Azure

Cloud Manager 3.8

NetApp
March 25, 2024

Sommaire

Azure

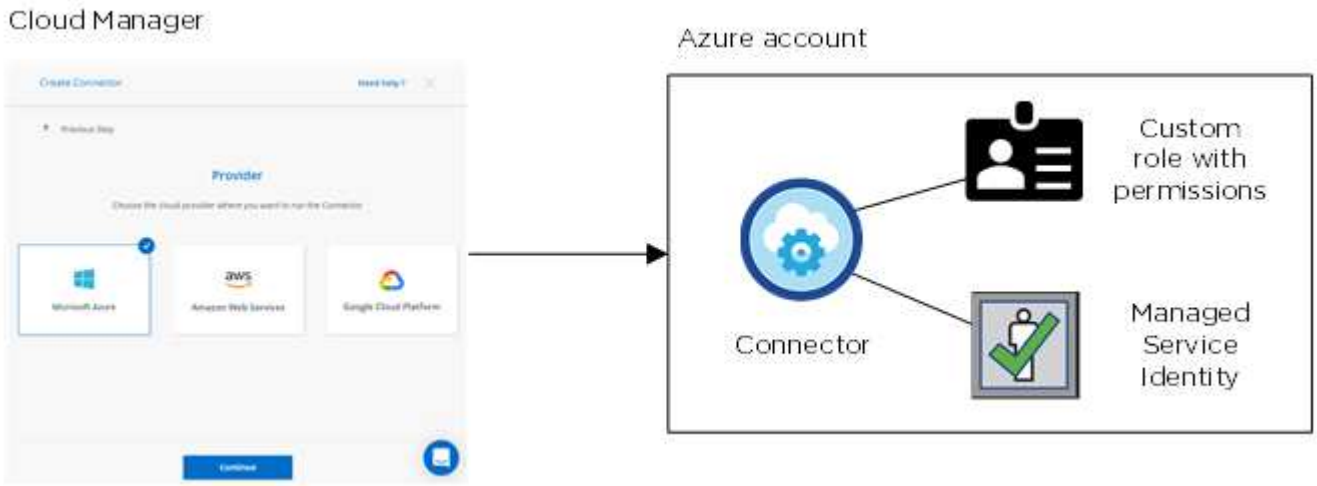
Identifiants et autorisations Azure

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.

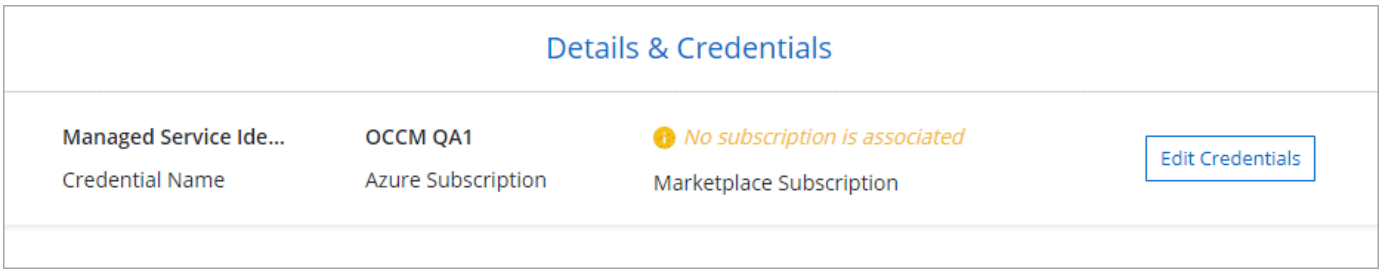
Les identifiants initiaux d'Azure

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 :

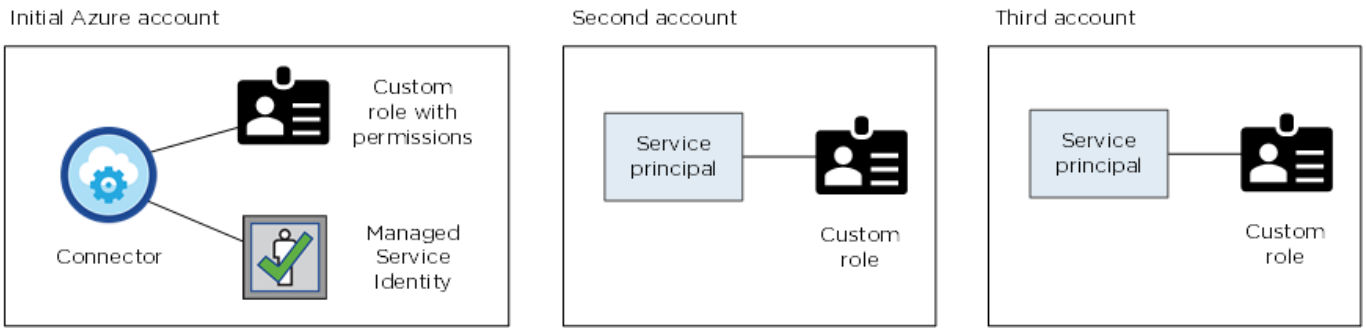


Des abonnements Azure supplémentaires pour une identité gérée

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".

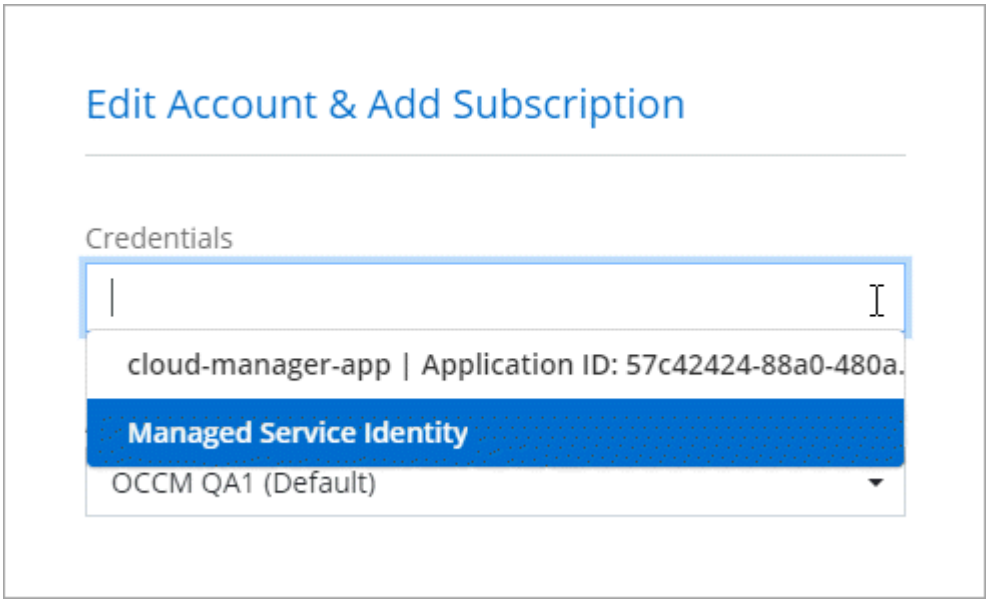
Autres identifiants Azure

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.

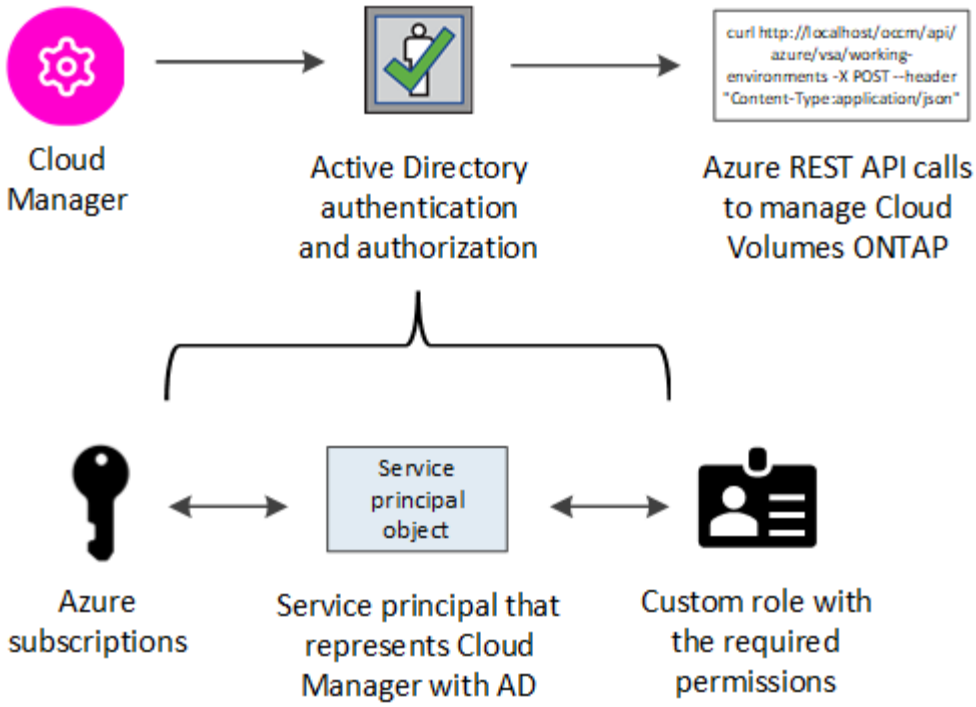
Lorsque vous déployez un connecteur depuis Cloud Manager, Cloud Manager ajoute automatiquement le compte Azure dans lequel vous avez déployé le connecteur. Un compte initial n'est pas ajouté si vous avez installé manuellement le logiciel Connector sur un système existant. "En savoir plus sur les comptes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

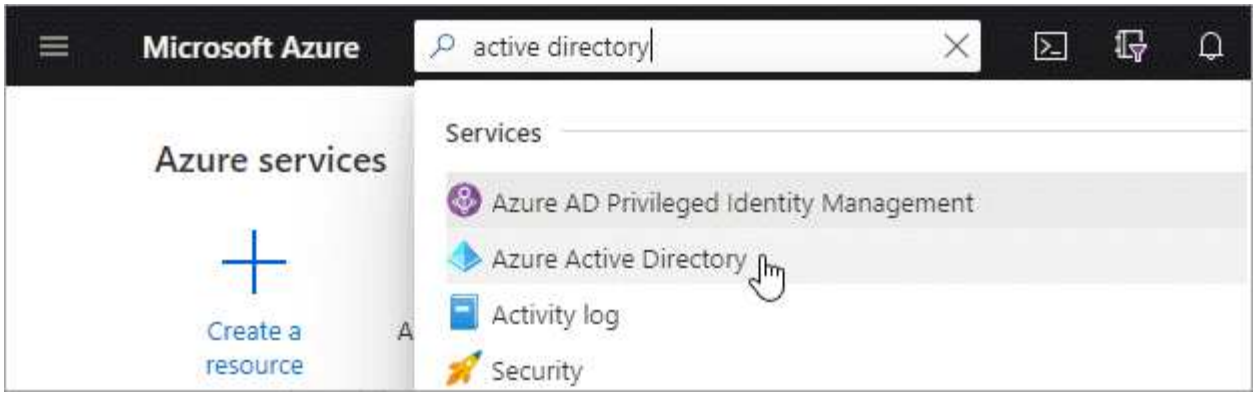
Créez une application Azure Active Directory (AD) et une entité de service que Cloud Manager peut utiliser pour le contrôle d'accès basé sur des rôles.

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**.

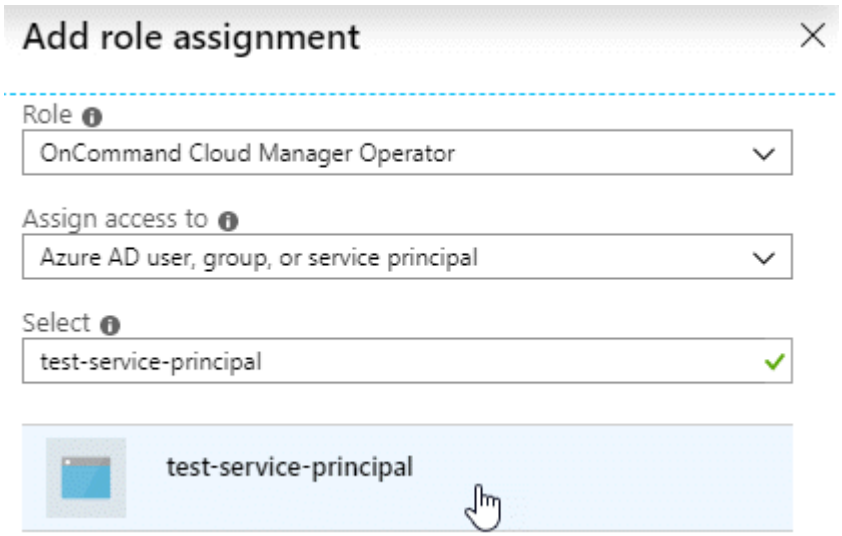
   b. Sélectionnez l'abonnement.

   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.

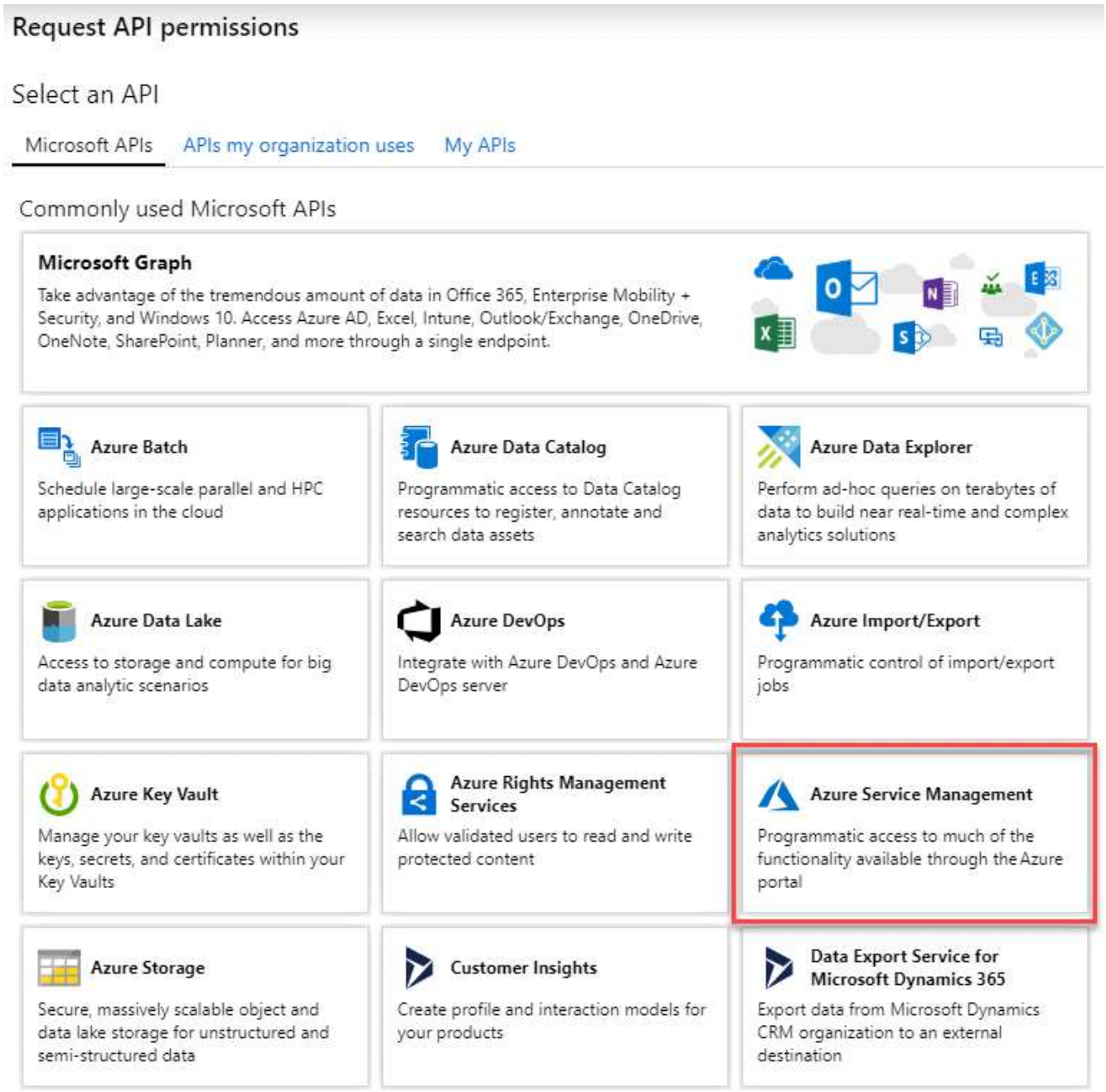
Si vous souhaitez déployer Cloud Volumes ONTAP à partir de plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. Cloud Manager vous permet de sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

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

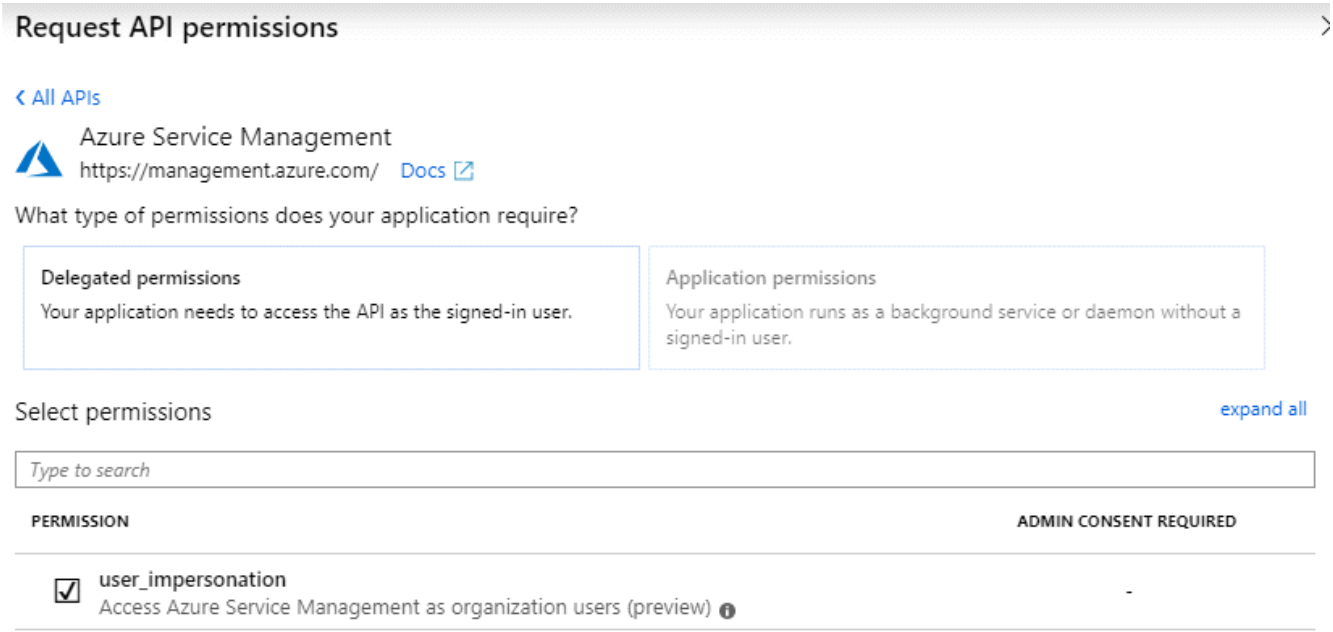
Le principal de service doit disposer d'autorisations « API de gestion des services Windows Azure ».

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**.

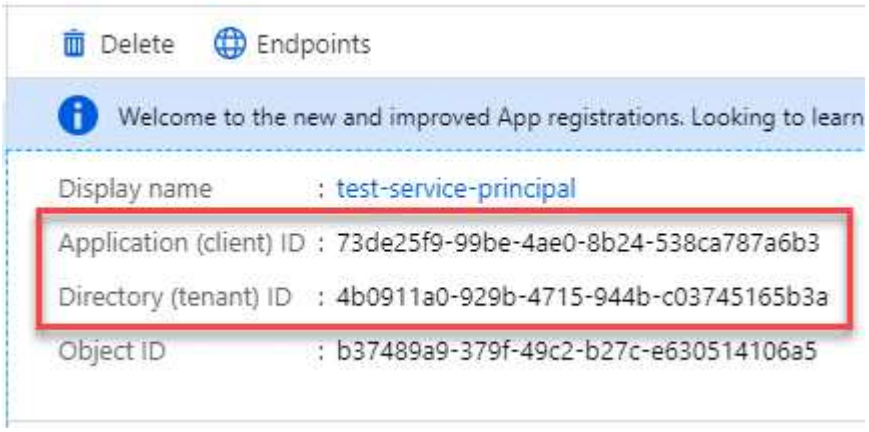


Obtention de l'ID d'application et de l'ID de répertoire

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

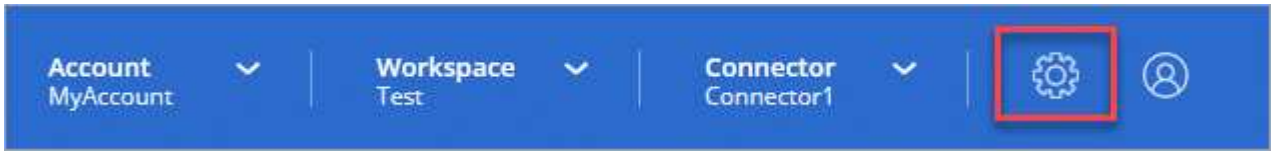
Une fois que vous avez autorisé à fournir un compte Azure, vous pouvez ajouter les identifiants de ce compte à Cloud Manager. Vous pouvez ainsi lancer les systèmes Cloud Volumes ONTAP de ce compte.

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**.



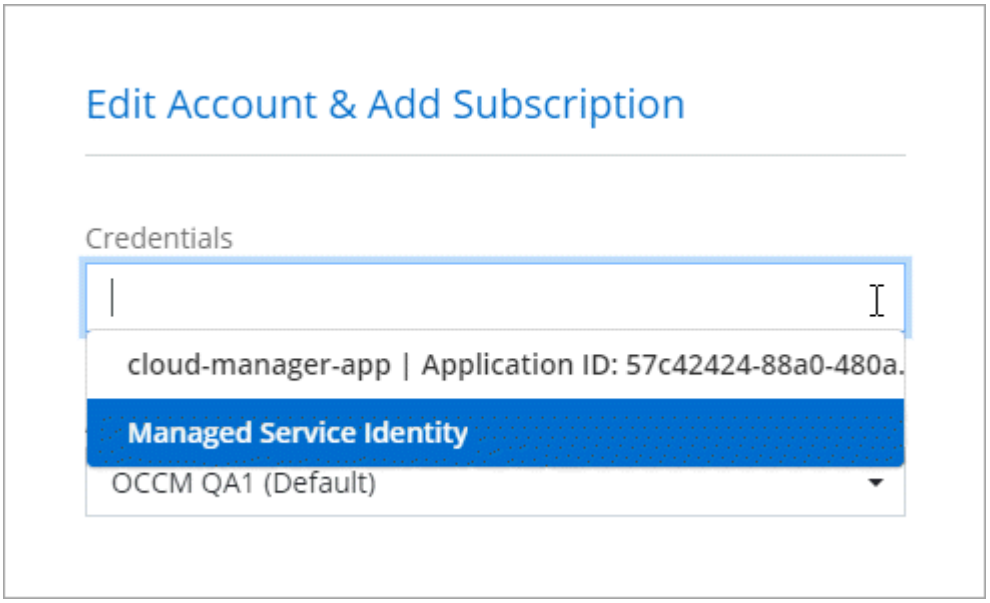
2. Cliquez sur **Ajouter des informations d'identification** et sélectionnez **Microsoft Azure**.
3. Entrez des informations sur l'entité de sécurité du service Azure Active Directory qui accorde les autorisations requises :
   - ID de l'application (client) : voir Obtention de l'ID d'application et 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 :

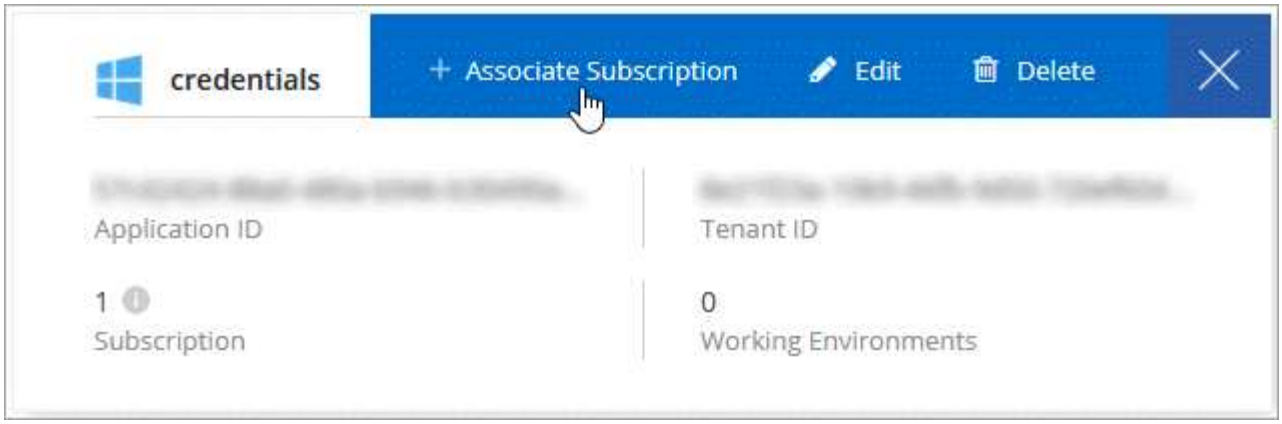
- Vous n'avez pas associé un abonnement lors de l'ajout initial des identifiants à Cloud Manager.
- Vous souhaitez remplacer un abonnement Azure Marketplace existant par un nouvel abonnement.

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

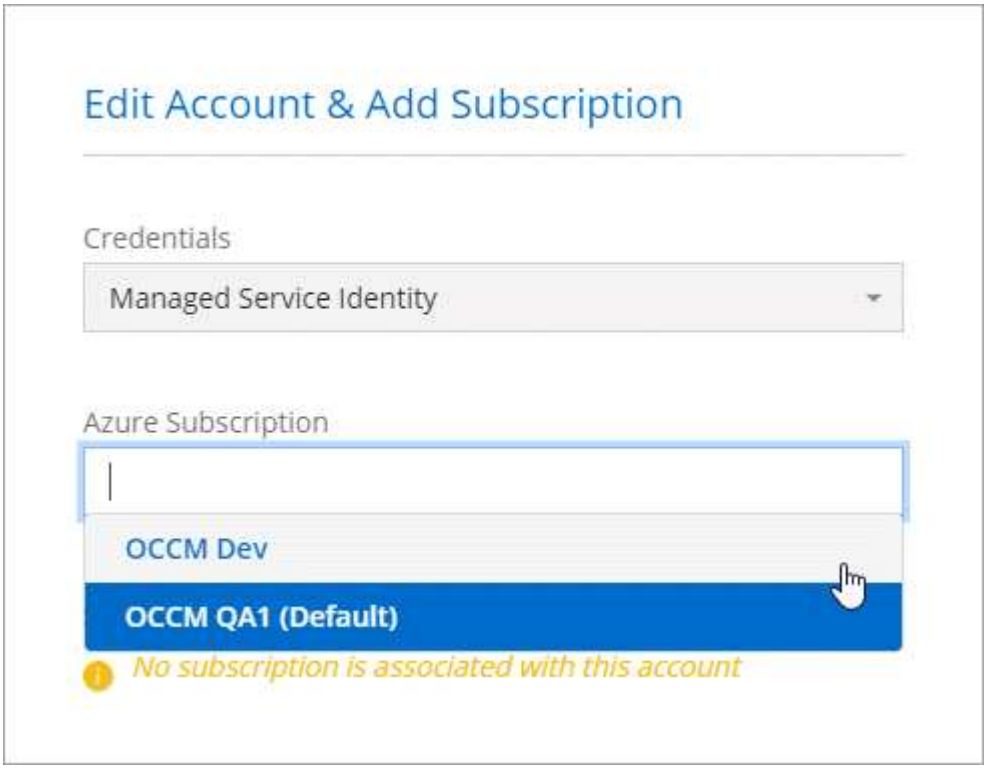
1. Connectez-vous au portail Azure.
2. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer Cloud Volumes ONTAP.
3. Cliquez sur **contrôle d'accès (IAM)**.
   a. Cliquez sur **Ajouter** > **Ajouter une affectation de rôle**, puis ajoutez les autorisations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



Informations sur le copyright

Informations sur les marques commerciales