Richten Sie einen Konnektor ein

Cloud Manager 3.8

NetApp
March 25, 2024

Inhalt

Richten Sie einen Konnektor ein

Erfahren Sie mehr über Steckverbinder

In den meisten Fällen muss ein Account-Administrator einen *Connector* in Ihrer Cloud oder Ihrem On-Premises-Netzwerk bereitstellen. Mit dem Connector kann Cloud Manager Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen.

Wenn ein Stecker erforderlich ist

Für die Nutzung der folgenden Funktionen in Cloud Manager ist ein Connector erforderlich:

- Cloud Volumes ONTAP
- On-Premises ONTAP Cluster
- Cloud-Compliance
- Kubernetes
- Backup in die Cloud
- Monitoring
- Lokales Tiering
- Globaler Datei-Cache
- Amazon S3 Bucket-Erkennung

Für Azure NetApp Files, Cloud Volumes Service oder Cloud Sync ist ein Stecker *_Not_ erforderlich.

Während kein Connector für die Einrichtung und das Management von Azure NetApp Files erforderlich ist, ist jedoch ein Connector erforderlich, wenn Sie Azure NetApp Files-Daten mithilfe von Cloud Compliance scannen möchten.

Unterstützte Standorte

Ein Connector wird an folgenden Stellen unterstützt:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- Vor Ort

Wenn Sie ein Cloud Volumes ONTAP-System in Google Cloud erstellen möchten, dann müssen Sie einen Connector in Google Cloud laufen, sowie. Sie können keinen Konnektor verwenden, der an einem anderen Standort ausgeführt wird.

Anschlüsse sollten weiterhin ausgeführt werden

Ein Steckverbinder sollte immer weiter laufen. Es ist wichtig für den fortwährenden Zustand und Betrieb der Services, die Sie ermöglichen.

Ein Connector ist beispielsweise eine wichtige Komponente im Zustand und Betrieb von Cloud Volumes ONTAP PAYGO-Systemen. Wenn ein Konnektor heruntergefahren wird, werden die Cloud Volumes ONTAP PAYGO-Systeme nach einem Verlust der Kommunikation mit einem Konnektor länger als 14 Tage heruntergefahren.

So erstellen Sie einen Konnektor

Ein Kontoadministrator muss einen Konnektor erstellen, bevor ein Workspace-Administrator eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen und eine der anderen oben aufgeführten Funktionen verwenden kann.

Ein Kontoadministrator kann auf verschiedene Arten einen Connector erstellen:

- Direkt über Cloud Manager (empfohlen)
  - "In AWS erstellen"
  - "In Azure erstellen"
  - "In GCP erstellen"
- "Über AWS Marketplace"
- "Über den Azure Marketplace"
- "Durch Herunterladen und Installieren der Software auf einem vorhandenen Linux-Host"

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector zu erstellen, falls noch kein Connector vorhanden ist.

Berechtigungen

Zur Erstellung des Connectors sind spezielle Berechtigungen erforderlich, und für die Instanz des Connectors selbst sind weitere Berechtigungen erforderlich.

Berechtigungen zum Erstellen eines Connectors

Der Benutzer, der einen Connector aus Cloud Manager erstellt, benötigt spezielle Berechtigungen, um die Instanz bei Ihrem bevorzugten Cloud-Provider bereitzustellen. Cloud Manager erinnert Sie an die Berechtigungsanforderungen bei der Erstellung eines Connectors.

"Zeigen Sie Richtlinien für jeden Cloud-Provider an".

Berechtigungen für die Connector-Instanz

Für die Ausführung von Vorgängen in Ihrem Auftrag benötigt der Connector spezielle Cloud-Provider-Berechtigungen. Beispiel für die Implementierung und das Management von Cloud Volumes ONTAP.

Wenn Sie einen Connector direkt aus Cloud Manager erstellen, erstellt Cloud Manager den Connector mit den entsprechenden Berechtigungen. Es gibt nichts, was Sie tun müssen.

Wenn Sie den Connector selbst über AWS Marketplace, Azure Marketplace oder die Software manuell installieren, müssen Sie sicherstellen, dass die entsprechenden Berechtigungen vorhanden sind.

"Zeigen Sie Richtlinien für jeden Cloud-Provider an".

Wann werden mehrere Anschlüsse verwendet

In einigen Fällen benötigen Sie möglicherweise nur einen Connector, aber Sie benötigen möglicherweise zwei oder mehr Anschlüsse.

Hier nur ein paar Beispiele:

- Sie nutzen eine Multi-Cloud-Umgebung (AWS und Azure), d. h. einen Connector in AWS und einen anderen in Azure. Jedes managt die Cloud Volumes ONTAP Systeme, die in diesen Umgebungen ausgeführt werden.
- Ein Service-Provider nutzt möglicherweise ein Cloud Central Konto, um seinen Kunden Services bereitzustellen, und nutzt ein anderes Konto, um eine seiner Geschäftsbereiche Disaster Recovery zu bieten. Jedes Konto hätte separate Anschlüsse.

Wann muss zwischen den Anschlüssen gewechselt werden

Wenn Sie Ihren ersten Connector erstellen, verwendet Cloud Manager diesen Connector automatisch für jede von Ihnen erstellte zusätzliche Arbeitsumgebung. Wenn Sie einen zusätzlichen Connector erstellen, müssen Sie zwischen diesen wechseln, um die für jeden Connector spezifischen Arbeitsumgebungen zu sehen.

"Erfahren Sie, wie Sie zwischen den Anschlüssen wechseln".

Die lokale Benutzeroberfläche

Während Sie fast alle Aufgaben aus dem ausführen sollten "SaaS-Benutzeroberfläche", Eine lokale Benutzeroberfläche ist weiterhin auf dem Connector verfügbar. Diese Schnittstelle wird für einige Aufgaben benötigt, die über den Connector selbst ausgeführt werden müssen:

- "Festlegen eines Proxyservers"
- Installation eines Patches (Sie arbeiten in der Regel mit NetApp Mitarbeitern zusammen, um einen Patch zu installieren)
- Herunterladen von AutoSupport-Meldungen (normalerweise gerichtet von NetApp Mitarbeitern, wenn Sie Probleme haben)

"Erfahren Sie, wie Sie auf die lokale Benutzeroberfläche zugreifen".

Connector-Upgrades

Der Connector aktualisiert seine Software automatisch auf die neueste Version, solange er hat "Outbound-Internetzugang" Um das Softwareupdate zu erhalten.

Netzwerkanforderungen für den Connector

Richten Sie Ihr Netzwerk ein, damit der Connector Ressourcen und Prozesse innerhalb Ihrer Public Cloud-Umgebung managen kann. Der wichtigste Schritt besteht darin, ausgehenden Internetzugriff auf verschiedene Endpunkte zu gewährleisten.

Wenn Ihr Netzwerk für die gesamte Kommunikation mit dem Internet einen Proxyserver verwendet, können Sie den Proxyserver über die Seite Einstellungen angeben. Siehe "Konfigurieren des Connectors für die Verwendung eines Proxy-Servers".

Verbindung zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu der Art der Arbeitsumgebung, die Sie erstellen und die Dienste, die Sie planen zu ermöglichen.

Wenn Sie beispielsweise einen Connector in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zur VPC oder vnet einrichten, in der Sie Cloud Volumes ONTAP starten.

Outbound-Internetzugang

Für den Connector ist ein abgehender Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung zu managen. Der ausgehende Internetzugang ist auch erforderlich, wenn Sie den Connector manuell auf einem Linux-Host installieren oder auf die lokale UI zugreifen möchten, die auf dem Connector ausgeführt wird.

In den folgenden Abschnitten werden die spezifischen Endpunkte beschrieben.

Endpunkte zum Management von Ressourcen in AWS

Ein Connector kontaktiert die folgenden Endpunkte beim Management von Ressourcen in AWS:

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3) Der genaue Endpunkt hängt von der Region ab, in der Sie Cloud Volumes ONTAP implementieren. "Weitere Informationen finden Sie in der AWS-Dokumentation."	Ermöglicht die Implementierung und das Management von Cloud Volumes ONTAP in AWS mit dem Connector
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://repo.cloud.support.netapp.com	Wird zum Herunterladen der Abhängigkeiten von Cloud Manager verwendet.
http://repo.mysql.com/	Zum Herunterladen von MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Ermöglicht dem Connector, auf Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images zuzugreifen und diese herunterzuladen.

Endpunkte	Zweck
https://cloudmanagerinfraprod.azurecr.io	Zugriff auf Software-Images von Container-Komponenten für eine Infrastruktur, die Docker ausführt und eine Lösung für die Service-Integration mit Cloud Manager bietet.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
https://netapp-cloud-account.auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Wird verwendet, um Ihre AWS Konto-ID der Liste der zugelassenen Benutzer für die Sicherung in S3 hinzuzufügen.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Kommunikation mit NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Kommunikation mit NetApp bei Systemlizenzrechten und Support-Registrierung
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Er ermöglicht NetApp, Informationen zu sammeln, die für die Behebung von Support-Problemen erforderlich sind.
https://ipa-signer.cloudmanager.netapp.com	Ermöglicht Cloud Manager die Generierung von Lizenzen (beispielsweise eine FlexCache Lizenz für Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden Mit den Endpunkten ist die Installation von NetApp Trident möglich.
Verschiedene Standorte von Drittanbietern, z. B.: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com An Standorten von Drittanbietern können Änderungen vorgenommen werden.	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

Endpunkte zum Managen von Ressourcen in Azure

Ein Connector kontaktiert folgende Endpunkte beim Managen von Ressourcen in Azure:

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den meisten Azure Regionen.
https://management.microsoftazure.de https://login.microsoftonline.de	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den Azure Germany Regionen.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den Azure US Gov Regionen.
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://repo.cloud.support.netapp.com	Wird zum Herunterladen der Abhängigkeiten von Cloud Manager verwendet.
http://repo.mysql.com/	Zum Herunterladen von MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Ermöglicht dem Connector, auf Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images zuzugreifen und diese herunterzuladen.
https://cloudmanagerinfraprod.azurecr.io	Zugriff auf Software-Images von Container-Komponenten für eine Infrastruktur, die Docker ausführt und eine Lösung für die Service-Integration mit Cloud Manager bietet.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
https://netapp-cloud-account.auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://mysupport.netapp.com	Kommunikation mit NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Kommunikation mit NetApp bei Systemlizenzrechten und Support-Registrierung

Endpunkte	Zweck
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Er ermöglicht NetApp, Informationen zu sammeln, die für die Behebung von Support-Problemen erforderlich sind.
https://ipa-signer.cloudmanager.netapp.com	Ermöglicht Cloud Manager die Generierung von Lizenzen (beispielsweise eine FlexCache Lizenz für Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden Mit den Endpunkten ist die Installation von NetApp Trident möglich.
*.blob.core.windows.net	Bei Verwendung eines Proxy erforderlich für HA-Paare
Verschiedene Standorte von Drittanbietern, z. B.: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com An Standorten von Drittanbietern können Änderungen vorgenommen werden.	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

Endpunkte für das Management von Ressourcen in GCP

Ein Connector kontaktiert die folgenden Endpunkte beim Management von Ressourcen in GCP:

Endpunkte	Zweck
https://www.googleapis.com	Ermöglicht dem Connector den Kontakt zu Google APIs für die Bereitstellung und das Management von Cloud Volumes ONTAP in GCP.
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://repo.cloud.support.netapp.com	Wird zum Herunterladen der Abhängigkeiten von Cloud Manager verwendet.
http://repo.mysql.com/	Zum Herunterladen von MySQL.

Endpunkte	Zweck
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Ermöglicht dem Connector, auf Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images zuzugreifen und diese herunterzuladen.
https://cloudmanagerinfraprod.azurecr.io	Zugriff auf Software-Images von Container-Komponenten für eine Infrastruktur, die Docker ausführt und eine Lösung für die Service-Integration mit Cloud Manager bietet.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
https://netapp-cloud-account.auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://mysupport.netapp.com	Kommunikation mit NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Kommunikation mit NetApp bei Systemlizenzrechten und Support-Registrierung
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Er ermöglicht NetApp, Informationen zu sammeln, die für die Behebung von Support-Problemen erforderlich sind.
https://ipa-signer.cloudmanager.netapp.com	Ermöglicht Cloud Manager die Generierung von Lizenzen (beispielsweise eine FlexCache Lizenz für Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden Mit den Endpunkten ist die Installation von NetApp Trident möglich.
Verschiedene Standorte von Drittanbietern, z. B.: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com An Standorten von Drittanbietern können Änderungen vorgenommen werden.	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

Endpunkte zum Installieren des Connectors auf einem Linux-Host

Sie haben die Möglichkeit, die Connector-Software manuell auf Ihrem eigenen Linux-Host zu installieren. In diesem Fall muss das Installationsprogramm für den Connector während des Installationsvorgangs auf die folgenden URLs zugreifen:

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

Der Host versucht möglicherweise, während der Installation Betriebssystempakete zu aktualisieren. Der Host kann verschiedene Spiegelungsstandorte für diese Betriebssystempakete kontaktieren.

Endpunkte, auf die Sie über Ihren Webbrowser zugreifen, wenn Sie die lokale Benutzeroberfläche verwenden

Während Sie fast alle Aufgaben über die SaaS-Benutzeroberfläche ausführen sollten, steht auf dem Connector weiterhin eine lokale Benutzeroberfläche zur Verfügung. Die Maschine, auf der der Webbrowser ausgeführt wird, muss über Verbindungen zu den folgenden Endpunkten verfügen:

Endpunkte	Zweck
Der Connector-Host	Sie müssen die IP-Adresse des Hosts aus einem Webbrowser eingeben, um die Cloud Manager-Konsole zu laden. Je nach Ihrer Verbindung mit Ihrem Cloud-Provider können Sie die private IP oder eine dem Host zugewiesene öffentliche IP verwenden: • Eine private IP funktioniert, wenn Sie über ein VPN verfügen und direkten Zugriff auf Ihr virtuelles Netzwerk haben • Eine öffentliche IP funktioniert in jedem Netzwerkszenario In jedem Fall sollten Sie den Netzwerkzugriff sichern, indem Sie sicherstellen, dass die Sicherheitsgruppenregeln den Zugriff nur von autorisierten IPs oder Subnetzen ermöglichen.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Ihr Webbrowser stellt über NetApp Cloud Central eine Verbindung zu diesen Endpunkten her, um eine zentralisierte Benutzerauthentifizierung zu ermöglichen.
https://widget.intercom.io	Für Ihren Produkt-Chat, der Ihnen das Gespräch mit NetApp Cloud-Experten ermöglicht.

Ports und Sicherheitsgruppen

Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn. HTTP und HTTPS bieten den Zugriff auf "Lokale Benutzeroberfläche", Die Sie in seltenen Fällen verwenden. SSH ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

Regeln für den Connector in AWS

Die Sicherheitsgruppe für den Konnektor erfordert sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln in der vordefinierten Sicherheitsgruppe ist 0.0.0.0/0.

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche und Verbindungen von Cloud Compliance
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
TCP	3128	Bietet die Cloud Compliance-Instanz einen Internetzugang, wenn Ihr AWS-Netzwerk keine NAT oder Proxy verwendet

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
Active Directory	TCP	88	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	TCP	139	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP	389	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	TCP	749	Active Directory-Gesamtstruktur	Active Directory Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	UDP	137	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	UDP	464	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an AWS und ONTAP und Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP Cluster Management LIF	API-Aufrufe für ONTAP
	TCP	8088	Backup auf S3	API-Aufrufe zur Sicherung in S3
DNS	UDP	53	DNS	Wird für die DNS-Auflösung durch Cloud Manager verwendet
Cloud-Compliance	HTTP	80	Cloud Compliance Instanz	Cloud Compliance für Cloud Volumes ONTAP

Regeln für den Connector in Azure

Die Sicherheitsgruppe für den Konnektor erfordert sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln in der vordefinierten Sicherheitsgruppe ist 0.0.0.0/0.

Port	Protokoll	Zweck
22	SSH	Bietet SSH-Zugriff auf den Connector-Host
80	HTTP	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
443	HTTPS	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

Port	Protokoll	Zweck
Alle	Alle TCP	Gesamter abgehender Datenverkehr
Alle	Alle UDP-Protokolle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

Service	Port	Protokoll	Ziel	Zweck
Active Directory	88	TCP	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	139	TCP	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	389	TCP	Active Directory-Gesamtstruktur	LDAP
	445	TCP	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	464	TCP	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	749	TCP	Active Directory-Gesamtstruktur	Active Directory Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	137	UDP	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	138	UDP	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	464	UDP	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
API-Aufrufe und AutoSupport	443	HTTPS	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an AWS und ONTAP und Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	3000	TCP	ONTAP Cluster Management LIF	API-Aufrufe für ONTAP
DNS	53	UDP	DNS	Wird für die DNS-Auflösung durch Cloud Manager verwendet

Regeln für den Connector in GCP

Die Firewall-Regeln für den Connector erfordern sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln in den vordefinierten Firewall-Regeln ist 0.0.0.0/0.

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche

Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector öffnen den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector enthalten die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
Active Directory	TCP	88	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	TCP	139	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP	389	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	TCP	749	Active Directory-Gesamtstruktur	Active Directory Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	UDP	137	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	UDP	464	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API ruft GCP und ONTAP ab und sendet AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP Cluster Management LIF	API-Aufrufe für ONTAP
DNS	UDP	53	DNS	Wird für die DNS-Auflösung durch Cloud Manager verwendet

Erstellen eines Connectors in AWS über Cloud Manager

Ein Kontoadministrator muss einen *Connector* bereitstellen, bevor Sie die meisten Funktionen von Cloud Manager nutzen können. "Informieren Sie sich, wann ein Anschluss erforderlich ist". Mit dem Connector kann Cloud Manager Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen.

Auf dieser Seite wird beschrieben, wie Sie einen Connector direkt aus Cloud Manager in AWS erstellen. Sie

haben auch die Möglichkeit zu wählen "Erstellen Sie den Connector über den AWS Marketplace", Oder auf "Laden Sie die Software herunter und installieren Sie sie auf Ihrem eigenen Host".

Diese Schritte müssen von einem Benutzer ausgeführt werden, der die Rolle „Account Admin“ hat. Ein Workspace-Administrator kann keinen Konnektor erstellen.

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector zu erstellen, falls noch kein Connector vorhanden ist.

Einrichtung von AWS Berechtigungen zum Erstellen eines Konnektors

Bevor Sie einen Connector von Cloud Manager implementieren können, müssen Sie sicherstellen, dass Ihr AWS-Konto die entsprechenden Berechtigungen hat.

Schritte

1. Laden Sie die IAM-Richtlinie für Connector von folgendem Speicherort herunter:

   "NetApp Cloud Manager: AWS, Azure und GCP-Richtlinien"

2. Erstellen Sie von der AWS IAM-Konsole aus Ihre eigene Richtlinie, indem Sie den Text aus der IAM-Richtlinie für Connector kopieren und einfügen.
3. Hängen Sie die Richtlinie, die Sie im vorherigen Schritt erstellt haben, dem IAM-Benutzer an, der den Connector aus Cloud Manager erstellt.

Ergebnis

Der AWS-Benutzer verfügt nun über die erforderlichen Berechtigungen, um den Connector aus Cloud Manager zu erstellen. Sie müssen für diesen Benutzer die AWS-Zugriffsschlüssel festlegen, wenn Sie von Cloud Manager aufgefordert werden.

Erstellen eines Konnektors in AWS

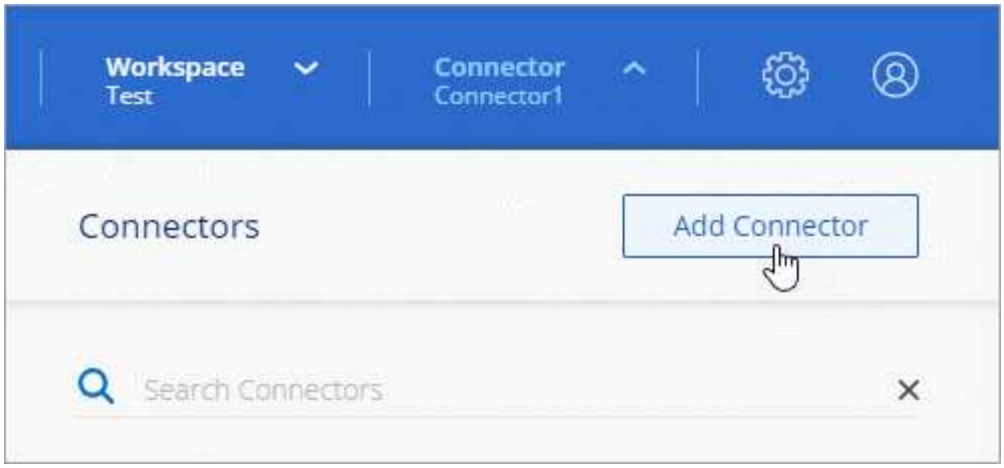
Mit Cloud Manager können Sie einen Connector in AWS direkt von der Benutzeroberfläche aus erstellen.

Was Sie benötigen

- Ein AWS-Zugriffsschlüssel und ein geheimer Schlüssel für einen IAM-Benutzer, der über den verfügt "Erforderliche Berechtigungen".
- Ein VPC, Subnetz und Schlüsselpairs in Ihrer bevorzugten AWS Region.

Schritte

1. Wenn Sie Ihre erste Arbeitsumgebung erstellen, klicken Sie auf **Arbeitsumgebung hinzufügen** und befolgen Sie die Anweisungen. Klicken Sie andernfalls auf das Dropdown-Menü **Connector** und wählen Sie **Connector hinzufügen** aus.



2. Klicken Sie auf **Let's Start**.
3. Wählen Sie als Cloud-Provider * Amazon Web Services* aus.

   Denken Sie daran, dass der Connector über eine Netzwerkverbindung mit der Art der Arbeitsumgebung, die Sie erstellen, und den Diensten, die Sie für die Aktivierung planen, verfügen muss.

   "Erfahren Sie mehr über die Netzwerkanforderungen für den Connector".

4. Überprüfen Sie, was Sie benötigen, und klicken Sie auf **Weiter**.
5. Geben Sie die erforderlichen Informationen ein:
   - **AWS Credentials**: Geben Sie einen Namen für die Instanz ein und geben Sie den AWS Zugriffsschlüssel und den geheimen Schlüssel an, der die Berechtigungsanforderungen erfüllt.
   - **Standort**: Geben Sie eine AWS Region, VPC und Subnetz für die Instanz an.
   - **Netzwerk**: Wählen Sie das Schlüsselpaar aus, das mit der Instanz verwendet werden soll, ob eine öffentliche IP-Adresse aktiviert werden soll, und geben Sie optional eine Proxy-Konfiguration an.
   - **Sicherheitsgruppe**: Wählen Sie aus, ob eine neue Sicherheitsgruppe erstellt werden soll oder ob eine vorhandene Sicherheitsgruppe ausgewählt werden soll, die einen eingehenden HTTP-, HTTPS- und SSH-Zugriff erlaubt.

   > Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn. HTTP und HTTPS bieten den Zugriff auf "Lokale Benutzeroberfläche", Die Sie in seltenen Fällen verwenden. SSH ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

6. Klicken Sie Auf **Erstellen**.

   Die Instanz sollte in ca. 7 Minuten fertig sein. Sie sollten auf der Seite bleiben, bis der Vorgang abgeschlossen ist.

Nachdem Sie fertig sind

Sie müssen einen Connector mit Arbeitsbereichen verknüpfen, damit Arbeitsbereichsadministratoren diese Connectors zum Erstellen von Cloud Volumes ONTAP-Systemen verwenden können. Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Connector mit Arbeitsbereichen zu verknüpfen. Account-Administratoren haben standardmäßig die Möglichkeit, auf alle Workspaces in Cloud Manager zuzugreifen. "Weitere Informationen .".

Erstellen eines Connectors in Azure über Cloud Manager

Ein Kontoadministrator muss einen *Connector* bereitstellen, bevor Sie die meisten Funktionen von Cloud Manager nutzen können. "Informieren Sie sich, wann ein Anschluss erforderlich ist". Mit dem Connector kann Cloud Manager Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen.

Auf dieser Seite wird beschrieben, wie Sie direkt aus Cloud Manager einen Connector in Azure erstellen. Sie haben auch die Möglichkeit zu wählen "Erstellen Sie den Connector aus dem Azure Marketplace", Oder auf "Laden Sie die Software herunter und installieren Sie sie auf Ihrem eigenen Host".

Diese Schritte müssen von einem Benutzer ausgeführt werden, der die Rolle „Account Admin“ hat. Ein Workspace-Administrator kann keinen Konnektor erstellen.

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector zu erstellen, falls noch kein Connector vorhanden ist.

Einrichten von Azure-Berechtigungen zum Erstellen eines Connectors

Bevor Sie einen Connector von Cloud Manager implementieren können, müssen Sie sicherstellen, dass Ihr Azure-Konto die entsprechenden Berechtigungen hat.

Schritte

1. Erstellen Sie mithilfe der Azure-Richtlinie für den Connector eine benutzerdefinierte Rolle:

   a. Laden Sie die herunter "Azure-Richtlinie für den Connector".

      Klicken Sie mit der rechten Maustaste auf den Link und klicken Sie auf **Link speichern unter…**, um die Datei herunterzuladen.

   b. Ändern Sie die JSON-Datei, indem Sie Ihre Azure Abonnement-ID dem zuweisbaren Umfang hinzufügen.

      Beispiel

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

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

      Im folgenden Beispiel wird gezeigt, wie eine benutzerdefinierte Rolle mithilfe der Azure CLI 2.0 erstellt wird:

      ```
      az role definition create --role-definition
      C:\Policy_for_Setup_As_Service_Azure.json
      ```

   Sie sollten jetzt eine benutzerdefinierte Rolle namens *Azure SetupAsService* haben.

2. Weisen Sie die Rolle dem Benutzer zu, der den Connector aus Cloud Manager bereitstellen soll:

a. Öffnen Sie den Dienst **Abonnements** und wählen Sie das Abonnement des Benutzers aus.

b. Klicken Sie auf **Access Control (IAM)**.

c. Klicken Sie auf **Hinzufügen** > **Rollenzuordnung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:

- Wählen Sie die Rolle **Azure SetupAsService** aus.

> Azure SetupAsService ist der Standardname, der in angegeben wird "Connector-Implementierungsrichtlinie für Azure". Wenn Sie einen anderen Namen für die Rolle ausgewählt haben, wählen Sie stattdessen diesen Namen aus.

- Weisen Sie einem **Azure AD-Benutzer, einer Gruppe oder einer Anwendung** Zugriff zu.
- Wählen Sie das Benutzerkonto aus.
- Klicken Sie Auf **Speichern**.

Ergebnis

Der Azure-Benutzer verfügt nun über die erforderlichen Berechtigungen, um den Connector aus Cloud Manager zu implementieren.

Erstellen eines Connectors in Azure

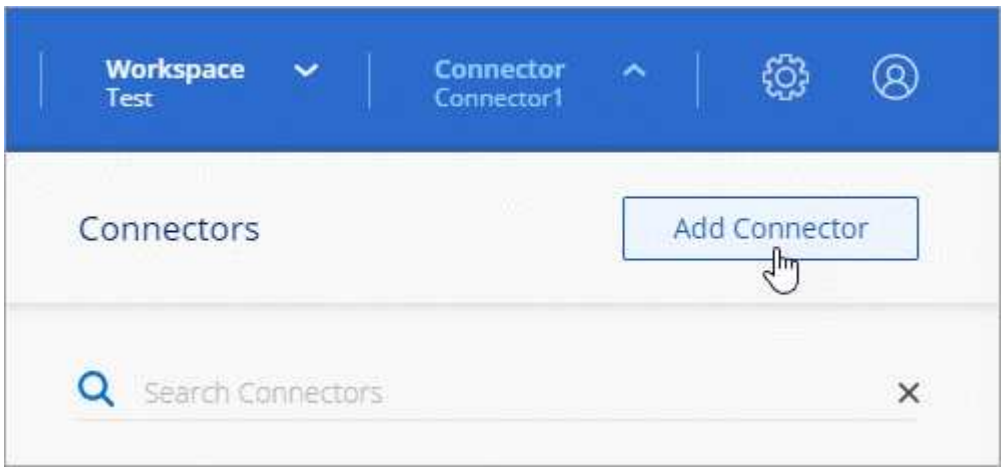
Mit Cloud Manager können Sie einen Connector in Azure direkt von der Benutzeroberfläche aus erstellen.

Was Sie benötigen

- Der "Erforderliche Berechtigungen" Für Ihr Azure Konto.
- Ein Azure Abonnement.
- Eine vnet und Subnetz in Ihrer bevorzugten Azure-Region.

Schritte

1. Wenn Sie Ihre erste Arbeitsumgebung erstellen, klicken Sie auf **Arbeitsumgebung hinzufügen** und befolgen Sie die Anweisungen. Klicken Sie andernfalls auf das Dropdown-Menü **Connector** und wählen Sie **Connector hinzufügen** aus.



2. Klicken Sie auf **Let's Start**.
3. Wählen Sie als Cloud-Provider * Microsoft Azure* aus.

Denken Sie daran, dass der Connector über eine Netzwerkverbindung mit der Art der Arbeitsumgebung, die Sie erstellen, und den Diensten, die Sie für die Aktivierung planen, verfügen muss.

"Erfahren Sie mehr über die Netzwerkanforderungen für den Connector".

4. Überprüfen Sie, was Sie benötigen, und klicken Sie auf **Weiter**.
5. Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Microsoft-Konto an, das über die erforderlichen Berechtigungen zum Erstellen der virtuellen Maschine verfügt.

   Das Formular ist Eigentum von Microsoft und wird von Microsoft gehostet. Ihre Zugangsdaten werden nicht an NetApp bereitgestellt.

   Wenn Sie bereits bei einem Azure-Konto angemeldet sind, nutzt Cloud Manager das Konto automatisch. Wenn Sie über mehrere Konten verfügen, müssen Sie sich möglicherweise erst abmelden, um sicherzustellen, dass Sie das richtige Konto verwenden.

6. Geben Sie die erforderlichen Informationen ein:
   - **VM Authentication**: Geben Sie einen Namen für die virtuelle Maschine und einen Benutzernamen und ein Passwort oder einen öffentlichen Schlüssel ein.
   - **Grundeinstellungen**: Wählen Sie ein Azure-Abonnement, eine Azure-Region und ob Sie eine neue Ressourcengruppe erstellen oder eine vorhandene Ressourcengruppe verwenden möchten.
   - **Netzwerk**: Wählen Sie ein vnet und Subnetz, ob eine öffentliche IP-Adresse aktiviert werden soll, und geben Sie optional eine Proxy-Konfiguration an.
   - **Sicherheitsgruppe**: Wählen Sie aus, ob eine neue Sicherheitsgruppe erstellt werden soll oder ob eine vorhandene Sicherheitsgruppe ausgewählt werden soll, die einen eingehenden HTTP-, HTTPS- und SSH-Zugriff erlaubt.

   Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn. HTTP und HTTPS bieten den Zugriff auf "Lokale Benutzeroberfläche", Die Sie in seltenen Fällen verwenden. SSH ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

7. Klicken Sie Auf **Erstellen**.

   Die Virtual Machine sollte in ca. 7 Minuten einsatzbereit sein. Sie sollten auf der Seite bleiben, bis der Vorgang abgeschlossen ist.

Nachdem Sie fertig sind

Sie müssen einen Connector mit Arbeitsbereichen verknüpfen, damit Arbeitsbereichsadministratoren diese Connectors zum Erstellen von Cloud Volumes ONTAP-Systemen verwenden können. Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Connector mit Arbeitsbereichen zu verknüpfen. Account-Administratoren haben standardmäßig die Möglichkeit, auf alle Workspaces in Cloud Manager zuzugreifen. "Weitere Informationen .".

Erstellen eines Connectors in GCP über Cloud Manager

Ein Kontoadministrator muss einen *Connector* bereitstellen, bevor Sie die meisten Funktionen von Cloud Manager nutzen können. "Informieren Sie sich, wann ein Anschluss erforderlich ist". Mit dem Connector kann Cloud Manager Ressourcen und

Prozesse in Ihrer Public Cloud-Umgebung managen.

Auf dieser Seite wird beschrieben, wie ein Connector in GCP direkt aus Cloud Manager erstellt wird. Sie haben auch die Möglichkeit zu wählen "Laden Sie die Software herunter und installieren Sie sie auf Ihrem eigenen Host".

Diese Schritte müssen von einem Benutzer ausgeführt werden, der die Rolle „Account Admin“ hat. Ein Workspace-Administrator kann keinen Konnektor erstellen.

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector zu erstellen, falls noch kein Connector vorhanden ist.

Einrichten von GCP-Berechtigungen zum Erstellen eines Konnektors

Bevor Sie einen Connector von Cloud Manager bereitstellen können, müssen Sie sicherstellen, dass Ihr GCP-Konto die entsprechenden Berechtigungen hat und dass ein Servicekonto für die Connector-VM eingerichtet ist.

Schritte

1. Stellen Sie sicher, dass der GCP-Benutzer, der Cloud Manager über NetApp Cloud Central implementiert, die Berechtigungen in hat "Connector-Implementierungsrichtlinie für GCP".

   "Sie können eine benutzerdefinierte Rolle mit der YAML-Datei erstellen" Und verbinden Sie sie dann mit dem Benutzer. Sie müssen die gCloud-Befehlszeile verwenden, um die Rolle zu erstellen.

2. Richten Sie ein Service-Konto ein, das über die Berechtigungen verfügt, die Cloud Manager zum Erstellen und Managen von Cloud Volumes ONTAP-Systemen in Projekten benötigt.

   Dieses Servicekonto wird der Connector VM zugeordnet, wenn Sie es aus Cloud Manager erstellen.

   a. "Rolle in GCP anlegen" Dazu gehören die im definierten Berechtigungen "Cloud Manager-Richtlinie für GCP". Sie müssen die gCloud-Befehlszeile verwenden.

      Die in dieser YAML-Datei enthaltenen Berechtigungen unterscheiden sich von den Berechtigungen in Schritt 2a.

   b. "Erstellen Sie ein GCP-Service-Konto und wenden Sie die benutzerdefinierte Rolle an, die Sie gerade erstellt haben".

   c. Wenn Sie Cloud Volumes ONTAP in anderen Projekten implementieren möchten, "Sie gewähren Zugriff, indem Sie dem Projekt das Service-Konto mit der Rolle Cloud Manager hinzufügen". Sie müssen diesen Schritt für jedes Projekt wiederholen.

Ergebnis

Der GCP-Benutzer verfügt jetzt über die erforderlichen Berechtigungen, um den Connector aus Cloud Manager zu erstellen, und das Servicekonto für die Connector-VM wird eingerichtet.

Aktivieren von Google Cloud APIs

Für die Bereitstellung des Connectors und der Cloud Volumes ONTAP sind mehrere APIs erforderlich.

Schritt

1. "Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt".

- Cloud Deployment Manager V2-API
- Cloud-ProtokollierungsAPI
- Cloud Resource Manager API
- Compute Engine-API
- IAM-API (Identitäts- und Zugriffsmanagement

Erstellen eines Konnektors in GCP

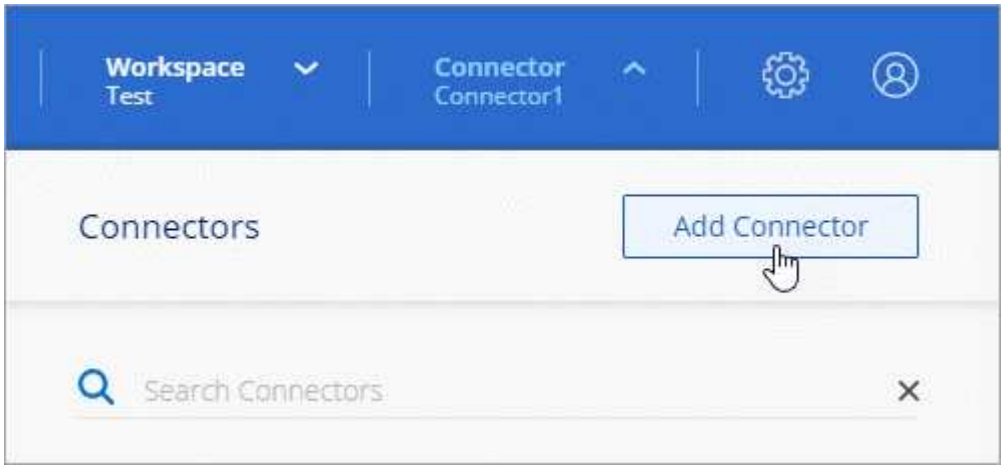
Mit Cloud Manager können Sie einen Connector in GCP direkt von der Benutzeroberfläche aus erstellen.

Was Sie benötigen

- Der "Erforderliche Berechtigungen" Für Ihren Google Cloud-Account.
- Ein Google Cloud-Projekt.
- Ein Servicekonto mit den erforderlichen Berechtigungen zum Erstellen und Verwalten von Cloud Volumes ONTAP.
- Ein VPC und Subnetz in Ihrer bevorzugten Google Cloud-Region.

Schritte

1. Wenn Sie Ihre erste Arbeitsumgebung erstellen, klicken Sie auf **Arbeitsumgebung hinzufügen** und befolgen Sie die Anweisungen. Klicken Sie andernfalls auf das Dropdown-Menü **Connector** und wählen Sie **Connector hinzufügen** aus.



2. Klicken Sie auf **Let's Start**.
3. Wählen Sie **Google Cloud Platform** als Cloud-Provider.

   Denken Sie daran, dass der Connector über eine Netzwerkverbindung mit der Art der Arbeitsumgebung, die Sie erstellen, und den Diensten, die Sie für die Aktivierung planen, verfügen muss.

   "Erfahren Sie mehr über die Netzwerkanforderungen für den Connector".

4. Überprüfen Sie, was Sie benötigen, und klicken Sie auf **Weiter**.
5. Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Google-Konto an, das über die erforderlichen Berechtigungen zum Erstellen der virtuellen Maschineninstanz verfügen sollte.

   Das Formular ist Eigentum und wird von Google gehostet. Ihre Zugangsdaten werden nicht an NetApp

bereitgestellt.

6. Geben Sie die erforderlichen Informationen ein:
   - **Grundeinstellungen**: Geben Sie einen Namen für die virtuelle Maschineninstanz ein und geben Sie ein Projekt- und Servicekonto an, das über die erforderlichen Berechtigungen verfügt.
   - **Ort**: Geben Sie eine Region, Zone, VPC und Subnetz für die Instanz an.
   - **Netzwerk**: Wählen Sie, ob eine öffentliche IP-Adresse aktiviert werden soll und geben Sie optional eine Proxy-Konfiguration an.
   - **Firewall-Richtlinie**: Wählen Sie, ob Sie eine neue Firewall-Richtlinie erstellen oder eine vorhandene Firewall-Richtlinie auswählen möchten, die einen eingehenden HTTP-, HTTPS- und SSH-Zugriff erlaubt.

   > Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn. HTTP und HTTPS bieten den Zugriff auf "Lokale Benutzeroberfläche", Die Sie in seltenen Fällen verwenden. SSH ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

7. Klicken Sie Auf **Erstellen**.

   Die Instanz sollte in ca. 7 Minuten fertig sein. Sie sollten auf der Seite bleiben, bis der Vorgang abgeschlossen ist.

Nachdem Sie fertig sind

Sie müssen einen Connector mit Arbeitsbereichen verknüpfen, damit Arbeitsbereichsadministratoren diese Connectors zum Erstellen von Cloud Volumes ONTAP-Systemen verwenden können. Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Connector mit Arbeitsbereichen zu verknüpfen. Account-Administratoren haben standardmäßig die Möglichkeit, auf alle Workspaces in Cloud Manager zuzugreifen. "Weitere Informationen .".

Copyright-Informationen

Markeninformationen