Azuré

NetApp Console setup and administration

NetApp
January 27, 2026

Sommaire

Azuré

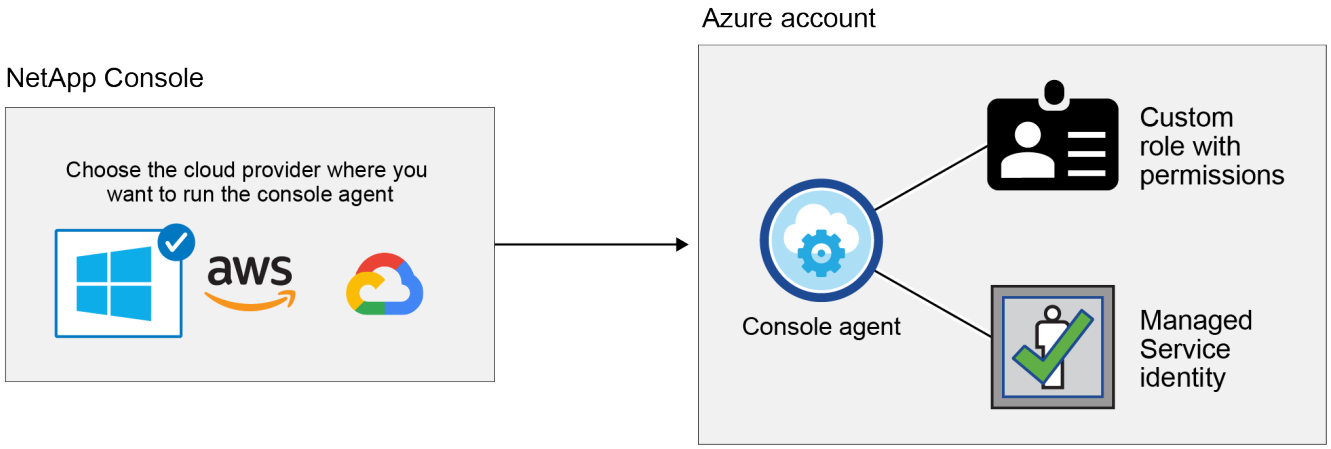
En savoir plus sur les informations d'identification et les autorisations Azure dans la NetApp Console

Découvrez comment la NetApp Console utilise les informations d'identification Azure pour effectuer des actions en votre nom et comment ces informations d'identification sont associées aux abonnements de la place de marché. Comprendre ces détails peut être utile lorsque vous gérez les informations d'identification d'un ou plusieurs abonnements Azure. Par exemple, vous souhaiterez peut-être savoir quand ajouter des informations d'identification Azure supplémentaires à la console.

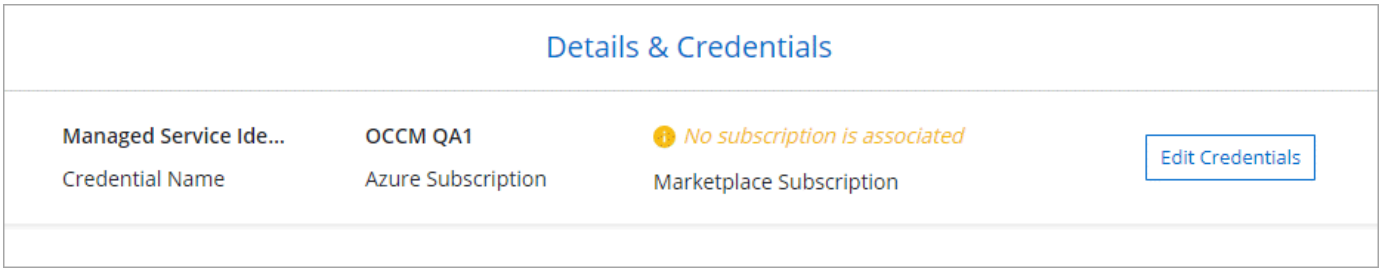
Informations d'identification Azure initiales

Lorsque vous déployez un agent de console à partir de la console, vous devez utiliser un compte Azure ou un principal de service disposant des autorisations nécessaires pour déployer la machine virtuelle de l'agent de console. Les autorisations requises sont répertoriées dans le"Politique de déploiement d'agent pour Azure" .

Lorsque la console déploie la machine virtuelle de l'agent de console dans Azure, elle active un "identité gérée attribuée par le système" sur la machine virtuelle, crée un rôle personnalisé et l'attribue à la machine virtuelle. Le rôle fournit à la console les autorisations requises pour gérer les ressources et les processus au sein de cet abonnement Azure. "Examiner comment la console utilise les autorisations" .



Si vous créez un nouveau système pour Cloud Volumes ONTAP, la console sélectionne ces informations d'identification Azure par défaut :



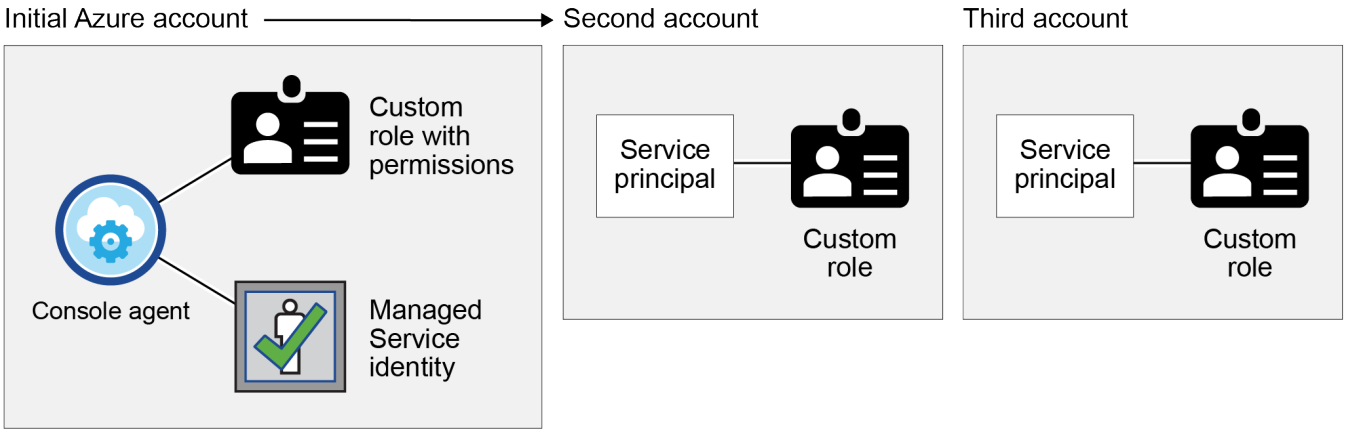
Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des informations d'identification Azure initiales ou ajouter des informations d'identification supplémentaires.

Abonnements Azure supplémentaires pour une identité gérée

L'identité gérée attribuée par le système à la machine virtuelle de l'agent de console est associée à l'abonnement dans lequel vous avez lancé l'agent de console. Si vous souhaitez sélectionner un autre abonnement Azure, vous devez"associer l'identité gérée à ces abonnements" .

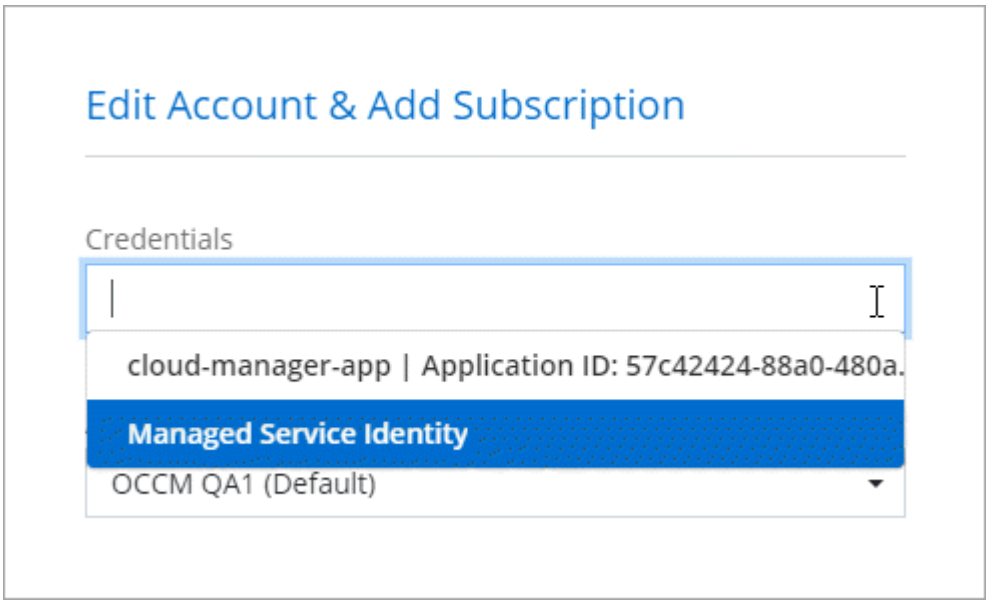
Informations d'identification Azure supplémentaires

Si vous souhaitez utiliser différentes informations d'identification Azure avec la console, vous devez accorder les autorisations requises en"création et configuration d'un principal de service dans Microsoft Entra ID" pour chaque compte Azure. L'image suivante montre deux comptes supplémentaires, chacun configuré avec un principal de service et un rôle personnalisé qui fournit des autorisations :



Vous voudriez alors"ajouter les informations d'identification du compte à la console" en fournissant des détails sur le principal du service AD.

Par exemple, vous pouvez basculer entre les informations d'identification lors de la création d'un nouveau système Cloud Volumes ONTAP :



Informations d’identification et abonnements à la place de marché

Les informations d’identification que vous ajoutez à un agent de console doivent être associées à un abonnement Azure Marketplace afin que vous puissiez payer Cloud Volumes ONTAP à un tarif horaire (PAYGO) ou des services de données NetApp ou via un contrat annuel.

"Découvrez comment associer un abonnement Azure" .

Notez les points suivants concernant les informations d’identification Azure et les abonnements à la place de marché :

- Vous ne pouvez associer qu’un seul abonnement Azure Marketplace à un ensemble d’informations d’identification Azure
- Vous pouvez remplacer un abonnement de marché existant par un nouvel abonnement

FAQ

La question suivante concerne les informations d’identification et les abonnements.

Puis-je modifier l’abonnement Azure Marketplace pour les systèmes Cloud Volumes ONTAP ?

Oui, tu peux. Lorsque vous modifiez l’abonnement Azure Marketplace associé à un ensemble d’informations d’identification Azure, tous les systèmes Cloud Volumes ONTAP existants et nouveaux seront facturés sur le nouvel abonnement.

"Découvrez comment associer un abonnement Azure" .

Puis-je ajouter plusieurs informations d’identification Azure, chacune avec des abonnements de marketplace différents ?

Toutes les informations d’identification Azure appartenant au même abonnement Azure seront associées au même abonnement Azure Marketplace.

Si vous disposez de plusieurs informations d’identification Azure appartenant à différents abonnements Azure, ces informations d’identification peuvent être associées au même abonnement Azure Marketplace ou à différents abonnements Marketplace.

Puis-je déplacer des systèmes Cloud Volumes ONTAP existants vers un autre abonnement Azure ?

Non, il n’est pas possible de déplacer les ressources Azure associées à votre système Cloud Volumes ONTAP vers un autre abonnement Azure.

Comment fonctionnent les informations d’identification pour les déploiements sur le marché et les déploiements sur site ?

Les sections ci-dessus décrivent la méthode de déploiement recommandée pour l’agent de console, qui provient de la console. Vous pouvez également déployer un agent de console dans Azure à partir de la Place de marché Azure et installer le logiciel de l’agent de console sur votre propre hôte Linux.

Si vous utilisez la Place de marché, vous pouvez fournir des autorisations en attribuant un rôle personnalisé à la machine virtuelle de l’agent de console et à une identité gérée attribuée par le système, ou vous pouvez utiliser un principal de service Microsoft Entra.

Pour les déploiements sur site, vous ne pouvez pas configurer une identité gérée pour l’agent de console,

mais vous pouvez fournir des autorisations à l'aide d'un principal de service.

Pour savoir comment configurer les autorisations, reportez-vous aux pages suivantes :

- Mode standard
  - "Configurer les autorisations pour un déploiement Azure Marketplace"
  - "Configurer les autorisations pour les déploiements sur site"
- Mode restreint
  - "Configurer les autorisations pour le mode restreint"

Gérer les informations d'identification Azure et les abonnements à la place de marché pour la NetApp Console

Ajoutez et gérez les informations d'identification Azure afin que la NetApp Console dispose des autorisations nécessaires pour déployer et gérer les ressources cloud dans vos abonnements Azure. Si vous gérez plusieurs abonnements Azure Marketplace, vous pouvez attribuer chacun d'eux à différentes informations d'identification Azure à partir de la page Informations d'identification.

Aperçu

Il existe deux manières d'ajouter des abonnements et des informations d'identification Azure supplémentaires dans la console.

1. Associez des abonnements Azure supplémentaires à l'identité gérée Azure.
2. Pour déployer Cloud Volumes ONTAP à l'aide de différentes informations d'identification Azure, accordez des autorisations Azure à l'aide d'un principal de service et ajoutez ses informations d'identification à la console.

Associer des abonnements Azure supplémentaires à une identité gérée

La console vous permet de choisir les informations d'identification 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 managée, sauf si vous l'associez "identité gérée" avec ces abonnements.

À propos de cette tâche

Une identité gérée est"le compte Azure initial" lorsque vous déployez un agent de console à partir de la console. Lorsque vous déployez l'agent de console, la console attribue le rôle d'opérateur de console à la machine virtuelle de l'agent de console.

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. Sélectionnez **Contrôle d'accès (IAM)**.
   a. Sélectionnez **Ajouter** > **Ajouter une attribution de rôle**, puis ajoutez les autorisations :
      - Sélectionnez le rôle **Opérateur de console**.

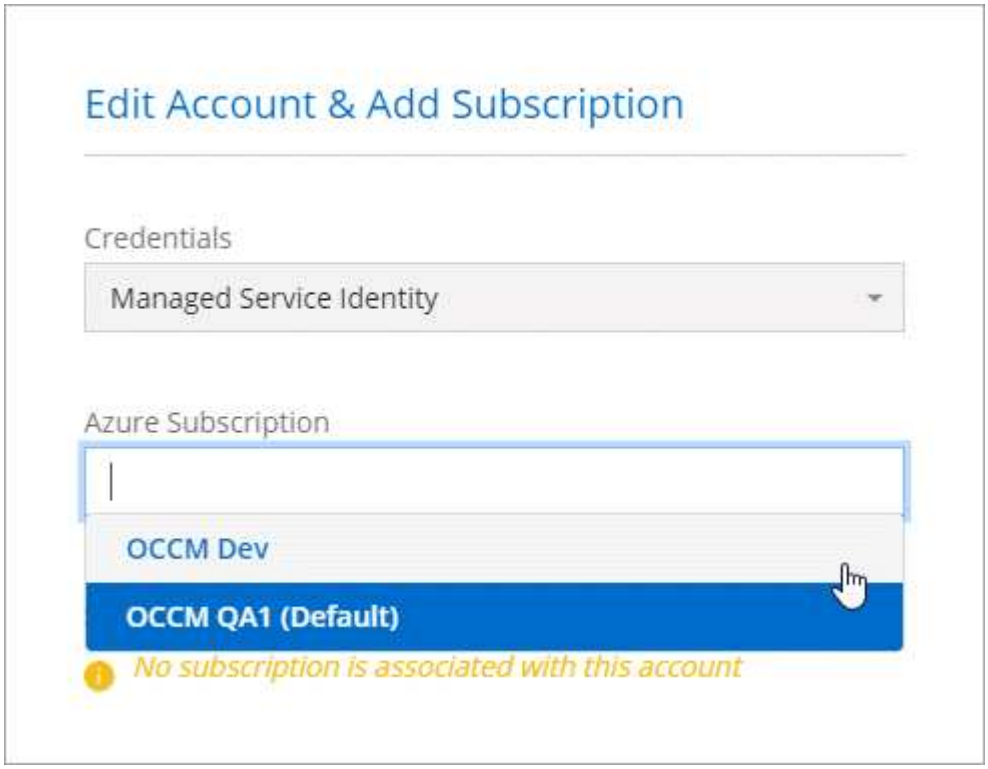
L'opérateur de console est le nom par défaut fourni dans une stratégie d'agent de console. Si vous avez choisi un nom différent pour le rôle, sélectionnez plutôt ce nom.

- Attribuer l'accès à une **machine virtuelle**.
- Sélectionnez l'abonnement dans lequel une machine virtuelle d'agent de console a été créée.
- Sélectionnez une machine virtuelle d'agent de console.
- Sélectionnez **Enregistrer**.

4. Répétez ces étapes pour des abonnements supplémentaires.

Résultat

Lors de la création d'un nouveau système, vous pouvez désormais choisir parmi plusieurs abonnements Azure pour le profil d'identité géré.



Ajouter des informations d'identification Azure supplémentaires à la NetApp Console

Lorsque vous déployez un agent de console à partir de la console, la console active une identité gérée attribuée par le système sur la machine virtuelle qui dispose des autorisations requises. La console sélectionne ces informations d'identification Azure par défaut lorsque vous créez un nouveau système pour Cloud Volumes ONTAP.

Un ensemble initial d'informations d'identification n'est pas ajouté si vous avez installé manuellement un logiciel d'agent de console sur un système existant. "En savoir plus sur les informations d'identification et les autorisations Azure" .

Si vous souhaitez déployer Cloud Volumes ONTAP à l'aide de *différentes* informations d'identification Azure, vous devez accorder les autorisations requises en créant et en configurant un principal de service dans

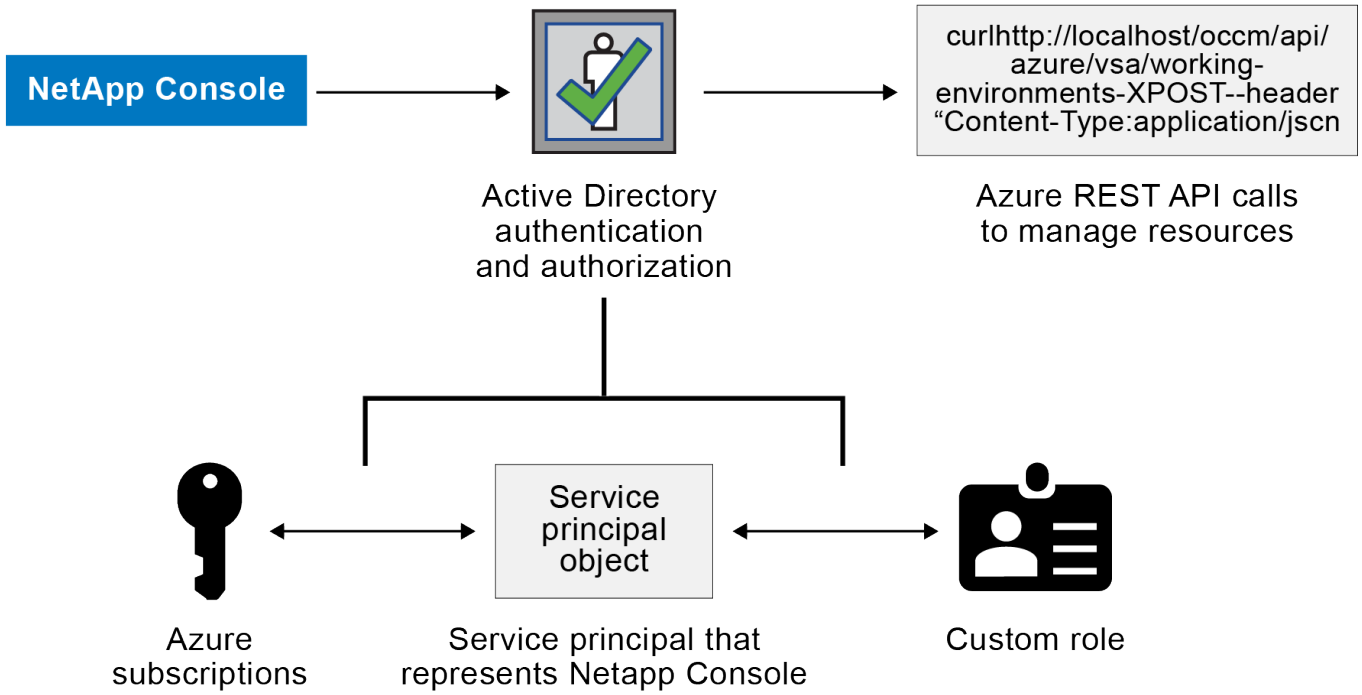
Microsoft Entra ID pour chaque compte Azure. Vous pouvez ensuite ajouter les nouvelles informations d'identification à la console.

Accorder des autorisations Azure à l'aide d'un principal de service

La console 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 un principal de service dans Microsoft Entra ID et en obtenant les informations d'identification Azure dont la console a besoin.

À propos de cette tâche

L'image suivante illustre comment la console obtient les autorisations pour effectuer des opérations dans Azure. Un objet principal de service, lié à un ou plusieurs abonnements Azure, représente la console dans Microsoft Entra ID et est attribué à un rôle personnalisé qui autorise les autorisations requises.



Étapes

1. Créer une application Microsoft Entra .
2. Affecter l'application à un rôle .
3. Ajouter des autorisations à l'API Windows Azure Service Management .
4. Obtenir l'ID de l'application et l'ID du répertoire .
5. Créer un secret client .

Créer une application Microsoft Entra

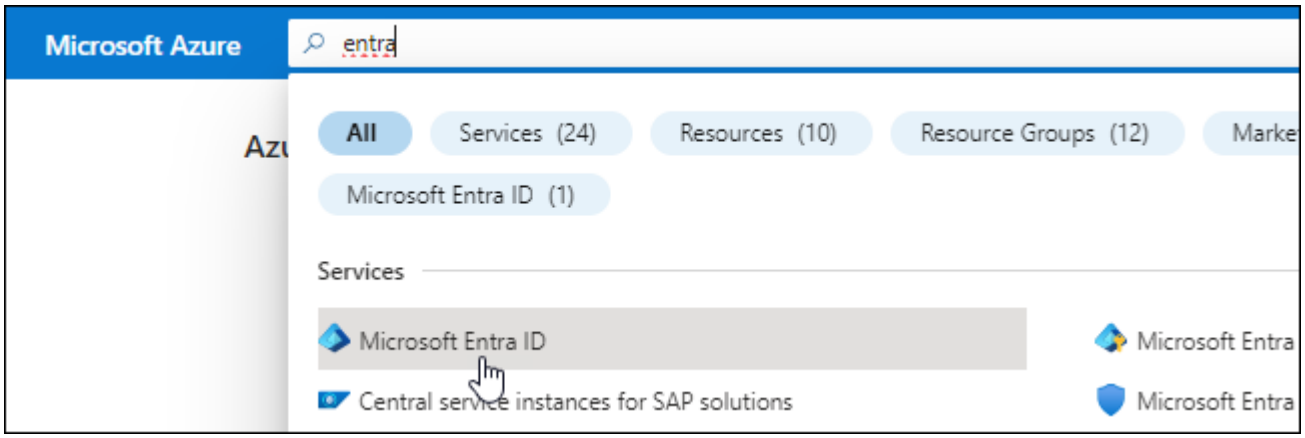
Créez une application Microsoft Entra et un principal de service que la console peut utiliser pour le contrôle d'accès basé sur les rôles.

Étapes

1. Assurez-vous que vous disposez des autorisations 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"

2. Depuis le portail Azure, ouvrez le service **Microsoft Entra ID**.



3. Dans le menu, sélectionnez **Inscriptions d'applications**.
4. Sélectionnez **Nouvelle inscription**.
5. Précisez les détails de l'application :
   - **Nom**: Saisissez un nom pour l'application.
   - **Type de compte** : sélectionnez un type de compte (n'importe lequel fonctionnera avec la NetApp Console).
   - **URI de redirection**: Vous pouvez laisser ce champ vide.
6. Sélectionnez **S'inscrire**.

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

Affecter l'application à un rôle

Vous devez lier le principal du service à un ou plusieurs abonnements Azure et lui attribuer le rôle personnalisé « Opérateur de console » afin que la console dispose d'autorisations dans Azure.

Étapes

1. Créer un rôle personnalisé :

   Notez que vous pouvez créer un rôle personnalisé Azure à l'aide du portail Azure, d'Azure PowerShell, d'Azure CLI ou de l'API REST. Les étapes suivantes montrent comment créer le rôle à l'aide de l'interface de ligne de commande Azure. Si vous préférez utiliser une méthode différente, reportez-vous à "Documentation Azure"

   a. Copiez le contenu du"autorisations de rôle personnalisées pour l'agent de la console" et les enregistrer dans un fichier JSON.

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

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

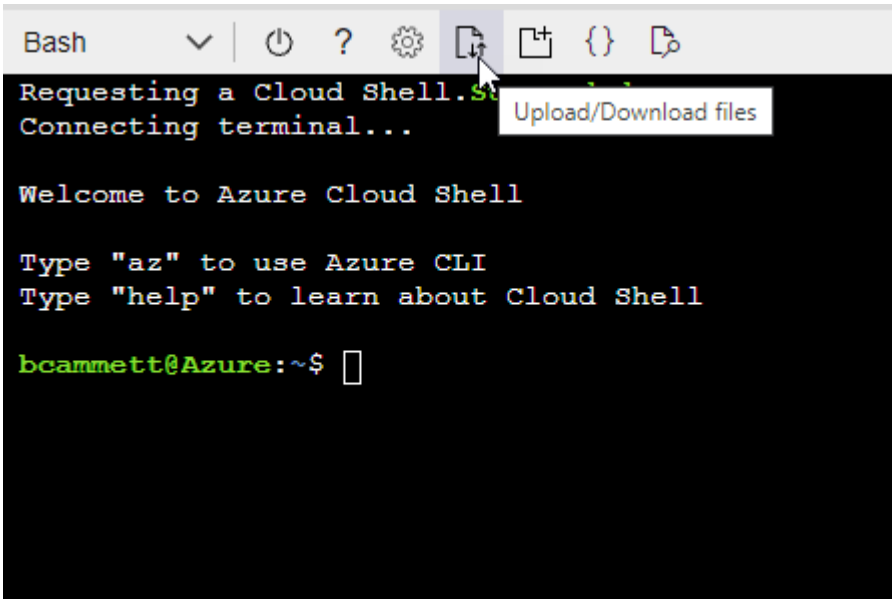
      Exemple

```
"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.

Les étapes suivantes décrivent comment créer le rôle à l'aide de Bash dans Azure Cloud Shell.

- Commencer "Azure Cloud Shell" et choisissez l'environnement Bash.
- Téléchargez le fichier JSON.



- Utilisez l'interface de ligne de commande Azure pour créer le rôle personnalisé :

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

Vous devriez maintenant avoir un rôle personnalisé appelé Opérateur de console que vous pouvez attribuer à la machine virtuelle de l'agent de console.

2. Affecter l'application au rôle :

a. Depuis le portail Azure, ouvrez le service **Abonnements**.

b. Sélectionnez l'abonnement.

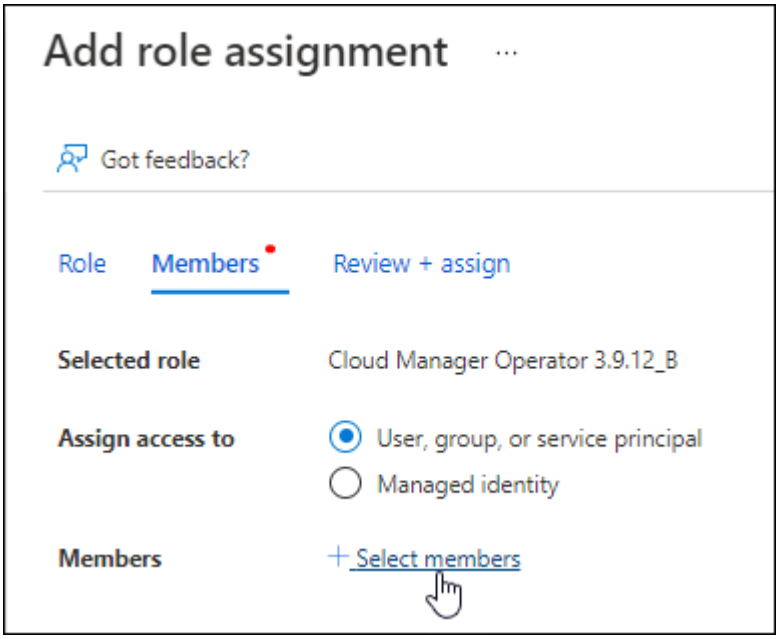
c. Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.

d. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.

e. Dans l'onglet **Membres**, procédez comme suit :

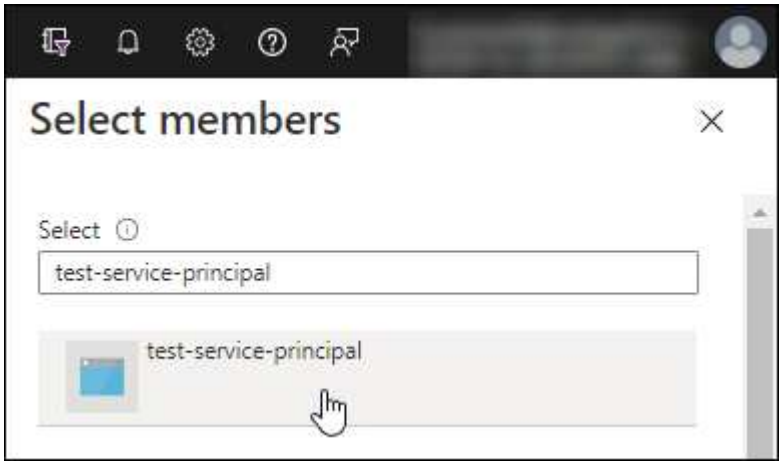
- Gardez **Utilisateur, groupe ou principal du service** sélectionné.

- Sélectionnez **Sélectionner les membres**.



- Recherchez le nom de l'application.

  Voici un exemple :



- Sélectionnez l'application et sélectionnez **Sélectionner**.
- Sélectionnez **Suivant**.

f. Sélectionnez **Réviser + attribuer**.

   Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

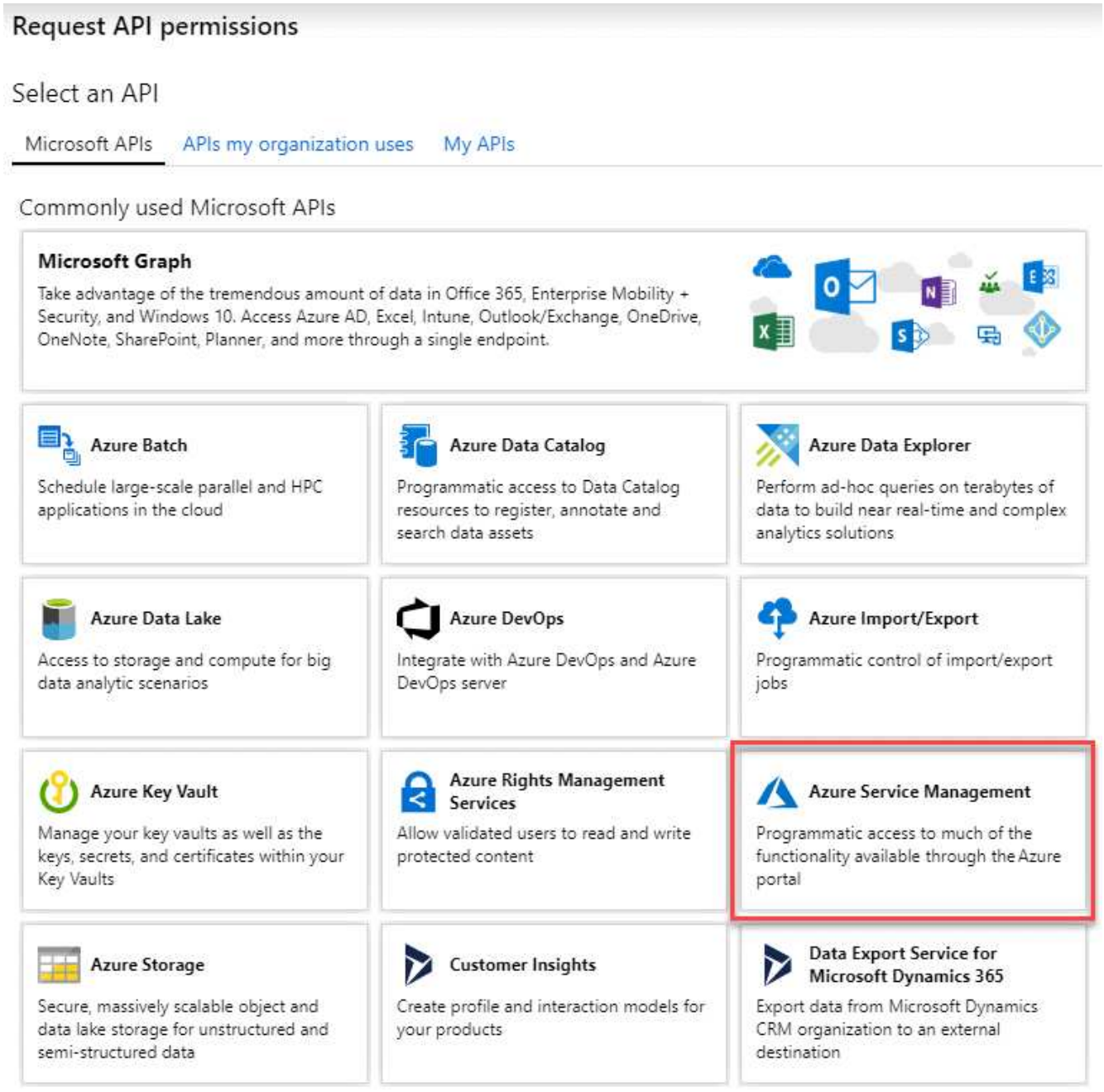
Si vous souhaitez déployer Cloud Volumes ONTAP à partir de plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. Dans la NetApp Console, vous pouvez sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

Ajouter des autorisations à l'API Windows Azure Service Management

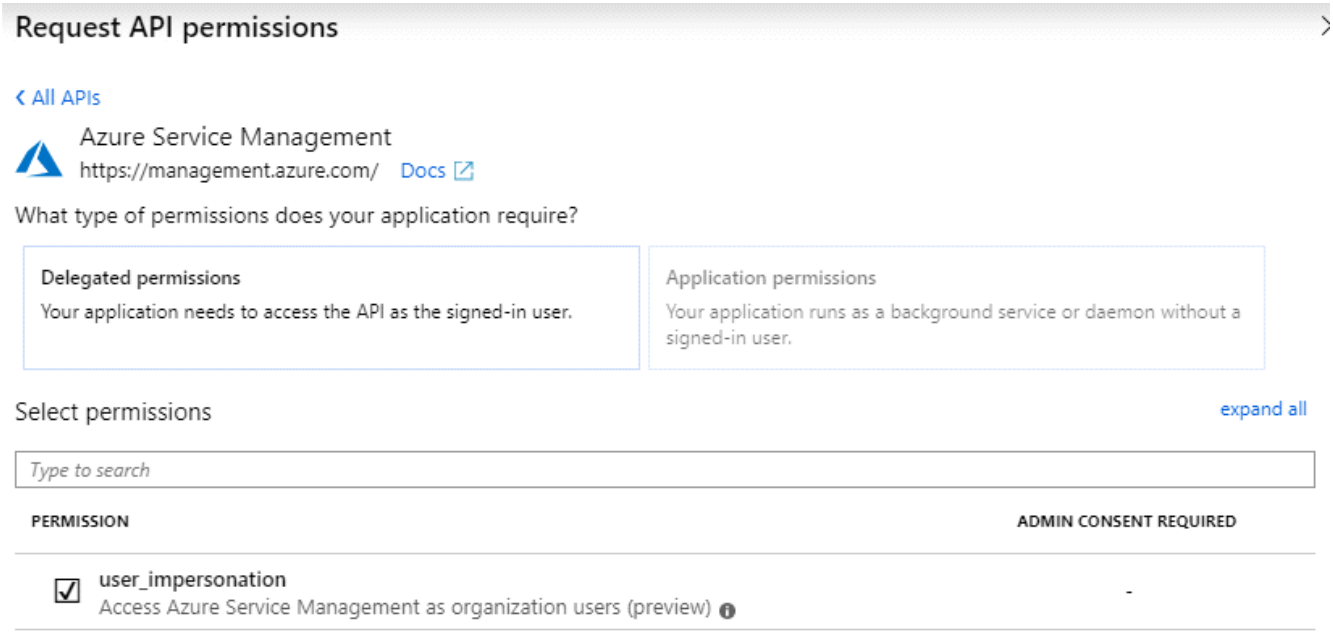
Vous devez attribuer les autorisations « API de gestion des services Windows Azure » au principal du service.

Étapes

1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Sélectionnez **Autorisations API > Ajouter une autorisation**.
3. Sous **API Microsoft**, sélectionnez **Azure Service Management**.



4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.

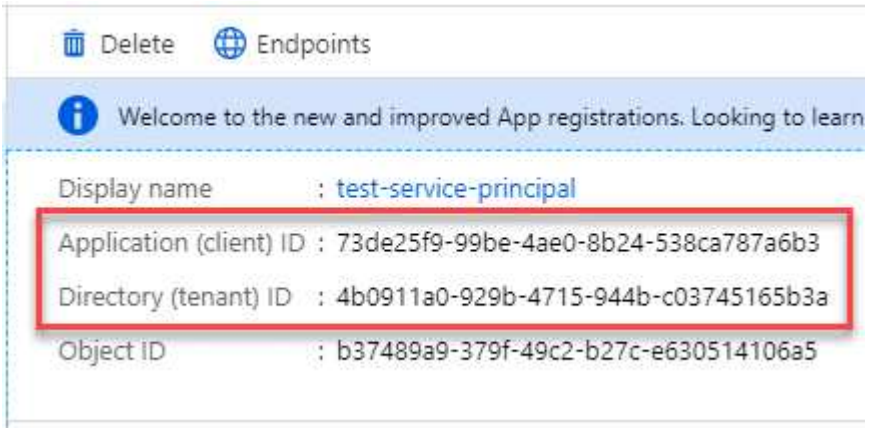


Obtenir l'ID de l'application et l'ID du répertoire

Lorsque vous ajoutez le compte Azure à la console, vous devez fournir l'ID d'application (client) et l'ID de répertoire (locataire) de l'application. La console utilise les identifiants pour se connecter par programmation.

Étapes

1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



Lorsque vous ajoutez le compte Azure à la console, vous devez fournir l'ID d'application (client) et l'ID de répertoire (locataire) de l'application. La console utilise les identifiants pour se connecter par programmation.

Créer un secret client

Créez un secret client et fournissez sa valeur à la console pour l'authentification avec Microsoft Entra ID.

Étapes

1. Ouvrez le service **Microsoft Entra ID**.
2. Sélectionnez **Inscriptions d'applications** et sélectionnez votre application.
3. Sélectionnez **Certificats et secrets > Nouveau secret client**.
4. Fournissez une description du secret et une durée.
5. Sélectionnez **Ajouter**.
6. Copiez 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 (locataire) et la valeur du secret client. Vous devez saisir ces informations dans la console lorsque vous ajoutez un compte Azure.

Ajoutez les informations d'identification à la console

Après avoir fourni à un compte Azure les autorisations requises, vous pouvez ajouter les informations d'identification de ce compte à la console. Cette étape vous permet de lancer Cloud Volumes ONTAP à l'aide de différentes informations d'identification Azure.

Avant de commencer

Si vous venez de créer ces informations d'identification auprès de votre fournisseur de cloud, il faudra peut-être quelques minutes avant qu'elles soient disponibles pour utilisation. Attendez quelques minutes avant d'ajouter les informations d'identification à la console.

Avant de commencer

Vous devez créer un agent de console avant de pouvoir modifier les paramètres de la console. "Apprenez à créer un agent de console" .

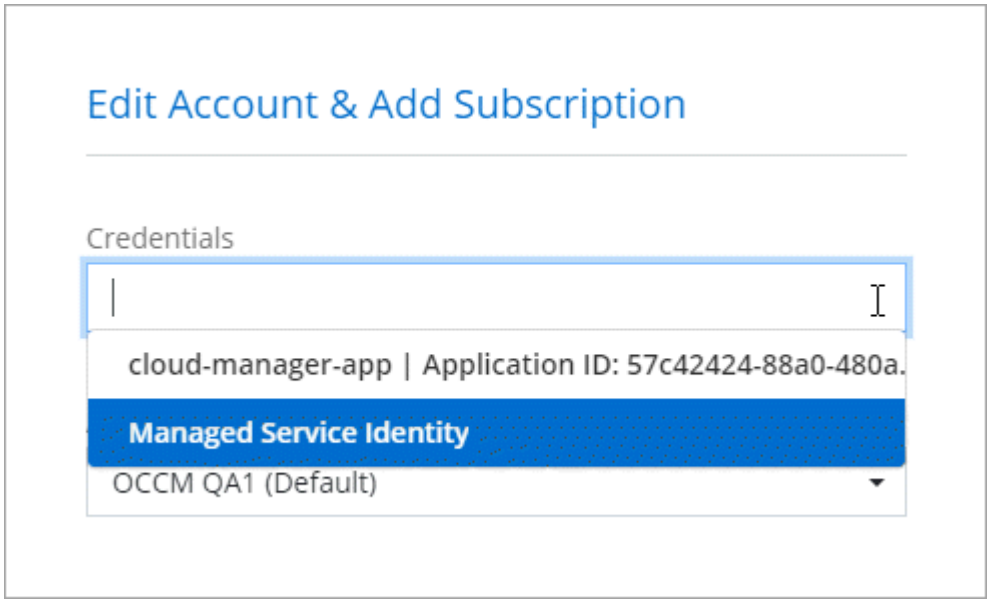
Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
   a. **Emplacement des informations d'identification** : sélectionnez **Microsoft Azure > Agent**.
   b. **Définir les informations d'identification** : saisissez les informations sur le principal du service Microsoft Entra qui accorde les autorisations requises :
      - ID de l'application (client)
      - ID du répertoire (locataire)
      - Secret client
   c. **Abonnement Marketplace** : Associez un abonnement Marketplace à ces informations d'identification en vous abonnant maintenant ou en sélectionnant un abonnement existant.

d. **Révision** : Confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Résultat

Vous pouvez passer à un autre ensemble d'informations d'identification à partir de la page Détails et informations d'identification. "lors de l'ajout d'un système à la console"



Gérer les informations d'identification existantes

Gérez les informations d'identification Azure que vous avez déjà ajoutées à la console en associant un abonnement Marketplace, en modifiant les informations d'identification et en les supprimant.

Associer un abonnement Azure Marketplace aux informations d'identification

Après avoir ajouté vos informations d'identification Azure à la console, vous pouvez associer un abonnement Azure Marketplace à ces informations d'identification. Vous pouvez utiliser l'abonnement pour créer un système Cloud Volumes ONTAP à la carte et accéder aux services de données NetApp .

Il existe deux scénarios dans lesquels vous pouvez associer un abonnement Azure Marketplace après avoir ajouté les informations d'identification à la console :

- Vous n'avez pas associé d'abonnement lorsque vous avez initialement ajouté les informations d'identification à la console.
- Vous souhaitez modifier l'abonnement Azure Marketplace associé aux informations d'identification Azure.

  Le remplacement de l'abonnement actuel au marché le met à jour pour les systèmes Cloud Volumes ONTAP existants et nouveaux.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'organisation**.
3. Sélectionnez le menu d'action pour un ensemble d'informations d'identification associées à un agent de console, puis sélectionnez **Configurer l'abonnement**.

   Vous devez sélectionner les informations d'identification associées à un agent de console. Vous ne pouvez

pas associer un abonnement au marché aux informations d'identification associées à la NetApp Console.

4. Pour associer les informations d'identification à un abonnement existant, sélectionnez l'abonnement dans la liste déroulante et sélectionnez **Configurer**.
5. Pour associer les informations d'identification à un nouvel abonnement, sélectionnez **Ajouter un abonnement > Continuer** et suivez les étapes dans la Place de marché Azure :

   a. Si vous y êtes invité, connectez-vous à votre compte Azure.

   b. Sélectionnez **S'abonner**.

   c. Remplissez le formulaire et sélectionnez **S'abonner**.

   d. Une fois le processus d'abonnement terminé, sélectionnez **Configurer le compte maintenant**.

      Vous serez redirigé vers la NetApp Console.

   e. À partir de la page **Affectation d'abonnement** :

      - Sélectionnez les organisations ou les comptes de la console auxquels vous souhaitez associer cet abonnement.
      - Dans le champ **Remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant pour une organisation ou un compte par ce nouvel abonnement.

        La console remplace l'abonnement existant pour toutes les informations d'identification de l'organisation ou du compte par ce nouvel abonnement. Si un ensemble d'informations d'identification n'a jamais été associé à un abonnement, ce nouvel abonnement ne sera pas associé à ces informations d'identification.

   Pour toutes les autres organisations ou comptes, vous devrez associer manuellement l'abonnement en répétant ces étapes.

   ◦ Sélectionnez **Enregistrer**.

Modifier les informations d'identification

Modifiez vos informations d'identification Azure dans la console. Par exemple, vous pouvez mettre à jour le secret client si un nouveau secret a été créé pour l'application principale de service.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'organisation**.
3. Sélectionnez le menu d'action pour un ensemble d'informations d'identification, puis sélectionnez **Modifier les informations d'identification**.
4. Apportez les modifications requises, puis sélectionnez **Appliquer**.

Supprimer les informations d'identification

Si vous n'avez plus besoin d'un ensemble d'informations d'identification, vous pouvez les supprimer. Vous ne pouvez supprimer que les informations d'identification qui ne sont pas associées à un système.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.

2. Sélectionnez **Informations d’identification de l’organisation**.
3. Sur la page **Informations d’identification de l’organisation**, sélectionnez le menu d’action pour un ensemble d’informations d’identification, puis sélectionnez **Supprimer les informations d’identification**.
4. Sélectionnez **Supprimer** pour confirmer.

Informations sur le copyright

Informations sur les marques commerciales