaktiviert, um die Konsole im Standardmodus zu verwenden. Sie sollten den eingeschränkten Modus nur aktivieren, wenn Sie über eine sichere Umgebung verfügen und dieses Konto von den Backend-Diensten der Konsole trennen möchten. Wenn das der Fall ist,"Befolgen Sie die Schritte, um mit der Konsole im eingeschränkten Modus zu beginnen" .

   d. Wählen Sie **Los geht's**.

Ergebnis

Sie haben jetzt den Konsolenagenten installiert und ihn mit Ihrer Konsolenorganisation eingerichtet.

Wenn Sie Azure Blob Storage im selben Azure-Abonnement haben, in dem Sie den Konsolen-Agent erstellt haben, wird auf der Seite **Systeme** automatisch ein Azure Blob Storage-System angezeigt. "Erfahren Sie, wie Sie Azure Blob Storage über die Konsole verwalten"

Schritt 5: Erteilen Sie dem Konsolenagenten Berechtigungen

Nachdem Sie den Konsolenagenten erstellt haben, müssen Sie ihm die zuvor eingerichteten Berechtigungen erteilen. Durch die Bereitstellung der Berechtigungen kann der Konsolenagent Ihre Daten und Speicherinfrastruktur in Azure verwalten.

Benutzerdefinierte 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.

Wie geht es weiter?

Gehen Sie zum "NetApp Console" um mit der Verwendung des Konsolenagenten zu beginnen.

Dienstprinzipal

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 Konsole verfügt jetzt über die erforderlichen Berechtigungen, um in Ihrem Namen Aktionen in Azure auszuführen.

Manuelles Installieren des Konsolen-Agents in Azure

Um den Konsolen-Agent manuell auf Ihrem eigenen Linux-Host zu installieren, müssen Sie die Hostanforderungen überprüfen, Ihr Netzwerk einrichten, Azure-Berechtigungen vorbereiten, den Konsolen-Agent installieren und dann die vorbereiteten Berechtigungen bereitstellen.

Bevor Sie beginnen

- Sie sollten über eine"Verständnis von Konsolenagenten" .
- Sie sollten überprüfen"Einschränkungen des Konsolenagenten" .

Schritt 1: Hostanforderungen prüfen

Die Konsolenagent-Software muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Portanforderungen usw. erfüllt.

> 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.

Azure-VM-Größe

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

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 2: 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 2. 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 3: Einrichten des Netzwerks

Stellen Sie sicher, dass der Netzwerkspeicherort, an dem Sie den Konsolenagenten installieren möchten, die folgenden Anforderungen unterstützt. Wenn diese Anforderungen erfüllt sind, kann der Konsolenagent Ressourcen und Prozesse in Ihrer Hybrid-Cloud-Umgebung verwalten.

Azure-Region

Wenn Sie Cloud Volumes ONTAP verwenden, sollte der Konsolenagent in derselben Azure-Region wie die von ihm verwalteten Cloud Volumes ONTAP -Systeme oder in der "Azure-Regionenpaar" für die Cloud Volumes ONTAP -Systeme. Diese Anforderung stellt sicher, dass zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten eine Azure Private Link-Verbindung verwendet wird.

"Erfahren Sie, wie Cloud Volumes ONTAP einen Azure Private Link verwendet"

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.

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.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.

Endpunkte	Zweck
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.
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"

Schritt 4: Einrichten der Bereitstellungsberechtigungen für den Konsolen-Agenten

Sie müssen dem Konsolen-Agenten Azure-Berechtigungen erteilen, indem Sie eine der folgenden Optionen verwenden:

- Option 1: Weisen Sie der Azure-VM mithilfe einer systemseitig zugewiesenen verwalteten Identität eine benutzerdefinierte Rolle zu.
- Option 2: Geben Sie dem Konsolen-Agenten die Anmeldeinformationen für einen Azure-Dienstprinzipal mit den erforderlichen Berechtigungen.

Befolgen Sie die Schritte, um Berechtigungen für den Konsolenagenten vorzubereiten.

Erstellen einer benutzerdefinierten Rolle für die Bereitstellung des Konsolenagenten

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.

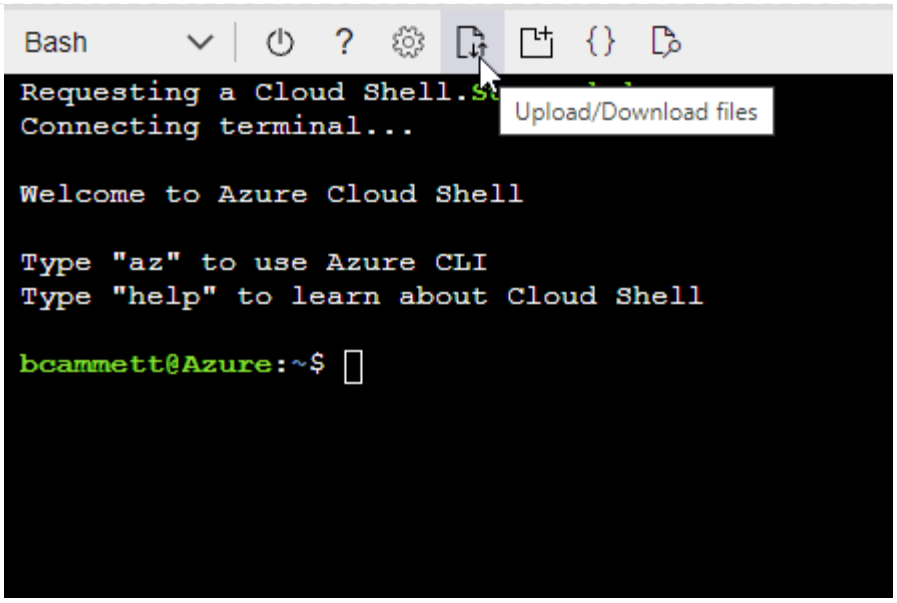
   Beispiel

   ```
   "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
```

Dienstprinzipal

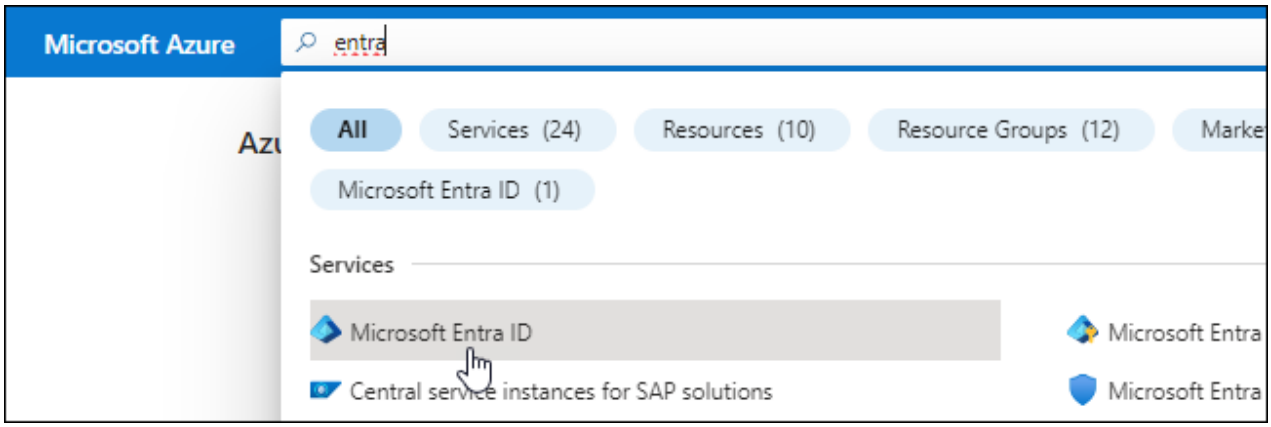
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die der Konsolenagent benötigt.

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.

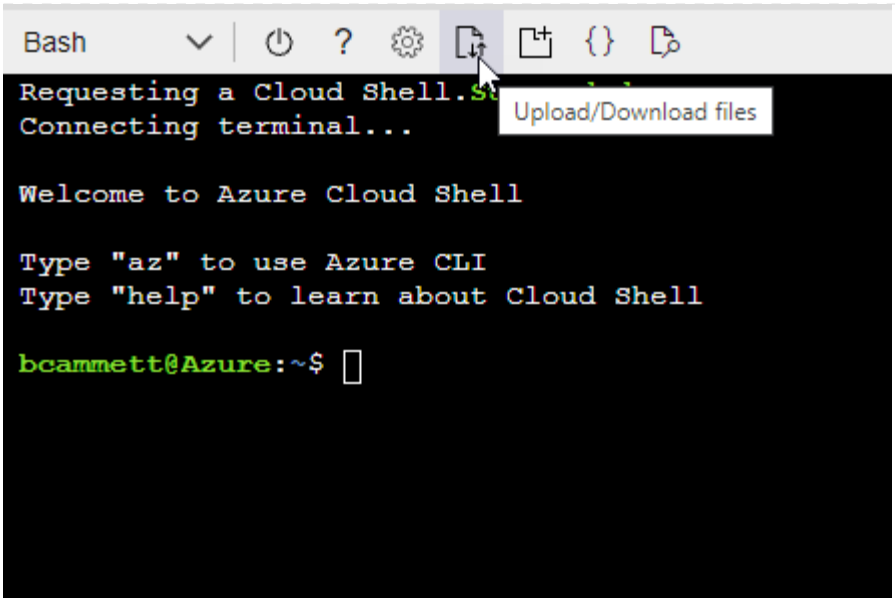
      Beispiel

      ```
      "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**.

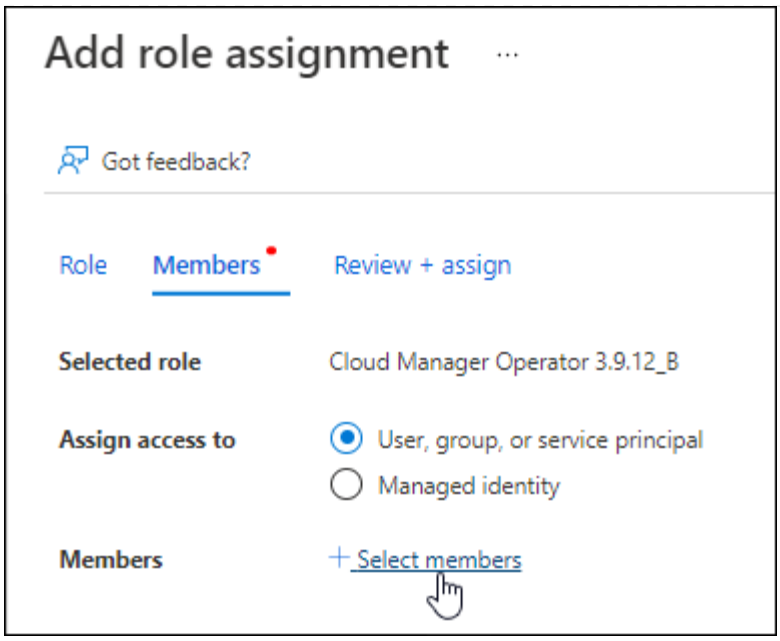
   b. Wählen Sie das Abonnement aus.

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

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

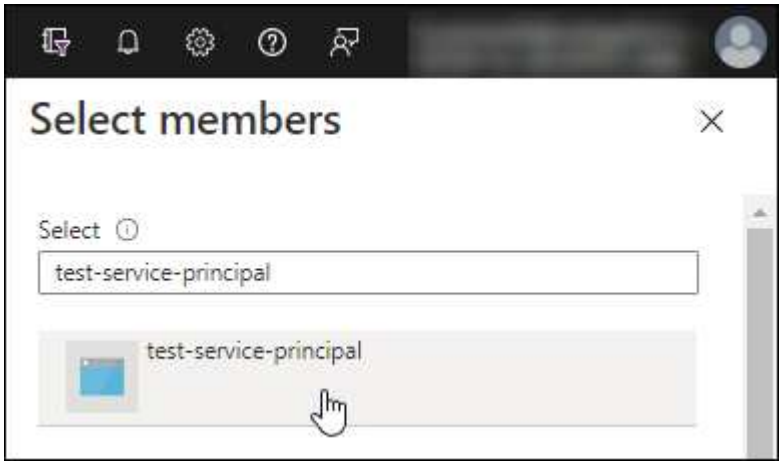
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - 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**.

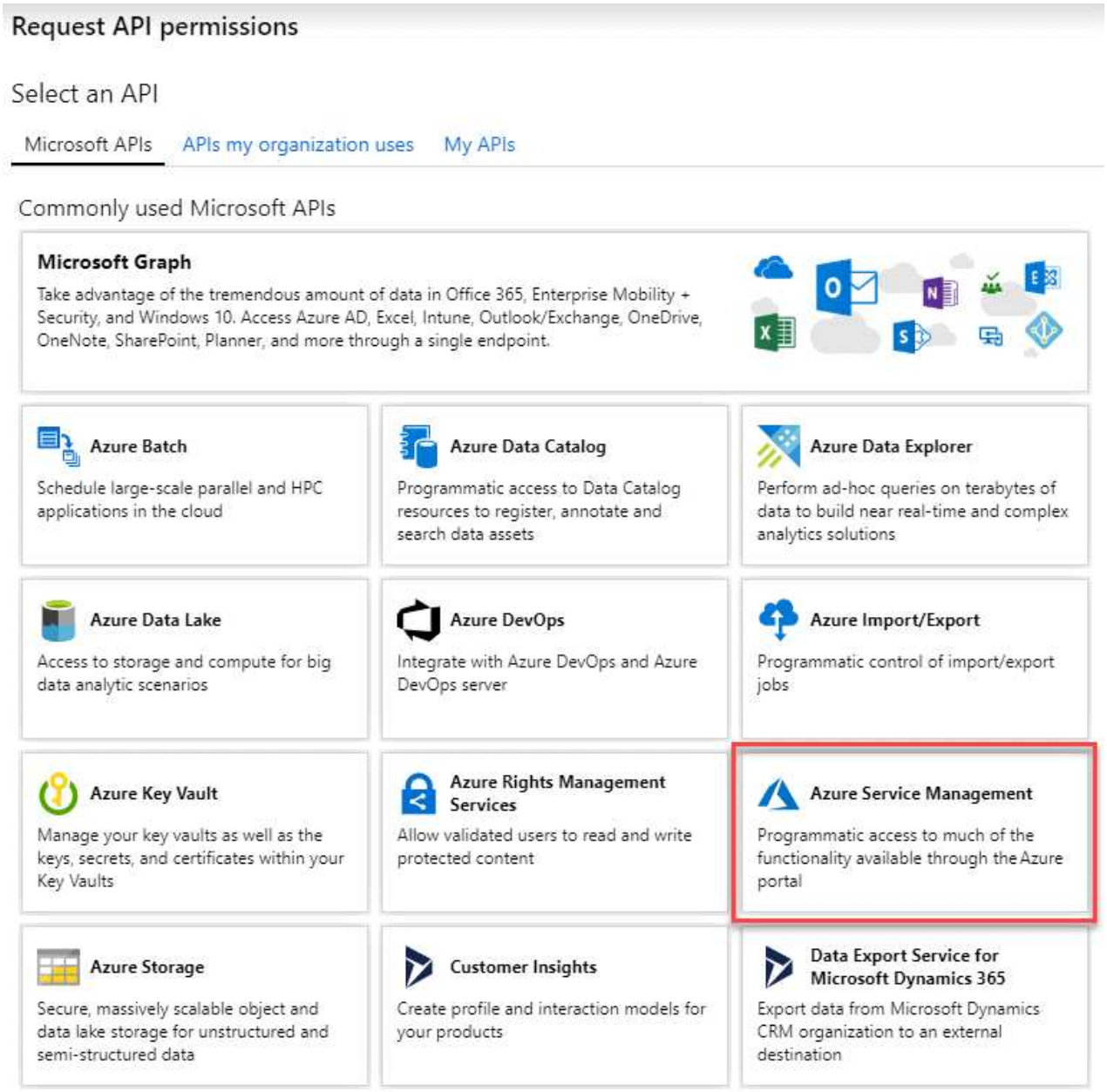
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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.

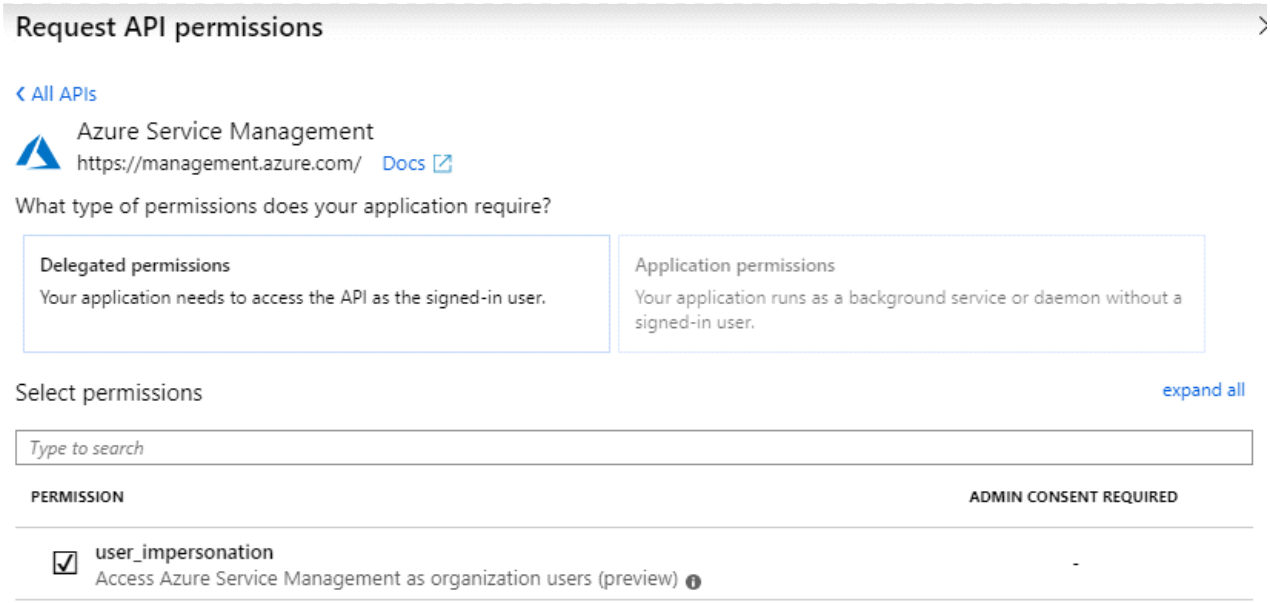
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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.

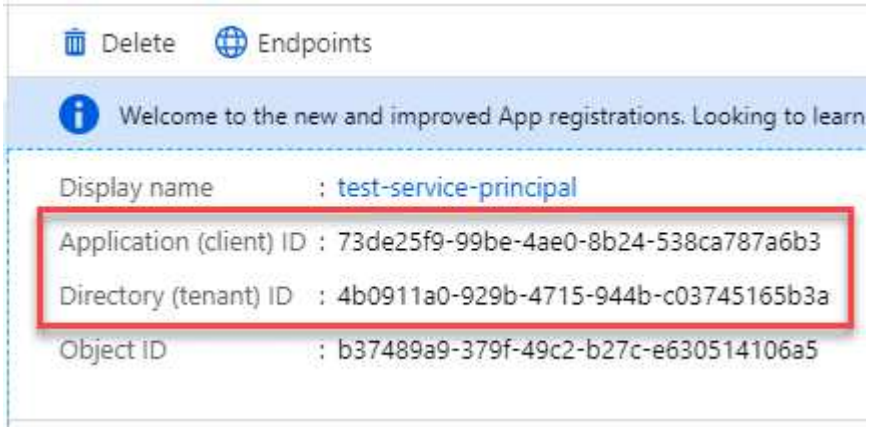


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

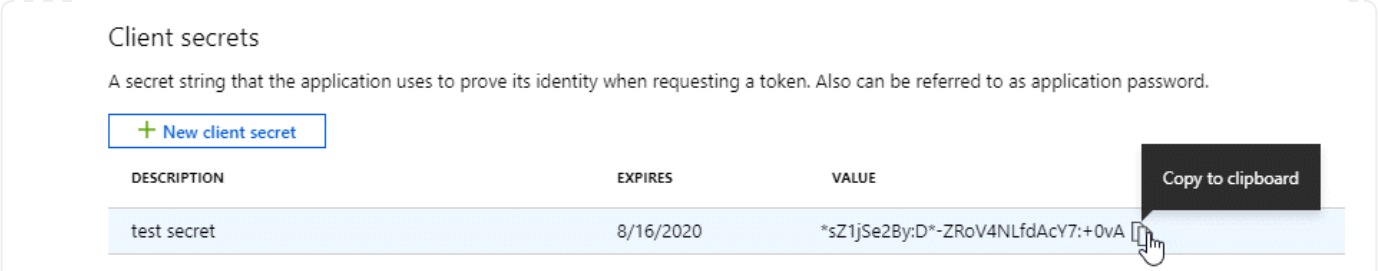
1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



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.



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.

Schritt 5: Installieren des Konsolenagenten

Nachdem die Voraussetzungen erfüllt sind, können Sie die Software manuell auf Ihrem eigenen Linux-Host installieren.

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

- Eine auf der VM in Azure aktivierte verwaltete Identität, sodass 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"

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.

2. Warten Sie, bis die Installation abgeschlossen ist.

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

Wenn die Installation fehlschlägt, können Sie den Installationsbericht und die Protokolle anzeigen, die Ihnen bei der Behebung der Probleme helfen."Erfahren Sie, wie Sie Installationsprobleme beheben."

1. Öffnen Sie einen Webbrowser auf einem Host, der über eine Verbindung zur virtuellen Maschine des Konsolenagenten verfügt, und geben Sie die folgende URL ein:

   https://ipaddress

2. Richten Sie nach der Anmeldung den Konsolenagenten ein:
   a. Geben Sie die Organisation 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.

      Sie sollten den eingeschränkten Modus deaktiviert lassen, da diese Schritte die Verwendung der Konsole im Standardmodus beschreiben. Sie sollten den eingeschränkten Modus nur aktivieren, wenn Sie über eine sichere Umgebung verfügen und dieses Konto von den Backend-Diensten trennen möchten. Wenn das der Fall ist,"Befolgen Sie die Schritte, um mit der NetApp Console im eingeschränkten Modus zu beginnen" .

   d. Wählen Sie **Los geht’s**.

Wenn Sie Azure Blob Storage im selben Azure-Abonnement haben, in dem Sie den Konsolen-Agent erstellt haben, wird auf der Seite **Systeme** automatisch ein Azure Blob Storage-System angezeigt. "Erfahren Sie, wie Sie Azure Blob Storage über die NetApp Console verwalten"

Schritt 6: Berechtigungen für die NetApp Console erteilen

Nachdem Sie den Konsolen-Agent installiert haben, müssen Sie dem Konsolen-Agenten die Azure-Berechtigungen erteilen, die Sie zuvor eingerichtet haben. Durch die Bereitstellung der Berechtigungen kann die Konsole Ihre Daten- und Speicherinfrastruktur in Azure verwalten.

Benutzerdefinierte 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.

Wie geht es weiter?

Gehen Sie zum "NetApp Console" um mit der Verwendung des Konsolenagenten zu beginnen.

Dienstprinzipal

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.

Google Cloud

Installationsoptionen für den Konsolenagenten in Google Cloud

Es gibt verschiedene Möglichkeiten, einen Konsolenagenten in Google Cloud zu erstellen. Der gängigste Weg ist die direkte Nutzung der NetApp Console .

Folgende Installationsoptionen stehen zur Verfügung:

- "Erstellen Sie den Konsolenagenten direkt aus der Konsole"(Dies ist die Standardoption)

  Diese Aktion startet eine VM-Instanz, auf der Linux und die Konsolenagent-Software in einer VPC Ihrer Wahl ausgeführt werden.

- "Erstellen Sie den Konsolenagenten mithilfe der Google Platform"

  Diese Aktion startet auch eine VM-Instanz, auf der Linux und die Konsolen-Agent-Software ausgeführt werden, die Bereitstellung wird jedoch direkt von Google Cloud und nicht von der Konsole aus initiiert.

- "Laden Sie die Software herunter und installieren Sie sie manuell auf Ihrem eigenen Linux-Host"

Die von Ihnen gewählte Installationsoption wirkt sich darauf aus, wie Sie sich auf die Installation vorbereiten. Dazu gehört, wie Sie der Konsole die erforderlichen Berechtigungen erteilen, die sie zum Authentifizieren und Verwalten von Ressourcen in Google Cloud benötigt.

Erstellen Sie einen Konsolenagenten in Google Cloud über die NetApp Console

Sie können über die Konsole einen Konsolenagenten in Google Cloud erstellen. Sie müssen Ihr Netzwerk einrichten, Google Cloud-Berechtigungen vorbereiten, Google Cloud-APIs aktivieren und dann den Konsolenagenten erstellen.

Bevor Sie beginnen

- Sie sollten über eine"Verständnis von Konsolenagenten" .
- Sie sollten überprüfen"Einschränkungen des Konsolenagenten" .

Schritt 1: Einrichten des Netzwerks

Richten Sie das Netzwerk ein, um sicherzustellen, dass der Konsolenagent Ressourcen verwalten kann, mit Verbindungen zu Zielnetzwerken und ausgehendem Internetzugang.

VPC und Subnetz

Wenn Sie den Konsolenagenten erstellen, müssen Sie die VPC und das Subnetz angeben, in dem er sich befinden soll.

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.

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
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	Zum Verwalten von Ressourcen in Google Cloud.
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.

Von der NetApp Konsole kontaktierte Endpunkte

Wenn Sie die webbasierte NetApp Console verwenden, die über die SaaS-Schicht bereitgestellt wird, kontaktiert diese mehrere Endpunkte, um Datenverwaltungsaufgaben abzuschließen. Dazu gehören Endpunkte, die kontaktiert werden, um den Konsolenagenten von der Konsole aus bereitzustellen.

"Zeigen Sie die Liste der von der NetApp Konsole kontaktierten Endpunkte an" .

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"

Implementieren Sie diese Netzwerkanforderung, nachdem Sie den Konsolenagenten erstellt haben.

Schritt 2: Richten Sie Berechtigungen zum Erstellen des Konsolenagenten ein

Bevor Sie einen Konsolenagenten über die Konsole bereitstellen können, müssen Sie Berechtigungen für den Google Platform-Benutzer einrichten, der die Konsolenagent-VM bereitstellt.

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in der Google Platform:

   a. Erstellen Sie eine YAML-Datei, die die folgenden Berechtigungen enthält:

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

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
```

```
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
```

```
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. Aktivieren Sie Cloud Shell in Google Cloud.

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

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

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

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

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

2. Weisen Sie diese benutzerdefinierte Rolle dem Benutzer zu, der den Konsolenagenten über die Konsole oder mithilfe von gcloud bereitstellt.

"Google Cloud-Dokumente: Gewähren einer einzelnen Rolle"

Schritt 3: Erstellen Sie ein Google Cloud-Dienstkonto zur Verwendung mit dem Agenten.

Ein Google Cloud-Dienstkonto ist erforderlich, um dem Konsolenagenten die Berechtigungen zu erteilen, die die Konsole zum Verwalten von Ressourcen in Google Cloud benötigt. Wenn Sie den Konsolen-Agenten erstellen, müssen Sie dieses Dienstkonto mit der Konsolen-Agent-VM verknüpfen.

Es liegt in Ihrer Verantwortung, die benutzerdefinierte Rolle zu aktualisieren, wenn in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. Wenn neue Berechtigungen erforderlich sind, werden diese in den

Versionshinweisen aufgeführt.

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in Google Cloud:

   a. Erstellen Sie eine YAML-Datei, die den Inhalt der"Dienstkontoberechtigungen für den Konsolenagenten" .

   b. Aktivieren Sie Cloud Shell in Google Cloud.

   c. Laden Sie die YAML-Datei hoch, die die erforderlichen Berechtigungen 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 connector --project=myproject --file=agent.yaml
      ```

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

2. Erstellen Sie ein Dienstkonto in Google Cloud und weisen Sie dem Dienstkonto die Rolle zu:

   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"

3. Wenn Sie Cloud Volumes ONTAP -Systeme in anderen Projekten als dem Projekt bereitstellen möchten, in dem sich der Konsolenagent befindet, müssen Sie dem Dienstkonto des Konsolenagenten Zugriff auf diese Projekte gewähren.

   Nehmen wir beispielsweise an, der Konsolenagent befindet sich in Projekt 1 und Sie möchten Cloud Volumes ONTAP -Systeme in Projekt 2 erstellen. Sie müssen dem Dienstkonto in Projekt 2 Zugriff gewähren.

   a. Wählen Sie im IAM- und Admin-Dienst das Google Cloud-Projekt aus, in dem Sie Cloud Volumes ONTAP -Systeme erstellen möchten.

   b. Wählen Sie auf der **IAM**-Seite **Zugriff gewähren** aus und geben Sie die erforderlichen Details ein.

      - Geben Sie die E-Mail-Adresse des Dienstkontos des Konsolenagenten ein.
      - Wählen Sie die benutzerdefinierte Rolle des Konsolenagenten aus.
      - Wählen Sie **Speichern**.

   Weitere Einzelheiten finden Sie unter "Google Cloud-Dokumentation"

Schritt 4: Einrichten freigegebener VPC-Berechtigungen

Wenn Sie eine gemeinsam genutzte VPC verwenden, um Ressourcen in einem Serviceprojekt bereitzustellen, müssen Sie Ihre Berechtigungen vorbereiten.

Diese Tabelle dient als Referenz und Ihre Umgebung sollte die Berechtigungstabelle widerspiegeln, wenn die IAM-Konfiguration abgeschlossen ist.

Berechtigungen für freigegebene VPCs anzeigen

Identität	Schöpfer	Gehostet in	Serviceprojektberechtigungen	Host-Projektberechtigungen	Zweck
Google-Konto zum Bereitstellen des Agenten	Brauch	Serviceprojekt	"Richtlinie zur Agentenbereitstellung"	compute.networkUser	Bereitstellen des Agenten im Serviceprojekt
Agent-Dienstkonto	Brauch	Serviceprojekt	"Agent-Dienstkontorichtlinie"	compute.networkUser deploymentmanager.editor	Bereitstellung und Wartung von Cloud Volumes ONTAP und Diensten im Serviceprojekt
Cloud Volumes ONTAP Dienstkonto	Brauch	Serviceprojekt	storage.admin-Mitglied: NetApp Console als serviceAccount.user	k. A.	(Optional) Für NetApp Cloud Tiering und NetApp Backup and Recovery
Google APIs-Dienstagent	Google Cloud	Serviceprojekt	(Standard-)Editor	compute.networkUser	Interagiert im Rahmen der Bereitstellung mit Google Cloud-APIs. Ermöglicht der Konsole die Verwendung des freigegebenen Netzwerks.
Standarddienstkonto von Google Compute Engine	Google Cloud	Serviceprojekt	(Standard-)Editor	compute.networkUser	Stellt Google Cloud-Instanzen und Recheninfrastruktur im Auftrag der Bereitstellung bereit. Ermöglicht der Konsole die Verwendung des freigegebenen Netzwerks.

Hinweise:

1. deploymentmanager.editor wird im Hostprojekt nur benötigt, wenn Sie keine Firewall-Regeln an die Bereitstellung übergeben und diese von der Konsole für Sie erstellen lassen. Die NetApp Console erstellt eine Bereitstellung im Hostprojekt, die die VPC0-Firewallregel enthält, wenn keine Regel angegeben ist.
2. firewall.create und firewall.delete sind nur erforderlich, wenn Sie keine Firewall-Regeln an die Bereitstellung übergeben und diese von der Konsole für Sie erstellen lassen möchten. Diese Berechtigungen befinden sich in der YAML-Datei des Konsolenkontos. Wenn Sie ein HA-Paar mithilfe einer gemeinsam genutzten VPC bereitstellen, werden diese Berechtigungen zum Erstellen der Firewall-Regeln für VPC1, 2 und 3 verwendet. Bei allen anderen Bereitstellungen werden diese Berechtigungen auch zum Erstellen von Regeln für VPC0 verwendet.
3. Für Cloud Tiering muss das Tiering-Dienstkonto über die Rolle serviceAccount.user für das Dienstkonto verfügen, nicht nur auf Projektebene. Wenn Sie derzeit serviceAccount.user auf Projektebene zuweisen, werden die Berechtigungen nicht angezeigt, wenn Sie das Dienstkonto mit getIAMPolicy abfragen.

Schritt 5: Google Cloud APIs aktivieren

Sie müssen mehrere Google Cloud-APIs aktivieren, bevor Sie den Konsolenagenten und Cloud Volumes ONTAP bereitstellen.

Schritt

1. Aktivieren Sie die folgenden Google Cloud-APIs in Ihrem Projekt:
   - Cloud Infrastructure Manager API
   - Cloud Deployment Manager V2 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 vom Kunden verwalteten Verschlüsselungsschlüsseln (CMEK) verwenden möchten)

"Google Cloud-Dokumentation: APIs aktivieren"

Schritt 6: Erstellen des Konsolenagenten

Erstellen Sie einen Konsolenagenten direkt aus der Konsole.

Durch Erstellen des Konsolenagenten wird eine VM-Instanz in Google Cloud mithilfe einer Standardkonfiguration bereitgestellt. Wechseln Sie nach dem Erstellen des Konsolenagenten nicht zu einer kleineren VM-Instanz mit weniger CPUs oder weniger RAM. "Erfahren Sie mehr über die Standardkonfiguration für den Konsolenagenten" .

Wenn Sie einen Agenten in Google Cloud bereitstellen, erstellt der Agent einen Bucket zum Speichern der Bereitstellungsdateien.

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Die erforderlichen Google Cloud-Berechtigungen zum Erstellen des Konsolen-Agenten und eines Dienstkontos für die Konsolen-Agent-VM.
- Eine VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt.
- Details zu einem Proxyserver, falls für den Internetzugriff vom Konsolenagenten ein Proxy erforderlich ist.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** die Option **Agent bereitstellen > Google Cloud**
3. Überprüfen Sie auf der Seite **Bereitstellen eines Agenten** die Details zu Ihren Anforderungen. Sie haben zwei Möglichkeiten:
   a. Wählen Sie **Weiter** aus, um die Bereitstellung mithilfe des Produkthandbuchs vorzubereiten. Jeder Schritt in der Produktanleitung enthält die Informationen, die auf dieser Seite der Dokumentation enthalten sind.

b. Wählen Sie **Zur Bereitstellung übergehen**, wenn Sie sich bereits durch Befolgen der Schritte auf dieser Seite vorbereitet haben.

4. Befolgen Sie die Schritte im Assistenten, um den Konsolenagenten zu erstellen:
   - Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Google-Konto an, das über die erforderlichen Berechtigungen zum Erstellen der Instanz der virtuellen Maschine verfügen sollte.

     Das Formular ist Eigentum von Google und wird von Google gehostet. Ihre Anmeldeinformationen werden NetApp nicht zur Verfügung gestellt.

   - **Details**: Geben Sie einen Namen für die VM-Instanz ein, geben Sie Tags an, wählen Sie ein Projekt aus und wählen Sie dann das Dienstkonto mit den erforderlichen Berechtigungen aus (weitere Informationen finden Sie im obigen Abschnitt).
   - **Standort**: Geben Sie eine Region, Zone, VPC und ein Subnetz für die Instanz an.
   - **Netzwerk**: Wählen Sie, ob eine öffentliche IP-Adresse aktiviert werden soll, und geben Sie optional eine Proxy-Konfiguration an.
   - **Netzwerk-Tags**: Fügen Sie der Konsolen-Agent-Instanz ein Netzwerk-Tag hinzu, wenn Sie einen transparenten Proxy verwenden. Netzwerk-Tags müssen mit einem Kleinbuchstaben beginnen und können Kleinbuchstaben, Zahlen und Bindestriche enthalten. Tags müssen mit einem Kleinbuchstaben oder einer Zahl enden. Sie können beispielsweise das Tag „console-agent-proxy“ verwenden.
   - **Firewall-Richtlinie**: Wählen Sie, ob Sie eine neue Firewall-Richtlinie erstellen oder eine vorhandene Firewall-Richtlinie auswählen möchten, die die erforderlichen eingehenden und ausgehenden Regeln zulässt.

     "Firewall-Regeln in Google Cloud"

5. Überprüfen Sie Ihre Auswahl, um sicherzustellen, dass Ihre Einrichtung korrekt ist.

   a. Das Kontrollkästchen **Agentenkonfiguration validieren** ist standardmäßig aktiviert, damit die Konsole bei der Bereitstellung die Anforderungen an die Netzwerkkonnektivität validiert. Wenn die Bereitstellung des Agenten durch die Konsole fehlschlägt, wird ein Bericht bereitgestellt, der Sie bei der Fehlerbehebung unterstützt. Wenn die Bereitstellung erfolgreich ist, wird kein Bericht bereitgestellt.

   Wenn Sie immer noch die"vorherige Endpunkte" für Agent-Upgrades verwendet wird, schlägt die Validierung mit einem Fehler fehl. Um dies zu vermeiden, deaktivieren Sie das Kontrollkästchen, um die Validierungsprüfung zu überspringen.

6. Wählen Sie **Hinzufügen**.

   Der Agent ist in etwa 10 Minuten bereit. Bleiben Sie auf der Seite, bis der Vorgang abgeschlossen ist.

Ergebnis

Nach Abschluss des Vorgangs steht der Konsolenagent zur Verwendung bereit.

Wenn die Bereitstellung fehlschlägt, können Sie einen Bericht und Protokolle von der Konsole herunterladen, die Ihnen bei der Behebung der Probleme helfen."Erfahren Sie, wie Sie Installationsprobleme beheben."

Wenn Sie Google Cloud Storage-Buckets im selben Google Cloud-Konto haben, in dem Sie den Konsolen-Agent erstellt haben, wird auf der Seite **Systeme** automatisch ein Google Cloud Storage-System angezeigt. "Erfahren Sie, wie Sie Google Cloud Storage über die Konsole verwalten"

Erstellen Sie einen Konsolenagenten aus Google Cloud

Um mithilfe von Google Cloud einen Konsolenagenten in Google Cloud zu erstellen, müssen Sie Ihr Netzwerk einrichten, Google Cloud-Berechtigungen vorbereiten, Google Cloud-APIs aktivieren und dann den Konsolenagenten erstellen.

Bevor Sie beginnen

- Sie sollten eine"Verständnis von Konsolenagenten" .
- Sie sollten überprüfen"Einschränkungen des Konsolenagenten" .

Schritt 1: Einrichten des Netzwerks

Richten Sie das Netzwerk ein, damit der Konsolenagent Ressourcen verwalten und eine Verbindung zu Zielnetzwerken und dem Internet herstellen kann.

VPC und Subnetz

Wenn Sie den Konsolenagenten erstellen, müssen Sie die VPC und das Subnetz angeben, in dem er sich befinden soll.

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.

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
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	Zum Verwalten von Ressourcen in Google Cloud.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.

Endpunkte	Zweck
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.
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.

Von der NetApp Konsole kontaktierte Endpunkte

Wenn Sie die webbasierte NetApp Console verwenden, die über die SaaS-Schicht bereitgestellt wird, kontaktiert diese mehrere Endpunkte, um Datenverwaltungsaufgaben abzuschließen. Dazu gehören Endpunkte, die kontaktiert werden, um den Konsolenagenten von der Konsole aus bereitzustellen.

"Zeigen Sie die Liste der von der NetApp Konsole kontaktierten Endpunkte an" .

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"

Implementieren Sie diese Netzwerkanforderung, nachdem Sie den Konsolenagenten erstellt haben.

Schritt 2: Richten Sie Berechtigungen zum Erstellen des Konsolenagenten ein

Richten Sie Berechtigungen für den Google Cloud-Benutzer ein, um die Konsolen-Agent-VM von Google Cloud bereitzustellen.

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in der Google Platform:

a. Erstellen Sie eine YAML-Datei, die die folgenden Berechtigungen enthält:

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

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

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

b. Aktivieren Sie Cloud Shell in Google Cloud.

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

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

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

```
gcloud iam roles create connectorDeployment --project=myproject --file=connector-deployment.yaml
```

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

2. Weisen Sie diese benutzerdefinierte Rolle dem Benutzer zu, der den Konsolenagenten von Google Cloud bereitstellt.

   "Google Cloud-Dokumente: Gewähren einer einzelnen Rolle"

Schritt 3: Berechtigungen für die Konsolen-Agent-Operationen einrichten

Ein Google Cloud-Dienstkonto ist erforderlich, um dem Konsolenagenten die Berechtigungen zu erteilen, die die Konsole zum Verwalten von Ressourcen in Google Cloud benötigt. Wenn Sie den Konsolen-Agenten erstellen, müssen Sie dieses Dienstkonto mit der Konsolen-Agent-VM verknüpfen.

Es liegt in Ihrer Verantwortung, die benutzerdefinierte Rolle zu aktualisieren, wenn in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. Wenn neue Berechtigungen erforderlich sind, werden diese in den Versionshinweisen aufgeführt.

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in Google Cloud:

   a. Erstellen Sie eine YAML-Datei, die den Inhalt der"Dienstkontoberechtigungen für den Konsolenagenten" .

   b. Aktivieren Sie Cloud Shell in Google Cloud.

   c. Laden Sie die YAML-Datei hoch, die die erforderlichen Berechtigungen 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 connector --project=myproject --file=agent.yaml
      ```

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

2. Erstellen Sie ein Dienstkonto in Google Cloud und weisen Sie dem Dienstkonto die Rolle zu:

   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"

3. Wenn Sie Cloud Volumes ONTAP -Systeme in anderen Projekten als dem Projekt bereitstellen möchten, in dem sich der Konsolenagent befindet, müssen Sie dem Dienstkonto des Konsolenagenten Zugriff auf diese Projekte gewähren.

   Nehmen wir beispielsweise an, der Konsolenagent befindet sich in Projekt 1 und Sie möchten Cloud Volumes ONTAP -Systeme in Projekt 2 erstellen. Sie müssen dem Dienstkonto in Projekt 2 Zugriff gewähren.

   a. Wählen Sie im IAM- und Admin-Dienst das Google Cloud-Projekt aus, in dem Sie Cloud Volumes

ONTAP -Systeme erstellen möchten.

b. Wählen Sie auf der **IAM**-Seite **Zugriff gewähren** aus und geben Sie die erforderlichen Details ein.
   - Geben Sie die E-Mail-Adresse des Dienstkontos des Konsolenagenten ein.
   - Wählen Sie die benutzerdefinierte Rolle des Konsolenagenten aus.
   - Wählen Sie **Speichern**.

Weitere Einzelheiten finden Sie unter "Google Cloud-Dokumentation"

Schritt 4: Einrichten freigegebener VPC-Berechtigungen

Wenn Sie eine gemeinsam genutzte VPC verwenden, um Ressourcen in einem Serviceprojekt bereitzustellen, müssen Sie Ihre Berechtigungen vorbereiten.

Diese Tabelle dient als Referenz und Ihre Umgebung sollte die Berechtigungstabelle widerspiegeln, wenn die IAM-Konfiguration abgeschlossen ist.

Berechtigungen für freigegebene VPCs anzeigen

Identität	Schöpfer	Gehostet in	Serviceprojektberechtigungen	Host-Projektberechtigungen	Zweck
Google-Konto zum Bereitstellen des Agenten	Brauch	Serviceprojekt	"Richtlinie zur Agentenbereitstellung"	compute.networkUser	Bereitstellen des Agenten im Serviceprojekt
Agent-Dienstkonto	Brauch	Serviceprojekt	"Agent-Dienstkontorichtlinie"	compute.networkUser deploymentmanager.editor	Bereitstellung und Wartung von Cloud Volumes ONTAP und Diensten im Serviceprojekt
Cloud Volumes ONTAP Dienstkonto	Brauch	Serviceprojekt	storage.admin-Mitglied: NetApp Console als serviceAccount.user	k. A.	(Optional) Für NetApp Cloud Tiering und NetApp Backup and Recovery
Google APIs-Dienstagent	Google Cloud	Serviceprojekt	(Standard-)Editor	compute.networkUser	Interagiert im Rahmen der Bereitstellung mit Google Cloud-APIs. Ermöglicht der Konsole die Verwendung des freigegebenen Netzwerks.
Standard dienstkonto von Google Compute Engine	Google Cloud	Serviceprojekt	(Standard-)Editor	compute.networkUser	Stellt Google Cloud-Instanzen und Recheninfrastruktur im Auftrag der Bereitstellung bereit. Ermöglicht der Konsole die Verwendung des freigegebenen Netzwerks.

Hinweise:

1. deploymentmanager.editor wird im Hostprojekt nur benötigt, wenn Sie keine Firewall-Regeln an die Bereitstellung übergeben und diese von der Konsole für Sie erstellen lassen. Die NetApp Console erstellt eine Bereitstellung im Hostprojekt, die die VPC0-Firewallregel enthält, wenn keine Regel angegeben ist.
2. firewall.create und firewall.delete sind nur erforderlich, wenn Sie keine Firewall-Regeln an die Bereitstellung übergeben und diese von der Konsole für Sie erstellen lassen möchten. Diese Berechtigungen befinden sich in der YAML-Datei des Konsolenkontos. Wenn Sie ein HA-Paar mithilfe einer gemeinsam genutzten VPC bereitstellen, werden diese Berechtigungen zum Erstellen der Firewall-Regeln für VPC1, 2 und 3 verwendet. Bei allen anderen Bereitstellungen werden diese Berechtigungen auch zum Erstellen von Regeln für VPC0 verwendet.
3. Für Cloud Tiering muss das Tiering-Dienstkonto über die Rolle serviceAccount.user für das Dienstkonto verfügen, nicht nur auf Projektebene. Wenn Sie derzeit serviceAccount.user auf Projektebene zuweisen, werden die Berechtigungen nicht angezeigt, wenn Sie das Dienstkonto mit getIAMPolicy abfragen.

Schritt 5: Google Cloud APIs aktivieren

Aktivieren Sie mehrere Google Cloud-APIs, bevor Sie den Konsolenagenten und Cloud Volumes ONTAP bereitstellen.

Schritt

1. Aktivieren Sie die folgenden Google Cloud-APIs in Ihrem Projekt:
   - Cloud Infrastructure Manager API
   - Cloud Deployment Manager V2 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 vom Kunden verwalteten Verschlüsselungsschlüsseln (CMEK) verwenden möchten)

"Google Cloud-Dokumentation: APIs aktivieren"

Schritt 6: Erstellen des Konsolenagenten

Erstellen Sie mithilfe von Google Cloud einen Konsolenagenten.

Durch das Erstellen des Konsolenagenten wird eine VM-Instanz in Google Cloud mit der Standardkonfiguration bereitgestellt. Wechseln Sie nach der Erstellung des Konsolenagenten nicht zu einer kleineren VM-Instanz mit weniger CPUs oder weniger RAM. "Erfahren Sie mehr über die Standardkonfiguration für den Konsolenagenten" .

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Die erforderlichen Google Cloud-Berechtigungen zum Erstellen des Konsolen-Agenten und eines Dienstkontos für die Konsolen-Agent-VM.
- Eine VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt.
- Ein Verständnis der Anforderungen an VM-Instanzen.
  - **CPU**: 8 Kerne oder 8 vCPUs
  - **RAM**: 32 GB
  - **Maschinentyp**: Wir empfehlen n2-standard-8.

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

Schritte

1. Melden Sie sich mit Ihrer bevorzugten Methode beim Google Cloud SDK an.

   In diesem Beispiel wird eine lokale Shell mit installiertem gcloud SDK verwendet. Sie können jedoch auch die Google Cloud Shell verwenden.

Weitere Informationen zum Google Cloud SDK finden Sie auf der"Google Cloud SDK-Dokumentationsseite" .

2. Stellen Sie sicher, dass Sie als Benutzer angemeldet sind, der über die erforderlichen Berechtigungen verfügt, die im obigen Abschnitt definiert sind:

```
gcloud auth list
```

Die Ausgabe sollte Folgendes anzeigen, wobei das *-Benutzerkonto das gewünschte Benutzerkonto ist, mit dem Sie sich anmelden möchten:

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install them,
please run:
$ gcloud components update
```

3. Führen Sie den `gcloud compute instances create` Befehl:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

Instanzname

Der gewünschte Instanzname für die VM-Instanz.

Projekt

(Optional) Das Projekt, in dem Sie die VM bereitstellen möchten.

Dienstkonto

Das in der Ausgabe von Schritt 2 angegebene Dienstkonto.

Zone

Die Zone, in der Sie die VM bereitstellen möchten

keine Adresse

(Optional) Es wird keine externe IP-Adresse verwendet (Sie benötigen ein Cloud-NAT oder einen Proxy, um den Datenverkehr ins öffentliche Internet zu leiten).

Netzwerk-Tag

(Optional) Fügen Sie Netzwerk-Tagging hinzu, um eine Firewall-Regel mithilfe von Tags mit der Konsolen-Agent-Instanz zu verknüpfen

Netzwerkpfad

(Optional) Fügen Sie den Namen des Netzwerks hinzu, in dem der Konsolenagent bereitgestellt werden soll (für eine freigegebene VPC benötigen Sie den vollständigen Pfad).

Subnetzpfad

(Optional) Fügen Sie den Namen des Subnetzes hinzu, in dem der Konsolenagent bereitgestellt werden soll (für eine freigegebene VPC benötigen Sie den vollständigen Pfad).

kms-Schlüsselpfad

(Optional) Fügen Sie einen KMS-Schlüssel hinzu, um die Festplatten des Konsolenagenten zu verschlüsseln (IAM-Berechtigungen müssen ebenfalls angewendet werden).

Weitere Informationen zu diesen Flaggen finden Sie auf der"Dokumentation zum Google Cloud Compute SDK" .

Durch Ausführen des Befehls wird der Konsolenagent bereitgestellt. Die Konsolen-Agentinstanz und -Software sollten in etwa fünf Minuten ausgeführt werden.

4. 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.

5. Richten Sie nach der Anmeldung den Konsolenagenten ein:
   a. Geben Sie die Konsolenorganisation an, die mit dem Konsolenagenten verknüpft werden soll.

      "Erfahren Sie mehr über Identitäts- und Zugriffsverwaltung" .

   b. Geben Sie einen Namen für das System ein.

Ergebnis

Der Konsolenagent ist jetzt installiert und mit Ihrer Konsolenorganisation eingerichtet.

Öffnen Sie einen Webbrowser und gehen Sie zu "NetApp Console" um mit der Verwendung des Konsolenagenten zu beginnen.

Installieren Sie den Konsolenagenten manuell in Google Cloud

Um den Konsolen-Agenten manuell auf Ihrem eigenen Linux-Host zu installieren, müssen Sie die Hostanforderungen überprüfen, Ihr Netzwerk einrichten, Google Cloud-Berechtigungen vorbereiten, Google Cloud-APIs aktivieren, die Konsole installieren und dann die vorbereiteten Berechtigungen bereitstellen.

Bevor Sie beginnen

- Sie sollten über eine"Verständnis von Konsolenagenten" .
- Sie sollten überprüfen"Einschränkungen des Konsolenagenten" .

Schritt 1: Hostanforderungen prüfen

Die Konsolenagent-Software muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Portanforderungen usw. erfüllt.

> 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.

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

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"

Schritt 2: 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 3. 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 3: Einrichten des Netzwerks

Richten Sie Ihr Netzwerk so ein, dass der Konsolenagent Ressourcen und Prozesse in Ihrer Hybrid-Cloud-Umgebung verwalten kann. Sie müssen beispielsweise sicherstellen, dass Verbindungen zu Zielnetzwerken verfügbar sind und dass ausgehender Internetzugang verfügbar ist.

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.

Endpunkte	Zweck
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	Zum Verwalten von Ressourcen in Google Cloud.
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.

Endpunkte	Zweck
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.
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"

Schritt 4: Berechtigungen für den Konsolen-Agent einrichten

Ein Google Cloud-Dienstkonto ist erforderlich, um dem Konsolenagenten die Berechtigungen zu erteilen, die die Konsole zum Verwalten von Ressourcen in Google Cloud benötigt. Wenn Sie den Konsolen-Agenten erstellen, müssen Sie dieses Dienstkonto mit der Konsolen-Agent-VM verknüpfen.

Es liegt in Ihrer Verantwortung, die benutzerdefinierte Rolle zu aktualisieren, wenn in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. Wenn neue Berechtigungen erforderlich sind, werden diese in den Versionshinweisen aufgeführt.

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in Google Cloud:

   a. Erstellen Sie eine YAML-Datei, die den Inhalt der"Dienstkontoberechtigungen für den Konsolenagenten" .

   b. Aktivieren Sie Cloud Shell in Google Cloud.

   c. Laden Sie die YAML-Datei hoch, die die erforderlichen Berechtigungen 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 connector --project=myproject --file=agent.yaml
      ```

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

2. Erstellen Sie ein Dienstkonto in Google Cloud und weisen Sie dem Dienstkonto die Rolle zu:

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"

3. Wenn Sie Cloud Volumes ONTAP -Systeme in anderen Projekten als dem Projekt bereitstellen möchten, in dem sich der Konsolenagent befindet, müssen Sie dem Dienstkonto des Konsolenagenten Zugriff auf diese Projekte gewähren.

   Nehmen wir beispielsweise an, der Konsolenagent befindet sich in Projekt 1 und Sie möchten Cloud Volumes ONTAP -Systeme in Projekt 2 erstellen. Sie müssen dem Dienstkonto in Projekt 2 Zugriff gewähren.

   a. Wählen Sie im IAM- und Admin-Dienst das Google Cloud-Projekt aus, in dem Sie Cloud Volumes ONTAP -Systeme erstellen möchten.
   b. Wählen Sie auf der **IAM**-Seite **Zugriff gewähren** aus und geben Sie die erforderlichen Details ein.
      - Geben Sie die E-Mail-Adresse des Dienstkontos des Konsolenagenten ein.
      - Wählen Sie die benutzerdefinierte Rolle des Konsolenagenten aus.
      - Wählen Sie **Speichern**.

   Weitere Einzelheiten finden Sie unter "Google Cloud-Dokumentation"

Schritt 5: Einrichten freigegebener VPC-Berechtigungen

Wenn Sie eine gemeinsam genutzte VPC verwenden, um Ressourcen in einem Serviceprojekt bereitzustellen, müssen Sie Ihre Berechtigungen vorbereiten.

Diese Tabelle dient als Referenz und Ihre Umgebung sollte die Berechtigungstabelle widerspiegeln, wenn die IAM-Konfiguration abgeschlossen ist.

Berechtigungen für freigegebene VPCs anzeigen

Identität	Schöpfer	Gehostet in	Serviceprojektberechtigungen	Host-Projektberechtigungen	Zweck
Google-Konto zum Bereitstellen des Agenten	Brauch	Serviceprojekt	"Richtlinie zur Agentenbereitstellung"	compute.networkUser	Bereitstellen des Agenten im Serviceprojekt
Agent-Dienstkonto	Brauch	Serviceprojekt	"Agent-Dienstkontorichtlinie"	compute.networkUser deploymentmanager.editor	Bereitstellung und Wartung von Cloud Volumes ONTAP und Diensten im Serviceprojekt
Cloud Volumes ONTAP Dienstkonto	Brauch	Serviceprojekt	storage.admin-Mitglied: NetApp Console als serviceAccount.user	k. A.	(Optional) Für NetApp Cloud Tiering und NetApp Backup and Recovery
Google APIs-Dienstagent	Google Cloud	Serviceprojekt	(Standard-)Editor	compute.networkUser	Interagiert im Rahmen der Bereitstellung mit Google Cloud-APIs. Ermöglicht der Konsole die Verwendung des freigegebenen Netzwerks.
Standarddienstkonto von Google Compute Engine	Google Cloud	Serviceprojekt	(Standard-)Editor	compute.networkUser	Stellt Google Cloud-Instanzen und Recheninfrastruktur im Auftrag der Bereitstellung bereit. Ermöglicht der Konsole die Verwendung des freigegebenen Netzwerks.

Hinweise:

1. deploymentmanager.editor wird im Hostprojekt nur benötigt, wenn Sie keine Firewall-Regeln an die Bereitstellung übergeben und diese von der Konsole für Sie erstellen lassen. Die NetApp Console erstellt eine Bereitstellung im Hostprojekt, die die VPC0-Firewallregel enthält, wenn keine Regel angegeben ist.
2. firewall.create und firewall.delete sind nur erforderlich, wenn Sie keine Firewall-Regeln an die Bereitstellung übergeben und diese von der Konsole für Sie erstellen lassen möchten. Diese Berechtigungen befinden sich in der YAML-Datei des Konsolenkontos. Wenn Sie ein HA-Paar mithilfe einer gemeinsam genutzten VPC bereitstellen, werden diese Berechtigungen zum Erstellen der Firewall-Regeln für VPC1, 2 und 3 verwendet. Bei allen anderen Bereitstellungen werden diese Berechtigungen auch zum Erstellen von Regeln für VPC0 verwendet.
3. Für Cloud Tiering muss das Tiering-Dienstkonto über die Rolle serviceAccount.user für das Dienstkonto verfügen, nicht nur auf Projektebene. Wenn Sie derzeit serviceAccount.user auf Projektebene zuweisen, werden die Berechtigungen nicht angezeigt, wenn Sie das Dienstkonto mit getIAMPolicy abfragen.

Schritt 6: Google Cloud APIs aktivieren

Bevor Sie einen Console-Agenten in Google Cloud bereitstellen können, müssen mehrere Google Cloud APIs aktiviert werden.

Schritt

1. Aktivieren Sie die folgenden Google Cloud-APIs in Ihrem Projekt:
   - Cloud Infrastructure Manager API
   - Cloud Deployment Manager V2 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 vom Kunden verwalteten Verschlüsselungsschlüsseln (CMEK) verwenden möchten)

"Google Cloud-Dokumentation: APIs aktivieren"

Schritt 7: Installieren des Konsolenagenten

Nachdem die Voraussetzungen erfüllt sind, können Sie die Software manuell auf Ihrem eigenen Linux-Host installieren.

Wenn Sie einen Agenten bereitstellen, erstellt das System auch einen Google Cloud-Bucket zum Speichern der Bereitstellungsdateien.

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.

2. Warten Sie, bis die Installation abgeschlossen ist.

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

Wenn die Installation fehlschlägt, können Sie den Installationsbericht und die Protokolle anzeigen, die Ihnen bei der Behebung der Probleme helfen."Erfahren Sie, wie Sie Installationsprobleme beheben."

1. Öffnen Sie einen Webbrowser auf einem Host, der über eine Verbindung zur virtuellen Maschine des Konsolenagenten verfügt, und geben Sie die folgende URL ein:

   https://ipaddress

2. Richten Sie nach der Anmeldung den Konsolenagenten ein:

   a. Geben Sie die Organisation 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.

      Sie sollten den eingeschränkten Modus deaktiviert lassen, da diese Schritte die Verwendung der Konsole im Standardmodus beschreiben. Sie sollten den eingeschränkten Modus nur aktivieren, wenn Sie über eine sichere Umgebung verfügen und dieses Konto von den Backend-Diensten trennen möchten. Wenn das der Fall ist,"Befolgen Sie die Schritte, um mit der NetApp Console im eingeschränkten Modus zu beginnen" .

   d. Wählen Sie **Los geht's**.

      Wenn die Installation fehlschlägt, können Sie Protokolle und einen Bericht anzeigen, die Ihnen bei der Fehlerbehebung helfen."Erfahren Sie, wie Sie Installationsprobleme beheben."

Wenn Sie Google Cloud Storage-Buckets im selben Google Cloud-Konto haben, in dem Sie den Konsolen-Agent erstellt haben, wird auf der Seite **Systeme** automatisch ein Google Cloud Storage-System angezeigt. "Erfahren Sie, wie Sie Google Cloud Storage über die NetApp Console verwalten"

Schritt 8: Erteilen Sie dem Konsolenagenten Berechtigungen

Sie müssen dem Konsolenagenten die Google Cloud-Berechtigungen erteilen, die Sie zuvor eingerichtet haben. Durch die Bereitstellung der Berechtigungen kann der Konsolenagent Ihre Daten und Speicherinfrastruktur in Google Cloud verwalten.

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 Google Cloud-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.

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

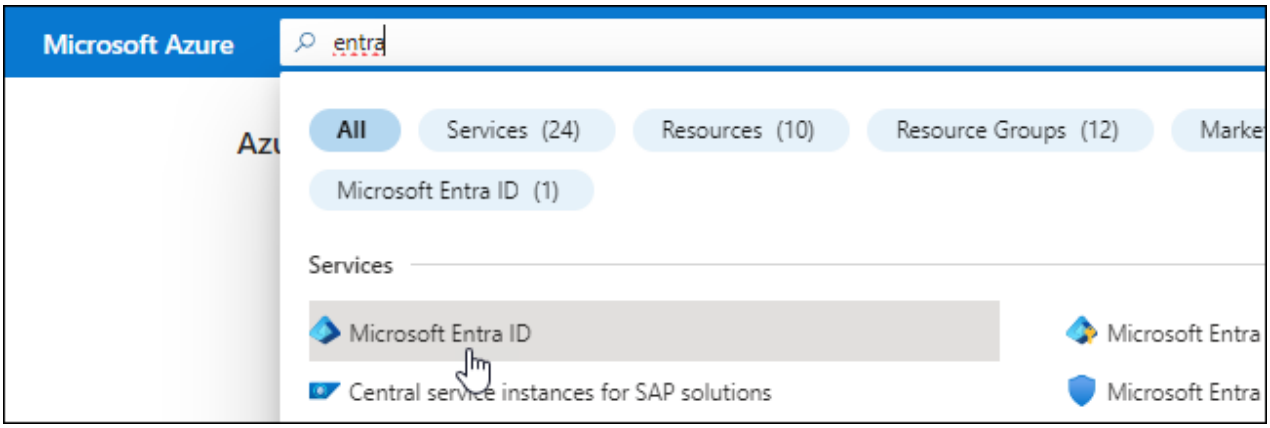
Wenn der Konsolen-Agent vor Ort installiert ist, müssen Sie dem Konsolen-Agenten Azure-Berechtigungen erteilen, indem Sie einen Dienstprinzipal in der Microsoft Entra ID einrichten und die Azure-Anmeldeinformationen abrufen, die der Konsolen-Agent benötigt.

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.

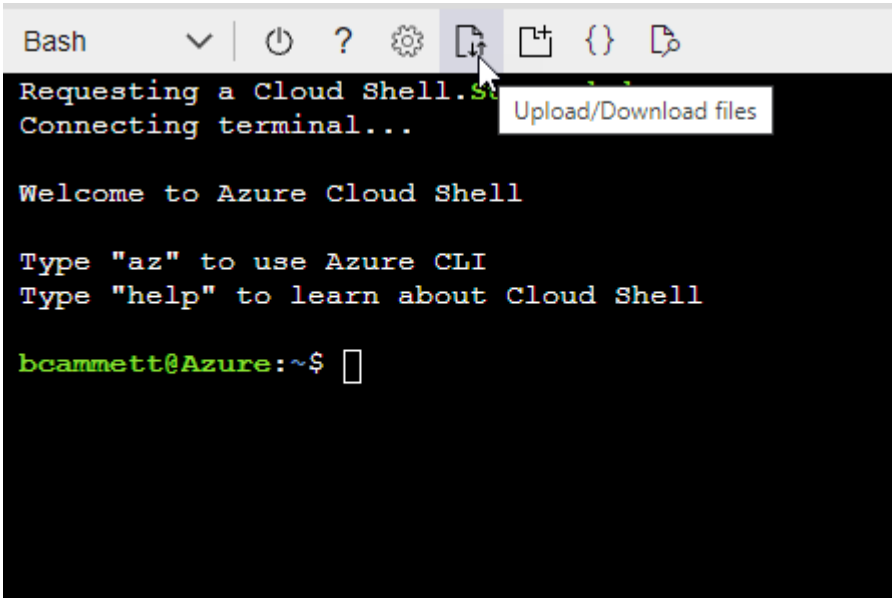
      Beispiel

      ```
      "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**.

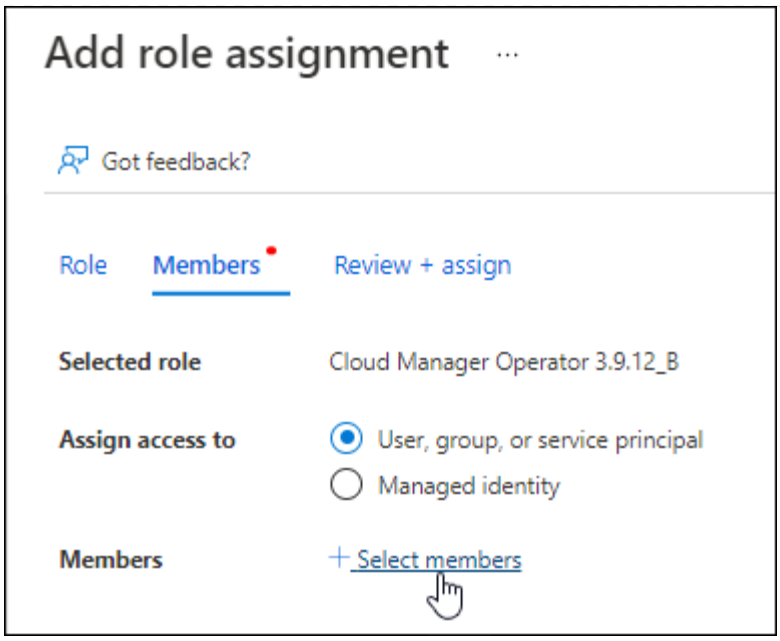
   b. Wählen Sie das Abonnement aus.

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

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

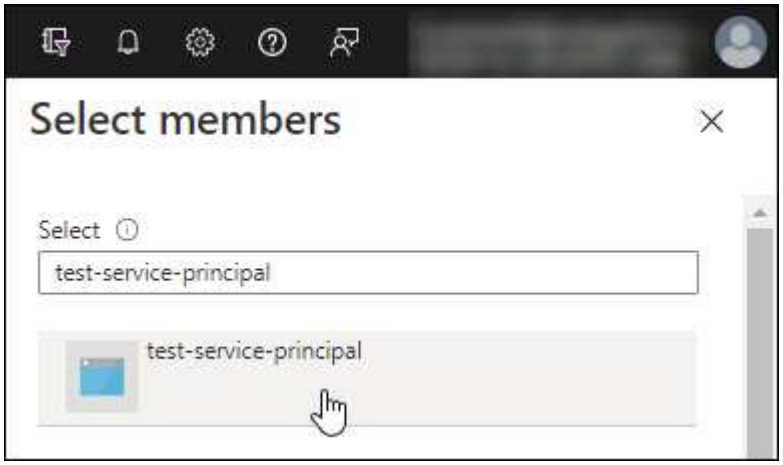
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - 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**.

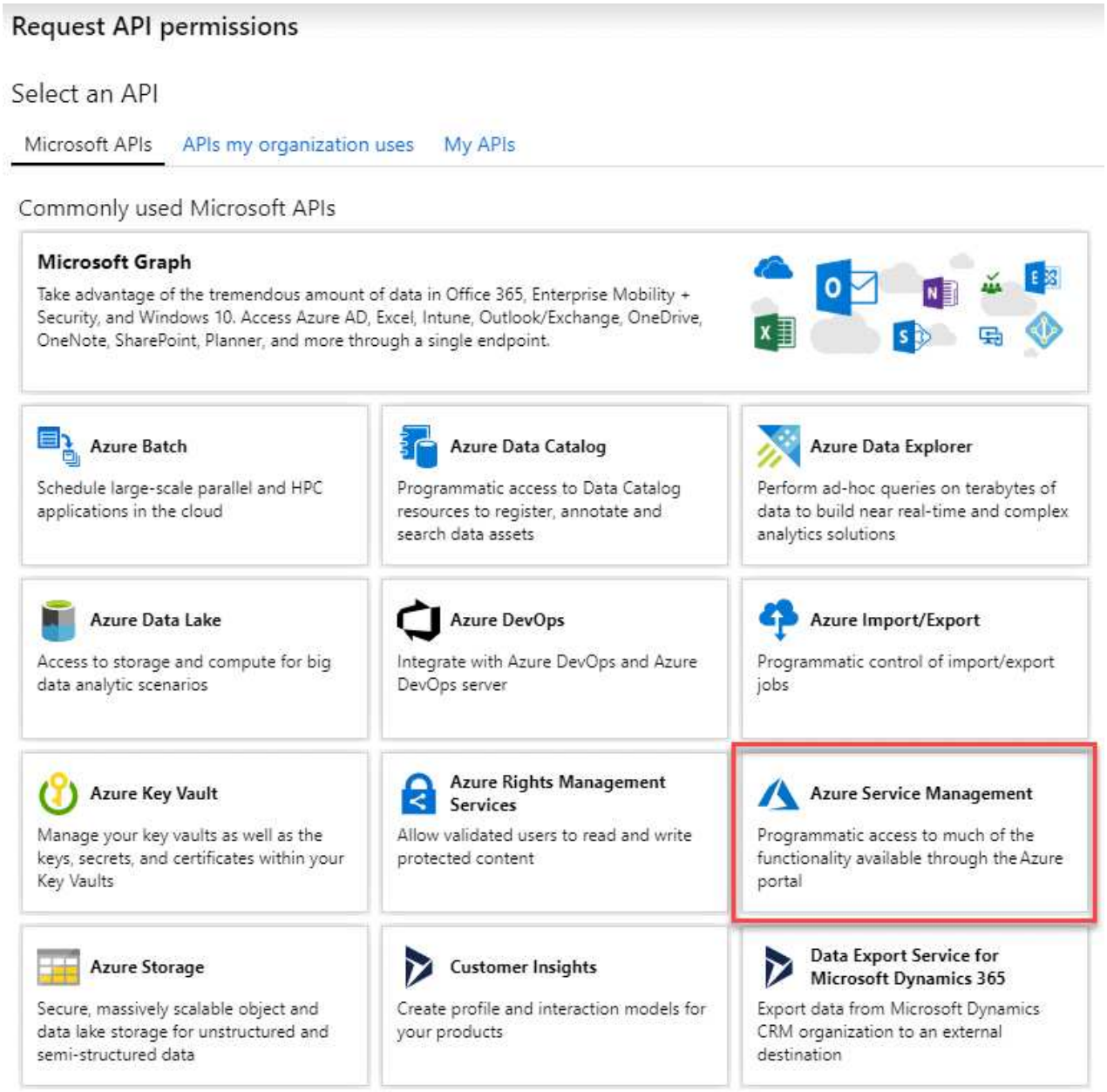
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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.

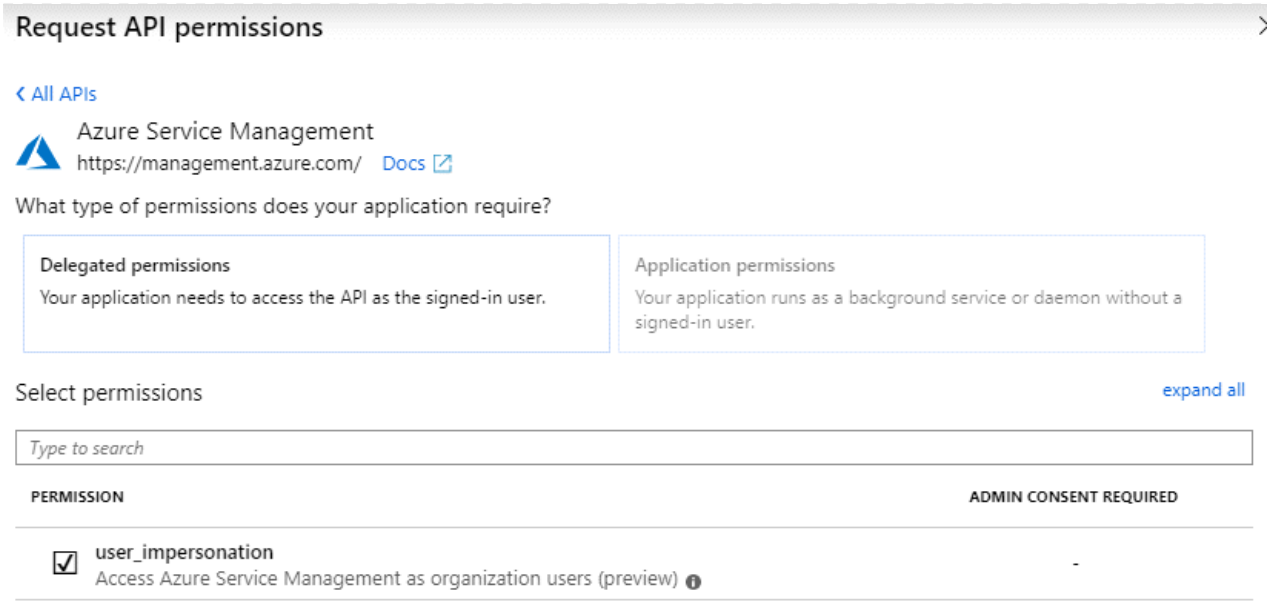
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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.

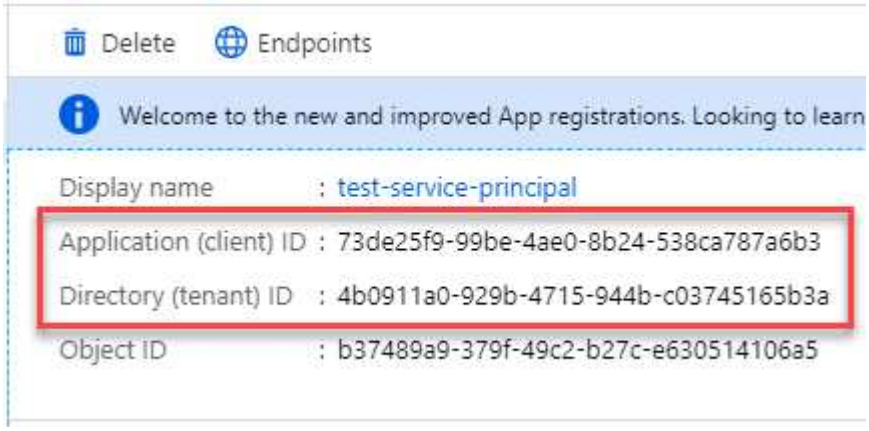


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

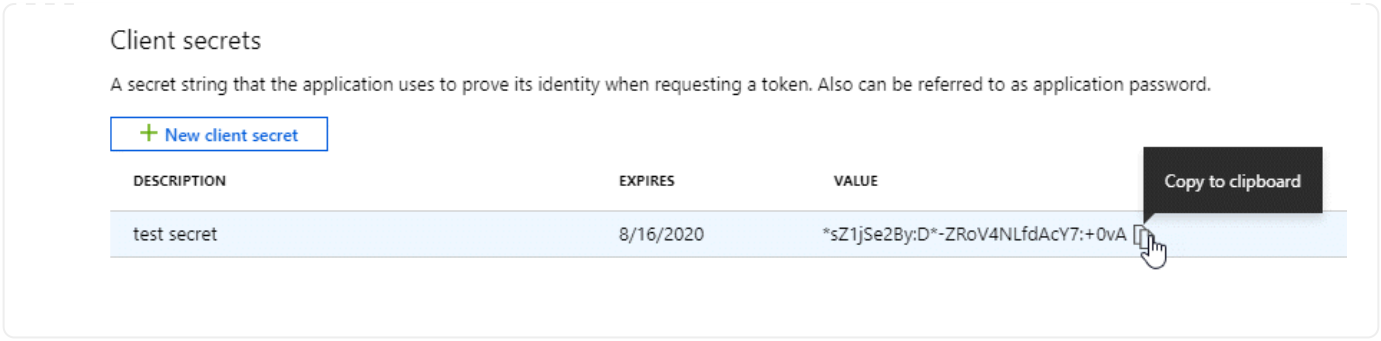
1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



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 4. 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

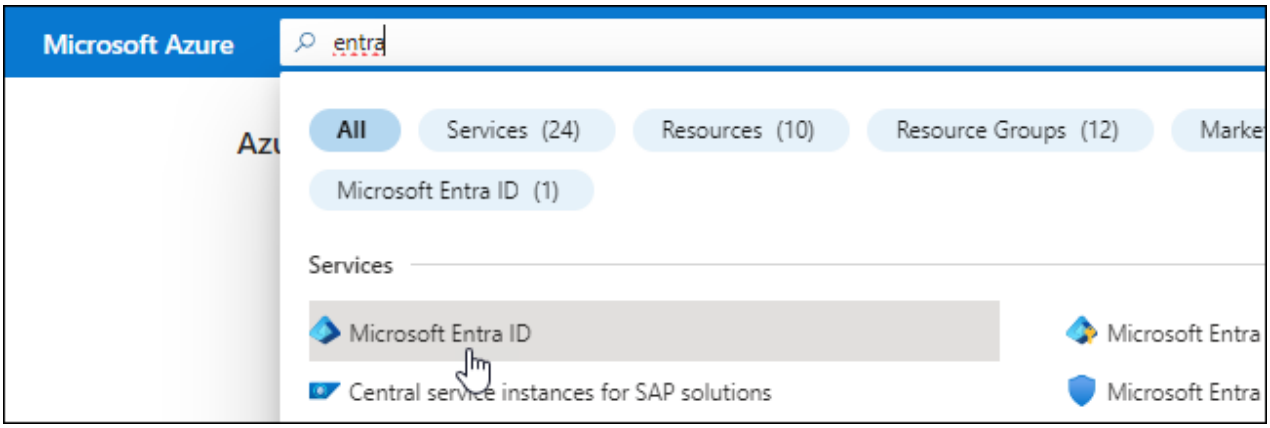
Wenn der Konsolen-Agent vor Ort installiert ist, müssen Sie dem Konsolen-Agenten Azure-Berechtigungen erteilen, indem Sie einen Dienstprinzipal in der Microsoft Entra ID einrichten und die Azure-Anmeldeinformationen abrufen, die der Konsolen-Agent benötigt.

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.

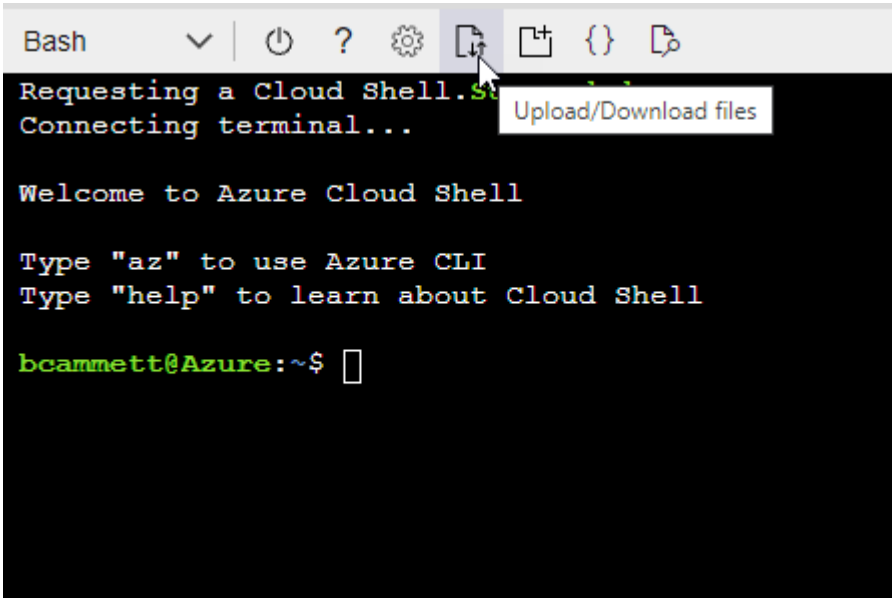
      Beispiel

      ```
      "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**.

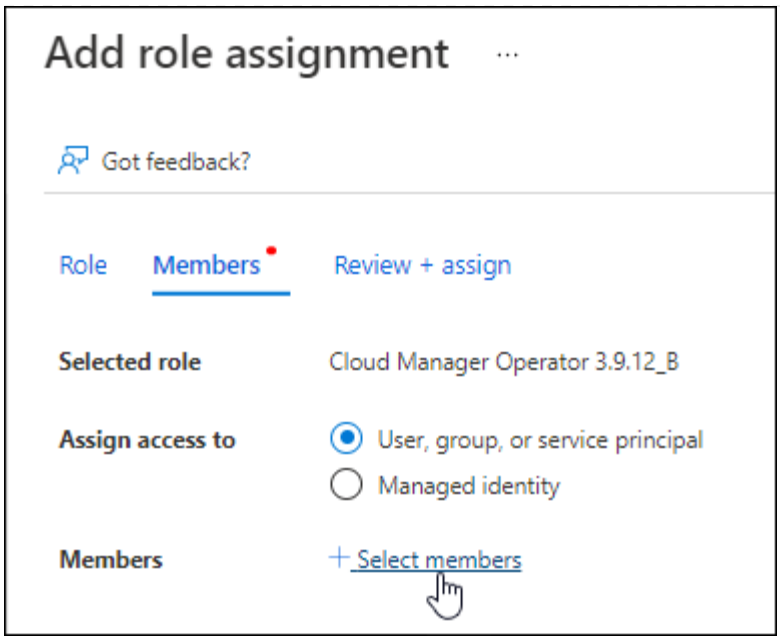
   b. Wählen Sie das Abonnement aus.

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

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

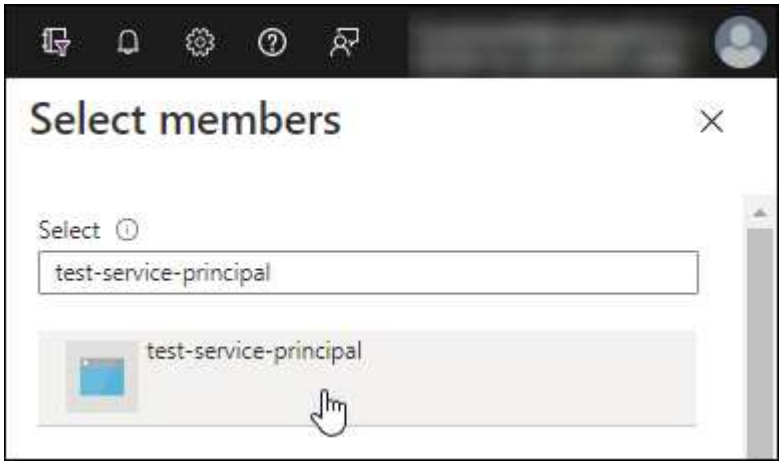
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - 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**.

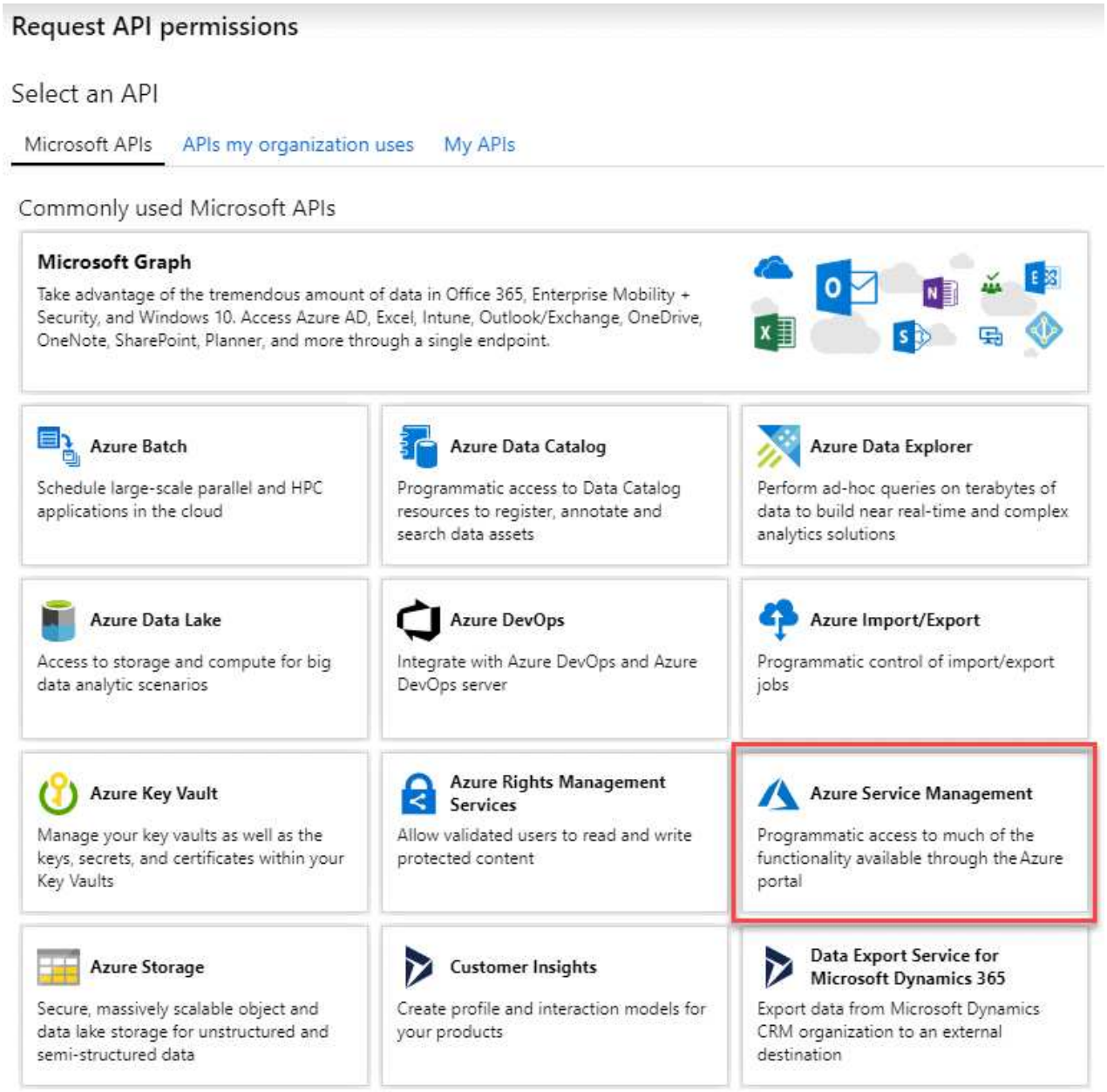
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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.

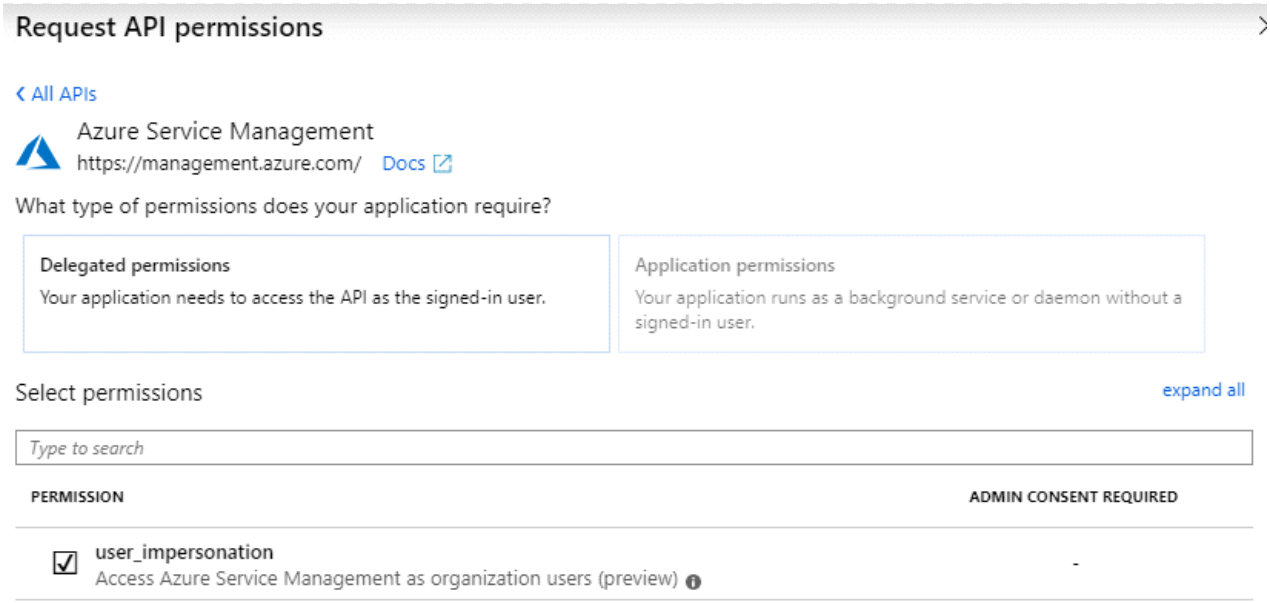
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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.

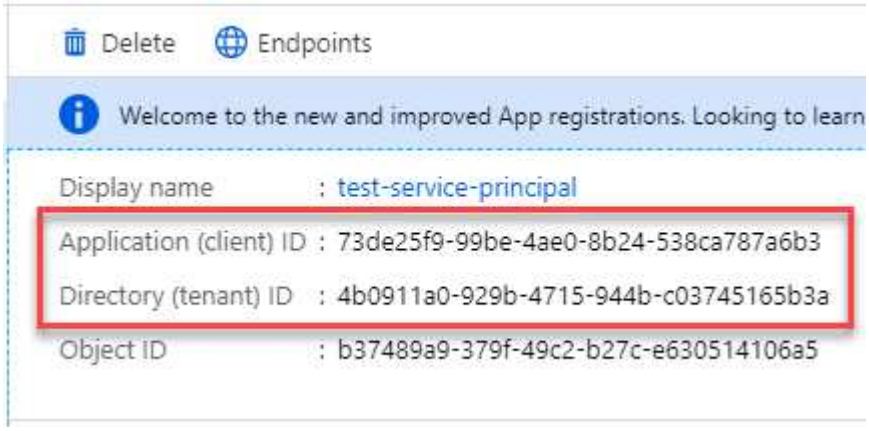


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

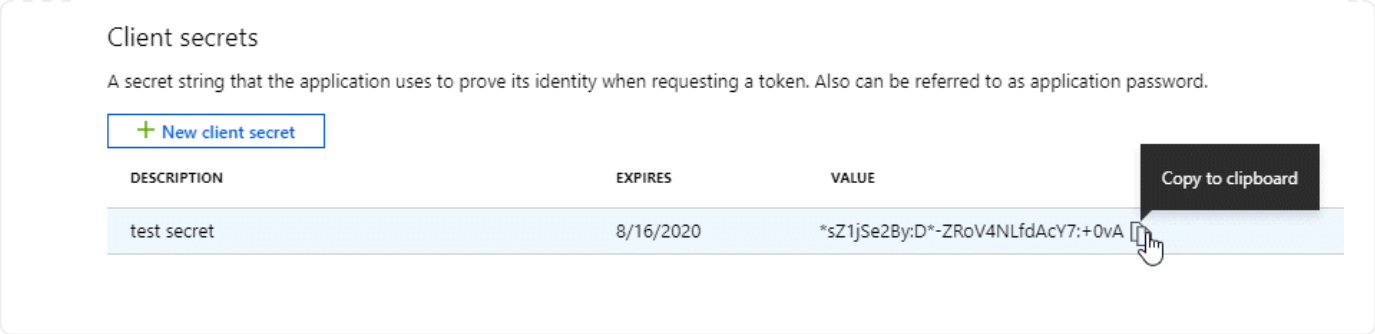
1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



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

Konsolenagenten verwalten

Verwalten Sie einen VCenter- oder ESXi-Host für den Konsolenagenten

Sie können nach der Bereitstellung des Konsolenagenten Änderungen an Ihrem vorhandenen VCenter- oder ESXi-Host vornehmen. Sie können beispielsweise die CPU oder den RAM der VM-Instanz erhöhen, die den Konsolenagenten hostet.

Führen Sie diese Wartungsaufgaben mithilfe der VM-Webkonsole durch:

- Erhöhen Sie die Festplattengröße
- Starten Sie den Agenten neu
- Aktualisieren statischer Routen
- Suchdomänen aktualisieren

Einschränkungen

Das Upgrade des Agenten über die Konsole wird noch nicht unterstützt. Darüber hinaus können Sie nur Informationen zur IP-Adresse, zum DNS und zu Gateways anzeigen.

Zugriff auf die VM-Wartungskonsole

Sie können vom VSphere-Client aus auf die Wartungskonsole zugreifen.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.

Ändern Sie das Kennwort des Wartungsbenutzers

Sie können das Passwort für die `maint` Benutzer.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `1` , um die `System Configuration` Speisekarte.
6. Eingeben `1` um das Wartungsbenutzerkennwort zu ändern und den Anweisungen auf dem Bildschirm zu folgen.

Erhöhen Sie die CPU oder den RAM der VM-Instanz

Sie können die CPU oder den RAM der VM-Instanz erhöhen, die den Konsolenagenten hostet.

Bearbeiten Sie die VM-Instanzeinstellungen in Ihrem VCenter- oder ESXi-Host und wenden Sie die Änderungen dann mit der Wartungskonsole an.

Schritte im VSphere-Client

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Klicken Sie mit der rechten Maustaste auf die VM-Instanz und wählen Sie **Einstellungen bearbeiten**.
4. Erhöhen Sie den für die Partition /opt oder /var verwendeten Festplattenspeicher.
   a. Wählen Sie **Festplatte 2**, um den für /opt verwendeten Festplattenspeicher zu erhöhen.
   b. Wählen Sie **Festplatte 3**, um den für /var verwendeten Festplattenspeicher zu erhöhen.
5. Speichern Sie Ihre Änderungen.

Schritte in der Wartungskonsole

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `1 to view the `System Configuration` Speisekarte.
6. Eingeben `2` und folgen Sie den Anweisungen auf dem Bildschirm. Die Konsole sucht nach neuen Einstellungen und vergrößert die Partitionen.

Netzwerkeinstellungen für die Agent-VM anzeigen

Zeigen Sie die Netzwerkeinstellungen für die Agent-VM im VSphere-Client an, um Netzwerkprobleme zu bestätigen oder zu beheben. Sie können die folgenden Netzwerkeinstellungen nur anzeigen (nicht

aktualisieren): IP-Adresse und DNS-Details.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `2` , um die `Network Configuration` Speisekarte.
6. Geben Sie eine Zahl zwischen 1 und 6 ein, um die entsprechenden Netzwerkeinstellungen anzuzeigen.

Aktualisieren Sie die statischen Routen für die Agent-VM

Fügen Sie nach Bedarf statische Routen für die Agent-VM hinzu, aktualisieren oder entfernen Sie sie.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `2` , um die `Network Configuration` Speisekarte.
6. Eingeben `7` um statische Routen zu aktualisieren und den Anweisungen auf dem Bildschirm zu folgen.
7. Drücken Sie die Eingabetaste.
8. Nehmen Sie optional weitere Änderungen vor.
9. Eingeben `9` um Ihre Änderungen zu übernehmen.

Aktualisieren der Domänensucheinstellungen für die Agent-VM

Sie können die Suchdomäneneinstellungen für die Agent-VM aktualisieren.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `2`` , um die `Network Configuration` Speisekarte.
6. Eingeben `8` um die Domänensucheinstellungen zu aktualisieren und den Anweisungen auf dem Bildschirm zu folgen.
7. Drücken Sie die Eingabetaste.

8. Nehmen Sie optional weitere Änderungen vor.
9. Eingeben `9` um Ihre Änderungen zu übernehmen.

Zugriff auf die Diagnosetools des Agenten

Greifen Sie auf Diagnosetools zu, um Probleme mit dem Konsolenagenten zu beheben. Der NetApp -Support fordert Sie möglicherweise bei der Fehlerbehebung dazu auf.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `3` um das Menü „Support und Diagnose“ anzuzeigen.
6. Eingeben `1` um auf die Diagnosetools zuzugreifen und den Anweisungen auf dem Bildschirm zu folgen. + Sie können beispielsweise überprüfen, ob alle Agentendienste ausgeführt werden. "Überprüfen Sie den Status des Konsolenagenten" .

Fernzugriff auf die Diagnosetools des Agenten

Mit einem Tool wie Putty können Sie remote auf Diagnosetools zugreifen. Aktivieren Sie den SSH-Zugriff auf die Agent-VM, indem Sie ein Einmalkennwort zuweisen.

Der SSH-Zugriff ermöglicht erweiterte Terminalfunktionen wie Kopieren und Einfügen.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `3` , um die `Support and Diagnostics` Speisekarte.
6. Eingeben `2` um auf die Diagnosetools zuzugreifen und den Anweisungen auf dem Bildschirm zu folgen, um ein Einmalkennwort zu konfigurieren, das nach 24 Stunden abläuft.
7. Verwenden Sie ein SSH-Tool wie Putty, um mit dem Benutzernamen eine Verbindung zur Agent-VM herzustellen `diag` und das von Ihnen konfigurierte Einmalkennwort.

Installieren Sie ein CA-signiertes Zertifikat für den webbasierten Konsolenzugriff

Wenn Sie die NetApp Console im eingeschränkten Modus verwenden, ist die Benutzeroberfläche über die virtuelle Maschine des Konsolenagenten zugänglich, die in Ihrer Cloud-Region oder vor Ort bereitgestellt wird. Standardmäßig verwendet die Konsole ein selbstsigniertes SSL-Zertifikat, um sicheren HTTPS-Zugriff auf die

webbasierte Konsole bereitzustellen, die auf dem Konsolenagenten ausgeführt wird.

Falls Ihr Unternehmen dies erfordert, können Sie ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat installieren, das einen besseren Sicherheitsschutz bietet als ein selbstsigniertes Zertifikat. Nachdem Sie das Zertifikat installiert haben, verwendet die Konsole das von der Zertifizierungsstelle signierte Zertifikat, wenn Benutzer auf die webbasierte Konsole zugreifen.

Installieren eines HTTPS-Zertifikats

Installieren Sie ein von einer Zertifizierungsstelle signiertes Zertifikat für den sicheren Zugriff auf die webbasierte Konsole, die auf dem Konsolenagenten ausgeführt wird.

Informationen zu diesem Vorgang

Sie können das Zertifikat mit einer der folgenden Optionen installieren:

- Generieren Sie eine Zertifikatsignieranforderung (CSR) von der Konsole aus, übermitteln Sie die Zertifikatsanforderung an eine Zertifizierungsstelle und installieren Sie dann das von der Zertifizierungsstelle signierte Zertifikat auf dem Konsolenagenten.

  Das Schlüsselpaar, das die Konsole zum Generieren der CSR verwendet, wird intern auf dem Konsolenagenten gespeichert. Die Konsole ruft automatisch dasselbe Schlüsselpaar (privater Schlüssel) ab, wenn Sie das Zertifikat auf dem Konsolenagenten installieren.

- Installieren Sie ein CA-signiertes Zertifikat, das Sie bereits haben.

  Bei dieser Option wird die CSR nicht über die Konsole generiert. Sie generieren die CSR separat und speichern den privaten Schlüssel extern. Sie stellen der Konsole den privaten Schlüssel zur Verfügung, wenn Sie das Zertifikat installieren.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **HTTPS-Setup**.

   Zum Bearbeiten muss der Konsolenagent verbunden sein.

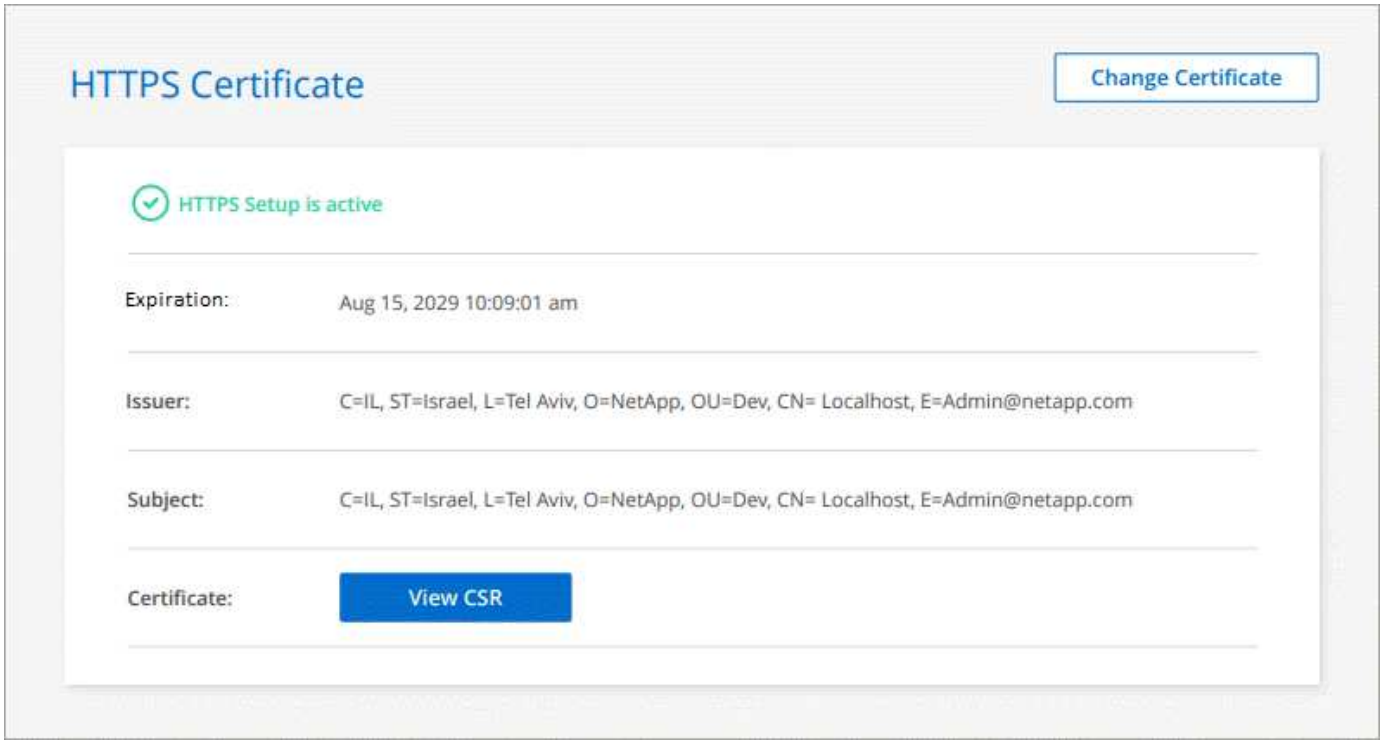
3. Installieren Sie auf der Seite „HTTPS-Setup“ ein Zertifikat, indem Sie eine Zertifikatsignieranforderung (CSR) generieren oder Ihr eigenes CA-signiertes Zertifikat installieren:

Option	Beschreibung
Erstellen Sie eine CSR	a. Geben Sie den Hostnamen oder DNS des Konsolenagent-Hosts (seinen allgemeinen Namen) ein und wählen Sie dann **CSR generieren**. Die Konsole zeigt eine Zertifikatsignieranforderung an. b. Verwenden Sie die CSR, um eine SSL-Zertifikatsanforderung an eine Zertifizierungsstelle zu senden. Das Zertifikat muss das Base-64-codierte X.509-Format von Privacy Enhanced Mail (PEM) verwenden. c. Laden Sie die Zertifikatsdatei hoch und wählen Sie dann **Installieren**.

Option	Beschreibung
Installieren Sie Ihr eigenes CA-signiertes Zertifikat	a. Wählen Sie **CA-signiertes Zertifikat installieren**. b. Laden Sie sowohl die Zertifikatsdatei als auch den privaten Schlüssel und wählen Sie dann **Installieren**. Das Zertifikat muss das Base-64-codierte X.509-Format von Privacy Enhanced Mail (PEM) verwenden.

Ergebnis

Der Konsolenagent verwendet jetzt das von der Zertifizierungsstelle signierte Zertifikat, um sicheren HTTPS-Zugriff bereitzustellen. Das folgende Bild zeigt einen Agenten, der für sicheren Zugriff konfiguriert ist:



Erneuern Sie das HTTPS-Zertifikat der Konsole

Sie sollten das HTTPS-Zertifikat des Agenten vor Ablauf erneuern, um einen sicheren Zugriff zu gewährleisten. Wenn Sie das Zertifikat nicht vor Ablauf erneuern, wird eine Warnung angezeigt, wenn Benutzer über HTTPS auf die Webkonsole zugreifen.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **HTTPS-Setup**.

   Es werden Details zum Zertifikat angezeigt, einschließlich des Ablaufdatums.

3. Wählen Sie **Zertifikat ändern** und folgen Sie den Schritten zum Generieren einer CSR oder zum Installieren Ihres eigenen CA-signierten Zertifikats.

Konfigurieren eines Konsolenagenten zur Verwendung eines Proxyservers

Wenn Ihre Unternehmensrichtlinien die Verwendung eines Proxyservers für die gesamte Kommunikation mit dem Internet erfordern, müssen Sie Ihre Agenten für die Verwendung dieses Proxyservers konfigurieren. Wenn Sie während der Installation keinen Konsolenagenten für die Verwendung eines Proxyservers konfiguriert haben, können Sie den Konsolenagenten jederzeit für die Verwendung dieses Proxyservers konfigurieren.

Der Proxyserver des Agenten ermöglicht ausgehenden Internetzugriff ohne öffentliche IP oder NAT-Gateway. Der Proxyserver bietet ausgehende Konnektivität nur für den Konsolenagenten, nicht für Cloud Volumes ONTAP Systeme.

Wenn Cloud Volumes ONTAP -Systeme keinen ausgehenden Internetzugang haben, konfiguriert die Konsole sie so, dass sie den Proxyserver des Konsolenagenten verwenden. Sie müssen sicherstellen, dass die Sicherheitsgruppe des Konsolenagenten eingehende Verbindungen über Port 3128 zulässt. Öffnen Sie diesen Port, nachdem Sie den Konsolenagenten bereitgestellt haben.

Wenn der Konsolenagent selbst keine ausgehende Internetverbindung hat, können Cloud Volumes ONTAP -Systeme den konfigurierten Proxyserver nicht verwenden.

Unterstützte Konfigurationen

- Transparente Proxyserver werden für Agenten unterstützt, die Cloud Volumes ONTAP -Systeme bedienen. Wenn Sie NetApp -Datendienste mit Cloud Volumes ONTAP verwenden, erstellen Sie einen dedizierten Agenten für Cloud Volumes ONTAP, bei dem Sie einen transparenten Proxyserver verwenden können.
- Explizite Proxyserver werden von allen Agenten unterstützt, einschließlich derjenigen, die Cloud Volumes ONTAP -Systeme verwalten, und derjenigen, die NetApp -Datendienste verwalten.
- HTTP und HTTPS.
- Der Proxyserver kann sich in der Cloud oder in Ihrem Netzwerk befinden.

Nachdem Sie einen Proxy konfiguriert haben, können Sie den Proxy-Typ nicht mehr ändern. Wenn Sie den Proxy-Typ ändern müssen, entfernen Sie den Konsolen-Agenten und fügen einen neuen Agenten mit dem neuen Proxy-Typ hinzu.

Aktivieren Sie einen expliziten Proxy auf einem Konsolenagenten

Wenn Sie einen Konsolenagenten für die Verwendung eines Proxyservers konfigurieren, verwenden dieser Agent und die von ihm verwalteten Cloud Volumes ONTAP -Systeme (einschließlich aller HA-Mediatoren) alle den Proxyserver.

Dieser Vorgang startet den Konsolenagenten neu. Stellen Sie sicher, dass der Konsolenagent im Leerlauf ist, bevor Sie fortfahren.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **Agent bearbeiten**.

   Zum Bearbeiten muss der Konsolenagent aktiv sein.

3. Wählen Sie **HTTP-Proxy-Konfiguration**.

4. Wählen Sie im Feld „Konfigurationstyp“ **Expliziter Proxy** aus.
5. Wählen Sie **Proxy aktivieren**.
6. Geben Sie den Server mit der Syntax an http://address:port oder https://address:port
7. Geben Sie einen Benutzernamen und ein Kennwort an, wenn für den Server eine Basisauthentifizierung erforderlich ist.

   Beachten Sie Folgendes:

   - Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.
   - Für einen Domänenbenutzer müssen Sie den ASCII-Code für das \ wie folgt eingeben: Domänenname%92Benutzername

     Beispiel: netapp%92proxy

   - Die Konsole unterstützt keine Passwörter, die das @-Zeichen enthalten.
8. Wählen Sie **Speichern**.

Aktivieren Sie einen transparenten Proxy für einen Konsolenagenten

Nur Cloud Volumes ONTAP unterstützt die Verwendung eines transparenten Proxys auf dem Konsolenagenten. Wenn Sie zusätzlich zu Cloud Volumes ONTAP NetApp -Datendienste verwenden, sollten Sie einen separaten Agenten für die Verwendung für Datendienste oder für Cloud Volumes ONTAP erstellen.

Stellen Sie vor der Aktivierung eines transparenten Proxys sicher, dass die folgenden Anforderungen erfüllt sind:

- Der Agent wird im selben Netzwerk wie der transparente Proxyserver installiert.
- Die TLS-Prüfung ist auf dem Proxyserver aktiviert.
- Sie verfügen über ein Zertifikat im PEM-Format, das mit dem auf dem transparenten Proxyserver verwendeten Zertifikat übereinstimmt.
- Sie verwenden den Konsolenagenten für keine anderen NetApp -Datendienste als Cloud Volumes ONTAP.

Um einen vorhandenen Agenten für die Verwendung eines transparenten Proxyservers zu konfigurieren, verwenden Sie das Wartungstool des Konsolenagenten, das über die Befehlszeile auf dem Konsolenagentenhost verfügbar ist.

Wenn Sie einen Proxyserver konfigurieren, wird der Konsolenagent neu gestartet. Stellen Sie sicher, dass der Konsolenagent im Leerlauf ist, bevor Sie fortfahren.

Schritte

Stellen Sie sicher, dass Sie über eine Zertifikatsdatei im PEM-Format für den Proxyserver verfügen. Wenn Sie kein Zertifikat haben, wenden Sie sich an Ihren Netzwerkadministrator, um eines zu erhalten.

1. Öffnen Sie eine Befehlszeilenschnittstelle auf dem Konsolenagent-Host.
2. Navigieren Sie zum Verzeichnis des Wartungstools des Konsolenagenten: `/opt/application/netapp/service-manager-2/agent-maint-console`
3. Führen Sie den folgenden Befehl aus, um den transparenten Proxy zu aktivieren. `/home/ubuntu/<certificate-file>.pem` ist das Verzeichnis und der Name der Zertifikatsdatei, die

Sie für den Proxyserver haben:

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

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

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

Ändern Sie den transparenten Proxy für den Konsolenagenten

Sie können den vorhandenen transparenten Proxy-Server eines Console-Agenten aktualisieren, indem Sie die folgende Funktion verwenden: `proxy update` Befehl oder entfernen Sie den transparenten Proxy-Server mithilfe des Befehls `proxy remove` Befehl. Weitere Informationen finden Sie in der Dokumentation zu"Agenten-Wartungskonsole" Die

> Nachdem Sie einen Proxy konfiguriert haben, können Sie den Proxy-Typ nicht mehr ändern. Wenn Sie den Proxy-Typ ändern müssen, entfernen Sie den Konsolen-Agenten und fügen einen neuen Agenten mit dem neuen Proxy-Typ hinzu.

Aktualisieren Sie den Proxy des Konsolenagenten, wenn dieser den Zugriff auf das Internet verliert

Wenn sich die Proxy-Konfiguration für Ihr Netzwerk ändert, verliert Ihr Agent möglicherweise den Zugriff auf das Internet. Zum Beispiel, wenn jemand das Passwort für den Proxyserver ändert oder das Zertifikat aktualisiert. In diesem Fall müssen Sie direkt vom Konsolenagent-Host auf die Benutzeroberfläche zugreifen und die Einstellungen aktualisieren. Stellen Sie sicher, dass Sie Netzwerkzugriff auf den Konsolen-Agent-Host haben und sich bei der Konsole anmelden können.

Aktivieren Sie den direkten API-Verkehr

Wenn Sie einen Console-Agenten für die Verwendung eines Proxy-Servers konfiguriert haben, können Sie den direkten API-Datenverkehr auf dem Console-Agenten aktivieren, um API-Aufrufe direkt an Cloud-Anbieterdienste zu senden, ohne den Proxy zu durchlaufen. Agenten, die in AWS, Azure oder Google Cloud ausgeführt werden, unterstützen diese Option.

Wenn Sie Azure Private Links mit Cloud Volumes ONTAP deaktivieren und Service-Endpunkte verwenden, aktivieren Sie den direkten API-Verkehr. Andernfalls wird der Datenverkehr nicht richtig weitergeleitet.

"Erfahren Sie mehr über die Verwendung eines Azure Private Link oder von Service-Endpunkten mit Cloud Volumes ONTAP"

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **Agent bearbeiten**.

   Zum Bearbeiten muss der Konsolenagent aktiv sein.

3. Wählen Sie **Direkten API-Verkehr unterstützen**.

4. Aktivieren Sie das Kontrollkästchen, um die Option zu aktivieren, und wählen Sie dann **Speichern**.

Fehlerbehebung beim Konsolen-Agent

Um Probleme mit einem Konsolenagenten zu beheben, können Sie die Probleme selbst überprüfen oder mit dem NetApp -Support zusammenarbeiten, der Sie möglicherweise nach Ihrer System-ID, Agentenversion oder den neuesten AutoSupport -Nachrichten fragt.

Wenn Sie über ein NetApp Support Site-Konto verfügen, können Sie auch die"NetApp Wissensdatenbank."

Häufige Fehlermeldungen und Lösungen

Diese Tabelle listet häufige Fehlermeldungen auf und zeigt, wie man sie beheben kann:

Fehlermeldung	Erläuterung	Was zu tun
Die Benutzeroberfläche des Konsolenagenten konnte nicht geladen werden	Die Agenteninstallation ist fehlgeschlagen	• Stellen Sie sicher, dass der Service Manager-Dienst aktiv ist. • Stellen Sie sicher, dass alle Container ausgeführt werden. • Stellen Sie sicher, dass Ihre Firewall den Zugriff auf den Dienst über Port 8888 zulässt. • Sollten weiterhin Probleme auftreten, wenden Sie sich bitte an den Support.
Auf die NetApp Agent-Benutzeroberfläche kann nicht zugegriffen werden	Diese Meldung wird angezeigt, wenn versucht wird, auf die IP-Adresse eines Agenten zuzugreifen. Die Initialisierung des Agenten kann fehlschlagen, wenn er nicht über den richtigen Netzwerkzugriff verfügt oder instabil ist.	• Stellen Sie eine Verbindung zum Konsolenagenten her. • Überprüfen Sie, ob der Service Manager-Dienst • Stellen Sie sicher, dass der Agent über den erforderlichen Netzwerkzugriff verfügt."Erfahren Sie mehr über erforderliche Endpunkte für den Netzwerkzugriff."
Agenteneinstellungen konnten nicht geladen werden	Die Konsole zeigt diese Meldung an, wenn Sie versuchen, auf die Seite mit den Agenteneinstellungen zuzugreifen.	• Überprüfen Sie, ob der OCCM-Container ausgeführt wird und funktioniert. • Wenn das Problem weiterhin besteht, wenden Sie sich an den Support.

Fehlermeldung	Erläuterung	Was zu tun
Supportinformationen für den Agenten konnten nicht geladen werden.	Diese Meldung wird angezeigt, wenn der Agent nicht auf Ihr Supportkonto zugreifen kann.	• Prüfen Sie, ob der Agent ausgehenden Zugriff auf die erforderlichen Endpunkte hat."Erfahren Sie mehr über erforderliche Endpunkte für den Netzwerkzugriff."

Überprüfen Sie den Status des Konsolenagenten

Verwenden Sie einen der folgenden Befehle, um Ihren Konsolenagenten zu überprüfen. Alle Dienste sollten den Status „Wird ausgeführt“ haben. Wenn dies nicht der Fall ist, wenden Sie sich an den NetApp Support.

Ausführlichere Informationen zum Zugriff auf die Konsolen-Agent-Diagnose finden Sie in den folgenden Themen:

- "Überprüfen Sie den Status des Konsolenagenten (für Linux-Hostbereitstellungen)."
- "Überprüfen Sie den Status des Konsolenagenten (für VCenter-Bereitstellungen)."

Docker (für Ubuntu- und VCenter-Bereitstellungen)

```
docker ps -a
```

Podman (für RedHat Enterprise Linux-Bereitstellungen)

```
podman ps -a
```

Anzeigen der Konsolen-Agent-Version

Zeigen Sie die Version des Konsolenagenten an, um das Upgrade zu bestätigen, oder teilen Sie sie Ihrem NetApp -Vertreter mit.

Schritte

1. Wählen Sie **Administration > Support > Agenten**.

   Die Konsole zeigt die Version oben auf der Seite an.

Überprüfen des Netzwerkzugriffs

Stellen Sie sicher, dass der Konsolenagent über den erforderlichen Netzwerkzugriff verfügt."Erfahren Sie mehr über die erforderlichen Netzwerkzugriffspunkte."

Führen Sie Konfigurationsprüfungen auf dem Konsolenagenten durch.

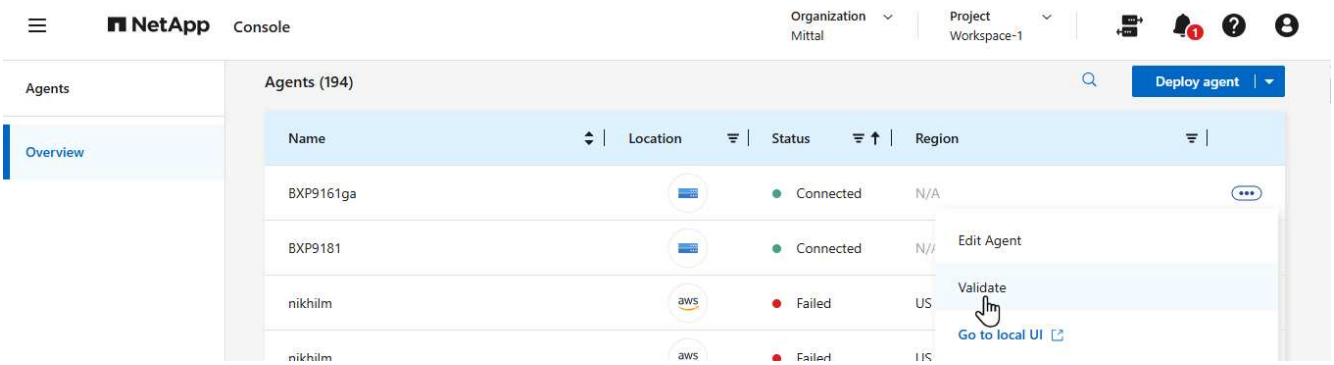
Führen Sie Konfigurationsprüfungen an den Konsolenagenten über die Konsole oder die Agentenwartungskonsole durch, um sicherzustellen, dass sie verbunden sind.

Sie können Konfigurationsprüfungen auch über die Agentenwartungskonsole durchführen."Erfahren Sie mehr über die Verwendung des Befehls config-checker validate."

Sie können nur Agenten validieren, die den Status **Verbunden** haben.

Schritte von der Konsole

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie im Aktionsmenü des Konsolenagenten, den Sie überprüfen möchten, die Option **Validieren** aus.



Die Validierung kann bis zu 15 Minuten dauern. Die Ergebnisse werden nach Abschluss des Vorgangs angezeigt.

Probleme bei der Installation des Konsolenagenten

Wenn die Installation fehlschlägt, sehen Sie sich den Bericht und die Protokolle an, um die Probleme zu beheben.

Sie können auch direkt vom Konsolen-Agent-Host in den folgenden Verzeichnissen auf den Validierungsbericht im JSON-Format und die Konfigurationsprotokolle zugreifen:

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- Bei der Bereitstellung neuer Agenten prüft NetApp die folgenden Endpunkte:"hier aufgeführt" . Diese Konfigurationsprüfung schlägt mit einem Fehler fehl, wenn Sie die vorherigen Endpunkte verwenden, die für Upgrades verwendet wurden."hier aufgeführt" . NetApp empfiehlt, Ihre Firewall-Regeln so schnell wie möglich zu aktualisieren, um den Zugriff auf die aktuellen Endpunkte zu ermöglichen und den Zugriff auf die vorherigen Endpunkte zu blockieren."Erfahren Sie, wie Sie Ihr Netzwerk aktualisieren" .
- Wenn Sie die Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Deaktivieren Sie Konfigurationsprüfungen für manuelle Installationen

Es kann vorkommen, dass Sie die Konfigurationsprüfungen deaktivieren müssen, die während der Installation die ausgehende Konnektivität überprüfen. Wenn Sie beispielsweise einen Agenten in Ihrer Government Cloud-Umgebung manuell installieren, müssen Sie die Konfigurationsprüfungen deaktivieren, da die Installation sonst fehlschlägt.

Schritte

Sie deaktivieren die Konfigurationsprüfung, indem Sie das Flag *skipConfigCheck* in der Datei *com/opt/application/netapp/service-manager-2/config.json* setzen. Standardmäßig ist dieses Flag auf „false“ gesetzt und die Konfigurationsprüfung überprüft den ausgehenden Zugriff für den Agenten. Setzen Sie dieses Flag auf „true“, um die Prüfung zu deaktivieren. Machen Sie sich mit der JSON-Syntax vertraut, bevor Sie diesen Schritt ausführen.

Um die Konfigurationsprüfung wieder zu aktivieren, führen Sie diese Schritte aus und setzen Sie das Flag *skipConfigCheck* auf „false“.

Schritte

1. Greifen Sie als Root oder mit Sudo-Berechtigungen auf den Konsolen-Agent-Host zu.
2. Erstellen Sie eine Sicherungskopie der Datei */opt/application/netapp/service-manager-2/config.json*, um sicherzustellen, dass Sie Ihre Änderungen rückgängig machen können.
3. Stoppen Sie den Dienst Service Manager 2, indem Sie den folgenden Befehl ausführen:

```
systemctl stop netapp-service-manager.service
```

1. Bearbeiten Sie die Datei */opt/application/netapp/service-manager-2/config.json* und ändern Sie den Wert des Flags *skipConfigCheck* auf „true“.

```
  "skipConfigCheck": true
```

2. Speichern Sie Ihre Datei.
3. Starten Sie den Dienst Service Manager 2 neu, indem Sie den folgenden Befehl ausführen:

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

Arbeiten Sie mit dem NetApp Support

Wenn Sie die Probleme mit Ihrem Konsolenagenten nicht lösen konnten, sollten Sie sich an den NetApp -Support wenden. Der NetApp Support fragt möglicherweise nach der Konsolen-Agent-ID oder fordert Sie auf, ihm die Konsolen-Agent-Protokolle zu senden, falls diese noch nicht vorliegen.

Suchen Sie die Konsolen-Agent-ID

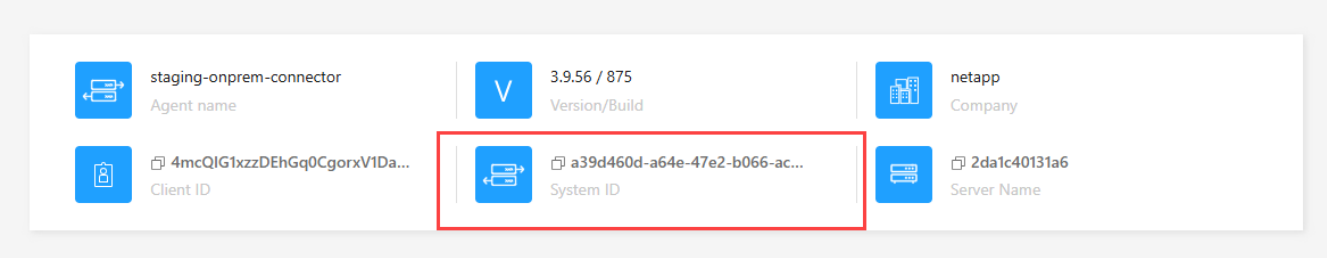
Um Ihnen den Einstieg zu erleichtern, benötigen Sie möglicherweise die System-ID Ihres Konsolenagenten. Die ID wird normalerweise für Lizenzierungs- und Fehlerbehebungszwecke verwendet.

Schritte

1. Wählen Sie **Administration > Support > Agenten**.

   Die System-ID finden Sie oben auf der Seite.

   Beispiel



2. Bewegen Sie den Mauszeiger über die ID und klicken Sie darauf, um sie zu kopieren.

Laden Sie eine AutoSupport -Nachricht herunter oder senden Sie sie

Wenn bei Ihnen Probleme auftreten, werden Sie von NetApp möglicherweise aufgefordert, zur Fehlerbehebung eine AutoSupport -Nachricht an den NetApp -Support zu senden.

Aufgrund des Lastenausgleichs benötigt die NetApp Console bis zu fünf Stunden, um AutoSupport -Nachrichten zu senden. Laden Sie für dringende Mitteilungen die Datei herunter und senden Sie sie manuell.

Schritte

1. Wählen Sie **Administration > Support > Agenten**.
2. Wählen Sie je nachdem, wie Sie die Informationen an den NetApp Support senden müssen, eine der folgenden Optionen:
   a. Wählen Sie die Option zum Herunterladen der AutoSupport -Nachricht auf Ihren lokalen Computer. Sie können es dann mit einer bevorzugten Methode an den NetApp -Support senden.
   b. Wählen Sie * AutoSupport senden*, um die Nachricht direkt an den NetApp -Support zu senden.

Beheben von Downloadfehlern bei Verwendung eines Google Cloud NAT-Gateways

Der Konsolenagent lädt automatisch Softwareupdates für Cloud Volumes ONTAP herunter. Ihre Konfiguration kann dazu führen, dass der Download fehlschlägt, wenn ein Google Cloud NAT-Gateway verwendet wird. Sie können dieses Problem beheben, indem Sie die Anzahl der Teile begrenzen, in die das Software-Image unterteilt ist. Dieser Schritt muss mithilfe der API abgeschlossen werden.

Schritt

1. Senden Sie eine PUT-Anfrage an /occm/config mit dem folgenden JSON als Text:

```
{
  "maxDownloadSessions": 32
}
```

Der Wert für *maxDownloadSessions* kann 1 oder eine beliebige Ganzzahl größer als 1 sein. Wenn der Wert 1 ist, wird das heruntergeladene Bild nicht geteilt.

Beachten Sie, dass 32 ein Beispielwert ist. Der Wert hängt von Ihrer NAT-Konfiguration und der Anzahl gleichzeitiger Sitzungen ab.

"Erfahren Sie mehr über den API-Aufruf /occm/config"

Holen Sie sich Hilfe von der NetApp Knowledge Base

"Informationen zur Fehlerbehebung anzeigen, die vom NetApp Support-Team erstellt wurden" .

Deinstallieren und Entfernen eines Konsolenagenten

Deinstallieren Sie einen Konsolenagenten, um Probleme zu beheben oder ihn dauerhaft vom Host zu entfernen. Die erforderlichen Schritte hängen vom verwendeten Bereitstellungsmodus ab. Nachdem Sie einen Konsolenagenten aus Ihrer Umgebung entfernt haben, können Sie ihn aus der Konsole entfernen.

"Erfahren Sie mehr über die Bereitstellungsmodi der NetApp Console" .

Deinstallieren Sie den Agenten, wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden

Wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden (mit anderen Worten, der Agent-Host verfügt über eine ausgehende Konnektivität), sollten Sie die folgenden Schritte ausführen, um den Agenten zu deinstallieren.

Schritte

1. Stellen Sie eine Verbindung zur Linux-VM für den Agenten her.
2. Führen Sie vom Linux-Host aus das Deinstallationsskript aus:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   silent führt das Skript aus, ohne Sie zur Bestätigung aufzufordern.

Entfernen von Konsolenagenten aus der Konsole

Wenn Sie eine Agenten-VM gelöscht oder den Agenten deinstalliert haben, sollten Sie ihn aus der Liste der Agenten in der Konsole entfernen. Nach dem Löschen einer Agenten-VM oder der Deinstallation der Agentensoftware wird der Agent in der Konsole als **Getrennt** angezeigt.

Beachten Sie beim Entfernen eines Konsolenagenten Folgendes:

- Durch diese Aktion wird die virtuelle Maschine nicht gelöscht.
- Diese Aktion kann nicht rückgängig gemacht werden. Wenn Sie einen Konsolenagenten einmal entfernt haben, können Sie ihn nicht wieder hinzufügen.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Auf der Seite **Übersicht** wählen Sie das Aktionsmenü für einen getrennten Agenten und anschließend **Agent entfernen**.
3. Geben Sie zur Bestätigung den Namen des Agenten ein und wählen Sie dann **Entfernen**.

Cloud-Anbieter-Zugangsdaten verwalten

AWS

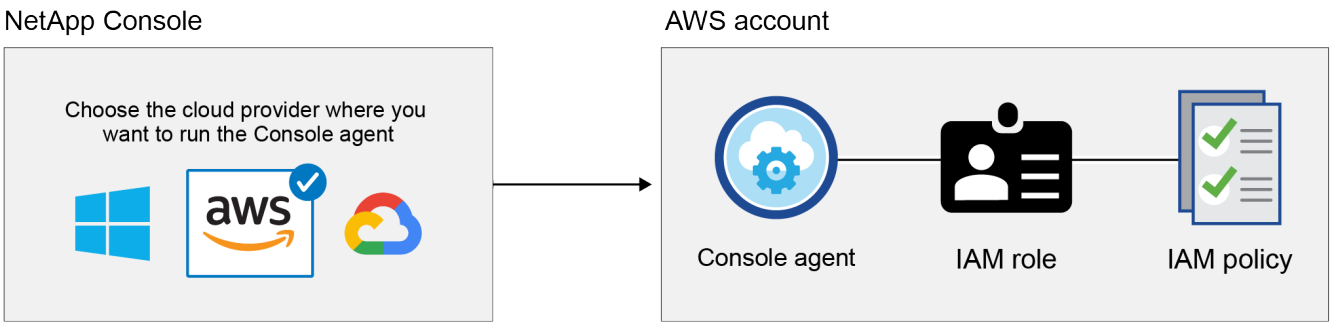
Erfahren Sie mehr über AWS-Anmeldeinformationen und Berechtigungen in der NetApp Console

Sie verwalten AWS-Zugangsdaten und Marketplace-Abonnements direkt über die NetApp Console , um eine sichere Bereitstellung von Cloud Volumes ONTAP und anderen Datendiensten zu gewährleisten, indem Sie während der Bereitstellung des Console-Agenten die entsprechenden IAM-Zugangsdaten angeben und diese zur Abrechnung mit AWS Marketplace-Abonnements verknüpfen.

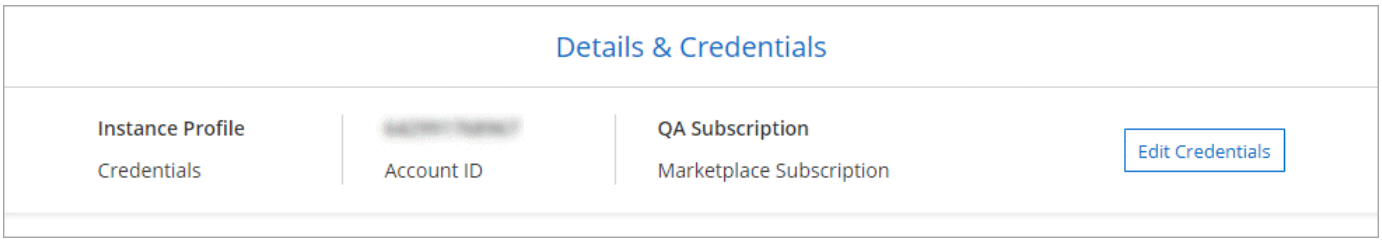
Anfängliche AWS-Anmeldeinformationen

Wenn Sie einen Konsolenagenten über die Konsole bereitstellen, müssen Sie die ARN einer IAM-Rolle oder Zugriffsschlüssel für einen IAM-Benutzer angeben. Die Authentifizierungsmethode muss über Berechtigungen zum Bereitstellen des Console-Agenten in AWS verfügen. Die erforderlichen Berechtigungen sind in der folgenden Liste aufgeführt:"Agentenbereitstellungsrichtlinie für AWS" Die

Wenn die Konsole den Konsolenagenten in AWS startet, erstellt sie eine IAM-Rolle und ein Profil für den Agenten. Außerdem wird eine Richtlinie angehängt, die dem Konsolenagenten die Berechtigung erteilt, Ressourcen und Prozesse innerhalb dieses AWS-Kontos zu verwalten. "Überprüfen Sie, wie der Agent die Berechtigungen verwendet".



Wenn Sie ein neues Cloud Volumes ONTAP -System hinzufügen, wählt die Konsole standardmäßig diese AWS-Anmeldeinformationen aus:



Stellen Sie alle Ihre Cloud Volumes ONTAP -Systeme mit den anfänglichen AWS-Anmeldeinformationen bereit, oder fügen Sie zusätzliche Anmeldeinformationen hinzu.

Zusätzliche AWS-Anmeldeinformationen

In den folgenden Fällen können Sie der Konsole zusätzliche AWS-Anmeldeinformationen hinzufügen:

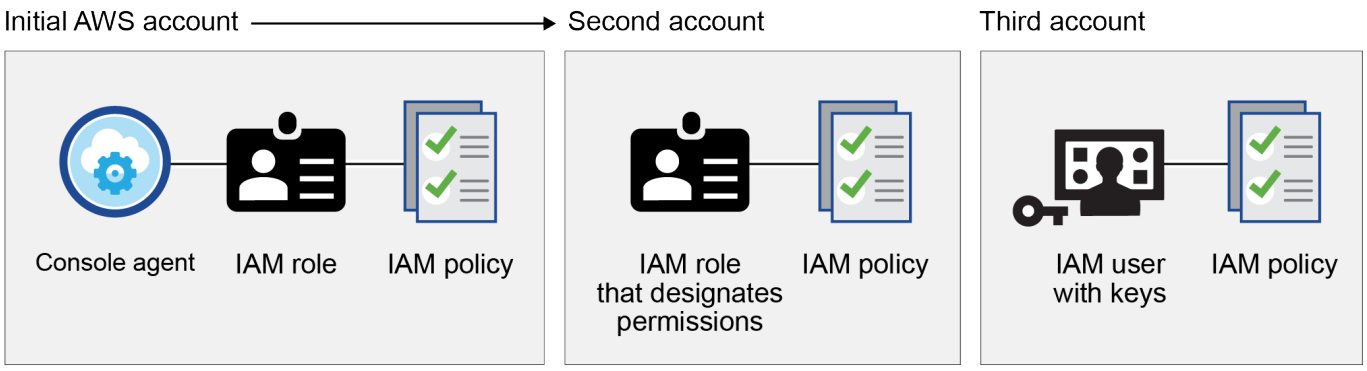
- Um Ihren bestehenden Console-Agenten mit einem zusätzlichen AWS-Konto zu verwenden
- So erstellen Sie einen neuen Agenten in einem bestimmten AWS-Konto

- So erstellen und verwalten Sie FSx for ONTAP Dateisysteme

Weitere Einzelheiten finden Sie in den folgenden Abschnitten.

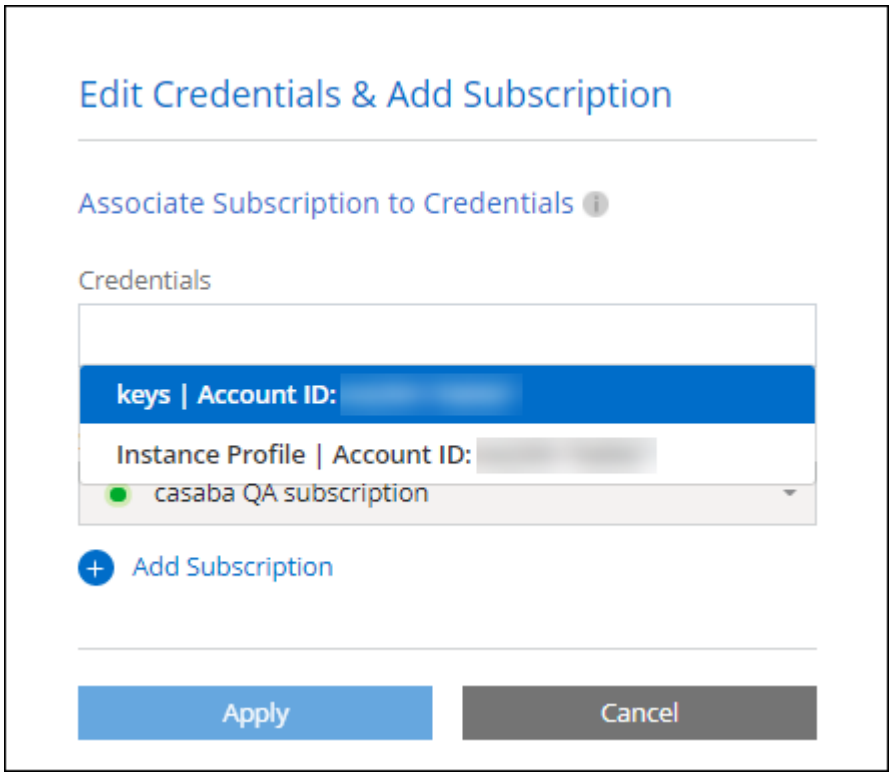
Fügen Sie AWS-Anmeldeinformationen hinzu, um einen Konsolenagenten mit einem anderen AWS-Konto zu verwenden

Um die Konsole mit zusätzlichen AWS-Konten zu verwenden, geben Sie AWS-Schlüssel oder den ARN einer Rolle in einem vertrauenswürdigen Konto an. Das folgende Bild zeigt zwei zusätzliche Konten, eines, das Berechtigungen über eine IAM-Rolle in einem vertrauenswürdigen Konto bereitstellt, und ein anderes über die AWS-Schlüssel eines IAM-Benutzers:



Sie fügen der Konsole Kontoanmeldeinformationen hinzu, indem Sie den Amazon Resource Name (ARN) der IAM-Rolle oder die AWS-Schlüssel für den IAM-Benutzer angeben.

Sie können beispielsweise beim Erstellen eines neuen Cloud Volumes ONTAP Systems zwischen Anmeldeinformationen wechseln:



"Erfahren Sie, wie Sie einem vorhandenen Agenten AWS-Anmeldeinformationen hinzufügen."

Fügen Sie AWS-Anmeldeinformationen hinzu, um einen Konsolenagenten zu erstellen

Durch das Hinzufügen von AWS-Anmeldeinformationen werden Berechtigungen zum Erstellen eines Konsolenagenten erteilt.

"Erfahren Sie, wie Sie der Konsole AWS-Anmeldeinformationen hinzufügen, um einen Konsolenagenten zu erstellen"

AWS-Anmeldeinformationen für FSx for ONTAP hinzufügen

Fügen Sie der Konsole AWS-Anmeldeinformationen hinzu, um die erforderlichen Berechtigungen zum Erstellen und Verwalten eines FSx for ONTAP Systems bereitzustellen.

"Erfahren Sie, wie Sie AWS-Anmeldeinformationen zur Konsole für Amazon FSx for ONTAP hinzufügen"

Anmeldeinformationen und Marktplatzabonnements

Sie müssen die Anmeldeinformationen, die Sie einem Console-Agenten hinzufügen, mit einem AWS Marketplace-Abonnement verknüpfen, um Cloud Volumes ONTAP auf Stundenbasis (PAYGO) und andere NetApp -Datendienste oder über einen Jahresvertrag zu bezahlen. "Erfahren Sie, wie Sie ein AWS-Abonnement zuordnen".

Beachten Sie Folgendes zu AWS-Anmeldeinformationen und Marktplatz-Abonnements:

- Sie können nur ein AWS Marketplace-Abonnement mit einem Satz AWS-Anmeldeinformationen verknüpfen
- Sie können ein bestehendes Marktplatz-Abonnement durch ein neues Abonnement ersetzen

FAQ

Die folgenden Fragen beziehen sich auf Anmeldeinformationen und Abonnements.

Wie kann ich meine AWS-Anmeldeinformationen sicher rotieren?

Wie in den obigen Abschnitten beschrieben, können Sie mit der Konsole AWS-Anmeldeinformationen auf verschiedene Weise bereitstellen: über eine mit dem Konsolenagenten verknüpfte IAM-Rolle, durch die Übernahme einer IAM-Rolle in einem vertrauenswürdigen Konto oder durch die Bereitstellung von AWS-Zugriffsschlüsseln.

Bei den ersten beiden Optionen verwendet die Konsole den AWS Security Token Service, um temporäre Anmeldeinformationen zu erhalten, die ständig rotieren. Dieses Verfahren ist die beste Vorgehensweise – es ist automatisch und sicher.

Wenn Sie der Konsole AWS-Zugriffsschlüssel bereitstellen, sollten Sie die Schlüssel rotieren, indem Sie sie in regelmäßigen Abständen in der Konsole aktualisieren. Dies ist ein vollständig manueller Prozess.

Kann ich das AWS Marketplace-Abonnement für Cloud Volumes ONTAP Systeme ändern?

Ja, das können Sie. Wenn Sie das AWS Marketplace-Abonnement ändern, das mit einem Satz Anmeldeinformationen verknüpft ist, werden alle vorhandenen und neuen Cloud Volumes ONTAP Systeme über das neue Abonnement abgerechnet.

"Erfahren Sie, wie Sie ein AWS-Abonnement zuordnen" .

Kann ich mehrere AWS-Anmeldeinformationen mit jeweils unterschiedlichen Marktplatz-Abonnements hinzufügen?

Alle AWS-Anmeldeinformationen, die zum selben AWS-Konto gehören, werden mit demselben AWS Marketplace-Abonnement verknüpft.

Wenn Sie über mehrere AWS-Anmeldeinformationen verfügen, die zu verschiedenen AWS-Konten gehören, können diese Anmeldeinformationen mit demselben AWS Marketplace-Abonnement oder mit verschiedenen Abonnements verknüpft sein.

Kann ich vorhandene Cloud Volumes ONTAP Systeme auf ein anderes AWS-Konto verschieben?

Nein, es ist nicht möglich, die mit Ihrem Cloud Volumes ONTAP -System verknüpften AWS-Ressourcen auf ein anderes AWS-Konto zu verschieben.

Wie funktionieren Anmeldeinformationen für Marktplatzbereitstellungen und lokale Bereitstellungen?

In den obigen Abschnitten wird die empfohlene Bereitstellungsmethode für den Konsolenagenten beschrieben, die von der Konsole aus erfolgt. Sie können auch einen Agenten in AWS über den AWS Marketplace bereitstellen und die Console-Agent-Software manuell auf Ihrem eigenen Linux-Host oder in Ihrem VCenter installieren.

Wenn Sie den Marketplace verwenden, werden die Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die IAM-Rolle manuell erstellen und einrichten und dann Berechtigungen für alle zusätzlichen Konten erteilen.

Bei lokalen Bereitstellungen können Sie keine IAM-Rolle für die Konsole einrichten, aber Sie können Berechtigungen mithilfe von AWS-Zugriffsschlüsseln erteilen.

Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

- Standardmodus
  - "Einrichten von Berechtigungen für eine AWS Marketplace-Bereitstellung"
  - "Einrichten von Berechtigungen für lokale Bereitstellungen"
- Eingeschränkter Modus
  - "Berechtigungen für den eingeschränkten Modus einrichten"

Verwalten Sie AWS-Anmeldeinformationen und Marktplatz-Abonnements für die NetApp Console

Fügen Sie AWS-Anmeldeinformationen hinzu und verwalten Sie diese, damit Sie Cloud-Ressourcen in Ihren AWS-Konten über die NetApp Console bereitstellen und verwalten können. Wenn Sie mehrere AWS Marketplace-Abonnements verwalten, können Sie jedem Abonnement auf der Seite „Anmeldeinformationen“ unterschiedliche AWS-Anmeldeinformationen zuweisen.

Überblick

Sie können AWS-Anmeldeinformationen zu einem vorhandenen Konsolenagenten oder direkt zur Konsole hinzufügen:

- Fügen Sie einem vorhandenen Agenten zusätzliche AWS-Anmeldeinformationen hinzu

Fügen Sie einem Konsolenagenten AWS-Anmeldeinformationen hinzu, um Cloud-Ressourcen zu verwalten. Erfahren Sie, wie Sie einem Konsolenagenten AWS-Anmeldeinformationen hinzufügen .

- Fügen Sie der Konsole AWS-Anmeldeinformationen hinzu, um einen Konsolenagenten zu erstellen

  Durch das Hinzufügen neuer AWS-Anmeldeinformationen zur Konsole erhalten Sie die erforderlichen Berechtigungen zum Erstellen eines Konsolenagenten. Erfahren Sie, wie Sie AWS-Anmeldeinformationen zur NetApp Console hinzufügen .

- AWS-Anmeldeinformationen zur Konsole für FSx for ONTAP hinzufügen

  Fügen Sie der Konsole neue AWS-Anmeldeinformationen hinzu, um FSx für ONTAP zu erstellen und zu verwalten. "Erfahren Sie, wie Sie Berechtigungen für FSx für ONTAP einrichten"

So rotieren Sie Anmeldeinformationen

Mit der NetApp Console können Sie AWS-Anmeldeinformationen auf verschiedene Weise bereitstellen: über eine mit der Agenteninstanz verknüpfte IAM-Rolle, durch die Übernahme einer IAM-Rolle in einem vertrauenswürdigen Konto oder durch die Bereitstellung von AWS-Zugriffsschlüsseln. "Erfahren Sie mehr über AWS-Anmeldeinformationen und -Berechtigungen" .

Bei den ersten beiden Optionen verwendet die Konsole den AWS Security Token Service, um temporäre Anmeldeinformationen zu erhalten, die ständig rotieren. Dieser Vorgang ist die beste Vorgehensweise, da er automatisch und sicher ist.

Rotieren Sie AWS-Zugriffsschlüssel manuell, indem Sie sie in der Konsole aktualisieren.

Hinzufügen zusätzlicher Anmeldeinformationen zu einem Konsolenagenten

Fügen Sie einem Konsolenagenten zusätzliche AWS-Anmeldeinformationen hinzu, damit er über die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen in Ihrer öffentlichen Cloud-Umgebung verfügt. Sie können entweder die ARN einer IAM-Rolle in einem anderen Konto angeben oder AWS-Zugriffsschlüssel bereitstellen.

"Erfahren Sie, wie die NetApp Console AWS-Anmeldeinformationen und -Berechtigungen verwendet".

Berechtigungen erteilen

Erteilen Sie Berechtigungen, bevor Sie einem Konsolenagenten AWS-Anmeldeinformationen hinzufügen. Die Berechtigungen ermöglichen einem Konsolenagenten, Ressourcen und Prozesse innerhalb dieses AWS-Kontos zu verwalten. Sie können die Berechtigungen mit der ARN einer Rolle in einem vertrauenswürdigen Konto oder mit AWS-Schlüsseln bereitstellen.

> Wenn Sie einen Konsolenagenten über die Konsole bereitgestellt haben, wurden automatisch AWS-Anmeldeinformationen für das Konto hinzugefügt, in dem Sie einen Konsolenagenten bereitgestellt haben. Dadurch wird sichergestellt, dass die erforderlichen Berechtigungen zum Verwalten von Ressourcen vorhanden sind.

Auswahl

- indem Sie eine IAM-Rolle in einem anderen Konto übernehmen
- Erteilen Sie Berechtigungen durch die Bereitstellung von AWS-Schlüsseln

Erteilen Sie Berechtigungen, indem Sie eine IAM-Rolle in einem anderen Konto übernehmen

Sie können mithilfe von IAM-Rollen eine Vertrauensbeziehung zwischen dem AWS-Quellkonto, in dem Sie einen Konsolenagenten bereitgestellt haben, und anderen AWS-Konten einrichten. Anschließend stellen Sie der Konsole die ARN der IAM-Rollen der vertrauenswürdigen Konten zur Verfügung.

Wenn ein Konsolenagent vor Ort installiert ist, können Sie diese Authentifizierungsmethode nicht verwenden. Sie müssen AWS-Schlüssel verwenden.

Schritte

1. Gehen Sie zur IAM-Konsole im Zielkonto, in dem Sie einem Konsolenagenten Berechtigungen erteilen möchten.
2. Wählen Sie unter „Zugriffsverwaltung“ **Rollen > Rolle erstellen** und befolgen Sie die Schritte zum Erstellen der Rolle.

   Stellen Sie sicher, dass Sie Folgendes tun:

   - Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
   - Wählen Sie **Ein anderes AWS-Konto** und geben Sie die ID des Kontos ein, in dem sich eine Konsolen-Agent-Instanz befindet.
   - Erstellen Sie die erforderlichen Richtlinien, indem Sie den Inhalt von kopieren und einfügen"die IAM-Richtlinien für einen Konsolenagenten" .
3. Kopieren Sie die Rollen-ARN der IAM-Rolle, damit Sie sie später in die Konsole einfügen können.

Ergebnis

Das Konto verfügt über die erforderlichen Berechtigungen. Sie können jetzt die Anmeldeinformationen zu einem Konsolenagenten hinzufügen .

Erteilen Sie Berechtigungen durch die Bereitstellung von AWS-Schlüsseln

Wenn Sie der Konsole AWS-Schlüssel für einen IAM-Benutzer bereitstellen möchten, müssen Sie diesem Benutzer die erforderlichen Berechtigungen erteilen. Die IAM-Richtlinie der Konsole definiert die AWS-Aktionen und -Ressourcen, die die Konsole verwenden darf.

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

Schritte

1. Erstellen Sie in der IAM-Konsole Richtlinien, indem Sie den Inhalt von"die IAM-Richtlinien für einen Konsolenagenten" .

   "AWS-Dokumentation: Erstellen von IAM-Richtlinien"
2. Ordnen Sie die Richtlinien einer IAM-Rolle oder einem IAM-Benutzer zu.
   - "AWS-Dokumentation: Erstellen von IAM-Rollen"
   - "AWS-Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"

Fügen Sie die Anmeldeinformationen zu einem vorhandenen Agenten hinzu

Nachdem Sie ein AWS-Konto mit den erforderlichen Berechtigungen versehen haben, können Sie die Anmeldeinformationen für dieses Konto einem vorhandenen Agenten hinzufügen. Dadurch können Sie Cloud Volumes ONTAP -Systeme in diesem Konto mit demselben Agenten starten.

Es kann einige Minuten dauern, bis neue Anmeldeinformationen bei Ihrem Cloud-Anbieter verfügbar sind.

Schritte

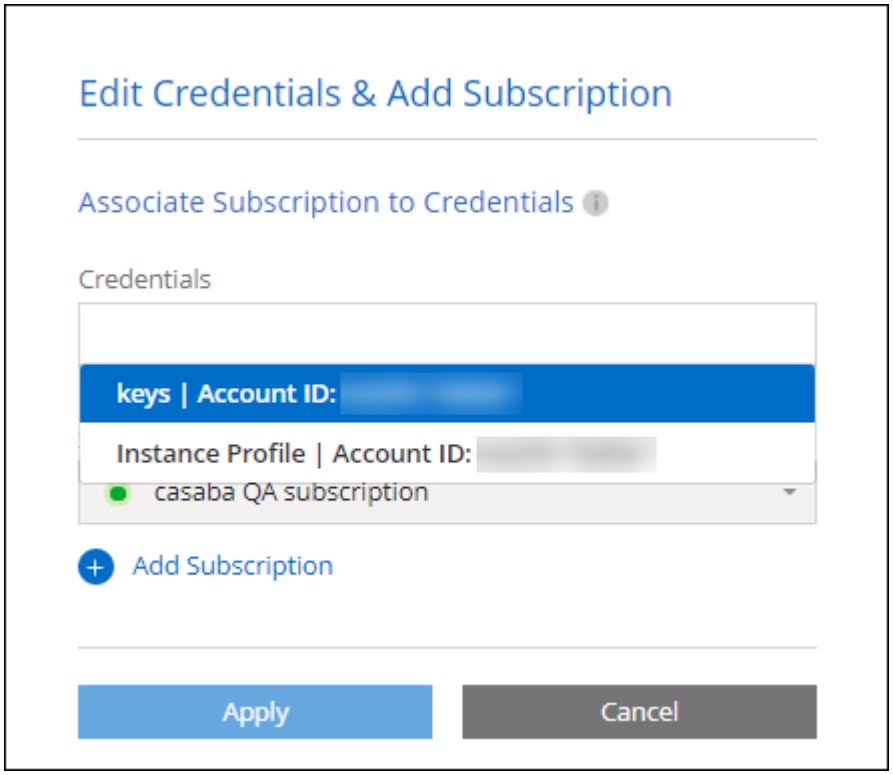
1. Wählen Sie über die obere Navigationsleiste einen Konsolenagenten aus, dem Sie Anmeldeinformationen hinzufügen möchten.
2. Wählen Sie in der linken Navigationsleiste **Administration > Anmeldeinformationen** aus.
3. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** die Option **Anmeldeinformationen hinzufügen** aus und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Amazon Web Services > Agent**.
   b. **Anmeldeinformationen definieren**: Geben Sie den ARN (Amazon Resource Name) einer vertrauenswürdigen IAM-Rolle an oder 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.

      Um Dienste mit einem Stundensatz (PAYGO) oder mit einem Jahresvertrag zu bezahlen, müssen Sie AWS-Anmeldeinformationen mit Ihrem AWS Marketplace-Abonnement verknüpfen.

   d. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Ergebnis

Sie können jetzt auf der Seite „Details und Anmeldeinformationen“ zu einem anderen Satz von Anmeldeinformationen wechseln, wenn Sie der Konsole ein Abonnement hinzufügen.



Fügen Sie der Konsole Anmeldeinformationen zum Erstellen eines Konsolenagenten hinzu

Fügen Sie AWS-Anmeldeinformationen hinzu, indem Sie die ARN einer IAM-Rolle angeben, die die zum Erstellen eines Konsolenagenten erforderlichen Berechtigungen erteilt. Sie können diese Anmeldeinformationen beim Erstellen eines neuen Agenten auswählen.

Einrichten der IAM-Rolle

Richten Sie eine IAM-Rolle ein, die es der NetApp Console -Software als Serviceebene (SaaS) ermöglicht, die Rolle zu übernehmen.

Schritte

1. Gehen Sie zur IAM-Konsole im Zielkonto.
2. Wählen Sie unter „Zugriffsverwaltung“ **Rollen > Rolle erstellen** und befolgen Sie die Schritte zum Erstellen der Rolle.

   Stellen Sie sicher, dass Sie Folgendes tun:

   - Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
   - Wählen Sie **Ein anderes AWS-Konto** und geben Sie die ID der NetApp Console SaaS ein: 952013314444
   - Bearbeiten Sie speziell für Amazon FSx for NetApp ONTAP die Richtlinie **Vertrauensbeziehungen**, um "AWS": "arn:aws:iam::952013314444:root" einzuschließen.

     Die Richtlinie sollte beispielsweise folgendermaßen aussehen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+
Siehe "AWS Identity and Access Management (IAM)-Dokumentation" für weitere Informationen zum kontoübergreifenden Ressourcenzugriff in IAM.

   - Erstellen Sie eine Richtlinie, die die zum Erstellen eines Konsolenagenten erforderlichen Berechtigungen enthält.
     - "Anzeigen der für FSx for ONTAP erforderlichen Berechtigungen"
     - "Anzeigen der Agent-Bereitstellungsrichtlinie"

3. Kopieren Sie die Rollen-ARN der IAM-Rolle, damit Sie sie im nächsten Schritt in die Konsole einfügen können.

Ergebnis

Die IAM-Rolle verfügt jetzt über die erforderlichen Berechtigungen. Sie können es jetzt zur Konsole hinzufügen.

Fügen Sie die Anmeldeinformationen hinzu

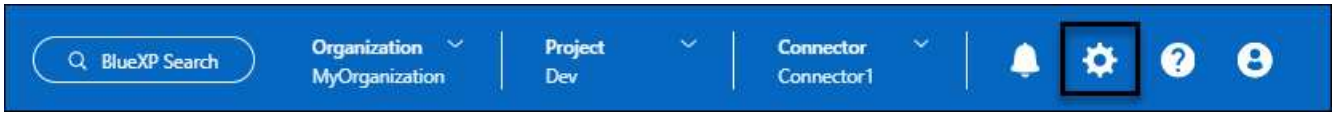
Nachdem Sie die IAM-Rolle mit den erforderlichen Berechtigungen ausgestattet haben, fügen Sie die Rollen-ARN zur Konsole hinzu.

Bevor Sie beginnen

Wenn Sie die IAM-Rolle gerade erst erstellt haben, kann es einige Minuten dauern, bis sie zur Verwendung verfügbar ist. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zur Konsole hinzufügen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.



2. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** die Option **Anmeldeinformationen hinzufügen** aus und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Amazon Web Services > Konsole**.
   b. **Anmeldeinformationen definieren**: Geben Sie den ARN (Amazon Resource Name) der IAM-Rolle an.
   c. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Anmeldeinformationen zur Konsole für Amazon FSx for ONTAP hinzufügen

Einzelheiten finden Sie im "die Konsolendokumentation für Amazon FSx for ONTAP"

Konfigurieren eines AWS-Abonnements

Nachdem Sie Ihre AWS-Anmeldeinformationen hinzugefügt haben, können Sie mit diesen Anmeldeinformationen ein AWS Marketplace-Abonnement konfigurieren. Mit dem Abonnement können Sie NetApp Datendienste und Cloud Volumes ONTAP auf Stundenbasis (PAYGO) oder über einen Jahresvertrag bezahlen.

Es gibt zwei Szenarien, in denen Sie ein AWS Marketplace-Abonnement konfigurieren können, nachdem Sie die Anmeldeinformationen bereits hinzugefügt haben:

- Sie haben beim ersten Hinzufügen der Anmeldeinformationen kein Abonnement konfiguriert.
- Sie möchten das AWS Marketplace-Abonnement ändern, das für die AWS-Anmeldeinformationen konfiguriert ist.

  Durch das Ersetzen des aktuellen Marktplatzabonnements durch ein neues Abonnement wird das Marktplatzabonnement für alle vorhandenen Cloud Volumes ONTAP Systeme und alle neuen Systeme geändert.

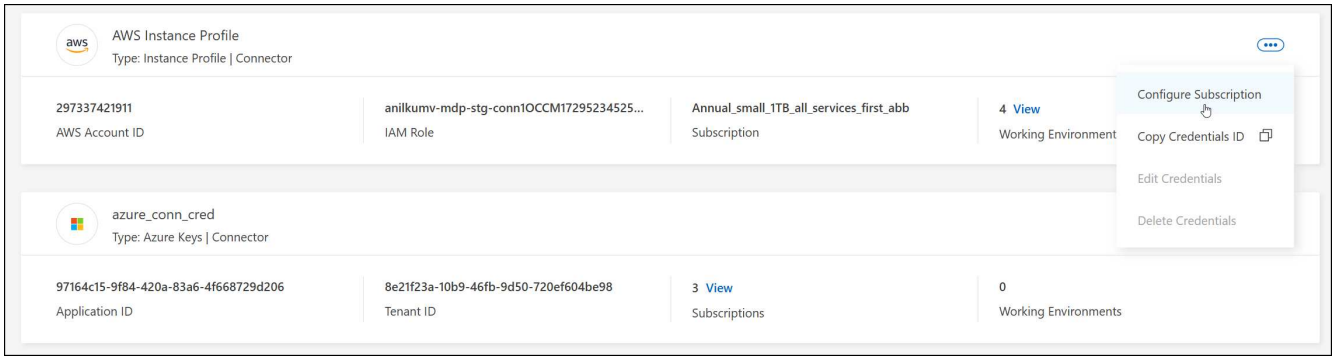
Bevor Sie beginnen

Sie müssen einen Konsolenagenten erstellen, bevor Sie ein Abonnement konfigurieren können. "Erfahren Sie, wie Sie einen Konsolenagenten erstellen" .

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**.

Verknüpfen Sie ein vorhandenes Abonnement mit Ihrer Organisation

Wenn Sie sich beim AWS Marketplace anmelden, besteht der letzte Schritt im Prozess darin, das Abonnement Ihrer Organisation zuzuordnen. Wenn Sie diesen Schritt nicht abgeschlossen haben, können Sie das Abonnement nicht mit Ihrer Organisation verwenden.

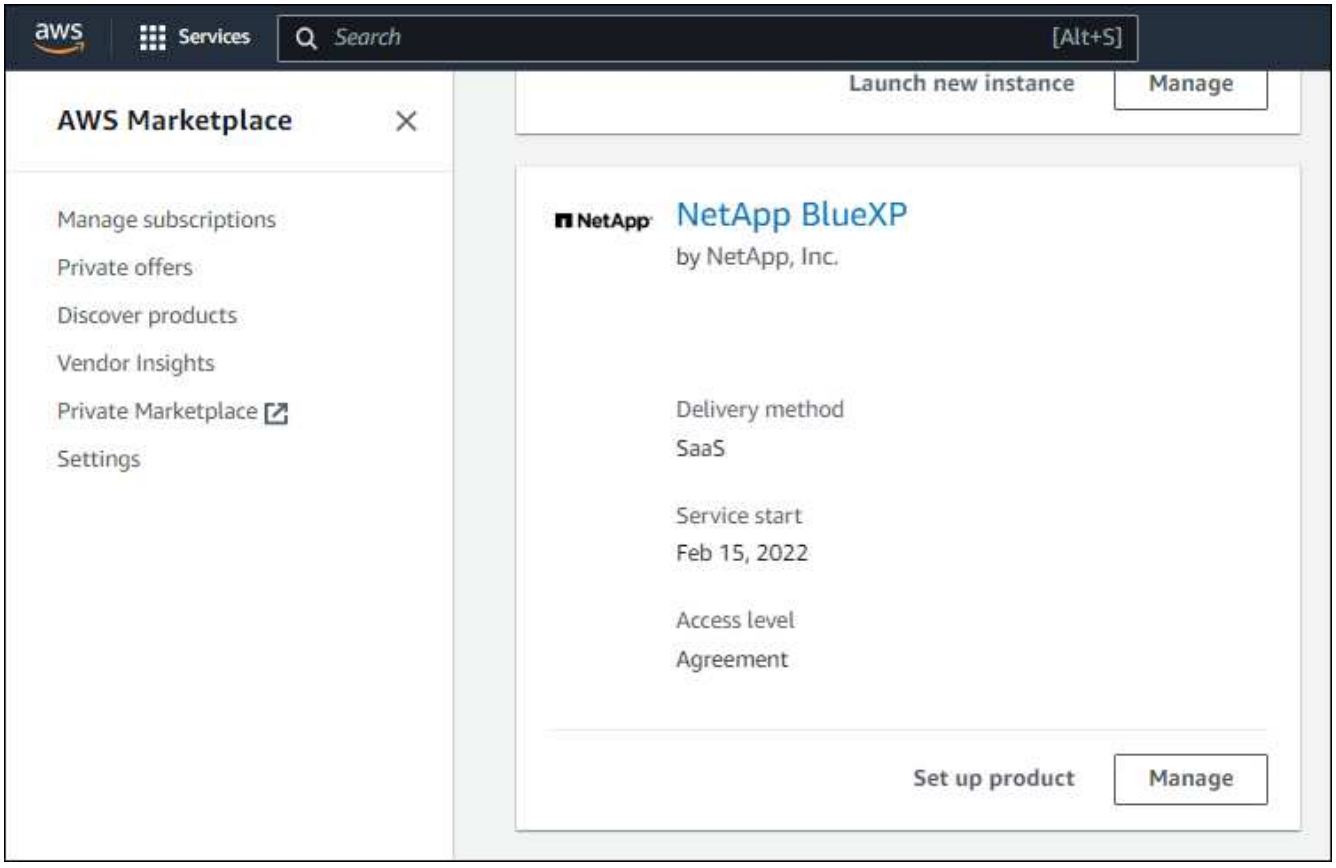
- "Erfahren Sie mehr über die Bereitstellungsmodi der Konsole"
- "Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der Konsole"

Führen Sie die folgenden Schritte aus, wenn Sie NetApp Intelligent Services vom AWS Marketplace abonniert haben, aber den Schritt zum Verknüpfen des Abonnements mit Ihrem Konto verpasst haben.

Schritte

1. Bestätigen Sie, dass Sie Ihr Abonnement nicht mit Ihrer Konsolenorganisation verknüpft haben.
   a. Wählen Sie im Navigationsmenü **Verwaltung > Licenses and subscriptions**.
   b. Wählen Sie **Abonnements** aus.
   c. Stellen Sie sicher, dass Ihr Abonnement nicht angezeigt wird.

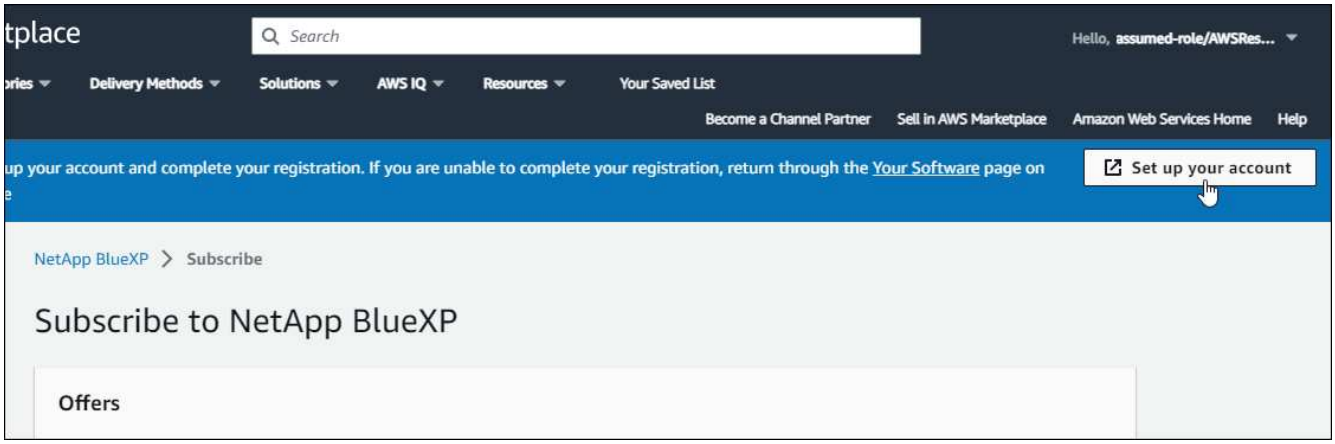
      Sie sehen nur die Abonnements, die mit der Organisation oder dem Konto verknüpft sind, das Sie gerade anzeigen. Wenn Ihr Abonnement nicht angezeigt wird, fahren Sie mit den folgenden Schritten fort.
2. Melden Sie sich bei der AWS-Konsole an und navigieren Sie zu **AWS Marketplace-Abonnements**.
3. Suchen Sie das Abonnement.



4. Wählen Sie **Produkt einrichten**.

   Die Abonnementangebotsseite sollte in einem neuen Browser-Tab oder -Fenster geladen werden.

5. Wählen Sie **Konto einrichten**.



   Die Seite **Abonnementzuweisung** auf netapp.com sollte in einem neuen Browser-Tab oder -Fenster geladen werden.

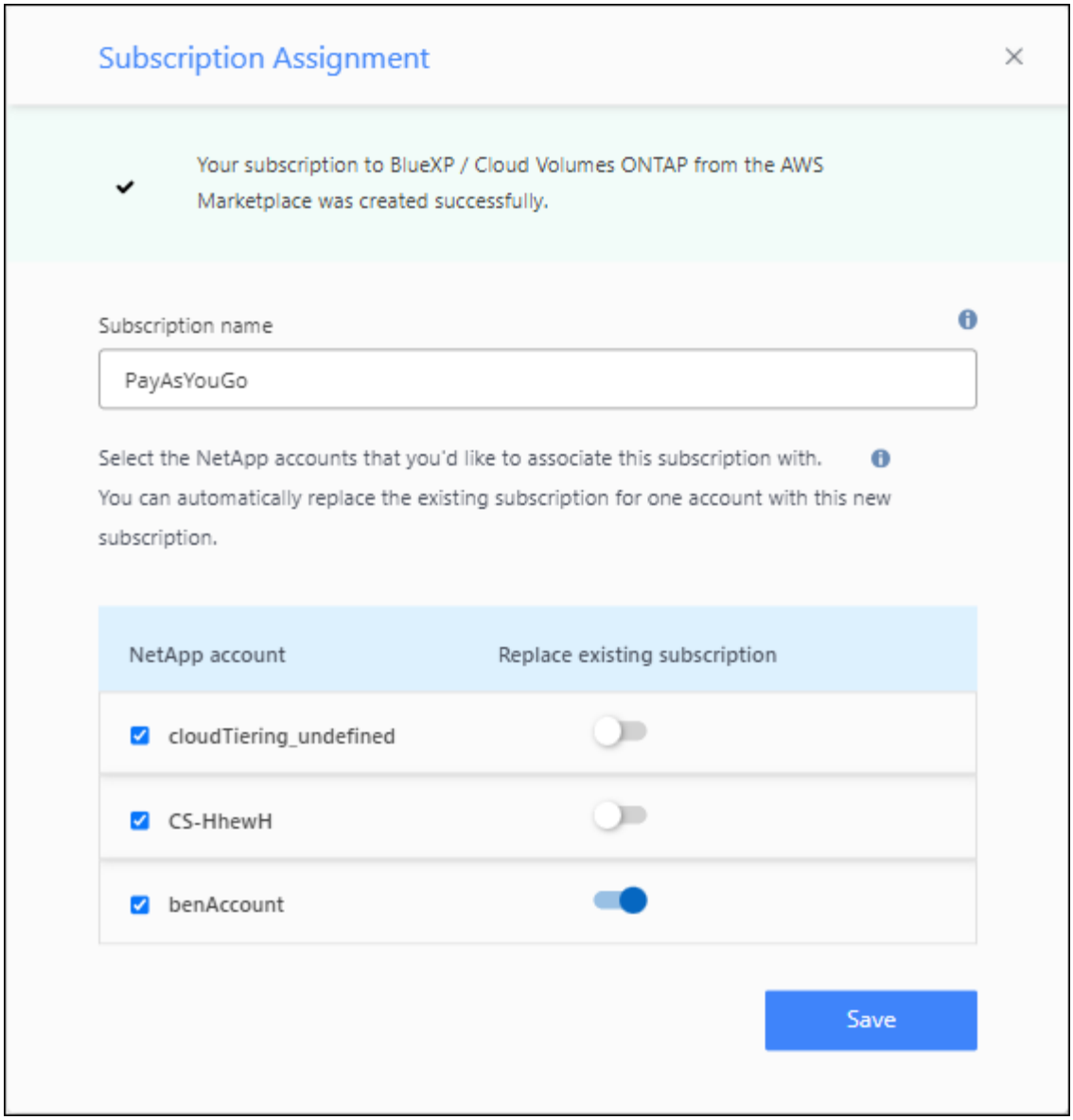
   Beachten Sie, dass Sie möglicherweise zuerst aufgefordert werden, sich bei der Konsole anzumelden.

6. 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.

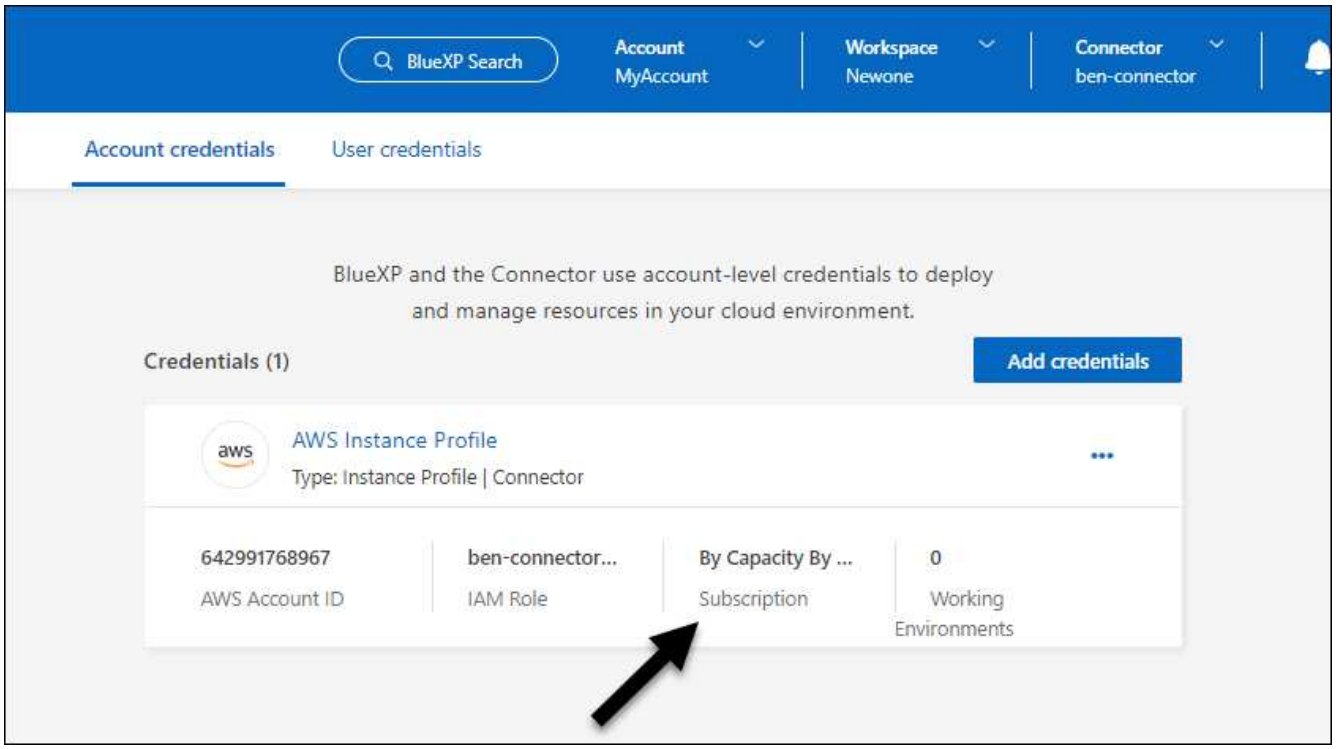
     Die Konsole ersetzt das vorhandene Abonnement für alle Anmeldeinformationen in der Organisation oder im Konto durch dieses neue Abonnement. Wenn ein Satz von Anmeldeinformationen nie mit einem Abonnement verknüpft war, wird dieses neue Abonnement nicht mit diesen Anmeldeinformationen verknüpft.

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



7. Bestätigen Sie, dass das Abonnement mit Ihrer Organisation verknüpft ist.
   a. Wählen Sie im Navigationsmenü **Administration > Lizenzen und Abonnements**.
   b. Wählen Sie **Abonnements** aus.
   c. Überprüfen Sie, ob Ihr Abonnement angezeigt wird.
8. Bestätigen Sie, dass das Abonnement mit Ihren AWS-Anmeldeinformationen verknüpft ist.
   a. Wählen Sie **Administration > Anmeldeinformationen**.
   b. Überprüfen Sie auf der Seite **Anmeldeinformationen der Organisation**, ob das Abonnement mit Ihren AWS-Anmeldeinformationen verknüpft ist.

      Hier ist ein Beispiel.



Anmeldeinformationen bearbeiten

Bearbeiten Sie Ihre AWS-Anmeldeinformationen, indem Sie den Kontotyp ändern (AWS-Schlüssel oder Rolle übernehmen), den Namen bearbeiten oder die Anmeldeinformationen selbst aktualisieren (die Schlüssel oder die Rollen-ARN).

Sie können die Anmeldeinformationen für ein Instanzprofil, das mit einer Konsolen-Agent-Instanz oder einer Amazon FSx for ONTAP -Instanz verknüpft ist, nicht bearbeiten. Sie können die Anmeldeinformationen nur für eine FSx for ONTAP Instanz umbenennen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Anmeldeinformationen bearbeiten**.
3. Nehmen Sie die erforderlichen Änderungen vor und wählen Sie dann **Übernehmen**.

Anmeldeinformationen löschen

Wenn Sie einen Satz Anmeldeinformationen nicht mehr benötigen, können Sie ihn löschen. Sie können nur Anmeldeinformationen löschen, die keinem System zugeordnet sind.

Sie können die Anmeldeinformationen für ein Instanzprofil, das einem Konsolenagenten zugeordnet ist, nicht löschen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** oder **Anmeldeinformationen des Kontos** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Anmeldeinformationen löschen**.

3. Wählen Sie zur Bestätigung **Löschen**.

Azurblau

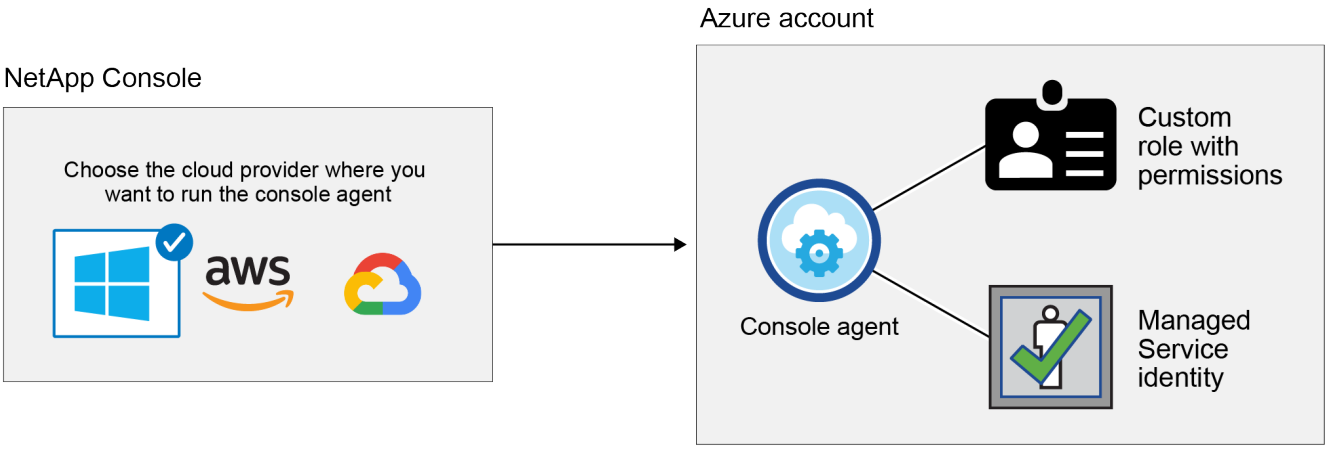
Erfahren Sie mehr über Azure-Anmeldeinformationen und Berechtigungen in der NetApp Console

Erfahren Sie, wie die NetApp Console Azure-Anmeldeinformationen verwendet, um Aktionen in Ihrem Namen auszuführen, und wie diese Anmeldeinformationen mit Marktplatzabonnements verknüpft werden. Das Verständnis dieser Details kann hilfreich sein, wenn Sie die Anmeldeinformationen für ein oder mehrere Azure-Abonnements verwalten. Sie möchten beispielsweise wissen, wann Sie der Konsole zusätzliche Azure-Anmeldeinformationen hinzufügen müssen.

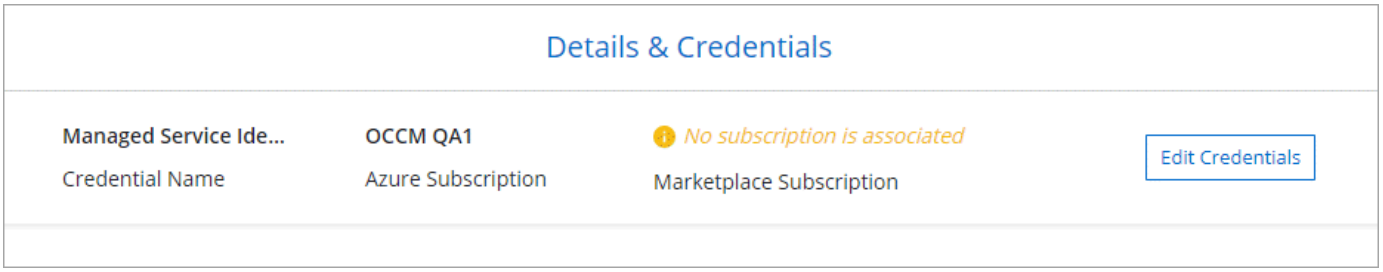
Anfängliche Azure-Anmeldeinformationen

Wenn Sie einen Konsolen-Agenten über die Konsole bereitstellen, müssen Sie ein Azure-Konto oder einen Dienstprinzipal verwenden, der über die Berechtigung zum Bereitstellen der virtuellen Maschine des Konsolen-Agenten verfügt. Die erforderlichen Berechtigungen sind in der"Agent-Bereitstellungsrichtlinie für Azure" .

Wenn die Konsole die virtuelle Maschine des Konsolen-Agenten in Azure bereitstellt, ermöglicht sie eine "systemseitig zugewiesene verwaltete Identität" auf der virtuellen Maschine, erstellt eine benutzerdefinierte Rolle und weist sie der virtuellen Maschine zu. Die Rolle stellt der Konsole die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen innerhalb dieses Azure-Abonnements zur Verfügung. "Überprüfen Sie, wie die Konsole die Berechtigungen verwendet" .



Wenn Sie ein neues System für Cloud Volumes ONTAP erstellen, wählt die Konsole standardmäßig diese Azure-Anmeldeinformationen aus:



Sie können alle Ihre Cloud Volumes ONTAP -Systeme mit den anfänglichen Azure-Anmeldeinformationen

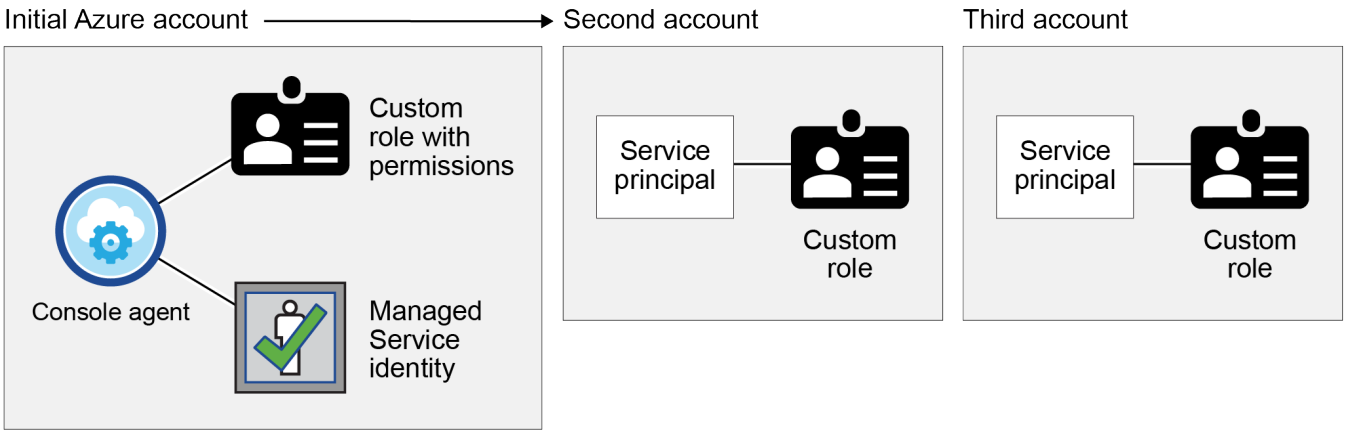
bereitstellen oder zusätzliche Anmeldeinformationen hinzufügen.

Zusätzliche Azure-Abonnements für eine verwaltete Identität

Die der Konsolen-Agent-VM zugewiesene, systemseitig verwaltete Identität ist dem Abonnement zugeordnet, in dem Sie den Konsolen-Agent gestartet haben. Wenn Sie ein anderes Azure-Abonnement auswählen möchten, müssen Sie"Verknüpfen Sie die verwaltete Identität mit diesen Abonnements" .

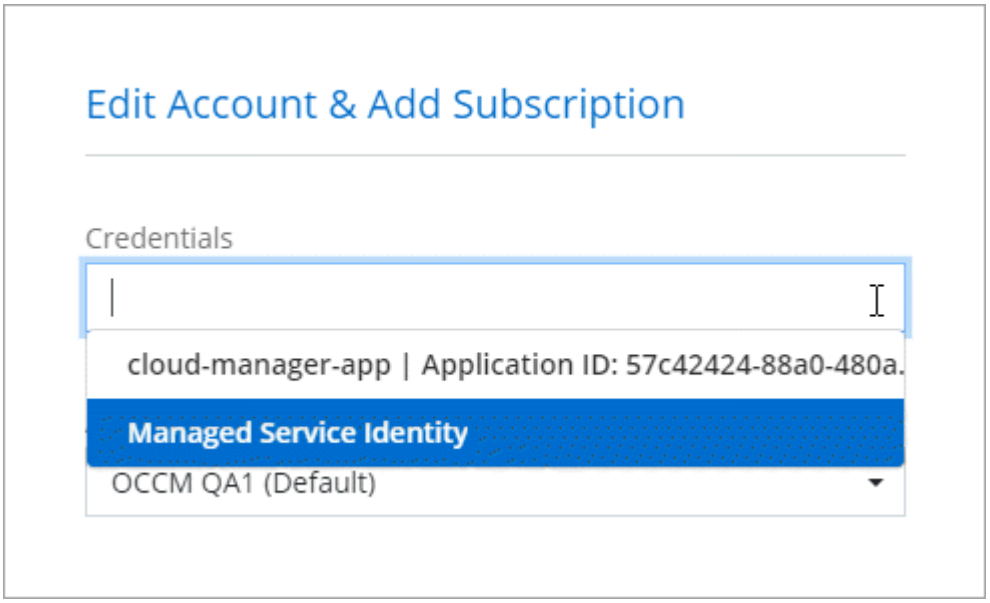
Zusätzliche Azure-Anmeldeinformationen

Wenn Sie andere Azure-Anmeldeinformationen mit der Konsole verwenden möchten, müssen Sie die erforderlichen Berechtigungen erteilen, indem Sie"Erstellen und Einrichten eines Dienstprinzipals in Microsoft Entra ID" für jedes Azure-Konto. Das folgende Bild zeigt zwei weitere Konten, die jeweils mit einem Dienstprinzipal und einer benutzerdefinierten Rolle eingerichtet sind, die Berechtigungen bereitstellt:



Sie würden dann"Fügen Sie die Kontoanmeldeinformationen zur Konsole hinzu" indem Sie Details zum AD-Dienstprinzipal angeben.

Sie können beispielsweise beim Erstellen eines neuen Cloud Volumes ONTAP Systems zwischen Anmeldeinformationen wechseln:



Anmeldeinformationen und Marktplatzabonnements

Die Anmeldeinformationen, die Sie einem Konsolenagenten hinzufügen, müssen mit einem Azure Marketplace-Abonnement verknüpft sein, damit Sie für Cloud Volumes ONTAP einen Stundensatz (PAYGO), NetApp -Datendienste oder einen Jahresvertrag bezahlen können.

"Erfahren Sie, wie Sie ein Azure-Abonnement zuordnen" .

Beachten Sie Folgendes zu Azure-Anmeldeinformationen und Marketplace-Abonnements:

- Sie können einem Satz Azure-Anmeldeinformationen nur ein Azure Marketplace-Abonnement zuordnen.
- Sie können ein bestehendes Marktplatz-Abonnement durch ein neues Abonnement ersetzen

FAQ

Die folgende Frage bezieht sich auf Anmeldeinformationen und Abonnements.

Kann ich das Azure Marketplace-Abonnement für Cloud Volumes ONTAP Systeme ändern?

Ja, das können Sie. Wenn Sie das Azure Marketplace-Abonnement ändern, das mit einem Satz Azure-Anmeldeinformationen verknüpft ist, werden alle vorhandenen und neuen Cloud Volumes ONTAP Systeme über das neue Abonnement abgerechnet.

"Erfahren Sie, wie Sie ein Azure-Abonnement zuordnen" .

Kann ich mehrere Azure-Anmeldeinformationen mit jeweils unterschiedlichen Marktplatzabonnements hinzufügen?

Alle Azure-Anmeldeinformationen, die zum selben Azure-Abonnement gehören, werden mit demselben Azure Marketplace-Abonnement verknüpft.

Wenn Sie über mehrere Azure-Anmeldeinformationen verfügen, die zu verschiedenen Azure-Abonnements gehören, können diese Anmeldeinformationen demselben Azure Marketplace-Abonnement oder verschiedenen Marketplace-Abonnements zugeordnet werden.

Kann ich vorhandene Cloud Volumes ONTAP Systeme in ein anderes Azure-Abonnement verschieben?

Nein, es ist nicht möglich, die mit Ihrem Cloud Volumes ONTAP -System verknüpften Azure-Ressourcen in ein anderes Azure-Abonnement zu verschieben.

Wie funktionieren Anmeldeinformationen für Marktplatzbereitstellungen und lokale Bereitstellungen?

In den obigen Abschnitten wird die empfohlene Bereitstellungsmethode für den Konsolenagenten beschrieben, die von der Konsole aus erfolgt. Sie können auch einen Konsolen-Agenten in Azure vom Azure Marketplace bereitstellen und die Konsolen-Agenten-Software auf Ihrem eigenen Linux-Host installieren.

Wenn Sie den Marketplace verwenden, können Sie Berechtigungen erteilen, indem Sie der Konsolen-Agent-VM und einer systemseitig zugewiesenen verwalteten Identität eine benutzerdefinierte Rolle zuweisen, oder Sie können einen Microsoft Entra-Dienstprinzipal verwenden.

Bei lokalen Bereitstellungen können Sie keine verwaltete Identität für den Konsolen-Agent einrichten, Sie können jedoch mithilfe eines Dienstprinzipals Berechtigungen erteilen.

Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

- Standardmodus
  - "Einrichten von Berechtigungen für eine Azure Marketplace-Bereitstellung"
  - "Einrichten von Berechtigungen für lokale Bereitstellungen"
- Eingeschränkter Modus
  - "Berechtigungen für den eingeschränkten Modus einrichten"

Verwalten Sie Azure-Anmeldeinformationen und Marketplace-Abonnements für die NetApp Console

Fügen Sie Azure-Anmeldeinformationen hinzu und verwalten Sie diese, damit die NetApp Console über die erforderlichen Berechtigungen zum Bereitstellen und Verwalten von Cloud-Ressourcen in Ihren Azure-Abonnements verfügt. Wenn Sie mehrere Azure Marketplace-Abonnements verwalten, können Sie jedem Abonnement auf der Seite „Anmeldeinformationen“ unterschiedliche Azure-Anmeldeinformationen zuweisen.

Überblick

Es gibt zwei Möglichkeiten, zusätzliche Azure-Abonnements und Anmeldeinformationen in der Konsole hinzuzufügen.

1. Ordnen Sie der von Azure verwalteten Identität zusätzliche Azure-Abonnements zu.
2. Um Cloud Volumes ONTAP mit unterschiedlichen Azure-Anmeldeinformationen bereitzustellen, erteilen Sie Azure Berechtigungen mithilfe eines Dienstprinzipals und fügen Sie dessen Anmeldeinformationen der Konsole hinzu.

Zuordnen zusätzlicher Azure-Abonnements zu einer verwalteten Identität

Über die Konsole können Sie die Azure-Anmeldeinformationen und das Azure-Abonnement auswählen, in dem Sie Cloud Volumes ONTAP bereitstellen möchten. Sie können kein anderes Azure-Abonnement für das verwaltete Identitätsprofil auswählen, es sei denn, Sie verknüpfen das "Verwaltete Identität" mit diesen Abonnements.

Informationen zu diesem Vorgang

Eine verwaltete Identität ist"das anfängliche Azure-Konto" wenn Sie einen Konsolenagenten von der Konsole aus bereitstellen. Wenn Sie den Konsolenagenten bereitstellen, weist die Konsole der virtuellen Maschine des Konsolenagenten die Rolle des Konsolenoperators zu.

Schritte

1. Melden Sie sich beim Azure-Portal an.
2. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP bereitstellen möchten.
3. Wählen Sie **Zugriffskontrolle (IAM)**.
   a. Wählen Sie **Hinzufügen** > **Rollenzuweisung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
      - Wählen Sie die Rolle **Konsolenoperator** aus.

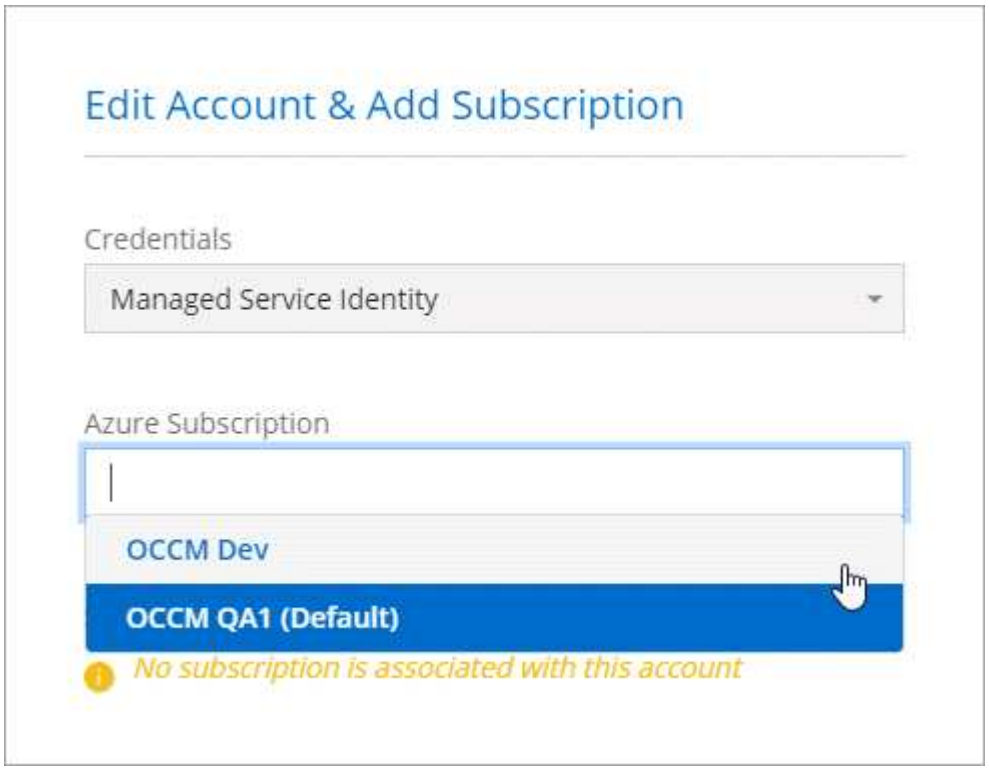
        „Konsolenoperator“ ist der Standardname, der in einer Konsolenagentrichtlinie angegeben wird. Wenn Sie einen anderen Namen für die Rolle gewählt haben, wählen Sie stattdessen diesen Namen aus.

- Weisen Sie einer **virtuellen Maschine** Zugriff zu.
- Wählen Sie das Abonnement aus, in dem eine virtuelle Maschine des Konsolen-Agenten erstellt wurde.
- Wählen Sie eine virtuelle Maschine des Konsolenagenten aus.
- Wählen Sie **Speichern**.

4. Wiederholen Sie diese Schritte für weitere Abonnements.

Ergebnis

Beim Erstellen eines neuen Systems können Sie jetzt aus mehreren Azure-Abonnements für das verwaltete Identitätsprofil auswählen.



Fügen Sie der NetApp Console zusätzliche Azure-Anmeldeinformationen hinzu

Wenn Sie einen Konsolenagenten über die Konsole bereitstellen, aktiviert die Konsole eine vom System zugewiesene verwaltete Identität auf der virtuellen Maschine, die über die erforderlichen Berechtigungen verfügt. Die Konsole wählt diese Azure-Anmeldeinformationen standardmäßig aus, wenn Sie ein neues System für Cloud Volumes ONTAP erstellen.

Wenn Sie eine Konsolenagentensoftware manuell auf einem vorhandenen System installiert haben, wird kein anfänglicher Satz Anmeldeinformationen hinzugefügt. "Erfahren Sie mehr über Azure-Anmeldeinformationen und -Berechtigungen" .

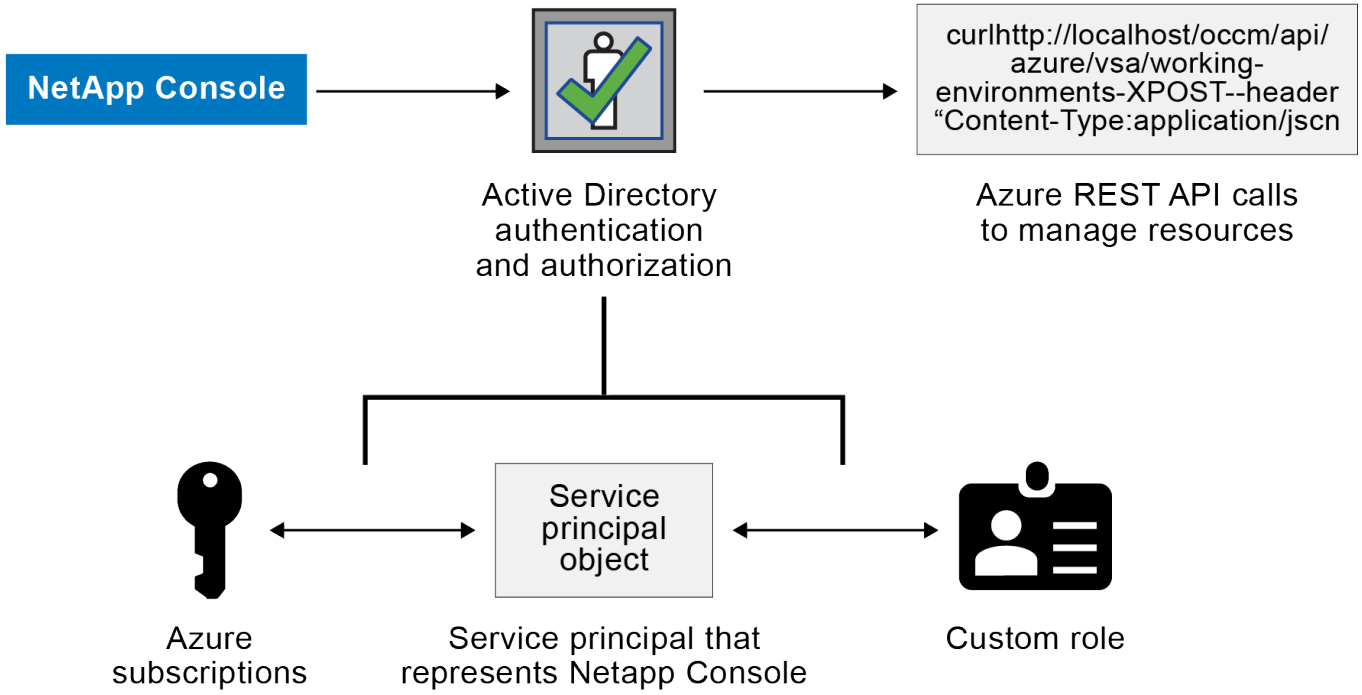
Wenn Sie Cloud Volumes ONTAP mit *verschiedenen* Azure-Anmeldeinformationen bereitstellen möchten, müssen Sie die erforderlichen Berechtigungen erteilen, indem Sie für jedes Azure-Konto einen Dienstprinzipal in der Microsoft Entra-ID erstellen und einrichten. Anschließend können Sie die neuen Anmeldeinformationen zur Konsole hinzufügen.

Gewähren von Azure-Berechtigungen mithilfe eines Dienstprinzipals

Die Konsole benötigt Berechtigungen, um Aktionen in Azure auszuführen. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie einen Dienstprinzipal in Microsoft Entra ID erstellen und einrichten und die Azure-Anmeldeinformationen abrufen, die die Konsole benötigt.

Informationen zu diesem Vorgang

Das folgende Bild zeigt, wie die Konsole Berechtigungen zum Ausführen von Vorgängen in Azure erhält. Ein Dienstprinzipalobjekt, das an ein oder mehrere Azure-Abonnements gebunden ist, stellt die Konsole in der Microsoft Entra ID dar und ist einer benutzerdefinierten Rolle zugewiesen, die die erforderlichen Berechtigungen gewährt.



Schritte

1. Erstellen einer Microsoft Entra-Anwendung .
2. Zuweisen der Anwendung zu einer Rolle .
3. Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu .
4. Abrufen der Anwendungs-ID und der Verzeichnis-ID .
5. Erstellen eines Client-Geheimnisses .

Erstellen einer Microsoft Entra-Anwendung

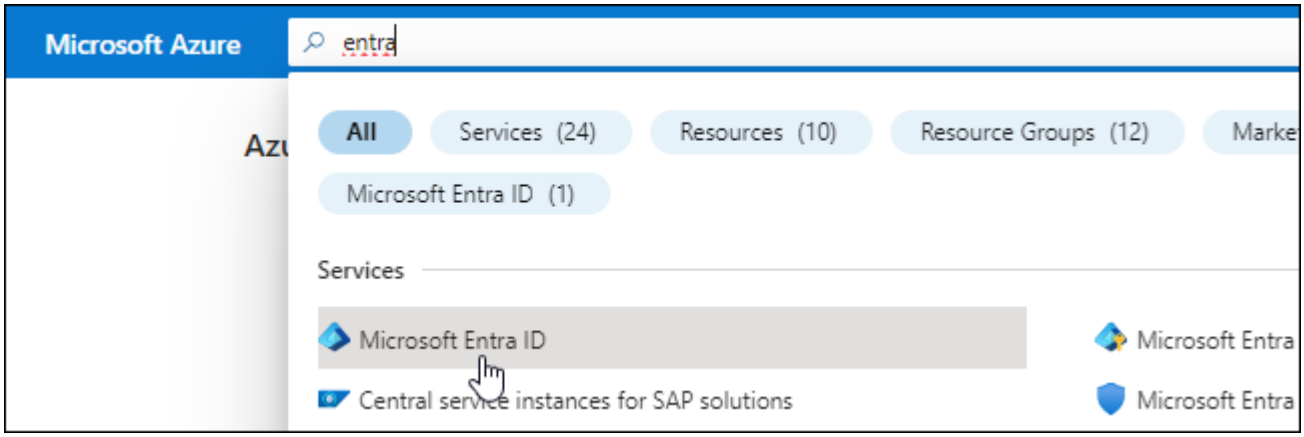
Erstellen Sie eine Microsoft Entra-Anwendung und einen Dienstprinzipal, den die Konsole für die rollenbasierte Zugriffskontrolle verwenden kann.

Schritte

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

Sie müssen den Dienstprinzipal an ein oder mehrere Azure-Abonnements binden und ihm die benutzerdefinierte Rolle „Konsolenoperator“ zuweisen, damit die Konsole über Berechtigungen in Azure verfügt.

Schritte

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.

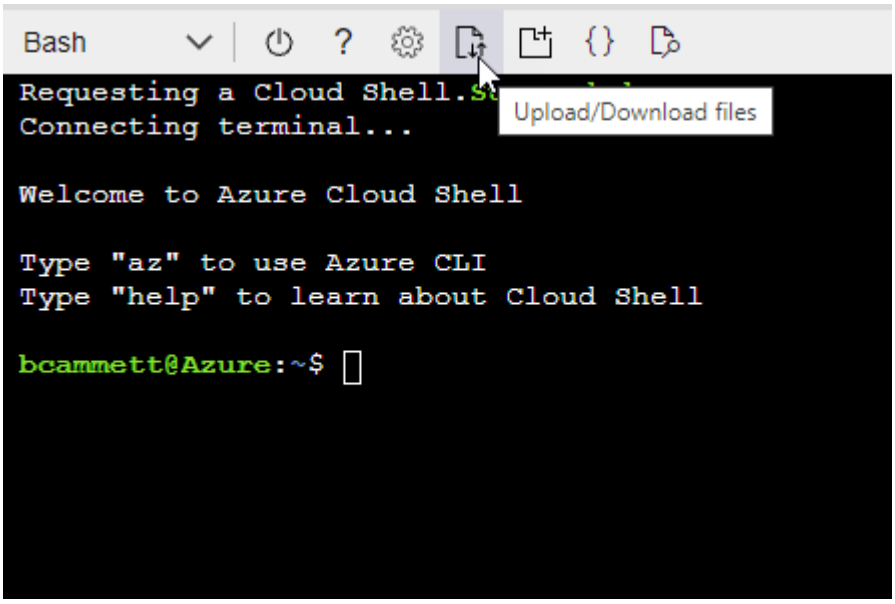
      Beispiel

```
"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.

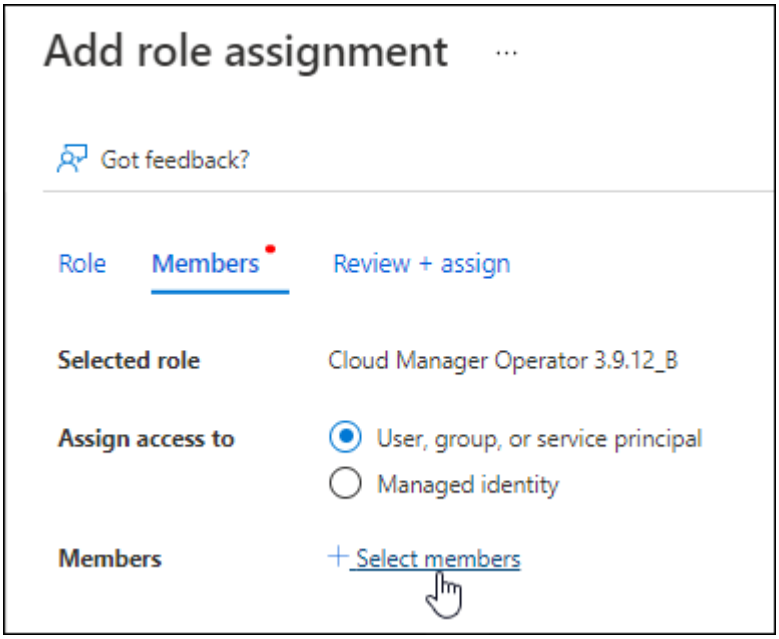
c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

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:

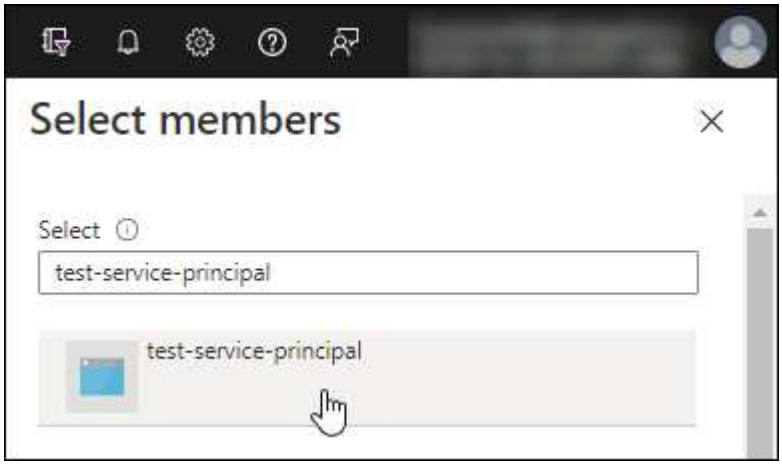
- Behalten Sie die Auswahl von **Benutzer, Gruppe oder Dienstprinzipal** bei.

- 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.

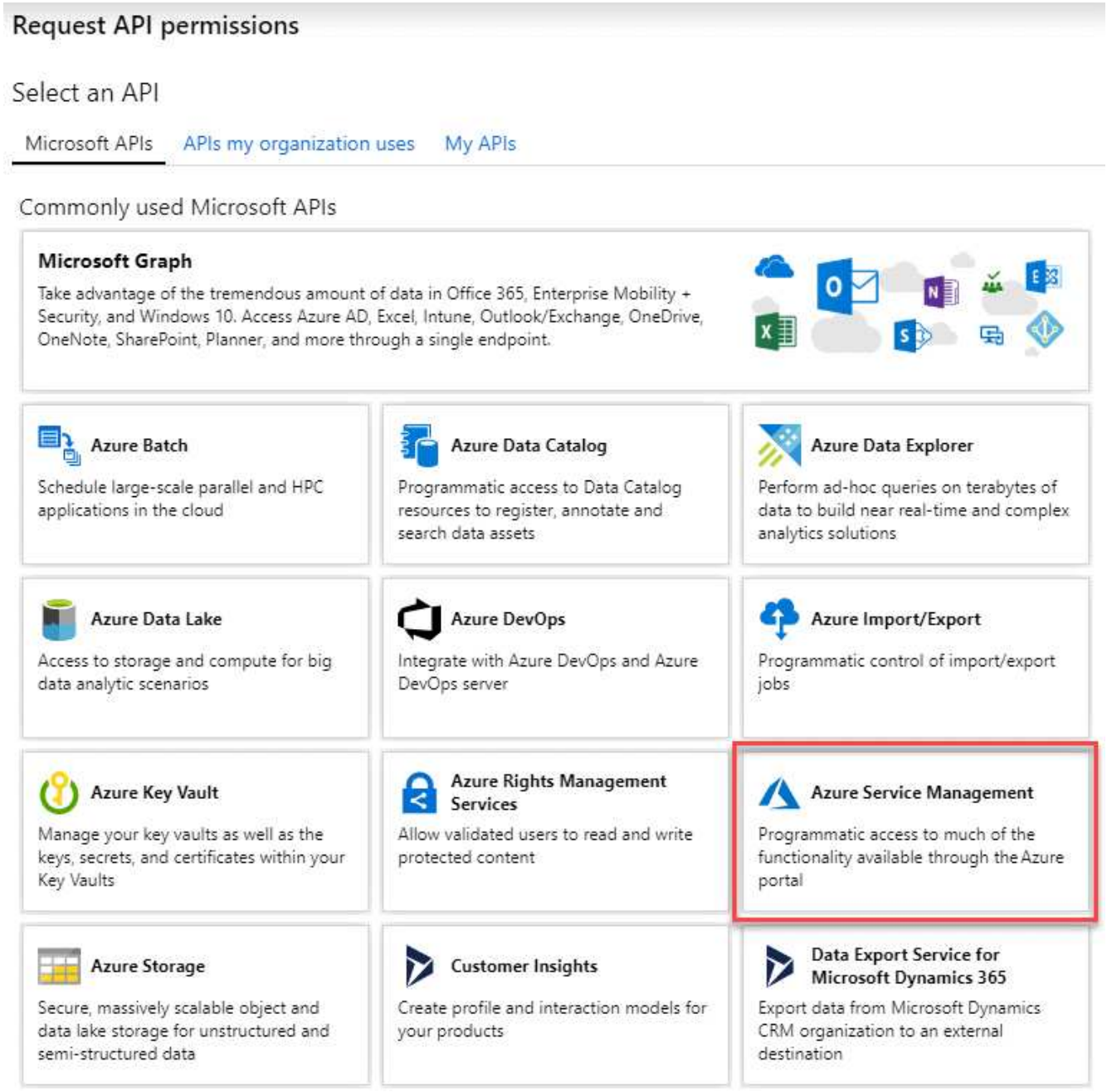
Wenn Sie Cloud Volumes ONTAP aus mehreren Azure-Abonnements bereitstellen möchten, müssen Sie den Dienstprinzipal an jedes dieser Abonnements binden. In der NetApp Console können Sie das Abonnement auswählen, das Sie beim Bereitstellen von Cloud Volumes ONTAP verwenden möchten.

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

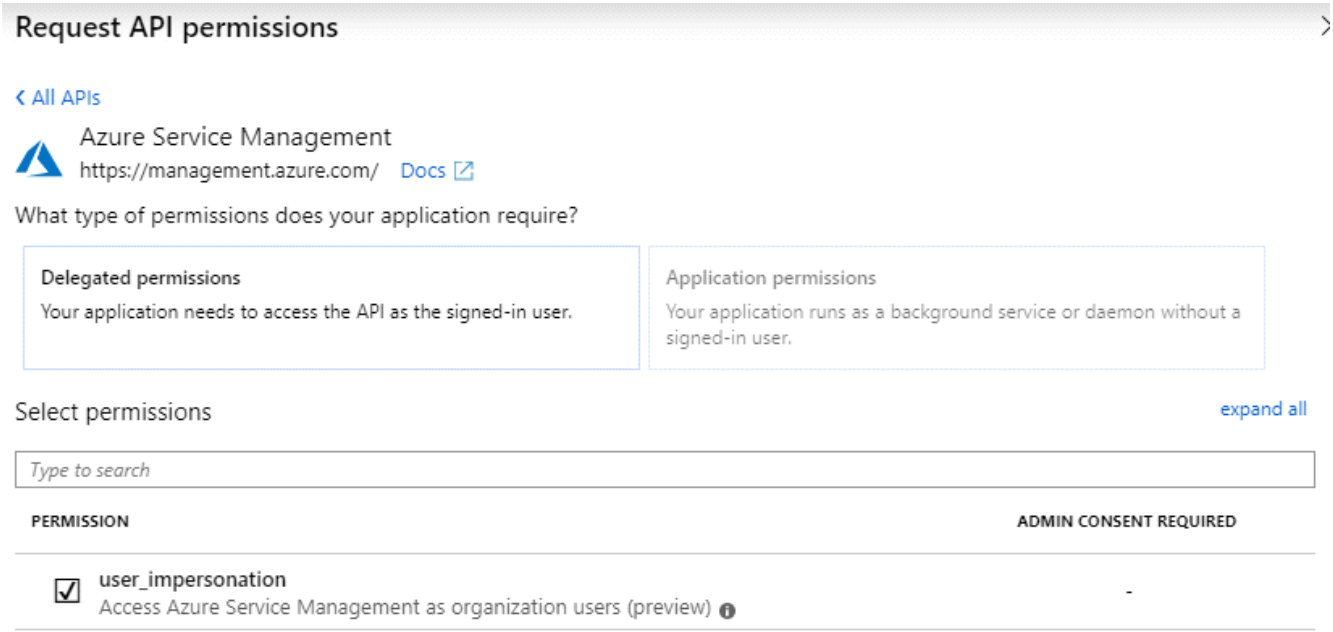
Sie müssen dem Dienstprinzipal die Berechtigung „Windows Azure Service Management API“ zuweisen.

Schritte

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**.

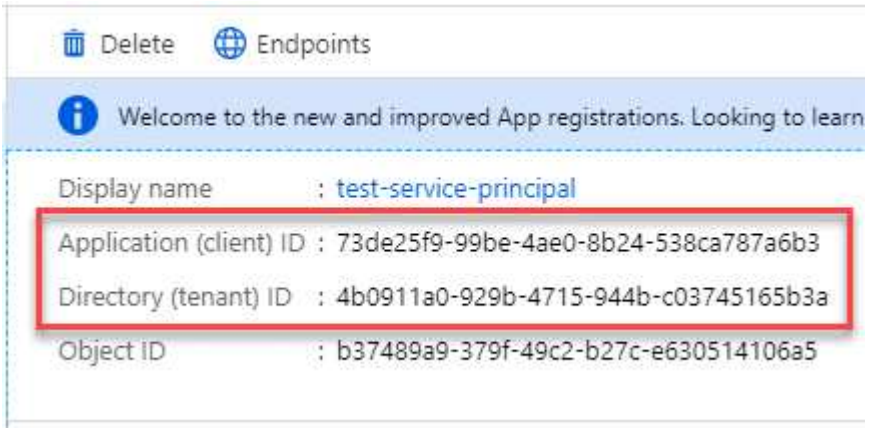


Abrufen der Anwendungs-ID und der Verzeichnis-ID

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.

Schritte

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

Erstellen Sie ein Client-Geheimnis und geben Sie dessen Wert an die Konsole zur Authentifizierung mit der Microsoft Entra-ID weiter.

Schritte

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.

Fügen Sie die Anmeldeinformationen zur Konsole hinzu

Nachdem Sie ein Azure-Konto mit den erforderlichen Berechtigungen bereitgestellt haben, können Sie die Anmeldeinformationen für dieses Konto zur Konsole hinzufügen. Wenn Sie diesen Schritt abschließen, können Sie Cloud Volumes ONTAP mit anderen Azure-Anmeldeinformationen starten.

Bevor Sie beginnen

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

Bevor Sie beginnen

Sie müssen einen Konsolenagenten erstellen, bevor Sie die Konsoleneinstellungen ändern können. "Erfahren Sie, wie Sie einen Konsolenagenten erstellen" .

Schritte

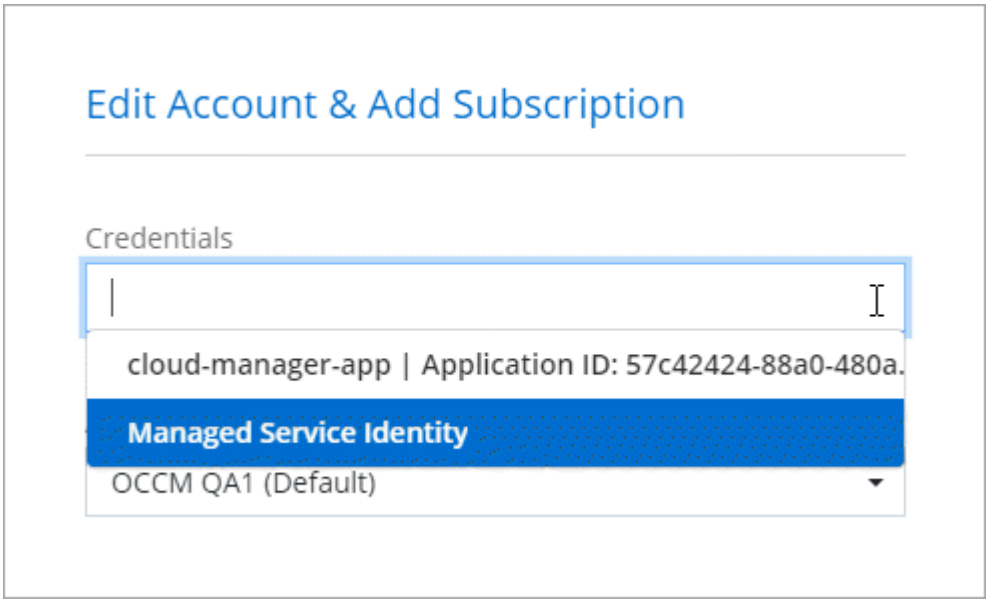
1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Microsoft Azure > Agent**.
   b. **Anmeldeinformationen definieren**: Geben Sie Informationen 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

Sie können auf der Seite „Details und Anmeldeinformationen“ zu einem anderen Satz von Anmeldeinformationen wechseln. "beim Hinzufügen eines Systems zur Konsole"



Vorhandene Anmeldeinformationen verwalten

Verwalten Sie die Azure-Anmeldeinformationen, die Sie der Konsole bereits hinzugefügt haben, indem Sie ein Marketplace-Abonnement zuordnen, Anmeldeinformationen bearbeiten und löschen.

Zuordnen eines Azure Marketplace-Abonnements zu Anmeldeinformationen

Nachdem Sie Ihre Azure-Anmeldeinformationen zur Konsole hinzugefügt haben, können Sie diesen Anmeldeinformationen ein Azure Marketplace-Abonnement zuordnen. Mit dem Abonnement können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und auf NetApp -Datendienste zugreifen.

Es gibt zwei Szenarien, in denen Sie ein Azure Marketplace-Abonnement zuordnen können, nachdem Sie die Anmeldeinformationen bereits zur Konsole hinzugefügt haben:

- Sie haben beim ersten Hinzufügen der Anmeldeinformationen zur Konsole kein Abonnement zugeordnet.
- Sie möchten das Azure Marketplace-Abonnement ändern, das mit Azure-Anmeldeinformationen verknüpft ist.

  Durch das Ersetzen des aktuellen Marktplatzabonnements wird es für vorhandene und neue Cloud Volumes ONTAP Systeme aktualisiert.

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**.

Anmeldeinformationen bearbeiten

Bearbeiten Sie Ihre Azure-Anmeldeinformationen in der Konsole. Sie können beispielsweise das Clientgeheimnis aktualisieren, wenn ein neues Geheimnis für die Dienstprinzipalanwendung erstellt wurde.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie das Aktionsmenü für einen Satz Anmeldeinformationen und wählen Sie dann **Anmeldeinformationen bearbeiten**.
4. Nehmen Sie die erforderlichen Änderungen vor und wählen Sie dann **Übernehmen**.

Anmeldeinformationen löschen

Wenn Sie einen Satz Anmeldeinformationen nicht mehr benötigen, können Sie ihn löschen. Sie können nur Anmeldeinformationen löschen, die keinem System zugeordnet sind.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Anmeldeinformationen löschen**.
4. Wählen Sie zur Bestätigung **Löschen**.

Google Cloud

Erfahren Sie mehr über Google Cloud-Projekte und -Berechtigungen

Erfahren Sie, wie die NetApp Console Google Cloud-Anmeldeinformationen verwendet, um Aktionen in Ihrem Namen auszuführen, und wie diese Anmeldeinformationen mit Marktplatzabonnements verknüpft werden. Das Verständnis dieser Details kann hilfreich sein, wenn Sie die Anmeldeinformationen für ein oder mehrere Google Cloud-Projekte verwalten. Beispielsweise möchten Sie möglicherweise mehr über das Dienstkonto erfahren, das mit der Konsolen-Agent-VM verknüpft ist.

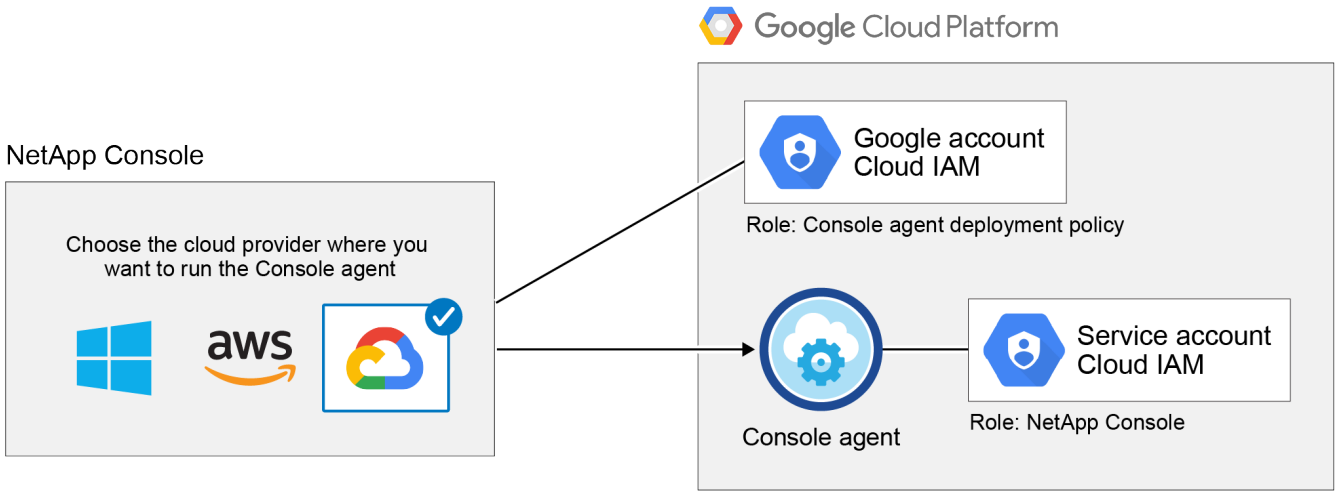
Projekt und Berechtigungen für die NetApp Console

Bevor Sie die Konsole zum Verwalten von Ressourcen in Ihrem Google Cloud-Projekt verwenden können, müssen Sie zunächst einen Konsolen-Agenten bereitstellen. Der Agent darf nicht bei Ihnen vor Ort oder bei einem anderen Cloud-Anbieter ausgeführt werden.

Bevor Sie einen Konsolenagenten direkt von der Konsole aus bereitstellen können, müssen zwei Berechtigungssätze vorhanden sein:

1. Sie müssen einen Konsolen-Agenten mit einem Google-Konto bereitstellen, das über die Berechtigung zum Starten des Konsolen-Agenten von der Konsole aus verfügt.
2. Beim Bereitstellen des Konsolenagenten werden Sie aufgefordert, einen "Dienstkonto" für den Agenten Die Konsole erhält vom Dienstkonto Berechtigungen zum Erstellen und Verwalten von Cloud Volumes ONTAP -Systemen, zum Verwalten von Backups mithilfe von NetApp Backup und Recovery und mehr. Berechtigungen werden erteilt, indem dem Dienstkonto eine benutzerdefinierte Rolle zugewiesen wird.

Die folgende Abbildung veranschaulicht die unter den Nummern 1 und 2 beschriebenen Berechtigungsanforderungen:



Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

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

Anmeldeinformationen und Marktplatzabonnements

Wenn Sie einen Konsolen-Agenten in Google Cloud bereitstellen, erstellt die Konsole einen Standardsatz von Anmeldeinformationen für das Google Cloud-Dienstkonto in dem Projekt, in dem sich der Konsolen-Agent befindet. Diese Anmeldeinformationen müssen mit einem Google Cloud Marketplace-Abonnement verknüpft sein, damit Sie für Cloud Volumes ONTAP und NetApp -Datendienste bezahlen können.

"Erfahren Sie, wie Sie ein Google Cloud Marketplace-Abonnement zuordnen" .

Beachten Sie Folgendes zu Google Cloud-Anmeldeinformationen und Marktplatz-Abonnements:

- Einem Konsolenagenten kann nur ein Satz Google Cloud-Anmeldeinformationen zugeordnet werden.
- Sie können den Anmeldeinformationen nur ein Google Cloud Marketplace-Abonnement zuordnen
- Sie können ein bestehendes Marktplatz-Abonnement durch ein neues Abonnement ersetzen

Projekt für Cloud Volumes ONTAP

Cloud Volumes ONTAP kann sich im selben Projekt wie der Konsolenagent oder in einem anderen Projekt befinden. Um Cloud Volumes ONTAP in einem anderen Projekt bereitzustellen, müssen Sie zuerst das Dienstkonto und die Rolle des Konsolenagenten zu diesem Projekt hinzufügen.

- "Erfahren Sie, wie Sie das Dienstkonto einrichten"
- "Erfahren Sie, wie Sie Cloud Volumes ONTAP in Google Cloud bereitstellen und ein Projekt auswählen"

Verwaltung der Console-Agentenberechtigungen für Google Cloud-Bereitstellungen

Gelegentlich aktualisiert NetApp die Berechtigungen, die für das Dienstkonto erforderlich sind, das für den Console-Agenten verwendet wird, wenn dieser in Google Cloud bereitgestellt wird.

"Überprüfen Sie die Liste der erforderlichen Google-Berechtigungen.".

Verwenden Sie die Google Cloud Console, um die dem Dienstkonto zugewiesene IAM-Rolle an die neuen Berechtigungen anzupassen.

"Google Cloud-Dokumentation: Bearbeiten einer benutzerdefinierten Rolle"