



Administration de BlueXP

Set up and administration

NetApp

December 01, 2022

This PDF was generated from <https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/task-managing-netapp-accounts.html> on December 01, 2022. Always check docs.netapp.com for the latest.

Table des matières

- Administration de BlueXP 1
 - Comptes NetApp 1
 - Connecteurs 16
 - Gérer les abonnements et les contrats PAYGO 48
 - Stockage cloud découvert 49
 - Identifiants AWS 54
 - Identifiants Azure 63
 - Identifiants Google Cloud 75
 - Ajoutez et gérez des comptes du site de support NetApp dans BlueXP 83
 - Mes opportunités 90

Administration de BlueXP

Comptes NetApp

Gestion de votre compte NetApp

"Après avoir effectué la configuration initiale", Vous pouvez gérer les paramètres de votre compte ultérieurement en gérant les utilisateurs, les comptes de service, les espaces de travail, les connecteurs et les abonnements.

"Découvrez comment fonctionnent les comptes NetApp".

Gestion de votre compte à l'aide de l'API de location

Si vous souhaitez gérer les paramètres de votre compte en envoyant des demandes API, vous devez utiliser l'API *Tenancy*. Cette API est différente de l'API BlueXP, que vous utilisez pour créer et gérer des environnements de travail Cloud Volumes ONTAP.

"Affichez les terminaux de l'API de colocation"

Création et gestion des utilisateurs

L'utilisateur de votre compte peut accéder aux ressources de gestion des espaces de travail de votre compte.

Ajout d'utilisateurs

Associez les utilisateurs à votre compte NetApp pour qu'ils puissent créer et gérer des environnements de travail dans BlueXP.

Étapes

1. Si l'utilisateur ne l'a pas déjà fait, demandez-lui d'aller à "[Site Web NetApp BlueXP](#)" et s'inscrire.
2. En haut de BlueXP, cliquez sur la liste déroulante **Account**.



3. Cliquez sur **gérer le compte** en regard du compte actuellement sélectionné.



4. Dans l'onglet membres, cliquez sur **associer utilisateur**.
5. Entrez l'adresse e-mail de l'utilisateur et sélectionnez un rôle pour l'utilisateur :
 - **Administrateur de compte**: Peut effectuer n'importe quelle action dans BlueXP.
 - **Workspace Admin** : permet de créer et de gérer des ressources dans des espaces de travail attribués.
 - **Compliance Viewer** : peut uniquement afficher les informations de conformité de Cloud Data Sense et générer des rapports pour les espaces de travail auxquels ils sont autorisés à accéder.
 - **Admin SnapCenter** : peut utiliser le service SnapCenter pour créer des sauvegardes cohérentes avec les applications et restaurer les données à l'aide de ces sauvegardes. *Ce service est actuellement en version bêta.*
6. Si vous avez sélectionné Workspace Admin ou Compliance Viewer, sélectionnez un ou plusieurs espaces de travail à associer à cet utilisateur.



The image shows a dialog box titled "Associate User" with a user icon at the top. It contains instructions on how to add a user, followed by three input fields: "User's Email" (containing "test@netapp.com"), "Role" (a dropdown menu showing "Workspace Admin"), and "Associate User to Workspaces" (a dropdown menu showing "Workspace-1" with a close button). At the bottom are "Cancel" and "Associate User" buttons.



Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1

Cancel Associate User

7. Cliquez sur **associé**.

L'utilisateur doit recevoir un e-mail de NetApp BlueXP intitulé « Account Association ». L'e-mail inclut les informations nécessaires pour accéder à BlueXP.

Suppression d'utilisateurs

En effet, la dissociation permet d'interdire l'accès aux ressources d'un compte NetApp.

Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.



2. Dans l'onglet membres, cliquez sur le menu d'action de la ligne correspondant à l'utilisateur.



3. Cliquez sur **Disassocier utilisateur** et cliquez sur **Disassocier** pour confirmer.

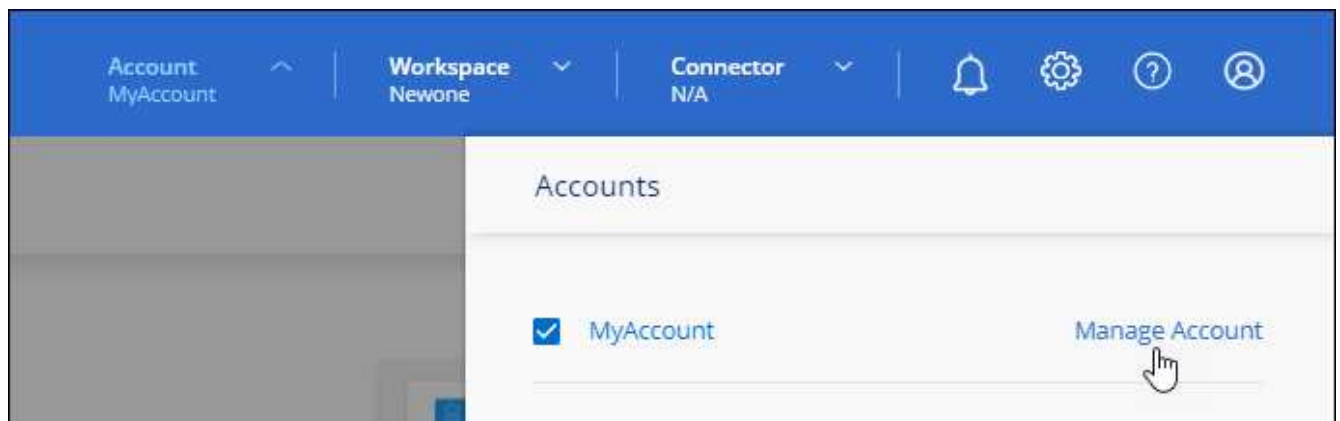
L'utilisateur ne peut plus accéder aux ressources de ce compte NetApp.

Gestion des espaces de travail d'un Workspace Admin

Vous pouvez associer et dissocier les administrateurs d'espace de travail avec des espaces de travail à tout moment. L'association de l'utilisateur lui permet de créer et d'afficher les environnements de travail dans cet espace de travail.

Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.



2. Dans l'onglet membres, cliquez sur le menu d'action de la ligne correspondant à l'utilisateur.

5 Members					
Type	Name	Email	Role	Workspace	
	Ben		☆ Account Admin	All Workspaces	...
	Tom		☆ Account Admin	All Workspaces	...
	Ben		Workspace Admin	Newone	

3. Cliquez sur **gérer les espaces de travail**.

4. Sélectionnez les espaces de travail à associer à l'utilisateur et cliquez sur **appliquer**.

L'utilisateur peut désormais accéder à ces espaces de travail depuis BlueXP, tant que le connecteur était également associé aux espaces de travail.

Création et gestion des comptes de service

Un compte de service agit comme un « utilisateur » qui peut effectuer des appels API autorisés vers BlueXP à des fins d'automatisation. Il est ainsi plus facile de gérer l'automatisation, car il n'est pas nécessaire de créer des scripts d'automatisation basés sur le compte d'utilisateur réel d'une personne qui quitte l'entreprise à tout moment. Et si vous utilisez la fédération, vous pouvez créer un jeton sans générer de jeton d'actualisation à partir du cloud.

Vous donnez des autorisations à un compte de service en lui attribuant un rôle, tout comme n'importe quel autre utilisateur BlueXP. Vous pouvez également associer le compte de service à des espaces de travail spécifiques afin de contrôler les environnements de travail (ressources) auxquels le service peut accéder.

Lorsque vous créez le compte de service, BlueXP vous permet de copier ou de télécharger un ID client et un secret client pour le compte de service. Cette paire de clés est utilisée pour l'authentification avec BlueXP.

Création d'un compte de service

Créez autant de comptes de services que nécessaire pour gérer les ressources de vos environnements de travail.

Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account**.



2. Cliquez sur **gérer le compte** en regard du compte actuellement sélectionné.



3. Dans l'onglet membres, cliquez sur **Créer un compte de service**.
4. Entrez un nom et sélectionnez un rôle. Si vous avez choisi un rôle autre que Administrateur de compte, choisissez l'espace de travail à associer à ce compte de service.
5. Cliquez sur **Créer**.
6. Copiez ou téléchargez l'ID client et le secret client.

Le secret client n'est visible qu'une seule fois et n'est pas stocké n'importe où par BlueXP. Copiez ou téléchargez le secret et rangez-le en toute sécurité.

7. Cliquez sur **Fermer**.

Obtention d'un jeton de porteur pour un compte de service

Pour passer des appels API à "[API de location](#)", vous devrez obtenir un jeton de porteur pour un compte de service.

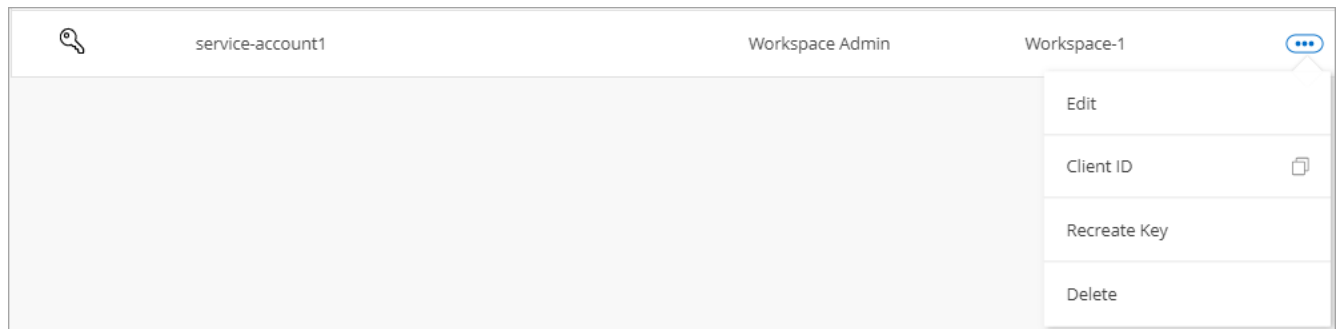
["Découvrez comment créer un jeton de compte de service"](#)

Copie de l'ID client

Vous pouvez copier l'ID client d'un compte de service à tout moment.

Étapes

1. Dans l'onglet membres, cliquez sur le menu d'action de la ligne correspondant au compte de service.



2. Cliquez sur **ID client**.
3. L'ID est copié dans le presse-papiers.

Recréation des clés

La recréation de la clé supprimera la clé existante pour ce compte de service, puis créera une nouvelle clé. Vous ne pourrez pas utiliser la touche précédente.

Étapes

1. Dans l'onglet membres, cliquez sur le menu d'action de la ligne correspondant au compte de service.



2. Cliquez sur **recréer la clé**.
3. Cliquez sur **recréer** pour confirmer.
4. Copiez ou téléchargez l'ID client et le secret client.

Le secret client n'est visible qu'une seule fois et n'est pas stocké n'importe où par BlueXP. Copiez ou téléchargez le secret et rangez-le en toute sécurité.

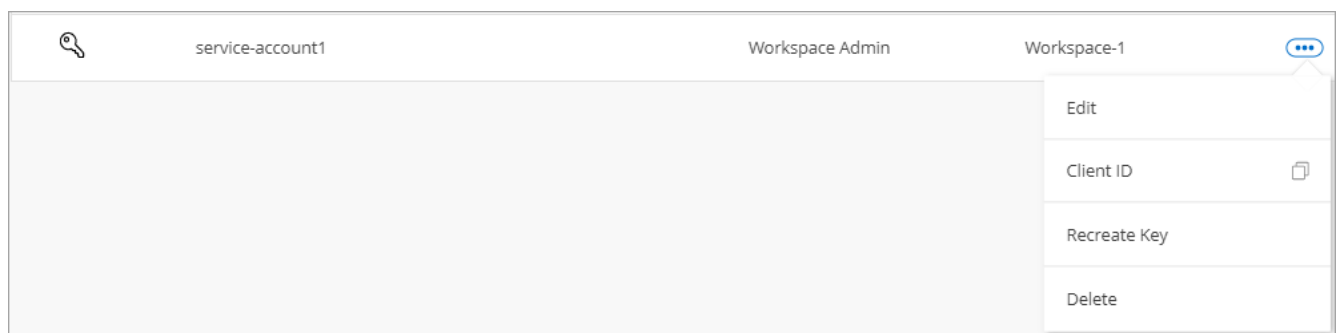
5. Cliquez sur **Fermer**.

Suppression d'un compte de service

Supprimez un compte de service si vous n'avez plus besoin de l'utiliser.

Étapes

1. Dans l'onglet membres, cliquez sur le menu d'action de la ligne correspondant au compte de service.



2. Cliquez sur **Supprimer**.
3. Cliquez à nouveau sur **Supprimer** pour confirmer.

Gestion des espaces de travail

Gérez vos espaces de travail en les créant, en les renommant et en les supprimant. Notez que vous ne pouvez pas supprimer un espace de travail s'il contient des ressources. Elle doit être vide.

Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Cliquez sur **espaces de travail**.
3. Choisissez l'une des options suivantes :
 - Cliquez sur **Ajouter un nouvel espace de travail** pour créer un nouvel espace de travail.
 - Cliquez sur **Renommer** pour renommer l'espace de travail.
 - Cliquez sur **Supprimer** pour supprimer l'espace de travail.

Gestion des espaces de travail d'un connecteur

Vous devez associer le connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent accéder à ces espaces de travail depuis BlueXP.

Si vous ne disposez que d'administrateurs de compte, il n'est pas nécessaire d'associer le connecteur aux espaces de travail. Les administrateurs de comptes peuvent accéder à tous les espaces de travail dans BlueXP par défaut.

["En savoir plus sur les utilisateurs, les espaces de travail et les connecteurs"](#).

Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Cliquez sur **connecteur**.
3. Cliquez sur **gérer les espaces de travail** pour le connecteur que vous souhaitez associer.
4. Sélectionnez les espaces de travail à associer au connecteur et cliquez sur **appliquer**.

Gestion des abonnements

Après vous être abonné au Marketplace d'un fournisseur cloud, chaque abonnement est disponible dans le widget Account Settings. Vous avez la possibilité de renommer un abonnement et de dissocier l'abonnement d'un ou plusieurs comptes.

Par exemple, disons que vous avez deux comptes et que chacun est facturé par le biais d'abonnements distincts. Vous pouvez dissocier un abonnement de l'un des comptes afin que les utilisateurs de ce compte ne choisissent pas accidentellement l'abonnement incorrect lors de la création d'un environnement de travail Cloud Volume ONTAP.

["En savoir plus sur les abonnements"](#).

Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Cliquez sur **abonnements**.

Vous ne verrez que les abonnements associés au compte que vous consultez actuellement.

3. Cliquez sur le menu d'action de la ligne correspondant à l'abonnement que vous souhaitez gérer.

2 Subscriptions

Name	Service	Cloud Provider	Status
QA Subscription	test-service	aws	Unsubscribed
metering service subscription QA !!!!	cloud-volumes-ontap	aws	Subscribed

Rename Subscription
Manage Accounts

4. Choisissez de renommer l'abonnement ou de gérer les comptes associés à l'abonnement.

Modification du nom de votre compte

Changez le nom de votre compte à tout moment pour le changer en quelque chose de significatif pour vous.

Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Dans l'onglet **vue d'ensemble**, cliquez sur l'icône de modification en regard du nom du compte.
3. Saisissez un nouveau nom de compte et cliquez sur **Enregistrer**.

Permettre des aperçus privés

Laissez des aperçus privés de votre compte accéder aux nouveaux services clouds NetApp disponibles dans BlueXP.

Les services d'aperçu privé ne sont pas garantis de se comporter comme prévu et peuvent supporter des interruptions et être des fonctionnalités manquantes.

Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Dans l'onglet **Présentation**, activez le paramètre **Autoriser aperçu privé**.

Permettre des services tiers

Autoriser les services tiers de votre compte à accéder à des services tiers disponibles dans BlueXP. Les services clouds tiers sont similaires aux services proposés par NetApp, mais ils sont gérés et pris en charge par des sociétés tierces.

Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Dans l'onglet **Présentation**, activez le paramètre **Autoriser les services tiers**.

Désactivation de la plateforme SaaS

Nous ne recommandons pas de désactiver la plate-forme SaaS sauf si vous devez vous conformer aux politiques de sécurité de votre entreprise. En désactivant la plateforme SaaS, vous vous limitez votre capacité à utiliser les services cloud intégrés de NetApp.

Les services suivants ne sont pas disponibles auprès de BlueXP si vous désactivez la plate-forme SaaS :

- Sens des données cloud
- Kubernetes
- Tiering dans le cloud
- Cache global de fichiers

Si vous désactivez la plateforme SaaS, vous devrez effectuer toutes les tâches à partir de "[Interface utilisateur locale disponible sur un connecteur](#)".



Il s'agit d'une action irréversible qui vous empêchera d'utiliser la plate-forme BlueXP SaaS. Vous devrez effectuer des actions à partir du connecteur local. Vous ne pourrez pas utiliser de nombreux services cloud intégrés de NetApp et mettre à disposition de la plateforme SaaS aura besoin de l'aide de NetApp.

Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Dans l'onglet vue d'ensemble, activez l'option pour désactiver l'utilisation de la plateforme SaaS.

Surveillance des opérations dans votre compte

Vous pouvez surveiller l'état des opérations que BlueXP effectue pour voir si des problèmes doivent être résolus. Vous pouvez afficher l'état dans le centre de notification, dans le calendrier ou envoyer des notifications à votre courrier électronique.

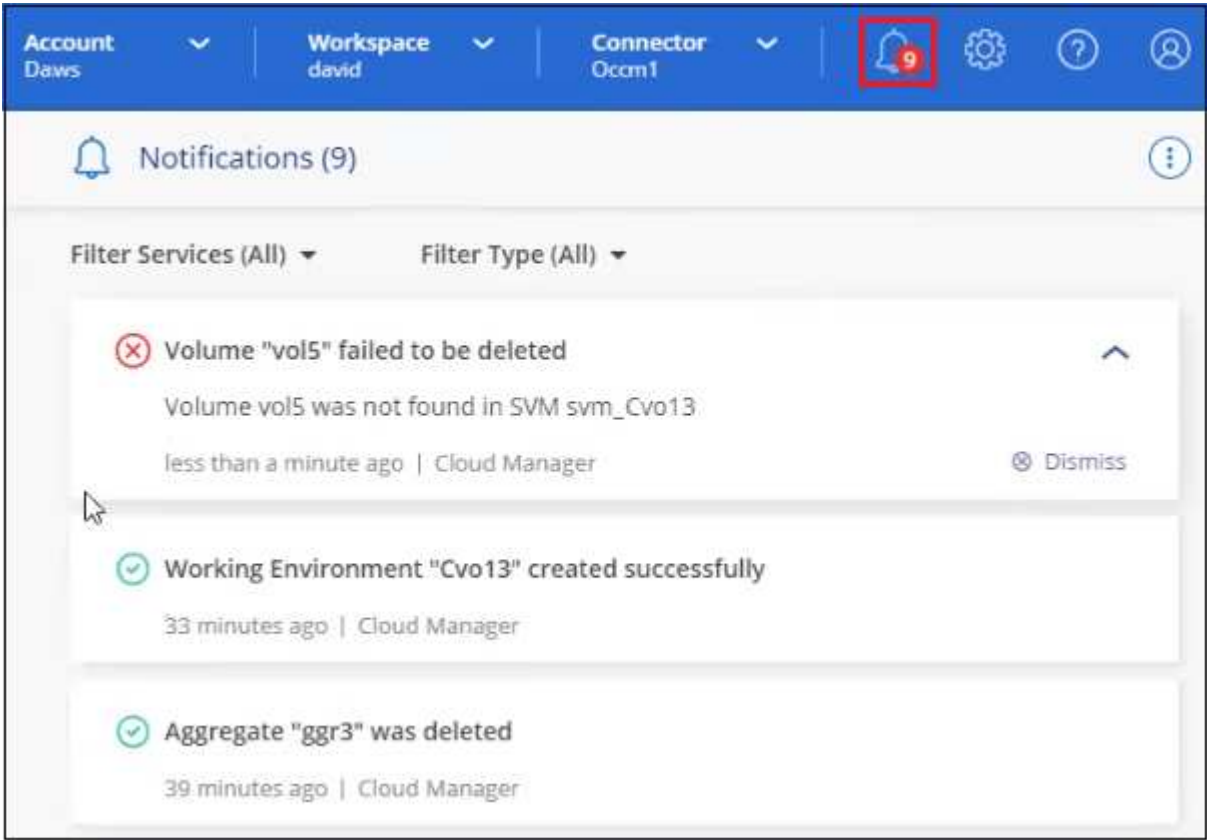
Ce tableau fournit une comparaison du centre de notification et du calendrier pour vous permettre de comprendre ce que chacun a à offrir.

Centre de notification	De la chronologie
Affiche l'état général des événements et des actions	Fournit des détails sur chaque événement ou action pour une enquête plus approfondie
Affiche l'état de la session de connexion en cours - les informations n'apparaîtront pas dans le Centre de notification après la déconnexion	Conserve le statut pour le dernier mois
Affiche uniquement les actions initiées dans l'interface utilisateur	Affiche toutes les actions à partir de l'interface utilisateur ou des API
Affiche les actions lancées par l'utilisateur	Affiche toutes les actions, qu'elles soient lancées par l'utilisateur ou par le système
Filtrez les résultats en fonction de l'importance	Filtrez par service, action, utilisateur, état, etc
Permet d'envoyer des notifications par e-mail aux utilisateurs du compte et à d'autres utilisateurs	Aucune capacité de messagerie

Surveillance des activités à l'aide du Centre de notification

Les notifications suivent la progression des opérations que vous avez lancées dans BlueXP pour vous permettre de vérifier si l'opération a réussi ou non. Elles vous permettent d'afficher l'état de nombreuses actions BlueXP que vous avez lancées pendant votre session de connexion actuelle. Tous les services ne rapportent pas d'informations au Centre de notification pour le moment.

Vous pouvez afficher les notifications en cliquant sur le signal sonore de notification (🔔) dans la barre de menus. La couleur de la petite bulle dans la cloche indique la notification de gravité de niveau le plus élevé qui est active. Si vous voyez une bulle rouge, cela signifie qu'il y a une notification importante que vous devriez regarder.



Vous pouvez également configurer BlueXP pour envoyer des notifications par e-mail afin de vous informer de l'activité système importante, même lorsque vous n'êtes pas connecté au système. Des e-mails sont envoyés à tous les utilisateurs qui font partie de votre compte cloud NetApp ou à tout autre destinataire ayant besoin de connaître certains types d'activité système. Voir email notification settings, Définition des paramètres de notification par e-mail ci-dessous.

Types de notification

Les notifications sont classées dans les catégories suivantes :

Type de notification	Description
Primordial	Un problème peut entraîner une interruption des services si des mesures correctives ne sont pas prises immédiatement.
Erreur	Une action ou un processus s'est terminé avec un échec ou pourrait entraîner un échec si aucune mesure corrective n'est prise.
Avertissement	Un problème que vous devez savoir pour vous assurer qu'il n'atteint pas la gravité critique. Les notifications de ce niveau de gravité n'entraînent pas d'interruption des services, mais une action corrective immédiate peut ne pas être nécessaire.

Type de notification	Description
Recommandation	Il est recommandé de prendre des mesures pour améliorer le système ou un service donné, par exemple : réduction des coûts, suggestion de nouveaux services, configuration de sécurité recommandée, etc
Informations	Message fournissant des informations supplémentaires sur une action ou un processus.
Réussite	Une action ou un processus s'est terminé avec succès.

Filtrage des notifications

Par défaut, toutes les notifications s'affichent. Vous pouvez filtrer les notifications que vous voyez dans le Centre de notification pour n'afficher que les notifications importantes pour vous. Vous pouvez filtrer par BlueXP "Service" et par notification "Type".

Par exemple, si vous souhaitez afficher uniquement les notifications "erreur" et "Avertissement" pour les opérations BlueXP, sélectionnez ces entrées et vous ne verrez que ces types de notifications.

Définition des paramètres de notification par e-mail

Vous pouvez envoyer par e-mail des types de notifications spécifiques afin de vous informer de l'activité système importante, même lorsque vous n'êtes pas connecté à BlueXP. Il est possible d'envoyer des e-mails aux utilisateurs qui font partie de votre compte NetApp ou à tout autre destinataire ayant besoin de connaître certains types d'activité système.



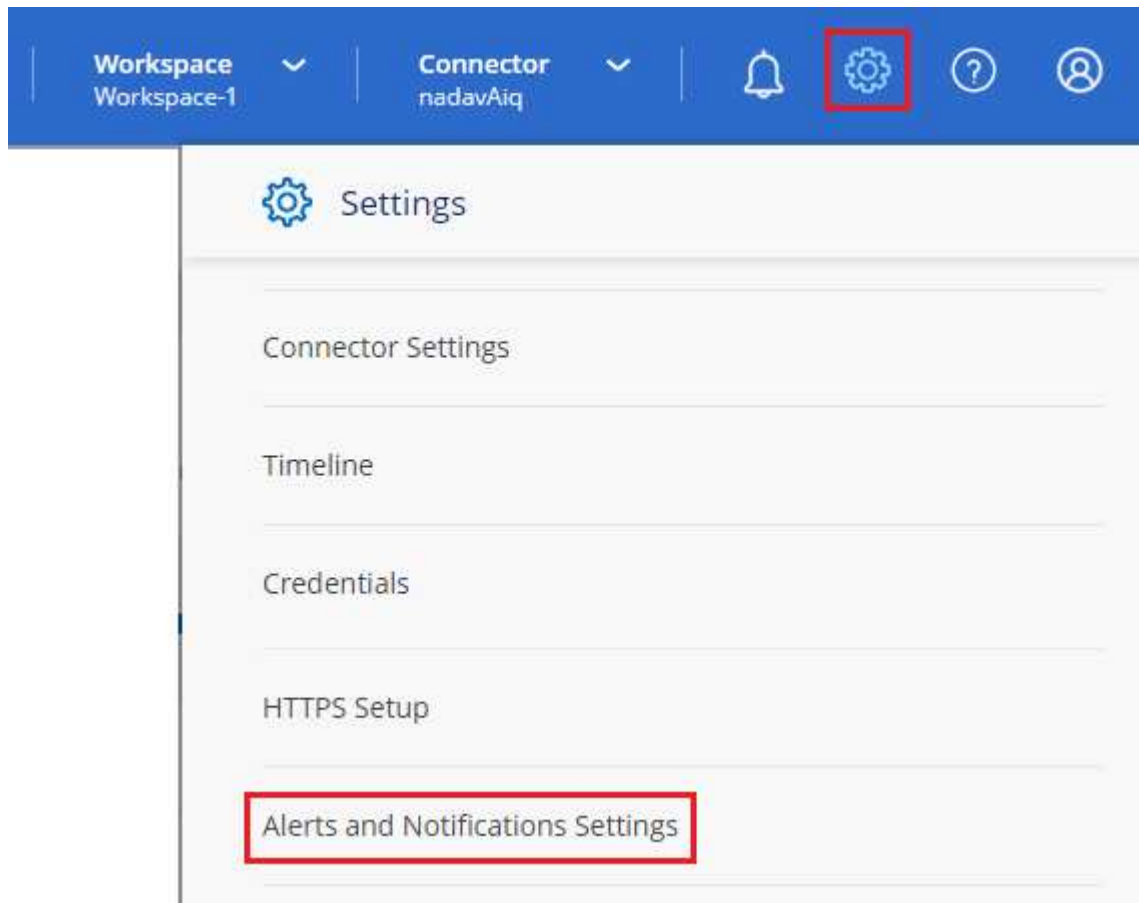
- À l'heure actuelle, seuls Cloud Sync et Cloud Backup envoient des notifications par e-mail. D'autres services seront ajoutés dans les prochaines versions.
- L'envoi de notifications par e-mail n'est pas pris en charge lorsque le connecteur est installé sur un site sans accès à Internet.

Par défaut, les administrateurs de compte BlueXP recevront des e-mails pour toutes les notifications « critiques » et « recommandations ». Par défaut, tous les autres utilisateurs et destinataires sont configurés pour ne pas recevoir d'e-mails de notification.

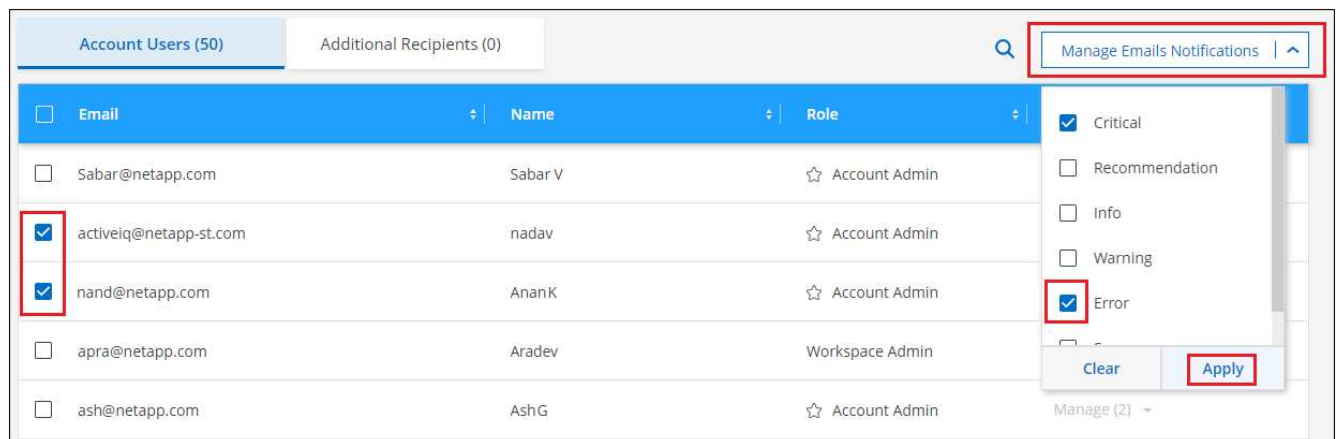
Pour personnaliser les paramètres de notifications, vous devez être administrateur de compte.

Étapes

1. Dans la barre de menus BlueXP, cliquez sur **Paramètres > Paramètres d'alertes et de notifications**.



2. Sélectionnez un utilisateur ou plusieurs utilisateurs à partir de l'onglet *Account Users* ou de l'onglet *Additional Recipients*, puis choisissez le type de notifications à envoyer :
 - Pour apporter des modifications à un seul utilisateur, cliquez sur le menu dans la colonne Notifications de cet utilisateur, cochez les types de notifications à envoyer et cliquez sur **appliquer**.
 - Pour apporter des modifications à plusieurs utilisateurs, cochez la case de chaque utilisateur, cliquez sur **gérer les notifications par e-mail**, cochez les types de notifications à envoyer et cliquez sur **appliquer**.

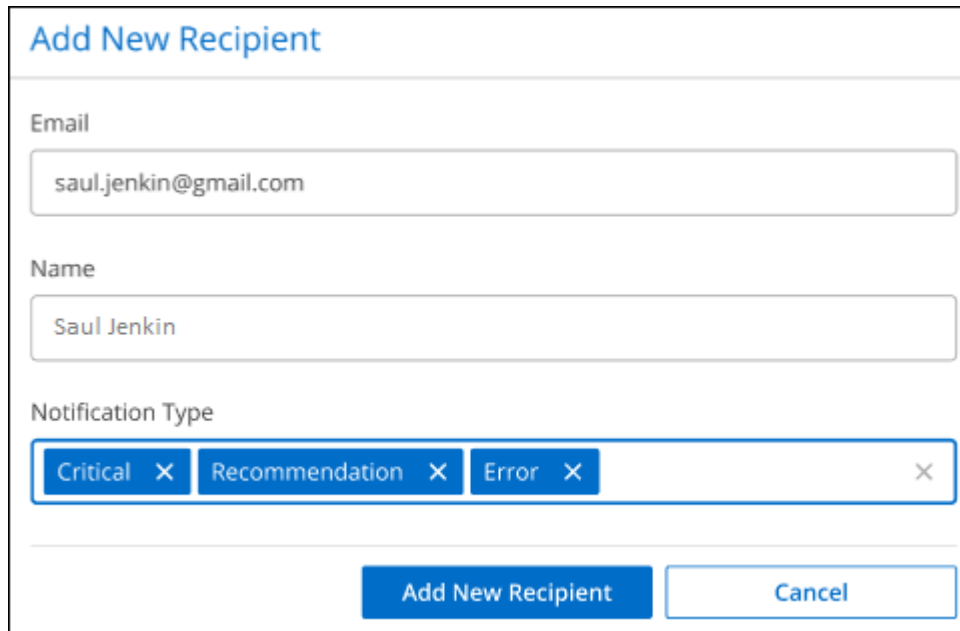


Ajout de destinataires d'e-mail supplémentaires

Les utilisateurs qui s'affichent dans l'onglet *Account Users* sont automatiquement renseignés à partir du site NetApp Account (du "[Gérer le compte](#)"). Vous pouvez ajouter des adresses e-mail dans l'onglet *destinataires supplémentaires* pour d'autres personnes ou groupes qui n'ont pas accès à BlueXP, mais qui doivent être informés de certains types d'alertes et de notifications.

Étapes

1. Dans la page Paramètres des alertes et notifications, cliquez sur **Ajouter de nouveaux destinataires**.



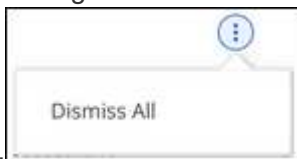
The screenshot shows a form titled "Add New Recipient". It has three input fields: "Email" with the value "saul.jenkin@gmail.com", "Name" with the value "Saul Jenkin", and "Notification Type" which is a multi-select dropdown containing "Critical", "Recommendation", and "Error". At the bottom, there are two buttons: "Add New Recipient" and "Cancel".

2. Entrez le nom, l'adresse e-mail et sélectionnez les types de notifications que le destinataire recevra, puis cliquez sur **Ajouter un nouveau destinataire**.

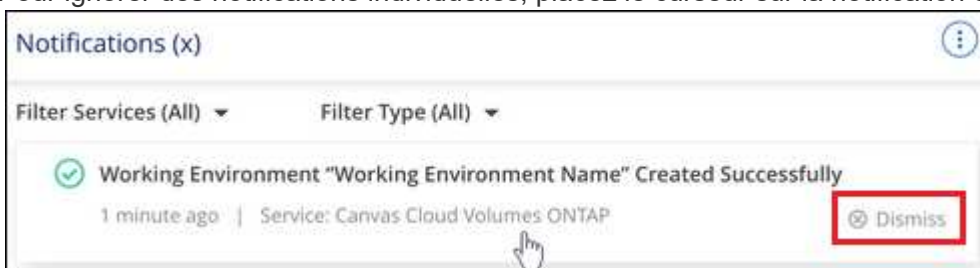
Rejet des notifications

Vous pouvez supprimer des notifications de la page si vous n'avez plus besoin de les voir. Vous pouvez rejeter toutes les notifications en une seule fois ou rejeter les notifications individuelles.

Pour ignorer toutes les notifications, dans le Centre de notification, cliquez sur  Et sélectionnez **rejeter tout**



Pour ignorer des notifications individuelles, placez le curseur sur la notification et cliquez sur **rejeter**



Audit de l'activité de l'utilisateur dans votre compte

Le Timeline de BlueXP affiche les actions que les utilisateurs ont effectuées pour gérer votre compte. Cela inclut des actions de gestion telles que l'association d'utilisateurs, la création d'espaces de travail, la création de connecteurs, etc.

La vérification de la chronologie peut être utile si vous devez identifier qui a effectué une action spécifique ou si vous devez identifier le statut d'une action.

Étapes

1. Dans la barre de menus BlueXP, cliquez sur **Paramètres > Chronologie**.
2. Sous filtres, cliquez sur **Service**, activez **Tenancy** et cliquez sur **appliquer**.

La chronologie est mise à jour pour vous montrer les actions de gestion de compte.

Rôles

Les rôles Administrateur de compte, Administrateur d'espace de travail, Visionneuse de conformité et Administrateur SnapCenter fournissent des autorisations spécifiques aux utilisateurs.

Le rôle Compliance Viewer permet l'accès en lecture seule à Cloud Data SENSE.

Tâche	Administrateur du compte	Administrateur de l'espace de travail	Visionneuse de conformité	Admin SnapCenter
Gérer les environnements de travail	Oui.	Oui.	Non	Non
Activer les services dans les environnements de travail	Oui.	Oui.	Non	Non
Afficher l'état de la réplication des données	Oui.	Oui.	Non	Non
Afficher la chronologie	Oui.	Oui.	Non	Non
Basculer entre les espaces de travail	Oui.	Oui.	Oui.	Non
Afficher les résultats de l'acquisition de détection de données	Oui.	Oui.	Oui.	Non
Supprimer les environnements de travail	Oui.	Non	Non	Non
Connectez les clusters Kubernetes aux environnements de travail	Oui.	Non	Non	Non

Tâche	Administrateur du compte	Administrateur de l'espace de travail	Visionneuse de conformité	Admin SnapCenter
Recevoir le rapport Cloud Volumes ONTAP	Oui.	Non	Non	Non
Créer des connecteurs	Oui.	Non	Non	Non
Gestion des comptes NetApp	Oui.	Non	Non	Non
Gérer les identifiants	Oui.	Non	Non	Non
Modifiez les paramètres BlueXP	Oui.	Non	Non	Non
Afficher et gérer le tableau de bord du support	Oui.	Non	Non	Non
Supprimez les environnements de travail de BlueXP	Oui.	Non	Non	Non
Installez un certificat HTTPS	Oui.	Non	Non	Non
Utiliser le service SnapCenter	Oui.	Oui.	Non	Oui.

Liens connexes

- ["Configuration d'espaces de travail et d'utilisateurs sur le compte NetApp"](#)
- ["Gestion des espaces de travail et des utilisateurs sur le compte NetApp"](#)

Connecteurs

Déploiement avancé

Créez un connecteur à partir d'AWS Marketplace

Dans le cas d'une région commerciale AWS, il est préférable de créer un connecteur directement depuis BlueXP, mais vous pouvez aussi lancer un connecteur depuis AWS Marketplace, si vous préférez. Pour les régions gouvernementales d'AWS, vous ne pouvez pas déployer le connecteur dans une région gouvernementale à partir du site Web BlueXP SaaS. La meilleure option consiste donc à le faire à partir d'AWS Marketplace.



Vous pouvez également télécharger et installer le logiciel Connector sur un hôte Linux existant de votre réseau ou dans le cloud. ["Découvrez comment installer le connecteur sur un hôte Linux existant"](#).

Créez le connecteur dans une région commerciale d’AWS

Vous pouvez lancer l’instance Connector dans une région commerciale d’AWS directement à partir de l’offre AWS Marketplace pour BlueXP.

L’utilisateur IAM qui crée le connecteur doit disposer d’autorisations AWS Marketplace pour s’abonner et se désabonner.

Étapes

1. Configurez les autorisations dans AWS :
 - a. À partir de la console IAM, créez les politiques requises en copiant et en collant le contenu de "[Les règles IAM pour le connecteur](#)".
 - b. Créez un rôle IAM avec le type de rôle Amazon EC2 et associez les règles créées à l’étape précédente au rôle.
2. Accédez au "[BlueXP, page sur AWS Marketplace](#)" Pour déployer le connecteur à partir d’une ami :
3. Sur la page Marketplace, cliquez sur **Continuer pour s’abonner**, puis cliquez sur **Continuer la configuration**.

a

Delivery Methods Solutions Migration Mapping Assistant Your Saved List **2** Partners Sell in AWS Marketplace Amazon Web Services Home

Cloud Manager - Manual Installation without access keys

By: [NetApp, Inc.](#) Latest Version: 3.8.4

Read below for instructions on how to deploy Cloud Volumes ONTAP.

Linux/Unix ★★★★★ 6 AWS reviews

[Continue to Subscribe](#)

[Save to List](#)

Typical Total Price
\$0.226/hr
Total pricing per instance for services hosted on t3.xlarge in US East (N. Virginia). [View Details](#)

Overview Pricing Usage Support Reviews

Product Overview

Do NOT subscribe on this page unless instructed by NetApp or redirected here from the NetApp website.

This listing lets you manually launch a Cloud Manager instance without providing your AWS credentials. After launching the Cloud Manager software in AWS, you can access it by entering the instance's IP address in a web browser. If you subscribe here, you still need to subscribe on the listing below for PAYGO charges.

Highlights

- See Product Overview for instructions on how to deploy NetApp Cloud Manager.

b

Delivery Methods Solutions Migration Mapping Assistant Your Saved List **2** Partners Sell in AWS Marketplace Amazon Web Services Home

Cloud Manager - Manual Installation without access keys

[Continue to Configuration](#)

[< Product Detail](#) [Subscribe](#)

Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

Terms and Conditions

NetApp, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

- Modifiez l'une des options par défaut et cliquez sur **Continuer pour lancer**.
- Sous **choisir action**, sélectionnez **lancer via EC2**, puis cliquez sur **lancer**.

Ces étapes décrivent comment lancer l'instance à partir de la console EC2, car la console vous permet d'associer un rôle IAM à l'instance de connecteur. Cela n'est pas possible en utilisant l'action **lancer à partir du site Web**.

- Suivez les invites pour configurer et déployer l'instance :
 - Nom et balises** : saisissez un nom et des balises pour l'instance.
 - Image de l'application et de l'OS** : passez cette section. Le connecteur ami est déjà sélectionné.
 - Type d'instance** : selon la disponibilité de la région, choisissez l'un des types d'instance pris en

charge (t3.XLarge est recommandé).

["Vérifiez les conditions requises pour l'instance"](#).

- **Paire de clés (login)** : sélectionnez la paire de clés que vous souhaitez utiliser pour vous connecter en toute sécurité à l'instance.
- **Paramètres réseau** : modifiez les paramètres réseau selon vos besoins :
 - Choisissez le VPC et le sous-réseau souhaités.
 - Spécifiez si l'instance doit avoir une adresse IP publique.
 - Spécifiez les paramètres de pare-feu qui activent les méthodes de connexion requises pour l'instance de connecteur : SSH, HTTP et HTTPS.
- **Configurer le stockage** : conservez les options de stockage par défaut.
- **Détails avancés** : sous **profil d'instance IAM**, choisissez le rôle IAM que vous avez créé à l'étape 1.
- **Résumé** : consultez le résumé et cliquez sur **lancer l'instance**.

AWS lance le logiciel avec les paramètres spécifiés. L'instance de connecteur et le logiciel doivent s'exécuter dans environ cinq minutes.

7. Ouvrez un navigateur Web à partir d'un hôte connecté à l'instance Connector et saisissez l'URL suivante :

`https://ipaddress[]`

8. Une fois connecté, configurez le connecteur :
 - a. Spécifiez le compte NetApp à associer au connecteur.

["En savoir plus sur les comptes NetApp"](#).

- b. Entrez un nom pour le système.



9. Ouvrez un navigateur Web et accédez à <https://cloudmanager.netapp.com> Pour commencer à utiliser le connecteur avec BlueXP.

Le connecteur est désormais installé et configuré avec votre compte NetApp. BlueXP utilisera automatiquement ce connecteur lorsque vous créez de nouveaux environnements de travail. Mais si vous avez plus d'un connecteur, vous devrez le faire "[basculer entre eux](#)".

Si vous disposez de compartiments Amazon S3 sur le même compte AWS que celui sur lequel vous avez créé le connecteur, l'environnement de travail Amazon S3 s'affiche automatiquement sur la fenêtre Canvas. "[Découvrez ce que vous pouvez faire dans cet environnement de travail](#)".

Créez le connecteur dans une région du gouvernement AWS

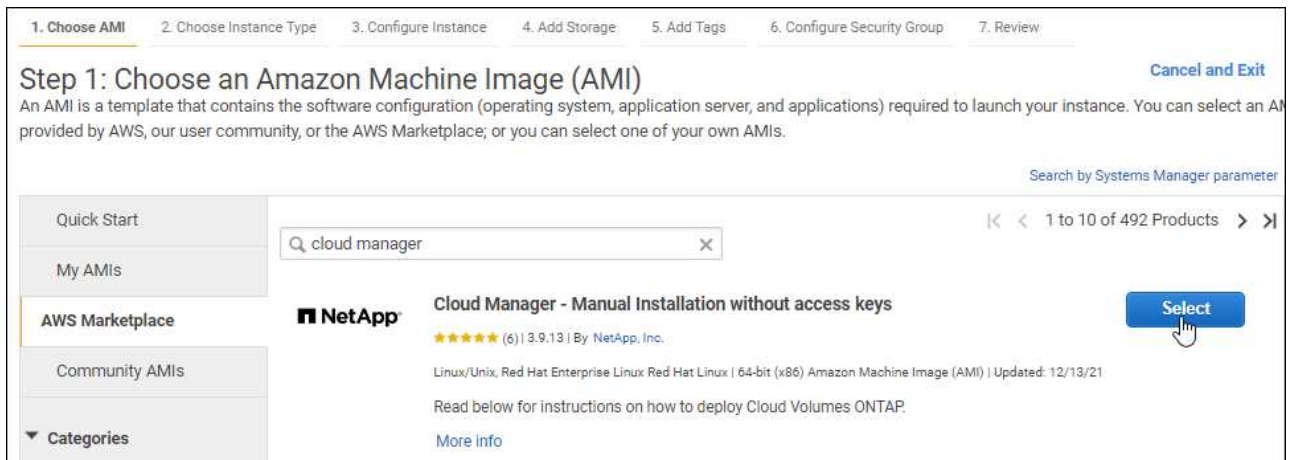
Pour déployer le connecteur dans une région AWS Government, vous devez accéder au service EC2 et sélectionner l'offre BlueXP depuis AWS Marketplace.

Étapes

1. Configurez les autorisations dans AWS :
 - a. À partir de la console IAM, créez votre propre politique en copiant et en collant le contenu de "[Politique IAM pour le connecteur](#)".
 - b. Créez un rôle IAM avec le type de rôle Amazon EC2 et associez la stratégie que vous avez créée à l'étape précédente au rôle.
2. Accédez à l'offre BlueXP sur AWS Marketplace.

L'utilisateur IAM doit disposer d'autorisations AWS Marketplace pour vous abonner et se désabonner.

- a. Ouvrez le service EC2 et sélectionnez **lancer l'instance**.
- b. Sélectionnez **AWS Marketplace**.
- c. Recherchez BlueXP et sélectionnez l'offre.



d. Cliquez sur **Continuer**.

3. Suivez les invites pour configurer et déployer l'instance :

- **Choisissez un type d'instance** : selon la disponibilité de la région, choisissez un des types d'instance pris en charge (t3.XLarge est recommandé).

"Vérifiez les conditions requises pour l'instance".

- **Configurer les détails de l'instance** : sélectionnez un VPC et un sous-réseau, choisissez le rôle IAM que vous avez créé à l'étape 1, activez la protection de terminaison (recommandée) et choisissez toutes les autres options de configuration qui répondent à vos exigences.

Number of instances	1	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-a76d91c2 VPC4QA (default)	Create new VPC
Subnet	subnet-39536c13 QASubnet1 us-east-1b 155 IP Addresses available	Create new subnet
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	Create new Capacity Reservation
IAM role	Cloud_Manager	Create new IAM role
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	

- **Ajouter stockage** : conservez les options de stockage par défaut.
- **Ajouter des balises** : saisissez des balises pour l'instance, si vous le souhaitez.
- **Configurer le groupe de sécurité** : spécifiez les méthodes de connexion requises pour l'instance de connecteur : SSH, HTTP et HTTPS.
- **Revue**: Passez en revue vos sélections et cliquez sur **lancer**.

AWS lance le logiciel avec les paramètres spécifiés. L'instance de connecteur et le logiciel doivent s'exécuter dans environ cinq minutes.

- Ouvrez un navigateur Web à partir d'un hôte connecté à l'instance Connector et saisissez l'URL suivante :

`https://ipaddress[]`

- Une fois connecté, configurez le connecteur :
 - Spécifiez le compte NetApp à associer au connecteur.

["En savoir plus sur les comptes NetApp"](#).

- Entrez un nom pour le système.



Le connecteur est désormais installé et configuré avec votre compte NetApp.

A chaque fois que vous souhaitez utiliser BlueXP, ouvrez votre navigateur Web et connectez-vous à l'adresse IP de l'instance de connecteur : `https://ipaddress[]`

Comme le connecteur a été déployé dans une région du gouvernement, il n'est pas accessible à partir de <https://cloudmanager.netapp.com>.

Ouvrez le port 3128 pour les messages AutoSupport

Si vous prévoyez de déployer des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible, BlueXP configure automatiquement Cloud Volumes ONTAP pour utiliser le connecteur comme serveur proxy.

La seule condition est de s'assurer que le groupe de sécurité du connecteur autorise les connexions *entrantes* sur le port 3128. Vous devrez ouvrir ce port après le déploiement du connecteur.

Si vous utilisez le groupe de sécurité par défaut pour Cloud Volumes ONTAP, aucune modification n'est nécessaire pour son groupe de sécurité. Mais si vous prévoyez de définir des règles de trafic sortant strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le groupe de sécurité Cloud Volumes ONTAP autorise les connexions *sortantes* sur le port 3128.

Créez un connecteur à partir d'Azure Marketplace

Pour une région commerciale d'Azure, il est préférable de créer un connecteur

directement depuis BlueXP, mais vous pouvez lancer un connecteur depuis Azure Marketplace, si vous préférez. Pour les régions gouvernementales d’Azure, vous ne pouvez pas déployer le connecteur dans une région gouvernementale à partir du site Web BlueXP SaaS. La meilleure option consiste donc à le faire à partir d’Azure Marketplace.



Vous pouvez également télécharger et installer le logiciel Connector sur un hôte Linux existant de votre réseau ou dans le cloud. ["Découvrez comment installer le connecteur sur un hôte Linux existant"](#).

Création d’un connecteur dans Azure

Déployez le connecteur dans Azure à l’aide de l’image contenue dans Azure Marketplace, puis connectez-vous au connecteur pour spécifier votre compte NetApp.

Étapes

1. Rendez-vous sur la page NetApp Connector VM du Marketplace Azure.
 - ["Page Azure Marketplace pour les régions commerciales"](#)
 - ["Page Azure Marketplace pour les régions Azure Government"](#)
2. Cliquez sur **l’obtenir maintenant**, puis sur **Continuer**.
3. Sur le portail Azure, cliquez sur **Créer** et suivez les étapes de configuration de la machine virtuelle.

Noter les éléments suivants lors de la configuration de la machine virtuelle :

- Le connecteur offre des performances optimales avec des disques durs ou SSD.
- Choisissez une taille de machine virtuelle qui répond aux exigences en matière de CPU et de RAM. Nous recommandons DS3 v2.

["Vérifier les exigences relatives aux machines virtuelles"](#).

- Pour le groupe de sécurité réseau, le connecteur nécessite des connexions entrantes via SSH, HTTP et HTTPS.

["En savoir plus sur les règles de groupe de sécurité pour le connecteur"](#).

- Sous **Management**, activez **l’identité gérée attribuée par le système** pour le connecteur en sélectionnant **On**.

Ce paramètre est important car une identité gérée permet à la machine virtuelle Connector de s’identifier à Azure Active Directory sans fournir d’informations d’identification. ["En savoir plus sur les identités gérées pour les ressources Azure"](#).

4. Dans la page **Revue + créer**, vérifiez vos sélections et cliquez sur **Créer** pour démarrer le déploiement.

Azure déploie la machine virtuelle avec les paramètres spécifiés. Le logiciel de la machine virtuelle et du connecteur doit s’exécuter en cinq minutes environ.

5. Ouvrez un navigateur Web à partir d’un hôte connecté à la machine virtuelle Connector et entrez l’URL suivante :

`https://ipaddress[]`

6. Une fois connecté, configurez le connecteur :
 - a. Spécifiez le compte NetApp à associer au connecteur.
"En savoir plus sur les comptes NetApp".
 - b. Entrez un nom pour le système.



Le connecteur est désormais installé et configuré avec votre compte NetApp.

Si le connecteur se trouve dans une région commerciale d'Azure, ouvrez un navigateur Web et rendez-vous sur <https://cloudmanager.netapp.com> Pour commencer à utiliser le connecteur avec BlueXP.

Si le connecteur se trouve dans une région d'administration Azure, vous pouvez utiliser BlueXP en ouvrant votre navigateur Web et en vous connectant à l'adresse IP de l'instance de connecteur : [https://ipaddress\[\]](https://ipaddress[])

Comme le connecteur a été déployé dans une région du gouvernement, il n'est pas accessible à partir de <https://cloudmanager.netapp.com>.

Octroi d'autorisations Azure

Lorsque vous avez déployé le connecteur dans Azure, vous devez avoir activé un "identité gérée attribuée par le système". Vous devez maintenant accorder les autorisations Azure requises en créant un rôle personnalisé, puis en attribuant le rôle à la machine virtuelle Connector pour un ou plusieurs abonnements.

Étapes

1. Création d'un rôle personnalisé :

- Copier le contenu du "[Autorisations de rôle personnalisées pour le connecteur](#)" Et les enregistrer dans un fichier JSON.
- 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.

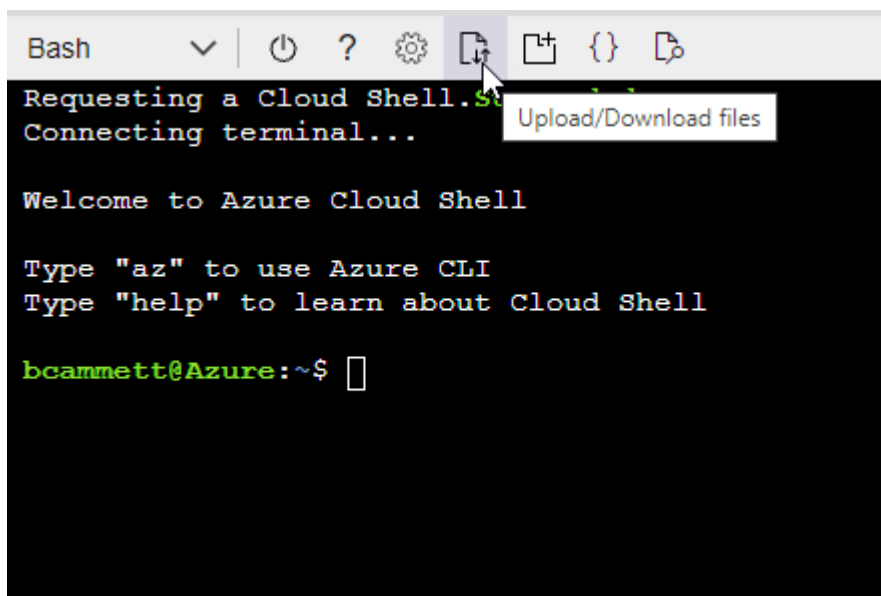
Exemple

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

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

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

- Démarrer "[Shell cloud Azure](#)" Et choisissez l'environnement Bash.
- Téléchargez le fichier JSON.



- Entrez la commande Azure CLI suivante :

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

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

2. Attribuez le rôle à la machine virtuelle Connector pour un ou plusieurs abonnements :

- a. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer des systèmes Cloud Volumes ONTAP.
- b. Cliquez sur **contrôle d'accès (IAM) > Ajouter > Ajouter affectation de rôle**.
- c. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et cliquez sur **Next**.



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

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

- Attribuez l'accès à une identité **gérée**.
- Cliquez sur **Sélectionner les membres**, sélectionnez l'abonnement dans lequel la machine virtuelle de connecteur a été créée, choisissez **machine virtuelle**, puis sélectionnez la machine virtuelle de connecteur.
- Cliquez sur **Sélectionner**.
- Cliquez sur **Suivant**.

e. Cliquez sur **Revue + affecter**.

- f. Si vous souhaitez déployer Cloud Volumes ONTAP à partir d'abonnements supplémentaires, passez à cet abonnement, puis répétez ces étapes.

Le connecteur dispose désormais des autorisations nécessaires pour gérer les ressources et les processus au sein de votre environnement de cloud public. BlueXP utilisera automatiquement ce connecteur lorsque vous créez de nouveaux environnements de travail. Mais si vous avez plus d'un connecteur, vous devrez le faire ["basculer entre eux"](#).

Si vous disposez d'un stockage Azure Blob dans le même compte Azure que celui sur lequel vous avez créé le connecteur, un environnement de travail Azure Blob s'affiche automatiquement sur la toile. ["Découvrez ce que vous pouvez faire dans cet environnement de travail"](#).

Ouvrez le port 3128 pour les messages AutoSupport

Si vous prévoyez de déployer des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible, BlueXP configure automatiquement Cloud Volumes ONTAP pour utiliser le connecteur comme serveur proxy.

La seule condition est de s'assurer que le groupe de sécurité du connecteur autorise les connexions *entrantes* sur le port 3128. Vous devrez ouvrir ce port après le déploiement du connecteur.

Si vous utilisez le groupe de sécurité par défaut pour Cloud Volumes ONTAP, aucune modification n'est nécessaire pour son groupe de sécurité. Mais si vous prévoyez de définir des règles de trafic sortant strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le groupe de sécurité Cloud Volumes ONTAP autorise les connexions *sortantes* sur le port 3128.

Installez le connecteur sur un hôte Linux existant ayant accès à Internet

La manière la plus courante de créer un connecteur est directement depuis BlueXP ou depuis le marché d'un fournisseur cloud. Mais vous avez la possibilité de télécharger et d'installer le logiciel Connector sur un hôte Linux existant de votre réseau ou dans le cloud. Ces étapes sont spécifiques aux hôtes disposant d'un accès Internet.

["Découvrez d'autres méthodes de déploiement d'un connecteur".](#)



Pour créer un système Cloud Volumes ONTAP dans Google Cloud, vous devez disposer d'un connecteur exécuté dans Google Cloud. Vous ne pouvez pas utiliser un connecteur exécuté sur AWS, Azure ou sur site.

Vérifiez les besoins de l'hôte

Le logiciel du connecteur doit être exécuté sur un hôte qui répond à des exigences spécifiques du système d'exploitation, de la RAM, des ports, etc.

Un hôte dédié est requis

Le connecteur n'est pas pris en charge sur un hôte partagé avec d'autres applications. L'hôte doit être un hôte dédié.

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Type d'instance AWS EC2

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons une instance t3.XLarge.

Taille des machines virtuelles Azure

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons DS3 v2.

Type de machine GCP

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons n2-standard-4.

Ce connecteur est pris en charge dans Google Cloud sur une instance de machine virtuelle avec un système d'exploitation pris en charge ["Fonctionnalités MV blindées"](#)

Systèmes d'exploitation pris en charge

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.6

Le système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels

tiers requis pendant l'installation du connecteur.

Le connecteur est pris en charge sur les versions en anglais de ces systèmes d'exploitation.

Hyperviseur

Un hyperviseur bare Metal ou hébergé certifié pour exécuter CentOS ou Red Hat Enterprise Linux <https://access.redhat.com/certified-hypervisors>["Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"^]

Espace disque dans /opt

100 Gio d'espace doit être disponible

Espace disque dans /var

20 Gio d'espace doit être disponible

Moteur Docker

Docker Engine version 19 ou ultérieure est requis sur l'hôte avant d'installer le connecteur. "[Voir les instructions d'installation](#)"

Accès Internet sortant

Le programme d'installation du connecteur doit accéder aux URL suivantes pendant le processus d'installation :

- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>
- https://*.blob.core.windows.net ou <https://hub.docker.com>

L'hôte peut essayer de mettre à jour les packages du système d'exploitation lors de l'installation. L'hôte peut contacter différents sites de mise en miroir pour ces packages OS.

Poser le connecteur

Après avoir vérifié que vous disposez d'un hôte Linux pris en charge, vous pouvez obtenir le logiciel Connector, puis l'installer.

Les privilèges root sont requis pour installer le connecteur.

Description de la tâche

- L'installation installe les outils de ligne de commande AWS (awscli), afin d'activer les procédures de reprise à partir du support NetApp.

Si vous recevez un message indiquant que l'installation de awscli a échoué, vous pouvez ignorer le message en toute sécurité. Le connecteur peut fonctionner sans outils.

- Le programme d'installation disponible sur le site du support NetApp peut être une version antérieure. Après l'installation, le connecteur se met automatiquement à jour si une nouvelle version est disponible.

Étapes

1. Vérifiez que docker est activé et exécuté.

```
sudo systemctl enable docker && sudo systemctl start docker
```

2. Téléchargez le logiciel du connecteur à partir du ["Site de support NetApp"](#), Puis copiez-le sur l'hôte Linux.

Pour obtenir de l'aide sur la connexion et la copie du fichier vers une instance EC2 dans AWS, reportez-vous à la section ["Documentation AWS : connexion à votre instance Linux à l'aide de SSH"](#).

3. Attribuez des autorisations pour exécuter le script.

```
chmod +x OnCommandCloudManager-V3.9.23.sh
```

4. Exécutez le script d'installation.

Si vous disposez d'un serveur proxy, vous devez entrer les paramètres de commande comme indiqué ci-dessous. Le programme d'installation ne vous invite pas à fournir des informations sur un proxy.

```
./OnCommandCloudManager-V3.9.23.sh --proxy  
http://occm:password@10.0.0.30:9090/ --cacert /root/rootca.pem
```

Le connecteur est maintenant installé. À la fin de l'installation, le service connecteur (ocm) redémarre deux fois si vous avez spécifié un serveur proxy.

5. Ouvrez un navigateur Web et entrez l'URL suivante :

[https://ipaddress\[\]](https://ipaddress[])

Ipaddress peut être localhost, une adresse IP privée ou une adresse IP publique, selon la configuration de l'hôte. Par exemple, si le connecteur est dans le Cloud public sans adresse IP publique, vous devez entrer une adresse IP privée à partir d'un hôte qui a une connexion à l'hôte du connecteur.

6. S'inscrire ou se connecter.
7. Si vous avez installé le connecteur dans Google Cloud, configurez un compte de service disposant des autorisations nécessaires à BlueXP pour créer et gérer des systèmes Cloud Volumes ONTAP dans des projets.
 - a. ["Créer un rôle dans GCP"](#) qui inclut les autorisations définies dans le ["Règle de connecteur pour GCP"](#).
 - b. ["Créez un compte de service GCP et appliquez le rôle personnalisé que vous venez de créer"](#).
 - c. ["Associer ce compte de service à la VM Connector"](#).
 - d. Si vous souhaitez déployer Cloud Volumes ONTAP dans d'autres projets, ["Accordez l'accès en ajoutant le compte de service avec le rôle BlueXP à ce projet"](#). Vous devrez répéter cette étape pour chaque projet.
8. Une fois connecté, configurez BlueXP :
 - a. Spécifiez le compte NetApp à associer au connecteur.
["En savoir plus sur les comptes NetApp"](#).
 - b. Entrez un nom pour le système.



Le connecteur est désormais installé et configuré avec votre compte NetApp. BlueXP utilisera automatiquement ce connecteur lorsque vous créez de nouveaux environnements de travail.

Configurez des autorisations pour que BlueXP puisse gérer les ressources et les processus au sein de votre environnement de cloud public :

- AWS : ["Configurez un compte AWS, puis ajoutez-le à BlueXP"](#)
- Azure : ["Configurez un compte Azure, puis ajoutez-le à BlueXP"](#)
- Google Cloud : voir étape 7 ci-dessus

Installez le connecteur sur site sans accès à Internet

Vous pouvez installer le connecteur sur un hôte Linux sur site qui n'a pas accès à Internet. Vous pouvez ensuite découvrir les clusters ONTAP sur site, répliquer les données entre eux, sauvegarder des volumes à l'aide de Cloud Backup et les analyser avec Cloud Data Sense.

Ces instructions d'installation s'affichent spécifiquement dans le cas d'utilisation décrit ci-dessus. ["Découvrez d'autres méthodes de déploiement d'un connecteur"](#).

Vérifiez les besoins de l'hôte

Le logiciel du connecteur doit être exécuté sur un hôte qui répond à des exigences spécifiques du système

d'exploitation, de la RAM, des ports, etc.

Un hôte dédié est requis

Le connecteur n'est pas pris en charge sur un hôte partagé avec d'autres applications. L'hôte doit être un hôte dédié.

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Systèmes d'exploitation pris en charge

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.6

Le système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis pendant l'installation du connecteur.

Le connecteur est pris en charge sur les versions en anglais de ces systèmes d'exploitation.

Hyperviseur

Un hyperviseur bare Metal ou hébergé certifié pour exécuter CentOS ou Red Hat Enterprise Linux <https://access.redhat.com/certified-hypervisors>["Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"]

Type de disque

Un disque SSD est requis

Espace disque dans /opt

100 Gio d'espace doit être disponible

Espace disque dans /var

20 Gio d'espace doit être disponible

Moteur Docker

Docker Engine version 19 ou ultérieure est requis sur l'hôte avant d'installer le connecteur. ["Voir les instructions d'installation"](#)

Poser le connecteur

Après avoir vérifié que vous disposez d'un hôte Linux pris en charge, vous pouvez obtenir le logiciel Connector, puis l'installer.

Les privilèges root sont requis pour installer le connecteur.

Étapes

1. Vérifiez que docker est activé et exécuté.

```
sudo systemctl enable docker && sudo systemctl start docker
```

2. Téléchargez le logiciel du connecteur à partir du "[Site de support NetApp](#)"
3. Copiez le programme d'installation sur l'hôte Linux.
4. Attribuez des autorisations pour exécuter le script.

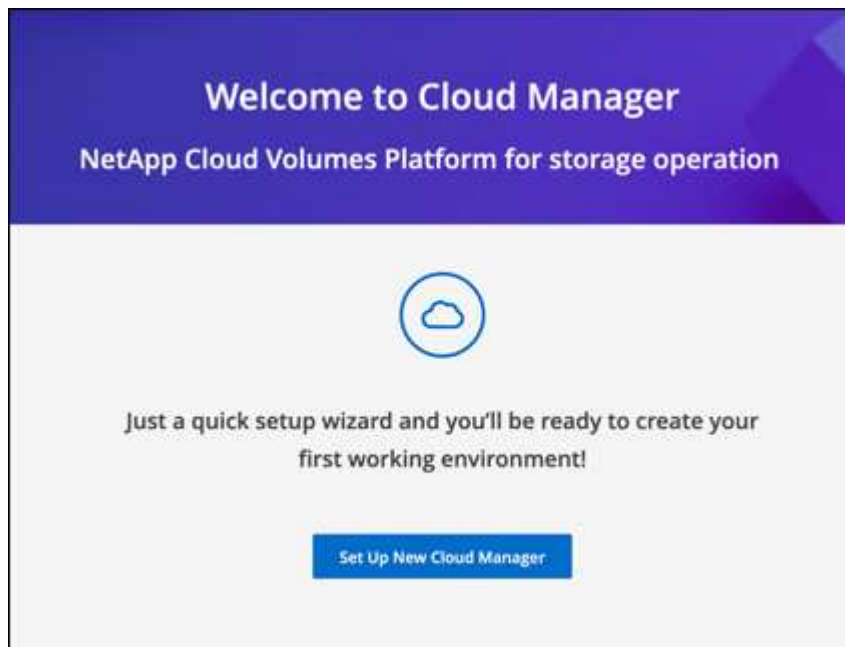
```
chmod +x /path/cloud-manager-connector-offline-v3.9.23
```

5. Exécutez le script d'installation :

```
sudo /path/cloud-manager-connector-offline-v3.9.23
```

6. Ouvrez un navigateur Web et entrez `https://ipaddress[]` Où *ipaddress* est l'adresse IP de l'hôte Linux.

Vous devriez voir l'écran suivant.



7. Cliquez sur **configurer New BlueXP** et suivez les invites pour configurer le système.
 - **Détails du système** : saisissez un nom pour le connecteur et le nom de votre société.

- **Créer un utilisateur Admin** : créez l'utilisateur admin pour le système.

Ce compte utilisateur s'exécute localement sur le système. Il n'y a pas de connexion au service auth0 disponible via BlueXP.

- **Revue** : consultez les détails, acceptez le contrat de licence, puis cliquez sur **configurer**.

8. Connectez-vous à BlueXP à l'aide de l'utilisateur admin que vous venez de créer.

Le connecteur est maintenant installé et vous pouvez commencer à utiliser les fonctions BlueXP disponibles dans un déploiement de site sombre.

Que dois-je faire ?'s ensuite ?

- ["Découvrez les clusters ONTAP sur site"](#)
- ["Réplication des données entre les clusters ONTAP sur site"](#)
- ["Sauvegarde des données de volumes ONTAP sur site dans StorageGRID à l'aide de Cloud Backup"](#)
- ["Analysez les données de volume ONTAP sur site à l'aide de la solution Cloud Data Sense"](#)

Dès que de nouvelles versions du logiciel Connector sont disponibles, elles seront publiées sur le site de support NetApp. ["Apprenez à mettre à niveau le connecteur"](#).

Recherche de l'ID système d'un connecteur

Pour vous aider à vous lancer, votre représentant NetApp peut vous demander l'ID système d'un connecteur. L'ID est généralement utilisé à des fins de licence et de dépannage.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide.
2. Cliquez sur **support > connecteur**.

L'ID du système apparaît en haut.

Exemple



Gestion des connecteurs existants

Après avoir créé un ou plusieurs connecteurs, vous pouvez les gérer en passant d'un connecteur à l'autre, en vous connectant à l'interface utilisateur locale s'exécutant sur un connecteur, et plus encore.

Basculer entre les connecteurs

Si vous avez plusieurs connecteurs, vous pouvez passer de l'un à l'autre pour voir les environnements de travail associés à un connecteur spécifique.

Imaginons par exemple que vous travaillez dans un environnement multicloud. Vous avez peut-être un connecteur dans AWS et un autre dans Google Cloud. Il faudrait basculer entre ces connecteurs pour gérer les systèmes Cloud Volumes ONTAP présents dans ces clouds.

Étape

1. Cliquez sur la liste déroulante **Connector**, sélectionnez un autre connecteur, puis cliquez sur **Switch**.



BlueXP actualise et affiche les environnements de travail associés au connecteur sélectionné.

Accédez à l'interface utilisateur locale

Bien que vous devriez effectuer presque toutes les tâches à partir de l'interface utilisateur SaaS, une interface utilisateur locale est toujours disponible sur le connecteur. Si vous accédez à BlueXP à partir d'une région du gouvernement ou d'un site qui ne dispose pas d'un accès Internet sortant, vous devez utiliser l'interface utilisateur locale s'exécutant sur le connecteur.

Étapes

1. Ouvrez un navigateur Web et entrez l'URL suivante :

`https://ipaddress[]`

Ipaddress peut être localhost, une adresse IP privée ou une adresse IP publique, selon la configuration de l'hôte. Par exemple, si le connecteur est dans le Cloud public sans adresse IP publique, vous devez entrer une adresse IP privée à partir d'un hôte qui a une connexion à l'hôte du connecteur.

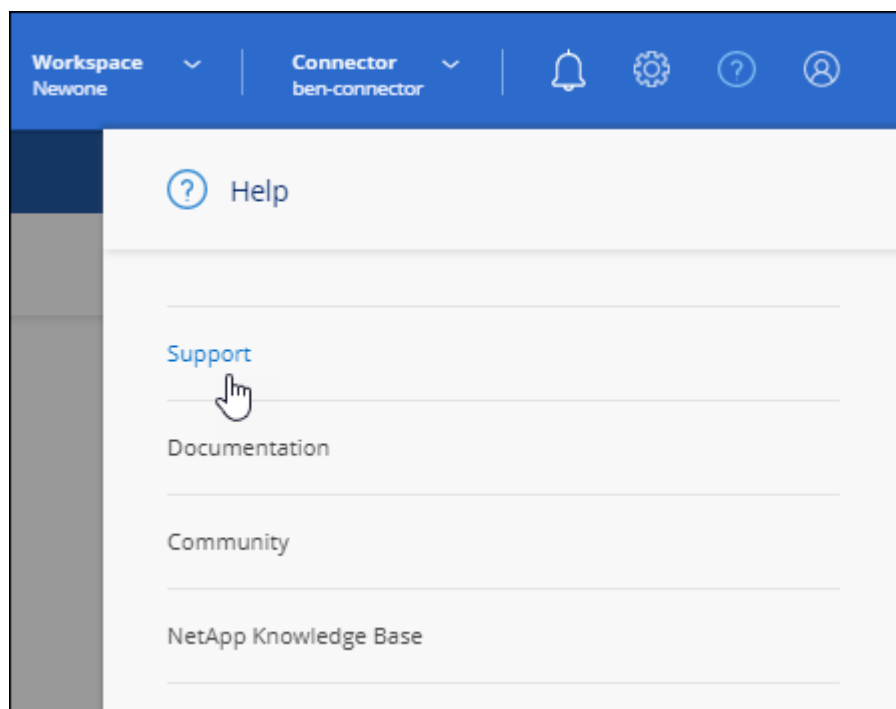
2. Entrez votre nom d'utilisateur et votre mot de passe pour vous connecter.

Téléchargez ou envoyez un message AutoSupport

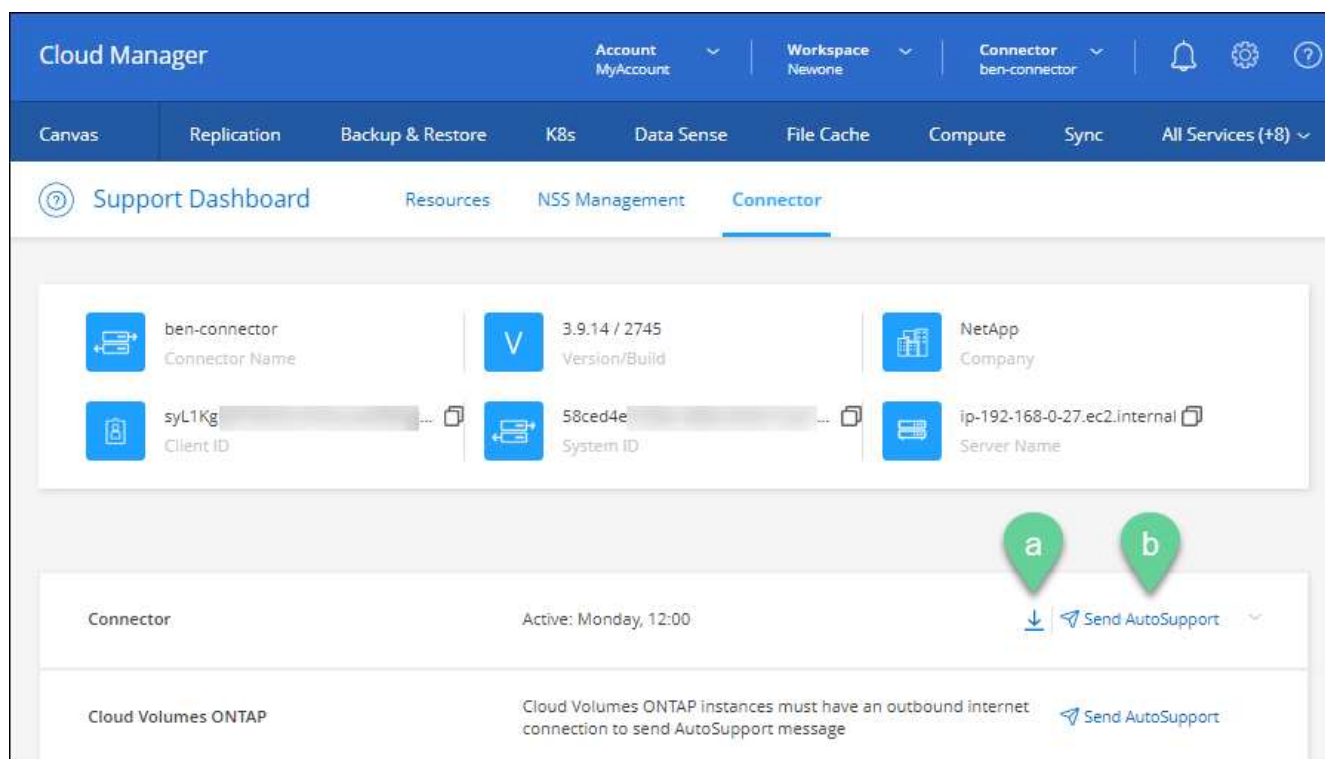
En cas de problème, les équipes NetApp peuvent vous demander d'envoyer un message AutoSupport au support NetApp à des fins de dépannage.

Étapes

1. Connectez-vous à l'interface utilisateur locale du connecteur, comme décrit dans la section ci-dessus.
2. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



3. Cliquez sur **connecteur**.
4. Selon le mode d'envoi des informations au support NetApp, choisissez l'une des options suivantes :
 - a. Sélectionnez l'option pour télécharger le message AutoSupport sur votre ordinateur local. Vous pouvez ensuite l'envoyer au support NetApp selon la méthode qui vous convient.
 - b. Cliquez sur **Envoyer AutoSupport** pour envoyer directement le message au support NetApp.



Connectez-vous à la machine virtuelle Linux

Si vous devez vous connecter à la machine virtuelle Linux sur laquelle s'exécute le connecteur, vous pouvez utiliser les options de connectivité disponibles auprès de votre fournisseur de cloud.

AWS

Lorsque vous avez créé l'instance Connector dans AWS, vous avez fourni une clé d'accès AWS et une clé secrète. Vous pouvez utiliser cette paire de clés vers SSH à l'instance.

["AWS Docs : connectez-vous à votre instance Linux"](#)

Azure

Lorsque vous avez créé la machine virtuelle Connector dans Azure, vous avez choisi de vous authentifier avec un mot de passe ou une clé publique SSH. Utilisez la méthode d'authentification que vous avez choisie pour vous connecter à la machine virtuelle.

["Azure Docs : connexion SSH à votre machine virtuelle"](#)

Google Cloud

Vous ne pouvez pas spécifier de méthode d'authentification lorsque vous créez un connecteur dans Google Cloud. Vous pouvez toutefois vous connecter à l'instance de machine virtuelle Linux à l'aide de Google Cloud Console ou de Google Cloud CLI (gCloud).

["Google Cloud Docs : connectez-vous aux machines virtuelles Linux"](#)

Appliquer les mises à jour de sécurité

Mettez à jour le système d'exploitation sur le connecteur pour vous assurer qu'il a été corrigé avec les dernières mises à jour de sécurité.

Étapes

1. Accéder au shell CLI sur l'hôte du connecteur.
2. Exécutez les commandes suivantes avec des privilèges élevés :

```
sudo -s
service netapp-service-manager stop
yum -y update --security
service netapp-service-manager start
```

Modifiez l'adresse IP d'un connecteur

Si votre entreprise l'exige, vous pouvez modifier l'adresse IP interne et l'adresse IP publique de l'instance de connecteur qui est automatiquement attribuée par votre fournisseur de cloud.

Étapes

1. Suivez les instructions de votre fournisseur de cloud pour modifier l'adresse IP locale ou l'adresse IP publique (ou les deux) de l'instance de connecteur.
2. Si vous avez modifié l'adresse IP publique et que vous devez vous connecter à l'interface utilisateur locale

s'exécutant sur le connecteur, redémarrez l'instance de connecteur pour enregistrer la nouvelle adresse IP avec BlueXP.

3. Si vous avez modifié l'adresse IP privée, mettez à jour l'emplacement de sauvegarde des fichiers de configuration Cloud Volumes ONTAP de manière à ce que les sauvegardes soient envoyées à la nouvelle adresse IP privée sur le connecteur.
 - a. Exécutez la commande suivante depuis l'interface de ligne de commande de Cloud Volumes ONTAP pour supprimer la cible de sauvegarde actuelle :

```
system configuration backup settings modify -destination ""
```

- b. Allez à BlueXP et ouvrez l'environnement de travail.
- c. Cliquez sur le menu et sélectionnez **Avancé > sauvegarde de la configuration**.
- d. Cliquez sur **définir la cible de sauvegarde**.

Modifier les URI d'un connecteur

Ajouter et supprimer les URI d'un connecteur.

Étapes

1. Cliquez sur la liste déroulante **Connector** dans l'en-tête BlueXP.
2. Cliquez sur **gérer les connecteurs**.
3. Cliquez sur le menu d'action d'un connecteur et cliquez sur **Modifier URI**.
4. Ajoutez et supprimez des URI, puis cliquez sur **appliquer**.

Corrigez les échecs de téléchargement lors de l'utilisation d'une passerelle Google Cloud NAT

Le connecteur télécharge automatiquement les mises à jour logicielles pour Cloud Volumes ONTAP. Le téléchargement peut échouer si votre configuration utilise une passerelle NAT Google Cloud. Vous pouvez corriger ce problème en limitant le nombre de pièces dans lesquelles l'image logicielle est divisée. Cette étape doit être effectuée à l'aide de l'API BlueXP.

Étape

1. Soumettre une demande PUT à `/ocm/config` au format JSON suivant :

```
{
  "maxDownloadSessions": 32
}
```

La valeur de `maxDownloadSessions` peut être 1 ou n'importe quel entier supérieur à 1. Si la valeur est 1, l'image téléchargée ne sera pas divisée.

Notez que 32 est un exemple de valeur. La valeur que vous devez utiliser dépend de votre configuration NAT et du nombre de sessions que vous pouvez avoir simultanément.

["En savoir plus sur l'appel API /ocm/config"](#).

Mettez à niveau le connecteur sur site sans accès à Internet

Si vous "[Installez le connecteur sur un hôte sur site qui ne dispose pas d'un accès Internet](#)", Vous pouvez mettre à niveau le connecteur lorsqu'une version plus récente est disponible sur le site de support NetApp.

Le connecteur doit redémarrer pendant le processus de mise à niveau pour que l'interface utilisateur ne soit pas disponible pendant la mise à niveau.

Étapes

1. Téléchargez le logiciel du connecteur à partir du "[Site de support NetApp](#)".
2. Copiez le programme d'installation sur l'hôte Linux.
3. Attribuez des autorisations pour exécuter le script.

```
chmod +x /path/cloud-manager-connector-offline-v3.9.14
```

4. Exécutez le script d'installation :

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

5. Une fois la mise à niveau terminée, vous pouvez vérifier la version du connecteur en accédant à **aide > support > connecteur**.

Qu'en est-il des mises à niveau logicielles sur les hôtes disposant d'un accès Internet ?

Le connecteur met automatiquement à jour son logiciel avec la dernière version, tant qu'il dispose d'un accès Internet sortant pour obtenir la mise à jour du logiciel.

Retirer les connecteurs de BlueXP

Si un connecteur est inactif, vous pouvez le retirer de la liste des connecteurs dans BlueXP. Vous pouvez le faire si vous avez supprimé la machine virtuelle Connector ou si vous avez désinstallé le logiciel Connector.

Notez ce qui suit sur le retrait d'un connecteur :

- Cette action ne supprime pas la machine virtuelle.
- Cette action ne peut pas être rétablie — une fois que vous avez supprimé un connecteur de BlueXP, vous ne pouvez pas l'ajouter à nouveau

Étapes

1. Cliquez sur la liste déroulante **Connector** dans l'en-tête BlueXP.
2. Cliquez sur **gérer les connecteurs**.
3. Cliquez sur le menu d'action d'un connecteur inactif et cliquez sur **Supprimer le connecteur**.



4. Entrez le nom du connecteur à confirmer, puis cliquez sur Supprimer.

BlueXP supprime le connecteur de ses enregistrements.

Désinstallez le logiciel du connecteur

Désinstallez le logiciel du connecteur pour résoudre les problèmes ou pour supprimer définitivement le logiciel de l'hôte. Les étapes que vous devez utiliser dépendent de l'installation ou non du connecteur sur un hôte disposant d'un accès Internet ou sur un hôte d'un réseau restreint ne disposant pas d'un accès Internet.

Désinstallation à partir d'un hôte disposant d'un accès à Internet

Le connecteur en ligne inclut un script de désinstallation que vous pouvez utiliser pour désinstaller le logiciel.

Étape

1. À partir de l'hôte Linux, exécutez le script de désinstallation :

`/opt/application/netapp/cloudmanager/bin/uninstall.sh [silencieux]`

silent exécute le script sans vous demander de confirmer.

Désinstallation à partir d'un hôte sans accès à Internet

Utilisez ces commandes si vous avez téléchargé le logiciel Connector depuis le site de support NetApp et l'avez installé dans un réseau restreint qui ne dispose pas d'un accès Internet.

Étape

1. Depuis l'hôte Linux, exécutez les commandes suivantes :

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v
rm -rf /opt/application/netapp/ds
```

Gestion d'un certificat HTTPS pour l'accès sécurisé

Par défaut, BlueXP utilise un certificat auto-signé pour l'accès HTTPS à la console Web. Vous pouvez installer un certificat signé par une autorité de certification (CA), qui offre une meilleure protection de la sécurité qu'un certificat auto-signé.

Avant de commencer

Vous devez créer un connecteur avant de pouvoir modifier les paramètres BlueXP. "[Découvrez comment](#)".

Installation d'un certificat HTTPS

Installez un certificat signé par une autorité de certification pour un accès sécurisé.

Étapes

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



2. Dans la page Configuration HTTPS, installez un certificat en générant une requête de signature de certificat (CSR) ou en installant votre propre certificat signé par l'autorité de certification :

Option	Description
Générez une RSC	<ol style="list-style-type: none">a. Entrez le nom d'hôte ou le DNS de l'hôte du connecteur (son nom commun), puis cliquez sur generate CSR. BlueXP affiche une demande de signature de certificat.b. Utilisez la RSC pour envoyer une demande de certificat SSL à une autorité de certification. Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.c. Téléchargez le fichier de certificat, puis cliquez sur installer.
Installez votre propre certificat signé par l'autorité de certification	<ol style="list-style-type: none">a. Sélectionnez installer le certificat signé CA.b. Chargez le fichier de certificat et la clé privée, puis cliquez sur installer. Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.

BlueXP utilise désormais le certificat signé par l'autorité de certification pour fournir un accès HTTPS sécurisé. L'image suivante montre un compte BlueXP configuré pour un accès sécurisé :



Renouvellement du certificat HTTPS BlueXP

Vous devez renouveler le certificat HTTPS BlueXP avant son expiration pour garantir un accès sécurisé à la console BlueXP. Si vous ne renouvelez pas le certificat avant son expiration, un avertissement s'affiche lorsque les utilisateurs accèdent à la console Web via HTTPS.

Étapes

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

Des détails sur le certificat BlueXP s'affichent, y compris la date d'expiration.

2. Cliquez sur **Modifier le certificat** et suivez les étapes pour générer une RSC ou installer votre propre certificat signé par une CA.

BlueXP utilise le nouveau certificat signé par une autorité de certification pour fournir un accès HTTPS sécurisé.

Configuration d'un connecteur pour utiliser un serveur proxy HTTP

Si vos stratégies d'entreprise nécessitent l'utilisation d'un serveur proxy pour toutes les communications HTTP vers Internet, vous devez configurer vos connecteurs pour qu'ils utilisent un serveur proxy HTTP. Le serveur proxy peut se trouver dans le cloud ou dans votre réseau.



BlueXP ne prend pas en charge l'utilisation d'un proxy HTTPS avec le connecteur.

La configuration du connecteur pour utiliser un serveur proxy HTTP fournit un accès Internet sortant si une adresse IP publique ou une passerelle NAT n'est pas disponible. Ce serveur proxy fournit uniquement le connecteur avec une connexion sortante. Il n'offre aucune connectivité pour les systèmes Cloud Volumes

ONTAP.

Si les systèmes Cloud Volumes ONTAP ne disposent pas d'une connexion Internet sortante pour envoyer des messages AutoSupport, BlueXP configure automatiquement ces systèmes Cloud Volumes ONTAP pour utiliser un serveur proxy inclus avec le connecteur. La seule condition est de s'assurer que le groupe de sécurité du connecteur autorise les connexions entrantes sur le port 3128. Vous devrez ouvrir ce port après le déploiement du connecteur.

Activez un proxy sur un connecteur

Lorsque vous configurez un connecteur pour utiliser un serveur proxy, ce connecteur et les systèmes Cloud Volumes ONTAP qu'il gère (y compris les médiateurs HA) utilisent tous le serveur proxy.

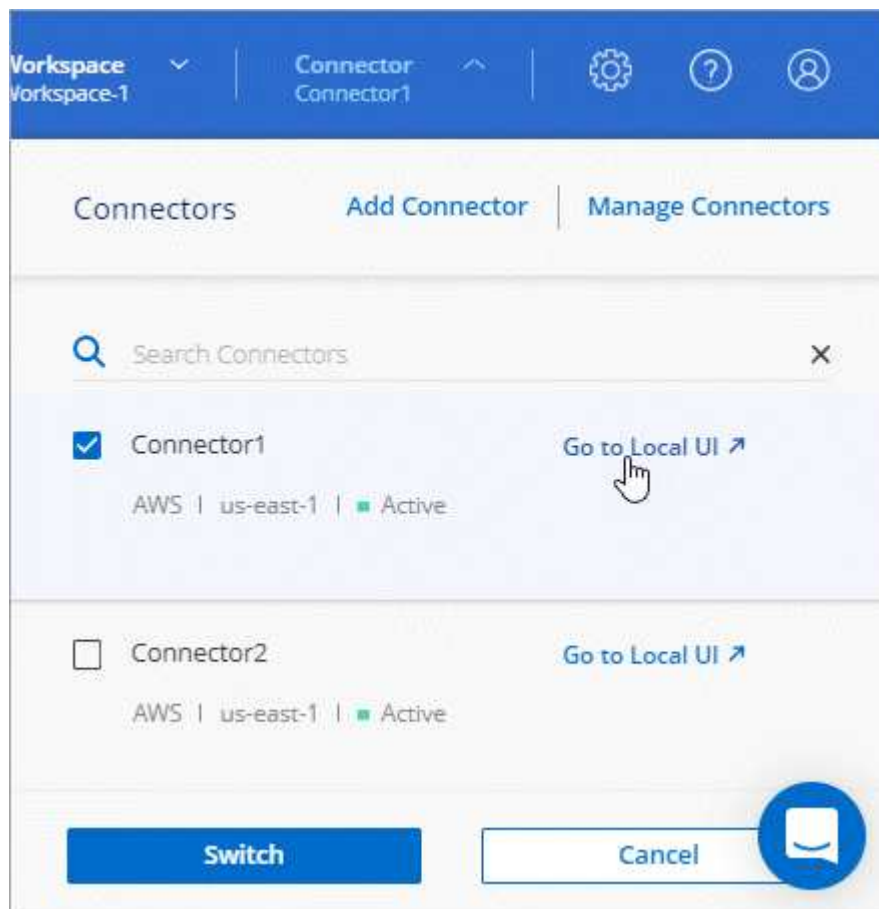
Notez que cette opération redémarre le connecteur. Assurez-vous que le connecteur n'effectue aucune opération avant de continuer.

Étapes

1. "[Connectez-vous à l'interface BlueXP SaaS](#)" À partir d'une machine dotée d'une connexion réseau à l'instance de connecteur.

Si le connecteur n'est pas doté d'une adresse IP publique, vous aurez besoin d'une connexion VPN ou vous devrez vous connecter à partir d'un hôte de secours situé sur le même réseau que le connecteur.

2. Cliquez sur la liste déroulante **Connector**, puis cliquez sur **allez à l'interface utilisateur locale** pour un connecteur spécifique.



L'interface BlueXP exécutée sur le connecteur se charge dans un nouvel onglet de navigateur.

3. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres, puis sélectionnez **Paramètres du connecteur**.



4. Sous **général**, cliquez sur **Configuration du proxy HTTP**.
5. Configurez le proxy :
 - a. Cliquez sur **Activer proxy**.
 - b. Spécifiez le serveur à l'aide de la syntaxe `http://address:port[]`
 - c. Spécifiez un nom d'utilisateur et un mot de passe si une authentification de base est requise pour le serveur
 - d. Cliquez sur **Enregistrer**.



BlueXP ne prend pas en charge les mots de passe contenant le caractère @.

Activation du trafic API direct

Si vous avez configuré un serveur proxy, vous pouvez envoyer des appels API directement à BlueXP sans passer par le proxy. Cette option est prise en charge avec des connecteurs s'exécutant dans AWS, dans Azure ou dans Google Cloud.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres, puis sélectionnez **Paramètres du connecteur**.



2. Sous **général**, cliquez sur **support Direct API Traffic**.
3. Cochez la case pour activer l'option, puis cliquez sur **Enregistrer**.

Configuration par défaut du connecteur

Vous voudrez peut-être en savoir plus sur le connecteur avant de le déployer ou pour résoudre d'autres problèmes.

Configuration par défaut avec accès à Internet

Les informations de configuration suivantes s'appliquent si vous avez déployé le connecteur depuis BlueXP, depuis le Marketplace de votre fournisseur de services cloud ou si vous avez installé manuellement le connecteur sur un hôte Linux sur site disposant d'un accès Internet.

Détails d’AWS

Si vous avez déployé le connecteur depuis BlueXP ou depuis le marché du fournisseur cloud, remarque :

- Le type d’instance EC2 est t3.XLarge.
- Le système d’exploitation de l’image est Red Hat Enterprise Linux 7.6 (HVM).

Le système d’exploitation n’inclut pas d’interface graphique. Vous devez utiliser un terminal pour accéder au système.

- Le nom d’utilisateur de l’instance Linux EC2 est utilisateur ec2.
- Le disque système par défaut est un disque gp2 de 100 Gio.

Détails d’Azure

Si vous avez déployé le connecteur depuis BlueXP ou depuis le marché du fournisseur cloud, remarque :

- Le type de machine virtuelle est DS3 v2.
- Le système d’exploitation de l’image est CentOS 7.6.

Le système d’exploitation n’inclut pas d’interface graphique. Vous devez utiliser un terminal pour accéder au système.

- Le disque système par défaut est un disque SSD premium de 100 Gio.

Détails sur Google Cloud

Si vous avez déployé le connecteur depuis BlueXP ou depuis le marché du fournisseur cloud, remarque :

- L’instance de machine virtuelle est n2-standard-4.
- Le système d’exploitation de l’image est Red Hat Enterprise Linux 8.6.

Le système d’exploitation n’inclut pas d’interface graphique. Vous devez utiliser un terminal pour accéder au système.

- Le disque système par défaut est un disque persistant SSD de 100 Gio.

Dossier d’installation

Le dossier d’installation du connecteur se trouve à l’emplacement suivant :

/opt/application/netapp/cloudmanager

Fichiers journaux

Les fichiers journaux sont contenus dans les dossiers suivants :

- /opt/application/netapp/cloudmanager/log

Les journaux de ce dossier fournissent des détails sur les images Connector et docker.

- /opt/application/netapp/cloudmanager/docker_ocm/data/log

Les journaux de ce dossier fournissent des détails sur les services Cloud et le service BlueXP qui

s'exécute sur le connecteur.

Service des connecteurs

- Le service BlueXP est nommé ocm.
- Le service occm dépend du service MySQL.

Si le service MySQL est en panne, le service occm est également en panne.

Packs

BlueXP installe les modules suivants sur l'hôte Linux, s'ils ne sont pas déjà installés :

- 7Zip
- AWSCLI
- Java
- Kubectl
- MySQL
- Tridentctl
- Tirer
- Wget

Ports

Le connecteur utilise les ports suivants sur l'hôte Linux :

- 80 pour l'accès HTTP
- 443 pour l'accès HTTPS
- 3306 pour la base de données BlueXP
- 8080 pour le proxy API BlueXP
- 8666 pour l'API du Gestionnaire de services
- 8777 pour l'API du service de conteneurs Health-Checker

Configuration par défaut sans accès à Internet

La configuration suivante s'applique si vous avez installé manuellement le connecteur sur un hôte Linux sur site qui n'a pas accès à Internet. ["En savoir plus sur cette option d'installation"](#).

- Le dossier d'installation du connecteur se trouve à l'emplacement suivant :

`/opt/application/netapp/ds`

- Les fichiers journaux sont contenus dans les dossiers suivants :

`/var/lib/docker/volumes/ds_ocmdata/_data/log`

Les journaux de ce dossier fournissent des détails sur les images Connector et docker.

- Tous les services s'exécutent dans des conteneurs docker

Ces services dépendent du service d'exécution docker exécuté

- Le connecteur utilise les ports suivants sur l'hôte Linux :
 - 80 pour l'accès HTTP
 - 443 pour l'accès HTTPS

Gérer les abonnements et les contrats PAYGO

Lorsque vous vous abonnez à BlueXP depuis le marché d'un fournisseur de services Cloud, vous êtes redirigé vers le site Web BlueXP où vous devez enregistrer votre abonnement et l'associer à des comptes spécifiques. Après votre inscription, vous pouvez gérer chaque abonnement à partir du porte-monnaie numérique.

Afficher vos abonnements

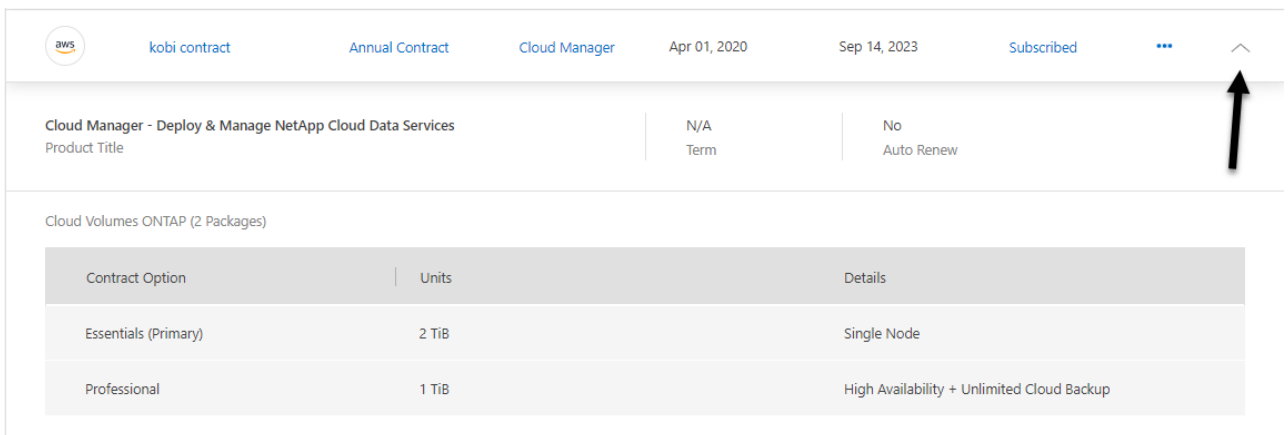
Le porte-monnaie numérique fournit des informations détaillées sur chaque abonnement PAYGO et contrat annuel associé à votre compte BlueXP et à Astra (Astra utilise le service de facturation de BlueXP).

Étapes

1. Dans le menu de navigation BlueXP, sélectionnez **gouvernance > porte-monnaie numérique**.
2. Sélectionnez **abonnements**.

Vous ne verrez que les abonnements associés au compte que vous consultez actuellement.

3. Lorsque vous affichez les informations relatives à vos abonnements, vous pouvez interagir avec les détails du tableau comme suit :
 - Développez une ligne pour afficher plus de détails.



Product Title	Term	Auto Renew
Cloud Manager - Deploy & Manage NetApp Cloud Data Services	N/A	No

Contract Option	Units	Details
Essentials (Primary)	2 TiB	Single Node
Professional	1 TiB	High Availability + Unlimited Cloud Backup

- Cliquez sur  pour choisir les colonnes qui s'affichent dans le tableau.

Notez que les colonnes Term et Auto Renew n'apparaissent pas par défaut. La colonne Renouvellement automatique affiche les informations de renouvellement des contrats Azure uniquement.

Notez ce qui suit à propos de ce que vous voyez dans le tableau :

Date de début

La date de début est la date à laquelle vous avez correctement associé l'abonnement à votre compte et que la facturation a commencé.

S/O

Si vous voyez N/A dans le tableau, les informations ne sont pas disponibles dans l'API du fournisseur de cloud pour le moment.

Contrats

- Si vous développez les détails d'un contrat, le porte-monnaie numérique affiche les éléments disponibles pour votre plan actuel : les options et unités du contrat (capacité ou nombre de nœuds).
- Le porte-monnaie numérique identifie la date de fin et indique si le contrat sera bientôt renouvelé ou s'il a déjà pris fin.
- Si vous avez souscrit un contrat AWS et que vous avez modifié l'une des options du contrat après la date de début, veuillez à valider les options de contrat depuis AWS.

Gérez vos abonnements

Vous pouvez gérer vos abonnements à partir du porte-monnaie numérique en renommant un abonnement et en choisissant les comptes associés à l'abonnement.

Par exemple, disons que vous avez deux comptes et que chacun est facturé par le biais d'abonnements distincts. Vous pouvez dissocier un abonnement de l'un des comptes afin que les utilisateurs de ce compte ne choisissent pas accidentellement l'abonnement incorrect lors de la création d'un environnement de travail Cloud Volume ONTAP.

Étapes

1. Dans le menu de navigation BlueXP, sélectionnez **gouvernance > porte-monnaie numérique**.
2. Sélectionnez **abonnements**.
3. Cliquez sur le menu d'action de la ligne correspondant à l'abonnement que vous souhaitez gérer.

Provider	Name	Type	Service	Start Date	End Date	Status	
aws	aws-sub-a2	PAYGO	Cloud Manager	Apr 02, 2020	N/A	Subscribed	⋮
aws	Aleksey_aws_marketplace	Annual Contract	Astra	Oct 18, 2022	Oct 18, 2023		⋮
aws	By Capacity By Node 3	PAYGO	Cloud Manager	Mar 31, 2020	N/A	Subscribed	⋮

4. Vous pouvez renommer l'abonnement ou gérer les comptes NetApp associés à cet abonnement.

Stockage cloud découvert

Affichage des compartiments Amazon S3

Une fois que vous avez installé un connecteur dans AWS, BlueXP peut détecter automatiquement les informations relatives aux compartiments Amazon S3 qui résident

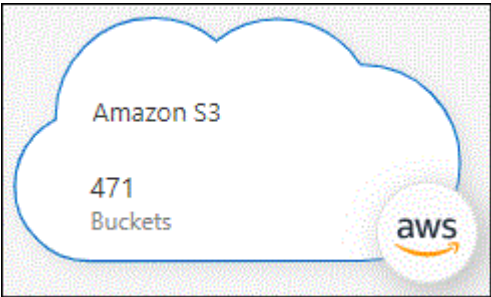
dans le compte AWS où le connecteur est installé. Un environnement de travail Amazon S3 est ajouté à Canvas pour que vous puissiez visualiser ces informations.

Vous pouvez afficher des informations détaillées sur vos compartiments S3, notamment la région, les règles d'accès, le compte, la capacité totale et utilisée. Ces compartiments peuvent être utilisés comme destinations pour les opérations Cloud Backup, Cloud Tiering ou Cloud Sync. Vous pouvez également utiliser Cloud Data Sense pour scanner ces compartiments.

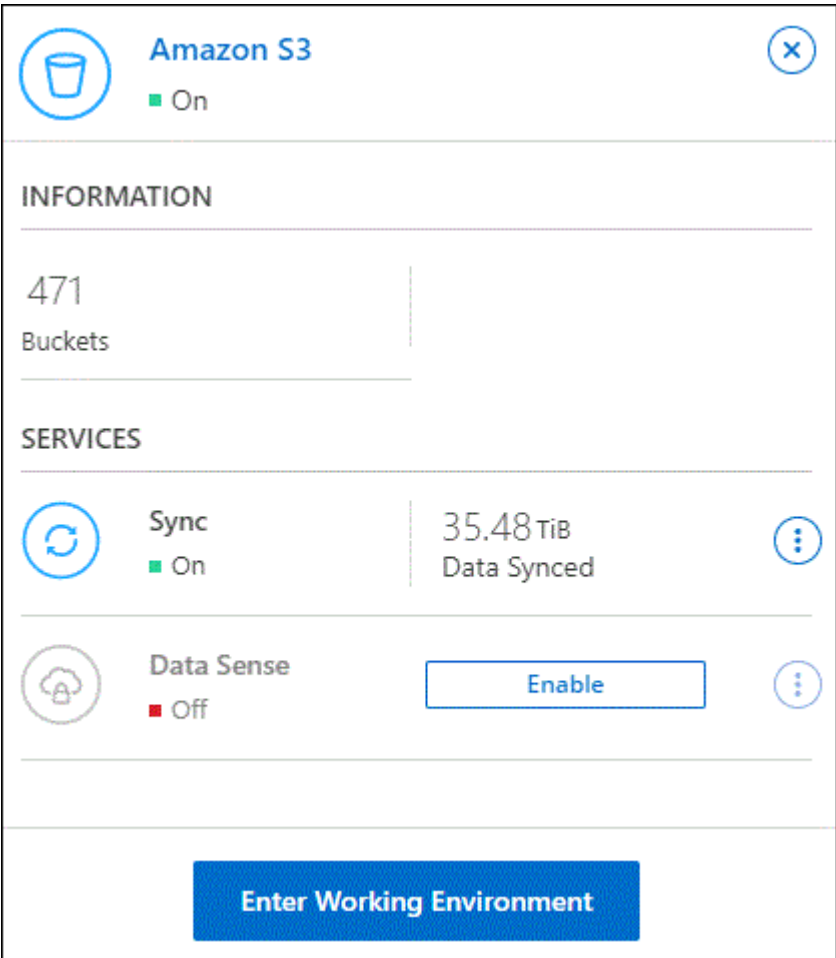
Étapes

- 1. "Installer un connecteur" Dans le compte AWS où vous souhaitez afficher vos compartiments Amazon S3.
- 2. Dans le menu de navigation, sélectionnez **stockage > Canvas**.

Vous devriez voir automatiquement un environnement de travail Amazon S3 peu après.



- 3. Cliquez sur l'environnement de travail et sélectionnez une action dans le volet droit.



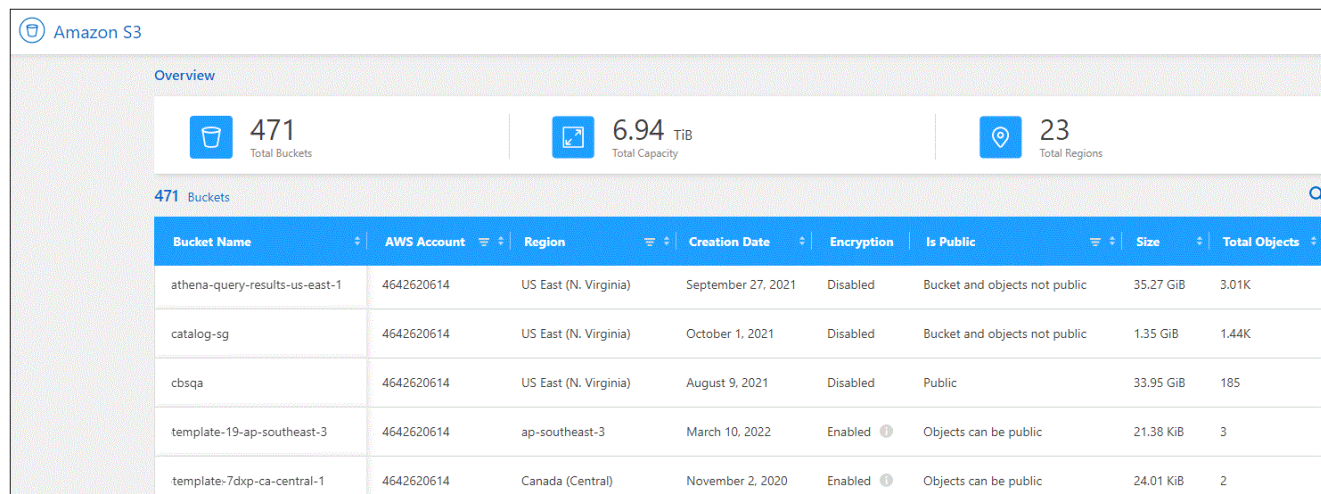
4. Cliquez sur **Synchroniser les données** pour synchroniser les données vers ou à partir de compartiments S3.

Pour plus de détails, voir ["La présentation du service Cloud Sync"](#).

5. Cliquez sur **Activer** si vous souhaitez que Cloud Data SENSE analyse les compartiments S3 pour les données personnelles et sensibles.

Pour plus de détails, voir ["Mise en route de Cloud Data Sense pour Amazon S3"](#).

6. Cliquez sur **entrer environnement de travail** pour afficher des détails sur les compartiments S3 de votre compte AWS.



Bucket Name	AWS Account	Region	Creation Date	Encryption	Is Public	Size	Total Objects
athena-query-results-us-east-1	4642620614	US East (N. Virginia)	September 27, 2021	Disabled	Bucket and objects not public	35.27 GiB	3.01K
catalog-sg	4642620614	US East (N. Virginia)	October 1, 2021	Disabled	Bucket and objects not public	1.35 GiB	1.44K
cbsqa	4642620614	US East (N. Virginia)	August 9, 2021	Disabled	Public	33.95 GiB	185
template-19-ap-southeast-3	4642620614	ap-southeast-3	March 10, 2022	Enabled	Objects can be public	21.38 KiB	3
template-7dxc-ca-central-1	4642620614	Canada (Central)	November 2, 2020	Enabled	Objects can be public	24.01 KiB	2

Affichage de vos comptes Azure Blob

Une fois que vous avez installé un connecteur dans Azure, BlueXP peut détecter automatiquement des informations sur les comptes de stockage Azure qui résident dans les abonnements Azure où le connecteur est installé. Un environnement de travail Azure Blob est ajouté à Canvas pour vous permettre d'afficher ces informations.

Vous pouvez afficher des informations détaillées sur vos comptes de stockage Azure, notamment l'emplacement, le groupe de ressources, la capacité totale et utilisée, etc. Ces comptes peuvent être utilisés comme destinations pour les opérations Cloud Backup, Cloud Tiering ou Cloud Sync.

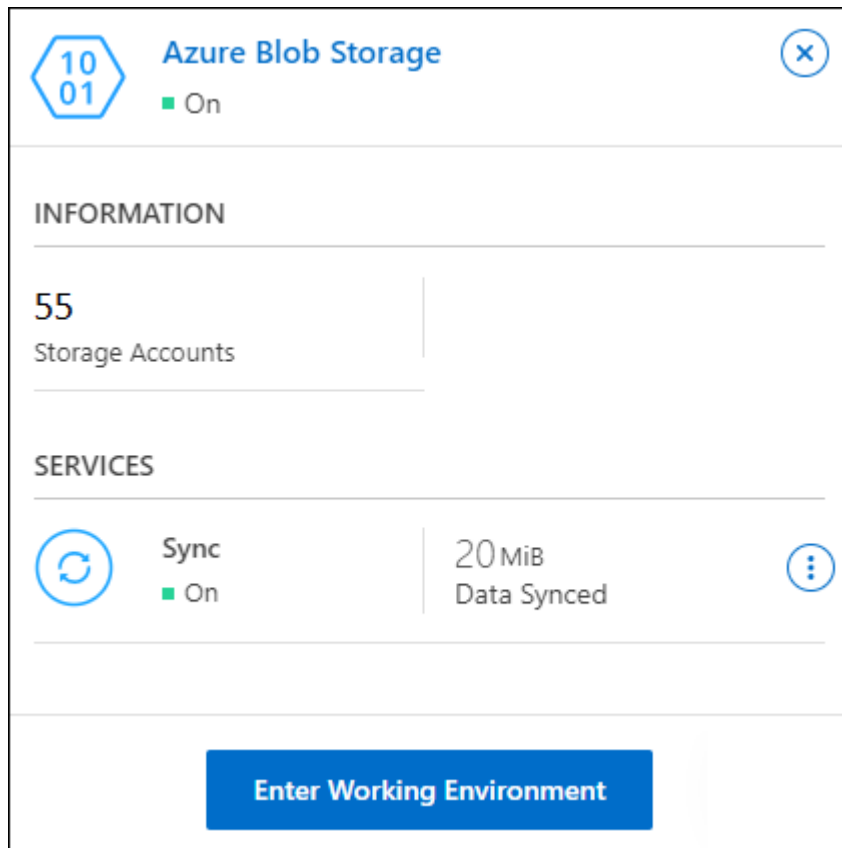
Étapes

1. ["Installer un connecteur"](#) Dans le compte Azure où vous voulez afficher vos comptes de stockage Azure
2. Dans le menu de navigation, sélectionnez **stockage > Canvas**.

Vous devriez voir automatiquement un environnement de travail Azure Blob peu de temps après.



3. Cliquez sur l'environnement de travail et sélectionnez une action dans le volet droit.



4. Cliquez sur **Synchroniser les données** pour synchroniser les données vers ou depuis le stockage Azure Blob.

Pour plus de détails, voir "[La présentation du service Cloud Sync](#)".

5. Cliquez sur **entrer environnement de travail** pour afficher les détails sur les comptes de stockage Azure dans vos blobs Azure.

Azure blob

Overview

637

Total Storage Accounts

1.5

TiB

Total Capacity

16

Total Locations

637

Storage Accounts

Storage Account Name	Subscription	Location	Creation Date	Resource Group	Blob Capacity
ovu8llxvqdfypxn	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	170 B
rootsa9ktjpjzcm	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	950.22 GiB
scvdwjcwehfswli	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	22.12 MiB
65qtx0smegmq2vt	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	170 B
bu9klxthymr1be	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	1.01 MiB
8jzsvybviwieww8	OCCM QA1	Canada Central	December 12, 2019	aff1-rg	170 B

Afficher les compartiments de stockage Google Cloud

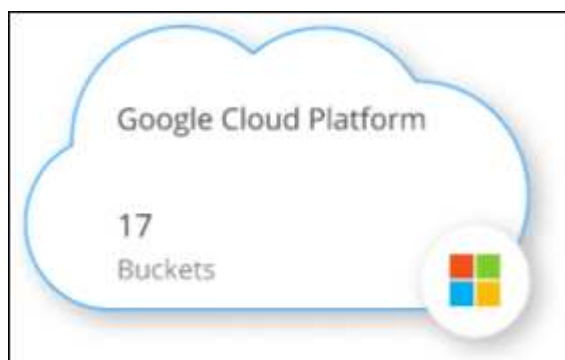
Après avoir installé un connecteur dans Google Cloud, BlueXP peut automatiquement découvrir des informations sur les compartiments Google Cloud Storage qui résident dans le compte Google où le connecteur est installé. Un environnement de travail Google Cloud Storage est ajouté à Canvas pour vous permettre de visualiser ces informations.

Vous trouverez des informations détaillées sur vos compartiments Google Cloud Storage : l'emplacement, l'état d'accès, la classe de stockage, la capacité totale et utilisée, entre autres. Ces compartiments peuvent être utilisés comme destinations pour les opérations Cloud Backup, Cloud Tiering ou Cloud Sync.

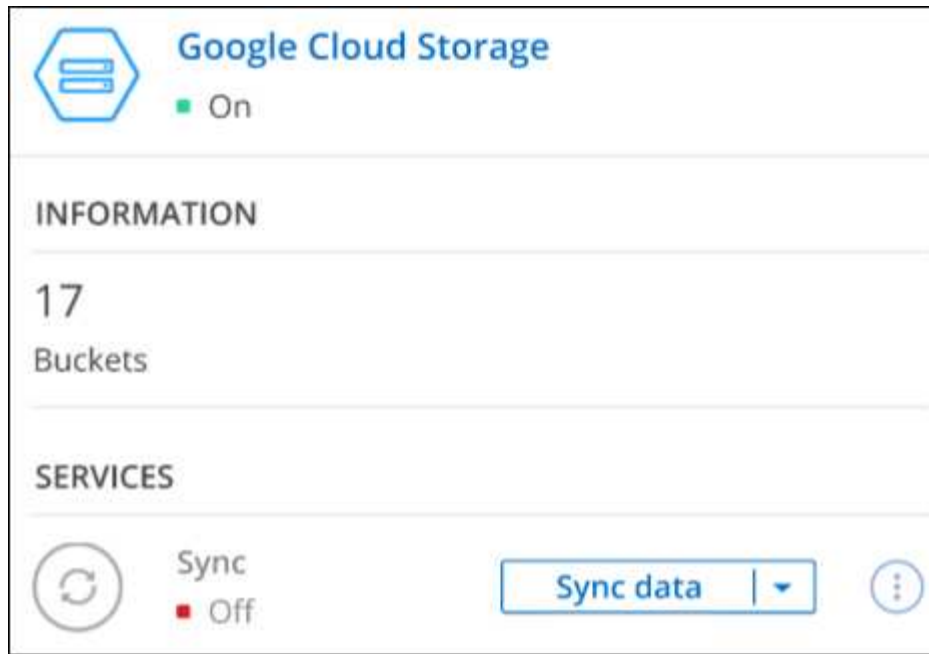
Étapes

1. "[Installer un connecteur](#)" Dans le compte Google où vous souhaitez consulter vos compartiments Google Cloud Storage.
2. Dans le menu de navigation, sélectionnez **stockage > Canvas**.

Vous devriez voir automatiquement un environnement de travail Google Cloud Storage peu après.



3. Cliquez sur l'environnement de travail et sélectionnez une action dans le volet droit.



4. Cliquez sur **Synchroniser les données** pour synchroniser les données vers ou depuis des compartiments Google Cloud Storage.

Pour plus de détails, voir "[La présentation du service Cloud Sync](#)".

5. Cliquez sur **entrer environnement de travail** pour afficher les détails des rubriques de votre compte Google.

The screenshot shows the Google Cloud Storage Overview page. At the top, there's a header with the Google Cloud Storage logo. Below this is an 'Overview' section with three cards: '17 Total buckets', '1.76 TiB Total capacity | Calculating', and '6 Total locations'. Below the overview section is a table titled '17 Buckets'. The table has columns: Bucket Name, Location, Creation Date, Public Access, Default Storage Class, and Total Capacity. The table lists five buckets with their respective details.

Bucket Name	Location	Creation Date	Public Access	Default Storage Class	Total Capacity
BucketName 1	US East (N. Virginia)	May 04 2021	Yes	StorageClass 1	...
BucketName 2	US West (Oregon)	May 04 2021	Yes	StorageClass 2	...
BucketName 3	US East (N. Virginia)	May 04 2021	No	StorageClass 3	...
BucketName 4	US East (N. Virginia)	May 04 2021	No	StorageClass 4	...
BucketName 5	US East (N. Virginia)	May 04 2021	Yes	StorageClass 5	...

Identifiants AWS

Identifiants et autorisations AWS

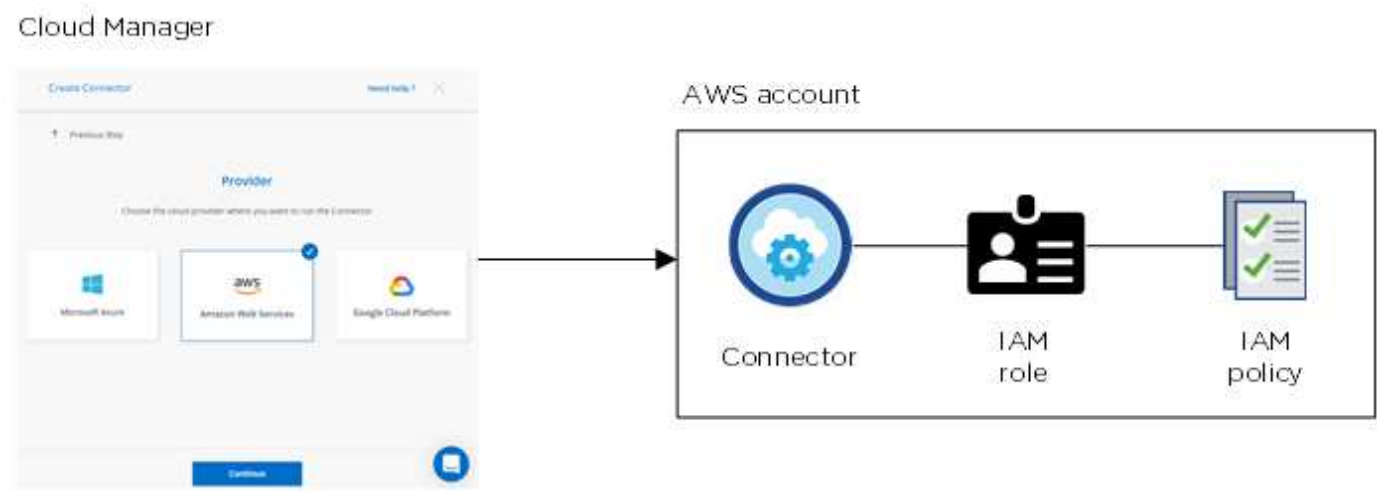
BlueXP vous permet de choisir les informations d'identification AWS à utiliser lors du déploiement de Cloud Volumes ONTAP. Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des identifiants AWS initiaux, ou ajouter des identifiants

supplémentaires.

Identifiants AWS initiaux

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

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



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

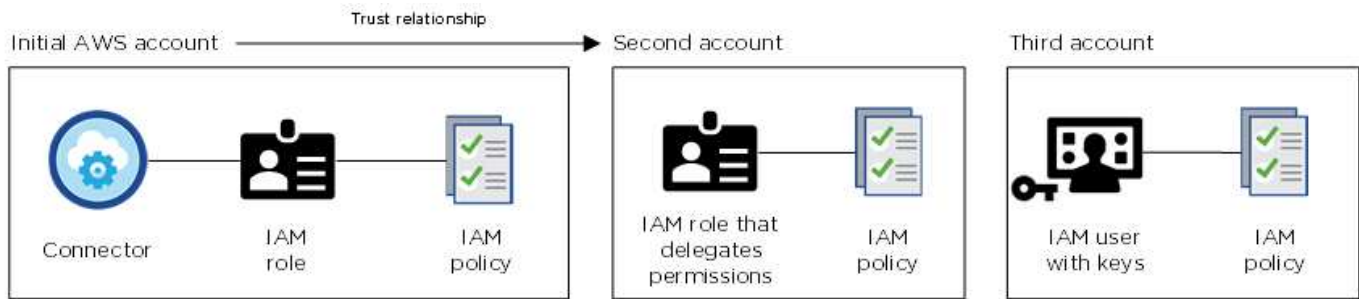
Details & Credentials			
Instance Profile		QA Subscription	Edit Credentials
Credentials	Account ID	Marketplace Subscription	

Autres identifiants AWS

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

Ajoutez des identifiants AWS à un connecteur existant

Si vous souhaitez lancer Cloud Volumes ONTAP sur différents comptes AWS, vous pouvez l'un ou l'autre ["Fournir des clés AWS pour un utilisateur IAM ou le numéro ARN d'un rôle dans un compte de confiance"](#). L'image suivante montre deux comptes supplémentaires, l'un avec des autorisations par le biais d'un rôle IAM dans un compte de confiance et l'autre avec les clés AWS d'un utilisateur IAM :



Vous le feriez alors "[Ajoutez les informations d'identification du compte à BlueXP](#)" En spécifiant le nom de ressource Amazon (ARN) du rôle IAM ou les clés AWS pour l'utilisateur IAM.

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

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 AWS directement à BlueXP

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

Qu'en est-il des déploiements Marketplace et des déploiements sur site ?

Les sections ci-dessus décrivent la méthode de déploiement recommandée pour le connecteur, qui provient de BlueXP. Vous pouvez également déployer un connecteur dans AWS à partir du "[AWS Marketplace](#)" et vous le pouvez "[Installer le connecteur sur site](#)".

Si vous utilisez Marketplace, des autorisations sont fournies de la même manière. Il vous suffit de créer et de configurer manuellement le rôle IAM, puis de fournir des autorisations pour tous les comptes supplémentaires.

Pour les déploiements sur site, vous ne pouvez pas configurer de rôle IAM pour le système BlueXP, mais vous pouvez fournir des autorisations exactement comme pour d'autres comptes AWS.

Comment faire tourner mes identifiants AWS en toute sécurité ?

Comme décrit ci-dessus, BlueXP vous permet de fournir des identifiants AWS de diverses manières : un rôle IAM associé à l'instance Connector, en assumant un rôle IAM dans un compte de confiance ou en fournissant des clés d'accès AWS.

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

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

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

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

Présentation

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

- Ajoutez des identifiants AWS supplémentaires à un connecteur existant

L'ajout d'identifiants AWS à un connecteur existant offre les autorisations nécessaires pour gérer les ressources et les processus au sein de votre environnement de cloud public. [credentials to a Connector](#), Découvrez comment ajouter des identifiants AWS à un connecteur.

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

L'ajout de nouvelles informations d'identification AWS à BlueXP offre à BlueXP les autorisations nécessaires pour créer un connecteur. [credentials to BlueXP for creating a Connector](#), Découvrez comment ajouter des identifiants AWS à BlueXP.

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

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

Comment faire pivoter les informations d'identification

BlueXP vous permet de fournir des identifiants AWS de diverses manières : un rôle IAM associé à l'instance Connector, en assumant un rôle IAM dans un compte de confiance ou en fournissant des clés d'accès AWS. ["En savoir plus sur les identifiants et les autorisations AWS"](#).

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

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

Ajouter des informations d'identification à un connecteur

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

Accorder des autorisations

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



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

Choix

- permissions by assuming an IAM role in another account
- permissions by providing AWS keys

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

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

Étapes

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

Assurez-vous de faire ce qui suit :

- Sous **Type d'entité approuvée**, sélectionnez **compte AWS**.
- Sélectionnez **un autre compte AWS** et entrez l'ID du compte sur lequel réside l'instance de connecteur.
- Créez les politiques requises en copiant et en collant le contenu de ["Les règles IAM pour le connecteur"](#).

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

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

Accordez des autorisations en fournissant des clés AWS

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

Étapes

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

["Documentation AWS : création de règles IAM"](#)

2. Associez les règles à un rôle IAM ou à un utilisateur IAM.
 - ["Documentation AWS : création de rôles IAM"](#)
 - ["Documentation AWS : ajout et suppression de règles IAM"](#)

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

Ajoutez les informations d'identification

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

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

Étapes

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



3. Cliquez sur **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
 - a. **Emplacement des informations d'identification** : sélectionnez **Amazon Web Services > connecteur**.
 - b. **Définir les informations d'identification** : fournir l'ARN (Amazon Resource Name) d'un rôle IAM approuvé, ou entrer une clé d'accès AWS et une clé secrète.
 - c. **Abonnement Marketplace** : associez un abonnement Marketplace à ces identifiants en vous abonnant maintenant ou en sélectionnant un abonnement existant.

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

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

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 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 BlueXP pour créer un connecteur

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

Configurer le rôle IAM

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

Étapes

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

Assurez-vous de faire ce qui suit :

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

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

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

Ajoutez les informations d'identification

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

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

Étapes

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



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

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

Associez un abonnement AWS

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

Deux scénarios peuvent vous être associés à un abonnement AWS Marketplace une fois que vous avez déjà ajouté les identifiants à BlueXP :

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

Vous devez créer un connecteur avant de pouvoir modifier les paramètres BlueXP. ["Apprenez à créer un connecteur"](#).

Étapes

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



3. Sélectionnez un abonnement existant dans la liste déroulante ou cliquez sur **Ajouter un abonnement** et suivez les étapes pour créer un nouvel abonnement.

► https://docs.netapp.com/fr-fr/cloud-manager-setup-admin//media/video_subscribing_aws.mp4 (video)

Modifier les informations d'identification

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



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

Étapes

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

Suppression des informations d'identification

Si vous n'avez plus besoin d'un ensemble d'informations d'identification, vous pouvez les supprimer de BlueXP. Vous ne pouvez supprimer que les informations d'identification qui ne sont pas associées à un environnement de travail.



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

Étapes

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

Identifiants Azure

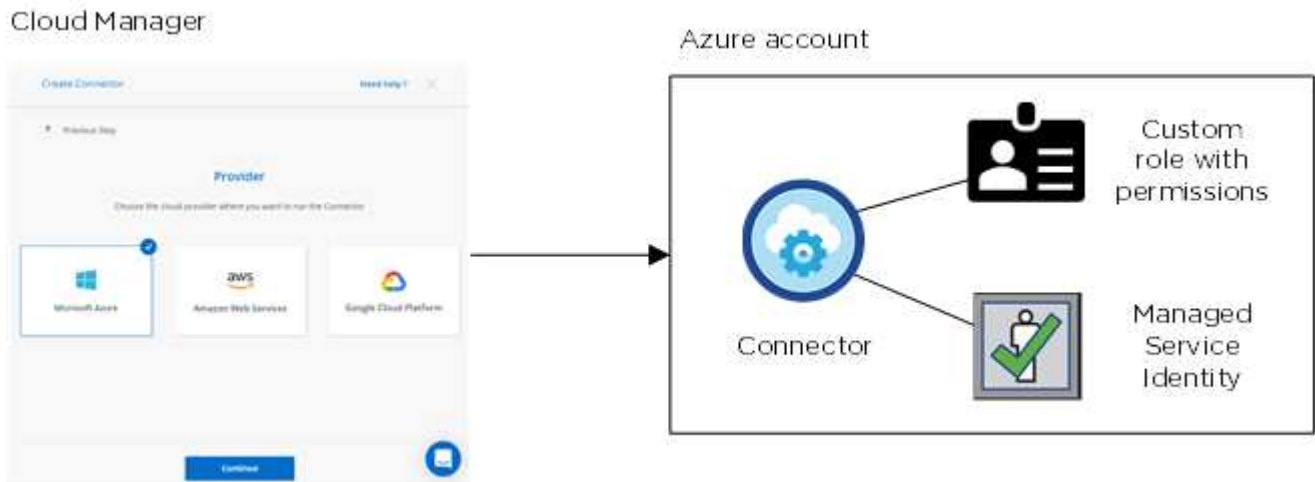
Identifiants et autorisations Azure

BlueXP vous permet de choisir les informations d'identification 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 BlueXP, vous devez utiliser un compte ou un service principal Azure disposant des autorisations pour déployer la machine virtuelle Connector. Les autorisations requises sont répertoriées dans le ["Stratégie de déploiement de Connector pour Azure"](#).

Lorsque BlueXP déploie la machine virtuelle Connector dans Azure, il active un ["identité gérée attribuée par le système"](#) sur une machine virtuelle, crée un rôle personnalisé et le attribue à la machine virtuelle. Le rôle fournit à BlueXP les autorisations requises pour gérer les ressources et les processus au sein de cet abonnement Azure. ["Consultez la manière dont BlueXP utilise les autorisations"](#).



BlueXP sélectionne ces informations d'identification Azure par défaut lorsque vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP :

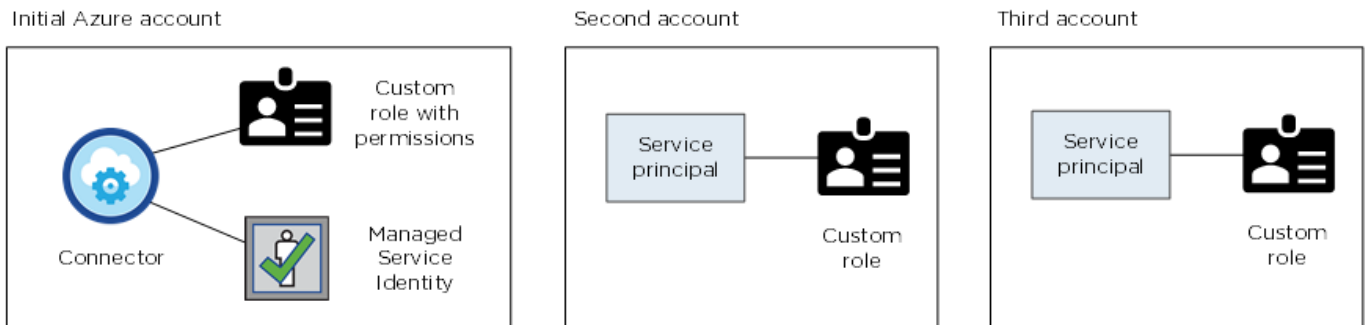
Details & Credentials			
Managed Service Ide...	OCCM QA1	ⓘ No subscription is associated	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

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 :



Vous le feriez alors "[Ajoutez les informations d'identification du compte à BlueXP](#)" 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 :

The screenshot shows the **Edit Account & Add Subscription** dialog box. The **Credentials** section is highlighted, and a dropdown menu is open, showing the following options:

- cloud-manager-app | Application ID: 57c42424-88a0-480a.
- Managed Service Identity** (highlighted in blue)
- 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 BlueXP. 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 informations d'identification et des abonnements Azure pour BlueXP

Lorsque vous créez un système Cloud Volumes ONTAP, vous devez sélectionner les identifiants Azure à utiliser avec ce système. Vous devez également choisir un abonnement Marketplace, si vous utilisez une licence payante à l'utilisation. Suivez les étapes indiquées sur cette page si vous devez utiliser plusieurs identifiants Azure ou plusieurs abonnements Azure Marketplace pour Cloud Volumes ONTAP.

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

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

Association d'abonnements Azure supplémentaires à une identité gérée

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

Une identité gérée est "[Compte Azure initial](#)". Lorsque vous déployez un connecteur depuis BlueXP. Lorsque vous avez déployé le connecteur, BlueXP a créé le rôle opérateur BlueXP et l'a affecté à la machine virtuelle Connector.

Étapes

1. Connectez-vous au portail Azure.
2. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer Cloud Volumes ONTAP.
3. Cliquez sur **contrôle d'accès (IAM)**.
 - a. Cliquez sur **Ajouter > Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
 - Sélectionnez le rôle **opérateur BlueXP**.



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

- Attribuez l'accès à une **machine virtuelle**.
- Sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée.
- Sélectionnez la machine virtuelle Connector.
- Cliquez sur **Enregistrer**.

4. Répétez ces étapes pour les abonnements supplémentaires.

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

Ajout d'informations d'identification Azure supplémentaires à BlueXP

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



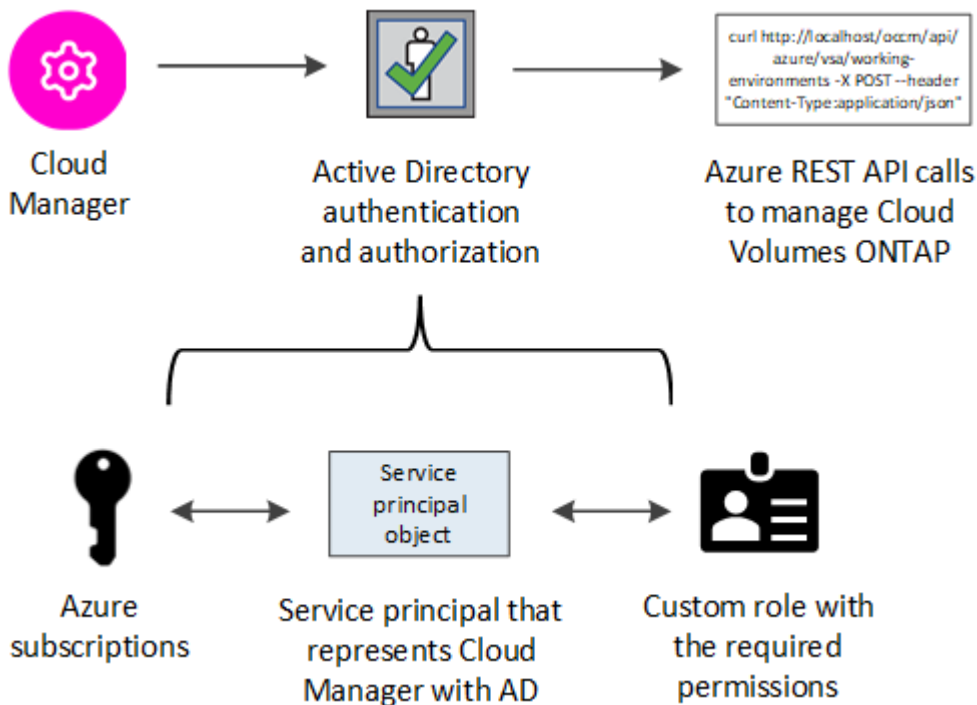
Un jeu initial d'informations d'identification n'est pas ajouté si vous avez installé manuellement le logiciel du connecteur sur un système existant. ["En savoir plus sur les identifiants et les autorisations Azure"](#).

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

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

BlueXP a besoin d'autorisations pour effectuer des actions dans Azure. Vous pouvez accorder les autorisations requises à un compte Azure en créant et en configurant un service principal dans Azure Active Directory et en obtenant les informations d'identification Azure requises par BlueXP.

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



Étapes

1. an Azure Active Directory application, Créez une application Azure Active Directory.
2. the application to a role, Attribuez l'application à un rôle.
3. Windows Azure Service Management API permissions, Ajoutez des autorisations d'API de gestion de service Windows Azure.
4. the application ID and directory ID, Obtenir l'ID de l'application et l'ID du répertoire.
5. a client secret, Créez un secret client.

Création d'une application Azure Active Directory

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

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 BlueXP).
 - **URI de redirection**: Vous pouvez laisser ce champ vide.
5. Cliquez sur **Enregistrer**.

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

Affectation de l'application à un rôle

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

Étapes

1. Création d'un rôle personnalisé :
 - a. Copier le contenu du "[Autorisations de rôle personnalisées pour le connecteur](#)" Et les enregistrer dans un fichier JSON.
 - b. Modifiez le fichier JSON en ajoutant des identifiants d'abonnement Azure à l'étendue assignable.

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

Exemple

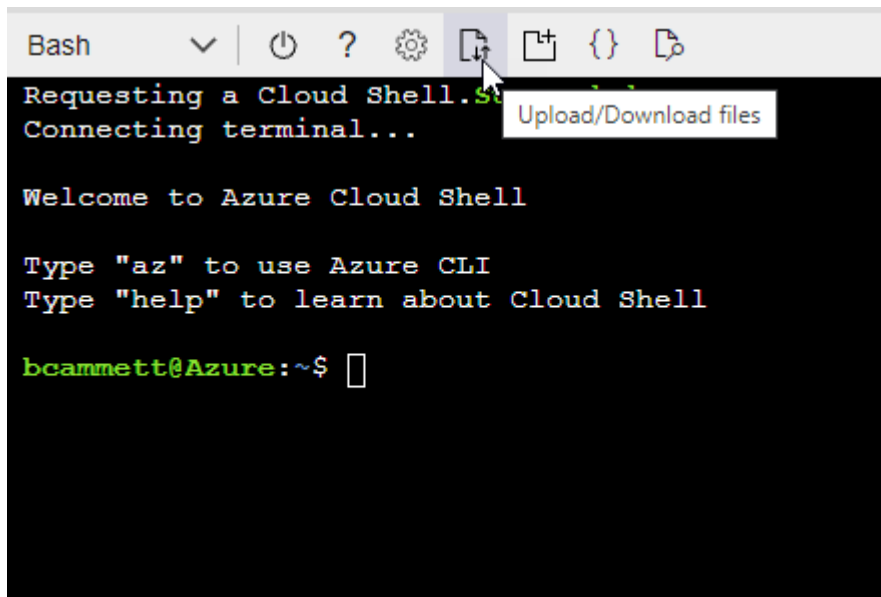
```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

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

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

- Démarrer "[Shell cloud Azure](#)" Et choisissez l'environnement Bash.

- Téléchargez le fichier JSON.



- Entrez la commande Azure CLI suivante :

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

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

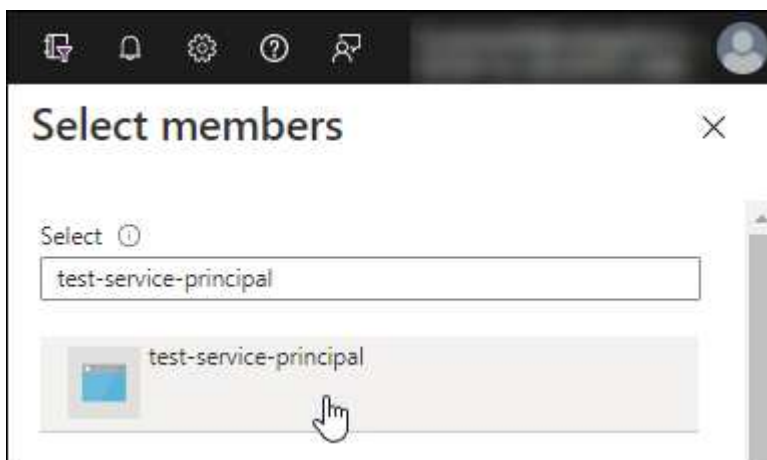
2. Attribuez l'application au rôle :

- À partir du portail Azure, ouvrez le service **abonnements**.
- Sélectionnez l'abonnement.
- Cliquez sur **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.
- Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et cliquez sur **Next**.
- Dans l'onglet **membres**, procédez comme suit :
 - Conserver **utilisateur, groupe ou entité de service** sélectionnée.
 - Cliquez sur **Sélectionner les membres**.



- Recherchez le nom de l'application.

Voici un exemple :



- Sélectionnez l'application et cliquez sur **Sélectionner**.
 - Cliquez sur **Suivant**.
- f. Cliquez sur **Revue + affecter**.

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

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

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.

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

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](#)

Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation 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 à BlueXP, vous devez fournir l'ID d'application (client) et l'ID de répertoire (tenant) de l'application. BlueXP utilise les ID pour se connecter par programmation.

Étapes

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



Création d'un secret client

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

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*-ZR0V4NLfdAcY7:+0vA	

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

Ajout des informations d'identification à BlueXP

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

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

Vous devez créer un connecteur avant de pouvoir modifier les paramètres BlueXP. ["Découvrez comment"](#).

Étapes

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

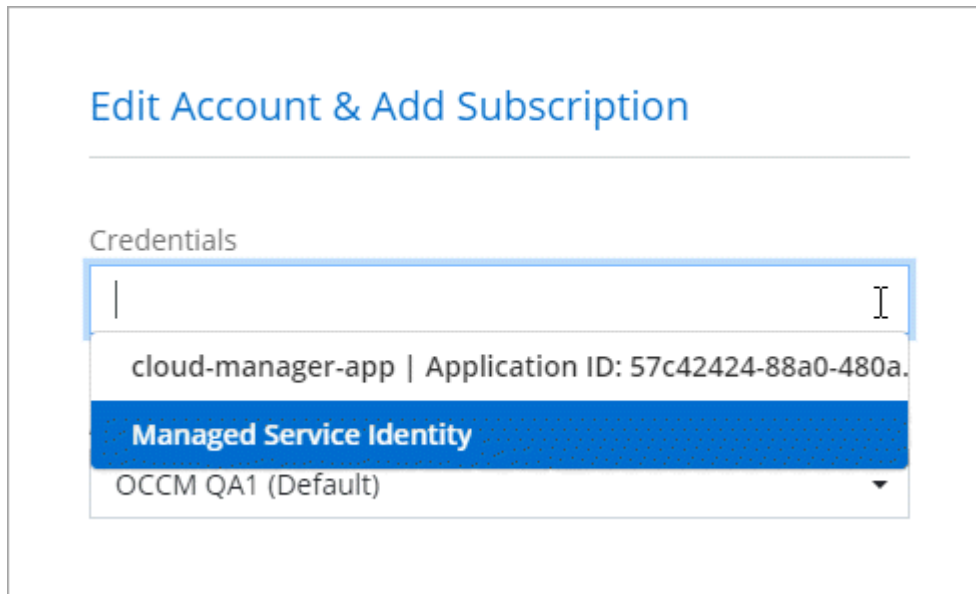


2. Cliquez sur **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
 - a. **Emplacement des informations d'identification** : sélectionnez **Microsoft Azure > connecteur**.
 - b. **Définir les informations d'identification** : saisissez des informations sur l'entité principale du service Azure Active Directory qui accorde les autorisations requises :
 - ID de l'application (client) : voir the application ID and directory ID.
 - ID de répertoire (locataire) : voir the application ID and directory ID.
 - Secret client : voir a client secret.
 - c. **Abonnement Marketplace** : associez un abonnement Marketplace à ces identifiants en vous abonnant maintenant ou en sélectionnant un abonnement existant.

Pour payer Cloud Volumes ONTAP à l'heure (PAYGO), ces identifiants Azure doivent être associés à un abonnement depuis Azure Marketplace.

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

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



Gérer les identifiants existants

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

Association d'un abonnement à Azure Marketplace aux identifiants

Après avoir ajouté vos informations d'identification Azure à BlueXP, vous pouvez associer un abonnement Azure Marketplace 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.

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

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

Vous devez créer un connecteur avant de pouvoir modifier les paramètres BlueXP. "[Découvrez comment](#)".

Étapes

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



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

Modification des informations d'identification

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

Étapes

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

Suppression des informations d'identification

Si vous n'avez plus besoin d'un ensemble d'informations d'identification, vous pouvez les supprimer de BlueXP. Vous ne pouvez supprimer que les informations d'identification qui ne sont pas associées à un environnement de travail.

Étapes

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

Identifiants Google Cloud

Projets, autorisations et comptes Google Cloud

Un compte de service fournit à BlueXP des autorisations de déploiement et de gestion de

systèmes Cloud Volumes ONTAP dans le même projet que le connecteur, ou dans des projets différents.

Projet et autorisations pour BlueXP

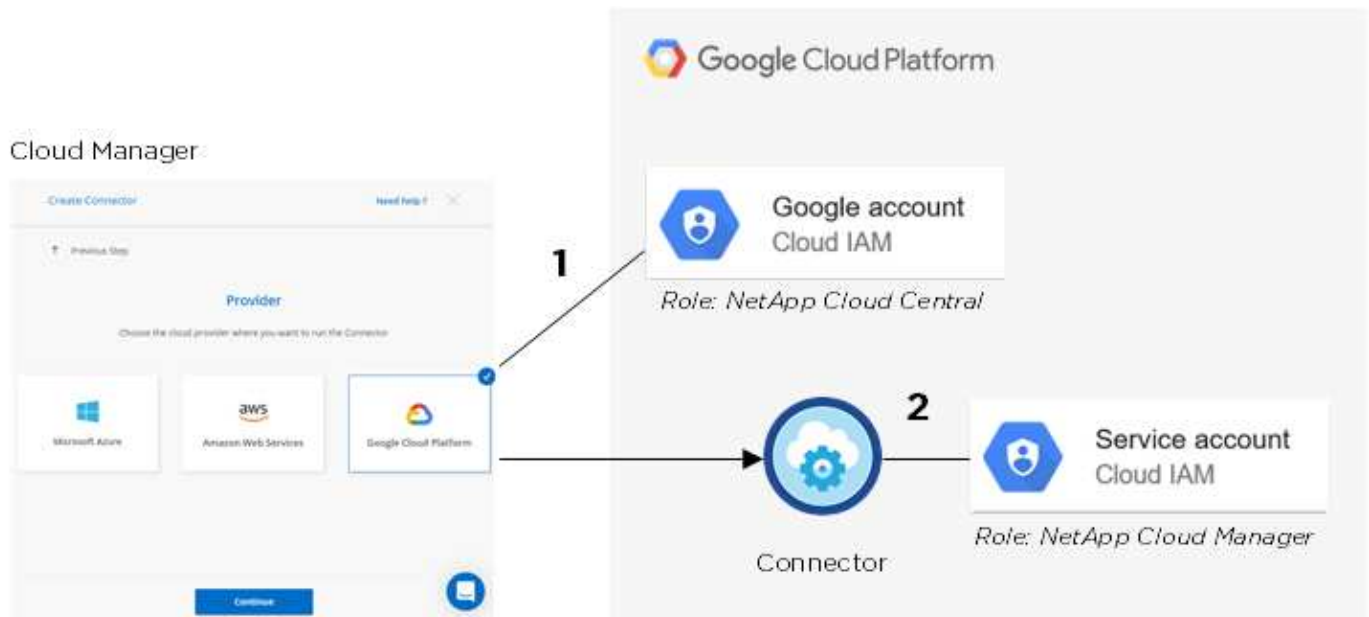
Avant de déployer Cloud Volumes ONTAP dans Google Cloud, vous devez d'abord déployer un connecteur dans un projet Google Cloud. Il ne peut pas s'exécuter sur site ou dans un autre fournisseur cloud.

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

1. Vous devez déployer un connecteur à l'aide d'un compte Google disposant des autorisations nécessaires pour lancer l'instance VM Connector à partir de BlueXP.
2. Lorsque vous déployez le connecteur, vous êtes invité à sélectionner un ["compte de service"](#) Pour l'instance de VM. BlueXP obtient les autorisations du compte de service pour créer et gérer des 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"](#)
- ["Découvrez comment déployer Cloud Volumes ONTAP dans GCP et sélectionner un projet"](#)

Gestion des informations d'identification et des abonnements Google Cloud pour BlueXP

Vous pouvez gérer les informations d'identification associées à l'instance de VM Connector.

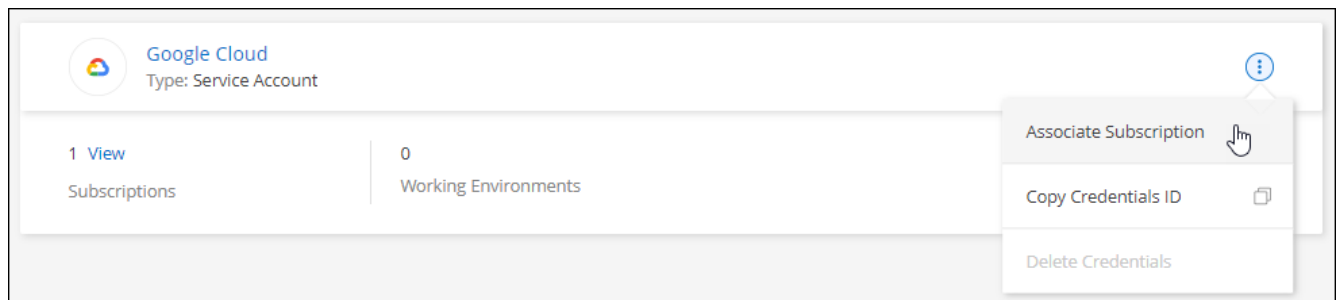
Association d'un abonnement Marketplace aux informations d'identification GCP

Lorsque vous déployez un connecteur dans GCP, BlueXP crée un ensemble d'informations d'identification par défaut qui sont associées à l'instance de VM connecteur. Il s'agit des informations d'identification utilisées par BlueXP 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 BlueXP, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Cliquez sur le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **associer un abonnement**.



3. Sélectionnez un projet et un abonnement Google Cloud dans la liste déroulante.

A screenshot of a form for selecting a Google Cloud Project and Subscription. The 'Google Cloud Project' dropdown menu is set to 'OCCM-Dev'. The 'Subscription' dropdown menu is set to 'GCP subscription for staging', which is preceded by a green dot icon. At the bottom of the form, there is a blue button with a plus sign and the text 'Add Subscription'.

4. Cliquez sur **associé**.
5. Si vous n'avez pas encore d'abonnement, cliquez sur **Ajouter un abonnement** et suivez les étapes ci-

dessous pour créer un nouvel abonnement.




Avant de terminer les étapes suivantes, assurez-vous que vous disposez des deux privilèges d'administrateur de facturation dans votre compte Google Cloud ainsi que d'une connexion BlueXP.

6. Redécouvrez les étapes de l'abonnement et cliquez sur **Continuer**.

Add Subscription



Subscription Steps:


- 1 Cloud Manager**
Clicking **Continue** to create your subscription from the Google Cloud Marketplace.
- 2 Google Cloud Marketplace**
Subscribe and then then click **Register With NetApp** to configure your account from Cloud Central.
- 3 Cloud Central**
Save your subscription.
- 4 Cloud Manager**
Associate the Marketplace subscription with your Google Cloud project.


 View video instructions

ContinueCancel

7. Après avoir été redirigé vers le "[Page NetApp BlueXP sur Google Cloud Marketplace](#)", assurez-vous que le projet correct est sélectionné dans le menu de navigation supérieur.

 Google Cloud Platform 





Cloud Manager for Cloud Volumes ONTAP

NetApp, Inc.

Enterprise-grade data management and protection

[SUBSCRIBE](#)

[OVERVIEW](#) [PRICING](#) [SUPPORT](#)

Overview

Cloud Volumes ONTAP is a data-management layer that runs natively on Google Cloud infrastructure enabling enhanced control, data protection, mobility and agility for business application data. Get consistent enterprise-grade storage across your hybrid cloud platforms with built-in disaster recovery, backup and ransomware protection. Seamlessly migrate enterprise applications without reengineering. Create company-wide file shares with simultaneous NFS and CIFS/SMB access and iSCSI block storage for GCE instances with scalability up to 368TB. Automate persistent storage provisioning for your Kubernetes clusters. Accelerate CI/CD cycles with instant, zero-capacity data replication. Reduce storage costs by 70% with advanced storage efficiencies. Cloud Manager is the console used to deploy, manage and automate Cloud Volumes ONTAP instances across the hybrid multi-cloud.

[Learn more](#)

Additional details

Type: [APIs & services](#)

Last updated: 3/26/21

Category: [Storage](#)

Runs on: NetApp, Inc. Cloud Servers

8. Cliquez sur **Subscribe**.

9. Sélectionnez le compte de facturation approprié et acceptez les conditions générales.

2. Purchase details

Select a billing account *

Secondary_Billing_Account

3. Terms

Cancellation and change policy

- Usage fee is billed every month.
- You can cancel the service at any time and it will take effect immediately. You will be billed by the amount you used for that month.

Additional terms

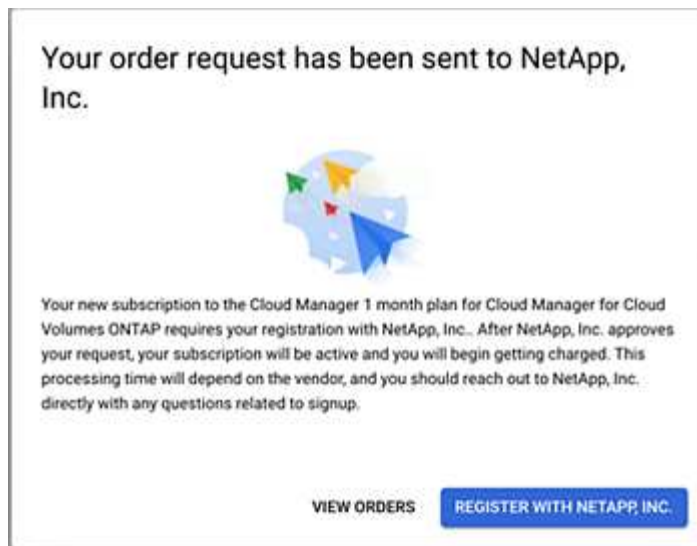
- ☒ I understand this subscription will be automatically renewed at the end of the current term.
- ☒ I authorize Google LLC and its affiliates ("Google") to share my purchase, usage, operational (e.g., project lifecycle events), support ticket, and account information with NetApp, Inc., its affiliates and subcontractors, for the purposes of providing the service, sales attribution, and technical support. I represent that I have the authority to bind my company.
- ☒ By deploying the software or accessing the service you are agreeing to comply with the [End User License Agreement](#), [GCP Marketplace Terms of Service](#), and the terms of applicable open source software licenses bundled with the software or service. Please review these terms and licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.
- By using this product, you understand that certain account and usage information may be shared with NetApp, Inc. for the purposes of financial accounting, sales attribution, performance analysis, and support. ⓘ
- Google is providing this software or service "as-is" and any support for this software or service will be provided by NetApp, Inc. under their terms of service.

SUBSCRIBE

10. Cliquez sur **Subscribe**.

Cette étape envoie votre demande de transfert à NetApp.

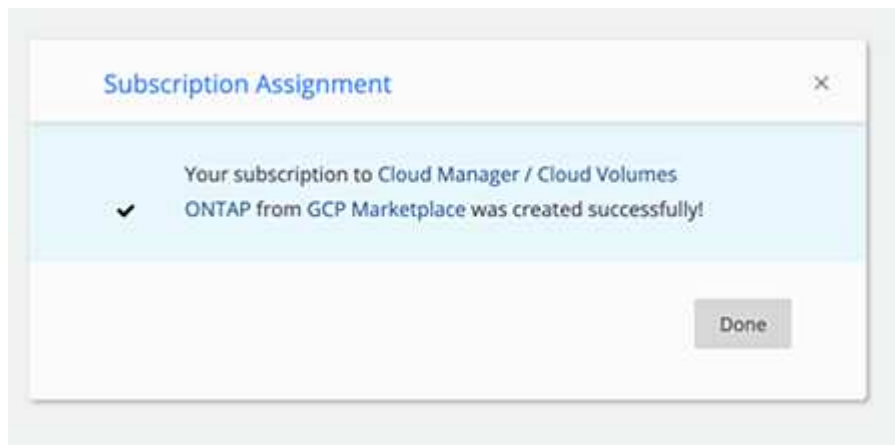
11. Dans la boîte de dialogue contextuelle, cliquez sur **s'inscrire auprès de NetApp, Inc.** pour être redirigé vers le site Web NetApp BlueXP.



Cette étape doit être terminée pour lier l'abonnement GCP à votre compte NetApp. Le processus de liaison d'un abonnement n'est pas terminé tant que vous n'êtes pas redirigé à partir de cette page, puis vous connecter à BlueXP.

12. Après avoir été redirigé vers BlueXP, connectez-vous ou inscrivez-vous, puis cliquez sur **Done** pour continuer.

L'abonnement GCP sera lié à tous les comptes NetApp auxquels vous êtes associé.



Si un membre de votre entreprise a déjà souscrit à l'abonnement NetApp BlueXP à partir de votre compte de facturation, vous serez redirigé vers "[La page Cloud Volumes ONTAP sur le site web de BlueXP](#)" à la place. Si cela est inattendu, contactez votre équipe commerciale NetApp. Google n'autorise qu'un seul abonnement par compte de facturation Google.

13. Une fois ce processus terminé, revenez à la page d'informations d'identification dans BlueXP et sélectionnez ce nouvel abonnement.

Google Cloud Project

OCCM-Dev
▼

Subscription

● GCP subscription for staging
▼

+ Add Subscription

Dépannage du processus d'abonnement Marketplace

Parfois, l'abonnement à Cloud Volumes ONTAP via Google Cloud Marketplace peut devenir fragmenté en raison d'autorisations incorrectes ou accidentellement ne suivant pas la redirection vers le site Web BlueXP. Dans ce cas, procédez comme suit pour terminer le processus d'abonnement.

Étapes

1. Accédez au ["Page NetApp BlueXP sur Google Cloud Marketplace"](#) pour vérifier l'état de la commande. Si la page indique **Manage on Provider**, faites défiler la page vers le bas et cliquez sur **Manage Orders**.

Pricing

✓ The product was purchased on 12/9/20.

MANAGE ORDERS

- a. Si la commande affiche une coche verte et que cela est inattendu, il est possible que quelqu'un d'autre de l'entreprise utilisant le même compte de facturation soit déjà abonné. Si cela est inattendu ou si vous avez besoin des détails de cet abonnement, contactez votre équipe commerciale NetApp.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
✓	2eebbc...	Cloud Manager	-	10/21/21	1 month	-	Postpay	N/A	N/A	⋮

- b. Si la commande affiche une horloge et l'état **en attente**, revenez à la page Marketplace et choisissez **gérer sur fournisseur** pour terminer le processus comme indiqué ci-dessus.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
🕒	d56c66...	Cloud Manager	-	Pending	1 month	Pending	Postpay	N/A	N/A	⋮

Ajoutez et gérez des comptes du site de support NetApp dans BlueXP

Fournissez les identifiants de vos comptes sur le site du support NetApp (NSS) pour vous inscrire au support, activer des workflows clés pour Cloud Volumes ONTAP et bien plus encore.

Présentation

Vous devez ajouter votre compte sur le site de support NetApp à BlueXP pour activer les tâches suivantes :

- Pour obtenir de l'aide
- Pour déployer Cloud Volumes ONTAP lorsque vous utilisez votre propre licence (BYOL)

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

- Pour enregistrer des systèmes Cloud Volumes ONTAP avec paiement à l'utilisation

Vous devez fournir votre compte NSS afin d'activer le support pour votre système et d'accéder aux ressources du support technique NetApp.

- Pour mettre à niveau le logiciel Cloud Volumes ONTAP vers la dernière version

Vous devrez également saisir vos informations d'identification NSS pour utiliser Digital Advisor (anciennement Active IQ) dans BlueXP. Ces informations d'identification sont directement associées à votre compte utilisateur et ne peuvent être utilisées qu'avec Digital Advisor. Vous trouverez plus de détails dans la section qui suit.

Gérer un compte NSS associé à Digital Advisor

Lorsque vous accédez à Digital Advisor dans BlueXP, vous êtes invité à vous connecter à Digital Advisor en saisissant vos informations d'identification NSS. Une fois vos identifiants NSS saisi, ce compte NSS s'affiche en haut de la page gestion NSS. Vous pouvez alors gérer ces informations d'identification selon vos besoins.

Remarque :

- 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.
- Le compte ne peut pas être utilisé avec d'autres fonctionnalités BlueXP : pas avec la création, la licence ou le support Cloud Volumes ONTAP.
- Il ne peut y avoir qu'un seul compte NSS associé à Digital Advisor, par utilisateur.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Cliquez sur **NSS Management**.
3. Sous **vos informations d'identification NSS**, cliquez sur **action** et choisissez l'une des options suivantes :
 - **Utilisateur associé NSS** : ajoutez des identifiants pour un compte sur le site de support NetApp afin que vous puissiez accéder à Digital Advisor dans BlueXP.
 - **Mettre à jour vos identifiants existants** : mettez à jour les identifiants pour votre compte sur le site de support NetApp.
 - **Supprimer** : supprimez le compte associé à Digital Advisor.

BlueXP met à jour le compte NSS associé à Digital Advisor.

Ajouter un compte NSS

Le tableau de bord du support vous permet d'ajouter et de gérer vos comptes sur le site de support NetApp pour les utiliser avec BlueXP au niveau de votre compte NetApp.

- Si vous avez un compte au niveau du client, vous pouvez ajouter un ou plusieurs comptes NSS.
- Si vous avez un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés en même temps que les comptes au niveau du client.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Cliquez sur **NSS Management > Ajouter un compte NSS**.
3. Lorsque vous y êtes invité, cliquez sur **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences.

4. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

Ces actions permettent à BlueXP d'utiliser votre compte NSS pour des opérations telles que le téléchargement de licences, la vérification de la mise à niveau logicielle et les inscriptions de support futures.

Notez ce qui suit :

- Le compte doit être un compte de niveau client (et non un compte invité ou temporaire).
- Une fois la connexion établie, NetApp stockera le nom d'utilisateur NSS. Il s'agit d'un ID généré par le système qui correspond à votre courrier électronique. Sur la page **NSS Management**, vous pouvez afficher votre courriel 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. Cette option vous invite à vous reconnecter.

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

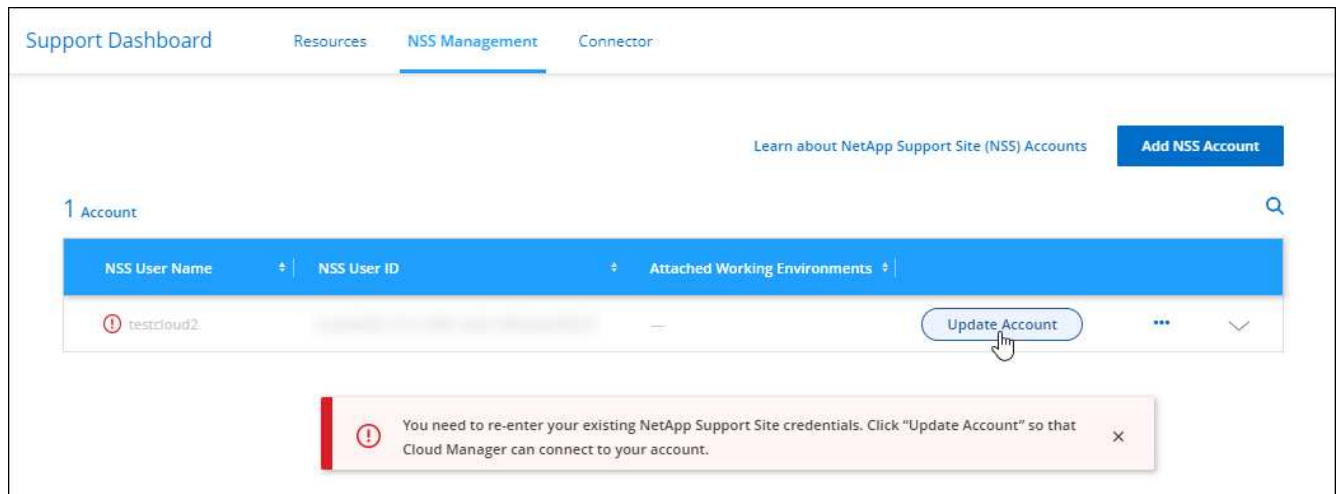
- ["Lancement d'Cloud Volumes ONTAP dans AWS"](#)
- ["Lancement d'Cloud Volumes ONTAP dans Azure"](#)
- ["Lancement d'Cloud Volumes ONTAP dans GCP"](#)
- ["Enregistrement des systèmes de paiement à l'utilisation"](#)

Mettre à jour un compte NSS pour la nouvelle méthode d'authentification

Depuis novembre 2021, NetApp utilise désormais Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences. Suite à cette mise à jour, BlueXP vous invitera à mettre à jour les informations d'identification de tous les comptes existants que vous avez ajoutés précédemment.

Étapes

1. Si ce n'est déjà fait, "[Créez un compte Microsoft Azure Active Directory B2C qui sera lié à votre compte NetApp actuel](#)".
2. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.
3. Cliquez sur **NSS Management**.
4. Pour le compte NSS à mettre à jour, cliquez sur **mettre à jour le compte**.



5. Lorsque vous y êtes invité, cliquez sur **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences.

6. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

Une fois le processus terminé, le compte que vous avez mis à jour doit maintenant être répertorié comme un *nouveau* compte dans la table. La *vieille* version du compte est toujours répertoriée dans le tableau, ainsi que toutes les associations d'environnement de travail existantes.

7. Si des environnements de travail Cloud Volumes ONTAP existants sont associés à l'ancienne version du compte, suivez les étapes ci-dessous à a working environment to a different NSS account, Reliez ces environnements de travail à un autre compte NSS.
8. Accédez à l'ancienne version du compte NSS, cliquez sur **...** Puis sélectionnez **Supprimer**.

Mettre à jour les identifiants NSS

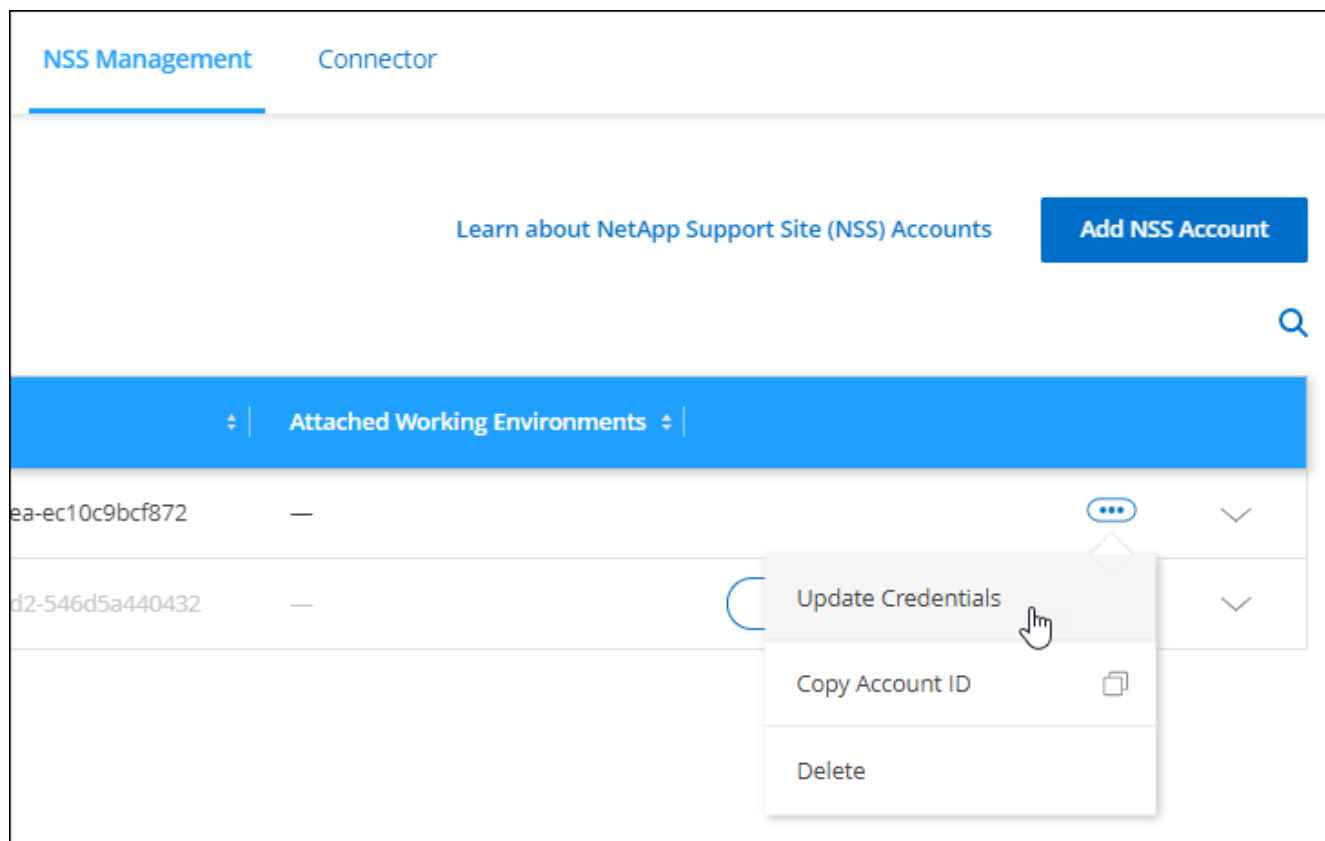
Vous devrez mettre à jour les informations d'identification de vos comptes NSS dans BlueXP lorsque l'un des cas suivants se produit :

- Vous modifiez les informations d'identification du compte

- Le jeton de renouvellement associé à votre compte expire au bout de 3 mois

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.
2. Cliquez sur **NSS Management**.
3. Pour le compte NSS que vous souhaitez mettre à jour, cliquez sur **...** Puis sélectionnez **mettre à jour les informations d'identification**.



4. Lorsque vous y êtes invité, cliquez sur **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences.

5. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

Associez un environnement de travail à un autre compte NSS

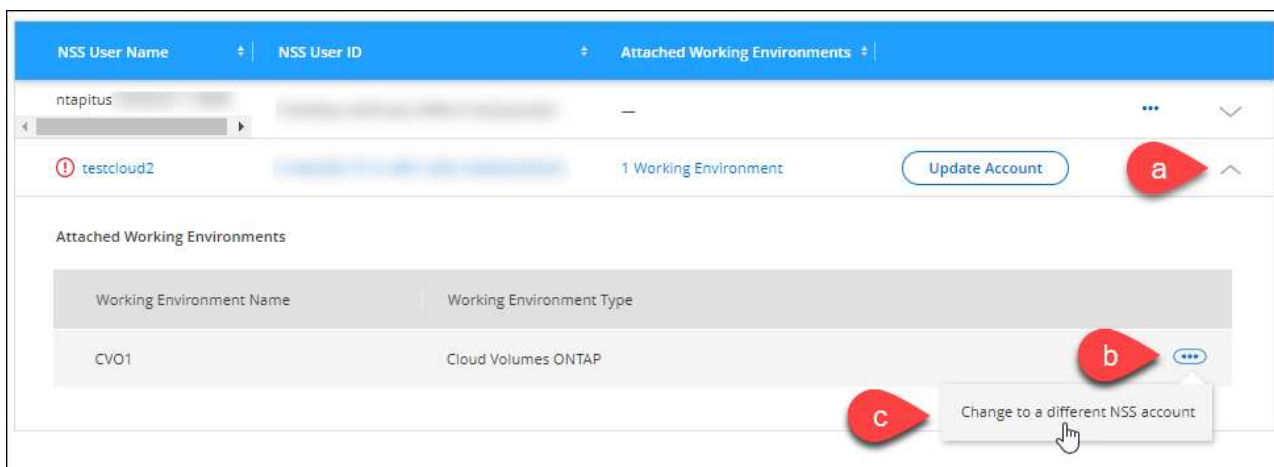
Si votre entreprise compte plusieurs comptes sur le site de support NetApp, vous pouvez modifier le compte associé à un système Cloud Volumes ONTAP.

Cette fonctionnalité n'est prise en charge que avec les comptes NSS configurés pour utiliser Microsoft Azure AD adopté par NetApp pour la gestion des identités. Avant de pouvoir utiliser cette fonction, vous devez cliquer sur **Ajouter un compte NSS** ou **mettre à jour le compte**.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.

2. Cliquez sur **NSS Management**.
3. Pour modifier le compte NSS, procédez comme suit :
 - a. Développez la ligne du compte du site de support NetApp auquel l'environnement de travail est actuellement associé.
 - b. Pour l'environnement de travail pour lequel vous souhaitez modifier l'association, cliquez sur ...
 - c. Sélectionnez **changer pour un autre compte NSS**.



- d. Sélectionnez le compte, puis cliquez sur **Enregistrer**.

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

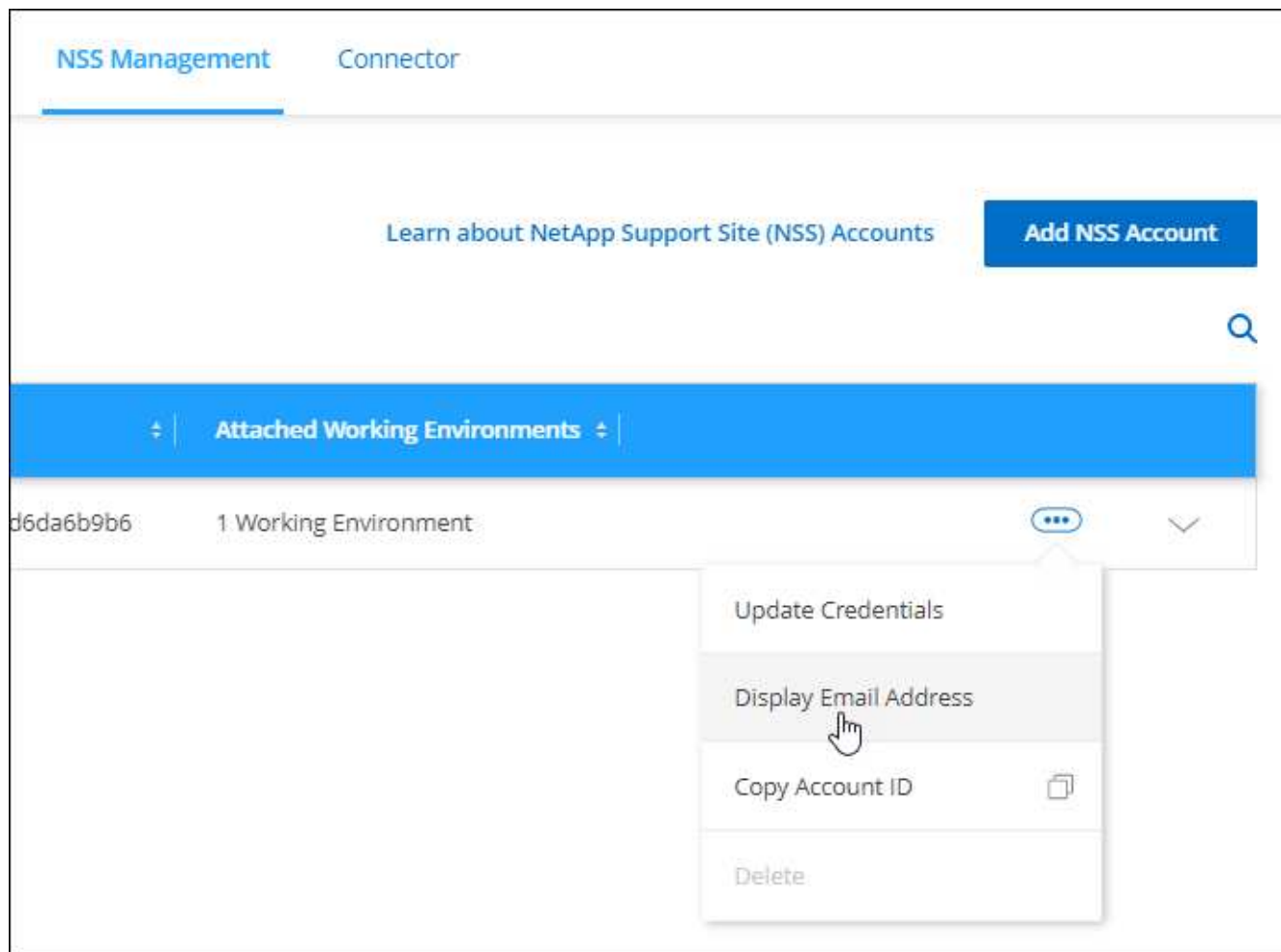
Lorsque les comptes du site de support NetApp utilisent Microsoft Azure Active Directory pour les services d'authentification, le nom d'utilisateur NSS qui s'affiche dans BlueXP est généralement un identifiant généré par Azure AD. Par conséquent, il se peut que vous ne sachiez pas immédiatement l'adresse e-mail associée à ce compte. Mais BlueXP a une option pour vous montrer l'adresse e-mail associée.



Lorsque vous accédez à la page gestion NSS, BlueXP génère un jeton pour chaque compte de la table. Ce token inclut des informations sur l'adresse e-mail associée. Le jeton est alors 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 le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.
2. Cliquez sur **NSS Management**.
3. Pour le compte NSS que vous souhaitez mettre à jour, cliquez sur ... Puis sélectionnez **Afficher l'adresse électronique**.



BlueXP affiche le nom d'utilisateur du site de support NetApp ainsi que l'adresse e-mail associée. Vous pouvez utiliser le bouton Copier pour copier l'adresse e-mail.

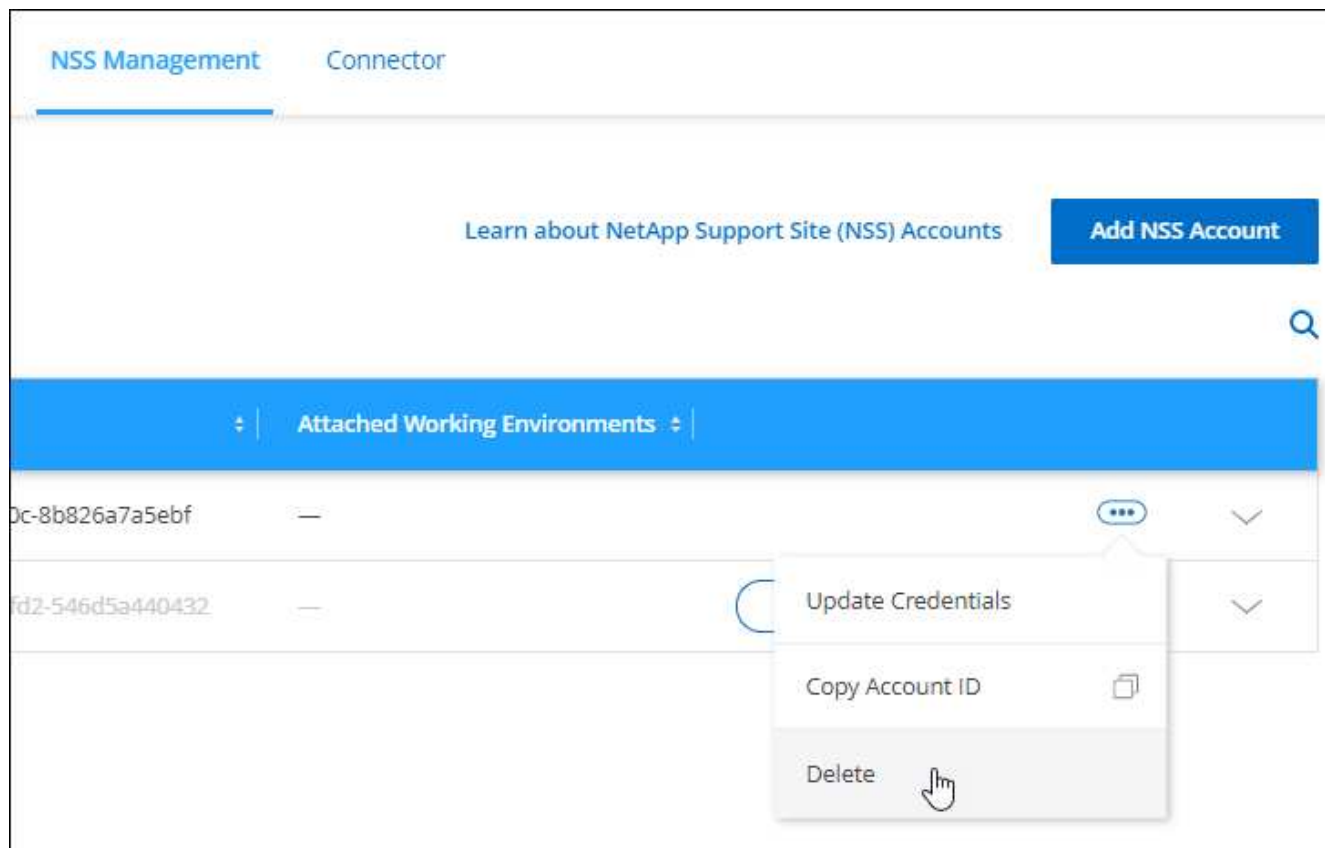
Supprimer un compte NSS

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

Notez que vous ne pouvez pas supprimer un compte actuellement associé à un environnement de travail Cloud Volumes ONTAP. Vous devez d'abord associer un environnement de travail à un autre compte NSS, Reliez ces environnements de travail à un autre compte NSS.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.
2. Cliquez sur **NSS Management**.
3. Pour le compte NSS que vous souhaitez supprimer, cliquez sur **...** Puis sélectionnez **Supprimer**.



4. Cliquez sur **Supprimer** pour confirmer.

Mes opportunités

Sur le Canvas, l'onglet **Mes opportunités** fournit un emplacement centralisé pour découvrir les ressources existantes que vous pouvez ajouter à BlueXP afin de garantir la cohérence des services de données et des opérations dans votre environnement multicloud hybride.

Actuellement, My Opportunities vous permet de découvrir les systèmes de fichiers FSX existants pour les systèmes de fichiers ONTAP dans votre compte AWS.

["Découvrez comment découvrir FSX pour ONTAP à l'aide de Mes opportunités"](#)

Informations sur le copyright

Copyright © 2022 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.