



Bereitstellen eines Konsolenagenten

NetApp Console setup and administration

NetApp

February 11, 2026

Inhalt

Bereitstellen eines Konsolenagenten	1
AWS	1
Installationsoptionen für Konsolenagenten in AWS	1
Erstellen Sie einen Konsolenagenten in AWS über die NetApp Console	1
Erstellen Sie einen Konsolenagenten aus dem AWS Marketplace	9
Manuelle Installation des Konsolenagenten in AWS	15
Azurblau	29
Installationsoptionen für den Konsolen-Agenten in Azure	30
Erstellen Sie einen Konsolen-Agenten in Azure über die NetApp Console	30
Erstellen eines Konsolen-Agents aus dem Azure Marketplace	44
Manuelles Installieren des Konsolen-Agents in Azure	59
Google Cloud	81
Installationsoptionen für den Konsolenagenten in Google Cloud	81
Erstellen Sie einen Konsolenagenten in Google Cloud über die NetApp Console	81
Erstellen Sie einen Konsolenagenten aus Google Cloud	91
Installieren Sie den Konsolenagenten manuell in Google Cloud	103
Installieren eines Agenten vor Ort	118
Manuelle Installation eines Konsolen-Agenten vor Ort	119
Installieren Sie einen Konsolenagenten vor Ort mit VCenter	143
Ports für den lokalen Konsolenagenten	160

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): <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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.blueexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.blueexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://blueexpinfraprod.eastus2.data.azurecr.io https://blueexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. <ul style="list-style-type: none"> • 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. <p>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".</p> <ul style="list-style-type: none"> • 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: Bedingungelement"](#)

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
<p>AWS-Dienste (amazonaws.com):</p> <ul style="list-style-type: none"> • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3) 	<p>Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab.</p> <p>"Weitere Einzelheiten finden Sie in der AWS-Dokumentation."</p>
<p>Amazon FsX für NetApp ONTAP:</p> <ul style="list-style-type: none"> • api.workloads.netapp.com 	<p>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.</p>
https://mysupport.netapp.com	<p>Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.</p>
https://signin.b2c.netapp.com	<p>So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.</p>
https://support.netapp.com	<p>Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.</p>
<p>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</p>	<p>Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.</p>

Endpunkte	Zweck
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	<p>Um Bilder für Upgrades des Konsolenagenten zu erhalten.</p> <ul style="list-style-type: none"> • 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. <p>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" .</p> <ul style="list-style-type: none"> • 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:

- Geben Sie die Konsolenorganisation an, die mit dem Konsolenagenten verknüpft werden soll.
- Geben Sie einen Namen für das System ein.
- 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"](#) .

- 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 <ul style="list-style-type: none">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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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): <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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.blueexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.blueexp.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	<p>Um Bilder für Upgrades des Konsolenagenten zu erhalten.</p> <ul style="list-style-type: none"> • 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. <p>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" .</p> <ul style="list-style-type: none"> • 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 Backslashes 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 Konsolenagentendienst (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:

```
<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>
```

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.blueexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.blueexp.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	<p>Um Bilder für Upgrades des Konsolenagenten zu erhalten.</p> <ul style="list-style-type: none"> • 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. <p>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" .</p> <ul style="list-style-type: none"> • 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/read",
    "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

```

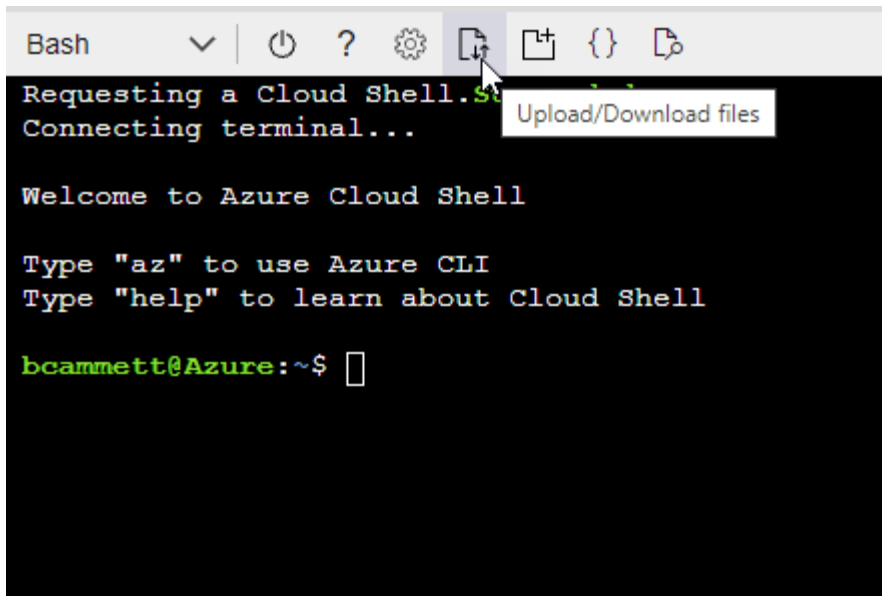
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
]

```

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.

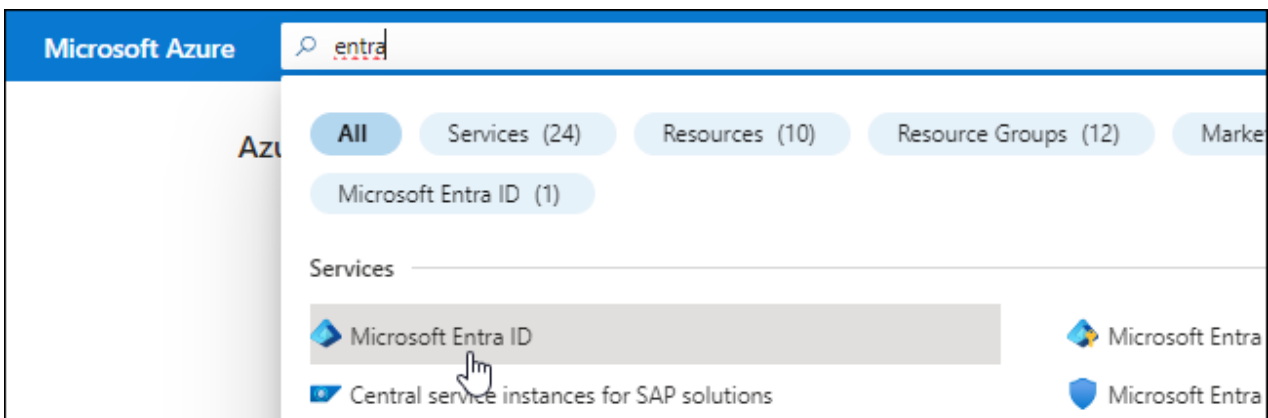
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die die Konsole benötigt.

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**.

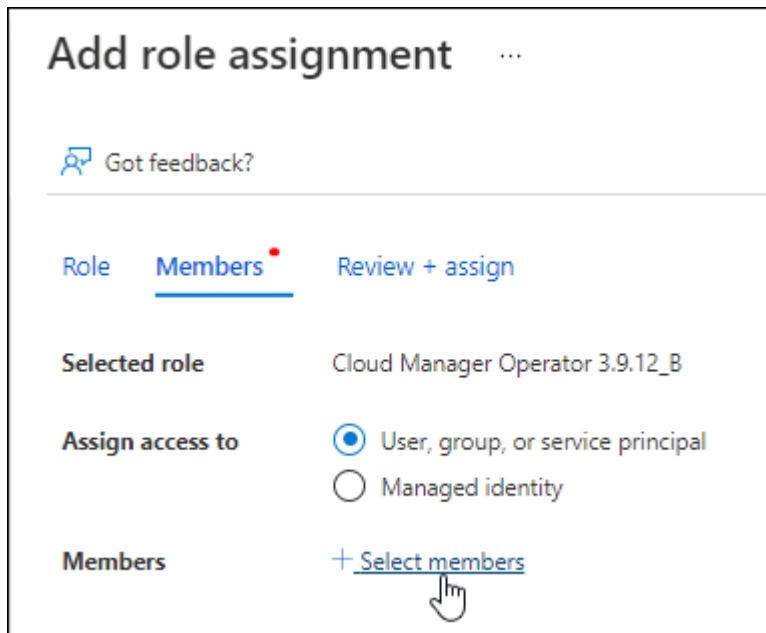


3. Wählen Sie im Menü **App-Registrierungen** aus.
4. Wählen Sie **Neuregistrierung**.
5. Geben Sie Details zur Anwendung an:
 - **Name:** Geben Sie einen Namen für die Anwendung ein.
 - **Kontotyp:** Wählen Sie einen Kontotyp aus (alle funktionieren mit der NetApp Console).
 - **Umleitungs-URI:** Sie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

Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

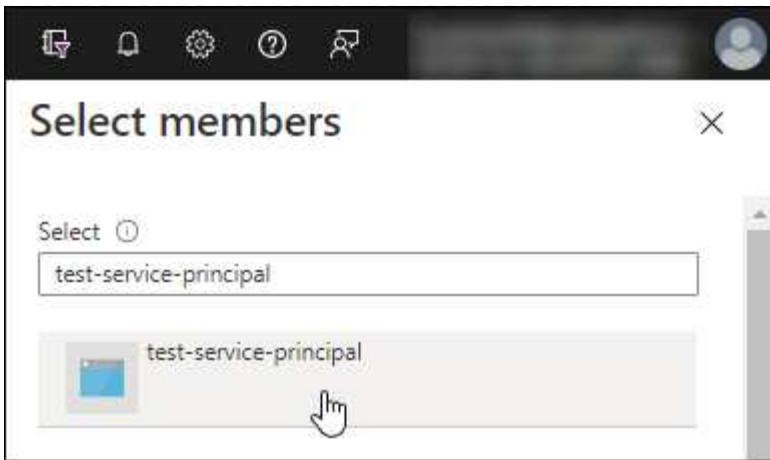
Zuweisen der benutzerdefinierten Rolle zur Anwendung

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.


Request API permissions


Select an API


Microsoft APIs APIs my organization uses My APIs


Commonly used Microsoft APIs


Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.





**Azure Batch**
Schedule large-scale parallel and HPC applications in the cloud


**Azure Data Catalog**
Programmatic access to Data Catalog resources to register, annotate and search data assets


**Azure Data Explorer**
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions


**Azure Data Lake**
Access to storage and compute for big data analytic scenarios


**Azure DevOps**
Integrate with Azure DevOps and Azure DevOps server


**Azure Import/Export**
Programmatic control of import/export jobs


**Azure Key Vault**
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

**Azure Rights Management Services**
Allow validated users to read and write protected content

**Azure Service Management**
Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

**Customer Insights**
Create profile and interaction models for your products

**Data Export Service for Microsoft Dynamics 365**
Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

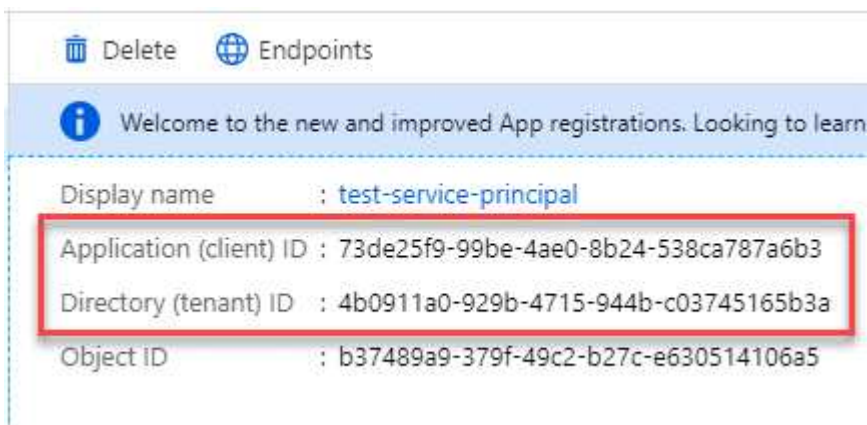


user_impersonation

Access Azure Service Management as organization users (preview)

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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.blueexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.blueexp.netapp.com https://cdn.auth0.com	<p>Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.</p>
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	<p>Um Bilder für Upgrades des Konsolenagenten zu erhalten.</p> <ul style="list-style-type: none"> • 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. <p>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".</p> <ul style="list-style-type: none"> • 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.

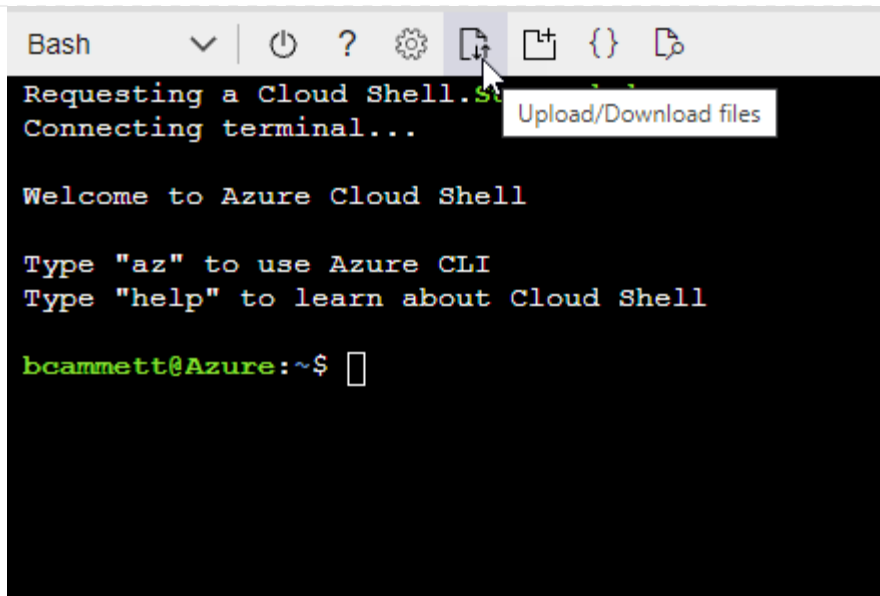
Beispiel

```
"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

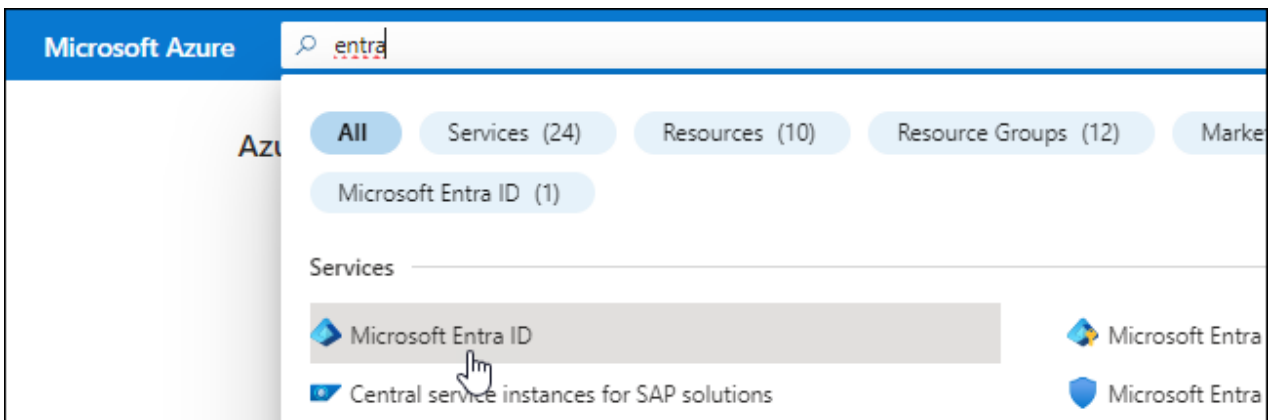
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die die Konsole benötigt.

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"](#)

- Kopieren Sie den Inhalt der ["benutzerdefinierte Rollenberechtigungen für den Konsolenagenten"](#) und speichern Sie sie in einer JSON-Datei.
- 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.

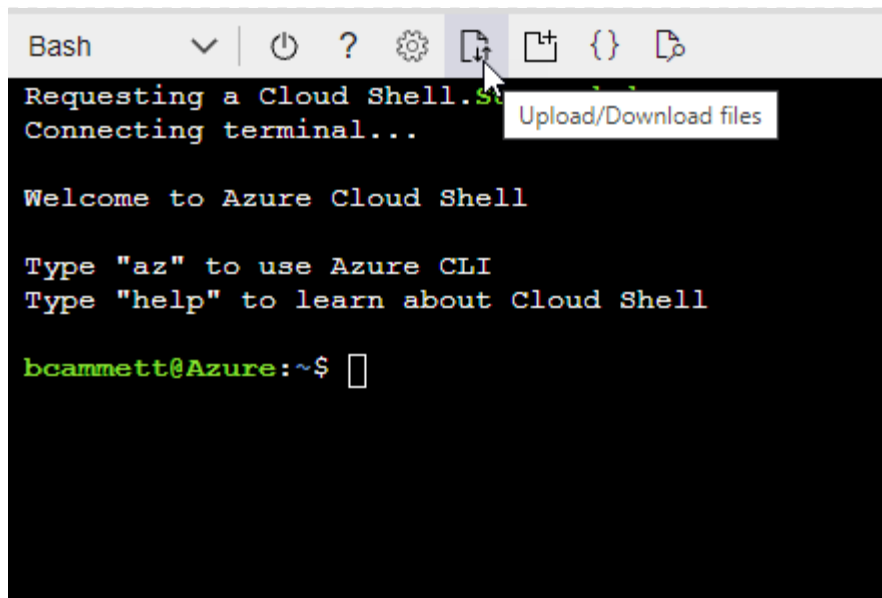
Beispiel

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

- 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.



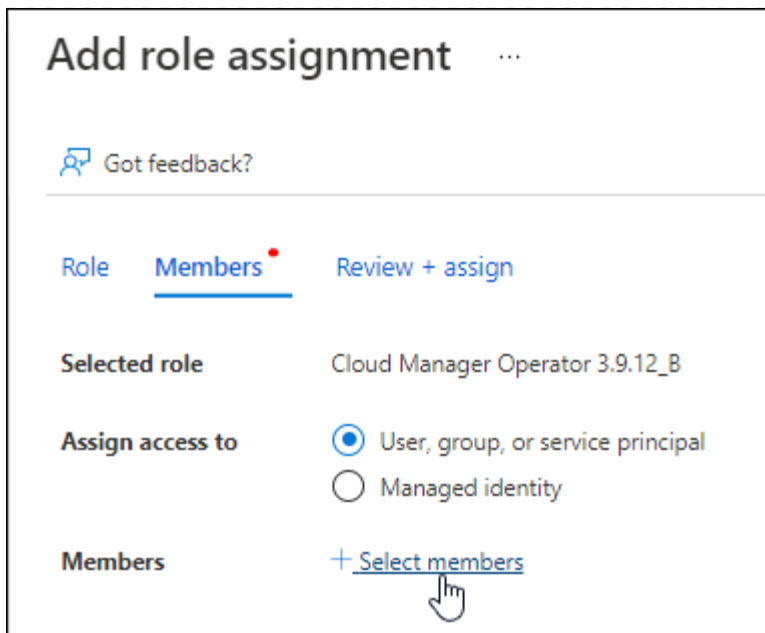
- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
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.

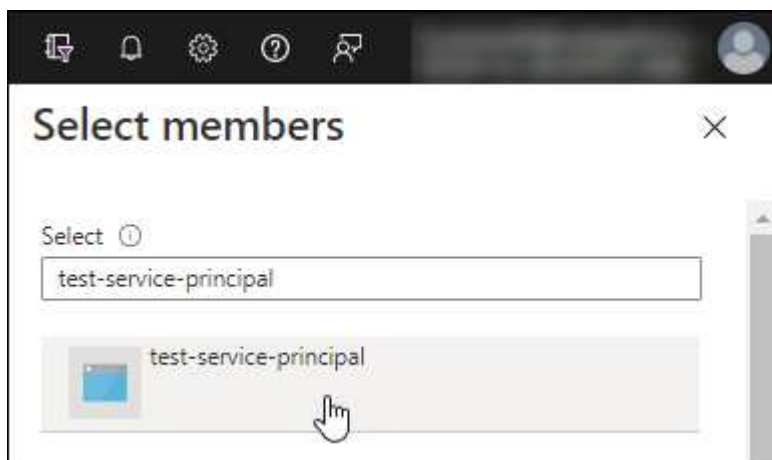
2. Weisen Sie die Anwendung der Rolle zu:

- Öffnen Sie im Azure-Portal den Dienst **Abonnements**.
- Wählen Sie das Abonnement aus.
- Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
- Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.
- 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.

Request API permissions

Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

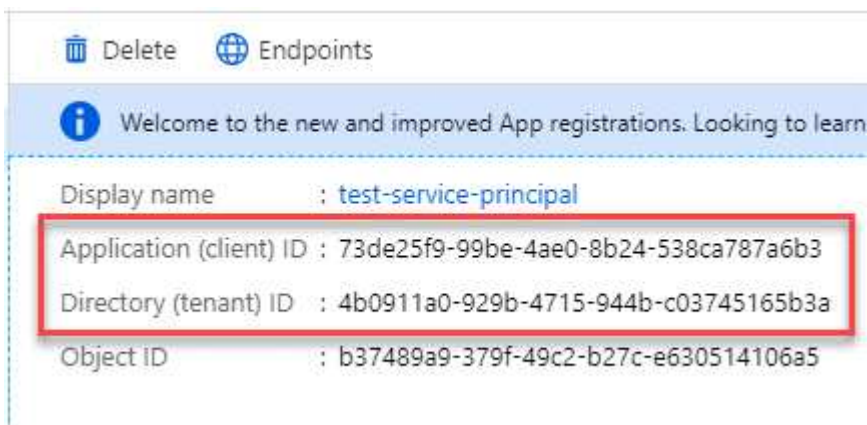


user_impersonation

Access Azure Service Management as organization users (preview)

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

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:

```
<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>
```

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 <ul style="list-style-type: none">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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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` 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.blueexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.blueexp.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	<p>Um Bilder für Upgrades des Konsolenagenten zu erhalten.</p> <ul style="list-style-type: none"> • 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. <p>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" .</p> <ul style="list-style-type: none"> • 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 Berechtigungsberechtigungen 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.

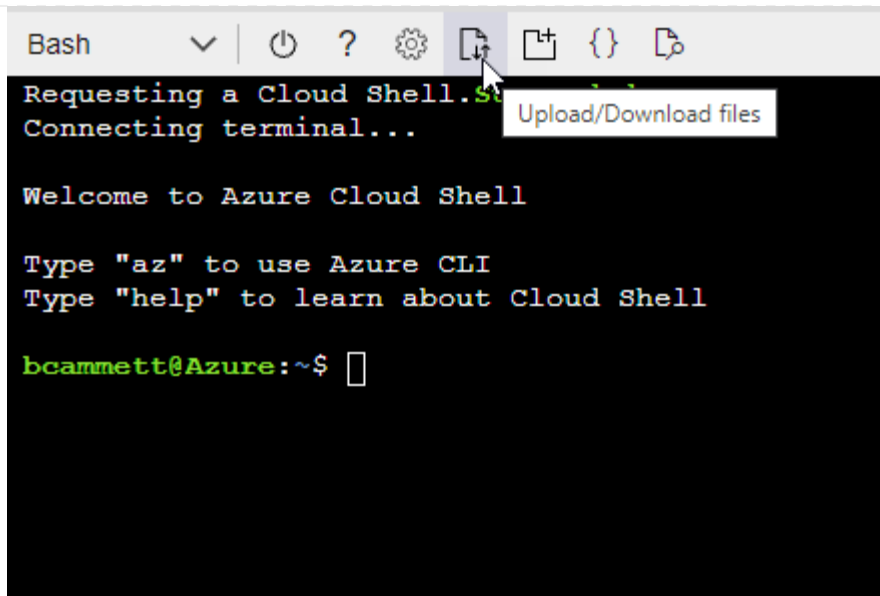
Beispiel

```
"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

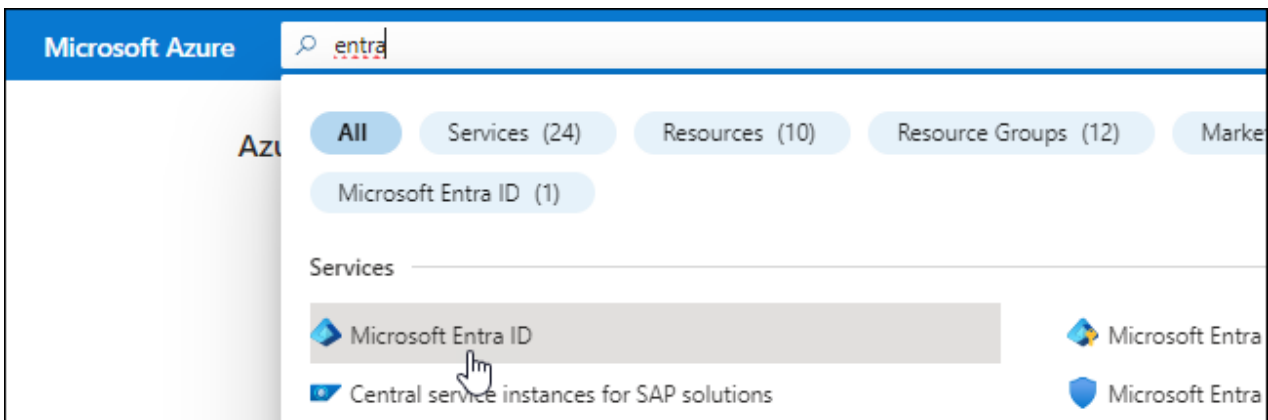
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die der Konsolenagent benötigt.

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"](#)

- Kopieren Sie den Inhalt der ["benutzerdefinierte Rollenberechtigungen für den Konsolenagenten"](#) und speichern Sie sie in einer JSON-Datei.
- 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.

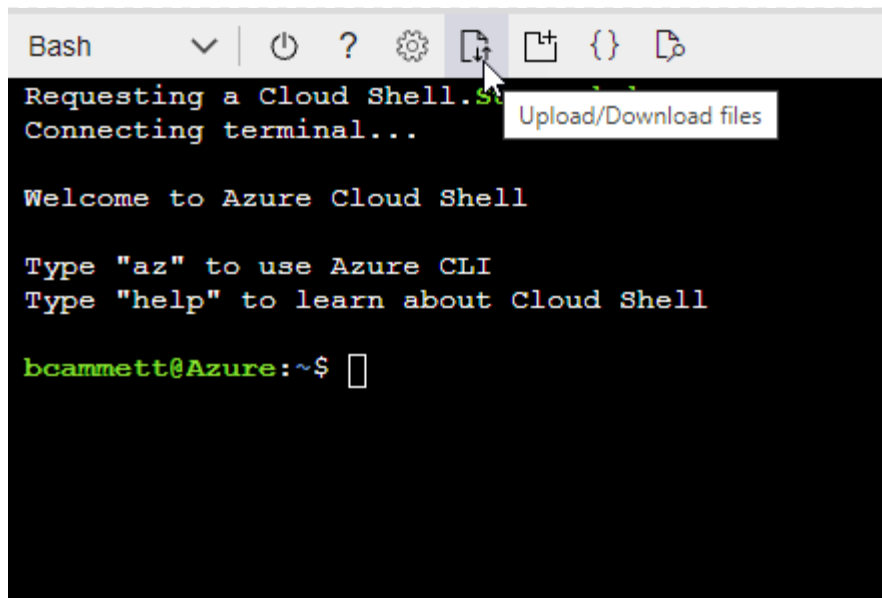
Beispiel

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

- 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:

- Öffnen Sie im Azure-Portal den Dienst **Abonnements**.
- Wählen Sie das Abonnement aus.
- Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
- Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.
- Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:
 - Behalten Sie die Auswahl von **Benutzer, Gruppe oder Dienstprinzipal** bei.
 - Wählen Sie **Mitglieder auswählen**.

Add role assignment ...

Got feedback?

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12_B

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

- Suchen Sie nach dem Namen der Anwendung.

Hier ist ein Beispiel:

Select members ✕

Select ⓘ

test-service-principal

test-service-principal

- 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.

Request API permissions

Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

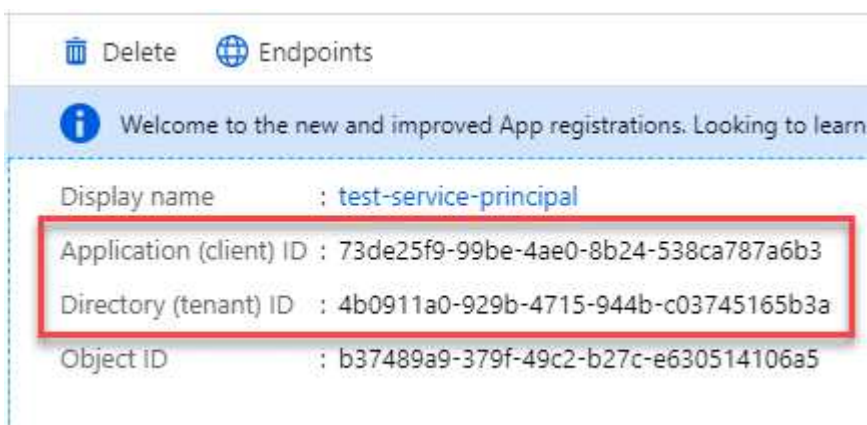


user_impersonation

Access Azure Service Management as organization users (preview)

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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 Backslashes 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 Konsolenagentendienst (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:

```
<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>
```

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.blueexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.blueexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://blueexpinfraprod.eastus2.data.azurecr.io https://blueexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. <ul style="list-style-type: none"> • 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. <p>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".</p> <ul style="list-style-type: none"> • 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.network User	Bereitstellen des Agenten im Serviceprojekt
Agent-Dienstkonto	Brauch	Serviceprojekt	"Agent-Dienstkontorichtlinie"	compute.network User 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.network User	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.network User	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 Deployment Manager V2 API
 - Cloud Infrastructure Manager API
 - Cloud Logging API
 - Cloud Resource Manager-API
 - Compute Engine-API
 - API für Identitäts- und Zugriffsverwaltung (IAM)
 - Cloud Key Management Service (KMS) API (Nur erforderlich, wenn Sie NetApp Backup and Recovery mit kundenseitig verwalteten Verschlüsselungsschlüsseln (CMEK) verwenden möchten)
 - Cloud Quotas API (erforderlich für Cloud Volumes ONTAP Deployments mit Infrastructure Manager)

["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 Produkthanleitung 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.blueexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.blueexp.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	<p>Um Bilder für Upgrades des Konsolenagenten zu erhalten.</p> <ul style="list-style-type: none"> • 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. <p>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" .</p> <ul style="list-style-type: none"> • 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 Plattform:

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.preview.get
- config.preview.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.network User	Bereitstellen des Agenten im Serviceprojekt
Agent-Dienstkonto	Brauch	Serviceprojekt	"Agent-Dienstkontorichtlinie"	compute.network User 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.network User	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.network User	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 Deployment Manager V2 API
 - Cloud Infrastructure Manager API
 - Cloud Logging API
 - Cloud Resource Manager-API
 - Compute Engine-API
 - API für Identitäts- und Zugriffsverwaltung (IAM)
 - Cloud Key Management Service (KMS) API (Nur erforderlich, wenn Sie NetApp Backup and Recovery mit kundenseitig verwalteten Verschlüsselungsschlüsseln (CMEK) verwenden möchten)
 - Cloud Quotas API (erforderlich für Cloud Volumes ONTAP Deployments mit Infrastructure Manager)

["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 <ul style="list-style-type: none">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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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.blueexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.blueexp.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	<p>Um Bilder für Upgrades des Konsolenagenten zu erhalten.</p> <ul style="list-style-type: none"> • 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. <p>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" .</p> <ul style="list-style-type: none"> • 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.network User	Bereitstellen des Agenten im Serviceprojekt
Agent-Dienstkonto	Brauch	Serviceprojekt	"Agent-Dienstkontorichtlinie"	compute.network User 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.network User	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.network User	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 Deployment Manager V2 API
 - Cloud Infrastructure Manager API
 - Cloud Logging API
 - Cloud Resource Manager-API
 - Compute Engine-API
 - API für Identitäts- und Zugriffsverwaltung (IAM)
 - Cloud Key Management Service (KMS) API (Nur erforderlich, wenn Sie NetApp Backup and Recovery mit kundenseitig verwalteten Verschlüsselungsschlüsseln (CMEK) verwenden möchten)
 - Cloud Quotas API (erforderlich für Cloud Volumes ONTAP Deployments mit Infrastructure Manager)

["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 Backslashes 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 Konsolenagentendienst (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 <ul style="list-style-type: none">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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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): <ul style="list-style-type: none">• CloudFormation• Elastische Compute Cloud (EC2)• Identitäts- und Zugriffsverwaltung (IAM)• Schlüsselvewaltungsdienst (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: <ul style="list-style-type: none">• 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	<p>Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.</p>
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	<p>Um Bilder für Upgrades des Konsolenagenten zu erhalten.</p> <ul style="list-style-type: none"> • 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. <p>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".</p> <ul style="list-style-type: none"> • 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	<p>Zum Verwalten von Ressourcen in öffentlichen Azure-Regionen.</p>
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	<p>Zum Verwalten von Ressourcen in Azure China-Regionen.</p>

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.blueexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.blueexp.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	<p>Um Bilder für Upgrades des Konsolenagenten zu erhalten.</p> <ul style="list-style-type: none"> • 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. <p>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".</p> <ul style="list-style-type: none"> • 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

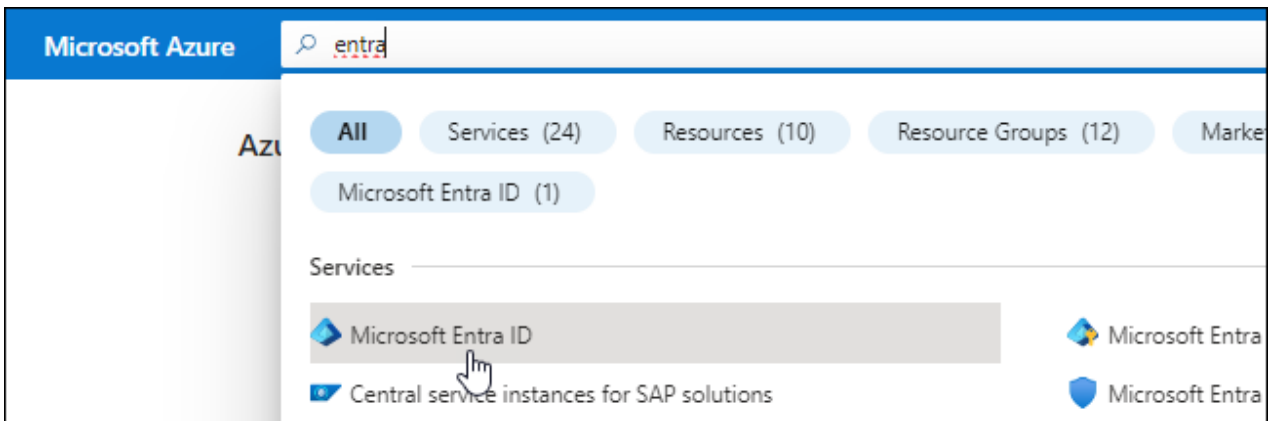
Wenn der Konsolen-Agent vor Ort installiert ist, müssen Sie dem Konsolen-Agenten Azure-Berechtigungen erteilen, indem Sie einen Dienstprinzipal in der Microsoft Entra ID einrichten und die Azure-Anmeldeinformationen abrufen, die der Konsolen-Agent benötigt.

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.

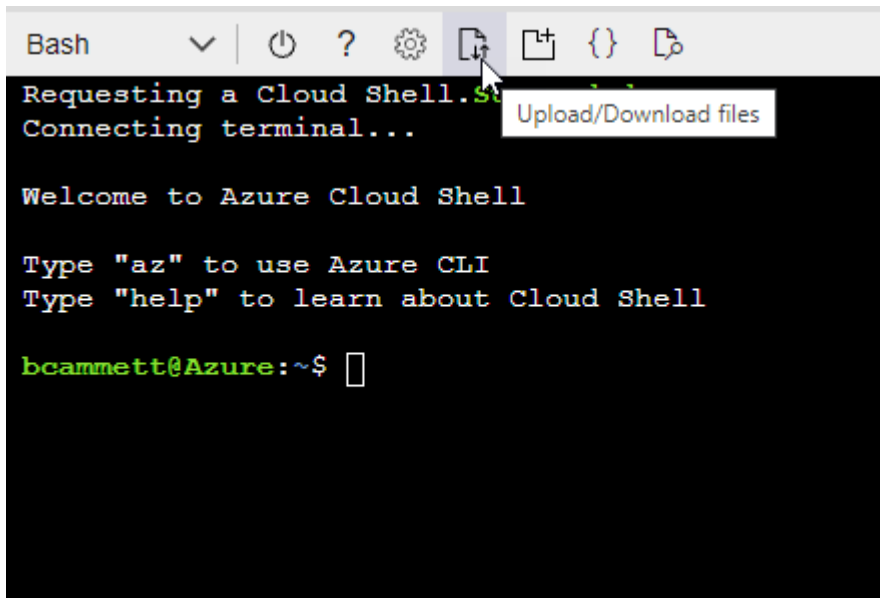
Beispiel

```
"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:

- Öffnen Sie im Azure-Portal den Dienst **Abonnements**.
- Wählen Sie das Abonnement aus.
- Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
- Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.
- Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:
 - Behalten Sie die Auswahl von **Benutzer, Gruppe oder Dienstprinzipal** bei.
 - Wählen Sie **Mitglieder auswählen**.

Add role assignment ...

Got feedback?

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12_B

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

- Suchen Sie nach dem Namen der Anwendung.

Hier ist ein Beispiel:

Select members ✕

Select ⓘ

test-service-principal

test-service-principal

- 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.

Request API permissions

Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

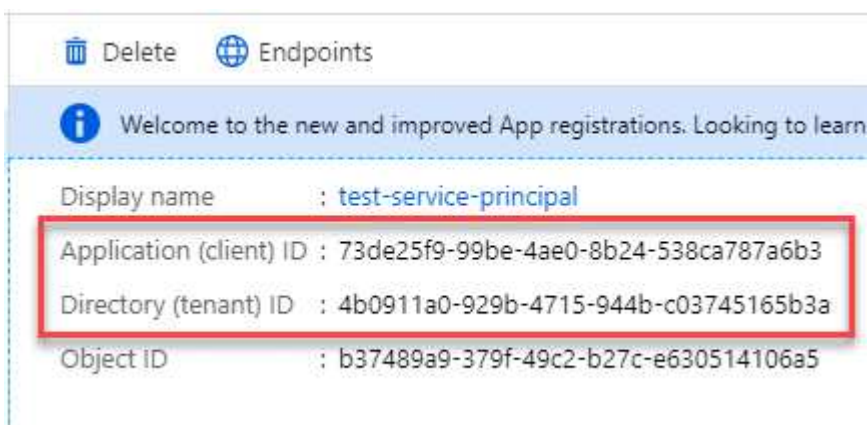


user_impersonation

Access Azure Service Management as organization users (preview)

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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](#)"

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 Backslashes 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): <ul style="list-style-type: none">• CloudFormation• Elastische Compute Cloud (EC2)• Identitäts- und Zugriffsverwaltung (IAM)• Schlüsselvewaltungsdienst (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: <ul style="list-style-type: none">• 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	<p>Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.</p>
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	<p>Um Bilder für Upgrades des Konsolenagenten zu erhalten.</p> <ul style="list-style-type: none"> • 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. <p>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".</p> <ul style="list-style-type: none"> • 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	<p>Zum Verwalten von Ressourcen in öffentlichen Azure-Regionen.</p>
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	<p>Zum Verwalten von Ressourcen in Azure China-Regionen.</p>

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.blueexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.blueexp.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	<p>Um Bilder für Upgrades des Konsolenagenten zu erhalten.</p> <ul style="list-style-type: none"> • 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. <p>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".</p> <ul style="list-style-type: none"> • 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

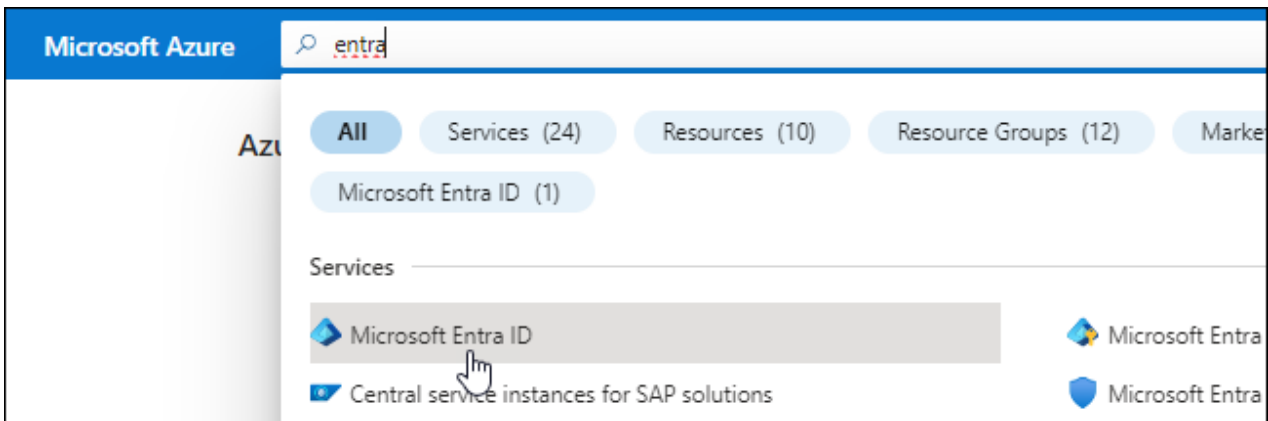
Wenn der Konsolen-Agent vor Ort installiert ist, müssen Sie dem Konsolen-Agenten Azure-Berechtigungen erteilen, indem Sie einen Dienstprinzipal in der Microsoft Entra ID einrichten und die Azure-Anmeldeinformationen abrufen, die der Konsolen-Agent benötigt.

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.

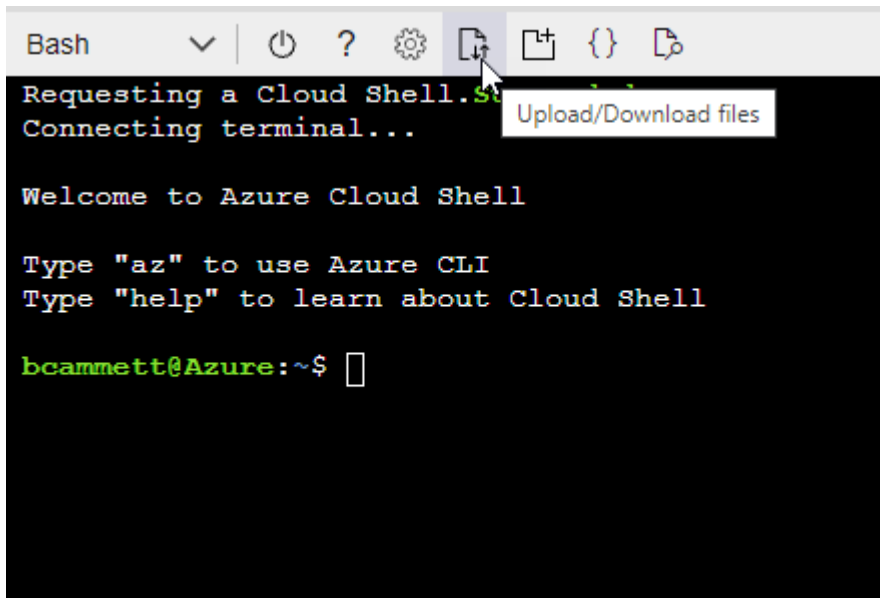
Beispiel

```
"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.



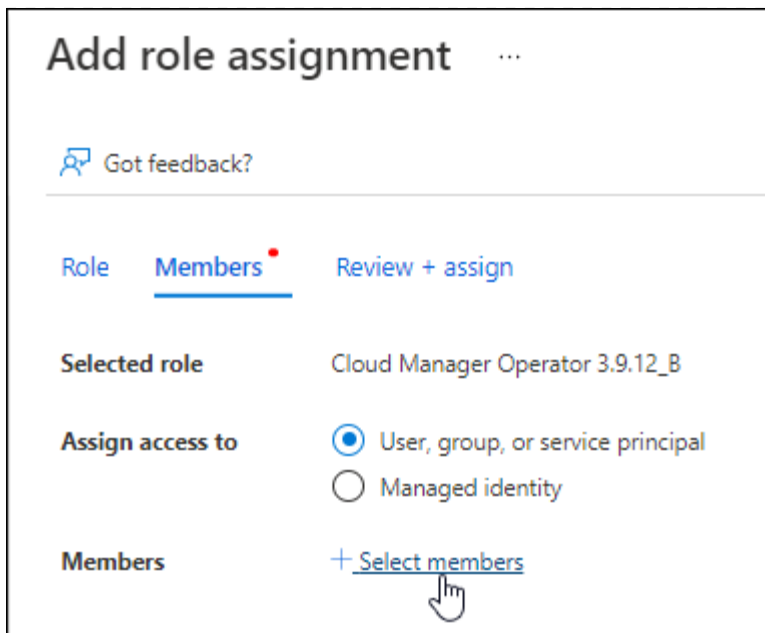
- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
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.

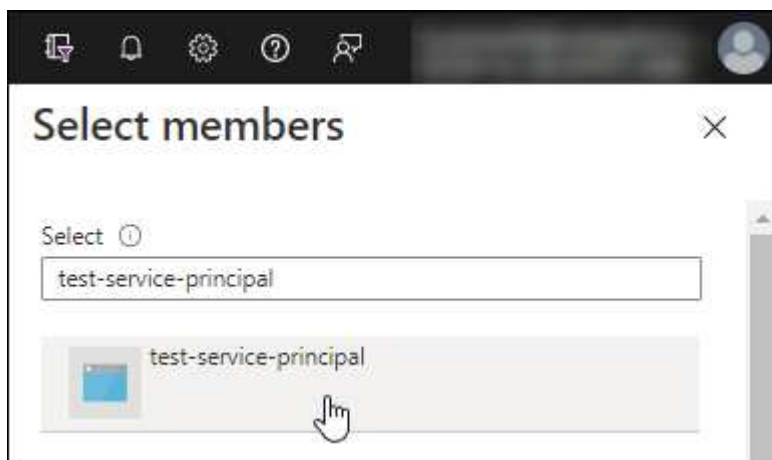
2. Weisen Sie die Anwendung der Rolle zu:

- Öffnen Sie im Azure-Portal den Dienst **Abonnements**.
- Wählen Sie das Abonnement aus.
- Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
- Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.
- 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.

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

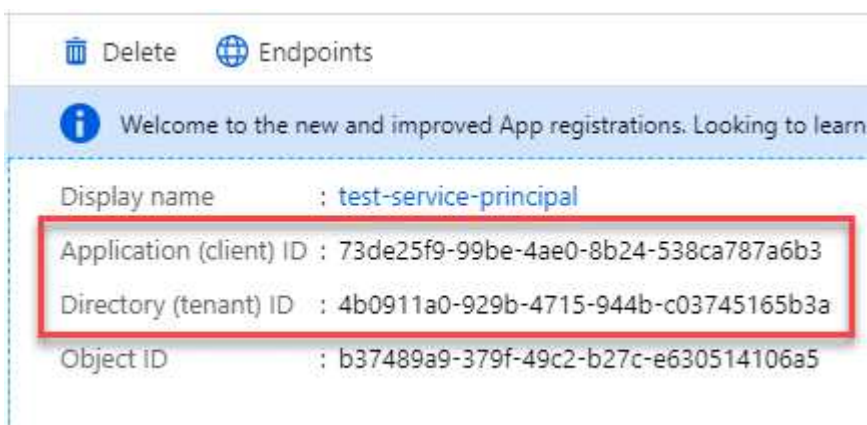


user_impersonation

Access Azure Service Management as organization users (preview)

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

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:

- Geben Sie die Konsolenorganisation an, die mit dem Konsolenagenten verknüpft werden soll.
- Geben Sie einen Namen für das System ein.
- 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	<ul style="list-style-type: none">• 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

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.