Connecteurs

Setup and administration

NetApp
April 26, 2024

Sommaire

Connecteurs

Recherchez l'ID système d'un connecteur

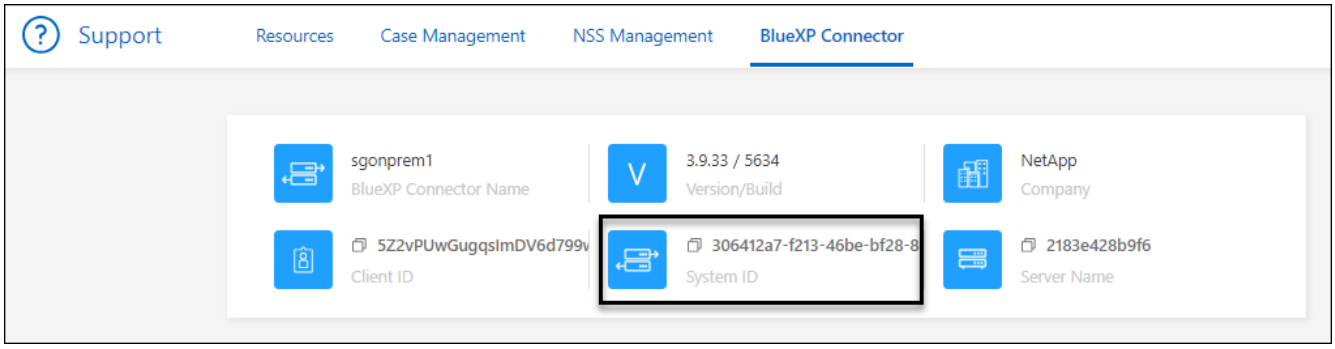
Pour vous aider à démarrer, votre conseiller NetApp peut vous demander l'identifiant système de votre connecteur. L'ID est généralement utilisé à des fins de licence et de dépannage.

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".

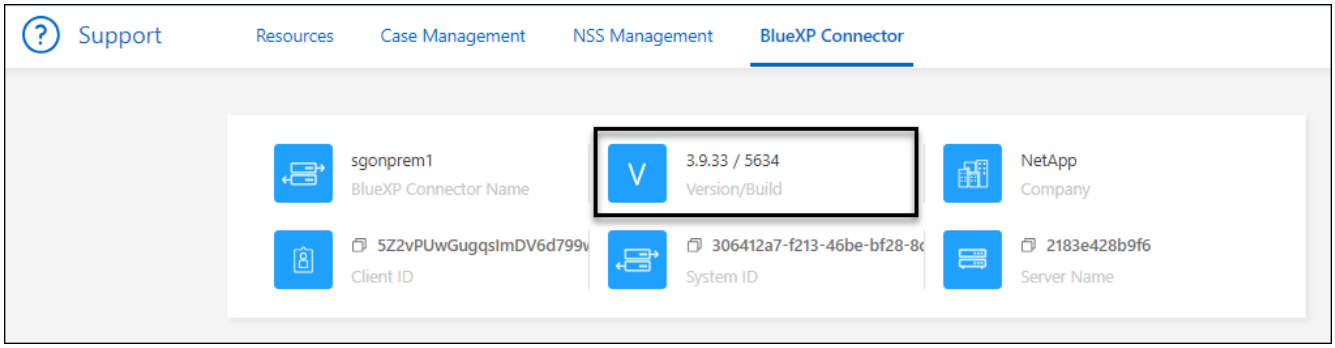
Afficher la version d'un connecteur

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

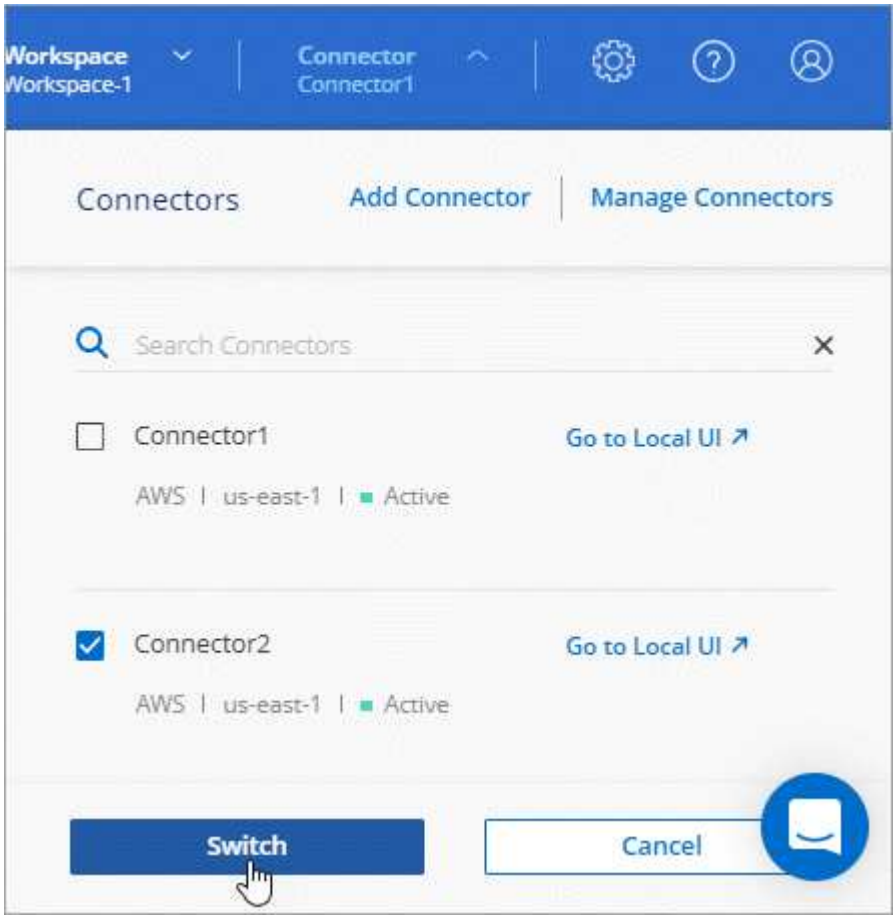
Si vous avez plusieurs connecteurs, vous pouvez passer de l'un à l'autre pour voir les environnements de travail associés à un connecteur spécifique.

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

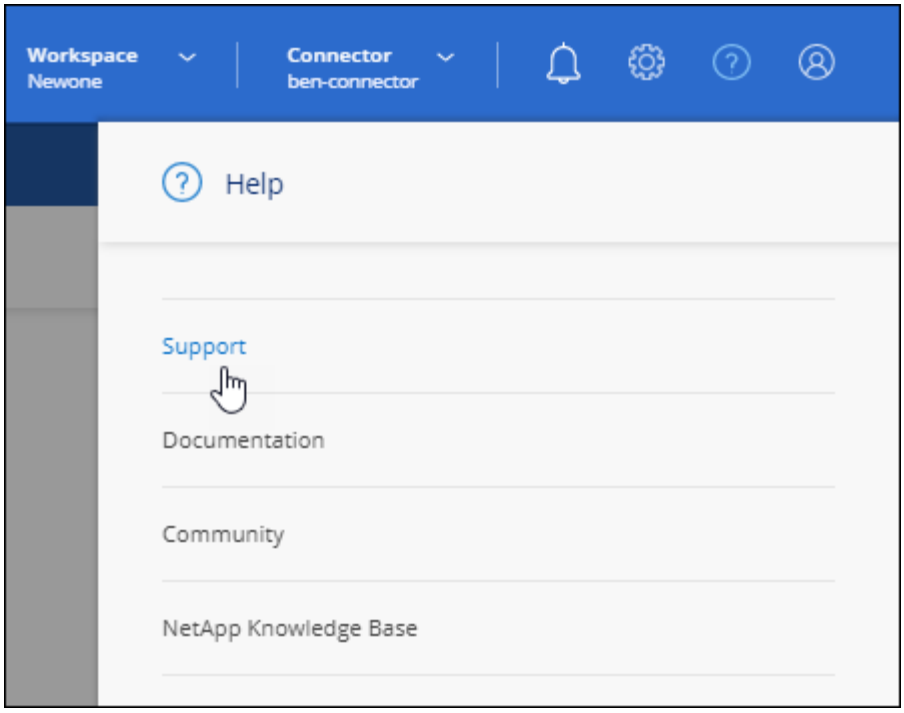
BlueXP actualise et affiche les environnements de travail associés au connecteur sélectionné.

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

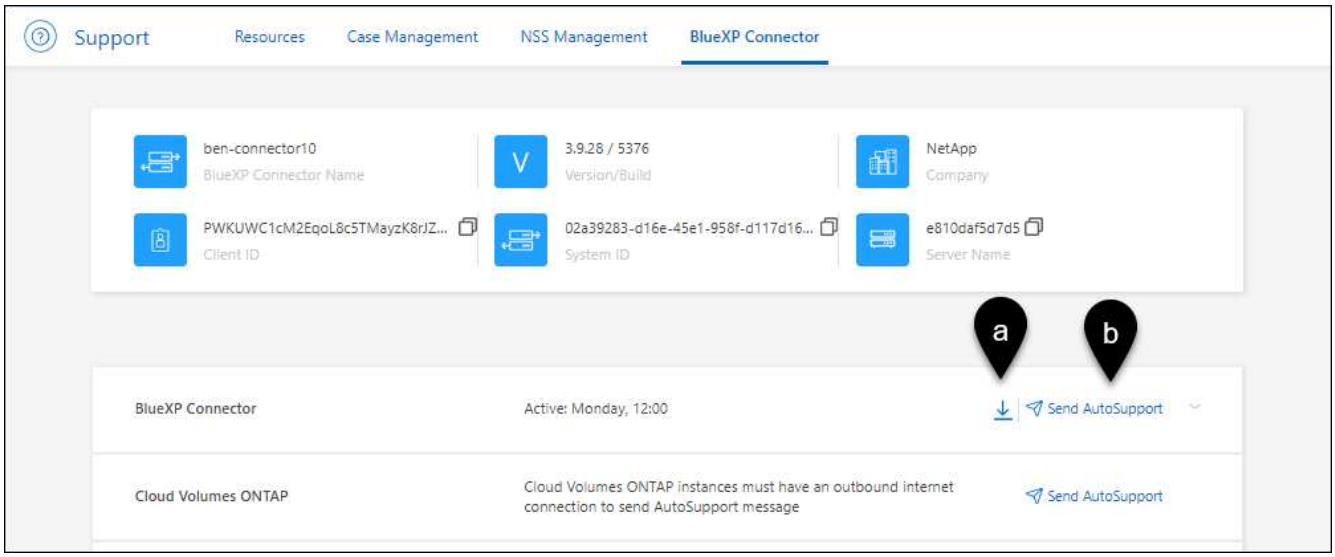
1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône aide, puis sélectionnez **support**.



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

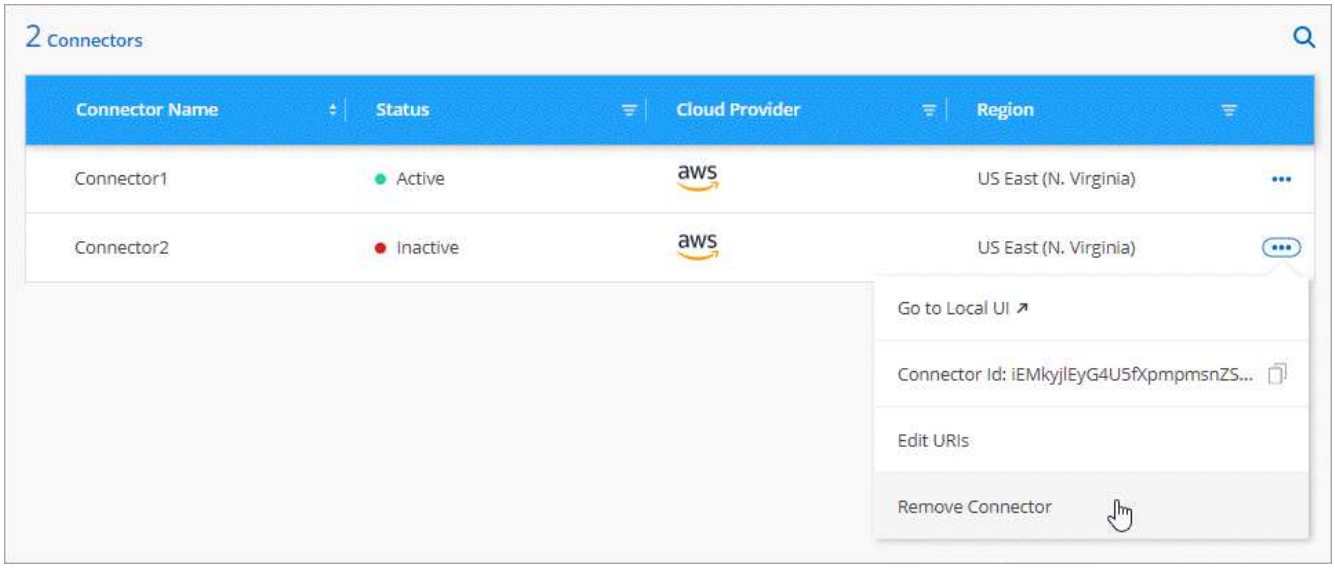
Si un connecteur est inactif, vous pouvez le retirer de la liste des connecteurs dans BlueXP. Vous pouvez le faire si vous avez supprimé la machine virtuelle Connector ou si vous avez désinstallé le logiciel Connector.

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

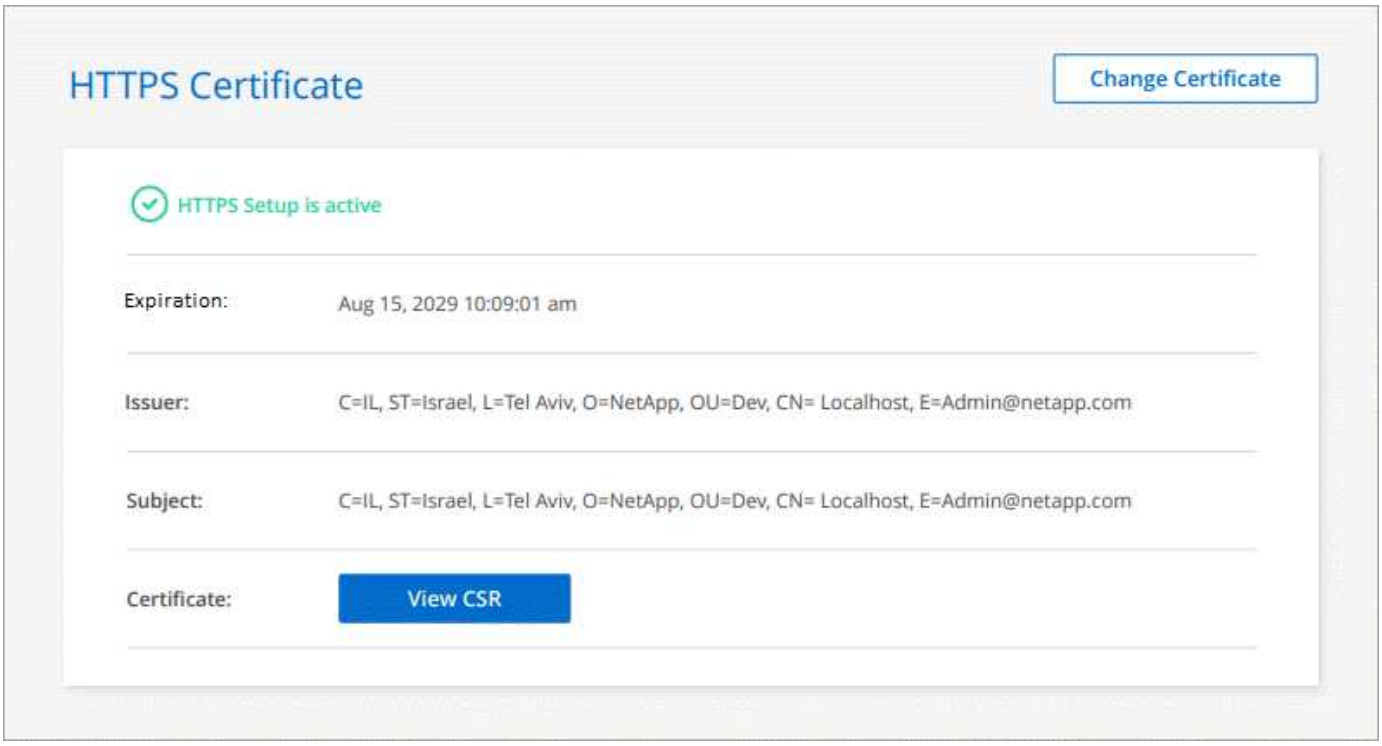
1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **HTTPS Setup**.

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

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**.

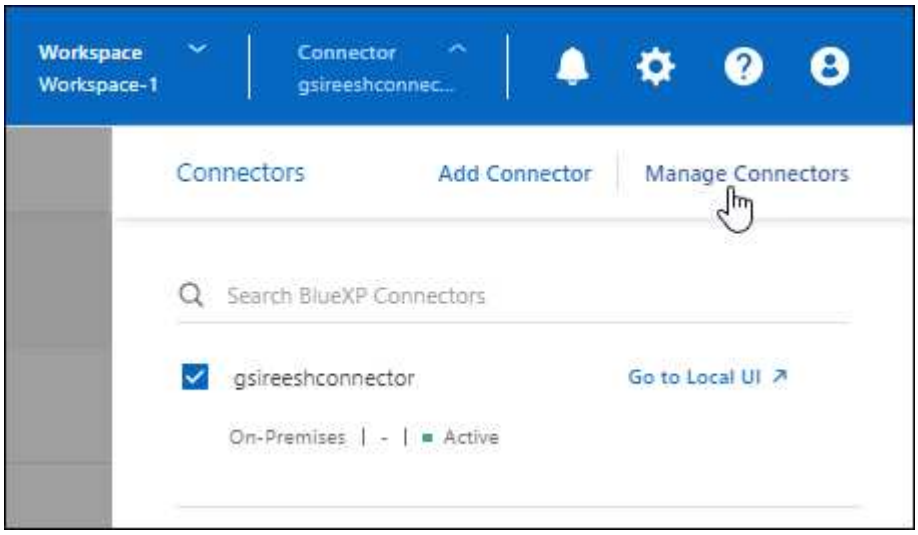
   La navigation dépend de si vous utilisez BlueXP en mode standard (accès à l'interface BlueXP depuis le

site web SaaS) ou BlueXP en mode restreint ou privé (accès à l’interface BlueXP en local depuis l’hôte Connector).

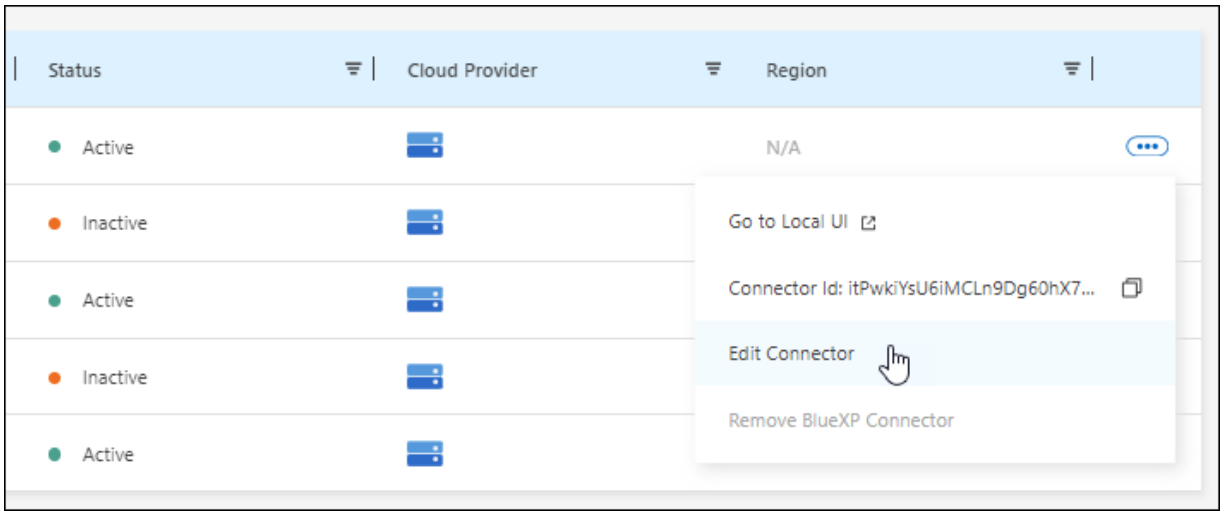
Mode standard

a. Sélectionnez la liste déroulante **Connector** dans l'en-tête BlueXP.

b. Sélectionnez **gérer les connecteurs**.



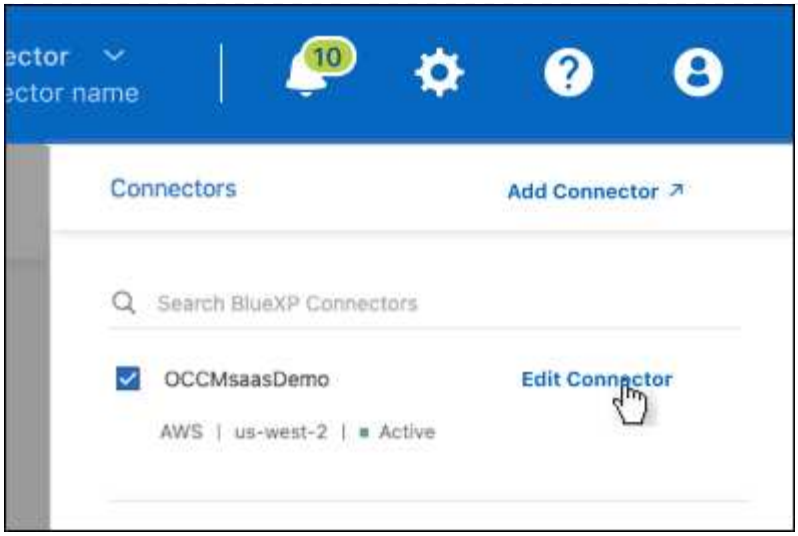
c. Sélectionnez le menu d'action d'un connecteur et sélectionnez **Modifier le connecteur**.



Mode restreint ou privé

a. Sélectionnez la liste déroulante **Connector** dans l'en-tête BlueXP.

b. 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 comprenant 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

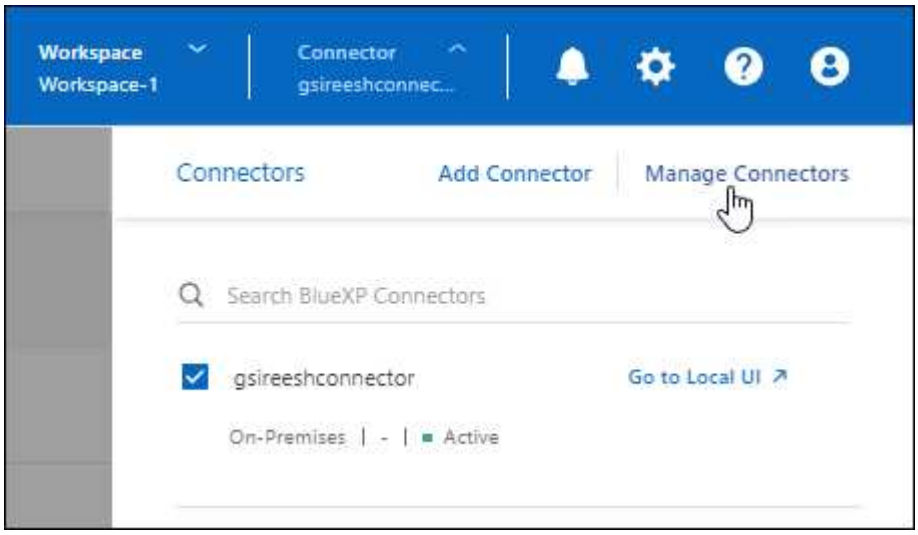
1. Accédez à la page **Edit BlueXP Connector** :

   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).

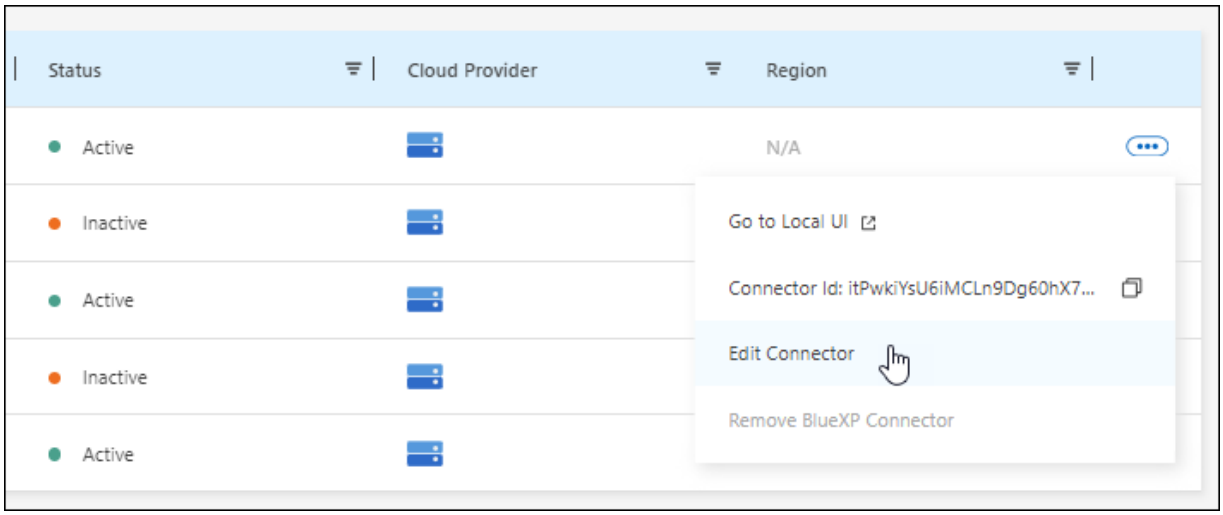
Mode standard

a. Sélectionnez la liste déroulante **Connector** dans l'en-tête BlueXP.

b. Sélectionnez **gérer les connecteurs**.



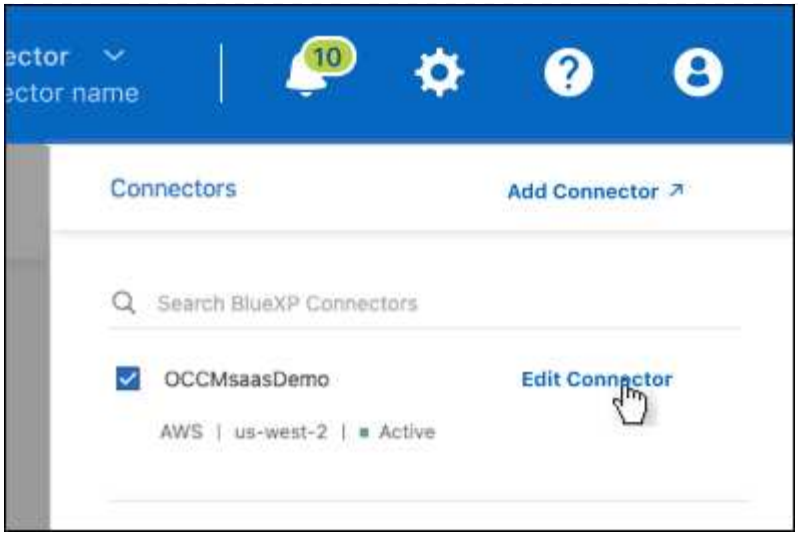
c. Sélectionnez le menu d'action d'un connecteur et sélectionnez **Modifier le connecteur**.



Mode restreint ou privé

a. Sélectionnez la liste déroulante **Connector** dans l'en-tête BlueXP.

b. 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