Administration de Cloud Manager

Cloud Manager 3.8

NetApp
March 25, 2024

Sommaire

Administration de Cloud Manager . . . 1
Recherche de l'ID système Cloud Manager . . . 1
Gérer les connecteurs . . . 1
Gérer les identifiants . . . 17
Gestion des utilisateurs, des espaces de travail, des connecteurs et des abonnements . . . 41
Gestion d'un certificat HTTPS pour l'accès sécurisé . . . 47
Suppression des environnements de travail Cloud Volumes ONTAP . . . 49
Configuration d'un connecteur pour utiliser un serveur proxy . . . 50
Remplacement des verrouillages CIFS pour Cloud Volumes ONTAP HA dans Azure . . . 51
Référence . . . 52

Administration de Cloud Manager

Recherche de l'ID système Cloud Manager

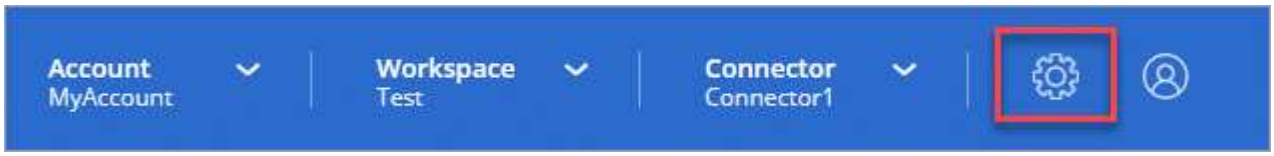
Pour vous aider à vous lancer, votre représentant NetApp peut vous demander votre identifiant de système Cloud Manager. L'ID est généralement utilisé à des fins de licence et de dépannage.

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres.



2. Cliquez sur **support Dashboard**.

   L'ID de votre système apparaît dans le coin supérieur droit.

   Exemple

Gérer les connecteurs

Gestion des connecteurs existants

Après avoir créé un ou plusieurs connecteurs, vous pouvez les gérer en passant d'un connecteur à l'autre, en vous connectant à l'interface utilisateur locale s'exécutant sur un connecteur, et plus encore.

Basculement entre les connecteurs

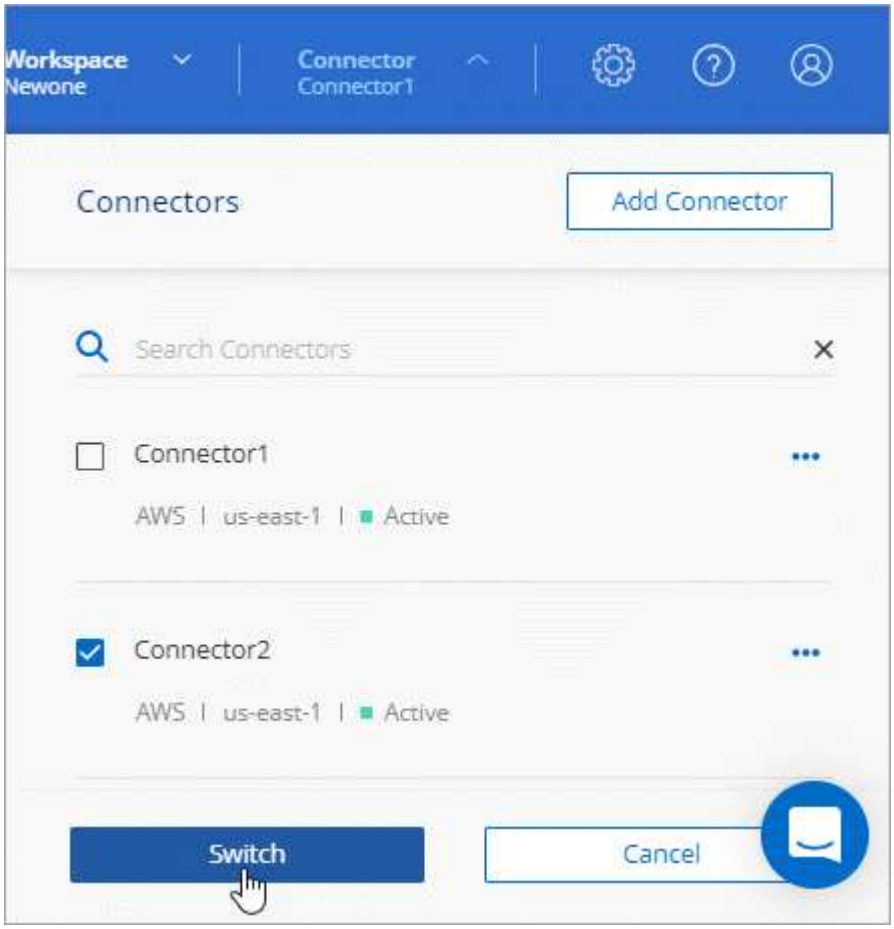
Si vous avez plusieurs connecteurs, vous pouvez passer de l'un à l'autre pour voir les environnements de travail associés à un connecteur spécifique.

Imaginons par exemple que vous travaillez dans un environnement multicloud. Vous avez peut-être un

connecteur dans AWS et un autre dans Google Cloud. Il faudrait basculer entre ces connecteurs pour gérer les systèmes Cloud Volumes ONTAP présents dans ces clouds.

Étape

1. Cliquez sur la liste déroulante **Connector**, sélectionnez un autre connecteur, puis cliquez sur **Switch**.



Cloud Manager actualise et affiche les environnements de travail associés au connecteur sélectionné.

Accès à 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. Cette interface est nécessaire pour quelques tâches qui doivent être effectuées à partir du connecteur lui-même :

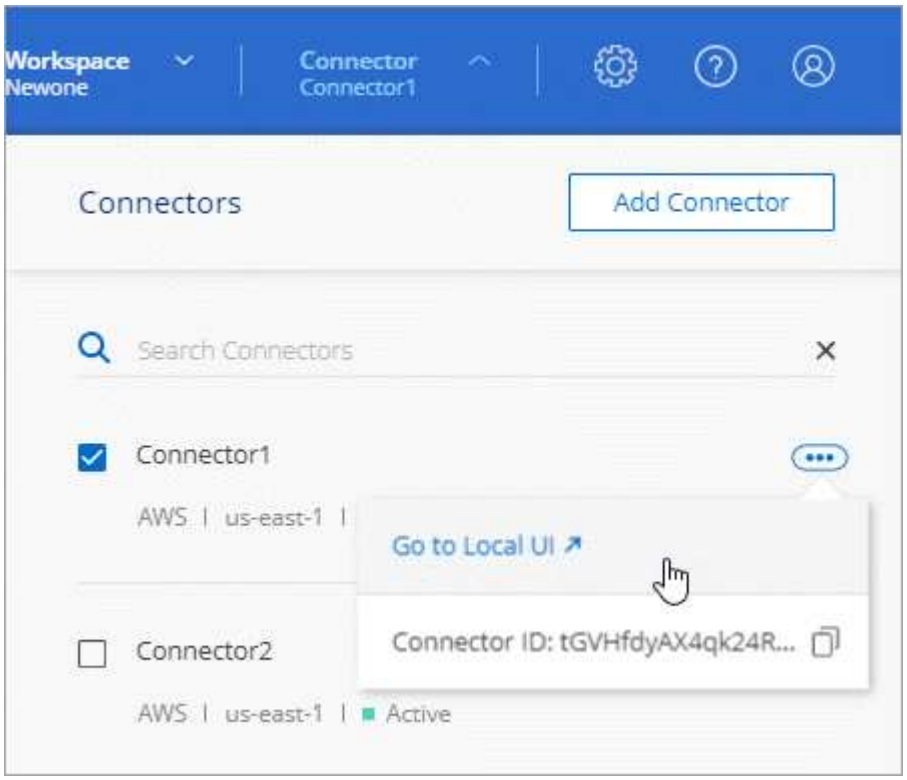
- "Configuration d'un serveur proxy"
- Installation d'un correctif (en général, vous travaillerez avec le personnel NetApp pour installer un correctif)
- Téléchargement de messages AutoSupport (généralement dirigés par le personnel NetApp en cas de problème)

Étapes

1. "Connectez-vous à l'interface SaaS Cloud Manager" À partir d'une machine dotée d'une connexion réseau à l'instance de connecteur.

   Si le connecteur n'est pas doté d'une adresse IP publique, vous aurez besoin d'une connexion VPN ou vous devrez vous connecter à partir d'un hôte de secours situé sur le même réseau que le connecteur.

2. Cliquez sur la liste déroulante **Connector**, cliquez sur le menu d'action d'un connecteur, puis cliquez sur **allez à l'interface utilisateur locale**.



L'interface Cloud Manager exécutée sur le connecteur est chargée dans un nouvel onglet du navigateur.

Retrait de connecteurs de Cloud Manager

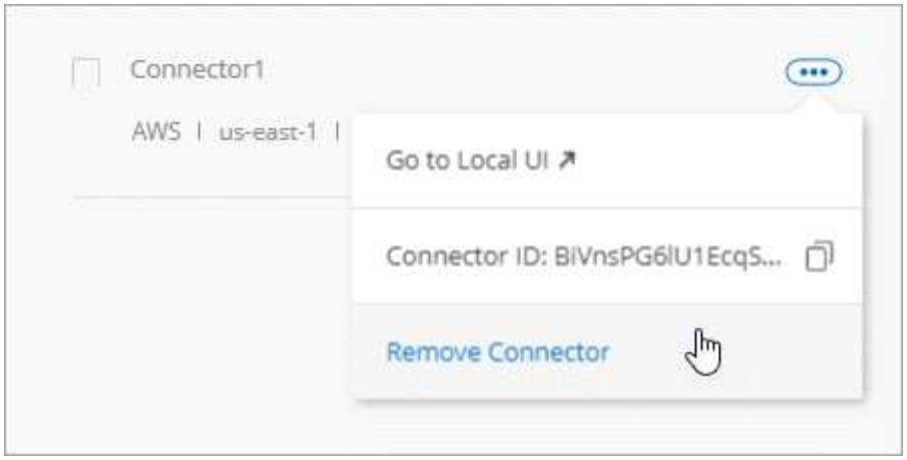
Si un connecteur est inactif, vous pouvez le supprimer de la liste des connecteurs dans Cloud Manager. Vous pouvez le faire si vous avez supprimé la machine virtuelle Connector ou si vous avez désinstallé le logiciel Connector.

Notez ce qui suit sur le retrait d'un connecteur :

- Cette action ne supprime pas la machine virtuelle.
- Cette action ne peut pas être rétablie, car une fois que vous avez supprimé un connecteur de Cloud Manager, vous ne pouvez pas le réintégrer.

Étapes

1. Dans la liste déroulante connecteur, cliquez sur l'en-tête Cloud Manager.
2. Cliquez sur le menu d'action d'un connecteur inactif et cliquez sur **Supprimer le connecteur**.



3. Entrez le nom du connecteur à confirmer, puis cliquez sur Supprimer.

Résultat

Cloud Manager élimine le connecteur de ses enregistrements.

Désinstallation du logiciel du connecteur

Le connecteur inclut un script de désinstallation que vous pouvez utiliser pour désinstaller le logiciel pour résoudre des problèmes ou pour supprimer définitivement le logiciel de l'hôte.

Étape

1. À partir de l'hôte Linux, exécutez le script de désinstallation :

   /opt/application/netapp/cloudmanager/bin/uninstall.sh [silencieux]

   silent exécute le script sans vous demander de confirmer.

Qu'en est-il des mises à niveau logicielles

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.

Autres façons de créer des connecteurs

Exigences relatives à l'hôte de connecteur

Le logiciel du connecteur doit être exécuté sur un hôte qui répond à des exigences spécifiques du système d'exploitation, de la RAM, des ports, etc.

Un hôte dédié est requis

Le connecteur n'est pas pris en charge sur un hôte partagé avec d'autres applications. L'hôte doit être un hôte dédié.

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Type d'instance AWS EC2

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons une instance t3.XLarge d'utiliser ce type d'instance lorsque vous déployez le connecteur directement depuis Cloud Manager.

Taille des machines virtuelles Azure

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons la version DS3 v2 et d'utiliser cette taille de machine virtuelle lorsque vous déployez le connecteur directement depuis Cloud Manager.

Type de machine GCP

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons n1-standard-4 et d'utiliser ce type de machine lorsque vous déployez le connecteur directement depuis Cloud Manager.

Systèmes d'exploitation pris en charge

- CentOS 7.6
- CentOS 7.7
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7

  Le système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis pendant l'installation du connecteur.

  Le connecteur est pris en charge sur les versions en anglais de ces systèmes d'exploitation.

Hyperviseur

Un hyperviseur bare Metal ou hébergé certifié pour exécuter CentOS ou Red Hat Enterprise Linuxhttps://access.redhat.com/certified-hypervisors["Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"^]

Espace disque dans /opt

100 Go d'espace doivent être disponibles

Accès Internet sortant

Un accès Internet sortant est nécessaire pour installer le connecteur et pour que le connecteur gère les ressources et les processus au sein de votre environnement de cloud public. Pour obtenir la liste des noeuds finaux, reportez-vous à la section "Exigences de mise en réseau pour le connecteur".

Création d'un connecteur à partir d'AWS Marketplace

Il est préférable de créer un connecteur directement depuis Cloud Manager, mais vous pouvez lancer un connecteur depuis AWS Marketplace, si vous ne souhaitez pas spécifier de clés d'accès AWS. Une fois que vous avez créé et configuré ce connecteur, Cloud Manager l'utilise automatiquement lors de la création de nouveaux environnements de travail.

Étapes

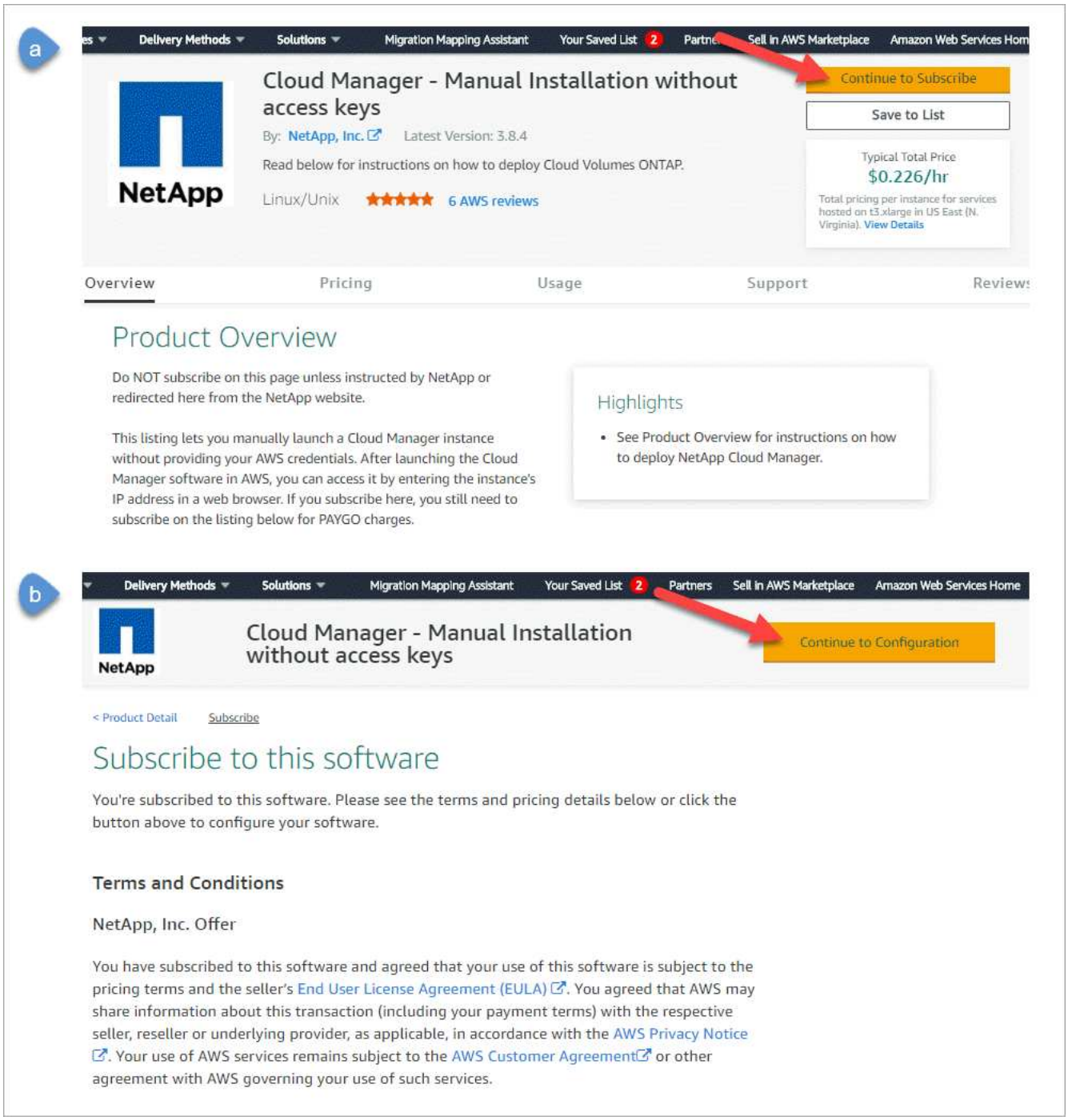
1. Créer une règle IAM et un rôle pour l'instance EC2 :
   a. Téléchargez la politique IAM de Cloud Manager à partir de l'emplacement suivant :

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

   b. À partir de la console IAM, créez votre propre stratégie en copiant et en collant le texte de la stratégie IAM de Cloud Manager.
   c. Créez un rôle IAM avec le type de rôle Amazon EC2 et associez la stratégie que vous avez créée à l'étape précédente au rôle.
2. Maintenant, allez au "Page Cloud Manager sur AWS Marketplace" Pour déployer Cloud Manager à partir d'une ami.

   L'utilisateur IAM doit disposer d'autorisations AWS Marketplace pour vous abonner et se désabonner.

3. Sur la page Marketplace, cliquez sur **Continuer pour s'abonner**, puis cliquez sur **Continuer la configuration**.



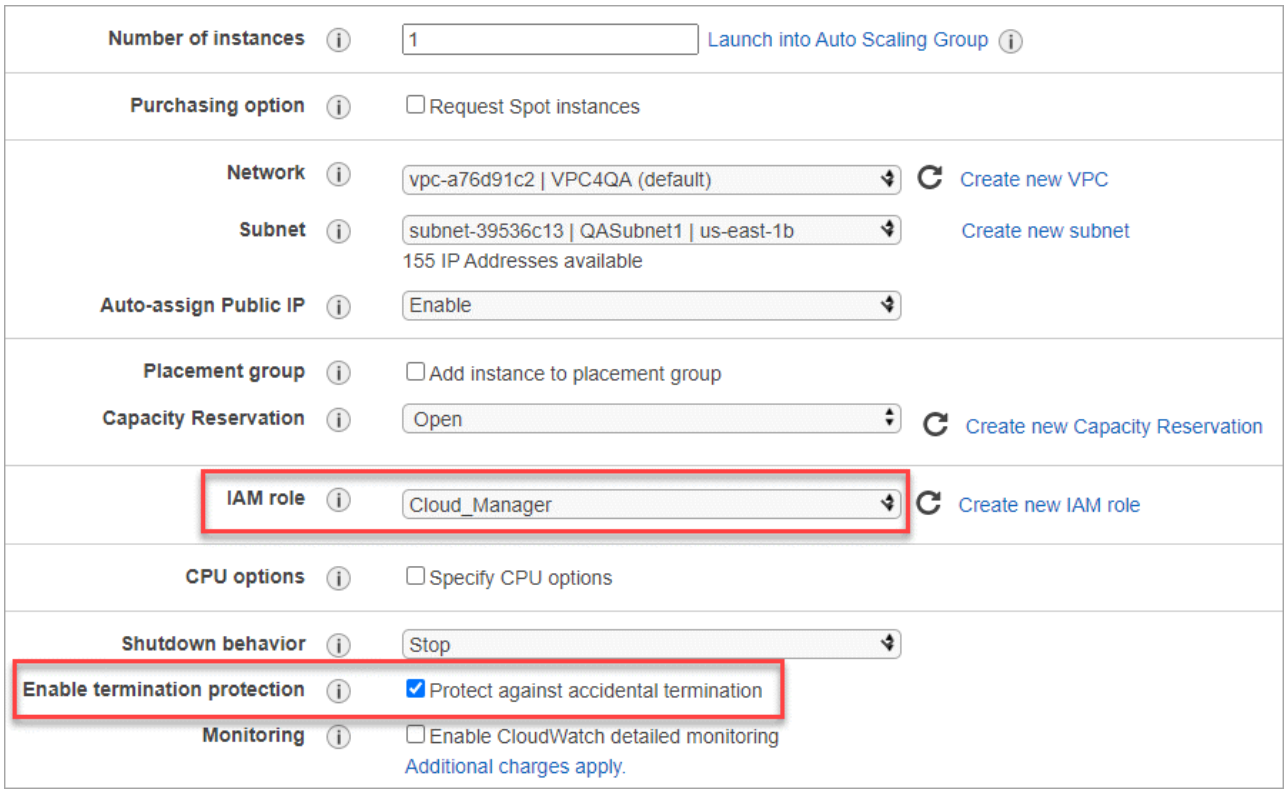
4. Modifiez l'une des options par défaut et cliquez sur **Continuer pour lancer**.
5. Sous **choisir action**, sélectionnez **lancer via EC2**, puis cliquez sur **lancer**.

   Ces étapes expliquent comment lancer l'instance à partir de la console EC2, car la console vous permet d'associer un rôle IAM à l'instance Cloud Manager. Cela n'est pas possible en utilisant l'action **lancer à partir du site Web**.

6. Suivez les invites pour configurer et déployer l'instance :
   - **Choisissez le type d'instance** : selon la disponibilité de la région, choisissez l'un des types d'instance pris en charge (t3.XLarge est recommandé).

     "Vérifiez les conditions requises pour l'instance".

- **Configurer l'instance** : sélectionnez un VPC et un sous-réseau, choisissez le rôle IAM que vous avez créé à l'étape 1, activez la protection de terminaison (recommandée) et choisissez toutes les autres options de configuration qui répondent à vos exigences.



- **Ajouter stockage** : conservez les options de stockage par défaut.
- **Ajouter des balises** : saisissez des balises pour l'instance, si vous le souhaitez.
- **Configurer le groupe de sécurité** : spécifiez les méthodes de connexion requises pour l'instance de connecteur : SSH, HTTP et HTTPS.
- **Revue**: Passez en revue vos sélections et cliquez sur **lancer**.

  AWS lance le logiciel avec les paramètres spécifiés. L'instance de connecteur et le logiciel doivent s'exécuter dans environ cinq minutes.

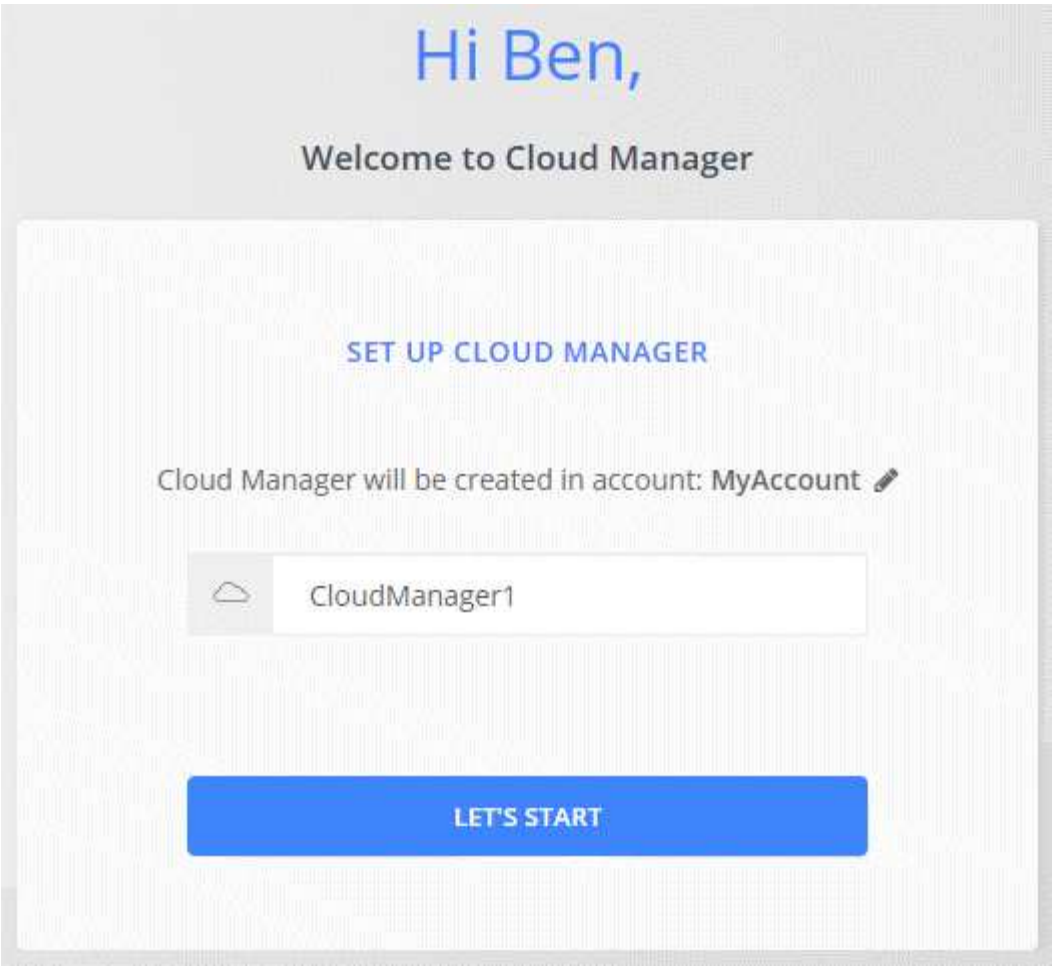
7. Ouvrez un navigateur Web à partir d'un hôte connecté à l'instance Connector et saisissez l'URL suivante :

   http://ipaddress:80

8. Une fois connecté, configurez le connecteur :
   a. Spécifiez le compte Cloud Central à associer au connecteur.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Résultat

Le connecteur est maintenant installé et configuré avec votre compte Cloud Central. Cloud Manager utilisera automatiquement ce connecteur lors de la création de nouveaux environnements de travail. Mais si vous avez plus d'un connecteur, vous devrez le faire "basculer entre eux".

Création d'un connecteur à partir d'Azure Marketplace

Il est préférable de créer un connecteur directement depuis Cloud Manager, mais vous pouvez également lancer un connecteur depuis Azure Marketplace, si vous préférez. Une fois que vous avez créé et configuré ce connecteur, Cloud Manager l'utilise automatiquement lors de la création de nouveaux environnements de travail.

Création d'un connecteur dans Azure

Déployez le connecteur dans Azure en utilisant l'image dans Azure Marketplace, puis connectez-vous au connecteur pour spécifier votre compte Cloud Central.

Étapes

1. "Accédez à la page Azure Marketplace pour Cloud Manager".
2. Cliquez sur **l'obtenir maintenant**, puis sur **Continuer**.
3. Sur le portail Azure, cliquez sur **Créer** et suivez les étapes de configuration de la machine virtuelle.

   Noter les éléments suivants lors de la configuration de la machine virtuelle :

- Cloud Manager peut fonctionner de manière optimale avec des disques durs ou SSD.
- Choisissez une taille de machine virtuelle qui répond aux exigences en matière de CPU et de RAM. Nous recommandons DS3 v2.

  "Vérifier les exigences relatives aux machines virtuelles".

- Pour le groupe de sécurité réseau, le connecteur nécessite des connexions entrantes via SSH, HTTP et HTTPS.

  "En savoir plus sur les règles de groupe de sécurité pour le connecteur".

- Sous **Management**, activez **l'identité gérée attribuée par le système** pour le connecteur en sélectionnant **On**.

  Ce paramètre est important car une identité gérée permet à la machine virtuelle Connector de s'identifier à Azure Active Directory sans fournir d'informations d'identification. "En savoir plus sur les identités gérées pour les ressources Azure".

4. Dans la page **Revue + créer**, vérifiez vos sélections et cliquez sur **Créer** pour démarrer le déploiement.

   Azure déploie la machine virtuelle avec les paramètres spécifiés. Le logiciel de la machine virtuelle et du connecteur doit s'exécuter en cinq minutes environ.

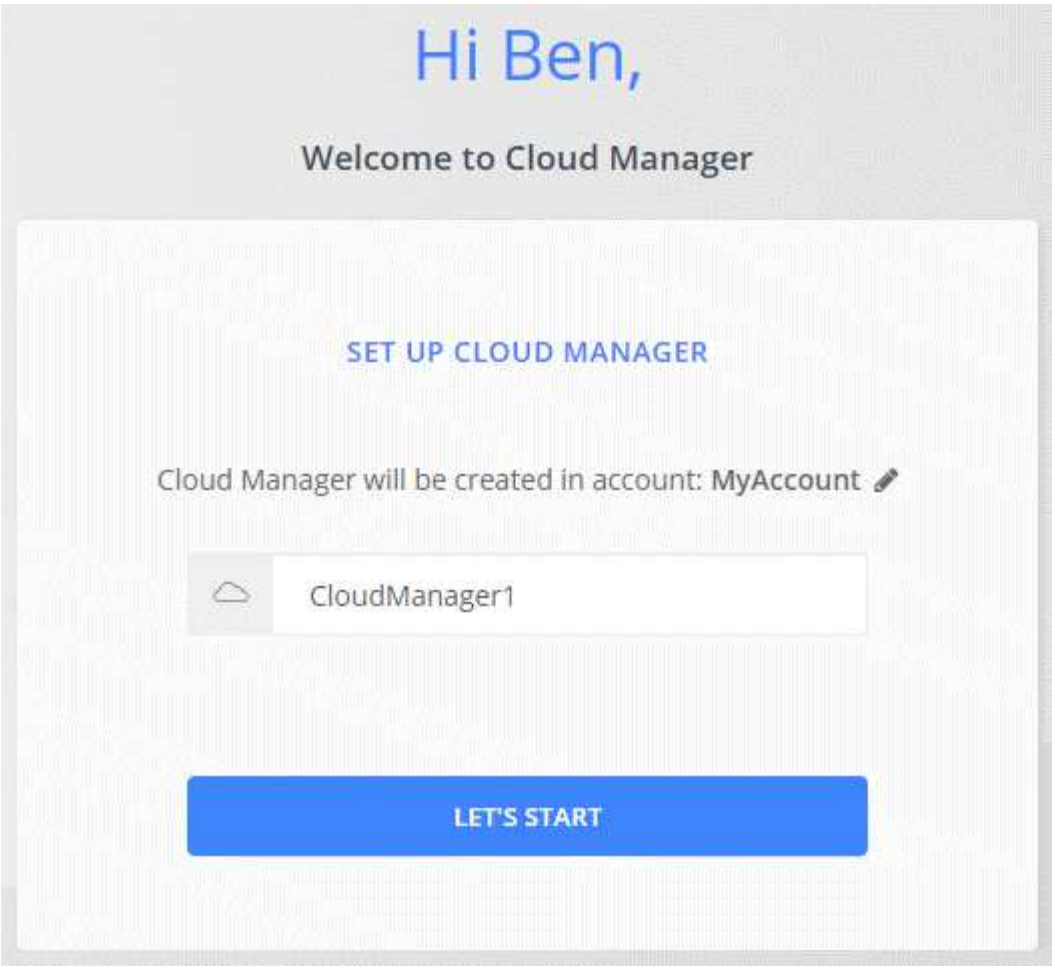
5. Ouvrez un navigateur Web à partir d'un hôte connecté à la machine virtuelle Connector et entrez l'URL suivante :

   http://ipaddress:80

6. Une fois connecté, configurez le connecteur :
   a. Spécifiez le compte Cloud Central à associer au connecteur.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Résultat

Le connecteur est maintenant installé et configuré. Vous devez accorder des autorisations Azure avant que les utilisateurs puissent déployer Cloud Volumes ONTAP dans Azure.

Octroi d'autorisations Azure

Lorsque vous avez déployé le connecteur dans Azure, vous devez avoir activé un "identité gérée attribuée par le système". Vous devez maintenant accorder les autorisations Azure requises en créant un rôle personnalisé, puis en attribuant le rôle à la machine virtuelle Connector pour un ou plusieurs abonnements.

Étapes

1. Créez un rôle personnalisé à l'aide de la stratégie Cloud Manager :

   a. Téléchargez le "Politique de Cloud Manager Azure".

   b. Modifiez le fichier JSON en ajoutant des identifiants d'abonnement Azure à l'étendue assignable.

      Vous devez ajouter l'ID de chaque abonnement Azure à partir duquel les utilisateurs créeront des systèmes Cloud Volumes ONTAP.

      Exemple

      « Assigner les Scopes » : [»/abonnements/d333af45-0d07-4154-943d-c25fbzzzzzzzzzz »,
      «/abonnements/54b91999-b3e6-4599-908e-416e0zzzzzz », «/abonnements/8e474b-94b-4b-4b-4b-4b-4439-4b-4b-4b-4b-4b-4b-4b-4b-4b-4b-

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_cloud_Manager_Azure_3.8.7.json
   ```

Vous devez maintenant avoir un rôle personnalisé appelé opérateur Cloud Manager que vous pouvez attribuer à la machine virtuelle Connector.

2. Attribuez le rôle à la machine virtuelle Connector pour un ou plusieurs abonnements :
   a. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer des systèmes Cloud Volumes ONTAP.
   b. Cliquez sur **contrôle d'accès (IAM)**.
   c. Cliquez sur **Ajouter** > **Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
      - Sélectionnez le rôle **opérateur** de Cloud Manager.

        L'opérateur de Cloud Manager est le nom par défaut fourni dans "Politique de Cloud Manager". Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

      - Attribuez l'accès à une **machine virtuelle**.
      - Sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée.
      - Sélectionnez la machine virtuelle Connector.
      - Cliquez sur **Enregistrer**.
   d. Si vous souhaitez déployer Cloud Volumes ONTAP à partir d'abonnements supplémentaires, passez à cet abonnement, puis répétez ces étapes.

Résultat

Le connecteur dispose désormais des autorisations nécessaires pour gérer les ressources et les processus au sein de votre environnement de cloud public. Cloud Manager utilisera automatiquement ce connecteur lors de la création de nouveaux environnements de travail. Mais si vous avez plus d'un connecteur, vous devrez le faire "basculer entre eux".

Installation du logiciel de connecteur sur un hôte Linux existant

La méthode la plus courante pour créer un connecteur consiste à partir de Cloud Manager ou du Marketplace d'un fournisseur cloud. Mais vous avez la possibilité de télécharger et d'installer le logiciel Connector sur un hôte Linux existant de votre réseau ou dans le cloud.

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.

De formation

- L'hôte doit se réunir "Configuration requise pour le connecteur".
- Un système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il

n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis pendant l'installation.

- Le programme d'installation du connecteur accède à plusieurs URL pendant le processus d'installation. Vous devez vous assurer que l'accès Internet sortant est autorisé à ces noeuds finaux :
  - 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.

Description de la tâche

- Les privilèges root ne sont pas nécessaires pour installer le connecteur.
- L'installation installe les outils de ligne de commande AWS (awscli), afin d'activer les procédures de reprise à partir du support NetApp.

  Si vous recevez un message indiquant que l'installation de awscli a échoué, vous pouvez ignorer le message en toute sécurité. Le connecteur peut fonctionner sans outils.

- Le programme d'installation disponible sur le site du support NetApp peut être une version antérieure. Après l'installation, le connecteur se met automatiquement à jour si une nouvelle version est disponible.

Étapes

1. Téléchargez le logiciel Cloud Manager sur le "Site de support NetApp", Puis copiez-le sur l'hôte Linux.

   Pour obtenir de l'aide sur la connexion et la copie du fichier vers une instance EC2 dans AWS, reportez-vous à la section "Documentation AWS : connexion à votre instance Linux à l'aide de SSH".

2. Attribuez des autorisations pour exécuter le script.

   Exemple

   ```
    chmod +x OnCommandCloudManager-V3.8.4.sh
   . Exécutez le script d'installation :
   ```

   ```
   ./OnCommandCloudManager-V3.8.4.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent exécute l'installation sans vous demander des informations.

   proxy est requis si l'hôte est derrière un serveur proxy.

   proxyport est le port du serveur proxy.

   proxyuser est le nom d'utilisateur du serveur proxy, si une authentification de base est requise.

   proxypwd est le mot de passe du nom d'utilisateur que vous avez spécifié.

3. Sauf si vous avez spécifié le paramètre silencieux, tapez **y** pour continuer le script, puis entrez les ports HTTP et HTTPS lorsque vous y êtes invité.

   Cloud Manager est maintenant installé. À la fin de l'installation, le service Cloud Manager (occm) redémarre deux fois si vous avez spécifié un serveur proxy.

4. Ouvrez un navigateur Web et entrez l'URL suivante :

   https://ipaddress:port

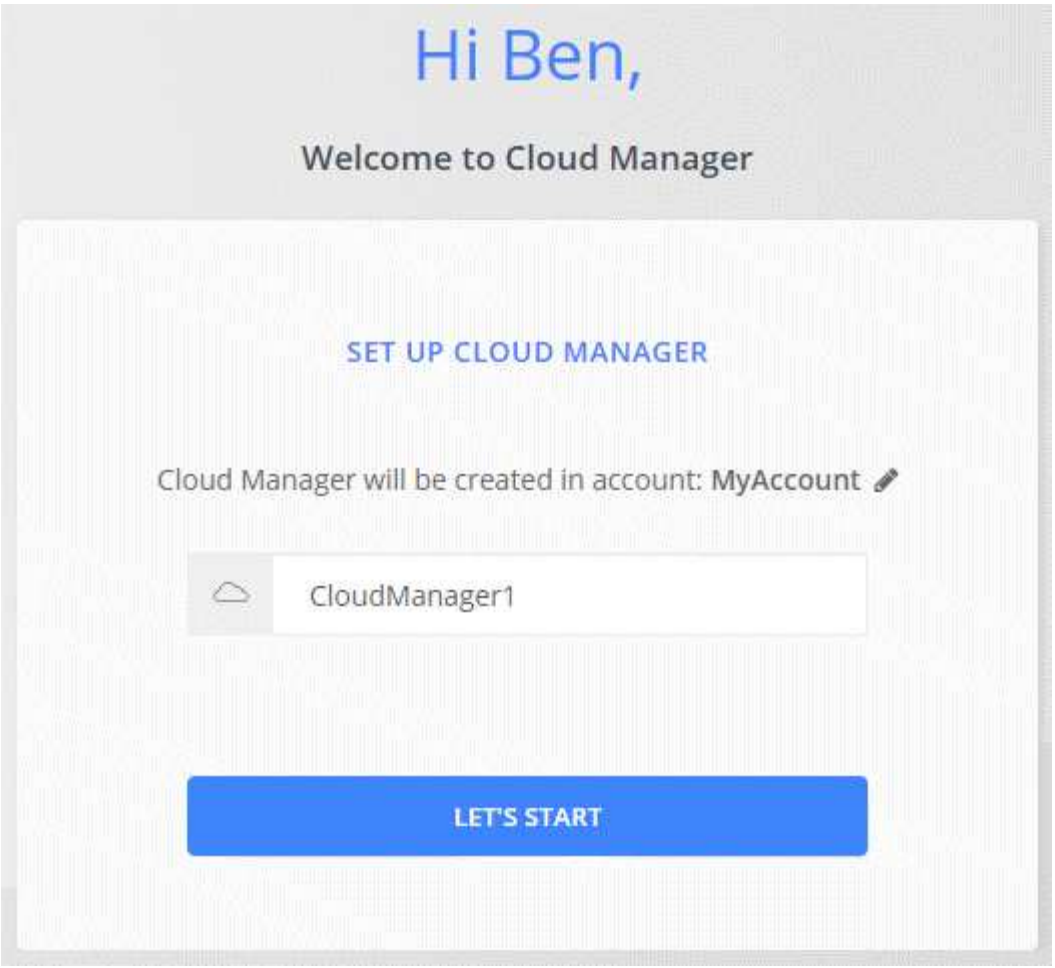
   Ipaddress peut être localhost, une adresse IP privée ou une adresse IP publique, selon la configuration de l'hôte. Par exemple, si le connecteur est dans le Cloud public sans adresse IP publique, vous devez entrer une adresse IP privée à partir d'un hôte qui a une connexion à l'hôte du connecteur.

   Port est nécessaire si vous avez modifié les ports HTTP (80) ou HTTPS (443) par défaut. Par exemple, si le port HTTPS a été modifié en 8443, vous pouvez entrer https://ipaddress:8443

5. Inscrivez-vous sur NetApp Cloud Central ou connectez-vous.
6. Une fois connecté, configurez Cloud Manager :
   a. Spécifiez le compte Cloud Central à associer au connecteur.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Résultat

Le connecteur est maintenant installé et configuré avec votre compte Cloud Central. Cloud Manager utilisera automatiquement ce connecteur lors de la création de nouveaux environnements de travail.

Une fois que vous avez terminé

Configurez des autorisations pour que Cloud Manager puisse gérer les ressources et les processus dans votre environnement de cloud public :

- AWS : "Configurez un compte AWS, puis ajoutez-le à Cloud Manager".
- Azure : "Configurez un compte Azure, puis ajoutez-le à Cloud Manager".
- GCP : configurez un compte de service disposant des autorisations nécessaires à Cloud Manager pour créer et gérer des systèmes Cloud Volumes ONTAP dans des projets.
  a. "Créer un rôle dans GCP" qui inclut les autorisations définies dans le "Règle Cloud Manager pour GCP".
  b. "Créez un compte de service GCP et appliquez le rôle personnalisé que vous venez de créer".
  c. "Associer ce compte de service à la VM Connector".
  d. 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.

Configuration par défaut du connecteur

Si vous devez dépanner le connecteur, il peut vous aider à comprendre sa configuration.

- Si vous avez déployé le connecteur depuis Cloud Manager (ou directement depuis le Marketplace d'un fournisseur cloud), remarque :
  - Dans AWS, le nom d'utilisateur de l'instance Linux EC2 est ec2-user.
  - Le système d'exploitation de l'image est le suivant :
    - AWS : Red Hat Enterprise Linux 7.5 (HVM)
    - Azure : Red Hat Enterprise Linux 7.6 (HVM)
    - GCP : CentOS 7.6

      Le système d'exploitation n'inclut pas d'interface graphique. Vous devez utiliser un terminal pour accéder au système.
- Le dossier d'installation du connecteur se trouve à l'emplacement suivant :

  /opt/application/netapp/cloudmanager
- Les fichiers journaux se trouvent dans le dossier suivant :

  /opt/application/netapp/cloudmanager/log
- Le service Cloud Manager s'appelle occm.
- Le service occm dépend du service MySQL.

  Si le service MySQL est en panne, le service occm est également en panne.
- Cloud Manager installe les packages suivants sur l'hôte Linux, s'ils ne sont pas déjà installés :
  - 7Zip
  - AWSCLI
  - Docker
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Tirer
  - Wget
- Le connecteur utilise les ports suivants sur l'hôte Linux :
  - 80 pour l'accès HTTP
  - 443 pour l'accès HTTPS
  - 3306 pour la base de données Cloud Manager
  - 8080 pour le proxy API Cloud Manager
  - 8666 pour l'API du Gestionnaire de services

◦ 8777 pour l'API du service de conteneurs Health-Checker

Gérer les identifiants

AWS

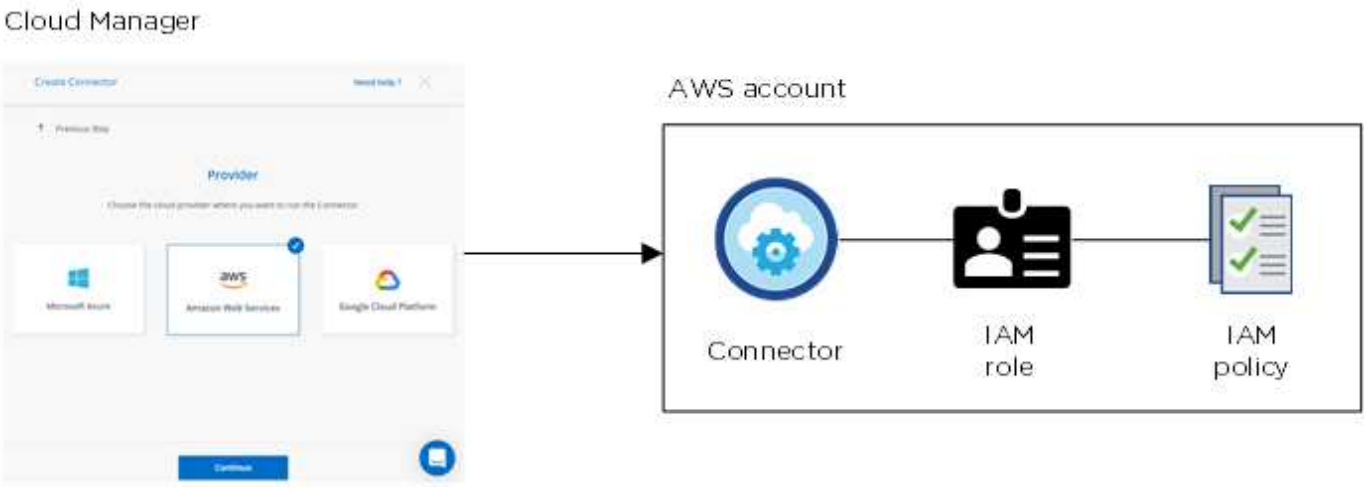
Identifiants et autorisations AWS

Cloud Manager vous permet de choisir les identifiants AWS à utiliser lors du déploiement de Cloud Volumes ONTAP. Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des identifiants AWS initiaux, ou ajouter des identifiants supplémentaires.

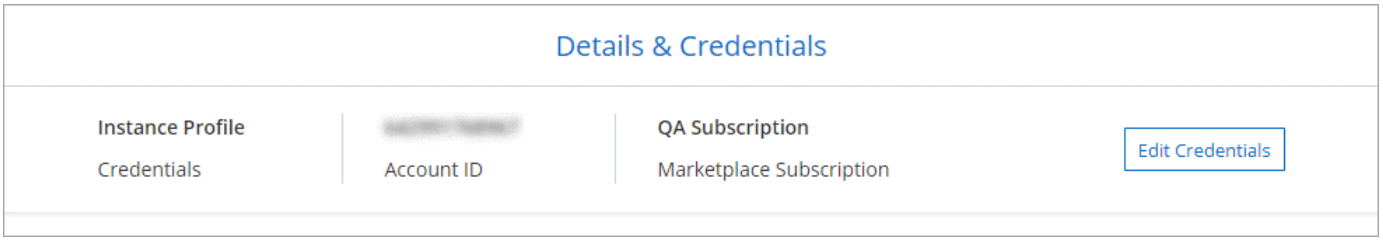
Identifiants AWS initiaux

Lorsque vous déployez un connecteur depuis Cloud Manager, vous devez utiliser un compte AWS avec des autorisations pour lancer l'instance de connecteur. Les autorisations requises sont répertoriées dans le "Règle de déploiement du connecteur pour AWS".

Lorsque Cloud Manager lance l'instance de connecteur dans AWS, il crée un rôle IAM et un profil d'instance pour l'instance. Il attache également une règle qui fournit les autorisations nécessaires à Cloud Manager pour gérer les ressources et les processus de ce compte AWS. "Examinez comment Cloud Manager utilise les autorisations".



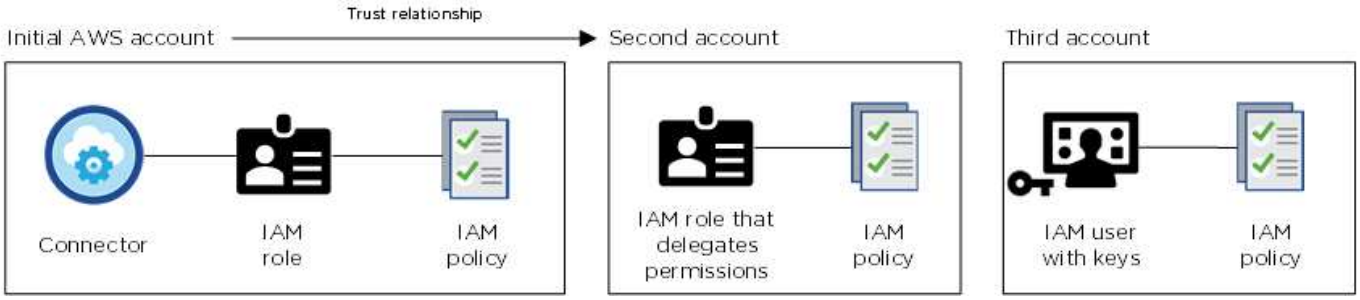
Cloud Manager sélectionne ces identifiants AWS par défaut lorsque vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP :



Autres identifiants AWS

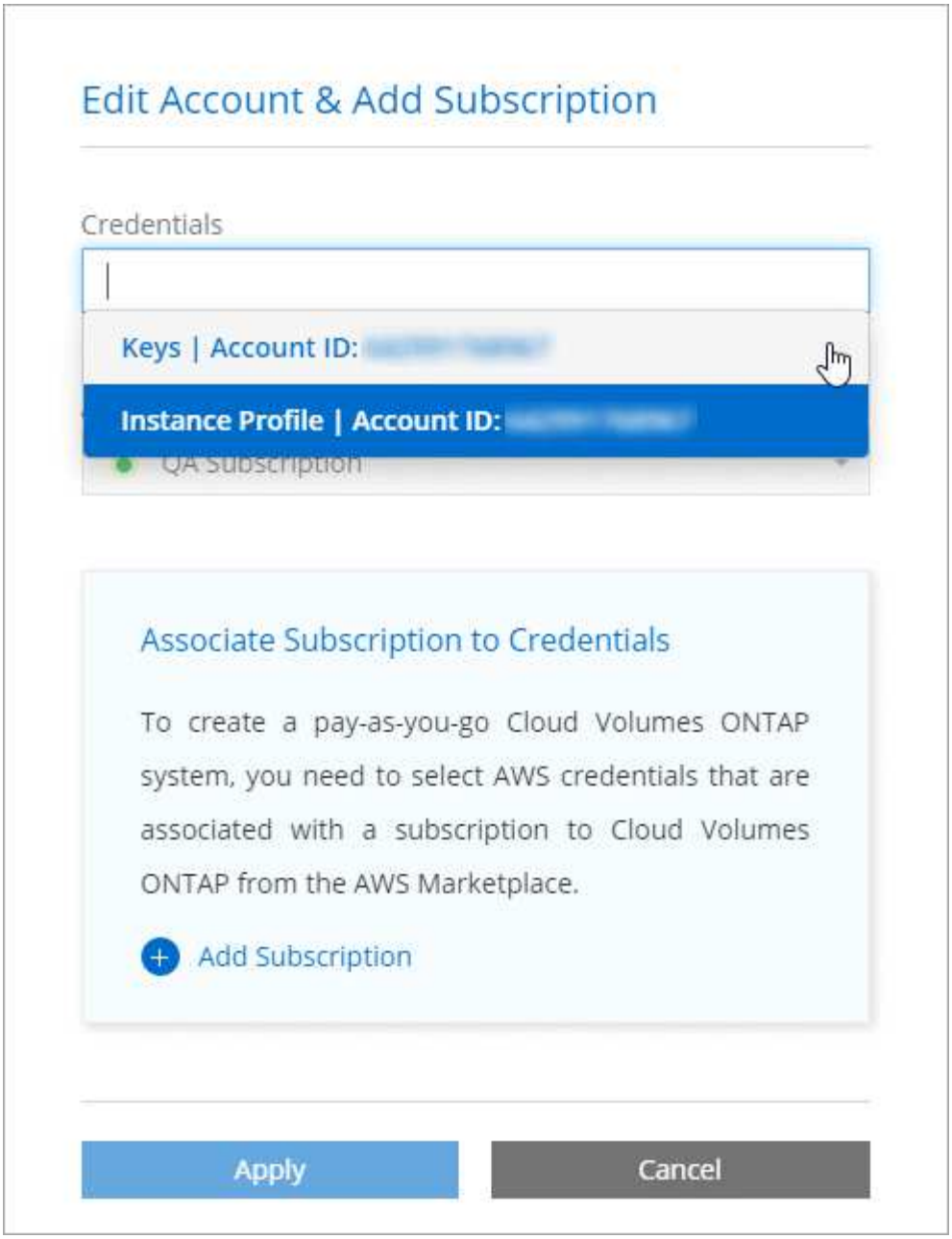
Si vous souhaitez lancer Cloud Volumes ONTAP sur différents comptes AWS, vous pouvez l'un ou l'autre "Fournir des clés AWS pour un utilisateur IAM ou le numéro ARN d'un rôle dans un compte de confiance".

L’image suivante montre deux comptes supplémentaires, l’un avec des autorisations par le biais d’un rôle IAM dans un compte de confiance et l’autre avec les clés AWS d’un utilisateur IAM :



Vous le feriez alors "Ajoutez les identifiants du compte à Cloud Manager" En spécifiant le nom de ressource Amazon (ARN) du rôle IAM ou les clés AWS pour l’utilisateur IAM.

Après avoir ajouté un autre ensemble d’informations d’identification, vous pouvez les passer lors de la création d’un nouvel environnement de travail :



Qu'en est-il des déploiements Marketplace et des déploiements sur site ?

Dans les sections ci-dessus, nous décrivons la méthode de déploiement recommandée pour le connecteur, qui provient de Cloud Manager. Vous pouvez également déployer un connecteur dans AWS à partir du "AWS Marketplace" et vous le pouvez "Installer le connecteur sur site".

Si vous utilisez Marketplace, des autorisations sont fournies de la même manière. Il vous suffit de créer et de configurer manuellement le rôle IAM, puis de fournir des autorisations pour tous les comptes supplémentaires.

Pour les déploiements sur site, vous ne pouvez pas configurer de rôle IAM pour le système Cloud Manager, mais vous pouvez fournir des autorisations exactement comme vous le feriez pour d'autres comptes AWS.

Comment faire tourner mes identifiants AWS en toute sécurité ?

Comme décrit ci-dessus, Cloud Manager vous permet de fournir des identifiants AWS de différentes manières : un rôle IAM associé à l'instance Connector, en assumant un rôle IAM dans un compte de confiance ou en

fournissant des clés d'accès AWS.

Avec les deux premières options, Cloud Manager utilise le service de token de sécurité AWS pour obtenir des identifiants temporaires qui pivotent en permanence. Ce processus est la meilleure pratique—il automatique et sécurisé.

Si vous fournissez les clés d'accès AWS à Cloud Manager, il est conseillé de les mettre à jour régulièrement dans Cloud Manager. Il s'agit d'un processus entièrement manuel.

Gestion des identifiants AWS et des abonnements pour Cloud Manager

Lorsque vous créez un système Cloud Volumes ONTAP, vous devez sélectionner les identifiants AWS et l'abonnement à utiliser avec ce système. Si vous gérez plusieurs abonnements AWS, vous pouvez les attribuer à différentes informations d'identification AWS à partir de la page informations d'identification.

Avant d'ajouter des identifiants AWS à Cloud Manager, vous devez fournir les autorisations requises pour ce compte. Les autorisations permettent à Cloud Manager de gérer les ressources et les processus de ce compte AWS. La manière dont vous fournissez les autorisations dépend de votre choix si vous souhaitez fournir Cloud Manager avec des clés AWS ou le NRA d'un rôle dans un compte de confiance.

Lorsque vous avez déployé un connecteur depuis Cloud Manager, Cloud Manager a automatiquement ajouté des identifiants AWS pour le compte dans lequel vous avez déployé le connecteur. Ce compte initial n'est pas ajouté si vous avez installé manuellement le logiciel Connector sur un système existant. "En savoir plus sur les identifiants et les autorisations AWS".

Choix

- Octroi d'autorisations en fournissant des clés AWS
- Octroi d'autorisations en assumant des rôles IAM dans d'autres comptes

Comment faire tourner mes identifiants AWS en toute sécurité ?

Cloud Manager vous permet de fournir des identifiants AWS de quelques façons : un rôle IAM associé à l'instance Connector, en assumant un rôle IAM dans un compte de confiance ou en fournissant des clés d'accès AWS. "En savoir plus sur les identifiants et les autorisations AWS".

Avec les deux premières options, Cloud Manager utilise le service de token de sécurité AWS pour obtenir des identifiants temporaires qui pivotent en permanence. Ce processus est la meilleure pratique, il est automatique et sécurisé.

Si vous fournissez les clés d'accès AWS à Cloud Manager, il est conseillé de les mettre à jour régulièrement dans Cloud Manager. Il s'agit d'un processus entièrement manuel.

Octroi d'autorisations en fournissant des clés AWS

Si vous souhaitez fournir Cloud Manager avec des clés AWS pour un utilisateur IAM, vous devez accorder les autorisations requises à cet utilisateur. La stratégie IAM de Cloud Manager définit les actions et les ressources AWS que Cloud Manager est autorisé à utiliser.

Étapes

1. Téléchargez la politique IAM de Cloud Manager à partir du "Page Cloud Manager Policies".
2. À partir de la console IAM, créez votre propre stratégie en copiant et en collant le texte de la stratégie IAM de Cloud Manager.

   "Documentation AWS : création de règles IAM"

3. Joignez la politique à un rôle IAM ou à un utilisateur IAM.
   - "Documentation AWS : création de rôles IAM"
   - "Documentation AWS : ajout et suppression de règles IAM"

Résultat

Le compte dispose désormais des autorisations requises. Vous pouvez désormais l'ajouter à Cloud Manager.

Octroi d'autorisations en assumant des rôles IAM dans d'autres comptes

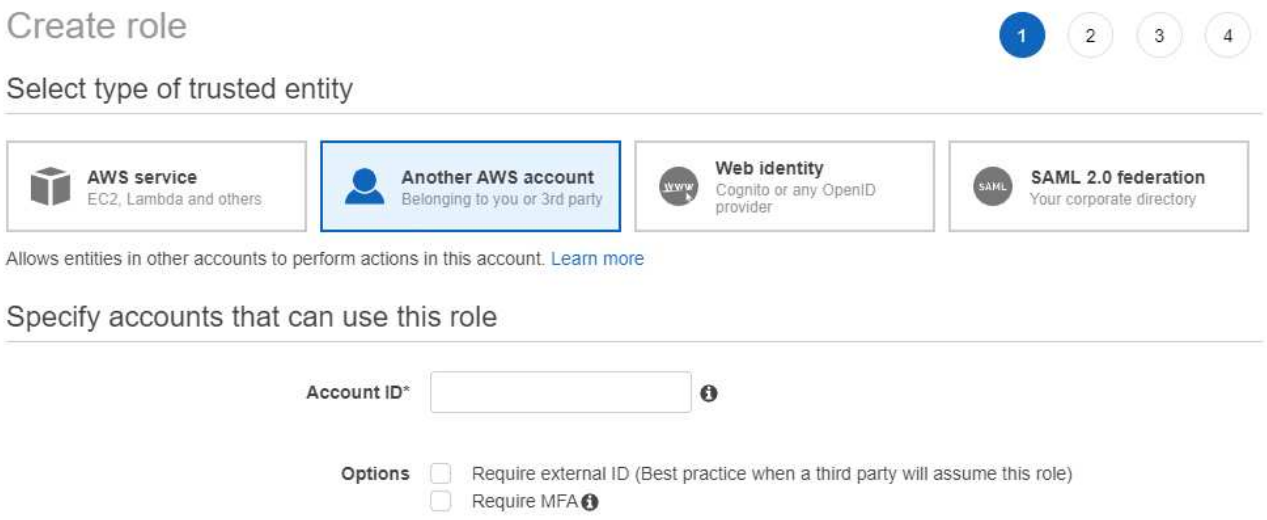
Vous pouvez définir une relation de confiance entre le compte AWS source dans lequel vous avez déployé l'instance Connector et d'autres comptes AWS en utilisant les rôles IAM. Vous pouvez ensuite fournir à Cloud Manager l'ARN des rôles IAM depuis les comptes de confiance.

Étapes

1. Accédez au compte cible sur lequel vous souhaitez déployer Cloud Volumes ONTAP et créez un rôle IAM en sélectionnant **un autre compte AWS**.

   Assurez-vous de faire ce qui suit :

   - Saisissez l'ID du compte sur lequel réside l'instance de connecteur.
   - Joignez la politique IAM de Cloud Manager, disponible à partir du "Page Cloud Manager Policies".



2. Accédez au compte source où se trouve l'instance de connecteur et sélectionnez le rôle IAM associé à l'instance.

   a. Cliquez sur **attacher des stratégies**, puis sur **Créer une stratégie**.

   b. Créez une stratégie qui inclut l'action « sts:AssumeRole » et l'ARN du rôle que vous avez créé dans le compte cible.

Exemple

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

Résultat

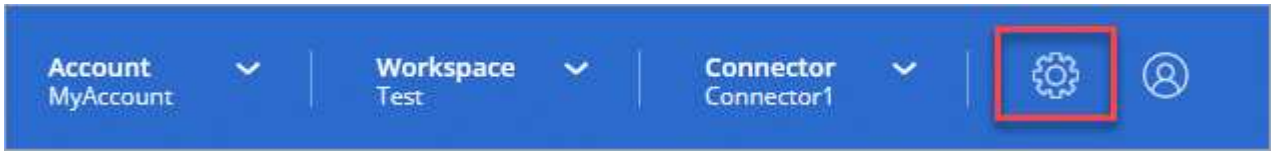
Le compte dispose désormais des autorisations requises. Vous pouvez désormais l'ajouter à Cloud Manager.

Ajout d'identifiants AWS à Cloud Manager

Une fois que vous avez passé un compte AWS avec les autorisations requises, vous pouvez ajouter les identifiants de ce compte à Cloud Manager. Vous pouvez ainsi lancer les systèmes Cloud Volumes ONTAP de ce compte.

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



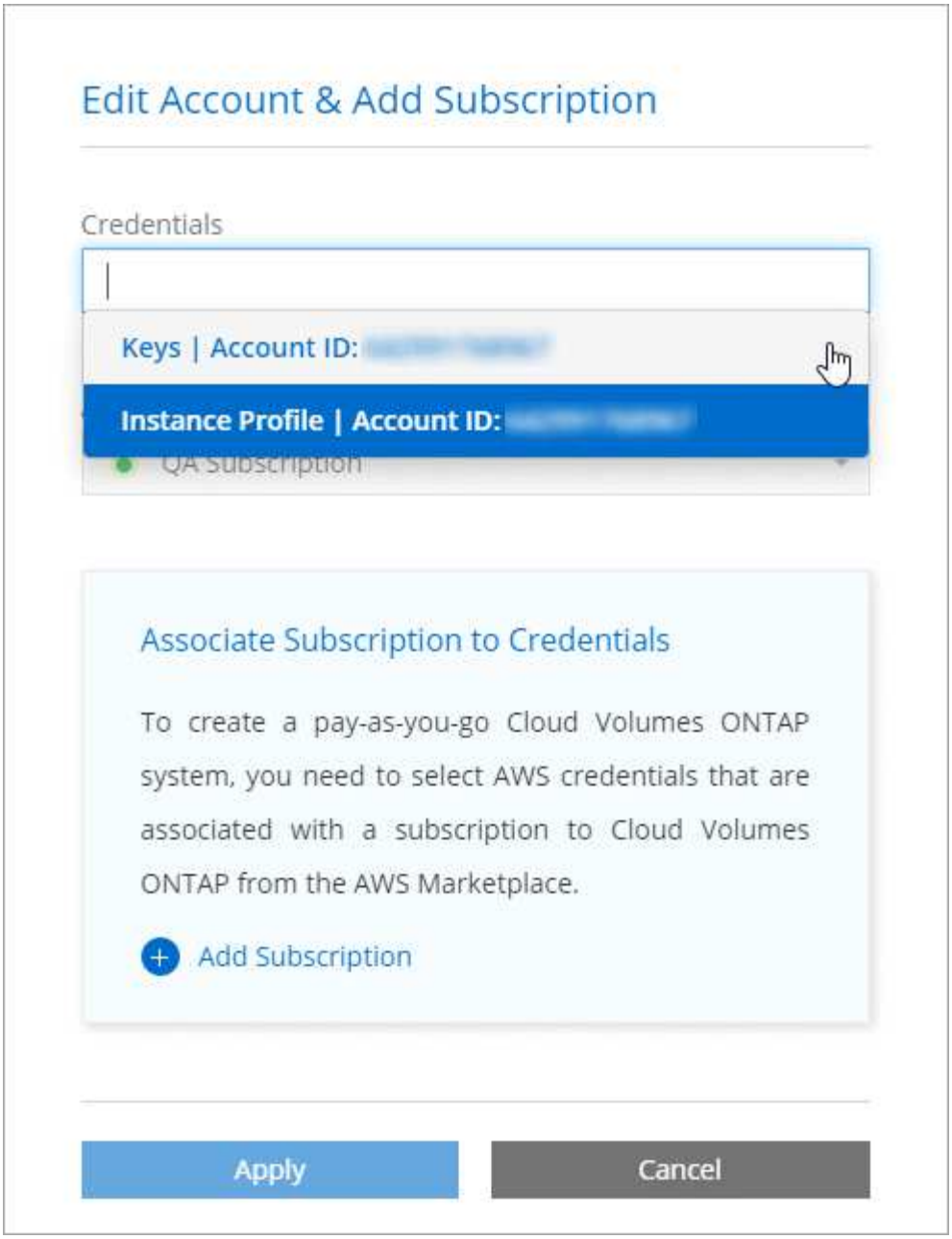
2. Cliquez sur **Ajouter des informations d'identification** et sélectionnez **AWS**.
3. Vous pouvez fournir des clés AWS ou l'ARN d'un rôle IAM approuvé.
4. Vérifiez que les exigences de la politique ont été respectées et cliquez sur **Continuer**.
5. Choisissez l'abonnement payant à l'utilisation que vous souhaitez associer aux informations d'identification ou cliquez sur **Ajouter un abonnement** si vous n'en avez pas encore.

   Pour créer un système Cloud Volumes ONTAP avec paiement à l'utilisation, vous devez associer des identifiants AWS à un abonnement à Cloud Volumes ONTAP à partir d'AWS Marketplace.

6. Cliquez sur **Ajouter**.

Résultat

Vous pouvez maintenant passer à un autre ensemble d'informations d'identification à partir de la page Détails et informations d'identification lors de la création d'un nouvel environnement de travail :



Association d'un abonnement AWS aux identifiants

Après avoir ajouté vos identifiants AWS à Cloud Manager, vous pouvez associer un abonnement AWS Marketplace à ces identifiants. Cet abonnement vous permet de créer un système Cloud Volumes ONTAP basé sur l'utilisation et d'utiliser d'autres services cloud NetApp.

Deux scénarios peuvent vous être associés à un abonnement AWS Marketplace une fois que vous avez déjà ajouté les identifiants à Cloud Manager :

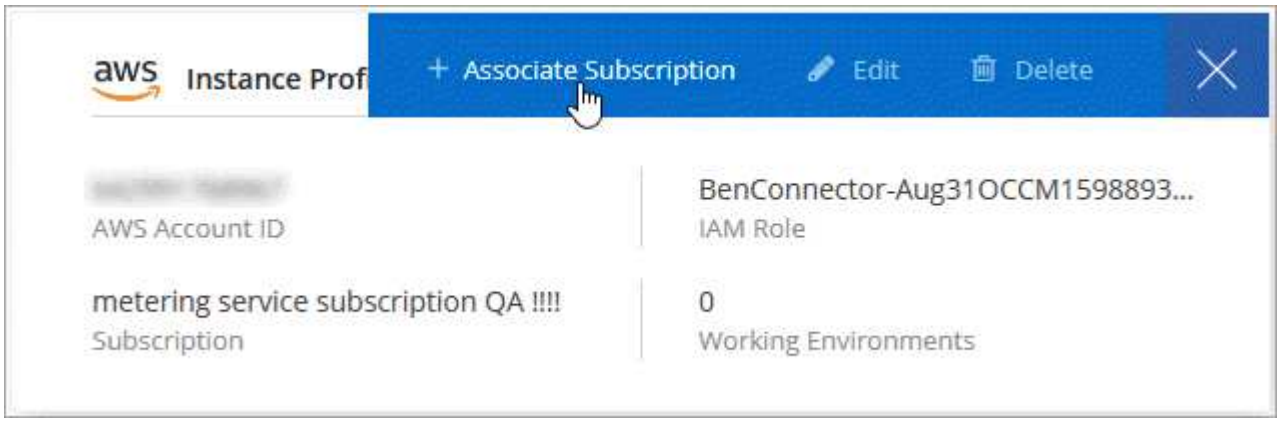
- Vous n'avez pas associé un abonnement lors de l'ajout initial des identifiants à Cloud Manager.
- Vous souhaitez remplacer un abonnement AWS Marketplace existant par un nouvel abonnement.

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Passez le curseur de la souris sur un ensemble d'informations d'identification et cliquez sur le menu d'action.
3. Dans le menu, cliquez sur **associer abonnement**.



4. Sélectionnez un abonnement dans la liste déroulante ou cliquez sur **Ajouter un abonnement** et suivez les étapes pour créer un nouvel abonnement.

   ► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_aws.mp4 *(video)*

Azure

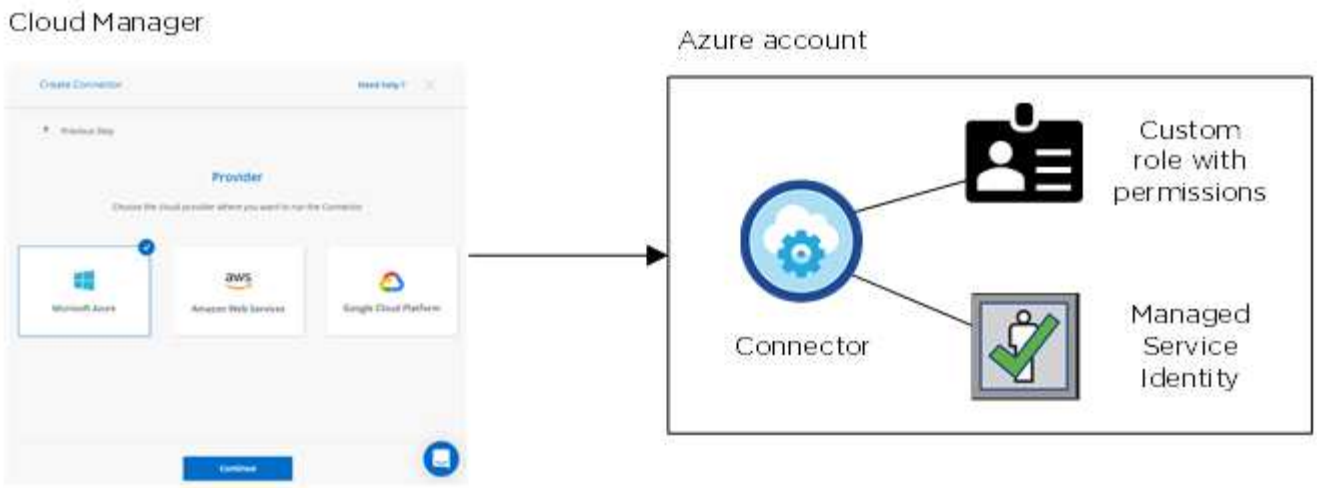
Identifiants et autorisations Azure

Cloud Manager vous permet de choisir les identifiants Azure à utiliser lors du déploiement de Cloud Volumes ONTAP. Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des identifiants Azure initiaux, ou ajouter des identifiants supplémentaires.

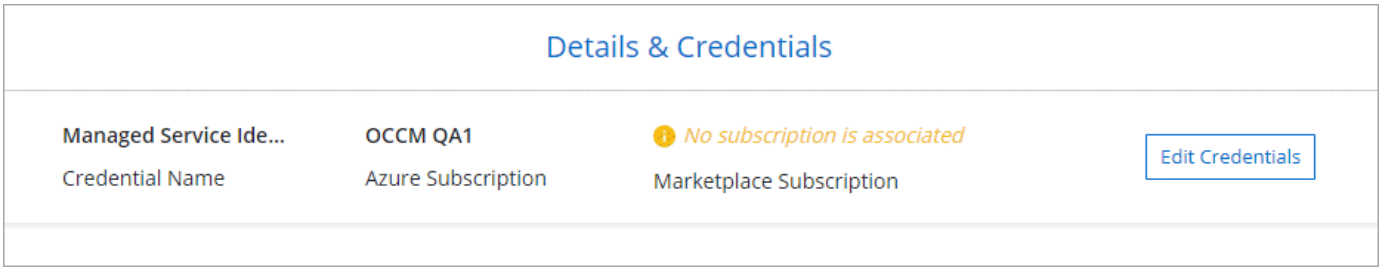
Les identifiants initiaux d'Azure

Lorsque vous déployez un connecteur depuis Cloud Manager, vous devez utiliser un compte Azure avec les autorisations de déployer la machine virtuelle Connector. Les autorisations requises sont répertoriées dans le "Stratégie de déploiement de Connector pour Azure".

Lorsque Cloud Manager déploie la machine virtuelle de connecteur dans Azure, il active une "identité gérée attribuée par le système" sur une machine virtuelle, crée un rôle personnalisé et le attribue à la machine virtuelle. Le rôle fournit à Cloud Manager des autorisations de gestion des ressources et des processus au sein de cet abonnement Azure. "Examinez comment Cloud Manager utilise les autorisations".



Cloud Manager sélectionne ces identifiants Azure par défaut lorsque vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP :

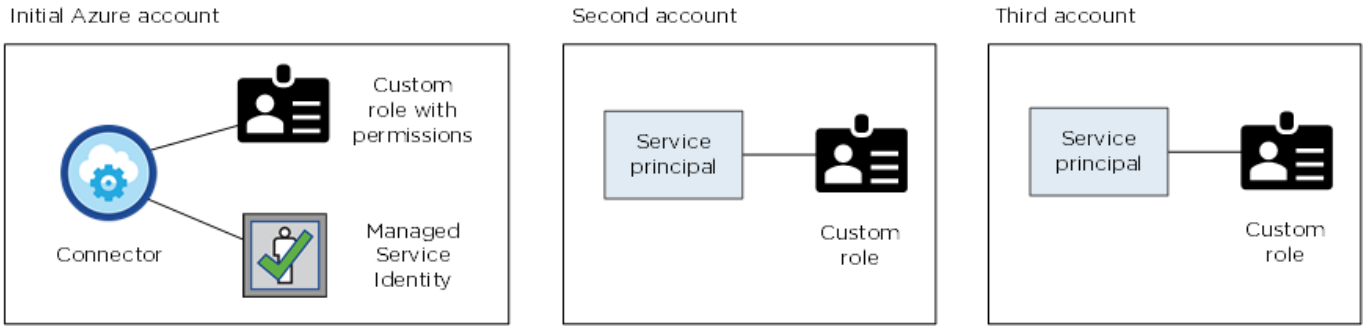


Des abonnements Azure supplémentaires pour une identité gérée

L'identité gérée est associée à l'abonnement dans lequel vous avez lancé le connecteur. Si vous souhaitez sélectionner un autre abonnement Azure, vous devez le faire "associez l'identité gérée à ces abonnements".

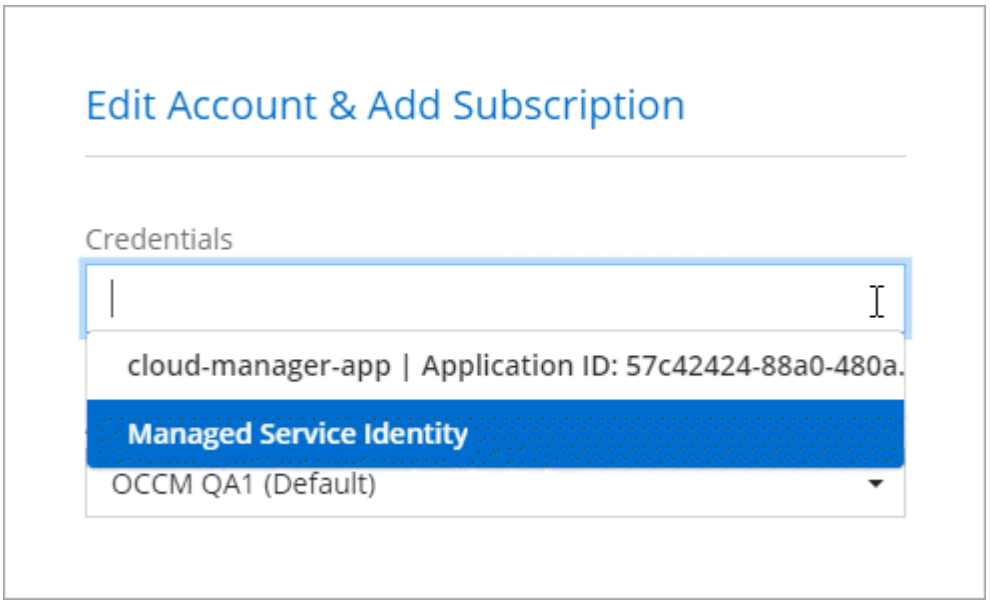
Autres identifiants Azure

Si vous souhaitez déployer Cloud Volumes ONTAP avec différents identifiants Azure, vous devez accorder les autorisations requises par "Création et configuration d'une entité de service dans Azure Active Directory" Pour chaque compte Azure. L'image suivante montre deux comptes supplémentaires, chacun étant doté d'un rôle principal de service et personnalisé qui fournit des autorisations :



Vous le feriez alors "Ajoutez les identifiants du compte à Cloud Manager" En fournissant des détails sur le principal du service AD.

Après avoir ajouté un autre ensemble d'informations d'identification, vous pouvez les passer lors de la création d'un nouvel environnement de travail :



Qu'en est-il des déploiements Marketplace et des déploiements sur site ?

Les sections ci-dessus décrivent la méthode de déploiement recommandée pour le connecteur, qui provient de NetApp Cloud Central. Vous pouvez également déployer un connecteur dans Azure à partir du "Azure Marketplace", et vous pouvez "Installer le connecteur sur site".

Si vous utilisez Marketplace, des autorisations sont fournies de la même manière. Il vous suffit de créer et de configurer manuellement l'identité gérée pour le connecteur, puis de fournir des autorisations pour tous les comptes supplémentaires.

Pour les déploiements sur site, vous ne pouvez pas configurer une identité gérée pour le connecteur, mais vous pouvez fournir des autorisations comme vous le feriez pour des comptes supplémentaires en utilisant une entité de service.

Gestion des identifiants Azure et des abonnements pour Cloud Manager

Lorsque vous créez un système Cloud Volumes ONTAP, vous devez sélectionner les identifiants Azure et l'abonnement Marketplace pour les utiliser avec ce système. Si vous gérez plusieurs abonnements Azure Marketplace, vous pouvez les attribuer à différentes informations d'identification Azure à partir de la page informations d'identification.

Il existe deux façons de gérer les identifiants Azure dans Cloud Manager. Tout d'abord, si vous souhaitez déployer Cloud Volumes ONTAP sur différents comptes Azure, vous devez fournir les autorisations requises et ajouter les identifiants à Cloud Manager. La deuxième méthode consiste à associer des abonnements supplémentaires à l'identité gérée Azure.

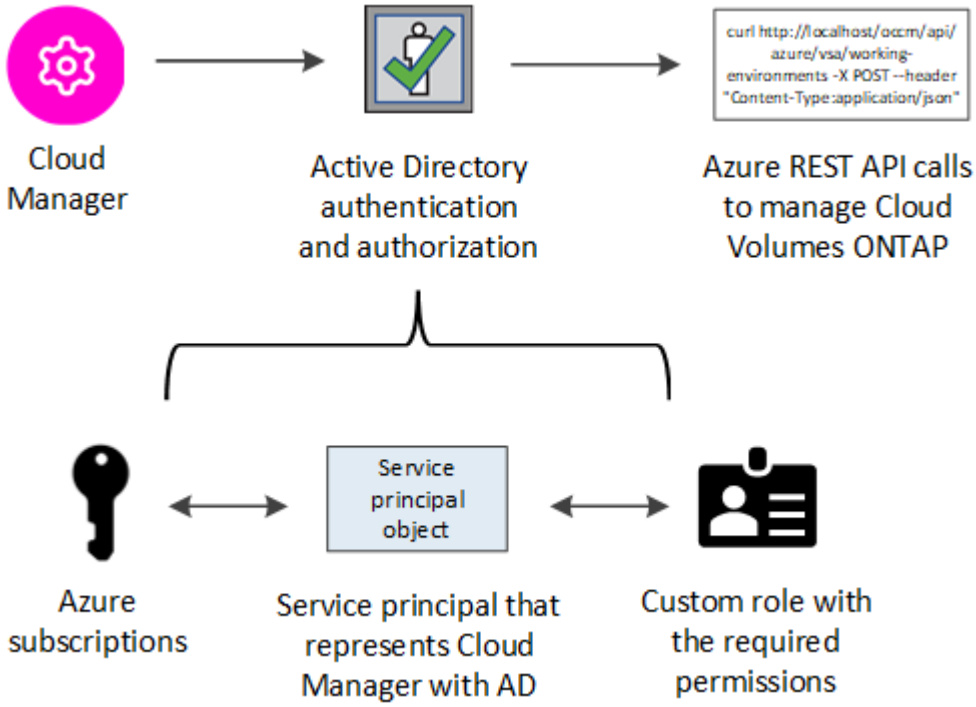
Lorsque vous déployez un connecteur depuis Cloud Manager, Cloud Manager ajoute automatiquement le compte Azure dans lequel vous avez déployé le connecteur. Un compte initial n'est pas ajouté si vous avez installé manuellement le logiciel Connector sur un système existant. "En savoir plus sur les comptes et les autorisations Azure".

Octroi d'autorisations Azure à l'aide d'une entité de sécurité de service

Cloud Manager a besoin d'autorisations pour effectuer des actions dans Azure. Vous pouvez accorder les autorisations requises à un compte Azure en créant et en configurant une entité de sécurité de service dans Azure Active Directory et en obtenant les informations d'identification Azure requises par Cloud Manager.

Description de la tâche

L'image suivante illustre comment Cloud Manager obtient les autorisations nécessaires pour effectuer des opérations dans Azure. Un objet principal de service, lié à un ou plusieurs abonnements Azure, représente Cloud Manager dans Azure Active Directory et est affecté à un rôle personnalisé qui permet les autorisations requises.



Étapes

1. Créez une application Azure Active Directory.
2. Attribuez l'application à un rôle.
3. Ajoutez des autorisations d'API de gestion de service Windows Azure.
4. Obtenir l'ID de l'application et l'ID du répertoire.
5. Créez un secret client.

Création d'une application Azure Active Directory

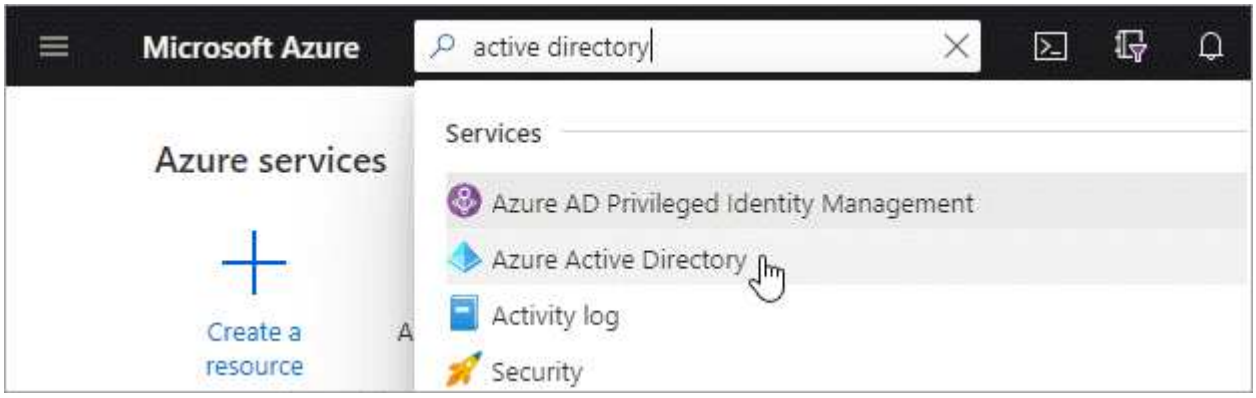
Créez une application Azure Active Directory (AD) et une entité de service que Cloud Manager peut utiliser pour le contrôle d'accès basé sur des rôles.

Avant de commencer

Vous devez disposer des droits d'accès dans Azure pour créer une application Active Directory et attribuer l'application à un rôle. Pour plus de détails, reportez-vous à "Documentation Microsoft Azure : autorisations requises".

Étapes

1. À partir du portail Azure, ouvrez le service **Azure Active Directory**.



2. Dans le menu, cliquez sur **enregistrements d'applications**.
3. Cliquez sur **Nouvelle inscription**.
4. Spécifiez les détails de l'application :
   - **Nom** : saisissez un nom pour l'application.
   - **Type de compte** : sélectionnez un type de compte (tout fonctionne avec Cloud Manager).
   - **Redirect URI** : sélectionnez **Web**, puis entrez n'importe quelle URL, par exemple, https://url
5. Cliquez sur **Enregistrer**.

Résultat

Vous avez créé l'application AD et le principal de service.

Affectation de l'application à un rôle

Vous devez lier la principale de service à un ou plusieurs abonnements Azure et lui attribuer le rôle « opérateur OnCommand Cloud Manager » personnalisé pour que Cloud Manager possède des autorisations dans Azure.

Étapes

1. Création d'un rôle personnalisé :

   a. Téléchargez le "Politique de Cloud Manager Azure".

   b. Modifiez le fichier JSON en ajoutant des identifiants d'abonnement Azure à l'étendue assignable.

   Vous devez ajouter l'ID de chaque abonnement Azure à partir duquel les utilisateurs créeront des systèmes Cloud Volumes ONTAP.

   Exemple

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

   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_cloud_Manager_Azure_3.8.7.json
```

Vous devriez maintenant avoir un rôle personnalisé appelé *Cloud Manager Operator*.

2. Attribuez l'application au rôle :

   a. À partir du portail Azure, ouvrez le service **abonnements**.

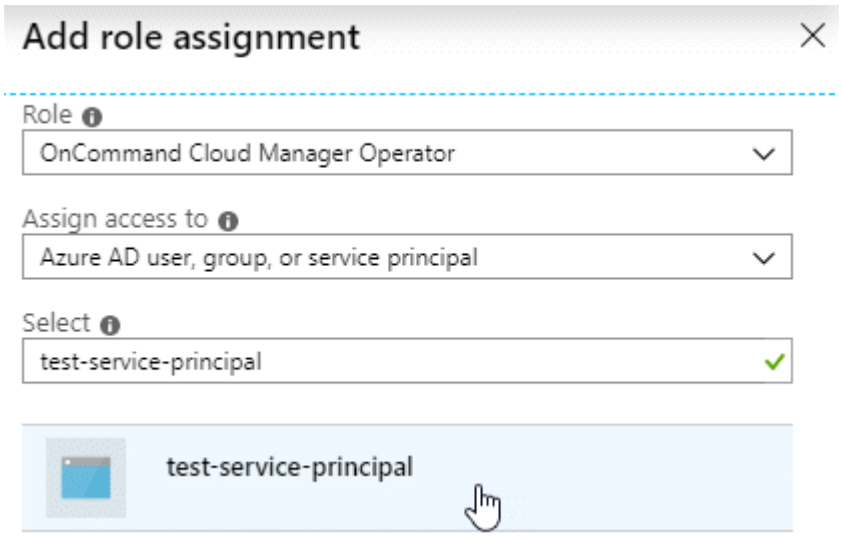
   b. Sélectionnez l'abonnement.

   c. Cliquez sur **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.

   d. Sélectionnez le rôle **opérateur** de Cloud Manager.

   e. Conserver *l'utilisateur, le groupe ou le principal de service AD d'Azure sélectionné.

   f. Recherchez le nom de l'application (vous ne pouvez pas le trouver dans la liste en faisant défiler la liste).



   g. Sélectionnez l'application et cliquez sur **Enregistrer**.

   Le principal de service de Cloud Manager dispose désormais des autorisations Azure requises pour cet abonnement.

Si vous souhaitez déployer Cloud Volumes ONTAP à partir de plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. Cloud Manager vous permet de sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

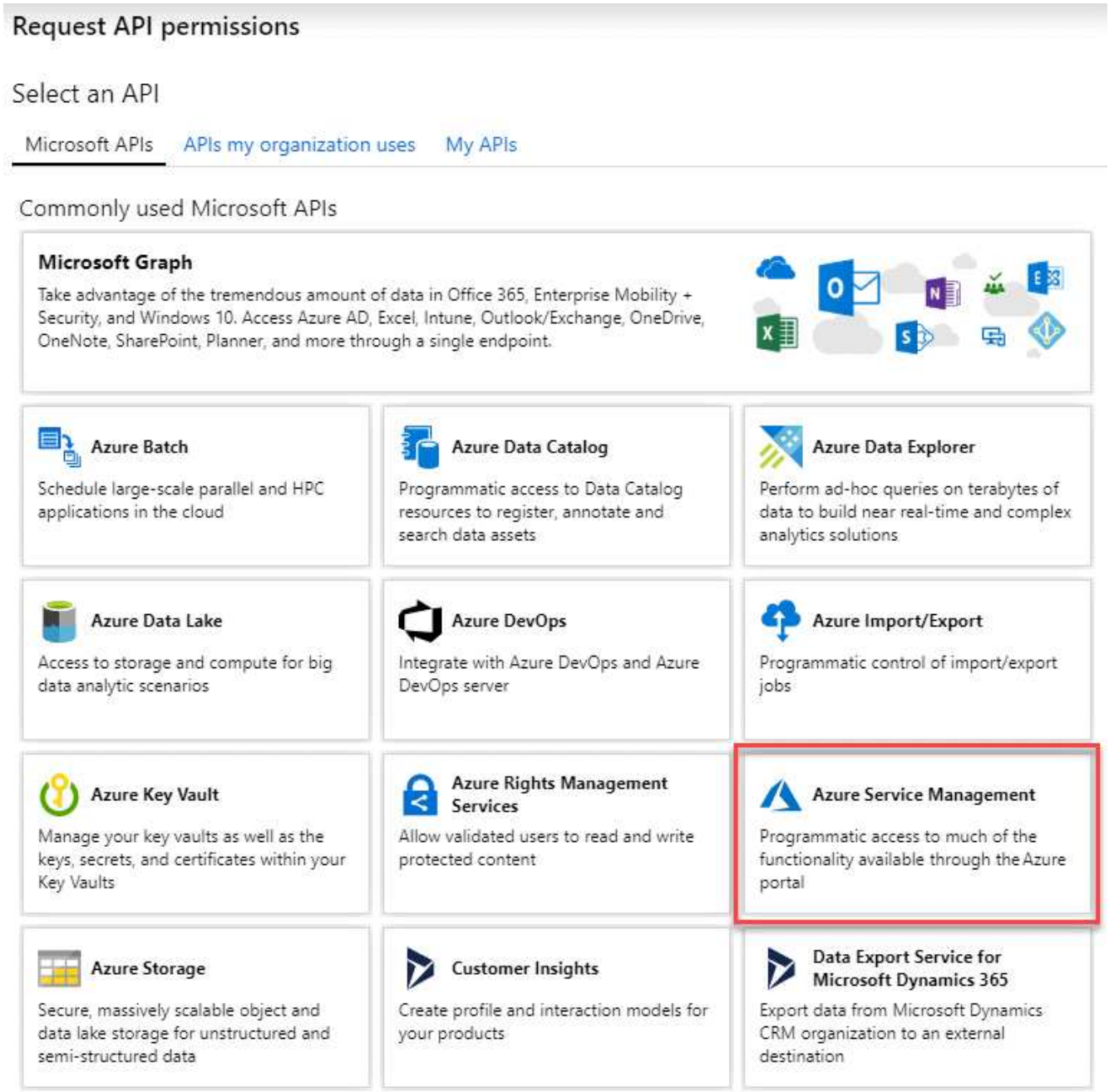
Ajout d'autorisations d'API de gestion des services Windows Azure

Le principal de service doit disposer d'autorisations « API de gestion des services Windows Azure ».

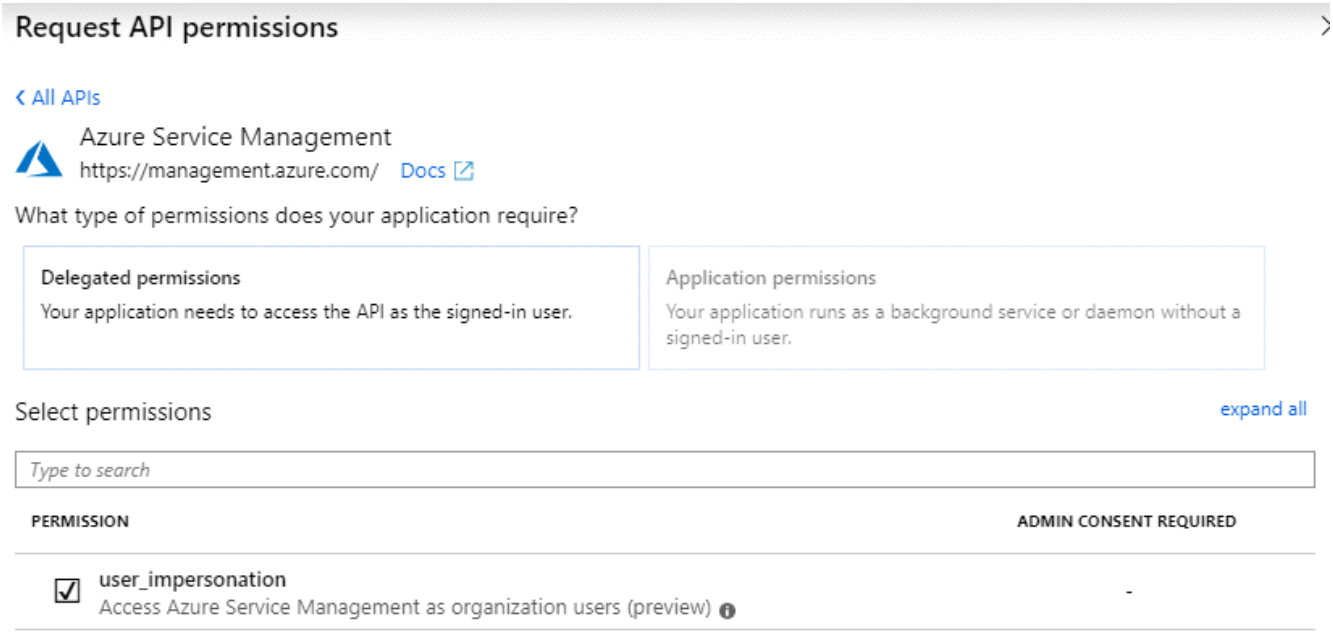
Étapes

1. Dans le service **Azure Active Directory**, cliquez sur **App inscriptions** et sélectionnez l'application.
2. Cliquez sur **autorisations API > Ajouter une autorisation**.

3. Sous **Microsoft API**, sélectionnez **Azure Service Management**.



4. Cliquez sur **Access Azure Service Management en tant qu'utilisateurs d'organisation**, puis sur **Add permissions**.

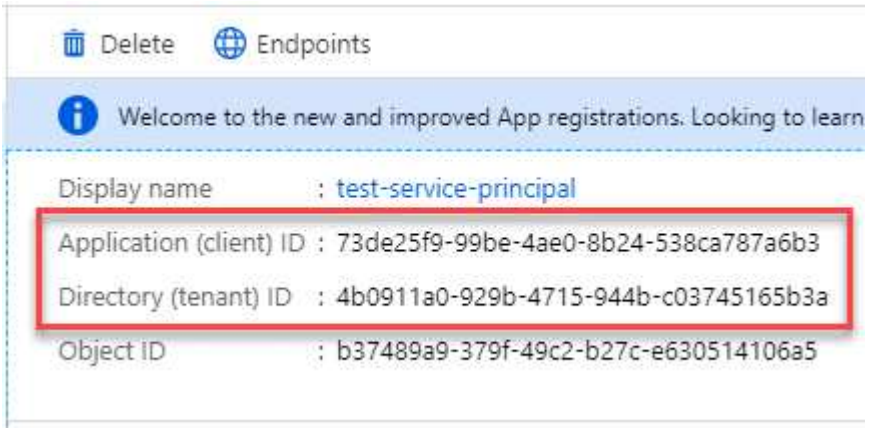


Obtention de l'ID d'application et de l'ID de répertoire

Lorsque vous ajoutez le compte Azure dans Cloud Manager, vous devez fournir l'ID d'application (client) et l'ID de répertoire (locataire) de l'application. Cloud Manager utilise ces identifiants pour vous connecter automatiquement.

Étapes

1. Dans le service **Azure Active Directory**, cliquez sur **App inscriptions** et sélectionnez l'application.
2. Copiez l'ID **application (client)** et l'ID **Directory (tenant)**.



Création d'un secret client

Vous devez créer un secret client, puis fournir à Cloud Manager la valeur du secret pour que Cloud Manager puisse l'utiliser pour vous authentifier avec Azure AD.

Lorsque vous ajoutez le compte à Cloud Manager, Cloud Manager fait référence au secret client en tant que clé d'application.

Étapes

1. Ouvrez le service **Azure Active Directory**.
2. Cliquez sur **App Inregistrations** et sélectionnez votre application.
3. Cliquez sur **certificats et secrets > Nouveau secret client**.
4. Fournissez une description du secret et une durée.
5. Cliquez sur **Ajouter**.
6. Copier la valeur du secret client.

Résultat

Votre principal de service est maintenant configuré et vous devez avoir copié l'ID de l'application (client), l'ID du répertoire (tenant) et la valeur du secret client. Vous devez saisir ces informations dans Cloud Manager lorsque vous ajoutez un compte Azure.

Ajout d'identifiants Azure à Cloud Manager

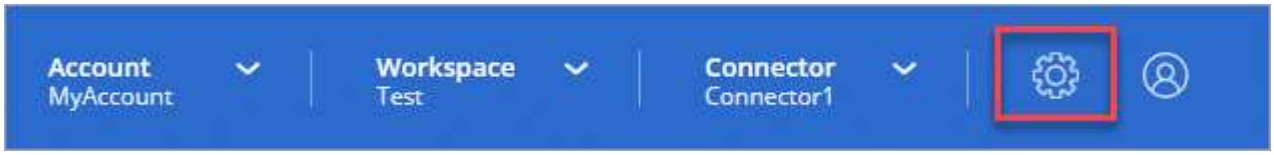
Une fois que vous avez autorisé à fournir un compte Azure, vous pouvez ajouter les identifiants de ce compte à Cloud Manager. Vous pouvez ainsi lancer les systèmes Cloud Volumes ONTAP de ce compte.

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



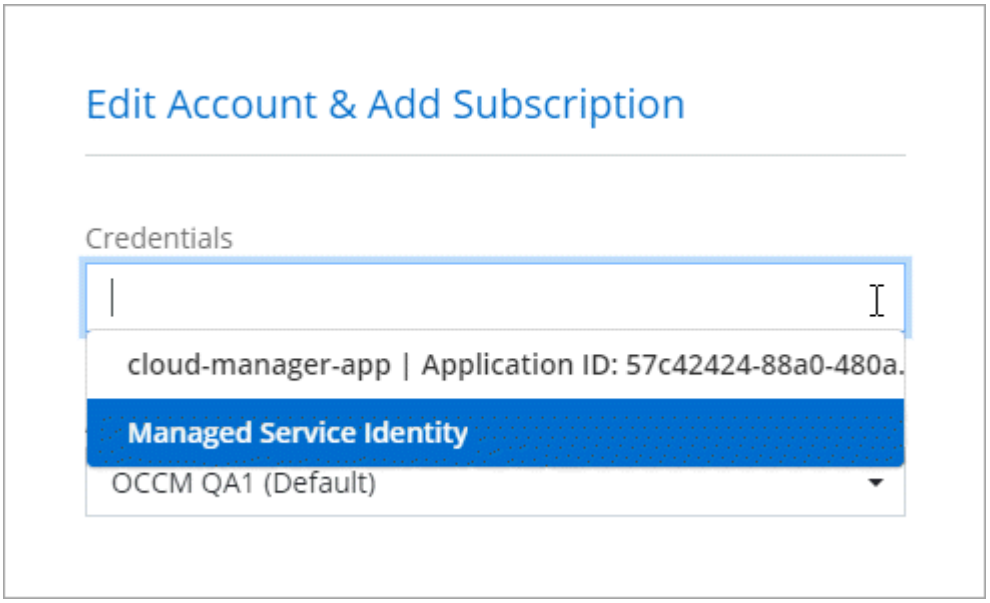
2. Cliquez sur **Ajouter des informations d'identification** et sélectionnez **Microsoft Azure**.
3. Entrez des informations sur l'entité de sécurité du service Azure Active Directory qui accorde les autorisations requises :
   - ID de l'application (client) : voir Obtention de l'ID d'application et de l'ID de répertoire.
   - ID de répertoire (locataire) : voir Obtention de l'ID d'application et de l'ID de répertoire.
   - Secret client : voir Création d'un secret client.
4. Vérifiez que les exigences de la stratégie ont été respectées, puis cliquez sur **Continuer**.
5. Choisissez l'abonnement payant à l'utilisation que vous souhaitez associer aux informations d'identification ou cliquez sur **Ajouter un abonnement** si vous n'en avez pas encore.

Pour créer un système Cloud Volumes ONTAP basé sur l'utilisation, vous devez associer des identifiants Azure à un abonnement à Cloud Volumes ONTAP à partir d'Azure Marketplace.

6. Cliquez sur **Ajouter**.

Résultat

Vous pouvez maintenant passer à différents ensembles d'informations d'identification à partir de la page Détails et informations d'identification "lors de la création d'un nouvel environnement de travail":



Association d'un abonnement à Azure Marketplace aux identifiants

Après avoir ajouté vos identifiants Azure à Cloud Manager, vous pouvez associer un abonnement Azure Marketplace à ces identifiants. Cet abonnement vous permet de créer un système Cloud Volumes ONTAP basé sur l'utilisation et d'utiliser d'autres services cloud NetApp.

Deux scénarios peuvent s'avérer nécessaires pour associer un abonnement Azure Marketplace une fois que vous avez déjà ajouté les identifiants à Cloud Manager :

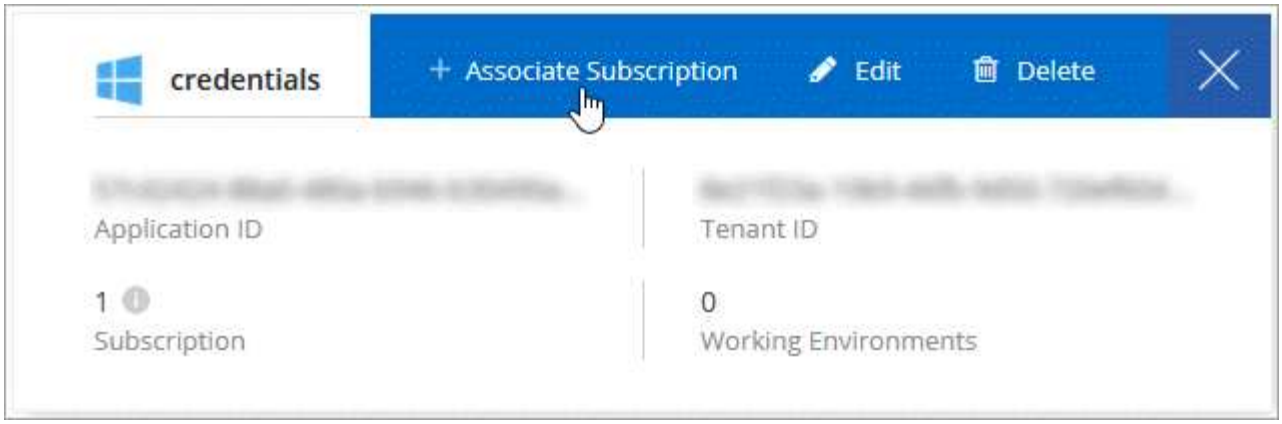
- Vous n'avez pas associé un abonnement lors de l'ajout initial des identifiants à Cloud Manager.
- Vous souhaitez remplacer un abonnement Azure Marketplace existant par un nouvel abonnement.

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Passez le curseur de la souris sur un ensemble d'informations d'identification et cliquez sur le menu d'action.
3. Dans le menu, cliquez sur **associer abonnement**.



4. Sélectionnez un abonnement dans la liste déroulante ou cliquez sur **Ajouter un abonnement** et suivez les étapes pour créer un nouvel abonnement.

   La vidéo suivante démarre à partir du contexte de l'assistant de l'environnement de travail, mais vous montre le même flux de travail après avoir cliqué sur **Ajouter un abonnement** :

   ► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_azure.mp4 *(video)*

Association d'abonnements Azure supplémentaires à une identité gérée

Cloud Manager vous permet de choisir les identifiants Azure et l'abonnement Azure dans lesquels vous souhaitez déployer Cloud Volumes ONTAP. Vous ne pouvez pas sélectionner un autre abonnement Azure pour le profil d'identité gérée à moins d'associer le "identité gérée" avec ces abonnements.

Description de la tâche

Une identité gérée est "Compte Azure initial" Lorsque vous déployez un connecteur depuis Cloud Manager. Une fois que vous avez déployé Connector, Cloud Manager a créé le rôle de l'opérateur Cloud Manager et l'a attribué à la machine virtuelle du connecteur.

Étapes

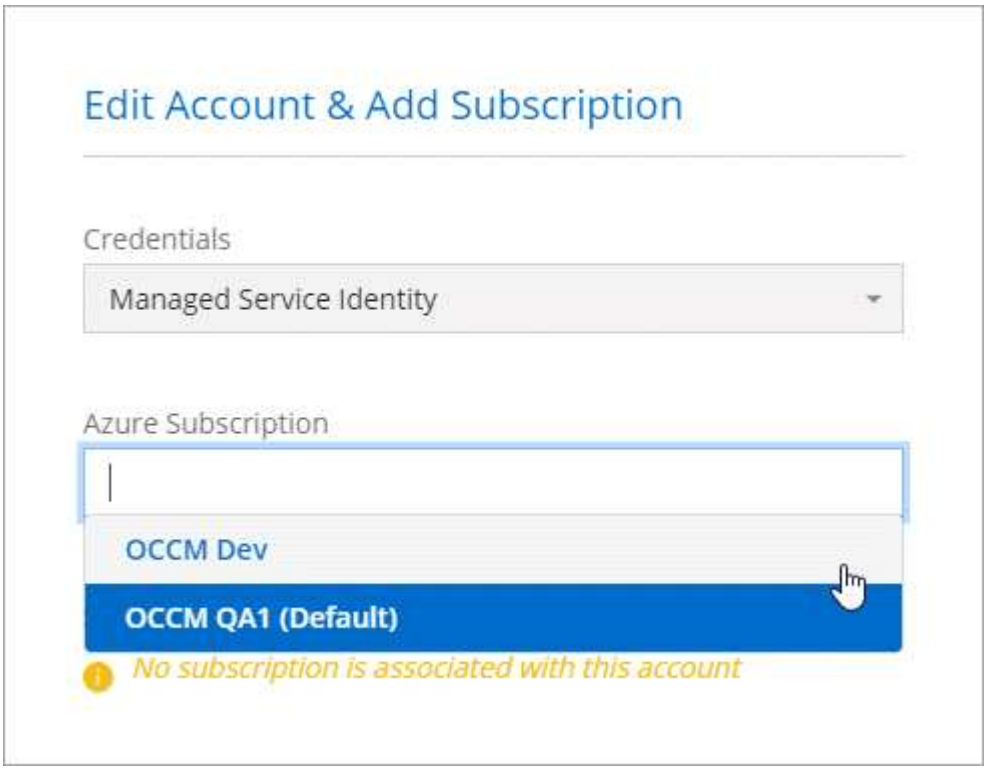
1. Connectez-vous au portail Azure.
2. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer Cloud Volumes ONTAP.
3. Cliquez sur **contrôle d'accès (IAM)**.
   a. Cliquez sur **Ajouter** > **Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
      - Sélectionnez le rôle **opérateur** de Cloud Manager.

        L'opérateur de Cloud Manager est le nom par défaut fourni dans "Politique de Cloud Manager". Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

      - Attribuez l'accès à une **machine virtuelle**.
      - Sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée.
      - Sélectionnez la machine virtuelle Connector.
      - Cliquez sur **Enregistrer**.
4. Répétez ces étapes pour les abonnements supplémentaires.

Résultat

Lorsque vous créez un nouvel environnement de travail, vous devriez désormais pouvoir sélectionner plusieurs abonnements Azure pour le profil d'identité géré.



GCP

Projets, autorisations et comptes Google Cloud

Un compte de service fournit à Cloud Manager les autorisations de déploiement et de gestion des systèmes Cloud Volumes ONTAP dans le même projet que Cloud Manager, ou dans des projets différents.

Projet et autorisations pour Cloud Manager

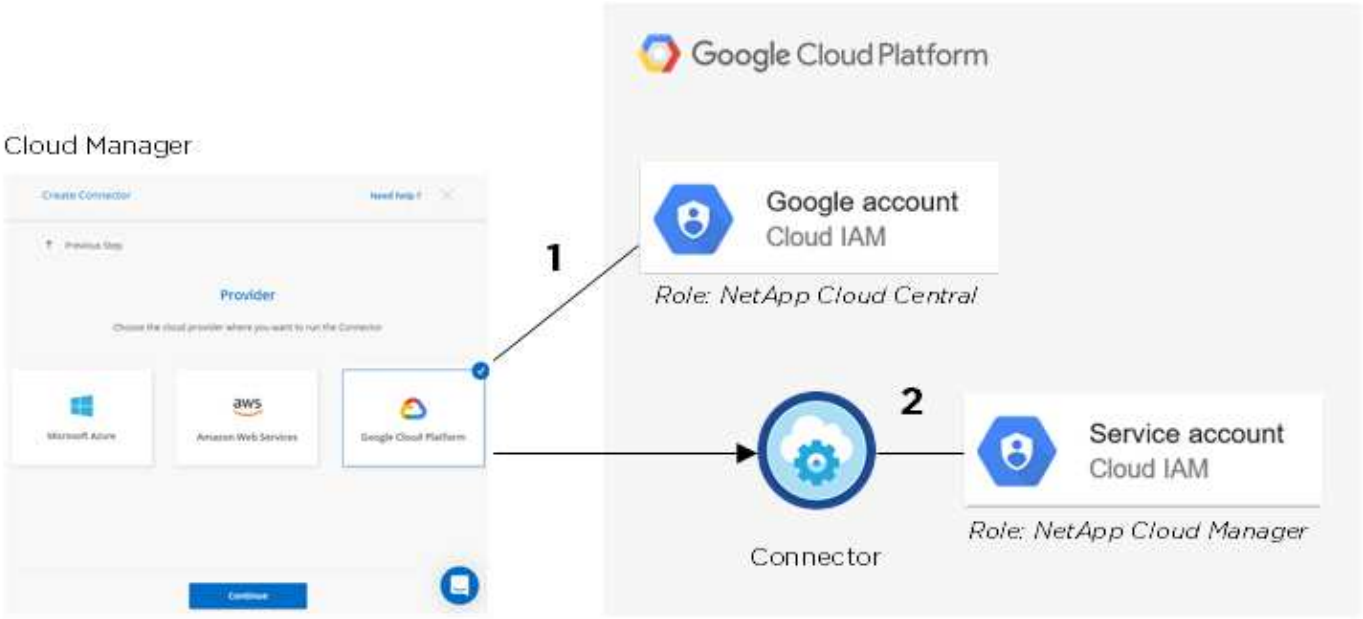
Avant de déployer Cloud Volumes ONTAP dans Google Cloud, vous devez d'abord déployer un connecteur dans un projet Google Cloud. Il ne peut pas s'exécuter sur site ou dans un autre fournisseur cloud.

Deux ensembles d'autorisations doivent être en place avant de déployer un connecteur directement depuis Cloud Manager :

1. Vous devez déployer un connecteur à l'aide d'un compte Google disposant des autorisations nécessaires pour lancer l'instance de VM Connector à partir de Cloud Manager.
2. Lorsque vous déployez le connecteur, vous êtes invité à sélectionner un "compte de service" Pour l'instance de VM. Cloud Manager obtient les autorisations du compte de service pour créer et gérer les systèmes Cloud Volumes ONTAP en votre nom. Les autorisations sont fournies en ajoutant un rôle personnalisé au compte de service.

Nous avons configuré deux fichiers YAML qui incluent les autorisations requises pour l'utilisateur et le compte de service. "Découvrez comment utiliser les fichiers YAML pour configurer les autorisations".

L'image suivante décrit les conditions d'autorisation décrites aux numéros 1 et 2 ci-dessus :



Projet pour Cloud Volumes ONTAP

Cloud Volumes ONTAP peut résider dans le même projet que le connecteur ou dans un autre projet. Pour déployer Cloud Volumes ONTAP dans un autre projet, vous devez d'abord ajouter le compte de service Connector et le rôle à ce projet.

- "Découvrez comment configurer un compte de service (voir étape 2)".
- "Découvrez comment déployer Cloud Volumes ONTAP dans GCP et sélectionner un projet".

Compte tenu du Tiering des données

Cloud Manager requiert un compte GCP pour Cloud Volumes ONTAP 9.6, mais pas pour la version 9.7 et ultérieure. Si vous souhaitez utiliser le Tiering des données avec Cloud Volumes ONTAP 9.7, suivez les étapes 4 à "Mise en route de Cloud Volumes ONTAP dans Google Cloud Platform".

L'ajout d'un compte Google Cloud à Cloud Manager permet le Tiering des données sur un système Cloud Volumes ONTAP 9.6. Le Tiering des données transfère automatiquement les données inactives vers un stockage objet plus économique, ce qui vous permet de récupérer de l'espace dans votre stockage primaire et de réduire le stockage secondaire.

Lorsque vous ajoutez ce compte, vous devez fournir à Cloud Manager une clé d'accès de stockage pour un compte de service disposant des autorisations d'administrateur de stockage. Cloud Manager utilise les clés d'accès pour configurer et gérer un compartiment de stockage cloud pour le Tiering des données.

Une fois que vous avez ajouté un compte Google Cloud, vous pouvez activer le Tiering des données sur les volumes individuels lorsque vous les créez, les modifiez ou les répliquez.

- "Découvrez comment configurer et ajouter des comptes GCP à Cloud Manager".
- "Découvrez comment transférer des données inactives vers un stockage objet à faible coût".

Gestion des identifiants GCP et des abonnements pour Cloud Manager

Vous pouvez gérer deux types d'identifiants Google Cloud Platform dans Cloud Manager

: les identifiants qui sont associés à l'instance de machine virtuelle de connecteur et les clés d'accès de stockage utilisées avec un système Cloud Volumes ONTAP 9.6 pour "tiering des données".

Association d'un abonnement Marketplace aux informations d'identification GCP

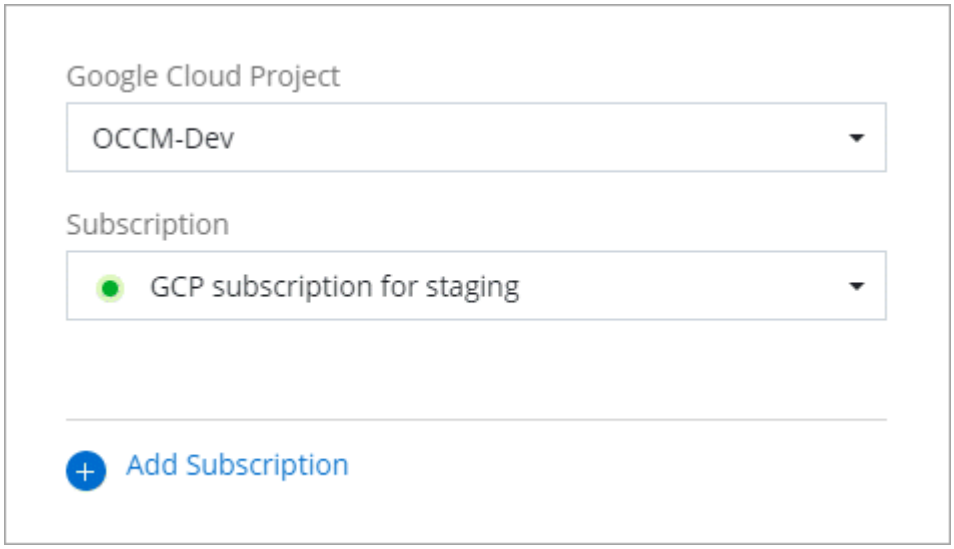
Lorsque vous déployez un connecteur dans GCP, Cloud Manager crée un ensemble d'identifiants par défaut associés à l'instance de VM de connecteur. Ce sont les identifiants utilisés par Cloud Manager pour déployer Cloud Volumes ONTAP.

Vous pouvez à tout moment modifier l'abonnement Marketplace associé à ces informations d'identification. Cet abonnement vous permet de créer un système Cloud Volumes ONTAP basé sur l'utilisation et d'utiliser d'autres services cloud NetApp.

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Passez le curseur de la souris sur un ensemble d'informations d'identification et cliquez sur le menu d'action.
3. Dans le menu, cliquez sur **associer abonnement**.

4. Sélectionnez un projet et un abonnement Google Cloud dans la liste déroulante ou cliquez sur **Ajouter un abonnement** et suivez les étapes pour créer un nouvel abonnement.



5. Cliquez sur **associé**.

Configuration et ajout de comptes GCP pour le Tiering des données avec Cloud Volumes ONTAP 9.6

Si vous souhaitez activer un système Cloud Volumes ONTAP 9.6 pour "tiering des données", Vous devez fournir à Cloud Manager une clé d'accès au stockage pour un compte de service disposant des autorisations d'administrateur de stockage. Cloud Manager utilise les clés d'accès pour configurer et gérer un compartiment de stockage cloud pour le Tiering des données.

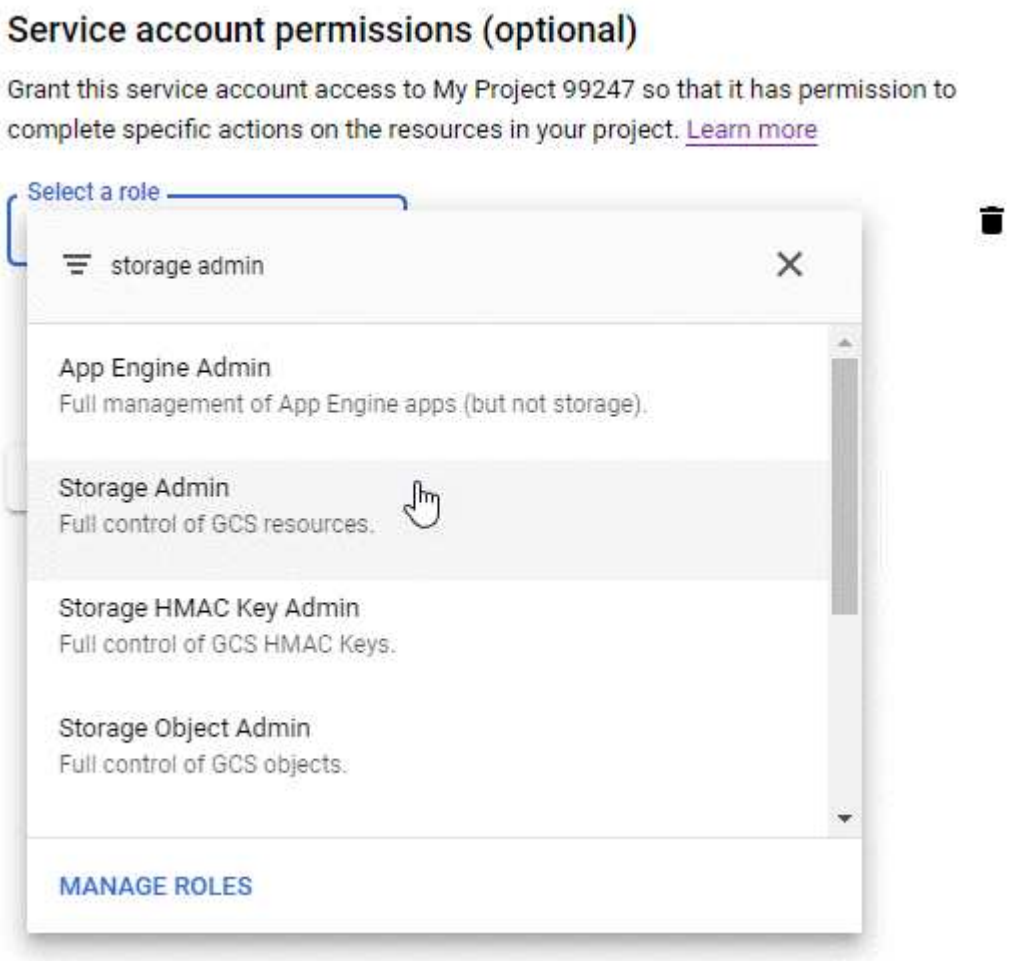
Si vous souhaitez utiliser le Tiering des données avec Cloud Volumes ONTAP 9.7, suivez les étapes 4 à "Mise en route de Cloud Volumes ONTAP dans Google Cloud Platform".

Configurer un compte de service et des clés d'accès pour Google Cloud Storage

Un compte de service permet à Cloud Manager d'authentifier et d'accéder aux compartiments Cloud Storage utilisés pour le Tiering des données. Les clés sont requises pour que Google Cloud Storage sache qui effectue la demande.

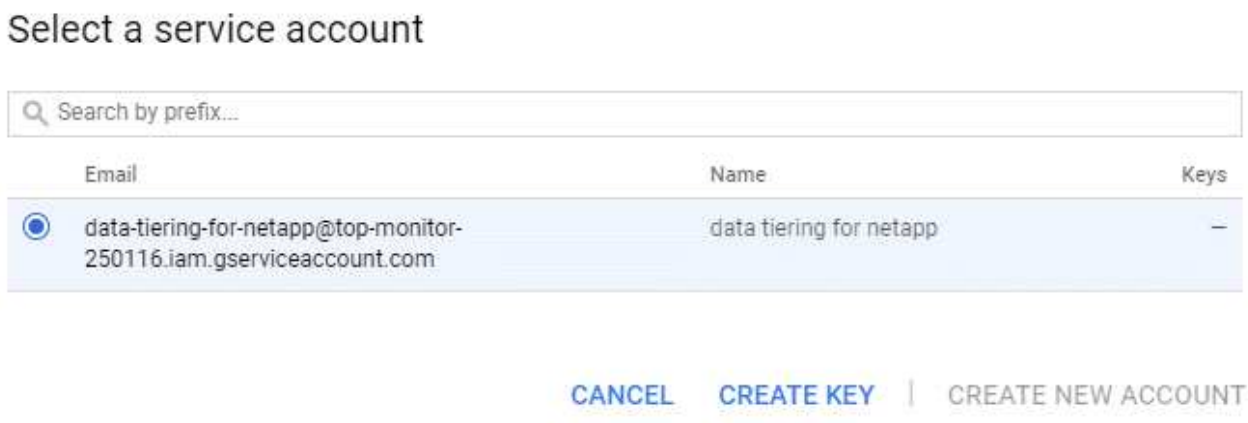
Étapes

1. Ouvrez la console IAM GCP et "Créez un compte de service avec le rôle d'administrateur du stockage".



2. Accédez à "Paramètres de stockage GCP".
3. Si vous y êtes invité, sélectionnez un projet.

4. Cliquez sur l'onglet **Interoperability**.
5. Si ce n'est déjà fait, cliquez sur **Activer l'accès à l'interopérabilité**.
6. Sous **clés d'accès pour les comptes de service**, cliquez sur **Créer une clé pour un compte de service**.
7. Sélectionnez le compte de service que vous avez créé à l'étape 1.



8. Cliquez sur **Créer clé**.
9. Copiez la clé d'accès et le secret.

   Lorsque vous ajoutez le compte GCP pour le Tiering des données, vous devez entrer ces informations dans Cloud Manager.

Ajout d'un compte GCP à Cloud Manager

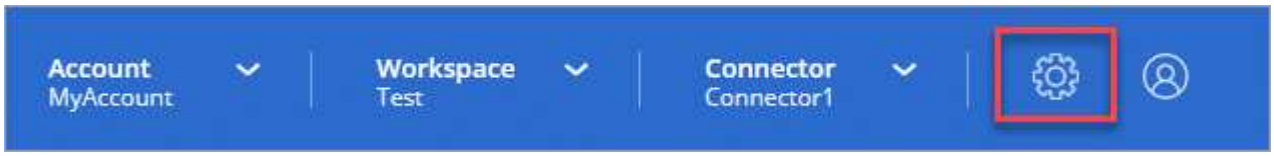
Vous pouvez désormais ajouter cette clé à Cloud Manager.

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



2. Cliquez sur **Ajouter des informations d'identification** et sélectionnez **Google Cloud**.
3. Saisissez la clé d'accès et le secret du compte de service.

   Les clés permettent à Cloud Manager de configurer un compartiment Cloud Storage pour le Tiering des données.

4. Vérifiez que les exigences de la stratégie ont été respectées, puis cliquez sur **Créer un compte**.

Et la suite ?

Vous pouvez désormais activer le Tiering des données sur les volumes individuels d'un système Cloud Volumes ONTAP 9.6 lorsque vous les créez, les modifiez ou les répliquez. Pour plus de détails, voir "Tiering des données inactives vers un stockage objet à faible coût".

Mais avant cela, assurez-vous que le sous-réseau dans lequel réside Cloud Volumes ONTAP est configuré pour un accès privé à Google. Pour obtenir des instructions, reportez-vous à la section "Documentation Google Cloud : configuration de Private Google Access".

Ajout de comptes du site de support NetApp à Cloud Manager

Vous devez ajouter votre compte sur le site de support NetApp à Cloud Manager pour déployer un système BYOL. Il est également nécessaire d'enregistrer des systèmes avec paiement à l'utilisation et de mettre à niveau le logiciel ONTAP.

Découvrez dans cette vidéo comment ajouter des comptes sur le site de support NetApp à Cloud Manager. Ou faites défiler vers le bas pour lire les étapes.

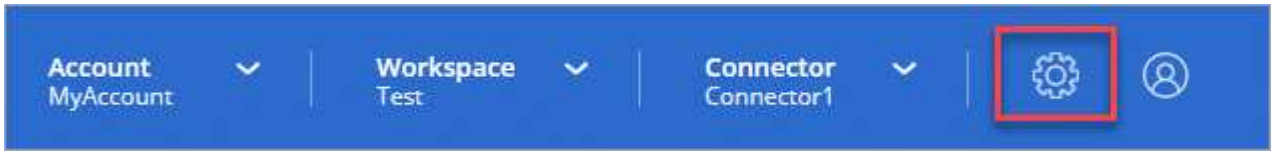
[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Si vous ne disposez pas encore d'un compte sur le site de support NetApp, "inscrivez-vous pour en créer un".
2. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



3. Cliquez sur **Add Credentials** et sélectionnez **NetApp support site**.
4. Spécifiez un nom pour le compte, puis entrez le nom d'utilisateur et le mot de passe.
   - Le compte doit être un compte de niveau client (et non un compte invité ou temporaire).
   - Si vous prévoyez de déployer des systèmes BYOL :
     - Le compte doit être autorisé à accéder aux numéros de série des systèmes BYOL.
     - Si vous avez acheté un abonnement BYOL sécurisé, un compte NSS sécurisé est requis.
5. Cliquez sur **Créer un compte.**

Et la suite ?

Les utilisateurs peuvent désormais sélectionner le compte lors de la création de nouveaux systèmes Cloud Volumes ONTAP et lors de l'enregistrement de systèmes existants.

- "Lancement d'Cloud Volumes ONTAP dans AWS"
- "Lancement d'Cloud Volumes ONTAP dans Azure"
- "Enregistrement des systèmes de paiement à l'utilisation"

- "Découvrez comment Cloud Manager gère les fichiers de licences"

Gestion des utilisateurs, des espaces de travail, des connecteurs et des abonnements

"Après avoir effectué la configuration initiale"Vous devrez peut-être gérer ultérieurement les paramètres de votre compte en gérant les utilisateurs, les espaces de travail, les connecteurs et les abonnements.

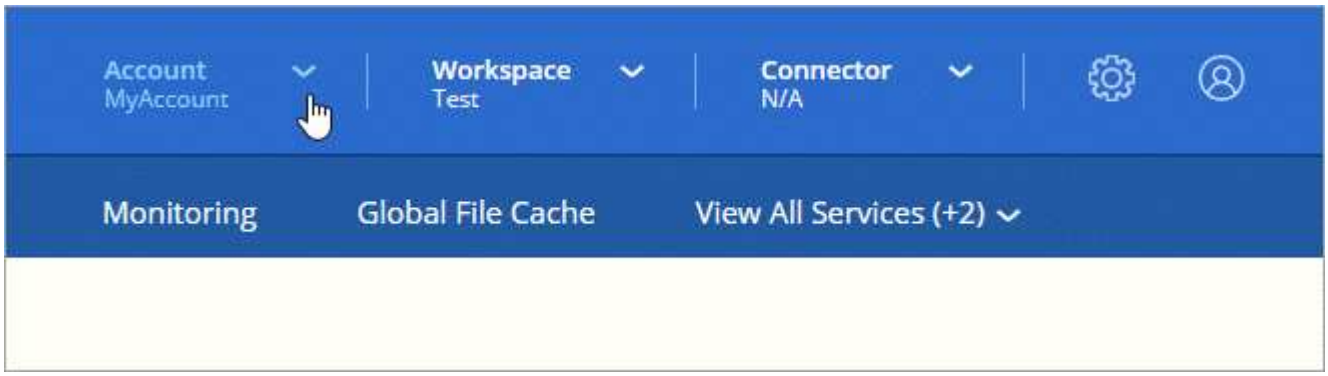
"Découvrez comment fonctionnent les comptes Cloud Central".

Ajout d'utilisateurs

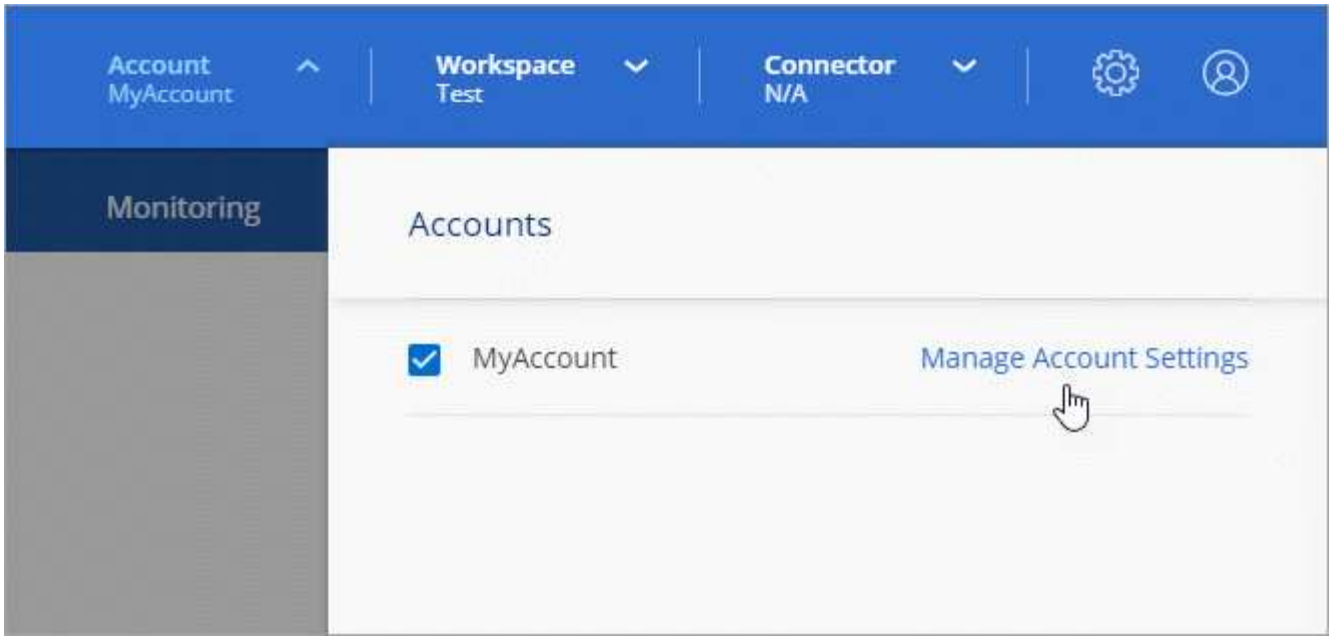
Associez les utilisateurs de Cloud Central au compte Cloud Central pour qu'ils puissent créer et gérer des environnements de travail dans Cloud Manager.

Étapes

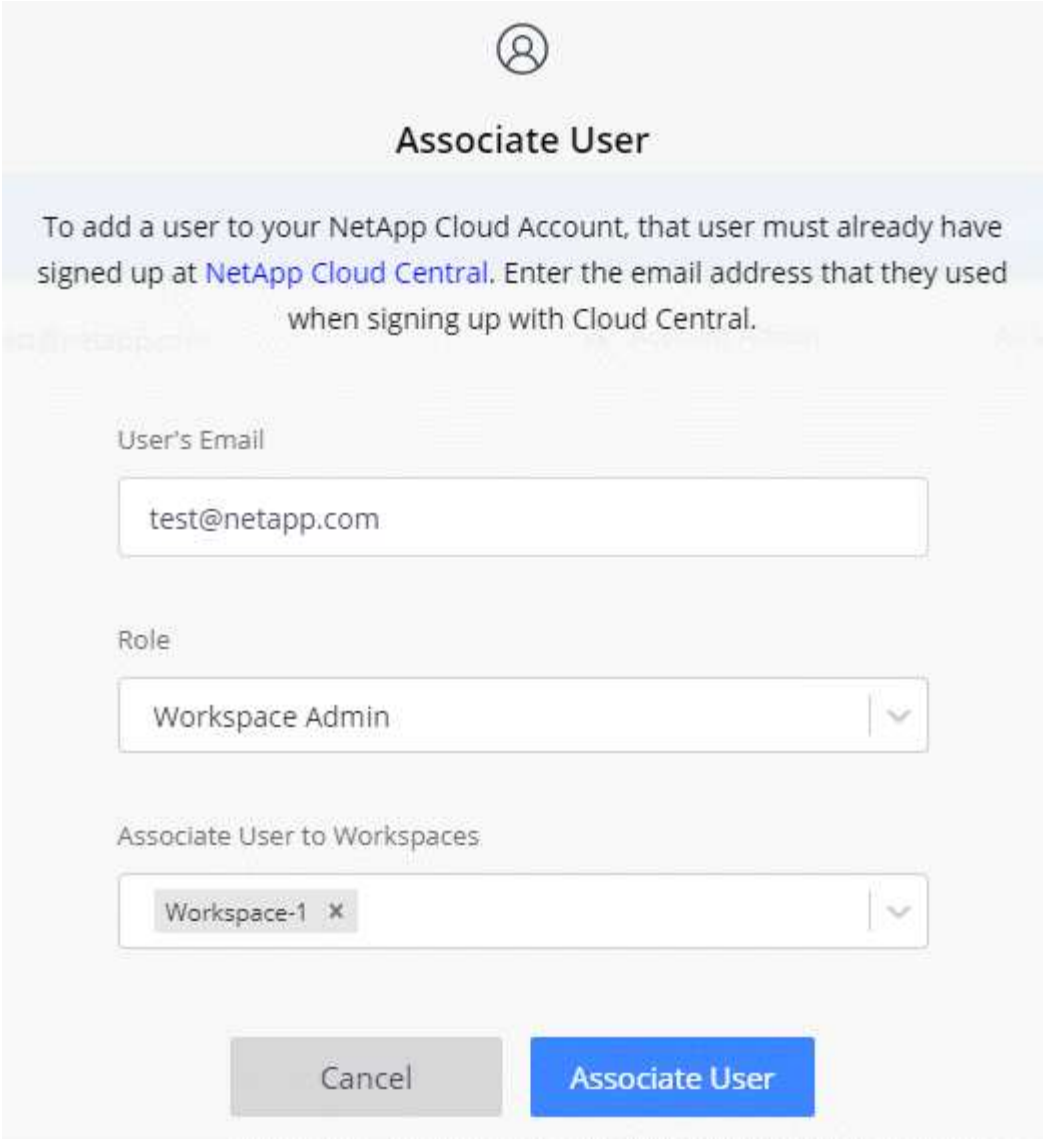
1. Si l'utilisateur ne l'a pas déjà fait, demandez-lui d'aller à "NetApp Cloud Central" et s'inscrire.
2. Dans la partie supérieure de Cloud Manager, cliquez sur la liste déroulante **Account**.



3. Cliquez sur **gérer le compte** en regard du compte actuellement sélectionné.



4. Dans l'onglet utilisateurs, cliquez sur **associer utilisateur**.
5. Entrez l'adresse e-mail de l'utilisateur et sélectionnez un rôle pour l'utilisateur :
   - **Administrateur de compte** : peut effectuer n'importe quelle action dans Cloud Manager.
   - **Workspace Admin** : permet de créer et de gérer des ressources dans des espaces de travail attribués.
   - **Compliance Viewer** : peut uniquement afficher les informations de conformité et générer des rapports pour les espaces de travail auxquels ils ont la permission d'accéder.
6. Si vous avez sélectionné Workspace Admin ou Compliance Viewer, sélectionnez un ou plusieurs espaces de travail à associer à cet utilisateur.



7. Cliquez sur **associer utilisateur**.

Résultat

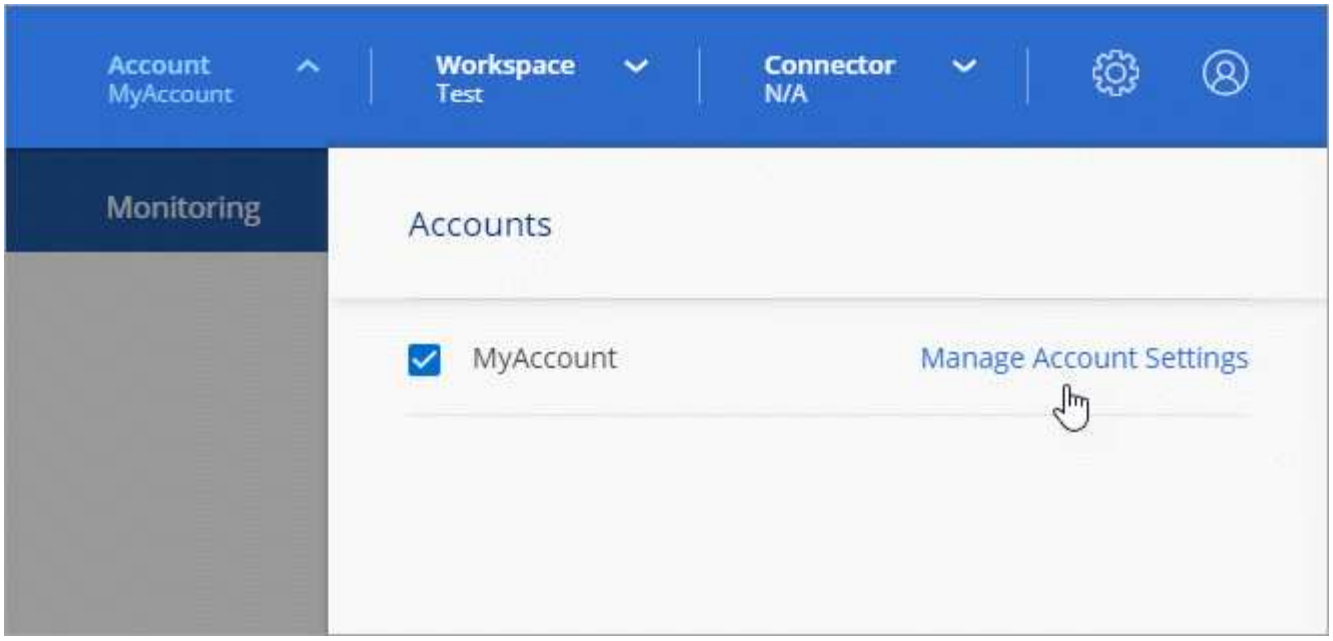
L'utilisateur doit recevoir un e-mail de la part de NetApp Cloud Central intitulé « Account Association ». Il contient les informations nécessaires pour accéder à Cloud Manager.

Suppression d'utilisateurs

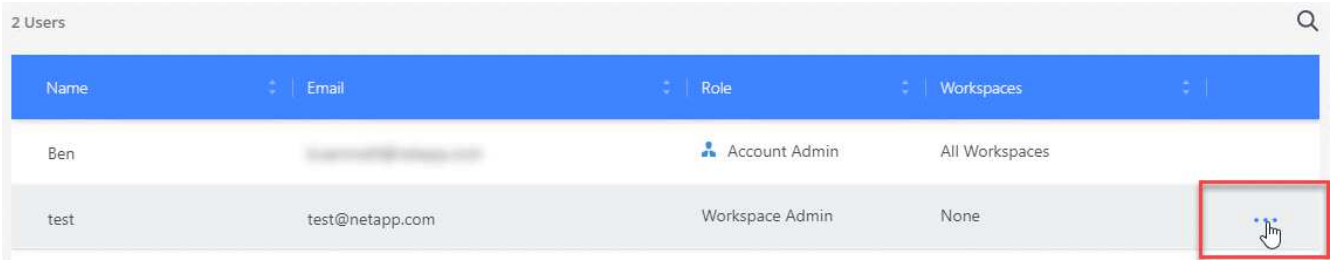
La dissociation permet d'interdire l'accès aux ressources d'un compte Cloud Central.

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.



2. Dans l'onglet utilisateurs, cliquez sur le menu d'action de la ligne correspondant à l'utilisateur.



3. Cliquez sur **Disassocier utilisateur** et cliquez sur **Disassocier** pour confirmer.

Résultat

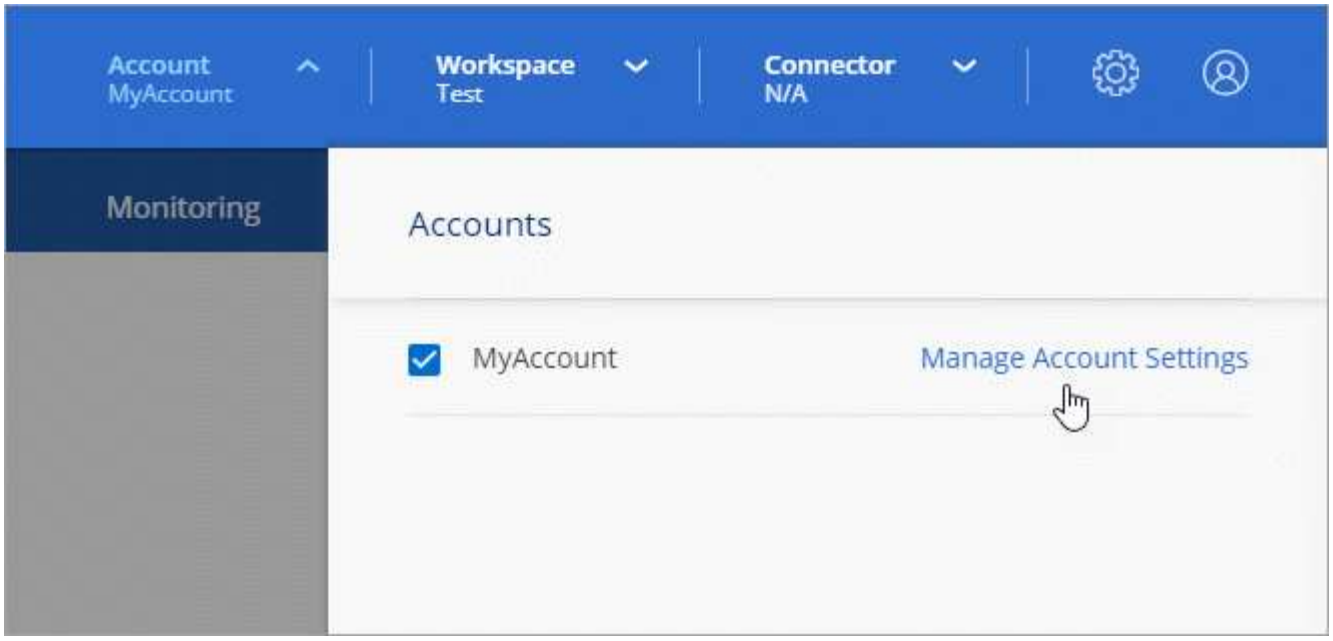
L'utilisateur ne peut plus accéder aux ressources de ce compte Cloud Central.

Gestion des espaces de travail d'un administrateur d'espace de travail

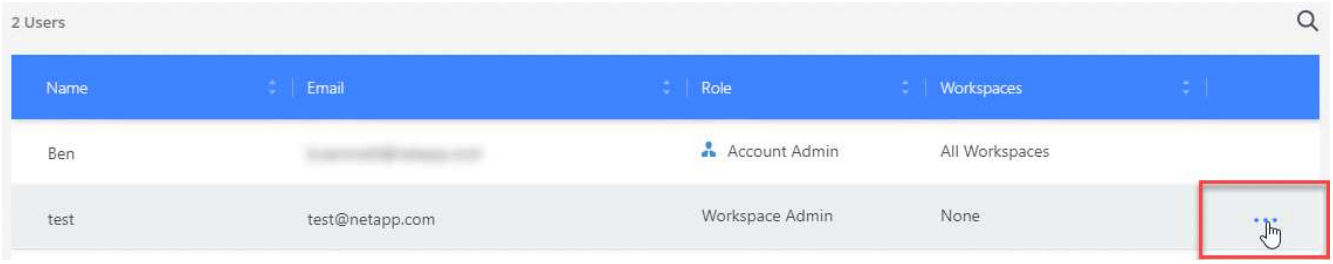
Vous pouvez associer et dissocier les administrateurs d'espace de travail avec des espaces de travail à tout moment. L'association de l'utilisateur lui permet de créer et d'afficher les environnements de travail dans cet espace de travail.

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.



2. Dans l'onglet utilisateurs, cliquez sur le menu d'action de la ligne correspondant à l'utilisateur.



3. Cliquez sur **gérer les espaces de travail**.
4. Sélectionnez les espaces de travail à associer à l'utilisateur et cliquez sur **appliquer**.

Résultat

L'utilisateur peut désormais accéder à ces espaces de travail à partir de Cloud Manager, tant que le connecteur était également associé aux espaces de travail.

Gestion des espaces de travail

Gérez vos espaces de travail en les créant, en les renommant et en les supprimant. Notez que vous ne pouvez pas supprimer un espace de travail s'il contient des ressources. Elle doit être vide.

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.
2. Cliquez sur **espaces de travail**.
3. Choisissez l'une des options suivantes :
   - Cliquez sur **Ajouter un nouvel espace de travail** pour créer un nouvel espace de travail.
   - Cliquez sur **Renommer** pour renommer l'espace de travail.
   - Cliquez sur **Supprimer** pour supprimer l'espace de travail.

Gestion des espaces de travail d'un connecteur

Vous devez associer le connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent accéder à ces espaces de travail à partir de Cloud Manager.

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 sur les utilisateurs, les espaces de travail et les connecteurs".

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.
2. Cliquez sur **connecteur**.
3. Cliquez sur **gérer les espaces de travail** pour le connecteur que vous souhaitez associer.
4. Sélectionnez les espaces de travail à associer au connecteur et cliquez sur **appliquer**.

Gestion des abonnements

Après vous être abonné au Marketplace d'un fournisseur cloud, chaque abonnement est disponible dans le widget Account Settings. Vous avez la possibilité de renommer un abonnement et de dissocier l'abonnement d'un ou plusieurs comptes.

Par exemple, disons que vous avez deux comptes et que chacun est facturé par le biais d'abonnements distincts. Vous pouvez dissocier un abonnement de l'un des comptes afin que les utilisateurs de ce compte ne choisissent pas accidentellement l'abonnement incorrect lors de la création d'un environnement de travail Cloud Volume ONTAP.

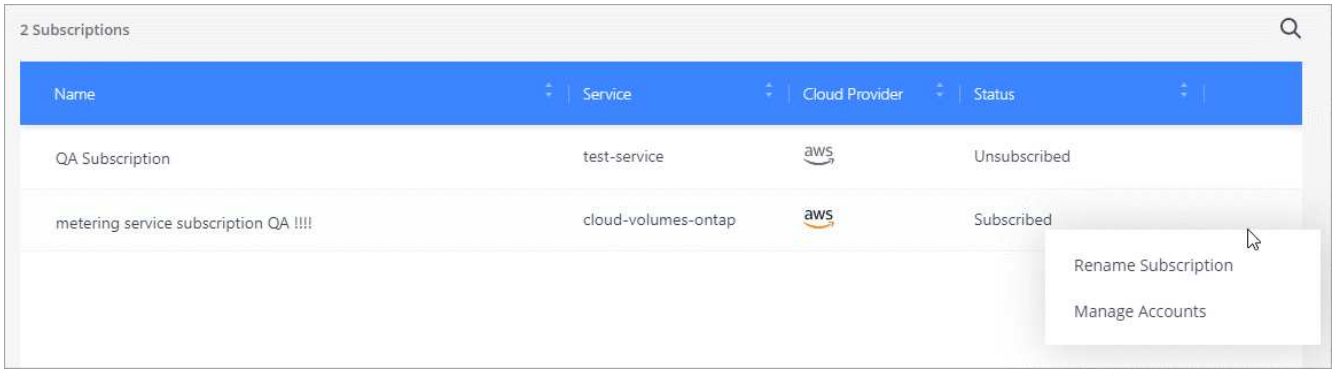
"En savoir plus sur les abonnements".

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.
2. Cliquez sur **abonnements**.

   Vous ne verrez que les abonnements associés au compte que vous consultez actuellement.

3. Cliquez sur le menu d'action de la ligne correspondant à l'abonnement que vous souhaitez gérer.



4. Choisissez de renommer l'abonnement ou de gérer les comptes associés à l'abonnement.

Modification du nom du compte

Changez le nom de votre compte à tout moment pour le changer en quelque chose de significatif pour vous.

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.
2. Dans l'onglet **vue d'ensemble**, cliquez sur l'icône de modification en regard du nom du compte.
3. Saisissez un nouveau nom de compte et cliquez sur **Enregistrer**.

Activation ou désactivation de la plateforme SaaS

Nous ne recommandons pas de désactiver la plate-forme SaaS sauf si vous devez vous conformer aux politiques de sécurité de votre entreprise. En désactivant la plateforme SaaS, vous vous limitent votre capacité à utiliser les services cloud intégrés de NetApp.

Si vous désactivez la plateforme SaaS, les services suivants ne sont pas disponibles depuis Cloud Manager :

- Conformité cloud
- Kubernetes
- Tiering dans le cloud
- Cache global de fichiers
- Surveillance (Cloud Insights)

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.
2. Dans l'onglet **Présentation**, activez l'option utiliser la plateforme SaaS.

Gestion d'un certificat HTTPS pour l'accès sécurisé

Par défaut, Cloud Manager utilise un certificat auto-signé pour l'accès HTTPS à la console Web. Vous pouvez installer un certificat signé par une autorité de certification (CA), qui offre une meilleure protection de la sécurité qu'un certificat auto-signé.

Avant de commencer

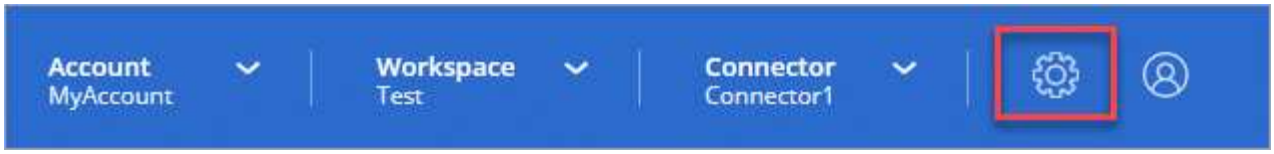
Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Installation d'un certificat HTTPS

Installez un certificat signé par une autorité de certification pour un accès sécurisé.

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **HTTPS Setup**.

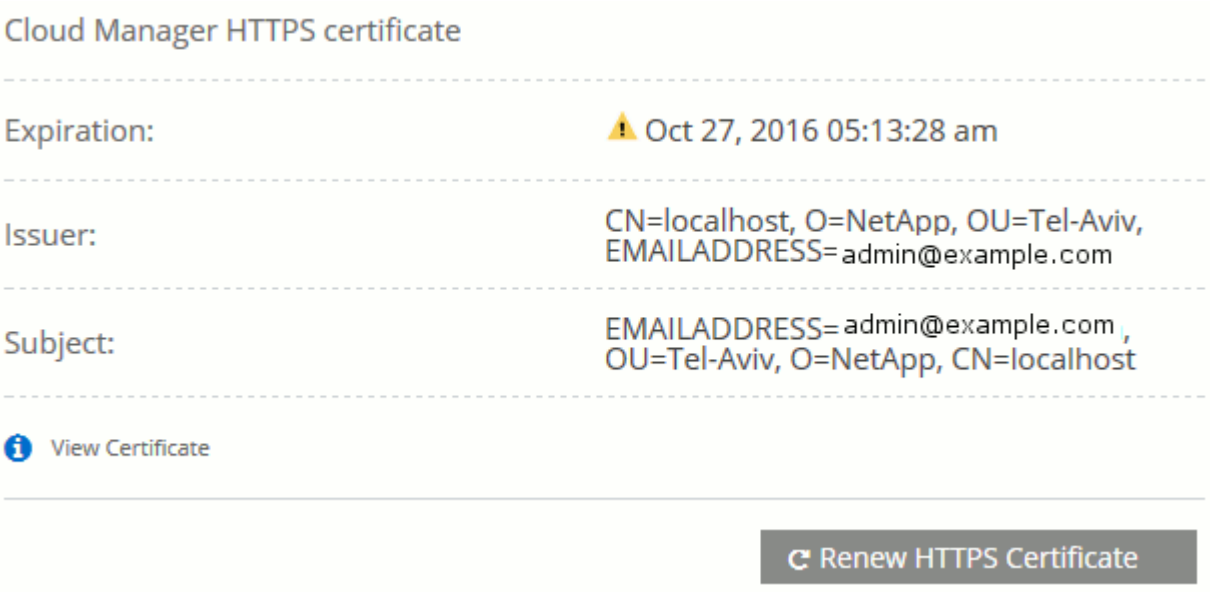


2. Dans la page Configuration HTTPS, installez un certificat en générant une requête de signature de certificat (CSR) ou en installant votre propre certificat signé par l'autorité de certification :

Option	Description
Générez une RSC	a. Entrez le nom d'hôte ou le DNS de l'hôte du connecteur (son nom commun), puis cliquez sur **generate CSR**. Cloud Manager affiche une demande de signature de certificat. b. Utilisez la RSC pour envoyer une demande de certificat SSL à une autorité de certification. Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64. c. Copiez le contenu du certificat signé, collez-le dans le champ certificat, puis cliquez sur **installer**.
Installez votre propre certificat signé par l'autorité de certification	a. Sélectionnez **installer le certificat signé CA**. b. Chargez le fichier de certificat et la clé privée, puis cliquez sur **installer**. Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.

Résultat

Cloud Manager utilise désormais le certificat signé par l'autorité de certification pour fournir un accès HTTPS sécurisé. L'image suivante montre un système Cloud Manager configuré pour un accès sécurisé :



Renouvellement du certificat HTTPS de Cloud Manager

Vous devez renouveler le certificat HTTPS de Cloud Manager avant son expiration pour garantir un accès sécurisé à la console Web de Cloud Manager. Si vous ne renouvelez pas le certificat avant son expiration, un avertissement s'affiche lorsque les utilisateurs accèdent à la console Web via HTTPS.

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **HTTPS Setup**.

   Des informations détaillées sur le certificat Cloud Manager s'affichent, y compris la date d'expiration.

2. Cliquez sur **renouveler le certificat HTTPS** et suivez les étapes pour générer une RSC ou installer votre propre certificat signé par une CA.

Résultat

Cloud Manager utilise le nouveau certificat signé par l'autorité de certification pour fournir un accès HTTPS sécurisé.

Suppression des environnements de travail Cloud Volumes ONTAP

L'administrateur des comptes peut supprimer un environnement de travail Cloud Volumes ONTAP pour le déplacer vers un autre système ou pour résoudre les problèmes de détection.

Description de la tâche

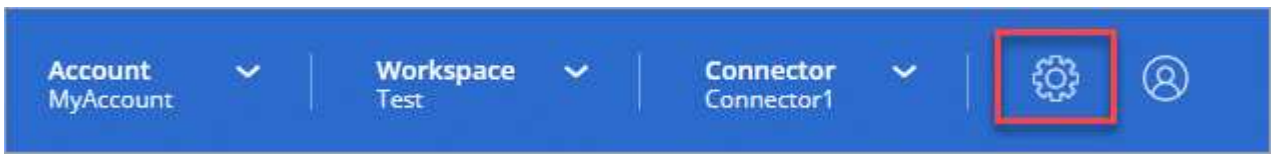
La suppression d'un environnement de travail Cloud Volumes ONTAP le supprime de Cloud Manager. Il ne supprime pas le système Cloud Volumes ONTAP. Vous pourrez par la suite redécouvrir l'environnement de travail.

La suppression d'un environnement de travail de Cloud Manager vous permet d'effectuer les opérations suivantes :

- Redécouvrez-le dans un autre espace de travail
- Redécouvrez-le à partir d'un autre système Cloud Manager
- Redécouvrez-le si vous avez rencontré des problèmes lors de la découverte initiale

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres, puis sélectionnez **Outils**.



2. Dans la page Outils, cliquez sur **lancer**.
3. Sélectionnez l'environnement de travail Cloud Volumes ONTAP que vous souhaitez supprimer.
4. Sur la page Revue et approbation, cliquez sur **Go**.

Résultat

Cloud Manager supprime l'environnement de travail. Les utilisateurs peuvent à tout moment redécouvrir cet environnement de travail à partir de la page des environnements de travail.

Configuration d'un connecteur pour utiliser un serveur proxy

Si vos stratégies d'entreprise exigent que vous utilisiez un serveur proxy pour toutes les communications HTTP vers Internet, vous devez configurer vos connecteurs pour utiliser ce serveur proxy. Le serveur proxy peut se trouver dans le cloud ou dans votre réseau.

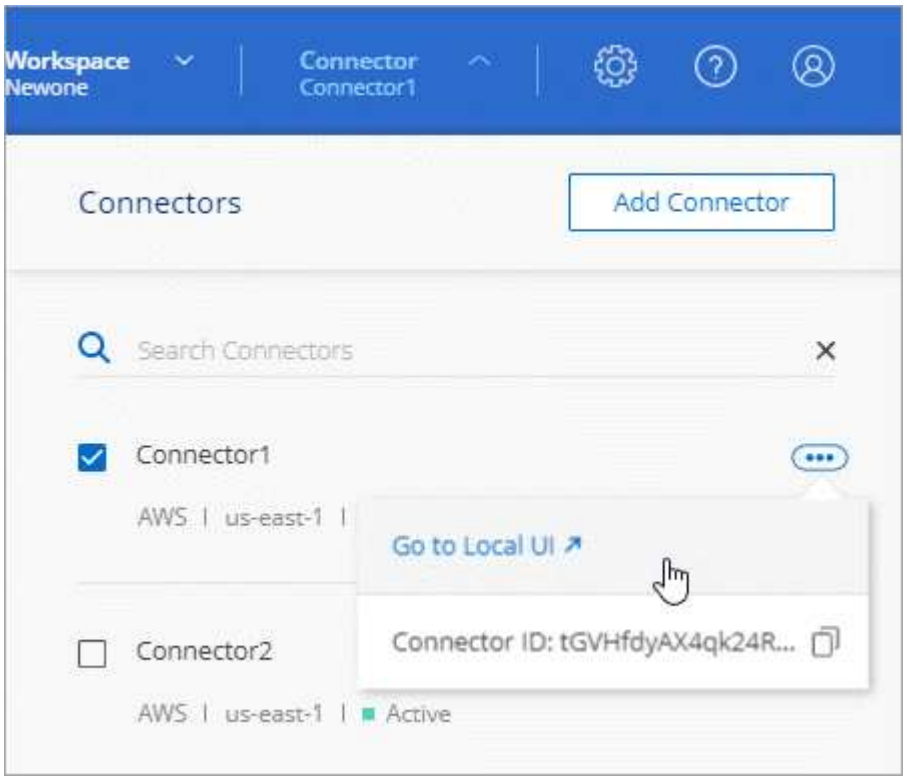
Lorsque vous configurez un connecteur pour utiliser un serveur proxy, ce connecteur et les systèmes Cloud Volumes ONTAP qu'il gère (y compris les médiateurs HA) utilisent tous le serveur proxy.

Étapes

1. "Connectez-vous à l'interface SaaS Cloud Manager" À partir d'une machine dotée d'une connexion réseau à l'instance de connecteur.

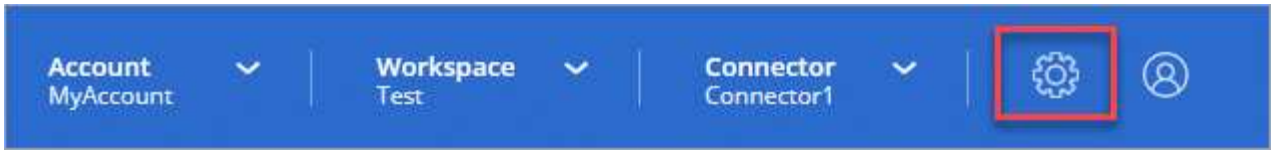
   Si le connecteur n'est pas doté d'une adresse IP publique, vous aurez besoin d'une connexion VPN ou vous devrez vous connecter à partir d'un hôte de secours situé sur le même réseau que le connecteur.

2. Cliquez sur la liste déroulante **Connector**, puis cliquez sur **allez à l'interface utilisateur locale** pour un connecteur spécifique.



   L'interface Cloud Manager exécutée sur le connecteur est chargée dans un nouvel onglet du navigateur.

3. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **Cloud Manager Settings**.



4. Sous Proxy HTTP, entrez le serveur à l’aide de la syntaxe http://address:port, Indiquez un nom d’utilisateur et un mot de passe si une authentification de base est requise pour le serveur, puis cliquez sur Enregistrer.

Cloud Manager ne prend pas en charge les mots de passe comprenant le caractère @.

Résultat

Après avoir spécifié le serveur proxy, les nouveaux systèmes Cloud Volumes ONTAP sont automatiquement configurés pour utiliser le serveur proxy lors de l'envoi de messages AutoSupport. Si vous n'avez pas spécifié le serveur proxy avant que les utilisateurs créent des systèmes Cloud Volumes ONTAP, ils doivent utiliser le Gestionnaire système pour définir manuellement le serveur proxy dans les options AutoSupport de chaque système.

Remplacement des verrouillages CIFS pour Cloud Volumes ONTAP HA dans Azure

L'administrateur du compte peut activer un paramètre dans Cloud Manager qui empêche les problèmes liés au basculement du stockage Cloud Volumes ONTAP lors des événements de maintenance Azure. Lorsque vous activez ce paramètre, Cloud Volumes ONTAP vetoes les verrous CIFS et réinitialise les sessions CIFS actives.

Description de la tâche

Microsoft Azure planifie des événements de maintenance périodiques sur ses machines virtuelles. Lorsqu'un événement de maintenance se produit sur un nœud d'une paire haute disponibilité Cloud Volumes ONTAP, la paire haute disponibilité démarre le basculement du stockage. S'il existe des sessions CIFS actives au cours de cet événement de maintenance, les verrous sur les fichiers CIFS peuvent empêcher le basculement du stockage.

Si vous activez ce paramètre, Cloud Volumes ONTAP veto aux verrous et réinitialise les sessions CIFS actives. Par conséquent, la paire haute disponibilité peut effectuer le basculement du stockage lors de ces opérations de maintenance.

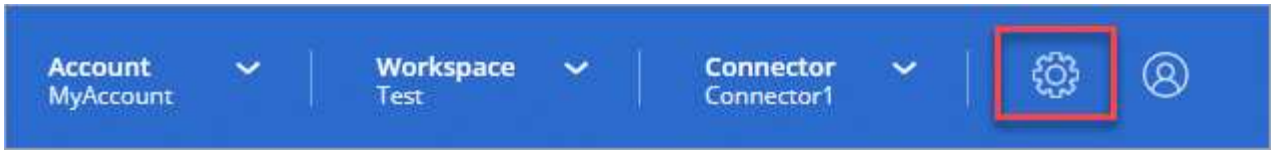
Ce processus peut entraîner des perturbations pour les clients CIFS. Les données qui ne sont pas validées auprès des clients CIFS pourraient être perdues.

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **Cloud Manager Settings**.



2. Sous **HA CIFS Locks**, cochez la case et cliquez sur **Save**.

Référence

Rôles

Les rôles Administrateur de compte, Administrateur d'espace de travail et Visionneuse de conformité cloud fournissent des autorisations spécifiques aux utilisateurs.

Tâche	Administrateur du compte	Administrateur de l'espace de travail	Visualiseur Cloud Compliance
Gérer les environnements de travail	Oui.	Oui.	Non
Activer les services dans les environnements de travail	Oui.	Oui.	Non
Afficher l'état de la réplication des données	Oui.	Oui.	Non
Afficher la chronologie	Oui.	Oui.	Non
Basculer entre les espaces de travail	Oui.	Oui.	Oui.
Afficher les résultats de l'analyse de conformité	Oui.	Oui.	Oui.
Supprimer les environnements de travail	Oui.	Non	Non
Connectez les clusters Kubernetes aux environnements de travail	Oui.	Non	Non
Recevoir le rapport Cloud Volumes ONTAP	Oui.	Non	Non
Créer des connecteurs	Oui.	Non	Non
Gérez les comptes Cloud Central	Oui.	Non	Non
Gérer les identifiants	Oui.	Non	Non
Modifiez les paramètres de Cloud Manager	Oui.	Non	Non
Afficher et gérer le tableau de bord du support	Oui.	Non	Non
Supprimez les environnements de travail de Cloud Manager	Oui.	Non	Non

Tâche	Administrateur du compte	Administrateur de l'espace de travail	Visualiseur Cloud Compliance
Installez un certificat HTTPS	Oui.	Non	Non

Liens connexes

- "Configuration d'espaces de travail et d'utilisateurs sur le compte Cloud Central"
- "Gestion des espaces de travail et des utilisateurs sur le compte Cloud Central"

Comment Cloud Manager utilise les autorisations du fournisseur cloud

Cloud Manager nécessite des autorisations pour effectuer des actions dans votre fournisseur cloud. Ces autorisations sont incluses dans "Règles fournies par NetApp". Vous pouvez comprendre ce que fait Cloud Manager avec ces autorisations.

Ce que fait Cloud Manager avec les autorisations AWS

Cloud Manager utilise un compte AWS pour effectuer des appels API vers plusieurs services AWS, notamment EC2, S3, CloudFormation, IAM, Security Token Service (STS) et le service de gestion des clés (KMS).

Actions	Objectif
"ec2:StartInstances", "ec2:StopInstances", "ec2:Décrivez les occurrences", "ec2:Ddescriptif InstanceStatus", "ec2:RunInstances", « ec2:TerminateInstances », « ec2:ModimodificationAttribute »,	Lance une instance Cloud Volumes ONTAP et arrête, démarre et surveille l'instance.
"EC2:DescribeInstanceAttribute",	Vérifie que la mise en réseau améliorée est activée pour les types d'instance pris en charge.
"ec2:descriptifs", "ec2:descriptifs",	Lance une configuration Cloud Volumes ONTAP HA.
"EC2:CreateTags",	Marque chaque ressource créée par Cloud Manager à l'aide des balises WorkingEnvironment et WorkingEnvironmentId. Cloud Manager utilise ces balises pour la maintenance et l'allocation des coûts.
« ec2:CreateVolume », « ec2:Describevolumes », « ec2:ModityVolumeAttribute », « ec2:AttachVolume », « ec2:DeleteVolume », « ec2:DetachVolume »,	Gère les volumes EBS utilisés par Cloud Volumes ONTAP en tant que stockage back-end.
« ec2:CreateSecurityGroup », « ec2:DeleteSecurityGroup », « ec2:descriptif SecurityGroups », « ec2:RevokeSecurityGroupEgress », « ec2:AuthoreSecurityGroupEgress », « ec2:AuthoreSecurityGroupEgress », « ec2:AuthoreSecurityGroupIngress », « ec2:RevokeSecurityGroupIngress »,	Crée des groupes de sécurité prédéfinis pour Cloud Volumes ONTAP.
« ec2:CreateNetworkinterface », « ec2:DescribeNetworkinterfaces », « ec2:DeleteNetworkinterface », « ec2:ModityNetworkInterfaceAttribute »,	Crée et gère des interfaces réseau pour Cloud Volumes ONTAP dans le sous-réseau cible.

Actions	Objectif
"ec2:DescribeSubnets", "ec2:DescribeVpcs",	Récupère la liste des sous-réseaux de destination et des groupes de sécurité nécessaires à la création d'un nouvel environnement de travail pour Cloud Volumes ONTAP.
"EC2:DescribeDhcpOptions",	Détermine les serveurs DNS et le nom de domaine par défaut lors du lancement des instances Cloud Volumes ONTAP.
« ec2:CreateSnapshot », « ec2:DeleteSnapshot », « ec2:Ddescriptif »,	Prend des snapshots des volumes EBS lors de la configuration initiale et chaque fois qu'une instance Cloud Volumes ONTAP est arrêtée.
" EC2:GetConsoleOutput ",	Capture la console Cloud Volumes ONTAP, associée aux messages AutoSupport.
"EC2:DécribeKeyPair",	Obtient la liste des paires de clés disponibles lors du lancement d'instances.
"EC2:DécribeRegions",	Récupère une liste des régions AWS disponibles.
« ec2:DeleteTags », « ec2:Ddescriptif »,	Gère les balises des ressources associées aux instances Cloud Volumes ONTAP.
"Cloudformation:CreateStack", "cloudformation:DeleteStack", "cloudformation:DescribeSacks", "cloudformation:DescribeStackEvents", "cloudformation:ValidateTemplate",	Lance les instances Cloud Volumes ONTAP.
« iam:PassRole », « iam:CreateRole », « iam:DeleteRole », « iam:PutRolePolicy », « iam:CreateInstanceProfile », "iam:DeleteRolePolicy", "iam:AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "iam:DeleteInstanceProfile",	Lance une configuration Cloud Volumes ONTAP HA.
« iam:ListenInstanceProfiles », « sts:DecodeAuthorationmessage », « ec2:AssociationIamInstanceProfile », « ec2:DécrideIamInstanceInstanceProfileassociations », « ec2:DisassociateIamInstanceProfile »,	Gère les profils d'instance des instances Cloud Volumes ONTAP.
« s3:GetBuckeTagging », « s3:GetBuckeLocation », « s3:ListAllMyPets », « s3:ListBucket »	Obtenez des informations sur les compartiments AWS S3 pour que Cloud Manager puisse s'intégrer au service NetApp Data Fabric Cloud Sync.
« s3:CreateBucket », « s3:DeleteBucket », « s3:GetLifecyclConfiguration », « s3:PutLifecycleConfiguration », « s3:PutBuckeTagging », « s3:ListBuckeVersions », « s3:GetBuckePolicyStatus », « s3:GetBuckePublicAccessBlock », « s3:GetBuckeAcl », « s3:GetBuckePolicy », « s3:GetBuckePolicy », "s3:PutBuckePublicAccessBlock"	Gère le compartiment S3 utilisé par un système Cloud Volumes ONTAP comme Tier de capacité pour le Tiering des données.

Actions	Objectif
"Km:liste*", "km:reEncrypt*", "km:décrire*", "km:CreateGrant",	Chiffrement des données d'Cloud Volumes ONTAP à l'aide du service AWS Key Management Service (KMS).
"ce:GetReservationUtilization", "ce:GetDimensionValues", "ce:GetCostAndUsage", "ce:GetTags"	Obtient les données de coût AWS pour Cloud Volumes ONTAP.
« ec2:CreatePlaceGroup », « ec2:Deleteplacer GroupeDe »	Lorsque vous déployez une configuration HA dans une seule zone de disponibilité AWS, Cloud Manager lance les deux nœuds HA et le médiateur dans un groupe de placement AWS.
« ec2:descriptifsd'InstanciquesOfferings »	Cloud Manager utilise l'autorisation dans le cadre du déploiement de Cloud Compliance pour choisir le type d'instance à utiliser.
« s3:DeleteBucket », « s3:GetLifecyclConfiguration », « s3:PutLifecycletConfiguration », « s3:PutBuckeTagging », « s3:ListBuckeVersions », « s3:GetObject », « s3:ListBucket », « s3:ListAllMyPets », « s3:GetBuckeTagging », « s3:GetBuckeLocation » « s3:GetBuckePolicyStatus », "s3:GetBuckePublicAccessBlock", "s3:GetBuckeAcl", "s3:GetBuckePolicy", "s3:PutBuckePublicAccessBlock"	Cloud Manager utilise ces autorisations lorsque vous activez le service Backup vers S3.

Ce que fait Cloud Manager avec les autorisations Azure

La stratégie Cloud Manager Azure inclut les autorisations dont Cloud Manager a besoin pour déployer et gérer Cloud Volumes ONTAP dans Azure.

Actions	Objectif
« Microsoft.Compute/locations/operations/read", « Microsoft.Compute/locations/vmSizes/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/start/action", « Microsoft.Compute/virtualMachines/deallocate/action", « Microsoft.Compute/virtualMachines/vmSizes/read", « Microsoft.Compute/virtualMachines/write",	Crée Cloud Volumes ONTAP et arrête, démarre, supprime et obtient l'état du système.
« Microsoft.Compute/images/write", « Microsoft.Compute/images/read",	Permet le déploiement de Cloud Volumes ONTAP à partir d'un disque VHD.

Actions	Objectif
« Microsoft.Compute/disks/delete", « Microsoft.Compute/disks/read", « Microsoft.Compute/disks/write", Microsoft.Storage/checkkamedisponibilité/read », « Microsoft.Storage/Operations/read », « Microsoft.Storage/storageAccounts/listkeys/action », « Microsoft.Storage/storageAccounts/read », « Microsoft.Storage/storageAccounts/redynamekey/action », « Microsoft.Storage/storageAccounts/write » « Microsoft.Storage/StorageAccounts/delete », « Microsoft.Storage/eancs/read »,	Gère les comptes et les disques de stockage Azure et les connecte à Cloud Volumes ONTAP.
« Microsoft.Network/networkInterfaces/read", « Microsoft.Network/networkInterfaces/write", « Microsoft.Network/networkInterfaces/join/action",	Crée et gère des interfaces réseau pour Cloud Volumes ONTAP dans le sous-réseau cible.
« Microsoft.Network/networkSecurityGroups/read", « Microsoft.Network/networkSecurityGroups/write", « Microsoft.Network/networkSecurityGroups/join/action",	Crée des groupes de sécurité réseau prédéfinis pour Cloud Volumes ONTAP.
« Microsoft.Resources/abonnements/emplacements/lecture », « Microsoft.Network/locations/operationResults/read", « Microsoft.Network/locations/operations/read", « Microsoft.Network/virtualNetworks/read", « Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", » « Microsoft.Network/virtualNetworks/subnets/read", « Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", « Microsoft.Network/virtualNetworks/virtualMachines/read", « Microsoft.Network/virtualNetworks/subnets/join/action",	Récupère les informations réseau sur les régions, le VNet cible et le sous-réseau, et ajoute Cloud Volumes ONTAP aux VNets.
« Microsoft.Network/virtualNetworks/subnets/write", « Microsoft.Network/routeTables/join/action",	Active les terminaux de service VNet pour le hiérarchisation des données.
« Microsoft.Resources/déploiements/opérations/lecture », « Microsoft.Resources/déploiements/lecture », « Microsoft.Resources/déploiements/écriture »,	Déploie Cloud Volumes ONTAP à partir d’un modèle.

Actions	Objectif
« Microsoft.Resources/déploiements/opérations/lecture », « Microsoft.Resources/déploiements/lecture », « Microsoft.Resources/déploiements/écriture », « Microsoft.Resources/Resources/read », « Microsoft.Resources/abonnements/résultats d'opération/lecture », « Microsoft.Resources/souscriptions/resourceGroups/delete », « Microsoft.Resources/souscriptions/resourceGroups/read », « Microsoft.Resources/souscriptions/resourcesgroupe/resources/read », « Microsoft.Resources/souscriptions/resourceGroups/write »,	Crée et gère des groupes de ressources pour Cloud Volumes ONTAP.
« Microsoft.Compute/snapshots/write", « Microsoft.Compute/snapshots/read", « Microsoft.Compute/disks/beginGetAccess/action"	Crée et gère les snapshots gérés par Azure.
« Microsoft.Compute/availabilitySets/write", « Microsoft.Compute/availabilitySets/read",	Crée et gère des ensembles de disponibilité pour Cloud Volumes ONTAP.
« Microsoft.MarketplaceOrdering/Offres/éditeurs/offres/plans/accords/lecture », « Microsoft.MarketplaceOrdering/Offres/Offres/plans/accords/write »	Permet des déploiements programmatiques depuis Azure Marketplace.
« 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/frontendIPConfigurations/read", « Microsoft.Network/loadBalancers/loadBalancingRules/read", « Microsoft.Network/loadBalancers/probes/read", « Microsoft.Network/loadBalancers/probes/join/action",	Gère un équilibreur de charge Azure pour les paires HA.
" Microsoft.Authorization/locks/* "	Permet la gestion des verrous sur les disques Azure.
"Microsoft.Authorization/roleDefinitions/écrire", "Microsoft.Authorization/roleassignations/écrire", "Microsoft.Web/sites/*"	Gestion du basculement pour les paires haute disponibilité.

Actions	Objectif
« Microsoft.Network/privateEndpoints/write", « Microsoft.Storage/StorageAccounts/PrivateEndpointConnectionsApproval/action », « Microsoft.Storage/storageAccounts/EndprivatepointConnections/read », « 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",	Permet la gestion des terminaux privés. Les terminaux privés sont utilisés lorsque la connectivité n'est pas fournie à l'extérieur du sous-réseau. Cloud Manager crée le compte de stockage pour la haute disponibilité avec une connectivité interne uniquement au sein du sous-réseau.
« Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",	Permet à Cloud Manager de supprimer des volumes pour Azure NetApp Files.
« Microsoft.Resources/déploiements/opérations Statelis/lectures »	Azure requiert cette autorisation pour certains déploiements de machines virtuelles (elle dépend du matériel physique sous-jacent utilisé lors du déploiement).
« Microsoft.Resources/déploiements/opérations Statelis/lire », « Microsoft.Insights/Metrics/Read », « Microsoft.Compute/virtualMachines/extensions/write", « Microsoft.Compute/virtualMachines/extensions/read", « Microsoft.Compute/virtualMachines/extensions/delete", « Microsoft.Compute/virtualMachines/delete", « Microsoft.Network/networkInterfaces/delete", « Microsoft.Network/networkSecurityGroups/delete", Microsoft.Resources/déploiements/suppression »,	Permet d'utiliser Global File cache.
« Microsoft.Compute/diskEncryptionSets/read"	Permet à Cloud Manager de chiffrer les disques gérés Azure sur des systèmes Cloud Volumes ONTAP à un seul nœud à l'aide de clés externes provenant d'un autre compte. Cette fonctionnalité est prise en charge à l'aide d'API.

Avantages de Cloud Manager avec les autorisations GCP

La règle Cloud Manager pour GCP inclut les autorisations nécessaires à Cloud Manager pour déployer et gérer Cloud Volumes ONTAP.

Actions	Objectif
- Compute.disks.create - Compute.disks.createSnapshot - compute.disks.delete - Compute.disks.get - Compute.disks.list - compute.disks.setLabels - compute.disks.use	Pour créer et gérer des disques pour Cloud Volumes ONTAP.

Actions	Objectif
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Pour créer des règles de pare-feu pour Cloud Volumes ONTAP.
- Compute.globalOperations.get	Pour obtenir l'état des opérations.
- Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly	Pour obtenir les images des instances de VM.
- compute.instances.attachDisk - compute.instances.detachDisk	Pour attacher et détacher les disques à Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Pour créer et supprimer des instances de VM Cloud Volumes ONTAP.
- compute.instances.get	Pour afficher la liste des instances de VM.
- compute.instances.getSerialPortOutput	Pour obtenir les journaux de la console.
- compute.instances.list	Pour récupérer la liste des instances dans une zone.
- compute.instances.setDeletionProtection	Pour définir la protection de suppression sur l'instance.
- compute.instances.setLabels	Pour ajouter des étiquettes.
- compute.instances.setMachineType	Pour modifier le type de machine pour Cloud Volumes ONTAP.
- compute.instances.setMetadata	Pour ajouter des métadonnées.
- compute.instances.setTags	Pour ajouter des balises pour les règles de pare-feu.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Pour démarrer et arrêter Cloud Volumes ONTAP.
- Compute.machineTypes.get	Pour obtenir le nombre de cœurs à vérifier qoupas.
- compute.projects.get	Pour prendre en charge des projets multiples.
- Compute.snapshots.create - compute.snapshots.delete - Compute.snapshots.get - Compute.snapshots.list - compute.snapshots.setLabels	Pour créer et gérer des snapshots de disques persistants.
- compute.networks.get - compute.networks.list - Compute.rerégions.get - Compute.rerégions.list - Compute.subNetworks.get - Compute.subNetworks.list - Compute.zoneOperations.get - Compute.zones.get - Compute.zones.zones.list	Pour obtenir les informations de mise en réseau nécessaires à la création d'une nouvelle instance de machine virtuelle Cloud Volumes ONTAP.

Actions	Objectif
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifestes.get - deploymentmanager.manifestes.list - deploymentmanager.Operations.get - deploymentmanager.Operations.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get.types.deploymentmanager.deploymentmanager.deploymentlist.types.deploymentmanager.deploymentlist.deploymentmanager.deploymentmanager.Deploymenttypes.DeploymentManager.Deploymentlist.Deploymenttypes.DeploymentManager.Deployment	Pour déployer l'instance de machine virtuelle Cloud Volumes ONTAP à l'aide de Google Cloud Deployment Manager.
- Logging.logEntries.list - logging.privateLogEntries.list	Pour obtenir les disques de consignation des piles.
- resourcemanager.projects.get	Pour prendre en charge des projets multiples.
- storage.seaux.create - storage.buckets.delete - storage.seaux.get - storage.seaux.list - storage.seaux.update	Pour créer et gérer un compartiment Google Cloud Storage pour le Tiering des données.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.crypKeys.list - cloudkms.keyrings.list	Pour utiliser des clés de chiffrement gérées par le client à partir du service Cloud Key Management avec Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list	Pour définir un compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations de Tiering des données vers un compartiment Google Cloud Storage.

Pages AWS Marketplace pour Cloud Manager et Cloud Volumes ONTAP

Plusieurs offres sont disponibles sur AWS Marketplace pour Cloud Manager et Cloud Volumes ONTAP. Si vous avez besoin d'aide pour comprendre le but de chaque page, lisez les descriptions ci-dessous.

Dans tous les cas, n'oubliez pas que vous ne pouvez pas lancer Cloud Volumes ONTAP sur AWS à partir d'AWS Marketplace. Vous devez le lancer directement depuis Cloud Manager.

Objectif	Page AWS Marketplace à utiliser	Plus d'informations
Activez l'utilisation de Cloud Volumes ONTAP PAYGO, Cloud Tiering, Cloud Compliance et d'autres services d'extension	"Cloud Manager - déploiement et gestion des services de données cloud NetApp"	Cet abonnement permet de facturer la version PAYGO de Cloud Volumes ONTAP 9.6 et versions ultérieures. Il permet également de facturer les services de Tiering cloud, de conformité cloud et d'autres services complémentaires. Vous devez vous abonner à cette offre lorsque Cloud Manager vous invite à vous rediriger vers la page. Cloud Manager vous invite dans l'assistant Working Environment ou lorsque vous ajoutez de nouveaux identifiants dans les paramètres. Cette page ne vous permet pas de lancer Cloud Manager dans AWS. Cela devrait être fait à partir de "NetApp Cloud Central", Ou bien en utilisant l'ami répertorié à la ligne 3 de ce tableau.
Faciliter l'utilisation Cloud Volumes ONTAP de PAYGO, Cloud Tiering, Cloud Compliance et d'autres services d'extension *par le biais d'un contrat annuel*	"Cloud Manager (contrats) - déploiement et gestion des services de données cloud NetApp"	Cet abonnement est une alternative à l'abonnement sur la première ligne. Il vous permet d'obtenir un paiement annuel initial pour vos offres. Elle s'adresse principalement aux partenaires NetApp.
Déployez Cloud Manager depuis AWS Marketplace à l'aide d'une ami	"Cloud Manager : installation manuelle sans clés d'accès"	Nous vous recommandons de lancer Cloud Manager dans AWS à partir de "NetApp Cloud Central", Mais vous pouvez le lancer à partir de cette page AWS Marketplace, si vous préférez.
Déploiement de la formule de facturation Cloud Volumes ONTAP (9.5 ou antérieure)	• "Cloud Volumes ONTAP pour AWS" • "Cloud Volumes ONTAP pour AWS - haute disponibilité"	Ces pages AWS Marketplace vous permettent de vous abonner aux versions à un nœud ou haute disponibilité de Cloud Volumes ONTAP PAYGO pour les versions 9.5 et précédentes. À partir de la version 9.6, vous devez vous inscrire sur la page AWS Marketplace (première ligne de ce tableau pour les déploiements PAYGO).

Informations sur le copyright

Informations sur les marques commerciales