Erste Schritte

NetApp Console setup and administration

NetApp
January 27, 2026

This PDF was generated from https://docs.netapp.com/de-de/console-setup-admin/concept-overview.html on January 27, 2026. Always check docs.netapp.com for the latest.

Inhalt

Erste Schritte

Lernen Sie die Grundlagen

Erfahren Sie mehr über die NetApp Console

Die Konsole vereinheitlicht Speicherverwaltung und -schutz über eine hybride Multi-Cloud mit integrierten Datendiensten zum Schutz und zur Optimierung von Daten.

Es ist als Service-Plattform (SaaS) oder als selbstgehostete Option verfügbar, die Sie in Ihrer eigenen Cloud installieren können. Es bietet Speichermanagement, Datenmobilität, Datenschutz sowie Datenanalyse und -kontrolle. Die Managementfunktionen werden über eine webbasierte Konsole und APIs bereitgestellt.

Zentralisierte Speicherverwaltung

Entdecken, implementieren und verwalten Sie Cloud- und lokalen Speicher mit der Konsole.

Unterstützter Cloud- und On-Premises-Speicher

Sie können die folgenden Speichertypen über die Konsole verwalten:

Cloud-Speicherlösungen

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

Lokaler Flash- und Objektspeicher

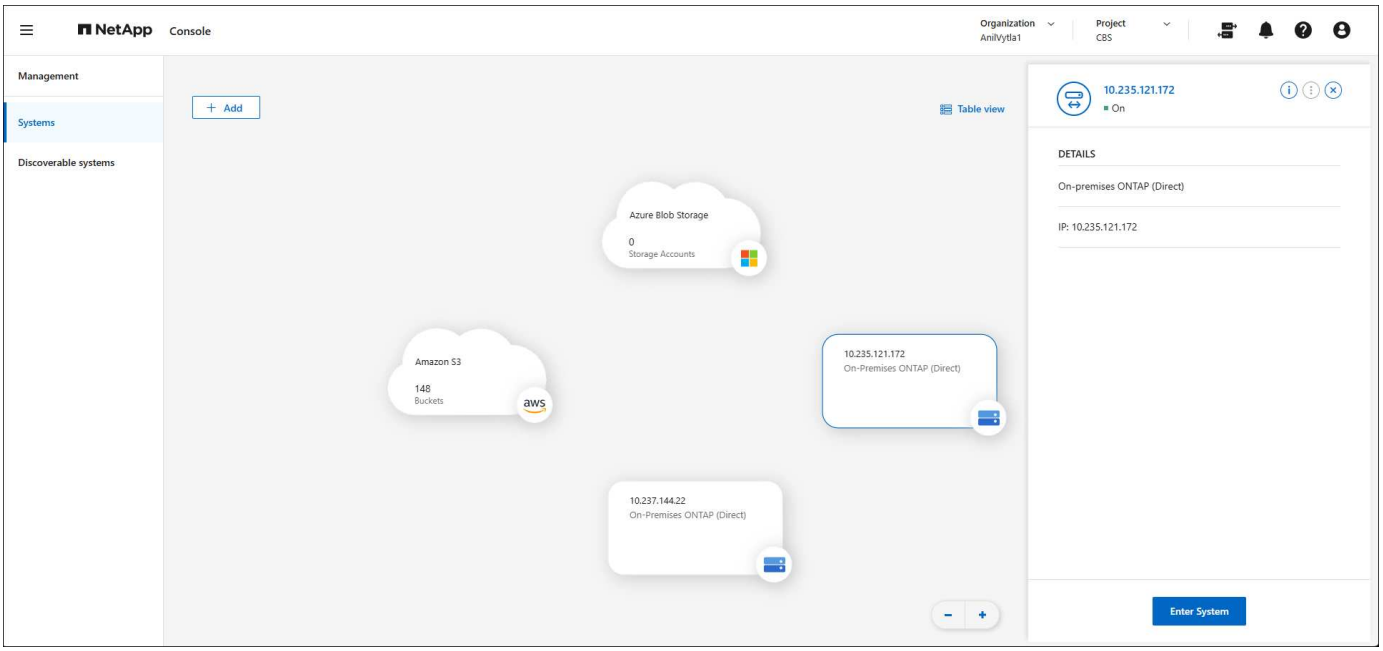
- Systeme der E-Serie
- ONTAP -Cluster
- StorageGRID -Systeme

Cloud-Objektspeicher

- Amazon S3-Speicher
- Azure Blob-Speicher
- Google Cloud-Speicher

Speicherverwaltung

Innerhalb der Konsole stellen *Systeme* erkannten oder bereitgestellten Speicher dar. Sie können ein *System* auswählen, um es in NetApp -Datendienste zu integrieren oder den Speicher zu verwalten, beispielsweise durch Hinzufügen von Volumes.



Integrierte Datendienste und Speicherverwaltung zum Schutz, zur Sicherung und zur Optimierung von Daten

Die Konsole bietet Datendienste zur Sicherung und Aufrechterhaltung der Speicherverfügbarkeit.

Speicherwarnungen

Zeigen Sie Probleme im Zusammenhang mit Kapazität, Verfügbarkeit, Leistung, Schutz und Sicherheit in Ihrer ONTAP Umgebung an.

Automatisierungszentrum

Verwenden Sie skriptbasierte Lösungen, um die Bereitstellung und Integration von NetApp -Produkten und -Services zu automatisieren.

NetApp Backup and Recovery

Sichern und Wiederherstellen von Cloud- und lokalen Daten.

NetApp Data Classification

Machen Sie Ihre Anwendungsdaten und Cloud-Umgebungen datenschutzbereit.

NetApp Copy and Sync

Synchronisieren Sie Daten zwischen lokalen und Cloud-Datenspeichern.

NetApp Digital Advisor (Active IQ)

Nutzen Sie prädiktive Analysen und proaktiven Support, um Ihre Dateninfrastruktur zu optimieren.

Licenses and subscriptions

Verwalten und überwachen Sie Ihre Lizenzen und Abonnements.

NetApp Disaster Recovery

Schützen Sie lokale VMware-Workloads mithilfe von VMware Cloud auf Amazon FSx für ONTAP als Disaster Recovery-Site.

Lebenszyklusplanung

Identifizieren Sie Cluster mit aktueller oder prognostizierter geringer Kapazität und implementieren Sie Empfehlungen zur Datenschichtung oder zusätzlichen Kapazität.

NetApp Ransomware Resilience

Erkennen Sie Anomalien, die zu Ransomware-Angriffen führen könnten. Schützen und stellen Sie Workloads wieder her.

NetApp Replication

Replizieren Sie Daten zwischen Speichersystemen, um Backup und Notfallwiederherstellung zu unterstützen.

Software-Updates

Automatisieren Sie die Bewertung, Planung und Ausführung von ONTAP -Upgrades.

Nachhaltigkeits-Dashboard

Analysieren Sie die Nachhaltigkeit Ihrer Speichersysteme.

NetApp Cloud Tiering

Erweitern Sie Ihren lokalen ONTAP -Speicher auf die Cloud.

NetApp Volume Caching

Erstellen Sie ein beschreibbares Cache-Volume, um den Datenzugriff zu beschleunigen oder den Datenverkehr von stark beanspruchten Volumes zu entlasten.

NetApp Workloads

Entwerfen, einrichten und betreiben Sie wichtige Workloads mit Amazon FSx for NetApp ONTAP.

"Erfahren Sie mehr über die NetApp Console und die verfügbaren Datendienste"

Unterstützte Cloud-Anbieter

Mit der Konsole können Sie Cloud-Speicher verwalten und Cloud-Dienste in Amazon Web Services, Microsoft Azure und Google Cloud nutzen.

Kosten

Für die NetApp Console fallen keine Gebühren an. Wenn Sie Konsolenagenten in der Cloud bereitstellen oder den in der Cloud bereitgestellten eingeschränkten Modus verwenden, entstehen Ihnen Kosten. Mit einigen NetApp -Datendiensten sind Kosten verbunden.https://bluexp.netapp.com/pricing["Informieren Sie sich über die Preise für NetApp Datenservices"^]

So funktioniert die NetApp Console

Die NetApp Console ist eine webbasierte Konsole, die über die SaaS-Schicht, ein Ressourcen- und Zugriffsverwaltungssystem, Konsolenagenten, die Speichersysteme verwalten und NetApp Datendienste aktivieren, sowie verschiedene Bereitstellungsmodi bereitgestellt wird, um Ihren Geschäftsanforderungen gerecht zu werden.

Software-as-a-Service

Sie greifen auf die Konsole zu über eine "webbasierte Schnittstelle" und APIs. Mit dieser SaaS-Erfahrung können Sie automatisch auf die neuesten Funktionen zugreifen, sobald diese veröffentlicht werden.

Identitäts- und Zugriffsverwaltung (IAM)

Die Konsole bietet Identitäts- und Zugriffsverwaltung (IAM) für die Ressourcen- und Zugriffsverwaltung. Dieses IAM-Modell ermöglicht eine detaillierte Verwaltung von Ressourcen und Berechtigungen:

- Eine Top-Level-Organisation ermöglicht Ihnen die Verwaltung des Zugriffs über Ihre verschiedenen Projekte hinweg.
- *Ordner* ermöglichen es Ihnen, verwandte Projekte zusammenzufassen
- Mit der Ressourcenverwaltung können Sie eine Ressource einem oder mehreren Ordnern oder Projekten zuordnen
- Mit der Zugriffsverwaltung können Sie Mitgliedern auf verschiedenen Ebenen der Organisationshierarchie eine Rolle zuweisen
- "Erfahren Sie mehr über IAM in der NetApp Console"

Konsolenagenten

Für einige zusätzliche Funktionen und Datendienste wird ein Konsolenagent benötigt. Es ermöglicht Ihnen, Ressourcen und Prozesse in Ihren lokalen und Cloud-Umgebungen zu verwalten. Sie benötigen es, um einige Systeme zu verwalten (z. B. Cloud Volumes ONTAP) und um einige NetApp -Datendienste zu verwenden.

"Erfahren Sie mehr über Konsolenagenten" .

SaaS versus souveräne Cloud-Bereitstellung

Sie können die NetApp Console nutzen, indem Sie sich für das SaaS-Angebot anmelden oder es in Ihrer eigenen Cloud bereitstellen. Wenn Sie die NetApp Console in einer souveränen Cloud einsetzen, beschränkt NetApp die ausgehende Konnektivität, um die Sicherheits- und Compliance-Anforderungen Ihrer Organisation zu erfüllen. Nicht alle Funktionen und Dienste sind verfügbar, wenn die Konsole in einer souveränen Cloud bereitgestellt wird.

NetApp bietet BlueXP weiterhin für Standorte an, die keine ausgehende Konnektivität benötigen. BlueXP kann in Ihrem Netzwerk ohne ausgehende Verbindungen installiert werden. "Informieren Sie sich über BlueXP (privater Modus) für Websites ohne Internetverbindung."

"Weitere Informationen zu Bereitstellungsmodi" .

SOC 2 Typ 2-Zertifizierung

Eine unabhängige Wirtschaftsprüfungsgesellschaft und ein Wirtschaftsprüfer haben die Konsole geprüft und bestätigt, dass sie SOC 2 Typ 2-Berichte auf Grundlage der geltenden Trust Services-Kriterien erreicht hat.

"Sehen Sie sich die SOC 2-Berichte von NetApp an"

Erfahren Sie mehr über die Bereitstellungsmodi der NetApp Console

Die NetApp Console bietet mehrere Bereitstellungsmodi, mit denen Sie Ihre Geschäfts- und Sicherheitsanforderungen erfüllen können.

- Der *Standardmodus* nutzt eine Software-as-a-Service-Schicht (SaaS), um die volle Funktionalität bereitzustellen. Benutzer greifen über eine webbasierte gehostete Schnittstelle auf die Konsole zu
- Der *Eingeschränkte Modus* ist für Organisationen mit Konnektivitätsbeschränkungen verfügbar, die die NetApp Console in ihrer eigenen öffentlichen Cloud installieren möchten. Benutzer greifen über eine

webbasierte Schnittstelle auf die Konsole zu, die auf einem Konsolenagenten in ihrer Cloud-Umgebung gehostet wird.

Die NetApp Console schränkt den Datenverkehr, die Kommunikation und die Daten im eingeschränkten Modus ein und Sie müssen sicherstellen, dass Ihre Umgebung (vor Ort und in der Cloud) den erforderlichen Vorschriften entspricht.

Überblick

Jeder Bereitstellungsmodus unterscheidet sich hinsichtlich ausgehender Konnektivität, Standort, Installation, Authentifizierung, Datendiensten und Abrechnungsmethoden.

Standardmodus

Sie nutzen einen SaaS-Dienst über die webbasierte Konsole. Abhängig von den Datendiensten und Funktionen, die Sie verwenden möchten, erstellt ein Konsolenorganisationsadministrator einen oder mehrere Konsolenagenten, um die Daten in Ihrer Hybrid-Cloud-Umgebung zu verwalten.

Dieser Modus verwendet eine verschlüsselte Datenübertragung über das öffentliche Internet.

Eingeschränkter Modus

Sie installieren einen Konsolenagenten in der Cloud (in einer Regierungs-, souveränen oder kommerziellen Region) und dieser verfügt über eine eingeschränkte ausgehende Konnektivität zur NetApp Console SaaS-Schicht.

Dieser Modus wird normalerweise von staatlichen und lokalen Behörden sowie regulierten Unternehmen verwendet.

Erfahren Sie mehr über die ausgehende Konnektivität zur SaaS-Schicht .

BlueXP -Privatmodus (nur ältere BlueXP Schnittstelle)

Der private BlueXP Modus (alte BlueXP -Schnittstelle) wird normalerweise in lokalen Umgebungen ohne Internetverbindung und mit sicheren Cloud-Regionen verwendet, darunter AWS Secret Cloud, AWS Top Secret Cloud und Azure IL6. NetApp unterstützt diese Umgebungen weiterhin mit der alten BlueXP Schnittstelle."PDF-Dokumentation für den privaten Modus von BlueXP"

Die folgende Tabelle bietet einen Vergleich der NetApp Konsole.

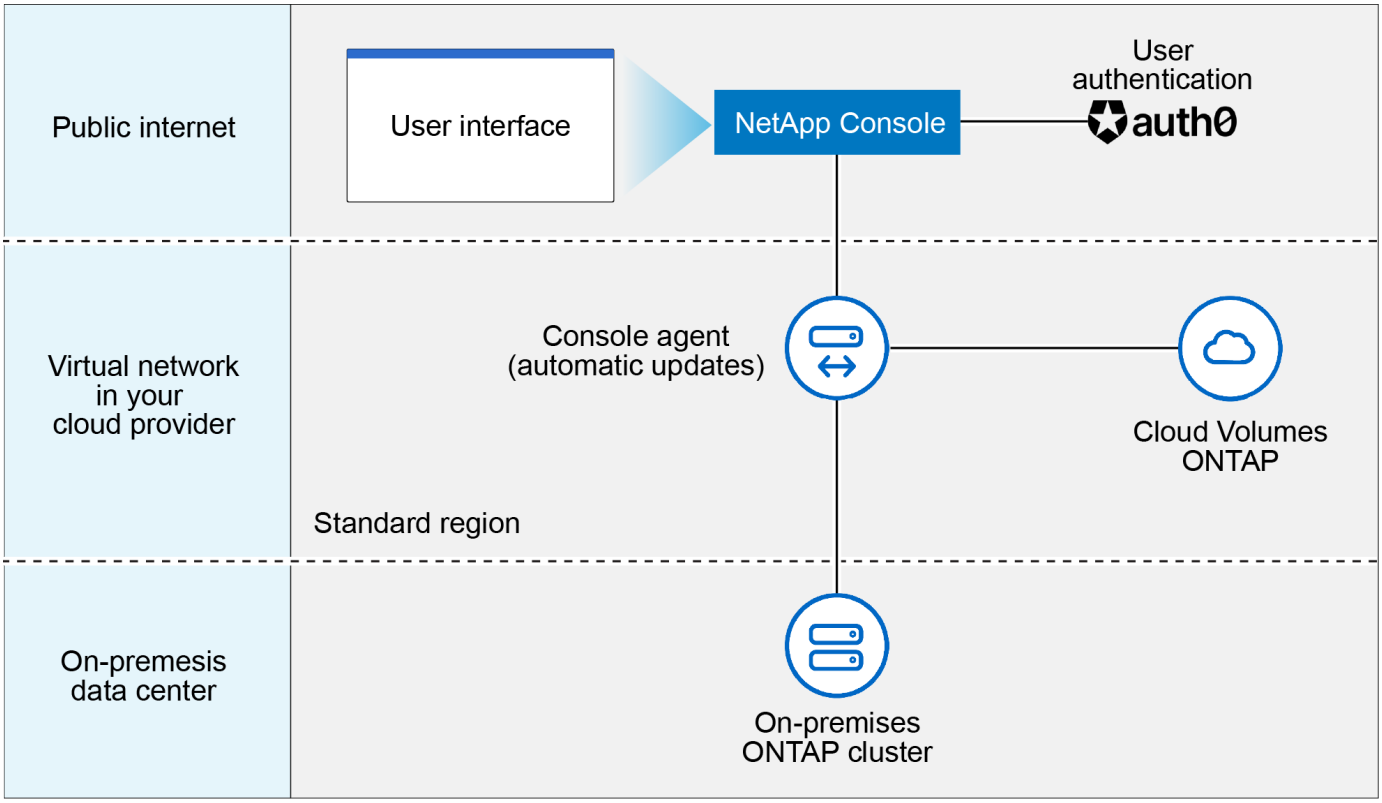
	Standardmodus	Eingeschränkter Modus
Verbindung zur NetApp Console SaaS-Schicht erforderlich?	Ja	Nur ausgehend
Verbindung zu Ihrem Cloud-Anbieter erforderlich?	Ja	Ja, innerhalb der Region
Installation des Konsolenagenten	Über die Konsole, den Cloud-Marktplatz oder die manuelle Installation	Cloud-Marktplatz oder manuelle Installation
Upgrades des Konsolenagenten	Automatische Upgrades	Automatische Upgrades
UI-Zugriff	Von der Konsolen-SaaS-Ebene	Lokal von einer Agent-VM

	Standardmodus	Eingeschränkter Modus
API-Endpunkt	Die Konsolen-SaaS-Schicht	Ein Konsolenagent
Authentifizierung	Über SaaS mit Auth0, NSS-Login oder Identitätsföderation	Durch SaaS mit Auth0 oder Identitätsföderation
Multi-Faktor-Authentifizierung	Verfügbar für lokale Benutzer	Nicht verfügbar
Speicher- und Datendienste	Alle werden unterstützt	Viele werden unterstützt
Lizenzierungsoptionen für Datendienste	Marktplatzabonnements und BYOL	Marktplatzabonnements und BYOL

Lesen Sie die folgenden Abschnitte, um mehr über diese Modi zu erfahren, einschließlich der Informationen darüber, welche Funktionen und Dienste der NetApp Console unterstützt werden.

Standardmodus

Das folgende Bild ist ein Beispiel für eine Bereitstellung im Standardmodus.



Die Konsole funktioniert im Standardmodus wie folgt:

Ausgehende Kommunikation

Für den täglichen Betrieb ist eine Konnektivität von einem Konsolenagenten zur SaaS-Ebene der Konsole, zu den öffentlich verfügbaren Ressourcen Ihres Cloud-Anbieters und zu anderen wichtigen Komponenten erforderlich.

- "Endpunkte, die ein Agent in AWS kontaktiert"

- "Endpunkte, die ein Agent in Azure kontaktiert"
- "Endpunkte, die ein Agent in Google Cloud kontaktiert"

Unterstützter Standort für einen Agenten

Im Standardmodus wird ein Agent in der Cloud oder bei Ihnen vor Ort unterstützt.

Installation des Konsolenagenten

Sie können einen Agenten mit einer der folgenden Methoden installieren:

- Von der Konsole aus
- Vom AWS- oder Azure Marketplace
- Aus dem Google Cloud SDK
- Manuelle Verwendung eines Installationsprogramms auf einem Linux-Host in Ihrem Rechenzentrum oder Ihrer Cloud
- Verwenden Sie die bereitgestellte OVA in Ihrer VCenter-Umgebung.

Upgrades des Konsolenagenten

NetApp führt für Ihren Agenten automatisch monatliche Upgrades durch.p.

Zugriff auf die Benutzeroberfläche

Auf die Benutzeroberfläche kann über die webbasierte Konsole zugegriffen werden, die über die SaaS-Schicht bereitgestellt wird.

API-Endpunkt

API-Aufrufe werden an den folgenden Endpunkt gesendet: https://api.bluexp.netapp.com

Authentifizierung

Authentifizierung mit Auth0- oder NetApp Support Site (NSS)-Anmeldungen. Identitätsföderation ist verfügbar.

Unterstützte Datendienste

Alle NetApp -Datendienste werden unterstützt. "Erfahren Sie mehr über NetApp Datenservices" .

Unterstützte Lizenzierungsoptionen

Marketplace-Abonnements und BYOL werden im Standardmodus unterstützt. Die unterstützten Lizenzierungsoptionen hängen jedoch davon ab, welchen NetApp Datendienst Sie verwenden. Lesen Sie die Dokumentation zu jedem Dienst, um mehr über die verfügbaren Lizenzierungsoptionen zu erfahren.

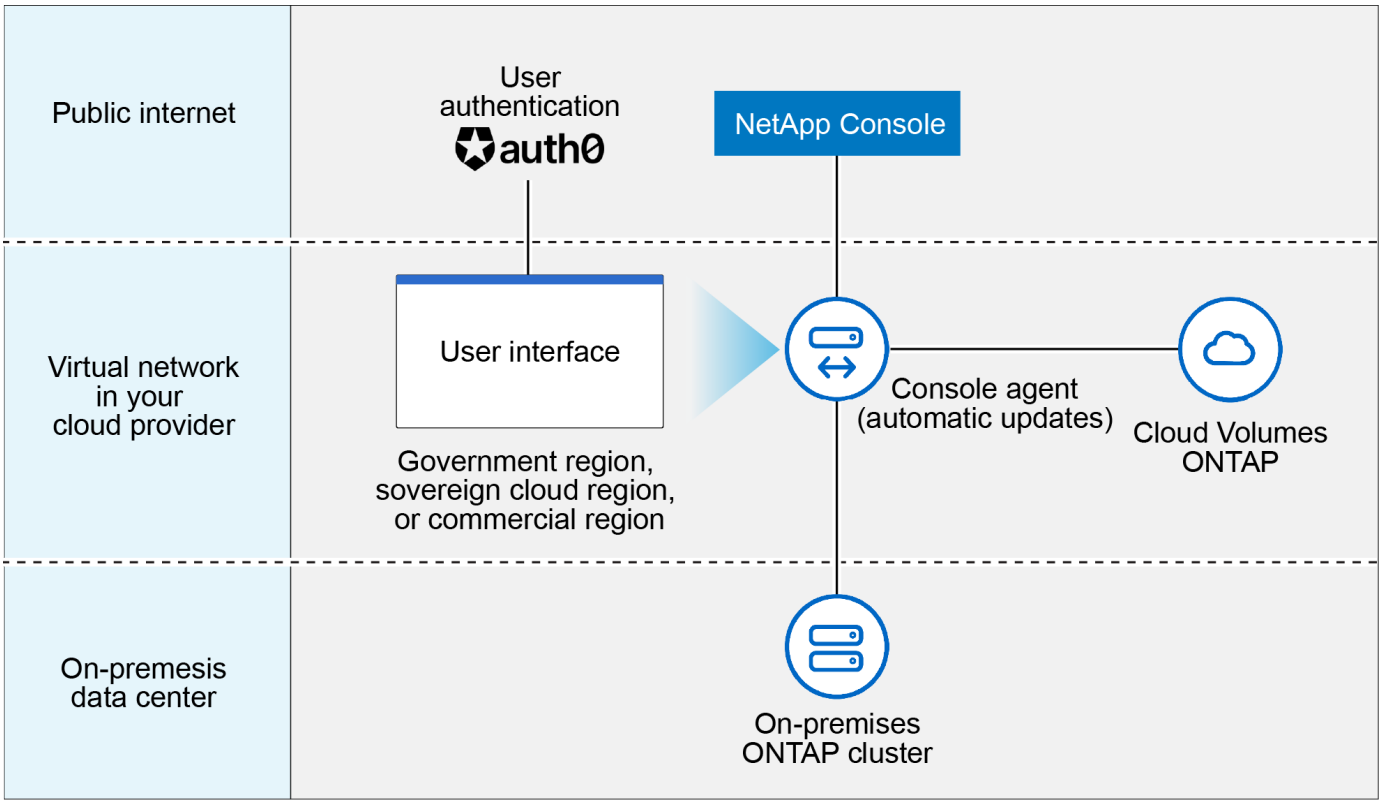
Erste Schritte mit dem Standardmodus

Gehen Sie zum "NetApp Console" und melden Sie sich an.

"Erfahren Sie, wie Sie mit dem Standardmodus beginnen" .

Eingeschränkter Modus

Das folgende Bild ist ein Beispiel für eine Bereitstellung im eingeschränkten Modus.



Im eingeschränkten Modus funktioniert die Konsole wie folgt:

Ausgehende Kommunikation

Ein Agent benötigt eine ausgehende Verbindung zur SaaS-Ebene der Konsole für Datendienste, Software-Upgrades, Authentifizierung und Metadatenübertragung.

Die SaaS-Ebene der Konsole initiiert keine Kommunikation mit einem Agenten. Agenten initiieren die gesamte Kommunikation mit der SaaS-Ebene der Konsole und ziehen oder übertragen Daten nach Bedarf.

Außerdem ist eine Verbindung zu Cloud-Provider-Ressourcen innerhalb der Region erforderlich.

Unterstützter Standort für einen Agenten

Im eingeschränkten Modus wird ein Agent in der Cloud unterstützt: in einer Regierungsregion, einer souveränen Region oder einer kommerziellen Region.

Installation des Konsolenagenten

Sie können die Installation vom AWS- oder Azure Marketplace oder manuell auf Ihrem eigenen Linux-Host durchführen oder eine herunterladbare OVA in Ihrer VCenter-Umgebung verwenden.

Upgrades des Konsolenagenten

NetApp aktualisiert Ihre Agentensoftware automatisch mit monatlichen Updates.

Zugriff auf die Benutzeroberfläche

Auf die Benutzeroberfläche kann von einer Agent-VM aus zugegriffen werden, die in Ihrer Cloud-Region bereitgestellt wird.

API-Endpunkt

Es werden API-Aufrufe an die virtuelle Agentenmaschine gesendet.

Authentifizierung

Die Authentifizierung erfolgt über auth0. Identitätsföderation ist ebenfalls verfügbar.

Unterstützte Speicherverwaltung und Datendienste

Die folgenden Speicher- und Datendienste mit eingeschränktem Modus:

Unterstützte Dienste	Hinweise
Azure NetApp Files	Volle Unterstützung
Sicherung und Wiederherstellung	Wird in Regierungsregionen und kommerziellen Regionen mit eingeschränktem Modus unterstützt. Wird in souveränen Regionen mit eingeschränktem Modus nicht unterstützt. Im eingeschränkten Modus unterstützt NetApp Backup and Recovery nur die Sicherung und Wiederherstellung von ONTAP Volume-Daten. "Sehen Sie sich die Liste der unterstützten Backup-Ziele für ONTAP -Daten an" Das Sichern und Wiederherstellen von Anwendungsdaten und Daten virtueller Maschinen wird nicht unterstützt.
NetApp Data Classification	Wird in Regierungsregionen mit eingeschränktem Modus unterstützt. Wird in kommerziellen Regionen oder in souveränen Regionen mit eingeschränktem Modus nicht unterstützt.
Cloud Volumes ONTAP	Volle Unterstützung
Licenses and subscriptions	Sie können mit den unten aufgeführten unterstützten Lizenzierungsoptionen für den eingeschränkten Modus auf Lizenz- und Abonnementinformationen zugreifen.
On-Premises- ONTAP -Cluster	Sowohl die Erkennung mit einem Konsolenagenten als auch die Erkennung ohne Konsolenagenten (direkte Erkennung) werden unterstützt. Wenn Sie einen lokalen Cluster ohne Konsolenagenten entdecken, wird die erweiterte Ansicht (System Manager) nicht unterstützt.
Replikation	Wird in Regierungsregionen mit eingeschränktem Modus unterstützt. Wird in kommerziellen Regionen oder in souveränen Regionen mit eingeschränktem Modus nicht unterstützt.

Unterstützte Lizenzierungsoptionen

Die folgenden Lizenzierungsoptionen werden im eingeschränkten Modus unterstützt:

- Marktplatz-Abonnements (Stunden- und Jahresverträge)

  Beachten Sie Folgendes:

  - Für Cloud Volumes ONTAP wird nur die kapazitätsbasierte Lizenzierung unterstützt.
  - In Azure werden Jahresverträge mit Regierungsregionen nicht unterstützt.

- BYOL

  Für Cloud Volumes ONTAP werden mit BYOL sowohl kapazitätsbasierte als auch knotenbasierte Lizenzierungen unterstützt.

Erste Schritte mit dem eingeschränkten Modus

Sie müssen den eingeschränkten Modus aktivieren, wenn Sie Ihre NetApp Console Konsolenorganisation erstellen.

Wenn Sie noch keine Organisation haben, werden Sie aufgefordert, Ihre Organisation zu erstellen und den eingeschränkten Modus zu aktivieren, wenn Sie sich zum ersten Mal von einem Konsolenagenten aus bei der Konsole anmelden, den Sie manuell installiert oder im Marktplatz Ihres Cloud-Anbieters erstellt haben.

Sie können die Einstellung für den eingeschränkten Modus nach dem Erstellen der Organisation nicht mehr ändern.

"Erfahren Sie, wie Sie mit dem eingeschränkten Modus beginnen" .

Service- und Funktionsvergleich

Mithilfe der folgenden Tabelle können Sie schnell feststellen, welche Dienste und Funktionen im eingeschränkten Modus unterstützt werden.

Beachten Sie, dass einige Dienste möglicherweise nur eingeschränkt unterstützt werden. Weitere Einzelheiten zur Unterstützung dieser Dienste im eingeschränkten Modus finden Sie in den obigen Abschnitten.

Produktbereich	NetApp -Datendienst oder -Funktion	Eingeschränkter Modus
Speicher Dieser Teil der Tabelle listet die Unterstützung für die Verwaltung von Speichersystemen über die Konsole auf. Es werden nicht die unterstützten Sicherungsziele für NetApp Backup and Recovery angezeigt.	Amazon FSx für ONTAP	Nein
	Amazon S3	Nein
	Azure-Blob	Nein
	Azure NetApp Files	Ja
	Cloud Volumes ONTAP	Ja
	Google Cloud NetApp Volumes	Nein
	Google Cloud-Speicher	Nein
	On-Premises- ONTAP -Cluster	Ja
	E-Series	Nein
	StorageGRID	Nein

Produktbereich	NetApp -Datendienst oder -Funktion	Eingeschränkter Modus
Datendienste	NetApp Backup und Recovery	Jahttps://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-limited-internet-connectivity["Liste der unterstützten Backup-Ziele für ONTAP Volume-Daten anzeigen"^]
	NetApp Data Classification	Ja
	NetApp Copy and Sync	Nein
	NetApp Disaster Recovery	Nein
	NetApp Ransomware Resilience	Nein
	NetApp Replication	Ja
	NetApp Cloud Tiering	Nein
	NetApp Volume-Caching	Nein
	NetApp Workload Factory	Nein
Merkmale	Warnungen	Nein
	Digital Advisor	Nein
	Lizenz- und Abonnementverwaltung	Ja
	Identitäts- und Zugriffsverwaltung	Ja
	Anmeldeinformationen	Ja
	Föderation	Ja
	Lebenszyklusplanung	Nein
	Multi-Faktor-Authentifizierung	Ja
	NSS-Konten	Ja
	Benachrichtigungen	Ja
	Suche	Ja
	Software-Updates	Nein
	Nachhaltigkeit	Nein
	Prüfung	Ja

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

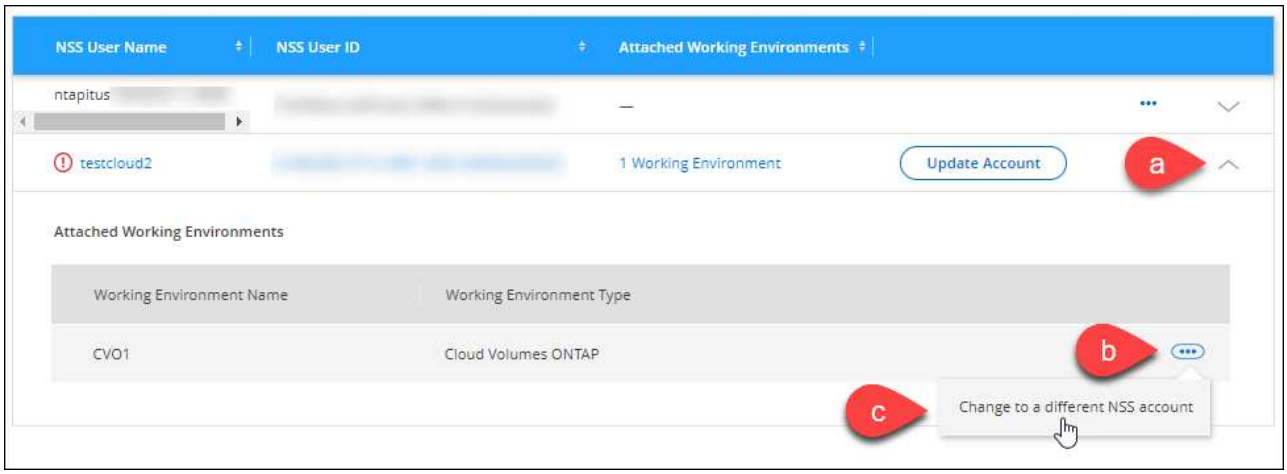
Wenn Ihr Unternehmen über mehrere NetApp Support Site-Konten verfügt, können Sie ändern, welches Konto mit einem Cloud Volumes ONTAP -System verknüpft ist.

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**.

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.

Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der NetApp Console

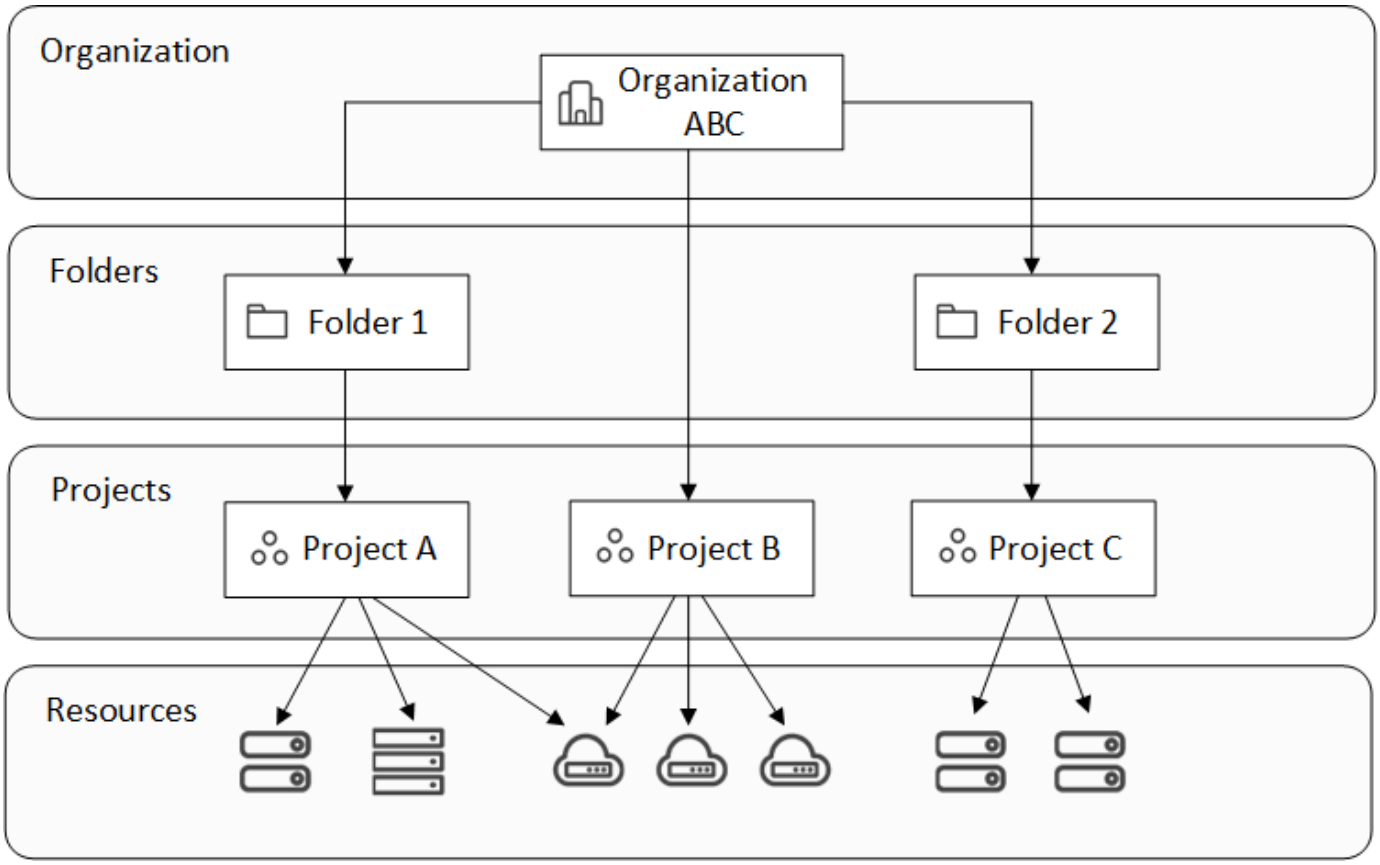
Mit der Identitäts- und Zugriffsverwaltung (IAM) der NetApp Console können Sie Ihre NetApp -Ressourcen organisieren und den Zugriff entsprechend Ihrer Unternehmensstruktur steuern – nach Standort, Abteilung oder Projekt.

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 Mitgliedern auf Organisations-, Ordner- oder Projektebene rollenbasierte Zugriffskontrollberechtigungen (RBAC) zu, um sicherzustellen, dass die Benutzer den entsprechenden 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

Zu den Ressourcen gehören Speichersysteme, Keystone Abonnements 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 der NetApp Console verwalten. Die NetApp Console unterstützt die Verwaltung von sowohl lokalen als auch Cloud-Speichersystemen. Bevor jemand auf ein Projekt zugreifen kann, muss diesem ein Speichersystem hinzugefügt werden.

Speichersysteme werden automatisch dem Projekt zugeordnet, in dem sie hinzugefügt werden. Sie können sie aber auch über die Seite **Ressourcen** mit anderen Projekten oder Ordnern verknüpfen.

Keystone -Abonnements sind außerdem Ressourcen, die Sie Projekten zuordnen können, um Benutzern Zugriff auf das Abonnement in der NetApp Console zu gewähren.

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 der NetApp Console (SaaS)

Workflow für den Einstieg (SaaS)

Beginnen Sie mit der NetApp Console (SaaS), indem Sie die Netzwerkkonfiguration für die Console vorbereiten, sich anmelden und ein Konto erstellen und mithilfe des Console-

Assistenten die grundlegenden Funktionen einrichten.

Sie greifen auf eine webbasierte Konsole zu, die als Software-as-a-Service (SaaS)-Produkt von NetApp gehostet wird. Mit der Konsole können Sie Ihre Hybrid-Cloud-Speicherumgebung verwalten und NetApp Datendienste nutzen.

1 "Vorbereiten des Netzwerks für die Verwendung der NetApp Konsole"

Stellen Sie sicher, dass die Computer, die auf die NetApp Konsole zugreifen, über Netzwerkzugriff auf die erforderlichen Endpunkte verfügen.

"Erfahren Sie, wie Sie die Netzwerkverbindung für die NetApp -Konsole vorbereiten."

2 "Registrieren und eine Organisation erstellen"

Gehe zu "NetApp Konsole" und melde dich an. Wenn Sie aufgefordert werden, eine Organisation zu erstellen, und Sie der Meinung sind, dass für Ihr Unternehmen bereits eine Organisation existiert, schließen Sie das Dialogfeld und informieren Sie Ihren Organisationsadministrator. Falls es in Ihrem Unternehmen derzeit keinen Organisationsadministrator gibt, können Sie diese Rolle beanspruchen. "Erfahren Sie, wie Sie einen Organisationsadministrator kontaktieren können."

An diesem Punkt sind Sie angemeldet und können den NetApp Assistenten verwenden, um mit der Konfiguration der Konsole zu beginnen. Um den vollen Funktionsumfang zu aktivieren, müssen Sie zunächst Ihr NetApp Supportkonto und einen Console-Agenten verknüpfen.

Wenn Sie sich gegen die Verwendung des NetApp Assistenten oder die Installation eines Konsolenagenten entscheiden, können Sie mit der Speicherverwaltung und der Nutzung von Diensten wie Digital Advisor, Amazon FSx for ONTAP, Azure NetApp Files und anderen beginnen. "Erfahren Sie, was Sie ohne Konsolenagent tun können"Die

3 Verknüpfen Sie Ihr NetApp Support Site (NSS)-Konto

Durch die Verknüpfung Ihres NetApp Support Site (NSS)-Kontos mit der Konsole können Sie Ihre Lizenzen und Abonnements einfacher verwalten sowie direkt über die Konsole auf Supportressourcen zugreifen.

4 Erstellen Sie einen Konsolenagenten

Für erweiterte Speicherverwaltungsfunktionen und einige NetApp Datendienste ist die Installation eines Konsolenagenten erforderlich. Der Konsolenagent ermöglicht der Konsole die Verwaltung von Ressourcen und Prozessen innerhalb Ihrer Hybrid-Cloud-Umgebung.

Sie können einen Konsolenagenten in Ihrer Cloud oder Ihrem lokalen Netzwerk erstellen.

- "Erfahren Sie mehr darüber, wann Konsolenagenten erforderlich sind und wie sie funktionieren"
- "Erfahren Sie, wie Sie einen Konsolenagenten in AWS erstellen"
- "Erfahren Sie, wie Sie einen Konsolen-Agent in Azure erstellen"
- "Erfahren Sie, wie Sie einen Konsolenagenten in Google Cloud erstellen"
- "Erfahren Sie, wie Sie einen Konsolenagenten vor Ort erstellen"

5 **Füge der Konsole ein Speichersystem hinzu.**

In der NetApp Console können Sie Speichersysteme hinzufügen oder entdecken, um Ihre hybride Cloud-Speicherumgebung zu verwalten. Verwenden Sie den NetApp Assistenten, um Ihr erstes Speichersystem hinzuzufügen.

Wenn Sie einen Console-Agenten in AWS, Microsoft Azure oder Google Cloud installieren, ermittelt die Console automatisch Informationen über die Amazon S3-Buckets, Azure Blob Storage- oder Google Cloud Storage-Buckets an dem Ort, an dem der Agent installiert ist. Diese Systeme werden automatisch zur Seite **Systeme** hinzugefügt.

- "Erfahren Sie, wie Sie ein ONTAP System entdecken können."
- "Erfahren Sie, wie Sie ein StorageGRID System entdecken können."
- "Erfahren Sie, wie Sie ein E-Series-System entdecken können."

6 **"Abonnieren Sie NetApp Intelligent Services (optional)"**

Melden Sie sich über Ihren Cloud-Anbieter für NetApp Intelligent Services an und wählen Sie zwischen stündlicher (PAYGO) oder jährlicher Abrechnung. Ein Abonnement umfasst NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience, NetApp Disaster Recovery und NetApp Data Classification.

Netzwerkzugriff für die NetApp Console vorbereiten

NetApp Console, der NetApp Console Agent und NetApp Datendienste erfordern ausgehenden Internetzugang und die Möglichkeit, die erforderlichen Endpunkte zu kontaktieren.

Sie müssen den Netzwerkzugriff für Folgendes einrichten:

- Computer, die als Software as a Service (SaaS) auf die NetApp Console zugreifen
- Konsolenagenten, die Sie vor Ort oder in der Cloud installieren. Konsolenagenten.

Mit 4.0.0 hat NetApp die erforderlichen Netzwerkendpunkte für die Konsole und Konsolenagenten reduziert, wodurch die Sicherheit verbessert und die Bereitstellung vereinfacht wird. Wichtig ist, dass alle Bereitstellungen vor Version 4.0.0 weiterhin vollständig unterstützt werden. Während vorherige Endpunkte für vorhandene Agenten weiterhin verfügbar bleiben, empfiehlt NetApp dringend, die Firewall-Regeln auf die aktuellen Endpunkte zu aktualisieren, nachdem die erfolgreichen Agent-Upgrades bestätigt wurden."Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren."

Von der NetApp Console und den Konsolenagenten kontaktierte Endpunkte

Jeder von Ihnen bereitgestellte Agent und jeder Computer, der auf die NetApp Console zugreift, muss über Verbindungen zu den unten aufgeführten Endpunkten verfügen.

Konsolenagenten, die bei Ihrem Cloud-Anbieter bereitgestellt werden, benötigen Zugriff auf die jeweiligen Endpunkte dieses Cloud-Anbieters.

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.
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.

Cloud-Provider-Endpunkte haben den Konsolen-Agenten kontaktiert

Konsolenagenten müssen Zugriff auf zusätzliche Endpunkte haben, wenn diese bei Ihrem Cloud-Anbieter bereitgestellt werden.

Richten Sie den Netzwerk-Endpunktzugriff des Cloud-Anbieters ein, bevor Sie den Konsolen-Agenten installieren.

- "Einrichten des AWS-Netzwerkzugriffs für einen Konsolenagenten"
- "Einrichten des Azure-Netzwerkzugriffs für einen Konsolen-Agent"
- "Einrichten des Google Cloud-Netzwerkzugriffs für einen Konsolenagenten"

Vom Konsolenagenten kontaktierte Datendienstendpunkte

Einige NetApp -Datendienste sowie Cloud Volumes ONTAP erfordern, dass der Agent über zusätzlichen ausgehenden Internetzugang verfügt.

Endpunkte für Cloud Volumes ONTAP

- "Endpunkte für Cloud Volumes ONTAP in AWS"
- "Endpunkte für Cloud Volumes ONTAP in Azure"
- "Endpunkte für Cloud Volumes ONTAP in Google Cloud"

Endpunkte für Workloads

Der Console-Agent muss für NetApp -Workloads auf den folgenden Endpunkt zugreifen können.

Endpunkte	Zweck
https://api.workloads.netapp.com	Die webbasierte Konsole kontaktiert diesen Endpunkt, um mit den Workload Factory APIs zu interagieren und FSx for ONTAP-basierte Workloads zu verwalten und zu betreiben.

Registrieren oder bei der NetApp Console anmelden

Um die Konsole zu nutzen, registrieren Sie sich oder melden Sie sich mit Ihren NetApp Support Site-Zugangsdaten an oder erstellen Sie ein NetApp Console Login. Wenn Sie sich als Erster aus Ihrem Unternehmen anmelden, erstellen Sie als Administrator eine neue Organisation. Falls Ihr Unternehmen bereits über eine Organisation verfügt, registrieren Sie sich oder melden Sie sich mit Ihren bestehenden NetApp Support Site-Zugangsdaten oder Ihrem unternehmensinternen Single Sign-On (SSO) an.

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 wird zum Organisationsadministrator und verwaltet Benutzerkonten und Berechtigungen. Sie können die Rollen aktualisieren und später weitere Administratoren 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 Benutzer und Organisationsadministrator folgen Sie einem geführten Prozess, um Speicherressourcen 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.

Erste Schritte mit dem NetApp Console Assistenten

Wenn Sie die NetApp Console (SaaS) zum ersten Mal mit der Rolle eines Organisationsadministrators verwenden, können Sie sich mithilfe des Console-Assistenten durch den Ersteinrichtungsprozess führen lassen. Der Assistent hilft Ihnen beim Hinzufügen eines NetApp Support Site (NSS)-Kontos, eines Console-Agenten, eines Clusters sowie einer Lizenz oder eines Abonnements und erleichtert Ihnen so den Einstieg in die Datenverwaltung.

Erforderliche Rollen für den Zugriff auf den Konsolenassistenten

Der Konsolenassistent ist nur für Benutzer mit der Rolle „Organisationsadministrator“ verfügbar.

Standardmäßig wird der Konsolenassistent auf der Startseite der NetApp Console für Erstbenutzer mit der Rolle „Organisationsadministrator“ angezeigt. Es bleibt so lange verfügbar, bis Sie die obligatorischen Aufgaben der Erstellung eines Konsolenagenten und des Hinzufügens eines Systems abgeschlossen haben.

Nutzen Sie den Assistenten, um diese Aufgaben zu erledigen. Dadurch wird die minimale Einrichtung Ihrer NetApp Console Umgebung sichergestellt:

- Fügen Sie ein NetApp Support Site (NSS)-Konto hinzu.

  "Erfahren Sie, wie Sie ein NSS-Konto hinzufügen."Die

- Stellen Sie eine Verbindung zu Ihrem Speichersystem her, indem Sie einen Console-Agenten einsetzen.

  "Erfahren Sie, wie Sie einen Console-Agenten lokal installieren."

- Verwalten Sie ein Speichersystem durch Hinzufügen oder Erkennen eines Clusters
- Fügen Sie ein Marktplatzabonnement oder eine PAYGO-Lizenz hinzu.

  "Erfahren Sie, wie Sie Lizenzen und Abonnements hinzufügen."Die

- Informationen zu Datendiensten prüfen.

Erste Schritte mit der NetApp Console (eingeschränkter Modus)

Workflow „Erste Schritte“ (eingeschränkter Modus)

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

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

1 **"Vorbereiten der Bereitstellung"**

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

2 **"Bereitstellen des Konsolenagenten"**

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

3 **"Abonnieren Sie NetApp Intelligent Services (optional)"**

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

Vorbereiten der Bereitstellung im eingeschränkten Modus

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

Schritt 1: Verstehen, wie der eingeschränkte Modus funktioniert

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

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

Darüber hinaus sind nicht alle Konsolenfunktionen und NetApp Datendienste verfügbar.

"Erfahren Sie, wie der eingeschränkte Modus funktioniert" .

Schritt 2: Überprüfen der Installationsoptionen

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

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

Schritt 3: Hostanforderungen prüfen

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

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

Dedizierter Host

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

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

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

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

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

AWS EC2-Instanztyp

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

Azure-VM-Größe

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

Google Cloud-Maschinentyp

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

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

Hypervisor

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

Betriebssystem- und Containeranforderungen

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

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

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

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

Schritt 4: Installieren Sie Podman oder Docker Engine

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

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

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

  Sehen Sie sich die unterstützten Podman-Versionen an .

- Für Ubuntu ist Docker Engine erforderlich.

  Anzeigen der unterstützten Docker Engine-Versionen .

Beispiel 1. Schritte

Podman

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

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

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

Schritte

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

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

2. Installieren Sie Podman.

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

   a. Für Red Hat Enterprise Linux 9,6:

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

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

   b. Für Red Hat Enterprise Linux 9.1 bis 9.4:

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

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

   c. Für Red Hat Enterprise Linux 8:

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

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

unterstützten Podman-Versionen an .

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

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

4. Installieren Sie python3.

```
sudo dnf install python3
```

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

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

6. Bei Verwendung von Red Hat Enterprise 9:

   a. Installieren Sie das EPEL-Repository-Paket.

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

   +

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

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

7. Bei Verwendung von Red Hat Enterprise Linux 8:

   a. Installieren Sie das EPEL-Repository-Paket.

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

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

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. Starten Sie Podman neu.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker-Engine

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

Schritte

1. "Installationsanweisungen von Docker anzeigen"

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

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

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

Schritt 5: Netzwerkzugriff vorbereiten

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

Verbindungen zu Zielnetzwerken

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

Vorbereiten des Netzwerks für den Benutzerzugriff auf die NetApp Console

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

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

+

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

Ausgehender Internetzugang für den täglichen Betrieb

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

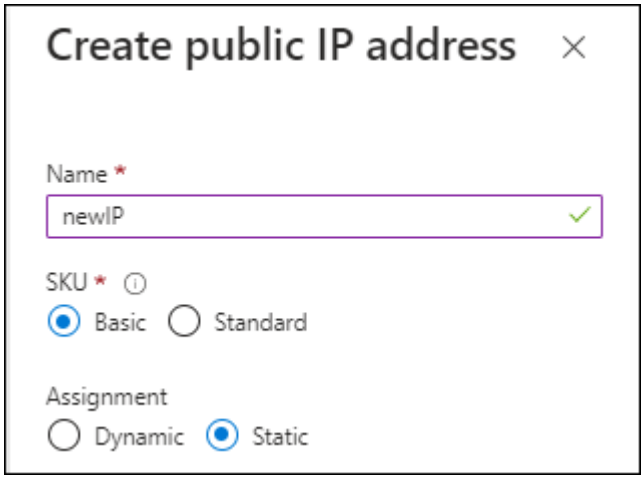
Endpunkte	Zweck
AWS-Umgebungen	AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)
Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt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

Endpunkte	Zweck
Zum Verwalten von Ressourcen in Google Cloud.	• NetApp Console -Endpunkte*
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.

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

Öffentliche IP-Adresse in Azure

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



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

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

"Azure-Dokumentation: Öffentliche IP-SKU"

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

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

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

Aktivieren von NTP

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

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

Schritt 6: Cloud-Berechtigungen vorbereiten

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

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

AWS IAM-Rolle

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

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

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

Schritte

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

Ergebnis

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

AWS-Zugriffsschlüssel

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

Schritte

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

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

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

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

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

Azure-Rolle

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

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

Schritte

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

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

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

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

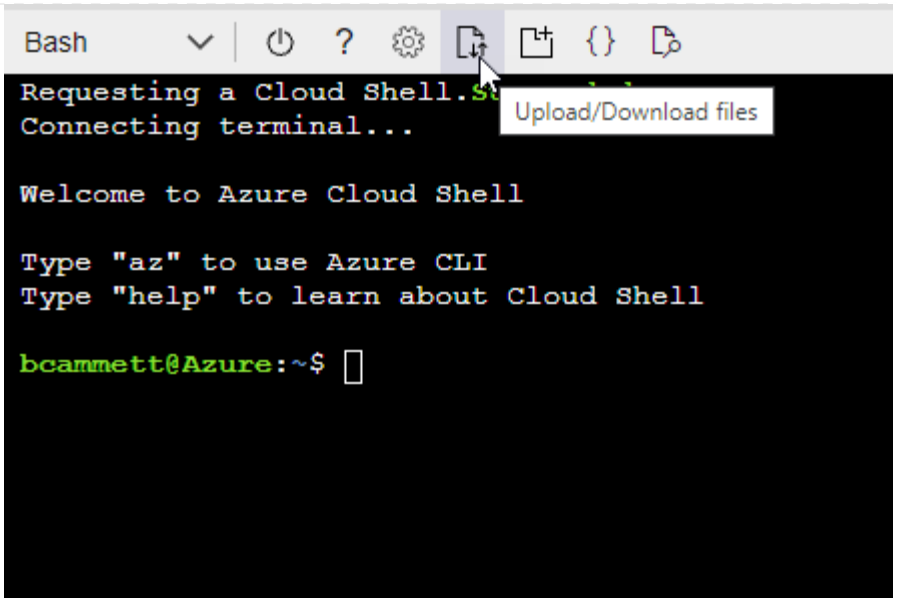
   Beispiel

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

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

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

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



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

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

Azure-Dienstprinzipal

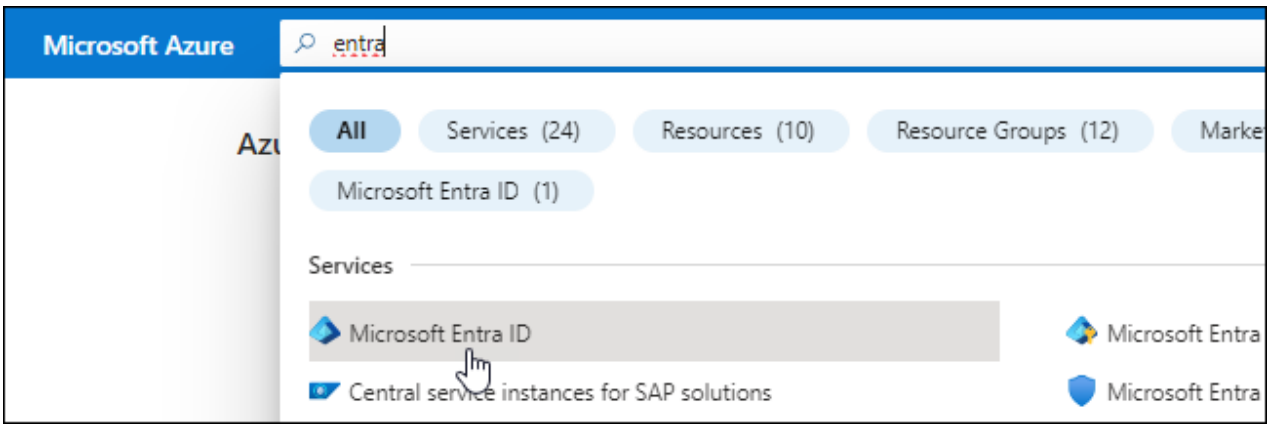
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die die Konsole benötigt. Sie müssen der Konsole diese Anmeldeinformationen bereitstellen, nachdem Sie den Konsolenagenten installiert haben.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffskontrolle

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

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

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



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

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

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der Anwendung zu einer Rolle

1. Erstellen Sie eine benutzerdefinierte Rolle:

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

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

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

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

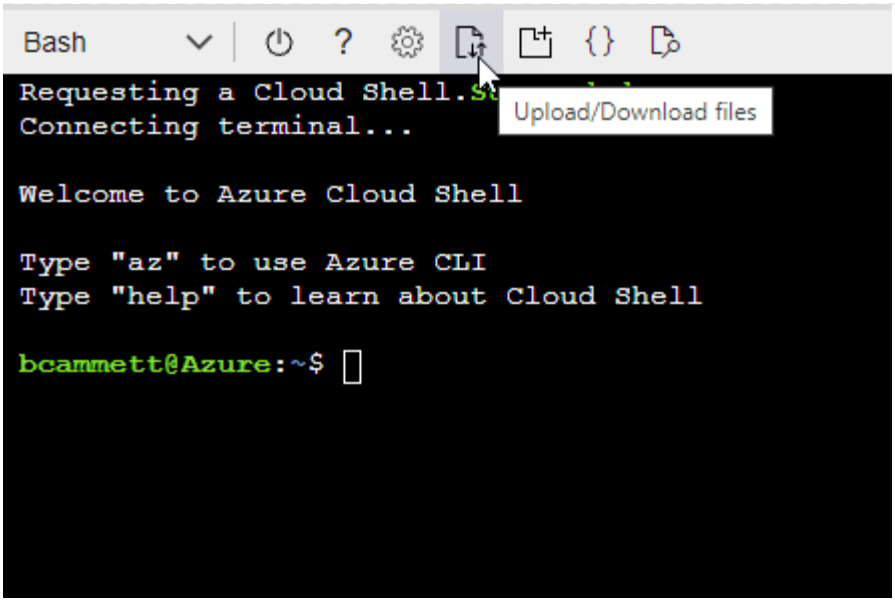
      Beispiel

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

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

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

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



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

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

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

2. Weisen Sie die Anwendung der Rolle zu:

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

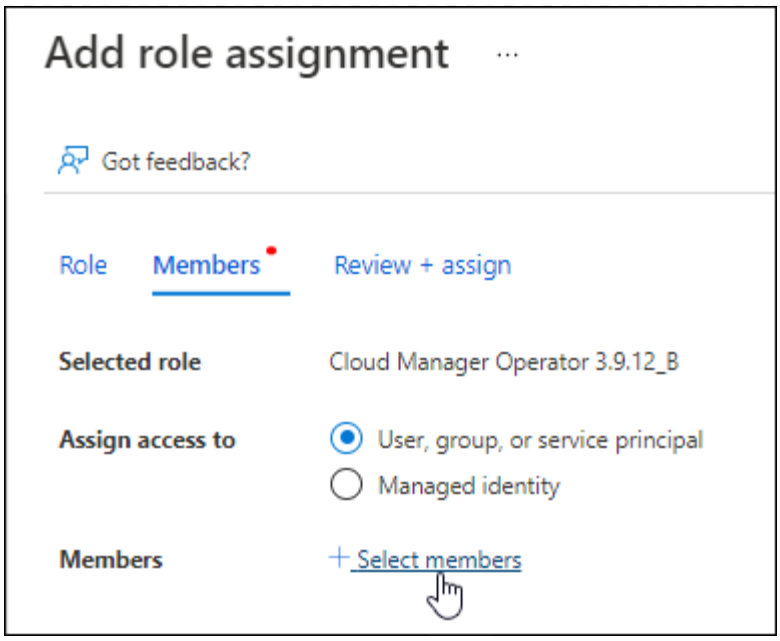
   b. Wählen Sie das Abonnement aus.

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

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

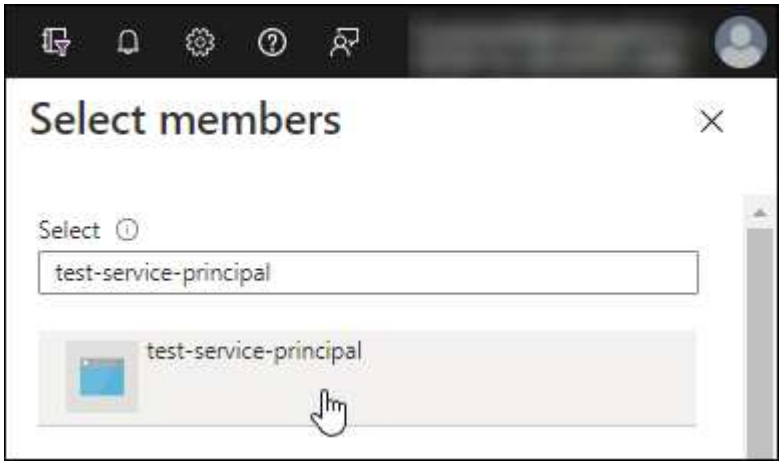
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

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



- Suchen Sie nach dem Namen der Anwendung.

  Hier ist ein Beispiel:



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

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

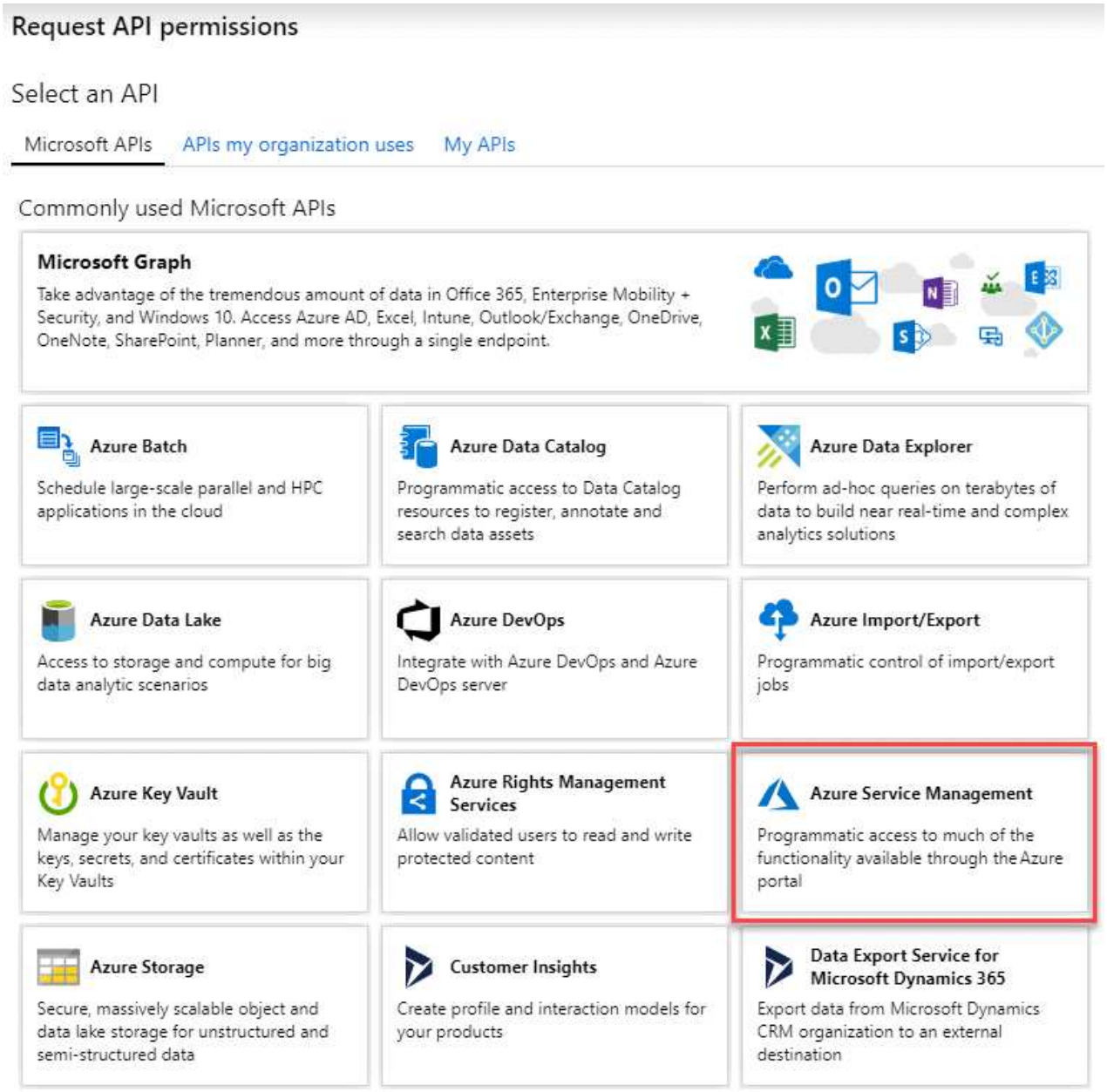
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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

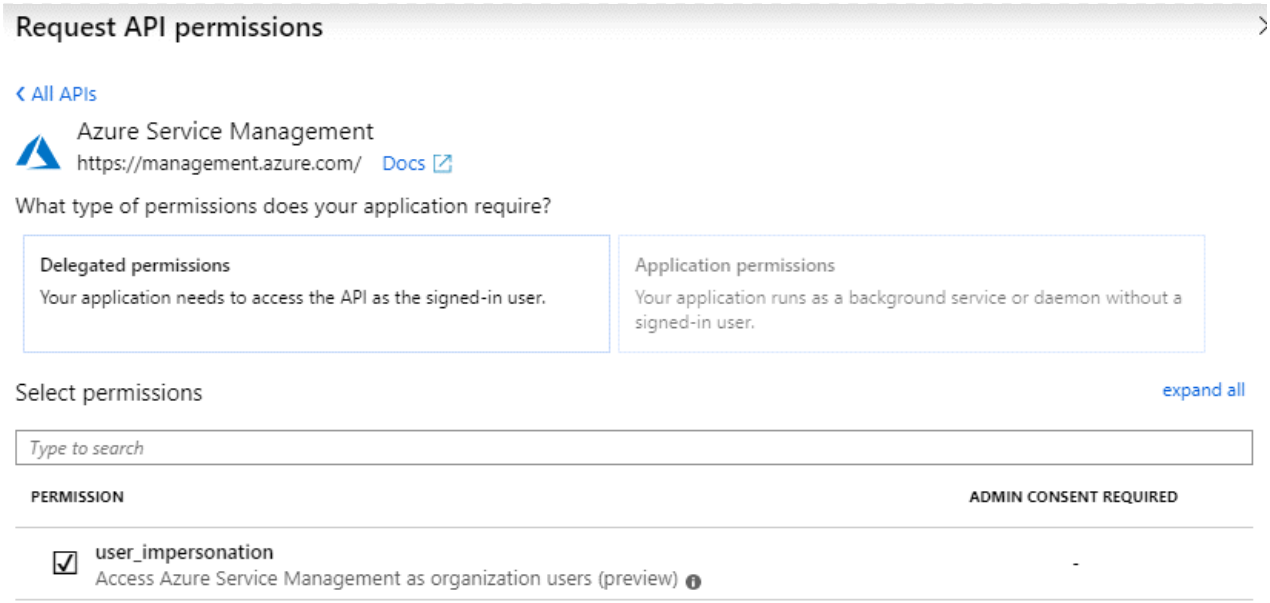
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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

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

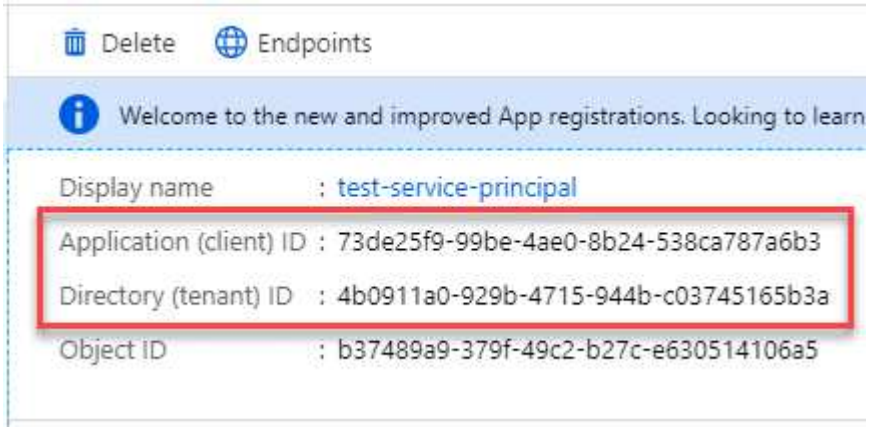


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

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



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

Erstellen eines Client-Geheimnisses

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

Ergebnis

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

Google Cloud-Dienstkonto

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

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in Google Cloud:

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

   b. Aktivieren Sie Cloud Shell in Google Cloud.

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

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

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

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

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

2. Erstellen Sie ein Dienstkonto in Google Cloud:

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

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

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

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

      "Google Cloud-Dokumente: Erstellen eines Dienstkontos"

Schritt 7: Google Cloud APIs aktivieren

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

Schritt

1. "Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt"
    - Cloud Infrastructure Manager API
    - Cloud Deployment Manager V2 API
    - Cloud Logging API
    - Cloud Resource Manager-API
    - Compute Engine-API
    - API für Identitäts- und Zugriffsverwaltung (IAM)
    - Cloud Key Management Service (KMS)-API

      (Nur erforderlich, wenn Sie NetApp Backup and Recovery mit vom Kunden verwalteten Verschlüsselungsschlüsseln (CMEK) verwenden möchten)

Bereitstellen des Konsolenagenten im eingeschränkten Modus

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

Schritt 1: Installieren des Konsolenagenten

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

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

AWS Commercial Marketplace

Bevor Sie beginnen

Halten Sie Folgendes bereit:

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

  "Informieren Sie sich über die Netzwerkanforderungen"

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

  "Erfahren Sie, wie Sie AWS-Berechtigungen einrichten"

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

  "Überprüfen Sie die Agentenanforderungen".

- Ein Schlüsselpaar für die EC2-Instanz.

Schritte

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

   Der Abonnementvorgang kann einige Minuten dauern.

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

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

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

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

          "Sicherheitsgruppenregeln für AWS anzeigen" .

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

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

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

Ergebnis

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

Wie geht es weiter?

Richten Sie die NetApp Console ein.

AWS Gov Marketplace

Bevor Sie beginnen

Halten Sie Folgendes bereit:

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

  "Informieren Sie sich über die Netzwerkanforderungen"

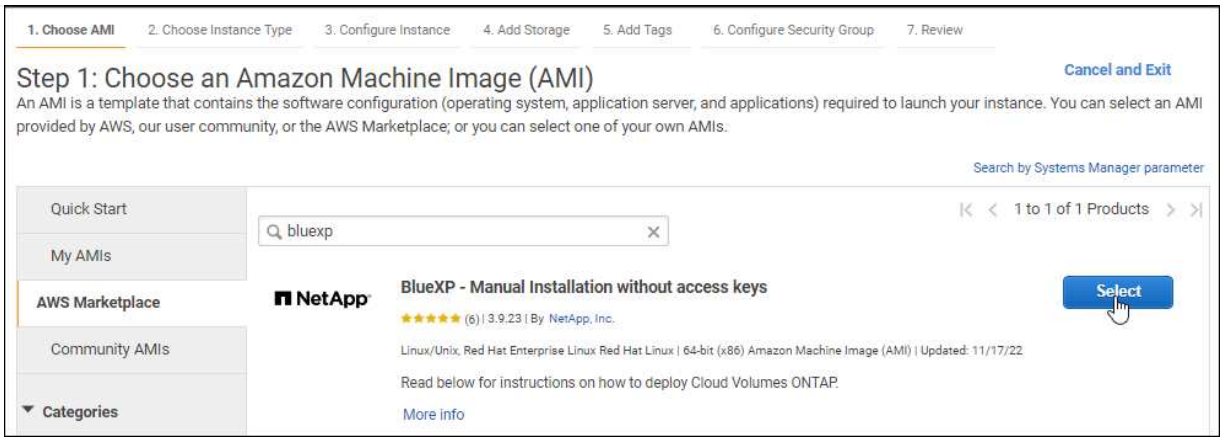
- Eine IAM-Rolle mit einer angehängten Richtlinie, die die erforderlichen Berechtigungen für den Konsolenagenten enthält.

  "Erfahren Sie, wie Sie AWS-Berechtigungen einrichten"

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

Schritte

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



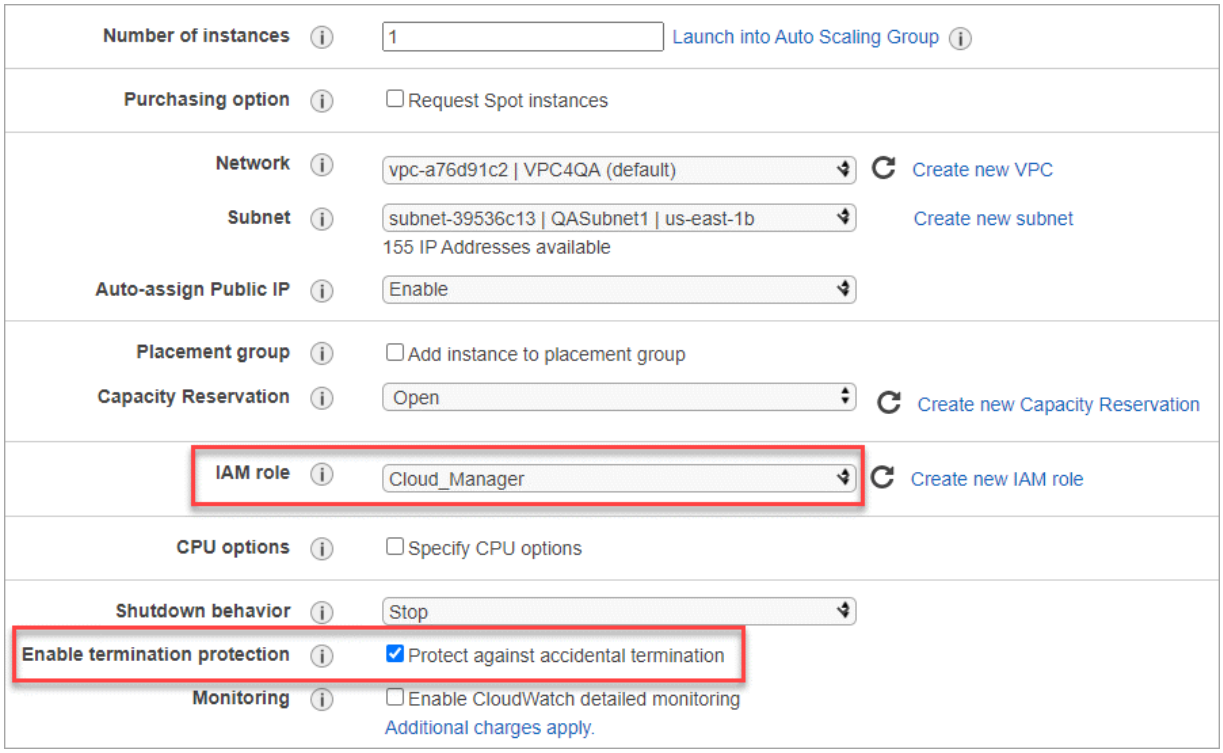
d. Wählen Sie **Weiter**.

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

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

     "Überprüfen der Instanzanforderungen" .

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



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

Ergebnis

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

Wie geht es weiter?

Richten Sie die Konsole ein.

Azure Gov Marketplace

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Ein VNet und Subnetz, das die Netzwerkanforderungen erfüllt.

  "Informieren Sie sich über die Netzwerkanforderungen"

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

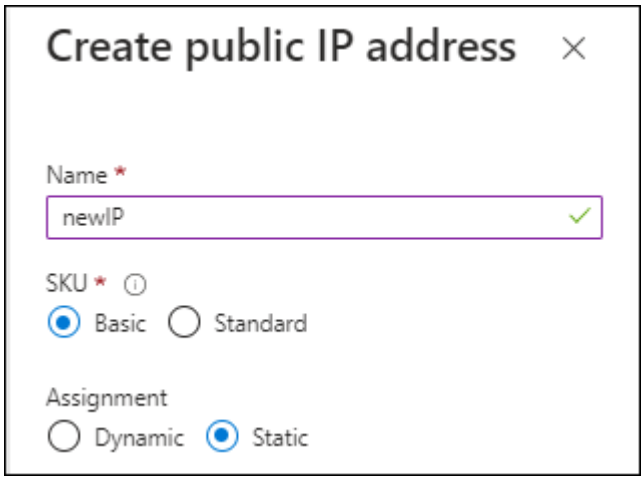
  "Erfahren Sie, wie Sie Azure-Berechtigungen einrichten"

Schritte

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

   Beachten Sie beim Konfigurieren der VM Folgendes:

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



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

"Azure-Dokumentation: Öffentliche IP-SKU"

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

  "Anzeigen von Sicherheitsgruppenregeln für Azure" .

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

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

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

Ergebnis

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

Wie geht es weiter?

Richten Sie die NetApp Console ein.

Manuelle Installation (muss für Google Cloud verwendet werden)

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

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

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

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

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

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

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

Informationen zu diesem Vorgang

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

Schritte

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

   ```
   unset http_proxy
   unset https_proxy
   ```

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

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

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

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

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

3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

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

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

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

5. Führen Sie das Installationsskript aus.

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

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

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

+

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

+

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

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

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

+ Beachten Sie Folgendes:

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

+ Zum Beispiel:

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

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

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

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

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

      Beispiel:

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

a. Starten Sie die virtuelle Maschine des Konsolenagenten neu.

Ergebnis

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

Wie geht es weiter?

Richten Sie die NetApp Console ein.

Schritt 2: NetApp Console einrichten

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

Bevor Sie beginnen

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

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

Schritte

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

   a. Geben Sie einen Namen für den Konsolenagenten ein.

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

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

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

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

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

a. Wählen Sie **Los geht's**.

Ergebnis

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

Wie geht es weiter?

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

Schritt 3: Erteilen Sie dem Konsolenagenten Berechtigungen

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

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

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

AWS IAM-Rolle

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

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

Schritte

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

AWS-Zugriffsschlüssel

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

Schritte

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

Azure-Rolle

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

Schritte

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

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

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

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

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

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

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

Azure-Dienstprinzipal

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

Schritte

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

Ergebnis

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

Google Cloud-Dienstkonto

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

Schritte

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

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

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

Abonnieren Sie NetApp Intelligent Services (eingeschränkter Modus)

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

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

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

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

Bevor Sie beginnen

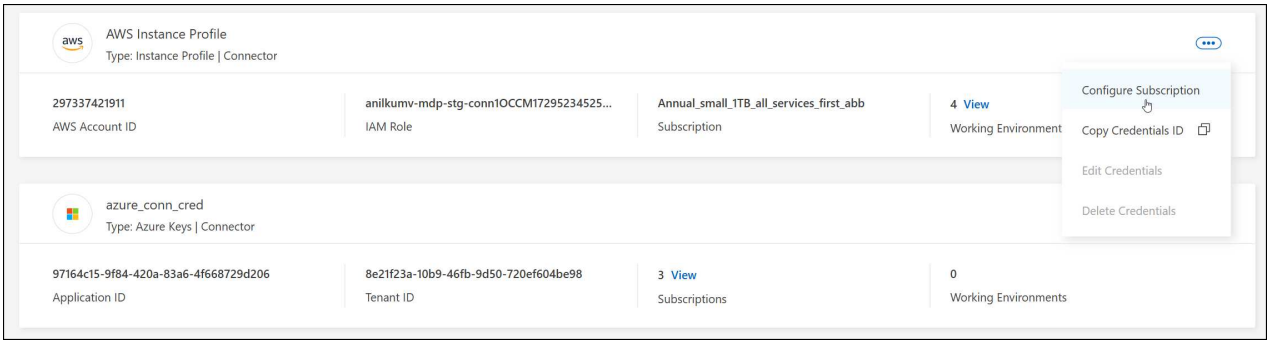
Sie müssen bereits einen Konsolenagenten bereitgestellt haben, um Datendienste abonnieren zu können. Sie müssen den mit einem Konsolenagenten verbundenen Cloud-Anmeldeinformationen ein Marktplatzabonnement zuordnen.

AWS

Schritte

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

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



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

   a. Wählen Sie **Kaufoptionen anzeigen**.

   b. Wählen Sie **Abonnieren**.

   c. Wählen Sie **Konto einrichten**.

      Sie werden zur NetApp Console weitergeleitet.

   d. Auf der Seite **Abonnementzuweisung**:

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

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

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

   - Wählen Sie **Speichern**.

Azurblau

Schritte

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

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

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

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

      Sie werden zur NetApp Console weitergeleitet.

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

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

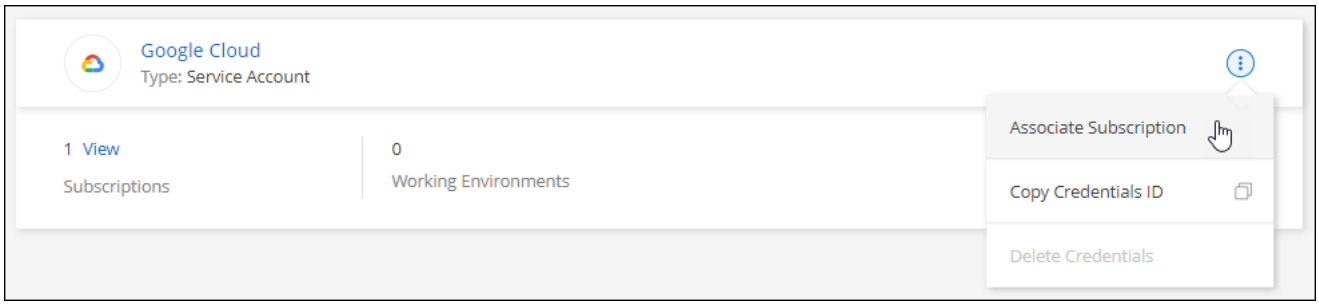
   Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.

   ◦ Wählen Sie **Speichern**.

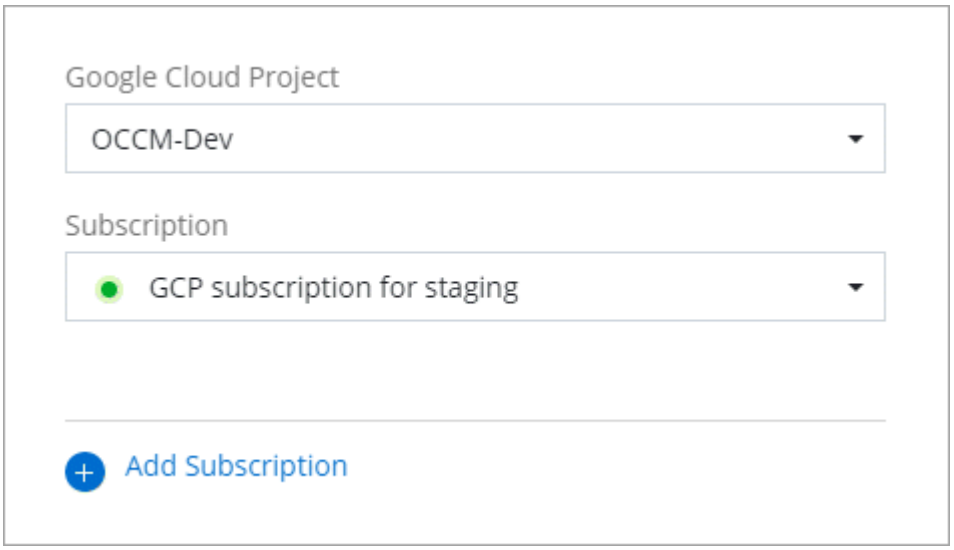
Google Cloud

Schritte

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



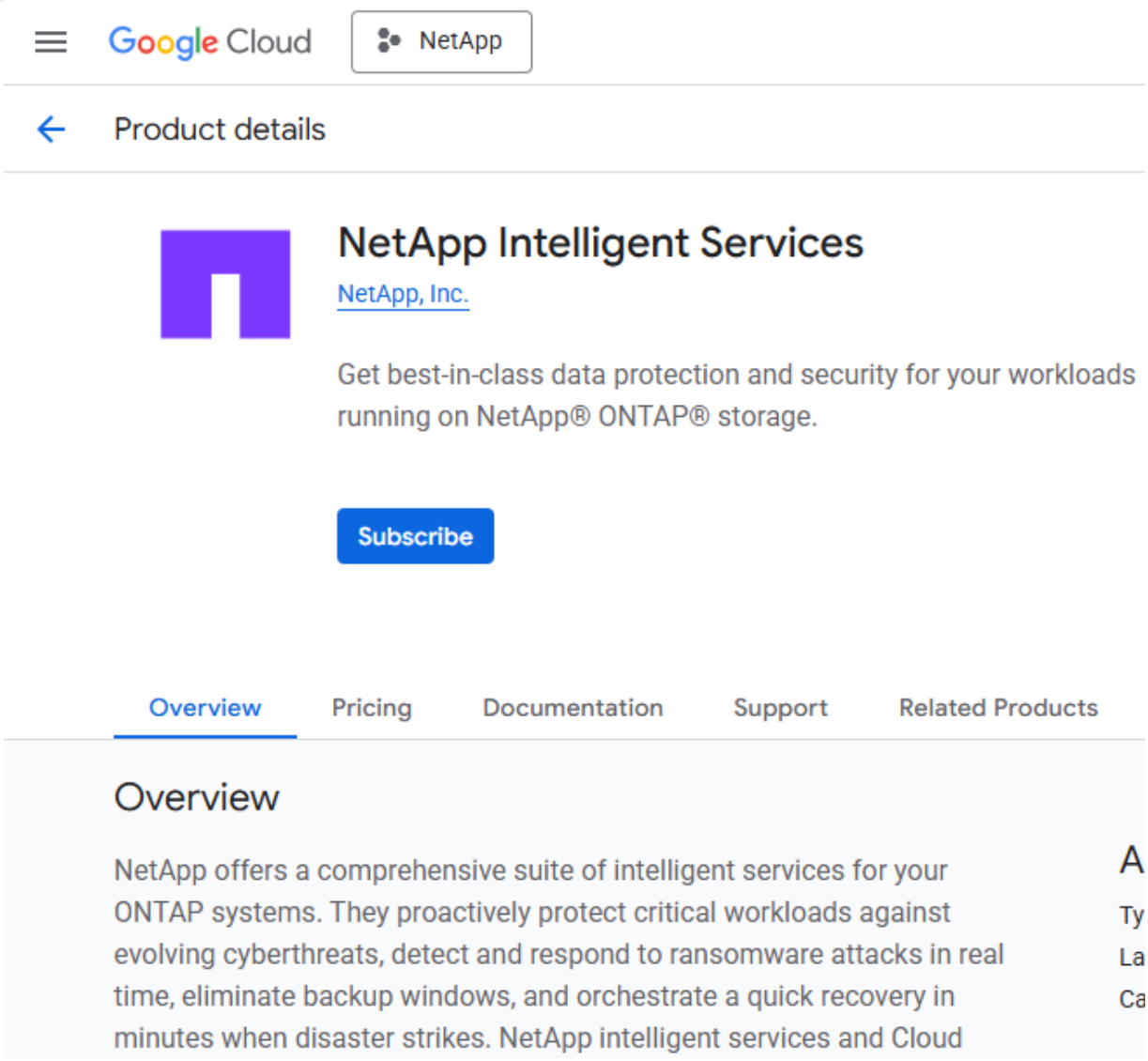
1. Um ein vorhandenes Abonnement mit den ausgewählten Anmeldeinformationen zu konfigurieren, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Dropdown-Liste aus und wählen Sie dann **Konfigurieren**.



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

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

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



b. Wählen Sie **Abonnieren**.

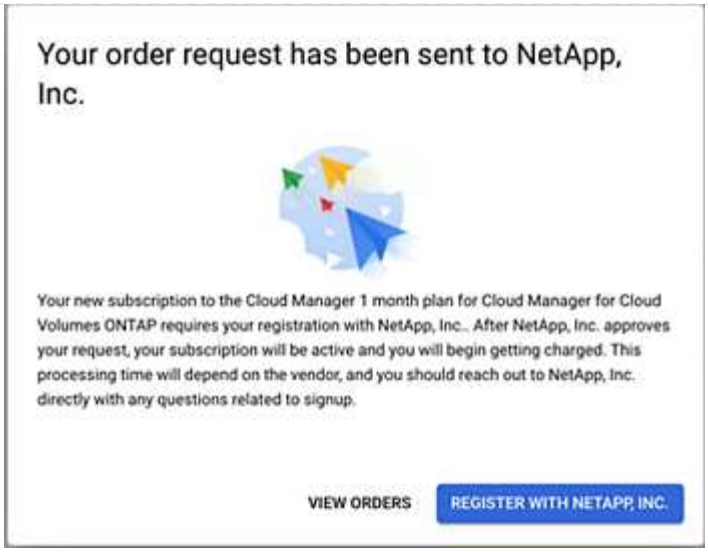
c. Wählen Sie das entsprechende Abrechnungskonto aus und stimmen Sie den Allgemeinen Geschäftsbedingungen zu.

d. Wählen Sie **Abonnieren**.

   Dieser Schritt sendet Ihre Übertragungsanforderung an NetApp.

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

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



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

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

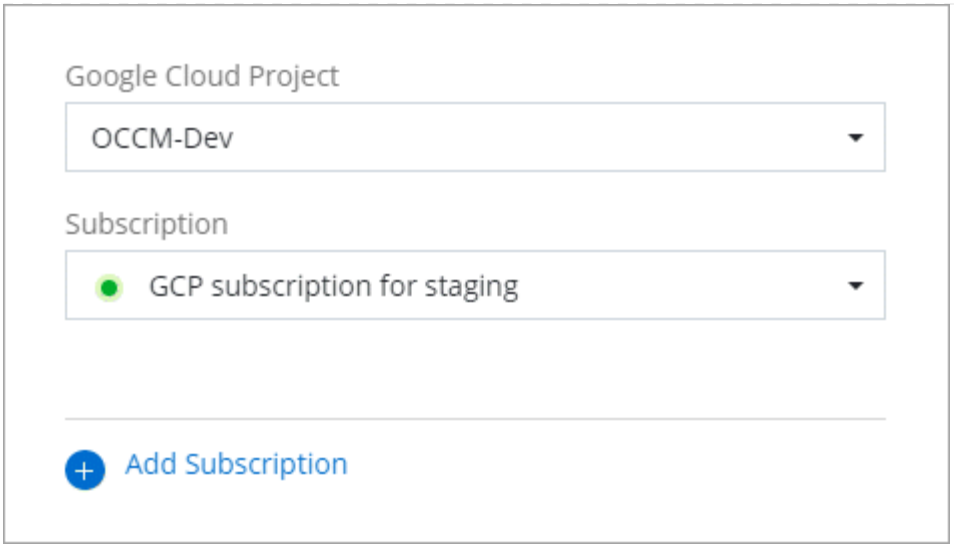
- Wählen Sie die Konsolenorganisation aus, mit der Sie dieses Abonnement verknüpfen möchten.
- Wählen Sie im Feld **Vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für eine Organisation automatisch durch dieses neue Abonnement ersetzen möchten.

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

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

◦ Wählen Sie **Speichern**.

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



Ähnliche Informationen

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

Was Sie als Nächstes tun können (eingeschränkter Modus)

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

Hilfe finden Sie in der Dokumentation zu diesen Diensten:

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

Ähnliche Informationen

"Bereitstellungsmodi der NetApp Console"

Beginnen Sie mit dem privaten Modus

Erste Schritte mit dem Workflow (BlueXP -Privatmodus)

Der private BlueXP Modus (alte BlueXP -Schnittstelle) wird normalerweise in lokalen Umgebungen ohne Internetverbindung und mit sicheren Cloud-Regionen verwendet, darunter AWS Secret Cloud, AWS Top Secret Cloud und Azure IL6. NetApp unterstützt diese Umgebungen weiterhin mit der alten BlueXP Schnittstelle.

"PDF-Dokumentation für den privaten Modus von BlueXP"

Im privaten Modus unterstützte Funktionen und Datendienste

Mithilfe der folgenden Tabelle können Sie schnell erkennen, welche BlueXP -Dienste und -Funktionen im privaten Modus unterstützt werden.

Beachten Sie, dass einige Dienste möglicherweise nur eingeschränkt unterstützt werden.

Produktbereich	BlueXP -Dienst oder -Funktion	Privatmodus
Arbeitsumgebungen Dieser Teil der Tabelle listet die Unterstützung für die Verwaltung von Arbeitsumgebungen aus dem BlueXP Canvas auf. Es werden keine unterstützten Sicherungsziele für die BlueXP backup and recovery angezeigt.	Amazon FSx für ONTAP	Nein
	Amazon S3	Nein
	Azure-Blob	Nein
	Azure NetApp Files	Nein
	Cloud Volumes ONTAP	Ja
	Google Cloud NetApp Volumes	Nein
	Google Cloud-Speicher	Nein
	On-Premises- ONTAP -Cluster	Ja
	E-Series	Nein
	StorageGRID	Nein

Produktbereich	BlueXP -Dienst oder -Funktion	Privatmodus
Dienstleistungen	Warnungen	Nein
	Sicherung und Wiederherstellung	Jahttps://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-no-internet-connectivity["Liste der unterstützten Backup-Ziele für ONTAP Volume-Daten anzeigen"^]
	Einstufung	Ja
	Kopieren und synchronisieren	Nein
	Digitaler Berater	Nein
	Digitale Geldbörse	Ja
	Notfallwiederherstellung	Nein
	Wirtschaftlichkeit	Nein
	Ransomware-Resilienz	Nein
	Replikation	Ja
	Software-Updates	Nein
	Nachhaltigkeit	Nein
	Abstufung	Nein
	Volume-Caching	Nein
	Workload-Factory	Nein
Merkmale	Identitäts- und Zugriffsverwaltung	Ja
	Anmeldeinformationen	Ja
	Föderation	Nein
	Multi-Faktor-Authentifizierung	Nein
	NSS-Konten	Nein
	Benachrichtigungen	Nein
	Suche	Nein
	Zeitleiste	Ja

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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