



# Gérer les identifiants

## Cloud Manager 3.8

NetApp  
March 25, 2024

# Sommaire

- Gérer les identifiants ..... 1
  - AWS ..... 1
  - Azure ..... 8
  - GCP ..... 19
- Ajout de comptes du site de support NetApp à Cloud Manager ..... 24

# Gérer les identifiants

## AWS

### Identifiants et autorisations AWS

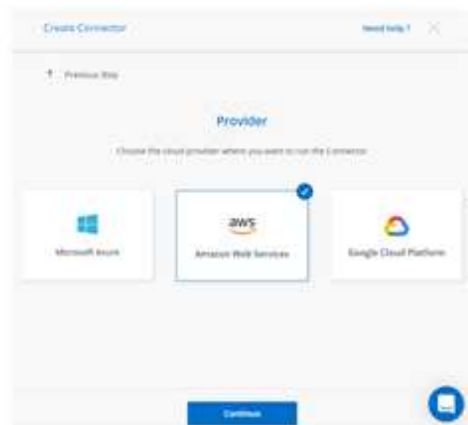
Cloud Manager vous permet de choisir les identifiants AWS à utiliser lors du déploiement de Cloud Volumes ONTAP. Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des identifiants AWS initiaux, ou ajouter des identifiants supplémentaires.

#### Identifiants AWS initiaux

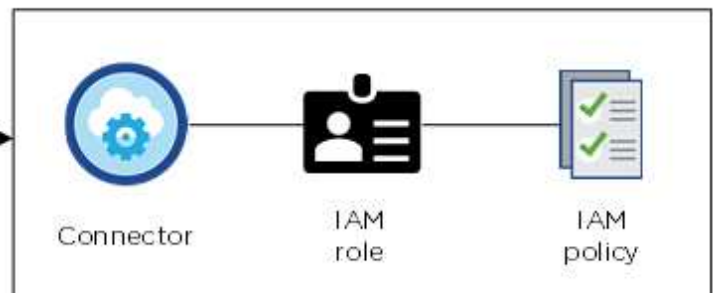
Lorsque vous déployez un connecteur depuis Cloud Manager, vous devez utiliser un compte AWS avec des autorisations pour lancer l'instance de connecteur. Les autorisations requises sont répertoriées dans le ["Règle de déploiement du connecteur pour AWS"](#).

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



AWS account



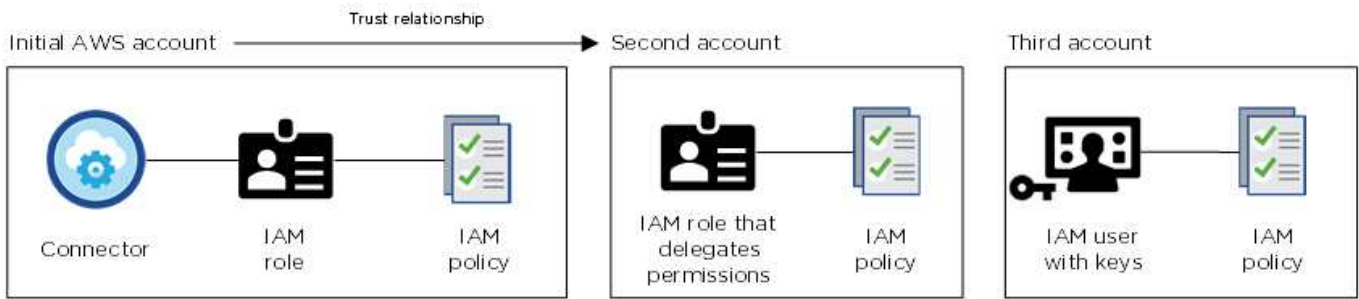
Cloud Manager sélectionne ces identifiants AWS par défaut lorsque vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP :

Details & Credentials			
Instance Profile		QA Subscription	<a href="#">Edit Credentials</a>
Credentials	Account ID	Marketplace Subscription	

#### 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 :

**Edit Account & Add Subscription**

Credentials

- Keys | Account ID: [redacted]
- Instance Profile | Account ID: [redacted]**
- QA Subscription

**Associate Subscription to Credentials**

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

**+ Add Subscription**

**Apply** **Cancel**

## 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 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.

## 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"](#).

## Create role



### Select type of trusted entity

 <b>AWS service</b> EC2, Lambda and others	 <b>Another AWS account</b> Belonging to you or 3rd party	 <b>Web identity</b> Cognito or any OpenID provider	 <b>SAML 2.0 federation</b> Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

### Specify accounts that can use this role

Account ID\*  ⓘ

- Options**
- Require external ID (Best practice when a third party will assume this role)
  - Require MFA ⓘ

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 :



## Edit Account & Add Subscription

### Credentials

Keys   Account ID: [redacted]
<b>Instance Profile   Account ID: [redacted]</b>
QA Subscription

### Associate Subscription to Credentials

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

[+ Add Subscription](#)

Apply

Cancel

### 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 :

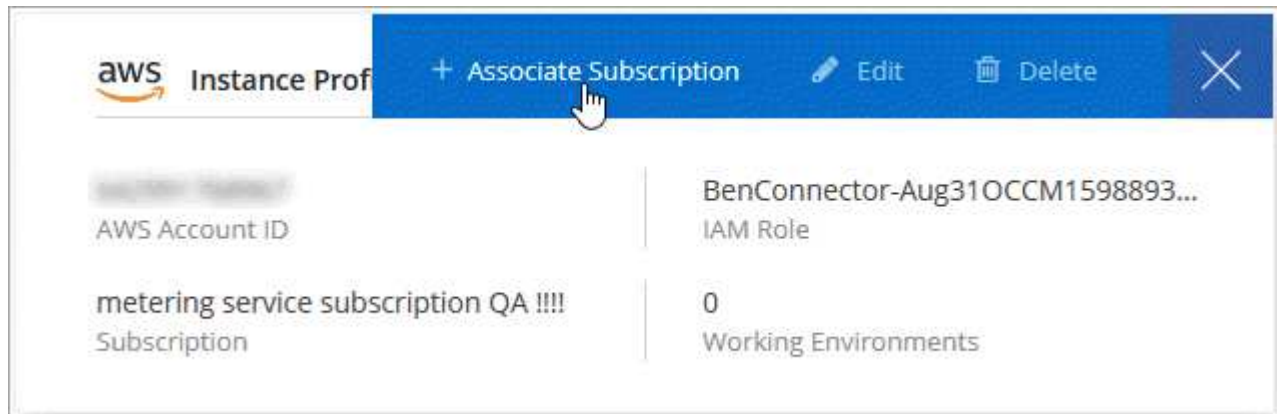
- Vous n'avez pas associé un abonnement lors de l'ajout initial des identifiants à Cloud Manager.
- Vous souhaitez remplacer un abonnement AWS Marketplace existant par un nouvel abonnement.

### 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](https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_aws.mp4) (video)

## Azure

### Identifiants et autorisations Azure

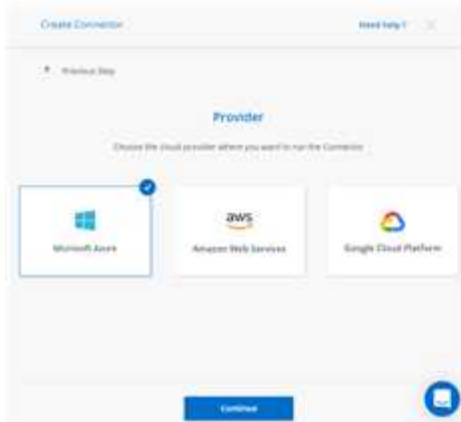
Cloud Manager vous permet de choisir les identifiants Azure à utiliser lors du déploiement de Cloud Volumes ONTAP. Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des identifiants Azure initiaux, ou ajouter des identifiants supplémentaires.

#### Les identifiants initiaux d'Azure

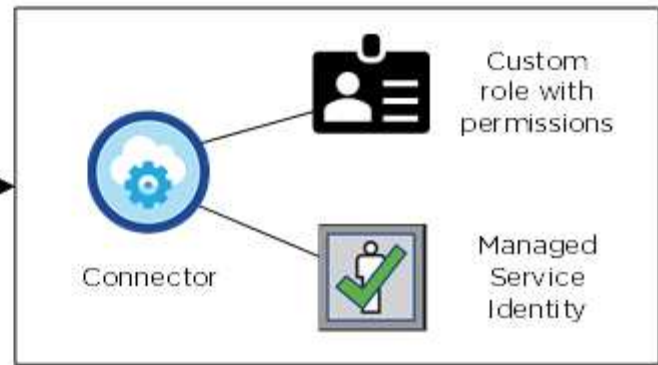
Lorsque vous déployez un connecteur depuis Cloud Manager, vous devez utiliser un compte Azure avec les autorisations de déployer la machine virtuelle Connector. Les autorisations requises sont répertoriées dans le "[Stratégie de déploiement de Connector pour Azure](#)".

Lorsque Cloud Manager déploie la machine virtuelle de connecteur dans Azure, il active une "[identité gérée attribuée par le système](#)" sur une machine virtuelle, crée un rôle personnalisé et le attribue à la machine virtuelle. Le rôle fournit à Cloud Manager des autorisations de gestion des ressources et des processus au sein de cet abonnement Azure. "[Examinez comment Cloud Manager utilise les autorisations](#)".

## Cloud Manager



## Azure account



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

Details & Credentials			
Managed Service Ide...	OCCM QA1	<span style="color: orange;">ⓘ No subscription is associated</span>	<a href="#">Edit Credentials</a>
Credential Name	Azure Subscription	Marketplace Subscription	

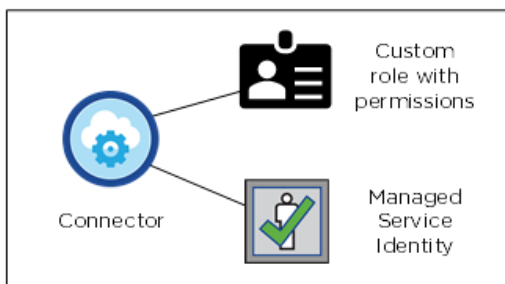
## Des abonnements Azure supplémentaires pour une identité gérée

L'identité gérée est associée à l'abonnement dans lequel vous avez lancé le connecteur. Si vous souhaitez sélectionner un autre abonnement Azure, vous devez le faire "[associez l'identité gérée à ces abonnements](#)".

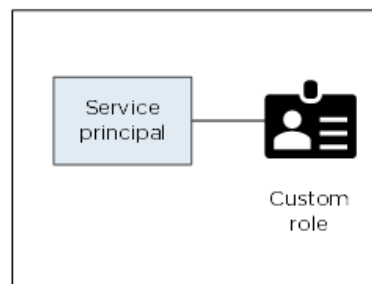
## Autres identifiants Azure

Si vous souhaitez déployer Cloud Volumes ONTAP avec différents identifiants Azure, vous devez accorder les autorisations requises par "[Création et configuration d'une entité de service dans Azure Active Directory](#)". Pour chaque compte Azure. L'image suivante montre deux comptes supplémentaires, chacun étant doté d'un rôle principal de service et personnalisé qui fournit des autorisations :

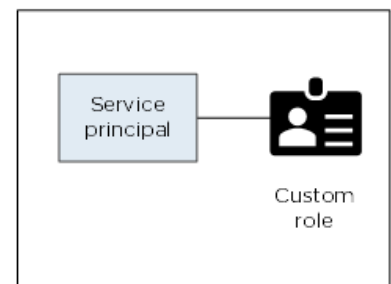
Initial Azure account



Second account



Third account



Vous le feriez alors "[Ajoutez les identifiants du compte à Cloud Manager](#)" En fournissant des détails sur le principal du service AD.

Après avoir ajouté un autre ensemble d'informations d'identification, vous pouvez les passer lors de la création d'un nouvel environnement de travail :

## Edit Account & Add Subscription

### Credentials

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

**Managed Service Identity**

OCCM QA1 (Default) ▼

### 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 NetApp Cloud Central. Vous pouvez également déployer un connecteur dans Azure à partir du "[Azure Marketplace](#)", et vous 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 l'identité gérée pour le connecteur, puis de fournir des autorisations pour tous les comptes supplémentaires.

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

## Gestion des identifiants Azure et des abonnements pour Cloud Manager

Lorsque vous créez un système Cloud Volumes ONTAP, vous devez sélectionner les identifiants Azure et l'abonnement Marketplace pour les utiliser avec ce système. Si vous gérez plusieurs abonnements Azure Marketplace, vous pouvez les attribuer à différentes informations d'identification Azure à partir de la page informations d'identification.

Il existe deux façons de gérer les identifiants Azure dans Cloud Manager. Tout d'abord, si vous souhaitez déployer Cloud Volumes ONTAP sur différents comptes Azure, vous devez fournir les autorisations requises et ajouter les identifiants à Cloud Manager. La deuxième méthode consiste à associer des abonnements supplémentaires à l'identité gérée Azure.



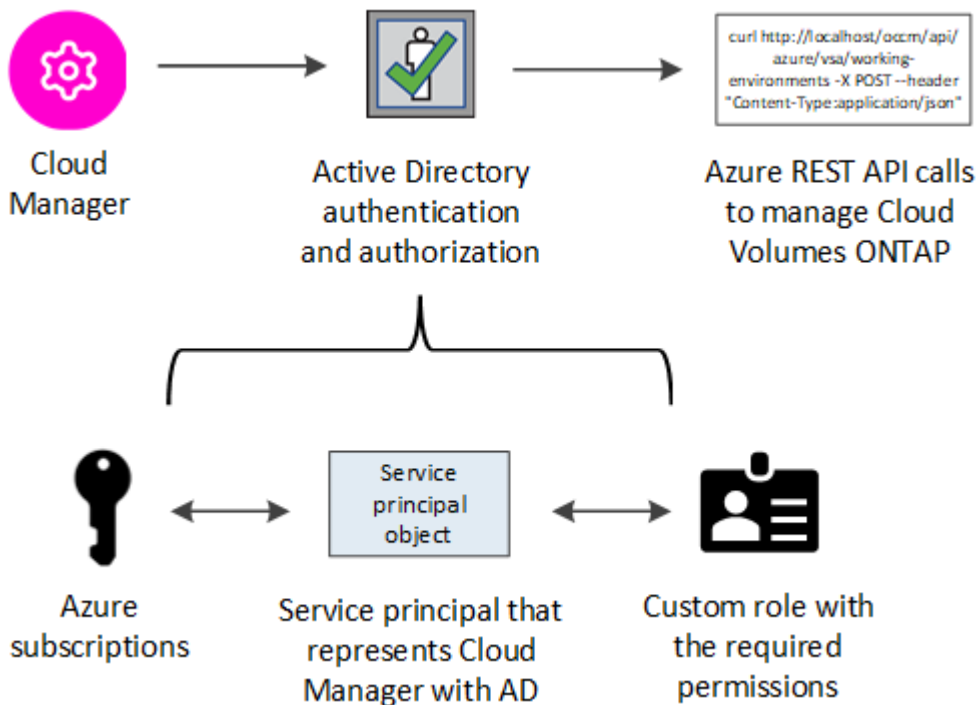
Lorsque vous déployez un connecteur depuis Cloud Manager, Cloud Manager ajoute automatiquement le compte Azure dans lequel vous avez déployé le connecteur. Un compte initial n'est pas ajouté si vous avez installé manuellement le logiciel Connector sur un système existant. "[En savoir plus sur les comptes et les autorisations Azure](#)".

## Octroi d'autorisations Azure à l'aide d'une entité de sécurité de service

Cloud Manager 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 une entité de sécurité de service dans Azure Active Directory et en obtenant les informations d'identification Azure requises par Cloud Manager.

### Description de la tâche

L'image suivante illustre comment Cloud Manager obtient les autorisations nécessaires pour effectuer des opérations dans Azure. Un objet principal de service, lié à un ou plusieurs abonnements Azure, représente Cloud Manager dans Azure Active Directory et est affecté à un rôle personnalisé qui permet les autorisations requises.



### Étapes

1. [Créez une application Azure Active Directory.](#)
2. [Attribuez l'application à un rôle.](#)
3. [Ajoutez des autorisations d'API de gestion de service Windows Azure.](#)
4. [Obtenir l'ID de l'application et l'ID du répertoire.](#)
5. [Créez un secret client.](#)

### Création d'une application Azure Active Directory

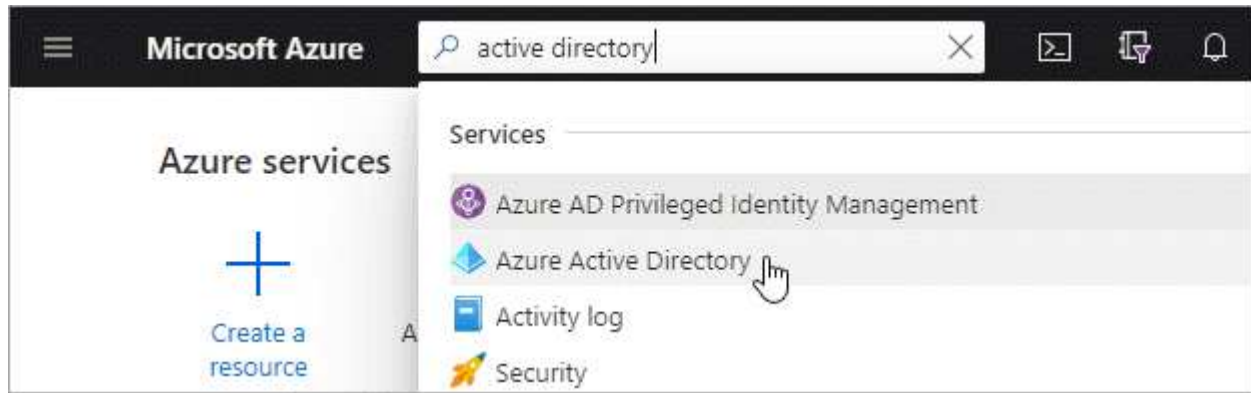
Créez une application Azure Active Directory (AD) et une entité de service que Cloud Manager peut utiliser pour le contrôle d'accès basé sur des rôles.

### Avant de commencer

Vous devez disposer des droits d'accès 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](#)".

### Étapes

1. À partir du portail Azure, ouvrez le service **Azure Active Directory**.



2. Dans le menu, cliquez sur **enregistrements d'applications**.

3. Cliquez sur **Nouvelle inscription**.

4. Spécifiez les détails de l'application :

- **Nom** : saisissez un nom pour l'application.
- **Type de compte** : sélectionnez un type de compte (tout fonctionne avec Cloud Manager).
- **Redirect URI** : sélectionnez **Web**, puis entrez n'importe quelle URL, par exemple, <https://url>

5. Cliquez sur **Enregistrer**.

## Résultat

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

## Affectation de l'application à un rôle

Vous devez lier la principale de service à un ou plusieurs abonnements Azure et lui attribuer le rôle « opérateur OnCommand Cloud Manager » personnalisé pour que Cloud Manager possède des autorisations dans Azure.

## Étapes

1. Création d'un rôle personnalisé :

- a. Téléchargez le "[Politique de Cloud Manager Azure](#)".
- b. Modifiez le fichier JSON en ajoutant des identifiants d'abonnement Azure à l'étendue assignable.

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

## Exemple

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

c. Utilisez le fichier JSON pour créer un rôle personnalisé dans Azure.

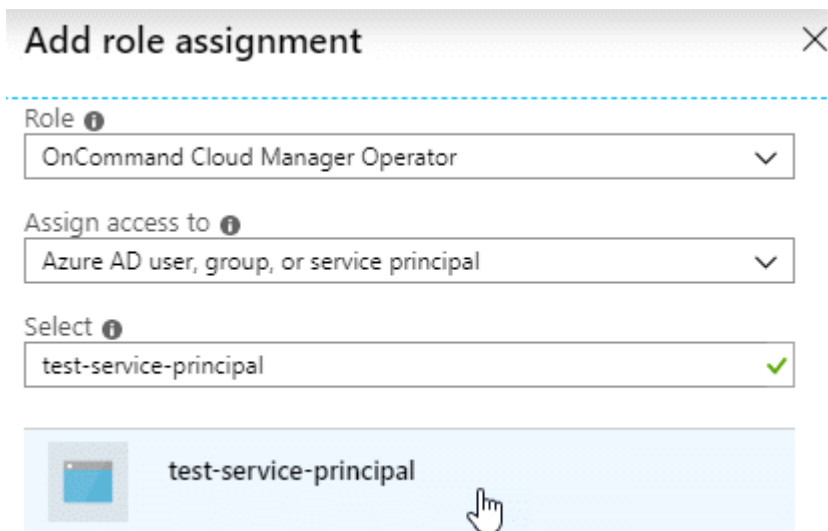
L'exemple suivant montre comment créer un rôle personnalisé à l'aide de l'interface de ligne de commande Azure CLI 2.0 :

```
az role definition create --role-definition
C:\Policy_for_cloud_Manager_Azure_3.8.7.json
```

Vous devriez maintenant avoir un rôle personnalisé appelé *Cloud Manager Operator*.

2. Attribuez l'application au rôle :

- a. À partir du portail Azure, ouvrez le service **abonnements**.
- b. Sélectionnez l'abonnement.
- c. Cliquez sur **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.
- d. Sélectionnez le rôle **opérateur** de Cloud Manager.
- e. Conserver \*l'utilisateur, le groupe ou le principal de service AD d'Azure sélectionné.
- f. Recherchez le nom de l'application (vous ne pouvez pas le trouver dans la liste en faisant défiler la liste).



- g. Sélectionnez l'application et cliquez sur **Enregistrer**.

Le principal de service de Cloud Manager dispose désormais des autorisations Azure requises pour cet abonnement.

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. Cloud Manager vous permet de sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

#### Ajout d'autorisations d'API de gestion des services Windows Azure

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

#### Étapes

1. Dans le service **Azure Active Directory**, cliquez sur **App inscriptions** et sélectionnez l'application.
2. Cliquez sur **autorisations API > Ajouter une autorisation**.

3. Sous **Microsoft API**, 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.




 <b>Azure Batch</b> Schedule large-scale parallel and HPC applications in the cloud	 <b>Azure Data Catalog</b> Programmatic access to Data Catalog resources to register, annotate and search data assets	 <b>Azure Data Explorer</b> Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 <b>Azure Data Lake</b> Access to storage and compute for big data analytic scenarios	 <b>Azure DevOps</b> Integrate with Azure DevOps and Azure DevOps server	 <b>Azure Import/Export</b> Programmatic control of import/export jobs
 <b>Azure Key Vault</b> Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 <b>Azure Rights Management Services</b> Allow validated users to read and write protected content	 <b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal
 <b>Azure Storage</b> Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 <b>Customer Insights</b> Create profile and interaction models for your products	 <b>Data Export Service for Microsoft Dynamics 365</b> Export data from Microsoft Dynamics CRM organization to an external destination

4. Cliquez sur **Access Azure Service Management en tant qu'utilisateurs d'organisation**, puis sur **Add permissions**.



## 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](#)

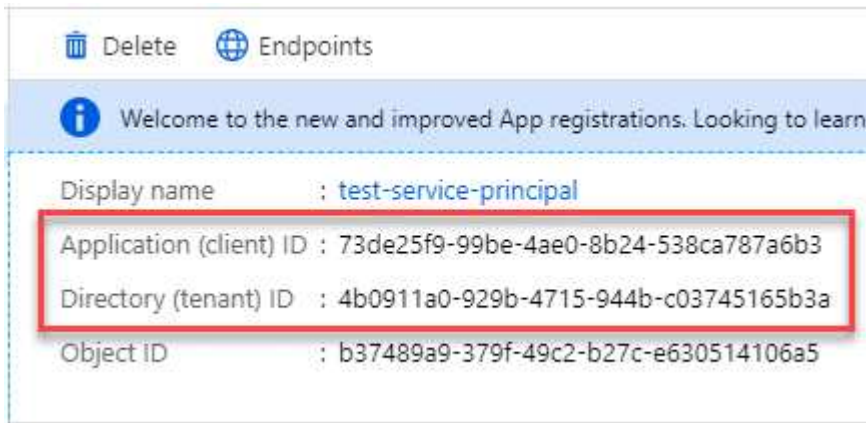
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) 	-

## Obtention de l'ID d'application et de l'ID de répertoire

Lorsque vous ajoutez le compte Azure dans Cloud Manager, vous devez fournir l'ID d'application (client) et l'ID de répertoire (locataire) de l'application. Cloud Manager utilise ces identifiants pour vous connecter automatiquement.

### Étapes

1. Dans le service **Azure Active Directory**, cliquez sur **App inscriptions** et sélectionnez l'application.
2. Copiez l'ID **application (client)** et l'ID **Directory (tenant)**.



The screenshot shows the 'App Registrations' page in Azure Active Directory. At the top, there are 'Delete' and 'Endpoints' icons. Below that is a blue banner with an information icon and the text 'Welcome to the new and improved App registrations. Looking to learn...'. The main content area shows details for an application named 'test-service-principal'. The 'Application (client) ID' is 73de25f9-99be-4ae0-8b24-538ca787a6b3 and the 'Directory (tenant) ID' is 4b0911a0-929b-4715-944b-c03745165b3a. These two IDs are highlighted with a red rectangular box. The 'Object ID' is b37489a9-379f-49c2-b27c-e630514106a5.

## Création d'un secret client

Vous devez créer un secret client, puis fournir à Cloud Manager la valeur du secret pour que Cloud Manager puisse l'utiliser pour vous authentifier avec Azure AD.



Lorsque vous ajoutez le compte à Cloud Manager, Cloud Manager fait référence au secret client en tant que clé d'application.

### Étapes

1. Ouvrez le service **Azure Active Directory**.
2. Cliquez sur **App Inregistrations** et sélectionnez votre application.
3. Cliquez sur **certificats et secrets > Nouveau secret client**.
4. Fournissez une description du secret et une durée.
5. Cliquez sur **Ajouter**.
6. Copier 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	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRov4NLfdAcY7:+0vA	

### Résultat

Votre principal de service est maintenant configuré et vous devez avoir copié l'ID de l'application (client), l'ID du répertoire (tenant) et la valeur du secret client. Vous devez saisir ces informations dans Cloud Manager lorsque vous ajoutez un compte Azure.

### Ajout d'identifiants Azure à Cloud Manager

Une fois que vous avez autorisé à fournir un compte Azure, vous pouvez ajouter les identifiants de ce compte à Cloud Manager. Vous pouvez ainsi lancer les systèmes Cloud Volumes ONTAP de ce compte.

### 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**.



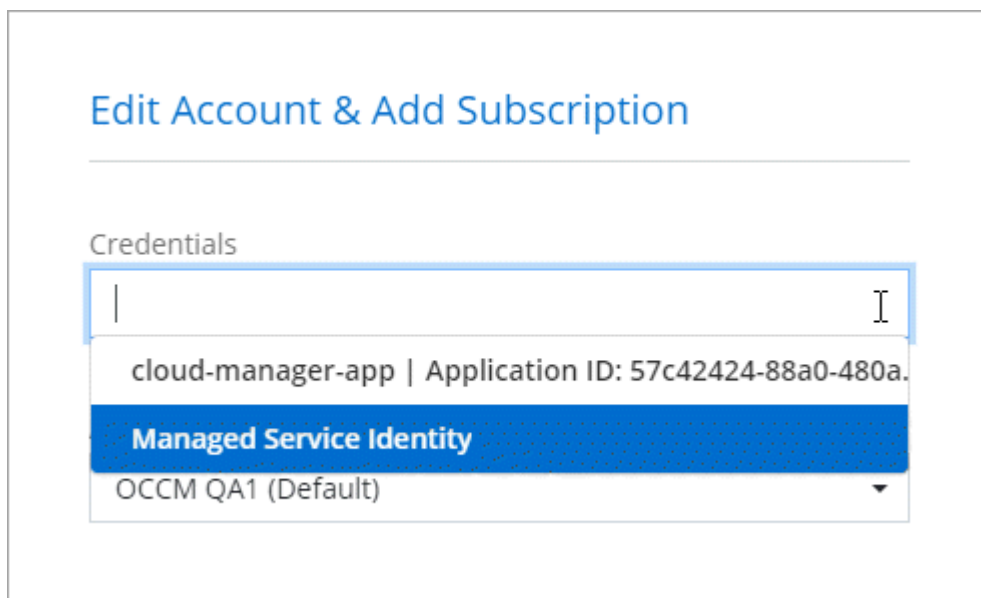
2. Cliquez sur **Ajouter des informations d'identification** et sélectionnez **Microsoft Azure**.
3. Entrez des informations sur l'entité de sécurité du service Azure Active Directory qui accorde les autorisations requises :
  - ID de l'application (client) : voir [Obtention de l'ID d'application et de l'ID de répertoire](#).
  - ID de répertoire (locataire) : voir [Obtention de l'ID d'application et de l'ID de répertoire](#).
  - Secret client : voir [Création d'un secret client](#).
4. Vérifiez que les exigences de la stratégie ont été respectées, puis 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 basé sur l'utilisation, vous devez associer des identifiants Azure à un abonnement à Cloud Volumes ONTAP à partir d'Azure Marketplace.

6. Cliquez sur **Ajouter**.

### Résultat

Vous pouvez maintenant passer à différents ensembles d'informations d'identification à partir de la page Détails et informations d'identification "[lors de la création d'un nouvel environnement de travail](#)":



### Association d'un abonnement à Azure Marketplace aux identifiants

Après avoir ajouté vos identifiants Azure à Cloud Manager, vous pouvez associer un abonnement Azure 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 s'avérer nécessaires pour associer un abonnement Azure Marketplace une fois que vous avez déjà ajouté les identifiants à Cloud Manager :

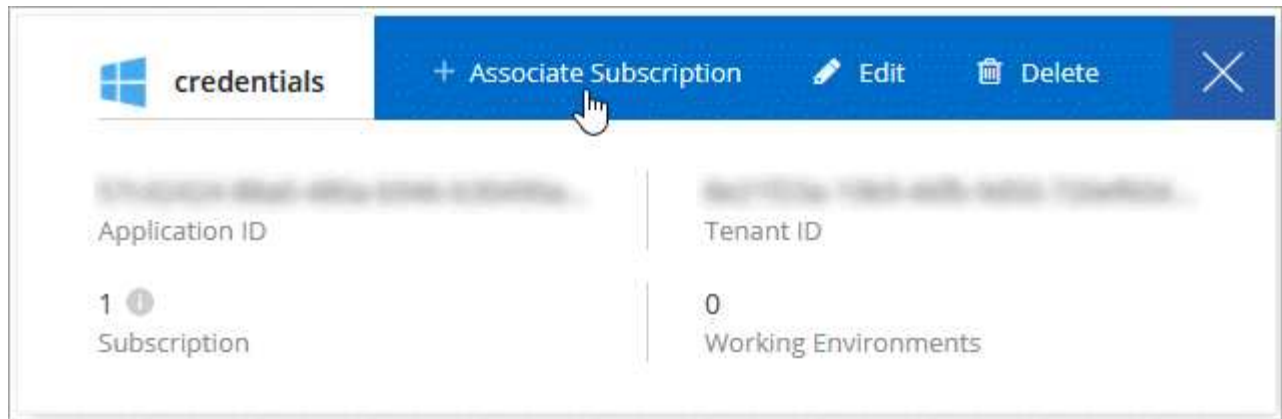
- Vous n'avez pas associé un abonnement lors de l'ajout initial des identifiants à Cloud Manager.
- Vous souhaitez remplacer un abonnement Azure Marketplace existant par un nouvel abonnement.

### 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.

La vidéo suivante démarre à partir du contexte de l'assistant de l'environnement de travail, mais vous montre le même flux de travail après avoir cliqué sur **Ajouter un abonnement** :

► [https://docs.netapp.com/fr-fr/occm38//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_azure.mp4) (video)

### Association d'abonnements Azure supplémentaires à une identité gérée

Cloud Manager vous permet de choisir les identifiants Azure et l'abonnement Azure dans lesquels vous souhaitez déployer Cloud Volumes ONTAP. Vous ne pouvez pas sélectionner un autre abonnement Azure pour le profil d'identité gérée à moins d'associer le "identité gérée" avec ces abonnements.

#### Description de la tâche

Une identité gérée est "Compte Azure initial" Lorsque vous déployez un connecteur depuis Cloud Manager. Une fois que vous avez déployé Connector, Cloud Manager a créé le rôle de l'opérateur Cloud Manager et l'a attribué à la machine virtuelle du connecteur.

#### 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. Cliquez sur **contrôle d'accès (IAM)**.
  - a. Cliquez sur **Ajouter** > **Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
    - Sélectionnez le rôle **opérateur** de Cloud Manager.

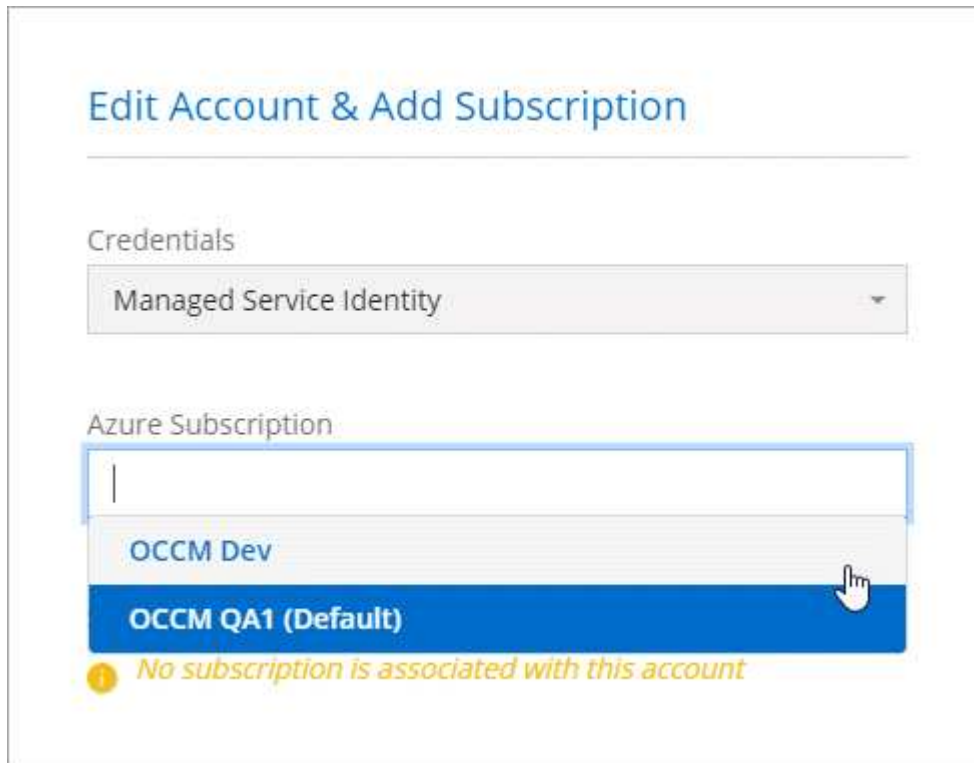


L'opérateur de Cloud Manager est le nom par défaut fourni dans "Politique de Cloud Manager". Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

- Attribuez l'accès à une **machine virtuelle**.
  - Sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée.
  - Sélectionnez la machine virtuelle Connector.
  - Cliquez sur **Enregistrer**.
4. Répétez ces étapes pour les abonnements supplémentaires.

## Résultat

Lorsque vous créez un nouvel environnement de travail, vous devriez désormais pouvoir sélectionner plusieurs abonnements Azure pour le profil d'identité géré.



## GCP

### Projets, autorisations et comptes Google Cloud

Un compte de service fournit à Cloud Manager les autorisations de déploiement et de gestion des systèmes Cloud Volumes ONTAP dans le même projet que Cloud Manager, ou dans des projets différents.

#### Projet et autorisations pour Cloud Manager

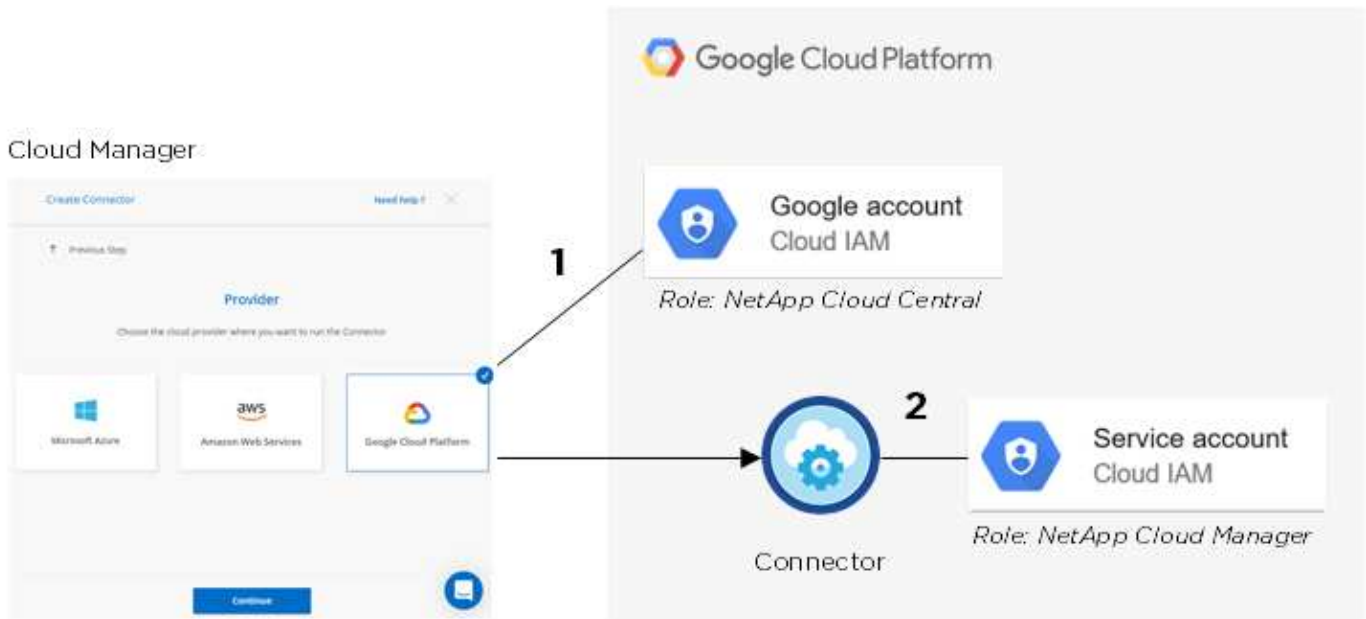
Avant de déployer Cloud Volumes ONTAP dans Google Cloud, vous devez d'abord déployer un connecteur dans un projet Google Cloud. Il ne peut pas s'exécuter sur site ou dans un autre fournisseur cloud.

Deux ensembles d'autorisations doivent être en place avant de déployer un connecteur directement depuis Cloud Manager :

1. Vous devez déployer un connecteur à l'aide d'un compte Google disposant des autorisations nécessaires pour lancer l'instance de VM Connector à partir de Cloud Manager.
2. Lorsque vous déployez le connecteur, vous êtes invité à sélectionner un "compte de service" Pour l'instance de VM. Cloud Manager obtient les autorisations du compte de service pour créer et gérer les systèmes Cloud Volumes ONTAP en votre nom. Les autorisations sont fournies en ajoutant un rôle personnalisé au compte de service.

Nous avons configuré deux fichiers YAML qui incluent les autorisations requises pour l'utilisateur et le compte de service. "[Découvrez comment utiliser les fichiers YAML pour configurer les autorisations](#)".

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



## Projet pour Cloud Volumes ONTAP

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

- ["Découvrez comment configurer un compte de service \(voir étape 2\)".](#)
- ["Découvrez comment déployer Cloud Volumes ONTAP dans GCP et sélectionner un projet".](#)

## Compte tenu du Tiering des données



Cloud Manager requiert un compte GCP pour Cloud Volumes ONTAP 9.6, mais pas pour la version 9.7 et ultérieure. Si vous souhaitez utiliser le Tiering des données avec Cloud Volumes ONTAP 9.7, suivez les étapes 4 à ["Mise en route de Cloud Volumes ONTAP dans Google Cloud Platform"](#).

L'ajout d'un compte Google Cloud à Cloud Manager permet le Tiering des données sur un système Cloud Volumes ONTAP 9.6. Le Tiering des données transfère automatiquement les données inactives vers un stockage objet plus économique, ce qui vous permet de récupérer de l'espace dans votre stockage primaire et de réduire le stockage secondaire.

Lorsque vous ajoutez ce compte, vous devez fournir à Cloud Manager une clé d'accès de stockage pour un compte de service disposant des autorisations d'administrateur de stockage. Cloud Manager utilise les clés d'accès pour configurer et gérer un compartiment de stockage cloud pour le Tiering des données.

Une fois que vous avez ajouté un compte Google Cloud, vous pouvez activer le Tiering des données sur les volumes individuels lorsque vous les créez, les modifiez ou les répliquez.

- ["Découvrez comment configurer et ajouter des comptes GCP à Cloud Manager".](#)
- ["Découvrez comment transférer des données inactives vers un stockage objet à faible coût".](#)

## Gestion des identifiants GCP et des abonnements pour Cloud Manager

Vous pouvez gérer deux types d'identifiants Google Cloud Platform dans Cloud Manager : les identifiants qui sont associés à l'instance de machine virtuelle de connecteur et les clés d'accès de stockage utilisées avec un système Cloud Volumes ONTAP 9.6 pour "tiering des données".

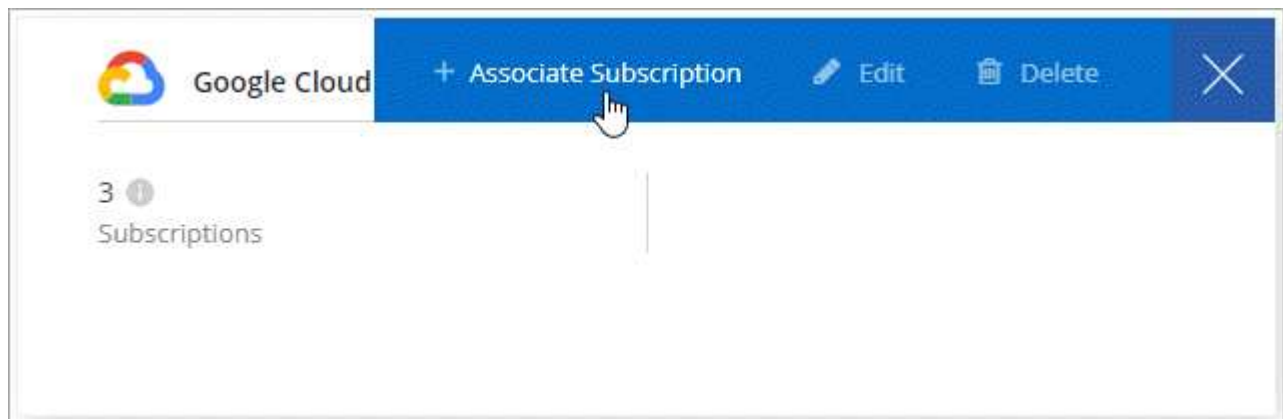
### Association d'un abonnement Marketplace aux informations d'identification GCP

Lorsque vous déployez un connecteur dans GCP, Cloud Manager crée un ensemble d'identifiants par défaut associés à l'instance de VM de connecteur. Ce sont les identifiants utilisés par Cloud Manager pour déployer Cloud Volumes ONTAP.

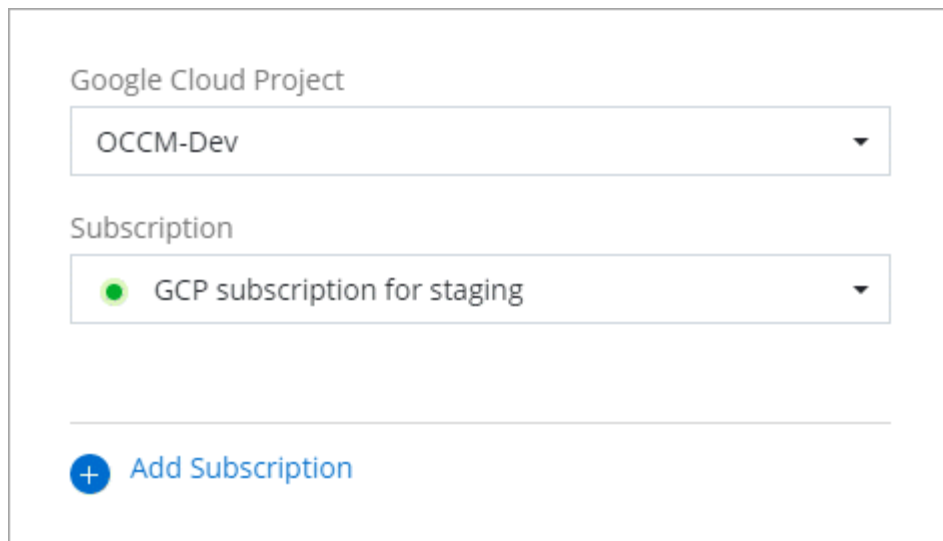
Vous pouvez à tout moment modifier l'abonnement Marketplace associé à ces informations d'identification. Cet abonnement vous permet de créer un système Cloud Volumes ONTAP basé sur l'utilisation et d'utiliser d'autres services cloud NetApp.

### 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 projet et un abonnement Google Cloud dans la liste déroulante ou cliquez sur **Ajouter un abonnement** et suivez les étapes pour créer un nouvel abonnement.



5. Cliquez sur **associé**.

### Configuration et ajout de comptes GCP pour le Tiering des données avec Cloud Volumes ONTAP 9.6

Si vous souhaitez activer un système Cloud Volumes ONTAP 9.6 pour "[tiering des données](#)", Vous devez fournir à Cloud Manager une clé d'accès au stockage pour un compte de service disposant des autorisations d'administrateur de stockage. Cloud Manager utilise les clés d'accès pour configurer et gérer un compartiment de stockage cloud pour le Tiering des données.



Si vous souhaitez utiliser le Tiering des données avec Cloud Volumes ONTAP 9.7, suivez les étapes 4 à "[Mise en route de Cloud Volumes ONTAP dans Google Cloud Platform](#)".

### Configurer un compte de service et des clés d'accès pour Google Cloud Storage

Un compte de service permet à Cloud Manager d'authentifier et d'accéder aux compartiments Cloud Storage utilisés pour le Tiering des données. Les clés sont requises pour que Google Cloud Storage sache qui effectue la demande.

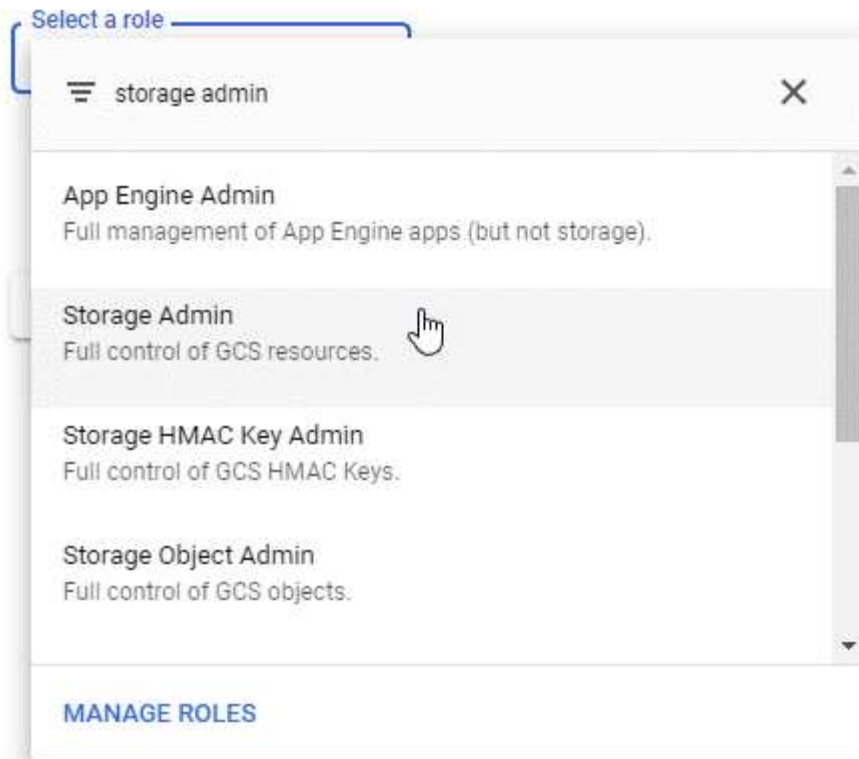
#### Étapes

1. Ouvrez la console IAM GCP et "[Créez un compte de service avec le rôle d'administrateur du stockage](#)".



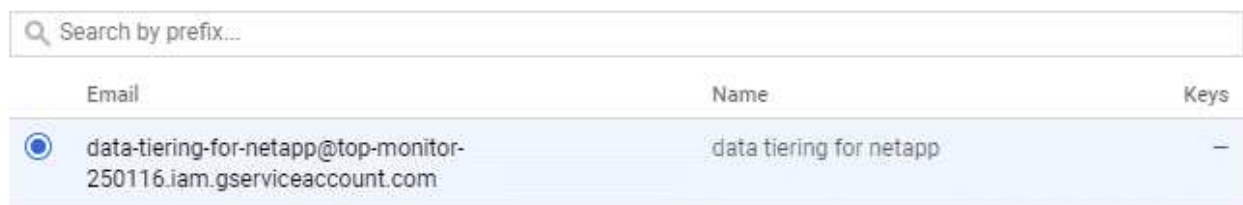
## Service account permissions (optional)

Grant this service account access to My Project 99247 so that it has permission to complete specific actions on the resources in your project. [Learn more](#)



2. Accédez à "[Paramètres de stockage GCP](#)".
3. Si vous y êtes invité, sélectionnez un projet.
4. Cliquez sur l'onglet **Interoperability**.
5. Si ce n'est déjà fait, cliquez sur **Activer l'accès à l'interopérabilité**.
6. Sous **clés d'accès pour les comptes de service**, cliquez sur **Créer une clé pour un compte de service**.
7. Sélectionnez le compte de service que vous avez créé à l'étape 1.

## Select a service account



[CANCEL](#) [CREATE KEY](#) | [CREATE NEW ACCOUNT](#)

8. Cliquez sur **Créer clé**.

9. Copiez la clé d'accès et le secret.

Lorsque vous ajoutez le compte GCP pour le Tiering des données, vous devez entrer ces informations dans Cloud Manager.

### Ajout d'un compte GCP à Cloud Manager

Vous pouvez désormais ajouter cette clé à Cloud Manager.

#### 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. Cliquez sur **Ajouter des informations d'identification** et sélectionnez **Google Cloud**.
3. Saisissez la clé d'accès et le secret du compte de service.

Les clés permettent à Cloud Manager de configurer un compartiment Cloud Storage pour le Tiering des données.

4. Vérifiez que les exigences de la stratégie ont été respectées, puis cliquez sur **Créer un compte**.

#### Et la suite ?

Vous pouvez désormais activer le Tiering des données sur les volumes individuels d'un système Cloud Volumes ONTAP 9.6 lorsque vous les créez, les modifiez ou les répliquez. Pour plus de détails, voir "[Tiering des données inactives vers un stockage objet à faible coût](#)".

Mais avant cela, assurez-vous que le sous-réseau dans lequel réside Cloud Volumes ONTAP est configuré pour un accès privé à Google. Pour obtenir des instructions, reportez-vous à la section "[Documentation Google Cloud : configuration de Private Google Access](#)".

## Ajout de comptes du site de support NetApp à Cloud Manager

Vous devez ajouter votre compte sur le site de support NetApp à Cloud Manager pour déployer un système BYOL. Il est également nécessaire d'enregistrer des systèmes avec paiement à l'utilisation et de mettre à niveau le logiciel ONTAP.

Découvrez dans cette vidéo comment ajouter des comptes sur le site de support NetApp à Cloud Manager. Ou faites défiler vers le bas pour lire les étapes.

📺 | <https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg>

#### Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "[Découvrez comment](#)".

## Étapes

1. Si vous ne disposez pas encore d'un compte sur le site de support NetApp, "[inscrivez-vous pour en créer un](#)".
2. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



3. Cliquez sur **Add Credentials** et sélectionnez **NetApp support site**.
4. Spécifiez un nom pour le compte, puis entrez le nom d'utilisateur et le mot de passe.
  - Le compte doit être un compte de niveau client (et non un compte invité ou temporaire).
  - Si vous prévoyez de déployer des systèmes BYOL :
    - Le compte doit être autorisé à accéder aux numéros de série des systèmes BYOL.
    - Si vous avez acheté un abonnement BYOL sécurisé, un compte NSS sécurisé est requis.
5. Cliquez sur **Créer un compte**.

## Et la suite ?

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

- "[Lancement d'Cloud Volumes ONTAP dans AWS](#)"
- "[Lancement d'Cloud Volumes ONTAP dans Azure](#)"
- "[Enregistrement des systèmes de paiement à l'utilisation](#)"
- "[Découvrez comment Cloud Manager gère les fichiers de licences](#)"

## Informations sur le copyright

Copyright © 2024 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.