Azure

Setup and administration

NetApp
April 26, 2024

Sommaire

Azure

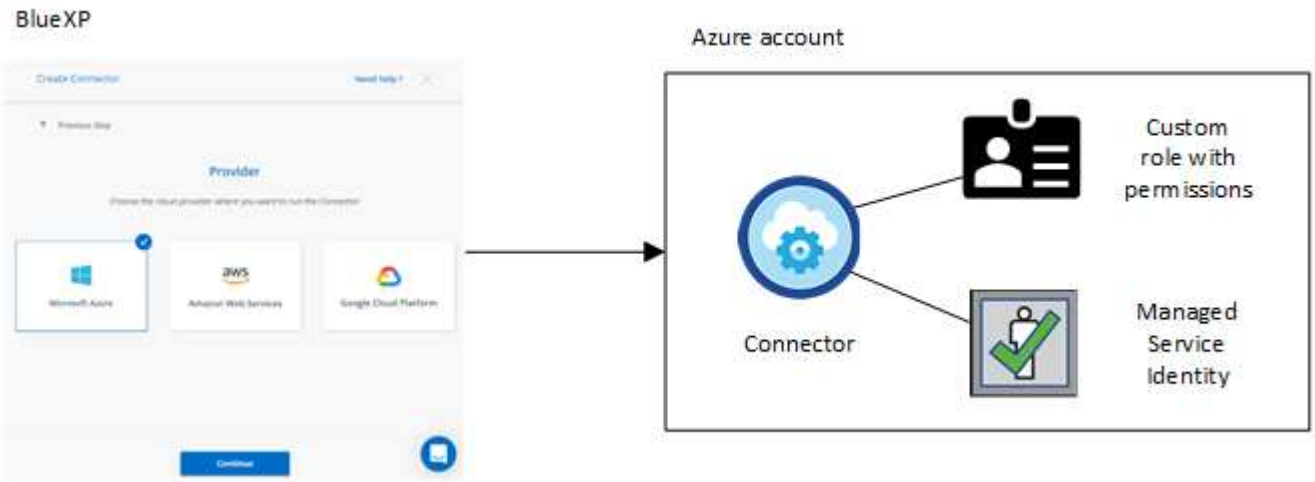
En savoir plus sur les identifiants et les autorisations Azure

Découvrez comment BlueXP utilise les identifiants Azure pour effectuer des actions en votre nom et comment ces identifiants sont associés aux abonnements Marketplace. Ces informations peuvent vous être utiles lorsque vous gérez les identifiants d'un ou plusieurs abonnements Azure. Par exemple, vous pouvez savoir quand ajouter des informations d'identification Azure supplémentaires à BlueXP.

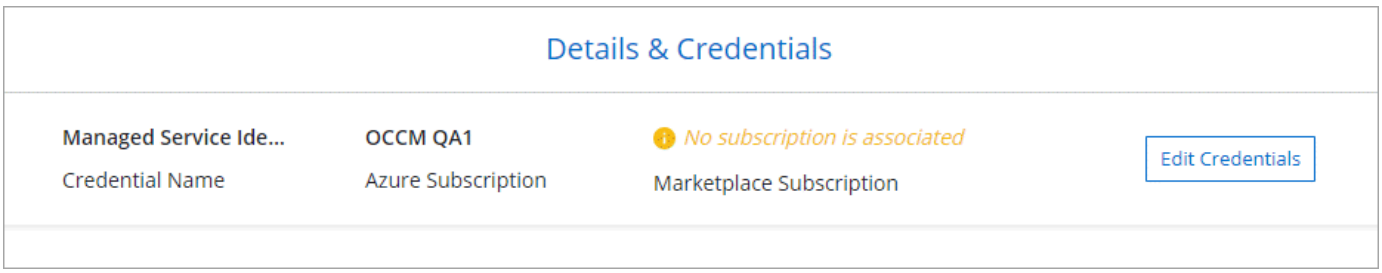
Les identifiants initiaux d'Azure

Lorsque vous déployez un connecteur depuis BlueXP, vous devez utiliser un compte ou un service principal Azure disposant des autorisations pour déployer la machine virtuelle Connector. Les autorisations requises sont répertoriées dans le "Stratégie de déploiement de Connector pour Azure".

Lorsque BlueXP déploie la machine virtuelle Connector dans Azure, il active un "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 BlueXP les autorisations requises pour gérer les ressources et les processus au sein de cet abonnement Azure. "Consultez la manière dont BlueXP utilise les autorisations".



Si vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP, BlueXP sélectionne les informations d'identification Azure suivantes par défaut :



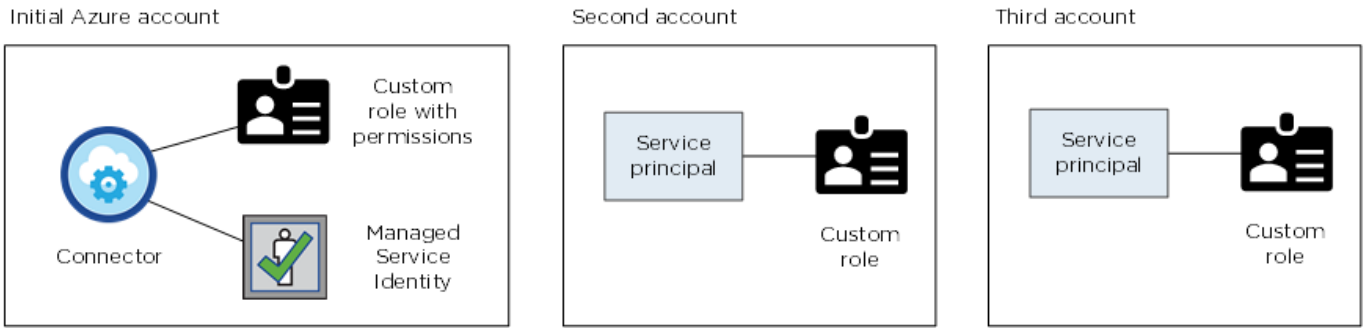
Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des identifiants Azure initiaux, ou ajouter des identifiants supplémentaires.

Des abonnements Azure supplémentaires pour une identité gérée

L'identité gérée attribuée par le système à la VM Connector 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".

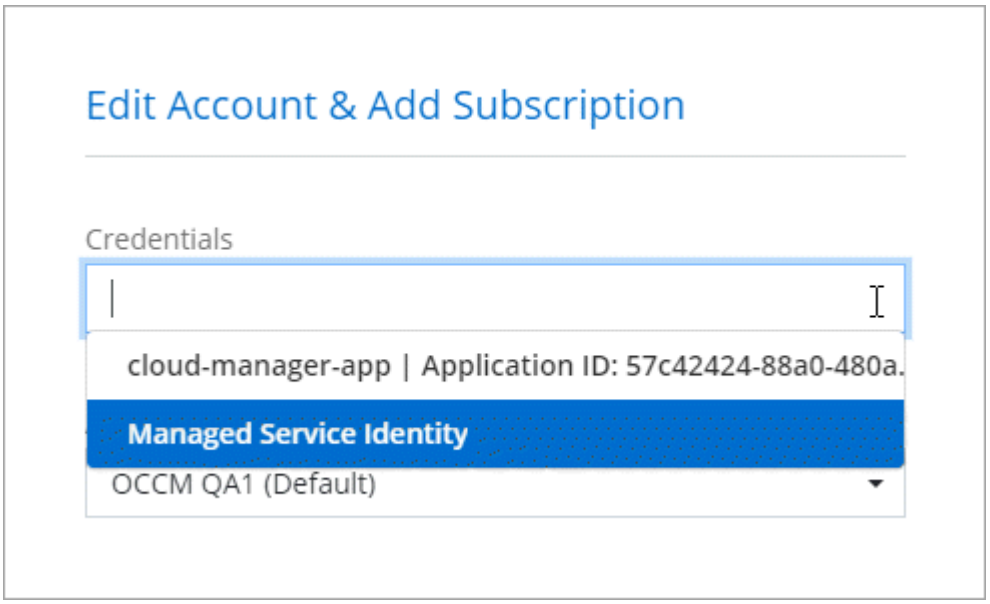
Autres identifiants Azure

Si vous souhaitez utiliser d'autres identifiants Azure avec BlueXP, vous devez accorder les autorisations requises par "Création et configuration d'une entité de service dans Microsoft Entra ID" 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 informations d'identification du compte à BlueXP" 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 nouvel environnement de travail Cloud Volumes ONTAP :



Informations d'identification et abonnements Marketplace

Les identifiants que vous ajoutez à un connecteur doivent être associés à un abonnement Azure Marketplace de sorte que vous puissiez payer Cloud Volumes ONTAP à un taux horaire (PAYGO) ou un contrat annuel, et utiliser d'autres services BlueXP.

"Découvrez comment associer un abonnement Azure".

Notez ce qui suit à propos des identifiants Azure et des abonnements Marketplace :

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

FAQ

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

Est-il possible de modifier l'abonnement Azure Marketplace pour les environnements de travail Cloud Volumes ONTAP ?

Oui, c'est possible. Lorsque vous modifiez l'abonnement Azure Marketplace associé à un ensemble d'identifiants Azure, tous les environnements de travail Cloud Volumes ONTAP existants et nouveaux sont facturés pour le nouvel abonnement.

"Découvrez comment associer un abonnement Azure".

Puis-je ajouter plusieurs identifiants Azure, chacun avec des abonnements Marketplace différents ?

Tous les identifiants Azure qui appartiennent au même abonnement Azure seront associés au même abonnement Azure Marketplace.

Si plusieurs identifiants Azure appartiennent à différents abonnements Azure, ces identifiants peuvent être associés au même abonnement Azure Marketplace ou à d'autres abonnements Marketplace.

Est-il possible de déplacer des environnements de travail Cloud Volumes ONTAP existants vers un autre abonnement Azure ?

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

Comment fonctionnent les identifiants pour les déploiements sur site et sur le marché ?

Les sections ci-dessus décrivent la méthode de déploiement recommandée pour le connecteur, qui provient de BlueXP. Vous pouvez également déployer un connecteur dans Azure à partir d'Azure Marketplace et installer le logiciel Connector sur votre propre hôte Linux.

Si vous utilisez Marketplace, vous pouvez fournir des autorisations en attribuant un rôle personnalisé à la machine virtuelle Connector et à une identité gérée attribuée par le système, ou vous pouvez utiliser une entité de service Microsoft Entra.

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

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

- Mode standard
  - "Configurez les autorisations d'un déploiement Azure Marketplace"
  - "Configurez des autorisations pour les déploiements sur site"

- "Définissez les autorisations pour le mode restreint"
- "Configurez les autorisations pour le mode privé"

Gérez les identifiants Azure et les abonnements Marketplace pour BlueXP

Ajoutez et gérez des identifiants Azure pour que BlueXP dispose des autorisations dont il a besoin pour déployer et gérer des ressources cloud dans vos abonnements Azure. 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.

Suivez les étapes indiquées sur cette page si vous devez utiliser plusieurs identifiants Azure ou plusieurs abonnements Azure Marketplace pour Cloud Volumes ONTAP.

Présentation

Il existe deux façons d'ajouter des abonnements et des informations d'identification Azure supplémentaires dans BlueXP.

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

Associez des abonnements Azure supplémentaires à une identité gérée

BlueXP 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 BlueXP. Lorsque vous avez déployé le connecteur, BlueXP a créé le rôle opérateur BlueXP et l'a affecté à la machine virtuelle Connector.

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 affectation de rôle**, puis ajoutez les autorisations :
      - Sélectionnez le rôle **opérateur BlueXP**.

        BlueXP Operator est le nom par défaut fourni dans la stratégie de connecteur. Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

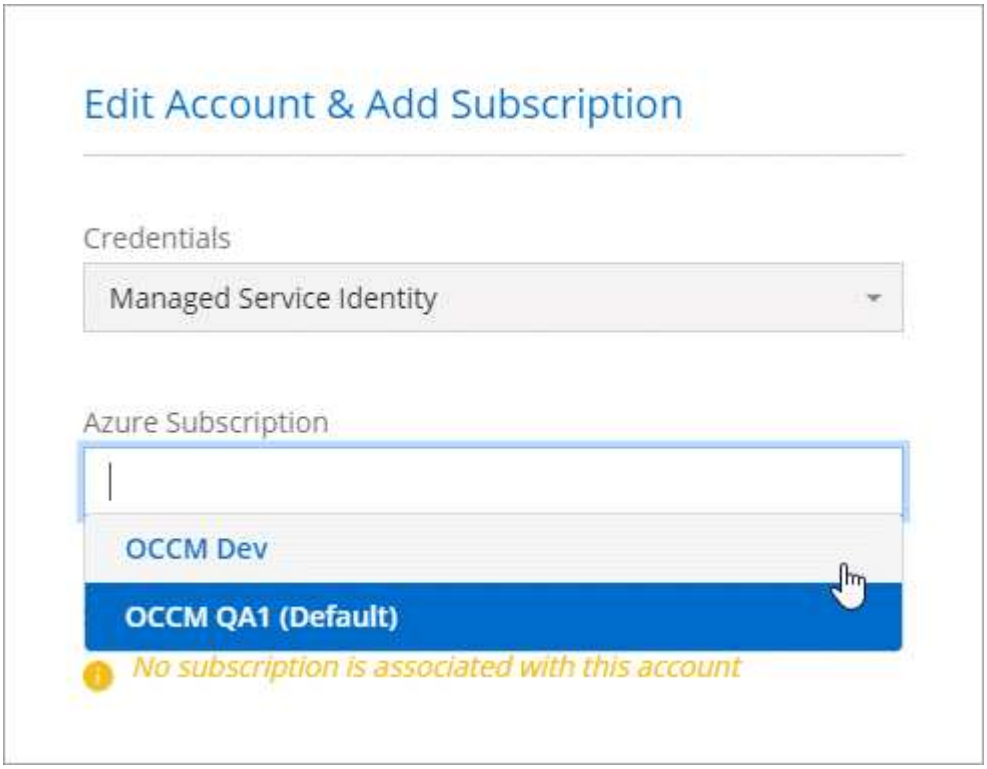
      - Attribuez l'accès à une **machine virtuelle**.

- Sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée.
- Sélectionnez la machine virtuelle Connector.
- Sélectionnez **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.



Ajoutez des identifiants Azure supplémentaires à BlueXP

Lorsque vous déployez un connecteur depuis BlueXP, BlueXP active une identité gérée attribuée par le système sur la machine virtuelle qui dispose des autorisations requises. BlueXP sélectionne ces informations d'identification Azure par défaut lorsque vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP.

> Un jeu initial d'informations d'identification n'est pas ajouté si vous avez installé manuellement le logiciel du connecteur sur un système existant. "En savoir plus sur les identifiants et les autorisations Azure".

Si vous souhaitez déployer Cloud Volumes ONTAP à l'aide des informations d'identification *différent* Azure, vous devez accorder les autorisations requises en créant et en configurant une entité de service dans Microsoft Entra ID pour chaque compte Azure. Vous pouvez ensuite ajouter les nouvelles informations d'identification à BlueXP.

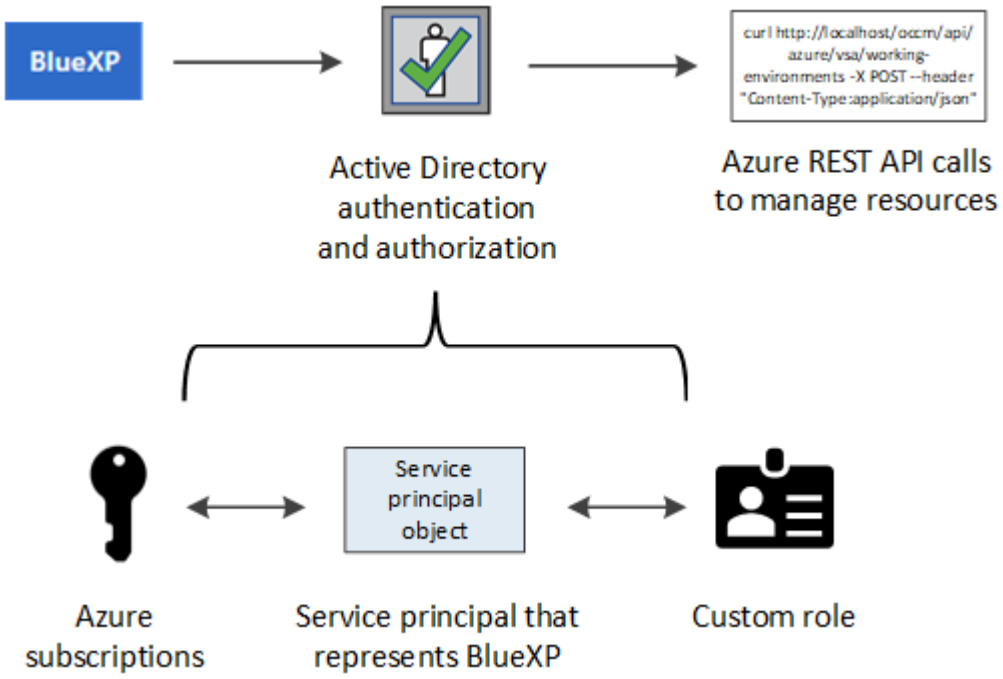
Accordez des autorisations Azure à l'aide d'un principal de service

BlueXP 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 requises par BlueXP.

Description de la tâche

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



Étapes

1. Créez une application Microsoft Entra.
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.

Créez une application Microsoft Entra

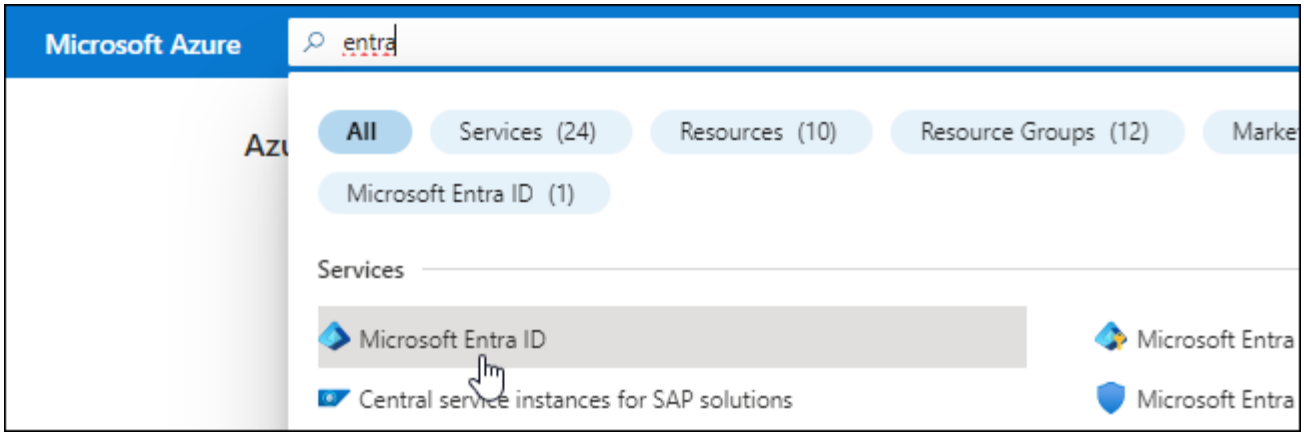
Créez une application et un principal de service Microsoft Entra que BlueXP peut utiliser pour le contrôle d'accès basé sur des rôles.

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. À partir du portail Azure, ouvrez le service **Microsoft Entra ID**.



3. Dans le menu, sélectionnez **enregistrements d'applications**.
4. Sélectionnez **nouvel enregistrement**.
5. Spécifiez les détails de l'application :
   - **Nom** : saisissez un nom pour l'application.
   - **Type de compte** : sélectionnez un type de compte (tout fonctionne avec BlueXP).
   - **URI de redirection**: Vous pouvez laisser ce champ vide.
6. Sélectionnez **Enregistrer**.

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

Résultat

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

Attribuez l'application à un rôle

Vous devez lier l'entité de service à un ou plusieurs abonnements Azure et lui attribuer le rôle "opérateur BlueXP" personnalisé afin que BlueXP dispose d'autorisations dans Azure.

Étapes

1. Création d'un rôle personnalisé :

   Notez que vous pouvez créer un rôle personnalisé Azure à l'aide du portail Azure, d'Azure PowerShell, de l'interface de ligne de commandes Azure ou de l'API REST. La procédure suivante explique comment créer le rôle à l'aide de l'interface de ligne de commandes Azure. Si vous préférez utiliser une autre méthode, reportez-vous à la section "Documentation Azure"

   a. Copier le contenu du "Autorisations de rôle personnalisées pour le connecteur" Et les enregistrer dans un fichier JSON.

   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.

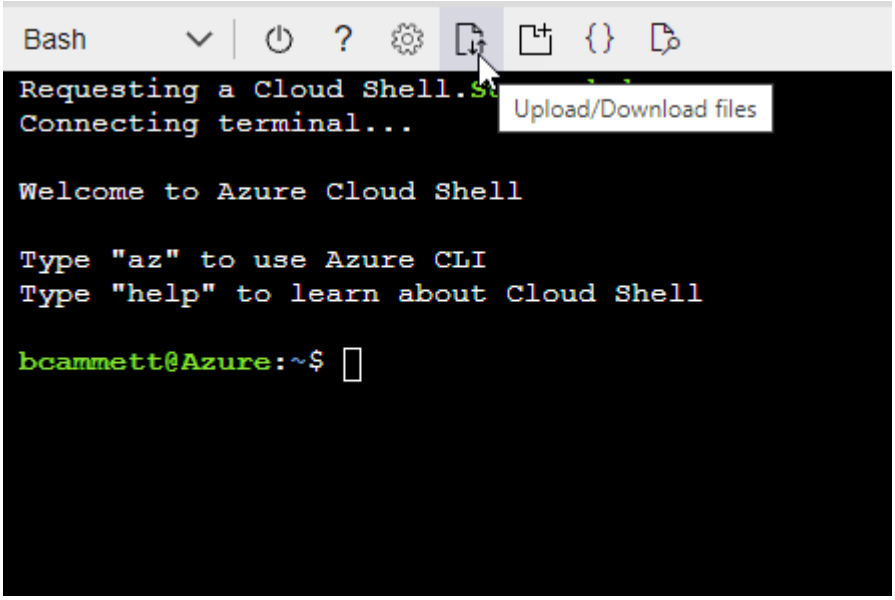
      Exemple

```
"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.

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

- Démarrer "Shell cloud Azure" Et choisissez l'environnement Bash.
- Téléchargez le fichier JSON.



- Pour créer le rôle personnalisé, utilisez l'interface de ligne de commandes Azure :

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

Vous devez maintenant avoir un rôle personnalisé appelé opérateur BlueXP que vous pouvez affecter à la machine virtuelle connecteur.

2. Attribuez l'application au rôle :

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

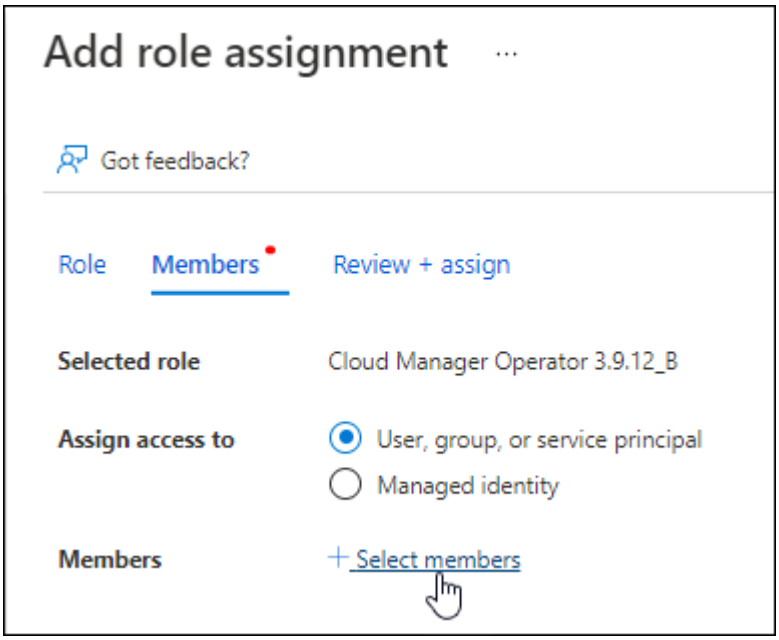
b. Sélectionnez l'abonnement.

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

d. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.

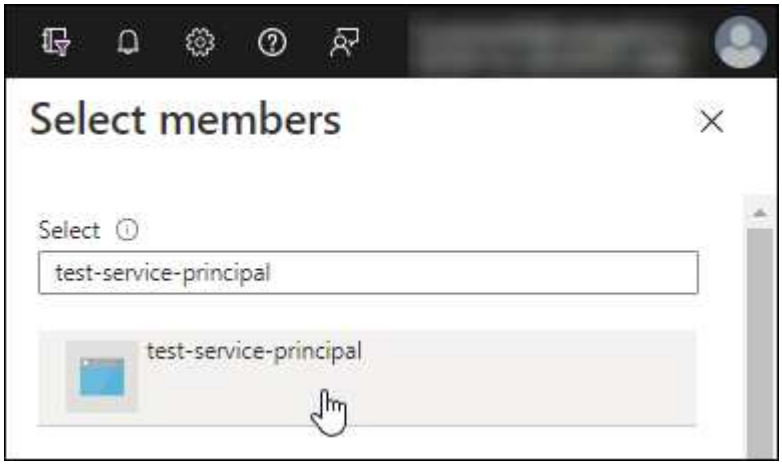
e. Dans l'onglet **membres**, procédez comme suit :

- Conserver **utilisateur, groupe ou entité de service** sélectionnée.
- Sélectionnez **Sélectionner membres**.



- Recherchez le nom de l'application.

  Voici un exemple :



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

f. Sélectionnez **consulter + affecter**.

   Le principal de service dispose désormais des autorisations Azure nécessaires pour déployer le connecteur.

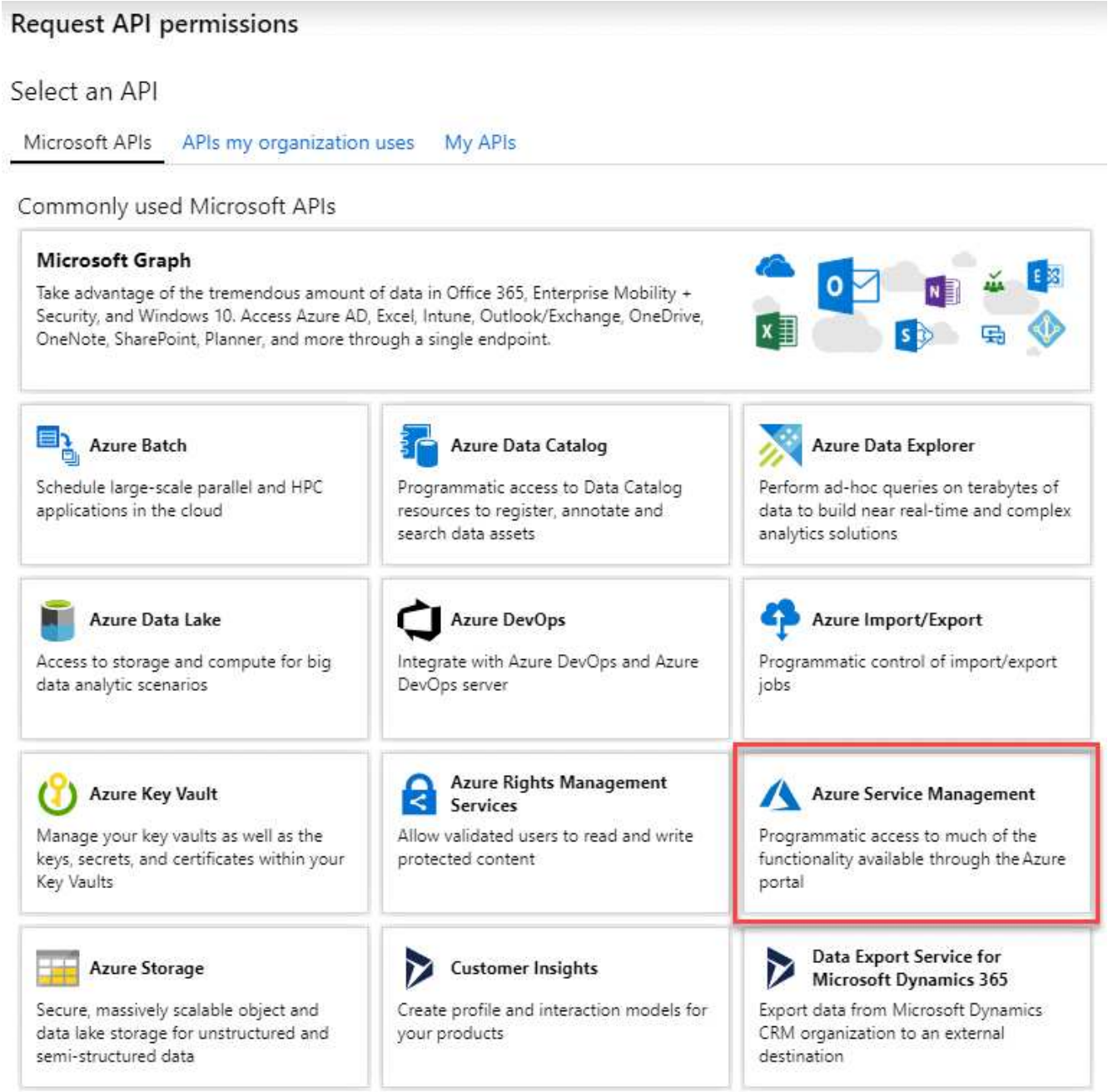
Si vous souhaitez déployer Cloud Volumes ONTAP à partir de plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. BlueXP vous permet de sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

Ajoutez des autorisations d'API de gestion de service Windows Azure

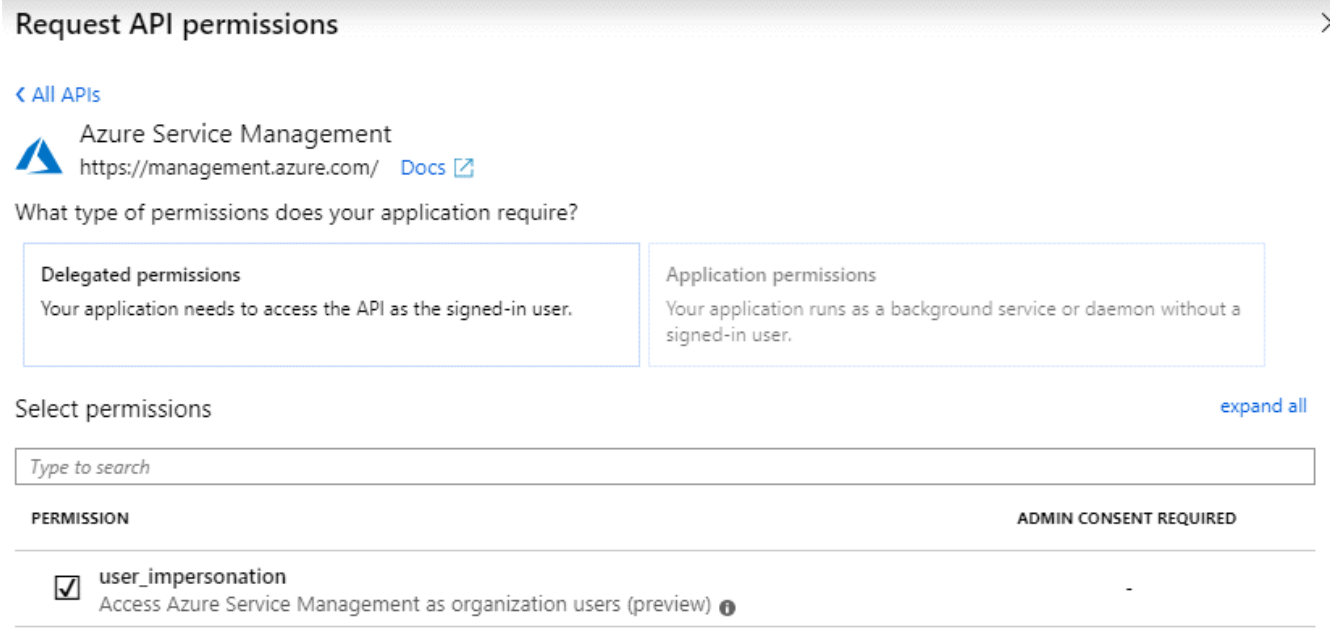
Le principal de service doit disposer d'autorisations « API de gestion des services Windows Azure ».

Étapes

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



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

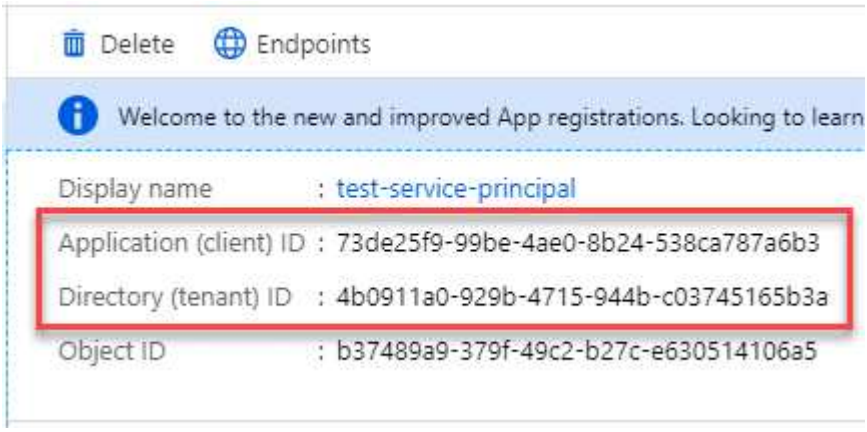


Obtenir l'ID de l'application et l'ID du répertoire

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

Étapes

1. Dans le service **Microsoft Entra ID**, sélectionnez **enregistrements d'applications** et sélectionnez l'application.
2. Copiez l'ID **application (client)** et l'ID **Directory (tenant)**.



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

Créez un secret client

Vous devez créer un secret client, puis fournir à BlueXP la valeur du secret afin que BlueXP puisse l'utiliser pour s'authentifier auprès de Microsoft Entra ID.

Étapes

1. Ouvrez le service **Microsoft Entra ID**.
2. Sélectionnez **enregistrements 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. Copier la valeur du secret client.

BlueXP peut maintenant utiliser un code client pour s'authentifier auprès de Microsoft Entra ID.

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 BlueXP lorsque vous ajoutez un compte Azure.

Ajoutez les identifiants à BlueXP

Une fois que vous avez mis à disposition un compte Azure avec les autorisations requises, vous pouvez ajouter les informations d'identification pour ce compte à BlueXP. Cette étape vous permet de lancer Cloud Volumes ONTAP à l'aide de différentes identifiants Azure.

Avant de commencer

Si vous venez de créer ces identifiants dans votre fournisseur cloud, il vous faudra quelques minutes pour les utiliser. Attendez quelques minutes avant d'ajouter les informations d'identification à BlueXP.

Avant de commencer

Vous devez créer un connecteur avant de pouvoir modifier les paramètres BlueXP. "Apprenez à créer un connecteur".

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **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 > connecteur**.
   b. **Définir les informations d'identification** : saisissez les informations relatives à l'entité de service

Microsoft Entra qui accorde les autorisations requises :

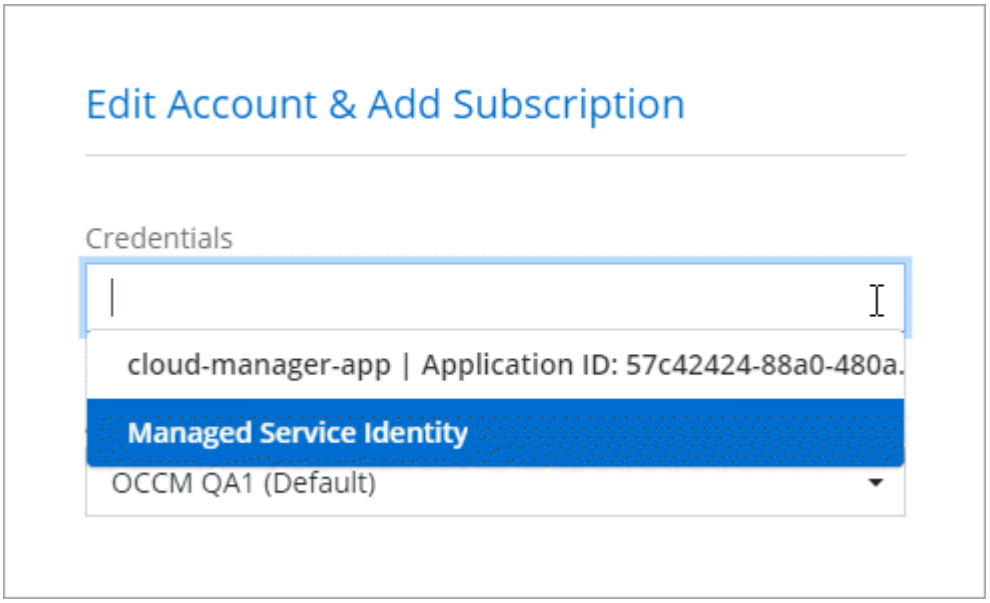
- ID de l'application (client)
- ID du répertoire (locataire)
- Secret client

c. **Abonnement Marketplace** : associez un abonnement Marketplace à ces identifiants 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 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"



Gérer les identifiants existants

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

Associez un abonnement Azure Marketplace à vos identifiants

Après avoir ajouté vos informations d'identification Azure à BlueXP, vous pouvez associer un abonnement Azure Marketplace à ces informations d'identification. L'abonnement vous permet de créer un système Cloud Volumes ONTAP avec paiement à l'utilisation et d'utiliser d'autres services BlueXP.

Deux scénarios peuvent vous être associés à un abonnement Azure Marketplace une fois que vous avez déjà ajouté les informations d'identification à BlueXP :

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

  Le remplacement de l'abonnement Marketplace actuel par un nouvel abonnement modifie l'abonnement Marketplace pour tous les environnements de travail Cloud Volumes ONTAP existants et tous les nouveaux environnements de travail.

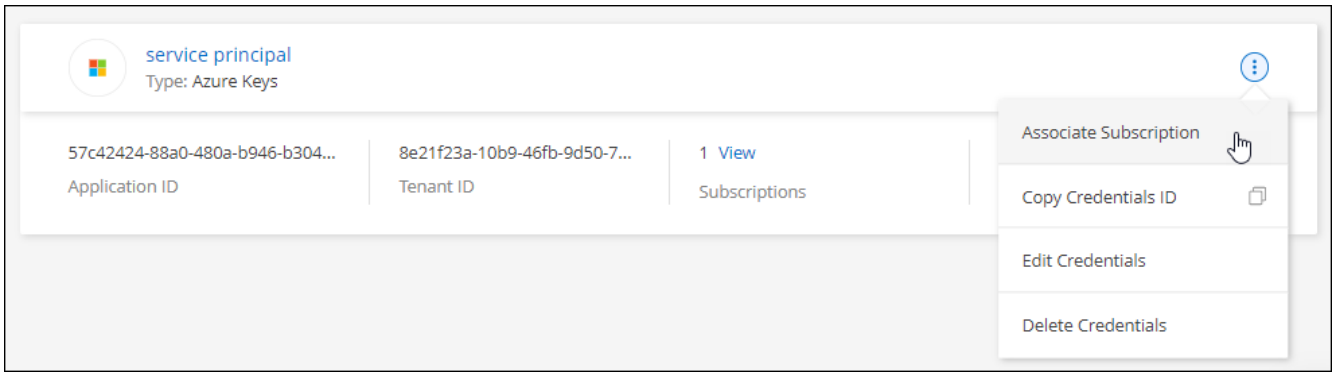
Avant de commencer

Vous devez créer un connecteur avant de pouvoir modifier les paramètres BlueXP. "Découvrez comment".

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
2. Sélectionnez le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **abonnement associé**.

   Vous devez sélectionner les informations d'identification associées à un connecteur. Vous ne pouvez pas associer un abonnement Marketplace aux informations d'identification associées à BlueXP.



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

   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 le site Web BlueXP.

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

      - Sélectionnez les comptes BlueXP avec lesquels vous souhaitez associer cet abonnement.
      - Dans le champ **remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant pour un compte par ce nouvel abonnement.

        BlueXP remplace l'abonnement existant pour toutes les informations d'identification 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 tous les autres comptes, vous devez associer manuellement l'abonnement en répétant ces étapes.

      - Sélectionnez **Enregistrer**.

        La vidéo suivante explique comment vous abonner à Azure Marketplace :

Abonnez-vous à BlueXP depuis Azure Marketplace

Modifier les informations d'identification

Modifiez vos informations d'identification Azure dans BlueXP en modifiant les informations d'identification de votre service Azure. Par exemple, vous devrez peut-être mettre à jour le secret client si un nouveau secret a été créé pour l'application principale du service.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
2. Sur la page **informations d'identification du compte**, sélectionnez le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **Modifier les informations d'identification**.
3. Effectuez 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 de BlueXP. Vous ne pouvez supprimer que les informations d'identification qui ne sont pas associées à un environnement de travail.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
2. Sur la page **informations d'identification du compte**, sélectionnez le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **Supprimer les informations d'identification**.
3. Sélectionnez **Supprimer** pour confirmer.