



Administration de BlueXP

Setup and administration

NetApp
April 26, 2024

This PDF was generated from <https://docs.netapp.com/fr-fr/bluexp-setup-admin/concept-federation.html> on April 26, 2024. Always check docs.netapp.com for the latest.

Sommaire

- Administration de BlueXP 1
 - Utilisation de la fédération des identités avec BlueXP 1
 - Comptes BlueXP 6
 - Connecteurs 21
 - Informations d'identification et abonnements 41

Administration de BlueXP

Utilisation de la fédération des identités avec BlueXP

fédération des identités active l'authentification unique avec BlueXP pour que les utilisateurs puissent se connecter à l'aide d'identifiants à partir de votre identité d'entreprise. Pour commencer, découvrez le fonctionnement de la fédération des identités avec BlueXP, puis passez en revue un aperçu du processus de configuration.

fédération des identités avec informations d'identification NSS

Si vous utilisez vos identifiants du site du support NetApp (NSS) pour vous connecter à BlueXP, vous ne devez pas suivre les instructions sur cette page pour configurer la fédération des identités. Procédez comme suit :

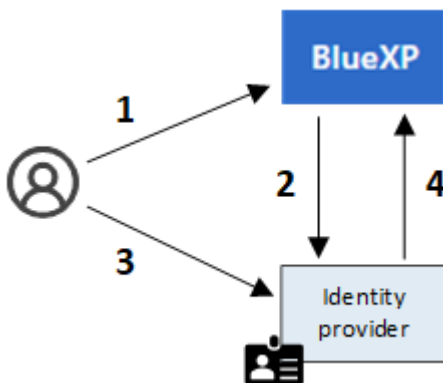
- Téléchargez et complétez le ["Formulaire de demande de la fédération NetApp"](#)
- Envoyez le formulaire à l'adresse électronique indiquée dans le formulaire

L'équipe de gestion des identités et des accès de NetApp examine votre demande.

Fonctionnement de la fédération des identités

La configuration de la fédération des identités crée une connexion de confiance entre le fournisseur de services d'authentification (auth0) de BlueXP et votre propre fournisseur de gestion des identités.

L'image suivante décrit le fonctionnement de la fédération des identités avec BlueXP :



1. Un utilisateur saisit son adresse e-mail sur la page de connexion BlueXP.
2. BlueXP identifie que le domaine de messagerie fait partie d'une connexion fédérée et envoie la demande d'authentification au fournisseur d'identités via la connexion approuvée.

Lorsque vous configurez une connexion fédérée, BlueXP utilise toujours cette connexion fédérée pour l'authentification.

3. L'utilisateur s'authentifie à l'aide des informations d'identification de votre annuaire d'entreprise.
4. Votre fournisseur d'identités authentifie l'identité de l'utilisateur et celui-ci est connecté à BlueXP.

La fédération des identités utilise des normes ouvertes, telles que SAML (Security assertion Markup Language) 2.0 et OIDC (OpenID Connect).

Fournisseurs d'identité pris en charge

BlueXP prend en charge les fournisseurs d'identités suivants :

- Fournisseurs d'identité SAML (Security assertion Markup Language)
- ID Microsoft Entra
- ADFS (Active Directory Federation Services)
- PingFederate

BlueXP prend uniquement en charge les SSO initiées par le fournisseur de services (initiées par le processeur de service). L'authentification unique initiée par le fournisseur d'identité (IDP) n'est pas prise en charge.

Présentation du processus de configuration


Avant de configurer une connexion entre BlueXP et votre fournisseur de gestion des identités, vous devez connaître les étapes à suivre pour vous préparer en conséquence.

Ces étapes sont spécifiques aux utilisateurs qui se connectent à BlueXP via un identifiant cloud NetApp. Si vous utilisez vos identifiants NSS pour vous connecter à BlueXP, [Découvrez comment configurer la fédération des identités avec les informations d'identification NSS](#).

Fournisseur d'identité SAML

Sur un plan général, la configuration d'une connexion fédérée entre BlueXP et un fournisseur d'identité SAML comprend les étapes suivantes :


Étape	Terminé par	Description
1	Administrateur Active Directory (AD)	<p>Configurez votre fournisseur d'identités SAML pour activer la fédération des identités avec BlueXP.</p> <p>Afficher les instructions pour votre fournisseur d'identité SAML :</p> <ul style="list-style-type: none">• "ADFS"• "Okta"• "OneLogin"• "PingFederate"• "Une plateforme Salesforce"• "SiteMinder"• "SSOCircle" <p>Si votre fournisseur d'identité n'apparaît pas dans la liste ci-dessus, "suivez ces instructions génériques"</p> <div><p>Faites <i>not</i> terminez les étapes qui décrivent comment créer une connexion dans auth0. Vous allez créer cette connexion à l'étape suivante.</p></div>

Étape	Terminé par	Description
2	Administrateur BlueXP	<p>Accédez au "Page d'installation de la fédération NetApp" Et créez la connexion avec BlueXP.</p> <p>Pour effectuer cette étape, vous devez obtenir les informations suivantes auprès de votre administrateur AD concernant le fournisseur d'identité :</p> <ul style="list-style-type: none"> • URL de connexion • Un certificat de signature X509 (format PEM ou CER) • URL de déconnexion (facultatif) <p>Après avoir créé la connexion à l'aide de ces informations, la page Configuration de la fédération répertorie les paramètres que vous pouvez envoyer à votre administrateur AD pour terminer la configuration à l'étape suivante.</p> <div>  <p>Notez la date d'expiration du certificat. Vous devez revenir à la page de configuration de la fédération et mettre à jour le certificat <i>avant</i> qu'il n'expire. C'est votre responsabilité. BlueXP ne suit pas la date d'expiration. Il est préférable de travailler avec votre équipe AD pour être alerté à temps.</p> </div>
3	AD admin	Terminez la configuration sur le fournisseur d'identité en utilisant les paramètres indiqués sur la page Configuration de la fédération après avoir terminé l'étape 2.
4	Administrateur BlueXP	<p>Tester et activer la connexion à partir du "Page d'installation de la fédération NetApp"</p> <p>Notez que la page s'actualise entre le test de la connexion et l'activation de la connexion.</p>

ID Microsoft Entra

Sur un plan général, la configuration d'une connexion fédérée entre BlueXP et Microsoft Entra ID comprend les étapes suivantes :


Étape	Terminé par	Description
1	AD admin	<p>Configurez Microsoft Entra ID pour activer la fédération des identités avec BlueXP.</p> <p>"Afficher les instructions d'enregistrement de l'application avec Microsoft Entra ID"</p> <div>  <p>Faites <i>not</i> terminez les étapes qui décrivent comment créer une connexion dans auth0. Vous allez créer cette connexion à l'étape suivante.</p> </div>

Étape	Terminé par	Description
2	Administrateur BlueXP	<p>Accédez au "Page d'installation de la fédération NetApp" Et créez la connexion avec BlueXP.</p> <p>Pour effectuer cette étape, vous devez obtenir les informations suivantes auprès de votre administrateur AD :</p> <ul style="list-style-type: none"> • ID client • Valeur secrète du client • Domaine d'ID Microsoft Entra <p>Après avoir créé la connexion à l'aide de ces informations, la page Configuration de la fédération répertorie les paramètres que vous pouvez envoyer à votre administrateur AD pour terminer la configuration à l'étape suivante.</p> <div>  <p>Notez la date d'expiration de la clé secrète. Vous devez revenir à la page de configuration de la fédération et mettre à jour le certificat <i>avant</i> qu'il n'expire. C'est votre responsabilité. BlueXP ne suit pas la date d'expiration. Il est préférable de travailler avec votre équipe AD pour être alerté à temps.</p> </div>
3	AD admin	Terminez la configuration dans Microsoft Entra ID à l'aide des paramètres affichés sur la page Configuration de la fédération après avoir terminé l'étape 2.
4	Administrateur BlueXP	<p>Tester et activer la connexion à partir du "Page d'installation de la fédération NetApp"</p> <p>Notez que la page s'actualise entre le test de la connexion et l'activation de la connexion.</p>

ADFS


Sur un plan général, la configuration d'une connexion fédérée entre BlueXP et ADFS comprend les étapes suivantes :


Étape	Terminé par	Description
1	AD admin	<p>Configurez le serveur ADFS pour activer la fédération des identités avec BlueXP.</p> <p>"Afficher les instructions de configuration du serveur ADFS avec auth0"</p>

Étape	Terminé par	Description
2	Administrateur BlueXP	<p>Accédez au "Page d'installation de la fédération NetApp" Et créez la connexion avec BlueXP.</p> <p>Pour effectuer cette étape, vous devez obtenir les informations suivantes auprès de votre administrateur AD : l'URL du serveur ADFS ou du fichier de métadonnées de fédération.</p> <p>Après avoir créé la connexion à l'aide de ces informations, la page Configuration de la fédération répertorie les paramètres que vous pouvez envoyer à votre administrateur AD pour terminer la configuration à l'étape suivante.</p> <div>  <p>Notez la date d'expiration du certificat. Vous devez revenir à la page de configuration de la fédération et mettre à jour le certificat <i>avant</i> qu'il n'expire. C'est votre responsabilité. BlueXP ne suit pas la date d'expiration. Il est préférable de travailler avec votre équipe AD pour être alerté à temps.</p> </div>
3	AD admin	Terminez la configuration sur le serveur ADFS en utilisant les paramètres indiqués sur la page Configuration de la fédération après avoir terminé l'étape 2.
4	Administrateur BlueXP	<p>Tester et activer la connexion à partir du "Page d'installation de la fédération NetApp"</p> <p>Notez que la page s'actualise entre le test de la connexion et l'activation de la connexion.</p>

PingFederate

Sur un niveau général, la configuration d'une connexion fédérée entre BlueXP et un serveur PingFederate comprend les étapes suivantes :

Étape	Terminé par	Description
1	AD admin	<p>Configurez votre serveur PingFederate pour activer la fédération des identités avec BlueXP.</p> <p>"Afficher les instructions de création d'une connexion"</p> <div>  <p>Faites <i>not</i> terminez les étapes qui décrivent comment créer une connexion dans auth0. Vous allez créer cette connexion à l'étape suivante.</p> </div>

Étape	Terminé par	Description
2	Administrateur BlueXP	<p>Accédez au "Page d'installation de la fédération NetApp" Et créez la connexion avec BlueXP.</p> <p>Pour effectuer cette étape, vous devez obtenir les informations suivantes auprès de votre administrateur AD :</p> <ul style="list-style-type: none"> • URL du serveur PingFederate • Un certificat de signature X509 (format PEM ou CER) <p>Après avoir créé la connexion à l'aide de ces informations, la page Configuration de la fédération répertorie les paramètres que vous pouvez envoyer à votre administrateur AD pour terminer la configuration à l'étape suivante.</p> <div>  <p>Notez la date d'expiration du certificat. Vous devez revenir à la page de configuration de la fédération et mettre à jour le certificat <i>avant</i> qu'il n'expire. C'est votre responsabilité. BlueXP ne suit pas la date d'expiration. Il est préférable de travailler avec votre équipe AD pour être alerté à temps.</p> </div>
3	AD admin	Terminez la configuration sur le serveur PingFederate en utilisant les paramètres indiqués sur la page Configuration de la fédération après avoir terminé l'étape 2.
4	Administrateur BlueXP	<p>Tester et activer la connexion à partir du "Page d'installation de la fédération NetApp"</p> <p>Notez que la page s'actualise entre le test de la connexion et l'activation de la connexion.</p>

Mise à jour d'une connexion fédérée

Une fois que l'administrateur BlueXP a active une connexion, il peut mettre à jour la connexion à tout moment à partir du ["Page d'installation de la fédération NetApp"](#)

Par exemple, vous devrez peut-être mettre à jour la connexion en téléchargeant un nouveau certificat.

L'administrateur BlueXP qui a créé la connexion est le seul utilisateur autorisé à mettre à jour la connexion. Si vous souhaitez ajouter d'autres administrateurs, contactez le support NetApp.

Comptes BlueXP

Gestion de votre compte BlueXP

Lorsque vous créez un compte BlueXP, celui-ci inclut uniquement un utilisateur admin et un espace de travail. Vous pouvez gérer le compte en fonction des besoins de votre entreprise en ajoutant des utilisateurs, en créant des comptes de service à des fins d'automatisation, en ajoutant des espaces de travail, etc.

["Découvrez le fonctionnement des comptes BlueXP"](#).

Gérez votre compte avec 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"](#)

Créer et gérer des utilisateurs

Les utilisateurs de votre compte peuvent accéder aux ressources et les gérer dans des espaces de travail spécifiques.

Ajouter des utilisateurs

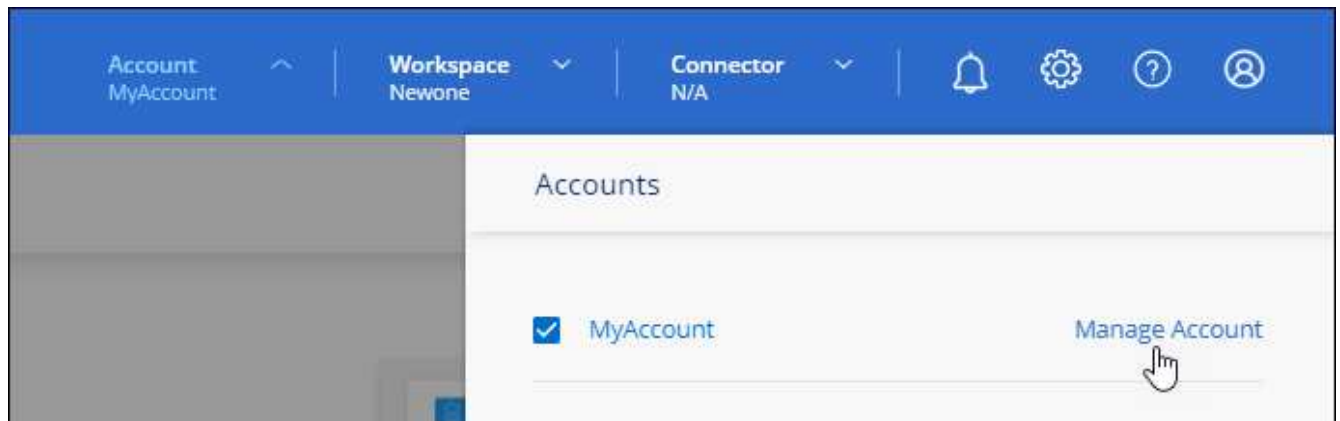
Associez les utilisateurs à votre compte BlueXP pour créer et gérer des environnements de travail dans BlueXP.

Étapes

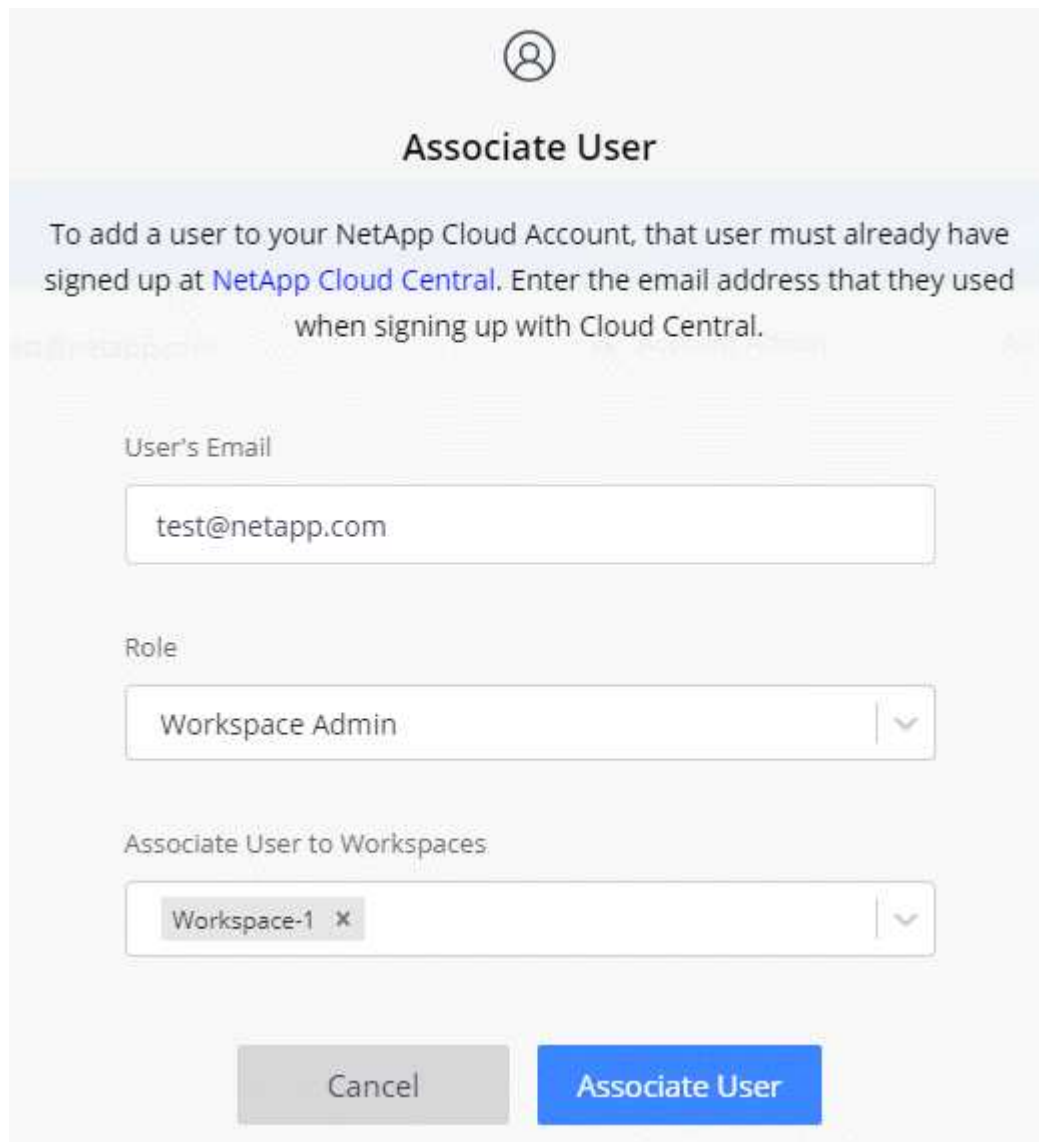
1. Si l'utilisateur ne l'a pas déjà fait, demandez-lui d'aller à ["Site Web NetApp BlueXP"](#) et s'inscrire.
2. Dans le haut de BlueXP, sélectionnez la liste déroulante **compte**.




3. Sélectionnez **gérer le compte** en regard du compte actuellement sélectionné.



4. Dans l'onglet membres, sélectionnez **associer un 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 pour la classification BlueXP et générer des rapports pour les espaces de travail auxquels ils ont accès.
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 web interface for associating a user. At the top is a user icon and the title "Associate User". Below is a light blue banner with instructions: "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." The form has three sections: "User's Email" with a text input containing "test@netapp.com"; "Role" with a dropdown menu showing "Workspace Admin"; and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and 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. Sélectionnez **associer**.

Résultat

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

Supprimer des utilisateurs

La dissociation d'un utilisateur permet de ne plus accéder aux ressources d'un compte BlueXP.

Étapes

1. En haut de BlueXP, sélectionnez la liste déroulante **compte** et sélectionnez **gérer le compte**.



2. Dans l'onglet membres, sélectionnez le menu d'action dans la ligne correspondant à l'utilisateur.



3. Sélectionnez **dissocier utilisateur** et sélectionnez **dissocier** pour confirmer.

Résultat

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

Gérer les espaces de travail d'un administrateur d'espace de travail

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.



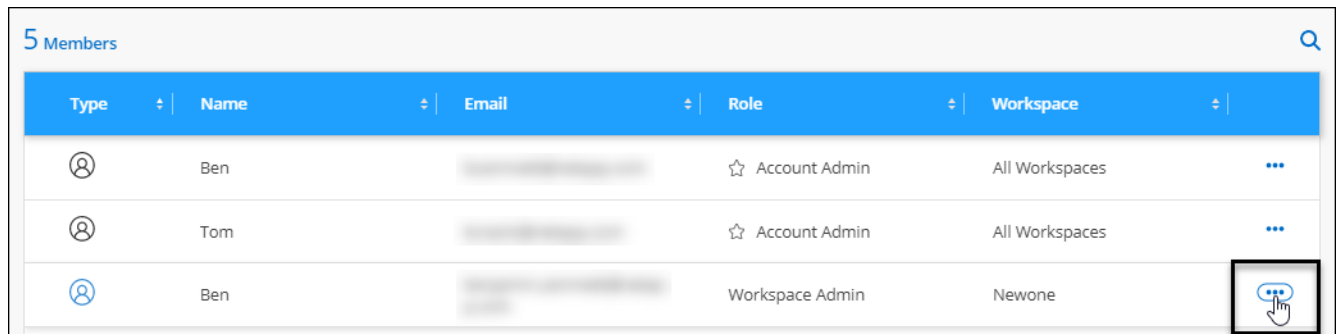
Vous devez également associer le connecteur à des espaces de travail pour que les administrateurs d'espace de travail puissent accéder à ces espaces de travail à partir de BlueXP. ["Apprenez à gérer les espaces de travail d'un connecteur"](#).

Étapes

1. En haut de BlueXP, sélectionnez la liste déroulante **compte** et sélectionnez **gérer le compte**.



2. Dans l'onglet membres, sélectionnez le menu d'action dans la ligne correspondant à l'utilisateur.



3. Sélectionnez **gérer les espaces de travail**.

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

Résultat

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 de 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.

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.

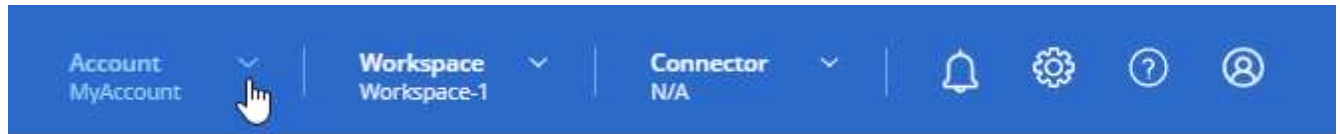
Notez qu'un jeton d'actualisation n'est pas requis pour les opérations d'API lors de l'utilisation d'un compte de service. ["En savoir plus sur les jetons d'actualisation"](#)

Créez un compte de service

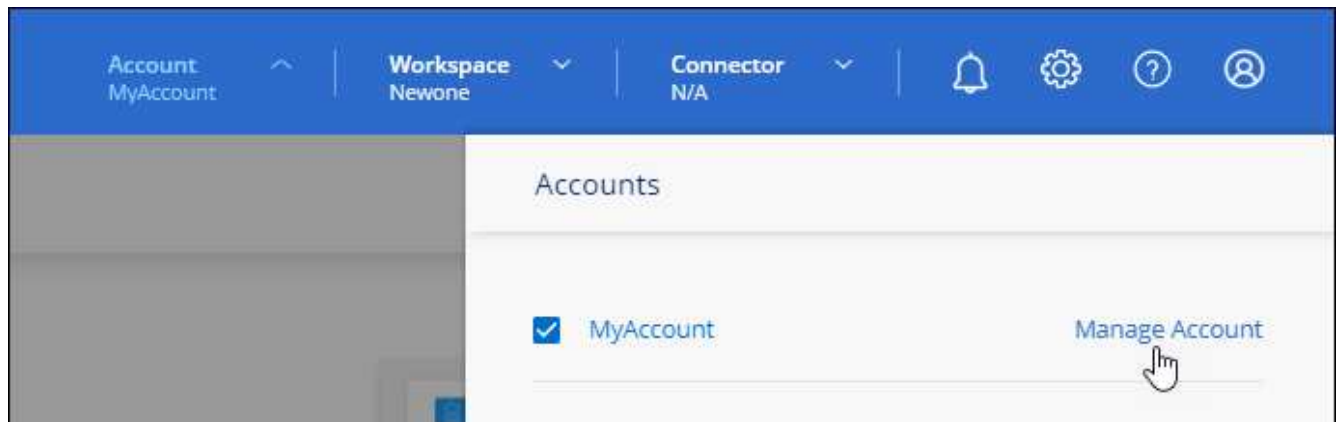
Créez autant de comptes de services que nécessaire pour gérer les ressources de vos environnements de travail.

Étapes

1. Dans le haut de BlueXP, sélectionnez la liste déroulante **compte**.



2. Sélectionnez **gérer le compte** en regard du compte actuellement sélectionné.



3. Dans l'onglet membres, sélectionnez **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. Sélectionnez **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. Sélectionnez **Fermer**.

Obtenir un jeton 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"](#)

Copiez l'ID client

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

Étapes

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



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

Recréez les 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, sélectionnez le menu d'action dans la ligne correspondant au compte de service.



2. Sélectionnez **recréer la clé**.
3. Sélectionnez **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. Sélectionnez **Fermer**.

Supprimer un compte de service

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

Étapes

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



2. Sélectionnez **Supprimer**.
3. Sélectionnez de nouveau **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, sélectionnez la liste déroulante **compte** et sélectionnez **gérer le compte**.
2. Sélectionnez **espaces de travail**.
3. Choisissez l'une des options suivantes :
 - Sélectionnez **Ajouter un nouvel espace de travail** pour créer un nouvel espace de travail.
 - Sélectionnez **Renommer** pour renommer l'espace de travail.
 - Sélectionnez **Supprimer** pour supprimer l'espace de travail.

Si vous avez créé un nouvel espace de travail, vous devez également ajouter le connecteur à cet espace de travail. Si vous n'ajoutez pas le connecteur, les administrateurs de l'espace de travail ne peuvent pas accéder aux ressources de l'espace de travail. Reportez-vous à la section suivante pour plus de détails.

Gérer les 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, sélectionnez la liste déroulante **compte** et sélectionnez **gérer le compte**.
2. Sélectionnez **connecteur**.
3. Sélectionnez **gérer les espaces de travail** pour le connecteur que vous souhaitez associer.
4. Sélectionnez les espaces de travail à associer au connecteur et sélectionnez **appliquer**.

Modifiez le 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, sélectionnez la liste déroulante **compte** et sélectionnez **gérer le compte**.
2. Dans l'onglet **vue d'ensemble**, sélectionnez l'icône de modification située en regard du nom du compte.
3. Saisissez un nouveau nom de compte et sélectionnez **Enregistrer**.

Autoriser les aperçus privés

Autoriser les préversions privées dans votre compte pour accéder aux nouveaux services disponibles en aperçu 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, sélectionnez la liste déroulante **compte** et sélectionnez **gérer le compte**.
2. Dans l'onglet **Présentation**, activez le paramètre **Autoriser aperçu privé**.

Autoriser les 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, sélectionnez la liste déroulante **compte** et sélectionnez **gérer le compte**.
2. Dans l'onglet **Présentation**, activez le paramètre **Autoriser les services tiers**.

Contrôlez les 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.

Le tableau suivant présente une comparaison entre le Centre de notification et le Calendrier pour vous permettre de comprendre ce que chacun a à offrir.

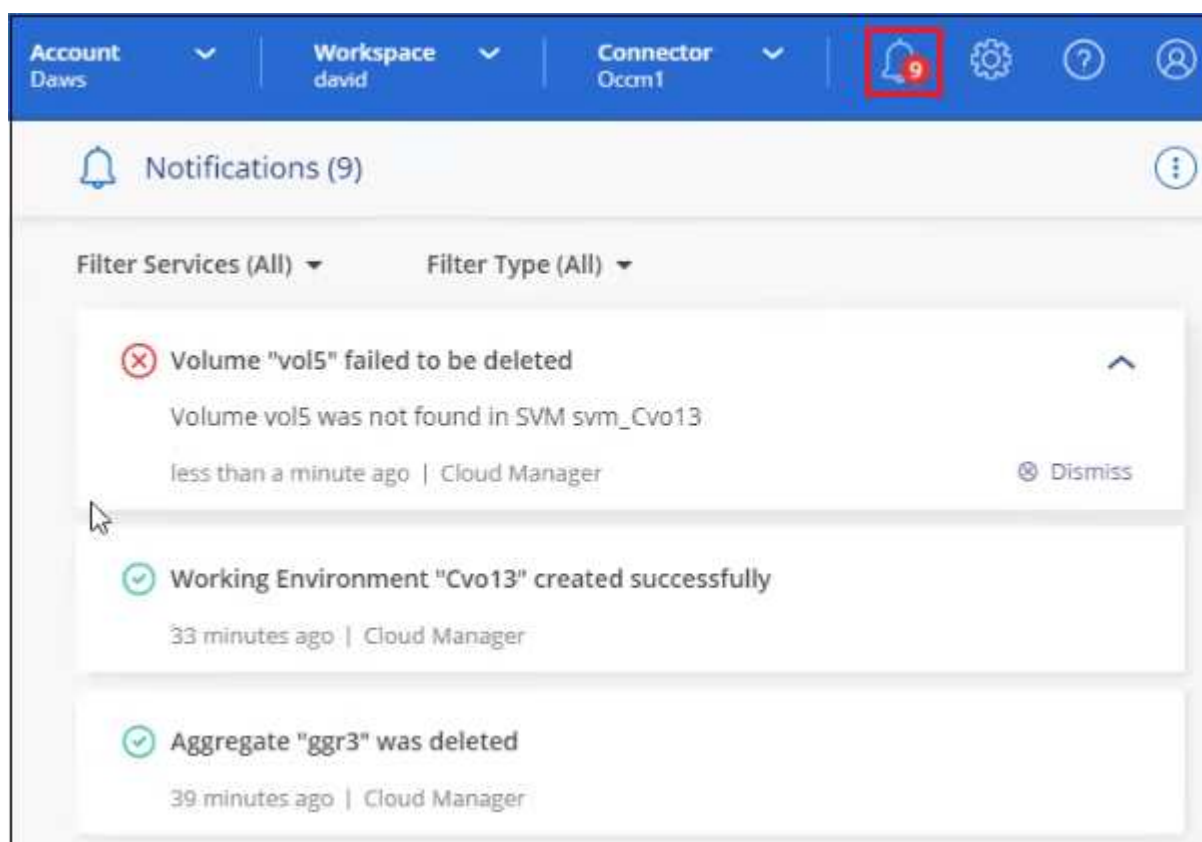
Centre de notification	De la chronologie
Affiche l'état général des événements et des actions	Fournit des détails sur chaque événement ou action pour une enquête plus approfondie
Affiche l'état de la session de connexion en cours (les informations n'apparaîtront pas dans le Centre de notification après 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

Centre de notification	De la chronologie
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

Surveiller les 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 BlueXP ne rapportent pas d'informations dans le Centre de notification pour le moment.

Vous pouvez afficher les notifications en sélectionnant la sonnerie de notification (🔔³) 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 certains types de notifications par e-mail afin de vous tenir informé de l'activité système importante, même si vous n'êtes pas connecté au système. Des e-mails peuvent être envoyés à tous les utilisateurs qui font partie de votre compte BlueXP ou à tout autre destinataire qui doit connaître certains types d'activité système. Découvrez comment [définir les paramètres de notification par e-mail](#).

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.
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.

Filtrer les notifications

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

The image shows a user interface for filtering notifications. It consists of two side-by-side panels, each with a title and a list of items with checkboxes, and buttons at the bottom.

Filter Services (All) ▲

- ☒ Digital Wallet (3)
- ☒ Active IQ (2)
- ☐ AppTemplate (1)

Clear **Apply**

Filter Type (All) ▲


- ☐ Information (0)
- ☐ Success (1)
- ☒ Warning (2)
- ☒ Error (1)
- ☒ Critical (0)
- ☐ Recommendation (0)

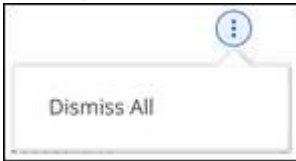
Clear **Apply**

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.

Rejeter les 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, sélectionnez  Et sélectionnez **rejeter tout**.



Pour ignorer les notifications individuelles, placez le curseur sur la notification et sélectionnez **rejeter**.



Définir les 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. Des e-mails peuvent être envoyés à tous les utilisateurs qui font partie de votre compte BlueXP ou à tout autre destinataire qui doit connaître certains types d'activité système.



- Des notifications sont alors envoyées par e-mail pour les fonctionnalités et services BlueXP suivants : connecteur, portefeuille digital BlueXP, copie et synchronisation BlueXP, sauvegarde et restauration BlueXP, Tiering BlueXP et rapports de migration BlueXP. 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.

Les filtres définis dans le Centre de notification ne déterminent pas les types de notifications que vous recevrez par e-mail. Par défaut, les administrateurs de compte BlueXP recevront des e-mails pour toutes les notifications « critiques » et « recommandations ». Ces notifications concernent tous les services. Vous ne pouvez pas choisir de recevoir de notifications pour certains services uniquement, par exemple les connecteurs ou la sauvegarde et restauration BlueXP.

Tous les autres utilisateurs et destinataires sont configurés pour ne pas recevoir d'e-mails de notification. Vous devez donc configurer les paramètres de notification pour les utilisateurs supplémentaires.

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

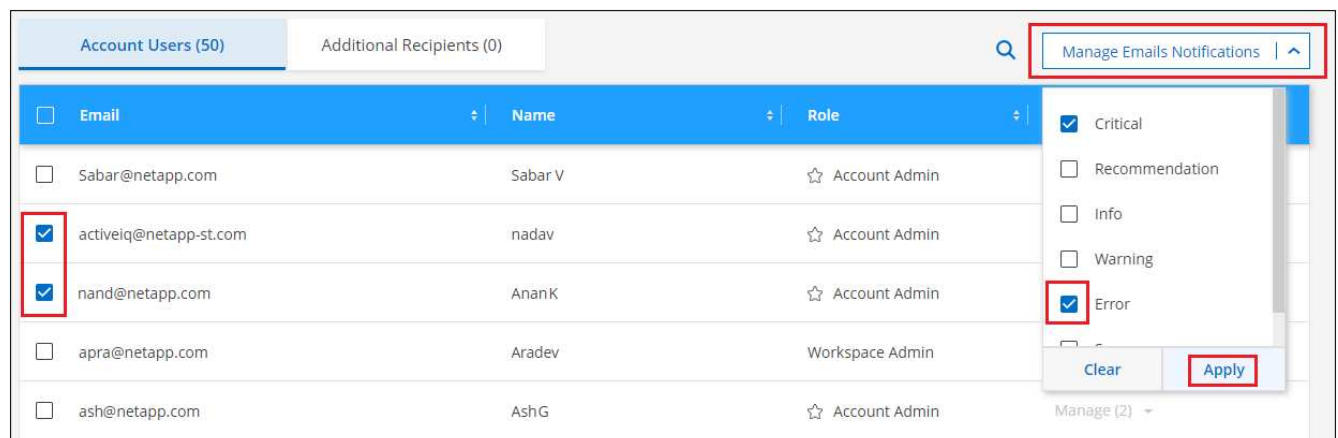
Étapes

1. Dans la barre de menus BlueXP, sélectionnez **Paramètres > Paramètres des alertes et des 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, sélectionnez le menu dans la colonne Notifications de cet utilisateur, vérifiez les types de notifications à envoyer et sélectionnez **appliquer**.
- Pour apporter des modifications à plusieurs utilisateurs, cochez la case correspondant à chaque utilisateur, sélectionnez **gérer les notifications par e-mail**, cochez les types de notifications à envoyer et sélectionnez **appliquer**.



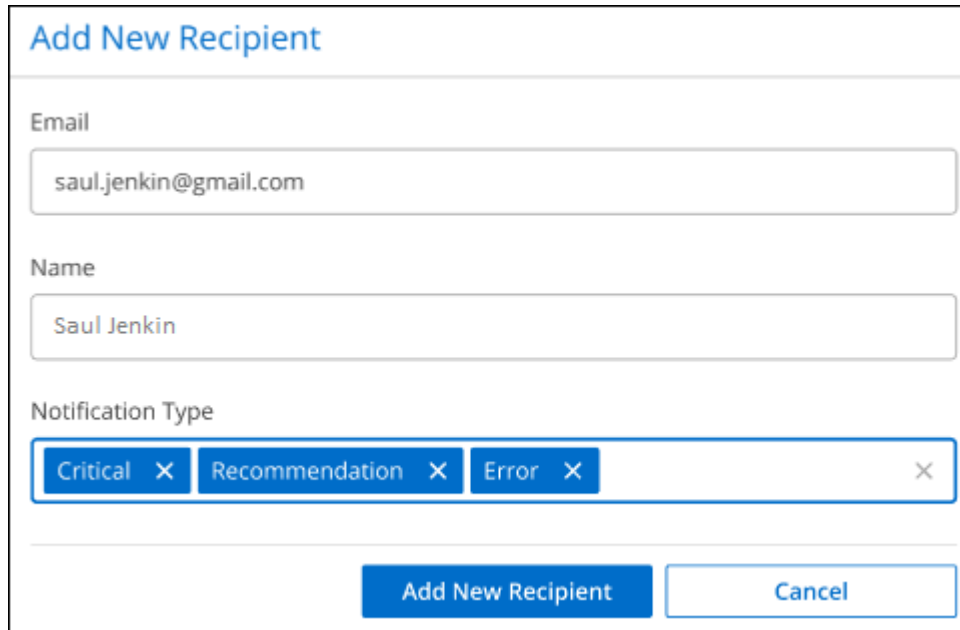
Ajoutez des destinataires supplémentaires

Les utilisateurs qui apparaissent dans l'onglet *Account Users* sont automatiquement renseignés à partir des utilisateurs de votre compte BlueXP (à partir 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, sélectionnez **Ajouter de nouveaux destinataires**.



The screenshot shows a web form titled "Add New Recipient". It contains three input fields: "Email" with the value "saul.jenkin@gmail.com", "Name" with the value "Saul Jenkin", and "Notification Type" which is a tag-based selector showing "Critical", "Recommendation", and "Error". At the bottom of the form 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 sélectionnez **Ajouter nouveau destinataire**.

Audit de l'activité des utilisateurs 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, sélectionnez **Paramètres > Chronologie**.
2. Sous filtres, sélectionnez **Service**, activez **Location** et sélectionnez **appliquer**.

Résultat

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

Créez un autre compte BlueXP

Lorsque vous vous inscrivez à BlueXP, vous êtes invité à créer un compte pour votre entreprise. Ce compte peut être tout ce dont vous avez besoin, mais si votre entreprise a besoin de plusieurs comptes, vous devrez créer des comptes supplémentaires à l'aide de l'API de location.

Utilisez l'appel d'API suivant pour créer un compte BlueXP supplémentaire :

POST /tenancy/account/{accountName}

Si vous souhaitez activer le mode restreint, vous devez inclure les éléments suivants dans le corps de la demande :

```
{
  "isSaasDisabled": true
}
```



Vous ne pouvez pas modifier le paramètre de mode restreint une fois le compte créé par BlueXP. Vous ne pouvez pas activer le mode restreint ultérieurement et vous ne pouvez pas le désactiver ultérieurement. Elle doit être définie au moment de la création du compte.

["Découvrez comment utiliser cet appel d'API"](#)

Liens connexes

- ["Découvrez les comptes BlueXP"](#)
- ["Découvrez les modes de déploiement BlueXP"](#)

Rôles utilisateur

Les rôles Administrateur de compte, Administrateur d'espace de travail, Visionneuse de conformité et Administrateur SnapCenter fournissent des autorisations spécifiques aux utilisateurs. Vous pouvez attribuer l'un de ces rôles lorsque vous associez un nouvel utilisateur à votre compte BlueXP.

Le rôle Compliance Viewer est destiné à l'accès à la classification BlueXP en lecture seule.

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
Supprimer des environnements de travail d'un espace de travail	Oui.	Oui.	Non	Non
Supprimer 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

Tâche	Administrateur du compte	Administrateur de l'espace de travail	Visionneuse de conformité	Admin SnapCenter
Basculer entre les espaces de travail	Oui.	Oui.	Oui.	Non
Afficher les résultats de l'analyse de classification BlueXP	Oui.	Oui.	Oui.	Non
Recevoir le rapport Cloud Volumes ONTAP	Oui.	Non	Non	Non
Créer des connecteurs	Oui.	Non	Non	Non
Gestion des comptes BlueXP	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
Installez un certificat HTTPS	Oui.	Non	Non	Non

Liens connexes

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

Connecteurs

Recherchez l'ID système d'un connecteur

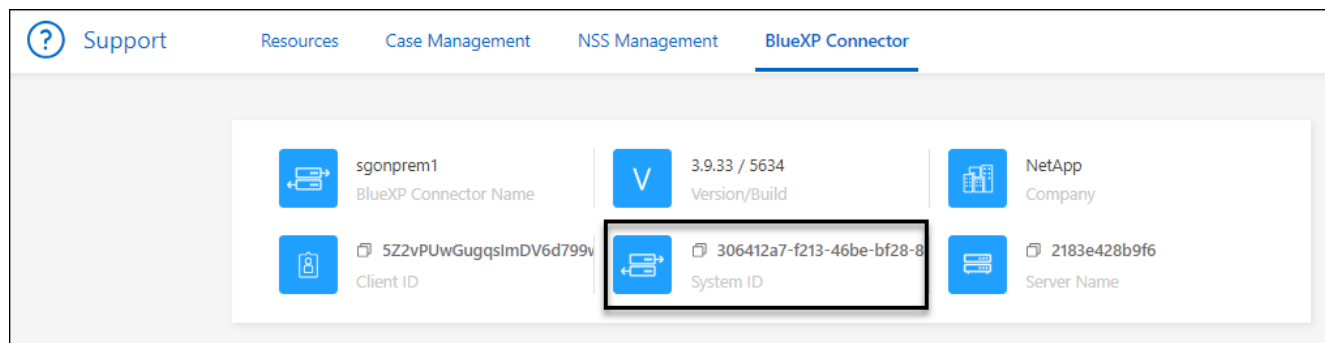
Pour vous aider à démarrer, votre conseiller NetApp peut vous demander l'identifiant système de votre connecteur. L'ID est généralement utilisé à des fins de licence et de dépannage.

Étapes

1. Dans l'angle supérieur droit de la console BlueXP, sélectionnez l'icône aide.
2. Sélectionnez **support > BlueXP Connector**.

L'ID système apparaît en haut de la page.

Exemple



Gérer les connecteurs existants

Une fois que vous avez créé un connecteur, vous devrez peut-être le gérer de temps en temps. Par exemple, vous pouvez basculer entre les connecteurs si vous en avez plusieurs. Vous pouvez également avoir besoin de mettre à niveau manuellement le connecteur lorsque vous utilisez BlueXP en mode privé.

["Découvrez le fonctionnement des connecteurs".](#)



Le connecteur comprend une interface utilisateur locale, accessible à partir de l'hôte du connecteur. Cette interface utilisateur est fournie pour les clients qui utilisent BlueXP en mode restreint ou privé. Lorsque vous utilisez BlueXP en mode standard, vous devez accéder à l'interface utilisateur à partir du ["Console SaaS BlueXP"](#)

["Découvrez les modes de déploiement BlueXP".](#)

Maintenance du système d'exploitation et des machines virtuelles

La maintenance du système d'exploitation sur l'hôte du connecteur relève de votre responsabilité. Par exemple, vous devez appliquer des mises à jour de sécurité au système d'exploitation sur l'hôte du connecteur en suivant les procédures standard de votre entreprise pour la distribution du système d'exploitation.

Notez que vous n'avez pas besoin d'arrêter les services sur l'hôte du connecteur lors de l'exécution d'une mise à jour du système d'exploitation.

Si vous devez arrêter puis démarrer le connecteur VM, vous devez le faire depuis la console de votre fournisseur cloud ou en utilisant les procédures standard de gestion sur site.

["Notez que le connecteur doit être opérationnel en permanence".](#)

Type de machine virtuelle ou d'instance

Si vous avez créé un connecteur directement à partir de BlueXP, BlueXP a déployé une instance de machine virtuelle dans votre fournisseur cloud à l'aide d'une configuration par défaut. Après avoir créé le connecteur, vous ne devez pas passer à une instance de machine virtuelle plus petite qui a moins de CPU ou de RAM.

Les exigences relatives au CPU et à la RAM sont les suivantes :

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

["En savoir plus sur la configuration par défaut du connecteur".](#)

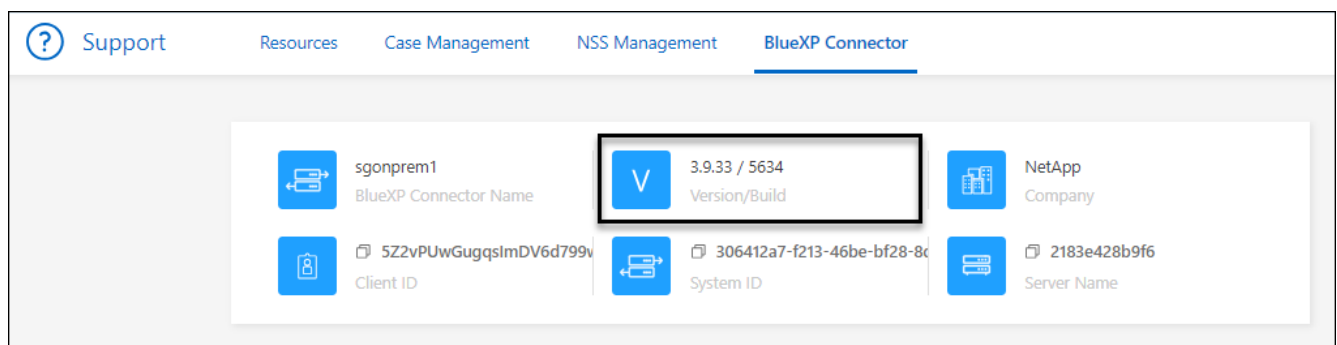
Afficher la version d'un connecteur

Vous pouvez afficher la version de votre connecteur pour vérifier que le connecteur est automatiquement mis à niveau vers la dernière version ou parce que vous devez le partager avec votre représentant NetApp.

Étapes

1. Dans l'angle supérieur droit de la console BlueXP, sélectionnez l'icône aide.
2. Sélectionnez **support > BlueXP Connector**.

La version s'affiche en haut de la page.



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. Sélectionnez la liste déroulante **Connector**, sélectionnez un autre connecteur, puis sélectionnez **Switch**.



Résultat

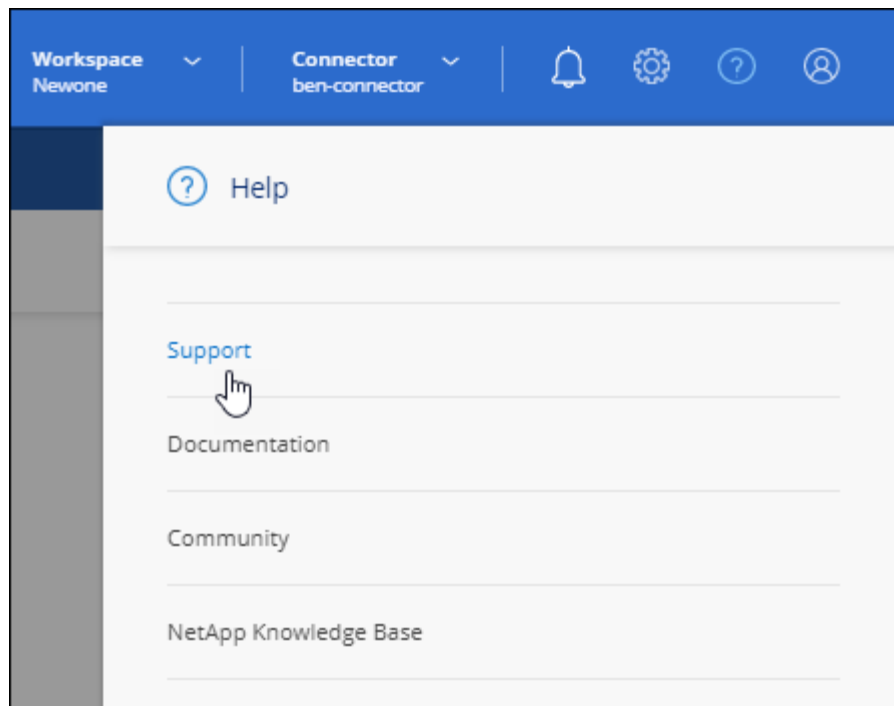
BlueXP actualise et affiche les environnements de travail associés au connecteur sélectionné.

Téléchargez ou envoyez un message AutoSupport

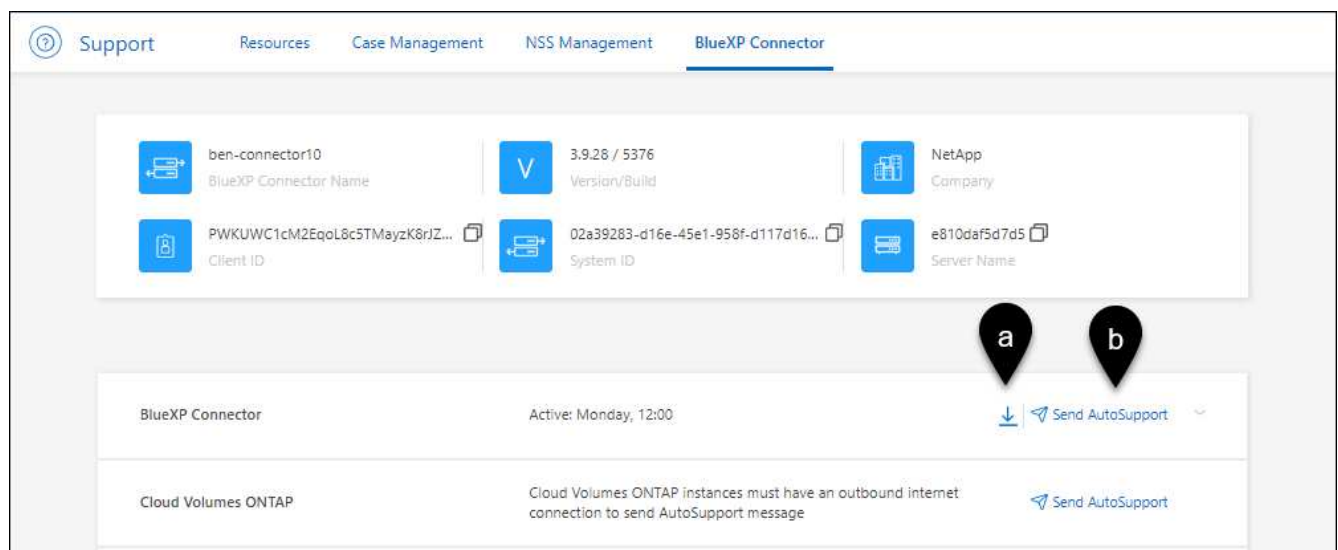
En cas de problème, les équipes NetApp peuvent vous demander d'envoyer un message AutoSupport au support NetApp à des fins de dépannage.

Étapes

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



2. Sélectionnez **BlueXP Connector**.
3. 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. Sélectionnez **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. Le nom d'utilisateur de l'instance

EC2 Linux est ubuntu (pour les connecteurs créés avant mai 2023, le nom d'utilisateur était ec2-user).

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

Azure

Lorsque vous avez créé la machine virtuelle du connecteur dans Azure, vous avez spécifié un nom d'utilisateur et choisi de vous authentifier à l'aide d'un mot de passe ou d'une clé publique SSH. Utiliser 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"](#)

Requièrent l'utilisation d'IMDSv2 sur les instances Amazon EC2

À partir de mars 2024, BlueXP prend désormais en charge Amazon EC2 instance Metadata Service version 2 (IMDSv2) avec le connecteur et avec Cloud Volumes ONTAP (y compris le médiateur pour les déploiements HA). Dans la plupart des cas, IMDSv2 est automatiquement configuré sur les nouvelles instances EC2. IMDSv1 a été activé avant mars 2024. Si vos stratégies de sécurité l'exigent, vous devrez peut-être configurer manuellement IMDSv2 sur vos instances EC2.

Description de la tâche

IMDSv2 fournit une protection améliorée contre les vulnérabilités. ["Pour en savoir plus sur IMDSv2, consultez le blog sur la sécurité AWS"](#)

Le service IMDS (instance Metadata Service) est activé comme suit sur les instances EC2 :

- Pour les déploiements de nouveaux connecteurs à partir de BlueXP ou à l'aide de ["Scripts Terraform"](#), IMDSv2 est activé par défaut sur l'instance EC2.
- Si vous lancez une nouvelle instance EC2 dans AWS, puis installez manuellement le logiciel Connector, IMDSv2 est également activé par défaut.
- Si vous lancez le connecteur à partir d'AWS Marketplace, IMDSv1 est activé par défaut. Vous pouvez configurer manuellement IMDSv2 sur l'instance EC2.
- Pour les connecteurs existants, IMDSv1 est toujours pris en charge, mais vous pouvez configurer manuellement IMDSv2 sur l'instance EC2 si vous le souhaitez.
- Pour Cloud Volumes ONTAP, IMDSv1 est activé par défaut sur les instances nouvelles et existantes. Si vous le souhaitez, vous pouvez configurer manuellement IMDSv2 sur les instances EC2.

Avant de commencer

- La version du connecteur doit être 3.9.38 ou ultérieure.
- Cloud Volumes ONTAP doit exécuter l'une des versions suivantes :
 - 9.12.1 P2 (ou tout correctif ultérieur)
 - 9.13.0 P4 (ou tout correctif ultérieur)
 - 9.13.1 ou toute version ultérieure à cette version
- Cette modification nécessite le redémarrage des instances Cloud Volumes ONTAP.

Description de la tâche

Ces étapes nécessitent l'utilisation de l'interface de ligne de commande AWS, car vous devez définir la limite de sauts de réponse sur 3.

Étapes

1. Nécessite l'utilisation d'IMDSv2 sur l'instance de connecteur :

- a. Connectez-vous à la VM Linux pour le connecteur.

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. Le nom d'utilisateur de l'instance EC2 Linux est ubuntu (pour les connecteurs créés avant mai 2023, le nom d'utilisateur était ec2-user).

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

- b. Installez l'interface de ligne de commande AWS.

["Documents AWS : installez la dernière version de l'interface de ligne de commande AWS ou effectuez une mise à jour"](#)

- c. Utilisez le `aws ec2 modify-instance-metadata-options` Pour exiger l'utilisation d'IMDSv2 et pour modifier la limite de saut de réponse PUT à 3.

Exemple

```
aws ec2 modify-instance-metadata-options \
  --instance-id <instance-id> \
  --http-put-response-hop-limit 3 \
  --http-tokens required \
  --http-endpoint enabled
```



Le `http-tokens` Le paramètre définit IMDSv2 sur requis. Quand `http-tokens` est obligatoire, vous devez également définir `http-endpoint` sur activé.

2. Exiger l'utilisation d'IMDSv2 sur les instances Cloud Volumes ONTAP :

- a. Accédez au ["Console Amazon EC2"](#)
- b. Dans le volet de navigation, sélectionnez **instances**.
- c. Sélectionnez une instance Cloud Volumes ONTAP.
- d. Sélectionnez **actions > Paramètres de l'instance > Modifier les options de métadonnées de l'instance**.
- e. Dans la boîte de dialogue **Modifier les options de métadonnées** de l'instance, sélectionnez les options suivantes :
 - Pour **instance metadata service**, sélectionnez **Enable**.
 - Pour **IMDSv2**, sélectionnez **obligatoire**.
 - Sélectionnez **Enregistrer**.

- f. Répétez cette procédure pour les autres instances de Cloud Volumes ONTAP, y compris le médiateur

HA.

g. "Arrêtez et démarrez les instances Cloud Volumes ONTAP"

Résultat

L'instance de connecteur et les instances Cloud Volumes ONTAP sont maintenant configurées pour utiliser IMDSv2.

Mettez à niveau le connecteur lorsque vous utilisez le mode privé

Si vous utilisez BlueXP en mode privé, vous pouvez mettre à niveau le connecteur dès qu'une version plus récente est disponible sur le site du support NetApp.

Le connecteur doit redémarrer pendant le processus de mise à niveau afin que la console Web ne soit pas disponible pendant la mise à niveau.



Lorsque vous utilisez BlueXP en mode standard ou restreint, le connecteur met automatiquement à jour ses logiciels vers la dernière version, tant qu'il dispose d'un accès Internet sortant pour obtenir la mise à jour logicielle.

Étapes

1. Téléchargez le logiciel du connecteur à partir du ["Site de support NetApp"](#).

Assurez-vous de télécharger le programme d'installation hors ligne pour les réseaux privés sans accès à Internet.

2. Copiez le programme d'installation sur l'hôte Linux.
3. Attribuez des autorisations pour exécuter le script.

```
chmod +x /path/BlueXP-Connector-offline-<version>
```

Où <version> est la version du connecteur que vous avez téléchargé.

4. Exécutez le script d'installation :

```
sudo /path/BlueXP-Connector-offline-<version>
```

Où <version> est la version du connecteur que vous avez téléchargé.

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

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.

Vous devez mettre à jour l'emplacement de sauvegarde de chaque système Cloud Volumes ONTAP.

- a. Lancer la commande suivante depuis l'interface de ligne de commandes de Cloud Volumes ONTAP pour afficher la cible de sauvegarde actuelle :

```
system configuration backup show
```

- b. Exécutez la commande suivante pour mettre à jour l'adresse IP de la cible de sauvegarde :

```
system configuration backup settings modify -destination <target-  
location>
```

Modifier les URI d'un connecteur

Ajoutez et supprimez l'URI (Uniform Resource identifier) d'un connecteur.

Étapes

1. Sélectionnez la liste déroulante **Connector** dans l'en-tête BlueXP.
2. Sélectionnez **gérer les connecteurs**.
3. Sélectionnez le menu d'action d'un connecteur et sélectionnez **Modifier les URI**.
4. Ajoutez et supprimez des URI, puis sélectionnez **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"](#)

Retirer les connecteurs de BlueXP

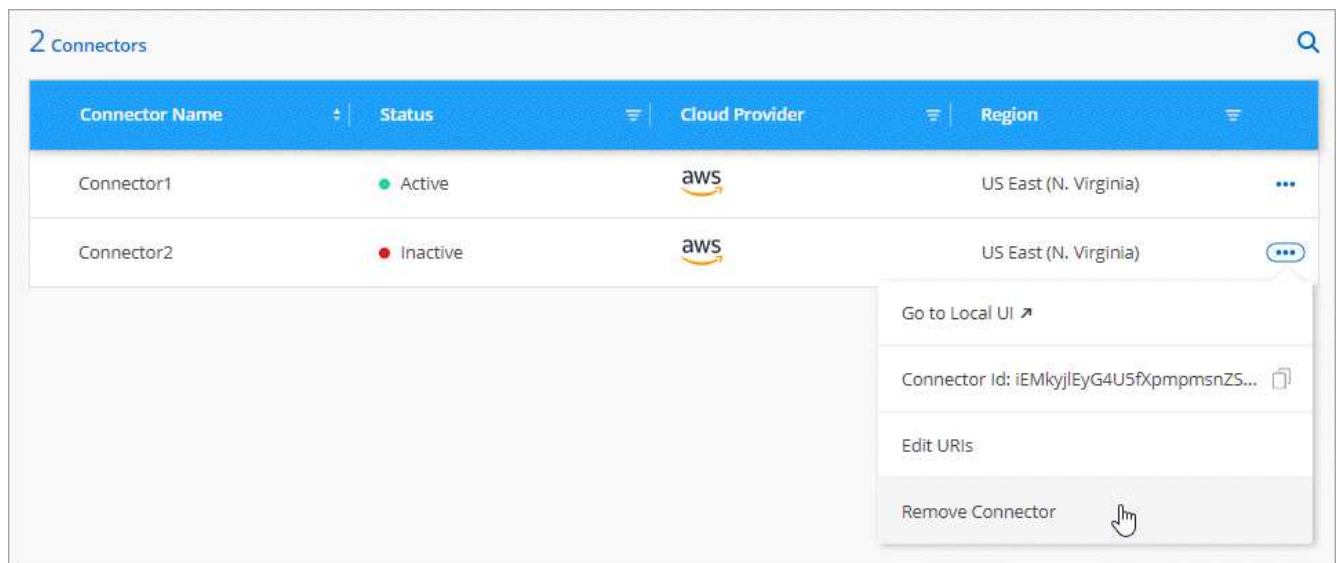
Si un connecteur est inactif, vous pouvez le retirer de la liste des connecteurs dans BlueXP. Vous pouvez le faire si vous avez supprimé la machine virtuelle Connector ou si vous avez désinstallé le logiciel Connector.

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 le réintégrer.

Étapes

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



4. Entrez le nom du connecteur à confirmer, puis sélectionnez **Supprimer**.

Résultat

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 à suivre dépendent de l'installation du connecteur sur un hôte disposant d'un accès à Internet (mode standard ou mode restreint) ou sur un hôte d'un réseau ne disposant pas d'un accès à Internet (mode privé).

Désinstallation en mode standard ou en mode restreint

Les étapes ci-dessous vous permettent de désinstaller le logiciel Connector lorsque vous utilisez BlueXP en mode standard ou restreint.

Étapes

1. Connectez-vous à la VM Linux pour le connecteur.
2. À partir de l'hôte Linux, exécutez le script de désinstallation :

```
/opt/application/netapp/service-manager-2/uninstall.sh [silent]
```

silent exécute le script sans vous demander de confirmer.

Désinstallation en mode privé

Les étapes ci-dessous vous permettent de désinstaller le logiciel Connector lors de l'utilisation de BlueXP en mode privé sans accès à Internet.

Étapes

1. Connectez-vous à la VM Linux pour le connecteur.
2. Depuis l'hôte Linux, exécutez les commandes suivantes :

```
./opt/application/netapp/ds/cleanup.sh  
rm -rf /opt/application/netapp/ds
```

Installez un certificat HTTPS pour un accès sécurisé

Par défaut, BlueXP utilise un certificat auto-signé pour l'accès HTTPS à la console Web. Si votre entreprise l'exige, vous pouvez installer un certificat signé par une autorité de certification, ce qui offre une meilleure protection de sécurité qu'un certificat auto-signé.

Avant de commencer

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

Installez 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, sélectionnez l'icône Paramètres, puis sélectionnez **HTTPS Setup**.

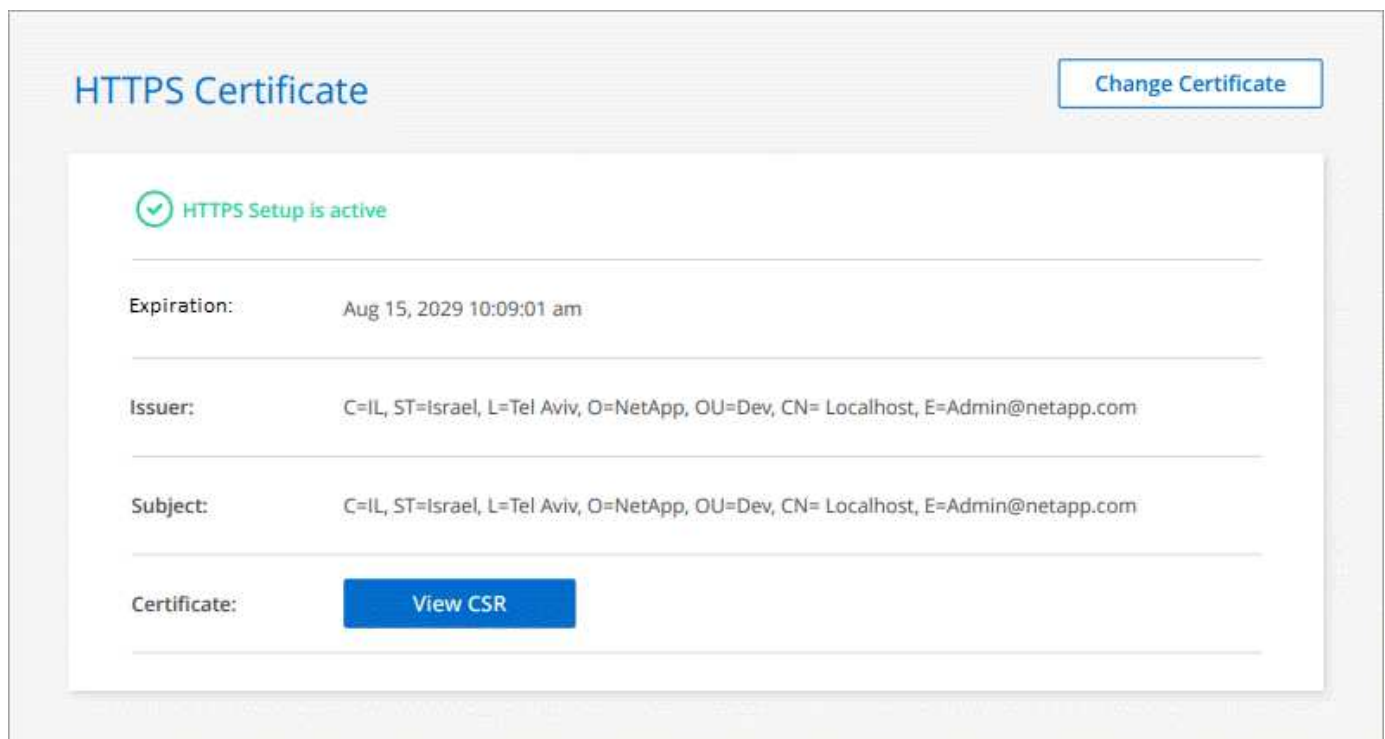


2. Dans la page Configuration HTTPS, installez un certificat en générant une requête de signature de certificat (CSR) ou en installant votre propre certificat signé par l'autorité de certification :

Option	Description
Générez une RSC	<p>a. Entrez le nom d'hôte ou le DNS de l'hôte du connecteur (son nom commun), puis sélectionnez Generate CSR.</p> <p>BlueXP affiche une demande de signature de certificat.</p> <p>b. Utilisez la RSC pour envoyer une demande de certificat SSL à une autorité de certification.</p> <p>Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.</p> <p>c. Téléchargez le fichier de certificat, puis sélectionnez installer.</p>
Installez votre propre certificat signé par l'autorité de certification	<p>a. Sélectionnez installer le certificat signé CA.</p> <p>b. Chargez le fichier de certificat et la clé privée, puis sélectionnez installer.</p> <p>Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.</p>

Résultat

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 :



Renouvelez le 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, sélectionnez l'icône Paramètres, puis sélectionnez **HTTPS Setup**.

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

2. Sélectionnez **Modifier le certificat** et suivez les étapes pour générer une RSC ou installer votre propre certificat signé par l'autorité de certification.

Résultat

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

Configurez un connecteur pour utiliser un serveur proxy

Si vos stratégies d'entreprise nécessitent l'utilisation d'un serveur proxy pour toutes les communications vers Internet, vous devez configurer vos connecteurs pour utiliser ce serveur proxy. Si vous n'avez pas configuré de connecteur pour utiliser un serveur proxy pendant l'installation, vous pouvez configurer le connecteur pour qu'il utilise ce serveur proxy à tout moment.

La configuration du connecteur pour utiliser un serveur proxy 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.

Configurations compatibles

- BlueXP prend en charge HTTP et HTTPS.
- Le serveur proxy peut se trouver dans le cloud ou dans votre réseau.
- BlueXP ne prend pas en charge les serveurs proxy transparents.

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

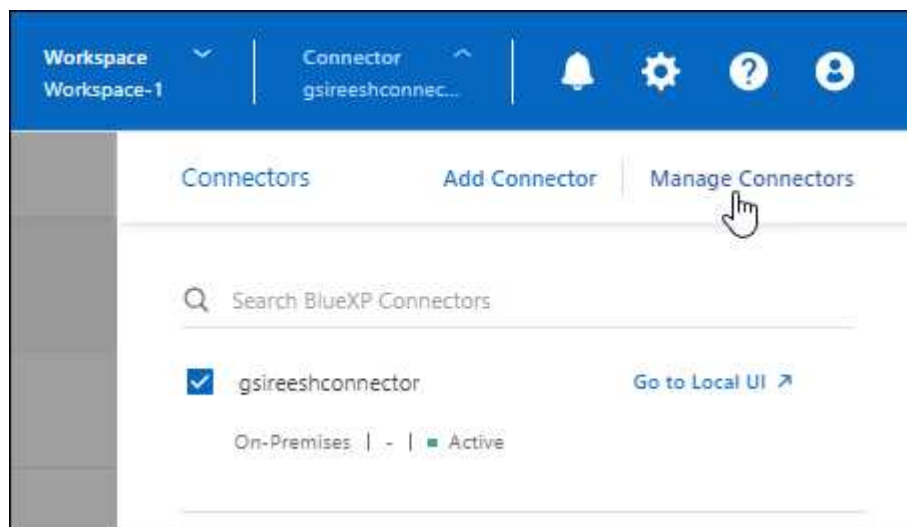
1. Accédez à la page **Edit BlueXP Connector**.

La navigation dépend de si vous utilisez BlueXP en mode standard (accès à l'interface BlueXP depuis le site web SaaS) ou BlueXP en mode restreint ou privé (accès à l'interface BlueXP en local depuis l'hôte

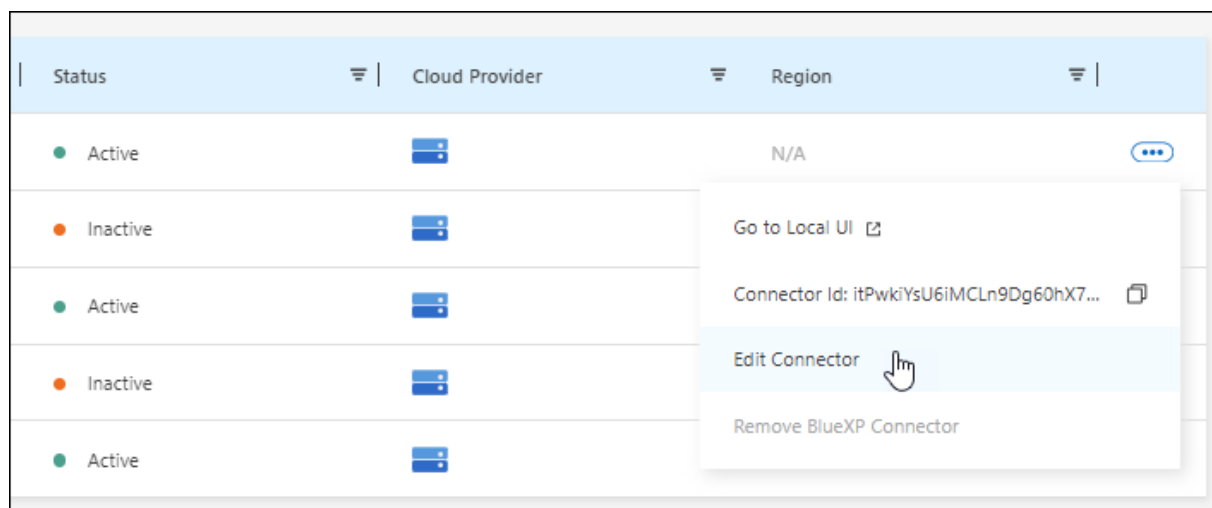
Connector).

Mode standard

- Sélectionnez la liste déroulante **Connector** dans l'en-tête BlueXP.
- Sélectionnez **gérer les connecteurs**.

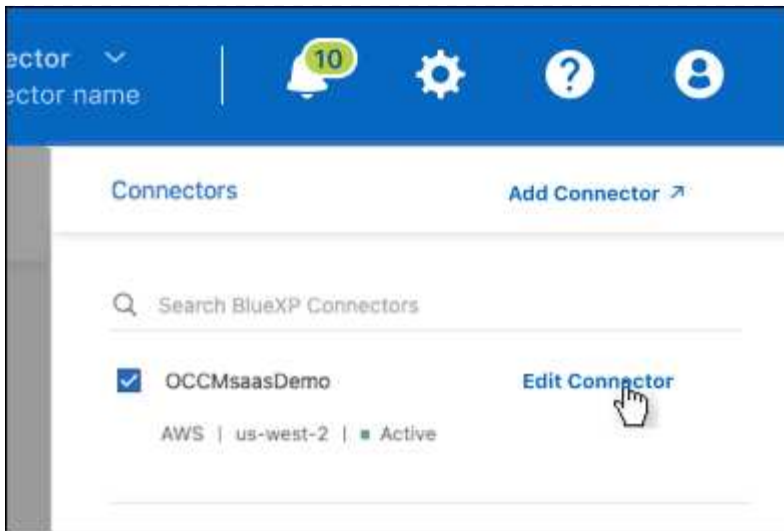


- Sélectionnez le menu d'action d'un connecteur et sélectionnez **Modifier le connecteur**.



Mode restreint ou privé

- Sélectionnez la liste déroulante **Connector** dans l'en-tête BlueXP.
- Sélectionnez **Modifier le connecteur**.



2. Sélectionnez **HTTP Proxy Configuration**.

3. Configurez le proxy :

a. Sélectionnez **Activer le proxy**.

b. Spécifiez le serveur à l'aide de la syntaxe `http://address:port` ou `https://address:port`

c. Spécifiez un nom d'utilisateur et un mot de passe si une authentification de base est requise pour le serveur.

Notez ce qui suit :

- L'utilisateur peut être un utilisateur local ou un utilisateur de domaine.
- Pour un utilisateur de domaine, vous devez entrer le code ASCII du \ comme suit : nom-domaine%92nom-utilisateur

Par exemple : proxy netapp%92proxy

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

d. Sélectionnez **Enregistrer**.

Activation du trafic API direct

Si vous avez configuré un connecteur pour utiliser un serveur proxy, vous pouvez activer le trafic API direct sur le connecteur afin d'envoyer des appels API directement aux services du fournisseur cloud sans passer par le proxy. Cette option est prise en charge avec des connecteurs s'exécutant dans AWS, dans Azure ou dans Google Cloud.

Si vous avez désactivé l'utilisation des liens privés Azure avec Cloud Volumes ONTAP et que vous utilisez plutôt des terminaux de service, vous devez activer le trafic d'API direct. Sinon, le trafic ne sera pas acheminé correctement.

["En savoir plus sur l'utilisation d'un lien privé Azure ou de terminaux de service avec Cloud Volumes ONTAP"](#)

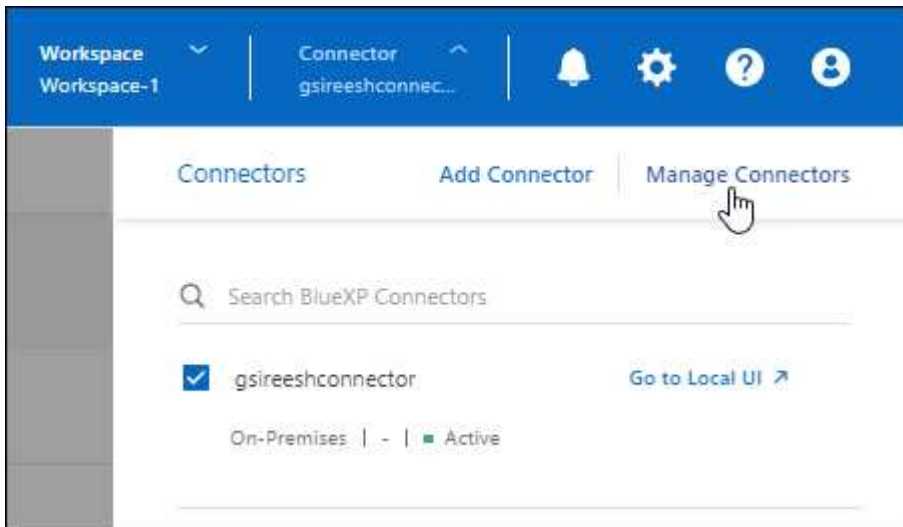
Étapes

1. Accédez à la page **Edit BlueXP Connector** :

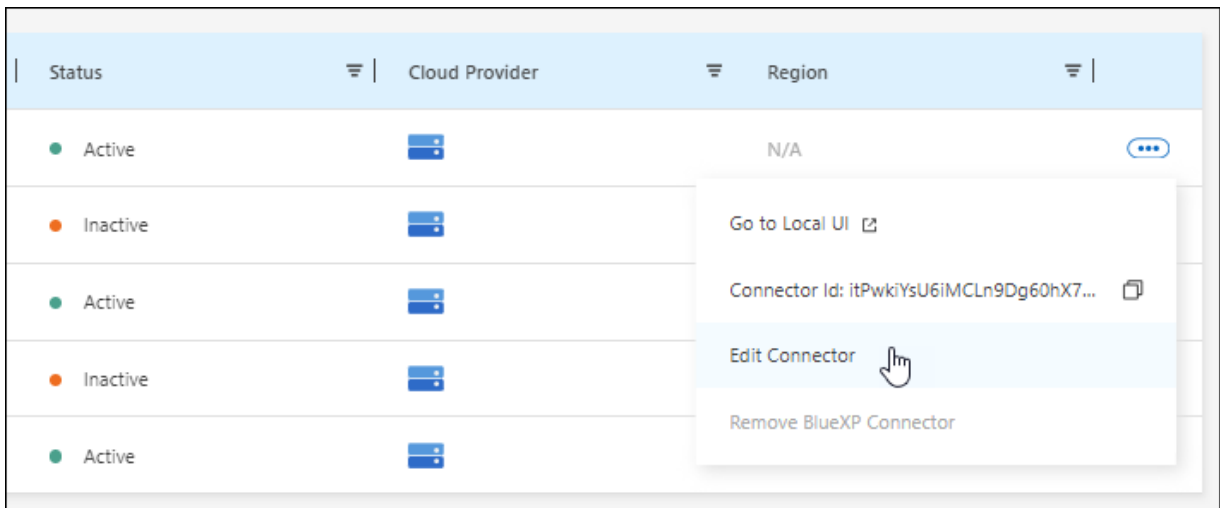
La navigation dépend de si vous utilisez BlueXP en mode standard (accès à l'interface BlueXP depuis le site web SaaS) ou BlueXP en mode restreint ou privé (accès à l'interface BlueXP en local depuis l'hôte Connector).

Mode standard

- Sélectionnez la liste déroulante **Connector** dans l'en-tête BlueXP.
- Sélectionnez **gérer les connecteurs**.

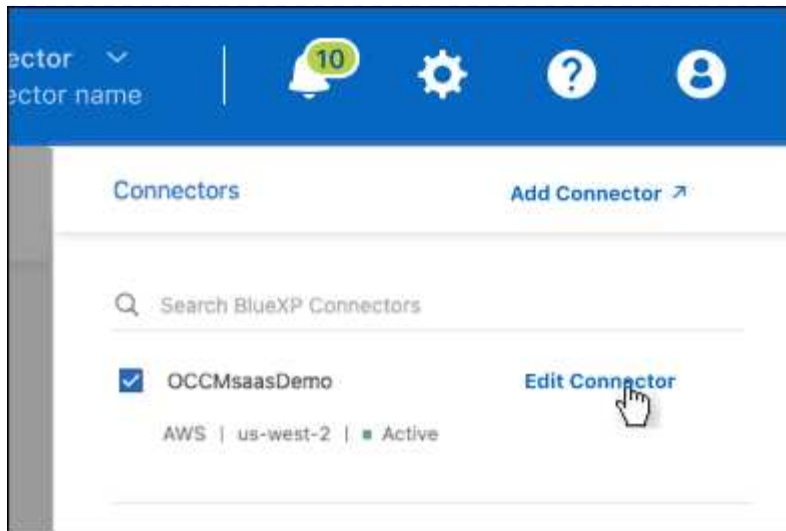


- Sélectionnez le menu d'action d'un connecteur et sélectionnez **Modifier le connecteur**.



Mode restreint ou privé

- Sélectionnez la liste déroulante **Connector** dans l'en-tête BlueXP.
- Sélectionnez **Modifier le connecteur**.



2. Sélectionnez **support Direct API Traffic**.
3. Cochez la case pour activer l'option, puis sélectionnez **Enregistrer**.

Configuration par défaut du connecteur

Vous pouvez en savoir plus sur la configuration du connecteur avant de le déployer ou si vous devez résoudre des 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 Ubuntu 22.04 LTS.

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 EC2 Linux est ubuntu (pour les connecteurs créés avant mai 2023, le nom d'utilisateur était ec2-user).
- 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 Ubuntu 22.04 LTS.

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 à partir de BlueXP, notez les points suivants :

- L'instance de machine virtuelle est n2-standard-4.
- Le système d'exploitation de l'image est Ubuntu 22.04 LTS.

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`
ou
- `/opt/application/netapp/service-manager-2/logs` (à partir de 3.9.23 nouvelles installations)

Les journaux de ces dossiers fournissent des détails sur le connecteur et les images de 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.

Ports

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

- 80 pour l'accès HTTP
- 443 pour l'accès HTTPS

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

Informations d'identification et abonnements

AWS

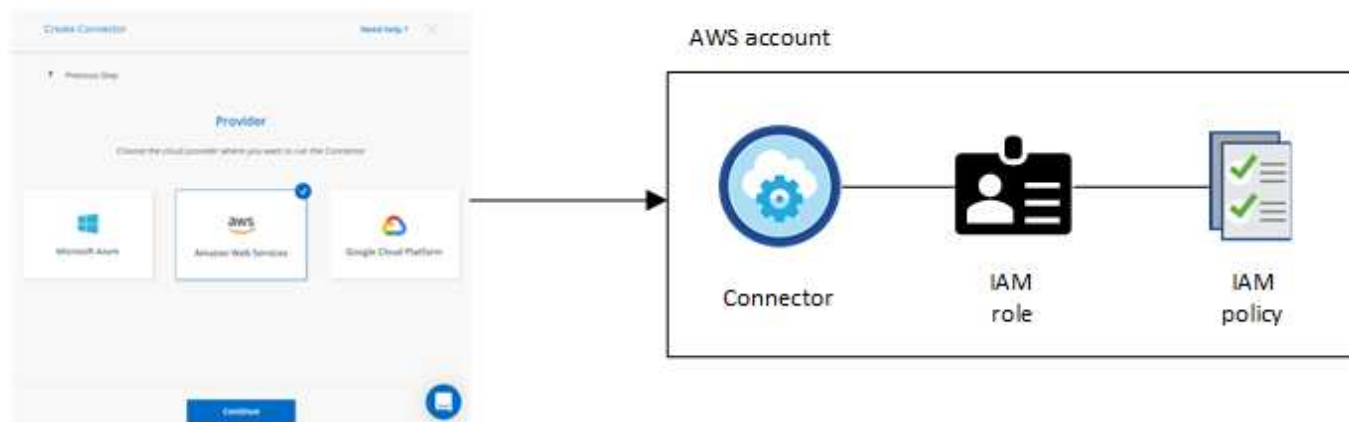
En savoir plus sur les identifiants et les autorisations AWS

Découvrez comment BlueXP utilise les identifiants AWS pour effectuer des actions en votre nom et comment ces identifiants sont associés aux abonnements Marketplace. Ces informations peuvent vous être utiles lorsque vous gérez les identifiants d'un ou plusieurs comptes AWS dans BlueXP. Par exemple, vous pouvez savoir quand ajouter des informations d'identification AWS supplémentaires à BlueXP.

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 ["Politique de déploiement de 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"](#).



Si vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP, BlueXP sélectionne les informations d'identification AWS suivantes par défaut :

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

Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des identifiants AWS initiaux, ou ajouter des identifiants supplémentaires.

Autres identifiants AWS

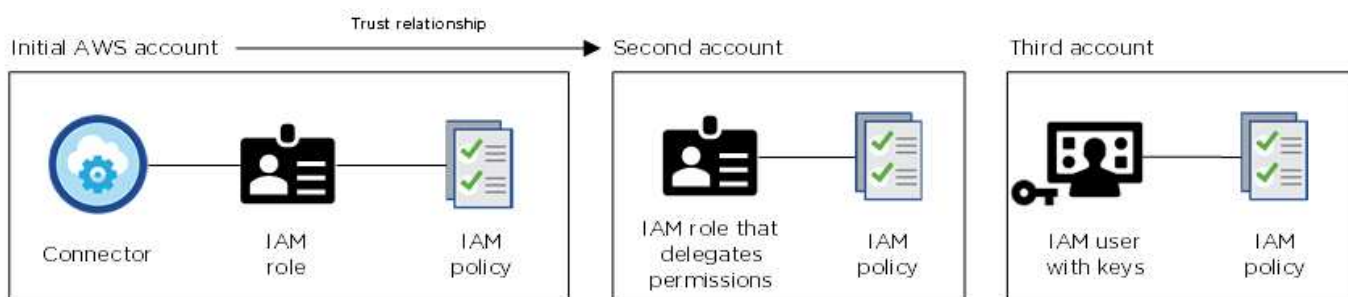
Il existe deux façons d'ajouter des informations d'identification AWS :

- Vous pouvez ajouter des informations d'identification AWS à un connecteur existant
- Vous pouvez ajouter des identifiants AWS directement à BlueXP

Consultez les sections ci-dessous pour en savoir plus.

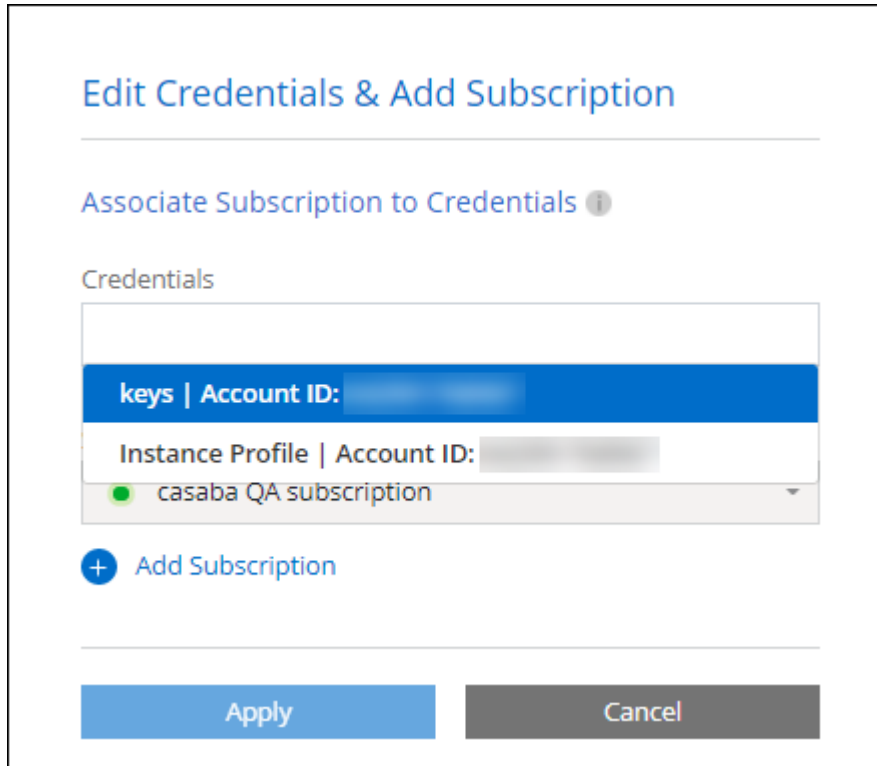
Ajoutez des identifiants AWS à un connecteur existant

Si vous souhaitez utiliser BlueXP avec d'autres comptes AWS, vous pouvez fournir des clés AWS pour un utilisateur IAM ou l'ARN d'un rôle dans un compte approuvé. 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 pouvez ensuite ajouter les informations d'identification du compte à BlueXP en spécifiant le nom de ressource Amazon (ARN) du rôle IAM ou les clés AWS de l'utilisateur IAM.

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



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

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.

- ["Découvrez comment ajouter des identifiants AWS à BlueXP pour Amazon FSX pour ONTAP"](#)
- ["Découvrez comment ajouter des informations d'identification AWS à BlueXP pour créer un connecteur"](#)

Informations d'identification et abonnements Marketplace

Les identifiants que vous ajoutez à un connecteur doivent être associés à un abonnement AWS Marketplace pour que vous puissiez payer Cloud Volumes ONTAP à un taux horaire (PAYGO) ou un contrat annuel, et pour utiliser d'autres services BlueXP.

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

Notez les informations d'identification et les abonnements Marketplace d'AWS :

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

FAQ

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

Comment faire tourner mes identifiants AWS en toute sécurité ?

Comme décrit dans les sections ci-dessus, BlueXP vous permet de fournir des identifiants AWS de quelques manières : un rôle IAM associé à l'instance Connector, en supposant un rôle IAM dans un compte approuvé 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.

Est-il possible de modifier l'abonnement AWS Marketplace pour les environnements de travail Cloud Volumes ONTAP ?

Oui, c'est possible. Lorsque vous modifiez l'abonnement AWS Marketplace associé à un ensemble d'identifiants, tous les environnements de travail Cloud Volumes ONTAP existants et nouveaux seront facturés pour le nouvel abonnement.

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

Puis-je ajouter plusieurs identifiants AWS, chacun avec des abonnements Marketplace différents ?

Tous les identifiants AWS qui appartiennent au même compte AWS seront associés au même abonnement AWS Marketplace.

Si plusieurs identifiants AWS appartiennent à différents comptes AWS, ils peuvent être associés au même abonnement AWS Marketplace ou à d'autres abonnements.

Est-il possible de déplacer les environnements de travail Cloud Volumes ONTAP existants vers un autre compte AWS ?

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

Comment fonctionnent les identifiants pour les déploiements sur site et sur le marché ?

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 d'AWS Marketplace et installer manuellement le logiciel Connector sur votre propre hôte Linux.

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 à l'aide de clés d'accès AWS.

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

- Mode standard

- "Configurez les autorisations d'un déploiement AWS Marketplace"
- "Configurez des autorisations pour les déploiements sur site"
- "Définissez les autorisations pour le mode restreint"
- "Configurez les autorisations pour le mode privé"

Gérez les identifiants AWS et les abonnements Marketplace 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 Marketplace, vous pouvez attribuer chacun d'eux à des informations d'identification AWS différentes à partir de la page d'identification.

Présentation

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

- Ajoutez des identifiants AWS supplémentaires à un connecteur existant

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

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

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

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

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

Comment faire pivoter les informations d'identification

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

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

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

Ajoutez des informations d'identification supplémentaires à un connecteur

Ajoutez des identifiants AWS supplémentaires à un connecteur afin 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.

Si vous venez de commencer à utiliser BlueXP, ["Découvrez comment BlueXP utilise les identifiants et les autorisations AWS"](#).

Accorder des autorisations

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



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

Choix

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

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

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

Si le connecteur est installé sur site, vous ne pouvez pas utiliser cette méthode d'authentification. Vous devez utiliser des clés AWS.

Étapes

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

Assurez-vous de faire ce qui suit :

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

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

Résultat

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

Accordez des autorisations en fournissant des clés AWS

Si vous voulez fournir des clés BlueXP avec AWS pour un utilisateur IAM, vous devez accorder les

autorisations requises à cet utilisateur. La politique de BlueXP IAM définit les actions et les ressources AWS que BlueXP est autorisé à utiliser.

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

Étapes

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

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

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

Résultat

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

Ajoutez les informations d'identification

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

Avant de commencer

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

Étapes

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



3. Sur la page **informations d'identification du compte**, sélectionnez **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 les services BlueXP à un taux horaire (PAYGO) ou dans le cadre d'un contrat annuel, les identifiants AWS doivent être associés à un abonnement AWS Marketplace.

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

Résultat

Vous pouvez maintenant passer à un autre ensemble d'informations d'identification à partir de la page Détails et informations d'identification lors de la création d'un nouvel environnement de travail :

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

keys Account ID:	
Instance Profile Account ID:	

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 à la couche SaaS BlueXP de jouer ce rôle.

Étapes

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

Assurez-vous de faire ce qui suit :

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

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

Résultat

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

Ajoutez les informations d'identification

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

Avant de commencer

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

Étapes

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



2. Sur la page **informations d'identification du compte**, sélectionnez **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. **Révision** : confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Résultat

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

Ajoutez des identifiants à BlueXP pour Amazon FSX pour ONTAP

Pour plus de détails, reportez-vous à la ["Documentation BlueXP pour Amazon FSX pour ONTAP"](#)

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 Cloud Volumes ONTAP à un taux horaire (PAYGO) ou à l'aide d'un contrat annuel, et d'utiliser d'autres services BlueXP.

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 modifier l'abonnement AWS Marketplace associé aux identifiants AWS.

Le remplacement de l'abonnement Marketplace actuel par un nouvel abonnement modifie l'abonnement Marketplace pour tous les environnements de travail Cloud Volumes ONTAP existants et tous les nouveaux environnements de travail.

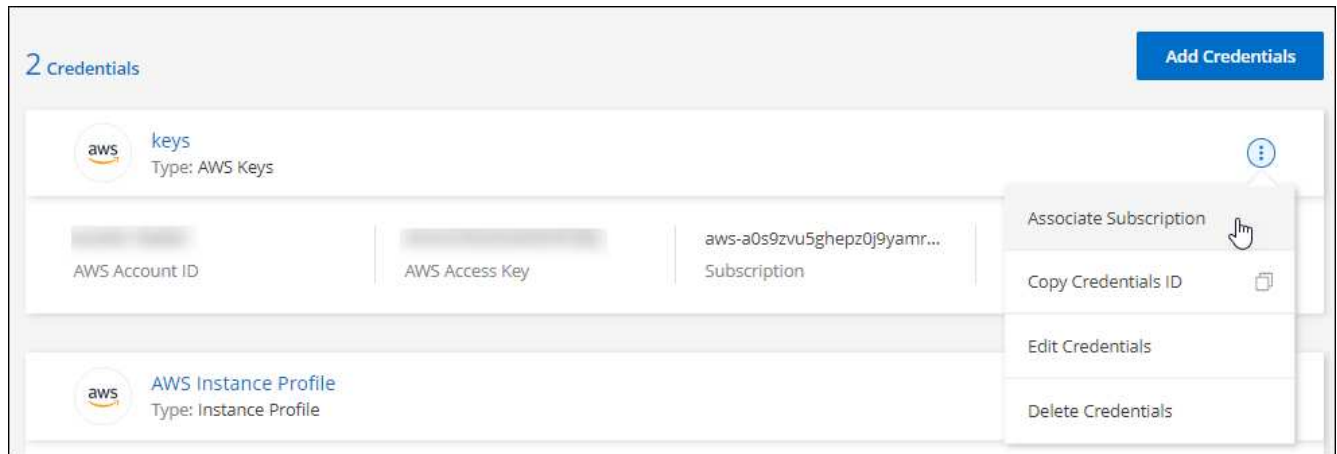
Avant de commencer

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, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
2. Sélectionnez le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **abonnement associé**.

Vous devez sélectionner les informations d'identification associées à un connecteur. Vous ne pouvez pas associer un abonnement Marketplace aux informations d'identification associées à BlueXP.



3. Pour associer les informations d'identification à un abonnement existant, sélectionnez l'abonnement dans la liste déroulante et sélectionnez **associer**.
4. Pour associer les informations d'identification à un nouvel abonnement, sélectionnez **Ajouter un abonnement > Continuer** et suivez les étapes indiquées dans AWS Marketplace :
 - a. Sélectionnez **Afficher les options d'achat**.
 - b. Sélectionnez **s'abonner**.
 - c. Sélectionnez **configurer votre compte**.

Vous serez redirigé vers le site Web BlueXP.

- d. À partir de la page **attribution d'abonnement** :

- Sélectionnez les comptes BlueXP avec lesquels vous souhaitez associer cet abonnement.
- Dans le champ **remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant pour un compte par ce nouvel abonnement.

BlueXP remplace l'abonnement existant pour toutes les informations d'identification du compte par ce nouvel abonnement. Si un ensemble d'informations d'identification n'a jamais été associé à un abonnement, ce nouvel abonnement ne sera pas associé à ces informations d'identification.

Pour tous les autres comptes, vous devez associer manuellement l'abonnement en répétant ces étapes.

- Sélectionnez **Enregistrer**.

La vidéo suivante décrit la procédure de souscription à partir d'AWS Marketplace :

[Abonnez-vous à BlueXP sur AWS Marketplace](#)

Associer un abonnement existant à votre compte

Lorsque vous vous abonnez à BlueXP depuis AWS Marketplace, la dernière étape du processus consiste à associer l'abonnement à vos comptes BlueXP depuis le site web BlueXP. Si vous n'avez pas effectué cette étape, vous ne pouvez pas utiliser l'abonnement avec votre compte BlueXP.

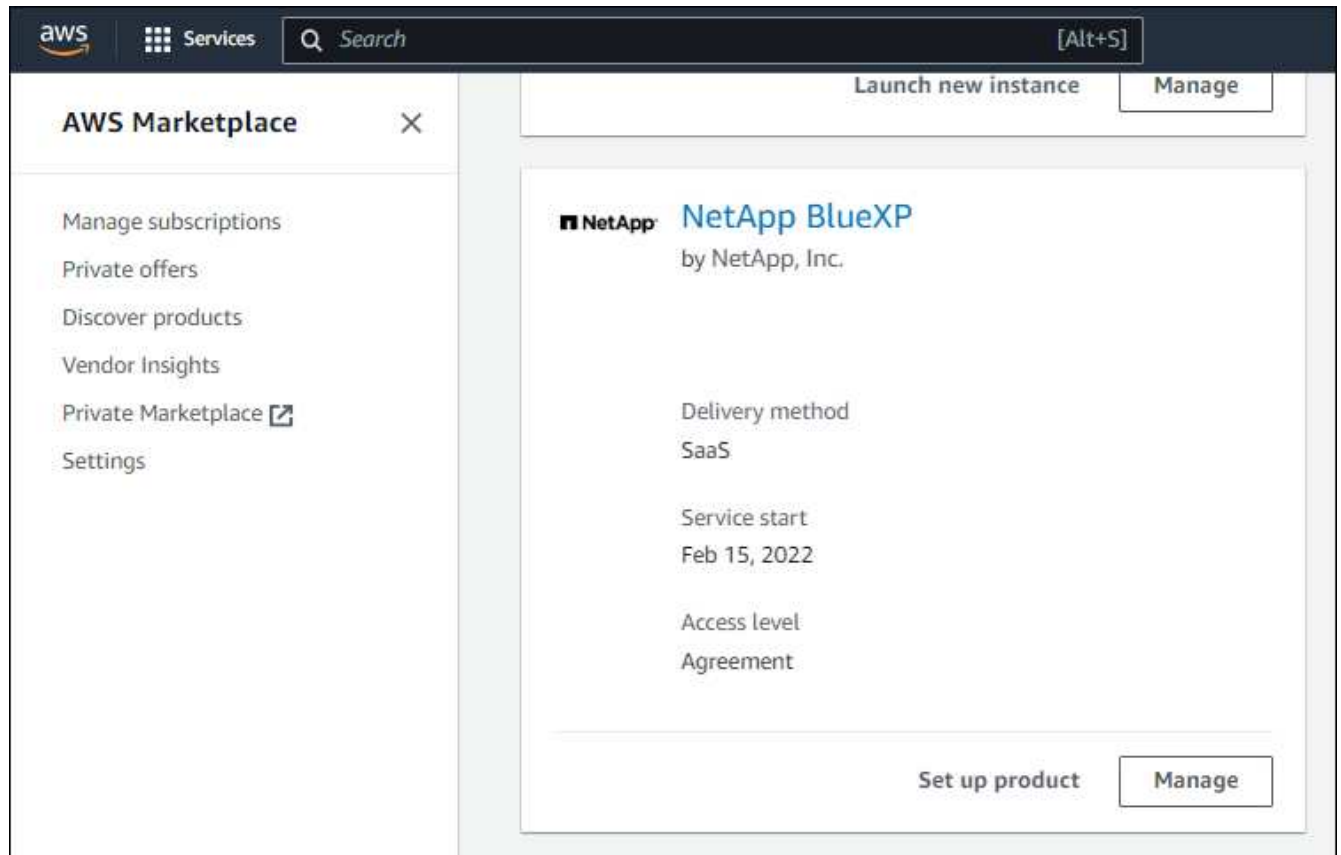
Suivez les étapes ci-dessous si vous avez souscrit à BlueXP depuis AWS Marketplace, mais que vous n'avez pas vu l'étape d'association de l'abonnement à votre compte.

Étapes

1. Accédez au portefeuille digital BlueXP pour vérifier que vous n'avez pas associé votre abonnement à votre compte BlueXP.
 - a. Dans le menu de navigation BlueXP, sélectionnez **gouvernance > porte-monnaie numérique**.
 - b. Sélectionnez **abonnements**.
 - c. Vérifiez que votre abonnement BlueXP n'apparaît pas.

Vous ne verrez que les abonnements associés au compte que vous consultez actuellement. Si vous ne voyez pas votre abonnement, procédez comme suit.

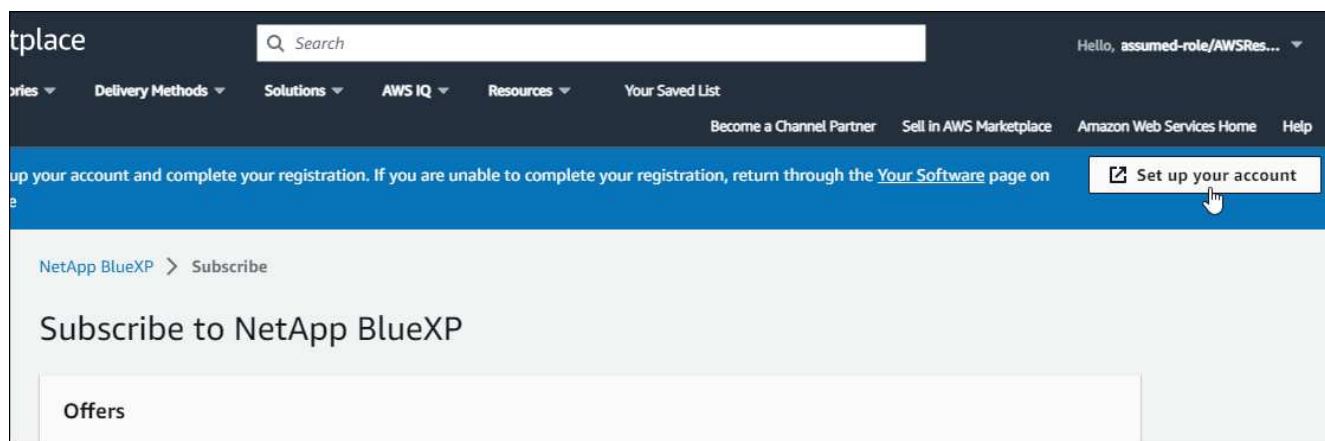
2. Connectez-vous à la console AWS et accédez à **abonnements AWS Marketplace**.
3. Découvrez l'abonnement NetApp BlueXP.



4. Sélectionnez **configurer le produit**.

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

5. Sélectionnez **configurer votre compte**.



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

Notez que vous pouvez être invité à vous connecter à BlueXP en premier.

6. À partir de la page **attribution d'abonnement** :

- Sélectionnez les comptes BlueXP avec lesquels vous souhaitez associer cet abonnement.
- Dans le champ **remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant pour un compte par ce nouvel abonnement.

BlueXP remplace l'abonnement existant pour toutes les informations d'identification du compte par ce nouvel abonnement. Si un ensemble d'informations d'identification n'a jamais été associé à un abonnement, ce nouvel abonnement ne sera pas associé à ces informations d'identification.

Pour tous les autres comptes, vous devez associer manuellement l'abonnement en répétant ces étapes.

Subscription Assignment
×

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

Subscription name
i

PayAsYouGo

Select the NetApp accounts that you'd like to associate this subscription with.
i

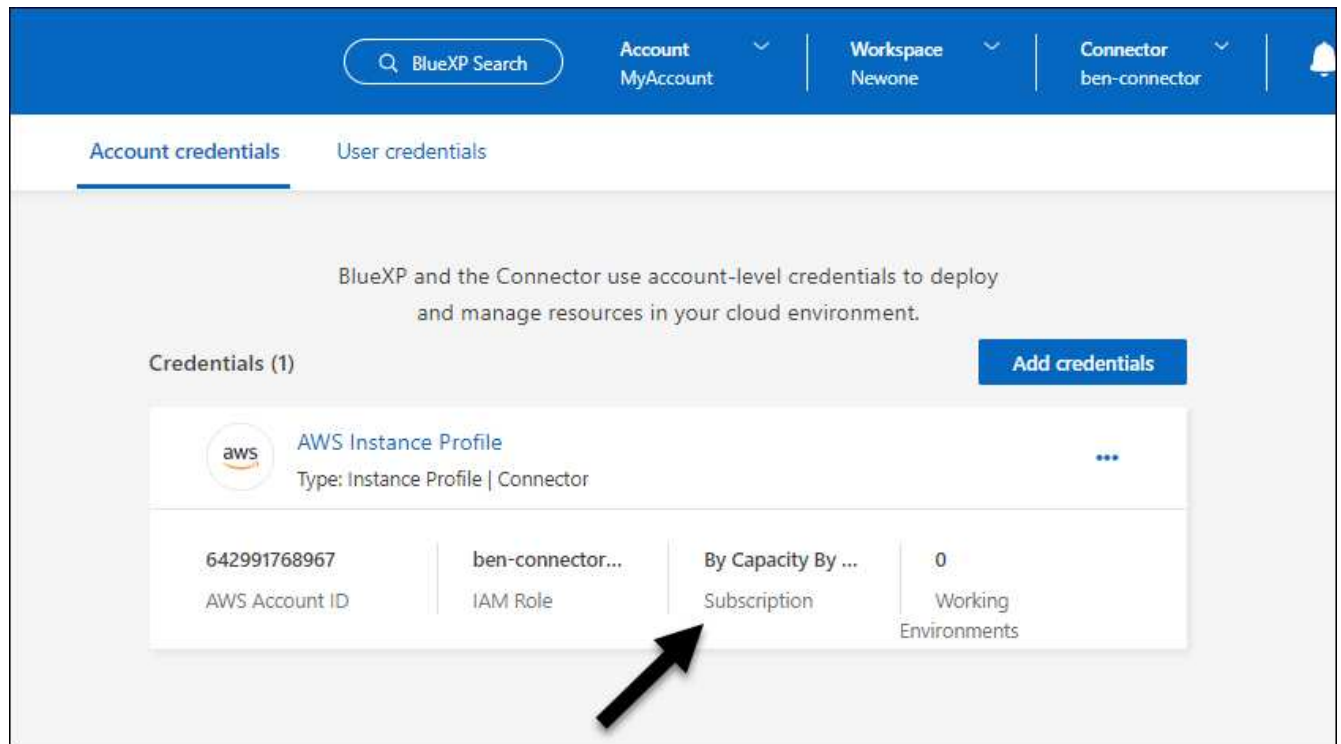
You can automatically replace the existing subscription for one account with this new subscription.

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

Save

7. Accédez au portefeuille digital BlueXP pour vérifier que l'abonnement est associé à votre compte BlueXP.
 - a. Dans le menu de navigation BlueXP, sélectionnez **gouvernance > porte-monnaie numérique**.
 - b. Sélectionnez **abonnements**.
 - c. Vérifiez que votre abonnement BlueXP s'affiche.
8. Vérifiez que l'abonnement est associé à vos identifiants AWS.
 - a. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
 - b. Sur la page **informations d'identification du compte**, vérifiez que l'abonnement est associé à vos informations d'identification AWS.

Voici un exemple.



Modifier les informations d'identification

Modifiez vos informations d'identification AWS 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, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
2. Sur la page **informations d'identification du compte**, sélectionnez le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **Modifier les informations d'identification**.
3. Effectuez les modifications requises, puis sélectionnez **appliquer**.

Supprimer les informations d'identification

Si vous n'avez plus besoin d'un ensemble d'informations d'identification, vous pouvez les supprimer 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, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.

2. Sur la page **informations d'identification du compte**, sélectionnez le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **Supprimer les informations d'identification**.
3. Sélectionnez **Supprimer** pour confirmer.

Azure

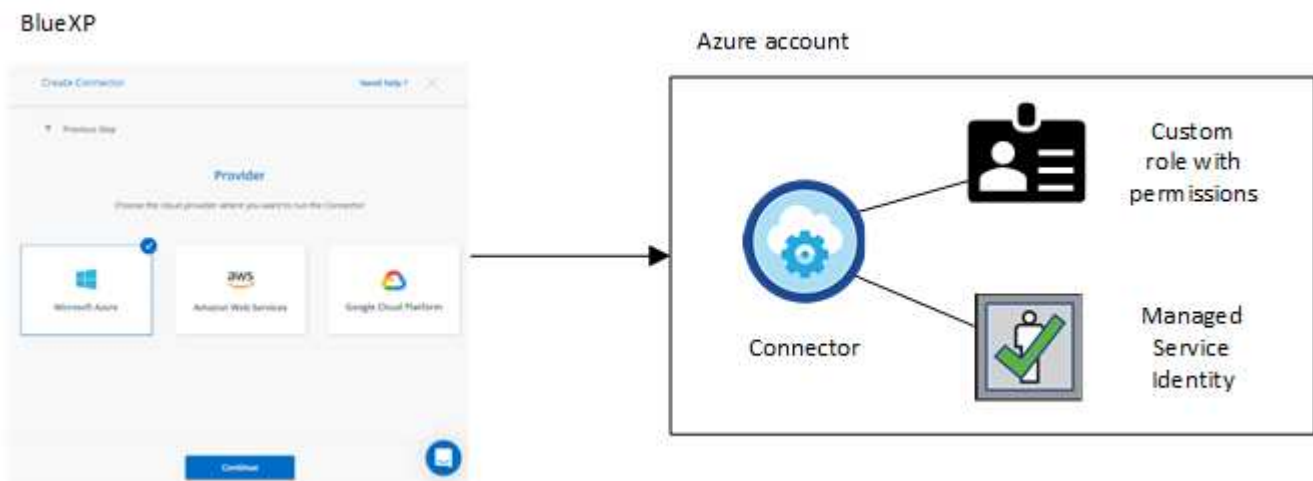
En savoir plus sur les identifiants et les autorisations Azure

Découvrez comment BlueXP utilise les identifiants Azure pour effectuer des actions en votre nom et comment ces identifiants sont associés aux abonnements Marketplace. Ces informations peuvent vous être utiles lorsque vous gérez les identifiants d'un ou plusieurs abonnements Azure. Par exemple, vous pouvez savoir quand ajouter des informations d'identification Azure supplémentaires à BlueXP.

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"](#).



Si vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP, BlueXP sélectionne les informations d'identification Azure suivantes par défaut :

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

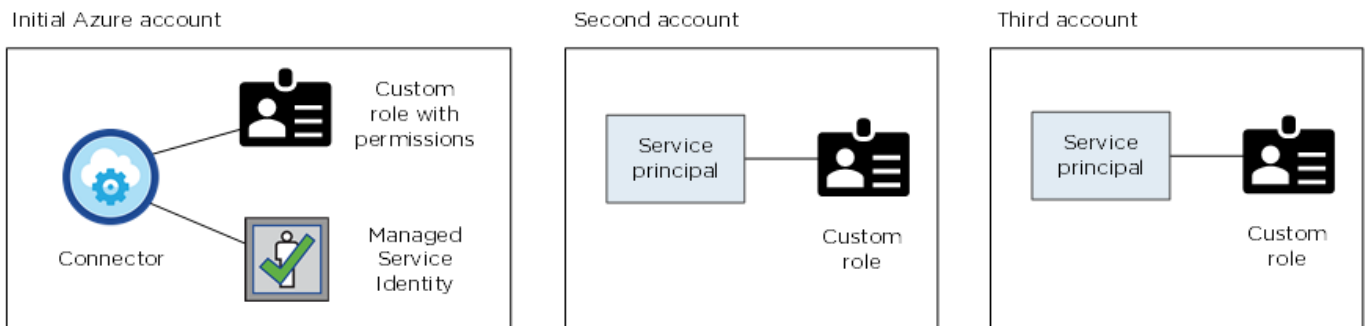
Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des identifiants Azure initiaux, ou ajouter des identifiants supplémentaires.

Des abonnements Azure supplémentaires pour une identité gérée

L'identité gérée attribuée par le système à la VM Connector 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 utiliser d'autres identifiants Azure avec BlueXP, vous devez accorder les autorisations requises par ["Création et configuration d'une entité de service dans Microsoft Entra ID"](#) 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.

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

The screenshot shows the 'Edit Account & Add Subscription' interface. It features a 'Credentials' section with a text input field containing the text 'cloud-manager-app | Application ID: 57c42424-88a0-480a.'. Below this is a dropdown menu labeled 'Managed Service Identity' with 'OCCM QA1 (Default)' selected.

Informations d'identification et abonnements Marketplace

Les identifiants que vous ajoutez à un connecteur doivent être associés à un abonnement Azure Marketplace de sorte que vous puissiez payer Cloud Volumes ONTAP à un taux horaire (PAYGO) ou un contrat annuel, et

utiliser d'autres services BlueXP.

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

Notez ce qui suit à propos des identifiants Azure et des abonnements Marketplace :

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

FAQ

La question suivante concerne les informations d'identification et les abonnements.

Est-il possible de modifier l'abonnement Azure Marketplace pour les environnements de travail Cloud Volumes ONTAP ?

Oui, c'est possible. Lorsque vous modifiez l'abonnement Azure Marketplace associé à un ensemble d'identifiants Azure, tous les environnements de travail Cloud Volumes ONTAP existants et nouveaux sont facturés pour le nouvel abonnement.

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

Puis-je ajouter plusieurs identifiants Azure, chacun avec des abonnements Marketplace différents ?

Tous les identifiants Azure qui appartiennent au même abonnement Azure seront associés au même abonnement Azure Marketplace.

Si plusieurs identifiants Azure appartiennent à différents abonnements Azure, ces identifiants peuvent être associés au même abonnement Azure Marketplace ou à d'autres abonnements Marketplace.

Est-il possible de déplacer des environnements de travail Cloud Volumes ONTAP existants vers un autre abonnement Azure ?

Non, il n'est pas possible de déplacer les ressources Azure associées à votre environnement de travail Cloud Volumes ONTAP vers un autre abonnement Azure.

Comment fonctionnent les identifiants pour les déploiements sur site et sur le marché ?

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 d'Azure Marketplace et installer le logiciel Connector sur votre propre hôte Linux.

Si vous utilisez Marketplace, vous pouvez fournir des autorisations en attribuant un rôle personnalisé à la machine virtuelle Connector et à une identité gérée attribuée par le système, ou vous pouvez utiliser une entité de service Microsoft Entra.

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

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

- Mode standard
 - ["Configurez les autorisations d'un déploiement Azure Marketplace"](#)

- "Configurez des autorisations pour les déploiements sur site"
- "Définissez les autorisations pour le mode restreint"
- "Configurez les autorisations pour le mode privé"

Gérez les identifiants Azure et les abonnements Marketplace pour BlueXP

Ajoutez et gérez des identifiants Azure pour que BlueXP dispose des autorisations dont il a besoin pour déployer et gérer des ressources cloud dans vos abonnements Azure. Si vous gérez plusieurs abonnements Azure Marketplace, vous pouvez les attribuer à différentes informations d'identification Azure à partir de la page informations d'identification.

Suivez les étapes indiquées sur cette page si vous devez utiliser plusieurs identifiants Azure ou plusieurs abonnements Azure Marketplace pour Cloud Volumes ONTAP.

Présentation

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.

Associez des 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.

Description de la tâche

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. Sélectionnez **contrôle d'accès (IAM)**.
 - a. Sélectionnez **Ajouter > Ajouter une affectation de rôle**, puis ajoutez les autorisations :
 - 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.
- Sélectionnez **Enregistrer**.

4. Répétez ces étapes pour les abonnements supplémentaires.

Résultat

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

The screenshot shows a web interface titled "Edit Account & Add Subscription". Under the "Credentials" section, a dropdown menu is set to "Managed Service Identity". Below this, the "Azure Subscription" section has a dropdown menu that is open, displaying two options: "OCCM Dev" and "OCCM QA1 (Default)". The "OCCM QA1 (Default)" option is selected and highlighted in blue. At the bottom of the interface, a yellow message icon is followed by the text "No subscription is associated with this account".

Ajoutez des identifiants 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"](#).

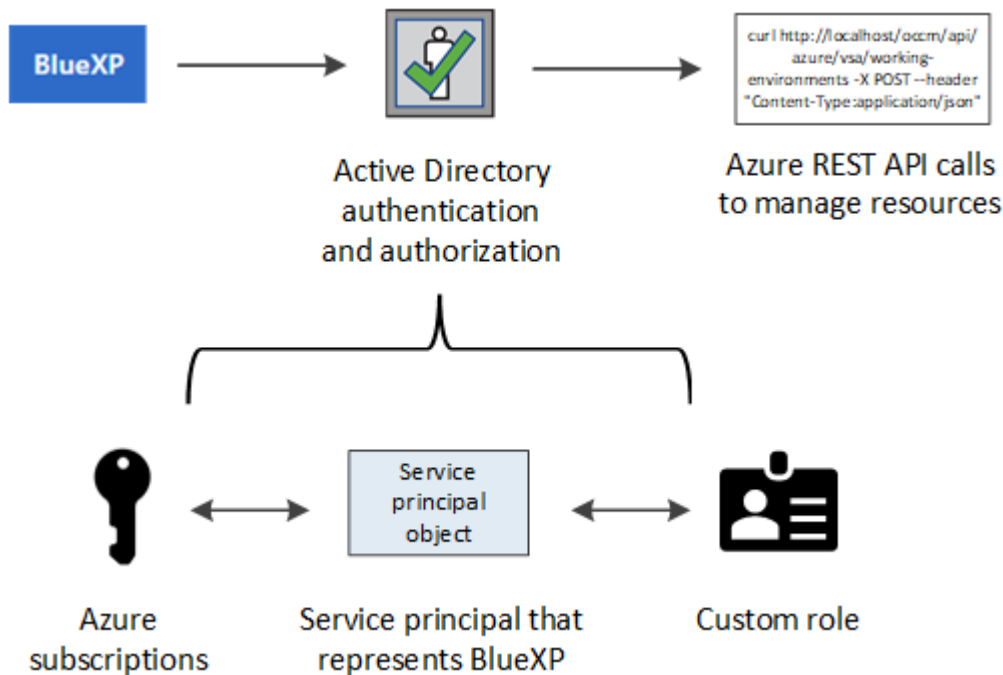
Si vous souhaitez déployer Cloud Volumes ONTAP à l'aide des informations d'identification *différent* Azure, vous devez accorder les autorisations requises en créant et en configurant une entité de service dans Microsoft Entra ID pour chaque compte Azure. Vous pouvez ensuite ajouter les nouvelles informations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

Accordez des autorisations Azure à l'aide d'un principal 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 principal de service dans Microsoft Entra ID et en obtenant les informations d'identification Azure requises par BlueXP.

Description de la tâche

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 un ID Microsoft Entra et est attribué à un rôle personnalisé qui autorise les autorisations requises.



Étapes

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

Créez une application Microsoft Entra

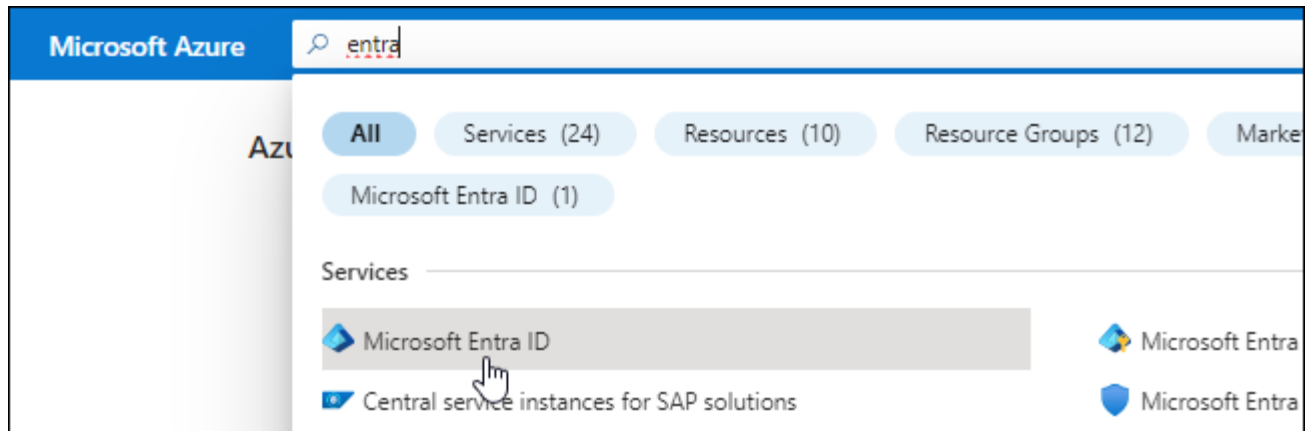
Créez une application et un principal de service Microsoft Entra que BlueXP peut utiliser pour le contrôle d'accès basé sur des rôles.

Étapes

1. Assurez-vous que vous disposez des autorisations dans Azure pour créer une application Active Directory et attribuer l'application à un rôle.

Pour plus de détails, reportez-vous à "[Documentation Microsoft Azure : autorisations requises](#)"

2. À partir du portail Azure, ouvrez le service **Microsoft Entra ID**.



3. Dans le menu, sélectionnez **enregistrements d'applications**.
4. Sélectionnez **nouvel enregistrement**.
5. 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.
6. Sélectionnez **Enregistrer**.

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

Résultat

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

Attribuez 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 :

Notez que vous pouvez créer un rôle personnalisé Azure à l'aide du portail Azure, d'Azure PowerShell, de l'interface de ligne de commandes Azure ou de l'API REST. La procédure suivante explique comment créer le rôle à l'aide de l'interface de ligne de commandes Azure. Si vous préférez utiliser une autre méthode, reportez-vous à la section "[Documentation Azure](#)"

- 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.



- Pour créer le rôle personnalisé, utilisez l'interface de ligne de commandes Azure :

```
az role definition create --role-definition Connector_Policy.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.
- Sélectionnez **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.
- Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.
- Dans l'onglet **membres**, procédez comme suit :
 - Conserver **utilisateur, groupe ou entité de service** sélectionnée.
 - Sélectionnez **Sélectionner membres**.

Add role assignment ...

Got feedback?

[Role](#) **[Members](#)** [Review + assign](#)

Selected role Cloud Manager Operator 3.9.12_B

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

- Recherchez le nom de l'application.

Voici un exemple :

Select members [X]

Select ⓘ

test-service-principal

test-service-principal

- Sélectionnez l'application et sélectionnez **Sélectionner**.
 - Sélectionnez **Suivant**.
- f. Sélectionnez **consulter + 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.

Ajoutez des autorisations d'API de gestion de service Windows Azure

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

Étapes

1. Dans le service **Microsoft Entra ID**, sélectionnez **enregistrements d'applications** et sélectionnez l'application.
2. Sélectionnez **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.

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

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

Request API permissions

[← All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

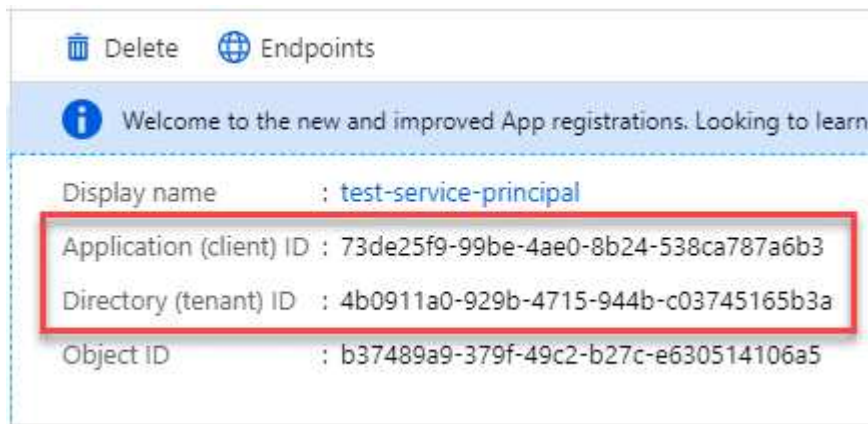
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview)	-

Obtenir l'ID de l'application et l'ID du répertoire

Lorsque vous ajoutez le compte Azure à 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 **Microsoft Entra ID**, sélectionnez **enregistrements d'applications** et sélectionnez l'application.
2. Copiez l'ID **application (client)** et l'ID **Directory (tenant)**.



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.

Créez un secret client

Vous devez créer un secret client, puis fournir à BlueXP la valeur du secret afin que BlueXP puisse l'utiliser pour s'authentifier auprès de Microsoft Entra ID.

Étapes

1. Ouvrez le service **Microsoft Entra ID**.
2. Sélectionnez **enregistrements d'applications** et sélectionnez votre application.
3. Sélectionnez **certificats et secrets > Nouveau secret client**.
4. Fournissez une description du secret et une durée.
5. Sélectionnez **Ajouter**.
6. 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
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

BlueXP peut maintenant utiliser un code client pour s'authentifier auprès de Microsoft Entra ID.

Résultat

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

Ajoutez les identifiants 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.

Avant de commencer

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

Avant de commencer

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, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.



2. Sélectionnez **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
 - a. **Emplacement des informations d'identification** : sélectionnez **Microsoft Azure > connecteur**.
 - b. **Définir les informations d'identification** : saisissez les informations relatives à l'entité de service

Microsoft Entra qui accorde les autorisations requises :

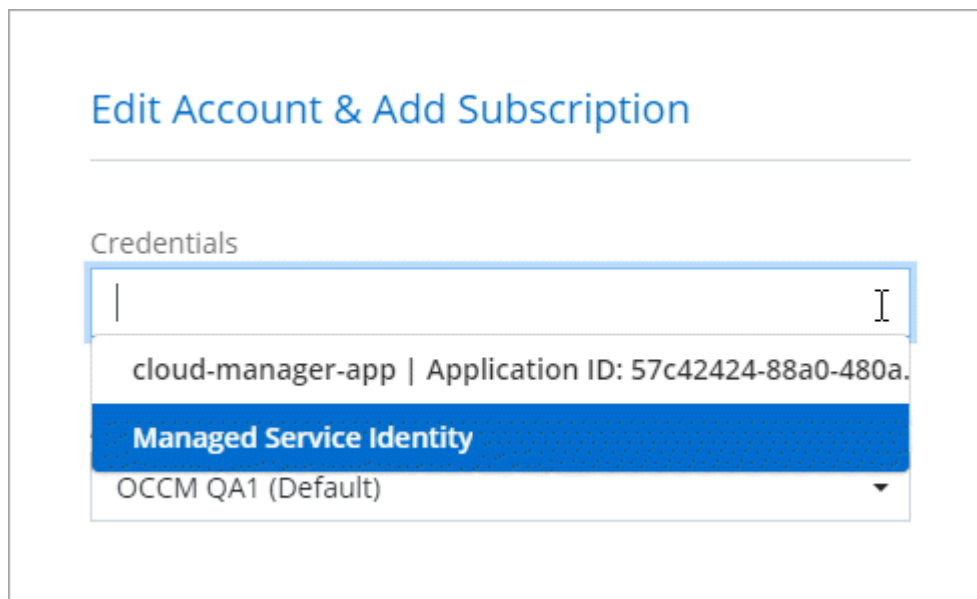
- ID de l'application (client)
- ID du répertoire (locataire)
- Secret client

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

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

Résultat

Vous pouvez 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.

Associez un abonnement Azure Marketplace à vos identifiants

Après avoir ajouté vos informations d'identification Azure à BlueXP, vous pouvez associer un abonnement Azure Marketplace à ces informations d'identification. L'abonnement vous permet de créer un système Cloud Volumes ONTAP avec paiement à l'utilisation et d'utiliser d'autres services BlueXP.

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 modifier l'abonnement Azure Marketplace associé aux informations d'identification Azure.

Le remplacement de l'abonnement Marketplace actuel par un nouvel abonnement modifie l'abonnement Marketplace pour tous les environnements de travail Cloud Volumes ONTAP existants et tous les nouveaux environnements de travail.

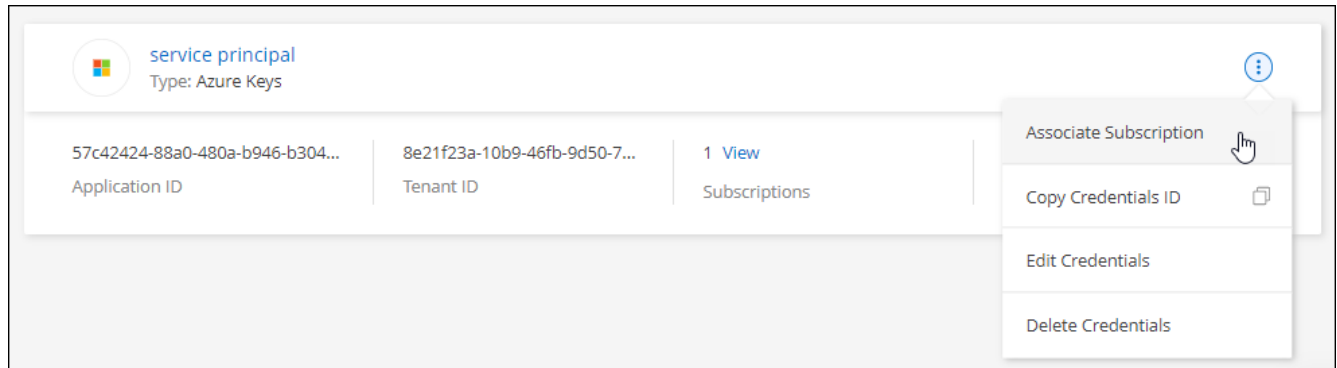
Avant de commencer

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, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
2. Sélectionnez le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **abonnement associé**.

Vous devez sélectionner les informations d'identification associées à un connecteur. Vous ne pouvez pas associer un abonnement Marketplace aux informations d'identification associées à BlueXP.



3. Pour associer les informations d'identification à un abonnement existant, sélectionnez l'abonnement dans la liste déroulante et sélectionnez **associer**.
4. Pour associer les informations d'identification à un nouvel abonnement, sélectionnez **Ajouter un abonnement > Continuer** et suivez les étapes dans Azure Marketplace :
 - a. Si vous y êtes invité, connectez-vous à votre compte Azure.
 - b. Sélectionnez **s'abonner**.
 - c. Remplissez le formulaire et sélectionnez **s'abonner**.
 - d. Une fois le processus d'abonnement terminé, sélectionnez **configurer le compte maintenant**.

Vous serez redirigé vers le site Web BlueXP.

- e. À partir de la page **attribution d'abonnement** :

- Sélectionnez les comptes BlueXP avec lesquels vous souhaitez associer cet abonnement.
- Dans le champ **remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant pour un compte par ce nouvel abonnement.

BlueXP remplace l'abonnement existant pour toutes les informations d'identification du compte par ce nouvel abonnement. Si un ensemble d'informations d'identification n'a jamais été associé à un abonnement, ce nouvel abonnement ne sera pas associé à ces informations d'identification.

Pour tous les autres comptes, vous devez associer manuellement l'abonnement en répétant ces étapes.

- Sélectionnez **Enregistrer**.

La vidéo suivante explique comment vous abonner à Azure Marketplace :

Modifier les 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, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
2. Sur la page **informations d'identification du compte**, sélectionnez le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **Modifier les informations d'identification**.
3. Effectuez les modifications requises, puis sélectionnez **appliquer**.

Supprimer les informations d'identification

Si vous n'avez plus besoin d'un ensemble d'informations d'identification, vous pouvez les supprimer 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, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
2. Sur la page **informations d'identification du compte**, sélectionnez le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **Supprimer les informations d'identification**.
3. Sélectionnez **Supprimer** pour confirmer.

Google Cloud

Découvrez les projets et les autorisations Google Cloud

Découvrez comment BlueXP utilise les identifiants Google Cloud pour effectuer des actions en votre nom et comment ces identifiants sont associés aux abonnements Marketplace. Ces informations peuvent vous être utiles lorsque vous gérez les identifiants d'un ou plusieurs projets Google Cloud. Par exemple, vous pourriez vouloir en savoir plus sur le compte de service associé à la VM Connector.

Projet et autorisations pour BlueXP

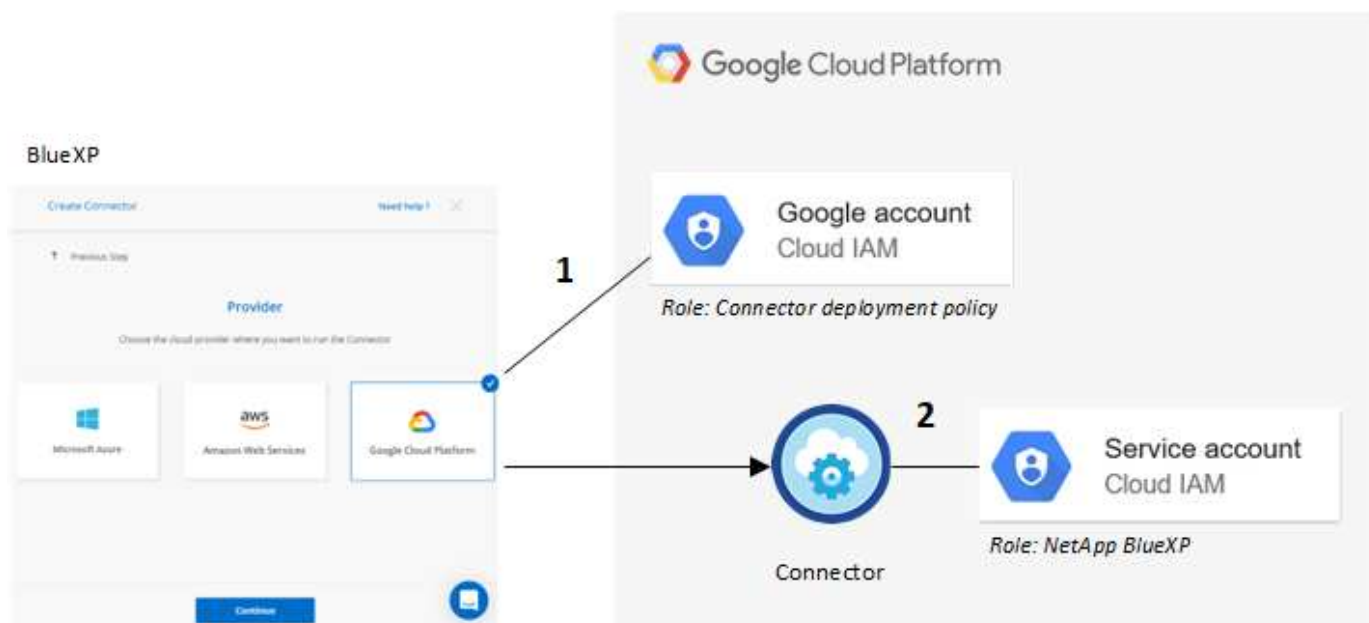
Avant de pouvoir utiliser BlueXP pour gérer les ressources de votre projet Google Cloud, vous devez d'abord déployer un connecteur. Il ne peut pas s'exécuter sur site ou dans un autre fournisseur cloud.

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 les systèmes

Cloud Volumes ONTAP, gérer les sauvegardes à l'aide de la sauvegarde et de la restauration BlueXP, etc. Les autorisations sont fournies en ajoutant un rôle personnalisé au compte de service.

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



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

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

Informations d'identification et abonnements Marketplace

Lorsque vous déployez un connecteur dans Google Cloud, BlueXP crée un ensemble d'informations d'identification par défaut pour le compte de service Google Cloud dans le projet où réside le connecteur. Ces identifiants doivent être associés à un abonnement à Google Cloud Marketplace afin que vous puissiez payer Cloud Volumes ONTAP à un taux horaire (PAYGO) et utiliser d'autres services BlueXP.

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

Remarque : concernant les identifiants Google Cloud et les abonnements Marketplace, vous devez :

- Un seul ensemble d'identifiants Google Cloud peut être associé à un connecteur
- Vous ne pouvez associer qu'un seul abonnement Google Cloud Marketplace aux identifiants
- Vous pouvez remplacer un abonnement Marketplace existant par un nouvel abonnement

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 le compte de service"](#)

- ["Découvrez comment déployer Cloud Volumes ONTAP dans Google Cloud et sélectionner un projet"](#)

Gérez les identifiants Google Cloud et les abonnements pour BlueXP

Vous pouvez gérer les informations d'identification Google Cloud associées à l'instance de VM Connector en associant un abonnement Marketplace et en dépannant le processus d'abonnement. Ces deux tâches vous permettent d'utiliser votre abonnement Marketplace pour payer les services BlueXP.

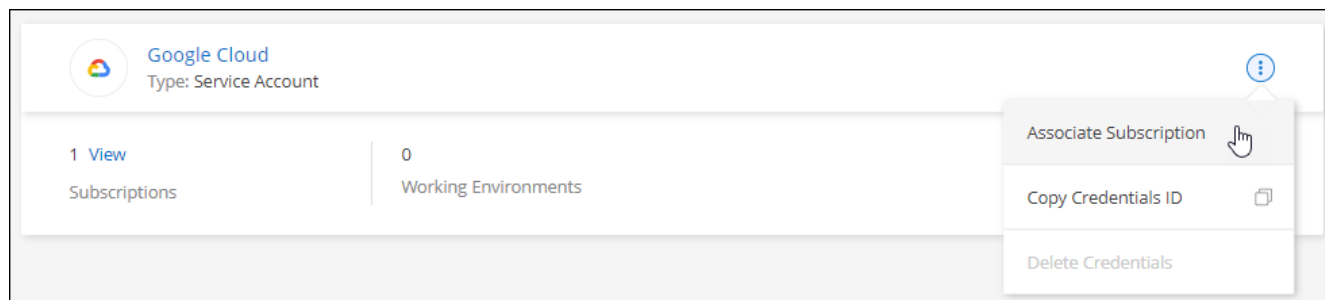
Associez un abonnement Marketplace avec des identifiants Google Cloud

Lorsque vous déployez un connecteur dans Google Cloud, BlueXP crée un ensemble d'informations d'identification par défaut qui sont associées à l'instance de VM Connector. Vous pouvez à tout moment modifier l'abonnement Google Cloud Marketplace associé à ces informations d'identification. L'abonnement vous permet de créer un système Cloud Volumes ONTAP avec paiement à l'utilisation et d'utiliser d'autres services BlueXP.

Le remplacement de l'abonnement Marketplace actuel par un nouvel abonnement modifie l'abonnement Marketplace pour tous les environnements de travail Cloud Volumes ONTAP existants et tous les nouveaux environnements de travail.

Étapes

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



3. Pour associer les informations d'identification à un abonnement existant, sélectionnez un projet Google Cloud et un abonnement dans la liste déroulante, puis sélectionnez **associer**.

Google Cloud Project

OCCM-Dev

Subscription

GCP subscription for staging

Add Subscription

4. Si vous n'avez pas encore d'abonnement, sélectionnez **Ajouter un abonnement > Continuer** et suivez les étapes indiquées dans Google Cloud Marketplace.



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.

- a. 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

netapp.com

←

Product details

NetApp

NetApp BlueXP
[NetApp, Inc.](#)

BlueXP lets you build, protect, and govern your hybrid multicloud data estate.

SUBSCRIBE

OVERVIEW

PRICING

DOCUMENTATION

SUPPORT

Overview

BlueXP is NetApp's hybrid multicloud storage and data services experience that helps organizations build and operate a centrally controlled data foundation across on-premises, edge, and cloud environments.

BlueXP abstracts the complexity of architecting the underlying Google Cloud infrastructure resources making it easier to deploy and operate NetApp's storage, mobility, protection, and analysis services within your Google Cloud environment.

Additional details

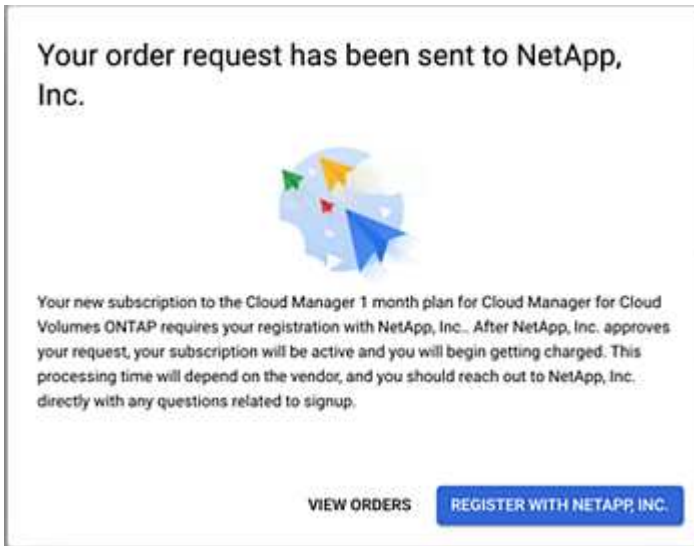
Type: [SaaS & APIs](#)
Last updated: 12/19/22
Category: [Analytics](#), [Developer tools](#), [Storage](#)

- b. Sélectionnez **s'abonner**.
- c. Sélectionnez le compte de facturation approprié et acceptez les conditions générales.
- d. Sélectionnez **s'abonner**.

Cette étape envoie votre demande de transfert à NetApp.

- e. Dans la boîte de dialogue qui s'affiche, sélectionnez **s'inscrire auprès de NetApp, Inc.**

Cette étape doit être effectuée pour lier l'abonnement Google Cloud à votre compte BlueXP. 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.



- f. Suivez les étapes de la page **attribution d'abonnement** :



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.

- Sélectionnez les comptes BlueXP avec lesquels vous souhaitez associer cet abonnement.
- Dans le champ **remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant pour un compte par ce nouvel abonnement.

BlueXP remplace l'abonnement existant pour toutes les informations d'identification du compte par ce nouvel abonnement. Si un ensemble d'informations d'identification n'a jamais été associé à un abonnement, ce nouvel abonnement ne sera pas associé à ces informations d'identification.

Pour tous les autres comptes, vous devez associer manuellement l'abonnement en répétant ces étapes.

- Sélectionnez **Enregistrer**.

Dans cette vidéo, vous instructions pour vous abonner à Google Cloud Marketplace :


[Abonnez-vous à BlueXP depuis Google Cloud Marketplace](#)


- a. 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](#)

Dépanner le processus d'abonnement Marketplace

L'abonnement à BlueXP via Google Cloud Marketplace peut parfois être fragmenté à cause d'autorisations incorrectes ou accidentellement non après la redirection vers le site web de 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 **gérer sur le fournisseur**, faites défiler la page vers le bas et sélectionnez **gérer les commandes**.

Pricing



The product was purchased on 12/9/20.

[MANAGE ORDERS](#)

- 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	⋮

- 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	⋮

Gérez les identifiants NSS associés à un compte BlueXP

Associez un compte du site de support NetApp à votre compte BlueXP pour activer les workflows clés pour Cloud Volumes ONTAP. Ces informations d'identification NSS sont associées à l'ensemble du compte BlueXP.



BlueXP prend également en charge l'association d'un compte NSS par utilisateur BlueXP. "[Découvrez comment gérer les identifiants de niveau utilisateur](#)".

Présentation

Pour activer les tâches suivantes dans BlueXP, vous devez associer les informations d'identification du site de support NetApp à votre ID de compte BlueXP :

- Déploiement d'Cloud Volumes ONTAP avec modèle BYOL (Bring Your Own License)

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.

- Enregistrement 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.

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

Ces identifiants sont associés à votre ID de compte BlueXP. Les utilisateurs qui appartiennent au compte BlueXP peuvent accéder à ces informations d'identification depuis **support > gestion NSS**.

Ajouter un compte NSS

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

- 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, sélectionnez l'icône aide, puis sélectionnez **support**.



2. Sélectionnez **gestion NSS > Ajouter un compte NSS**.
3. Lorsque vous y êtes invité, sélectionnez **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Entra ID comme fournisseur d'identité pour les services d'authentification spécifiques à la prise en charge et à l'octroi de 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 NSS doit être un compte de niveau client (pas un compte invité ou temporaire). Vous pouvez avoir plusieurs comptes NSS de niveau client.
- Il ne peut y avoir qu'un seul compte NSS si ce compte est un compte de niveau partenaire. Si vous essayez d'ajouter des comptes NSS de niveau client et qu'un compte de niveau partenaire existe, le message d'erreur suivant s'affiche :

"Le type de client NSS n'est pas autorisé pour ce compte car il existe déjà des utilisateurs NSS de type différent."

Il en va de même si vous possédez des comptes NSS client préexistants et que vous essayez d'ajouter un compte de niveau partenaire.

- 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. Notez que le jeton de ces comptes expire après 90 jours.

Une notification sera publiée pour vous en informer.

Et la suite ?

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

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

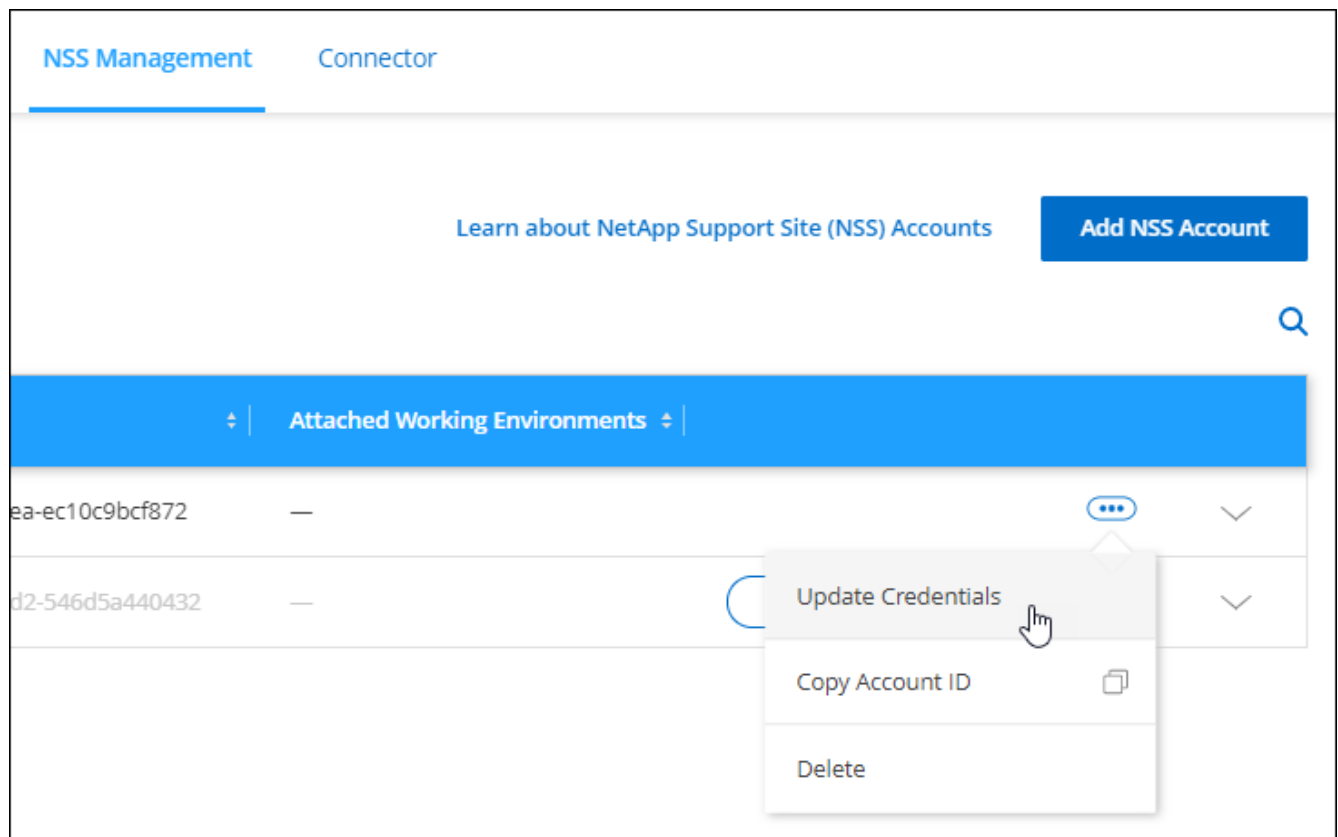
Mettre à jour les identifiants NSS

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, sélectionnez l'icône aide, puis sélectionnez **support**.
2. Sélectionnez **gestion NSS**.
3. Pour le compte NSS que vous souhaitez mettre à jour, sélectionnez **...** Puis sélectionnez **mettre à jour les informations d'identification**.



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

NetApp utilise Microsoft Entra ID comme fournisseur d'identité pour les services d'authentification spécifiques à la prise en charge et à l'octroi de 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.

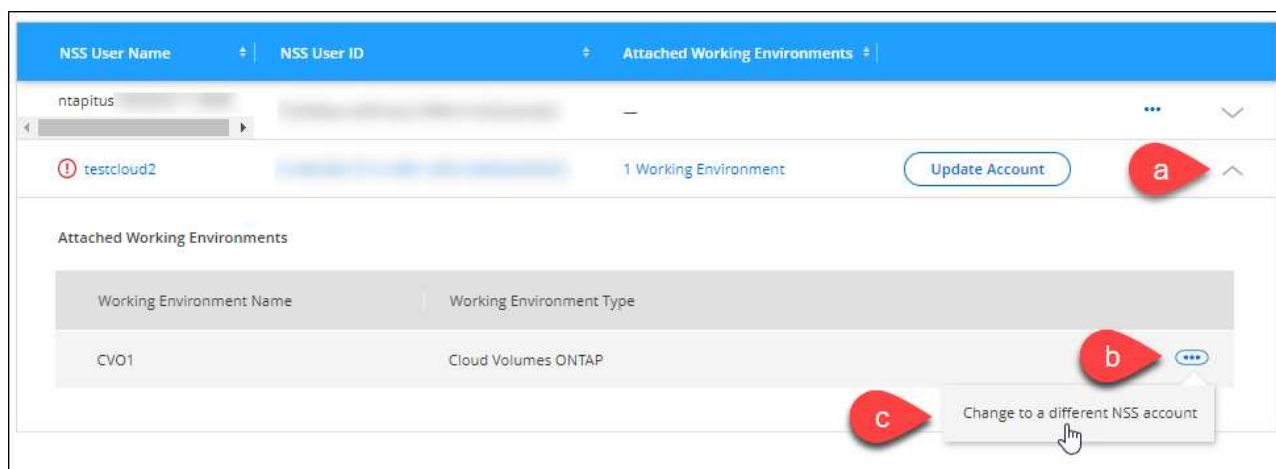
Associez un environnement de travail à un autre compte NSS

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 est uniquement prise en charge avec les comptes NSS configurés pour utiliser Microsoft Entra ID adopté par NetApp pour la gestion des identités. Avant de pouvoir utiliser cette fonction, vous devez sélectionner **Ajouter un compte NSS** ou **mettre à jour le compte**.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône aide, puis sélectionnez **support**.
2. Sélectionnez **gestion NSS**.
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, sélectionnez **...**
 - c. Sélectionnez **changer pour un autre compte NSS**.



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

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

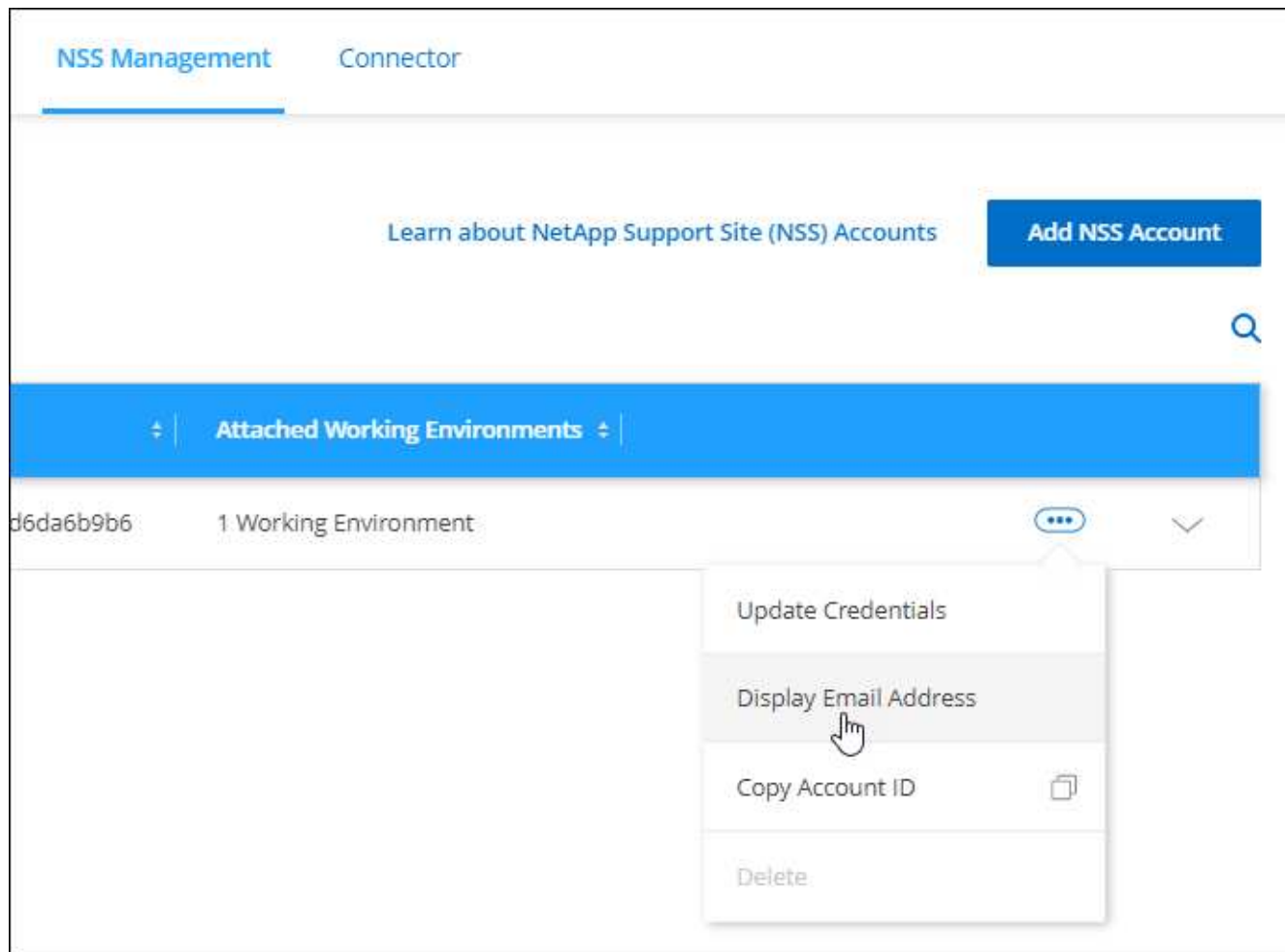
Maintenant que les comptes du site de support NetApp utilisent l'ID Microsoft Entra pour les services d'authentification, le nom d'utilisateur NSS qui s'affiche dans BlueXP est généralement un identifiant généré par Microsoft Entra. Par conséquent, il se peut que vous ne sachiez pas immédiatement l'adresse 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, sélectionnez l'icône aide, puis sélectionnez **support**.
2. Sélectionnez **gestion NSS**.
3. Pour le compte NSS que vous souhaitez mettre à jour, sélectionnez **...** Puis sélectionnez **Afficher l'adresse électronique**.



Résultat

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.

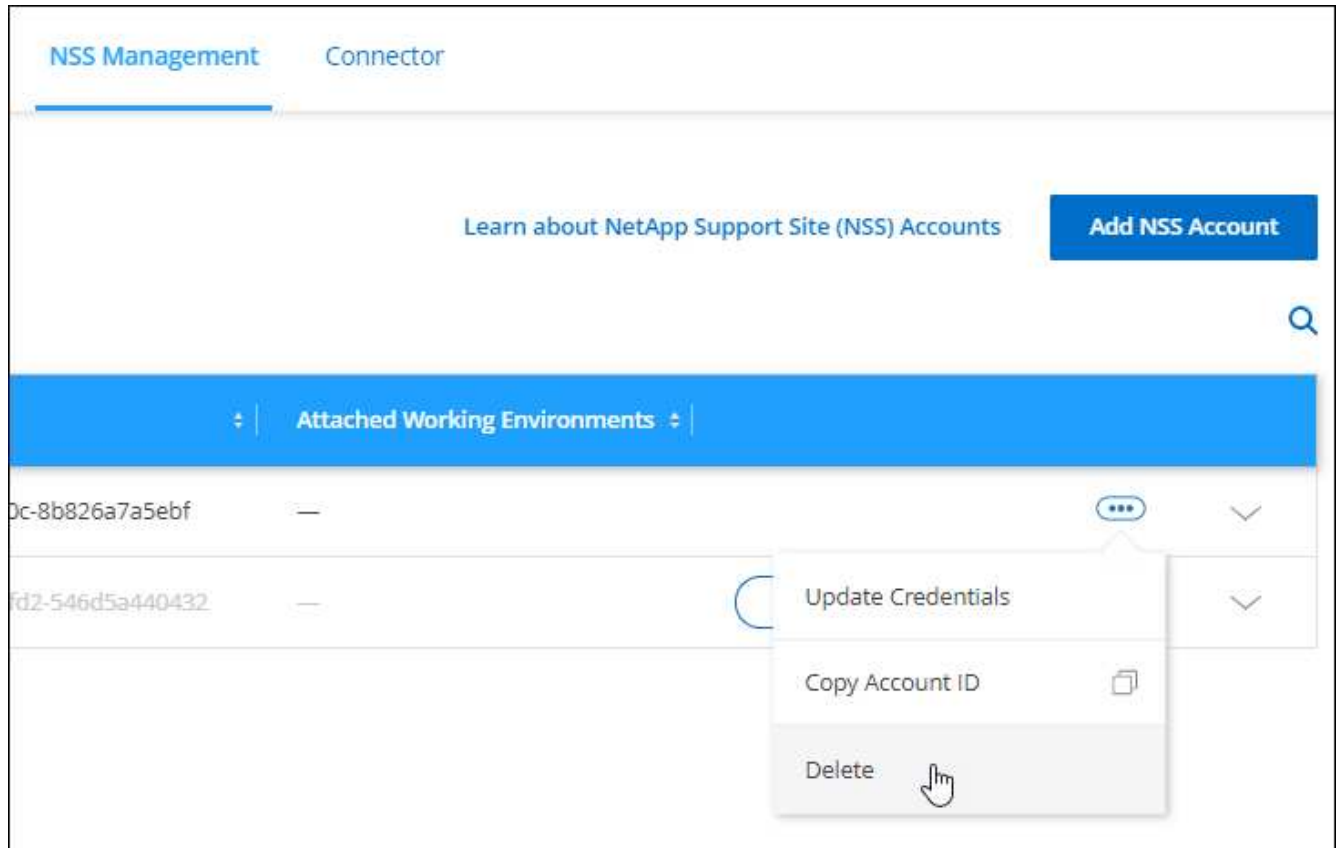
Supprimer un compte NSS

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 [Reliez ces environnements de travail à un autre compte NSS](#).

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône aide, puis sélectionnez **support**.
2. Sélectionnez **gestion NSS**.
3. Pour le compte NSS à supprimer, sélectionnez **...** Puis sélectionnez **Supprimer**.



4. Sélectionnez **Supprimer** pour confirmer.

Gestion des identifiants associés à votre connexion BlueXP

Selon les actions que vous avez effectuées dans BlueXP, vous pouvez avoir associé des informations d'identification ONTAP et des identifiants NSS (NetApp support site) avec votre identifiant utilisateur BlueXP. Vous pouvez afficher et gérer ces identifiants dans BlueXP une fois que vous les avez associés. Par exemple, si vous modifiez le mot de passe de ces informations d'identification, vous devez le mettre à jour dans BlueXP.

Identifiants ONTAP

Lorsque vous détectez directement un cluster ONTAP sur site sans utiliser de connecteur, vous êtes invité à saisir les informations d'identification ONTAP pour le cluster. Ces informations d'identification sont gérées au niveau de l'utilisateur, ce qui signifie qu'elles ne sont pas visibles par les autres utilisateurs qui se connectent.

Identifiants NSS

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

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

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

["Découvrez comment vous inscrire à de l'aide"](#)

- Lorsque vous accédez à **support > case Management**, vous êtes invité à entrer vos informations d'identification NSS, si vous ne l'avez pas déjà fait. Cette page vous permet de créer et de gérer les dossiers de demande de support associés à votre compte NSS et à votre entreprise.
- Lorsque vous accédez à Digital Advisor dans BlueXP, vous êtes invité à vous connecter à Digital Advisor en saisissant vos informations d'identification NSS.

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

- 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.
- Par utilisateur, il ne peut y avoir qu'un seul compte NSS associé à Digital Advisor et à la gestion des dossiers de support.
- Si vous essayez d'associer un compte du site de support NetApp à un environnement de travail Cloud Volumes ONTAP, vous pouvez uniquement choisir parmi les comptes NSS ajoutés au compte BlueXP dont vous êtes membre.

Les identifiants NSS au niveau du compte sont différents du compte NSS associé à votre connexion BlueXP. Les identifiants NSS de niveau compte vous permettent de déployer Cloud Volumes ONTAP avec votre propre licence (BYOL), d'enregistrer des systèmes PAYGO et de mettre à niveau le logiciel Cloud Volumes ONTAP.

["En savoir plus sur l'utilisation des identifiants NSS avec votre compte BlueXP".](#)

Gérez vos informations d'identification utilisateur

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

Étapes


1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
2. Sélectionnez **informations d'identification utilisateur**.
3. Si vous ne possédez pas encore d'informations d'identification, vous pouvez sélectionner **Ajouter des informations d'identification NSS** pour ajouter votre compte sur le site de support NetApp.
4. Gérez les informations d'identification existantes en choisissant les options suivantes :
 - **Mettre à jour les informations d'identification** : mettez à jour le nom d'utilisateur et le mot de passe du compte.
 - **Supprimer les informations d'identification** : supprimez le compte associé à votre compte utilisateur BlueXP.

[Account credentials](#)[User credentials](#)


BlueXP uses these credentials to authenticate you with your digital advisor account, for support case management, and for on-premises ONTAP clusters accessed without a Connector.

Credentials (2)

Add NSS credentials


tami@netapp.com
Type: NSS

1234567890123456789012345678901234567890
User ID

OK
Status

Update credentials

Delete credentials

tami
Type: ONTAP

10.20.3.0
Cluster IP

id-324553636
Working environment ID

Résultat

BlueXP met à jour vos identifiants. Les modifications seront répercutées lorsque vous accédez au cluster ONTAP, au conseiller digital ou à la page case Management.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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