Configurer un connecteur

Cloud Manager 3.8

NetApp
October 22, 2024

Sommaire

Configurer un connecteur

En savoir plus sur les connecteurs

Dans la plupart des cas, un administrateur de compte devra déployer un *Connector* dans votre réseau cloud ou sur site. Ce connecteur permet à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public.

Lorsqu'un connecteur est nécessaire

Un connecteur est nécessaire pour utiliser l'une des fonctionnalités suivantes dans Cloud Manager :

- Cloud Volumes ONTAP
- Clusters ONTAP sur site
- Conformité cloud
- Kubernetes
- Sauvegarde dans le cloud
- Contrôle
- Tiering sur site
- Cache global de fichiers
- Découverte des compartiments Amazon S3

Un connecteur est ***NOT*** requis pour Azure NetApp Files, Cloud Volumes Service ou Cloud Sync.

Même si aucun connecteur n'est nécessaire pour configurer et gérer Azure NetApp Files, un connecteur est nécessaire si vous souhaitez utiliser Cloud Compliance pour analyser les données Azure NetApp Files.

Emplacements pris en charge

Un connecteur est pris en charge aux emplacements suivants :

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- Sur site

Pour créer un système Cloud Volumes ONTAP dans Google Cloud, vous devez également disposer d'un connecteur exécuté dans Google Cloud. Vous ne pouvez pas utiliser un connecteur qui fonctionne à un autre emplacement.

Les connecteurs doivent rester en fonctionnement

Un connecteur doit rester en fonctionnement en permanence. Il est important pour la santé et le fonctionnement continus des services que vous proposez.

Par exemple, un connecteur est un composant clé de la santé et du fonctionnement des systèmes Cloud Volumes ONTAP PAYGO. Si un connecteur est hors tension, les systèmes Cloud Volumes ONTAP PAYGO s'arrêtent après une perte de communication avec un connecteur pendant plus de 14 jours.

Comment créer un connecteur

Un administrateur de compte doit créer un connecteur avant qu'un administrateur d'espace de travail puisse créer un environnement de travail Cloud Volumes ONTAP et utiliser les autres fonctionnalités répertoriées ci-dessus.

Un administrateur de compte peut créer un connecteur de différentes façons :

- Directement dans Cloud Manager (recommandé)
  - "Création dans AWS"
  - "Création dans Azure"
  - "Création dans GCP"
- "Depuis AWS Marketplace"
- "À partir d'Azure Marketplace"
- "En téléchargeant et installant le logiciel sur un hôte Linux existant"

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore créé.

Autorisations

Des autorisations spécifiques sont nécessaires pour créer le connecteur et un autre ensemble d'autorisations est nécessaire pour l'instance de connecteur elle-même.

Autorisations pour créer un connecteur

L'utilisateur qui crée un connecteur depuis Cloud Manager a besoin de permissions spécifiques pour déployer l'instance dans votre fournisseur de cloud de votre choix. Cloud Manager vous rappelle les exigences d'autorisation lorsque vous créez un connecteur.

"Affichez les règles de chaque fournisseur cloud".

Autorisations pour l'instance de connecteur

Le connecteur nécessite des autorisations spécifiques de fournisseurs cloud pour effectuer des opérations en votre nom. Par exemple, pour déployer et gérer Cloud Volumes ONTAP.

Lorsque vous créez un connecteur directement depuis Cloud Manager, Cloud Manager crée le connecteur avec les autorisations dont il a besoin. Vous n'avez rien à faire.

Si vous créez vous-même le connecteur à partir d'AWS Marketplace, d'Azure Marketplace ou d'une installation manuelle du logiciel, vous devez vous assurer que les autorisations appropriées sont en place.

"Affichez les règles de chaque fournisseur cloud".

Quand utiliser plusieurs connecteurs

Dans certains cas, vous n'avez peut-être besoin que d'un seul connecteur, mais vous pourriez avoir besoin de deux connecteurs ou plus.

Voici quelques exemples :

- Vous utilisez un environnement multicloud (AWS et Azure), c'est pourquoi vous avez un connecteur dans AWS et un autre dans Azure. Chacun gère les systèmes Cloud Volumes ONTAP exécutés dans ces environnements.
- Un fournisseur de services peut utiliser un seul compte Cloud Central pour fournir des services à ses clients, tout en utilisant un autre compte pour assurer la reprise après incident de l'une de ses business units. Chaque compte aurait des connecteurs distincts.

Quand passer d'un connecteur à un autre

Lorsque vous créez votre premier connecteur, Cloud Manager utilise automatiquement ce connecteur pour chaque environnement de travail supplémentaire que vous créez. Une fois que vous avez créé un connecteur supplémentaire, vous devrez passer de l'un à l'autre pour voir les environnements de travail spécifiques à chaque connecteur.

"Apprenez à passer d'un connecteur à un autre".

Interface utilisateur locale

Pendant que vous devriez effectuer presque toutes les tâches à partir du "Interface utilisateur SaaS", Une interface utilisateur locale est toujours disponible sur le connecteur. Cette interface est nécessaire pour quelques tâches qui doivent être effectuées à partir du connecteur lui-même :

- "Configuration d'un serveur proxy"
- Installation d'un correctif (en général, vous travaillerez avec le personnel NetApp pour installer un correctif)
- Téléchargement de messages AutoSupport (généralement dirigés par le personnel NetApp en cas de problème)

"Découvrez comment accéder à l'interface utilisateur locale".

Mises à niveau des connecteurs

Le connecteur met automatiquement à jour son logiciel à la dernière version, tant qu'il l'a fait "accès internet sortant" pour obtenir la mise à jour logicielle.

Exigences de mise en réseau pour le connecteur

Configurez votre réseau de sorte que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. L'étape la plus importante consiste à garantir l'accès Internet sortant à différents terminaux.

Si votre réseau utilise un serveur proxy pour toutes les communications vers Internet, vous pouvez spécifier le serveur proxy à partir de la page Paramètres. Reportez-vous à la section "Configuration du connecteur pour utiliser un serveur proxy".

Connexion aux réseaux cibles

Un connecteur nécessite une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

Par exemple, si vous installez un connecteur sur le réseau de votre entreprise, vous devez configurer une connexion VPN sur le VPC ou le vnet dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public. L'accès Internet sortant est également requis si vous souhaitez installer manuellement le connecteur sur un hôte Linux ou accéder à l'interface utilisateur locale exécutée sur le connecteur.

Les sections suivantes identifient les terminaux spécifiques.

Terminaux pour gérer les ressources dans AWS

Lors de la gestion des ressources dans AWS, un connecteur contacte les terminaux suivants :

Terminaux	Objectif
Services AWS (amazonaws.com): • CloudFormation • Cloud de calcul élastique (EC2) • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3) Le noeud final exact dépend de la région dans laquelle vous déployez Cloud Volumes ONTAP. "Reportez-vous à la documentation AWS pour plus de détails."	Permet à Connector de déployer et de gérer Cloud Volumes ONTAP dans AWS.
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger 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	Permet au connecteur d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.

Terminaux	Objectif
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Permet d'ajouter votre ID de compte AWS à la liste des utilisateurs autorisés pour Backup vers S3.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Communication avec 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	Communication avec NetApp pour les licences système et l'inscription au support.
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	Il permet à NetApp de collecter les informations nécessaires à la résolution des problèmes.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

Terminaux pour gérer les ressources dans Azure

Lors de la gestion des ressources dans Azure, un connecteur contacte les terminaux suivants :

Terminaux	Objectif
https://management.azure.com https://login.microsoftonline.com	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans la plupart des régions d'Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans les régions d'Azure Allemagne.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans les régions d'Azure US Gov.
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger 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	Permet au connecteur d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://mysupport.netapp.com	Communication avec 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	Communication avec NetApp pour les licences système et l'inscription au support.
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	Il permet à NetApp de collecter les informations nécessaires à la résolution des problèmes.

Terminaux	Objectif
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.
*.blob.core.windows.net	Requis pour les paires haute disponibilité lors de l'utilisation d'un proxy.
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

Des terminaux pour gérer les ressources dans GCP

Lors de la gestion des ressources dans GCP, un connecteur contacte les terminaux suivants :

Terminaux	Objectif
https://www.googleapis.com	Permet au connecteur de contacter les API Google pour le déploiement et la gestion de Cloud Volumes ONTAP dans GCP.
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger 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	Permet au connecteur d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.

Terminaux	Objectif
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://mysupport.netapp.com	Communication avec 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	Communication avec NetApp pour les licences système et l'inscription au support.
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	Il permet à NetApp de collecter les informations nécessaires à la résolution des problèmes.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

Noeuds finaux pour installer le connecteur sur un hôte Linux

Vous avez la possibilité d'installer manuellement le logiciel Connector sur votre propre hôte Linux. Dans ce cas, le programme d'installation du connecteur doit accéder aux URL suivantes pendant le processus d'installation :

- 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

L'hôte peut essayer de mettre à jour les packages du système d'exploitation lors de l'installation. L'hôte peut contacter différents sites de mise en miroir pour ces packages OS.

Les terminaux accessibles à partir de votre navigateur Web lors de l'utilisation de l'interface utilisateur locale

Bien que vous devriez effectuer presque toutes les tâches à partir de l'interface utilisateur SaaS, une interface utilisateur locale est toujours disponible sur le connecteur. La machine exécutant le navigateur Web doit disposer de connexions aux terminaux suivants :

Terminaux	Objectif
L'hôte du connecteur	Vous devez entrer l'adresse IP de l'hôte depuis un navigateur Web pour charger la console Cloud Manager. En fonction de votre connectivité avec votre fournisseur de cloud, vous pouvez utiliser l'IP privée ou une adresse IP publique attribuée à l'hôte : • Une adresse IP privée fonctionne si vous disposez d'un VPN et d'un accès direct à votre réseau virtuel • Un IP public fonctionne dans tous les scénarios de mise en réseau Dans tous les cas, vous devez sécuriser l'accès au réseau en vous assurant que les règles du groupe de sécurité autorisent l'accès à partir des adresses IP ou des sous-réseaux autorisés uniquement.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces terminaux pour une authentification centralisée des utilisateurs via NetApp Cloud Central.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

Ports et groupes de sécurité

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez. HTTP et HTTPS permettent l'accès au "Interface utilisateur locale", que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

Règles pour le connecteur dans AWS

Le groupe de sécurité du connecteur nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

La source des règles entrantes dans le groupe de sécurité prédéfini est 0.0.0.0/0.

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP depuis les navigateurs Web du client vers l'interface utilisateur locale et les connexions à partir de Cloud Compliance

Protocole	Port	Objectif
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale
TCP	3128	Fournit l'instance Cloud Compliance avec un accès Internet si votre réseau AWS n'utilise pas de NAT ou de proxy

Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour le connecteur inclut les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.

L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Active Directory	TCP	88	Forêt Active Directory	Authentification Kerberos V.
	TCP	139	Forêt Active Directory	Session de service NetBIOS
	TCP	389	Forêt Active Directory	LDAP
	TCP	445	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	TCP	749	Forêt Active Directory	Modification et définition du mot de passe de Kerberos V Active Directory (RPCSEC_GSS)
	UDP	137	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	Forêt Active Directory	Service de datagrammes NetBIOS
	UDP	464	Forêt Active Directory	Administration des clés Kerberos
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	API appelle AWS et ONTAP et envoie des messages AutoSupport à NetApp
Appels API	TCP	3000	LIF de gestion de cluster ONTAP	Appels API vers ONTAP
	TCP	8088	Sauvegarde vers S3	Appels d'API vers Backup vers S3
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par Cloud Manager
Conformité cloud	HTTP	80	Instance Cloud Compliance	Cloud Compliance pour Cloud Volumes ONTAP

Règles pour le connecteur dans Azure

Le groupe de sécurité du connecteur nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

La source des règles entrantes dans le groupe de sécurité prédéfini est 0.0.0.0/0.

Port	Protocole	Objectif
22	SSH	Fournit un accès SSH à l'hôte du connecteur
80	HTTP	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
443	HTTPS	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour le connecteur inclut les règles de trafic sortant suivantes.

Port	Protocole	Objectif
Tout	Tous les protocoles TCP	Tout le trafic sortant
Tout	Tous les protocoles UDP	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.

L'adresse IP source est l'hôte du connecteur.

Service	Port	Protocole	Destination	Objectif
Active Directory	88	TCP	Forêt Active Directory	Authentification Kerberos V.
	139	TCP	Forêt Active Directory	Session de service NetBIOS
	389	TCP	Forêt Active Directory	LDAP
	445	TCP	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	464	TCP	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	749	TCP	Forêt Active Directory	Modification et définition du mot de passe de Kerberos V Active Directory (RPCSEC_GSS)
	137	UDP	Forêt Active Directory	Service de noms NetBIOS
	138	UDP	Forêt Active Directory	Service de datagrammes NetBIOS
	464	UDP	Forêt Active Directory	Administration des clés Kerberos
Appels API et AutoSupport	443	HTTPS	LIF de gestion de cluster ONTAP et Internet sortant	API appelle AWS et ONTAP et envoie des messages AutoSupport à NetApp
Appels API	3000	TCP	LIF de gestion de cluster ONTAP	Appels API vers ONTAP
DNS	53	UDP	DNS	Utilisé pour la résolution DNS par Cloud Manager

Règles pour le connecteur dans GCP

Les règles de pare-feu du connecteur exigent à la fois des règles entrantes et sortantes.

Règles entrantes

La source des règles entrantes dans les règles de pare-feu prédéfinies est 0.0.0.0/0.

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

Règles de sortie

Les règles de pare-feu prédéfinies pour le connecteur ouvrent tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Les règles de pare-feu prédéfinies pour le connecteur comprennent les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.

L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Active Directory	TCP	88	Forêt Active Directory	Authentification Kerberos V.
	TCP	139	Forêt Active Directory	Session de service NetBIOS
	TCP	389	Forêt Active Directory	LDAP
	TCP	445	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	TCP	749	Forêt Active Directory	Modification et définition du mot de passe de Kerberos V Active Directory (RPCSEC_GSS)
	UDP	137	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	Forêt Active Directory	Service de datagrammes NetBIOS
	UDP	464	Forêt Active Directory	Administration des clés Kerberos
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Par des appels d'API à GCP et à ONTAP, et par l'envoi de messages AutoSupport à NetApp
Appels API	TCP	3000	LIF de gestion de cluster ONTAP	Appels API vers ONTAP
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par Cloud Manager

Création d'un connecteur dans AWS à partir de Cloud Manager

Un administrateur de compte doit déployer un *Connector* avant de pouvoir utiliser la plupart des fonctionnalités de Cloud Manager. "Apprenez quand un connecteur est nécessaire". Ce connecteur permet à Cloud Manager de gérer les ressources et les

processus au sein de votre environnement de cloud public.

Cette page explique comment créer un connecteur dans AWS directement depuis Cloud Manager. Vous avez également la possibilité de "Créez le connecteur à partir d'AWS Marketplace", ou à "téléchargez le logiciel et installez-le sur votre propre hôte".

Ces étapes doivent être réalisées par un utilisateur qui a le rôle d'administrateur de compte. Un administrateur d'espace de travail ne peut pas créer de connecteur.

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore créé.

Configuration des autorisations AWS pour créer un connecteur

Avant de déployer un connecteur depuis Cloud Manager, vous devez vous assurer que votre compte AWS dispose des autorisations appropriées.

Étapes

1. Téléchargez la politique IAM des connecteurs à l'emplacement suivant :

   "NetApp Cloud Manager : règles AWS, Azure et GCP"

2. Dans la console IAM AWS, créez votre propre règle en copiant et collant le texte de la politique IAM du connecteur.
3. Associez la règle que vous avez créée à l'étape précédente à l'utilisateur IAM qui crée le connecteur à partir de Cloud Manager.

Résultat

L'utilisateur AWS dispose désormais des autorisations nécessaires pour créer le connecteur à partir de Cloud Manager. Vous devez spécifier les clés d'accès AWS pour cet utilisateur lorsque vous y êtes invité par Cloud Manager.

Création d'un connecteur dans AWS

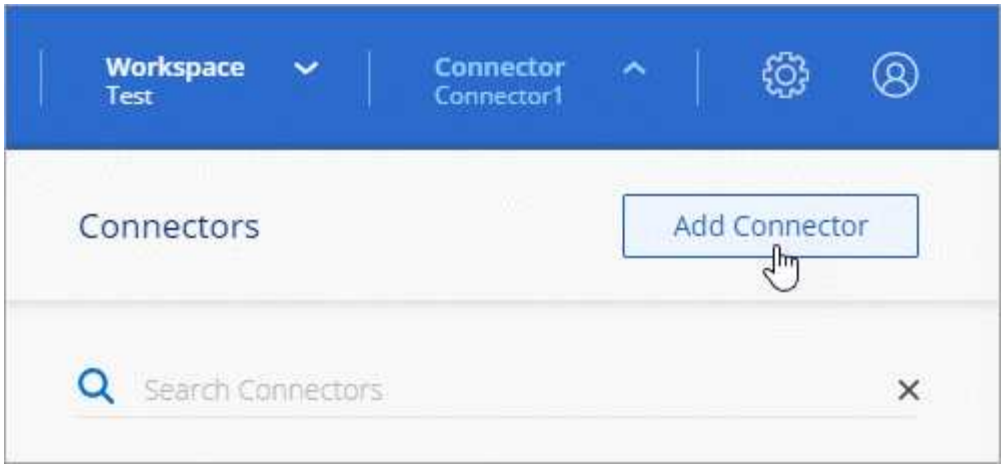
Avec Cloud Manager, vous pouvez créer un connecteur dans AWS directement depuis son interface utilisateur.

Ce dont vous avez besoin

- Une clé d'accès AWS et une clé secrète pour un utilisateur IAM qui dispose de la "autorisations requises".
- Un VPC, un sous-réseau et un keyair dans votre région AWS de votre choix.

Étapes

1. Si vous créez votre premier environnement de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites. Sinon, cliquez sur la liste déroulante **Connector** et sélectionnez **Add Connector**.



2. Cliquez sur **commençons**.
3. Choisissez **Amazon Web Services** comme fournisseur de cloud.

   Rappelez-vous que le connecteur doit disposer d'une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

   "En savoir plus sur les exigences de mise en réseau pour le connecteur".

4. Passez en revue ce dont vous aurez besoin et cliquez sur **Continuer**.
5. Fournissez les informations requises :
   - **Informations d'identification AWS** : saisissez un nom pour l'instance et spécifiez la clé d'accès AWS et la clé secrète qui répondent aux exigences d'autorisation.
   - **Location** : spécifiez une région AWS, un VPC et un sous-réseau pour l'instance.
   - **Réseau** : sélectionnez la paire de clés à utiliser avec l'instance, si vous souhaitez activer une adresse IP publique et spécifiez éventuellement une configuration proxy.
   - **Groupe de sécurité** : choisissez de créer ou non un nouveau groupe de sécurité ou de sélectionner un groupe de sécurité existant qui autorise l'accès HTTP, HTTPS et SSH entrant.

     Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez. HTTP et HTTPS permettent l'accès au "Interface utilisateur locale", que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

6. Cliquez sur **Créer**.

   L'instance doit être prête dans environ 7 minutes. Vous devez rester sur la page jusqu'à ce que le processus soit terminé.

Une fois que vous avez terminé

Vous devez associer un connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent utiliser ces connecteurs pour créer des systèmes Cloud Volumes ONTAP. Si vous ne disposez que d'administrateurs de compte, il n'est pas nécessaire d'associer le connecteur aux espaces de travail. Ils peuvent accéder par défaut à tous les espaces de travail dans Cloud Manager. "En savoir plus >>".

Création d'un connecteur dans Azure à partir de Cloud Manager

Un administrateur de compte doit déployer un *Connector* avant de pouvoir utiliser la plupart des fonctionnalités de Cloud Manager. "Apprenez quand un connecteur est nécessaire". Ce connecteur permet à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public.

Cette page explique comment créer un connecteur dans Azure directement depuis Cloud Manager. Vous avez également la possibilité de "Créez le connecteur à partir d'Azure Marketplace", ou à "téléchargez le logiciel et installez-le sur votre propre hôte".

Ces étapes doivent être réalisées par un utilisateur qui a le rôle d'administrateur de compte. Un administrateur d'espace de travail ne peut pas créer de connecteur.

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore créé.

Configuration des autorisations Azure pour créer un connecteur

Avant de déployer un connecteur depuis Cloud Manager, vous devez vous assurer que votre compte Azure dispose des autorisations appropriées.

Étapes

1. Créer un rôle personnalisé à l'aide de la politique Azure pour le connecteur :

   a. Téléchargez le "Règle Azure pour le connecteur".

      Cliquez avec le bouton droit de la souris sur le lien et cliquez sur **Enregistrer le lien sous…** pour télécharger le fichier.

   b. Modifiez le fichier JSON en ajoutant votre ID d'abonnement Azure à la portée attribuable.

      Exemple

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

   c. Utilisez le fichier JSON pour créer un rôle personnalisé dans Azure.

      L'exemple suivant montre comment créer un rôle personnalisé à l'aide de l'interface de ligne de commande Azure CLI 2.0 :

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

Vous devez maintenant avoir un rôle personnalisé appelé *Azure SetupAsService*.

2. Attribuez le rôle à l'utilisateur qui déploiera le connecteur à partir de Cloud Manager :
   a. Ouvrez le service **abonnements** et sélectionnez l'abonnement de l'utilisateur.
   b. Cliquez sur **contrôle d'accès (IAM)**.
   c. Cliquez sur **Ajouter** > **Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
      - Sélectionnez le rôle **Azure SetupAsService**.

        Azure SetupAsService est le nom par défaut fourni dans "Stratégie de déploiement de Connector pour Azure". Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

      - Attribuez l'accès à un utilisateur, groupe ou application AD **Azure**.
      - Sélectionnez le compte utilisateur.
      - Cliquez sur **Enregistrer**.

Résultat

L'utilisateur Azure dispose désormais des autorisations nécessaires pour déployer le connecteur à partir de Cloud Manager.

Création d'un connecteur dans Azure

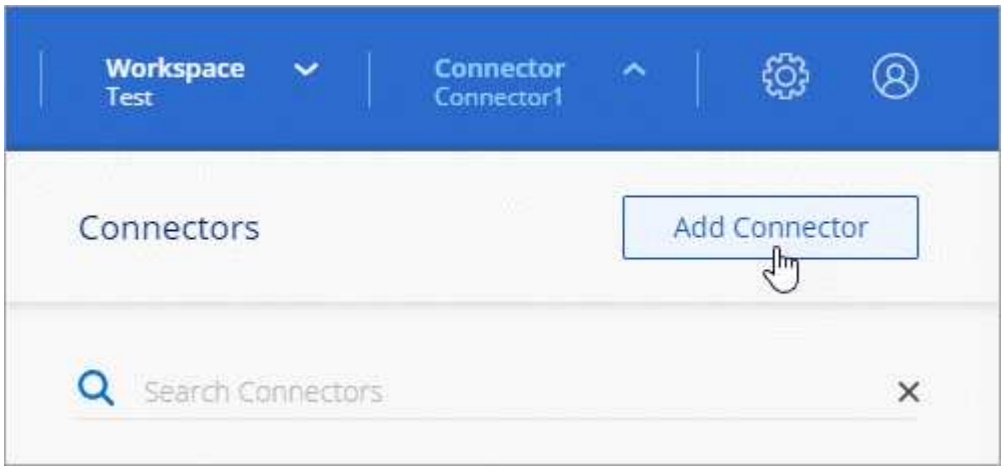
Cloud Manager vous permet de créer un connecteur dans Azure directement à partir de son interface utilisateur.

Ce dont vous avez besoin

- Le "autorisations requises" Pour votre compte Azure.
- Un abonnement Azure.
- Un vnet et un sous-réseau dans votre région Azure de votre choix.

Étapes

1. Si vous créez votre premier environnement de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites. Sinon, cliquez sur la liste déroulante **Connector** et sélectionnez **Add Connector**.



2. Cliquez sur **commençons**.
3. Choisissez **Microsoft Azure** comme fournisseur cloud.

Rappelez-vous que le connecteur doit disposer d'une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

"En savoir plus sur les exigences de mise en réseau pour le connecteur".

4. Passez en revue ce dont vous aurez besoin et cliquez sur **Continuer**.
5. Si vous y êtes invité, connectez-vous à votre compte Microsoft, qui devrait disposer des autorisations requises pour créer la machine virtuelle.

   Ce formulaire est détenu et hébergé par Microsoft. Vos identifiants ne sont pas fournis à NetApp.

   Si vous êtes déjà connecté à un compte Azure, Cloud Manager l'utilise automatiquement. Si vous avez plusieurs comptes, vous devrez peut-être vous déconnecter d'abord pour vous assurer que vous utilisez le bon compte.

6. Fournissez les informations requises :
   - **Authentification VM** : saisissez un nom pour la machine virtuelle ainsi qu'un nom d'utilisateur et un mot de passe ou une clé publique.
   - **Paramètres de base** : choisissez un abonnement Azure, une région Azure, et si vous souhaitez créer un nouveau groupe de ressources ou utiliser un groupe de ressources existant.
   - **Réseau** : choisissez un réseau VNet et un sous-réseau, si vous souhaitez activer une adresse IP publique, et spécifiez éventuellement une configuration proxy.
   - **Groupe de sécurité** : choisissez de créer ou non un nouveau groupe de sécurité ou de sélectionner un groupe de sécurité existant qui autorise l'accès HTTP, HTTPS et SSH entrant.

     Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez. HTTP et HTTPS permettent l'accès au "Interface utilisateur locale", que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

7. Cliquez sur **Créer**.

   La machine virtuelle doit être prête en 7 minutes environ. Vous devez rester sur la page jusqu'à ce que le processus soit terminé.

Une fois que vous avez terminé

Vous devez associer un connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent utiliser ces connecteurs pour créer des systèmes Cloud Volumes ONTAP. Si vous ne disposez que d'administrateurs de compte, il n'est pas nécessaire d'associer le connecteur aux espaces de travail. Ils peuvent accéder par défaut à tous les espaces de travail dans Cloud Manager. "En savoir plus >>".

Création d'un connecteur dans GCP à partir de Cloud Manager

Un administrateur de compte doit déployer un *Connector* avant de pouvoir utiliser la plupart des fonctionnalités de Cloud Manager. "Apprenez quand un connecteur est nécessaire". Ce connecteur permet à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public.

Cette page explique comment créer un connecteur dans GCP directement depuis Cloud Manager. Vous avez également la possibilité de "téléchargez le logiciel et installez-le sur votre propre hôte".

Ces étapes doivent être réalisées par un utilisateur qui a le rôle d'administrateur de compte. Un administrateur d'espace de travail ne peut pas créer de connecteur.

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore créé.

Configuration des autorisations GCP pour créer un connecteur

Avant de déployer un connecteur depuis Cloud Manager, vous devez vous assurer que votre compte GCP dispose des autorisations appropriées et qu'un compte de service est configuré pour la machine virtuelle Connector.

Étapes

1. Assurez-vous que l'utilisateur GCP qui déploie Cloud Manager à partir de NetApp Cloud Central dispose des autorisations dans le "Règle de déploiement du connecteur pour GCP".

   "Vous pouvez créer un rôle personnalisé à l'aide du fichier YAML" puis joignez-le à l'utilisateur. Vous devrez utiliser la ligne de commande gcloud pour créer le rôle.

2. Configurez un compte de service disposant des autorisations nécessaires à Cloud Manager pour créer et gérer des systèmes Cloud Volumes ONTAP dans des projets.

   Vous allez associer ce compte de service à la machine virtuelle Connector lorsque vous la créez à partir de Cloud Manager.

   a. "Créer un rôle dans GCP" qui inclut les autorisations définies dans le "Règle Cloud Manager pour GCP". Là encore, vous devrez utiliser la ligne de commande gcloud.

      Les autorisations contenues dans ce fichier YAML sont différentes des autorisations de l'étape 2a.

   b. "Créez un compte de service GCP et appliquez le rôle personnalisé que vous venez de créer".

   c. Si vous souhaitez déployer Cloud Volumes ONTAP dans d'autres projets, "Accordez l'accès en ajoutant le compte de service avec le rôle Cloud Manager à ce projet". Vous devrez répéter cette étape pour chaque projet.

Résultat

L'utilisateur GCP dispose désormais des autorisations nécessaires pour créer le connecteur depuis Cloud Manager et le compte de service de la machine virtuelle Connector est configuré.

Activation des API Google Cloud

Plusieurs API sont nécessaires pour déployer le connecteur et Cloud Volumes ONTAP.

Étape

1. "Activez les API Google Cloud suivantes dans votre projet".
   - API Cloud Deployment Manager V2
   - API de journalisation cloud
   - API Cloud Resource Manager

- API du moteur de calcul
- API de gestion des identités et des accès

Création d'un connecteur dans GCP

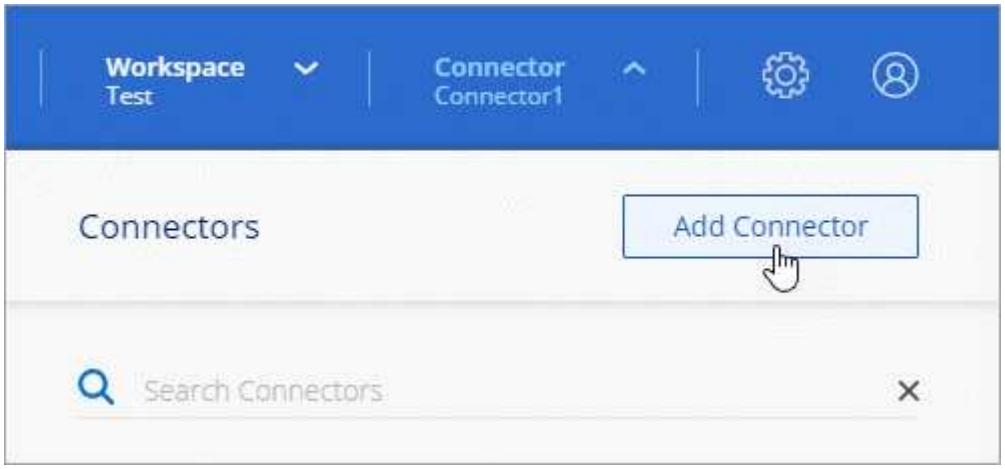
Avec Cloud Manager, vous pouvez créer un connecteur dans GCP directement à partir de son interface utilisateur.

Ce dont vous avez besoin

- Le "autorisations requises" Pour votre compte Google Cloud.
- Un projet Google Cloud.
- Compte de service disposant des autorisations requises pour créer et gérer Cloud Volumes ONTAP.
- VPC et sous-réseau dans votre région Google Cloud.

Étapes

1. Si vous créez votre premier environnement de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites. Sinon, cliquez sur la liste déroulante **Connector** et sélectionnez **Add Connector**.



2. Cliquez sur **commençons**.
3. Choisissez **Google Cloud Platform** comme fournisseur de cloud.

   Rappelez-vous que le connecteur doit disposer d'une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

   "En savoir plus sur les exigences de mise en réseau pour le connecteur".

4. Passez en revue ce dont vous aurez besoin et cliquez sur **Continuer**.
5. Si vous y êtes invité, connectez-vous à votre compte Google, qui devrait disposer des autorisations requises pour créer l'instance de machine virtuelle.

   Le formulaire est détenu et hébergé par Google. Vos identifiants ne sont pas fournis à NetApp.

6. Fournissez les informations requises :
   - **Paramètres de base** : saisissez un nom pour l'instance de machine virtuelle et spécifiez un compte de projet et de service disposant des autorisations requises.
   - **Location** : spécifiez une région, une zone, un VPC et un sous-réseau pour l'instance.

- **Réseau** : permet d'activer ou non une adresse IP publique et de spécifier éventuellement une configuration proxy.
- **Politique de pare-feu** : Choisissez si vous souhaitez créer une nouvelle politique de pare-feu ou si vous souhaitez sélectionner une politique de pare-feu existante qui autorise l'accès HTTP, HTTPS et SSH entrant.

> Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez. HTTP et HTTPS permettent l'accès au "Interface utilisateur locale", que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

7. Cliquez sur **Créer**.

   L'instance doit être prête dans environ 7 minutes. Vous devez rester sur la page jusqu'à ce que le processus soit terminé.

Une fois que vous avez terminé

Vous devez associer un connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent utiliser ces connecteurs pour créer des systèmes Cloud Volumes ONTAP. Si vous ne disposez que d'administrateurs de compte, il n'est pas nécessaire d'associer le connecteur aux espaces de travail. Ils peuvent accéder par défaut à tous les espaces de travail dans Cloud Manager. "En savoir plus >>".

Informations sur le copyright

Informations sur les marques commerciales