AWS

Cloud Manager 3.8

NetApp
March 25, 2024

Sommaire

AWS 1
Identifiants et autorisations AWS 1
Gestion des identifiants AWS et des abonnements pour Cloud Manager 3

AWS

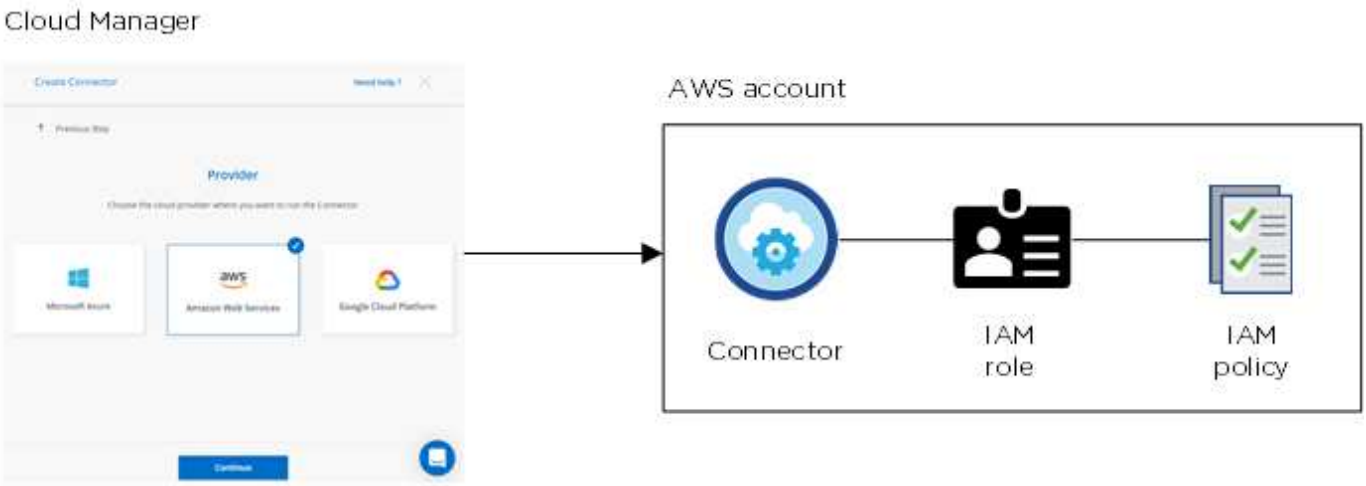
Identifiants et autorisations AWS

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.

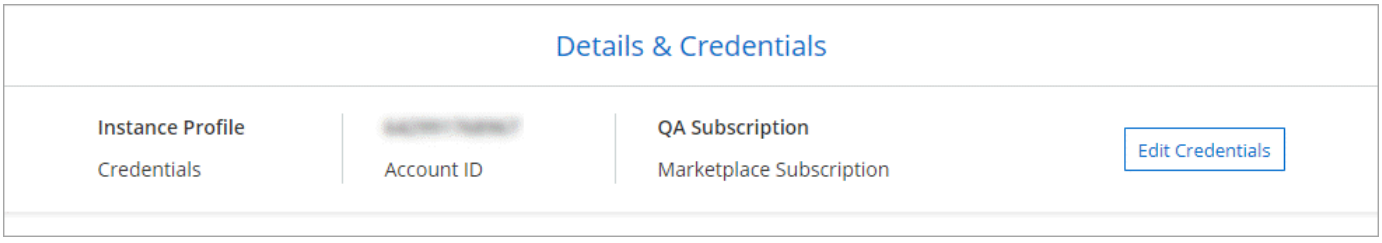
Identifiants AWS initiaux

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".

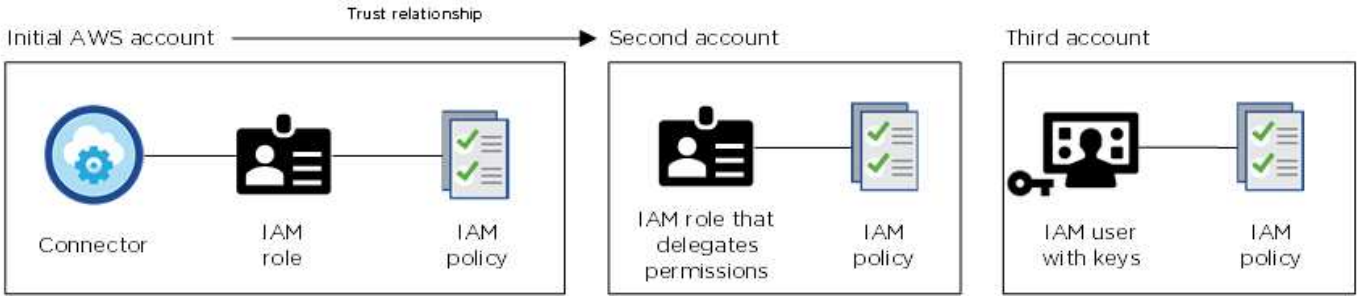


Cloud Manager sélectionne ces identifiants AWS par défaut lorsque vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP :



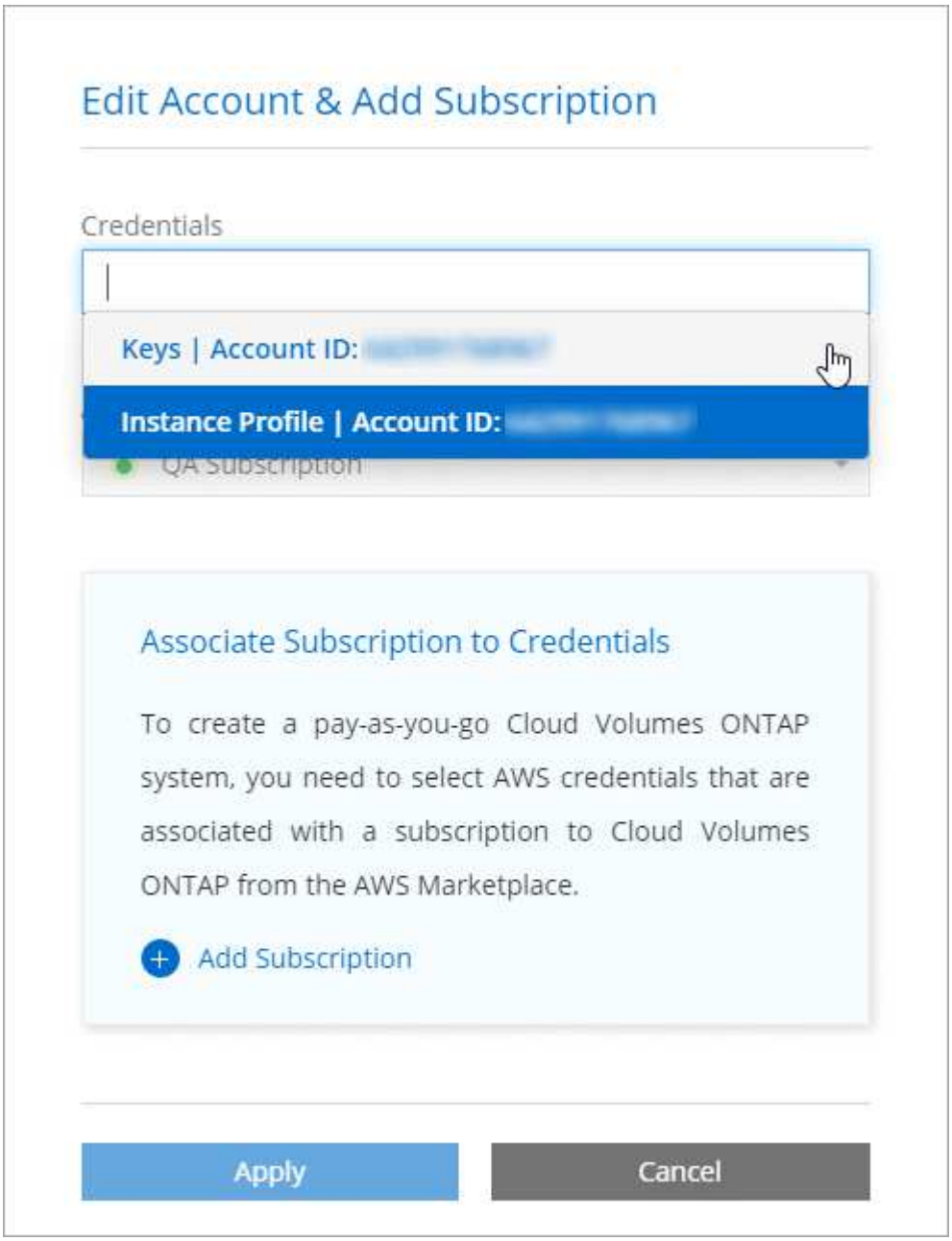
Autres identifiants AWS

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

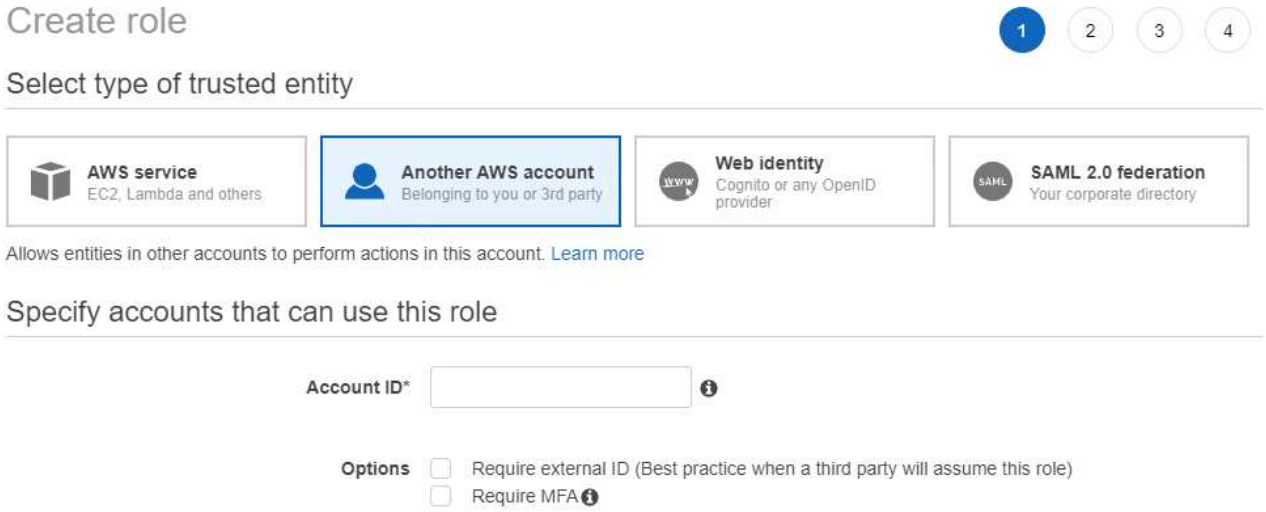
Vous pouvez définir une relation de confiance entre le compte AWS source dans lequel vous avez déployé l'instance Connector et d'autres comptes AWS en utilisant les rôles IAM. Vous pouvez ensuite fournir à Cloud Manager l'ARN des rôles IAM depuis les comptes de confiance.

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

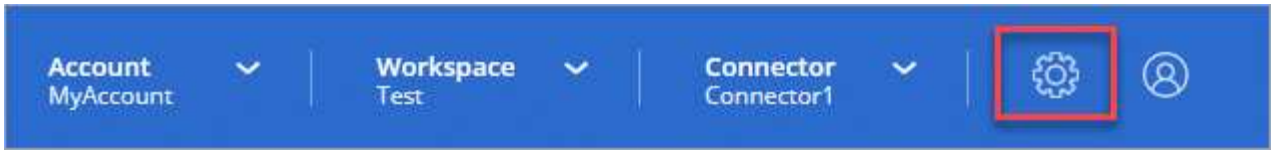
Le compte dispose désormais des autorisations requises. Vous pouvez désormais l'ajouter à Cloud Manager.

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**.



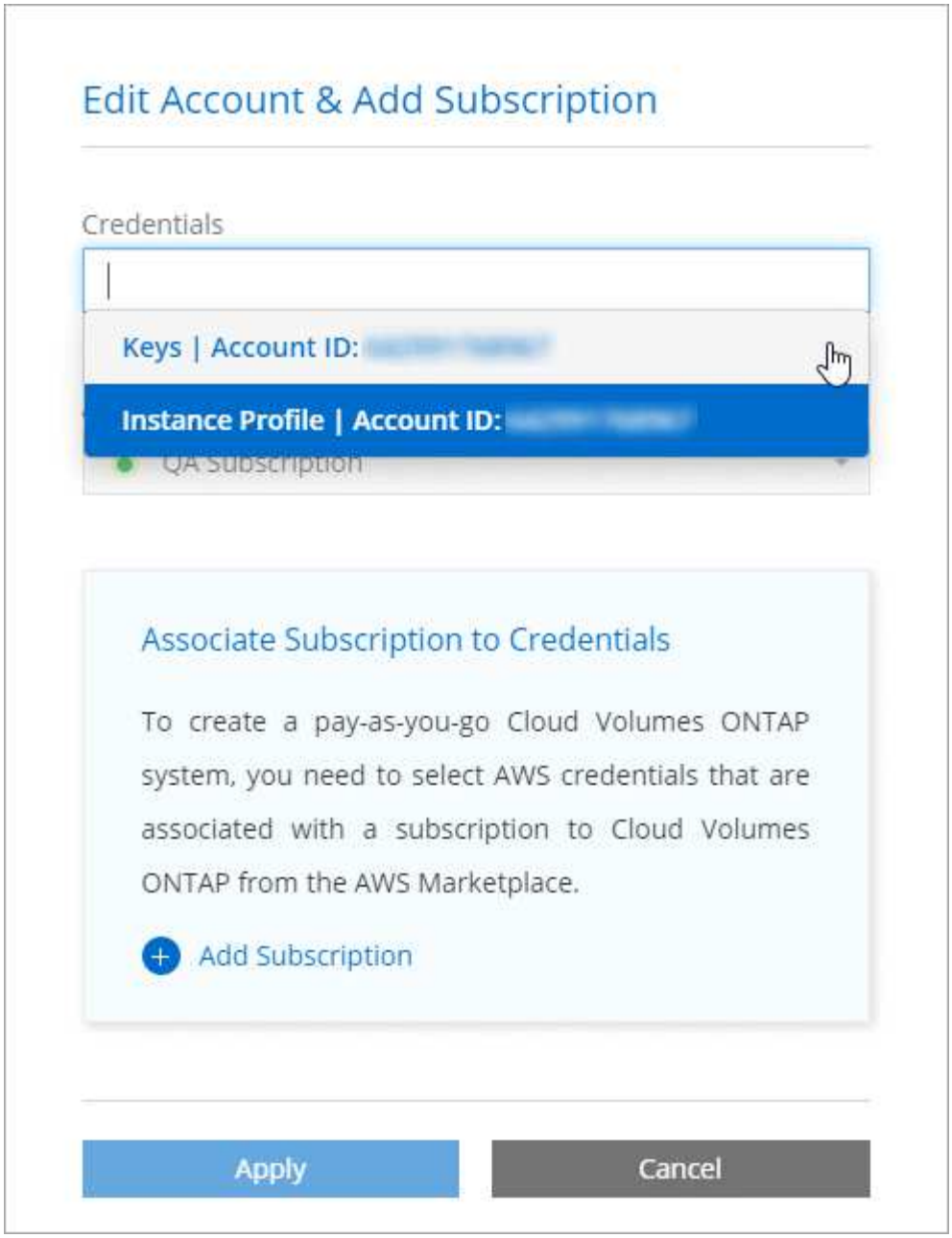
2. Cliquez sur **Ajouter des informations d'identification** et sélectionnez **AWS**.
3. Vous pouvez fournir des clés AWS ou l'ARN d'un rôle IAM approuvé.
4. Vérifiez que les exigences de la politique ont été respectées et cliquez sur **Continuer**.
5. Choisissez l'abonnement payant à l'utilisation que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

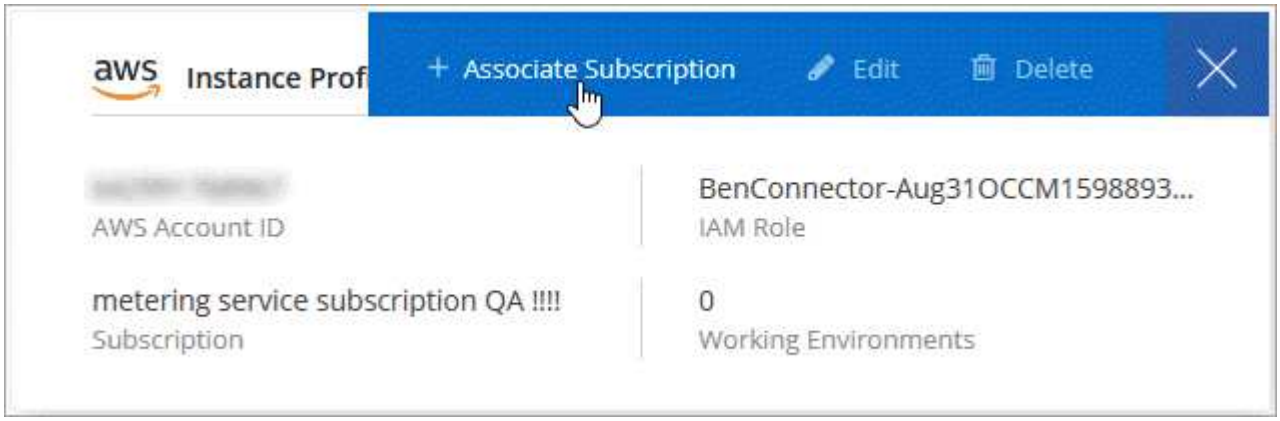
- Vous n'avez pas associé un abonnement lors de l'ajout initial des identifiants à Cloud Manager.
- Vous souhaitez remplacer un abonnement AWS Marketplace existant par un nouvel abonnement.

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)*