Dokumentation zur Einrichtung und Verwaltung der NetApp Console

NetApp Console setup and administration

NetApp
October 10, 2025

This PDF was generated from https://docs.netapp.com/de-de/console-setup-admin/index.html on October 10, 2025. Always check docs.netapp.com for the latest.

Inhalt

Dokumentation zur Einrichtung und Verwaltung der NetApp Console . . . 1
Versionshinweise . . . 2
Was ist neu . . . 2
6. Oktober 2025 . . . 2
BlueXP heißt jetzt NetApp Console . . . 2
Konsolenagent 4.0.0 . . . 8
NetApp Console . . . 9
11. August 2025 . . . 10
31. Juli 2025 . . . 10
21. Juli 2025 . . . 11
14. Juli 2025 . . . 11
9. Juni 2025 . . . 13
29. Mai 2025 . . . 14
12. Mai 2025 . . . 14
14. April 2025 . . . 16
28. März 2025 . . . 16
10. März 2025 . . . 17
6. März 2025 . . . 17
18. Februar 2025 . . . 18
10. Februar 2025 . . . 18
13. Januar 2025 . . . 20
16. Dezember 2024 . . . 21
9. Dezember 2024 . . . 22
26. November 2024 . . . 22
11. November 2024 . . . 23
10. Oktober 2024 . . . 23
7. Oktober 2024 . . . 24
30. September 2024 . . . 25
9. September 2024 . . . 26
22. August 2024 . . . 27
8. August 2024 . . . 28
31. Juli 2024 . . . 29
15. Juli 2024 . . . 30
8. Juli 2024 . . . 30
12. Juni 2024 . . . 30
4. Juni 2024 . . . 30
17. Mai 2024 . . . 31
Bekannte Einschränkungen der NetApp Console . . . 32
Einschränkungen des Konsolenagenten . . . 32
Änderungen an unterstützten Linux-Betriebssystemen . . . 33
Unterstützte Betriebssysteme . . . 33
Unterstützung für RHEL 8 und 9 . . . 34
Ende des Supports für RHEL 7 und CentOS 7 . . . 35

Ähnliche Informationen . . . 35
Erste Schritte . . . 37
Lernen Sie die Grundlagen . . . 37
Erfahren Sie mehr über die NetApp Console . . . 37
Erfahren Sie mehr über NetApp Console -Agenten . . . 40
Erfahren Sie mehr über die Bereitstellungsmodi der NetApp Console . . . 44
Erste Schritte mit dem NetApp Console Assistenten . . . 51
Erste Schritte mit dem NetApp Console Assistenten . . . 51
Erste Schritte mit dem Standardmodus . . . 52
Workflow „Erste Schritte“ (Standardmodus) . . . 52
Netzwerkzugriff für die NetApp Console vorbereiten . . . 53
Registrieren oder bei der NetApp Console anmelden . . . 56
Erstellen eines Konsolenagenten . . . 57
Abonnieren Sie NetApp Intelligent Services (Standardmodus) . . . 211
Was Sie als Nächstes tun können (Standardmodus) . . . 217
Erste Schritte mit dem eingeschränkten Modus . . . 217
Workflow „Erste Schritte“ (eingeschränkter Modus) . . . 217
Vorbereiten der Bereitstellung im eingeschränkten Modus . . . 218
Bereitstellen des Konsolenagenten im eingeschränkten Modus . . . 238
Abonnieren Sie NetApp Intelligent Services (eingeschränkter Modus) . . . 250
Was Sie als Nächstes tun können (eingeschränkter Modus) . . . 256
Erste Schritte mit der BlueXP -Legacy-Schnittstelle (privater Modus) . . . 257
Erste Schritte mit dem Workflow (BlueXP -Privatmodus) . . . 257
Verwenden Sie die NetApp Console . . . 259
Melden Sie sich bei der NetApp Console an . . . 259
Anzeigen von Metriken auf der Startseite der NetApp Console . . . 261
Erforderliche NetApp Console . . . 261
Aktivieren Sie die Anzeige von Metriken auf der Startseite . . . 263
Gesamtspeicherkapazität anzeigen . . . 263
ONTAP Warnmeldungen anzeigen . . . 264
Anzeigen der Speicherleistungskapazität . . . 265
Zeigen Sie die Lizenzen und Abonnements an, die Sie haben . . . 265
Ransomware-Resilienzstatus anzeigen . . . 266
Anzeigen des Sicherungs- und Wiederherstellungsstatus . . . 266
Verwalten Sie Ihre NetApp Console . . . 266
Ändern Sie Ihren Anzeigenamen . . . 267
Konfigurieren der mehrstufigen Authentifizierung . . . 267
MFA-Wiederherstellungscode neu generieren . . . 268
Löschen Sie Ihre MFA-Konfiguration . . . 268
Wenden Sie sich an den Administrator Ihrer Organisation . . . 268
Dunkelmodus konfigurieren (dunkles Design) . . . 269
NetApp Console verwalten . . . 270
Identitäts- und Zugriffsverwaltung . . . 270
Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der NetApp Console . . . 270
Erste Schritte mit Identität und Zugriff in der NetApp Console . . . 277

Organisieren Sie Ihre NetApp Console -Ressourcen mit Ordnern und Projekten . . . 278
Fügen Sie der NetApp Console Mitglieder und Dienstkonten hinzu . . . 282
Verwenden Sie Rollen, um den Benutzerzugriff auf NetApp Console -Ressourcen zu verwalten . . . 286
Verwalten Sie die Ressourcenhierarchie in Ihrer NetApp Console Organisation . . . 288
Verknüpfen Sie einen Konsolenagenten mit anderen Ordnern und Projekten . . . 291
Wechseln Sie zwischen Konsolenorganisationen, Projekten und Agenten . . . 292
Organisations- und Projekt-IDs . . . 294
Überwachen oder prüfen Sie die IAM-Aktivität . . . 295
NetApp Console . . . 296
Partnerorganisationen . . . 315
Partnerschaften in der NetApp Console . . . 315
Verwalten Sie Partnerschaften in der NetApp Console . . . 319
Mitglieder für eine Partnerschaftsorganisation verwalten . . . 321
Gewähren Sie Partnerschaftsbenutzern Zugriff auf Ressourcen . . . 322
Arbeit in einer Partnerorganisation . . . 324
Identitätsföderation . . . 325
Aktivieren Sie Single Sign-On durch die Verwendung der Identitätsföderation mit der NetApp Console 325
Domänenüberprüfung . . . 327
Konfigurieren von Föderationen . . . 327
Föderationen in der NetApp Console verwalten . . . 335
Importieren Sie Ihre Föderation in die NetApp Console . . . 337
Konsolenagenten . . . 338
Warten der Konsolen-Agent-VM und des Betriebssystems . . . 338
Verwalten Sie einen VCenter- oder ESXi-Host für den Konsolenagenten . . . 340
Installieren Sie ein CA-signiertes Zertifikat für den webbasierten Konsolenzugriff . . . 344
Konfigurieren eines Konsolenagenten zur Verwendung eines Proxyservers . . . 346
Erfordert die Verwendung von IMDSv2 auf Amazon EC2-Instanzen . . . 349
Upgrades des Konsolenagenten verwalten . . . 351
Arbeiten mit mehreren Konsolenagenten . . . 353
Fehlerbehebung beim Konsolen-Agent . . . 355
Deinstallieren und Entfernen eines Konsolenagenten . . . 359
Standardkonfiguration für den Konsolenagenten . . . 360
Erzwingen Sie ONTAP -Berechtigungen für ONTAP Advanced View (ONTAP System Manager). . . . 362
Anmeldeinformationen und Abonnements . . . 363
AWS . . . 363
Azurblau . . . 378
Google Cloud . . . 392
Verwalten der mit der NetApp Console verknüpften NSS-Anmeldeinformationen . . . 398
Verwalten Sie die mit Ihrer NetApp Console verknüpften Anmeldeinformationen . . . 401
Überwachen Sie NetApp Console . . . 402
Überwachen Sie die Benutzeraktivität auf der Seite „Überwachen“. . . . 403
Überwachen Sie Aktivitäten mithilfe des Benachrichtigungscenters . . . 404
Referenz . . . 407
Agenten-Wartungskonsole . . . 407
Konsolen-Agent-Wartungskonsole . . . 407

Berechtigungen . . . 408
Berechtigungsübersicht für die NetApp Console . . . 408
AWS-Berechtigungen für den Konsolenagenten . . . 412
Azure-Berechtigungen für den Konsolen-Agent . . . 443
Google Cloud-Berechtigungen für den Konsolenagenten . . . 462
Häfen . . . 468
Sicherheitsgruppenregeln für Konsolenagenten in AWS . . . 468
Sicherheitsgruppenregeln für Konsolen-Agents in Azure . . . 469
Agent-Firewallregeln in Google Cloud . . . 471
Ports für den lokalen Konsolenagenten . . . 472
Erforderliche Netzwerkzugriffspunkte für 3.9.55 und darunter . . . 472
Aktualisieren Sie Ihre Endpunktliste auf die überarbeitete Liste für 4.0.0 und höher . . . 473
Von der NetApp Console kontaktierte Endpunkte . . . 473
Vom Konsolenagenten kontaktierte Endpunkte . . . 474
Lokale Agent-Endpunkte . . . 477
Wissen und Unterstützung . . . 478
Für Support registrieren . . . 478
Übersicht zur Support-Registrierung . . . 478
Registrieren Sie die NetApp Console für den NetApp Support . . . 478
NSS-Anmeldeinformationen für Cloud Volumes ONTAP Support zuordnen . . . 480
Hilfe erhalten . . . 482
Erhalten Sie Unterstützung für den Dateidienst eines Cloud-Anbieters . . . 482
Nutzen Sie Möglichkeiten zur Selbsthilfe . . . 482
Erstellen Sie einen Fall mit dem NetApp Support . . . 482
Verwalten Sie Ihre Supportfälle . . . 485
Rechtliche Hinweise . . . 487
Copyright . . . 487
Marken . . . 487
Patente . . . 487
Datenschutzrichtlinie . . . 487
Open Source . . . 487

Dokumentation zur Einrichtung und Verwaltung der NetApp Console

Versionshinweise

Was ist neu

Informieren Sie sich über die Neuerungen bei den Verwaltungsfunktionen der NetApp Console : Identitäts- und Zugriffsverwaltung (IAM), Konsolenagenten, Anmeldeinformationen von Cloud-Anbietern und mehr.

6. Oktober 2025

BlueXP heißt jetzt NetApp Console

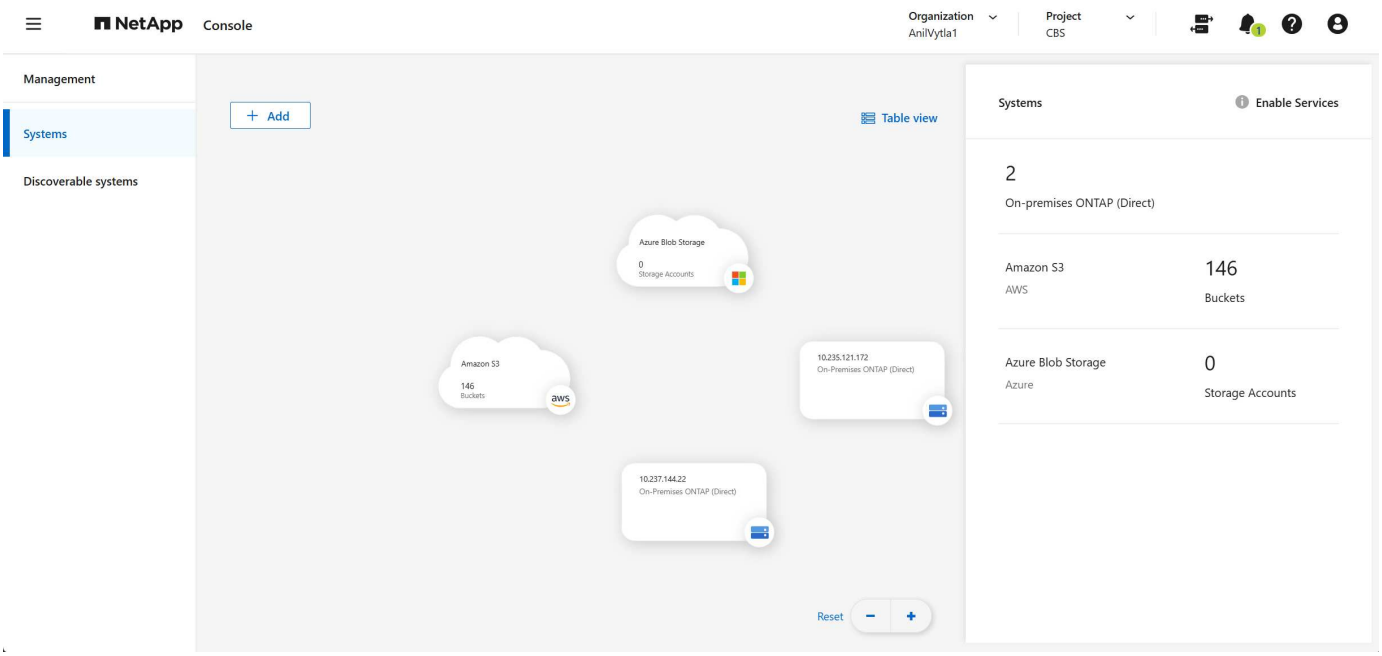
Die NetApp Console basiert auf der verbesserten und neu strukturierten BlueXP -Grundlage und ermöglicht die zentrale Verwaltung von NetApp Storage und NetApp Data Services in On-Premises- und Cloud-Umgebungen auf Unternehmensniveau. Sie liefert Einblicke in Echtzeit, schnellere Workflows und eine vereinfachte Administration, die äußerst sicher und konform ist.

Navigationsmenüs und -seiten

NetApp hat die meisten Menüoptionen in den linken Navigationsbereich verschoben und die Menüs neu organisiert, um die Navigation in der NetApp Console zu erleichtern.

Canvas wird durch die Seite „Systeme“ ersetzt

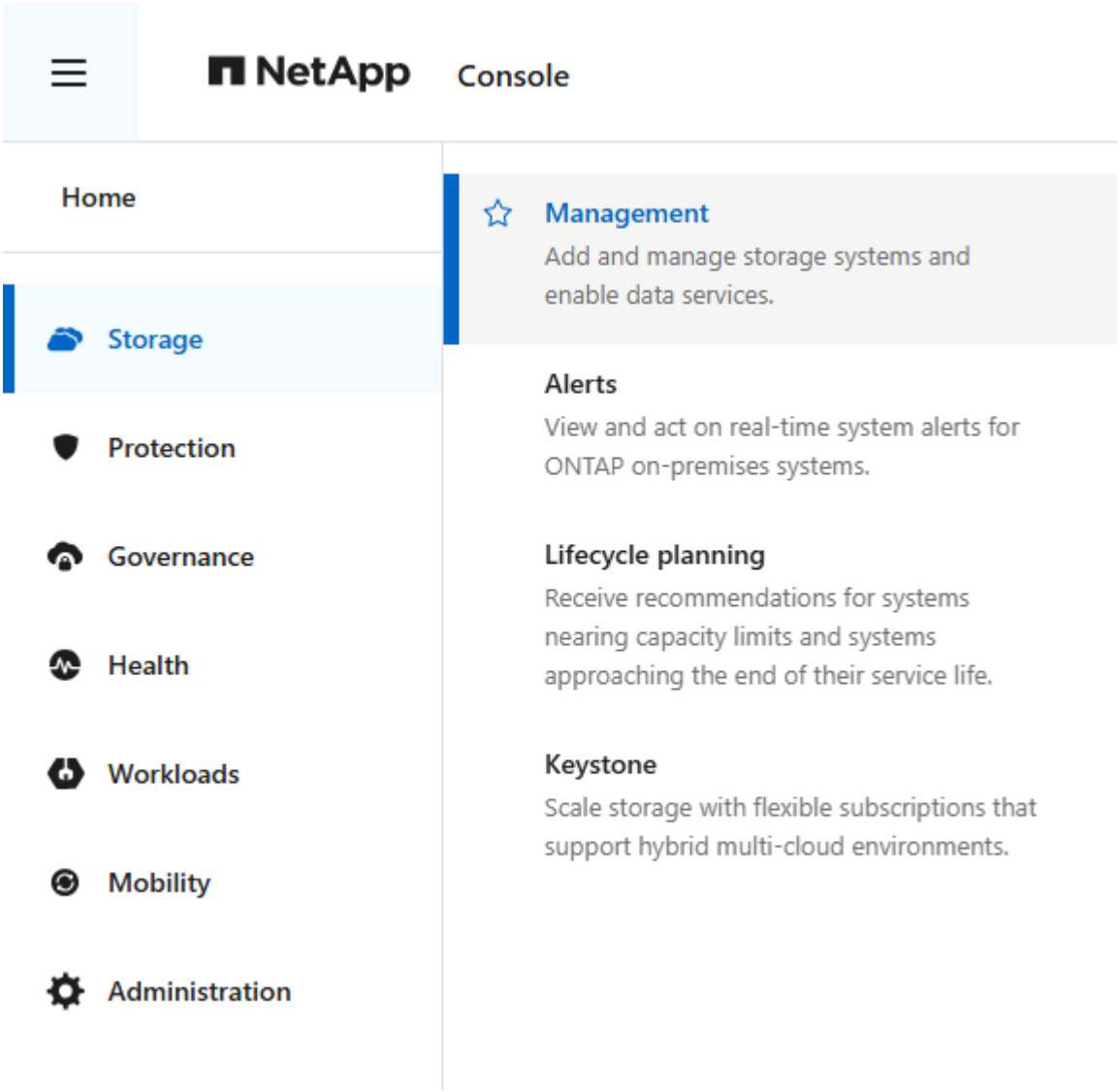
NetApp hat den Canvas in die Seite **Systeme** umbenannt. Navigieren Sie über das Menü **Speicher > Verwaltung** zur Seite **System**.



Erweitertes Speichermenü

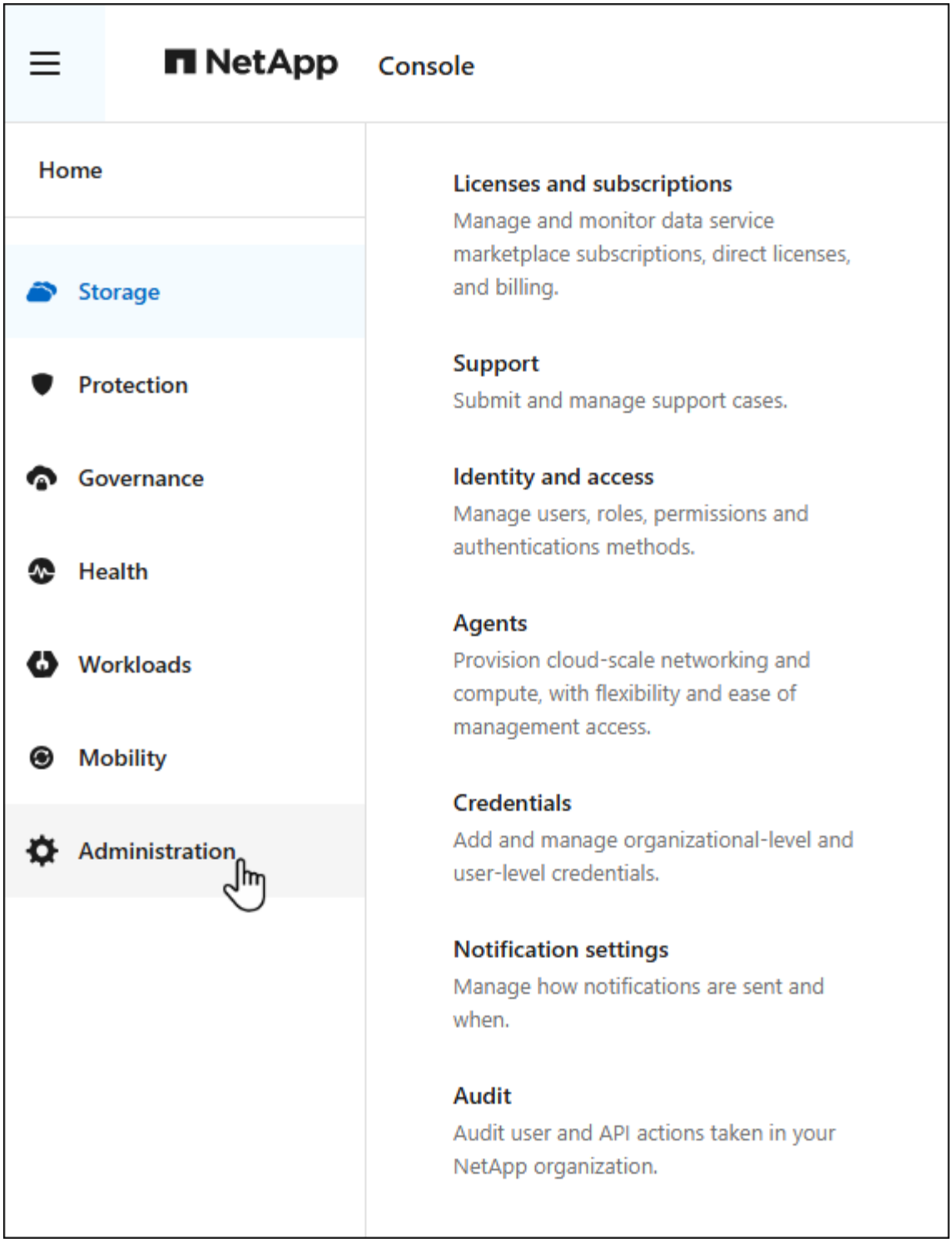
Das Menü **Speicher** umfasst **Warnungen** zum Anzeigen von ONTAP -Systemwarnungen und **Lebenszyklusplanung** (früher **Wirtschaftlichkeit**) zum Identifizieren ungenutzter oder nicht ausreichend genutzter Ressourcen.

NetApp hat Keystone in das Menü **Speicher** verschoben, wo Sie Ihre NetApp Keystone -Abonnements verwalten und Ihre Nutzung anzeigen können.



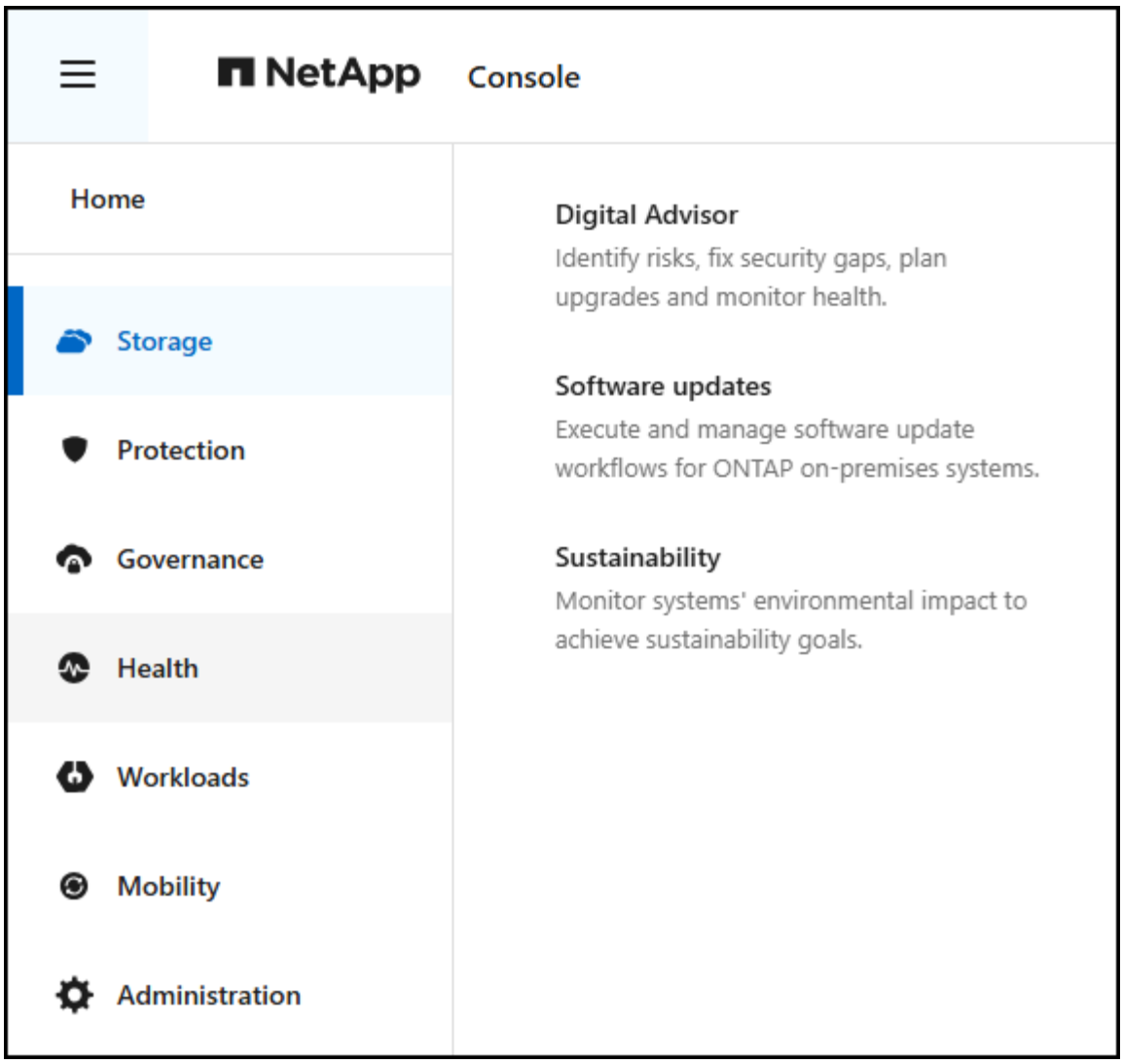
Menü „Verwaltung“

Verwenden Sie das zentralisierte Menü **Administration**, um die NetApp Console, Supportfälle, Lizenzen und Abonnements (früher als digitale Geldbörse bezeichnet) zu verwalten.



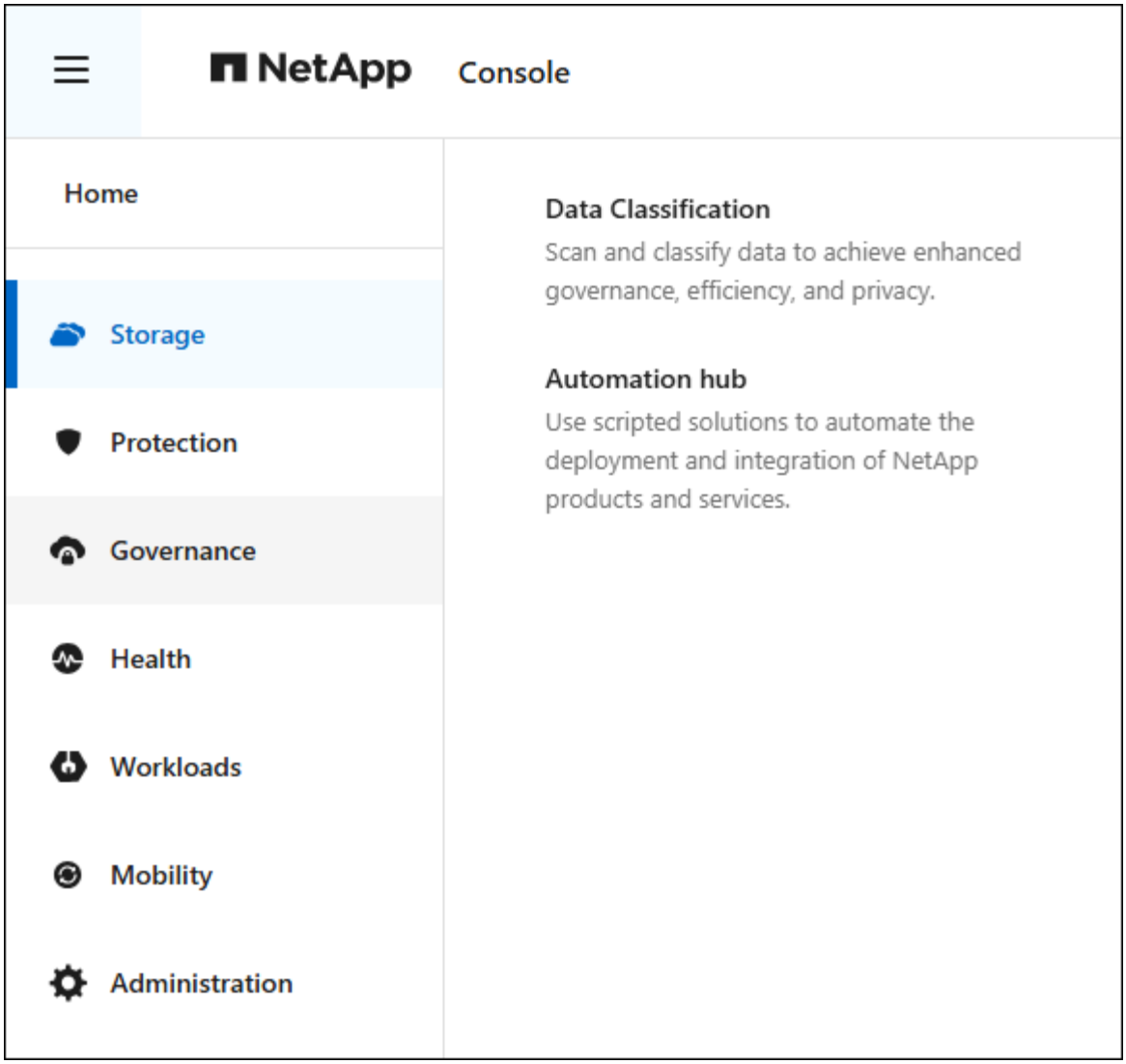
Gesundheitsmenü

Ein effizientes **Health**-Menü umfasst **Software-Updates**, wo Sie ONTAP -Software-Updates verwalten können, **Sustainability**, wo Sie Ihre Umweltauswirkungen überwachen können, und * Digital Advisor*, wo Sie proaktive Empfehlungen zur Optimierung Ihrer Speicherumgebung erhalten.



Governance-Menü

Das Menü **Governance** umfasst die **Datenklassifizierung**, wo Sie die Datenklassifizierung und -konformität verwalten können, und den **Automatisierungs-Hub**, wo Sie Automatisierungs-Workflows erstellen und verwalten können.



Intuitivere Benennung von Elementen, Datendiensten und Funktionen

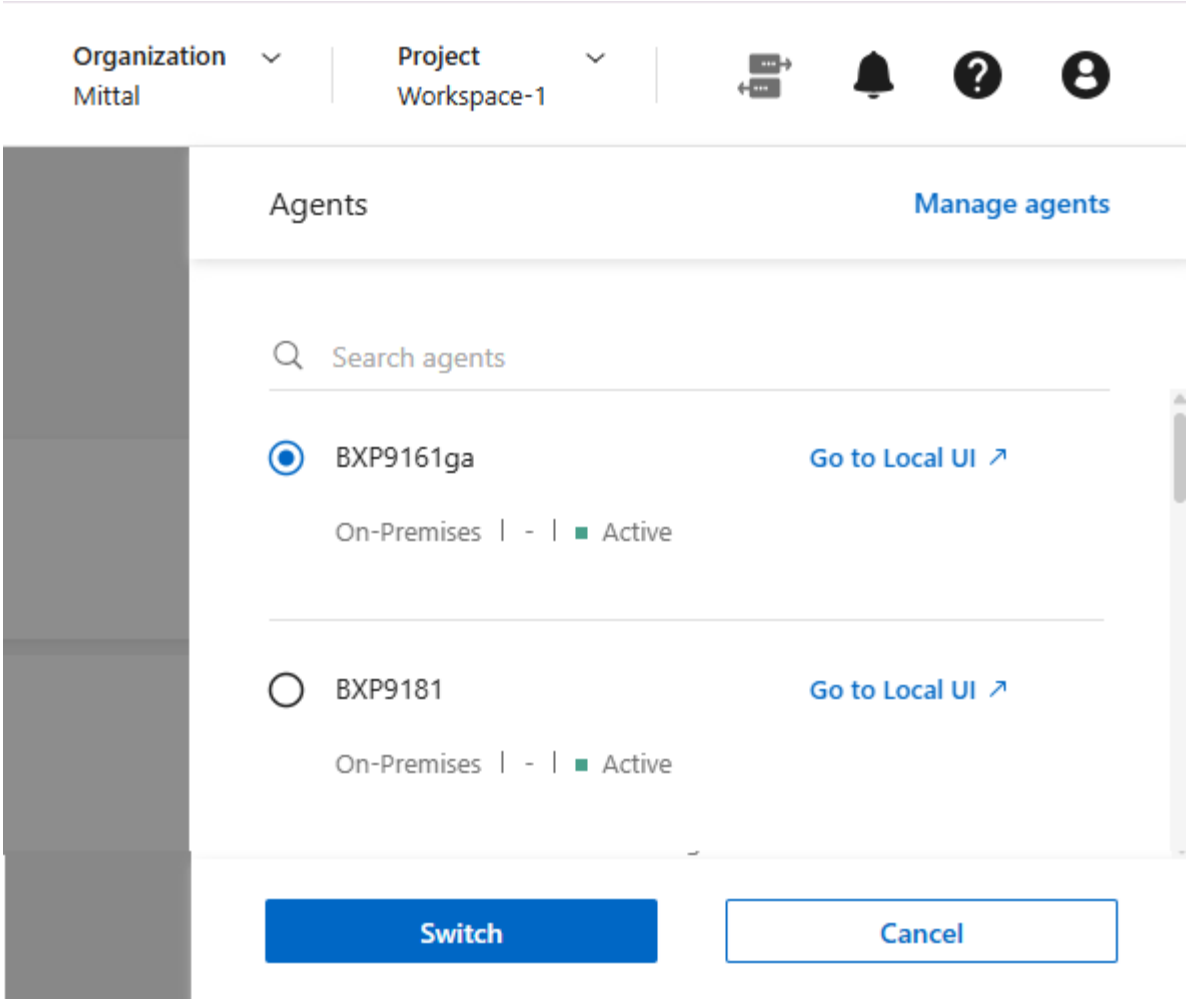
NetApp hat mehrere Elemente, Datendienste und Funktionen umbenannt, um ihren Zweck zu verdeutlichen. Zu den wichtigsten Änderungen gehören:

Vorheriger Name	* NetApp Console *
Anschlüsse	Konsolenagenten. Sie können Ihre Agenten über das Menü **Administration > Agenten** anzeigen, hinzufügen und verwalten.
Zeitleistenseite	Audit-Seite Zeigen Sie die Aktivität der Audit-Konsole über das Menü **Administration > Audit** an.

Vorheriger Name	* NetApp Console *
Arbeitsumgebungen	Systeme Zeigen Sie Ihre Systeme über das Menü **Speicher > Verwaltung** an, fügen Sie sie hinzu und verwalten Sie sie.
BlueXP Ransomware-Schutz	NetApp Ransomware Resilience. Ransomware Resilience hilft Ihnen, Ihre Daten zu schützen und sich schnell von einem Ransomware-Angriff zu erholen.
BlueXP Wirtschaftlichkeit	Lebenszyklusplanung. Mithilfe der Lebenszyklusplanung können Sie Ihre Speicherkosten optimieren, indem Sie ungenutzte und nicht ausreichend genutzte Ressourcen identifizieren. Greifen Sie über das Menü **Speicher > Lebenszyklusplanung** auf die Lebenszyklusplanung zu.
BlueXP digital wallet	Licenses and subscriptions Greifen Sie über das Menü **Administration > Licenses and subscriptions und Abonnements** auf Ihre Lizenzen und Abonnements zu.

Konsolenagenten

Greifen Sie über das Menü **Administration > Agenten** auf Ihre Konsolenagenten zu und verwalten Sie sie. NetApp hat die Art und Weise geändert, wie ein Konsolenagent für die Seite **Systeme** (früher Canvas) ausgewählt wird. NetApp hat den Connector-Menünamen durch ein Symbol ersetzt , sodass Sie den Konsolenagenten auswählen können, für den Sie Systeme anzeigen möchten.



Sie können Ihre Agenten auch über das Menü **Administration > Agenten** verwalten.

Konsolenagent 4.0.0

Diese Version des Konsolenagenten enthält Sicherheitsverbesserungen, Fehlerbehebungen und die folgenden neuen Funktionen.

Die Version 4.0.0 ist für den Standardmodus und den eingeschränkten Modus verfügbar.

Konsolidierung und Reduzierung der benötigten Netzwerkendpunkte

NetApp hat 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" .
- "Erfahren Sie mehr über erforderliche Endpunkte."

Unterstützung für die VCenter-Bereitstellung von Konsolenagenten

Sie können Konsolenagenten in VMware-Umgebungen mithilfe einer OVA-Datei bereitstellen. Die OVA-Datei enthält ein vorkonfiguriertes VM-Image mit Konsolen-Agent-Software und Einstellungen für die Verbindung mit

der NetApp Console. Ein Dateidownload oder eine URL-Bereitstellung ist direkt über die NetApp Console möglich."Erfahren Sie, wie Sie einen Konsolenagenten in VMware-Umgebungen bereitstellen."

Der Console Agent OVA für VMware bietet ein vorkonfiguriertes VM-Image für eine schnelle Bereitstellung.

Validierungsberichte für fehlgeschlagene Agentenbereitstellungen

Wenn Sie einen Konsolenagenten von der NetApp Console aus bereitstellen, haben Sie jetzt die Möglichkeit, die Agentenkonfiguration zu validieren. Wenn die Bereitstellung des Agenten durch die Konsole fehlschlägt, wird ein herunterladbarer Bericht bereitgestellt, der Sie bei der Fehlerbehebung unterstützt.

Verbesserte Fehlerbehebung für Konsolenagenten

Der Konsolenagent verfügt über verbesserte Fehlermeldungen, die Ihnen helfen, Probleme besser zu verstehen."Erfahren Sie, wie Sie Probleme mit Konsolenagenten beheben."

NetApp Console

Die NetApp Console umfasst die folgenden neuen Funktionen:

Startseiten-Dashboard

Das Dashboard auf der Startseite der NetApp Konsole bietet Echtzeit-Einblicke in die Speicherinfrastruktur mit Kennzahlen zu Zustand, Kapazität, Lizenzstatus und Datendiensten."Erfahren Sie mehr über die Startseite."

NetApp Assistent

Neue Benutzer mit der Rolle „Organisationsadministrator“ können den NetApp Assistenten zum Konfigurieren der Konsole verwenden, einschließlich des Hinzufügens eines Agenten, des Verknüpfens eines NetApp -Supportkontos und des Hinzufügens eines Speichersystems."Erfahren Sie mehr über den NetApp Assistenten."

Dienstkontoauthentifizierung

Die NetApp Console unterstützt die Authentifizierung von Servicekonten entweder mithilfe einer systemgenerierten Client-ID und geheimer oder kundenverwalteter JWTs. So können Unternehmen den Ansatz auswählen, der ihren Sicherheitsanforderungen und Integrations-Workflows am besten entspricht. Die JWT-Client-Authentifizierung mit privatem Schlüssel verwendet asymmetrische Kryptografie und bietet eine höhere Sicherheit als herkömmliche Client-ID- und Geheimmethoden. Die Private Key JWT-Client-Authentifizierung verwendet asymmetrische Kryptografie, wodurch der private Schlüssel in der Umgebung des Kunden sicher bleibt, das Risiko des Diebstahls von Anmeldeinformationen verringert und die Sicherheit Ihres Automatisierungsstapels und Ihrer Client-Anwendungen verbessert wird."Erfahren Sie, wie Sie ein Dienstkonto hinzufügen."

Sitzungs-Timeouts

Das System meldet Benutzer nach 24 Stunden oder beim Schließen ihres Webbrowsers ab.

Unterstützung von Partnerschaften zwischen Organisationen

Sie können in der NetApp Console Partnerschaften erstellen, die es Partnern ermöglichen, NetApp -Ressourcen über Unternehmensgrenzen hinweg sicher zu verwalten, wodurch die Zusammenarbeit vereinfacht und die Sicherheit verbessert wird. "Erfahren Sie, wie Sie Partnerschaften verwalten" .

Super-Admin- und Super-Viewer-Rollen

Die Rollen **Super-Admin** und **Super-Viewer** wurden hinzugefügt. **Superadministrator** gewährt vollständigen Verwaltungszugriff auf Konsolenfunktionen, Speicher und Datendienste. **Super Viewer** bietet Prüfern und Stakeholdern schreibgeschützte Sichtbarkeit. Diese Rollen sind für kleinere Teams mit erfahrenen Mitgliedern nützlich, bei denen ein breiter Zugriff üblich ist. Zur Verbesserung der Sicherheit und Überprüfbarkeit wird Organisationen empfohlen, den **Superadministrator**-Zugriff sparsam zu verwenden und nach Möglichkeit fein abgestufte Rollen zuzuweisen."Erfahren Sie mehr über Zugriffsrollen."

Zusätzliche Rolle für Ransomware-Resilienz

Die Rollen **Ransomware Resilience-Benutzerverhaltensadministrator** und **Ransomware Resilience-Benutzerverhaltensbetrachter** wurden hinzugefügt. Mit diesen Rollen können Benutzer das Benutzerverhalten und Analysedaten konfigurieren und anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Support-Chat entfernt

NetApp hat die Support-Chat-Funktion aus der NetApp Console entfernt. Verwenden Sie die Seite **Administration > Support**, um Supportfälle zu erstellen und zu verwalten.

11. August 2025

Connector 3.9.55

Diese Version des BlueXP Connector enthält Sicherheitsverbesserungen und Fehlerbehebungen.

Die Version 3.9.55 ist für den Standardmodus und den eingeschränkten Modus verfügbar.

Unterstützung der japanischen Sprache

Die BlueXP -Benutzeroberfläche ist jetzt in japanischer Sprache verfügbar. Wenn Ihre Browsersprache Japanisch ist, wird BlueXP auf Japanisch angezeigt. Um auf die Dokumentation auf Japanisch zuzugreifen, verwenden Sie das Sprachmenü auf der Dokumentationswebsite.

Funktion zur betrieblichen Ausfallsicherheit

Die Funktion „Betriebsstabilität“ wurde aus BlueXP entfernt. Wenden Sie sich bei Problemen an den NetApp -Support.

BlueXP Identitäts- und Zugriffsmanagement (IAM)

Das Identitäts- und Zugriffsmanagement in BlueXP bietet jetzt die folgende Funktion.

Neue Zugriffsrolle für den operativen Support

BlueXP unterstützt jetzt die Rolle eines Betriebssupportanalysten. Diese Rolle erteilt einem Benutzer die Berechtigung, Speicherwarnungen zu überwachen, die BlueXP Audit-Zeitleiste anzuzeigen und NetApp Supportfälle einzugeben und zu verfolgen.

"Erfahren Sie mehr über die Verwendung von Zugriffsrollen."

31. Juli 2025

Freigabe des Privatmodus (3.9.54)

Eine neue Version des privaten Modus steht jetzt zum Download bereit von der "NetApp Support Site"

Die Version 3.9.54 enthält Updates für die folgenden BlueXP Komponenten und -Dienste.

Komponente oder Dienst	In dieser Version enthaltene Version	Änderungen seit der letzten Version des privaten Modus
Anschluss	3.9.54, 3.9.53	Gehen Sie zum "Was gibt es Neues auf der BlueXP -Seite?" und beziehen Sie sich auf die Änderungen, die in den Versionen 3.9.54 und 3.9.53 enthalten sind.
Sicherung und Wiederherstellung	28. Juli 2025	Gehen Sie zum "Was ist neu auf der BlueXP backup and recovery?" und beziehen Sie sich auf die Änderungen, die in der Version vom Juli 2025 enthalten sind.
Einstufung	14. Juli 2025 (Version 1.45)	Gehen Sie zum "Was ist neu auf der BlueXP classification ?" .

Weitere Einzelheiten zum privaten Modus, einschließlich der Aktualisierungsinformationen, finden Sie hier:

- "Erfahren Sie mehr über den privaten Modus"
- "Erfahren Sie, wie Sie mit BlueXP im privaten Modus beginnen"
- "Erfahren Sie, wie Sie den Connector im privaten Modus aktualisieren."

21. Juli 2025

Unterstützung für Google Cloud NetApp Volumes

Sie können jetzt Google Cloud NetApp Volumes in BlueXP anzeigen."Erfahren Sie mehr über Google Cloud NetApp Volumes."

BlueXP Identitäts- und Zugriffsmanagement (IAM)

Neue Zugriffsrolle für Google Cloud NetApp Volumes

BlueXP unterstützt jetzt die Verwendung einer Zugriffsrolle für das folgende Speichersystem:

- Google Cloud NetApp Volumes

"Erfahren Sie mehr über die Verwendung von Zugriffsrollen."

14. Juli 2025

Connector 3.9.54

Diese Version des BlueXP Connectors enthält Sicherheitsverbesserungen, Fehlerbehebungen und die folgenden neuen Funktionen:

- Unterstützung für transparente Proxys für Connectors, die speziell für die Unterstützung von Cloud Volumes ONTAP Diensten vorgesehen sind."Erfahren Sie mehr über die Konfiguration eines transparenten Proxys."
- Möglichkeit zur Verwendung von Netzwerk-Tags zur Weiterleitung des Connector-Datenverkehrs, wenn der Connector in einer Google Cloud-Umgebung bereitgestellt wird.
- Zusätzliche produktinterne Benachrichtigungen zur Überwachung des Connector-Zustands, einschließlich CPU- und RAM-Auslastung.

Derzeit ist die Version 3.9.54 für den Standardmodus und den eingeschränkten Modus verfügbar.

BlueXP Identitäts- und Zugriffsmanagement (IAM)

Identitäts- und Zugriffsmanagement in BlueXP bietet jetzt die folgenden Funktionen:

- Unterstützung für IAM im privaten Modus, sodass Sie den Benutzerzugriff und die Berechtigungen für BlueXP -Dienste und -Anwendungen verwalten können.
- Optimierte Verwaltung von Identitätsföderationen, einschließlich einfacherer Navigation, klarerer Optionen zum Konfigurieren föderierter Verbindungen und verbesserter Transparenz in vorhandenen Föderationen.
- Zugriffsrollen für BlueXP backup and recovery, BlueXP disaster recovery und Föderationsverwaltung.

Unterstützung für IAM im privaten Modus

BlueXP unterstützt jetzt IAM im privaten Modus, sodass Sie den Benutzerzugriff und die Berechtigungen für BlueXP -Dienste und -Anwendungen verwalten können. Diese Verbesserung ermöglicht es Kunden im privaten Modus, die rollenbasierte Zugriffskontrolle (RBAC) für mehr Sicherheit und Compliance zu nutzen.

"Erfahren Sie mehr über IAM in BlueXP."

Optimierte Verwaltung von Identitätsföderationen

BlueXP bietet jetzt eine intuitivere Schnittstelle zur Verwaltung der Identitätsföderation. Dazu gehören eine einfachere Navigation, klarere Optionen zum Konfigurieren föderierter Verbindungen und eine verbesserte Transparenz in vorhandenen Föderationen.

Durch die Aktivierung von Single Sign-On (SSO) über die Identitätsföderation können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei BlueXP anmelden. Dies verbessert die Sicherheit, reduziert die Verwendung von Passwörtern und vereinfacht das Onboarding.

Sie werden aufgefordert, alle vorhandenen Verbundverbindungen in die neue Schnittstelle zu importieren, um Zugriff auf die neuen Verwaltungsfunktionen zu erhalten. Auf diese Weise können Sie die neuesten Verbesserungen nutzen, ohne Ihre Verbundverbindungen neu erstellen zu müssen."Erfahren Sie mehr über das Importieren Ihrer vorhandenen Verbundverbindung zu BlueXP."

Durch die verbesserte Föderationsverwaltung können Sie:

- Fügen Sie einer Verbundverbindung mehr als eine verifizierte Domäne hinzu, sodass Sie mehrere Domänen mit demselben Identitätsanbieter (IdP) verwenden können.
- Deaktivieren oder löschen Sie Verbundverbindungen bei Bedarf und behalten Sie so die Kontrolle über Benutzerzugriff und Sicherheit.
- Steuern Sie den Zugriff auf die Föderationsverwaltung mit IAM-Rollen.

"Erfahren Sie mehr über die Identitätsföderation in BlueXP."

Neue Zugriffsrollen für BlueXP backup and recovery, BlueXP disaster recovery und Föderationsverwaltung

BlueXP unterstützt jetzt die Verwendung von IAM-Rollen für die folgenden Funktionen und Datendienste:

- BlueXP backup and recovery
- BlueXP disaster recovery
- Föderation

"Erfahren Sie mehr über die Verwendung von Zugriffsrollen."

9. Juni 2025

Connector 3.9.53

Diese Version des BlueXP Connector enthält Sicherheitsverbesserungen und Fehlerbehebungen.

Die Version 3.9.53 ist für den Standardmodus und den eingeschränkten Modus verfügbar.

Warnungen zur Speicherplatznutzung

Das Benachrichtigungscenter enthält jetzt Warnungen zur Speicherplatznutzung auf dem Connector."Erfahren Sie mehr."

Audit-Verbesserungen

Die Zeitleiste enthält jetzt Anmelde- und Abmeldeereignisse für Benutzer. Sie können die Anmeldeaktivität sehen, was bei der Prüfung und Sicherheitsüberwachung hilfreich sein kann. API-Benutzer mit der Rolle „Organisationsadministrator“ können die E-Mail-Adresse des angemeldeten Benutzers anzeigen, indem sie Folgendes angeben: `includeUserData=true` Parameter wie im Folgenden: `/audit/<account_id>?includeUserData=true` .

Keystone -Abonnementverwaltung in BlueXP verfügbar

Sie können Ihr NetApp Keystone Abonnement von BlueXP aus verwalten.

"Erfahren Sie mehr über die Keystone -Abonnementverwaltung in BlueXP."

BlueXP Identitäts- und Zugriffsmanagement (IAM)

Multi-Faktor-Authentifizierung (MFA)

Nicht föderierte Benutzer können MFA für ihre BlueXP -Konten aktivieren, um die Sicherheit zu verbessern. Administratoren können MFA-Einstellungen verwalten und MFA für Benutzer nach Bedarf zurücksetzen oder deaktivieren. Dies wird nur im Standardmodus unterstützt.

"Erfahren Sie, wie Sie die Multi-Faktor-Authentifizierung selbst einrichten." "Erfahren Sie mehr über die Verwaltung der Multi-Faktor-Authentifizierung für Benutzer."

Arbeitslasten

Sie können jetzt Anmeldeinformationen für Amazon FSx for NetApp ONTAP auf der Anmeldeinformationsseite in BlueXP anzeigen und löschen.

29. Mai 2025

Freigabe des Privatmodus (3.9.52)

Eine neue Version des privaten Modus steht jetzt zum Download bereit von der "NetApp Support Site"

Die Version 3.9.52 enthält Updates für die folgenden BlueXP Komponenten und -Dienste.

Komponente oder Dienst	In dieser Version enthaltene Version	Änderungen seit der letzten Version des privaten Modus
Anschluss	3.9.52, 3.9.51	Gehen Sie zum "Was ist neu auf der BlueXP Connector-Seite?" und beziehen Sie sich auf die Änderungen, die in den Versionen 3.9.52 und 3.9.50 enthalten sind.
Sicherung und Wiederherstellung	12. Mai 2025	Gehen Sie zum "Was ist neu auf der BlueXP backup and recovery?" und beziehen Sie sich auf die Änderungen, die in der Version vom Mai 2025 enthalten sind.
Einstufung	12. Mai 2025 (Version 1.43)	Gehen Sie zum "Was ist neu auf der BlueXP classification ?" und beziehen Sie sich auf die in den Versionen 1.38 bis 1.371.41 enthaltenen Änderungen.

Weitere Einzelheiten zum privaten Modus, einschließlich der Aktualisierungsinformationen, finden Sie hier:

- "Erfahren Sie mehr über den privaten Modus"
- "Erfahren Sie, wie Sie mit BlueXP im privaten Modus beginnen"
- "Erfahren Sie, wie Sie den Connector im privaten Modus aktualisieren."

12. Mai 2025

Connector 3.9.52

Diese Version des BlueXP Connector enthält kleinere Sicherheitsverbesserungen und Fehlerbehebungen sowie einige zusätzliche Updates.

Derzeit ist die Version 3.9.52 für den Standardmodus und den eingeschränkten Modus verfügbar.

Unterstützung für Docker 27 und Docker 28

Docker 27 und Docker 28 werden jetzt mit dem Connector unterstützt.

Cloud Volumes ONTAP

Cloud Volumes ONTAP -Knoten werden nicht mehr heruntergefahren, wenn der Connector nicht konform ist oder länger als 14 Tage ausfällt. Cloud Volumes ONTAP sendet weiterhin Event Management-Nachrichten, wenn der Zugriff auf den Connector verloren geht. Diese Änderung soll sicherstellen, dass Cloud Volumes ONTAP auch dann weiterbetrieben werden kann, wenn der Connector für einen längeren Zeitraum ausfällt. Die

Compliance-Anforderungen für den Connector werden dadurch nicht geändert.

Keystone -Verwaltung in BlueXP verfügbar

Die Beta für NetApp Keystone in BlueXP hat Zugriff auf die Keystone -Verwaltung hinzugefügt. Sie können über die linke Navigationsleiste von BlueXP auf die Anmeldeseite für die Betaversion von NetApp Keystone zugreifen.

BlueXP Identitäts- und Zugriffsmanagement (IAM)

Neue Speicherverwaltungsrollen

Die Rollen „Speicheradministrator“, „Systemintegritätsspezialist“ und „Speicherbetrachter“ sind verfügbar und können Benutzern zugewiesen werden.

Mithilfe dieser Rollen können Sie verwalten, wer in Ihrem Unternehmen Speicherressourcen ermitteln und verwalten sowie Informationen zum Speicherzustand anzeigen und Softwareupdates durchführen kann.

Diese Rollen werden zur Steuerung des Zugriffs auf die folgenden Speicherressourcen unterstützt:

- Systeme der E-Serie
- StorageGRID -Systeme
- On-Premises- ONTAP -Systeme

Sie können diese Rollen auch verwenden, um den Zugriff auf die folgenden BlueXP -Dienste zu steuern:

- Software-Updates
- Digitaler Berater
- Betriebsstabilität
- Wirtschaftlichkeit
- Nachhaltigkeit

Die folgenden Rollen wurden hinzugefügt:

- **Speicheradministrator**

  Verwalten Sie die Speicherintegrität, Governance und Erkennung für die Speicherressourcen in der Organisation. Diese Rolle kann auch Software-Updates für Speicherressourcen durchführen.

- **Systemintegritätsspezialist**

  Verwalten Sie die Speicherintegrität und -verwaltung für die Speicherressourcen in der Organisation. Diese Rolle kann auch Software-Updates für Speicherressourcen durchführen. Diese Rolle kann keine Arbeitsumgebungen ändern oder löschen.

- **Speicheranzeige**

  Zeigen Sie Informationen zum Speicherzustand und Governance-Daten an.

  "Erfahren Sie mehr über Zugriffsrollen."

14. April 2025

Connector 3.9.51

Diese Version des BlueXP Connector enthält kleinere Sicherheitsverbesserungen und Fehlerbehebungen.

Derzeit ist die Version 3.9.51 für den Standardmodus und den eingeschränkten Modus verfügbar.

Sichere Endpunkte für Connector-Downloads werden jetzt für Backup und Wiederherstellung sowie Ransomware-Schutz unterstützt

Wenn Sie Backup und Wiederherstellung oder Ransomware-Schutz verwenden, können Sie jetzt sichere Endpunkte für Connector-Downloads verwenden."Informieren Sie sich über sichere Endpunkte für Connector-Downloads."

BlueXP Identitäts- und Zugriffsmanagement (IAM)

- Benutzern ohne Organisationsadministrator oder Ordner- oder Projektadministrator muss eine Ransomware-Schutzrolle zugewiesen werden, um Zugriff auf den Ransomware-Schutz zu haben. Sie können einem Benutzer eine von zwei Rollen zuweisen: Ransomware-Schutz-Administrator oder Ransomware-Schutz-Betrachter.
- Benutzern ohne Org-Admin oder Ordner- oder Projekt-Admin muss eine Keystone -Rolle zugewiesen werden, um Zugriff auf Keystone zu haben. Sie können einem Benutzer eine von zwei Rollen zuweisen: Keystone -Administrator oder Keystone Viewer.

  "Erfahren Sie mehr über Zugriffsrollen."

- Wenn Sie über die Rolle „Organisationsadministrator“, „Ordner-“ oder „Projektadministrator“ verfügen, können Sie jetzt ein Keystone -Abonnement mit einem IAM-Projekt verknüpfen. Durch die Verknüpfung eines Keystone -Abonnements mit einem IAM-Projekt können Sie den Zugriff auf Keystone innerhalb von BlueXP steuern.

28. März 2025

Freigabe des Privatmodus (3.9.50)

Eine neue Version des privaten Modus steht jetzt zum Download bereit von der "NetApp Support Site"

Die Version 3.9.50 enthält Updates für die folgenden BlueXP Komponenten und -Dienste.

Komponente oder Dienst	In dieser Version enthaltene Version	Änderungen seit der letzten Version des privaten Modus
Anschluss	3.9.50, 3.9.49	Gehen Sie zum "Was ist neu auf der BlueXP Connector-Seite?" und beziehen Sie sich auf die Änderungen, die in den Versionen 3.9.50 und 3.9.49 enthalten sind.
Sicherung und Wiederherstellung	17. März 2025	Gehen Sie zum "Was ist neu auf der BlueXP backup and recovery?" und beziehen Sie sich auf die Änderungen, die in der Version vom März 2024 enthalten sind.

Komponente oder Dienst	In dieser Version enthaltene Version	Änderungen seit der letzten Version des privaten Modus
Einstufung	10. März 2025 (Version 1.41)	Gehen Sie zum "Was ist neu auf der BlueXP classification ?" und beziehen Sie sich auf die in den Versionen 1.38 bis 1.371.41 enthaltenen Änderungen.

Weitere Einzelheiten zum privaten Modus, einschließlich der Aktualisierungsinformationen, finden Sie hier:

- "Erfahren Sie mehr über den privaten Modus"
- "Erfahren Sie, wie Sie mit BlueXP im privaten Modus beginnen"
- "Erfahren Sie, wie Sie den Connector im privaten Modus aktualisieren."

10. März 2025

Connector 3.9.50

Diese Version des BlueXP Connector enthält kleinere Sicherheitsverbesserungen und Fehlerbehebungen.

- Die Verwaltung von Cloud Volumes ONTAP -Systemen wird jetzt von Connectors unterstützt, auf deren Betriebssystem SELinux aktiviert ist.

  "Erfahren Sie mehr über SELinux"

Derzeit ist die Version 3.9.50 für den Standardmodus und den eingeschränkten Modus verfügbar.

NetApp Keystone Beta in BlueXP verfügbar

NetApp Keystone wird in Kürze bei BlueXP erhältlich sein und befindet sich derzeit in der Betaphase. Sie können über die linke Navigationsleiste von BlueXP auf die Anmeldeseite für die Betaversion von NetApp Keystone zugreifen.

6. März 2025

Connector 3.9.49-Update

ONTAP System Manager-Zugriff, wenn BlueXP einen Connector verwendet

Ein BlueXP Administrator (Benutzer mit der Rolle „Organisationsadministrator“) kann BlueXP so konfigurieren, dass Benutzer aufgefordert werden, ihre ONTAP Anmeldeinformationen einzugeben, um auf den ONTAP -Systemmanager zuzugreifen. Wenn diese Einstellung aktiviert ist, müssen Benutzer jedes Mal ihre ONTAP Anmeldeinformationen eingeben, da diese nicht in BlueXP gespeichert sind.

Diese Funktion ist in Connector-Version 3.9.49 und höher verfügbar. "Erfahren Sie, wie Sie die Anmeldeinformationseinstellungen konfigurieren." .

Connector 3.9.48-Update

Möglichkeit, die automatische Upgrade-Einstellung für den Connector zu deaktivieren

Sie können die automatische Upgrade-Funktion des Connectors deaktivieren.

Wenn Sie BlueXP im Standardmodus oder eingeschränkten Modus verwenden, aktualisiert BlueXP Ihren Connector automatisch auf die neueste Version, sofern der Connector über ausgehenden Internetzugang verfügt, um das Softwareupdate zu erhalten. Wenn Sie manuell verwalten müssen, wann der Connector aktualisiert wird, können Sie jetzt automatische Upgrades für den Standardmodus oder den eingeschränkten Modus deaktivieren.

Diese Änderung hat keine Auswirkungen auf den privaten Modus von BlueXP , in dem Sie den Connector immer selbst aktualisieren müssen.

Diese Funktion ist in Connector-Version 3.9.48 und höher verfügbar.

"Erfahren Sie, wie Sie das automatische Upgrade für den Connector deaktivieren."

18. Februar 2025

Freigabe des Privatmodus (3.9.48)

Eine neue Version des privaten Modus steht jetzt zum Download bereit von der "NetApp Support Site"

Die Version 3.9.48 enthält Updates für die folgenden BlueXP Komponenten und -Dienste.

Komponente oder Dienst	In dieser Version enthaltene Version	Änderungen seit der letzten Version des privaten Modus
Anschluss	3.9.48	Gehen Sie zum "Was ist neu auf der BlueXP Connector-Seite?" und beziehen Sie sich auf die in den Versionen 3.9.48 enthaltenen Änderungen.
Sicherung und Wiederherstellung	21. Februar 2025	Gehen Sie zum "Was ist neu auf der BlueXP backup and recovery?" und beziehen Sie sich auf die Änderungen, die in der Version vom Februar 2025 enthalten sind.
Einstufung	22. Januar 2025 (Version 1.39)	Gehen Sie zum "Was ist neu auf der BlueXP classification ?" und beziehen Sie sich auf die in der Version 1.39 enthaltenen Änderungen.

10. Februar 2025

Connector 3.9.49

Diese Version des BlueXP Connector enthält kleinere Sicherheitsverbesserungen und Fehlerbehebungen.

Derzeit ist die Version 3.9.49 für den Standardmodus und den eingeschränkten Modus verfügbar.

BlueXP Identitäts- und Zugriffsmanagement (IAM)

- Unterstützung für die Zuweisung mehrerer Rollen zu einem BlueXP Benutzer.
- Unterstützung für die Zuweisung einer Rolle für mehrere Ressourcen der BlueXP -Organisation (Org/Ordner/Projekt)
- Rollen sind jetzt einer von zwei Kategorien zugeordnet: Plattform und Datendienst.

Der eingeschränkte Modus verwendet jetzt BlueXP IAM

Das Identitäts- und Zugriffsmanagement (IAM) von BlueXP wird jetzt im eingeschränkten Modus verwendet.

BlueXP Identity and Access Management (IAM) ist ein Ressourcen- und Zugriffsverwaltungsmodell, das die bisherige Funktionalität von BlueXP -Konten ersetzt und erweitert, wenn BlueXP im Standard- und eingeschränkten Modus verwendet wird.

Ähnliche Informationen

- "Erfahren Sie mehr über BlueXP IAM"
- "Erste Schritte mit BlueXP IAM"

BlueXP IAM bietet eine detailliertere Verwaltung von Ressourcen und Berechtigungen:

- Eine *Organisation* auf oberster Ebene ermöglicht Ihnen die Verwaltung des Zugriffs über Ihre verschiedenen *Projekte* hinweg.
- *Ordner* ermöglichen Ihnen, verwandte Projekte zu gruppieren.
- Dank der erweiterten Ressourcenverwaltung können Sie eine Ressource einem oder mehreren Ordnern oder Projekten zuordnen.

  Sie können beispielsweise ein Cloud Volumes ONTAP -System mit mehreren Projekten verknüpfen.

- Dank der erweiterten Zugriffsverwaltung können Sie Mitgliedern auf verschiedenen Ebenen der Organisationshierarchie eine Rolle zuweisen.

Diese Verbesserungen bieten eine bessere Kontrolle über die Aktionen, die Benutzer ausführen können, und die Ressourcen, auf die sie zugreifen können.

Wie sich BlueXP IAM im eingeschränkten Modus auf Ihr bestehendes Konto auswirkt

Wenn Sie sich bei BlueXP anmelden, werden Sie diese Änderungen bemerken:

- Ihr *Konto* heißt jetzt *Organisation*
- Ihre *Arbeitsbereiche* heißen jetzt *Projekte*
- Die Namen der Benutzerrollen haben sich geändert:
  - *Kontoadministrator* ist jetzt *Organisationsadministrator*
  - *Arbeitsbereichsadministrator* ist jetzt *Ordner- oder Projektadministrator*
  - *Compliance Viewer* heißt jetzt *Classification Viewer*
- Unter Einstellungen können Sie auf die BlueXP -Identitäts- und Zugriffsverwaltung zugreifen, um diese Verbesserungen zu nutzen

Beachten Sie Folgendes:

- An Ihren bestehenden Benutzern oder Arbeitsumgebungen ergeben sich keine Änderungen.

- Während sich die Namen der Rollen geändert haben, gibt es aus Sicht der Berechtigungen keine Unterschiede. Den Benutzern stehen weiterhin dieselben Arbeitsumgebungen wie bisher zur Verfügung.
- Es gibt keine Änderungen an der Anmeldung bei BlueXP. BlueXP IAM funktioniert mit NetApp Cloud-Anmeldungen, Anmeldeinformationen für die NetApp Support-Site und Verbundverbindungen, genau wie BlueXP Konten.
- Wenn Sie mehrere BlueXP -Konten hatten, verfügen Sie jetzt über mehrere BlueXP -Organisationen.

API für BlueXP IAM

Diese Änderung führt eine neue API für BlueXP IAM ein, ist jedoch abwärtskompatibel mit der vorherigen Tenancy-API. "Erfahren Sie mehr über die API für BlueXP IAM"

Unterstützte Bereitstellungsmodi

BlueXP IAM wird unterstützt, wenn BlueXP im Standard- und eingeschränkten Modus verwendet wird. Wenn Sie BlueXP im privaten Modus verwenden, verwenden Sie weiterhin ein BlueXP -Konto, um Arbeitsbereiche, Benutzer und Ressourcen zu verwalten.

Freigabe des Privatmodus (3.9.48)

Eine neue Version des privaten Modus steht jetzt zum Download bereit von der "NetApp Support Site"

Die Version 3.9.48 enthält Updates für die folgenden BlueXP Komponenten und -Dienste.

Komponente oder Dienst	In dieser Version enthaltene Version	Änderungen seit der letzten Version des privaten Modus
Anschluss	3.9.48	Gehen Sie zum "Was ist neu auf der BlueXP Connector-Seite?" und beziehen Sie sich auf die in den Versionen 3.9.48 enthaltenen Änderungen.
Sicherung und Wiederherstellung	21. Februar 2025	Gehen Sie zum "Was ist neu auf der BlueXP backup and recovery?" und beziehen Sie sich auf die Änderungen, die in der Version vom Februar 2025 enthalten sind.
Einstufung	22. Januar 2025 (Version 1.39)	Gehen Sie zum "Was ist neu auf der BlueXP classification ?" und beziehen Sie sich auf die in der Version 1.39 enthaltenen Änderungen.

13. Januar 2025

Connector 3.9.48

Diese Version des BlueXP Connector enthält kleinere Sicherheitsverbesserungen und Fehlerbehebungen.

Derzeit ist die Version 3.9.48 für den Standardmodus und den eingeschränkten Modus verfügbar.

BlueXP Identitäts- und Zugriffsverwaltung

- Auf der Ressourcenseite werden jetzt unentdeckte Ressourcen angezeigt. Unentdeckte Ressourcen sind Speicherressourcen, die BlueXP kennt, für die Sie aber keine Arbeitsumgebungen erstellt haben. Beispielsweise werden Ressourcen, die im Digital Advisor angezeigt werden und noch keine Arbeitsumgebungen haben, auf der Seite „Ressourcen“ als unentdeckte Ressourcen angezeigt.
- Amazon FSx for NetApp ONTAP -Ressourcen werden auf der IAM-Ressourcenseite nicht angezeigt, da Sie sie keiner IAM-Rolle zuordnen können. Sie können diese Ressourcen auf ihrer jeweiligen Leinwand oder aus Arbeitslasten anzeigen.

Erstellen Sie einen Supportfall für zusätzliche BlueXP -Dienste

Nachdem Sie BlueXP für den Support registriert haben, können Sie direkt über die webbasierte BlueXP -Konsole einen Supportfall erstellen. Wenn Sie den Fall erstellen, müssen Sie den Dienst auswählen, mit dem das Problem verknüpft ist.

Ab dieser Version können Sie jetzt einen Supportfall erstellen und ihn mit zusätzlichen BlueXP Diensten verknüpfen:

- BlueXP disaster recovery
- BlueXP ransomware protection

"Erfahren Sie mehr über das Erstellen eines Supportfalls" .

16. Dezember 2024

Neue sichere Endpunkte zum Abrufen von Connector-Bildern

Wenn Sie den Connector installieren oder wenn ein automatisches Upgrade erfolgt, kontaktiert der Connector Repositorys, um Images für die Installation oder das Upgrade herunterzuladen. Standardmäßig hat der Connector immer die folgenden Endpunkte kontaktiert:

- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

Der erste Endpunkt enthält ein Platzhalterzeichen, da wir keinen definitiven Standort angeben können. Der Lastenausgleich des Repository wird vom Dienstanbieter verwaltet, was bedeutet, dass die Downloads von verschiedenen Endpunkten aus erfolgen können.

Zur Erhöhung der Sicherheit kann der Connector jetzt Installations- und Upgrade-Images von dedizierten Endpunkten herunterladen:

- https://bluexpinfraprod.eastus2.data.azurecr.io
- https://bluexpinfraprod.azurecr.io

Wir empfehlen Ihnen, mit der Verwendung dieser neuen Endpunkte zu beginnen, indem Sie die vorhandenen Endpunkte aus Ihren Firewall-Regeln entfernen und die neuen Endpunkte zulassen.

Diese neuen Endpunkte werden ab der Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.

Beachten Sie Folgendes:

- Die vorhandenen Endpunkte werden weiterhin unterstützt. Wenn Sie die neuen Endpunkte nicht verwenden möchten, sind keine Änderungen erforderlich.
- Der Connector kontaktiert zuerst die vorhandenen Endpunkte. Wenn diese Endpunkte nicht erreichbar sind, kontaktiert der Connector automatisch die neuen Endpunkte.
- Die neuen Endpunkte werden in den folgenden Szenarien nicht unterstützt:
  - Wenn der Connector in einer Regierungsregion installiert ist.
  - Wenn Sie den Connector mit BlueXP backup and recovery oder BlueXP ransomware protection verwenden.

  Für beide Szenarien können Sie die vorhandenen Endpunkte weiterhin verwenden.

9. Dezember 2024

Connector 3.9.47

Diese Version des BlueXP Connectors enthält Fehlerbehebungen und eine Änderung der Endpunkte, die während der Connector-Installation kontaktiert werden.

Derzeit ist die Version 3.9.47 für den Standardmodus und den eingeschränkten Modus verfügbar.

Endpunkt zur Kontaktaufnahme mit dem NetApp -Support während der Installation

Wenn Sie den Connector manuell installieren, kontaktiert das Installationsprogramm nicht mehr https://support.netapp.com.

Der Installateur kontaktiert weiterhin https://mysupport.netapp.com.

BlueXP Identitäts- und Zugriffsverwaltung

Auf der Seite „Konnektoren“ werden nur die derzeit verfügbaren Konnektoren aufgelistet. Von Ihnen entfernte Konnektoren werden nicht mehr angezeigt.

26. November 2024

Freigabe des Privatmodus (3.9.46)

Eine neue Version des privaten Modus steht jetzt zum Download bereit von der "NetApp Support Site"

Die Version 3.9.46 enthält Updates für die folgenden BlueXP Komponenten und -Dienste.

Komponente oder Dienst	In dieser Version enthaltene Version	Änderungen seit der letzten Version des privaten Modus
Anschluss	3.9.46	Kleinere Sicherheitsverbesserungen und Fehlerbehebungen
Sicherung und Wiederherstellung	22. November 2024	Gehen Sie zum "Was ist neu auf der BlueXP backup and recovery?" und beziehen Sie sich auf die Änderungen, die in der Version vom November 2024 enthalten sind

Komponente oder Dienst	In dieser Version enthaltene Version	Änderungen seit der letzten Version des privaten Modus
Einstufung	4. November 2024 (Version 1.37)	Gehen Sie zum "Was ist neu auf der BlueXP classification ?" und beziehen Sie sich auf die Änderungen in den Versionen 1.32 bis 1.37
Cloud Volumes ONTAP Verwaltung	11. November 2024	Gehen Sie zum "Neuigkeiten zur Cloud Volumes ONTAP -Verwaltungsseite" und beziehen Sie sich auf die Änderungen, die in den Versionen vom Oktober 2024 und November 2024 enthalten sind
On-Premises ONTAP Clusterverwaltung	26. November 2024	Gehen Sie zum "Neuigkeiten zur On-Premises ONTAP -Clusterverwaltungsseite" und beziehen Sie sich auf die Änderungen, die in der Version vom November 2024 enthalten sind

Obwohl die BlueXP digital wallet und die BlueXP replication auch im privaten Modus enthalten sind, gibt es gegenüber der vorherigen Version des privaten Modus keine Änderungen.

Weitere Einzelheiten zum privaten Modus, einschließlich der Aktualisierungsinformationen, finden Sie hier:

- "Erfahren Sie mehr über den privaten Modus"
- "Erfahren Sie, wie Sie mit BlueXP im privaten Modus beginnen"
- "Erfahren Sie, wie Sie den Connector im privaten Modus aktualisieren."

11. November 2024

Connector 3.9.46

Diese Version des BlueXP Connector enthält kleinere Sicherheitsverbesserungen und Fehlerbehebungen.

Derzeit ist die Version 3.9.46 für den Standardmodus und den eingeschränkten Modus verfügbar.

ID für IAM-Projekte

Sie können jetzt die ID für ein Projekt aus der BlueXP Identitäts- und Zugriffsverwaltung anzeigen. Möglicherweise müssen Sie die ID verwenden, wenn Sie einen API-Aufruf tätigen.

"Erfahren Sie, wie Sie die ID für ein Projekt erhalten" .

10. Oktober 2024

Connector 3.9.45-Patch

Dieser Patch enthält Fehlerbehebungen.

7. Oktober 2024

BlueXP Identitäts- und Zugriffsverwaltung

BlueXP Identity and Access Management (IAM) ist ein neues Ressourcen- und Zugriffsverwaltungsmodell, das die bisherige Funktionalität der BlueXP -Konten bei Verwendung von BlueXP im Standardmodus ersetzt und erweitert.

BlueXP IAM bietet eine detailliertere Verwaltung von Ressourcen und Berechtigungen:

- Eine *Organisation* auf oberster Ebene ermöglicht Ihnen die Verwaltung des Zugriffs über Ihre verschiedenen *Projekte* hinweg.
- *Ordner* ermöglichen Ihnen, verwandte Projekte zu gruppieren.
- Dank der erweiterten Ressourcenverwaltung können Sie eine Ressource einem oder mehreren Ordnern oder Projekten zuordnen.

  Sie können beispielsweise ein Cloud Volumes ONTAP -System mit mehreren Projekten verknüpfen.

- Dank der erweiterten Zugriffsverwaltung können Sie Mitgliedern auf verschiedenen Ebenen der Organisationshierarchie eine Rolle zuweisen.

Diese Verbesserungen bieten eine bessere Kontrolle über die Aktionen, die Benutzer ausführen können, und die Ressourcen, auf die sie zugreifen können.

Wie sich BlueXP IAM auf Ihr bestehendes Konto auswirkt

Wenn Sie sich bei BlueXP anmelden, werden Sie diese Änderungen bemerken:

- Ihr *Konto* heißt jetzt *Organisation*
- Ihre *Arbeitsbereiche* heißen jetzt *Projekte*
- Die Namen der Benutzerrollen haben sich geändert:
  - *Kontoadministrator* ist jetzt *Organisationsadministrator*
  - *Arbeitsbereichsadministrator* ist jetzt *Ordner- oder Projektadministrator*
  - *Compliance Viewer* heißt jetzt *Classification Viewer*
- Unter Einstellungen können Sie auf die BlueXP -Identitäts- und Zugriffsverwaltung zugreifen, um diese Verbesserungen zu nutzen

Beachten Sie Folgendes:

- An Ihren bestehenden Benutzern oder Arbeitsumgebungen ergeben sich keine Änderungen.
- Während sich die Namen der Rollen geändert haben, gibt es aus Sicht der Berechtigungen keine Unterschiede. Den Benutzern stehen weiterhin dieselben Arbeitsumgebungen wie bisher zur Verfügung.
- Es gibt keine Änderungen an der Anmeldung bei BlueXP. BlueXP IAM funktioniert mit NetApp Cloud-Anmeldungen, Anmeldeinformationen für die NetApp Support-Site und Verbundverbindungen, genau wie BlueXP Konten.
- Wenn Sie mehrere BlueXP -Konten hatten, verfügen Sie jetzt über mehrere BlueXP -Organisationen.

API für BlueXP IAM

Diese Änderung führt eine neue API für BlueXP IAM ein, ist jedoch abwärtskompatibel mit der vorherigen Tenancy-API. "Erfahren Sie mehr über die API für BlueXP IAM"

Unterstützte Bereitstellungsmodi

BlueXP IAM wird unterstützt, wenn BlueXP im Standardmodus verwendet wird. Wenn Sie BlueXP im eingeschränkten oder privaten Modus verwenden, verwenden Sie weiterhin ein BlueXP -*Konto*, um Arbeitsbereiche, Benutzer und Ressourcen zu verwalten.

Wohin als nächstes?

- "Erfahren Sie mehr über BlueXP IAM"
- "Erste Schritte mit BlueXP IAM"

Connector 3.9.45

Diese Version enthält erweiterte Betriebssystemunterstützung und Fehlerbehebungen.

Die Version 3.9.45 ist für den Standardmodus und den eingeschränkten Modus verfügbar.

Unterstützung für Ubuntu 24.04 LTS

Ab der Version 3.9.45 unterstützt BlueXP jetzt Neuinstallationen des Connectors auf Ubuntu 24.04 LTS-Hosts, wenn BlueXP im Standardmodus oder eingeschränkten Modus verwendet wird.

"Hostanforderungen für View Connector" .

Unterstützung für SELinux mit RHEL-Hosts

BlueXP unterstützt jetzt den Connector mit Red Hat Enterprise Linux-Hosts, auf denen SELinux entweder im Enforcing- oder im Permissive-Modus aktiviert ist.

Die Unterstützung für SELinux beginnt mit der Version 3.9.40 für den Standardmodus und den eingeschränkten Modus und mit der Version 3.9.42 für den privaten Modus.

Beachten Sie die folgenden Einschränkungen:

- BlueXP unterstützt SELinux mit Ubuntu-Hosts nicht.
- Die Verwaltung von Cloud Volumes ONTAP -Systemen wird von Connectors nicht unterstützt, auf deren Betriebssystem SELinux aktiviert ist.

"Erfahren Sie mehr über SELinux"

30. September 2024

Freigabe des Privatmodus (3.9.44)

Eine neue Version des privaten Modus steht jetzt zum Download von der NetApp Support-Site bereit.

Diese Version enthält die folgenden Versionen der BlueXP Komponenten und -Dienste, die im privaten Modus unterstützt werden.

Service	Version enthalten
Anschluss	3.9.44
Sicherung und Wiederherstellung	27. September 2024
Einstufung	15. Mai 2024 (Version 1.31)

Service	Version enthalten
Cloud Volumes ONTAP Verwaltung	9. September 2024
Digitale Geldbörse	30. Juli 2023
On-Premises ONTAP Clusterverwaltung	22. April 2024
Replikation	18. September 2022

Für den Connector enthält die Version 3.9.44 für den privaten Modus die in den Versionen vom August 2024 und September 2024 eingeführten Updates. Vor allem die Unterstützung für Red Hat Enterprise Linux 9.4.

Weitere Informationen zum Inhalt der Versionen dieser BlueXP Komponenten und -Dienste finden Sie in den Versionshinweisen zu den einzelnen BlueXP Diensten:

- "Was ist neu in der Connector-Version vom September 2024?"
- "Was ist neu in der Connector-Version vom August 2024?"
- "Was ist neu bei BlueXP backup and recovery"
- "Was ist neu bei der BlueXP classification?"
- "Was ist neu beim Cloud Volumes ONTAP -Management in BlueXP"

Weitere Einzelheiten zum privaten Modus, einschließlich der Aktualisierungsinformationen, finden Sie hier:

- "Erfahren Sie mehr über den privaten Modus"
- "Erfahren Sie, wie Sie mit BlueXP im privaten Modus beginnen"
- "Erfahren Sie, wie Sie den Connector im privaten Modus aktualisieren."

9. September 2024

Konnektor 3.9.44

Diese Version enthält Unterstützung für Docker Engine 26, eine Verbesserung der SSL-Zertifikate und Fehlerbehebungen.

Die Version 3.9.44 ist für den Standardmodus und den eingeschränkten Modus verfügbar.

Unterstützung für Docker Engine 26 bei Neuinstallationen

Ab der Version 3.9.44 des Connectors wird Docker Engine 26 jetzt mit *neuen* Connector-Installationen auf Ubuntu-Hosts unterstützt.

Wenn Sie über einen vorhandenen Connector verfügen, der vor der Version 3.9.44 erstellt wurde, ist Docker Engine 25.0.5 immer noch die maximal unterstützte Version auf Ubuntu-Hosts.

"Erfahren Sie mehr über die Anforderungen der Docker Engine" .

Aktualisiertes SSL-Zertifikat für den lokalen UI-Zugriff

Wenn Sie BlueXP im eingeschränkten oder privaten Modus verwenden, ist die Benutzeroberfläche über die Connector-VM zugänglich, die in Ihrer Cloud-Region oder vor Ort bereitgestellt wird. Standardmäßig verwendet BlueXP ein selbstsigniertes SSL-Zertifikat, um sicheren HTTPS-Zugriff auf die webbasierte Konsole bereitzustellen, die auf dem Connector ausgeführt wird.

In dieser Version haben wir Änderungen am SSL-Zertifikat für neue und vorhandene Connectors

vorgenommen:

- Der allgemeine Name für das Zertifikat entspricht jetzt dem kurzen Hostnamen
- Der alternative Name des Zertifikatsinhabers ist der vollqualifizierte Domänenname (FQDN) des Hostcomputers

Unterstützung für RHEL 9.4

BlueXP unterstützt jetzt die Installation des Connectors auf einem Red Hat Enterprise Linux 9.4-Host, wenn BlueXP im Standardmodus oder eingeschränkten Modus verwendet wird.

Die Unterstützung für RHEL 9.4 beginnt mit der Version 3.9.40 des Connectors.

Die aktualisierte Liste der unterstützten RHEL-Versionen für den Standardmodus und den eingeschränkten Modus enthält jetzt Folgendes:

- 8,6 bis 8,10
- 9,1 bis 9,4

"Erfahren Sie mehr über die Unterstützung für RHEL 8 und 9 mit dem Connector" .

Unterstützung für Podman 4.9.4 mit allen RHEL-Versionen

Podman 4.9.4 wird jetzt mit allen unterstützten Versionen von Red Hat Enterprise Linux unterstützt. Version 4.9.4 wurde zuvor nur mit RHEL 8.10 unterstützt.

Die aktualisierte Liste der unterstützten Podman-Versionen umfasst 4.6.1 und 4.9.4 mit Red Hat Enterprise Linux-Hosts.

Podman ist für RHEL-Hosts ab der Version 3.9.40 des Connectors erforderlich.

"Erfahren Sie mehr über die Unterstützung für RHEL 8 und 9 mit dem Connector" .

Aktualisierte AWS- und Azure-Berechtigungen

Wir haben die AWS- und Azure-Richtlinien für den Connector aktualisiert, um nicht mehr benötigte Berechtigungen zu entfernen. Die Berechtigungen bezogen sich auf das BlueXP -Edge-Caching sowie die Erkennung und Verwaltung von Kubernetes-Clustern, die ab August 2024 nicht mehr unterstützt werden.

- "Erfahren Sie, was sich in der AWS-Richtlinie geändert hat" .
- "Erfahren Sie, was sich in der Azure-Richtlinie geändert hat" .

22. August 2024

Connector 3.9.43-Patch

Wir haben den Connector aktualisiert, um die Version 9.15.1 von Cloud Volumes ONTAP zu unterstützen.

Der Support für diese Version umfasst ein Update der Connector-Richtlinie für Azure. Die Richtlinie umfasst jetzt die folgenden Berechtigungen:

```
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Compute/virtualMachineScaleSets/read",
"Microsoft.Compute/virtualMachineScaleSets/delete"
```

Diese Berechtigungen sind für die Cloud Volumes ONTAP Unterstützung von Virtual Machine Scale Sets erforderlich. Wenn Sie über vorhandene Connectors verfügen und diese neue Funktion verwenden möchten, müssen Sie diese Berechtigungen den benutzerdefinierten Rollen hinzufügen, die Ihren Azure-Anmeldeinformationen zugeordnet sind.

- "Erfahren Sie mehr über die Version Cloud Volumes ONTAP 9.15.1"
- "Anzeigen von Azure-Berechtigungen für den Connector" .

8. August 2024

Konnektor 3.9.43

Diese Version enthält kleinere Verbesserungen und Fehlerbehebungen.

Die Version 3.9.43 ist für den Standardmodus und den eingeschränkten Modus verfügbar.

Aktualisierte CPU- und RAM-Anforderungen

Um eine höhere Zuverlässigkeit zu gewährleisten und die Leistung von BlueXP und Connector zu verbessern, benötigen wir jetzt zusätzliche CPU und RAM für die virtuelle Connector-Maschine:

- CPU: 8 Kerne oder 8 vCPUs (die vorherige Anforderung war 4)
- RAM: 32 GB (bisher waren 14 GB erforderlich)

Als Ergebnis dieser Änderung lautet der Standard-VM-Instanztyp beim Bereitstellen des Connectors von BlueXP oder vom Marktplatz des Cloud-Anbieters wie folgt:

- AWS: t3.2xlarge
- Azure: Standard_D8s_v3
- Google Cloud: n2-standard-8

Die aktualisierten CPU- und RAM-Anforderungen gelten für alle neuen Connectors. Für vorhandene Connectors wird eine Erhöhung der CPU und des RAM empfohlen, um eine verbesserte Leistung und Zuverlässigkeit zu erzielen.

Unterstützung für Podman 4.9.4 mit RHEL 8.10

Podman Version 4.9.4 wird jetzt unterstützt, wenn der Connector auf einem Red Hat Enterprise Linux 8.10-Host installiert wird.

Benutzervalidierung für die Identitätsföderation

Wenn Sie die Identitätsföderation mit BlueXP verwenden, muss jeder Benutzer, der sich zum ersten Mal bei BlueXP anmeldet, ein kurzes Formular ausfüllen, um seine Identität zu bestätigen.

31. Juli 2024

Freigabe des Privatmodus (3.9.42)

Eine neue Version des privaten Modus steht jetzt zum Download von der NetApp Support-Site bereit.

Unterstützung für RHEL 8 und 9

Diese Version umfasst Unterstützung für die Installation des Connectors auf einem Red Hat Enterprise Linux 8- oder 9-Host, wenn BlueXP im privaten Modus verwendet wird. Die folgenden Versionen von RHEL werden unterstützt:

- 8,6 bis 8,10
- 9,1 bis 9,3

Für diese Betriebssysteme wird Podman als Container-Orchestrierungstool benötigt.

Sie sollten sich über die Podman-Anforderungen und bekannten Einschränkungen im Klaren sein, eine Zusammenfassung der Betriebssystemunterstützung erhalten, wissen, was zu tun ist, wenn Sie einen RHEL 7-Host haben, wie Sie beginnen und mehr.

"Erfahren Sie mehr über die Unterstützung für RHEL 8 und 9 mit dem Connector" .

In dieser Version enthaltene Versionen

Diese Version enthält die folgenden Versionen der BlueXP -Dienste, die im privaten Modus unterstützt werden.

Service	Version enthalten
Anschluss	3.9.42
Sicherung und Wiederherstellung	18. Juli 2024
Einstufung	1. Juli 2024 (Version 1.33)
Cloud Volumes ONTAP Verwaltung	10. Juni 2024
Digitale Geldbörse	30. Juli 2023
On-Premises ONTAP Clusterverwaltung	30. Juli 2023
Replikation	18. September 2022

Weitere Informationen zum Inhalt der Versionen dieser BlueXP -Dienste finden Sie in den Versionshinweisen zu den einzelnen BlueXP Diensten.

- "Erfahren Sie mehr über den privaten Modus"
- "Erfahren Sie, wie Sie mit BlueXP im privaten Modus beginnen"
- "Erfahren Sie, wie Sie den Connector im privaten Modus aktualisieren."
- "Erfahren Sie, was es Neues bei BlueXP backup and recovery gibt"
- "Erfahren Sie, was es Neues bei der BlueXP classification gibt"
- "Erfahren Sie, was es Neues beim Cloud Volumes ONTAP Management in BlueXP gibt"

15. Juli 2024

Unterstützung für RHEL 8.10

BlueXP unterstützt jetzt die Installation des Connectors auf einem Red Hat Enterprise Linux 8.10-Host im Standardmodus oder eingeschränkten Modus.

Die Unterstützung für RHEL 8.10 beginnt mit der Version 3.9.40 des Connectors.

"Erfahren Sie mehr über die Unterstützung für RHEL 8 und 9 mit dem Connector" .

8. Juli 2024

Konnektor 3.9.42

Diese Version enthält kleinere Verbesserungen, Fehlerbehebungen und Unterstützung für den Connector in der AWS-Region Kanada West (Calgary).

Die Version 3.9.42 ist für den Standardmodus und den eingeschränkten Modus verfügbar.

Aktualisierte Docker Engine-Anforderungen

Wenn der Connector auf einem Ubuntu-Host installiert ist, ist die minimal unterstützte Version der Docker Engine jetzt 23.0.6. Zuvor war es 19.3.1.

Die maximal unterstützte Version ist weiterhin 25.0.5.

"Hostanforderungen für View Connector" .

E-Mail-Verifizierung jetzt erforderlich

Neue Benutzer, die sich bei BlueXP anmelden, müssen jetzt ihre E-Mail-Adresse bestätigen, bevor sie sich anmelden können.

12. Juni 2024

Konnektor 3.9.41

Diese Version des BlueXP Connector enthält kleinere Sicherheitsverbesserungen und Fehlerbehebungen.

Die Version 3.9.41 ist für den Standardmodus und den eingeschränkten Modus verfügbar.

4. Juni 2024

Freigabe des Privatmodus (3.9.40)

Eine neue Version des privaten Modus steht jetzt zum Download von der NetApp Support-Site bereit. Diese Version enthält die folgenden Versionen der BlueXP -Dienste, die im privaten Modus unterstützt werden.

Beachten Sie, dass diese Version im privaten Modus *keine* Unterstützung für den Connector mit Red Hat Enterprise Linux 8 und 9 enthält.

Service	Version enthalten
Anschluss	3.9.40
Sicherung und Wiederherstellung	17. Mai 2024
Einstufung	15. Mai 2024 (Version 1.31)
Cloud Volumes ONTAP Verwaltung	17. Mai 2024
Digitale Geldbörse	30. Juli 2023
On-Premises ONTAP Clusterverwaltung	30. Juli 2023
Replikation	18. September 2022

Weitere Informationen zum Inhalt der Versionen dieser BlueXP -Dienste finden Sie in den Versionshinweisen zu den einzelnen BlueXP Diensten.

- "Erfahren Sie mehr über den privaten Modus"
- "Erfahren Sie, wie Sie mit BlueXP im privaten Modus beginnen"
- "Erfahren Sie, wie Sie den Connector im privaten Modus aktualisieren."
- "Erfahren Sie, was es Neues bei BlueXP backup and recovery gibt"
- "Erfahren Sie, was es Neues bei der BlueXP classification gibt"
- "Erfahren Sie, was es Neues beim Cloud Volumes ONTAP Management in BlueXP gibt"

17. Mai 2024

Konnektor 3.9.40

Diese Version des BlueXP Connector umfasst Unterstützung für zusätzliche Betriebssysteme, kleinere Sicherheitsverbesserungen und Fehlerbehebungen.

Derzeit ist die Version 3.9.40 für den Standardmodus und den eingeschränkten Modus verfügbar.

Unterstützung für RHEL 8 und 9

Der Connector wird jetzt auf Hosts unterstützt, auf denen die folgenden Versionen von Red Hat Enterprise Linux mit *neuen* Connector-Installationen ausgeführt werden, wenn BlueXP im Standardmodus oder eingeschränkten Modus verwendet wird:

- 8,6 bis 8,9
- 9,1 bis 9,3

Für diese Betriebssysteme wird Podman als Container-Orchestrierungstool benötigt.

Sie sollten sich über die Podman-Anforderungen und bekannten Einschränkungen im Klaren sein, eine Zusammenfassung der Betriebssystemunterstützung erhalten, wissen, was zu tun ist, wenn Sie einen RHEL 7-Host haben, wie Sie beginnen und mehr.

"Erfahren Sie mehr über die Unterstützung für RHEL 8 und 9 mit dem Connector" .

Ende des Supports für RHEL 7 und CentOS 7

Am 30. Juni 2024 erreicht RHEL 7 das Ende der Wartung (EOM), während CentOS 7 das Ende seiner Lebensdauer (EOL) erreicht. NetApp wird den Connector auf diesen Linux-Distributionen bis zum 30. Juni

2024 weiterhin unterstützen.

"Erfahren Sie, was zu tun ist, wenn Sie einen vorhandenen Connector auf RHEL 7 oder CentOS 7 ausführen."
.

AWS-Berechtigungsaktualisierung

In der Version 3.9.38 haben wir die Connector-Richtlinie für AWS aktualisiert, um die Berechtigung „ec2:DescribeAvailabilityZones“ einzuschließen. Diese Berechtigung ist jetzt erforderlich, um AWS Local Zones mit Cloud Volumes ONTAP zu unterstützen.

- "AWS-Berechtigungen für den Connector anzeigen" .
- "Erfahren Sie mehr über die Unterstützung für AWS Local Zones"

Bekannte Einschränkungen der NetApp Console

Bekannte Einschränkungen kennzeichnen Plattformen, Geräte oder Funktionen, die von dieser Produktversion nicht unterstützt werden oder nicht ordnungsgemäß mit ihr zusammenarbeiten. Lesen Sie diese Einschränkungen sorgfältig durch.

Diese Einschränkungen gelten speziell für die Einrichtung der NEtApp-Konsole und -Verwaltung: den Agenten, die Software-as-a-Service-Plattform (SaaS) und mehr.

Einschränkungen des Konsolenagenten

Möglicher Konflikt mit IP-Adressen im Bereich 172

Die NetApp Console stellt einen Agenten mit zwei Schnittstellen bereit, die IP-Adressen in den Bereichen 172.17.0.0/16 und 172.18.0.0/16 haben.

Wenn in Ihrem Netzwerk ein Subnetz mit einem dieser Bereiche konfiguriert ist, kann es bei der Konsole zu Verbindungsfehlern kommen. Beispielsweise kann die Erkennung lokaler ONTAP Cluster in der Konsole fehlschlagen.

Siehe Knowledge Base-Artikel"Agent-IP-Konflikt mit vorhandenem Netzwerk" Anweisungen zum Ändern der IP-Adresse der Schnittstellen des Agenten.

SSL-Entschlüsselung wird nicht unterstützt

Die Konsole unterstützt keine Firewall-Konfigurationen mit aktivierter SSL-Entschlüsselung. Wenn die SSL-Entschlüsselung aktiviert ist, werden in der Konsole Fehlermeldungen angezeigt und die Agenteninstanz wird als inaktiv angezeigt.

Für mehr Sicherheit haben Sie die Möglichkeit,"Installieren Sie ein von einer Zertifizierungsstelle (CA) signiertes HTTPS-Zertifikat." .

Leere Seite beim Laden der lokalen Benutzeroberfläche

Wenn Sie die webbasierte Konsole laden, die auf einem Agenten ausgeführt wird, kann es vorkommen, dass die Schnittstelle manchmal nicht angezeigt wird und Sie nur eine leere Seite erhalten.

Dieses Problem hängt mit einem Caching-Problem zusammen. Die Problemumgehung besteht darin, eine Inkognito- oder private Webbrowser-Sitzung zu verwenden.

Gemeinsam genutzte Linux-Hosts werden nicht unterstützt

Der Agent wird auf einer VM, die mit anderen Anwendungen gemeinsam genutzt wird, nicht unterstützt. Die VM muss der Agentensoftware gewidmet sein.

Agenten und Erweiterungen von Drittanbietern

Agenten oder VM-Erweiterungen von Drittanbietern werden auf der Agent-VM nicht unterstützt.

Änderungen an unterstützten Linux-Betriebssystemen

NetApp fügt gelegentlich Unterstützung für den Konsolenagenten auf bestimmten Linux-Betriebssystemen hinzu und entfernt diese wieder. Erfahren Sie, wie sich diese Unterstützung auf Ihre vorhandenen Konsolenagenten auswirkt.

Unterstützte Betriebssysteme

NetApp unterstützt den Agenten mit den folgenden Linux-Betriebssystemen.

Standardmodus

Manuelle Installation

- Ubuntu 24.04 LTS
- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8,6 bis 8,10
  - 9,1 bis 9,4

Bereitstellung über die NetApp Console

Ubuntu 22.04 LTS

Bereitstellung über den AWS Marketplace

Ubuntu 22.04 LTS

Bereitstellung über den Azure Marketplace

Ubuntu 22.04 LTS

Eingeschränkter Modus

Manuelle Installation

- Ubuntu 24.04 LTS
- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8,6 bis 8,10
  - 9,1 bis 9,4

Bereitstellung über den AWS Marketplace

Ubuntu 22.04 LTS

Bereitstellung über den Azure Marketplace

Ubuntu 22.04 LTS

Privatmodus

Manuelle Installation

- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8,6 bis 8,10
  - 9,1 bis 9,4

Unterstützung für RHEL 8 und 9

Beachten Sie Folgendes zur Unterstützung für RHEL 8 und 9:

Einschränkungen

NetApp Data Classification wird unterstützt, wenn Sie den Agenten auf einem RHEL 8- oder 9-Host installieren, der sich vor Ort befindet. Es wird nicht unterstützt, wenn sich der RHEL 8- oder 9-Host in AWS,

Azure oder Google Cloud befindet.

Container-Orchestrierungstool

Sie müssen das Podman-Tool als Container-Orchestrierungstool verwenden, wenn Sie den Konsolenagenten auf einem RHEL 8- oder 9-Host installieren. Docker Engine wird mit RHEL 8 und 9 nicht unterstützt.

Bereitstellungsmodus

RHEL 8 und 9 werden unterstützt, wenn die Konsole im Standardmodus und im eingeschränkten Modus verwendet wird.

Unterstützte Konsolen-Agent-Versionen

NetApp unterstützt RHEL 8 und 9 ab den folgenden Versionen des Konsolenagenten:

- 3.9.40 bei Verwendung der Konsole im Standardmodus oder eingeschränkten Modus

Nur neue manuelle Installationen

RHEL 8 und 9 werden mit *neuen* Agenteninstallationen unterstützt, wenn Agenten manuell auf Hosts installiert werden, die bei Ihnen vor Ort oder in der Cloud ausgeführt werden.

RHEL-Upgrades

Wenn Sie einen vorhandenen Agenten auf einem RHEL 7-Host ausführen, unterstützt NetApp kein Upgrade des RHEL 7-Betriebssystems auf RHEL 8 oder 9. Erfahren Sie mehr über vorhandene Konsolenagenten auf RHEL 7 oder CentOS 7 .

Ende des Supports für RHEL 7 und CentOS 7

Am 30. Juni 2024 erreichte RHEL 7 das Ende der Wartung (EOM), während CentOS 7 das Ende seiner Lebensdauer (EOL) erreichte. NetApp hat den Support für Agenten auf diesen Linux-Distributionen am 30. Juni 2024 eingestellt.

"Red Hat: Was Sie über das Ende der Wartung für Red Hat Enterprise Linux 7 wissen sollten"

Vorhandene Konsolenagenten auf RHEL 7 oder CentOS 7

Wenn Sie einen vorhandenen Agenten haben, der auf RHEL 7 oder CentOS 7 ausgeführt wird, unterstützt NetApp kein Upgrade oder keine Konvertierung des Betriebssystems auf RHEL 8 oder 9. Sie müssen einen neuen Agenten auf einem unterstützten Betriebssystem erstellen.

1. Richten Sie einen RHEL 8- oder 9-Host ein.
2. Installieren Sie Podman.
3. Installieren Sie einen *neuen* Agenten.
4. Konfigurieren Sie den Agenten so, dass er die Systeme erkennt, die der vorherige Agent verwaltet hat.

Ähnliche Informationen

Erste Schritte mit RHEL 8 und 9

Auf den folgenden Seiten finden Sie Einzelheiten zu Hostanforderungen, Podman-Anforderungen und Schritten zur Installation von Podman und Cagent:

Standardmodus

- "Installieren und Einrichten eines Konsolen-Agenten vor Ort"
- "Manuelle Installation des Konsolenagenten in AWS"
- "Manuelles Installieren des Konsolen-Agents in Azure"
- "Installieren Sie den Konsolenagenten manuell in Google Cloud"

Eingeschränkter Modus

"Vorbereiten der Bereitstellung im eingeschränkten Modus"

So entdecken Sie Ihre Systeme neu

Auf den folgenden Seiten erfahren Sie, wie Sie Ihre Systeme nach der Bereitstellung eines neuen Konsolenagenten neu erkennen.

- "Hinzufügen vorhandener Cloud Volumes ONTAP -Systeme"
- "Entdecken Sie lokale ONTAP -Cluster"
- "Erstellen oder entdecken Sie ein FSx für ONTAP -System"
- "Erstellen eines Azure NetApp Files Systems"
- "Entdecken Sie die Systeme der E-Serie"
- "Entdecken Sie StorageGRID -Systeme"

Erste Schritte

Lernen Sie die Grundlagen

Erfahren Sie mehr über die NetApp Console

Die NetApp Console ermöglicht die zentrale Verwaltung von NetApp Storage und NetApp Data Services in On-Premises- und Cloud-Umgebungen auf Unternehmensniveau. Sie liefert Einblicke in Echtzeit, schnellere Workflows und vereinfachte Administration mit hoher Sicherheit und Konformität.

Es ist als Serviceplattform (SaaS) verfügbar und bietet Speicherverwaltung, Datenmobilität, Datenschutz sowie Datenanalyse und -kontrolle. Verwaltungsfunktionen werden über eine webbasierte Konsole und APIs bereitgestellt.

Features

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

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

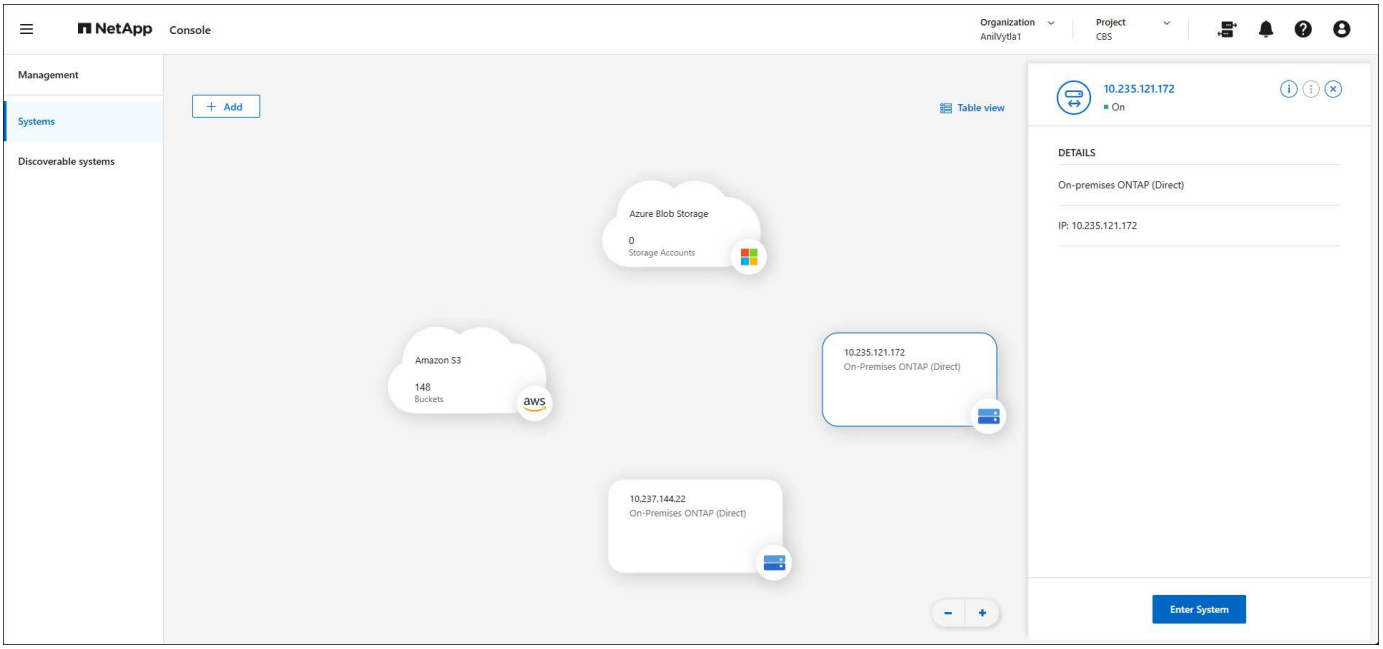
Cloud-Objektspeicher

- 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" .

Bereitstellungsmodi

NetApp bietet zwei Bereitstellungsmodi für die NetApp Console: Der *Standardmodus* verwendet eine Software-as-a-Service-Schicht (SaaS) für die volle Funktionalität, während der *eingeschränkte Modus* die ausgehende Konnektivität begrenzt.

NetApp bietet BlueXP weiterhin für Standorte an, die keine ausgehende Konnektivität benötigen. BlueXP ist nur im privaten Modus verfügbar."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 NetApp Console -Agenten

Ein *Konsolenagent* wird in Ihrem Cloud-Netzwerk oder lokalen Netzwerk ausgeführt. Sie verwenden einen Konsolenagenten, um NetApp Console mit Ihren Speicherumgebungen zu verbinden.

Was Sie ohne Konsolenagent tun können

Einige Konsolenfunktionen und -dienste sind verfügbar, wenn Sie keinen Konsolenagenten bereitstellen:

- Amazon FSx for NetApp ONTAP

Für einige Aktionen ist ein Konsolenagent oder ein NetApp Workloads-Link erforderlich. "Erfahren Sie, für welche Aktionen ein Konsolenagent oder -link erforderlich ist"

- Automatisierungszentrum
- Azure NetApp Files

  Sie benötigen keinen Konsolenagenten, um Azure NetApp Files zu verwalten, aber Sie benötigen einen, um Azure NetApp Files mithilfe der NetApp Data Classification zu scannen.

- Google Cloud NetApp Volumes
- NetApp Copy and Sync
- Digitaler Berater
- Überwachen Sie die Lizenznutzung. Für die Abonnementüberwachung ist ein Konsolenagent erforderlich.

  Normalerweise können Sie der NetApp Console eine Lizenz ohne Konsolenagent hinzufügen.

  Zum Hinzufügen knotenbasierter Lizenzen für Cloud Volumes ONTAP ist ein Agent erforderlich, da die Daten aus den auf Cloud Volumes ONTAP Systemen installierten Lizenzen stammen.

- Direkte Erkennung von On-Premises- ONTAP -Clustern

  Sie benötigen keinen Konsolenagenten, um der Konsole einen lokalen ONTAP Cluster hinzuzufügen, für zusätzliche Konsolenfunktionen und Datendienste ist jedoch einer erforderlich.

  "Erfahren Sie mehr über Erkennungs- und Verwaltungsoptionen für lokale ONTAP Cluster"

- Software-Updates
- Nachhaltigkeit
- NetApp Workloads

Wenn ein Konsolenagent erforderlich ist

Im Standardmodus benötigt die Konsole einen Konsolenagenten für:

- Warnungen
- Amazon FSx für ONTAP -Verwaltungsfunktionen
- Amazon S3-Speicher
- Azure Blob-Speicher
- NetApp Backup and Recovery
- Datenklassifizierung
- Cloud Volumes ONTAP
- NetApp Disaster Recovery
- Systeme der E-Serie
- Wirtschaftlichkeit [1]
- Google Cloud Storage-Buckets
- On-Premises- ONTAP -Cluster-Integration mit NetApp -Datendiensten
- NetApp Ransomware-Resilienz

- StorageGRID -Systeme
- NetApp Cloud Tiering
- NetApp Volume Caching

[1] Sie können auf diese Dienste ohne einen Konsolenagenten zugreifen, zum Einleiten von Aktionen ist jedoch ein Konsolenagent erforderlich.

Sie benötigen immer einen Konsolenagenten, um die Konsole im eingeschränkten Modus zu verwenden.

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. Wie Sie beginnen, hängt davon ab, ob Sie die Konsole im Standardmodus oder im eingeschränkten Modus

verwenden.

- "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-Berechtigungen

Sie benötigen spezielle Berechtigungen, um den Konsolenagenten direkt von der NetApp Console aus zu erstellen, und einen weiteren Satz von Berechtigungen für die Konsolenagenteninstanz 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.

Im Standard- oder eingeschränkten Modus aktualisiert sich der Konsolenagent automatisch, wenn 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 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"

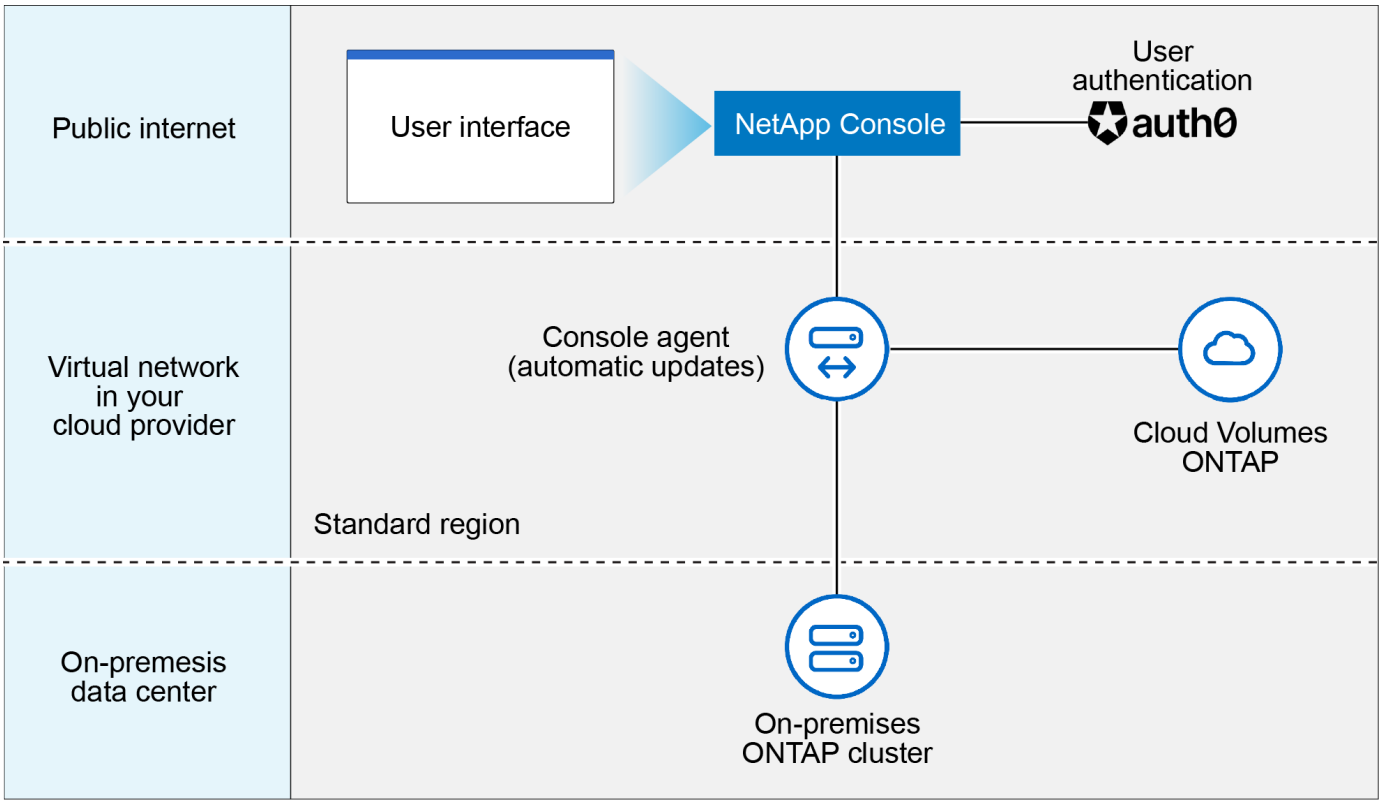
Die folgende Tabelle bietet einen Vergleich der NetApp Konsole.

	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
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.

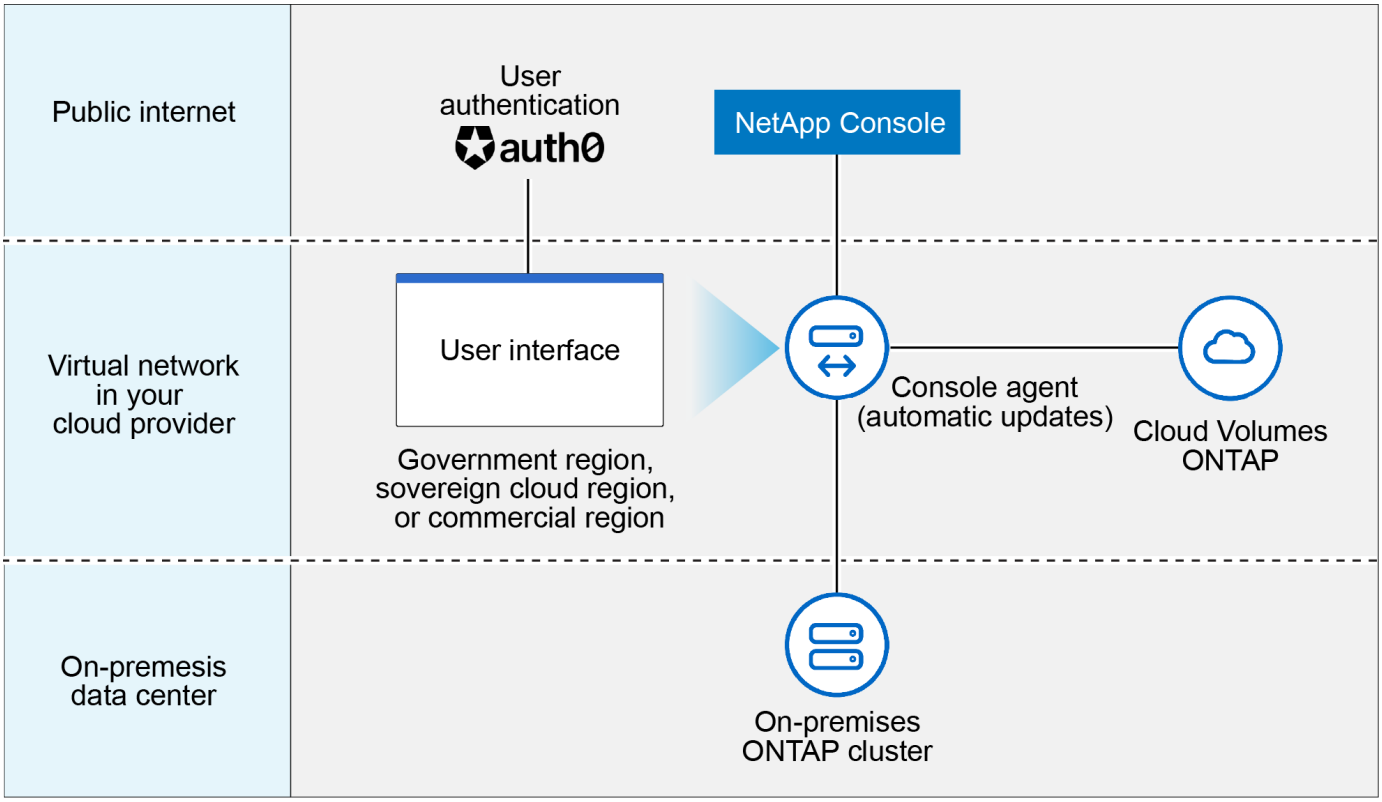
Erste Schritte mit dem Standardmodus

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.

Unterstützte Dienste	Hinweise
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
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

Produktbereich	NetApp -Datendienst oder -Funktion	Eingeschränkter Modus
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

Erste Schritte mit dem NetApp Console Assistenten

Erste Schritte mit dem NetApp Console Assistenten

Wenn Sie die NetApp Console zum ersten Mal mit der Rolle „Organisationsadministrator“ verwenden, können Sie den Konsolenassistenten verwenden, der Sie durch den anfänglichen Einrichtungsprozess führt. Der Assistent unterstützt Sie beim Hinzufügen eines NetApp Support Site (NSS)-Kontos, eines Konsolenagenten, eines Clusters und einer Lizenz oder eines Abonnements und erleichtert Ihnen so den Einstieg in die Verwaltung Ihrer Daten.

Erforderliche Rollen für den Zugriff auf den Konsolenassistenten

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

Wann erscheint der Konsolenassistent?

Der Konsolenassistent ist auf der Startseite der NetApp Console verfügbar, bis die obligatorischen Einrichtungsaufgaben abgeschlossen sind.

Nutzen Sie den Assistenten, um diese, teilweise obligatorischen Aufgaben zu erledigen:

- Fügen Sie ein NetApp Support Site (NSS)-Konto hinzu.
- Stellen Sie eine Verbindung zu Ihrem Speicherbestand her, indem Sie einen Konsolenagenten bereitstellen (obligatorischer Schritt).
- Verwalten Sie Ihr System, indem Sie einen Cluster hinzufügen oder erkennen (obligatorischer Schritt).

- Fügen Sie ein Marktplatzabonnement oder eine PAYGO-Lizenz hinzu.
- Links zu offenen Datendiensten.

Aktivieren Sie den Konsolenassistenten

Standardmäßig zeigt die NetApp Console den Konsolenassistenten auf der Startseite für Erstbenutzer mit der Rolle „Organisationsadministrator“ an.

Sie können den Assistenten erst dann selbst entlassen, wenn Sie oder jemand anderes die obligatorischen Aufgaben erledigt hat. Nachdem Sie die obligatorischen Elemente abgeschlossen haben, wird der Assistent für alle Benutzer in Ihrer Organisation geschlossen und nicht erneut angezeigt.

Verwenden Sie den Konsolenassistenten, um loszulegen

Der Konsolenassistent führt Sie mit den folgenden Aufgaben durch die Einrichtung Ihrer NetApp Console :

- Fügen Sie ein NetApp Support Site (NSS)-Konto hinzu.
- Stellen Sie eine Verbindung zu Ihrem Speicherbestand her, indem Sie einen Konsolenagenten bereitstellen, entweder vor Ort oder in der Cloud. Sie können es manuell oder durch Herunterladen einer OVA bereitstellen. Dieser Schritt ist obligatorisch.
- Verwalten Sie Ihr System, indem Sie einen Cluster hinzufügen oder erkennen. Dieser Schritt ist obligatorisch.
- Fügen Sie ein Marktplatzabonnement oder eine PAYGO-Lizenz hinzu.
- Erfahren Sie mehr über NetApp Datenservices.

Erste Schritte mit dem Standardmodus

Workflow „Erste Schritte“ (Standardmodus)

Beginnen Sie mit der NetApp Console im Standardmodus, indem Sie das Netzwerk für die Konsole vorbereiten, sich anmelden und ein Konto erstellen und optional einen Konsolenagenten erstellen.

Im Standardmodus greifen Sie auf eine webbasierte Konsole zu, die als Software-as-a-Service (SaaS)-Produkt von NetApp gehostet wird. Bevor Sie beginnen, stellen Sie sicher, dass Sie verstehen"Bereitstellungsmodi" Und"Konsolenagenten" .

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

Computer, die auf die NetApp Konsole zugreifen, sollten Verbindungen zu bestimmten Endpunkten haben. Wenn Ihr Netzwerk den ausgehenden Zugriff einschränkt, sollten Sie sicherstellen, dass diese Endpunkte zugelassen werden.

2 **"Registrieren und eine Organisation erstellen"**

Gehen Sie zum "NetApp Konsole" und melden Sie sich an. Sie haben die Möglichkeit, eine Organisation zu erstellen. Sie sollten diesen Schritt jedoch überspringen, wenn Ihr Unternehmen bereits über eine bestehende

Organisation verfügt.

An diesem Punkt sind Sie angemeldet und können mit der Speicherverwaltung und der Verwendung von Diensten wie Digital Advisor, Amazon FSx for ONTAP, Azure NetApp Files und mehr beginnen. "Erfahren Sie, was Sie ohne Konsolenagent tun können" .

Erstellen eines 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"

Um NetApp Intelligent Data Services zum Verwalten von Speicher und Daten in Google Cloud zu verwenden, stellen Sie sicher, dass der Konsolenagent in Google Cloud ausgeführt wird.

"Abonnieren Sie NetApp Intelligent Services (optional)"

Melden Sie sich über Ihren Cloud-Anbieter für NetApp Intelligent Services an und zahlen Sie stundenweise (PAYGO) oder über einen Jahresvertrag. 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.

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
- Netzwerkstandorte, an denen Sie Konsolenagenten bereitstellen, die Sie vor Ort oder in der Cloud installieren.
- Zusätzliche Endpunkte für bestimmte NetApp -Datendienste, einschließlich Cloud Volumes ONTAP.

NetApp hat 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 kontaktierte Endpunkte

Jeder Computer, der auf die NetApp Console zugreift, muss über Verbindungen zu den unten aufgeführten Endpunkten verfügen.

Das System kontaktiert diese Endpunkte in zwei Szenarien:

- Von einem Computer aus, der auf die "NetApp Console" als Software as a Service (SaaS).
- Von einem Computer aus, der direkt auf einen Konsolen-Agent-Host zugreift, entweder um sich anzumelden und ihn einzurichten oder um vom Agent-Host aus auf die Konsole zuzugreifen.

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

Vorbereiten des Netzwerks für den Konsolenagenten

Sie installieren den Konsolenagenten vor Ort oder in der Cloud und er kontaktiert Endpunkte, um von der Konsole initiierte Aktionen abzuschließen.

Konsolenagenten müssen Zugriff auf dieselben Endpunkte haben wie die NetApp Console sowie auf zusätzliche Endpunkte, je nachdem, wo Sie den Agenten installieren.

Richten Sie den Netzwerk-Endpunktzugriff 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"
- "Einrichten des lokalen Netzwerkzugriffs für einen Konsolen-Agenten"

Vorbereiten des Netzwerks für Cloud Volumes ONTAP

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"

"Weitere Informationen finden Sie in der entsprechenden Dokumentation zu NetApp Datendiensten."

Registrieren oder bei der NetApp Console anmelden

Auf die NetApp Console kann über eine webbasierte Konsole zugegriffen werden. Um mit der Konsole zu beginnen, müssen Sie sich zunächst mit Ihren Anmeldeinformationen für die NetApp Support-Site registrieren oder anmelden oder ein Login für die NetApp Console erstellen.

Informationen zu diesem Vorgang

Wenn Sie zum ersten Mal auf die Konsole zugreifen, können Sie sich mit einer der folgenden Optionen registrieren oder anmelden:

NetApp Console -Anmeldung

Sie können sich anmelden, indem Sie ein Login erstellen. Bei dieser Authentifizierungsmethode müssen Sie Ihre E-Mail-Adresse und ein Passwort angeben. Nachdem Sie Ihre E-Mail-Adresse bestätigt haben, können Sie sich anmelden und dann eine Organisation erstellen, falls Sie noch keiner angehören.

Anmeldeinformationen für die NetApp Support Site (NSS)

Wenn Sie bereits über Anmeldeinformationen für die NetApp -Support-Site verfügen, müssen Sie sich nicht für die Konsole anmelden. Sie melden sich mit Ihren NSS-Anmeldeinformationen an und werden dann von der Konsole aufgefordert, eine Organisation zu erstellen, falls Sie noch keiner angehören.

Sie erhalten einen Einmalpasscode (OTP) an die registrierte E-Mail-Adresse. Bei jedem Anmeldeversuch wird ein neues OTP generiert.

Verbundverbindung

Wenn Ihr Unternehmen bereits über eine NetApp Console verfügt, hat Ihr Konsolenadministrator möglicherweise Single Sign-On eingerichtet, um sich mit Anmeldeinformationen aus Ihrem Unternehmensverzeichnis anzumelden (föderierte Identität).

"Erfahren Sie, wie Sie die Identitätsföderation mit der NetApp Console nutzen" .

Schritte

1. Öffnen Sie einen Webbrowser und gehen Sie zu "NetApp Console"
2. Wenn Sie über ein NetApp Support Site-Konto verfügen oder bereits eine Identitätsföderation eingerichtet haben, geben Sie die mit Ihrem Konto verknüpfte E-Mail-Adresse direkt auf der Seite **Anmelden** ein.

   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**.

      Beachten Sie, dass im Anmeldeformular nur englische Zeichen zulässig sind.

   b. Suchen Sie in Ihrem Posteingang nach einer E-Mail von NetApp mit Anweisungen zur Bestätigung Ihrer E-Mail-Adresse.

      Dieser Schritt ist erforderlich, bevor Sie sich bei der Konsole anmelden können.

4. Lesen Sie nach der Anmeldung die Endbenutzer-Lizenzvereinbarung und akzeptieren Sie die Bedingungen.

   Wenn Ihr Benutzerkonto noch nicht zu einer Konsolenorganisation gehört, werden Sie aufgefordert, eines

zu erstellen.

5. Geben Sie auf der **Willkommensseite** einen Namen für Ihre Konsolenorganisation ein.

   Die Konsole definiert eine Organisation als oberstes Element im Identitäts- und Zugriffsmanagement (IAM) der Konsole. "Erfahren Sie mehr über IAM" .

   Wenn Ihr Unternehmen bereits über eine Organisation verfügt und Sie dieser beitreten möchten, schließen Sie die Konsole und bitten Sie den Organisationsadministrator, Sie mit der Organisation zu verknüpfen. Nachdem Sie hinzugefügt wurden, können Sie sich anmelden und haben Zugriff auf die Konsolenorganisation. "Erfahren Sie, wie Sie einer bestehenden Organisation Mitglieder hinzufügen" .

6. Wählen Sie **Los geht's**.

Erstellen eines Konsolenagenten

AWS

Installationsoptionen für Konsolenagenten in AWS

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

Folgende Installationsoptionen stehen zur Verfügung:

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

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

- "Erstellen Sie einen Konsolenagenten aus dem AWS Marketplace"

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

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

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

Erstellen Sie einen Konsolenagenten in AWS über die NetApp Console

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

Bevor Sie beginnen

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

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

Stellen Sie sicher, dass der Netzwerkspeicherort, an dem Sie den Konsolenagenten installieren möchten, die

folgenden Anforderungen unterstützt. Diese Anforderungen ermöglichen es dem Konsolenagenten, Ressourcen und Prozesse in Ihrer Hybrid Cloud zu verwalten.

VPC und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)	Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab. "Weitere Einzelheiten finden Sie in der AWS-Dokumentation."
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.

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

Von der NetApp Konsole kontaktierte Endpunkte

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

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

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

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

Aktivieren von NTP

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

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

Schritt 2: AWS-Berechtigungen für den Konsolenagenten einrichten

Die Konsole muss sich bei AWS authentifizieren, bevor sie die Konsolen-Agent-Instanz in Ihrem VPC bereitstellen kann. Sie können eine dieser Authentifizierungsmethoden auswählen:

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

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

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

Dokumentation: Bedingungselement"

Schritte

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

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

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

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

5. Wählen Sie **Weiter** und fügen Sie bei Bedarf Tags hinzu.
6. Wählen Sie **Weiter** und geben Sie einen Namen und eine Beschreibung ein.
7. Wählen Sie **Richtlinie erstellen**.
8. Hängen Sie die Richtlinie entweder an eine IAM-Rolle an, die die Konsole übernehmen kann, oder an

einen IAM-Benutzer, damit Sie der Konsole Zugriffsschlüssel bereitstellen können:

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

Ergebnis

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

Schritt 3: Erstellen des Konsolenagenten

Erstellen Sie den Konsolenagenten direkt von der webbasierten Konsole aus.

Informationen zu diesem Vorgang

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Eine AWS-Authentifizierungsmethode: entweder eine IAM-Rolle oder Zugriffsschlüssel für einen IAM-Benutzer mit den erforderlichen Berechtigungen.
- Eine VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt.

- Ein Schlüsselpaar für die EC2-Instanz.
- Details zu einem Proxyserver, falls für den Internetzugriff vom Konsolenagenten ein Proxy erforderlich ist.
- Aufstellen"Netzwerkanforderungen" .
- Aufstellen"AWS-Berechtigungen" .

Schritte

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

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

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

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

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

   "Sicherheitsgruppenregeln für AWS anzeigen" .

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

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

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

10. Wählen Sie **Hinzufügen**.

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

Ergebnis

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

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

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

Erstellen Sie einen Konsolenagenten aus dem AWS Marketplace

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

Bevor Sie beginnen

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

Schritt 1: Einrichten des Netzwerks

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

VPC und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)	Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab. "Weitere Einzelheiten finden Sie in der AWS-Dokumentation."
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

- HTTP (80) und HTTPS (443) ermöglichen den Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) wird nur benötigt, wenn Sie zur Fehlerbehebung eine Verbindung zum Host herstellen müssen.

- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP -Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

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

Aktivieren von NTP

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

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

Schritt 2: AWS-Berechtigungen einrichten

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

Schritte

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

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

Ergebnis

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

Schritt 3: Überprüfen der Instanzanforderungen

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

CPU

8 Kerne oder 8 vCPUs

RAM

32 GB

AWS EC2-Instanztyp

Ein Instanztyp, der die oben genannten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen t3.2xlarge.

Schritt 4: Erstellen des Konsolenagenten

Erstellen Sie den Konsolenagenten direkt vom AWS Marketplace.

Informationen zu diesem Vorgang

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

Schritte

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

   Der Abonnementvorgang kann einige Minuten dauern.

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

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

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

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

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

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

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

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

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

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

Ergebnis

Der Konsolenagent ist jetzt installiert und mit Ihrer Konsolenorganisation eingerichtet.

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

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

Manuelle Installation des Konsolenagenten in AWS

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

Bevor Sie beginnen

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

Schritt 1: Hostanforderungen prüfen

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

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

Dedizierter Host

Der Konsolenagent wird auf einem Host, der mit anderen Anwendungen gemeinsam genutzt wird, nicht unterstützt. Der Host muss ein dedizierter Host sein. Der Host kann jede Architektur aufweisen, die die folgenden 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 in `/var` weil Docker oder Podman so konzipiert sind, dass sie die Container in diesem Verzeichnis erstellen. Konkret werden sie Container in der `/var/lib/containers/storage` Verzeichnis. Externe Mounts oder Symlinks funktionieren für diesen Bereich nicht.

Hypervisor

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

Betriebssystem- und Containeranforderungen

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

Betriebssystem	Unterstützte Betriebssystemversionen	Unterstützte Agent-Versionen	Erforderliches Container-Tool	SELinux a
Red Hat Enterprise Linux	9,1 bis 9,4 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 Podman-Konfigurationsanforderungen anzeigen .	Unterstützt im Durchsetzungsmodus oder im Permissivmodus • Die Verwaltung von Cloud Volumes ONTAP -Systemen wird NICHT von Agenten unterstützt, auf deren Betriebssystem SELinux aktiviert ist.
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

AWS EC2-Instanztyp

Ein Instanztyp, der die oben genannten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen t3.2xlarge.

Schlüsselpaar

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

PUT-Antwort-Hop-Limit bei Verwendung von IMDSv2

Wenn IMDSv2 auf der EC2-Instance aktiviert ist (dies ist die Standardeinstellung für neue EC2-Instances), müssen Sie das Hop-Limit für PUT-Antworten auf der Instanz auf 3 ändern. Wenn Sie das Limit der EC2-Instance nicht ändern, erhalten Sie beim Versuch, den Agenten einzurichten, einen UI-Initialisierungsfehler.

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

Speicherplatz in /opt

100 GiB Speicherplatz müssen verfügbar sein

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

Speicherplatz in /var

20 GiB Speicherplatz müssen verfügbar sein

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

Schritt 2: Installieren Sie Podman oder Docker Engine

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

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

  Sehen Sie sich die unterstützten Podman-Versionen an .

- Für Ubuntu ist Docker Engine erforderlich.

  Anzeigen der unterstützten Docker Engine-Versionen .

Beispiel 1. Schritte

Podman

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

- Aktivieren und starten Sie den Dienst podman.socket
- Installieren Sie Python3
- Installieren Sie das Podman-Compose-Paket Version 1.0.6
- Fügen Sie podman-compose zur Umgebungsvariablen PATH hinzu
- Wenn Sie Red Hat Enterprise Linux 8 verwenden, überprüfen Sie, ob Ihre Podman-Version 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.

   Für Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

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

   Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<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.
6. Bei Verwendung von Red Hat Enterprise:

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

   Für Red Hat Enterprise Linux 9:

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

   Für Red Hat Enterprise Linux 8:

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

7. 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.

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

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

```
podman info | grep networkBackend
```

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

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

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

d. 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` .

9. Starten Sie Podman neu.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker-Engine

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

Schritte

1. "Installationsanweisungen von Docker anzeigen"

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

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

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

Schritt 3: Einrichten des Netzwerks

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Von Computern kontaktierte Endpunkte bei Verwendung der webbasierten NetApp Console

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

"Vorbereiten des Netzwerks für die NetApp Konsole" .

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)	Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab. "Weitere Einzelheiten finden Sie in der AWS-Dokumentation."
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

- HTTP (80) und HTTPS (443) ermöglichen den Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) wird nur benötigt, wenn Sie zur Fehlerbehebung eine Verbindung zum Host herstellen müssen.

- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP -Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

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

Aktivieren von NTP

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

Schritt 4: AWS-Berechtigungen für die Konsole einrichten

Sie müssen der NetApp Console AWS-Berechtigungen erteilen, indem Sie eine der folgenden Optionen verwenden:

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

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

IAM-Rolle

Schritte

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

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

Ergebnis

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

AWS-Zugriffsschlüssel

Schritte

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

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

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

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

Ergebnis

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

Schritt 5: Installieren des Konsolenagenten

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

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

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

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

Informationen zu diesem Vorgang

Das auf der NetApp Support-Site verfügbare Installationsprogramm ist möglicherweise eine frühere Version. 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 von der "NetApp Support Site" , und kopieren Sie es dann auf den Linux-Host.

   Sie sollten das „Online“-Agent-Installationsprogramm herunterladen, das für die Verwendung in Ihrem Netzwerk oder in der Cloud vorgesehen ist.

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, wenn Ihr Netzwerk einen Proxy für den Internetzugang benötigt. Sie können entweder einen transparenten oder einen expliziten Proxy hinzufügen. Die Parameter --proxy und --cacert sind optional und Sie werden nicht aufgefordert, sie hinzuzufügen. Wenn Sie einen Proxyserver haben, müssen Sie die Parameter wie gezeigt eingeben.

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://Adresse:Port
- http://Benutzername:Passwort@Adresse:Port
- http://Domänenname%92Benutzername:Passwort@Adresse:Port
- https://Adresse:Port
- https://Benutzername:Passwort@Adresse:Port
- https://Domänenname%92Benutzername:Passwort@Adresse: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 Konsolenagent unterstützt keine Benutzernamen oder Passwörter, die das @-Zeichen enthalten.
  - Wenn das Kennwort eines der folgenden Sonderzeichen enthält, müssen Sie dieses Sonderzeichen durch Voranstellen eines Backslashs maskieren: & oder !

    Beispiel:

http://bxpproxyuser:netapp1\!@Adresse:3128

`--cacert`Gibt ein von einer Zertifizierungsstelle signiertes Zertifikat an, das für den HTTPS-Zugriff zwischen dem Konsolenagenten und dem Proxyserver verwendet werden soll. Dieser Parameter ist für HTTPS-Proxyserver, abfangende Proxyserver und transparente Proxyserver erforderlich.

+ Hier ist ein Beispiel für die Konfiguration eines transparenten Proxyservers. Wenn Sie einen transparenten Proxy konfigurieren, müssen Sie den Proxyserver nicht definieren. Sie fügen Ihrem Konsolen-Agent-Host lediglich ein von einer Zertifizierungsstelle signiertes Zertifikat hinzu:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
      ...
      # 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
      ...
      Esc:wq
      ```

   c. Starten Sie die virtuelle Maschine des Konsolenagenten neu.
2. Warten Sie, bis die Installation abgeschlossen ist.

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

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

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

   https://ipaddress

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

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

    d. Wählen Sie **Los geht's**.

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

Schritt 6: Berechtigungen für die NetApp Console erteilen

Nachdem Sie den Konsolenagenten installiert haben, müssen Sie der Konsole die AWS-Berechtigungen erteilen, die Sie zuvor eingerichtet haben. Durch die Bereitstellung der Berechtigungen kann der Konsolenagent Ihre Daten und Speicherinfrastruktur in AWS verwalten.

IAM-Rolle

Fügen Sie die zuvor erstellte IAM-Rolle der EC2-Instance des Konsolenagenten hinzu.

Schritte

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

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

AWS-Zugriffsschlüssel

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

Schritte

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

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

Azurblau

Installationsoptionen für den Konsolen-Agenten in Azure

Es gibt verschiedene Möglichkeiten, einen Konsolen-Agent in Azure zu erstellen. Der gängigste Weg ist die direkte Nutzung der NetApp Console .

Folgende Installationsoptionen stehen zur Verfügung:

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

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

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

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

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

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

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

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

Bevor Sie beginnen

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

Schritt 1: Einrichten des Netzwerks

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

Azure-Region

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

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

VNet und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

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

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

Von der NetApp Konsole kontaktierte Endpunkte

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

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

verwendet.

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

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

Aktivieren von NTP

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

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

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

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

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

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

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

Schritte

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

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

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

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
        "Microsoft.Network/virtualNetworks/virtualMachines/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/networkSecurityGroups/securityRules/read",
        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "Microsoft.Network/publicIPAddresses/join/action",

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

```
        "Microsoft.Resources/deployments/cancel/action",
        "Microsoft.Resources/deployments/validate/action",
        "Microsoft.Resources/resources/read",
        "Microsoft.Resources/subscriptions/operationresults/read",
        "Microsoft.Resources/subscriptions/resourceGroups/delete",
        "Microsoft.Resources/subscriptions/resourceGroups/read",

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

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/read",

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

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

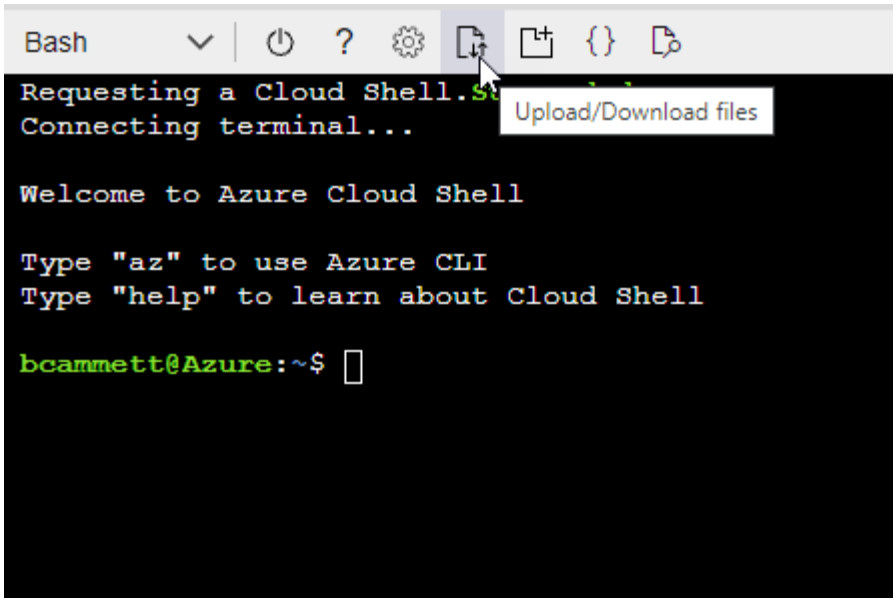
   Beispiel

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

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

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

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



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

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

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

Schritt 3: Authentifizierung einrichten

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

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

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

Azure-Konto

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

Schritte

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

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

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

Dienstprinzipal

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

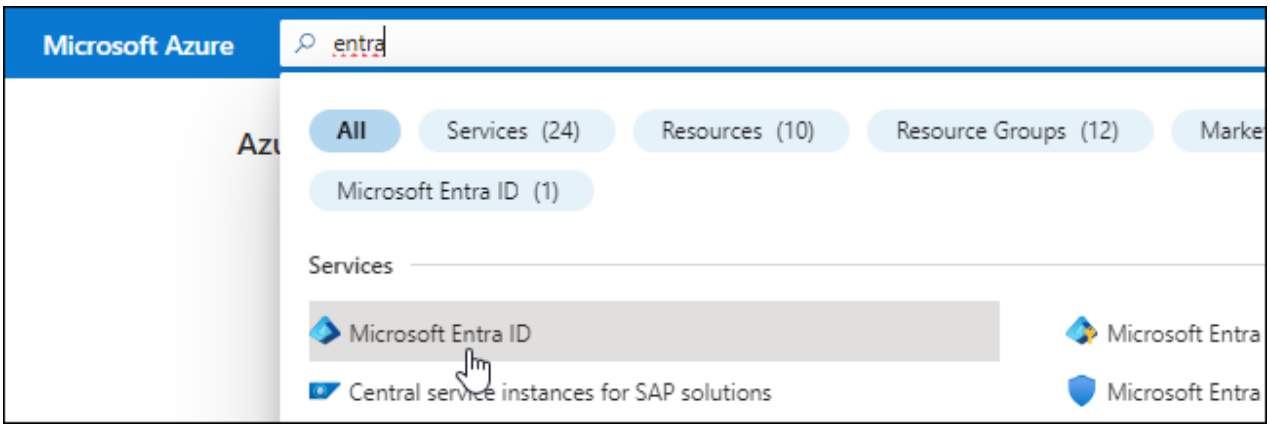
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die die Konsole benötigt.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffskontrolle

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

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

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



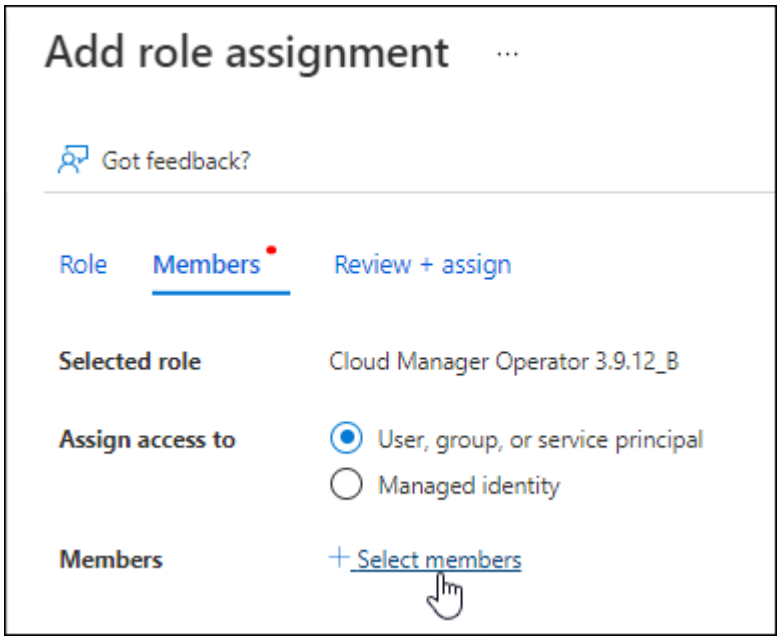
3. Wählen Sie im Menü **App-Registrierungen** aus.
4. Wählen Sie **Neuregistrierung**.
5. Geben Sie Details zur Anwendung an:
   - **Name**: Geben Sie einen Namen für die Anwendung ein.
   - **Kontotyp**: Wählen Sie einen Kontotyp aus (alle funktionieren mit der NetApp Console).
   - **Umleitungs-URI**: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

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der benutzerdefinierten Rolle zur Anwendung

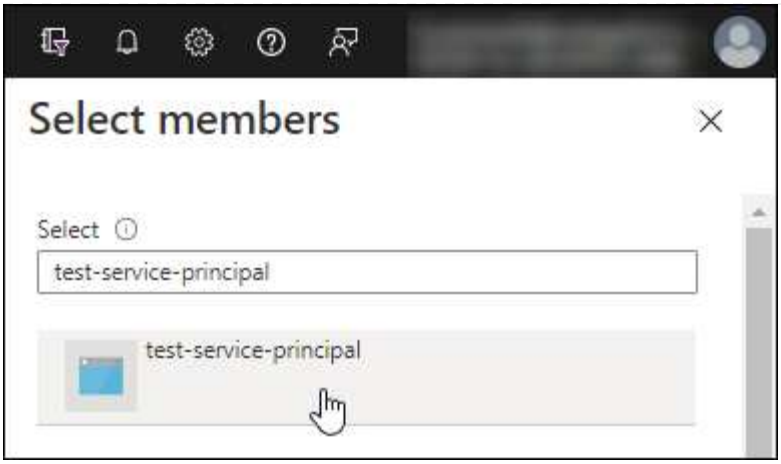
1. Öffnen Sie im Azure-Portal den Dienst **Abonnements**.
2. Wählen Sie das Abonnement aus.
3. Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
4. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenoperator** aus und klicken Sie auf **Weiter**.
5. Führen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

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



   c. Suchen Sie nach dem Namen der Anwendung.

      Hier ist ein Beispiel:



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

b. Klicken Sie auf **Weiter**.

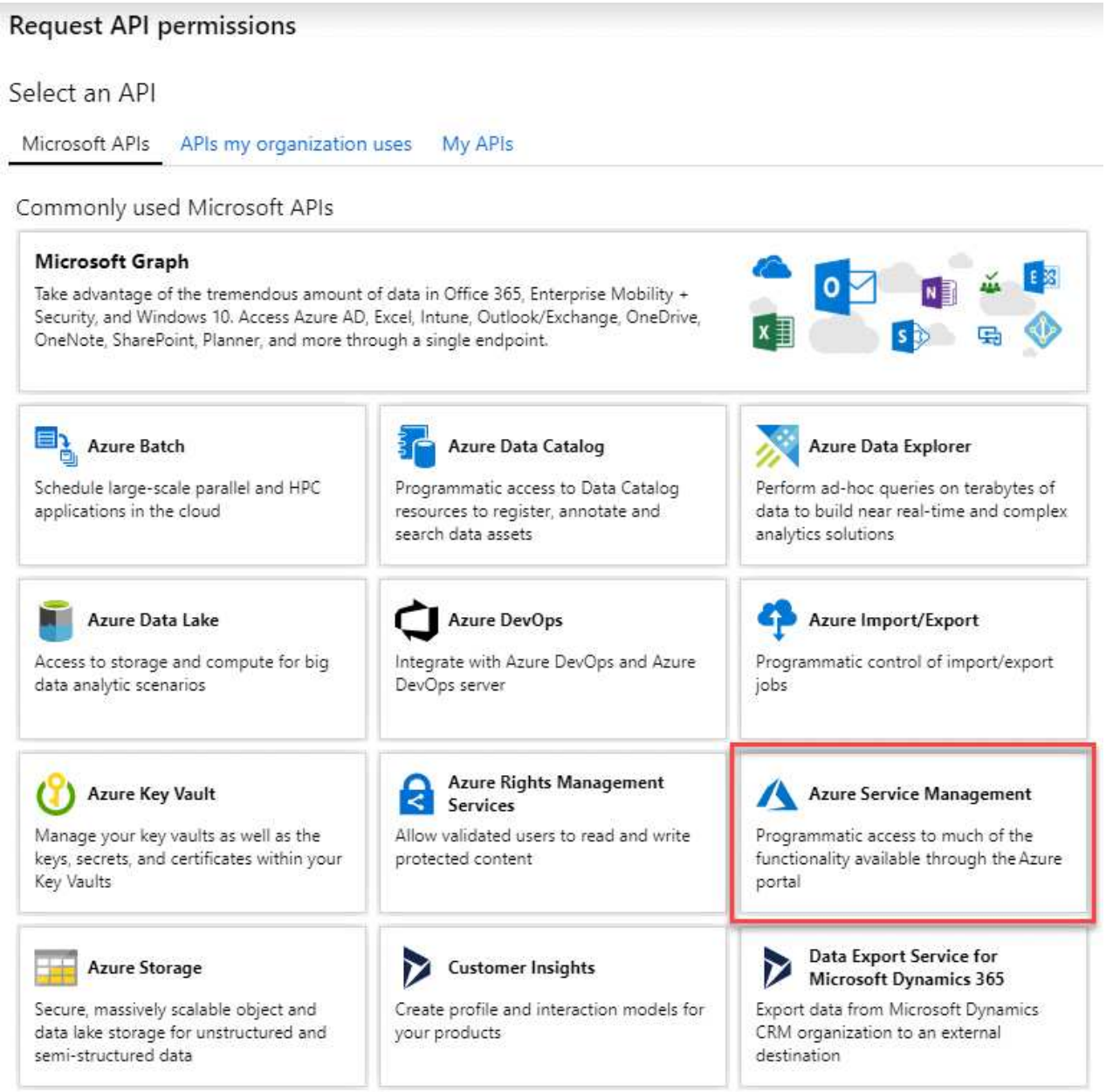
6. Klicken Sie auf **Überprüfen + zuweisen**.

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

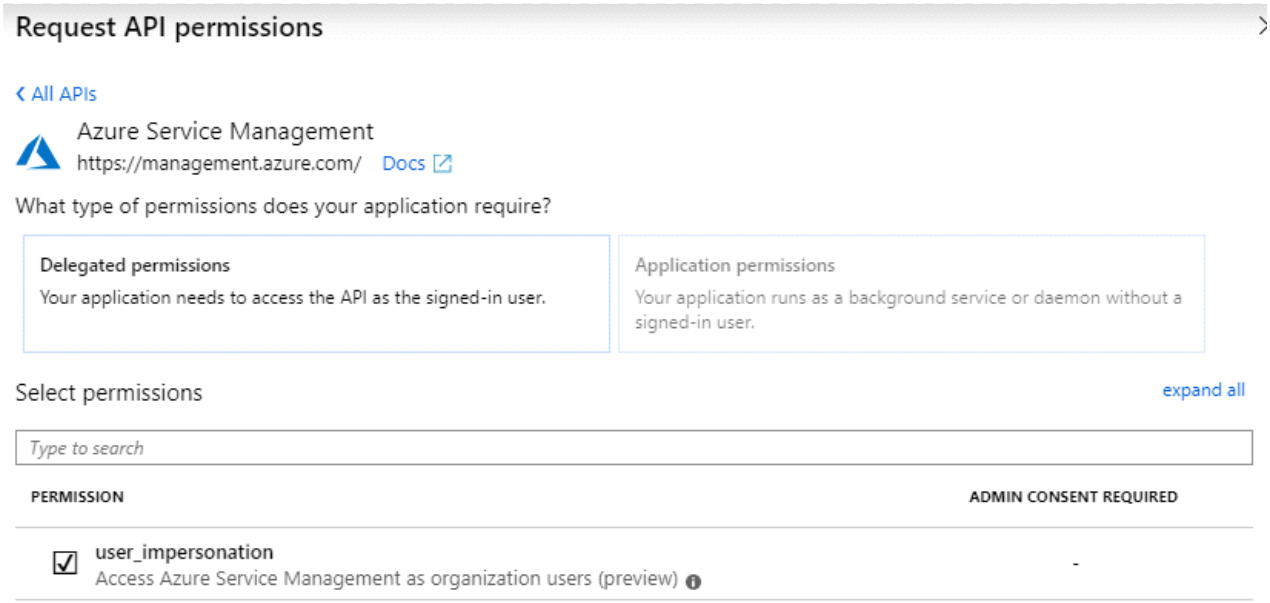
   Wenn Sie Ressourcen in mehreren Azure-Abonnements verwalten möchten, müssen Sie den Dienstprinzipal an jedes dieser Abonnements binden. Beispielsweise können Sie in der Konsole das Abonnement auswählen, das Sie bei der Bereitstellung von Cloud Volumes ONTAP verwenden möchten.

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

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

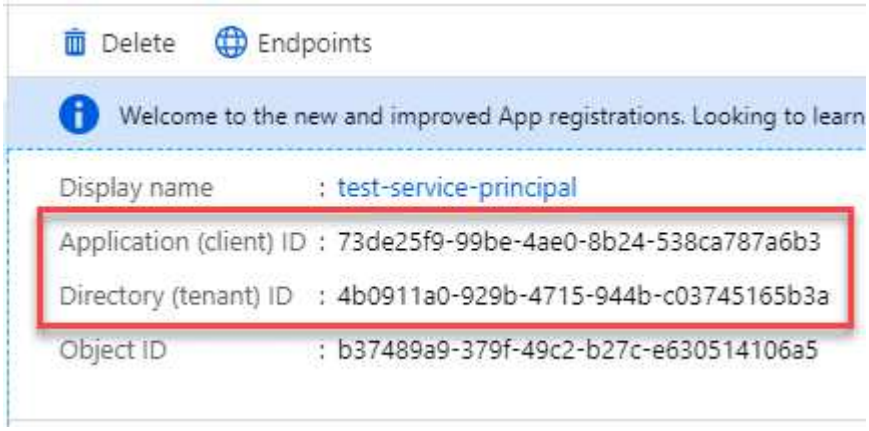


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

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



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

Erstellen eines Client-Geheimnisses

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

Ergebnis

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

Schritt 4: Erstellen des Konsolenagenten

Erstellen Sie den Konsolenagenten direkt von der NetApp Console aus.

Informationen zu diesem Vorgang

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

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

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

  Diese Berechtigungen gelten für die Konsolen-Agentinstanz selbst. Es handelt sich um einen anderen Satz

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

Schritte

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

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

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

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

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

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

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

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

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

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

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

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

"Anzeigen von Sicherheitsgruppenregeln für Azure" .

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

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

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

9. Wählen Sie **Hinzufügen**.

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

Ergebnis

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

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

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

Erstellen eines Konsolen-Agents aus dem Azure Marketplace

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

Bevor Sie beginnen

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

Schritt 1: Einrichten des Netzwerks

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

Azure-Region

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

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

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

VNet und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

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

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

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

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

Aktivieren von NTP

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

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

Schritt 2: Überprüfen der VM-Anforderungen

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

CPU

8 Kerne oder 8 vCPUs

RAM

32 GB

Azure-VM-Größe

Ein Instanztyp, der die oben genannten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen Standard_D8s_v3.

Schritt 3: Berechtigungen einrichten

Sie können Berechtigungen auf folgende Weise erteilen:

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

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

Benutzerdefinierte Rolle

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

Schritte

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

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

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

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

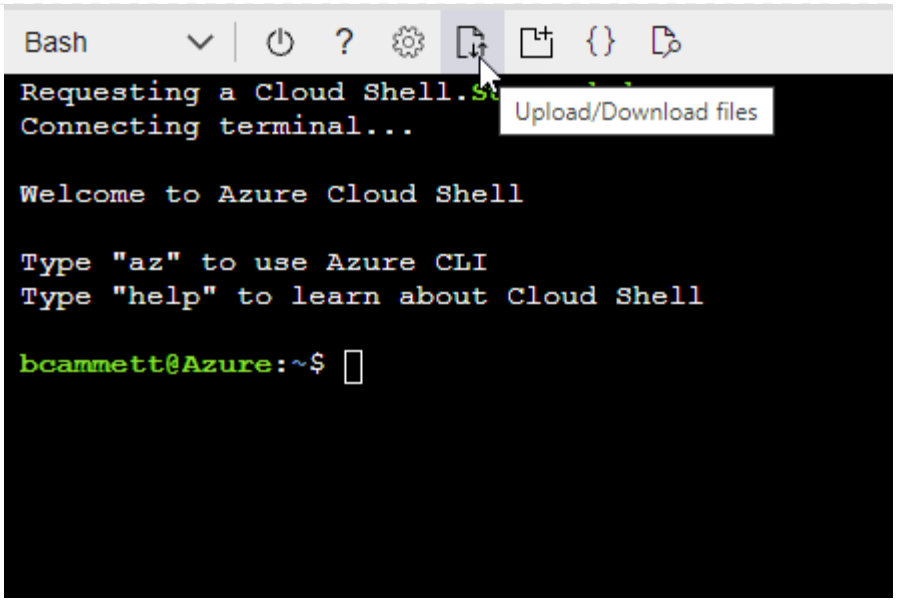
   Beispiel

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

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

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

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



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

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

Dienstprinzipal

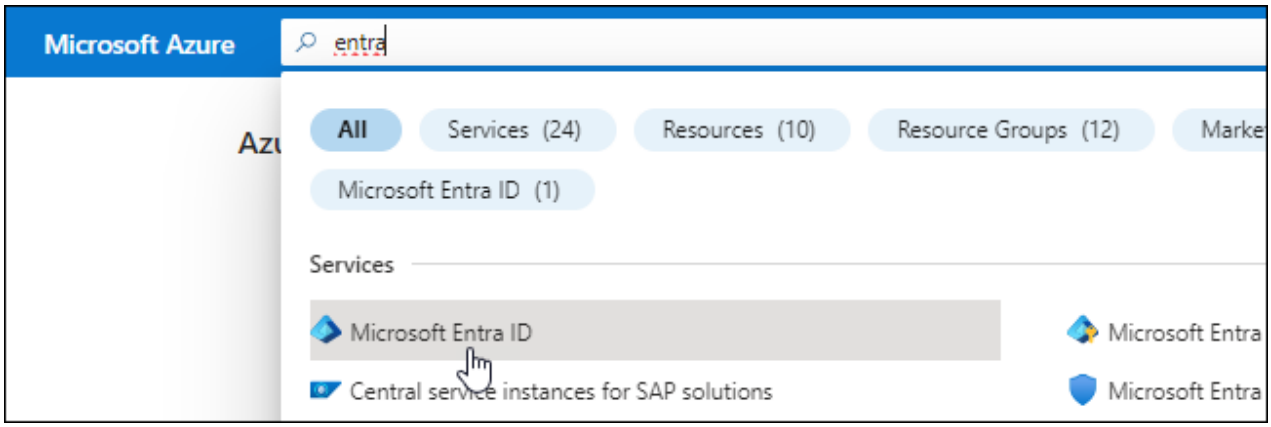
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die die Konsole benötigt.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffskontrolle

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

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

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



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

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

6. Wählen Sie **Registrieren**.

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der Anwendung zu einer Rolle

1. Erstellen Sie eine benutzerdefinierte Rolle:

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

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

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

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

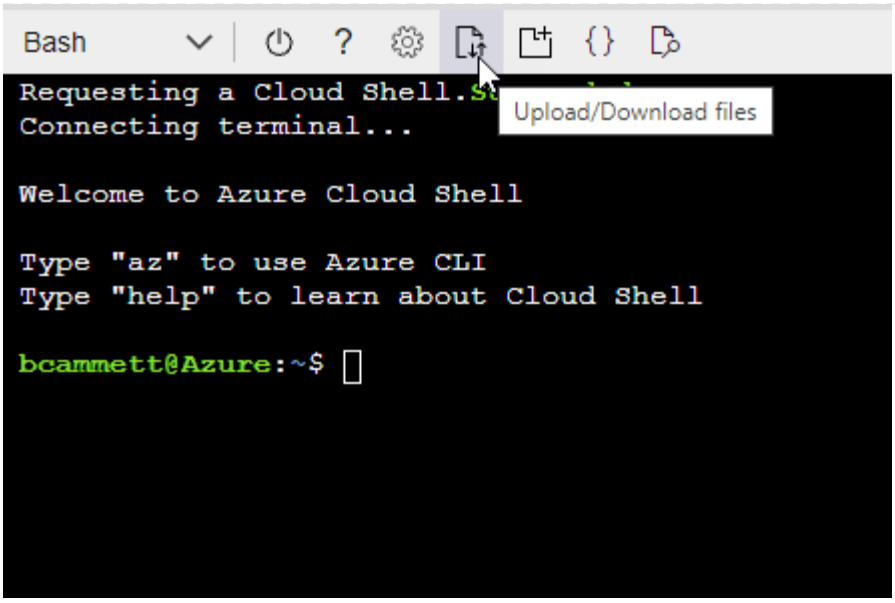
      Beispiel

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

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

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

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



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

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

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

2. Weisen Sie die Anwendung der Rolle zu:

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

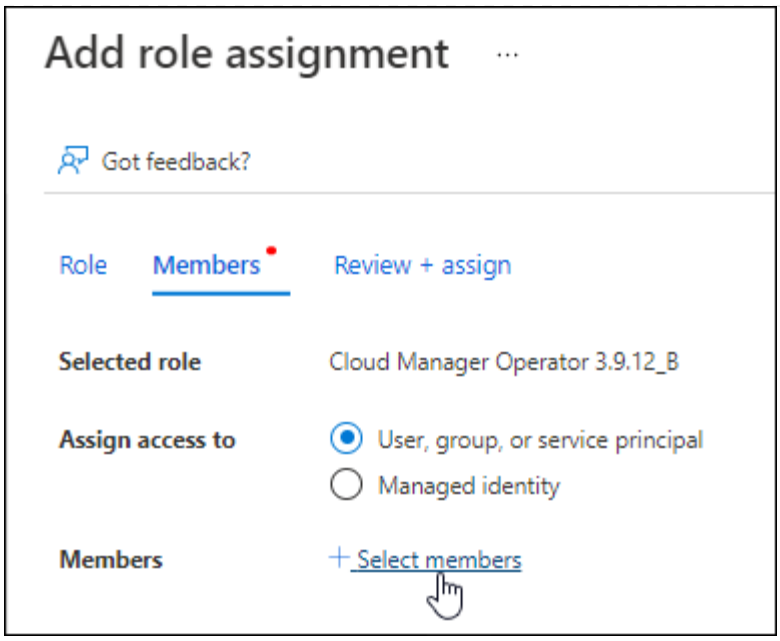
   b. Wählen Sie das Abonnement aus.

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

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

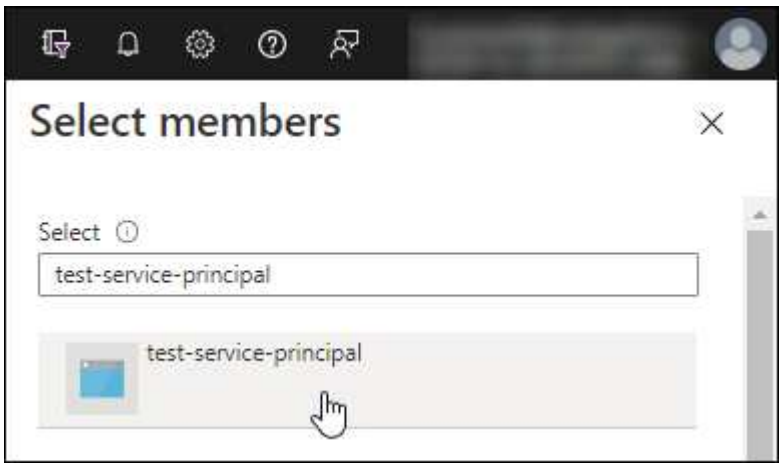
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

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



- Suchen Sie nach dem Namen der Anwendung.

  Hier ist ein Beispiel:



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

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

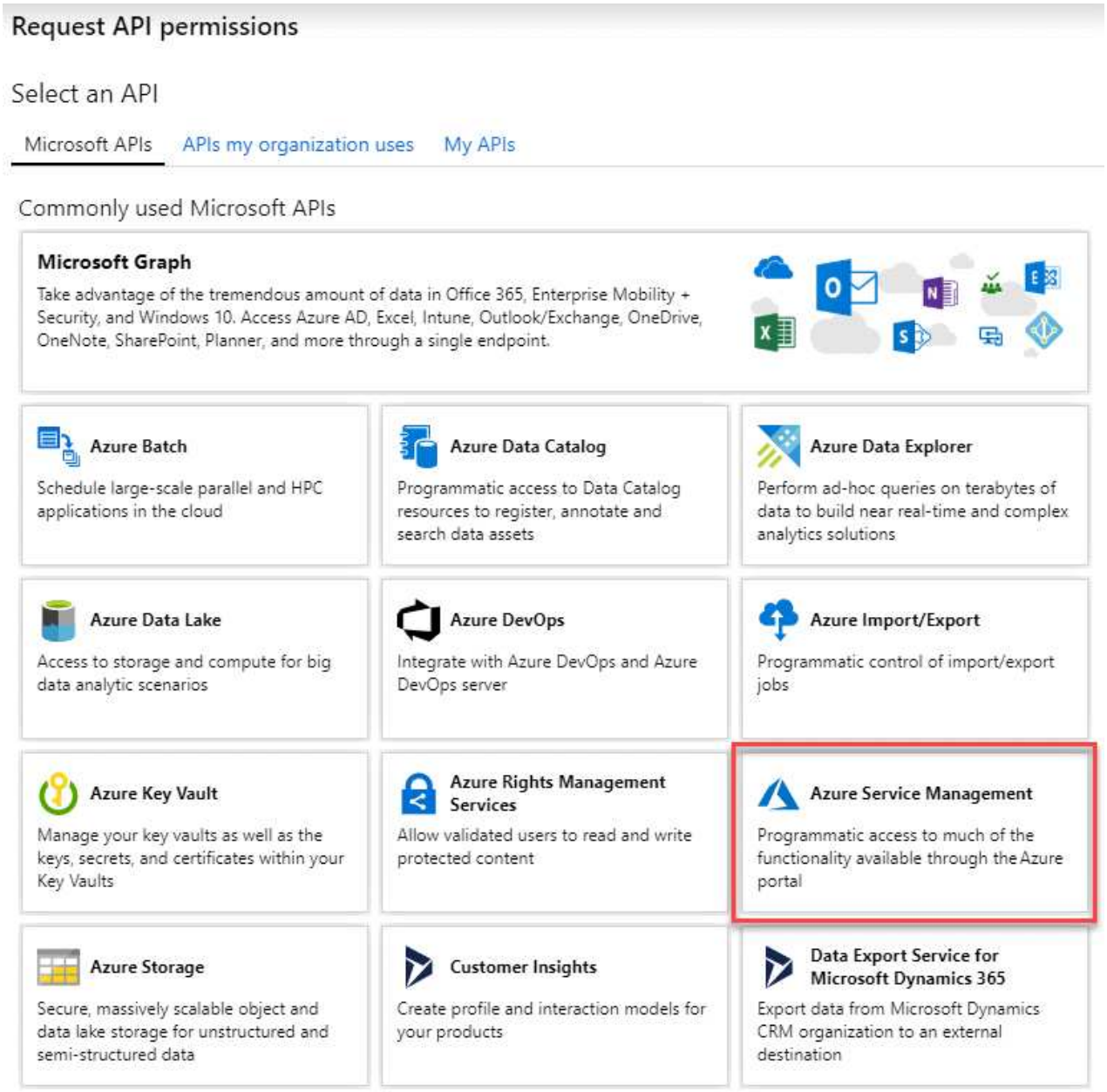
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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

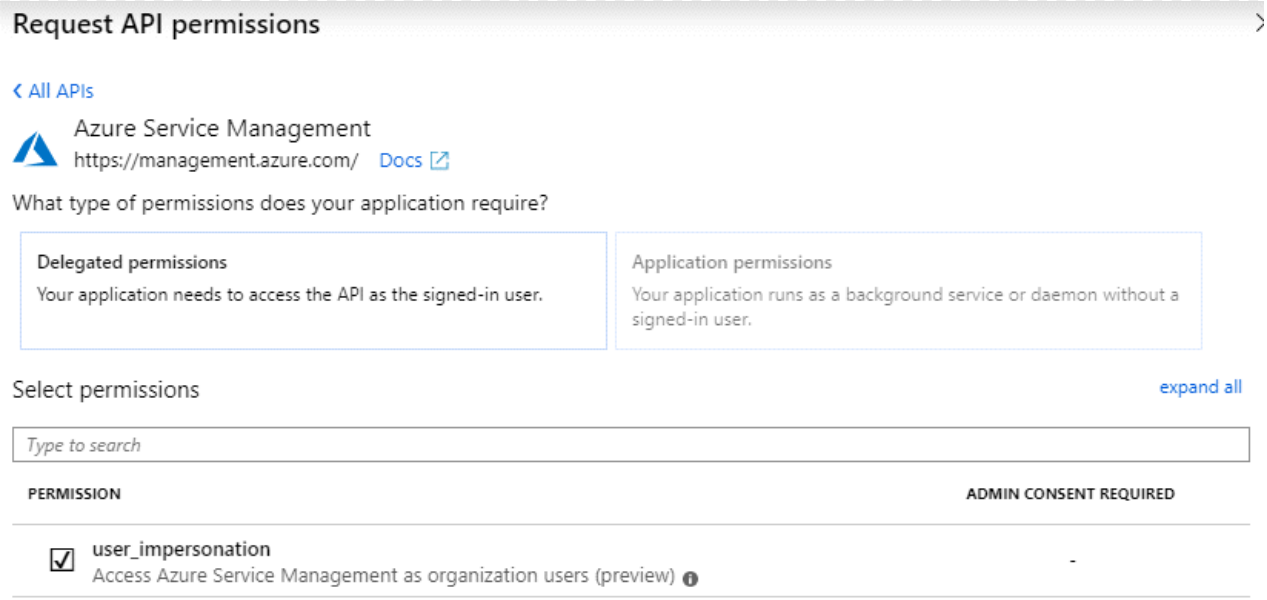
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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

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

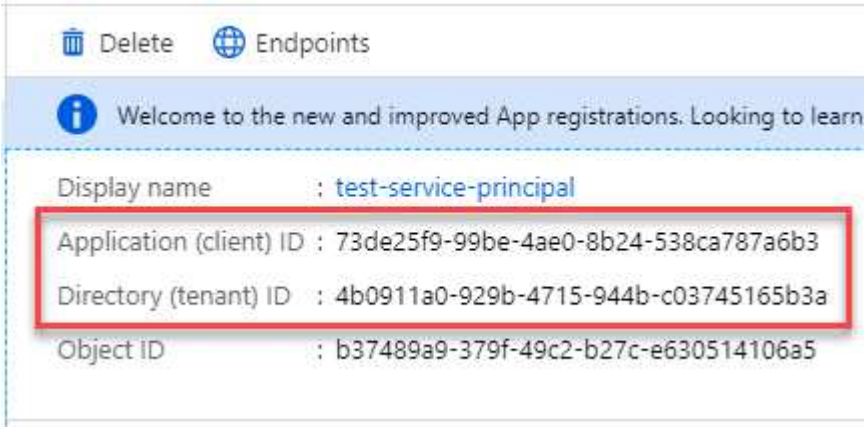


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

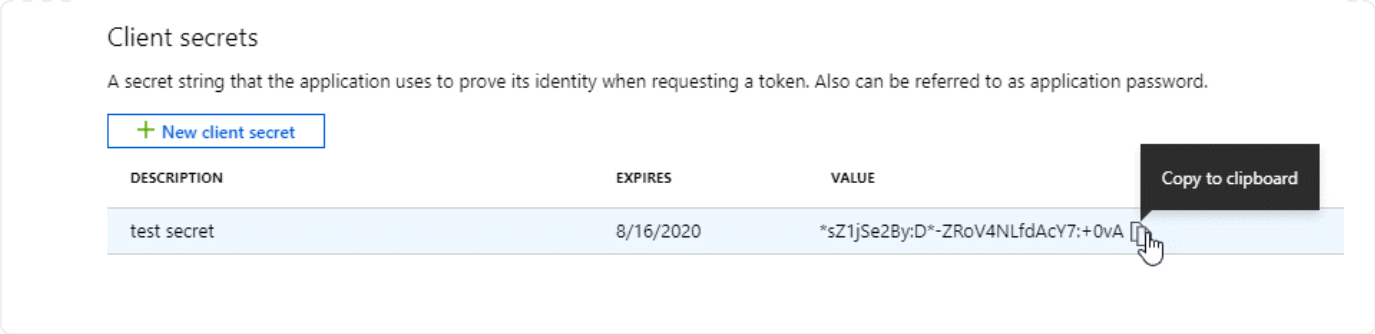
1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



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

Erstellen eines Client-Geheimnisses

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



Schritt 4: Erstellen des Konsolenagenten

Starten Sie den Konsolen-Agent direkt vom Azure Marketplace.

Informationen zu diesem Vorgang

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

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

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

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

Schritte

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

   "Azure Marketplace-Seite für kommerzielle Regionen"

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

Beachten Sie beim Konfigurieren der VM Folgendes:

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

  "Anzeigen von Sicherheitsgruppenregeln für Azure" .

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

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

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

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

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

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

   https://ipaddress

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

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

   d. Wählen Sie **Los geht's**.

Ergebnis

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

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

Schritt 5: Erteilen Sie dem Konsolenagenten Berechtigungen

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

Benutzerdefinierte Rolle

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

Schritte

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

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

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

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

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

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

Wie geht es weiter?

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

Dienstprinzipal

Schritte

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

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

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

Ergebnis

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

Manuelles Installieren des Konsolen-Agents in Azure

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

Bevor Sie beginnen

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

Schritt 1: Hostanforderungen prüfen

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

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

Dedizierter Host

Der Konsolenagent wird auf einem Host, der mit anderen Anwendungen gemeinsam genutzt wird, nicht unterstützt. Der Host muss ein dedizierter Host sein. Der Host kann jede Architektur aufweisen, die die folgenden 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 in `/var` weil Docker oder Podman so konzipiert

sind, dass sie die Container in diesem Verzeichnis erstellen. Konkret werden sie Container in der `/var/lib/containers/storage` Verzeichnis. Externe Mounts oder Symlinks funktionieren für diesen Bereich nicht.

Hypervisor

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

Betriebssystem- und Containeranforderungen

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

Betriebssystem	Unterstützte Betriebssystemversionen	Unterstützte Agent-Versionen	Erforderliches Container-Tool	SELinux a
Red Hat Enterprise Linux	9,1 bis 9,4 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 Podman-Konfigurationsanforderungen anzeigen .	Unterstützt im Durchsetzungsmodus oder im Permissivmodus • Die Verwaltung von Cloud Volumes ONTAP -Systemen wird NICHT von Agenten unterstützt, auf deren Betriebssystem SELinux aktiviert ist.
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

Azure-VM-Größe

Ein Instanztyp, der die oben genannten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen Standard_D8s_v3.

Speicherplatz in /opt

100 GiB Speicherplatz müssen verfügbar sein

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

Speicherplatz in /var

20 GiB Speicherplatz müssen verfügbar sein

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

Schritt 2: Installieren Sie Podman oder Docker Engine

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

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

  Sehen Sie sich die unterstützten Podman-Versionen an .

- Für Ubuntu ist Docker Engine erforderlich.

  Anzeigen der unterstützten Docker Engine-Versionen .

Beispiel 2. Schritte

Podman

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

- Aktivieren und starten Sie den Dienst podman.socket
- Installieren Sie Python3
- Installieren Sie das Podman-Compose-Paket Version 1.0.6
- Fügen Sie podman-compose zur Umgebungsvariablen PATH hinzu
- Wenn Sie Red Hat Enterprise Linux 8 verwenden, überprüfen Sie, ob Ihre Podman-Version 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.

   Für Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

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

   Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<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.
6. Bei Verwendung von Red Hat Enterprise:

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

   Für Red Hat Enterprise Linux 9:

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

   Für Red Hat Enterprise Linux 8:

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

7. 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.

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

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

```
podman info | grep networkBackend
```

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

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

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

d. 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` .

9. Starten Sie Podman neu.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker-Engine

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

Schritte

1. "Installationsanweisungen von Docker anzeigen"

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

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

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

Schritt 3: Einrichten des Netzwerks

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

Azure-Region

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

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Von Computern kontaktierte Endpunkte bei Verwendung der webbasierten NetApp Console

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

"Vorbereiten des Netzwerks für die NetApp Konsole" .

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

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

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

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

seltenen Fällen verwenden werden.

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

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

Aktivieren von NTP

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

Schritt 4: Einrichten der Bereitstellungsberechtigungen für den Konsolen-Agenten

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

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

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

Erstellen einer benutzerdefinierten Rolle für die Bereitstellung des Konsolenagenten

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

Schritte

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

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

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

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

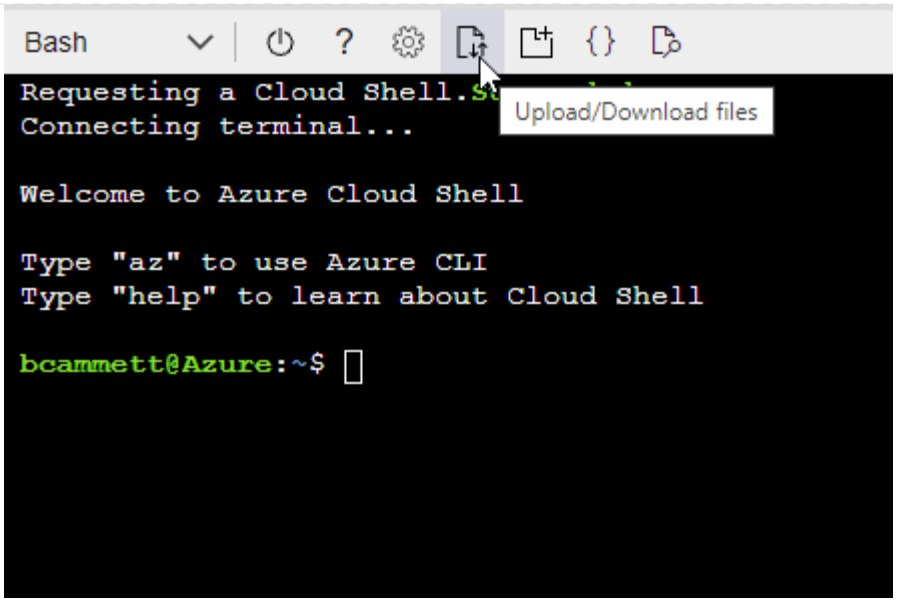
   Beispiel

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

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

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

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



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

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

Dienstprinzipal

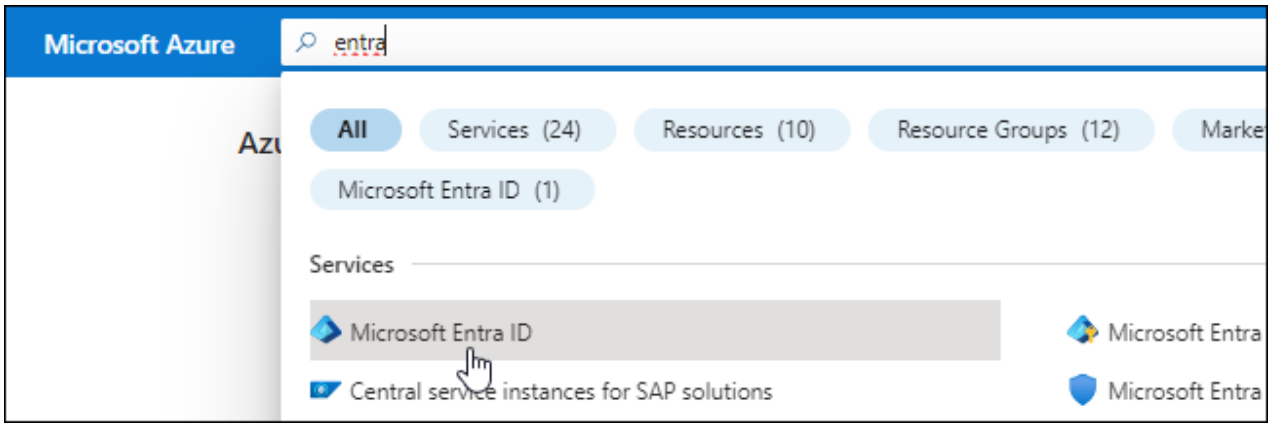
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die der Konsolenagent benötigt.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffskontrolle

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

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

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



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

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

6. Wählen Sie **Registrieren**.

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der Anwendung zu einer Rolle

1. Erstellen Sie eine benutzerdefinierte Rolle:

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

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

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

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

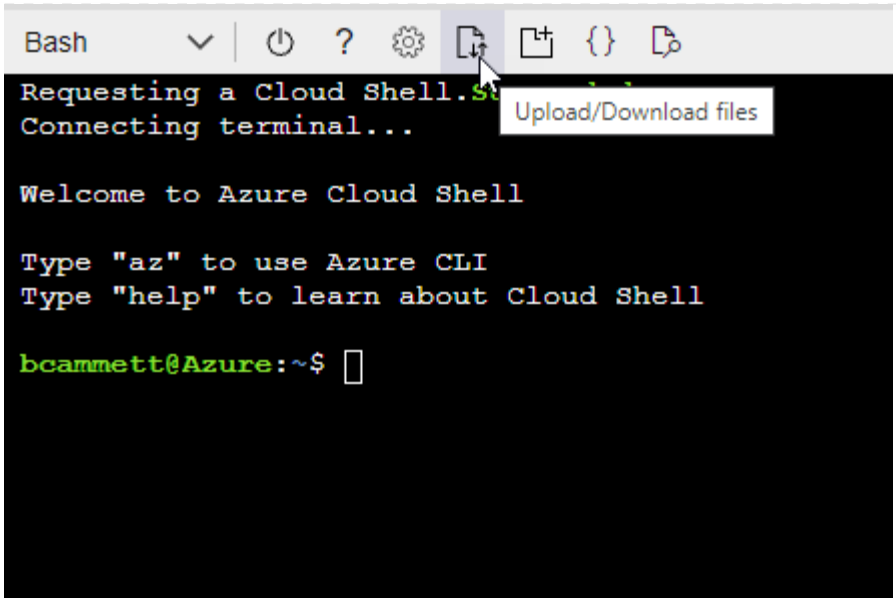
      Beispiel

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

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

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

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



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

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

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

2. Weisen Sie die Anwendung der Rolle zu:

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

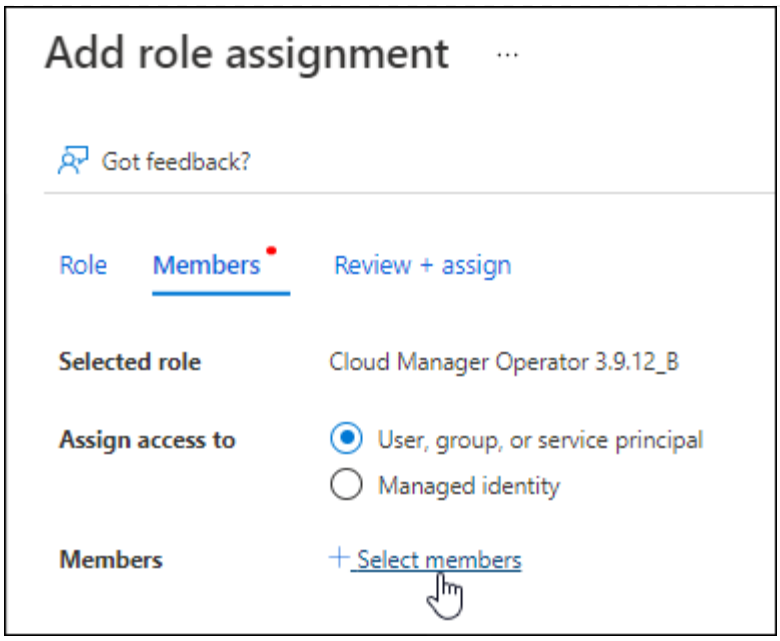
   b. Wählen Sie das Abonnement aus.

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

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

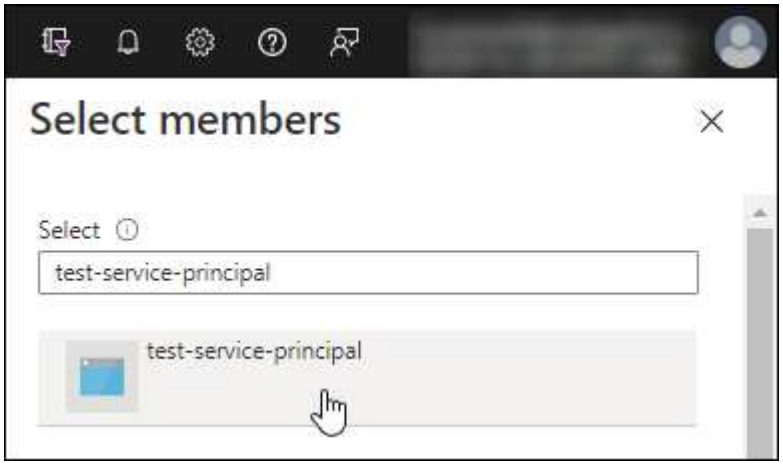
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

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



- Suchen Sie nach dem Namen der Anwendung.

  Hier ist ein Beispiel:



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

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

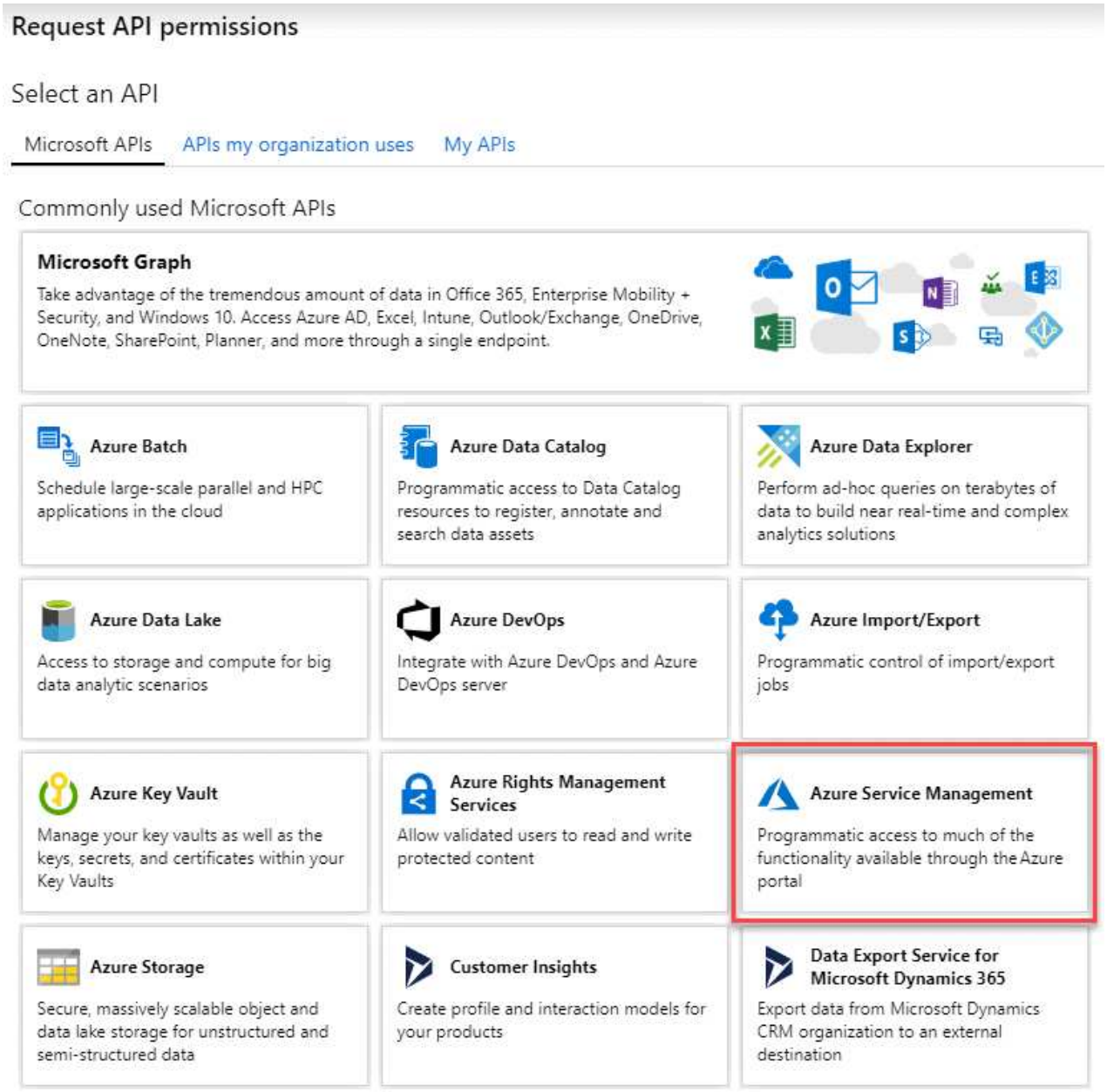
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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

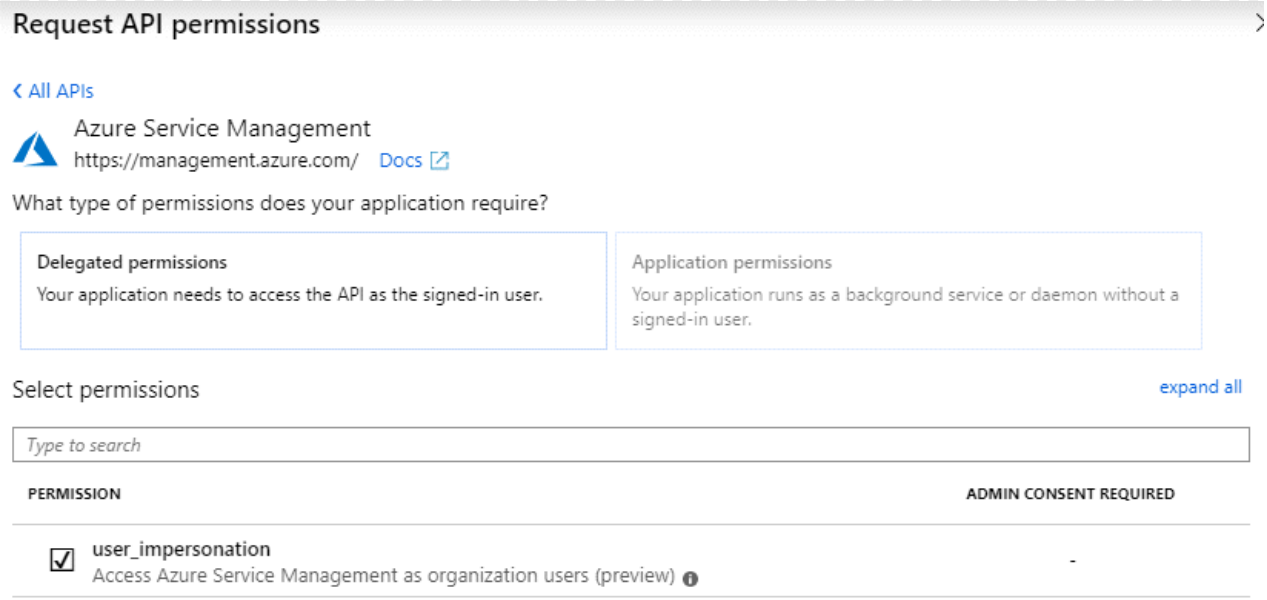
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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

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

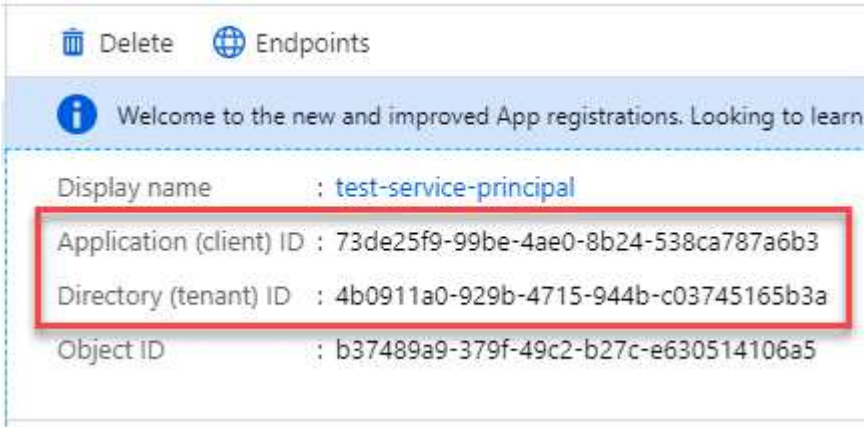


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

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



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

Erstellen eines Client-Geheimnisses

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

Ergebnis

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

Schritt 5: Installieren des Konsolenagenten

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

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

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

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

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

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

Informationen zu diesem Vorgang

Das auf der NetApp Support-Site verfügbare Installationsprogramm ist möglicherweise eine frühere Version. 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 von der "NetApp Support Site" , und kopieren Sie es dann auf den Linux-Host.

   Sie sollten das „Online“-Agent-Installationsprogramm herunterladen, das für die Verwendung in Ihrem Netzwerk oder in der Cloud vorgesehen ist.

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, wenn Ihr Netzwerk einen Proxy für den Internetzugang benötigt. Sie können entweder einen transparenten oder einen expliziten Proxy hinzufügen. Die Parameter --proxy und --cacert sind optional und Sie werden nicht aufgefordert, sie hinzuzufügen. Wenn Sie einen Proxyserver haben, müssen Sie die Parameter wie gezeigt eingeben.

   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://Adresse:Port
   - http://Benutzername:Passwort@Adresse:Port
   - http://Domänenname%92Benutzername:Passwort@Adresse:Port
   - https://Adresse:Port

- https://Benutzername:Passwort@Adresse:Port
- https://Domänenname%92Benutzername:Passwort@Adresse: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 Konsolenagent unterstützt keine Benutzernamen oder Passwörter, die das @-Zeichen enthalten.
  - Wenn das Kennwort eines der folgenden Sonderzeichen enthält, müssen Sie dieses Sonderzeichen durch Voranstellen eines Backslashs maskieren: & oder !

    Beispiel:

http://bxpproxyuser:netapp1\!@Adresse:3128

`--cacert`Gibt ein von einer Zertifizierungsstelle signiertes Zertifikat an, das für den HTTPS-Zugriff zwischen dem Konsolenagenten und dem Proxyserver verwendet werden soll. Dieser Parameter ist für HTTPS-Proxyserver, abfangende Proxyserver und transparente Proxyserver erforderlich.

+ Hier ist ein Beispiel für die Konfiguration eines transparenten Proxyservers. Wenn Sie einen transparenten Proxy konfigurieren, müssen Sie den Proxyserver nicht definieren. Sie fügen Ihrem Konsolen-Agent-Host lediglich ein von einer Zertifizierungsstelle signiertes Zertifikat hinzu:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
      ...
      # 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
      ...
      Esc:wq
      ```

c. Starten Sie die virtuelle Maschine des Konsolenagenten neu.

2. Warten Sie, bis die Installation abgeschlossen ist.

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

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

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

   https://ipaddress

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

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

   d. Wählen Sie **Los geht's**.

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

Schritt 6: Berechtigungen für die NetApp Console erteilen

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

Benutzerdefinierte Rolle

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

Schritte

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

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

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

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

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

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

Wie geht es weiter?

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

Dienstprinzipal

Schritte

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

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

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

Ergebnis

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

Google Cloud

Installationsoptionen für den Konsolenagenten in Google Cloud

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

Folgende Installationsoptionen stehen zur Verfügung:

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

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

- "Erstellen Sie den Konsolenagenten mithilfe der Google Platform"

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

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

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

Erstellen Sie einen Konsolenagenten in Google Cloud über die NetApp Console

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

Bevor Sie beginnen

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

Schritt 1: Einrichten des Netzwerks

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

VPC und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Zum Verwalten von Ressourcen in Google Cloud.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.

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

Von der NetApp Konsole kontaktierte Endpunkte

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

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

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

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

Aktivieren von NTP

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

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

Schritt 2: Richten Sie Berechtigungen zum Erstellen des Konsolenagenten ein

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

Schritte

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

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

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

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

```
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. Aktivieren Sie Cloud Shell in Google Cloud.

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

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

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

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

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

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

"Google Cloud-Dokumente: Gewähren einer einzelnen Rolle"

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

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

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

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in Google Cloud:

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

b. Aktivieren Sie Cloud Shell in Google Cloud.

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

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

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

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

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

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

      "Google Cloud-Dokumente: Erstellen eines Dienstkontos"

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

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

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

   Weitere Einzelheiten finden Sie unter "Google Cloud-Dokumentation"

Schritt 4: Einrichten freigegebener VPC-Berechtigungen

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

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

Berechtigungen für freigegebene VPCs anzeigen

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

Hinweise:

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

Schritt 5: Google Cloud APIs aktivieren

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

Schritt

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

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

"Google Cloud-Dokumentation: APIs aktivieren"

Schritt 6: Erstellen des Konsolenagenten

Erstellen Sie einen Konsolenagenten direkt aus der Konsole.

Informationen zu diesem Vorgang

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

Schritte

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

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

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

     "Firewall-Regeln in Google Cloud"
5. Überprüfen Sie Ihre Auswahl, um sicherzustellen, dass Ihre Einrichtung korrekt ist.
   a. Das Kontrollkästchen **Agentenkonfiguration validieren** ist standardmäßig aktiviert, damit die Konsole bei der Bereitstellung die Anforderungen an die Netzwerkkonnektivität validiert. Wenn die Bereitstellung des Agenten durch die Konsole fehlschlägt, wird ein Bericht bereitgestellt, der Sie bei der Fehlerbehebung unterstützt. Wenn die Bereitstellung erfolgreich ist, wird kein Bericht bereitgestellt.

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

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

Ergebnis

Nach Abschluss des Vorgangs steht der Konsolenagent zur Verwendung bereit.

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

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

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

Bevor Sie beginnen

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

Schritt 1: Einrichten des Netzwerks

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

VPC und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Zum Verwalten von Ressourcen in Google Cloud.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.

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

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

Von der NetApp Konsole kontaktierte Endpunkte

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

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

verwendet.

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

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

Aktivieren von NTP

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

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

Schritt 2: Richten Sie Berechtigungen zum Erstellen des Konsolenagenten ein

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

Schritte

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

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

```
title: Console agent deployment policy
description: Permissions for the user who deploys the NetApp Console
agent
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
```

```
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. Aktivieren Sie Cloud Shell in Google Cloud.

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

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

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

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

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

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

"Google Cloud-Dokumente: Gewähren einer einzelnen Rolle"

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

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

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

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in Google Cloud:

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

b. Aktivieren Sie Cloud Shell in Google Cloud.

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

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

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

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

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

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

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

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

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

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

"Google Cloud-Dokumente: Erstellen eines Dienstkontos"

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

diese Projekte gewähren.

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

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

Weitere Einzelheiten finden Sie unter "Google Cloud-Dokumentation"

Schritt 4: Einrichten freigegebener VPC-Berechtigungen

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

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

Berechtigungen für freigegebene VPCs anzeigen

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

Hinweise:

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

Schritt 5: Google Cloud APIs aktivieren

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

Schritt

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

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

"Google Cloud-Dokumentation: APIs aktivieren"

Schritt 6: Erstellen des Konsolenagenten

Erstellen Sie mithilfe von Google Cloud einen Konsolenagenten.

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

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

Schritte

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

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

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

Dokumentationsseite" .

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

```
gcloud auth list
```

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

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

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

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

Instanzname
: Der gewünschte Instanzname für die VM-Instanz.

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

Dienstkonto
: Das in der Ausgabe von Schritt 2 angegebene Dienstkonto.

Zone

Die Zone, in der Sie die VM bereitstellen möchten

keine Adresse

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

Netzwerk-Tag

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

Netzwerkpfad

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

Subnetzpfad

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

kms-Schlüsselpfad

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

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

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

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

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

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

      "Erfahren Sie mehr über Identitäts- und Zugriffsverwaltung" .

   b. Geben Sie einen Namen für das System ein.

Ergebnis

Der Konsolenagent ist jetzt installiert und mit Ihrer Konsolenorganisation eingerichtet.

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

Installieren Sie den Konsolenagenten manuell in Google Cloud

Um den Konsolen-Agenten manuell auf Ihrem eigenen Linux-Host zu installieren, müssen Sie die Hostanforderungen überprüfen, Ihr Netzwerk einrichten, Google Cloud-

Berechtigungen vorbereiten, Google Cloud-APIs aktivieren, die Konsole installieren und dann die vorbereiteten Berechtigungen bereitstellen.

Bevor Sie beginnen

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

Schritt 1: Hostanforderungen prüfen

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

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

Dedizierter Host

Der Konsolenagent wird auf einem Host, der mit anderen Anwendungen gemeinsam genutzt wird, nicht unterstützt. Der Host muss ein dedizierter Host sein. Der Host kann jede Architektur aufweisen, die die folgenden 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 in `/var` weil Docker oder Podman so konzipiert sind, dass sie die Container in diesem Verzeichnis erstellen. Konkret werden sie Container in der `/var/lib/containers/storage` Verzeichnis. Externe Mounts oder Symlinks funktionieren für diesen Bereich nicht.

Hypervisor

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

Betriebssystem- und Containeranforderungen

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

Betriebssystem	Unterstützte Betriebssystemversionen	Unterstützte Agent-Versionen	Erforderliches Container-Tool	SELinux a
Red Hat Enterprise Linux	9,1 bis 9,4 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 Podman-Konfigurationsanforderungen anzeigen .	Unterstützt im Durchsetzungsmodus oder im Permissivmodus • Die Verwaltung von Cloud Volumes ONTAP -Systemen wird NICHT von Agenten unterstützt, auf deren Betriebssystem SELinux aktiviert ist.
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

Google Cloud-Maschinentyp

Ein Instanztyp, der die oben genannten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen n2-standard-8.

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

Speicherplatz in /opt

100 GiB Speicherplatz müssen verfügbar sein

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

Speicherplatz in /var

20 GiB Speicherplatz müssen verfügbar sein

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

Schritt 2: Installieren Sie Podman oder Docker Engine

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

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

  Sehen Sie sich die unterstützten Podman-Versionen an .

- Für Ubuntu ist Docker Engine erforderlich.

  Anzeigen der unterstützten Docker Engine-Versionen .

Beispiel 3. Schritte

Podman

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

- Aktivieren und starten Sie den Dienst podman.socket
- Installieren Sie Python3
- Installieren Sie das Podman-Compose-Paket Version 1.0.6
- Fügen Sie podman-compose zur Umgebungsvariablen PATH hinzu
- Wenn Sie Red Hat Enterprise Linux 8 verwenden, überprüfen Sie, ob Ihre Podman-Version 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.

   Für Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

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

   Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<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.
6. Bei Verwendung von Red Hat Enterprise:

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

   Für Red Hat Enterprise Linux 9:

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

   Für Red Hat Enterprise Linux 8:

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

7. 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.

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

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

```
podman info | grep networkBackend
```

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

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

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

d. 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` .

9. Starten Sie Podman neu.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker-Engine

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

Schritte

1. "Installationsanweisungen von Docker anzeigen"

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

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

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

Schritt 3: Einrichten des Netzwerks

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Von Computern kontaktierte Endpunkte bei Verwendung der webbasierten NetApp Console

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

"Vorbereiten des Netzwerks für die NetApp Konsole" .

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Zum Verwalten von Ressourcen in Google Cloud.
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

- HTTP (80) und HTTPS (443) ermöglichen den Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) wird nur benötigt, wenn Sie zur Fehlerbehebung eine Verbindung zum Host herstellen müssen.

- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP -Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

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

Aktivieren von NTP

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

Schritt 4: Berechtigungen für den Konsolen-Agent einrichten

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

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

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle in Google Cloud:

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

   b. Aktivieren Sie Cloud Shell in Google Cloud.

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

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

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

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

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

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

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

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

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

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

      "Google Cloud-Dokumente: Erstellen eines Dienstkontos"

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

diese Projekte gewähren.

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

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

Weitere Einzelheiten finden Sie unter "Google Cloud-Dokumentation"

Schritt 5: Einrichten freigegebener VPC-Berechtigungen

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

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

Berechtigungen für freigegebene VPCs anzeigen

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

Hinweise:

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

Schritt 6: Google Cloud APIs aktivieren

Bevor Sie Cloud Volumes ONTAP -Systeme in Google Cloud bereitstellen können, müssen mehrere Google Cloud-APIs aktiviert werden.

Schritt

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

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

"Google Cloud-Dokumentation: APIs aktivieren"

Schritt 7: Installieren des Konsolenagenten

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

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

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

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

Informationen zu diesem Vorgang

Das auf der NetApp Support-Site verfügbare Installationsprogramm ist möglicherweise eine frühere Version. 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 von der "NetApp Support Site" , und kopieren Sie es dann auf den Linux-Host.

   Sie sollten das „Online“-Agent-Installationsprogramm herunterladen, das für die Verwendung in Ihrem Netzwerk oder in der Cloud vorgesehen ist.

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, wenn Ihr Netzwerk einen Proxy für den Internetzugang benötigt. Sie können entweder einen transparenten oder einen expliziten Proxy hinzufügen. Die Parameter --proxy und --cacert sind optional und Sie werden nicht aufgefordert, sie hinzuzufügen. Wenn Sie einen Proxyserver haben, müssen Sie die Parameter wie gezeigt eingeben.

   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://Adresse:Port
   - http://Benutzername:Passwort@Adresse:Port
   - http://Domänenname%92Benutzername:Passwort@Adresse:Port
   - https://Adresse:Port

- https://Benutzername:Passwort@Adresse:Port
- https://Domänenname%92Benutzername:Passwort@Adresse: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 Konsolenagent unterstützt keine Benutzernamen oder Passwörter, die das @-Zeichen enthalten.
  - Wenn das Kennwort eines der folgenden Sonderzeichen enthält, müssen Sie dieses Sonderzeichen durch Voranstellen eines Backslashs maskieren: & oder !

    Beispiel:

http://bxpproxyuser:netapp1\!@Adresse:3128

`--cacert`Gibt ein von einer Zertifizierungsstelle signiertes Zertifikat an, das für den HTTPS-Zugriff zwischen dem Konsolenagenten und dem Proxyserver verwendet werden soll. Dieser Parameter ist für HTTPS-Proxyserver, abfangende Proxyserver und transparente Proxyserver erforderlich.

+ Hier ist ein Beispiel für die Konfiguration eines transparenten Proxyservers. Wenn Sie einen transparenten Proxy konfigurieren, müssen Sie den Proxyserver nicht definieren. Sie fügen Ihrem Konsolen-Agent-Host lediglich ein von einer Zertifizierungsstelle signiertes Zertifikat hinzu:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
      ...
      # 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
      ...
      Esc:wq
      ```

c. Starten Sie die virtuelle Maschine des Konsolenagenten neu.

2. Warten Sie, bis die Installation abgeschlossen ist.

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

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

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

   https://ipaddress

2. Richten Sie nach der Anmeldung den Konsolenagenten ein:

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

   b. Geben Sie einen Namen für das System ein.

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

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

   d. Wählen Sie **Los geht's**.

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

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

Schritt 8: Erteilen Sie dem Konsolenagenten Berechtigungen

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

Schritte

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

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

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

Installieren eines Agenten vor Ort

Manuelle Installation eines Konsolen-Agenten vor Ort

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

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

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

Vorbereiten der Installation des Konsolenagenten

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

Überprüfen der Hostanforderungen für den Konsolenagenten

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

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

Dedizierter Host

Der Konsolenagent wird auf einem Host, der mit anderen Anwendungen gemeinsam genutzt wird, nicht unterstützt. Der Host muss ein dedizierter Host sein. Der Host kann jede Architektur aufweisen, die die folgenden 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 in `/var` weil Docker oder Podman so konzipiert sind, dass sie die Container in diesem Verzeichnis erstellen. Konkret werden sie Container in der `/var/lib/containers/storage` Verzeichnis. Externe Mounts oder Symlinks funktionieren für diesen Bereich nicht.

Hypervisor

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

Betriebssystem- und Containeranforderungen

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

Betriebssystem	Unterstützte Betriebssystemversionen	Unterstützte Agent-Versionen	Erforderliches Container-Tool	SELinux a
Red Hat Enterprise Linux	9,1 bis 9,4 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 Podman-Konfigurationsanforderungen anzeigen .	Unterstützt im Durchsetzungsmodus oder im Permissivmodus • Die Verwaltung von Cloud Volumes ONTAP -Systemen wird NICHT von Agenten unterstützt, auf deren Betriebssystem SELinux aktiviert ist.
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

Einrichten des Netzwerkzugriffs für den Konsolenagenten

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Von Computern kontaktierte Endpunkte bei Verwendung der webbasierten NetApp Console

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

"Vorbereiten des Netzwerks für die NetApp Konsole" .

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

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

AWS

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)	Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab. "Weitere Einzelheiten finden Sie in der AWS-Dokumentation."
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.

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

Azurblau

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

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Zum Verwalten von Ressourcen in öffentlichen Azure-Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Zum Verwalten von Ressourcen in Azure China-Regionen.

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

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

- HTTP (80) und HTTPS (443) ermöglichen den Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) wird nur benötigt, wenn Sie zur Fehlerbehebung eine Verbindung zum Host herstellen müssen.

- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP -Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

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

Aktivieren von NTP

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

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

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

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

AWS

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

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

Schritte

1. Melden Sie sich bei der AWS-Konsole an und navigieren Sie zum IAM-Dienst.
2. Erstellen Sie eine Richtlinie:

   a. Wählen Sie **Richtlinien > Richtlinie erstellen**.

   b. Wählen Sie **JSON** und kopieren und fügen Sie den Inhalt des"IAM-Richtlinie für den Konsolenagenten" .

   c. Führen Sie die restlichen Schritte aus, um die Richtlinie zu erstellen.

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

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

3. Hängen Sie die Richtlinien an einen IAM-Benutzer an.
   - "AWS-Dokumentation: Erstellen von IAM-Rollen"
   - "AWS-Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"
4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie der NetApp Console hinzufügen können, nachdem Sie den Konsolen-Agenten installiert haben.

Ergebnis

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

Azurblau

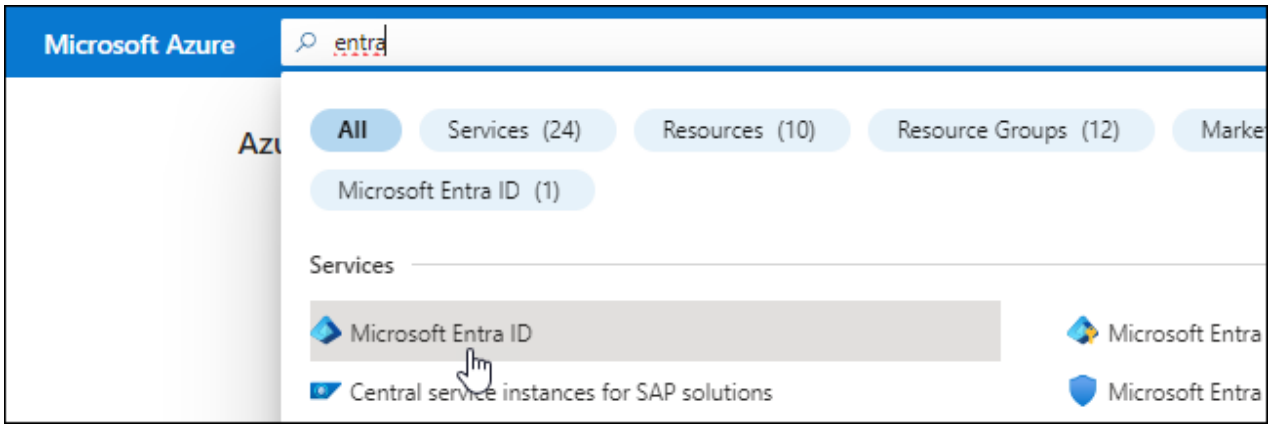
Wenn der Konsolen-Agent vor Ort installiert ist, müssen Sie dem Konsolen-Agenten Azure-Berechtigungen erteilen, indem Sie einen Dienstprinzipal in der Microsoft Entra ID einrichten und die Azure-Anmeldeinformationen abrufen, die der Konsolen-Agent benötigt.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffskontrolle

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

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

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



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

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der Anwendung zu einer Rolle

1. Erstellen Sie eine benutzerdefinierte Rolle:

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

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

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

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

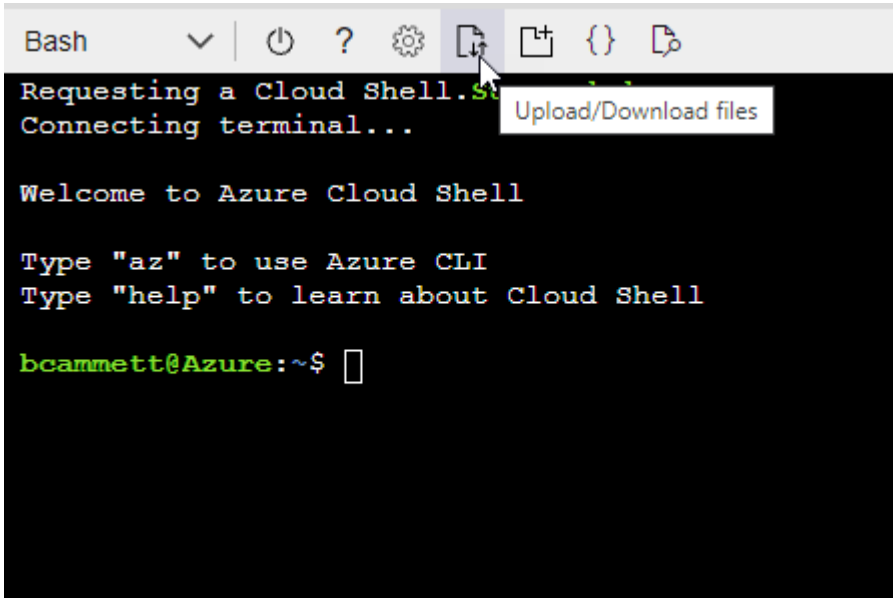
      Beispiel

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

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

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

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



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

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

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

2. Weisen Sie die Anwendung der Rolle zu:

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

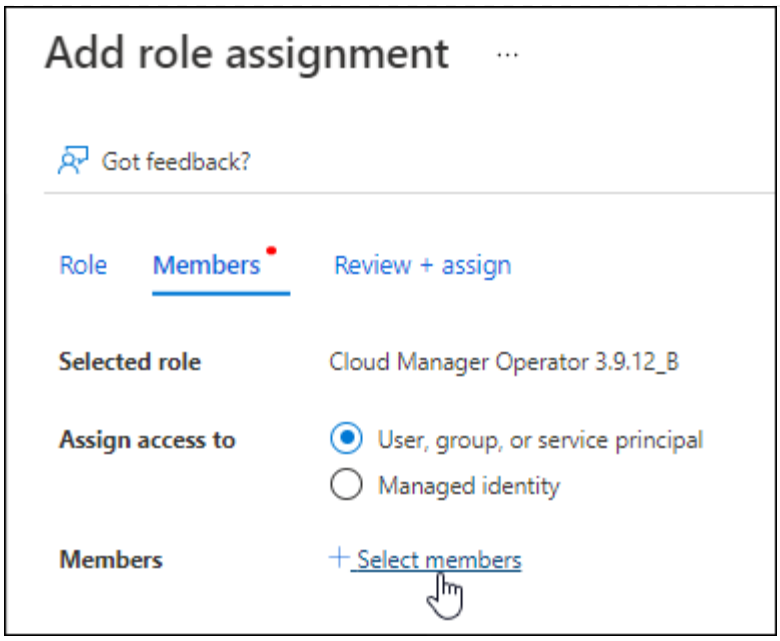
   b. Wählen Sie das Abonnement aus.

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

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

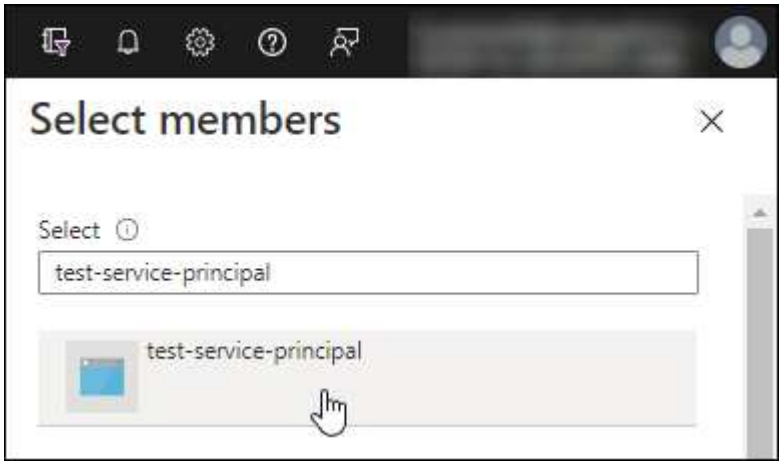
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

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



- Suchen Sie nach dem Namen der Anwendung.

  Hier ist ein Beispiel:



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

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

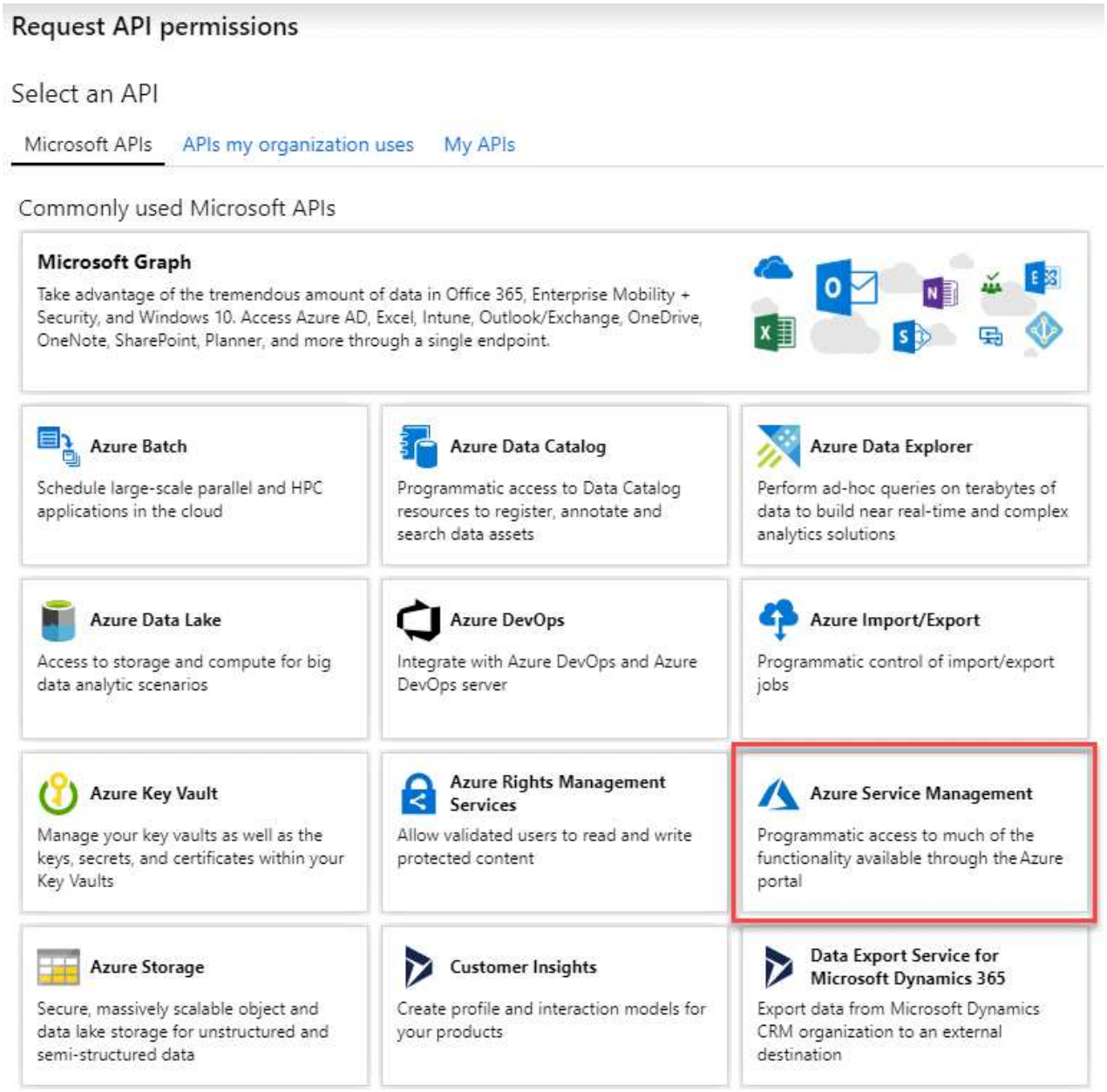
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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

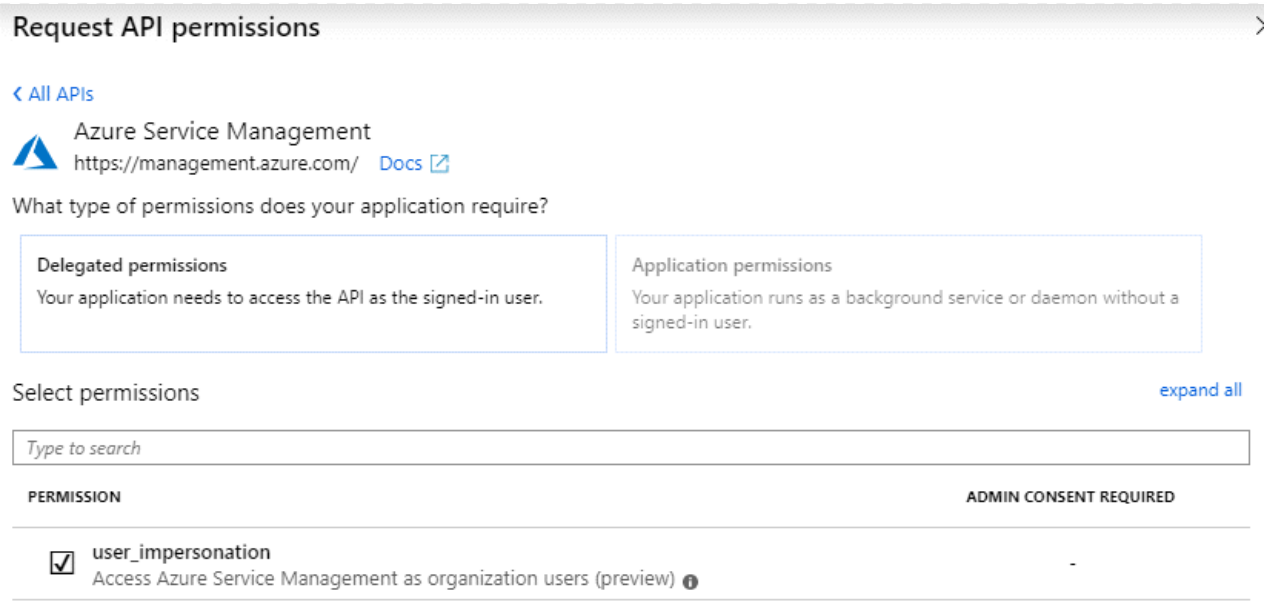
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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

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

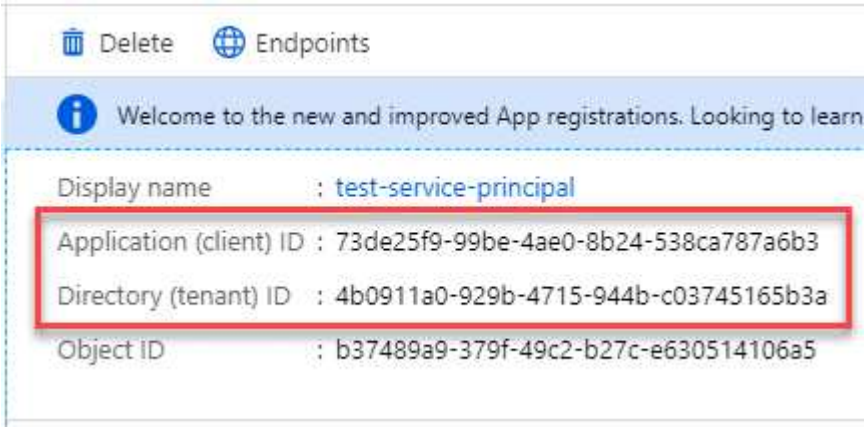


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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

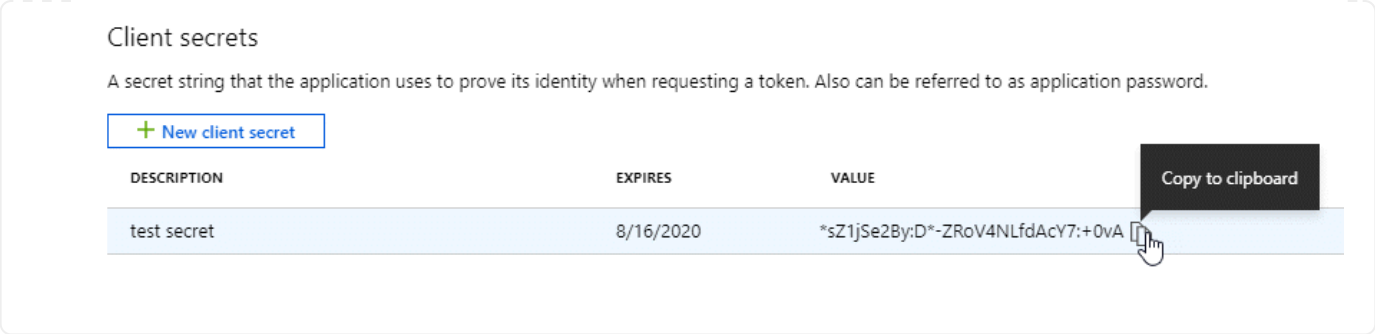
1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



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

Erstellen eines Client-Geheimnisses

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



Manuelles Installieren eines Konsolenagenten

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

Installieren Sie Podman oder Docker Engine

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

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

  Sehen Sie sich die unterstützten Podman-Versionen an .

- Für Ubuntu ist Docker Engine erforderlich.

  Anzeigen der unterstützten Docker Engine-Versionen .

Beispiel 4. Schritte

Podman

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

- Aktivieren und starten Sie den Dienst podman.socket
- Installieren Sie Python3
- Installieren Sie das Podman-Compose-Paket Version 1.0.6
- Fügen Sie podman-compose zur Umgebungsvariablen PATH hinzu
- Wenn Sie Red Hat Enterprise Linux 8 verwenden, überprüfen Sie, ob Ihre Podman-Version 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.

   Für Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

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

   Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<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.
6. Bei Verwendung von Red Hat Enterprise:

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

   Für Red Hat Enterprise Linux 9:

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

   Für Red Hat Enterprise Linux 8:

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

7. 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.

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

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

```
podman info | grep networkBackend
```

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

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

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

d. 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` .

9. Starten Sie Podman neu.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker-Engine

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

Schritte

1. "Installationsanweisungen von Docker anzeigen"

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

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

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

Installieren Sie den Konsolenagenten manuell

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

Bevor Sie beginnen

Folgendes sollten Sie haben:

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

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

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

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

Informationen zu diesem Vorgang

Das auf der NetApp Support-Site verfügbare Installationsprogramm ist möglicherweise eine frühere Version. 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 von der "NetApp Support Site" , und kopieren Sie es dann auf den Linux-Host.

   Sie sollten das „Online“-Agent-Installationsprogramm herunterladen, das für die Verwendung in Ihrem Netzwerk oder in der Cloud vorgesehen ist.

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, wenn Ihr Netzwerk einen Proxy für den Internetzugang benötigt. Sie können entweder einen transparenten oder einen expliziten Proxy hinzufügen. Die Parameter --proxy und --cacert sind optional und Sie werden nicht aufgefordert, sie hinzuzufügen. Wenn Sie einen Proxyserver haben, müssen Sie die Parameter wie gezeigt eingeben.

   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://Adresse:Port
- http://Benutzername:Passwort@Adresse:Port
- http://Domänenname%92Benutzername:Passwort@Adresse:Port
- https://Adresse:Port
- https://Benutzername:Passwort@Adresse:Port
- https://Domänenname%92Benutzername:Passwort@Adresse: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 Konsolenagent unterstützt keine Benutzernamen oder Passwörter, die das @-Zeichen enthalten.
  - Wenn das Kennwort eines der folgenden Sonderzeichen enthält, müssen Sie dieses Sonderzeichen durch Voranstellen eines Backslashs maskieren: & oder !

    Beispiel:

http://bxpproxyuser:netapp1\!@Adresse:3128

`--cacert`Gibt ein von einer Zertifizierungsstelle signiertes Zertifikat an, das für den HTTPS-Zugriff zwischen dem Konsolenagenten und dem Proxyserver verwendet werden soll. Dieser Parameter ist für HTTPS-Proxyserver, abfangende Proxyserver und transparente Proxyserver erforderlich.

+ Hier ist ein Beispiel für die Konfiguration eines transparenten Proxyservers. Wenn Sie einen transparenten Proxy konfigurieren, müssen Sie den Proxyserver nicht definieren. Sie fügen Ihrem Konsolen-Agent-Host lediglich ein von einer Zertifizierungsstelle signiertes Zertifikat hinzu:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
...
# 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
...
Esc:wq
```

c. Starten Sie die virtuelle Maschine des Konsolenagenten neu.

Wie geht es weiter?

Sie müssen den Konsolenagenten in der NetApp Console registrieren.

Registrieren Sie den Konsolenagenten bei der NetApp Console

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

Schritte

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

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

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

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

   d. Wählen Sie **Los geht’s**.

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

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

AWS

Bevor Sie beginnen

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

Schritte

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

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

Azurblau

Bevor Sie beginnen

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

Schritte

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

Ergebnis

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

zu beginnen.

Installieren Sie einen Konsolenagenten vor Ort mit VCenter

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

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

Vorbereiten der Installation des Konsolenagenten

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

Überprüfen der Hostanforderungen für den Konsolenagenten

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

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

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

Einrichten des Netzwerkzugriffs für den Konsolenagenten

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

Verbindungen zu Zielnetzwerken

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

Ausgehender Internetzugang

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

Von Computern kontaktierte Endpunkte bei Verwendung der webbasierten NetApp Console

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

"Vorbereiten des Netzwerks für die NetApp Konsole" .

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

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

AWS

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

Vom Konsolenagenten kontaktierte Endpunkte

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

Die unten aufgeführten Endpunkte sind alle CNAME-Einträge.

Endpunkte	Zweck
AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)	Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab. "Weitere Einzelheiten finden Sie in der AWS-Dokumentation."
https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://signin.b2c.netapp.com	So aktualisieren Sie die Anmeldeinformationen der NetApp Support Site (NSS) oder fügen der NetApp Console neue NSS-Anmeldeinformationen hinzu.
https://support.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden sowie um Software-Updates für Cloud Volumes ONTAP zu erhalten.

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

Azurblau

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

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Zum Verwalten von Ressourcen in öffentlichen Azure-Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Zum Verwalten von Ressourcen in Azure China-Regionen.

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

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

Proxyserver

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

- IP-Adresse
- Anmeldeinformationen
- HTTPS-Zertifikat

Häfen

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

- HTTP (80) und HTTPS (443) ermöglichen den Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) wird nur benötigt, wenn Sie zur Fehlerbehebung eine Verbindung zum Host herstellen müssen.

- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP -Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

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

Aktivieren von NTP

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

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

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

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

AWS

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

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

Schritte

1. Melden Sie sich bei der AWS-Konsole an und navigieren Sie zum IAM-Dienst.
2. Erstellen Sie eine Richtlinie:

   a. Wählen Sie **Richtlinien > Richtlinie erstellen**.

   b. Wählen Sie **JSON** und kopieren und fügen Sie den Inhalt des"IAM-Richtlinie für den Konsolenagenten" .

   c. Führen Sie die restlichen Schritte aus, um die Richtlinie zu erstellen.

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

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

3. Hängen Sie die Richtlinien an einen IAM-Benutzer an.
   - "AWS-Dokumentation: Erstellen von IAM-Rollen"
   - "AWS-Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"
4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie der NetApp Console hinzufügen können, nachdem Sie den Konsolen-Agenten installiert haben.

Ergebnis

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

Azurblau

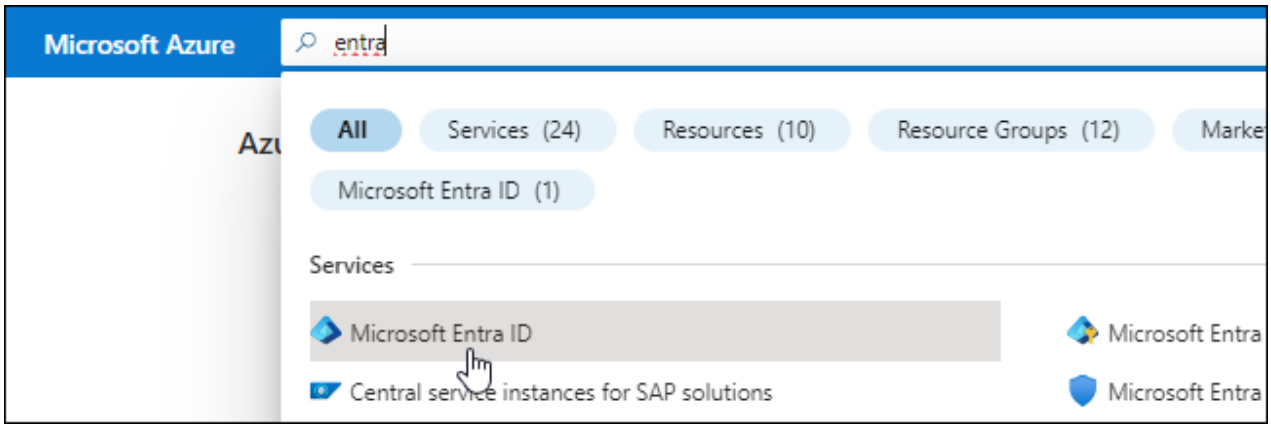
Wenn der Konsolen-Agent vor Ort installiert ist, müssen Sie dem Konsolen-Agenten Azure-Berechtigungen erteilen, indem Sie einen Dienstprinzipal in der Microsoft Entra ID einrichten und die Azure-Anmeldeinformationen abrufen, die der Konsolen-Agent benötigt.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffskontrolle

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

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

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



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

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der Anwendung zu einer Rolle

1. Erstellen Sie eine benutzerdefinierte Rolle:

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

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

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

      Sie sollten die ID für jedes Azure-Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP -Systeme erstellen.

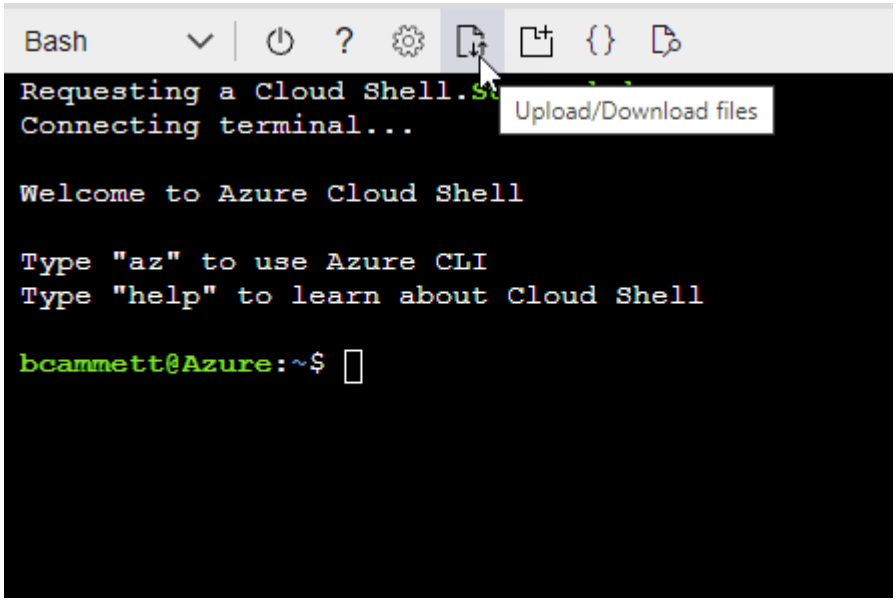
      Beispiel

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

   c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

Die folgenden Schritte beschreiben, wie Sie die Rolle mithilfe von Bash in Azure Cloud Shell erstellen.

- Start "Azure Cloud Shell" und wählen Sie die Bash-Umgebung.
- Laden Sie die JSON-Datei hoch.



- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
az role definition create --role-definition
Connector_Policy.json
```

Sie sollten jetzt über eine benutzerdefinierte Rolle namens „Konsolenoperator“ verfügen, die Sie der virtuellen Maschine des Konsolenagenten zuweisen können.

2. Weisen Sie die Anwendung der Rolle zu:

   a. Öffnen Sie im Azure-Portal den Dienst **Abonnements**.

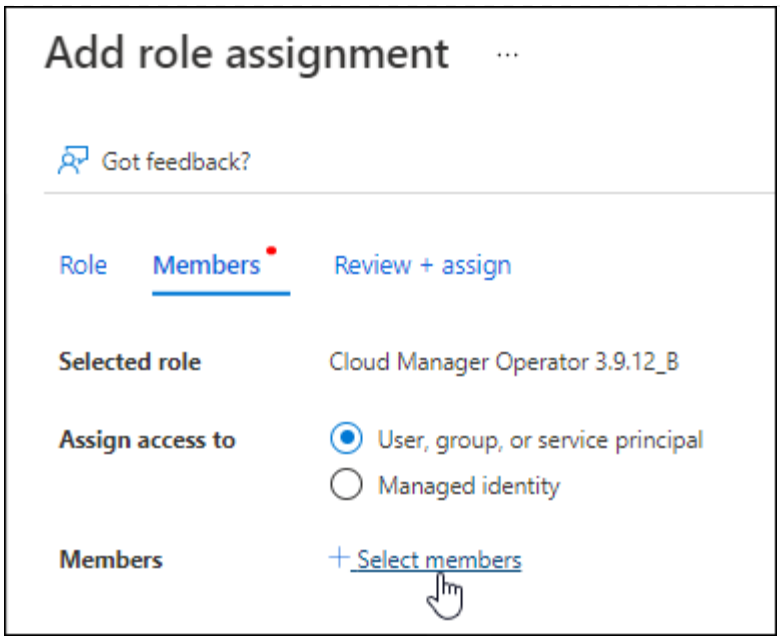
   b. Wählen Sie das Abonnement aus.

   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

   d. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.

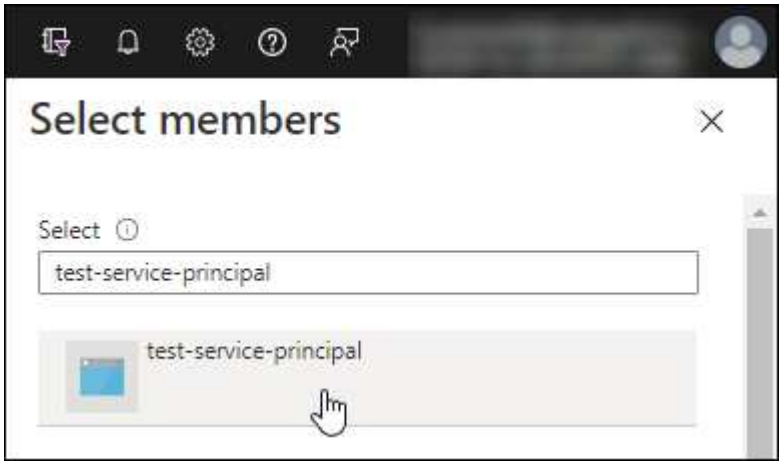
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - Behalten Sie die Auswahl von **Benutzer, Gruppe oder Dienstprinzipal** bei.
      - Wählen Sie **Mitglieder auswählen**.



- Suchen Sie nach dem Namen der Anwendung.

  Hier ist ein Beispiel:



- Wählen Sie die Anwendung aus und wählen Sie **Auswählen**.
- Wählen Sie **Weiter**.

f. Wählen Sie **Überprüfen + zuweisen**.

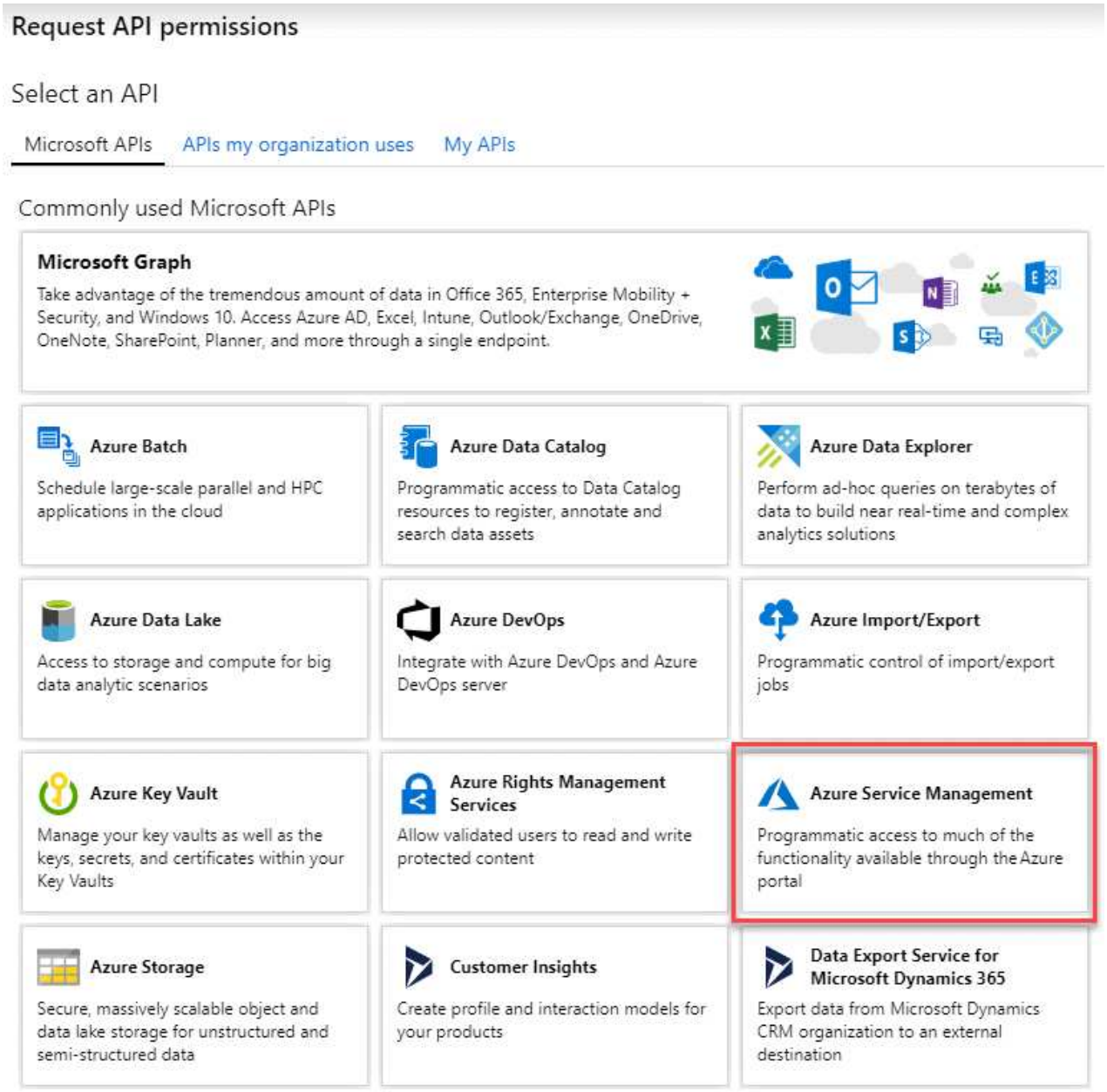
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

Wenn Sie Cloud Volumes ONTAP aus mehreren Azure-Abonnements bereitstellen möchten, müssen Sie den Dienstprinzipal an jedes dieser Abonnements binden. In der NetApp Console können Sie das Abonnement auswählen, das Sie beim Bereitstellen von Cloud Volumes ONTAP verwenden möchten.

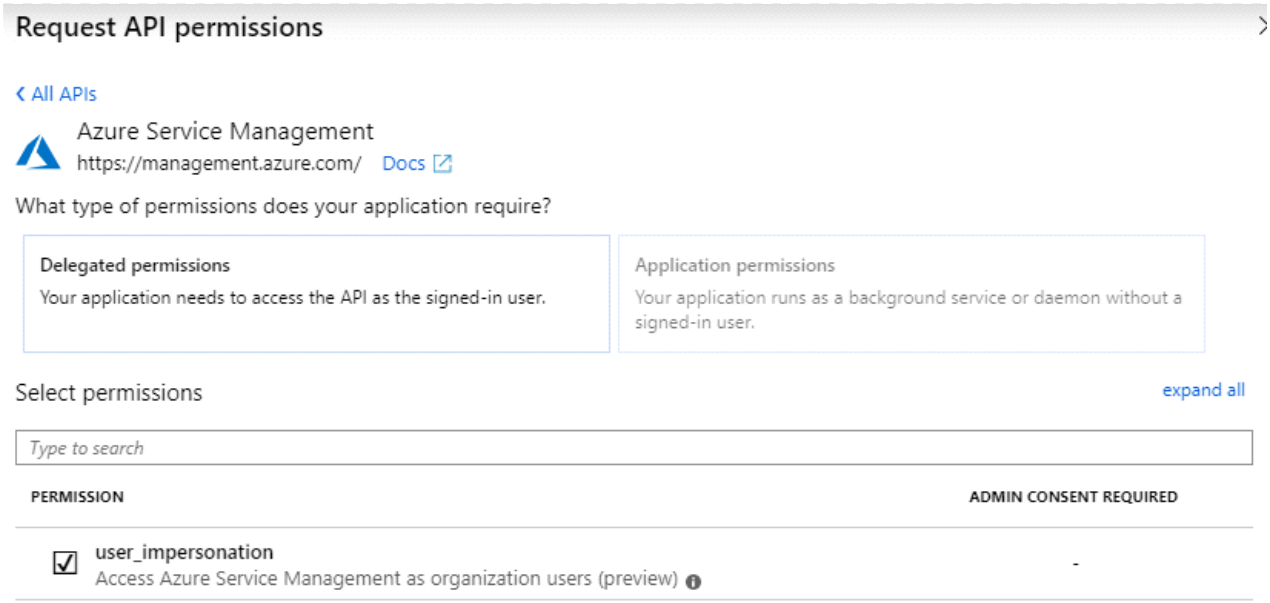
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Wählen Sie **API-Berechtigungen > Berechtigung hinzufügen**.

3. Wählen Sie unter **Microsoft-APIs Azure Service Management** aus.

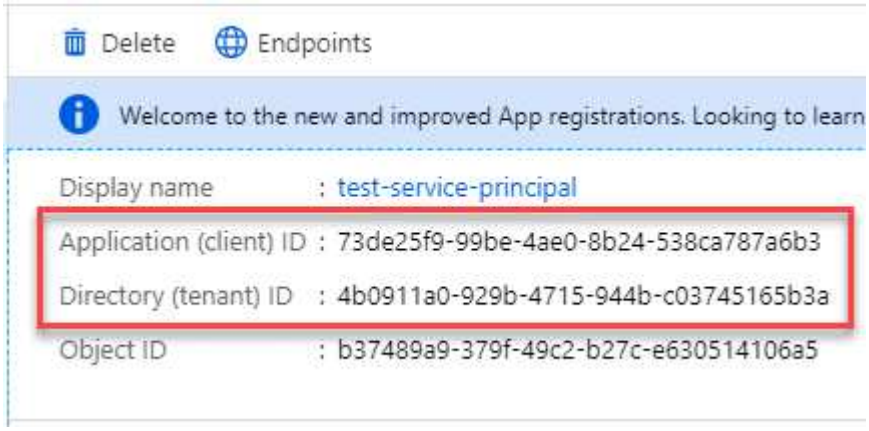


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



Abrufen der Anwendungs-ID und Verzeichnis-ID für die Anwendung

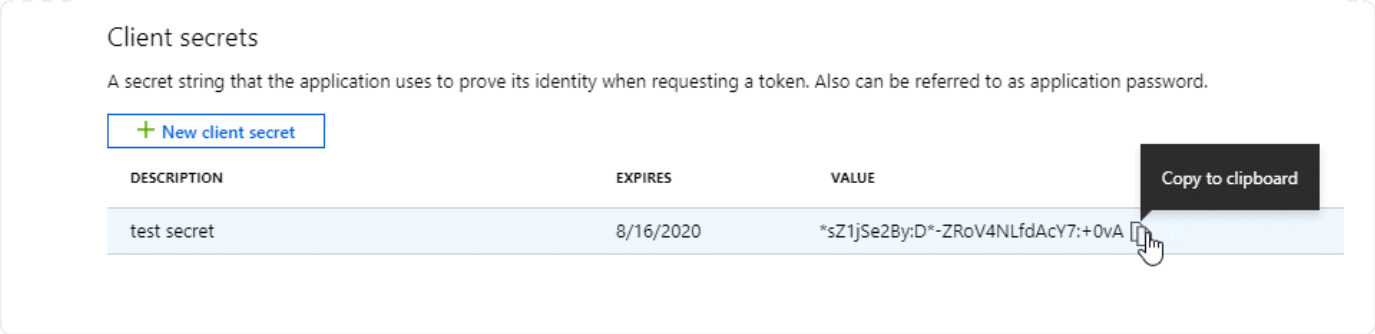
1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



Wenn Sie das Azure-Konto zur Konsole hinzufügen, müssen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) für die Anwendung angeben. Die Konsole verwendet die IDs zur programmgesteuerten Anmeldung.

Erstellen eines Client-Geheimnisses

1. Öffnen Sie den Dienst **Microsoft Entra ID**.
2. Wählen Sie **App-Registrierungen** und wählen Sie Ihre Anwendung aus.
3. Wählen Sie **Zertifikate und Geheimnisse > Neues Clientgeheimnis**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Wählen Sie **Hinzufügen**.
6. Kopieren Sie den Wert des Client-Geheimnisses.



Installieren Sie einen Konsolenagenten in Ihrer VCenter-Umgebung

NetApp unterstützt die Installation des Konsolenagenten in Ihrer VCenter-Umgebung. Die OVA-Datei enthält ein vorkonfiguriertes VM-Image, das Sie in Ihrer VMware-Umgebung bereitstellen können. Ein Dateidownload oder eine URL-Bereitstellung ist direkt über die NetApp Console möglich. Es umfasst die Konsolenagent-Software und ein selbstsigniertes Zertifikat.

Laden Sie die OVA herunter oder kopieren Sie die URL

Laden Sie die OVA herunter oder kopieren Sie die OVA-URL direkt von der NetApp Console.

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** die Option **Agent bereitstellen > Vor Ort** aus.
3. Wählen Sie **Mit OVA**.
4. Sie können entweder die OVA herunterladen oder die URL zur Verwendung in VCenter kopieren.

Stellen Sie den Agenten in Ihrem VCenter bereit

Melden Sie sich bei Ihrer VCenter-Umgebung an, um den Agenten bereitzustellen.

Schritte

1. Laden Sie das selbstsignierte Zertifikat zu Ihren vertrauenswürdigen Zertifikaten hoch, wenn Ihre Umgebung dies erfordert. Sie ersetzen dieses Zertifikat nach der Installation."Erfahren Sie, wie Sie das selbstsignierte Zertifikat ersetzen."
2. Stellen Sie die OVA aus der Inhaltsbibliothek oder dem lokalen System bereit.

Vom lokalen System	Aus der Inhaltsbibliothek
a. Klicken Sie mit der rechten Maustaste und wählen Sie **OVF-Vorlage bereitstellen…**. b. Wählen Sie die OVA-Datei aus der URL aus oder navigieren Sie zu ihrem Speicherort und wählen Sie dann **Weiter**.	a. Gehen Sie zu Ihrer Inhaltsbibliothek und wählen Sie die OVA des Konsolenagenten aus. b. Wählen Sie **Aktionen** > **Neue VM aus dieser Vorlage**

3. Schließen Sie den Assistenten „OVF-Vorlage bereitstellen“ ab, um den Konsolenagenten bereitzustellen.
4. Wählen Sie einen Namen und einen Ordner für die VM aus und wählen Sie dann **Weiter**.
5. Wählen Sie eine Computeressource aus und klicken Sie dann auf **Weiter**.
6. Überprüfen Sie die Details der Vorlage und wählen Sie dann **Weiter**.
7. Akzeptieren Sie die Lizenzvereinbarung und wählen Sie dann **Weiter**.

8. Wählen Sie den Typ der Proxy-Konfiguration, den Sie verwenden möchten: expliziter Proxy, transparenter Proxy oder kein Proxy.
9. Wählen Sie den Datenspeicher aus, in dem Sie die VM bereitstellen möchten, und wählen Sie dann **Weiter**. Stellen Sie sicher, dass es die Hostanforderungen erfüllt.
10. Wählen Sie das Netzwerk aus, mit dem Sie die VM verbinden möchten, und wählen Sie dann **Weiter**. Stellen Sie sicher, dass das Netzwerk IPv4 ist und über ausgehenden Internetzugriff auf die erforderlichen Endpunkte verfügt.
11. Füllen Sie im Fenster **Vorlage anpassen** die folgenden Felder aus:
    - **Proxy-Informationen**
      - Wenn Sie einen expliziten Proxy ausgewählt haben, geben Sie den Hostnamen oder die IP-Adresse und die Portnummer des Proxyservers sowie den Benutzernamen und das Kennwort ein.
      - Wenn Sie einen transparenten Proxy ausgewählt haben, laden Sie das entsprechende Zertifikat hoch.
    - **Konfiguration der virtuellen Maschine**
      - **Konfigurationsprüfung überspringen**: Dieses Kontrollkästchen ist standardmäßig deaktiviert, was bedeutet, dass der Agent eine Konfigurationsprüfung durchführt, um den Netzwerkzugriff zu validieren.
        - NetApp empfiehlt, dieses Kontrollkästchen deaktiviert zu lassen, damit die Installation eine Konfigurationsprüfung des Agenten umfasst. Die Konfigurationsprüfung bestätigt, dass der Agent Netzwerkzugriff auf die erforderlichen Endpunkte hat. Wenn die Bereitstellung aufgrund von Verbindungsproblemen fehlschlägt, können Sie auf den Validierungsbericht und die Protokolle vom Agent-Host zugreifen. In einigen Fällen können Sie die Prüfung überspringen, wenn Sie sicher sind, dass der Agent über Netzwerkzugriff verfügt. Wenn Sie beispielsweise immer noch die"vorherige Endpunkte" für Agent-Upgrades verwendet wird, schlägt die Validierung mit einem Fehler fehl. Um dies zu vermeiden, aktivieren Sie das Kontrollkästchen, um die Installation ohne Validierungsprüfung durchzuführen. "Erfahren Sie, wie Sie Ihre Endpunktliste aktualisieren" .
      - **Wartungskennwort**: Legen Sie das Kennwort für die `maint` Benutzer, der Zugriff auf die Agenten-Wartungskonsole ermöglicht.
      - **NTP-Server**: Geben Sie einen oder mehrere NTP-Server für die Zeitsynchronisierung an.
      - **Hostname**: Legen Sie den Hostnamen für diese VM fest. Die Suchdomäne darf nicht enthalten sein. Beispielsweise sollte ein FQDN von console10.searchdomain.company.com als console10 eingegeben werden.
      - **Primärer DNS**: Geben Sie den primären DNS-Server an, der für die Namensauflösung verwendet werden soll.
      - **Sekundärer DNS**: Geben Sie den sekundären DNS-Server an, der für die Namensauflösung verwendet werden soll.
      - Suchdomänen: Geben Sie den Suchdomänennamen an, der beim Auflösen des Hostnamens verwendet werden soll. Wenn der FQDN beispielsweise console10.searchdomain.company.com lautet, geben Sie searchdomain.company.com ein.
      - **IPv4-Adresse**: Die IP-Adresse, die dem Hostnamen zugeordnet ist.
      - **IPv4-Subnetzmaske**: Die Subnetzmaske für die IPv4-Adresse.
      - **IPv4-Gateway-Adresse**: Die Gateway-Adresse für die IPv4-Adresse.
12. Wählen Sie **Weiter**.
13. Überprüfen Sie die Details im Fenster **Bereit zum Abschließen** und wählen Sie **Fertig**.

Die vSphere-Taskleiste zeigt den Fortschritt der Bereitstellung des Konsolenagenten an.

14. Schalten Sie die VM ein.

> Wenn die Bereitstellung fehlschlägt, können Sie auf den Validierungsbericht und die Protokolle vom Agent-Host zugreifen."Erfahren Sie, wie Sie Installationsprobleme beheben."

Registrieren Sie den Konsolenagenten bei der NetApp Console

Melden Sie sich bei der Konsole an und verknüpfen Sie den Konsolenagenten mit Ihrer Organisation. Die Art der Anmeldung hängt vom Modus ab, in dem Sie die Konsole verwenden. Wenn Sie die Konsole im Standardmodus verwenden, melden Sie sich über die SaaS-Website an. Wenn Sie die Konsole im eingeschränkten oder privaten Modus verwenden, melden Sie sich lokal vom Konsolen-Agent-Host aus an.

Schritte

1. Öffnen Sie einen Webbrowser und geben Sie die Host-URL des Konsolenagenten ein:

   Die Host-URL der Konsole kann je nach Konfiguration des Hosts ein lokaler Host, eine private IP-Adresse oder eine öffentliche IP-Adresse sein. Wenn sich der Konsolenagent beispielsweise in der öffentlichen Cloud ohne öffentliche IP-Adresse befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der über eine Verbindung zum Host des Konsolenagenten verfügt.

2. Registrieren oder anmelden.
3. Richten Sie nach der Anmeldung die Konsole ein:
   a. Geben Sie die Konsolenorganisation an, die mit dem Konsolenagenten verknüpft werden soll.
   b. Geben Sie einen Namen für das System ein.
   c. Lassen Sie unter **Arbeiten Sie in einer sicheren Umgebung?** den eingeschränkten Modus deaktiviert.

      Der eingeschränkte Modus wird nicht unterstützt, wenn der Konsolen-Agent vor Ort installiert ist.

   d. Wählen Sie **Los geht’s**.

Fügen Sie der Konsole Anmeldeinformationen des Cloud-Anbieters hinzu

Nachdem Sie den Konsolen-Agenten installiert und eingerichtet haben, fügen Sie Ihre Cloud-Anmeldeinformationen hinzu, damit der Konsolen-Agent über die erforderlichen Berechtigungen zum Ausführen von Aktionen in AWS oder Azure verfügt.

AWS

Bevor Sie beginnen

Wenn Sie diese AWS-Anmeldeinformationen gerade erstellt haben, kann es einige Minuten dauern, bis sie verfügbar sind. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zur Konsole hinzufügen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie *Amazon Web Services > Agent.
   b. **Anmeldeinformationen definieren**: Geben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel ein.
   c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.
   d. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Sie können jetzt zu "NetApp Console" um mit der Verwendung des Konsolenagenten zu beginnen.

Azurblau

Bevor Sie beginnen

Wenn Sie diese Azure-Anmeldeinformationen gerade erstellt haben, kann es einige Minuten dauern, bis sie verfügbar sind. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zum Konsolenagenten hinzufügen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Microsoft Azure > Agent**.
   b. **Anmeldeinformationen definieren**: Geben Sie Informationen zum Microsoft Entra-Dienstprinzipal ein, der die erforderlichen Berechtigungen erteilt:
      - Anwendungs-ID (Client-ID)
      - Verzeichnis-ID (Mandant)
      - Client-Geheimnis
   c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.
   d. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Ergebnis

Der Konsolenagent verfügt jetzt über die erforderlichen Berechtigungen, um in Ihrem Namen Aktionen in Azure auszuführen. Sie können jetzt zu "NetApp Console" um mit der Verwendung des Konsolenagenten

zu beginnen.

Abonnieren Sie NetApp Intelligent Services (Standardmodus)

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 NetApp -Datendienste:

- 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

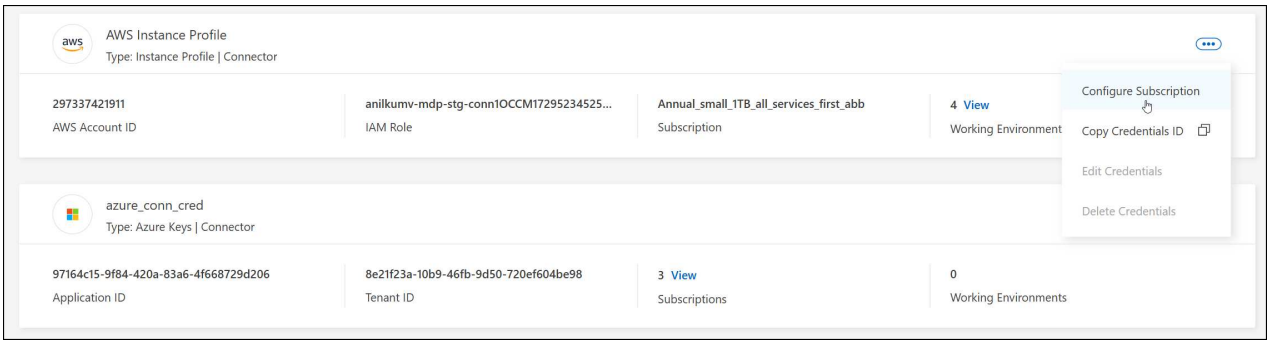
Das folgende Video zeigt die Schritte zum Abonnieren von NetApp Intelligent Services vom AWS Marketplace:

Abonnieren Sie NetApp Intelligent Services vom AWS Marketplace

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**.

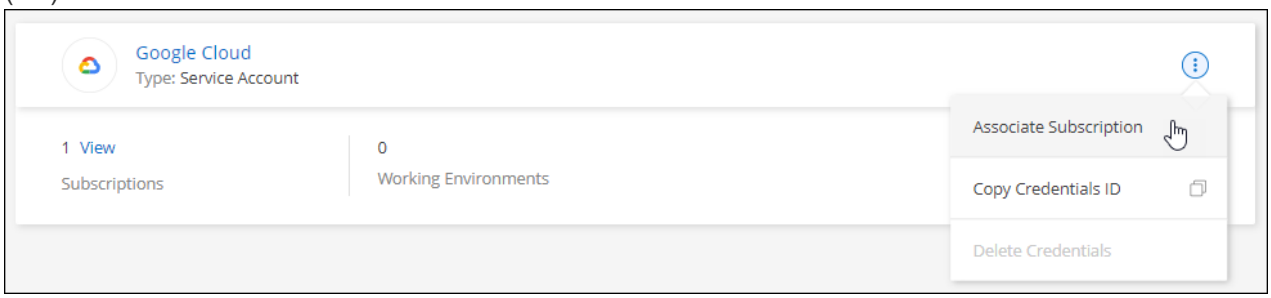
        Das folgende Video zeigt die Schritte zum Abonnieren über den Azure Marketplace:

Abonnieren Sie NetApp Intelligent Services vom Azure Marketplace

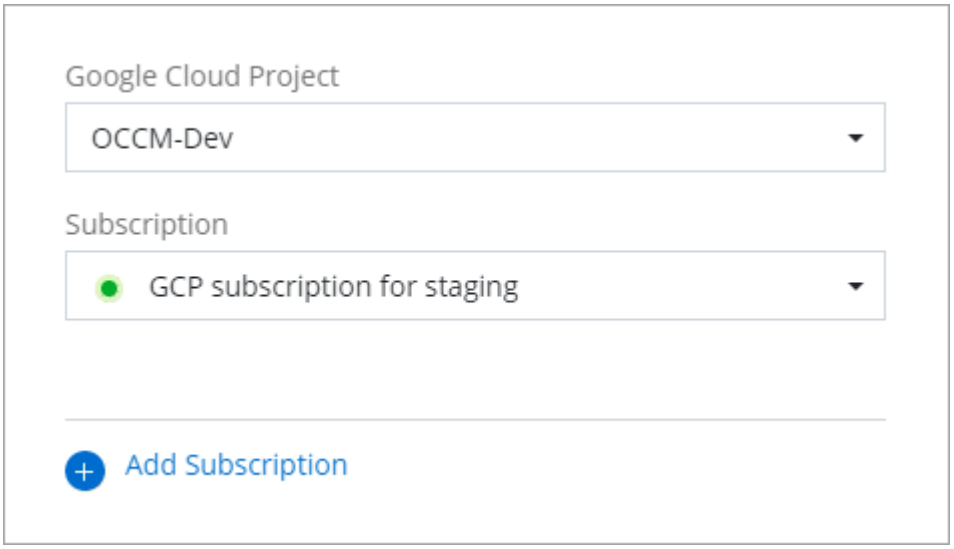
Google Cloud

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**. +neuer Screenshot erforderlich
(TS)



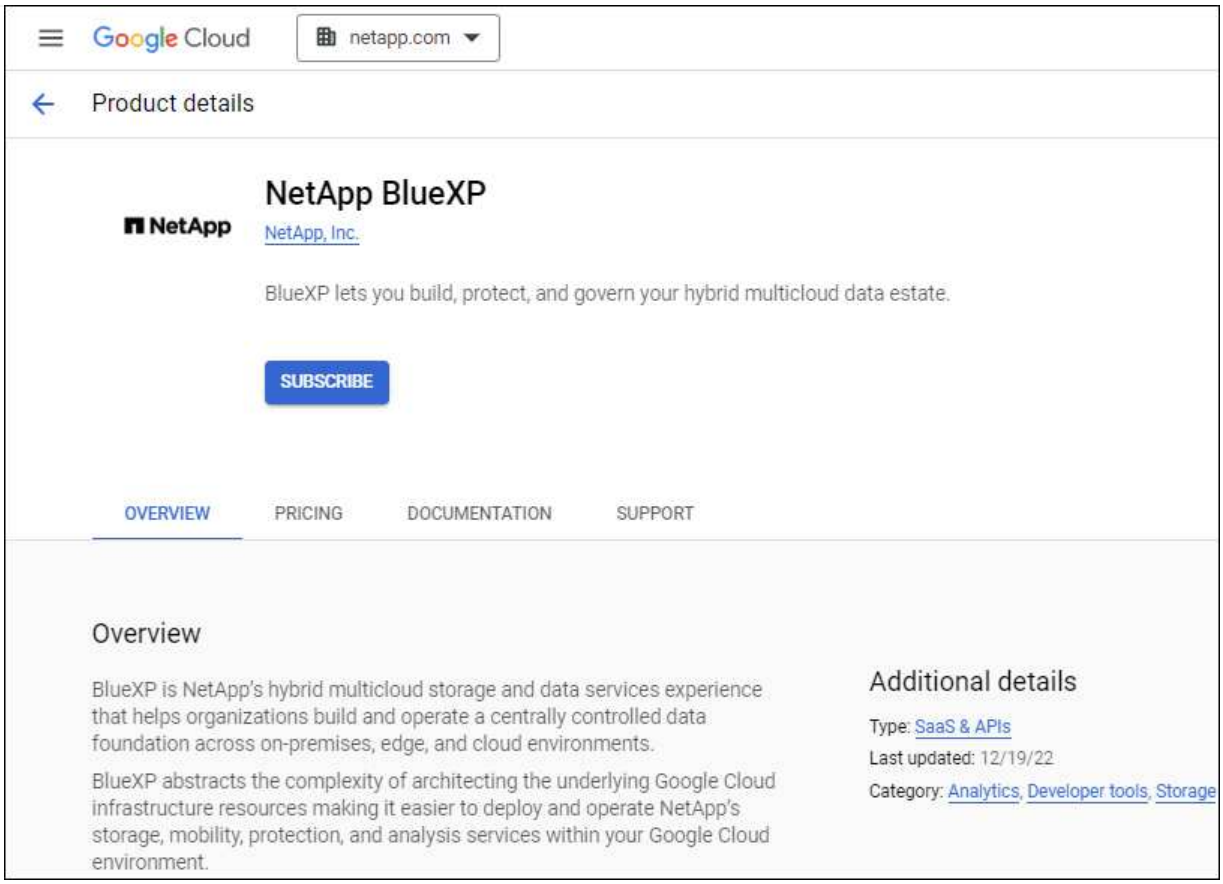
4. Um ein vorhandenes Abonnement mit den ausgewählten Anmeldeinformationen zu konfigurieren, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Dropdown-Liste aus und wählen Sie dann **Konfigurieren**.



5. 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.

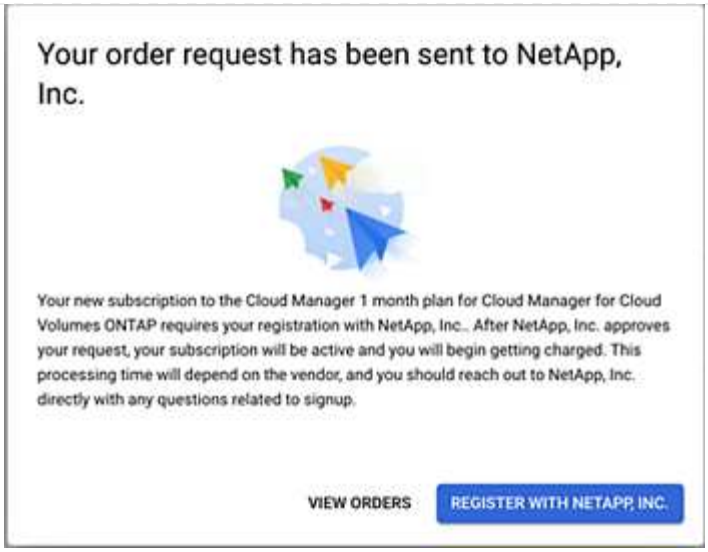


b. Wählen Sie **Abonnieren**.
c. Wählen Sie das entsprechende Abrechnungskonto aus und stimmen Sie den Allgemeinen Geschäftsbedingungen zu.
d. Wählen Sie **Abonnieren**.

   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 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.

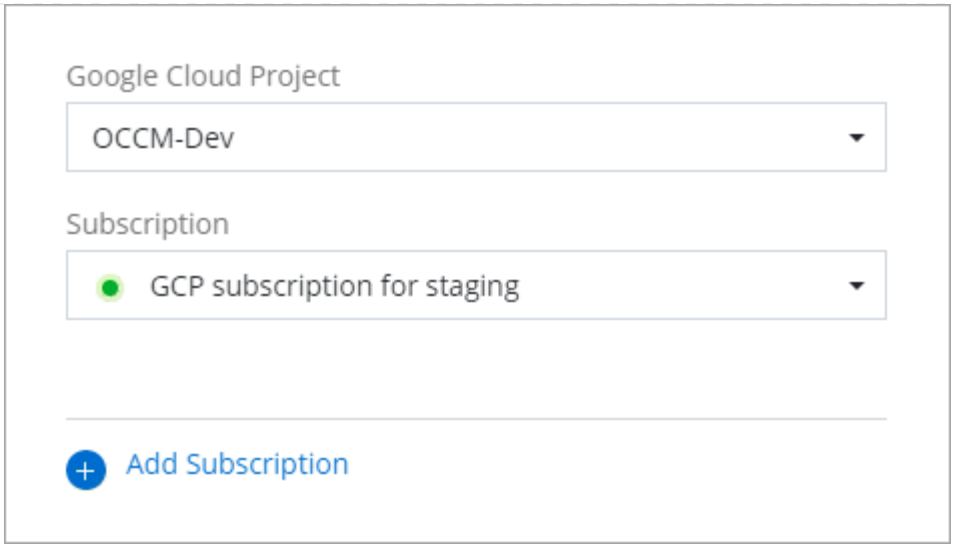
Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.

- Wählen Sie **Speichern**.

  Das folgende Video zeigt die Schritte zum Abonnieren vom Google Cloud Marketplace:

Abonnieren Sie über den Google Cloud Marketplace

a. 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 (Standardmodus)

Nachdem Sie sich angemeldet und die NetApp Console im Standardmodus eingerichtet haben, können Benutzer Speichersysteme erstellen und erkennen sowie NetApp -Datendienste verwenden.

Wenn Sie einen Konsolenagenten in AWS, Microsoft Azure oder Google Cloud installiert haben, erkennt die Konsole automatisch Informationen zu den Amazon S3-Buckets, Azure Blob Storage oder Google Cloud Storage-Buckets am Standort, an dem der Agent installiert ist. Diese Systeme werden automatisch zur Seite **Systeme** hinzugefügt.

Hilfe erhalten Sie unter "Homepage für die NetApp Console Dokumentation" um die Dokumentation zur NetApp Console anzuzeigen.

Ähnliche Informationen

"Bereitstellungsmodi der NetApp Console"

Erste Schritte mit dem eingeschränkten 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" .

"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.

"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.

"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 wird auf einem Host, der mit anderen Anwendungen gemeinsam genutzt wird, nicht unterstützt. Der Host muss ein dedizierter Host sein. Der Host kann jede Architektur aufweisen, die die folgenden 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 in `/var` weil Docker oder Podman so konzipiert sind, dass sie die Container in diesem Verzeichnis erstellen. Konkret werden sie Container in der `/var/lib/containers/storage` Verzeichnis. Externe Mounts oder Symlinks funktionieren für diesen Bereich nicht.

Hypervisor

Es ist ein Bare-Metal- oder gehosteter Hypervisor erforderlich, der für die Ausführung eines unterstützten Betriebssystems zertifiziert ist.

Betriebssystem- und Containeranforderungen

Der Konsolenagent wird von den folgenden Betriebssystemen unterstützt, wenn die Konsole im Standardmodus oder eingeschränkten Modus verwendet wird. Vor der Installation des Agenten ist ein Container-Orchestrierungstool erforderlich.

Betriebssystem	Unterstützte Betriebssystemversionen	Unterstützte Agent-Versionen	Erforderliches Container-Tool	SELinux a
Red Hat Enterprise Linux	9,1 bis 9,4 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 Podman-Konfigurationsanforderungen anzeigen .	Unterstützt im Durchsetzungsmodus oder im Permissivmodus • Die Verwaltung von Cloud Volumes ONTAP -Systemen wird NICHT von Agenten unterstützt, auf deren Betriebssystem SELinux aktiviert ist.
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

AWS EC2-Instanztyp

Ein Instanztyp, der die oben genannten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen t3.2xlarge.

Azure-VM-Größe

Ein Instanztyp, der die oben genannten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen Standard_D8s_v3.

Google Cloud-Maschinentyp

Ein Instanztyp, der die oben genannten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen n2-standard-8.

Der Konsolenagent wird in Google Cloud auf einer VM-Instanz mit einem Betriebssystem unterstützt, das "Funktionen von Shielded VM"

Speicherplatz in /opt

100 GiB Speicherplatz müssen verfügbar sein

Der Agent verwendet `/opt` zur Installation des `/opt/application/netapp` Verzeichnis und dessen Inhalt.

Speicherplatz in /var

20 GiB Speicherplatz müssen verfügbar sein

Der Konsolenagent benötigt diesen Speicherplatz in `/var` weil Docker oder Podman so konzipiert sind, dass sie die Container in diesem Verzeichnis erstellen. Konkret werden sie Container in der `/var/lib/containers/storage` Verzeichnis. Externe Mounts oder Symlinks funktionieren für diesen Bereich nicht.

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 5. 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 8 verwenden, überprüfen Sie, ob Ihre Podman-Version 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.

   Für Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Dabei ist <Version> die unterstützte Version von Podman, die Sie installieren. Sehen Sie sich die unterstützten Podman-Versionen an .

   Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<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.
6. Bei Verwendung von Red Hat Enterprise:

   Dieser Schritt ist erforderlich, da podman-compose im Repository „Extra Packages for Enterprise Linux“ (EPEL) verfügbar ist.

   Für Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   Für Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

7. 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.

8. Wenn Sie Red Hat Enterprise Linux 8 verwenden, überprüfen Sie, ob Ihre Podman-Version NetAvark mit Aardvark DNS anstelle von CNI verwendet.

   a. Überprüfen Sie, ob Ihr Netzwerk-Backend auf CNI eingestellt ist, indem Sie den folgenden Befehl ausführen:

```
podman info | grep networkBackend
```

   b. Wenn das Netzwerk-Backend auf `CNI` , müssen Sie es ändern in `netavark` .

   c. Installieren `netavark` Und `aardvark-dns` mit dem folgenden Befehl:

```
dnf install aardvark-dns netavark
```

d. 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` .

9. Starten Sie Podman neu.

```
systemctl restart podman
```

10. 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.

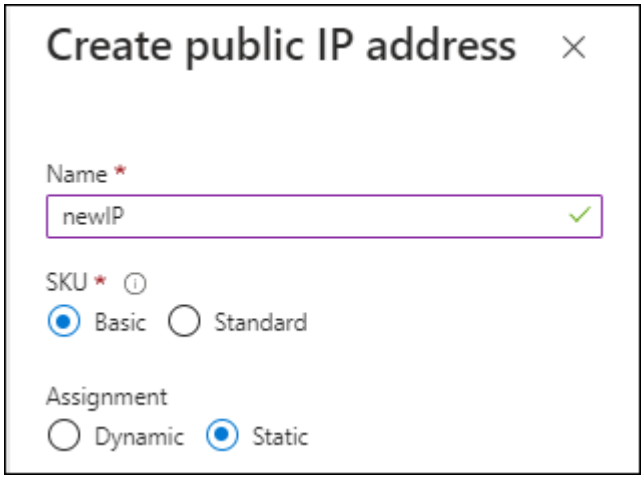
Endpunkte	Zweck
AWS-Umgebungen	AWS-Dienste (amazonaws.com): • CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)
Zur Verwaltung von AWS-Ressourcen. Der Endpunkt hängt von Ihrer AWS-Region ab. "Weitere Einzelheiten finden Sie in der AWS-Dokumentation."	**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.

Endpunkte	Zweck
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://www.googleapis.com/deploymentmanager/v2/projects
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://support.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.

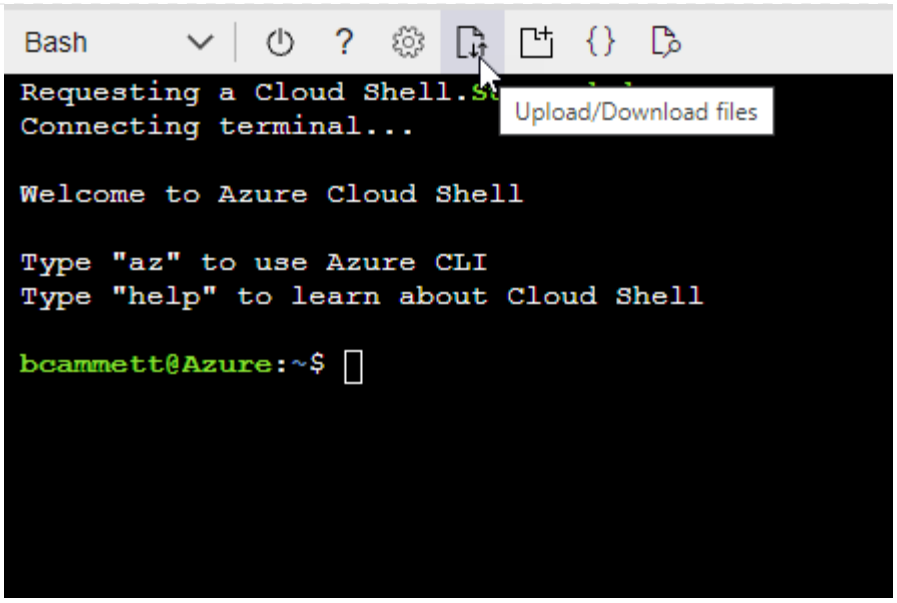
   Beispiel

   ```
   "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 Connector_Policy.json
```

Azure-Dienstprinzipal

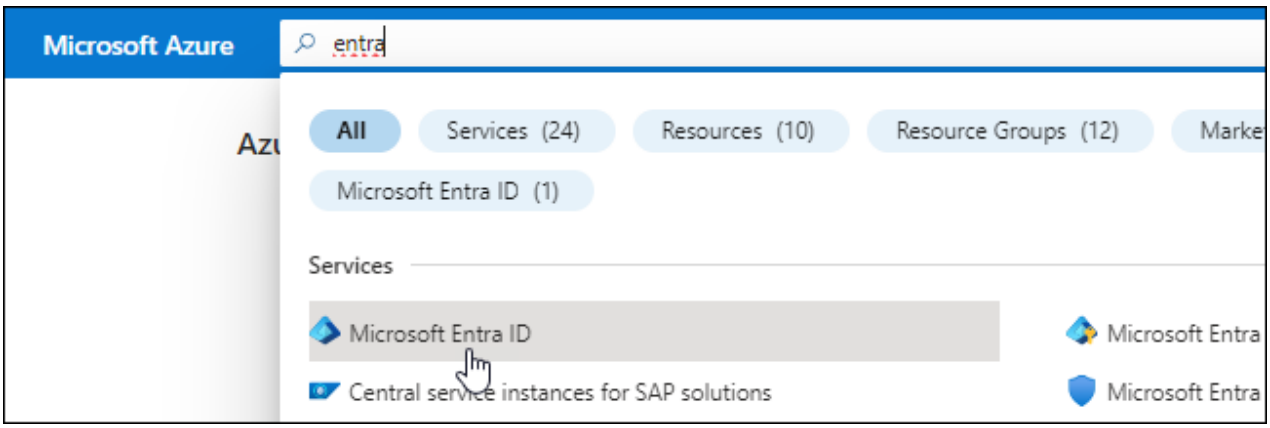
Erstellen und richten Sie einen Dienstprinzipal in Microsoft Entra ID ein und rufen Sie die Azure-Anmeldeinformationen ab, die die Konsole benötigt. Sie müssen der Konsole diese Anmeldeinformationen bereitstellen, nachdem Sie den Konsolenagenten installiert haben.

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.

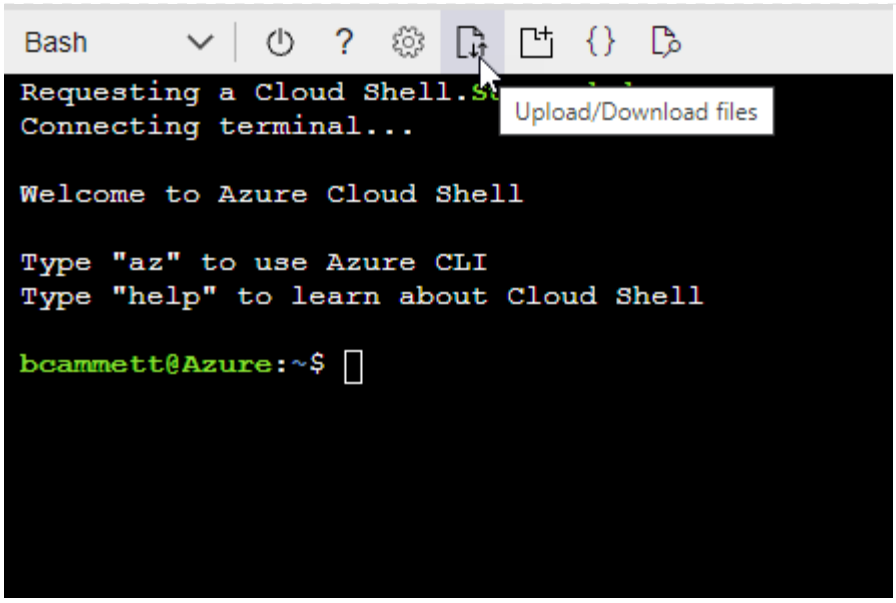
      Beispiel

      ```
      "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
Connector_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**.

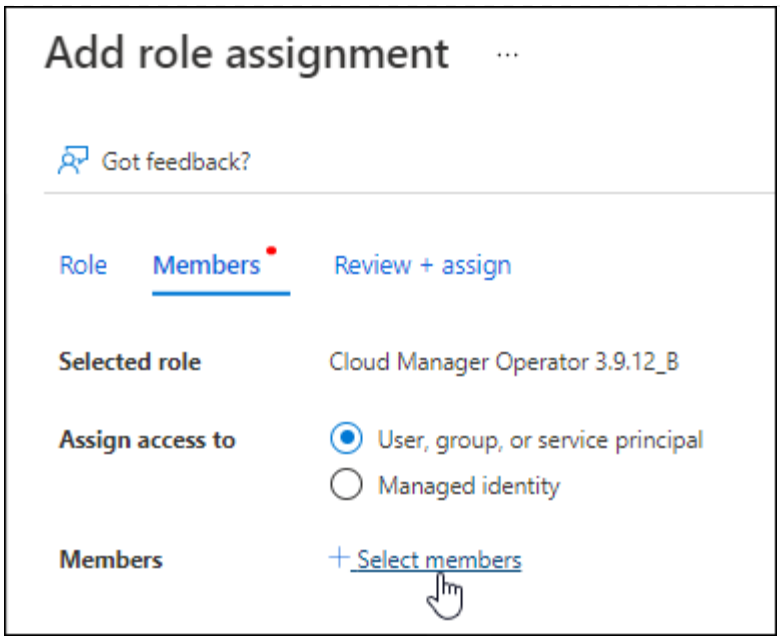
   b. Wählen Sie das Abonnement aus.

   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

   d. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.

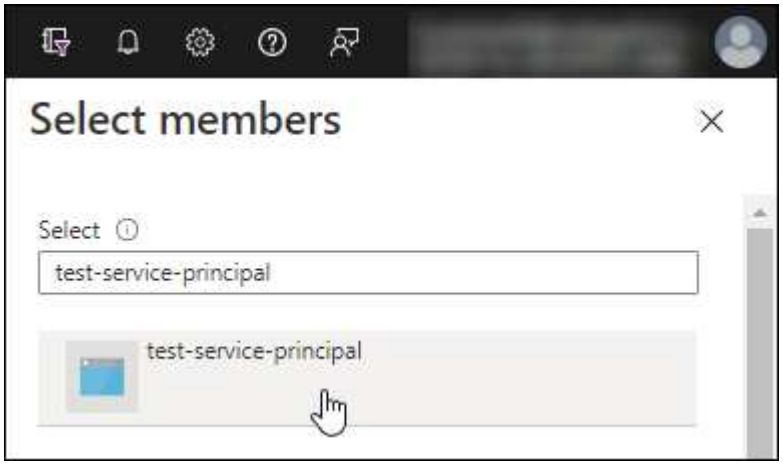
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - 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**.

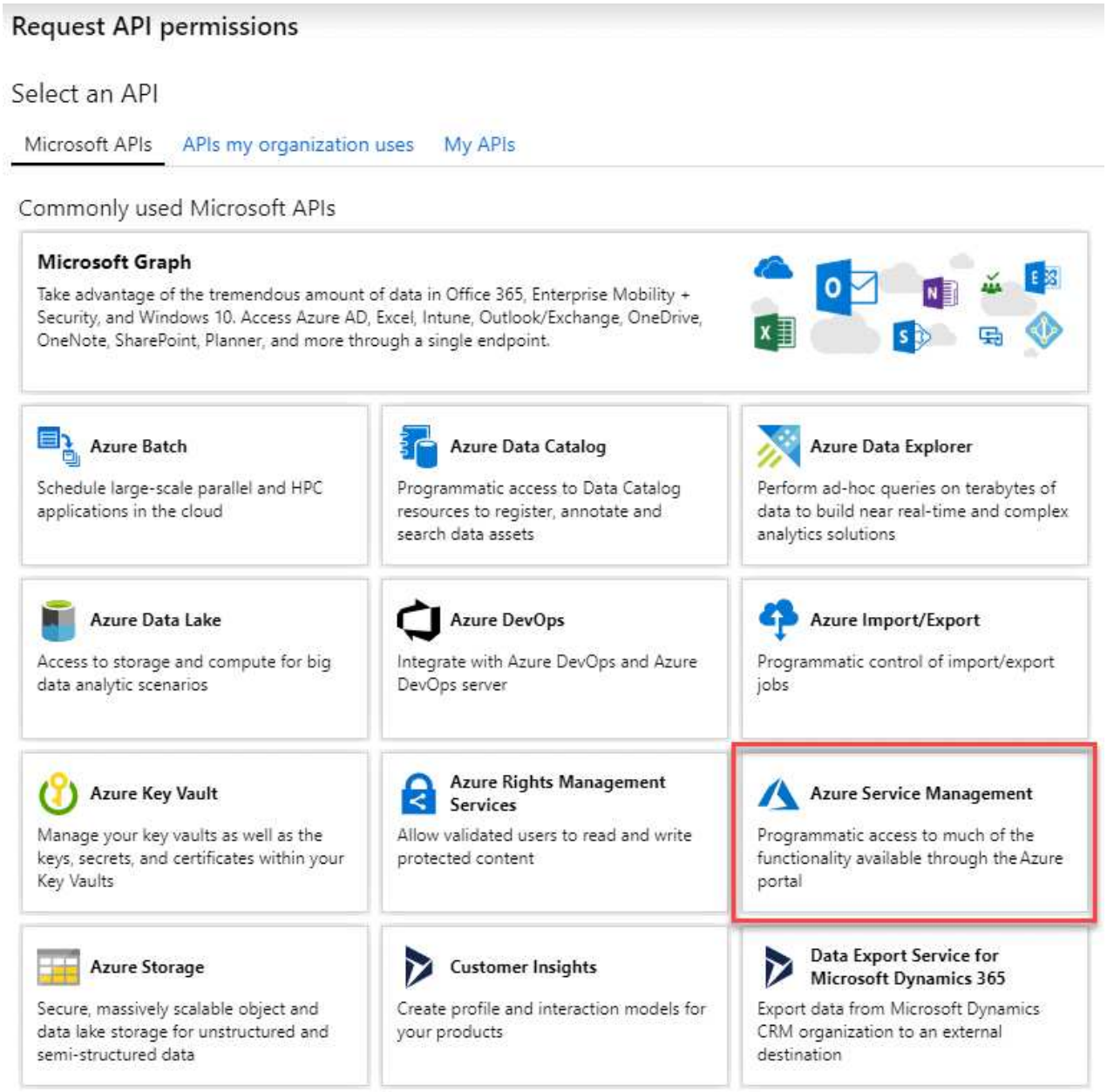
Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

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.

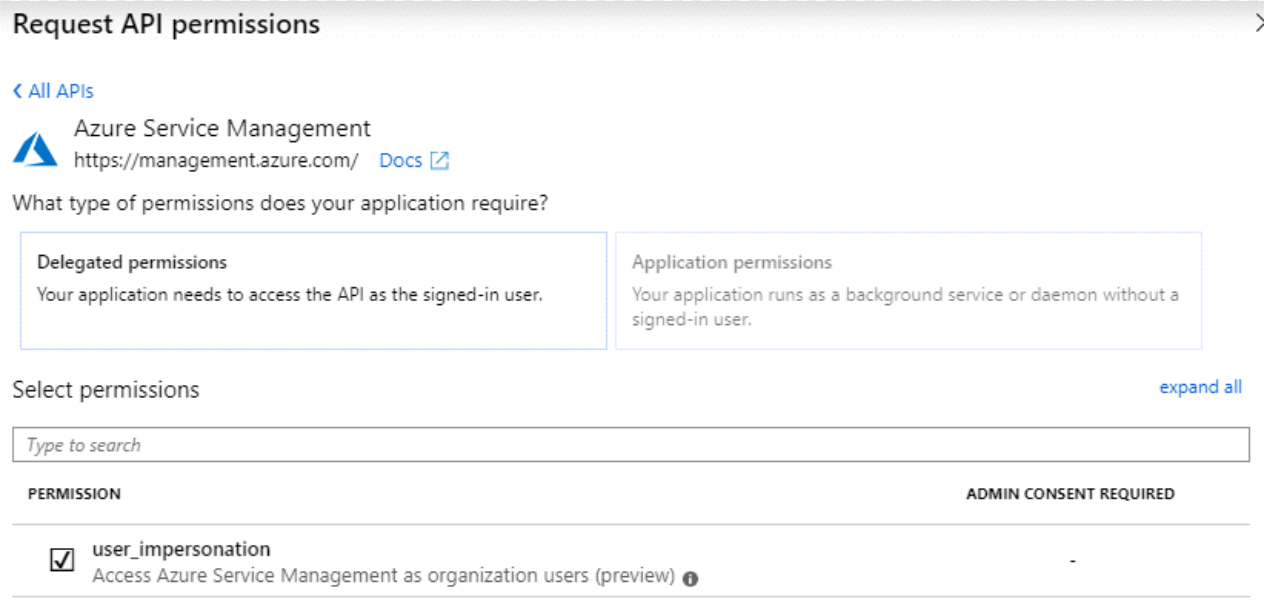
Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

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.

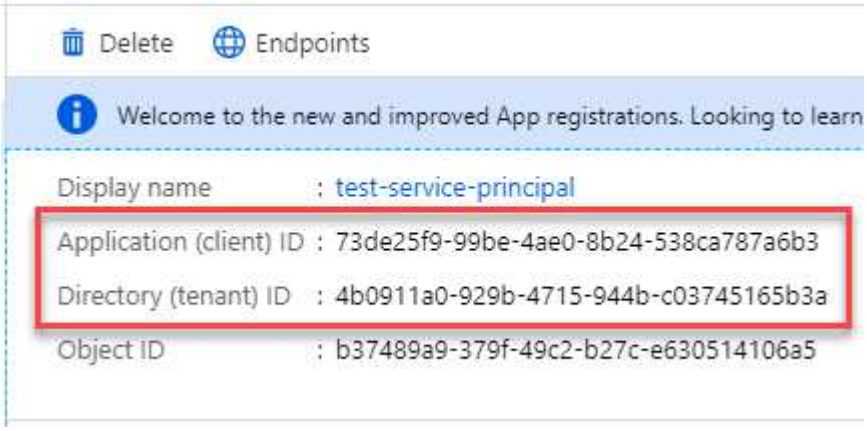


4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.



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 auf Projektebene eine Rolle mit dem Namen „Connector“:

```
gcloud iam roles create connector --project=myproject
--file=connector.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"

Ergebnis

Sie verfügen jetzt über ein Dienstkonto, das Sie der VM-Instanz des Konsolenagenten zuweisen können.

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 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.

AWS Commercial Marketplace

Bevor Sie beginnen

Folgendes sollten Sie haben:

- 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 die Instanz.

  "Überprüfen der Instanzanforderungen" .

- 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 Konsolen-Agentinstanz und -Software werden in etwa fünf Minuten ausgeführt.

Wie geht es weiter?

Richten Sie die NetApp Console ein.

AWS Gov Marketplace

Bevor Sie beginnen

Folgendes sollten Sie haben:

- Eine VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt.

  "Informieren Sie sich über die Netzwerkanforderungen"

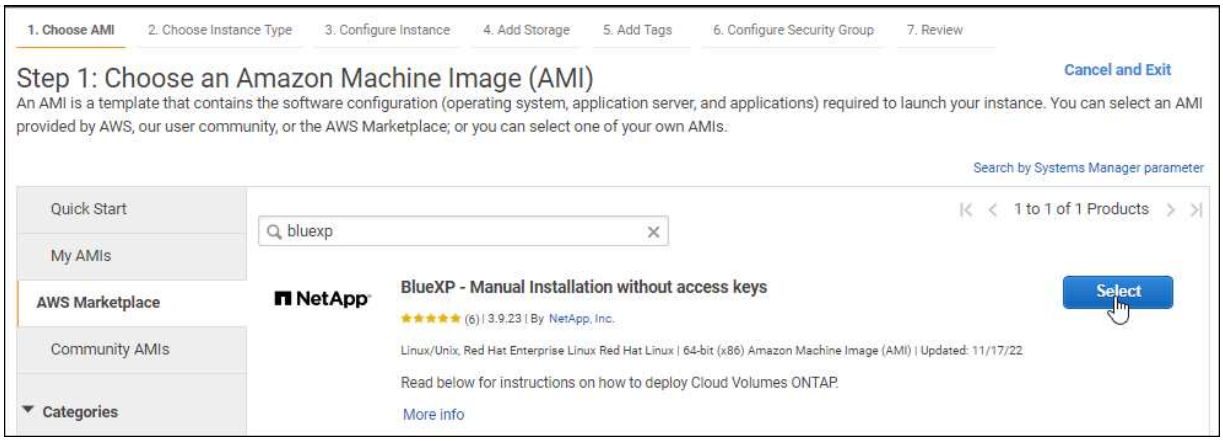
- Eine IAM-Rolle mit einer angehängten Richtlinie, die die erforderlichen Berechtigungen für den Konsolenagenten enthält.

  "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.



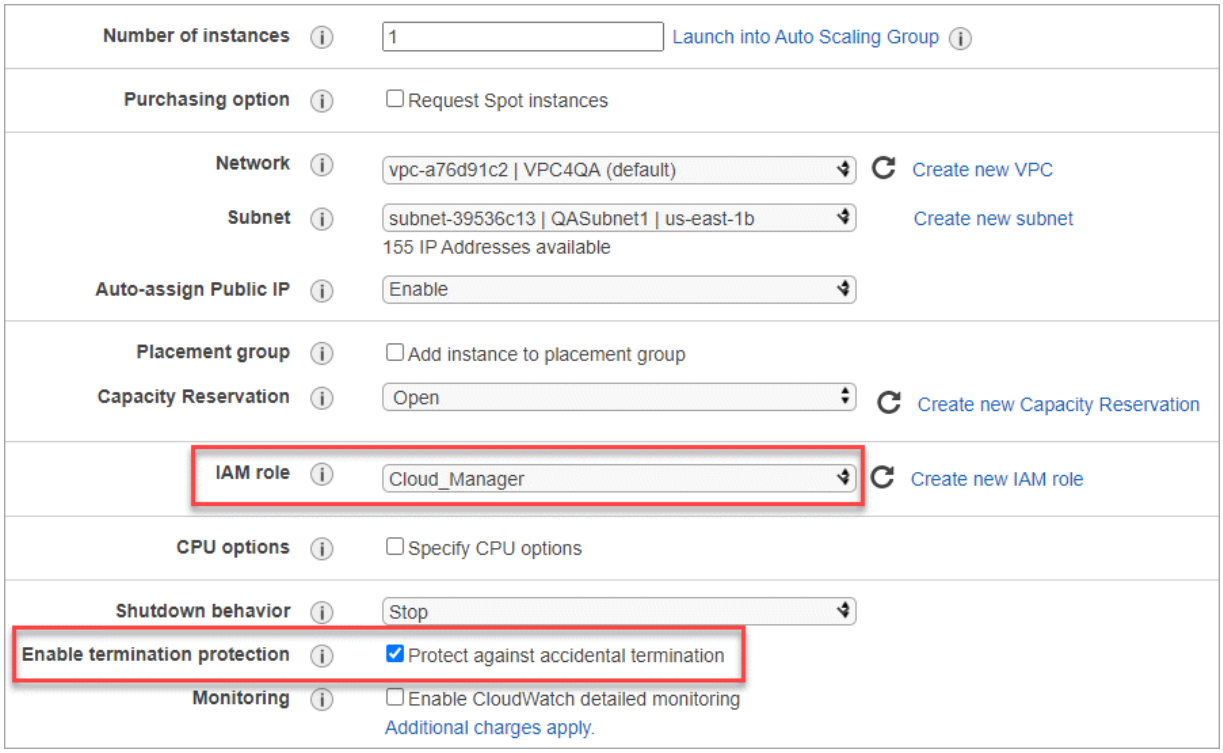
d. Wählen Sie **Weiter**.

2. Folgen Sie den Anweisungen zum Konfigurieren und Bereitstellen der Instanz:

   - **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 Konsolen-Agentinstanz und -Software werden in etwa fünf Minuten ausgeführt.

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.

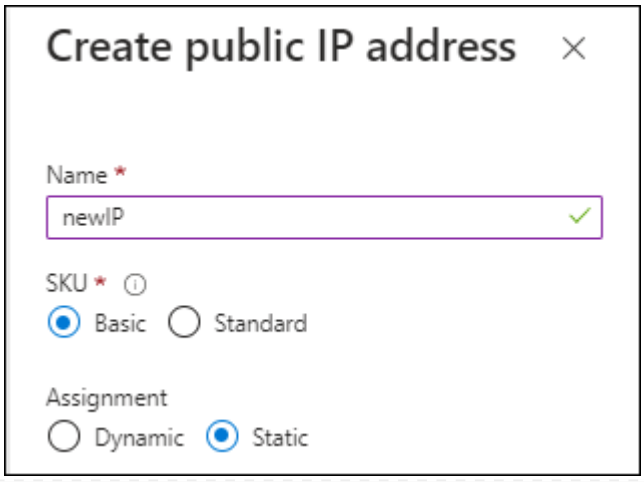
  "Erfahren Sie, wie Sie Azure-Berechtigungen einrichten"

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**: Wenn Sie eine öffentliche IP-Adresse mit der Konsolen-Agent-VM 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"

- **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**.

  Diese Einstellung ist wichtig, da eine verwaltete Identität es der virtuellen Maschine des Konsolenagenten ermöglicht, sich gegenüber der Microsoft Entra ID zu identifizieren, ohne Anmeldeinformationen angeben zu müssen. "Erfahren Sie mehr über verwaltete Identitäten für Azure-Ressourcen" .

4. Überprüfen Sie auf der Seite **Überprüfen + Erstellen** Ihre Auswahl und wählen Sie **Erstellen** aus, um die Bereitstellung zu starten.

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

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" .

- 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

Das auf der NetApp Support-Site verfügbare Installationsprogramm ist möglicherweise eine frühere Version. 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 von der "NetApp Support Site" , und kopieren Sie es dann auf den Linux-Host.

   Sie sollten das „Online“-Agent-Installationsprogramm herunterladen, das für die Verwendung in Ihrem Netzwerk oder in der Cloud vorgesehen ist.

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, wenn Ihr Netzwerk einen Proxy für den Internetzugang benötigt. Sie können entweder einen transparenten oder einen expliziten Proxy hinzufügen. Die Parameter --proxy und --cacert sind optional und Sie werden nicht aufgefordert, sie hinzuzufügen. Wenn Sie einen Proxyserver haben, müssen Sie die Parameter wie gezeigt eingeben.

   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://Adresse:Port
- http://Benutzername:Passwort@Adresse:Port
- http://Domänenname%92Benutzername:Passwort@Adresse:Port
- https://Adresse:Port
- https://Benutzername:Passwort@Adresse:Port
- https://Domänenname%92Benutzername:Passwort@Adresse: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 Konsolenagent unterstützt keine Benutzernamen oder Passwörter, die das @-Zeichen enthalten.
  - Wenn das Kennwort eines der folgenden Sonderzeichen enthält, müssen Sie dieses Sonderzeichen durch Voranstellen eines Backslashs maskieren: & oder !

    Beispiel:

http://bxpproxyuser:netapp1\!@Adresse:3128

`--cacert`Gibt ein von einer Zertifizierungsstelle signiertes Zertifikat an, das für den HTTPS-Zugriff zwischen dem Konsolenagenten und dem Proxyserver verwendet werden soll. Dieser Parameter ist für HTTPS-Proxyserver, abfangende Proxyserver und transparente Proxyserver erforderlich.

+ Hier ist ein Beispiel für die Konfiguration eines transparenten Proxyservers. Wenn Sie einen transparenten Proxy konfigurieren, müssen Sie den Proxyserver nicht definieren. Sie fügen Ihrem Konsolen-Agent-Host lediglich ein von einer Zertifizierungsstelle signiertes Zertifikat hinzu:

+

```
 ./NetApp_Console_Agent_Cloud_v4.0.0 --cacert
/tmp/cacert/certificate.cer
```

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
...
# 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
...
Esc:wq
```

c. 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.

Wenn Ihr Login mit einer anderen Organisation verknüpft ist, müssen Sie sich mit einem neuen Login anmelden. Andernfalls wird die Option zum Aktivieren des eingeschränkten Modus auf dem Einrichtungsbildschirm 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: Berechtigungen für die NetApp Console erteilen

Wenn Sie den Konsolen-Agenten aus dem Azure Marketplace bereitgestellt oder die Konsolen-Agenten-Software manuell installiert haben, müssen Sie die zuvor eingerichteten Berechtigungen angeben.

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

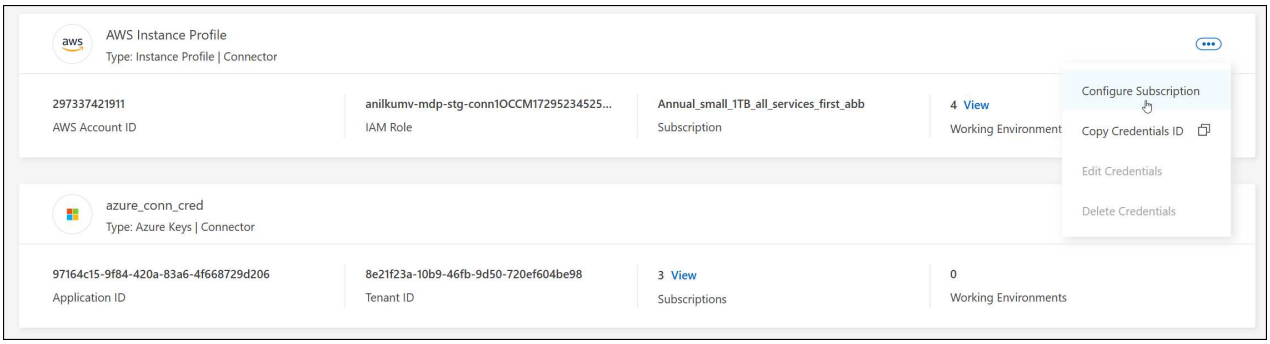
Das folgende Video zeigt die Schritte zum Abonnieren von NetApp Intelligent Services vom AWS Marketplace:

Abonnieren Sie NetApp Intelligent Services vom AWS Marketplace

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**.

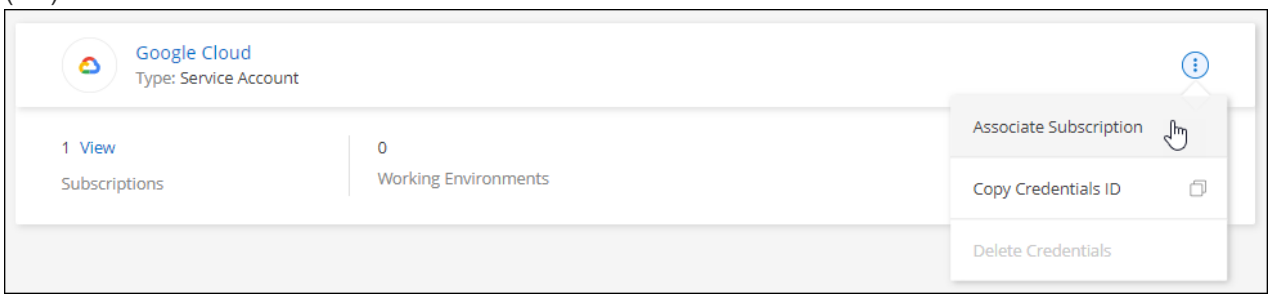
        Das folgende Video zeigt die Schritte zum Abonnieren über den Azure Marketplace:

Abonnieren Sie NetApp Intelligent Services vom Azure Marketplace

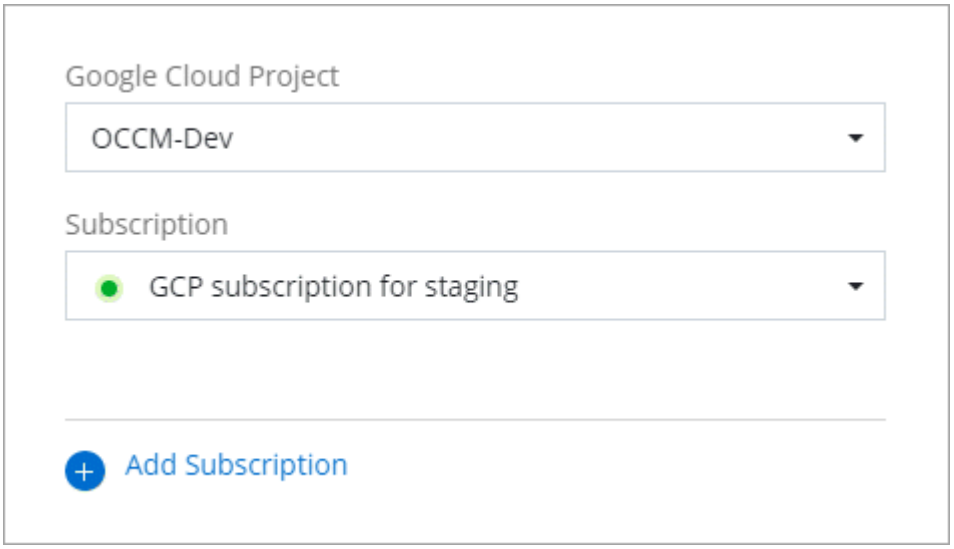
Google Cloud

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**. +neuer Screenshot erforderlich
(TS)



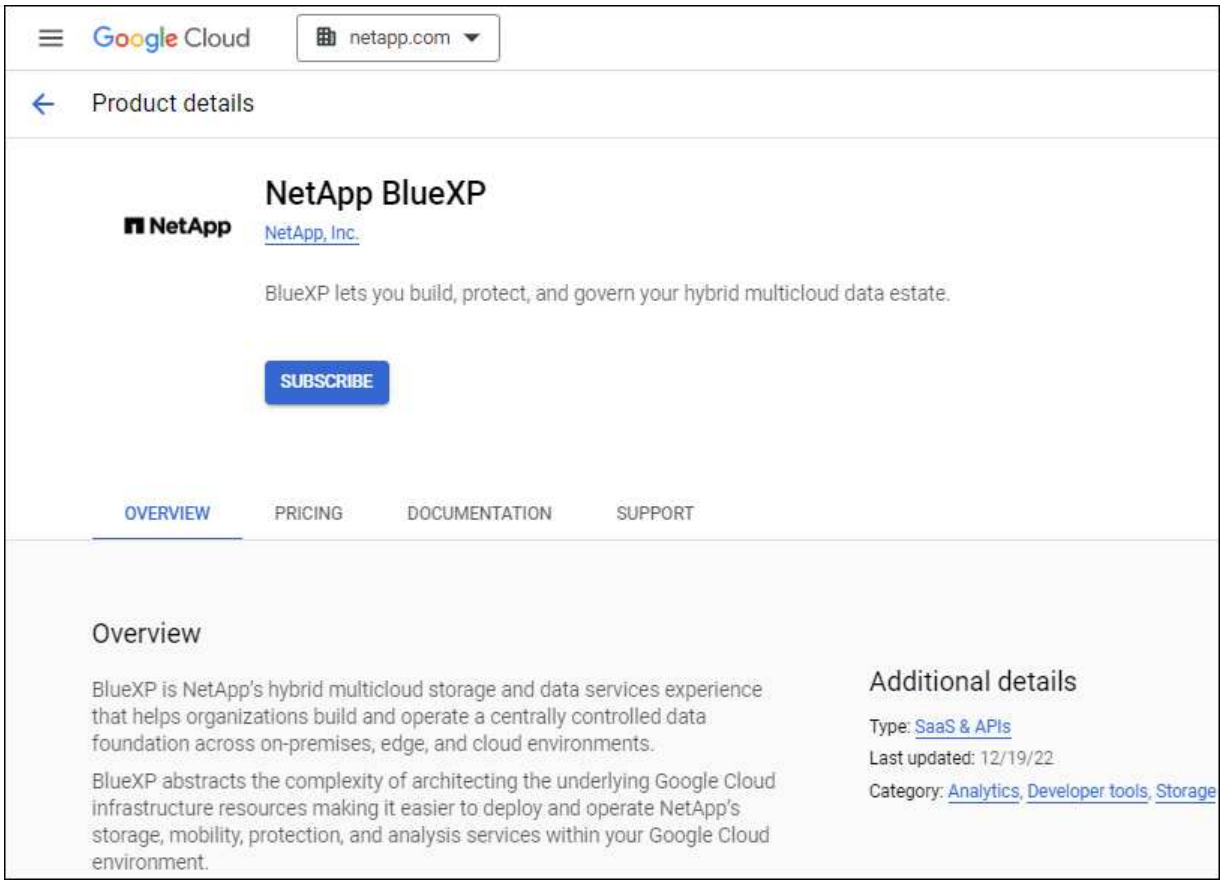
4. Um ein vorhandenes Abonnement mit den ausgewählten Anmeldeinformationen zu konfigurieren, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Dropdown-Liste aus und wählen Sie dann **Konfigurieren**.



5. 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.

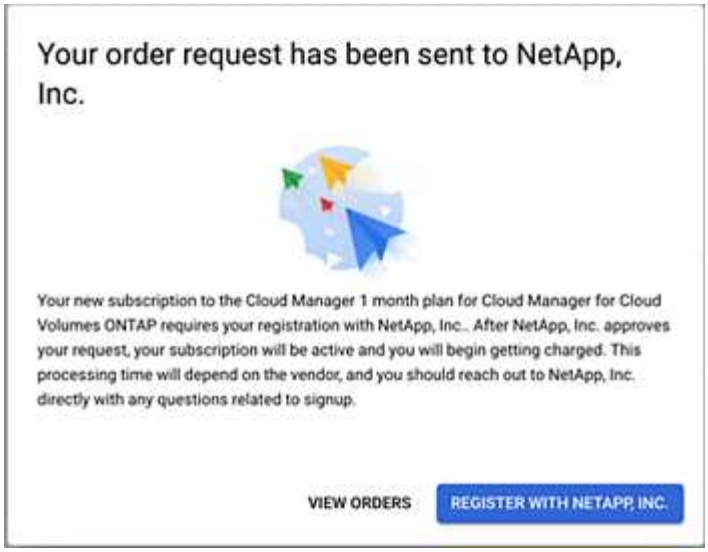


b. Wählen Sie **Abonnieren**.
c. Wählen Sie das entsprechende Abrechnungskonto aus und stimmen Sie den Allgemeinen Geschäftsbedingungen zu.
d. Wählen Sie **Abonnieren**.

   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 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.

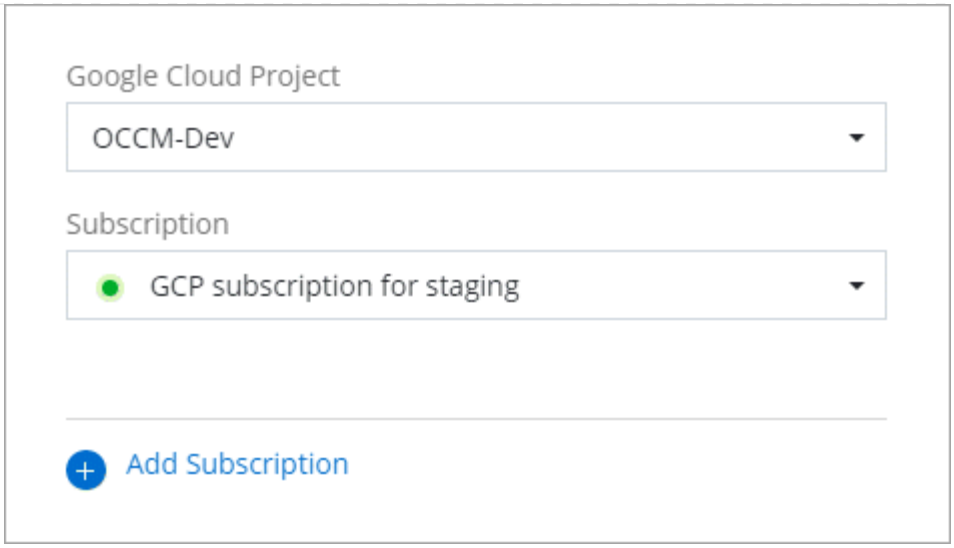
Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.

- Wählen Sie **Speichern**.

  Das folgende Video zeigt die Schritte zum Abonnieren vom Google Cloud Marketplace:

Abonnieren Sie über den Google Cloud Marketplace

a. 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"

Erste Schritte mit der BlueXP -Legacy-Schnittstelle (privater 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-Schutz	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

Verwenden Sie die NetApp Console

Melden Sie sich bei der NetApp Console an

Wie Sie sich bei der NetApp Console anmelden, hängt davon ab, welchen Bereitstellungsmodus Sie verwenden.

Sie werden nach 24 Stunden oder beim Schließen Ihres Browsers automatisch abgemeldet.

"Informationen zu den Bereitstellungsmodi der Konsole" .

Standardmodus

Nachdem Sie sich bei der NetApp Console angemeldet haben, können Sie sich von der webbasierten Konsole aus anmelden, um mit der Verwaltung Ihrer Daten- und Speicherinfrastruktur zu beginnen.

Informationen zu diesem Vorgang

Sie können sich mit einer der folgenden Optionen bei der NetApp Console anmelden:

- Ihre vorhandenen Anmeldeinformationen für die NetApp Support Site (NSS)
- Ein NetApp Console mit Ihrer E-Mail-Adresse und einem Passwort
- Eine Verbundverbindung

  Sie können Single Sign-On verwenden, um sich mit den Anmeldeinformationen aus Ihrem Unternehmensverzeichnis anzumelden (föderierte Identität). "Erfahren Sie, wie Sie eine Identitätsföderation einrichten" .

Schritte

1. Öffnen Sie einen Webbrowser und gehen Sie zu "NetApp Console"
2. Geben Sie auf der Seite **Anmelden** die E-Mail-Adresse ein, die mit Ihrem Login verknüpft ist.
3. Abhängig von der mit Ihrer Anmeldung verknüpften Authentifizierungsmethode werden Sie aufgefordert, Ihre Anmeldeinformationen einzugeben:
   - NetApp Cloud-Anmeldeinformationen: Geben Sie Ihr Passwort ein
   - Verbundbenutzer: Geben Sie Ihre Verbundidentitäts-Anmeldeinformationen ein
   - NetApp Support Site-Konto: Geben Sie Ihre NetApp Support Site-Anmeldeinformationen ein

Ergebnis

Sie sind jetzt angemeldet und können mit der Verwaltung Ihrer hybriden Multi-Cloud-Infrastruktur beginnen.

Eingeschränkter Modus

Wenn Sie die Konsole im eingeschränkten Modus verwenden, müssen Sie sich über die Benutzeroberfläche, die lokal auf dem Agenten ausgeführt wird, bei der Konsole anmelden.

Informationen zu diesem Vorgang

Die Konsole unterstützt im eingeschränkten Modus die Anmeldung mit einer der folgenden Optionen:

- Eine NetApp Console mit Ihrer E-Mail-Adresse und einem Passwort
- Eine Verbundverbindung

  Sie können Single Sign-On verwenden, um sich mit den Anmeldeinformationen aus Ihrem Unternehmensverzeichnis anzumelden (föderierte Identität). "Erfahren Sie, wie Sie die Identitätsföderation nutzen" .

Schritte

1. Öffnen Sie einen Webbrowser und geben Sie die IP-Adresse ein, unter der der Agent installiert ist.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein, um sich anzumelden.

Anzeigen von Metriken auf der Startseite der NetApp Console

Durch die Überwachung des Zustands Ihres Speicherbestands wird sichergestellt, dass Sie über Probleme mit dem Speicherschutz informiert sind und Schritte zu deren Lösung unternehmen können. Zeigen Sie auf der Startseite der NetApp Console den Status Ihrer Sicherungen und Wiederherstellungen von NetApp Backup and Recovery sowie die Anzahl der Workloads an, die einem Ransomware-Angriff ausgesetzt sind oder gemäß NetApp Ransomware Resilience geschützt sind. Sie können die Speicherkapazität für einzelne Cluster und Cloud Volumes ONTAP, ONTAP Warnmeldungen, die Speicherleistungskapazität pro Cluster oder Cloud Volumes ONTAP System, die verschiedenen Arten Ihrer Lizenzen und mehr überprüfen.

Alle Bereiche auf der Startseite zeigen Daten auf Organisationsebene. In den Bereichen „Speicherkapazität“ und „Speicherleistung“ werden mit Projekten verknüpfte Systeme angezeigt, auf die der Benutzer basierend auf IAM-Berechtigungen zugreifen kann.

Das System aktualisiert die Daten auf der Startseite alle fünf Minuten. Durch das Caching können die Daten auf dieser Seite bis zu 15 Minuten lang von den tatsächlichen Werten abweichen.

Für genaue Messwerte auf der Startseite sind entsprechend dimensionierte und konfigurierte Konsolenagenten erforderlich.

Erforderliche NetApp Console

Jeder Bereich auf der Startseite erfordert unterschiedliche Benutzerrollen:

- **Speicherkapazitätsbereich**: Möglichkeit, die Seite „NetApp Console Konsolensysteme“ anzuzeigen
- * ONTAP -Warnbereich*: Ordner- oder Projektadministrator, Operations Support Analyst, Organisationsadministrator, Organisationsbetrachter, Superadministrator, Superbetrachter
- **Speicherleistungskapazitätsbereich**: Möglichkeit, die Seite „NetApp Console Konsolensysteme“ anzuzeigen
- * Bereich „Licenses and subscriptions“ *: Ordner- oder Projektadministrator, Organisationsadministrator, Organisationsbetrachter, Superadministrator, Superbetrachter
- **Ransomware-Resilience-Bereich**: Ordner- oder Projektadministrator, Organisationsadministrator, Ransomware-Resilience-Administrator, Ransomware-Resilience-Viewer, Superadministrator, Super-Viewer
- **Bereich „Backup und Wiederherstellung“**: Backup- und Wiederherstellungs-Backup-Administrator, Super-Admin für Backup und Wiederherstellung, Backup- und Wiederherstellungs-Backup-Viewer, Backup- und Wiederherstellungs-Klon-Administrator, Ordner- oder Projekt-Administrator, Organisations-Administrator, Backup- und Wiederherstellungs-Wiederherstellungs-Administrator, Super-Admin, Super-Viewer

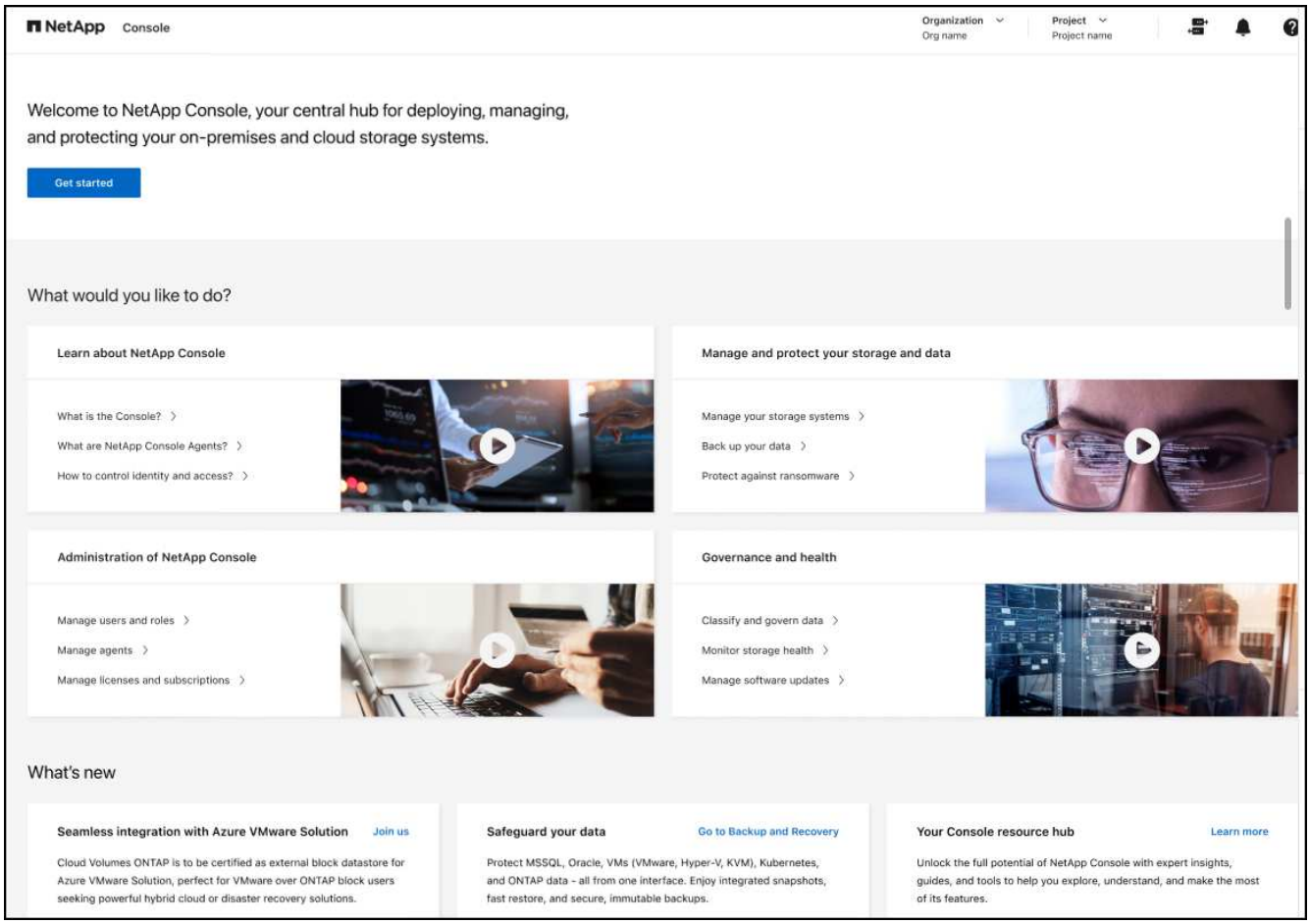
Wenn Sie nicht über die Berechtigung zum Zugriff auf einen Bereich verfügen, wird in dem Bereich eine Meldung angezeigt, die darauf hinweist, dass Ihnen die Berechtigung zur Verwendung des Bereichs fehlt.

"Informieren Sie sich über die Zugriffsrollen der NetApp Console ." .

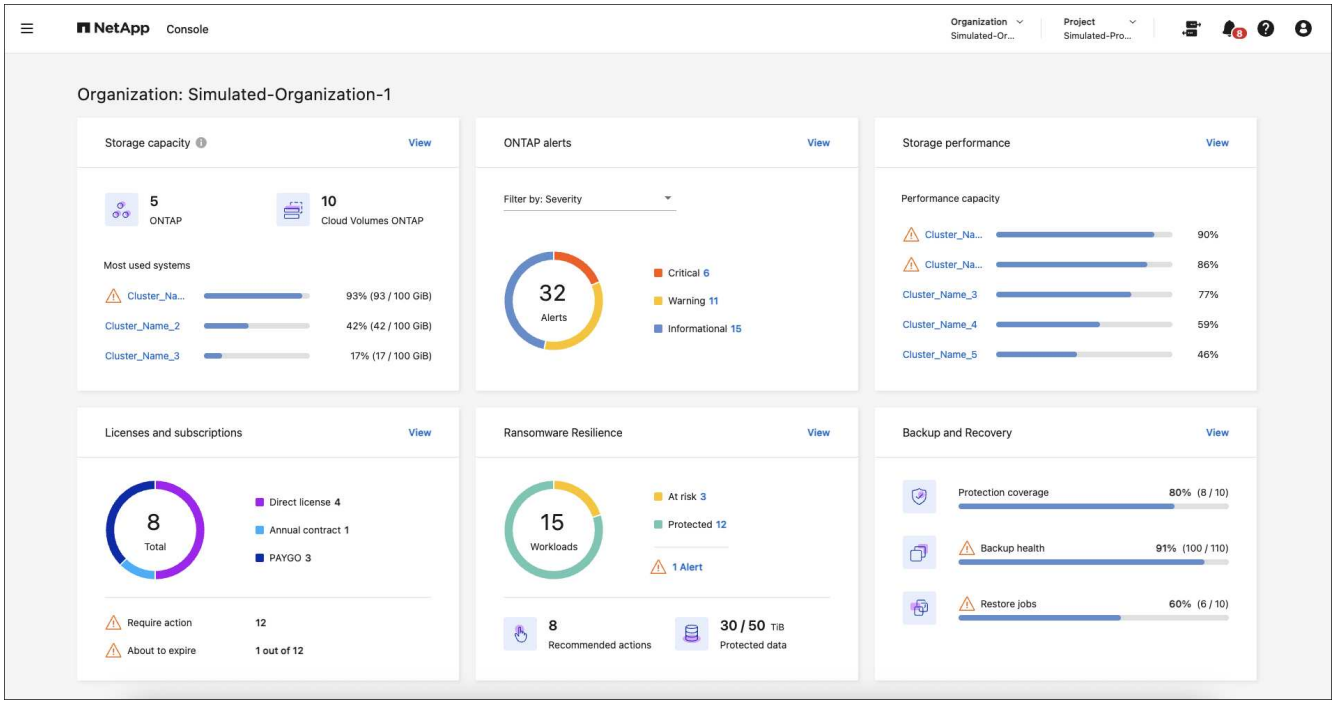
Schritte

1. Wählen Sie im NetApp Console **Home** aus.

   Wenn Sie über die Rolle des Organisationsadministrators verfügen und kein Agent oder Speichersystem eingerichtet ist, werden auf der Startseite Informationen zu den ersten Schritten angezeigt.



   Wenn Sie die NetApp Console bereits eingerichtet haben, mindestens ein Konsolenagent aktiviert ist und mindestens ein Cluster oder Cloud Volumes ONTAP System auf diesem Agenten hinzugefügt wurde, werden auf der Startseite Kennzahlen zu Ihrer Speicherumgebung angezeigt.



Aktivieren Sie die Anzeige von Metriken auf der Startseite

Sie können Metriken auf der Startseite sehen, wenn die folgenden Bedingungen erfüllt sind:

- Sie sind bei einer SaaS-Instanz der NetApp Console angemeldet.
- Sie gehören zu einer Organisation mit vorhandenen Speicherressourcen (Agent und Cluster oder Cloud Volumes ONTAP System).
- Mindestens ein Konsolenagent ist aktiviert.
- Auf diesem Agenten wurde mindestens ein Cluster oder Cloud Volumes ONTAP -System hinzugefügt.

Führen Sie die folgenden Aufgaben aus, um die Anzeige von Metriken auf der Startseite zu aktivieren:

- Aktivieren Sie mindestens einen Konsolenagenten.
- Fügen Sie mit diesem Agenten mindestens einen Cluster oder ein Cloud Volumes ONTAP hinzu.

Gesamtspeicherkapazität anzeigen

Der Bereich „Speicherkapazität“ bietet die folgenden Informationen zu ONTAP Clustern und Cloud Volumes ONTAP Systemen:

- Anzahl der in der Konsole erkannten ONTAP -Systeme
- Anzahl der in der Konsole erkannten Cloud Volumes ONTAP -Systeme
- Kapazitätsnutzung pro Cluster

Die Reihenfolge der Cluster bzw. Cloud Volumes ONTAP -Systeme richtet sich nach der genutzten Kapazität. Zur einfachen Identifizierung wird der Cluster oder das System mit der höchsten Kapazität zuerst angezeigt.

Warnanzeigen werden für Cluster mit 80 % Kapazität angezeigt, wobei die Daten alle fünf Minuten aktualisiert werden.

Wenn Sie mehrere Projekte haben, werden im Bereich „Speicherkapazität“ möglicherweise andere Daten angezeigt als auf der Seite „Systeme“. Dies liegt daran, dass auf der Seite „Systeme“ Informationen auf Projektebene angezeigt werden, während im Bereich „Speicherkapazität“ Informationen auf Organisationsebene angezeigt werden. Außerdem können die Daten in diesem Bereich maximal 15 Minuten lang von den tatsächlichen Werten abweichen, da die Daten für diesen Zeitraum zwischengespeichert werden, um die Leistung zu optimieren.

Schritte

1. Überprüfen Sie im NetApp Console den Bereich „Speicherkapazität“.
2. Wählen Sie im Bereich „Speicherkapazität“ **Anzeigen** aus, um zur Seite „Konsolensysteme“ zu gelangen.
3. Wählen Sie auf der Seite „Systeme“ das Projekt aus, das den Cluster enthält, den Sie anzeigen möchten.
4. Wählen Sie auf der Seite „Systeme“ einen Cluster aus, um weitere Details zu diesem Cluster anzuzeigen.

ONTAP Warnmeldungen anzeigen

Zeigen Sie Probleme oder potenzielle Risiken in Ihren lokalen NetApp ONTAP Umgebungen an. Sie können einige Nicht-EMS-Warnungen und einige EMS-Warnungen sehen.

Die Daten werden alle 5 Minuten aktualisiert.

Sie können ONTAP -Warnmeldungen mit diesen Schweregraden sehen:

- Kritisch
- Warnung
- Informativ

Sie können ONTAP -Warnmeldungen für diese betroffenen Bereiche sehen:

- Kapazität
- Performance
- Schutz
- Verfügbarkeit
- Sicherheit

Durch das Zwischenspeichern wird die Leistung optimiert, es kann jedoch dazu führen, dass die Daten in diesem Bereich bis zu 15 Minuten lang von den tatsächlichen Werten abweichen.

Unterstützte Systeme

- Ein lokales ONTAP NAS- oder SAN-System wird unterstützt.
- Cloud Volumes ONTAP -Systeme werden nicht unterstützt.

Unterstützte Datenquellen

Zeigen Sie Warnungen zu bestimmten Ereignissen an, die in ONTAP auftreten. Sie sind eine Kombination aus EMS- und metrischen Warnungen.

Weitere Informationen zu ONTAP -Warnmeldungen finden Sie unter "Informationen zu ONTAP

-Warnmeldungen" .

Eine Liste der möglicherweise angezeigten Warnmeldungen finden Sie unter "Mögliche Risiken im ONTAP -Speicher anzeigen" .

Schritte

1. Überprüfen Sie im NetApp Console den Bereich „ONTAP -Warnmeldungen“.
2. Filtern Sie die Warnungen optional, indem Sie den Schweregrad auswählen, oder ändern Sie den Filter, um Warnungen basierend auf dem Auswirkungsbereich anzuzeigen.
3. Wählen Sie im Bereich „ONTAP -Warnmeldungen“ die Option „Anzeigen“ aus, um zur Seite „Konsolenwarnungen“ zu gelangen.

Anzeigen der Speicherleistungskapazität

Überprüfen Sie die pro Cluster oder Cloud Volumes ONTAP System verwendete Speicherleistungskapazität, um festzustellen, wie sich Leistungskapazität, Latenz und IOPS auf Ihre Workloads auswirken. Beispielsweise stellen Sie möglicherweise fest, dass Sie Workloads verschieben müssen, um die Latenz zu minimieren und IOPS und Durchsatz für Ihre kritischen Workloads zu maximieren.

Das System ordnet Cluster und Systeme nach Leistungskapazität an und listet zur einfachen Identifizierung die Systeme mit der höchsten Kapazität zuerst auf.

Durch das Zwischenspeichern wird die Leistung optimiert, es kann jedoch dazu führen, dass die Daten in diesem Bereich bis zu 15 Minuten lang von den tatsächlichen Werten abweichen.

Schritte

1. Überprüfen Sie im NetApp Console den Bereich „Speicherleistung“.
2. Wählen Sie im Bereich „Speicherleistung“ **Anzeigen** aus, um zu einer Leistungsseite zu gelangen, auf der alle Cluster- und Cloud Volumes ONTAP -Systemdaten hinsichtlich Leistungskapazität, IOPS und Latenz aufgelistet sind.
3. Wählen Sie einen Cluster aus, um seine Details im System Manager anzuzeigen.

Zeigen Sie die Lizenzen und Abonnements an, die Sie haben

Überprüfen Sie die folgenden Informationen im Bereich „Licenses and subscriptions“ :

- Die Gesamtzahl Ihrer Lizenzen und Abonnements.
- Die Anzahl der einzelnen Lizenz- und Abonnementtypen, die Sie besitzen (Direktlizenz, Jahresvertrag oder PAYGO).
- Die Anzahl der Lizenzen und Abonnements, die aktiv sind, Maßnahmen erfordern oder bald ablaufen.
- Das System zeigt Indikatoren neben den Lizenztypen an, bei denen Maßnahmen erforderlich sind oder die bald ablaufen.

Die Daten werden alle 5 Minuten aktualisiert.

Durch das Zwischenspeichern wird die Leistung optimiert, es kann jedoch dazu führen, dass die Daten in diesem Bereich bis zu 15 Minuten lang von den tatsächlichen Werten abweichen.

Schritte

1. Überprüfen Sie im NetApp Console den Bereich „Licenses and subscriptions“ .
2. Wählen Sie im Bereich „Licenses and subscriptions“ die Option „Anzeigen“ aus, um zur Seite „Konsolenlizenzen und Licenses and subscriptions“ zu gelangen.

Ransomware-Resilienzstatus anzeigen

Finden Sie mit dem NetApp Ransomware Resilience -Datendienst heraus, ob Workloads einem Risiko durch Ransomware-Angriffe ausgesetzt sind oder geschützt sind. Sie können die Gesamtmenge der geschützten Daten überprüfen, die Anzahl der empfohlenen Aktionen anzeigen und die Anzahl der Warnungen im Zusammenhang mit dem Ransomware-Schutz einsehen.

Die Daten werden alle 5 Minuten aktualisiert und stimmen mit den im NetApp Ransomware Resilience Dashboard angezeigten Daten überein.

"Erfahren Sie mehr über NetApp Ransomware Resilience" .

Schritte

1. Überprüfen Sie im NetApp Console den Bereich „Ransomware-Resilienz“.
2. Führen Sie im Bereich „Ransomware-Resilienz“ einen der folgenden Schritte aus:
   - Wählen Sie **Anzeigen**, um zum NetApp Ransomware Resilience Dashboard zu gelangen. Weitere Einzelheiten finden Sie unter "Überwachen Sie den Workload-Zustand mit dem NetApp Ransomware Resilience Dashboard" .
   - Lesen Sie die „Empfohlenen Maßnahmen“ im NetApp Ransomware Resilience Dashboard. Weitere Einzelheiten finden Sie unter "Überprüfen Sie die Schutzempfehlungen im NetApp Ransomware Resilience Dashboard" .
   - Wählen Sie den Warnlink aus, um Warnmeldungen auf der Seite „NetApp Ransomware Resilience Alerts“ zu überprüfen. Weitere Einzelheiten finden Sie unter "Behandeln Sie erkannte Ransomware-Warnmeldungen mit NetApp Ransomware Resilience" .

Anzeigen des Sicherungs- und Wiederherstellungsstatus

Überprüfen Sie den Gesamtstatus Ihrer Backups und Wiederherstellungen von NetApp Backup and Recovery. Sie können die Anzahl der geschützten und ungeschützten Ressourcen sehen. Sie können auch den Prozentsatz der Sicherungs- und Wiederherstellungsvorgänge zum Schutz Ihrer Workloads sehen. Ein höherer Prozentsatz weist auf einen verbesserten Datenschutz hin.

Die Daten werden alle 5 Minuten aktualisiert.

Durch das Zwischenspeichern wird die Leistung optimiert, es kann jedoch dazu führen, dass die Daten in diesem Bereich bis zu 15 Minuten lang von den tatsächlichen Werten abweichen.

Schritte

1. Überprüfen Sie im NetApp Console den Bereich „Backup und Wiederherstellung“.
2. Wählen Sie **Anzeigen**, um zum NetApp Backup and Recovery Dashboard zu gelangen. Weitere Einzelheiten finden Sie unter "NetApp Backup and Recovery -Dokumentation" .

Verwalten Sie Ihre NetApp Console

Sie können Ihr Konsolenprofil ändern, einschließlich der Änderung Ihres Kennworts, die

Aktivierung der Multi-Faktor-Authentifizierung (MFA) und sehen, wer Ihr Konsolenadministrator ist.

Innerhalb der Konsole verfügt jeder Benutzer über ein Profil, das Informationen über den Benutzer und seine Einstellungen enthält. Sie können Ihre Profileinstellungen anzeigen und bearbeiten.

Ändern Sie Ihren Anzeigenamen

Sie können den Anzeigenamen Ihrer Konsole ändern, der zu Ihrer Identifizierung dient und für andere Benutzer sichtbar ist. Ihr Anzeigename ist nicht identisch mit Ihrem Benutzernamen oder Ihrer E-Mail-Adresse und kann nicht geändert werden.

Schritte

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke der Konsole aus, um das Bedienfeld „Benutzereinstellungen“ anzuzeigen.
2. Wählen Sie das Symbol **Bearbeiten** neben Ihrem Namen.
3. Geben Sie Ihren neuen Anzeigenamen in das Feld **Name** ein.

Konfigurieren der mehrstufigen Authentifizierung

Konfigurieren Sie die Multi-Faktor-Authentifizierung (MFA), um die Sicherheit durch die Anforderung einer zweiten Überprüfungsmethode zu verbessern.

Benutzer, die Single Sign-On mit einem externen Identitätsanbieter oder der NetApp -Support-Site verwenden, können MFA nicht aktivieren. Wenn einer dieser Punkte auf Sie zutrifft, wird die Option zum Aktivieren von MFA in Ihren Profileinstellungen nicht angezeigt.

Aktivieren Sie MFA nicht, wenn Ihr Benutzerkonto für den API-Zugriff verwendet wird. Die Multi-Faktor-Authentifizierung stoppt den API-Zugriff, wenn sie für ein Benutzerkonto aktiviert ist. Verwenden Sie Dienstkonten für den gesamten API-Zugriff.

Bevor Sie beginnen

- Sie müssen bereits eine Authentifizierungs-App wie Google Authenticator oder Microsoft Authenticator auf Ihr Gerät heruntergeladen haben.
- Sie benötigen Ihr Passwort, um MFA einzurichten.

> Wenn Sie keinen Zugriff auf Ihre Authentifizierungs-App haben oder Ihren Wiederherstellungscode verlieren, wenden Sie sich an Ihren Konsolenadministrator, um Hilfe zu erhalten.

Schritte

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke der Konsole aus, um das Bedienfeld „Benutzereinstellungen“ anzuzeigen.
2. Wählen Sie neben der Überschrift **Multi-Faktor-Authentifizierung Konfigurieren** aus.
3. Folgen Sie den Anweisungen, um MFA für Ihr Konto einzurichten.
4. Wenn Sie fertig sind, werden Sie aufgefordert, Ihren Wiederherstellungscode zu speichern. Wählen Sie, ob Sie den Code kopieren oder eine Textdatei mit dem Code herunterladen möchten. Bewahren Sie diesen Code an einem sicheren Ort auf. Sie benötigen den Wiederherstellungscode, wenn Sie den Zugriff auf Ihre Authentifizierungs-App verlieren.

Nachdem Sie MFA eingerichtet haben, werden Sie von der Konsole bei jeder Anmeldung aufgefordert, einen Einmalcode aus Ihrer Authentifizierungs-App einzugeben.

MFA-Wiederherstellungscode neu generieren

Sie können Wiederherstellungscodes nur einmal verwenden. Wenn Sie Ihr Konto verwenden oder verlieren, erstellen Sie ein neues.

Schritte

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke der Konsole aus, um das Bedienfeld „Benutzereinstellungen“ anzuzeigen.
2. Wählen ••• neben der Überschrift **Multi-Faktor-Authentifizierung**.
3. Wählen Sie **Wiederherstellungscode neu generieren**.
4. Kopieren Sie den generierten Wiederherstellungscode und speichern Sie ihn an einem sicheren Ort.

Löschen Sie Ihre MFA-Konfiguration

Um die Verwendung der Multi-Faktor-Authentifizierung (MFA) für Ihre Anmeldung zu beenden, löschen Sie Ihre MFA-Konfiguration. Dadurch entfällt die Notwendigkeit, beim Anmelden einen Einmalcode aus Ihrer Authentifizierungs-App einzugeben.

Wenn Sie nicht auf Ihre Authentifizierungs-App oder Ihren Wiederherstellungscode zugreifen können, müssen Sie sich an Ihren Organisationsadministrator wenden, um Ihre MFA-Konfiguration zurückzusetzen.

Schritte

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke der Konsole aus, um das Bedienfeld „Benutzereinstellungen“ anzuzeigen.
2. Wählen ••• neben der Überschrift **Multi-Faktor-Authentifizierung**.
3. Wählen Sie **Löschen**.

Wenden Sie sich an den Administrator Ihrer Organisation

Wenn Sie den Administrator Ihrer Organisation kontaktieren müssen, können Sie ihm direkt von der Konsole aus eine E-Mail senden. Der Administrator verwaltet Benutzerkonten und Berechtigungen innerhalb Ihrer Organisation.

Um die Funktion **Administratoren kontaktieren** verwenden zu können, muss für Ihren Browser eine Standard-E-Mail-Anwendung konfiguriert sein.

Schritte

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke der Konsole aus, um das Bedienfeld „Benutzereinstellungen“ anzuzeigen.
2. Wählen Sie **Administratoren kontaktieren** aus, um eine E-Mail an den Administrator Ihrer Organisation zu senden.
3. Wählen Sie die zu verwendende E-Mail-Anwendung aus.
4. Beenden Sie die E-Mail und wählen Sie **Senden**.

Dunkelmodus konfigurieren (dunkles Design)

Sie können die Konsole so einstellen, dass sie im Dunkelmodus angezeigt wird.

Schritte

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke der Konsole aus, um das Bedienfeld „Benutzereinstellungen“ anzuzeigen.
2. Bewegen Sie den Schieberegler **Dunkles Design**, um es zu aktivieren.

NetApp Console verwalten

Identitäts- und Zugriffsverwaltung

Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der NetApp Console

Mit Identity and Access Management (IAM) in der NetApp Console können Sie den Zugriff auf Ihre NetApp -Ressourcen organisieren und steuern. Sie können Ihre Ressourcen entsprechend der Hierarchie Ihrer Organisation organisieren. Sie können Ressourcen beispielsweise nach geografischem Standort, Standort oder Geschäftseinheit organisieren. Anschließend können Sie Mitgliedern in bestimmten Teilen der Hierarchie IAM-Rollen zuweisen, wodurch der Zugriff auf Ressourcen in anderen Teilen der Hierarchie verhindert wird.

- "Informationen zu den Bereitstellungsmodi der Konsole"

So funktioniert IAM

Mit IAM können Sie Ressourcenzugriff gewähren, indem Sie Benutzern Zugriffsrollen für bestimmte Teile der Hierarchie zuweisen. Beispielsweise kann einem Mitglied die Rolle des Ordner- oder Projektadministrators für ein Projekt mit fünf Ressourcen zugewiesen werden.

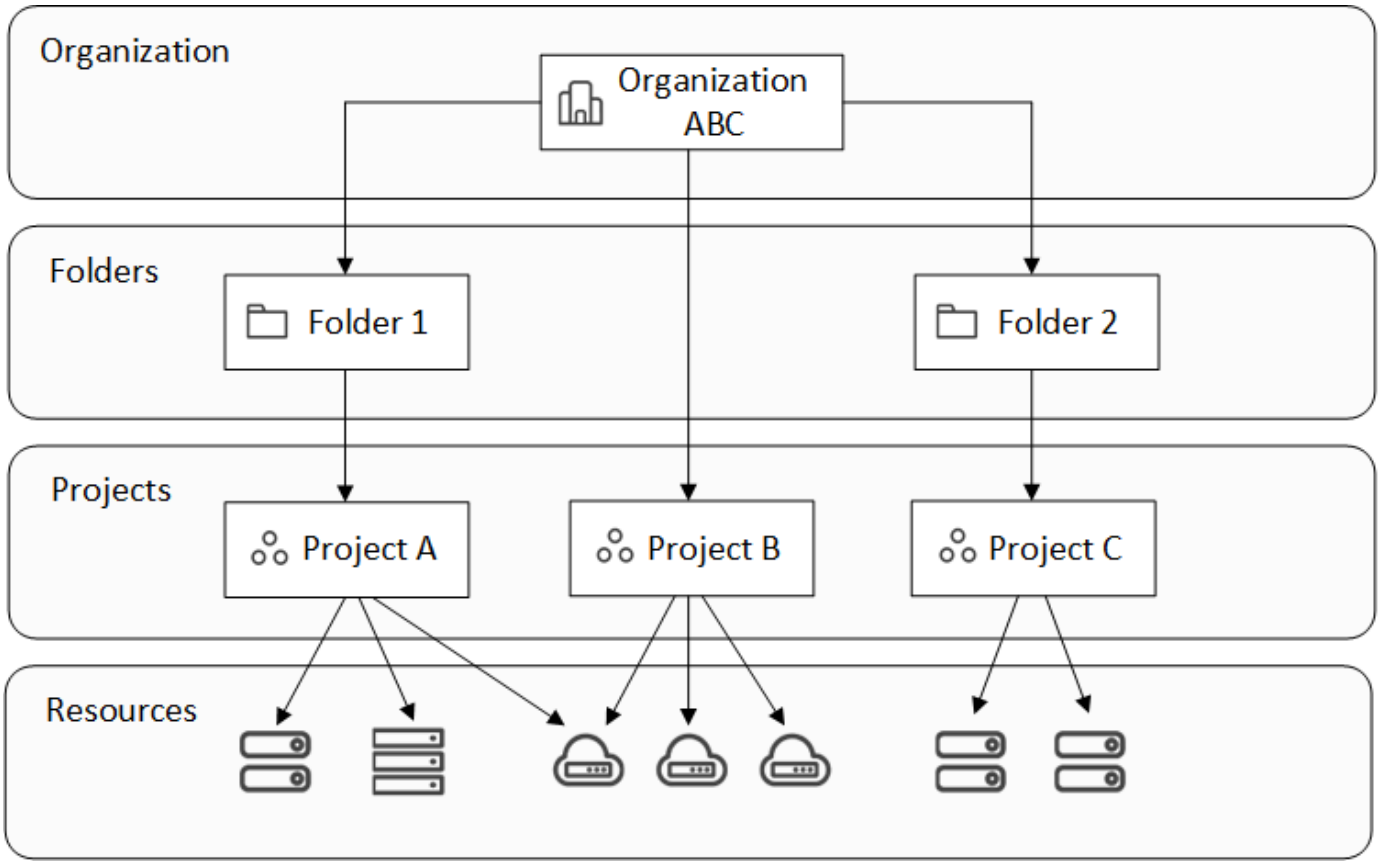
Bei der Verwendung von IAM verwalten Sie die folgenden Komponenten:

- Die Organisation
- Ordner
- Projekte
- Ressourcen
- Mitglieder
- Rollen und Berechtigungen
- Konsolenagenten

Ressourcen sind hierarchisch organisiert:

- Die Organisation steht an der Spitze der Hierarchie.
- Ordner sind untergeordnete Elemente der Organisation oder eines anderen Ordners.
- Projekte sind untergeordnete Elemente der Organisation oder eines Ordners.
- Ressourcen sind mit einem oder mehreren Ordnern oder Projekten verknüpft.

Das folgende Bild veranschaulicht diese Hierarchie auf einer grundlegenden Ebene.



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.

Ordner

Ein *Ordner* ermöglicht es Ihnen, verwandte Projekte zu gruppieren und sie von anderen Projekten in Ihrer Organisation zu trennen. Ein Ordner kann beispielsweise einen geografischen Standort (EU oder US-Ost), einen Standort (London oder Toronto) oder eine Geschäftseinheit (Technik oder Marketing) darstellen.

Sie können Ordner so organisieren, dass sie Projekte, andere Ordner oder beides enthalten. Sie sind optional.

Projekte

Ein *Projekt* stellt einen Arbeitsbereich in der Konsole dar, auf den Mitglieder der Organisation von der Seite **Systeme** aus zugreifen, um Ressourcen zu verwalten. Ein Projekt kann beispielsweise ein Cloud Volumes ONTAP -System, einen lokalen ONTAP Cluster oder ein FSx für ONTAP Dateisystem umfassen.

Eine Organisation kann ein oder mehrere Projekte haben. Ein Projekt kann sich direkt unter der Organisation oder in einem Ordner befinden.

Ressourcen

Eine *Ressource* ist ein System, das Sie in der Konsole erstellt oder entdeckt haben.

Wenn Sie eine Ressource erstellen oder entdecken, wird die Ressource mit dem aktuell ausgewählten Projekt verknüpft. Dies ist möglicherweise das einzige Projekt, mit dem Sie diese Ressource verknüpfen möchten. Sie

können die Ressource jedoch auch mit weiteren Projekten in Ihrer Organisation verknüpfen.

Sie können beispielsweise ein Cloud Volumes ONTAP -System mit einem zusätzlichen Projekt oder mit allen Projekten in Ihrer Organisation verknüpfen. Wie Sie eine Ressource zuordnen, hängt von den Anforderungen Ihrer Organisation ab.

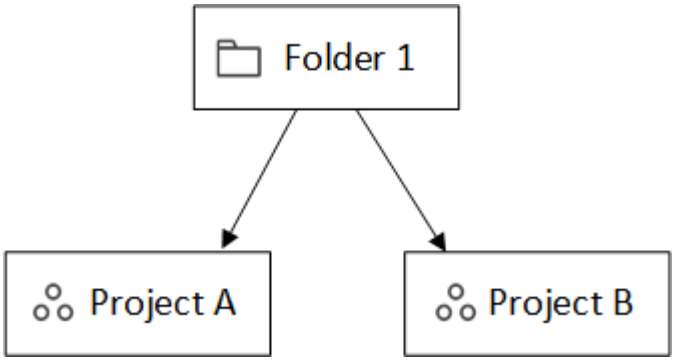
Agenten können auch mehr als einem Projekt zugeordnet werden. Erfahren Sie mehr über die Verwendung von Agenten mit IAM .

Wann sollte eine Ressource einem Ordner zugeordnet werden?

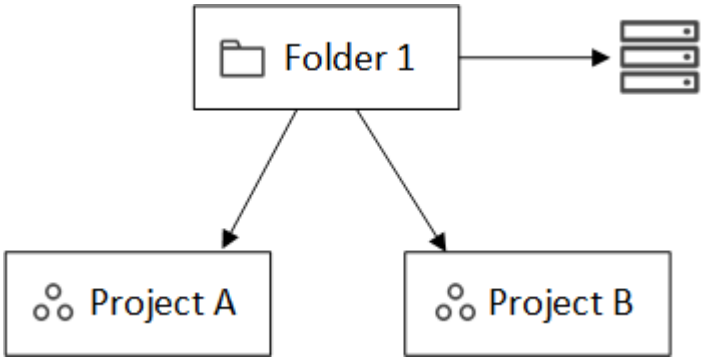
Sie haben auch die Möglichkeit, eine Ressource mit einem Ordner zu verknüpfen. Dies ist jedoch optional und dient den Anforderungen eines bestimmten Anwendungsfalls.

Ein *Organisationsadministrator* kann eine Ressource mit einem Ordner verknüpfen, sodass ein *Ordner- oder Projektadministrator* sie mit den entsprechenden Projekten im Ordner verknüpfen kann.

Nehmen wir beispielsweise an, Sie haben einen Ordner, der zwei Projekte enthält:

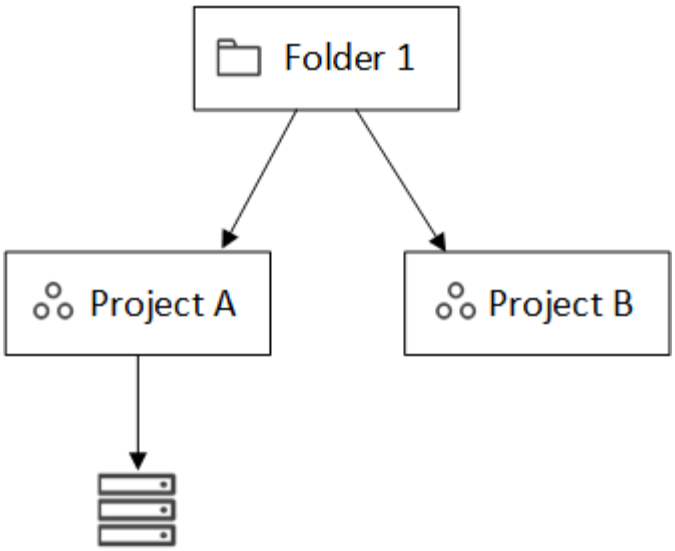


Der *Organisationsadministrator* kann eine Ressource mit dem Ordner verknüpfen:



Durch die Verknüpfung einer Ressource mit einem Ordner wird diese nicht für alle Projekte zugänglich; nur der Ordner- oder Projektadministrator kann sie sehen. Der *Ordner- oder Projektadministrator* entscheidet, welche Projekte darauf zugreifen können und ordnet die Ressource den entsprechenden Projekten zu.

In diesem Beispiel verknüpft der Administrator die Ressource mit Projekt A:



Mitglieder, die über Berechtigungen für Projekt A verfügen, können jetzt auf die Ressource zugreifen.

Mitglieder

Mitglieder Ihrer Organisation sind Benutzerkonten oder Dienstkonten. Ein Dienstkonto wird normalerweise von einer Anwendung verwendet, um bestimmte Aufgaben ohne menschliches Eingreifen abzuschließen.

Jede Organisation umfasst mindestens einen Benutzer mit der Rolle „Organisationsadministrator“ (die Konsole weist diese Rolle automatisch dem Benutzer zu, der die Organisation erstellt). Sie können der Organisation weitere Mitglieder hinzufügen und auf verschiedenen Ebenen der Ressourcenhierarchie unterschiedliche Berechtigungen zuweisen.

Rollen und Berechtigungen

Sie erteilen den Mitgliedern der Organisation keine Berechtigungen direkt. Stattdessen weisen Sie jedem Mitglied eine Rolle zu. Eine Rolle enthält eine Reihe von Berechtigungen, die es einem Mitglied ermöglichen, bestimmte Aktionen auf einer bestimmten Ebene der Ressourcenhierarchie auszuführen.

Durch die Zuweisung von Rollen auf Hierarchieebene wird der Zugriff auf die Ressourcen und Dienste eingeschränkt, die ein Mitglied benötigt.

Wo Sie in der Hierarchie Rollen zuweisen können

Wenn Sie einem Mitglied eine Rolle zuordnen, müssen Sie die gesamte Organisation, einen bestimmten Ordner oder ein bestimmtes Projekt auswählen. Die von Ihnen ausgewählte Rolle erteilt einem Mitglied Berechtigungen für die Ressourcen im ausgewählten Teil der Hierarchie.

Rollenvererbung

Wenn Sie eine Rolle zuweisen, wird diese Rolle in der Organisationshierarchie nach unten vererbt:

Organisation
: Wenn Sie einem Mitglied eine Zugriffsrolle auf Organisationsebene erteilen, erhält es Berechtigungen für alle Ordner, Projekte und Ressourcen.

Ordner
: Wenn Sie eine Zugriffsrolle auf Ordnerebene erben, erben alle Ordner, Projekte und Ressourcen im Ordner

diese Rolle.

Wenn Sie beispielsweise eine Rolle auf Ordnerebene zuweisen und dieser Ordner drei Projekte enthält, verfügt das Mitglied über Berechtigungen für diese drei Projekte und alle zugehörigen Ressourcen.

Projekte

Wenn Sie eine Zugriffsrolle auf Projektebene erteilen, erben alle mit diesem Projekt verknüpften Ressourcen diese Rolle.

Mehrere Rollen

Sie können jedem Organisationsmitglied eine Rolle auf verschiedenen Ebenen der Organisationshierarchie zuweisen. Es kann sich um dieselbe oder eine andere Rolle handeln. Sie können beispielsweise für Projekt 1 und Projekt 2 eine Mitgliedsrolle A zuweisen. Oder Sie können einem Mitglied die Rolle A für Projekt 1 und die Rolle B für Projekt 2 zuweisen.

Zugriffsrollen

Die Konsole bietet Zugriffsrollen, die Sie den Mitgliedern Ihrer Organisation zuweisen können.

"Informationen zu Zugriffsrollen" .

Konsolenagenten

Wenn ein *Organisationsadministrator* einen Konsolenagenten erstellt, verknüpft die Konsole diesen Agenten automatisch mit der Organisation und dem aktuell ausgewählten Projekt. Der *Organisationsadministrator* hat automatisch von überall in der Organisation Zugriff auf diesen Agenten. Wenn es in Ihrer Organisation jedoch andere Mitglieder mit anderen Rollen gibt, können diese Mitglieder nur über das Projekt, in dem der Agent erstellt wurde, auf diesen Agenten zugreifen, es sei denn, Sie verknüpfen diesen Agenten mit anderen Projekten.

In den folgenden Fällen stellen Sie einen Konsolenagenten für ein anderes Projekt zur Verfügung:

- Sie möchten Mitgliedern Ihrer Organisation erlauben, einen vorhandenen Agenten zu verwenden, um zusätzliche Systeme in einem anderen Projekt zu erstellen oder zu entdecken
- Sie haben eine vorhandene Ressource mit einem anderen Projekt verknüpft und diese Ressource wird von einem Konsolenagenten verwaltet

  Wenn eine Ressource, die Sie mit einem zusätzlichen Projekt verknüpfen, mithilfe eines Konsolenagenten erkannt wird, müssen Sie den Agenten auch mit dem Projekt verknüpfen, mit dem die Ressource jetzt verknüpft ist. Andernfalls sind der Agent und die zugehörige Ressource von der Seite **Systeme** aus für Mitglieder, die nicht über die Rolle *Organisationsadministrator* verfügen, nicht zugänglich.

Sie können eine Zuordnung von der Seite **Agenten** innerhalb der IAM-Konsole aus erstellen:

- Verknüpfen Sie einen Konsolenagenten mit einem Projekt

  Wenn Sie einem Projekt einen Konsolenagenten zuordnen, ist dieser Agent beim Anzeigen des Projekts von der Seite **Systeme** aus zugänglich.

- Verknüpfen Sie einen Konsolenagenten mit einem Ordner

  Durch die Verknüpfung eines Konsolenagenten mit einem Ordner wird dieser Agent nicht automatisch von allen Projekten im Ordner aus zugänglich. Mitglieder der Organisation können nicht von einem Projekt aus

auf einen Konsolenagenten zugreifen, bis Sie den Agenten mit diesem bestimmten Projekt verknüpfen.

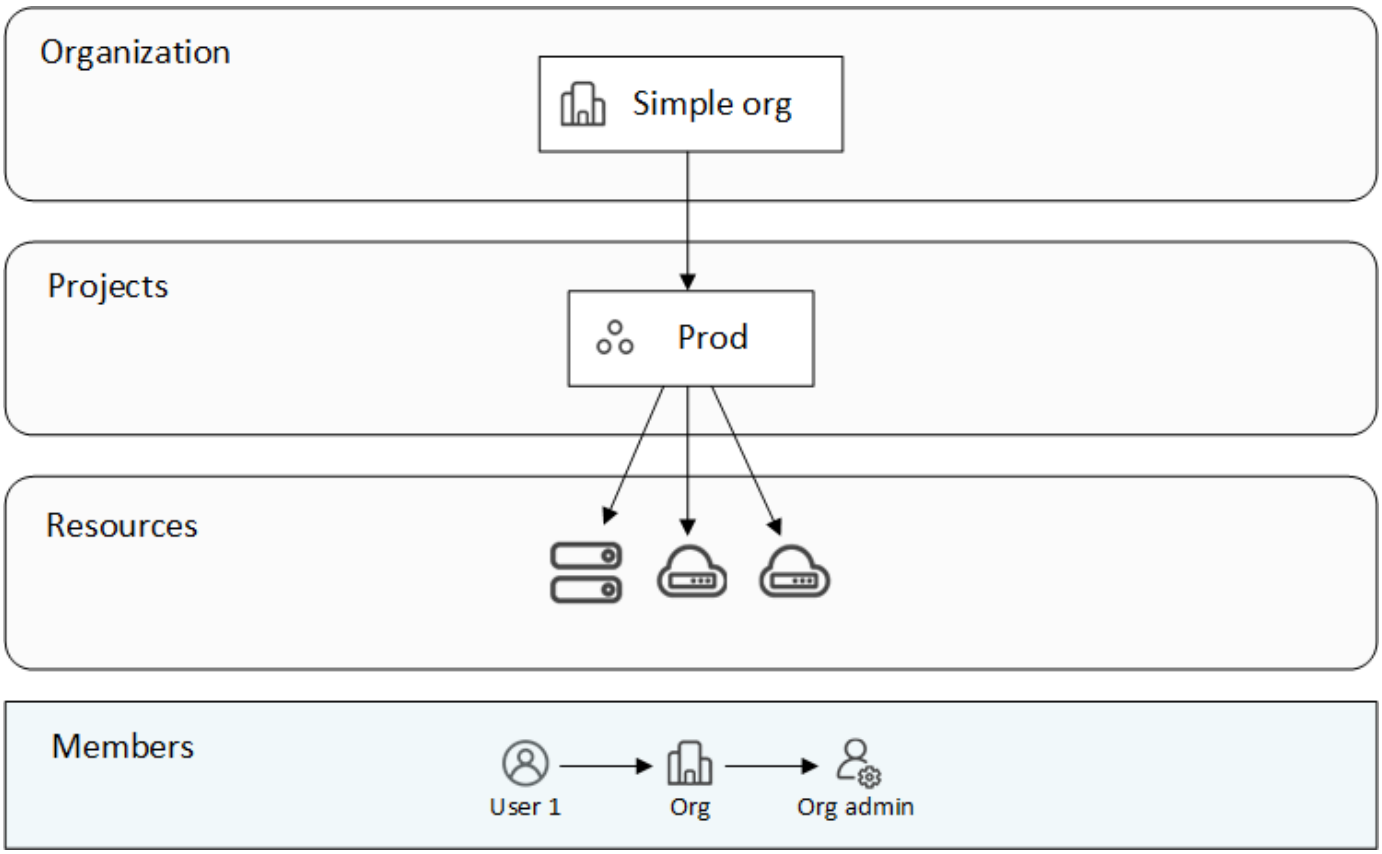
Ein *Organisationsadministrator* kann einen Konsolenagenten mit einem Ordner verknüpfen, sodass der *Ordner- oder Projektadministrator* die Entscheidung treffen kann, diesen Agenten mit den entsprechenden Projekten zu verknüpfen, die sich im Ordner befinden.

IAM-Beispiele

Diese Beispiele zeigen, wie Sie Ihre Organisation aufbauen könnten.

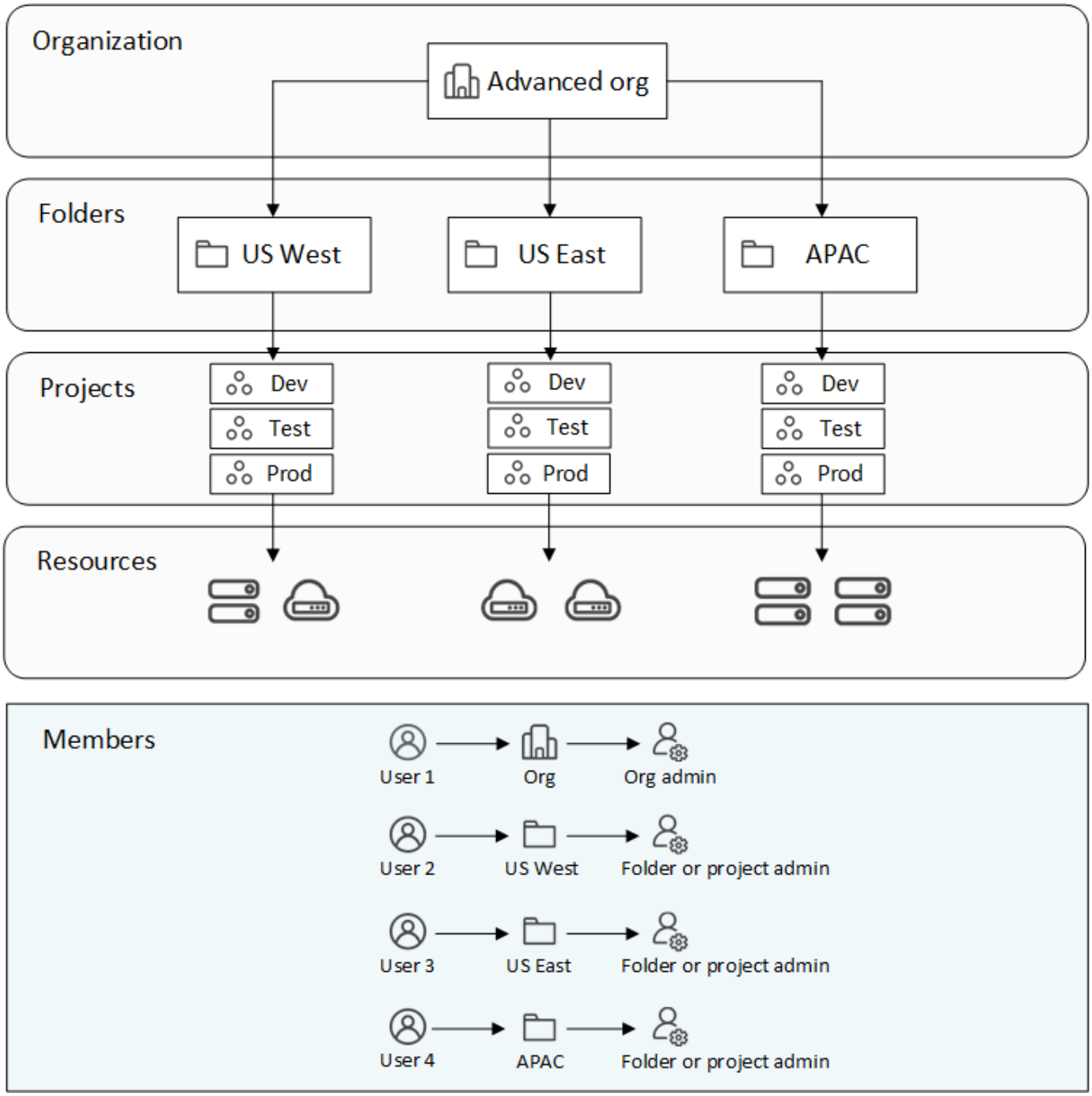
Einfache Organisation

Das folgende Diagramm zeigt ein einfaches Beispiel einer Organisation, die das Standardprojekt und keine Ordner verwendet. Ein einzelnes Mitglied verwaltet die gesamte Organisation.



Erweiterte Organisation

Das folgende Diagramm zeigt eine Organisation, die Ordner verwendet, um die Projekte für jeden geografischen Standort im Unternehmen zu organisieren. Jedes Projekt verfügt über einen eigenen Satz zugehöriger Ressourcen. Zu den Mitgliedern gehören ein Organisationsadministrator und ein Administrator für jeden Ordner in der Organisation.



Was Sie mit IAM tun können

Die folgenden Beispiele beschreiben, wie Sie IAM zum Verwalten Ihrer Konsolenorganisation verwenden können:

- Weisen Sie bestimmten Mitgliedern bestimmte Rollen zu, sodass sie nur die erforderlichen Aufgaben erledigen können.
- Ändern Sie die Berechtigungen von Mitgliedern, weil sie die Abteilung gewechselt haben oder zusätzliche Verantwortlichkeiten haben.
- Entfernen Sie einen Benutzer, der das Unternehmen verlassen hat.
- Fügen Sie Ihrer Hierarchie Ordner oder Projekte hinzu, weil eine neue Geschäftseinheit NetApp -Speicher hinzugefügt hat.

- Ordnen Sie eine Ressource einem anderen Projekt zu, da diese Ressource über Kapazitäten verfügt, die ein anderes Team nutzen kann.
- Zeigen Sie die Ressourcen an, auf die ein Mitglied zugreifen kann.
- Zeigen Sie die Mitglieder und Ressourcen an, die mit einem bestimmten Projekt verknüpft sind.

Wohin als nächstes?

- "Erste Schritte mit IAM in der NetApp Console"
- "Organisieren Sie Ihre Ressourcen in der NetApp Console mit Ordnern und Projekten"
- "Verwalten Sie NetApp Console Mitglieder und ihre Berechtigungen"
- "Verwalten Sie die Ressourcenhierarchie in Ihrer NetApp Console Organisation"
- "Agenten Ordnern und Projekten zuordnen"
- "Wechseln Sie zwischen NetApp Console -Projekten und -Organisationen"
- "Benennen Sie Ihre NetApp Console um"
- "Überwachen oder prüfen Sie die IAM-Aktivität"
- "NetApp Console"
- "Erfahren Sie mehr über die API für NetApp Console IAM"

Erste Schritte mit Identität und Zugriff in der NetApp Console

Wenn Sie sich für die NetApp Console anmelden, werden Sie aufgefordert, eine neue Organisation zu erstellen. Die Organisation umfasst ein Mitglied (einen Organisationsadministrator) und ein Standardprojekt. Um die Identitäts- und Zugriffsverwaltung (IAM) so einzurichten, dass sie Ihren Geschäftsanforderungen entspricht, müssen Sie die Hierarchie Ihrer Organisation anpassen, zusätzliche Mitglieder hinzufügen, Ressourcen hinzufügen oder ermitteln und diese Ressourcen in Ihrer Hierarchie verknüpfen.

Sie müssen über die Berechtigung **Organisationsadministrator** verfügen, um die Identität und den Zugriff für Ihre gesamte Organisation zu verwalten. Wenn Sie über die Berechtigung **Ordner- oder Projektadministrator** verfügen, können Sie nur die Ordner und Projekte verwalten, für die Sie über die Berechtigung verfügen.

Befolgen Sie diese Schritte, um eine neue Organisation einzurichten. Die Reihenfolge kann je nach den Anforderungen Ihrer Organisation variieren.

1 Bearbeiten Sie das Standardprojekt oder fügen Sie es der Hierarchie Ihrer Organisation hinzu

Verwenden Sie das Standardprojekt oder erstellen Sie zusätzliche Projekte und Ordner, die Ihrer Unternehmenshierarchie entsprechen.

"Erfahren Sie, wie Sie Ihre Ressourcen mit Ordnern und Projekten organisieren" .

2 Ordnen Sie Mitglieder Ihrer Organisation zu

Verknüpfen Sie Benutzerkonten mit Ihrer Organisation und weisen Sie Berechtigungen zu. Sie haben auch die Möglichkeit, Ihrer Organisation Dienstkonten hinzuzufügen.

"Erfahren Sie, wie Sie Mitglieder und ihre Berechtigungen verwalten" .

3 Ressourcen hinzufügen oder entdecken

Fügen Sie der Konsole Ressourcen (Systeme) hinzu oder ermitteln Sie sie. Mitglieder der Organisation verwalten Systeme innerhalb eines Projekts.

Erfahren Sie, wie Sie Ressourcen erstellen oder entdecken:

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Systeme der E-Serie"
- "On-Premises- ONTAP -Cluster"
- "StorageGRID"

4 Ressourcen zusätzlichen Projekten zuordnen

Durch das Hinzufügen oder Erkennen eines Systems in der Konsole wird die Ressource automatisch dem aktuell ausgewählten Projekt zugeordnet. Um diese Ressource einem anderen Projekt in Ihrer Organisation zur Verfügung zu stellen, verknüpfen Sie sie mit dem jeweiligen Projekt. Wenn zur Verwaltung der Ressource ein Konsolenagent verwendet wird, ordnen Sie den Konsolenagenten dem jeweiligen Projekt zu.

- "Erfahren Sie, wie Sie die Ressourcenhierarchie Ihres Unternehmens verwalten" .
- "Erfahren Sie, wie Sie einen Konsolenagenten mit einem Ordner oder Projekt verknüpfen" .

Ähnliche Informationen

- "Erfahren Sie mehr über Identitäts- und Zugriffsmanagement in der NetApp Console"
- "Erfahren Sie mehr über die API für Identität und Zugriff"

Organisieren Sie Ihre NetApp Console -Ressourcen mit Ordnern und Projekten

In der NetApp Console organisieren Sie Ihre NetApp -Ressourcen mithilfe von Projekten und Ordnern. Ein *Projekt* stellt einen Arbeitsbereich in der Konsole dar, auf den Mitglieder der Organisation zugreifen, um *Ressourcen* zu verwalten (z. B. ein Cloud Volumes ONTAP System). Ein *Ordner* fasst verwandte Projekte zusammen. Nachdem Sie Ihre Ressourcen in Ordnern und Projekten organisiert haben, können Sie einen differenzierten Zugriff auf die Ressourcen gewähren, indem Sie den Mitgliedern der Organisation Berechtigungen für bestimmte Ordner und Projekte erteilen.

Einen Ordner oder ein Projekt hinzufügen

Wenn Sie Ihre Organisation erstellen, umfasst diese ein einzelnes Projekt. Fügen Sie Projekte hinzu, um Ressourcen zu verwalten, und Ordner, um verwandte Projekte zu gruppieren.

Die Ressourcenhierarchie Ihrer Organisation kann bis zu sieben Ebenen umfassen, wobei Ordner sechs Ebenen tief verschachtelt sind und Projekte auf der siebten Ebene liegen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Organisation** aus.
3. Wählen Sie auf der Seite **Organisation** die Option **Ordner oder Projekt hinzufügen** aus.
4. Wählen Sie **Ordner** oder **Projekt**.
5. Geben Sie Details zum Ordner oder Projekt an:

   - **Name und Speicherort**: Geben Sie einen Namen ein und wählen Sie einen Speicherort in der Hierarchie für den Ordner oder das Projekt. Ein Ordner oder Projekt kann sich direkt unter der Organisation oder innerhalb eines Ordners befinden.
   - **Ressourcen**: Wählen Sie die Ressourcen aus, die Sie diesem Ordner oder Projekt zuordnen möchten.

     Sie können Ressourcen auswählen, die mit dem übergeordneten Ordner oder Projekt verknüpft sind.

     "Erfahren Sie, wann Sie eine Ressource mit einem Ordner verknüpfen müssen" .
   - **Zugriff**: Zeigen Sie die Mitglieder an, die basierend auf den bereits in Ihrer Ressourcenhierarchie definierten Berechtigungen Zugriff auf den Ordner oder das Projekt haben.

     Wählen Sie **Mitglied hinzufügen**, um weiteren Mitgliedern Zugriff und eine Rolle zuzuweisen. Eine Rolle definiert die Berechtigungen, die Mitglieder für den Ordner oder das Projekt haben.

   "Informationen zu Zugriffsrollen" .
6. Wählen Sie **Hinzufügen**.

Umbenennen eines Ordners oder Projekts

Bei Bedarf können Sie die Namen Ihrer Ordner und Projekte ändern.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.
2. Geben Sie auf der Seite **Bearbeiten** einen neuen Namen ein und wählen Sie **Übernehmen**.

Löschen eines Ordners oder Projekts

Löschen Sie Ordner und Projekte, die Sie nicht mehr benötigen.

Bevor Sie beginnen

- Stellen Sie sicher, dass dem Ordner oder Projekt keine Ressourcen zugeordnet sind. Erfahren Sie, wie Sie die Zuordnung von Ressourcen aufheben .
- Stellen Sie sicher, dass dem Ordner oder Projekt keine Ressourcen zugeordnet sind.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Löschen**.
2. Bestätigen Sie, dass Sie den Ordner oder das Projekt löschen möchten.

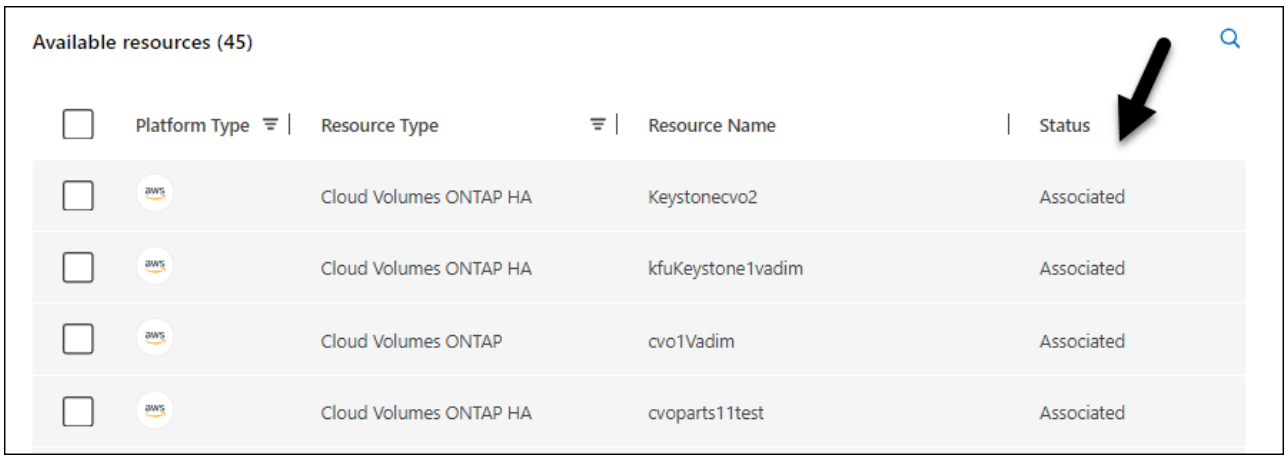
Anzeigen der mit einem Ordner oder Projekt verknüpften Ressourcen

Zeigen Sie an, welche Ressourcen und Mitglieder mit einem Ordner oder Projekt verknüpft sind.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.

2. Auf der Seite **Bearbeiten** können Sie Details zum ausgewählten Ordner oder Projekt anzeigen, indem Sie die Abschnitte **Ressourcen** oder **Zugriff** erweitern.
   - Wählen Sie **Ressourcen** aus, um die zugehörigen Ressourcen anzuzeigen. In der Tabelle identifiziert die Spalte **Status** die Ressourcen, die mit dem Ordner oder Projekt verknüpft sind.



Ändern der mit einem Ordner oder Projekt verknüpften Ressourcen

Mitglieder mit Berechtigungen für einen Ordner oder ein Projekt können auf die zugehörigen Ressourcen zugreifen.

Bevor Sie beginnen

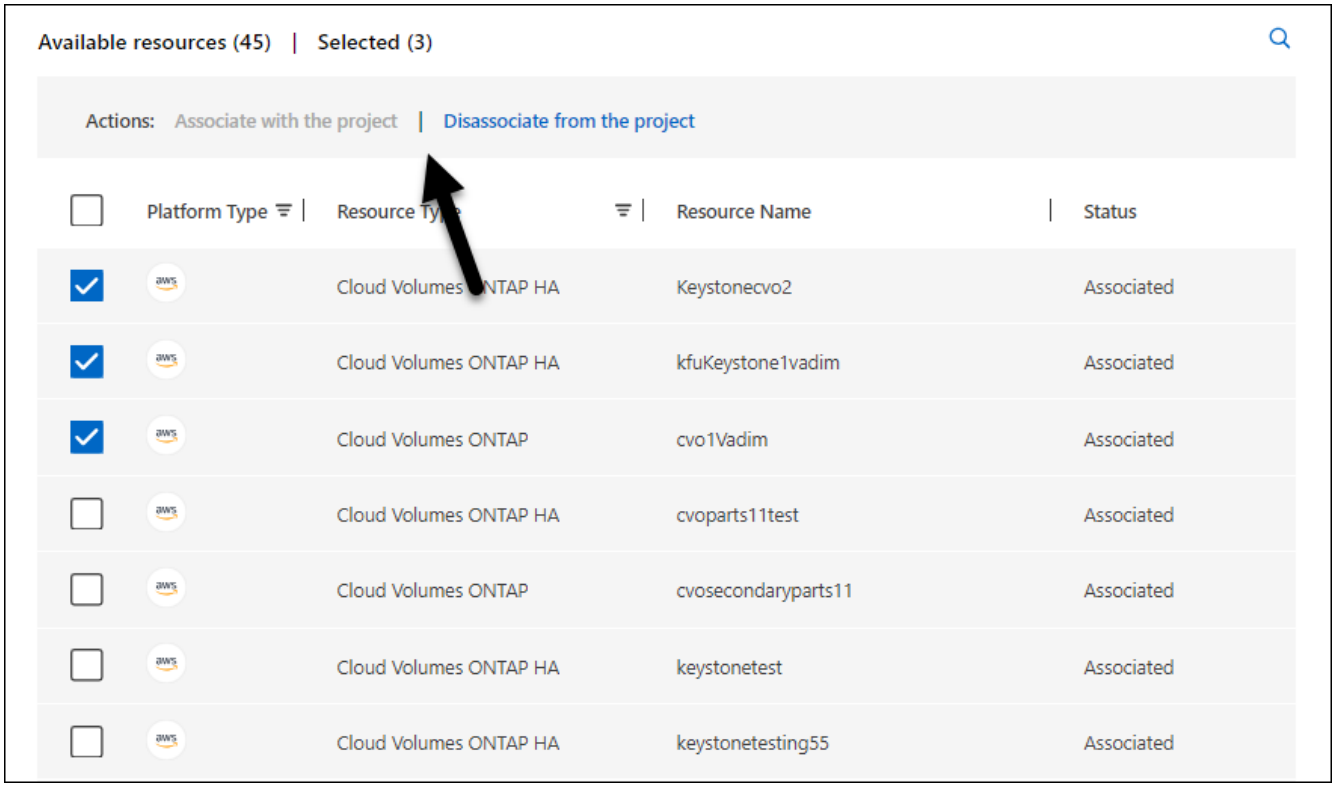
"Erfahren Sie, wann Sie eine Ressource mit einem Ordner verknüpfen müssen" .

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.
2. Wählen Sie auf der Seite **Bearbeiten Ressourcen** aus.

   In der Tabelle identifiziert die Spalte **Status** die Ressourcen, die mit dem Ordner oder Projekt verknüpft sind.

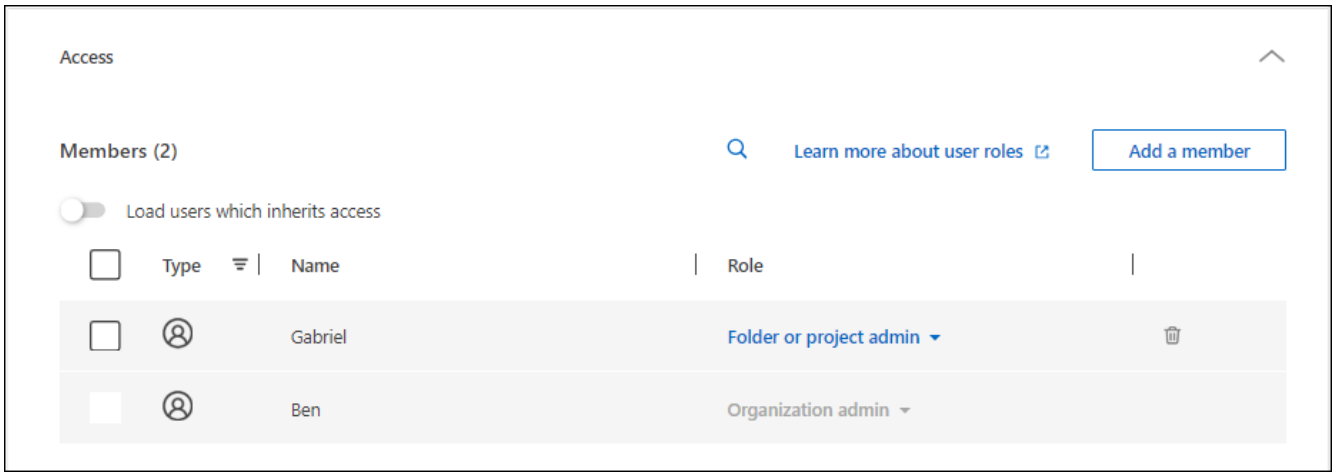
3. Wählen Sie die Ressourcen aus, die Sie zuordnen oder deren Zuordnung Sie aufheben möchten.
4. Wählen Sie je nach den von Ihnen ausgewählten Ressourcen entweder **Mit dem Projekt verknüpfen** oder **Vom Projekt trennen**.



5. Wählen Sie **Übernehmen**

Anzeigen von Mitgliedern, die einem Ordner oder Projekt zugeordnet sind

- Wählen Sie **Zugriff** aus, um die Mitglieder anzuzeigen, die Zugriff auf den Ordner oder das Projekt haben.



Ändern des Mitgliederzugriffs auf einen Ordner oder ein Projekt

Ändern Sie den Mitgliederzugriff, um sicherzustellen, dass die richtigen Mitglieder auf die zugehörigen Ressourcen zugreifen können.

Der auf einer höheren Hierarchieebene gewährte Mitgliederzugriff kann auf niedrigeren Ebenen nicht geändert werden. Aktualisieren Sie die Mitgliedsberechtigungen auf der höheren Hierarchieebene, um den Zugriff zu ändern. Alternativ können Sie"Verwalten Sie Berechtigungen auf der Seite „Mitglieder“" .

"Erfahren Sie mehr über die Rollenvererbung" .

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.
2. Wählen Sie auf der Seite **Bearbeiten Zugriff** aus, um die Liste der Mitglieder anzuzeigen, die Zugriff auf den ausgewählten Ordner oder das ausgewählte Projekt haben.
3. Mitgliederzugriff ändern:
   - **Mitglied hinzufügen**: Wählen Sie das Mitglied aus, das Sie dem Ordner oder Projekt hinzufügen möchten, und weisen Sie ihm eine Rolle zu.
   - **Rolle eines Mitglieds ändern**: Wählen Sie für alle Mitglieder mit einer anderen Rolle als „Organisationsadministrator“ ihre vorhandene Rolle und dann eine neue Rolle aus.
   - **Mitgliederzugriff entfernen**: Sie können den Zugriff von Mitgliedern entfernen, denen für den Ordner oder das Projekt, das Sie gerade anzeigen, eine Rolle definiert ist.
4. Wählen Sie **Übernehmen**.

Ähnliche Informationen

- "Erfahren Sie mehr über Identität und Zugriff in der NetApp Console"
- "Erste Schritte mit Identität und Zugriff"
- "Erfahren Sie mehr über die Identitäts- und Zugriffs-API"

Fügen Sie der NetApp Console Mitglieder und Dienstkonten hinzu

In der Konsole können Sie Ihrer Organisation Benutzer und Dienstkonten hinzufügen und ihnen eine oder mehrere Rollen in Ihrer Ressourcenhierarchie zuweisen. Eine *Rolle* enthält eine Reihe von Berechtigungen, die es einem Mitglied (Benutzer- oder Dienstkonto) ermöglichen, bestimmte Aktionen auf einer bestimmten Ebene der Ressourcenhierarchie auszuführen.

Zum Verwalten von Benutzern und Berechtigungen benötigen Sie eine der folgenden Rollen:

- Organisationsadministrator

  Benutzer mit dieser Rolle können alle Mitglieder verwalten

- Ordner- oder Projektadministrator

  Benutzer mit dieser Rolle können nur Mitglieder eines bestimmten Ordners oder Projekts verwalten.

  Ordner- oder Projektadministratoren können alle Mitglieder auf der Seite **Mitglieder** anzeigen, aber nur die Berechtigungen für Ordner und Projekte verwalten, auf die sie Zugriff haben. "Erfahren Sie mehr über die Aktionen, die ein Ordner- oder Projektadministrator ausführen kann." .

Fügen Sie Ihrer Organisation Mitglieder hinzu

Sie können Ihrer Organisation zwei Arten von Mitgliedern hinzufügen: ein Benutzerkonto und ein Dienstkonto. Anwendungen verwenden Dienstkonten, um API-Aufgaben ohne menschliches Eingreifen auszuführen. Normalerweise verwendet eine Person ein Benutzerkonto, um sich anzumelden und Ressourcen zu verwalten.

Benutzer müssen sich für die NetApp Console anmelden, bevor Sie sie zu einer Organisation hinzufügen oder ihnen eine Rolle zuweisen können. Sie erstellen Dienstkonten direkt von der Konsole aus.

Um Benutzer und ihre Berechtigungen zu verwalten, müssen Sie über die Rolle **Organisationsadministrator** oder die Rolle **Ordner- oder Projektadministrator** verfügen. Denken Sie daran, dass Benutzer mit der Rolle **Ordner- oder Projektadministrator** nur Mitglieder für die Ordner oder Projekte verwalten können, für die sie über Administratorberechtigungen verfügen.

Hinzufügen eines Benutzerkontos

Obwohl sich Benutzer selbst für die NetApp Console anmelden, müssen sie explizit einer Organisation oder bestimmten Ordnern oder Projekten hinzugefügt werden, um auf Ressourcen in der Konsole zugreifen zu können.

Schritte

1. Leiten Sie den Benutzer zum Besuch weiter "NetApp Console" um sich anzumelden.

   Sobald sich Benutzer angemeldet haben, füllen sie die Seite **Anmelden** aus, überprüfen ihre E-Mails und melden sich an. Wenn die Konsole Benutzer auffordert, eine Organisation zu erstellen, schließen sie diese und benachrichtigen Sie über die Erstellung ihres Kontos. Anschließend können Sie den Benutzer zu Ihrer bestehenden Organisation hinzufügen.

   "Erfahren Sie, wie Sie sich für die NetApp Console anmelden" .

2. Wählen Sie **Verwaltung > Identität und Zugriff**.
3. Wählen Sie **Mitglieder** aus.
4. Wählen Sie **Mitglied hinzufügen**.
5. Behalten Sie für **Mitgliedstyp** die Auswahl von **Benutzer** bei.
6. Geben Sie bei **E-Mail des Benutzers** die E-Mail-Adresse des Benutzers ein, die mit der von ihm erstellten Anmeldung verknüpft ist.
7. Verwenden Sie den Abschnitt **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**, um die Ebene Ihrer Ressourcenhierarchie auszuwählen, für die das Mitglied Berechtigungen haben soll.

   Beachten Sie Folgendes:

   - Sie können nur aus den Ordnern und Projekten auswählen, für die Sie Berechtigungen haben.
   - Durch die Auswahl einer Organisation oder eines Ordners erhält das Mitglied Zugriff auf alle Inhalte.
   - Sie können die Rolle **Organisationsadministrator** nur auf Organisationsebene zuweisen.
8. **Wählen Sie eine Kategorie** und dann eine **Rolle** aus, die dem Mitglied Berechtigungen für die Ressourcen erteilt, die mit der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt verknüpft sind.

   "Informationen zu Zugriffsrollen" .

9. Optional: Wählen Sie eine zusätzliche Rolle oder ein zusätzliches Projekt aus. Wenn Sie Zugriff auf weitere

Ordner oder Projekte innerhalb Ihrer Organisation gewähren oder dem Benutzer zusätzliche Rollen im ausgewählten Bereich zuweisen möchten, wählen Sie **Rolle hinzufügen**, geben Sie einen anderen Ordner oder ein anderes Projekt oder eine andere Rollenkategorie an und wählen Sie dann eine Rolle aus.

10. Wählen Sie **Hinzufügen**.

    Die Konsole sendet dem Benutzer eine E-Mail mit Anweisungen.

Hinzufügen eines Dienstkontos

Sie können Aufgaben automatisieren und eine sichere Integration mit Konsolen-APIs über Dienstkonten durchführen. Wenn Sie ein Dienstkonto erstellen, wählen Sie zwischen zwei Authentifizierungsmethoden: mithilfe einer Client-ID und eines Geheimnisses oder mithilfe der JWT-Authentifizierung (JSON Web Token). Die Client-ID und die geheime Methode eignen sich für einfache Setups, während die JWT-Authentifizierung eine stärkere Sicherheit für automatisierte oder Cloud-native Umgebungen bietet. Wählen Sie die Option, die Ihren Sicherheitsanforderungen und der geplanten Verwendung der Konsole am besten entspricht.

Wenn Sie die JWT-Authentifizierung verwenden möchten, halten Sie Ihren öffentlichen Schlüssel oder Ihr Zertifikat einsatzbereit.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie **Mitglied hinzufügen**.
4. Wählen Sie für **Mitgliedstyp Dienstkonto** aus.
5. Geben Sie einen Namen für das Dienstkonto ein.
6. Wenn Sie die JWT-Authentifizierung verwenden möchten, wählen Sie **JWT-Authentifizierung mit privatem Schlüssel verwenden** und laden Sie Ihren öffentlichen RSA-Schlüssel oder Ihr Zertifikat hoch. Überspringen Sie diesen Schritt, wenn Sie stattdessen eine Client-ID und ein Geheimnis verwenden möchten.

   Ihr X.509-Zertifikat. Es muss im PEM-, CRT- oder CER-Format vorliegen.

7. Verwenden Sie den Abschnitt **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**, um die Ebene Ihrer Ressourcenhierarchie auszuwählen, für die das Mitglied Berechtigungen haben soll.

   Beachten Sie Folgendes:

   - Sie können nur aus den Ordnern und Projekten auswählen, für die Sie Berechtigungen haben.
   - Durch die Auswahl einer Organisation oder eines Ordners erhält das Mitglied Zugriff auf alle Inhalte.
   - Sie können die Rolle **Organisationsadministrator** nur auf Organisationsebene zuweisen.

8. Wählen Sie eine **Kategorie** und dann eine **Rolle** aus, die dem Mitglied Berechtigungen für die Ressourcen erteilt, die mit der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt verknüpft sind.

   "Informationen zu Zugriffsrollen" .

9. Optional: Wählen Sie eine zusätzliche Rolle oder ein zusätzliches Projekt aus. Wenn Sie Zugriff auf weitere Ordner oder Projekte innerhalb Ihrer Organisation gewähren oder dem Benutzer zusätzliche Rollen im ausgewählten Bereich zuweisen möchten, wählen Sie **Rolle hinzufügen**, geben Sie einen anderen Ordner oder ein anderes Projekt oder eine andere Rollenkategorie an und wählen Sie dann eine Rolle aus.
10. Wenn Sie sich nicht für die Verwendung der JWT-Authentifizierung entschieden haben, laden Sie die

Client-ID und das Client-Geheimnis herunter oder kopieren Sie sie. + Die Konsole zeigt das Client-Geheimnis nur einmal an. Kopieren Sie es sicher. Sie können es später bei Bedarf neu erstellen.

11. Wenn Sie die JWT-Authentifizierung gewählt haben, laden Sie die Client-ID und die JWT-Zielgruppe herunter oder kopieren Sie sie. Diese Informationen werden nur einmal angezeigt und können später nicht mehr abgerufen werden.
12. Wählen Sie **Schließen**.

Organisationsmitglieder anzeigen

Um zu verstehen, welche Ressourcen und Berechtigungen einem Mitglied zur Verfügung stehen, können Sie die dem Mitglied auf verschiedenen Ebenen der Ressourcenhierarchie Ihrer Organisation zugewiesenen Rollen anzeigen."Erfahren Sie, wie Sie mithilfe von Rollen den Zugriff auf Konsolenressourcen steuern."

Sie können sowohl Benutzerkonten als auch Dienstkonten auf der Seite **Mitglieder** anzeigen.

Sie können auch alle Mitglieder anzeigen, die einem bestimmten Ordner oder Projekt zugeordnet sind. "Mehr erfahren" .

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.

   In der Tabelle **Mitglieder** sind die Mitglieder Ihrer Organisation aufgelistet.

3. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.

Entfernen eines Mitglieds aus Ihrer Organisation

Möglicherweise müssen Sie ein Mitglied aus Ihrer Organisation entfernen, beispielsweise wenn es Ihr Unternehmen verlässt.

Das System entfernt die Berechtigungen des Mitglieds, behält jedoch seine Konsolen- und NetApp Support-Site-Konten.

Schritte

1. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• Wählen Sie dann **Benutzer löschen**.
2. Bestätigen Sie, dass Sie das Mitglied aus Ihrer Organisation entfernen möchten.

Erstellen Sie die Anmeldeinformationen für ein Dienstkonto neu

Erstellen Sie neue Anmeldeinformationen, wenn Sie sie verlieren oder aktualisieren müssen.

Wenn Sie die Anmeldeinformationen neu erstellen, löschen Sie die vorhandenen Anmeldeinformationen für das Dienstkonto und erstellen neue. Sie können die vorherigen Anmeldeinformationen nicht verwenden.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Navigieren Sie in der Tabelle **Mitglieder** zu einem Dienstkonto, wählen Sie ••• und wählen Sie dann

Geheimnisse neu erstellen.

4. Wählen Sie **Neu erstellen**.
5. Laden Sie die Client-ID und das Client-Geheimnis herunter oder kopieren Sie sie. + Das Client-Geheimnis wird nur einmal angezeigt. Kopieren oder laden Sie es herunter und speichern Sie es sicher.

Verwalten der Multi-Faktor-Authentifizierung (MFA) eines Benutzers

Wenn ein Benutzer den Zugriff auf sein MFA-Gerät verliert, können Sie seine MFA-Konfiguration entweder entfernen oder deaktivieren.

Benutzer müssen MFA nach der Entfernung bei der Anmeldung neu konfigurieren. Wenn der Benutzer den Zugriff auf sein MFA-Gerät nur vorübergehend verloren hat, kann er zur Anmeldung den Wiederherstellungscode verwenden, den er beim Einrichten von MFA gespeichert hat.

Wenn sie ihren Wiederherstellungscode nicht haben, deaktivieren Sie MFA vorübergehend, um die Anmeldung zu ermöglichen. Wenn Sie MFA für einen Benutzer deaktivieren, wird es nur für acht Stunden deaktiviert und dann automatisch wieder aktiviert. Dem Benutzer ist während dieser Zeit eine Anmeldung ohne MFA gestattet. Nach Ablauf der acht Stunden muss der Benutzer MFA verwenden, um sich anzumelden.

Um die Multi-Faktor-Authentifizierung eines Benutzers zu verwalten, müssen Sie über eine E-Mail-Adresse in derselben Domäne wie der betroffene Benutzer verfügen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.

   In der Tabelle **Mitglieder** sind die Mitglieder Ihrer Organisation aufgelistet.

3. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Multi-Faktor-Authentifizierung verwalten**.
4. Wählen Sie, ob die MFA-Konfiguration des Benutzers entfernt oder deaktiviert werden soll.

Verwenden Sie Rollen, um den Benutzerzugriff auf NetApp Console -Ressourcen zu verwalten

Innerhalb der Konsole können Sie Benutzern Rollen zuweisen, je nachdem, was sie tun müssen und wo.

Benutzer mit der Rolle **Organisationsadministrator** oder **Ordner- oder Projektadministrator** sind dafür verantwortlich, anderen Benutzern Rollen zuzuweisen. Sie können Zugriffsrollen auf Projekt- oder Ordnerbasis zuweisen. Sie können einem Benutzer beispielsweise für ein Projekt die Administratorrolle für den Ransomware-Schutz und für ein anderes Projekt die Administratorrolle für SnapCenter zuweisen. Wenn ein Benutzer alternativ die Klassifizierungsadministratorrolle für alle Projekte in einem bestimmten Ordner benötigt, können Sie ihm diese Rolle auf Ordnerebene zuweisen.

Verwenden Sie Zugriffsrollen, um den Zugriff auf Speicherressourcen basierend auf den spezifischen Aufgaben zuzuweisen, die Benutzer ausführen müssen. Wenn ein Benutzer beispielsweise mit Ransomware-Schutzdiensten interagieren muss, muss ihm eine Zugriffsrolle zugewiesen werden, die entweder Anzeige- oder Administratorberechtigungen für den Ransomware-Schutzdienst für das Projekt umfasst, für das die Zugriffsrolle gewährt wird.

Weisen Sie Benutzern basierend auf Ihrer IAM-Strategie Rollen zu, um die Sicherheit zu erhöhen. IAM-Rollen

stellen sicher, dass Benutzer nur den Zugriff haben, den sie benötigen.

> Denken Sie daran, dass Sie keinen direkten Zugriff auf Ressourcen gewähren können. Weisen Sie den Projekten zunächst Ressourcen zu. Erwägen Sie die Einrichtung Ihrer Ressourcenhierarchie, bevor Sie Benutzern Zugriff zuweisen."Erfahren Sie, wie Sie Ihre Ressourcen mit Ordnern und Projekten organisieren."

Einem Mitglied zugewiesene Rollen anzeigen

Wenn Sie Ihrer Organisation ein Mitglied hinzufügen, werden Sie aufgefordert, ihm eine Rolle zuzuweisen. Sie können bei Mitgliedern überprüfen, welche Rollen ihnen derzeit zugewiesen sind.

Wenn Sie die Rolle „Ordner- oder Projektadministrator“ haben, werden auf der Seite alle Mitglieder der Organisation angezeigt. Sie können jedoch nur die Mitgliedsberechtigungen für die Ordner und Projekte anzeigen und verwalten, für die Sie über Berechtigungen verfügen. "Erfahren Sie mehr über die Aktionen, die ein Ordner- oder Projektadministrator ausführen kann." .

1. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.
2. Erweitern Sie in der Tabelle die jeweilige Zeile für die Organisation, den Ordner oder das Projekt, in dem Sie die zugewiesene Rolle des Mitglieds anzeigen möchten, und wählen Sie in der Spalte **Rolle** die Option **Anzeigen** aus.

Einem Mitglied eine Zugriffsrolle hinzufügen

Normalerweise weisen Sie eine Rolle zu, wenn Sie ein Mitglied zu Ihrer Organisation hinzufügen, Sie können sie jedoch jederzeit aktualisieren, indem Sie Rollen entfernen oder hinzufügen.

Sie können einem Benutzer eine Zugriffsrolle für Ihre Organisation, Ihren Ordner oder Ihr Projekt zuweisen.

Mitglieder können innerhalb desselben Projekts und in verschiedenen Projekten mehrere Rollen haben. Beispielsweise können kleinere Organisationen alle verfügbaren Zugriffsrollen demselben Benutzer zuweisen, während größere Organisationen Benutzer mit spezialisierteren Aufgaben betrauen. Alternativ können Sie einem Benutzer auch die Administratorrolle für den Ransomware-Schutz einer Organisation zuweisen. In diesem Beispiel könnte der Benutzer Ransomware-Schutzaufgaben für alle Projekte innerhalb Ihrer Organisation durchführen.

Ihre Zugriffsrollenstrategie sollte mit der Art und Weise übereinstimmen, wie Sie Ihre NetApp -Ressourcen organisiert haben.

> Einem Mitglied, dem die Rolle „Organisationsadministrator“ zugewiesen ist, können keine weiteren Rollen zugewiesen werden. Sie verfügen bereits über Berechtigungen für die gesamte Organisation. Einem Mitglied mit der Ordner- oder Projektrolle können innerhalb des Ordners oder Projekts, in dem es diese Rolle bereits hat, keine anderen Rollen zugewiesen werden. Beide Rollen bieten Zugriff auf alle Dienste im ihnen zugewiesenen Umfang.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie das Aktionsmenü ••• neben dem Mitglied, dem Sie eine Rolle zuweisen möchten, und wählen Sie **Rolle hinzufügen** aus.
3. Um eine Rolle hinzuzufügen, führen Sie die Schritte im Dialogfeld aus:

- **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**: Wählen Sie die Ebene Ihrer Ressourcenhierarchie aus, für die das Mitglied Berechtigungen haben soll.

  Wenn Sie die Organisation oder einen Ordner auswählen, verfügt das Mitglied über Berechtigungen für alles, was sich innerhalb der Organisation oder des Ordners befindet.

- **Kategorie auswählen**: Wählen Sie eine Rollenkategorie. "Informationen zu Zugriffsrollen" .
- Wählen Sie eine **Rolle**: Wählen Sie eine Rolle, die dem Mitglied Berechtigungen für die Ressourcen erteilt, die mit der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt verknüpft sind.
- **Rolle hinzufügen**: Wenn Sie Zugriff auf zusätzliche Ordner oder Projekte innerhalb Ihrer Organisation gewähren möchten, wählen Sie **Rolle hinzufügen**, geben Sie einen weiteren Ordner oder ein weiteres Projekt oder eine weitere Rollenkategorie an und wählen Sie dann eine Rollenkategorie und eine entsprechende Rolle aus.

4. Wählen Sie **Neue Rollen hinzufügen**.

Ändern der einem Mitglied zugewiesenen Rolle

Sie können die zugewiesenen Rollen für ein Mitglied ändern, falls Sie den Zugriff für einen Benutzer anpassen müssen.

Benutzern muss mindestens eine Rolle zugewiesen sein. Sie können einem Benutzer nicht alle Rollen entziehen. Wenn Sie alle Rollen entfernen müssen, müssen Sie den Benutzer aus Ihrer Organisation löschen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.
3. Erweitern Sie in der Tabelle die jeweilige Zeile für die Organisation, den Ordner oder das Projekt, in dem Sie die zugewiesene Rolle des Mitglieds ändern möchten, und wählen Sie in der Spalte **Rolle Anzeigen** aus, um die diesem Mitglied zugewiesenen Rollen anzuzeigen.
4. Sie können eine vorhandene Rolle für ein Mitglied ändern oder eine Rolle entfernen.
   a. Um die Rolle eines Mitglieds zu ändern, wählen Sie **Ändern** neben der Rolle, die Sie ändern möchten. Sie können eine Rolle nur in eine Rolle innerhalb derselben Rollenkategorie ändern. Sie können beispielsweise von einer Datendienstrolle zu einer anderen wechseln. Bestätigen Sie die Änderung.
   b. Um die Rolle eines Mitglieds aufzuheben, wählen Sie 🗑 neben der Rolle, um dem Mitglied die jeweilige Rolle zu entziehen. Sie werden aufgefordert, die Entfernung zu bestätigen.

Verwalten Sie die Ressourcenhierarchie in Ihrer NetApp Console Organisation

Wenn Sie ein Mitglied Ihrer Organisation zuordnen, erteilen Sie Berechtigungen auf Organisations-, Ordner- oder Projektebene. Um sicherzustellen, dass diese Mitglieder über die Berechtigungen zum Zugriff auf die richtigen Ressourcen verfügen, müssen Sie die Ressourcenhierarchie Ihrer Organisation verwalten, indem Sie Ressourcen bestimmten Projekten und Ordnern zuordnen. Eine *Ressource* ist ein Speichersystem oder ein Konsolenagent, den die Konsole bereits verwaltet oder kennt.

Zeigen Sie die Ressourcen in Ihrer Organisation an

Sie können sowohl entdeckte als auch unentdeckte Ressourcen anzeigen, die mit Ihrer Organisation verknüpft sind. Unentdeckte Ressourcen sind Speicherressourcen, die identifiziert, aber noch nicht zur Konsole hinzugefügt wurden.

HINWEIS: Auf der Seite „Ressourcen“ sind Amazon FSx for NetApp ONTAP -Ressourcen nicht enthalten, da Benutzer sie keiner Rolle zuordnen können. Zeigen Sie sie auf der Seite „Systeme“ oder unter „Workloads“ an.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Ressourcen** aus.
3. Wählen Sie **Erweiterte Suche und Filterung**.
4. Verwenden Sie eine der verfügbaren Optionen, um die gesuchte Ressource zu finden:
   - **Suche nach Ressourcennamen**: Geben Sie eine Textzeichenfolge ein und wählen Sie **Hinzufügen**.
   - **Plattform**: Wählen Sie eine oder mehrere Plattformen aus, beispielsweise Amazon Web Services.
   - **Ressourcen**: Wählen Sie eine oder mehrere Ressourcen aus, beispielsweise Cloud Volumes ONTAP.
   - **Organisation, Ordner oder Projekt**: Wählen Sie die gesamte Organisation, einen bestimmten Ordner oder ein bestimmtes Projekt aus.
5. Wählen Sie **Suchen**.

Zuordnen einer Ressource zu Ordnern und Projekten

Ordnen Sie eine Ressource einem Ordner oder Projekt zu, um sie verfügbar zu machen.

Bevor Sie beginnen

Sie sollten verstehen, wie die Ressourcenzuordnung funktioniert. "Informieren Sie sich über Ressourcen, beispielsweise darüber, wann eine Ressource einem Ordner zugeordnet werden sollte." .

Schritte

1. Navigieren Sie auf der Seite **Ressourcen** zu einer Ressource in der Tabelle, wählen Sie ••• und wählen Sie dann **Mit Ordnern oder Projekten verknüpfen**.
2. Wählen Sie einen Ordner oder ein Projekt aus und wählen Sie dann **Akzeptieren**.
3. Um einen zusätzlichen Ordner oder ein zusätzliches Projekt zuzuordnen, wählen Sie **Ordner oder Projekt hinzufügen** und wählen Sie dann den Ordner oder das Projekt aus.

   Beachten Sie, dass Sie nur aus den Ordnern und Projekten auswählen können, für die Sie über Administratorberechtigungen verfügen.

4. Wählen Sie **Ressourcen zuordnen**.
   - Wenn Sie die Ressource mit Projekten verknüpft haben, können Mitglieder, die über Berechtigungen für diese Projekte verfügen, jetzt über die Konsole auf die Ressource zugreifen.
   - Wenn Sie die Ressource mit einem Ordner verknüpft haben, kann ein *Ordner- oder Projektadministrator* jetzt auf die Ressource zugreifen und sie mit einem Projekt innerhalb des Ordners verknüpfen. "Informationen zum Verknüpfen einer Ressource mit einem Ordner" .

Nach Abschluss

Wenn Sie mithilfe eines Konsolenagenten eine Ressource entdecken, verknüpfen Sie den Konsolenagenten mit dem Projekt, um Zugriff zu gewähren. Andernfalls sind der Konsolenagent und die zugehörige Ressource für Mitglieder ohne die Rolle „Organisationsadministrator“ nicht zugänglich.

"Erfahren Sie, wie Sie einen Konsolenagenten mit einem Ordner oder Projekt verknüpfen" .

Anzeigen der mit einer Ressource verknüpften Ordner und Projekte

Sie können die Ordner und Projekte anzeigen, die mit einer bestimmten Ressource verknüpft sind.

Wenn Sie herausfinden möchten, welche Organisationsmitglieder Zugriff auf die Ressource haben, können Sie"Zeigen Sie die Mitglieder an, die Zugriff auf die Ordner und Projekte haben, die mit der Ressource verknüpft sind." .

Schritte

1. Navigieren Sie auf der Seite **Ressourcen** zu einer Ressource in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.

Das folgende Beispiel zeigt eine Ressource, die mit einem Projekt verknüpft ist.

Wenn Sie feststellen möchten, welche Organisationsmitglieder Zugriff auf die Ressource haben, können Sie"Zeigen Sie die Mitglieder an, die Zugriff auf die Ordner und Projekte haben, die mit der Ressource verknüpft sind." .

Entfernen einer Ressource aus einem Ordner oder Projekt

Um eine Ressource aus einem Ordner oder Projekt zu entfernen, müssen Sie die Verknüpfung zwischen dem Ordner oder Projekt und der Ressource entfernen. Wenn Sie die Zuordnung entfernen, können Mitglieder die Ressource im Ordner oder Projekt nicht mehr verwalten.

Um eine erkannte Ressource aus der gesamten Organisation zu entfernen, entfernen Sie das System von der Seite **Systeme**.

Schritte

1. Navigieren Sie auf der Seite **Ressourcen** zu einer Ressource in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.
2. Wählen Sie für den Ordner oder das Projekt, für das Sie die Ressource entfernen möchten, 🗑
3. Bestätigen Sie, dass Sie die Zuordnung entfernen möchten, indem Sie **Löschen** auswählen.

Ähnliche Informationen

- "Erfahren Sie mehr über Identität und Zugriff in der NetApp Console"
- "Erste Schritte mit Identität und Zugriff in der NetApp Console"
- "Erfahren Sie mehr über die API für Identität und Zugriff"

Verknüpfen Sie einen Konsolenagenten mit anderen Ordnern und Projekten

Wenn ein *Organisationsadministrator* einen Konsolenagenten erstellt, wird der Konsolenagent automatisch mit dem aktuell ausgewählten Projekt innerhalb der Organisation verknüpft. Allerdings kann jemand mit der Rolle „Organisationsadministrator“ von überall in der Organisation auf diesen Konsolenagenten zugreifen. Andere Mitglieder Ihrer Organisation können auf diesen Konsolenagenten nur über das Projekt zugreifen, in dem er erstellt wurde, es sei denn, Sie verknüpfen diesen Konsolenagenten mit anderen Projekten.

Bevor Sie beginnen

Überprüfen Sie, wie die Zuordnung von Konsolenagenten funktioniert. "Erfahren Sie mehr über die Verwendung des Konsolenagenten mit Identity and Access" .

Informationen zu diesem Vorgang

Ein *Ordner- oder Projektadministrator* kann alle Konsolenagenten auf der **Agenten**-Seite anzeigen, kann Konsolenagenten jedoch nur mit Ordnern und Projekten verknüpfen, für die er über Berechtigungen verfügt. "Erfahren Sie mehr über die Aktionen, die ein Ordner- oder Projektadministrator ausführen kann." .

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff** > **Agenten**.
2. Suchen Sie in der Tabelle den Konsolenagenten, den Sie zuordnen möchten.

   Verwenden Sie die Suche über der Tabelle, um einen bestimmten Konsolenagenten zu finden, oder filtern Sie die Tabelle nach Ressourcenhierarchie.

3. Um die mit dem Konsolenagenten verknüpften Ordner und Projekte anzuzeigen, wählen Sie ••• und wählen Sie dann **Details anzeigen**.

   Auf der Seite werden Details zu den Ordnern und Projekten angezeigt, die mit dem Konsolenagenten verknüpft sind.

4. Wählen Sie **Mit Ordner oder Projekt verknüpfen**.
5. Wählen Sie einen Ordner oder ein Projekt aus und wählen Sie dann **Akzeptieren**.
6. Um den Konsolenagenten mit einem zusätzlichen Ordner oder Projekt zu verknüpfen, wählen Sie **Ordner oder Projekt hinzufügen** und wählen Sie dann den Ordner oder das Projekt aus.
7. Wählen Sie **Associate Agent** aus.

Nach Abschluss

Ordnen Sie die Ressourcen des Konsolenagenten denselben Ordnern und Projekten von der Seite **Ressourcen** zu.

"Erfahren Sie, wie Sie eine Ressource mit Ordnern und Projekten verknüpfen" .

Ähnliche Informationen

- "Erfahren Sie mehr über NetApp Console -Agenten"
- "Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der NetApp Console"
- "Erste Schritte mit Identität und Zugriff"
- "Erfahren Sie mehr über die API für Identitäts- und Zugriffsverwaltung"

Wechseln Sie zwischen Konsolenorganisationen, Projekten und Agenten

Möglicherweise gehören Sie mehreren Konsolenorganisationen an oder verfügen über Berechtigungen zum Zugriff auf mehrere Projekte oder Agenten innerhalb einer Organisation. Bei Bedarf können Sie problemlos zwischen Organisationen, Projekten und Konsolenagenten wechseln, um auf die mit dieser Organisation, diesem Projekt oder diesem Agenten verknüpften Ressourcen zuzugreifen.

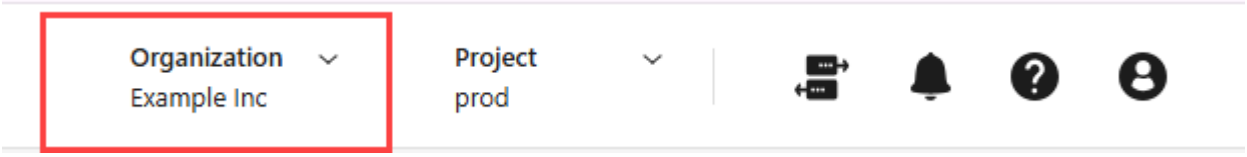
Sie können mehreren Organisationen angehören, wenn Sie von einer anderen Organisation zum Beitritt eingeladen werden oder wenn Sie selbst eine Organisation gründen. Sie können mithilfe der API eine zusätzliche Organisation erstellen. "Erfahren Sie, wie Sie eine neue Organisation erstellen"

Wechseln zwischen Organisationen

Wenn Sie Mitglied in mehreren Organisationen sind, können Sie jederzeit zwischen diesen wechseln.

Schritte

1. Wählen Sie in der oberen Kopfzeile der Konsole **Organisation** aus.



2. Wenn Sie Partnerorganisationen haben, wählen Sie die Registerkarte **Partnerschaft** aus, um die verfügbaren Partnerorganisationen anzuzeigen.

+ Die Registerkarte **Partnerschaft** wird nicht angezeigt, wenn Sie keine Partnerorganisationen haben.

1. Wählen Sie eine andere Organisation aus und wählen Sie dann **Wechseln**.

+ Wenn Sie Partnerorganisationen haben, wählen Sie die Registerkarte **Partnerschaft** aus, um die verfügbaren Partnerorganisationen anzuzeigen.

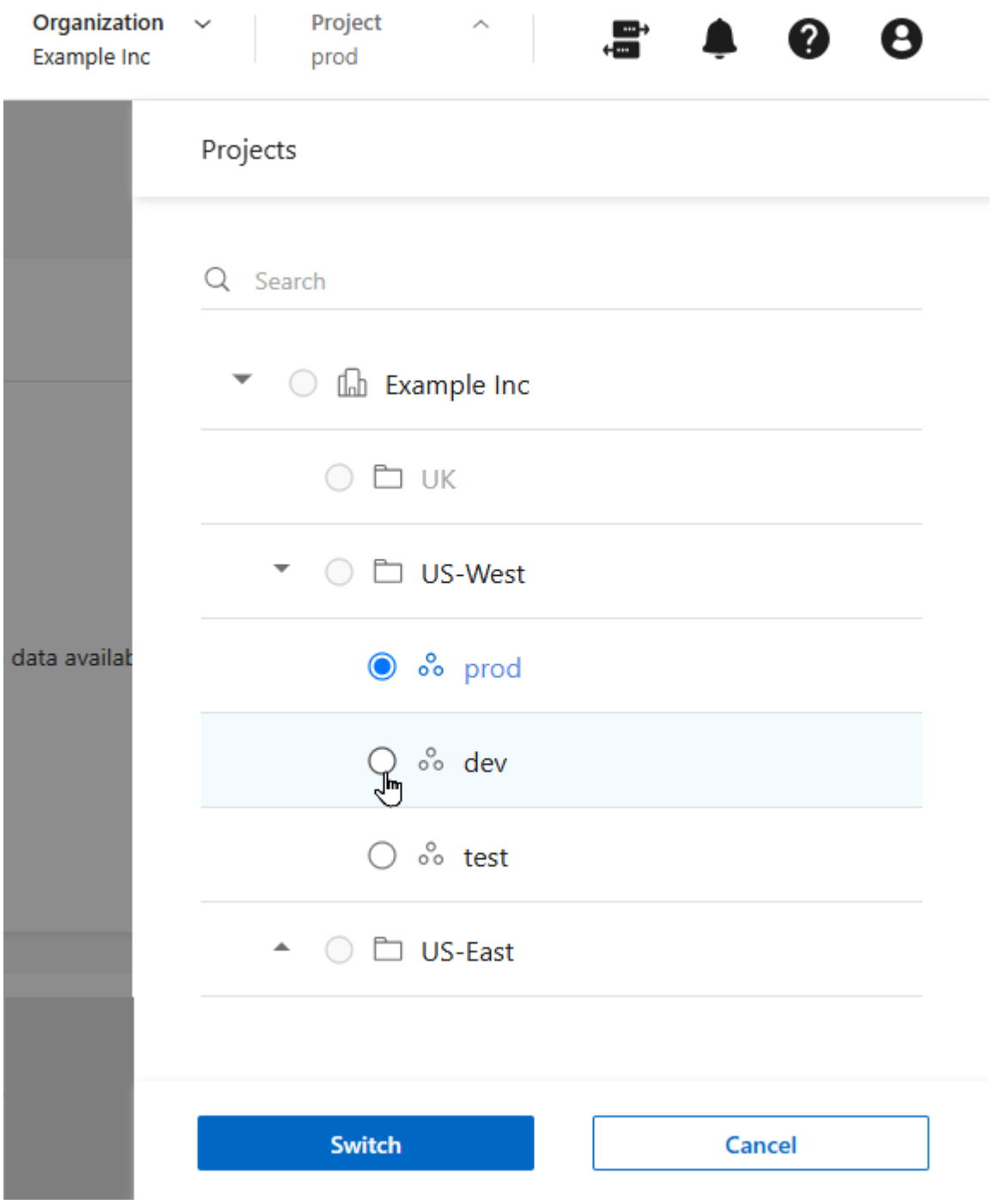
Zwischen Projekten wechseln

Wenn Ihre Organisation mehrere Projekte umfasst und Sie Zugriff auf diese Projekte haben, können Sie jederzeit zwischen ihnen wechseln.

Sie können nicht zu einem anderen Projekt wechseln, während Sie eine der Seiten „Identität und Zugriff“ anzeigen.

Schritte

1. Wählen Sie in der oberen Kopfzeile der Konsole **Projekt** aus.
2. Durchsuchen Sie die Ordner und Projekte in Ihrer Organisation, wählen Sie das gewünschte Projekt aus und wählen Sie dann **Wechseln**.



Wechseln zwischen Konsolenagenten

Wenn Sie über mehrere Konsolenagenten verfügen, können Sie zwischen ihnen wechseln, um die Systeme anzuzeigen, die einem bestimmten Agenten zugeordnet sind.

Schritte

1. Wählen Sie in der oberen Kopfzeile der Konsole das Agentensymbol aus.

2. Wählen Sie einen anderen Agenten und dann **Wechseln**.

Ähnliche Informationen

"Agenten Ordnern und Projekten zuordnen" .

Ähnliche Informationen

- "Erfahren Sie mehr über Identität und Zugriff in der NetApp Console"
- "Erste Schritte mit Identität und Zugriff"
- "Erfahren Sie mehr über die API für Identität und Zugriff"

Organisations- und Projekt-IDs

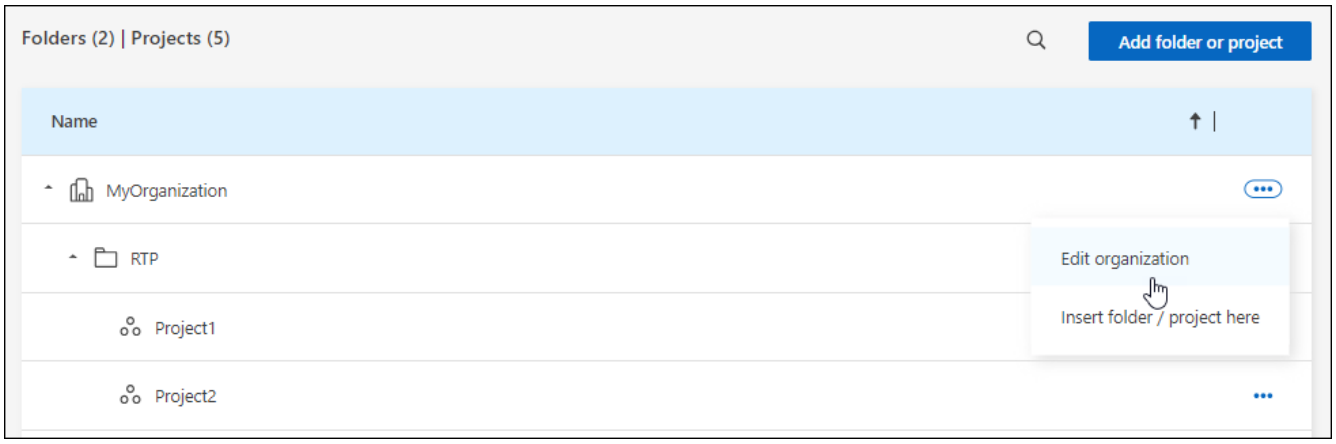
Ihre NetApp Console Konsolenorganisation hat einen Namen und eine ID. Sie können einen Namen für Ihre Organisation auswählen, um sie leichter zu identifizieren. Möglicherweise müssen Sie für bestimmte Integrationen auch die Organisations-ID abrufen.

Benennen Sie Ihre Organisation um

Sie können Ihre Organisation umbenennen. Dies ist hilfreich, wenn Sie mehr als nur die Organisation unterstützen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Organisation** aus.
3. Navigieren Sie auf der Seite **Organisation** zur ersten Zeile in der Tabelle und wählen Sie ••• und wählen Sie dann **Organisation bearbeiten**.



4. Geben Sie einen neuen Organisationsnamen ein und wählen Sie **Übernehmen**.

Abrufen der Organisations-ID

Die Organisations-ID wird für bestimmte Integrationen mit der Konsole verwendet.

Sie können die Organisations-ID auf der Seite „Organisationen“ anzeigen und sie für Ihren Bedarf in die Zwischenablage kopieren.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff** > **Organisation**.
2. Suchen Sie auf der Seite **Organisation** in der Übersichtsleiste nach Ihrer Organisations-ID und kopieren Sie sie in die Zwischenablage. Sie können dies zur späteren Verwendung speichern oder direkt dorthin kopieren, wo Sie es benötigen.

Abrufen der ID für ein Projekt

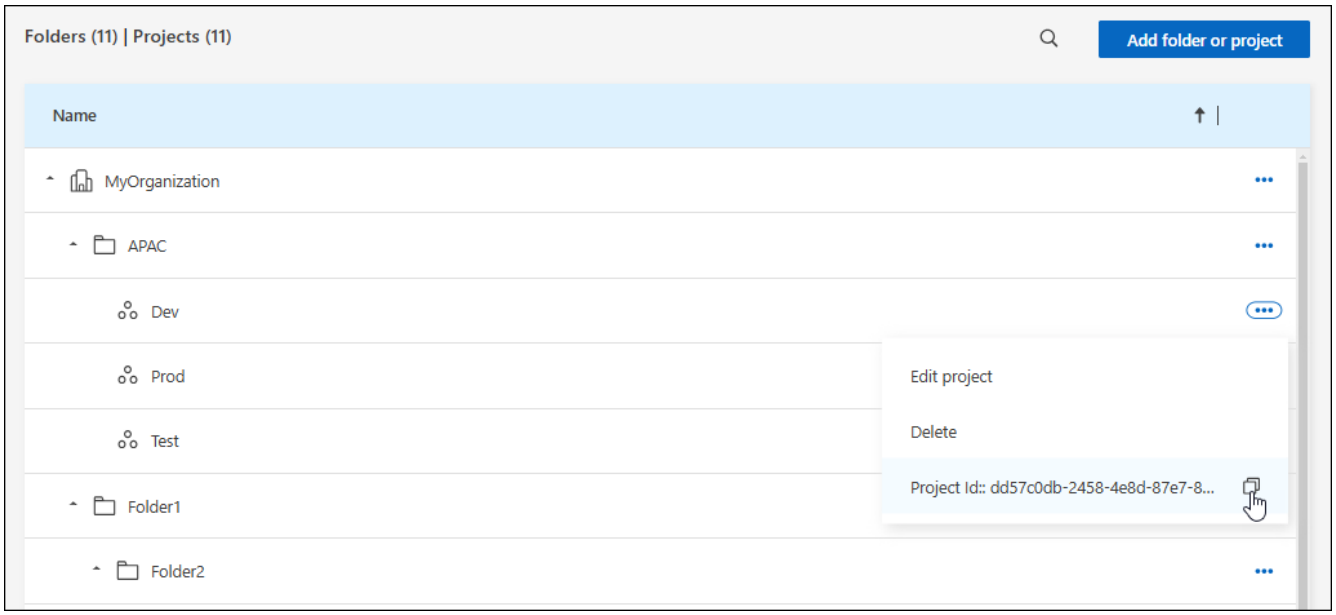
Sie müssen die ID für ein Projekt abrufen, wenn Sie die API verwenden. Beispielsweise beim Erstellen eines Cloud Volumes ONTAP -Systems.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt in der Tabelle und wählen Sie •••

   Die Projekt-ID wird angezeigt.

2. Um die ID zu kopieren, wählen Sie die Schaltfläche „Kopieren“.



Ähnliche Informationen

- "Erfahren Sie mehr über Identitäts- und Zugriffsverwaltung"
- "Erste Schritte mit Identität und Zugriff"
- "Erfahren Sie mehr über die API für Identität und Zugriff"

Überwachen oder prüfen Sie die IAM-Aktivität

Wenn Sie eine abgeschlossene Aktion im Zusammenhang mit Identität und Zugriff überwachen oder prüfen müssen, können Sie Details auf der Seite „Prüfung“ anzeigen. Sie möchten beispielsweise überprüfen, wer ein Mitglied zu einer Organisation hinzugefügt hat oder ob ein Projekt erfolgreich gelöscht wurde.

Schritte

1. Wählen Sie **Administration > Audit**.

2. Verwenden Sie auf der Seite **Audit** die Filter, um die Ergebnisse einzugrenzen. Wählen Sie **Service** und dann **Tenancy**.
3. Verwenden Sie einen der anderen Filter, um zu ändern, welche Aktionen in der Tabelle angezeigt werden.

   Sie können beispielsweise den Filter **Benutzer** verwenden, um Aktionen anzuzeigen, die sich auf ein bestimmtes Benutzerkonto beziehen.

NetApp Console

Erfahren Sie mehr über die Zugriffsrollen der NetApp Console

Das Identitäts- und Zugriffsmanagement (IAM) in der NetApp Console bietet vordefinierte Rollen, die Sie den Mitgliedern Ihrer Organisation auf verschiedenen Ebenen Ihrer Ressourcenhierarchie zuweisen können. Bevor Sie diese Rollen zuweisen, sollten Sie sich über die Berechtigungen im Klaren sein, die jede Rolle umfasst. Rollen fallen in die folgenden Kategorien: Plattform, Anwendung und Datendienst.

Plattformrollen

Plattformrollen gewähren Administratorberechtigungen für die NetApp Console , einschließlich Rollenzuweisung und Benutzerverwaltung. Die Konsole hat mehrere Plattformrollen.

Plattformrolle	Aufgaben
"Organisationsadministrator"	Ermöglicht einem Benutzer uneingeschränkten Zugriff auf alle Projekte und Ordner innerhalb einer Organisation, das Hinzufügen von Mitgliedern zu Projekten oder Ordnern sowie das Ausführen beliebiger Aufgaben und die Verwendung beliebiger Datendienste, denen keine explizite Rolle zugeordnet ist. Benutzer mit dieser Rolle verwalten Ihre Organisation, indem sie Ordner und Projekte erstellen, Rollen zuweisen, Benutzer hinzufügen und Systeme verwalten, wenn sie über die entsprechenden Anmeldeinformationen verfügen. Dies ist die einzige Zugriffsrolle, die Konsolenagenten erstellen kann.
"Ordner- oder Projektadministrator"	Ermöglicht einem Benutzer uneingeschränkten Zugriff auf zugewiesene Projekte und Ordner. Kann Mitglieder zu Ordnern oder Projekten hinzufügen, die sie verwalten, sowie beliebige Aufgaben ausführen und beliebige Datendienste oder Anwendungen auf Ressourcen innerhalb des ihnen zugewiesenen Ordners oder Projekts verwenden. Ordner- oder Projektadministratoren können keine Konsolenagenten erstellen.
"Föderationsadministrator"	Ermöglicht einem Benutzer das Erstellen und Verwalten von Föderationen mit der Konsole, wodurch Single Sign-On (SSO) ermöglicht wird.
"Föderationsbetrachter"	Ermöglicht einem Benutzer, vorhandene Föderationen mit der Konsole anzuzeigen. Föderationen können nicht erstellt oder verwaltet werden.
"Partnerschaftsadministrator"	Ermöglicht einem Benutzer, Partnerschaften zu erstellen und zu verwalten.
"Partnerschafts-Viewer"	Ermöglicht einem Benutzer, bestehende Partnerschaften anzuzeigen. Partnerschaften können nicht erstellt oder verwaltet werden.

Plattformrolle	Aufgaben
"Super-Admin"	Gibt dem Benutzer eine Teilmenge von Administratorrollen. Diese Rolle ist für kleinere Organisationen gedacht, die die Konsolenverantwortlichkeiten möglicherweise nicht auf mehrere Benutzer verteilen müssen.
"Super Viewer"	Gibt dem Benutzer eine Teilmenge der Viewer-Rollen. Diese Rolle ist für kleinere Organisationen gedacht, die die Konsolenverantwortlichkeiten möglicherweise nicht auf mehrere Benutzer verteilen müssen.

Anwendungsrollen

Nachfolgend finden Sie eine Liste der Rollen in der Anwendungskategorie. Jede Rolle gewährt innerhalb ihres festgelegten Umfangs spezifische Berechtigungen. Benutzer ohne die erforderliche Anwendungs- oder Plattformrolle können nicht auf die jeweilige Anwendung zugreifen.

Anwendungsrolle	Aufgaben
"Google Cloud NetApp Volumes Administrator"	Benutzer mit der Rolle „Google Cloud NetApp Volumes“ können Google Cloud NetApp Volumes erkennen und verwalten.
"Keystone -Administrator"	Benutzer mit der Keystone Administratorrolle können Serviceanfragen erstellen. Ermöglicht Benutzern, Nutzung, Ressourcen und Administratordetails innerhalb des Keystone Mandanten, auf den sie zugreifen, zu überwachen und anzuzeigen.
"Keystone -Viewer"	Benutzer mit der Keystone Viewer-Rolle KÖNNEN KEINE Serviceanfragen erstellen. Ermöglicht Benutzern die Überwachung und Anzeige von Verbrauch, Anlagen und Verwaltungsinformationen innerhalb des Keystone Mandanten, auf den sie zugreifen.
ONTAP Mediator-Setup-Rolle	Dienstkonten mit der Setup-Rolle „ONTAP Mediator“ können Dienstanfragen erstellen. Diese Rolle ist in einem Dienstkonto erforderlich, um eine Instanz des"ONTAP Cloud Mediator" .
"Betriebsunterstützungsanalyst"	Bietet Zugriff auf Warn- und Überwachungstools und die Möglichkeit, Supportfälle einzugeben und zu verwalten.
"Speicheradministrator"	Verwalten Sie Speicherintegritäts- und Governance-Funktionen, ermitteln Sie Speicherressourcen und ändern und löschen Sie vorhandene Systeme.
"Speicheranzeige"	Zeigen Sie Speicherintegrität und Governance-Funktionen an und zeigen Sie zuvor erkannte Speicherressourcen an. Vorhandene Speichersysteme können nicht erkannt, geändert oder gelöscht werden.
"Systemintegritätsspezialist"	Verwalten Sie Speicher-, Integritäts- und Governance-Funktionen. Alle Berechtigungen des Speicheradministrators sind zulässig, außer dass er vorhandene Systeme nicht ändern oder löschen kann.

Datendienstrollen

Nachfolgend finden Sie eine Liste der Rollen in der Kategorie Datendienste. Jede Rolle gewährt innerhalb ihres festgelegten Umfangs spezifische Berechtigungen. Benutzer, die nicht über die erforderliche Datendienstrolle oder Plattformrolle verfügen, können nicht auf den Datendienst zugreifen.

Datendienstrolle	Aufgaben
"Superadministrator für Backup und Wiederherstellung"	Führen Sie beliebige Aktionen in NetApp Backup and Recovery durch.
"Backup- und Wiederherstellungsadministrator"	Führen Sie Sicherungen auf lokalen Snapshots durch, replizieren Sie auf sekundären Speicher und sichern Sie auf Objektspeicher.
"Administrator für die Wiederherstellung von Backup und Wiederherstellung"	Stellen Sie Workloads in Backup und Recovery wieder her.
"Backup- und Wiederherstellungsklon-Administrator"	Klonen Sie Anwendungen und Daten in der Sicherung und Wiederherstellung.
"Backup- und Wiederherstellungs-Viewer"	Informationen zur Sicherung und Wiederherstellung anzeigen.
"Disaster Recovery-Administrator"	Führen Sie alle Aktionen im NetApp Disaster Recovery -Dienst aus.
"Disaster Recovery-Failover-Administrator"	Führen Sie Failover und Migrationen durch.
"Disaster Recovery-Anwendungsadministrator"	Erstellen Sie Replikationspläne, ändern Sie Replikationspläne und starten Sie Test-Failover.
"Disaster Recovery-Viewer"	Nur Informationen anzeigen.
Klassifizierungsanzeige	Ermöglicht Benutzern das Anzeigen der Scanergebnisse der NetApp Data Classification . Benutzer mit dieser Rolle können Compliance-Informationen anzeigen und Berichte für Ressourcen erstellen, auf die sie Zugriffsberechtigung haben. Diese Benutzer können das Scannen von Volumes, Buckets oder Datenbankschemata weder aktivieren noch deaktivieren. Die Klassifizierung hat keine Betrachterrolle.
"Ransomware-Resilienz-Administrator"	Verwalten Sie Aktionen auf den Registerkarten „Schützen“, „Warnungen“, „Wiederherstellen“, „Einstellungen“ und „Berichte“ von NetApp Ransomware Resilience.
"Ransomware Resilience-Viewer"	Zeigen Sie Arbeitslastdaten und Warndaten an, laden Sie Wiederherstellungsdaten herunter und laden Sie Berichte in Ransomware Resilience herunter.
"Ransomware Resilience-Benutzerverhaltensadministrator"	Konfigurieren, verwalten und zeigen Sie die Erkennung, Warnungen und Überwachung verdächtigen Benutzerverhaltens in Ransomware Resilience an.
"Ransomware Resilience-Benutzerverhaltensanzeige"	Zeigen Sie Warnungen und Einblicke zu verdächtigem Benutzerverhalten in Ransomware Resilience an.
SnapCenter -Administrator	Bietet die Möglichkeit, Snapshots von lokalen ONTAP Clustern mithilfe von NetApp Backup and Recovery für Anwendungen zu sichern. Ein Mitglied mit dieser Rolle kann die folgenden Aktionen ausführen: * Alle Aktionen unter „Sicherung und Wiederherstellung > Anwendungen“ ausführen * Alle Systeme in den Projekten und Ordnern verwalten, für die es Berechtigungen hat * Alle NetApp Console verwenden SnapCenter hat keine Viewer-Rolle.

Weiterführende Links

- "Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der NetApp Console"
- "Erste Schritte mit NetApp Console IAM"
- "Verwalten Sie NetApp Console Mitglieder und ihre Berechtigungen"
- "Erfahren Sie mehr über die API für NetApp Console IAM"

Plattformzugriffsrollen für die NetApp Console

Weisen Sie Benutzern Plattformrollen zu, um ihnen Berechtigungen zum Verwalten der NetApp Console, zum Zuweisen von Rollen, zum Hinzufügen von Benutzern, zum Erstellen von Konsolenagenten und zum Verwalten von Föderationen zu erteilen.

Beispiel für Organisationsrollen für eine große multinationale Organisation

Die XYZ Corporation organisiert den Datenspeicherzugriff nach Regionen – Nordamerika, Europa und Asien-Pazifik – und bietet regionale Kontrolle mit zentraler Aufsicht.

Der **Organisationsadministrator** in der Konsole der XYZ Corporation erstellt eine anfängliche Organisation und separate Ordner für jede Region. Der **Ordner- oder Projektadministrator** für jede Region organisiert Projekte (mit zugehörigen Ressourcen) innerhalb des Ordners der Region.

Regionale Administratoren mit der Rolle **Ordner- oder Projektadministrator** verwalten ihre Ordner aktiv, indem sie Ressourcen und Benutzer hinzufügen. Diese regionalen Administratoren können auch von ihnen verwaltete Ordner und Projekte hinzufügen, entfernen oder umbenennen. Der **Organisationsadministrator** erbt Berechtigungen für alle neuen Ressourcen und behält so die Übersicht über die Speichernutzung in der gesamten Organisation.

Innerhalb derselben Organisation wird einem Benutzer die Rolle **Föderationsadministrator** zugewiesen, um die Föderation der Organisation mit ihrem Unternehmens-IdP zu verwalten. Dieser Benutzer kann föderierte Organisationen hinzufügen oder entfernen, kann jedoch keine Benutzer oder Ressourcen innerhalb der Organisation verwalten. Der **Organisationsadministrator** weist einem Benutzer die Rolle **Föderationsbetrachter** zu, um den Föderationsstatus zu überprüfen und föderierte Organisationen anzuzeigen.

Die folgenden Tabellen zeigen die Aktionen, die jede Konsolenplattformrolle ausführen kann.

Rollen in der Organisationsverwaltung

Aufgabe	Organisationsadministrator	Ordner- oder Projektadministrator
Agenten erstellen	Ja	Nein
Erstellen, Ändern oder Löschen von Systemen über die Konsole (Hinzufügen oder Erkennen von Systemen)	Ja	Ja
Erstellen von Ordnern und Projekten, einschließlich Löschen	Ja	Nein
Vorhandene Ordner und Projekte umbenennen	Ja	Ja
Rollen zuweisen und Benutzer hinzufügen	Ja	Ja
Ressourcen mit Ordnern und Projekten verknüpfen	Ja	Ja

Aufgabe	Organisationsadministrator	Ordner- oder Projektadministrator
Agenten Ordnern und Projekten zuordnen	Ja	Nein
Agenten aus Ordnern und Projekten entfernen	Ja	Nein
Agenten verwalten (Zertifikate, Einstellungen usw. bearbeiten)	Ja	Nein
Verwalten Sie Anmeldeinformationen unter „Verwaltung > Anmeldeinformationen“.	Ja	Ja
Erstellen, Verwalten und Anzeigen von Föderationen	Ja	Nein
Registrieren Sie sich für den Support und reichen Sie Fälle über die Konsole ein	Ja	Ja
Verwenden Sie Datendienste, die keiner expliziten Zugriffsrolle zugeordnet sind	Ja	Ja
Anzeigen der Audit-Seite und Benachrichtigungen	Ja	Ja

Föderationsrollen

Aufgabe	Föderationsadministrator	Föderationsbetrachter
Erstellen einer Föderation	Ja	Nein
Verifizieren einer Domäne	Ja	Nein
Hinzufügen einer Domäne zu einem Verbund	Ja	Nein
Deaktivieren und Löschen von Föderationen	Ja	Nein
Testverbände	Ja	Nein
Verbände und deren Details anzeigen	Ja	Ja

Partnerschaftsrollen

Aufgabe	Partnerschaftsadministrator	Partnerschafts-Viewer
Kann eine Partnerschaft schaffen	Ja	Nein
Zuweisen von Rollen zu Partnermitgliedern	Ja	Nein
Kann Mitglieder zu einer Partnerschaft hinzufügen	Ja	Nein
Kann Details zur Organisationspartnerschaft anzeigen	Ja	Ja

Superadministrator- und Viewer-Rollen

Die Rolle **Superadministrator** bietet vollständigen Zugriff auf die Verwaltung von Konsolenfunktionen, Speicher und Datendiensten. Diese Rolle eignet sich für Personen, die für die Verwaltung und Governance zuständig sind. Im Gegensatz dazu bietet die Rolle „Super Viewer“ schreibgeschützten Zugriff, ideal für Prüfer oder Stakeholder, die Einblick benötigen, ohne Änderungen vorzunehmen.

Organisationen sollten den **Superadministrator**-Zugriff sparsam verwenden, um Sicherheitsrisiken zu minimieren und das Prinzip der geringsten Privilegien einzuhalten. Die meisten Organisationen sollten fein abgestufte Rollen mit nur den erforderlichen Berechtigungen zuweisen, um das Risiko zu verringern und die Überprüfbarkeit zu verbessern.

Beispiel für Superrollen

ABC Corporation verfügt über ein kleines fünfköpfiges Team, das die NetApp Console für Datendienste und Speicherverwaltung nutzt. Anstatt mehrere Rollen zu verteilen, weisen sie die Rolle des **Superadministrators** zwei leitenden Teammitgliedern zu, die alle Verwaltungsaufgaben übernehmen, einschließlich Benutzerverwaltung und Ressourcenkonfiguration. Den übrigen drei Teammitgliedern wird die Rolle „Super Viewer“ zugewiesen, die es ihnen ermöglicht, die Speicherintegrität und den Status des Datendienstes zu überwachen, ohne die Möglichkeit zu haben, Einstellungen zu ändern.

Rolle	Geerbte Rollen
Super-Admin	• Organisationsadministrator • Ordner- oder Projektadministrator • Föderationsadministrator • Partnerschaftsadministrator • Ransomware-Resilienz-Administrator • Notfallwiederherstellungsadministrator • Backup-Superadministrator • Speicheradministrator • Keystone -Administrator • Google Cloud NetApp Volumes Administrator
Super Viewer	• Organisationsanzeige • Föderationsbetrachter • Partnerschafts-Viewer • Ransomware Resilience-Viewer • Disaster Recovery-Viewer • Backup-Viewer • Speicheranzeige • Keystone -Viewer • Google Cloud NetApp Volumes Viewer

Anwendungsrollen

Google Cloud NetApp Volumes -Rollen in der NetApp Console

Sie können Benutzern die folgende Rolle zuweisen, um ihnen Zugriff auf die Google Cloud NetApp Volumes in der NetApp Console zu gewähren.

Google Cloud NetApp Volumes verwendet die folgende Rolle:

- * Google Cloud NetApp Volumes Administrator*: Entdecken und verwalten Sie Google Cloud NetApp Volumes in der Konsole.

Keystone -Zugriffsrollen in der NetApp Console

Keystone -Rollen bieten Zugriff auf die Keystone Dashboards und ermöglichen Benutzern das Anzeigen und Verwalten ihres Keystone Abonnements. Es gibt zwei Keystone -Rollen: Keystone -Administrator und Keystone Viewer. Der Hauptunterschied zwischen den beiden Rollen besteht in den Aktionen, die sie in Keystone ausführen können. Die Keystone Administratorrolle ist die einzige Rolle, die Serviceanfragen erstellen oder Abonnements ändern darf.

Beispiel für Keystone -Rollen in der NetApp Console

Bei der XYZ Corporation sind vier Speicheringenieure aus verschiedenen Abteilungen damit beschäftigt, die Keystone Abonnementinformationen anzuzeigen. Obwohl alle diese Benutzer das Keystone Abonnement überwachen müssen, darf nur der Teamleiter Serviceanfragen stellen. Drei Teammitglieder erhalten die Rolle „Keystone -Viewer“, während der Teamleiter die Rolle „Keystone Administrator“ erhält, sodass es einen Kontrollpunkt für die Serviceanfragen des Unternehmens gibt.

Die folgende Tabelle zeigt die Aktionen, die jede Keystone -Rolle ausführen kann.

Funktion und Aktion	Keystone -Administrator	Keystone -Viewer
Zeigen Sie die folgenden Registerkarten an: Abonnement, Assets, Monitor und Verwaltung	Ja	Ja
* Keystone -Abonnementseite*:		
Abonnements anzeigen	Ja	Ja
Abonnements ändern oder verlängern	Ja	Nein
* Keystone -Asset-Seite*:		
Assets anzeigen	Ja	Ja
Verwalten von Assets	Ja	Nein
* Keystone -Warnseite*:		
Warnungen anzeigen	Ja	Ja
Verwalten von Warnungen	Ja	Nein

Funktion und Aktion	Keystone -Administrator	Keystone -Viewer
Erstellen Sie Benachrichtigungen für sich selbst	Ja	Ja
* Licenses and subscriptions*:		
Kann Lizenzen und Abonnements anzeigen	Ja	Ja
* Keystone -Berichtsseite*:		
Berichte herunterladen	Ja	Ja
Berichte verwalten	Ja	Ja
Berichte für sich selbst erstellen	Ja	Ja
Serviceanfragen:		
Serviceanfragen erstellen	Ja	Nein
Zeigen Sie Serviceanfragen an, die von einem beliebigen Benutzer innerhalb der Organisation erstellt wurden	Ja	Ja

Zugriffsrolle „Operational Support Analyst“ für die NetApp Console

Sie können Benutzern die folgende Rolle zuweisen, um ihnen Zugriff auf Warnungen und Überwachung zu gewähren. Benutzer mit dieser Rolle können auch Supportfälle eröffnen.

Analyst für operative Unterstützung

Aufgabe	Kann durchführen
Verwalten Sie Ihre eigenen Benutzeranmeldeinformationen unter „Einstellungen > Anmeldeinformationen“.	Ja
Erkannte Ressourcen anzeigen	Ja
Registrieren Sie sich für den Support und reichen Sie Fälle über die Konsole ein	Ja
Ja	Anzeigen der Audit-Seite und Benachrichtigungen
Ja	Anzeigen, Herunterladen und Konfigurieren von Warnungen

Speicherzugriffsrollen für die NetApp Console

Sie können Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf die Speicherverwaltungsfunktionen in der NetApp Console zu gewähren. Sie können

Benutzern eine Administratorrolle zum Verwalten des Speichers oder eine Viewer-Rolle zum Überwachen zuweisen.

Diese Rollen sind über die NetApp Console Partnerschafts-API nicht verfügbar.

Administratoren können Benutzern Speicherrollen für die folgenden Speicherressourcen und -funktionen zuweisen:

Speicherressourcen:

- On-Premises- ONTAP -Cluster
- StorageGRID
- E-Series

Konsolendienste und -funktionen:

- Digitaler Berater
- Software-Updates
- Lebenszyklusplanung
- Nachhaltigkeit

Beispiel für Speicherrollen in der NetApp Console

XYZ Corporation, ein multinationales Unternehmen, verfügt über ein großes Team von Speicheringenieuren und Speicheradministratoren. Sie ermöglichen diesem Team die Verwaltung von Speicherressourcen für ihre Regionen und beschränken gleichzeitig den Zugriff auf zentrale Konsolenaufgaben wie Benutzerverwaltung, Agentenerstellung und Lizenzverwaltung.

Innerhalb eines 12-köpfigen Teams erhalten zwei Benutzer die Rolle „Speicherbetrachter“, die es ihnen ermöglicht, die Speicherressourcen zu überwachen, die mit den ihnen zugewiesenen Konsolenprojekten verknüpft sind. Den restlichen neun wird die Rolle „Storage-Admin“ zugewiesen, die die Möglichkeit umfasst, Software-Updates zu verwalten, über die Konsole auf ONTAP System Manager zuzugreifen und Speicherressourcen zu ermitteln (Systeme hinzuzufügen). Einer Person im Team wird die Rolle „Systemintegritätsspezialist“ zugewiesen, damit sie die Integrität der Speicherressourcen in ihrer Region verwalten, aber keine Systeme ändern oder löschen kann. Diese Person kann auch Software-Updates auf den Speicherressourcen für die ihr zugewiesenen Projekte durchführen.

Die Organisation verfügt über zwei weitere Benutzer mit der Rolle **Organisationsadministrator**, die alle Aspekte der Konsole verwalten können, einschließlich Benutzerverwaltung, Agentenerstellung und Lizenzverwaltung, sowie mehrere Benutzer mit der Rolle **Ordner- oder Projektadministrator**, die Konsolenverwaltungsaufgaben für die ihnen zugewiesenen Ordner und Projekte ausführen können.

Die folgende Tabelle zeigt die Aktionen, die jede Speicherrolle ausführt.

Funktion und Aktion	Speicheradministrator	Systemintegritätsspezialist	Speicheranzeige
Speicherverwaltung:			
Neue Ressourcen entdecken (Systeme erstellen)	Ja	Ja	Nein

Funktion und Aktion	Speicheradministrator	Systemintegritätsspezialist	Speicheranzeige
Erkannte Systeme anzeigen	Ja	Ja	Nein
Systeme aus der Konsole löschen	Ja	Nein	Nein
Systeme ändern	Ja	Nein	Nein
Agenten erstellen	Nein	Nein	Nein
Digitaler Berater			
Alle Seiten und Funktionen anzeigen	Ja	Ja	Ja
* Licenses and subscriptions*			
Alle Seiten und Funktionen anzeigen	Nein	Nein	Nein
Software-Updates			
Zielseite und Empfehlungen anzeigen	Ja	Ja	Ja
Überprüfen Sie mögliche Versionsempfehlungen und Hauptvorteile	Ja	Ja	Ja
Anzeigen von Updatedetails für einen Cluster	Ja	Ja	Ja
Führen Sie vor dem Update Prüfungen durch und laden Sie den Upgrade-Plan herunter	Ja	Ja	Ja
Installieren Sie Softwareupdates	Ja	Ja	Nein
Lebenszyklusplanung			
Überprüfen des Kapazitätsplanungsstatus	Ja	Ja	Ja
Nächste Aktion auswählen (Best Practice, Stufe)	Ja	Nein	Nein
Verteilen Sie kalte Daten in den Cloud-Speicher und geben Sie Speicherplatz frei	Ja	Ja	Nein
Erinnerungen einrichten	Ja	Ja	Ja
Nachhaltigkeit			
Dashboard und Empfehlungen anzeigen	Ja	Ja	Ja
Berichtsdaten herunterladen	Ja	Ja	Ja

Funktion und Aktion	Speicheradministrator	Systemintegritätsspezialist	Speicheranzeige
Prozentsatz der CO2-Minderung bearbeiten	Ja	Ja	Nein
Empfehlungen zur Fehlerbehebung	Ja	Ja	Nein
Empfehlungen aufschieben	Ja	Ja	Nein
Systemmanager-Zugriff			
Darf Anmeldeinformationen eingeben	Ja	Ja	Nein
Referenzen			
Benutzeranmeldeinformationen	Ja	Ja	Nein

Datendienstrollen

NetApp Backup and Recovery -Rollen in der NetApp Console

Sie können Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf NetApp Backup and Recovery innerhalb der Konsole zu gewähren. Mithilfe von Sicherungs- und Wiederherstellungsrollen können Sie Benutzern flexibel eine Rolle zuweisen, die speziell auf die Aufgaben zugeschnitten ist, die sie in Ihrem Unternehmen erledigen müssen. Wie Sie Rollen zuweisen, hängt von Ihren eigenen Geschäfts- und Speicherverwaltungspraktiken ab.

Der Dienst verwendet die folgenden Rollen, die spezifisch für NetApp Backup and Recovery sind.

- **Superadministrator für Backup und Wiederherstellung**: Führen Sie beliebige Aktionen in NetApp Backup and Recovery aus.
- **Backup- und Recovery-Backup-Administrator**: Führen Sie Sicherungen auf lokalen Snapshots durch, replizieren Sie auf sekundären Speicher und sichern Sie Aktionen auf Objektspeicher in NetApp Backup and Recovery.
- **Backup- und Recovery-Wiederherstellungsadministrator**: Stellen Sie Workloads mit NetApp Backup and Recovery wieder her.
- **Backup- und Recovery-Klonadministrator**: Klonen Sie Anwendungen und Daten mit NetApp Backup and Recovery.
- **Backup- und Recovery-Viewer**: Informationen in NetApp Backup and Recovery anzeigen, aber keine Aktionen ausführen.

Einzelheiten zu allen NetApp Console finden Sie unter "die Dokumentation zur Einrichtung und Verwaltung der Konsole" .

Für allgemeine Aktionen verwendete Rollen

Die folgende Tabelle zeigt die Aktionen, die jede NetApp Backup and Recovery -Rolle für alle Workloads ausführen kann.

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungsklon-Administrator	Backup- und Wiederherstellungs-Viewer
Hosts hinzufügen, bearbeiten oder löschen	Ja	Nein	Nein	Nein	Nein
Plugins installieren	Ja	Nein	Nein	Nein	Nein
Anmeldeinformationen hinzufügen (Host, Instanz, vCenter)	Ja	Nein	Nein	Nein	Nein
Dashboard und alle Registerkarten anzeigen	Ja	Ja	Ja	Ja	Ja
Kostenlose Testversion starten	Ja	Nein	Nein	Nein	Nein
Ermittlung von Workloads initiieren	Nein	Ja	Ja	Ja	Nein
Lizenzinformationen anzeigen	Ja	Ja	Ja	Ja	Ja
Lizenz aktivieren	Ja	Nein	Nein	Nein	Nein
Hosts anzeigen	Ja	Ja	Ja	Ja	Ja
Zeitpläne:					
Zeitpläne aktivieren	Ja	Ja	Ja	Ja	Nein
Zeitpläne aussetzen	Ja	Ja	Ja	Ja	Nein
Richtlinien und Schutz:					
Schutzpläne anzeigen	Ja	Ja	Ja	Ja	Ja
Erstellen, Ändern oder Löschen von Schutzplänen	Ja	Ja	Nein	Nein	Nein
Wiederherstellen von Workloads	Ja	Nein	Ja	Nein	Nein
Erstellen, Teilen oder Löschen von Klonen	Ja	Nein	Nein	Ja	Nein

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungsklon-Administrator	Backup- und Wiederherstellungs-Viewer
Richtlinie erstellen, ändern oder löschen	Ja	Ja	Nein	Nein	Nein
Berichte:					
Berichte anzeigen	Ja	Ja	Ja	Ja	Ja
Erstellen von Berichten	Ja	Ja	Ja	Ja	Nein
Berichte löschen	Ja	Nein	Nein	Nein	Nein
Von SnapCenter importieren und Host verwalten:					
Importierte SnapCenter -Daten anzeigen	Ja	Ja	Ja	Ja	Ja
Daten aus SnapCenter importieren	Ja	Ja	Nein	Nein	Nein
Host verwalten (migrieren)	Ja	Ja	Nein	Nein	Nein
Einstellungen konfigurieren:					
Konfigurieren des Protokollverzeichnisses	Ja	Ja	Ja	Nein	Nein
Instanzanmeldeinformationen zuordnen oder entfernen	Ja	Ja	Ja	Nein	Nein
Eimer:					
Buckets anzeigen	Ja	Ja	Ja	Ja	Ja
Bucket erstellen, bearbeiten oder löschen	Ja	Ja	Nein	Nein	Nein

Für Workload-spezifische Aktionen verwendete Rollen

Die folgende Tabelle zeigt die Aktionen, die jede NetApp Backup and Recovery -Rolle für bestimmte Workloads ausführen kann.

Kubernetes-Workloads

Diese Tabelle zeigt die Aktionen, die jede NetApp Backup and Recovery -Rolle für Aktionen ausführen kann, die spezifisch für Kubernetes-Workloads sind.

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungs-Viewer
Cluster, Namespaces, Speicherklassen und API-Ressourcen anzeigen	Ja	Ja	Ja	Ja
Neue Kubernetes-Cluster hinzufügen	Ja	Ja	Nein	Nein
Aktualisieren von Clusterkonfigurationen	Ja	Nein	Nein	Nein
Entfernen von Clustern aus der Verwaltung	Ja	Nein	Nein	Nein
Anwendungen anzeigen	Ja	Ja	Ja	Ja
Erstellen und Definieren neuer Anwendungen	Ja	Ja	Nein	Nein
Aktualisieren von Anwendungskonfigurationen	Ja	Ja	Nein	Nein
Entfernen von Anwendungen aus der Verwaltung	Ja	Ja	Nein	Nein
Anzeigen geschützter Ressourcen und Sicherungsstatus	Ja	Ja	Ja	Ja
Erstellen Sie Backups und schützen Sie Anwendungen mit Richtlinien	Ja	Ja	Nein	Nein
Schutz von Apps aufheben und Backups löschen	Ja	Ja	Nein	Nein
Anzeigen von Wiederherstellungspunkten und Ressourcen-Viewer-Ergebnissen	Ja	Ja	Ja	Ja

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungs-Viewer
Wiederherstellen von Anwendungen aus Wiederherstellungspunkten	Ja	Nein	Ja	Nein
Kubernetes-Sicherungsrichtlinien anzeigen	Ja	Ja	Ja	Ja
Erstellen von Kubernetes-Sicherungsrichtlinien	Ja	Ja	Ja	Nein
Aktualisieren der Sicherungsrichtlinien	Ja	Ja	Ja	Nein
Löschen von Sicherungsrichtlinien	Ja	Ja	Ja	Nein
Ausführungs-Hooks und Hook-Quellen anzeigen	Ja	Ja	Ja	Ja
Erstellen Sie Ausführungs-Hooks und Hook-Quellen	Ja	Ja	Ja	Nein
Aktualisieren von Ausführungs-Hooks und Hook-Quellen	Ja	Ja	Ja	Nein
Ausführungs-Hooks und Hook-Quellen löschen	Ja	Ja	Ja	Nein
Vorlagen für Ausführungs-Hooks anzeigen	Ja	Ja	Ja	Ja
Erstellen von Ausführungs-Hook-Vorlagen	Ja	Ja	Ja	Nein
Aktualisieren von Ausführungs-Hook-Vorlagen	Ja	Ja	Ja	Nein
Ausführungs-Hook-Vorlagen löschen	Ja	Ja	Ja	Nein
Übersicht über die Arbeitslast und Analyse-Dashboards anzeigen	Ja	Ja	Ja	Ja

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungs-Viewer
StorageGRID -Buckets und Speicherziele anzeigen	Ja	Ja	Ja	Ja

NetApp Disaster Recovery Rollen in der NetApp Console

Sie können Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf NetApp Disaster Recovery innerhalb der Konsole zu gewähren. Mithilfe von Disaster Recovery-Rollen können Sie Benutzern flexibel Rollen zuweisen, die speziell auf die Aufgaben zugeschnitten sind, die sie in Ihrer Organisation erledigen müssen. Wie Sie Rollen zuweisen, hängt von Ihren eigenen Geschäfts- und Speicherverwaltungspraktiken ab.

Disaster Recovery verwendet die folgenden Rollen:

- **Notfallwiederherstellungsadministrator**: Führen Sie alle Aktionen aus.
- **Disaster Recovery Failover-Administrator**: Führen Sie Failover und Migrationen durch.
- **Administrator der Notfallwiederherstellungsanwendung**: Erstellen Sie Replikationspläne. Replikationspläne ändern. Starten Sie Test-Failover.
- **Disaster Recovery Viewer**: Nur Informationen anzeigen.

Die folgende Tabelle zeigt die Aktionen, die jede Rolle ausführen kann.

Funktion und Aktion	Notfallwiederherstellungsadministrator	Administrator für Notfallwiederherstellungs-Failover	Administrator der Notfallwiederherstellungsanwendung	Disaster Recovery-Viewer
Dashboard und alle Registerkarten anzeigen	Ja	Ja	Ja	Ja
Kostenlose Testversion starten	Ja	Nein	Nein	Nein
Ermittlung von Workloads initiieren	Ja	Nein	Nein	Nein
Lizenzinformationen anzeigen	Ja	Ja	Ja	Ja
Lizenz aktivieren	Ja	Nein	Ja	Nein
Auf der Registerkarte „Sites“:				
Websites anzeigen	Ja	Ja	Ja	Ja

Funktion und Aktion	Notfallwiederherstellungsadministrator	Administrator für Notfallwiederherstellungs-Failover	Administrator der Notfallwiederherstellungsanwendung	Disaster Recovery-Viewer
Hinzufügen, Ändern oder Löschen von Sites	Ja	Nein	Nein	Nein
Auf der Registerkarte Replikationspläne:				
Replikationspläne anzeigen	Ja	Ja	Ja	Ja
Anzeigen von Replikationsplandetails	Ja	Ja	Ja	Ja
Erstellen oder Ändern von Replikationsplänen	Ja	Ja	Ja	Nein
Erstellen von Berichten	Ja	Nein	Nein	Nein
Snapshots anzeigen	Ja	Ja	Ja	Ja
Durchführen von Failover-Tests	Ja	Ja	Ja	Nein
Durchführen von Failovers	Ja	Ja	Nein	Nein
Failbacks durchführen	Ja	Ja	Nein	Nein
Migrationen durchführen	Ja	Ja	Nein	Nein
Auf der Registerkarte „Ressourcengruppen“:				
Anzeigen von Ressourcengruppen	Ja	Ja	Ja	Ja
Erstellen, Ändern oder Löschen von Ressourcengruppen	Ja	Nein	Ja	Nein
Auf der Registerkarte „Jobüberwachung“:				
Jobs anzeigen	Ja	Nein	Ja	Ja
Aufträge abbrechen	Ja	Ja	Ja	Nein

Ransomware Resilience-Zugriffsrollen für die NetApp Console

Ransomware Resilience-Rollen bieten Benutzern Zugriff auf NetApp Ransomware Resilience. Die beiden Rollen sind Ransomware-Schutzadministrator und Ransomware-Schutzbetrachter. Der Hauptunterschied zwischen den beiden Rollen besteht in den Aktionen, die sie im Rahmen der Ransomware-Resilienz durchführen können.

Die folgende Tabelle zeigt die Aktionen, die jede Rolle ausführen kann.

Funktion und Aktion	Ransomware-Resilienz-Administrator	Ransomware Resilience-Viewer	Ransomware Resilience-Benutzerverhaltensadministrator	Ransomware Resilience-Benutzerverhaltensanzeige
Dashboard und alle Registerkarten anzeigen	Ja	Ja	Nein	Nein
Aktualisieren Sie den Empfehlungsstatus auf dem Dashboard	Ja	Nein	Nein	Nein
Kostenlose Testversion starten	Ja	Nein	Nein	Nein
Ermittlung von Workloads initiieren	Ja	Nein	Nein	Nein
Neuermittlung von Workloads einleiten	Ja	Nein	Nein	Nein
Auf der Registerkarte „Schützen“:				
Schutzpläne hinzufügen, ändern oder löschen	Ja	Nein	Nein	Nein
Workloads schützen	Ja	Nein	Nein	Nein
Identifizieren Sie die Gefährdung sensibler Daten	Ja	Nein	Nein	Nein
Listen Sie Schutzpläne und Details auf	Ja	Ja	Nein	Nein
Auflisten von Schutzgruppen	Ja	Ja	Nein	Nein
Anzeigen von Schutzgruppendetails	Ja	Ja	Nein	Nein
Schutzgruppe erstellen, bearbeiten oder löschen	Ja	Nein	Nein	Nein
Daten herunterladen	Ja	Ja	Nein	Nein
Auf der Registerkarte „Warnungen“:				
Anzeigen von Warnungen und Warnungsdetails	Ja	Ja	Nein	Nein
Vorfallstatus bearbeiten	Ja	Nein	Nein	Nein
Alarm zur Wiederherstellung markieren	Ja	Nein	Nein	Nein
Vorfalldetails anzeigen	Ja	Ja	Nein	Nein
Vorfälle verwerfen oder lösen	Ja	Nein	Nein	Nein

Funktion und Aktion	Ransomware-Resilienz-Administrator	Ransomware Resilience-Viewer	Ransomware Resilience-Benutzerverhaltensadministrator	Ransomware Resilience-Benutzerverhaltensanzeige
Benutzer blockieren	Ja	Nein	Nein	Nein
Vollständige Liste der betroffenen Dateien abrufen	Ja	Nein	Nein	Nein
Warndaten herunterladen	Ja	Ja	Nein	Nein
Anzeigen verdächtiger Benutzeraktivitäten	Nein	Nein	Ja	Ja
Auf der Registerkarte „Wiederherstellen“:				
Betroffene Dateien herunterladen	Ja	Nein	Nein	Nein
Workload wiederherstellen	Ja	Nein	Nein	Nein
Wiederherstellungsdaten herunterladen	Ja	Ja	Nein	Nein
Berichte herunterladen	Ja	Ja	Nein	Nein
Auf der Registerkarte „Einstellungen“:				
Hinzufügen oder Ändern von Sicherungszielen	Ja	Nein	Nein	Nein
Auflisten der Sicherungsziele	Ja	Ja	Nein	Nein
Verbundene SIEM-Ziele anzeigen	Ja	Ja	Nein	Nein
SIEM-Ziele hinzufügen oder ändern	Ja	Nein	Nein	Nein
Bereitschaftsübung konfigurieren	Ja	Nein	Nein	Nein
Starten Sie die Bereitschaftsübung	Ja	Nein	Nein	Nein
Übung zur Reset-Bereitschaft	Ja	Nein	Nein	Nein
Bereitschaftsübung bearbeiten	Ja	Nein	Nein	Nein
Status der Bereitschaftsübung überprüfen	Ja	Ja	Nein	Nein
Aktualisieren der Erkennungskonfiguration	Ja	Nein	Nein	Nein

Funktion und Aktion	Ransomware-Resilienz-Administrator	Ransomware Resilience-Viewer	Ransomware Resilience-Benutzerverhaltensadministrator	Ransomware Resilience-Benutzerverhaltensanzeige
Anzeigen der Erkennungskonfiguration	Ja	Ja	Nein	Nein
Konfigurieren Sie Einstellungen für verdächtiges Benutzerverhalten	Nein	Nein	Ja	Nein
Auf der Registerkarte „Berichte“:				
Berichte herunterladen	Ja	Ja	Nein	Nein

Partnerorganisationen

Partnerschaften in der NetApp Console

Durch die Schaffung von Partnerschaften zwischen Organisationen ermöglicht die NetApp Console Partnern die sichere Verwaltung von NetApp Ressourcen über Organisationsgrenzen hinweg, wodurch die Zusammenarbeit optimiert und die Sicherheit verbessert wird.

Erforderliche Rollen

Partnerschaftsadministrator"Erfahren Sie mehr über Zugriffsrollen."

Partnerschaften ermöglichen die sichere Verwaltung von NetApp -Ressourcen in verschiedenen Organisationen mithilfe rollenbasierter Beziehungen in der Konsole. Die initiierende Organisation gewährt Zugriff auf ihre Ressourcen, während die akzeptierende Organisation die Benutzer oder Dienstkonten bereitstellt, denen Zugriff gewährt werden soll. Partnerschaften werden über einen Self-Service-Workflow eingerichtet, der der initiierenden Organisation die volle Kontrolle darüber gibt, welche Ressourcen gemeinsam genutzt und welche Rollen zugewiesen werden. Außerdem hat sie die Möglichkeit, den Partnerzugriff nach Bedarf zu integrieren, zu verwalten oder zu widerrufen.

Kunden können MSPs oder Wiederverkäufer zur Verwaltung von NetApp -Umgebungen autorisieren, ohne dass komplizierte Setups erforderlich sind. Kunden können steuern, auf welche Cluster Partner zugreifen können und welche Rollen sie haben. Außerdem können sie den Zugriff jederzeit widerrufen, um die Sicherheit und Compliance aufrechtzuerhalten.

Als Partner erhalten Sie zentrale Transparenz und Kontrolle über alle Kundenumgebungen. Sie können problemlos zur Organisation eines Kunden wechseln, um Ressourcen zu verwalten, Datendienste auszuführen und den Zustand innerhalb definierter Grenzen zu überwachen. Dadurch wird der Bedarf an benutzerdefinierten Tools reduziert und die Übereinstimmung mit den Richtlinien jedes Kunden sichergestellt.

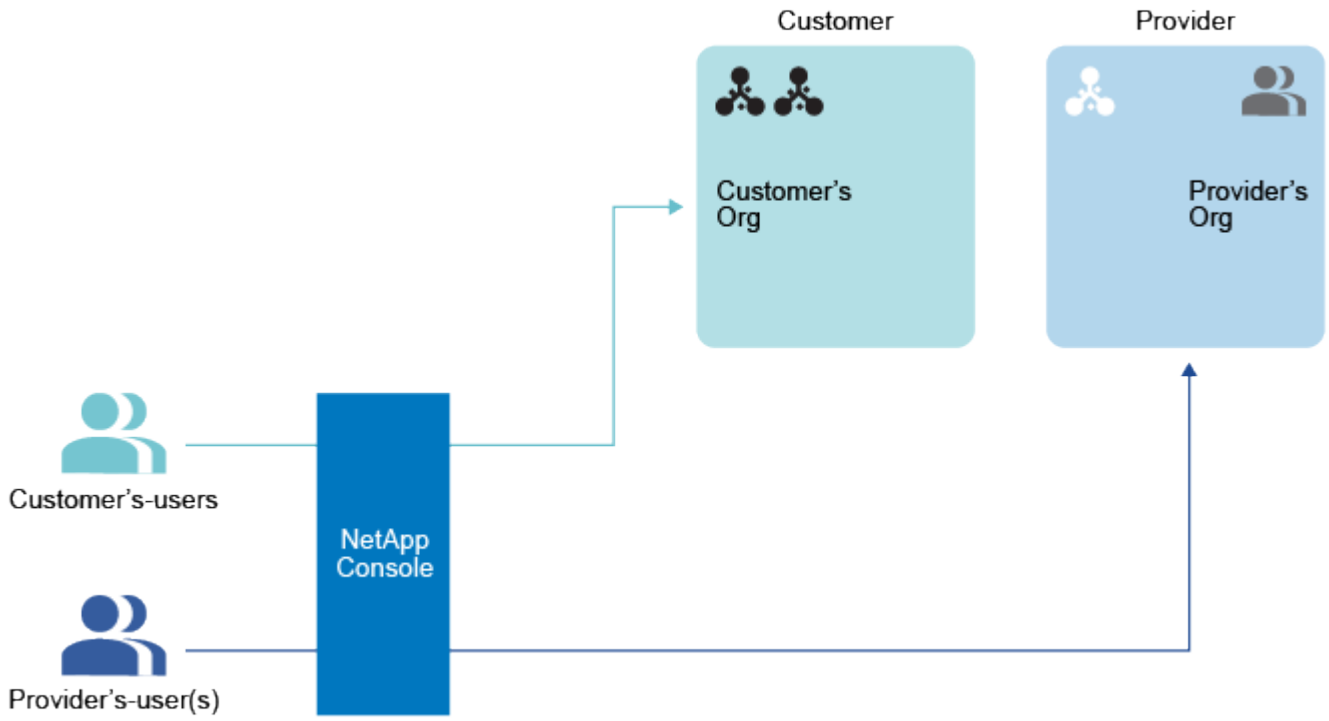
1. **Weisen Sie einem oder mehreren Benutzern die Rolle „Partnerschaftsadministrator“ zu.**

Weisen Sie einem oder mehreren Benutzern in der initiierenden und der empfangenden Organisation die Rolle „Partnerschaftsadministrator“ zu, um Partnerschaften zu erstellen und zu verwalten. Sie können die Rolle „Partnerschaftsbetrachter“ Benutzern zuweisen, die Partnerschaften nur anzeigen, aber nicht verwalten müssen.

2 Teilen Sie Ihre Organisations-ID mit der initiierenden Organisation

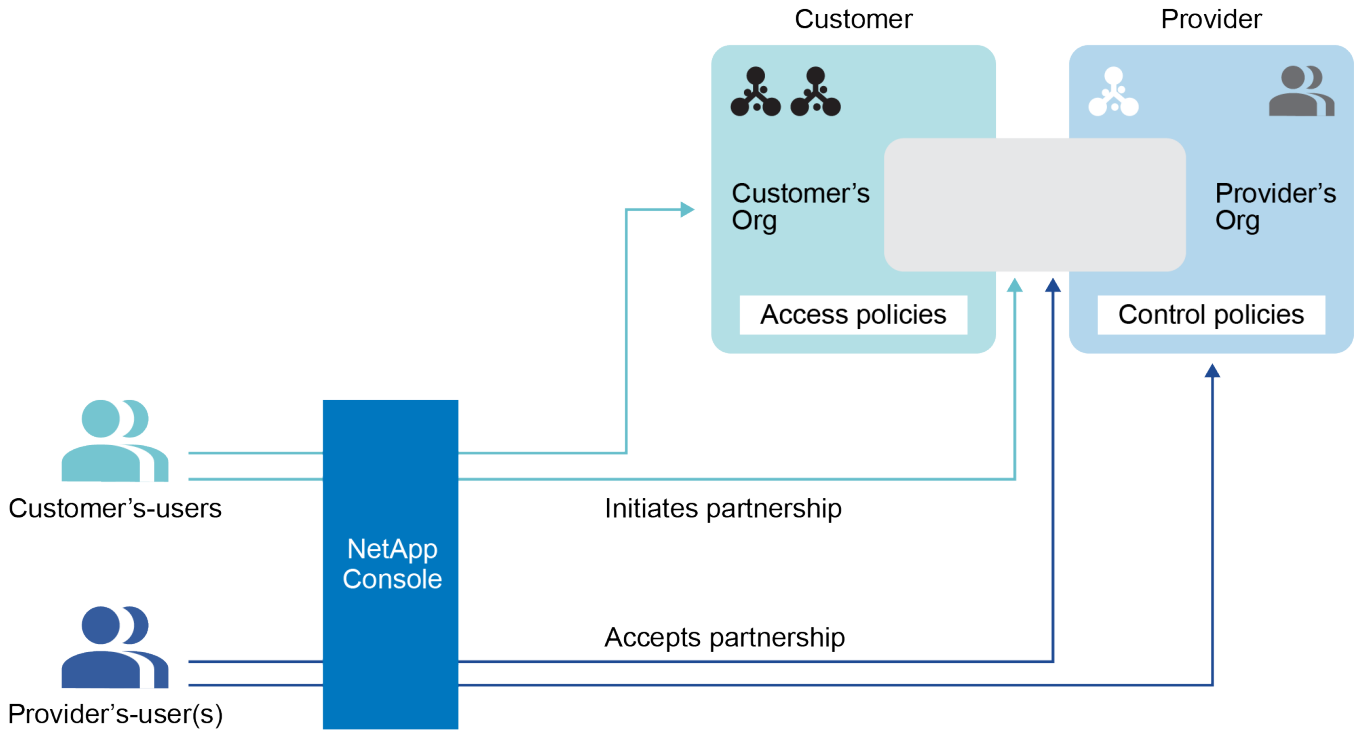
Um eine Partnerschaft zu initiieren, muss der Initiator die Organisations-ID der Zielorganisation kennen. Auf diese Organisations-ID kann nur die jeweilige Organisation zugreifen. Geben Sie es direkt per E-Mail oder auf andere Weise außerhalb der NetApp Console an die initiierende Organisation weiter.

Die initiierende Organisation ist die Organisation, die Zugriff auf ihre Ressourcen gewährt.



3 Initiieren Sie die Partnerschaft innerhalb der NetApp Console

Die Organisation, die die Partnerschaft initiiert, tut dies innerhalb der NetApp Console, indem sie eine Partnerschaftsanfrage sendet.



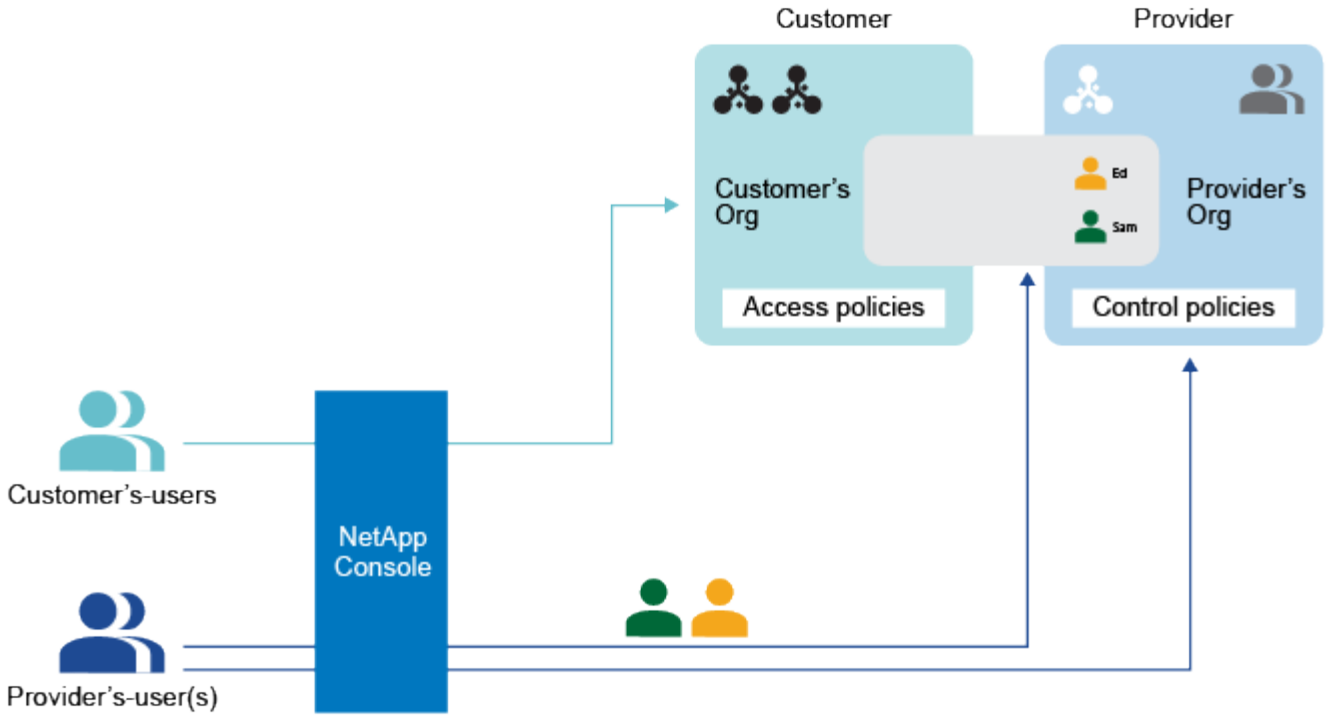
4 **Genehmigen Sie die Partnerschaft**

Die empfangende Organisation muss die Anfrage annehmen.

Die empfangende Organisation ist die Organisation, der Zugriff auf Ressourcen gewährt wird.

5 **Zuweisen von Benutzern zur Partnerschaft**

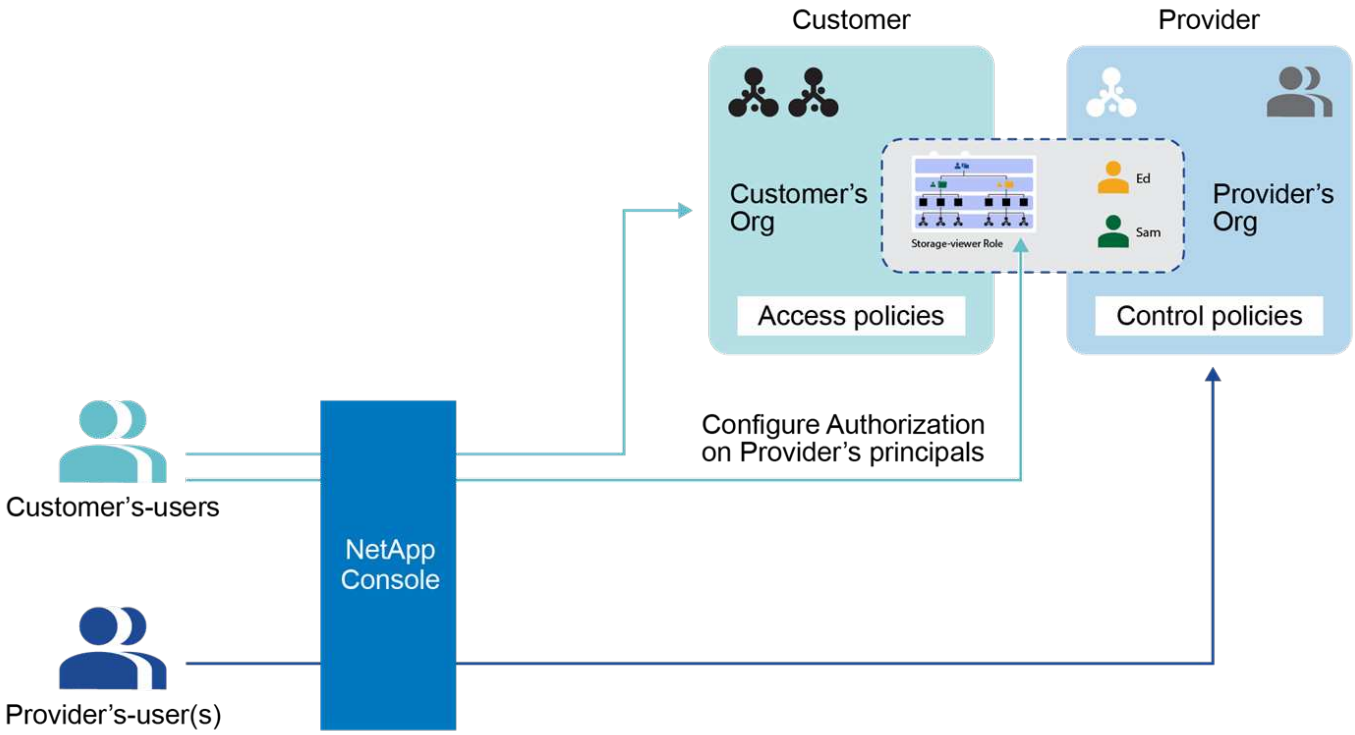
Die empfangende Organisation weist der Partnerschaft bestimmte Benutzer oder Dienstkonten aus Ihrer Organisation zu. Die initiierende Organisation weist diesen Benutzern Rollen zu.



6 **Gewähren Sie zugewiesenen Benutzern Zugriff auf Ressourcen**

Wenn Sie die initiierende Organisation sind, können Sie den Benutzern, die der Partnerschaft zugewiesen wurden, Zugriff auf bestimmte Ressourcen gewähren. Sie können den Zugriff jederzeit widerrufen.

Dies erreichen Sie, indem Sie Rollen für bestimmte Projekte oder Ordner innerhalb Ihrer Organisation zuweisen.



Verwalten Sie Partnerschaften in der NetApp Console

Bauen Sie Partnerschaften auf, um sichere, verwaltete Verbindungen zwischen Ihrem Unternehmen und vertrauenswürdigen Partnern für ein kollaboratives NetApp Ressourcenmanagement herzustellen.

Durch Partnerschaften können Sie NetApp -Ressourcen über Grenzen hinweg sicher verwalten, indem Sie rollenbasierte Beziehungen in der Konsole nutzen. Die initiierende Organisation gewährt Zugriff auf ihre Ressourcen, während die akzeptierende Organisation die Benutzer oder Dienstkonten bereitstellt, denen Zugriff gewährt werden soll. Partnerschaften werden über einen Self-Service-Workflow eingerichtet, der der initiierenden Organisation die volle Kontrolle darüber gibt, welche Ressourcen gemeinsam genutzt und welche Rollen zugewiesen werden. Außerdem hat sie die Möglichkeit, den Partnerzugriff nach Bedarf zu integrieren, zu verwalten oder zu widerrufen.

Erforderliche Rollen

Zum Erstellen und Verwalten von Partnerschaften ist die Rolle **Partnerschaftsadministrator** erforderlich. Der **Partnerschaftsbetrachter** kann die Seite „Partnerschaften“ anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Initiieren Sie eine Organisationspartnerschaft

Sie können eine Partnerschaft mit einer anderen Organisation beantragen, wenn Sie deren Organisations-ID kennen. Die empfangende Organisation genehmigt die Anfrage, bevor die Partnerschaft fortgesetzt werden kann.

Bevor Sie beginnen, stellen Sie sicher, dass Sie über die Organisations-ID der Partnerorganisation verfügen und dass Ihnen die Rolle **Partnerschaftsadministrator** zugewiesen wurde.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.

2. Wählen Sie die Registerkarte **Partnerschaften**.
3. Wählen Sie **Partnerschaft hinzufügen**.
4. Geben Sie im Dialogfeld **Partnerschaft erstellen** die Partnerorganisations-ID des gewünschten Partners ein und wählen Sie **Hinzufügen**.

   Die Partnerschaftsanfrage wird zur Genehmigung an die Partnerorganisation gesendet. Den Status der Partnerschaftsanfrage können Sie auf der Seite **Partnerschaften** einsehen.

Genehmigen einer Organisationspartnerschaft

Eine Anfrage für eine Organisationspartnerschaft muss von der empfangenden Organisation angenommen werden, bevor die Partnerschaft fortgesetzt werden kann. Sie müssen über die Rolle **Partnerschaftsadministrator** verfügen, um Partnerschaften zu genehmigen und zu verwalten.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Partnerschaften** aus.
3. Wählen Sie die Registerkarte **Partnerschaft erhalten**.
4. Navigieren Sie zu der empfangenen Partnerschaft, die Sie genehmigen möchten, und wählen Sie ••• und wählen Sie dann **Genehmigen**.
5. Überprüfen Sie die Details der Partnerschaft, einschließlich des Namens und der Organisations-ID der Organisation, die die Partnerschaft angefordert hat, und wählen Sie **Weiter** aus.
6. Fügen Sie optional Organisationsmitglieder zur Partnerschaft hinzu und wählen Sie **Übernehmen**.

   Sie können jederzeit weitere Mitglieder über die Seite **Partnerschaft** hinzufügen.

   Alle von Ihnen hinzugefügten Mitglieder werden in der Organisation des Partners sichtbar, wo der Partner sie Ressourcen zuweisen kann.

Ergebnis

Die von Ihnen genehmigte Partnerschaft weist jetzt den Status **Etabliert** auf. Benutzer mit der Rolle **Partnerschaftsadministrator** oder **Partnerschaftsbetrachter** in einer der beiden Organisationen können die Partnerschaft anzeigen.

Partnerschaftsstatus anzeigen

Sehen Sie sich den Status Ihrer Partnerschaften an.

Erforderliche Rolle

Partnerschaftsadministrator, Partnerschaftsbetrachter."Erfahren Sie mehr über Zugriffsrollen."

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die **Partnerschaften** aus.
3. Wählen Sie entweder die Registerkarte **Initiierte Partnerschaften** oder **Erhaltene Partnerschaften**.
4. Sehen Sie sich die jeweilige Tabelle an, in der Partnerschaften und deren Status angezeigt werden.

Deaktivieren einer Organisationspartnerschaft

Um eine Partnerschaft zu deaktivieren, müssen Sie Mitglied der initiierenden Organisation sein. Durch die Deaktivierung einer Partnerschaft wird der Zugriff auf alle Ressourcen in Ihrer Organisation, die mit der Partnerorganisation geteilt wurden, sofort widerrufen.

Erforderliche Rolle

Partnerschaftsverwaltung."Erfahren Sie mehr über Zugriffsrollen."

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die **Partnerschaften** aus.
3. Wählen Sie entweder die Registerkarte **Initiierte Partnerschaften** aus.
4. Sehen Sie sich die jeweilige Tabelle an, in der Partnerschaften und deren Status angezeigt werden.
5. Navigieren Sie zu der initiierten Partnerschaft, die Sie deaktivieren möchten, und wählen Sie ••• und wählen Sie dann **Deaktivieren**.

Mitglieder für eine Partnerschaftsorganisation verwalten

Sie können Benutzer zu einer Partnerschaft hinzufügen, indem Sie sie der Partnerorganisation hinzufügen. Nachdem Sie Benutzer hinzugefügt haben, ist die Partnerorganisation dafür verantwortlich, ihnen Rollen für bestimmte Ressourcen in ihrer Organisation zuzuweisen.

Erforderliche Rollen

Zum Erstellen und Verwalten von Partnerschaften ist die Rolle **Partnerschaftsadministrator** erforderlich. Der **Partnerschaftsbetrachter** kann die Seite „Partnerschaften“ anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Sie können Benutzer jederzeit aus einer Partnerschaft entfernen. Durch das Entfernen eines Benutzers aus einer Partnerschaft wird dessen Zugriff auf alle Ressourcen in der Partnerorganisation sofort widerrufen.

Mitglieder zu einer Partnerschaft hinzufügen

Wenn Sie einer Partnerschaft Mitglieder hinzufügen, muss der **Partnerschaftsadministrator** der Partnerorganisation ihnen Rollen für bestimmte Ressourcen in seiner Organisation zuweisen, bevor sie auf diese Ressourcen zugreifen können.

Nachdem Sie Mitglieder zu einer Partnerschaft hinzugefügt haben, werden die Mitglieder als Mitglieder in der Partnerorganisation angezeigt, wo der Partner sie Ressourcen zuweisen kann.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Partnerschaften** aus.
3. Wählen Sie die Registerkarte **Partnerschaft erhalten**.
4. Wählen Sie das Aktionsmenü ••• neben der bestehenden Partnerschaft, der Sie Mitglieder hinzufügen möchten, und wählen Sie **Mitglieder hinzufügen**.
5. Wählen Sie ein oder mehrere Mitglieder aus, die Sie der Partnerschaft hinzufügen möchten, und wählen Sie **Hinzufügen**.

Mitglieder aus einer Partnerschaft entfernen

Sie können Mitglieder jederzeit aus einer Partnerschaft entfernen. Durch das Entfernen eines Benutzers aus einer Partnerschaft wird dessen Zugriff auf alle Ressourcen in der Partnerorganisation sofort widerrufen.

Wenn Sie die Rolle eines Mitglieds oder die Ressourcen, auf die es zugreifen kann, anpassen möchten, muss der Partnerschaftsadministrator der Partnerorganisation diese Änderungen vornehmen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Partnerschaften** aus.
3. Wählen Sie die Registerkarte **Partnerschaft erhalten**.
4. Wählen Sie das Aktionsmenü ••• neben dem Mitglied, das Sie entfernen möchten, und wählen Sie **Zuordnung entfernen**.
5. Bestätigen Sie die Aktion, indem Sie im Dialogfeld **Entfernen** auswählen.

Anzeigen von Rolleninformationen für einen Benutzer

Sie können die einem Benutzer zugewiesene Rolle und die zugehörigen Ressourcen anzeigen.

Sie können die einem Benutzer zugeordnete Rolle nicht ändern. Wenn Sie Fragen zu den Ressourcen oder der bereitgestellten Rolle haben, wenden Sie sich an den Administrator der Partnerorganisation.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Partnerschaften** aus.
3. Wählen Sie die Registerkarte **Partnerschaft erhalten**.
4. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.
5. Erweitern Sie in der Tabelle die jeweilige Zeile für die Organisation, den Ordner oder das Projekt, in der Sie die zugewiesene Rolle des Mitglieds anzeigen möchten, und wählen Sie die Nummer in der Spalte **Rolle** aus.

Gewähren Sie Partnerschaftsbenutzern Zugriff auf Ressourcen

Sie können Partnerschaftsbenutzern Zugriff gewähren, indem Sie ihnen bestimmte Rollen für Ordner und Projekte innerhalb Ihrer Organisation zuweisen.

Erforderliche Rollen

Partnerschaftsverwaltung."Erfahren Sie mehr über Zugriffsrollen."

Eine Partnerorganisation muss zunächst Mitglieder zur Partnerschaft hinzufügen, bevor Sie ihnen Rollen für Ressourcen in Ihrer Organisation zuweisen können."Erfahren Sie, wie Sie einer Partnerschaft Mitglieder hinzufügen."

Verstehen Sie die Rollen für Partnerschaftsbenutzer

Sie können Rollen für Mitglieder von Partnerorganisationen auf dieselbe Weise verwalten wie für Ihre eigenen. Allerdings stehen Partnerschaftsbenutzern nicht alle Rollen zur Verfügung. Insbesondere können Sie Partnerbenutzern keine Rolle zuweisen, die Softwareupdates zulässt. Das Aktualisieren der ONTAP -Software

erfordert im Allgemeinen direkten Netzwerkzugriff.

Sie können Partnerbenutzern folgende Rollen zuweisen:

- "Organisationsadministrator"
- "Ordner- oder Projektadministrator"
- "Föderationsadministrator"
- "Föderationsbetrachter"
- "Backup- und Wiederherstellungsadministrator"
- "Backup-Viewer"
- "Administrator wiederherstellen"
- "Klonadministrator"
- "Notfallwiederherstellungsadministrator"
- "Administrator für Notfallwiederherstellungs-Failover"
- "Administrator der Notfallwiederherstellungsanwendung"
- "Disaster Recovery-Viewer"
- "Betriebsunterstützungsanalyst"
- "Klassifizierungsanzeige"

"Erfahren Sie mehr über vordefinierte Rollen"

Einem Partnerbenutzer eine Rolle hinzufügen

Sie gewähren Zugriff auf die Ressourcen Ihrer Organisation, indem Sie einem Mitglied eine Rolle zuweisen. Wenn Sie eine Rolle zuweisen, geben Sie eine Ressource und eine Rolle an. Sie können einem Benutzer mehr als eine Rolle zuweisen.

Wenn Sie beispielsweise zwei Projekte hätten und möchten, dass derselbe Benutzer für beide die Rolle des Backup- und Wiederherstellungsadministrators hat, müssten Sie dem Benutzer für jedes Projekt die Rolle zuweisen. Wenn Sie einem Benutzer für dasselbe Projekt zwei verschiedene Rollen zuweisen möchten, müssen Sie ihm jede Rolle separat zuweisen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Partnerschaften** aus.
3. Wählen Sie die Registerkarte **Partnerschaft initiiert**.
4. Wählen Sie das Aktionsmenü ••• neben der bestehenden Partnerschaft, die Sie anzeigen möchten, und wählen Sie **Details anzeigen** aus.

   In der Liste **Mitglieder** werden die Mitglieder angezeigt, die die Partnerorganisation zur Partnerschaft hinzugefügt hat.

5. Wählen Sie das Aktionsmenü ••• neben dem Mitglied, dem Sie eine Rolle zuweisen möchten, und wählen Sie **Rolle hinzufügen** aus.
6. Um eine Rolle hinzuzufügen, führen Sie die Schritte im Dialogfeld aus:
   - **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**: Wählen Sie die Ebene Ihrer

Ressourcenhierarchie aus, für die das Mitglied Berechtigungen haben soll.

Wenn Sie die Organisation oder einen Ordner auswählen, verfügt das Mitglied über Berechtigungen für alles, was sich innerhalb der Organisation oder des Ordners befindet.

- **Kategorie auswählen**: Wählen Sie eine Rollenkategorie. "Informationen zu Zugriffsrollen" .
- Wählen Sie eine **Rolle**: Wählen Sie eine Rolle, die dem Mitglied Berechtigungen für die Ressourcen erteilt, die mit der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt verknüpft sind.
- **Rolle hinzufügen**: Wenn Sie Zugriff auf zusätzliche Ordner oder Projekte innerhalb Ihrer Organisation gewähren möchten, wählen Sie **Rolle hinzufügen**, geben Sie einen weiteren Ordner oder ein weiteres Projekt oder eine weitere Rollenkategorie an und wählen Sie dann eine Rollenkategorie und eine entsprechende Rolle aus.

7. Wählen Sie **Neue Rollen hinzufügen**.

Ändern oder Entfernen einer Rolle eines Partnerbenutzers

Sie können eine Rolle ändern oder entfernen, die Sie einem Mitglied einer Partnerorganisation zugewiesen haben.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Partnerschaften** aus.
3. Wählen Sie die Registerkarte **Partnerschaft initiiert**.
4. Wählen Sie das Aktionsmenü ••• neben der bestehenden Partnerschaft, die Sie anzeigen möchten, und wählen Sie **Details anzeigen** aus.

   In der Liste **Mitglieder** werden die Mitglieder angezeigt, die die Partnerorganisation zur Partnerschaft hinzugefügt hat.

5. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.
6. Erweitern Sie in der Tabelle die jeweilige Zeile für die Organisation, den Ordner oder das Projekt, in dem Sie die zugewiesene Rolle des Mitglieds ändern möchten, und wählen Sie in der Spalte **Rolle Anzeigen** aus, um die diesem Mitglied zugewiesenen Rollen anzuzeigen.
7. Sie können eine vorhandene Rolle für ein Mitglied ändern oder eine Rolle entfernen.
   a. Um die Rolle eines Mitglieds zu ändern, wählen Sie **Ändern** neben der Rolle, die Sie ändern möchten. Sie können eine Rolle nur in eine Rolle innerhalb derselben Rollenkategorie ändern. Sie können beispielsweise von einer Datendienstrolle zu einer anderen wechseln. Bestätigen Sie die Änderung.
   b. Um die Rolle eines Mitglieds aufzuheben, wählen Sie 🗑 neben der Rolle, um dem Mitglied die jeweilige Rolle zu entziehen. Sie werden aufgefordert, die Entfernung zu bestätigen.

Arbeit in einer Partnerorganisation

Sobald Ihnen eine Rolle in einer Partnerorganisation zugewiesen wurde, können Sie zu dieser Organisation wechseln und Aktionen ausführen, für die Sie die Berechtigung haben.

Verwenden Sie das Menü „Organisation“, um zwischen Ihren Organisationen und allen Partnerorganisationen zu wechseln, auf die Sie Zugriff haben."Erfahren Sie mehr über den Wechsel von Organisationen und

Projekten."

Sie können die Ressourcen sehen, die in der Partnerorganisation mit Ihnen geteilt wurden, und Aktionen basierend auf der Ihnen zugewiesenen Rolle ausführen. Arbeiten Sie mit Ihrem Partnerschaftsadministrator zusammen, um sicherzustellen, dass Sie über die entsprechende Rolle für die Ressourcen verfügen, auf die Sie zugreifen müssen.

Identitätsföderation

Aktivieren Sie Single Sign-On durch die Verwendung der Identitätsföderation mit der NetApp Console

Single-Sign-On (Föderation) vereinfacht den Anmeldevorgang und erhöht die Sicherheit, indem Benutzer sich mit ihren Unternehmensanmeldeinformationen bei der NetApp Console anmelden können. Sie können Single Sign-On (SSO) bei Ihrem Identitätsanbieter (IdP) oder über die NetApp Support-Site aktivieren.

Erforderliche Rolle

Organisationsadministrator, Föderationsadministrator, Föderationsbetrachter."Erfahren Sie mehr über Zugriffsrollen."

Identitätsföderation mit der NetApp -Support-Site

Durch die Verbindung mit der NetApp -Support-Site können sich Benutzer mit denselben Anmeldeinformationen bei der Konsole, Active IQ Digital Advisor und anderen zugehörigen Apps anmelden.

> Wenn Sie eine Verbindung mit der NetApp -Support-Site herstellen, können Sie nicht gleichzeitig eine Verbindung mit Ihrem Corporate Identity Management-Anbieter herstellen. Wählen Sie die Option aus, die für Ihr Unternehmen am besten geeignet ist.

Schritte

1. Laden Sie die "NetApp Federation-Antragsformular" .
2. Senden Sie das Formular an die im Formular angegebene E-Mail-Adresse.

   Das NetApp Supportteam prüft und bearbeitet Ihre Anfrage.

Richten Sie eine Verbundverbindung mit Ihrem Identitätsanbieter ein

Sie können eine Verbundverbindung mit Ihrem Identitätsanbieter einrichten, um Single Sign-On (SSO) für die Konsole zu aktivieren. Der Vorgang umfasst die Konfiguration Ihres Identitätsanbieters, sodass dieser NetApp als Dienstanbieter vertraut, und die anschließende Herstellung der Verbindung in der Konsole.

> Wenn Sie die Föderation zuvor mit NetApp Cloud Central (einer externen Anwendung der Konsole) konfiguriert haben, müssen Sie Ihre Föderation über die Föderationsseite importieren, um sie in der Konsole zu verwalten."Erfahren Sie, wie Sie Ihre Föderation importieren."

Unterstützte Identitätsanbieter

NetApp unterstützt die folgenden Protokolle und Identitätsanbieter für die Föderation:

Protokolle

- Security Assertion Markup Language (SAML)-Identitätsanbieter
- Active Directory-Verbunddienste (AD FS)

Identitätsanbieter

- Microsoft Entra ID
- PingFederate

Föderation mit NetApp Console -Workflow

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in der Konsole eine Verbindung erstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Föderation mit Ihrer E-Mail-Domäne oder mit einer anderen Domäne, die Ihnen gehört, herstellen. Um eine Föderation mit einer anderen Domäne als Ihrer E-Mail-Domäne herzustellen, bestätigen Sie zunächst, dass Sie der Eigentümer der Domäne sind.

Bestätigen Sie Ihre Domäne (wenn Sie nicht Ihre E-Mail-Domäne verwenden)

Um eine Föderation mit einer anderen Domäne als Ihrer E-Mail-Domäne herzustellen, bestätigen Sie, dass Sie deren Eigentümer sind. Sie können Ihre E-Mail-Domäne ohne zusätzliche Schritte föderieren.

Konfigurieren Sie Ihren IdP so, dass er NetApp als Serviceprovider vertraut

Konfigurieren Sie Ihren Identitätsanbieter so, dass er NetApp vertraut, indem Sie eine neue Anwendung erstellen und Details wie die ACS-URL, die Entitäts-ID oder andere Anmeldeinformationen angeben. Die Informationen zum Dienstanbieter variieren je nach Identitätsanbieter. Weitere Informationen finden Sie in der Dokumentation Ihres spezifischen Identitätsanbieters. Sie müssen mit Ihrem IdP-Administrator zusammenarbeiten, um diesen Schritt abzuschließen.

Erstellen Sie die Verbundverbindung in der Konsole

Geben Sie die SAML-Metadaten-URL oder -Datei von Ihrem Identitätsanbieter an, um die Verbindung herzustellen. Diese Informationen werden verwendet, um die Vertrauensbeziehung zwischen der Konsole und Ihrem Identitätsanbieter herzustellen. Die von Ihnen bereitgestellten Informationen hängen von dem von Ihnen verwendeten IdP ab. Wenn Sie beispielsweise die Microsoft Entra ID verwenden, müssen Sie die Client-ID, das Geheimnis und die Domäne angeben.

Testen Sie Ihre Föderation in der Konsole

Testen Sie Ihre Verbundverbindung, bevor Sie sie aktivieren. Verwenden Sie die Testoption auf der Seite „Föderation“ in der Konsole, um zu überprüfen, ob sich Ihr Testbenutzer erfolgreich authentifizieren kann. Wenn der Test erfolgreich ist, können Sie die Verbindung aktivieren.

Aktivieren Sie Ihre Verbindung in der Konsole

Nachdem Sie die Verbindung aktiviert haben, können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden.

Lesen Sie zunächst das Thema für Ihr jeweiliges Protokoll oder Ihren IdP:

- "Einrichten einer Verbundverbindung mit AD FS"
- "Einrichten einer Verbundverbindung mit der Microsoft Entra ID"
- "Einrichten einer Verbundverbindung mit PingFederate"
- "Einrichten einer Verbundverbindung mit einem SAML-Identitätsanbieter"

Domänenüberprüfung

Überprüfen Sie die E-Mail-Domäne für Ihre Verbundverbindung

Wenn Sie eine Föderation mit einer Domäne durchführen möchten, die sich von Ihrer E-Mail-Domäne unterscheidet, müssen Sie zunächst bestätigen, dass Sie der Eigentümer der Domäne sind. Sie können für die Föderation nur verifizierte Domänen verwenden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Zur Überprüfung Ihrer Domäne müssen Sie den DNS-Einstellungen Ihrer Domäne einen TXT-Eintrag hinzufügen. Dieser Datensatz dient als Nachweis dafür, dass Sie der Eigentümer der Domäne sind, und ermöglicht der NetApp Console, der Domäne für die Föderation zu vertrauen. Möglicherweise müssen Sie sich mit Ihrem IT- oder Netzwerkadministrator abstimmen, um diesen Schritt abzuschließen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Wählen Sie **Domänenbesitz bestätigen**.
5. Geben Sie die Domäne ein, die Sie verifizieren möchten, und wählen Sie **Weiter**.
6. Kopieren Sie den bereitgestellten TXT-Eintrag.
7. Gehen Sie zu den DNS-Einstellungen Ihrer Domäne und konfigurieren Sie den TXT-Wert, der als TXT-Eintrag für Ihre Domäne bereitgestellt wurde. Arbeiten Sie bei Bedarf mit Ihrem IT- oder Netzwerkadministrator zusammen.
8. Nachdem der TXT-Eintrag hinzugefügt wurde, kehren Sie zur Konsole zurück und wählen Sie **Überprüfen**.

Konfigurieren von Föderationen

Verbinden Sie die NetApp Console mit Active Directory Federation Services (AD FS).

Verbinden Sie Ihre Active Directory Federation Services (AD FS) mit der NetApp Console , um Single Sign-On (SSO) für die NetApp Console zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. NetApp empfiehlt, sich für das eine oder das andere zu entscheiden, aber nicht für beides.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Konfigurieren Sie zunächst den Identitätsanbieter so, dass er der NetApp Console als Dienstanbieter vertraut. Erstellen Sie dann mithilfe der Konfiguration Ihres Identitätsanbieters eine Verbindung in der Konsole.

Sie können eine Föderation mit Ihrem AD FS-Server einrichten, um Single Sign-On (SSO) für die NetApp Console zu aktivieren. Der Vorgang umfasst die Konfiguration Ihres AD FS, sodass es der Konsole als Dienstanbieter vertraut, und die anschließende Herstellung der Verbindung in der NetApp Console.

Bevor Sie beginnen

- Es ist ein IdP-Konto mit Administratorrechten erforderlich. Koordinieren Sie die Durchführung der Schritte mit Ihrem IdP-Administrator.
- Identifizieren Sie die Domäne, die Sie für die Föderation verwenden möchten. Sie können Ihre E-Mail-Domäne oder eine andere Domäne verwenden, die Ihnen gehört. Wenn Sie eine andere Domäne als Ihre E-Mail-Domäne verwenden möchten, müssen Sie die Domäne zuerst in der Konsole verifizieren. Sie können dies tun, indem Sie die Schritte in der"Überprüfen Sie Ihre Domäne in der NetApp Console" Thema.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Geben Sie Ihre Domänendetails ein:
   a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
   b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
   c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
5. Wählen Sie **Weiter**.
6. Wählen Sie als Verbindungsmethode **Protokoll** und dann **Active Directory Federation Services (AD FS)**.
7. Wählen Sie **Weiter**.
8. Erstellen Sie eine Vertrauensstellung der vertrauenden Seite auf Ihrem AD FS-Server. Sie können PowerShell verwenden oder es manuell auf Ihrem AD FS-Server konfigurieren. Weitere Informationen zum Erstellen einer Vertrauensstellung der vertrauenden Seite finden Sie in der AD FS-Dokumentation.
   a. Erstellen Sie die Vertrauensstellung mithilfe von PowerShell und dem folgenden Skript:

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

   b. Alternativ können Sie die Vertrauensstellung manuell in der AD FS-Verwaltungskonsole erstellen.

Verwenden Sie beim Erstellen der Vertrauensstellung die folgenden NetApp Console :

- Verwenden Sie beim Erstellen der Relying Trust Identifier den Wert **YOUR_TENANT**: `netapp-cloud-account`
- Wenn Sie **Unterstützung für WS-Federation aktivieren** auswählen, verwenden Sie den Wert **YOUR_AUTH0_DOMAIN**: `netapp-cloud-account.auth0.com`

c. Kopieren Sie nach dem Erstellen der Vertrauensstellung die Metadaten-URL von Ihrem AD FS-Server oder laden Sie die Verbundmetadatendatei herunter. Sie benötigen diese URL oder Datei, um die Verbindung in der Konsole herzustellen.

NetApp empfiehlt die Verwendung der Metadaten-URL, damit die NetApp Console automatisch die neueste AD FS-Konfiguration abrufen kann. Wenn Sie die Federation-Metadatendatei herunterladen, müssen Sie sie bei jeder Änderung Ihrer AD FS-Konfiguration manuell in der NetApp Console aktualisieren.

9. Kehren Sie zur Konsole zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.
10. Stellen Sie die Verbindung mit AD FS her.
    a. Geben Sie die **AD FS-URL** ein, die Sie im vorherigen Schritt von Ihrem AD FS-Server kopiert haben, oder laden Sie die Verbundmetadatendatei hoch, die Sie von Ihrem AD FS-Server heruntergeladen haben.
11. Wählen Sie **Verbindung erstellen**. Das Herstellen der Verbindung kann einige Sekunden dauern.
12. Wählen Sie **Weiter**.
13. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zu einer Anmeldeseite für Ihren IdP-Server weitergeleitet. Melden Sie sich mit Ihren IdP-Anmeldeinformationen an, um den Test abzuschließen, und kehren Sie zur Konsole zurück, um die Verbindung zu aktivieren.
14. Wählen Sie **Weiter**.
15. Überprüfen Sie auf der Seite **Föderation aktivieren** die Föderationsdetails und wählen Sie dann **Föderation aktivieren** aus.
16. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nachdem Sie die Föderation aktiviert haben, können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei der NetApp Console anmelden.

Verbinden Sie die NetApp Console mit der Microsoft Entra-ID

Verbinden Sie sich mit Ihrem Microsoft Entra ID IdP-Anbieter, um Single Sign-On (SSO) für die NetApp Console zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen anmelden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. NetApp empfiehlt, sich für das eine oder das andere zu entscheiden, aber nicht für beides.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in

der Konsole eine Verbindung erstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Verbundverbindung mit der Microsoft Entra ID einrichten, um Single Sign-On (SSO) für die Konsole zu aktivieren. Der Vorgang umfasst die Konfiguration Ihrer Microsoft Entra-ID, um der Konsole als Dienstanbieter zu vertrauen, und das anschließende Erstellen der Verbindung in der Konsole.

Bevor Sie beginnen

- Es ist ein IdP-Konto mit Administratorrechten erforderlich. Koordinieren Sie die Durchführung der Schritte mit Ihrem IdP-Administrator.
- Identifizieren Sie die Domäne, die Sie für die Föderation verwenden möchten. Sie können Ihre E-Mail-Domäne oder eine andere Domäne verwenden, die Ihnen gehört. Wenn Sie eine andere Domäne als Ihre E-Mail-Domäne verwenden möchten, müssen Sie die Domäne zuerst in der Konsole verifizieren. Sie können dies tun, indem Sie die Schritte in der"Überprüfen Sie Ihre Domäne in der NetApp Console" Thema.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.

Domänendetails

1. Geben Sie Ihre Domänendetails ein:
   a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
   b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
   c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
2. Wählen Sie **Weiter**.

Verbindungsmethode

1. Wählen Sie als Verbindungsmethode **Anbieter** und dann **Microsoft Entra ID**.
2. Wählen Sie **Weiter**.

Konfigurationshinweise

1. Konfigurieren Sie Ihre Microsoft Entra-ID, um NetApp als Dienstanbieter zu vertrauen. Sie müssen diesen Schritt auf Ihrem Microsoft Entra ID-Server ausführen.
   a. Verwenden Sie beim Registrieren Ihrer Microsoft Entra ID-App die folgenden Werte, um der Konsole zu vertrauen:
      - Verwenden Sie für die **Umleitungs-URL** `https://services.cloud.netapp.com`
      - Verwenden Sie für die **Antwort-URL** `https://netapp-cloud-account.auth0.com/login/callback`
   b. Erstellen Sie ein Clientgeheimnis für Ihre Microsoft Entra ID-App. Sie müssen die Client-ID, das Client-Geheimnis und den Entra-ID-Domänennamen angeben, um die Föderation abzuschließen.
2. Kehren Sie zur Konsole zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.

Verbindung erstellen

1. Erstellen Sie die Verbindung mit der Microsoft Entra ID
   a. Geben Sie die Client-ID und das Client-Geheimnis ein, die Sie im vorherigen Schritt erstellt haben.
   b. Geben Sie den Domänennamen der Microsoft Entra ID ein.
2. Wählen Sie **Verbindung erstellen**. Das System stellt die Verbindung in wenigen Sekunden her.

Testen und aktivieren Sie die Verbindung

1. Wählen Sie **Weiter**.
2. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zu einer Anmeldeseite für Ihren IdP-Server weitergeleitet. Melden Sie sich mit Ihren IdP-Anmeldeinformationen an, um den Test abzuschließen, und kehren Sie zur Konsole zurück, um die Verbindung zu aktivieren.
3. Wählen Sie **Weiter**.
4. Überprüfen Sie auf der Seite **Föderation aktivieren** die Föderationsdetails und wählen Sie dann **Föderation aktivieren** aus.
5. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nachdem Sie die Föderation aktiviert haben, können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei der NetApp Console anmelden.

Föderieren Sie die NetApp Console mit PingFederate

Verbinden Sie sich mit Ihrem PingFederate IdP-Anbieter, um Single Sign-On (SSO) für die NetApp Console zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen anmelden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen."Erfahren Sie mehr über Zugriffsrollen."

> Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. NetApp empfiehlt, sich für das eine oder das andere zu entscheiden, aber nicht für beides.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in der Konsole eine Verbindung erstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können mit PingFederate eine Verbundverbindung einrichten, um Single Sign-On (SSO) für die Konsole zu aktivieren. Der Vorgang umfasst die Konfiguration Ihres PingFederate-Servers, sodass dieser der Konsole als Dienstanbieter vertraut, und die anschließende Herstellung der Verbindung in der Konsole.

Bevor Sie beginnen

- Es ist ein IdP-Konto mit Administratorrechten erforderlich. Koordinieren Sie die Durchführung der Schritte mit Ihrem IdP-Administrator.
- Identifizieren Sie die Domäne, die Sie für die Föderation verwenden möchten. Sie können Ihre E-Mail-Domäne oder eine andere Domäne verwenden, die Ihnen gehört. Wenn Sie eine andere Domäne als Ihre E-Mail-Domäne verwenden möchten, müssen Sie die Domäne zuerst in der Konsole verifizieren. Sie können dies tun, indem Sie die Schritte in der"Überprüfen Sie Ihre Domäne in der NetApp Console" Thema.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Geben Sie Ihre Domänendetails ein:
   a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
   b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
   c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
5. Wählen Sie **Weiter**.
6. Wählen Sie als Verbindungsmethode **Provider** und dann **PingFederate**.
7. Wählen Sie **Weiter**.
8. Konfigurieren Sie Ihren PingFederate-Server so, dass er NetApp als Dienstanbieter vertraut. Sie müssen diesen Schritt auf Ihrem PingFederate-Server ausführen.
   a. Verwenden Sie die folgenden Werte, wenn Sie PingFederate so konfigurieren, dass es der NetApp Console vertraut:
      - Für die **Antwort-URL** oder **Assertion Consumer Service (ACS)-URL** verwenden Sie `https://netapp-cloud-account.auth0.com/login/callback`
      - Verwenden Sie für die **Abmelde-URL** `https://netapp-cloud-account.auth0.com/logout`
      - Verwenden Sie für **Zielgruppen-/Entitäts-ID** `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` wobei <fed-domain-name-pingfederate> der Domänenname für die Föderation ist. Wenn Ihre Domäne beispielsweise `example.com` , wäre die Zielgruppen-/Entitäts-ID `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .
   b. Kopieren Sie die URL des PingFederate-Servers. Sie benötigen diese URL, wenn Sie die Verbindung in der Konsole herstellen.
   c. Laden Sie das X.509-Zertifikat von Ihrem PingFederate-Server herunter. Es muss im Base64-codierten PEM-Format (.pem, .crt, .cer) vorliegen.
9. Kehren Sie zur Konsole zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.
10. Erstellen Sie die Verbindung mit PingFederate
    a. Geben Sie die PingFederate-Server-URL ein, die Sie im vorherigen Schritt kopiert haben.
    b. Laden Sie das X.509-Signaturzertifikat hoch. Das Zertifikat muss im PEM-, CER- oder CRT-Format vorliegen.
11. Wählen Sie **Verbindung erstellen**. Das System stellt die Verbindung in wenigen Sekunden her.
12. Wählen Sie **Weiter**.
13. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zu einer Anmeldeseite für Ihren IdP-Server weitergeleitet. Melden Sie sich mit Ihren IdP-Anmeldeinformationen an, um den Test abzuschließen, und kehren Sie zur Konsole zurück, um die Verbindung zu aktivieren.
14. Wählen Sie **Weiter**.
15. Überprüfen Sie auf der Seite **Föderation aktivieren** die Föderationsdetails und wählen Sie dann **Föderation aktivieren** aus.
16. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nachdem Sie die Föderation aktiviert haben, können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei der NetApp Console anmelden.

Föderieren Sie mit einem SAML-Identitätsanbieter

Verbinden Sie sich mit Ihrem SAML 2.0-IdP-Anbieter, um Single Sign-On (SSO) für die NEtApp-Konsole zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen anmelden.

Erforderliche Rolle

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. Sie können nicht mit beiden eine Föderation bilden.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in der Konsole eine Verbindung erstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Verbundverbindung mit Ihrem SAML 2.0-Anbieter einrichten, um Single Sign-On (SSO) für die Konsole zu aktivieren. Der Vorgang umfasst die Konfiguration Ihres Providers, sodass dieser NetApp als Serviceprovider vertraut, und die anschließende Herstellung der Verbindung in der Konsole.

Bevor Sie beginnen

- Es ist ein IdP-Konto mit Administratorrechten erforderlich. Koordinieren Sie die Durchführung der Schritte mit Ihrem IdP-Administrator.
- Identifizieren Sie die Domäne, die Sie für die Föderation verwenden möchten. Sie können Ihre E-Mail-Domäne oder eine andere Domäne verwenden, die Ihnen gehört. Wenn Sie eine andere Domäne als Ihre E-Mail-Domäne verwenden möchten, müssen Sie die Domäne zuerst in der Konsole verifizieren. Sie können dies tun, indem Sie die Schritte in der"Überprüfen Sie Ihre Domäne in der NetApp Console" Thema.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Föderation** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Geben Sie Ihre Domänendetails ein:
    a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
    b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
    c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
5. Wählen Sie **Weiter**.
6. Wählen Sie als Verbindungsmethode **Protokoll** und dann **SAML-Identitätsanbieter**.
7. Wählen Sie **Weiter**.
8. Konfigurieren Sie Ihren SAML-Identitätsanbieter so, dass er NetApp als Dienstanbieter vertraut. Sie müssen diesen Schritt auf dem Server Ihres SAML-Anbieters ausführen.

a. Stellen Sie sicher, dass Ihr IdP das Attribut `email` auf die E-Mail-Adresse des Benutzers eingestellt. Dies ist erforderlich, damit die Konsole Benutzer korrekt identifizieren kann:

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">
        <saml:AttributeValue xsi:type="xs:string">
email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

b. Verwenden Sie die folgenden Werte, wenn Sie Ihre SAML-Anwendung bei der Konsole registrieren:
   - Für die **Antwort-URL** oder **Assertion Consumer Service (ACS)-URL** verwenden Sie `https://netapp-cloud-account.auth0.com/login/callback`
   - Verwenden Sie für die **Abmelde-URL** `https://netapp-cloud-account.auth0.com/logout`
   - Verwenden Sie für **Zielgruppen-/Entitäts-ID** `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` wobei <fed-domain-name-saml> der Domänenname ist, den Sie für die Föderation verwenden möchten. Wenn Ihre Domäne beispielsweise `example.com` , wäre die Zielgruppen-/Entitäts-ID `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .

c. Kopieren Sie nach dem Erstellen des Vertrauens die folgenden Werte vom Server Ihres SAML-Anbieters:
   - Anmelde-URL
   - Abmelde-URL (optional)

d. Laden Sie das X.509-Zertifikat vom Server Ihres SAML-Anbieters herunter. Es muss im PEM-, CER- oder CRT-Format vorliegen.

9. Kehren Sie zur Konsole zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.
10. Stellen Sie die Verbindung mit SAML her.
    a. Geben Sie die **Anmelde-URL** Ihres SAML-Servers ein.
    b. Laden Sie das X.509-Zertifikat hoch, das Sie vom Server Ihres SAML-Anbieters heruntergeladen haben.
    c. Geben Sie optional die **Abmelde-URL** Ihres SAML-Servers ein.
11. Wählen Sie **Verbindung erstellen**. Das System stellt die Verbindung in wenigen Sekunden her.
12. Wählen Sie **Weiter**.
13. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zu einer Anmeldeseite für Ihren IdP-Server weitergeleitet. Melden Sie sich mit Ihren IdP-Anmeldeinformationen an, um den Test abzuschließen, und kehren Sie zur Konsole zurück, um die Verbindung zu aktivieren.
14. Wählen Sie **Weiter**.
15. Überprüfen Sie auf der Seite **Föderation aktivieren** die Föderationsdetails und wählen Sie dann

Föderation aktivieren aus.

16. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nachdem Sie die Föderation aktiviert haben, können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei der NetApp Console anmelden.

Föderationen in der NetApp Console verwalten

Sie können Ihre Föderation in der NetApp Console verwalten. Sie können es deaktivieren, abgelaufene Anmeldeinformationen aktualisieren und es deaktivieren, wenn Sie es nicht mehr benötigen.

Wenn Sie die Föderation mit NetApp Cloud Central konfiguriert haben, importieren Sie sie über die Seite **Föderation**, um sie in der Konsole zu verwalten."Erfahren Sie, wie Sie Ihre Föderation importieren"

Sie können einer vorhandenen Föderation auch eine verifizierte Domäne hinzufügen, wodurch Sie mehrere Domänen für Ihre föderierte Verbindung verwenden können.

Ereignisse der Föderationsverwaltung wie das Aktivieren, Deaktivieren und Aktualisieren von Föderationen werden in der Zeitleiste angezeigt."Erfahren Sie mehr über die Überwachung von Vorgängen in der NetApp Console."

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist die Rolle des Föderationsadministrators erforderlich. Der Federation-Viewer kann die Federation-Seite anzeigen."Erfahren Sie mehr über Zugriffsrollen."

Aktivieren einer Föderation

Wenn Sie eine Föderation erstellt haben, diese aber nicht aktiviert ist, können Sie sie über die Seite **Föderation** aktivieren. Durch die Aktivierung einer Föderation können sich die mit der Föderation verknüpften Benutzer mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden. Erstellen und testen Sie die Föderation erfolgreich, bevor Sie sie aktivieren.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü ••• neben der Föderation, die Sie aktivieren möchten, und wählen Sie **Aktivieren** aus.

Hinzufügen einer verifizierten Domäne zu einer vorhandenen Föderation

Sie können einer vorhandenen Föderation in der Konsole eine verifizierte Domäne hinzufügen, um mehrere Domänen mit demselben Identitätsanbieter (IdP) zu verwenden.

Sie müssen die Domäne bereits in der Konsole verifiziert haben, bevor Sie sie zu einer Föderation hinzufügen können. Wenn Sie die Domäne noch nicht verifiziert haben, können Sie dies tun, indem Sie die Schritte in"Überprüfen Sie Ihre Domäne in der Konsole" .

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Domänen aktualisieren** aus. Im Dialogfeld **Domänen aktualisieren** wird die Domäne angezeigt, die bereits mit dieser Föderation verknüpft ist.
4. Wählen Sie eine verifizierte Domäne aus der Liste der verfügbaren Domänen aus.
5. Wählen Sie **Aktualisieren**. Neue Domänenbenutzer können innerhalb von 30 Sekunden föderierten Konsolenzugriff erhalten.

Aktualisieren einer ablaufende Verbundverbindung

Sie können die Details einer Föderation in der Konsole aktualisieren. Sie müssen beispielsweise die Föderation aktualisieren, wenn Anmeldeinformationen wie ein Zertifikat oder ein Client-Geheimnis ablaufen. Aktualisieren Sie bei Bedarf das Benachrichtigungsdatum, um Sie daran zu erinnern, die Verbindung zu aktualisieren, bevor sie abläuft.

Aktualisieren Sie zuerst die Konsole, bevor Sie Ihren IdP aktualisieren, um Anmeldeprobleme zu vermeiden. Bleiben Sie während des Vorgangs bei der Konsole angemeldet.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü (drei vertikale Punkte) neben der Föderation, die Sie aktualisieren möchten, und wählen Sie **Föderation aktualisieren**.
4. Aktualisieren Sie die Details der Föderation nach Bedarf.
5. Wählen Sie **Aktualisieren**.

Testen einer vorhandenen Föderation

Testen Sie die Verbindung einer vorhandenen Föderation, um sicherzustellen, dass sie funktioniert. Auf diese Weise können Sie etwaige Probleme mit der Föderation erkennen und beheben.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Verbindung testen** aus.
4. Wählen Sie **Test**. Das System fordert Sie auf, sich mit Ihren Unternehmensanmeldeinformationen anzumelden. Wenn die Verbindung erfolgreich ist, werden Sie zur NetApp Console weitergeleitet. Wenn die Verbindung fehlschlägt, wird eine Fehlermeldung angezeigt, die auf das Problem mit der Föderation hinweist.
5. Wählen Sie **Fertig**, um zur Registerkarte **Föderation** zurückzukehren.

Deaktivieren einer Föderation

Wenn Sie eine Föderation nicht mehr benötigen, können Sie sie deaktivieren. Dadurch wird verhindert, dass sich mit der Föderation verknüpfte Benutzer mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden. Sie können die Föderation bei Bedarf später wieder aktivieren.

Deaktivieren Sie eine Föderation, bevor Sie sie löschen, beispielsweise wenn Sie den IdP außer Betrieb nehmen oder die Föderation beenden. Auf diese Weise können Sie es bei Bedarf später wieder aktivieren.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Deaktivieren** aus.

Löschen einer Föderation

Wenn Sie eine Föderation nicht mehr benötigen, können Sie sie löschen. Dadurch wird die Föderation entfernt und alle mit der Föderation verknüpften Benutzer können sich nicht mehr mit ihren Unternehmensanmeldeinformationen bei der Konsole anmelden. Beispielsweise, wenn der IdP außer Betrieb genommen wird oder die Föderation nicht mehr benötigt wird.

Sie können eine Föderation nicht wiederherstellen, nachdem Sie sie gelöscht haben. Sie müssen eine neue Föderation erstellen.

Sie müssen eine Föderation deaktivieren, bevor Sie sie löschen können. Sie können eine Föderation nach dem Löschen nicht wiederherstellen.

Schritte

1. Wählen Sie **Administration > Identität und Zugriff**.
2. Wählen Sie **Föderationen** aus, um die Seite **Föderationen** anzuzeigen.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Löschen** aus.

Importieren Sie Ihre Föderation in die NetApp Console

Wenn Sie zuvor die Föderation über NetApp Cloud Central (eine externe Anwendung der NetApp Console) eingerichtet haben, werden Sie auf der Föderationsseite aufgefordert, Ihre vorhandene föderierte Verbindung in die Konsole zu importieren, damit Sie sie in der neuen Schnittstelle verwalten können. Sie können dann die neuesten Verbesserungen nutzen, ohne Ihre Verbundverbindung neu erstellen zu müssen.

Nachdem Sie Ihre vorhandene Föderation importiert haben, können Sie die Föderation auf der Seite **Föderationen** verwalten."Erfahren Sie mehr über die Verwaltung von Föderationen."

Erforderliche Rolle

Organisationsadministrator oder Föderationsadministrator."Erfahren Sie mehr über Zugriffsrollen."

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie die Registerkarte **Föderation** aus.
3. Wählen Sie **Föderation importieren**.

Konsolenagenten

Warten der Konsolen-Agent-VM und des Betriebssystems

Die Wartung des Betriebssystems auf dem Konsolenagent-Host liegt in Ihrer (der Verantwortung des Kunden). Beispielsweise sollten Sie (der Kunde) Sicherheitsupdates auf das Betriebssystem auf dem Agent-Host anwenden, indem Sie die Standardverfahren Ihres Unternehmens zur Betriebssystemverteilung befolgen.

Wenn Sie bereits einen Agenten haben, sollten Sie Folgendes beachten:"Änderungen an unterstützten Linux-Betriebssystemen" .

Betriebssystem-Patches und der Agent

Wenden Sie Betriebssystem-Sicherheitspatches an, ohne die Agent-Hostdienste zu stoppen.

VM- oder Instanztyp

Wenn Sie einen Konsolenagenten aus der Konsole erstellen, stellt dieser eine VM-Instanz mit einer Standardkonfiguration bei Ihrem Cloud-Anbieter bereit. Wechseln Sie nach dem Erstellen des Agenten nicht zu einer kleineren VM-Instanz mit weniger CPU oder RAM.

In der folgenden Tabelle sind die CPU- und RAM-Anforderungen aufgeführt:

CPU
: 8 Kerne oder 8 vCPUs

RAM
: 32 GB

"Erfahren Sie mehr über die Standardkonfiguration für den Agenten" .

Überwachen des Agenten

Die Konsole benachrichtigt Sie, wenn die Agent-VM fehlerhaft ist, beispielsweise bei Problemen mit Speicherplatz, RAM und CPU. Überwachen Sie diese Benachrichtigungen im Benachrichtigungscenter in der Konsole oder konfigurieren Sie E-Mail-Benachrichtigungen. Gelegentliche Erhöhungen des Speicherplatzes, des Arbeitsspeichers oder der CPU-Auslastung sind normal. Wenn dies jedoch häufig vorkommt, sollten Sie Maßnahmen zur Behebung des Problems ergreifen.

Beispielsweise benachrichtigt Sie die Konsole, wenn eine Agentenressource (CPU, RAM oder Festplattenspeicher) 30 Minuten lang hintereinander 90 % ihrer Gesamtkapazität überschreitet. Wenn die Ressourcennutzung anschließend unter diesen Schwellenwert fällt, wird die Benachrichtigung im Benachrichtigungscenter als behoben (grün) angezeigt.

Wenden Sie sich an den NetApp -Support, wenn Sie Fragen zum Ändern Ihrer Agent-VM haben.

"Erfahren Sie mehr."

Benachrichtigung	Handlungsbedarf
Der Speicherplatz ist zu groß	"Lesen Sie den NetApp Knowledge Base-Artikel" .
Die CPU-Auslastung ist zu hoch	Erhöhen Sie die CPU-Größe der Agent-VM bei Ihrem Cloud-Anbieter oder vor Ort, je nachdem, wo Sie sie installiert haben. Alternativ können Sie zusätzliche Agenten erstellen und die Arbeitslast auf mehrere Agenten verteilen. Die RAM-Auslastung kann je nach Umgebung, ONTAP Workloads, Anzahl der Cloud Volumes ONTAP Systeme und den von Ihnen verwendeten Datendiensten variieren.
Die RAM-Auslastung ist zu hoch	Erhöhen Sie den RAM der Agent-VM bei Ihrem Cloud-Anbieter oder vor Ort, je nachdem, wo Sie sie installiert haben. Alternativ können Sie zusätzliche Agenten erstellen und die Arbeitslast auf mehrere Agenten verteilen. Die RAM-Auslastung kann je nach Umgebung, ONTAP Workloads, Anzahl der Cloud Volumes ONTAP Systeme und den von Ihnen verwendeten Datendiensten variieren.

Stoppen und Starten der Agent-VM

Stoppen und starten Sie die Agent-VM bei Bedarf über die Konsole Ihres Cloud-Anbieters oder über standardmäßige Verfahren vor Ort.

"Beachten Sie, dass der Konsolenagent jederzeit betriebsbereit sein muss" .

Herstellen einer Verbindung mit der Linux-VM

Wenn Sie eine Verbindung mit der Linux-VM herstellen müssen, auf der der Agent ausgeführt wird, verwenden Sie die Konnektivitätsoptionen Ihres Cloud-Anbieters.

AWS

Wenn Sie die Agenteninstanz in AWS erstellen, geben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel an. Sie können dieses Schlüsselpaar verwenden, um per SSH auf die Instanz zuzugreifen. Verwenden Sie den Benutzernamen „ubuntu“ für die EC2-Linux-Instanz. Verwenden Sie für Agenten, die vor Mai 2023 erstellt wurden, den Benutzernamen „ec2-user“.

"AWS Docs: Verbinden Sie sich mit Ihrer Linux-Instance"

Azurblau

Wenn Sie die Agent-VM in Azure erstellen, geben Sie einen Benutzernamen an und wählen die Authentifizierung mit einem Kennwort oder einem öffentlichen SSH-Schlüssel. Verwenden Sie die von Ihnen gewählte Authentifizierungsmethode, um eine Verbindung mit der VM herzustellen.

"Azure-Dokumente: SSH in Ihre VM"

Google Cloud

Sie können keine Authentifizierungsmethode angeben, wenn Sie einen Agenten in Google Cloud erstellen. Sie können jedoch über die Google Cloud Console oder die Google Cloud CLI (gcloud) eine Verbindung zur Linux-VM-Instanz herstellen.

"Google Cloud Docs: Verbindung zu Linux-VMs herstellen"

Ändern der IP-Adresse für einen Agenten

Sie können die internen und öffentlichen IP-Adressen der von Ihrem Cloud-Anbieter zugewiesenen Agenteninstanz bei Bedarf ändern.

Schritte

1. Befolgen Sie die Anweisungen Ihres Cloud-Anbieters, um die lokale IP-Adresse oder die öffentliche IP-Adresse (oder beide) für die Agenteninstanz zu ändern.
2. Starten Sie die Agenteninstanz neu, um eine neue öffentliche IP-Adresse bei der Konsole zu registrieren.
3. Wenn Sie die private IP-Adresse geändert haben, aktualisieren Sie den Sicherungsspeicherort für die Konfigurationsdateien von Cloud Volumes ONTAP, sodass die Sicherungen an die neue private IP-Adresse auf dem Agenten gesendet werden.

   Aktualisieren Sie den Sicherungsspeicherort für jedes Cloud Volumes ONTAP -System.

   a. Legen Sie in der Cloud Volumes ONTAP CLI die Berechtigungsstufe auf „Erweitert“ fest:

   ```
   set -privilege advanced
   ```

   b. Führen Sie den folgenden Befehl aus, um das aktuelle Sicherungsziel anzuzeigen:

   ```
   system configuration backup settings show
   ```

   c. Führen Sie den folgenden Befehl aus, um die IP-Adresse für das Sicherungsziel zu aktualisieren:

   ```
   system configuration backup settings modify -destination <target-
   location>
   ```

Bearbeiten der URIs eines Agenten

Sie können den Uniform Resource Identifier (URI) für einen Agenten hinzufügen und entfernen.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **Agent bearbeiten**.

   Zum Bearbeiten muss der Konsolenagent aktiv sein.

3. Erweitern Sie die Leiste **Agent-URIs**, um Agent-URIs anzuzeigen.
4. Fügen Sie URIs hinzu und entfernen Sie sie, und wählen Sie dann **Übernehmen** aus.

Verwalten Sie einen VCenter- oder ESXi-Host für den Konsolenagenten

Sie können nach der Bereitstellung des Konsolenagenten Änderungen an Ihrem vorhandenen VCenter- oder ESXi-Host vornehmen. Sie können beispielsweise die CPU

oder den RAM der VM-Instanz erhöhen, die den Konsolenagenten hostet.

Führen Sie diese Wartungsaufgaben mithilfe der VM-Webkonsole durch:

- Erhöhen Sie die Festplattengröße
- Starten Sie den Agenten neu
- Aktualisieren statischer Routen
- Suchdomänen aktualisieren

Einschränkungen

Das Upgrade des Agenten über die Konsole wird noch nicht unterstützt. Darüber hinaus können Sie nur Informationen zur IP-Adresse, zum DNS und zu Gateways anzeigen.

Zugriff auf die VM-Wartungskonsole

Sie können vom VSphere-Client aus auf die Wartungskonsole zugreifen.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.

Ändern Sie das Kennwort des Wartungsbenutzers

Sie können das Passwort für die `maint` Benutzer.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `1` , um die `System Configuration` Speisekarte.
6. Eingeben `1` um das Wartungsbenutzerkennwort zu ändern und den Anweisungen auf dem Bildschirm zu folgen.

Erhöhen Sie die CPU oder den RAM der VM-Instanz

Sie können die CPU oder den RAM der VM-Instanz erhöhen, die den Konsolenagenten hostet.

Bearbeiten Sie die VM-Instanzeinstellungen in Ihrem VCenter- oder ESXi-Host und wenden Sie die Änderungen dann mit der Wartungskonsole an.

Schritte im VSphere-Client

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Klicken Sie mit der rechten Maustaste auf die VM-Instanz und wählen Sie **Einstellungen bearbeiten**.
4. Erhöhen Sie den für die Partition /opt oder /var verwendeten Festplattenspeicher.
   a. Wählen Sie **Festplatte 2**, um den für /opt verwendeten Festplattenspeicher zu erhöhen.
   b. Wählen Sie **Festplatte 3**, um den für /var verwendeten Festplattenspeicher zu erhöhen.
5. Speichern Sie Ihre Änderungen.

Schritte in der Wartungskonsole

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `1 to view the `System Configuration` Speisekarte.
6. Eingeben `2` und folgen Sie den Anweisungen auf dem Bildschirm. Die Konsole sucht nach neuen Einstellungen und vergrößert die Partitionen.

Netzwerkeinstellungen für die Agent-VM anzeigen

Zeigen Sie die Netzwerkeinstellungen für die Agent-VM im VSphere-Client an, um Netzwerkprobleme zu bestätigen oder zu beheben. Sie können die folgenden Netzwerkeinstellungen nur anzeigen (nicht aktualisieren): IP-Adresse und DNS-Details.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `2` , um die `Network Configuration` Speisekarte.
6. Geben Sie eine Zahl zwischen 1 und 6 ein, um die entsprechenden Netzwerkeinstellungen anzuzeigen.

Aktualisieren Sie die statischen Routen für die Agent-VM

Fügen Sie nach Bedarf statische Routen für die Agent-VM hinzu, aktualisieren oder entfernen Sie sie.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim

Erstellen der VM-Instanz angegeben haben.

5. Eingeben `2` , um die `Network Configuration` Speisekarte.
6. Eingeben `7` um statische Routen zu aktualisieren und den Anweisungen auf dem Bildschirm zu folgen.
7. Drücken Sie die Eingabetaste.
8. Nehmen Sie optional weitere Änderungen vor.
9. Eingeben `9` um Ihre Änderungen zu übernehmen.

Aktualisieren der Domänensucheinstellungen für die Agent-VM

Sie können die Suchdomäneneinstellungen für die Agent-VM aktualisieren.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `2`` , um die `Network Configuration` Speisekarte.
6. Eingeben `8` um die Domänensucheinstellungen zu aktualisieren und den Anweisungen auf dem Bildschirm zu folgen.
7. Drücken Sie die Eingabetaste.
8. Nehmen Sie optional weitere Änderungen vor.
9. Eingeben `9` um Ihre Änderungen zu übernehmen.

Zugriff auf die Diagnosetools des Agenten

Greifen Sie auf Diagnosetools zu, um Probleme mit dem Konsolenagenten zu beheben. Der NetApp -Support fordert Sie möglicherweise bei der Fehlerbehebung dazu auf.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `3` um das Menü „Support und Diagnose“ anzuzeigen.
6. Eingeben `1` um auf die Diagnosetools zuzugreifen und den Anweisungen auf dem Bildschirm zu folgen. + Sie können beispielsweise überprüfen, ob alle Agentendienste ausgeführt werden. "Überprüfen Sie den Status des Konsolenagenten" .

Fernzugriff auf die Diagnosetools des Agenten

Mit einem Tool wie Putty können Sie remote auf Diagnosetools zugreifen. Aktivieren Sie den SSH-Zugriff auf die Agent-VM, indem Sie ein Einmalkennwort zuweisen.

Der SSH-Zugriff ermöglicht erweiterte Terminalfunktionen wie Kopieren und Einfügen.

Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `3` , um die `Support and Diagnostics` Speisekarte.
6. Eingeben `2` um auf die Diagnosetools zuzugreifen und den Anweisungen auf dem Bildschirm zu folgen, um ein Einmalkennwort zu konfigurieren, das nach 24 Stunden abläuft.
7. Verwenden Sie ein SSH-Tool wie Putty, um mit dem Benutzernamen eine Verbindung zur Agent-VM herzustellen `diag` und das von Ihnen konfigurierte Einmalkennwort.

Installieren Sie ein CA-signiertes Zertifikat für den webbasierten Konsolenzugriff

Wenn Sie die NetApp Console im eingeschränkten Modus verwenden, ist die Benutzeroberfläche über die virtuelle Maschine des Konsolenagenten zugänglich, die in Ihrer Cloud-Region oder vor Ort bereitgestellt wird. Standardmäßig verwendet die Konsole ein selbstsigniertes SSL-Zertifikat, um sicheren HTTPS-Zugriff auf die webbasierte Konsole bereitzustellen, die auf dem Konsolenagenten ausgeführt wird.

Falls Ihr Unternehmen dies erfordert, können Sie ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat installieren, das einen besseren Sicherheitsschutz bietet als ein selbstsigniertes Zertifikat. Nachdem Sie das Zertifikat installiert haben, verwendet die Konsole das von der Zertifizierungsstelle signierte Zertifikat, wenn Benutzer auf die webbasierte Konsole zugreifen.

Installieren eines HTTPS-Zertifikats

Installieren Sie ein von einer Zertifizierungsstelle signiertes Zertifikat für den sicheren Zugriff auf die webbasierte Konsole, die auf dem Konsolenagenten ausgeführt wird.

Informationen zu diesem Vorgang

Sie können das Zertifikat mit einer der folgenden Optionen installieren:

- Generieren Sie eine Zertifikatsignieranforderung (CSR) von der Konsole aus, übermitteln Sie die Zertifikatsanforderung an eine Zertifizierungsstelle und installieren Sie dann das von der Zertifizierungsstelle signierte Zertifikat auf dem Konsolenagenten.

  Das Schlüsselpaar, das die Konsole zum Generieren der CSR verwendet, wird intern auf dem Konsolenagenten gespeichert. Die Konsole ruft automatisch dasselbe Schlüsselpaar (privater Schlüssel) ab, wenn Sie das Zertifikat auf dem Konsolenagenten installieren.

- Installieren Sie ein CA-signiertes Zertifikat, das Sie bereits haben.

Bei dieser Option wird die CSR nicht über die Konsole generiert. Sie generieren die CSR separat und speichern den privaten Schlüssel extern. Sie stellen der Konsole den privaten Schlüssel zur Verfügung, wenn Sie das Zertifikat installieren.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **HTTPS-Setup**.

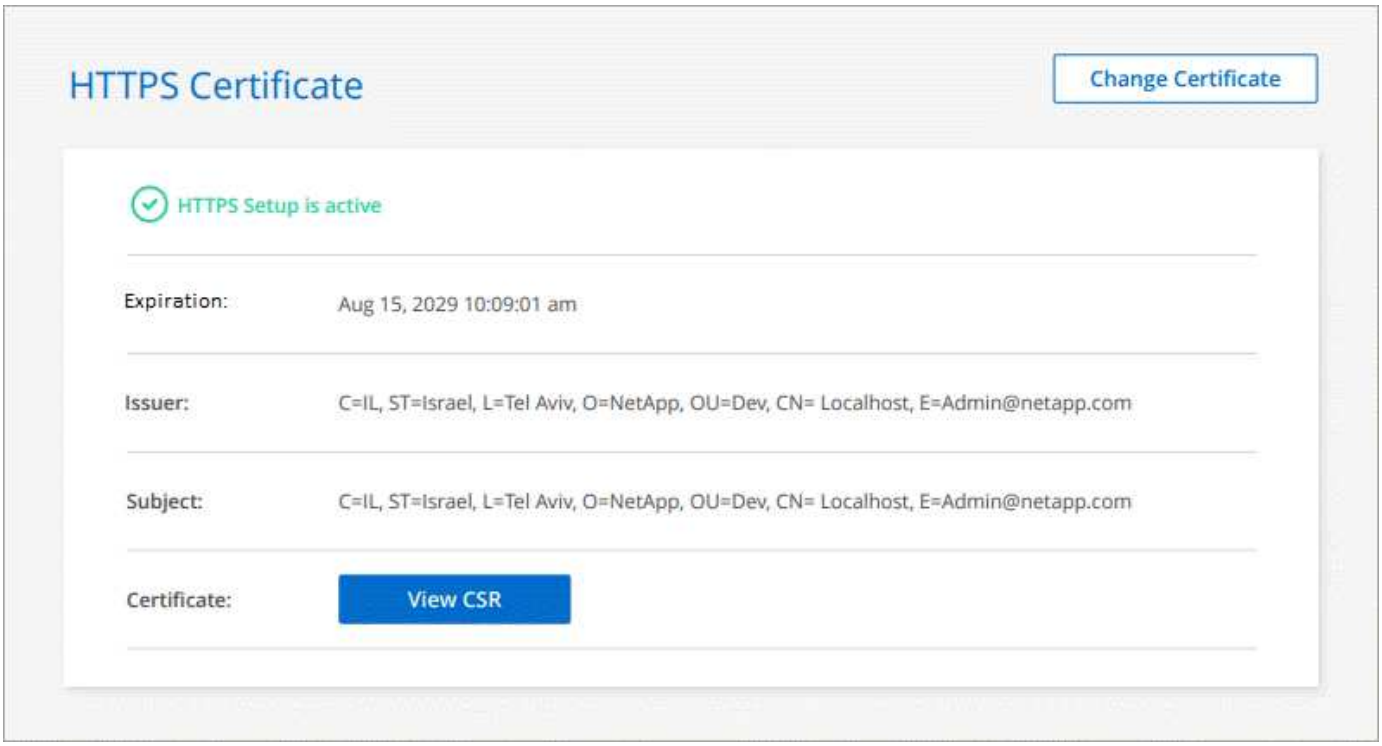
   Zum Bearbeiten muss der Konsolenagent aktiv sein.

3. Installieren Sie auf der Seite „HTTPS-Setup“ ein Zertifikat, indem Sie eine Zertifikatsignieranforderung (CSR) generieren oder Ihr eigenes CA-signiertes Zertifikat installieren:

Option	Beschreibung
Erstellen Sie eine CSR	a. Geben Sie den Hostnamen oder DNS des Konsolenagent-Hosts (seinen allgemeinen Namen) ein und wählen Sie dann **CSR generieren**. Die Konsole zeigt eine Zertifikatsignieranforderung an. b. Verwenden Sie die CSR, um eine SSL-Zertifikatsanforderung an eine Zertifizierungsstelle zu senden. Das Zertifikat muss das Base-64-codierte X.509-Format von Privacy Enhanced Mail (PEM) verwenden. c. Laden Sie die Zertifikatsdatei hoch und wählen Sie dann **Installieren**.
Installieren Sie Ihr eigenes CA-signiertes Zertifikat	a. Wählen Sie **CA-signiertes Zertifikat installieren**. b. Laden Sie sowohl die Zertifikatsdatei als auch den privaten Schlüssel und wählen Sie dann **Installieren**. Das Zertifikat muss das Base-64-codierte X.509-Format von Privacy Enhanced Mail (PEM) verwenden.

Ergebnis

Der Konsolenagent verwendet jetzt das von der Zertifizierungsstelle signierte Zertifikat, um sicheren HTTPS-Zugriff bereitzustellen. Das folgende Bild zeigt einen Agenten, der für sicheren Zugriff konfiguriert ist:



Erneuern Sie das HTTPS-Zertifikat der Konsole

Sie sollten das HTTPS-Zertifikat des Agenten vor Ablauf erneuern, um einen sicheren Zugriff zu gewährleisten. Wenn Sie das Zertifikat nicht vor Ablauf erneuern, wird eine Warnung angezeigt, wenn Benutzer über HTTPS auf die Webkonsole zugreifen.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **HTTPS-Setup**.

   Es werden Details zum Zertifikat angezeigt, einschließlich des Ablaufdatums.

3. Wählen Sie **Zertifikat ändern** und folgen Sie den Schritten zum Generieren einer CSR oder zum Installieren Ihres eigenen CA-signierten Zertifikats.

Konfigurieren eines Konsolenagenten zur Verwendung eines Proxyservers

Wenn Ihre Unternehmensrichtlinien die Verwendung eines Proxyservers für die gesamte Kommunikation mit dem Internet erfordern, müssen Sie Ihre Agenten für die Verwendung dieses Proxyservers konfigurieren. Wenn Sie während der Installation keinen Konsolenagenten für die Verwendung eines Proxyservers konfiguriert haben, können Sie den Konsolenagenten jederzeit für die Verwendung dieses Proxyservers konfigurieren.

Der Proxyserver des Agenten ermöglicht ausgehenden Internetzugriff ohne öffentliche IP oder NAT-Gateway. Der Proxyserver bietet ausgehende Konnektivität nur für den Konsolenagenten, nicht für Cloud Volumes ONTAP Systeme.

Wenn Cloud Volumes ONTAP -Systeme keinen ausgehenden Internetzugang haben, konfiguriert die Konsole sie so, dass sie den Proxyserver des Konsolenagenten verwenden. Sie müssen sicherstellen, dass die

Sicherheitsgruppe des Konsolenagenten eingehende Verbindungen über Port 3128 zulässt. Öffnen Sie diesen Port, nachdem Sie den Konsolenagenten bereitgestellt haben.

Wenn der Konsolenagent selbst keine ausgehende Internetverbindung hat, können Cloud Volumes ONTAP -Systeme den konfigurierten Proxyserver nicht verwenden.

Unterstützte Konfigurationen

- Transparente Proxyserver werden für Agenten unterstützt, die Cloud Volumes ONTAP -Systeme bedienen. Wenn Sie NetApp -Datendienste mit Cloud Volumes ONTAP verwenden, erstellen Sie einen dedizierten Agenten für Cloud Volumes ONTAP, bei dem Sie einen transparenten Proxyserver verwenden können.
- Explizite Proxyserver werden von allen Agenten unterstützt, einschließlich derjenigen, die Cloud Volumes ONTAP -Systeme verwalten, und derjenigen, die NetApp -Datendienste verwalten.
- HTTP und HTTPS.
- Der Proxyserver kann sich in der Cloud oder in Ihrem Netzwerk befinden.

Nachdem Sie einen Proxy konfiguriert haben, können Sie den Proxy-Typ nicht mehr ändern. Wenn Sie den Proxy-Typ ändern müssen, entfernen Sie den Konsolen-Agenten und fügen einen neuen Agenten mit dem neuen Proxy-Typ hinzu.

Aktivieren Sie einen expliziten Proxy auf einem Konsolenagenten

Wenn Sie einen Konsolenagenten für die Verwendung eines Proxyservers konfigurieren, verwenden dieser Agent und die von ihm verwalteten Cloud Volumes ONTAP -Systeme (einschließlich aller HA-Mediatoren) alle den Proxyserver.

Dieser Vorgang startet den Konsolenagenten neu. Stellen Sie sicher, dass der Konsolenagent im Leerlauf ist, bevor Sie fortfahren.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **Agent bearbeiten**.

   Zum Bearbeiten muss der Konsolenagent aktiv sein.

3. Wählen Sie **HTTP-Proxy-Konfiguration**.
4. Wählen Sie im Feld „Konfigurationstyp“ **Expliziter Proxy** aus.
5. Wählen Sie **Proxy aktivieren**.
6. Geben Sie den Server mit der Syntax an http://address:port oder https://address:port
7. Geben Sie einen Benutzernamen und ein Kennwort an, wenn für den Server eine Basisauthentifizierung erforderlich ist.

   Beachten Sie Folgendes:

   - Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.
   - Für einen Domänenbenutzer müssen Sie den ASCII-Code für das \ wie folgt eingeben: Domänenname%92Benutzername

Beispiel: netapp%92proxy

- Die Konsole unterstützt keine Passwörter, die das @-Zeichen enthalten.

8. Wählen Sie **Speichern**.

Aktivieren Sie einen transparenten Proxy für einen Konsolenagenten

Nur Cloud Volumes ONTAP unterstützt die Verwendung eines transparenten Proxys auf dem Konsolenagenten. Wenn Sie zusätzlich zu Cloud Volumes ONTAP NetApp -Datendienste verwenden, sollten Sie einen separaten Agenten für die Verwendung für Datendienste oder für Cloud Volumes ONTAP erstellen.

Stellen Sie vor der Aktivierung eines transparenten Proxys sicher, dass die folgenden Anforderungen erfüllt sind:

- Der Agent wird im selben Netzwerk wie der transparente Proxyserver installiert.
- Die TLS-Prüfung ist auf dem Proxyserver aktiviert.
- Sie verfügen über ein Zertifikat im PEM-Format, das mit dem auf dem transparenten Proxyserver verwendeten Zertifikat übereinstimmt.
- Sie verwenden den Konsolenagenten für keine anderen NetApp -Datendienste als Cloud Volumes ONTAP.

Um einen vorhandenen Agenten für die Verwendung eines transparenten Proxyservers zu konfigurieren, verwenden Sie das Wartungstool des Konsolenagenten, das über die Befehlszeile auf dem Konsolenagentenhost verfügbar ist.

Wenn Sie einen Proxyserver konfigurieren, wird der Konsolenagent neu gestartet. Stellen Sie sicher, dass der Konsolenagent im Leerlauf ist, bevor Sie fortfahren.

Schritte

Stellen Sie sicher, dass Sie über eine Zertifikatsdatei im PEM-Format für den Proxyserver verfügen. Wenn Sie kein Zertifikat haben, wenden Sie sich an Ihren Netzwerkadministrator, um eines zu erhalten.

1. Öffnen Sie eine Befehlszeilenschnittstelle auf dem Konsolenagent-Host.
2. Navigieren Sie zum Verzeichnis des Wartungstools des Konsolenagenten: `/opt/application/netapp/service-manager-2/agent-maint-console`
3. Führen Sie den folgenden Befehl aus, um den transparenten Proxy zu aktivieren. `/home/ubuntu/<certificate-file>.pem` ist das Verzeichnis und der Name der Zertifikatsdatei, die Sie für den Proxyserver haben:

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

   Stellen Sie sicher, dass die Zertifikatsdatei im PEM-Format vorliegt und sich im selben Verzeichnis wie der Befehl befindet, oder geben Sie den vollständigen Pfad zur Zertifikatsdatei an.

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

Ändern Sie den transparenten Proxy für den Konsolenagenten

Sie können den vorhandenen transparenten Proxy-Server eines Konsolen-Agenten aktualisieren, indem Sie den `proxy update` Befehl oder entfernen Sie den transparenten Proxyserver mithilfe des `proxy remove` Befehl. Weitere Informationen finden Sie in der Dokumentation zu"Agenten-Wartungskonsole" .

> Nachdem Sie einen Proxy konfiguriert haben, können Sie den Proxy-Typ nicht mehr ändern. Wenn Sie den Proxy-Typ ändern müssen, entfernen Sie den Konsolen-Agenten und fügen einen neuen Agenten mit dem neuen Proxy-Typ hinzu.

Aktualisieren Sie den Proxy des Konsolenagenten, wenn dieser den Zugriff auf das Internet verliert

Wenn sich die Proxy-Konfiguration für Ihr Netzwerk ändert, verliert Ihr Agent möglicherweise den Zugriff auf das Internet. Zum Beispiel, wenn jemand das Passwort für den Proxyserver ändert oder das Zertifikat aktualisiert. In diesem Fall müssen Sie direkt vom Konsolenagent-Host auf die Benutzeroberfläche zugreifen und die Einstellungen aktualisieren. Stellen Sie sicher, dass Sie Netzwerkzugriff auf den Konsolen-Agent-Host haben und sich bei der Konsole anmelden können.

Aktivieren Sie den direkten API-Verkehr

Wenn Sie einen Konsolenagenten für die Verwendung eines Proxyservers konfiguriert haben, können Sie den direkten API-Verkehr auf dem Konsolenagenten aktivieren, um API-Aufrufe direkt an die Dienste des Cloud-Anbieters zu senden, ohne den Proxy zu durchlaufen. Agenten, die in AWS, Azure oder Google Cloud ausgeführt werden, unterstützen diese Option.

Wenn Sie Azure Private Links mit Cloud Volumes ONTAP deaktivieren und Service-Endpunkte verwenden, aktivieren Sie den direkten API-Verkehr. Andernfalls wird der Datenverkehr nicht richtig weitergeleitet.

"Erfahren Sie mehr über die Verwendung eines Azure Private Link oder von Service-Endpunkten mit Cloud Volumes ONTAP"

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **Agent bearbeiten**.

   Zum Bearbeiten muss der Konsolenagent aktiv sein.

3. Wählen Sie **Direkten API-Verkehr unterstützen**.
4. Aktivieren Sie das Kontrollkästchen, um die Option zu aktivieren, und wählen Sie dann **Speichern**.

Erfordert die Verwendung von IMDSv2 auf Amazon EC2-Instanzen

Die NetApp Console unterstützt den Amazon EC2 Instance Metadata Service Version 2 (IMDSv2) mit dem Konsolenagenten und mit Cloud Volumes ONTAP (einschließlich des Mediators für HA-Bereitstellungen). In den meisten Fällen wird IMDSv2 auf neuen EC2-Instanzen automatisch konfiguriert. IMDSv1 wurde vor März 2024 aktiviert. Falls Ihre Sicherheitsrichtlinien dies erfordern, müssen Sie IMDSv2 möglicherweise manuell auf Ihren EC2-Instances konfigurieren.

Bevor Sie beginnen

- Die Version des Konsolenagenten muss 3.9.38 oder höher sein.
- Cloud Volumes ONTAP muss eine der folgenden Versionen ausführen:
  - 9.12.1 P2 (oder ein nachfolgender Patch)
  - 9.13.0 P4 (oder ein nachfolgender Patch)
  - 9.13.1 oder jede Version nach dieser Veröffentlichung
- Diese Änderung erfordert einen Neustart der Cloud Volumes ONTAP Instanzen.
- Für diese Schritte ist die Verwendung der AWS CLI erforderlich, da Sie das Antwort-Hop-Limit auf 3 ändern müssen.

Informationen zu diesem Vorgang

IMDSv2 bietet verbesserten Schutz vor Schwachstellen. "Weitere Informationen zu IMDSv2 finden Sie im AWS Security Blog"

Der Instance Metadata Service (IMDS) wird auf EC2-Instances wie folgt aktiviert:

- Für neue Konsolen-Agent-Bereitstellungen über die Konsole oder mithilfe von "Terraform-Skripte" , IMDSv2 ist auf der EC2-Instance standardmäßig aktiviert.
- Wenn Sie eine neue EC2-Instanz in AWS starten und dann die Konsolenagent-Software manuell installieren, ist IMDSv2 standardmäßig ebenfalls aktiviert.
- Wenn Sie den Konsolenagenten vom AWS Marketplace aus starten, ist IMDSv1 standardmäßig aktiviert. Sie können IMDSv2 auf der EC2-Instance manuell konfigurieren.
- Für vorhandene Konsolenagenten wird IMDSv1 weiterhin unterstützt, Sie können IMDSv2 jedoch auch manuell auf der EC2-Instance konfigurieren, wenn Sie dies bevorzugen.
- Für Cloud Volumes ONTAP ist IMDSv1 standardmäßig auf neuen und vorhandenen Instanzen aktiviert. Sie können IMDSv2 auf den EC2-Instanzen manuell konfigurieren, wenn Sie dies bevorzugen.

Schritte

1. Erfordert die Verwendung von IMDSv2 auf der Konsolen-Agenteninstanz:

   a. Stellen Sie eine Verbindung zur Linux-VM für den Konsolen-Agenten her.

      Als Sie die Konsolen-Agent-Instanz in AWS erstellt haben, haben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel angegeben. Sie können dieses Schlüsselpaar verwenden, um per SSH auf die Instanz zuzugreifen. Der Benutzername für die EC2-Linux-Instanz ist ubuntu (für Konsolenagenten, die vor Mai 2023 erstellt wurden, war der Benutzername ec2-user).

      "AWS Docs: Verbinden Sie sich mit Ihrer Linux-Instance"

   b. Installieren Sie die AWS CLI.

      "AWS-Dokumente: Installieren oder aktualisieren Sie auf die neueste Version der AWS CLI"

   c. Verwenden Sie die `aws ec2 modify-instance-metadata-options` Befehl, um die Verwendung von IMDSv2 zu verlangen und das Hop-Limit für PUT-Antworten auf 3 zu ändern.

      Beispiel

```
aws ec2 modify-instance-metadata-options \
    --instance-id <instance-id> \
    --http-put-response-hop-limit 3 \
    --http-tokens required \
    --http-endpoint enabled
```

Der `http-tokens` Der Parameter setzt IMDSv2 auf „erforderlich“. Wann `http-tokens` erforderlich ist, müssen Sie auch `http-endpoint` auf aktiviert.

2. Erfordert die Verwendung von IMDSv2 auf Cloud Volumes ONTAP -Instanzen:
   a. Gehen Sie zum "Amazon EC2-Konsole"
   b. Wählen Sie im Navigationsbereich **Instanzen** aus.
   c. Wählen Sie eine Cloud Volumes ONTAP Instanz aus.
   d. Wählen Sie **Aktionen > Instanzeinstellungen > Optionen für Instanzmetadaten ändern**.
   e. Wählen Sie im Dialogfeld **Optionen für Instanzmetadaten ändern** Folgendes aus:
      - Wählen Sie für **Instanzmetadatendienst Aktivieren** aus.
      - Wählen Sie für **IMDSv2 Erforderlich** aus.
      - Wählen Sie **Speichern**.
   f. Wiederholen Sie diese Schritte für andere Cloud Volumes ONTAP Instanzen, einschließlich des HA-Mediators.
   g. "Stoppen und starten Sie die Cloud Volumes ONTAP -Instanzen"

Ergebnis

Die Konsolen-Agent-Instanz und die Cloud Volumes ONTAP Instanzen sind jetzt für die Verwendung von IMDSv2 konfiguriert.

Upgrades des Konsolenagenten verwalten

Wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden, aktualisiert die NetApp Console Ihren Konsolenagenten automatisch auf die neueste Version, sofern der Konsolenagent über ausgehenden Internetzugang verfügt, um das Softwareupdate abzurufen.

Wenn Sie manuell verwalten müssen, wann der Konsolenagent aktualisiert wird, können Sie automatische Upgrades für den Standardmodus oder den eingeschränkten Modus deaktivieren.

Automatische Upgrades deaktivieren

Das Deaktivieren des automatischen Upgrades für Ihren Konsolenagenten umfasst zwei Schritte. Zuerst müssen Sie sicherstellen, dass Ihr Konsolenagent fehlerfrei und auf dem neuesten Stand ist. Anschließend bearbeiten Sie eine Konfigurationsdatei, um automatische Upgrades zu deaktivieren.

Sie können automatische Upgrades nur deaktivieren, wenn Sie über einen Konsolenagenten der Version 3.9.48 oder höher verfügen.

Überprüfen Sie den Zustand Ihres Agenten

Sie sollten überprüfen, ob Ihr Agent stabil ist und alle auf Ihrer Agent-VM ausgeführten Container fehlerfrei und funktionsfähig sind. Nachdem Sie automatische Upgrades deaktiviert haben, sucht Ihre Agent-VM nicht mehr nach neuen Diensten oder Upgrade-Paketen.

Verwenden Sie einen der folgenden Befehle, um Ihren Konsolenagenten zu überprüfen. Alle Dienste sollten den Status „Wird ausgeführt“ haben. Wenn dies nicht der Fall ist, wenden Sie sich an den NetApp -Support, bevor Sie das automatische Upgrade deaktivieren.

Docker (für Ubuntu- und VCenter-Bereitstellungen)

```
docker ps -a
```

Podman

```
podman ps -a
```

Automatisches Upgrade für den Agenten deaktivieren

Sie deaktivieren automatische Upgrades, indem Sie das Flag *isUpgradeDisabled* in der Datei *com/opt/application/netapp/service-manager-2/config.json* setzen. Standardmäßig ist dieses Flag auf „Falsch“ gesetzt und Ihr Agent wird automatisch aktualisiert. Sie können dieses Flag auf „true“ setzen, um automatische Upgrades zu deaktivieren. Sie sollten mit der JSON-Syntax vertraut sein, bevor Sie diesen Schritt abschließen.

Um das automatische Upgrade wieder zu aktivieren, führen Sie diese Schritte aus und setzen Sie das Flag *isUpgradeDisabled* auf „false“.

Schritte

1. Stellen Sie sicher, dass Sie überprüft haben, dass Ihr Agent auf dem neuesten Stand und fehlerfrei ist.
2. Erstellen Sie eine Sicherungskopie der Datei */opt/application/netapp/service-manager-2/config.json*, um sicherzustellen, dass Sie Ihre Änderungen rückgängig machen können.
3. Bearbeiten Sie die Datei */opt/application/netapp/service-manager-2/config.json* und ändern Sie den Wert des Flags *isUpgradeDisabled* in „true“.

   ```
   "isUpgradeDisabled": true,
   ```

4. Speichern Sie Ihre Datei.
5. Starten Sie den Dienst Service Manager 2 neu, indem Sie den folgenden Befehl ausführen:

   ```
   systemctl restart netapp-service-manager.service
   ```

6. Führen Sie den folgenden Befehl aus und überprüfen Sie, ob der Status des Agenten als *aktiv (wird ausgeführt)* angezeigt wird: _

```
systemctl status netapp-service-manager.service
_
```

Aktualisieren Sie den Konsolenagenten

Der Konsolenagent muss während des Upgradevorgangs neu gestartet werden, sodass die NetApp Console während des Upgrades nicht verfügbar ist.

Schritte

1. Laden Sie die Console-Agent-Software von der "NetApp Support Site" .
2. Kopieren Sie das Installationsprogramm auf den Linux-Host.
3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

   ```
   chmod +x /path/NetApp-Console-Agent-Offline-<version>
   ```

   Dabei ist <Version> die Version des Konsolenagenten, die Sie heruntergeladen haben.

4. Führen Sie das Installationsskript aus:

   ```
   sudo /path/NetApp-Console-Agent-Offline-<version>
   ```

   Dabei ist <Version> die Version des Agenten, die Sie heruntergeladen haben.

5. Nachdem das Upgrade abgeschlossen ist, können Sie die Version des Agenten überprüfen, indem Sie zu **Administration > Support > Agenten** gehen.

Arbeiten mit mehreren Konsolenagenten

Wenn Sie mehrere Konsolenagenten verwenden, können Sie direkt von der Konsole aus zwischen diesen Konsolenagenten wechseln, um die zugehörigen Systeme anzuzeigen.

Wechseln zwischen Konsolenagenten

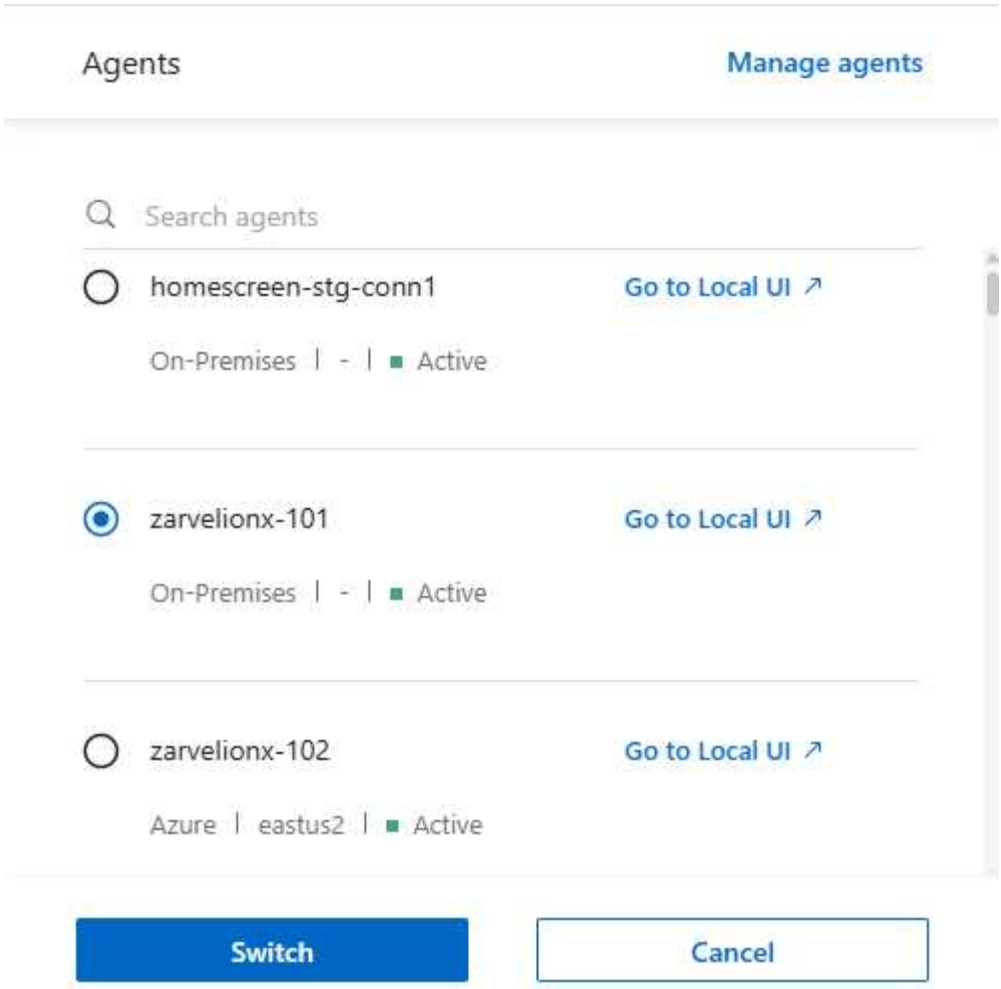
Wenn Sie über mehrere Konsolenagenten verfügen, können Sie zwischen ihnen wechseln, um die Systeme anzuzeigen, die einem bestimmten Agenten zugeordnet sind.

Beispielsweise haben Sie in einer Multi-Cloud-Umgebung möglicherweise einen Agenten in AWS und einen anderen in Google Cloud. Wechseln Sie zwischen diesen Agenten, um die Cloud Volumes ONTAP -Systeme in den jeweiligen Cloud-Umgebungen zu verwalten.

Diese Option ist nicht verfügbar, wenn Sie die NetApp Console über die lokale Benutzeroberfläche des Agenten anzeigen.

Schritt

1. Wählen Sie das Symbol „Konsolenagenten“ ( ), um die Liste der verfügbaren Agenten anzuzeigen.



Ergebnis

Die Konsole wird aktualisiert und zeigt die mit dem ausgewählten Agenten verknüpften Systeme an.

Einrichten einer Notfallwiederherstellungskonfiguration

Sie können ein System zur Notfallwiederherstellung gleichzeitig mit mehreren Konsolenagenten verwalten. Wenn ein Konsolenagent ausfällt, können Sie zum anderen Agenten wechseln, um das System sofort zu verwalten.

Schritte

1. Wechseln Sie zu dem anderen Konsolenagenten, den Sie mit dem Konsolenagenten verwalten möchten.
2. Entdecken Sie das vorhandene System.
   - "Fügen Sie vorhandene Cloud Volumes ONTAP -Systeme zur Konsole hinzu"
   - "Entdecken Sie ONTAP Cluster"
3. Wenn Sie ein Cloud Volumes ONTAP -System verwalten, stellen Sie den Kapazitätsverwaltungsmodus auf **Manueller Modus** ein.

   Um Konflikte zu vermeiden, sollte nur der Hauptkonsolenagent auf den **Automatikmodus** eingestellt werden.

   "Erfahren Sie mehr über den Kapazitätsverwaltungsmodus"

Fehlerbehebung beim Konsolen-Agent

Um Probleme mit einem Konsolenagenten zu beheben, können Sie die Probleme selbst überprüfen oder mit dem NetApp -Support zusammenarbeiten, der Sie möglicherweise nach Ihrer System-ID, Agentenversion oder den neuesten AutoSupport -Nachrichten fragt.

Wenn Sie über ein NetApp Support Site-Konto verfügen, können Sie auch die"NetApp Wissensdatenbank."

Häufige Fehlermeldungen und Lösungen

In der Tabelle sind häufige Fehlermeldungen und Lösungsvorschläge aufgeführt:

Fehlermeldung	Erläuterung	Was zu tun
Die Benutzeroberfläche des Konsolenagenten konnte nicht geladen werden	Die Agenteninstallation ist fehlgeschlagen	• Stellen Sie sicher, dass der Service Manager-Dienst aktiv ist. • Stellen Sie sicher, dass alle Container ausgeführt werden. • Stellen Sie sicher, dass Ihre Firewall den Zugriff auf den Dienst über Port 8888 zulässt. • Wenn das Problem weiterhin besteht, wenden Sie sich an den Support.
Auf die NetApp Agent-Benutzeroberfläche kann nicht zugegriffen werden	Diese Meldung wird angezeigt, wenn versucht wird, auf die IP-Adresse eines Agenten zuzugreifen. Die Initialisierung des Agenten kann fehlschlagen, wenn er nicht über den richtigen Netzwerkzugriff verfügt oder instabil ist.	• Stellen Sie eine Verbindung zum Konsolenagenten her. • Überprüfen Sie, ob der Service Manager-Dienst • Stellen Sie sicher, dass der Agent über den erforderlichen Netzwerkzugriff verfügt."Erfahren Sie mehr über erforderliche Endpunkte für den Netzwerkzugriff."
Agenteneinstellungen konnten nicht geladen werden	Die Konsole zeigt diese Meldung an, wenn Sie versuchen, auf die Seite mit den Agenteneinstellungen zuzugreifen.	• Überprüfen Sie, ob der OCCM-Container ausgeführt wird und funktioniert. • Wenn das Problem weiterhin besteht, wenden Sie sich an den Support.
Supportinformationen für den Agenten konnten nicht geladen werden.	Diese Meldung wird angezeigt, wenn der Agent nicht auf Ihr Supportkonto zugreifen kann.	• *.

Überprüfen Sie den Status des Konsolenagenten

Verwenden Sie einen der folgenden Befehle, um Ihren Konsolenagenten zu überprüfen. Alle Dienste sollten den Status „Wird ausgeführt“ haben. Wenn dies nicht der Fall ist, wenden Sie sich an den NetApp Support.

Ausführlichere Informationen zum Zugriff auf die Konsolen-Agent-Diagnose finden Sie in den folgenden Themen:

- "Überprüfen Sie den Status des Konsolenagenten (für Linux-Hostbereitstellungen)."
- "Überprüfen Sie den Status des Konsolenagenten (für VCenter-Bereitstellungen)."

Docker (für Ubuntu- und VCenter-Bereitstellungen)

```
docker ps -a
```

Podman (für RedHat Enterprise Linux-Bereitstellungen)

```
podman ps -a
```

Anzeigen der Konsolen-Agent-Version

Zeigen Sie die Version des Konsolenagenten an, um das Upgrade zu bestätigen, oder teilen Sie sie Ihrem NetApp -Vertreter mit.

Schritte

1. Wählen Sie **Administration > Support > Agenten**.

   Die Konsole zeigt die Version oben auf der Seite an.

Überprüfen des Netzwerkzugriffs

Stellen Sie sicher, dass der Konsolenagent über den erforderlichen Netzwerkzugriff verfügt."Erfahren Sie mehr über die erforderlichen Netzwerkzugriffspunkte."

Probleme bei der Installation des Konsolenagenten

Wenn die Installation fehlschlägt, sehen Sie sich den Bericht und die Protokolle an, um die Probleme zu beheben.

Sie können auch direkt vom Konsolen-Agent-Host in den folgenden Verzeichnissen auf den Validierungsbericht im JSON-Format und die Konfigurationsprotokolle zugreifen:

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- Bei der Bereitstellung neuer Agenten prüft NetApp die folgenden Endpunkte:"hier aufgeführt" . Diese Konfigurationsprüfung schlägt mit einem Fehler fehl, wenn Sie die vorherigen Endpunkte verwenden, die für Upgrades verwendet wurden."hier aufgeführt" . NetApp empfiehlt, Ihre Firewall-Regeln so schnell wie möglich zu aktualisieren, um den Zugriff auf die aktuellen Endpunkte zu ermöglichen und den Zugriff auf die vorherigen Endpunkte zu blockieren."Erfahren Sie, wie Sie Ihr Netzwerk aktualisieren" .
- Wenn Sie die Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

Deaktivieren Sie Konfigurationsprüfungen für manuelle Installationen

Es kann vorkommen, dass Sie die Konfigurationsprüfungen deaktivieren müssen, die während der Installation die ausgehende Konnektivität überprüfen. Beispiel:

- Wenn Sie einen Agenten manuell in Ihrer Government Cloud-Umgebung installieren, müssen Sie die Konfigurationsprüfungen deaktivieren, sonst schlägt die Installation fehl.
- Sie können diese Prüfungen auch deaktivieren, wenn Sie für Agent-Upgrades weiterhin die vorherige Endpunktliste verwenden.

Schritte

Sie deaktivieren die Konfigurationsprüfung, indem Sie das Flag *skipConfigCheck* in der Datei *com/opt/application/netapp/service-manager-2/config.json* setzen. Standardmäßig ist dieses Flag auf „false“ gesetzt und die Konfigurationsprüfung überprüft den ausgehenden Zugriff für den Agenten. Setzen Sie dieses Flag auf „true“, um die Prüfung zu deaktivieren. Sie sollten mit der JSON-Syntax vertraut sein, bevor Sie diesen Schritt abschließen.

Um die Konfigurationsprüfung wieder zu aktivieren, führen Sie diese Schritte aus und setzen Sie das Flag *skipConfigCheck* auf „false“.

Schritte

1. Greifen Sie als Root oder mit Sudo-Berechtigungen auf den Konsolen-Agent-Host zu.
2. Erstellen Sie eine Sicherungskopie der Datei */opt/application/netapp/service-manager-2/config.json*, um sicherzustellen, dass Sie Ihre Änderungen rückgängig machen können.
3. Stoppen Sie den Dienst Service Manager 2, indem Sie den folgenden Befehl ausführen:

```
systemctl stop netapp-service-manager.service
```

1. Bearbeiten Sie die Datei */opt/application/netapp/service-manager-2/config.json* und ändern Sie den Wert des Flags *skipConfigCheck* auf „true“.

```
  "skipConfigCheck": true,
```

2. Speichern Sie Ihre Datei.
3. Starten Sie den Dienst Service Manager 2 neu, indem Sie den folgenden Befehl ausführen:

```
systemctl restart netapp-service-manager.service
```

Fehlgeschlagene Installation auf den für Upgrades verwendeten Endpunkten

Wenn Sie immer noch die"vorherige Endpunkte" für Agent-Upgrades verwendet wird, schlägt die Validierung mit einem Fehler fehl. Um dies zu vermeiden, deaktivieren Sie das Kontrollkästchen **Validierungsagent-Konfiguration** oder überspringen Sie die Konfigurationsprüfung bei der Installation in einem VCenter.

NetApp empfiehlt, Ihre Firewall-Regeln zu aktualisieren, um den Zugriff auf die"aktuelle Endpunkte" so bald wie möglich. "Erfahren Sie, wie Sie Ihre Endpunkte aktualisieren" .

Stellen Sie sicher, dass der einzige Fehler mit den vorherigen Endpunkten zusammenhängt:

- https://bluexpinfraprod.eastus2.data.azurecr.io
- https://bluexpinfraprod.azurecr.io

Wenn weitere Fehler vorliegen, müssen Sie diese beheben, bevor Sie fortfahren.

Arbeiten Sie mit dem NetApp Support

Wenn Sie die Probleme mit Ihrem Konsolenagenten nicht lösen konnten, sollten Sie sich an den NetApp -Support wenden. Der NetApp Support fragt möglicherweise nach der Konsolen-Agent-ID oder fordert Sie auf, ihm die Konsolen-Agent-Protokolle zu senden, falls diese noch nicht vorliegen.

Suchen Sie die Konsolen-Agent-ID

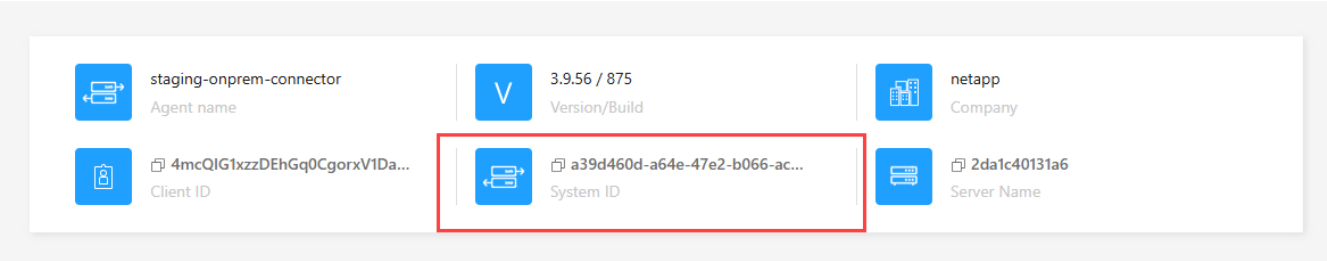
Um Ihnen den Einstieg zu erleichtern, benötigen Sie möglicherweise die System-ID Ihres Konsolenagenten. Die ID wird normalerweise für Lizenzierungs- und Fehlerbehebungszwecke verwendet.

Schritte

1. Wählen Sie **Administration > Support > Agenten**.

   Die System-ID finden Sie oben auf der Seite.

   Beispiel

2. Bewegen Sie den Mauszeiger über die ID und klicken Sie darauf, um sie zu kopieren.

Laden Sie eine AutoSupport -Nachricht herunter oder senden Sie sie

Wenn bei Ihnen Probleme auftreten, werden Sie von NetApp möglicherweise aufgefordert, zur Fehlerbehebung eine AutoSupport -Nachricht an den NetApp -Support zu senden.

Aufgrund des Lastenausgleichs benötigt die NetApp Console bis zu fünf Stunden, um AutoSupport -Nachrichten zu senden. Laden Sie für dringende Mitteilungen die Datei herunter und senden Sie sie manuell.

Schritte

1. Wählen Sie **Administration > Support > Agenten**.
2. Wählen Sie je nachdem, wie Sie die Informationen an den NetApp Support senden müssen, eine der folgenden Optionen:
   a. Wählen Sie die Option zum Herunterladen der AutoSupport -Nachricht auf Ihren lokalen Computer. Sie können es dann mit einer bevorzugten Methode an den NetApp -Support senden.
   b. Wählen Sie * AutoSupport senden*, um die Nachricht direkt an den NetApp -Support zu senden.

Beheben von Downloadfehlern bei Verwendung eines Google Cloud NAT-Gateways

Der Konsolenagent lädt automatisch Softwareupdates für Cloud Volumes ONTAP herunter. Ihre Konfiguration kann dazu führen, dass der Download fehlschlägt, wenn ein Google Cloud NAT-Gateway verwendet wird. Sie können dieses Problem beheben, indem Sie die Anzahl der Teile begrenzen, in die das Software-Image unterteilt ist. Dieser Schritt muss mithilfe der API abgeschlossen werden.

Schritt

1. Senden Sie eine PUT-Anfrage an /occm/config mit dem folgenden JSON als Text:

```
{
  "maxDownloadSessions": 32
}
```

   Der Wert für *maxDownloadSessions* kann 1 oder eine beliebige Ganzzahl größer als 1 sein. Wenn der Wert 1 ist, wird das heruntergeladene Bild nicht geteilt.

   Beachten Sie, dass 32 ein Beispielwert ist. Der Wert hängt von Ihrer NAT-Konfiguration und der Anzahl gleichzeitiger Sitzungen ab.

"Erfahren Sie mehr über den API-Aufruf /occm/config"

Holen Sie sich Hilfe von der NetApp Knowledge Base

"Informationen zur Fehlerbehebung anzeigen, die vom NetApp Support-Team erstellt wurden" .

Deinstallieren und Entfernen eines Konsolenagenten

Deinstallieren Sie einen Konsolenagenten, um Probleme zu beheben oder ihn dauerhaft vom Host zu entfernen. Die erforderlichen Schritte hängen vom verwendeten Bereitstellungsmodus ab. Nachdem Sie einen Konsolenagenten aus Ihrer Umgebung entfernt haben, können Sie ihn aus der Konsole entfernen.

"Erfahren Sie mehr über die Bereitstellungsmodi der NetApp Console" .

Deinstallieren Sie den Agenten, wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden

Wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden (mit anderen Worten, der Agent-Host verfügt über eine ausgehende Konnektivität), sollten Sie die folgenden Schritte ausführen, um den Agenten zu deinstallieren.

Schritte

1. Stellen Sie eine Verbindung zur Linux-VM für den Agenten her.
2. Führen Sie vom Linux-Host aus das Deinstallationsskript aus:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   silent führt das Skript aus, ohne Sie zur Bestätigung aufzufordern.

Entfernen von Konsolenagenten aus der Konsole

Wenn ein Konsolenagent inaktiv ist, können Sie ihn aus der Agentenliste entfernen. Dies ist möglicherweise der Fall, wenn Sie die virtuelle Agentenmaschine löschen oder die Agentensoftware deinstallieren.

Beachten Sie beim Entfernen eines Konsolenagenten Folgendes:

- Durch diese Aktion wird die virtuelle Maschine nicht gelöscht.
- Diese Aktion kann nicht rückgängig gemacht werden. Wenn Sie einen Konsolenagenten einmal entfernt haben, können Sie ihn nicht wieder hinzufügen.

Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen inaktiven Agenten und wählen Sie **Agent entfernen**.
3. Geben Sie zur Bestätigung den Namen des Agenten ein und wählen Sie dann **Entfernen**.

Standardkonfiguration für den Konsolenagenten

Informieren Sie sich vor der Bereitstellung des Konsolenagenten über dessen Konfiguration.

Standardkonfiguration mit Internetzugang

Die folgenden Konfigurationsdetails gelten, wenn Sie einen Konsolenagenten von der NetApp Console oder vom Marktplatz Ihres Cloud-Anbieters bereitgestellt haben oder wenn Sie einen Konsolenagenten manuell auf einem lokalen Linux-Host mit Internetzugang installiert haben.

AWS-Details

Wenn Sie einen Konsolenagenten über die Konsole oder den Marktplatz des Cloud-Anbieters bereitgestellt haben, beachten Sie Folgendes:

- Der EC2-Instanztyp ist t3.2xlarge.
- Das Betriebssystem für das Image ist Ubuntu 22.04 LTS.

  Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Die Installation umfasst Docker Engine, das erforderliche Container-Orchestrierungstool.
- Der Benutzername für die EC2-Linux-Instanz ist ubuntu (für Agenten, die vor Mai 2023 erstellt wurden, lautet der Benutzername ec2-user).

- Die Standardsystemfestplatte ist eine 100-GiB-gp2-Festplatte.

Azure-Details

Wenn Sie einen Konsolenagenten über die Konsole oder den Marktplatz des Cloud-Anbieters bereitgestellt haben, beachten Sie Folgendes:

- Der VM-Typ ist Standard_D8s_v3.
- Das Betriebssystem für das Image ist Ubuntu 22.04 LTS.

  Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Die Installation umfasst Docker Engine, das erforderliche Container-Orchestrierungstool.
- Die Standardsystemfestplatte ist eine 100-GiB-Premium-SSD-Festplatte.

Google Cloud-Details

Wenn Sie einen Konsolenagenten über die Konsole bereitgestellt haben, beachten Sie Folgendes:

- Die VM-Instanz ist n2-standard-8.
- Das Betriebssystem für das Image ist Ubuntu 22.04 LTS.

  Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Die Installation umfasst Docker Engine, das erforderliche Container-Orchestrierungstool.
- Die Standardsystemfestplatte ist eine persistente SSD-Festplatte mit 100 GiB.

Installationsordner

Der Installationsordner des Agenten befindet sich am folgenden Speicherort:

/opt/application/netapp/cloudmanager

Protokolldateien

Protokolldateien sind in den folgenden Ordnern enthalten:

- /opt/application/netapp/cloudmanager/log oder
- /opt/application/netapp/service-manager-2/logs (beginnend mit neuen 3.9.23-Installationen)

  Die Protokolle in diesen Ordnern enthalten Details zum Konsolenagenten.

- /opt/application/netapp/cloudmanager/docker_occm/data/log

  Die Protokolle in diesem Ordner enthalten Details zu Cloud-Diensten und dem Konsolendienst, der auf dem Konsolenagenten ausgeführt wird.

Konsolenagentdienst

- Der Konsolenagentdienst heißt occm.

- Der OCCM-Dienst ist vom MySQL-Dienst abhängig.

  Wenn der MySQL-Dienst ausfällt, fällt auch der OCCM-Dienst aus.

Häfen

Der Agent verwendet die folgenden Ports auf dem Linux-Host:

- 80 für HTTP-Zugriff
- 443 für HTTPS-Zugriff

Standardkonfiguration ohne Internetzugang

Die folgende Konfiguration gilt, wenn Sie den Konsolen-Agent manuell auf einem lokalen Linux-Host installiert haben, der keinen Internetzugang hat. "Erfahren Sie mehr über diese Installationsoption" .

- Der Installationsordner des Agenten befindet sich am folgenden Speicherort:

  /opt/application/netapp/ds

- Protokolldateien sind in den folgenden Ordnern enthalten:

  /var/lib/docker/volumes/ds_occmdata/_data/log

  Die Protokolle in diesem Ordner enthalten Details zum Konsolenagenten und zu Docker-Images.

- Alle Dienste werden in Docker-Containern ausgeführt

  Die Dienste sind abhängig vom laufenden Docker-Runtime-Dienst

- Der Agent verwendet die folgenden Ports auf dem Linux-Host:
  - 80 für HTTP-Zugriff
  - 443 für HTTPS-Zugriff

Erzwingen Sie ONTAP -Berechtigungen für ONTAP Advanced View (ONTAP System Manager).

Standardmäßig ermöglichen die Anmeldeinformationen des Konsolenagenten den Benutzern den Zugriff auf die erweiterte Ansicht (ONTAP System Manager). Sie können Benutzer stattdessen zur Eingabe ihrer ONTAP Anmeldeinformationen auffordern. Dadurch wird sichergestellt, dass die ONTAP Berechtigungen eines Benutzers angewendet werden, wenn er mit ONTAP Clustern sowohl in Cloud Volumes ONTAP als auch in lokalen ONTAP -Clustern arbeitet.

Sie müssen über die Rolle des Organisationsadministrators verfügen, um die Einstellungen des Konsolenagenten bearbeiten zu können.

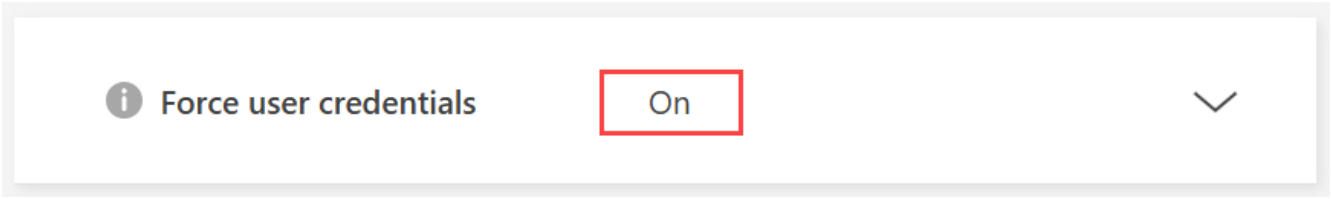
Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **Agent**

bearbeiten.

Zum Bearbeiten muss der Konsolenagent aktiv sein.

3. Erweitern Sie die Option **Anmeldeinformationen erzwingen**.
4. Aktivieren Sie das Kontrollkästchen, um die Option **Anmeldeinformationen erzwingen** zu aktivieren, und wählen Sie dann **Speichern**.
5. Stellen Sie sicher, dass die Option **Anmeldeinformationen erzwingen** aktiviert ist.



Anmeldeinformationen und Abonnements

AWS

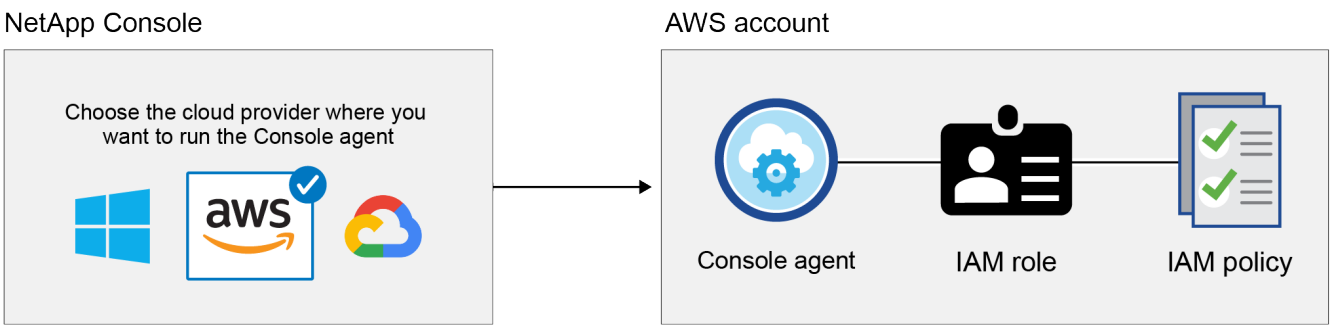
Erfahren Sie mehr über AWS-Anmeldeinformationen und Berechtigungen in der NetApp Console

Erfahren Sie, wie die NetApp Console AWS-Anmeldeinformationen verwendet, um Aktionen in Ihrem Namen auszuführen, und wie diese Anmeldeinformationen mit Marktplatzabonnements verknüpft werden. Das Verständnis dieser Details kann hilfreich sein, wenn Sie die Anmeldeinformationen für ein oder mehrere AWS-Konten in der NetApp Console verwalten. Sie möchten beispielsweise erfahren, wann Sie zusätzliche AWS-Anmeldeinformationen hinzufügen müssen.

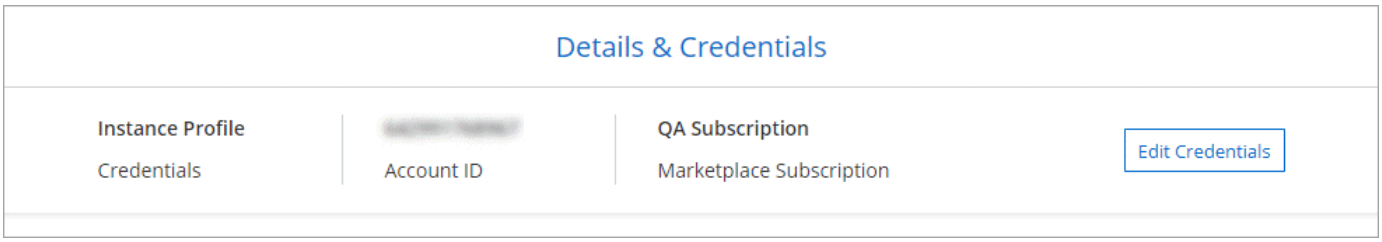
Anfängliche AWS-Anmeldeinformationen

Wenn Sie einen Konsolenagenten über die Konsole bereitstellen, müssen Sie die ARN einer IAM-Rolle oder Zugriffsschlüssel für einen IAM-Benutzer angeben. Die Authentifizierungsmethode muss über Berechtigungen zum Bereitstellen der Konsole in AWS verfügen. Die erforderlichen Berechtigungen sind im Link:task-install-agent-aws-the Console.html#console-permissions-aws[Agent-Bereitstellungsrichtlinie für AWS] aufgeführt.

Wenn die Konsole die Konsolenagentinstanz in AWS startet, erstellt sie eine IAM-Rolle und ein Instanzprofil für die Instanz. Außerdem wird eine Richtlinie angehängt, die dem Konsolenagenten die Berechtigung erteilt, Ressourcen und Prozesse innerhalb dieses AWS-Kontos zu verwalten. "Überprüfen Sie, wie die Konsole die Berechtigungen verwendet" .



Wenn Sie ein neues Cloud Volumes ONTAP -System hinzufügen, wählt die Konsole standardmäßig diese AWS-Anmeldeinformationen aus:



Stellen Sie alle Ihre Cloud Volumes ONTAP -Systeme mit den anfänglichen AWS-Anmeldeinformationen bereit, oder fügen Sie zusätzliche Anmeldeinformationen hinzu.

Zusätzliche AWS-Anmeldeinformationen

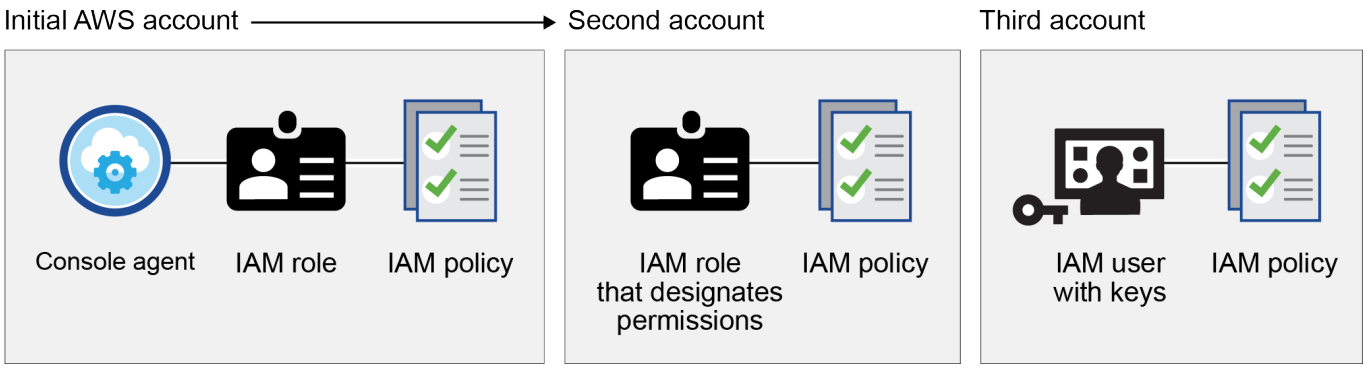
In den folgenden Fällen können Sie der Konsole zusätzliche AWS-Anmeldeinformationen hinzufügen:

- So verwenden Sie Ihren vorhandenen Konsolenagenten mit einem zusätzlichen AWS-Konto
- So erstellen Sie einen neuen Agenten in einem bestimmten AWS-Konto
- So erstellen und verwalten Sie FSx for ONTAP Dateisysteme

Weitere Einzelheiten finden Sie in den folgenden Abschnitten.

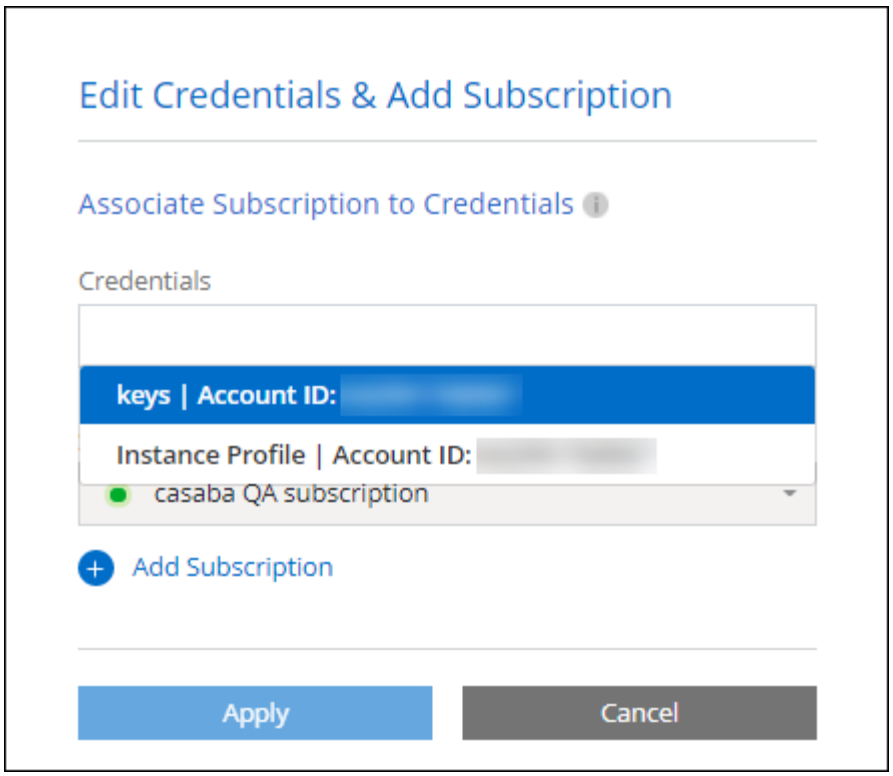
Fügen Sie AWS-Anmeldeinformationen hinzu, um einen Konsolenagenten mit einem anderen AWS-Konto zu verwenden

Wenn Sie die Konsole mit zusätzlichen AWS-Konten verwenden möchten, können Sie entweder AWS-Schlüssel für einen IAM-Benutzer oder die ARN einer Rolle in einem vertrauenswürdigen Konto angeben. Das folgende Bild zeigt zwei zusätzliche Konten, eines, das Berechtigungen über eine IAM-Rolle in einem vertrauenswürdigen Konto bereitstellt, und ein anderes über die AWS-Schlüssel eines IAM-Benutzers:



Anschließend fügen Sie die Kontoanmeldeinformationen zur Konsole hinzu, indem Sie den Amazon-Ressourcennamen (ARN) der IAM-Rolle oder die AWS-Schlüssel für den IAM-Benutzer angeben.

Sie können beispielsweise beim Erstellen eines neuen Cloud Volumes ONTAP Systems zwischen Anmeldeinformationen wechseln:



"Erfahren Sie, wie Sie einem vorhandenen Agenten AWS-Anmeldeinformationen hinzufügen."

Fügen Sie AWS-Anmeldeinformationen hinzu, um einen Konsolenagenten zu erstellen

Durch das Hinzufügen neuer AWS-Anmeldeinformationen zur Konsole erhalten Sie die erforderlichen Berechtigungen zum Erstellen eines Konsolenagenten.

"Erfahren Sie, wie Sie der Konsole AWS-Anmeldeinformationen hinzufügen, um einen Konsolenagenten zu erstellen"

AWS-Anmeldeinformationen für FSx for ONTAP hinzufügen

Fügen Sie der Konsole AWS-Anmeldeinformationen hinzu, um die erforderlichen Berechtigungen zum Erstellen und Verwalten eines FSx for ONTAP Systems bereitzustellen.

"Erfahren Sie, wie Sie AWS-Anmeldeinformationen zur Konsole für Amazon FSx for ONTAP hinzufügen"

Anmeldeinformationen und Marktplatzabonnements

Die Anmeldeinformationen, die Sie einem Konsolenagenten hinzufügen, müssen mit einem AWS Marketplace-Abonnement verknüpft sein, damit Sie Cloud Volumes ONTAP zu einem Stundensatz (PAYGO) und andere NetApp -Datendienste oder über einen Jahresvertrag bezahlen können. "Erfahren Sie, wie Sie ein AWS-Abonnement zuordnen" .

Beachten Sie Folgendes zu AWS-Anmeldeinformationen und Marktplatz-Abonnements:

- Sie können nur ein AWS Marketplace-Abonnement mit einem Satz AWS-Anmeldeinformationen verknüpfen
- Sie können ein bestehendes Marktplatz-Abonnement durch ein neues Abonnement ersetzen

FAQ

Die folgenden Fragen beziehen sich auf Anmeldeinformationen und Abonnements.

Wie kann ich meine AWS-Anmeldeinformationen sicher rotieren?

Wie in den obigen Abschnitten beschrieben, können Sie mit der Konsole AWS-Anmeldeinformationen auf verschiedene Weise bereitstellen: über eine IAM-Rolle, die mit der Agenteninstanz der Konsole verknüpft ist, durch die Übernahme einer IAM-Rolle in einem vertrauenswürdigen Konto oder durch die Bereitstellung von AWS-Zugriffsschlüsseln.

Bei den ersten beiden Optionen verwendet die Konsole den AWS Security Token Service, um temporäre Anmeldeinformationen zu erhalten, die ständig rotieren. Dieser Prozess ist die beste Vorgehensweise – er ist automatisch und sicher.

Wenn Sie der Konsole AWS-Zugriffsschlüssel bereitstellen, sollten Sie die Schlüssel rotieren, indem Sie sie in regelmäßigen Abständen in der Konsole aktualisieren. Dies ist ein vollständig manueller Prozess.

Kann ich das AWS Marketplace-Abonnement für Cloud Volumes ONTAP Systeme ändern?

Ja, das können Sie. Wenn Sie das AWS Marketplace-Abonnement ändern, das mit einem Satz Anmeldeinformationen verknüpft ist, werden alle vorhandenen und neuen Cloud Volumes ONTAP Systeme über das neue Abonnement abgerechnet.

"Erfahren Sie, wie Sie ein AWS-Abonnement zuordnen" .

Kann ich mehrere AWS-Anmeldeinformationen mit jeweils unterschiedlichen Marktplatz-Abonnements hinzufügen?

Alle AWS-Anmeldeinformationen, die zum selben AWS-Konto gehören, werden mit demselben AWS Marketplace-Abonnement verknüpft.

Wenn Sie über mehrere AWS-Anmeldeinformationen verfügen, die zu verschiedenen AWS-Konten gehören, können diese Anmeldeinformationen mit demselben AWS Marketplace-Abonnement oder mit verschiedenen Abonnements verknüpft sein.

Kann ich vorhandene Cloud Volumes ONTAP Systeme auf ein anderes AWS-Konto verschieben?

Nein, es ist nicht möglich, die mit Ihrem Cloud Volumes ONTAP -System verknüpften AWS-Ressourcen auf ein anderes AWS-Konto zu verschieben.

Wie funktionieren Anmeldeinformationen für Marktplatzbereitstellungen und lokale Bereitstellungen?

In den obigen Abschnitten wird die empfohlene Bereitstellungsmethode für den Konsolenagenten beschrieben, die von der Konsole aus erfolgt. Sie können auch einen Agenten in AWS vom AWS Marketplace aus bereitstellen und die Konsolen-Agent-Software manuell auf Ihrem eigenen Linux-Host installieren.

Wenn Sie den Marketplace verwenden, werden die Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die IAM-Rolle manuell erstellen und einrichten und dann Berechtigungen für alle zusätzlichen Konten erteilen.

Bei lokalen Bereitstellungen können Sie keine IAM-Rolle für die Konsole einrichten, aber Sie können Berechtigungen mithilfe von AWS-Zugriffsschlüsseln erteilen.

Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

- Standardmodus
  - "Einrichten von Berechtigungen für eine AWS Marketplace-Bereitstellung"
  - "Einrichten von Berechtigungen für lokale Bereitstellungen"
- Eingeschränkter Modus
  - "Berechtigungen für den eingeschränkten Modus einrichten"

Verwalten Sie AWS-Anmeldeinformationen und Marktplatz-Abonnements für die NetApp Console

Fügen Sie AWS-Anmeldeinformationen hinzu und verwalten Sie diese, damit Sie Cloud-Ressourcen in Ihren AWS-Konten über die NetApp Console bereitstellen und verwalten können. Wenn Sie mehrere AWS Marketplace-Abonnements verwalten, können Sie jedem Abonnement auf der Seite „Anmeldeinformationen“ unterschiedliche AWS-Anmeldeinformationen zuweisen.

Überblick

Sie können AWS-Anmeldeinformationen zu einem vorhandenen Konsolenagenten oder direkt zur Konsole hinzufügen:

- Fügen Sie einem vorhandenen Agenten zusätzliche AWS-Anmeldeinformationen hinzu

  Fügen Sie einem Konsolenagenten AWS-Anmeldeinformationen hinzu, um Cloud-Ressourcen zu verwalten. Erfahren Sie, wie Sie einem Konsolenagenten AWS-Anmeldeinformationen hinzufügen .

- Fügen Sie der Konsole AWS-Anmeldeinformationen hinzu, um einen Konsolenagenten zu erstellen

  Durch das Hinzufügen neuer AWS-Anmeldeinformationen zur Konsole erhalten Sie die erforderlichen Berechtigungen zum Erstellen eines Konsolenagenten. Erfahren Sie, wie Sie AWS-Anmeldeinformationen zur NetApp Console hinzufügen .

- AWS-Anmeldeinformationen zur Konsole für FSx for ONTAP hinzufügen

  Fügen Sie der Konsole neue AWS-Anmeldeinformationen hinzu, um FSx für ONTAP zu erstellen und zu verwalten. "Erfahren Sie, wie Sie Berechtigungen für FSx für ONTAP einrichten"

So rotieren Sie Anmeldeinformationen

Mit der NetApp Console können Sie AWS-Anmeldeinformationen auf verschiedene Weise bereitstellen: über eine mit der Agenteninstanz verknüpfte IAM-Rolle, durch die Übernahme einer IAM-Rolle in einem vertrauenswürdigen Konto oder durch die Bereitstellung von AWS-Zugriffsschlüsseln. "Erfahren Sie mehr über AWS-Anmeldeinformationen und -Berechtigungen" .

Bei den ersten beiden Optionen verwendet die Konsole den AWS Security Token Service, um temporäre Anmeldeinformationen zu erhalten, die ständig rotieren. Dieser Vorgang ist die beste Vorgehensweise, da er automatisch und sicher ist.

Rotieren Sie AWS-Zugriffsschlüssel manuell, indem Sie sie in der Konsole aktualisieren.

Hinzufügen zusätzlicher Anmeldeinformationen zu einem Konsolenagenten

Fügen Sie einem Konsolenagenten zusätzliche AWS-Anmeldeinformationen hinzu, damit er über die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen in Ihrer öffentlichen Cloud-

Umgebung verfügt. Sie können entweder die ARN einer IAM-Rolle in einem anderen Konto angeben oder AWS-Zugriffsschlüssel bereitstellen.

Wenn Sie gerade erst mit der Konsole beginnen,"Erfahren Sie, wie die NetApp Console AWS-Anmeldeinformationen und -Berechtigungen verwendet" .

Berechtigungen erteilen

Erteilen Sie Berechtigungen, bevor Sie einem Konsolenagenten AWS-Anmeldeinformationen hinzufügen. Die Berechtigungen ermöglichen einem Konsolenagenten, Ressourcen und Prozesse innerhalb dieses AWS-Kontos zu verwalten. Sie können die Berechtigungen mit der ARN einer Rolle in einem vertrauenswürdigen Konto oder mit AWS-Schlüsseln bereitstellen.

> Wenn Sie einen Konsolenagenten über die Konsole bereitgestellt haben, wurden automatisch AWS-Anmeldeinformationen für das Konto hinzugefügt, in dem Sie einen Konsolenagenten bereitgestellt haben. Dadurch wird sichergestellt, dass die erforderlichen Berechtigungen zum Verwalten von Ressourcen vorhanden sind. "Erfahren Sie mehr über AWS-Anmeldeinformationen und -Berechtigungen" .

Auswahl

- indem Sie eine IAM-Rolle in einem anderen Konto übernehmen
- Erteilen Sie Berechtigungen durch die Bereitstellung von AWS-Schlüsseln

Erteilen Sie Berechtigungen, indem Sie eine IAM-Rolle in einem anderen Konto übernehmen

Sie können mithilfe von IAM-Rollen eine Vertrauensbeziehung zwischen dem AWS-Quellkonto, in dem Sie eine Konsolen-Agent-Instanz bereitgestellt haben, und anderen AWS-Konten einrichten. Anschließend stellen Sie der Konsole die ARN der IAM-Rollen der vertrauenswürdigen Konten zur Verfügung.

Wenn ein Konsolenagent vor Ort installiert ist, können Sie diese Authentifizierungsmethode nicht verwenden. Sie müssen AWS-Schlüssel verwenden.

Schritte

1. Gehen Sie zur IAM-Konsole im Zielkonto, in dem Sie einem Konsolenagenten Berechtigungen erteilen möchten.
2. Wählen Sie unter „Zugriffsverwaltung“ **Rollen > Rolle erstellen** und befolgen Sie die Schritte zum Erstellen der Rolle.

   Stellen Sie sicher, dass Sie Folgendes tun:

   - Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
   - Wählen Sie **Ein anderes AWS-Konto** und geben Sie die ID des Kontos ein, in dem sich eine Konsolen-Agent-Instanz befindet.
   - Erstellen Sie die erforderlichen Richtlinien, indem Sie den Inhalt von kopieren und einfügen"die IAM-Richtlinien für einen Konsolenagenten" .
3. Kopieren Sie die Rollen-ARN der IAM-Rolle, damit Sie sie später in die Konsole einfügen können.

Ergebnis

Das Konto verfügt über die erforderlichen Berechtigungen. Sie können jetzt die Anmeldeinformationen zu einem Konsolenagenten hinzufügen .

Erteilen Sie Berechtigungen durch die Bereitstellung von AWS-Schlüsseln

Wenn Sie der Konsole AWS-Schlüssel für einen IAM-Benutzer bereitstellen möchten, müssen Sie diesem Benutzer die erforderlichen Berechtigungen erteilen. Die IAM-Richtlinie der Konsole definiert die AWS-Aktionen und -Ressourcen, die die Konsole verwenden darf.

Sie müssen diese Authentifizierungsmethode verwenden, wenn ein Konsolenagent vor Ort installiert ist. Sie können keine IAM-Rolle verwenden.

Schritte

1. Erstellen Sie in der IAM-Konsole Richtlinien, indem Sie den Inhalt von"die IAM-Richtlinien für einen Konsolenagenten" .

   "AWS-Dokumentation: Erstellen von IAM-Richtlinien"

2. Ordnen Sie die Richtlinien einer IAM-Rolle oder einem IAM-Benutzer zu.
   - "AWS-Dokumentation: Erstellen von IAM-Rollen"
   - "AWS-Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"

Ergebnis

Das Konto verfügt über die erforderlichen Berechtigungen. Sie können jetzt die Anmeldeinformationen zu einem Konsolenagenten hinzufügen .

Fügen Sie die Anmeldeinformationen hinzu

Nachdem Sie ein AWS-Konto mit den erforderlichen Berechtigungen versehen haben, können Sie die Anmeldeinformationen für dieses Konto einem vorhandenen Agenten hinzufügen. Dadurch können Sie Cloud Volumes ONTAP -Systeme in diesem Konto mit demselben Agenten starten.

```
 New credentials in your cloud provider may take a few minutes to become
available. Then, add the credentials.
.Schritte
. Wählen Sie über die obere Navigationsleiste einen Konsolenagenten aus,
dem Sie Anmeldeinformationen hinzufügen möchten.
. Wählen Sie in der linken Navigationsleiste *Administration >
Anmeldeinformationen* aus.
. Wählen Sie auf der Seite *Anmeldeinformationen der Organisation* die
Option *Anmeldeinformationen hinzufügen* aus und folgen Sie den Schritten
des Assistenten.
```

+
.. **Speicherort der Anmeldeinformationen**: Wählen Sie **Amazon Web Services > Agent**.
.. **Anmeldeinformationen definieren**: Geben Sie den ARN (Amazon Resource Name) einer vertrauenswürdigen IAM-Rolle an oder geben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel ein.
.. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.

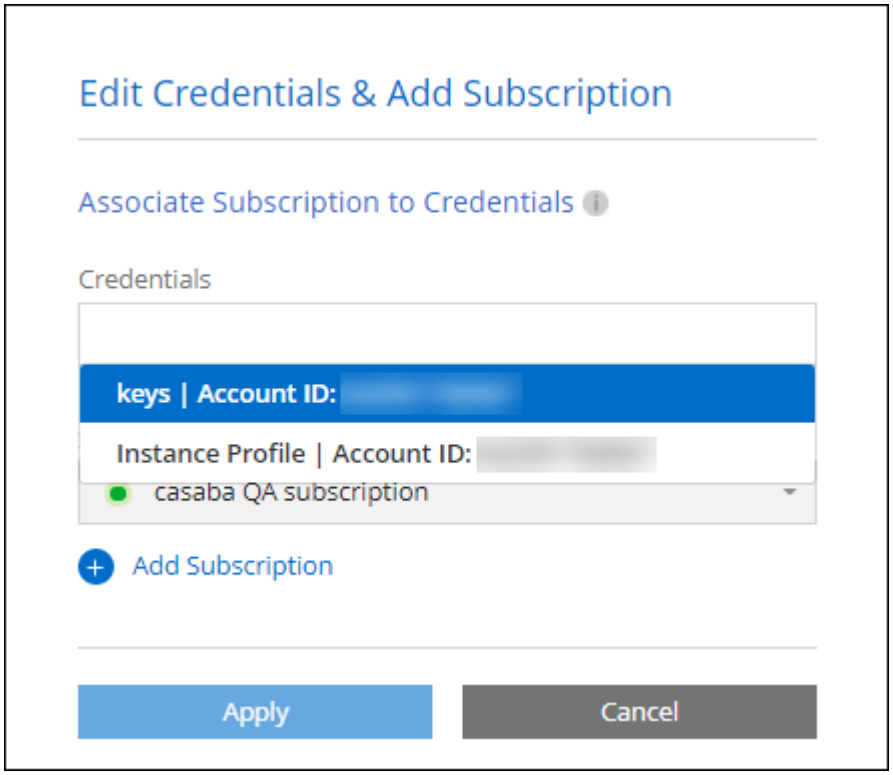
+
Um Dienste mit einem Stundensatz (PAYGO) oder mit einem Jahresvertrag zu bezahlen, müssen Sie AWS-

Anmeldeinformationen mit Ihrem AWS Marketplace-Abonnement verknüpfen.

a. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Ergebnis

Sie können jetzt auf der Seite „Details und Anmeldeinformationen“ zu einem anderen Satz von Anmeldeinformationen wechseln, wenn Sie der Konsole ein System hinzufügen.



Fügen Sie der Konsole Anmeldeinformationen zum Erstellen eines Konsolenagenten hinzu

Fügen Sie AWS-Anmeldeinformationen hinzu, indem Sie die ARN einer IAM-Rolle angeben, die die zum Erstellen eines Konsolenagenten erforderlichen Berechtigungen erteilt. Sie können diese Anmeldeinformationen beim Erstellen eines neuen Agenten auswählen.

Einrichten der IAM-Rolle

Richten Sie eine IAM-Rolle ein, die es der NetApp Console -Software als Serviceebene (SaaS) ermöglicht, die Rolle zu übernehmen.

Schritte

1. Gehen Sie zur IAM-Konsole im Zielkonto.
2. Wählen Sie unter „Zugriffsverwaltung“ **Rollen > Rolle erstellen** und befolgen Sie die Schritte zum Erstellen der Rolle.

   Stellen Sie sicher, dass Sie Folgendes tun:

   - Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
   - Wählen Sie **Ein anderes AWS-Konto** und geben Sie die ID der NetApp Console SaaS ein: 952013314444

- Bearbeiten Sie speziell für Amazon FSx for NetApp ONTAP die Richtlinie **Vertrauensbeziehungen**, um "AWS": "arn:aws:iam::952013314444:root" einzuschließen.

  Die Richtlinie sollte beispielsweise folgendermaßen aussehen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+
Siehe "AWS Identity and Access Management (IAM)-Dokumentation" für weitere Informationen zum kontoübergreifenden Ressourcenzugriff in IAM.

- Erstellen Sie eine Richtlinie, die die zum Erstellen eines Konsolenagenten erforderlichen Berechtigungen enthält.
  - "Anzeigen der für FSx for ONTAP erforderlichen Berechtigungen"
  - "Anzeigen der Agent-Bereitstellungsrichtlinie"

3. Kopieren Sie die Rollen-ARN der IAM-Rolle, damit Sie sie im nächsten Schritt in die Konsole einfügen können.

Ergebnis

Die IAM-Rolle verfügt jetzt über die erforderlichen Berechtigungen. Sie können es jetzt zur Konsole hinzufügen .

Fügen Sie die Anmeldeinformationen hinzu

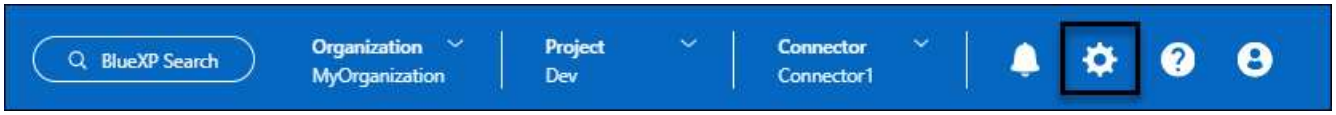
Nachdem Sie die IAM-Rolle mit den erforderlichen Berechtigungen ausgestattet haben, fügen Sie die Rollen-ARN zur Konsole hinzu.

Bevor Sie beginnen

Wenn Sie die IAM-Rolle gerade erst erstellt haben, kann es einige Minuten dauern, bis sie zur Verwendung verfügbar ist. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zur Konsole hinzufügen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.



2. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** oder **Anmeldeinformationen des Kontos** die Option **Anmeldeinformationen hinzufügen** aus und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Amazon Web Services > NetApp Console**.
   b. **Anmeldeinformationen definieren**: Geben Sie den ARN (Amazon Resource Name) der IAM-Rolle an.
   c. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Anmeldeinformationen zur Konsole für Amazon FSx for ONTAP hinzufügen

Einzelheiten finden Sie im "die Konsolendokumentation für Amazon FSx for ONTAP"

Konfigurieren eines AWS-Abonnements

Nachdem Sie Ihre AWS-Anmeldeinformationen hinzugefügt haben, können Sie mit diesen Anmeldeinformationen ein AWS Marketplace-Abonnement konfigurieren. Mit dem Abonnement können Sie Cloud Volumes ONTAP auf Stundenbasis (PAYGO) oder über einen Jahresvertrag bezahlen und weitere Datendienste nutzen.

Es gibt zwei Szenarien, in denen Sie ein AWS Marketplace-Abonnement konfigurieren können, nachdem Sie die Anmeldeinformationen bereits hinzugefügt haben:

- Sie haben beim ersten Hinzufügen der Anmeldeinformationen kein Abonnement konfiguriert.
- Sie möchten das AWS Marketplace-Abonnement ändern, das für die AWS-Anmeldeinformationen konfiguriert ist.

  Durch das Ersetzen des aktuellen Marktplatzabonnements durch ein neues Abonnement wird das Marktplatzabonnement für alle vorhandenen Cloud Volumes ONTAP Systeme und alle neuen Systeme geändert.

Bevor Sie beginnen

Sie müssen einen Konsolenagenten erstellen, bevor Sie ein Abonnement konfigurieren können. "Erfahren Sie, wie Sie einen Konsolenagenten erstellen" .

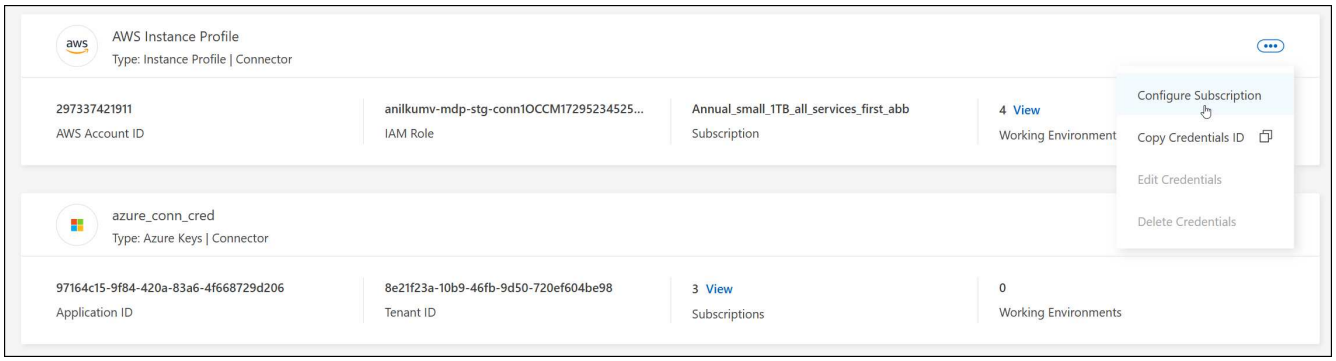
Das folgende Video zeigt die Schritte zum Abonnieren von NetApp Intelligent Services vom AWS Marketplace:

Abonnieren Sie NetApp Intelligent Services vom AWS Marketplace

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen aus, die einem Konsolenagenten zugeordnet sind, und wählen Sie dann **Abonnement konfigurieren**.

   Sie müssen Anmeldeinformationen auswählen, die einem Konsolenagenten zugeordnet sind. Sie können ein Marktplatzabonnement nicht mit Anmeldeinformationen verknüpfen, die mit der NetApp Console verknüpft sind.



4. Um die Anmeldeinformationen mit einem vorhandenen Abonnement zu verknüpfen, wählen Sie das Abonnement aus der Dropdown-Liste aus und wählen Sie **Konfigurieren**.
5. Um die Anmeldeinformationen einem neuen Abonnement zuzuordnen, wählen Sie **Abonnement hinzufügen > Fortfahren** und folgen Sie den Schritten im AWS Marketplace:

   a. Wählen Sie **Kaufoptionen anzeigen**.

   b. Wählen Sie **Abonnieren**.

   c. Wählen Sie **Konto einrichten**.

      Sie werden zur NetApp Console weitergeleitet.

   d. Auf der Seite **Abonnementzuweisung**:

      - Wählen Sie die Konsolenorganisationen oder -konten aus, mit denen Sie dieses Abonnement verknüpfen möchten.
      - Wählen Sie im Feld **Vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

        Die Konsole ersetzt das vorhandene Abonnement für alle Anmeldeinformationen in der Organisation oder im Konto durch dieses neue Abonnement. Wenn ein Satz von Anmeldeinformationen nie mit einem Abonnement verknüpft war, wird dieses neue Abonnement nicht mit diesen Anmeldeinformationen verknüpft.

   Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.

   ◦ Wählen Sie **Speichern**.

Verknüpfen Sie ein vorhandenes Abonnement mit Ihrer Organisation oder Ihrem Konto

Wenn Sie sich beim AWS Marketplace anmelden, besteht der letzte Schritt im Prozess darin, das Abonnement Ihrer Organisation zuzuordnen. Wenn Sie diesen Schritt nicht abgeschlossen haben, können Sie das Abonnement nicht mit Ihrer Organisation oder Ihrem Konto verwenden.

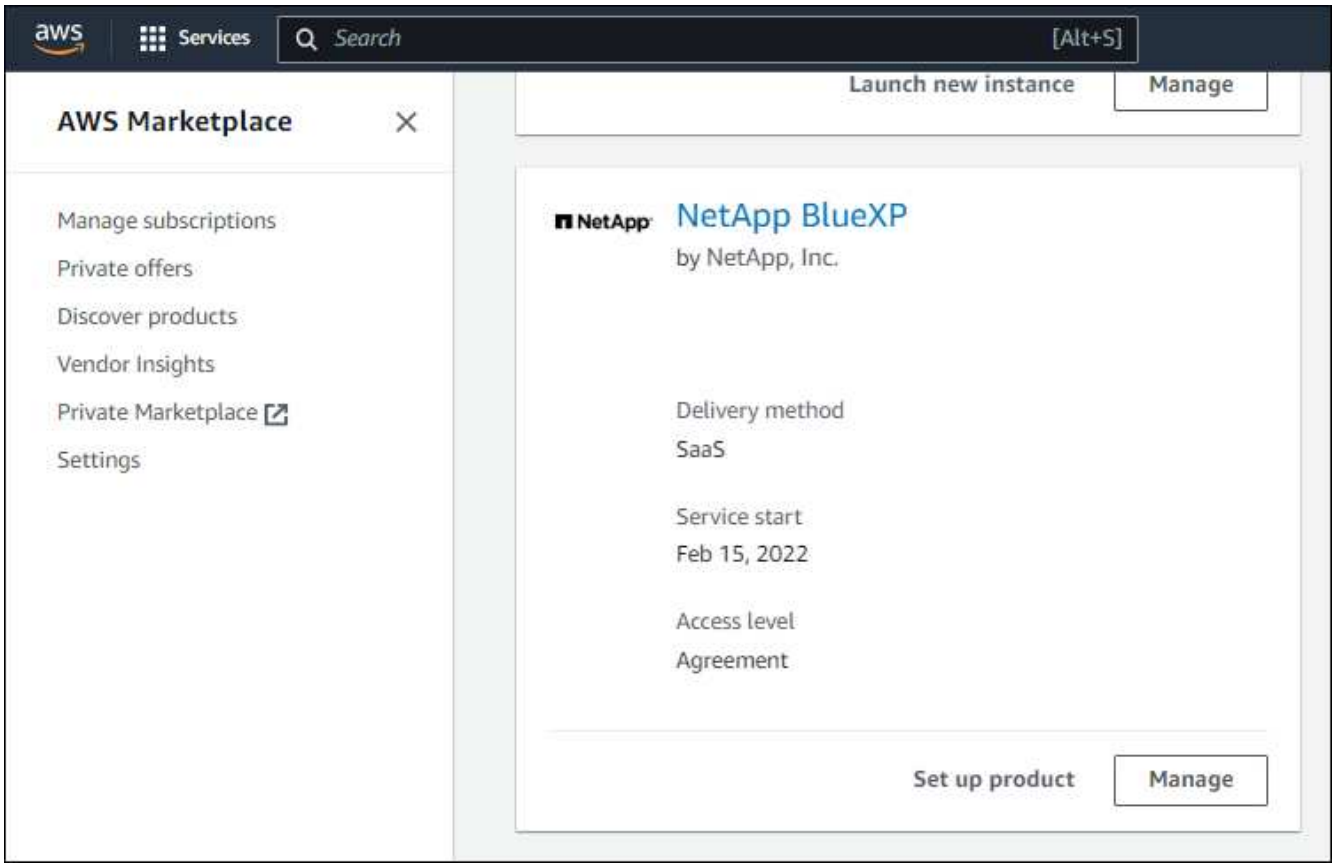
- "Erfahren Sie mehr über die Bereitstellungsmodi der Konsole"
- "Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der Konsole"

Führen Sie die folgenden Schritte aus, wenn Sie NetApp Intelligent Data Services vom AWS Marketplace abonniert haben, aber den Schritt zum Verknüpfen des Abonnements mit Ihrem Konto verpasst haben.

Schritte

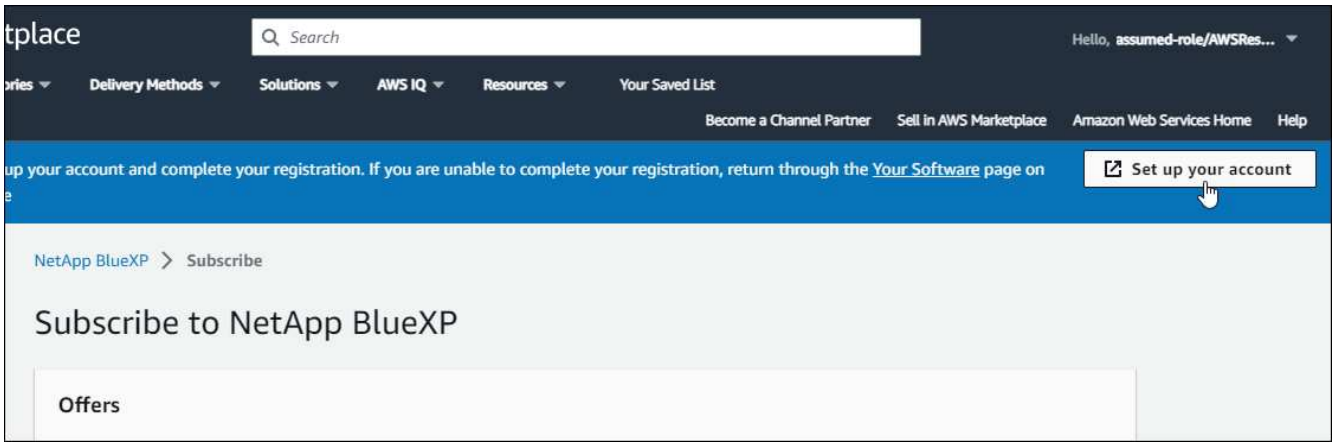
1. Bestätigen Sie, dass Sie Ihr Abonnement nicht mit Ihrer Konsolenorganisation oder Ihrem Konsolenkonto verknüpft haben.
   a. Wählen Sie im Navigationsmenü **Verwaltung > Licenses and subscriptions**.
   b. Wählen Sie **Abonnements** aus.
   c. Stellen Sie sicher, dass Ihr Abonnement nicht angezeigt wird.

      Sie sehen nur die Abonnements, die mit der Organisation oder dem Konto verknüpft sind, das Sie gerade anzeigen. Wenn Ihr Abonnement nicht angezeigt wird, fahren Sie mit den folgenden Schritten fort.
2. Melden Sie sich bei der AWS-Konsole an und navigieren Sie zu **AWS Marketplace-Abonnements**.
3. Suchen Sie das Abonnement.



4. Wählen Sie **Produkt einrichten**.

   Die Abonnementangebotsseite sollte in einem neuen Browser-Tab oder -Fenster geladen werden.
5. Wählen Sie **Konto einrichten**.



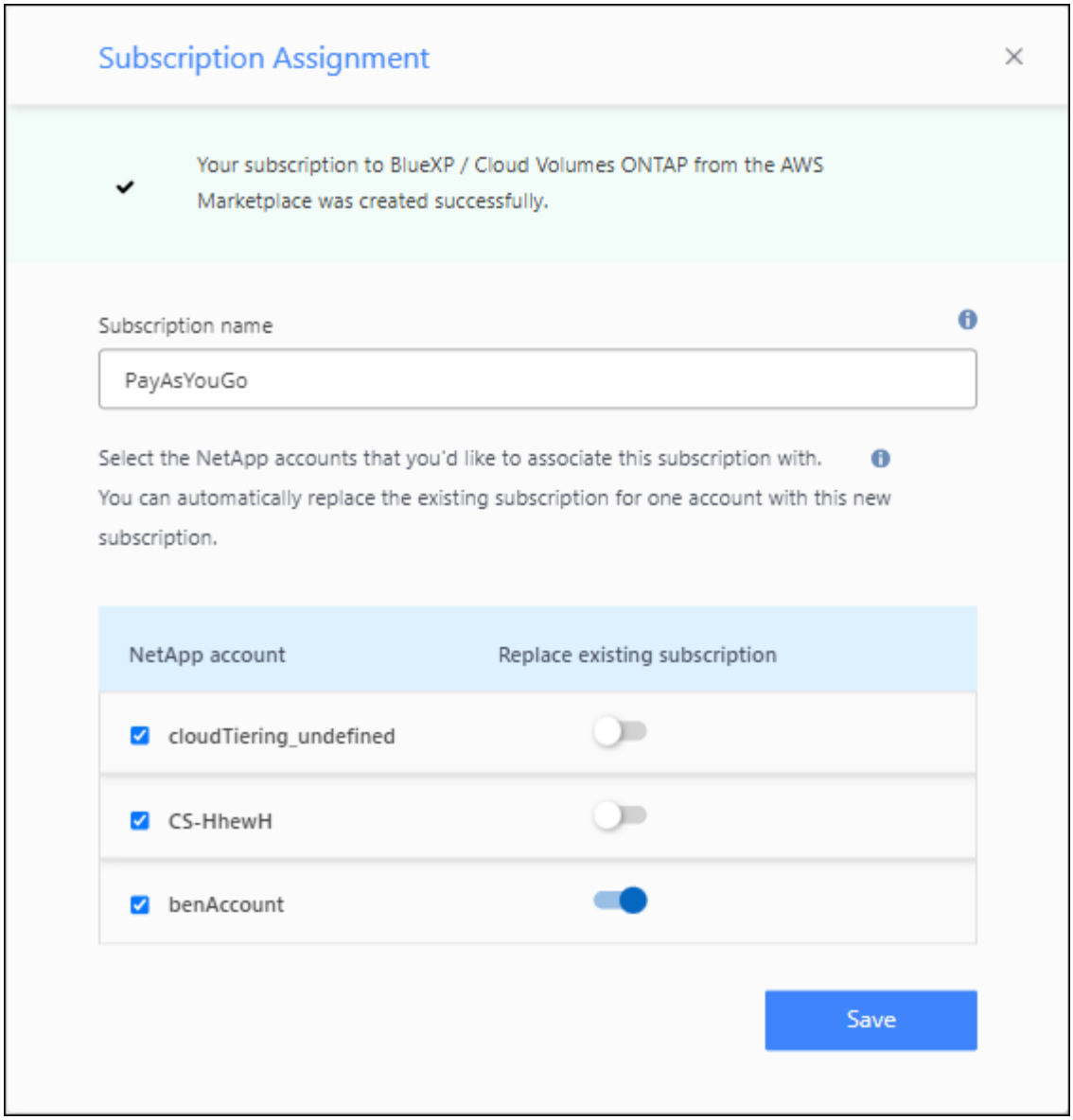
Die Seite **Abonnementzuweisung** auf netapp.com sollte in einem neuen Browser-Tab oder -Fenster geladen werden.

Beachten Sie, dass Sie möglicherweise zuerst aufgefordert werden, sich bei der Konsole anzumelden.

6. Auf der Seite **Abonnementzuweisung**:
   - Wählen Sie die Konsolenorganisationen oder -konten aus, mit denen Sie dieses Abonnement verknüpfen möchten.
   - Wählen Sie im Feld **Vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

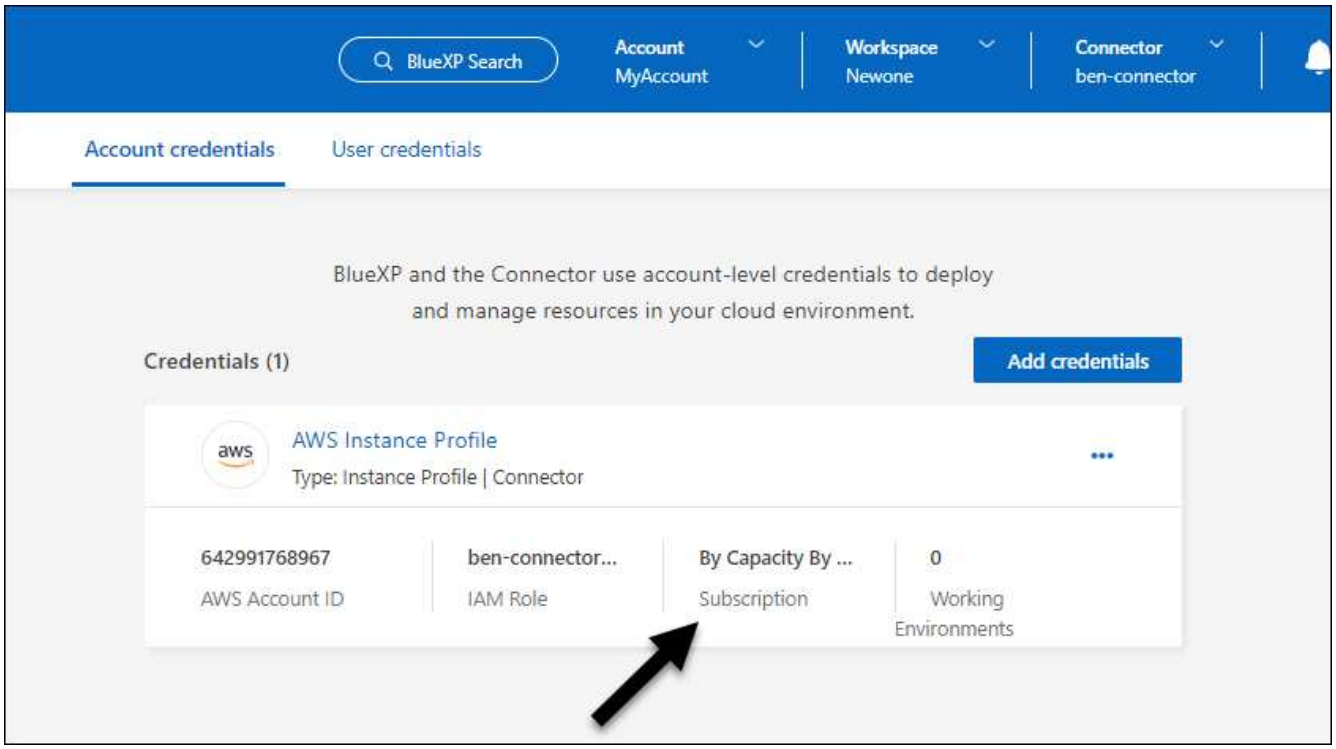
     Die Konsole ersetzt das vorhandene Abonnement für alle Anmeldeinformationen in der Organisation oder im Konto durch dieses neue Abonnement. Wenn ein Satz von Anmeldeinformationen nie mit einem Abonnement verknüpft war, wird dieses neue Abonnement nicht mit diesen Anmeldeinformationen verknüpft.

     Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.



7. Bestätigen Sie, dass das Abonnement mit Ihrer Organisation oder Ihrem Konto verknüpft ist.
   a. Wählen Sie im Navigationsmenü **Administration > Lizenzen und Abonnements**.
   b. Wählen Sie **Abonnements** aus.
   c. Überprüfen Sie, ob Ihr Abonnement angezeigt wird.
8. Bestätigen Sie, dass das Abonnement mit Ihren AWS-Anmeldeinformationen verknüpft ist.
   a. Wählen Sie oben rechts in der Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.
   b. Überprüfen Sie auf der Seite **Anmeldeinformationen der Organisation**, ob das Abonnement mit Ihren AWS-Anmeldeinformationen verknüpft ist.

      Hier ist ein Beispiel.



Anmeldeinformationen bearbeiten

Bearbeiten Sie Ihre AWS-Anmeldeinformationen, indem Sie den Kontotyp ändern (AWS-Schlüssel oder Rolle übernehmen), den Namen bearbeiten oder die Anmeldeinformationen selbst aktualisieren (die Schlüssel oder die Rollen-ARN).

Sie können die Anmeldeinformationen für ein Instanzprofil, das mit einer Konsolen-Agent-Instanz oder einer Amazon FSx for ONTAP -Instanz verknüpft ist, nicht bearbeiten. Sie können die Anmeldeinformationen nur für eine FSx for ONTAP Instanz umbenennen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** oder **Anmeldeinformationen des Kontos** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Anmeldeinformationen bearbeiten**.
3. Nehmen Sie die erforderlichen Änderungen vor und wählen Sie dann **Übernehmen**.

Anmeldeinformationen löschen

Wenn Sie einen Satz Anmeldeinformationen nicht mehr benötigen, können Sie ihn löschen. Sie können nur Anmeldeinformationen löschen, die keinem System zugeordnet sind.

Sie können die Anmeldeinformationen für ein Instanzprofil, das einer Konsolenagenteninstanz zugeordnet ist, nicht löschen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** oder **Anmeldeinformationen des Kontos** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann

Anmeldeinformationen löschen.

3. Wählen Sie zur Bestätigung **Löschen**.

Azurblau

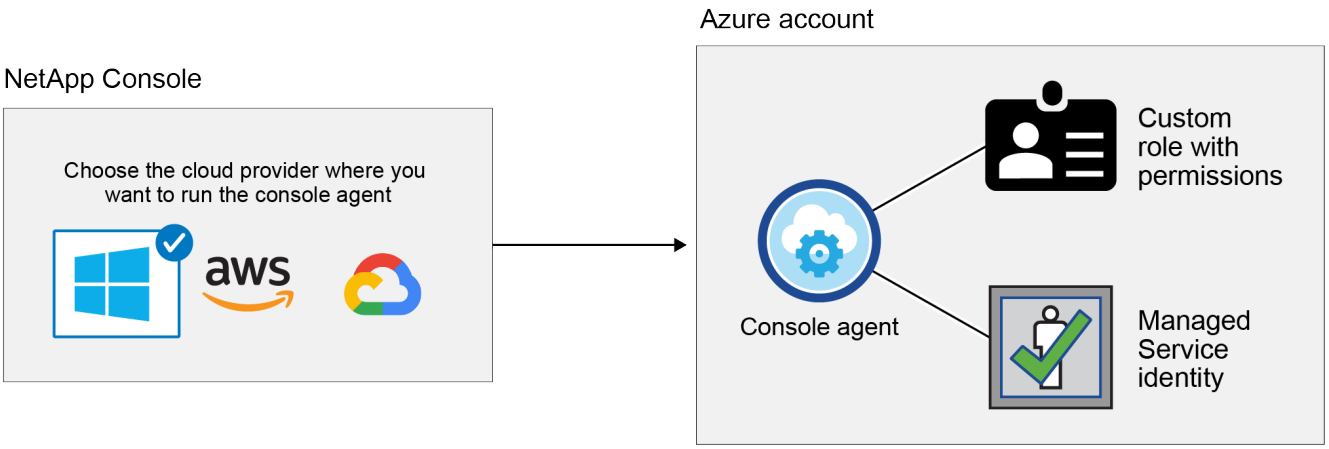
Erfahren Sie mehr über Azure-Anmeldeinformationen und Berechtigungen in der NetApp Console

Erfahren Sie, wie die NetApp Console Azure-Anmeldeinformationen verwendet, um Aktionen in Ihrem Namen auszuführen, und wie diese Anmeldeinformationen mit Marktplatzabonnements verknüpft werden. Das Verständnis dieser Details kann hilfreich sein, wenn Sie die Anmeldeinformationen für ein oder mehrere Azure-Abonnements verwalten. Sie möchten beispielsweise wissen, wann Sie der Konsole zusätzliche Azure-Anmeldeinformationen hinzufügen müssen.

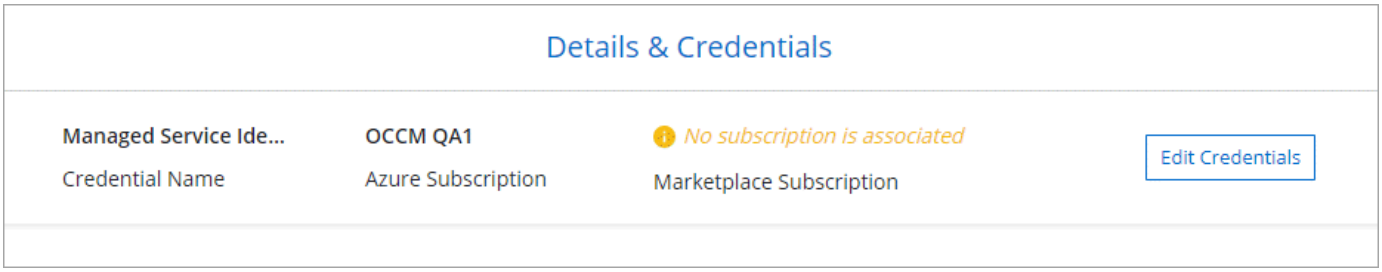
Anfängliche Azure-Anmeldeinformationen

Wenn Sie einen Konsolen-Agenten über die Konsole bereitstellen, müssen Sie ein Azure-Konto oder einen Dienstprinzipal verwenden, der über die Berechtigung zum Bereitstellen der virtuellen Maschine des Konsolen-Agenten verfügt. Die erforderlichen Berechtigungen sind in der"Agent-Bereitstellungsrichtlinie für Azure" .

Wenn die Konsole die virtuelle Maschine des Konsolen-Agenten in Azure bereitstellt, ermöglicht sie eine "systemseitig zugewiesene verwaltete Identität" auf der virtuellen Maschine, erstellt eine benutzerdefinierte Rolle und weist sie der virtuellen Maschine zu. Die Rolle stellt der Konsole die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen innerhalb dieses Azure-Abonnements zur Verfügung. "Überprüfen Sie, wie die Konsole die Berechtigungen verwendet" .



Wenn Sie ein neues System für Cloud Volumes ONTAP erstellen, wählt die Konsole standardmäßig diese Azure-Anmeldeinformationen aus:



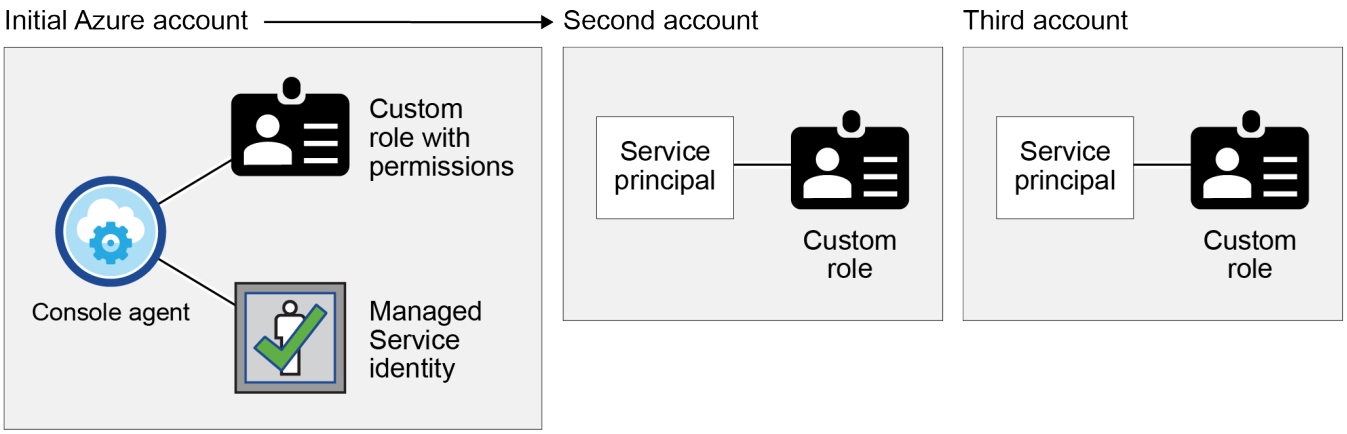
Sie können alle Ihre Cloud Volumes ONTAP -Systeme mit den anfänglichen Azure-Anmeldeinformationen bereitstellen oder zusätzliche Anmeldeinformationen hinzufügen.

Zusätzliche Azure-Abonnements für eine verwaltete Identität

Die der Konsolen-Agent-VM zugewiesene, systemseitig verwaltete Identität ist dem Abonnement zugeordnet, in dem Sie den Konsolen-Agent gestartet haben. Wenn Sie ein anderes Azure-Abonnement auswählen möchten, müssen Sie"Verknüpfen Sie die verwaltete Identität mit diesen Abonnements" .

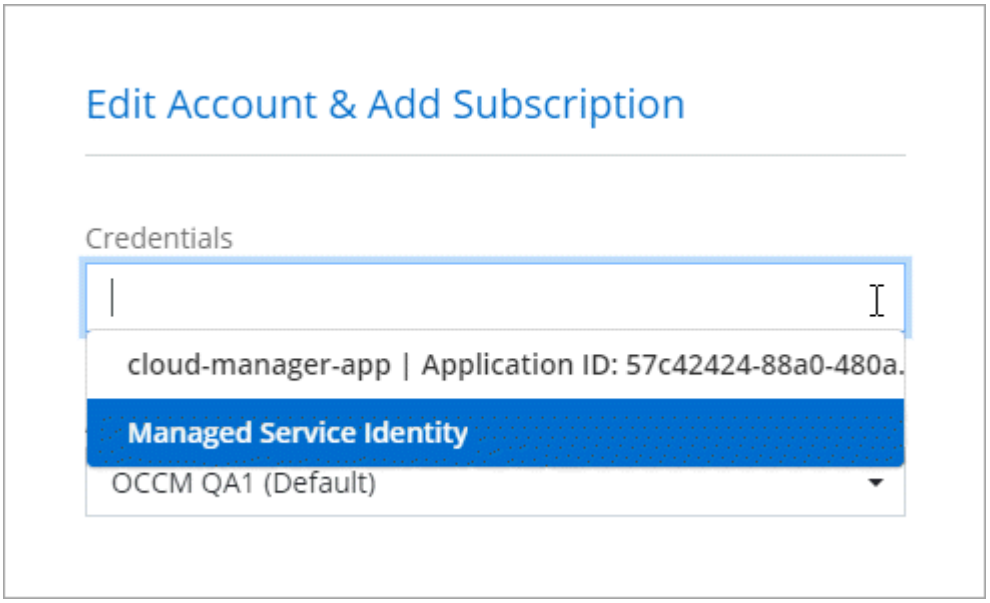
Zusätzliche Azure-Anmeldeinformationen

Wenn Sie andere Azure-Anmeldeinformationen mit der Konsole verwenden möchten, müssen Sie die erforderlichen Berechtigungen erteilen, indem Sie"Erstellen und Einrichten eines Dienstprinzipals in Microsoft Entra ID" für jedes Azure-Konto. Das folgende Bild zeigt zwei weitere Konten, die jeweils mit einem Dienstprinzipal und einer benutzerdefinierten Rolle eingerichtet sind, die Berechtigungen bereitstellt:



Sie würden dann"Fügen Sie die Kontoanmeldeinformationen zur Konsole hinzu" indem Sie Details zum AD-Dienstprinzipal angeben.

Sie können beispielsweise beim Erstellen eines neuen Cloud Volumes ONTAP Systems zwischen Anmeldeinformationen wechseln:



Anmeldeinformationen und Marktplatzabonnements

Die Anmeldeinformationen, die Sie einem Konsolenagenten hinzufügen, müssen mit einem Azure Marketplace-Abonnement verknüpft sein, damit Sie für Cloud Volumes ONTAP einen Stundensatz (PAYGO), NetApp -Datendienste oder einen Jahresvertrag bezahlen können.

"Erfahren Sie, wie Sie ein Azure-Abonnement zuordnen" .

Beachten Sie Folgendes zu Azure-Anmeldeinformationen und Marketplace-Abonnements:

- Sie können einem Satz Azure-Anmeldeinformationen nur ein Azure Marketplace-Abonnement zuordnen.
- Sie können ein bestehendes Marktplatz-Abonnement durch ein neues Abonnement ersetzen

FAQ

Die folgende Frage bezieht sich auf Anmeldeinformationen und Abonnements.

Kann ich das Azure Marketplace-Abonnement für Cloud Volumes ONTAP Systeme ändern?

Ja, das können Sie. Wenn Sie das Azure Marketplace-Abonnement ändern, das mit einem Satz Azure-Anmeldeinformationen verknüpft ist, werden alle vorhandenen und neuen Cloud Volumes ONTAP Systeme über das neue Abonnement abgerechnet.

"Erfahren Sie, wie Sie ein Azure-Abonnement zuordnen" .

Kann ich mehrere Azure-Anmeldeinformationen mit jeweils unterschiedlichen Marktplatzabonnements hinzufügen?

Alle Azure-Anmeldeinformationen, die zum selben Azure-Abonnement gehören, werden mit demselben Azure Marketplace-Abonnement verknüpft.

Wenn Sie über mehrere Azure-Anmeldeinformationen verfügen, die zu verschiedenen Azure-Abonnements gehören, können diese Anmeldeinformationen demselben Azure Marketplace-Abonnement oder verschiedenen Marketplace-Abonnements zugeordnet werden.

Kann ich vorhandene Cloud Volumes ONTAP Systeme in ein anderes Azure-Abonnement verschieben?

Nein, es ist nicht möglich, die mit Ihrem Cloud Volumes ONTAP -System verknüpften Azure-Ressourcen in ein anderes Azure-Abonnement zu verschieben.

Wie funktionieren Anmeldeinformationen für Marktplatzbereitstellungen und lokale Bereitstellungen?

In den obigen Abschnitten wird die empfohlene Bereitstellungsmethode für den Konsolenagenten beschrieben, die von der Konsole aus erfolgt. Sie können auch einen Konsolen-Agenten in Azure vom Azure Marketplace bereitstellen und die Konsolen-Agenten-Software auf Ihrem eigenen Linux-Host installieren.

Wenn Sie den Marketplace verwenden, können Sie Berechtigungen erteilen, indem Sie der Konsolen-Agent-VM und einer systemseitig zugewiesenen verwalteten Identität eine benutzerdefinierte Rolle zuweisen, oder Sie können einen Microsoft Entra-Dienstprinzipal verwenden.

Bei lokalen Bereitstellungen können Sie keine verwaltete Identität für den Konsolen-Agent einrichten, Sie können jedoch mithilfe eines Dienstprinzipals Berechtigungen erteilen.

Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

- Standardmodus
  - "Einrichten von Berechtigungen für eine Azure Marketplace-Bereitstellung"
  - "Einrichten von Berechtigungen für lokale Bereitstellungen"
- Eingeschränkter Modus
  - "Berechtigungen für den eingeschränkten Modus einrichten"

Verwalten Sie Azure-Anmeldeinformationen und Marketplace-Abonnements für die NetApp Console

Fügen Sie Azure-Anmeldeinformationen hinzu und verwalten Sie diese, damit die NetApp Console über die erforderlichen Berechtigungen zum Bereitstellen und Verwalten von Cloud-Ressourcen in Ihren Azure-Abonnements verfügt. Wenn Sie mehrere Azure Marketplace-Abonnements verwalten, können Sie jedem Abonnement auf der Seite „Anmeldeinformationen“ unterschiedliche Azure-Anmeldeinformationen zuweisen.

Überblick

Es gibt zwei Möglichkeiten, zusätzliche Azure-Abonnements und Anmeldeinformationen in der Konsole hinzuzufügen.

1. Ordnen Sie der von Azure verwalteten Identität zusätzliche Azure-Abonnements zu.
2. Um Cloud Volumes ONTAP mit unterschiedlichen Azure-Anmeldeinformationen bereitzustellen, erteilen Sie Azure Berechtigungen mithilfe eines Dienstprinzipals und fügen Sie dessen Anmeldeinformationen der Konsole hinzu.

Zuordnen zusätzlicher Azure-Abonnements zu einer verwalteten Identität

Über die Konsole können Sie die Azure-Anmeldeinformationen und das Azure-Abonnement auswählen, in dem Sie Cloud Volumes ONTAP bereitstellen möchten. Sie können kein anderes Azure-Abonnement für das verwaltete Identitätsprofil auswählen, es sei denn, Sie verknüpfen das "Verwaltete Identität" mit diesen Abonnements.

Informationen zu diesem Vorgang

Eine verwaltete Identität ist"das anfängliche Azure-Konto" wenn Sie einen Konsolenagenten von der Konsole aus bereitstellen. Wenn Sie den Konsolenagenten bereitstellen, weist die Konsole der virtuellen Maschine des Konsolenagenten die Rolle des Konsolenoperators zu.

Schritte

1. Melden Sie sich beim Azure-Portal an.
2. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP bereitstellen möchten.
3. Wählen Sie **Zugriffskontrolle (IAM)**.
   a. Wählen Sie **Hinzufügen** > **Rollenzuweisung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
      - Wählen Sie die Rolle **Konsolenoperator** aus.

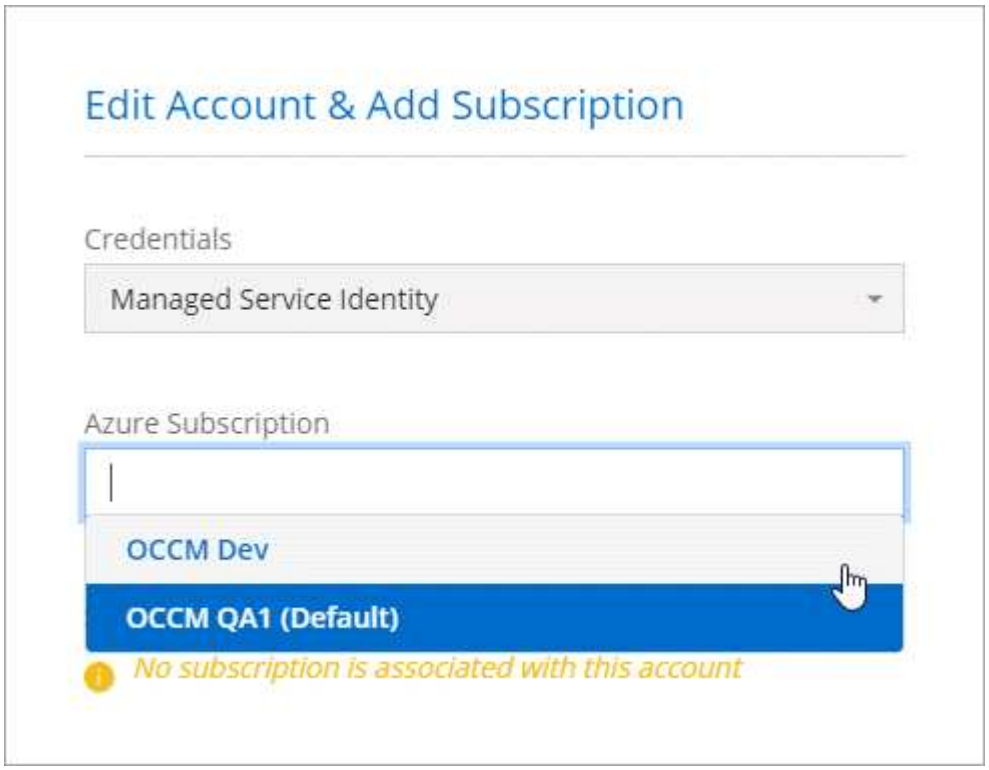
        „Konsolenoperator“ ist der Standardname, der in einer Konsolenagentrichtlinie angegeben wird. Wenn Sie einen anderen Namen für die Rolle gewählt haben, wählen Sie stattdessen diesen Namen aus.

- Weisen Sie einer **virtuellen Maschine** Zugriff zu.
- Wählen Sie das Abonnement aus, in dem eine virtuelle Maschine des Konsolen-Agenten erstellt wurde.
- Wählen Sie eine virtuelle Maschine des Konsolenagenten aus.
- Wählen Sie **Speichern**.

4. Wiederholen Sie diese Schritte für weitere Abonnements.

Ergebnis

Beim Erstellen eines neuen Systems können Sie jetzt aus mehreren Azure-Abonnements für das verwaltete Identitätsprofil auswählen.



Fügen Sie der NetApp Console zusätzliche Azure-Anmeldeinformationen hinzu

Wenn Sie einen Konsolenagenten über die Konsole bereitstellen, aktiviert die Konsole eine vom System zugewiesene verwaltete Identität auf der virtuellen Maschine, die über die erforderlichen Berechtigungen verfügt. Die Konsole wählt diese Azure-Anmeldeinformationen standardmäßig aus, wenn Sie ein neues System für Cloud Volumes ONTAP erstellen.

Wenn Sie eine Konsolenagentensoftware manuell auf einem vorhandenen System installiert haben, wird kein anfänglicher Satz Anmeldeinformationen hinzugefügt. "Erfahren Sie mehr über Azure-Anmeldeinformationen und -Berechtigungen" .

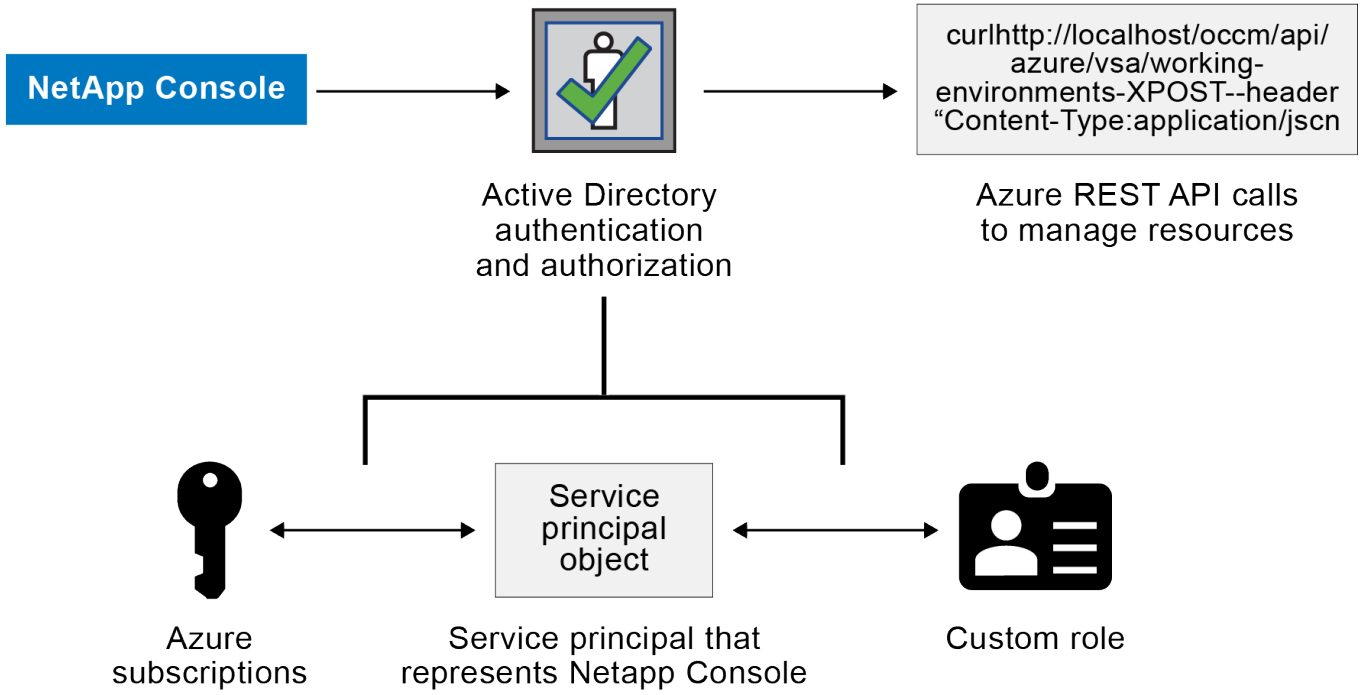
Wenn Sie Cloud Volumes ONTAP mit *verschiedenen* Azure-Anmeldeinformationen bereitstellen möchten, müssen Sie die erforderlichen Berechtigungen erteilen, indem Sie für jedes Azure-Konto einen Dienstprinzipal in der Microsoft Entra-ID erstellen und einrichten. Anschließend können Sie die neuen Anmeldeinformationen zur Konsole hinzufügen.

Gewähren von Azure-Berechtigungen mithilfe eines Dienstprinzipals

Die Konsole benötigt Berechtigungen, um Aktionen in Azure auszuführen. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie einen Dienstprinzipal in Microsoft Entra ID erstellen und einrichten und die Azure-Anmeldeinformationen abrufen, die die Konsole benötigt.

Informationen zu diesem Vorgang

Das folgende Bild zeigt, wie die Konsole Berechtigungen zum Ausführen von Vorgängen in Azure erhält. Ein Dienstprinzipalobjekt, das an ein oder mehrere Azure-Abonnements gebunden ist, stellt die Konsole in der Microsoft Entra ID dar und ist einer benutzerdefinierten Rolle zugewiesen, die die erforderlichen Berechtigungen gewährt.



Schritte

1. Erstellen einer Microsoft Entra-Anwendung .
2. Zuweisen der Anwendung zu einer Rolle .
3. Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu .
4. Abrufen der Anwendungs-ID und der Verzeichnis-ID .
5. Erstellen eines Client-Geheimnisses .

Erstellen einer Microsoft Entra-Anwendung

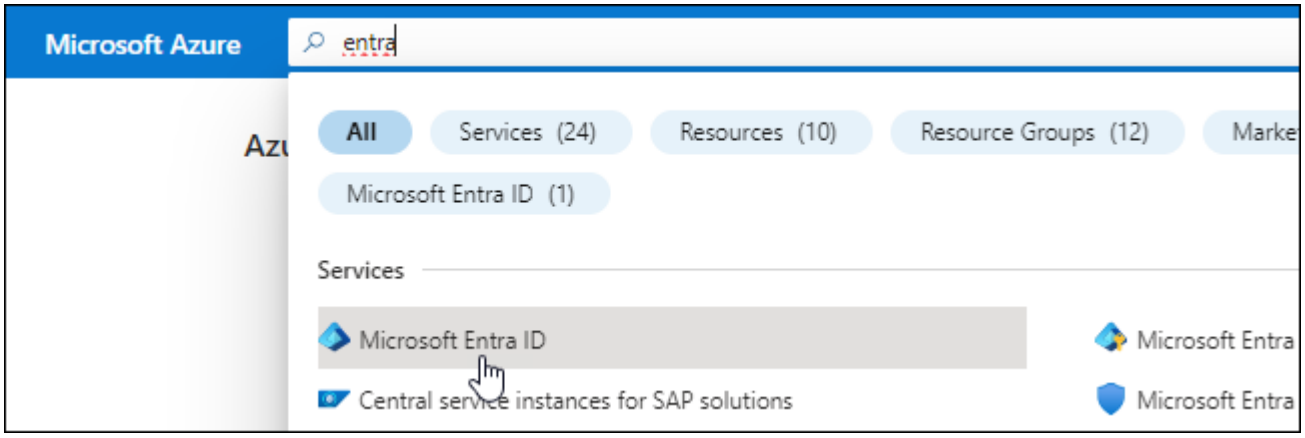
Erstellen Sie eine Microsoft Entra-Anwendung und einen Dienstprinzipal, den die Konsole für die rollenbasierte Zugriffskontrolle verwenden kann.

Schritte

1. Stellen Sie sicher, dass Sie in Azure über die Berechtigung verfügen, eine Active Directory-Anwendung zu erstellen und die Anwendung einer Rolle zuzuweisen.

   Weitere Einzelheiten finden Sie unter "Microsoft Azure-Dokumentation: Erforderliche Berechtigungen"

2. Öffnen Sie im Azure-Portal den Dienst **Microsoft Entra ID**.



3. Wählen Sie im Menü **App-Registrierungen** aus.
4. Wählen Sie **Neuregistrierung**.
5. Geben Sie Details zur Anwendung an:
   - **Name**: Geben Sie einen Namen für die Anwendung ein.
   - **Kontotyp**: Wählen Sie einen Kontotyp aus (alle funktionieren mit der NetApp Console).
   - **Umleitungs-URI**: Sie können dieses Feld leer lassen.
6. Wählen Sie **Registrieren**.

   Sie haben die AD-Anwendung und den Dienstprinzipal erstellt.

Zuweisen der Anwendung zu einer Rolle

Sie müssen den Dienstprinzipal an ein oder mehrere Azure-Abonnements binden und ihm die benutzerdefinierte Rolle „Konsolenoperator“ zuweisen, damit die Konsole über Berechtigungen in Azure verfügt.

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle:

   Beachten Sie, dass Sie eine benutzerdefinierte Azure-Rolle mithilfe des Azure-Portals, Azure PowerShell, Azure CLI oder REST-API erstellen können. Die folgenden Schritte zeigen, wie Sie die Rolle mithilfe der Azure CLI erstellen. Wenn Sie eine andere Methode bevorzugen, lesen Sie bitte "Azure-Dokumentation"

   a. Kopieren Sie den Inhalt der"benutzerdefinierte Rollenberechtigungen für den Konsolenagenten" und speichern Sie sie in einer JSON-Datei.

   b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

      Sie sollten die ID für jedes Azure-Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP -Systeme erstellen.

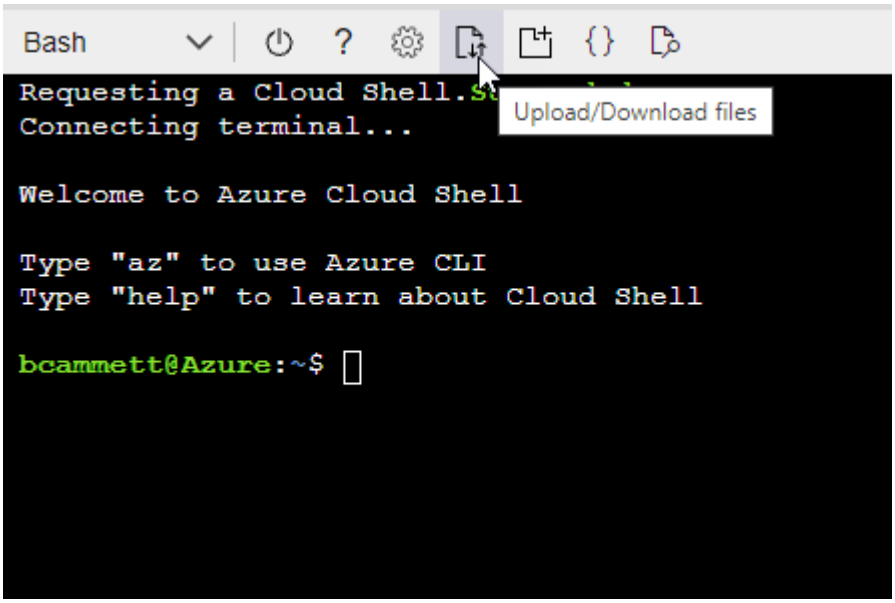
      Beispiel

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

Die folgenden Schritte beschreiben, wie Sie die Rolle mithilfe von Bash in Azure Cloud Shell erstellen.

- Start "Azure Cloud Shell" und wählen Sie die Bash-Umgebung.
- Laden Sie die JSON-Datei hoch.



- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
az role definition create --role-definition Connector_Policy.json
```

Sie sollten jetzt über eine benutzerdefinierte Rolle namens „Konsolenoperator“ verfügen, die Sie der virtuellen Maschine des Konsolenagenten zuweisen können.

2. Weisen Sie die Anwendung der Rolle zu:

a. Öffnen Sie im Azure-Portal den Dienst **Abonnements**.

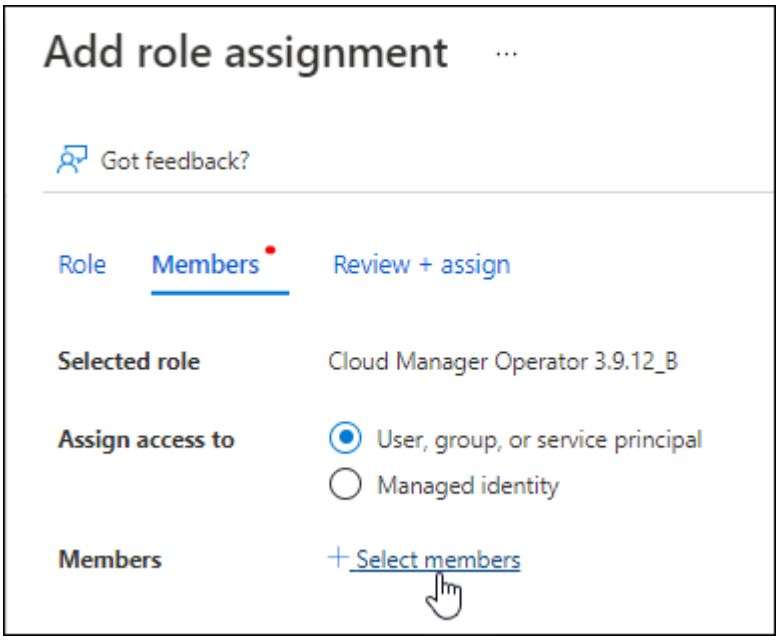
b. Wählen Sie das Abonnement aus.

c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

d. Wählen Sie auf der Registerkarte **Rolle** die Rolle **Konsolenbediener** aus und klicken Sie auf **Weiter**.

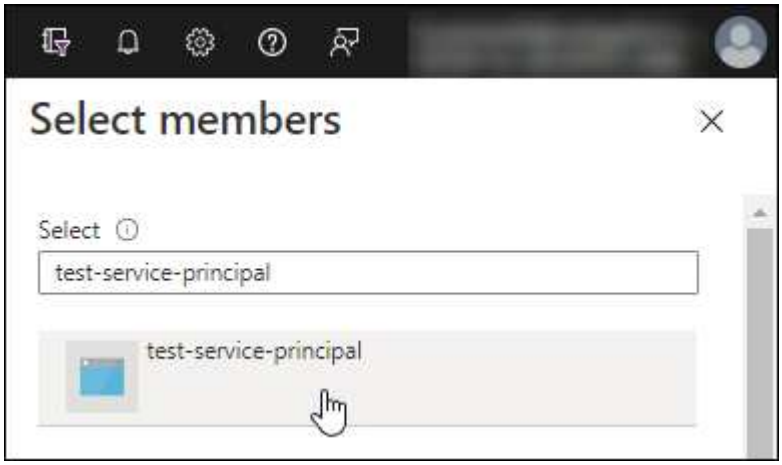
e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

- Behalten Sie die Auswahl von **Benutzer, Gruppe oder Dienstprinzipal** bei.
- Wählen Sie **Mitglieder auswählen**.



- Suchen Sie nach dem Namen der Anwendung.

  Hier ist ein Beispiel:



- Wählen Sie die Anwendung aus und wählen Sie **Auswählen**.
- Wählen Sie **Weiter**.

f. Wählen Sie **Überprüfen + zuweisen**.

   Der Dienstprinzipal verfügt jetzt über die erforderlichen Azure-Berechtigungen zum Bereitstellen des Konsolen-Agenten.

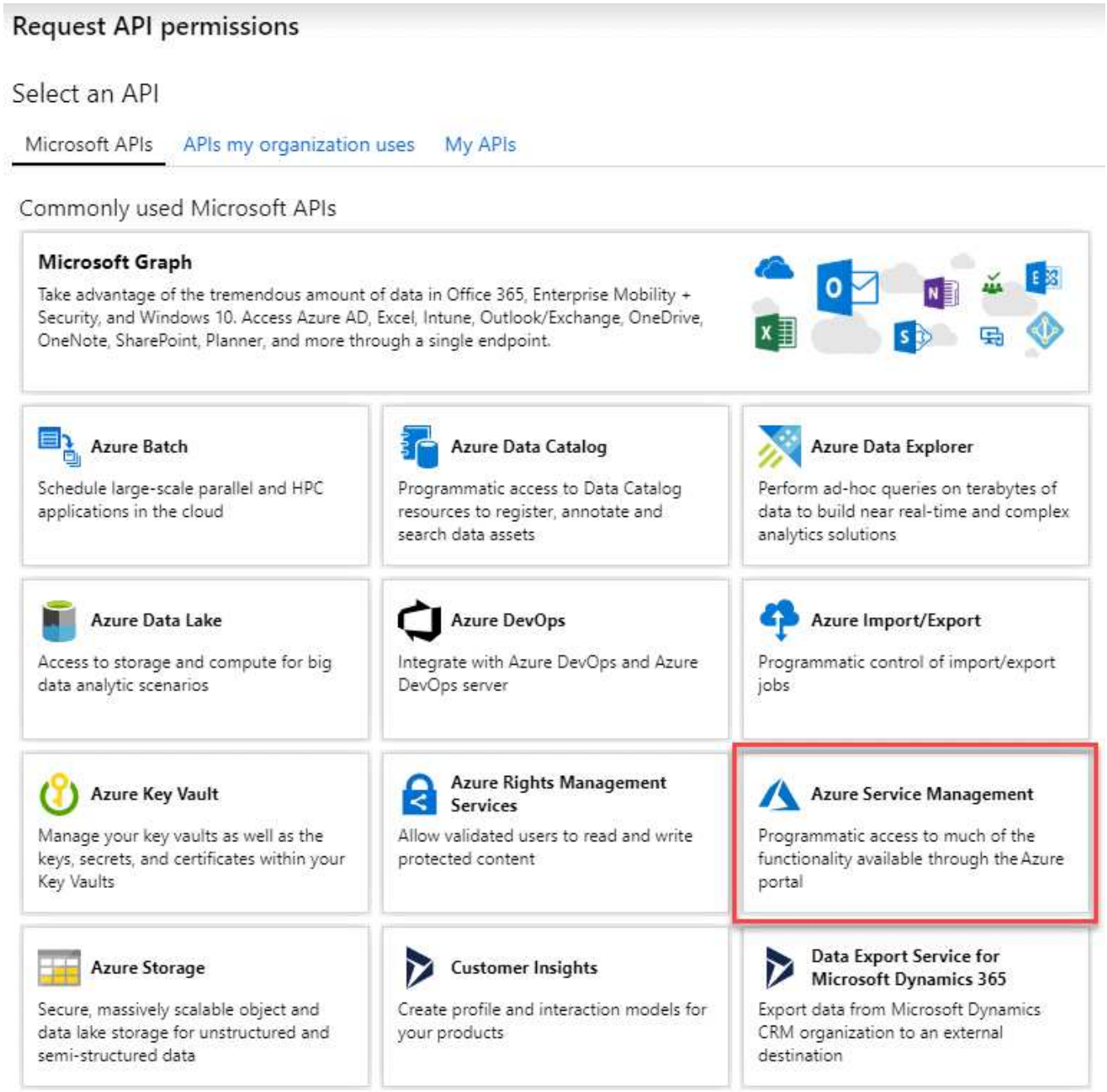
Wenn Sie Cloud Volumes ONTAP aus mehreren Azure-Abonnements bereitstellen möchten, müssen Sie den Dienstprinzipal an jedes dieser Abonnements binden. In der NetApp Console können Sie das Abonnement auswählen, das Sie beim Bereitstellen von Cloud Volumes ONTAP verwenden möchten.

Fügen Sie Berechtigungen für die Windows Azure Service Management-API hinzu

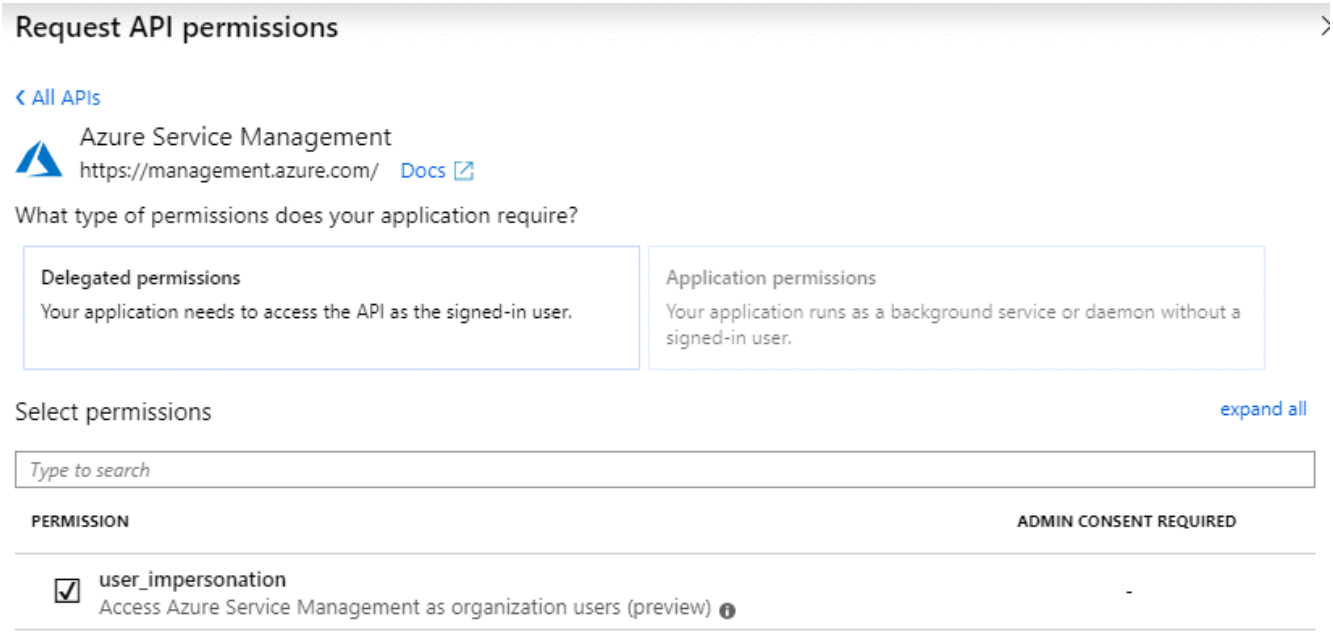
Sie müssen dem Dienstprinzipal die Berechtigung „Windows Azure Service Management API“ zuweisen.

Schritte

1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Wählen Sie **API-Berechtigungen > Berechtigung hinzufügen**.
3. Wählen Sie unter **Microsoft-APIs Azure Service Management** aus.



4. Wählen Sie **Auf Azure Service Management als Organisationsbenutzer zugreifen** und dann **Berechtigungen hinzufügen**.

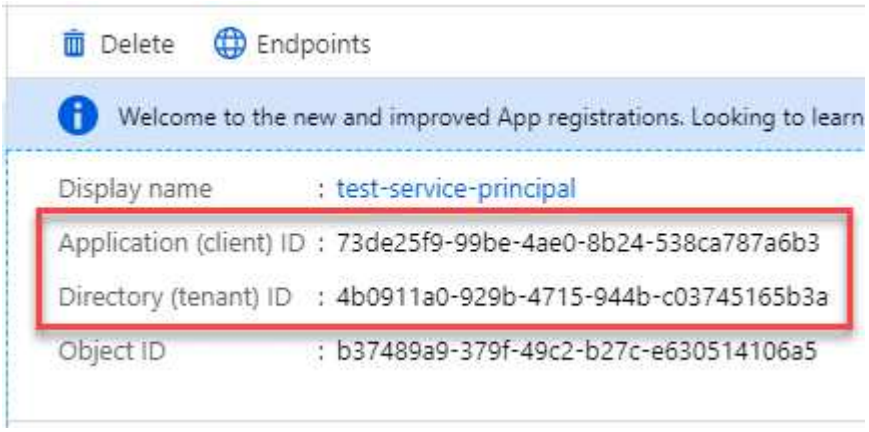


Abrufen der Anwendungs-ID und der Verzeichnis-ID

Wenn Sie das Azure-Konto zur Konsole hinzufügen, müssen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) für die Anwendung angeben. Die Konsole verwendet die IDs zur programmgesteuerten Anmeldung.

Schritte

1. Wählen Sie im Dienst **Microsoft Entra ID App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



Wenn Sie das Azure-Konto zur Konsole hinzufügen, müssen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) für die Anwendung angeben. Die Konsole verwendet die IDs zur programmgesteuerten Anmeldung.

Erstellen eines Client-Geheimnisses

Erstellen Sie ein Client-Geheimnis und geben Sie dessen Wert an die Konsole zur Authentifizierung mit der Microsoft Entra-ID weiter.

Schritte

1. Öffnen Sie den Dienst **Microsoft Entra ID**.
2. Wählen Sie **App-Registrierungen** und wählen Sie Ihre Anwendung aus.
3. Wählen Sie **Zertifikate und Geheimnisse > Neues Clientgeheimnis**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Wählen Sie **Hinzufügen**.
6. Kopieren Sie den Wert des Client-Geheimnisses.

Ergebnis

Ihr Dienstprinzipal ist jetzt eingerichtet und Sie sollten die Anwendungs-ID (Client-ID), die Verzeichnis-ID (Mandant-ID) und den Wert des Client-Geheimnisses kopiert haben. Sie müssen diese Informationen in der Konsole eingeben, wenn Sie ein Azure-Konto hinzufügen.

Fügen Sie die Anmeldeinformationen zur Konsole hinzu

Nachdem Sie ein Azure-Konto mit den erforderlichen Berechtigungen bereitgestellt haben, können Sie die Anmeldeinformationen für dieses Konto zur Konsole hinzufügen. Wenn Sie diesen Schritt abschließen, können Sie Cloud Volumes ONTAP mit anderen Azure-Anmeldeinformationen starten.

Bevor Sie beginnen

Wenn Sie diese Anmeldeinformationen gerade bei Ihrem Cloud-Anbieter erstellt haben, kann es einige Minuten dauern, bis sie zur Verwendung verfügbar sind. Warten Sie einige Minuten, bevor Sie die Anmeldeinformationen zur Konsole hinzufügen.

Bevor Sie beginnen

Sie müssen einen Konsolenagenten erstellen, bevor Sie die Konsoleneinstellungen ändern können. "Erfahren Sie, wie Sie einen Konsolenagenten erstellen" .

Schritte

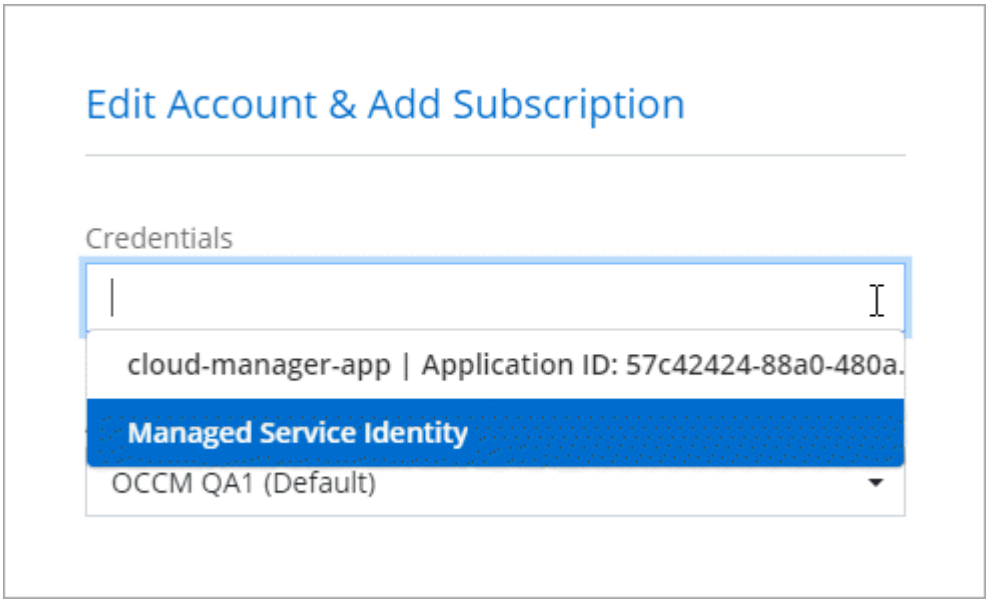
1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
   a. **Speicherort der Anmeldeinformationen**: Wählen Sie **Microsoft Azure > Agent**.
   b. **Anmeldeinformationen definieren**: Geben Sie Informationen zum Microsoft Entra-Dienstprinzipal ein, der die erforderlichen Berechtigungen erteilt:
      - Anwendungs-ID (Client-ID)
      - Verzeichnis-ID (Mandant)
      - Client-Geheimnis

c. **Marketplace-Abonnement**: Verknüpfen Sie ein Marketplace-Abonnement mit diesen Anmeldeinformationen, indem Sie sich jetzt anmelden oder ein vorhandenes Abonnement auswählen.

d. **Überprüfen**: Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und wählen Sie **Hinzufügen**.

Ergebnis

Sie können auf der Seite „Details und Anmeldeinformationen“ zu einem anderen Satz von Anmeldeinformationen wechseln. "beim Hinzufügen eines Systems zur Konsole"



Vorhandene Anmeldeinformationen verwalten

Verwalten Sie die Azure-Anmeldeinformationen, die Sie der Konsole bereits hinzugefügt haben, indem Sie ein Marketplace-Abonnement zuordnen, Anmeldeinformationen bearbeiten und löschen.

Zuordnen eines Azure Marketplace-Abonnements zu Anmeldeinformationen

Nachdem Sie Ihre Azure-Anmeldeinformationen zur Konsole hinzugefügt haben, können Sie diesen Anmeldeinformationen ein Azure Marketplace-Abonnement zuordnen. Mit dem Abonnement können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und auf NetApp -Datendienste zugreifen.

Es gibt zwei Szenarien, in denen Sie ein Azure Marketplace-Abonnement zuordnen können, nachdem Sie die Anmeldeinformationen bereits zur Konsole hinzugefügt haben:

- Sie haben beim ersten Hinzufügen der Anmeldeinformationen zur Konsole kein Abonnement zugeordnet.
- Sie möchten das Azure Marketplace-Abonnement ändern, das mit Azure-Anmeldeinformationen verknüpft ist.

  Durch das Ersetzen des aktuellen Marktplatzabonnements wird es für vorhandene und neue Cloud Volumes ONTAP Systeme aktualisiert.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.

3. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen aus, die einem Konsolenagenten zugeordnet sind, und wählen Sie dann **Abonnement konfigurieren**.

   Sie müssen Anmeldeinformationen auswählen, die einem Konsolenagenten zugeordnet sind. Sie können ein Marktplatzabonnement nicht mit Anmeldeinformationen verknüpfen, die mit der NetApp Console verknüpft sind.

4. Um die Anmeldeinformationen mit einem vorhandenen Abonnement zu verknüpfen, wählen Sie das Abonnement aus der Dropdown-Liste aus und wählen Sie **Konfigurieren**.
5. Um die Anmeldeinformationen einem neuen Abonnement zuzuordnen, wählen Sie **Abonnement hinzufügen > Fortfahren** und befolgen Sie die Schritte im Azure Marketplace:

   a. Melden Sie sich bei entsprechender Aufforderung bei Ihrem Azure-Konto an.

   b. Wählen Sie **Abonnieren**.

   c. Füllen Sie das Formular aus und wählen Sie **Abonnieren**.

   d. Nachdem der Abonnementvorgang abgeschlossen ist, wählen Sie **Konto jetzt konfigurieren**.

      Sie werden zur NetApp Console weitergeleitet.

   e. Auf der Seite **Abonnementzuweisung**:

      - Wählen Sie die Konsolenorganisationen oder -konten aus, mit denen Sie dieses Abonnement verknüpfen möchten.
      - Wählen Sie im Feld **Vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

        Die Konsole ersetzt das vorhandene Abonnement für alle Anmeldeinformationen in der Organisation oder im Konto durch dieses neue Abonnement. Wenn ein Satz von Anmeldeinformationen nie mit einem Abonnement verknüpft war, wird dieses neue Abonnement nicht mit diesen Anmeldeinformationen verknüpft.

      Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.

      - Wählen Sie **Speichern**.

        Das folgende Video zeigt die Schritte zum Abonnieren über den Azure Marketplace:

   Abonnieren Sie NetApp Intelligent Services vom Azure Marketplace

Anmeldeinformationen bearbeiten

Bearbeiten Sie Ihre Azure-Anmeldeinformationen in der Konsole. Sie können beispielsweise das Clientgeheimnis aktualisieren, wenn ein neues Geheimnis für die Dienstprinzipalanwendung erstellt wurde.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie das Aktionsmenü für einen Satz Anmeldeinformationen und wählen Sie dann **Anmeldeinformationen bearbeiten**.

4. Nehmen Sie die erforderlichen Änderungen vor und wählen Sie dann **Übernehmen**.

Anmeldeinformationen löschen

Wenn Sie einen Satz Anmeldeinformationen nicht mehr benötigen, können Sie ihn löschen. Sie können nur Anmeldeinformationen löschen, die keinem System zugeordnet sind.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie auf der Seite **Anmeldeinformationen der Organisation** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Anmeldeinformationen löschen**.
4. Wählen Sie zur Bestätigung **Löschen**.

Google Cloud

Erfahren Sie mehr über Google Cloud-Projekte und -Berechtigungen

Erfahren Sie, wie die NetApp Console Google Cloud-Anmeldeinformationen verwendet, um Aktionen in Ihrem Namen auszuführen, und wie diese Anmeldeinformationen mit Marktplatzabonnements verknüpft werden. Das Verständnis dieser Details kann hilfreich sein, wenn Sie die Anmeldeinformationen für ein oder mehrere Google Cloud-Projekte verwalten. Beispielsweise möchten Sie möglicherweise mehr über das Dienstkonto erfahren, das mit der Konsolen-Agent-VM verknüpft ist.

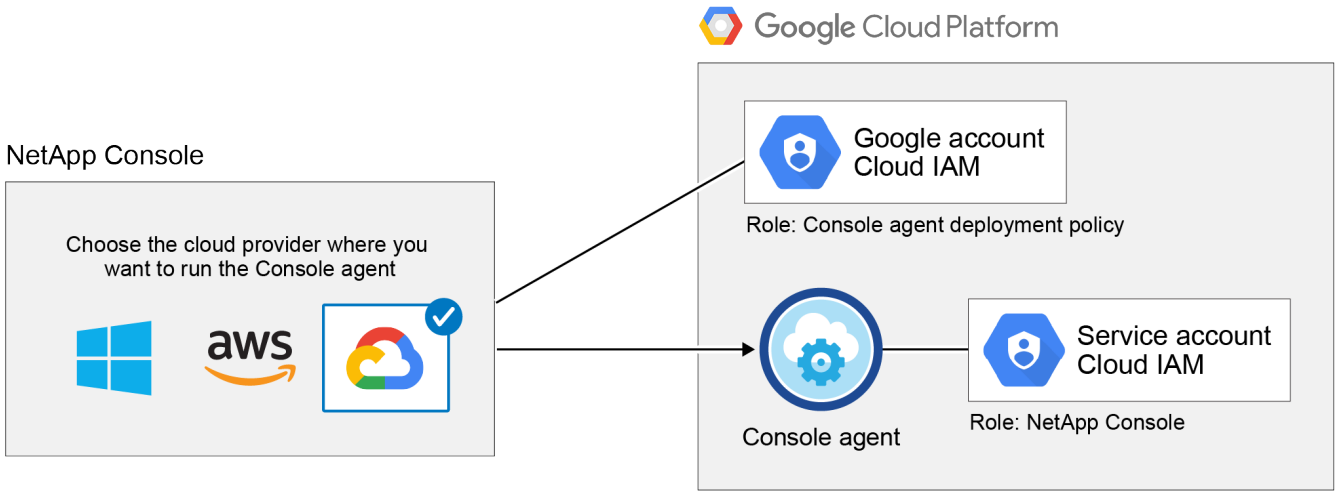
Projekt und Berechtigungen für die NetApp Console

Bevor Sie die Konsole zum Verwalten von Ressourcen in Ihrem Google Cloud-Projekt verwenden können, müssen Sie zunächst einen Konsolen-Agenten bereitstellen. Der Agent darf nicht bei Ihnen vor Ort oder bei einem anderen Cloud-Anbieter ausgeführt werden.

Bevor Sie einen Konsolenagenten direkt von der Konsole aus bereitstellen können, müssen zwei Berechtigungssätze vorhanden sein:

1. Sie müssen einen Konsolen-Agenten mit einem Google-Konto bereitstellen, das über die Berechtigung zum Starten der VM-Instanz des Konsolen-Agenten von der Konsole aus verfügt.
2. Beim Bereitstellen des Konsolenagenten werden Sie aufgefordert, einen "Dienstkonto" für die VM-Instanz. Die Konsole erhält vom Dienstkonto die Berechtigung, Cloud Volumes ONTAP -Systeme zu erstellen und zu verwalten, Backups mithilfe von NetApp Backup und Recovery zu verwalten und mehr. Berechtigungen werden erteilt, indem dem Dienstkonto eine benutzerdefinierte Rolle zugewiesen wird.

Die folgende Abbildung veranschaulicht die unter den Nummern 1 und 2 beschriebenen Berechtigungsanforderungen:



Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

- "Google Cloud-Berechtigungen für den Standardmodus einrichten"
- "Berechtigungen für den eingeschränkten Modus einrichten"

Anmeldeinformationen und Marktplatzabonnements

Wenn Sie einen Konsolen-Agenten in Google Cloud bereitstellen, erstellt die Konsole einen Standardsatz von Anmeldeinformationen für das Google Cloud-Dienstkonto in dem Projekt, in dem sich der Konsolen-Agent befindet. Diese Anmeldeinformationen müssen mit einem Google Cloud Marketplace-Abonnement verknüpft sein, damit Sie für Cloud Volumes ONTAP und NetApp -Datendienste bezahlen können.

"Erfahren Sie, wie Sie ein Google Cloud Marketplace-Abonnement zuordnen" .

Beachten Sie Folgendes zu Google Cloud-Anmeldeinformationen und Marktplatz-Abonnements:

- Einem Konsolenagenten kann nur ein Satz Google Cloud-Anmeldeinformationen zugeordnet werden.
- Sie können den Anmeldeinformationen nur ein Google Cloud Marketplace-Abonnement zuordnen
- Sie können ein bestehendes Marktplatz-Abonnement durch ein neues Abonnement ersetzen

Projekt für Cloud Volumes ONTAP

Cloud Volumes ONTAP kann sich im selben Projekt wie der Konsolenagent oder in einem anderen Projekt befinden. Um Cloud Volumes ONTAP in einem anderen Projekt bereitzustellen, müssen Sie zuerst das Dienstkonto und die Rolle des Konsolenagenten zu diesem Projekt hinzufügen.

- "Erfahren Sie, wie Sie das Dienstkonto einrichten"
- "Erfahren Sie, wie Sie Cloud Volumes ONTAP in Google Cloud bereitstellen und ein Projekt auswählen"

Verwalten Sie Google Cloud-Anmeldeinformationen und Abonnements für die NetApp Console

Sie können die Google Cloud-Anmeldeinformationen verwalten, die einer VM-Instanz des Console-Agenten zugeordnet sind, indem Sie ein Marktplatzabonnement zuordnen und den Abonnementprozess beheben. Beide Aufgaben stellen sicher, dass Sie Ihr Marktplatz-Abonnement zum Bezahlen von Datendiensten verwenden können.

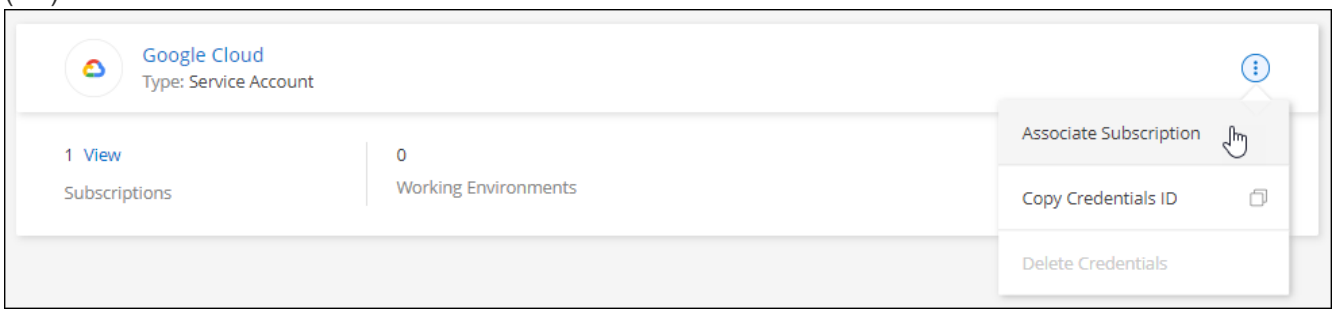
Verknüpfen Sie ein Marketplace-Abonnement mit Google Cloud-Anmeldeinformationen

Wenn Sie einen Konsolenagenten in Google Cloud bereitstellen, erstellt die Konsole einen Standardsatz von Anmeldeinformationen, die einer VM-Instanz des Konsolenagenten zugeordnet sind. Sie können das mit diesen Anmeldeinformationen verknüpfte Google Cloud Marketplace-Abonnement jederzeit ändern. Mit dem Abonnement können Sie ein Cloud Volumes ONTAP -System mit nutzungsbasierter Abrechnung erstellen und andere Datendienste nutzen.

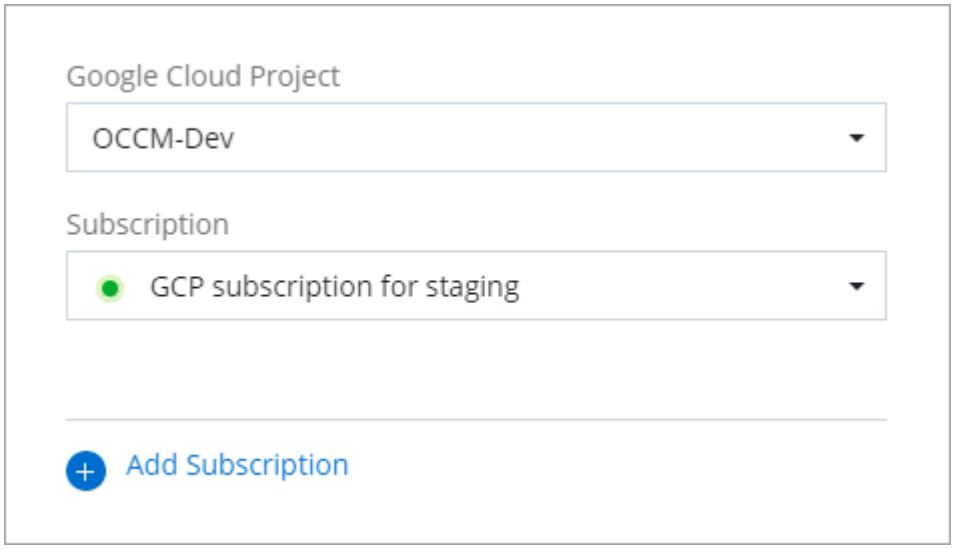
Durch das Ersetzen des aktuellen Marktplatzabonnements durch ein neues Abonnement wird das Marktplatzabonnement für alle vorhandenen Cloud Volumes ONTAP Systeme und alle neuen Systeme geändert.

Schritte

1. Wählen Sie **Administration > *Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen der Organisation** aus.
3. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen aus, die einem Konsolenagenten zugeordnet sind, und wählen Sie dann **Abonnement konfigurieren**. +neuer Screenshot erforderlich (TS)



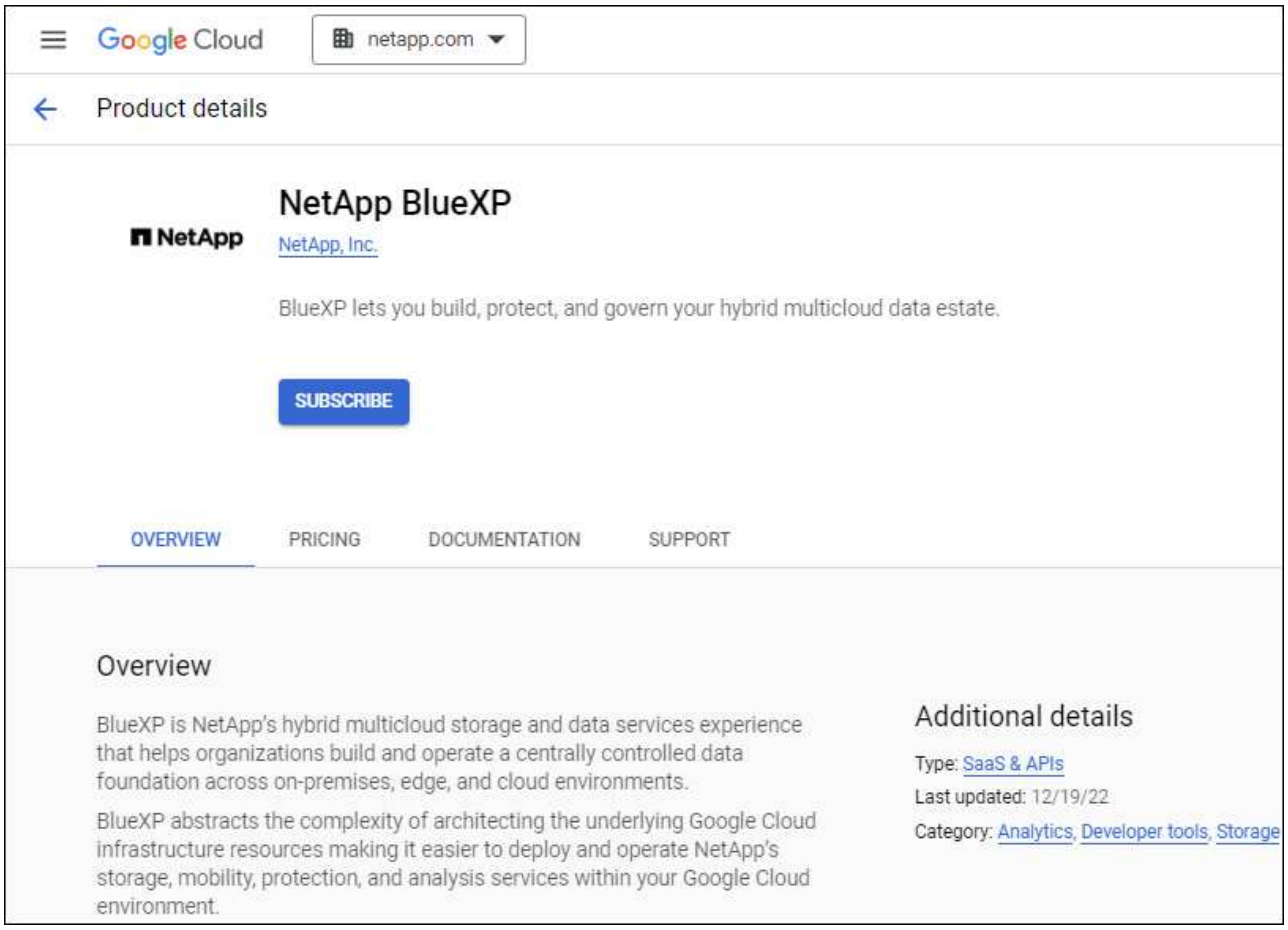
4. Um ein vorhandenes Abonnement mit den ausgewählten Anmeldeinformationen zu konfigurieren, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Dropdown-Liste aus und wählen Sie dann **Konfigurieren**.



5. 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**.

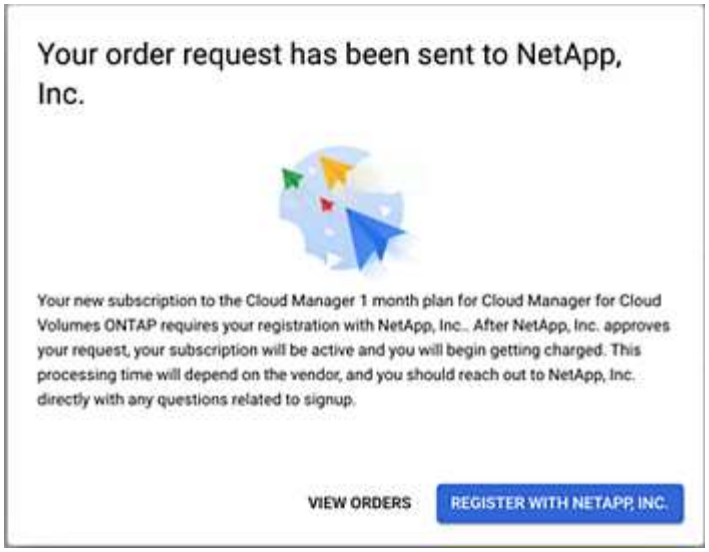
c. Wählen Sie das entsprechende Abrechnungskonto aus und stimmen Sie den Allgemeinen Geschäftsbedingungen zu.

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 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.

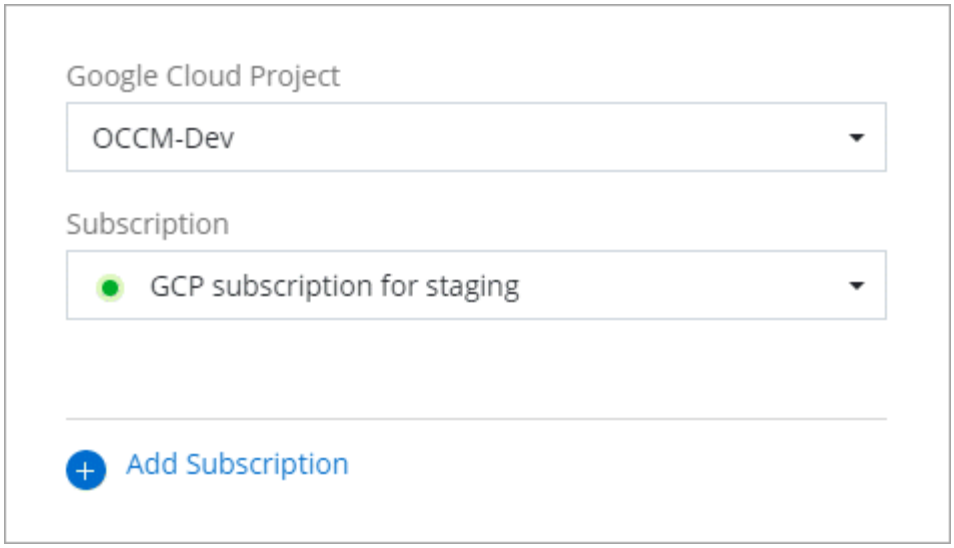
Für alle anderen Organisationen oder Konten müssen Sie das Abonnement manuell zuordnen, indem Sie diese Schritte wiederholen.

- Wählen Sie **Speichern**.

  Das folgende Video zeigt die Schritte zum Abonnieren vom Google Cloud Marketplace:

Abonnieren Sie über den Google Cloud Marketplace

a. Navigieren Sie nach Abschluss dieses Vorgangs zurück zur Seite „Anmeldeinformationen“ in der Konsole und wählen Sie dieses neue Abonnement aus.

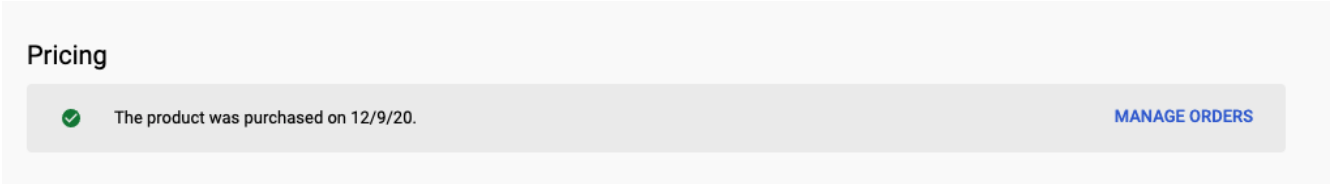


Fehlerbehebung beim Marketplace-Abonnementprozess

Manchmal kann das Abonnieren von NetApp -Datendiensten über den Google Cloud Marketplace aufgrund falscher Berechtigungen oder einer versehentlichen Nichtbefolgung der Umleitung zur Konsole fragmentiert werden. Führen Sie in diesem Fall die folgenden Schritte aus, um den Abonnementvorgang abzuschließen.

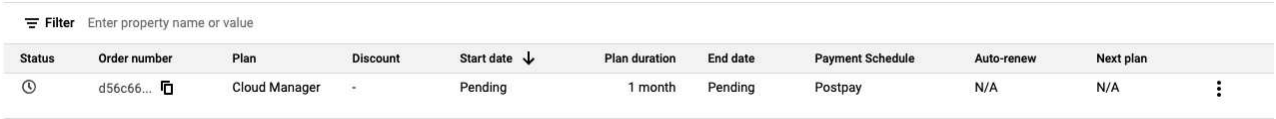
Schritte

1. Navigieren Sie zum "NetApp -Seite im Google Cloud Marketplace" um den Status der Bestellung zu überprüfen. Wenn auf der Seite „Beim Anbieter verwalten“ steht, scrollen Sie nach unten und wählen Sie „Bestellungen verwalten“ aus.



   - Wenn die Bestellung unerwarteterweise ein grünes Häkchen aufweist, ist möglicherweise bereits jemand anderes aus der Organisation, der dasselbe Abrechnungskonto verwendet, angemeldet. Wenn dies unerwartet ist oder Sie die Details dieses Abonnements benötigen, wenden Sie sich an Ihr NetApp Vertriebsteam.

   - Wenn für die Bestellung eine Uhr und der Status **Ausstehend** angezeigt werden, gehen Sie zurück zur Marktplatzseite und wählen Sie **Beim Anbieter verwalten**, um den Vorgang wie oben dokumentiert abzuschließen.



Verwalten der mit der NetApp Console verknüpften NSS-Anmeldeinformationen

Verknüpfen Sie ein NetApp Support Site-Konto mit Ihrer Konsolenorganisation, um wichtige Workflows für die Speicherverwaltung zu aktivieren. Diese NSS-Anmeldeinformationen sind mit der gesamten Organisation verknüpft.

Die Konsole unterstützt auch die Zuordnung eines NSS-Kontos pro Benutzerkonto. "Erfahren Sie, wie Sie Anmeldeinformationen auf Benutzerebene verwalten" .

Überblick

Um die folgenden Aufgaben zu ermöglichen, müssen Sie die Anmeldeinformationen der NetApp Support Site mit der Seriennummer Ihres spezifischen Konsolenkontos verknüpfen:

- Bereitstellen von Cloud Volumes ONTAP mit eigener Lizenz (BYOL)

  Die Angabe Ihres NSS-Kontos ist erforderlich, damit die Konsole Ihren Lizenzschlüssel hochladen und das Abonnement für die von Ihnen erworbene Laufzeit aktivieren kann. Hierzu gehören automatische Updates bei Laufzeitverlängerungen.

- Registrieren von Pay-as-you-go Cloud Volumes ONTAP Systemen

  Die Angabe Ihres NSS-Kontos ist erforderlich, um den Support für Ihr System zu aktivieren und Zugriff auf die technischen Supportressourcen von NetApp zu erhalten.

- Aktualisieren der Cloud Volumes ONTAP -Software auf die neueste Version

Diese Anmeldeinformationen sind mit der Seriennummer Ihres spezifischen Konsolenkontos verknüpft. Benutzer können über **Support > NSS-Verwaltung** auf diese Anmeldeinformationen zugreifen.

Hinzufügen eines NSS-Kontos

Sie können Ihre NetApp Support Site-Konten zur Verwendung mit der Konsole über das Support-Dashboard in der Konsole hinzufügen und verwalten.

Wenn Sie Ihr NSS-Konto hinzugefügt haben, verwendet die Konsole diese Informationen für Dinge wie Lizenzdownloads, Überprüfung von Software-Upgrades und zukünftige Support-Registrierungen.

Sie können Ihrer Organisation mehrere NSS-Konten zuordnen. Sie können jedoch nicht innerhalb derselben Organisation Kundenkonten und Partnerkonten haben.

NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsdienste speziell für Support und Lizenzierung.

Schritte

1. Unter **Administration > Support**.
2. Wählen Sie **NSS-Verwaltung**.
3. Wählen Sie **NSS-Konto hinzufügen**.
4. Wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite weitergeleitet zu werden.
5. Geben Sie auf der Anmeldeseite Ihre für die NetApp Support-Site registrierte E-Mail-Adresse und Ihr Kennwort ein.

Nach erfolgreicher Anmeldung speichert NetApp den NSS-Benutzernamen.

Dies ist eine vom System generierte ID, die Ihrer E-Mail-Adresse zugeordnet ist. Auf der Seite **NSS-Verwaltung** können Sie Ihre E-Mail-Adresse aus dem ••• Speisekarte.

- Wenn Sie Ihre Anmeldeinformationen aktualisieren müssen, gibt es auch die Option **Anmeldeinformationen aktualisieren** im ••• Speisekarte.

  Bei Verwendung dieser Option werden Sie aufgefordert, sich erneut anzumelden. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Sie werden durch eine entsprechende Benachrichtigung darauf aufmerksam gemacht.

Wie geht es weiter?

Benutzer können jetzt das Konto auswählen, wenn sie neue Cloud Volumes ONTAP -Systeme erstellen und wenn sie vorhandene Cloud Volumes ONTAP -Systeme registrieren.

- "Starten von Cloud Volumes ONTAP in AWS"
- "Starten von Cloud Volumes ONTAP in Azure"
- "Starten von Cloud Volumes ONTAP in Google Cloud"
- "Registrierung von Umlagesystemen"

NSS-Anmeldeinformationen aktualisieren

Aus Sicherheitsgründen müssen Sie Ihre NSS-Anmeldeinformationen alle 90 Tage aktualisieren. Sie werden im Benachrichtigungscenter der Konsole benachrichtigt, wenn Ihre NSS-Anmeldeinformationen abgelaufen sind. "Erfahren Sie mehr über das Benachrichtigungscenter" .

Abgelaufene Anmeldeinformationen können unter anderem Folgendes beeinträchtigen:

- Lizenzaktualisierungen, was bedeutet, dass Sie die neu erworbene Kapazität nicht nutzen können.
- Möglichkeit zum Einreichen und Verfolgen von Supportfällen.

Darüber hinaus können Sie die mit Ihrer Organisation verknüpften NSS-Anmeldeinformationen aktualisieren, wenn Sie das mit Ihrer Organisation verknüpfte NSS-Konto ändern möchten. Zum Beispiel, wenn die mit Ihrem NSS-Konto verknüpfte Person Ihr Unternehmen verlassen hat.

Schritte

1. Unter **Administration > Support**.
2. Wählen Sie **NSS-Verwaltung**.
3. Wählen Sie für das NSS-Konto, das Sie aktualisieren möchten, ••• und wählen Sie dann **Anmeldeinformationen aktualisieren**.
4. Wenn Sie dazu aufgefordert werden, wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite weitergeleitet zu werden.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsdienste im Zusammenhang mit Support und Lizenzierung.

5. Geben Sie auf der Anmeldeseite Ihre für die NetApp Support-Site registrierte E-Mail-Adresse und Ihr Kennwort ein.

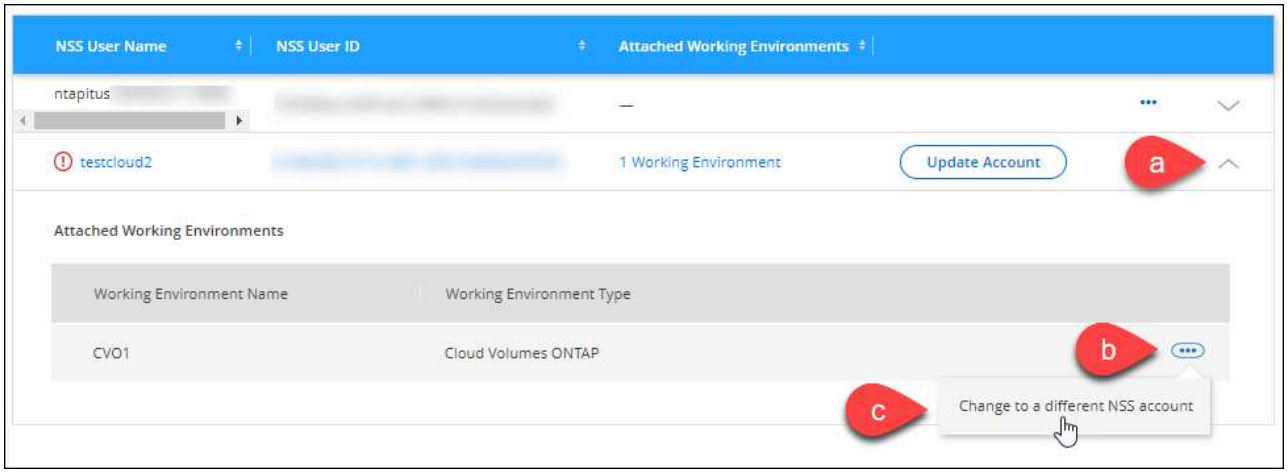
Verbinden Sie ein System mit einem anderen NSS-Konto

Wenn Ihr Unternehmen über mehrere NetApp Support Site-Konten verfügt, können Sie ändern, welches Konto mit einem Cloud Volumes ONTAP -System verknüpft ist.

Sie müssen das Konto zunächst mit der Konsole verknüpft haben.

Schritte

1. Unter **Administration > Support**.
2. Wählen Sie **NSS-Verwaltung**.
3. Führen Sie die folgenden Schritte aus, um das NSS-Konto zu ändern:
   a. Erweitern Sie die Zeile für das NetApp Support Site-Konto, mit dem das System derzeit verknüpft ist.
   b. Wählen Sie für das System, für das Sie die Zuordnung ändern möchten, •••
   c. Wählen Sie **Zu einem anderen NSS-Konto wechseln**.



   d. Wählen Sie das Konto aus und wählen Sie dann **Speichern**.

E-Mail-Adresse für ein NSS-Konto anzeigen

Aus Sicherheitsgründen wird die mit einem NSS-Konto verknüpfte E-Mail-Adresse standardmäßig nicht angezeigt. Sie können die E-Mail-Adresse und den zugehörigen Benutzernamen für ein NSS-Konto anzeigen.

Wenn Sie zur NSS-Verwaltungsseite gehen, generiert die Konsole für jedes Konto in der Tabelle ein Token. Dieses Token enthält Informationen zur zugehörigen E-Mail-Adresse. Das Token wird entfernt, wenn Sie die Seite verlassen. Die Informationen werden niemals zwischengespeichert, was zum Schutz Ihrer Privatsphäre beiträgt.

Schritte

1. Unter **Administration > Support**.
2. Wählen Sie **NSS-Verwaltung**.
3. Wählen Sie für das NSS-Konto, das Sie aktualisieren möchten, ••• und wählen Sie dann **E-Mail-Adresse anzeigen**. Über die Schaltfläche „Kopieren“ können Sie die E-Mail-Adresse kopieren.

Entfernen eines NSS-Kontos

Löschen Sie alle NSS-Konten, die Sie nicht mehr mit der Konsole verwenden möchten.

Sie können kein Konto löschen, das derzeit mit einem Cloud Volumes ONTAP System verknüpft ist. Sie müssen zuerstVerbinden Sie diese Systeme mit einem anderen NSS-Konto .

Schritte

1. Unter **Administration > Support**.
2. Wählen Sie **NSS-Verwaltung**.
3. Wählen Sie für das NSS-Konto, das Sie löschen möchten, ••• und wählen Sie dann **Löschen**.
4. Wählen Sie zur Bestätigung **Löschen**.

Verwalten Sie die mit Ihrer NetApp Console verknüpften Anmeldeinformationen

Abhängig von den Aktionen, die Sie in der Konsole ausgeführt haben, haben Sie möglicherweise ONTAP Anmeldeinformationen und Anmeldeinformationen für die NetApp Support Site (NSS) mit Ihrer Benutzeranmeldung verknüpft. Sie können diese Anmeldeinformationen anzeigen und verwalten, nachdem Sie sie verknüpft haben. Wenn Sie beispielsweise das Kennwort für diese Anmeldeinformationen ändern, müssen Sie das Kennwort in der Konsole aktualisieren.

ONTAP -Anmeldeinformationen

Benutzer benötigen ONTAP Administratoranmeldeinformationen, um ONTAP Cluster in der Konsole zu erkennen. Der Zugriff auf den ONTAP System Manager hängt jedoch davon ab, ob Sie einen Konsolenagenten verwenden oder nicht.

Ohne einen Konsolenagenten

Benutzer werden aufgefordert, ihre ONTAP Anmeldeinformationen einzugeben, um auf den ONTAP System Manager für den Cluster zuzugreifen. Benutzer können diese Anmeldeinformationen in der Konsole speichern, sodass sie nicht jedes Mal aufgefordert werden, sie einzugeben. Benutzeranmeldeinformationen sind nur für den jeweiligen Benutzer sichtbar und können auf der Seite „Benutzeranmeldeinformationen“ verwaltet werden.

Mit einem Konsolenagenten

Standardmäßig werden Benutzer nicht aufgefordert, ihre ONTAP Anmeldeinformationen einzugeben, um auf den ONTAP System Manager zuzugreifen. Ein Konsolenadministrator (mit der Rolle „Organisationsadministrator“) kann die Konsole jedoch so konfigurieren, dass Benutzer aufgefordert werden, ihre ONTAP Anmeldeinformationen einzugeben. Wenn diese Einstellung aktiviert ist, müssen Benutzer jedes Mal ihre ONTAP Anmeldeinformationen eingeben.

"Erfahren Sie mehr."

NSS -Anmeldeinformationen

Die mit Ihrer NetApp Console Anmeldung verknüpften NSS-Anmeldeinformationen ermöglichen die Support-Registrierung, das Fallmanagement und den Zugriff auf Digital Advisor.

- Wenn Sie auf **Support > Ressourcen** zugreifen und sich für den Support registrieren, werden Sie aufgefordert, NSS-Anmeldeinformationen mit Ihrem Login zu verknüpfen.

Dadurch wird Ihre Organisation oder Ihr Konto für den Support registriert und der Supportanspruch aktiviert. Nur ein Benutzer in Ihrer Organisation muss seinem Login ein NetApp Support Site-Konto zuordnen, um sich für den Support zu registrieren und den Supportanspruch zu aktivieren. Nachdem dies abgeschlossen ist, wird auf der Seite **Ressourcen** angezeigt, dass Ihr Konto für den Support registriert ist.

"Erfahren Sie, wie Sie sich für den Support registrieren"

- Wenn Sie auf **Administration > Support > Fallmanagement** zugreifen, werden Sie aufgefordert, Ihre NSS-Anmeldeinformationen einzugeben, falls Sie dies nicht bereits getan haben. Auf dieser Seite können Sie die mit Ihrem NSS-Konto und Ihrem Unternehmen verbundenen Supportfälle erstellen und verwalten.
- Wenn Sie in der Konsole auf Digital Advisor zugreifen, werden Sie aufgefordert, sich bei Digital Advisor anzumelden, indem Sie Ihre NSS-Anmeldeinformationen eingeben.

Beachten Sie Folgendes zum NSS-Konto, das mit Ihrer Anmeldung verknüpft ist:

- Das Konto wird auf Benutzerebene verwaltet, was bedeutet, dass es für andere Benutzer, die sich anmelden, nicht sichtbar ist.
- Pro Benutzer kann nur ein NSS-Konto mit Digital Advisor und Support-Fallmanagement verknüpft sein.
- Wenn Sie versuchen, ein NetApp Support Site-Konto mit einem Cloud Volumes ONTAP -System zu verknüpfen, können Sie nur aus den NSS-Konten auswählen, die der Organisation hinzugefügt wurden, deren Mitglied Sie sind.

  Die Anmeldeinformationen auf NSS-Kontoebene unterscheiden sich von dem NSS-Konto, das mit Ihrer Anmeldung verknüpft ist. Mit den Anmeldeinformationen auf NSS-Kontoebene können Sie Cloud Volumes ONTAP mit BYOL bereitstellen, PAYGO-Systeme registrieren und die Software aktualisieren.

  "Erfahren Sie mehr über die Verwendung von NSS-Anmeldeinformationen mit Ihrer NetApp Console -Organisation oder Ihrem NetApp Console-Konto" .

Verwalten Sie Ihre Benutzeranmeldeinformationen

Verwalten Sie Ihre Benutzeranmeldeinformationen, indem Sie den Benutzernamen und das Kennwort aktualisieren oder die Anmeldeinformationen löschen.

Schritte

1. Wählen Sie **Administration > Anmeldeinformationen**.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wenn Sie noch keine Benutzeranmeldeinformationen haben, können Sie **NSS-Anmeldeinformationen hinzufügen** auswählen, um Ihr NetApp Support Site-Konto hinzuzufügen.
4. Verwalten Sie vorhandene Anmeldeinformationen, indem Sie im Menü „Aktionen“ die folgenden Optionen auswählen:
   - **Anmeldeinformationen aktualisieren**: Aktualisieren Sie den Benutzernamen und das Kennwort für das Konto.
   - **Anmeldeinformationen löschen**: Entfernen Sie das mit Ihrer Konsolenanmeldung verknüpfte NSS-Konto.

Überwachen Sie NetApp Console

Sie können den Status der von der Konsole ausgeführten Vorgänge überwachen, um

festzustellen, ob Probleme vorliegen, die Sie beheben müssen. Sie können den Status auf der Audit-Seite oder im Benachrichtigungscenter anzeigen oder sich Benachrichtigungen per E-Mail senden lassen.

Die Tabelle hebt die Funktionen der Audit-Seite und des Benachrichtigungscenters durch einen Vergleich hervor.

Benachrichtigungscenter	Audit-Seite
Zeigt den Status auf hoher Ebene für Ereignisse und Aktionen an	Bietet Details zu jedem Ereignis oder jeder Aktion zur weiteren Untersuchung
Zeigt den Status der aktuellen Anmeldesitzung an (die Informationen werden nach der Abmeldung nicht im Benachrichtigungscenter angezeigt)	Behält den Status des letzten Monats bei
Zeigt nur Aktionen an, die in der Benutzeroberfläche initiiert wurden	Zeigt alle Aktionen der Benutzeroberfläche oder APIs an
Zeigt vom Benutzer initiierte Aktionen an	Zeigt alle Aktionen an, egal ob vom Benutzer oder vom System initiiert
Ergebnisse nach Wichtigkeit filtern	Filtern Sie nach Dienst, Aktion, Benutzer, Status und mehr
Bietet die Möglichkeit, Benachrichtigungen per E-Mail an Benutzer und andere zu senden	Keine E-Mail-Funktion

Überwachen Sie die Benutzeraktivität auf der Seite „Überwachen“.

Auf der Seite „Audit“ werden die Aktionen angezeigt, die Benutzer zur Verwaltung Ihrer Organisation oder Ihres Kontos ausgeführt haben. Dazu gehören Verwaltungsaktionen wie das Zuordnen von Benutzern, das Erstellen von Systemen, das Erstellen von Agenten und mehr.

Verwenden Sie die Audit-Seite, um zu ermitteln, wer eine Aktion ausgeführt hat oder welchen Status sie hat.

Schritte

1. Wählen Sie **Administration > Audit**.
2. Verwenden Sie die Filter über der Tabelle, um zu ändern, welche Aktionen in der Tabelle angezeigt werden.

   Sie können beispielsweise den Filter **Dienst** verwenden, um Aktionen anzuzeigen, die sich auf einen bestimmten Dienst beziehen, oder Sie können den Filter **Benutzer** verwenden, um Aktionen anzuzeigen, die sich auf ein bestimmtes Benutzerkonto beziehen.

Laden Sie Überwachungsprotokolle von der Überwachungsseite herunter

Sie können die Audit-Protokolle von der Audit-Seite in eine CSV-Datei herunterladen. Auf diese Weise können Sie die Aktionen protokollieren, die Benutzer in Ihrer Organisation ausführen. Die CSV-Datei enthält alle Spalten in der heruntergeladenen CSV-Datei, unabhängig von Filtern oder angezeigten Spalten auf der Audit-Seite.

Schritte

1. Wählen Sie auf der Seite **Audit** das Download-Symbol in der oberen rechten Ecke der Tabelle aus.

Überwachen Sie Aktivitäten mithilfe des Benachrichtigungscenters

Benachrichtigungen verfolgen Konsolenvorgänge, um den Erfolg zu bestätigen. Sie ermöglichen Ihnen, den Status vieler Konsolenaktionen anzuzeigen, die Sie während Ihrer aktuellen Anmeldesitzung initiiert haben. Nicht alle Konsolendienste melden Informationen an das Benachrichtigungscenter.

Sie können die Benachrichtigungen anzeigen, indem Sie die Benachrichtigungsglocke ( ) in der Menüleiste. Die Farbe der kleinen Blase in der Glocke zeigt die aktive Benachrichtigung mit dem höchsten Schweregrad an. Wenn Sie also eine rote Blase sehen, bedeutet dies, dass es eine wichtige Benachrichtigung gibt, die Sie beachten sollten.

Sie können die Konsole auch so konfigurieren, dass bestimmte Arten von Benachrichtigungen per E-Mail gesendet werden, sodass Sie über wichtige Systemaktivitäten informiert werden, auch wenn Sie nicht beim System angemeldet sind. E-Mails können an alle Benutzer Ihrer Organisation oder an andere Empfänger gesendet werden, die über bestimmte Arten von Systemaktivitäten informiert werden müssen. Erfahren Sie, wie SieE-Mail-Benachrichtigungseinstellungen festlegen .

Vergleich des Benachrichtigungscenters mit Warnungen

Über das Benachrichtigungscenter können Sie den Status der von Ihnen eingeleiteten Vorgänge anzeigen und Warnbenachrichtigungen für bestimmte Arten von Systemaktivitäten einrichten. Mithilfe von Warnmeldungen können Sie Probleme oder potenzielle Risiken in Ihrer ONTAP Speicherumgebung im Zusammenhang mit Kapazität, Verfügbarkeit, Leistung, Schutz und Sicherheit erkennen.

"Erfahren Sie mehr über NetApp Console -Warnmeldungen"

Benachrichtigungstypen

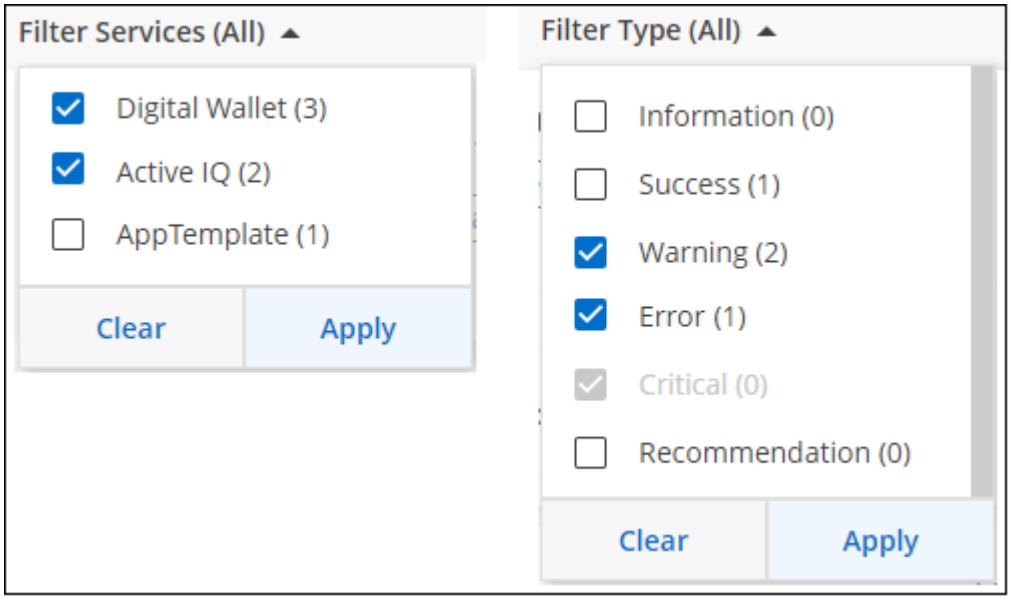
Die Konsole klassifiziert Benachrichtigungen in die folgenden Kategorien:

Benachrichtigungstyp	Beschreibung
Kritisch	Es ist ein Problem aufgetreten, das zu einer Dienstunterbrechung führen kann, wenn nicht sofort Abhilfemaßnahmen ergriffen werden.
Fehler	Eine Aktion oder ein Prozess endete mit einem Fehler oder könnte zu einem Fehler führen, wenn keine Korrekturmaßnahmen ergriffen werden.
Warnung	Ein Problem, dessen Sie sich bewusst sein sollten, um sicherzustellen, dass es nicht den kritischen Schweregrad erreicht. Benachrichtigungen dieses Schweregrads verursachen keine Dienstunterbrechung und es sind möglicherweise keine sofortigen Korrekturmaßnahmen erforderlich.
Empfehlung	Eine Systemempfehlung für Sie, Maßnahmen zur Verbesserung des Systems oder eines bestimmten Dienstes zu ergreifen; zum Beispiel: Kosteneinsparungen, Vorschläge für neue Dienste, empfohlene Sicherheitskonfiguration usw.
Information	Eine Nachricht, die zusätzliche Informationen zu einer Aktion oder einem Prozess bereitstellt.
Erfolg	Eine Aktion oder ein Prozess wurde erfolgreich abgeschlossen.

Benachrichtigungen filtern

Standardmäßig werden alle aktiven Benachrichtigungen im Benachrichtigungscenter angezeigt. Sie können die angezeigten Benachrichtigungen filtern, um nur die Benachrichtigungen anzuzeigen, die für Sie wichtig

sind. Sie können nach „Dienst“ und nach „Typ“ der Benachrichtigung filtern.



Wenn Sie beispielsweise für Konsolenvorgänge nur Benachrichtigungen vom Typ „Fehler“ und „Warnung“ sehen möchten, wählen Sie diese Einträge aus, und Sie sehen nur diese Benachrichtigungstypen.

Benachrichtigungen verwerfen

Sie können Benachrichtigungen von der Seite entfernen, wenn Sie sie nicht mehr sehen müssen. Sie können Benachrichtigungen einzeln oder alle auf einmal ablehnen.

Um alle Benachrichtigungen zu schließen, wählen Sie im Benachrichtigungscenter ⋮ und wählen Sie **Alle verwerfen**.

Um einzelne Benachrichtigungen abzulehnen, bewegen Sie den Cursor über die Benachrichtigung und wählen Sie **Ablehnen**.

E-Mail-Benachrichtigungseinstellungen festlegen

Sie können bestimmte Arten von Benachrichtigungen per E-Mail senden, sodass Sie über wichtige Systemaktivitäten informiert werden, auch wenn Sie nicht angemeldet sind. E-Mails können an alle Benutzer gesendet werden, die Teil Ihrer Organisation oder Ihres Kontos sind, oder an alle anderen Empfänger, die über bestimmte Arten von Systemaktivitäten informiert werden müssen.

- Die Konsole sendet E-Mail-Benachrichtigungen für den Agenten, Lizenzen und Abonnements, NetApp Copy and Sync und NetApp Backup and Recovery.
- Das Senden von E-Mail-Benachrichtigungen wird nicht unterstützt, wenn der Konsolenagent auf einer Site ohne Internetzugang installiert ist.

Die Filter, die Sie im Benachrichtigungscenter festlegen, bestimmen nicht die Art der Benachrichtigungen, die Sie per E-Mail erhalten. Standardmäßig erhält jeder Organisationsadministrator E-Mails für alle „Kritischen“ und „Empfehlungs“-Benachrichtigungen. Diese Benachrichtigungen gelten für alle Dienste. Sie können nicht auswählen, nur für bestimmte Dienste Benachrichtigungen zu erhalten, beispielsweise für Agenten oder NetApp Backup and Recovery.

Alle anderen Benutzer und Empfänger sind so konfiguriert, dass sie keine Benachrichtigungs-E-Mails erhalten.

Daher müssen Sie für alle weiteren Benutzer die Benachrichtigungseinstellungen konfigurieren.

Sie müssen über die Rolle des Organisationsadministrators verfügen, um die Benachrichtigungseinstellungen anzupassen.

Schritte

1. Wählen Sie **Verwaltung > Benachrichtigungseinstellungen**.
2. Wählen Sie **Benutzer der Organisation** oder **Zusätzliche Empfänger**.

   Auf der Seite **Zusätzliche Empfänger** können Sie die Konsole so konfigurieren, dass Personen benachrichtigt werden, die Mitglieder Ihrer Konsolenorganisation sind.

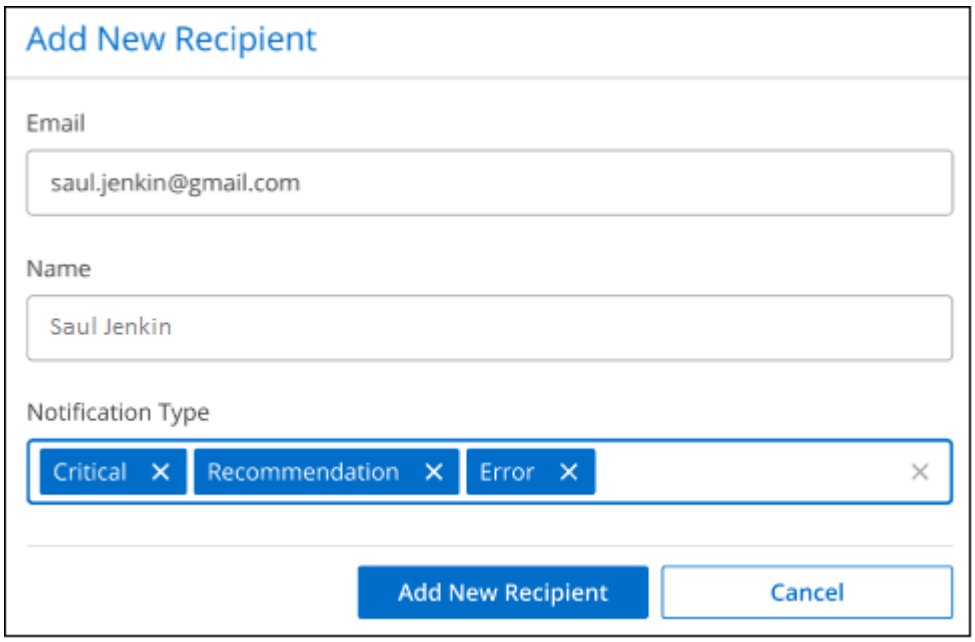
3. Wählen Sie einen oder mehrere Benutzer entweder auf der Seite „Benutzer der Organisation“ oder auf der Seite „Zusätzliche Empfänger“ aus und wählen Sie die Art der zu sendenden Benachrichtigungen:
   - Um Änderungen für einen einzelnen Benutzer vorzunehmen, wählen Sie das Menü in der Spalte „Benachrichtigungen“ für diesen Benutzer aus, überprüfen Sie die zu sendenden Benachrichtigungstypen und wählen Sie „Übernehmen“ aus.
   - Um Änderungen für mehrere Benutzer vorzunehmen, aktivieren Sie das Kontrollkästchen für jeden Benutzer, wählen Sie **E-Mail-Benachrichtigungen verwalten**, aktivieren Sie die zu sendenden Benachrichtigungstypen und wählen Sie **Übernehmen**.

Zusätzliche E-Mail-Empfänger hinzufügen

Die Benutzer, die auf der Seite „Benutzer der Organisation“ angezeigt werden, werden automatisch aus den Benutzern Ihrer Organisation oder Ihres Kontos gefüllt. Sie können auf der Seite „Zusätzliche Empfänger“ E-Mail-Adressen für andere Personen oder Gruppen hinzufügen, die keinen Zugriff auf die Konsole haben, aber über bestimmte Arten von Warnungen und Benachrichtigungen benachrichtigt werden müssen.

Schritte

1. Wählen Sie auf der Seite **Benachrichtigungseinstellungen** die Option **Neue Empfänger hinzufügen** aus.



2. Geben Sie den Namen und die E-Mail-Adresse ein, wählen Sie die Benachrichtigungstypen aus, die der Empfänger erhalten soll, und wählen Sie **Neuen Empfänger hinzufügen**.

Referenz

Agenten-Wartungskonsole

Konsolen-Agent-Wartungskonsole

Sie können die Wartungskonsole des Konsolenagenten verwenden, um einen Konsolenagenten für die Verwendung eines transparenten Proxyservers zu konfigurieren.

Zugriff auf die Agenten-Wartungskonsole

Sie können vom Konsolenagent-Host aus auf die Wartungskonsole zugreifen. Navigieren Sie zum folgenden Verzeichnis:

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

Transparente Proxy-Befehle

Die Agenten-Wartungskonsole bietet Befehle zum Konfigurieren des Agenten für die Verwendung eines transparenten Proxyservers.

Aktuelle transparente Proxy-Konfiguration anzeigen

Um die aktuelle transparente Proxy-Konfiguration anzuzeigen, verwenden Sie den folgenden Befehl:

```
./agent-maint-console proxy get
```

Fügen Sie einen transparenten Proxyserver hinzu

Um einen transparenten Proxyserver hinzuzufügen, verwenden Sie den folgenden Befehl, wobei `/home/ubuntu/myCA1.pem` ist der Pfad zur Zertifikatsdatei für den Proxyserver. Die Zertifikatsdatei muss im PEM-Format vorliegen:

```
./agent-maint-console proxy add -c /home/ubuntu/myCA1.pem
```

Stellen Sie sicher, dass sich die Zertifikatsdatei im selben Verzeichnis wie der Befehl befindet, oder geben Sie den vollständigen Pfad zur Zertifikatsdatei an.

Aktualisieren des Zertifikats für einen transparenten Proxyserver

Um das Zertifikat für einen transparenten Proxyserver zu aktualisieren, verwenden Sie den folgenden Befehl, wobei `/home/ubuntu/myCA1.pem` ist der Pfad zur neuen Zertifikatsdatei für den Proxyserver. Die Zertifikatsdatei muss im PEM-Format vorliegen:

```
./agent-maint-console proxy update -c /home/ubuntu/myCA1.pem
```

Stellen Sie sicher, dass sich die Zertifikatsdatei im selben Verzeichnis wie der Befehl befindet, oder geben Sie den vollständigen Pfad zur Zertifikatsdatei an.

Entfernen eines transparenten Proxyservers

Um den transparenten Proxyserver zu entfernen, verwenden Sie den folgenden Befehl:

```
./agent-maint-console proxy remove
```

Hilfe zu jedem Befehl anzeigen

Um Hilfe zu einem Befehl anzuzeigen, fügen Sie an `--help` zum Befehl. Um beispielsweise Hilfe für die `proxy add` Befehl, verwenden Sie den folgenden Befehl:

```
./agent-maint-console proxy add --help
```

Berechtigungen

Berechtigungsübersicht für die NetApp Console

Um die Funktionen und Dienste der NetApp Console nutzen zu können, müssen Sie Berechtigungen erteilen, damit die Konsole Vorgänge in Ihrer Cloud-Umgebung ausführen kann. Verwenden Sie die Links auf dieser Seite, um schnell auf die Berechtigungen zuzugreifen, die Sie je nach Ihrem Ziel benötigen.

AWS-Berechtigungen

Die NetApp Console erfordert AWS-Berechtigungen für einen Konsolenagenten und für einzelne Dienste.

Konsolenagenten

Ziel	Beschreibung	Link
Bereitstellen eines Konsolenagenten über die Konsole	Der Benutzer, der einen Konsolenagenten aus der Konsole erstellt, benötigt bestimmte Berechtigungen, um die Instanz in AWS bereitzustellen.	"AWS-Berechtigungen einrichten"
Berechtigungen für einen Konsolenagenten bereitstellen	Wenn die Konsole einen Konsolenagenten bereitstellt, fügt sie der Instanz eine Richtlinie hinzu, die die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen in Ihrem AWS-Konto bereitstellt. Sie müssen die Richtlinie selbst einrichten, wenn Sie einen Konsolen-Agenten vom AWS Marketplace bereitstellen, wenn Sie einen Konsolen-Agenten manuell installieren oder wenn Sie"Fügen Sie einem Konsolenagenten weitere AWS-Anmeldeinformationen hinzu" . Sie müssen außerdem sicherstellen, dass die Richtlinie auf dem neuesten Stand ist, da in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden.	"AWS-Berechtigungen für einen Konsolenagenten"

NetApp Backup and Recovery

Ziel	Beschreibung	Link
Sichern Sie lokale ONTAP -Cluster mit NetApp Backup and Recovery auf Amazon S3	Beim Aktivieren von Backups auf Ihren ONTAP Volumes werden Sie von NetApp Backup and Recovery aufgefordert, einen Zugriffsschlüssel und ein Geheimnis für einen IAM-Benutzer mit bestimmten Berechtigungen einzugeben.	"S3-Berechtigungen für Backups einrichten"

Cloud Volumes ONTAP

Ziel	Beschreibung	Link
Berechtigungen für Cloud Volumes ONTAP -Knoten bereitstellen	Jedem Cloud Volumes ONTAP Knoten in AWS muss eine IAM-Rolle zugeordnet werden. Dasselbe gilt für den HA-Mediator. Die Standardoption besteht darin, die IAM-Rollen von der Konsole erstellen zu lassen. Sie können jedoch auch Ihre eigenen Rollen verwenden, wenn Sie das System in der Konsole erstellen.	"Erfahren Sie, wie Sie die IAM-Rollen selbst einrichten"

NetApp Copy and Sync

Ziel	Beschreibung	Link
Bereitstellen des Datenbrokers in AWS	Das AWS-Benutzerkonto, das Sie zum Bereitstellen des Datenbrokers verwenden, muss über bestimmte Berechtigungen verfügen.	"Erforderliche Berechtigungen zum Bereitstellen des Datenbrokers in AWS"
Berechtigungen für den Datenbroker bereitstellen	Wenn NetApp Copy and Sync den Datenbroker bereitstellt, wird eine IAM-Rolle für die Datenbrokerinstanz erstellt. Sie können den Datenbroker bei Bedarf mit Ihrer eigenen IAM-Rolle bereitstellen.	"Voraussetzungen für die Nutzung einer eigenen IAM-Rolle beim AWS-Datenbroker"
Aktivieren Sie den AWS-Zugriff für einen manuell installierten Datenbroker	Wenn Sie den Datenbroker mit einer Synchronisierungsbeziehung verwenden, die einen S3-Bucket umfasst, sollten Sie den Linux-Host für den AWS-Zugriff vorbereiten. Wenn Sie den Datenbroker installieren, müssen Sie AWS-Schlüssel für einen IAM-Benutzer bereitstellen, der über programmgesteuerten Zugriff und bestimmte Berechtigungen verfügt.	"Aktivieren des Zugriffs auf AWS"

FSx für ONTAP

Ziel	Beschreibung	Link
Erstellen und verwalten Sie FSx für ONTAP	Um ein Amazon FSx for NetApp ONTAP System zu erstellen oder zu verwalten, müssen Sie der Konsole AWS-Anmeldeinformationen hinzufügen, indem Sie die ARN einer IAM-Rolle angeben, die der Konsole die erforderlichen Berechtigungen erteilt.	"Erfahren Sie, wie Sie AWS-Anmeldeinformationen für FSx einrichten"

NetApp Cloud Tiering

Ziel	Beschreibung	Link
Tiering von lokalen ONTAP -Clustern auf Amazon S3	Wenn Sie NetApp Cloud Tiering für AWS aktivieren, fordert Sie der Assistent auf, einen Zugriffsschlüssel und einen geheimen Schlüssel einzugeben. Diese Anmeldeinformationen werden an den ONTAP Cluster weitergegeben, damit ONTAP Daten in den S3-Bucket einstufen kann.	"Einrichten von S3-Berechtigungen für das Tiering"

Azure-Berechtigungen

Die Konsole erfordert Azure-Berechtigungen für einen Konsolen-Agenten und für einzelne Dienste.

Konsolenagent

Ziel	Beschreibung	Link
Bereitstellen eines Konsolenagenten über die Konsole	Wenn Sie einen Konsolen-Agenten über die Konsole bereitstellen, müssen Sie ein Azure-Konto oder einen Dienstprinzipal verwenden, der über die Berechtigung zum Bereitstellen einer Konsolen-Agent-VM in Azure verfügt.	"Einrichten von Azure-Berechtigungen"
Berechtigungen für einen Konsolenagenten bereitstellen	Wenn die Konsole eine Konsolen-Agent-VM in Azure bereitstellt, erstellt sie eine benutzerdefinierte Rolle, die die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen innerhalb dieses Azure-Abonnements bereitstellt. Sie müssen die benutzerdefinierte Rolle selbst einrichten, wenn Sie einen Konsolen-Agenten vom Marktplatz aus starten, wenn Sie einen Konsolen-Agenten manuell installieren oder wenn Sie"Fügen Sie einem Konsolen-Agenten weitere Azure-Anmeldeinformationen hinzu" . Sie müssen außerdem sicherstellen, dass die Richtlinie auf dem neuesten Stand ist, da in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden.	"Azure-Berechtigungen für einen Konsolen-Agent"

NetApp Backup and Recovery

Ziel	Beschreibung	Link
Sichern Sie Cloud Volumes ONTAP im Azure Blob Storage	Wenn Sie NetApp Backup and Recovery zum Sichern von Cloud Volumes ONTAP verwenden, müssen Sie in den folgenden Szenarien einem Konsolenagenten Berechtigungen hinzufügen: • Sie möchten die Funktion „Suchen und Wiederherstellen“ verwenden • Sie möchten vom Kunden verwaltete Verschlüsselungsschlüssel (CMEK) verwenden	• "Sichern Sie Cloud Volumes ONTAP Daten mit Backup und Recovery im Azure Blob-Speicher"

Ziel	Beschreibung	Link
Sichern Sie lokale ONTAP -Cluster im Azure Blob Storage	Wenn Sie NetApp Backup and Recovery zum Sichern von ONTAP-Clustern vor Ort verwenden, müssen Sie einem Konsolenagenten Berechtigungen hinzufügen, um die Funktion „Suchen und Wiederherstellen“ verwenden zu können.	"Sichern Sie lokale ONTAP -Daten mit Backup und Recovery im Azure Blob-Speicher"

NetApp Kopieren und Synchronisieren

Ziel	Beschreibung	Link
Bereitstellen des Datenbrokers in Azure	Das Azure-Benutzerkonto, das Sie zum Bereitstellen des Datenbrokers verwenden, muss über die erforderlichen Berechtigungen verfügen.	"Erforderliche Berechtigungen zum Bereitstellen des Datenbrokers in Azure"

Google Cloud-Berechtigungen

Die Konsole erfordert Google Cloud-Berechtigungen für einen Konsolenagenten und für einzelne Dienste.

Konsolenagenten

Ziel	Beschreibung	Link
Bereitstellen eines Konsolenagenten über die Konsole	Der Google Cloud-Benutzer, der einen Konsolen-Agenten von der Konsole aus bereitstellt, benötigt bestimmte Berechtigungen, um einen Konsolen-Agenten in Google Cloud bereitzustellen.	"Richten Sie Berechtigungen zum Erstellen eines Konsolenagenten ein"
Berechtigungen für einen Konsolenagenten bereitstellen	Das Dienstkonto für eine VM-Instanz des Konsolenagenten muss über bestimmte Berechtigungen für den täglichen Betrieb verfügen. Sie müssen das Dienstkonto während der Bereitstellung mit einem Konsolenagenten verknüpfen. Sie müssen außerdem sicherstellen, dass die Richtlinie auf dem neuesten Stand ist, da in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden.	"Einrichten von Berechtigungen für einen Konsolenagenten"

NetApp Backup and Recovery

Ziel	Beschreibung	Link
Sichern Sie Cloud Volumes ONTAP in Google Cloud	Wenn Sie NetApp Backup and Recovery zum Sichern von Cloud Volumes ONTAP verwenden, müssen Sie in den folgenden Szenarien einem Konsolenagenten Berechtigungen hinzufügen: • Sie möchten die Funktion „Suchen und Wiederherstellen“ verwenden • Sie möchten vom Kunden verwaltete Verschlüsselungsschlüssel (CMEK) verwenden	• "Sichern Sie Cloud Volumes ONTAP Daten mit Backup und Recovery in Google Cloud Storage" • "Berechtigungen für CMEKs"

Ziel	Beschreibung	Link
Sichern Sie lokale ONTAP -Cluster in der Google Cloud	Wenn Sie NetApp Backup and Recovery zum Sichern von ONTAP-Clustern vor Ort verwenden, müssen Sie einem Konsolenagenten Berechtigungen hinzufügen, um die Funktion „Suchen und Wiederherstellen“ verwenden zu können.	"Sichern Sie lokale ONTAP -Daten mit Backup und Recovery in Google Cloud Storage"

NetApp Copy and Sync

Ziel	Beschreibung	Link
Bereitstellen des Datenbrokers in Google Cloud	Stellen Sie sicher, dass der Google Cloud-Benutzer, der den Datenbroker bereitstellt, über die erforderlichen Berechtigungen verfügt.	"Erforderliche Berechtigungen zum Bereitstellen des Datenbrokers in Google Cloud"
Aktivieren Sie den Google Cloud-Zugriff für einen manuell installierten Datenbroker	Wenn Sie den Datenbroker mit einer Synchronisierungsbeziehung verwenden möchten, die einen Google Cloud Storage-Bucket umfasst, sollten Sie den Linux-Host für den Google Cloud-Zugriff vorbereiten. Wenn Sie den Datenbroker installieren, müssen Sie einen Schlüssel für ein Dienstkonto mit bestimmten Berechtigungen angeben.	"Zugriff auf Google Cloud aktivieren"

StorageGRID Berechtigungen

Die Konsole benötigt StorageGRID -Berechtigungen für zwei Dienste.

NetApp Backup and Recovery

Ziel	Beschreibung	Link
Sichern Sie lokale ONTAP -Cluster auf StorageGRID	Wenn Sie StorageGRID als Sicherungsziel für ONTAP Cluster vorbereiten, werden Sie von NetApp Backup and Recovery aufgefordert, einen Zugriffsschlüssel und ein Geheimnis für einen IAM-Benutzer mit bestimmten Berechtigungen einzugeben.	"Bereiten Sie StorageGRID als Ihr Sicherungsziel vor"

NetApp Cloud Tiering

Ziel	Beschreibung	Link
Tiering von lokalen ONTAP -Clustern auf StorageGRID	Wenn Sie NetApp Cloud Tiering für StorageGRID einrichten, müssen Sie Cloud Tiering einen S3-Zugriffsschlüssel und einen geheimen Schlüssel bereitstellen. Beim Cloud-Tiering werden die Schlüssel für den Zugriff auf Ihre Buckets verwendet.	"Tiering für StorageGRID vorbereiten"

AWS-Berechtigungen für den Konsolenagenten

Wenn die NetApp Console eine Konsolen-Agent-Instanz in AWS startet, fügt sie der Instanz eine Richtlinie hinzu, die dem Agenten die Berechtigung zum Verwalten von Ressourcen und Prozessen innerhalb dieses AWS-Kontos erteilt. Der Agent verwendet die Berechtigungen, um API-Aufrufe an mehrere AWS-Dienste zu tätigen, darunter EC2,

S3, CloudFormation, IAM, den Key Management Service (KMS) und mehr.

IAM-Richtlinien

Die unten verfügbaren IAM-Richtlinien bieten die Berechtigungen, die ein Konsolenagent benötigt, um Ressourcen und Prozesse in Ihrer öffentlichen Cloud-Umgebung basierend auf Ihrer AWS-Region zu verwalten.

Beachten Sie Folgendes:

- Wenn Sie einen Konsolenagenten in einer Standard-AWS-Region direkt von der Konsole aus erstellen, wendet die Konsole automatisch Richtlinien auf den Agenten an.
- Sie müssen die Richtlinien selbst einrichten, wenn Sie den Agenten vom AWS Marketplace bereitstellen, wenn Sie den Agenten manuell auf einem Linux-Host installieren oder wenn Sie der Konsole zusätzliche AWS-Anmeldeinformationen hinzufügen möchten.
- In beiden Fällen müssen Sie sicherstellen, dass die Richtlinien auf dem neuesten Stand sind, da in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. Wenn neue Berechtigungen erforderlich sind, werden diese in den Versionshinweisen aufgeführt.
- Bei Bedarf können Sie die IAM-Richtlinien einschränken, indem Sie die IAM `Condition` Element. "AWS-Dokumentation: Bedingungselement"
- Schritt-für-Schritt-Anleitungen zur Verwendung dieser Richtlinien finden Sie auf den folgenden Seiten:
  - "Einrichten von Berechtigungen für eine AWS Marketplace-Bereitstellung"
  - "Einrichten von Berechtigungen für lokale Bereitstellungen"
  - "Berechtigungen für den eingeschränkten Modus einrichten"

Wählen Sie Ihre Region aus, um die erforderlichen Richtlinien anzuzeigen:

Standardregionen

Für Standardregionen sind die Berechtigungen auf zwei Richtlinien verteilt. Aufgrund einer maximalen Zeichengrößenbeschränkung für verwaltete Richtlinien in AWS sind zwei Richtlinien erforderlich.

Richtlinie Nr. 1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DescribeTags",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:CreatePlacementGroup",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
```

```
                "ec2:UnassignPrivateIpAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteRoute",
                "ec2:DeletePlacementGroup",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumesModifications",
                "ec2:ModifyVolume",
                "cloudformation:CreateStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "cloudformation:DeleteStack",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:ListInstanceProfiles",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DeleteInstanceProfile",
                "iam:GetRolePolicy",
                "iam:GetRole",
                "sts:DecodeAuthorizationMessage",
                "sts:AssumeRole",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketPolicy",
                "s3:GetBucketAcl",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:PutObject",
                "s3:ListAllMyBuckets",
                "s3:GetObject",
```

```
                "s3:GetEncryptionConfiguration",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "fsx:Describe*",
                "fsx:List*",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "cvoServicePolicy"
        },
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "kms:List*",
                "kms:Describe*",
                "ec2:DescribeVpcEndpoints",
                "kms:ListAliases",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
```

```
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        },
        {
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:DeleteBucket",
                "s3:GetObjectVersionTagging",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObjectVersionTagging",
                "s3:PutObjectRetention",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
```

```
            ],
            "Effect": "Allow",
            "Sid": "backupS3Policy"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteBucket"
            ],
            "Resource": [
                "arn:aws:s3:::fabric-pool*"
            ],
            "Effect": "Allow",
            "Sid": "fabricPoolS3Policy"
        },
        {
            "Action": [
                "ec2:DescribeRegions"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "fabricPoolPolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/netapp-adc-manager": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
```

```
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:StopInstances",
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        }
    ]
```

```
}
```

Richtlinie Nr. 2

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "tag:getResources",
                "tag:getTagKeys",
                "tag:getTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "tagServicePolicy"
        }
    ]
}
```

GovCloud (USA)-Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListInstanceProfiles",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "ec2:ModifyVolumeAttribute",
                "sts:DecodeAuthorizationMessage",
                "ec2:DescribeImages",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstances",
                "iam:PassRole",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
```

```
                "ec2:DescribeSnapshots",
                "ec2:StopInstances",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:CreateBucket",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
```

```
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::fabric-pool*"
            ]
        },
        {
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::netapp-backup-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
```

```
                "arn:aws-us-gov:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Streng geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

So werden die AWS-Berechtigungen verwendet

In den folgenden Abschnitten wird beschrieben, wie die Berechtigungen für die einzelnen NetApp Console -Verwaltungs- oder Datendienste verwendet werden. Diese Informationen können hilfreich sein, wenn Ihre Unternehmensrichtlinien vorschreiben, dass Berechtigungen nur bei Bedarf erteilt werden.

Amazon FSx für ONTAP

Der Konsolenagent stellt die folgenden API-Anfragen, um ein Amazon FSx for ONTAP Dateisystem zu verwalten:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribute
- ec2:DescribeRouteTables
- ec2:DescribeImages
- ec2:CreateTags
- ec2:DescribeVolumes
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkInterfaces

- ec2:DescribeSubnets
- ec2:Vpcs beschreiben
- ec2:DescribeDhcpOptions
- ec2:DescribeSnapshots
- ec2:DescribeKeyPairs
- ec2:DescribeRegions
- ec2:DescribeTags
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeReservedInstancesOfferings
- ec2:DescribeVpcEndpoints
- ec2:Vpcs beschreiben
- ec2:DescribeVolumesModifications
- ec2:DescribePlacementGroups
- km:Liste*
- km:Beschreiben*
- kms:CreateGrant
- kms:ListAliases
- fsx:Beschreiben*
- fsx:Liste*

Amazon S3 Bucket-Erkennung

Der Konsolenagent stellt die folgende API-Anfrage, um Amazon S3-Buckets zu ermitteln:

s3:GetEncryptionConfiguration

NetApp Backup and Recovery

Der Agent stellt die folgenden API-Anfragen, um Backups in Amazon S3 zu verwalten:

- s3:GetBucketLocation
- s3:ListeAlleMeineBuckets
- s3:ListBucket
- s3:Bucket erstellen
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- km:Liste*

- km:Beschreiben*
- s3:GetObject
- ec2:DescribeVpcEndpoints
- kms:ListAliases
- s3:PutEncryptionConfiguration

Der Agent stellt die folgenden API-Anfragen, wenn Sie die Methode „Suchen und Wiederherstellen“ zum Wiederherstellen von Volumes und Dateien verwenden:

- s3:Bucket erstellen
- s3:Objekt löschen
- s3:DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMultipartUpload
- s3:ListMultipartUploadParts
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- Kleber: Datenbank erstellen
- Kleber: Tabelle erstellen
- Kleber: BatchDeletePartition

Der Agent stellt die folgenden API-Anfragen, wenn Sie DataLock und NetApp Ransomware Resilience für Ihre Volume-Backups verwenden:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:Objekt löschen
- s3:DeleteObjectTagging
- s3:GetObjectRetention

- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:ListBucketByTags
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Der Agent stellt die folgenden API-Anfragen, wenn Sie für Ihre Cloud Volumes ONTAP -Backups ein anderes AWS-Konto verwenden als für die Quellvolumes:

- s3:PutBucketPolicy
- s3:PutBucketOwnershipControls

Einstufung

Der Agent stellt die folgenden API-Anfragen, um NetApp Data Classification bereitzustellen:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:CreateTags
- ec2:CreateVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2:DeleteSecurityGroup
- ec2:DescribeSecurityGroups

- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface
- ec2:DescribeSubnets
- ec2:Vpcs beschreiben
- ec2:CreateSnapshot
- ec2:DescribeRegions
- Cloudformation:CreateStack
- Cloudformation:DeleteStack
- Cloudformation:DescribeStacks
- Cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

Der Agent stellt die folgenden API-Anfragen, um S3-Buckets zu scannen, wenn Sie NetApp Data Classification verwenden:

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:ListeAlleMeineBuckets
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3:Objekt löschen
- s3:DeleteObjectVersion
- s3:PutObject
- sts:Rolle übernehmen

Cloud Volumes ONTAP

Der Agent stellt die folgenden API-Anfragen, um Cloud Volumes ONTAP in AWS bereitzustellen und zu verwalten.

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und verwalten Sie IAM-Rollen und Instanzprofile für Cloud Volumes ONTAP -Instanzen	iam:ListInstanceProfiles	Ja	Ja	Nein
	iam:CreateRole	Ja	Nein	Nein
	iam:DeleteRole	Nein	Ja	Ja
	iam:PutRolePolicy	Ja	Nein	Nein
	iam:CreateInstanceProfile	Ja	Nein	Nein
	iam:DeleteRolePolicy	Nein	Ja	Ja
	iam:AddRoleToInstanceProfile	Ja	Nein	Nein
	iam:RemoveRoleFromInstanceProfile	Nein	Ja	Ja
	iam:DeleteInstanceProfile	Nein	Ja	Ja
	iam:PassRole	Ja	Nein	Nein
	ec2:AssociateIamInstanceProfile	Ja	Ja	Nein
	ec2:DescribeIamInstanceProfileAssociations	Ja	Ja	Nein
	ec2:DisassociateIamInstanceProfile	Nein	Ja	Nein
Dekodieren von Autorisierungsstatusmeldungen	sts:DecodeAuthorizationMessage	Ja	Ja	Nein
Beschreiben Sie die angegebenen Bilder (AMIs), die für das Konto verfügbar sind	ec2:DescribeImages	Ja	Ja	Nein
Beschreiben Sie die Routentabellen in einer VPC (nur für HA-Paare erforderlich)	ec2:DescribeRouteTables	Ja	Nein	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Stoppen, Starten und Überwachen von Instanzen	ec2:StartInstances	Ja	Ja	Nein
	ec2:StopInstances	Ja	Ja	Nein
	ec2:DescribeInstances	Ja	Ja	Nein
	ec2:DescribeInstanceStatus	Ja	Ja	Nein
	ec2:RunInstances	Ja	Nein	Nein
	ec2:TerminateInstances	Nein	Nein	Ja
	ec2:ModifyInstanceAttribute	Nein	Ja	Nein
Überprüfen Sie, ob Enhanced Networking für unterstützte Instance-Typen aktiviert ist.	ec2:DescribeInstanceAttribute	Nein	Ja	Nein
Kennzeichnen Sie Ressourcen mit den Tags „WorkingEnvironment“ und „WorkingEnvironmentId“, die für die Wartung und Kostenzuordnung verwendet werden	ec2:CreateTags	Ja	Ja	Nein
Verwalten Sie EBS-Volumes, die Cloud Volumes ONTAP als Back-End-Speicher verwendet	ec2:CreateVolume	Ja	Ja	Nein
	ec2:DescribeVolumes	Ja	Ja	Ja
	ec2:ModifyVolumeAttribute	Nein	Ja	Ja
	ec2:AttachVolume	Ja	Ja	Nein
	ec2:DeleteVolume	Nein	Ja	Ja
	ec2:DetachVolume	Nein	Ja	Ja

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und verwalten Sie Sicherheitsgruppen für Cloud Volumes ONTAP	ec2:CreateSecurityGroup	Ja	Nein	Nein
	ec2:DeleteSecurityGroup	Nein	Ja	Ja
	ec2:DescribeSecurityGroups	Ja	Ja	Ja
	ec2:RevokeSecurityGroupEgress	Ja	Nein	Nein
	ec2:AuthorizeSecurityGroupEgress	Ja	Nein	Nein
	ec2:AuthorizeSecurityGroupIngress	Ja	Nein	Nein
	ec2:RevokeSecurityGroupIngress	Ja	Ja	Nein
Erstellen und Verwalten von Netzwerkschnittstellen für Cloud Volumes ONTAP im Zielsubnetz	ec2:CreateNetworkInterface	Ja	Nein	Nein
	ec2:DescribeNetworkInterfaces	Ja	Ja	Nein
	ec2:DeleteNetworkInterface	Nein	Ja	Ja
	ec2:ModifyNetworkInterfaceAttribute	Nein	Ja	Nein
Abrufen der Liste der Zielsubnetze und Sicherheitsgruppen	ec2:DescribeSubnets	Ja	Ja	Nein
	ec2:Vpcs beschreiben	Ja	Ja	Nein
DNS-Server und den Standarddomänennamen für Cloud Volumes ONTAP -Instanzen abrufen	ec2:DescribeDhcpOptions	Ja	Nein	Nein
Erstellen Sie Snapshots von EBS-Volumes für Cloud Volumes ONTAP	ec2:CreateSnapshot	Ja	Ja	Nein
	ec2:DeleteSnapshot	Nein	Ja	Ja
	ec2:DescribeSnapshots	Nein	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erfassen Sie die Cloud Volumes ONTAP Konsole, die an AutoSupport -Nachrichten angehängt ist	ec2:GetConsoleOutput	Ja	Ja	Nein
Holen Sie sich die Liste der verfügbaren Schlüsselpaare	ec2:DescribeKeyPairs	Ja	Nein	Nein
Holen Sie sich die Liste der verfügbaren AWS-Regionen	ec2:DescribeRegions	Ja	Ja	Nein
Verwalten von Tags für Ressourcen, die mit Cloud Volumes ONTAP -Instanzen verknüpft sind	ec2:DeleteTags	Nein	Ja	Ja
	ec2:DescribeTags	Nein	Ja	Nein
Erstellen und Verwalten von Stacks für AWS CloudFormation-Vorlagen	Cloudformation:CreateStack	Ja	Nein	Nein
	Cloudformation:DeleteStack	Ja	Nein	Nein
	Cloudformation:DescribeStacks	Ja	Ja	Nein
	Cloudformation:DescribeStackEvents	Ja	Nein	Nein
	Cloudformation:ValidateTemplate	Ja	Nein	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und verwalten Sie einen S3-Bucket, den ein Cloud Volumes ONTAP System als Kapazitätsebene für das Daten-Tiering verwendet.	s3:Bucket erstellen	Ja	Ja	Nein
	s3:Bucket löschen	Nein	Ja	Ja
	s3:GetLifecycleConfiguration	Nein	Ja	Nein
	s3:PutLifecycleConfiguration	Nein	Ja	Nein
	s3:PutBucketTagging	Nein	Ja	Nein
	s3:ListBucketVersions	Nein	Ja	Nein
	s3:GetBucketPolicyStatus	Nein	Ja	Nein
	s3:GetBucketPublicAccessBlock	Nein	Ja	Nein
	s3:GetBucketAcl	Nein	Ja	Nein
	s3:GetBucketPolicy	Nein	Ja	Nein
	s3:PutBucketPublicAccessBlock	Nein	Ja	Nein
	s3:GetBucketTagging	Nein	Ja	Nein
	s3:GetBucketLocation	Nein	Ja	Nein
	s3:ListeAlleMeineBuckets	Nein	Nein	Nein
	s3:ListBucket	Nein	Ja	Nein
Aktivieren Sie die Datenverschlüsselung von Cloud Volumes ONTAP mithilfe des AWS Key Management Service (KMS).	km:Liste*	Ja	Ja	Nein
	kms:Neuverschlüsseln*	Ja	Nein	Nein
	km:Beschreiben*	Ja	Ja	Nein
	kms:CreateGrant	Ja	Ja	Nein
	kms:GenerateDataKeyWithoutPlaintext	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und verwalten Sie eine AWS-Spread-Placement-Gruppe für zwei HA-Knoten und den Mediator in einer einzigen AWS-Verfügbarkeitszone	ec2:CreatePlacementGroup	Ja	Nein	Nein
	ec2:DeletePlacementGroup	Nein	Ja	Ja
Erstellen von Berichten	fsx:Beschreiben*	Nein	Ja	Nein
	fsx:Liste*	Nein	Ja	Nein
Erstellen und verwalten Sie Aggregate, die die Funktion „Amazon EBS Elastic Volumes“ unterstützen	ec2:DescribeVolumesModifications	Nein	Ja	Nein
	ec2:ModifyVolume	Nein	Ja	Nein
Überprüfen Sie, ob die Availability Zone eine lokale AWS-Zone ist und ob alle Bereitstellungsparameter kompatibel sind.	ec2:DescribeAvailabilityZones	Ja	Nein	Ja

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt oder entfernt werden, vermerken wir dies in den folgenden Abschnitten.

9. September 2024

Berechtigungen wurden aus Richtlinie Nr. 2 für Standardregionen entfernt, da die NetApp Console NetApp -Edge-Caching sowie die Erkennung und Verwaltung von Kubernetes-Clustern nicht mehr unterstützt.

Anzeigen der Berechtigungen, die aus der Richtlinie entfernt wurden

```
        {
            "Action": [
                "ec2:DescribeRegions",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "iam:GetInstanceProfile"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "K8sServicePolicy"
        },
        {
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudwatch:GetMetricStatistics",
                "cloudformation:ListStacks"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "GFCservicePolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GFCInstance": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
```

9. Mai 2024

Für Cloud Volumes ONTAP sind jetzt die folgenden Berechtigungen erforderlich:

ec2:DescribeAvailabilityZones

6. Juni 2023

Für Cloud Volumes ONTAP ist jetzt die folgende Berechtigung erforderlich:

kms:GenerateDataKeyWithoutPlaintext

14. Februar 2023

Für NetApp Cloud Tiering ist nun folgende Berechtigung erforderlich:

ec2:DescribeVpcEndpoints

Azure-Berechtigungen für den Konsolen-Agent

Wenn die NetApp Console einen Konsolenagenten in Azure startet, weist sie der VM eine benutzerdefinierte Rolle zu, die dem Agenten die Berechtigung zum Verwalten von Ressourcen und Prozessen innerhalb dieses Azure-Abonnements erteilt. Der Agent verwendet die Berechtigungen, um API-Aufrufe an mehrere Azure-Dienste zu tätigen.

Ob Sie diese benutzerdefinierte Rolle für den Agenten erstellen müssen, hängt davon ab, wie Sie sie bereitgestellt haben.

Bereitstellen über die NetApp Console

Wenn Sie die Konsole verwenden, um die Agent-VM in Azure bereitzustellen, ermöglicht dies eine "systemseitig zugewiesene verwaltete Identität" auf der virtuellen Maschine, erstellt eine benutzerdefinierte Rolle und weist sie der virtuellen Maschine zu. Die Rolle stellt der Konsole die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen innerhalb dieses Azure-Abonnements zur Verfügung. Die Berechtigungen der Rolle werden beim Upgrade des Agenten auf dem neuesten Stand gehalten. Sie müssen diese Rolle für den Agenten nicht erstellen oder Updates verwalten.

Manuelle Bereitstellung oder Bereitstellung über den Azure Marketplace

Wenn Sie den Agenten vom Azure Marketplace bereitstellen oder den Agenten manuell auf einem Linux-Host installieren, müssen Sie die benutzerdefinierte Rolle selbst einrichten und ihre Berechtigungen bei allen Änderungen beibehalten.

Sie müssen sicherstellen, dass die Rolle auf dem neuesten Stand ist, da in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. Wenn neue Berechtigungen erforderlich sind, werden diese in den Versionshinweisen aufgeführt.

- Schritt-für-Schritt-Anleitungen zur Verwendung dieser Richtlinien finden Sie auf den folgenden Seiten:
  - "Einrichten von Berechtigungen für eine Azure Marketplace-Bereitstellung"
  - "Einrichten von Berechtigungen für lokale Bereitstellungen"
  - "Berechtigungen für den eingeschränkten Modus einrichten"

```
{
    "Name": "Console Operator",
    "Actions": [
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Compute/disks/read",
```

```
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Compute/locations/operations/read",
                    "Microsoft.Compute/locations/vmSizes/read",
                    "Microsoft.Resources/subscriptions/locations/read",
                    "Microsoft.Compute/operations/read",
                    "Microsoft.Compute/virtualMachines/instanceView/read",
                    "Microsoft.Compute/virtualMachines/powerOff/action",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/restart/action",
                    "Microsoft.Compute/virtualMachines/deallocate/action",
                    "Microsoft.Compute/virtualMachines/start/action",
                    "Microsoft.Compute/virtualMachines/vmSizes/read",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/images/read",
                    "Microsoft.Network/locations/operationResults/read",
                    "Microsoft.Network/locations/operations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Resources/deployments/operations/read",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Resources/deployments/write",
                    "Microsoft.Resources/resources/read",

"Microsoft.Resources/subscriptions/operationresults/read",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
```

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
                    "Microsoft.Storage/checknameavailability/read",
                    "Microsoft.Storage/operations/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/read",
                    "Microsoft.Storage/storageAccounts/delete",
                    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/usages/read",
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Compute/availabilitySets/write",
                    "Microsoft.Compute/availabilitySets/read",
                    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
                    "Microsoft.Network/loadBalancers/read",
                    "Microsoft.Network/loadBalancers/write",
                    "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
                    "Microsoft.Network/loadBalancers/probes/read",
                    "Microsoft.Network/loadBalancers/probes/join/action",
                    "Microsoft.Authorization/locks/*",
                    "Microsoft.Network/routeTables/join/action",
                    "Microsoft.NetApp/netAppAccounts/read",
                    "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
                    "Microsoft.Network/privateEndpoints/write",
```

```
"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",

"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
                    "Microsoft.Network/privateEndpoints/read",
                    "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
                    "Microsoft.Network/virtualNetworks/join/action",
                    "Microsoft.Network/privateDnsZones/A/write",
                    "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Insights/Metrics/Read",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Compute/virtualMachines/extensions/delete",
                    "Microsoft.Compute/virtualMachines/extensions/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/networkSecurityGroups/delete",
                    "Microsoft.Resources/deployments/delete",
                    "Microsoft.Compute/diskEncryptionSets/read",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Network/privateEndpoints/delete",
                    "Microsoft.Compute/availabilitySets/delete",
                    "Microsoft.KeyVault/vaults/read",
                    "Microsoft.KeyVault/vaults/accessPolicies/write",
                    "Microsoft.Compute/diskEncryptionSets/write",
                    "Microsoft.KeyVault/vaults/deploy/action",
                    "Microsoft.Compute/diskEncryptionSets/delete",
                    "Microsoft.Resources/tags/read",
                    "Microsoft.Resources/tags/write",
                    "Microsoft.Resources/tags/delete",
                    "Microsoft.Network/applicationSecurityGroups/write",
                    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",
                    "Microsoft.Network/applicationSecurityGroups/delete",
```

```
"Microsoft.Network/networkSecurityGroups/securityRules/delete",
                    "Microsoft.Synapse/workspaces/write",
                    "Microsoft.Synapse/workspaces/read",
                    "Microsoft.Synapse/workspaces/delete",
                    "Microsoft.Synapse/register/action",
                    "Microsoft.Synapse/checkNameAvailability/action",
                    "Microsoft.Synapse/workspaces/operationStatuses/read",
                    "Microsoft.Synapse/workspaces/firewallRules/read",

"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
                    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.Compute/images/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
                    "Microsoft.Compute/virtualMachineScaleSets/write",
                    "Microsoft.Compute/virtualMachineScaleSets/read",
                    "Microsoft.Compute/virtualMachineScaleSets/delete"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Console Permissions",
    "IsCustom": "true"
}
```

So werden Azure-Berechtigungen verwendet

In den folgenden Abschnitten wird beschrieben, wie die Berechtigungen für jedes NetApp -Speichersystem und jeden Datendienst verwendet werden. Diese Informationen können hilfreich sein, wenn Ihre Unternehmensrichtlinien vorschreiben, dass Berechtigungen nur bei Bedarf erteilt werden.

Azure NetApp Files

Der Agent stellt die folgenden API-Anforderungen, wenn Sie die NetApp Data Classification zum Scannen von Azure NetApp Files -Daten verwenden:

- NetApp/netAppAccounts/read
- NetApp/netAppAccounts/capacityPools/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/delete

NetApp Backup and Recovery

Der Konsolenagent stellt die folgenden API-Anfragen für NetApp Backup and Recovery:

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.KeyVault/vaults/read
- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Authorization/locks/*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/write
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/read
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/deployments/delete
- Microsoft.ManagedIdentity/userAssignedIdentities/assign/action

Der Agent stellt die folgenden API-Anfragen, wenn Sie die Such- und Wiederherstellungsfunktion verwenden:

- Microsoft.Synapse/workspaces/write
- Microsoft.Synapse/workspaces/read
- Microsoft.Synapse/workspaces/delete
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameAvailability/action
- Microsoft.Synapse/workspaces/operationStatuses/read
- Microsoft.Synapse/workspaces/firewallRules/read

- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft.Synapse/workspaces/operationResults/read
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

NetApp Data Classification

Der Agent stellt die folgenden API-Anfragen, wenn Sie die Datenklassifizierung verwenden.

Aktion	Für die Einrichtung verwendet?	Wird es für den täglichen Betrieb verwendet?
Microsoft.Compute/Standorte/Operationen/Lesen	Ja	Ja
Microsoft.Compute/locations/vmSizes/read	Ja	Ja
Microsoft.Compute/operations/read	Ja	Ja
Microsoft.Compute/virtualMachines/instanceView/read	Ja	Ja
Microsoft.Compute/virtualMachines/powerOff/action	Ja	Nein
Microsoft.Compute/virtualMachines/read	Ja	Ja
Microsoft.Compute/virtualMachines/restart/action	Ja	Nein
Microsoft.Compute/virtualMachines/start/action	Ja	Nein
Microsoft.Compute/virtualMachines/vmSizes/read	Nein	Ja
Microsoft.Compute/virtualMachines/write	Ja	Nein
Microsoft.Compute/images/read	Ja	Ja
Microsoft.Compute/disks/delete	Ja	Nein
Microsoft.Compute/disks/read	Ja	Ja
Microsoft.Compute/disks/write	Ja	Nein
Microsoft.Storage/checknameavailability/read	Ja	Ja
Microsoft.Storage/operations/read	Ja	Ja
Microsoft.Storage/storageAccounts/listkeys/action	Ja	Nein
Microsoft.Storage/storageAccounts/read	Ja	Ja
Microsoft.Storage/storageAccounts/write	Ja	Nein

Aktion	Für die Einrichtung verwendet?	Wird es für den täglichen Betrieb verwendet?
Microsoft.Storage/storageAccounts/blobServices/containers/read	Ja	Ja
Microsoft.Network/networkInterfaces/read	Ja	Ja
Microsoft.Network/networkInterfaces/write	Ja	Nein
Microsoft.Network/networkInterfaces/join/action	Ja	Nein
Microsoft.Network/networkSecurityGroups/read	Ja	Ja
Microsoft.Network/networkSecurityGroups/write	Ja	Nein
Microsoft.Resources/subscriptions/locations/read	Ja	Ja
Microsoft.Network/locations/operationResults/read	Ja	Ja
Microsoft.Network/locations/operations/read	Ja	Ja
Microsoft.Network/virtualNetworks/read	Ja	Ja
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Ja	Ja
Microsoft.Network/virtualNetworks/subnets/read	Ja	Ja
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Ja	Ja
Microsoft.Network/virtualNetworks/virtualMachines/read	Ja	Ja
Microsoft.Network/virtualNetworks/subnets/join/action	Ja	Nein
Microsoft.Network/virtualNetworks/subnets/write	Ja	Nein
Microsoft.Network/routeTables/join/action	Ja	Nein
Microsoft.Resources/deployments/operations/read	Ja	Ja
Microsoft.Resources/deployments/read	Ja	Ja
Microsoft.Resources/deployments/write	Ja	Nein

Aktion	Für die Einrichtung verwendet?	Wird es für den täglichen Betrieb verwendet?
Microsoft.Resources/resources/read	Ja	Ja
Microsoft.Resources/subscriptions/operationresults/read	Ja	Ja
Microsoft.Resources/subscriptions/resourceGroups/delete	Ja	Nein
Microsoft.Resources/subscriptions/resourceGroups/read	Ja	Ja
Microsoft.Resources/subscriptions/resourcegroups/resources/read	Ja	Ja
Microsoft.Resources/subscriptions/resourceGroups/write	Ja	Nein

Cloud Volumes ONTAP

Der Agent stellt die folgenden API-Anfragen, um Cloud Volumes ONTAP in Azure bereitzustellen und zu verwalten.

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Verwalten von VMs	Microsoft.Compute/Standorte/Operationen/Lesen	Ja	Ja	Nein
	Microsoft.Compute/locations/vmSizes/read	Ja	Ja	Nein
	Microsoft.Resources/subscriptions/locations/read	Ja	Nein	Nein
	Microsoft.Compute/operations/read	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/instanceView/read	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/powerOff/action	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/read	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/restart/action	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/start/action	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/deallocate/action	Nein	Ja	Ja
	Microsoft.Compute/virtualMachines/vmSizes/read	Nein	Ja	Nein
	Microsoft.Compute/virtualMachines/write	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/delete	Ja	Ja	Ja
	Microsoft.Resources/deployments/delete	Ja	Nein	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Aktivieren der Bereitstellung von einer VHD	Microsoft.Compute/images/read	Ja	Nein	Nein
	Microsoft.Compute/images/write	Ja	Nein	Nein
Erstellen und Verwalten von Netzwerkschnittstellen im Zielsubnetz	Microsoft.Network/networkInterfaces/read	Ja	Ja	Nein
	Microsoft.Network/networkInterfaces/write	Ja	Ja	Nein
	Microsoft.Network/networkInterfaces/join/action	Ja	Ja	Nein
	Microsoft.Network/networkInterfaces/delete	Ja	Ja	Nein
Erstellen und Verwalten von Netzwerksicherheitsgruppen	Microsoft.Network/networkSecurityGroups/read	Ja	Ja	Nein
	Microsoft.Network/networkSecurityGroups/write	Ja	Ja	Nein
	Microsoft.Network/networkSecurityGroups/join/action	Ja	Nein	Nein
	Microsoft.Network/networkSecurityGroups/delete	Nein	Ja	Ja

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Abrufen von Netzwerkinformationen zu Regionen, dem Ziel-VNet und Subnetz und Hinzufügen der VMs zu VNets	Microsoft.Network/locations/operationResults/read	Ja	Ja	Nein
	Microsoft.Network/locations/operations/read	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/read	Ja	Nein	Nein
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Ja	Nein	Nein
	Microsoft.Network/virtualNetworks/subnets/read	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/virtualMachines/read	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/subnets/join/action	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Verwalten von Ressourcengruppen	Microsoft.Resources /deployments/operations/read	Ja	Ja	Nein
	Microsoft.Resources /deployments/read	Ja	Ja	Nein
	Microsoft.Resources /deployments/write	Ja	Ja	Nein
	Microsoft.Resources /resources/read	Ja	Ja	Nein
	Microsoft.Resources /subscriptions/operationresults/read	Ja	Ja	Nein
	Microsoft.Resources /subscriptions/resourceGroups/delete	Ja	Ja	Ja
	Microsoft.Resources /subscriptions/resourceGroups/read	Nein	Ja	Nein
	Microsoft.Resources /subscriptions/resourcegroups/resources/read	Ja	Ja	Nein
	Microsoft.Resources /subscriptions/resourceGroups/write	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Verwalten von Azure-Speicherkonten und -Datenträgern	Microsoft.Compute/disks/read	Ja	Ja	Ja
	Microsoft.Compute/disks/write	Ja	Ja	Nein
	Microsoft.Compute/disks/delete	Ja	Ja	Ja
	Microsoft.Storage/checknameavailability/read	Ja	Ja	Nein
	Microsoft.Storage/operations/read	Ja	Ja	Nein
	Microsoft.Storage/storageAccounts/listkeys/action	Ja	Ja	Nein
	Microsoft.Storage/storageAccounts/read	Ja	Ja	Nein
	Microsoft.Storage/storageAccounts/delete	Nein	Ja	Ja
	Microsoft.Storage/storageAccounts/write	Ja	Ja	Nein
	Microsoft.Storage/usages/read	Nein	Ja	Nein
Aktivieren Sie Sicherungen im Blob-Speicher und die Verschlüsselung von Speicherkonten	Microsoft.Storage/storageAccounts/blobServices/containers/read	Ja	Ja	Nein
	Microsoft.KeyVault/vaults/read	Ja	Ja	Nein
	Microsoft.KeyVault/vaults/accessPolicies/write	Ja	Ja	Nein
Aktivieren von VNet-Dienstendpunkten für Datentiering	Microsoft.Network/virtualNetworks/subnets/write	Ja	Ja	Nein
	Microsoft.Network/routeTables/join/action	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Verwalten von Azure-verwalteten Snapshots	Microsoft.Compute/Snapshots/Schreiben	Ja	Ja	Nein
	Microsoft.Compute/snapshots/read	Ja	Ja	Nein
	Microsoft.Compute/snapshots/delete	Nein	Ja	Ja
	Microsoft.Compute/disks/beginGetAccess/action	Nein	Ja	Nein
Erstellen und Verwalten von Verfügbarkeitsgruppen	Microsoft.Compute/availabilitySets/write	Ja	Nein	Nein
	Microsoft.Compute/availabilitySets/read	Ja	Nein	Nein
Aktivieren Sie programmgesteuerte Bereitstellungen vom Marktplatz aus	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read	Ja	Nein	Nein
	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Verwalten eines Load Balancers für HA-Paare	Microsoft.Network/loadBalancers/read	Ja	Ja	Nein
	Microsoft.Network/loadBalancers/write	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/delete	Nein	Ja	Ja
	Microsoft.Network/loadBalancers/backendAddressPools/read	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	Ja	Ja	Nein
	Microsoft.Network/loadBalancers/loadBalancingRules/read	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/probes/read	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/probes/join/action	Ja	Nein	Nein
Aktivieren der Sperrverwaltung auf Azure-Datenträgern	Microsoft.Authorization/locks/*	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Aktivieren Sie private Endpunkte für HA-Paare, wenn außerhalb des Subnetzes keine Konnektivität besteht.	Microsoft.Network/privateEndpoints/write	Ja	Ja	Nein
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	Ja	Nein	Nein
	Microsoft.Storage/storageAccounts/privateEndpointConnections/read	Ja	Ja	Ja
	Microsoft.Network/privateEndpoints/read	Ja	Ja	Ja
	Microsoft.Network/privateDnsZones/write	Ja	Ja	Nein
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/join/action	Ja	Ja	Nein
	Microsoft.Network/privateDnsZones/A/write	Ja	Ja	Nein
	Microsoft.Network/privateDnsZones/read	Ja	Ja	Nein
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	Ja	Ja	Nein
Erforderlich für einige VM-Bereitstellungen, abhängig von der zugrunde liegenden physischen Hardware	Microsoft.Resources/deployments/operationStatuses/read	Ja	Ja	Nein
Entfernen Sie Ressourcen aus einer Ressourcengruppe, falls die Bereitstellung fehlschlägt oder gelöscht wird	Microsoft.Network/privateEndpoints/delete	Ja	Ja	Nein
	Microsoft.Compute/availabilitySets/delete	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Aktivieren Sie die Verwendung von vom Kunden verwalteten Verschlüsselungsschlüsseln bei der Verwendung der API	Microsoft.Compute/diskEncryptionSets/read	Ja	Ja	Ja
	Microsoft.Compute/diskEncryptionSets/write	Ja	Ja	Nein
	Microsoft.KeyVault/vaults/deploy/action	Ja	Nein	Nein
	Microsoft.Compute/diskEncryptionSets/delete	Ja	Ja	Ja
Konfigurieren Sie eine Anwendungssicherheitsgruppe für ein HA-Paar, um die HA-Verbindung und die Cluster-Netzwerk-NICs zu isolieren.	Microsoft.Network/applicationSecurityGroups/write	Nein	Ja	Nein
	Microsoft.Network/applicationSecurityGroups/read	Nein	Ja	Nein
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	Nein	Ja	Nein
	Microsoft.Network/networkSecurityGroups/securityRules/write	Ja	Ja	Nein
	Microsoft.Network/applicationSecurityGroups/delete	Nein	Ja	Ja
	Microsoft.Network/networkSecurityGroups/securityRules/delete	Nein	Ja	Ja
Mit Cloud Volumes ONTAP -Ressourcen verknüpfte Tags lesen, schreiben und löschen	Microsoft.Resources/tags/read	Nein	Ja	Nein
	Microsoft.Resources/tags/write	Ja	Ja	Nein
	Microsoft.Resources/tags/delete	Ja	Nein	Nein
Verschlüsseln von Speicherkonten während der Erstellung	Microsoft.ManagedIdentity/userAssignedIdentities/assign/action	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Verwenden Sie Virtual Machine Scale Sets im flexiblen Orchestrierungsmodus, um bestimmte Zonen für Cloud Volumes ONTAP anzugeben	Microsoft.Compute/virtualMachineScaleSets/write	Ja	Nein	Nein
	Microsoft.Compute/virtualMachineScaleSets/read	Ja	Nein	Nein
	Microsoft.Compute/virtualMachineScaleSets/delete	Nein	Nein	Ja

Abstufung

Der Agent stellt die folgenden API-Anfragen, wenn Sie NetApp Cloud Tiering einrichten.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/locations/read

Der Konsolenagent stellt für den täglichen Betrieb die folgenden API-Anfragen.

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Storage/storageAccounts/read

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt oder entfernt werden, vermerken wir dies in den folgenden Abschnitten.

9. September 2024

Die folgenden Berechtigungen wurden aus der JSON-Richtlinie entfernt, da die Konsole die Erkennung und Verwaltung von Kubernetes-Clustern nicht mehr unterstützt:

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/action
- Microsoft.ContainerService/managedClusters/read

22. August 2024

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt, da sie für die Cloud Volumes ONTAP Unterstützung von Virtual Machine Scale Sets erforderlich sind:

- Microsoft.Compute/virtualMachineScaleSets/write
- Microsoft.Compute/virtualMachineScaleSets/read
- Microsoft.Compute/virtualMachineScaleSets/delete

5. Dezember 2023

Die folgenden Berechtigungen werden für NetApp Backup and Recovery beim Sichern von Volumedaten im Azure Blob-Speicher nicht mehr benötigt:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete

Diese Berechtigungen sind für andere Konsolenspeicherdienste erforderlich, sodass sie weiterhin in der benutzerdefinierten Rolle für den Agenten verbleiben, wenn Sie diese anderen Speicherdienste verwenden.

12. Mai 2023

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt, da sie für die Verwaltung von Cloud Volumes ONTAP erforderlich sind:

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read

Die folgenden Berechtigungen wurden aus der JSON-Richtlinie entfernt, da sie nicht mehr benötigt werden:

- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.Network/publicIPAddresses/delete

23. März 2023

Die Berechtigung „Microsoft.Storage/storageAccounts/delete“ wird für die Datenklassifizierung nicht mehr benötigt.

Diese Berechtigung ist für Cloud Volumes ONTAP weiterhin erforderlich.

5. Januar 2023

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt:

- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

  Diese Berechtigungen sind für NetApp Backup and Recovery erforderlich.

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

  Diese Berechtigung ist für die Bereitstellung von Cloud Volumes ONTAP erforderlich.

Google Cloud-Berechtigungen für den Konsolenagenten

Die NetApp Console benötigt Berechtigungen zum Ausführen von Aktionen in Google Cloud. Diese Berechtigungen sind in einer benutzerdefinierten Rolle enthalten, die von

NetApp bereitgestellt wird. Sie sollten verstehen, was der Agent mit diesen Berechtigungen macht.

Dienstkontoberechtigungen

Die unten gezeigte benutzerdefinierte Rolle bietet die Berechtigungen, die ein Konsolenagent zum Verwalten von Ressourcen und Prozessen in Ihrem Google Cloud-Netzwerk benötigt.

Sie müssen diese benutzerdefinierte Rolle auf ein Dienstkonto anwenden, das an die Konsolen-Agent-VM angehängt wird.

- "Google Cloud-Berechtigungen für den Standardmodus einrichten"
- "Berechtigungen für den eingeschränkten Modus einrichten"

Sie müssen außerdem sicherstellen, dass die Rolle auf dem neuesten Stand ist, da in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. Wenn neue Berechtigungen erforderlich sind, werden diese in den Versionshinweisen aufgeführt.

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
```

```
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
```

```
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
```

So werden Google Cloud-Berechtigungen verwendet

Aktionen	Zweck
- compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	Zum Erstellen und Verwalten von Festplatten für Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	So erstellen Sie Firewall-Regeln für Cloud Volumes ONTAP.
- compute.globalOperations.get	Um den Status von Vorgängen abzurufen.
- compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	Um Bilder für VM-Instanzen zu erhalten.
- compute.instances.attachDisk - compute.instances.detachDisk	So schließen Sie Festplatten an Cloud Volumes ONTAP an und trennen sie davon.

Aktionen	Zweck
- compute.instances.create - compute.instances.delete	Zum Erstellen und Löschen von Cloud Volumes ONTAP VM-Instanzen.
- compute.instances.get	Zum Auflisten von VM-Instanzen.
- compute.instances.getSerialPortOutput	Um Konsolenprotokolle zu erhalten.
- compute.instances.list	Zum Abrufen der Liste der Instanzen in einer Zone.
- compute.instances.setDeletionProtection	Um den Löschschutz für die Instanz festzulegen.
- compute.instances.setLabels	Um Beschriftungen hinzuzufügen.
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	So ändern Sie den Maschinentyp für Cloud Volumes ONTAP.
- compute.instances.setMetadata	Um Metadaten hinzuzufügen.
- compute.instances.setTags	So fügen Sie Tags für Firewall-Regeln hinzu.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	So starten und stoppen Sie Cloud Volumes ONTAP.
- compute.machineTypes.get	Um die Anzahl der Kerne zu ermitteln und die Quoten zu überprüfen.
- compute.projects.get	Zur Unterstützung mehrerer Projekte.
- compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels	Zum Erstellen und Verwalten persistenter Festplatten-Snapshots.
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get - compute.zones.get - compute.zones.list	Um die Netzwerkinformationen zu erhalten, die zum Erstellen einer neuen Cloud Volumes ONTAP VM-Instanz erforderlich sind.
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifests.list - deploymentmanager.operations.get - deploymentmanager.operations.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.types.get - deploymentmanager.types.list	So stellen Sie die Cloud Volumes ONTAP VM-Instanz mithilfe von Google Cloud Deployment Manager bereit.
- logging.logEntries.list - logging.privateLogEntries.list	Um Stack-Log-Laufwerke zu erhalten.
- resourcemanager.projects.get	Zur Unterstützung mehrerer Projekte.

Aktionen	Zweck
- storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update	So erstellen und verwalten Sie einen Google Cloud Storage-Bucket für die Datenschichtung.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyRings.list	So verwenden Sie vom Kunden verwaltete Verschlüsselungsschlüssel vom Cloud Key Management Service mit Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects.get - storage.objects.list	So richten Sie ein Dienstkonto auf der Cloud Volumes ONTAP -Instanz ein. Dieses Dienstkonto bietet Berechtigungen für die Datenschichtung in einem Google Cloud Storage-Bucket.
- compute.addresses.list	Zum Abrufen der Adressen in einer Region beim Bereitstellen eines HA-Paares.
- compute.backendServices.create - compute.regionBackendServices.create - compute.regionBackendServices.get - compute.regionBackendServices.list	So konfigurieren Sie einen Backend-Dienst zum Verteilen des Datenverkehrs in einem HA-Paar.
- compute.networks.updatePolicy	So wenden Sie Firewall-Regeln auf die VPCs und Subnetze für ein HA-Paar an.
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	So aktivieren Sie die NetApp Data Classification.
- compute.instanceGroups.get - compute.addresses.get - compute.instances.updateNetworkInterface	Zum Erstellen und Verwalten von Speicher-VMs auf Cloud Volumes ONTAP HA-Paaren.
- monitoring.timeSeries.list - storage.buckets.getIamPolicy	Um Informationen zu Google Cloud Storage-Buckets zu erhalten.
- cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.getIamPolicy - cloudkms.cryptoKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudkms.keyRings.get - cloudkms.keyRings.getIamPolicy - cloudkms.keyRings.list - cloudkms.keyRings.setIamPolicy	So wählen Sie im Aktivierungsassistenten von NetApp Backup and Recovery Ihre eigenen, vom Kunden verwalteten Schlüssel aus, anstatt die standardmäßigen, von Google verwalteten Verschlüsselungsschlüssel zu verwenden.

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt oder entfernt werden, vermerken wir dies in den folgenden Abschnitten.

06.02.2023

Die folgende Berechtigung wurde dieser Richtlinie hinzugefügt:

- compute.instances.updateNetworkInterface

Diese Berechtigung ist für Cloud Volumes ONTAP erforderlich.

27.01.2023

Die folgenden Berechtigungen wurden der Richtlinie hinzugefügt:

- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

Diese Berechtigungen sind für NetApp Backup and Recovery erforderlich.

Häfen

Sicherheitsgruppenregeln für Konsolenagenten in AWS

Die AWS-Sicherheitsgruppe für den Agenten erfordert sowohl eingehende als auch ausgehende Regeln. Die NetApp Console erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Konsolenagenten von der Konsole aus erstellen. Sie müssen diese Sicherheitsgruppe für alle anderen Installationsoptionen einrichten.

Eingehende Regeln

Protokoll	Hafen	Zweck
SSH	22	Bietet SSH-Zugriff auf den Agent-Host
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Upgrade-Prozesses von Cloud Volumes ONTAP verwendet
HTTPS	443	Bietet HTTPS-Zugriff auf die lokale Benutzeroberfläche und Verbindungen von der NetApp Data Classification Instanz
TCP	3128	Bietet Cloud Volumes ONTAP Internetzugang. Sie müssen diesen Port nach der Bereitstellung manuell öffnen.

Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den Agenten öffnet den gesamten ausgehenden Datenverkehr. Wenn das akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Nachrichten. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Ausgangsregeln.

Grundlegende Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den Agenten umfasst die folgenden ausgehenden Regeln.

Protokoll	Hafen	Zweck
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für den ausgehenden Verkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Agenten benötigt werden

Die Quell-IP-Adresse ist der Agent-Host.

Service	Protokoll	Hafen	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster-Management-LIF	API-Aufrufe an AWS, ONTAP, NetApp Data Classification und Senden von AutoSupport -Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP HA-Mediator	Kommunikation mit dem ONTAP HA Mediator
	TCP	8080	Datenklassifizierung	Testen der Datenklassifizierung sinstanz während der Bereitstellung
DNS	UDP	53	DNS	Wird von der Konsole für die DNS-Auflösung verwendet

Sicherheitsgruppenregeln für Konsolen-Agents in Azure

Die Azure-Sicherheitsgruppe für den Agenten erfordert sowohl eingehende als auch ausgehende Regeln. Die NetApp Console erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Konsolenagenten von der Konsole aus erstellen. Für andere Installationsoptionen müssen Sie diese Sicherheitsgruppe manuell einrichten.

Eingehende Regeln

Protokoll	Hafen	Zweck
SSH	22	Bietet SSH-Zugriff auf den Agent-Host
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Upgrade-Prozesses von Cloud Volumes ONTAP verwendet

Protokoll	Hafen	Zweck
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche und Verbindungen von der NetApp Data Classification -Instanz
TCP	3128	Bietet Cloud Volumes ONTAP Internetzugang, um AutoSupport Nachrichten an den NetApp Support zu senden. Sie müssen diesen Port nach der Bereitstellung manuell öffnen. "Erfahren Sie, wie der Agent als Proxy für AutoSupport -Nachrichten verwendet wird"

Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den Agenten öffnet den gesamten ausgehenden Datenverkehr. Wenn das akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Nachrichten. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Ausgangsregeln.

Grundlegende Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den Agenten umfasst die folgenden ausgehenden Regeln.

Protokoll	Hafen	Zweck
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für den ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Agenten erforderlich sind.

Die Quell-IP-Adresse ist der Agent-Host.

Service	Protokoll	Hafen	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster-Management-LIF	API-Aufrufe an Azure, an ONTAP, an NetApp Data Classification und Senden von AutoSupport -Nachrichten an NetApp

Service	Protokoll	Hafen	Ziel	Zweck
API-Aufrufe	TCP	8080	Datenklassifizierung	Testen der Datenklassifizierung sinstanz während der Bereitstellung
DNS	UDP	53	DNS	Wird von der Konsole für die DNS-Auflösung verwendet

Agent-Firewallregeln in Google Cloud

Die Google Cloud-Firewallregeln für den Agenten erfordern sowohl eingehende als auch ausgehende Regeln. Die NetApp Console erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Konsolenagenten aus der Konsole erstellen. Für andere Installationsoptionen müssen Sie diese Sicherheitsgruppe manuell einrichten.

Eingehende Regeln

Protokoll	Hafen	Zweck
SSH	22	Bietet SSH-Zugriff auf den Agent-Host
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Upgrade-Prozesses von Cloud Volumes ONTAP verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
TCP	3128	Bietet Cloud Volumes ONTAP Internetzugang. Sie müssen diesen Port nach der Bereitstellung manuell öffnen.

Ausgangsregeln

Die vordefinierten Firewall-Regeln des Agenten öffnen den gesamten ausgehenden Datenverkehr. Befolgen Sie die grundlegenden Ausgangsregeln, sofern dies akzeptabel ist, oder verwenden Sie erweiterte Ausgangsregeln für strengere Anforderungen.

Grundlegende Ausgangsregeln

Die vordefinierten Firewall-Regeln für den Agenten umfassen die folgenden ausgehenden Regeln.

Protokoll	Hafen	Zweck
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für den ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Agenten erforderlich sind.

Die Quell-IP-Adresse ist der Agent-Host.

Service	Protokoll	Hafen	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster-Management-LIF	API-Aufrufe an Google Cloud, an ONTAP, an NetApp Data Classification und Senden von AutoSupport -Nachrichten an NetApp
API-Aufrufe	TCP	8080	Datenklassifizierung	Testen der Datenklassifizierung sinstanz während der Bereitstellung
DNS	UDP	53	DNS	Wird für die DNS-Auflösung durch Datenklassifizierung verwendet

Ports für den lokalen Konsolenagenten

Der Konsolenagent verwendet *eingehende* Ports, wenn er manuell auf einem lokalen Linux-Host installiert wird. Beziehen Sie sich bei Planungen auf diese Häfen.

Diese eingehenden Regeln gelten für alle Bereitstellungsmodi der NetApp Console .

Protokoll	Hafen	Zweck
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Upgrade-Prozesses von Cloud Volumes ONTAP verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche

Erforderliche Netzwerkzugriffspunkte für 3.9.55 und darunter

In diesem Thema wird der Netzwerkzugriff beschrieben, der für Versionen des NetApp Console Standardmodus vor der Version 4.0.0 der NetApp Console, des NetApp Console Agenten und des ausgehenden Internetzugriffs der NetApp -Datendienste sowie die Möglichkeit zur Kontaktaufnahme mit den erforderlichen Endpunkten erforderlich ist. Sie müssen sicherstellen, dass die Konsole und alle von Ihnen installierten Agenten über den richtigen Netzwerkzugriff auf die Funktionseigenschaft verfügen.

Sie müssen den Netzwerkzugriff für Computer einrichten, die als Software as a Service (SaaS) auf die NetApp Console zugreifen, sowie für alle Konsolenagenten, die Sie vor Ort oder in der Cloud installieren. Möglicherweise benötigen Sie auch zusätzliche Endpunkte für bestimmte NetApp -Datendienste, einschließlich

Cloud Volumes ONTAP.

Aktualisieren Sie Ihre Endpunktliste auf die überarbeitete Liste für 4.0.0 und höher

Ab Version 4.0.0 benötigen Konsolenagenten weniger Endpunkte. Vorhandene Bereitstellungen vor 4.0.0 werden weiterhin unterstützt. Nach dem Upgrade auf 4.0.0 oder höher können Sie die alten Endpunkte bei Bedarf aus Ihrer Zulassungsliste entfernen.

NetApp empfiehlt, dass Sie Ihre Firewall-Regeln aktualisieren, um die überarbeitete Endpunktliste zu verwenden. Die überarbeitete Liste ist kleiner und somit sicherer und einfacher zu verwalten.

Rezension"unterstützte Endpunkte für 4.0.0 und höher"

Schritte

1. Whitelist der Endpunkte in"Unterstützte Endpunkte für 4.0.0 und höher" .
2. Starten Sie den Dienst „Service Manager 2“ auf jedem Agenten neu, indem Sie den folgenden Befehl ausführen:

```
systemctl restart netapp-service-manager.service
```

3. Führen Sie den folgenden Befehl aus und überprüfen Sie, ob der Status des Agenten als *aktiv (wird ausgeführt)* angezeigt wird: _

```
systemctl status netapp-service-manager.service
```

4. Entfernen Sie die alten Endpunkte aus Ihrer Zulassungsliste.

Von der NetApp Console kontaktierte Endpunkte

Jeder Computer, der auf die NetApp Console zugreift, muss über Verbindungen zu den unten aufgeführten Endpunkten verfügen.

Das System kontaktiert diese Endpunkte in zwei Szenarien:

- Von einem Computer aus, der auf die "NetApp Console" als Software as a Service (SaaS).
- Von einem Computer aus, der direkt auf einen Agentenhost zugreift, entweder um sich anzumelden und ihn einzurichten oder um vom Agentenhost aus auf die Konsole zuzugreifen.

Endpunkte	Zweck
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com	Um Funktionen und Dienste innerhalb der NetApp Console bereitzustellen.

Endpunkte	Zweck
Wählen Sie zwischen zwei Endpunktsätzen: • Option 1 (empfohlen) https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. NetApp empfiehlt, Endpunkte der Option 1 in Ihrer Firewall zuzulassen, da diese sicherer sind, und Endpunkte der Option 2 nicht zuzulassen, es sei denn, Sie verwenden Ransomware Resilience oder Backup and Recovery. Beachten Sie Folgendes zu diesen Endpunkten: • Endpunkte der Option 1 werden in 3.9.47 und höher unterstützt. Versionen vor 3.9.47 unterstützen keine Abwärtskompatibilität. • Der Konsolenagent initiiert zuerst den Kontakt mit den Endpunkten in Option 2. Wenn diese Endpunkte nicht erreichbar sind, werden automatisch die Endpunkte in Option 1 kontaktiert. • Wenn Sie den Konsolenagenten mit NetApp Backup and Recovery oder Ransomware Resilience verwenden, unterstützt das System keine Endpunkte der Option 1. Erlauben Sie Endpunkte der Option 2 und verbieten Sie Option 1.

Vom Konsolenagenten kontaktierte Endpunkte

Sie installieren den Konsolenagenten vor Ort oder in der Cloud und er kontaktiert Endpunkte, um von der Konsole initiierte Aktionen abzuschließen.

Konsolenagenten benötigen Zugriff auf dieselben Endpunkte wie die NetApp Console sowie auf zusätzliche Endpunkte, wenn Sie den Agenten bei Ihrem Cloud-Anbieter bereitstellen.

Agent-Endpunkte für AWS

Diese Endpunkte sind für Konsolenagenten vor 4.0.0 anwendbar.

Endpunkte	Zweck
AWS-Dienste (amazonaws.com): CloudFormation Elastic Compute Cloud (EC2) Identity and Access Management (IAM) Key Management Service (KMS) Security Token Service (STS) Simple Storage Service (S3)	Zum Verwalten von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. Weitere Informationen zum Abrufen von Lizenzinformationen und zum Senden von AutoSupport -Nachrichten an den NetApp Support finden Sie in der AWS-Dokumentation.
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.

Endpunkte	Zweck
Wählen Sie zwischen zwei Endpunktsätzen: • Option 1 (empfohlen) https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. NetApp empfiehlt, Endpunkte der Option 1 in Ihrer Firewall zuzulassen, da diese sicherer sind, und Endpunkte der Option 2 nicht zuzulassen, es sei denn, Sie verwenden Ransomware Resilience oder Backup and Recovery. Beachten Sie Folgendes zu diesen Endpunkten: • Endpunkte der Option 1 werden in 3.9.47 und höher unterstützt. Versionen vor 3.9.47 unterstützen keine Abwärtskompatibilität. • Der Konsolenagent initiiert zuerst den Kontakt mit den Endpunkten in Option 2. Wenn diese Endpunkte nicht erreichbar sind, werden automatisch die Endpunkte in Option 1 kontaktiert. • Wenn Sie den Konsolenagenten mit NetApp Backup and Recovery oder Ransomware Resilience verwenden, unterstützt das System keine Endpunkte der Option 1. Erlauben Sie Endpunkte der Option 2 und verbieten Sie Option 1.

Agent-Endpunkte für Azure

Diese Endpunkte gelten für Konsolenagenten vor 4.0.0.

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Zum Verwalten von Ressourcen in öffentlichen Azure-Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Zum Verwalten von Ressourcen in Azure China-Regionen.
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.

Endpunkte	Zweck
Wählen Sie zwischen zwei Endpunktsätzen: • Option 1 (empfohlen) https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. NetApp empfiehlt, Endpunkte der Option 1 in Ihrer Firewall zuzulassen, da diese sicherer sind, und Endpunkte der Option 2 nicht zuzulassen, es sei denn, Sie verwenden Ransomware Resilience oder Backup and Recovery. Beachten Sie Folgendes zu diesen Endpunkten: • Endpunkte der Option 1 werden in 3.9.47 und höher unterstützt. Versionen vor 3.9.47 unterstützen keine Abwärtskompatibilität. • Der Konsolenagent initiiert zuerst den Kontakt mit den Endpunkten in Option 2. Wenn diese Endpunkte nicht erreichbar sind, werden automatisch die Endpunkte in Option 1 kontaktiert. • Wenn Sie den Konsolenagenten mit NetApp Backup and Recovery oder Ransomware Resilience verwenden, unterstützt das System keine Endpunkte der Option 1. Erlauben Sie Endpunkte der Option 2 und verbieten Sie Option 1.

Agent-Endpunkte für Google Cloud

Diese Endpunkte gelten für Konsolenagenten vor 4.0.0.

Endpunkte	Zweck
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/project	Zum Verwalten von Ressourcen in Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport -Nachrichten an den NetApp Support zu senden.

Endpunkte	Zweck
Wählen Sie zwischen zwei Endpunktsätzen: • Option 1 (empfohlen) https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Um Bilder für Upgrades des Konsolenagenten zu erhalten. NetApp empfiehlt, Endpunkte der Option 1 in Ihrer Firewall zuzulassen, da diese sicherer sind, und Endpunkte der Option 2 nicht zuzulassen. Beachten Sie Folgendes zu diesen Endpunkten: • Ab der Version 3.9.47 des Konsolenagenten unterstützt das System die in Option 1 aufgeführten Endpunkte. Frühere Versionen des Konsolenagenten unterstützen keine Abwärtskompatibilität. • Der Konsolenagent kontaktiert die Endpunkte zuerst in Option 2. Wenn diese Endpunkte nicht erreichbar sind, werden automatisch die Endpunkte in Option 1 kontaktiert. • Wenn Sie den Konsolenagenten mit NetApp Backup and Recovery oder Ransomware Resilience verwenden, unterstützt das System keine Endpunkte der Option 1. Erlauben Sie Endpunkte der Option 2 und verbieten Sie Option 1.

Lokale Agent-Endpunkte

Wissen und Unterstützung

Für Support registrieren

Um technischen Support speziell für die NetApp Console und ihre Speicherlösungen und Datendienste zu erhalten, ist eine Support-Registrierung erforderlich. Eine Support-Registrierung ist auch erforderlich, um wichtige Workflows für Cloud Volumes ONTAP Systeme zu aktivieren.

Durch die Registrierung für den Support wird kein NetApp Support für den Dateidienst eines Cloud-Anbieters aktiviert. Technischen Support für den Dateidienst eines Cloud-Anbieters, seine Infrastruktur oder eine Lösung, die den Dienst nutzt, erhalten Sie unter „Hilfe erhalten“ in der Dokumentation des jeweiligen Produkts.

- "Amazon FSx für ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Übersicht zur Support-Registrierung

Zur Aktivierung des Supportanspruchs stehen zwei Registrierungsformen zur Verfügung:

- Registrieren Sie die Seriennummer Ihres NetApp Console (Ihre 20-stellige Seriennummer 960xxxxxxxx, die Sie auf der Seite „Supportressourcen“ in der Konsole finden).

  Dies dient als Ihre einzige Support-Abonnement-ID für alle Dienste innerhalb der Konsole. Jedes Konsolenkonto muss registriert werden.

- Registrieren Sie die mit einem Abonnement verknüpften Cloud Volumes ONTAP Seriennummern im Marktplatz Ihres Cloud-Anbieters (dies sind 20-stellige 909201xxxxxxxx-Seriennummern).

  Diese Seriennummern werden allgemein als *PAYGO-Seriennummern* bezeichnet und von der NetApp Console zum Zeitpunkt der Bereitstellung von Cloud Volumes ONTAP generiert.

Durch die Registrierung beider Seriennummerntypen werden Funktionen wie das Öffnen von Support-Tickets und die automatische Fallgenerierung ermöglicht. Die Registrierung wird abgeschlossen, indem Sie der Konsole NetApp Support Site (NSS)-Konten hinzufügen, wie unten beschrieben.

Registrieren Sie die NetApp Console für den NetApp Support

Um sich für den Support zu registrieren und den Supportanspruch zu aktivieren, muss ein Benutzer in Ihrem NetApp Console seinem Konsolen-Login ein NetApp Support-Site-Konto zuordnen. Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über ein NetApp Support Site (NSS)-Konto verfügen.

Bestandskunde mit NSS-Konto

Wenn Sie ein NetApp -Kunde mit einem NSS-Konto sind, müssen Sie sich lediglich über die Konsole für den Support registrieren.

Schritte

1. Wählen Sie **Administration** > **Anmeldeinformationen**.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wählen Sie **NSS-Anmeldeinformationen hinzufügen** und folgen Sie der Authentifizierungsaufforderung der NetApp Support Site (NSS).
4. Um zu bestätigen, dass der Registrierungsvorgang erfolgreich war, wählen Sie das Hilfesymbol und dann **Support**.

   Auf der Seite **Ressourcen** sollte angezeigt werden, dass Ihr Konsolenkonto für den Support registriert ist.

   Beachten Sie, dass anderen Konsolenbenutzern dieser Support-Registrierungsstatus nicht angezeigt wird, wenn sie ihrem Login kein NetApp Support Site-Konto zugeordnet haben. Dies bedeutet jedoch nicht, dass Ihr Konto nicht für den Support registriert ist. Sofern ein Benutzer in der Organisation diese Schritte befolgt hat, wurde Ihr Konto registriert.

Bestandskunde, aber kein NSS-Konto

Wenn Sie bereits NetApp -Kunde mit vorhandenen Lizenzen und Seriennummern, aber *keinem* NSS-Konto sind, müssen Sie ein NSS-Konto erstellen und es mit Ihrem Konsolen-Login verknüpfen.

Schritte

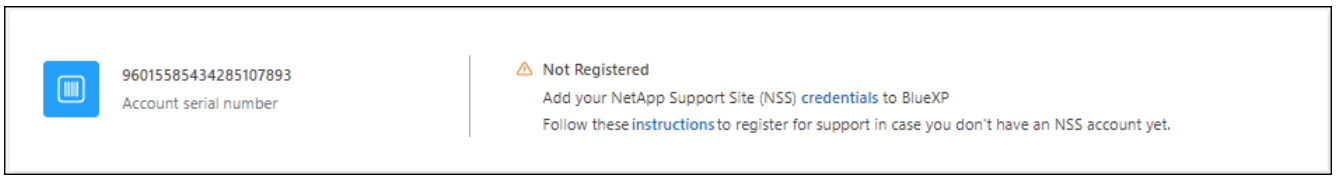
1. Erstellen Sie ein NetApp Support Site-Konto, indem Sie das "Registrierungsformular für Benutzer der NetApp Support-Site"
   a. Achten Sie darauf, die entsprechende Benutzerebene auszuwählen, in der Regel „NetApp -Kunde/Endbenutzer“.
   b. Denken Sie daran, die Seriennummer des Konsolenkontos (960xxxx) zu kopieren, die oben für das Feld „Seriennummer“ verwendet wurde. Dies beschleunigt die Kontobearbeitung.
2. Verknüpfen Sie Ihr neues NSS-Konto mit Ihrem Konsolen-Login, indem Sie die folgenden Schritte ausführenBestandskunde mit NSS-Konto .

Ganz neu bei NetApp

Wenn Sie NetApp noch nicht kennen und kein NSS-Konto haben, befolgen Sie die nachstehenden Schritte.

Schritte

1. Wählen Sie oben rechts in der Konsole das Hilfesymbol und dann **Support** aus.
2. Suchen Sie auf der Support-Registrierungsseite nach der Seriennummer Ihrer Konto-ID.



3. Navigieren Sie zu "Support-Registrierungssite von NetApp" und wählen Sie **Ich bin kein registrierter NetApp -Kunde**.
4. Füllen Sie die Pflichtfelder (mit roten Sternchen gekennzeichnet) aus.
5. Wählen Sie im Feld **Produktlinie Cloud Manager** und dann Ihren entsprechenden Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer Ihres Kontos aus Schritt 2 oben, schließen Sie die Sicherheitsüberprüfung

ab und bestätigen Sie anschließend, dass Sie die globale Datenschutzrichtlinie von NetApp gelesen haben.

Um diese sichere Transaktion abzuschließen, wird umgehend eine E-Mail an das angegebene Postfach gesendet. Überprüfen Sie unbedingt Ihren Spam-Ordner, wenn die Bestätigungs-E-Mail nicht innerhalb weniger Minuten eintrifft.

7. Bestätigen Sie die Aktion in der E-Mail.

   Durch die Bestätigung wird Ihre Anfrage an NetApp übermittelt und es wird empfohlen, dass Sie ein NetApp Support Site-Konto erstellen.

8. Erstellen Sie ein NetApp Support Site-Konto, indem Sie das "Registrierungsformular für Benutzer der NetApp Support-Site"
   a. Achten Sie darauf, die entsprechende Benutzerebene auszuwählen, in der Regel „NetApp -Kunde/Endbenutzer“.
   b. Denken Sie daran, die oben für das Seriennummernfeld verwendete Kontoseriennummer (960xxxx) zu kopieren. Dadurch wird die Bearbeitung beschleunigt.

Nach Abschluss

NetApp sollte sich während dieses Vorgangs mit Ihnen in Verbindung setzen. Dies ist eine einmalige Onboarding-Übung für neue Benutzer.

Sobald Sie über Ihr NetApp Support Site-Konto verfügen, verknüpfen Sie das Konto mit Ihrem Konsolen-Login, indem Sie die folgenden Schritte ausführenBestandskunde mit NSS-Konto .

NSS-Anmeldeinformationen für Cloud Volumes ONTAP Support zuordnen

Um die folgenden wichtigen Workflows für Cloud Volumes ONTAP zu aktivieren, müssen Sie Ihrem Konsolenkonto Anmeldeinformationen für die NetApp Support Site zuordnen:

- Registrieren von Pay-as-you-go Cloud Volumes ONTAP Systemen für den Support

  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.

- 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.

- Aktualisieren der Cloud Volumes ONTAP -Software auf die neueste Version

Die Zuordnung von NSS-Anmeldeinformationen zu Ihrem NetApp Console unterscheidet sich von der Zuordnung des NSS-Kontos zu einer Konsolenbenutzeranmeldung.

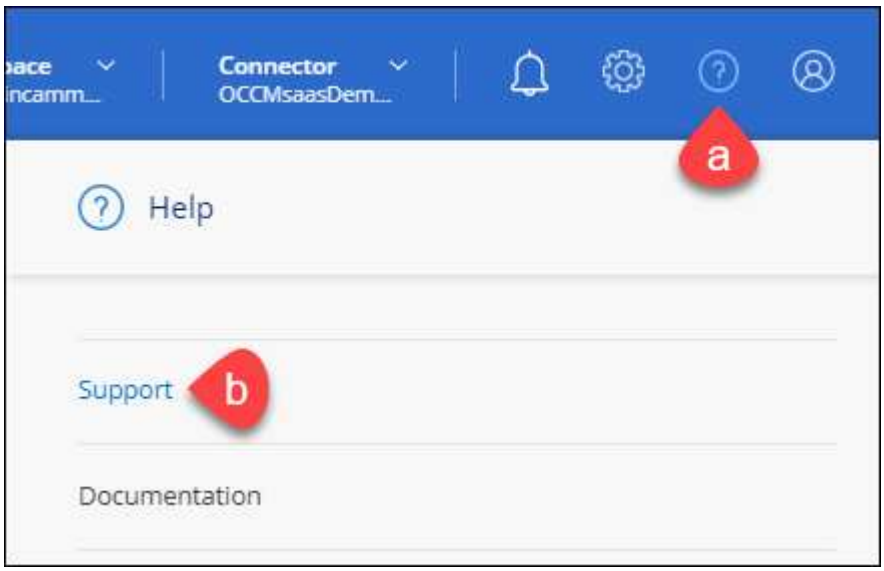
Diese NSS-Anmeldeinformationen sind mit Ihrer spezifischen Konsolenkonto-ID verknüpft. Benutzer, die zur Konsolenorganisation gehören, können über **Support > NSS-Verwaltung** auf diese Anmeldeinformationen zugreifen.

- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen.

- Wenn Sie über ein Partner- oder Reseller-Konto verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen, diese können jedoch nicht zusammen mit Konten auf Kundenebene hinzugefügt werden.

Schritte

1. Wählen Sie oben rechts in der Konsole das Hilfesymbol und dann **Support** aus.



2. Wählen Sie **NSS-Verwaltung > NSS-Konto hinzufügen**.
3. 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 speziell für Support und Lizenzierung.

4. Geben Sie auf der Anmeldeseite Ihre bei der NetApp Support Site registrierte E-Mail-Adresse und Ihr Kennwort ein, um den Authentifizierungsprozess durchzuführen.

   Diese Aktionen ermöglichen der Konsole, Ihr NSS-Konto für Dinge wie Lizenzdownloads, Überprüfung von Software-Upgrades und zukünftige Support-Registrierungen zu verwenden.

   Beachten Sie Folgendes:

   - Das NSS-Konto muss ein Konto auf Kundenebene sein (kein Gast- oder temporäres Konto). Sie können mehrere NSS-Konten auf Kundenebene haben.
   - Es kann nur ein NSS-Konto geben, wenn es sich bei diesem Konto um ein Konto auf Partnerebene handelt. Wenn Sie versuchen, NSS-Konten auf Kundenebene hinzuzufügen und ein Konto auf Partnerebene vorhanden ist, erhalten Sie die folgende Fehlermeldung:

     „Der NSS-Kundentyp ist für dieses Konto nicht zulässig, da bereits NSS-Benutzer eines anderen Typs vorhanden sind.“

   Dasselbe gilt, wenn Sie bereits über NSS-Konten auf Kundenebene verfügen und versuchen, ein Konto auf Partnerebene hinzuzufügen.

   - 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.

Hilfe erhalten

NetApp bietet auf vielfältige Weise Support für die NetApp Console und ihre Cloud-Dienste. Umfangreiche kostenlose Selbsthilfeoptionen stehen rund um die Uhr zur Verfügung, beispielsweise Knowledge Base-Artikel (KB) und ein Community-Forum. Ihre Support-Registrierung beinhaltet technischen Remote-Support per Web-Ticketing.

Erhalten Sie Unterstützung für den Dateidienst eines Cloud-Anbieters

Technischen Support zu einem Dateidienst eines Cloud-Anbieters, seiner Infrastruktur oder einer Lösung, die den Dienst nutzt, finden Sie in der Dokumentation zu diesem Produkt.

- "Amazon FSx für ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Um technischen Support speziell für NetApp und seine Speicherlösungen und Datendienste zu erhalten, verwenden Sie die unten beschriebenen Supportoptionen.

Nutzen Sie Möglichkeiten zur Selbsthilfe

Diese Optionen stehen Ihnen 24 Stunden am Tag, 7 Tage die Woche kostenlos zur Verfügung:

- Dokumentation

  Die NetApp Console Konsolendokumentation, die Sie gerade anzeigen.

- "Wissensdatenbank"

  Durchsuchen Sie die NetApp Wissensdatenbank nach hilfreichen Artikeln zur Problembehebung.

- "Gemeinschaften"

  Treten Sie der NetApp Console Community bei, um aktuelle Diskussionen zu verfolgen oder neue zu starten.

Erstellen Sie einen Fall mit dem NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie nach der Aktivierung des Supports mit einem NetApp -Support-Spezialisten zusammenarbeiten, um alle Probleme zu lösen.

Bevor Sie beginnen

- Um die Funktion **Fall erstellen** zu verwenden, müssen Sie zunächst Ihre Anmeldeinformationen für die NetApp -Support-Site mit Ihrem Konsolen-Login verknüpfen. "Erfahren Sie, wie Sie die mit Ihrer

Konsolenanmeldung verknüpften Anmeldeinformationen verwalten." .

- Wenn Sie einen Fall für ein ONTAP -System mit einer Seriennummer eröffnen, muss Ihr NSS-Konto mit der Seriennummer für dieses System verknüpft sein.

Schritte

1. Wählen Sie in der NetApp Console*Hilfe > Support*.
2. Wählen Sie auf der Seite **Ressourcen** unter „Technischer Support“ eine der verfügbaren Optionen aus:

   a. Wählen Sie **Rufen Sie uns an**, wenn Sie mit jemandem telefonieren möchten. Sie werden zu einer Seite auf netapp.com weitergeleitet, auf der die Telefonnummern aufgeführt sind, die Sie anrufen können.

   b. Wählen Sie **Fall erstellen**, um ein Ticket bei einem NetApp -Support-Spezialisten zu öffnen:

      - **Dienst**: Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispiel: * NetApp Console*, wenn es sich speziell um ein technisches Supportproblem mit Workflows oder Funktionen innerhalb der Konsole handelt.
      - **System**: Wählen Sie, falls für den Speicher zutreffend, * Cloud Volumes ONTAP* oder **On-Prem** und dann die zugehörige Arbeitsumgebung aus.

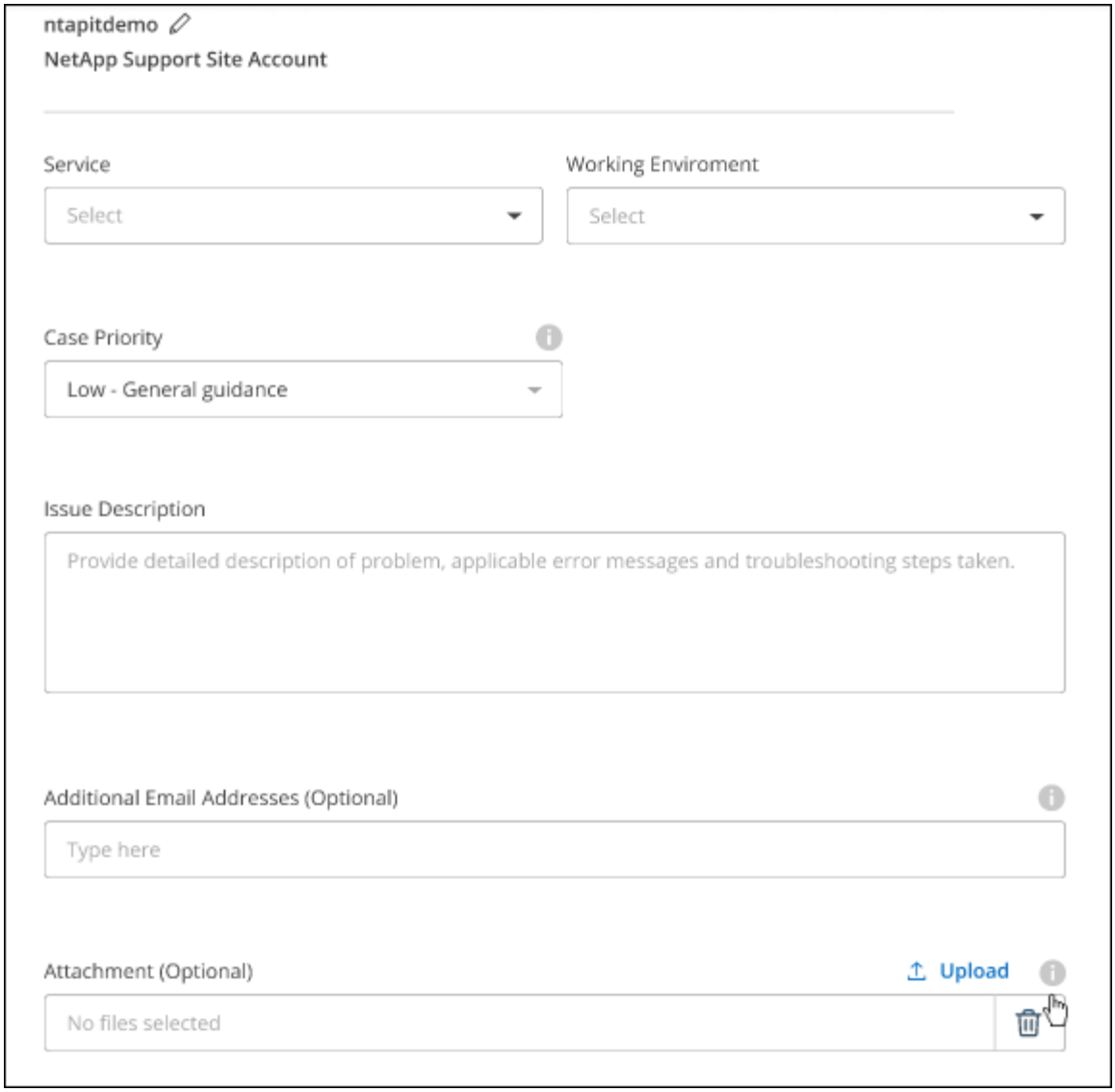
        Die Liste der Systeme liegt im Rahmen der Konsolenorganisation und des Konsolenagenten, den Sie im oberen Banner ausgewählt haben.

      - **Fallpriorität**: Wählen Sie die Priorität für den Fall. Sie kann „Niedrig“, „Mittel“, „Hoch“ oder „Kritisch“ sein.

        Um weitere Einzelheiten zu diesen Prioritäten zu erfahren, bewegen Sie die Maus über das Informationssymbol neben dem Feldnamen.

      - **Problembeschreibung**: Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller zutreffenden Fehlermeldungen oder Schritte zur Fehlerbehebung, die Sie durchgeführt haben.
      - **Zusätzliche E-Mail-Adressen**: Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderen auf dieses Problem aufmerksam machen möchten.
      - **Anhang (optional)**: Laden Sie bis zu fünf Anhänge hoch, einen nach dem anderen.

        Anhänge sind auf 25 MB pro Datei begrenzt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.



Nach Abschluss

Es erscheint ein Popup mit Ihrer Support-Fallnummer. Ein NetApp -Support-Spezialist wird Ihren Fall prüfen und sich in Kürze bei Ihnen melden.

Um einen Verlauf Ihrer Supportfälle anzuzeigen, können Sie **Einstellungen > Zeitleiste** auswählen und nach Aktionen mit der Bezeichnung „Supportfall erstellen“ suchen. Über eine Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Beim Versuch, einen Fall zu erstellen, kann es sein, dass die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Fall für den ausgewählten Dienst zu erstellen.“

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das damit verknüpfte Unternehmen nicht dasselbe Unternehmen sind, für das die Seriennummer des NetApp Console gilt (d. h. 960xxxx) oder die Seriennummer der Arbeitsumgebung. Sie können auf eine der folgenden Arten Hilfe anfordern:

- Senden Sie einen nicht-technischen Fall an https://mysupport.netapp.com/site/help

Verwalten Sie Ihre Supportfälle

Sie können aktive und gelöste Supportfälle direkt von der Konsole aus anzeigen und verwalten. Sie können die mit Ihrem NSS-Konto und Ihrem Unternehmen verknüpften Fälle verwalten.

Beachten Sie Folgendes:

- Das Fallmanagement-Dashboard oben auf der Seite bietet zwei Ansichten:
  - Die Ansicht links zeigt die Gesamtzahl der Fälle, die in den letzten drei Monaten von dem von Ihnen angegebenen NSS-Benutzerkonto eröffnet wurden.
  - Die Ansicht rechts zeigt die Gesamtzahl der in den letzten drei Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto.

  Die Ergebnisse in der Tabelle spiegeln die Fälle wider, die mit der von Ihnen ausgewählten Ansicht in Zusammenhang stehen.
- Sie können interessante Spalten hinzufügen oder entfernen und den Inhalt von Spalten wie „Priorität“ und „Status“ filtern. Andere Spalten bieten lediglich Sortierfunktionen.

  Weitere Einzelheiten finden Sie in den folgenden Schritten.
- Auf Einzelfallebene bieten wir die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Abgeschlossen“ oder „Ausstehend abgeschlossen“ befindet.

Schritte

1. Wählen Sie in der NetApp Console*Hilfe > Support*.
2. Wählen Sie **Fallmanagement** und fügen Sie bei entsprechender Aufforderung Ihr NSS-Konto zur Konsole hinzu.

   Auf der Seite **Fallverwaltung** werden offene Fälle angezeigt, die sich auf das NSS-Konto beziehen, das mit Ihrem Konsolenbenutzerkonto verknüpft ist. Dies ist dasselbe NSS-Konto, das oben auf der **NSS-Verwaltungsseite** angezeigt wird.
3. Ändern Sie optional die in der Tabelle angezeigten Informationen:
   - Wählen Sie unter **Fälle der Organisation** die Option **Anzeigen** aus, um alle mit Ihrem Unternehmen verknüpften Fälle anzuzeigen.
   - Ändern Sie den Datumsbereich, indem Sie einen genauen Datumsbereich oder einen anderen Zeitrahmen auswählen.
   - Filtern Sie den Inhalt der Spalten.
   - Ändern Sie die in der Tabelle angezeigten Spalten, indem Sie und wählen Sie dann die Spalten aus, die Sie anzeigen möchten.
4. Verwalten Sie einen vorhandenen Fall, indem Sie und wählen Sie eine der verfügbaren Optionen aus:
   - **Fall anzeigen**: Alle Details zu einem bestimmten Fall anzeigen.
   - **Fallnotizen aktualisieren**: Geben Sie zusätzliche Details zu Ihrem Problem an oder wählen Sie **Dateien hochladen**, um bis zu fünf Dateien anzuhängen.

     Anhänge sind auf 25 MB pro Datei begrenzt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.

- **Fall schließen**: Geben Sie Details zum Grund für das Schließen des Falls an und wählen Sie **Fall schließen** aus.

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der Patente im Besitz von NetApp finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

Hinweisdateien enthalten Informationen zu Urheberrechten und Lizenzen Dritter, die in der NetApp -Software verwendet werden.

"Hinweis zur NetApp Console"

Copyright-Informationen

Copyright © 2025 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.