Verwalten und überwachen

NetApp Console setup and administration

NetApp
February 11, 2026

Inhalt

Verwalten und überwachen

NetApp Supportkonten

Verwalten der mit der NetApp Console verknüpften NSS-Anmeldeinformationen

Verknüpfen Sie ein NetApp Support Site-Konto mit Ihrer Konsolenorganisation, um wichtige Workflows für die Speicherverwaltung zu aktivieren. Diese NSS-Anmeldeinformationen sind mit der gesamten Organisation verknüpft.

Die Konsole unterstützt auch die Zuordnung eines NSS-Kontos pro Benutzerkonto. "Erfahren Sie, wie Sie Anmeldeinformationen auf Benutzerebene verwalten" .

Überblick

Um die folgenden Aufgaben zu ermöglichen, müssen Sie die Anmeldeinformationen der NetApp Support Site mit der Seriennummer Ihres spezifischen Konsolenkontos verknüpfen:

- Bereitstellen von Cloud Volumes ONTAP mit eigener Lizenz (BYOL)

  Die Angabe Ihres NSS-Kontos ist erforderlich, damit die Konsole Ihren Lizenzschlüssel hochladen und das Abonnement für die von Ihnen erworbene Laufzeit aktivieren kann. Hierzu gehören automatische Updates bei Laufzeitverlängerungen.

- Registrieren von Pay-as-you-go Cloud Volumes ONTAP Systemen

  Die Angabe Ihres NSS-Kontos ist erforderlich, um den Support für Ihr System zu aktivieren und Zugriff auf die technischen Supportressourcen von NetApp zu erhalten.

- Aktualisieren der Cloud Volumes ONTAP -Software auf die neueste Version

Diese Anmeldeinformationen sind mit der Seriennummer Ihres spezifischen Konsolenkontos verknüpft. Benutzer können über **Support > NSS-Verwaltung** auf diese Anmeldeinformationen zugreifen.

Hinzufügen eines NSS-Kontos

Sie können Ihre NetApp Support Site-Konten zur Verwendung mit der Konsole über das Support-Dashboard in der Konsole hinzufügen und verwalten.

Wenn Sie Ihr NSS-Konto hinzugefügt haben, verwendet die Konsole diese Informationen für Dinge wie Lizenzdownloads, Überprüfung von Software-Upgrades und zukünftige Support-Registrierungen.

Sie können Ihrer Organisation mehrere NSS-Konten zuordnen. Sie können jedoch nicht innerhalb derselben Organisation Kundenkonten und Partnerkonten haben.

NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsdienste speziell für Support und Lizenzierung.

Schritte

1. Unter **Administration > Support**.
2. Wählen Sie **NSS-Verwaltung**.

3. Wählen Sie **NSS-Konto hinzufügen**.
4. Wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite weitergeleitet zu werden.
5. Geben Sie auf der Anmeldeseite Ihre für die NetApp Support-Site registrierte E-Mail-Adresse und Ihr Kennwort ein.

   Nach erfolgreicher Anmeldung speichert NetApp den NSS-Benutzernamen.

   Dies ist eine vom System generierte ID, die Ihrer E-Mail-Adresse zugeordnet ist. Auf der Seite **NSS-Verwaltung** können Sie Ihre E-Mail-Adresse aus dem ••• Speisekarte.

   - Wenn Sie Ihre Anmeldeinformationen aktualisieren müssen, gibt es auch die Option **Anmeldeinformationen aktualisieren** im ••• Speisekarte.

     Bei Verwendung dieser Option werden Sie aufgefordert, sich erneut anzumelden. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Sie werden durch eine entsprechende Benachrichtigung darauf aufmerksam gemacht.

Wie geht es weiter?

Benutzer können jetzt das Konto auswählen, wenn sie neue Cloud Volumes ONTAP -Systeme erstellen und wenn sie vorhandene Cloud Volumes ONTAP -Systeme registrieren.

- "Starten von Cloud Volumes ONTAP in AWS"
- "Starten von Cloud Volumes ONTAP in Azure"
- "Starten von Cloud Volumes ONTAP in Google Cloud"
- "Registrierung von Umlagesystemen"

NSS-Anmeldeinformationen aktualisieren

Aus Sicherheitsgründen müssen Sie Ihre NSS-Anmeldeinformationen alle 90 Tage aktualisieren. Sie werden im Benachrichtigungscenter der Konsole benachrichtigt, wenn Ihre NSS-Anmeldeinformationen abgelaufen sind. "Erfahren Sie mehr über das Benachrichtigungscenter" .

Abgelaufene Anmeldeinformationen können unter anderem Folgendes beeinträchtigen:

- Lizenzaktualisierungen, was bedeutet, dass Sie die neu erworbene Kapazität nicht nutzen können.
- Möglichkeit zum Einreichen und Verfolgen von Supportfällen.

Darüber hinaus können Sie die mit Ihrer Organisation verknüpften NSS-Anmeldeinformationen aktualisieren, wenn Sie das mit Ihrer Organisation verknüpfte NSS-Konto ändern möchten. Zum Beispiel, wenn die mit Ihrem NSS-Konto verknüpfte Person Ihr Unternehmen verlassen hat.

Schritte

1. Unter **Administration > Support**.
2. Wählen Sie **NSS-Verwaltung**.
3. Wählen Sie für das NSS-Konto, das Sie aktualisieren möchten, ••• und wählen Sie dann **Anmeldeinformationen aktualisieren**.
4. Wenn Sie dazu aufgefordert werden, wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite weitergeleitet zu werden.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsdienste im

Zusammenhang mit Support und Lizenzierung.

5. Geben Sie auf der Anmeldeseite Ihre für die NetApp Support-Site registrierte E-Mail-Adresse und Ihr Kennwort ein.

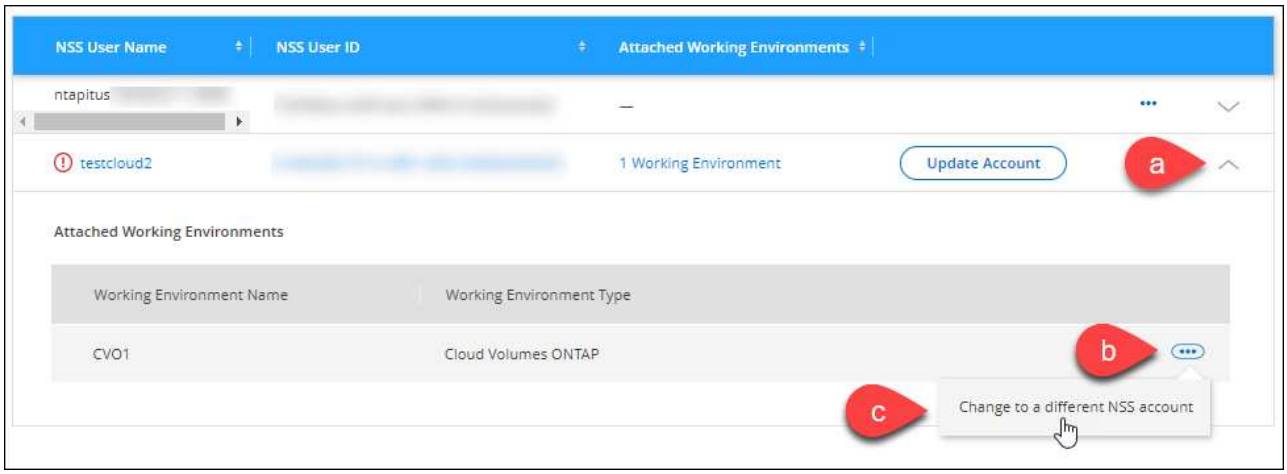
Verbinden Sie ein System mit einem anderen NSS-Konto

Wenn Ihr Unternehmen über mehrere NetApp Support Site-Konten verfügt, können Sie ändern, welches Konto mit einem Cloud Volumes ONTAP -System verknüpft ist.

Sie müssen das Konto zunächst mit der Konsole verknüpft haben.

Schritte

1. Unter **Administration > Support**.
2. Wählen Sie **NSS-Verwaltung**.
3. Führen Sie die folgenden Schritte aus, um das NSS-Konto zu ändern:
   a. Erweitern Sie die Zeile für das NetApp Support Site-Konto, mit dem das System derzeit verknüpft ist.
   b. Wählen Sie für das System, für das Sie die Zuordnung ändern möchten, •••
   c. Wählen Sie **Zu einem anderen NSS-Konto wechseln**.



   d. Wählen Sie das Konto aus und wählen Sie dann **Speichern**.

E-Mail-Adresse für ein NSS-Konto anzeigen

Aus Sicherheitsgründen wird die mit einem NSS-Konto verknüpfte E-Mail-Adresse standardmäßig nicht angezeigt. Sie können die E-Mail-Adresse und den zugehörigen Benutzernamen für ein NSS-Konto anzeigen.

Wenn Sie zur NSS-Verwaltungsseite gehen, generiert die Konsole für jedes Konto in der Tabelle ein Token. Dieses Token enthält Informationen zur zugehörigen E-Mail-Adresse. Das Token wird entfernt, wenn Sie die Seite verlassen. Die Informationen werden niemals zwischengespeichert, was zum Schutz Ihrer Privatsphäre beiträgt.

Schritte

1. Unter **Administration > Support**.
2. Wählen Sie **NSS-Verwaltung**.
3. Wählen Sie für das NSS-Konto, das Sie aktualisieren möchten, ••• und wählen Sie dann **E-Mail-Adresse**

anzeigen. Über die Schaltfläche „Kopieren“ können Sie die E-Mail-Adresse kopieren.

Entfernen eines NSS-Kontos

Löschen Sie alle NSS-Konten, die Sie nicht mehr mit der Konsole verwenden möchten.

Sie können kein Konto löschen, das derzeit mit einem Cloud Volumes ONTAP System verknüpft ist. Sie müssen zuerstVerbinden Sie diese Systeme mit einem anderen NSS-Konto .

Schritte

1. Unter **Administration > Support**.
2. Wählen Sie **NSS-Verwaltung**.
3. Wählen Sie für das NSS-Konto, das Sie löschen möchten, ••• und wählen Sie dann **Löschen**.
4. Wählen Sie zur Bestätigung **Löschen**.

Verwalten Sie die mit Ihrer NetApp Console verknüpften Anmeldeinformationen

Abhängig von den Aktionen, die Sie in der Konsole ausgeführt haben, haben Sie möglicherweise ONTAP Anmeldeinformationen und Anmeldeinformationen für die NetApp Support Site (NSS) mit Ihrer Benutzeranmeldung verknüpft. Sie können diese Anmeldeinformationen anzeigen und verwalten, nachdem Sie sie verknüpft haben. Wenn Sie beispielsweise das Kennwort für diese Anmeldeinformationen ändern, müssen Sie das Kennwort in der Konsole aktualisieren.

ONTAP -Anmeldeinformationen

Benutzer benötigen ONTAP Administratoranmeldeinformationen, um ONTAP Cluster in der Konsole zu erkennen. Der Zugriff auf den ONTAP System Manager hängt jedoch davon ab, ob Sie einen Konsolenagenten verwenden oder nicht.

Ohne einen Konsolenagenten

Benutzer werden aufgefordert, ihre ONTAP Anmeldeinformationen einzugeben, um auf den ONTAP System Manager für den Cluster zuzugreifen. Benutzer können diese Anmeldeinformationen in der Konsole speichern, sodass sie nicht jedes Mal aufgefordert werden, sie einzugeben. Benutzeranmeldeinformationen sind nur für den jeweiligen Benutzer sichtbar und können auf der Seite „Benutzeranmeldeinformationen“ verwaltet werden.

Mit einem Konsolenagenten

Standardmäßig werden Benutzer nicht aufgefordert, ihre ONTAP Anmeldeinformationen einzugeben, um auf den ONTAP System Manager zuzugreifen. Ein Konsolenadministrator (mit der Rolle „Organisationsadministrator“) kann die Konsole jedoch so konfigurieren, dass Benutzer aufgefordert werden, ihre ONTAP Anmeldeinformationen einzugeben. Wenn diese Einstellung aktiviert ist, müssen Benutzer jedes Mal ihre ONTAP Anmeldeinformationen eingeben.

"Erfahren Sie mehr."

NSS -Anmeldeinformationen

Die mit Ihrer NetApp Console Anmeldung verknüpften NSS-Anmeldeinformationen ermöglichen die Support-Registrierung, das Fallmanagement und den Zugriff auf Digital Advisor.

- Wenn Sie auf **Support > Ressourcen** zugreifen und sich für den Support registrieren, werden Sie

aufgefordert, NSS-Anmeldeinformationen mit Ihrem Login zu verknüpfen.

Dadurch wird Ihre Organisation oder Ihr Konto für den Support registriert und der Supportanspruch aktiviert. Nur ein Benutzer in Ihrer Organisation muss seinem Login ein NetApp Support Site-Konto zuordnen, um sich für den Support zu registrieren und den Supportanspruch zu aktivieren. Nachdem dies abgeschlossen ist, wird auf der Seite **Ressourcen** angezeigt, dass Ihr Konto für den Support registriert ist.

"Erfahren Sie, wie Sie sich für den Support registrieren"

- Wenn Sie auf **Administration > Support > Fallmanagement** zugreifen, werden Sie aufgefordert, Ihre NSS-Anmeldeinformationen einzugeben, falls Sie dies nicht bereits getan haben. Auf dieser Seite können Sie die mit Ihrem NSS-Konto und Ihrem Unternehmen verbundenen Supportfälle erstellen und verwalten.
- Wenn Sie in der Konsole auf Digital Advisor zugreifen, werden Sie aufgefordert, sich bei Digital Advisor anzumelden, indem Sie Ihre NSS-Anmeldeinformationen eingeben.

Beachten Sie Folgendes zum NSS-Konto, das mit Ihrer Anmeldung verknüpft ist:

- Das Konto wird auf Benutzerebene verwaltet, was bedeutet, dass es für andere Benutzer, die sich anmelden, nicht sichtbar ist.
- Pro Benutzer kann nur ein NSS-Konto mit Digital Advisor und Support-Fallmanagement verknüpft sein.
- Wenn Sie versuchen, ein NetApp Support Site-Konto mit einem Cloud Volumes ONTAP -System zu verknüpfen, können Sie nur aus den NSS-Konten auswählen, die der Organisation hinzugefügt wurden, deren Mitglied Sie sind.

  Die Anmeldeinformationen auf NSS-Kontoebene unterscheiden sich von dem NSS-Konto, das mit Ihrer Anmeldung verknüpft ist. Mit den Anmeldeinformationen auf NSS-Kontoebene können Sie Cloud Volumes ONTAP mit BYOL bereitstellen, PAYGO-Systeme registrieren und die Software aktualisieren.

  "Erfahren Sie mehr über die Verwendung von NSS-Anmeldeinformationen mit Ihrer NetApp Console -Organisation oder Ihrem NetApp Console-Konto" .

Verwalten Sie Ihre Benutzeranmeldeinformationen

Verwalten Sie Ihre Benutzeranmeldeinformationen, indem Sie den Benutzernamen und das Kennwort aktualisieren oder die Anmeldeinformationen löschen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wenn Sie noch keine Benutzeranmeldeinformationen haben, können Sie **NSS-Anmeldeinformationen hinzufügen** auswählen, um Ihr NetApp Support Site-Konto hinzuzufügen.
4. Verwalten Sie vorhandene Anmeldeinformationen, indem Sie im Menü „Aktionen“ die folgenden Optionen auswählen:
   - **Anmeldeinformationen aktualisieren**: Aktualisieren Sie den Benutzernamen und das Kennwort für das Konto.
   - **Anmeldeinformationen löschen**: Entfernen Sie das mit Ihrer Konsolenanmeldung verknüpfte NSS-Konto.

Konsolenagenten

Erfahren Sie mehr über NetApp Console -Agenten

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

Ein Konsolenagent ermöglicht Ihnen Folgendes:

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

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

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

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

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

[1] Die Lebenszyklusplanung kann auch ohne Konsolenagent angezeigt werden, jedoch ist ein Konsolenagent erforderlich, um Aktionen auszulösen.

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

Konsolenagenten erforderlich.

Konsolenagenten müssen jederzeit betriebsbereit sein

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

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

Unterstützte Standorte

Sie können Agenten an den folgenden Orten installieren:

- Amazon Web Services
- Microsoft Azure

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

- Google Cloud

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

- Bei Ihnen vor Ort

Kommunikation mit Cloud-Anbietern

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

Eingeschränkter Modus

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

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

So installieren Sie einen Konsolenagenten

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

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

Cloud-Anbieter-Berechtigungen

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

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

Informationen zum Einrichten von Berechtigungen finden Sie hier:

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

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

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

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

Agent-Upgrades

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

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

Betriebssystem- und VM-Wartung

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

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

Wenn Sie (der Kunde) die Konsolen-Agent-VM stoppen und dann starten müssen, sollten Sie dies über die Konsole Ihres Cloud-Anbieters oder mithilfe der Standardverfahren für die lokale Verwaltung tun.

Der Konsolenagent muss jederzeit betriebsbereit sein .

Mehrere Systeme und Agenten

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

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

Hier sind einige Beispiele für Agentenbereitstellungen:

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

Bereitstellen eines Konsolenagenten

AWS

Installationsoptionen für Konsolenagenten in AWS

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

Folgende Installationsoptionen stehen zur Verfügung:

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

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

- "Erstellen Sie einen Konsolenagenten aus dem AWS Marketplace"

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

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

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

Erstellen Sie einen Konsolenagenten in AWS über die NetApp Console

Sie können einen Konsolenagenten in AWS direkt von der NetApp Console aus erstellen. Bevor Sie über die Konsole einen Konsolenagenten in AWS erstellen, müssen Sie Ihr Netzwerk einrichten und AWS-Berechtigungen vorbereiten.

Bevor Sie beginnen

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

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

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

VPC und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)	Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab. "Weitere Einzelheiten finden Sie in der AWS-Dokumentation."
Amazon FsX für NetApp ONTAP: • api.workloads.netapp.com	Die webbasierte Konsole kontaktiert diesen Endpunkt, um mit den Workload Factory APIs zu interagieren und so FSx for ONTAP basierte Workloads zu verwalten und zu betreiben.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.

Endpunkte	Zweck
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. • Wenn Sie einen neuen Agenten bereitstellen, testet die Validierungsprüfung die Konnektivität zu aktuellen Endpunkten. Wenn Sie"vorherige Endpunkte" , schlägt die Validierungsprüfung fehl. Um diesen Fehler zu vermeiden, überspringen Sie die Validierungsprüfung. Obwohl die vorherigen Endpunkte weiterhin unterstützt werden, empfiehlt NetApp , Ihre Firewall-Regeln so schnell wie möglich auf die aktuellen Endpunkte zu aktualisieren. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" . • Wenn Sie auf die aktuellen Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Von der NetApp Konsole kontaktierte Endpunkte

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

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

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

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

Aktivieren von NTP

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

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

Schritt 2: AWS-Berechtigungen für den Konsolenagenten einrichten

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

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

über die erforderlichen Berechtigungen verfügt.

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

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

Schritte

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

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "kms:ListAliases",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:TerminateInstances"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/OCCMInstance": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

5. Wählen Sie **Weiter** und fügen Sie bei Bedarf Tags hinzu.

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

Ergebnis

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

Schritt 3: Erstellen des Konsolenagenten

Erstellen Sie den Konsolenagenten direkt von der webbasierten Konsole aus.

Informationen zu diesem Vorgang

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

Schritte

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

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

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

   Stellen Sie sicher, dass Sie über das richtige Schlüsselpaar für den Zugriff auf die virtuelle Maschine des Konsolenagenten verfügen. Ohne Schlüsselpaar ist ein Zugriff nicht möglich.

8. Wählen Sie auf der Seite **Sicherheitsgruppe** aus, ob Sie eine neue Sicherheitsgruppe erstellen oder eine vorhandene Sicherheitsgruppe auswählen möchten, die die erforderlichen eingehenden und ausgehenden Regeln zulässt.

   "Sicherheitsgruppenregeln für AWS anzeigen" .

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

   a. Das Kontrollkästchen **Agentenkonfiguration validieren** ist standardmäßig aktiviert, damit die Konsole bei der Bereitstellung die Anforderungen an die Netzwerkkonnektivität validiert. Wenn die

Bereitstellung des Agenten durch die Konsole fehlschlägt, wird ein Bericht bereitgestellt, der Sie bei der Fehlerbehebung unterstützt. Wenn die Bereitstellung erfolgreich ist, wird kein Bericht bereitgestellt.

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

10. Wählen Sie **Hinzufügen**.

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

Ergebnis

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

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

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

Erstellen Sie einen Konsolenagenten aus dem AWS Marketplace

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

Bevor Sie beginnen

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

Schritt 1: Einrichten des Netzwerks

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

VPC und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)	Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab. "Weitere Einzelheiten finden Sie in der AWS-Dokumentation."
Amazon FsX für NetApp ONTAP: • api.workloads.netapp.com	Die webbasierte Konsole kontaktiert diesen Endpunkt, um mit den Workload Factory APIs zu interagieren und so FSx for ONTAP basierte Workloads zu verwalten und zu betreiben.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.

Endpunkte	Zweck
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. • Wenn Sie einen neuen Agenten bereitstellen, testet die Validierungsprüfung die Konnektivität zu aktuellen Endpunkten. Wenn Sie"vorherige Endpunkte" , schlägt die Validierungsprüfung fehl. Um diesen Fehler zu vermeiden, überspringen Sie die Validierungsprüfung. Obwohl die vorherigen Endpunkte weiterhin unterstützt werden, empfiehlt NetApp , Ihre Firewall-Regeln so schnell wie möglich auf die aktuellen Endpunkte zu aktualisieren. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" . • Wenn Sie auf die aktuellen Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

- HTTP (80) und HTTPS (443) ermöglichen den Zugriff auf die lokale Benutzeroberfläche, die Sie in

seltenen Fällen verwenden werden.

- SSH (22) wird nur benötigt, wenn Sie zur Fehlerbehebung eine Verbindung zum Host herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP -Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

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

Aktivieren von NTP

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

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

Schritt 2: AWS-Berechtigungen einrichten

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

Schritte

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

      Möglicherweise müssen Sie basierend auf den NetApp -Datendiensten, die Sie verwenden möchten, eine zweite Richtlinie erstellen. Für Standardregionen sind die Berechtigungen auf zwei Richtlinien verteilt. Aufgrund einer maximalen Zeichengrößenbeschränkung für verwaltete Richtlinien in AWS sind zwei Richtlinien erforderlich. "Weitere Informationen zu IAM-Richtlinien für den Konsolenagenten" .
3. Erstellen Sie eine IAM-Rolle:
   a. Wählen Sie **Rollen > Rolle erstellen**.
   b. Wählen Sie **AWS-Dienst > EC2**.
   c. Fügen Sie Berechtigungen hinzu, indem Sie die gerade erstellte Richtlinie anhängen.
   d. Führen Sie die restlichen Schritte aus, um die Rolle zu erstellen.

Ergebnis

Sie verfügen jetzt über eine IAM-Rolle, die Sie während der Bereitstellung vom AWS Marketplace aus mit der EC2-Instance verknüpfen können.

Schritt 3: Überprüfen der Instanzanforderungen

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

CPU
8 Kerne oder 8 vCPUs

RAM
32 GB

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

Schritt 4: Erstellen des Konsolenagenten

Erstellen Sie den Konsolenagenten direkt vom AWS Marketplace.

Informationen zu diesem Vorgang

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Eine VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt.
- Eine IAM-Rolle mit einer angehängten Richtlinie, die die erforderlichen Berechtigungen für den Konsolenagenten enthält.
- Berechtigungen zum Abonnieren und Abbestellen des AWS Marketplace für Ihren IAM-Benutzer.
- Ein Verständnis der CPU- und RAM-Anforderungen für die Instanz.
- Ein Schlüsselpaar für die EC2-Instanz.

Schritte

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

   Der Abonnementvorgang kann einige Minuten dauern.

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

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

7. Folgen Sie den Anweisungen zum Konfigurieren und Bereitstellen der Instanz:

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

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

  Wenn Sie die Amazon EBS-Verschlüsselung auf dem Stammvolume aktivieren möchten, wählen Sie **Erweitert**, erweitern Sie **Volume 1**, wählen Sie **Verschlüsselt** und wählen Sie dann einen KMS-Schlüssel.
- **Erweiterte Details**: Wählen Sie unter **IAM-Instanzprofil** die IAM-Rolle aus, die die erforderlichen Berechtigungen für den Konsolenagenten enthält.
- **Zusammenfassung**: Überprüfen Sie die Zusammenfassung und wählen Sie **Instanz starten**.

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

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

8. Öffnen Sie einen Webbrowser auf einem Host, der über eine Verbindung zur virtuellen Maschine des Konsolen-Agenten und zur URL des Konsolen-Agenten verfügt.
9. Richten Sie nach der Anmeldung den Konsolenagenten ein:
   a. Geben Sie die Konsolenorganisation an, die mit dem Konsolenagenten verknüpft werden soll.
   b. Geben Sie einen Namen für das System ein.
   c. Lassen Sie unter **Arbeiten Sie in einer sicheren Umgebung?** den eingeschränkten Modus deaktiviert.

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

Ergebnis

Der Konsolenagent ist jetzt installiert und mit Ihrer Konsolenorganisation eingerichtet.

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

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

Manuelle Installation des Konsolenagenten in AWS

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

Bevor Sie beginnen

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

Schritt 1: Hostanforderungen prüfen

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

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

Dedizierter Host

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

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

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

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

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

AWS EC2-Instanztyp

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

Hypervisor

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

Betriebssystem- und Containeranforderungen

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

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

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

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

Schlüsselpaar

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

PUT-Antwort-Hop-Limit bei Verwendung von IMDSv2

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

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

Schritt 2: Installieren Sie Podman oder Docker Engine

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

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

  Sehen Sie sich die unterstützten Podman-Versionen an .

- Für Ubuntu ist Docker Engine erforderlich.

  Anzeigen der unterstützten Docker Engine-Versionen .

Beispiel 1. Schritte

Podman

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

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

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

Schritte

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

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

2. Installieren Sie Podman.

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

   a. Für Red Hat Enterprise Linux 9,6:

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

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

   b. Für Red Hat Enterprise Linux 9.1 bis 9.4:

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

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

   c. Für Red Hat Enterprise Linux 8:

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

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

unterstützten Podman-Versionen an .

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

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

4. Installieren Sie python3.

```
sudo dnf install python3
```

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

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

6. Bei Verwendung von Red Hat Enterprise 9:

   a. Installieren Sie das EPEL-Repository-Paket.

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

   +

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

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

7. Bei Verwendung von Red Hat Enterprise Linux 8:

   a. Installieren Sie das EPEL-Repository-Paket.

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

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

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. Starten Sie Podman neu.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker-Engine

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

Schritte

1. "Installationsanweisungen von Docker anzeigen"

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

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

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

Schritt 3: Einrichten des Netzwerks

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Von Computern kontaktierte Endpunkte bei Verwendung der webbasierten NetApp Console

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

"Vorbereiten des Netzwerks für die NetApp Konsole" .

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)	Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab. "Weitere Einzelheiten finden Sie in der AWS-Dokumentation."
Amazon FsX für NetApp ONTAP: • api.workloads.netapp.com	Die webbasierte Konsole kontaktiert diesen Endpunkt, um mit den Workload Factory APIs zu interagieren und so FSx for ONTAP basierte Workloads zu verwalten und zu betreiben.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.

Endpunkte	Zweck
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. • Wenn Sie einen neuen Agenten bereitstellen, testet die Validierungsprüfung die Konnektivität zu aktuellen Endpunkten. Wenn Sie"vorherige Endpunkte" , schlägt die Validierungsprüfung fehl. Um diesen Fehler zu vermeiden, überspringen Sie die Validierungsprüfung. Obwohl die vorherigen Endpunkte weiterhin unterstützt werden, empfiehlt NetApp , Ihre Firewall-Regeln so schnell wie möglich auf die aktuellen Endpunkte zu aktualisieren. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" . • Wenn Sie auf die aktuellen Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

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

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

Aktivieren von NTP

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

Schritt 4: AWS-Berechtigungen für die Konsole einrichten

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

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

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

IAM-Rolle

Schritte

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

      Abhängig von den NetApp -Datendiensten, die Sie verwenden möchten, müssen Sie möglicherweise eine zweite Richtlinie erstellen. Für Standardregionen sind die Berechtigungen auf zwei Richtlinien verteilt. Aufgrund einer maximalen Zeichengrößenbeschränkung für verwaltete Richtlinien in AWS sind zwei Richtlinien erforderlich. "Weitere Informationen zu IAM-Richtlinien für den Konsolenagenten" .
3. Erstellen Sie eine IAM-Rolle:
   a. Wählen Sie **Rollen > Rolle erstellen**.
   b. Wählen Sie **AWS-Dienst > EC2**.
   c. Fügen Sie Berechtigungen hinzu, indem Sie die gerade erstellte Richtlinie anhängen.
   d. Führen Sie die restlichen Schritte aus, um die Rolle zu erstellen.

Ergebnis

Sie verfügen jetzt über eine IAM-Rolle, die Sie nach der Installation des Konsolenagenten mit der EC2-Instance verknüpfen können.

AWS-Zugriffsschlüssel

Schritte

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

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

   Für Standardregionen sind die Berechtigungen auf zwei Richtlinien verteilt. Aufgrund einer maximalen Zeichengrößenbeschränkung für verwaltete Richtlinien in AWS sind zwei Richtlinien erforderlich. "Weitere Informationen zu IAM-Richtlinien für den Konsolenagenten" .
3. Hängen Sie die Richtlinien an einen IAM-Benutzer an.
   - "AWS-Dokumentation: Erstellen von IAM-Rollen"
   - "AWS-Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"
4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie der NetApp

Console hinzufügen können, nachdem Sie den Konsolen-Agenten installiert haben.

Ergebnis

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

Schritt 5: Installieren des Konsolenagenten

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

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

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

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

Informationen zu diesem Vorgang

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

Schritte

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

   ```
   unset http_proxy
   unset https_proxy
   ```

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

2. Laden Sie die Console-Agent-Software herunter und kopieren Sie sie anschließend auf den Linux-Host. Sie können es entweder von der NetApp Console oder von der NetApp -Support-Website herunterladen.
   - NetApp Console: Gehen Sie zu **Agents > Management > Agent bereitstellen > On-Premise > Manuelle Installation**.

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

   - NetApp Supportseite (erforderlich, falls Sie noch keinen Zugriff auf die Konsole haben) "NetApp Support Site" ,
3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

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

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

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

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

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

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

+

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

+

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

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

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

+ Beachten Sie Folgendes:

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

+ Zum Beispiel:

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

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

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

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

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

      Beispiel:

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

   a. Starten Sie die virtuelle Maschine des Konsolenagenten neu.

2. Warten Sie, bis die Installation abgeschlossen ist.

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

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

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

   https://ipaddress

2. Richten Sie nach der Anmeldung den Konsolenagenten ein:

   a. Geben Sie die Organisation an, die mit dem Konsolenagenten verknüpft werden soll.

   b. Geben Sie einen Namen für das System ein.

   c. Lassen Sie unter **Arbeiten Sie in einer sicheren Umgebung?** den eingeschränkten Modus deaktiviert.

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

   d. Wählen Sie **Los geht’s**.

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

Schritt 6: Berechtigungen für die NetApp Console erteilen

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

IAM-Rolle

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

Schritte

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

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

AWS-Zugriffsschlüssel

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

Schritte

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

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

Azurblau

Installationsoptionen für den Konsolen-Agenten in Azure

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

gängigste Weg ist die direkte Nutzung der NetApp Console .

Folgende Installationsoptionen stehen zur Verfügung:

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

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

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

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

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

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

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

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

Bevor Sie beginnen

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

Schritt 1: Einrichten des Netzwerks

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

Azure-Region

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

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

VNet und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Zum Verwalten von Ressourcen in öffentlichen Azure-Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Zum Verwalten von Ressourcen in Azure China-Regionen.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.

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

Von der NetApp Konsole kontaktierte Endpunkte

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

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

verwendet.

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

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

Aktivieren von NTP

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

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

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

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

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

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

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

Schritte

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

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

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

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

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

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

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

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

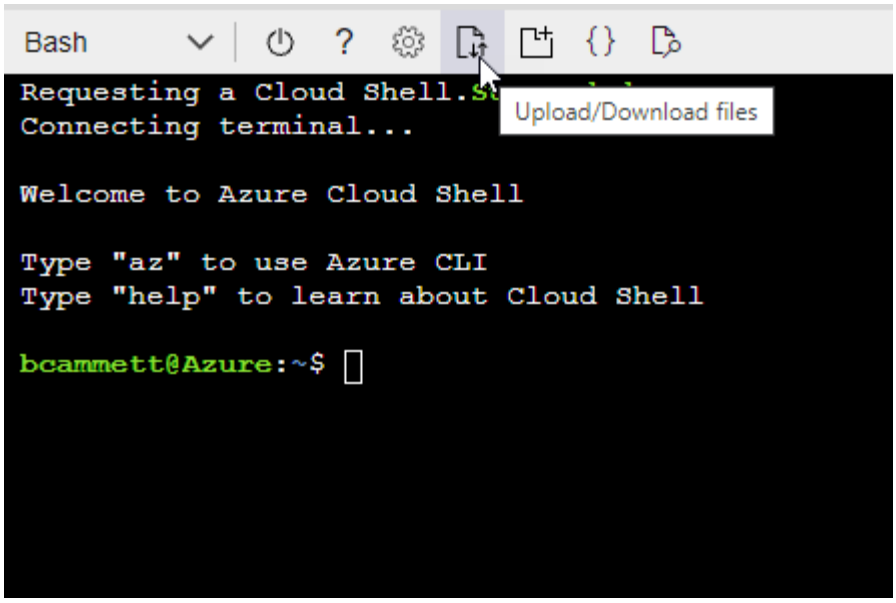
   Beispiel

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

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

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

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



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

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

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

Schritt 3: Authentifizierung einrichten

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

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

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

Azure-Konto

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

Schritte

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

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

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

Dienstprinzipal

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

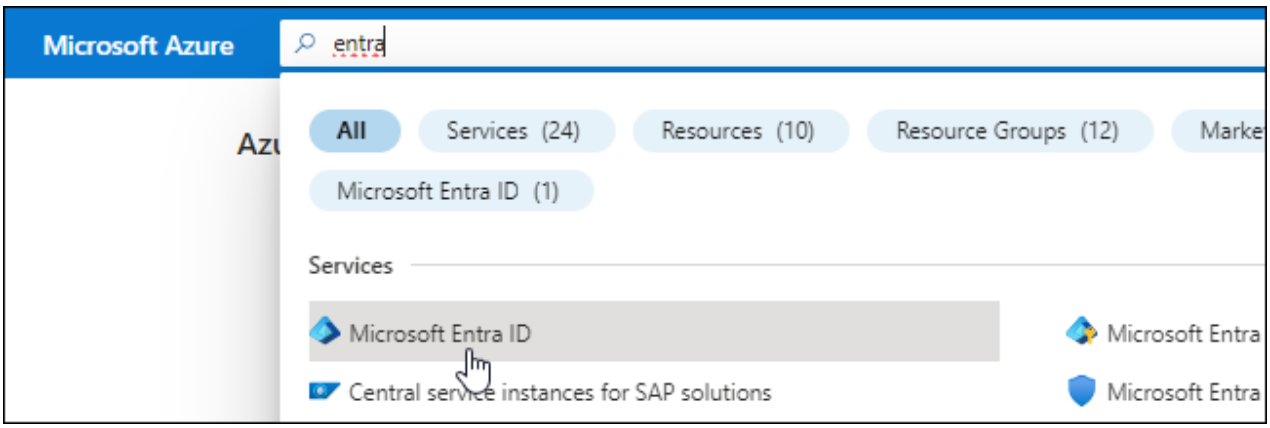
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die die Konsole benötigt.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffskontrolle

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

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

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



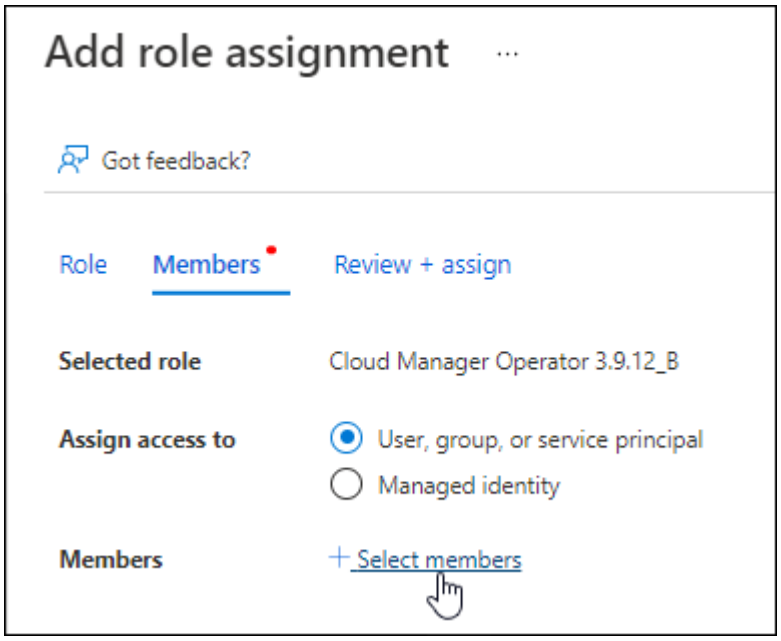
3. Wählen Sie im Menü **App-Registrierungen** aus.
4. Wählen Sie **Neuregistrierung**.
5. Geben Sie Details zur Anwendung an:
   - **Name**: Geben Sie einen Namen für die Anwendung ein.
   - **Kontotyp**: Wählen Sie einen Kontotyp aus (alle funktionieren mit der NetApp Console).
   - **Umleitungs-URI**: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

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der benutzerdefinierten Rolle zur Anwendung

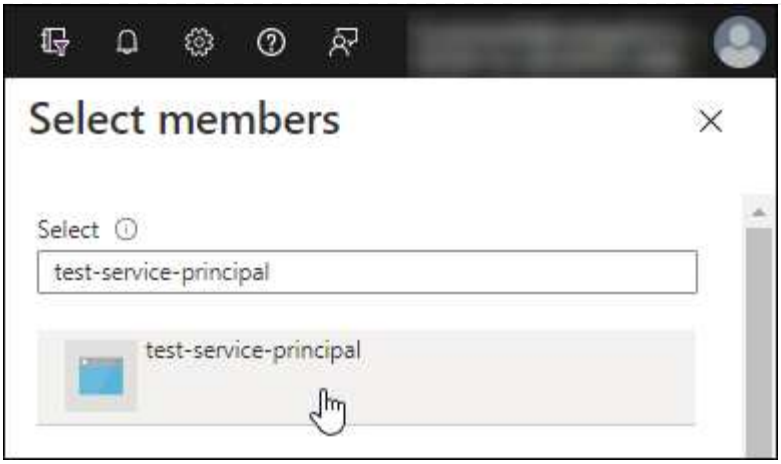
1. Öffnen Sie im Azure-Portal den Dienst **Abonnements**.
2. Wählen Sie das Abonnement aus.
3. Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
4. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenoperator** aus und klicken Sie auf **Weiter**.
5. Führen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

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



   c. Suchen Sie nach dem Namen der Anwendung.

      Hier ist ein Beispiel:



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

b. Klicken Sie auf **Weiter**.

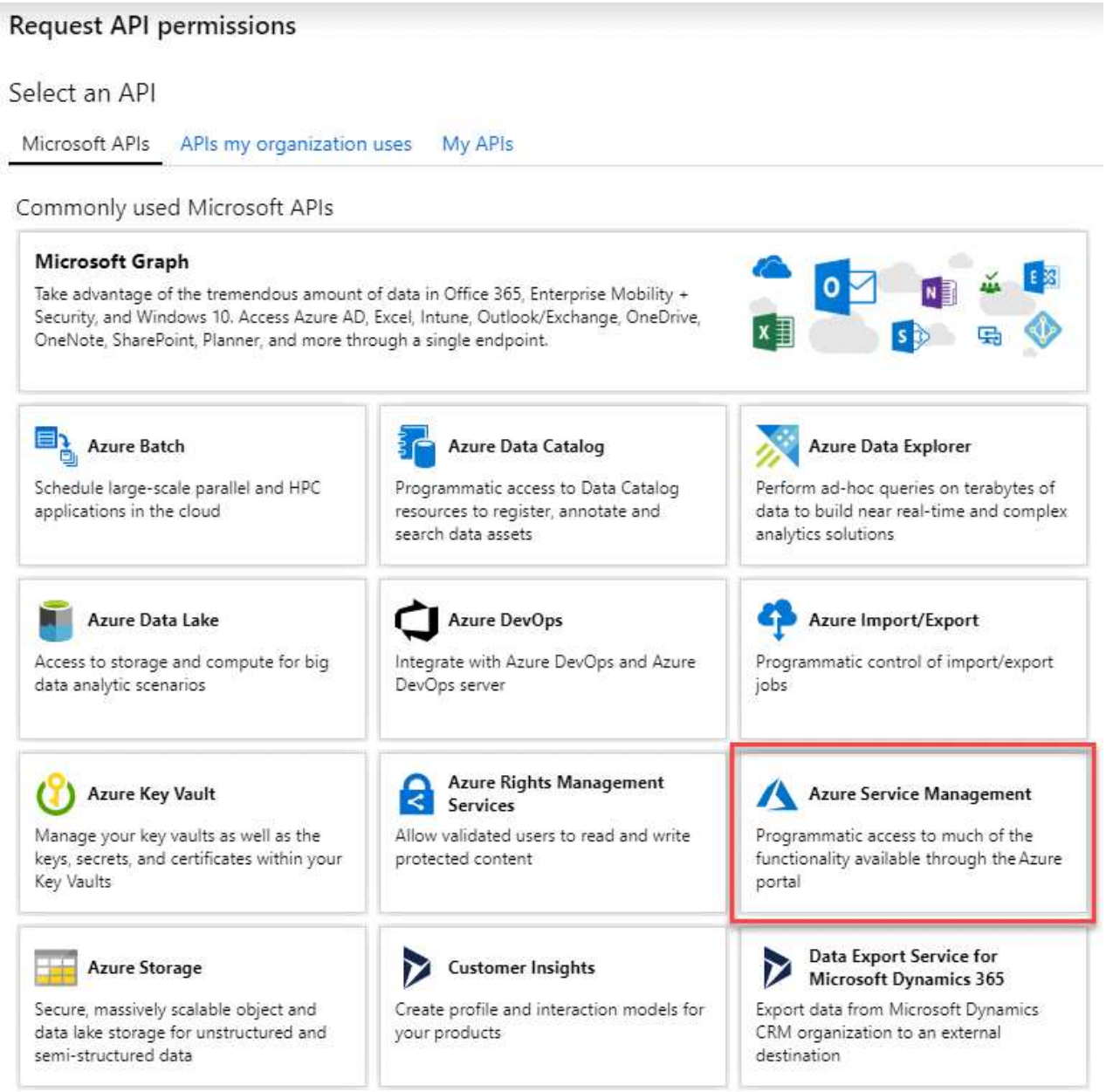
6. Klicken Sie auf **Überprüfen + zuweisen**.

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

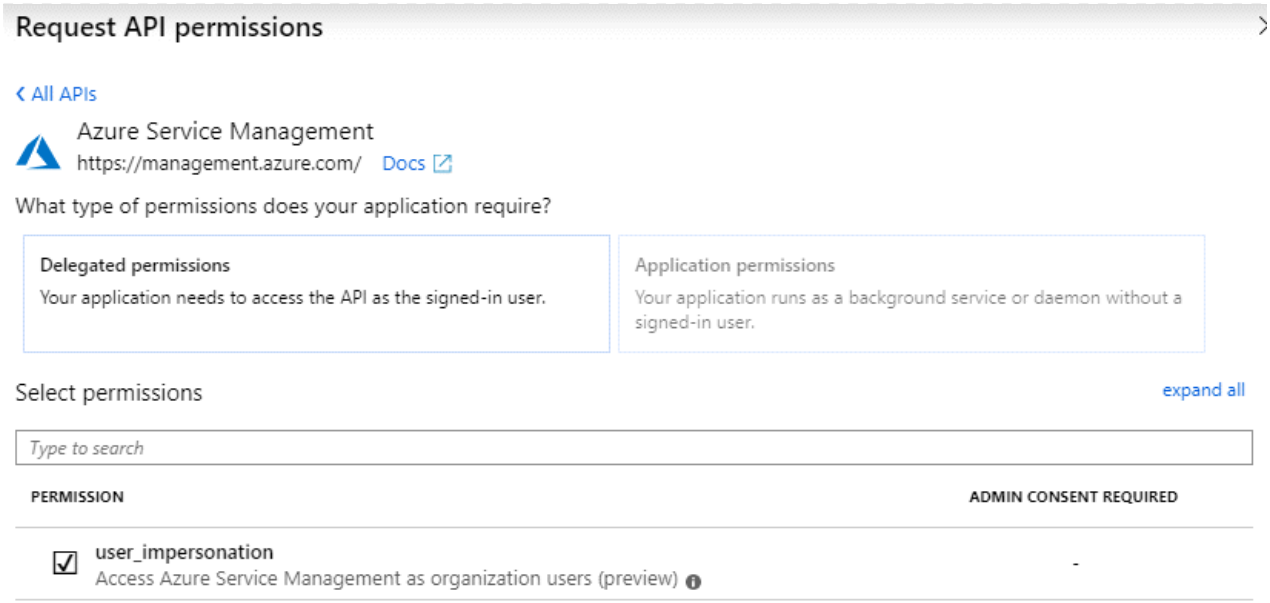
   Wenn Sie Ressourcen in mehreren Azure-Abonnements verwalten möchten, müssen Sie den Dienstprinzipal an jedes dieser Abonnements binden. Beispielsweise können Sie in der Konsole das Abonnement auswählen, das Sie bei der Bereitstellung von Cloud Volumes ONTAP verwenden möchten.

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

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

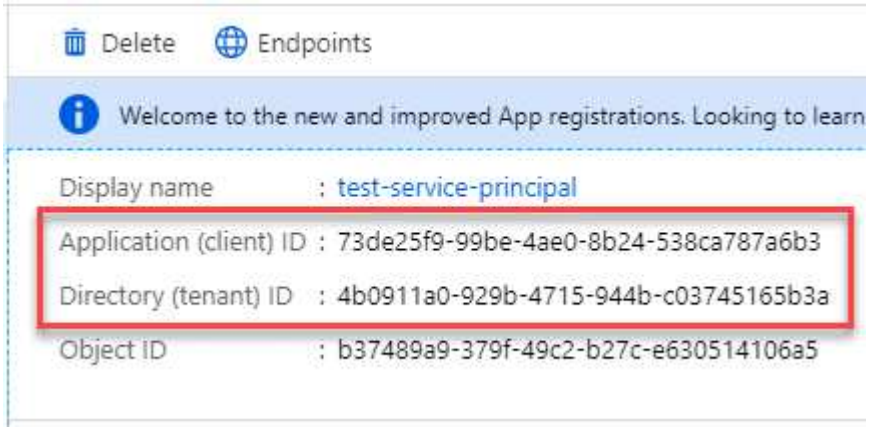


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

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



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

Erstellen eines Client-Geheimnisses

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

Ergebnis

Ihr Dienstprinzipal ist jetzt eingerichtet und Sie sollten die Anwendungs-ID (Client-ID), die Verzeichnis-ID (Mandanten-ID) und den Wert des Client-Geheimnisses kopiert haben. Sie müssen diese Informationen in die Konsole eingeben, wenn Sie den Konsolenagenten erstellen.

Schritt 4: Erstellen des Konsolenagenten

Erstellen Sie den Konsolenagenten direkt von der NetApp Console aus.

Informationen zu diesem Vorgang

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

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

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

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

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

Schritte

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

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

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

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

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

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

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

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

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

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

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

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

"Anzeigen von Sicherheitsgruppenregeln für Azure" .

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

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

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

9. Wählen Sie **Hinzufügen**.

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

Ergebnis

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

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

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

Erstellen eines Konsolen-Agents aus dem Azure Marketplace

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

Bevor Sie beginnen

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

Schritt 1: Einrichten des Netzwerks

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

Azure-Region

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

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

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

VNet und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Zum Verwalten von Ressourcen in öffentlichen Azure-Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Zum Verwalten von Ressourcen in Azure China-Regionen.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.

Endpunkte	Zweck
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. • Wenn Sie einen neuen Agenten bereitstellen, testet die Validierungsprüfung die Konnektivität zu aktuellen Endpunkten. Wenn Sie"vorherige Endpunkte" , schlägt die Validierungsprüfung fehl. Um diesen Fehler zu vermeiden, überspringen Sie die Validierungsprüfung. Obwohl die vorherigen Endpunkte weiterhin unterstützt werden, empfiehlt NetApp , Ihre Firewall-Regeln so schnell wie möglich auf die aktuellen Endpunkte zu aktualisieren. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" . • Wenn Sie auf die aktuellen Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

- HTTP (80) und HTTPS (443) ermöglichen den Zugriff auf die lokale Benutzeroberfläche, die Sie in

seltenen Fällen verwenden werden.

- SSH (22) wird nur benötigt, wenn Sie zur Fehlerbehebung eine Verbindung zum Host herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP -Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

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

Aktivieren von NTP

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

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

Schritt 2: Überprüfen der VM-Anforderungen

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

CPU

8 Kerne oder 8 vCPUs

RAM

32 GB

Azure-VM-Größe

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

Schritt 3: Berechtigungen einrichten

Sie können Berechtigungen auf folgende Weise erteilen:

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

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

Benutzerdefinierte Rolle

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

Schritte

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

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

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

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

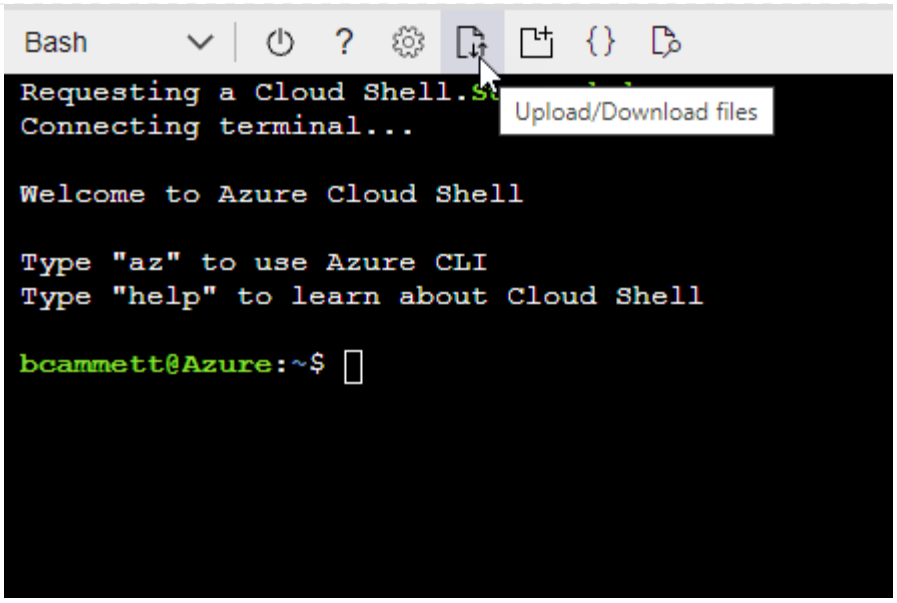
   Beispiel

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

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

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

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



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

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

Dienstprinzipal

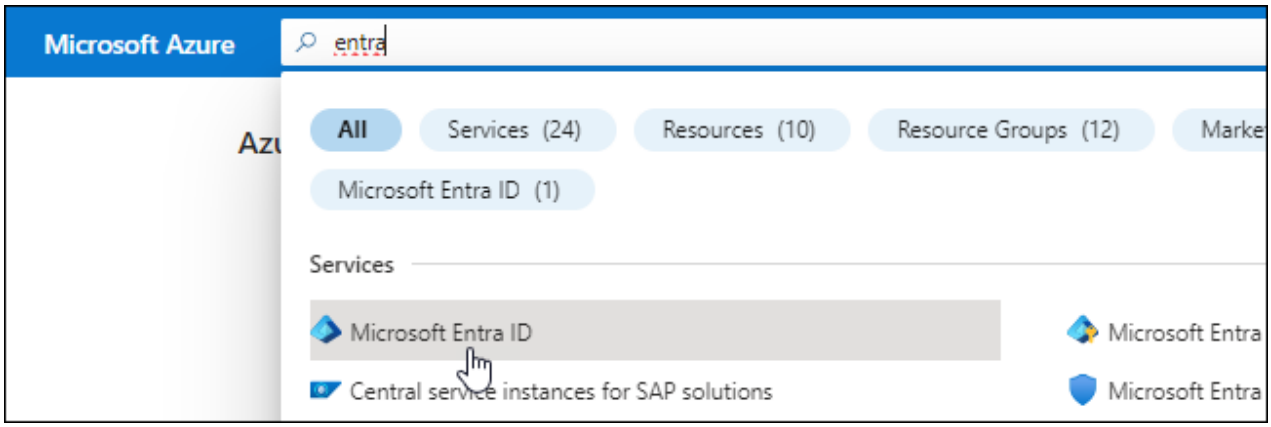
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die die Konsole benötigt.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffskontrolle

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

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

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



3. Wählen Sie im Menü **App-Registrierungen** aus.
4. Wählen Sie **Neuregistrierung**.
5. Geben Sie Details zur Anwendung an:

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

6. Wählen Sie **Registrieren**.

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der Anwendung zu einer Rolle

1. Erstellen Sie eine benutzerdefinierte Rolle:

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

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

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

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

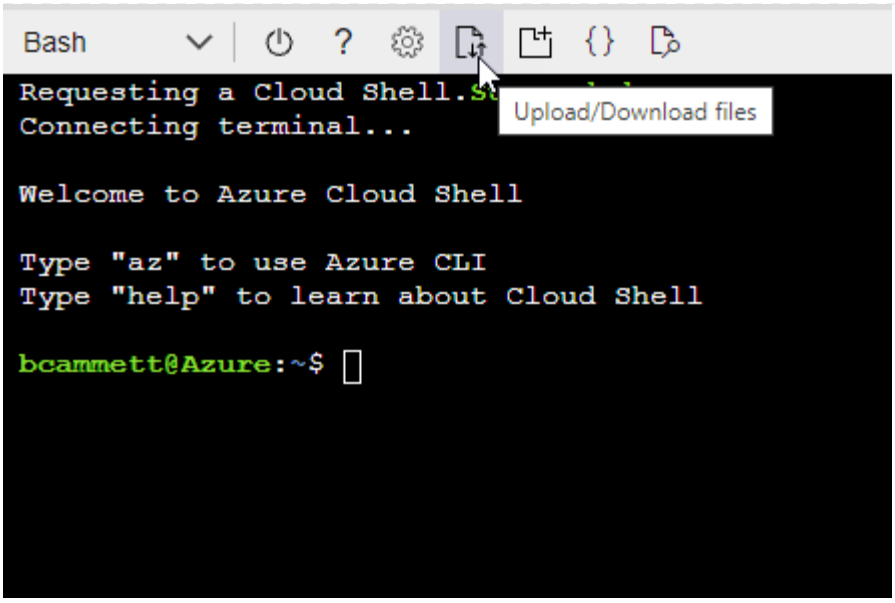
      Beispiel

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

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

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

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



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

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

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

2. Weisen Sie die Anwendung der Rolle zu:

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

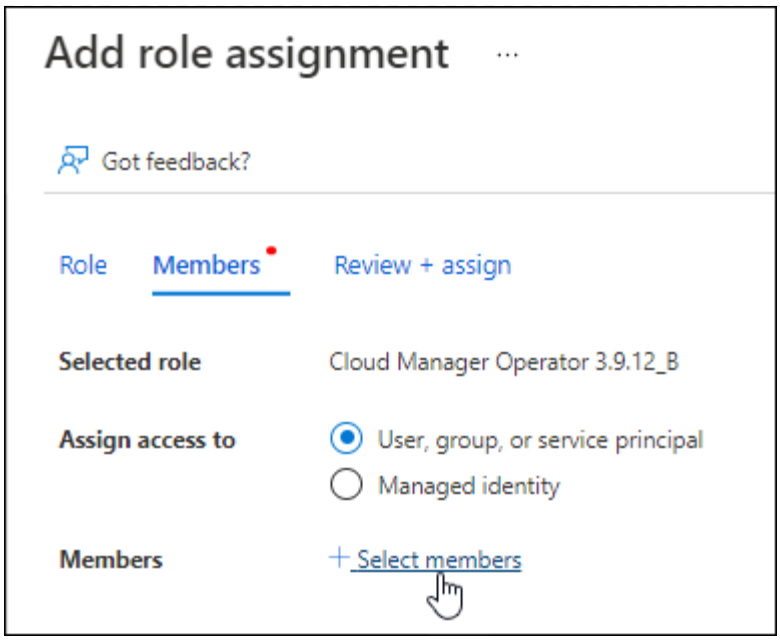
   b. Wählen Sie das Abonnement aus.

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

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

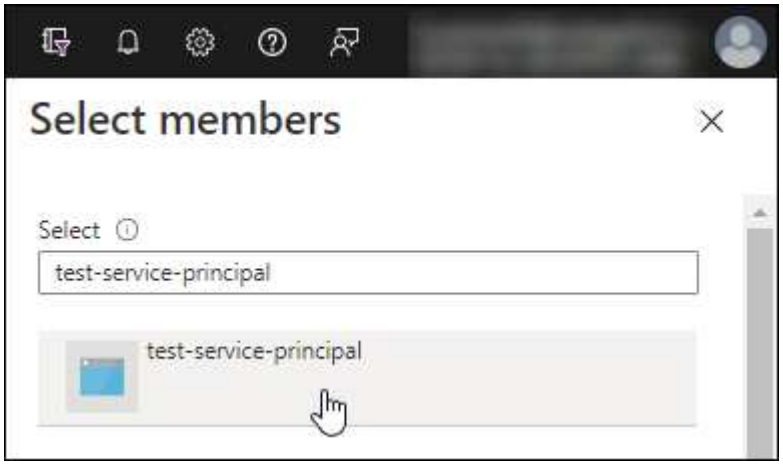
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

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



- Suchen Sie nach dem Namen der Anwendung.

  Hier ist ein Beispiel:



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

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

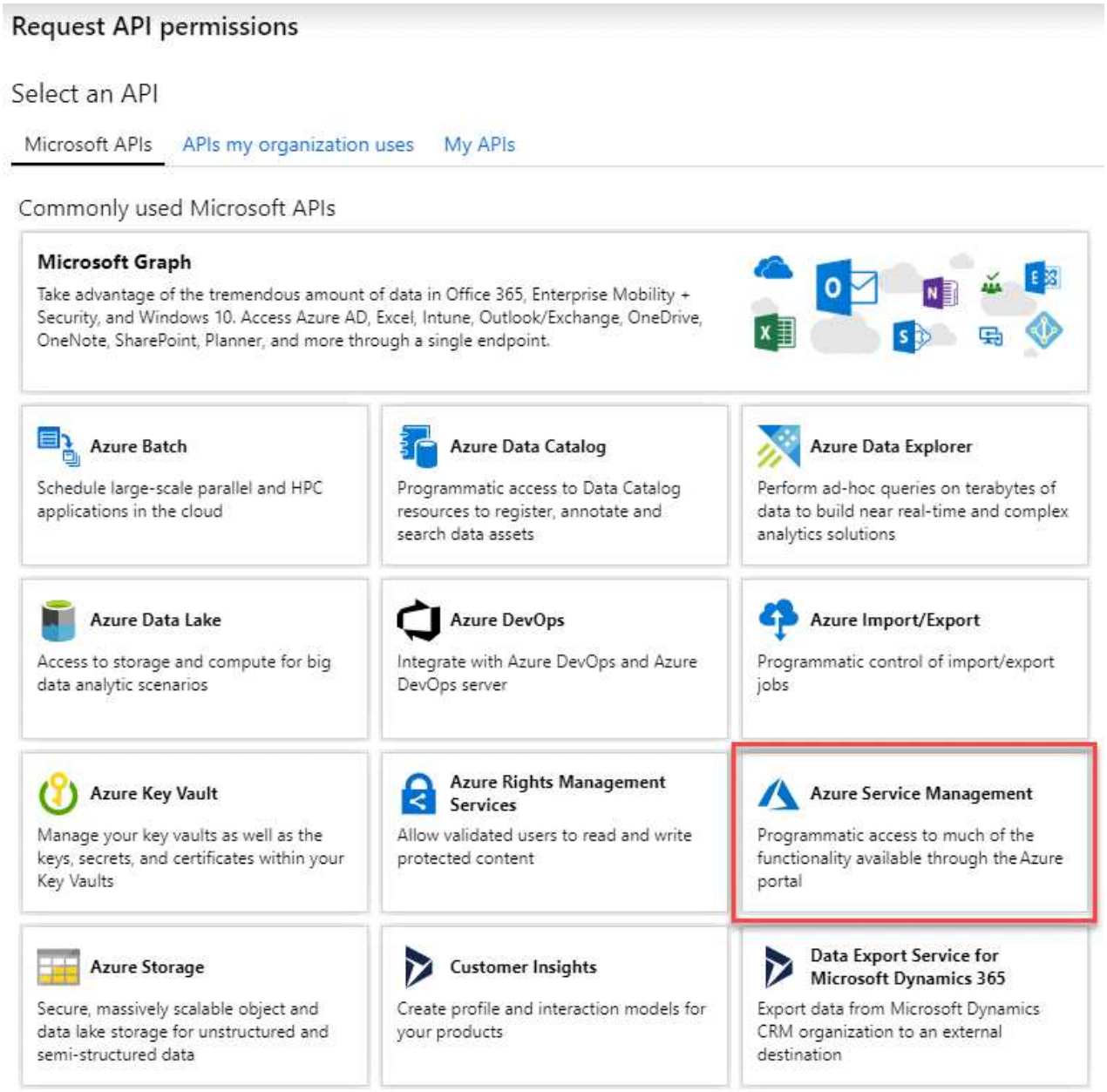
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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

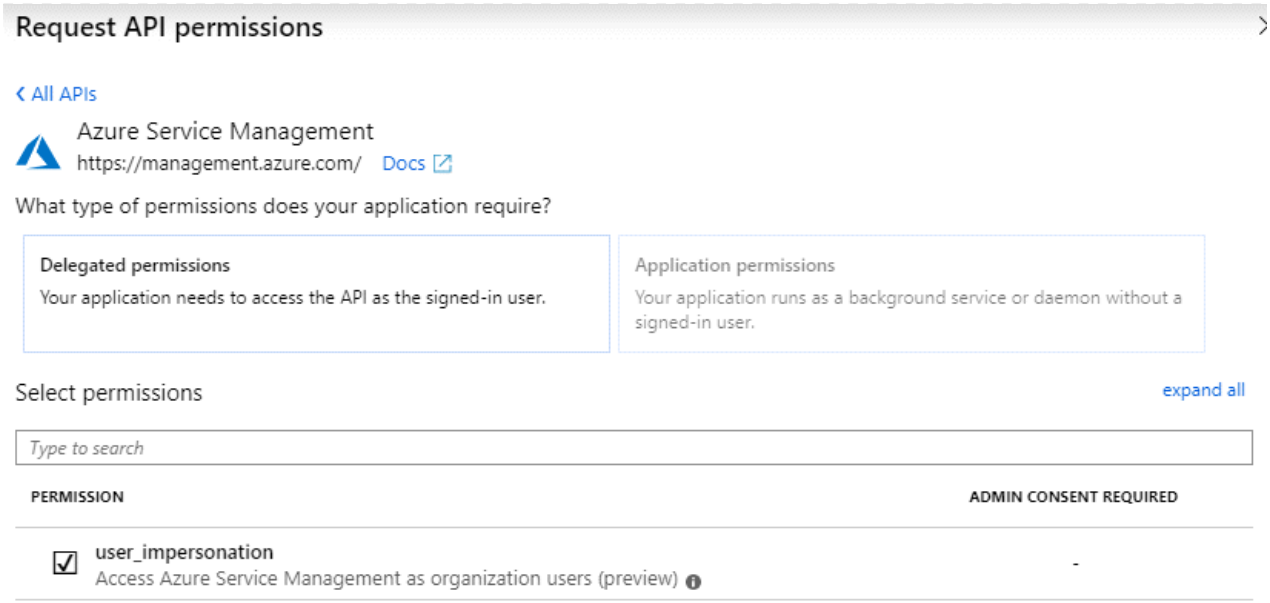
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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

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

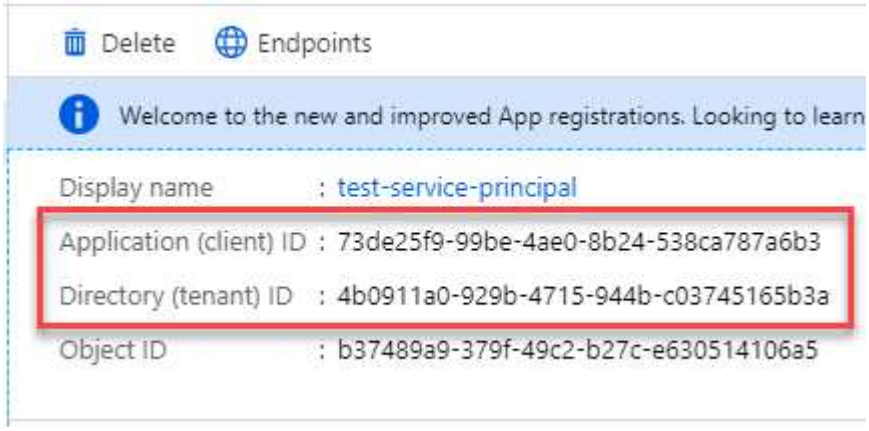


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

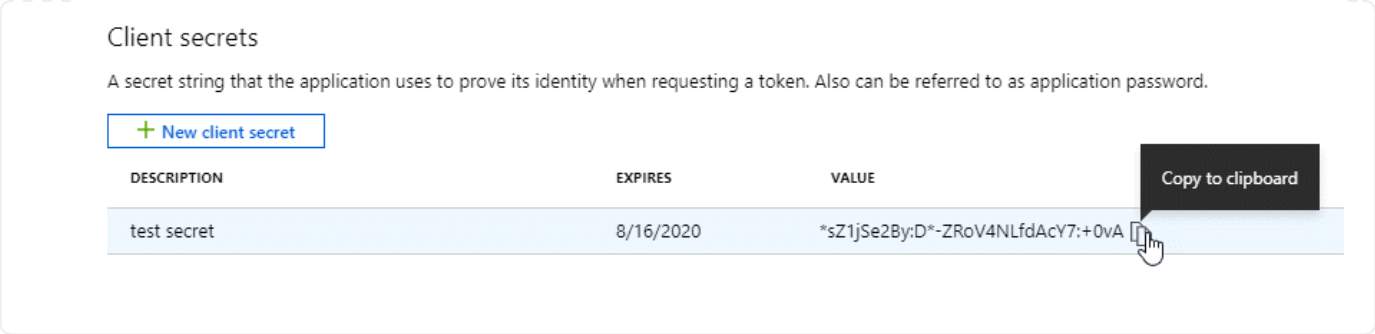
1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



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

Erstellen eines Client-Geheimnisses

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



Schritt 4: Erstellen des Konsolenagenten

Starten Sie den Konsolen-Agent direkt vom Azure Marketplace.

Informationen zu diesem Vorgang

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

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

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

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

Schritte

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

   "Azure Marketplace-Seite für kommerzielle Regionen"

2. Wählen Sie **Jetzt holen** und dann **Weiter**.
3. Wählen Sie im Azure-Portal **Erstellen** aus und befolgen Sie die Schritte zum Konfigurieren der virtuellen Maschine.

Beachten Sie beim Konfigurieren der VM Folgendes:

- **VM-Größe**: Wählen Sie eine VM-Größe, die den CPU- und RAM-Anforderungen entspricht. Wir empfehlen Standard_D8s_v3.
- **Festplatten**: Der Konsolenagent kann mit HDD- oder SSD-Festplatten optimal funktionieren.
- **Netzwerksicherheitsgruppe**: Der Konsolenagent erfordert eingehende Verbindungen über SSH, HTTP und HTTPS.

  "Anzeigen von Sicherheitsgruppenregeln für Azure" .

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

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

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

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

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

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

   https://ipaddress

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

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

   d. Wählen Sie **Los geht's**.

Ergebnis

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

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

Schritt 5: Erteilen Sie dem Konsolenagenten Berechtigungen

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

Benutzerdefinierte Rolle

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

Schritte

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

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

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

2. Wählen Sie **Zugriffskontrolle (IAM)** > **Hinzufügen** > **Rollenzuweisung hinzufügen**.
3. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.

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

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

Wie geht es weiter?

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

Dienstprinzipal

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Microsoft Azure > Agent**.
   b. **Anmeldeinformationen definieren**: Geben Sie Informationen zum Microsoft Entra-Dienstprinzipal ein, der die erforderlichen Berechtigungen erteilt:
      - Anwendungs-ID (Client-ID)
      - Verzeichnis-ID (Mandant)
      - Client-Geheimnis

c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.

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

Ergebnis

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

Manuelles Installieren des Konsolen-Agents in Azure

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

Bevor Sie beginnen

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

Schritt 1: Hostanforderungen prüfen

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

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

Dedizierter Host

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

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

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

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

    Der Konsolenagent benötigt diesen Speicherplatz. `/var` weil Podman oder Docker so konzipiert sind, dass die Container in diesem Verzeichnis erstellt werden. Konkret werden sie Container

erstellen in der `/var/lib/containers/storage` Verzeichnis und `/var/lib/docker` für Docker. Externe Mounts oder Symlinks funktionieren für diesen Bereich nicht.

Azure-VM-Größe

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

Hypervisor

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

Betriebssystem- und Containeranforderungen

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

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

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

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

Schritt 2: Installieren Sie Podman oder Docker Engine

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

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

  Sehen Sie sich die unterstützten Podman-Versionen an .

- Für Ubuntu ist Docker Engine erforderlich.

  Anzeigen der unterstützten Docker Engine-Versionen .

Beispiel 2. Schritte

Podman

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

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

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

Schritte

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

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

2. Installieren Sie Podman.

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

   a. Für Red Hat Enterprise Linux 9,6:

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

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

   b. Für Red Hat Enterprise Linux 9.1 bis 9.4:

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

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

   c. Für Red Hat Enterprise Linux 8:

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

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

unterstützten Podman-Versionen an .

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

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

4. Installieren Sie python3.

```
sudo dnf install python3
```

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

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

6. Bei Verwendung von Red Hat Enterprise 9:

   a. Installieren Sie das EPEL-Repository-Paket.

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

   +

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

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

7. Bei Verwendung von Red Hat Enterprise Linux 8:

   a. Installieren Sie das EPEL-Repository-Paket.

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

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

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. Starten Sie Podman neu.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker-Engine

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

Schritte

1. "Installationsanweisungen von Docker anzeigen"

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

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

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

Schritt 3: Einrichten des Netzwerks

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

Azure-Region

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

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Von Computern kontaktierte Endpunkte bei Verwendung der webbasierten NetApp Console

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

"Vorbereiten des Netzwerks für die NetApp Konsole" .

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Zum Verwalten von Ressourcen in öffentlichen Azure-Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Zum Verwalten von Ressourcen in Azure China-Regionen.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.

Endpunkte	Zweck
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. • Wenn Sie einen neuen Agenten bereitstellen, testet die Validierungsprüfung die Konnektivität zu aktuellen Endpunkten. Wenn Sie"vorherige Endpunkte" , schlägt die Validierungsprüfung fehl. Um diesen Fehler zu vermeiden, überspringen Sie die Validierungsprüfung. Obwohl die vorherigen Endpunkte weiterhin unterstützt werden, empfiehlt NetApp , Ihre Firewall-Regeln so schnell wie möglich auf die aktuellen Endpunkte zu aktualisieren. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" . • Wenn Sie auf die aktuellen Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

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

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

Aktivieren von NTP

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

Schritt 4: Einrichten der Bereitstellungsberechtigungen für den Konsolen-Agenten

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

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

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

Erstellen einer benutzerdefinierten Rolle für die Bereitstellung des Konsolenagenten

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

Schritte

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

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

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

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

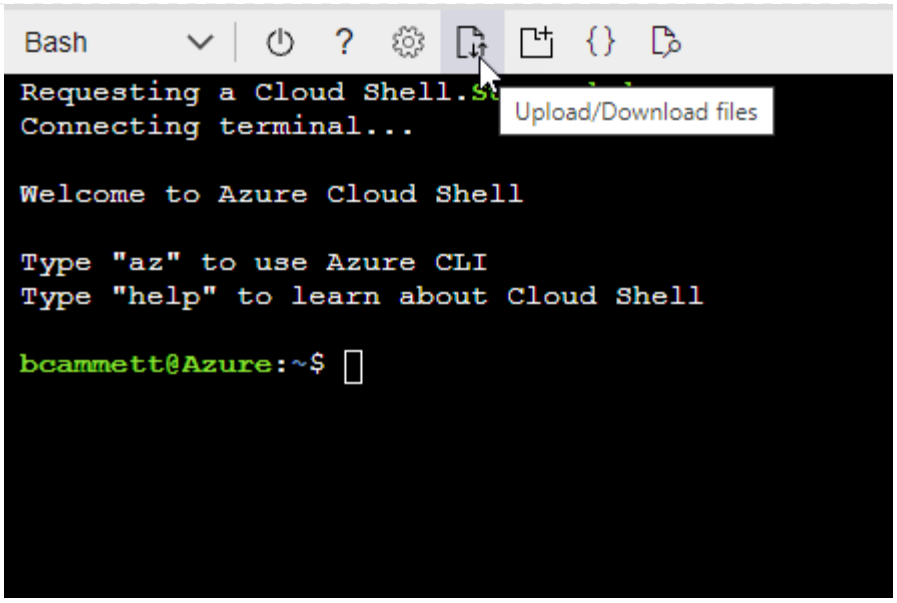
   Beispiel

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

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

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

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



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

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

Dienstprinzipal

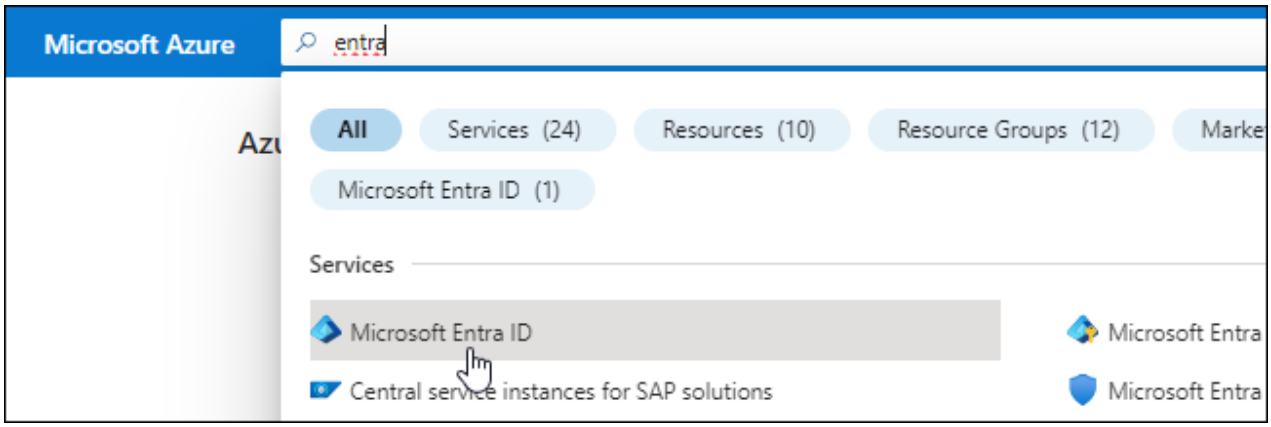
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die der Konsolenagent benötigt.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffskontrolle

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

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

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



3. Wählen Sie im Menü **App-Registrierungen** aus.
4. Wählen Sie **Neuregistrierung**.
5. Geben Sie Details zur Anwendung an:

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

6. Wählen Sie **Registrieren**.

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der Anwendung zu einer Rolle

1. Erstellen Sie eine benutzerdefinierte Rolle:

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

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

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

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

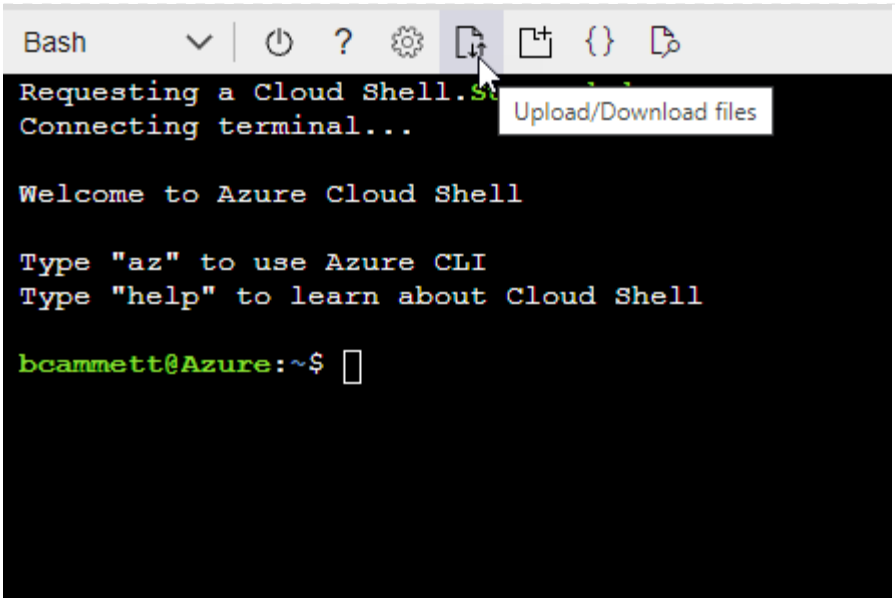
      Beispiel

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

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

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

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



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

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

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

2. Weisen Sie die Anwendung der Rolle zu:

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

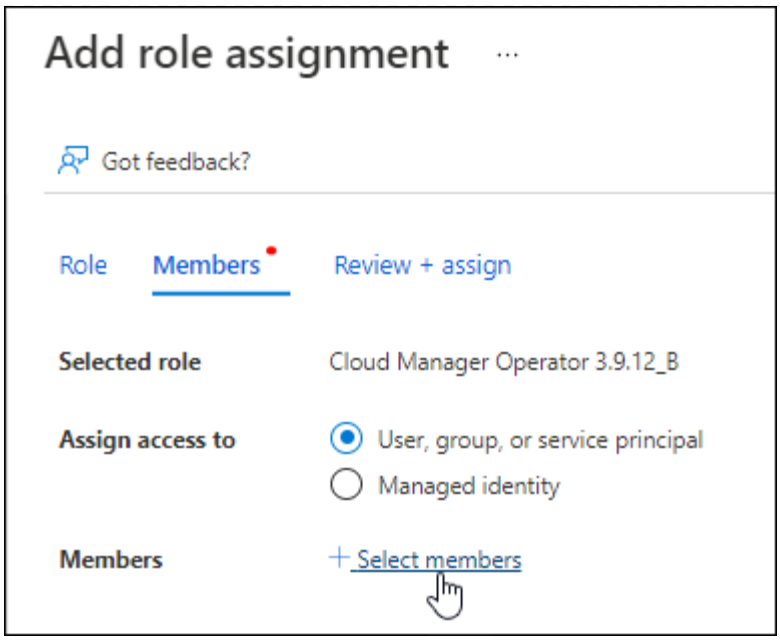
   b. Wählen Sie das Abonnement aus.

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

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

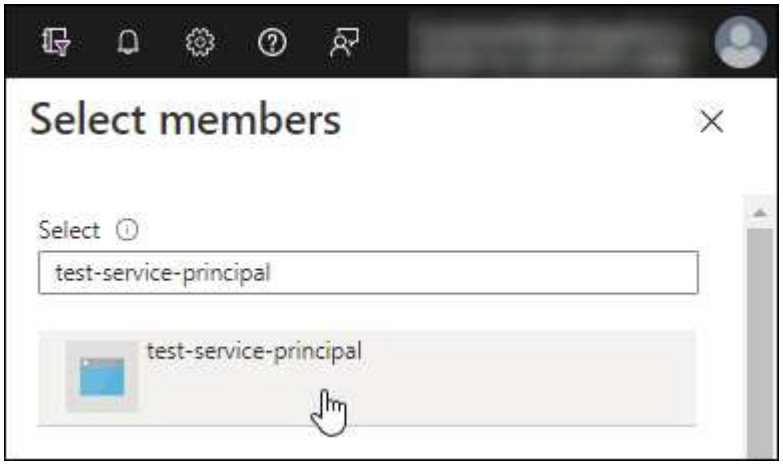
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

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



- Suchen Sie nach dem Namen der Anwendung.

  Hier ist ein Beispiel:



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

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

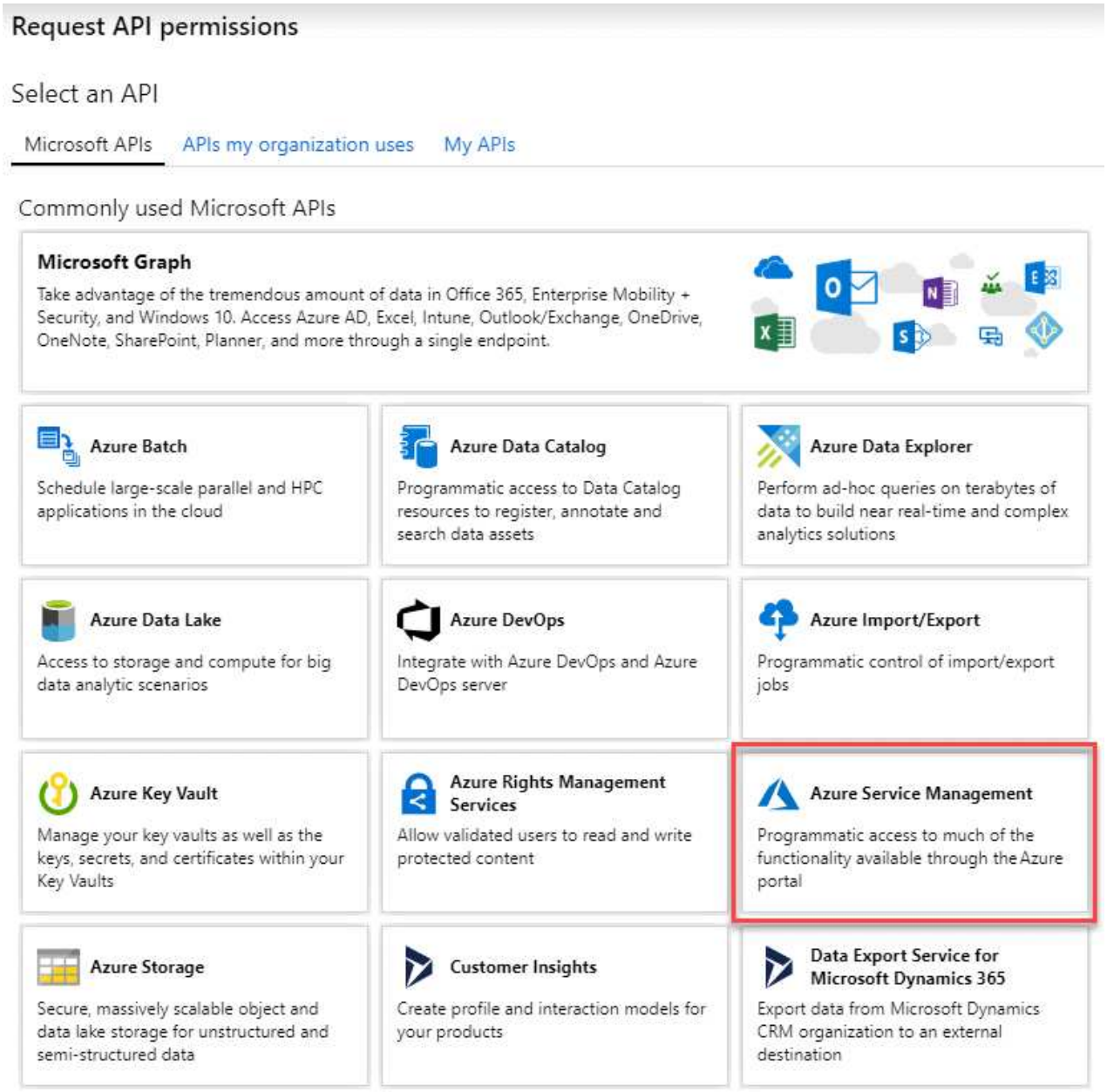
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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

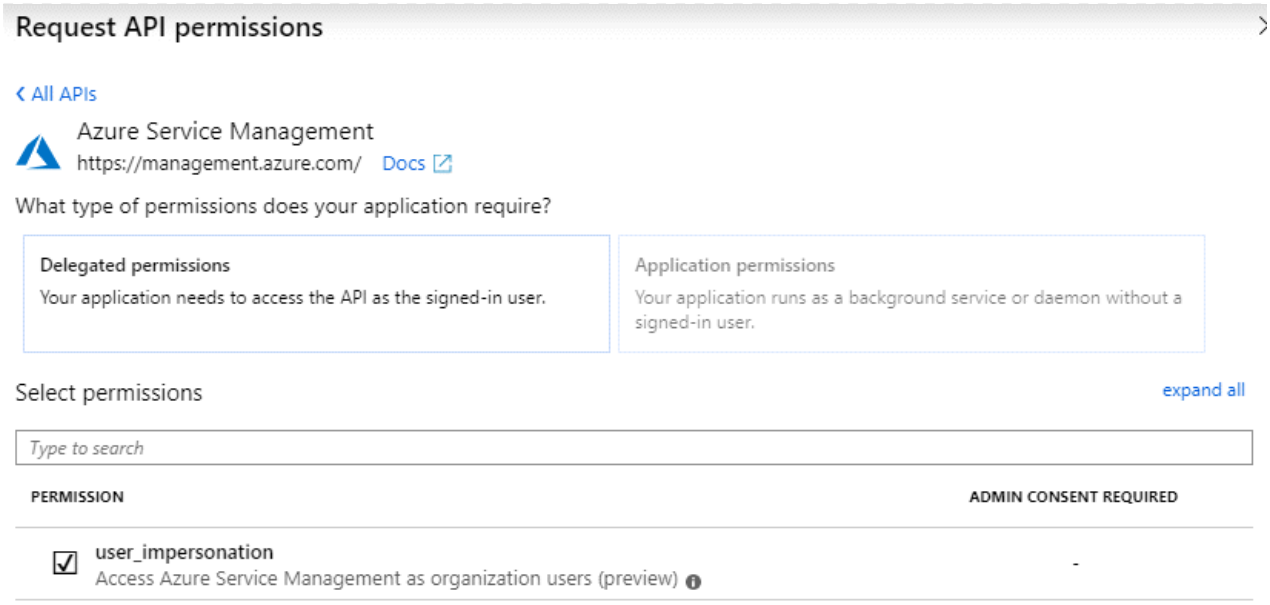
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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

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

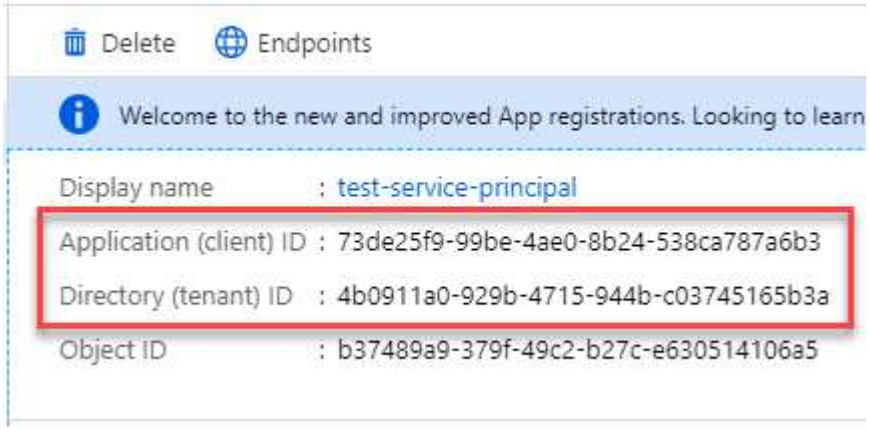


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

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



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

Erstellen eines Client-Geheimnisses

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

Ergebnis

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

Schritt 5: Installieren des Konsolenagenten

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

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

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

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

- Eine auf der VM in Azure aktivierte verwaltete Identität, sodass Sie die erforderlichen Azure-Berechtigungen über eine benutzerdefinierte Rolle bereitstellen können.

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

Informationen zu diesem Vorgang

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

Schritte

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

```
unset http_proxy
unset https_proxy
```

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

2. Laden Sie die Console-Agent-Software herunter und kopieren Sie sie anschließend auf den Linux-Host. Sie können es entweder von der NetApp Console oder von der NetApp -Support-Website herunterladen.
   - NetApp Console: Gehen Sie zu **Agents > Management > Agent bereitstellen > On-Premise > Manuelle Installation**.

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

   - NetApp Supportseite (erforderlich, falls Sie noch keinen Zugriff auf die Konsole haben) "NetApp Support Site" ,
3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

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

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

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

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

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

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

+

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

+

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

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

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

+ Beachten Sie Folgendes:

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

+ Zum Beispiel:

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

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

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

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

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

      Beispiel:

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

   a. Starten Sie die virtuelle Maschine des Konsolenagenten neu.

2. Warten Sie, bis die Installation abgeschlossen ist.

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

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

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

   https://ipaddress

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

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

   d. Wählen Sie **Los geht’s**.

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

Schritt 6: Berechtigungen für die NetApp Console erteilen

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

Benutzerdefinierte Rolle

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

Schritte

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

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

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

2. Wählen Sie **Zugriffskontrolle (IAM)** > **Hinzufügen** > **Rollenzuweisung hinzufügen**.
3. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.

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

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

Wie geht es weiter?

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

Dienstprinzipal

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Microsoft Azure > Agent**.
   b. **Anmeldeinformationen definieren**: Geben Sie Informationen zum Microsoft Entra-Dienstprinzipal ein, der die erforderlichen Berechtigungen erteilt:
      - Anwendungs-ID (Client-ID)
      - Verzeichnis-ID (Mandant)
      - Client-Geheimnis

c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.

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

Ergebnis

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

Google Cloud

Installationsoptionen für den Konsolenagenten in Google Cloud

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

Folgende Installationsoptionen stehen zur Verfügung:

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

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

- "Erstellen Sie den Konsolenagenten mithilfe der Google Platform"

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

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

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

Erstellen Sie einen Konsolenagenten in Google Cloud über die NetApp Console

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

Bevor Sie beginnen

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

Schritt 1: Einrichten des Netzwerks

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

VPC und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://config.googleapis.com/v1/projects	Zum Verwalten von Ressourcen in Google Cloud.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.

Endpunkte	Zweck
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. • Wenn Sie einen neuen Agenten bereitstellen, testet die Validierungsprüfung die Konnektivität zu aktuellen Endpunkten. Wenn Sie"vorherige Endpunkte" , schlägt die Validierungsprüfung fehl. Um diesen Fehler zu vermeiden, überspringen Sie die Validierungsprüfung. Obwohl die vorherigen Endpunkte weiterhin unterstützt werden, empfiehlt NetApp , Ihre Firewall-Regeln so schnell wie möglich auf die aktuellen Endpunkte zu aktualisieren. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" . • Wenn Sie auf die aktuellen Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Von der NetApp Konsole kontaktierte Endpunkte

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

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

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

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

Aktivieren von NTP

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

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

Schritt 2: Richten Sie Berechtigungen zum Erstellen des Konsolenagenten ein

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

Schritte

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

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

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

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

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

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

b. Aktivieren Sie Cloud Shell in Google Cloud.

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

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

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

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

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

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

"Google Cloud-Dokumente: Gewähren einer einzelnen Rolle"

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

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

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

Versionshinweisen aufgeführt.

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in Google Cloud:

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

   b. Aktivieren Sie Cloud Shell in Google Cloud.

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

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

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

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

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

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

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

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

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

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

      "Google Cloud-Dokumente: Erstellen eines Dienstkontos"

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

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

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

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

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

   Weitere Einzelheiten finden Sie unter "Google Cloud-Dokumentation"

Schritt 4: Einrichten freigegebener VPC-Berechtigungen

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

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

Berechtigungen für freigegebene VPCs anzeigen

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

Hinweise:

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

Schritt 5: Google Cloud APIs aktivieren

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

Schritt

1. Aktivieren Sie die folgenden Google Cloud-APIs in Ihrem Projekt:
    - Cloud 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 Produktanleitung enthält die Informationen, die auf dieser Seite der Dokumentation enthalten sind.

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

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

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

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

     "Firewall-Regeln in Google Cloud"

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

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

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

6. Wählen Sie **Hinzufügen**.

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

Ergebnis

Nach Abschluss des Vorgangs steht der Konsolenagent zur Verwendung bereit.

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

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

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

Bevor Sie beginnen

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

Schritt 1: Einrichten des Netzwerks

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

VPC und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://config.googleapis.com/v1/projects	Zum Verwalten von Ressourcen in Google Cloud.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.

Endpunkte	Zweck
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. • Wenn Sie einen neuen Agenten bereitstellen, testet die Validierungsprüfung die Konnektivität zu aktuellen Endpunkten. Wenn Sie"vorherige Endpunkte" , schlägt die Validierungsprüfung fehl. Um diesen Fehler zu vermeiden, überspringen Sie die Validierungsprüfung. Obwohl die vorherigen Endpunkte weiterhin unterstützt werden, empfiehlt NetApp , Ihre Firewall-Regeln so schnell wie möglich auf die aktuellen Endpunkte zu aktualisieren. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" . • Wenn Sie auf die aktuellen Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Von der NetApp Konsole kontaktierte Endpunkte

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

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

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

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

Aktivieren von NTP

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

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

Schritt 2: Richten Sie Berechtigungen zum Erstellen des Konsolenagenten ein

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

Schritte

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

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

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

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

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

b. Aktivieren Sie Cloud Shell in Google Cloud.

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

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

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

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

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

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

   "Google Cloud-Dokumente: Gewähren einer einzelnen Rolle"

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

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

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

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in Google Cloud:

   a. Erstellen Sie eine YAML-Datei, die den Inhalt der"Dienstkontoberechtigungen für den Konsolenagenten" .
   b. Aktivieren Sie Cloud Shell in Google Cloud.
   c. Laden Sie die YAML-Datei hoch, die die erforderlichen Berechtigungen enthält.
   d. Erstellen Sie eine benutzerdefinierte Rolle mithilfe der `gcloud iam roles create` Befehl.

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

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

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

2. Erstellen Sie ein Dienstkonto in Google Cloud und weisen Sie dem Dienstkonto die Rolle zu:
   a. Wählen Sie im IAM- und Admin-Dienst **Dienstkonten > Dienstkonto erstellen**.
   b. Geben Sie die Details des Dienstkontos ein und wählen Sie **Erstellen und fortfahren**.
   c. Wählen Sie die Rolle aus, die Sie gerade erstellt haben.
   d. Führen Sie die restlichen Schritte aus, um die Rolle zu erstellen.

      "Google Cloud-Dokumente: Erstellen eines Dienstkontos"

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

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

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

ONTAP -Systeme erstellen möchten.

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

Weitere Einzelheiten finden Sie unter "Google Cloud-Dokumentation"

Schritt 4: Einrichten freigegebener VPC-Berechtigungen

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

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

Berechtigungen für freigegebene VPCs anzeigen

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

Hinweise:

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

Schritt 5: Google Cloud APIs aktivieren

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.

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

Bevor Sie beginnen

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

Schritt 1: Hostanforderungen prüfen

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

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

Dedizierter Host

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

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

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

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

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

Google Cloud-Maschinentyp

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

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

Hypervisor

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

Betriebssystem- und Containeranforderungen

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

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

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

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

Google Cloud-Maschinentyp

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

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

Schritt 2: Installieren Sie Podman oder Docker Engine

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

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

  Sehen Sie sich die unterstützten Podman-Versionen an .

- Für Ubuntu ist Docker Engine erforderlich.

  Anzeigen der unterstützten Docker Engine-Versionen .

Beispiel 3. Schritte

Podman

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

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

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

Schritte

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

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

2. Installieren Sie Podman.

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

   a. Für Red Hat Enterprise Linux 9,6:

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

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

   b. Für Red Hat Enterprise Linux 9.1 bis 9.4:

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

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

   c. Für Red Hat Enterprise Linux 8:

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

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

unterstützten Podman-Versionen an .

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

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

4. Installieren Sie python3.

```
sudo dnf install python3
```

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

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

6. Bei Verwendung von Red Hat Enterprise 9:

   a. Installieren Sie das EPEL-Repository-Paket.

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

   +

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

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

7. Bei Verwendung von Red Hat Enterprise Linux 8:

   a. Installieren Sie das EPEL-Repository-Paket.

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

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

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. Starten Sie Podman neu.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker-Engine

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

Schritte

1. "Installationsanweisungen von Docker anzeigen"

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

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

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

Schritt 3: Einrichten des Netzwerks

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Von Computern kontaktierte Endpunkte bei Verwendung der webbasierten NetApp Console

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

"Vorbereiten des Netzwerks für die NetApp Konsole" .

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://config.googleapis.com/v1/projects	Zum Verwalten von Ressourcen in Google Cloud.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.

Endpunkte	Zweck
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. • Wenn Sie einen neuen Agenten bereitstellen, testet die Validierungsprüfung die Konnektivität zu aktuellen Endpunkten. Wenn Sie"vorherige Endpunkte" , schlägt die Validierungsprüfung fehl. Um diesen Fehler zu vermeiden, überspringen Sie die Validierungsprüfung. Obwohl die vorherigen Endpunkte weiterhin unterstützt werden, empfiehlt NetApp , Ihre Firewall-Regeln so schnell wie möglich auf die aktuellen Endpunkte zu aktualisieren. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" . • Wenn Sie auf die aktuellen Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

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

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

Aktivieren von NTP

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

Schritt 4: Berechtigungen für den Konsolen-Agent einrichten

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

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

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in Google Cloud:

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

   b. Aktivieren Sie Cloud Shell in Google Cloud.

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

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

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

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

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

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

a. Wählen Sie im IAM- und Admin-Dienst **Dienstkonten > Dienstkonto erstellen**.
b. Geben Sie die Details des Dienstkontos ein und wählen Sie **Erstellen und fortfahren**.
c. Wählen Sie die Rolle aus, die Sie gerade erstellt haben.
d. Führen Sie die restlichen Schritte aus, um die Rolle zu erstellen.

"Google Cloud-Dokumente: Erstellen eines Dienstkontos"

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

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

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

   Weitere Einzelheiten finden Sie unter "Google Cloud-Dokumentation"

Schritt 5: Einrichten freigegebener VPC-Berechtigungen

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

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

Berechtigungen für freigegebene VPCs anzeigen

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

Hinweise:

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

Schritt 6: Google Cloud APIs aktivieren

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

Schritt

1. Aktivieren Sie die folgenden Google Cloud-APIs in Ihrem Projekt:
    - Cloud 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 Backslashs maskieren: & oder !

+ Zum Beispiel:

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

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

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

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

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

      Beispiel:

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

   a. Starten Sie die virtuelle Maschine des Konsolenagenten neu.

2. Warten Sie, bis die Installation abgeschlossen ist.

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

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

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

   https://ipaddress

2. Richten Sie nach der Anmeldung den Konsolenagenten ein:

   a. Geben Sie die Organisation an, die mit dem Konsolenagenten verknüpft werden soll.

   b. Geben Sie einen Namen für das System ein.

   c. Lassen Sie unter **Arbeiten Sie in einer sicheren Umgebung?** den eingeschränkten Modus deaktiviert.

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

   d. Wählen Sie **Los geht's**.

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

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

Schritt 8: Erteilen Sie dem Konsolenagenten Berechtigungen

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

Schritte

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

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

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

Installieren eines Agenten vor Ort

Manuelle Installation eines Konsolen-Agenten vor Ort

Installieren Sie einen Konsolenagenten vor Ort, melden Sie sich dann an und richten Sie

ihn für die Arbeit mit Ihrer Konsolenorganisation ein.

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

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

Vorbereiten der Installation des Konsolenagenten

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

Überprüfen der Hostanforderungen für den Konsolenagenten

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

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

Dedizierter Host

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

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

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

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

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

Hypervisor

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

Betriebssystem- und Containeranforderungen

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

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

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

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

Einrichten des Netzwerkzugriffs für den Konsolenagenten

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Von Computern kontaktierte Endpunkte bei Verwendung der webbasierten NetApp Console

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

"Vorbereiten des Netzwerks für die NetApp Konsole" .

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

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

AWS

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)	Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab. "Weitere Einzelheiten finden Sie in der AWS-Dokumentation."
Amazon FsX für NetApp ONTAP: • api.workloads.netapp.com	Die webbasierte Konsole kontaktiert diesen Endpunkt, um mit den Workload Factory APIs zu interagieren und so FSx for ONTAP basierte Workloads zu verwalten und zu betreiben.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.

Endpunkte	Zweck
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. • Wenn Sie einen neuen Agenten bereitstellen, testet die Validierungsprüfung die Konnektivität zu aktuellen Endpunkten. Wenn Sie"vorherige Endpunkte" , schlägt die Validierungsprüfung fehl. Um diesen Fehler zu vermeiden, überspringen Sie die Validierungsprüfung. Obwohl die vorherigen Endpunkte weiterhin unterstützt werden, empfiehlt NetApp , Ihre Firewall-Regeln so schnell wie möglich auf die aktuellen Endpunkte zu aktualisieren. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" . • Wenn Sie auf die aktuellen Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Azurblau

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

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Zum Verwalten von Ressourcen in öffentlichen Azure-Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Zum Verwalten von Ressourcen in Azure China-Regionen.

Endpunkte	Zweck
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

- HTTP (80) und HTTPS (443) ermöglichen den Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) wird nur benötigt, wenn Sie zur Fehlerbehebung eine Verbindung zum Host herstellen müssen.

- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP -Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

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

Aktivieren von NTP

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

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

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

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

AWS

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

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

Schritte

1. Melden Sie sich bei der AWS-Konsole an und navigieren Sie zum IAM-Dienst.
2. Erstellen Sie eine Richtlinie:

   a. Wählen Sie **Richtlinien > Richtlinie erstellen**.

   b. Wählen Sie **JSON** und kopieren und fügen Sie den Inhalt des"IAM-Richtlinie für den Konsolenagenten" .

   c. Führen Sie die restlichen Schritte aus, um die Richtlinie zu erstellen.

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

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

3. Hängen Sie die Richtlinien an einen IAM-Benutzer an.
   - "AWS-Dokumentation: Erstellen von IAM-Rollen"
   - "AWS-Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"
4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie der NetApp Console hinzufügen können, nachdem Sie den Konsolen-Agenten installiert haben.

Ergebnis

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

Azurblau

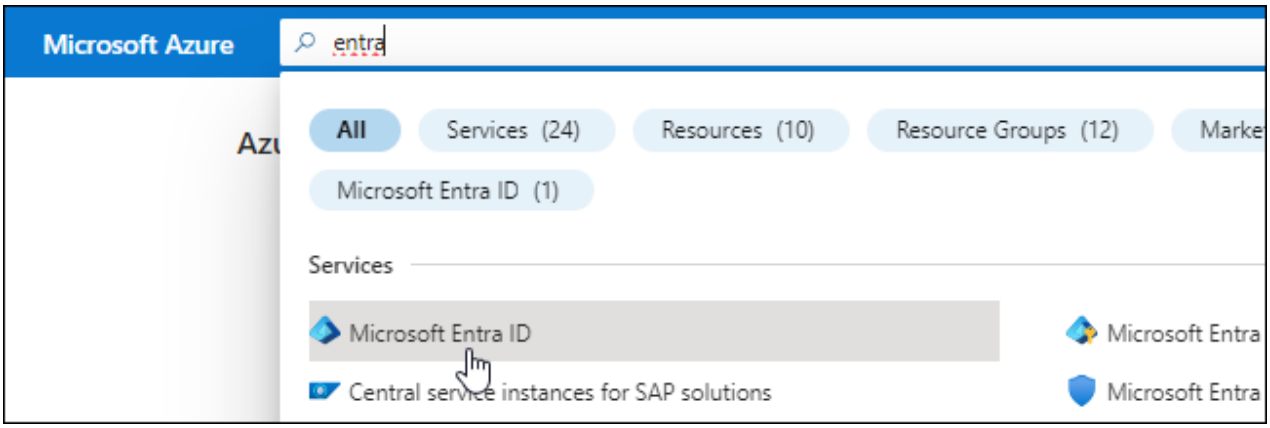
Wenn der Konsolen-Agent vor Ort installiert ist, müssen Sie dem Konsolen-Agenten Azure-Berechtigungen erteilen, indem Sie einen Dienstprinzipal in der Microsoft Entra ID einrichten und die Azure-Anmeldeinformationen abrufen, die der Konsolen-Agent benötigt.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffskontrolle

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

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

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



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

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der Anwendung zu einer Rolle

1. Erstellen Sie eine benutzerdefinierte Rolle:

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

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

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

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

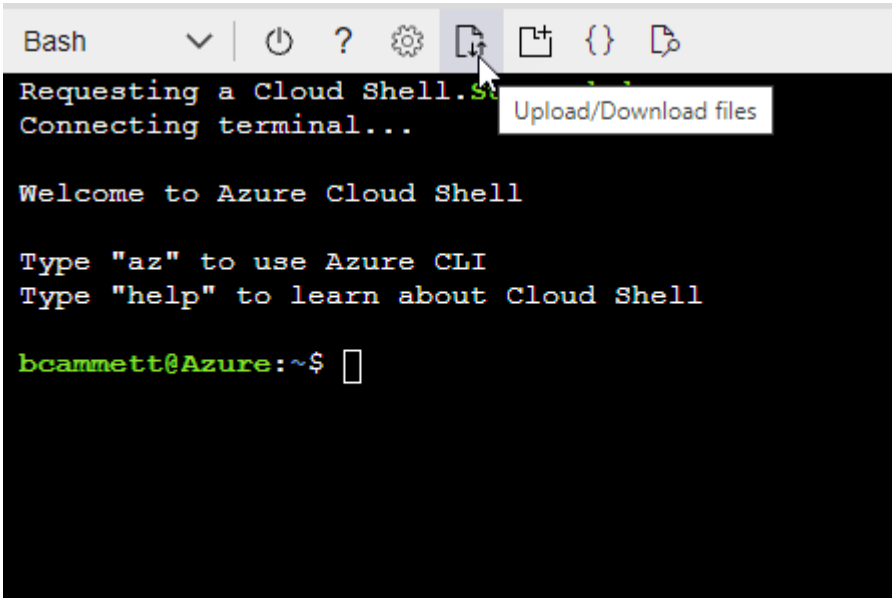
      Beispiel

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

   c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

Die folgenden Schritte beschreiben, wie Sie die Rolle mithilfe von Bash in Azure Cloud Shell erstellen.

- Start "Azure Cloud Shell" und wählen Sie die Bash-Umgebung.
- Laden Sie die JSON-Datei hoch.



- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
az role definition create --role-definition agent_Policy.json
```

Sie sollten jetzt über eine benutzerdefinierte Rolle namens „Konsolenoperator“ verfügen, die Sie der virtuellen Maschine des Konsolenagenten zuweisen können.

2. Weisen Sie die Anwendung der Rolle zu:

   a. Öffnen Sie im Azure-Portal den Dienst **Abonnements**.

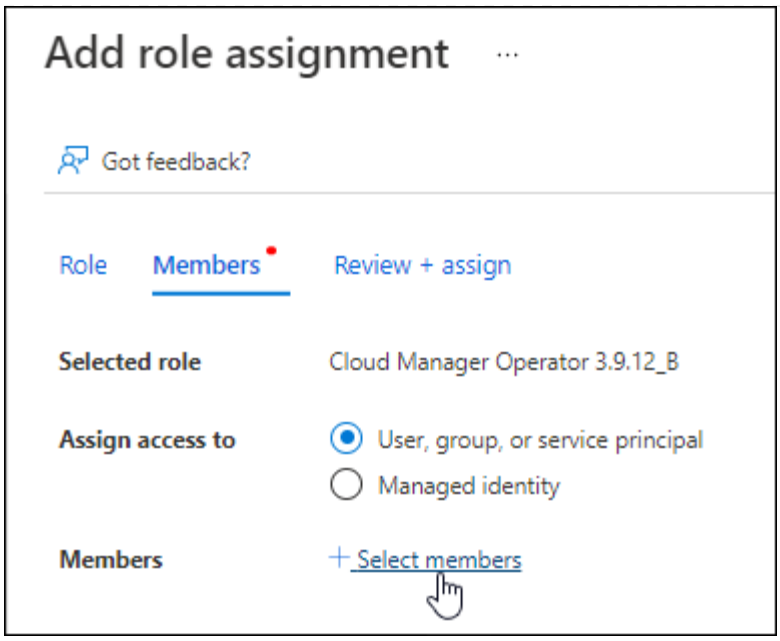
   b. Wählen Sie das Abonnement aus.

   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

   d. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.

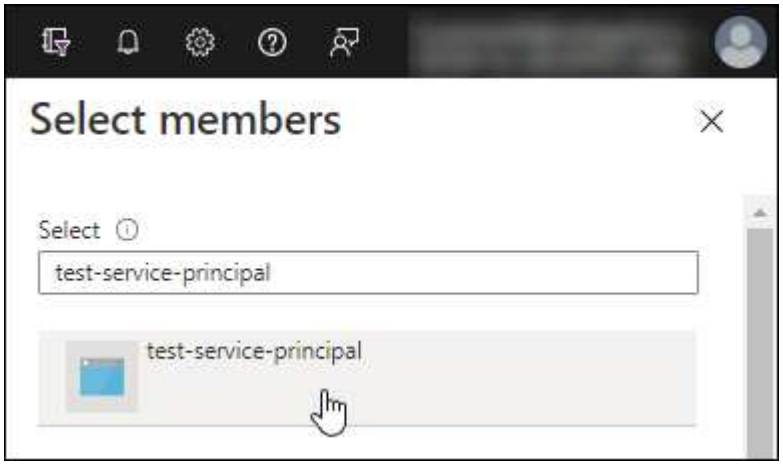
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - Behalten Sie die Auswahl von **Benutzer, Gruppe oder Dienstprinzipal** bei.
      - Wählen Sie **Mitglieder auswählen**.



- Suchen Sie nach dem Namen der Anwendung.

  Hier ist ein Beispiel:



- Wählen Sie die Anwendung aus und wählen Sie **Auswählen**.
- Wählen Sie **Weiter**.

f. Wählen Sie **Überprüfen + zuweisen**.

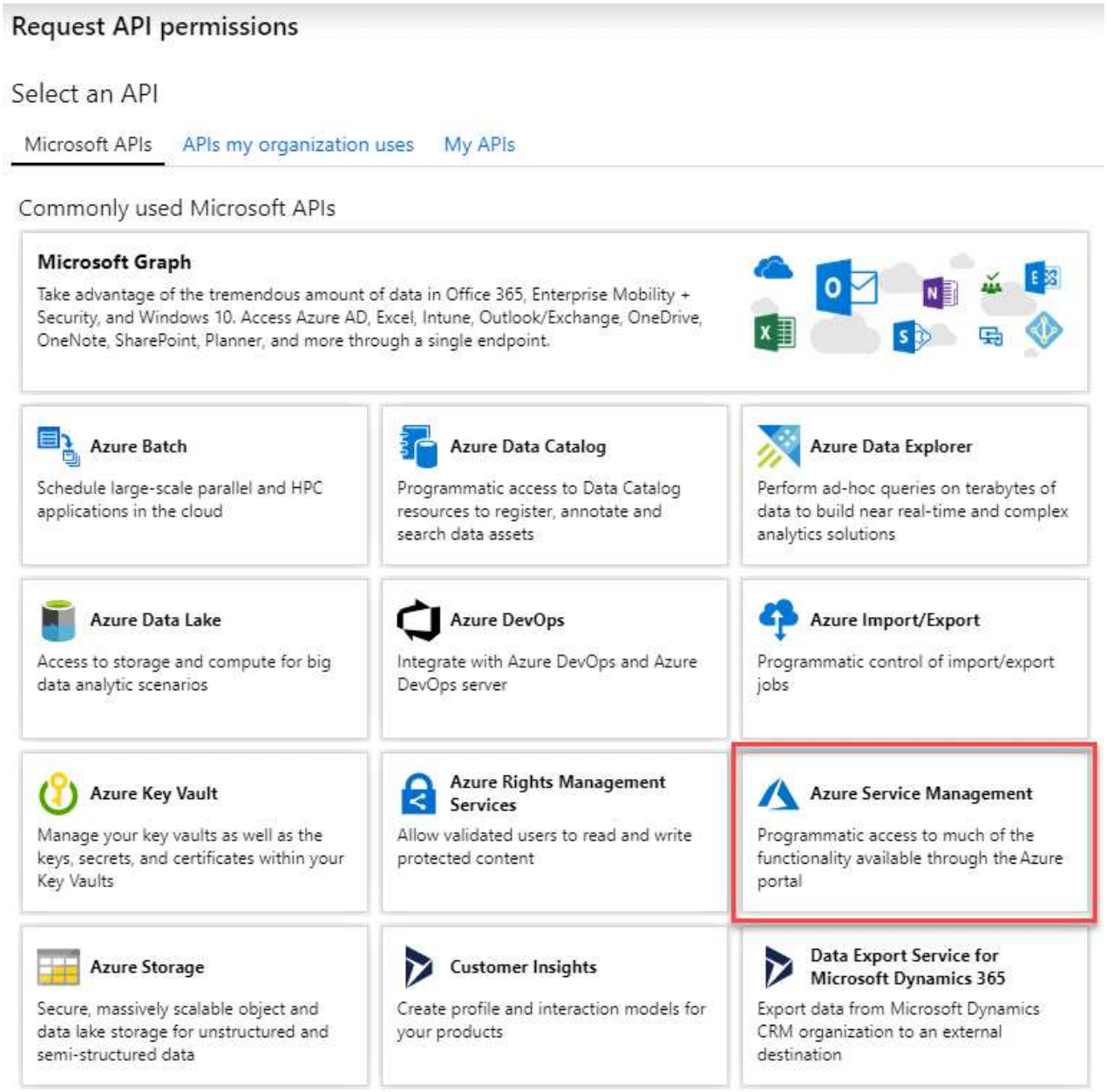
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

Wenn Sie Cloud Volumes ONTAP aus mehreren Azure-Abonnements bereitstellen möchten, müssen Sie den Dienstprinzipal an jedes dieser Abonnements binden. In der NetApp Console können Sie das Abonnement auswählen, das Sie beim Bereitstellen von Cloud Volumes ONTAP verwenden möchten.

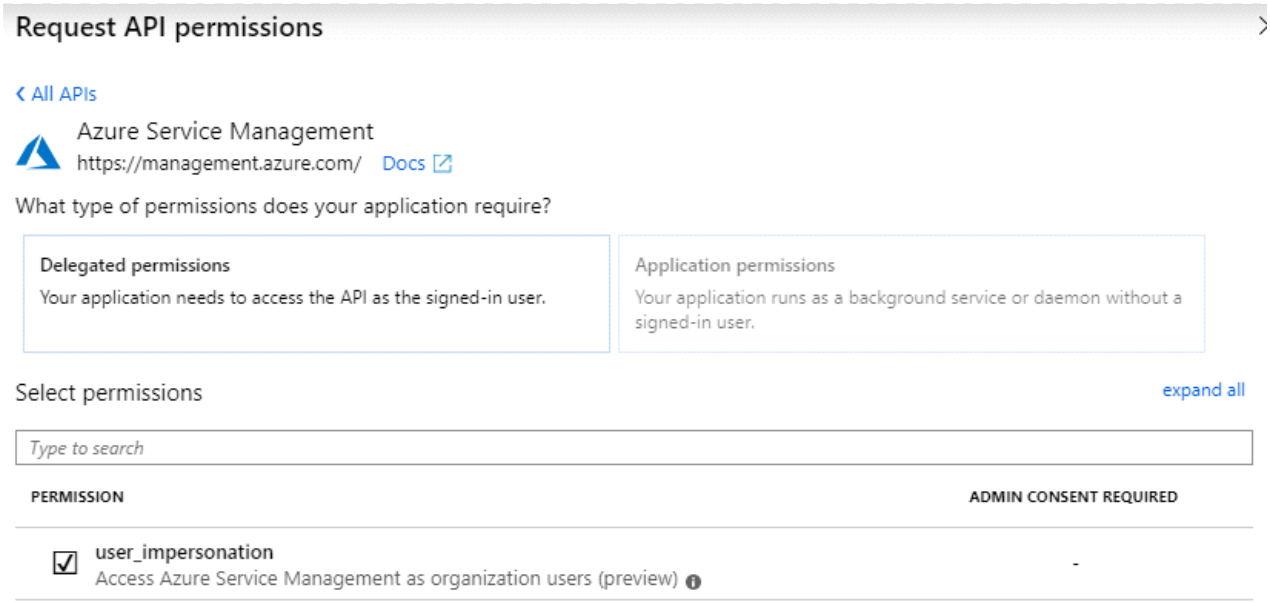
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Wählen Sie **API-Berechtigungen > Berechtigung hinzufügen**.

3. Wählen Sie unter **Microsoft-APIs Azure Service Management** aus.

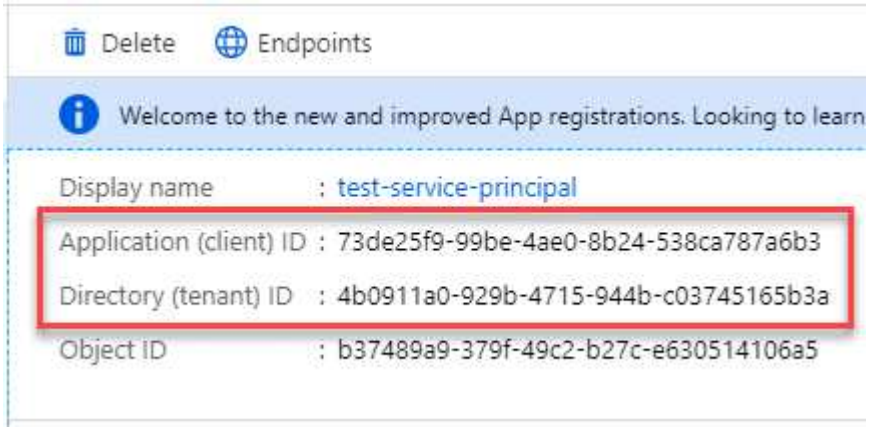


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



Abrufen der Anwendungs-ID und Verzeichnis-ID für die Anwendung

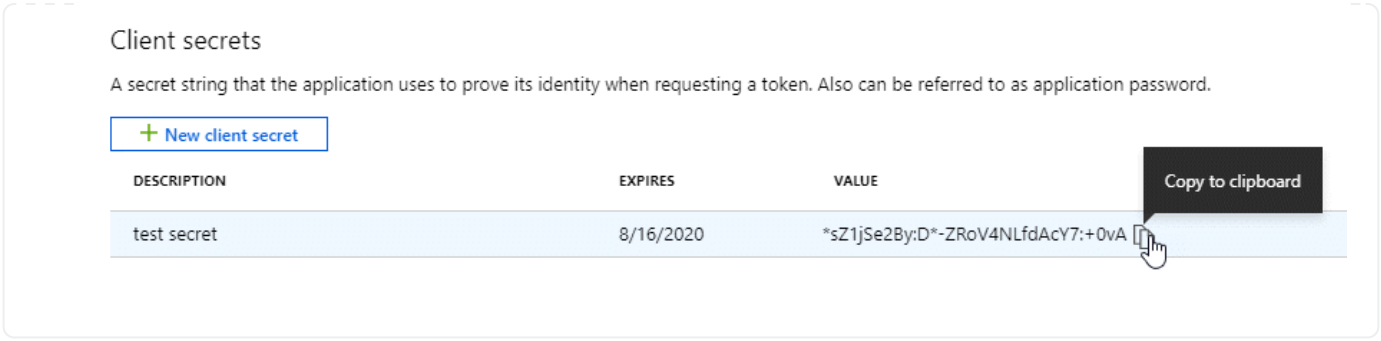
1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



Wenn Sie das Azure-Konto zur Konsole hinzufügen, müssen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) für die Anwendung angeben. Die Konsole verwendet die IDs zur programmgesteuerten Anmeldung.

Erstellen eines Client-Geheimnisses

1. Öffnen Sie den Dienst **Microsoft Entra ID**.
2. Wählen Sie **App-Registrierungen** und wählen Sie Ihre Anwendung aus.
3. Wählen Sie **Zertifikate und Geheimnisse > Neues Clientgeheimnis**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Wählen Sie **Hinzufügen**.
6. Kopieren Sie den Wert des Client-Geheimnisses.



Manuelles Installieren eines Konsolenagenten

Wenn Sie einen Konsolenagenten manuell installieren, müssen Sie Ihre Computerumgebung so vorbereiten, dass sie die Anforderungen erfüllt. Sie benötigen eine Linux-Maschine und müssen je nach Linux-Betriebssystem Podman oder Docker installieren.

Installieren Sie Podman oder Docker Engine

Abhängig von Ihrem Betriebssystem ist vor der Installation des Agenten entweder Podman oder Docker Engine erforderlich.

- Podman wird für Red Hat Enterprise Linux 8 und 9 benötigt.

  Sehen Sie sich die unterstützten Podman-Versionen an .

- Für Ubuntu ist Docker Engine erforderlich.

  Anzeigen der unterstützten Docker Engine-Versionen .

Beispiel 4. Schritte

Podman

Befolgen Sie diese Schritte, um Podman zu installieren und zu konfigurieren:

- Aktivieren und starten Sie den Dienst podman.socket
- Installieren Sie Python3
- Installieren Sie das Podman-Compose-Paket Version 1.0.6
- Fügen Sie podman-compose zur Umgebungsvariablen PATH hinzu
- Wenn Sie Red Hat Enterprise Linux verwenden, überprüfen Sie, ob Ihre Podman-Version Netavark Aardvark DNS anstelle von CNI verwendet

> Passen Sie den Aardvark-DNS-Port (Standard: 53) nach der Installation des Agenten an, um DNS-Portkonflikte zu vermeiden. Befolgen Sie die Anweisungen zum Konfigurieren des Ports.

Schritte

1. Entfernen Sie das Podman-Docker-Paket, falls es auf dem Host installiert ist.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Installieren Sie Podman.

   Sie können Podman aus den offiziellen Red Hat Enterprise Linux-Repositories beziehen.

   a. Für Red Hat Enterprise Linux 9,6:

   ```
   sudo dnf install podman-5:<version>
   ```

   Dabei ist <Version> die unterstützte Version von Podman, die Sie installieren. Sehen Sie sich die unterstützten Podman-Versionen an .

   b. Für Red Hat Enterprise Linux 9.1 bis 9.4:

   ```
   sudo dnf install podman-4:<version>
   ```

   Dabei ist <Version> die unterstützte Version von Podman, die Sie installieren. Sehen Sie sich die unterstützten Podman-Versionen an .

   c. Für Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-4:<version>
   ```

   Dabei ist <Version> die unterstützte Version von Podman, die Sie installieren. Sehen Sie sich die

unterstützten Podman-Versionen an .

3. Aktivieren und starten Sie den Dienst podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Installieren Sie python3.

```
sudo dnf install python3
```

5. Installieren Sie das EPEL-Repository-Paket, falls es auf Ihrem System noch nicht verfügbar ist.

   Dieser Schritt ist erforderlich, da podman-compose im Repository „Extra Packages for Enterprise Linux“ (EPEL) verfügbar ist.

6. Bei Verwendung von Red Hat Enterprise 9:

   a. Installieren Sie das EPEL-Repository-Paket.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. Installieren Sie das Podman-Compose-Paket 1.5.0.

```
sudo dnf install podman-compose-1.5.0
```

7. Bei Verwendung von Red Hat Enterprise Linux 8:

   a. Installieren Sie das EPEL-Repository-Paket.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. Installieren Sie das Podman-Compose-Paket 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```

> Verwenden des `dnf install` Der Befehl erfüllt die Anforderung zum Hinzufügen von „podman-compose“ zur Umgebungsvariablen PATH. Der Installationsbefehl fügt podman-compose zu /usr/bin hinzu, das bereits im `secure_path` Option auf dem Host.

c. Wenn Sie Red Hat Enterprise Linux 8 verwenden, überprüfen Sie, ob Ihre Podman-Version NetAvark mit Aardvark DNS anstelle von CNI verwendet.

i. Überprüfen Sie, ob Ihr Netzwerk-Backend auf CNI eingestellt ist, indem Sie den folgenden Befehl ausführen:

```
podman info | grep networkBackend
```

ii. Wenn das Netzwerk-Backend auf `CNI` , müssen Sie es ändern in `netavark` .

iii. Installieren `netavark` Und `aardvark-dns` mit dem folgenden Befehl:

```
dnf install aardvark-dns netavark
```

iv. Öffnen Sie die `/etc/containers/containers.conf` Datei und ändern Sie die Option network_backend, um „netavark“ anstelle von „cni“ zu verwenden.

Wenn `/etc/containers/containers.conf` nicht vorhanden ist, nehmen Sie die Konfigurationsänderungen vor, um `/usr/share/containers/containers.conf` .

v. Starten Sie Podman neu.

```
systemctl restart podman
```

vi. Bestätigen Sie mit dem folgenden Befehl, dass networkBackend jetzt in „netavark“ geändert wurde:

```
podman info | grep networkBackend
```

Docker-Engine

Befolgen Sie die Dokumentation von Docker, um Docker Engine zu installieren.

Schritte

1. "Installationsanweisungen von Docker anzeigen"

   Befolgen Sie die Schritte, um eine unterstützte Docker Engine-Version zu installieren. Installieren Sie nicht die neueste Version, da diese von der Konsole nicht unterstützt wird.

2. Stellen Sie sicher, dass Docker aktiviert und ausgeführt wird.

```
sudo systemctl enable docker && sudo systemctl start docker
```

Installieren Sie den Konsolenagenten manuell

Laden Sie die Konsolen-Agent-Software herunter und installieren Sie sie auf einem vorhandenen Linux-Host vor Ort.

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Root-Berechtigungen zum Installieren des Konsolenagenten.
- Details zu einem Proxyserver, falls für den Internetzugriff vom Konsolenagenten ein Proxy erforderlich ist.

  Sie haben die Möglichkeit, nach der Installation einen Proxyserver zu konfigurieren, hierzu ist jedoch ein Neustart des Konsolenagenten erforderlich.

- Ein von einer Zertifizierungsstelle signiertes Zertifikat, wenn der Proxyserver HTTPS verwendet oder wenn es sich bei dem Proxy um einen abfangenden Proxy handelt.

> Sie können bei der manuellen Installation des Konsolenagenten kein Zertifikat für einen transparenten Proxyserver festlegen. Wenn Sie ein Zertifikat für einen transparenten Proxyserver festlegen müssen, müssen Sie nach der Installation die Wartungskonsole verwenden. Erfahren Sie mehr über die "Agenten-Wartungskonsole"Die

Informationen zu diesem Vorgang

Nach der Installation aktualisiert sich der Konsolenagent automatisch, wenn eine neue Version verfügbar ist.

Schritte

1. Wenn die Systemvariablen *http_proxy* oder *https_proxy* auf dem Host festgelegt sind, entfernen Sie sie:

   ```
   unset http_proxy
   unset https_proxy
   ```

   Wenn Sie diese Systemvariablen nicht entfernen, schlägt die Installation fehl.

2. Laden Sie die Console-Agent-Software herunter und kopieren Sie sie anschließend auf den Linux-Host. Sie können es entweder von der NetApp Console oder von der NetApp -Support-Website herunterladen.
   - NetApp Console: Gehen Sie zu **Agents > Management > Agent bereitstellen > On-Premise > Manuelle Installation**.

     Wählen Sie entweder die Agenteninstallationsdateien oder eine URL zu den Dateien zum Herunterladen.

   - NetApp Supportseite (erforderlich, falls Sie noch keinen Zugriff auf die Konsole haben) "NetApp Support Site" ,
3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

   ```
   chmod +x NetApp_Console_Agent_Cloud_<version>
   ```

   Dabei ist <Version> die Version des Konsolenagenten, die Sie heruntergeladen haben.

4. Deaktivieren Sie bei der Installation in einer Government Cloud-Umgebung die Konfigurationsprüfungen."Erfahren Sie, wie Sie Konfigurationsprüfungen für manuelle Installationen deaktivieren."
5. Führen Sie das Installationsskript aus.

```
./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

Sie müssen Proxy-Informationen hinzufügen, falls Ihr Netzwerk einen Proxy für den Internetzugang benötigt. Sie können während der Installation einen expliziten Proxy hinzufügen. Die `--proxy` und `--cacert` Parameter sind optional und Sie werden nicht dazu aufgefordert, sie hinzuzufügen. Wenn Sie einen expliziten Proxyserver haben, müssen Sie die Parameter wie gezeigt eingeben.

Wenn Sie einen transparenten Proxy konfigurieren möchten, können Sie dies nach der Installation tun. "Erfahren Sie mehr über die Agentenwartungskonsole."

+

Hier ist ein Beispiel für die Konfiguration eines expliziten Proxyservers mit einem von einer Zertifizierungsstelle signierten Zertifikat:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert /tmp/cacert/certificate.cer
```

+
`--proxy` konfiguriert den Konsolenagenten für die Verwendung eines HTTP- oder HTTPS-Proxyservers in einem der folgenden Formate:

+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-name:password@address:port * https://address:port * https://user-name:password@address:port * https://domain-name%92user-name:password@address:port

+ Beachten Sie Folgendes:

+ **Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.** Für einen Domänenbenutzer müssen Sie den ASCII-Code für ein \ verwenden, wie oben gezeigt. **Der Console-Agent unterstützt keine Benutzernamen oder Passwörter, die das @-Zeichen enthalten.** Wenn das Passwort eines der folgenden Sonderzeichen enthält, müssen Sie dieses Sonderzeichen durch Voranstellen eines Backslashs maskieren: & oder !

+ Zum Beispiel:

+ http://bxpproxyuser:netapp1\!@address:3128

1. Wenn Sie Podman verwendet haben, müssen Sie den Aardvark-DNS-Port anpassen.

   a. Stellen Sie eine SSH-Verbindung zur virtuellen Maschine des Konsolenagenten her.

b. Öffnen Sie die Datei podman_/usr/share/containers/containers.conf_ und ändern Sie den gewählten Port für den Aardvark-DNS-Dienst. Ändern Sie ihn beispielsweise in 54.

```
vi /usr/share/containers/containers.conf
```

Beispiel:

```
# Port to use for dns forwarding daemon with netavark in rootful bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services should
# run on the machine.
#
dns_bind_port = 54
```

a. Starten Sie die virtuelle Maschine des Konsolenagenten neu.

Wie geht es weiter?

Sie müssen den Konsolenagenten in der NetApp Console registrieren.

Registrieren Sie den Konsolenagenten bei der NetApp Console

Melden Sie sich bei der Konsole an und verknüpfen Sie den Konsolenagenten mit Ihrer Organisation. Die Art der Anmeldung hängt vom Modus ab, in dem Sie die Konsole verwenden. Wenn Sie die Konsole im Standardmodus verwenden, melden Sie sich über die SaaS-Website an. Wenn Sie die Konsole im eingeschränkten Modus verwenden, melden Sie sich lokal vom Konsolen-Agent-Host aus an.

Schritte

1. Öffnen Sie einen Webbrowser und geben Sie die Host-URL des Konsolenagenten ein:

   Die Host-URL der Konsole kann je nach Konfiguration des Hosts ein lokaler Host, eine private IP-Adresse oder eine öffentliche IP-Adresse sein. Wenn sich der Konsolenagent beispielsweise in der öffentlichen Cloud ohne öffentliche IP-Adresse befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der über eine Verbindung zum Host des Konsolenagenten verfügt.

2. Registrieren oder anmelden.
3. Richten Sie nach der Anmeldung die Konsole ein:
   a. Geben Sie die Konsolenorganisation an, die mit dem Konsolenagenten verknüpft werden soll.
   b. Geben Sie einen Namen für das System ein.
   c. Lassen Sie unter **Arbeiten Sie in einer sicheren Umgebung?** den eingeschränkten Modus deaktiviert.

      Der eingeschränkte Modus wird nicht unterstützt, wenn der Konsolen-Agent vor Ort installiert ist.

   d. Wählen Sie **Los geht’s**.

Geben Sie die Anmeldeinformationen des Cloud-Anbieters an die NetApp Console weiter

Nachdem Sie den Konsolen-Agenten installiert und eingerichtet haben, fügen Sie Ihre Cloud-

Anmeldeinformationen hinzu, damit der Konsolen-Agent über die erforderlichen Berechtigungen zum Ausführen von Aktionen in AWS oder Azure verfügt.

AWS

Bevor Sie beginnen

Wenn Sie diese AWS-Anmeldeinformationen gerade erstellt haben, kann es einige Minuten dauern, bis sie verfügbar sind. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zur Konsole hinzufügen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie *Amazon Web Services > Agent.
   b. **Anmeldeinformationen definieren**: Geben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel ein.
   c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.
   d. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Sie können jetzt zu "NetApp Console" um mit der Verwendung des Konsolenagenten zu beginnen.

Azurblau

Bevor Sie beginnen

Wenn Sie diese Azure-Anmeldeinformationen gerade erstellt haben, kann es einige Minuten dauern, bis sie verfügbar sind. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zum Konsolenagenten hinzufügen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Microsoft Azure > Agent**.
   b. **Anmeldeinformationen definieren**: Geben Sie Informationen zum Microsoft Entra-Dienstprinzipal ein, der die erforderlichen Berechtigungen erteilt:
      - Anwendungs-ID (Client-ID)
      - Verzeichnis-ID (Mandant)
      - Client-Geheimnis
   c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.
   d. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Ergebnis

Der Konsolenagent verfügt jetzt über die erforderlichen Berechtigungen, um in Ihrem Namen Aktionen in Azure auszuführen. Sie können jetzt zu "NetApp Console" um mit der Verwendung des Konsolenagenten

zu beginnen.

Installieren Sie einen Konsolenagenten vor Ort mit VCenter

Wenn Sie ein VMWare-Benutzer sind, können Sie eine OVA verwenden, um einen Konsolenagenten in Ihrem VCenter zu installieren. Der OVA-Download oder die URL ist über die NetApp Console verfügbar.

Wenn Sie einen Konsolenagenten mit Ihren VCenter-Tools installieren, können Sie die VM-Webkonsole verwenden, um Wartungsaufgaben durchzuführen."Erfahren Sie mehr über die VM-Konsole für den Agenten."

Vorbereiten der Installation des Konsolenagenten

Stellen Sie vor der Installation sicher, dass Ihr VM-Host die Anforderungen erfüllt und der Konsolenagent auf das Internet und die Zielnetzwerke zugreifen kann. Um NetApp -Datendienste oder Cloud Volumes ONTAP zu verwenden, erstellen Sie Anmeldeinformationen für den Cloud-Anbieter, damit der Konsolenagent Aktionen in Ihrem Namen ausführen kann.

Überprüfen der Hostanforderungen für den Konsolenagenten

Stellen Sie sicher, dass Ihr Hostcomputer die Installationsanforderungen erfüllt, bevor Sie den Konsolenagenten installieren.

- CPU: 8 Kerne oder 8 vCPUs
- Arbeitsspeicher: 32 GB
- Festplattenspeicher: 165 GB (Thick Provisioning)
- vSphere 7.0 oder höher
- ESXi-Host 7.03 oder höher

Installieren Sie den Agenten in einer vCenter-Umgebung und nicht direkt auf einem ESXi-Host.

Einrichten des Netzwerkzugriffs für den Konsolenagenten

Arbeiten Sie mit Ihrem Netzwerkadministrator zusammen, um sicherzustellen, dass der Konsolenagent ausgehenden Zugriff auf die erforderlichen Endpunkte und Verbindungen zu Zielnetzwerken hat.

Verbindungen zu Zielnetzwerken

Der Konsolenagent erfordert eine Netzwerkverbindung zu dem Standort, an dem Sie Systeme erstellen und verwalten möchten. Beispielsweise das Netzwerk, in dem Sie Cloud Volumes ONTAP -Systeme oder ein Speichersystem in Ihrer lokalen Umgebung erstellen möchten.

Ausgehender Internetzugang

Der Netzwerkstandort, an dem Sie den Konsolenagenten bereitstellen, muss über eine ausgehende Internetverbindung verfügen, um bestimmte Endpunkte zu kontaktieren.

Von Computern kontaktierte Endpunkte bei Verwendung der webbasierten NetApp Console

Computer, die über einen Webbrowser auf die Konsole zugreifen, müssen in der Lage sein, mehrere Endpunkte zu kontaktieren. Sie müssen die Konsole verwenden, um den Konsolenagenten einzurichten und für die tägliche Verwendung der Konsole.

"Vorbereiten des Netzwerks für die NetApp Konsole" .

Vom Konsolenagenten kontaktierte Endpunkte

Der Konsolenagent benötigt ausgehenden Internetzugang, um die folgenden Endpunkte zu kontaktieren und Ressourcen und Prozesse innerhalb Ihrer öffentlichen Cloud-Umgebung für den täglichen Betrieb zu verwalten.

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

> Sie können keine Ressourcen in Google Cloud verwalten, wenn bei Ihnen vor Ort ein Konsolenagent installiert ist. Installieren Sie zum Verwalten von Google Cloud-Ressourcen einen Agenten in Google Cloud.

AWS

Wenn der Konsolenagent vor Ort installiert wird, benötigt er Netzwerkzugriff auf die folgenden AWS-Endpunkte, um in AWS bereitgestellte NetApp -Systeme (wie Cloud Volumes ONTAP) zu verwalten.

Vom Konsolenagenten kontaktierte Endpunkte

Der Konsolenagent benötigt ausgehenden Internetzugang, um die folgenden Endpunkte zu kontaktieren und Ressourcen und Prozesse innerhalb Ihrer öffentlichen Cloud-Umgebung für den täglichen Betrieb zu verwalten.

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)	Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab. "Weitere Einzelheiten finden Sie in der AWS-Dokumentation."
Amazon FsX für NetApp ONTAP: • api.workloads.netapp.com	Die webbasierte Konsole kontaktiert diesen Endpunkt, um mit den Workload Factory APIs zu interagieren und so FSx for ONTAP basierte Workloads zu verwalten und zu betreiben.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.

Endpunkte	Zweck
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. • Wenn Sie einen neuen Agenten bereitstellen, testet die Validierungsprüfung die Konnektivität zu aktuellen Endpunkten. Wenn Sie"vorherige Endpunkte" , schlägt die Validierungsprüfung fehl. Um diesen Fehler zu vermeiden, überspringen Sie die Validierungsprüfung. Obwohl die vorherigen Endpunkte weiterhin unterstützt werden, empfiehlt NetApp , Ihre Firewall-Regeln so schnell wie möglich auf die aktuellen Endpunkte zu aktualisieren. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" . • Wenn Sie auf die aktuellen Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Azurblau

Wenn der Konsolenagent vor Ort installiert wird, benötigt er Netzwerkzugriff auf die folgenden Azure-Endpunkte, um in Azure bereitgestellte NetApp -Systeme (wie Cloud Volumes ONTAP) zu verwalten.

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Zum Verwalten von Ressourcen in öffentlichen Azure-Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Zum Verwalten von Ressourcen in Azure China-Regionen.

Endpunkte	Zweck
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.

Endpunkte	Zweck
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. • Wenn Sie einen neuen Agenten bereitstellen, testet die Validierungsprüfung die Konnektivität zu aktuellen Endpunkten. Wenn Sie"vorherige Endpunkte" , schlägt die Validierungsprüfung fehl. Um diesen Fehler zu vermeiden, überspringen Sie die Validierungsprüfung. Obwohl die vorherigen Endpunkte weiterhin unterstützt werden, empfiehlt NetApp , Ihre Firewall-Regeln so schnell wie möglich auf die aktuellen Endpunkte zu aktualisieren. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" . • Wenn Sie auf die aktuellen Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Proxyserver

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Wenn Sie einen transparenten Proxy verwenden, müssen Sie nur das Zertifikat für den Proxyserver angeben. Wenn Sie einen expliziten Proxy verwenden, benötigen Sie auch die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

Es gibt keinen eingehenden Datenverkehr zum Konsolenagenten, es sei denn, Sie initiieren ihn oder er wird als Proxy zum Senden von AutoSupport Nachrichten von Cloud Volumes ONTAP an den NetApp Support verwendet.

- HTTP (80) und HTTPS (443) ermöglichen den Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) wird nur benötigt, wenn Sie zur Fehlerbehebung eine Verbindung zum Host herstellen müssen.

- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP -Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

  Wenn Cloud Volumes ONTAP -Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport Nachrichten haben, konfiguriert die Konsole diese Systeme automatisch für die Verwendung eines Proxyservers, der im Konsolenagenten enthalten ist. Die einzige Voraussetzung besteht darin, sicherzustellen, dass die Sicherheitsgruppe des Konsolenagenten eingehende Verbindungen über Port 3128 zulässt. Sie müssen diesen Port öffnen, nachdem Sie den Konsolenagenten bereitgestellt haben.

Aktivieren von NTP

Wenn Sie NetApp Data Classification zum Scannen Ihrer Unternehmensdatenquellen verwenden möchten, sollten Sie sowohl auf dem Konsolenagenten als auch auf dem NetApp Data Classification -System einen Network Time Protocol (NTP)-Dienst aktivieren, damit die Zeit zwischen den Systemen synchronisiert wird. "Erfahren Sie mehr über die NetApp Datenklassifizierung"

Erstellen Sie Cloud-Berechtigungen für den Konsolenagenten für AWS oder Azure

Wenn Sie NetApp Datendienste in AWS oder Azure mit einem lokalen Konsolenagenten verwenden möchten, müssen Sie bei Ihrem Cloud-Anbieter Berechtigungen einrichten, damit Sie dem Konsolenagenten nach der Installation die Anmeldeinformationen hinzufügen können.

Sie können keine Ressourcen in Google Cloud verwalten, wenn bei Ihnen vor Ort ein Konsolenagent installiert ist. Wenn Sie Google Cloud-Ressourcen verwalten möchten, müssen Sie einen Agenten in Google Cloud installieren.

AWS

Stellen Sie für lokale Konsolenagenten AWS-Berechtigungen bereit, indem Sie IAM-Benutzerzugriffsschlüssel hinzufügen.

Verwenden Sie IAM-Benutzerzugriffsschlüssel für lokale Konsolen-Agenten. IAM-Rollen werden für lokale Konsolen-Agenten nicht unterstützt.

Schritte

1. Melden Sie sich bei der AWS-Konsole an und navigieren Sie zum IAM-Dienst.
2. Erstellen Sie eine Richtlinie:

   a. Wählen Sie **Richtlinien > Richtlinie erstellen**.

   b. Wählen Sie **JSON** und kopieren und fügen Sie den Inhalt des"IAM-Richtlinie für den Konsolenagenten" .

   c. Führen Sie die restlichen Schritte aus, um die Richtlinie zu erstellen.

      Abhängig von den NetApp -Datendiensten, die Sie verwenden möchten, müssen Sie möglicherweise eine zweite Richtlinie erstellen.

   Für Standardregionen sind die Berechtigungen auf zwei Richtlinien verteilt. Aufgrund einer maximalen Zeichengrößenbeschränkung für verwaltete Richtlinien in AWS sind zwei Richtlinien erforderlich. "Weitere Informationen zu IAM-Richtlinien für den Konsolenagenten" .

3. Hängen Sie die Richtlinien an einen IAM-Benutzer an.
   - "AWS-Dokumentation: Erstellen von IAM-Rollen"
   - "AWS-Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"
4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie der NetApp Console hinzufügen können, nachdem Sie den Konsolen-Agenten installiert haben.

Ergebnis

Sie sollten jetzt über IAM-Benutzerzugriffsschlüssel mit den erforderlichen Berechtigungen verfügen. Nachdem Sie den Konsolenagenten installiert haben, verknüpfen Sie diese Anmeldeinformationen mit dem Konsolenagenten aus der Konsole.

Azurblau

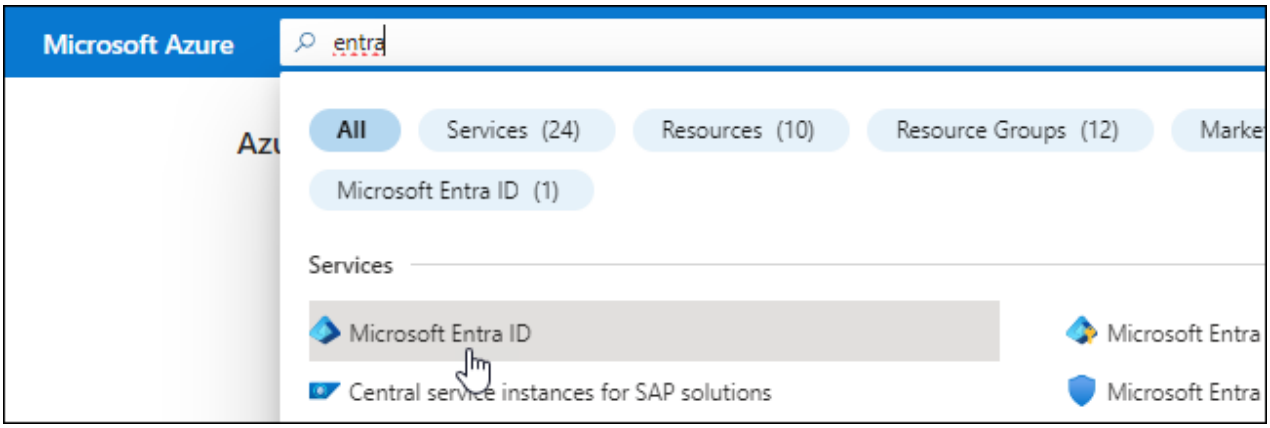
Wenn der Konsolen-Agent vor Ort installiert ist, müssen Sie dem Konsolen-Agenten Azure-Berechtigungen erteilen, indem Sie einen Dienstprinzipal in der Microsoft Entra ID einrichten und die Azure-Anmeldeinformationen abrufen, die der Konsolen-Agent benötigt.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffskontrolle

1. Stellen Sie sicher, dass Sie in Azure über die Berechtigung verfügen, eine Active Directory-Anwendung zu erstellen und die Anwendung einer Rolle zuzuweisen.

   Weitere Einzelheiten finden Sie unter "Microsoft Azure-Dokumentation: Erforderliche Berechtigungen"

2. Öffnen Sie im Azure-Portal den Dienst **Microsoft Entra ID**.



3. Wählen Sie im Menü **App-Registrierungen** aus.
4. Wählen Sie **Neuregistrierung**.
5. Geben Sie Details zur Anwendung an:
   - **Name**: Geben Sie einen Namen für die Anwendung ein.
   - **Kontotyp**: Wählen Sie einen Kontotyp aus (alle funktionieren mit der NetApp Console).
   - **Umleitungs-URI**: Sie können dieses Feld leer lassen.
6. Wählen Sie **Registrieren**.

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der Anwendung zu einer Rolle

1. Erstellen Sie eine benutzerdefinierte Rolle:

   Beachten Sie, dass Sie eine benutzerdefinierte Azure-Rolle mithilfe des Azure-Portals, Azure PowerShell, Azure CLI oder REST-API erstellen können. Die folgenden Schritte zeigen, wie Sie die Rolle mithilfe der Azure CLI erstellen. Wenn Sie eine andere Methode bevorzugen, lesen Sie bitte "Azure-Dokumentation"

   a. Kopieren Sie den Inhalt der"benutzerdefinierte Rollenberechtigungen für den Konsolenagenten" und speichern Sie sie in einer JSON-Datei.

   b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

      Sie sollten die ID für jedes Azure-Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP -Systeme erstellen.

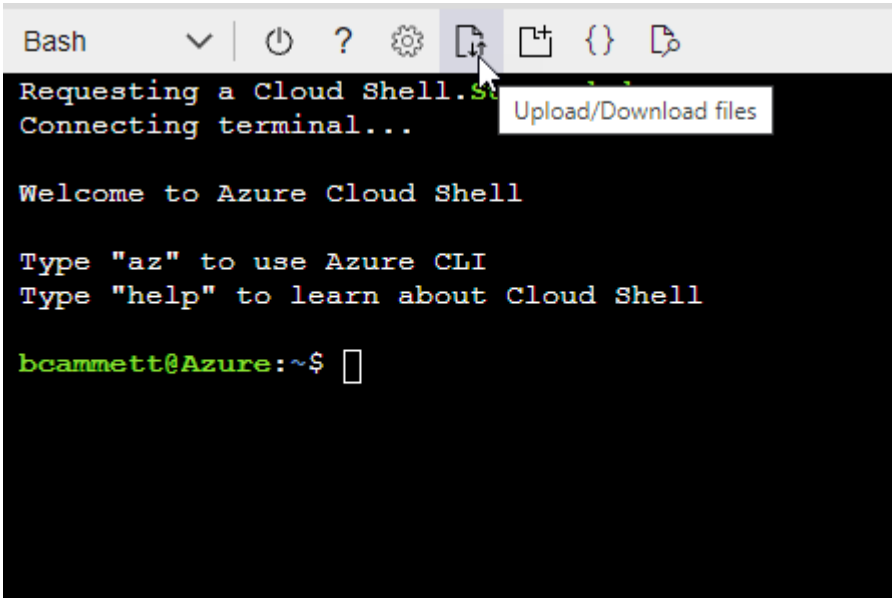
      Beispiel

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ]
      ```

   c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

Die folgenden Schritte beschreiben, wie Sie die Rolle mithilfe von Bash in Azure Cloud Shell erstellen.

- Start "Azure Cloud Shell" und wählen Sie die Bash-Umgebung.
- Laden Sie die JSON-Datei hoch.



- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
az role definition create --role-definition agent_Policy.json
```

Sie sollten jetzt über eine benutzerdefinierte Rolle namens „Konsolenoperator“ verfügen, die Sie der virtuellen Maschine des Konsolenagenten zuweisen können.

2. Weisen Sie die Anwendung der Rolle zu:

   a. Öffnen Sie im Azure-Portal den Dienst **Abonnements**.

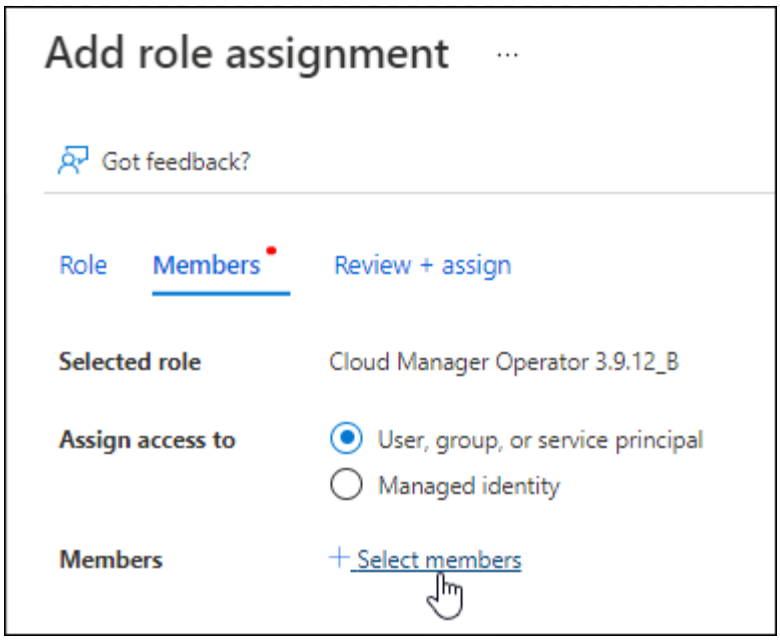
   b. Wählen Sie das Abonnement aus.

   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

   d. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.

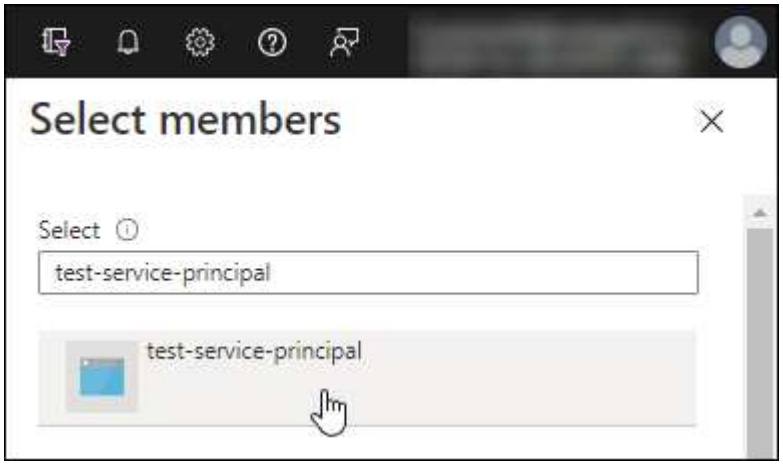
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - Behalten Sie die Auswahl von **Benutzer, Gruppe oder Dienstprinzipal** bei.
      - Wählen Sie **Mitglieder auswählen**.



- Suchen Sie nach dem Namen der Anwendung.

  Hier ist ein Beispiel:



- Wählen Sie die Anwendung aus und wählen Sie **Auswählen**.
- Wählen Sie **Weiter**.

f. Wählen Sie **Überprüfen + zuweisen**.

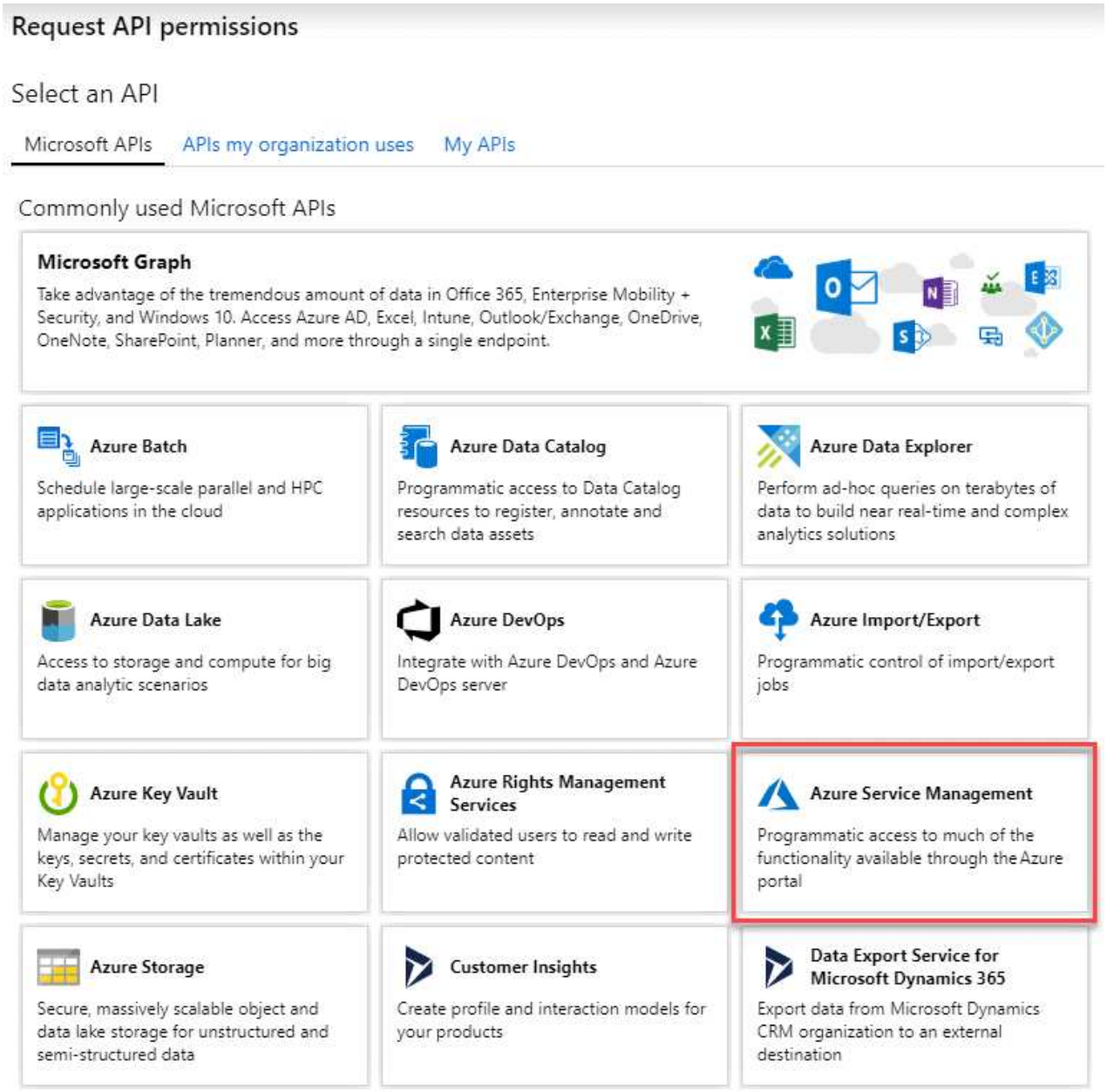
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

Wenn Sie Cloud Volumes ONTAP aus mehreren Azure-Abonnements bereitstellen möchten, müssen Sie den Dienstprinzipal an jedes dieser Abonnements binden. In der NetApp Console können Sie das Abonnement auswählen, das Sie beim Bereitstellen von Cloud Volumes ONTAP verwenden möchten.

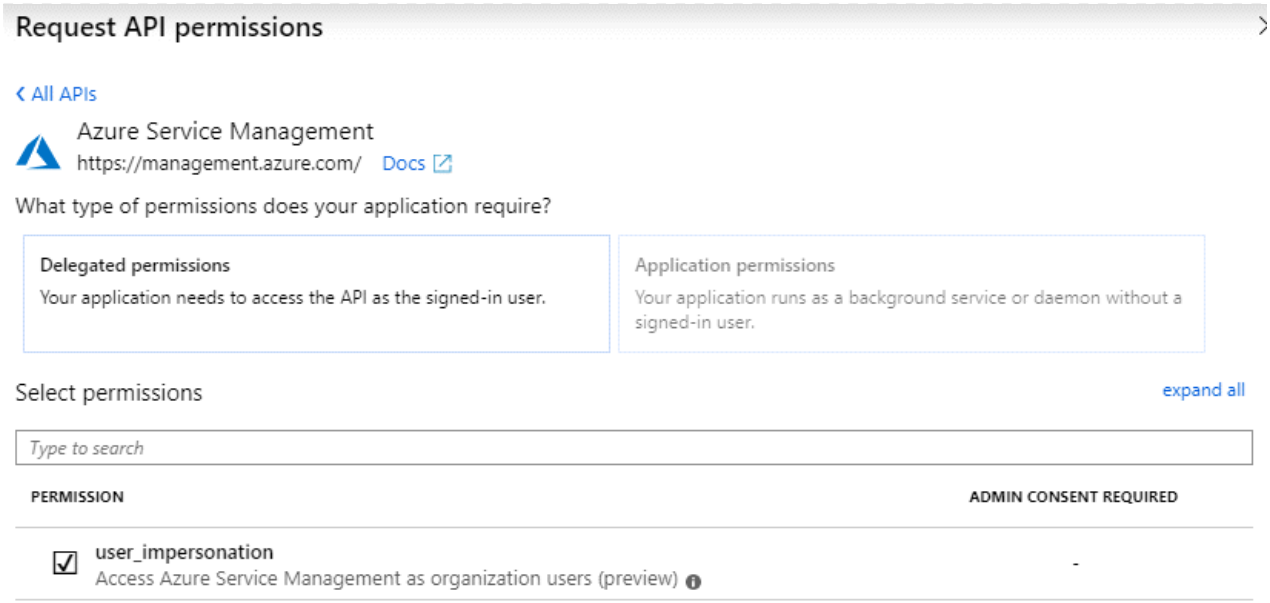
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Wählen Sie **API-Berechtigungen > Berechtigung hinzufügen**.

3. Wählen Sie unter **Microsoft-APIs Azure Service Management** aus.

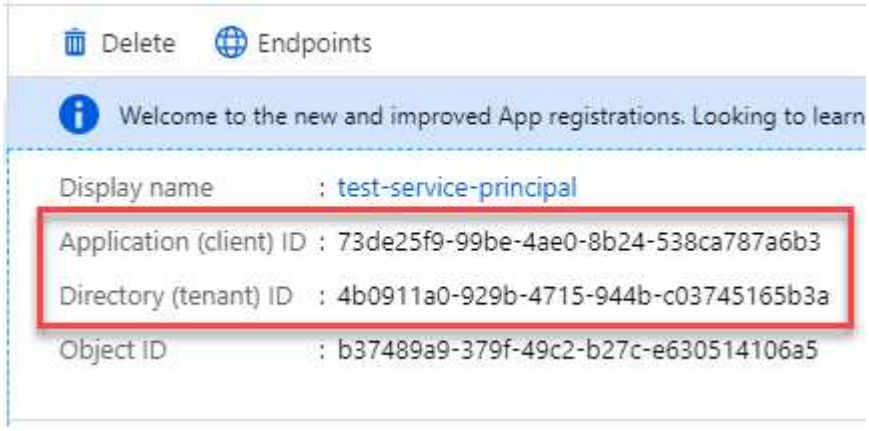


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



Abrufen der Anwendungs-ID und Verzeichnis-ID für die Anwendung

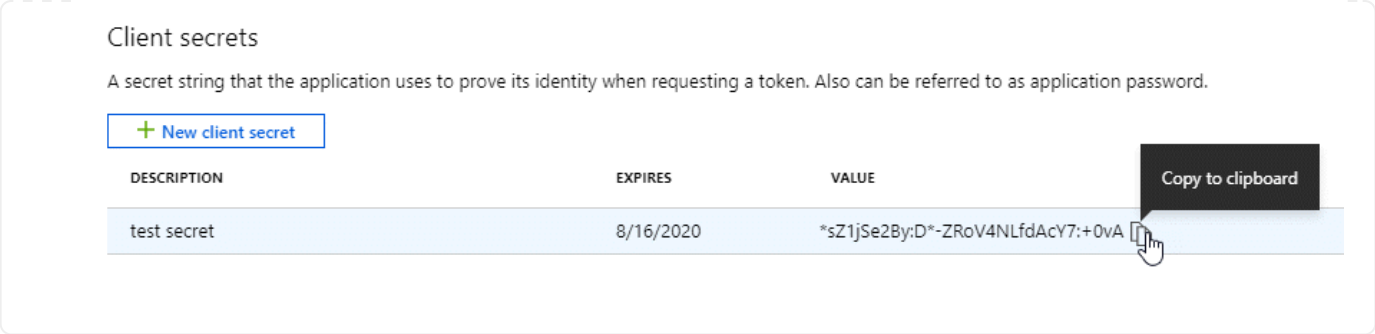
1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



Wenn Sie das Azure-Konto zur Konsole hinzufügen, müssen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) für die Anwendung angeben. Die Konsole verwendet die IDs zur programmgesteuerten Anmeldung.

Erstellen eines Client-Geheimnisses

1. Öffnen Sie den Dienst **Microsoft Entra ID**.
2. Wählen Sie **App-Registrierungen** und wählen Sie Ihre Anwendung aus.
3. Wählen Sie **Zertifikate und Geheimnisse > Neues Clientgeheimnis**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Wählen Sie **Hinzufügen**.
6. Kopieren Sie den Wert des Client-Geheimnisses.



Installieren Sie einen Konsolenagenten in Ihrer VCenter-Umgebung

NetApp unterstützt die Installation des Konsolenagenten in Ihrer VCenter-Umgebung. Die OVA-Datei enthält ein vorkonfiguriertes VM-Image, das Sie in Ihrer VMware-Umgebung bereitstellen können. Ein Dateidownload oder eine URL-Bereitstellung ist direkt über die NetApp Console möglich. Es umfasst die Konsolenagent-Software und ein selbstsigniertes Zertifikat.

Laden Sie die OVA herunter oder kopieren Sie die URL

Laden Sie die OVA herunter oder kopieren Sie die OVA-URL direkt von der NetApp Console.

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** die Option **Agent bereitstellen > Vor Ort** aus.
3. Wählen Sie **Mit OVA**.
4. Sie können entweder die OVA herunterladen oder die URL zur Verwendung in VCenter kopieren.

Stellen Sie den Agenten in Ihrem VCenter bereit

Melden Sie sich bei Ihrer VCenter-Umgebung an, um den Agenten bereitzustellen.

Schritte

1. Laden Sie das selbstsignierte Zertifikat zu Ihren vertrauenswürdigen Zertifikaten hoch, wenn Ihre Umgebung dies erfordert. Sie ersetzen dieses Zertifikat nach der Installation."Erfahren Sie, wie Sie das selbstsignierte Zertifikat ersetzen."
2. Stellen Sie die OVA aus der Inhaltsbibliothek oder dem lokalen System bereit.

Vom lokalen System	Aus der Inhaltsbibliothek
a. Klicken Sie mit der rechten Maustaste und wählen Sie **OVF-Vorlage bereitstellen…**. b. Wählen Sie die OVA-Datei aus der URL aus oder navigieren Sie zu ihrem Speicherort und wählen Sie dann **Weiter**.	a. Gehen Sie zu Ihrer Inhaltsbibliothek und wählen Sie die OVA des Konsolenagenten aus. b. Wählen Sie **Aktionen** > **Neue VM aus dieser Vorlage**

3. Schließen Sie den Assistenten „OVF-Vorlage bereitstellen“ ab, um den Konsolenagenten bereitzustellen.
4. Wählen Sie einen Namen und einen Ordner für die VM aus und wählen Sie dann **Weiter**.
5. Wählen Sie eine Computeressource aus und klicken Sie dann auf **Weiter**.
6. Überprüfen Sie die Details der Vorlage und wählen Sie dann **Weiter**.
7. Akzeptieren Sie die Lizenzvereinbarung und wählen Sie dann **Weiter**.

8. Wählen Sie den Typ der Proxy-Konfiguration, den Sie verwenden möchten: expliziter Proxy, transparenter Proxy oder kein Proxy.
9. Wählen Sie den Datenspeicher aus, in dem Sie die VM bereitstellen möchten, und wählen Sie dann **Weiter**. Stellen Sie sicher, dass es die Hostanforderungen erfüllt.
10. Wählen Sie das Netzwerk aus, mit dem Sie die VM verbinden möchten, und wählen Sie dann **Weiter**. Stellen Sie sicher, dass das Netzwerk IPv4 ist und über ausgehenden Internetzugriff auf die erforderlichen Endpunkte verfügt.
11. Füllen Sie im Fenster **Vorlage anpassen** die folgenden Felder aus:
    - **Proxy-Informationen**
      - Wenn Sie einen expliziten Proxy ausgewählt haben, geben Sie den Hostnamen oder die IP-Adresse und die Portnummer des Proxyservers sowie den Benutzernamen und das Kennwort ein.
      - Wenn Sie einen transparenten Proxy ausgewählt haben, laden Sie das entsprechende Zertifikat hoch.
    - **Konfiguration der virtuellen Maschine**
      - **Konfigurationsprüfung überspringen**: Dieses Kontrollkästchen ist standardmäßig deaktiviert, was bedeutet, dass der Agent eine Konfigurationsprüfung durchführt, um den Netzwerkzugriff zu validieren.
        - NetApp empfiehlt, dieses Kontrollkästchen deaktiviert zu lassen, damit die Installation eine Konfigurationsprüfung des Agenten umfasst. Die Konfigurationsprüfung bestätigt, dass der Agent Netzwerkzugriff auf die erforderlichen Endpunkte hat. Wenn die Bereitstellung aufgrund von Verbindungsproblemen fehlschlägt, können Sie auf den Validierungsbericht und die Protokolle vom Agent-Host zugreifen. In einigen Fällen können Sie die Prüfung überspringen, wenn Sie sicher sind, dass der Agent über Netzwerkzugriff verfügt. Wenn Sie beispielsweise immer noch die"vorherige Endpunkte" für Agent-Upgrades verwendet wird, schlägt die Validierung mit einem Fehler fehl. Um dies zu vermeiden, aktivieren Sie das Kontrollkästchen, um die Installation ohne Validierungsprüfung durchzuführen. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" .
      - **Wartungskennwort**: Legen Sie das Kennwort für die `maint` Benutzer, der Zugriff auf die Agenten-Wartungskonsole ermöglicht.
      - **NTP-Server**: Geben Sie einen oder mehrere NTP-Server für die Zeitsynchronisierung an.
      - **Hostname**: Legen Sie den Hostnamen für diese VM fest. Die Suchdomäne darf nicht enthalten sein. Beispielsweise sollte ein FQDN von console10.searchdomain.company.com als console10 eingegeben werden.
      - **Primärer DNS**: Geben Sie den primären DNS-Server an, der für die Namensauflösung verwendet werden soll.
      - **Sekundärer DNS**: Geben Sie den sekundären DNS-Server an, der für die Namensauflösung verwendet werden soll.
      - Suchdomänen: Geben Sie den Suchdomänennamen an, der beim Auflösen des Hostnamens verwendet werden soll. Wenn der FQDN beispielsweise console10.searchdomain.company.com lautet, geben Sie searchdomain.company.com ein.
      - **IPv4-Adresse**: Die IP-Adresse, die dem Hostnamen zugeordnet ist.
      - **IPv4-Subnetzmaske**: Die Subnetzmaske für die IPv4-Adresse.
      - **IPv4-Gateway-Adresse**: Die Gateway-Adresse für die IPv4-Adresse.
12. Wählen Sie **Weiter**.
13. Überprüfen Sie die Details im Fenster **Bereit zum Abschließen** und wählen Sie **Fertig**.

Die vSphere-Taskleiste zeigt den Fortschritt der Bereitstellung des Konsolenagenten an.

14. Schalten Sie die VM ein.

> Wenn die Bereitstellung fehlschlägt, können Sie auf den Validierungsbericht und die Protokolle vom Agent-Host zugreifen."Erfahren Sie, wie Sie Installationsprobleme beheben."

Registrieren Sie den Konsolenagenten bei der NetApp Console

Melden Sie sich bei der Konsole an und verknüpfen Sie den Konsolenagenten mit Ihrer Organisation. Die Art der Anmeldung hängt vom Modus ab, in dem Sie die Konsole verwenden. Wenn Sie die Konsole im Standardmodus verwenden, melden Sie sich über die SaaS-Website an. Wenn Sie die Konsole im eingeschränkten oder privaten Modus verwenden, melden Sie sich lokal vom Konsolen-Agent-Host aus an.

Schritte

1. Öffnen Sie einen Webbrowser und geben Sie die Host-URL des Konsolenagenten ein:

   Die Host-URL der Konsole kann je nach Konfiguration des Hosts ein lokaler Host, eine private IP-Adresse oder eine öffentliche IP-Adresse sein. Wenn sich der Konsolenagent beispielsweise in der öffentlichen Cloud ohne öffentliche IP-Adresse befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der über eine Verbindung zum Host des Konsolenagenten verfügt.

2. Registrieren oder anmelden.
3. Richten Sie nach der Anmeldung die Konsole ein:
   a. Geben Sie die Konsolenorganisation an, die mit dem Konsolenagenten verknüpft werden soll.
   b. Geben Sie einen Namen für das System ein.
   c. Lassen Sie unter **Arbeiten Sie in einer sicheren Umgebung?** den eingeschränkten Modus deaktiviert.

      Der eingeschränkte Modus wird nicht unterstützt, wenn der Konsolen-Agent vor Ort installiert ist.

   d. Wählen Sie **Los geht’s**.

Fügen Sie der Konsole Anmeldeinformationen des Cloud-Anbieters hinzu

Nachdem Sie den Konsolen-Agenten installiert und eingerichtet haben, fügen Sie Ihre Cloud-Anmeldeinformationen hinzu, damit der Konsolen-Agent über die erforderlichen Berechtigungen zum Ausführen von Aktionen in AWS oder Azure verfügt.

AWS

Bevor Sie beginnen

Wenn Sie diese AWS-Anmeldeinformationen gerade erstellt haben, kann es einige Minuten dauern, bis sie verfügbar sind. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zur Konsole hinzufügen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie *Amazon Web Services > Agent.
   b. **Anmeldeinformationen definieren**: Geben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel ein.
   c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.
   d. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Sie können jetzt zu "NetApp Console" um mit der Verwendung des Konsolenagenten zu beginnen.

Azurblau

Bevor Sie beginnen

Wenn Sie diese Azure-Anmeldeinformationen gerade erstellt haben, kann es einige Minuten dauern, bis sie verfügbar sind. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zum Konsolenagenten hinzufügen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Microsoft Azure > Agent**.
   b. **Anmeldeinformationen definieren**: Geben Sie Informationen zum Microsoft Entra-Dienstprinzipal ein, der die erforderlichen Berechtigungen erteilt:
      - Anwendungs-ID (Client-ID)
      - Verzeichnis-ID (Mandant)
      - Client-Geheimnis
   c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.
   d. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Ergebnis

Der Konsolenagent verfügt jetzt über die erforderlichen Berechtigungen, um in Ihrem Namen Aktionen in Azure auszuführen. Sie können jetzt zu "NetApp Console" um mit der Verwendung des Konsolenagenten

zu beginnen.

Ports für den lokalen Konsolenagenten

Der Konsolenagent verwendet *eingehende* Ports, wenn er manuell auf einem lokalen Linux-Host installiert wird. Beziehen Sie sich bei Planungen auf diese Häfen.

Diese eingehenden Regeln gelten für alle Bereitstellungsmodi der NetApp Console .

Protokoll	Hafen	Zweck
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Upgrade-Prozesses von Cloud Volumes ONTAP verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche

Konsolenagenten verwalten

Verwalten Sie einen VCenter- oder ESXi-Host für den Konsolenagenten

Sie können nach der Bereitstellung des Konsolenagenten Änderungen an Ihrem vorhandenen VCenter- oder ESXi-Host vornehmen. Sie können beispielsweise die CPU oder den RAM der VM-Instanz erhöhen, die den Konsolenagenten hostet.

Führen Sie diese Wartungsaufgaben mithilfe der VM-Webkonsole durch:

- Erhöhen Sie die Festplattengröße
- Starten Sie den Agenten neu
- Aktualisieren statischer Routen
- Suchdomänen aktualisieren

Einschränkungen

Das Upgrade des Agenten über die Konsole wird noch nicht unterstützt. Darüber hinaus können Sie nur Informationen zur IP-Adresse, zum DNS und zu Gateways anzeigen.

Zugriff auf die VM-Wartungskonsole

Sie können vom VSphere-Client aus auf die Wartungskonsole zugreifen.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.

Ändern Sie das Kennwort des Wartungsbenutzers

Sie können das Passwort für die `maint` Benutzer.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `1` , um die `System Configuration` Speisekarte.
6. Eingeben `1` um das Wartungsbenutzerkennwort zu ändern und den Anweisungen auf dem Bildschirm zu folgen.

Erhöhen Sie die CPU oder den RAM der VM-Instanz

Sie können die CPU oder den RAM der VM-Instanz erhöhen, die den Konsolenagenten hostet.

Bearbeiten Sie die VM-Instanzeinstellungen in Ihrem VCenter- oder ESXi-Host und wenden Sie die Änderungen dann mit der Wartungskonsole an.

Schritte im VSphere-Client

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Klicken Sie mit der rechten Maustaste auf die VM-Instanz und wählen Sie **Einstellungen bearbeiten**.
4. Erhöhen Sie den für die Partition /opt oder /var verwendeten Festplattenspeicher.
   a. Wählen Sie **Festplatte 2**, um den für /opt verwendeten Festplattenspeicher zu erhöhen.
   b. Wählen Sie **Festplatte 3**, um den für /var verwendeten Festplattenspeicher zu erhöhen.
5. Speichern Sie Ihre Änderungen.

Schritte in der Wartungskonsole

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `1 to view the `System Configuration` Speisekarte.
6. Eingeben `2` und folgen Sie den Anweisungen auf dem Bildschirm. Die Konsole sucht nach neuen Einstellungen und vergrößert die Partitionen.

Netzwerkeinstellungen für die Agent-VM anzeigen

Zeigen Sie die Netzwerkeinstellungen für die Agent-VM im VSphere-Client an, um Netzwerkprobleme zu bestätigen oder zu beheben. Sie können die folgenden Netzwerkeinstellungen nur anzeigen (nicht

aktualisieren): IP-Adresse und DNS-Details.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `2` , um die `Network Configuration` Speisekarte.
6. Geben Sie eine Zahl zwischen 1 und 6 ein, um die entsprechenden Netzwerkeinstellungen anzuzeigen.

Aktualisieren Sie die statischen Routen für die Agent-VM

Fügen Sie nach Bedarf statische Routen für die Agent-VM hinzu, aktualisieren oder entfernen Sie sie.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `2` , um die `Network Configuration` Speisekarte.
6. Eingeben `7` um statische Routen zu aktualisieren und den Anweisungen auf dem Bildschirm zu folgen.
7. Drücken Sie die Eingabetaste.
8. Nehmen Sie optional weitere Änderungen vor.
9. Eingeben `9` um Ihre Änderungen zu übernehmen.

Aktualisieren der Domänensucheinstellungen für die Agent-VM

Sie können die Suchdomäneneinstellungen für die Agent-VM aktualisieren.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `2`` , um die `Network Configuration` Speisekarte.
6. Eingeben `8` um die Domänensucheinstellungen zu aktualisieren und den Anweisungen auf dem Bildschirm zu folgen.
7. Drücken Sie die Eingabetaste.

8. Nehmen Sie optional weitere Änderungen vor.
9. Eingeben `9` um Ihre Änderungen zu übernehmen.

Zugriff auf die Diagnosetools des Agenten

Greifen Sie auf Diagnosetools zu, um Probleme mit dem Konsolenagenten zu beheben. Der NetApp -Support fordert Sie möglicherweise bei der Fehlerbehebung dazu auf.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `3` um das Menü „Support und Diagnose“ anzuzeigen.
6. Eingeben `1` um auf die Diagnosetools zuzugreifen und den Anweisungen auf dem Bildschirm zu folgen. + Sie können beispielsweise überprüfen, ob alle Agentendienste ausgeführt werden. "Überprüfen Sie den Status des Konsolenagenten" .

Fernzugriff auf die Diagnosetools des Agenten

Mit einem Tool wie Putty können Sie remote auf Diagnosetools zugreifen. Aktivieren Sie den SSH-Zugriff auf die Agent-VM, indem Sie ein Einmalkennwort zuweisen.

Der SSH-Zugriff ermöglicht erweiterte Terminalfunktionen wie Kopieren und Einfügen.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `3` , um die `Support and Diagnostics` Speisekarte.
6. Eingeben `2` um auf die Diagnosetools zuzugreifen und den Anweisungen auf dem Bildschirm zu folgen, um ein Einmalkennwort zu konfigurieren, das nach 24 Stunden abläuft.
7. Verwenden Sie ein SSH-Tool wie Putty, um mit dem Benutzernamen eine Verbindung zur Agent-VM herzustellen `diag` und das von Ihnen konfigurierte Einmalkennwort.

Installieren Sie ein CA-signiertes Zertifikat für den webbasierten Konsolenzugriff

Wenn Sie die NetApp Console im eingeschränkten Modus verwenden, ist die Benutzeroberfläche über die virtuelle Maschine des Konsolenagenten zugänglich, die in Ihrer Cloud-Region oder vor Ort bereitgestellt wird. Standardmäßig verwendet die Konsole ein selbstsigniertes SSL-Zertifikat, um sicheren HTTPS-Zugriff auf die

webbasierte Konsole bereitzustellen, die auf dem Konsolenagenten ausgeführt wird.

Falls Ihr Unternehmen dies erfordert, können Sie ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat installieren, das einen besseren Sicherheitsschutz bietet als ein selbstsigniertes Zertifikat. Nachdem Sie das Zertifikat installiert haben, verwendet die Konsole das von der Zertifizierungsstelle signierte Zertifikat, wenn Benutzer auf die webbasierte Konsole zugreifen.

Installieren eines HTTPS-Zertifikats

Installieren Sie ein von einer Zertifizierungsstelle signiertes Zertifikat für den sicheren Zugriff auf die webbasierte Konsole, die auf dem Konsolenagenten ausgeführt wird.

Informationen zu diesem Vorgang

Sie können das Zertifikat mit einer der folgenden Optionen installieren:

- Generieren Sie eine Zertifikatsignieranforderung (CSR) von der Konsole aus, übermitteln Sie die Zertifikatsanforderung an eine Zertifizierungsstelle und installieren Sie dann das von der Zertifizierungsstelle signierte Zertifikat auf dem Konsolenagenten.

  Das Schlüsselpaar, das die Konsole zum Generieren der CSR verwendet, wird intern auf dem Konsolenagenten gespeichert. Die Konsole ruft automatisch dasselbe Schlüsselpaar (privater Schlüssel) ab, wenn Sie das Zertifikat auf dem Konsolenagenten installieren.

- Installieren Sie ein CA-signiertes Zertifikat, das Sie bereits haben.

  Bei dieser Option wird die CSR nicht über die Konsole generiert. Sie generieren die CSR separat und speichern den privaten Schlüssel extern. Sie stellen der Konsole den privaten Schlüssel zur Verfügung, wenn Sie das Zertifikat installieren.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **HTTPS-Setup**.

   Zum Bearbeiten muss der Konsolenagent verbunden sein.

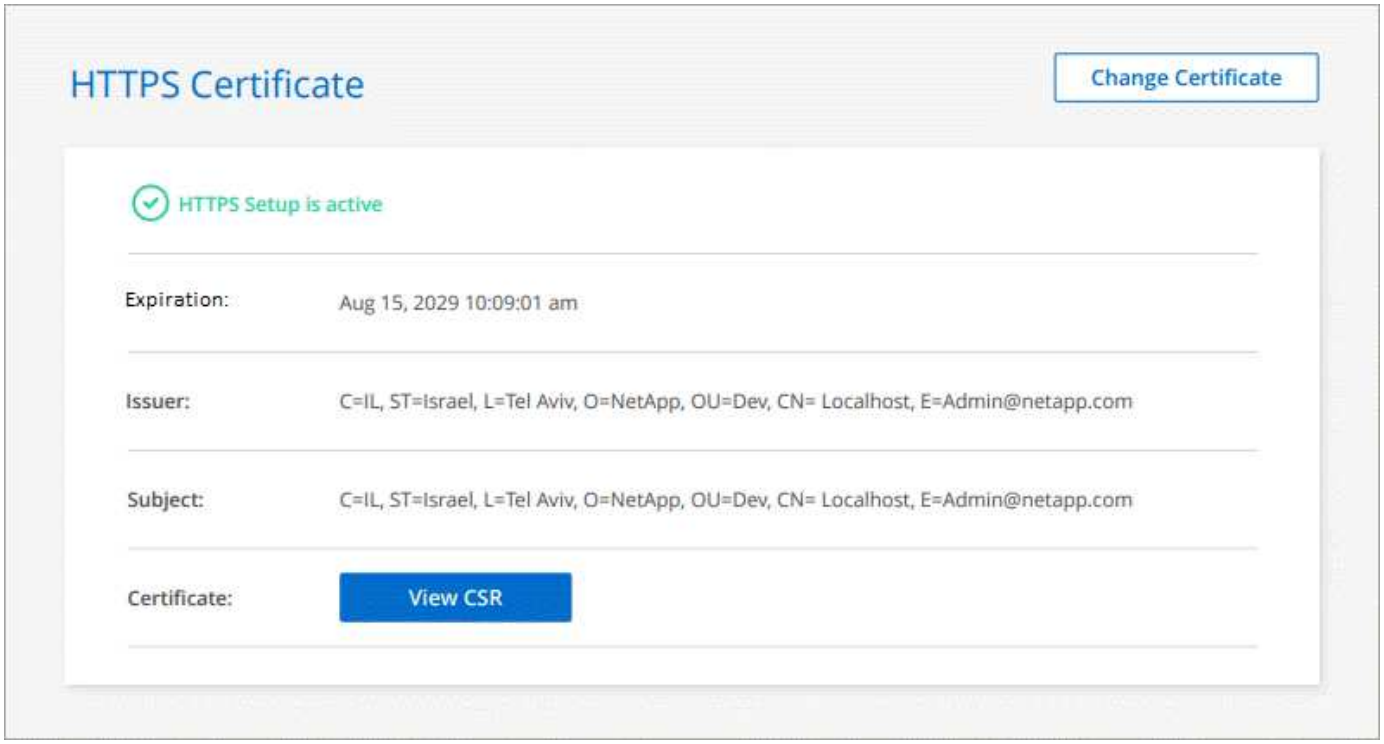
3. Installieren Sie auf der Seite „HTTPS-Setup“ ein Zertifikat, indem Sie eine Zertifikatsignieranforderung (CSR) generieren oder Ihr eigenes CA-signiertes Zertifikat installieren:

Option	Beschreibung
Erstellen Sie eine CSR	a. Geben Sie den Hostnamen oder DNS des Konsolenagent-Hosts (seinen allgemeinen Namen) ein und wählen Sie dann **CSR generieren**. Die Konsole zeigt eine Zertifikatsignieranforderung an. b. Verwenden Sie die CSR, um eine SSL-Zertifikatsanforderung an eine Zertifizierungsstelle zu senden. Das Zertifikat muss das Base-64-codierte X.509-Format von Privacy Enhanced Mail (PEM) verwenden. c. Laden Sie die Zertifikatsdatei hoch und wählen Sie dann **Installieren**.

Option	Beschreibung
Installieren Sie Ihr eigenes CA-signiertes Zertifikat	a. Wählen Sie **CA-signiertes Zertifikat installieren**. b. Laden Sie sowohl die Zertifikatsdatei als auch den privaten Schlüssel und wählen Sie dann **Installieren**. Das Zertifikat muss das Base-64-codierte X.509-Format von Privacy Enhanced Mail (PEM) verwenden.

Ergebnis

Der Konsolenagent verwendet jetzt das von der Zertifizierungsstelle signierte Zertifikat, um sicheren HTTPS-Zugriff bereitzustellen. Das folgende Bild zeigt einen Agenten, der für sicheren Zugriff konfiguriert ist:



Erneuern Sie das HTTPS-Zertifikat der Konsole

Sie sollten das HTTPS-Zertifikat des Agenten vor Ablauf erneuern, um einen sicheren Zugriff zu gewährleisten. Wenn Sie das Zertifikat nicht vor Ablauf erneuern, wird eine Warnung angezeigt, wenn Benutzer über HTTPS auf die Webkonsole zugreifen.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **HTTPS-Setup**.

   Es werden Details zum Zertifikat angezeigt, einschließlich des Ablaufdatums.

3. Wählen Sie **Zertifikat ändern** und folgen Sie den Schritten zum Generieren einer CSR oder zum Installieren Ihres eigenen CA-signierten Zertifikats.

Konfigurieren eines Konsolenagenten zur Verwendung eines Proxyservers

Wenn Ihre Unternehmensrichtlinien die Verwendung eines Proxyservers für die gesamte Kommunikation mit dem Internet erfordern, müssen Sie Ihre Agenten für die Verwendung dieses Proxyservers konfigurieren. Wenn Sie während der Installation keinen Konsolenagenten für die Verwendung eines Proxyservers konfiguriert haben, können Sie den Konsolenagenten jederzeit für die Verwendung dieses Proxyservers konfigurieren.

Der Proxyserver des Agenten ermöglicht ausgehenden Internetzugriff ohne öffentliche IP oder NAT-Gateway. Der Proxyserver bietet ausgehende Konnektivität nur für den Konsolenagenten, nicht für Cloud Volumes ONTAP Systeme.

Wenn Cloud Volumes ONTAP -Systeme keinen ausgehenden Internetzugang haben, konfiguriert die Konsole sie so, dass sie den Proxyserver des Konsolenagenten verwenden. Sie müssen sicherstellen, dass die Sicherheitsgruppe des Konsolenagenten eingehende Verbindungen über Port 3128 zulässt. Öffnen Sie diesen Port, nachdem Sie den Konsolenagenten bereitgestellt haben.

Wenn der Konsolenagent selbst keine ausgehende Internetverbindung hat, können Cloud Volumes ONTAP -Systeme den konfigurierten Proxyserver nicht verwenden.

Unterstützte Konfigurationen

- Transparente Proxyserver werden für Agenten unterstützt, die Cloud Volumes ONTAP -Systeme bedienen. Wenn Sie NetApp -Datendienste mit Cloud Volumes ONTAP verwenden, erstellen Sie einen dedizierten Agenten für Cloud Volumes ONTAP, bei dem Sie einen transparenten Proxyserver verwenden können.
- Explizite Proxyserver werden von allen Agenten unterstützt, einschließlich derjenigen, die Cloud Volumes ONTAP -Systeme verwalten, und derjenigen, die NetApp -Datendienste verwalten.
- HTTP und HTTPS.
- Der Proxyserver kann sich in der Cloud oder in Ihrem Netzwerk befinden.

> Nachdem Sie einen Proxy konfiguriert haben, können Sie den Proxy-Typ nicht mehr ändern. Wenn Sie den Proxy-Typ ändern müssen, entfernen Sie den Konsolen-Agenten und fügen einen neuen Agenten mit dem neuen Proxy-Typ hinzu.

Aktivieren Sie einen expliziten Proxy auf einem Konsolenagenten

Wenn Sie einen Konsolenagenten für die Verwendung eines Proxyservers konfigurieren, verwenden dieser Agent und die von ihm verwalteten Cloud Volumes ONTAP -Systeme (einschließlich aller HA-Mediatoren) alle den Proxyserver.

Dieser Vorgang startet den Konsolenagenten neu. Stellen Sie sicher, dass der Konsolenagent im Leerlauf ist, bevor Sie fortfahren.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **Agent bearbeiten**.

   Zum Bearbeiten muss der Konsolenagent aktiv sein.

3. Wählen Sie **HTTP-Proxy-Konfiguration**.

4. Wählen Sie im Feld „Konfigurationstyp“ **Expliziter Proxy** aus.
5. Wählen Sie **Proxy aktivieren**.
6. Geben Sie den Server mit der Syntax an http://address:port oder https://address:port
7. Geben Sie einen Benutzernamen und ein Kennwort an, wenn für den Server eine Basisauthentifizierung erforderlich ist.

   Beachten Sie Folgendes:

   - Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.
   - Für einen Domänenbenutzer müssen Sie den ASCII-Code für das \ wie folgt eingeben: Domänenname%92Benutzername

     Beispiel: netapp%92proxy

   - Die Konsole unterstützt keine Passwörter, die das @-Zeichen enthalten.
8. Wählen Sie **Speichern**.

Aktivieren Sie einen transparenten Proxy für einen Konsolenagenten

Nur Cloud Volumes ONTAP unterstützt die Verwendung eines transparenten Proxys auf dem Konsolenagenten. Wenn Sie zusätzlich zu Cloud Volumes ONTAP NetApp -Datendienste verwenden, sollten Sie einen separaten Agenten für die Verwendung für Datendienste oder für Cloud Volumes ONTAP erstellen.

Stellen Sie vor der Aktivierung eines transparenten Proxys sicher, dass die folgenden Anforderungen erfüllt sind:

- Der Agent wird im selben Netzwerk wie der transparente Proxyserver installiert.
- Die TLS-Prüfung ist auf dem Proxyserver aktiviert.
- Sie verfügen über ein Zertifikat im PEM-Format, das mit dem auf dem transparenten Proxyserver verwendeten Zertifikat übereinstimmt.
- Sie verwenden den Konsolenagenten für keine anderen NetApp -Datendienste als Cloud Volumes ONTAP.

Um einen vorhandenen Agenten für die Verwendung eines transparenten Proxyservers zu konfigurieren, verwenden Sie das Wartungstool des Konsolenagenten, das über die Befehlszeile auf dem Konsolenagentenhost verfügbar ist.

Wenn Sie einen Proxyserver konfigurieren, wird der Konsolenagent neu gestartet. Stellen Sie sicher, dass der Konsolenagent im Leerlauf ist, bevor Sie fortfahren.

Schritte

Stellen Sie sicher, dass Sie über eine Zertifikatsdatei im PEM-Format für den Proxyserver verfügen. Wenn Sie kein Zertifikat haben, wenden Sie sich an Ihren Netzwerkadministrator, um eines zu erhalten.

1. Öffnen Sie eine Befehlszeilenschnittstelle auf dem Konsolenagent-Host.
2. Navigieren Sie zum Verzeichnis des Wartungstools des Konsolenagenten: `/opt/application/netapp/service-manager-2/agent-maint-console`
3. Führen Sie den folgenden Befehl aus, um den transparenten Proxy zu aktivieren. `/home/ubuntu/<certificate-file>.pem` ist das Verzeichnis und der Name der Zertifikatsdatei, die

Sie für den Proxyserver haben:

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

Stellen Sie sicher, dass die Zertifikatsdatei im PEM-Format vorliegt und sich im selben Verzeichnis wie der Befehl befindet, oder geben Sie den vollständigen Pfad zur Zertifikatsdatei an.

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

Ändern Sie den transparenten Proxy für den Konsolenagenten

Sie können den vorhandenen transparenten Proxy-Server eines Console-Agenten aktualisieren, indem Sie die folgende Funktion verwenden: `proxy update` Befehl oder entfernen Sie den transparenten Proxy-Server mithilfe des Befehls `proxy remove` Befehl. Weitere Informationen finden Sie in der Dokumentation zu"Agenten-Wartungskonsole" Die

> Nachdem Sie einen Proxy konfiguriert haben, können Sie den Proxy-Typ nicht mehr ändern. Wenn Sie den Proxy-Typ ändern müssen, entfernen Sie den Konsolen-Agenten und fügen einen neuen Agenten mit dem neuen Proxy-Typ hinzu.

Aktualisieren Sie den Proxy des Konsolenagenten, wenn dieser den Zugriff auf das Internet verliert

Wenn sich die Proxy-Konfiguration für Ihr Netzwerk ändert, verliert Ihr Agent möglicherweise den Zugriff auf das Internet. Zum Beispiel, wenn jemand das Passwort für den Proxyserver ändert oder das Zertifikat aktualisiert. In diesem Fall müssen Sie direkt vom Konsolenagent-Host auf die Benutzeroberfläche zugreifen und die Einstellungen aktualisieren. Stellen Sie sicher, dass Sie Netzwerkzugriff auf den Konsolen-Agent-Host haben und sich bei der Konsole anmelden können.

Aktivieren Sie den direkten API-Verkehr

Wenn Sie einen Console-Agenten für die Verwendung eines Proxy-Servers konfiguriert haben, können Sie den direkten API-Datenverkehr auf dem Console-Agenten aktivieren, um API-Aufrufe direkt an Cloud-Anbieterdienste zu senden, ohne den Proxy zu durchlaufen. Agenten, die in AWS, Azure oder Google Cloud ausgeführt werden, unterstützen diese Option.

Wenn Sie Azure Private Links mit Cloud Volumes ONTAP deaktivieren und Service-Endpunkte verwenden, aktivieren Sie den direkten API-Verkehr. Andernfalls wird der Datenverkehr nicht richtig weitergeleitet.

"Erfahren Sie mehr über die Verwendung eines Azure Private Link oder von Service-Endpunkten mit Cloud Volumes ONTAP"

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **Agent bearbeiten**.

   Zum Bearbeiten muss der Konsolenagent aktiv sein.

3. Wählen Sie **Direkten API-Verkehr unterstützen**.

4. Aktivieren Sie das Kontrollkästchen, um die Option zu aktivieren, und wählen Sie dann **Speichern**.

Fehlerbehebung beim Konsolen-Agent

Um Probleme mit einem Konsolenagenten zu beheben, können Sie die Probleme selbst überprüfen oder mit dem NetApp -Support zusammenarbeiten, der Sie möglicherweise nach Ihrer System-ID, Agentenversion oder den neuesten AutoSupport -Nachrichten fragt.

Wenn Sie über ein NetApp Support Site-Konto verfügen, können Sie auch die"NetApp Wissensdatenbank."

Häufige Fehlermeldungen und Lösungen

Diese Tabelle listet häufige Fehlermeldungen auf und zeigt, wie man sie beheben kann:

Fehlermeldung	Erläuterung	Was zu tun
Die Benutzeroberfläche des Konsolenagenten konnte nicht geladen werden	Die Agenteninstallation ist fehlgeschlagen	• Stellen Sie sicher, dass der Service Manager-Dienst aktiv ist. • Stellen Sie sicher, dass alle Container ausgeführt werden. • Stellen Sie sicher, dass Ihre Firewall den Zugriff auf den Dienst über Port 8888 zulässt. • Sollten weiterhin Probleme auftreten, wenden Sie sich bitte an den Support.
Auf die NetApp Agent-Benutzeroberfläche kann nicht zugegriffen werden	Diese Meldung wird angezeigt, wenn versucht wird, auf die IP-Adresse eines Agenten zuzugreifen. Die Initialisierung des Agenten kann fehlschlagen, wenn er nicht über den richtigen Netzwerkzugriff verfügt oder instabil ist.	• Stellen Sie eine Verbindung zum Konsolenagenten her. • Überprüfen Sie, ob der Service Manager-Dienst • Stellen Sie sicher, dass der Agent über den erforderlichen Netzwerkzugriff verfügt."Erfahren Sie mehr über erforderliche Endpunkte für den Netzwerkzugriff."
Agenteneinstellungen konnten nicht geladen werden	Die Konsole zeigt diese Meldung an, wenn Sie versuchen, auf die Seite mit den Agenteneinstellungen zuzugreifen.	• Überprüfen Sie, ob der OCCM-Container ausgeführt wird und funktioniert. • Wenn das Problem weiterhin besteht, wenden Sie sich an den Support.

Fehlermeldung	Erläuterung	Was zu tun
Supportinformationen für den Agenten konnten nicht geladen werden.	Diese Meldung wird angezeigt, wenn der Agent nicht auf Ihr Supportkonto zugreifen kann.	• Prüfen Sie, ob der Agent ausgehenden Zugriff auf die erforderlichen Endpunkte hat."Erfahren Sie mehr über erforderliche Endpunkte für den Netzwerkzugriff."

Überprüfen Sie den Status des Konsolenagenten

Verwenden Sie einen der folgenden Befehle, um Ihren Konsolenagenten zu überprüfen. Alle Dienste sollten den Status „Wird ausgeführt“ haben. Wenn dies nicht der Fall ist, wenden Sie sich an den NetApp Support.

Ausführlichere Informationen zum Zugriff auf die Konsolen-Agent-Diagnose finden Sie in den folgenden Themen:

- "Überprüfen Sie den Status des Konsolenagenten (für Linux-Hostbereitstellungen)."
- "Überprüfen Sie den Status des Konsolenagenten (für VCenter-Bereitstellungen)."

Docker (für Ubuntu- und VCenter-Bereitstellungen)

```
docker ps -a
```

Podman (für RedHat Enterprise Linux-Bereitstellungen)

```
podman ps -a
```

Anzeigen der Konsolen-Agent-Version

Zeigen Sie die Version des Konsolenagenten an, um das Upgrade zu bestätigen, oder teilen Sie sie Ihrem NetApp -Vertreter mit.

Schritte

1. Wählen Sie **Administration > Support > Agenten**.

   Die Konsole zeigt die Version oben auf der Seite an.

Überprüfen des Netzwerkzugriffs

Stellen Sie sicher, dass der Konsolenagent über den erforderlichen Netzwerkzugriff verfügt."Erfahren Sie mehr über die erforderlichen Netzwerkzugriffspunkte."

Führen Sie Konfigurationsprüfungen auf dem Konsolenagenten durch.

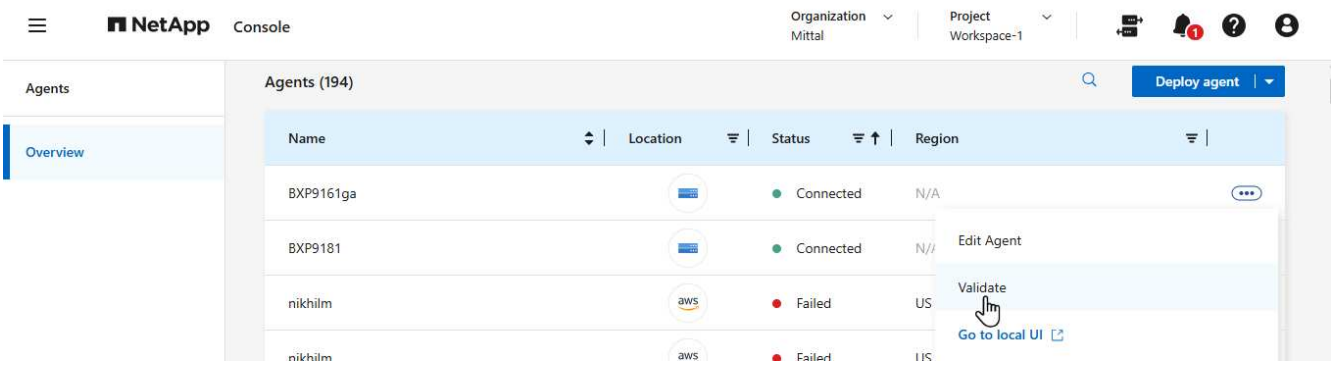
Führen Sie Konfigurationsprüfungen an den Konsolenagenten über die Konsole oder die Agentenwartungskonsole durch, um sicherzustellen, dass sie verbunden sind.

Sie können Konfigurationsprüfungen auch über die Agentenwartungskonsole durchführen."Erfahren Sie mehr über die Verwendung des Befehls config-checker validate."

Sie können nur Agenten validieren, die den Status **Verbunden** haben.

Schritte von der Konsole

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie im Aktionsmenü des Konsolenagenten, den Sie überprüfen möchten, die Option **Validieren** aus.



Die Validierung kann bis zu 15 Minuten dauern. Die Ergebnisse werden nach Abschluss des Vorgangs angezeigt.

Probleme bei der Installation des Konsolenagenten

Wenn die Installation fehlschlägt, sehen Sie sich den Bericht und die Protokolle an, um die Probleme zu beheben.

Sie können auch direkt vom Konsolen-Agent-Host in den folgenden Verzeichnissen auf den Validierungsbericht im JSON-Format und die Konfigurationsprotokolle zugreifen:

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- Bei der Bereitstellung neuer Agenten prüft NetApp die folgenden Endpunkte:"hier aufgeführt" . Diese Konfigurationsprüfung schlägt mit einem Fehler fehl, wenn Sie die vorherigen Endpunkte verwenden, die für Upgrades verwendet wurden."hier aufgeführt" . NetApp empfiehlt, Ihre Firewall-Regeln so schnell wie möglich zu aktualisieren, um den Zugriff auf die aktuellen Endpunkte zu ermöglichen und den Zugriff auf die vorherigen Endpunkte zu blockieren."Erfahren Sie, wie Sie Ihr Netzwerk aktualisieren" .
- Wenn Sie die Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Deaktivieren Sie Konfigurationsprüfungen für manuelle Installationen

Es kann vorkommen, dass Sie die Konfigurationsprüfungen deaktivieren müssen, die während der Installation die ausgehende Konnektivität überprüfen. Wenn Sie beispielsweise einen Agenten in Ihrer Government Cloud-Umgebung manuell installieren, müssen Sie die Konfigurationsprüfungen deaktivieren, da die Installation sonst fehlschlägt.

Schritte

Sie deaktivieren die Konfigurationsprüfung, indem Sie das Flag *skipConfigCheck* in der Datei *com/opt/application/netapp/service-manager-2/config.json* setzen. Standardmäßig ist dieses Flag auf „false“ gesetzt und die Konfigurationsprüfung überprüft den ausgehenden Zugriff für den Agenten. Setzen Sie dieses Flag auf „true“, um die Prüfung zu deaktivieren. Machen Sie sich mit der JSON-Syntax vertraut, bevor Sie diesen Schritt ausführen.

Um die Konfigurationsprüfung wieder zu aktivieren, führen Sie diese Schritte aus und setzen Sie das Flag *skipConfigCheck* auf „false“.

Schritte

1. Greifen Sie als Root oder mit Sudo-Berechtigungen auf den Konsolen-Agent-Host zu.
2. Erstellen Sie eine Sicherungskopie der Datei */opt/application/netapp/service-manager-2/config.json*, um sicherzustellen, dass Sie Ihre Änderungen rückgängig machen können.
3. Stoppen Sie den Dienst Service Manager 2, indem Sie den folgenden Befehl ausführen:

```
systemctl stop netapp-service-manager.service
```

1. Bearbeiten Sie die Datei */opt/application/netapp/service-manager-2/config.json* und ändern Sie den Wert des Flags *skipConfigCheck* auf „true“.

```
  "skipConfigCheck": true
```

2. Speichern Sie Ihre Datei.
3. Starten Sie den Dienst Service Manager 2 neu, indem Sie den folgenden Befehl ausführen:

```
systemctl restart netapp-service-manager.service
```

Arbeiten Sie mit dem NetApp Support

Wenn Sie die Probleme mit Ihrem Konsolenagenten nicht lösen konnten, sollten Sie sich an den NetApp -Support wenden. Der NetApp Support fragt möglicherweise nach der Konsolen-Agent-ID oder fordert Sie auf, ihm die Konsolen-Agent-Protokolle zu senden, falls diese noch nicht vorliegen.

Suchen Sie die Konsolen-Agent-ID

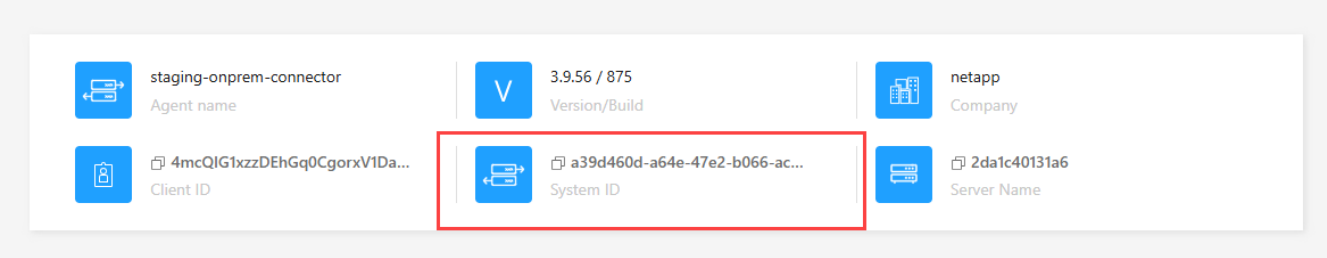
Um Ihnen den Einstieg zu erleichtern, benötigen Sie möglicherweise die System-ID Ihres Konsolenagenten. Die ID wird normalerweise für Lizenzierungs- und Fehlerbehebungszwecke verwendet.

Schritte

1. Wählen Sie **Administration > Support > Agenten**.

   Die System-ID finden Sie oben auf der Seite.

   Beispiel



2. Bewegen Sie den Mauszeiger über die ID und klicken Sie darauf, um sie zu kopieren.

Laden Sie eine AutoSupport -Nachricht herunter oder senden Sie sie

Wenn bei Ihnen Probleme auftreten, werden Sie von NetApp möglicherweise aufgefordert, zur Fehlerbehebung eine AutoSupport -Nachricht an den NetApp -Support zu senden.

Aufgrund des Lastenausgleichs benötigt die NetApp Console bis zu fünf Stunden, um AutoSupport -Nachrichten zu senden. Laden Sie für dringende Mitteilungen die Datei herunter und senden Sie sie manuell.

Schritte

1. Wählen Sie **Administration > Support > Agenten**.
2. Wählen Sie je nachdem, wie Sie die Informationen an den NetApp Support senden müssen, eine der folgenden Optionen:
   a. Wählen Sie die Option zum Herunterladen der AutoSupport -Nachricht auf Ihren lokalen Computer. Sie können es dann mit einer bevorzugten Methode an den NetApp -Support senden.
   b. Wählen Sie * AutoSupport senden*, um die Nachricht direkt an den NetApp -Support zu senden.

Beheben von Downloadfehlern bei Verwendung eines Google Cloud NAT-Gateways

Der Konsolenagent lädt automatisch Softwareupdates für Cloud Volumes ONTAP herunter. Ihre Konfiguration kann dazu führen, dass der Download fehlschlägt, wenn ein Google Cloud NAT-Gateway verwendet wird. Sie können dieses Problem beheben, indem Sie die Anzahl der Teile begrenzen, in die das Software-Image unterteilt ist. Dieser Schritt muss mithilfe der API abgeschlossen werden.

Schritt

1. Senden Sie eine PUT-Anfrage an /occm/config mit dem folgenden JSON als Text:

```
{
  "maxDownloadSessions": 32
}
```

Der Wert für *maxDownloadSessions* kann 1 oder eine beliebige Ganzzahl größer als 1 sein. Wenn der Wert 1 ist, wird das heruntergeladene Bild nicht geteilt.

Beachten Sie, dass 32 ein Beispielwert ist. Der Wert hängt von Ihrer NAT-Konfiguration und der Anzahl gleichzeitiger Sitzungen ab.

"Erfahren Sie mehr über den API-Aufruf /occm/config"

Holen Sie sich Hilfe von der NetApp Knowledge Base

"Informationen zur Fehlerbehebung anzeigen, die vom NetApp Support-Team erstellt wurden" .

Deinstallieren und Entfernen eines Konsolenagenten

Deinstallieren Sie einen Konsolenagenten, um Probleme zu beheben oder ihn dauerhaft vom Host zu entfernen. Die erforderlichen Schritte hängen vom verwendeten Bereitstellungsmodus ab. Nachdem Sie einen Konsolenagenten aus Ihrer Umgebung entfernt haben, können Sie ihn aus der Konsole entfernen.

"Erfahren Sie mehr über die Bereitstellungsmodi der NetApp Console" .

Deinstallieren Sie den Agenten, wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden

Wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden (mit anderen Worten, der Agent-Host verfügt über eine ausgehende Konnektivität), sollten Sie die folgenden Schritte ausführen, um den Agenten zu deinstallieren.

Schritte

1. Stellen Sie eine Verbindung zur Linux-VM für den Agenten her.
2. Führen Sie vom Linux-Host aus das Deinstallationsskript aus:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   silent führt das Skript aus, ohne Sie zur Bestätigung aufzufordern.

Entfernen von Konsolenagenten aus der Konsole

Wenn Sie eine Agenten-VM gelöscht oder den Agenten deinstalliert haben, sollten Sie ihn aus der Liste der Agenten in der Konsole entfernen. Nach dem Löschen einer Agenten-VM oder der Deinstallation der Agentensoftware wird der Agent in der Konsole als **Getrennt** angezeigt.

Beachten Sie beim Entfernen eines Konsolenagenten Folgendes:

- Durch diese Aktion wird die virtuelle Maschine nicht gelöscht.
- Diese Aktion kann nicht rückgängig gemacht werden. Wenn Sie einen Konsolenagenten einmal entfernt haben, können Sie ihn nicht wieder hinzufügen.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Auf der Seite **Übersicht** wählen Sie das Aktionsmenü für einen getrennten Agenten und anschließend **Agent entfernen**.
3. Geben Sie zur Bestätigung den Namen des Agenten ein und wählen Sie dann **Entfernen**.

Cloud-Anbieter-Zugangsdaten verwalten

AWS

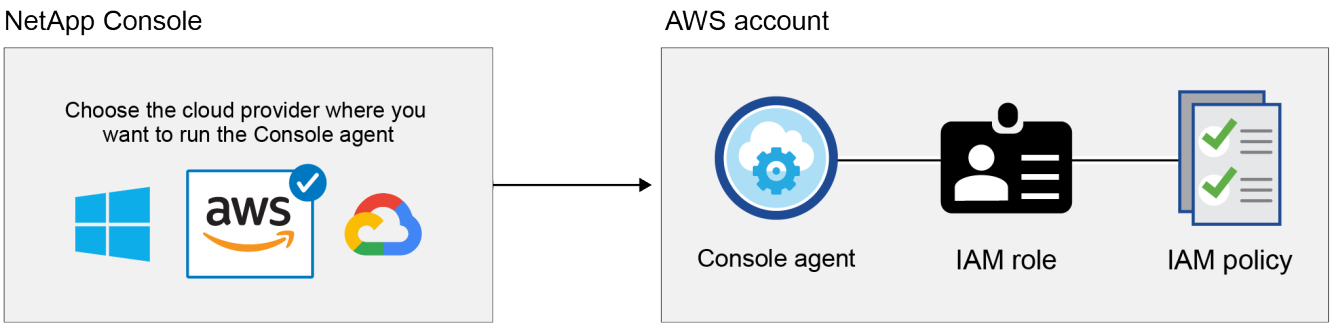
Erfahren Sie mehr über AWS-Anmeldeinformationen und Berechtigungen in der NetApp Console

Sie verwalten AWS-Zugangsdaten und Marketplace-Abonnements direkt über die NetApp Console , um eine sichere Bereitstellung von Cloud Volumes ONTAP und anderen Datendiensten zu gewährleisten, indem Sie während der Bereitstellung des Console-Agenten die entsprechenden IAM-Zugangsdaten angeben und diese zur Abrechnung mit AWS Marketplace-Abonnements verknüpfen.

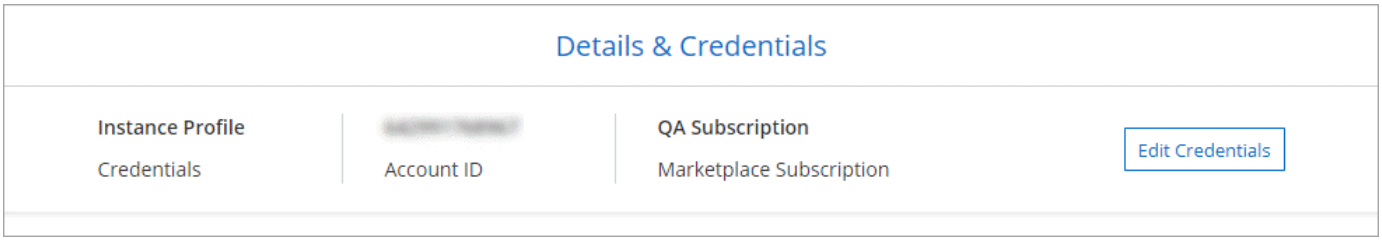
Anfängliche AWS-Anmeldeinformationen

Wenn Sie einen Konsolenagenten über die Konsole bereitstellen, müssen Sie die ARN einer IAM-Rolle oder Zugriffsschlüssel für einen IAM-Benutzer angeben. Die Authentifizierungsmethode muss über Berechtigungen zum Bereitstellen des Console-Agenten in AWS verfügen. Die erforderlichen Berechtigungen sind in der folgenden Liste aufgeführt:"Agentenbereitstellungsrichtlinie für AWS" Die

Wenn die Konsole den Konsolenagenten in AWS startet, erstellt sie eine IAM-Rolle und ein Profil für den Agenten. Außerdem wird eine Richtlinie angehängt, die dem Konsolenagenten die Berechtigung erteilt, Ressourcen und Prozesse innerhalb dieses AWS-Kontos zu verwalten. "Überprüfen Sie, wie der Agent die Berechtigungen verwendet".



Wenn Sie ein neues Cloud Volumes ONTAP -System hinzufügen, wählt die Konsole standardmäßig diese AWS-Anmeldeinformationen aus:



Stellen Sie alle Ihre Cloud Volumes ONTAP -Systeme mit den anfänglichen AWS-Anmeldeinformationen bereit, oder fügen Sie zusätzliche Anmeldeinformationen hinzu.

Zusätzliche AWS-Anmeldeinformationen

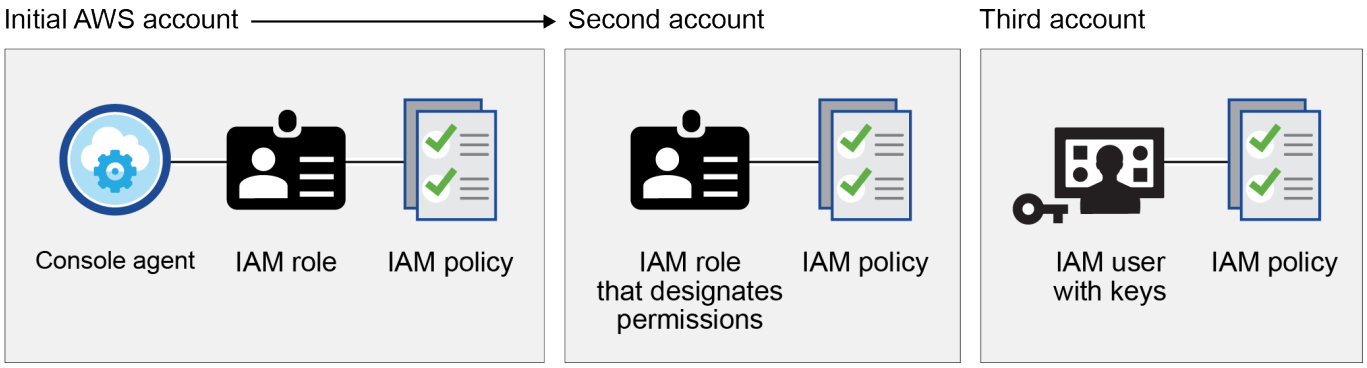
In den folgenden Fällen können Sie der Konsole zusätzliche AWS-Anmeldeinformationen hinzufügen:

- Um Ihren bestehenden Console-Agenten mit einem zusätzlichen AWS-Konto zu verwenden
- So erstellen Sie einen neuen Agenten in einem bestimmten AWS-Konto
- So erstellen und verwalten Sie FSx for ONTAP Dateisysteme

Weitere Einzelheiten finden Sie in den folgenden Abschnitten.

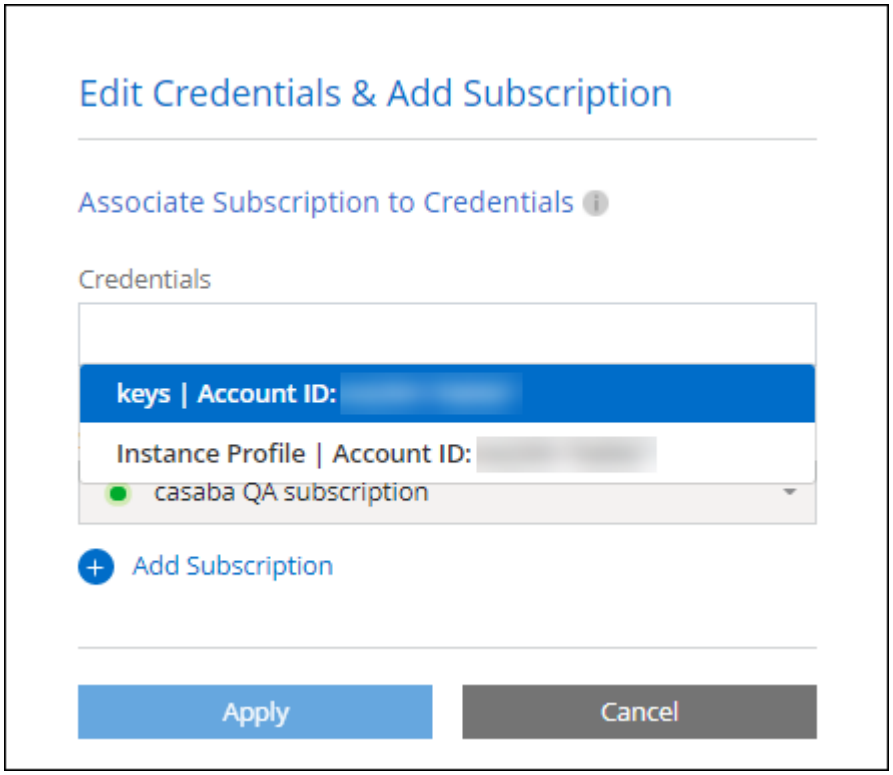
Fügen Sie AWS-Anmeldeinformationen hinzu, um einen Konsolenagenten mit einem anderen AWS-Konto zu verwenden

Um die Konsole mit zusätzlichen AWS-Konten zu verwenden, geben Sie AWS-Schlüssel oder den ARN einer Rolle in einem vertrauenswürdigen Konto an. Das folgende Bild zeigt zwei zusätzliche Konten, eines, das Berechtigungen über eine IAM-Rolle in einem vertrauenswürdigen Konto bereitstellt, und ein anderes über die AWS-Schlüssel eines IAM-Benutzers:



Sie fügen der Konsole Kontoanmeldeinformationen hinzu, indem Sie den Amazon Resource Name (ARN) der IAM-Rolle oder die AWS-Schlüssel für den IAM-Benutzer angeben.

Sie können beispielsweise beim Erstellen eines neuen Cloud Volumes ONTAP Systems zwischen Anmeldeinformationen wechseln:



"Erfahren Sie, wie Sie einem vorhandenen Agenten AWS-Anmeldeinformationen hinzufügen."

Fügen Sie AWS-Anmeldeinformationen hinzu, um einen Konsolenagenten zu erstellen

Durch das Hinzufügen von AWS-Anmeldeinformationen werden Berechtigungen zum Erstellen eines Konsolenagenten erteilt.

"Erfahren Sie, wie Sie der Konsole AWS-Anmeldeinformationen hinzufügen, um einen Konsolenagenten zu erstellen"

AWS-Anmeldeinformationen für FSx for ONTAP hinzufügen

Fügen Sie der Konsole AWS-Anmeldeinformationen hinzu, um die erforderlichen Berechtigungen zum Erstellen und Verwalten eines FSx for ONTAP Systems bereitzustellen.

"Erfahren Sie, wie Sie AWS-Anmeldeinformationen zur Konsole für Amazon FSx for ONTAP hinzufügen"

Anmeldeinformationen und Marktplatzabonnements

Sie müssen die Anmeldeinformationen, die Sie einem Console-Agenten hinzufügen, mit einem AWS Marketplace-Abonnement verknüpfen, um Cloud Volumes ONTAP auf Stundenbasis (PAYGO) und andere NetApp -Datendienste oder über einen Jahresvertrag zu bezahlen. "Erfahren Sie, wie Sie ein AWS-Abonnement zuordnen".

Beachten Sie Folgendes zu AWS-Anmeldeinformationen und Marktplatz-Abonnements:

- Sie können nur ein AWS Marketplace-Abonnement mit einem Satz AWS-Anmeldeinformationen verknüpfen
- Sie können ein bestehendes Marktplatz-Abonnement durch ein neues Abonnement ersetzen

FAQ

Die folgenden Fragen beziehen sich auf Anmeldeinformationen und Abonnements.

Wie kann ich meine AWS-Anmeldeinformationen sicher rotieren?

Wie in den obigen Abschnitten beschrieben, können Sie mit der Konsole AWS-Anmeldeinformationen auf verschiedene Weise bereitstellen: über eine mit dem Konsolenagenten verknüpfte IAM-Rolle, durch die Übernahme einer IAM-Rolle in einem vertrauenswürdigen Konto oder durch die Bereitstellung von AWS-Zugriffsschlüsseln.

Bei den ersten beiden Optionen verwendet die Konsole den AWS Security Token Service, um temporäre Anmeldeinformationen zu erhalten, die ständig rotieren. Dieses Verfahren ist die beste Vorgehensweise – es ist automatisch und sicher.

Wenn Sie der Konsole AWS-Zugriffsschlüssel bereitstellen, sollten Sie die Schlüssel rotieren, indem Sie sie in regelmäßigen Abständen in der Konsole aktualisieren. Dies ist ein vollständig manueller Prozess.

Kann ich das AWS Marketplace-Abonnement für Cloud Volumes ONTAP Systeme ändern?

Ja, das können Sie. Wenn Sie das AWS Marketplace-Abonnement ändern, das mit einem Satz Anmeldeinformationen verknüpft ist, werden alle vorhandenen und neuen Cloud Volumes ONTAP Systeme über das neue Abonnement abgerechnet.

"Erfahren Sie, wie Sie ein AWS-Abonnement zuordnen" .

Kann ich mehrere AWS-Anmeldeinformationen mit jeweils unterschiedlichen Marktplatz-Abonnements hinzufügen?

Alle AWS-Anmeldeinformationen, die zum selben AWS-Konto gehören, werden mit demselben AWS Marketplace-Abonnement verknüpft.

Wenn Sie über mehrere AWS-Anmeldeinformationen verfügen, die zu verschiedenen AWS-Konten gehören, können diese Anmeldeinformationen mit demselben AWS Marketplace-Abonnement oder mit verschiedenen Abonnements verknüpft sein.

Kann ich vorhandene Cloud Volumes ONTAP Systeme auf ein anderes AWS-Konto verschieben?

Nein, es ist nicht möglich, die mit Ihrem Cloud Volumes ONTAP -System verknüpften AWS-Ressourcen auf ein anderes AWS-Konto zu verschieben.

Wie funktionieren Anmeldeinformationen für Marktplatzbereitstellungen und lokale Bereitstellungen?

In den obigen Abschnitten wird die empfohlene Bereitstellungsmethode für den Konsolenagenten beschrieben, die von der Konsole aus erfolgt. Sie können auch einen Agenten in AWS über den AWS Marketplace bereitstellen und die Console-Agent-Software manuell auf Ihrem eigenen Linux-Host oder in Ihrem VCenter installieren.

Wenn Sie den Marketplace verwenden, werden die Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die IAM-Rolle manuell erstellen und einrichten und dann Berechtigungen für alle zusätzlichen Konten erteilen.

Bei lokalen Bereitstellungen können Sie keine IAM-Rolle für die Konsole einrichten, aber Sie können Berechtigungen mithilfe von AWS-Zugriffsschlüsseln erteilen.

Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

- Standardmodus
  - "Einrichten von Berechtigungen für eine AWS Marketplace-Bereitstellung"
  - "Einrichten von Berechtigungen für lokale Bereitstellungen"
- Eingeschränkter Modus
  - "Berechtigungen für den eingeschränkten Modus einrichten"

Verwalten Sie AWS-Anmeldeinformationen und Marktplatz-Abonnements für die NetApp Console

Fügen Sie AWS-Anmeldeinformationen hinzu und verwalten Sie diese, damit Sie Cloud-Ressourcen in Ihren AWS-Konten über die NetApp Console bereitstellen und verwalten können. Wenn Sie mehrere AWS Marketplace-Abonnements verwalten, können Sie jedem Abonnement auf der Seite „Anmeldeinformationen“ unterschiedliche AWS-Anmeldeinformationen zuweisen.

Überblick

Sie können AWS-Anmeldeinformationen zu einem vorhandenen Konsolenagenten oder direkt zur Konsole hinzufügen:

- Fügen Sie einem vorhandenen Agenten zusätzliche AWS-Anmeldeinformationen hinzu

Fügen Sie einem Konsolenagenten AWS-Anmeldeinformationen hinzu, um Cloud-Ressourcen zu verwalten. Erfahren Sie, wie Sie einem Konsolenagenten AWS-Anmeldeinformationen hinzufügen .

- Fügen Sie der Konsole AWS-Anmeldeinformationen hinzu, um einen Konsolenagenten zu erstellen

  Durch das Hinzufügen neuer AWS-Anmeldeinformationen zur Konsole erhalten Sie die erforderlichen Berechtigungen zum Erstellen eines Konsolenagenten. Erfahren Sie, wie Sie AWS-Anmeldeinformationen zur NetApp Console hinzufügen .

- AWS-Anmeldeinformationen zur Konsole für FSx for ONTAP hinzufügen

  Fügen Sie der Konsole neue AWS-Anmeldeinformationen hinzu, um FSx für ONTAP zu erstellen und zu verwalten. "Erfahren Sie, wie Sie Berechtigungen für FSx für ONTAP einrichten"

So rotieren Sie Anmeldeinformationen

Mit der NetApp Console können Sie AWS-Anmeldeinformationen auf verschiedene Weise bereitstellen: über eine mit der Agenteninstanz verknüpfte IAM-Rolle, durch die Übernahme einer IAM-Rolle in einem vertrauenswürdigen Konto oder durch die Bereitstellung von AWS-Zugriffsschlüsseln. "Erfahren Sie mehr über AWS-Anmeldeinformationen und -Berechtigungen" .

Bei den ersten beiden Optionen verwendet die Konsole den AWS Security Token Service, um temporäre Anmeldeinformationen zu erhalten, die ständig rotieren. Dieser Vorgang ist die beste Vorgehensweise, da er automatisch und sicher ist.

Rotieren Sie AWS-Zugriffsschlüssel manuell, indem Sie sie in der Konsole aktualisieren.

Hinzufügen zusätzlicher Anmeldeinformationen zu einem Konsolenagenten

Fügen Sie einem Konsolenagenten zusätzliche AWS-Anmeldeinformationen hinzu, damit er über die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen in Ihrer öffentlichen Cloud-Umgebung verfügt. Sie können entweder die ARN einer IAM-Rolle in einem anderen Konto angeben oder AWS-Zugriffsschlüssel bereitstellen.

"Erfahren Sie, wie die NetApp Console AWS-Anmeldeinformationen und -Berechtigungen verwendet".

Berechtigungen erteilen

Erteilen Sie Berechtigungen, bevor Sie einem Konsolenagenten AWS-Anmeldeinformationen hinzufügen. Die Berechtigungen ermöglichen einem Konsolenagenten, Ressourcen und Prozesse innerhalb dieses AWS-Kontos zu verwalten. Sie können die Berechtigungen mit der ARN einer Rolle in einem vertrauenswürdigen Konto oder mit AWS-Schlüsseln bereitstellen.

> Wenn Sie einen Konsolenagenten über die Konsole bereitgestellt haben, wurden automatisch AWS-Anmeldeinformationen für das Konto hinzugefügt, in dem Sie einen Konsolenagenten bereitgestellt haben. Dadurch wird sichergestellt, dass die erforderlichen Berechtigungen zum Verwalten von Ressourcen vorhanden sind.

Auswahl

- indem Sie eine IAM-Rolle in einem anderen Konto übernehmen
- Erteilen Sie Berechtigungen durch die Bereitstellung von AWS-Schlüsseln

Erteilen Sie Berechtigungen, indem Sie eine IAM-Rolle in einem anderen Konto übernehmen

Sie können mithilfe von IAM-Rollen eine Vertrauensbeziehung zwischen dem AWS-Quellkonto, in dem Sie einen Konsolenagenten bereitgestellt haben, und anderen AWS-Konten einrichten. Anschließend stellen Sie der Konsole die ARN der IAM-Rollen der vertrauenswürdigen Konten zur Verfügung.

Wenn ein Konsolenagent vor Ort installiert ist, können Sie diese Authentifizierungsmethode nicht verwenden. Sie müssen AWS-Schlüssel verwenden.

Schritte

1. Gehen Sie zur IAM-Konsole im Zielkonto, in dem Sie einem Konsolenagenten Berechtigungen erteilen möchten.
2. Wählen Sie unter „Zugriffsverwaltung“ **Rollen > Rolle erstellen** und befolgen Sie die Schritte zum Erstellen der Rolle.

   Stellen Sie sicher, dass Sie Folgendes tun:

   - Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
   - Wählen Sie **Ein anderes AWS-Konto** und geben Sie die ID des Kontos ein, in dem sich eine Konsolen-Agent-Instanz befindet.
   - Erstellen Sie die erforderlichen Richtlinien, indem Sie den Inhalt von kopieren und einfügen"die IAM-Richtlinien für einen Konsolenagenten" .
3. Kopieren Sie die Rollen-ARN der IAM-Rolle, damit Sie sie später in die Konsole einfügen können.

Ergebnis

Das Konto verfügt über die erforderlichen Berechtigungen. Sie können jetzt die Anmeldeinformationen zu einem Konsolenagenten hinzufügen .

Erteilen Sie Berechtigungen durch die Bereitstellung von AWS-Schlüsseln

Wenn Sie der Konsole AWS-Schlüssel für einen IAM-Benutzer bereitstellen möchten, müssen Sie diesem Benutzer die erforderlichen Berechtigungen erteilen. Die IAM-Richtlinie der Konsole definiert die AWS-Aktionen und -Ressourcen, die die Konsole verwenden darf.

Sie müssen diese Authentifizierungsmethode verwenden, wenn ein Konsolenagent vor Ort installiert ist. Sie können keine IAM-Rolle verwenden.

Schritte

1. Erstellen Sie in der IAM-Konsole Richtlinien, indem Sie den Inhalt von"die IAM-Richtlinien für einen Konsolenagenten" .

   "AWS-Dokumentation: Erstellen von IAM-Richtlinien"
2. Ordnen Sie die Richtlinien einer IAM-Rolle oder einem IAM-Benutzer zu.
   - "AWS-Dokumentation: Erstellen von IAM-Rollen"
   - "AWS-Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"

Fügen Sie die Anmeldeinformationen zu einem vorhandenen Agenten hinzu

Nachdem Sie ein AWS-Konto mit den erforderlichen Berechtigungen versehen haben, können Sie die Anmeldeinformationen für dieses Konto einem vorhandenen Agenten hinzufügen. Dadurch können Sie Cloud Volumes ONTAP -Systeme in diesem Konto mit demselben Agenten starten.

Es kann einige Minuten dauern, bis neue Anmeldeinformationen bei Ihrem Cloud-Anbieter verfügbar sind.

Schritte

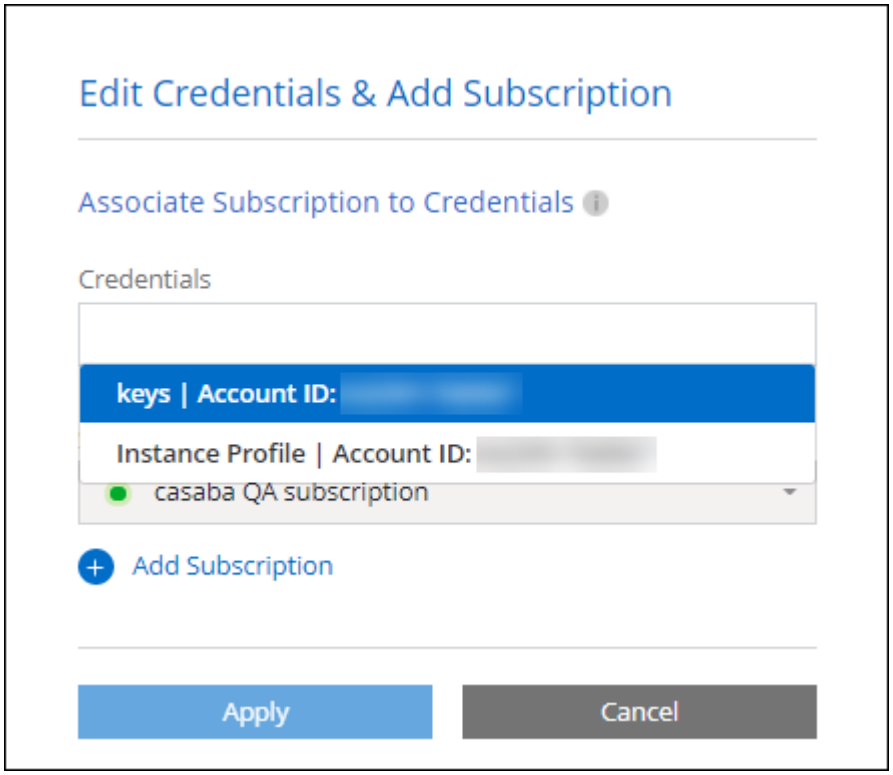
1. Wählen Sie über die obere Navigationsleiste einen Konsolenagenten aus, dem Sie Anmeldeinformationen hinzufügen möchten.
2. Wählen Sie in der linken Navigationsleiste **Administration > Anmeldeinformationen** aus.
3. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** die Option **Anmeldeinformationen hinzufügen** aus und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Amazon Web Services > Agent**.
   b. **Anmeldeinformationen definieren**: Geben Sie den ARN (Amazon Resource Name) einer vertrauenswürdigen IAM-Rolle an oder geben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel ein.
   c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.

      Um Dienste mit einem Stundensatz (PAYGO) oder mit einem Jahresvertrag zu bezahlen, müssen Sie AWS-Anmeldeinformationen mit Ihrem AWS Marketplace-Abonnement verknüpfen.

   d. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Ergebnis

Sie können jetzt auf der Seite „Details und Anmeldeinformationen“ zu einem anderen Satz von Anmeldeinformationen wechseln, wenn Sie der Konsole ein Abonnement hinzufügen.



Fügen Sie der Konsole Anmeldeinformationen zum Erstellen eines Konsolenagenten hinzu

Fügen Sie AWS-Anmeldeinformationen hinzu, indem Sie die ARN einer IAM-Rolle angeben, die die zum Erstellen eines Konsolenagenten erforderlichen Berechtigungen erteilt. Sie können diese Anmeldeinformationen beim Erstellen eines neuen Agenten auswählen.

Einrichten der IAM-Rolle

Richten Sie eine IAM-Rolle ein, die es der NetApp Console -Software als Serviceebene (SaaS) ermöglicht, die Rolle zu übernehmen.

Schritte

1. Gehen Sie zur IAM-Konsole im Zielkonto.
2. Wählen Sie unter „Zugriffsverwaltung“ **Rollen > Rolle erstellen** und befolgen Sie die Schritte zum Erstellen der Rolle.

   Stellen Sie sicher, dass Sie Folgendes tun:

   - Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
   - Wählen Sie **Ein anderes AWS-Konto** und geben Sie die ID der NetApp Console SaaS ein: 952013314444
   - Bearbeiten Sie speziell für Amazon FSx for NetApp ONTAP die Richtlinie **Vertrauensbeziehungen**, um "AWS": "arn:aws:iam::952013314444:root" einzuschließen.

     Die Richtlinie sollte beispielsweise folgendermaßen aussehen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+
Siehe "AWS Identity and Access Management (IAM)-Dokumentation" für weitere Informationen zum kontoübergreifenden Ressourcenzugriff in IAM.

   - Erstellen Sie eine Richtlinie, die die zum Erstellen eines Konsolenagenten erforderlichen Berechtigungen enthält.
     - "Anzeigen der für FSx for ONTAP erforderlichen Berechtigungen"
     - "Anzeigen der Agent-Bereitstellungsrichtlinie"

3. Kopieren Sie die Rollen-ARN der IAM-Rolle, damit Sie sie im nächsten Schritt in die Konsole einfügen können.

Ergebnis

Die IAM-Rolle verfügt jetzt über die erforderlichen Berechtigungen. Sie können es jetzt zur Konsole hinzufügen.

Fügen Sie die Anmeldeinformationen hinzu

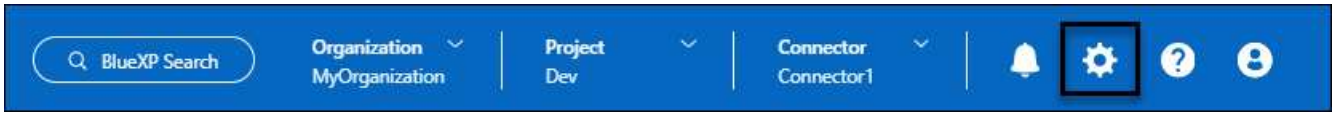
Nachdem Sie die IAM-Rolle mit den erforderlichen Berechtigungen ausgestattet haben, fügen Sie die Rollen-ARN zur Konsole hinzu.

Bevor Sie beginnen

Wenn Sie die IAM-Rolle gerade erst erstellt haben, kann es einige Minuten dauern, bis sie zur Verwendung verfügbar ist. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zur Konsole hinzufügen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.



2. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** die Option **Anmeldeinformationen hinzufügen** aus und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Amazon Web Services > Konsole**.
   b. **Anmeldeinformationen definieren**: Geben Sie den ARN (Amazon Resource Name) der IAM-Rolle an.
   c. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Anmeldeinformationen zur Konsole für Amazon FSx for ONTAP hinzufügen

Einzelheiten finden Sie im "die Konsolendokumentation für Amazon FSx for ONTAP"

Konfigurieren eines AWS-Abonnements

Nachdem Sie Ihre AWS-Anmeldeinformationen hinzugefügt haben, können Sie mit diesen Anmeldeinformationen ein AWS Marketplace-Abonnement konfigurieren. Mit dem Abonnement können Sie NetApp Datendienste und Cloud Volumes ONTAP auf Stundenbasis (PAYGO) oder über einen Jahresvertrag bezahlen.

Es gibt zwei Szenarien, in denen Sie ein AWS Marketplace-Abonnement konfigurieren können, nachdem Sie die Anmeldeinformationen bereits hinzugefügt haben:

- Sie haben beim ersten Hinzufügen der Anmeldeinformationen kein Abonnement konfiguriert.
- Sie möchten das AWS Marketplace-Abonnement ändern, das für die AWS-Anmeldeinformationen konfiguriert ist.

  Durch das Ersetzen des aktuellen Marktplatzabonnements durch ein neues Abonnement wird das Marktplatzabonnement für alle vorhandenen Cloud Volumes ONTAP Systeme und alle neuen Systeme geändert.

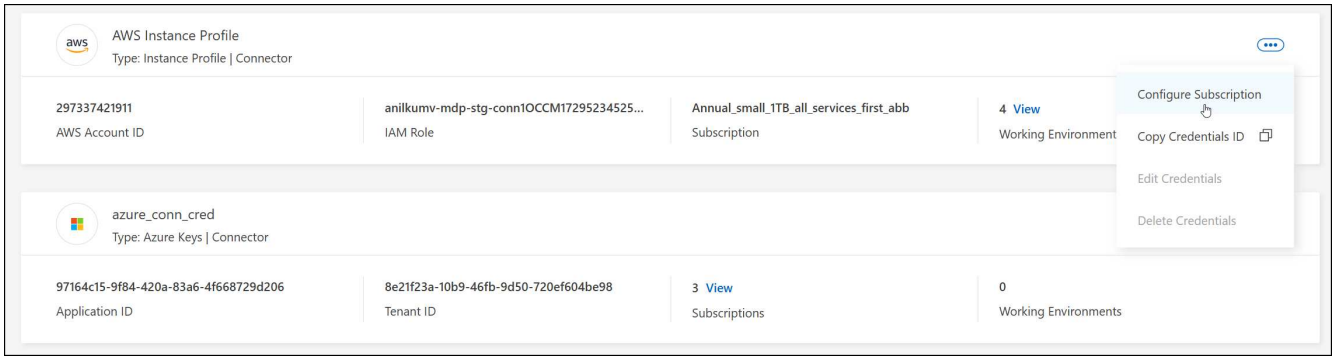
Bevor Sie beginnen

Sie müssen einen Konsolenagenten erstellen, bevor Sie ein Abonnement konfigurieren können. "Erfahren Sie, wie Sie einen Konsolenagenten erstellen" .

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen aus, die einem Konsolenagenten zugeordnet sind, und wählen Sie dann **Abonnement konfigurieren**.

   Sie müssen Anmeldeinformationen auswählen, die einem Konsolenagenten zugeordnet sind. Sie können ein Marktplatzabonnement nicht mit Anmeldeinformationen verknüpfen, die mit der NetApp Console verknüpft sind.



4. Um die Anmeldeinformationen mit einem vorhandenen Abonnement zu verknüpfen, wählen Sie das Abonnement aus der Dropdown-Liste aus und wählen Sie **Konfigurieren**.
5. Um die Anmeldeinformationen einem neuen Abonnement zuzuordnen, wählen Sie **Abonnement hinzufügen > Fortfahren** und folgen Sie den Schritten im AWS Marketplace:

   a. Wählen Sie **Kaufoptionen anzeigen**.

   b. Wählen Sie **Abonnieren**.

   c. Wählen Sie **Konto einrichten**.

      Sie werden zur NetApp Console weitergeleitet.

   d. Auf der Seite **Abonnementzuweisung**:

      - Wählen Sie die Konsolenorganisationen oder -konten aus, mit denen Sie dieses Abonnement verknüpfen möchten.
      - Wählen Sie im Feld **Vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

        Die Konsole ersetzt das vorhandene Abonnement für alle Anmeldeinformationen in der Organisation oder im Konto durch dieses neue Abonnement. Wenn ein Satz von Anmeldeinformationen nie mit einem Abonnement verknüpft war, wird dieses neue Abonnement nicht mit diesen Anmeldeinformationen verknüpft.

   Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.

- Wählen Sie **Speichern**.

Verknüpfen Sie ein vorhandenes Abonnement mit Ihrer Organisation

Wenn Sie sich beim AWS Marketplace anmelden, besteht der letzte Schritt im Prozess darin, das Abonnement Ihrer Organisation zuzuordnen. Wenn Sie diesen Schritt nicht abgeschlossen haben, können Sie das Abonnement nicht mit Ihrer Organisation verwenden.

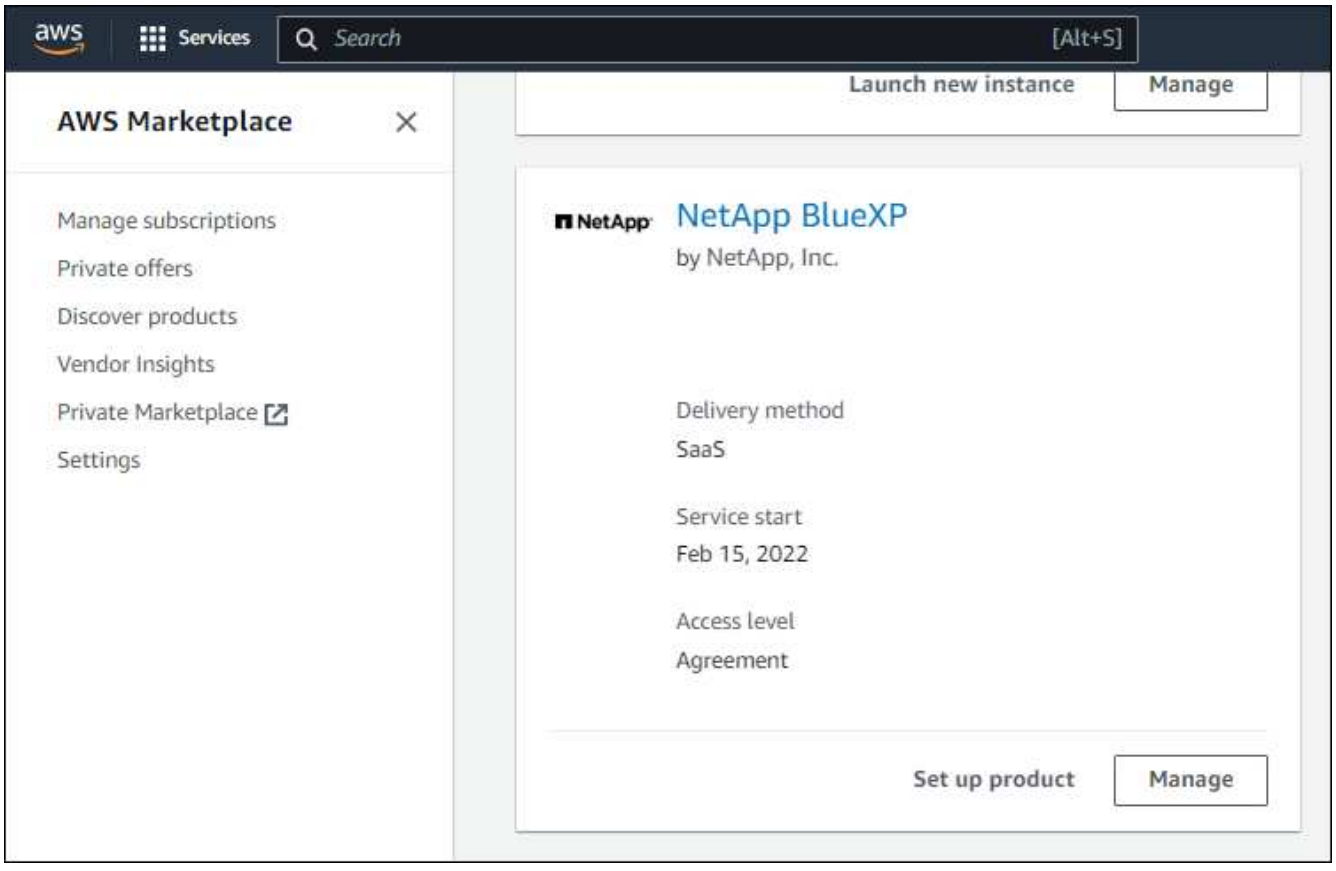
- "Erfahren Sie mehr über die Bereitstellungsmodi der Konsole"
- "Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der Konsole"

Führen Sie die folgenden Schritte aus, wenn Sie NetApp Intelligent Services vom AWS Marketplace abonniert haben, aber den Schritt zum Verknüpfen des Abonnements mit Ihrem Konto verpasst haben.

Schritte

1. Bestätigen Sie, dass Sie Ihr Abonnement nicht mit Ihrer Konsolenorganisation verknüpft haben.
   a. Wählen Sie im Navigationsmenü **Verwaltung > Licenses and subscriptions**.
   b. Wählen Sie **Abonnements** aus.
   c. Stellen Sie sicher, dass Ihr Abonnement nicht angezeigt wird.

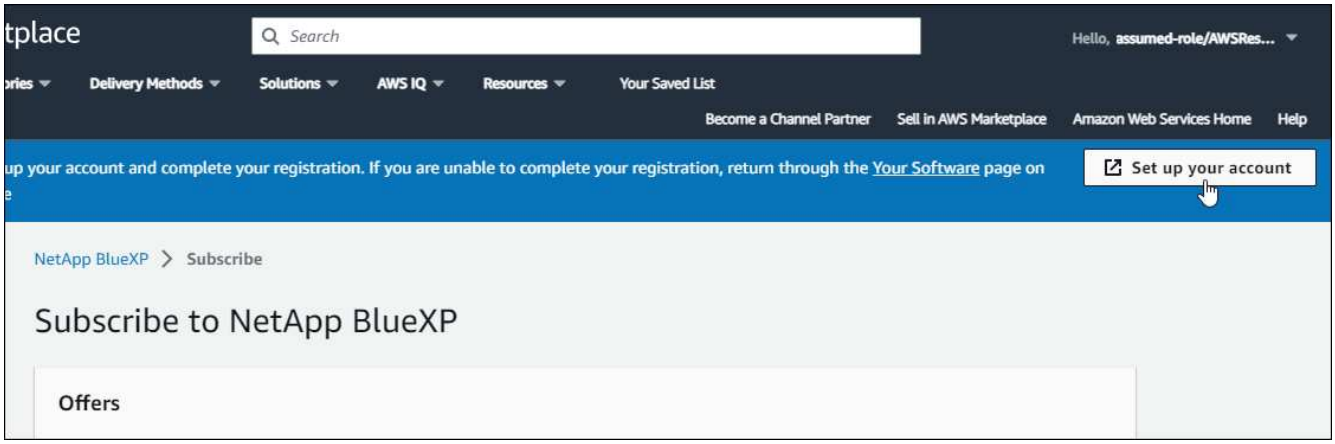
      Sie sehen nur die Abonnements, die mit der Organisation oder dem Konto verknüpft sind, das Sie gerade anzeigen. Wenn Ihr Abonnement nicht angezeigt wird, fahren Sie mit den folgenden Schritten fort.
2. Melden Sie sich bei der AWS-Konsole an und navigieren Sie zu **AWS Marketplace-Abonnements**.
3. Suchen Sie das Abonnement.



4. Wählen Sie **Produkt einrichten**.

   Die Abonnementangebotsseite sollte in einem neuen Browser-Tab oder -Fenster geladen werden.

5. Wählen Sie **Konto einrichten**.



   Die Seite **Abonnementzuweisung** auf netapp.com sollte in einem neuen Browser-Tab oder -Fenster geladen werden.

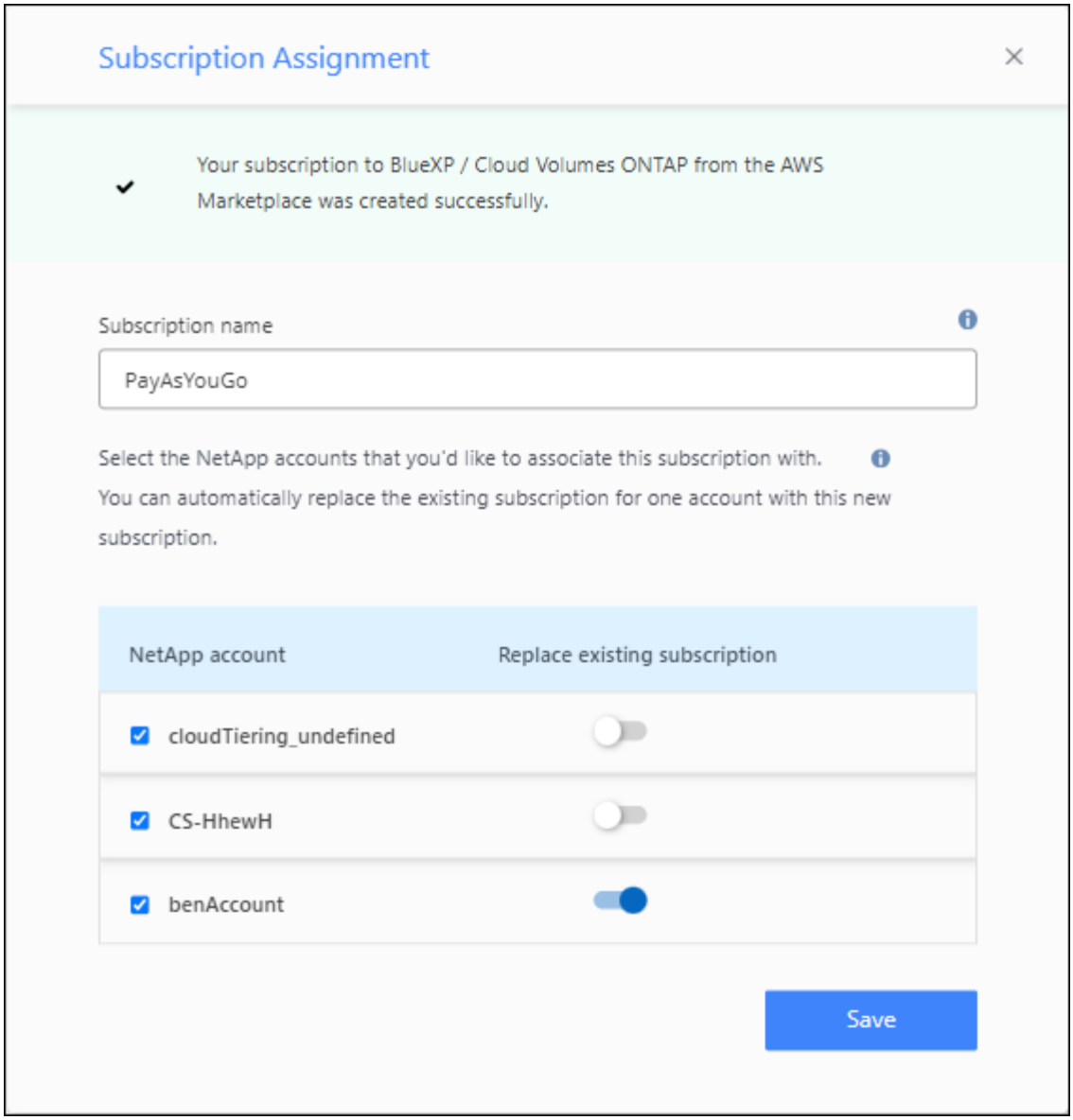
   Beachten Sie, dass Sie möglicherweise zuerst aufgefordert werden, sich bei der Konsole anzumelden.

6. Auf der Seite **Abonnementzuweisung**:

   - Wählen Sie die Konsolenorganisationen oder -konten aus, mit denen Sie dieses Abonnement verknüpfen möchten.
   - Wählen Sie im Feld **Vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

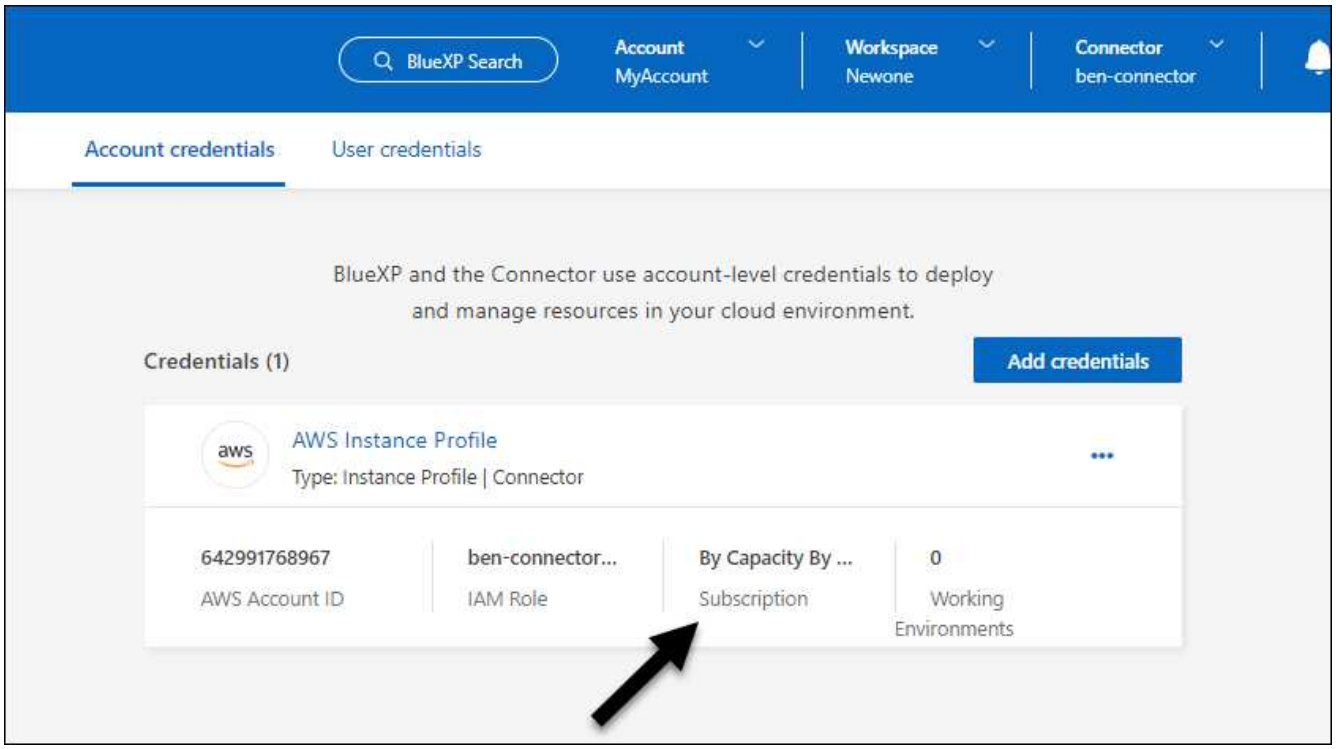
     Die Konsole ersetzt das vorhandene Abonnement für alle Anmeldeinformationen in der Organisation oder im Konto durch dieses neue Abonnement. Wenn ein Satz von Anmeldeinformationen nie mit einem Abonnement verknüpft war, wird dieses neue Abonnement nicht mit diesen Anmeldeinformationen verknüpft.

     Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.



7. Bestätigen Sie, dass das Abonnement mit Ihrer Organisation verknüpft ist.
   a. Wählen Sie im Navigationsmenü **Administration > Lizenzen und Abonnements**.
   b. Wählen Sie **Abonnements** aus.
   c. Überprüfen Sie, ob Ihr Abonnement angezeigt wird.
8. Bestätigen Sie, dass das Abonnement mit Ihren AWS-Anmeldeinformationen verknüpft ist.
   a. Wählen Sie **Administration > Anmeldeinformationen**.
   b. Überprüfen Sie auf der Seite **Anmeldeinformationen der Organisation**, ob das Abonnement mit Ihren AWS-Anmeldeinformationen verknüpft ist.

      Hier ist ein Beispiel.



Anmeldeinformationen bearbeiten

Bearbeiten Sie Ihre AWS-Anmeldeinformationen, indem Sie den Kontotyp ändern (AWS-Schlüssel oder Rolle übernehmen), den Namen bearbeiten oder die Anmeldeinformationen selbst aktualisieren (die Schlüssel oder die Rollen-ARN).

Sie können die Anmeldeinformationen für ein Instanzprofil, das mit einer Konsolen-Agent-Instanz oder einer Amazon FSx for ONTAP -Instanz verknüpft ist, nicht bearbeiten. Sie können die Anmeldeinformationen nur für eine FSx for ONTAP Instanz umbenennen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Anmeldeinformationen bearbeiten**.
3. Nehmen Sie die erforderlichen Änderungen vor und wählen Sie dann **Übernehmen**.

Anmeldeinformationen löschen

Wenn Sie einen Satz Anmeldeinformationen nicht mehr benötigen, können Sie ihn löschen. Sie können nur Anmeldeinformationen löschen, die keinem System zugeordnet sind.

Sie können die Anmeldeinformationen für ein Instanzprofil, das einem Konsolenagenten zugeordnet ist, nicht löschen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** oder **Anmeldeinformationen des Kontos** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann

Anmeldeinformationen löschen.

3. Wählen Sie zur Bestätigung **Löschen**.

Azurblau

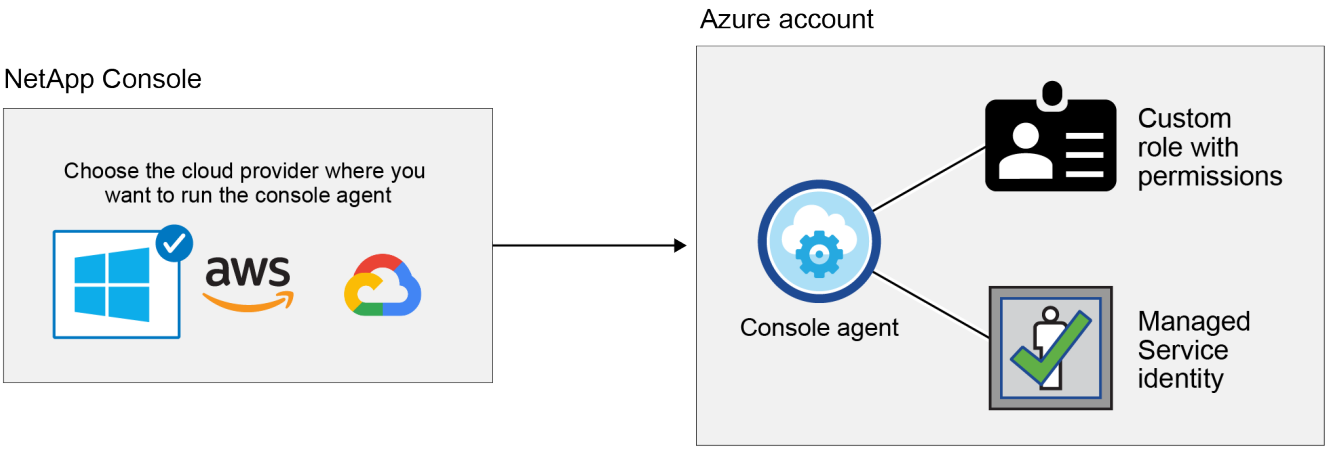
Erfahren Sie mehr über Azure-Anmeldeinformationen und Berechtigungen in der NetApp Console

Erfahren Sie, wie die NetApp Console Azure-Anmeldeinformationen verwendet, um Aktionen in Ihrem Namen auszuführen, und wie diese Anmeldeinformationen mit Marktplatzabonnements verknüpft werden. Das Verständnis dieser Details kann hilfreich sein, wenn Sie die Anmeldeinformationen für ein oder mehrere Azure-Abonnements verwalten. Sie möchten beispielsweise wissen, wann Sie der Konsole zusätzliche Azure-Anmeldeinformationen hinzufügen müssen.

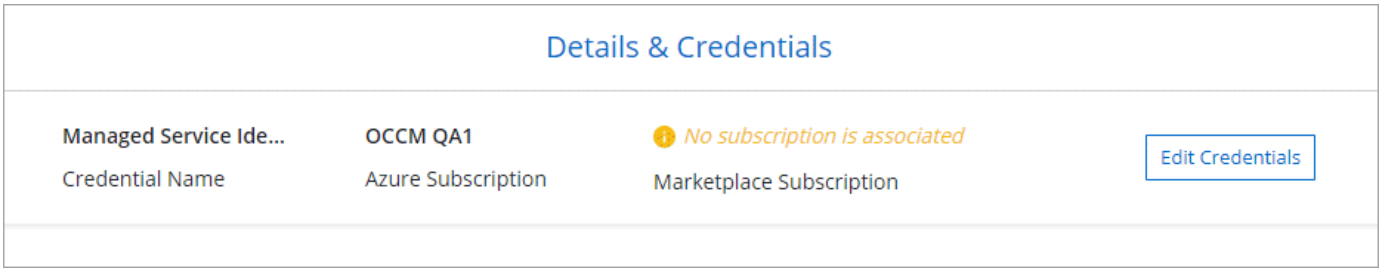
Anfängliche Azure-Anmeldeinformationen

Wenn Sie einen Konsolen-Agenten über die Konsole bereitstellen, müssen Sie ein Azure-Konto oder einen Dienstprinzipal verwenden, der über die Berechtigung zum Bereitstellen der virtuellen Maschine des Konsolen-Agenten verfügt. Die erforderlichen Berechtigungen sind in der"Agent-Bereitstellungsrichtlinie für Azure" .

Wenn die Konsole die virtuelle Maschine des Konsolen-Agenten in Azure bereitstellt, ermöglicht sie eine "systemseitig zugewiesene verwaltete Identität" auf der virtuellen Maschine, erstellt eine benutzerdefinierte Rolle und weist sie der virtuellen Maschine zu. Die Rolle stellt der Konsole die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen innerhalb dieses Azure-Abonnements zur Verfügung. "Überprüfen Sie, wie die Konsole die Berechtigungen verwendet" .



Wenn Sie ein neues System für Cloud Volumes ONTAP erstellen, wählt die Konsole standardmäßig diese Azure-Anmeldeinformationen aus:



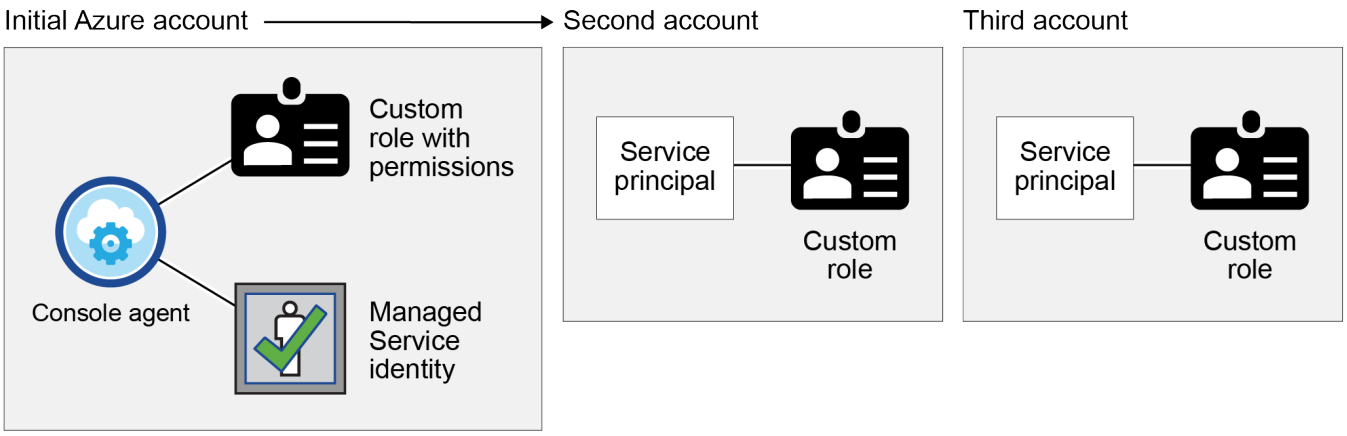
Sie können alle Ihre Cloud Volumes ONTAP -Systeme mit den anfänglichen Azure-Anmeldeinformationen bereitstellen oder zusätzliche Anmeldeinformationen hinzufügen.

Zusätzliche Azure-Abonnements für eine verwaltete Identität

Die der Konsolen-Agent-VM zugewiesene, systemseitig verwaltete Identität ist dem Abonnement zugeordnet, in dem Sie den Konsolen-Agent gestartet haben. Wenn Sie ein anderes Azure-Abonnement auswählen möchten, müssen Sie"Verknüpfen Sie die verwaltete Identität mit diesen Abonnements" .

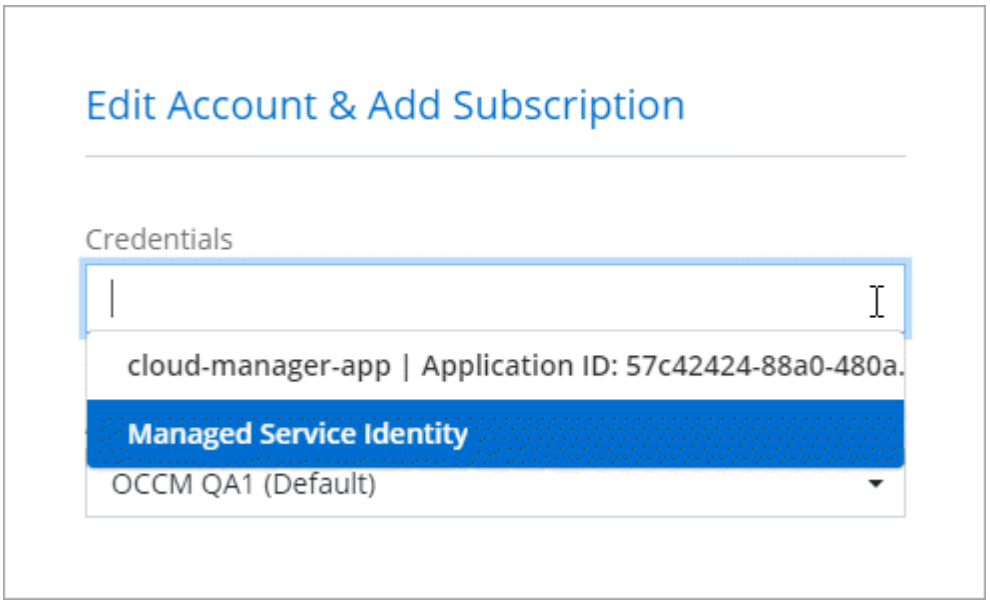
Zusätzliche Azure-Anmeldeinformationen

Wenn Sie andere Azure-Anmeldeinformationen mit der Konsole verwenden möchten, müssen Sie die erforderlichen Berechtigungen erteilen, indem Sie"Erstellen und Einrichten eines Dienstprinzipals in Microsoft Entra ID" für jedes Azure-Konto. Das folgende Bild zeigt zwei weitere Konten, die jeweils mit einem Dienstprinzipal und einer benutzerdefinierten Rolle eingerichtet sind, die Berechtigungen bereitstellt:



Sie würden dann"Fügen Sie die Kontoanmeldeinformationen zur Konsole hinzu" indem Sie Details zum AD-Dienstprinzipal angeben.

Sie können beispielsweise beim Erstellen eines neuen Cloud Volumes ONTAP Systems zwischen Anmeldeinformationen wechseln:



Anmeldeinformationen und Marktplatzabonnements

Die Anmeldeinformationen, die Sie einem Konsolenagenten hinzufügen, müssen mit einem Azure Marketplace-Abonnement verknüpft sein, damit Sie für Cloud Volumes ONTAP einen Stundensatz (PAYGO), NetApp -Datendienste oder einen Jahresvertrag bezahlen können.

"Erfahren Sie, wie Sie ein Azure-Abonnement zuordnen" .

Beachten Sie Folgendes zu Azure-Anmeldeinformationen und Marketplace-Abonnements:

- Sie können einem Satz Azure-Anmeldeinformationen nur ein Azure Marketplace-Abonnement zuordnen.
- Sie können ein bestehendes Marktplatz-Abonnement durch ein neues Abonnement ersetzen

FAQ

Die folgende Frage bezieht sich auf Anmeldeinformationen und Abonnements.

Kann ich das Azure Marketplace-Abonnement für Cloud Volumes ONTAP Systeme ändern?

Ja, das können Sie. Wenn Sie das Azure Marketplace-Abonnement ändern, das mit einem Satz Azure-Anmeldeinformationen verknüpft ist, werden alle vorhandenen und neuen Cloud Volumes ONTAP Systeme über das neue Abonnement abgerechnet.

"Erfahren Sie, wie Sie ein Azure-Abonnement zuordnen" .

Kann ich mehrere Azure-Anmeldeinformationen mit jeweils unterschiedlichen Marktplatzabonnements hinzufügen?

Alle Azure-Anmeldeinformationen, die zum selben Azure-Abonnement gehören, werden mit demselben Azure Marketplace-Abonnement verknüpft.

Wenn Sie über mehrere Azure-Anmeldeinformationen verfügen, die zu verschiedenen Azure-Abonnements gehören, können diese Anmeldeinformationen demselben Azure Marketplace-Abonnement oder verschiedenen Marketplace-Abonnements zugeordnet werden.

Kann ich vorhandene Cloud Volumes ONTAP Systeme in ein anderes Azure-Abonnement verschieben?

Nein, es ist nicht möglich, die mit Ihrem Cloud Volumes ONTAP -System verknüpften Azure-Ressourcen in ein anderes Azure-Abonnement zu verschieben.

Wie funktionieren Anmeldeinformationen für Marktplatzbereitstellungen und lokale Bereitstellungen?

In den obigen Abschnitten wird die empfohlene Bereitstellungsmethode für den Konsolenagenten beschrieben, die von der Konsole aus erfolgt. Sie können auch einen Konsolen-Agenten in Azure vom Azure Marketplace bereitstellen und die Konsolen-Agenten-Software auf Ihrem eigenen Linux-Host installieren.

Wenn Sie den Marketplace verwenden, können Sie Berechtigungen erteilen, indem Sie der Konsolen-Agent-VM und einer systemseitig zugewiesenen verwalteten Identität eine benutzerdefinierte Rolle zuweisen, oder Sie können einen Microsoft Entra-Dienstprinzipal verwenden.

Bei lokalen Bereitstellungen können Sie keine verwaltete Identität für den Konsolen-Agent einrichten, Sie können jedoch mithilfe eines Dienstprinzipals Berechtigungen erteilen.

Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

- Standardmodus
  - "Einrichten von Berechtigungen für eine Azure Marketplace-Bereitstellung"
  - "Einrichten von Berechtigungen für lokale Bereitstellungen"
- Eingeschränkter Modus
  - "Berechtigungen für den eingeschränkten Modus einrichten"

Verwalten Sie Azure-Anmeldeinformationen und Marketplace-Abonnements für die NetApp Console

Fügen Sie Azure-Anmeldeinformationen hinzu und verwalten Sie diese, damit die NetApp Console über die erforderlichen Berechtigungen zum Bereitstellen und Verwalten von Cloud-Ressourcen in Ihren Azure-Abonnements verfügt. Wenn Sie mehrere Azure Marketplace-Abonnements verwalten, können Sie jedem Abonnement auf der Seite „Anmeldeinformationen“ unterschiedliche Azure-Anmeldeinformationen zuweisen.

Überblick

Es gibt zwei Möglichkeiten, zusätzliche Azure-Abonnements und Anmeldeinformationen in der Konsole hinzuzufügen.

1. Ordnen Sie der von Azure verwalteten Identität zusätzliche Azure-Abonnements zu.
2. Um Cloud Volumes ONTAP mit unterschiedlichen Azure-Anmeldeinformationen bereitzustellen, erteilen Sie Azure Berechtigungen mithilfe eines Dienstprinzipals und fügen Sie dessen Anmeldeinformationen der Konsole hinzu.

Zuordnen zusätzlicher Azure-Abonnements zu einer verwalteten Identität

Über die Konsole können Sie die Azure-Anmeldeinformationen und das Azure-Abonnement auswählen, in dem Sie Cloud Volumes ONTAP bereitstellen möchten. Sie können kein anderes Azure-Abonnement für das verwaltete Identitätsprofil auswählen, es sei denn, Sie verknüpfen das "Verwaltete Identität" mit diesen Abonnements.

Informationen zu diesem Vorgang

Eine verwaltete Identität ist"das anfängliche Azure-Konto" wenn Sie einen Konsolenagenten von der Konsole aus bereitstellen. Wenn Sie den Konsolenagenten bereitstellen, weist die Konsole der virtuellen Maschine des Konsolenagenten die Rolle des Konsolenoperators zu.

Schritte

1. Melden Sie sich beim Azure-Portal an.
2. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP bereitstellen möchten.
3. Wählen Sie **Zugriffskontrolle (IAM)**.
   a. Wählen Sie **Hinzufügen** > **Rollenzuweisung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
      - Wählen Sie die Rolle **Konsolenoperator** aus.

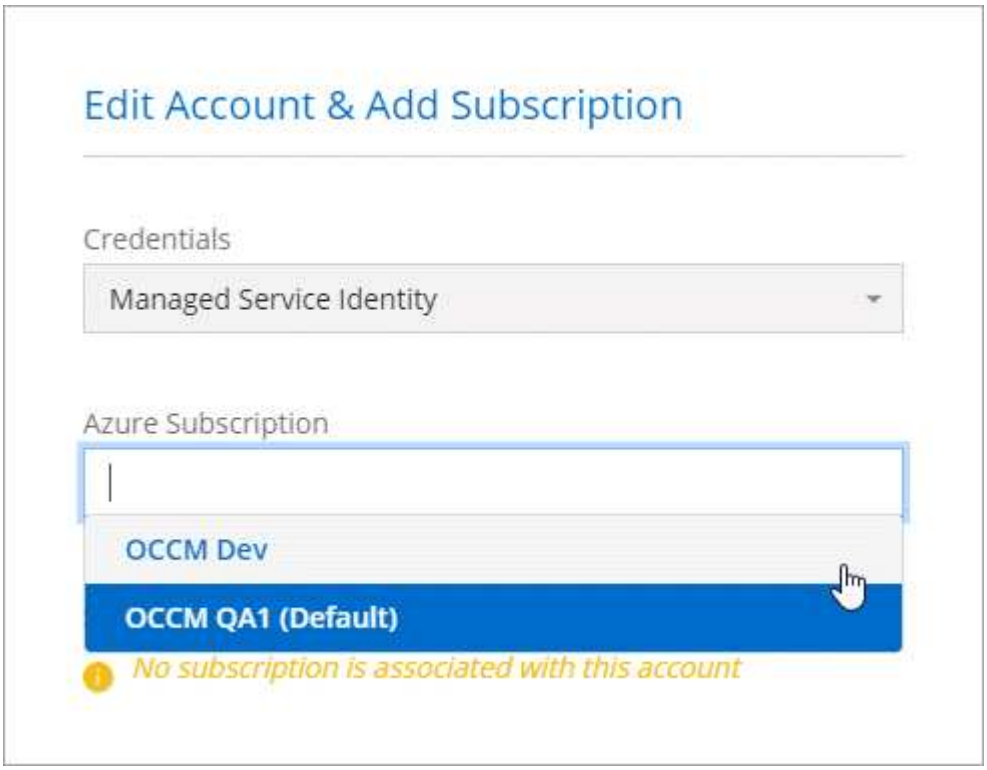
        „Konsolenoperator“ ist der Standardname, der in einer Konsolenagentrichtlinie angegeben wird. Wenn Sie einen anderen Namen für die Rolle gewählt haben, wählen Sie stattdessen diesen Namen aus.

- Weisen Sie einer **virtuellen Maschine** Zugriff zu.
- Wählen Sie das Abonnement aus, in dem eine virtuelle Maschine des Konsolen-Agenten erstellt wurde.
- Wählen Sie eine virtuelle Maschine des Konsolenagenten aus.
- Wählen Sie **Speichern**.

4. Wiederholen Sie diese Schritte für weitere Abonnements.

Ergebnis

Beim Erstellen eines neuen Systems können Sie jetzt aus mehreren Azure-Abonnements für das verwaltete Identitätsprofil auswählen.



Fügen Sie der NetApp Console zusätzliche Azure-Anmeldeinformationen hinzu

Wenn Sie einen Konsolenagenten über die Konsole bereitstellen, aktiviert die Konsole eine vom System zugewiesene verwaltete Identität auf der virtuellen Maschine, die über die erforderlichen Berechtigungen verfügt. Die Konsole wählt diese Azure-Anmeldeinformationen standardmäßig aus, wenn Sie ein neues System für Cloud Volumes ONTAP erstellen.

Wenn Sie eine Konsolenagentensoftware manuell auf einem vorhandenen System installiert haben, wird kein anfänglicher Satz Anmeldeinformationen hinzugefügt. "Erfahren Sie mehr über Azure-Anmeldeinformationen und -Berechtigungen" .

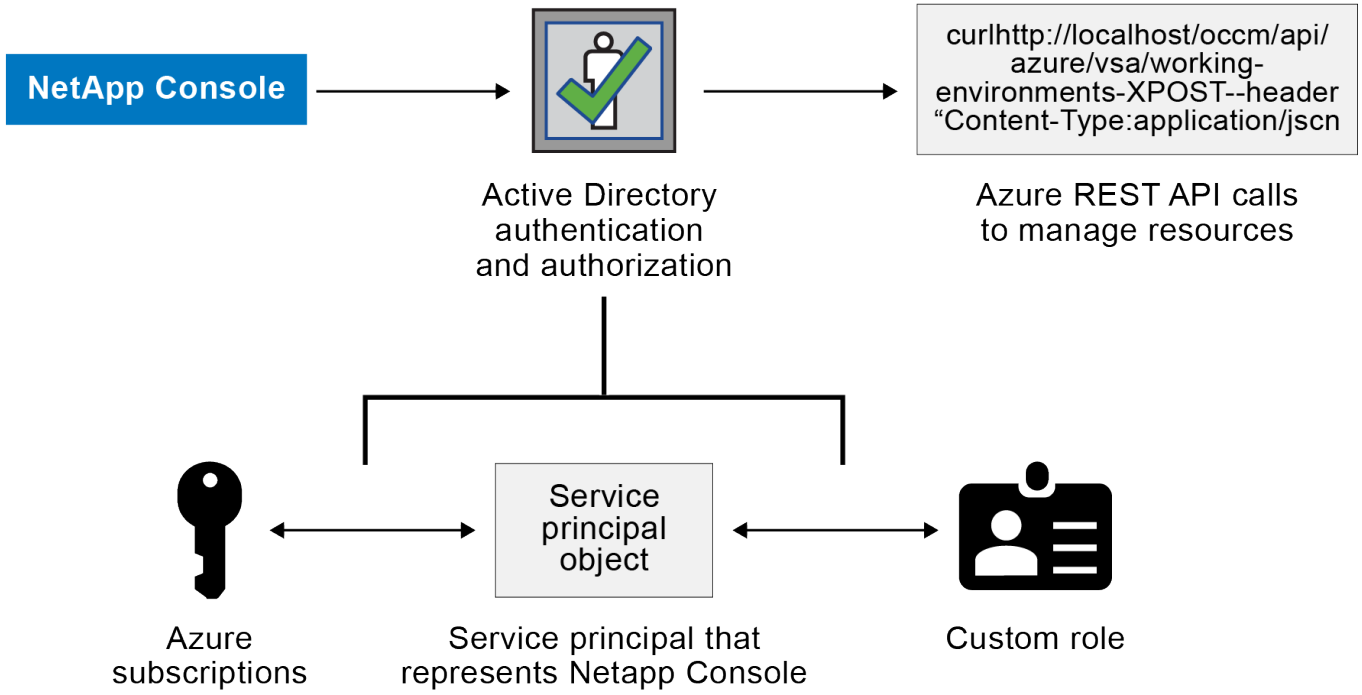
Wenn Sie Cloud Volumes ONTAP mit *verschiedenen* Azure-Anmeldeinformationen bereitstellen möchten, müssen Sie die erforderlichen Berechtigungen erteilen, indem Sie für jedes Azure-Konto einen Dienstprinzipal in der Microsoft Entra-ID erstellen und einrichten. Anschließend können Sie die neuen Anmeldeinformationen zur Konsole hinzufügen.

Gewähren von Azure-Berechtigungen mithilfe eines Dienstprinzipals

Die Konsole benötigt Berechtigungen, um Aktionen in Azure auszuführen. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie einen Dienstprinzipal in Microsoft Entra ID erstellen und einrichten und die Azure-Anmeldeinformationen abrufen, die die Konsole benötigt.

Informationen zu diesem Vorgang

Das folgende Bild zeigt, wie die Konsole Berechtigungen zum Ausführen von Vorgängen in Azure erhält. Ein Dienstprinzipalobjekt, das an ein oder mehrere Azure-Abonnements gebunden ist, stellt die Konsole in der Microsoft Entra ID dar und ist einer benutzerdefinierten Rolle zugewiesen, die die erforderlichen Berechtigungen gewährt.



Schritte

1. Erstellen einer Microsoft Entra-Anwendung .
2. Zuweisen der Anwendung zu einer Rolle .
3. Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu .
4. Abrufen der Anwendungs-ID und der Verzeichnis-ID .
5. Erstellen eines Client-Geheimnisses .

Erstellen einer Microsoft Entra-Anwendung

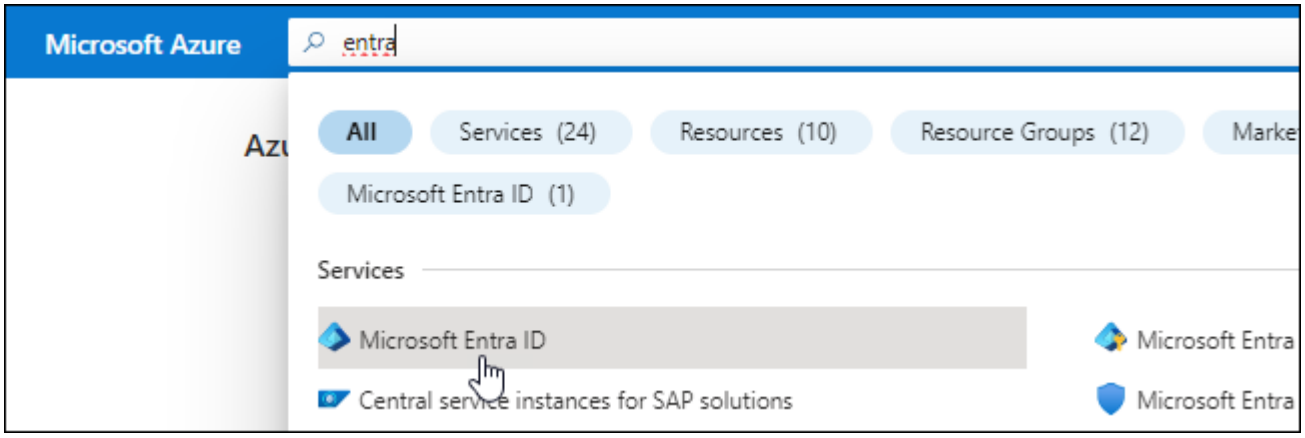
Erstellen Sie eine Microsoft Entra-Anwendung und einen Dienstprinzipal, den die Konsole für die rollenbasierte Zugriffskontrolle verwenden kann.

Schritte

1. Stellen Sie sicher, dass Sie in Azure über die Berechtigung verfügen, eine Active Directory-Anwendung zu erstellen und die Anwendung einer Rolle zuzuweisen.

   Weitere Einzelheiten finden Sie unter "Microsoft Azure-Dokumentation: Erforderliche Berechtigungen"

2. Öffnen Sie im Azure-Portal den Dienst **Microsoft Entra ID**.



3. Wählen Sie im Menü **App-Registrierungen** aus.
4. Wählen Sie **Neuregistrierung**.
5. Geben Sie Details zur Anwendung an:
   - **Name**: Geben Sie einen Namen für die Anwendung ein.
   - **Kontotyp**: Wählen Sie einen Kontotyp aus (alle funktionieren mit der NetApp Console).
   - **Umleitungs-URI**: Sie können dieses Feld leer lassen.
6. Wählen Sie **Registrieren**.

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der Anwendung zu einer Rolle

Sie müssen den Dienstprinzipal an ein oder mehrere Azure-Abonnements binden und ihm die benutzerdefinierte Rolle „Konsolenoperator“ zuweisen, damit die Konsole über Berechtigungen in Azure verfügt.

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle:

   Beachten Sie, dass Sie eine benutzerdefinierte Azure-Rolle mithilfe des Azure-Portals, Azure PowerShell, Azure CLI oder REST-API erstellen können. Die folgenden Schritte zeigen, wie Sie die Rolle mithilfe der Azure CLI erstellen. Wenn Sie eine andere Methode bevorzugen, lesen Sie bitte "Azure-Dokumentation"

   a. Kopieren Sie den Inhalt der"benutzerdefinierte Rollenberechtigungen für den Konsolenagenten" und speichern Sie sie in einer JSON-Datei.

   b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

      Sie sollten die ID für jedes Azure-Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP -Systeme erstellen.

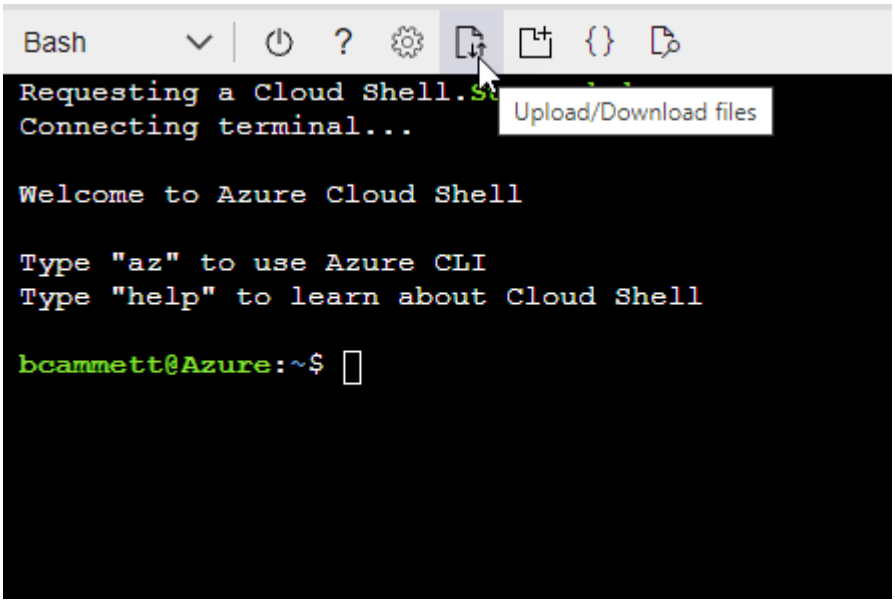
      Beispiel

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]
```

c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

Die folgenden Schritte beschreiben, wie Sie die Rolle mithilfe von Bash in Azure Cloud Shell erstellen.

- Start "Azure Cloud Shell" und wählen Sie die Bash-Umgebung.
- Laden Sie die JSON-Datei hoch.



- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
az role definition create --role-definition agent_Policy.json
```

Sie sollten jetzt über eine benutzerdefinierte Rolle namens „Konsolenoperator“ verfügen, die Sie der virtuellen Maschine des Konsolenagenten zuweisen können.

2. Weisen Sie die Anwendung der Rolle zu:

a. Öffnen Sie im Azure-Portal den Dienst **Abonnements**.

b. Wählen Sie das Abonnement aus.

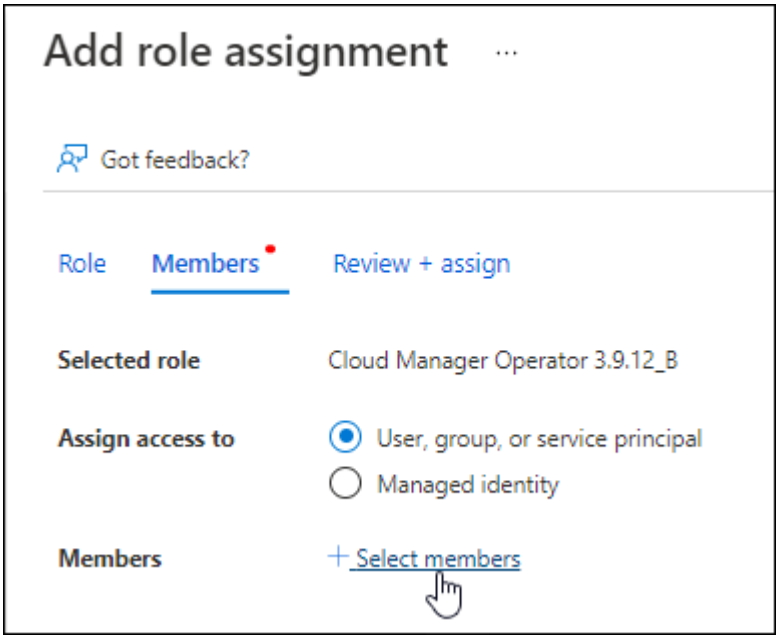
c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

d. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.

e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

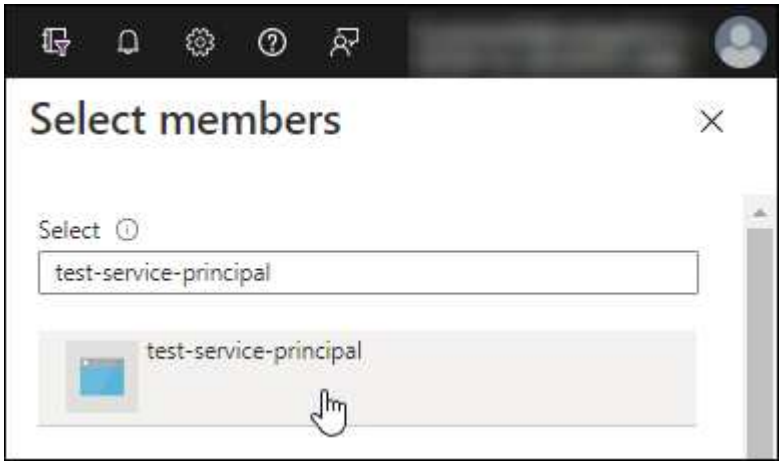
- Behalten Sie die Auswahl von **Benutzer, Gruppe oder Dienstprinzipal** bei.

- Wählen Sie **Mitglieder auswählen**.



- Suchen Sie nach dem Namen der Anwendung.

  Hier ist ein Beispiel:



- Wählen Sie die Anwendung aus und wählen Sie **Auswählen**.
- Wählen Sie **Weiter**.

f. Wählen Sie **Überprüfen + zuweisen**.

   Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

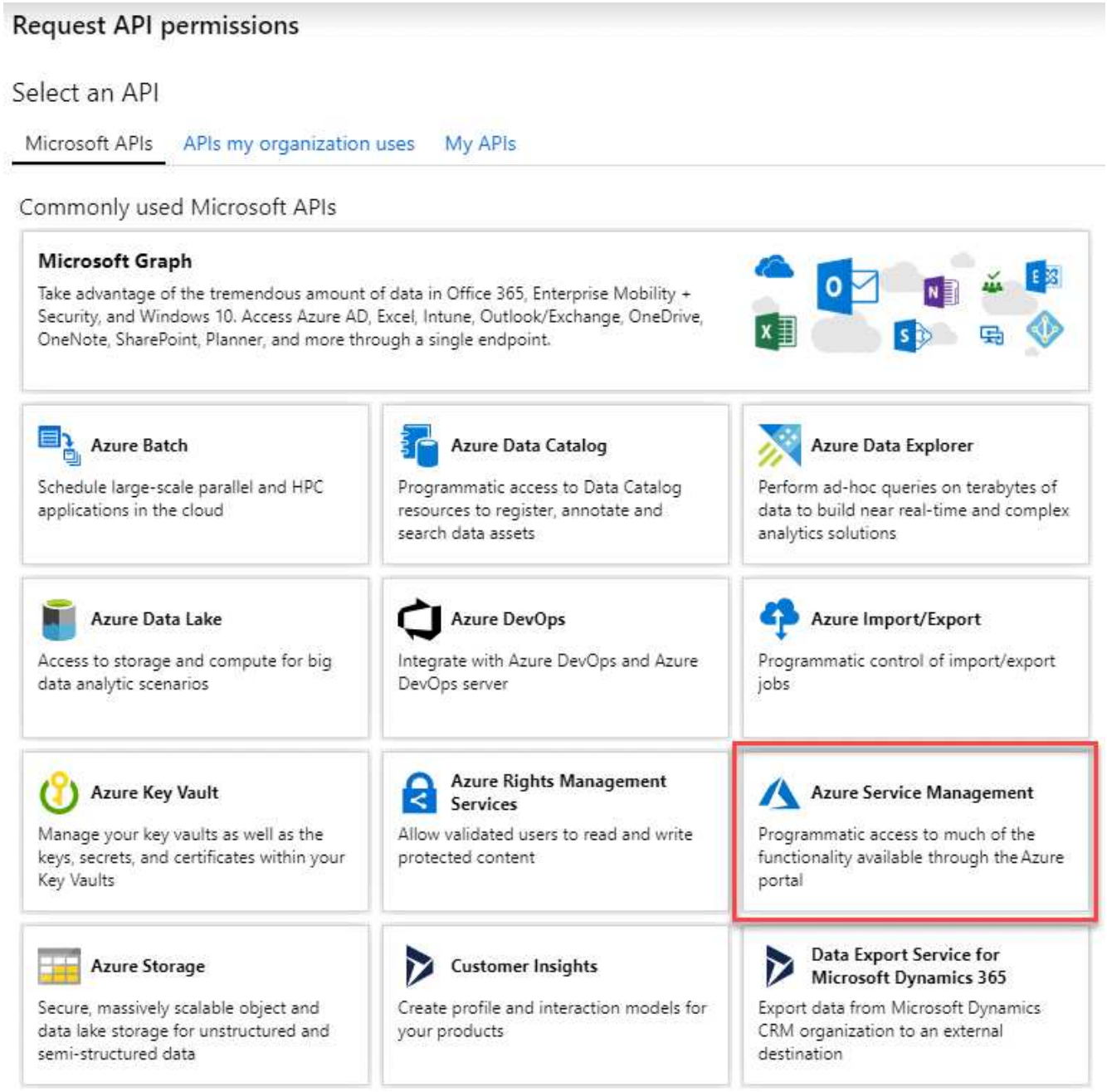
Wenn Sie Cloud Volumes ONTAP aus mehreren Azure-Abonnements bereitstellen möchten, müssen Sie den Dienstprinzipal an jedes dieser Abonnements binden. In der NetApp Console können Sie das Abonnement auswählen, das Sie beim Bereitstellen von Cloud Volumes ONTAP verwenden möchten.

Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

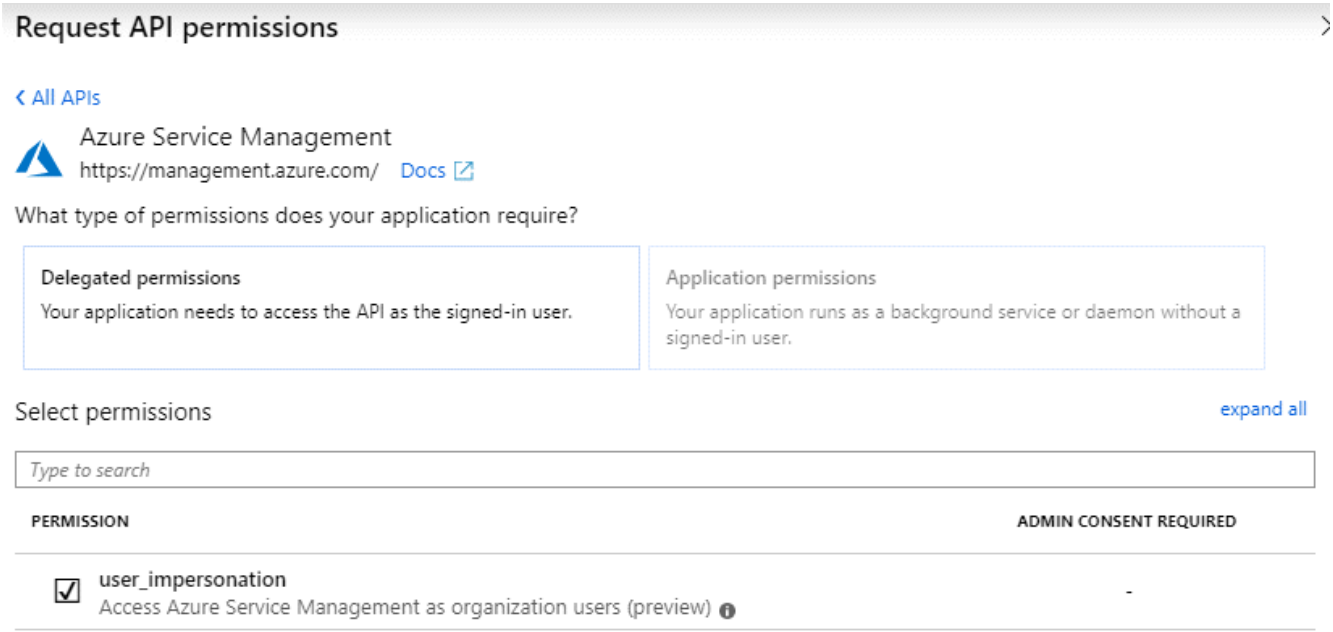
Sie müssen dem Dienstprinzipal die Berechtigung „Windows Azure Service Management API“ zuweisen.

Schritte

1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Wählen Sie **API-Berechtigungen > Berechtigung hinzufügen**.
3. Wählen Sie unter **Microsoft-APIs Azure Service Management** aus.



4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.

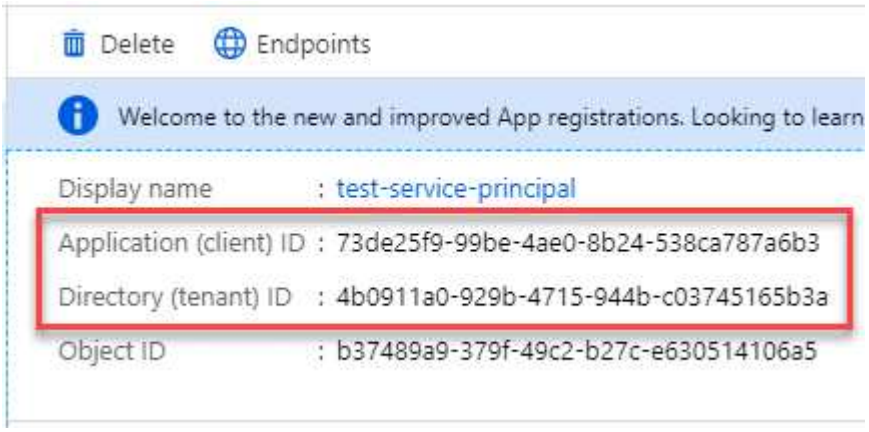


Abrufen der Anwendungs-ID und der Verzeichnis-ID

Wenn Sie das Azure-Konto zur Konsole hinzufügen, müssen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) für die Anwendung angeben. Die Konsole verwendet die IDs zur programmgesteuerten Anmeldung.

Schritte

1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



Wenn Sie das Azure-Konto zur Konsole hinzufügen, müssen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) für die Anwendung angeben. Die Konsole verwendet die IDs zur programmgesteuerten Anmeldung.

Erstellen eines Client-Geheimnisses

Erstellen Sie ein Client-Geheimnis und geben Sie dessen Wert an die Konsole zur Authentifizierung mit der Microsoft Entra-ID weiter.

Schritte

1. Öffnen Sie den Dienst **Microsoft Entra ID**.
2. Wählen Sie **App-Registrierungen** und wählen Sie Ihre Anwendung aus.
3. Wählen Sie **Zertifikate und Geheimnisse > Neues Clientgeheimnis**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Wählen Sie **Hinzufügen**.
6. Kopieren Sie den Wert des Client-Geheimnisses.

Ergebnis

Ihr Dienstprinzipal ist jetzt eingerichtet und Sie sollten die Anwendungs-ID (Client-ID), die Verzeichnis-ID (Mandant-ID) und den Wert des Client-Geheimnisses kopiert haben. Sie müssen diese Informationen in der Konsole eingeben, wenn Sie ein Azure-Konto hinzufügen.

Fügen Sie die Anmeldeinformationen zur Konsole hinzu

Nachdem Sie ein Azure-Konto mit den erforderlichen Berechtigungen bereitgestellt haben, können Sie die Anmeldeinformationen für dieses Konto zur Konsole hinzufügen. Wenn Sie diesen Schritt abschließen, können Sie Cloud Volumes ONTAP mit anderen Azure-Anmeldeinformationen starten.

Bevor Sie beginnen

Wenn Sie diese Anmeldeinformationen gerade bei Ihrem Cloud-Anbieter erstellt haben, kann es einige Minuten dauern, bis sie zur Verwendung verfügbar sind. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zur Konsole hinzufügen.

Bevor Sie beginnen

Sie müssen einen Konsolenagenten erstellen, bevor Sie die Konsoleneinstellungen ändern können. "Erfahren Sie, wie Sie einen Konsolenagenten erstellen" .

Schritte

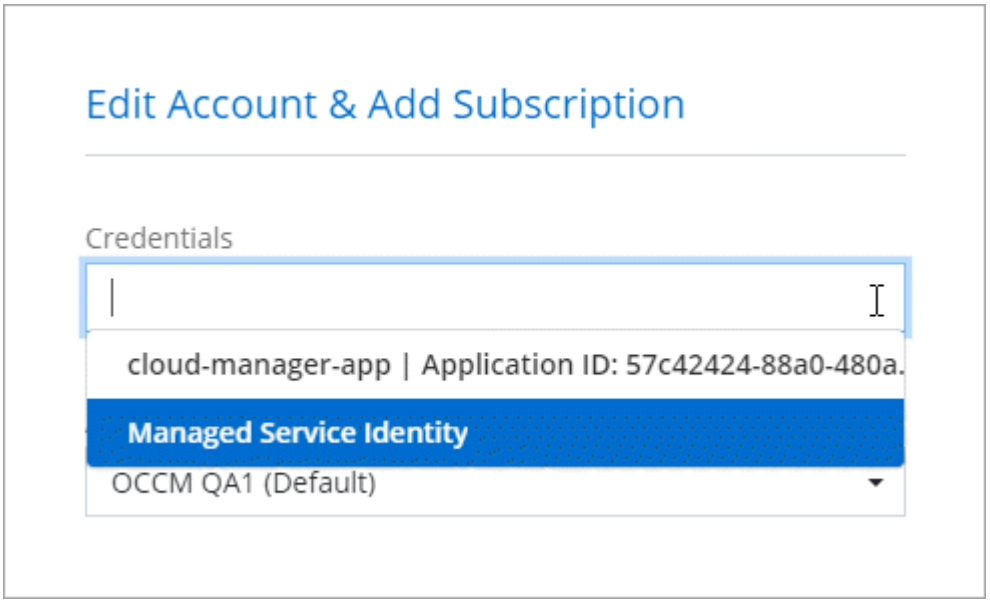
1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Microsoft Azure > Agent**.
   b. **Anmeldeinformationen definieren**: Geben Sie Informationen zum Microsoft Entra-Dienstprinzipal ein, der die erforderlichen Berechtigungen erteilt:
      - Anwendungs-ID (Client-ID)
      - Verzeichnis-ID (Mandant)
      - Client-Geheimnis

c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.

d. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Ergebnis

Sie können auf der Seite „Details und Anmeldeinformationen“ zu einem anderen Satz von Anmeldeinformationen wechseln. "beim Hinzufügen eines Systems zur Konsole"



Vorhandene Anmeldeinformationen verwalten

Verwalten Sie die Azure-Anmeldeinformationen, die Sie der Konsole bereits hinzugefügt haben, indem Sie ein Marketplace-Abonnement zuordnen, Anmeldeinformationen bearbeiten und löschen.

Zuordnen eines Azure Marketplace-Abonnements zu Anmeldeinformationen

Nachdem Sie Ihre Azure-Anmeldeinformationen zur Konsole hinzugefügt haben, können Sie diesen Anmeldeinformationen ein Azure Marketplace-Abonnement zuordnen. Mit dem Abonnement können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und auf NetApp -Datendienste zugreifen.

Es gibt zwei Szenarien, in denen Sie ein Azure Marketplace-Abonnement zuordnen können, nachdem Sie die Anmeldeinformationen bereits zur Konsole hinzugefügt haben:

- Sie haben beim ersten Hinzufügen der Anmeldeinformationen zur Konsole kein Abonnement zugeordnet.
- Sie möchten das Azure Marketplace-Abonnement ändern, das mit Azure-Anmeldeinformationen verknüpft ist.

  Durch das Ersetzen des aktuellen Marktplatzabonnements wird es für vorhandene und neue Cloud Volumes ONTAP Systeme aktualisiert.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.

3. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen aus, die einem Konsolenagenten zugeordnet sind, und wählen Sie dann **Abonnement konfigurieren**.

   Sie müssen Anmeldeinformationen auswählen, die einem Konsolenagenten zugeordnet sind. Sie können ein Marktplatzabonnement nicht mit Anmeldeinformationen verknüpfen, die mit der NetApp Console verknüpft sind.

4. Um die Anmeldeinformationen mit einem vorhandenen Abonnement zu verknüpfen, wählen Sie das Abonnement aus der Dropdown-Liste aus und wählen Sie **Konfigurieren**.
5. Um die Anmeldeinformationen einem neuen Abonnement zuzuordnen, wählen Sie **Abonnement hinzufügen > Fortfahren** und befolgen Sie die Schritte im Azure Marketplace:

   a. Melden Sie sich bei entsprechender Aufforderung bei Ihrem Azure-Konto an.

   b. Wählen Sie **Abonnieren**.

   c. Füllen Sie das Formular aus und wählen Sie **Abonnieren**.

   d. Nachdem der Abonnementvorgang abgeschlossen ist, wählen Sie **Konto jetzt konfigurieren**.

      Sie werden zur NetApp Console weitergeleitet.

   e. Auf der Seite **Abonnementzuweisung**:

      - Wählen Sie die Konsolenorganisationen oder -konten aus, mit denen Sie dieses Abonnement verknüpfen möchten.
      - Wählen Sie im Feld **Vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

        Die Konsole ersetzt das vorhandene Abonnement für alle Anmeldeinformationen in der Organisation oder im Konto durch dieses neue Abonnement. Wenn ein Satz von Anmeldeinformationen nie mit einem Abonnement verknüpft war, wird dieses neue Abonnement nicht mit diesen Anmeldeinformationen verknüpft.

   Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.

      ◦ Wählen Sie **Speichern**.

Anmeldeinformationen bearbeiten

Bearbeiten Sie Ihre Azure-Anmeldeinformationen in der Konsole. Sie können beispielsweise das Clientgeheimnis aktualisieren, wenn ein neues Geheimnis für die Dienstprinzipalanwendung erstellt wurde.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie das Aktionsmenü für einen Satz Anmeldeinformationen und wählen Sie dann **Anmeldeinformationen bearbeiten**.
4. Nehmen Sie die erforderlichen Änderungen vor und wählen Sie dann **Übernehmen**.

Anmeldeinformationen löschen

Wenn Sie einen Satz Anmeldeinformationen nicht mehr benötigen, können Sie ihn löschen. Sie können nur Anmeldeinformationen löschen, die keinem System zugeordnet sind.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Anmeldeinformationen löschen**.
4. Wählen Sie zur Bestätigung **Löschen**.

Google Cloud

Erfahren Sie mehr über Google Cloud-Projekte und -Berechtigungen

Erfahren Sie, wie die NetApp Console Google Cloud-Anmeldeinformationen verwendet, um Aktionen in Ihrem Namen auszuführen, und wie diese Anmeldeinformationen mit Marktplatzabonnements verknüpft werden. Das Verständnis dieser Details kann hilfreich sein, wenn Sie die Anmeldeinformationen für ein oder mehrere Google Cloud-Projekte verwalten. Beispielsweise möchten Sie möglicherweise mehr über das Dienstkonto erfahren, das mit der Konsolen-Agent-VM verknüpft ist.

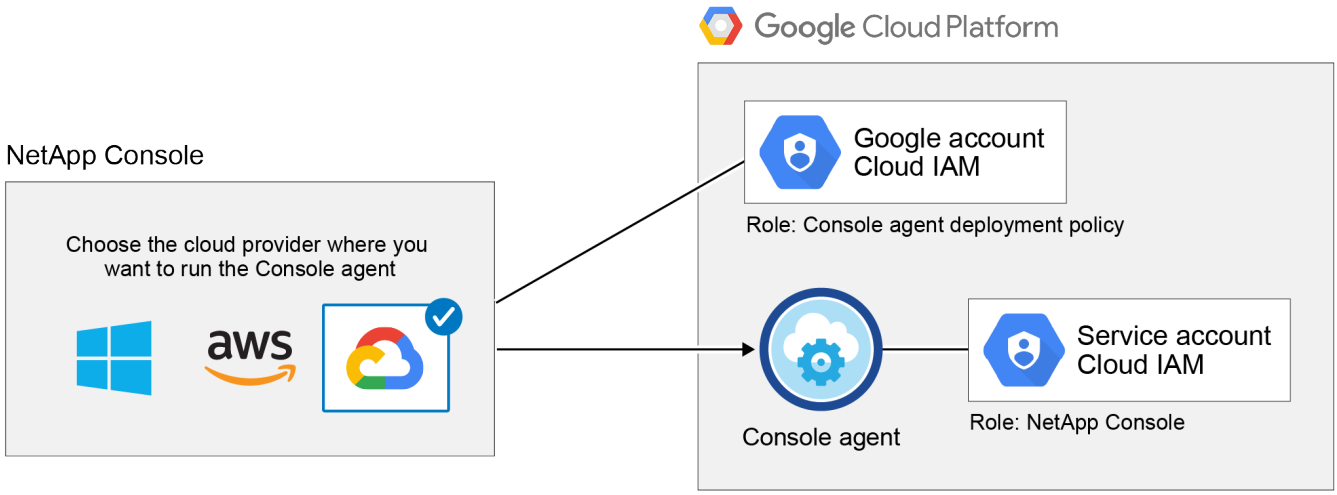
Projekt und Berechtigungen für die NetApp Console

Bevor Sie die Konsole zum Verwalten von Ressourcen in Ihrem Google Cloud-Projekt verwenden können, müssen Sie zunächst einen Konsolen-Agenten bereitstellen. Der Agent darf nicht bei Ihnen vor Ort oder bei einem anderen Cloud-Anbieter ausgeführt werden.

Bevor Sie einen Konsolenagenten direkt von der Konsole aus bereitstellen können, müssen zwei Berechtigungssätze vorhanden sein:

1. Sie müssen einen Konsolen-Agenten mit einem Google-Konto bereitstellen, das über die Berechtigung zum Starten des Konsolen-Agenten von der Konsole aus verfügt.
2. Beim Bereitstellen des Konsolenagenten werden Sie aufgefordert, einen "Dienstkonto" für den Agenten Die Konsole erhält vom Dienstkonto Berechtigungen zum Erstellen und Verwalten von Cloud Volumes ONTAP -Systemen, zum Verwalten von Backups mithilfe von NetApp Backup und Recovery und mehr. Berechtigungen werden erteilt, indem dem Dienstkonto eine benutzerdefinierte Rolle zugewiesen wird.

Die folgende Abbildung veranschaulicht die unter den Nummern 1 und 2 beschriebenen Berechtigungsanforderungen:



Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

- "Google Cloud-Berechtigungen für den Standardmodus einrichten"
- "Berechtigungen für den eingeschränkten Modus einrichten"

Anmeldeinformationen und Marktplatzabonnements

Wenn Sie einen Konsolen-Agenten in Google Cloud bereitstellen, erstellt die Konsole einen Standardsatz von Anmeldeinformationen für das Google Cloud-Dienstkonto in dem Projekt, in dem sich der Konsolen-Agent befindet. Diese Anmeldeinformationen müssen mit einem Google Cloud Marketplace-Abonnement verknüpft sein, damit Sie für Cloud Volumes ONTAP und NetApp -Datendienste bezahlen können.

"Erfahren Sie, wie Sie ein Google Cloud Marketplace-Abonnement zuordnen" .

Beachten Sie Folgendes zu Google Cloud-Anmeldeinformationen und Marktplatz-Abonnements:

- Einem Konsolenagenten kann nur ein Satz Google Cloud-Anmeldeinformationen zugeordnet werden.
- Sie können den Anmeldeinformationen nur ein Google Cloud Marketplace-Abonnement zuordnen
- Sie können ein bestehendes Marktplatz-Abonnement durch ein neues Abonnement ersetzen

Projekt für Cloud Volumes ONTAP

Cloud Volumes ONTAP kann sich im selben Projekt wie der Konsolenagent oder in einem anderen Projekt befinden. Um Cloud Volumes ONTAP in einem anderen Projekt bereitzustellen, müssen Sie zuerst das Dienstkonto und die Rolle des Konsolenagenten zu diesem Projekt hinzufügen.

- "Erfahren Sie, wie Sie das Dienstkonto einrichten"
- "Erfahren Sie, wie Sie Cloud Volumes ONTAP in Google Cloud bereitstellen und ein Projekt auswählen"

Google Cloud-Anmeldeinformationen und Abonnements für die NetApp Console verwalten

Sie können die Google Cloud-Anmeldeinformationen, die mit einer Console-Agent-VM-Instanz verknüpft sind, verwalten, indem Sie ein Marketplace-Abonnement zuordnen und den Abonnementprozess beheben. Beide Aufgaben gewährleisten, dass Sie Ihr Marketplace-Abonnement zur Bezahlung von Datendiensten nutzen können.

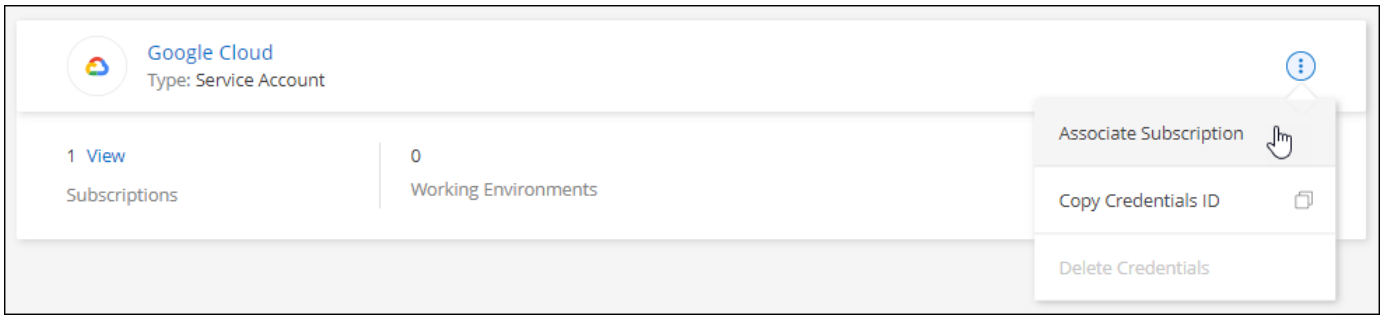
Verknüpfen Sie ein Marketplace-Abonnement mit Google Cloud-Anmeldeinformationen

Wenn Sie einen Console-Agenten in Google Cloud bereitstellen, erstellt die Console standardmäßig einen Satz von Anmeldeinformationen, die mit einer Console-Agent-VM-Instanz verknüpft sind. Sie können das Google Cloud Marketplace-Abonnement, das mit diesen Anmeldeinformationen verknüpft ist, jederzeit ändern. Das Abonnement ermöglicht es Ihnen, ein Cloud Volumes ONTAP System mit nutzungsbasierter Abrechnung zu erstellen und andere Datendienste zu nutzen.

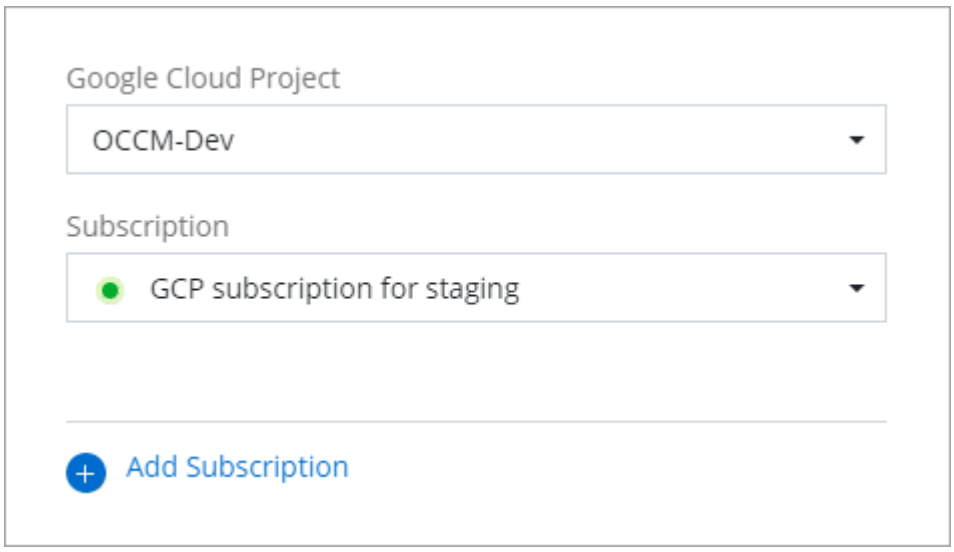
Durch das Ersetzen des aktuellen Marktplatzabonnements durch ein neues Abonnement wird das Marktplatzabonnement für alle vorhandenen Cloud Volumes ONTAP Systeme und alle neuen Systeme geändert.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen aus, die einem Konsolenagenten zugeordnet sind, und wählen Sie dann **Abonnement konfigurieren**.



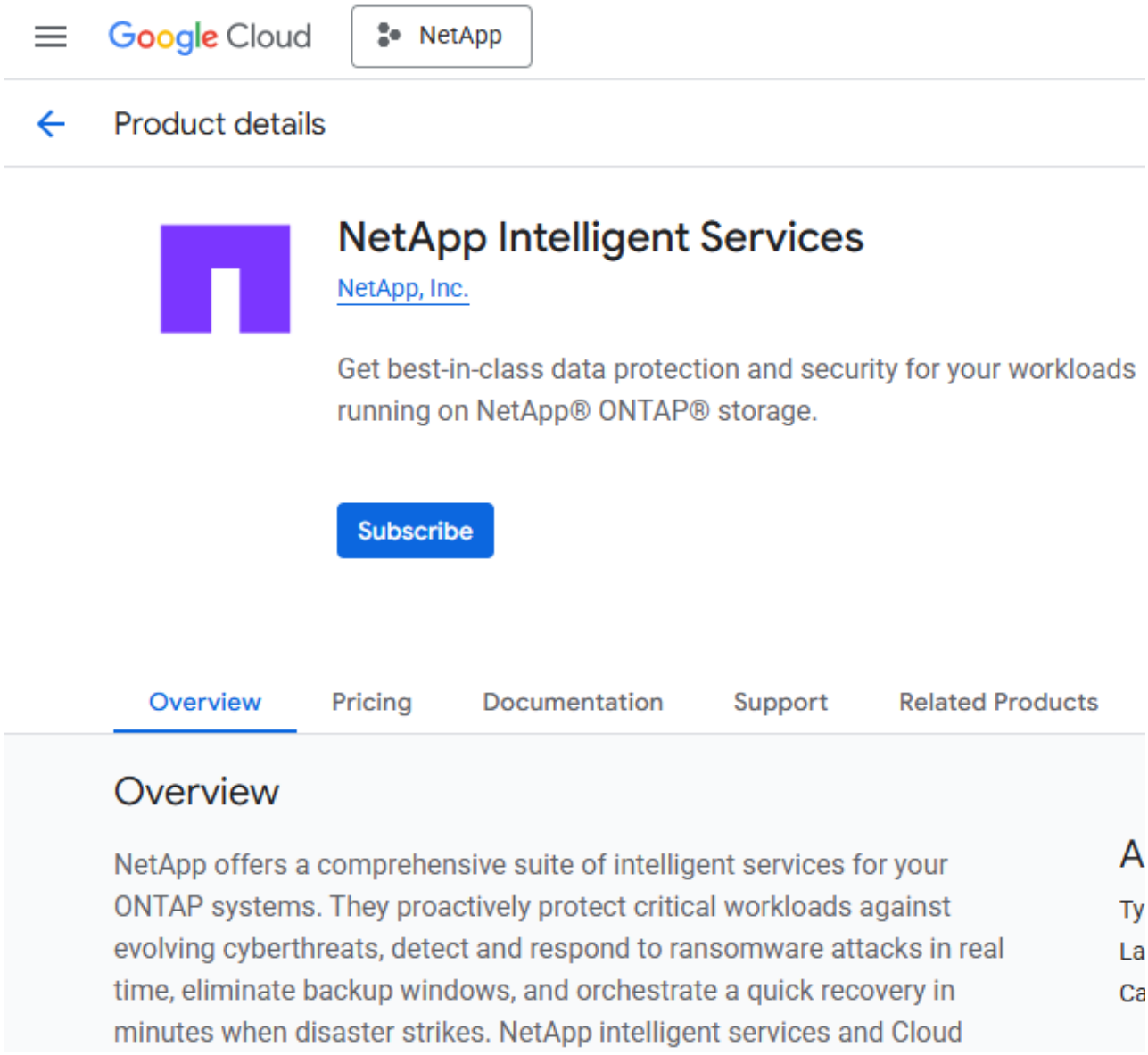
1. Um ein vorhandenes Abonnement mit den ausgewählten Anmeldeinformationen zu konfigurieren, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Dropdown-Liste aus und wählen Sie dann **Konfigurieren**.



2. Wenn Sie noch kein Abonnement haben, wählen Sie **Abonnement hinzufügen > Fortfahren** und folgen Sie den Schritten im Google Cloud Marketplace.

Bevor Sie die folgenden Schritte ausführen, stellen Sie sicher, dass Sie sowohl über Abrechnungsadministratorberechtigungen in Ihrem Google Cloud-Konto als auch über eine NetApp Console verfügen.

a. Nachdem Sie weitergeleitet wurden auf die "NetApp Intelligent Services -Seite im Google Cloud Marketplace" , stellen Sie sicher, dass im oberen Navigationsmenü das richtige Projekt ausgewählt ist.



b. Wählen Sie **Abonnieren**.

c. Wählen Sie das entsprechende Abrechnungskonto aus und stimmen Sie den Allgemeinen Geschäftsbedingungen zu.

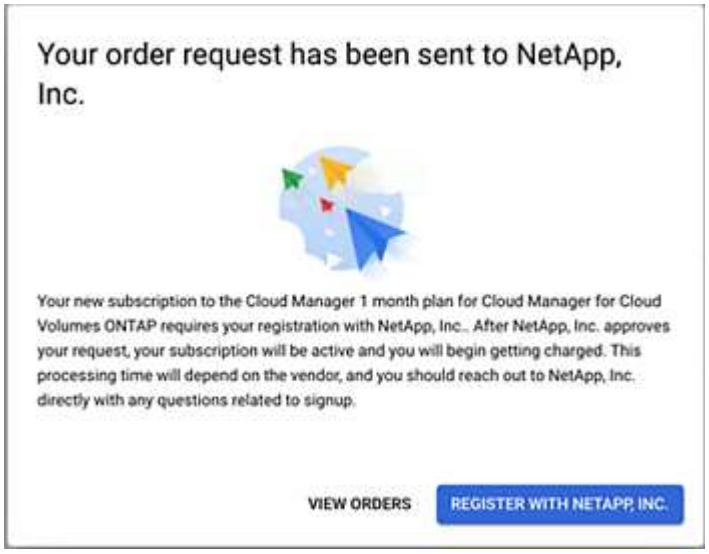
d. Wählen Sie **Abonnieren**.

Dieser Schritt sendet Ihre Übertragungsanforderung an NetApp.

e. Wählen Sie im Popup-Dialogfeld **Bei NetApp, Inc. registrieren** aus.

Dieser Schritt muss abgeschlossen werden, um das Google Cloud-Abonnement mit Ihrer Konsolenorganisation oder Ihrem Konsolenkonto zu verknüpfen. Der Vorgang zum Verknüpfen eines

Abonnements ist erst abgeschlossen, wenn Sie von dieser Seite umgeleitet werden und sich dann bei der Konsole anmelden.



f. Führen Sie die Schritte auf der Seite **Abonnementzuweisung** aus:

> Wenn jemand aus Ihrer Organisation bereits ein Marktplatz-Abonnement von Ihrem Abrechnungskonto hat, werden Sie weitergeleitet zu "die Cloud Volumes ONTAP -Seite in der NetApp Console" stattdessen. Wenn dies unerwartet vorkommt, wenden Sie sich an Ihr NetApp -Vertriebsteam. Google ermöglicht nur ein Abonnement pro Google-Abrechnungskonto.

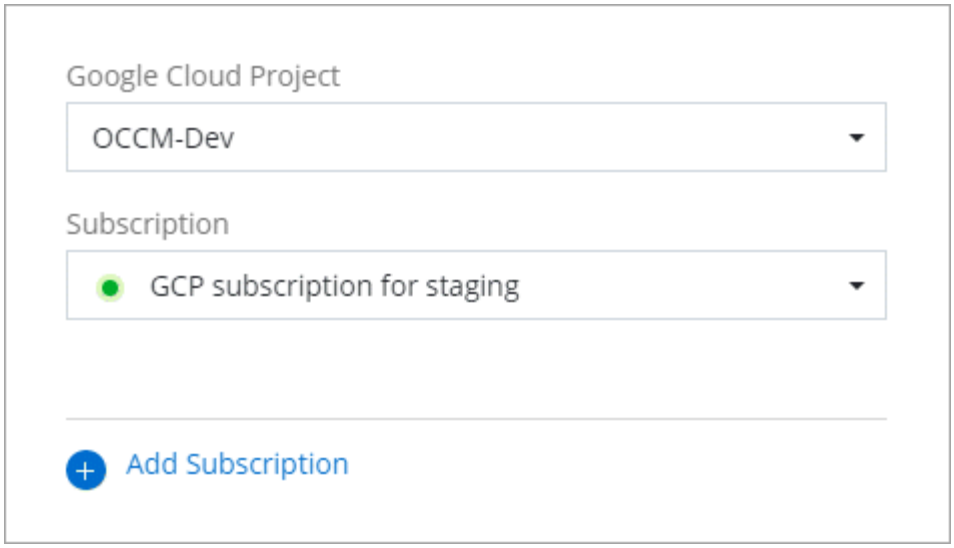
- Wählen Sie die Konsolenorganisation aus, mit der Sie dieses Abonnement verknüpfen möchten.
- Wählen Sie im Feld **Vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für eine Organisation automatisch durch dieses neue Abonnement ersetzen möchten.

  Die Konsole ersetzt das vorhandene Abonnement für alle Anmeldeinformationen in der Organisation durch dieses neue Abonnement. Wenn ein Satz von Anmeldeinformationen nie mit einem Abonnement verknüpft war, wird dieses neue Abonnement nicht mit diesen Anmeldeinformationen verknüpft.

Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.

◦ Wählen Sie **Speichern**.

3. Navigieren Sie nach Abschluss dieses Vorgangs zurück zur Seite „Anmeldeinformationen“ in der Konsole und wählen Sie dieses neue Abonnement aus.

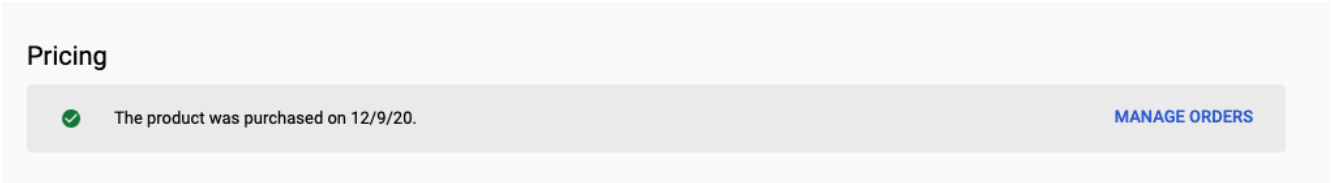


Fehlerbehebung beim Marketplace-Abonnementprozess

Manchmal kann das Abonnieren von NetApp Datendiensten über den Google Cloud Marketplace aufgrund fehlerhafter Berechtigungen oder weil die Weiterleitung zur Console versehentlich nicht befolgt wurde, fragmentiert werden. Wenn dies passiert, verwenden Sie die folgenden Schritte, um den Abonnementprozess abzuschließen.

Schritte

1. Navigieren Sie zu "NetApp page auf dem Google Cloud Marketplace", um den Status der Bestellung zu überprüfen. Wenn auf der Seite **Beim Anbieter verwalten** angezeigt wird, scrollen Sie nach unten und wählen Sie **Bestellungen verwalten**.



   - Wenn die Bestellung ein grünes Häkchen anzeigt und dies unerwartet ist, könnte jemand anderes aus der Organisation, der dasselbe Abrechnungskonto verwendet, bereits abonniert haben. Wenn dies unerwartet ist oder Sie die Details dieses Abonnements benötigen, wenden Sie sich an Ihr NetApp Vertriebsteam.

   - Wenn bei der Bestellung eine Uhr und der Status **Pending** angezeigt werden, gehen Sie zurück zur Marketplace-Seite und wählen Sie **Manage on Provider**, um den Vorgang wie oben dokumentiert abzuschließen.

Identitäts- und Zugriffsverwaltung

Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der NetApp Console

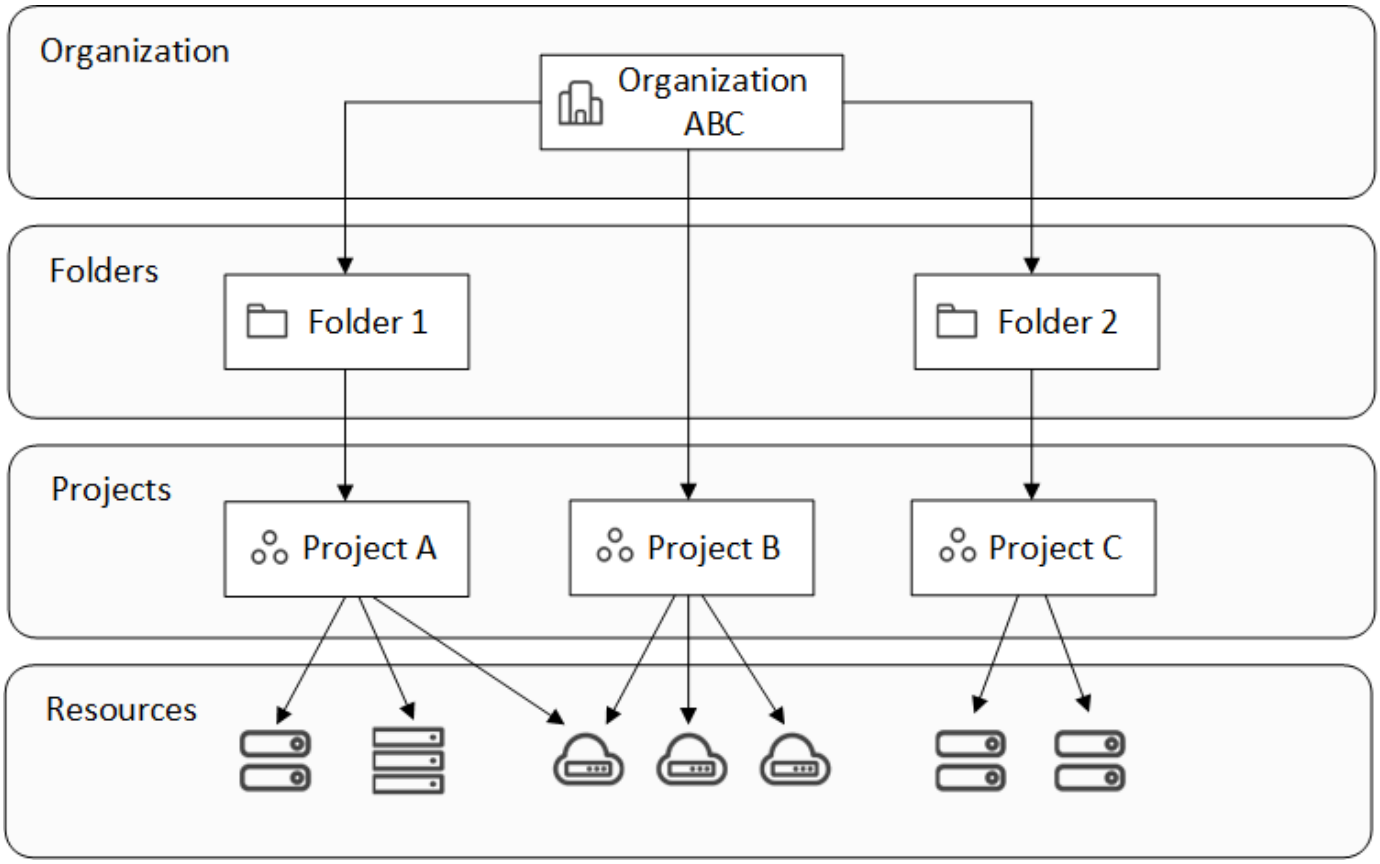
Mit der Identitäts- und Zugriffsverwaltung (IAM) der NetApp Console können Sie Ihre NetApp -Ressourcen organisieren und den Zugriff entsprechend Ihrer Unternehmensstruktur steuern – nach Standort, Abteilung oder Projekt.

Die Ressourcen sind hierarchisch angeordnet: An oberster Stelle steht die Organisation, gefolgt von Ordnern (die weitere Ordner oder Projekte enthalten können) und dann Projekten, die Speichersysteme, Workloads und Agenten enthalten.

Weisen Sie Zugriffsrollen auf Organisations-, Ordner- oder Projektebene zu, damit Benutzer den richtigen Zugriff auf Ressourcen haben.

Sie benötigen die Rollen *Super admin*, *Organization admin* oder *Folder or project admin*, um IAM in der NetApp Console zu verwalten.

Das folgende Bild veranschaulicht diese Hierarchie auf einer grundlegenden Ebene.



]

Komponenten für Identitäts- und Zugriffsmanagement

In der NetApp Console organisieren Sie Ihre Speicherressourcen mithilfe von drei Hauptkomponenten: Organisationskomponenten, Ressourcenkomponenten und Benutzerzugriffskomponenten.

Projekte und Ordner innerhalb Ihrer Organisation

Innerhalb Ihrer IAM-Struktur arbeiten Sie mit drei Organisationskomponenten: Organisationen, Projekten und Ordnern. Sie können Benutzern Zugriff gewähren, indem Sie ihnen Rollen auf einer dieser Ebenen zuweisen.

Organisation

Eine *Organisation* ist die oberste Ebene des Console IAM-Systems und repräsentiert normalerweise Ihr Unternehmen. Ihre Organisation besteht aus Ordnern, Projekten, Mitgliedern, Rollen und Ressourcen. Agenten sind bestimmten Projekten in der Organisation zugeordnet.

Projekte

Ein *Projekt* dient dazu, Zugriff auf eine Speicherressource zu ermöglichen. Sie müssen Ressourcen einem Projekt zuweisen, bevor jemand darauf zugreifen kann. Sie können einem einzelnen Projekt mehrere Ressourcen zuweisen und Sie können auch mehrere Projekte haben. Anschließend weisen Sie den Benutzern Berechtigungen für das Projekt zu, um ihnen Zugriff auf die darin enthaltenen Ressourcen zu gewähren.

Sie können beispielsweise ein lokales ONTAP System einem einzelnen Projekt oder allen Projekten in Ihrer Organisation zuordnen, je nach Ihren Bedürfnissen.

"Erfahren Sie, wie Sie Projekte zu Ihrer Organisation hinzufügen."

Ordner

Gruppieren Sie verwandte Projekte in Ordnern, um sie nach Standort, Standort oder Geschäftsbereich zu organisieren. Ressourcen können nicht direkt Ordnern zugeordnet werden, aber durch die Zuweisung einer Rolle auf Ordnerebene erhält der Benutzer Zugriff auf alle Projekte in diesem Ordner.

"Erfahren Sie, wie Sie Ordner zu Ihrer Organisation hinzufügen."

Ressourcen

Eine *Ressource* ist eine Entität, die der Console bekannt ist und die einem Projekt zugewiesen werden kann. *Ressourcen* umfassen Speichersysteme, Keystone-Abonnements, einige NetApp Backup and Recovery-Workloads sowie Console-Agenten.

+ Eine Ressource muss einem Projekt zugeordnet werden, bevor jemand darauf zugreifen kann.

+

Beispielsweise können Sie ein Cloud Volumes ONTAP -System einem einzelnen Projekt oder allen Projekten in Ihrer Organisation zuordnen. Wie Sie eine Ressource zuordnen, hängt von den Bedürfnissen Ihrer Organisation ab.

+

"Erfahren Sie, wie Sie Ressourcen Projekten zuordnen."

Speichersysteme und Keystone -Abonnements

Speichersysteme sind die primären Ressourcen, die Sie in NetApp Console verwalten. NetApp Console unterstützt die Verwaltung sowohl lokaler als auch Cloud-Speichersysteme. Sie müssen einem Projekt ein Speichersystem hinzufügen, damit die dem Projekt zugewiesenen Personen darauf zugreifen können.

Speichersysteme

Speichersysteme werden automatisch dem Projekt zugeordnet, in dem sie hinzugefügt werden, aber Sie können sie auf der Seite **Ressourcen** auch anderen Projekten oder Ordnern zuordnen. Sie können FSx for

NetApp ONTAP-Speichersysteme nicht Projekten oder Ordnern zuordnen, aber Sie können sie auf der Seite **Systeme** oder unter Workloads einsehen.

Keystone -Abonnements

Keystone -Abonnements sind außerdem Ressourcen, die Sie Projekten zuordnen können, um Benutzern Zugriff auf das Abonnement in der NetApp Console zu gewähren.

Backup and Recovery-Workloads (Oracle und Microsoft SQL Server)

Einige Backup und Recovery Workloads werden ebenfalls als Ressourcen betrachtet. Sie können Benutzern Berechtigungen für den Zugriff auf Backup und

Konsolenagenten

Organisationsadministratoren erstellen Konsolenagenten, um Speichersysteme zu verwalten und NetApp -Datendienste zu aktivieren. Agenten sind zunächst an das Projekt gebunden, in dem sie erstellt wurden. Administratoren können sie jedoch von der Agentenseite aus anderen Projekten oder Ordnern hinzufügen.

Durch die Zuordnung eines Agenten zu einem Projekt wird die Verwaltung von Ressourcen in diesem Projekt ermöglicht, während die Zuordnung eines Agenten zu einem Ordner es Ordner- oder Projektadministratoren erlaubt, zu entscheiden, welche Projekte den Agenten verwenden sollen. Um Managementfunktionen bereitstellen zu können, müssen Agenten bestimmten Projekten zugeordnet werden.

"Erfahren Sie, wie Sie Agenten Projekten zuordnen."

Mitglieder und Rollen

Mitglieder

Mitglieder Ihrer Organisation sind Benutzerkonten oder Dienstkonten. Ein Dienstkonto wird normalerweise von einer Anwendung verwendet, um bestimmte Aufgaben ohne menschliches Eingreifen abzuschließen.

Sie müssen Mitglieder zu Ihrer Organisation hinzufügen, nachdem diese sich bei der NetApp Console angemeldet haben. Sobald sie hinzugefügt wurden, können Sie ihnen Rollen zuweisen, um ihnen Zugriff auf Ressourcen zu gewähren. Sie können Servicekonten manuell über die Konsole hinzufügen oder deren Erstellung und Verwaltung über die NetApp Console IAM API automatisieren.

"Erfahren Sie, wie Sie Mitglieder zu Ihrer Organisation hinzufügen."

Zugriffsrollen

Die Konsole bietet Zugriffsrollen, die Sie den Mitgliedern Ihrer Organisation zuweisen können.

Wenn Sie einem Mitglied eine Rolle zuweisen, können Sie diese Rolle für die gesamte Organisation, einen bestimmten Ordner oder ein bestimmtes Projekt vergeben. Die von Ihnen ausgewählte Rolle gewährt einem Mitglied Berechtigungen für die Ressourcen im ausgewählten Teil der Hierarchie.

Die NetApp Console bietet differenzierte Rollen, die dem Prinzip der „minimalen Berechtigungen“ folgen. Das bedeutet, dass Zugriffsrollen so gestaltet sind, dass Benutzer nur auf das zugreifen können, was sie benötigen.

Dies bedeutet, dass Benutzern im Zuge der Erweiterung ihrer Aufgaben mehrere Rollen zugewiesen werden können.

"Informationen zu Zugriffsrollen" .

Beispiele für IAM-Strategien

Strategie für kleine Organisationen

Für Organisationen mit weniger als 50 Benutzern und zentralisierter Speicherverwaltung empfiehlt sich ein vereinfachter Ansatz mit den Rollen Super-Administrator und Super-Betrachter.

Beispiel: ABC Corporation (5-köpfiges Team)

- **Struktur:** Einzelne Organisation mit 3 Projekten (Produktion, Entwicklung, Backup)
- **Rollen:**
  - 2 hochrangige Mitglieder: **Super-Admin**-Rolle für vollen administrativen Zugriff
  - 3 Teammitglieder: **Superbeobachter**-Rolle zur Überwachung ohne Änderungsrechte
- **Agentenstrategie:** Ein einziger Agent ist allen Projekten für den gemeinsamen Ressourcenzugriff zugeordnet.
- **Vorteile:** Vereinfachte Administration, reduzierte Rollenkomplexität, geeignet für Teams, die einen breiten Zugriff benötigen

Strategie für ein multiregionales Unternehmen

Bei großen Organisationen mit regionalen Niederlassungen und spezialisierten Teams empfiehlt sich ein hierarchischer Ansatz mit Ordnern, die geografische oder Geschäftsbereichsgrenzen repräsentieren.

Beispiel: XYZ Corporation (multinationales Unternehmen)

- **Struktur:** Organisation > Regionale Ordner (Nordamerika, Europa, Asien-Pazifik) > Projektordner pro Region
- **Plattformrollen:**
  - 1 **Organisationsverwaltung**: Globale Aufsicht und Richtlinienmanagement
  - 3 **Ordner- oder Projektadministratoren**: Regionale Kontrolle (einer pro Region)
  - 1 **Verbandsverwaltung**: Integration des Corporate Identity Providers
- **Speicherrollen nach Region:**
  - 9 **Speicheradministration**: Speichersysteme in zugewiesenen Regionen erkennen und verwalten
  - 2 **Speicheranzeige**: Überwachen Sie Speicherressourcen regionsübergreifend
  - 1 **Systemgesundheitsspezialist**: Speicherzustand ohne Systemänderungen verwalten
- **Rollen im Bereich Datendienste:**
  - **Administrator für Datensicherung und -wiederherstellung**: Projektbezogen basierend auf den Aufgaben im Bereich Datensicherung
  - **Administrator für Ransomware-Resilienz**: Überwachung der Sicherheitsteams in verschiedenen Projekten
- **Agentenstrategie:** Regionale Agenten, die geeigneten geografischen Projekten zugeordnet sind
- **Vorteile:** Erhöhte Sicherheit durch Rollentrennung, regionale Autonomie und Einhaltung lokaler Vorschriften

Strategie der Fachbereichsspezialisierung

Für Organisationen mit spezialisierten Teams, die einen spezifischen Zugriff auf Datendienste benötigen, sollten gezielte Rollenzuweisungen auf der Grundlage funktionaler Verantwortlichkeiten verwendet werden.

Beispiel: TechCorp (mittelständisches Technologieunternehmen)

- **Struktur:** Organisation > Abteilungsordner (IT, Sicherheit, Entwicklung) > Projektspezifische Ressourcen
- **Spezialisierte Rollen:**
  - Sicherheitsteam: **Administrator für Ransomware-Resilienz** und **Klassifizierungsbetrachter** (Rollen)
  - Backup-Team: **Super-Administrator für Backup und Wiederherstellung** für umfassende Backup-Operationen
  - Entwicklungsteam: **Speicheradministrator** für die Testumgebungsverwaltung
  - Compliance-Team: **Analyst für operative Unterstützung** für Überwachung und Fallmanagement
- **Agentenstrategie:** Agenten werden basierend auf der Ressourcenverantwortung Abteilungsprojekten zugeordnet.
- **Vorteile:** Maßgeschneiderte Zugangskontrolle, verbesserte betriebliche Effizienz und klare Verantwortlichkeiten für spezialisierte Aufgaben

Nächste Schritte mit IAM in der NetApp Console

- "Erste Schritte mit IAM in der NetApp Console"
- "Überwachen oder prüfen Sie die IAM-Aktivität"
- "Erfahren Sie mehr über die API für NetApp Console IAM"

Erste Schritte mit Identität und Zugriff in der NetApp Console

Wenn Sie sich für die NetApp Console anmelden, werden Sie aufgefordert, eine neue Organisation zu erstellen. Die Organisation umfasst ein Mitglied (einen Organisationsadministrator) und ein Standardprojekt. Um die Identitäts- und Zugriffsverwaltung (IAM) so einzurichten, dass sie Ihren Geschäftsanforderungen entspricht, müssen Sie die Hierarchie Ihrer Organisation anpassen, zusätzliche Mitglieder hinzufügen, Ressourcen hinzufügen oder ermitteln und diese Ressourcen in Ihrer Hierarchie verknüpfen.

Sie benötigen die Berechtigungen **Organisationsadministrator** oder **Superadministrator**, um Identität und Zugriff für Ihre Organisation zu verwalten. Mit **Ordner- oder Projektadministratorberechtigungen** können Sie nur die Ordner und Projekte verwalten, auf die Sie Zugriff haben.

Befolgen Sie diese Schritte, um eine neue Organisation einzurichten. Die Reihenfolge kann je nach den Anforderungen Ihrer Organisation variieren.

1 Bearbeiten Sie das Standardprojekt oder fügen Sie es der Hierarchie Ihrer Organisation hinzu

Verwenden Sie das Standardprojekt oder erstellen Sie zusätzliche Projekte und Ordner, die Ihrer Unternehmenshierarchie entsprechen.

"Erfahren Sie, wie Sie Ihre Ressourcen mit Ordnern und Projekten organisieren" .

2 Ordnen Sie Mitglieder Ihrer Organisation zu

Nachdem sich Benutzer bei NetApp Console registriert haben, müssen Sie sie explizit Ihrer Console-Organisation hinzufügen. Sie haben außerdem die Möglichkeit, Ihrer Organisation Servicekonten hinzuzufügen.

"Erfahren Sie, wie Sie Mitglieder und ihre Berechtigungen verwalten" .

3 Ressourcen hinzufügen oder entdecken

Fügen Sie der Konsole Ressourcen (Systeme) hinzu oder ermitteln Sie sie. Mitglieder der Organisation verwalten Systeme innerhalb eines Projekts.

Erfahren Sie, wie Sie Ressourcen erstellen oder entdecken:

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Systeme der E-Serie"
- "On-Premises- ONTAP -Cluster"
- "StorageGRID"

4 Ressourcen zusätzlichen Projekten zuordnen

Durch das Hinzufügen oder Erkennen eines Systems in der Konsole wird die Ressource automatisch dem aktuell ausgewählten Projekt zugeordnet. Um diese Ressource einem anderen Projekt in Ihrer Organisation zur Verfügung zu stellen, verknüpfen Sie sie mit dem jeweiligen Projekt. Wenn zur Verwaltung der Ressource ein Konsolenagent verwendet wird, ordnen Sie den Konsolenagenten dem jeweiligen Projekt zu.

- "Erfahren Sie, wie Sie die Ressourcenhierarchie Ihres Unternehmens verwalten" .
- "Erfahren Sie, wie Sie einen Konsolenagenten mit einem Ordner oder Projekt verknüpfen" .

Ähnliche Informationen

- "Erfahren Sie mehr über Identitäts- und Zugriffsmanagement in der NetApp Console"
- "Erfahren Sie mehr über die API für Identität und Zugriff"

Richten Sie Ihre Konsolenorganisation ein.

Fügen Sie Ihrer NetApp Console Organisation Ordner und Projekte hinzu.

Fügen Sie Ordner und Projekte hinzu, die Ihrer Unternehmensstruktur entsprechen. Nachdem Sie Ordner und Projekte erstellt haben, können Sie ihnen Ressourcen zuordnen und den Zugriff von Mitgliedern auf diese Projekte verwalten.

Die Konsole erstellt automatisch ein Projekt für Sie, wenn Sie eine neue Organisation anlegen. Die meisten Organisationen benötigen mehr als ein Projekt sowie Ordner, um die Dinge übersichtlich zu organisieren. "Erfahren Sie mehr über die Ressourcenhierarchie in der NetApp Console."Die

Ressourcen mithilfe von Ordnern und Projekten organisieren

In der NetApp Console enthält eine Organisation Ordner und Projekte, die Ihnen helfen, Ihre Ressourcen zu organisieren. Ordner helfen Ihnen, zusammengehörige Projekte zu gruppieren, und Projekte helfen Ihnen, Ressourcen und den Mitgliederzugriff zu verwalten.

Ordner

Ordner helfen Ihnen, zusammengehörige Projekte zu organisieren. Sie können verschachtelte Ordner erstellen, um verschiedene Ebenen der Struktur Ihrer Organisation darzustellen. Beispielsweise könnten Sie für jede Geschäftseinheit einen Ordner der obersten Ebene erstellen und darin Unterordner für die verschiedenen Teams innerhalb dieser Geschäftseinheit anlegen. Anschließend erstellen Sie Projekte in Ordnern.

Ordner ermöglichen Ihnen außerdem eine effizientere Verwaltung der Mitgliederzugriffe durch Rollenvererbung. Wenn Sie Mitgliedern Rollen auf Ordnerebene zuweisen, erben diese die Berechtigungen für alle untergeordneten Projekte und Ordner.

Ordner sind ein Organisationswerkzeug und für Mitglieder, die keine IAM-Berechtigungen wie z. B. die Rollen Organisationsadministrator, Ordner- oder Projektadministrator oder Superadministrator besitzen, nicht sichtbar. Mitglieder greifen auf Projekte zu, nicht auf Ordner.

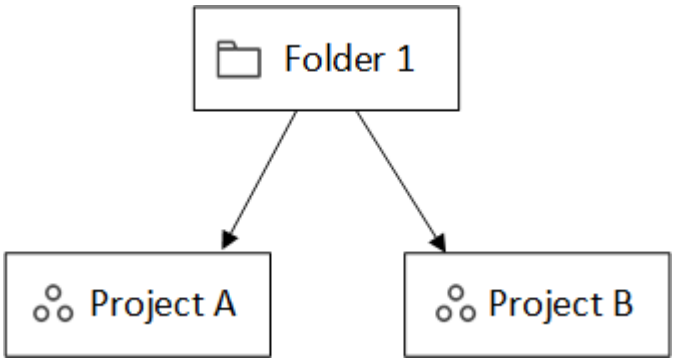
Organisationsadministratoren können administrative Aufgaben delegieren, indem sie Ordner erstellen. Nach dem Erstellen eines Ordners kann ein Organisationsadministrator einem Mitglied die Ordner- oder Projektadministratorrolle für bestimmte Ordner zuweisen. Diese Mitglieder können dann alle Projekte innerhalb dieses Ordners verwalten, ohne Zugriff auf die gesamte Organisation zu haben.

Ordner können andere Ordner oder Projekte als Unterordner haben, aber es können keine Ressourcen direkt mit ihnen verknüpft sein. Ressourcen müssen einem Projekt zugeordnet werden.

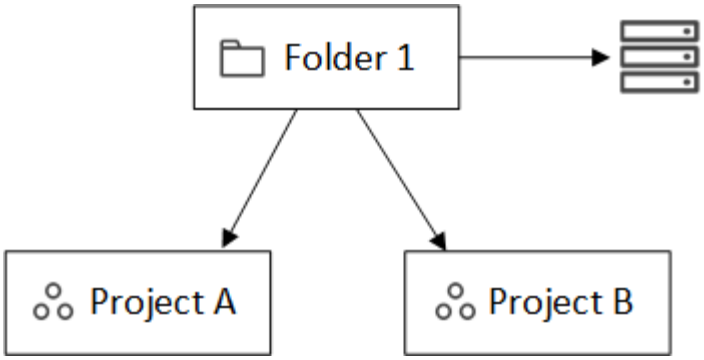
Wann sollte eine Ressource einem Ordner zugeordnet werden?

Ein *Organisationsadministrator* kann eine Ressource mit einem Ordner verknüpfen, sodass ein *Ordner- oder Projektadministrator* sie mit den entsprechenden Projekten im Ordner verknüpfen kann.

Nehmen wir beispielsweise an, Sie haben einen Ordner, der zwei Projekte enthält:

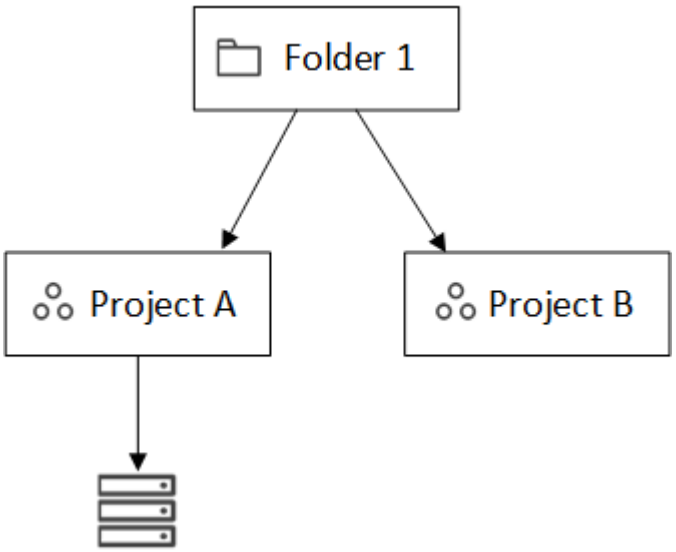


Der *Organisationsadministrator* kann eine Ressource mit dem Ordner verknüpfen:



Durch die Verknüpfung einer Ressource mit einem Ordner wird diese nicht für alle Projekte zugänglich; nur der Ordner- oder Projektadministrator kann sie sehen. Der *Ordner- oder Projektadministrator* entscheidet, welche Projekte darauf zugreifen können und ordnet die Ressource den entsprechenden Projekten zu.

In diesem Beispiel verknüpft der Administrator die Ressource mit Projekt A:



Mitglieder, die über Berechtigungen für Projekt A verfügen, können jetzt auf die Ressource zugreifen.

Projekte

Ordnen Sie Ressourcen Projekten zu, damit die Mitglieder diese verwalten können. Ressourcen müssen einem Projekt zugeordnet werden, damit sie verwaltet und von Benutzern zugänglich gemacht werden können.

Eine Organisation kann ein oder mehrere Projekte haben. Ein Projekt kann sich direkt unter der Organisation oder in einem Ordner befinden. Wenn ein Agent zur Ermittlung von Ressourcen innerhalb eines Projekts verwendet wird, müssen Sie den Agenten auch diesem Projekt zuordnen.

Auf der Seite **Systeme** navigieren die Benutzer zwischen den ihnen zugewiesenen Projekten, um die Ressourcen zu verwalten, die mit jedem Projekt verbunden sind.

Einen Ordner oder ein Projekt hinzufügen

Fügen Sie Projekte hinzu, um Ressourcen zu verwalten, und Ordner, um zusammengehörige Projekte zu gruppieren. Wenn Sie eine neue Organisation erstellen, enthält die Konsole ein Projekt.

Sie können in der Ressourcenstruktur Ihrer Organisation bis zu sieben Ebenen von Ordnern und Projekten erstellen. Erstellen Sie nach Bedarf verschachtelte Ordner, um Ihre Ressourcen zu organisieren.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Organisation** aus.
3. Wählen Sie auf der Seite **Organisation** die Option **Ordner oder Projekt hinzufügen** aus.
4. Wählen Sie **Ordner** oder **Projekt**.
5. Ordner- oder Projektdetails eingeben:
   - **Name und Speicherort**: Geben Sie einen Namen ein und wählen Sie einen Speicherort für den Ordner oder das Projekt. Sie können Ordner oder Projekte innerhalb der Organisation oder in einem anderen Ordner ablegen.
   - **Ressourcen**: Wählen Sie die Ressourcen aus, die Sie diesem Ordner oder Projekt zuordnen möchten. Falls Sie der Konsole noch keine Speichersysteme hinzugefügt haben, können Sie diesen Schritt später durchführen.

     Mitglieder können erst dann auf Ressourcen in einem Ordner zugreifen, wenn diese Ressourcen einem Projekt zugewiesen wurden. Verwenden Sie Ordner, um Ressourcen vorübergehend zu speichern, bis Sie die benötigten Projekte erstellt haben. Dies kann dem Organisationsadministrator helfen, die Ressourcenzuweisung an einen Ordner- oder Projektadministrator zu delegieren, der dann Ressourcen den Projekten innerhalb des Ordners zuweist.

   - **Zugriff**: Wählen Sie **Mitglied hinzufügen**, um Zugriffsrechte und eine Rolle zuzuweisen. Sie können jederzeit Mitglieder zum Projekt oder Ordner hinzufügen oder daraus entfernen.

     "Informationen zu Zugriffsrollen" .
6. Wählen Sie **Hinzufügen**.

Umbenennen eines Ordners oder Projekts

Benennen Sie einen Ordner oder ein Projekt nach Bedarf um. Die Umbenennung hat keine Auswirkungen auf zugehörige Ressourcen oder den Mitgliederzugriff.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.
2. Geben Sie auf der Seite **Bearbeiten** einen neuen Namen ein und wählen Sie **Übernehmen**.

Löschen eines Ordners oder Projekts

Löschen Sie Ordner und Projekte, die Sie nicht mehr benötigen, beispielsweise nach einer Teamumstrukturierung oder nach Projektabschluss.

Bevor Sie einen Ordner oder ein Projekt löschen, vergewissern Sie sich, dass es keine Ressourcen mehr enthält. Erfahren Sie, wie Sie Ressourcen entfernen.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und

wählen Sie dann **Löschen**.

2. Bestätigen Sie, dass Sie den Ordner oder das Projekt löschen möchten.

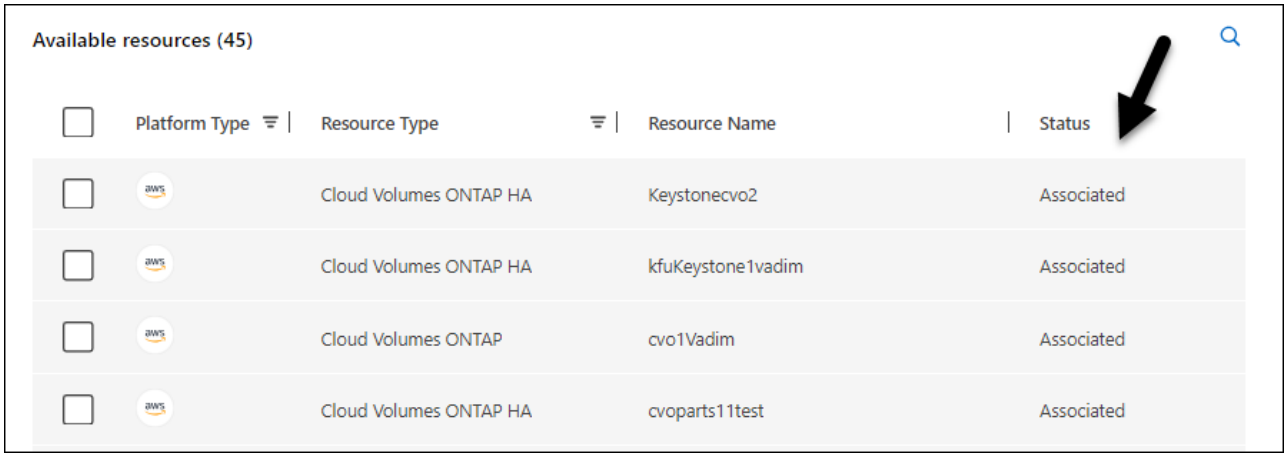
Anzeigen der mit einem Ordner oder Projekt verknüpften Ressourcen

Zeigen Sie an, welche Ressourcen und Mitglieder mit einem Ordner oder Projekt verknüpft sind.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.

2. Auf der Seite **Bearbeiten** können Sie Details zum ausgewählten Ordner oder Projekt anzeigen, indem Sie die Abschnitte **Ressourcen** oder **Zugriff** erweitern.
   - Wählen Sie **Ressourcen** aus, um die zugehörigen Ressourcen anzuzeigen. In der Tabelle identifiziert die Spalte **Status** die Ressourcen, die mit dem Ordner oder Projekt verknüpft sind.



Ändern Sie die Ressourcen, die einem Ordner oder Projekt zugeordnet sind.

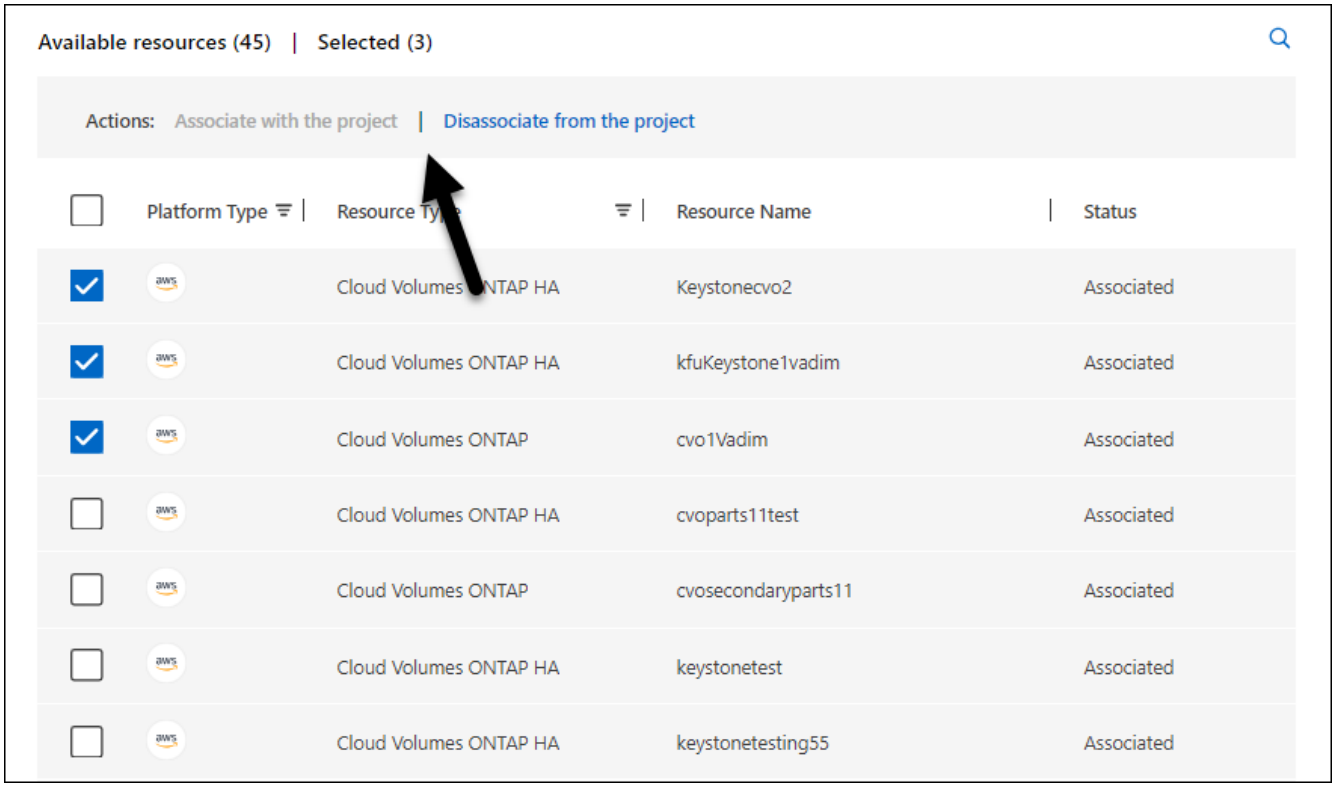
Sie können die einem Ordner oder Projekt zugeordneten Ressourcen ändern, wenn sich die Bedürfnisse Ihrer Organisation ändern.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.
2. Wählen Sie auf der Seite **Bearbeiten Ressourcen** aus.

   In der Tabelle identifiziert die Spalte **Status** die Ressourcen, die mit dem Ordner oder Projekt verknüpft sind.

3. Wählen Sie die Ressourcen aus, die Sie zuordnen oder deren Zuordnung Sie aufheben möchten.
4. Basierend auf den von Ihnen ausgewählten Ressourcen wählen Sie entweder **Dem Projekt zuordnen** oder **Vom Projekt trennen**.



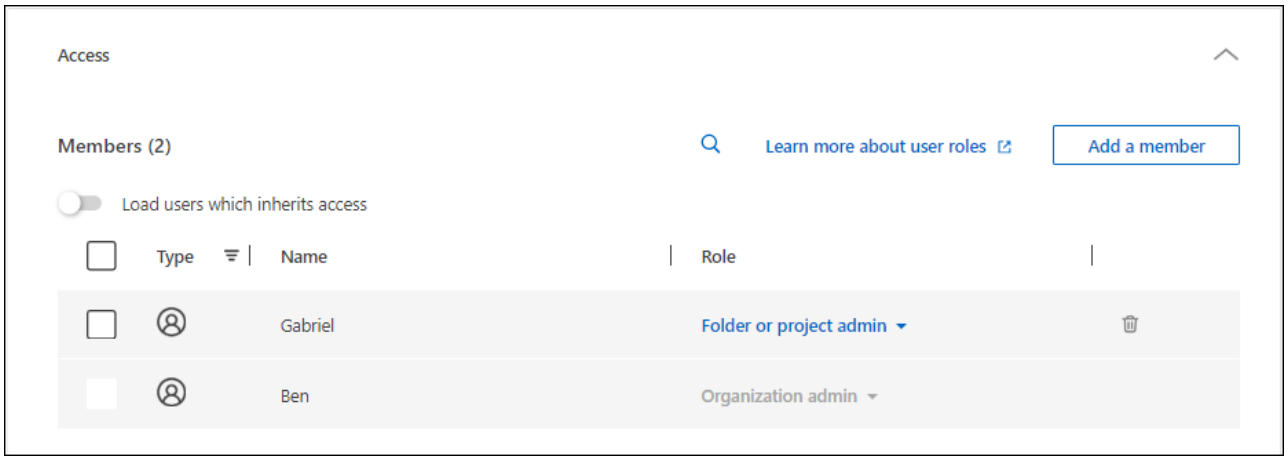
5. Wählen Sie **Übernehmen**.

Anzeigen von Mitgliedern, die einem Ordner oder Projekt zugeordnet sind

Auf der Seite **Organisation** können Sie die Mitglieder anzeigen, die einem Ordner oder Projekt zugeordnet sind.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.
2. Wählen Sie auf der Seite **Bearbeiten Zugriff** aus, um die Liste der Mitglieder anzuzeigen, die Zugriff auf den ausgewählten Ordner oder das ausgewählte Projekt haben.
   - Wählen Sie **Zugriff** aus, um die Mitglieder anzuzeigen, die Zugriff auf den Ordner oder das Projekt haben.



Ändern des Mitgliederzugriffs auf einen Ordner oder ein Projekt

Ändern Sie die Zugriffsrechte der Mitglieder, um den Ressourcenzugriff zu steuern. Beachten Sie, dass Rollen, die auf Ordnerebene zugewiesen werden, an alle untergeordneten Projekte und Ordner vererbt werden.

Die Zugriffsrechte von Mitgliedern auf niedrigeren Ebenen können nicht geändert werden, wenn sie von der Ordner- oder Organisationsebene übernommen wurden. Ändern Sie die Berechtigungen des Mitglieds auf der höheren Hierarchieebene, um den Zugriff zu ändern. Alternativ können Sie "Verwalten Sie Berechtigungen auf der Seite „Mitglieder“"Die

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.
2. Wählen Sie auf der Seite **Bearbeiten Zugriff** aus, um die Liste der Mitglieder anzuzeigen, die Zugriff auf den ausgewählten Ordner oder das ausgewählte Projekt haben.
3. Mitgliederzugriff ändern:
   - **Mitglied hinzufügen**: Wählen Sie das Mitglied aus, das Sie dem Ordner oder Projekt hinzufügen möchten, und weisen Sie ihm eine Rolle zu.
   - **Rolle eines Mitglieds ändern**: Wählen Sie für alle Mitglieder mit einer anderen Rolle als „Organisationsadministrator“ ihre vorhandene Rolle und dann eine neue Rolle aus.
   - **Mitgliederzugriff entfernen**: Sie können den Zugriff von Mitgliedern entfernen, denen für den Ordner oder das Projekt, das Sie gerade anzeigen, eine Rolle definiert ist.
4. Wählen Sie **Übernehmen**.

Ähnliche Informationen

- "Erfahren Sie mehr über Identität und Zugriff in der NetApp Console"
- "Erste Schritte mit Identität und Zugriff"
- "Erfahren Sie mehr über die Identitäts- und Zugriffs-API"

Fügen Sie Ressourcen zu Ordnern und Projekten in der NetApp Console hinzu.

Steuern Sie den Benutzerzugriff auf Ressourcen, indem Sie diese Projekten und Ordnern in Ihrer NetApp Console -Organisation hinzufügen. Benutzern Zugriff auf Projektebene gewähren.

Eine *Ressource* ist eine Entität, die der Konsole bekannt ist, wie beispielsweise eine Speicherressource, ein Konsolenagent oder eine Backup- und Wiederherstellungs-Workload.

Auf der Seite **Ressourcen** in der Konsole können Sie Ressourcen anzeigen und verwalten.

Konsolenressourcentypen

Sie können in Ihrer NetApp Console Organisation verschiedene Ressourcentypen Projekten zuordnen:

Speicherressourcen

Speicherressourcen sind die am häufigsten vorkommende Ressourcenart in Ihrem Unternehmen und umfassen sowohl lokale als auch Cloud-Speichersysteme. Wenn Sie ein Speichersystem zur Konsole hinzufügen, können Sie es einem Ordner oder Projekt hinzufügen. Bis dahin wird es in der Konsole als nicht entdeckt markiert und nicht auf der Seite **Ressourcen** angezeigt.

Konsolenagenten

Wenn Sie einen Console-Agenten zur Erkennung von Speichersystemen verwendet haben, fügen Sie den Agenten demselben Ordner oder Projekt hinzu. Dies ermöglicht es Benutzern, agentenbasierte Funktionen auszuführen, wie z. B. Datendienste oder die native Speicherverwaltung der Konsole. Sie können Agenten über die Seite **Agenten** in der Konsole Ordnern oder Projekten hinzufügen. "Erfahren Sie, wie Sie einen Konsolenagenten mit einem Ordner oder Projekt verknüpfen"Die

Keystone -Abonnements

Wenn Sie in Ihrer Organisation Keystone Abonnements haben, können Sie diese auf der Seite **Ressourcen** einsehen. Sie können Keystone -Abonnements mit Ordnern oder Projekten verknüpfen, um Mitgliedern, die über Berechtigungen für diese Ordner oder Projekte verfügen, Zugriff zu gewähren.

Zeigen Sie die Ressourcen in Ihrer Organisation an

Sie können sowohl entdeckte als auch unentdeckte Ressourcen anzeigen, die mit Ihrer Organisation verknüpft sind. Das System findet Speicherressourcen und markiert sie als nicht entdeckt, bis Sie sie zur Konsole hinzufügen.

> Die Konsole schließt Amazon FSx for NetApp ONTAP Ressourcen von der Ressourcenseite aus, da Benutzer sie keiner Rolle zuordnen können. Sie können diese Ressourcen auf der Seite **Systeme** oder unter Workloads einsehen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Ressourcen** aus.
3. Wählen Sie **Erweiterte Suche und Filterung**.
4. Nutzen Sie die verfügbaren Optionen, um eine Ressource zu finden:
   - **Suche nach Ressourcennamen**: Geben Sie eine Textzeichenfolge ein und wählen Sie **Hinzufügen**.
   - **Plattform**: Wählen Sie eine oder mehrere Plattformen aus, beispielsweise Amazon Web Services.
   - **Ressourcen**: Wählen Sie eine oder mehrere Ressourcen aus, beispielsweise Cloud Volumes ONTAP.
   - **Organisation, Ordner oder Projekt**: Wählen Sie die gesamte Organisation, einen bestimmten Ordner oder ein bestimmtes Projekt aus.
5. Wählen Sie **Suchen**.

Zuordnen einer Ressource zu Ordnern und Projekten

Verknüpfen Sie eine Ressource mit einem Ordner oder Projekt, um sie Mitgliedern zur Verfügung zu stellen, die über Berechtigungen für diesen Ordner oder dieses Projekt verfügen.

Schritte

1. Navigieren Sie auf der Seite **Ressourcen** zu einer Ressource in der Tabelle, wählen Sie ••• und wählen Sie dann **Mit Ordnern oder Projekten verknüpfen**.
2. Wählen Sie einen Ordner oder ein Projekt aus und wählen Sie dann **Akzeptieren**.
3. Um einen zusätzlichen Ordner oder ein zusätzliches Projekt zuzuordnen, wählen Sie **Ordner oder Projekt hinzufügen** und wählen Sie dann den Ordner oder das Projekt aus.

   Beachten Sie, dass Sie nur aus den Ordnern und Projekten auswählen können, für die Sie über Administratorberechtigungen verfügen.

4. Wählen Sie **Ressourcen zuordnen**.
   - Wenn Sie die Ressource mit Projekten verknüpft haben, können Mitglieder, die über Berechtigungen für diese Projekte verfügen, jetzt über die Konsole auf die Ressource zugreifen.
   - Wenn Sie die Ressource mit einem Ordner verknüpft haben, kann ein *Ordner- oder Projektadministrator* jetzt auf die Ressource zugreifen und sie mit einem Projekt innerhalb des Ordners verknüpfen. "Informationen zum Verknüpfen einer Ressource mit einem Ordner"Die

Nach Abschluss

Wenn Sie mithilfe eines Konsolenagenten eine Ressource entdecken, verknüpfen Sie den Konsolenagenten mit dem Projekt, um Zugriff zu gewähren. Andernfalls sind der Konsolenagent und die zugehörige Ressource für Mitglieder ohne die Rolle „Organisationsadministrator“ nicht zugänglich.

"Erfahren Sie, wie Sie einen Konsolenagenten mit einem Ordner oder Projekt verknüpfen".

Anzeigen der mit einer Ressource verknüpften Ordner und Projekte

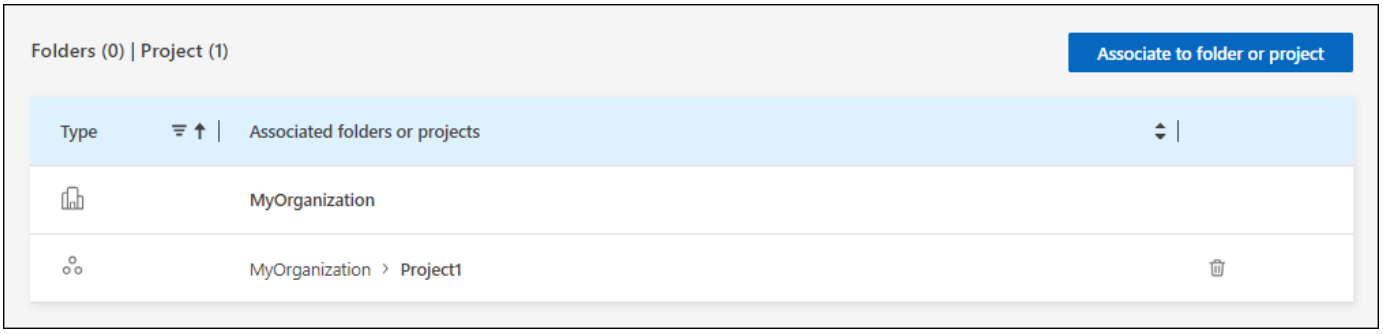
Sie können die Ordner und Projekte anzeigen, die mit einer bestimmten Ressource verknüpft sind.

Wenn Sie herausfinden möchten, welche Organisationsmitglieder Zugriff auf die Ressource haben, können Sie"Zeigen Sie die Mitglieder an, die Zugriff auf die Ordner und Projekte haben, die mit der Ressource verknüpft sind." .

Schritte

1. Navigieren Sie auf der Seite **Ressourcen** zu einer Ressource in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.

Das folgende Beispiel zeigt eine Ressource, die mit einem Projekt verknüpft ist.



Um zu sehen, welche Organisationsmitglieder Zugriff auf die Ressource haben,"Mitglieder mit Zugriff auf zugehörige Ordner und Projekte anzeigen" Die

Entfernen einer Ressource aus einem Ordner oder Projekt

Um eine Ressource aus einem Ordner oder Projekt zu entfernen, muss ihre Zuordnung aufgehoben werden. Dies verhindert, dass Mitglieder die Ressource in diesem Ordner oder Projekt verwalten können.

Um eine gefundene Ressource aus der gesamten Organisation zu entfernen, gehen Sie zur Seite **Systeme** und entfernen Sie das System.

Schritte

1. Navigieren Sie auf der Seite **Ressourcen** zu einer Ressource in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.
2. Um eine Ressource aus einem Ordner oder Projekt zu entfernen, wählen Sie Folgendes aus: 🗑 neben dem Ordner oder Projekt.
3. Wählen Sie **Löschen**, um die Verknüpfung zu entfernen.

Ähnliche Informationen

- "Erfahren Sie mehr über Identität und Zugriff in der NetApp Console"
- "Erste Schritte mit Identität und Zugriff in der NetApp Console"
- "Erfahren Sie mehr über die API für Identität und Zugriff"

Verknüpfen Sie einen Konsolenagenten mit anderen Ordnern und Projekten

Ordnen Sie Console-Agenten spezifischen Projekten zu, um Ressourcenmanagement und Datenzugriff zu ermöglichen. Für Ressourcen, die über einen Console-Agenten gefunden werden, müssen sowohl die Ressource als auch der Agent den gleichen Projekten zugeordnet sein, damit das Team darauf zugreifen kann.

Super-Administratoren und Organisationsadministratoren können Agenten erstellen und jeden Agenten einem beliebigen Projekt oder Ordner zuordnen. Ordner- oder Projektadministratoren können nur vorhandene Agenten Ordnern und Projekten zuordnen, für die sie die entsprechenden Berechtigungen besitzen. "Erfahren Sie mehr über die Aktionen, die ein Ordner- oder Projektadministrator ausführen kann."Die

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff** > **Agenten**.
2. Suchen Sie in der Tabelle den Konsolenagenten, den Sie zuordnen möchten.

   Verwenden Sie die Suche über der Tabelle, um einen bestimmten Konsolenagenten zu finden, oder filtern Sie die Tabelle nach Ressourcenhierarchie.

3. Um die mit dem Konsolenagenten verknüpften Ordner und Projekte anzuzeigen, wählen Sie ••• und wählen Sie dann **Details anzeigen**.

   Auf der Seite werden Details zu den Ordnern und Projekten angezeigt, die mit dem Konsolenagenten verknüpft sind.

4. Wählen Sie **Mit Ordner oder Projekt verknüpfen**.

5. Wählen Sie einen Ordner oder ein Projekt aus und wählen Sie dann **Akzeptieren**.
6. Um den Konsolenagenten mit einem zusätzlichen Ordner oder Projekt zu verknüpfen, wählen Sie **Ordner oder Projekt hinzufügen** und wählen Sie dann den Ordner oder das Projekt aus.
7. Wählen Sie **Associate Agent** aus.

Nach Abschluss

Ordnen Sie die Ressourcen des Konsolenagenten denselben Ordnern und Projekten von der Seite **Ressourcen** zu.

"Erfahren Sie, wie Sie eine Ressource mit Ordnern und Projekten verknüpfen" .

Ähnliche Informationen

- "Erfahren Sie mehr über NetApp Console -Agenten"
- "Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der NetApp Console"
- "Erste Schritte mit Identität und Zugriff"
- "Erfahren Sie mehr über die API für Identitäts- und Zugriffsverwaltung"

Fügen Sie Ihrer Konsolenorganisation Benutzer hinzu.

Fügen Sie Benutzer zu einer NetApp Console Organisation hinzu

Innerhalb der Konsole gewähren Sie Benutzern Zugriff auf Projekte oder Ordner entsprechend einer Zugriffsrolle. Eine Zugriffsrolle enthält eine Reihe von Berechtigungen, die es einem Mitglied (Benutzer oder Dienstkonto) ermöglichen, bestimmte Aktionen auf der zugewiesenen Ebene der Ressourcenhierarchie durchzuführen.

Erforderliche Zugriffsrollen

Super-Admin, Organisations-Admin oder Ordner- bzw. Projekt-Admin (für die von ihnen verwalteten Ordner und Projekte). "Informationen zu Zugriffsrollen"Die

Verstehen Sie, wie der Zugriff in der NetApp Console gewährt wird.

Die NetApp Console verwendet rollenbasierte Zugriffskontrolle (RBAC) zur Verwaltung von Berechtigungen. Weisen Sie Benutzern Rollen einzeln oder über föderierte Gruppen zu. Jede Rolle definiert die zulässigen Aktionen für bestimmte Ressourcen.

Beachten Sie Folgendes bezüglich der Zugriffsgewährung in der NetApp Console:

- Alle Benutzer müssen sich zunächst bei der NetApp Console registrieren, bevor ihnen Zugriff auf Ressourcen gewährt werden kann.
- Sie müssen jedem Benutzer in der Konsole explizit eine Rolle zuweisen, bevor er auf Ressourcen zugreifen kann, selbst wenn er Mitglied einer Verbundgruppe ist, der eine Rolle zugewiesen wurde.
- Sie können Dienstkonten direkt über die Konsole hinzufügen und ihnen Rollen zuweisen.

Fügen Sie Ihrer Organisation Mitglieder hinzu

Die NetApp Console unterstützt drei Arten von Mitgliedern: Benutzerkonten, Dienstkonten und Verbundgruppen.

Benutzer müssen sich bei der NetApp Console registrieren, bevor Sie sie hinzufügen und ihnen eine Rolle zuweisen können, selbst wenn sie Mitglied einer Verbundgruppe sind. Dienstkonten können direkt in der Konsole erstellt werden.

Alle Mitglieder müssen mindestens eine Rolle explizit zugewiesen bekommen haben, um auf Ressourcen zugreifen zu können.

Beim Hinzufügen eines Mitglieds wählen Sie die Ressourcenebene (Organisation, Ordner oder Projekt) und weisen Sie eine oder mehrere Rollen mit den erforderlichen Berechtigungen zu.

Einen Benutzer hinzufügen

Benutzer registrieren sich für die NetApp Console, aber ein Organisationsadministrator, Ordner- oder Projektadministrator muss sie einer Organisation, einem Ordner oder einem Projekt hinzufügen, damit sie auf Ressourcen zugreifen können.

Bevor Sie beginnen:

Der Benutzer muss sich bereits für die NetApp Console registriert haben. Falls sie sich noch nicht angemeldet haben, leiten Sie sie bitte weiter zu "Registrieren Sie sich für die NetApp Console."

> Wenn Sie einen Benutzer hinzufügen, der Teil einer Verbundgruppe ist, stellen Sie sicher, dass sich der Benutzer bereits bei der NetApp Console registriert hat und ihm explizit eine Rolle in der Console zugewiesen wurde. NetApp empfiehlt, eine minimale Zugriffsrolle wie z. B. „Organisationsbetrachter“ zuzuweisen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie **Mitglied hinzufügen**.
4. Behalten Sie für **Mitgliedstyp** die Auswahl von **Benutzer** bei.
5. Geben Sie bei **E-Mail des Benutzers** die E-Mail-Adresse des Benutzers ein, die mit der von ihm erstellten Anmeldung verknüpft ist.
6. Verwenden Sie den Abschnitt **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**, um die Ebene Ihrer Ressourcenhierarchie auszuwählen, für die das Mitglied Berechtigungen haben soll.

   Beachten Sie Folgendes:

   - Sie können nur die Ordner und Projekte auswählen, für die Sie die entsprechenden Berechtigungen besitzen.
   - Wenn Sie eine Organisation oder einen Ordner auswählen, erteilen Sie dem Mitglied Berechtigungen für alle darin enthaltenen Inhalte.
   - Sie können die Rolle **Organisationsadministrator** nur auf Organisationsebene zuweisen.
7. **Wählen Sie eine Kategorie** und dann eine **Rolle** aus, die dem Mitglied Berechtigungen für die Ressourcen erteilt, die mit der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt verknüpft sind.

   "Informationen zu Zugriffsrollen" .
8. Um Zugriff auf weitere Ordner, Projekte oder Rollen zu gewähren, wählen Sie **Rolle hinzufügen**, wählen Sie die Ordner-, Projekt- oder Rollenkategorie und anschließend eine Rolle aus.

9. Wählen Sie **Hinzufügen**.

   Die Konsole sendet dem Benutzer eine E-Mail mit Anweisungen.

Hinzufügen eines Dienstkontos

Dienstkonten ermöglichen die Automatisierung von Aufgaben und die sichere Verbindung mit Console-APIs. Wählen Sie eine Client-ID und ein Client-Geheimnis für einfache Setups oder JWT (JSON Web Token) für eine höhere Sicherheit in automatisierten oder Cloud-nativen Umgebungen. Wählen Sie die Methode, die Ihren Sicherheitsanforderungen entspricht.

Bevor Sie beginnen:

Bereiten Sie für die JWT-Authentifizierung Ihren öffentlichen Schlüssel oder Ihr Zertifikat vor.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie **Mitglied hinzufügen**.
4. Wählen Sie für **Mitgliedstyp Dienstkonto** aus.
5. Geben Sie einen Namen für das Dienstkonto ein.
6. Um die JWT-Authentifizierung zu verwenden, wählen Sie **Private-Key-JWT-Authentifizierung verwenden** und laden Sie Ihren öffentlichen RSA-Schlüssel oder Ihr Zertifikat hoch. Überspringen, falls Client-ID und Client-Geheimnis verwendet werden.

   Ihr X.509-Zertifikat. Es muss im PEM-, CRT- oder CER-Format vorliegen.

   a. Richten Sie Ablaufbenachrichtigungen für Ihr Zertifikat ein. Sie haben die Wahl zwischen sieben Tagen oder 30 Tagen. Ablaufbenachrichtigungen werden per E-Mail versendet und Benutzern mit der Rolle „Super-Admin“ oder „Org-Admin“ in der Konsole angezeigt.
7. Verwenden Sie den Abschnitt **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**, um die Ebene Ihrer Ressourcenhierarchie auszuwählen, für die das Mitglied Berechtigungen haben soll.

   Beachten Sie Folgendes:

   - Sie können nur aus den Ordnern und Projekten auswählen, für die Sie Berechtigungen haben.
   - Durch die Auswahl einer Organisation oder eines Ordners erhält das Mitglied Zugriff auf alle Inhalte.
   - Sie können die Rolle **Organisationsadministrator** nur auf Organisationsebene zuweisen.
8. Wählen Sie eine **Kategorie** und anschließend eine **Rolle** aus, die dem Mitglied Berechtigungen für die Ressourcen in der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt erteilt.

   "Informationen zu Zugriffsrollen" .
9. Um Zugriff auf weitere Ordner, Projekte oder Rollen zu gewähren, wählen Sie **Rolle hinzufügen**, wählen Sie die Ordner-, Projekt- oder Rollenkategorie und anschließend eine Rolle aus.
10. Wenn Sie sich nicht für die Verwendung der JWT-Authentifizierung entschieden haben, laden Sie die Client-ID und das Client-Geheimnis herunter oder kopieren Sie sie.

    Die Konsole zeigt das Client-Geheimnis nur einmal an. Sicher kopieren; falls Sie es verlieren, können Sie es später wiederherstellen.

11. Wenn Sie die JWT-Authentifizierung gewählt haben, laden Sie die Client-ID und die JWT-Zielgruppe herunter oder kopieren Sie sie. Die Konsole zeigt diese Informationen nur einmal an und erlaubt es Ihnen nicht, sie später abzurufen.
12. Wählen Sie **Schließen**.

Fügen Sie Ihrer Organisation eine föderierte Gruppe hinzu.

Sie können eine föderierte Gruppe von Ihrem Identitätsanbieter (IdP) zu Ihrer Organisation hinzufügen und ihr eine oder mehrere Rollen zuweisen. Die Mitglieder der föderierten Gruppe erben die Rollen, die Sie der Gruppe in der Konsole zuweisen.

Bevor Sie einer föderierten Gruppe eine Rolle zuweisen können, stellen Sie Folgendes sicher:

- Richten Sie eine Föderation zwischen Ihrem IdP und der Konsole ein. "Erfahren Sie, wie Sie eine Föderation einrichten."
- Die Gruppe muss bereits in Ihrem Identitätsanbieter existieren und über App-Zugriff auf die Konsole verfügen.
- Benutzer, die dieser Gruppe angehören, müssen sich bereits für die NetApp Console registriert haben und ihnen muss explizit eine Rolle in der Console zugewiesen worden sein. NetApp empfiehlt, eine minimale Zugriffsrolle wie z. B. „Organisationsbetrachter“ zuzuweisen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie **Mitglied hinzufügen**.
4. Wählen Sie unter **Mitgliedstyp** die Option **Verbundgruppe**.
5. Wählen Sie den Verband aus, dem die Gruppe angehört.
6. Geben Sie unter **Gruppenname** den genauen Namen der Gruppe in Ihrem IdP ein.
7. Verwenden Sie den Abschnitt **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**, um die Ebene Ihrer Ressourcenhierarchie auszuwählen, für die das Mitglied Berechtigungen haben soll.

   Beachten Sie Folgendes:

   - Sie können nur aus den Ordnern und Projekten auswählen, für die Sie Berechtigungen haben.
   - Durch die Auswahl einer Organisation oder eines Ordners erhält das Mitglied Zugriff auf alle Inhalte.
   - Sie können die Rolle **Organisationsadministrator** nur auf Organisationsebene zuweisen.
8. Wählen Sie eine **Kategorie** und anschließend eine **Rolle** aus, die dem Mitglied Berechtigungen für die Ressourcen in der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt erteilt.

   "Informationen zu Zugriffsrollen" .
9. Um Zugriff auf weitere Ordner, Projekte oder Rollen zu gewähren, wählen Sie **Rolle hinzufügen**, wählen Sie die Ordner-, Projekt- oder Rollenkategorie und anschließend eine Rolle aus.

Ähnliche Informationen

- "Erfahren Sie mehr über Identitäts- und Zugriffsmanagement in der NetApp Console"
- "Erste Schritte mit Identität und Zugriff"

- "NetApp Console"
- "Erfahren Sie mehr über die API für Identität und Zugriff"

Benutzerzugriff und Sicherheit verwalten

Erfahren Sie mehr über die rollenbasierte Zugriffskontrolle (RBAC) der NetApp Console .

Verwalten Sie den Benutzerzugriff auf die NetApp Console mit rollenbasierter Zugriffskontrolle (RBAC), indem Sie vordefinierte Rollen auf Organisations-, Ordner- oder Projektebene zuweisen. Jede Rolle gewährt spezifische Berechtigungen, die definieren, welche Aktionen Benutzer innerhalb ihres zugewiesenen Bereichs ausführen können.

NetApp entwirft Konsolenrollen nach dem Prinzip der minimalen Berechtigungen, sodass jede Rolle nur die Berechtigungen enthält, die für ihre Aufgaben erforderlich sind. Dieser Ansatz erhöht die Sicherheit, indem der Zugriff auf das beschränkt wird, was jedes Mitglied benötigt.

Nachdem Sie die Ressourcen in Ordnern und Projekten organisiert haben, weisen Sie den Organisationsmitgliedern eine oder mehrere Rollen für bestimmte Ordner oder Projekte zu, die es ihnen ermöglichen, nur ihre jeweiligen Verantwortlichkeiten wahrzunehmen.

Beispielsweise können Sie einem Mitglied die Administratorrolle für Ransomware-Resilienz auf einer bestimmten Projektebene zuweisen, sodass dieses Mitglied Ransomware-Resilienzmaßnahmen für Ressourcen innerhalb dieses Projekts durchführen kann, ohne ihm einen umfassenderen Zugriff auf die gesamte Organisation zu gewähren. Diesem Benutzer kann die Rolle für mehrere Projekte innerhalb Ihrer Organisation zugewiesen werden.

Sie können Benutzern je nach ihren Verantwortlichkeiten mehrere Rollen für denselben oder für verschiedene Verantwortungsbereiche zuweisen. In einer kleineren Organisation könnte beispielsweise ein und derselbe Benutzer sowohl die Aufgaben der Ransomware-Resilienz als auch der Datensicherung und -wiederherstellung auf Organisationsebene verwalten, während in einer größeren Organisation auf Projektebene unterschiedliche Benutzer den einzelnen Rollen zugeordnet sein könnten.

Arten von Konsolenorganisationsmitgliedern

In einer NetApp Console Organisation gibt es drei Arten von Mitgliedern: * *Benutzerkonten*: Einzelne Benutzer, die sich bei der NetApp Console anmelden, um Ressourcen zu verwalten. Benutzer müssen sich bei der NetApp Console registrieren, bevor sie einer Organisation hinzugefügt werden können. * *Servicekonten*: Nicht-menschliche Konten, die von Anwendungen oder Diensten verwendet werden, um über APIs mit der NetApp Console zu interagieren. Sie können Dienstkonten direkt zu Ihrer Konsolenorganisation hinzufügen. * *Verbundene Gruppen*: Gruppen, die von Ihrem Identitätsanbieter (IdP) synchronisiert werden und es Ihnen ermöglichen, den Zugriff für mehrere Benutzer gemeinsam zu verwalten. Jeder Benutzer innerhalb einer föderierten Gruppe muss sich bei der NetApp Console registriert haben und Ihrer Organisation mit einer Zugriffsrolle hinzugefügt worden sein, bevor er auf die der Gruppe zugewiesenen Ressourcen zugreifen kann.

"Erfahren Sie, wie Sie Mitglieder zu Ihrer Organisation hinzufügen."

Vordefinierte Rollen in der NetApp Console

Die NetApp Console enthält vordefinierte Rollen, die Sie Organisationsmitgliedern zuweisen können. Jede Rolle beinhaltet Berechtigungen, die festlegen, welche Aktionen ein Mitglied innerhalb seines zugewiesenen Bereichs (Organisation, Ordner oder Projekt) durchführen kann.

Die NetApp Console -Rollen verwenden das Prinzip der minimalen Berechtigungen, um sicherzustellen, dass

Mitglieder nur über die für ihre Aufgaben erforderlichen Berechtigungen verfügen, und kategorisieren die Rollen nach der Art des Zugriffs, den sie gewähren:

- Plattformrollen: Konsolenadministrationsberechtigungen bereitstellen
- Datendienstrollen: Berechtigungen für die Verwaltung spezifischer Datendienste wie Ransomware-Resilienz und Datensicherung und -wiederherstellung bereitstellen.
- Anwendungsrollen: Berechtigungen für die Speicherverwaltung sowie für die Überwachung von Konsolenereignissen und -warnungen bereitstellen.

Sie können einem Mitglied mehrere Rollen entsprechend seinen Verantwortlichkeiten zuweisen. Beispielsweise könnten Sie einem Mitglied für ein bestimmtes Projekt sowohl die Administratorrolle für Ransomware-Resilienz als auch die Administratorrolle für Datensicherung und -wiederherstellung zuweisen.

"Erfahren Sie mehr über die in der NetApp Console verfügbaren vordefinierten Rollen."Die

Mitgliederzugriffe in der NetApp Console verwalten

Verwalten Sie den Mitgliederzugriff in Ihrer Console-Organisation. Weisen Sie Rollen zu, um Berechtigungen festzulegen. Mitglieder werden entfernt, wenn sie das Unternehmen verlassen.

Erforderliche Zugriffsrollen

Super-Admin, Organisations-Admin oder Ordner- bzw. Projekt-Admin (für die von ihnen verwalteten Ordner und Projekte). Link:reference-iam-predefined-roles.html[Erfahren Sie mehr über Zugriffsrollen].

Sie können Zugriffsrollen projekt- oder ordnerbasiert zuweisen. Weisen Sie beispielsweise einem Benutzer eine Rolle für zwei bestimmte Projekte zu oder weisen Sie die Rolle auf Ordnerebene zu, um einem Benutzer die Administratorrolle für Ransomware-Resilienz für alle Projekte in einem Ordner zu geben.

Fügen Sie Ihre Ordner und Projekte hinzu, bevor Sie Benutzern Zugriffsrechte zuweisen. "Erfahren Sie, wie Sie Ordner und Projekte hinzufügen."

Verstehen Sie, wie der Zugriff in der NetApp Console gewährt wird.

Die NetApp Console verwendet ein rollenbasiertes Zugriffskontrollmodell (RBAC) zur Verwaltung von Benutzerberechtigungen. Sie können Mitgliedern vordefinierte Rollen einzeln oder über föderierte Gruppen zuweisen. Sie können Dienstkonten und Verbundgruppen Rollen hinzufügen und zuweisen. Jede Rolle definiert, welche Aktionen ein Mitglied an den zugehörigen Ressourcen durchführen kann.

Beachten Sie Folgendes bezüglich der Zugriffsgewährung in der NetApp Console:

- Alle Benutzer müssen sich zunächst bei der NetApp Console registrieren, bevor ihnen Zugriff auf Ressourcen gewährt werden kann.
- Sie müssen jedem Benutzer in der Konsole explizit eine Rolle zuweisen, bevor er auf Ressourcen zugreifen kann, selbst wenn er Mitglied einer Verbundgruppe ist, der eine Rolle zugewiesen wurde.
- Sie können Dienstkonten direkt über die Konsole hinzufügen und ihnen Rollen zuweisen.

Verwendung der Rollenvererbung

Wenn Sie in der NetApp Console eine Rolle auf Organisations-, Ordner- oder Projektebene zuweisen, wird diese Rolle automatisch an alle Ressourcen innerhalb des ausgewählten Bereichs vererbt. Beispielsweise gelten Rollen auf Ordnerebene für alle darin enthaltenen Projekte, während Rollen auf Projektebene für alle

Ressourcen innerhalb dieses Projekts gelten.

Organisationsmitglieder anzeigen

Um zu verstehen, welche Ressourcen und Berechtigungen einem Mitglied zur Verfügung stehen, können Sie die dem Mitglied auf verschiedenen Ebenen der Ressourcenhierarchie Ihrer Organisation zugewiesenen Rollen anzeigen."Erfahren Sie, wie Sie mithilfe von Rollen den Zugriff auf Konsolenressourcen steuern."

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.

   In der Tabelle **Mitglieder** sind die Mitglieder Ihrer Organisation aufgelistet.

3. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.

Einem Mitglied zugewiesene Rollen anzeigen

Sie können überprüfen, welche Rollen ihnen aktuell zugewiesen sind.

Wenn Sie die Rolle „Ordner- oder Projektadministrator“ haben, werden auf der Seite alle Mitglieder der Organisation angezeigt. Sie können jedoch nur die Mitgliedsberechtigungen für die Ordner und Projekte anzeigen und verwalten, für die Sie über Berechtigungen verfügen. "Erfahren Sie mehr über die Aktionen, die ein Ordner- oder Projektadministrator ausführen kann." .

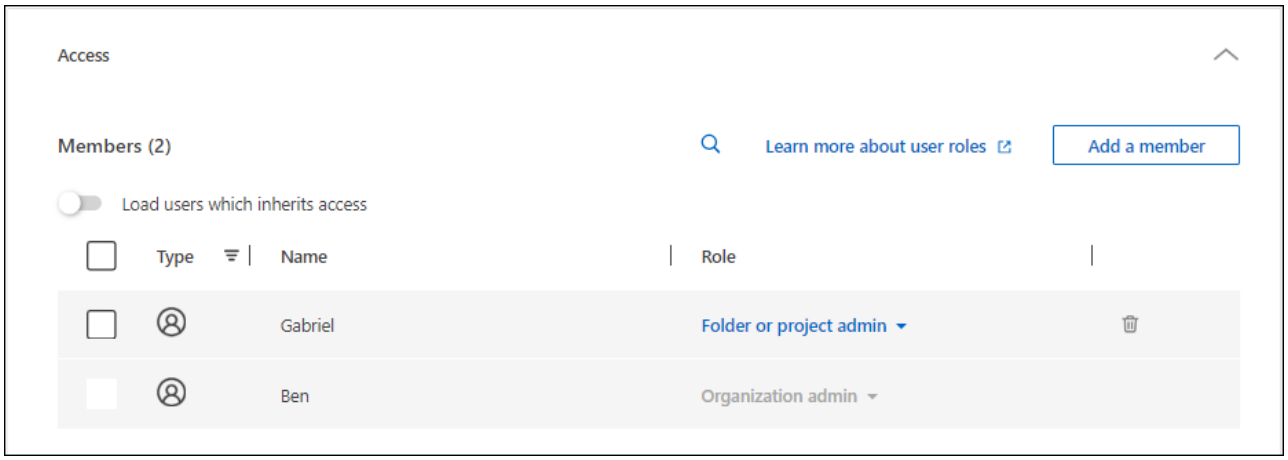
1. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle und wählen Sie es aus. ••• und wählen Sie dann **Details anzeigen**.
2. Erweitern Sie in der Tabelle die jeweilige Zeile für die Organisation, den Ordner oder das Projekt, in dem Sie die zugewiesene Rolle des Mitglieds anzeigen möchten, und wählen Sie in der Spalte **Rolle** die Option **Anzeigen** aus.

Anzeigen von Mitgliedern, die einem Ordner oder Projekt zugeordnet sind

Sie können die Mitglieder anzeigen, die Zugriff auf einen bestimmten Ordner oder ein bestimmtes Projekt haben.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Organisation** aus.
3. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.
   - Wählen Sie **Zugriff** aus, um die Mitglieder anzuzeigen, die Zugriff auf den Ordner oder das Projekt haben.



Mitgliederzugriff zuweisen oder ändern

Nach der Registrierung eines Benutzers bei der NetApp Console können Sie ihn Ihrer Organisation hinzufügen und ihm eine Rolle zuweisen, um ihm Zugriff auf Ressourcen zu gewähren. "Erfahren Sie, wie Sie Mitglieder zu Ihrer Organisation hinzufügen."

Sie können die Zugriffsrechte eines Mitglieds anpassen, indem Sie nach Bedarf Rollen hinzufügen oder entfernen.

Einem Mitglied eine Zugriffsrolle hinzufügen

Normalerweise weisen Sie eine Rolle zu, wenn Sie ein Mitglied zu Ihrer Organisation hinzufügen, Sie können sie jedoch jederzeit aktualisieren, indem Sie Rollen entfernen oder hinzufügen.

Sie können einem Benutzer eine Zugriffsrolle für Ihre Organisation, Ihren Ordner oder Ihr Projekt zuweisen.

Mitglieder können innerhalb desselben Projekts und in verschiedenen Projekten mehrere Rollen innehaben. Kleinere Organisationen weisen beispielsweise alle verfügbaren Zugriffsrollen demselben Benutzer zu, während größere Organisationen ihre Benutzer mit spezialisierteren Aufgaben betrauen. Alternativ könnten Sie auch einem Benutzer die Administratorrolle für Ransomware-Resilienz auf Organisationsebene zuweisen. In diesem Beispiel könnte der Benutzer Ransomware-Resilienzmaßnahmen für alle Projekte innerhalb seiner Organisation durchführen.

Ihre Zugriffsrollenstrategie sollte mit der Art und Weise übereinstimmen, wie Sie Ihre NetApp -Ressourcen organisiert haben.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie einen der Mitglieder-Tabs aus: **Benutzer**, **Dienstkonten** oder **Verbundgruppen**.
4. Wählen Sie das Aktionsmenü ••• neben dem Mitglied, dem Sie eine Rolle zuweisen möchten, und wählen Sie **Rolle hinzufügen** aus.
5. Um eine Rolle hinzuzufügen, führen Sie die Schritte im Dialogfeld aus:
   - **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**: Wählen Sie die Ebene Ihrer Ressourcenhierarchie aus, für die das Mitglied Berechtigungen haben soll.

     Wenn Sie die Organisation oder einen Ordner auswählen, verfügt das Mitglied über Berechtigungen für alles, was sich innerhalb der Organisation oder des Ordners befindet.

- **Kategorie auswählen**: Wählen Sie eine Rollenkategorie. "Informationen zu Zugriffsrollen" .
- Wählen Sie eine **Rolle**: Wählen Sie eine Rolle, die dem Mitglied Berechtigungen für die Ressourcen erteilt, die mit der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt verknüpft sind.
- **Rolle hinzufügen**: Wenn Sie Zugriff auf zusätzliche Ordner oder Projekte innerhalb Ihrer Organisation gewähren möchten, wählen Sie **Rolle hinzufügen**, geben Sie einen weiteren Ordner oder ein weiteres Projekt oder eine weitere Rollenkategorie an und wählen Sie dann eine Rollenkategorie und eine entsprechende Rolle aus.

6. Wählen Sie **Neue Rollen hinzufügen**.

Ändern der einem Mitglied zugewiesenen Rolle

Ändern Sie die Rollen eines Mitglieds, um dessen Zugriffsrechte zu aktualisieren.

> Benutzern muss mindestens eine Rolle zugewiesen sein. Sie können einem Benutzer nicht alle Rollen entziehen. Wenn Sie alle Rollen entfernen müssen, müssen Sie den Benutzer aus Ihrer Organisation löschen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie einen der Mitglieder-Tabs aus: **Benutzer**, **Dienstkonten** oder **Verbundgruppen**.
4. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.
5. Erweitern Sie in der Tabelle die jeweilige Zeile für die Organisation, den Ordner oder das Projekt, in dem Sie die zugewiesene Rolle des Mitglieds ändern möchten, und wählen Sie in der Spalte **Rolle Anzeigen** aus, um die diesem Mitglied zugewiesenen Rollen anzuzeigen.
6. Sie können eine vorhandene Rolle für ein Mitglied ändern oder eine Rolle entfernen.
   a. Um die Rolle eines Mitglieds zu ändern, wählen Sie **Ändern** neben der Rolle, die Sie ändern möchten. Sie können eine Rolle nur in eine Rolle innerhalb derselben Rollenkategorie ändern. Sie können beispielsweise von einer Datendienstrolle zu einer anderen wechseln. Bestätigen Sie die Änderung.
   b. Um die Rolle eines Mitglieds aufzuheben, wählen Sie aus 🗑 neben der Rolle, um die jeweilige Rolle vom Mitglied zu entfernen. Sie werden aufgefordert, die Entfernung zu bestätigen.

Entfernen eines Mitglieds aus Ihrer Organisation

Entfernen Sie ein Mitglied, wenn es Ihre Organisation verlässt.

Wenn Sie ein Mitglied entfernen, entzieht das System ihm die Konsolenberechtigungen, behält aber seine Konsolen- und NetApp -Support-Site-Konten bei.

> **Verbandsmitglieder**
>
> - Verbundbenutzer verlieren automatisch den Zugriff auf die NetApp Console, wenn sie von Ihrem Identitätsanbieter entfernt werden. Sie sollten sie aber trotzdem aus Ihrer Console-Organisation entfernen, um Ihre Mitgliederliste aktuell zu halten.
> - Wenn Sie einen Benutzer aus einer Verbundgruppe in Ihrem Identitätsanbieter entfernen, verliert er den mit dieser Gruppe verbundenen Konsolenzugriff. Sie behalten jedoch weiterhin alle Zugriffsrechte, die mit einer ihnen in der Konsole explizit zugewiesenen Rolle verbunden sind.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie einen der Mitglieder-Tabs aus: **Benutzer**, **Dienstkonten** oder **Verbundgruppen**.
4. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• Wählen Sie dann **Benutzer löschen**.
5. Bestätigen Sie, dass Sie das Mitglied aus Ihrer Organisation entfernen möchten.

Benutzersicherheit

Sichern Sie den Benutzerzugriff auf Ihre NetApp Console -Organisation durch die Verwaltung der Sicherheitseinstellungen der Mitglieder. Sie können Benutzerpasswörter zurücksetzen, die Multi-Faktor-Authentifizierung (MFA) verwalten und die Anmeldeinformationen für Dienstkonten neu erstellen.

Erforderliche Zugriffsrollen

Super-Admin, Organisations-Admin oder Ordner- bzw. Projekt-Admin (für die von ihnen verwalteten Ordner und Projekte). Link:reference-iam-predefined-roles.html[Erfahren Sie mehr über Zugriffsrollen].

Benutzerpasswörter zurücksetzen (nur für lokale Benutzer)

Organisationsadministratoren können die Passwörter lokaler Benutzer nicht zurücksetzen. Sie können die Benutzer jedoch anweisen, ihre Passwörter selbst zurückzusetzen.

Weisen Sie den Benutzer an, sein Passwort auf der Anmeldeseite der Konsole zurückzusetzen, indem er **Passwort vergessen?** auswählt.

Diese Option steht Benutzern in einer föderierten Organisation nicht zur Verfügung.

Verwalten der Multi-Faktor-Authentifizierung (MFA) eines Benutzers

Wenn ein Benutzer den Zugriff auf sein MFA-Gerät verliert, können Sie seine MFA-Konfiguration entweder entfernen oder deaktivieren.

Die Multi-Faktor-Authentifizierung ist nur für lokale Benutzer verfügbar. Verbundbenutzer können MFA nicht aktivieren.

Nach der Deaktivierung müssen die Nutzer die Multi-Faktor-Authentifizierung (MFA) bei der nächsten Anmeldung erneut einrichten. Wenn der Benutzer vorübergehend den Zugriff auf sein MFA-Gerät verliert, kann er sich mit seinem gespeicherten Wiederherstellungscode anmelden.

Wenn sie ihren Wiederherstellungscode nicht haben, deaktivieren Sie MFA vorübergehend, um die Anmeldung zu ermöglichen. Wenn Sie MFA für einen Benutzer deaktivieren, wird es nur für acht Stunden deaktiviert und dann automatisch wieder aktiviert. Dem Benutzer ist während dieser Zeit eine Anmeldung ohne MFA gestattet. Nach Ablauf der acht Stunden muss der Benutzer MFA verwenden, um sich anzumelden.

Um die Multi-Faktor-Authentifizierung eines Benutzers zu verwalten, müssen Sie über eine E-Mail-Adresse in derselben Domäne wie der betroffene Benutzer verfügen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.

   In der Tabelle **Mitglieder** sind die Mitglieder Ihrer Organisation aufgelistet.

3. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Multi-Faktor-Authentifizierung verwalten**.
4. Wählen Sie, ob die MFA-Konfiguration des Benutzers entfernt oder deaktiviert werden soll.

Erstellen Sie die Anmeldeinformationen für ein Dienstkonto neu

Sie können neue Zugangsdaten für einen Dienst erstellen, falls Sie diese verlieren oder aktualisieren müssen.

Durch das Erstellen neuer Anmeldeinformationen werden die alten gelöscht. Die alten Zugangsdaten können nicht verwendet werden.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Navigieren Sie in der Tabelle **Mitglieder** zu einem Dienstkonto, wählen Sie ••• und wählen Sie dann **Geheimnisse neu erstellen**.
4. Wählen Sie **Neu erstellen**.
5. Laden Sie die Client-ID und das Client-Geheimnis herunter oder kopieren Sie sie.

   Die Konsole zeigt das Client-Geheimnis nur einmal an. Stellen Sie sicher, dass Sie die Datei kopieren oder herunterladen und sicher aufbewahren.

NetApp Console

Erfahren Sie mehr über die Zugriffsrollen der NetApp Console

Das Identitäts- und Zugriffsmanagement (IAM) in der NetApp Console bietet vordefinierte Rollen, die Sie den Mitgliedern Ihrer Organisation auf verschiedenen Ebenen Ihrer Ressourcenhierarchie zuweisen können. Bevor Sie diese Rollen zuweisen, sollten Sie sich über die Berechtigungen im Klaren sein, die jede Rolle umfasst. Rollen fallen in die folgenden Kategorien: Plattform, Anwendung und Datendienst.

Plattformrollen

Plattformrollen gewähren Administratorberechtigungen für die NetApp Console , einschließlich Rollenzuweisung und Benutzerverwaltung. Die Konsole hat mehrere Plattformrollen.

Plattformrolle	Aufgaben
"Organisationsadministrator"	Ermöglicht einem Benutzer uneingeschränkten Zugriff auf alle Projekte und Ordner innerhalb einer Organisation, das Hinzufügen von Mitgliedern zu Projekten oder Ordnern sowie das Ausführen beliebiger Aufgaben und die Verwendung beliebiger Datendienste, denen keine explizite Rolle zugeordnet ist. Benutzer mit dieser Rolle verwalten Ihre Organisation, indem sie Ordner und Projekte erstellen, Rollen zuweisen, Benutzer hinzufügen und Systeme verwalten, wenn sie über die entsprechenden Anmeldeinformationen verfügen. Dies ist die einzige Zugriffsrolle, die Konsolenagenten erstellen kann.
"Ordner- oder Projektadministrator"	Ermöglicht einem Benutzer uneingeschränkten Zugriff auf zugewiesene Projekte und Ordner. Kann Mitglieder zu Ordnern oder Projekten hinzufügen, die sie verwalten, sowie beliebige Aufgaben ausführen und beliebige Datendienste oder Anwendungen auf Ressourcen innerhalb des ihnen zugewiesenen Ordners oder Projekts verwenden. Ordner- oder Projektadministratoren können keine Konsolenagenten erstellen.
"Föderationsadministrator"	Ermöglicht einem Benutzer das Erstellen und Verwalten von Föderationen mit der Konsole, wodurch Single Sign-On (SSO) ermöglicht wird.
"Föderationsbetrachter"	Ermöglicht einem Benutzer, vorhandene Föderationen mit der Konsole anzuzeigen. Föderationen können nicht erstellt oder verwaltet werden.
"Partnerschaftsadministrator"	Ermöglicht einem Benutzer, Partnerschaften zu erstellen und zu verwalten.
"Partnerschafts-Viewer"	Ermöglicht einem Benutzer, bestehende Partnerschaften anzuzeigen. Partnerschaften können nicht erstellt oder verwaltet werden.
"Super-Admin"	Gibt dem Benutzer eine Teilmenge von Administratorrollen. Diese Rolle ist für kleinere Organisationen gedacht, die die Konsolenverantwortlichkeiten möglicherweise nicht auf mehrere Benutzer verteilen müssen.
"Super Viewer"	Gibt dem Benutzer eine Teilmenge der Viewer-Rollen. Diese Rolle ist für kleinere Organisationen gedacht, die die Konsolenverantwortlichkeiten möglicherweise nicht auf mehrere Benutzer verteilen müssen.

Anwendungsrollen

Nachfolgend finden Sie eine Liste der Rollen in der Anwendungskategorie. Jede Rolle gewährt innerhalb ihres festgelegten Umfangs spezifische Berechtigungen. Benutzer ohne die erforderliche Anwendungs- oder Plattformrolle können nicht auf die jeweilige Anwendung zugreifen.

Anwendungsrolle	Aufgaben
"Google Cloud NetApp Volumes Administrator"	Benutzer mit der Rolle „Google Cloud NetApp Volumes“ können Google Cloud NetApp Volumes erkennen und verwalten.
"Google Cloud NetApp Volumes Viewer"	Benutzer mit der Benutzerrolle „Google Cloud NetApp Volumes“ können Google Cloud NetApp Volumes anzeigen.

Anwendungsrolle	Aufgaben
"Keystone -Administrator"	Benutzer mit der Keystone Administratorrolle können Serviceanfragen erstellen. Ermöglicht Benutzern, Nutzung, Ressourcen und Administratordetails innerhalb des Keystone Mandanten, auf den sie zugreifen, zu überwachen und anzuzeigen.
"Keystone -Viewer"	Benutzer mit der Keystone Viewer-Rolle KÖNNEN KEINE Serviceanfragen erstellen. Ermöglicht Benutzern die Überwachung und Anzeige von Verbrauch, Anlagen und Verwaltungsinformationen innerhalb des Keystone Mandanten, auf den sie zugreifen.
ONTAP Mediator-Setup-Rolle	Dienstkonten mit der Setup-Rolle „ONTAP Mediator“ können Dienstanfragen erstellen. Diese Rolle ist in einem Dienstkonto erforderlich, um eine Instanz des"ONTAP Cloud Mediator" .
"Betriebsunterstützungsanalyst"	Bietet Zugriff auf Warn- und Überwachungstools und die Möglichkeit, Supportfälle einzugeben und zu verwalten.
"Speicheradministrator"	Verwalten Sie Speicherintegritäts- und Governance-Funktionen, ermitteln Sie Speicherressourcen und ändern und löschen Sie vorhandene Systeme.
"Speicheranzeige"	Zeigen Sie Speicherintegrität und Governance-Funktionen an und zeigen Sie zuvor erkannte Speicherressourcen an. Vorhandene Speichersysteme können nicht erkannt, geändert oder gelöscht werden.
"Systemintegritätsspezialist"	Verwalten Sie Speicher-, Integritäts- und Governance-Funktionen. Alle Berechtigungen des Speicheradministrators sind zulässig, außer dass er vorhandene Systeme nicht ändern oder löschen kann.

Datendienstrollen

Nachfolgend finden Sie eine Liste der Rollen in der Kategorie Datendienste. Jede Rolle gewährt innerhalb ihres festgelegten Umfangs spezifische Berechtigungen. Benutzer, die nicht über die erforderliche Datendienstrolle oder Plattformrolle verfügen, können nicht auf den Datendienst zugreifen.

Datendienstrolle	Aufgaben
"Superadministrator für Backup und Wiederherstellung"	Führen Sie beliebige Aktionen in NetApp Backup and Recovery durch.
"Backup- und Wiederherstellungsadministrator"	Führen Sie Sicherungen auf lokalen Snapshots durch, replizieren Sie auf sekundären Speicher und sichern Sie auf Objektspeicher.
"Administrator für die Wiederherstellung von Backup und Wiederherstellung"	Stellen Sie Workloads in Backup und Recovery wieder her.
"Backup- und Wiederherstellungsklon-Administrator"	Klonen Sie Anwendungen und Daten in der Sicherung und Wiederherstellung.
"Backup- und Wiederherstellungs-Viewer"	Informationen zur Sicherung und Wiederherstellung anzeigen.
"Disaster Recovery-Administrator"	Führen Sie alle Aktionen im NetApp Disaster Recovery -Dienst aus.

Datendienstrolle	Aufgaben
"Disaster Recovery-Failover-Administrator"	Führen Sie Failover und Migrationen durch.
"Disaster Recovery-Anwendungsadministrator"	Erstellen Sie Replikationspläne, ändern Sie Replikationspläne und starten Sie Test-Failover.
"Disaster Recovery-Viewer"	Nur Informationen anzeigen.
Klassifizierungsanzeige	Ermöglicht Benutzern das Anzeigen der Scanergebnisse der NetApp Data Classification . Benutzer mit dieser Rolle können Compliance-Informationen anzeigen und Berichte für Ressourcen erstellen, auf die sie Zugriffsberechtigung haben. Diese Benutzer können das Scannen von Volumes, Buckets oder Datenbankschemata weder aktivieren noch deaktivieren. Die Klassifizierung hat keine Administratorrolle.
"Ransomware-Resilienz-Administrator"	Verwalten Sie Aktionen auf den Registerkarten „Schützen“, „Warnungen“, „Wiederherstellen“, „Einstellungen“ und „Berichte“ von NetApp Ransomware Resilience.
"Ransomware Resilience-Viewer"	Zeigen Sie Arbeitslastdaten und Warndaten an, laden Sie Wiederherstellungsdaten herunter und laden Sie Berichte in Ransomware Resilience herunter.
"Ransomware Resilience-Benutzerverhaltensadministrator"	Konfigurieren, verwalten und zeigen Sie die Erkennung, Warnungen und Überwachung verdächtigen Benutzerverhaltens in Ransomware Resilience an.
"Ransomware Resilience-Benutzerverhaltensanzeige"	Zeigen Sie Warnungen und Einblicke zu verdächtigem Benutzerverhalten in Ransomware Resilience an.
SnapCenter -Administrator	Bietet die Möglichkeit, Snapshots von lokalen ONTAP Clustern mithilfe von NetApp Backup and Recovery für Anwendungen zu sichern. Ein Mitglied mit dieser Rolle kann die folgenden Aktionen ausführen: * Alle Aktionen unter „Sicherung und Wiederherstellung > Anwendungen“ ausführen * Alle Systeme in den Projekten und Ordnern verwalten, für die es Berechtigungen hat * Alle NetApp Console verwenden SnapCenter hat keine Viewer-Rolle.

Weiterführende Links

- "Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der NetApp Console"
- "Erste Schritte mit NetApp Console IAM"
- "Verwalten Sie NetApp Console Mitglieder und ihre Berechtigungen"
- "Erfahren Sie mehr über die API für NetApp Console IAM"

Plattformzugriffsrollen für die NetApp Console

Weisen Sie Benutzern Plattformrollen zu, um ihnen Berechtigungen zum Verwalten der NetApp Console, zum Zuweisen von Rollen, zum Hinzufügen von Benutzern, zum Erstellen von Konsolenagenten und zum Verwalten von Föderationen zu erteilen.

Beispiel für Organisationsrollen für eine große multinationale Organisation

Die XYZ Corporation organisiert den Datenspeicherzugriff nach Regionen – Nordamerika, Europa und Asien-Pazifik – und bietet regionale Kontrolle mit zentraler Aufsicht.

Der **Organisationsadministrator** in der Konsole der XYZ Corporation erstellt eine anfängliche Organisation und separate Ordner für jede Region. Der **Ordner- oder Projektadministrator** für jede Region organisiert Projekte (mit zugehörigen Ressourcen) innerhalb des Ordners der Region.

Regionale Administratoren mit der Rolle **Ordner- oder Projektadministrator** verwalten ihre Ordner aktiv, indem sie Ressourcen und Benutzer hinzufügen. Diese regionalen Administratoren können auch von ihnen verwaltete Ordner und Projekte hinzufügen, entfernen oder umbenennen. Der **Organisationsadministrator** erbt Berechtigungen für alle neuen Ressourcen und behält so die Übersicht über die Speichernutzung in der gesamten Organisation.

Innerhalb derselben Organisation wird einem Benutzer die Rolle **Föderationsadministrator** zugewiesen, um die Föderation der Organisation mit ihrem Unternehmens-IdP zu verwalten. Dieser Benutzer kann föderierte Organisationen hinzufügen oder entfernen, kann jedoch keine Benutzer oder Ressourcen innerhalb der Organisation verwalten. Der **Organisationsadministrator** weist einem Benutzer die Rolle **Föderationsbetrachter** zu, um den Föderationsstatus zu überprüfen und föderierte Organisationen anzuzeigen.

Die folgenden Tabellen zeigen die Aktionen, die jede Konsolenplattformrolle ausführen kann.

Rollen in der Organisationsverwaltung

Aufgabe	Organisationsadministrator	Ordner- oder Projektadministrator
Agenten erstellen	Ja	Nein
Erstellen, Ändern oder Löschen von Systemen über die Konsole (Hinzufügen oder Erkennen von Systemen)	Ja	Ja
Erstellen von Ordnern und Projekten, einschließlich Löschen	Ja	Nein
Vorhandene Ordner und Projekte umbenennen	Ja	Ja
Rollen zuweisen und Benutzer hinzufügen	Ja	Ja
Ressourcen mit Ordnern und Projekten verknüpfen	Ja	Ja
Agenten Ordnern und Projekten zuordnen	Ja	Nein
Agenten aus Ordnern und Projekten entfernen	Ja	Nein
Agenten verwalten (Zertifikate, Einstellungen usw. bearbeiten)	Ja	Nein
Verwalten Sie Anmeldeinformationen unter „Verwaltung > Anmeldeinformationen“.	Ja	Ja
Erstellen, Verwalten und Anzeigen von Föderationen	Ja	Nein
Registrieren Sie sich für den Support und reichen Sie Fälle über die Konsole ein	Ja	Ja
Verwenden Sie Datendienste, die keiner expliziten Zugriffsrolle zugeordnet sind	Ja	Ja
Anzeigen der Audit-Seite und Benachrichtigungen	Ja	Ja

Föderationsrollen

Aufgabe	Föderationsadministrator	Föderationsbetrachter
Erstellen einer Föderation	Ja	Nein
Verifizieren einer Domäne	Ja	Nein
Hinzufügen einer Domäne zu einem Verbund	Ja	Nein
Deaktivieren und Löschen von Föderationen	Ja	Nein
Testverbände	Ja	Nein
Verbände und deren Details anzeigen	Ja	Ja

Partnerschaftsrollen

Aufgabe	Partnerschaftsadministrator	Partnerschafts-Viewer
Kann eine Partnerschaft schaffen	Ja	Nein
Zuweisen von Rollen zu Partnermitgliedern	Ja	Nein
Kann Mitglieder zu einer Partnerschaft hinzufügen	Ja	Nein
Kann Details zur Organisationspartnerschaft anzeigen	Ja	Ja

Superadministrator- und Viewer-Rollen

Die Rolle **Superadministrator** bietet vollständigen Zugriff auf die Verwaltung von Konsolenfunktionen, Speicher und Datendiensten. Diese Rolle eignet sich für Personen, die für die Verwaltung und Governance zuständig sind. Im Gegensatz dazu bietet die Rolle „Super Viewer“ schreibgeschützten Zugriff, ideal für Prüfer oder Stakeholder, die Einblick benötigen, ohne Änderungen vorzunehmen.

Organisationen sollten den **Superadministrator**-Zugriff sparsam verwenden, um Sicherheitsrisiken zu minimieren und das Prinzip der geringsten Privilegien einzuhalten. Die meisten Organisationen sollten fein abgestufte Rollen mit nur den erforderlichen Berechtigungen zuweisen, um das Risiko zu verringern und die Überprüfbarkeit zu verbessern.

Beispiel für Superrollen

ABC Corporation verfügt über ein kleines fünfköpfiges Team, das die NetApp Console für Datendienste und Speicherverwaltung nutzt. Anstatt mehrere Rollen zu verteilen, weisen sie die Rolle des **Superadministrators** zwei leitenden Teammitgliedern zu, die alle Verwaltungsaufgaben übernehmen, einschließlich Benutzerverwaltung und Ressourcenkonfiguration. Den übrigen drei Teammitgliedern wird die Rolle „Super Viewer“ zugewiesen, die es ihnen ermöglicht, die Speicherintegrität und den Status des Datendienstes zu überwachen, ohne die Möglichkeit zu haben, Einstellungen zu ändern.

Rolle	Geerbte Rollen
Super-Admin	• Organisationsadministrator • Ordner- oder Projektadministrator • Föderationsadministrator • Partnerschaftsadministrator • Ransomware-Resilienz-Administrator • Notfallwiederherstellungsadministrator • Backup-Superadministrator • Speicheradministrator • Keystone -Administrator • Google Cloud NetApp Volumes Administrator
Super Viewer	• Organisationsanzeige • Föderationsbetrachter • Partnerschafts-Viewer • Ransomware Resilience-Viewer • Disaster Recovery-Viewer • Backup-Viewer • Speicheranzeige • Keystone -Viewer • Google Cloud NetApp Volumes Viewer

Anwendungsrollen

Google Cloud NetApp Volumes -Rollen in der NetApp Console

Sie können Benutzern die folgende Rolle zuweisen, um ihnen Zugriff auf die Google Cloud NetApp Volumes in der NetApp Console zu gewähren.

Google Cloud NetApp Volumes verwendet die folgende Rolle:

- * Google Cloud NetApp Volumes Administrator*: Entdecken und verwalten Sie Google Cloud NetApp Volumes in der Konsole.
- * Google Cloud NetApp Volumes Viewer*: Google Cloud NetApp Volumes in der Konsole anzeigen.

Keystone -Zugriffsrollen in der NetApp Console

Keystone -Rollen bieten Zugriff auf die Keystone Dashboards und ermöglichen Benutzern das Anzeigen und Verwalten ihres Keystone Abonnements. Es gibt zwei Keystone -Rollen: Keystone -Administrator und Keystone Viewer. Der Hauptunterschied zwischen den beiden Rollen besteht in den Aktionen, die sie in Keystone ausführen können. Die Keystone Administratorrolle ist die einzige Rolle, die Serviceanfragen erstellen oder Abonnements ändern darf.

Beispiel für Keystone -Rollen in der NetApp Console

Bei der XYZ Corporation sind vier Speicheringenieure aus verschiedenen Abteilungen damit beschäftigt, die Keystone Abonnementinformationen anzuzeigen. Obwohl alle diese Benutzer das Keystone Abonnement überwachen müssen, darf nur der Teamleiter Serviceanfragen stellen. Drei Teammitglieder erhalten die Rolle „Keystone -Viewer“, während der Teamleiter die Rolle „Keystone Administrator“ erhält, sodass es einen Kontrollpunkt für die Serviceanfragen des Unternehmens gibt.

Die folgende Tabelle zeigt die Aktionen, die jede Keystone -Rolle ausführen kann.

Funktion und Aktion	Keystone -Administrator	Keystone -Viewer
Zeigen Sie die folgenden Registerkarten an: Abonnement, Assets, Monitor und Verwaltung	Ja	Ja
* Keystone -Abonnementseite*:		
Abonnements anzeigen	Ja	Ja
Abonnements ändern oder verlängern	Ja	Nein
* Keystone -Asset-Seite*:		
Assets anzeigen	Ja	Ja
Verwalten von Assets	Ja	Nein
* Keystone -Warnseite*:		
Warnungen anzeigen	Ja	Ja
Verwalten von Warnungen	Ja	Nein
Erstellen Sie Benachrichtigungen für sich selbst	Ja	Ja
* Licenses and subscriptions*:		
Kann Lizenzen und Abonnements anzeigen	Ja	Ja
* Keystone -Berichtsseite*:		
Berichte herunterladen	Ja	Ja

Funktion und Aktion	Keystone -Administrator	Keystone -Viewer
Berichte verwalten	Ja	Ja
Berichte für sich selbst erstellen	Ja	Ja
Serviceanfragen:		
Serviceanfragen erstellen	Ja	Nein
Zeigen Sie Serviceanfragen an, die von einem beliebigen Benutzer innerhalb der Organisation erstellt wurden	Ja	Ja

Zugriffsrolle „Operational Support Analyst“ für die NetApp Console

Sie können Benutzern die Rolle des Operational Support Analyst zuweisen, um ihnen Zugriff auf Warnmeldungen und Überwachungsfunktionen zu gewähren. Benutzer mit dieser Rolle können auch Supportfälle eröffnen.

Analyst für operative Unterstützung

Aufgabe	Kann durchführen
Verwalten Sie Ihre eigenen Benutzeranmeldeinformationen unter „Einstellungen > Anmeldeinformationen“.	Ja
Erkannte Ressourcen anzeigen	Ja
Registrieren Sie sich für den Support und reichen Sie Fälle über die Konsole ein	Ja
Anzeigen der Audit-Seite und Benachrichtigungen	Ja
Anzeigen, Herunterladen und Konfigurieren von Warnungen	Ja

Speicherzugriffsrollen für die NetApp Console

Sie können Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf die Speicherverwaltungsfunktionen in der NetApp Console zu gewähren. Sie können Benutzern eine Administratorrolle zum Verwalten des Speichers oder eine Viewer-Rolle zum Überwachen zuweisen.

Diese Rollen sind über die NetApp Console Partnerschafts-API nicht verfügbar.

Administratoren können Benutzern Speicherrollen für die folgenden Speicherressourcen und -funktionen zuweisen:

Speicherressourcen:

- On-Premises- ONTAP -Cluster
- StorageGRID
- E-Series

Konsolendienste und -funktionen:

- Digitaler Berater
- Software-Updates
- Lebenszyklusplanung
- Nachhaltigkeit

Beispiel für Speicherrollen in der NetApp Console

XYZ Corporation, ein multinationales Unternehmen, verfügt über ein großes Team von Speicheringenieuren und Speicheradministratoren. Sie ermöglichen diesem Team die Verwaltung von Speicherressourcen für ihre Regionen und beschränken gleichzeitig den Zugriff auf zentrale Konsolenaufgaben wie Benutzerverwaltung, Agentenerstellung und Lizenzverwaltung.

Innerhalb eines 12-köpfigen Teams erhalten zwei Benutzer die Rolle „Speicherbetrachter“, die es ihnen ermöglicht, die Speicherressourcen zu überwachen, die mit den ihnen zugewiesenen Konsolenprojekten verknüpft sind. Den restlichen neun wird die Rolle „Storage-Admin“ zugewiesen, die die Möglichkeit umfasst, Software-Updates zu verwalten, über die Konsole auf ONTAP System Manager zuzugreifen und Speicherressourcen zu ermitteln (Systeme hinzuzufügen). Einer Person im Team wird die Rolle „Systemintegritätsspezialist“ zugewiesen, damit sie die Integrität der Speicherressourcen in ihrer Region verwalten, aber keine Systeme ändern oder löschen kann. Diese Person kann auch Software-Updates auf den Speicherressourcen für die ihr zugewiesenen Projekte durchführen.

Die Organisation verfügt über zwei weitere Benutzer mit der Rolle **Organisationsadministrator**, die alle Aspekte der Konsole verwalten können, einschließlich Benutzerverwaltung, Agentenerstellung und Lizenzverwaltung, sowie mehrere Benutzer mit der Rolle **Ordner- oder Projektadministrator**, die Konsolenverwaltungsaufgaben für die ihnen zugewiesenen Ordner und Projekte ausführen können.

Die folgende Tabelle zeigt die Aktionen, die jede Speicherrolle ausführt.

Funktion und Aktion	Speicheradministrator	Systemintegritätsspezialist	Speicheranzeige
Speicherverwaltung:			
Neue Ressourcen entdecken (Systeme erstellen)	Ja	Ja	Nein
Erkannte Systeme anzeigen	Ja	Ja	Nein
Systeme aus der Konsole löschen	Ja	Nein	Nein
Systeme ändern	Ja	Nein	Nein
Agenten erstellen	Nein	Nein	Nein
Digitaler Berater			

Funktion und Aktion	Speicheradministrator	Systemintegritätsspezialist	Speicheranzeige
Alle Seiten und Funktionen anzeigen	Ja	Ja	Ja
* Licenses and subscriptions*			
Alle Seiten und Funktionen anzeigen	Nein	Nein	Nein
Software-Updates			
Zielseite und Empfehlungen anzeigen	Ja	Ja	Ja
Überprüfen Sie mögliche Versionsempfehlungen und Hauptvorteile	Ja	Ja	Ja
Anzeigen von Updatedetails für einen Cluster	Ja	Ja	Ja
Führen Sie vor dem Update Prüfungen durch und laden Sie den Upgrade-Plan herunter	Ja	Ja	Ja
Installieren Sie Softwareupdates	Ja	Ja	Nein
Lebenszyklusplanung			
Überprüfen des Kapazitätsplanungsstatus	Ja	Ja	Ja
Nächste Aktion auswählen (Best Practice, Stufe)	Ja	Nein	Nein
Verteilen Sie kalte Daten in den Cloud-Speicher und geben Sie Speicherplatz frei	Ja	Ja	Nein
Erinnerungen einrichten	Ja	Ja	Ja
Nachhaltigkeit			
Dashboard und Empfehlungen anzeigen	Ja	Ja	Ja
Berichtsdaten herunterladen	Ja	Ja	Ja
Prozentsatz der CO2-Minderung bearbeiten	Ja	Ja	Nein
Empfehlungen zur Fehlerbehebung	Ja	Ja	Nein
Empfehlungen aufschieben	Ja	Ja	Nein
Systemmanager-Zugriff			
Darf Anmeldeinformationen eingeben	Ja	Ja	Nein

Funktion und Aktion	Speicheradministrator	Systemintegritätsspezialist	Speicheranzeige
Referenzen			
Benutzeranmeldeinformationen	Ja	Ja	Nein

Datendienstrollen

NetApp Backup and Recovery -Rollen in der NetApp Console

Sie können Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf NetApp Backup and Recovery innerhalb der Konsole zu gewähren. Mithilfe von Sicherungs- und Wiederherstellungsrollen können Sie Benutzern flexibel eine Rolle zuweisen, die speziell auf die Aufgaben zugeschnitten ist, die sie in Ihrem Unternehmen erledigen müssen. Wie Sie Rollen zuweisen, hängt von Ihren eigenen Geschäfts- und Speicherverwaltungspraktiken ab.

Der Dienst verwendet die folgenden Rollen, die spezifisch für NetApp Backup and Recovery sind.

- **Superadministrator für Backup und Wiederherstellung**: Führen Sie beliebige Aktionen in NetApp Backup and Recovery aus.
- **Backup- und Recovery-Backup-Administrator**: Führen Sie Sicherungen auf lokalen Snapshots durch, replizieren Sie auf sekundären Speicher und sichern Sie Aktionen auf Objektspeicher in NetApp Backup and Recovery.
- **Backup- und Recovery-Wiederherstellungsadministrator**: Stellen Sie Workloads mit NetApp Backup and Recovery wieder her.
- **Backup- und Recovery-Klonadministrator**: Klonen Sie Anwendungen und Daten mit NetApp Backup and Recovery.
- **Backup- und Recovery-Viewer**: Informationen in NetApp Backup and Recovery anzeigen, aber keine Aktionen ausführen.

Einzelheiten zu allen NetApp Console finden Sie unter "die Dokumentation zur Einrichtung und Verwaltung der Konsole" .

Für allgemeine Aktionen verwendete Rollen

Die folgende Tabelle zeigt die Aktionen, die jede NetApp Backup and Recovery -Rolle für alle Workloads ausführen kann.

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungsklon-Administrator	Backup- und Wiederherstellungs-Viewer
Hosts hinzufügen, bearbeiten oder löschen	Ja	Nein	Nein	Nein	Nein

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungsklon-Administrator	Backup- und Wiederherstellungs-Viewer
Plugins installieren	Ja	Nein	Nein	Nein	Nein
Anmeldeinformationen hinzufügen (Host, Instanz, vCenter)	Ja	Nein	Nein	Nein	Nein
Dashboard und alle Registerkarten anzeigen	Ja	Ja	Ja	Ja	Ja
Kostenlose Testversion starten	Ja	Nein	Nein	Nein	Nein
Ermittlung von Workloads initiieren	Nein	Ja	Ja	Ja	Nein
Lizenzinformationen anzeigen	Ja	Ja	Ja	Ja	Ja
Lizenz aktivieren	Ja	Nein	Nein	Nein	Nein
Hosts anzeigen	Ja	Ja	Ja	Ja	Ja
Zeitpläne:					
Zeitpläne aktivieren	Ja	Ja	Ja	Ja	Nein
Zeitpläne aussetzen	Ja	Ja	Ja	Ja	Nein
Richtlinien und Schutz:					
Schutzpläne anzeigen	Ja	Ja	Ja	Ja	Ja
Erstellen, Ändern oder Löschen von Schutzplänen	Ja	Ja	Nein	Nein	Nein
Wiederherstellen von Workloads	Ja	Nein	Ja	Nein	Nein
Erstellen, Teilen oder Löschen von Klonen	Ja	Nein	Nein	Ja	Nein
Richtlinie erstellen, ändern oder löschen	Ja	Ja	Nein	Nein	Nein
Berichte:					

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungsklon-Administrator	Backup- und Wiederherstellungs-Viewer
Berichte anzeigen	Ja	Ja	Ja	Ja	Ja
Erstellen von Berichten	Ja	Ja	Ja	Ja	Nein
Berichte löschen	Ja	Nein	Nein	Nein	Nein
Von SnapCenter importieren und Host verwalten:					
Importierte SnapCenter -Daten anzeigen	Ja	Ja	Ja	Ja	Ja
Daten aus SnapCenter importieren	Ja	Ja	Nein	Nein	Nein
Host verwalten (migrieren)	Ja	Ja	Nein	Nein	Nein
Einstellungen konfigurieren:					
Konfigurieren des Protokollverzeichnisses	Ja	Ja	Ja	Nein	Nein
Instanzanmeldeinformationen zuordnen oder entfernen	Ja	Ja	Ja	Nein	Nein
Eimer:					
Buckets anzeigen	Ja	Ja	Ja	Ja	Ja
Bucket erstellen, bearbeiten oder löschen	Ja	Ja	Nein	Nein	Nein

Für Workload-spezifische Aktionen verwendete Rollen

Die folgende Tabelle zeigt die Aktionen, die jede NetApp Backup and Recovery -Rolle für bestimmte Workloads ausführen kann.

Kubernetes-Workloads

Diese Tabelle zeigt die Aktionen, die jede NetApp Backup and Recovery -Rolle für Aktionen ausführen kann, die spezifisch für Kubernetes-Workloads sind.

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungs-Viewer
Cluster, Namespaces, Speicherklassen und API-Ressourcen anzeigen	Ja	Ja	Ja	Ja
Neue Kubernetes-Cluster hinzufügen	Ja	Ja	Nein	Nein
Aktualisieren von Clusterkonfigurationen	Ja	Nein	Nein	Nein
Entfernen von Clustern aus der Verwaltung	Ja	Nein	Nein	Nein
Anwendungen anzeigen	Ja	Ja	Ja	Ja
Erstellen und Definieren neuer Anwendungen	Ja	Ja	Nein	Nein
Aktualisieren von Anwendungskonfigurationen	Ja	Ja	Nein	Nein
Entfernen von Anwendungen aus der Verwaltung	Ja	Ja	Nein	Nein
Anzeigen geschützter Ressourcen und Sicherungsstatus	Ja	Ja	Ja	Ja
Erstellen Sie Backups und schützen Sie Anwendungen mit Richtlinien	Ja	Ja	Nein	Nein
Schutz von Apps aufheben und Backups löschen	Ja	Ja	Nein	Nein
Anzeigen von Wiederherstellungspunkten und Ressourcen-Viewer-Ergebnissen	Ja	Ja	Ja	Ja
Wiederherstellen von Anwendungen aus Wiederherstellungspunkten	Ja	Nein	Ja	Nein

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungs-Viewer
Kubernetes-Sicherungsrichtlinien anzeigen	Ja	Ja	Ja	Ja
Erstellen von Kubernetes-Sicherungsrichtlinien	Ja	Ja	Ja	Nein
Aktualisieren der Sicherungsrichtlinien	Ja	Ja	Ja	Nein
Löschen von Sicherungsrichtlinien	Ja	Ja	Ja	Nein
Ausführungs-Hooks und Hook-Quellen anzeigen	Ja	Ja	Ja	Ja
Erstellen Sie Ausführungs-Hooks und Hook-Quellen	Ja	Ja	Ja	Nein
Aktualisieren von Ausführungs-Hooks und Hook-Quellen	Ja	Ja	Ja	Nein
Ausführungs-Hooks und Hook-Quellen löschen	Ja	Ja	Ja	Nein
Vorlagen für Ausführungs-Hooks anzeigen	Ja	Ja	Ja	Ja
Erstellen von Ausführungs-Hook-Vorlagen	Ja	Ja	Ja	Nein
Aktualisieren von Ausführungs-Hook-Vorlagen	Ja	Ja	Ja	Nein
Ausführungs-Hook-Vorlagen löschen	Ja	Ja	Ja	Nein
Übersicht über die Arbeitslast und Analyse-Dashboards anzeigen	Ja	Ja	Ja	Ja
StorageGRID -Buckets und Speicherziele anzeigen	Ja	Ja	Ja	Ja

NetApp Disaster Recovery Rollen in der NetApp Console

Sie können Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf NetApp Disaster Recovery innerhalb der Konsole zu gewähren. Mithilfe von Disaster Recovery-Rollen können Sie Benutzern flexibel Rollen zuweisen, die speziell auf die Aufgaben zugeschnitten sind, die sie in Ihrer Organisation erledigen müssen. Wie Sie Rollen zuweisen, hängt von Ihren eigenen Geschäfts- und Speicherverwaltungspraktiken ab.

Disaster Recovery verwendet die folgenden Rollen:

- **Notfallwiederherstellungsadministrator**: Führen Sie alle Aktionen aus.
- **Disaster Recovery Failover-Administrator**: Führen Sie Failover und Migrationen durch.
- **Administrator der Notfallwiederherstellungsanwendung**: Erstellen Sie Replikationspläne. Replikationspläne ändern. Starten Sie Test-Failover.
- **Disaster Recovery Viewer**: Nur Informationen anzeigen.

Die folgende Tabelle zeigt die Aktionen, die jede Rolle ausführen kann.

Funktion und Aktion	Notfallwiederherstellungsadministrator	Administrator für Notfallwiederherstellungs-Failover	Administrator der Notfallwiederherstellungsanwendung	Disaster Recovery-Viewer
Dashboard und alle Registerkarten anzeigen	Ja	Ja	Ja	Ja
Kostenlose Testversion starten	Ja	Nein	Nein	Nein
Ermittlung von Workloads initiieren	Ja	Nein	Nein	Nein
Lizenzinformationen anzeigen	Ja	Ja	Ja	Ja
Lizenz aktivieren	Ja	Nein	Ja	Nein
Auf der Registerkarte „Sites“:				
Websites anzeigen	Ja	Ja	Ja	Ja
Hinzufügen, Ändern oder Löschen von Sites	Ja	Nein	Nein	Nein
Auf der Registerkarte Replikationspläne:				
Replikationspläne anzeigen	Ja	Ja	Ja	Ja
Anzeigen von Replikationsplandetails	Ja	Ja	Ja	Ja
Erstellen oder Ändern von Replikationsplänen	Ja	Ja	Ja	Nein

Funktion und Aktion	Notfallwiederherstellungsadministrator	Administrator für Notfallwiederherstellungs-Failover	Administrator der Notfallwiederherstellungsanwendung	Disaster Recovery-Viewer
Erstellen von Berichten	Ja	Nein	Nein	Nein
Snapshots anzeigen	Ja	Ja	Ja	Ja
Durchführen von Failover-Tests	Ja	Ja	Ja	Nein
Durchführen von Failovers	Ja	Ja	Nein	Nein
Failbacks durchführen	Ja	Ja	Nein	Nein
Migrationen durchführen	Ja	Ja	Nein	Nein
Auf der Registerkarte „Ressourcengruppen“:				
Anzeigen von Ressourcengruppen	Ja	Ja	Ja	Ja
Erstellen, Ändern oder Löschen von Ressourcengruppen	Ja	Nein	Ja	Nein
Auf der Registerkarte „Jobüberwachung“:				
Jobs anzeigen	Ja	Nein	Ja	Ja
Aufträge abbrechen	Ja	Ja	Ja	Nein

Ransomware Resilience-Zugriffsrollen für die NetApp Console

Ransomware Resilience-Rollen bieten Benutzern Zugriff auf NetApp Ransomware Resilience. Ransomware Resilience unterstützt die folgenden Rollen:

Basisrollen

- Ransomware-Resilience-Administrator – Konfigurieren Sie die Ransomware-Resilience-Einstellungen; untersuchen Sie Verschlüsselungswarnungen und reagieren Sie darauf.
- Ransomware Resilience Viewer – Anzeigen von Verschlüsselungsvorfällen, Berichten und Erkennungseinstellungen

Aktivitätsrollen für Benutzerverhalten"Erkennung verdächtiger Benutzeraktivitäten" Warnungen bieten Einblick in Daten wie Dateiaktivitätsereignisse. Diese Warnungen umfassen Dateinamen und vom Benutzer ausgeführte Dateiaktionen (wie Lesen, Schreiben, Löschen, Umbenennen). Um die Sichtbarkeit dieser Daten einzuschränken, können nur Benutzer mit diesen Rollen diese Warnungen verwalten oder anzeigen.

- Ransomware Resilience-Benutzerverhaltensadministrator – Aktivieren Sie die Erkennung verdächtiger Benutzeraktivitäten, untersuchen Sie verdächtige Benutzeraktivitäten und reagieren Sie auf Warnungen zu verdächtigen Benutzeraktivitäten

- Ransomware Resilience-Benutzerverhaltensanzeige – Anzeigen von Warnungen zu verdächtigen Benutzeraktivitäten

> Benutzerverhaltensrollen sind keine eigenständigen Rollen. Sie sind dafür vorgesehen, den Administrator- oder Viewer-Rollen von Ransomware Resilience hinzugefügt zu werden. Weitere Informationen finden Sie unter Benutzerverhaltensrollen.

Ausführliche Beschreibungen der einzelnen Rollen finden Sie in den folgenden Tabellen.

Basisrollen

In der folgenden Tabelle werden die Aktionen beschrieben, die den Administrator- und Viewer-Rollen von Ransomware Resilience zur Verfügung stehen.

Funktion und Aktion	Ransomware-Resilienz-Administrator	Ransomware Resilience-Viewer
Dashboard und alle Registerkarten anzeigen	Ja	Ja
Aktualisieren Sie den Empfehlungsstatus auf dem Dashboard	Ja	Nein
Kostenlose Testversion starten	Ja	Nein
Ermittlung von Workloads initiieren	Ja	Nein
Neuermittlung von Workloads einleiten	Ja	Nein
Auf der Registerkarte „Schützen“:		
Hinzufügen, Ändern oder Löschen von Schutzplänen für _Verschlüsselungs_richtlinien	Ja	Nein
Workloads schützen	Ja	Nein
Identifizieren Sie die Gefährdung sensibler Daten mit der Datenklassifizierung	Ja	Nein
Listen Sie Schutzpläne und Details auf	Ja	Ja
Auflisten von Schutzgruppen	Ja	Ja
Anzeigen von Schutzgruppendetails	Ja	Ja
Erstellen, Bearbeiten oder Löschen von Schutzgruppen	Ja	Nein
Daten herunterladen	Ja	Ja
Auf der Registerkarte „Warnungen“:		
Anzeigen von Verschlüsselungswarnungen und Warnungsdetails	Ja	Ja

Funktion und Aktion	Ransomware-Resilienz-Administrator	Ransomware Resilience-Viewer
Verschlüsselungsvorfallstatus bearbeiten	Ja	Nein
Verschlüsselungsalarm zur Wiederherstellung markieren	Ja	Nein
Details zum Verschlüsselungsvorfall anzeigen	Ja	Ja
Verschlüsselungsvorfälle verwerfen oder beheben	Ja	Nein
Vollständige Liste der betroffenen Dateien im Verschlüsselungsereignis abrufen	Ja	Nein
Daten zu Verschlüsselungsereigniswarnungen herunterladen	Ja	Ja
Benutzer blockieren (mit Workload Security-Agent-Konfiguration)	Ja	Nein
Auf der Registerkarte „Wiederherstellen“:		
Herunterladen der betroffenen Dateien vom Verschlüsselungsereignis	Ja	Nein
Workload nach Verschlüsselungsereignis wiederherstellen	Ja	Nein
Wiederherstellungsdaten aus dem Verschlüsselungsereignis herunterladen	Ja	Ja
Laden Sie Berichte vom Verschlüsselungsereignis herunter	Ja	Ja
Auf der Registerkarte „Einstellungen“:		
Hinzufügen oder Ändern von Sicherungszielen	Ja	Nein
Auflisten der Sicherungsziele	Ja	Ja
Verbundene SIEM-Ziele anzeigen	Ja	Ja
SIEM-Ziele hinzufügen oder ändern	Ja	Nein
Bereitschaftsübung konfigurieren	Ja	Nein
Bereitschaftsübung starten, zurücksetzen oder bearbeiten	Ja	Nein
Status der Bereitschaftsübung überprüfen	Ja	Ja
Aktualisieren der Erkennungskonfiguration	Ja	Nein

Funktion und Aktion	Ransomware-Resilienz-Administrator	Ransomware Resilience-Viewer
Anzeigen der Erkennungskonfiguration	Ja	Ja
Auf der Registerkarte „Berichte“:		
Berichte herunterladen	Ja	Ja

Benutzerverhaltensrollen

Um Einstellungen für verdächtiges Benutzerverhalten zu konfigurieren und auf Warnungen zu reagieren, muss ein Benutzer über die Administratorrolle „Ransomware Resilience-Benutzerverhalten“ verfügen. Um nur Warnungen zu verdächtigem Benutzerverhalten anzuzeigen, sollte ein Benutzer über die Rolle „Ransomware Resilience-Benutzerverhaltensanzeiger“ verfügen.

Benutzerverhaltensrollen sollten Benutzern mit vorhandenen Ransomware Resilience-Administrator- oder Viewer-Berechtigungen zugewiesen werden, die Zugriff auf Folgendes benötigen:"Einstellungen und Warnungen bei verdächtigen Benutzeraktivitäten" . Ein Benutzer mit der Administratorrolle „Ransomware Resilience“ sollte beispielsweise die Administratorrolle „Ransomware Resilience-Benutzerverhalten“ erhalten, um Benutzeraktivitäts-Agenten zu konfigurieren und Benutzer zu sperren oder die Sperrung aufzuheben. Die Administratorrolle für das Benutzerverhalten von Ransomware Resilience sollte keinem Ransomware Resilience-Viewer übertragen werden.

Um die Erkennung verdächtiger Benutzeraktivitäten zu aktivieren, müssen Sie über die Administratorrolle der Konsolenorganisation verfügen.

In der folgenden Tabelle werden die Aktionen beschrieben, die für die Administrator- und Viewer-Rollen des Benutzerverhaltens von Ransomware Resilience verfügbar sind.

Funktion und Aktion	Ransomware Resilience-Benutzerverhaltensadministrator	Ransomware Resilience-Benutzerverhaltensanzeige
Auf der Registerkarte „Einstellungen“:		
Erstellen, Ändern oder Löschen eines Benutzeraktivitätsagenten	Ja	Nein
Benutzerverzeichnis-Connector erstellen oder löschen	Ja	Nein
Datensammler anhalten oder fortsetzen	Ja	Nein
Führen Sie eine Übung zur Vorbereitung auf Datenschutzverletzungen durch	Ja	Nein
Auf der Registerkarte „Schützen“:		
Hinzufügen, Ändern oder Löschen von Schutzplänen für Richtlinien zu *verdächtigem Benutzerverhalten*	Ja	Nein
Auf der Registerkarte „Warnungen“:		
Anzeigen von Benutzeraktivitätswarnungen und Warnungsdetails	Ja	Ja

Funktion und Aktion	Ransomware Resilience-Benutzerverhaltensadministrator	Ransomware Resilience-Benutzerverhaltensanzeige
Bearbeiten des Vorfallstatus für Benutzeraktivitäten	Ja	Nein
Benutzeraktivitätswarnung zur Wiederherstellung markieren	Ja	Nein
Details zum Vorfall mit Benutzeraktivität anzeigen	Ja	Ja
Abweisen oder Lösen von Vorfällen im Zusammenhang mit Benutzeraktivitäten	Ja	Nein
Vollständige Liste der betroffenen Dateien nach verdächtigem Benutzer abrufen	Ja	Ja
Laden Sie Ereigniswarnungsdaten zu Benutzeraktivitäten herunter	Ja	Ja
Benutzer blockieren oder entsperren	Ja	Nein
Auf der Registerkarte „Wiederherstellen“:		
Herunterladen betroffener Dateien für Benutzeraktivitätsereignisse	Ja	Nein
Wiederherstellen der Arbeitslast aus dem Benutzeraktivitätsereignis	Ja	Nein
Laden Sie Wiederherstellungsdaten aus dem Benutzeraktivitätsereignis herunter	Ja	Ja
Laden Sie Berichte zum Benutzeraktivitätsereignis herunter	Ja	Ja

Identitäts- und Zugriffs-API

Organisations- und Projekt-IDs

Ihre NetApp Console Konsolenorganisation hat einen Namen und eine ID. Sie können einen Namen für Ihre Organisation auswählen, um sie leichter zu identifizieren. Möglicherweise müssen Sie für bestimmte Integrationen auch die Organisations-ID abrufen.

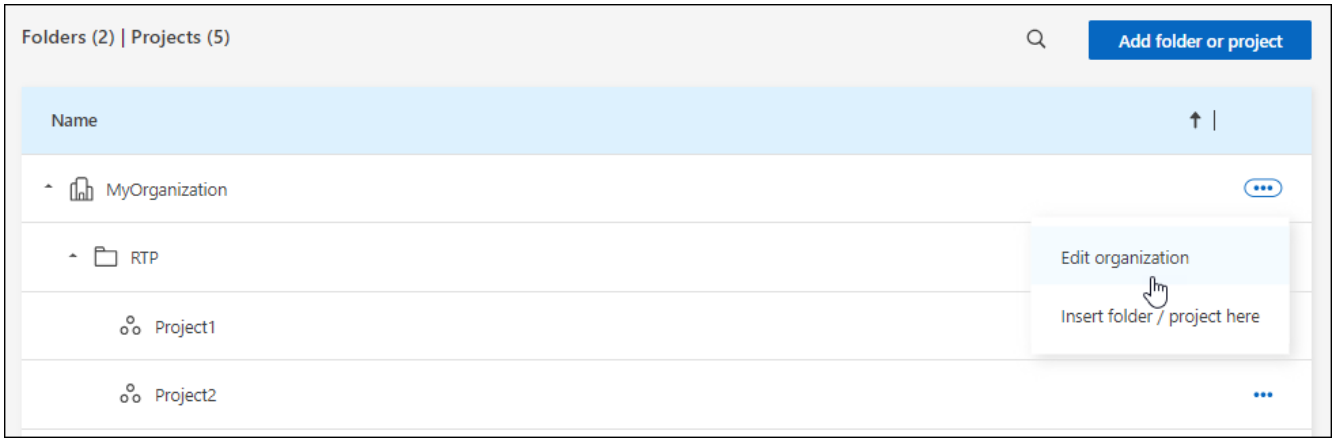
Benennen Sie Ihre Organisation um

Sie können Ihre Organisation umbenennen. Dies ist hilfreich, wenn Sie mehr als nur die Organisation unterstützen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Organisation** aus.
3. Navigieren Sie auf der Seite **Organisation** zur ersten Zeile in der Tabelle und wählen Sie ••• und wählen

Sie dann **Organisation bearbeiten**.



4. Geben Sie einen neuen Organisationsnamen ein und wählen Sie **Übernehmen**.

Abrufen der Organisations-ID

Die Organisations-ID wird für bestimmte Integrationen mit der Konsole verwendet.

Sie können die Organisations-ID auf der Seite „Organisationen“ anzeigen und sie für Ihren Bedarf in die Zwischenablage kopieren.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff** > **Organisation**.
2. Suchen Sie auf der Seite **Organisation** in der Übersichtsleiste nach Ihrer Organisations-ID und kopieren Sie sie in die Zwischenablage. Sie können dies zur späteren Verwendung speichern oder direkt dorthin kopieren, wo Sie es benötigen.

Abrufen der ID für ein Projekt

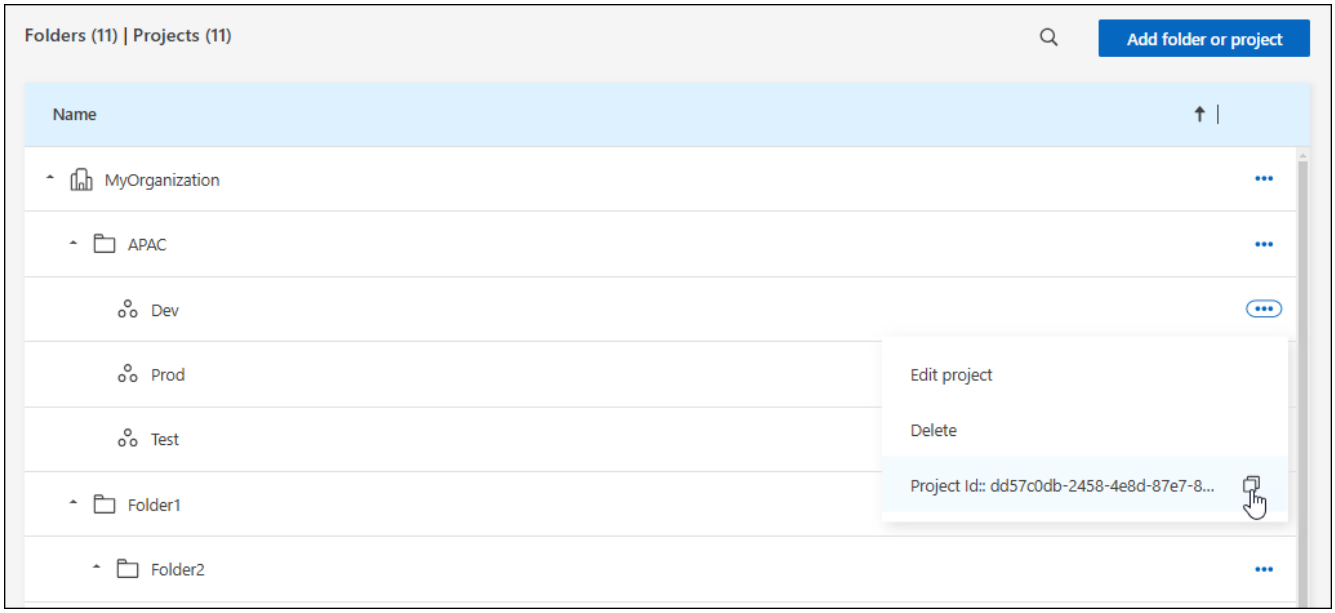
Sie müssen die ID für ein Projekt abrufen, wenn Sie die API verwenden. Beispielsweise beim Erstellen eines Cloud Volumes ONTAP -Systems.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt in der Tabelle und wählen Sie •••

   Die Projekt-ID wird angezeigt.

2. Um die ID zu kopieren, wählen Sie die Schaltfläche „Kopieren“.



Ähnliche Informationen

- "Erfahren Sie mehr über Identitäts- und Zugriffsverwaltung"
- "Erste Schritte mit Identität und Zugriff"
- "Erfahren Sie mehr über die API für Identität und Zugriff"

Sicherheit und Compliance

Identitätsföderation

Aktivieren Sie Single Sign-On durch die Verwendung der Identitätsföderation mit der NetApp Console

Single-Sign-On (Föderation) vereinfacht den Anmeldevorgang und erhöht die Sicherheit, indem Benutzer sich mit ihren Unternehmensanmeldeinformationen bei der NetApp Console anmelden können. Sie können Single Sign-On (SSO) bei Ihrem Identitätsanbieter (IdP) oder über die NetApp Support-Site aktivieren.

Erforderliche Rolle

Organisationsadministrator, Föderationsadministrator, Föderationsbetrachter."Erfahren Sie mehr über Zugriffsrollen."

Einmaliges Anmelden mit NetApp Support Site

Durch die Verbindung mit der NetApp -Support-Site können sich Benutzer mit denselben Anmeldeinformationen bei der Konsole, Active IQ Digital Advisor und anderen zugehörigen Apps anmelden.

Wenn Sie eine Verbindung mit der NetApp -Support-Site herstellen, können Sie nicht gleichzeitig eine Verbindung mit Ihrem Corporate Identity Management-Anbieter herstellen. Wählen Sie die Option aus, die für Ihr Unternehmen am besten geeignet ist.

Schritte

1. Laden Sie die "NetApp Federation-Antragsformular" .

2. Senden Sie das Formular an die im Formular angegebene E-Mail-Adresse.

   Das NetApp Supportteam prüft und bearbeitet Ihre Anfrage.

Einmaliges Anmelden mit Ihrem Identitätsanbieter

Sie können eine Verbundverbindung mit Ihrem Identitätsanbieter einrichten, um Single Sign-On (SSO) für die Konsole zu aktivieren. Der Vorgang umfasst die Konfiguration Ihres Identitätsanbieters, sodass dieser NetApp als Dienstanbieter vertraut, und die anschließende Herstellung der Verbindung in der Konsole.

Wenn Sie die Föderation zuvor mit NetApp Cloud Central (einer externen Anwendung der Konsole) konfiguriert haben, müssen Sie Ihre Föderation über die Föderationsseite importieren, um sie in der Konsole zu verwalten."Erfahren Sie, wie Sie Ihre Föderation importieren."

Unterstützte Identitätsanbieter

NetApp unterstützt die folgenden Protokolle und Identitätsanbieter für die Föderation:

Protokolle

- Security Assertion Markup Language (SAML)-Identitätsanbieter
- Active Directory-Verbunddienste (AD FS)

Identitätsanbieter

- Microsoft Entra ID
- PingFederate

Föderation mit NetApp Console -Workflow

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in der Konsole eine Verbindung erstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Föderation mit Ihrer E-Mail-Domäne oder mit einer anderen Domäne, die Ihnen gehört, herstellen. Um eine Föderation mit einer anderen Domäne als Ihrer E-Mail-Domäne herzustellen, bestätigen Sie zunächst, dass Sie der Eigentümer der Domäne sind.

Bestätigen Sie Ihre Domäne (wenn Sie nicht Ihre E-Mail-Domäne verwenden)

Um eine Föderation mit einer anderen Domäne als Ihrer E-Mail-Domäne herzustellen, bestätigen Sie, dass Sie deren Eigentümer sind. Sie können Ihre E-Mail-Domäne ohne zusätzliche Schritte föderieren.

Konfigurieren Sie Ihren IdP so, dass er NetApp als Serviceprovider vertraut

Konfigurieren Sie Ihren Identitätsanbieter so, dass er NetApp vertraut, indem Sie eine neue Anwendung erstellen und Details wie die ACS-URL, die Entitäts-ID oder andere Anmeldeinformationen angeben. Die Informationen zum Dienstanbieter variieren je nach Identitätsanbieter. Weitere Informationen finden Sie in der Dokumentation Ihres spezifischen Identitätsanbieters. Sie müssen mit Ihrem IdP-Administrator zusammenarbeiten, um diesen Schritt abzuschließen.

3 Erstellen Sie die Verbundverbindung in der Konsole

Geben Sie die SAML-Metadaten-URL oder -Datei von Ihrem Identitätsanbieter an, um die Verbindung herzustellen. Diese Informationen werden verwendet, um die Vertrauensbeziehung zwischen der Konsole und Ihrem Identitätsanbieter herzustellen. Die von Ihnen bereitgestellten Informationen hängen von dem von Ihnen verwendeten IdP ab. Wenn Sie beispielsweise die Microsoft Entra ID verwenden, müssen Sie die Client-ID, das Geheimnis und die Domäne angeben.

4 Testen Sie Ihre Föderation in der Konsole

Testen Sie Ihre Verbundverbindung, bevor Sie sie aktivieren. Verwenden Sie die Testoption auf der Seite „Föderation“ in der Konsole, um zu überprüfen, ob sich Ihr Testbenutzer erfolgreich authentifizieren kann. Wenn der Test erfolgreich ist, können Sie die Verbindung aktivieren.

5 Aktivieren Sie Ihre Verbindung in der Konsole

Nachdem Sie die Verbindung aktiviert haben, können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden.

Lesen Sie zunächst das Thema für Ihr jeweiliges Protokoll oder Ihren IdP:

- "Einrichten einer Verbundverbindung mit AD FS"
- "Einrichten einer Verbundverbindung mit der Microsoft Entra ID"
- "Einrichten einer Verbundverbindung mit PingFederate"
- "Einrichten einer Verbundverbindung mit einem SAML-Identitätsanbieter"

Domänenüberprüfung

Überprüfen Sie die E-Mail-Domäne für Ihre Verbundverbindung

Wenn Sie eine Föderation mit einer Domäne durchführen möchten, die sich von Ihrer E-Mail-Domäne unterscheidet, müssen Sie zunächst bestätigen, dass Sie der Eigentümer der Domäne sind. Sie können für die Föderation nur verifizierte Domänen verwenden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Zur Überprüfung Ihrer Domäne müssen Sie den DNS-Einstellungen Ihrer Domäne einen TXT-Eintrag hinzufügen. Dieser Datensatz dient als Nachweis dafür, dass Sie der Eigentümer der Domäne sind, und ermöglicht der NetApp Console, der Domäne für die Föderation zu vertrauen. Möglicherweise müssen Sie sich mit Ihrem IT- oder Netzwerkadministrator abstimmen, um diesen Schritt abzuschließen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Wählen Sie **Domänenbesitz bestätigen**.

5. Geben Sie die Domäne ein, die Sie verifizieren möchten, und wählen Sie **Weiter**.
6. Kopieren Sie den bereitgestellten TXT-Eintrag.
7. Gehen Sie zu den DNS-Einstellungen Ihrer Domäne und konfigurieren Sie den TXT-Wert, der als TXT-Eintrag für Ihre Domäne bereitgestellt wurde. Arbeiten Sie bei Bedarf mit Ihrem IT- oder Netzwerkadministrator zusammen.
8. Nachdem der TXT-Eintrag hinzugefügt wurde, kehren Sie zur Konsole zurück und wählen Sie **Überprüfen**.

Konfigurieren von Föderationen

Verbinden Sie die NetApp Console mit Active Directory Federation Services (AD FS).

Verbinden Sie Ihre Active Directory Federation Services (AD FS) mit der NetApp Console , um Single Sign-On (SSO) für die NetApp Console zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen."Erfahren Sie mehr über Zugriffsrollen."

> Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. NetApp empfiehlt, sich für das eine oder das andere zu entscheiden, aber nicht für beides.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Konfigurieren Sie zunächst den Identitätsanbieter so, dass er der NetApp Console als Dienstanbieter vertraut. Erstellen Sie dann mithilfe der Konfiguration Ihres Identitätsanbieters eine Verbindung in der Konsole.

Sie können eine Föderation mit Ihrem AD FS-Server einrichten, um Single Sign-On (SSO) für die NetApp Console zu aktivieren. Der Vorgang umfasst die Konfiguration Ihres AD FS, sodass es der Konsole als Dienstanbieter vertraut, und die anschließende Herstellung der Verbindung in der NetApp Console.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Geben Sie Ihre Domänendetails ein:
   a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
   b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
   c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
5. Wählen Sie **Weiter**.
6. Wählen Sie als Verbindungsmethode **Protokoll** und dann **Active Directory Federation Services (AD FS)**.
7. Wählen Sie **Weiter**.
8. Erstellen Sie eine Vertrauensstellung der vertrauenden Seite auf Ihrem AD FS-Server. Sie können PowerShell verwenden oder es manuell auf Ihrem AD FS-Server konfigurieren. Weitere Informationen zum Erstellen einer Vertrauensstellung der vertrauenden Seite finden Sie in der AD FS-Dokumentation.

a. Erstellen Sie die Vertrauensstellung mithilfe von PowerShell und dem folgenden Skript:

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

b. Alternativ können Sie die Vertrauensstellung manuell in der AD FS-Verwaltungskonsole erstellen. Verwenden Sie beim Erstellen der Vertrauensstellung die folgenden NetApp Console :

- Verwenden Sie beim Erstellen der Relying Trust Identifier den Wert **YOUR_TENANT**: `netapp-cloud-account`
- Wenn Sie **Unterstützung für WS-Federation aktivieren** auswählen, verwenden Sie den Wert **YOUR_AUTH0_DOMAIN**: `netapp-cloud-account.auth0.com`

c. Kopieren Sie nach dem Erstellen der Vertrauensstellung die Metadaten-URL von Ihrem AD FS-Server oder laden Sie die Verbundmetadatendatei herunter. Sie benötigen diese URL oder Datei, um die Verbindung in der Konsole herzustellen.

NetApp empfiehlt die Verwendung der Metadaten-URL, damit die NetApp Console automatisch die neueste AD FS-Konfiguration abrufen kann. Wenn Sie die Federation-Metadatendatei herunterladen, müssen Sie sie bei jeder Änderung Ihrer AD FS-Konfiguration manuell in der NetApp Console aktualisieren.

9. Kehren Sie zur Konsole zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.
10. Stellen Sie die Verbindung mit AD FS her.
    a. Geben Sie die **AD FS-URL** ein, die Sie im vorherigen Schritt von Ihrem AD FS-Server kopiert haben, oder laden Sie die Verbundmetadatendatei hoch, die Sie von Ihrem AD FS-Server heruntergeladen haben.
11. Wählen Sie **Verbindung erstellen**. Das Herstellen der Verbindung kann einige Sekunden dauern.
12. Wählen Sie **Weiter**.
13. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zu einer Anmeldeseite für Ihren IdP-Server weitergeleitet. Melden Sie sich mit Ihren IdP-Zugangsdaten an. Nach dem Einloggen müssen Sie zur Konsole zurückkehren, um die Verbindung zu aktivieren.

> ⓘ Wenn Sie die Konsole im eingeschränkten Modus verwenden, kopieren Sie die URL entweder in ein Inkognito-Browserfenster oder in einen separaten Browser, um sich bei Ihrem Identitätsanbieter anzumelden.

14. Wählen Sie in der Konsole **Weiter**, um die Zusammenfassungsseite anzuzeigen.
15. Benachrichtigungen einrichten.

    Sie haben die Wahl zwischen sieben Tagen oder 30 Tagen. Das System versendet E-Mail-Benachrichtigungen über das Ablaufdatum und zeigt diese in der Konsole allen Benutzern mit den folgenden Rollen an: Super-Admin, Organisations-Admin, Verbund-Admin und Verbund-Viewer.

16. Überprüfen Sie die Föderationsdetails und wählen Sie dann **Föderation aktivieren**.
17. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nach der Aktivierung der Föderation melden sich die Benutzer mit ihren Unternehmensanmeldeinformationen bei der NetApp Console an.

Verbinden Sie die NetApp Console mit der Microsoft Entra-ID

Verbinden Sie sich mit Ihrem Microsoft Entra ID IdP-Anbieter, um Single Sign-On (SSO) für die NetApp Console zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen anmelden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. NetApp empfiehlt, sich für das eine oder das andere zu entscheiden, aber nicht für beides.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in der Konsole eine Verbindung erstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Verbundverbindung mit der Microsoft Entra ID einrichten, um Single Sign-On (SSO) für die Konsole zu aktivieren. Der Vorgang umfasst die Konfiguration Ihrer Microsoft Entra-ID, um der Konsole als Dienstanbieter zu vertrauen, und das anschließende Erstellen der Verbindung in der Konsole.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.

Domänendetails

1. Geben Sie Ihre Domänendetails ein:
   a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
   b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
   c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
2. Wählen Sie **Weiter**.

Verbindungsmethode

1. Wählen Sie als Verbindungsmethode **Anbieter** und dann **Microsoft Entra ID**.
2. Wählen Sie **Weiter**.

Konfigurationshinweise

1. Konfigurieren Sie Ihre Microsoft Entra-ID, um NetApp als Dienstanbieter zu vertrauen. Sie müssen diesen Schritt auf Ihrem Microsoft Entra ID-Server ausführen.
   a. Verwenden Sie beim Registrieren Ihrer Microsoft Entra ID-App die folgenden Werte, um der Konsole zu

vertrauen:

- Verwenden Sie für die **Umleitungs-URL** `https://services.cloud.netapp.com`
- Verwenden Sie für die **Antwort-URL** `https://netapp-cloud-account.auth0.com/login/callback`

b. Erstellen Sie ein Clientgeheimnis für Ihre Microsoft Entra ID-App. Sie müssen die Client-ID, das Client-Geheimnis und den Entra-ID-Domänennamen angeben, um die Föderation abzuschließen.

2. Kehren Sie zur Konsole zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.

Verbindung erstellen

1. Erstellen Sie die Verbindung mit der Microsoft Entra ID
   a. Geben Sie die Client-ID und das Client-Geheimnis ein, die Sie im vorherigen Schritt erstellt haben.
   b. Geben Sie den Domänennamen der Microsoft Entra ID ein.
2. Wählen Sie **Verbindung erstellen**. Das System stellt die Verbindung in wenigen Sekunden her.

Testen und aktivieren Sie die Verbindung

1. Wählen Sie **Weiter**.
2. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zu einer Anmeldeseite für Ihren IdP-Server weitergeleitet. Melden Sie sich mit Ihren IdP-Zugangsdaten an. Nach dem Einloggen müssen Sie zur Konsole zurückkehren, um die Verbindung zu aktivieren.

   Wenn Sie die Konsole im eingeschränkten Modus verwenden, kopieren Sie die URL entweder in ein Inkognito-Browserfenster oder in einen separaten Browser, um sich bei Ihrem Identitätsanbieter anzumelden.

3. Wählen Sie in der Konsole **Weiter**, um die Zusammenfassungsseite anzuzeigen.
4. Benachrichtigungen einrichten.

   Sie haben die Wahl zwischen sieben Tagen oder 30 Tagen. Das System versendet E-Mail-Benachrichtigungen über das Ablaufdatum und zeigt diese in der Konsole allen Benutzern mit den folgenden Rollen an: Super-Admin, Organisations-Admin, Verbund-Admin und Verbund-Viewer.

5. Überprüfen Sie die Föderationsdetails und wählen Sie dann **Föderation aktivieren**.
6. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nach der Aktivierung der Föderation melden sich die Benutzer mit ihren Unternehmensanmeldeinformationen bei der NetApp Console an.

Föderieren Sie die NetApp Console mit PingFederate

Verbinden Sie sich mit Ihrem PingFederate IdP-Anbieter, um Single Sign-On (SSO) für die NetApp Console zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen anmelden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. NetApp empfiehlt, sich für das eine oder das andere zu entscheiden, aber nicht für beides.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in der Konsole eine Verbindung erstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können mit PingFederate eine Verbundverbindung einrichten, um Single Sign-On (SSO) für die Konsole zu aktivieren. Der Vorgang umfasst die Konfiguration Ihres PingFederate-Servers, sodass dieser der Konsole als Dienstanbieter vertraut, und die anschließende Herstellung der Verbindung in der Konsole.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Geben Sie Ihre Domänendetails ein:
   a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
   b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
   c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
5. Wählen Sie **Weiter**.
6. Wählen Sie als Verbindungsmethode **Provider** und dann **PingFederate**.
7. Wählen Sie **Weiter**.
8. Konfigurieren Sie Ihren PingFederate-Server so, dass er NetApp als Dienstanbieter vertraut. Sie müssen diesen Schritt auf Ihrem PingFederate-Server ausführen.
   a. Verwenden Sie die folgenden Werte, wenn Sie PingFederate so konfigurieren, dass es der NetApp Console vertraut:
      - Für die **Antwort-URL** oder **Assertion Consumer Service (ACS)-URL** verwenden Sie `https://netapp-cloud-account.auth0.com/login/callback`
      - Verwenden Sie für die **Abmelde-URL** `https://netapp-cloud-account.auth0.com/logout`
      - Verwenden Sie für **Zielgruppen-/Entitäts-ID** `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` wobei <fed-domain-name-pingfederate> der Domänenname für die Föderation ist. Wenn Ihre Domäne beispielsweise `example.com` , wäre die Zielgruppen-/Entitäts-ID `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .
   b. Kopieren Sie die URL des PingFederate-Servers. Sie benötigen diese URL, wenn Sie die Verbindung in der Konsole herstellen.
   c. Laden Sie das X.509-Zertifikat von Ihrem PingFederate-Server herunter. Es muss im Base64-codierten PEM-Format (.pem, .crt, .cer) vorliegen.
9. Kehren Sie zur Konsole zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.
10. Erstellen Sie die Verbindung mit PingFederate
    a. Geben Sie die PingFederate-Server-URL ein, die Sie im vorherigen Schritt kopiert haben.
    b. Laden Sie das X.509-Signaturzertifikat hoch. Das Zertifikat muss im PEM-, CER- oder CRT-Format vorliegen.

11. Wählen Sie **Verbindung erstellen**. Das System stellt die Verbindung in wenigen Sekunden her.
12. Wählen Sie **Weiter**.
13. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zu einer Anmeldeseite für Ihren IdP-Server weitergeleitet. Melden Sie sich mit Ihren IdP-Zugangsdaten an. Nach dem Einloggen müssen Sie zur Konsole zurückkehren, um die Verbindung zu aktivieren.

    Wenn Sie die Konsole im eingeschränkten Modus verwenden, kopieren Sie die URL entweder in ein Inkognito-Browserfenster oder in einen separaten Browser, um sich bei Ihrem Identitätsanbieter anzumelden.

14. Wählen Sie in der Konsole **Weiter**, um die Zusammenfassungsseite anzuzeigen.
15. Benachrichtigungen einrichten.

    Sie haben die Wahl zwischen sieben Tagen oder 30 Tagen. Das System versendet E-Mail-Benachrichtigungen über das Ablaufdatum und zeigt diese in der Konsole allen Benutzern mit den folgenden Rollen an: Super-Admin, Organisations-Admin, Verbund-Admin und Verbund-Viewer.

16. Überprüfen Sie die Föderationsdetails und wählen Sie dann **Föderation aktivieren**.
17. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nach der Aktivierung der Föderation melden sich die Benutzer mit ihren Unternehmensanmeldeinformationen bei der NetApp Console an.

Föderieren Sie mit einem SAML-Identitätsanbieter

Verbinden Sie sich mit Ihrem SAML 2.0-IdP-Anbieter, um Single Sign-On (SSO) für die NEtApp-Konsole zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen anmelden.

Erforderliche Rolle

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. Sie können nicht mit beiden eine Föderation bilden.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in der Konsole eine Verbindung erstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Verbundverbindung mit Ihrem SAML 2.0-Anbieter einrichten, um Single Sign-On (SSO) für die Konsole zu aktivieren. Der Vorgang umfasst die Konfiguration Ihres Providers, sodass dieser NetApp als Serviceprovider vertraut, und die anschließende Herstellung der Verbindung in der Konsole.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Geben Sie Ihre Domänendetails ein:

a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.

b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.

c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.

5. Wählen Sie **Weiter**.
6. Wählen Sie als Verbindungsmethode **Protokoll** und dann **SAML-Identitätsanbieter**.
7. Wählen Sie **Weiter**.
8. Konfigurieren Sie Ihren SAML-Identitätsanbieter so, dass er NetApp als Dienstanbieter vertraut. Sie müssen diesen Schritt auf dem Server Ihres SAML-Anbieters ausführen.

a. Stellen Sie sicher, dass Ihr IdP das Attribut `email` auf die E-Mail-Adresse des Benutzers eingestellt. Dies ist erforderlich, damit die Konsole Benutzer korrekt identifizieren kann:

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. Verwenden Sie die folgenden Werte, wenn Sie Ihre SAML-Anwendung bei der Konsole registrieren:
   - Für die **Antwort-URL** oder **Assertion Consumer Service (ACS)-URL** verwenden Sie `https://netapp-cloud-account.auth0.com/login/callback`
   - Verwenden Sie für die **Abmelde-URL** `https://netapp-cloud-account.auth0.com/logout`
   - Verwenden Sie für **Zielgruppen-/Entitäts-ID** `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` wobei <fed-domain-name-saml> der Domänenname ist, den Sie für die Föderation verwenden möchten. Wenn Ihre Domäne beispielsweise `example.com` , wäre die Zielgruppen-/Entitäts-ID `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .
2. Kopieren Sie nach dem Erstellen des Vertrauens die folgenden Werte vom Server Ihres SAML-Anbieters:
   - Anmelde-URL
   - Abmelde-URL (optional)
3. Laden Sie das X.509-Zertifikat vom Server Ihres SAML-Anbieters herunter. Es muss im PEM-, CER- oder CRT-Format vorliegen.

a. Kehren Sie zur Konsole zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.

b. Stellen Sie die Verbindung mit SAML her.

4. Geben Sie die **Anmelde-URL** Ihres SAML-Servers ein.
5. Laden Sie das X.509-Zertifikat hoch, das Sie vom Server Ihres SAML-Anbieters heruntergeladen haben.
6. Geben Sie optional die **Abmelde-URL** Ihres SAML-Servers ein.

a. Wählen Sie **Verbindung erstellen**. Das System stellt die Verbindung in wenigen Sekunden her.

b. Wählen Sie **Weiter**.

c. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zu einer Anmeldeseite für Ihren IdP-Server weitergeleitet. Melden Sie sich mit Ihren IdP-Zugangsdaten an. Nach dem Einloggen müssen Sie zur Konsole zurückkehren, um die Verbindung zu aktivieren.

> Wenn Sie die Konsole im eingeschränkten Modus verwenden, kopieren Sie die URL entweder in ein Inkognito-Browserfenster oder in einen separaten Browser, um sich bei Ihrem Identitätsanbieter anzumelden.

d. Wählen Sie in der Konsole **Weiter**, um die Zusammenfassungsseite anzuzeigen.

e. Benachrichtigungen einrichten.

   Sie haben die Wahl zwischen sieben Tagen oder 30 Tagen. Das System versendet E-Mail-Benachrichtigungen über das Ablaufdatum und zeigt diese in der Konsole allen Benutzern mit den folgenden Rollen an: Super-Admin, Organisations-Admin, Verbund-Admin und Verbund-Viewer.

f. Überprüfen Sie die Föderationsdetails und wählen Sie dann **Föderation aktivieren**.

g. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nach der Aktivierung der Föderation melden sich die Benutzer mit ihren Unternehmensanmeldeinformationen bei der NetApp Console an.

Föderationen verwalten

Föderationen in der NetApp Console verwalten

Sie können Ihre Föderation in der NetApp Console verwalten. Sie können es deaktivieren, abgelaufene Anmeldeinformationen aktualisieren und es deaktivieren, wenn Sie es nicht mehr benötigen.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Sie können einer bestehenden Föderation auch eine zusätzliche verifizierte Domäne hinzufügen, wodurch Sie mehrere Domänen für Ihre föderierte Verbindung nutzen können.

- Wenn Sie die Föderation mit NetApp Cloud Central konfiguriert haben, importieren Sie sie über die Seite **Föderation**, um sie in der Konsole zu verwalten."Erfahren Sie, wie Sie Ihre Föderation importieren"
- Auf der Seite „Überwachung“ können Sie Ereignisse der Föderationsverwaltung wie das Aktivieren, Deaktivieren und Aktualisieren von Föderationen einsehen. "Erfahren Sie mehr über die Überwachung von Vorgängen in der NetApp Console."

Aktivieren einer Föderation

Wenn Sie eine Föderation erstellt haben, diese aber nicht aktiviert ist, können Sie sie über die Seite **Föderation** aktivieren. Durch die Aktivierung einer Föderation können sich die mit der Föderation verknüpften Benutzer mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden. Erstellen und testen Sie

die Föderation erfolgreich, bevor Sie sie aktivieren.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü ••• neben der Föderation, die Sie aktivieren möchten, und wählen Sie **Aktivieren** aus.

Hinzufügen einer verifizierten Domäne zu einer vorhandenen Föderation

Sie können einer vorhandenen Föderation in der Konsole eine verifizierte Domäne hinzufügen, um mehrere Domänen mit demselben Identitätsanbieter (IdP) zu verwenden.

Sie müssen die Domäne bereits in der Konsole verifiziert haben, bevor Sie sie zu einer Föderation hinzufügen können. Wenn Sie die Domäne noch nicht verifiziert haben, können Sie dies tun, indem Sie die Schritte in"Überprüfen Sie Ihre Domäne in der Konsole" .

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü⋮ neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Domänen aktualisieren** aus. Im Dialogfeld **Domänen aktualisieren** wird die Domäne angezeigt, die bereits mit dieser Föderation verknüpft ist.
4. Wählen Sie eine verifizierte Domäne aus der Liste der verfügbaren Domänen aus.
5. Wählen Sie **Aktualisieren**. Neue Domänenbenutzer können innerhalb von 30 Sekunden föderierten Konsolenzugriff erhalten.

Aktualisieren einer ablaufende Verbundverbindung

Sie können die Details einer Föderation in der Konsole aktualisieren. Sie müssen beispielsweise die Föderation aktualisieren, wenn Anmeldeinformationen wie ein Zertifikat oder ein Client-Geheimnis ablaufen. Aktualisieren Sie bei Bedarf das Benachrichtigungsdatum, um Sie daran zu erinnern, die Verbindung zu aktualisieren, bevor sie abläuft.

Aktualisieren Sie zuerst die Konsole, bevor Sie Ihren IdP aktualisieren, um Anmeldeprobleme zu vermeiden. Bleiben Sie während des Vorgangs bei der Konsole angemeldet.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü (drei vertikale Punkte) neben der Föderation, die Sie aktualisieren möchten, und wählen Sie **Föderation aktualisieren**.
4. Aktualisieren Sie die Details der Föderation nach Bedarf.
5. Wählen Sie **Aktualisieren**.

Testen einer vorhandenen Föderation

Testen Sie die Verbindung einer vorhandenen Föderation, um sicherzustellen, dass sie funktioniert. Auf diese Weise können Sie etwaige Probleme mit der Föderation erkennen und beheben.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Verbindung testen** aus.
4. Wählen Sie **Test**. Das System fordert Sie auf, sich mit Ihren Unternehmensanmeldeinformationen anzumelden. Wenn die Verbindung erfolgreich ist, werden Sie zur NetApp Console weitergeleitet. Wenn die Verbindung fehlschlägt, wird eine Fehlermeldung angezeigt, die auf das Problem mit der Föderation hinweist.
5. Wählen Sie **Fertig**, um zur Registerkarte **Föderation** zurückzukehren.

Deaktivieren einer Föderation

Wenn Sie eine Föderation nicht mehr benötigen, können Sie sie deaktivieren. Dadurch wird verhindert, dass sich mit der Föderation verknüpfte Benutzer mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden. Sie können die Föderation bei Bedarf später wieder aktivieren.

Deaktivieren Sie eine Föderation, bevor Sie sie löschen, beispielsweise wenn Sie den IdP außer Betrieb nehmen oder die Föderation beenden. Auf diese Weise können Sie es bei Bedarf später wieder aktivieren.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Deaktivieren** aus.

Löschen einer Föderation

Wenn Sie eine Föderation nicht mehr benötigen, können Sie sie löschen. Dadurch wird die Föderation entfernt und alle mit der Föderation verknüpften Benutzer können sich nicht mehr mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden. Beispielsweise, wenn der IdP außer Betrieb genommen wird oder die Föderation nicht mehr benötigt wird.

Sie können eine Föderation nicht wiederherstellen, nachdem Sie sie gelöscht haben. Sie müssen eine neue Föderation erstellen.

Sie müssen eine Föderation deaktivieren, bevor Sie sie löschen können. Sie können eine Föderation nach dem Löschen nicht wiederherstellen.

Schritte

1. Wählen Sie **Administration > Identität und Zugriff**.
2. Wählen Sie **Föderationen** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Löschen** aus.

Importieren Sie Ihre Föderation in die NetApp Console

Wenn Sie zuvor die Föderation über NetApp Cloud Central (eine externe Anwendung der NetApp Console) eingerichtet haben, werden Sie auf der Föderationsseite aufgefordert,

Ihre vorhandene föderierte Verbindung in die Konsole zu importieren, damit Sie sie in der neuen Schnittstelle verwalten können. Sie können dann die neuesten Verbesserungen nutzen, ohne Ihre Verbundverbindung neu erstellen zu müssen.

Nachdem Sie Ihre vorhandene Föderation importiert haben, können Sie die Föderation auf der Seite **Föderationen** verwalten."Erfahren Sie mehr über die Verwaltung von Föderationen."

Erforderliche Rolle

Organisationsadministrator oder Föderationsadministrator."Erfahren Sie mehr über Zugriffsrollen."

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie **Föderation importieren**.

Erzwingen Sie ONTAP -Berechtigungen für ONTAP Advanced View (ONTAP System Manager).

Standardmäßig ermöglichen die Anmeldeinformationen des Konsolenagenten den Benutzern den Zugriff auf die erweiterte Ansicht (ONTAP System Manager). Sie können Benutzer stattdessen zur Eingabe ihrer ONTAP Anmeldeinformationen auffordern. Dadurch wird sichergestellt, dass die ONTAP Berechtigungen eines Benutzers angewendet werden, wenn er mit ONTAP Clustern sowohl in Cloud Volumes ONTAP als auch in lokalen ONTAP -Clustern arbeitet.

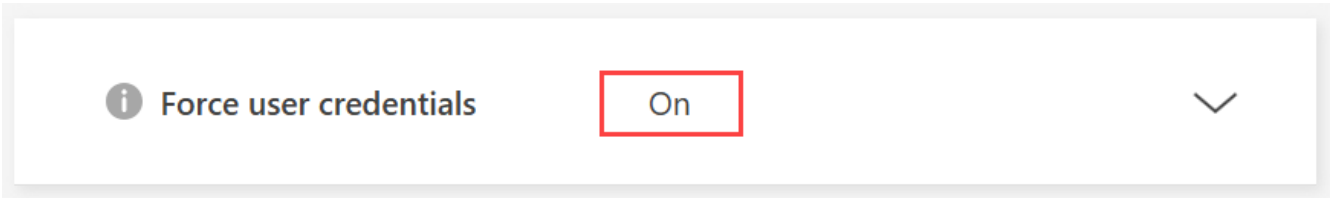
Sie müssen über die Rolle des Organisationsadministrators verfügen, um die Einstellungen des Konsolenagenten bearbeiten zu können.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **Agent bearbeiten**.

   Zum Bearbeiten muss der Konsolenagent aktiv sein.

3. Erweitern Sie die Option **Anmeldeinformationen erzwingen**.
4. Aktivieren Sie das Kontrollkästchen, um die Option **Anmeldeinformationen erzwingen** zu aktivieren, und wählen Sie dann **Speichern**.
5. Stellen Sie sicher, dass die Option **Anmeldeinformationen erzwingen** aktiviert ist.



Aktivieren Sie den Nur-Lese-Modus für eine NetApp Console Organisation

Als Sicherheitsmaßnahme können Sie den Nur-Lese-Modus für Ihre NetApp Console Organisation aktivieren. Im Nur-Lese-Modus können Benutzer Ressourcen und Einstellungen einsehen, aber keine Änderungen vornehmen.

Im Nur-Lese-Modus müssen Benutzer mit Administratorrechten ihre Berechtigungen manuell erhöhen, um Änderungen vornehmen zu können. Dadurch wird sichergestellt, dass die Änderungen beabsichtigt sind.

Erforderliche Zugriffsrollen

Super-Admin oder Organisationsadministrator.

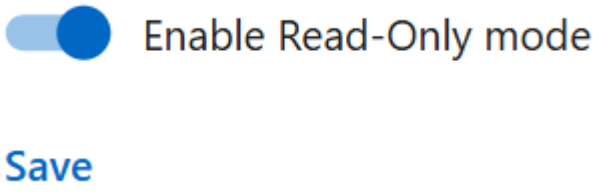
Aktivieren Sie den schreibgeschützten Modus für Ihre Konsolenorganisation.

Aktivieren Sie den Nur-Lese-Modus, um Änderungen an Ihrer Konsolenorganisation einzuschränken. Alle Benutzer können weiterhin auf die Ressourcen zugreifen. Benutzer mit Administratorrechten können in der Konsole keine Aktionen durchführen, ohne ihre Berechtigungen manuell zu erhöhen.

Wenn der Nur-Lese-Modus aktiviert ist, sehen die Benutzer ein Banner, das sie darüber informiert, dass sich die Organisation im Nur-Lese-Modus befindet. Benutzer müssen in die Benutzereinstellungen gehen, um ihre Rolle zu erhöhen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie auf der Registerkarte **Organisationen** die Option **Organisationseinstellungen bearbeiten** für die Organisation aus, die Sie in den Nur-Lese-Modus versetzen möchten.
3. Im Abschnitt **Schreibgeschützter Modus** aktivieren Sie den schreibgeschützten Modus, indem Sie den Schalter in die Position **Ein** bewegen und anschließend **Speichern** auswählen.



Registrieren Sie sich als erster Organisationsadministrator für die NetApp Console.

Falls Ihr Unternehmen noch keine NetApp Console -Organisation besitzt, registrieren Sie sich, um eine zu erstellen. Der erste Benutzer ist der Administrator und verwaltet Konten und Berechtigungen. Sie können Rollen aktualisieren und Administratoren später hinzufügen.

Schritte

1. Öffnen Sie einen Webbrowser und gehen Sie zu "NetApp Console"
2. Wenn Sie über ein NetApp Support Site-Konto verfügen, geben Sie die mit Ihrem Konto verknüpfte E-Mail-Adresse direkt auf der **Anmeldeseite** ein.

   Die Konsole registriert Sie im Rahmen dieser ersten Anmeldung mit Ihren Zugangsdaten für die NetApp Support Site.

3. Wenn Sie sich durch Erstellen eines Konsolen-Logins anmelden möchten, wählen Sie **Anmelden**.
   a. Geben Sie auf der Seite **Anmelden** die erforderlichen Informationen ein und wählen Sie **Weiter**.

      Im Anmeldeformular sind nur englische Zeichen zulässig.

   b. Suchen Sie in Ihrem Posteingang nach einer E-Mail von NetApp mit Anweisungen zur Bestätigung Ihrer E-Mail-Adresse.

      Bitte bestätigen Sie Ihre E-Mail-Adresse, um die Anmeldung abzuschließen.

4. Nachdem Sie sich angemeldet haben, lesen und akzeptieren Sie bitte die Endbenutzer-Lizenzvereinbarung.
5. Auf der **Willkommensseite** können Sie eine Organisation erstellen.
6. Wählen Sie **Los geht's**.

+ Als erstmaliger Administrator folgen Sie dem geführten Prozess, um Speicher hinzuzufügen, einen Konsolenagenten zu erstellen und vieles mehr. "Erfahren Sie mehr über die Verwendung des Konsolenassistenten."

Nächste Schritte

Als Administrator sollten Sie, nachdem Sie die im Konsolenassistenten enthaltenen Schritte abgeschlossen haben, Ihre Identitäts- und Zugriffsstrategie planen, Benutzer zu Ihrer Organisation hinzufügen und Rollen zuweisen. "Erfahren Sie mehr über Identitäts- und Zugriffsmanagement für die NetApp Console."

Registrieren Sie sich oder melden Sie sich bei der NetApp Console an, wenn bereits eine Organisation existiert.

Falls Ihr Unternehmen bereits über eine NetApp Console Organisation verfügt, registrieren Sie sich oder melden Sie sich an, um darauf zuzugreifen. Die Art Ihrer Registrierung oder Anmeldung hängt davon ab, ob Ihr Unternehmen eine Identitätsföderation nutzt oder über Anmeldeinformationen für die NetApp Support Site verfügt. Falls nicht, erstellen Sie ein NetApp Console -Login.

Schritte

1. Öffnen Sie einen Webbrowser und gehen Sie zu "NetApp Console"
2. Wenn Sie über ein NetApp Support Site-Konto verfügen oder Ihr Unternehmen Single Sign-On (SSO) eingerichtet hat, geben Sie Ihre zugehörige E-Mail-Adresse oder Ihre SSO-Anmeldeinformationen auf der Seite **Anmelden** ein. Folgen Sie den Anweisungen, um die Anmeldung abzuschließen.

   In beiden Fällen werden Sie im Rahmen dieser ersten Anmeldung für die Konsole angemeldet.

3. Wenn Sie sich durch Erstellen eines Konsolen-Logins anmelden möchten, wählen Sie **Anmelden**.
   a. Geben Sie auf der Seite **Anmelden** die erforderlichen Informationen ein und wählen Sie **Weiter**.

      Im Anmeldeformular sind nur englische Zeichen zulässig.

   b. Suchen Sie in Ihrem Posteingang nach einer E-Mail von NetApp mit Anweisungen zur Bestätigung Ihrer E-Mail-Adresse.

      Bitte bestätigen Sie Ihre E-Mail-Adresse, um die Anmeldung abzuschließen.

4. Nachdem Sie sich angemeldet haben, lesen und akzeptieren Sie bitte die Endbenutzer-

Lizenzvereinbarung.

5. Wenn Sie vom System aufgefordert werden, eine Organisation zu erstellen, schließen Sie das Dialogfeld und informieren Sie einen Konsolenadministrator, damit dieser Sie Ihrer Konsolenorganisation hinzufügen und Ihnen Zugriff gewähren kann. "Erfahren Sie, wie Sie einen Organisationsadministrator kontaktieren können."

Nächste Schritte

Sobald Sie Zugriff auf Ihre Organisation erhalten haben, können Sie mit der Verwaltung des Speichers und der Nutzung der Ihnen zugewiesenen Datendienste beginnen.

Organisationspartnerschaften verwalten

Organisationspartnerschaften in NetApp Console

Durch die Schaffung von Partnerschaften zwischen Organisationen in der NetApp Console können Partner NetApp Ressourcen über Organisationsgrenzen hinweg sicher verwalten, die Zusammenarbeit optimieren und die Sicherheit erhöhen.

Erforderliche Rollen

Partnerschaftsadministrator"Erfahren Sie mehr über Zugriffsrollen."

Partnerschaften ermöglichen die sichere Verwaltung von NetApp -Ressourcen in verschiedenen Organisationen mithilfe rollenbasierter Beziehungen in der Konsole. Die initiierende Organisation gewährt Zugriff auf ihre Ressourcen, während die akzeptierende Organisation die Benutzer oder Dienstkonten bereitstellt, denen Zugriff gewährt werden soll. Partnerschaften werden über einen Self-Service-Workflow eingerichtet, der der initiierenden Organisation die volle Kontrolle darüber gibt, welche Ressourcen gemeinsam genutzt und welche Rollen zugewiesen werden. Außerdem hat sie die Möglichkeit, den Partnerzugriff nach Bedarf zu integrieren, zu verwalten oder zu widerrufen.

Kunden können MSPs oder Wiederverkäufer zur Verwaltung von NetApp -Umgebungen autorisieren, ohne dass komplizierte Setups erforderlich sind. Kunden können steuern, auf welche Cluster Partner zugreifen können und welche Rollen sie haben. Außerdem können sie den Zugriff jederzeit widerrufen, um die Sicherheit und Compliance aufrechtzuerhalten.

Als Partner erhalten Sie zentrale Transparenz und Kontrolle über alle Kundenumgebungen. Sie können problemlos zur Organisation eines Kunden wechseln, um Ressourcen zu verwalten, Datendienste auszuführen und den Zustand innerhalb definierter Grenzen zu überwachen. Dadurch wird der Bedarf an benutzerdefinierten Tools reduziert und die Übereinstimmung mit den Richtlinien jedes Kunden sichergestellt.

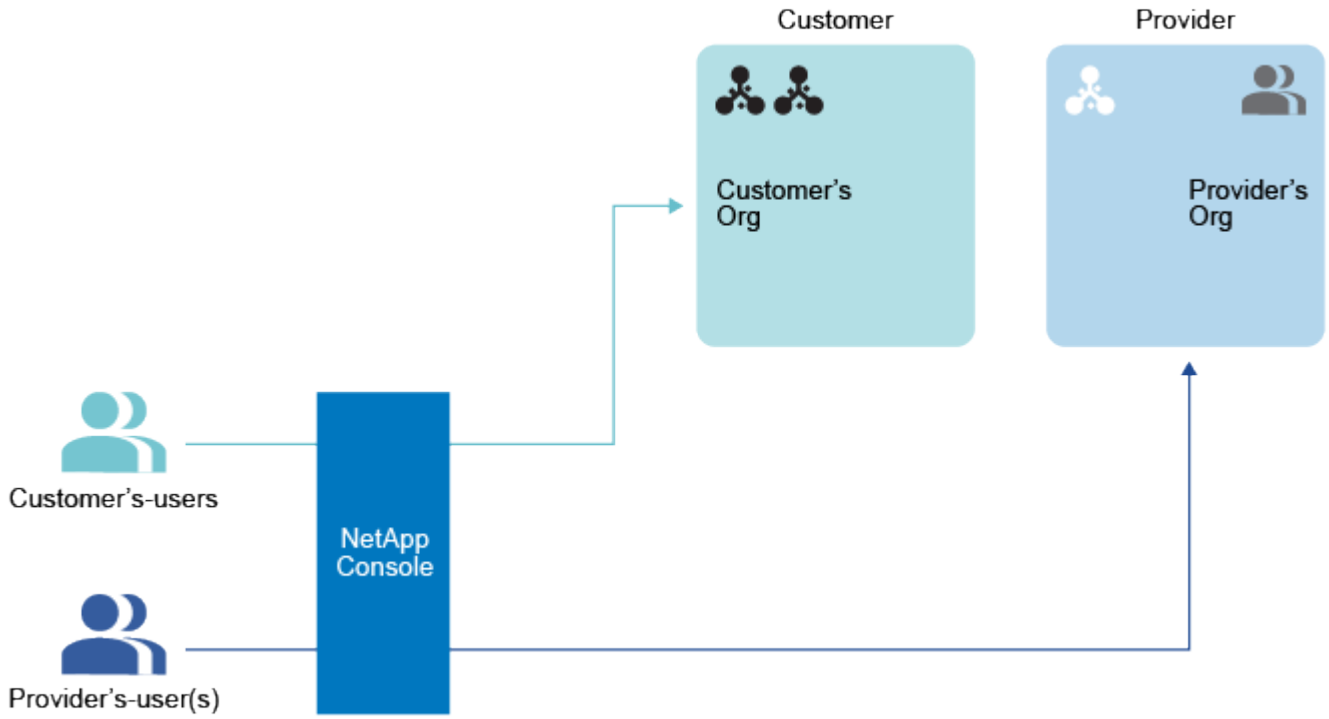
Weisen Sie einem oder mehreren Benutzern die Rolle „Partnerschaftsadministrator“ zu.

Weisen Sie einem oder mehreren Benutzern in der initiierenden und der empfangenden Organisation die Rolle Partnership admin zu, damit sie Partnerschaften erstellen und verwalten können. Sie können Benutzern, die Partnerschaften lediglich einsehen, aber nicht verwalten müssen, die Rolle Partnership viewer zuweisen.

Teilen Sie Ihre Organisations-ID mit der initiierenden Organisation

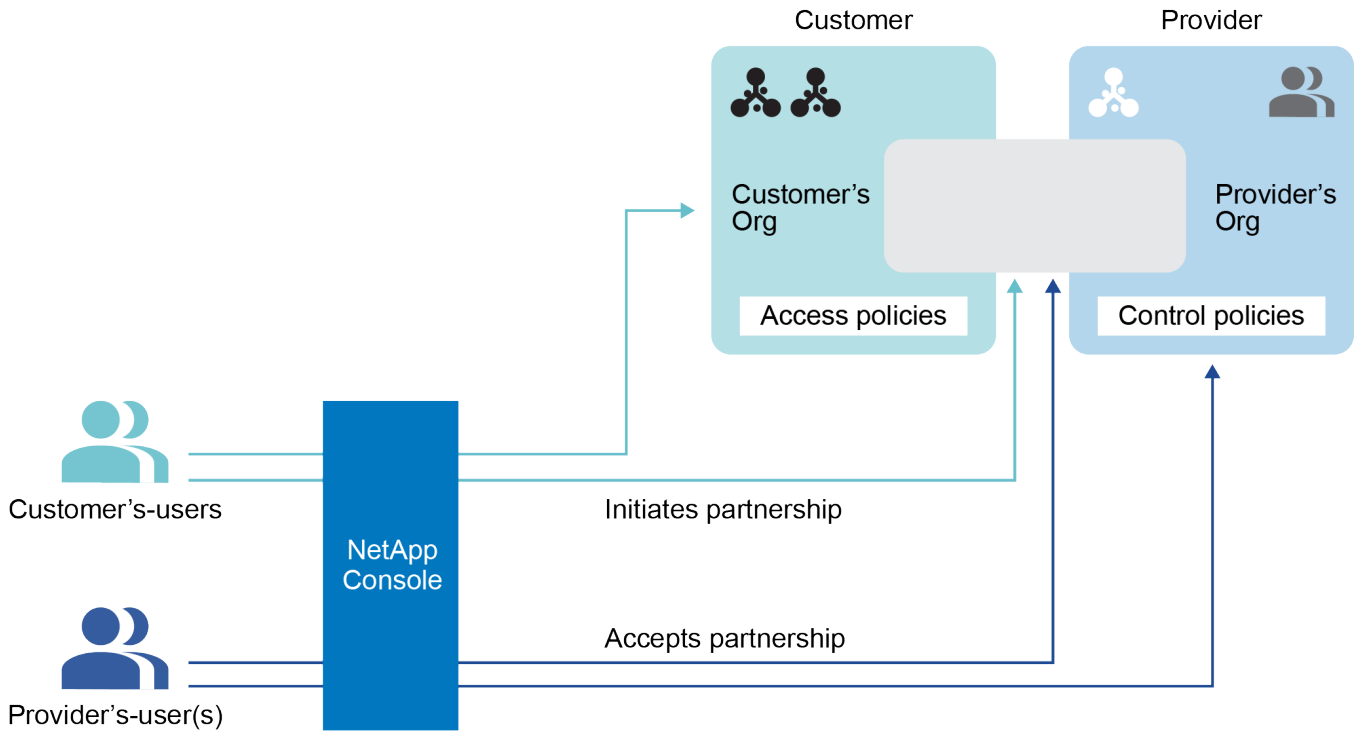
Um eine Partnerschaft zu initiieren, muss der Initiator die Organisations-ID der Zielorganisation kennen. Auf diese Organisations-ID kann nur die jeweilige Organisation zugreifen. Geben Sie es direkt per E-Mail oder auf andere Weise außerhalb der NetApp Console an die initiierende Organisation weiter.

Die initiierende Organisation ist die Organisation, die Zugriff auf ihre Ressourcen gewährt.



3 Initiieren Sie die Partnerschaft innerhalb der NetApp Console

Die Organisation, die die Partnerschaft initiiert, tut dies innerhalb der NetApp Console, indem sie eine Partnerschaftsanfrage sendet.



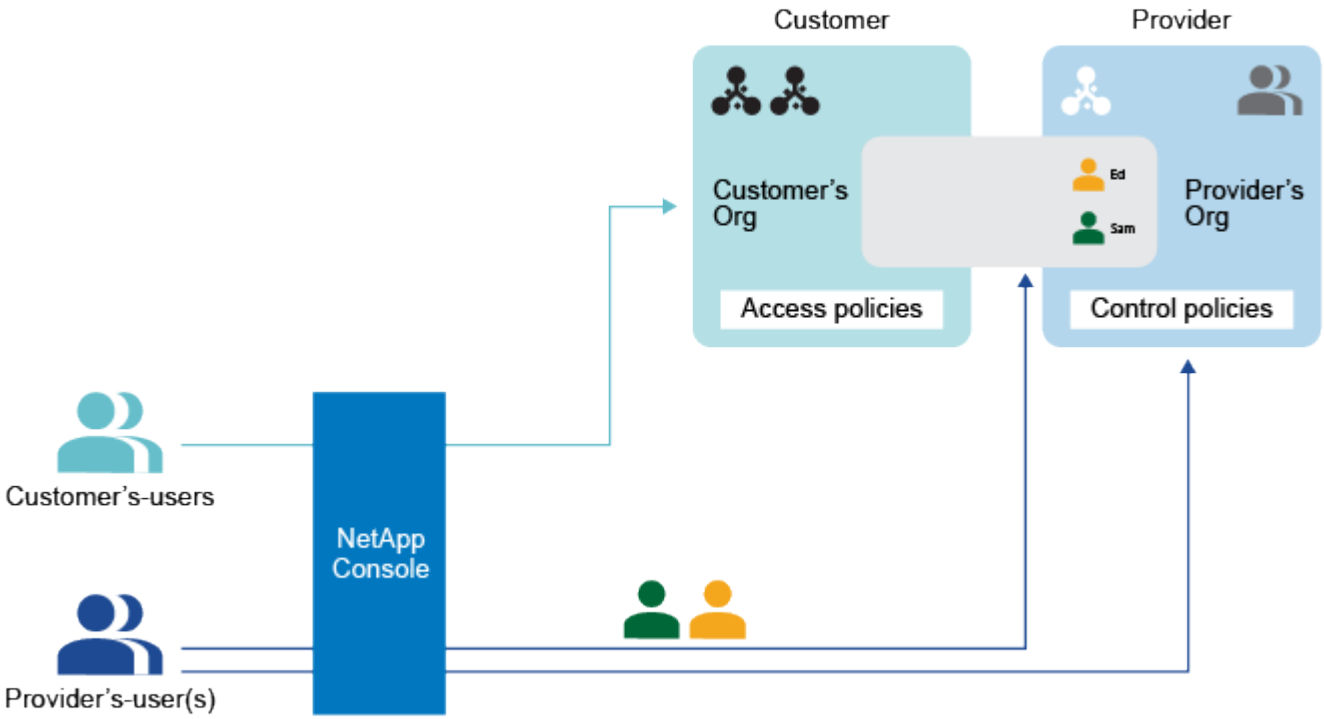
4 Genehmigen Sie die Partnerschaft

Die empfangende Organisation muss die Anfrage annehmen.

Die empfangende Organisation ist die Organisation, der Zugriff auf Ressourcen gewährt wird.

5 Zuweisen von Benutzern zur Partnerschaft

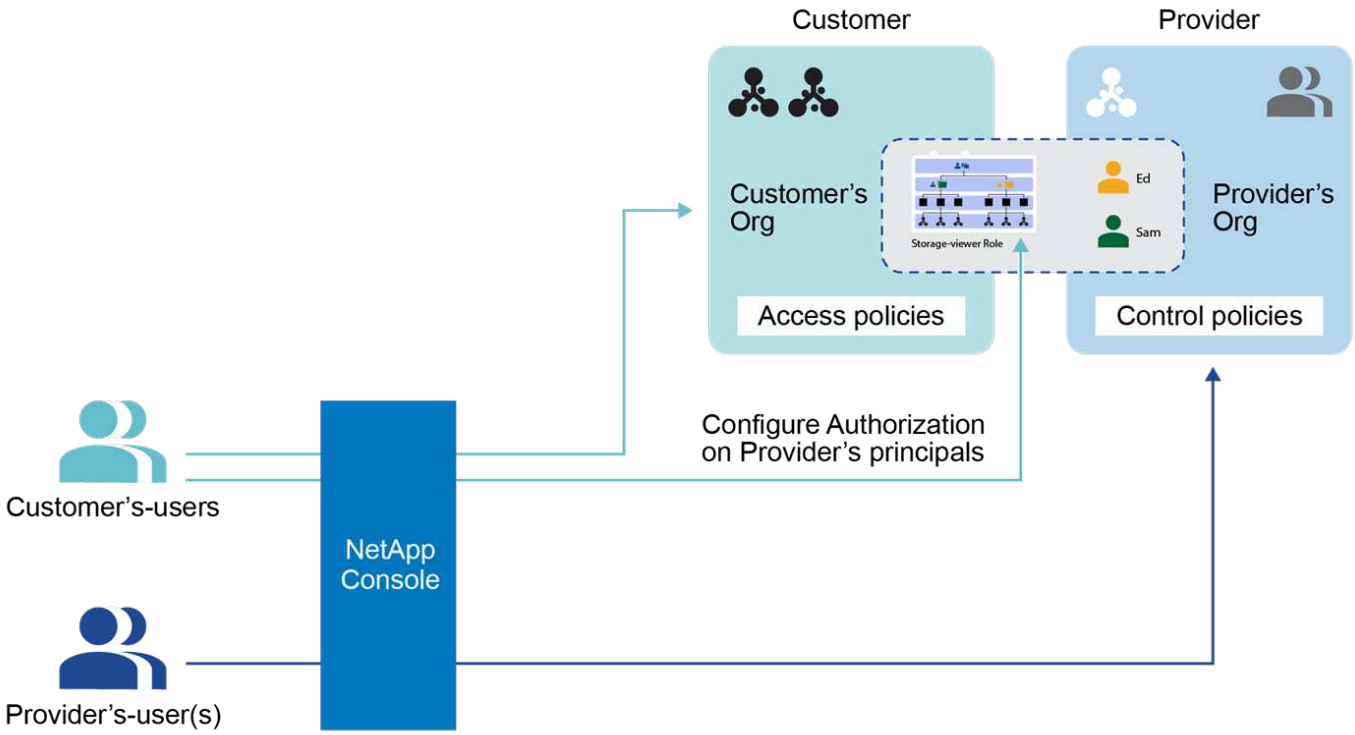
Die empfangende Organisation weist der Partnerschaft bestimmte Benutzer oder Dienstkonten aus Ihrer Organisation zu. Die initiierende Organisation weist diesen Benutzern Rollen zu.



6 Gewähren Sie zugewiesenen Benutzern Zugriff auf Ressourcen

Wenn Sie die initiierende Organisation sind, können Sie den Benutzern, die der Partnerschaft zugewiesen wurden, Zugriff auf bestimmte Ressourcen gewähren. Sie können den Zugriff jederzeit widerrufen.

Dies erreichen Sie, indem Sie Rollen für bestimmte Projekte oder Ordner innerhalb Ihrer Organisation zuweisen.



Verwalten Sie Partnerschaften in der NetApp Console

Bauen Sie Partnerschaften auf, um sichere, verwaltete Verbindungen zwischen Ihrem Unternehmen und vertrauenswürdigen Partnern für ein kollaboratives NetApp Ressourcenmanagement herzustellen.

Durch Partnerschaften können Sie NetApp -Ressourcen über Grenzen hinweg sicher verwalten, indem Sie rollenbasierte Beziehungen in der Konsole nutzen. Die initiierende Organisation gewährt Zugriff auf ihre Ressourcen, während die akzeptierende Organisation die Benutzer oder Dienstkonten bereitstellt, denen Zugriff gewährt werden soll. Partnerschaften werden über einen Self-Service-Workflow eingerichtet, der der initiierenden Organisation die volle Kontrolle darüber gibt, welche Ressourcen gemeinsam genutzt und welche Rollen zugewiesen werden. Außerdem hat sie die Möglichkeit, den Partnerzugriff nach Bedarf zu integrieren, zu verwalten oder zu widerrufen.

Erforderliche Rollen

Zum Erstellen und Verwalten von Partnerschaften ist die Rolle **Partnerschaftsadministrator** erforderlich. Der **Partnerschaftsbetrachter** kann die Seite „Partnerschaften“ anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Initiieren Sie eine Organisationspartnerschaft

Sie können eine Partnerschaft mit einer anderen Organisation beantragen, wenn Sie deren Organisations-ID kennen. Die empfangende Organisation genehmigt die Anfrage, bevor die Partnerschaft fortgesetzt werden kann.

Bevor Sie beginnen, stellen Sie sicher, dass Sie über die Organisations-ID der Partnerorganisation verfügen und dass Ihnen die Rolle **Partnerschaftsadministrator** zugewiesen wurde.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.

2. Wählen Sie die Registerkarte **Partnerschaften**.
3. Wählen Sie **Partnerschaft hinzufügen**.
4. Geben Sie im Dialogfeld **Partnerschaft erstellen** die Partnerorganisations-ID des gewünschten Partners ein und wählen Sie **Hinzufügen**.

   Die Partnerschaftsanfrage wird zur Genehmigung an die Partnerorganisation gesendet. Den Status der Partnerschaftsanfrage können Sie auf der Seite **Partnerschaften** einsehen.

Genehmigen einer Organisationspartnerschaft

Eine Anfrage für eine Organisationspartnerschaft muss von der empfangenden Organisation angenommen werden, bevor die Partnerschaft fortgesetzt werden kann. Sie müssen über die Rolle **Partnerschaftsadministrator** verfügen, um Partnerschaften zu genehmigen und zu verwalten.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Partnerschaften** aus.
3. Wählen Sie die Registerkarte **Partnerschaft erhalten**.
4. Navigieren Sie zu der empfangenen Partnerschaft, die Sie genehmigen möchten, und wählen Sie ••• und wählen Sie dann **Genehmigen**.
5. Überprüfen Sie die Details der Partnerschaft, einschließlich des Namens und der Organisations-ID der Organisation, die die Partnerschaft angefordert hat, und wählen Sie **Weiter** aus.
6. Fügen Sie optional Organisationsmitglieder zur Partnerschaft hinzu und wählen Sie **Übernehmen**.

   Sie können jederzeit weitere Mitglieder über die Seite **Partnerschaft** hinzufügen.

   Alle von Ihnen hinzugefügten Mitglieder werden in der Organisation des Partners sichtbar, wo der Partner sie Ressourcen zuweisen kann.

Ergebnis

Die von Ihnen genehmigte Partnerschaft weist jetzt den Status **Etabliert** auf. Benutzer mit der Rolle **Partnerschaftsadministrator** oder **Partnerschaftsbetrachter** in einer der beiden Organisationen können die Partnerschaft anzeigen.

Partnerschaftsstatus anzeigen

Sehen Sie sich den Status Ihrer Partnerschaften an.

Erforderliche Rolle

Partnerschaftsadministrator, Partnerschaftsbetrachter."Erfahren Sie mehr über Zugriffsrollen."

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die **Partnerschaften** aus.
3. Wählen Sie entweder die Registerkarte **Initiierte Partnerschaften** oder **Erhaltene Partnerschaften**.
4. Sehen Sie sich die jeweilige Tabelle an, in der Partnerschaften und deren Status angezeigt werden.

Deaktivieren einer Organisationspartnerschaft

Um eine Partnerschaft zu deaktivieren, müssen Sie Mitglied der initiierenden Organisation sein. Durch die Deaktivierung einer Partnerschaft wird der Zugriff auf alle Ressourcen in Ihrer Organisation, die mit der Partnerorganisation geteilt wurden, sofort widerrufen.

Erforderliche Rolle

Partnerschaftsverwaltung."Erfahren Sie mehr über Zugriffsrollen."

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die **Partnerschaften** aus.
3. Wählen Sie entweder die Registerkarte **Initiierte Partnerschaften** aus.
4. Sehen Sie sich die jeweilige Tabelle an, in der Partnerschaften und deren Status angezeigt werden.
5. Navigieren Sie zu der initiierten Partnerschaft, die Sie deaktivieren möchten, und wählen Sie ••• und wählen Sie dann **Deaktivieren**.

Mitglieder für eine Partnerschaftsorganisation verwalten

Sie können Benutzer zu einer Partnerschaft hinzufügen, indem Sie sie der Partnerorganisation hinzufügen. Nachdem Sie Benutzer hinzugefügt haben, ist die Partnerorganisation dafür verantwortlich, ihnen Rollen für bestimmte Ressourcen in ihrer Organisation zuzuweisen.

Erforderliche Rollen

Zum Erstellen und Verwalten von Partnerschaften ist die Rolle **Partnerschaftsadministrator** erforderlich. Der **Partnerschaftsbetrachter** kann die Seite „Partnerschaften“ anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Sie können Benutzer jederzeit aus einer Partnerschaft entfernen. Durch das Entfernen eines Benutzers aus einer Partnerschaft wird dessen Zugriff auf alle Ressourcen in der Partnerorganisation sofort widerrufen.

Mitglieder zu einer Partnerschaft hinzufügen

Wenn Sie einer Partnerschaft Mitglieder hinzufügen, muss der **Partnerschaftsadministrator** der Partnerorganisation ihnen Rollen für bestimmte Ressourcen in seiner Organisation zuweisen, bevor sie auf diese Ressourcen zugreifen können.

Nachdem Sie Mitglieder zu einer Partnerschaft hinzugefügt haben, werden die Mitglieder als Mitglieder in der Partnerorganisation angezeigt, wo der Partner sie Ressourcen zuweisen kann.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Partnerschaften** aus.
3. Wählen Sie die Registerkarte **Partnerschaft erhalten**.
4. Wählen Sie das Aktionsmenü ••• neben der bestehenden Partnerschaft, der Sie Mitglieder hinzufügen möchten, und wählen Sie **Mitglieder hinzufügen**.
5. Wählen Sie ein oder mehrere Mitglieder aus, die Sie der Partnerschaft hinzufügen möchten, und wählen Sie **Hinzufügen**.

Mitglieder aus einer Partnerschaft entfernen

Sie können Mitglieder jederzeit aus einer Partnerschaft entfernen. Durch das Entfernen eines Benutzers aus einer Partnerschaft wird dessen Zugriff auf alle Ressourcen in der Partnerorganisation sofort widerrufen.

Wenn Sie die Rolle eines Mitglieds oder die Ressourcen, auf die es zugreifen kann, anpassen möchten, muss der Partnerschaftsadministrator der Partnerorganisation diese Änderungen vornehmen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Partnerschaften** aus.
3. Wählen Sie die Registerkarte **Partnerschaft erhalten**.
4. Wählen Sie das Aktionsmenü ••• neben dem Mitglied, das Sie entfernen möchten, und wählen Sie **Zuordnung entfernen**.
5. Bestätigen Sie die Aktion, indem Sie im Dialogfeld **Entfernen** auswählen.

Anzeigen von Rolleninformationen für einen Benutzer

Sie können die einem Benutzer zugewiesene Rolle und die zugehörigen Ressourcen anzeigen.

Sie können die einem Benutzer zugeordnete Rolle nicht ändern. Wenn Sie Fragen zu den Ressourcen oder der bereitgestellten Rolle haben, wenden Sie sich an den Administrator der Partnerorganisation.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Partnerschaften** aus.
3. Wählen Sie die Registerkarte **Partnerschaft erhalten**.
4. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.
5. Erweitern Sie in der Tabelle die jeweilige Zeile für die Organisation, den Ordner oder das Projekt, in der Sie die zugewiesene Rolle des Mitglieds anzeigen möchten, und wählen Sie die Nummer in der Spalte **Rolle** aus.

Gewähren Sie Partnerschaftsbenutzern Zugriff auf Ressourcen

Sie können Partnerschaftsbenutzern Zugriff gewähren, indem Sie ihnen bestimmte Rollen für Ordner und Projekte innerhalb Ihrer Organisation zuweisen.

Erforderliche Rollen

Partnerschaftsverwaltung."Erfahren Sie mehr über Zugriffsrollen."

Eine Partnerorganisation muss zunächst Mitglieder zur Partnerschaft hinzufügen, bevor Sie ihnen Rollen für Ressourcen in Ihrer Organisation zuweisen können."Erfahren Sie, wie Sie einer Partnerschaft Mitglieder hinzufügen."

Verstehen Sie die Rollen für Partnerschaftsbenutzer

Sie können Rollen für Mitglieder von Partnerorganisationen auf dieselbe Weise verwalten wie für Ihre eigenen. Allerdings stehen Partnerschaftsbenutzern nicht alle Rollen zur Verfügung. Insbesondere können Sie Partnerbenutzern keine Rolle zuweisen, die Softwareupdates zulässt. Das Aktualisieren der ONTAP -Software

erfordert im Allgemeinen direkten Netzwerkzugriff.

Sie können Partnerbenutzern folgende Rollen zuweisen:

- "Organisationsadministrator"
- "Ordner- oder Projektadministrator"
- "Föderationsadministrator"
- "Föderationsbetrachter"
- "Backup- und Wiederherstellungsadministrator"
- "Backup-Viewer"
- "Administrator wiederherstellen"
- "Klonadministrator"
- "Notfallwiederherstellungsadministrator"
- "Administrator für Notfallwiederherstellungs-Failover"
- "Administrator der Notfallwiederherstellungsanwendung"
- "Disaster Recovery-Viewer"
- "Betriebsunterstützungsanalyst"
- "Klassifizierungsanzeige"

"Erfahren Sie mehr über vordefinierte Rollen"

Einem Partnerbenutzer eine Rolle hinzufügen

Sie gewähren Zugriff auf die Ressourcen Ihrer Organisation, indem Sie einem Mitglied eine Rolle zuweisen. Wenn Sie eine Rolle zuweisen, geben Sie eine Ressource und eine Rolle an. Sie können einem Benutzer mehr als eine Rolle zuweisen.

Wenn Sie beispielsweise zwei Projekte hätten und möchten, dass derselbe Benutzer für beide die Rolle des Backup- und Wiederherstellungsadministrators hat, müssten Sie dem Benutzer für jedes Projekt die Rolle zuweisen. Wenn Sie einem Benutzer für dasselbe Projekt zwei verschiedene Rollen zuweisen möchten, müssen Sie ihm jede Rolle separat zuweisen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Partnerschaften** aus.
3. Wählen Sie die Registerkarte **Partnerschaft initiiert**.
4. Wählen Sie das Aktionsmenü ••• neben der bestehenden Partnerschaft, die Sie anzeigen möchten, und wählen Sie **Details anzeigen** aus.

   In der Liste **Mitglieder** werden die Mitglieder angezeigt, die die Partnerorganisation zur Partnerschaft hinzugefügt hat.

5. Wählen Sie das Aktionsmenü ••• neben dem Mitglied, dem Sie eine Rolle zuweisen möchten, und wählen Sie **Rolle hinzufügen** aus.
6. Um eine Rolle hinzuzufügen, führen Sie die Schritte im Dialogfeld aus:
   - **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**: Wählen Sie die Ebene Ihrer

Ressourcenhierarchie aus, für die das Mitglied Berechtigungen haben soll.

Wenn Sie die Organisation oder einen Ordner auswählen, verfügt das Mitglied über Berechtigungen für alles, was sich innerhalb der Organisation oder des Ordners befindet.

- **Kategorie auswählen**: Wählen Sie eine Rollenkategorie. "Informationen zu Zugriffsrollen" .
- Wählen Sie eine **Rolle**: Wählen Sie eine Rolle, die dem Mitglied Berechtigungen für die Ressourcen erteilt, die mit der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt verknüpft sind.
- **Rolle hinzufügen**: Wenn Sie Zugriff auf zusätzliche Ordner oder Projekte innerhalb Ihrer Organisation gewähren möchten, wählen Sie **Rolle hinzufügen**, geben Sie einen weiteren Ordner oder ein weiteres Projekt oder eine weitere Rollenkategorie an und wählen Sie dann eine Rollenkategorie und eine entsprechende Rolle aus.

7. Wählen Sie **Neue Rollen hinzufügen**.

Ändern oder Entfernen einer Rolle eines Partnerbenutzers

Sie können eine Rolle ändern oder entfernen, die Sie einem Mitglied einer Partnerorganisation zugewiesen haben.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Partnerschaften** aus.
3. Wählen Sie die Registerkarte **Partnerschaft initiiert**.
4. Wählen Sie das Aktionsmenü ••• neben der bestehenden Partnerschaft, die Sie anzeigen möchten, und wählen Sie **Details anzeigen** aus.

   In der Liste **Mitglieder** werden die Mitglieder angezeigt, die die Partnerorganisation zur Partnerschaft hinzugefügt hat.

5. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.
6. Erweitern Sie in der Tabelle die jeweilige Zeile für die Organisation, den Ordner oder das Projekt, in dem Sie die zugewiesene Rolle des Mitglieds ändern möchten, und wählen Sie in der Spalte **Rolle Anzeigen** aus, um die diesem Mitglied zugewiesenen Rollen anzuzeigen.
7. Sie können eine vorhandene Rolle für ein Mitglied ändern oder eine Rolle entfernen.
   a. Um die Rolle eines Mitglieds zu ändern, wählen Sie **Ändern** neben der Rolle, die Sie ändern möchten. Sie können eine Rolle nur in eine Rolle innerhalb derselben Rollenkategorie ändern. Sie können beispielsweise von einer Datendienstrolle zu einer anderen wechseln. Bestätigen Sie die Änderung.
   b. Um die Rolle eines Mitglieds aufzuheben, wählen Sie aus 🗑 neben der Rolle, um die jeweilige Rolle vom Mitglied zu entfernen. Sie werden aufgefordert, die Entfernung zu bestätigen.

Arbeit in einer Partnerorganisation

Sobald Ihnen eine Rolle in einer Partnerorganisation zugewiesen wurde, können Sie zu dieser Organisation wechseln und Aktionen ausführen, für die Sie die Berechtigung haben.

Verwenden Sie das Menü „Organisation“, um zwischen Ihren Organisationen und allen Partnerorganisationen zu wechseln, auf die Sie Zugriff haben."Erfahren Sie mehr über den Wechsel von Organisationen und

Projekten."

Sie können die Ressourcen sehen, die in der Partnerorganisation mit Ihnen geteilt wurden, und Aktionen basierend auf der Ihnen zugewiesenen Rolle ausführen. Arbeiten Sie mit Ihrem Partnerschaftsadministrator zusammen, um sicherzustellen, dass Sie über die entsprechende Rolle für die Ressourcen verfügen, auf die Sie zugreifen müssen.

Überwachen Sie NetApp Console

Sie können den Status der von der Konsole ausgeführten Vorgänge überwachen, um festzustellen, ob Probleme vorliegen, die Sie beheben müssen. Sie können den Status auf der Audit-Seite oder im Benachrichtigungscenter anzeigen oder sich Benachrichtigungen per E-Mail senden lassen.

Die Tabelle hebt die Funktionen der Audit-Seite und des Benachrichtigungscenters durch einen Vergleich hervor.

Benachrichtigungscenter	Audit-Seite
Zeigt den Status auf hoher Ebene für Ereignisse und Aktionen an	Bietet Details zu jedem Ereignis oder jeder Aktion zur weiteren Untersuchung
Zeigt den Status der aktuellen Anmeldesitzung an (die Informationen werden nach der Abmeldung nicht im Benachrichtigungscenter angezeigt)	Behält den Status des letzten Monats bei
Zeigt nur Aktionen an, die in der Benutzeroberfläche initiiert wurden	Zeigt alle Aktionen der Benutzeroberfläche oder APIs an
Zeigt vom Benutzer initiierte Aktionen an	Zeigt alle Aktionen an, egal ob vom Benutzer oder vom System initiiert
Ergebnisse nach Wichtigkeit filtern	Filtern Sie nach Dienst, Aktion, Benutzer, Status und mehr
Bietet die Möglichkeit, Benachrichtigungen per E-Mail an Benutzer und andere zu senden	Keine E-Mail-Funktion

Überwachen Sie die Benutzeraktivität auf der Seite „Überwachen“.

Verwenden Sie die Audit-Seite, um zu ermitteln, wer eine Aktion ausgeführt hat oder welchen Status sie hat.

Auf der Seite „Audit“ werden die Aktionen angezeigt, die Benutzer zur Verwaltung Ihrer Organisation oder Ihres Kontos ausgeführt haben. Dazu gehören Verwaltungsaktionen wie das Zuordnen von Benutzern, das Erstellen von Systemen, das Erstellen von Agenten und mehr.

Sie können auch überprüfen, wer ein Mitglied zu einer Organisation hinzugefügt hat oder ob ein Projekt erfolgreich gelöscht wurde.

Schritte

1. Wählen Sie **Administration > Audit**.
2. Verwenden Sie die Filter über der Tabelle, um zu ändern, welche Aktionen in der Tabelle angezeigt werden.

Sie können beispielsweise den Filter **Dienst** verwenden, um Aktionen anzuzeigen, die sich auf einen bestimmten Dienst beziehen, oder Sie können den Filter **Benutzer** verwenden, um Aktionen anzuzeigen, die sich auf ein bestimmtes Benutzerkonto beziehen.

Laden Sie Überwachungsprotokolle von der Überwachungsseite herunter

Sie können die Audit-Protokolle von der Audit-Seite in eine CSV-Datei herunterladen. Auf diese Weise können Sie die Aktionen protokollieren, die Benutzer in Ihrer Organisation ausführen. Die CSV-Datei enthält alle Spalten in der heruntergeladenen CSV-Datei, unabhängig von Filtern oder angezeigten Spalten auf der Audit-Seite.

Schritte

1. Wählen Sie auf der Seite **Audit** das Download-Symbol in der oberen rechten Ecke der Tabelle aus.

Überwachen Sie Aktivitäten mithilfe des Benachrichtigungscenters

Benachrichtigungen verfolgen Konsolenvorgänge, um den Erfolg zu bestätigen. Sie ermöglichen Ihnen, den Status vieler Konsolenaktionen anzuzeigen, die Sie während Ihrer aktuellen Anmeldesitzung initiiert haben. Nicht alle Konsolendienste melden Informationen an das Benachrichtigungscenter.

Sie können die Benachrichtigungen anzeigen, indem Sie die Benachrichtigungsglocke () in der Menüleiste. Die Farbe der kleinen Blase in der Glocke zeigt die aktive Benachrichtigung mit dem höchsten Schweregrad an. Wenn Sie also eine rote Blase sehen, bedeutet dies, dass es eine wichtige Benachrichtigung gibt, die Sie beachten sollten.

Sie können die Konsole auch so konfigurieren, dass bestimmte Arten von Benachrichtigungen per E-Mail gesendet werden, sodass Sie über wichtige Systemaktivitäten informiert werden, auch wenn Sie nicht beim System angemeldet sind. E-Mails können an alle Benutzer Ihrer Organisation oder an andere Empfänger gesendet werden, die über bestimmte Arten von Systemaktivitäten informiert werden müssen. Erfahren Sie, wie SieE-Mail-Benachrichtigungseinstellungen festlegen .

Vergleich des Benachrichtigungscenters mit Warnungen

Über das Benachrichtigungscenter können Sie den Status der von Ihnen eingeleiteten Vorgänge anzeigen und Warnbenachrichtigungen für bestimmte Arten von Systemaktivitäten einrichten. Mithilfe von Warnmeldungen können Sie Probleme oder potenzielle Risiken in Ihrer ONTAP Speicherumgebung im Zusammenhang mit Kapazität, Verfügbarkeit, Leistung, Schutz und Sicherheit erkennen.

"Erfahren Sie mehr über NetApp Console -Warnmeldungen"

Benachrichtigungstypen

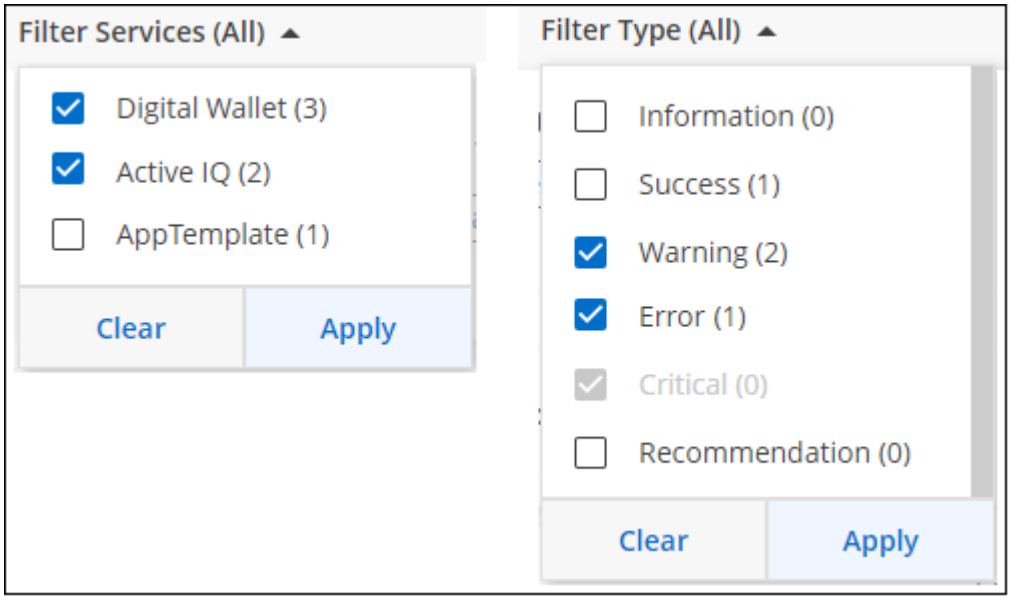
Die Konsole klassifiziert Benachrichtigungen in die folgenden Kategorien:

Benachrichtigungstyp	Beschreibung
Kritisch	Es ist ein Problem aufgetreten, das zu einer Dienstunterbrechung führen kann, wenn nicht sofort Abhilfemaßnahmen ergriffen werden.
Fehler	Eine Aktion oder ein Prozess endete mit einem Fehler oder könnte zu einem Fehler führen, wenn keine Korrekturmaßnahmen ergriffen werden.

Benachrichtigungstyp	Beschreibung
Warnung	Ein Problem, dessen Sie sich bewusst sein sollten, um sicherzustellen, dass es nicht den kritischen Schweregrad erreicht. Benachrichtigungen dieses Schweregrads verursachen keine Dienstunterbrechung und es sind möglicherweise keine sofortigen Korrekturmaßnahmen erforderlich.
Empfehlung	Eine Systemempfehlung für Sie, Maßnahmen zur Verbesserung des Systems oder eines bestimmten Dienstes zu ergreifen; zum Beispiel: Kosteneinsparungen, Vorschläge für neue Dienste, empfohlene Sicherheitskonfiguration usw.
Information	Eine Nachricht, die zusätzliche Informationen zu einer Aktion oder einem Prozess bereitstellt.
Erfolg	Eine Aktion oder ein Prozess wurde erfolgreich abgeschlossen.

Benachrichtigungen filtern

Standardmäßig werden alle aktiven Benachrichtigungen im Benachrichtigungscenter angezeigt. Sie können die angezeigten Benachrichtigungen filtern, um nur die Benachrichtigungen anzuzeigen, die für Sie wichtig sind. Sie können nach „Dienst“ und nach „Typ“ der Benachrichtigung filtern.



Wenn Sie beispielsweise für Konsolenvorgänge nur Benachrichtigungen vom Typ „Fehler“ und „Warnung“ sehen möchten, wählen Sie diese Einträge aus, und Sie sehen nur diese Benachrichtigungstypen.

Benachrichtigungen verwerfen

Sie können Benachrichtigungen von der Seite entfernen, wenn Sie sie nicht mehr sehen müssen. Sie können Benachrichtigungen einzeln oder alle auf einmal ablehnen.

Um alle Benachrichtigungen zu schließen, wählen Sie im Benachrichtigungscenter ⋮ und wählen Sie **Alle verwerfen**.

Um einzelne Benachrichtigungen abzulehnen, bewegen Sie den Cursor über die Benachrichtigung und wählen Sie **Ablehnen**.

E-Mail-Benachrichtigungseinstellungen festlegen

Sie können bestimmte Arten von Benachrichtigungen per E-Mail senden, sodass Sie über wichtige Systemaktivitäten informiert werden, auch wenn Sie nicht angemeldet sind. E-Mails können an alle Benutzer gesendet werden, die Teil Ihrer Organisation oder Ihres Kontos sind, oder an alle anderen Empfänger, die über bestimmte Arten von Systemaktivitäten informiert werden müssen.

- Die Konsole sendet E-Mail-Benachrichtigungen für den Agenten, Lizenzen und Abonnements, NetApp Copy and Sync und NetApp Backup and Recovery.
- Das Senden von E-Mail-Benachrichtigungen wird nicht unterstützt, wenn der Konsolenagent auf einer Site ohne Internetzugang installiert ist.

Die Filter, die Sie im Benachrichtigungscenter festlegen, bestimmen nicht die Art der Benachrichtigungen, die Sie per E-Mail erhalten. Standardmäßig erhält jeder Organisationsadministrator E-Mails für alle „Kritischen“ und „Empfehlungs“-Benachrichtigungen. Diese Benachrichtigungen gelten für alle Dienste. Sie können nicht auswählen, nur für bestimmte Dienste Benachrichtigungen zu erhalten, beispielsweise für Agenten oder NetApp Backup and Recovery.

Alle anderen Benutzer und Empfänger sind so konfiguriert, dass sie keine Benachrichtigungs-E-Mails erhalten. Daher müssen Sie für alle weiteren Benutzer die Benachrichtigungseinstellungen konfigurieren.

Sie müssen über die Rolle des Organisationsadministrators verfügen, um die Benachrichtigungseinstellungen anzupassen.

Schritte

1. Wählen Sie **Verwaltung > Benachrichtigungseinstellungen**.
2. Wählen Sie **Benutzer der Organisation** oder **Zusätzliche Empfänger**.

   Auf der Seite **Zusätzliche Empfänger** können Sie die Konsole so konfigurieren, dass Personen benachrichtigt werden, die Mitglieder Ihrer Konsolenorganisation sind.

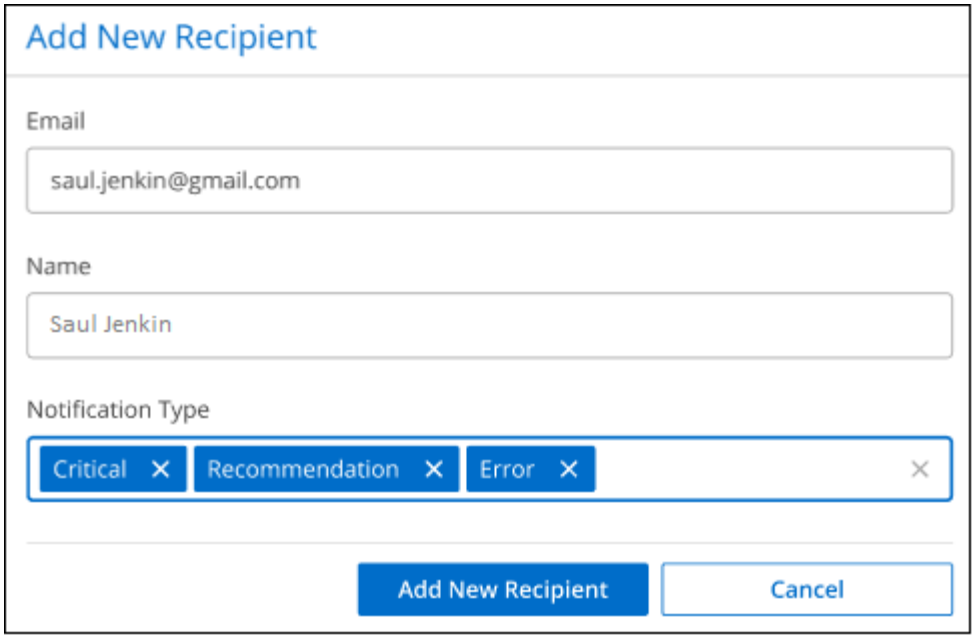
3. Wählen Sie einen oder mehrere Benutzer entweder auf der Seite „Benutzer der Organisation“ oder auf der Seite „Zusätzliche Empfänger“ aus und wählen Sie die Art der zu sendenden Benachrichtigungen:
   - Um Änderungen für einen einzelnen Benutzer vorzunehmen, wählen Sie das Menü in der Spalte „Benachrichtigungen“ für diesen Benutzer aus, überprüfen Sie die zu sendenden Benachrichtigungstypen und wählen Sie „Übernehmen“ aus.
   - Um Änderungen für mehrere Benutzer vorzunehmen, aktivieren Sie das Kontrollkästchen für jeden Benutzer, wählen Sie **E-Mail-Benachrichtigungen verwalten**, aktivieren Sie die zu sendenden Benachrichtigungstypen und wählen Sie **Übernehmen**.

Zusätzliche E-Mail-Empfänger hinzufügen

Die Benutzer, die auf der Seite „Benutzer der Organisation“ angezeigt werden, werden automatisch aus den Benutzern Ihrer Organisation oder Ihres Kontos gefüllt. Sie können auf der Seite „Zusätzliche Empfänger“ E-Mail-Adressen für andere Personen oder Gruppen hinzufügen, die keinen Zugriff auf die Konsole haben, aber über bestimmte Arten von Warnungen und Benachrichtigungen benachrichtigt werden müssen.

Schritte

1. Wählen Sie auf der Seite **Benachrichtigungseinstellungen** die Option **Neue Empfänger hinzufügen** aus.



2. Geben Sie den Namen und die E-Mail-Adresse ein, wählen Sie die Benachrichtigungstypen aus, die der Empfänger erhalten soll, und wählen Sie **Neuen Empfänger hinzufügen**.