



Informations d'identification et abonnements

NetApp Console setup and administration

NetApp
December 11, 2025

This PDF was generated from <https://docs.netapp.com/fr-fr/console-setup-admin/concept-accounts-aws.html> on December 11, 2025. Always check docs.netapp.com for the latest.

Sommaire

Informations d'identification et abonnements	1
AWS	1
En savoir plus sur les informations d'identification et les autorisations AWS dans la NetApp Console	1
Gérer les informations d'identification AWS et les abonnements au marché pour NetApp Console	5
Azuré	15
En savoir plus sur les informations d'identification et les autorisations Azure dans la NetApp Console	15
Gérer les informations d'identification Azure et les abonnements à la place de marché pour la NetApp Console	18
Google Cloud	30
En savoir plus sur les projets et les autorisations Google Cloud	30
Gestion des autorisations de l'agent de la console pour les déploiements Google Cloud	31
Gérer les informations d'identification NSS associées à la NetApp Console	31
Aperçu	32
Ajouter un compte NSS	32
Mettre à jour les informations d'identification NSS	33
Attacher un système à un autre compte NSS	33
Afficher l'adresse e-mail d'un compte NSS	34
Supprimer un compte NSS	34
Gérer les informations d'identification associées à votre connexion à la NetApp Console	35
Informations d'identification ONTAP	35
Informations d'identification NSS	35
Gérez vos identifiants d'utilisateur	36

Informations d'identification et abonnements

AWS

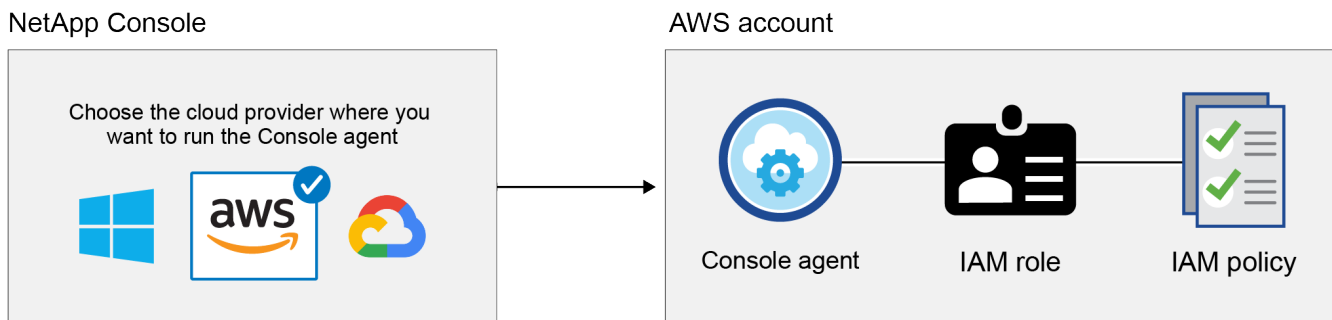
En savoir plus sur les informations d'identification et les autorisations AWS dans la NetApp Console

Vous gérez les informations d'identification AWS et les abonnements Marketplace directement depuis la NetApp Console pour garantir le déploiement sécurisé de Cloud Volumes ONTAP et d'autres services de données en fournissant les informations d'identification IAM appropriées lors du déploiement de l'agent de la console et en les associant aux abonnements AWS Marketplace pour la facturation.

Informations d'identification AWS initiales

Lorsque vous déployez un agent de console à partir de la console, vous devez fournir l'ARN d'un rôle IAM ou des clés d'accès pour un utilisateur IAM. La méthode d'authentification doit disposer des autorisations nécessaires pour déployer l'agent Console dans AWS. Les autorisations requises sont listées dans le ["Politique de déploiement d'agents pour AWS"](#).

Lorsque la console lance l'agent de console dans AWS, elle crée un rôle IAM et un profil pour l'agent. Il attache également une politique qui fournit à l'agent de la console des autorisations pour gérer les ressources et les processus au sein de ce compte AWS. ["Vérifiez comment l'agent utilise les autorisations"](#).



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

Details & Credentials			
Instance Profile		QA Subscription	Edit Credentials
Credentials	Account ID	Marketplace Subscription	

Déployez tous vos systèmes Cloud Volumes ONTAP à l'aide des informations d'identification AWS initiales ou vous pouvez ajouter des informations d'identification supplémentaires.

Informations d'identification AWS supplémentaires

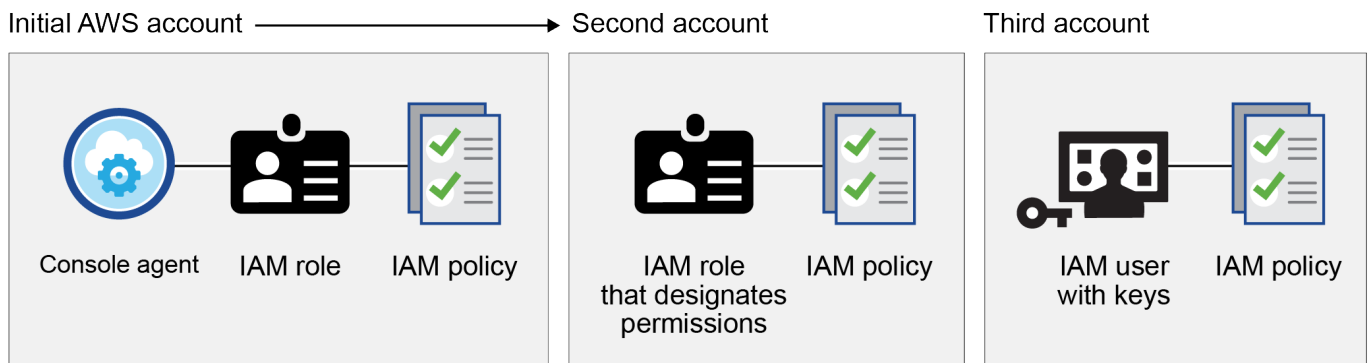
Vous pouvez ajouter des informations d'identification AWS supplémentaires à la console dans les cas suivants :

- Pour utiliser votre agent Console existant avec un compte AWS supplémentaire
- Pour créer un nouvel agent dans un compte AWS spécifique
- Pour créer et gérer les systèmes de fichiers FSx pour ONTAP

Consultez les sections ci-dessous pour plus de détails.

Ajoutez des informations d'identification AWS pour utiliser un agent de console avec un autre compte AWS

Pour utiliser la console avec des comptes AWS supplémentaires, fournissez des clés AWS ou l'ARN d'un rôle dans un compte de confiance. L'image suivante montre deux comptes supplémentaires, l'un fournissant des autorisations via un rôle IAM dans un compte approuvé et l'autre via les clés AWS d'un utilisateur IAM :



Vous ajoutez les informations d'identification du compte à la console en spécifiant le nom de ressource Amazon (ARN) du rôle IAM ou les clés AWS de l'utilisateur IAM.

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

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

keys | Account ID: [redacted]

Instance Profile | Account ID: [redacted]

casaba QA subscription

+ Add Subscription

Apply

Cancel

["Découvrez comment ajouter des informations d'identification AWS à un agent existant."](#)

Ajoutez les informations d'identification AWS pour créer un agent de console

L'ajout des identifiants AWS permet de créer un agent de console.

["Découvrez comment ajouter des informations d'identification AWS à la console pour créer un agent de console"](#)

Ajouter les informations d'identification AWS pour FSx pour ONTAP

Ajoutez les informations d'identification AWS à la console pour fournir les autorisations nécessaires à la création et à la gestion d'un système FSx pour ONTAP .

["Découvrez comment ajouter des informations d'identification AWS à la console pour Amazon FSx for ONTAP"](#)

Informations d'identification et abonnements à la place de marché

Vous devez associer les informations d'identification que vous ajoutez à un agent de console à un abonnement AWS Marketplace pour payer Cloud Volumes ONTAP à un tarif horaire (PAYGO) et d'autres services de données NetApp ou par le biais d'un contrat annuel. ["Découvrez comment associer un abonnement AWS"](#).

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

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

FAQ

Les questions suivantes concernent les informations d'identification et les abonnements.

Comment puis-je faire pivoter mes informations d'identification AWS en toute sécurité ?

Comme décrit dans les sections ci-dessus, la console vous permet de fournir des informations d'identification AWS de plusieurs manières : un rôle IAM associé à l'agent de la console, en assumant un rôle IAM dans un compte approuvé ou en fournissant des clés d'accès AWS.

Avec les deux premières options, la console utilise le service AWS Security Token pour obtenir des informations d'identification temporaires qui changent constamment. Ce processus représente la meilleure pratique : il est automatique et sécurisé.

Si vous fournissez à la console des clés d'accès AWS, vous devez faire tourner les clés en les mettant à jour dans la console à intervalles réguliers. Il s'agit d'un processus entièrement manuel.

Puis-je modifier l'abonnement AWS Marketplace pour les systèmes Cloud Volumes ONTAP ?

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

["Découvrez comment associer un abonnement AWS"](#) .

Puis-je ajouter plusieurs informations d'identification AWS, chacune avec des abonnements de marché différents ?

Toutes les informations d'identification AWS appartenant au même compte AWS seront associées au même abonnement AWS Marketplace.

Si vous disposez de plusieurs informations d'identification AWS appartenant à différents comptes AWS, ces informations d'identification peuvent être associées au même abonnement AWS Marketplace ou à des abonnements différents.

Puis-je déplacer des systèmes Cloud Volumes ONTAP existants vers un autre compte AWS ?

Non, il n'est pas possible de déplacer les ressources AWS associées à votre système Cloud Volumes ONTAP vers un autre compte AWS.

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 sur AWS depuis AWS Marketplace et installer manuellement le logiciel agent Console sur votre propre hôte Linux ou dans votre vCenter.

Si vous utilisez la Marketplace, les 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 la console, mais vous pouvez fournir des autorisations à l'aide de clés d'accès AWS.

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

- Mode standard

- ["Configurer les autorisations pour un déploiement AWS Marketplace"](#)
- ["Configurer les autorisations pour les déploiements sur site"](#)
- Mode restreint
 - ["Configurer les autorisations pour le mode restreint"](#)

Gérer les informations d'identification AWS et les abonnements au marché pour NetApp Console

Ajoutez et gérez les informations d'identification AWS afin de déployer et de gérer les ressources cloud dans vos comptes AWS à partir de la NetApp Console. Si vous gérez plusieurs abonnements AWS Marketplace, vous pouvez attribuer chacun d'eux à différentes informations d'identification AWS à partir de la page Informations d'identification.

Aperçu

Vous pouvez ajouter des informations d'identification AWS à un agent de console existant ou directement à la console :

- Ajouter des informations d'identification AWS supplémentaires à un agent existant

Ajoutez les informations d'identification AWS à un agent de console pour gérer les ressources cloud. [Découvrez comment ajouter des informations d'identification AWS à un agent de console](#) .

- Ajoutez les informations d'identification AWS à la console pour créer un agent de console

L'ajout de nouvelles informations d'identification AWS à la console fournit les autorisations nécessaires pour créer un agent de console. [Découvrez comment ajouter des informations d'identification AWS à la NetApp Console](#) .

- Ajouter les informations d'identification AWS à la console pour FSx pour ONTAP

Ajoutez de nouvelles informations d'identification AWS à la console pour créer et gérer FSx pour ONTAP. ["Découvrez comment configurer les autorisations pour FSx pour ONTAP"](#)

Comment faire tourner les informations d'identification

La NetApp Console vous permet de fournir des informations d'identification AWS de plusieurs manières : un rôle IAM associé à l'instance de l'agent, en assumant un rôle IAM dans un compte approuvé ou en fournissant des clés d'accès AWS. ["En savoir plus sur les informations d'identification et les autorisations AWS"](#) .

Avec les deux premières options, la console utilise le service AWS Security Token pour obtenir des informations d'identification temporaires qui changent constamment. Ce processus est la meilleure pratique car il est automatique et sécurisé.

Faites pivoter manuellement les clés d'accès AWS en les mettant à jour dans la console.

Ajouter des informations d'identification supplémentaires à un agent de console

Ajoutez des informations d'identification AWS supplémentaires à un agent de console afin qu'il dispose des autorisations nécessaires pour gérer les ressources et les processus au sein de votre environnement de cloud

public. Vous pouvez soit fournir l'ARN d'un rôle IAM dans un autre compte, soit fournir des clés d'accès AWS.

["Découvrez comment la NetApp Console utilise les informations d'identification et les autorisations AWS".](#)

Accorder des autorisations

Accordez des autorisations avant d'ajouter des informations d'identification AWS à un agent de console. Les autorisations permettent à un agent de console de gérer les ressources et les processus au sein de ce compte AWS. Vous pouvez fournir les autorisations avec l'ARN d'un rôle dans un compte approuvé ou des clés AWS.



Si vous avez déployé un agent de console à partir de la console, les informations d'identification AWS pour le compte dans lequel vous avez déployé un agent de console ont été automatiquement ajoutées. Cela garantit que les autorisations nécessaires sont en place pour la gestion des ressources.

Choix

- [Accorder des autorisations en assumant un rôle IAM dans un autre compte](#)
- [Accorder des autorisations en fournissant des clés AWS](#)

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

Vous pouvez configurer une relation d'approbation entre le compte AWS source dans lequel vous avez déployé un agent de console et d'autres comptes AWS à l'aide de rôles IAM. Vous devez ensuite fournir à la console l'ARN des rôles IAM à partir des comptes approuvés.

Si un agent de console est installé sur site, vous ne pouvez pas utiliser cette méthode d'authentification. Vous devez utiliser des clés AWS.

Étapes

1. Accédez à la console IAM du compte cible dans lequel vous souhaitez fournir des autorisations à un agent de console.
2. Sous Gestion des accès, sélectionnez **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 compte sur lequel réside une instance d'agent de console.
 - Créez les politiques requises en copiant et en collant le contenu de ["les politiques IAM pour un agent de console"](#) .
3. Copiez l'ARN du rôle IAM afin de pouvoir le coller ultérieurement dans la console.

Résultat

Le compte dispose des autorisations requises. [Vous pouvez désormais ajouter les informations d'identification à un agent de console](#) .

Accorder des autorisations en fournissant des clés AWS

Si vous souhaitez fournir à la console des clés AWS pour un utilisateur IAM, vous devez accorder les autorisations requises à cet utilisateur. La politique IAM de la console définit les actions et ressources AWS que la console est autorisée à utiliser.

Vous devez utiliser cette méthode d'authentification si un agent de console est installé sur site. Vous ne pouvez pas utiliser un rôle IAM.

Étapes

1. Depuis la console IAM, créez des politiques en copiant et en collant le contenu de "[les politiques IAM pour un agent de console](#)".

["Documentation AWS : Création de politiques IAM"](#)

2. Attachez les politiques à un rôle IAM ou à un utilisateur IAM.
 - ["Documentation AWS : Création de rôles IAM"](#)
 - ["Documentation AWS : Ajout et suppression de stratégies IAM"](#)

Ajouter les informations d'identification à un agent existant

Après avoir fourni à un compte AWS les autorisations requises, vous pouvez ajouter les informations d'identification de ce compte à un agent existant. Cela vous permet de lancer des systèmes Cloud Volumes ONTAP dans ce compte à l'aide du même agent.



Les nouvelles informations d'identification de votre fournisseur de cloud peuvent prendre quelques minutes pour être disponibles.

Étapes

1. Utilisez la barre de navigation supérieure pour sélectionner un agent de console auquel vous souhaitez ajouter des informations d'identification.
2. Dans la barre de navigation de gauche, sélectionnez **Administration > Informations d'identification**.
3. Sur la page **Informations d'identification de l'organisation**, sélectionnez **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
 - a. **Emplacement des informations d'identification** : Sélectionnez **Amazon Web Services > Agent**.
 - b. **Définir les informations d'identification** : fournissez l'ARN (Amazon Resource Name) d'un rôle IAM approuvé ou saisissez une clé d'accès AWS et une clé secrète.
 - c. **Abonnement Marketplace** : Associez un abonnement Marketplace à ces informations d'identification en vous abonnant maintenant ou en sélectionnant un abonnement existant.

Pour payer les services à un tarif horaire (PAYGO) ou avec un contrat annuel, vous devez associer les informations d'identification AWS à votre abonnement AWS Marketplace.

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

Résultat

Vous pouvez désormais 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 abonnement à la console.

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

- keys | Account ID: [redacted]
- Instance Profile | Account ID: [redacted]
- casaba QA subscription

+ Add Subscription

Apply Cancel

Ajoutez des informations d'identification à la console pour créer un agent de console

Ajoutez les informations d'identification AWS en fournissant l'ARN d'un rôle IAM qui donne les autorisations nécessaires pour créer un agent de console. Vous pouvez choisir ces informations d'identification lors de la création d'un nouvel agent.

Configurer le rôle IAM

Configurez un rôle IAM qui permet à la couche logicielle en tant que service (SaaS) de la NetApp Console d'assumer le rôle.

Étapes

1. Accédez à la console IAM dans le compte cible.
2. Sous Gestion des accès, sélectionnez **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 de la NetApp Console SaaS : 952013314444
- Pour Amazon FSx for NetApp ONTAP en particulier, modifiez la politique **Relations de confiance** pour inclure « AWS » : « arn:aws:iam::952013314444:root ».

Par exemple, la politique devrait ressembler à ceci :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+

Se référer à ["Documentation AWS Identity and Access Management \(IAM\)"](#) pour plus d'informations sur l'accès aux ressources inter-comptes dans IAM.

- Créez une politique qui inclut les autorisations requises pour créer un agent de console.
 - ["Afficher les autorisations nécessaires pour FSx pour ONTAP"](#)
 - ["Afficher la politique de déploiement de l'agent"](#)

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

Résultat

Le rôle IAM dispose désormais des autorisations requises. [Vous pouvez maintenant l'ajouter à la console.](#)

Ajoutez les informations d'identification

Après avoir fourni au rôle IAM les autorisations requises, ajoutez l'ARN du rôle à la console.

Avant de commencer

Si vous venez de créer le rôle IAM, il faudra peut-être quelques minutes avant qu'il soit disponible pour utilisation. Attendez quelques minutes avant d'ajouter les informations d'identification à la console.

Étapes

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



2. Sur la page **Informations d'identification de l'organisation**, sélectionnez **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
- a. **Emplacement des informations d'identification** : sélectionnez **Amazon Web Services > Console**.
 - b. **Définir les informations d'identification** : indiquez l'ARN (Amazon Resource Name) du rôle IAM.
 - c. **Révision** : Confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Ajouter des informations d'identification à la console pour Amazon FSx for ONTAP

Pour plus de détails, reportez-vous à la ["la documentation de la console pour Amazon FSx pour ONTAP"](#)

Configurer un abonnement AWS

Après avoir ajouté vos informations d'identification AWS, vous pouvez configurer un abonnement AWS Marketplace avec ces informations d'identification. L'abonnement vous permet de payer les services de données NetApp et Cloud Volumes ONTAP à un tarif horaire (PAYGO) ou via un contrat annuel.

Il existe deux scénarios dans lesquels vous pouvez configurer un abonnement AWS Marketplace après avoir ajouté les informations d'identification :

- Vous n'avez pas configuré d'abonnement lorsque vous avez initialement ajouté les informations d'identification.
- Vous souhaitez modifier l'abonnement AWS Marketplace configuré avec les informations d'identification AWS.

Le remplacement de l'abonnement actuel au marché par un nouvel abonnement modifie l'abonnement au marché pour tous les systèmes Cloud Volumes ONTAP existants et tous les nouveaux systèmes.

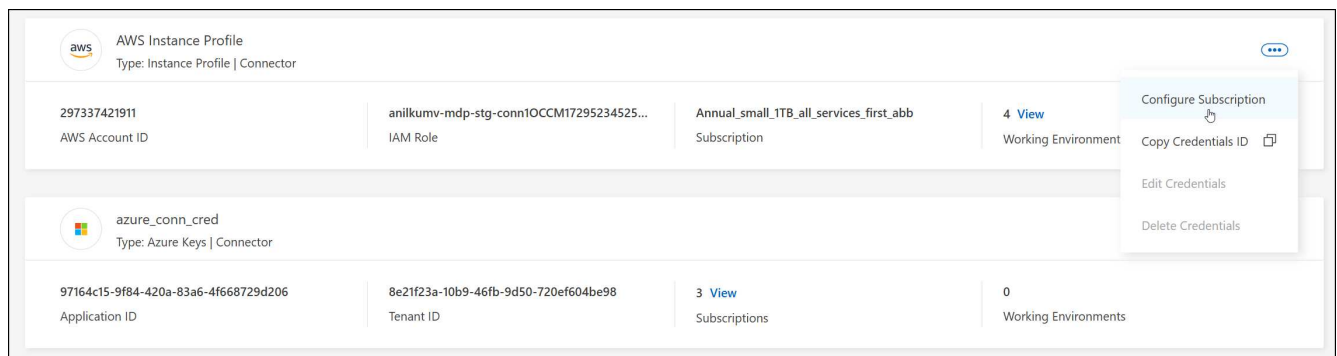
Avant de commencer

Vous devez créer un agent de console avant de pouvoir configurer un abonnement. ["Apprenez à créer un agent de console"](#) .

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 AWS Marketplace :
 - a. Sélectionnez **Afficher les options d'achat**.

- b. Sélectionnez **S'abonner**.
- c. Sélectionnez **Configurer votre compte**.

Vous serez redirigé vers la NetApp Console.

- d. 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**.

Associer un abonnement existant à votre organisation

Lorsque vous vous abonnez à partir d'AWS Marketplace, la dernière étape du processus consiste à associer l'abonnement à votre organisation. Si vous n'avez pas effectué cette étape, vous ne pourrez pas utiliser l'abonnement avec votre organisation.

- ["En savoir plus sur les modes de déploiement de la console"](#)
- ["En savoir plus sur la gestion des identités et des accès à la console"](#)

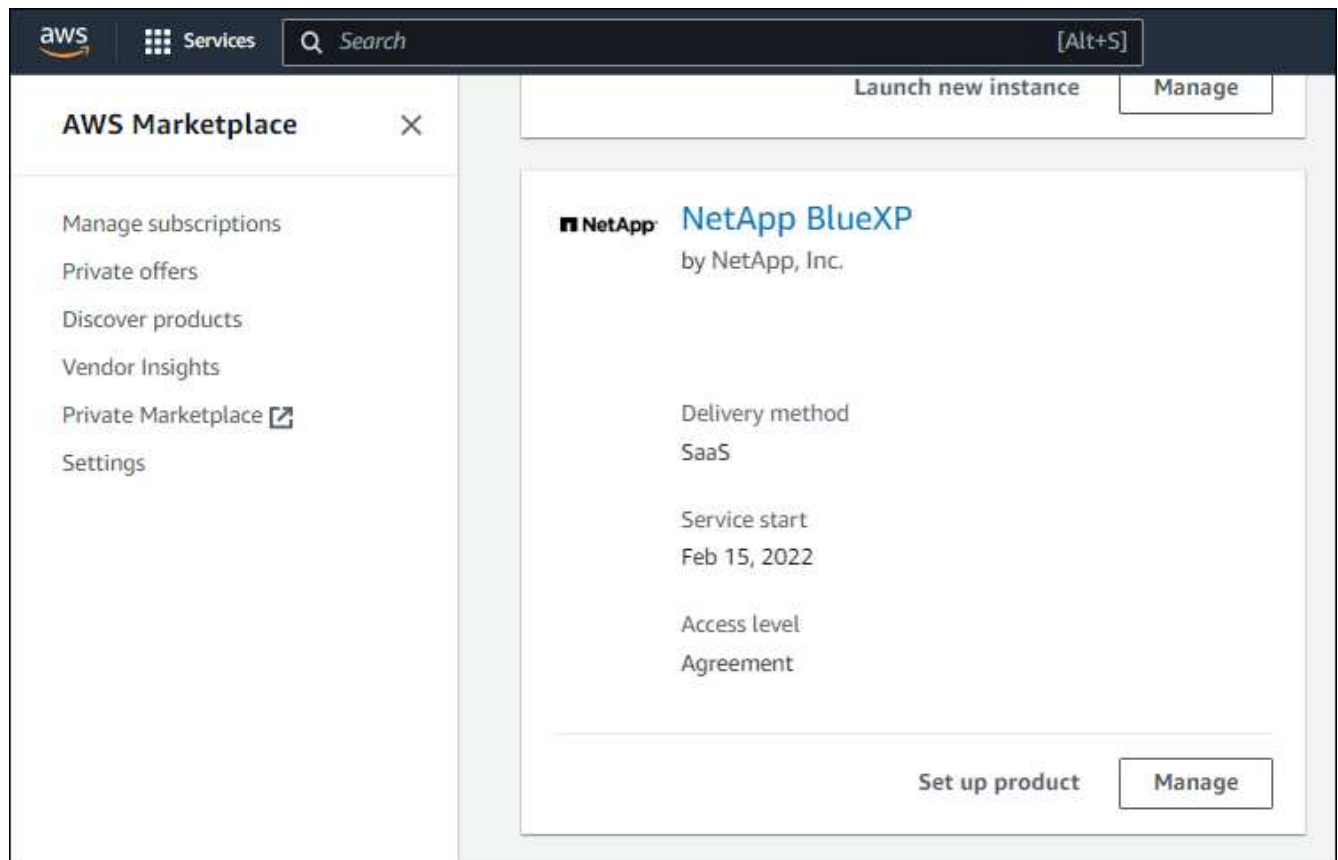
Suivez les étapes ci-dessous si vous vous êtes abonné à NetApp Intelligent Services depuis AWS Marketplace, mais que vous avez manqué l'étape permettant d'associer l'abonnement à votre compte.

Étapes

1. Confirmez que vous n'avez pas associé votre abonnement à votre organisation Console.
 - a. Dans le menu de navigation, sélectionnez **Administration > Licenses and subscriptions**.
 - b. Sélectionnez **Abonnements**.
 - c. Vérifiez que votre abonnement n'apparaît pas.

Vous ne verrez que les abonnements associés à l'organisation ou au compte que vous consultez actuellement. Si vous ne voyez pas votre abonnement, procédez aux étapes suivantes.

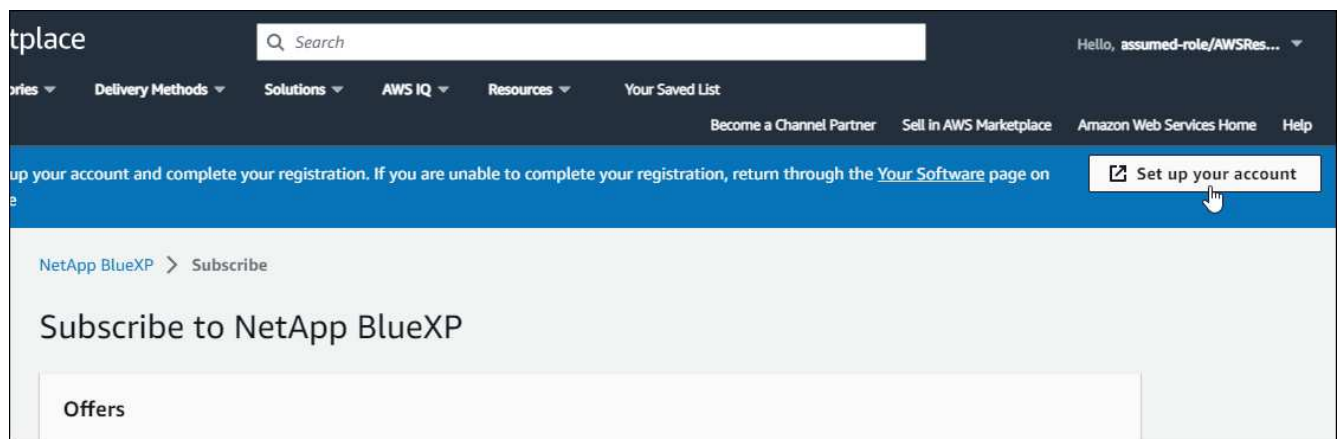
2. Connectez-vous à la console AWS et accédez à **Abonnements AWS Marketplace**.
3. Trouver l'abonnement.



4. Sélectionnez **Configurer le produit**.

La page de l'offre d'abonnement doit se charger dans un nouvel onglet ou une nouvelle fenêtre du navigateur.

5. Sélectionnez **Configurer votre compte**.



La page **Affectation d'abonnement** sur netapp.com doit se charger dans un nouvel onglet ou une nouvelle fenêtre de navigateur.

Notez que vous serez peut-être invité à vous connecter d'abord à la console.

6. 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.

Subscription Assignment [X]

✓ Your subscription to BlueXP / Cloud Volumes ONTAP from the AWS Marketplace was created successfully.

Subscription name ⓘ
PayAsYouGo

Select the NetApp accounts that you'd like to associate this subscription with. ⓘ
You can automatically replace the existing subscription for one account with this new subscription.

NetApp account	Replace existing subscription
<input checked="" type="checkbox"/> cloudTiering_undefined	<input type="checkbox"/>
<input checked="" type="checkbox"/> CS-HhewH	<input type="checkbox"/>
<input checked="" type="checkbox"/> benAccount	<input checked="" type="checkbox"/>

Save

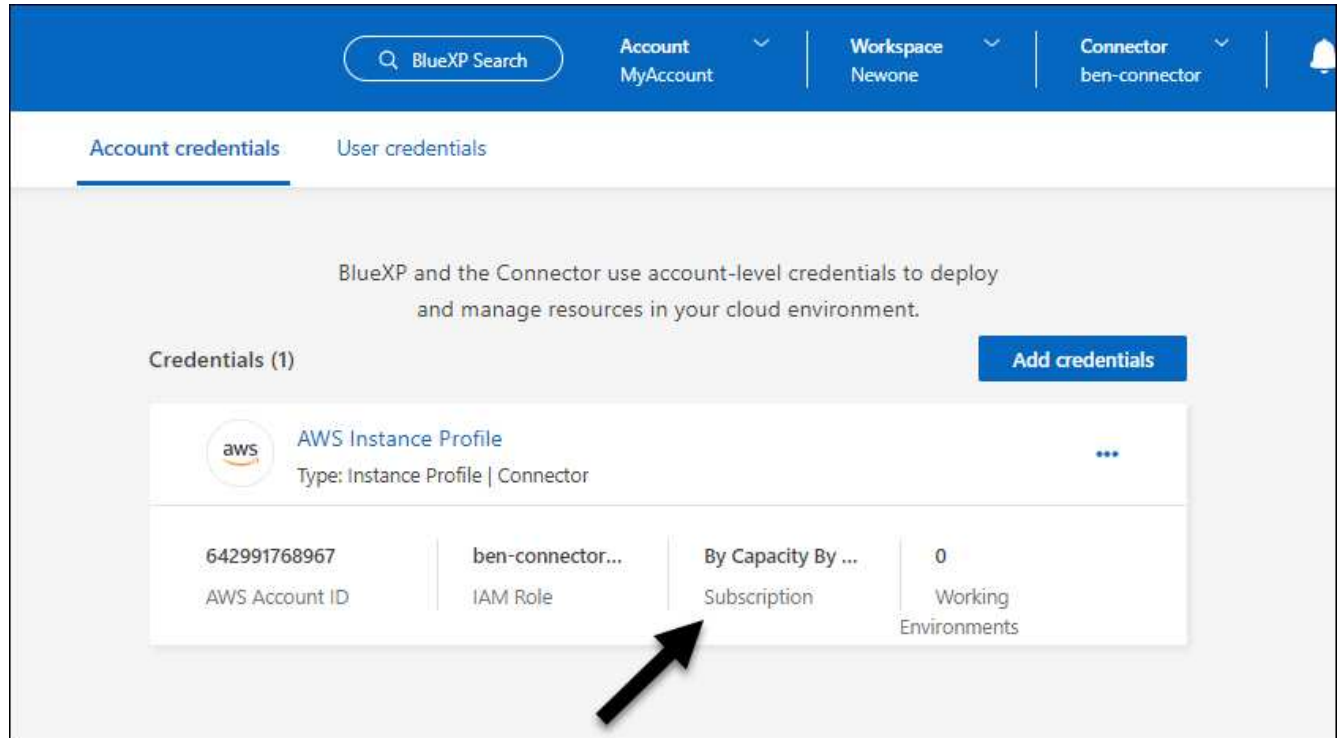
7. Confirmez que l'abonnement est associé à votre organisation.
 - a. Dans le menu de navigation, sélectionnez **Administration > Licences et abonnements**.
 - b. Sélectionnez **Abonnements**.
 - c. Vérifiez que votre abonnement apparaît.

8. Confirmez que l'abonnement est associé à vos informations d'identification AWS.

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

b. Sur la page **Informations d'identification de l'organisation**, vérifiez que l'abonnement est associé à vos informations d'identification AWS.

Voici un exemple.



Modifier les informations d'identification

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



Vous ne pouvez pas modifier les informations d'identification d'un profil d'instance associé à une instance d'agent de console ou à une instance Amazon FSx for ONTAP . Vous ne pouvez renommer les informations d'identification que pour une instance FSx for ONTAP .

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sur la page **Informations d'identification de l'organisation**, sélectionnez le menu d'action pour un ensemble d'informations d'identification, puis sélectionnez **Modifier les informations d'identification**.
3. 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.



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

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sur la page **Informations d'identification de l'organisation** ou **Informations d'identification du compte**, sélectionnez le menu d'action pour un ensemble d'informations d'identification, puis sélectionnez **Supprimer les informations d'identification**.
3. Sélectionnez **Supprimer** pour confirmer.

Azuré

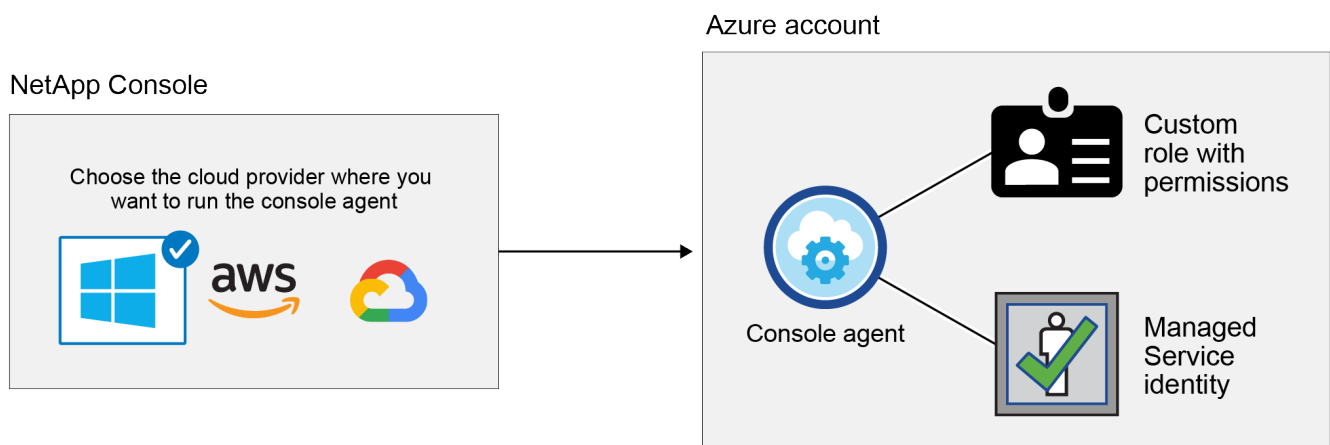
En savoir plus sur les informations d'identification et les autorisations Azure dans la NetApp Console

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 souhaitez 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 :

Details & Credentials			
Managed Service Ide...	OCCM QA1	 <i>No subscription is associated</i>	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

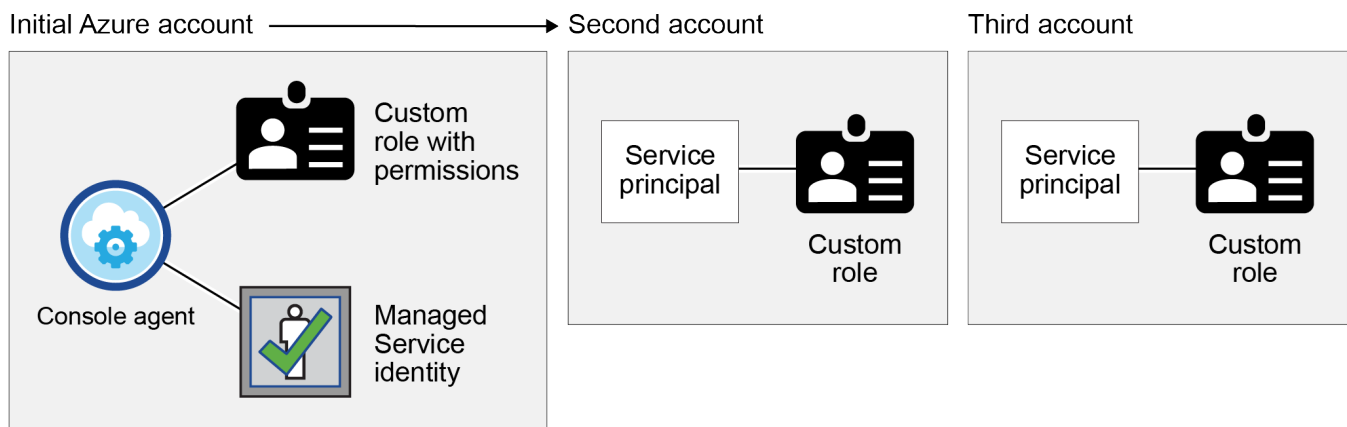
Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des informations d'identification Azure initiales ou ajouter des informations d'identification supplémentaires.

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 :

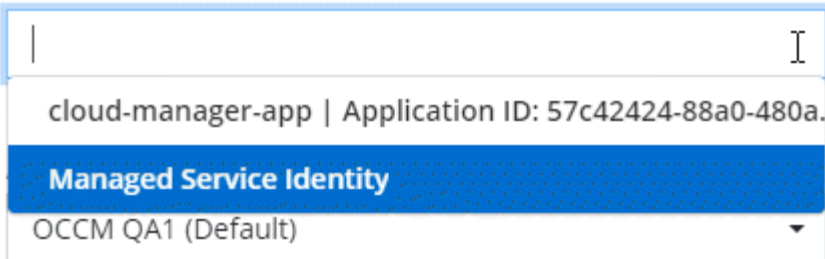


Vous voudriez alors ["ajouter les informations d'identification du compte à la console"](#) en fournissant des détails sur le principal du service AD.

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

Edit Account & Add Subscription

Credentials



cloud-manager-app | Application ID: 57c42424-88a0-480a.

Managed Service Identity

OCCM QA1 (Default)

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**.

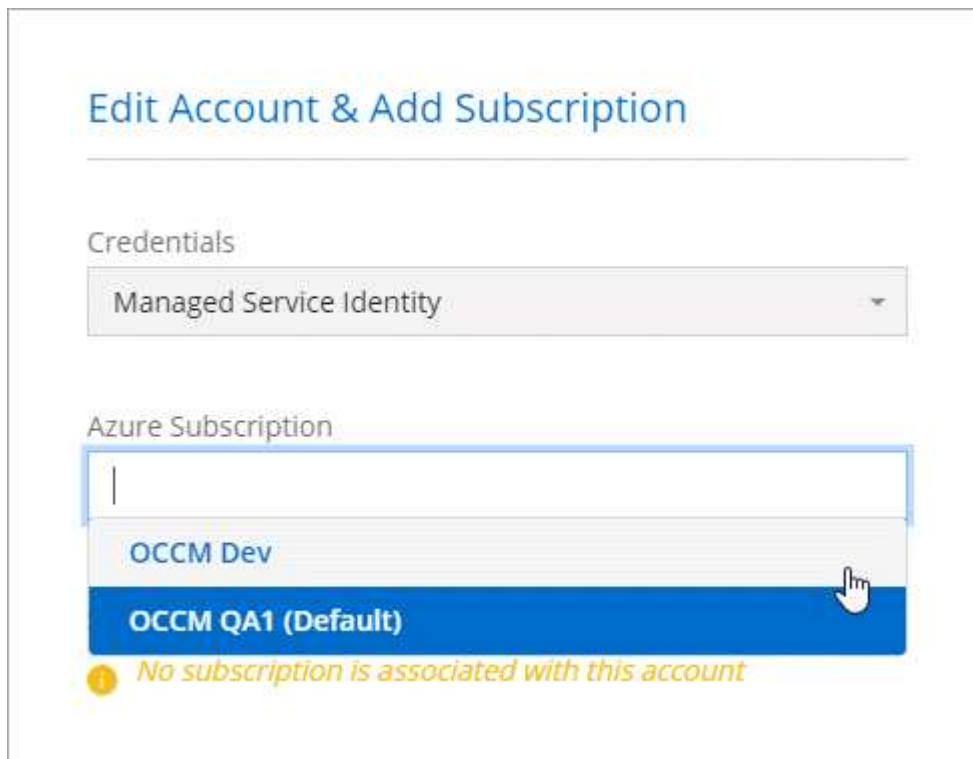


L'opérateur de console est le nom par défaut fourni dans une stratégie d'agent de console. Si vous avez choisi un nom différent pour le rôle, sélectionnez plutôt ce nom.

- 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"](#).

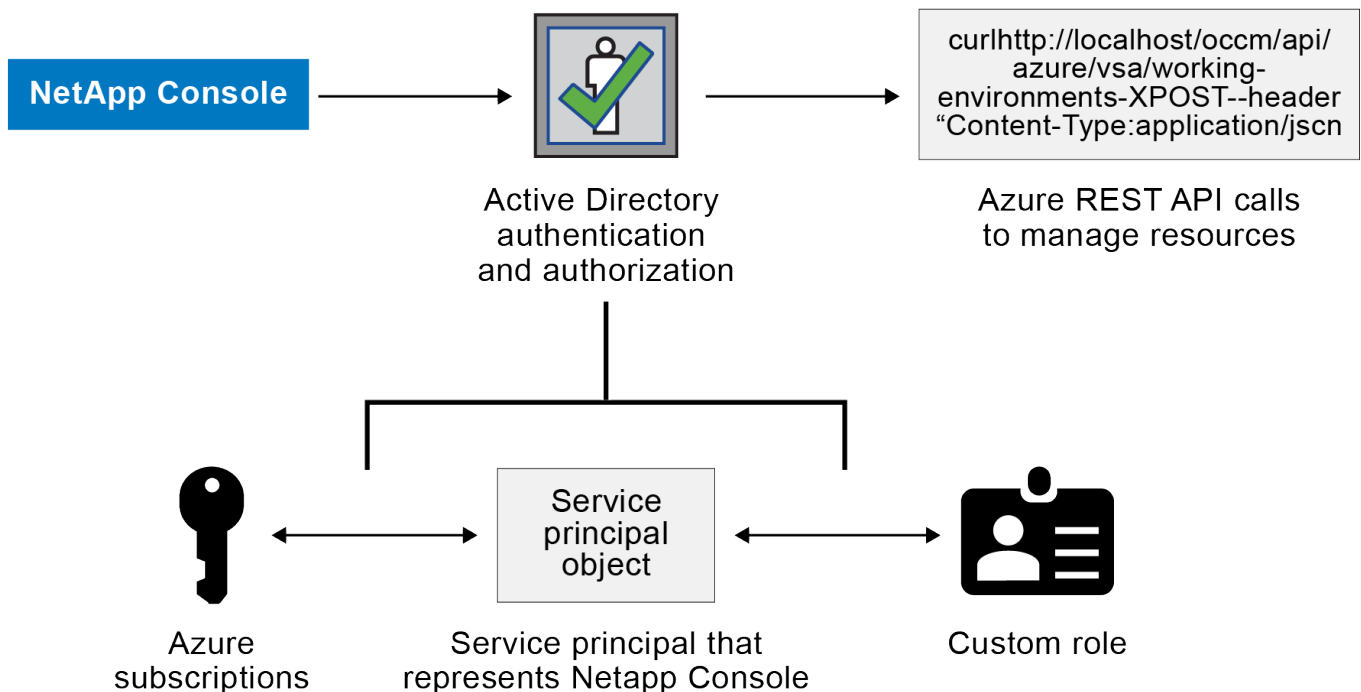
Si vous souhaitez déployer Cloud Volumes ONTAP à l'aide de *différentes* informations d'identification Azure, vous devez accorder les autorisations requises en créant et en configurant un principal de service dans Microsoft Entra ID pour chaque compte Azure. Vous pouvez ensuite ajouter les nouvelles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

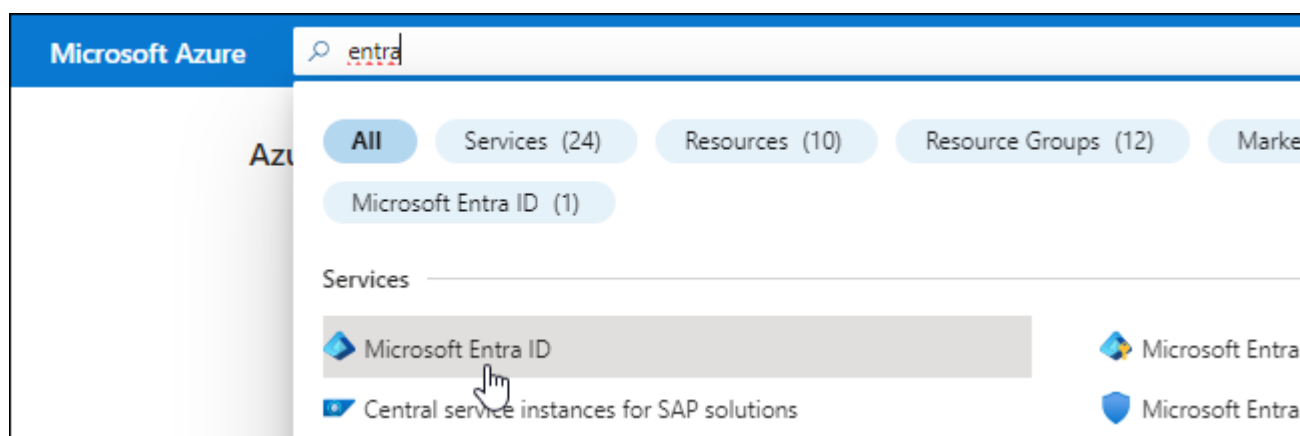
Créez une application Microsoft Entra et un principal de service que la console peut utiliser pour le contrôle d'accès basé sur les rôles.

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"](#)

- Copiez le contenu du ["autorisations de rôle personnalisées pour l'agent de la console"](#) et les enregistrer dans un fichier JSON.
- 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 .

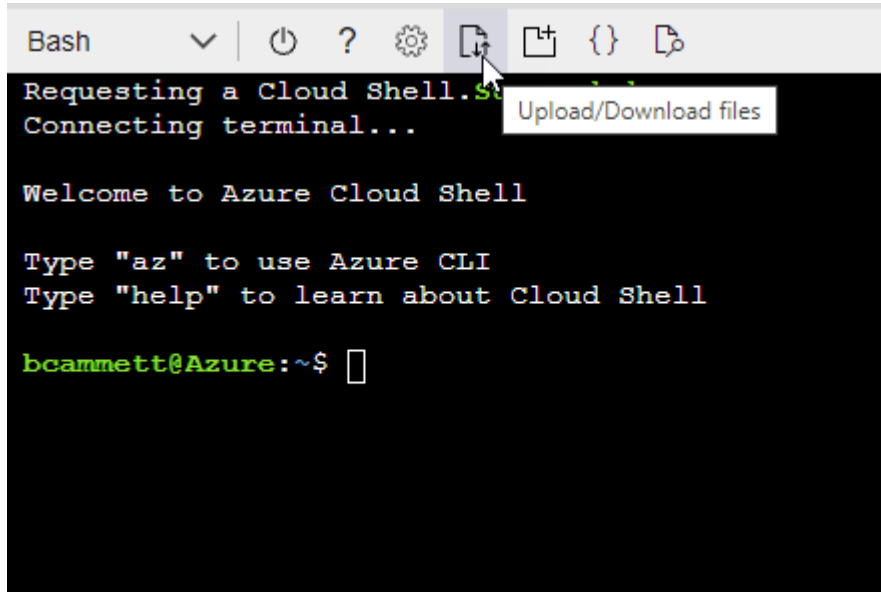
Exemple

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"  
]
```

- 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 :

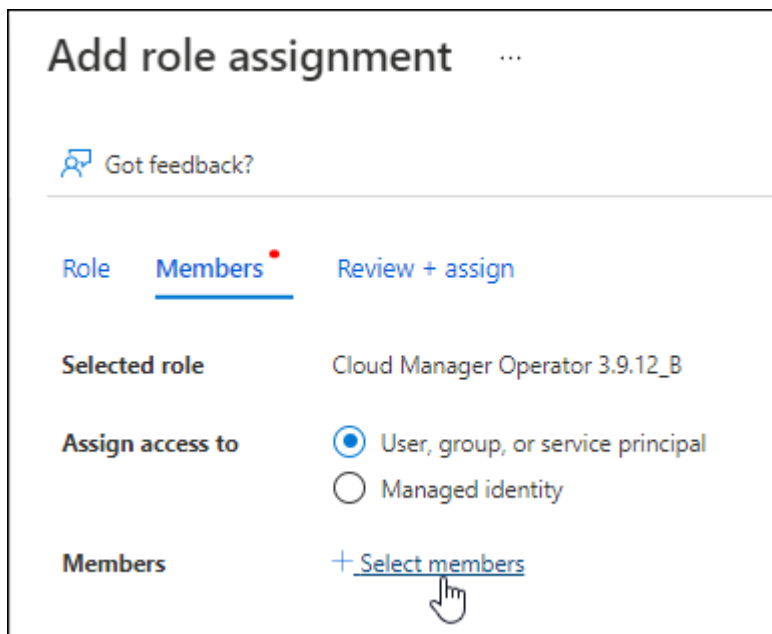
```
az role definition create --role-definition agent_Policy.json
```

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 :

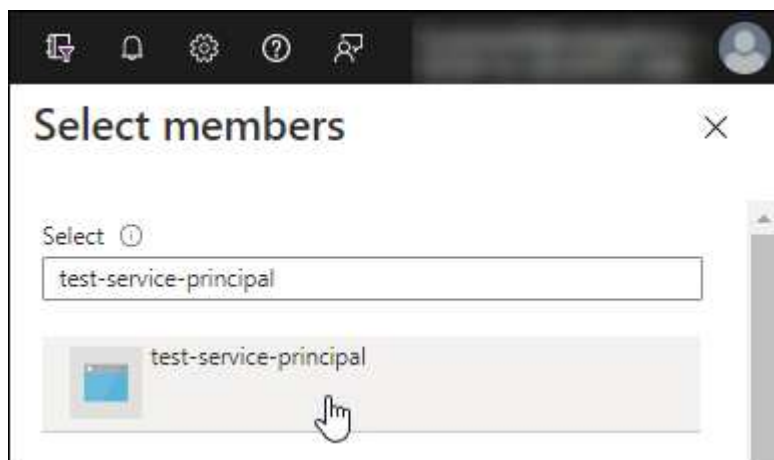
- Depuis le portail Azure, ouvrez le service **Abonnements**.
- Sélectionnez l'abonnement.
- Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.
- Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.
- Dans l'onglet **Membres**, 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**.


Request API permissions


Select an API


[Microsoft APIs](#) [APIs my organization uses](#) [My APIs](#)


Commonly used Microsoft APIs


Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.





**Azure Batch**
Schedule large-scale parallel and HPC applications in the cloud


**Azure Data Catalog**
Programmatic access to Data Catalog resources to register, annotate and search data assets


**Azure Data Explorer**
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions


**Azure Data Lake**
Access to storage and compute for big data analytic scenarios


**Azure DevOps**
Integrate with Azure DevOps and Azure DevOps server


**Azure Import/Export**
Programmatic control of import/export jobs


**Azure Key Vault**
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

**Azure Rights Management Services**
Allow validated users to read and write protected content

**Azure Service Management**
Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

**Customer Insights**
Create profile and interaction models for your products

**Data Export Service for Microsoft Dynamics 365**
Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

< All APIs



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

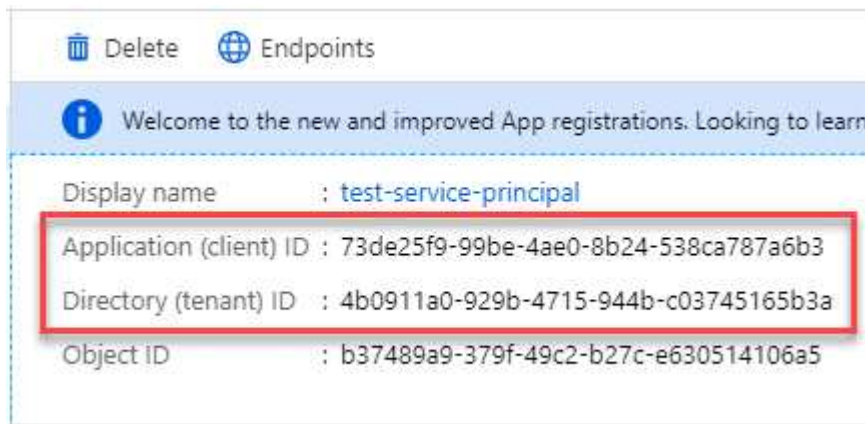
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) ⓘ	-

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA

Copy to clipboard

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"](#).

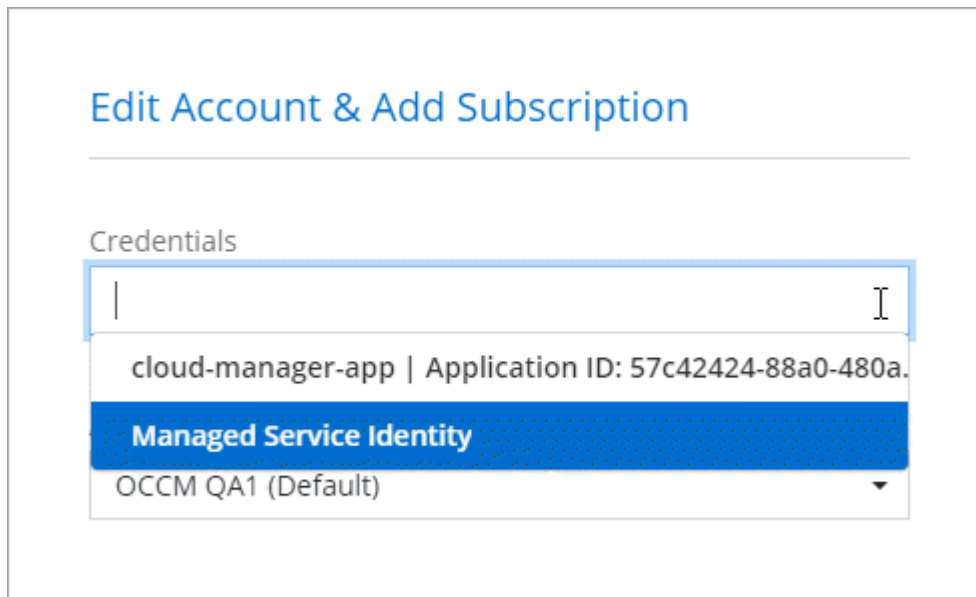
Étapes

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.

Google Cloud

En savoir plus sur les projets et les autorisations Google Cloud

Découvrez comment la NetApp Console utilise les informations d'identification Google Cloud 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 projets Google Cloud. Par exemple, vous souhaitez peut-être en savoir plus sur le compte de service associé à la machine virtuelle de l'agent de console.

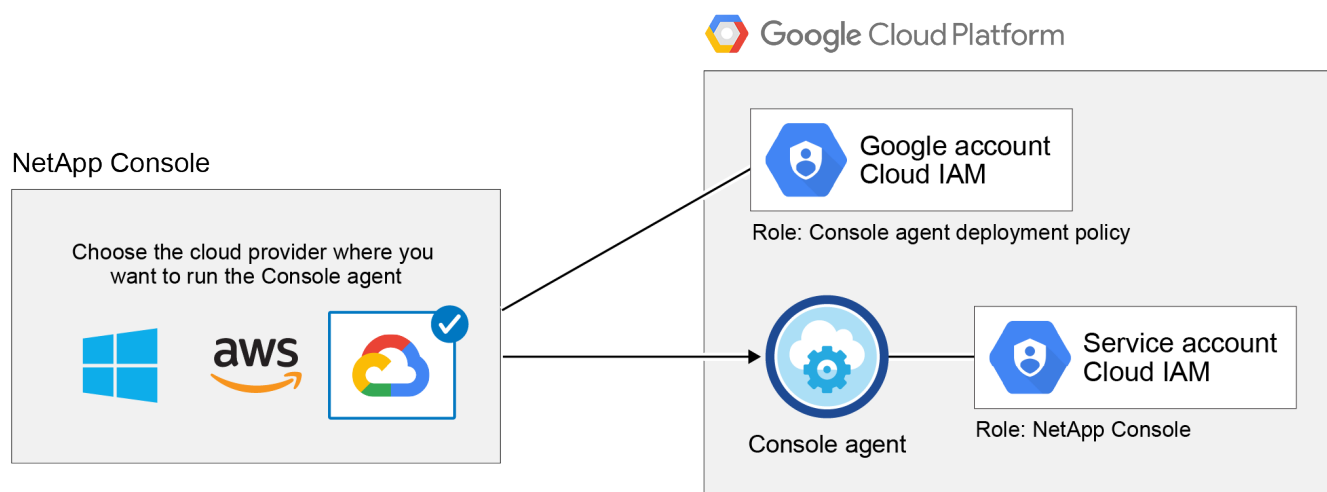
Projet et autorisations pour la NetApp Console

Avant de pouvoir utiliser la console pour gérer les ressources de votre projet Google Cloud, vous devez d'abord déployer un agent de console. L'agent ne peut pas être exécuté dans vos locaux ou chez un autre fournisseur de cloud.

Deux ensembles d'autorisations doivent être en place avant de déployer un agent de console directement à partir de la console :

1. Vous devez déployer un agent de console à l'aide d'un compte Google disposant des autorisations nécessaires pour lancer l'agent de console à partir de la console.
2. Lors du déploiement de l'agent de console, vous êtes invité à sélectionner un **"compte de service"** pour l'agent. La console obtient des autorisations du compte de service pour créer et gérer les systèmes Cloud Volumes ONTAP, pour gérer les sauvegardes à l'aide de la sauvegarde et de la récupération NetApp, et bien plus encore. Les autorisations sont fournies en associant un rôle personnalisé au compte de service.

L'image suivante illustre les exigences d'autorisation décrites aux numéros 1 et 2 ci-dessus :



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

- ["Configurer les autorisations Google Cloud pour le mode standard"](#)
- ["Configurer les autorisations pour le mode restreint"](#)

Informations d'identification et abonnements à la place de marché

Lorsque vous déployez un agent de console dans Google Cloud, la console crée un ensemble d'informations d'identification par défaut pour le compte de service Google Cloud dans le projet dans lequel réside l'agent de console. Ces informations d'identification doivent être associées à un abonnement Google Cloud Marketplace afin que vous puissiez payer les services de données Cloud Volumes ONTAP et NetApp .

["Découvrez comment associer un abonnement Google Cloud Marketplace"](#) .

Notez les points suivants concernant les informations d'identification Google Cloud et les abonnements à la place de marché :

- Un seul ensemble d'informations d'identification Google Cloud peut être associé à un agent de console
- Vous ne pouvez associer qu'un seul abonnement Google Cloud Marketplace aux informations d'identification
- Vous pouvez remplacer un abonnement de marché existant par un nouvel abonnement

Projet pour Cloud Volumes ONTAP

Cloud Volumes ONTAP peut résider dans le même projet que l'agent de la console ou dans un projet différent. Pour déployer Cloud Volumes ONTAP dans un autre projet, vous devez d'abord ajouter le compte de service et le rôle de l'agent de console à ce projet.

- ["Apprenez à configurer le compte de service"](#)
- ["Découvrez comment déployer Cloud Volumes ONTAP dans Google Cloud et sélectionner un projet"](#)

Gestion des autorisations de l'agent de la console pour les déploiements Google Cloud

Il arrive que NetApp mette à jour les autorisations requises pour le compte de service utilisé par l'agent Console lorsqu'il est déployé sur Google Cloud.

["Vérifiez la liste des autorisations Google requises"](#).

Utilisez la console Google Cloud pour mettre à jour le rôle IAM attribué au compte de service afin qu'il corresponde au nouvel ensemble d'autorisations.

["Documentation Google Cloud : Modifier un rôle personnalisé"](#)

Gérer les informations d'identification NSS associées à la NetApp Console

Associez un compte de site de support NetApp à votre organisation de console pour activer les flux de travail clés pour la gestion du stockage. Ces informations d'identification NSS sont associées à l'ensemble de l'organisation.

La console prend également en charge l'association d'un compte NSS par compte utilisateur. ["Apprenez à](#)

Aperçu

L'association des informations d'identification du site de support NetApp à votre numéro de série de compte de console spécifique est requise pour activer les tâches suivantes :

- Déploiement de Cloud Volumes ONTAP lorsque vous apportez votre propre licence (BYOL)

Il est nécessaire de fournir votre compte NSS pour que la console puisse télécharger votre clé de licence et activer l'abonnement pour la durée que vous avez achetée. Cela inclut les mises à jour automatiques pour les renouvellements de mandat.

- Enregistrement des systèmes Cloud Volumes ONTAP à paiement à l'utilisation

Fournir votre compte NSS est nécessaire pour activer le support de votre système et pour accéder aux ressources de support technique NetApp .

- Mise à niveau du logiciel Cloud Volumes ONTAP vers la dernière version

Ces informations d'identification sont associées au numéro de série de votre compte de console spécifique. Les utilisateurs peuvent accéder à ces informations d'identification depuis **Support > Gestion NSS**.

Ajouter un compte NSS

Vous pouvez ajouter et gérer vos comptes de site de support NetApp à utiliser avec la console à partir du tableau de bord de support dans la console.

Une fois que vous avez ajouté votre compte NSS, la console utilise ces informations pour des tâches telles que les téléchargements de licences, la vérification des mises à niveau logicielles et les futures inscriptions au support.

Vous pouvez associer plusieurs comptes NSS à votre organisation ; cependant, vous ne pouvez pas avoir de comptes clients et de comptes partenaires au sein de la même organisation.



NetApp utilise Microsoft Entra ID comme fournisseur d'identité pour les services d'authentification spécifiques au support et aux licences.

Étapes

1. Dans **Administration > Support**.
2. Sélectionnez **Gestion NSS**.
3. Sélectionnez **Ajouter un compte NSS**.
4. Sélectionnez **Continuer** pour être redirigé vers une page de connexion Microsoft.
5. Sur la page de connexion, indiquez votre adresse e-mail et votre mot de passe enregistrés sur le site de support NetApp .

Une fois la connexion réussie, NetApp stockera le nom d'utilisateur NSS.

Il s'agit d'un identifiant généré par le système qui correspond à votre e-mail. Sur la page **Gestion NSS**, vous pouvez afficher votre e-mail à partir du **...** menu.

- Si vous avez besoin d'actualiser vos jetons d'identification de connexion, il existe également une option

Mettre à jour les informations d'identification dans le **☰** menu.

L'utilisation de cette option vous invite à vous reconnecter. Notez que le jeton de ces comptes expire après 90 jours. Une notification sera publiée pour vous en informer.

Quelle est la prochaine étape ?

Les utilisateurs peuvent désormais sélectionner le compte lors de la création de nouveaux systèmes Cloud Volumes ONTAP et lors de l'enregistrement de systèmes Cloud Volumes ONTAP existants.

- ["Lancement de Cloud Volumes ONTAP dans AWS"](#)
- ["Lancement de Cloud Volumes ONTAP dans Azure"](#)
- ["Lancement de Cloud Volumes ONTAP dans Google Cloud"](#)
- ["Enregistrement des systèmes de paiement à l'utilisation"](#)

Mettre à jour les informations d'identification NSS

Pour des raisons de sécurité, vous devez mettre à jour vos informations d'identification NSS tous les 90 jours. Vous serez averti dans le centre de notifications de la console si vos informations d'identification NSS ont expiré. ["En savoir plus sur le centre de notifications"](#) .

Les informations d'identification expirées peuvent perturber les éléments suivants, sans toutefois s'y limiter :

- Mises à jour de licence, ce qui signifie que vous ne pourrez pas profiter de la capacité nouvellement achetée.
- Possibilité de soumettre et de suivre les cas d'assistance.

De plus, vous pouvez mettre à jour les informations d'identification NSS associées à votre organisation si vous souhaitez modifier le compte NSS associé à votre organisation. Par exemple, si la personne associée à votre compte NSS a quitté votre entreprise.

Étapes

1. Dans **Administration > Support**.
2. Sélectionnez **Gestion NSS**.
3. Pour le compte NSS que vous souhaitez mettre à jour, sélectionnez **☰** puis sélectionnez **Mettre à jour les informations d'identification**.
4. Lorsque vous y êtes invité, sélectionnez **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Entra ID comme fournisseur d'identité pour les services d'authentification liés au support et aux licences.

5. Sur la page de connexion, indiquez votre adresse e-mail et votre mot de passe enregistrés sur le site de support NetApp .

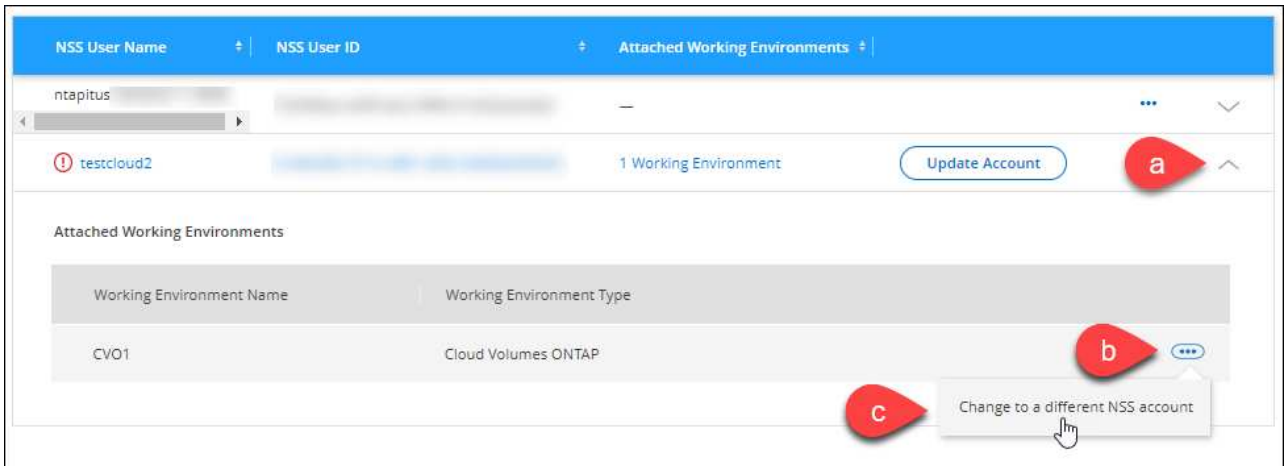
Attacher un système à un autre compte NSS

Si votre organisation dispose de plusieurs comptes de site de support NetApp , vous pouvez modifier le compte associé à un système Cloud Volumes ONTAP .

Vous devez d'abord avoir associé le compte à la Console.

Étapes

1. Dans **Administration > Support**.
2. Sélectionnez **Gestion NSS**.
3. Suivez les étapes suivantes pour modifier le compte NSS :
 - a. Développez la ligne du compte du site de support NetApp auquel le système est actuellement associé.
 - b. Pour le système pour lequel vous souhaitez modifier l'association, sélectionnez **...**
 - c. Sélectionnez **Changer de compte NSS**.



- d. Sélectionnez le compte puis sélectionnez **Enregistrer**.

Afficher l'adresse e-mail d'un compte NSS

Pour des raisons de sécurité, l'adresse e-mail associée à un compte NSS n'est pas affichée par défaut. Vous pouvez afficher l'adresse e-mail et le nom d'utilisateur associé à un compte NSS.



Lorsque vous accédez à la page de gestion NSS, la console génère un jeton pour chaque compte du tableau. Ce jeton inclut des informations sur l'adresse e-mail associée. Le jeton est supprimé lorsque vous quittez la page. Les informations ne sont jamais mises en cache, ce qui contribue à protéger votre vie privée.

Étapes

1. Dans **Administration > Support**.
2. Sélectionnez **Gestion NSS**.
3. Pour le compte NSS que vous souhaitez mettre à jour, sélectionnez **...** puis sélectionnez **Afficher l'adresse e-mail**. Vous pouvez utiliser le bouton Copier pour copier l'adresse e-mail.

Supprimer un compte NSS

Supprimez tous les comptes NSS que vous ne souhaitez plus utiliser avec la console.

Vous ne pouvez pas supprimer un compte actuellement associé à un système Cloud Volumes ONTAP . Vous devez d'abord [attacher ces systèmes à un autre compte NSS](#) .

Étapes

1. Dans **Administration > Support**.

2. Sélectionnez **Gestion NSS**.
3. Pour le compte NSS que vous souhaitez supprimer, sélectionnez **...** puis sélectionnez **Supprimer**.
4. Sélectionnez **Supprimer** pour confirmer.

Gérer les informations d'identification associées à votre connexion à la NetApp Console

Selon les actions que vous avez effectuées dans la console, vous avez peut-être associé les informations d'identification ONTAP et les informations d'identification du site de support NetApp (NSS) à votre connexion utilisateur. Vous pouvez afficher et gérer ces informations d'identification après les avoir associées. Par exemple, si vous modifiez le mot de passe de ces informations d'identification, vous devrez mettre à jour le mot de passe dans la console.

Informations d'identification ONTAP

Les utilisateurs ont besoin des informations d'identification d'administrateur ONTAP pour découvrir les clusters ONTAP dans la console. Cependant, l'accès à ONTAP System Manager dépend de l'utilisation ou non d'un agent de console.

Sans agent de console

Les utilisateurs sont invités à saisir leurs informations d'identification ONTAP pour accéder à ONTAP System Manager pour le cluster. Les utilisateurs peuvent choisir d'enregistrer ces informations d'identification dans la console, ce qui signifie qu'ils ne seront pas invités à les saisir à chaque fois. Les informations d'identification de l'utilisateur ne sont visibles que par l'utilisateur concerné et peuvent être gérées à partir de la page Informations d'identification de l'utilisateur.

Avec un agent de console

Par défaut, les utilisateurs ne sont pas invités à saisir leurs informations d'identification ONTAP pour accéder à ONTAP System Manager. Cependant, un administrateur de console (avec le rôle d'administrateur d'organisation) peut configurer la console pour inviter les utilisateurs à saisir leurs informations d'identification ONTAP. Lorsque ce paramètre est activé, les utilisateurs doivent saisir leurs informations d'identification ONTAP à chaque fois.

["Apprendre encore plus."](#)

Informations d'identification NSS

Les informations d'identification NSS associées à votre connexion à la NetApp Console permettent l'enregistrement du support, la gestion des cas et l'accès à Digital Advisor.

- Lorsque vous accédez à **Support > Ressources** et que vous vous inscrivez à l'assistance, vous êtes invité à associer les informations d'identification NSS à votre connexion.

Cela enregistre votre organisation ou votre compte pour l'assistance et active le droit à l'assistance. Un seul utilisateur de votre organisation doit associer un compte de site de support NetApp à sa connexion pour s'inscrire au support et activer le droit au support. Une fois cette opération terminée, la page **Ressources** indique que votre compte est enregistré pour l'assistance.

["Apprenez comment vous inscrire pour bénéficier de l'assistance"](#)

- Lorsque vous accédez à **Administration > Support > Gestion des cas**, vous êtes invité à saisir vos informations d'identification NSS, si vous ne l'avez pas déjà fait. Cette page vous permet de créer et de gérer les cas d'assistance associés à votre compte NSS et à votre entreprise.
- Lorsque vous accédez à Digital Advisor dans la console, vous êtes invité à vous connecter à Digital Advisor en saisissant vos informations d'identification NSS.

Notez les points suivants concernant le compte NSS associé à votre connexion :

- Le compte est géré au niveau de l'utilisateur, ce qui signifie qu'il n'est pas visible par les autres utilisateurs qui se connectent.
- Il ne peut y avoir qu'un seul compte NSS associé à Digital Advisor et à la gestion des cas d'assistance, par utilisateur.
- Si vous essayez d'associer un compte de site de support NetApp à un système Cloud Volumes ONTAP , vous ne pouvez choisir que parmi les comptes NSS qui ont été ajoutés à l'organisation dont vous êtes membre.

Les informations d'identification au niveau du compte NSS sont différentes du compte NSS associé à votre connexion. Les informations d'identification au niveau du compte NSS vous permettent de déployer Cloud Volumes ONTAP avec BYOL, d'enregistrer les systèmes PAYGO et de mettre à niveau son logiciel.

["En savoir plus sur l'utilisation des informations d'identification NSS avec votre organisation ou votre compte NetApp Console"](#) .

Gérez vos identifiants d'utilisateur

Gérez vos informations d'identification utilisateur en mettant à jour le nom d'utilisateur et le mot de passe ou en supprimant les informations d'identification.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'utilisateur**.
3. Si vous ne disposez pas encore d'informations d'identification utilisateur, vous pouvez sélectionner **Ajouter des informations d'identification NSS** pour ajouter votre compte de site de support NetApp .
4. Gérez les informations d'identification existantes en choisissant les options suivantes dans le menu Actions :
 - **Mettre à jour les informations d'identification** : Mettez à jour le nom d'utilisateur et le mot de passe du compte.
 - **Supprimer les informations d'identification** : supprimez le compte NSS associé à votre connexion à la console.

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.