Identifiants AWS

Set up and administration

NetApp
December 15, 2022

Table des matières

Identifiants AWS

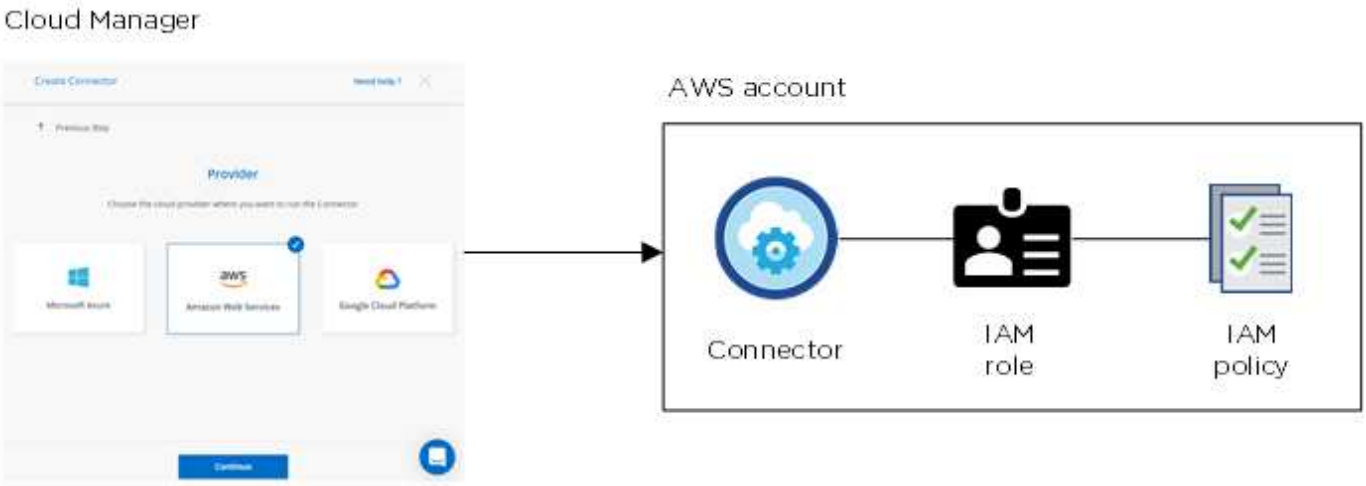
Identifiants et autorisations AWS

BlueXP vous permet de choisir les informations d'identification 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.

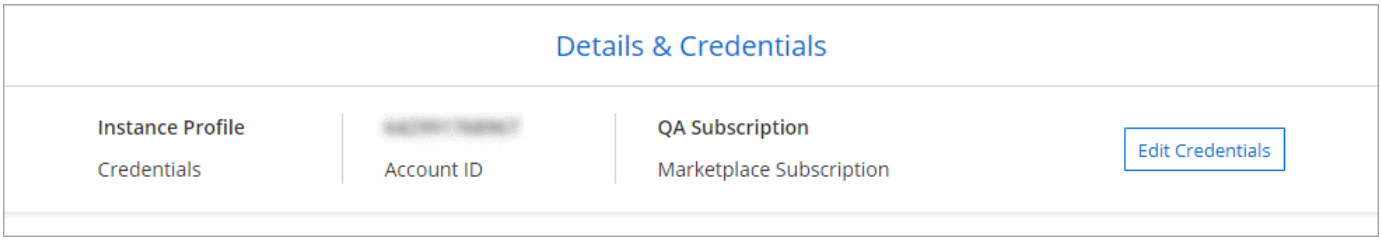
Identifiants AWS initiaux

Lorsque vous déployez un connecteur depuis BlueXP, vous devez fournir l'ARN d'un rôle IAM ou de clés d'accès pour un utilisateur IAM. La méthode d'authentification que vous utilisez doit disposer des autorisations requises pour déployer l'instance de connecteur dans AWS. Les autorisations requises sont répertoriées dans le "Règle de déploiement du connecteur pour AWS".

Lorsque BlueXP lance l'instance Connector dans AWS, il crée un rôle IAM et un profil d'instance pour l'instance. Il attache également une règle qui fournit au connecteur les autorisations nécessaires pour gérer les ressources et les processus de ce compte AWS. "Consultez la manière dont BlueXP utilise les autorisations".



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

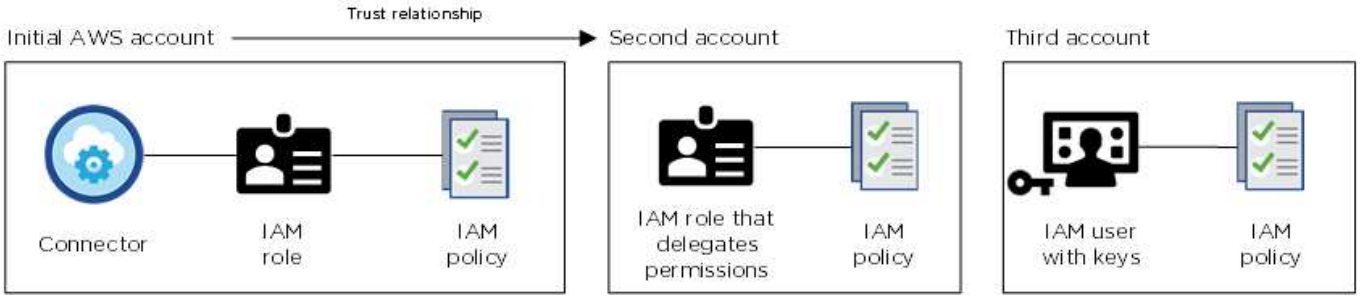


Autres identifiants AWS

Il existe deux façons d'ajouter des identifiants AWS supplémentaires.

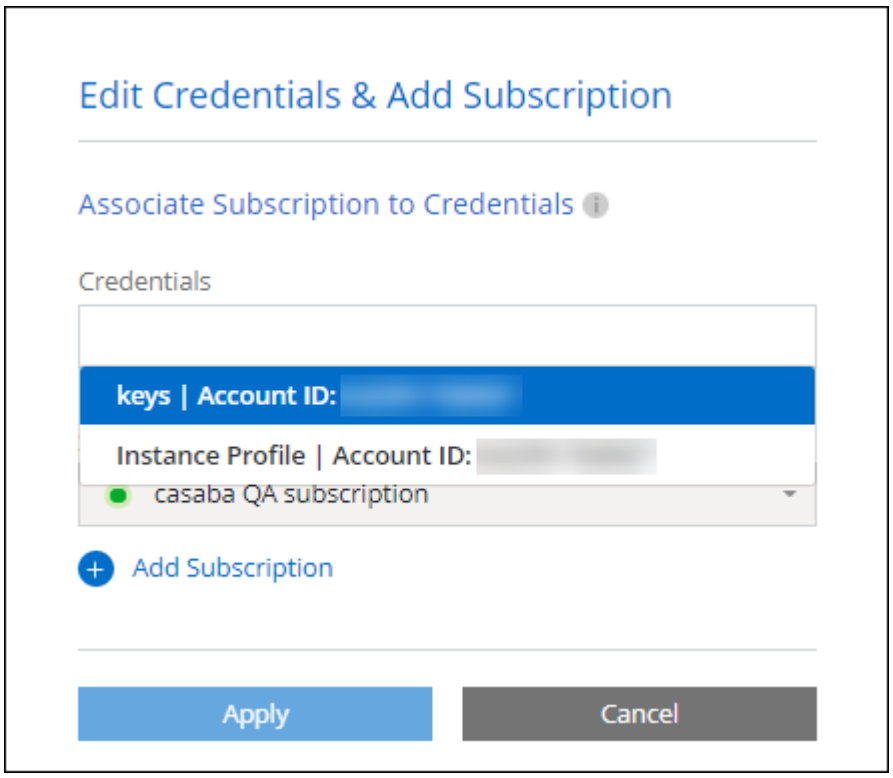
Ajoutez des identifiants AWS à un connecteur existant

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 informations d'identification du compte à BlueXP" 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 :



Ajoutez des informations d'identification AWS directement à BlueXP

L'ajout de nouvelles informations d'identification AWS à BlueXP fournit les autorisations nécessaires pour créer et gérer un environnement de travail FSX pour ONTAP ou pour créer un connecteur.

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

BlueXP. 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 BlueXP, mais vous pouvez fournir des autorisations exactement comme pour d'autres comptes AWS.

Comment faire tourner mes identifiants AWS en toute sécurité ?

Comme décrit ci-dessus, BlueXP vous permet de fournir des identifiants AWS de diverses 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, BlueXP utilise AWS Security Token Service pour obtenir des informations d'identification temporaires qui tournent en permanence. Ce processus est la meilleure pratique—il automatique et sécurisé.

Si vous fournissez des clés d'accès AWS BlueXP, vous devez les mettre à jour régulièrement dans BlueXP. Il s'agit d'un processus entièrement manuel.

Gérez les informations d'identification et les abonnements AWS pour BlueXP

Ajoutez et gérez des identifiants AWS de sorte que BlueXP dispose des autorisations nécessaires pour déployer et gérer des ressources cloud dans vos comptes AWS. Si vous gérez plusieurs abonnements AWS, vous pouvez les attribuer à différentes informations d'identification AWS à partir de la page informations d'identification.

Présentation

Vous pouvez ajouter des informations d'identification AWS à un connecteur existant ou directement à BlueXP :

- Ajoutez des identifiants AWS supplémentaires à un connecteur existant

  L'ajout d'identifiants AWS à un connecteur existant offre les autorisations nécessaires pour gérer les ressources et les processus au sein de votre environnement de cloud public. Découvrez comment ajouter des identifiants AWS à un connecteur.

- Ajoutez des informations d'identification AWS à BlueXP pour créer un connecteur

  L'ajout de nouvelles informations d'identification AWS à BlueXP offre à BlueXP les autorisations nécessaires pour créer un connecteur. Découvrez comment ajouter des identifiants AWS à BlueXP.

- Ajoutez des informations d'identification AWS à BlueXP pour FSX pour ONTAP

  L'ajout de nouvelles informations d'identification AWS à BlueXP offre à BlueXP les autorisations nécessaires pour créer et gérer FSX pour ONTAP. "Découvrez comment configurer des autorisations pour FSX pour ONTAP"

Comment faire pivoter les informations d'identification

BlueXP vous permet de fournir des identifiants AWS de diverses 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. "En savoir plus sur les identifiants et les autorisations AWS".

Avec les deux premières options, BlueXP utilise AWS Security Token Service pour obtenir des informations d'identification temporaires qui tournent en permanence. Ce processus est la meilleure pratique car il est automatique et sécurisé.

Si vous fournissez des clés d'accès AWS BlueXP, vous devez les mettre à jour régulièrement dans BlueXP. Il s'agit d'un processus entièrement manuel.

Ajouter des informations d'identification à un connecteur

Ajoutez des identifiants AWS à un connecteur pour qu'il dispose des autorisations nécessaires pour gérer les ressources et les processus au sein de votre environnement de cloud public. Vous pouvez indiquer l'ARN d'un rôle IAM dans un autre compte ou fournir les clés d'accès AWS.

Accorder des autorisations

Avant d'ajouter des identifiants AWS à un connecteur, vous devez fournir les autorisations requises. Les autorisations permettent à BlueXP de gérer les ressources et les processus au sein de ce compte AWS. La manière dont vous fournissez les autorisations dépend du fait que vous souhaitez fournir à BlueXP l'ARN d'un rôle dans un compte de confiance ou des clés AWS.

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

Choix

- Accorder des autorisations en assumant un rôle IAM dans un autre compte
- Accordez des autorisations en fournissant des clés AWS

Accorder des autorisations en assumant un rôle IAM dans un autre compte

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 fournissez ensuite à BlueXP les rôles ARN des IAM des comptes de confiance.

Étapes

1. Accédez à la console IAM dans le compte cible dans lequel vous souhaitez fournir le connecteur avec les autorisations.
2. Sous gestion des accès, cliquez sur **rôles > Créer un rôle** et suivez les étapes pour créer le rôle.

   Assurez-vous de faire ce qui suit :

   - Sous **Type d'entité approuvée**, sélectionnez **compte AWS**.
   - Sélectionnez **un autre compte AWS** et entrez l'ID du compte sur lequel réside l'instance de connecteur.

- Créez les politiques requises en copiant et en collant le contenu de "Les règles IAM pour le connecteur".

3. Copiez le rôle ARN du rôle IAM afin de pouvoir le coller ultérieurement dans BlueXP.

Résultat

Le compte dispose désormais des autorisations requises. Vous pouvez désormais ajouter les informations d'identification à un connecteur.

Accordez des autorisations en fournissant des clés AWS

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

Étapes

1. À partir de la console IAM, créez des politiques en copiant et en collant le contenu de "Les règles IAM pour le connecteur".

   "Documentation AWS : création de règles IAM"

2. Associez les règles 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 ajouter les informations d'identification à un connecteur.

Ajoutez les informations d'identification

Une fois que vous avez passé un compte AWS avec les autorisations requises, vous pouvez ajouter les identifiants de ce compte à un connecteur existant. Cela vous permet de lancer des systèmes Cloud Volumes ONTAP dans ce compte à l'aide du même connecteur.

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.

Étapes

1. Assurez-vous que le bon connecteur est actuellement sélectionné dans BlueXP.
2. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.

3. Cliquez sur **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
   a. **Emplacement des informations d'identification** : sélectionnez **Amazon Web Services > connecteur**.

b. **Définir les informations d'identification** : fournir l'ARN (Amazon Resource Name) d'un rôle IAM approuvé, ou entrer une clé d'accès AWS et une clé secrète.

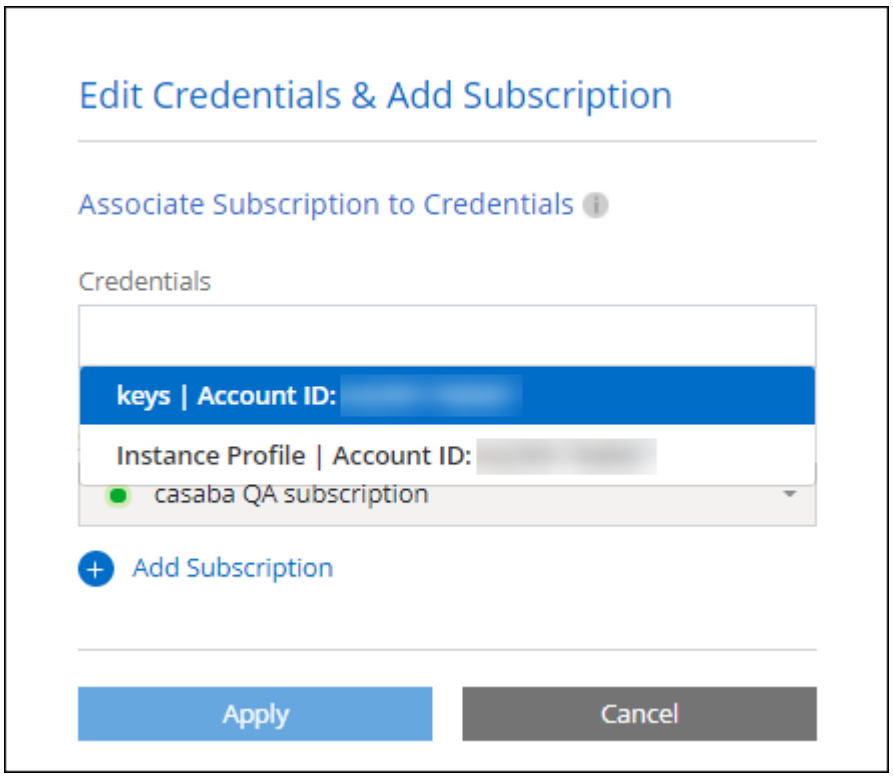
c. **Abonnement Marketplace** : associez un abonnement Marketplace à ces identifiants en vous abonnant maintenant ou en sélectionnant un abonnement existant.

   Pour payer Cloud Volumes ONTAP à l'heure (PAYGO) ou par un contrat annuel, vous devez associer des identifiants AWS à un abonnement à Cloud Volumes ONTAP depuis AWS Marketplace.

d. **Review** : confirmez les détails des nouvelles informations d'identification et cliquez sur **Add**.

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 :



Ajoutez des informations d'identification à BlueXP pour créer un connecteur

Ajoutez des informations d'identification AWS à BlueXP en fournissant l'ARN d'un rôle IAM qui donne à BlueXP les autorisations nécessaires pour créer un connecteur. Vous pouvez choisir ces informations d'identification lors de la création d'un nouveau connecteur.

Configurer le rôle IAM

Configurez un rôle IAM qui permet au service BlueXP SaaS de prendre en charge le rôle.

Étapes

1. Accédez à la console IAM dans le compte cible.
2. Sous gestion des accès, cliquez sur **rôles > Créer un rôle** et suivez les étapes pour créer le rôle.

   Assurez-vous de faire ce qui suit :

- Sous **Type d'entité approuvée**, sélectionnez **compte AWS**.
- Sélectionnez **un autre compte AWS** et saisissez l'ID du service BlueXP SaaS : 952013314444
- Créez une stratégie qui inclut les autorisations requises pour créer un connecteur.
  - "Affichez les autorisations nécessaires pour FSX pour ONTAP"
  - "Afficher la règle de déploiement des connecteurs"

3. Copiez le rôle ARN du rôle IAM afin de pouvoir le coller dans BlueXP à l'étape suivante.

Résultat

Le rôle IAM dispose désormais des autorisations requises. Vous pouvez maintenant l'ajouter à BlueXP.

Ajoutez les informations d'identification

Une fois que vous avez autorisé le rôle IAM, ajoutez le rôle ARN à BlueXP.

Avant de commencer

Si vous venez de créer le rôle IAM, l'utilisation peut prendre quelques minutes. Attendez quelques minutes avant d'ajouter les informations d'identification à BlueXP.

Étapes

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

2. Cliquez sur **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
   a. **Informations d'identification Location** : sélectionnez **Amazon Web Services > BlueXP**.
   b. **Définir les informations d'identification** : fournir l'ARN (Amazon Resource Name) du rôle IAM.
   c. **Review** : confirmez les détails des nouvelles informations d'identification et cliquez sur **Add**.

Résultat

Vous pouvez maintenant utiliser les informations d'identification lors de la création d'un nouveau connecteur.

Associez un abonnement AWS

Après avoir ajouté vos identifiants AWS à BlueXP, vous pouvez associer un abonnement AWS Marketplace à ces identifiants. L'abonnement vous permet de payer le prix Cloud Volumes ONTAP à l'heure (PAYGO) ou de souscrire un contrat annuel 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 BlueXP :

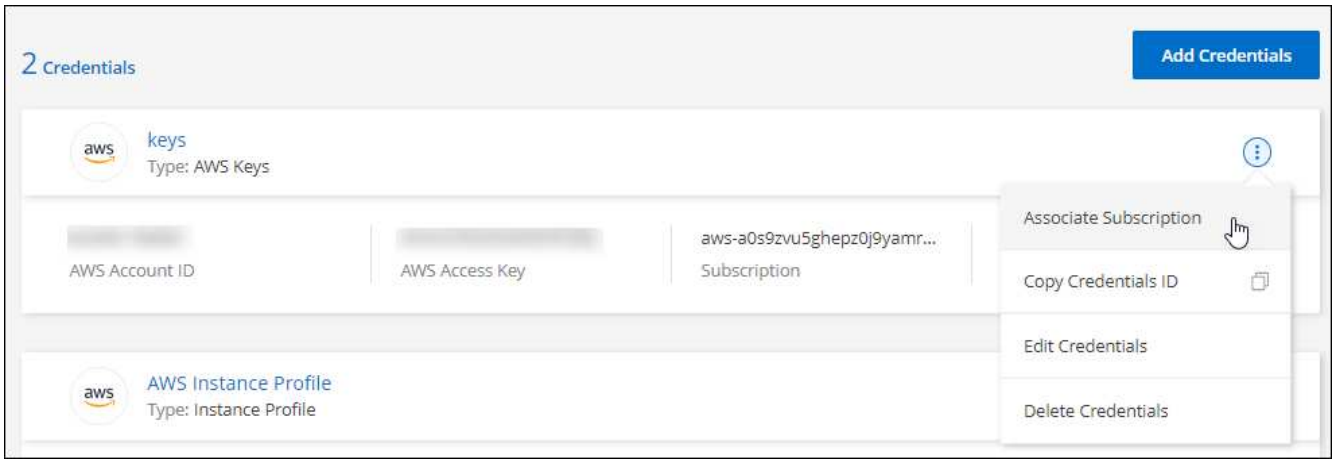
- Vous n'avez pas associé d'abonnement lorsque vous avez initialement ajouté les informations d'identification à BlueXP.
- Vous souhaitez remplacer un abonnement AWS Marketplace existant par un nouvel abonnement.

Ce dont vous avez besoin

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, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Cliquez sur le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **associer un abonnement**.



3. Sélectionnez un abonnement existant 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/cloud-manager-setup-admin//media/video_subscribing_aws.mp4 *(video)*

Modifier les informations d'identification

Modifiez vos informations d'identification AWS dans BlueXP en modifiant le type de compte (clés AWS ou rôle supposons), en modifiant le nom ou en mettant à jour les informations d'identification elles-mêmes (clés ou rôle ARN).

Vous ne pouvez pas modifier les informations d'identification d'un profil d'instance associé à une instance de connecteur.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Cliquez sur le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **Modifier les informations d'identification**.
3. Apportez les modifications requises, puis cliquez sur **appliquer**.

Suppression des 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.

Vous ne pouvez pas supprimer les informations d'identification d'un profil d'instance associé à une instance de connecteur.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Cliquez sur le menu d'action pour un ensemble d'informations d'identification, puis sélectionnez **Supprimer les informations d'identification**.
3. Cliquez sur **Supprimer** pour confirmer.